



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 6.5.0 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)

© 2015–2019 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 バージョン 6.5.0 の新機能 2

システムへのログイン 13

ユーザ ロールで表示および実行可能な対象の制御 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 17

システムの設定 17

インターフェイスの接続 18

ASA 5508-X および 5516-X の配線 18

ASA 5525-X、5545-X、および 5555-X の配線 19

Firepower 1010 のケーブル配線 20

Firepower 1120、1140 のケーブル配線 21

Firepower 2100の配線 22

Firepower 4100 のケーブル配線 23

Firepower 9300 のケーブル配線 24

仮想ケーブル接続 : Firepower Threat Defense Virtual 25

ISA 3000 のケーブル配線 27

初期設定の完了 28

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 31

初期設定前のデフォルト設定 32

初期セットアップ後の設定 35

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
ルールまたはオブジェクトを検索	43
変更の展開	44
インスペクション エンジン を再起動する設定の変更	46
インターフェイスと管理ステータスの表示	47
システム タスク ステータスの表示	48
CLI コンソールを使用した設定の監視およびテスト	49
Firepower Device Manager と REST API の併用	51

第 2 章**Firepower Threat Defense の使用例 53**

Firepower Device Manager でデバイスを設定する方法	53
ネットワーク トラフィックを調べる方法	59
脅威をブロックする方法	67
マルウェアをブロックする方法	74
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	77
アプリケーションの使用を制御する方法	82
サブネットを追加する方法	86
ネットワーク上のトラフィックをパッシブにモニタする方法	93
その他の例	99

第 3 章**システムのライセンス 101**

Firepower システムのスマート ライセンス	101
Cisco Smart Software Manager	101
ライセンス認証局との定期通信	102
スマート ライセンスのタイプ	102
ファイル ポリシーのライセンス要件	104
期限切れまたは無効なオプション ライセンスの影響	105
スマート ライセンスの管理	105
デバイスの登録	107

オプション ライセンスの有効化と無効化 108

Cisco Smart Software Manager との同期 109

デバイスの登録解除 109

第 1 部 : システム モニタリング 111

第 4 章 デバイスのモニタリング 113

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 113

イベント タイプ 113

設定可能な接続ロギング 115

自動接続ロギング 115

接続ロギングのためのヒント 115

外部の Syslog サーバへのイベントの送信 116

Cisco Threat Response などの Cisco Cloud ベースのサービスを使用したイベントの評価 117

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 117

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 121

イベントの表示 121

カスタム ビューの設定 123

イベントのフィルタリング 124

イベント フィールドの説明 125

第 5 章 Cisco ISA 3000 のアラーム 137

アラームについて 137

アラーム入力インターフェイス 138

アラーム出力インターフェイス 138

Syslog アラーム 139

SNMP トラップアラーム 139

アラームのデフォルト 140

ISA 3000 のアラームの設定 140

アラーム入力コンタクトの設定 141

電源アラームの設定 143

温度アラームの設定	145
アラームのモニタリング	147
アラーム ステータスのモニタリング	147
アラームに関する Syslog メッセージのモニタリング	147
外部アラームをオフにする	148

第 II 部 :	再利用可能なオブジェクト	149
----------	--------------	-----

第 6 章	オブジェクト	151
	オブジェクト タイプ	151
	オブジェクトの管理	155
	ネットワーク オブジェクトとグループの設定	156
	ポート オブジェクトとグループの設定	157
	セキュリティ ゾーンの設定	159
	アプリケーション フィルタ オブジェクトの設定	160
	URL オブジェクトとグループの設定	163
	地理位置情報オブジェクトの設定	165
	Syslog サーバの設定	166

第 7 章	証明書	169
	証明書について	169
	公開キー暗号化	170
	各機能で使用される証明書タイプ	170
	例 : OpenSSL を使用した内部証明書の生成	171
	証明書の設定	172
	内部および内部 CA 証明書のアップロード	173
	自己署名内部および内部 CA 証明書の生成	175
	信頼できる CA 証明書のアップロード	176

第 8 章	アイデンティティ ソース	179
	アイデンティティ ソースについて	179

Active Directory (AD) アイデンティティレルム	181
サポートされるディレクトリ サーバ	181
ユーザ数の制限	181
ディレクトリ ベースの DN の決定	182
AD アイデンティティレルムの設定	183
ディレクトリ サーバ接続のトラブルシューティング	186
RADIUS サーバおよびグループ	188
RADIUS サーバの設定	188
RADIUS サーバ グループの設定	190
RADIUS サーバおよびグループのトラブルシューティング	192
Identity Services Engine (ISE)	192
ISE に関する注意事項と制限事項	193
Identity Services Engine の設定	193
ISE/ISE-PIC アイデンティティソースのトラブルシューティング	195
ローカル ユーザ	196
ローカル ユーザの設定	197
<hr/>	
第 III 部 :	基本 199
<hr/>	
第 9 章	Firepower 4100/9300 上の論理デバイス 201
Firepower インターフェイスについて	201
シャーシ管理インターフェイス	201
インターフェイス タイプ	202
シャーシとアプリケーションの独立したインターフェイスの状態	202
Firepower 9300 ハードウェアとソフトウェアの組み合わせの要件と前提条件	203
論理デバイスに関する注意事項と制約事項	203
Firepower インターフェイスに関する注意事項と制約事項	204
一般的なガイドラインと制限事項	204
インターフェイスの設定	204
インターフェイスの有効化または無効化	205
物理インターフェイスの設定	205

EtherChannel (ポート チャネル) の追加	205
論理デバイスの設定	206
FDM 用スタンドアロン Firepower Threat Defense の追加	207
ハイ アベイラビリティ ペアの追加	207
Firepower Threat Defense 論理デバイスのインターフェイスの変更	208
アプリケーションのコンソールへの接続	212
Firepower 4100/9300 論理デバイスの履歴	213

第 10 章

ハイ アベイラビリティ (フェールオーバー)	215
ハイ アベイラビリティ (フェールオーバー) について	215
アクティブ/スタンバイ フェールオーバーについて	216
プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス	216
起動時のアクティブ装置の判別	216
フェールオーバー イベント	216
フェールオーバー リンクとステートフルフェールオーバー リンク	218
フェールオーバー リンク	218
ステートフルフェールオーバー リンク	219
フェールオーバー リンクとステート リンクのインターフェイス	219
フェールオーバーおよびステートフルフェールオーバー インターフェイスの接続	220
フェールオーバー リンクとデータ リンクの中断の回避	220
ステートフルフェールオーバーがユーザ接続に与える影響	222
サポートされる機能	222
サポートされない機能	224
スタンバイ装置で許可される設定の変更とアクション	224
ハイ アベイラビリティのシステム要件	225
HA のハードウェア要件	225
HA のソフトウェア要件	225
HA のライセンス要件	226
ハイ アベイラビリティのガイドライン	227
ハイ アベイラビリティの設定	229
2 台の装置でのハイ アベイラビリティの準備	230

ハイ アベイラビリティ用のプライマリ装置の設定	232
ハイ アベイラビリティ用のセカンダリ装置の設定	235
ヘルスマonitoringのフェールオーバー基準の設定	236
ピア装置のヘルスマonitoring フェールオーバー基準の設定	237
インターフェイスのヘルスマonitoring フェールオーバー基準の設定	238
システムがインターフェイスヘルスをテストする方法	241
スタンバイ IP および MAC アドレスの設定	242
ハイ アベイラビリティ設定の確認	243
ハイ アベイラビリティの管理	244
ハイ アベイラビリティの中断または再開	246
ハイ アベイラビリティの破棄	247
アクティブ ピアとスタンバイ ピアの切り替え (強制フェールオーバー)	248
フェールオーバー後の未展開の設定変更の保持	249
ハイ アベイラビリティ モードでのライセンスと登録の変更	250
HA IPsec 暗号キーまたは HA 設定の編集	250
障害のある装置の正常な装置としてのマーキング	251
HA デバイスでのソフトウェア アップグレードのインストール	251
HA デバイスをアップグレードする際の変更の展開	254
ハイ アベイラビリティ ペアでの装置交換	254
ハイ アベイラビリティのモニタ	255
フェールオーバーの全般的なステータスと履歴のモニタリング	255
HA モニタ対象インターフェイスのステータスのモニタリング	257
HA 関連の Syslog メッセージのモニタリング	258
ピア装置での CLI コマンドのリモート実行	258
ハイ アベイラビリティ (フェールオーバー) のトラブルシューティング	259
装置の障害状態のトラブルシューティング	261
HA アプリケーション同期障害のトラブルシューティング	262
<hr/>	
第 11 章	インターフェイス 267
	FTD インターフェイスについて 267
	インターフェイス モード 268

管理/診断インターフェイス	269
個別の管理ネットワークの設定に関する推奨事項	270
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	270
セキュリティ ゾーン	271
IPv6 アドレス指定	271
Auto-MDI/MDIX 機能	272
インターフェイスに関する注意事項と制限事項	272
インターフェイス設定の制限事項	272
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	273
物理インターフェイスの設定	274
ブリッジ グループの設定	279
EtherChannel の設定	284
EtherChannel について	284
チャネル グループ インターフェイス	284
別のデバイスの EtherChannel への接続	285
リンク集約制御プロトコル	286
ロード バランシング	286
EtherChannel MAC アドレス	287
EtherChannel インターフェイスのガイドライン	287
EtherChannel の追加	289
VLAN インターフェイスおよびスイッチポートの設定 (Firepower 1010)	294
Firepower 1010 ポートおよびインターフェイスについて	294
Firepower 1010 スイッチ ポートの注意事項と制約事項	295
VLAN インターフェイスの設定	296
スイッチ ポートのアクセス ポートとしての設定	301
スイッチ ポートのトランク ポートとしての設定	304
Power over Ethernet の設定	306
VLAN サブインターフェイスと 802.1Q トランキングの設定	308
パッシブ インターフェイスの設定	313
パッシブ インターフェイスを使用する理由	314
パッシブ インターフェイスの制限	315

ハードウェア Firepower 脅威デバイス パッシブ インターフェイスのスイッチの設定	315
Firepower Threat Defense Virtual パッシブ インターフェイスの VLAN の設定	316
パッシブ モードでの物理インターフェイスの設定	317
高度なインターフェイス オプションの設定	318
MAC アドレスについて	318
MTU について	319
パス MTU ディスカバリ	319
MTU およびフラグメンテーション	319
MTU とジャンボ フレーム	320
詳細オプションの設定	320
インターフェイスの変更のスキャンとインターフェイスの移行	323
インターフェイスのスキャンと移行について	323
インターフェイスのスキャンと移行に関する注意事項と制限事項	325
インターフェイスのスキャンと移行	326
ISA 3000 のハードウェア バイパスの設定	329
停電時の自動ハードウェア バイパスの設定 (ISA 3000)	330
ハードウェア バイパス (ISA 3000) を手動で起動	331
モニタリング インターフェイス	332
インターフェイスの例	333

第 12 章

ルーティング 335

ルーティングの概要	335
ルート タイプ	335
ルーティング テーブルとルート選択	336
ルーティング テーブルへの入力方法	336
転送の決定方法	339
管理トラフィック用ルーティングテーブル	340
等コスト マルチパス (ECMP) ルーティング	341
スタティック ルート	341
スタティック ルートとデフォルト ルートについて	341
Default Route	342

スタティック ルート	342
スタティック ルートのバックアップとスタティック ルートのトラッキング	342
スタティック ルーティングのガイドライン	343
スタティック ルートの設定	344
SLA モニタ オブジェクトの設定	346
ルーティングのモニタリング	347

第 IV 部 : **セキュリティ ポリシー** **349**

第 13 章 **SSL 復号** **351**

SSL 復号について	351
SSL 復号を実装する理由	352
暗号化されたトラフィックに適用できるアクション	352
再署名の復号	352
既知のキーの復号	353
復号禁止	354
ブロック	354
自動的に生成された SSL 復号ルール	354
復号できないトラフィックの処理	354
SSL 復号のためのライセンス要件	355
SSL 復号のガイドライン	355
SSL 復号ポリシーの実装および管理方法	356
SSL 復号ポリシーの設定	358
SSL 復号ポリシーの有効化	360
SSL 復号のデフォルト アクションの設定	361
SSL 復号ルールの設定	362
SSL 復号ルールの送信元/送信先基準	364
SSL 復号ルールのアプリケーション基準	366
SSL 復号ルールの URL 基準	367
SSL 復号ルールのユーザ基準	368
SSL 復号ルールの詳細条件	369

既知のキーと復号の再署名の証明書の設定	370
再署名の復号ルールの CA 証明書のダウンロード	371
例：ネットワークからの古い SSL/TLS バージョンのブロック	373
SSL 復号のモニタリングとトラブルシューティング	375
SSL 復号のモニタリング	375
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)	376

 第 14 章

アイデンティティ ポリシー 379

アイデンティティ ポリシーの概要	379
パッシブ認証によるユーザ アイデンティティの確立	380
アクティブ認証によるユーザ ID の確立	380
不明なユーザの対処	380
アイデンティティ ポリシーを実装する方法	381
アイデンティティ ポリシーの設定	382
アイデンティティ ポリシーの設定	383
アイデンティティ ポリシーのデフォルトアクションの設定	385
アイデンティティ ルールの設定	386
トランスペアレント ユーザ認証の有効化	390
トランスペアレント認証の要件	391
トランスペアレント認証用の Internet Explorer の設定	391
トランスペアレント認証用の Firefox の設定	393
アイデンティティ ポリシーのモニタリング	394
アイデンティティ ポリシーの例	394

 第 15 章

セキュリティ インテリジェンス 395

セキュリティ インテリジェンスについて	395
ブラックリストの例外の作成	396
セキュリティ インテリジェンス フィード カテゴリ	396
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	397
セキュリティ インテリジェンスの設定	397

セキュリティ インテリジェンスのモニタリング 399

セキュリティ インテリジェンスの例 399

第 16 章

アクセス制御 401

アクセス コントロールの概要 401

アクセス コントロール ルールとデフォルト アクション 401

アプリケーション フィルタリング 402

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 402

Common Industrial Protocol (CIP) および Modbus アプリケーション (ISA 3000) でのフィ
ルタリング 403

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 403

URL フィルタリング 404

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 404

カテゴリとレピュテーションでの URL の検索 405

手動 URL フィルタリング 405

HTTPS トラフィックのフィルタリング 406

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 408

効果的な URL フィルタリングのベスト プラクティス 408

Web サイトのブロック時にユーザに表示される内容 409

侵入、ファイル、マルウェアのインスペクション 410

アクセス制御ルールの順序のベスト プラクティス 411

NAT とアクセス ルール 411

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 411

アクセス制御のためのライセンス要件 412

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 412

アクセス コントロール ポリシーを設定する 415

デフォルト アクションの設定 416

アクセス コントロール ルールの設定 416

送信元/宛先基準 418

アプリケーション基準 420

URL 基準 422

ユーザ基準	424
侵入ポリシーの設定	425
ファイルポリシーの設定	426
ロギングの設定	427
アクセスコントロールポリシーのモニタリング	429
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	429
ルールヒットカウンターの調査	430
アクセス制御に関する Syslog メッセージのモニタリング	431
CLI でのアクセスコントロールポリシーのモニタリング	431
アクセス制御の例	432
Trustsec セキュリティグループタグを使用したネットワークアクセスの制御方法	432
セキュリティグループタグ (SGT) について	432
セキュリティグループタグ (SGT) に基づくアクセス制御の設定	433

第 17 章

侵入ポリシー 451

侵入ポリシーとネットワーク分析ポリシーについて	451
システム定義のネットワーク分析および侵入ポリシー	452
侵入ルールおよびプリプロセッサルール	453
侵入ルール属性	453
デフォルトの侵入変数セット	454
ジェネレータ識別子	455
ネットワーク分析ポリシー	457
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	457
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	459
侵入ポリシーのためのライセンス要件	459
侵入ポリシーの管理	460
アクセス制御ルールでの侵入ポリシーの適用	460
侵入ルールのアクションの変更	461
侵入イベントの Syslog の設定	462
侵入ポリシーのモニタリング	463
侵入ポリシーの例	463

第 18 章	ネットワーク アドレス変換 (NAT)	465
	NAT を使用する理由	465
	NAT の基本	466
	NAT の用語	466
	NAT タイプ	467
	ルーテッド モードの NAT	467
	自動 NAT および 手動 NAT	468
	自動 NAT	468
	手動 NAT	469
	自動 NAT と 手動 NAT の比較	469
	NAT ルールの順序	470
	NAT インターフェイス	472
	NAT のルーティング設定	473
	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	473
	一意のネットワーク上のアドレス	473
	実際のアドレスと同じアドレス (アイデンティティ NAT)	473
	NAT のガイドライン	474
	インターフェイスのガイドライン	474
	IPv6 NAT のガイドライン	474
	IPv6 NAT のベスト プラクティス	475
	インスペクション対象プロトコルに対する NAT サポート	475
	NAT のその他のガイドライン	477
	NAT の設定	479
	ダイナミック NAT	480
	ダイナミック NAT について	480
	ダイナミック NAT の欠点と利点	481
	ダイナミック自動 NAT の設定	482
	ダイナミック手動 NAT の設定	483
	ダイナミック PAT	486
	ダイナミック PAT について	486

ダイナミック PAT の欠点と利点	487
ダイナミック自動 PAT の設定	488
ダイナミック手動 PAT の設定	489
スタティック NAT	492
スタティック NAT について	492
スタティック自動 NAT の設定	496
スタティック手動 NAT の設定	499
アイデンティティ NAT	502
アイデンティティ自動 NAT の設定	503
アイデンティティ手動 NAT の設定	505
Firepower Threat Defense の NAT ルール プロパティ	508
自動 NAT のパケット変換プロパティ	508
手動 NAT のパケット変換プロパティ	510
詳細 NAT プロパティ	512
IPv6 ネットワークの変換	513
NAT64/46 : IPv6 アドレスの IPv4 への変換	514
NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット	514
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	516
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換	521
NAT66 の例 : ネットワーク間のスタティック変換	522
NAT66 の例 : シンプルな IPv6 インターフェイス PAT	524
NAT のモニタリング	528
NAT の例	528
内部 Web サーバへのアクセスの提供 (スタティック自動 NAT)	528
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)	531
宛先に応じて異なる変換 (ダイナミック手動 PAT)	538
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)	543
NAT を使用した DNS クエリと応答の書き換え	549
DNS 64 応答修正	550

DNS 応答修正：外部の DNS サーバ	556
DNS 応答修正：ホスト ネットワーク上の DNS サーバ	560

第 V 部：	バーチャル プライベート ネットワーク (VPN)	563
--------	---------------------------	-----

第 19 章	サイト間 VPN	565
--------	----------	-----

VPN の基本	565
インターネット キー エクスチェンジ (IKE)	566
VPN 接続の安全性を確保する方法	567
使用する暗号化アルゴリズムの決定	567
使用するハッシュ アルゴリズムの決定	568
使用する Diffie-Hellman 係数グループの決定	569
使用する認証方式の決定	570
VPN トポロジ	571
動的にアドレス指定されたピアによるサイト間 VPN 接続の確立	571
サイト間 VPN の管理	572
サイト間 VPN 接続の設定	573
サイト間 VPN 経路によるトラフィックの許可	577
グローバル IKE ポリシーの設定	577
IKEv1 ポリシーの設定	579
IKEv2 ポリシーの設定	580
IPsec プロポーザルの設定	583
IKEv1 の IPsec プロポーザルの設定	583
IKEv2 の IPsec プロポーザルの設定	585
サイト間 VPN 接続の確認	586
サイト間 VPN のモニタリング	589
サイト間 VPN の例	589
NAT からのサイト間 VPN トラフィックの除外	589
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)	596

第 20 章

リモート アクセス VPN 605

リモート アクセス VPN の概要 605

デバイス モデル別の同時 VPN セッションの最大数 605

AnyConnect クライアント ソフトウェアのダウンロード 606

AnyConnect ソフトウェアのインストール方法 607

RADIUS およびグループ ポリシーを使用したユーザの権限および属性の制御 608

RADIUS サーバに送信された属性 608

RADIUS サーバから受信した属性 609

二要素認証 610

RSA 二要素認証 610

RADIUS を使用した Duo 二要素認証 611

LDAP を使用した Duo 二要素認証 612

リモート アクセス VPN のライセンス要件 612

リモート アクセス VPN に関する注意事項と制限事項 613

リモート アクセス VPN の設定 613

クライアント プロファイルの設定およびアップロード 615

リモート アクセス VPN によるトラフィックの許可 617

リモート アクセス VPN 設定の確認 617

リモート アクセス VPN 設定の管理 619

RA VPN 接続プロファイルの設定 620

接続プロファイルのための AAA の設定 624

接続プロファイルのための証明書認証の設定 627

RA VPN のクライアント アドレス指定の設定 627

RA VPN のグループ ポリシーの設定 628

一般属性 629

セッション設定属性 630

アドレス割り当て属性 631

スプリット トンネリング属性 631

AnyConnect 属性 633

トラフィック フィルタ属性 634

Windows ブラウザ プロキシ属性	635
リモート アクセス VPN のモニタリング	636
リモート アクセス VPN のトラブルシューティング	636
SSL 接続問題のトラブルシューティング	636
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	637
AnyConnect 接続問題のトラブルシューティング	637
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	638
リモート アクセス VPN の例	639
RADIUS 認可変更の実装方法	639
認可変更へのシステム フロー	640
FTD デバイスでの認可変更の設定	641
ISE での認可変更の設定	645
Duo LDAP を使用した二要素認証の設定方法	649
Duo LDAP セカンダリ認証のシステム フロー	649
Duo LDAP セカンダリ認証の設定	650
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)	658
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	663
グループによって RA VPN アクセスを制御する方法	679

第 VI 部 : システム管理 685

第 21 章 システム設定 687

管理アクセスの設定	687
管理アクセス リストの設定	688
Firepower Device Manager Web サーバ証明書の設定	690
システム ログिंगの設定	690
重大度	691
リモート syslog サーバのログिंगの設定	691
内部バッファへのログिंगの設定	693
コンソールへのログिंगの設定	694

イベントリストフィルタの設定	695
DHCP サーバの設定	696
DNS の設定	698
DNS グループの設定	698
データと管理インターフェイスの DNS の設定	700
DNS の一般的な問題のトラブルシューティング	702
管理インターフェイスの設定	703
デバイスのホスト名の設定	705
Network Time Protocol (NTP) の設定	706
URL フィルタリングの設定	707
クラウドサービスの設定	708
クラウド管理の設定 (Cisco Defense Orchestrator)	708
Cisco Success Network への接続	709
シスコクラウドサービスの登録の無効化	710
Web 分析の有効化と無効化	711
Cisco Cloud へのイベントの送信	712

第 22 章
システム管理 713

ソフトウェアアップデートのインストール	713
システム データベースおよびフィードの更新	713
システム データベースおよびフィードの更新の概要	713
システム データベースの更新	715
Cisco Security Intelligence フィードの更新	716
Firepower Threat Defenseソフトウェアのアップグレード	717
デバイスの再イメージ化	719
システムのバックアップと復元	720
システムの即時バックアップ	721
スケジュールされた時間でのシステムのバックアップ	721
定期的なバックアップ スケジュールの設定	722
バックアップの復元	723
ISA 3000 デバイスの交換	725

バックアップ ファイルの管理	725
監査と変更管理	726
監査イベント	726
監査ログの表示および分析	728
監査ログのフィルタリング	729
展開およびエンティティ変更履歴の確認	731
保留中の全変更の廃棄	732
デバイス設定のエクスポート	733
FDM および FTD ユーザ アクセスの管理	734
FDM (HTTPS) ユーザ用の外部認証 (AAA) 設定	734
FTD CLI (SSH) ユーザ用の外部認証 (AAA) 設定	736
Firepower Device Manager ユーザ セッションの管理	738
外部ユーザ用のスタンバイ HA ユニットでの FDM アクセスの有効化	738
FTD CLI のローカル ユーザ アカウントの作成	739
システムの再起動またはシャットダウン	741
システムのトラブルシューティング	742
接続をテストするための ping アドレス	742
ホストまでのルートの追跡	744
Firepower Threat Defense デバイスのトレースルートへの表示	746
NTP のトラブルシューティング	747
管理インターフェイスの DNS のトラブルシューティング	749
CPU およびメモリ使用率の分析	752
ログの表示	753
トラブルシューティング ファイルの作成	755
一般的でない管理タスク	755
ローカル管理とリモート管理の切り替え	755
ファイアウォール モードの変更	758
設定のリセット	762

付録 A :

詳細設定	765
Smart CLI と FlexConfig について	765

Smart CLI と FlexConfig の推奨される使用法	766
Smart CLI および FlexConfig オブジェクトの CLI コマンド	767
ソフトウェアのアップグレードが FlexConfig ポリシーに与える影響	767
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	768
禁止された CLI コマンド	768
Smart CLI テンプレート	775
Smart CLI および FlexConfig に関する注意事項と制限事項	776
Smart CLI オブジェクトの設定	776
FlexConfig ポリシーの設定	779
FlexConfig オブジェクトの設定	780
FlexConfig オブジェクトの変数の作成	783
FlexConfig 変数の参照と値の取得	784
変数参照 : {{variable}} または {{{variable}}}	784
セクション {{#key}} {{/key}} と逆セクション {{^key}} {{/key}}	788
FlexConfig オブジェクト内の Smart CLI オブジェクトの参照	790
秘密キー オブジェクトの設定	791
FlexConfig ポリシーのトラブルシューティング	792
FlexConfig の例	793
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	793
FlexConfig の変更を元に戻す方法	799
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	801
高精度時間プロトコルの設定方法 (ISA 3000)	805



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 バージョン 6.5.0 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](#) (17 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。

クラウドベースのアプリケーションである Cisco Defense Orchestrator を使用して、1 つまたは複数のデバイスを管理することもできます。クラウド管理の方法については、<https://youtu.be/fsIfsHhnpQU> でビデオを視聴し、Cisco Defense Orchestrator ポータル (<http://www.cisco.com/go/cdo>) を熟読してください。製品マニュアルは <https://docs.defenseorchestrator.com/> で検索できます。Cisco Defense Orchestrator へのデバイスの接続の詳細については、[クラウド管理の設定 \(Cisco Defense Orchestrator\)](#) (708 ページ) を参照してください。

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 1010、1120、1140	6.4
Firepower 1150	6.5
Firepower 2110、2120、2130、2140	6.2.1
Firepower 4110、4115、4120、4125、4140、4145、4150	6.5
Firepower 9300	6.5
Firepower Threat Defense Virtual VMware 用	6.2.2
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
Firepower Threat Defense Virtual Microsoft Azure クラウド用	6.5
ASA 5508-X、5516-X	6.1
ASA 5525-X、5545-X、5555-X	6.1
ASA 5515-X (注) ASA 5515-X のサポートは 6.4 (許可される最後のバージョン) で終了します。このモデルにバージョン 6.5 以降をインストールすることはできません。	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 バージョン 6.5.0 の新機能

リリース : 2019 年 9 月 26 日

次の表は、Firepower Device Manager を使用して設定した場合に、FTD 6.5.0 で使用可能な新機能を示しています。

機能	説明
Firepower 4100/9300 の FDM のサポート。	FDM を使用して Firepower 4100/9300 で Firepower Threat Defense を設定できるようになりました。ネイティブ インスタンスのみがサポートされています。コンテナ インスタンスはサポートされていません。

機能	説明
Microsoft Azure クラウド用 Firepower Threat Defense Virtual の FDM のサポート。	Firepower Device Manager を使用して Microsoft Azure クラウド用 Firepower Threat Defense Virtual で Firepower Threat Defense を設定できます。
Firepower 1150 のサポート。	Firepower 1150 用の FTD が導入されました。
Firepower 1010 ハードウェア スイッチのサポート、PoE+ のサポート。	<p>Firepower 1010 では、各イーサネット インターフェイスをスイッチポートまたは通常のファイアウォールインターフェイスとして設定できます。各スイッチポートを VLAN インターフェイスに割り当てます。Firepower 1010 は、Ethernet1/7 および Ethernet 1/8 での Power over Ethernet+ (PoE+) もサポートしています。</p> <p>デフォルト設定で、Ethernet1/1 が外部として設定され、Ethernet1/2 ~ 1/8 が内部 VLAN1 インターフェイスのスイッチポートとして設定されるようになりました。バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。</p>
インターフェイスのスキャンと置き換え。	インターフェイス スキャンでは、シャージで追加、削除、または復元されたインターフェイスが検出されます。設定で古いインターフェイスを新しいインターフェイスに置き換えることもできるため、インターフェイスの変更がシームレスに行えます。
インターフェイス表示の向上。	[デバイス (Device)]>[インターフェイス (Interfaces)] ページの構成が改められました。物理インターフェイス、ブリッジグループ、Etherchannel、および VLAN 用のタブが別々に設けられました。任意の対象デバイス モデルについて、モデルに関連するタブのみが表示されます。たとえば、[VLAN] タブは Firepower 1010 モデルでのみ使用できます。また、各インターフェイスの設定と使用方法に関する詳細情報がリストに表示されます。

機能	説明
ISA 3000 の新しいデフォルト設定。	<p>ISA 3000 のデフォルト設定が次のように変更されました。</p> <ul style="list-style-type: none"> • すべてのインターフェイスが BV11 のブリッジグループメンバーとなりました。BV11 には名前が付いていないため、ルーティングには参加しません。 • GigabitEthernet1/1 および 1/3 は外部インターフェイスとなり、GigabitEthernet1/2 および 1/4 は内部インターフェイスとなります。 • 内部/外部ペアごとにハードウェアバイパスが有効になります（使用可能な場合）。 • すべてのトラフィックについて、内部から外部、および外部から内部が許可されます。 <p>バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。</p>
ASA 5515-X のサポート終了。最後にサポートされるリリースは FTD 6.4。	<p>ASA 5515-X に FTD 6.5 をインストールすることはできません。ASA 5515-X 用に最後にサポートされるリリースは FTD 6.4 です。</p>
Cisco ISA 3000 デバイスのアクセス制御ルールにおける Common Industrial Protocol (CIP) および Modbus アプリケーションフィルタリングのサポート。	<p>Cisco ISA 3000 デバイスで Common Industrial Protocol (CIP) および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write というように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。</p> <p>プリプロセッサを有効にするには、CLI セッション (SSH またはコンソール) でエキスパート モードに移行し、sudo /usr/local/sf/bin/enable_scada.sh {cip modbus both} コマンドを発行する必要があります。展開のたびに展開後にプリプロセッサがオフになるため、展開のたびにこのコマンドを発行する必要があります。</p>

機能	説明
<p>ISA 3000 デバイスの高精度時間プロトコル (PTP) の設定。</p>	<p>FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル (PTP) を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。</p> <p>FlexConfig オブジェクトに、ptp および igmp (インターフェイスモード) コマンド、およびグローバルコマンド ptp mode e2transparent と ptp domain を追加できるようになりました。また、FTD CLI に show ptp コマンドが追加されました。</p>
<p>EtherChannel (ポート チャネル) インターフェイス。</p>	<p>EtherChannel インターフェイス (ポート チャネルとも呼ばれます) を設定できます。</p> <p>(注) FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス (Interfaces)] ページに表示されます。</p> <p>[デバイス (Device)] > [インターフェイス (Interfaces)] ページが更新され、EtherChannel の作成ができるようになりました。</p>
<p>FDM からシステムを再起動およびシャットダウンする機能。</p>	<p>新しい [再起動/シャットダウン (Reboot/Shutdown)] システム設定ページからシステムを再起動またはシャットダウンできるようになりました。以前は、FDM の CLI コンソールを使用して、あるいは SSH または コンソールセッションから、reboot および shutdown コマンドを発行する必要がありました。これらのコマンドを使用するには、管理者権限が必要です。</p>
<p>FDM CLI コンソールでの failover コマンドのサポート。</p>	<p>FDM CLI コンソールを使用して failover コマンドを発行できるようになりました。</p>
<p>スタティック ルート用のサービス レベル契約 (SLA) モニタ。</p>	<p>スタティックルートとともに使用するためのサービスレベル契約 (SLA) モニタオブジェクトを設定します。SLA モニタを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。SLA モニタオブジェクトを選択できるように、[オブジェクト (Object)] ページに [SLA モニタ (SLA Monitors)] を追加し、スタティックルートを更新しました。</p>

機能	説明
Smart CLI および FTD API でのルーティングの変更。	<p>今回のリリースには、Smart CLI および FTD API でのルーティング設定に対していくつかの変更が追加されています。以前のリリースでは、BGP 用として単一の Smart CLI テンプレートがありました。今回は、BGP（ルーティングプロセス設定）用と BGP 一般設定（グローバル設定）用に別々のテンプレートが用意されました。</p> <p>FTD API では、新しい BGP 一般設定のメソッドを除いて、すべてのメソッドのパスが変更され、パスに「/virtualrouter」が挿入されました。</p> <ul style="list-style-type: none"> • スタティックルートメソッドのパスは、以前は /devices/default/routing/{parentId}/staticrouteentries でしたが、今後は /devices/default/routing/virtualrouters/default/staticrouteentries になります。 • BGP メソッドは、/devices/default/routing/bgpgeneralsettings と /devices/default/routing/virtualrouters/default/bgp の 2 つの新しいパスに分割されました。 • OSPF パスは /devices/default/routing/virtualrouters/default/ospf および /devices/default/routing/virtualrouters/default/ospfinterfaceentries になりました。 <p>FTD API を使用してルーティングプロセスを設定している場合は、呼び出しを調べて必要に応じて修正してください。</p>

機能	説明
<p>新しいURLカテゴリおよびレピュテーションデータベース。</p>	<p>システムは、Cisco Talos とは別の URL データベースを使用します。新しいデータベースでは、URL のカテゴリにいくつかの違いがあります。アップグレードすると、もう存在していないカテゴリがアクセス制御や SSL 復号ルールで使用されている場合、システムはそのカテゴリを適切な新しいカテゴリに置き換えます。変更を有効にするには、アップグレード後に設定を展開します。カテゴリの変更についての詳細は、[保留中の変更 (Pending Changes)] ダイアログに表示されます。引き続き希望する結果が得られることを確認するため、URL フィルタリングポリシーを調べる必要がある場合があります。</p> <p>アクセス制御ポリシーと SSL 復号ポリシーの [URL] タブ、および [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)] ページに URL ルックアップ機能を追加しました。この機能を使用すると、特定の URL に割り当てられているカテゴリを確認できます。同意しない場合は、カテゴリの異議を送信するリンクもあります。このどちらの機能も、URL に関する詳細情報を提供する外部 Web サイトを使用します。</p>
<p>セキュリティインテリジェンスでは、ホスト名ではなく IP アドレスを使用する URL 要求に対して IP アドレスの評価を使用する。</p>	<p>HTTP/HTTPS 要求の宛先が、ホスト名ではなく IP アドレスを使用する URL である場合は、ネットワークアドレスリストにある IP アドレスの評価が検索されます。ネットワークおよび URL リストで IP アドレスを重複させる必要はありません。これにより、エンドユーザがプロキシを使用してセキュリティインテリジェンスの評価のブロックを回避することが困難になります。</p>
<p>接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントを Cisco Cloud に送信するためのサポート。</p>	<p>Cisco Cloud サーバにイベントを送信できます。このサーバから、各種のシスコクラウドサービスがイベントにアクセスできます。イベント送信後に、Cisco Threat Response などのクラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。このサービスを有効にすると、デバイスから、接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントがシスコのクラウドに送信されます。</p> <p>[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] にある Cisco Threat Response の項目を「Cisco Cloud にイベントを送信 (Send Events to the Cisco Cloud)」に変更しました。</p>

機能	説明
シスコ クラウドサービスのリージョンサポート。	<p>スマートライセンスへの登録時に、シスコクラウドサービスリージョンの選択が求められるようになりました。このリージョンは、Cisco Defense Orchestrator、Cisco Threat Response、Cisco Success Network、および Cisco Cloud を通過するすべてのクラウド機能で使用されます。登録済みデバイスを以前のリリースからアップグレードすると、自動的に US リージョンに割り当てられます。リージョンを変更する必要がある場合は、スマートライセンスを登録解除して、改めて再登録して新しいリージョンを選択する必要があります。</p> <p>[スマートライセンス (Smart License)] ページと初期デバイスセットアップウィザードで、ライセンス登録プロセスにステップを追加しました。また、[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページでもリージョンを確認できます。</p>
FTD REST API バージョン 4 (v4)。	<p>ソフトウェア バージョン 6.5 用の FTD REST API のバージョン番号が 4 になりました。API の URL の v1/v2/v3 を v4 に置き換える必要があります。v4 の API には、ソフトウェアバージョン 6.5 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソース モデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。</p>

機能	説明
<p>FTD アクセス制御ルールで送信元および宛先の一致基準として使用できる TrustSec セキュリティグループの API サポート。</p>	<p>FTD API を使用して、送信元または宛先のトラフィックの一致基準に TrustSec セキュリティグループを使用したアクセスコントロールポリシールールを設定できます。ISE からセキュリティグループタグ (SGT) のリストがダウンロードされます。SXP の更新がないかリッスンし、スタティック SGT から IP アドレスへのマッピングを取得するように、システムを設定できます。</p> <p>GET /object/securitygrouptag メソッドを使用して、ダウンロードしたタグのリストを表示でき、SGTDynamicObject リソースを使用して 1 つ以上のタグを表す動的オブジェクトを作成できます。この動的オブジェクトをアクセス制御ルールで使用して、送信元または宛先のセキュリティグループに基づくトラフィックの一致基準を定義できます。</p> <p>セキュリティグループに関連する ISE オブジェクトまたはアクセス制御ルールに変更を加えると、FDM でそれらのオブジェクトを編集しても変更が保持されます。ただし、FDM でルールを編集する場合、アクセスルールのセキュリティグループの基準を表示することはできません。API を使用してセキュリティグループに基づくアクセスルールを設定する場合は、その後 FDM を使用してアクセスコントロールポリシーのルールを編集する際に注意が必要です。</p> <p>AccessRule (sourceDynamicObjects および destinationDynamicObjects 属性)、IdentityServicesEngine (subscribeToSessionDirectoryTopic および subscribeToSxpTopic 属性)、SecurityGroupTag、SGTDynamicObject の各 FTD API リソースを追加または変更しました。</p> <p>イベントビューアに、送信元と宛先のセキュリティグループタグと名前を列として追加しました。</p>

機能	説明
FTD API を使用した設定のインポート/エクスポート。	<p>FTD API を使用して、デバイス設定のエクスポートや設定ファイルのインポートが行えます。設定ファイルを編集して、インターフェイスに割り当てられている IP アドレスなどの値を変更できます。こうしたインポート/エクスポートを使用して新しいデバイス用のテンプレートを作成できます。そのため、ベースラインの構成をすばやく適用し、新しいデバイスをより迅速にオンラインにすることができます。デバイスのイメージを再作成した後、インポート/エクスポートを使用して設定を復元することもできます。または、単に一連のネットワーク オブジェクトや他の項目をデバイスのグループに配布する目的で使用することもできます。</p> <p>ConfigurationImportExport のリソースとメソッド (@config, @configlets, @configlets, @configlets, @configlets, @configlets, @configlets) を追加しました。</p>
カスタムファイルポリシーの作成と選択。	<p>FTD API を使用してカスタム ファイル ポリシーを作成し、FDM を使用してアクセス制御ルールでそれらのポリシーを選択することができます。</p> <p>filepolicies、filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections の各 FTD API FileAndMalwarePolicies リソースを追加しました。</p> <p>また、「Block Office Document and PDF Upload, Block Malware Others」と「Block Office Documents Upload, Block Malware Others」の2つの定義済みポリシーを削除しました。これらのポリシーを使用している場合は、ユーザが編集できるようにアップグレード中にユーザ定義のポリシーに変換されます。</p>
FTD API を使用したセキュリティインテリジェンス DNS ポリシーの設定。	<p>FTD API を使用してセキュリティインテリジェンス DNS ポリシーを設定できます。このポリシーはFDMには表示されません。</p> <p>domainnamefeeds、domainnamegroups、domainnamefeedcategories、securityintelligencednspolicies の各 SecurityIntelligence リソースを追加しました。</p>

機能	説明
<p>Duo LDAP を使用したリモートアクセス VPN 二要素認証。</p>	<p>リモートアクセス VPN 接続プロファイルの 2 番目の認証ソースとして Duo LDAP を設定し、Duo パスコード、プッシュ通知、または通話を使用して二要素認証を実現できます。FTD API を使用して Duo LDAP ID ソースオブジェクトを作成する必要がありますが、FDM を使用してそのオブジェクトを RA VPN 接続プロファイルの認証ソースとして選択することができます。</p> <p>duoldapidentitysources のリソースとメソッドを FTD API に追加しました。</p>
<p>FTD リモートアクセス VPN 接続の認可に使用する LDAP 属性マップの API サポート。</p>	<p>カスタムの LDAP 属性マップを使用して、リモートアクセス VPN の LDAP 認証を強化することができます。LDAP 属性マップにより、顧客固有の LDAP 属性名および値がシスコの属性名および値と同等になります。これらのマッピングを使用して、LDAP 属性値に基づいてユーザにグループポリシーを割り当てることができます。これらのマップは FTD API を使用してのみ設定できます。FDM を使用して設定することはできません。ただし、API を使用してこれらのオプションを設定すれば、後で FDM で Active Directory のアイデンティティソースを編集することで設定を保存できます。</p> <p>LdapAttributeMap、LdapAttributeMapping、LdapAttributeToGroupPolicyMapping、LDAPRealm、LdapToCiscoValueMapping、LdapToGroupPolicyValueMapping、RadiusIdentitySource の各 FTD API オブジェクトモデルを追加または変更しました。</p>

機能	説明
<p>FTD サイト間 VPN 接続におけるリバースルートインジェクションとセキュリティアソシエーション (SA) のライフタイムの API サポート。</p>	<p>FTD API を使用して、サイト間 VPN 接続のリバースルートインジェクションを有効にすることができます。逆ルート注入 (RRI) とは、リモートトンネルエンドポイントによって保護されているネットワークおよびホストのルーティングプロセスに、スタティックルートを自動的に組み込む機能です。デフォルトでは、スタティック RRI が有効になっており、接続の設定時にルートが追加されます。ダイナミック RRI は無効になっています。ダイナミック RRI では、セキュリティアソシエーション (SA) が確立されたときのみルートが挿入され、その後 SA が切断されたときにルートが削除されます。ダイナミック RRI は IKEv2 接続でのみサポートされています。</p> <p>また、接続のセキュリティアソシエーション (SA) のライフタイムを秒単位または送信キロバイト単位で設定することもできます。ライフタイムを期限なしに設定することもできます。デフォルトのライフタイムは、28,800 秒 (8 時間) および 4,608,000 キロバイト (10 メガバイト/秒で 1 時間) です。ライフタイムに到達すると、エンドポイントで新しいセキュリティアソシエーションと秘密キーがネゴシエートされます。</p> <p>FDM を使用してこれらの機能を設定することはできません。ただし、API を使用してこれらのオプションを設定すれば、後で FDM で接続プロファイルを編集することで設定を保存できます。</p> <p>dynamicRRIEnabled、ipsecLifetimeInSeconds、ipsecLifetimeInKiloBytes、ipsecLifetimeUnlimited、rriEnabled の各属性を SToSConnectionProfile リソースに追加しました。</p>
<p>IKE ポリシーの Diffie-Hellman グループ 14、15、および 16 のサポート。</p>	<p>Dh グループ 14 を使用するように IKEv2 ポリシーを設定し、DH グループ 14、15、および 16 を使用するように IKEv1 ポリシーを設定できるようになりました。IKEv1 を使用している場合は、グループ 2 と 5 が今後のリリースで削除されるため、すべてのポリシーを DH グループ 14 にアップグレードしてください。また、IKEv2 ポリシーで DH グループ 24 を使用したり、IKE バージョンで MD5 を使用したりしないでください。これらも今後のリリースで削除されます。</p>

機能	説明
変更を展開する際のパフォーマンスの向上。	システムの強化により、アクセス制御ルールを追加、編集、または削除した場合に、以前のリリースと比べて変更がより迅速に展開されるようになりました。 フェールオーバー用のハイアベイラビリティグループに設定しているシステムでは、展開した変更をスタンバイデバイスに同期させるプロセスが改良され、同期がより迅速に完了するようになりました。
システムダッシュボード上のCPUおよびメモリ使用率の計算の改良。	CPUとメモリの使用率を計算する方法が改良され、システムダッシュボードに表示される情報に、デバイスの実際の状態がより正確に反映されるようになりました。
FTD 6.5にアップグレードした場合に履歴レポートデータは使用できなくなる。	既存のシステムをFTD 6.5にアップグレードした場合、データベーススキーマの変更のために履歴レポートデータが使用できなくなります。そのため、アップグレード前の時点における使用状況データはダッシュボードに表示されません。

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。

ユーザ ロールで表示および実行可能な対象の制御

ユーザ名はロールに割り当てられ、Firepower Device Manager で何を実行できるか、また何を表示できるかがユーザ ロールによって決まります。ローカルに定義される [管理者 (admin)] ユーザにはすべての権限がありますが、別のアカウントを使用してログインすると権限が少なくなります。

Firepower Device Manager ウィンドウの右上隅にユーザ名と権限レベルが表示されます。

admin
Administrator 

権限は次のとおりです。

- [管理者 (Administrator)] : すべての機能を表示および使用できます。
- [読み取り/書き込みユーザ (Read-Write User)] : 読み取り専用ユーザが実行できることをすべて実行できます。また、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、他の Firepower Device Manager ユーザセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- [読み取り専用ユーザ (Read-Only User)] : ダッシュボードおよび設定を表示できますが、変更することはできません。変更しようとする、権限がないことを示すエラーメッセージが表示されます。

これらの権限は、CLI ユーザが利用できる権限とは関連していません。

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

最初は、**admin** ユーザ名を使用してのみ Firepower Device Manager にログインできます。ただし、[FDM および FTD ユーザアクセスの管理 \(734 ページ\)](#) に説明されているように、外部 AAA サーバに定義されている追加ユーザの認証は設定できます。

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。ISA 3000 の場合、デフォルトでは管理インターフェイスにのみ接続できます。

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 デバイスに定義されているユーザ名とパスワードを入力し、[ログイン (Login)] をクリックします。

事前定義されたユーザであるユーザ名 **admin** を使用できます。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 2100/4100/9300 デバイスでは、コンソールポートの CLI は FXOS です。Firepower 2100 の場合は、**connect ftd** コマンドを使用して FTD CLI にアクセスできます。Firepower 4100/9300 の場合は、[アプリケーションのコンソールへの接続 \(212 ページ\)](#) を参照してください。FXOS CLI はシャーシ レベルのトラブルシューティングにのみ使用します。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（688 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 Command Reference](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。
- **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。
- 外部サーバで SSH アクセス用のユーザアカウントを作成できます。SSH アクセス用の外部認証の設定については、[FTD CLI（SSH）ユーザ用の外部認証（AAA）設定（736 ページ）](#)を参照してください。

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。

始める前に

この手順は、ローカルユーザにのみ適用されます。ユーザアカウントが外部 AAA サーバで定義されている場合、そのサーバでパスワードを変更する必要があります。

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。

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 \(32 ページ\)](#) 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 (18 ページ)

ステップ2 初期設定の完了 (28 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 \(35ページ\)](#) を参照してください。

インターフェイスの接続

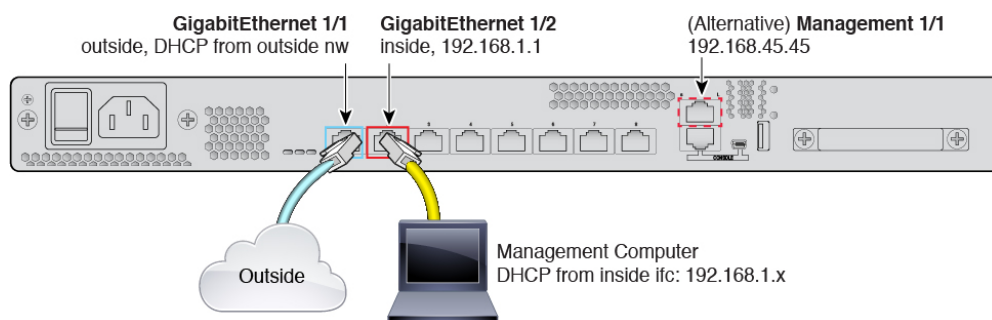
デフォルト設定では、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの前提に基づいてネットワークケーブルをインターフェイスに接続すると、初期設定の実行が容易になります。

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 5508-X および 5516-X の配線



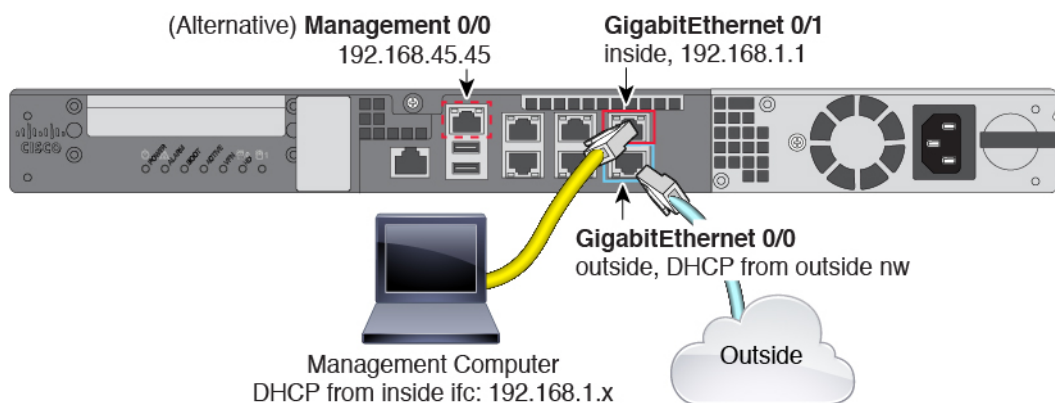
- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。

- 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 5525-X、5545-X、および 5555-X の配線



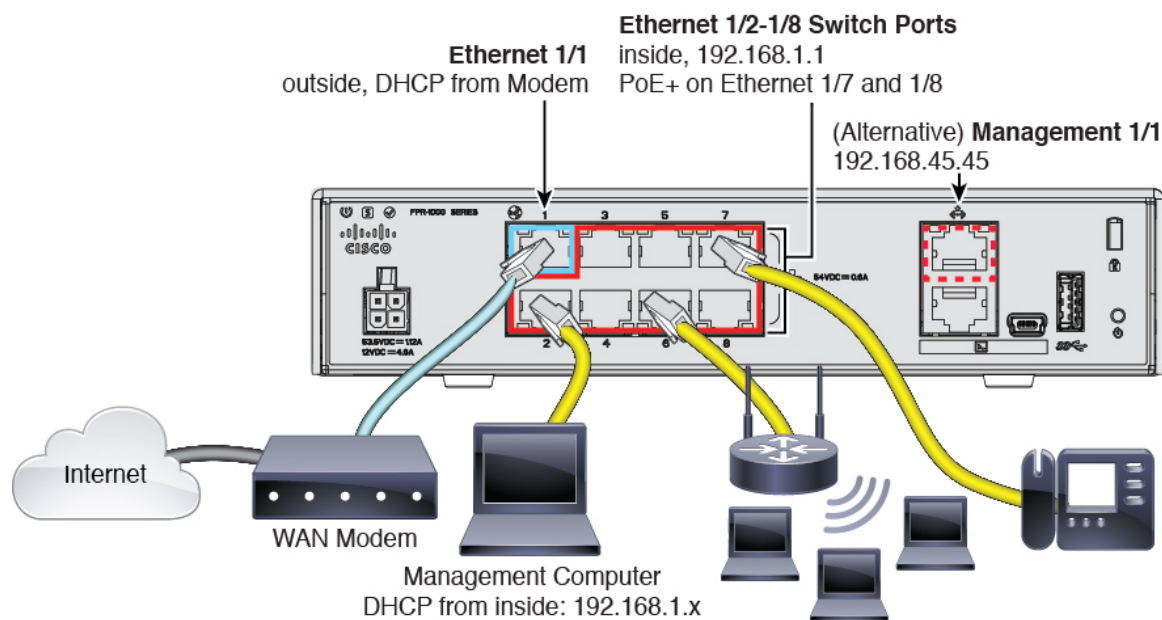
- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 0/0 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティックアドレスを設定することもできます。
- GigabitEthernet 0/1 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



- (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 1010 のケーブル配線

図 1: Firepower 1010 のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
 - Ethernet 1/2 ~ 1/8 : 管理コンピュータをいずれかの内部スイッチポート (Ethernet 1/2 ~ 1/8) に直接接続します。内部にはデフォルトの IP アドレス (192.168.1.1) があり、クライアントに IP アドレスを提供するために DHCP サーバも実行されます (管理コンピュータを含む)。したがって、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
 - Management 1/1 : 管理コンピュータを Management 1/1 に直接接続します。または、Management 1/1 を管理ネットワークに接続します。Management 1/1 にはデフォルトの IP アドレス (192.168.45.45) があり、クライアント (管理コンピュータを含む) に IP

アドレスを提供するためにDHCPサーバも実行されるため、これらの設定が既存の管理ネットワークの設定と競合しないようにしてください。

- 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。

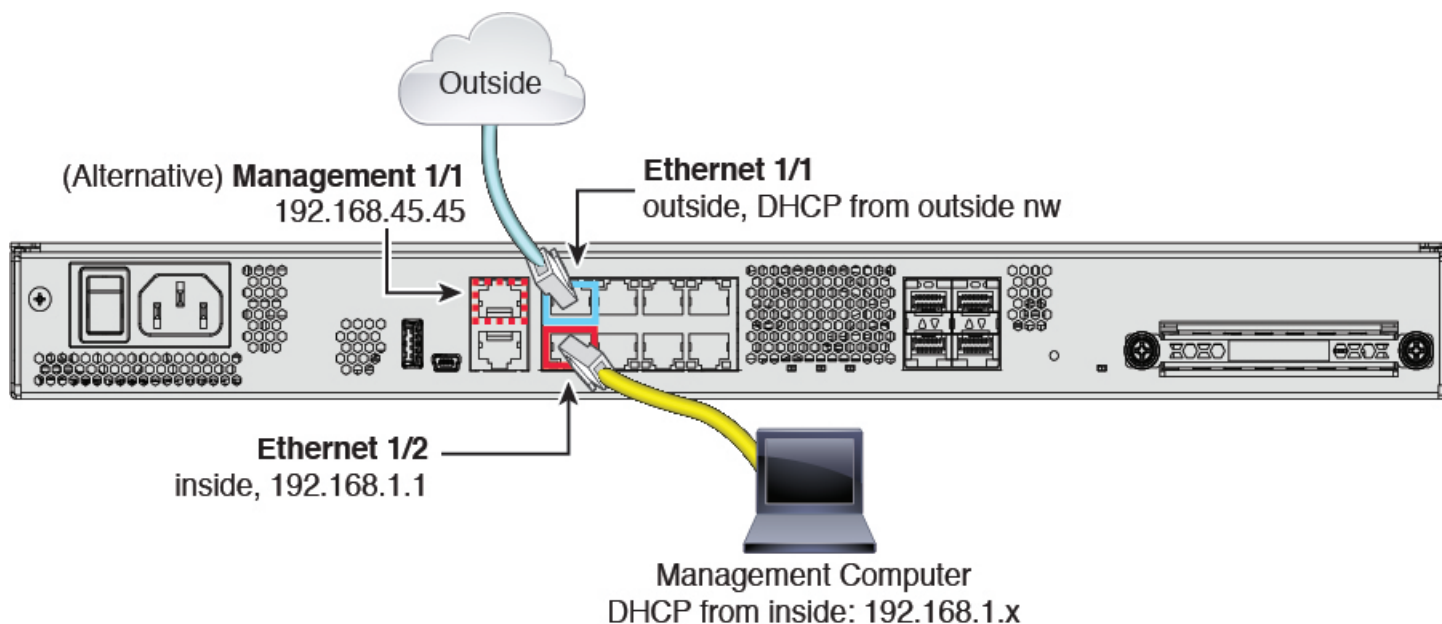
デフォルトでは、IPアドレスはDHCPを使用して取得しますが、初期設定時にスタティックアドレスを設定することもできます。

- 内部デバイスを残りのスイッチポート（Ethernet 1/2 ～ 1/8）に接続します。

Ethernet 1/7 および 1/8 は Power over Ethernet+（PoE+）ポートです。

Firepower 1120、1140 のケーブル配線

図 2: Firepower 1120、1140 のケーブル配線

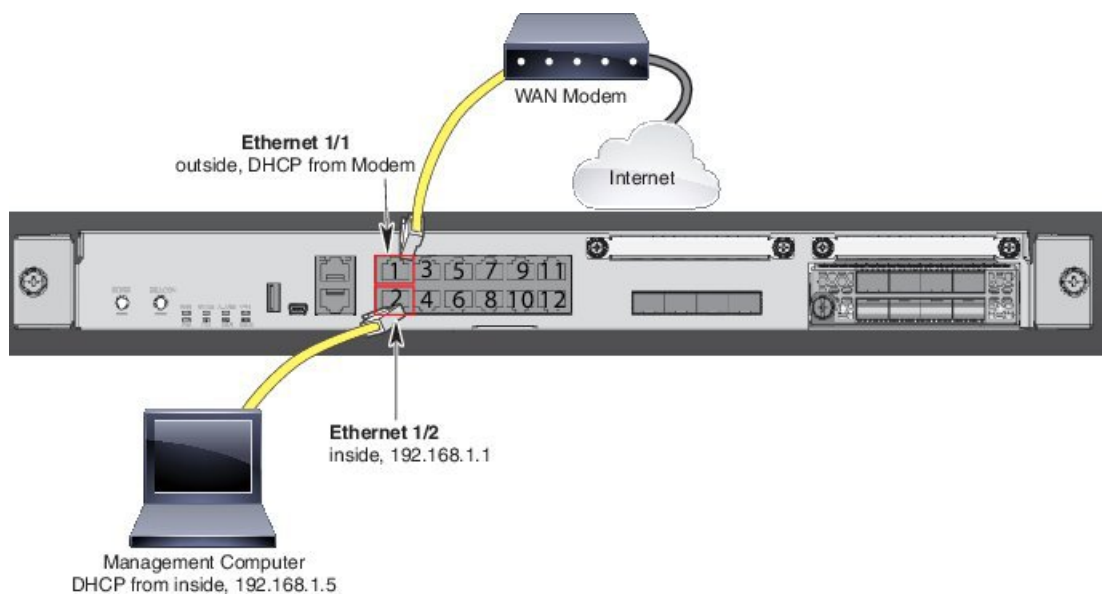


- ISP/WAN モデムまたはその他の外部デバイスに Ethernet 1/1 を接続します。デフォルトでは、IPアドレスはDHCPを使用して取得しますが、初期設定時にスタティックアドレスを設定することもできます。
- Ethernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCPを使用してIPアドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



- (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、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。

Firepower 2100の配線

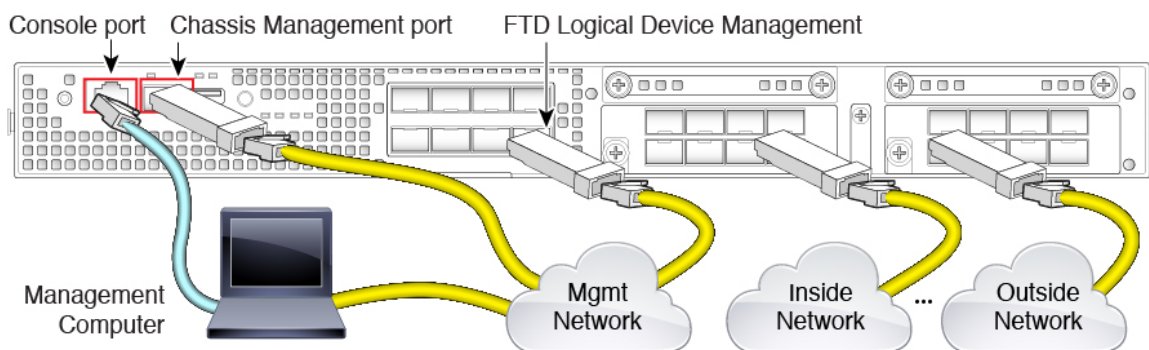


- ISP/WAN モデムまたはその他の外部デバイスに Ethernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- Ethernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



- (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。

Firepower 4100 のケーブル配線



論理デバイスの管理インターフェイスで FTD の初期設定を実行します。後で、任意のデータインターフェイスから管理を有効にすることができます。FTD では、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、FTD の展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で FDM でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- コンソールポート：管理コンピュータをコンソールポートに接続して、シャーシの初期設定を実行します。Firepower 4100 には、RS-232 - RJ-45 シリアル コンソール ケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。
- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- FTD 論理デバイス管理インターフェイス：シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。

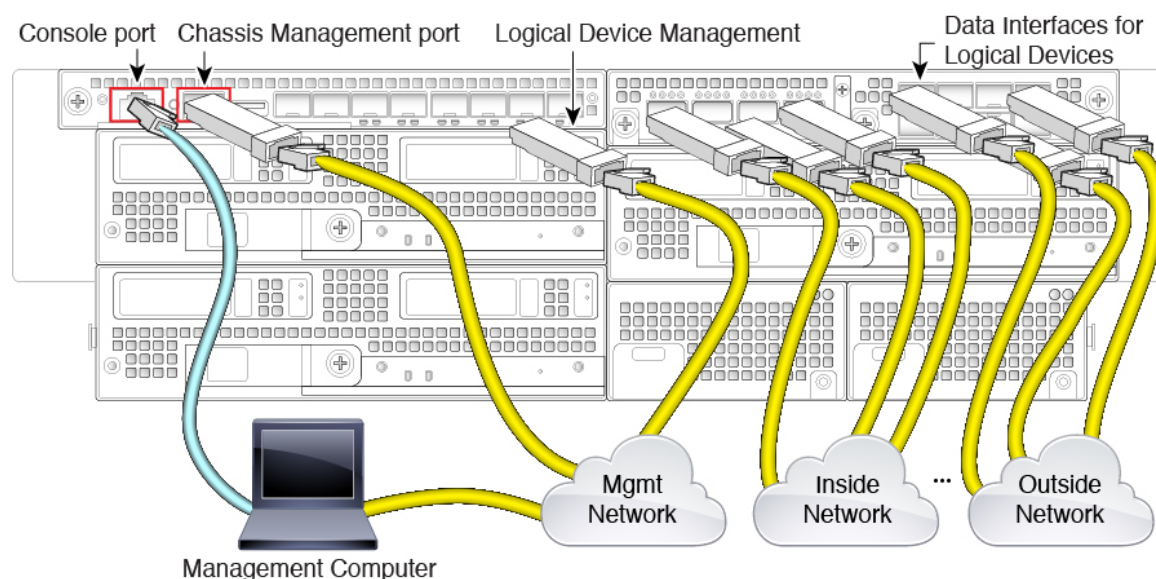
- データ インターフェイス：データ インターフェイスを論理デバイス データ ネットワークに接続します。物理インターフェイス、Etherchannel、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。

ハイ アベイラビリティの場合は、フェールオーバー/ステートリンクにデータ インターフェイスを使用します。



- (注) コンソールポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『[Hardware Installation Guide](#)』を参照してください。

Firepower 9300 のケーブル配線



論理デバイスの管理インターフェイスで FTD の初期設定を実行します。後で、任意のデータ インターフェイスから管理を有効にすることができます。FTD では、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、FTD の展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータ インターフェイスに管理トラフィックをルーティングする必要がある場合は、後で FDM でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- コンソールポート：管理コンピュータをコンソールポートに接続して、シャーシの初期設定を実行します。Firepower 9300 には、RS-232 - RJ-45 シリアル コンソール ケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。

- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
 - 論理デバイス管理インターフェイス：1つ以上のインターフェイスを使用して論理デバイスを管理します。シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。管理インターフェイスは論理デバイス間で共有できます。また、論理デバイスごとに別のインターフェイスを使用することもできます。通常は、管理インターフェイスをすべての論理デバイスと共有します。または、別個のインターフェイスを使用する場合は、それらを単一の管理ネットワークに配置します。ただし、正確なネットワーク要件は場合によって異なります。
 - データインターフェイス：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、Etherchannel、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。ネットワークのニーズに応じて、複数の論理デバイスを同じネットワークまたは異なるネットワークにケーブル接続できます。トラフィックはすべて、1つのインターフェイス上のシャーシを終端とし、別の論理デバイスに到達する場合は別のインターフェイスに戻る必要があります。
- ハイアベイラビリティの場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。



(注) コンソールポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『[Hardware Installation Guide](#)』を参照してください。

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、Microsoft Azure 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、必ずリストの最後にインターフェイスを追加してください。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤った順番になります。

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。

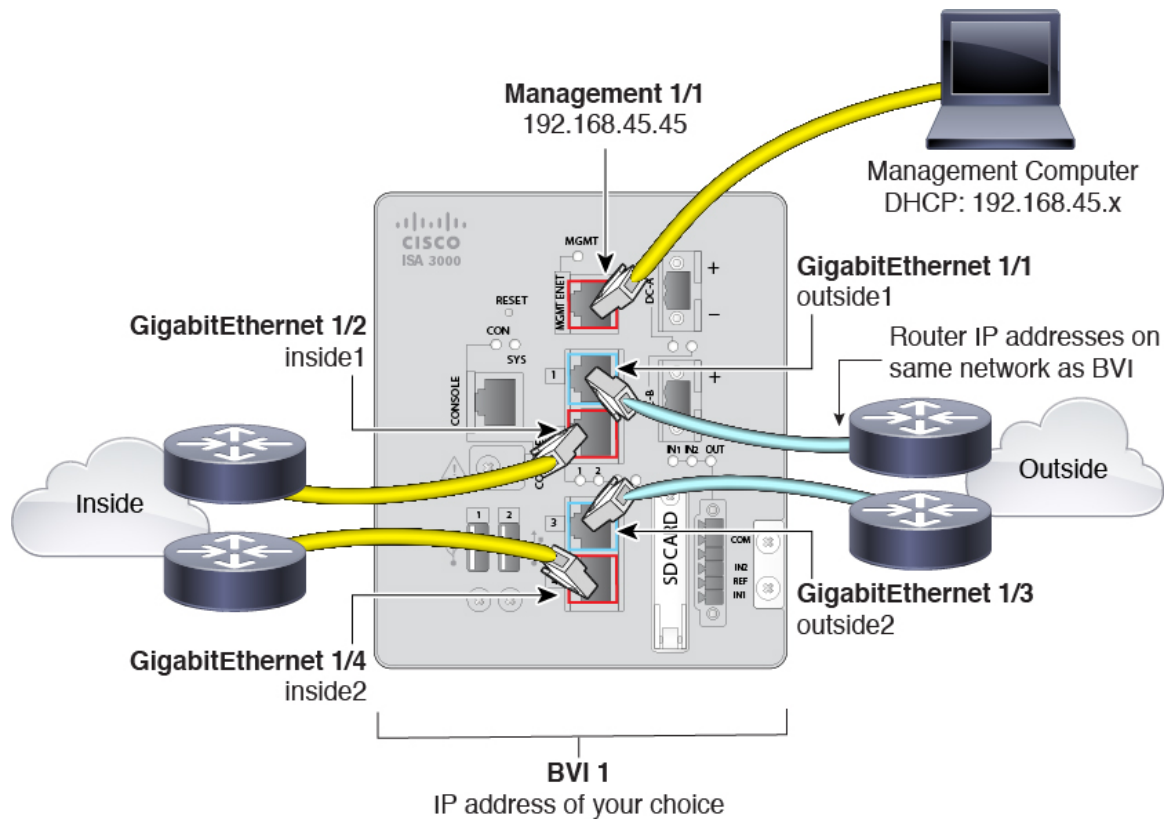
表 2: 送信元から宛先ネットワークへのマッピング

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	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
Network adapter 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
Network adapter 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部データ
Network adapter 5	GigabitEthernet0-2	GigabitEthernet0/2	データ トラフィック

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 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データ トラフィック
Network adapter 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データ トラフィック
Network adapter 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データ トラフィック
Network adapter 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データ トラフィック
Network adapter 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データ トラフィック

ISA 3000 のケーブル配線

図 3: ISA 3000



- GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。これらのインターフェイスによってハードウェア バイパス ペアが形成されます。
- GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

銅線ポートを備えたモデルの場合は、これらのインターフェイスによってハードウェアバイパスペアが形成されます。ファイバはハードウェアバイパスをサポートしていません。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパスを提供します。これら4つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

- Management 1/1 を管理 PC（またはネットワーク）に接続します。

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。

ハイアベイラビリティ設定でデバイスを使用する予定の場合は、[2台の装置でのハイアベイラビリティの準備（230 ページ）](#)を参照してください。



- (注) Firepower 4100/9300 および ISA 3000 ではセットアップ ウィザードがサポートされていないため、この手順はこれらのモデルには適用されません。Firepower 4100/9300 では、シャーシから論理デバイスを展開するときに、すべての初期設定が設定されます。ISA 3000 の場合は、出荷前に特別なデフォルト設定が適用されます。

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（18 ページ）](#) および [初期設定前のデフォルト設定（32 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せん。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。このアドレスは次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]**。
 - (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 \(32 ページ\)](#) 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

た後に 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 \(749 ページ\)](#) 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。Firepower 4100/9300 デバイスでは、FDM を使用して NTP を設定しません。FXOS で NTP を設定します。

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、デバイスを登録するオプションを選択し、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て、新しいトークンを作成し、編集ボックスにそのトークンをコピーします。また、サービス リージョンを選択し、Cisco Success Network に使用状況データを送信するかどうかを決定する必要があります。前述の設定については、画面上のテキストで詳しく説明されています。

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。これは、Cisco Defense Orchestrator を使用してデバイスを管理する場合に推奨されるオプションです。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 \(108 ページ\)](#) 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

細については、[サブネットを追加する方法 \(86 ページ\)](#) および [インターフェイス \(267 ページ\)](#) 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 \(688 ページ\)](#) 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 \(53 ページ\)](#) 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。

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 Firepower 4100/9300 : 論理デバイスの展開時にパスワードを設定します。	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 Firepower 4100/9300 : 論理デバイスの展開時に管理 IP アドレスを設定します。	番号 Firepower 4100/9300 の場合 : 可。

設定	デフォルト	初期設定時に変更できるか
管理ゲートウェイ	<p>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、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。</p> <p>Firepower 4100/9300 : 論理デバイスの展開時にゲートウェイ IP アドレスを設定します。</p> <p>Firepower Threat Defense Virtual 192.168.45.1</p>	<p>番号</p> <p>Firepower 4100/9300 の場合 : 可。</p>
管理インターフェイスの DHCP サーバ	<p>アドレス プール 192.168.45.46 ~ 192.168.45.254 で有効です。</p> <p>Firepower 4100/9300 : DHCP サーバが有効になっていません。</p> <p>Firepower Threat Defense Virtual : DHCP サーバが有効になっていません。</p>	不可。
管理インターフェイスの DNS サーバ	<p>OpenDNS のパブリック DNS サーバ、208.67.220.220 および 208.67.222.222。</p> <p>Firepower 4100/9300 : 論理デバイスの展開時に DNS サーバを設定します。</p>	可。
内部インターフェイスの IP アドレス	<p>192.168.1.1/24</p> <p>Firepower 4100/9300 : データインターフェイスが事前設定されていません。</p> <p>ISA 3000 : BV11 IP アドレスが事前設定されていません。BV11 にはすべての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ます。</p> <p>Firepower Threat Defense Virtual : 192.168.45.1/24</p>	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 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 4100/9300 : DHCP サーバが有効になっていません。 ISA 3000 : DHCP サーバが有効になっていません。 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。
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。 Firepower 4100/9300 : データインターフェイスが事前設定されていません。 ISA 3000 : BV11 IP アドレスが事前設定されていません。BV11 にはすべての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 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet 0/0	GigabitEthernet 0/1

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
Firepower 1010	Ethernet1/1	VLAN1。物理ファイアウォール インターフェイスである外部インターフェイスを除く他のすべてのスイッチポートが含まれます。
Firepower 1120、1140、1150	Ethernet1/1	Ethernet1/2
Firepower 2100 シリーズ	Ethernet1/1	Ethernet1/2
Firepower 4100 シリーズ	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Firepower 9300 アプライアンス	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Firepower Threat Defense Virtual	GigabitEthernet 0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 および GigabitEthernet1/3 GigabitEthernet1/1（外部1）と1/2（内部1）、および GigabitEthernet1/3（外部2）と1/4（内部2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 すべての内部インターフェイスと外部インターフェイスはBVIIの一部です。	GigabitEthernet1/2 および GigabitEthernet1/4

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。



(注) Firepower 4100/9300 と ISA 3000 は、セットアップウィザードをサポートしていません。Firepower 4100/9300 では、シャーシから論理デバイスを展開するときに、すべての初期設定が設定されます。ISA 3000 の場合は、出荷前に特別なデフォルト設定が適用されます。

設定	設定 (Configuration)	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

設定	設定 (Configuration)	明示的/暗黙的な設定、またはデフォルト設定
管理 IP アドレス	192.168.45.45 Firepower 4100/9300 : 論理デバイスの展開時に設定した管理 IP アドレス。	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 4100/9300 : 論理デバイスの展開時に設定したゲートウェイ IP アドレス。 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 4100/9300 : DHCP サーバが有効になっていません。 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 Firepower 4100/9300 : 論理デバイスの展開時に設定した DNS サーバ。 ISA 3000 : なし。	明示的
管理ホスト名	firepower または任意の入力値 Firepower 4100/9300 : 論理デバイスの展開時に設定したホスト名。	明示的

設定	設定 (Configuration)	明示的/暗黙的な設定、またはデフォルト設定
データ インターフェイスを通過する管理アクセス	<p>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。</p> <p>Firepower 4100/9300: 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。</p> <p>ISA 3000 : 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。</p> <p>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。</p>	暗黙的
システム時間	<p>選択したタイム ゾーンおよび NTP サーバ。</p> <p>Firepower 4100/9300 : システム時刻はシャーンシから継承されます。</p> <p>ISA 3000 : なし。</p>	明示的
スマート ライセンス	<p>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。</p> <p>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。</p>	明示的
内部インターフェイスの IP アドレス	<p>192.168.1.1/24</p> <p>Firepower 4100/9300 : データインターフェイスが事前設定されていません。</p> <p>ISA 3000 : なし。BVII の IP アドレスを手動で設定する必要があります。</p> <p>Firepower Threat Defense Virtual : 192.168.45.1/24</p>	デフォルト
内部クライアントの DHCP サーバ	<p>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。</p> <p>Firepower 4100/9300 : DHCP サーバが有効になっていません。</p> <p>ISA 3000 : DHCP サーバが有効になっていません。</p> <p>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。</p>	デフォルト

設定	設定 (Configuration)	明示的/暗黙的な設定、またはデフォルト設定
<p>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)</p>	<p>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。</p> <p>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。</p>	<p>明示的 (ただし間接的)</p>
<p>データ インターフェイスの設定</p>	<ul style="list-style-type: none"> • Firepower 1010 : 外部インターフェイス (Ethernet1/1) は物理ファイアウォール インターフェイスです。その他のインターフェイスはすべてスイッチ ポートです。これらのポートは有効になり、内部インターフェイスである VLAN1 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。 • Firepower 4100/9300 : データ インターフェイスはすべて無効になります。 • ISA 3000 : すべてのデータ インターフェイスが有効になり、同じブリッジグループ BV11 の一部となります。GigabitEthernet1/1 および 1/3 は外部インターフェイスとなり、GigabitEthernet1/2 および 1/4 は内部インターフェイスとなります。GigabitEthernet1/1 (外部 1) と 1/2 (内部 1)、および GigabitEthernet1/3 (外部 2) と 1/4 (内部 2) (非光ファイバモデルのみ) は、ハードウェアバイパスペアとして設定されます。 • 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。 	<p>デフォルト</p>
<p>外部の物理インターフェイスおよび IP アドレス</p>	<p>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 (32 ページ) を参照してください。</p> <p>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)。</p> <p>Firepower 4100/9300 : データ インターフェイスが事前設定されていません。</p> <p>ISA 3000 : なし。BV11 の IP アドレスを手動で設定する必要があります。</p>	<p>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</p>

設定	設定 (Configuration)	明示的/暗黙的な設定、またはデフォルト設定
スタティック ルート	<p>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。</p> <p>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。</p>	暗黙的
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。Firepower 4100/9300 では、このセキュリティゾーンにインターフェイスを手動で追加する必要があります。</p> <p>外部インターフェイスを含む outside_zone。Firepower 4100/9300 では、このゾーンにインターフェイスを手動で追加する必要があります。</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>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> <p>Firepower 4100/9300 : 事前に設定されたアクセスルールはありません。</p> <p>ISA 3000 : inside_zone から outside_zone へのすべてのトラフィックを信頼するルールと、outside_zone から inside_zone へのすべてのトラフィックを信頼するルール。トラフィックはブロックされません。また、デバイスには、inside_zone 内のインターフェイスと outside_zone 内のインターフェイス間におけるすべてのトラフィックを信頼するルールもあります。これにより、内部のユーザ間のすべてのトラフィックと、外部のユーザ間のすべてのトラフィックを検査する必要がなくなります。</p>	暗黙的

設定	設定 (Configuration)	明示的/暗黙的な設定、またはデフォルト設定
NAT	<p>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>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> <p>Firepower 4100/9300 : NAT は事前に設定されていません。</p> <p>ISA 3000 : NAT は事前に設定されていません。</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 \(47 ページ\)](#) 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。こ

の領域には、機能を設定するためのリンクを含め、ハイアベイラビリティステータスも表示されます。[ハイアベイラビリティ（フェールオーバー）（215ページ）](#)を参照してください。

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（267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（335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（713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（687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（101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（720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（755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（572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（613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 \(765 ページ\)](#) を参照してください。
- [デバイス管理 (Device Administration)] : 監査ログを表示するか、設定のコピーをエクスポートします。 [監査と変更管理 \(726 ページ\)](#) 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 \(44 ページ\)](#) 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 \(358 ページ\)](#) 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 \(382 ページ\)](#) 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 \(397 ページ\)](#) 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 \(479 ページ\)](#) 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 \(415 ページ\)](#) 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 \(460 ページ\)](#) 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 \(44 ページ\)](#) を参照してください。

ルールまたはオブジェクトを検索

ポリシールールまたはオブジェクトのリストで全文検索を使用すると、編集する項目を探すことができます。これは、数百のルールのあるポリシーや長いオブジェクトリストを処理するとき特に便利です。

ルールおよびオブジェクトの検索を使用するための方法は、どの種類のポリシー (侵入ポリシーを除く) またはオブジェクトでも同じです。[検索 (Search)] フィールドに検索する文字列を入力し、Enter キーを押します。

この文字列はルールまたはオブジェクトの任意の部分に存在することができ、部分的な文字列でも構いません。アスタリスク (*) を、0 個以上の文字と一致するワイルドカードとして使用できます。検索文字列の一部としてサポートされていないため、?、~、!、{、}、<、>、:、% は使用しないでください。;、#、& は無視されます。

文字列は、グループのオブジェクト内に出現することがあります。たとえば、IP アドレスを入力し、そのアドレスを指定するネットワークオブジェクトまたはグループを検索することができます。

完了したら、検索ボックスの右側にある [x] をクリックしてフィルタをクリアします。

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 \(46 ページ\)](#) 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。



[保留中の変更 (Pending Changes)] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集され

た要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

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、アイコンをクリックすると最後に成功した展開ジョブの日時を確認できます。展開履歴を表示するリンクもあり、クリックすると展開ジョブだけを表示するようにフィルタ処理された監査ページに移動します。



ステップ 2 変更内容に問題がない場合は、[今すぐ展開 (Deploy Now)] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じて、ジョブは停止しません。結果は、タスクリストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴 (Deployment History)] リンクをクリックすると結果が表示されます。

状況に応じて、次の手順を実行できます。

- [ジョブの命名 (Name the Job)] : 展開ジョブに名前を付けるには、[今すぐ展開 (Deploy Now)] ボタンのドロップダウン矢印をクリックして、[展開ジョブの命名 (Name the Deployment Job)] を選択します。名前を入力して [展開 (Deploy)] をクリックします。名前は、ジョブの一部として監査および展開履歴に表示されるため、ジョブの検索が容易になります。

たとえば、ジョブの名前を「DMZ Interface Configuration」にした場合、成功した展開の名前は「Deployment Completed: DMZ Interface Configuration」になります。さらに、その名前は、展開ジョブに関連する [タスク開始 (Task Started)] イベントと [タスク完了 (Task Completed)] イベントの [イベント名 (Event Name)] として使用されます。

- [変更の破棄 (Discard Changes)] : 保留中の変更をすべて破棄するには、[詳細オプション (More Options)] > [すべて破棄 (Discard All)] をクリックします。確認を求められません。
- [変更のコピー (Copy Changes)] : 変更の一覧をクリップボードにコピーするには、[詳細オプション (More Options)] > [クリップボードにコピー (Copy to Clipboard)] をクリックします。このオプションは、変更の数が 500 未満の場合にのみ機能します。
- [変更のダウンロード (Download Changes)] : 変更の一覧をファイルとしてダウンロードするには、[詳細オプション (More Options)] > [テキストとしてダウンロード (Download as Text)] をクリックします。自分のワークステーションにファイルを保存するように求められます。このファイルは YAML 形式です。YAML 形式に対応しているエディタがない場合は、テキスト エディタで表示できます。

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、いくつかのパケット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。
- VDB が更新された。
- 高可用性設定が作成または破棄された。

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、展開中に一部のパケット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 (747 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。

タスク リストには、システム タスクと展開ジョブの統合ステータスが表示されます。監査ログにはより詳細な情報が含まれており、[デバイス (Device)] > [デバイス管理 (Device Administration)] > [監査ログ (Audit Log)] の下にあります。たとえば、監査ログにはタスクの開始とタスクの終了ごとに個別のイベントが表示されます。一方、タスク リストではそれらのイベントが単一のエンTRIESにマージされます。さらに、展開の監査ログエンTRIESには、展開された変更に関する詳細情報が含まれています。

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

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。管理者権限を持っている場合は、**failover**、**reboot**、および **shutdown** コマンドを入力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 Command Reference』

(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。

Firepower Device Manager と REST API の併用

ローカル管理モードでデバイスをセットアップする場合、Firepower Device Manager と Firepower Threat Defense REST API を使用してデバイスを設定できます。実際には、Firepower Device Manager は REST API を使用してデバイスを設定します。

ただし、REST API は Firepower Device Manager で利用できる機能に加えて、その他の機能を提供できることを理解してください。したがって、所定の機能について、Firepower Device Manager で設定を確認するときには表示できない、REST API を使用した設定を行うことができます。

REST API で利用できて Firepower Device Manager で利用できない機能を設定する場合は、設定が完了していない可能性がある、Firepower Device Manager を使用したすべての機能（リモートアクセス VPN など）に変更を加えます。API のみの設定が維持されるかどうかは状況により異なります。多くの場合、FDM で使用できない設定に対する API の変更は FDM の編集を通じて保存されます。対象の機能について、変更が保存されているかどうかを確認する必要があります。

通常は、対象の機能について Firepower Device Manager と REST API を同時に使用することは避けてください。代わりに、デバイスを設定するために、機能ごとにいずれかの方法を選択します。

API エクスプローラを使用して、API のメソッドを表示でき、試すことができます。[詳細オプション (More options)] ボタン (☰) をクリックし、[API エクスプローラ (API Explorer)] を選択します。



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 \(53 ページ\)](#)
- [ネットワークトラフィックを調べる方法 \(59 ページ\)](#)
- [脅威をブロックする方法 \(67 ページ\)](#)
- [マルウェアをブロックする方法 \(74 ページ\)](#)
- [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 \(77 ページ\)](#)
- [アプリケーションの使用を制御する方法 \(82 ページ\)](#)
- [サブネットを追加する方法 \(86 ページ\)](#)
- [ネットワーク上のトラフィックをパッシブにモニタする方法 \(93 ページ\)](#)
- [その他の例 \(99 ページ\)](#)

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。

- 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。
- (Firepower 4100/9300) 事前に設定されたデータインターフェイスはありません。
- (ISA 3000) ブリッジグループには2つの内部インターフェイスと2つの外部インターフェイスが含まれています。セットアップを完了するにはBVIIのIPアドレスを手動で設定する必要があります。
- (Firepower 4100/9300 を除く) 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。

- (Firepower 4100/9300 を除く) 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。ISA 3000 の場合、内部から外部、および外部から内部へのすべてのトラフィックを許可するアクセスルールがあります。
- (Firepower 4100/9300 および ISA 3000 を除く) 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。
- (Firepower 4100/9300 および ISA 3000 を除く) 内部インターフェイスで実行されている 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。

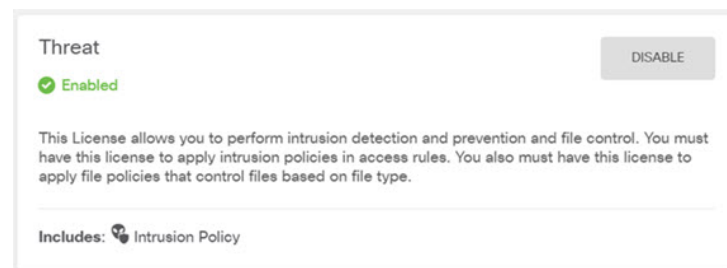
手順

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。[Register Device] 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してから、インターフェイスのタイプをクリックして、インターフェイスのリストを表示します。

- Firepower 4100/9300 では、名前、IP アドレス、またはセキュリティゾーンを使用して事前に設定されているデータインターフェイスがないため、使用するインターフェイスを有効にして設定する必要があります。
- ISA 3000 はすべてのデータ 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。ただし、BVI の IP アドレスを手動で設定する必要があります。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。

- Firepower 1010 の場合、Ethernet1/1 (外部) 以外のインターフェイスはすべて、VLAN1 (内部) に割り当てられたアクセスモードのスイッチポートです。スイッチポートをファイアウォールポートに変更することができます。それには、新しい VLAN インターフェイスを追加してスイッチポートを割り当てます。または、トランクモードのスイッチポートを設定します。

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: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces. [Learn More](#)

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type:

IP Address and Subnet Mask: /

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

Mode
 Routed Passive

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。

Add Server

Enabled DHCP Server

Interface
inside2

Address Pool
192.168.4.50-192.168.4.240
e.g. 192.168.45.46-192.168.45.254

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手元で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 options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text field containing 'isp-gateway'.
- Interface:** A text field containing 'outside'.
- Metric:** A text field containing '1'.
- Networks:** A dropdown menu showing '+ 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間のトラフィック 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りますか

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 ゾーンの間で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。

Order	Title	Action
2	Inside_DMZ	Allow

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
inside_zone	ANY	ANY	dmz-zone	ANY	ANY

ステップ 7 変更を保存します。

- 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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、許容するカテゴリ (金融など) 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 \(77 ページ\)](#) 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。

この例では、ユーザアイデンティティを取得するためにアクティブ認証を実装します。アクティブ認証を使用すると、デバイスからユーザ名とパスワードを求められます。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。アクティブ認証を使用している場合、アイデンティティポリシーは Active Directory 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 アドレスをユーザに関連付けます。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。
 c) [アイデンティティルールの作成 (Create Identity Rule)] ボタンまたは [+] ボタンをクリックして、アクティブ認証を義務付けるルールを作成します。

この例では、すべての人に認証を義務付けていると仮定しています。

- d) ルールの [名前 (Name)] を入力します。Require_Authentication など、任意の名前を選択できます。
 e) [送信元または宛先 (Source/Destination)] タブをデフォルトのままにします。これは、[任意 (Any)] 基準に適用されます。

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、[を参照してください。アイデンティティルールの設定 \(386 ページ\)](#)

- f) [アクション (Action)] で [アクティブ認証 (Active Auth)] を選択します。

いくつか未定義の設定があるため、アイデンティティポリシーの設定が行われていないと仮定して、[アイデンティティポリシー設定 (Identity Policy Configuration)] ダイアログボックスが開きます。


- g) アクティブ認証に必要な [キャプティブ ポータル (Captive Portal)] の設定と [SSL復号 (SSL Decryption)] の設定を行います。

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。キャプティブポータルにはSSL復号化ルールが必要です。このルールは、システムによって自動的に生成されますが、SSL復号化ルールに使用する証明書は選択する必要があります。

- [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。
- [再署名証明書の復号 (Decrypt Re-Sign Certificate)] : 再署名証明書での復号を実装するルールに使用する内部 CA 証明書を選択します。事前定義済みの NGFW-Default-InternalCA 証明書 (デフォルト) か、作成またはアップロードした証明書を使用できます。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。SSL復号化ポリシーをまだ有効にしている場合にも、復号化再署名証明書の入力が必要になります。

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 (371 ページ) も参照してください。

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

Identity Policy

ACTIVE AUTHENTICATION

Server Certificate: DefaultInternalCertificate

Port: 885
e.g. 885 or 1025-65535

SSL Decryption ⓘ

Decrypt Re-Sign Certificate: NGFW-Default-InternalCA

⚠️ ① Download the selected certificate. ② Install it on all client machines for all browsers. [Read detailed instructions](#)

If you do not install the certificate, users will see warnings for untrusted HTTPS connections.

CANCEL SAVE

- h) [保存 (Save)] をクリックしてアクティブ認証の設定を保存します。
- [アクティブ認証 (Active Authentication)] タブが [アクション (Action)] 設定の下に表示されます。
- i) [アクティブ認証 (Active Authentication)] タブで、[HTTPネゴシエート (HTTPNegotiate)] 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) HTTPBasic、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。

- j) [ADアイデンティティソース (AD Identity Source)] で [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。

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。(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 \(182 ページ\)](#) 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 <small>e.g. user@example.com</small>
Base DN	AD Primary Domain
ou=user,dc=example,dc=com <small>e.g. ou=user, dc=example, dc=com</small>	example.com <small>e.g. example.com</small>

DIRECTORY SERVER CONFIGURATION

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

- k) [ADアイデンティティソース（AD Identity Source）]で、作成したオブジェクトを選択します。

ルールは次のようになります。

Order	Title	AD Identity Source	Action
1	Require_Authentication	AD	Active Auth

Source / Destination [Active authentication](#)

Type	ACTIVE AUTHENTICATION
HTTP Negotiate	For HTTP connections only, prc specified identity source to obt connections, even non-HTTP, f prompted to authenticate again access. You must configure the Type – Select the authenticati
Fall Back as Guest	<input type="checkbox"/>

- l) [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。ユーザー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) (ISA 3000)。また、Outside_Inside_Rule、Inside_Inside_Rule および Outside_Outside_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。

- [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。

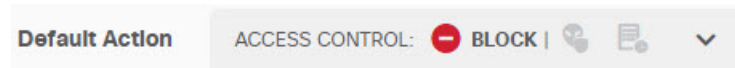
Order	Title	Action
1	Inside_Outside_Rule	Allow

- [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。

- 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) [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 Time

Sundays * 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ます。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

- 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) [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。

- 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。

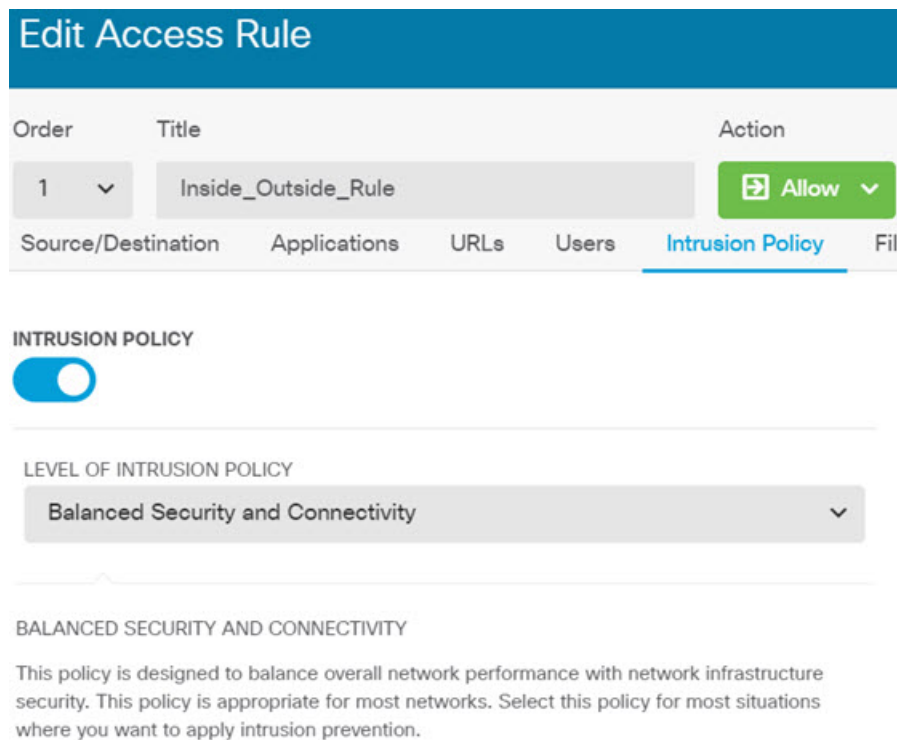
Order	Title	Action
1	Inside_Outside_Rule	Allow

- d) [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。



- 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に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。

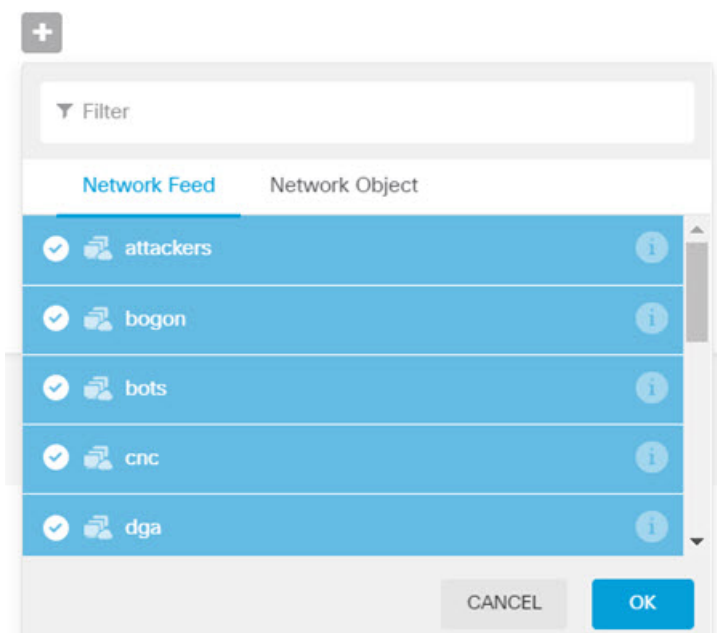
ステップ 4 既知の不正ホストやサイトとの接続を先制的にドロップするためのセキュリティインテリジェンス ポリシーを設定します。

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。

- a) [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。
- b) [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。
- c) 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。
- d) [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。
- e) 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。
- f) [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。

Blacklist (Block/Drop)



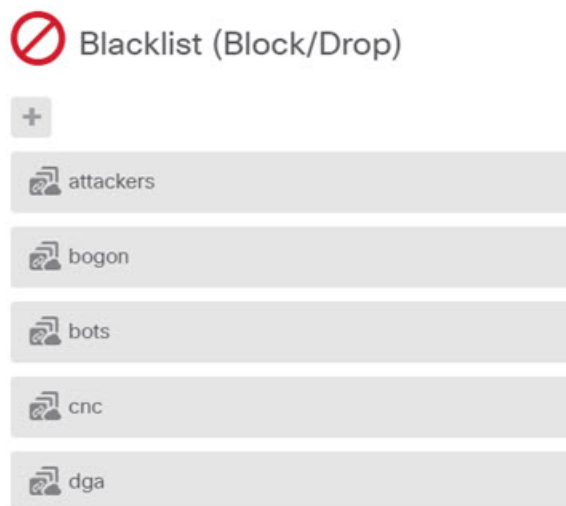
フィードが存在しないというメッセージが表示される場合は、後でもう一度試してください。フィードのダウンロードはまだ完了していません。この問題が解決しない場合は、管理 IP アドレスとインターネット間にパスがあることを確認してください。

- 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。

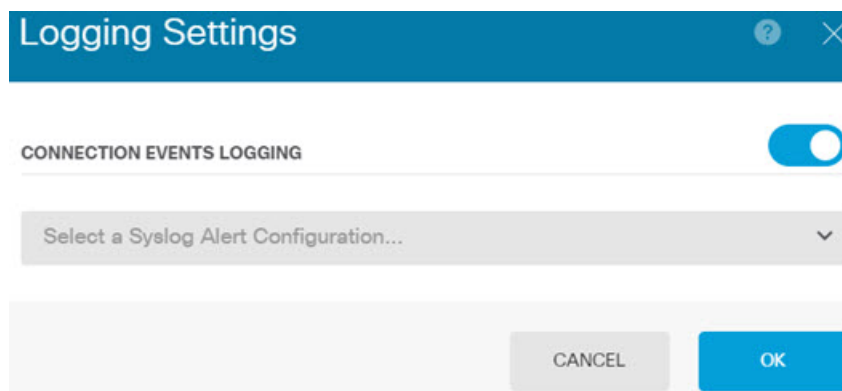
- h) [URL] タブをクリックし、[ブラックリスト (Blacklist)] の下にある [+] > [URL フィード (URL Feeds)] をクリックして、すべての URL フィードを選択します。[OK] をクリックして、それらをブラックリストに追加します。

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。



- 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

- 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) [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спекションを追加します。

- 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) 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。

- 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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（ギャンブルなど）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

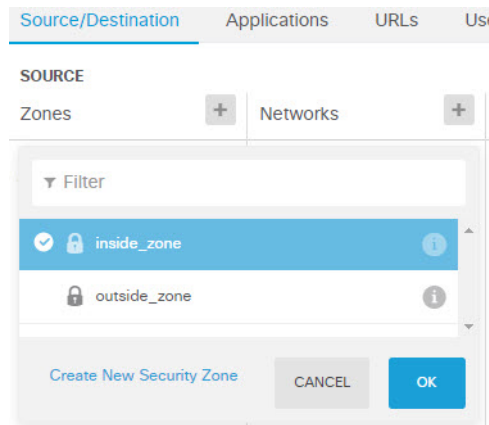
Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセスコントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。

- [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。

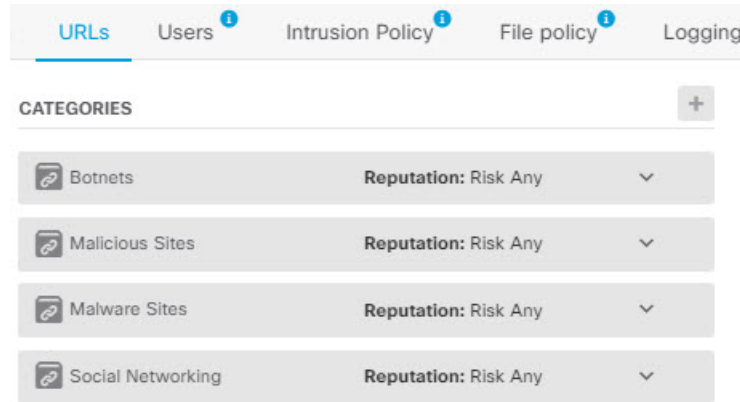


- e) 同じ技術を使用して、[接続先 (Destination)] > [ゾーン (Zones)] で [outside_zone] を選択します。

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

- 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、ボットネット、悪意のあるサイト、マルウェアサイト、およびソーシャルネットワークワーキングを選択します。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。ブロックしたいサイトがわかっている場合、そのカテゴリがわからない場合は、[確認するURL（URL to Check）]フィールドにURLを入力し、[実行（Go）]をクリックします。ルックアップ結果を示す Web サイトが表示されます。



- 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 Networking）] 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 [疑わしい（Questionable）] 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（Questionable）] と [信頼できない（Untrusted）] の範囲内にあるソーシャルネットワーク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ク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

Description

URL

- 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せん。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	Botnets Reputation: Risk Any
	Malicious Sites Reputation: Risk Any
	Malware Sites Reputation: Risk Any
	Social Networking Reputation: Questionable

- 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。ルックアップ結果の存続可能時間を設定できます。デフォルトは [使用しない (Never)] で、ルックアップ結果は更新されません。

- 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) 妥当な [URL 存続可能時間 (URL Time to Live)] (24 時間など) を選択します。
- e) [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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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場合、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 \(59 ページ\)](#) 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。

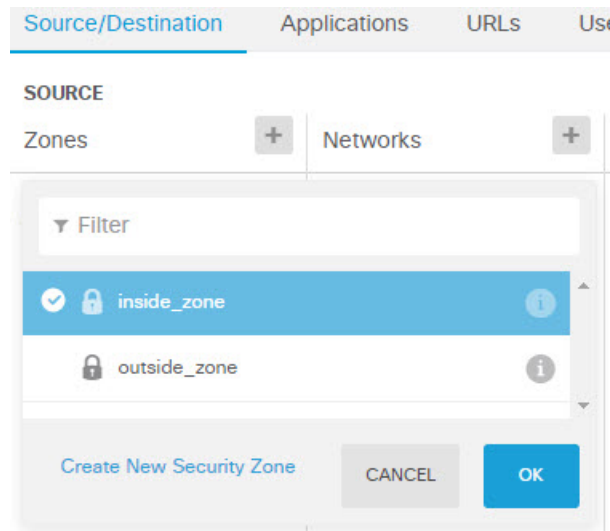
- a) メインメニューで [ポリシー (Policies)] をクリックします。
[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。
- b) [+] をクリックして新しいルールを追加します。
- c) 順序、タイトル、およびアクションを設定します。
 - [順序 (Order)] : デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル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 + Ports +</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)] リストから匿名マイザー/プロキシを選択します。

Filter Applications

[?](#) RESET FILTER

Risks	Categories 1 selected	Tags Any selected
Any	<input type="text" value="Search Categories"/> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> anonymizer/proxy mobile application VoIP web services provider e-commerce 	<input type="text" value="Search Tags"/> <ul style="list-style-type: none"> displays ads not work related high bandwidth file sharing/transfer share media
Business Relevance		
Any		
Types		
Any		

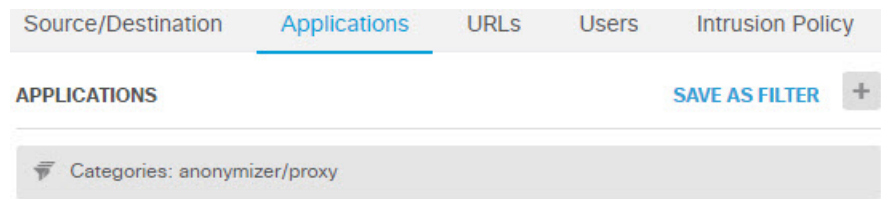
Filter the list of applications

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。



- 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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、許可されません。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、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、次にインターフェイスタイプをクリックして、インターフェイスのリストを表示します。
- b) 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)。
 - [モード (Mode)] : [ルーテッド (Routed)] を選択します。
 - [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: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces. [Learn More](#)

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type:

IP Address and Subnet Mask: /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

- 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。

GigabitEthernet1/5	inside_2	<input checked="" type="checkbox"/>	Routed	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。

- 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。

- e) [保存 (Save)] をクリックします。

Security Zones

3 objects

#	NAME	MODE	INTERFACES
1	inside_zone	Routed	inside, inside_2
2	outside_zone	Routed	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。

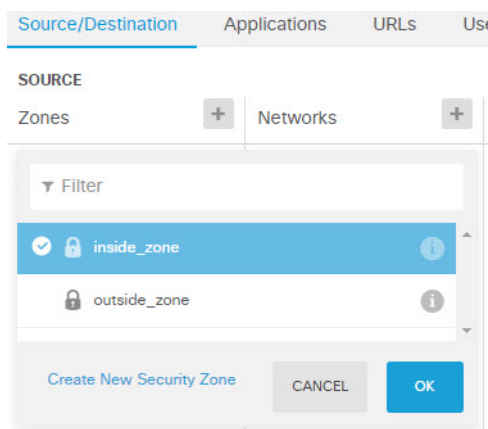
- b) [+] をクリックして新しいルールを追加します。

- c) 順序、タイトル、およびアクションを設定します。

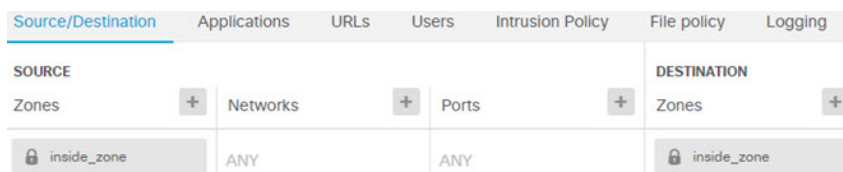
- [順序 (Order)] : デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです)。このルールでは、一意の送信元/宛先条件を使用するため、リストの最後にルールを追加できます。
- [タイトル (Title)] : ルールに Allow_Inside_Inside などの意味のある名前を付けます。
- [アクション (Action)] : [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 アドレスの一意的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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

ネットワーク上のトラフィックをパッシブにモニタする方法

Firepower Threat Defense デバイスは通常、アクティブなファイアウォールおよび IPS（侵入防御システム）セキュリティデバイスとして展開されます。デバイスの中核的機能は、ネットワークに対するアクティブな保護を提供し、不必要な接続や脅威を排除することにあります。

ただし、システムはパッシブモードで展開することもでき、その場合、デバイスは監視対象のスイッチポート上のトラフィックだけを分析します。このモードは、主にデモやテスト目的で使用されます。そうすることで、デバイスをアクティブなファイアウォールとして展開する前にそのデバイスに慣れることができます。パッシブ展開を使用すると、ネットワーク上に現れる脅威の種類（ユーザが参照している URL カテゴリなど）をモニタできます。

パッシブモードは、通常はデモやテスト目的で使用しますが、防御のない IDS（侵入検知システム）など、必要なサービスが提供される場合は、実稼働環境でパッシブモードを使用することもできます。パッシブインターフェイスをアクティブなファイアウォールのルーテッドインターフェイスと混在させることで、組織が必要とする的確なサービスの組み合わせを提供できます。

次の手順では、限られた数のスイッチポートからのトラフィックを分析するために、システムをパッシブに展開する方法を説明します。



- (注) この例は、ハードウェア Firepower Threat Defense デバイス向けです。Firepower Threat Defense Virtual にパッシブモードを使用することもできますが、ネットワークの設定は異なります。詳細については、[Firepower Threat Defense Virtual パッシブインターフェイスの VLAN の設定（316 ページ）](#) を参照してください。それ以外の場合、この手順は、Firepower Threat Defense Virtual にも当てはまります。

始める前に

次の手順は、内部インターフェイスと外部インターフェイスに接続し、デバイスの初期セットアップウィザードが完了していることを前提としています。パッシブ展開の場合でも、システムデータベースの更新をダウンロードするためにインターネットに接続する必要があります。また、Firepower Device Manager を開くために管理インターフェイスにも接続できる必要があります。これは、内部ポートまたは管理ポートへの直接接続を介して可能です。

手順

- ステップ 1** スイッチポートを SPAN（スイッチドポートアナライザ）ポートとして設定し、送信元インターフェイスのモニタリングセッションを設定します。

次の例では、Cisco Nexus 5000 シリーズ スイッチの 2 つの送信元インターフェイスに SPAN ポートとモニタリングセッションを設定します。異なる種類のスイッチを使用している場合は、必要なコマンドが異なることがあります。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

確認するには、次の手順に従います。

```
switch# show monitor session 1 brief
  session 1
-----
type           : local
state          : up
source intf    :
  rx           : Eth1/7      Eth1/8
  tx           : Eth1/7      Eth1/8
  both        : Eth1/7      Eth1/8
source VSANs   :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ 2 Firepower Threat Defense インターフェイスをスイッチの SPAN ポートに接続します。

Firepower Threat Defense デバイス上の現在未使用のポートを選択することをお勧めします。スイッチの設定例に基づいて、スイッチのイーサネット 1/48 にケーブルを接続します。これはモニタリングセッションの宛先インターフェイスです。

ステップ 3 Firepower Threat Defense インターフェイスをパッシブモードで設定します。

- a) [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[インターフェイス (Interfaces)] または [EtherChannels] をクリックします。
- b) 編集する物理インターフェイスまたは EtherChannel の編集アイコン (🔗) をクリックします。

現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブインターフェイスに変換する場合は、最初にセキュリティゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。

- c) [ステータス (Status)] スライダを [有効 (enabled)] 設定 (🔘) に設定します。
- d) 以下を設定します。

- [インターフェイス名 (Interface Name)]: 最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、**monitor** などです。

- [モード (Mode)] : [パッシブ (Passive)] を選択します。

Interface Name	Mode	Status
monitor	Passive	<input checked="" type="checkbox"/>

- e) [OK] をクリックします。

ステップ 4 インターフェイスのパッシブ セキュリティ ゾーンを作成します。

- a) [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。
- b) [+] ボタンをクリックします。
- c) オブジェクトの名前を入力し、任意で説明を入力します。例、 **passive_zone**。
- d) [モード (Mode)] で [パッシブ (Passive)] を選択します。
- e) [+] をクリックして、パッシブ インターフェイスを選択します。

Name

passive_zone

Description

Mode

Routed Passive

Interfaces

+

monitor

- f) [OK] をクリックします。

ステップ 5 パッシブ セキュリティ ゾーン用の 1 つ以上のアクセス制御ルールを設定します。

作成するルールの数と種類は、収集する情報によって異なります。たとえば、IDS（侵入検知システム）としてシステムを設定する場合は、割り当てられた侵入ポリシーを設定した [許可 (Allow)] ルールが少なくとも 1 つは必要です。URL カテゴリ データを収集する場合は、URL カテゴリの仕様を含むルールが少なくとも 1 つは必要です。

[ブロック (Block)] ルールを作成して、ルーテッド インターフェイスでアクティブにブロックされる接続を確認できます。インターフェイスがパッシブなので、それらの接続は実際にはブロックされませんが、システムによるネットワーク上のトラフィックの調整方法は明確に確認できます。

次の使用例では、アクセス制御ルールを主な使用方法について説明します。それらの使用例は、パッシブ インターフェイスにも当てはまります。作成するルールの送信元ゾーンとしてパッシブセキュリティゾーンを選択します。

- 脅威をブロックする方法 (67 ページ)
- マルウェアをブロックする方法 (74 ページ)
- アクセプトブルユース ポリシー (URL フィルタリング) の実装方法 (77 ページ)
- アプリケーションの使用を制御する方法 (82 ページ)

次の手順では、侵入ポリシーを適用して、URL カテゴリ データを収集する 2 つの [許可 (Allow)] ルールを作成します。

- [ポリシー (Policies)] > [アクセス コントロール (Access Control)] を選択します。
- [+] をクリックして、すべてのトラフィックを許可するが、侵入ポリシーを適用するルールを追加します。
- ルールの順序として **1** を選択します。このルールはデフォルトのルールよりも具体的ですが、デフォルトのルールとはオーバーラップしません。カスタムルールがすでにある場合は適切な位置を選択し、パッシブインターフェイス向けのトラフィックが代わりにそれらのルールと一致しないようにします。
- ルールの名前、**Passive_IDS** などを入力します。
- [アクション (Action)] として [許可 (Allow)] を選択します。
- [送信元/宛先 (Source/Destination)] タブの [送信元 (Source)] > [ゾーン (Zones)] でパッシブゾーンを選択します。このタブの他の設定は変更しないでください。

この時点で、評価モードで実行中のルールは次のようになります。

Order	Title	Action
1	Passive_IDS	Allow

Source/Destination	Applications	URLs	Users	Intrusion Policy
<p>SOURCE</p> <p>Zones <input type="button" value="+"/></p> <p>passive_zone</p>	<p>Networks <input type="button" value="+"/></p> <p>ANY</p>		<p>Ports <input type="button" value="+"/></p> <p>ANY</p>	

- [侵入ポリシー (Intrusion Policy)] タブをクリックし、スライダをクリックして [オン (On)] にして、ほとんどのネットワークに推奨される [バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ポリシーなどの侵入ポリシーを選択します。

INTRUSION POLICY



LEVEL OF INTRUSION POLICY

Balanced Security and Connectivity

- h) [ロギング (Logging)] タブをクリックし、ロギング オプションで [接続の終了時 (At End of Connection)] を選択します。

SELECT LOG ACTION

- At Beginning and End of Connection
- At End of Connection
- No Connection Logging

- i) [OK] をクリックします。
- j) [+] をクリックして、URL およびすべての HTTP 要求のカテゴリを判断するためにシステムがディープ インスペクションを実行する必要があるルールを追加します。
- このルールにより、ダッシュボードで URL カテゴリ情報を確認できるようになります。処理時間を短縮し、パフォーマンスを向上させるために、URL カテゴリ条件を指定する少なくとも 1 つのアクセス制御ルールが存在する場合にのみシステムは URL カテゴリを判断します。
- k) ルールの順序として **1** を選択します。これは、前のルール (Passive_IDS) の上に配置されます。(すべてのトラフィックに適用される) ルールの後に配置すると、今作成しているルールは決して一致しません。
- l) ルールの名前、**Determine_URL_Category** などを入力します。
- m) [アクション (Action)] として [許可 (Allow)] を選択します。
- または、[ブロック (Block)] を選択できます。いずれのアクションでも、このルールの目的が達成されます。
- n) [送信元/宛先 (Source/Destination)] タブの [送信元 (Source)] > [ゾーン (Zones)] でパッシブ ゾーンを選択します。このタブの他の設定は変更しないでください。

Order	Title	Action
1	Determine_URL_Category	Allow

Source/Destination Applications URLs Users Intrusion Policy

SOURCE

Zones	Networks	Ports
passive_zone	ANY	ANY

CATEGORIES

Search Engines and Portals Reputation: Risk Any

- o) [URL (URLs)] タブをクリックし、[カテゴリ (Categories)] 見出しの横にある [+] をクリックして、いずれかのカテゴリを選択します。たとえば、**[検索エンジンおよびポータル (Search Engines and Portals)]** を選択します。必要に応じて、レピュテーションレベルを選択するか、デフォルトの [任意 (Any)] のままにします。

- p) [侵入ポリシー (Intrusion Policy)] タブをクリックし、スライダをクリックして [オン (On)] にして、最初のルールに選択したのと同じ侵入ポリシーを選択します。
- q) [ログギング (Logging)] タブをクリックし、ログギング オプションで [接続の終了時 (At End of Connection)] を選択します。

ただし、アクションとして [ブロック (Block)] を選択した場合は、[接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。ブロックされた接続自体は終了しないため、接続の開始時にのみログ情報を取得できます。

- r) [OK] をクリックします。

ステップ 6 (オプション) その他のセキュリティポリシーを設定します。

次のセキュリティポリシーも設定して、トラフィックにどのような影響を与えるかを確認できます。

- [アイデンティティ (Identity)] : ユーザ情報を収集します。アイデンティティポリシーにルールを設定して、送信元 IP アドレスに関連付けられているユーザが確実に特定されるようにできます。パッシブインターフェイスのアイデンティティポリシーの実装プロセスは、ルーテッドインターフェイスのプロセスと同じです。[ネットワークトラフィックを調べる方法 \(59 ページ\)](#) で説明されている使用例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)] : 既知の不正な IP アドレスと URL をブロックします。詳細は、[脅威をブロックする方法 \(67 ページ\)](#) を参照してください。

- (注) パッシブインターフェイス上のすべての暗号化されたトラフィックは復号不可として分類されるため、SSL復号化ルールは無効になり、パッシブインターフェイスには適用されません。

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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 8 監視ダッシュボードを使用して、ネットワーク経由で到達するトラフィックや脅威の種類を分析します。Firepower Threat Defense デバイスに不要な接続をアクティブにドロップさせる場合は、デバイスを再展開して、監視対象ネットワークに対するファイアウォール保護を提供するアクティブなルーテッドインターフェイスを設定できます。

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。

アクセス制御

- [Trustsec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法 \(432 ページ\)](#)

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 \(スタティック自動 NAT\) \(528 ページ\)](#)
- [FTP、HTTP、および SMTP の単一アドレス \(ポート変換を設定したスタティック自動 NAT\) \(531 ページ\)](#)
- [宛先に応じて異なる変換 \(ダイナミック手動 PAT\) \(538 ページ\)](#)
- [宛先アドレスおよびポートに応じて異なる変換 \(ダイナミック手動 PAT\) \(543 ページ\)](#)
- [DNS 応答修正：外部の DNS サーバ \(556 ページ\)](#)
- [DNS 応答修正：ホスト ネットワーク上の DNS サーバ \(560 ページ\)](#)
- [NAT からのサイト間 VPN トラフィックの除外 \(589 ページ\)](#)

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 (514 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 (516 ページ)
- NAT66 の例：ネットワーク間のスタティック変換 (522 ページ)
- NAT66 の例：シンプルな IPv6 インターフェイス PAT (524 ページ)
- DNS 64 応答修正 (550 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)

- RADIUS 認可変更の実装方法 (639 ページ)
- Duo LDAP を使用した二要素認証の設定方法 (649 ページ)
- 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) (658 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 (663 ページ)
- グループによって RA VPN アクセスを制御する方法 (679 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 (589 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) (596 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 (373 ページ)

FlexConfig ポリシー (FlexConfig Policy)

- 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 (793 ページ)
- FlexConfig の変更を元に戻す方法 (799 ページ)
- 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 (801 ページ)
- 高精度時間プロトコルの設定方法 (ISA 3000) (805 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 \(101 ページ\)](#)
- [スマートライセンスの管理 \(105 ページ\)](#)

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。

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（自動的に含まれる）	永久	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。 [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。

ライセンス	期間	付与される機能
脅威	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>
マルウェア (Malware)	ターム ベース	<p>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。</p> <p>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。ファイルを保存するようにファイルポリシーを設定する場合は、マルウェアライセンスも必要です。詳細については、ファイルポリシーのライセンス要件 (104 ページ) を参照してください。</p>
URL フィルタリング	ターム ベース	<p>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。</p> <p>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。</p>

ライセンス	期間	付与される機能
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	<p>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。</p> <p>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 (612 ページ) を参照してください。</p> <p>『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。</p>

ファイルポリシーのライセンス要件

次の表では、ファイルポリシーを実装する際に必要なライセンスについて説明します。要件は、選択するアクションとオプションによって異なります。

表 4: ファイルポリシーのライセンス要件

アクション	[ファイルの保存 (Store Files)] オプションの選択	ライセンス要件
許可 ブロック ブロック (リセットあり)	なし	脅威
許可 ブロック ブロック (リセットあり)	あり	脅威 + マルウェア
マルウェアクラウドルックアップ マルウェアブロック マルウェアブロック (リセットあり)	「あり」または「なし」のいずれか	脅威 + マルウェア

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 RA VPN 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します。



(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 \(107 ページ\)](#) 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 \(108 ページ\)](#) 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 \(109 ページ\)](#)
- [デバイスの登録解除 \(109 ページ\)](#)

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。

始める前に

デバイスの登録時には、そのデバイスだけが登録されます。高可用性のために設定されているデバイスの場合は、その装置を登録するために、高可用性ペアにあるその他の装置にログイン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、[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 [デバイスの登録 (Register Device)] 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) シスコクラウドサービスの登録リージョンを選択します。

登録後、このリージョンを変更する必要がある場合は、デバイスの登録を解除してから再度登録し、新しいリージョンを選択する必要があります。

- e) 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。

f) [デバイスの登録 (Register Device)] 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RAVPN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。

高可用性の設定で動作する装置の場合は、アクティブな装置でのみライセンスを有効化または無効化します。スタンバイ装置が必要なライセンスを要求 (または解放) すると、次の設定の展開時にスタンバイ装置に変更内容が反映されます。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。

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。また、デバイスはクラウドおよびクラウドサービスから登録解除されます。

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。

始める前に

デバイスの登録解除時には、そのデバイスだけが登録解除されます。ハイアベイラビリティのために設定されているデバイスの場合は、その装置を登録解除するために、ハイアベイラビリティペアにあるその他の装置にログイン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、[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 [デバイスの登録解除 (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 1 部

システム モニタリング

- [デバイスのモニタリング](#) (113 ページ)
- [Cisco ISA 3000 のアラーム](#) (137 ページ)



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](#) (113 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](#) (117 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](#) (121 ページ)
- [イベントの表示](#) (121 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、ディスクバリデータ、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。
- リモートアクセス VPN 接続プロファイルの設定時に、[復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] オプションを選択した場合、または **sysopt connection permit-vpn** コマンドをイネーブルにした場合は、すべてのサイト間またはリモートアクセス VPN トラフィックがインスペクションとアクセス コントロール ポリシーをバイパスします。したがって、このトラフィックに対する接続イベントは発生せず、トラフィックは統計ダッシュボードには反映されません。

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。Syslog サーバにファイル/マルウェアイベントを送信するには、**[デバイス (Device)] > [システム設定 (System Settings)] > [ロギング設定 (Logging Settings)]** でサーバを設定します。

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](#) (166 ページ) を参照してください。

Cisco Threat Response などの Cisco Cloud ベースのサービスを使用したイベントの評価

イベント ビューアと独自の syslog サーバを使用することに加えて、接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントをシスコのクラウドベース サーバに送信できます。Cisco Threat Response などのシスコのクラウドベース サービスは、そのクラウドサーバからイベントをプルできます。ユーザはこれらのサービスを使用してイベントを評価できます。

これらのクラウドベースのサービスはFTD と FDM で別々になっています。これらのイベントをシスコのクラウドに送信する必要があるサービスを使用する場合は、[\[デバイス \(Device\)\] > \[システム設定 \(System Settings\)\] > \[クラウドサービス \(Cloud Services\)\]](#) ページで接続を有効にする必要があります。[Cisco Cloud へのイベントの送信](#) (712 ページ) を参照してください。

米国地域では <https://visibility.amp.cisco.com/> で、EU 地域では <https://visibility.eu.amp.cisco.com> で、Cisco Threat Response に接続できます。アプリケーションの使い方と利点についての動画は、YouTube でご視聴いただけます (<http://cs.co/CTRvideos>)。FTD での Cisco Threat Response の使い方の詳細については、『*Firepower And CTR Integration Guide*』を参照してください (<https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>)。

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。

ハイ アベイラビリティ グループ内の装置のダッシュボードには、そのデバイスの統計情報のみ表示されます。統計情報は装置間で同期されません。



- (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

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 ホワイティスト、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。

(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。
- [セッション (Sessions)] : Firepower Device Manager ユーザ セッションを表示および管理します。詳細については、[Firepower Device Manager ユーザ セッションの管理 \(738 ページ\)](#) を参照してください。

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 Command Reference』 (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** はデバイスを経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表示されます。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 \(113 ページ\)](#) 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するには、[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 \(123 ページ\)](#) 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 \(125 ページ\)](#) 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 \(124 ページ\)](#) 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 \(125 ページ\)](#) 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。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。

[宛先セキュリティ グループ タグ、宛先セキュリティ グループ タグ名 (Destination Security Group Tag, Destination Security Group Tag Name)]

宛先に関連付けられている TrustSec セキュリティ グループ タグの番号と名前 (存在する場合)。

[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。

[カスタム検出 (Custom Detection)]

ユーザがカスタム検出リストにファイルを追加したことを示します。

[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)]ルールがファイルを処理し、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、接続が記録された理由を説明しています。該当しない場合、このフィールドは空になります。

理由	説明
[DNS ブロック (DNS Block)]	ドメイン名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。[DNS ブロック (DNS Block)]の理由は、DNS ルールアクションに応じて、[ブロック (Block)]、[ドメインが見つかりません (Domain not found)]、[シンクホール (Sinkhole)]のアクションと対として組み合わせられます。
[DNS モニタ (DNS Monitor)]	システムはドメイン名とセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
[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。
[ファイルカスタム検出 (File Custom Detection)]	カスタム検出リストにある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。

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パケット (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ット数。

[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、フィールド 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。

[送信元セキュリティ グループ タグ、送信元セキュリティ グループ タグ名 (Source Security Group Tag, Source Security Group Tag Name)]

送信元に関連付けられている TrustSec セキュリティ グループ タグの番号と名前 (存在する場合)。

[実際のSSLアクション (SSL Actual Action)]

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。
[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

Cisco ISA 3000 のアラーム

Cisco ISA 3000 デバイスのアラームシステムを設定して、望ましくない状況になったときに警告することができます。

- [アラームについて \(137 ページ\)](#)
- [アラームのデフォルト \(140 ページ\)](#)
- [ISA 3000 のアラームの設定 \(140 ページ\)](#)
- [アラームのモニタリング \(147 ページ\)](#)

アラームについて

さまざまな条件でアラームを発行するように ISA 3000 を設定できます。いずれかの条件が設定と一致しない場合、アラームがトリガーされます。これにより、LED、Syslog メッセージ、SNMP トラップによって、またアラーム出力インターフェイスに接続された外部デバイスを通じて、アラートがレポートされます。デフォルトでは、トリガーされたアラームにより Syslog メッセージだけが発行されます。

次のものをモニタするようにアラーム システムを設定できます。

- 電源
- プライマリおよびセカンダリ温度センサー。
- アラーム入力インターフェイス。

ISA 3000 には内部センサーに加えて 2 つのアラーム入力インターフェイスと 1 つのアラーム出力インターフェイスがあります。アラーム入力インターフェイスにはドアセンサーなどの外部センサーを接続できます。アラーム出力インターフェイスにはブザーやライトなどの外部アラーム デバイスを接続できます。

アラーム出力インターフェイスはリレーメカニズムです。アラーム条件に応じて、リレーが活性化または非活性化されます。リレーが活性化されると、インターフェイスに接続されているすべてのデバイスがアクティブになります。リレーが非活性化されると、接続されているすべてのデバイスが非アクティブ状態になります。リレーは、アラームがトリガーされているかぎり、活性化状態のままになります。

外部センサーとアラームリレーの接続については、『[Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide](#)』を参照してください。

アラーム入力インターフェイス

アラーム入力インターフェイス（または接点）は外部センサー（ドアが開いているかどうかを検出するセンサーなど）に接続できます。

各アラーム入力インターフェイスには対応する LED があります。これらの LED は各アラーム入力のアラーム ステータスを示します。アラーム入力ごとにトリガーと重大度を設定できます。LEDに加えて、出力リレーのトリガー（外部アラームをアクティブにするため）、Syslog メッセージの送信、および SNMP トラップの送信を行うように接点を設定できます。

次の表に、アラーム入力のアラーム状態に応じた LED のステータスを示します。また、アラーム入力に対する出力リレー、Syslog メッセージ、および SNMP トラップの応答を有効にしている場合のそれらの動作も示します。

Alarm Status	LED	出力リレー	Syslog	SNMP トラップ
アラームが設定されていない	消灯	—	—	—
アラームがトリガーされていない	グリーンに点灯	—	—	—
アラームがアクティブになる	マイナー アラーム：赤色で点灯 メジャー アラーム：赤色で点滅	リレーの電源が入る	syslog が生成される	SNMP トラップが送信される
アラーム終了	グリーンに点灯	リレーの電源がオフになる	syslog が生成される	—

アラーム出力インターフェイス

アラーム出力インターフェイスにはブザーやライトなどの外部アラームを接続できます。

アラーム出力インターフェイスはリレーとして機能します。また、このインターフェイスには、入力インターフェイスに接続された外部センサーや、デュアル電源センサー、温度センサーなどの内部センサーのアラームステータスを示す、対応する LED があります。出力リレーをアクティブにする必要があるアラームがある場合は、そのアラームを設定します。

次の表に、アラーム状態に応じた LED と出力リレーのステータスを示します。また、アラームに対する Syslog メッセージおよび SNMP トラップの応答を有効にしている場合のそれらの動作も示します。

Alarm Status	LED	出力リレー	Syslog	SNMP トラップ
アラームが設定されていない	消灯	—	—	—
アラームがトリガーされていない	グリーンに点灯	—	—	—
アラームがアクティブになる	レッド（点灯）	リレーの電源が入る	syslog が生成される	SNMP トラップが送信される
アラーム終了	グリーンに点灯	リレーの電源がオフになる	syslog が生成される	—

Syslog アラーム

デフォルトでは、アラームがトリガーされるとシステムは syslog メッセージを送信します。メッセージを送信しない場合は、syslog メッセージングを無効にすることができます。

syslog アラームを機能させるには、**[デバイス (Device)] > [システム設定 (System Settings)] > [ロギング設定 (Logging Settings)]** で診断ロギングも有効にする必要があります。syslog サーバを設定して **[Syslog フィルタ (Syslog Filter)]** または **[コンソールロギング (Console Logging)]** を有効にするか、両方を設定します。

診断ロギングの宛先を有効にしなければ、アラームシステムはどこにも syslog メッセージを送信しません。

SNMP トラップアラーム

必要に応じて、SNMP トラップを SNMP サーバに送信するようにアラームを設定できます。SNMP トラップアラームが機能するには、SNMP を設定する必要があります。

FlexConfig を使用して SNMP を設定します。たとえば、内部インターフェイスを介して使用できる SNMP サーバ (192.168.1.25) への SNMP 接続を有効化し、SNMP サーバを使用してトラップだけを受信するには、FlexConfig オブジェクトを作成して次のコマンドを発行します。コミュニティストリングは、SNMP サーバで設定されているものに置き換えてください。

```
snmp-server host inside 192.168.1.25 trap
snmp-server community your-string
```

ネゲートテンプレートは次のようになります。

```
no snmp-server host inside 192.168.1.25 trap
no snmp-server community your-string
```

オブジェクトを作成したら、そのオブジェクトを FlexConfig ポリシーに追加し (**[デバイス (Device)] > [詳細設定 (Advanced Configuration)] > [FlexConfig]**)、設定を展開します。

これは最小の例であり、SNMP バージョン 1 および 2c に関して機能します。SNMP バージョン 3 の設定方法を含む SNMP の設定の詳細については、最新バージョンの ASA ソフトウェア用の『CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide』にある SNMP に関する章を参照してください。このガイドは、<https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html> から入手できます。

アラームのデフォルト

次の表に、アラーム入力インターフェイス（コンタクト）、冗長電源、および温度のデフォルト設定を示します。

	アラーム	Trigger	重大度	SNMP トラップ	出カリー	syslog メッセージ
アラーム コンタクト 1	イネーブル	クローズ状態	Minor	ディセーブル	ディセーブル	イネーブル
アラーム コンタクト 2	イネーブル	クローズ状態	Minor	ディセーブル	ディセーブル	イネーブル
冗長電源（有効な場合）	イネーブル	—	—	ディセーブル	ディセーブル	イネーブル
温度	プライマリ温度アラームで有効（高温と低温のデフォルトしきい値はそれぞれ 92 °C と -40 °C）。 セカンダリアラームでは無効。	—	—	プライマリ温度アラームについて有効	プライマリ温度アラームについて有効	プライマリ温度アラームについて有効

ISA 3000 のアラームの設定

ISA 3000 のアラームを設定するには FlexConfig を使用します。ここでは、さまざまなタイプのアラームの設定方法について説明します。

アラーム入力コンタクトの設定

アラーム入力コンタクト（インターフェイス）を外部センサーに接続する場合、センサーからの入力に基づいてアラームを発行するようコンタクトを設定できます。実際には、デフォルトで、コンタクトはクローズ状態つまりコンタクトを流れる電流が停止するとsyslogメッセージを送信するようになっています。デフォルトでは要件が満たされない場合にのみ、コンタクトを設定する必要があります。

アラームコンタクトには1および2の番号が付いているため、正しく設定するためにどのように物理ピンを接続するのかを理解する必要があります。コンタクトを個別に設定します。

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。たとえば、**Enable_Alarm_Contact** と入力します。
- ステップ5 [テンプレート (Template)] エディタで、コンタクトの設定に必要なコマンドを入力します。
 - a) アラームコンタクトの説明を設定します。

alarm contact {1 | 2} description *string*

たとえば、コンタクト1の説明を「Door Open」に設定するには、次のように入力します。

```
alarm contact 1 description Door Open
```
 - b) アラームコンタクトの重大度を設定します。

alarm contact {1 | 2 | any} severity {major | minor | none}

1つのコンタクトを設定するのではなく、**any** を指定してすべてのコンタクトの重大度を変更できます。重大度によって、コンタクトに関連付けられているLEDの動作が制御されます。

 - **major** : LED が赤色で点滅します。
 - **minor** : LED が赤色で点灯します。これがデフォルトです。
 - **none** : LED は消灯しています。

たとえば、コンタクト1の重大度をメジャーに設定するには、次のように入力します。

```
alarm contact 1 severity major
```
 - c) アラームコンタクトのトリガーを設定します。

alarm contact {1 | 2 | any} trigger {open | closed}

1つのコンタクトを設定するのではなく、**any**を指定してすべてのコンタクトのトリガーを変更できます。トリガーは、アラート信号を発する電気条件を決定します。

- **open** : コンタクトの通常状態はクローズです。つまり、コンタクトに電流が流れています。コンタクトがオープンになる、つまり電流が停止するとアラートがトリガーされます。
- **closed** : コンタクトの通常状態はオープンです。つまり、コンタクトに電流は流れていません。コンタクトがクローズになる、つまり電流がコンタクトを流れ始めるとアラートがトリガーされます。これはデフォルトです。

たとえば、ドアセンサーをアラーム入力コンタクト1に接続して、通常状態ではアラームコンタクトに電流は流れていない（オープン）とします。ドアが開くとコンタクトはクローズになり、アラームコンタクトに電流が流れます。アラームトリガーをクローズに設定しているため、電流が流れ始めたらアラームはオフになります。

```
alarm contact 1 trigger closed
```

- d) アラームコンタクトがトリガーされるときに実行するアクションを設定します。

alarm facility input-alarm {1 | 2} {relay | syslog | notifies}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー (relay)] : アラーム出力リレーに通電します。これにより、ブザーやフラッシュライトなどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog] : syslog メッセージを送信します。このオプションは、デフォルトで有効です。
- [通知 (notifies)] : SNMP トラップを送信します。

たとえば、アラーム入力コンタクト1のすべてのアクションを有効にするには、次のように入力します。

```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

- ステップ6** [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。

これらすべてのコマンドでは **no** 形式を使用して設定を無効化し、デフォルト設定に戻します。たとえば、テンプレートにこの手順で示したすべてのコマンド例が含まれている場合、ネゲートテンプレートは次のようになります。

```
no alarm contact 1 description Door Open
no alarm contact 1 severity major
no alarm contact 1 trigger closed
```

```
no alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 syslog
no alarm facility input-alarm 1 notifies
```

ステップ 7 [OK] をクリックしてオブジェクトを保存します。

ステップ 8 オブジェクトを FlexConfig ポリシーに追加します。

- a) 目次で [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。
- b) [グループリスト (Group List)] で [+] をクリックします。
- c) **Enable_Alarm_Contact** オブジェクトを選択して、[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。

- 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 9 展開が完了したら、CLI コンソールまたは SSH セッションで、**show running-config** コマンドを使用し、実行中の設定が正しく変更されていることを確認します。外部センサーをテストして、アラームがトリガーされていることを確認します。

電源アラームの設定

ISA 3000 には、電源装置が 2 台搭載されています。デフォルトでは、システムはシングル電源モードで稼働しています。ただし、デュアルモードでシステムを稼働するよう設定できます。その場合、プライマリ電源が故障すると 2 つ目の電源が自動的に電力を供給します。デュアルモードを有効にすると、電源アラームが自動的に有効になって syslog アラートが送信されますが、アラートを無効にしたり、SNMP トラップまたはアラーム ハードウェア リレーを有効にすることもできます。

次の手順では、デュアルモードを有効にする方法と電源アラームを設定する方法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)] 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。たとえば、**Enable_Power_Supply_Alarm** と入力します。

ステップ 5 [テンプレート (Template)] エディタで、電源アラームの設定に必要なコマンドを入力します。

- a) デュアル電源モードを有効にします。

```
power-supply dual
```

次に例を示します。

```
power-supply dual
```

- b) 電源アラームがトリガーされるときに実行するアクションを設定します。

alarm facility power-supply rps {relay | syslog | notifies | disable}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー (relay)] : アラーム出力リレーに通電します。これにより、ブザーやフラッシュライトなどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog] : syslog メッセージを送信します。このオプションは、デフォルトで有効です。
- [通知 (notifies)] : SNMP トラップを送信します。
- [無効化 (disable)] : 電源アラームを無効にします。電源アラームに設定されたその他のアクションは動作しなくなります。

たとえば、電源アラームのすべてのアクションを有効にするには、次のように入力します。

```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

- ステップ 6** [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。

これらすべてのコマンドでは **no** 形式を使用して設定を無効化し、デフォルト設定に戻します。たとえば、テンプレートにこの手順で示したすべてのコマンド例が含まれている場合、ネゲートテンプレートは次のようになります。

```
no power-supply dual
no alarm facility power-supply rps relay
no alarm facility power-supply rps syslog
no alarm facility power-supply rps notifies
```

- ステップ 7** [OK] をクリックしてオブジェクトを保存します。

- ステップ 8** オブジェクトを FlexConfig ポリシーに追加します。

- a) 目次で [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。
- b) [グループリスト (Group List)] で [+] をクリックします。
- c) Enable_Power_Supply_Alarm オブジェクトを選択して、[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。

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9 展開が完了したら、CLI コンソールまたはSSHセッションで、**show running-config** コマンドを使用し、実行中の設定が正しく変更されていることを確認します。

温度アラームの設定

デバイスのCPUカードの温度に基づいてアラームを設定できます。

プライマリ温度範囲とセカンダリ温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、およびSNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は-40°C～92°Cです。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35°C～85°Cの範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温のいずれかを設定すると、プライマリ設定にデフォルト以外の値を設定していたとしても、対応するプライマリ設定はこの設定によって無効になります。2つの異なる高温アラームと2つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみ的高温値および低温値を設定する必要があります。

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 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。たとえば、**Enable_Temperature_Alarm** と入力します。

ステップ5 [テンプレート (Template)] エディタで、温度アラームの設定に必要なコマンドを入力します。

a) 許容温度範囲を設定します。

```
alarm facility temperature {primary | secondary} {low | high} temperature
```

温度は摂氏で示されます。プライマリアラームの許容範囲は-40～92で、これがデフォルト範囲でもあります。セカンダリアラームの許容範囲は、-35～85です。低い値は、高い値より小さくする必要があります。

たとえば、セカンダリアラームの許容範囲内で、より制限された温度範囲の -20 ~ 80 を設定するには、次のようにセカンダリアラームを設定します。

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

- b) 温度アラームがトリガーされたときに実行するアクションを設定します。

alarm facility temperature {primary | secondary} {relay | syslog | notifies}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー (relay)] : アラーム出力リレーに通電します。これにより、ブザーやフラッシュライトなどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog] : syslog メッセージを送信します。
- [通知 (notifies)] : SNMP トラップを送信します。

たとえば、セカンダリ温度アラームのすべてのアクションを有効にするには、次のように入力します。

```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

- ステップ 6** [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。

次のすべてのコマンドでは、**no** 形式を使用してデフォルト設定に戻したり（プライマリアラームの場合）、設定を無効にします（セカンダリアラームの場合）。たとえば、テンプレートにこの手順で示したすべてのコマンド例が含まれている場合、ネゲートテンプレートは次のようになります。

```
no alarm facility temperature secondary low -20
no alarm facility temperature secondary high 80
no alarm facility temperature secondary relay
no alarm facility temperature secondary syslog
no alarm facility temperature secondary notifies
```

- ステップ 7** [OK] をクリックしてオブジェクトを保存します。

- ステップ 8** オブジェクトを FlexConfig ポリシーに追加します。

- a) 目次で [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。
- b) [グループリスト (Group List)] で [+] をクリックします。
- c) Enable_Temperature_Alarm オブジェクトを選択して、[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。

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 9 展開が完了したら、CLI コンソールまたは SSH セッションで、**show running-config** コマンドを使用し、実行中の設定が正しく変更されていることを確認します。

アラームのモニタリング

ここでは、アラームのモニタおよび管理方法について説明します。

アラーム ステータスのモニタリング

CLI で次のコマンドを使用してアラームをモニタすることができます。

- **show alarm settings**

使用可能な各アラームの現在の設定が表示されます。

- **show environment alarm-contact**

入力アラームコンタクトの物理ステータスに関する情報が表示されます。

- **show facility-alarm relay**

出力リレーをトリガーしたアラームに関する情報が表示されます。

- **show facility-alarm status[info |major |minor]**

トリガーされたすべてのアラームに関する情報が表示されます。**major** ステータスまたは **minor** ステータスでフィルタリングによって表示を絞り込むことができます。**info** キーワードを使用すると、キーワードを使用しない場合と同じ出力になります。

アラームに関する Syslog メッセージのモニタリング

設定するアラームのタイプに応じて、次の Syslog メッセージが表示される場合があります。

デュアル電源アラーム

- %FTD-1-735005: Power Supply Unit Redundancy OK
- %FTD-1-735006: Power Supply Unit Redundancy Lost

温度アラーム

これらのアラームでは、「*Celsius*」は、デバイス上で検出された温度（摂氏単位）に置き換えられます。

- %FTD-6-806001: Primary alarm CPU temperature is High *Celsius*

- %FTD-6-806002: Primary alarm for CPU high temperature is cleared
- %FTD-6-806003: Primary alarm CPU temperature is Low *Celsius*
- %FTD-6-806004: Primary alarm for CPU Low temperature is cleared
- %FTD-6-806005: Secondary alarm CPU temperature is High *Celsius*
- %FTD-6-806006: Secondary alarm for CPU high temperature is cleared
- %FTD-6-806007: Secondary alarm CPU temperature is Low *Celsius*
- %FTD-6-806008: Secondary alarm for CPU Low temperature is cleared

アラーム入力コンタクトアラーム

これらのアラームでは、「*description*」は、設定したコンタクトの説明です。

- %FTD-6-806009: Alarm asserted for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806010: Alarm cleared for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806011: Alarm asserted for ALARM_IN_2 *alarm_2_description*
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*

外部アラームをオフにする

アラーム出力にアタッチされる外部アラームを使用していて、アラームがトリガーされる場合、**clear facility-alarm output** コマンドを使用してデバイス CLI から外部アラームをオフにすることができます。このコマンドは、出力ピンの電源を切り、出力 LED もオフにします。



第 II 部

再利用可能なオブジェクト

- [オブジェクト \(151 ページ\)](#)
- [証明書 \(169 ページ\)](#)
- [アイデンティティソース \(179 ページ\)](#)



第 6 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 \(151 ページ\)](#)
- [オブジェクトの管理 \(155 ページ\)](#)

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 (615 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 (160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 管理Webサーバ。	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 (172ページ) を参照してください。
DNSグループ	管理インターフェイスとデータインターフェイスのDNS設定	DNSグループは、DNSサーバおよび関連付けられているいくつかの属性のリストを定義します。 www.example.comなどの完全修飾ドメイン名 (FQDN) をIPアドレスに解決するには、DNSサーバが必要です。 DNSグループの設定 (698ページ) を参照してください。
イベントリストフィルタ	選択したログの宛先のシステムログ設定。	イベントリストフィルタは、syslogメッセージ用のカスタムフィルタリストを作成します。これらを使用して、syslogサーバまたは内部ログバッファなどの特定のログの場所へ送信されるメッセージを制限できます。 イベントリストフィルタの設定 (695ページ) を参照してください。
位置情報 (GeoLocation)	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 (165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
アイデンティティソース	アイデンティティポリシー リモートアクセス VPN Firepower Device Manager へのアクセス。	アイデンティティソースは、ユーザアカウントを定義するサーバとデータベースです。この情報は、IP アドレスに関連付けられているユーザ ID を提供したり、Firepower Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。 アイデンティティソース (179 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 (577 ページ) を参照してください。
IPsec プロポーザル	VPN	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。 IPsec プロポーザルの設定 (583 ページ) を参照してください。
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	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）。 ネットワークオブジェクトとグループの設定 (156 ページ) を参照してください。
ポート	セキュリティポリシー	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）。 ポートオブジェクトとグループの設定 (157 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
秘密キー	Smart CLI および FlexConfig ポリシー	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。 秘密キーオブジェクトの設定 (791 ページ) を参照してください。
セキュリティゾーン	セキュリティ ポリシー	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。 セキュリティゾーンの設定 (159 ページ) を参照してください。
SLA モニタ	スタティック ルート	SLA モニタは、スタティック ルートのモニタリングに使用するターゲット IP アドレスを定義します。モニタが、ターゲット IP アドレスに到達できなくなったと判断した場合、システムはバックアップ スタティック ルートをインストールできます。 SLA モニタ オブジェクトの設定 (346 ページ) を参照してください。
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 ファイル/マルウェアポリシー	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 サーバの設定 (166 ページ) を参照してください。
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 (163 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
Users	リモート アクセス VPN	リモート アクセス VPN で使用するユーザアカウントをデバイスで直接作成できます。外部認証ソースの代わりに、またはそれに加えて、ローカルユーザアカウントを使用できます。 ローカルユーザの設定 (197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レクト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)。
- [範囲 (Range)] : ハイフンで区切られた開始アドレスと終了アドレスを備えたアドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。たとえば、192.168.1.10-192.168.1.250 または 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100 とします。
- [FQDN] : www.example.com などの単一の完全修飾ドメイン名を入力します。ワイルドカードを使用することはできません。また、[DNS解決 (DNS Resolution)] を選択して、IPv4 アドレス、IPv6 アドレス、または IPv4 アドレスと IPv6 アドレスの両方を FQDN と関連付けるかどうかも決定します。デフォルトは、IPv4 と IPv6 の両方です。これらのオブジェクトはアクセス制御ルールのみで使用できます。ルールでは、DNSルックアップによって FQDN 用に取得された IP アドレスを照合します。

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またはグループを選択するには、[+] 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にのみ存在できます。

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 ゾーンの [モード (Mode)] を選択します。

[ルーテッド (Routed)] または [パッシブ (Passive)] のいずれかのインターフェイスモードに直接関連付けます。ゾーンには、1 つのタイプのインターフェイスを含めることができます。通過トラフィックの通常のゾーンには、[ルーテッド (Routed)] を選択します。

ステップ 5 [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 6 [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、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 ポリシーにブロックを実装できます。

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的場合、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。


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。 [リモート syslog サーバのログgingsの設定 \(691 ページ\)](#) を参照してください。
- ファイル/マルウェアイベント。[デバイス (Device)] > [システム設定 (System Settings)] > [ロギング設定 (Logging Settings)] で syslog サーバを設定します。

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。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。

- [IPアドレス (IP Address)] : syslog サーバの IP アドレスを入力します。
- [プロトコルタイプ (Protocol Type)]、[ポート番号 (Port Number)] : プロトコルを選択して、syslog に使用するポート番号を入力します。デフォルトは UDP/514 です。[TCP] を選択すると、システムは syslog サーバが利用できない場合を認識して、サーバが再度利用可能になるまでイベントの送信を停止できます。デフォルト UDP ポートは 514、デフォルト TCP ポートは 1470 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。

- [デバイスログのインターフェイス (Interface for Device Logs)] : 診断 syslog メッセージの送信に使用するインターフェイスを選択します。接続、侵入、ファイル、マルウェアの各イベントタイプでは、常に管理インターフェイスが使用されます。インターフェイスの選択によって、syslogメッセージに関連付けられる IP アドレスが決まります。次のオプションのいずれかを選択します。
 - [データインターフェイス (Data Interface)] : 選択したデータ インターフェイスを診断 syslog メッセージに使用します。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。診断インターフェイス (物理的な管理インターフェイス) 経由でアクセスできる場合は、このオプションではなく [管理インターフェイス (Management Interface)] を選択することを推奨します。パッシブ インターフェイスを選択することはできません。

データインターフェイスで通信する場合、接続、侵入、ファイル、およびマルウェアの syslog メッセージでは、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。
 - [管理インターフェイス (Management Interface)] : すべてのタイプの syslog メッセージに仮想管理インターフェイスを使用します。データインターフェイスで通信する場合、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。

ステップ 4 [OK] をクリックして変更を保存します。



第 7 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（169 ページ）](#)
- [証明書の設定（172 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 \(170 ページ\)](#) 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、ユーザが自身を特定し、自分のユーザ名にデバイスの 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 レルム (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。

管理 Web サーバ（管理アクセス システム設定）：内部証明書

（オプション）Firepower Device Manager は Web ベースのアプリケーションであり、Web サーバで動作します。お使いのブラウザで有効として受け入れられる証明書をアップロードすると、Untrusted Authority の警告を受けるのを回避できます。

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。

サイト間 VPN：内部および信頼できる CA 証明書

サイト間 VPN 接続に証明書認証を使用する場合は、接続内のローカルピア認証に使用される内部アイデンティティ証明書を選択する必要があります。これは VPN 接続の定義の一部ではありませんが、システムがピアを認証できるように、ローカルおよびリモートピアのアイデンティティ証明書に署名するために使用した信頼できる CA 証明書をアップロード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 opendss.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 \(169 ページ\)](#) 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 \(170 ページ\)](#) 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
- DefaultWebserverCertificate
- 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 \(173 ページ\)](#)
- [自己署名内部および内部 CA 証明書の生成 \(175 ページ\)](#)
- [信頼できる CA 証明書のアップロード \(176 ページ\)](#)

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 \(171 ページ\)](#) 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 \(175 ページ\)](#) 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 \(170 ページ\)](#) 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: *.crt) 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
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZlZlc2V2Z21kZ210
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPhtK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZ1zJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfwxwCUn
RV7LRfQGfYd76V/5uor4Wx2ZCjgy6+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/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTikB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNzkBhOsPs1A8e60r5mImeDrtw+
Cc005cSfnlTAw5CgcGkcxTCaGIZmXmkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdlQgW/h39XFpkEXiIgmDL
(... 5 lines removed ...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2ST1Z3jERMZd29fjIRuJ9jpfC21IDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuuv6db8Rh+7L
MUOx09tvtbBUy9REJq1YJWTKpeKD+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 \(173 ページ\)](#) 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 \(170 ページ\)](#) 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 \(173 ページ\)](#) 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 \(170 ページ\)](#) 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 証明書を貼り付けます。

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
BAYTA1VTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAxk
OTIuMTY4LjEuMTEUMBIGA1UEAwWLTkyLjE2OC4xLjEwHhcNMjYxMDI3MjIzNDE3
WhcNMjYxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVVzELMAkGA1UECAwCVFgxDzAN
BgNVBACMBmFlc3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjEwExFDASBGNVBAMMCzE5
Mi4xNjguMS4xMIIICiJANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5J1F58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6H0gK1OwXbRvOdkstzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN200jv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 5 [OK] をクリックします。



第 8 章

アイデンティティ ソース

アイデンティティ ソースは、ユーザ アカウントを定義するサーバとデータベースです。この情報は、IP アドレスに関連付けられているユーザ ID を提供したり、Firepower Device Manager へのリモート アクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

ここでは、アイデンティティ ソースの定義方法について説明します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。

- [アイデンティティ ソースについて \(179 ページ\)](#)
- [Active Directory \(AD\) アイデンティティレルム \(181 ページ\)](#)
- [RADIUS サーバおよびグループ \(188 ページ\)](#)
- [Identity Services Engine \(ISE\) \(192 ページ\)](#)
- [ローカル ユーザ \(196 ページ\)](#)

アイデンティティ ソースについて

アイデンティティ ソースは、組織内のユーザのユーザアカウントを定義する AAA サーバおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザ ID を提供したり、Firepower Device Manager へのリモート アクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

[**オブジェクト (Objects)**] > [**アイデンティティ ソース (Identity Sources)**] ページを使用して、ソースを作成および管理します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。

サポートされているアイデンティティ ソースとその使用 방법은次のとおりです。

Active Directory (AD) アイデンティティレルム

Active Directory は、ユーザアカウントおよび認証情報を提供します。[Active Directory \(AD\) アイデンティティレルム \(181 ページ\)](#) を参照してください。

このソースは、次の目的で使用できます。

- リモートアクセス VPN (プライマリアイデンティティ ソースとして)。AD を RADIUS サーバと連携して使用することができます。

- アイデンティティポリシー（アクティブ認証用、およびパッシブ認証で使用されるユーザ アイデンティティ ソースとして）。

Cisco Identity Services Engine (ISE) または Cisco Identity Services Engine Passive Identity Connector (ISE PIC)

ISE を使用している場合は、Firepower Threat Defense デバイスと ISE 展開を統合できます。[Identity Services Engine \(ISE\) \(192 ページ\)](#) を参照してください。

このソースは、次の目的で使用できます。

- アイデンティティポリシー（ISE からユーザアイデンティティを収集するためのパッシブアイデンティティ ソースとして）。

RADIUS サーバ、RADIUS サーバグループ

RADIUS サーバを使用している場合は、それらを Firepower Device Manager で使用することもできます。それぞれのサーバを個別のオブジェクトとして定義し、それらをサーバグループ（特定グループ内のサーバは互いのコピー）に入れる必要があります。サーバグループを機能に割り当て、個々のサーバは割り当てないでください。[RADIUS サーバおよびグループ \(188 ページ\)](#) を参照してください。

このソースは、次の目的で使用できます。

- 認証、および許可、アカウントिंगのアイデンティティソースとしてのリモートアクセス VPN。AD を RADIUS サーバと連携して使用することができます。
- アイデンティティ ポリシー（リモートアクセス VPN ログインからユーザアイデンティティを収集するためのパッシブアイデンティティ ソースとして）。
- FDM または FTD CLI 管理ユーザの外部認証。異なる認可レベルの複数の管理ユーザをサポートできます。これらのユーザは、システムにログインして、デバイスの設定とモニタリングを行うことができます。

LocalIdentitySource

これはローカルユーザデータベースです。これには Firepower Device Manager で定義したユーザが含まれます。このデータベースのユーザアカウントを管理するには、**[オブジェクト (Objects)] > [ユーザ (Users)]** を選択します。[ローカルユーザ \(196 ページ\)](#) を参照してください。



- (注) ローカルアイデンティティ ソース データベースには、CLI アクセス用に CLI で設定するユーザ (**configure user add** コマンドを使用) は含まれません。CLI ユーザは、Firepower Device Manager で作成するユーザとはまったく別になります。

このソースは、次の目的で使用できます。

- リモートアクセス VPN（プライマリまたはフォールバック アイデンティティ ソースとして）。

- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザ アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

Active Directory (AD) アイデンティティレルム

Microsoft Active Directory (AD) はユーザアカウントを定義します。Active Directory ドメイン用に AD アイデンティティレルムを作成できます。ここでは、AD アイデンティティレルムの定義方法について説明します。

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
last name	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

ユーザ数の制限

Firepower Device Manager はディレクトリ サーバから最大 50,000 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 50,000 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 50,000 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 50,000 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。

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。

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。サポートする必要がある AD ドメインごとに個別のレルムを作成します。

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。
- **アクセス制御、SSL 復号**：ユーザの基準でレルムを選択すると、レルム内のすべてのユーザにルールを適用できます。

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ム (Create New Identity Realm)]** リンクをクリックして、アイデンティティレ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。

- AD レムを作成するには、**[+] > [AD]** をクリックします。作成可能なのは 1 つのレムのみです。
- 既存のレムを編集するには、そのレムの編集アイコン (🔍) 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 (trash can)]** アイコン (🗑️) をクリックします。

ステップ 3 基本レムのプロパティを設定します。

- **[名前 (Name)]** : ディレクトリ レムの名前。
- **[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=administrator,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 \(182 ページ\)](#) 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 レルムに複数のサーバがある場合は、[別の設定の追加 (Add Another Configuration)] をクリックし、追加サーバごとのプロパティを入力します。

最大 10 の AD サーバをレルムに追加することができます。これらのサーバは互いに複製である必要があります、同じ AD ドメインをサポートする必要があります。

各サーバエントリは適宜折りたたんだり展開したりすることができます。セクションには、ホスト名または IP アドレスとポートのラベルが付けられます。

ステップ 6 [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トリ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 \(186 ページ\)](#) を参照してください。

ステップ 7 [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。

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=administrator,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（663 ページ）](#) を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバを使用して、リモートアクセス VPN 接続、および FDM と FTDCLI 管理ユーザの認証および認可を行うことができます。たとえば、Cisco Identity Services Engine (ISE) とその RADIUS サーバも使用する場合は、Firepower Device Manager でそのサーバを使用できます。

RADIUS サーバを使用するように機能を設定する場合は、個別のサーバではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバの集合です。グループに複数のサーバがある場合は、それらは、1つのサーバが使用できなくなった場合に冗長性を提供する一連のバックアップサーバを形成します。ただし、サーバが1つしかない場合でも、機能の RADIUS サポートを設定するには、メンバーが1つのグループを作成する必要があります。

ここでは、サポートされている機能でできるように RADIUS サーバおよびグループを設定する方法について説明します。

RADIUS サーバの設定

RADIUS サーバは、AAA（認証、認可、アカウントिंग）サービスを提供します。RADIUS サーバを使用してユーザを認証および認可すると、これらのサーバを Firepower Device Manager と一緒に使用できます。

RADIUS サーバごとにオブジェクトを作成した後、重複サーバの各グループを含む RADIUS サーバグループを作成します。

始める前に

RA VPN のリダイレクト ACL を設定する場合は、スマート CLI を使用して、サーバオブジェクトを作成または編集する前に拡張 ACL を作成する必要があります。オブジェクトの編集集中に ACL を作成することはできません。

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。
- オブジェクトを作成するには、[+] > [RADIUSサーバ (RADIUS Server)] 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** 次のプロパティを設定します。

- [名前 (Name)]: オブジェクトの名前。サーバで設定されているものと一致している必要はありません。
- [サーバ名またはIPアドレス (Server Name or IP Address)]: サーバの完全修飾ホスト名 (FQDN) または IP アドレス。たとえば、radius.example.com または 10.100.10.10 とします。
- [認証ポート (Authentication Port)]: RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト (Timeout)]: 次のサーバに要求を送信する前にサーバからの応答を待機する時間の長さ (1 ~ 300 秒)。デフォルトは 10 秒です。認証トークンの入力を求めるなどのために、このサーバをリモートアクセス VPN のセカンダリ認証ソースとして使用している場合は、このタイムアウトを少なくとも 60 秒に増やします。これによりトークンを取得して入力する時間が得られます。
- [サーバ秘密キー (Server Secret Key)]: (オプション) Firepower Threat Defense デバイスと RADIUS サーバ間でデータを暗号化するために使用される共有秘密キー。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字または下線で開始する必要があります。特殊文字 \$ & - _ . + @ を使用できます。文字列は、RADIUS サーバで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。

ステップ 4 (オプション) リモートアクセス VPN の認可変更設定のためにサーバを使用している場合は、[RA VPNのみ (RA VPN Only)] リンクをクリックし、次のオプションを設定できます。

- [ACLのリダイレクト (Redirect ACL)]: RA VPN リダイレクト ACL を使用する拡張 ACL を選択します。[デバイス (Device)] > [詳細設定 (Advanced Configuration)] > [スマート CLI (Smart CLI)] > [オブジェクト (Objects)] ページのスマート CLI 拡張アクセスリストオブジェクトを使用して、拡張 ACL を作成します。

リダイレクト ACL の目的は、Cisco Identity Services Engine (ISE) がクライアントポスチャを評価できるように、初期トラフィックを ISE に送信することです。ACL は HTTPS トラフィックを ISE に送信する必要がありますが、すでに宛先が ISE に指定されているトラフィック、または名前解決のために DNS サーバに送信されるトラフィックは除きます。例については、[FTD デバイスでの認可変更の設定 \(641 ページ\)](#) を参照してください。

- [RADIUSサーバに接続するために使用されるインターフェイス (Interface Used to Connect to RADIUS Server)]: サーバと通信するとき使用するインターフェイス。[ルートルックアップ経由で解決する (Resolve via Route Lookup)] を選択した場合、システムは常にルーティングテーブルを使用して使用するインターフェイスを決定します。[インターフェイスを手動で選択する (Manually Choose Interface)] を選択すると、システムは常に選択されたインターフェイスを使用します。

認可変更を設定する場合、システムがインターフェイスで CoA リスナーを適切に有効にできるように、特定のインターフェイスを選択する必要があります。

サーバが管理アドレスと同じネットワーク上にある場合 (これは診断インターフェイスを選択することを意味します) 、診断インターフェイスで IP アドレスを設定する必要もあ

ります。管理 IP アドレスを設定するだけでは不十分です。[デバイス (Device)] > [インターフェイス (Interfaces)] に移動し、管理 IP アドレスと同じサブネット上にある診断インターフェイスで IP アドレスを設定します。

FDM 管理アクセスにもこのサーバを使用する場合、このインターフェイスは無視されません。管理アクセスの試行は、管理 IP アドレスを通じて常に認証されます。

ステップ 5 (任意。オブジェクトを編集する場合のみ) [テスト (Test)] をクリックして、システムがサーバに接続できるかどうか確認します。

ユーザ名とパスワードの入力を求められます。テストでは、サーバを接続できるかどうか、接続できる場合はユーザ名が認証されるかどうかを確認します。

ステップ 6 [OK] をクリックします。

RADIUS サーバグループの設定

RADIUS サーバグループには、1 つまたは複数の RADIUS サーバオブジェクトが含まれています。グループ内のサーバは、相互に複製である必要があります。これらのサーバはバックアップサーバのチェーンを形成します。そのため、最初のサーバが利用できなくなると、システムはリスト上の次のサーバを試すことができます。

ある機能に RADIUS サポートを設定する場合、サーバグループを選択する必要があります。したがって、RADIUS サーバが 1 台しかなくても、それを含むサーバグループを作成する必要があります。

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。

- オブジェクトを作成するには、[+] > [RADIUSサーバグループ (RADIUS Server Group)] 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 次のプロパティを設定します。

- [名前 (Name)] : オブジェクトの名前。サーバで設定されているものと一致している必要はありません。
- [デッドタイム (Dead Time)] : 失敗したサーバは、すべてのサーバが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバが失敗した後にすべてのサーバを

再アクティブ化するまで待機する時間の長さ（0～1440分）です。デフォルト値は10分です。

- [最大失敗試行回数 (Maximum Failed Attempts)] : 次のサーバを試行する前に、グループ内の RADIUS サーバに送信された AAA トランザクションの失敗数（応答がなかった要求の数）。1～5を指定できます。デフォルトは3です。最大失敗試行数を超えると、システムはサーバを故障としてマークします。

特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバが応答に失敗した場合、そのグループは非応答と見なされ、フォールバック方式が試行されます。サーバグループはデッドタイムの間、非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバグループへの接続は試行されず、フォールバック方式がすぐに使用されます。

- ダイナミック認証 (RA VPNの場合のみ)、ポート : RADIUS サーバグループ向けの RADIUS ダイナミック認証または認可変更 (CoA) サービスを有効にすると、グループは CoA 通知用に登録され、Cisco Identity Services Engine (ISE) からの指定した CoA ポリシー更新用ポートをリスンします。デフォルトのリスニングポートは 1700 ですが、1024～65535 の範囲で別のポートを指定することができます。このサーバグループを ISE と併せてリモートアクセス VPN で使用する場合にのみ動的認可をイネーブルにします。
- [RADIUSサーバをサポートするレルム (Realm that Supports the RADIUS Server)] : AD サーバを使用してユーザを認証するように RADIUS サーバが設定されている場合は、この RADIUS サーバと組み合わせて使用される AD サーバを指定する AD レルムを選択します。レルムが存在していない場合は、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。
- [RADIUSサーバリスト (RADIUS Server list)] : グループのサーバを定義する RADIUS サーバオブジェクトを最大 16 個選択します。優先順にこれらのオブジェクトを追加します。リストの最初のサーバが、非応答になるまで使用されます。オブジェクトを追加した後に、ドラッグアンドドロップで並び替えることができます。必要なオブジェクトがまだない場合は、[新規RADIUSサーバの作成 (Create New RADIUS Server)] をクリックしてすぐに追加します。

[テスト (Test)] リンクをクリックして、システムがサーバに接続できることを確認することもできます。ユーザ名とパスワードの入力を求められます。テストでは、サーバを接続できるかどうか、接続できる場合はユーザ名が認証されるかどうかを確認します。

ステップ 4 (オプション) [すべてのサーバをテスト (Test All Servers)] ボタンをクリックして、グループ内の各サーバへの接続を確認します。

ユーザ名とパスワードの入力を求められます。システムは、各サーバに接続できるかどうか、各サーバでユーザ名が認証されるかどうかを確認します。

ステップ 5 [OK] をクリックします。

RADIUS サーバおよびグループのトラブルシューティング

次に、外部認証が機能しない場合に確認する項目を示します。

- RADIUS サーバの [テスト (Test)] ボタンとサーバグループオブジェクトを使用して、デバイスからサーバに通信できることを確認します。テストする前に、必ずオブジェクトを保存してください。テストが失敗した場合：
 - テストでは、サーバに設定されているインターフェイスが無視され、常に管理インターフェイスが使用されるので注意してください。RADIUS 認証プロキシが、管理 IP アドレスからの要求に応答するように設定されていない場合、テストは失敗すると予想されます。
 - テスト中に正しいユーザ名/パスワードの組み合わせを入力していることを確認します。正しくない場合は、クレデンシャルが不正であるというメッセージが表示されます。
 - 秘密鍵、ポート、およびサーバの IP アドレスを確認します。ホスト名を使用している場合は、DNS が管理インターフェイス用に設定されていることを確認します。秘密鍵がデバイス設定ではなく RADIUS サーバで変更された可能性を考えます。
 - テストが引き続き失敗する場合は、RADIUS サーバへのスタティックルートを設定する必要があります。CLI コンソールまたは SSH セッションからサーバに ping を試行して、到達できるかどうか確認します。
- 外部認証が機能していたのに機能しなくなった場合は、すべてのサーバがデッドタイムになっている可能性を考えます。グループ内のすべての RADIUS サーバが失敗したときに、システムが最初のサーバを再試行する前に待機する時間 (分単位) がデッドタイムです。デフォルトは 10 分ですが、1440 分まで設定できます。
- HTTPS 外部認証が一部のユーザでしか機能しない場合は、各ユーザアカウントの RADIUS サーバで定義されている `cisco-av-pair` 属性を評価します。この属性の設定が正しくない可能性があります。属性が欠落しているか不正であると、そのユーザアカウントのすべての HTTPS アクセスがブロックされます。
- SSH 外部認証が一部のユーザでしか機能しない場合は、各ユーザアカウントの RADIUS サーバで定義されている `Service-Type` 属性を評価します。この属性の設定が正しくない可能性があります。属性が欠落しているか不正であると、そのユーザアカウントのすべての SSH アクセスがブロックされます。

Identity Services Engine (ISE)

パッシブ認証に ISE/ISE-PIC を使用するために、Cisco Identity Services Engine (ISE) または ISE Passive Identity Connector (ISE-PIC) 展開を Firepower Threat Defense デバイスと統合することができます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory (AD)、LDAP、RADIUS、またはRSA を使用して認証するユーザに関するユーザ認識データを提供します。ただし、Firepower Threat Defense では、AD との組み合わせでのみユーザアイデンティティ認識にISEを使用できます。さまざまな監視ダッシュボードおよびイベントでユーザ情報を表示できるだけでなく、アクセス制御およびSSL 復号ポリシーでユーザアイデンティティを一致基準として使用できます。

Cisco ISE/ISE-PIC の詳細については、『Cisco Identity Services Engine Administrator Guide』 (<https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html>) および『Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide』 (<https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html>) を参照してください。

ISEに関する注意事項と制限事項

- Firepower システムでは、システムによってデバイス認証がユーザと関連付けられることがないため、Active Directory 認証とともに 802.1x デバイス認証を使用することはできません。802.1x アクティブ ログインを使用する場合は、802.1x アクティブ ログイン (デバイスとユーザの両方) だけを報告するようにISEを設定します。このように設定すれば、デバイス ログインはシステムに 1 回だけ報告されます。
- ISE/ISE-PIC は、ISE ゲストサービスユーザのアクティビティをレポートしません。
- ISE/ISE-PIC サーバとデバイスの時刻を同期させます。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- 多数のユーザ グループをモニタするように ISE/ISE-PIC を設定した場合、システムはメモリ制限のためにグループに基づいてユーザマッピングをドロップすることがあります。その結果、レムムまたはユーザ条件を使用するルールが想定どおりに実行されない可能性があります。
- システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、『Cisco Firepower Compatibility Guide』 (<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html>) を参照してください。
- ご使用のバージョンの ISE が IPv6 をサポートしていることを確認できないかぎり、ISE サーバの IPv4 アドレスを使用してください。

Identity Services Engine の設定

Cisco Identity Services Engine (ISE) または Cisco Identity Services Engine Passive Identity Connector (ISE PIC) をパッシブ アイデンティティ ソースとして使用するには、ISE Platform Exchange Grid (pxGrid) サーバへの接続を設定する必要があります。

始める前に

- ISE から pxGrid サーバおよび MNT サーバの証明書をエクスポートします。たとえば、ISE PIC 2.2 では、**[証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [システム証明書 (System Certificates)]** ページにあります。MNT (モニタリングおよびトラブルシューティング ノード) は、証明書リストの **[使用者 (Used By)]** 列に **[管理者 (Admin)]** として表示されます。これらは、**[オブジェクト (Objects)] > [証明書 (Certificates)]** ページで信頼できる CA 証明書としてアップロードするか、次の手順でアップロードできます。これらのノードは、同じ証明書を使用することがあります。
- AD アイデンティティ レalm を設定する必要もあります。システムは、AD からユーザのリストを取得し、ISE から user-to-IP アドレス マッピングに関する情報を取得します。

手順

ステップ 1 **[オブジェクト (Objects)]** を選択し、目次から **[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。

- オブジェクトを作成するには、**[+] > [Identity Services Engine]** をクリックします。最大で 1 つの ISE オブジェクトを作成できます。
- 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 次のプロパティを設定します。

- **[名前 (Name)]** : オブジェクトの名前。
- **[ステータス (Status)]** : クリックしてオブジェクトを有効または無効にします。無効にすると、アイデンティティルールで ISE をアイデンティティソースとして使用できません。
- **[説明 (Description)]** : (オプション) オブジェクトの説明。
- **[プライマリノードホスト名/IPアドレス (Primary Node Hostname/IP Address)]** : プライマリ pxGrid ISE サーバのホスト名または IP アドレス。ISE バージョンが IPv6 をサポートしていることを確認しない限り、IPv6 アドレスを指定しないでください。
- **[セカンダリノードのホスト名/IPアドレス (Secondary Node Hostname/IP Address)]** : ハイアベイラビリティ向けにセカンダリ ISE サーバを設定している場合、**[セカンダリノードのホスト名/IPアドレスの追加 (Add Secondary Node Hostname/IP Address)]** をクリックし、セカンダリ pxGrid ISE サーバのホスト名または IP アドレスを入力します。
- **[pxGridサーバCA証明書 (pxGrid Server CA Certificate)]** : pxGrid フレームワークの信頼できる認証局の証明書。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

- [MNTサーバCA証明書 (MNT Server CA Certificate)] : 一括ダウンロードを実行する場合に使用する ISE 証明書の信頼できる認証局の証明書。これは、MNT (モニタリングおよびトラブルシューティング) サーバが分かれていない場合、pxGrid サーバ証明書と同じものにできます。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- [サーバ証明書 (Server Certificate)] : ISE への接続時または一括ダウンロードの実行時に Firepower Threat Defense デバイスが ISE に提供する必要がある内部アイデンティティ証明書。
- [ISE ネットワークフィルタ (ISE Network Filters)] : ISE がシステムに報告するデータを制限するように設定できる任意のフィルタ。ネットワーク フィルタを指定すると、ISE はフィルタ内のネットワークからのみデータを報告します。[+] をクリックして、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、[OK] をクリックします。オブジェクトを作成する必要がある場合は、[新しいネットワークの作成 (Create New Network)] をクリックします。IPv4 ネットワーク オブジェクトのみを設定します。

ステップ 4 [テスト (Test)] ボタンをクリックして、システムが ISE サーバに接続できることを確認します。

テストが失敗した場合は、[ログの表示 (See Logs)] リンクをクリックして、詳細なエラーメッセージを確認します。たとえば、次のメッセージはシステムが必要なポートでサーバに接続できなかったことを示しています。問題はホストへのルートが存在しないことである可能性があります。つまり、ISE サーバが予期されたポートを使用していないか、接続を妨げるアクセス制御ルールが存在します。

```
Captured Jabberwerx log:2018-05-11T16:10:30 [ ERROR]: connection timed out while trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

ステップ 5 [OK] をクリックしてオブジェクトを保存します。

次のタスク

ISE を設定したら、アイデンティティポリシーを有効にして、パッシブ認証ルールを設定し、その設定を展開します。その後、ISE/ISE PIC に移動して、デバイスをサブスクライバとして許可する必要があります。サブスクライバを自動的に許可するよう ISE/ISE PIC を設定している場合、サブスクリプションを手動で許可する必要はありません。

ISE/ISE-PIC アイデンティティソースのトラブルシューティング

ISE/ISE-PIC 接続

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE を Firepower Threat Defense デバイスに正常に統合するには、ISE の pxGrid アイデンティティ マッピング機能を有効にする必要があります。

- ISE サーバと Firepower Threat Defense デバイスの間の接続を成功させるには、ISE のクライアントを手動で承認する必要があります。
または、『Cisco Identity Services Engine Administrator Guide』の「Automatically approve new accounts」の章にある説明に従って、ISE で [新しいアカウントの自動承認 (Automatically approve new accounts)] を有効にできます。
- Firepower Threat Defense デバイス (サーバ) 証明書には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、他の拡張キー使用値を含むことはできません。clientAuth 拡張キーの使用が設定されている場合は、キーの使用も設定されていないか、デジタル署名キー使用値が設定されている必要があります。Firepower Device Manager を使用して作成できる自己署名アイデンティティ証明書は、これらの要件を満たしていません。
- ISE サーバの時間は、Firepower Threat Defense デバイスの時間と同期する必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

ISE/ISE-PIC ユーザデータ

ISE または ISE-PIC によって報告されるユーザデータに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ISE ユーザによるアクティビティは、アクセス制御ルールで処理されず、システムがユーザダウンロードでそのユーザに関する情報を正常に取得するまでダッシュボードに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- システムは、ISE ゲストサービスユーザのユーザデータを受信しません。

ローカル ユーザ

ローカルユーザデータベース (LocalIdentitySource) には Firepower Device Manager で定義したユーザが含まれます。

ローカル定義ユーザは、次の目的で使用できます。

- リモートアクセス VPN (プライマリまたはフォールバック アイデンティティ ソースとして)。
- 管理アクセス (Firepower Device Manager ユーザのプライマリまたはセカンダリソースとして)。

管理者ユーザはシステム定義のローカルユーザです。ただし、管理者ユーザはリモートアクセス VPN にログインできません。追加のローカル管理者ユーザは作成できません。

管理アクセスの外部認証を定義すると、デバイスにログインしている外部ユーザがローカルユーザのリストに表示されます。

- アイデンティティポリシー（間接的）（リモートアクセス VPN ログインからユーザアイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

ここでは、ローカルユーザの設定方法について説明します。

ローカル ユーザの設定

リモートアクセス VPN で使用するユーザ アカウントをデバイスで直接作成できます。外部認証ソースの代わりに、またはそれに加えて、ローカルユーザ アカウントを使用できます。

リモートアクセス VPN のフォールバック認証方式としてローカルユーザデータベースを使用する場合、必ず外部データベースの名前と同じユーザ名/パスワードをローカル データベースで設定します。そうしなければ、フォールバック メカニズムは効果を発揮しません。

ここで定義されたユーザは、デバイス CLI にログインできません。

手順

ステップ 1 [オブジェクト (Objects)] > [ユーザ (Users)] を選択します。

リストに、次のようなユーザ名とサービス タイプが表示されます。

- **MGMT** : Firepower Device Manager にログインできる管理ユーザ向け。管理者ユーザが常に定義されており、削除することはできません。また、追加の MGMT ユーザを設定することもできません。ただし、管理アクセス用の外部認証を定義すると、デバイスにログインする外部ユーザが MGMT ユーザとしてローカル ユーザ リストに表示されます。
- **RA VPN** : デバイスに設定されたリモート アクセス VPN にログインできるユーザ向け。プライマリ ソースまたはセカンダリ（フォールバック）ソースのローカル データベースも選択する必要があります。

ステップ 2 次のいずれかを実行します。

- ユーザを追加するには、[+] をクリックします。
- ユーザを編集するには、そのユーザの [編集 (edit)] アイコン (🔍) をクリックします。

特定のユーザアカウントが必要なくなったら、そのユーザの [削除 (delete)] アイコン (🗑️) をクリックします。

ステップ 3 ユーザ プロパティを設定します。

名前とパスワードには、印刷可能 ASCII 英数字または特殊文字（スペースと疑問符を除く）を使用できます。印刷可能文字は ASCII コード 33 ~ 126 です。

- [名前 (Name)] : リモート アクセス VPN にログインするためのユーザ名。名前には 4 ～ 64 文字を使用できますが、スペースは使用できません (例 : johndoe) 。
- [パスワード (Password)]、[パスワードの確認 (Confirm Password)] : アカウントのパスワードを入力します。パスワードの長さは、8 ～ 16 文字にする必要があります。同じ文字を連続して使用することはできません。数字、大文字、小文字、および特殊文字をそれぞれ 1 文字以上使用する必要もあります。

(注) ユーザは、自分のパスワードを変更できません。ユーザにパスワードを通知します。パスワードを変更する必要がある場合は、ユーザアカウントを編集する必要があります。また、外部 MGMT ユーザのパスワードは更新しないでください。パスワードは外部 AAA サーバによって制御されています。

ステップ 4 [OK] をクリックします。



第 III 部

基本

- [Firepower 4100/9300 上の論理デバイス \(201 ページ\)](#)
- [ハイアベイラビリティ \(フェールオーバー\) \(215 ページ\)](#)
- [インターフェイス \(267 ページ\)](#)
- [ルーティング \(335 ページ\)](#)



第 9 章

Firepower 4100/9300 上の論理デバイス

Firepower 4100/9300 は柔軟なセキュリティプラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。

シャーシインターフェイスを設定し、論理デバイスを追加し、Firepower Chassis Manager または FXOS の CLI を使用して Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。これらのタスクを FDM で実行することはできません。

この章では、基本的なインターフェイスの設定、および Firepower Chassis Manager を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。FXOS CLI を使用する場合は、『FXOS CLI 構成ガイド』を参照してください。高度な FXOS の手順とトラブルシューティングについては、『FXOS 構成ガイド』を参照してください。

- [Firepower インターフェイスについて \(201 ページ\)](#)
- [Firepower 9300 ハードウェアとソフトウェアの組み合わせの要件と前提条件 \(203 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(203 ページ\)](#)
- [インターフェイスの設定 \(204 ページ\)](#)
- [論理デバイスの設定 \(206 ページ\)](#)
- [Firepower 4100/9300 論理デバイスの履歴 \(213 ページ\)](#)

Firepower インターフェイスについて

Firepower 4100/9300 シャーシは、物理インターフェイスおよび EtherChannel (ポートチャネル) インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメソッドインターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で、FXOS シャーシの管理に使用されます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLIから設定にする必要があります。このインターフェイスについての情報をFXOS CLIで表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER connect local-mgmt

```
firepower(local-mgmt) # show mgmt-port
```

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

インターフェイスタイプ

各インターフェイスは、次のいずれかのタイプになります。

- **Data** : 通常のデータに使用します。データインターフェイスは論理デバイス間で共有できません。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- **Mgmt** : アプリケーションインスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。
- **Cluster** : クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは48番のポートチャンネル上に自動的に作成されます。このタイプは、EtherChannel インターフェイスのみでサポートされます。FDMはクラスタリングをサポートしていません。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシとアプリケーションの間に不一致が生じることがあります。

Firepower9300ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 9300 には、3つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- **セキュリティモジュール タイプ** : Firepower 9300 に異なるタイプのモジュールをインストールできます。たとえば、SM-36 をモジュール 1、SM-40 をモジュール 2、SM-44 をモジュール 3 としてインストールできます。
- **ネイティブインスタンスとコンテナインスタンス** : セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを1つのみインストールできます。一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。たとえば、モジュール 1 とモジュール 2 にネイティブインスタンスをインストールできますが、モジュール 3 にはコンテナインスタンスをインストールできません。
- **高可用性** : 高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- **ASA および FTD のアプリケーションタイプ** : 異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモジュール 2 に ASA をインストールし、モジュール 3 に FTD をインストールすることができます。
- **ASA または FTD のバージョン** : 個別のモジュールで異なるバージョンのアプリケーションインスタンスタイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

Firepower インターフェイスに関する注意事項と制約事項

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャンネルインターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

一般的なガイドラインと制限事項

ハイアベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- ハイアベイラビリティ フェールオーバーを設定される2つのユニットは、次の条件を満たしている必要があります。
 - 同じモデルであること。
 - ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
 - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 詳細については、[ハイアベイラビリティのシステム要件 \(225ページ\)](#) を参照してください。





インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、EtherChannel、インターフェイス プロパティを編集して。

インターフェイスの有効化または無効化

各インターフェイスの [Admin State (管理状態)] を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスはディセーブルになっています。

手順

-
- ステップ 1** [インターフェイス (Interfaces)] を選択して、[インターフェイス (Interfaces)] ページを開きます。
- [インターフェイス (Interface)] ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。
- ステップ 2** インターフェイスを有効にするには、[disabled スライダー ()] をクリックして、[enabled スライダー ()] に変更します。
- [はい (Yes)] をクリックして、変更を確定します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変化します。
- ステップ 3** インターフェイスを有効にするには、[disabled スライダー ()] をクリックして、[enabled スライダー ()] に変更します。
- [はい (Yes)] をクリックして、変更を確定します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。
-

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

EtherChannel (ポート チャネル) の追加

EtherChannel (別名ポートチャネル) には、同じタイプのメンバーインターフェイスを最大 16 個含めることができます。リンク集約制御プロトコル (LACP) では、2 つのネットワーク デバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データインターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。



(注) モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

各メンバーインターフェイスが LACP 更新を送受信するように、Firepower 4100/9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャンネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャンネルグループ内のスタンバイインターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止 (Suspended)] 状態 (Active LACP モードの場合) または [ダウン (Down)] 状態 (On LACP モードの場合) になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止 (Suspended)] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータインターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止 (Suspended)] または [ダウン (Down)] 状態に戻ります。

論理デバイスの設定

スタンドアロン論理デバイスまたはハイアベイラビリティのペアを Firepower 4100/9300 シャーシに追加します。

FDM 用スタンドアロン Firepower Threat Defense の追加

FDM はネイティブインスタンスで使用できます。コンテナインスタンスはサポートされていません。スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシにします。
- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません。
- また、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。
- 次の情報を用意します。
 - このデバイスのインターフェイス ID
 - 管理インターフェイス IP アドレスとネットワーク マスク
 - ゲートウェイ IP アドレス
 - DNS サーバの IP アドレス。
 - FTD ホスト名とドメイン名

手順

セキュリティポリシーの設定を始めるには、FDM のコンフィギュレーション ガイドを参照してください。

ハイ アベイラビリティ ペアの追加

FTD ハイ アベイラビリティ (フェールオーバーとも呼ばれます) は、FXOS ではなくアプリケーション内で設定されます。ただし、高可用性用にシャーシを準備する場合は、次のステップを参照してください。

始める前に

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
 - 同じモデルであること。

- ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
- インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- 他の高可用性システム要件については、[ハイアベイラビリティのシステム要件 \(225 ページ\)](#) を参照してください。

手順

-
- ステップ 1** 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイアベイラビリティは推奨されず、サポートされない可能性があります。
- ステップ 2** 各論理デバイスに同一のインターフェイスを割り当てます。
- ステップ 3** フェールオーバーリンクとステートリンクに1つまたは2つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間でハイアベイラビリティトラフィックを交換します。統合されたフェールオーバーリンクとステートリンクには、10GBのデータインターフェイスを使用することを推奨します。別のフェールオーバーおよび状態のリンクを使用できます使用可能なインターフェイスがあれば、状態のリンクには、ほとんどの帯域幅が必要です。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。同じネットワークセグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

- ステップ 4** 論理デバイスでハイアベイラビリティを有効にします。[ハイアベイラビリティ \(フェールオーバー\) \(215 ページ\)](#) を参照してください。
- ステップ 5** ハイアベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。
-

Firepower Threat Defense 論理デバイスのインターフェイスの変更

FTD 論理デバイスでは、インターフェイスの割り当てや割り当て解除、を行うことができます。その後、FDM でインターフェイス設定を同期できます。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、FTD の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバなど、FTD の設定における多くの

場所で直接参照されている可能性があります。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ FDM での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

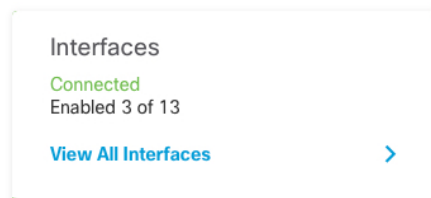
始める前に


- [物理インターフェイスの設定 \(205 ページ\)](#) および [EtherChannel \(ポートチャネル\) の追加 \(205 ページ\)](#) に従ってインターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには (たとえば、デフォルトですべてのインターフェイスがクラスタに割り当てられます)、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でデバイスに EtherChannel を割り当てることができます。
- 高可用性のため、FDM で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にスタンバイユニットでインターフェイスを変更してから、アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼさないことに注意してください。

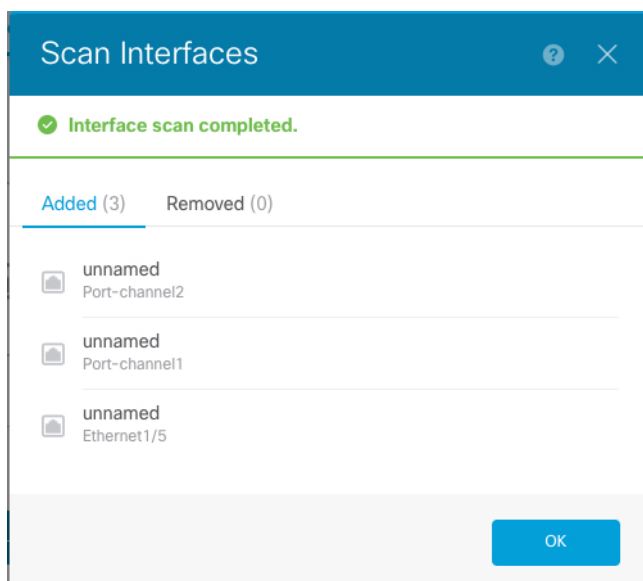
手順

ステップ 1 FDM でインターフェイスを同期して移行します。

- a) FDM にログインします。
- b) [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにある [すべてのインターフェイスを表示 (View All Interfaces)] リンクをクリックします。



- c) [インターフェイス (Interfaces)] アイコン () をクリックします。
- d) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

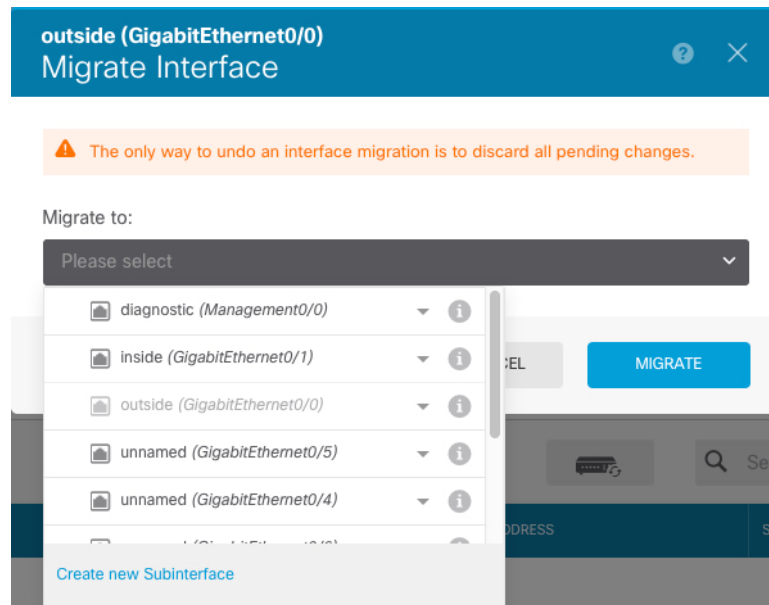


- e) 名前、IP アドレスなどを使用して新しいインターフェイスを設定します。
 削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでそれらの設定を使用できるように、ダミーの名前と IP アドレスを使用して古いインターフェイスを再設定する必要があります。
- f) 古いインターフェイスを新しいインターフェイスに置き換えるには、古いインターフェイスの [置換 (Replace)] アイコンをクリックします。

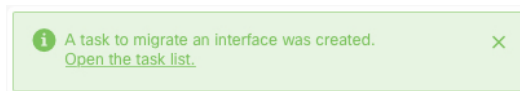


このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに置き換えられます。

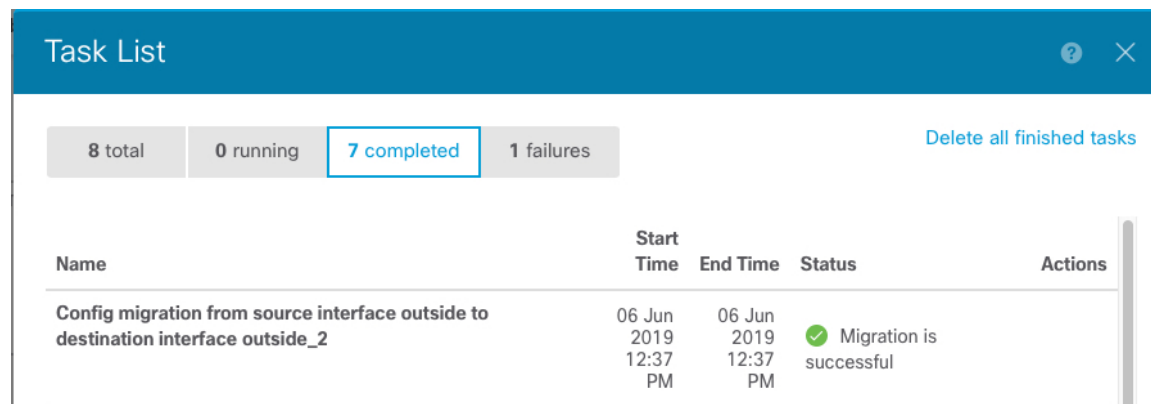
- g) [交換用インターフェイス (Replacement Interface)]: ドロップダウン リストから新しいインターフェイスを選択します。



- h) [インターフェイス (Interfaces)] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。

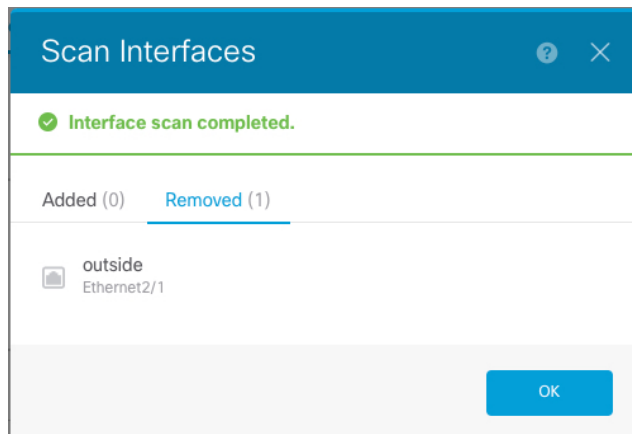


- i) [タスクリスト (Task List)] を調べて、移行が成功したことを確認します。



ステップ 2 FDM でインターフェイスを再度同期します。

図 4: FDM によるインターフェイスのスキャン



アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module slot_number {console | telnet}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect ftd name

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

ステップ3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- FTD：「**exit**」と入力します。

ステップ4 FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

a) ~と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-],.**と入力

Firepower 4100/9300 論理デバイスの履歴

機能	バージョン	詳細
Firepower 4100/9300 での FDM のサポート	6.5.0	Firepower 4100/9300 の FTD 論理デバイスで FDM を使用できるようになりました。FDM はマルチインスタンス機能をサポートしていません。ネイティブインスタンスのみがサポートされています。 (注) FXOS 2.7.1 が必要です。



第 10 章

ハイ アベイラビリティ（フェールオーバー）

ここでは、アクティブ/スタンバイ フェールオーバーを設定および管理して、Firepower Threat Defense システムのハイ アベイラビリティを実現する方法について説明します。

- [ハイ アベイラビリティ（フェールオーバー）について（215 ページ）](#)
- [ハイ アベイラビリティのシステム要件（225 ページ）](#)
- [ハイ アベイラビリティのガイドライン（227 ページ）](#)
- [ハイ アベイラビリティの設定（229 ページ）](#)
- [ハイ アベイラビリティの管理（244 ページ）](#)
- [ハイ アベイラビリティのモニタ（255 ページ）](#)
- [ハイ アベイラビリティ（フェールオーバー）のトラブルシューティング（259 ページ）](#)

ハイ アベイラビリティ（フェールオーバー）について

ハイ アベイラビリティまたはフェールオーバーセットアップは、プライマリ デバイスの障害時にセカンダリ デバイスで引き継ぐことができるように、2つのデバイスを結合します。これにより、デバイスの障害時にネットワーク運用を維持できます。

ハイアベイラビリティを設定するには、同じ Firepower Threat Defense デバイスが2台、専用のフェールオーバーリンク（オプションで、ステートリンク）で相互に接続されている必要があります。2台の装置はフェールオーバーリンクを介して常に通信し、各装置の動作状態を判断して、展開された設定の変更を同期します。システムでは、フェールオーバーが発生したときにユーザ接続が維持されるように、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。

この装置はアクティブ/スタンバイペアを形成します。1台の装置がアクティブ装置となり、トラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニタされま

す。これらの条件が満たされると、アクティブ装置がスタンバイ装置にフェールオーバーし、スタンバイ装置がアクティブになります。

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firepower Threat Defense デバイスに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリ ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニットが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ ユニットが常にアクティブ ユニットになります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ ユニットの MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ ユニットが行うアクション、スタンバイ ユニットが行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 5: フェールオーバー イベント

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
アクティブユニットが故障（電源またはハードウェア）	フェールオーバー	適用対象外	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバーリンクでhelloメッセージは受信されません。
以前にアクティブであったユニットの復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。
スタンバイユニットが故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	適用対象外	スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバーリンクがダウンしている間、ユニットはスタンバイユニットにフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
スタートアップ時にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバーリンクがダウンしていると、両方のユニットがアクティブになります。
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
アクティブユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクは2つの装置の間の専用接続です。ステートフル フェールオーバー リンクも専用接続ですが、1つのフェールオーバーリンクをフェールオーバーリンクとステートリンクが組み合わされたものとして使用することも、個別の専用ステートリンクを作成することもできます。フェールオーバーリンクだけを使用する場合は、ステートフルな情報もそのリンクを経由し、ステートフル フェールオーバー機能は失われません。

デフォルトでは、フェールオーバー リンクおよびステートフル フェールオーバー リンク上の通信はプレーンテキスト（暗号化されない）です。IPsec 暗号キーを設定することにより、通信を暗号化してセキュリティを強化できます。

ここでは、これらのインターフェイスについて詳しく説明するとともに、最良の結果を得るためのデバイスの配線方法に関する推奨事項を示します。

フェールオーバー リンク

フェールオーバーペアの2台の装置は、フェールオーバーリンク経由で常に通信して、各装置の動作ステータスを確認し、設定の変更を同期します。

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- Hello メッセージ（キープアライブ）
- ネットワーク リンク ステータス
- MAC アドレス交換
- 設定の複製と同期化

- システムデータベースの更新。これには、VDB やルールは含まれますが、地理位置情報データベースやセキュリティ インテリジェンス データベースは含まれません。各システムは、地理位置情報の更新やセキュリティ インテリジェンス の更新を個別にダウンロードします。更新スケジュールを作成する場合は、これらの同期が維持されます。ただし、アクティブデバイスで地理位置情報やセキュリティ インテリジェンス を手動更新する場合は、スタンバイデバイスでも更新する必要があります。



- (注) イベント、レポート、および監査ログデータは同期されません。イベントビューアとダッシュボードには、特定の装置に関連するデータのみが表示されます。また、展開履歴、タスク履歴、およびその他の監査ログイベントも同期されません。

ステートフル フェールオーバー リンク

システムは、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。

フェールオーバーリンクとステートフル フェールオーバー リンクの両方に単一のリンクを使用することは、インターフェイスを節約する最善の方法です。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステートリンクとフェールオーバーリンク専用のインターフェイスを検討する必要があります。

ステートフル フェールオーバー リンクの帯域幅は、デバイス上のデータインターフェイスの最大帯域幅と一致させることをお勧めします。

フェールオーバー リンクとステート リンクのインターフェイス

使用されていないが有効になっているデータインターフェイス（物理、または EtherChannel）は、いずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバーリンク インターフェイスは、通常のネットワークインターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバーリンク用にのみ使用できます（ステートリンク用としても使用できます）。管理インターフェイス、サブインターフェイス、VLAN インターフェイス、またはスイッチ ポートをフェールオーバーに使用することはできません。

FTD は、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。

フェールオーバーまたはステートリンクとして EtherChannel インターフェイスを使用している場合、高可用性を確立する前に、両方のデバイスで同じ ID とメンバー インターフェイスを備えた同じ EtherChannel が存在していることを確認する必要があります。EtherChannel の不一致がある場合は、先にセカンダリ装置で HA を無効にし、設定を修正する必要があります。順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバーおよびステートフル フェールオーバー インターフェイスの接続

未使用のデータ物理インターフェイスは、フェールオーバーリンクやオプションの専用ステートリンクとして使用できます。ただし、現在名前が設定されているインターフェイスやサブインターフェイスを持つインターフェイスは選択できません。フェールオーバーおよびステートフルフェールオーバー リンク インターフェイスは、通常のネットワークキングインターフェイスとして設定されません。フェールオーバー通信用にのみ存在し、通過トラフィックや管理アクセスに使用することはできません。

設定がデバイス間で同期されるため、リンクの両端に同じポート番号を選択する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで GigabitEthernet 1/3 を使用します。

次のいずれかの方法で、フェールオーバーリンクおよび専用ステートリンク（使用する場合）を接続します。

- **Firepower Threat Defense** デバイスのフェールオーバー インターフェイスと同じネットワークセグメント（ブロードキャストドメインまたはVLAN）に他の装置のないスイッチを使用する。専用ステートリンクの要件は同じですが、フェールオーバーリンクとは異なるネットワークセグメントに存在する必要があります。



(注) スイッチを使用する利点は、装置のいずれかのインターフェイスがダウンした場合、障害が発生したインターフェイスのトラブルシューティングが容易であることです。直接ケーブル接続を使用する場合、1つのインターフェイスに障害が発生すると、リンクが両方のピアでダウンし、どのデバイスで障害が発生しているのかを判別することが困難になります。

- イーサネットケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。Firepower Threat Defense デバイスは銅線イーサネットポートで Auto-MDI/MDIX をサポートしているので、クロスケーブルまたはストレートケーブルのどちらでも使用できます。ストレートケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの1つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステートリンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバーメッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバー リンクとデータ リンクの中断の回避

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバーリンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバーリンクがダウンした場合、フェールオーバーが必要かどうかの決定に、Firepower Threat Defense デバイスはデータインターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクの正常性が復元されるまで停止されます。

耐障害性フェールオーバーネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

2つの Firepower Threat Defense デバイス間のフェールオーバーとデータ インターフェイスの両方を接続するために1つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の Firepower Threat Defense デバイスがアクティブになります。したがって、次の図で示されている2つの接続方式は推奨しません。

図 5: 単一のスイッチを使用した接続：非推奨

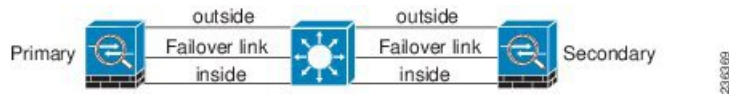
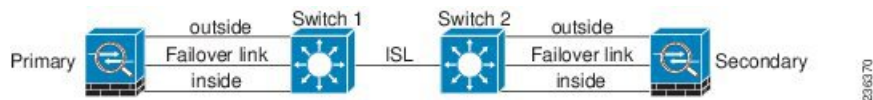


図 6: 2つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバーリンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバーリンクを接続します。

図 7: 異なるスイッチを使用した接続

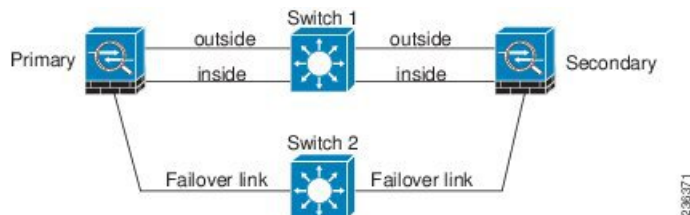
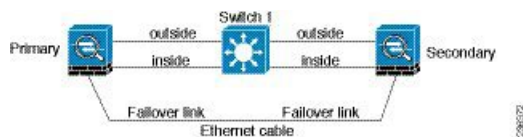


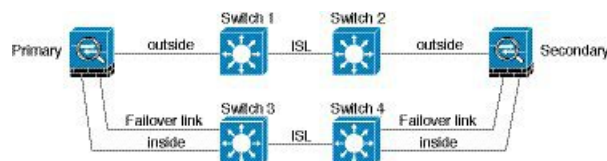
図 8: ケーブルを使用した接続



シナリオ 3：推奨

Firepower Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバーリンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 9: セキュア スイッチを使用した接続



ステートフル フェールオーバーがユーザ接続に与える影響

アクティブ装置は、接続状態情報をスタンバイ装置と共有します。これは、スタンバイ装置がユーザに影響を与えずに特定のタイプの接続を維持できることを意味します。

ただし、ステートフルフェールオーバーをサポートしないタイプの接続もあります。これらの接続については、フェールオーバーが発生した場合、ユーザが接続を再確立する必要があります。多くの場合、これは、接続で使用されているプロトコルの動作に基づいて自動的に実行されます。

ここでは、ステートフルフェールオーバーに関してサポートされる機能またはサポートされない機能について説明します。

サポートされる機能

ステートフルフェールオーバーでは、次のステート情報がスタンバイ Firepower Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および HTTP 接続状態を含む状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- 厳密な TCP 強制を含む、Snort の接続状態、インスペクション結果、およびピンホール情報。
- ARP テーブル
- レイヤ 2 ブリッジテーブル (ブリッジグループ用)
- ISAKMP および IPsec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリングセッションとピンホール。
- スタティックおよびダイナミックルーティングテーブル：ステートフルフェールオーバーはダイナミックルーティングプロトコル (OSPF や EIGRP など) に参加するため、アクティブ装置上のダイナミックルーティングプロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース (RIB) テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリユニットには最初にプライマリユニットをミラーリングするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。

フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIBテーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIBには新しくアクティブになった装置での最新のルーティングプロトコル転送情報が含まれています。



(注) ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミックルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性はありません。
- アクセス コントロール ポリシーの判断：フェールオーバー時には、トラフィックの照合（URL、URL カテゴリ、地理位置情報など）、侵入検知、マルウェア、ファイルタイプに関する判断が保持されます。ただし、フェールオーバーの時点で評価される接続には、次のような注意事項があります。
 - AVC：App-ID 判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に、App-ID 判定が完了および同期されていれば、正常に同期は行われます。
 - 侵入検知状態：フェールオーバーの際、フロー中にピックアップが発生すると、新しいインスペクションは完了しますが、古い状態は失われます。
 - ファイル マルウェア ブロッキング：ファイルの処分は、フェールオーバー前にできるようになる必要があります。
 - ファイルタイプ検出とブロッキング：ファイルタイプは、フェールオーバー前に特定される必要があります。元のアクティブ デバイスでファイルを特定している間にフェールオーバーが発生すると、ファイルタイプの同期は失われます。ファイルポリシーでそのファイルタイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。
- アイデンティティ ポリシーからのパッシブなユーザ識別の判断（キャプティブ ポータルを介したアクティブ認証を通じて収集されたもの以外）。
- セキュリティ インテリジェンス判断。
- RA VPN：リモートアクセス VPN エンドユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリ

ケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフルフェールオーバーでは、次のステート情報はスタンバイ Firepower Threat Defense デバイスに渡されません。

- GREやIP-in-IPなどのプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されず、新しいアクティブノードは、既存のインスペクションの判定を再利用して、正しいポリシールールを照合することができません。
- SSL復号ポリシーにより復号された接続：復号状態は同期されず、現在の復号された接続はリセットされ、ブロックされます。新しい接続が適切に機能します。（復号しないルールと一致する）復号されない接続は影響を受けず、他のTCP接続と同様に正しく複製されます。
- マルチキャストルーティング。

スタンバイ装置で許可される設定の変更とアクション

ハイアベイラビリティモードで運用している場合は、アクティブ装置にのみ設定の変更を加えます。設定を展開すると、新しい変更はスタンバイ装置にも送信されます。

ただし、一部のプロパティはスタンバイ装置固有です。スタンバイ装置では次の設定を変更できます。

- 管理IPアドレスとゲートウェイ。
- (CLIのみ) 管理ユーザアカウントのパスワード。この変更を行うことができるのはCLIのみで、FDMで行うことはできません。

さらに、スタンバイデバイスでは次のアクションを実行できます。

- HAの一時停止、再開、リセット、解除などのハイアベイラビリティアクションと、アクティブモードとスタンバイモードの切り替え。
- ダッシュボードとイベントデータはデバイスごとに一意であり、同期されません。これには、イベントビューアのカスタムビューが含まれます。
- 監査ログ情報はデバイスごとに一意です。
- スマートライセンスの登録。ただし、アクティブ装置でオプションのライセンスを有効または無効にする必要があります。このアクションはスタンバイ装置と同期され、適切なライセンスが要求または解放されます。
- バックアップ（ただし復元ではない）。バックアップを復元するには装置でHAを解除する必要があります。バックアップにHA設定が含まれている場合、装置はHAグループに再び参加します。

- ソフトウェアアップグレードのインストール。
- トラブルシューティングログの生成。
- 地理位置情報データベースまたはセキュリティインテリジェンスデータベースの手動更新。これらのデータベースは、装置間で同期されません。更新スケジュールを作成する場合、装置は独立して一貫性を維持できます。
- [モニタリング (Monitoring)] > [セッション (Sessions)] ページからアクティブな Firepower Device Manager のユーザセッションを表示したり、セッションを削除できます。

ハイアベイラビリティのシステム要件

ここでは、ハイアベイラビリティ設定に2台のデバイスを実装する前に満たさなくてはならない要件について説明します。

HA のハードウェア要件

高可用性設定で2つのデバイスを結び付けるには、次のハードウェア要件を満たす必要があります。

- デバイスはまったく同じハードウェアモデルである必要があります。

Firepower 9300 の場合、ハイアベイラビリティは同じタイプのモジュール間でのみサポートされていますが、2台のシャーシにモジュールを混在させることができます。たとえば、各シャーシには SM-36 および SM-44 があります。SM-36 モジュール間および SM-44 モジュール間でハイアベイラビリティペアを作成できます。
- デバイスは同じ数の同じタイプのインターフェイスを備えている必要があります。

Firepower 4100/9300 シャーシの場合は、HA を有効にする前に、FXOS ですべてのインターフェイスをまったく同じになるように事前に設定する必要があります。HA を有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でインターフェイスを変更し、アクティブユニットで同じ変更を行います。
- デバイスには同じモジュールが取り付けられている必要があります。たとえば、一方に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がある場合は、もう一方のデバイスに同じモジュールを取り付ける必要があります。

HA のソフトウェア要件

高可用性設定で2つのデバイスを結び付けるには、次のソフトウェア要件を満たす必要があります。

- デバイスは、まったく同じバージョンのソフトウェア（つまり、1番目のメジャー番号、2番目のマイナー番号、および3番目のメンテナンス番号が同じ）を実行する必要があります。バージョンは、Firepower Device Manager の [Devices] ページで確認できます。また、

CLI で **show version** コマンドを使用して確認することもできます。異なるバージョンを実行するデバイスでも参加できますが、設定がスタンバイ装置にインポートされず、装置を同じソフトウェアバージョンにアップグレードしないとフェールオーバーは機能しません。

- 両方のデバイスがローカル マネージャ モードになっている（つまり、Firepower Device Manager を使用して設定されている）必要があります。両方のシステムで Firepower Device Manager にログインできる場合は、それらがローカル マネージャ モードになっています。CLI で **show managers** コマンドを使用して確認することもできます。
- 各デバイスの初期セットアップ ウィザードを完了する必要があります。
- 各デバイスに固有の管理 IP アドレスが必要です。管理インターフェイスの設定は、デバイス間で同期されません。
- デバイスの NTP 設定が同じである必要があります。
- DHCP を使用してアドレスを取得するようにインターフェイスを設定することはできません。つまり、すべてのインターフェイスに静的 IP アドレスが必要です。
- Cisco Defense Orchestrator への登録ステータスが両方のデバイスで同じである必要があります（両方登録済みまたは両方未登録）。
- 次のクラウドサービスでは、プライマリデバイスとセカンダリデバイスの両方を有効にするか、セカンダリが有効になっている間はプライマリを無効にすることができます（セカンダリは HA 結合後に無効になります）。
 - Cisco Success Network
 - Cisco Threat Response
- ハイ アベイラビリティを設定する前に、保留中の変更を展開する必要があります。

HA のライセンス要件

高可用性を設定する前に、装置が同じ状態（両方とも基本ライセンスに登録されているか両方とも評価モードになっている）である必要があります。デバイスが登録されている場合は、それらを異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態（両方有効または両方無効）である必要があります。ただし、装置ごとに異なるオプションライセンスを有効にすることは可能です。両方のユニットに登録する場合は、デバイスに対して同じシスコクラウドサービスのリージョンを選択する必要があります。

運用時には、ハイ アベイラビリティ ペアの装置に同じライセンスが必要です。アクティブ装置で行ったライセンスの変更は、展開時にスタンバイ装置で繰り返されます。

ハイアベイラビリティ構成には、2つのスマートライセンス資格（ペアを構成するデバイスごとに1つ）が必要です。各デバイスに適用するためにアカウントに十分なライセンスがあることを確認する必要があります。ライセンスが不足している場合は、一方のデバイスが準拠状態でも、もう一方のデバイスが非準拠になる可能性があります。

たとえば、アクティブデバイスに基本ライセンスと脅威ライセンスが割り当てられており、スタンバイデバイスに基本ライセンスのみが割り当てられている場合、スタンバイ装置は Cisco Smart Software Manager と通信してアカウントから利用可能な脅威ライセンスを取得します。スマートライセンスアカウントに購入済みの十分な権限付与が含まれていない場合は、正しい数のライセンスが購入されるまで、アカウントがコンプライアンス適用外（そのため、アクティブデバイスにコンプライアンスが適用されていてもスタンバイデバイスはコンプライアンス適用外）になります。



- (注) 輸出規制対象の機能の設定が異なるアカウントに各デバイスを登録した場合、または1つの装置が登録済みで、もう1つが評価モードになっている HA ペアを作成しようすると、HA の結合に失敗する可能性があります。輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワークセグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置で HA を手動で中断する必要があります。

ハイアベイラビリティのガイドライン

モデルのサポート

- Firepower 9300 : Firepower 9300 で HA を設定することができます。ただし、同じ Firepower 9300 シャーシで別の論理デバイス間の HA を設定することはできません。
- Firepower 1010 :
 - 高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の高可用性のネットワーク設定では、両方のユニットのアクティブなスイッチポートがネットワークループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1つのスイッチポートを VLAN に配置して、高可用性を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
 - ファイアウォールインターフェイスはフェールオーバーリンクとしてのみ使用できます。
- Firepower Threat Defense Virtual : HA 設定は、Microsoft Azure クラウドの Firepower Threat Defense Virtual ではサポートされていません。

その他のガイドライン

- 169.254.0.0/16 と fd00:0:0:::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- アクティブ装置からの設定は、アクティブ装置で展開ジョブを実行したときに、スタンバイ装置に同期されます。ただし、一部の変更は、変更を展開するまでスタンバイ装置で同期されていない場合もあります。次のいずれかを変更した場合、変更は隠され、これらがスタンバイ装置で設定される前に展開ジョブを実行する必要があります。変更をすぐに適用する必要がある場合は、保留中の変更に表示されるその他の変更を行う必要があります。非表示となる変更には、ルール、ジオデータベース、セキュリティインテリジェンスまたは VDB 更新のスケジュール、バックアップのスケジュール、NTP、管理インターフェイスの DNS、ライセンス権限付与、クラウドサービス オプション、URL フィルタリング オプションの編集が含まれます。
- プライマリ装置とセカンダリ装置の両方でバックアップを実行する必要があります。バックアップを復元するには、まず HA を解除する必要があります。両方のユニットで同じバックアップを復元しないでください（両方のユニットがアクティブになってしまうため）。代わりに、まず、アクティブにする装置でバックアップを復元し、その後、別のユニットで同等のバックアップを復元してください。
- さまざまなアイデンティティソースの [テスト (Test)] ボタンは、アクティブ装置でのみ機能します。スタンバイデバイスのアイデンティティソース接続をテストする必要がある場合は、まず、モードを切り替えてスタンバイピアをアクティブピアにする必要があります。
- ハイアベイラビリティ設定を作成または解除すると、設定の変更が展開されたときに両方のデバイスで Snort 検査プロセスが再開されます。これにより、プロセスが完全に再開されるまでに通過トラフィックの中断が発生する可能性があります。
- ハイアベイラビリティの初期設定時に、セカンダリ上のセキュリティインテリジェンスおよび地理位置情報データベースのバージョンがプライマリ上のバージョンと異なる場合、データベースを更新するジョブはセカンダリ装置でスケジュールされます。これらのジョブは、次の展開時にアクティブ装置から実行されます。HA 結合に失敗した場合でも、これらのジョブはそのまま残り、次の展開時に実行されます。
- ユーザが外部アイデンティティソースに対して認証される場合（つまり、ローカル管理者ユーザではない場合）、そのユーザはスタンバイ装置にログインできなくなる可能性があります。アクティブ装置に少なくとも一度ログインし、設定を展開すると、スタンバイ装置にログインできます。この制限は、ローカル管理者ユーザには適用されません。
- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル (STP) を実行している接続済みスイッチポートが、トポロジの変化を検出すると 30～50 秒間ブロッキング状態になる可能性があります。ポートがブロッキングステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

```
interface interface_id spanning-tree portfast
```

この回避策は、ルーテッドモードおよびブリッジグループインターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディングモードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキングモードに遷移します。

- ハイアベイラビリティペアに接続されているスイッチでポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信上の問題が発生する可能性があります。この問題は、あるセキュアポートで設定または学習されたセキュア MAC アドレスが別のセキュアポートに移動するときに、スイッチのポートセキュリティ機能によって違反フラグが付けられるために発生します。
- アクティブ/スタンバイハイアベイラビリティと VPN IPsec トンネルの場合、VPN トンネル経由で SNMP を使用してアクティブ装置とスタンバイ装置の両方をモニタすることはできません。スタンバイ装置にはアクティブ VPN トンネルがなく、ネットワーク管理システム (NMS) 宛てのトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

ハイアベイラビリティの設定

ハイアベイラビリティのセットアップを使用して、デバイスで障害が発生している場合でもネットワーク接続を確保します。アクティブ/スタンバイハイアベイラビリティを使用して、2台のデバイスがリンクされます。そのため、アクティブデバイスが故障した場合、スタンバイデバイスが引き継ぎ、ユーザは接続の問題をほとんど感じません。

次の手順で、アクティブ/スタンバイハイアベイラビリティ (HA) ペアをセットアップするエンドツーエンドプロセスについて説明します。

手順

- ステップ 1 2台の装置でのハイアベイラビリティの準備 (230 ページ)。
- ステップ 2 ハイアベイラビリティ用のプライマリ装置の設定 (232 ページ)。
- ステップ 3 ハイアベイラビリティ用のセカンダリ装置の設定 (235 ページ)。
- ステップ 4 ヘルスモニタリングのフェールオーバー基準の設定 (236 ページ)。

基準には、ピアモニタリングとインターフェイスモニタリングが含まれます。すべてのフェールオーバー基準にはデフォルト設定がありますが、デフォルト設定を調べて、それらがネットワークで機能していることを確認する必要があります。

- ピア装置のヘルスモニタリングフェールオーバー基準の設定 (237 ページ)。
- インターフェイスのヘルスモニタリングフェールオーバー基準の設定 (238 ページ)。

インターフェイステストの詳細については、システムがインターフェイスヘルスをテストする方法 (241 ページ) を参照してください。

- ステップ5 (オプション。ただし推奨。) [スタンバイ IP および MAC アドレスの設定 \(242 ページ\)](#)。
ステップ6 (オプション) [ハイ アベイラビリティ設定の確認 \(243 ページ\)](#)。

2 台の装置でのハイ アベイラビリティの準備

高可用性を正常に設定するには、多くのことを事前に正しく準備する必要があります。

手順

ステップ1 デバイスが[HA のハードウェア要件 \(225 ページ\)](#) に説明されている要件を満たしていることを確認します。

ステップ2 単一のフェールオーバー リンクを使用するのか、別のフェールオーバー リンクとステートフルフェールオーバー リンクを使用するのかを決め、使用するポートを特定します。

各リンクのそれぞれのデバイスで同じポート番号を使用する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで [GigabitEthernet 1/3](#) を使用します。使用する内容を把握しておくことで、誤ってその他の目的で使用することがなくなります。詳細については、[フェールオーバー リンクとステートフルフェールオーバー リンク \(218 ページ\)](#) を参照してください。

ステップ3 デバイスをインストールしてネットワークに接続し、各デバイスで初期セットアップウィザードを完了します。

- [フェールオーバーリンクとデータリンクの中断の回避 \(220 ページ\)](#) で推奨のネットワーク設計を確認します。
- [インターフェイスの接続 \(18 ページ\)](#) の説明に従い、少なくとも外部インターフェイスだけは接続します。

その他のインターフェイスも接続できますが、特定のサブネットへの接続には各デバイスで同じポートを使用する必要があります。各デバイスでは同じ設定が共有されるため、デバイスは同じ方法でネットワークに接続する必要があります。

(注) セットアップウィザードでは、管理インターフェイスと内部インターフェイスの IP アドレスを変更できません。そのため、プライマリデバイス上のそれらのインターフェイスのいずれかをネットワークに接続する場合、セカンダリデバイスのインターフェイスは接続しないでください。接続すると IP アドレスの競合が発生します。ワークステーションをそれらのインターフェイスのいずれかに直接接続し、DHCP を介してアドレスを取得できるため、[Firepower Device Manager](#) に接続して、デバイスを設定できます。

- 各デバイスで初期セットアップウィザードを完了します。外部インターフェイスの静的 IP アドレスを指定していることを確認します。さらに、同じ NTP サーバを設定します。詳細については、[初期設定の完了 \(28 ページ\)](#) を参照してください。

各装置で同じライセンスと Cisco Success Network オプションを選択します。たとえば、それぞれに評価モードを選択したり、デバイスを登録したりします。

- d) セカンダリ デバイスで、**[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)]** を選択して一意の IP アドレスを設定し、必要に応じてゲートウェイを変更します。また、ニーズに合わせて DHCP サーバの設定を無効化または変更します。
- e) セカンダリ デバイスで、**[デバイス (Device)] > [インターフェイス (Interface)]** を選択し、内部インターフェイスを編集します。IP アドレスを削除するか、または変更します。また、同じネットワーク上に 2 つの DHCP サーバは定義できないため、インターフェイスに定義されている DHCP サーバを削除します。
- f) 設定をセカンダリ デバイスに展開します。
- g) ネットワーク トポロジに基づいて必要な場合は、プライマリ デバイスにログインして、管理アドレス、ゲートウェイ、DHCP サーバの設定、および内部インターフェイスの IP アドレスを変更します。変更を加えた場合は、設定を展開します。
- h) 内部インターフェイス、または管理インターフェイス (別の管理ネットワークを使用する場合) を接続していない場合は、ここでそれらのインターフェイスをスイッチに接続できます。

ステップ 4 デバイスのソフトウェアバージョンが完全に同じである (つまり、同じメジャー (1 番)、マイナー (2 番)、メンテナンス (3 番) の番号が付いている) ことを確認します。バージョンは、Firepower Device Manager の [Devices] ページで確認できます。また、CLI で **show version** コマンドを使用して確認することもできます。

同じソフトウェア バージョンが実行されていない場合は、Cisco.com から推奨のソフトウェア バージョンを取得して、各デバイスにインストールします。詳細は、[Firepower Threat Defense ソフトウェアのアップグレード \(717 ページ\)](#) を参照してください。

ステップ 5 接続して、フェールオーバー リンクとステートフルフェールオーバー リンクを設定します。

- a) ([フェールオーバーリンクとデータリンクの中断の回避 \(220 ページ\)](#) で選択した) 推奨のネットワーク設計に従い、適切に各デバイスのフェールオーバーインターフェイスをスイッチに接続するか、デバイス間で直接接続します。
- b) 別のステートリンクを使用している場合は、各デバイスのステートフルフェールオーバーインターフェイスも適切に接続します。
- c) 次に各デバイスにログインして、**[デバイス (Device)] > [インターフェイス (Interface)]** にアクセスします。各インターフェイスを編集し、インターフェイス名や IP アドレスが設定されていないことを確認します。

名前付きのインターフェイスが設定されている場合、その名前を削除する前に、セキュリティゾーンからそれらのインターフェイスを削除して、その他の設定を削除する必要がある場合があります。名前の削除に失敗した場合は、エラーメッセージを調べて、加える必要があるその他の変更を確認します。

ステップ 6 プライマリ デバイスで、残りのデータ インターフェイスを接続してデバイスを設定します。

- a) **[デバイス (Device)] > [インターフェイス (Interface)]** を選択し、トラフィックの通過に使用される各インターフェイスを編集し、プライマリ静的 IP アドレスを設定します。

- b) セキュリティゾーンにインターフェイスを追加し、接続されたネットワーク上のトラフィックの処理に必要な基本的なポリシーを設定します。設定例については、[Firepower Threat Defense の使用例 \(53 ページ\)](#) にリストされているトピックを参照してください。
- c) 設定を展開します。

ステップ 7 [HA のソフトウェア要件 \(225 ページ\)](#) で説明されているすべての要件を満たしていることを確認します。

ステップ 8 一貫性のあるライセンス（登録済みまたは評価モード）を保有していることを確認します。詳細については、[HA のライセンス要件 \(226 ページ\)](#) を参照してください。

ステップ 9 セカンダリ デバイスで、残りのデータ インターフェイスをプライマリ デバイスの同等のインターフェイスと同じネットワークに接続します。インターフェイスは設定しないでください。

ステップ 10 各デバイスで [デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] を選択し、Cisco Defense Orchestrator の設定および Cisco Success Network や Cisco Threat Defense などのその他のクラウドサービスの設定が同じであることを確認します。これで、プライマリ デバイスでハイアベイラビリティを設定する準備が整いました。

ハイアベイラビリティ用のプライマリ装置の設定

アクティブ/スタンバイハイアベイラビリティペアをセットアップするには、まず、プライマリデバイスを設定する必要があります。プライマリデバイスは、通常の状況下でアクティブにする予定の装置です。セカンダリデバイスは、プライマリ装置が使用できなくなるまでスタンバイモードのままです。

プライマリにするデバイスを選択し、そのデバイス上の Firepower Device Manager にログインして次の手順に従います。



- (注) いったんハイアベイラビリティペアを確立すると、この手順で説明する設定を編集するにはペアを破棄する必要があります。

始める前に

フェールオーバーリンクとステートフルフェールオーバーリンク用に設定するインターフェイスに名前が付いていないことを確認します。名前が付いている場合は、セキュリティゾーンオブジェクトを含め、それらを使用するポリシーからインターフェイスを削除してインターフェイスを編集し、名前を削除する必要があります。また、インターフェイスはパッシブモードではなくルーテッドモードにする必要があります。これらのインターフェイスは、HA 設定での使用専用にする必要があります。他のプロセスに使用することはできません。

保留中の変更がある場合は、それらを展開してから HA を設定する必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックします。

ステップ 2 デバイスの概要の右側で、[ハイアベイラビリティ (High Availability)] グループの横にある [設定 (Configure)] をクリックします。

デバイスで初めて HA を設定する場合、グループは次のように表示されます。



ステップ 3 [ハイアベイラビリティ (High Availability)] ページで、[プライマリデバイス (Primary Device)] ボックスをクリックします。

セカンダリデバイスがすでに設定されていて、その設定をクリップボードにコピーした場合は、[クリップボードから貼り付け (Paste from Clipboard)] ボタンをクリックすると設定を貼り付けることができます。これにより、適切な値でフィールドが更新され、後で確認できます。

ステップ 4 [フェールオーバーリンク (Failover Link)] プロパティを設定します。

フェールオーバーペアの2台の装置は、フェールオーバーリンク経由で常に通信して、各装置の動作ステータスを確認し、設定の変更を同期します。詳細については、[フェールオーバーリンク \(218 ページ\)](#) を参照してください。

- [物理インターフェイス (Physical Interface)] フェールオーバーリンクとして使用するセカンダリデバイスに接続したインターフェイスを選択します。名前が付いていないインターフェイスにする必要があります。

フェールオーバーまたはステートリンクとして EtherChannel インターフェイスを使用している場合、高可用性を確立する前に、両方のデバイスで同じ ID とメンバー インターフェイスを備えた同じ EtherChannel が存在していることを確認する必要があります。EtherChannel の不一致がある場合は、先にセカンダリ装置で HA を無効にし、設定を修正する必要があります。順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。

- [タイプ (Type)] : インターフェイスに IPv4 アドレスまたは IPv6 アドレスを使用するかどうかを選択します。設定できるアドレスタイプは 1 つのみです。
- [プライマリ IP (Primary IP)] : このデバイス上のインターフェイスの IP アドレスを入力します。たとえば、192.168.10.1 と入力します。IPv6 アドレスの場合、標準表記にプレフィックス長を含める必要があります (2001:a0a:b00::a0a:b70/64 など) 。
- [セカンダリ IP (Secondary IP)] : セカンダリ デバイス上のインターフェイスについて、リンクのもう一方の端に設定する必要がある IP アドレスを入力します。このアドレスはプライマリアドレスと同じサブネット上に存在し、プライマリアドレスとは異なるアドレスである必要があります (192.168.10.2 または 2001:a0a:b00::a0a:b71/64 など) 。

- [ネットマスク (Netmask)] (IPv4 のみ) : プライマリ/セカンダリ IP アドレスのサブネットマスクを入力します。

ステップ 5 [ステートフルフェールオーバーリンク (Stateful Failover Link)] プロパティを設定します。

システムは、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。フェールオーバーリンクと同じリンクを使用するか、別のリンクを設定することができます。

- [フェールオーバーリンクと同じインターフェイスを使用する (Use the Same Interface as the Failover Link)] : フェールオーバー通信およびステートフルフェールオーバー通信に単一のリンクを使用する場合は、このオプションを選択します。このオプションを選択する場合は、次の手順に進みます。
- [物理インターフェイス (Physical Interface)] : 別のステートフルフェールオーバーリンクを使用する場合は、ステートフルフェールオーバーリンクとして使用するセカンダリデバイスに接続したインターフェイスを選択します。名前が付いていないインターフェイスにする必要があります。次のプロパティを設定します。
 - [タイプ (Type)] : インターフェイスに IPv4 アドレスまたは IPv6 アドレスを使用するかどうかを選択します。設定できるアドレスタイプは 1 つのみです。
 - [プライマリ IP (Primary IP)] : このデバイス上のインターフェイスの IP アドレスを入力します。アドレスは、フェールオーバーリンクに使用されるものとは別のサブネット上にある必要があります。たとえば、192.168.11.1 と入力します。IPv6 アドレスの場合、標準表記にプレフィックス長を含める必要があります (2001:a0a:b00:a::a0a:b70/64 など) 。
 - [セカンダリ IP (Secondary IP)] : セカンダリ デバイス上のインターフェイスについて、リンクのもう一方の端に設定する必要がある IP アドレスを入力します。このアドレスはプライマリアドレスと同じサブネット上に存在し、プライマリアドレスとは異なるアドレスである必要があります (192.168.11.2 または 2001:a0a:b00:a::a0a:b71/64 など) 。
 - [ネットマスク (Netmask)] (IPv4 のみ) : プライマリ/セカンダリ IP アドレスのサブネットマスクを入力します。

ステップ 6 (オプション) ペアの 2 台の装置間での通信を暗号化する場合は、[IPsec暗号キー (IPsec Encryption Key)] 文字列を入力します。

セカンダリノードでまったく同じキーを設定する必要があるため、入力した文字列をメモしてください。

キーを入力しなければ、フェールオーバーリンクとステートフルフェールオーバーリンクでのすべての通信はプレーンテキストで実行されます。インターフェイス間をケーブルで直接接続していない場合、これによってセキュリティの問題が発生することがあります。

ステップ 7 [HAの有効化 (Activate HA)] をクリックします。

システムは、すぐにデバイスに設定を展開します。展開ジョブを開始する必要はありません。設定が保存され、展開が進行中であるというメッセージが表示されない場合は、ページ上部にスクロールして、エラーメッセージを確認します。

設定はクリップボードにもコピーされます。コピーを使用すると、簡単にセカンダリ装置を設定できます。セキュリティを強化するため、暗号キーはクリップボードのコピーには含まれません。

設定が完了すると、実行する必要がある次の手順を説明するメッセージが表示されます。情報を確認したら、[了解 (Got It)] をクリックします。

この時点で、[ハイアベイラビリティ (High Availability)] ページが表示され、デバイスステータスが [ネゴシエーション中 (Negotiating)] になっている必要があります。ステータスはピアの設定前でも [アクティブ (Active)] に変わります。設定するまで [故障 (Failed)] と表示されます。

PRIMARY DEVICE
Current Device Mode: **Active**  Peer: **Failed** 

これで、セカンダリ装置を設定できるようになりました。[ハイアベイラビリティ用のセカンダリ装置の設定 \(235 ページ\)](#) を参照してください。

(注) 選択したインターフェイスは直接設定されません。ただし、CLI に **show interface** と入力すると、インターフェイスが特定の IP アドレスを使用していることが表示されます。インターフェイスには「failover-link」という名前が付いています。別のステートリンクを設定する場合は「stateful-failover-link」になります。

ハイアベイラビリティ用のセカンダリ装置の設定

プライマリデバイスをアクティブ/スタンバイ ハイアベイラビリティ向けに設定した後、セカンダリデバイスを設定する必要があります。そのデバイス上の Firepower Device Manager にログインして、次の手順に従います。



(注) まだそのように設定していない場合は、プライマリデバイスからクリップボードにハイアベイラビリティ設定をコピーします。手動でデータを入力するより、コピーと貼り付けを使用してセカンダリデバイスを設定するほうがはるかに簡単です。

手順

- ステップ 1** [デバイス (Device)] をクリックします。
- ステップ 2** デバイスの概要の右側で、[ハイアベイラビリティ (High Availability)] グループの横にある [設定 (Configure)] をクリックします。

デバイスで初めて HA を設定する場合、グループは次のように表示されます。



ステップ 3 [ハイアベイラビリティ (High Availability)] ページで、[セカンダリデバイス (Secondary Device)] ボックスをクリックします。

ステップ 4 次のいずれかを実行します。

- [簡単な方法 (Easy method)] : [クリップボードから貼り付け (Paste from Clipboard)] ボタンをクリックして設定に貼り付け、[OK] をクリックします。これにより、適切な値でフィールドが更新され、後で確認できます。
- [手動の方法 (Manual method)] : フェールオーバー リンクとステートフルフェールオーバーリンクを直接設定します。プライマリデバイスに入力したのとまったく同じ設定をセカンダリデバイスに入力します。


ステップ 5 プライマリデバイスで [IPSec暗号キー (IPSec Encryption Key)] を設定した場合、まったく同じキーをセカンダリデバイスに入力します。

ステップ 6 [HAの有効化 (Activate HA)] をクリックします。

システムは、すぐにデバイスに設定を展開します。展開ジョブを開始する必要はありません。設定が保存され、展開が進行中であるというメッセージが表示されない場合は、ページ上部にスクロールして、エラーメッセージを確認します。

設定が完了すると、HA が設定されたことを示すメッセージが表示されます。[了解 (Got It)] をクリックして、メッセージを閉じます。

この時点で、[ハイアベイラビリティ (High Availability)] ページが表示され、デバイスステータスにこれがセカンダリデバイスであることが示されている必要があります。プライマリデバイスとの結合が成功した場合、デバイスはプライマリと同期して、最終的にはスタンバイモードになります。ピアがアクティブになります。

SECONDARY DEVICE
Current Device Mode: **Standby**  Peer Device: **Active**

- (注) 選択したインターフェイスは直接設定されません。ただし、CLI に **show interface** と入力すると、インターフェイスが特定の IP アドレスを使用していることが表示されます。インターフェイスには「failover-link」という名前が付いています。別のステートリンクを設定する場合は「stateful-failover-link」になります。

ヘルスマニタリングのフェールオーバー基準の設定

ハイアベイラビリティ設定の装置は、全体的な健全性とインターフェイスの健全性をモニタします。

フェールオーバー基準により、ピアに障害が発生したかどうかを判断するヘルスモニタリングメトリックが定義されます。アクティブピアが基準に違反した装置である場合、スタンバイ装置へのフェールオーバーがトリガーされます。スタンバイピアが基準に違反した装置である場合、スタンバイピアは障害が発生した装置としてマークされ、フェールオーバーに使用できなくなります。

アクティブデバイスでのみフェールオーバー基準を設定できます。

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。

表 6: フェールオーバー基準に基づくフェールオーバー時間

フェールオーバー トリガー イベント	最小	デフォルト	最大数
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ装置のインターフェイスの物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイステストを行っている。	5 秒	25 秒	75 秒

ここでは、フェールオーバーヘルスモニタリング基準をカスタマイズする方法と、システムがインターフェイスをテストする方法について説明します。

ピア装置のヘルス モニタリング フェールオーバー基準の設定

ハイアベイラビリティ設定の各ピアは、hello メッセージを使用してフェールオーバーリンクをモニタすることによって相手装置の状態を判断します。装置がフェールオーバーリンクで3回連続してhello メッセージを受信しない場合、装置はフェールオーバーリンクを含む各データインターフェイスにLANTEST メッセージを送信し、ピアが応答するかどうか検証します。デバイスが行うアクションは、相手装置からの応答によって異なります。

- デバイスがフェールオーバーリンクで応答を受信した場合は、フェールオーバーを行いません。
- デバイスがフェールオーバーリンクで応答を受信せず、データインターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバーリンクは故障とマークされます。フェールオーバーリンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
- デバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブモードに切り替わり、相手装置を故障に分類します。

hello メッセージのポーリング時間および保留時間を設定できます。

手順

ステップ 1 アクティブデバイスで、[デバイス (Device)] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ (High Availability)] リンクをクリックします。

フェールオーバー条件は、[ハイアベイラビリティ (High Availability)] ページの右側の列に表示されます。

ステップ 3 [ピアのタイミング設定 (Peer Timing Configuration)] を定義します。

これらの設定では、アクティブデバイスがスタンバイデバイスにフェールオーバーできる早さを決定します。ポーリング時間が短いほど、デバイスは短時間で障害を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。ほとんどの場合、デフォルト設定が適切です。

1 回のポーリング期間中に装置がフェールオーバー インターフェイスで hello パケットを検出できなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると考えられ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

- [ポーリング時間 (Poll Time)] : hello メッセージ間の間隔。1 ~ 15 秒または 200 ~ 999 ミリ秒を入力します。デフォルト値は 1 秒です。
- [保留時間 (Hold Time)] : 装置が、フェールオーバー リンクで hello メッセージを受信する間隔。この時間を経過すると、ピア装置で障害が発生したと見なされます。保留時間は、ポーリング時間の 3 倍以上にする必要があります。1 ~ 45 秒または 800 ~ 999 ミリ秒を入力します。デフォルトは 15 秒です。

ステップ 4 [保存 (Save)] をクリックします。

インターフェイスのヘルス モニタリング フェールオーバー基準の設定

デバイスモデルに応じて、最大 211 のインターフェイスをモニタできます。重要なインターフェイスをモニタする必要があります。たとえば、重要なネットワーク間のスループットを保証するインターフェイスなどです。スタンバイ IP アドレスを設定する場合、さらにインターフェイスを常にアップ状態にする必要がある場合にのみインターフェイスをモニタします。

装置が、2 回のポーリング期間中にモニタ対象のインターフェイス上で hello メッセージを受信しない場合、インターフェイステストを実行します。1 つのインターフェイスに対するすべてのインターフェイステストがすべて失敗したが、相手装置のこの同じインターフェイスが正常にトラフィックを渡し続けている場合、そのインターフェイスは故障していると考えられません。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われず。相手装置のインターフェイスもすべてのネットワークテストに失敗した場合、両方のインターフェイスが「Unknown」状態になり、フェールオーバー制限に向けてのカウントは行いません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したデバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイモードに戻ります。

show monitor-interface コマンドを使用して、CLI または CLI コンソールからインターフェイスの HA ステータスをモニタできます。詳細については、[HA モニタ対象インターフェイスのステータスのモニタリング \(257 ページ\)](#) を参照してください。



- (注) のインターフェイスの1つがダウンしたときも、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスがダウンしていることを装置が検出すると、インターフェイスの保留時間を待たずにすぐにフェールオーバーが発生します (1 インターフェイスのデフォルトしきい値を維持している場合)。インターフェイスの保留時間が有効であるのは、装置が自身のステータスを OK と見なしているときだけです (ピアから hello パケットを受信していなくても)。

始める前に

デフォルトでは、すべての名前付き物理インターフェイスが HA モニタリングに選択されています。したがって、重要ではない物理インターフェイスのモニタリングを無効にする必要があります。サブインターフェイスまたはブリッジグループでは、手動でモニタリングを有効にする必要があります。

インターフェイス モニタリングを完全に無効にしてインターフェイスの故障によるフェールオーバーを防止するには、単純に、HA モニタリングが有効になっているインターフェイスがないことを確認します。

手順

ステップ 1 アクティブデバイスで、[デバイス (Device)] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ (High Availability)] リンクをクリックします。

フェールオーバー条件は、[ハイアベイラビリティ (High Availability)] ページの右側の列に表示されます。

ステップ 3 [インターフェイス障害しきい値 (Interface Failure Threshold)] を定義します。

故障したインターフェイスの数がしきい値を満たすと、装置は自身を故障としてマークします。装置がアクティブ装置の場合、スタンバイ装置にフェールオーバーします。装置がスタンバイ装置の場合、自身を故障としてマークすることによって、アクティブ装置はその装置をフェールオーバーに利用できると見なさなくなります。

この条件を設定する場合、モニタするインターフェイスの数を考慮します。たとえば、2つのインターフェイスでのみモニタリングを有効にすると、10個のインターフェイスのしきい値に到達することはありません。インターフェイスのプロパティを編集するときに [詳細オプショ

ン (Advanced Options)] タブの [HAモニタリングの有効化 (Enable for HA Monitoring)] オプションを選択することで、インターフェイスのモニタリングを設定します。

デフォルトでは、1つのモニタ対象インターフェイスが故障すると、装置は自身を故障としてマークします。

次の [フェールオーバー条件 (Failover Criteria)] オプションのいずれかを選択して、インターフェイス障害のしきい値を設定できます。

- [故障したインターフェイスの数を超える (Number of failed interfaces exceeds)] : インターフェイスの生の数字を入力します。デフォルトは1です。実際には、最大値はデバイスモデルに依存して変わりますが、211 を超える数を入力することはできません。この条件を使用すると、デバイスサポートよりも大きい数を入力すると展開エラーが発生します。より小さい数を試すか、代わりにパーセンテージを使用します。
- [故障インターフェイスのパーセンテージを超える (Percentage of failed interfaces exceeds)] : 1 ~ 100 の数値を入力します。たとえば、50% と入力して 10 個のインターフェイスをモニタする場合、5 個のインターフェイスが故障するとデバイスは自身を故障としてマークします。

ステップ 4 [インターフェイス タイミング設定 (Interface Timing Configuration)] を定義します。

これらの設定では、インターフェイスで障害が発生したかどうかをアクティブデバイスが判断できる早さを決定します。ポーリング時間が短いほど、デバイスは短時間でインターフェイスの障害を検出できます。ただし、検出が早いほど、実際には健全な状態でもビジー状態のインターフェイスが障害発生とマークされ、必要以上に頻繁にフェールオーバーが生じる可能性があります。ほとんどの場合、デフォルト設定が適切です。

インターフェイスリンクがダウンしていると、インターフェイスのテストは実行されません。また、故障したインターフェイスの数が設定されたインターフェイスフェールオーバーしきい値に合致するかまたはそれを超過すると、スタンバイ装置は1回のインターフェイスポーリング期間でアクティブになります。

- [ポーリング時間 (Poll Time)] : hello パケットがデータインターフェイスで送信される頻度。1 ~ 15 秒または 500 ~ 999 ミリ秒を入力します。デフォルトは 5 秒です。
- [保留時間 (Hold Time)] : 保留時間によって、hello パケットを受信できなかったときからインターフェイスが故障とマークされるまでの時間が決まります。5 ~ 75 秒を入力します。ポーリング時間の 5 倍に満たない保持時間は入力できません。

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 モニタする各インターフェイスの HA モニタリングを有効にします。

a) [デバイス (Device)] > [インターフェイス (Interfaces)] を選択します。

インターフェイスをモニタしている場合、[HAのモニタ (Monitor for HA)] 列は [有効 (Enabled)] になります。

b) モニタリングステータスを変更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。

フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスは編集できません。インターフェイス モニタリングはそれらに適用されません。

- c) [詳細オプション (Advanced Options)] タブをクリックします。
- d) 必要に応じて、[HAモニタリングの有効化 (Enable for HA Monitoring)] チェックボックスを選択または選択解除します。
- e) [OK] をクリックします。

ステップ7 (オプション。ただし推奨。) モニタ対象インターフェイスのスタンバイ IP アドレスおよび MAC アドレスを設定します。 [スタンバイ IP および MAC アドレスの設定 \(242 ページ\)](#) を参照してください。

システムがインターフェイスヘルスをテストする方法

システムは、ユーザがハイ アベイラビリティ ヘルスをモニタしているインターフェイスを継続的にテストします。インターフェイスのテストに使用されるアドレスは、ユーザが設定するアドレスタイプに基づきます。

- インターフェイスに IPv4 アドレスと IPv6 アドレスの両方が設定されている場合、デバイスは IPv4 アドレスを使用してヘルスマニタリングを実行します。
- インターフェイスに IPv6 アドレスだけが設定されている場合、デバイスは ARP ではなく IPv6 ネイバー探索を使用してヘルスマニタリングテストを実行します。ブロードキャスト ping テストの場合、デバイスは IPv6 全ノードアドレス (FE02::1) を使用します。

システムは、各装置で次のテストを実行します。

1. リンクアップ/ダウンテスト：インターフェイスステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、装置はそれに障害が発生していると見なします。ステータスが Up (稼働中) の場合、装置はネットワーク動作のテストを実行します。
2. ネットワークアクティビティテスト：ネットワークの受信アクティビティのテストです。このテストの目的は、LANTEST メッセージを使用してネットワーク トラフィックを生成し、障害が発生しているユニット (いずれか1つ) を特定することです。テストの開始時に、各装置はインターフェイスの受信パケットカウントをリセットします。ユニットがテスト中にパケットを受信したらすぐに (最大5秒)、そのインターフェイスは動作可能と見なされます。いずれか一方の装置だけがトラフィックを受信している場合は、トラフィックを受信しなかった装置が故障していると見なされます。いずれの装置もトラフィックを受信しなかった場合、装置は ARP テストを開始します。
3. ARP テスト：取得したエントリの最後の2つの装置 ARP キャッシュの読み取り。ネットワーク トラフィックを発生させるため、ユニットから1回に1つずつ、これらのデバイスにARP要求が送信されます。各要求後、装置は最大5秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると思なされます。トラフィックが受信されなければ、次のデバイスにARP要求が送信され

ます。リストの最後まで来てもトラフィックが受信されない場合は、ping テストが実行されます。

4. ブロードキャスト ping テスト：このテストでは、ブロードキャスト ping 要求が送信されます。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなければ、ARP テストからやり直します。

スタンバイ IP および MAC アドレスの設定

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。スタンバイアドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイインターフェイスの状態を確認するためのネットワークテストを実行できません。リンクステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

1. プライマリ装置に障害が発生すると、セカンダリ装置はプライマリユニットの IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
2. 現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ネットワークデバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。しかし、プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワークトラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。


仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスは手動で設定できます。

仮想 MAC アドレスを設定しなかった場合、トラフィックフローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。Firepower Threat Defense デバイスは MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

手順

ステップ 1 [デバイス (Device)] > [インターフェイス (Interfaces)] を選択します。

少なくとも、HA をモニタしているインターフェイスのスタンバイ IP アドレスと MAC アドレスを設定する必要があります。インターフェイスをモニタしている場合、[HA のモニタ (Monitor for HA)] 列は [有効 (Enabled)] になります。

ステップ 2 スタンバイアドレスを設定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。

フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスは編集できません。ハイアベイラビリティを設定する場合、これらのインターフェイスの IP アドレスを設定します。

ステップ 3 [IPv4 アドレス (IPv4 Address)] タブおよび [IPv6 アドレス (IPv6 Address)] タブでスタンバイ IP アドレスを設定します。

スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニッツはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。使用している IP バージョンごとにスタンバイアドレスを設定します。

ステップ 4 [詳細オプション (Advance Options)] タブをクリックして、MAC アドレスを設定します。


デフォルトでは、システムはインターフェイスのネットワークインターフェイスカード (NIC) に焼き込まれた MAC アドレスを使用します。したがって、インターフェイスのすべてのサブインターフェイスは同じ MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MAC アドレス (MAC Address)] : H.H.H 形式の Media Access Control アドレス。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は 000C.F142.4CDE と入力します。MAC アドレスはマルチキャストビットセットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。
- [スタンバイ MAC アドレス (Standby MAC Address)] : 高可用性で使用します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 5 [OK] をクリックします。

ハイアベイラビリティ設定の確認

ハイアベイラビリティの設定が完了したら、両方のデバイスが「動作中」でアクティブ/スタンバイ モードであることが、デバイスのステータスに示されていることを確認します。

```
PRIMARY DEVICE
Current Device Mode: Active  Peer Device: Standby
```

次の手順を使用して、ハイアベイラビリティの設定が機能していることを確認できます。

手順

ステップ1 FTPなどを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

設定済みの各インターフェイスに接続されている、少なくとも1つのワークステーションからシステムへの接続をテストします。

ステップ2 次のいずれかを実行して、モードを切り替え、アクティブな装置をスタンバイ装置にします。

- Firepower Device Manager で、[デバイス (Device)] > [ハイアベイラビリティ (High Availability)] ページの歯車メニューから [モードの切り替え (Switch Mode)] を選択します。
- アクティブな装置の CLI で、**no failover active** を入力します。

ステップ3 接続テストを繰り返して、ハイアベイラビリティ ペア内のその他の装置からも同じ接続を確立できることを確認します。

テストが失敗する場合は、他の装置の同等インターフェイスと同じネットワークにその装置のインターフェイスを接続していることを確認します。

HA ステータスは [ハイアベイラビリティ (High Availability)] ページから確認できます。CLI または装置の CLI コンソールを使用し、**show failover** コマンドを入力して、フェールオーバー ステータスを確認することもできます。また、**show interface** コマンドを使用して、失敗した接続テストで使用されたインターフェイスのインターフェイス設定を確認できます。

これらの操作で問題を特定できない場合は、他の手順を実行することができます。[ハイアベイラビリティ \(フェールオーバー\) のトラブルシューティング \(259ページ\)](#) を参照してください。

ステップ4 完了したら、モードを切り替えて、元々アクティブだった装置をアクティブステータスに戻します。

ハイアベイラビリティの管理


ハイアベイラビリティ ペアを管理するには、[デバイス概要 (Device Summary)] ページの [ハイアベイラビリティ (High Availability)] リンクをクリックします。




[ハイアベイラビリティ (High Availability)] ページには次のものがあります。

- [ロールおよびモードステータス (Role and Mode Status)] : 左側のステータスエリアには、デバイスがグループ内のプライマリ デバイスかセカンダリ デバイスかが示されます。モードには、このデバイスがアクティブかスタンバイかや、HA が一時停止されているかデバイスがピアデバイスの参加を待っているかが示されます。また、ピアデバイスのステータ

ス（アクティブ、スタンバイ、一時停止、または障害）も示されます。たとえば、現在ログインしているデバイスがプライマリデバイスであり、アクティブデバイスでもある場合、セカンダリデバイスが正常で、必要に応じてフェールオーバーできる状態であれば、ステータスは次のように表示されます。ピアの間のアイコンをクリックすると、デバイス間の設定同期ステータスに関する情報を取得できます。

PRIMARY DEVICE
Current Device Mode: **Active**  Peer Device: **Standby**

- [フェールオーバー履歴（Failover History）] リンク：このリンクをクリックすると、ペアに含まれるデバイスのステータスの詳細な履歴を確認できます。CLI コンソールが開き、**show failover history details** コマンドが実行されます。
- [展開履歴（Deployment History）] リンク：このリンクをクリックすると、イベントがフィルタリングされて展開ジョブだけが表示された監査ログに移動します。
- 歯車ボタン ：このボタンをクリックすると、デバイス上でアクションが実行されます。
 - [HAの一時停止（Suspend HA）]/[HAの再開（Resume HA）]：HAを一時停止すると、HA設定を削除しなくても、デバイスがハイアベイラビリティペアとして機能しなくなります。その後、デバイスでHAを再開（つまり再有効化）することができます。詳細については、[ハイアベイラビリティの中断または再開（246 ページ）](#)を参照してください。
 - [HAの解除（Break HA）]：HAを解除すると、両方のデバイスからハイアベイラビリティ設定が削除され、それらがスタンドアロンデバイスに戻ります。詳細については、[ハイアベイラビリティの破棄（247 ページ）](#)を参照してください。
 - [モードの切り替え（Switch Mode）]：モードを切り替えることにより、アクションを実行するデバイスに応じて、強制的にアクティブデバイスをスタンバイにしたりスタンバイデバイスをアクティブにすることができます。詳細は、[アクティブピアとスタンバイピアの切り替え（強制フェールオーバー）（248 ページ）](#)を参照してください。
- [ハイアベイラビリティ設定（High Availability Configuration）]：このパネルには、フェールオーバーペアの設定が表示されます。[クリップボードにコピー（Copy to Clipboard）] ボタンをクリックすると情報をクリップボードにロードできます。そこから、セカンダリデバイスの設定に貼り付けることができます。情報を記録するために別のファイルにコピーすることもできます。この情報には、IPsec 暗号キーを定義したかどうかは示されません。



(注) HA のインターフェイス設定は、インターフェイスのページ（[デバイス（Device）]>[インターフェイス（Interfaces）]）に反映されません。HA 設定で使用しているインターフェイスは編集できません。

- [フェールオーバー基準 (Failover Criteria)]: このパネルには、「アクティブ装置に障害が発生したためにスタンバイ装置がアクティブ装置になる必要がある」かどうかを評価する際に使用される健全性の基準を決定する設定が含まれます。これらの基準を調整して、ネットワークで必要なフェールオーバーパフォーマンスを実現してください。詳細については、[ヘルスマonitoringのフェールオーバー基準の設定 \(236ページ\)](#) を参照してください。

ここでは、ハイアベイラビリティ設定に関連するさまざまな管理タスクについて説明します。

ハイアベイラビリティの中断または再開

ハイアベイラビリティ ペアの1つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状態で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。
- スタンバイデバイスのソフトウェアアップグレードをインストール中のフェールオーバーを防ぎたい場合。

ハイアベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の疑似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイアベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムでHAを再開するためのオプションがあります。これにより、既存の設定が有効になり、2台のデバイスがフェールオーバー ペアとして再び機能します。

アクティブ装置からハイアベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピアユニットとアクティブ/スタンバイ ステータスをネゴシエートします。



- (注) 必要に応じて、**configure high-availability suspend** コマンドを入力して、CLI から HA を中断できます。HA を再開するには、**configure high-availability resume** と入力します。

始める前に

Firepower Device Manager を使用してハイアベイラビリティを中断した場合、装置をリロードした場合でも、再開するまで中断のままになります。ただし、CLIを使用して中断した場合は一時的な状態なので、リロード時に装置のハイアベイラビリティの設定が自動的に再開され、ピアとアクティブ/スタンバイ状態がネゴシエートされます。

スタンバイ装置のハイアベイラビリティを中断する場合は、展開ジョブがアクティブな装置で実行中かどうかを確認してください。展開ジョブの進行中にモードを切り替えると、ジョブが失敗し、設定の変更は失われます。

手順

ステップ 1 [デバイス (Device)] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ (High Availability)] リンクをクリックします。

ステップ 3 歯車アイコン (⚙️) から適切なコマンドを選択します。

- [HAの中断 (Suspend HA)]: アクションの確認を求められます。メッセージを読んで、[OK] をクリックします。HA ステータスにデバイスが中断モードであることが表示されず。
- [HAの再開 (Resume HA)]: アクションの確認を求められます。メッセージを読んで、[OK] をクリックします。HA ステータスは、装置がピアとネゴシエートした後に正常 (アクティブまたはスタンバイ) に戻ります。

ハイアベイラビリティの破棄

2台のデバイスをハイアベイラビリティペアとして稼働させない場合は、HA設定を破棄できます。HAを破棄すると、各デバイスはスタンドアロンデバイスになります。これらの設定は、次のように変更されます。

- アクティブデバイスは破棄される前と変わらずすべての設定を維持し、HA設定が削除されます。
- スタンバイデバイスではHA設定だけでなくすべてのインターフェイス設定が削除されず。すべての物理インターフェイスは無効になりますが、サブインターフェイスは無効になりません。管理インターフェイスはアクティブなままであるため、デバイスにログインして再設定することができます。

破棄が装置にどのように影響するのかは、破棄を実行するときの各装置の状態によって変わります。

- 装置が健全なアクティブ/スタンバイ状態である場合、アクティブ装置からHAを破棄します。これにより、HAペアの両方のデバイスからHA設定が削除されます。スタンバイ装

置でのみ HA を破棄する場合は、スタンバイ装置にログインして HA を中断した後に HA を破棄できます。

- スタンバイ装置が中断状態または障害状態になっている場合、アクティブ装置から HA を破棄するとアクティブ装置からのみ HA 設定が削除されます。スタンバイ装置にログインして、スタンバイ装置の HA も破棄する必要があります。
- ピアが HA をネゴシエーションしていたり設定を同期している場合、HA を破棄することはできません。ネゴシエーションまたは同期が完了するか、タイムアウトになるまで待ちます。システムがこの状態でスタックしていると思われる場合は、HA を中断してから HA を破棄することができます。



(注) Firepower Device Manager を使用する場合、**configure high-availability disable** コマンドを使用して CLI から HA を破棄することはできません。

始める前に

理想的な結果を得るために、デバイスを健全なアクティブ/スタンバイ状態にして、アクティブデバイスからこの操作を実行します。

手順

- ステップ 1** [デバイス (Device)] をクリックします。
- ステップ 2** デバイスの概要の右側に表示される [ハイアベイラビリティ (High Availability)] リンクをクリックします。
- ステップ 3** 歯車アイコン (⚙️) から、[HAの破棄 (Break HA)] を選択します。
- ステップ 4** 確認メッセージを読み、オプションを選択してインターフェイスを無効にするかどうかを決定し、[OK] をクリックします。

スタンバイ装置から HA を破棄する場合は、インターフェイスを無効にするオプションを選択する必要があります。

システムはすぐに、このデバイスとピアデバイスの両方で変更を展開します（可能な場合）。各デバイスで展開が完了して、各デバイスが依存しなくなるまで数分かかることがあります。

アクティブピアとスタンバイピアの切り替え（強制フェールオーバー）

機能しているハイアベイラビリティピア（つまり、1つのピアがアクティブで、もう1つがスタンバイ）のアクティブ/スタンバイモードを切り替えることができます。たとえば、ソフト

ウェアアップグレードをインストールしている場合は、アクティブな装置をスタンバイに切り替えて、アップグレードがユーザトラフィックに影響を及ぼさないようにできます。

モードはアクティブまたはスタンバイ装置から切り替えることができますが、ピア装置はその他の装置の観点から機能している必要があります。中断中の装置がある場合、モードを切り替えることはできません（最初に HA を再開する必要があります）。そうしないと、失敗します。



- (注) 必要に応じて、CLIからアクティブモードとスタンバイモードを切り替えることができます。スタンバイ装置から **failover active** コマンドを入力します。アクティブな装置から **no failover active** コマンドを入力します。

始める前に

モードを切り替える前に、アクティブな装置で展開ジョブが進行中でないことを確認します。展開ジョブの完了を待ってから、モードを切り替えます。

アクティブな装置に保留中の展開していない変更がある場合は、モードを切り替える前に展開します。そうしないと、新しいアクティブな装置から展開ジョブを実行した場合に変更内容が失われます。

手順

- ステップ 1 [デバイス (Device)] をクリックします。
- ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ (High Availability)] リンクをクリックします。
- ステップ 3 歯車アイコンから (⚙️) から、[モードの切り替え (Switch Mode)] を選択します。
- ステップ 4 確認メッセージを読んで、[OK] をクリックします。

強制的にフェールオーバーが行われ、アクティブな装置がスタンバイになり、スタンバイ装置が新しいアクティブな装置になります。

フェールオーバー後の未展開の設定変更の保持

ハイアベイラビリティ ペアの装置の設定を変更する場合は、アクティブ装置で設定を編集します。その後、変更を展開すると、アクティブ装置とスタンバイ装置の両方が新しい設定で更新されます。アクティブ装置がプライマリデバイスであるかセカンダリデバイスであるかは関係ありません。

ただし、未展開の変更は装置間で同期されません。未展開の変更は、変更を行った装置でのみ利用できます。

そのため、未展開の変更があるときにフェールオーバーが発生すると、その変更は新しいアクティブ装置で利用できません。ただし、現在のスタンバイになっている装置では、変更が保持されています。

未展開の変更を取得するには、モードを切り替えてフェールオーバーを強制的に実行し、そのもう一方の装置をアクティブステータスに戻す必要があります。新しくアクティブになった装置にログインすると、未展開の変更が利用可能になり、それらを展開できます。[ハイアベイラビリティ (High Availability)]設定の歯車メニュー (⚙️) から [モードの切り替え (Switch Modes)]コマンドを使用します。

次の点に注意してください。

- スタンバイ装置上に未展開の変更があるときにアクティブ装置から変更を展開すると、スタンバイ装置上の未展開の変更が削除されます。そのため、それらを取得できなくなります。
- スタンバイ装置がハイアベイラビリティペアに参加すると、そのスタンバイ装置上の未展開の変更が削除されます。装置がペアに参加または再参加するたびに、設定が同期されます。
- 未展開の変更を持つ装置に致命的な障害が発生し、その装置を置き換えたり再イメージ化する必要があった場合は、未展開の変更が完全に失われます。

ハイアベイラビリティモードでのライセンスと登録の変更

ハイアベイラビリティペアの装置は、ライセンスと登録ステータスが同じである必要があります。変更するには、次の手順に従います。

- アクティブ装置でオプションのライセンスを有効または無効にします。その後、設定を展開すると、スタンバイ装置が必要なライセンスを要求 (または解放) します。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。
- 装置を個別に登録または登録解除します。正しく機能させるには、両方の装置を評価モードにするか、両方の装置に登録する必要があります。装置を異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態 (両方有効または両方無効) である必要があります。装置の登録ステータスに一貫性がない場合は、設定の変更を展開できません。

HA IPsec 暗号キーまたは HA 設定の編集

フェールオーバー基準を変更するには、アクティブ装置にログインし、変更を加えて、それらを展開します。

ただし、フェールオーバーリンクで使用される IPsec暗号キーを変更したり、フェールオーバーまたはステートフルフェールオーバーリンクのインターフェイスや IP アドレスを変更する必

必要がある場合は、まず HA 設定を解除する必要があります。その後、新しい暗号キーまたはフェールオーバー/ステートフルフェールオーバーリンク設定を使用してプライマリおよびセカンダリ装置を再設定できます。

障害のある装置の正常な装置としてのマーキング

ハイアベイラビリティ設定の装置は、定期的なヘルスマニタリングによって、障害が発生した装置としてマーキングされる場合があります。この装置が正常である場合は、ヘルスマニタリング要件を再度満たすと正常なステータスに戻ります。正常なデバイスが、頻繁に、障害が発生したデバイスとしてマーキングされる場合は、ピアタイムアウトの値を増やしたり、重要性の低い特定のインターフェイスのモニタリングを停止したり、インターフェイスのモニタリングタイムアウトを変更することができます。

CLI から **failover reset** コマンドを入力することにより、障害が発生した装置を強制的に正常な装置として表示させることができます。このコマンドは、アクティブ装置から入力することをお勧めします。それにより、スタンバイ装置のステータスがリセットされます。**show failover** コマンドまたは **show failover state** コマンドを使用することにより、装置のフェールオーバーステータスを表示できます。

障害が発生した装置を障害のない状態に復元しても、その装置は自動的にアクティブになりません。復元された装置は、（強制または通常の）フェールオーバーによってアクティブになるまではスタンバイ状態のままです。

デバイスステータスをリセットしても、障害が発生したデバイスとしてマーキングされる原因となった問題は解決されません。問題に対処しなかったり、モニタリングタイムアウトを緩和したりすると、そのデバイスは、障害が発生したデバイスとして再びマーキングされます。

HA デバイスでのソフトウェアアップグレードのインストール

ネットワーク内のトラフィックを中断することなく、高可用性ペアのデバイスで実行中のシステムソフトウェアをアップグレードできます。基本的にはスタンバイデバイスをアップグレードして、アクティブデバイスでトラフィックの処理を続行できるようにします。アップグレードが完了したら、役割を切り替えて、スタンバイ装置をもう一度アップグレードします。

高可用性グループ内の装置で異なるソフトウェアバージョンが実行されている間は、フェールオーバーはできません。通常の状態では、各装置で同じソフトウェアバージョンを実行する必要があります。別バージョンの実行が有効なのは、ソフトウェアアップグレードのインストールの進行中だけです。

この手順はアップグレードプロセスを要約したものです。詳細については、[Firepower Threat Defenseソフトウェアのアップグレード（717 ページ）](#) を参照してください。



- (注) アップグレード中、システムは自動展開を含むシステムライブラリの更新中に HA を一時停止します。このプロセスの最後の部分では、システムは SSH 接続に使用できます。そのため、アップグレードの適用後すぐにログインすると、HA が中断ステータスとして表示される場合があります。システムがスタンバイ状態に戻ることがなく、FDM が使用可能になり、自動展開が成功した後も、この問題が解消されない場合は、HA ページに移動し、HA を手動で再開してください。

始める前に

アップグレードプロセスを開始する前に保留中の変更をアクティブ ノードから展開していることを確認します。デバイスのアップグレード時には、設定を変更したり、1 台のデバイスのアップグレード後かつ他のデバイスのアップグレード前に展開を開始したりしないでください。展開が失敗し、変更内容が失われる可能性があります。

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のすべてのタスクが完了するまでお待ちください。また、スケジュールされたタスクがないかどうかを確認します。アップグレードタスクに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、アプリケーションフィルタ、アクセスルール、または SSL 復号ルールに非推奨のアプリケーションが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、以前に有効になっていたアプリケーションが廃止される可能性があります。この場合、アップグレードは失敗し、デバイスは使用不能状態のままになります。

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 Compatibility Guide』 (<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 スタンバイ装置にログインして、アップグレードをインストールします。

- a) [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。
- b) [システムアップグレード (System Upgrade)] グループで、[参照 (Browse)] または [別のファイルのアップロード (Upload Another File)] をクリックして、イメージをアップロードします。
- c) [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。

インストールが完了するまで待機したら、再度ログインして、システムが正常に機能していることを確認できます。

(注) 高可用性のステータスを確認すると、アプリケーションの同期エラーが表示されることがあります。このエラーは、スタンバイデバイスのソフトウェアをアップグレードしている間に、アクティブデバイスから変更を展開した場合にのみ発生します。

ステップ 2 スタンバイ装置で [デバイス (Device)] > [高可用性 (High Availability)] をクリックし、ギアメニュー (⚙️) から [モードの切り替え (Switch Mode)] を選択します。

この操作により、強制的にフェールオーバーが行われ、ログインしている装置がアクティブな装置になります。装置のステータスが「アクティブ」に変わるまで待ちます。

続行する前に、必要に応じてネットワークをテストして、デバイスの接続先ネットワークをトラフィックが通過していることを確認できます。

ステップ 3 元々はアクティブな装置だった新しいスタンバイ装置にログインして、アップグレードをインストールします。

このプロセスは前述のプロセスと同じです。ソフトウェアアップグレードは、他の装置からはコピーされないため、アップロードする必要があります。

インストールが完了したら、スタンバイ装置に再度ログインして、インストールが成功したこと、装置が通常のアクティブ/スタンバイ状態に戻っていることを確認します。装置のアクティブステータスは自動的に再開しません。

(注) 高可用性のステータスを確認すれば、アプリケーションの同期エラーが発生することはありません。各装置で同じソフトウェアバージョンが実行されているため、アクティブな装置からの設定のインポートが成功します。自動展開に失敗した場合、またはデバイスがスタンバイ完了状態に移行しない場合は、歯車メニューから [HA の再開 (Resume HA)] をクリックします。

ステップ 4 現在アクティブな装置にログインします。保留中の変更がある場合は、それらの変更を展開し、展開が正常に完了するまで待ちます。

ステップ 5 (オプション) 現在のスタンバイ装置のアクティブ ステータスを再開させる場合は、[デバイス (Device)] > [高可用性 (High Availability)] をクリックして、いずれかの装置のギアメニューから [モードの切り替え (Switch Mode)] を選択します。

たとえば、このプロセスの開始時点ではプライマリ装置がアクティブな装置であり、その状態にする場合はモードを切り替えます。

HA デバイスをアップグレードする際の変更の展開

ハイ アベイラビリティ グループ内のデバイスのシステム ソフトウェアをアップグレードするプロセスの間は、ある時点において、スタンバイ デバイスでアクティブ デバイスより新しいソフトウェアバージョンが実行されています。通常は、この時点でモードを切り替え、スタンバイ デバイスをアクティブ デバイスにしてから、2 番目のデバイスをアップグレードします。

ただし、こうしたアップグレード途中の状態ではアクティブ デバイスの設定を変更する必要がある場合は、次の手順を実行して変更を展開できるようにする必要があります。

手順

ステップ 1 スタンバイ デバイス (新しいソフトウェア バージョンを実行しているデバイス) で、[ハイアベイラビリティ (High Availability)] ページの歯車メニュー (⚙️) から [HA の中断 (Suspend HA)] を選択します。

ステップ 2 アクティブ デバイスで、変更を展開します。展開が正常に完了するまで待機します。

ステップ 3 中断したスタンバイ デバイスで、[ハイアベイラビリティ (High Availability)] ページの歯車メニュー (⚙️) から [HA の再開 (Resume HA)] を選択します。デバイスがアクティブ デバイスから自身の設定を同期し、最新の変更を取得します。

ステップ 4 再開したスタンバイ デバイスで、[ハイアベイラビリティ (High Availability)] ページの歯車メニュー (⚙️) から [スイッチモード (Switch Mode)] を選択します。これで、スタンバイ デバイスがアクティブ デバイスになり、アップグレードを進めることができます。[HA デバイスでのソフトウェア アップグレードのインストール \(251 ページ\)](#) を参照してください。

ハイ アベイラビリティ ペアでの装置交換

必要に応じて、ネットワーク トラフィックを中断することなくハイ アベイラビリティ グループ内の装置を交換できます。

手順

- ステップ 1** 交換する装置が機能している場合は、ピア装置にフェールオーバーするようにし、デバイス CLI の **shutdown** コマンドを使用して、デバイスをグレースフルシャットダウンします。装置が機能していない場合は、ピアがアクティブモードで動作していることを確認します。
- 管理者権限を持っている場合は、FDM CLI コンソールから **shutdown** コマンドを入力することもできます。
- ステップ 2** 装置をネットワークから取り除きます。
- ステップ 3** 交換装置を設置して、インターフェイスを再接続します。
- ステップ 4** 交換装置でデバイスセットアップウィザードを完了します。
- ステップ 5** ピア装置で[ハイアベイラビリティ (High Availability)] ページにアクセスし、設定をクリップボードにコピーします。装置がプライマリ装置か、セカンダリ装置かに注意してください。
- 保留中の変更がある場合は、それらの変更を展開し、展開が完了するまで待ってから続行します。
- ステップ 6** 交換装置で[ハイアベイラビリティ (High Availability)] グループで[設定 (Configure)] をクリックして、ピアから反対側の装置タイプを選択します。つまり、ピアがプライマリの場合は[セカンダリ (Secondary)] を選択し、ピアがセカンダリの場合は[プライマリ (Primary)] を選択します。
- ステップ 7** ピアから HA の設定を貼り付け、IPsec キーを入力します (使用する場合)。[HAの有効化 (Activate HA)] をクリックします。
- 展開が完了すると、装置はピアに連絡して HA グループに参加します。アクティブなピアの設定がインポートされ、選択内容に基づいて、交換装置がグループ内のプライマリ装置またはセカンダリ装置になります。これで、HA が正常に動作していることを確認し、必要に応じてモードを切り替えて、新しい装置をアクティブな装置にできます。

ハイアベイラビリティのモニタ

ここでは、ハイアベイラビリティをモニタする方法について説明します。

イベントビューアとダッシュボードには、ログインしているデバイスに関するデータだけが表示されることに注意してください。両方のデバイスの統合された情報は表示されません。

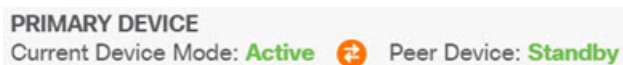
フェールオーバーの全般的なステータスと履歴のモニタリング

次の方法で、高可用性の全般的なステータスと履歴をモニタできます。

- [デバイス概要 (Device Summary)] ([デバイス (Device)] をクリック) の [ハイアベイラビリティ (High Availability)] グループに装置のステータスが表示されます。



- [ハイアベイラビリティ (High Availability)] ページ ([デバイス (Device)] > [ハイアベイラビリティ (High Availability)] をクリック) に両方の装置のステータスが表示されます。それらの間にある同期のアイコンをクリックすると、追加のステータスが表示されます。



- [ハイアベイラビリティ (High Availability)] ページで、ステータスの横にある [フェールオーバー履歴 (Failover History)] リンクをクリックします。CLI コンソールが開き、**show failover history details** コマンドが実行されます。このコマンドを CLI または CLI コンソールに直接入力することもできます。

CLI コマンド

CLI または CLI コンソールで次のコマンドを使用できます。

- **show failover**

装置のフェールオーバー状態についての情報を表示します。

- **show failover history [details]**

過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。**details** キーワードを追加すると、ピア装置のフェールオーバー履歴が表示されます。この情報は、トラブルシューティングに役立ちます。

- **show failover state**

両方の装置のフェールオーバー状態が表示されます。この情報には、装置のプライマリまたはセカンダリステータス、装置のアクティブ/スタンバイステータス、最後にレポートされたフェールオーバーの理由などが含まれます。

- **show failover statistics**

フェールオーバーインターフェイスの送信 (tx) パケット数と受信 (rx) パケット数が表示されます。たとえば、装置がパケットを送信しているのに受信パケットがないことが出力に示されている場合は、リンクに問題があります。ケーブルに問題がある、ピアで正しくない IP アドレスが設定されている、装置によってフェールオーバー インターフェイスが異なるサブネットに接続されているといった可能性があります。

```
> show failover statistics
    tx:320875
    rx:0
```

- **show failover interface**

フェールオーバーおよびステートフル フェールオーバー リンクの設定が表示されます。次に例を示します。

```
> show failover interface
interface failover-link GigabitEthernet1/3
  System IP Address: 192.168.10.1 255.255.255.0
  My IP Address      : 192.168.10.1
  Other IP Address   : 192.168.10.2
interface stateful-failover-link GigabitEthernet1/4
  System IP Address: 192.168.11.1 255.255.255.0
  My IP Address      : 192.168.11.1
  Other IP Address   : 192.168.11.2
```

• show monitor-interface

ハイアベイラビリティに関してモニタされているインターフェイスに関する情報が表示されます。詳細については、[HA モニタ対象インターフェイスのステータスのモニタリング \(257 ページ\)](#) を参照してください。

• show running-config failover

実行コンフィギュレーション内のフェールオーバーコマンドを表示します。これらは、ハイアベイラビリティを設定するコマンドです。

HA モニタ対象インターフェイスのステータスのモニタリング

いずれかのインターフェイスの HA モニタリングを有効にしている場合は、CLI または CLI コンソールで **show monitor-interface** コマンドを使用して、モニタ対象インターフェイスのステータスを確認できます。

```
> show monitor-interface
This host: Primary - Active
Interface inside (192.168.1.13): Normal (Monitored)
Interface outside (192.168.2.13): Normal (Monitored)
Other host: Secondary - Standby Ready
Interface inside (192.168.1.14): Normal (Monitored)
Interface outside (192.168.2.14): Normal (Monitored)
```

モニタ対象のインターフェイスには、次のステータスがあります。

- (Waiting) (Unknown (Waiting) などのように他のステータスと結合) : インターフェイスはピア装置上の対応するインターフェイスから hello パケットをまだ受信していません。
- Unknown : 初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合があります。
- Normal : インターフェイスはトラフィックを受信しています。
- Testing : ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down : インターフェイスまたは VLAN は管理上ダウンしています。

- No Link : インターフェイスの物理リンクがダウンしています。
- Failed : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

HA 関連の Syslog メッセージのモニタリング

システムは、深刻な状況を表すプライオリティレベル2のフェールオーバーについて、複数の Syslog メッセージを発行します。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです : 101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。Syslogメッセージの説明については、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.htmlにある『Cisco Firepower Threat Defense Syslog Messages』を参照してください。



- (注) フェールオーバー時には、システムが論理的にシャットダウンされた後にインターフェイスが起動し、Syslog メッセージ 411001 および 411002 が生成されます。これは通常のアクティビティです。

Syslog メッセージを表示するには、[デバイス (Device)] > [ロギング設定 (Logging Settings)] で診断ロギングを設定する必要があります。メッセージを確実にモニタできるように、外部 Syslog サーバを設定してください。

ピア装置での CLI コマンドのリモート実行

CLI から failover exec コマンドを使用することにより、ピアにログインすることなく、ピアデバイスに show コマンドを入力できます。

failover exec {active | standby | mate} コマンド

コマンドを実行する装置 (active または standby のどちらか) を指定するか、「ログインしている装置ではない方の装置が応答する」ことを指定する **mate** を入力します。

たとえば、ピアのインターフェイス設定と統計情報を表示するには、次のように入力します。

```
> failover exec mate show interface
```

configure コマンドを入力することはできません。この機能は **show** コマンドと一緒に使用しません。



- (注) アクティブ装置にログインしている場合は、**failover reload-standby** コマンドを使用してスタンバイ装置をリロードできます。

これらのコマンドは、Firepower Device Manager CLI コンソールからは入力できません。

ハイアベイラビリティ（フェールオーバー）のトラブルシューティング

ハイアベイラビリティグループ内の装置が期待どおりに機能していない場合は、次の手順による設定のトラブルシューティングを検討します。

アクティブな装置にピア装置が「障害 (Failed)」と表示されている場合は、[装置の障害状態のトラブルシューティング \(261 ページ\)](#) を参照してください。

手順

ステップ 1 各デバイス（プライマリとセカンダリ）から次の手順を実行します。

- フェールオーバーリンクの他方のデバイスの IP アドレスに ping を実行します。
- 別のリンクを使用する場合は、ステートフルフェールオーバーリンクの他方のデバイスの IP アドレスに ping を実行します。

ping が失敗する場合は、各デバイス上のインターフェイスが同じネットワークセグメントに接続されていることを確認します。直接ケーブル接続を使用している場合は、ケーブルを確認します。

ステップ 2 次の一般的なチェックを行います。

- プライマリとセカンダリで重複している管理 IP アドレスを確認します。
- 装置の重複しているフェールオーバー IP アドレスとステートフルフェールオーバー IP アドレスを確認します。
- 各デバイスの同等のインターフェイスポートが同じネットワークセグメントに接続されていることを確認します。

ステップ 3 スタンバイデバイスのタスクリストまたは監査ログを確認します。アクティブなデバイスで展開が成功するごとに、「アクティブノードからの設定のインポート (Configuration import from Active node)」タスクの成功を確認する必要があります。タスクが失敗する場合は、フェールオーバーリンクを確認して、展開を再度実行してください。

(注) 展開タスクの失敗がタスクリストに示されている場合は、展開ジョブ中にフェールオーバーが発生した可能性があります。展開タスクを開始した時点でスタンバイデバイスがアクティブユニットだったものの、タスク中にフェールオーバーが発生した場合には、展開は失敗します。この問題を解決するには、モードを切り替えて再度スタンバイユニットをアクティブユニットに設定してから、設定の変更を再展開します。

ステップ 4 show failover history コマンドを使用して、デバイスの状態変更に関する詳細情報を取得します。

以下の点を確認します。

- アプリケーションの同期エラー。

```
12:41:24 UTC Dec 6 2017
```

```
App Sync      Disabled      HA state progression failed due to APP SYNC timeout
```

アプリケーションの同期フェーズは、アクティブデバイスの設定がスタンバイデバイスに転送されるフェーズです。アプリケーションの同期エラーが発生するとデバイスは無効状態になり、そのデバイスをアクティブにすることはできなくなります。

アプリケーションの同期の問題により、デバイスが無効状態になっている場合は、フェールオーバーリンクとステートフルフェールオーバーリンクのエンドポイント用に、デバイスの別のインターフェイスを使用することができます。リンクの各端には同じポート番号を使用する必要があります。

show failover コマンドの結果、セカンダリデバイスが疑似スタンバイ状態にあると表示される場合は、セカンダリデバイスのフェールオーバーリンクに、プライマリデバイスに設定したアドレスとは異なる IP アドレスを設定している可能性があります。フェールオーバーリンクの両方のデバイスで同じプライマリ/セカンダリ IP アドレスを使用していることを確認します。

疑似スタンバイ状態は、プライマリとセカンダリで異なる IPsec キーが設定されている可能性も示しています。

その他のアプリケーションの同期の問題については、[HA アプリケーション同期障害のトラブルシューティング \(262 ページ\)](#) を参照してください。

- (アクティブからスタンバイに移行して戻る) フェールオーバーの頻度が異常に高い場合、フェールオーバーリンクに問題がある可能性があります。最悪のシナリオでは、両方の装置がアクティブになり、トラフィックの通過が中断されます。リンクの各端に ping を実行して接続を確認します。**show arp** を使用して、フェールオーバー IP アドレスと ARP マッピングが適切であるか確認することもできます。

フェールオーバーリンクが正常で正しく設定されている場合は、ピアのポーリング時間とホールド時間、インターフェイスのポーリング時間とホールド時間を増やすか、HA の監視対象インターフェイスの数を減らすか、インターフェイスのしきい値を増やすことを検討してください。

- インターフェイスチェックが原因のエラー。[インターフェイスチェック (Interface Check)] 理由には、障害が発生したと見なされるインターフェイスの一覧が含まれています。それらのインターフェイスをチェックして、正しく設定されていること、ハードウェアの問題がないことを確認します。リンクの反対側のスイッチの設定に問題がないことを確認します。問題がない場合は、それらのインターフェイスに対する HA モニタリングの無効化を検討します。または、インターフェイス障害のしきい値やタイミングを増やすこともできます。

```
06:17:51 UTC Jan 15 2017

Active    Failed    Interface check

          This Host:3

              admin: inside

              ctx-1: ctx1-1

              ctx-2: ctx2-1

          Other Host:0
```

- ステップ 5** スタンバイ装置を検出できず、フェールオーバーリンクの LAN またはケーブル接続の不良など、具体的な理由を見つけられない場合は、次の手順を実行します。
- スタンバイ装置で CLI にログインし、**failover reset** コマンドを入力します。このコマンドにより、装置の状態が「障害」から「非障害」に変わります。次に、アクティブデバイスの HA ステータスを確認します。スタンバイピアが検出される場合は、これで終了です。
 - アクティブな装置で CLI にログインし、**failover reset** コマンドを入力します。アクティブとスタンバイの両方の装置で HA ステータスがリセットされます。デバイス間のリンクが再確立されるのが理想的です。HA のステータスを確認します。正しくない場合は手順を続行します。
 - アクティブデバイスの CLI から、または Firepower Device Manager から、まず HA を中断してから HA を再開します。CLI コマンドは **configure high-availability suspend** と **configure high-availability resume** です。
 - これらの手順が失敗する場合は、スタンバイ デバイスを **reboot** します。

装置の障害状態のトラブルシューティング

ピア装置のハイ アベイラビリティ ステータス ([デバイス (Device)] または [デバイス (Device)] > [ハイアベイラビリティ (High Availability)] ページ) で装置が故障としてマークされている場合、アクティブ装置である装置 A と故障したピアである装置 B に基づいて、考えられる一般的な原因は次のとおりです

- 装置 B がハイアベイラビリティ向けに設定されていない場合 (スタンドアロンモードのままになっている場合)、装置 A は装置 B を故障として表示します。
- 装置 B で HA を一時停止すると、装置 A は装置 B を故障として表示します。
- 装置 B をリブートすると、装置 B がリブートを完了してフェールオーバーリンク経由で通信を再開するまで装置 A は装置 B を故障として表示します。
- 装置 B でアプリケーションの同期 (App Sync) が失敗すると、装置 A は装置 B を故障として表示します。[HA アプリケーション同期障害のトラブルシューティング \(262 ページ\)](#) を参照してください。

- 装置 B で装置またはインターフェイスのヘルスマonitoringが失敗すると、装置 A は装置 B を故障として表示します。システム上の問題がないか装置 B を確認します。デバイスをリブートしてみます。装置がおおむね正常な場合は、装置またはインターフェイスのヘルスマonitoring設定を緩和することを検討します。**show failover history** の出力にインターフェイスヘルスマonitoringの障害に関する情報が示されます。
- 両方の装置がアクティブな場合、各装置はピアを故障として表示します。通常、これはフェールオーバーリンクに問題があることを示しています。

ライセンスの問題を示す場合もあります。デバイスには、両方評価モードである、または両方登録済みの一貫性のあるライセンスが必要です。登録されている場合、使用するスマートライセンスアカウントは別々であっても構いませんが、どちらのアカウントも輸出制限対象の機能で有効または無効のいずれか同じものを選択している必要があります。輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワークセグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置で HA を手動で中断する必要があります。

HA アプリケーション同期障害のトラブルシューティング

ピア装置が HA グループへの参加に失敗する場合、またはアクティブ装置からの変更を展開しているときにピア装置で障害が発生する場合は、障害が発生した装置にログインして [ハイアベイラビリティ (High Availability)] ページに移動し、[フェールオーバー履歴 (Failover History)] リンクをクリックします。**show failover history** 出力にアプリケーション同期の障害が示されている場合、装置がハイアベイラビリティグループとして正しく機能できることをシステムが確認する、HA の検証段階に問題があります。

このタイプの障害は、次のように表示されます。

```

=====
From State          To State          Reason
=====
16:19:34 UTC May 9 2018
Not Detected       Disabled          No Error

17:08:25 UTC May 9 2018
Disabled           Negotiation       Set by the config command

17:09:10 UTC May 9 2018
Negotiation        Cold Standby      Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby       App Sync          Detected an Active mate

17:13:07 UTC May 9 2018
App Sync           Disabled          CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node

```

理想としては、From State が App Sync のときに「All validation passed」というメッセージが表示され、ノードが Standby Ready 状態になります。任意の検証で障害が発生すると、ピアは

Disabled (Failed) 状態になります。問題を解決して、ピアがハイ アベイラビリティ グループとして再度機能するようになる必要があります。アクティブ装置に変更を加えてアプリケーションの同期エラーを修正した場合は、ピア ノードを結合するために、それらを展開して HA を再開する必要があります。

次のメッセージは障害の発生を示しており、問題の解決方法について説明しています。これらのエラーは、ノードの結合と以降の各展開で発生する可能性があります。ノードの結合中は、システムにより、アクティブ装置で最後に展開された設定に対してチェックが実行されます。

- 「ライセンス登録モードがプライマリ ノードとセカンダリ ノードで一致していません。
(License registration mode mismatch between Primary and Secondary Node.)」

ライセンスエラーは、1つのピアが評価モードになっているときにもう一方のピアが登録されたことを示します。ピアを HA グループに参加させるには、ピアを両方とも登録するか、両方とも評価モードにする必要があります。登録したデバイスを評価モードに戻すことはできないため、**[デバイス (Device)] > [スマートライセンス (Smart License)]** ページからもう一方のピアを登録する必要があります。

登録するデバイスがアクティブ装置の場合、デバイスの登録後に展開を実行します。展開することで装置は強制的に更新され、設定が同期されます。これにより、セカンダリ装置はハイ アベイラビリティ グループに正しく参加できます。

- 「ライセンス エクスポート コンプライアンスがプライマリ ノードとセカンダリ ノードで一致していません。
(License export compliance mismatch between Primary and Secondary Node.)」

ライセンス コンプライアンス エラーは、デバイスが異なる Cisco Smart Software Manager アカウントに登録されており、1つのアカウントでは輸出規制された機能が有効で、もう一方のアカウントでは無効になっていることを示します。デバイスは、輸出規制された機能の設定（有効または無効）が同じアカウントに登録される必要があります。**[デバイス (Device)] > [スマートライセンス (Smart License)]** ページでデバイス登録を変更します。

- 「ソフトウェアバージョンがプライマリ ノードとセカンダリ ノードで一致していません。
(Software version mismatch between Primary and Secondary Node.)」

ソフトウェア不一致エラーは、ピアが異なるバージョンの Firepower Threat Defense ソフトウェアを実行していることを示します。一度に1台のデバイスにソフトウェアアップグレードをインストールしている場合、システムは一時的にのみ不一致を許容します。ただし、ピアのアップグレードの間に設定変更を展開することはできません。この問題を解決するには、ピアをアップグレードしてから展開をやり直します。

- 「物理インターフェイスがプライマリ ノードとセカンダリ ノードで一致していません。
(Physical interfaces mismatch between Primary and Secondary Node.)」

HA グループのスタンバイ装置には、アクティブ装置に存在するすべての物理インターフェイスを持たせる必要があります、それらのインターフェイスには同じハードウェア名とタイプ (GigabitEthernet1/1 など) を持たせる必要があります。このエラーは、アクティブ装置に存在する一部のインターフェイスがスタンバイ装置に存在しないことを示しています。スタンバイ装置にはアクティブ装置よりも多くのインターフェイスを含めることができま

す。そのため、アクティブにする装置を切り替えるか、または別のピア装置を選択してください。ただし、インターフェイスの不一致状態は一時的にする必要があります。たとえば、ある装置でインターフェイスモジュールを交換していて、そのモジュールを使用せずに短時間装置を実行する必要がある場合などです。通常の動作では、両方の装置についてインターフェイスの数とタイプが同じである必要があります。

- 「フェールオーバー リンク インターフェイスがプライマリ ノードとセカンダリ ノードで一致していません。（Failover link interface mismatch between Primary and Secondary Node.）」

各装置でフェールオーバー物理インターフェイスをネットワークにリンクする場合、同じ物理インターフェイスを選択する必要があります。たとえば、各装置で GigabitEthernet1/8 にします。このエラーは、異なるインターフェイスを使用したことを示しています。エラーを解決するには、ピア装置のケーブル配線を修正します。

- 「ステートフルフェールオーバー リンク インターフェイスが、プライマリ ノードとセカンダリ ノードで一致していません。（Stateful failover link interface mismatch between Primary and Secondary Node.）」

別々のステートフルフェールオーバー リンクを使用する場合、各装置でステートフルフェールオーバー インターフェイスをネットワークにリンクするときに、同じ物理インターフェイスを選択する必要があります。たとえば、各装置で GigabitEthernet1/7 にします。このエラーは、異なるインターフェイスを使用したことを示しています。エラーを解決するには、ピア装置のケーブル配線を修正します。

- 「フェールオーバー/ステートフルフェールオーバー リンク EtherChannel のメンバー インターフェイスが、プライマリ ノードとセカンダリ ノードで一致していません（Failover/Stateful failover link EtherChannel's member interfaces mismatch between Primary and Secondary Node）」

EtherChannel インターフェイスをフェールオーバーインターフェイスまたはステートフルフェールオーバー インターフェイスのいずれかとして選択した場合、Etherchannel には各デバイスで同じ ID とメンバー インターフェイスを持たせる必要があります。このエラーメッセージは、不一致を生じているのがフェールオーバー リンクなのかステートフルフェールオーバー リンクなのかを示します。エラーを解決するには、EtherChannel インターフェイスの設定を修正して、同じ ID を使用し、各デバイスに同じインターフェイスを含めます。

- 「デバイスのモデル番号がプライマリ ノードとセカンダリ ノードで一致していません。（Device Model Number mismatch between Primary and Secondary Node.）」

HA グループに参加するピアは、まったく同じモデルのデバイスである必要があります。このエラーは、ピアが同じデバイスモデルではないことを示しています。異なるピアを選択して HA を設定する必要があります。

- アクティブ ノードとスタンバイ ノードを同じシャーシ上に配置することはできません。

同じハードウェア シャーシ上でホストされているデバイスを使用してハイ アベイラビリティを設定することはできません。同じシャーシ上の複数のデバイスをサポートしているモデルでハイアベイラビリティを設定する場合は、個別のハードウェア上に存在するデバイスを選択する必要があります。

- 「不明なエラーが発生しました。もう一度お試しください。（Unknown error occurred, please try again.）」

アプリケーションの同期中に問題が発生しましたが、システムが問題を特定できませんでした。もう一度設定を展開してみてください。

- 「ルールパッケージが破損しています。ルールパッケージを更新して、もう一度試してください。（Rule package is corrupted. Please update the rule package and try again.）」

侵入ルールデータベースに問題があります。障害が発生したピアで、**[デバイス (Device)] > [更新 (Updates)]** に移動して、**[ルール (Rule)]** グループの **[今すぐ更新 (Update Now)]** をクリックします。更新が完了するのを待って、変更を展開します。アクティブ装置から展開を再試行できます。

- 「Cisco Success Network はアクティブで有効ですが、スタンバイでは有効になりません。（Cisco Success Network is enabled on Active but not Standby.）」

評価モードのデバイス向けに HA を設定する場合、ピア装置の Cisco Success Network 参加について同じオプションを選択する必要があります。このエラーを解決するには、**[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)]** に移動して、**[Cisco Success Network]** を有効にします。

- 「Cisco Defense Orchestrator はアクティブで有効ですが、スタンバイでは有効になりません。（Cisco Defense Orchestrator is enabled on Active but not Standby.）」

評価モードのデバイス向けに HA を設定する場合、ピア装置の Cisco Defense Orchestrator について同じオプションを選択する必要があります。両方とも登録するか、両方とも登録しない必要があります。このエラーを解決するには、**[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)]** に移動して、**[Cisco Defense Orchestrator]** グループのデバイスを登録します。

- 「Cisco Threat Response が、アクティブでは有効ですが、スタンバイでは有効になっていません。（Cisco Threat Response is enabled on Active but not Standby.）」

HA を設定する場合は、ピアユニットで同じ Cisco Threat Response のオプションを選択する必要があります。このエラーを解決するには、**[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)]** に移動して、**[Cisco Threat Response]** の **[Cisco Cloud にイベントを送信 (Send Events to the Cisco Cloud)]** を有効にします。

- アクティブ ノードとスタンバイ ノードとで異なるクラウドリージョンを設定することはできません。

デバイスが異なるシスコクラウドサービスリージョンに登録されています。どのリージョンが正しいかを確認し、スマートライセンスから他のデバイスの登録を解除し、再登録時に正しいリージョンを選択してください。両方のデバイスのリージョンが正しくない場合は、両方のデバイスの登録を解除し、正しいリージョンで再登録してください。

- 「展開パッケージが破損しています。（Deployment package is corrupted.）再度実行してください。（Please try again.）」

これはシステムエラーです。展開をもう一度試して、この問題を解決する必要があります。



第 11 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 \(267 ページ\)](#)
- [インターフェイスに関する注意事項と制限事項 \(272 ページ\)](#)
- [物理インターフェイスの設定 \(274 ページ\)](#)
- [ブリッジグループの設定 \(279 ページ\)](#)
- [EtherChannel の設定 \(284 ページ\)](#)
- [VLAN インターフェイスおよびスイッチポートの設定 \(Firepower 1010\) \(294 ページ\)](#)
- [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(308 ページ\)](#)
- [パッシブインターフェイスの設定 \(313 ページ\)](#)
- [高度なインターフェイス オプションの設定 \(318 ページ\)](#)
- [インターフェイスの変更のスキャンとインターフェイスの移行 \(323 ページ\)](#)
- [ISA 3000 のハードウェア バイパスの設定 \(329 ページ\)](#)
- [モニタリングインターフェイス \(332 ページ\)](#)
- [インターフェイスの例 \(333 ページ\)](#)

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。パッシブインターフェイスでは IP アドレスを設定しません。

[インターフェイス (Interface)] ページには、インターフェイスタイプに関する次のサブページが含まれています。[インターフェイス (Interfaces)] (物理インターフェイスの場合)、[ブリッジグループ (Bridge Groups)]、[EtherChannel (EtherChannels)]、および[VLAN (VLANs)] (Firepower 1010 の場合)。Firepower 4100/9300 EtherChannel は、[EtherChannel] ページではなく [インターフェイス (Interfaces)] ページに表示されます。これは、EtherChannel パラメータは、FDMではなくFXOSでのみ変更できるためです。各ページには、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、モード、および状態が表示されます。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、EtherChannel、またはVLAN 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。これらのインターフェイスは適切なリストにも表示されます。サポートされている親インターフェイスのサブインターフェイスを表示することもできます。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 \(26 ページ\)](#) 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

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。

パッシブ

パッシブインターフェイスは、スイッチSPAN (スイッチドポートアナライザ) またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニタします。SPANまたはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション (トラフィックのブロッキングやシェーピングなど) を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

スイッチポート (Firepower 1010)

ハードウェアのスイッチ機能を使用するレイヤ2のスイッチポート転送トラフィック。同じVLAN上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、FTDセキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数のVLANに属することができます。管理インターフェイスをスイッチポートとして設定することはできません。

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 \(688 ページ\)](#) 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。

各ゾーンは、ルーテッドまたはパッシブのいずれかのモードになっています。これはインターフェイスのモードに直接関係します。ルーテッドインターフェイスとパッシブインターフェイスは、同じモードのセキュリティゾーンにのみ追加できます。

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::<56 (from=fd00:: to=fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
 - 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::<8)
 - リンクローカル アドレス (fe80::<10)

- 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 インターフェイスの設定は可能ですが、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。
- 冗長インターフェイスは設定できません。
- FDM の Etherchannel は、Firepower 1000 および 2100 シリーズでのみ追加できます。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス (Interfaces)] ページに表示されます。
- 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。

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 1010	60
Firepower 1120	512
Firepower 1140、1150	1024
Firepower 2100	1024
Firepower 4100	1024
Firepower 9300	1024
Firepower Threat Defense Virtual	50
ASA 5508-X	50
ASA 5516-X	100

モデル	VLAN サブインターフェイスの最大数
ASA 5525-X	200
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、パッシブモードインターフェイスを設定している場合、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。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス (Interfaces)] ページに表示され、この手順はこれらの Etherchannel にも適用されます。シャーシ上の FXOS で、Firepower 4100/9300 Etherchannel のすべてのハードウェア設定を実行する必要があります。



(注) 物理インターフェイスを Firepower 1010 スイッチポートとして設定するには、[VLAN インターフェイスおよびスイッチポートの設定 \(Firepower 1010\) \(294 ページ\)](#) を参照してください。

物理インターフェイスをパッシブインターフェイスとして設定するには、[パッシブモードでの物理インターフェイスの設定 \(317 ページ\)](#) を参照してください。

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せん。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 (Interfaces)] 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 (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理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。

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。

高可用性設定でフェールオーバーリンクまたはステートフルフェールオーバーリンクとして使用しているインターフェイスを編集することはできません。

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：EtherChannel に追加するインターフェイスの名前は設定しないでください。


(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) [モード (Mode)] を選択します。

- [ルーテッド (Routed)] : ルーテッドモードインターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォールポリシーなど、すべてのファイアウォール機能の管理下に置かれます。これが通常のインターフェイスモードです。

- **[パッシブ (Passive)]** : パッシブ インターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワーク中のトラフィック フローをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション (トラフィックのブロッキングやシェーピングなど) を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、[パッシブモードでの物理インターフェイスの設定 \(317 ページ\)](#) を参照してください。パッシブのインターフェイスで IP アドレスを設定することはできません。
- **スイッチ ポート** : (Firepower 1010) スイッチポートにより、同じ VLAN 上でのポート間のハードウェアスイッチングが可能になります。スイッチングされたトラフィックはセキュリティポリシーの対象にはなりません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、次に参照してください。[VLAN インターフェイスおよびスイッチポートの設定 \(Firepower 1010\) \(294 ページ\)](#)

後でこのインターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

- c) **[ステータス (Status)]** スライダを [有効 (enabled)] 設定 () に設定します。

Firepower 4100/9300 デバイス上のインターフェイスの場合は、FXOS でもインターフェイスを有効にする必要があります。

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 トランキングの設定 \(308 ページ\)](#) に進みます。保存しない場合は、次に進みます。

(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。

- d) (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。ハイアベイラビリティを設定する場合、このオプションは使用できません。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。

高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットのネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。

(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 (696 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 ステータス自動設定では、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 \(271 ページ\)](#) 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。

- [スタンバイ IP アドレス (Standby IP Address)] : 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイアドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。
- [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 (320 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 \(159 ページ\)](#) 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。
- EtherChannelはブリッジグループメンバーとしてサポートされません。Firepower 4100/9300上のEtherchannelは、ブリッジグループメンバーにすることができます。
- 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。
- Firepower 1010では、同じブリッジグループ内に論理VLANインターフェイスと物理ファイアウォールインターフェイスを混在させることはできません。
- ISA 3000は、ブリッジグループBVIIを使用して事前に設定されています（名前は付けられていません。これは、ルーティングに参加しないことを意味します）。BVIIにはすべてのデータインターフェイス (GigabitEthernet1/1 (outside1)、GigabitEthernet1/2

(inside1)、GigabitEthernet1/3 (outside2)、GigabitEthernet1/4 (inside2)) が含まれています。ネットワークに合わせて BVII IP アドレスを設定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、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[ブリッジグループ (Bridge Groups)] をクリックします。

ブリッジグループのリストに、既存のブリッジグループが表示されます。各ブリッジグループのメンバーインターフェイスを表示するには、開/閉矢印をクリックします。また、メンバーインターフェイスは [インターフェイス (Interfaces)] または [VLAN (VLANs)] ページでも個別に表示されます。

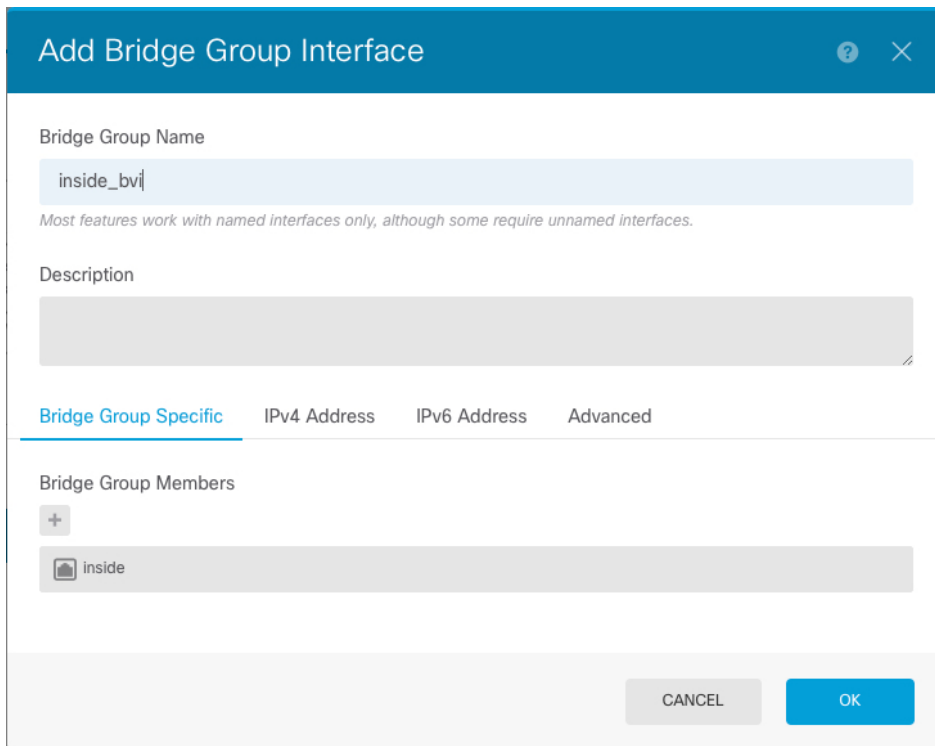
ステップ 2 次のいずれかを実行します。

- BVII ブリッジグループの編集アイコン () をクリックします。
- [ブリッジグループの作成 (Create Bridge Group)] をクリックするか、プラス アイコン () をクリックして、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。



The screenshot shows the 'Add Bridge Group Interface' dialog box. The 'Bridge Group Name' field contains 'inside_bvi'. Below it is a note: 'Most features work with named interfaces only, although some require unnamed interfaces.' The 'Description' field is empty. The 'Bridge Group Members' section has a plus icon and 'inside' listed. At the bottom are 'CANCEL' and 'OK' buttons.

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。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。

高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワークテストを使用してスタンバイインターフェイスをモニタできず、リンクステートをトラックすることしかできません。

- (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 \(696 ページ\)](#) 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。ハイアベイラビリティを設定する場合、このオプションは使用できません。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)]: ステータ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 \(271 ページ\)](#) 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。

- [スタンバイIPアドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。
- [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 (320 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 \(696 ページ\)](#) 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 \(159 ページ\)](#) 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。

EtherChannel の設定

ここでは、EtherChannel とそれらの設定方法について説明します。



- (注) FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャード上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス (Interfaces)] ページに表示されます。

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネットリンク (チャンネルグループ) のバンドルで構成される論理インターフェイスです (ポートチャンネルインターフェイスと呼びます)。ポートチャンネルインターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャンネルグループインターフェイス

各チャンネルグループは、最大 8 個のアクティブインターフェイスを設定できます。

チャンネルグループのインターフェイスはすべて、同じタイプおよび同じ速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

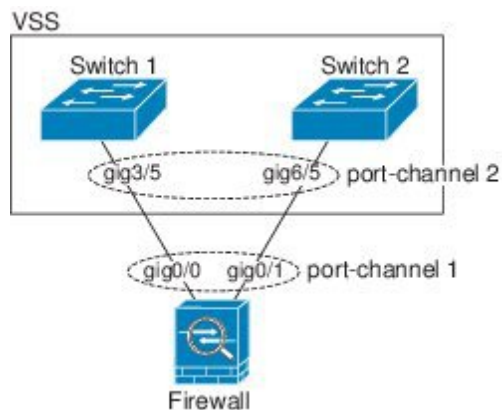
EtherChannelによって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュアルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

FTD EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

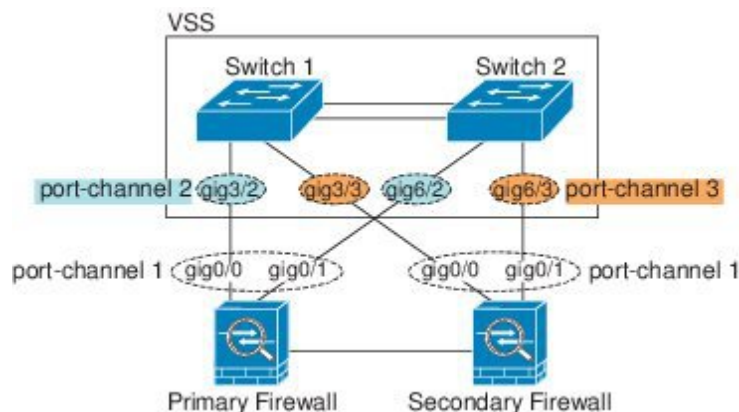
スイッチが仮想スイッチングシステム (VSS) または 仮想ポートチャンネル (vPC) の一部である場合、同じ EtherChannel 内の FTD インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチインターフェイスは同じ EtherChannel ポートチャンネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

図 10: VSS/vPC への接続



FTDをアクティブ/スタンバイフェールオーバー配置で使用する場合、FTDごとに1つ、VSS/vPC内のスイッチで個別のEtherChannelを作成する必要があります。各FTDで、1つのEtherChannelが両方のスイッチに接続します。すべてのスイッチインターフェイスを両方のFTDに接続する単一のEtherChannelにグループ化できる場合でも（この場合、個別のFTDシステムIDのため、EtherChannelは確立されません）、単一のEtherChannelは望ましくありません。これは、トラフィックをスタンバイFTDに送信しないようにするためです。

図 11: アクティブ/スタンバイ フェールオーバーと VSS/vPC



リンク集約制御プロトコル

リンク集約制御プロトコル (LACP) では、2つのネットワーク デバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- **アクティブ** : LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- **オン** : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャンネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャンネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

FTD は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します (この基準は設定可能です)。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。`hash_value mod active_links` の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスへ送信され、以降は結果が 1 となるものは 2 番目のインターフェイスへ、結果が 2 となるものは 3 番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブリンクがある場合、モジュロ演算では 0 ~ 14 の値が得られます。6 個のアクティブリンクの場合、値は 0 ~ 5 となり、以降も同様になります。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ2のスパニングツリーとレイヤ3のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1つのチャンネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannelはネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポートチャンネルインターフェイスは、最も小さいチャンネルグループインターフェイスのMAC アドレスをポート チャンネル MAC アドレスとして使用します。または、ポートチャンネルインターフェイスのMACアドレスを手動で設定することもできます。グループチャンネルインターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを設定することを推奨します。ポート チャンネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャンネルMACアドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

EtherChannel インターフェイスのガイドライン

ブリッジグループ

FDM で定義された EtherChannel はブリッジグループ メンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。

高可用性

- EtherChannel インターフェイスを高可用性 リンクとして使用する場合、高可用性 ペアの両方のユニットでその事前設定を行う必要があります。プライマリユニットで設定し、セカンダリ装置に複製されることは想定できません。これは、複製には高可用性 リンク自体が必要であるためです。
- EtherChannel インターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。Firepower 4100/9300 シャーシでは、Etherchannel を含むすべてのインターフェイスを両方のユニットで事前に設定する必要があります。
- **monitor-interface** コマンドを使用して、高可用性。アクティブなメンバーインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、デバイスレベルの高可用性をモニタしているときには、EtherChannel インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、EtherChannel インターフェイスで障害が発生しているように見えます。
- EtherChannel インターフェイスを高可用性またはステートリンクに対して使用する場合、パケットが順不同にならないように、EtherChannel 内の 1 つのインターフェイスのみが使

用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。高可用性リンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、高可用性を一時的に無効にする必要があります。これにより、高可用性がその期間に発生することはありません。

モデルのサポート

- FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス (Interfaces)] ページに表示されます。
- Etherchannel で Firepower 1010 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

EtherChannel の一般的なガイドライン

- モデルで使用可能なインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャンネルグループは、最大 8 個のアクティブインターフェイスを設定できます。
- チャンネルグループのインターフェイスはすべて、同じタイプおよび同じ速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。
- FTD の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- FTD は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS `vlan dot1Q tag native` コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると FTD はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する FTD では、スイッチスタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、FTD EtherChannel がクロススタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、`stack-mac persistent timer` コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 (無制限) などを設定します。または、15.1(1)S2 など、より安定したスイッチソフトウェアバージョンにアップグレードできます。
- すべての FTD コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。

EtherChannel の追加

EtherChannel を追加して、メンバー インターフェイスを割り当てます。



- (注) FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス (Interfaces)] ページに表示されます。

始める前に

- すべてのメンバーインターフェイスが同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。
- メンバー インターフェイスに名前を付けることはできません。



注意 すでにコンフィギュレーション内でインターフェイスを使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[EtherChannels] をクリックします。
- [EtherChannels] リストに、既存の Etherchannel とそれらの名前、アドレス、状態が表示されます。各 EtherChannel のメンバー インターフェイスを表示するには、開/閉矢印をクリックします。また、メンバー インターフェイスは [インターフェイス (Interfaces)] ページでも個別に表示されます。
- ステップ 2** [EtherChannel の作成 (Create EtherChannel)] をクリックするか (現在の EtherChannel がない場合)、またはプラスアイコン (+) をクリックして [EtherChannel] をクリックし、新しい EtherChannel を作成します。
- ステップ 3** 以下を設定します。

a) [インターフェイス名 (Interface Name)] を設定します。

EtherChannel 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]。

(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) [モード (Mode)] を設定します。

- [ルーテッド (Routed)] : ルーテッドモードインターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォールポリシーなど、すべてのファイアウォール機能の管

理下に置かれます。トラフィックがインターフェイスを経由するようにする場合は、このモードを使用します。これが通常のインターフェイス モードです。

- [パッシブ (Passive)]: パッシブ インターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワーク中のトラフィック フローをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション (トラフィックのブロッキングやシェーピングなど) を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、[パッシブモードでの物理インターフェイスの設定 \(317 ページ\)](#) を参照してください。

c) [EtherChannel ID] を 1 ~ 48 の範囲で設定します (Firepower 1010 の場合は 1 ~ 8) 。

d) [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。

e) (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。

f) [EtherChannelモード (EtherChannel Mode)] を指定します。

- [アクティブ (Active)]: LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- [オン (On)]: EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

g) [EtherChannelメンバー (EtherChannel Member)] を追加します。

EtherChannel には最大 8 つの (名前が付いていない) 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。

- [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。ハイアベイラビリティを設定する場合、このオプションは使用できません。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。

高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットのネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。

(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 (696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 ステータス自動設定では、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 \(271 ページ\)](#) 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。

- [スタンバイ IP アドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。
- [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 (320 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。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

- EtherChannel 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 \(159 ページ\)](#) を参照してください。

VLAN インターフェイスおよびスイッチポートの設定 (Firepower 1010)

各 Firepower 1010 インターフェイスは、通常のファイアウォールインターフェイスとしてまたはレイヤ2 ハードウェア スイッチ ポートとして実行するように設定できます。ここでは、スイッチ モードの有効化と無効化、VLAN インターフェイスの作成、VLAN へのスイッチ ポートの割り当てなど、スイッチポート設定を開始するためのタスクについて説明します。また、この項では、サポート対象のインターフェイスで Power on Ethernet (PoE) をカスタマイズする方法についても説明します。

Firepower 1010 ポートおよびインターフェイスについて

ポートとインターフェイス

Firepower 1010 物理インターフェイスごとに、ファイアウォールインターフェイスまたはスイッチ ポートとしてその動作を設定できます。物理インターフェイスとポートタイプ、およびスイッチ ポートを割り当てる論理 VLAN インターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとしておよび他のインターフェイスでレイヤ3インターフェイスとして統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット 1/1 インターフェイスはファイアウォールインターフェイスとして設定されています。また、これらのインターフェイスを IPS 専用 (パッシブインターフェイス) に設定することもできます。
- 物理スイッチ ポート：ハードウェアのスイッチ機能を使用するレイヤ2のスイッチ ポート転送トラフィック。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。トラフィックには、FTD セキュリティ ポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一の VLAN に割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数の VLAN に属することができます。デフォルトでは、イーサネット 1/2 ~ 1/8

は VLAN 1 のアクセス スイッチ ポートとして設定されています。診断 インターフェイスをスイッチ ポートとして設定することはできません。

- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、冗長インターフェイス、IPS 専用インターフェイス（インラインセットおよびパッシブインターフェイス）、または EtherChannel インターフェイスを作成できないという例外があります。スイッチ ポートが別のネットワークと通信する必要がある場合、FTD は VLAN インターフェイスにセキュリティ ポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループ メンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできません。同じ VLAN 上のスイッチ ポート間のトラフィックに FTD セキュリティ ポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティ ポリシーが適用されるため、特定のセグメント間のレイヤブリッジグループとスイッチ ポートを選択することができます。

Power Over Ethernet

イーサネット 1/7 およびイーサネット 1/8 は Power on Ethernet+ (PoE+) をサポートしています。

Firepower 1010 スイッチ ポートの注意事項と制約事項

高可用性

- 高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の高可用性のネットワーク設定では、両方のユニットのアクティブなスイッチポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1つのスイッチポートを VLAN に配置して、高可用性を正常に使用することができますが、代わりに物理ファイアウォール インターフェイスを使用する設定の方が簡単です。
- ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。

論理 VLAN インターフェイス

- 最大 60 の VLAN インターフェイスを作成できます。
- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID を使用することはできません。
- MAC アドレス：

- すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。 [詳細オプションの設定 \(320 ページ\)](#) を参照してください。

ブリッジグループ

同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLAN インターフェイスおよびスイッチポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- 等コストマルチパス (ECMP) ルーティング
- パッシブインターフェイス
- EtherChannel
- フェールオーバーおよびステート リンク

その他の注意事項と制約事項

- Firepower 1010 には、最大 60 の名前付きインターフェイスを設定できます。
- 診断 インターフェイスをスイッチポートとして設定することはできません。

デフォルト設定

- イーサネット 1/1 はファイアウォール インターフェイスです。
- イーサネット 1/2 ~ 1/8 は、VLAN 1 に割り当てられたスイッチポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

VLAN インターフェイスの設定

ここでは、関連付けられたスイッチポートで使用するための VLAN インターフェイスの設定方法について説明します。最初に、スイッチポートに割り当てる VLAN ごとに VLAN インターフェイスを設定する必要があります。



- (注) 特定の VLAN 上でのスイッチポート間のスイッチングのみを有効にし、VLAN と他の VLAN またはファイアウォールインターフェイス間のルーティングを望まない場合は、VLAN インターフェイス名を空のままにします。この場合は IP アドレスを設定する必要もありません。IP 設定はすべて無視されます。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[VLANs] をクリックします。
- [VLANs] リストに、既存の VLAN インターフェイスが表示されます。各 VLAN に関連付けられているスイッチポートを表示するには、開/閉矢印をクリックします。また、スイッチポートは [インターフェイス (Interfaces)] ページでも個別に表示されます。
- ステップ 2** [VLAN インターフェイスの作成 (Create VLAN Interface)] (現在の VLAN がない場合) またはプラスアイコン (+) をクリックして、新しい VLAN インターフェイスを作成します。
- ステップ 3** 以下を設定します。

Add VLAN Interface

Name: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces.

VLAN ID: Do not forward to this VLAN:

1 - 4090 1 - 4090

Description:

IPv4 Address [!] IPv6 Address Advanced

! If the DHCP server supplies an address on the same network configured statically for another interface, this interface will be disabled. Ensure that there is no overlap between the network addresses on this interface and the other interfaces on the device.

Type:

Route Metric: Obtain Default Route using DHCP

1 - 255

CANCEL OK

- a) [インターフェイス名 (Interface Name)] を設定します。


VLAN 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]。

VLAN と他の VLAN またはファイアウォール インターフェイス間のルーティングを望まない場合は、VLAN インターフェイス名を空のままにします。

(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) [モード (Mode)] は [ルーテッド (Routed)] のままにします。

後でこの VLAN インターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

- c) [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。
d) [VLAN ID] を 1 ~ 4070 の間で設定します。

インターフェイスを保存した後、VLANIDを変更することはできません。ここでのVLAN IDは、使用されるVLAN タグと設定内のインターフェイス ID の両方です。

- e) (任意) [このVLANに転送しない (Do not forward to this VLAN)] フィールドに、この VLAN インターフェイスがトラフィックを開始できない VLAN ID を入力します。

たとえば、1つのVLANをインターネットアクセスの外部に、もう1つを内部ビジネスネットワーク内に、そして3つ目をホームネットワークにそれぞれ割り当てます。自宅のネットワークはビジネスネットワークにアクセスする必要がないので、自宅のVLANで [このインターフェイスから次へのトラフィックをブロックする (Block Traffic From this Interface to)] オプションを使用できます。ビジネスネットワークは自宅のネットワークにアクセスできますが、その反対はできません。

- f) (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。ハイアベイラビリティを設定する場合、このオプションは使用できません。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。

高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場

合、アクティブユニットはネットワークテストを使用してスタンバイインターフェイスをモニタできず、リンクステートをトラックすることしかできません。

(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 (696 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 (271 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。

- [スタンバイIPアドレス (Standby IP Address)] : 高可用性を設定し、このインターフェイスのHAをモニタリングしている場合は、同じサブネット上にスタンバイIPv6アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイIPアドレスを設定しない場合、アクティブユニットはネットワークテストを使用してスタンバイインターフェイスをモニタできず、リンクステータスをトラッキングすることしかできません。
- [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 \(320 ページ\)](#)。

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。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

- VLAN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 \(159 ページ\)](#) を参照してください。

スイッチポートのアクセスポートとしての設定

1つのVLANにスイッチポートを割り当てるには、アクセスポートとして設定します。デフォルトでは、Ethernet1/2 ~ 1/8のスイッチポートが有効になっていて、VLAN 1に割り当てられています。



- (注) Firepower 1010 では、ネットワーク内のループ検出のためのスパニングツリープロトコルはサポートされません。したがって、FTD とのすべての接続がネットワークループに陥らないようにする必要があります。

始める前に

アクセスポートを割り当てる VLAN ID の VLAN インターフェイスを追加します。アクセスポートは、タグなしのトラフィックのみを受け入れます。[VLAN インターフェイスの設定 \(296 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] 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 (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理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。

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。

Ethernet1/7
Edit Physical Interface

Interface Name: [Empty field]
Mode: Switch Port
Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description: [Empty text area]

IPv4 Address | IPv6 Address | **VLAN** | PoE

Protected Port ⓘ

Usage Type

Access VLAN

Filter [Dropdown menu]
inside (Vlan1) ⓘ

- スイッチポートの[インターフェイス名 (Interface Name)] は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。
- [モード (Mode)] を [スイッチポート (Switch Port)] に設定します。
- [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。
- (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 [VLAN] をクリックし、次のように設定します。

- (任意) このスイッチポートを保護対象として設定するには、[保護ポート (Protected Port)] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

スイッチポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチポートにこのオプションを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

- b) [使用法の種類 (Usage Type)] で、[アクセス (Access)] をクリックします。
- c) [アクセスVLAN (Access VLAN)] の場合は、下矢印をクリックして既存の VLAN インターフェイスのいずれかを選択します。

新しい VLAN インターフェイスを追加するには、[新しい VLAN の作成 (Create new VLAN)] をクリックします。[VLAN インターフェイスの設定 \(296 ページ\)](#) を参照してください。

ステップ 5 [OK] をクリックします。

スイッチポートのトランクポートとしての設定

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランクポートの作成方法について説明します。トランクポートは、タグなしおよびタグ付きのトラフィックを受け入れます。許可された VLAN のトラフィックは、変更されないままトランクポートを通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブの VLAN ID トラフィックを送信するときに、VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランクポートに同じネイティブ VLAN を設定してください。

始める前に

トランクポートを割り当てる VLAN ID ごとに VLAN インターフェイスを追加します。[VLAN インターフェイスの設定 \(296 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] 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 (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理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。

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。

Ethernet1/8
Edit Physical Interface

Interface Name: [] Mode: Switch Port Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description: []

IPv4 Address IPv6 Address **VLAN** PoE

Protected Port ⓘ

Usage Type: Access **Trunk**

Native Trunk VLAN: Please select a VLAN

Associated VLANs: +

Filter: []

- dmz (Vlan100) ⓘ
- inside (Vlan1) ⓘ

Create new VLAN CANCEL OK

CANCEL OK

- スイッチポートの[インターフェイス名 (InterfaceName)]は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。
- [モード (Mode)]を[スイッチポート (Switch Port)]に設定します。
- [ステータス (Status)] スライダを[有効 (enabled)]設定 () に設定します。
- (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 [VLAN] をクリックし、次のように設定します。

- (任意) このスイッチポートを保護対象として設定するには、[保護ポート (Protected Port)] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

スイッチポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイ

スを相互に分離する場合に、スイッチポートが相互に通信しないようにします。たとえば、3つのWebサーバをホストするDMZがある場合、各スイッチポートにこのオプションを適用すると、Webサーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも3つのWebサーバすべてと通信でき、その逆も可能ですが、Webサーバは相互に通信できません。

- b) [使用法の種類 (Usage Type)] で、[トランク (Trunk)] をクリックします。
- c) (任意) [ネイティブトランクVLAN (Native Trunk VLAN)] の場合は、下矢印をクリックしてネイティブVLANの既存のVLANインターフェイスのいずれかを選択します。

デフォルトのネイティブVLAN IDは1です。

各ポートのネイティブVLANは1つのみですが、すべてのポートに同じネイティブVLANまたは異なるネイティブVLANを使用できます。

新しいVLANインターフェイスを追加するには、[新しいVLANの作成 (Create new VLAN)] をクリックします。[VLAN インターフェイスの設定 \(296 ページ\)](#) を参照してください。

- d) [関連付けられているVLAN (Associated VLANs)] で、プラスアイコン (+) をクリックして、1つまたは複数の既存のVLANインターフェイスを選択します。

このフィールドにネイティブVLANを含めても無視されます。トランクポートは、ネイティブVLANトラフィックをポートから送信するときに、常にVLANタグを削除します。また、まだネイティブVLANタグが付いているトラフィックを受信しません。

新しいVLANインターフェイスを追加するには、[新しいVLANの作成 (Create new VLAN)] をクリックします。[VLAN インターフェイスの設定 \(296 ページ\)](#) を参照してください。

ステップ5 [OK] をクリックします。

Power over Ethernet の設定

Ethernet 1/7 および Ethernet 1/8 は、IP 電話や無線アクセスポイントなどのデバイス用に Power over Ethernet (PoE) をサポートしています。Firepower 1010 は、IEEE 802.3af (PoE) と 802.3at (PoE+) の両方をサポートしています。PoE+ は、Link Layer Discovery Protocol (LLDP) を使用して電力レベルをネゴシエートします。PoE+ は、給電先デバイスに最大 30 ワットを供給できます。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。

PoE は、デフォルトで Ethernet 1/7 および Ethernet 1/8 で有効になっています。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する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、[インターフェイス (Interfaces)] 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 (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理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。

ステップ 2 Ethernet 1/7 または 1/8 の編集アイコン (🔗) をクリックします。

ステップ 3 [PoE] をクリックし、次のように設定します。

Ethernet1/8
Edit Physical Interface

Interface Name:
Mode: Switch Port
Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | VLAN | **PoE**

POWER OVER ETHERNET

Consumption Wattage:
4000 - 30000mW

CANCEL OK

a) [POWER OVER ETHERNET] を有効にするには、スライダ (🔗) をクリックして有効にします。

PoE はデフォルトでイネーブルです。

b) (任意) 必要なワット数が正確にわかっている場合は、[消費ワット数 (Consumption Wattage)] を入力します。

デフォルトでは、PoE は給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。Firepower 1010 は LLDP を使用して、適切なワット数をさらにネゴシエートします。具体的なワット数がわかっている、LLDP ネゴシエーションを無効にする場合は、4000 ~ 30000 ミリワットの値を入力します。

ステップ 4 [OK] をクリックします。

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。
- Firepower 1010：サブインターフェイスは、スイッチポートまたは VLAN インターフェイスではサポートされていません。
- 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ら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組み込みの 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的 MAC アドレスを割り当てることもできます。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的 MAC アドレスを割り当てることで、一意的 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 (Interfaces)] 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 (Interfaces)] タブがデフォルトで選択されます。EtherChannel にサブインターフェイスを追加するには、[EtherChannel] をクリックします。インターフェイスリストに、物理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。

ステップ 2 次のいずれかを実行します。

- [インターフェイス (Interfaces)] ページで、プラスアイコン (+) をクリックして、新しいサブインターフェイスを作成します。
- [EtherChannel] ページで、プラスと下矢印のアイコン (+v) をクリックし、[サブインターフェイス (Subinterface)] を選択します。
- 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。

Add Subinterface ? ×

Parent Interface	Subinterface Name	Mode	Status
<input style="width: 90%;" type="text" value="Ethernet1/1"/>	<input style="width: 90%;" type="text" value="engineering"/>	<input style="width: 90%;" type="text" value="Routed"/>	<input checked="" type="checkbox"/>

Most features work with named interfaces only, although some require unnamed interfaces.

Description

VLAN ID	Subinterface ID
<input style="width: 90%;" type="text" value="200"/>	<input style="width: 90%;" type="text" value="200"/>

1 - 4094

IPv4 Address
IPv6 Address
Advanced

Type

IP Address and Subnet Mask
 /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask
 /

e.g. 192.168.5.16

- 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) [モード (Mode)] を [ルーテッド (Routed)] に設定します。

後でこのインターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

- d) (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。

- e) [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。

- f) [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。ハイアベイラビリティを設定する場合、このオプションは使用できません。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。

高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワークテストを使用してスタンバイインターフェイスをモニタできず、リンクステートをトラックすることしかできません。

- (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 \(696 ページ\)](#) 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 \(271 ページ\)](#) 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。

- [スタンバイIPアドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスのHAをモニタリングしている場合は、同じサブネット上にスタンバイIPv6アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイIPアドレスを設定しない場合、アクティブユニットはネットワークテストを使用してスタンバイインターフェイスをモニタできず、リンクステータスをトラッキングすることしかできません。
- [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 \(320 ページ\)](#)。

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 \(159 ページ\)](#) を参照してください。

パッシブインターフェイスの設定

パッシブインターフェイスは、スイッチSPAN (スイッチドポートアナライザ) またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能によ

り、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。

パッシブ展開で設定されたシステムでは、特定のアクション（トラフィックのブロッキングなど）を実行できません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

パッシブインターフェイスを使用して、ネットワーク上のトラフィックをモニタし、トラフィックに関する情報を収集します。たとえば、侵入ポリシーを適用して、ネットワークを攻撃する脅威のタイプを特定したり、ユーザが作成している Web 要求の URL カテゴリを確認できます。さまざまなセキュリティポリシーおよびルールを実装して、アクティブに展開されたシステムの動作を確認し、アクセス制御やその他のルールに基づいてトラフィックをドロップできます。

ただし、パッシブインターフェイスはトラフィックに影響を与えることができないため、多数の設定上の制限が存在します。これらのインターフェイスは、システムがトラフィックをピークすることを可能にするだけです。パッシブインターフェイスに入るパケットがデバイスを出ることはありません。

ここでは、パッシブインターフェイスとそれらの設定方法について説明します。

パッシブインターフェイスを使用する理由

パッシブインターフェイスの主な目的は、単純なデモンストレーションモードを提供することです。単一の送信元ポートをモニタするようにスイッチをセットアップし、ワークステーションを使用して、パッシブインターフェイスでモニタしたテストトラフィックを送信できます。これにより、Firepower Threat Defense システムが接続を評価したり脅威を特定したりする方法を確認できます。システムの実行方法に問題がなければ、その方法をネットワーク内にアクティブに展開して、パッシブインターフェイスの設定を削除できます。

ただし、次のサービスを提供するために実稼働環境でパッシブインターフェイスを使用することもできます。

- **純粋な IDS 展開**：システムをファイアウォールまたは IPS（侵入防御システム）として使用しない場合、IDS（侵入検知システム）としてパッシブに展開できます。この展開方法では、アクセス制御ルールを使用してすべてのトラフィックに侵入ポリシーを適用します。また、システムでスイッチ上の複数の送信元ポートもモニタします。さらに、ダッシュボードを使用してネットワークで見られる脅威をモニタできます。ただし、このモードでは、この脅威を防ぐためにできることはありません。
- **混合展開**：アクティブルーテッドインターフェイスとパッシブインターフェイスを同じシステム上に混在させることができます。これにより、Firepower Threat Defense デバイスをいくつかのネットワークでファイアウォールとして展開すると同時に、複数のパッシブインターフェイスを他のネットワーク内のトラフィックをモニタするように設定することができます。

パッシブインターフェイスの制限

パッシブモードインターフェイスとして定義する物理インターフェイスには次の制限があります。

- パッシブインターフェイスのサブ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をブリッジグループに含めることはできません。
- パッシブインターフェイスで IPv4 アドレスまたは IPv6 アドレスを設定することはできません。
- パッシブインターフェイスに [管理専用 (Management Only)] オプションを選択することはできません。
- このインターフェイスはパッシブモードセキュリティゾーンにのみ含めることができます。ルーテッドセキュリティゾーンに含めることはできません。
- パッシブセキュリティゾーンをアクセス制御またはアイデンティティルールの送信元基準に含めることは可能です。パッシブゾーンを宛先基準で使用することはできません。パッシブゾーンとルーテッドゾーンを同じルールに混在させることもできません。
- パッシブインターフェイスの管理アクセスルール (HTTPS または SSH) を設定することはできません。
- パッシブインターフェイスを NAT ルールで使用することはできません。
- パッシブインターフェイスのスタティックルートを設定することはできません。パッシブインターフェイスをルーティングプロトコルの設定で使用することもできません。
- パッシブ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。パッシブインターフェイスを使用して自動設定で DHCP 設定を取得することもできません。
- パッシブインターフェイスを syslog サーバ設定で使用することはできません。
- パッシブインターフェイスではどのタイプの VPN も設定することはできません。

ハードウェア Firepower 脅威デバイスパッシブインターフェイスのスイッチの設定

ハードウェア Firepower Threat Defense デバイス上のパッシブインターフェイスは、ネットワークスイッチを正しく設定している場合にのみ機能します。次の手順は、Cisco Nexus 5000 シリーズスイッチに基づいています。別のタイプのスイッチでは、コマンドが異なる可能性があります。

基本的な考え方としては、SPAN (スイッチドポートアナライザ) またはミラーポートを設定し、そのポートにパッシブインターフェイスを接続し、スイッチでモニタリングセッションを設定して、1つまたは複数の送信元ポートから SPAN またはミラーポートにトラフィックのコピーを送信します。

手順

ステップ 1 スイッチ上のポートをモニタ（SPAN またはミラー）ポートとして設定します。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

ステップ 2 モニタへのポートを特定するモニタリングセッションを定義します。

SPAN またはミラーポートを宛先ポートとして定義していることを確認します。次の例では、2つの送信元ポートがモニタされています。

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

ステップ 3 （オプション）`show monitor session` コマンドを使用して、設定を確認します。

次の例に、セッション 1 の概要出力を示します。

```
switch# show monitor session 1 brief
  session 1
-----
type           : local
state          : up
source intf    :
  rx           : Eth1/7      Eth1/8
  tx           : Eth1/7      Eth1/8
  both        : Eth1/7      Eth1/8
source VSANs   :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ 4 Firepower Threat Defense パッシブインターフェイスからスイッチ上の宛先ポートにケーブルを物理的に接続します。

物理接続を行う前後に、パッシブモードでインターフェイスを設定できます。[パッシブモードでの物理インターフェイスの設定（317 ページ）](#) を参照してください。

Firepower Threat Defense Virtual パッシブ インターフェイスの VLAN の設定

Firepower Threat Defense Virtual デバイスのパッシブインターフェイスは、仮想ネットワーク上で VLAN を正しく設定した場合にのみ機能します。次の手順を実行してください。

- Firepower Threat Defense Virtual インターフェイスを、無差別モードで設定した VLAN に接続します。その後、[パッシブモードでの物理インターフェイスの設定 \(317ページ\)](#) での説明に従ってインターフェイスを設定します。パッシブインターフェイスでは、プロミスキュス VLAN 上のすべてのトラフィックのコピーが認識されます。
- 同じ VLAN に、1 つ以上のエンドポイント デバイス (仮想 Windows システムなど) を接続します。VLAN からインターネットへの接続がある場合は、単一のデバイスを使用できます。それ以外の場合は、トラフィックを通過させるために2つ以上のデバイスが必要です。URL カテゴリのデータを取得するには、インターネット接続が必要です。

パッシブモードでの物理インターフェイスの設定

インターフェイスはパッシブモードで設定できます。パッシブに機能する場合、インターフェイスは (ハードウェア デバイスの) スイッチそのものまたは (Firepower Threat Defense Virtual の) プロミスキュス VLAN に設定されたモニタリングセッションで送信元ポートからのトラフィックを単にモニタします。スイッチまたは仮想ネットワークで設定する必要がある内容の詳細については、次のトピックを参照してください。

- [ハードウェア Firepower 脅威デバイス パッシブ インターフェイスのスイッチの設定 \(315 ページ\)](#)
- [Firepower Threat Defense Virtual パッシブ インターフェイスの VLAN の設定 \(316 ページ\)](#)

トラフィックに影響を及ぼすことなくモニタ対象スイッチポートからのトラフィックを分析するには、パッシブモードを使用します。パッシブモードを使用するエンドツーエンドの例については、[ネットワーク上のトラフィックをパッシブにモニタする方法 \(93 ページ\)](#) 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、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[インターフェイス (Interfaces)] または [EtherChannel] をクリックします。
- ステップ 2** 編集する物理インターフェイスまたは EtherChannel の編集アイコン (🔧) をクリックします。
現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブインターフェイスに変換する場合は、最初にセキュリティゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。
- 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** 以下を設定します。
 - [インターフェイス名 (Interface Name)] : 最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、monitor などです。
 - [モード (Mode)] : [パッシブ (Passive)] を選択します。

- (オプション) [説明 (Description)] : 説明は 200 文字以内で、改行を入れずに 1 行で入力します。

(注) IPv4 アドレスまたは IPv6 アドレスを設定することはできません。[詳細 (Advanced)] タブで変更できるのは、MTU、デュプレックス、速度設定のみです。

ステップ 5 [OK] をクリックします。

次のタスク

パッシブインターフェイスを作成するだけでは、インターフェイスで確認されるトラフィックの情報を十分にダッシュボードに示すことはできません、次の手順も実行する必要があります。使用例で次の手順について説明します。[ネットワーク上のトラフィックをパッシブにモニタする方法 \(93 ページ\)](#) を参照してください。

- パッシブセキュリティゾーンを作成し、それにインターフェイスを追加します。[セキュリティゾーンの設定 \(159 ページ\)](#) を参照してください。
- パッシブセキュリティゾーンを送信元ゾーンとして使用するアクセス制御ルールを作成します。通常は、これらのルールに侵入ポリシーを適用して、IDS (侵入検知システム) モニ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 \(415 ページ\)](#) を参照してください。
- 必要に応じて、パッシブセキュリティゾーン向けに SSL 復号およびアイデンティティルールを作成し、セキュリティインテリジェンスポリシーを有効にします。

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。

MAC アドレスについて

Media Access Control (MAC) アドレスを手動で設定してデフォルトをオーバーライドできます。

高可用性設定の場合は、インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの両方を設定できます。アクティブユニットがフェールオーバーしてスタンバイユニットがアクティブになると、その新規アクティブユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010）：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。[詳細オプションの設定（320 ページ）](#) を参照してください。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャンネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。サブインターフェイスに固有の 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 コントロールを実行する場合があります。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。

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できます。

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 9000 です。Firepower 4100/9300 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。高可用性にデバイスが設定されている場合、スタンバイデバイスも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または高可用性を設定する場合にのみ、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 試行回数と HA モニタリングの有効化を除き、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 1000 または 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。
- Firepower 1010 スイッチ ポートでは [詳細 (Advanced)] オプションは使用できません。
- Firepower 4100/9300 では、インターフェイスのデュプレックスや速度は設定できません。インターフェイスのこれらの機能を設定するには、FXOS を使用します。
- パッシブ インターフェイスでは、MTU、デュプレックス、速度のみ設定できます。インターフェイスの管理のみを行うことはできません。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、次にインターフェイスタイプをクリックして、インターフェイスのリストを表示します。
- 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** インターフェイスの状態を高可用性設定でピア装置にフェールオーバーするかどうか判断する際の要素にする場合は、[HA モニタリングの有効化 (Enable for HA Monitoring)] を選択します。
- このオプションは、高可用性を設定しない場合は無視されます。インターフェイスの名前を設定しない場合も、無視されます。
- ステップ 5** データ インターフェイスを管理専用指定する場合は、[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指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 6** [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 9000、Firepower 4100/9300 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。高可用性にデバイスが設定されている場合、スタンバイ デバイスも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。

ステップ7 (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ているものだけです。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 \(272 ページ\)](#) 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 SFP 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8 [IPv6設定 (IPv6 Configuration)] を変更します。

- [IPv6アドレス設定用DHCPの有効化 (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。
- [IPv6非アドレス設定用DHCPの有効化 (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

の一貫性を検証します。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 9 (必要に応じて、サブインターフェイスおよび高可用性装置に推奨されます。) MAC アドレスを設定します。

デフォルトでは、システムはインターフェイスのネットワークインターフェイスカード (NIC) に焼き込まれた MAC アドレスを使用します。したがって、インターフェイスのすべてのサブインターフェイスは同じ MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MAC アドレス (MAC Address)] : H.H.H 形式の Media Access Control。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は 000C.F142.4CDE と入力します。MAC アドレスはマルチキャストビットセットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。
- [スタンバイ MAC アドレス (Standby MAC Address)] : 高可用性で使用します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 10 [OK] をクリックします。

インターフェイスの変更のスキャンとインターフェイスの移行

デバイスのインターフェイスを変更すると、変更が発生したことがデバイスから FDM に通知されます。インターフェイスのスキャンを実行するまで、設定を展開することはできません。FDM では、セキュリティ ポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。

インターフェイスのスキャンと移行について

Scanning

デバイスのインターフェイスを変更すると、変更が発生したことがデバイスから FDM に通知されます。インターフェイスのスキャンを実行するまで、設定を展開することはできません。スキャンの後、追加、削除、または復元されたインターフェイスが検出された場合は、設定を

展開できます。ただし、設定内で削除されたインターフェイスを参照している部分は展開されません。

スキャンを必要とするインターフェイスの変更には、インターフェイスの追加または削除が含まれます。たとえば、ネットワークモジュールの変更、Firepower 4100/9300 シャーシ上に割り当てられたインターフェイスの変更、FTDv でのインターフェイスの変更があります。

次の変更については、スキャン後も展開がブロックされません。

- セキュリティゾーンのメンバーシップ
- EtherChannel インターフェイスのメンバーシップ
- Firepower 1010 VLAN インターフェイス スイッチ ポートのメンバーシップ
- BVI を参照するポリシーの場合におけるブリッジグループ インターフェイスのメンバーシップ



- (注) syslog サーバの出力インターフェイスの変更によって展開がブロックされることはありませんが、手動で、またはインターフェイス交換機能を使用して syslog サーバの設定を修正する必要があります。

Migrating

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、FTD の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、セキュリティゾーン、NAT、VPN、ルーティング、DHCP サーバなど、FTD の設定における多くの場所で直接参照されている可能性があります。

FDM では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。



- (注) 移行機能では、名前、IP アドレス、およびその他の設定は 1 つのインターフェイスから別のインターフェイスにコピーされません。代わりに、古いインターフェイスではなく、新しいインターフェイスを参照するようにセキュリティポリシーが変更されます。移行する前に、新しいインターフェイス設定を手動で設定する必要があります。

インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。インターフェイスの追加と削除を同時に行っても移行プロセスは機能します。ただし、削除されたインターフェイスやそれらを参照するポリシーを「手動で」編集することはできません。そのため、移行を段階的に実行する方が簡単になる場合があります。

同じタイプのインターフェイスを交換する場合（たとえば、ネットワークモジュールを RMA する必要がある場合）は、次のことができます。1. シャーシからモジュールを取り外します。

2. スキャンを実行します。3. 削除されたインターフェイスとは関係のない変更を展開します。4. モジュールを交換します。5. 新しいスキャンを実行します。6. インターフェイスに関連する変更を含めて、設定を展開します。新しいインターフェイスのインターフェイス ID と特性が古いインターフェイスと同じである場合は、移行を実行する必要はありません。

インターフェイスのスキャンと移行に関する注意事項と制限事項

サポートされていないインターフェイスの移行

- 物理インターフェイスから BVI へ
- パッシブ インターフェイスからファイアウォール インターフェイスへ
- ブリッジ グループ メンバー
- EtherChannel インターフェイスのメンバー
- ISA 3000 ハードウェア バイパスのメンバー
- Firepower 1010 VLAN インターフェイスまたはスイッチ ポート
- 診断インターフェイス
- HA フェールオーバーおよびステートリンク
- 異なるタイプどうしのインターフェイスの移行（たとえば、ブリッジグループ インターフェイスを、物理インターフェイスを必要とする機能に移行するなど）

その他のガイドライン

- インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。
- FTDv では、インターフェイス リストの末尾でのみ、インターフェイスを追加および削除してください。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤った順番になります。
- スキャン/移行が失敗した場合は、シャージで元のインターフェイスを復元し、再スキャンを実行して元の状態に戻してください。
- バックアップの場合は、必ず新しいインターフェイスを使用して新しいバックアップを作成してください。古い設定を使用して復元すると、古いインターフェイス情報が復元されるため、スキャン/置換を再度実行する必要があります。
- HA の場合は、アクティブ ユニットでインターフェイスのスキャンを実行する前に、両方のユニットで同じインターフェイスの変更を行います。アクティブ ユニットでスキャン/移行を実行するだけで済みます。設定の変更はスタンバイ ユニットに複製されます。

インターフェイスのスキャンと移行

FDMでインターフェイスの変更をスキャンし、削除されたインターフェイスからインターフェイス設定を移行します。インターフェイス設定の移行のみを必要とする場合は（スキャンは不要）、次の手順のうちスキャンに関連するステップを無視してください。



- (注) 移行機能では、名前、IPアドレス、およびその他の設定は1つのインターフェイスから別のインターフェイスにコピーされません。代わりに、古いインターフェイスではなく、新しいインターフェイスを参照するようにセキュリティポリシーが変更されます。移行する前に、新しいインターフェイス設定を手動で設定する必要があります。

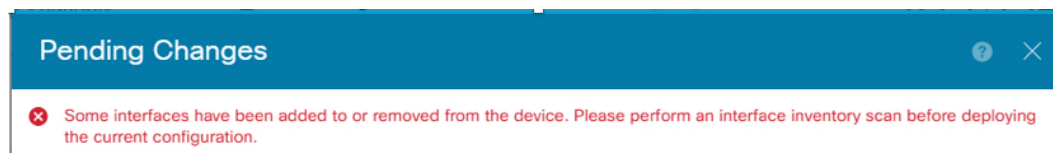
手順

ステップ1 シャーシでインターフェイスを追加または削除します。

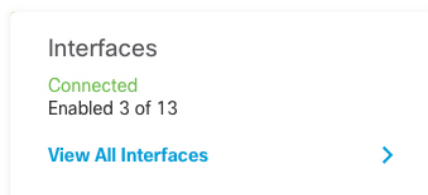
インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスの交換を行うことをお勧めします。


ステップ2 インターフェイスの変更をスキャンします。

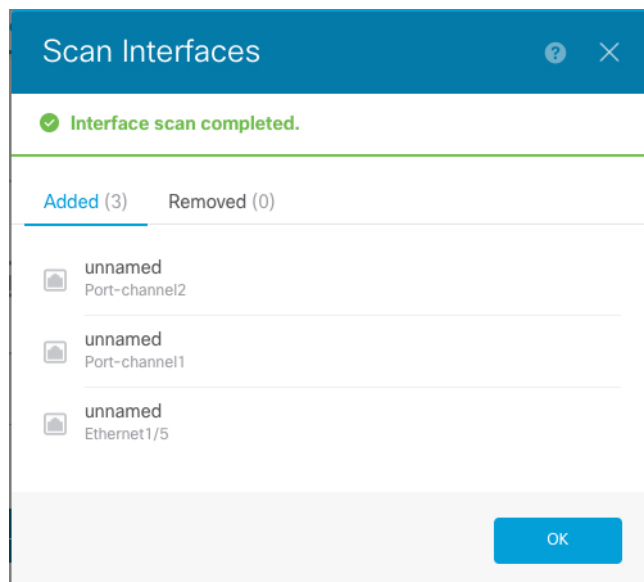
インターフェイスのスキャンを実行するまで、設定を展開することはできません。スキャンの前に展開しようとする、次のエラーが表示されます。



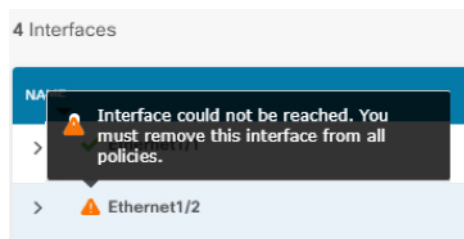
- a) [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにある [すべてのインターフェイスを表示 (View All Interfaces)] リンクをクリックします。



- b) [インターフェイス (Interfaces)] アイコン () をクリックします。
 c) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



スキャンの後、削除されたインターフェイスが警告記号とともに [インターフェイス (Interfaces)] ページに表示されます。



ステップ 3 既存のインターフェイスを新しいインターフェイスに移行するには、次のようにします。

- a) 名前、IP アドレスなどを使用して新しいインターフェイスを設定します。

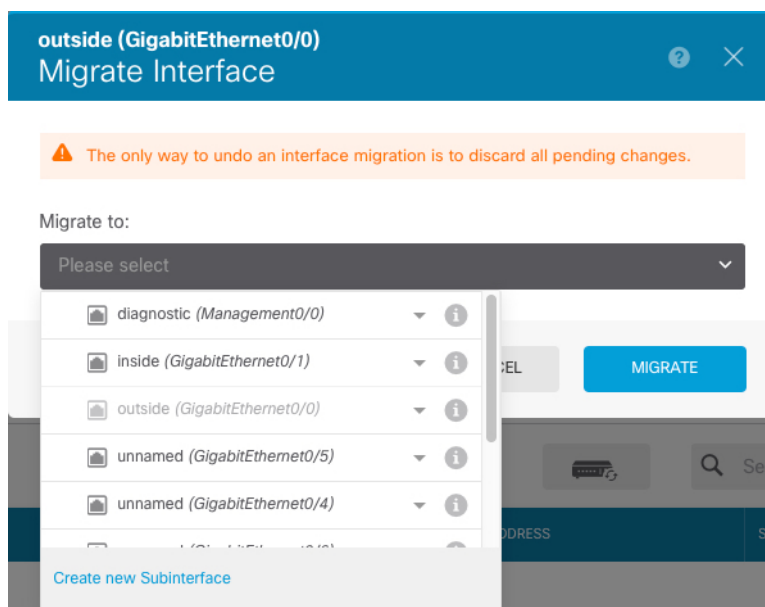
削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでそれらの設定を使用できるように、最初にダミーの名前と IP アドレスを使用して古いインターフェイスを再設定する必要があります。

- b) 古いインターフェイスの [移行 (Migrate)] アイコンをクリックします。

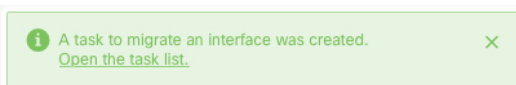


このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに移行されます。

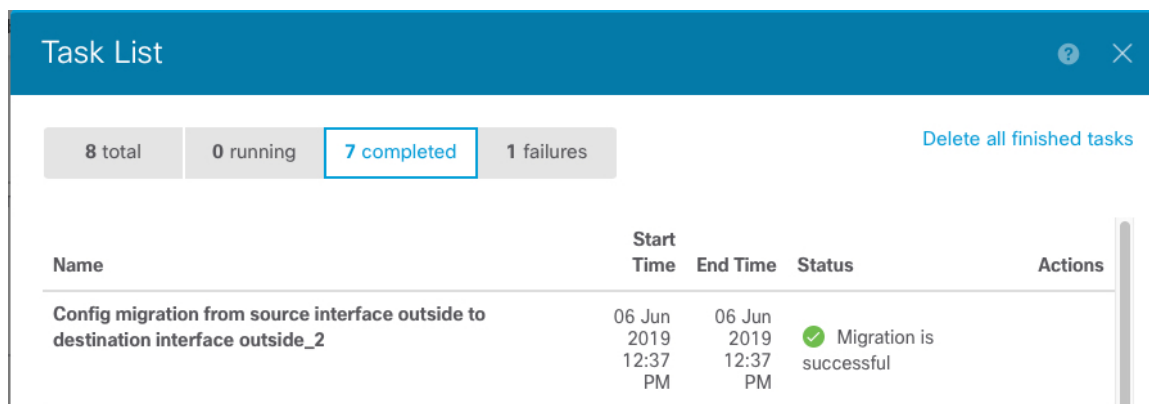
- c) [移行先 : (Migrate to:)] ドロップダウン リストから新しいインターフェイスを選択します。



- d) [インターフェイス (Interfaces)] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。



- e) [タスクリスト (Task List)] を調べて、移行が成功したことを確認します。

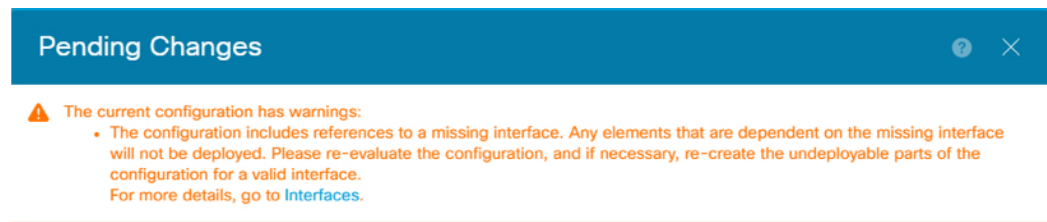


- f) 移行が失敗した場合は、API エクスプローラで理由を確認できます。

API エクスプローラを開くには、[詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。[インターフェイス (Interface)] > [GET/jobs/interfacemigrations] を選択し、[試してみる (Try it Out!)] をクリックします。

ステップ 4 設定を展開します。

設定のうち削除されたインターフェイスを参照する部分は展開されません。その場合は次のメッセージが表示されます。



ステップ 5 シャーシで古いインターフェイスを削除し、再度スキャンを実行します。

削除されたインターフェイスのうちポリシーで使用されなくなったものは、[インターフェイス (Interfaces)] ページから削除されます。

ステップ 6 設定を再度展開し、使用していないインターフェイスを設定から削除します。

ISA 3000 のハードウェアバイパスの設定

ハードウェアバイパスを有効にして、停電時でもトラフィックがインターフェイス ペア間を通過できるようにできます。サポートされているインターフェイスペアは銅線インターフェイスの GigabitEthernet 1/1 と 1/2、および GigabitEthernet 1/3 と 1/4 です。光ファイバーサネットモデルを保有している場合は、銅線イーサネットペア (GigabitEthernet 1/1 と 1/2) でのみハードウェアバイパスがサポートされます。

デフォルトでは、両方のインターフェイス ペアに対してハードウェアバイパスが有効になります (サポートされている場合)。ただし、[停電時の自動ハードウェアバイパスの設定 \(ISA 3000\) \(330 ページ\)](#) の説明に従って、TCPシーケンスのランダム化を無効にすることをお勧めします。

ハードウェアバイパスがアクティブの場合、トラフィックはレイヤ1でそれらのインターフェイス ペア間を通過します。FDM および FTD CLI のどちらも、インターフェイスがダウンしているものとみなします。ファイアウォール機能はないため、トラフィックのデバイス通過を許可することのリスクを理解している必要があります。

ハードウェアバイパスを機能させるための前提条件：

- インターフェイス ペアは同じブリッジグループに配置する必要があります。
- インターフェイスはスイッチのアクセスポートに接続する必要があります。トランクポートには接続しないでください。

次のトピックでは、ISA 3000 のハードウェアバイパスを設定する方法について説明します。

停電時の自動ハードウェアバイパスの設定 (ISA 3000)

次の手順では、ISA 3000 デバイスでの電源障害発生時の自動ハードウェアバイパスの設定方法について説明します。

(この手順で説明されている) TCP シーケンス番号のランダム化は無効にすることをお勧めします。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号 (ISN) が乱数に書き換えられます。ハードウェアバイパスがアクティブになると、ISA 3000 はデータパスには入らず、シーケンス番号は変換されません。受信側のクライアントが予期しないシーケンス番号を受信すると接続がドロップされるため、TCP セッションを再確立する必要があります。TCP シーケンス番号のランダム化が無効になっている場合でも、スイッチオーバー中に一時的にダウンするリンクがあるため、一部の TCP 接続は再確立する必要があります。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニタします。

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 (Interfaces)] サマリーにあるリンクをクリックします。

ページの上部にある [ハードウェアバイパス (Hardware Bypass)] セクションは、このデバイスに使用できるインターフェイスペアの現在の設定を示します。

ただし、ハードウェアバイパスを有効にする前に、ペアが同じブリッジグループで設定されていることを確認する必要があります。

ステップ 2 特定のペアの自動ハードウェアバイパスを有効または無効にするには、[電源オフ時にバイパス (Bypass When Power Down)] 列で、ペアのスライダーを移動します。

変更はすぐには適用されません。設定を展開する必要があります。

ステップ 3 (オプション) TCP シーケンス番号ランダム化を無効にするために必要な FlexConfig オブジェクトとポリシーを作成します。

- [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。
- 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。
- 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。たとえば、**Disable_TCP_Randomization** と入力します。
- [テンプレート (Template)] エディタに、TCP シーケンス番号のランダム化を無効にするコマンドを入力します。

コマンドは **set connection random-sequence-number disable** ですが、ポリシーマップ内の特定のクラスに対して設定する必要があります。最も簡単なアプローチは、ランダムな

シーケンス番号をグローバルに無効にする方法です。この場合、次のコマンドを入力する必要があります。

```
policy-map global_policy
  class default_class
    set connection random-sequence-number disable
```

- f) [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。

たとえば、TCP シーケンス番号のランダム化をグローバルに無効にしている場合、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 default_class
    set connection random-sequence-number enable
```

- g) [OK] をクリックしてオブジェクトを保存します。

ここで、オブジェクトを FlexConfig ポリシーに追加する必要があります。オブジェクトを作成するだけでは不十分です。

- h) 目次で [FlexConfigポリシー (FlexConfig Policy)] をクリックします。

- i) [グループリスト (Group List)] で [+] をクリックします。

- j) `Disable_TCP_Randomization` 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。

- k) [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。

ハードウェアバイパス (ISA 3000) を手動で起動

ハードウェアバイパスを手動で起動することができます。たとえば、システムをテストしたり、何らかの理由でデバイスを一時的にバイパスする必要がある場合があります。

次の手順では、ハードウェアバイパスを手動で有効または無効にする方法について説明します。ハードウェアバイパスの状態を変更するには、設定を展開する必要があることに注意してください。設定を変更するだけでは不十分です。

ハードウェアバイパスを手動で有効化または無効化すると、次の Syslog メッセージが表示されます。メッセージ内の *pair* は 1/1-1/2 または 1/3-1/4 です。

- %FTD-6-803002: no protection will be provided by the system for traffic over GigabitEthernet *pair*
- %FTD-6-803003: User disabled bypass manually on GigabitEthernet *pair*

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 (Interfaces)] サマリーにあるリンクをクリックします。

ページの上部にある [ハードウェアバイパス (Hardware Bypass)] セクションは、このデバイスに使用できるインターフェイスペアの現在の設定を示します。

ただし、ハードウェアバイパスを手動で有効または無効にする前に、ペアが同じブリッジグループで設定されていることを確認する必要があります。

ステップ 2 ペアのハードウェアバイパスを手動で有効にするには：

- a) [直ちにバイパス (Bypass Immediately)] 列で有効状態になるようにペアのスライダを移動します。
- b) 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、変更を展開します。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニタします。

ステップ 3 ペアのハードウェアバイパスを手動で無効にするには：

- a) [直ちにバイパス (Bypass Immediately)] 列で無効状態になるようにペアのスライダを移動します。
- b) 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、変更を展開します。

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、EtherChannel のメンバーシップ、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せん。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。
- **show switch vlan VLAN** とスイッチポートの関連付けを表示します。
- **show switch mac-address-table** スタティックおよびダイナミック MAC アドレス エントリを表示します。
- **show arp** ダイナミック、スタティック、およびプロキシ ARP エントリを表示します。
- **show power inline PoE** ステータスを表示します。

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 \(53 ページ\)](#)

- [サブネットを追加する方法 \(86 ページ\)](#)
- [ネットワーク上のトラフィックをパッシブにモニタする方法 \(93 ページ\)](#)



第 12 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 \(335 ページ\)](#)
- [スタティック ルート \(341 ページ\)](#)
- [ルーティングのモニタリング \(347 ページ\)](#)

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、システムはネイバー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、着信ルーティングアップデート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、BGP。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 7: 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 テーブル内のエントリと一致しない場合、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つのエントリと一致した場合、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トリと一致し、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定義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や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 ルーティングまたはダイナミックルーティングを使用して、ホストやネットワークへのルートを定義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。

Default Route

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 \(340 ページ\)](#) 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。

スタティックルートのバックアップとスタティックルートのトラッキング

スタティックルートの問題の1つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティックルートは、ネクストホップゲートウェイが使用できなくなった場合でも、ルーティングテーブルに保持されています。スタティックルートは、関連付けられたインターフェイスがダウンした場合に限りルーティングテーブルから削除されます。

ルートトラッキングを実装すると、サービスレベル契約 (SLA) モニタを使用してスタティックルートの可用性を追跡し、プライマリルートが失敗したら自動的にバックアップルートを

インストールすることができます。たとえば、ISPゲートウェイへのデフォルトルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップデフォルトルートを定義できます。

ルートトラッキングを使用する場合、トラッキング対象のルートに宛先ネットワークのターゲット IP アドレスを関連付けます。その後、システムは ICMP エコー要求を使用して、アドレスにアクセスできることを定期的に確認します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティングテーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップルートが使用されます。

したがって、デフォルトルートなどの特定の宛先にバックアップスタティックルートを使用するには、次を実行する必要があります。

1. ゲートウェイや常時稼働サーバ（Webサーバやsyslogサーバなど）のような、宛先ネットワーク上の信頼できるIPアドレスをモニタするSLAモニタを作成します。宛先ネットワークが正常かつ使用可能な状態の間にオフラインになる可能性のあるシステムのIPアドレスはモニタしません。[SLA モニタ オブジェクトの設定 \(346ページ\)](#) を参照してください。
2. 宛先へのプライマリルートを作成し、ルートのSLAモニタを選択します。このルートのメトリックは通常、1とする必要があります。[スタティック ルートの設定 \(344ページ\)](#) を参照してください。
3. プライマリルートが失敗した場合に使用されるバックアップスタティックルートを作成します。このルートには、プライマリルートより大きいメトリックが必要です。たとえば、プライマリルートが1の場合は、バックアップルートは10などが考えられます。また、通常はバックアップルートとは異なるインターフェイスを選択します。

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トラッキングは、ブリッジグループメンバーインターフェイスまたはBVIではサポートされません。

IPv6

- IPv6では、スタティックルートトラッキングはサポートされません。

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

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

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、ルートを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 (オプション、IPv4 ルートのみ)。このルートの有効性を追跡する **SLA モニタ** を選択します。

SLA モニタは、ターゲット ネットワーク上の常時利用可能なホストが到達可能であることを確認できます。到達不能になった場合、システムはバックアップルートをインストールできません。したがって、SLA モニタを設定する場合は、このネットワークに対してより大きなメトリックを持つ別のスタティックルートも設定する必要があります。たとえば、このルートにメトリック 1 がある場合は、メトリック 10 を使用してバックアップルートを作成します。詳細については、[スタティックルートのバックアップとスタティックルートのトラッキング \(342 ページ\)](#) を参照してください。

SLA モニタ オブジェクトがまだ存在しない場合は、リストの下部にある [SLA モニタの作成 (Create SLA Monitor)] リンクをクリックしてここで作成します。

(注) モニタ対象のアドレスが ping できないためにモニタ対象のルートが削除された場合は、そのルートがスタティック ルート テーブルに示され、ルートが到達不能であることを示す警告が表示されます。問題が一時的なものなのか、またはルートを再設定する必要があるかを判断してください。ルートが有効であるが、モニタ対象のアドレスが十分に信頼できるものではない可能性があることを考慮してください。

ステップ 5 [OK] をクリックします。

SLA モニタ オブジェクトの設定

スタティックルートとともに使用するためのサービスレベル契約 (SLA) モニタオブジェクトを設定します。SLA モニタを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。ルートトラッキングの詳細については、[スタティックルートのバックアップとスタティックルートのトラッキング \(342 ページ\)](#) を参照してください。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象はホスト ネットワーク オブジェクトで定義されている任意の IP アドレスとすることができますが、次の使用を検討する必要があります。

- ISP ゲートウェイアドレス (デュアル ISP サポート用)。
- ネクスト ホップ ゲートウェイ アドレス (ゲートウェイの使用可能状況に懸念がある場合)。
- システムが通信を行う必要のある対象ネットワーク上のサーバ (syslog サーバなど)。
- 宛先ネットワーク上の永続的な IP アドレス。夜間にシャットダウンすることがあるワークステーションは適しません。

手順

ステップ 1 [オブジェクト (Objects)] を選択して、目次から [SLA モニタ (SLA Monitors)] 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 SLA モニタに必要なオプションを定義します。

- [モニタアドレス (Monitor Address)]: 宛先ネットワークでモニタするアドレスを定義するホスト ネットワーク 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、[新しいネットワークの作成 (Create New Network)] をクリックします。

このアドレスは、SLA モニタをスタティック ルートに接続している場合にのみモニタされます。

- [インターフェイス (Interface)]: エコー要求パケットを送信する際に通過するインターフェイスを選択します。これは通常、スタティックルートを定義するインターフェイスになります。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。

ステップ5 (オプション) [IP ICMPエコーオプション (IP ICMP Echo Options)] を調整します。

ICMP オプションにはすべてデフォルト値があり、ほとんどの場合それらは適切ですが、要件に合わせて調整することができます。

- [しきい値 (Threshold)] : 宣言する上昇しきい値 (ミリ秒) (0 ~ 2147483647 の間)。デフォルトは 5000 (5 秒) です。この値は、タイムアウトに設定された値以下にする必要があります。しきい値は、しきい値超過イベントを示すためにだけ使用され、到達可能性には影響しません。しきい値イベントの頻度を使用すると、タイムアウトの設定を評価できます。
- [タイムアウト (Timeout)] : ルート監視操作が要求パケットからの応答を待つ時間 (ミリ秒) (0 ~ 604800000 ミリ秒 (7 日間) の間)。デフォルト値は 5000 ミリ秒 (5 秒) です。モニタがこの期間中に少なくとも 1 つのエコー要求への応答を受信しなかった場合、プロセスはバックアップルートを実インストールします。
- [頻度 (Frequency)] : SLA プロブ間のミリ秒数 (1000 ~ 604800000、1000 の倍数)。タイムアウト値未満の頻度を設定することはできません。デフォルト値は 60000 ミリ秒 (60 秒) です。
- [サービスタ입 (Service Type)] : ICMP エコー要求パケットの IP ヘッダーの Type of Service (ToS) タイプを定義する整数 (0 ~ 255 の間)。デフォルトは 0 です。
- [パケットの数 (Number of Packets)] : 各ポーリングを送信するパケットの数 (1 ~ 100 の間)。デフォルトは 1 パケットです。
- [データサイズ (Data Size)] : エコー要求パケットで使用するデータ ペイロードのサイズ (0 ~ 16384 バイトの間)。デフォルト値は 28 です。この設定では、ペイロードのサイズだけが指定されます。パケット全体のサイズは指定されません。

ステップ6 [OK] をクリックします。

これで、スタティックルートで SLA モニタ オブジェクトを使用することができます。

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 **IV** 部

セキュリティ ポリシー

- [SSL 復号 \(351 ページ\)](#)
- [アイデンティティ ポリシー \(379 ページ\)](#)
- [セキュリティ インテリジェンス \(395 ページ\)](#)
- [アクセス制御 \(401 ページ\)](#)
- [侵入ポリシー \(451 ページ\)](#)
- [ネットワーク アドレス変換 \(NAT\) \(465 ページ\)](#)



第 13 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 \(351 ページ\)](#)
- [SSL 復号のためのライセンス要件 \(355 ページ\)](#)
- [SSL 復号のガイドライン \(355 ページ\)](#)
- [SSL 復号ポリシーの実装および管理方法 \(356 ページ\)](#)
- [SSL 復号ポリシーの設定 \(358 ページ\)](#)
- [例：ネットワークからの古い SSL/TLS バージョンのブロック \(373 ページ\)](#)
- [SSL 復号のモニタリングとトラブルシューティング \(375 ページ\)](#)

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。



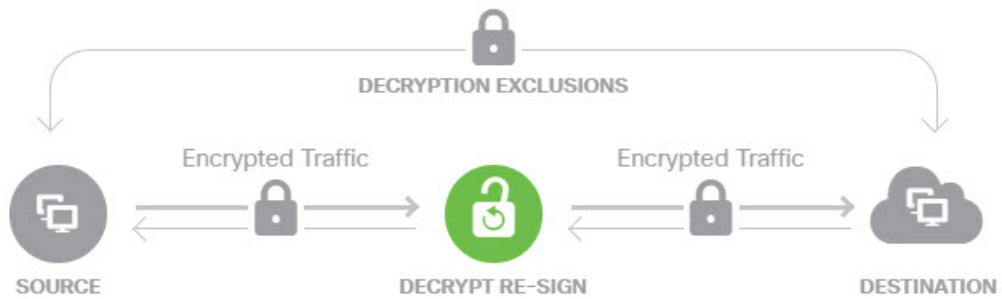
- (注) SSL 復号ポリシーを経由するすべてのトラフィックは、アクセスコントロールポリシーを経由する必要があります。SSL 復号ポリシーにドロップするトラフィックを除き、許可またはドロップの最終的な決定はアクセスコントロールポリシーに委ねられます。

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 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 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 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 \(370 ページ\)](#) 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。
- パッシブ インターフェイス トラフィック：パッシブ インターフェイス（パッシブ セキュリティ ゾーン）のすべてのトラフィックが復号不能です。

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 \(108 ページ\)](#) 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。
- アクティブ認証ルールを使用している場合は、SSL 復号ポリシーを無効にすることができません。SSL 復号ポリシーを無効にするには、アイデンティティ ポリシーを無効にするか、またはアクティブ認証を使用するアイデンティティ ルールを削除する必要があります。

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（175 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（173 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必要があるため、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（173 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（360 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（361 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（362 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（370 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（371 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 () 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 \(176 ページ\)](#) 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 \(356 ページ\)](#) 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 \(360 ページ\)](#)」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 \(361 ページ\)](#) 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復号を有効化 (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 \(370 ページ\)](#)
 - [再署名の復号ルールの CA 証明書のダウンロード \(371 ページ\)](#)
- 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 \(362 ページ\)](#) 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。
- URL カテゴリの削除または変更などが原因で特定のルールに問題が発生した場合、これらのルールのみを表示するには、検索ボックスの横にある [問題のあるルールを参照 (See Problem Rules)] リンクをクリックしてテーブルをフィルタリングします。これらのルールを編集および修正 (または削除) して、必要とするサービスが提供されるようになります。

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。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 \(370 ページ\)](#) 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 \(371 ページ\)](#) 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 \(370 ページ\)](#) 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。

[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 \(352 ページ\)](#)
- [既知のキーの復号 \(353 ページ\)](#)
- [復号禁止 \(354 ページ\)](#)
- [ブロック \(354 ページ\)](#)

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 \(364 ページ\)](#) 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 \(366 ページ\)](#) 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 \(367 ページ\)](#) を参照してください。
- [ユーザ (Users)] : アイデンティティ ソース、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 \(368 ページ\)](#) 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 \(369 ページ\)](#) 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)。
- [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 復号ルールのアプリケーション基準

SSL 復号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。ユーザー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 \(160ページ\)](#) 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、信頼できな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、または復号されます。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 \(404 ページ\)](#) 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)] スライダー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ー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 (Questionable 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、**[信頼できない (Untrusted)]** (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、**[好ましいサイト (Favorable sites)]** (レベル4) を復号しないルールを設定した場合、**[信頼できる (Trusted)]** (レベル5) サイトも自動的に復号されません。

URL のカテゴリの確認

特定の URL のカテゴリとレピュテーションをチェックすることができます。**[確認する URL (URL to Check)]** ボックスに URL を入力し、**[移動 (Go)]** をクリックします。結果を表示するには、外部の Web サイトに移動します。分類に同意しない場合は、**[URL カテゴリの異議を送信する (Submit a URL Category Dispute)]** リンクをクリックして弊社までお知らせください。

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。

そのソース内のすべてのユーザに適用するアイデンティティソースを選択することもできます。したがって、複数の Active Directory ドメインをサポートする場合は、ドメインに基づく差分復号を提供できます。

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。

- [アイデンティティソース (Identity Sources)] : AD レalmやローカル ユーザ データベースなど、選択したソースから取得したすべてのユーザにルールを適用するアイデンティティソースを選択します。必要なレalmがまだ存在しない場合、[新規アイデンティティレalmの作成 (Create New Identity Realm)] をクリックして作成します。
- [グループ (Groups)] : 目的の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。
- [ユーザ (Users)] : 個々のユーザを選択します。ユーザ名には、Realm\username などのアイデンティティソースがプレフィックスとして付けられます。

Special-Identities-Realm の下にはいくつかの組み込みユーザがあります。

- [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。

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 (ValidFrom)] 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 (371 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 (360 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。

The screenshot shows the configuration interface for adding an SSL Decryption Rule. The rule is titled "Block_SSL3.0_and_TLS1.0" and is set to "Block" action. The "Advanced" tab is selected, showing the following settings:

- CERTIFICATES:** Certificate Status is set to "Any", and Self Signed is set to "Any".
- SUPPORTED VERSION:** SSL 3.0 and TLS 1.0 are checked, while TLS 1.1 and TLS 1.2 are unchecked.

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」である必要があります。
- [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。

■ 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)



第 14 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 \(379 ページ\)](#)
- [アイデンティティ ポリシーを実装する方法 \(381 ページ\)](#)
- [アイデンティティ ポリシーの設定 \(382 ページ\)](#)
- [トランスペアレント ユーザ認証の有効化 \(390 ページ\)](#)
- [アイデンティティ ポリシーのモニタリング \(394 ページ\)](#)
- [アイデンティティ ポリシーの例 \(394 ページ\)](#)

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よう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。

ユーザ アイデンティティは、次の方法で取得できます。

- **パッシブ認証**：すべてのタイプの接続で、ユーザ名とパスワードを求められることなく、その他の認証サービスからユーザ アイデンティティを取得します。

- アクティブ認証：HTTP 接続でのみ、ユーザ名とパスワードの入力が求められ、送信元 IP アドレスのユーザアイデンティティを取得するために指定のアイデンティティソースに対する認証が行われます。

ここでは、ユーザアイデンティティについて詳しく説明します。

パッシブ認証によるユーザアイデンティティの確立

パッシブ認証では、ユーザにユーザ名とパスワードを求めることなくユーザIDを収集します。システムは、指定したアイデンティティソースからマッピングを取得します。

ユーザと IP アドレスのマッピングは次のソースから受動的に取得できます。

- リモートアクセスVPNログイン。パッシブアイデンティティについては次のユーザタイプがサポートされています。
 - 外部認証サーバで定義されたユーザアカウント。
 - Firepower Device Manager で定義されたローカルユーザアカウント。
- Cisco Identity Services Engine (ISE)、Cisco Identity Services Engine Passive Identity Connector (ISE PIC)。

特定のユーザが複数のソースによって識別される場合は、RA VPN ID が優先されます。

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）]>[アイデンティティソース（Identity Sources）]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 ポリシーを実装する方法

ユーザ アイデンティティの取得を有効にし、IP アドレスに関連付けられているユーザを認識させるには、いくつかの項目を設定する必要があります。正しく設定されている場合、監視ダッシュボードおよびイベントでユーザ名を確認できます。ユーザ アイデンティティは、アクセス制御ルールや SSL 復号化ルールでもトラフィック一致基準として使用できます。

次の手順では、アイデンティティ ポリシーを機能させるために設定する必要がある内容の概要を示します。

手順

ステップ 1 AD アイデンティティ レルムを設定します。

（ユーザ認証を要求して）ユーザ アイデンティティをアクティブに収集するか、またはパッシブに収集して、ユーザ アイデンティティ情報を含む Active Directory（AD）サーバを設定する必要があります。[AD アイデンティティ レルムの設定（183 ページ）](#) を参照してください。

ステップ 2 パッシブ認証アイデンティティ ルールを使用する場合は、パッシブ アイデンティティ ソースを設定します。

デバイスに実装しているサービスおよびネットワークで使用可能なサービスに基づき、次のいずれかを設定できます。

- リモート アクセス VPN : デバイスへのリモート アクセス VPN 接続をサポートする場合は、AD サーバまたは (Firepower Device Manager に定義されている) ローカルユーザに基づいて、ユーザログイン時にアイデンティティを提供できます。RA VPN の設定方法については、[リモート アクセス VPN の設定 \(613 ページ\)](#) を参照してください。
- Cisco Identity Services Engine (ISE) または Cisco Identity Services Engine Passive Identity Connector (ISE PIC) : これらの製品を使用する場合は、デバイスを pxGrid サブスクライバとして設定し、ISE からユーザアイデンティティを取得できます。[Identity Services Engine の設定 \(193 ページ\)](#) を参照してください。

ステップ 3 [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ます。[アイデンティティ ポリシーの設定 \(382 ページ\)](#) を参照してください。

ステップ 4 [アイデンティティ ポリシーの設定 \(383 ページ\)](#)。

システムに設定しているソースに基づいて、パッシブアイデンティティソースが自動的に選択されます。アクティブ認証を設定する場合は、キャプティブポータルおよび (SSL 復号ポリシーをまだ有効にしていない場合の) SSL 再署名復号用の証明書を設定する必要があります。

ステップ 5 [アイデンティティ ポリシーのデフォルトアクションの設定 \(385 ページ\)](#)。

パッシブ認証だけを使用する場合は、パッシブ認証に対するデフォルトアクションを設定でき、特定のルールを作成する必要はありません。

ステップ 6 [アイデンティティ ルールの設定 \(386 ページ\)](#)。

関連するネットワークからパッシブまたはアクティブユーザアイデンティティを収集するルールを作成します。

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 \(383 ページ\)](#) 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。
- [デフォルトアクション (Default Action)] を変更するには、アクションをクリックして、希望のアクションを選択します。[アイデンティティ ポリシーのデフォルトアクションの設定 \(385 ページ\)](#) を参照してください。
- 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 \(386 ページ\)](#) 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、ユーザアイデンティティ情報を提供する送信元を設定する必要があります。必要な設定は、設定するルールのタイプ (パッシブ、アクティブ、または両方) によって異なります。

別のセクションで、設定ダイアログボックスにこれらの設定が表示されます。ダイアログボックスにアクセスする方法に応じて、両方のセクションが表示されるか、または片方のセクションだけが表示されます。構成済みの必要な設定を使用せずに認証タイプのルールを作成しようとすると、自動的にダイアログボックスが表示されます。

次の手順で、すべてのダイアログボックスについて説明します。

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 [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 [パッシブ認証 (Passive Authentication)] オプションを設定します。

ダイアログボックスに、設定済みのパッシブ認証ソースが表示されます。

必要に応じて、このダイアログボックスで ISE を設定できます。ISE オブジェクトを設定していない場合は、[ISEの統合 (Integrate ISE)] リンクをクリックしてすぐに作成できます。オブジェクトが存在する場合は、状態 ([有効 (Enabled)] または [無効 (Disabled)]) とともに表示されます。

パッシブ認証ルールを作成するには、少なくとも1つの有効なパッシブアイデンティティソースを設定する必要があります。

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 (アクティブ認証のみ)。[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 (371 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 ポリシーのデフォルト アクションの設定

アイデンティティ ポリシーにはデフォルトアクションがあり、これは個別のアイデンティティ ルールに一致しない接続に実行されます。

実際には、ルールがないことがポリシーの有効な設定になります。すべてのトラフィックの送信元でパッシブ認証を使用する予定の場合は、単純にパッシブ認証をデフォルトアクションとして設定します。

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。

ステップ 2 [デフォルトアクション (Default Action)] をクリックして、次のいずれかを選択します。

- [パッシブ認証 (任意のアイデンティティソース) (Passive Auth (Any Identity Source))] : ユーザアイデンティティは、任意のアイデンティティ ルールに一致しない接続に対して設定されたすべてのパッシブアイデンティティ ソースを使用して特定されます。パッシブアイデンティティ ソースを設定しない場合は、パッシブ認証をデフォルトとして使用すると [認証なし (No Auth)] を使用することと同じになります。

- [認証なし (認証不要) (No Auth (No Authentication Required))] : ユーザ アイデンティティは、任意のアイデンティティ ルールに一致しない接続について特定されません。

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。

ステップ 5 [アクション (Action)] を選択し、必要に応じて [ADアイデンティティソース (AD Identity Source)] を選択します。

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almを選択する必要があります。必要なレalmがまだ存在しない場合、[新規アイデンティティレalmの作成 (Create New Identity Realm)] をクリックして作成します。

- [パッシブ認証 (Passive Auth)] : パッシブ認証を使用して、ユーザアイデンティティを判断します。設定されたすべてのアイデンティティソースが表示されます。ルールでは、設定されたすべてのソースが自動的に使用されます。
- [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 6 (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alm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せんが、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 \(390ページ\)](#) 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 7 (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 8 [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。ただし、パッシブ認証は任意のタイプのトラフィックに有効です。

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つを通過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。

(注) 1つのルールにパッシブセキュリティゾーンとルーテッドセキュリティゾーンを混在させることはできません。また、パッシブセキュリティゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

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せん。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 9 [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

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、**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。

パッシブ認証の場合、そのソースを使用しているときは、ISEオブジェクトの**[テスト (Test)]** ボタンを使用します。リモートアクセスVPNを使用している場合は、サービスが正常に機能していることと、ユーザがVPN接続を確立できることを確認します。問題の特定と解決の詳細については、これらの機能に関するトラブルシューティングのトピックを参照してください。

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 \(59 ページ\)](#) を参照してください。



第 15 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 \(395 ページ\)](#)
- [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 \(397 ページ\)](#)
- [セキュリティ インテリジェンスの設定 \(397 ページ\)](#)
- [セキュリティ インテリジェンスのモニタリング \(399 ページ\)](#)
- [セキュリティ インテリジェンスの例 \(399 ページ\)](#)

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。ネットワークオブジェクトには、FQDN または範囲指定を使用できないことに注意してください。

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。



- (注) HTTP/HTTPS 要求の宛先が、ホスト名ではなく IP アドレスを使用する URL である場合は、ネットワーク アドレス リストにある IP アドレスの評価が検索されます。ネットワークおよび URL リストで IP アドレスを重複させる必要はありません。

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ルドにある場合、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 8: 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PPER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。

カテゴリ	説明
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。
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 \(108 ページ\)](#) 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) フィードの説明については、フィードの横にある [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ドカテゴリ (396 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ルドなど、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 \(67 ページ\)](#) を参照してください。



第 16 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 \(401 ページ\)](#)
- [アクセス制御のためのライセンス要件 \(412 ページ\)](#)
- [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 \(412 ページ\)](#)
- [アクセス コントロール ポリシーを設定する \(415 ページ\)](#)
- [アクセス コントロール ポリシーのモニタリング \(429 ページ\)](#)
- [アクセス制御の例 \(432 ページ\)](#)

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)。
- 送信元と宛先の完全修飾ドメイン名 (FQDN) (ネットワーク オブジェクトの形式)。トラフィックの照合は、その名前に関して DNS ルックアップから返された IP アドレスに基づいて行われます。
- 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 \(420 ページ\)](#) 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。

Common Industrial Protocol (CIP) および Modbus アプリケーション (ISA 3000) でのフィルタリング

Cisco ISA 3000 デバイスで Common Industrial Protocol (CIP) および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write というように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。

プリプロセッサを有効にするには、CLI セッション (SSH または コンソール) でエキスパートモードに移行し、次のコマンドを発行して、これらの遠隔監視制御・情報取得 (SCADA) アプリケーションの一方または両方を有効にする必要があります。

```
sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}
```

たとえば、両方のプリプロセッサを有効にするには、次のようにします。

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```



- (注) すべての展開後にこのコマンドを発行する必要があります。これらのプリプロセッサは、展開時には無効になります。

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、[信頼できない (Untrusted)] (レベル 1) から [信頼できる (Trusted)] (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、アクセス制御を使用して、違法ドラッグカテゴリの信頼できない URL をブロックできます。

カテゴリの説明については、<https://www.talosintelligence.com/categories> を参照してください。

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 \(707 ページ\)](#) 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

特定の URL のカテゴリとレピュテーションをチェックすることができます。アクセス制御ルール、または SSL 復号ルールの [URL] タブに移動したり、[デバイス (Device)] > [システム設定 (System Settings)] > [URL フィルタリングの設定 (URL Filtering Preferences)] に移動することができます。そこで、[確認する URL (URL to Check)] ボックスに URL を入力し、[移動 (Go)] をクリックします。

ルックアップ結果を示す Web サイトが表示されます。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。

カテゴリに同意しない場合、FDM で [URL カテゴリの異議を送信する (Submit a URL Category Dispute)] をクリックしてご意見をお聞かせください。

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 [検索エンジンおよびポータル (Search Engines and 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。
- カテゴリが不明な高リスクサイトをブロックする場合は、[未分類 (Uncategorized)] カテゴリを選択し、評価スライダを [疑わしい (Questionable)] または [信頼できない (Untrusted)] に調整します。

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。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 (SSL Decryption)] 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せん。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 (Identity)] 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 (Security Intelligence)] 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 \(108 ページ\)](#) を参照してください。

- [URL フィルタリング (URL Filtering)] 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 (Threat)] 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 (Malware)] 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。マルウェアライセンスを必要とする条件の詳細については、[ファイル ポリシーのライセンス要件 \(104 ページ\)](#) を参照してください。

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。

- URL データベースの更新にカテゴリの追加 (新規、新着)、廃止 (削除予定)、または削除が含まれている場合は、影響を受けるアクセス制御ルールを変更するための猶予期間があります。影響を受けるルールは情報メッセージと一緒にマークされ、メッセージには、ルールに影響する問題についての説明と、カテゴリ変更に関する詳細情報がある Cisco Talos Intelligence Group (Talos) Web サイトへのリンクが記載されます。最新の URL デー

データベースで使用可能な適切なカテゴリを使用するように、ルールを更新する必要があります。

猶予期間に対応するため、廃止された削除予定カテゴリを削除せずに新しく追加された新着カテゴリを適切なルールに追加します。ルールは新旧のカテゴリの両方を含める必要があります。古いカテゴリが削除対象としてマークされると、新しいカテゴリが有効になります。古いカテゴリが最終的に削除されたら、ルールを編集して削除されたカテゴリを除去し、設定を再展開する必要があります。削除されたカテゴリを使用するすべてのルールを修正するまで、設定の展開はブロックされます。注意が必要なルールをフィルタリングするには、テーブルの上の[問題のあるルールを参照 (See Problem Rules)]リンクをクリックします。

- **Firepower Device Manager** はディレクトリ サーバから最大 50,000 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 50,000 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。

50,000 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 50,000 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 50,000 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。
- 完全修飾ドメイン名 (FQDN) ネットワーク オブジェクトを送信元または宛先の基準として使用するには、[デバイス (Device)] > [システム設定 (System Settings)] > [DNS サーバ (DNS Server)] でデータ インターフェイスの DNS も設定する必要があります。システムは、アクセス制御ルールで使用されている FQDN オブジェクトのロックアップを実行するために管理 DNS サーバ設定を使用しません。FQDN 解決のトラブルシューティングについては、[DNS の一般的な問題のトラブルシューティング \(702 ページ\)](#) を参照してください。

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

- DNS 応答はスプーフィングされる可能性があるため、完全に信頼された内部 DNS サーバのみを使用します。
- 一部の FQDN は、特にユーザが非常に多い一般的なサーバの場合、複数の頻繁に変更される IP アドレスを持つことがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザはキャッシュに存在しない新しいアドレスを取得する可能性があります。したがって、ユーザが多い一般的なサイトを FQDN でブロックすると、一貫性のない結果が提供される可能性があります。

- ユーザが多い一般的な FQDN では、異なる DNS サーバが異なるセットの IP アドレスを返す場合があります。したがって、構成したものと異なる DNS サーバをユーザが使用した場合、FQDN ベースのアクセス制御ルールが、クライアントで使用されているサイトのすべての IP アドレスに適用されない可能性があり、ルールに対して意図した結果が得られません。
- 一部の FQDN DNS エントリでは、存続可能時間 (TTL) 値が非常に短い場合があります。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。
- 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、送信元が接続の再確立を試み、新しいルールと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、5508-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。
- テーブルの上の**[ヒットカウントの切り替え (Toggle Hit Counts)]** アイコン (🎯) をクリックし、テーブルの**[ヒットカウント (Hit Count)]** 列を追加または削除します。**[ヒットカウント (Hit Count)]** 列は**[名前 (Name)]** 列の右側にあり、ルールの合計ヒット数と最新のヒットの日付と時刻が表示されます。ヒットカウント情報は、切り替えボタンをクリックしたときに取得されます。最新情報を取得するには、更新アイコン (🔄) をクリックします。
- URL カテゴリの削除または変更などが原因で特定のルールに問題が発生した場合、これらのルールのみを表示するには、検索ボックスの横にある**[問題のあるルールを参照 (See Problem Rules)]** リンクをクリックしてテーブルをフィルタリングします。これらのルールを編集および修正（または削除）して、必要とするサービスが提供されるようになります。

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 \(425 ページ\)](#) 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 \(427 ページ\)](#) 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 \(418 ページ\)](#) 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 \(420 ページ\)](#) 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 \(422 ページ\)](#) を参照してください。
- [ユーザ (Users)] : アイデンティティ ソース、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 \(424 ページ\)](#) 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 \(425 ページ\)](#) 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 \(426 ページ\)](#) 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 \(427 ページ\)](#) 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つを通過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。



- (注) 1つのルールにパッシブセキュリティゾーンとルーテッドセキュリティゾーンを混在させることはできません。また、パッシブセキュリティゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

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。完全修飾ドメイン名 (FQDN) を使用してアドレスを定義するオブジェクトを使用できます。このアドレスは DNS ルックアップによって判別されます。
- [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、信頼できな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。

カテゴリの説明については、<https://www.talosintelligence.com/categories> を参照してください。

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 (Questionable 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、[信頼できない (Untrusted)] (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、[好ましいサイト (Favorable sites)] (レベル 4) を許可するルールを設定した場合、[信頼できる (Trusted)] (レベル 5) サイトも自動的に許可されます。

URL のカテゴリの確認

特定の URL のカテゴリとレピュテーションをチェックすることができます。[確認する URL (URL to Check)] ボックスに URL を入力し、[移動 (Go)] をクリックします。結果を表示するには、外部の Web サイトに移動します。分類に同意しない場合は、[URL カテゴリの異議を送信する (Submit a URL Category Dispute)] リンクをクリックして弊社までお知らせください。

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。

そのソース内のすべてのユーザに適用するアイデンティティソースを選択することもできます。したがって、複数の Active Directory ドメインをサポートする場合は、ドメインに基づくリソースへの差分アクセスを提供できます。

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。

- [アイデンティティソース (Identity Sources)] : AD レalmやローカル ユーザデータベースなど、選択したソースから取得したすべてのユーザにルールを適用するアイデンティティソースを選択します。必要なレalmがまだ存在しない場合、[新規アイデンティティレalmの作成 (Create New Identity Realm)] をクリックして作成します。
- [グループ (Groups)] : 目的の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。
- [ユーザ (Users)] : 個々のユーザを選択します。ユーザ名には、Realm\usernameなどのアイデンティティソースがプレフィックスとして付けられます。

Special-Identities-Realm の下にはいくつかの組み込みユーザがあります。

- [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。

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 \(461 ページ\)](#) 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、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。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、マルウェアアップデートを実行するため、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を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る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る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。
- (カスタム ファイル ポリシー) : FTD API filepolicies リソース、およびその他の FileAndMalwarePolicies リソース (filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections など) を使用して、独自のファイル ポリシーを作成できます。ポリシーを作成して変更を展開した後、FDMでアクセス制御ルールを編集するときにポリシーを選択できます。ポリシーの説明は、選択したときにポリシーの下に表示されます。

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 イベントのロギングを有効にするには、[ファイルのロギング (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。

この設定は、接続イベントにのみ適用されます。syslog 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。Syslog にファイル/マルウェア イベントを送信するには、[デバイス (Device)] > [システム設定 (System Settings)] > [ロギング設定 (Logging Settings)] でサーバを設定します。

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 \(117 ページ\)](#) 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。

ルール ヒット カウントの調査

各アクセス制御ルールのヒットカウントを表示することができます。ヒットカウントは、接続がルールに一致する頻度を示します。この情報を使用して、最もアクティブなルールとアクティブの度合いが低いルールを特定できます。

回数は、アクションまたはシステムアップグレードによってシステムを再起動した最後の時間、またはあるルールまたはすべてのルールのヒットカウントをリセットしたときからカウントされます。

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 [ヒットカウントの切り替え (Toggle Hit Counts)] アイコンをクリックします (🎯)。

[ヒットカウント (Hit Count)] 列は [名前 (Name)] 列の右側にあり、ルールの合計ヒット数と最新のヒットの日付と時刻が表示されます。ヒットカウント情報は、切り替えボタンをクリックしたときに取得されます。

ヒットカウントの情報を使用して、次を行うことができます。

- ボタンの左側には、ヒットカウントが最後に更新されたときの情報が表示されます。最新の数字を取得するには、更新アイコン (🔄) をクリックします。
 - 特定のルールのヒット カウントの詳細表示を開くには、テーブルのヒット カウント番号をクリックして [ヒットカウント (Hit Count)] ダイアログ ボックスを開きます。ヒット カウント情報には、ヒットの回数と、ルールに一致した最後の接続の日付と時刻が含まれます。カウンタをゼロにリセットするには、[リセット (Reset)] リンクをクリックします。
- 一度にすべてのルールのヒットカウントをリセットする場合は、デバイスへの SSH セッションを開き、**clear rule hits** コマンドを発行します。
- 再度 [ヒットカウントの切り替え (Toggle Hit Counts)] アイコン (🎯) をクリックし、テーブルから [ヒットカウント (Hit Count)] 列を削除します。

アクセス制御に関する Syslog メッセージのモニタリング

イベントはイベントビューアで確認するだけでなく、アクセス制御ルール、侵入ポリシー、ファイル/マルウェアポリシー、およびセキュリティインテリジェンスポリシーを設定してイベントを syslog サーバに送信することができます。イベントは、次のメッセージ ID を使用します。

- 430001 : 侵入イベント。
- 430002 : 接続の開始時に記録された接続イベント。
- 430003 : 接続の終了時に記録された接続イベント。
- 430004 : ファイルイベント。
- 430005 : マルウェア イベント。

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 rule hits** は、**show access-control-config** および **show access-list** で表示されるカウントよりも正確な、統合されたヒットカウントを表示します。ヒットカウントをリセットするには、**clear rule hits** コマンドを使用します。
- **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 \(59 ページ\)](#)。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 \(67 ページ\)](#)。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 \(74 ページ\)](#)。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 \(77 ページ\)](#)。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 \(82 ページ\)](#)。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 \(86 ページ\)](#)。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。
- [ネットワーク上のトラフィックをパッシブにモニタする方法 \(93 ページ\)](#)

次に、その他の例を示します。

Trustsec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法

Cisco TrustSec ネットワークでトラフィックを分類するために Cisco Identity Services Engine (ISE) を使用してセキュリティ グループ タグ (SGT) を定義して使用する場合は、一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、直接 IP アドレスではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。

セキュリティ グループ タグ (SGT) について

Cisco Identity Services Engine (ISE) では、セキュリティ グループ タグ (SGT) を作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。また、ユーザアカウントに SGT を割り当て、SGT がユーザのトラフィックに割り当てられるようにすることもできます。ネットワーク内のスイッチおよびルータがそのように設定されている場合、これらのタグは、ISE、Cisco TrustSec クラウドによって制御されるネットワークに入るときにパケットに割り当てられます。

FDM で ISE アイデンティティ ソースを設定すると、FTD システムによって ISE から SGT のリストが自動的にダウンロードされます。その後、アクセス制御ルールでトラフィックの一致条件として SGT を使用できます。

たとえば、実稼働ユーザ タグを作成し、192.168.7.0/24 ネットワークをタグに関連付けることができます。これは、ラップトップや Wi-Fi クライアントなどのユーザエンドポイント用にそのネットワークを使用する場合に適しています。実稼働サーバ用に別のタグを作成し、関連するサーバまたはサブネットの IP アドレスをタグに割り当てることができます。その後 FTD で、タグに基づいてユーザネットワークから実稼働サーバへのアクセスを許可またはブロックすることができます。ISE でタグに関連付けられているホストまたはネットワークアドレスを後で変更する場合、FTD デバイスに定義されているアクセス制御ルールを変更する必要はありません。

FTD は、アクセス制御ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

1. パケット内で定義されている送信元 SGT タグ（存在する場合）。宛先の照合は、この手法では行われません。SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチおよびルータがそれらを追加するように設定されている必要があります。この方法を実装する方法については、ISE のマニュアルを参照してください。
2. ISE セッションディレクトリからダウンロードされるユーザセッションに割り当てられた SGT。この種の SGT 照合を行う場合、セッションディレクトリ情報をリッスンするオプションを有効にする必要がありますが、このオプションは、最初に ISE アイデンティティ ソースを作成するときにデフォルトで有効になっています。SGT は、送信元または宛先と照合することができます。必須ではありませんが、通常はパッシブ認証アイデンティティ ルールを設定し、ISE アイデンティティ ソースを AD レルムとともに使用してユーザ ID 情報を収集します。
3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックは SGT を使用するアクセス制御ルールと一致します。SGT は、送信元または宛先と照合することができます。

ISE は、セキュリティグループ交換プロトコル (SXP) を使用して、IP-to-SGT マッピング データベースをネットワーク デバイスに伝達します。ISE サーバを使用するように FTD デバイスを設定する場合は、ISE から SXP トピックをリッスンするオプションを有効にする必要があります。そのため、FTD デバイスは、セキュリティグループタグとマッピングについて ISE から直接学習し、ISE が更新されたセキュリティグループタグとマッピングを公開するたびに通知を受け取ります。これにより、デバイス上でセキュリティグループタグのリストが最新の状態に維持されるため、FTD は、ISE で定義されたポリシーを効果的に適用できるようになります。

セキュリティグループタグ (SGT) に基づくアクセス制御の設定

セキュリティグループタグ (SGT) を一致基準として使用するアクセス制御ルールを設定するには、最初に ISE サーバから SGT マッピングを取得するようにデバイスを設定する必要があります。

次の手順では、SXPで公開されているSGTからIPアドレスへのマッピングを含めて、ISEで定義されているすべてのマッピングを取得するという前提に基づいたプロセスについて詳しく説明します。または、下記の手順も実行できます。

- パケット内のSGT情報のみを使用し、ISEからダウンロードされたマッピングを使用しない場合は、[ダウンロードされたタグに対するSGT動的オブジェクトの作成 \(440 ページ\)](#) および[SGTに基づくアクセス制御ルールの設定 \(444 ページ\)](#) に定義されている手順を実行します。この場合、送信元条件としてのみSGTタグを使用できます。これらのタグは、宛先の基準に一致しません。
- パケット内部のSGTとユーザセッションのSGTマッピングのみを使用する場合は、ISEアイデンティティソースのSXPトピックをサブスクライブするオプションを有効にする必要はありません。また、SXPマッピングを公開するようにISEを設定する必要もありません。この情報は送信元と宛先の両方の一致条件に使用できます。

始める前に

ここでは、ネットワークでCisco TrustSecがすでに設定されており、FTDデバイスをポリシー適用ポイントとして追加するだけで済むと仮定します。まだCisco TrustSecを展開していない場合は、ISEから作業を開始し、ネットワークを設定してからこの手順に戻ってください。Cisco TrustSecについては、このドキュメントでは説明していません。

手順

-
- ステップ1 [ISEでのセキュリティグループとSXPパブリッシングの設定 \(434 ページ\)](#)。
 - ステップ2 [FDMでのISEアイデンティティソースの設定 \(437 ページ\)](#)。
 - ステップ3 [ダウンロードされたタグに対するSGT動的オブジェクトの作成 \(440 ページ\)](#)。
 - ステップ4 [SGTに基づくアクセス制御ルールの設定 \(444 ページ\)](#)。
-

ISEでのセキュリティグループとSXPパブリッシングの設定

Cisco Identity Services Engine (ISE) では、TrustSecポリシーとセキュリティグループタグ (SGT) を作成するために実行を必要とする設定が多数あります。TrustSecの実装の詳細については、ISEのマニュアルを参照してください。

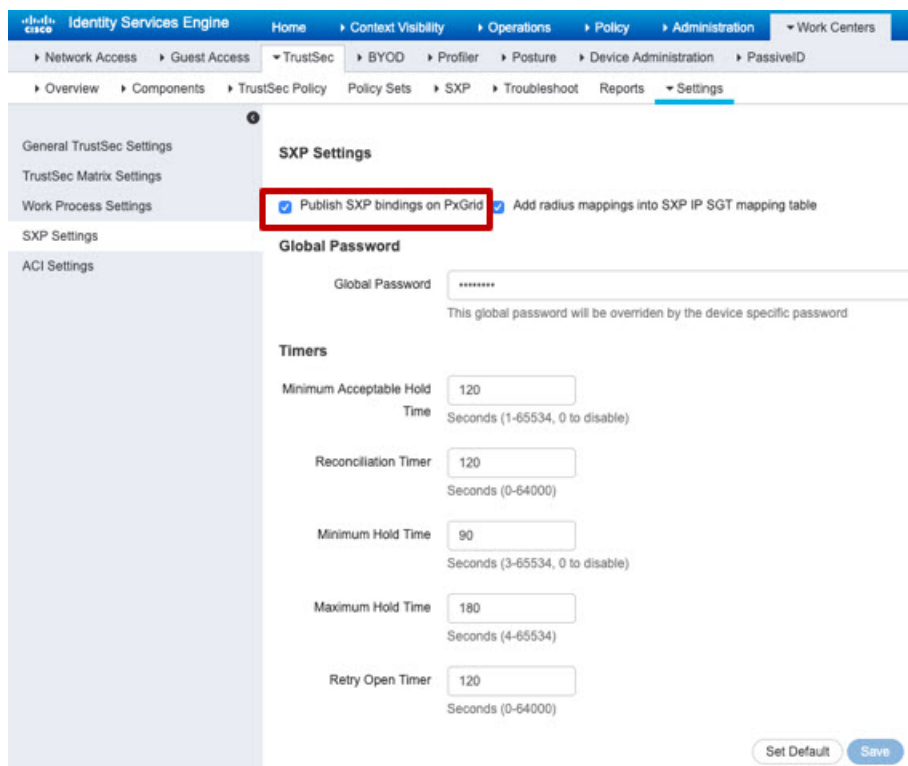
次の手順では、FTDデバイスがスタティックSGTからIPアドレスへのマッピングをダウンロードして適用できるようにするためにISEで設定する必要があるコア設定のうち、重要な部分を示します。この後、これらのマッピングを使用して、アクセスコントロールルールで送信元と宛先のSGT照合を実行できます。詳細については、ISEのマニュアルを参照してください。

この手順のスクリーンショットは、ISE 2.4に基づいています。これらの機能にアクセスするための正確な手順は後続のリリースで変更される可能性があります。概念と要件は同じです。ISE 2.4以降を推奨しますが、設定はISE 2.2パッチ1以降で動作します。

手順

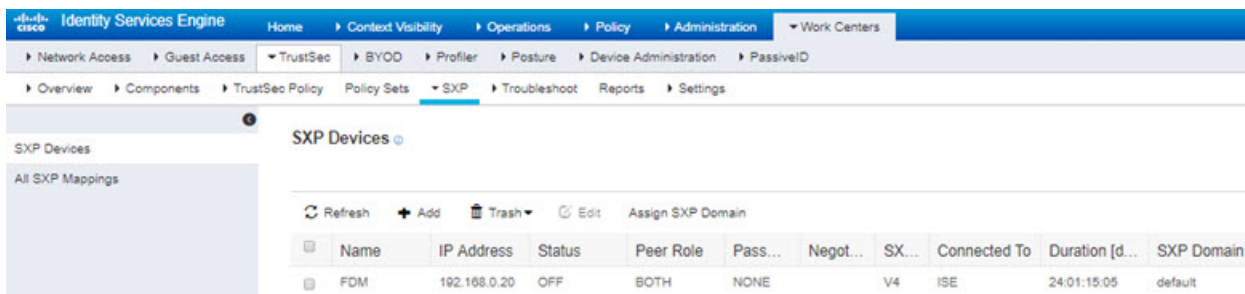
ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [SXP設定 (SXP Settings)] を選択し、[PxGridでSXPバインディングを公開 (Publish SXP Bindings on PxGrid)] オプションを選択します。

このオプションにより、ISE は SXP を使用して SGT マッピングを送出します。FTD デバイスがリストから SXP トピックに送られるものすべてを「傍受」できるようにする場合は、このオプションを選択する必要があります。FTD デバイスがスタティック SGT から IP アドレスへのマッピング情報を取得できるようにする場合は、このオプションを選択する必要があります。単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、必要ありません。

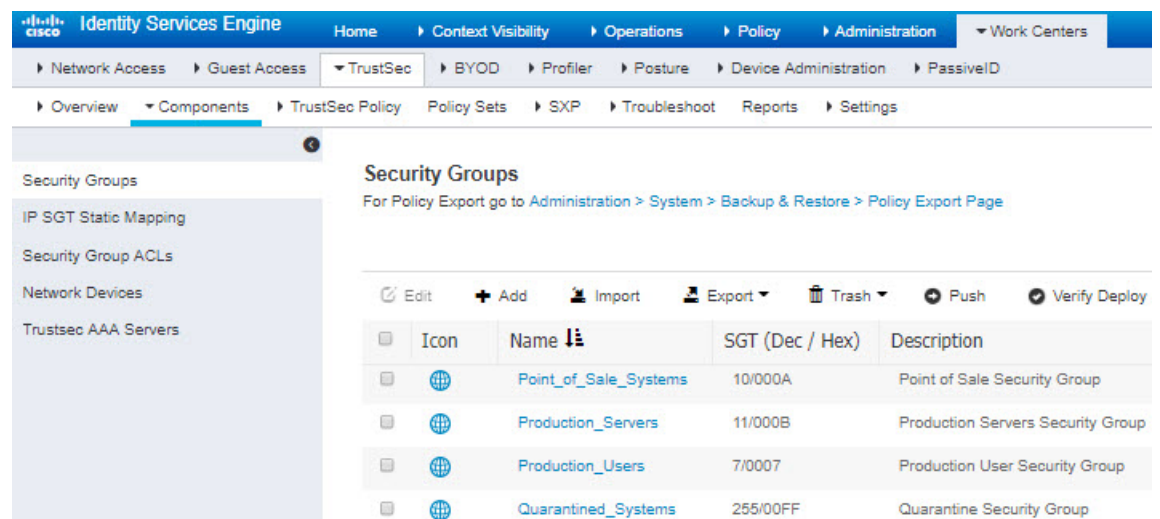


ステップ 2 [ワークセンター (Work Centers)] > [TrustSec] > [SXP] > [SXPデバイス (SXP Devices)] を選択し、デバイスを追加します。

これは実際のデバイスである必要はありませんが、FTD デバイスの管理 IP アドレスを使用することもできます。この表では、ISE がスタティック SGT から IP アドレスのマッピングを公開するために、デバイスが少なくとも 1 台必要です。単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

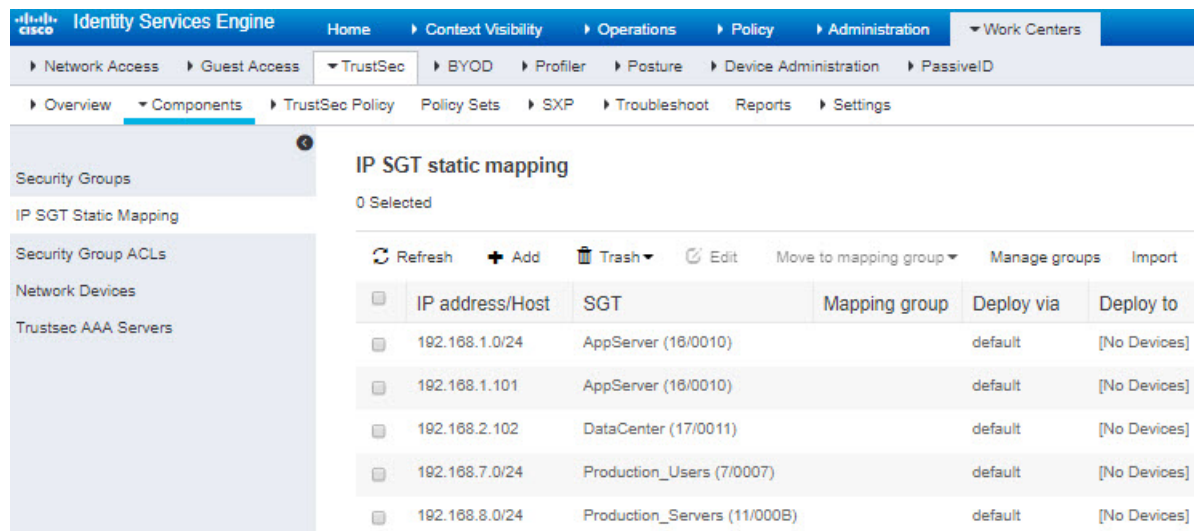


ステップ3 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ (Security Groups)] を選択し、セキュリティグループタグが定義されていることを確認します。必要に応じて新しいものを作成します。



ステップ4 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [IP SGT スタティックマッピング (IP SGT Static Mapping)] を選択し、ホストとネットワーク IP アドレスをセキュリティグループタグにマッピングします。

単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。



FDM での ISE アイデンティティ ソースの設定

ISE を使用して、ユーザセッション SGT マッピング、SXP を介したスタティック SGT から IP アドレスへのマッピング、またはその両方を取得できます。デフォルトでは、ISE アイデンティティ ソースを設定すると、ユーザセッションマッピングのみが取得されます。ISE から SXP トピックをリッスンするには、オプションを有効にする必要があります。

手順

- ステップ 1** FDM で、[Identity Services Engine の設定 \(193 ページ\)](#) の説明に従って ISE アイデンティティ オブジェクトを作成します。

AD レルムの設定は SXP の設定では必要ありませんが、ISE からユーザアイデンティティを取得する場合は AD サーバが必要です。
- ステップ 2** 変更を展開します。

この時点では必ずしも変更を展開する必要はありませんが、トラブルシューティングを簡素化する目的で API メソッドの使用を始める場合は、事前に FDM の変更を展開しておくことをお勧めします。ただし、アクセス制御ルールの場合など、FDM で部分的な設定を作成する場合は例外です。オブジェクトが設定途中の状態を展開されると正常な動作に干渉します。
- ステップ 3** [詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。

ブラウザの設定に応じて、API エクスプローラが別のタブまたはウィンドウで開きます。
- ステップ 4** [IdentityServicesEngine] をクリックしてフォルダを開き、使用可能なメソッドを確認します。
- ステップ 5** FDM で作成した ISE アイデンティティ オブジェクトを取得します。

- a) [GET /integration/identityservicesengine] メソッドをクリックします。
- b) メソッドの説明の最後にある [試してみる (Try It Out!)] ボタンをクリックします。

GET 呼び出しが送信され、ISE アイデンティティオブジェクトが正常に取得されます。[応答本文 (Response Body)] フィールドにオブジェクトが表示されます。[戻りコード (Return Code)] として 200 を探します。それ以外の結果が表示された場合は、応答本文にエラーメッセージがないか調べ、ISE アイデンティティ ソースを再度作成してみてください。

- c) クリックしてドラッグし、Ctrl + C を使用して、オブジェクト本体をクリップボードにコピーします。“items [” ブラケットの後ろにある最初の波カッコ { から、終わりのブラケット] の直前にある閉じカッコ } までをコピーします。“items” を含む行と、“items” の前の行、および最後のページング属性を残しておきます。オブジェクトの最初の属性は“version”で、最後の属性は“self”です。

次に例を示します。次のステップに必要な属性を強調表示しています。

```
{
  "version": "kbpeihi5cbarm",
  "name": "ISE",
  "description": null,
  "ftdCertificate": {
    "version": "epnkrwowkuhgk",
    "name": "ISE",
    "id": "565b03fd-8874-11e9-87fd-29bbc348546c",
    "type": "internalcertificate"
  },
  "pxGridCertificate": {
    "version": "pyzuuw7ja6coq",
    "name": "ISE_CA",
    "id": "5cf3b4b0-8874-11e9-87fd-6b0eb83b0b10",
    "type": "externalcacertificate"
  },
  "mntCertificate": {
    "version": "pyzuuw7ja6coq",
    "name": "ISE_CA",
    "id": "5cf3b4b0-8874-11e9-87fd-6b0eb83b0b10",
    "type": "externalcacertificate"
  },
  "iseNetworkFilters": [],
  "enabled": true,
  "subscribeToSessionDirectoryTopic": true,
  "subscribeToSxpTopic": false,
  "secondaryIseServer": null,
  "primaryIseServer": "192.168.0.9",
  "id": "8252f773-8874-11e9-87fd-67c87c391f4d",
  "type": "identityservicesengine",
  "links": {
    "self": "https://ftd.example.com/api/fdm/v3/integration/identityservicesengine/8252f773-8874-11e9-87fd-67c87c391f4d"
  }
}
```

- (注) ISE アイデンティティ ソースを作成すると、subscribeToSessionDirectoryTopic がデフォルトで true に設定されます。この属性によって、ユーザセッションの SGT マッピングを取得するかどうかが決まります。スタティック SGT から IP アドレスへのマッピングのみを使用し、ユーザセッションの SGT 情報を必要としない場合は、このオプションを false に設定できます。

ステップ 6 PUT を使用してオブジェクトを更新し、ISE の SXP トピックに登録するオプションを有効にします。

デフォルトでは、**subscribeToSxpTopic** 属性は **false** に設定されています。これを **true** に設定する必要があります。

- [PUT /integration/identityservicesengine/{objId}] メソッドをクリックします。
- オブジェクトの現在のバージョンを **body** パラメータの編集ボックスに貼り付け、リンク属性を（その中の **self** 属性を含めて）削除します。
- SubscribeToSxpTopic** 属性値を **true** に変更します。

```
...
"subscribeToSessionDirectoryTopic": true,
"subscribeToSxpTopic": true,
"secondaryIseServer": null,
...
```

この属性を **true** に設定すると、SGT から IP へのアドレス マッピングがダウンロードされます。これを **true** に設定しないと、ISE で定義されているスタティック SGT から IP アドレスへのマッピングが取得されません。これらのマッピングに基づいてアクセス制御を適用できなくなります。

- オブジェクトの **id** 属性の値をコピーします。4つの **id** 属性があり、それぞれが **ftdCertificate**、**pxGridCertificate**、**mntCertificate**、および ISE オブジェクトに対応していることに注意してください。オブジェクトの **id** は、**"type": "identityservicesengine"** 属性の直前に表示される最後の **id** です。
- このオブジェクト **id** を、**body** パラメータのすぐ上にある **objId** パラメータに貼り付けます。開き/閉じカッコは含めないでください。

Parameter	Value
objId	8252f773-8874-11e9-87fd-67c87c391f4d
body	<pre>"subscribeToSxpTopic": true, "secondaryIseServer": null, "primaryIseServer": "192.168.0.9", "id": "8252f773-8874-11e9-87fd-67c87c391f4d", "type": "identityservicesengine", "links": { "self": "https://ast0140-</pre>

Parameter content type: application/json ▼

- [試してみる (Try It Out!)] ボタンをクリックします。呼び出しが成功すると応答コード 200 が返され、変更が適用された新しいオブジェクトが応答本文に表示されます。

次に例を示します。

```
{
  "version": "117jndfp2qriq",
  "name": "ISE",
  "description": null,
```

ダウンロードされたタグに対する SGT 動的オブジェクトの作成

```

    "ftdCertificate": {
      "version": "epnkrwowkuhgk",
      "name": "ISE",
      "id": "565b03fd-8874-11e9-87fd-29bbc348546c",
      "type": "internalcertificate"
    },
    "pxGridCertificate": {
      "version": "pyzuuw7ja6coq",
      "name": "ISE_CA",
      "id": "5cf3b4b0-8874-11e9-87fd-6b0eb83b0b10",
      "type": "externalcacertificate"
    },
    "mntCertificate": {
      "version": "pyzuuw7ja6coq",
      "name": "ISE_CA",
      "id": "5cf3b4b0-8874-11e9-87fd-6b0eb83b0b10",
      "type": "externalcacertificate"
    },
    "iseNetworkFilters": [],
    "enabled": true,
    "subscribeToSessionDirectoryTopic": true,
    "subscribeToSxpTopic": true,
    "secondaryIseServer": null,
    "primaryIseServer": "192.168.0.9",
    "id": "8252f773-8874-11e9-87fd-67c87c391f4d",
    "type": "identityservicesengine",
    "links": {
      "self": "https://ftd.example.com/api/fdm/v3/integration/identityservicesengine/8252f773-8874-11e9-87fd-67c87c391f4d"
    }
  }
}

```

ステップ 7 FDM のウィンドウに戻り、変更を展開します。

ダウンロードされたタグに対する SGT 動的オブジェクトの作成

ISE アイデンティティ ソースを設定して変更を展開すると、ISE サーバからセキュリティ グループ タグ (SGT) 情報が取得されます。

ただし、ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT ダイナミック オブジェクトを作成する必要があります。SGT ダイナミック オブジェクトは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

手順

ステップ 1 [詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。

ステップ 2 ISE からダウンロードした SGT 情報を表示します。

- a) [SecurityGroupTag] をクリックしてフォルダを開き、使用可能なメソッドを確認します。
- b) [GET /object/securitygrouptags] メソッドをクリックします。
- c) メソッドの説明の最後にある [試してみる (Try It Out!)] ボタンをクリックします。

GET 呼び出しが送信され、ISE から取得した SGT 情報が正常に取得されます。この情報はタグのリストのみであり、IP アドレスのマッピングは含まれていません。応答本文に SGT 情報が表示され、応答コードは 200 になります。

デフォルトでは、GET 呼び出しによる情報は最初の 10 個のオブジェクトに制限されることに注意してください。

応答本文の一番下までスクロールし、ページング情報を確認します。次に例を示します。

```
"paging": {
  "prev": [],
  "next": [
    "https://ftd.example.com/api/fdm/v3/object/
    securitygrouptags?limit=10&offset=10"
  ],
  "limit": 10,
  "offset": 0,
  "count": 119,
  "pages": 0
}
```

この例では最初の 10 個の SGT のみが表示されていますが、合計 119 個の SGT (**count** 属性) がダウンロードされています。SGT の合計数は、ISE サーバで設定されている個数によって異なります。

- d) 完全なリストを取得するには、**limit** パラメータ値が表示されるまで上にスクロールして 120 を入力し、再度 [試してみる (Try It Out!)] をクリックします。

これで、120 の制限、119 の個数、および「ページなし」がページング属性に表示されるようになりました。

```
"paging": {
  "prev": [],
  "next": [],
  "limit": 120,
  "offset": 0,
  "count": 119,
  "pages": 0
}
```

応答本文をコピーしてテキストファイルに貼り付けることもできます。そうすることで、リストを簡単に確認でき、アクセス コントロール ポリシーの実装を必要とする SGT ダイナミック オブジェクトについて計画を立てられるようになります。

ステップ 3 必要な SGT ダイナミック オブジェクトを作成します。

SGT ごとに SGT ダイナミック オブジェクトを作成する必要はありません。必要なのはアクセス 制御ルールで使用するオブジェクトのみです。

この例では、ISE からダウンロードされた次の 2 つの SGT について考えます。

```
{
  "tag": 11,
  "name": "Production_Servers",
  "description": "Production Servers Security Group",
  "deleted": false,
  "id": "9423aa00-8c01-11e6-996c-525400b48521",
}
```

```

    "type": "securitygrouptag",
    "links": {
      "self": "https://ftd.example.com/api/fdm/v3/object/
securitygrouptags/9423aa00-8c01-11e6-996c-525400b48521"
    }
  },
  {
    "tag": 7,
    "name": "Production_Users",
    "description": "Production User Security Group",
    "deleted": false,
    "id": "9437a730-8c01-11e6-996c-525400b48521",
    "type": "securitygrouptag",
    "links": {
      "self": "https://ftd.example.com/api/fdm/v3/object/
securitygrouptags/9437a730-8c01-11e6-996c-525400b48521"
    }
  }
},

```

目的は、Production_Users セキュリティグループ (SGT 7) から Production_Servers セキュリティグループ (SGT 11) へのトラフィックを許可することです。これらの SGT は送信元と宛先の基準として個別に指定する必要があるため、2つの SGT ダイナミック オブジェクトが必要になります。オブジェクトを作成する手順は次のようになります。

- [SGTDynamicObject] をクリックしてフォルダを開き、使用可能なメソッドを確認します。
- [POST /object/sgtdynamicobjects] メソッドをクリックします。
- [パラメータ (Parameters)] セクションで、右側の [値の例 (Example Value)] 編集ボックスをクリックし、[データタイプ (Data Type)] 列で、[本文 (body)] 編集ボックスに例をロードします。
- バージョンと id の属性行を削除し、次のように他の属性を定義します。

```

{
  "name": "Production_Users_DSGT",
  "tags": [
    {
      "tag": 7,
      "externalId": "9437a730-8c01-11e6-996c-525400b48521",
      "type": "securitygrouptagentry"
    }
  ],
  "type": "sgtdynamicobject"
}

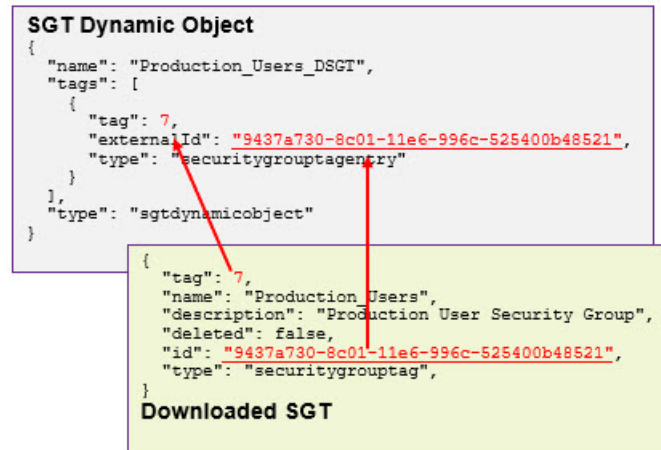
```

その属性は次のとおりです。

- name** : タグ自体の名前ではなく、SGT ダイナミック オブジェクトの名前。たとえば、Production_Users_DSGT とします。
- tags** : ISE からダウンロードしたタグを1つ以上指定できます。ダイナミック オブジェクトで複数の SGT を参照するには、{カッコ} 内の属性をコピーして貼り付け、各属性セットをカンマで区切ります。セットの **tags** [カッコ] 内はそのままにします。各タグには次の属性が必要です。
 - tag** : ISE で定義され、ダウンロードされた SGT のリストの tag 属性に表示される SGT タグ番号。この例では、7 です。

- **externalId** : ダウンロードされた SGT の **id** 値。ダウンロードされたリストには、FTD ではなく ISE で設定された項目が反映されるため、これは「外部」になります。この例では、9437a730-8c01-11e6-996c-525400b48521 です。
- **type** : これは常に **securitygroupentry** です。

次の図は、ダウンロードされたタグの属性と SGT ダイナミック オブジェクトの属性との関係を示しています。



- e) [試してみる (Try It Out!)] をクリックします。

POST が正常に完了すると、応答コード 200 と応答本文が新しいオブジェクトとともに生成されます。次に例を示します。

```

{
  "version": "odswykttumaao",
  "name": "Production_Users_DSGT",
  "tags": [
    {
      "tag": 7,
      "externalId": "9437a730-8c01-11e6-996c-525400b48521",
      "type": "securitygroupentry"
    }
  ],
  "id": "ba09cd90-8959-11e9-87fd-a7644255b0cd",
  "type": "sgtdynamicobject",
  "links": {
    "self": "https://ftd.example.com/api/fdm/v3/object/sgtdynamicobjects/ba09cd90-8959-11e9-87fd-a7644255b0cd"
  }
}

```

- f) 手順を繰り返して、実稼働サーバ用の SGT ダイナミック オブジェクトを作成します。POST 呼び出しの本文を、新しいオブジェクトに必要な本文に置き換え、[試してみる (Try It Out!)] をクリックします。

```

{
  "name": "Production_Servers_DSGT",
  "tags": [

```

```

    {
      "tag": 11,
      "externalId": "9423aa00-8c01-11e6-996c-525400b48521",
      "type": "securitygrouptagentry"
    }
  ],
  "type": "sgtdynamicobject"
}

```

応答本文は次のようになります。

```

{
  "version": "hbfqoryvvhz5xj",
  "name": "Production_Servers_DSGT",
  "tags": [
    {
      "tag": 11,
      "externalId": "9423aa00-8c01-11e6-996c-525400b48521",
      "type": "securitygrouptagentry"
    }
  ],
  "id": "eeede223-895a-11e9-87fd-31336e1d6199",
  "type": "sgtdynamicobject",
  "links": {
    "self": "https://ftd.example.com/api/fdm/v3/object/sgtdynamicobjects/eeede223-895a-11e9-87fd-31336e1d6199"
  }
}

```

- g) (オプション) **GET /object/sgtdynamicobjects** を使用して、両方の SGT ダイナミック オブジェクトが作成されたことを確認できます。

SGTに基づくアクセス制御ルールの設定

ISE サーバに接続するよう FTD を設定し、SGT ダイナミック オブジェクトを作成した後、SGT ダイナミック オブジェクトを使用するためのアクセス制御ルールを作成できます。

SGT ダイナミック オブジェクトをアクセスルールに追加するには、FTD API を使用する必要があります。ただし、最初のルール オブジェクトを作成する場合は、まず FDM を使用してルールを作成し、必要な他のすべての属性を指定し、API を使用して SGT 基準を追加するだけで、作業を簡単にすることができます。必要に応じて、API を使用してルール全体を最初から作成することもできます。

次の手順では、FDM を使用して基本ルールを作成した後、SGT ダイナミック オブジェクトをトラフィック一致基準として追加する方法について説明します。このルールにより、実稼働ユーザから実稼働サーバへのトラフィックが許可されます。ルールは SGT に完全に依存しません。送信元/宛先インターフェイスやその他の基準によって制限を受けることはありません。そのため、ルールはさまざまなインターフェイスからのトラフィックに動的に適用され、ISE でセキュリティグループのメンバーシップを変更するときに適用されます。パケットに送信元 SGT タグが明示的に含まれていない場合は、パケットの IP アドレスを、ユーザセッション情報または SXP 公開マッピングから取得される、SGT から IP アドレスへのマッピングと比較することによって、送信元/宛先の照合が行われます。

始める前に

ルールに追加する SGT ダイナミック オブジェクトの属性がわかっている必要があります。オブジェクトごとの属性と値ペアのコピーがない場合は、ここで **GET /object/sgtdynamicobjects** を使用して情報を取得します。ダウンロードされたタグに対する SGT 動的オブジェクトの作成 (440 ページ) を参照してください。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。

ステップ 2 [+] をクリックして新しいルールを追加し、次のフィールドを設定します。

- [順序 (Order)] : ルールを挿入する位置を選択します。デフォルトでは、ポリシーの最後に追加されます。必要に応じて後でルールを移動することができます。
- [名前 (Name)] : ルールの名前 (たとえば、ProductionServers など) 。
- [アクション (Action)] : [許可 (Allow)] を選択します。
- [ロギング (Logging)] タブ、[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。ダッシュボードにトラフィック統計情報を表示する場合は、ロギングを有効にする必要があります。情報を表示しない場合は、ロギングを無効にしておくことができます。
- その他のすべてのタブ : この例では、これらの設定をデフォルトのままにして、トラフィックが SGT または SGT から IP アドレスへのマッピングのみに基づいてルールに一致するようにします。これらについても具体的なニーズに合わせて設定できます。たとえば、URL フィルタリングを追加できます。脅威からの保護を目的として侵入ポリシーを適用することもできます。

(注) まだ変更を展開しないでください。このルールは、API エクスプローラで編集するまで完成しません。ここで展開した場合、意図しない結果になります。

ステップ 3 [詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。

ステップ 4 新しいルールを編集して SGT 基準を追加します。

- a) [AccessPolicy] をクリックしてフォルダを開き、使用可能なメソッドを確認します。
- b) [GET /policy/accesspolicies/{parentId}/accessrules] をクリックし、次のパラメータを設定します。
 - **parentId** : 「default」と入力します。アクセス コントロール ポリシーは 1 つしか設定できないため、ポリシー オブジェクトの実際の UUID の代わりに **default** を使用できます。
 - **offset**、**limit** : アクセス ルールのリストが大きい場合、ルール オブジェクトが見つけにくくなる場合があります。選択肢の 1 つとして、ルールの順序番号より 1 小さい値をオフセットとして入力し、**limit** には 1 を指定します。たとえば、ルールの順序が 2

の場合はオフセットを 1 (2-1=1) にします。これで、1 つのルールがポリシー内のその順序で返されます (オフセット変数は 1 からではなく 0 から始まるため、ルールの順序から 1 を差し引く必要があります)。

- c) [試してみる (Try It Out!)] をクリックします。

応答本文で新しいルールのオブジェクトを検索します。たとえば、offset/limit の方法を使用した応答本文は次のようになります。この例で、ページング属性のカウントには、アクセスコントロールポリシーに合計 2 つのルールがあることが示されていますが、ここでは 1 つのルールが表示されています。

```
{
  "items": [
    {
      "version": "bfd2jm5cmv3h2",
      "name": "ProductionServers",
      "ruleId": 268435458,
      "sourceZones": [],
      "destinationZones": [],
      "sourceNetworks": [],
      "destinationNetworks": [],
      "sourcePorts": [],
      "destinationPorts": [],
      "ruleAction": "PERMIT",
      "eventLogAction": "LOG_BOTH",
      "identitySources": [],
      "users": [],
      "embeddedAppFilter": null,
      "urlFilter": {
        "urlObjects": [],
        "urlCategories": [],
        "type": "embeddedurlfilter"
      },
      "intrusionPolicy": null,
      "filePolicy": null,
      "logFiles": false,
      "syslogServer": null,
      "destinationDynamicObjects": [],
      "sourceDynamicObjects": [],
      "id": "8d5e1db6-895d-11e9-87fd-894b42e34ebf",
      "type": "accessrule",
      "links": {
        "self": "https://ftd.example.com/api/fdm/v3/policy/accesspolicies/default/accessrules/8d5e1db6-895d-11e9-87fd-894b42e34ebf"
      }
    }
  ],
  "paging": {
    "prev": [],
    "next": [],
    "limit": 1,
    "offset": 1,
    "count": 2,
    "pages": 0
  }
}
```

- d) ルール オブジェクトをテキスト エディタ (**PUT /policy/accesspolicies/{parentId}/accessrules/{objId}** メソッドの **body** パラメータ) にコピー

して貼り付け、SGTダイナミックオブジェクトを送信元および宛先の基準として追加します。

フィールドは **destinationDynamicObjects**（宛先基準の場合）および **sourceDynamicObjects**（送信元基準の場合）です。各属性はカンマ区切りのオブジェクトのリストを受け取ることができるため、送信元または宛先の基準に複数の SGT ダイナミック オブジェクトを含めることができます。

リスト内の各オブジェクトには次の属性を持たせる必要があります。属性は **GET /object/sgtdynamicobjects** の応答本文から取得できます。これらの属性は、オブジェクトの識別はしますが、オブジェクトの内容は定義しません。

```
{
  "version": "string",
  "name": "string",
  "id": "string",
  "type": "sgtdynamicobject"
}
```

[ダウンロードされたタグに対する SGT 動的オブジェクトの作成 \(440 ページ\)](#) で作成したオブジェクトを使用して、Destinationdynamicobjects に Production_Servers_DSGT を追加し、Sourcedestinationobjects に Production_Users_DSGT を追加すると、次のようになります（変更部分を強調表示しています）。

```
{
  "version": "bfd2jm5cmv3h2",
  "name": "ProductionServers",
  "ruleId": 268435458,
  "sourceZones": [],
  "destinationZones": [],
  "sourceNetworks": [],
  "destinationNetworks": [],
  "sourcePorts": [],
  "destinationPorts": [],
  "ruleAction": "PERMIT",
  "eventLogAction": "LOG_BOTH",
  "identitySources": [],
  "users": [],
  "embeddedAppFilter": null,
  "urlFilter": {
    "urlObjects": [],
    "urlCategories": [],
    "type": "embeddedurlfilter"
  },
  "intrusionPolicy": null,
  "filePolicy": null,
  "logFiles": false,
  "syslogServer": null,
  "destinationDynamicObjects": [
    {
      "version": "hbfqoryvhz5xj",
      "name": "Production_Servers_DSGT",
      "id": "eeede223-895a-11e9-87fd-31336e1d6199",
      "type": "sgtdynamicobject"
    }
  ],
  "sourceDynamicObjects": [
    {
```

```

    "version": "odswykttumaeo",
    "name": "Production_Users_DSGT",
    "id": "ba09cd90-8959-11e9-87fd-a7644255b0cd",
    "type": "sgtdynamicobject"
  }
],
"id": "8d5e1db6-895d-11e9-87fd-894b42e34ebf",
"type": "accessrule"
}

```

- e) [PUT /policy/accesspolicies/{parentId}/accessrules/{objId}] をクリックしてメソッドを開きます。
- f) 次の属性を設定します。
- **parentId** : 「default」と入力します。
 - **objectId** : 新しいアクセス ルール オブジェクトからの **id** 値を入力します。前述の例では、8d5e1db6-895d-11e9-87fd-894b42e34ebf です。これは、“type”:“accessrule” 属性の直前の id 属性です。
 - **body** : 更新された destinationDynamicObject および sourceDynamicObject プロパティを使用して本文に貼り付けます。
- g) [試してみる (Try It Out!)] をクリックします。

422 (処理不可能なエンティティ (Unprocessable Entity)) エラーは、スペルミスを示します。応答本文でエラーメッセージを確認します。たとえば、開き/閉じ波カッコ、ブラケット、丸カッコが一致していない、本来あってはならない場所にカンマがある、などのミスを確認します。実際は、該当する問題が不要なカンマであるときに、必要なカッコに関するメッセージが表示されることがあります。これは、カンマの存在によりパーサーがカッコの存在を想定するためです。

正常な結果として返されるのは 200 応答コードです。正常な応答本文は次のようになります。

```

{
  "version": "kugnhxghj2ubx",
  "name": "ProductionServers",
  "ruleId": 268435458,
  "sourceZones": [],
  "destinationZones": [],
  "sourceNetworks": [],
  "destinationNetworks": [],
  "sourcePorts": [],
  "destinationPorts": [],
  "ruleAction": "PERMIT",
  "eventLogAction": "LOG_BOTH",
  "identitySources": [],
  "users": [],
  "embeddedAppFilter": null,
  "urlFilter": {
    "urlObjects": [],
    "urlCategories": [],
    "type": "embeddedurlfilter"
  },
  "intrusionPolicy": null,
  "filePolicy": null,

```



```

"logFiles": false,
"syslogServer": null,
"destinationDynamicObjects": [
  {
    "version": "hbfgoryvzh5xj",
    "name": "Production_Servers_DSGT",
    "id": "eeede223-895a-11e9-87fd-31336e1d6199",
    "type": "sgtdynamicobject"
  }
],
"sourceDynamicObjects": [
  {
    "version": "odswyktumaeo",
    "name": "Production_Users_DSGT",
    "id": "ba09cd90-8959-11e9-87fd-a7644255b0cd",
    "type": "sgtdynamicobject"
  }
],
"id": "8d5e1db6-895d-11e9-87fd-894b42e34ebf",
"type": "accessrule",
"links": {
  "self": "https://ftd.example.com/api/fdm/v3/policy/
accesspolicies/default/accessrules/8d5e1db6-895d-11e9-87fd-894b42e34ebf"
}
}

```

ステップ 5 FDM のウィンドウに戻り、変更を展開します。

[保留中の変更 (Pending Changes)] ウィンドウに、更新されたアクセスルールと SGT の変更が表示されます。SGT ダイナミック オブジェクトをまだ展開していない場合は、それらも表示されます。

+ Access Rule Added: *ProductionServers*

-	logFiles: false
-	ruleId: 268435458
-	name: ProductionServers
destinationDynamicObjects:	
-	Production_Servers_DSGT
sourceDynamicObjects:	
-	Production_Users_DSGT

+ SGT Dynamic Object Added: *Production_Users_DSGT*

-	tags[0].tag: 7
-	tags[0].externalId: 9437a730-8c01-11e6-996c-525400b48521
-	name: Production_Users_DSGT

⌘ Access Policy Edited: *NGFW-Access-Policy*

+ SGT Dynamic Object Added: *Production_Servers_DSGT*

-	tags[0].tag: 11
-	tags[0].externalId: 9423aa00-8c01-11e6-996c-525400b48521
-	name: Production_Servers_DSGT

変更履歴には FTD API を使用して行った変更が表示されますが、FDM でルールを編集するときに SGT 情報を表示することはできません。



第 17 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（451 ページ）](#)
- [侵入ポリシーのためのライセンス要件（459 ページ）](#)
- [侵入ポリシーの管理（460 ページ）](#)
- [侵入ポリシーのモニタリング（463 ページ）](#)
- [侵入ポリシーの例（463 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 \(715 ページ\)](#) 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 \(454 ページ\)](#) 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 \(455 ページ\)](#) 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。

アクション

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 (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。

ステータス

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

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 9: 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す。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 \(108 ページ\)](#) 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 \(459ページ\)](#) 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 \(453 ページ\)](#) 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。

侵入イベントのメッセージ ID は 430001 です。

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 \(117ページ\)](#) 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 syslog サーバを設定した場合、侵入イベントのメッセージ ID は 430001 です。

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 \(67 ページ\)](#)
- [ネットワーク上のトラフィックをパッシブにモニタする方法 \(93 ページ\)](#)



第 18 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 \(465 ページ\)](#)
- [NAT の基本 \(466 ページ\)](#)
- [NAT のガイドライン \(474 ページ\)](#)
- [NAT の設定 \(479 ページ\)](#)
- [IPv6 ネットワークの変換 \(513 ページ\)](#)
- [NAT のモニタリング \(528 ページ\)](#)
- [NAT の例 \(528 ページ\)](#)

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

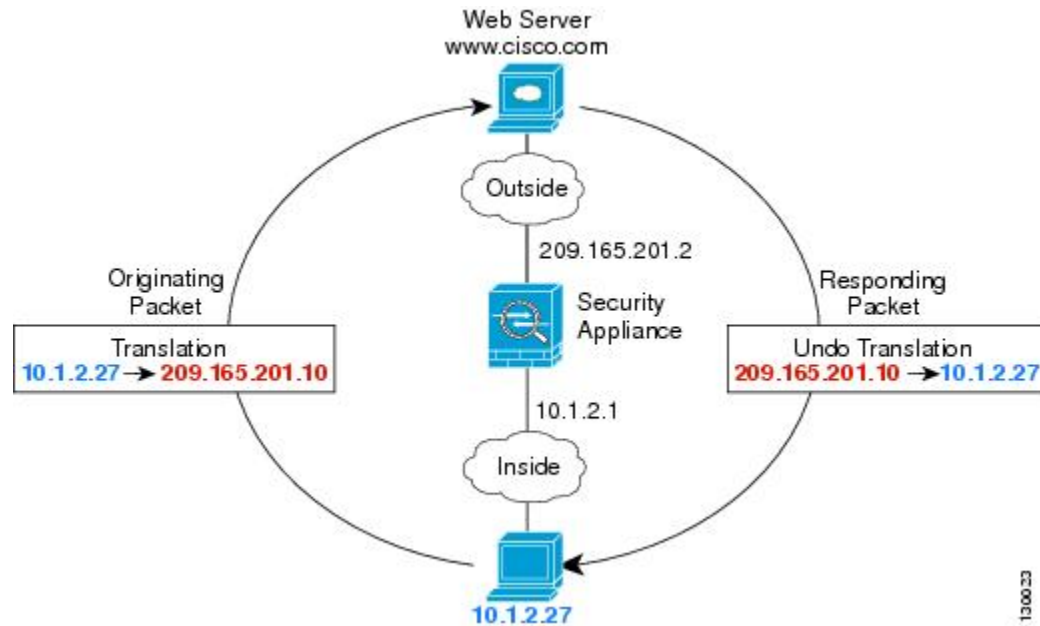
NAT は、次の方法を使用して実装できます。

- 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 \(480 ページ\)](#) 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 \(486 ページ\)](#) 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 \(492 ページ\)](#) 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 \(502 ページ\)](#) 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 12: 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. 応答時、サーバはマッピングアドレス 209.165.201.10 に応答を送信します。Firepower Threat Defense デバイスはプロキシ ARP を実行してパケットを要求するため、Firepower Threat Defense デバイスがパケットを受信します。
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 10: 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。

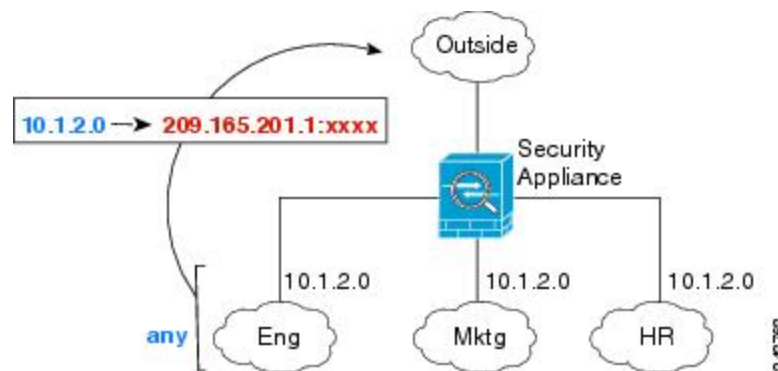
- 192.168.1.1/32 (スタティック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

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 13: 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。

パッシブインターフェイスでは NAT を設定できません。

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 デバイスをポイントす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ため、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 11: 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を使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。



(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 \(467 ページ\)](#)」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 \(468 ページ\)](#)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 \(480 ページ\)](#)
- [ダイナミック PAT \(486 ページ\)](#)
- [スタティック NAT \(492 ページ\)](#)
- [アイデンティティ NAT \(502 ページ\)](#)

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

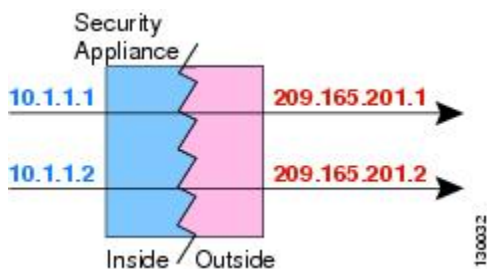
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、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。

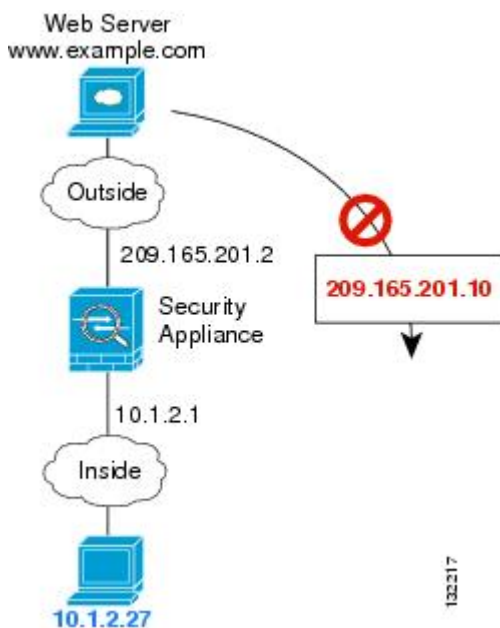
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 14: 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 15: 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、範囲、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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

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 ([すべて (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 \(549 ページ\)](#) 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、範囲、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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

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。

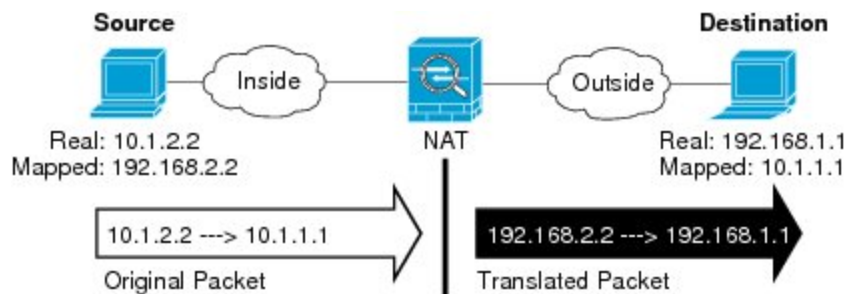
ステップ 4 次のインターフェイス オプションを設定します。

- [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 ([すべて (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。



- [元の送信元アドレス (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。
- [元の宛先アドレス (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 \(549 ページ\)](#) 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。

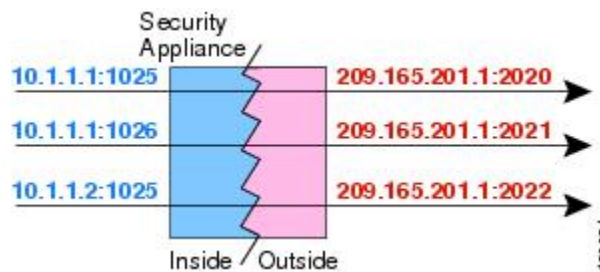
ダイナミック PAT について

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 16: 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 \(475 ページ\)](#) 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、範囲、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 ([すべて (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、範囲、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。

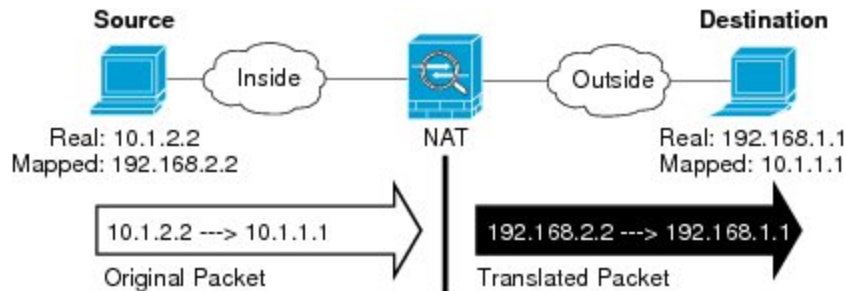
ステップ 4 次のインターフェイス オプションを設定します。

- [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 ([すべて (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。



- [元の送信元アドレス (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。
- [元の宛先アドレス (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

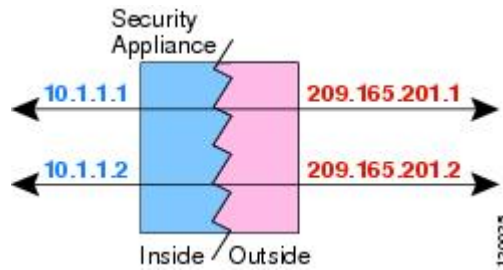
ここでは、スタティック NAT とその実装方法について説明します。

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 17:スタティック NAT



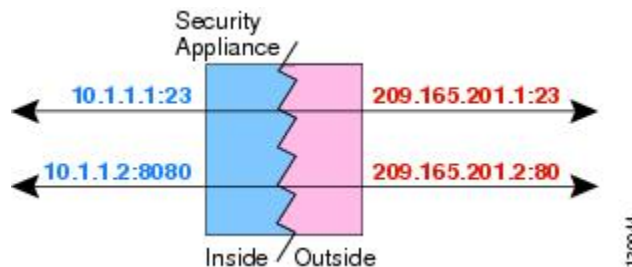
ポート変換を設定したスタティック NAT

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 18: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

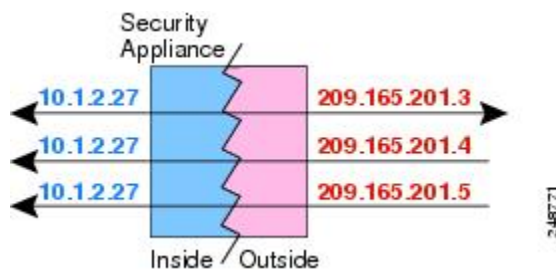
スタティック NAT は、実際のアドレスをインターフェイスアドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

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。

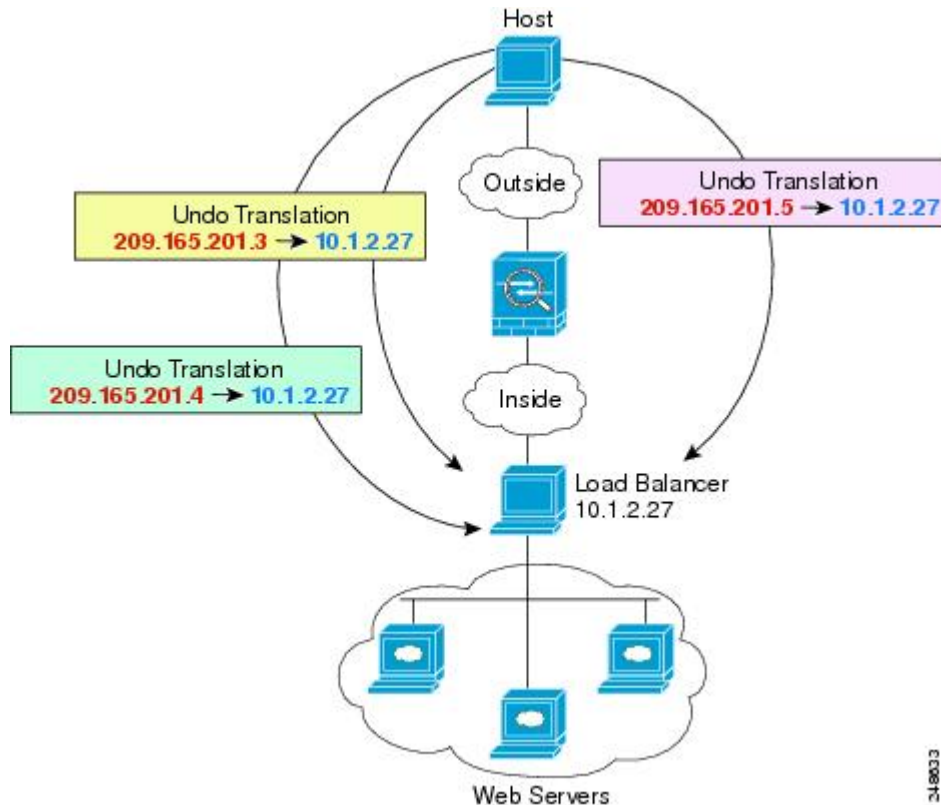
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 19: 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 20:1 対多のスタティック NAT の例



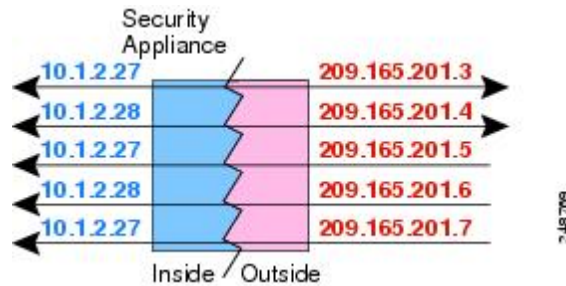
他のマッピングシナリオ（非推奨）

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 21: 少対多のスタティック NAT



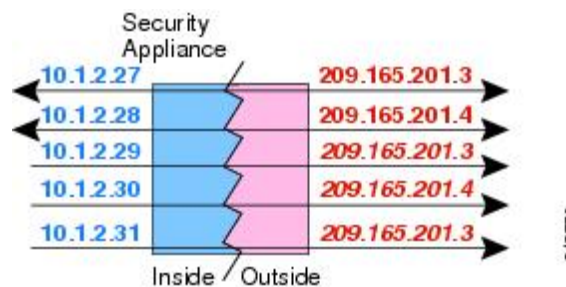
多対少または多対1コンフィギュレーションでは、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングプールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。



- (注) 多対少または多対1の NAT は PAT ではありません。2つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 22: 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) にする必要があります。ホスト、範囲、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、範囲、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 ([すべて (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 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 \(549 ページ\)](#) 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、範囲、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、範囲、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。

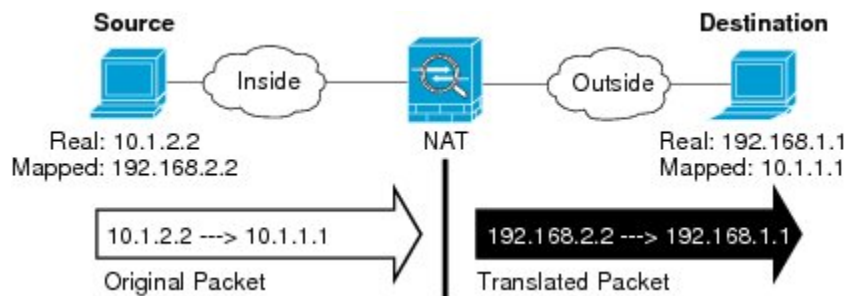
- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上に挿入できます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は送信元アドレスのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

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 ([すべて (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。



- [元の送信元アドレス (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。
- [元の宛先アドレス (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 \(549 ページ\)](#) 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。

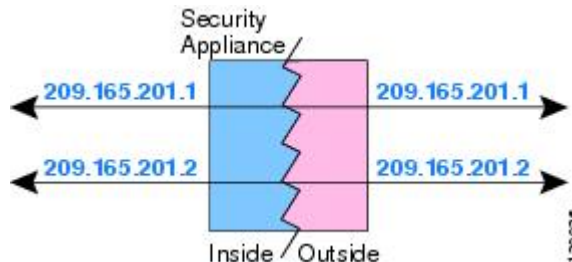
アイデンティティ NAT

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 23: 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、範囲、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 ([すべて (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、範囲、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。

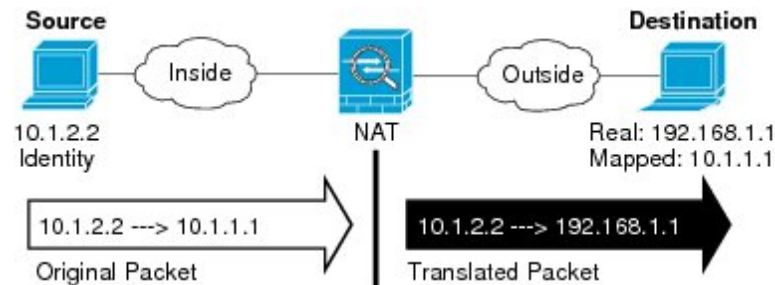
- [ルール of 作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルール of 配置 (Rule Placement)] : ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上下に挿入できます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

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 ([すべて (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。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 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 ([すべて (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ます、ホスト、範囲、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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- **[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、範囲、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 ([すべて (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、範囲、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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- [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、範囲、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 packets および変換済み packets 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 \(549 ページ\)](#) 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

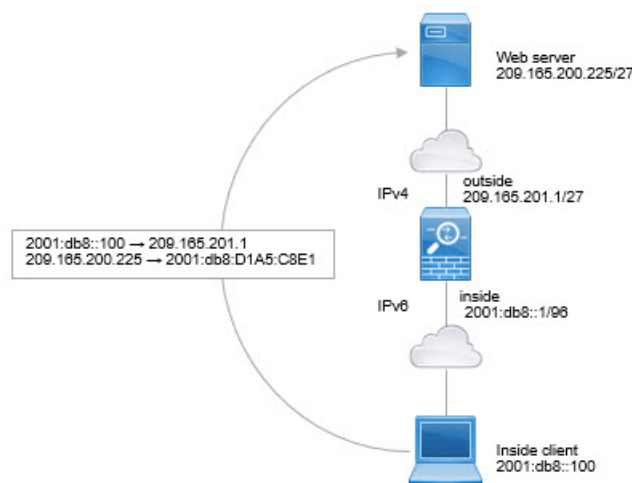
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2つのアドレスプール（IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレスプールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレスプール）を定義する必要があります。

- 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。

- [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。
- 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

- [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。

- [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)] = [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。
- [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

Packet Translation Advanced Options

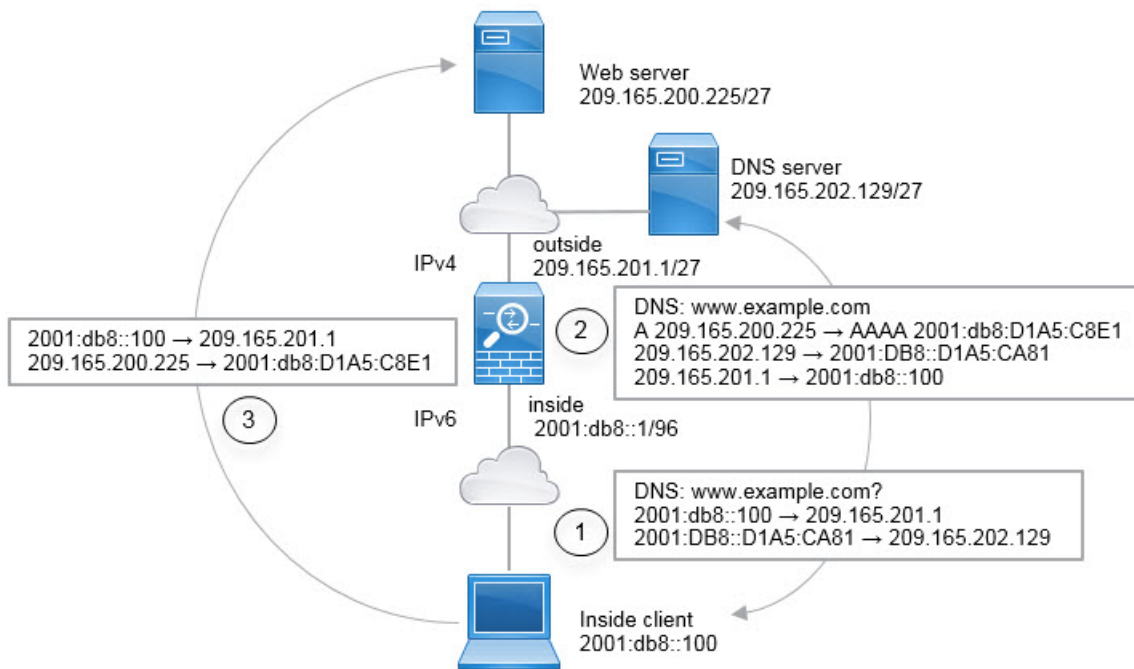
ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Source Address	inside_v6	Source Address	Interface
Source Port	Any	Source Port	Any
Destination Address	inside_v6	Destination Address	any-ipv4
Destination Port	Any	Destination Port	Any

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。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。

Add Network Object

Name

Description

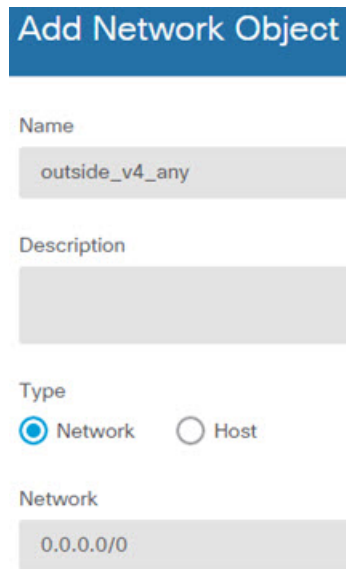
Type

Network
 Host

Network

- 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。

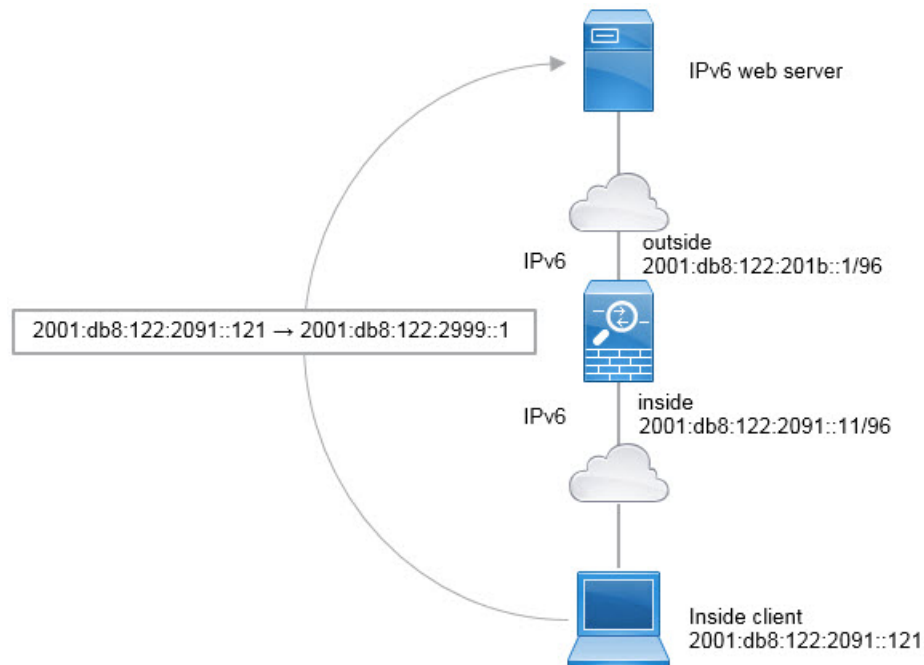
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

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。動的 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、動的 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。

- [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。
- 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

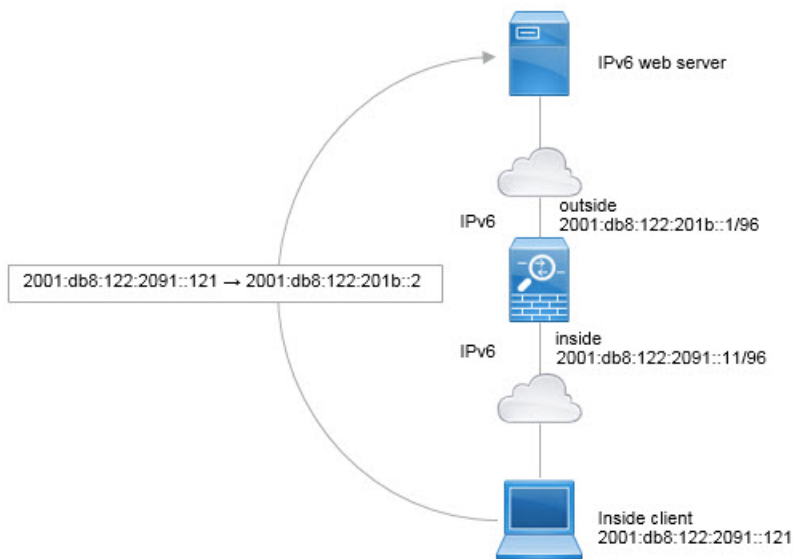
d) [OK] をクリックします。

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 サブネットワーク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動的 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。

- [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。
- 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** 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。

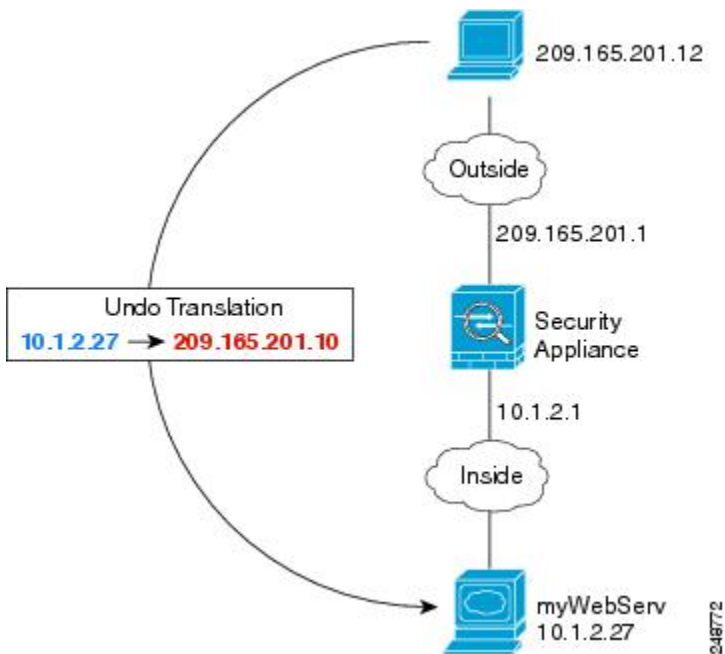
内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

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 24: 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	WebServerPrivate	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）

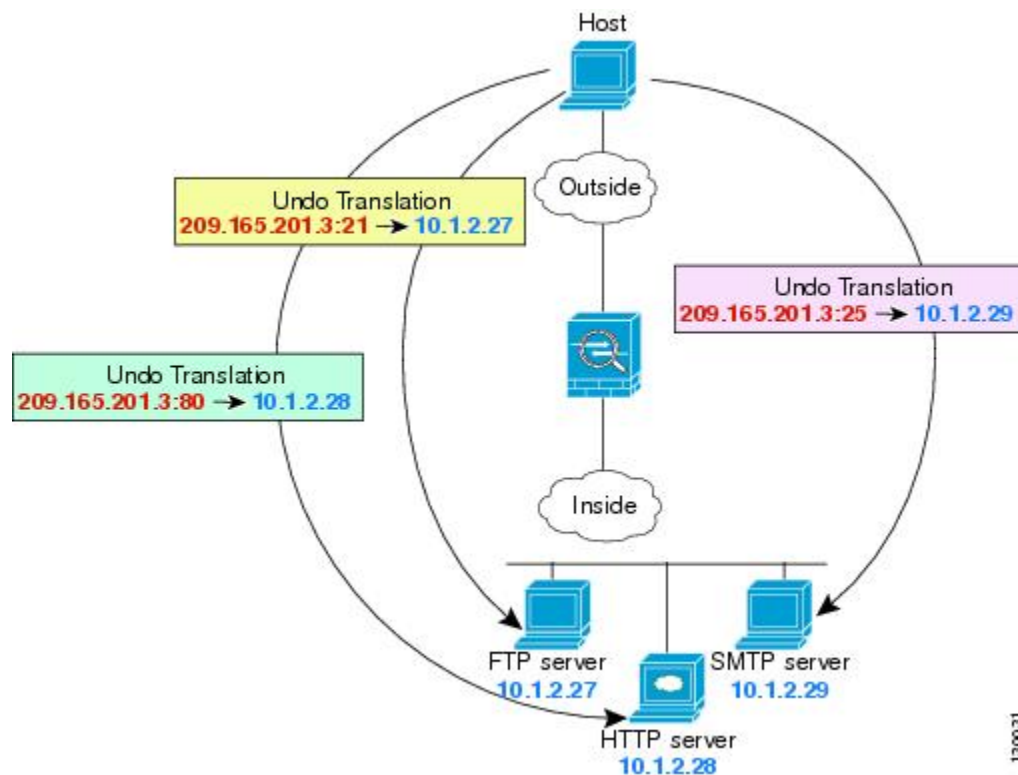
次のポート変換を設定したスタティック NAT の例では、リモートユーザがFTP、HTTP、およびSMTPにアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定した

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。

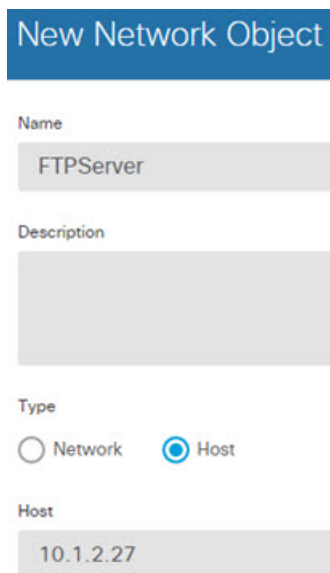
図 25: ポート変換を設定したスタティック NAT



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

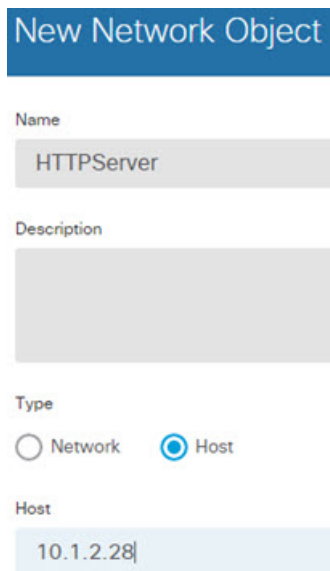
Type
 Network Host

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

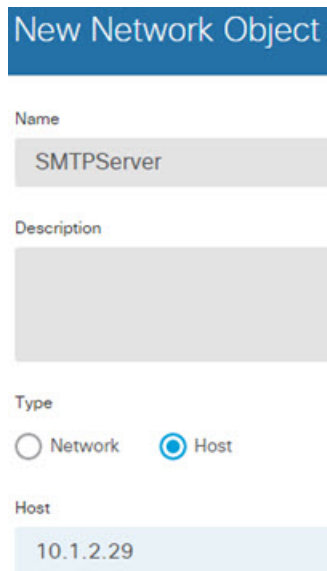
Type
 Network Host

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

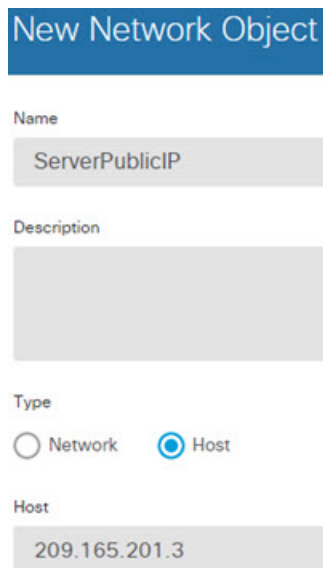
Host
10.1.2.29

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)。

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)。

Add NAT Rule

Title: HTTPServer 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		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	HTTPServer	Translated Address	ServerPublicIP
Original Port	HTTP	Translated Port	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。

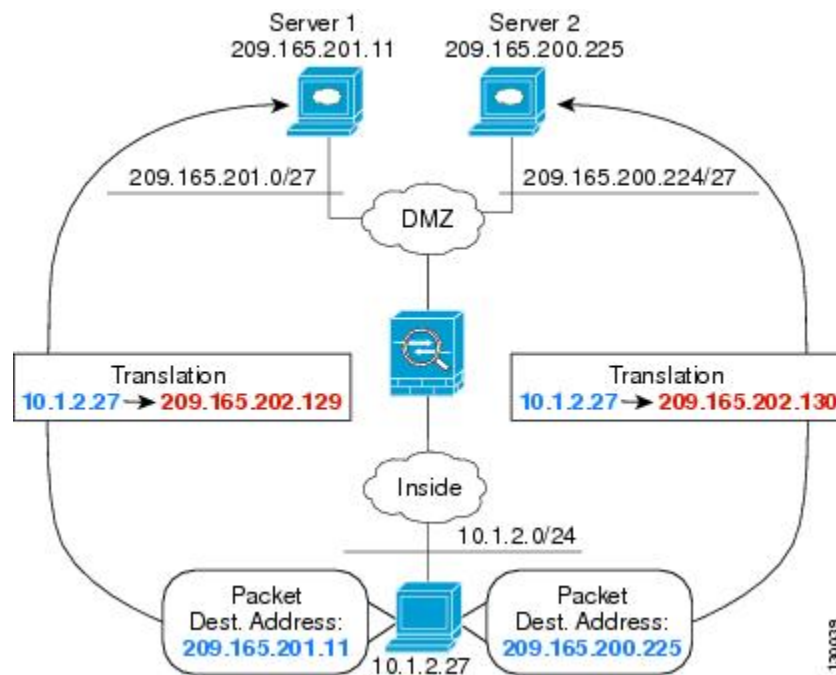
宛先に応じて異なる変換 (ダイナミック手動 PAT)

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 26: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。

The screenshot shows the 'New Network Object' configuration form. The 'Name' field contains 'PATaddress1'. The 'Description' field is empty. Under the 'Type' section, the 'Host' radio button is selected. The 'Host' field contains the IP address '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）。

The screenshot shows the 'New Network Object' configuration form. The 'Name' field contains 'DMZnetwork2'. The 'Description' field is empty. Under the 'Type' section, the 'Network' radio button is selected. The 'Network' field contains the IP address and subnet mask '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

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。

- [+] 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） = DMZNetwork2（または任意の別の名前）。
 - [ルールを作成対象（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）

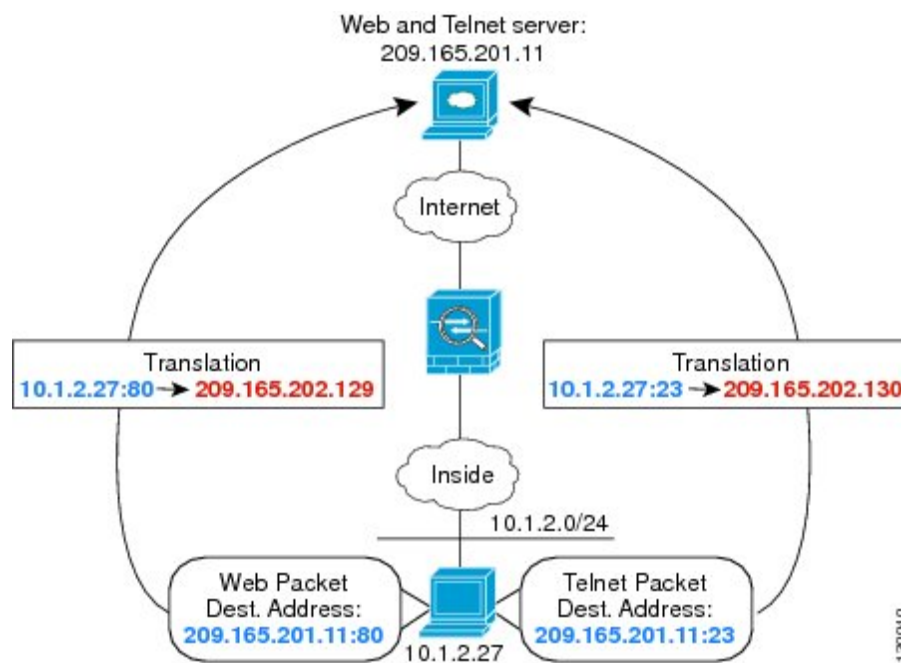
次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:

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。

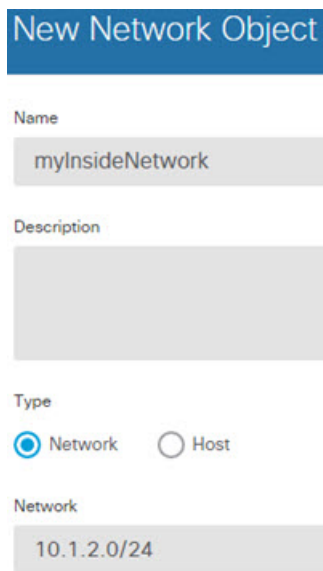
図 27:異なる宛先ポートを使用する手動 NAT



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

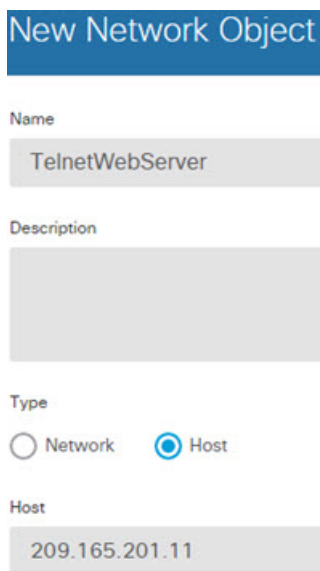
Type
 Network Host

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 を使用するときには、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。

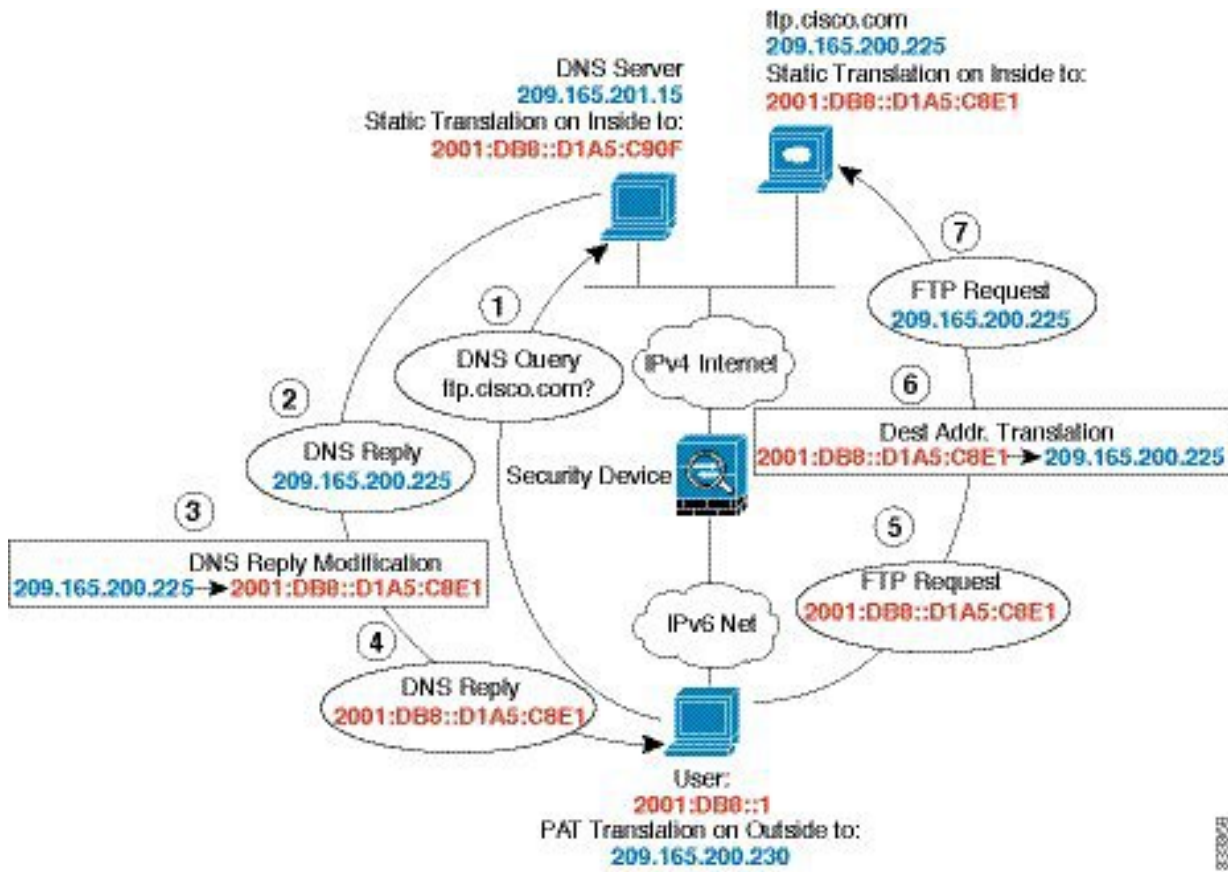
次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

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	Create Rule for	Status
PAT64Rule	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	Dynamic ▼

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 ▼	ipv4_pat ▼	Any

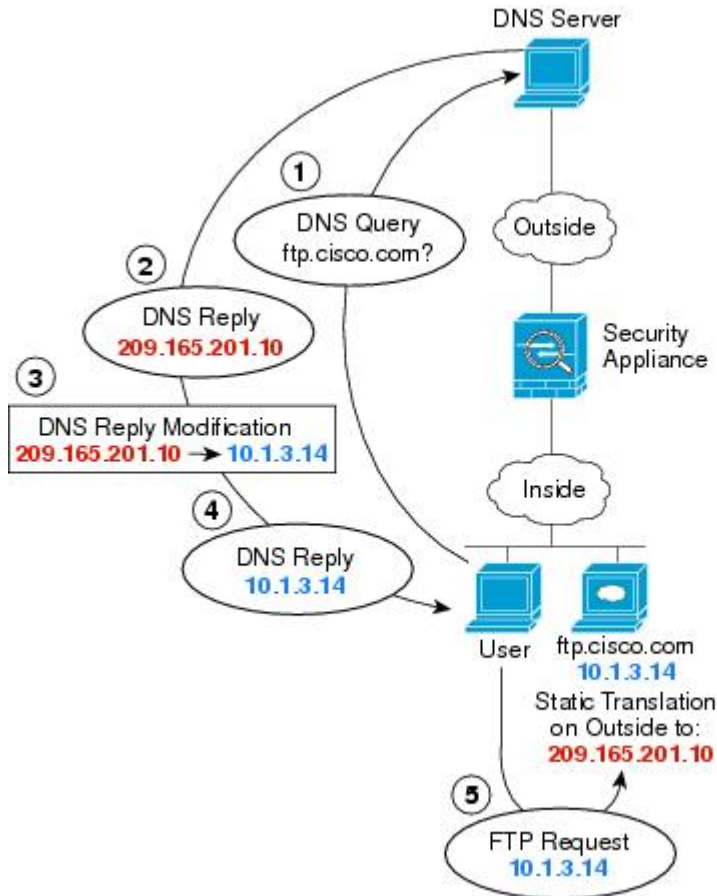
d) [OK] をクリックします。

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

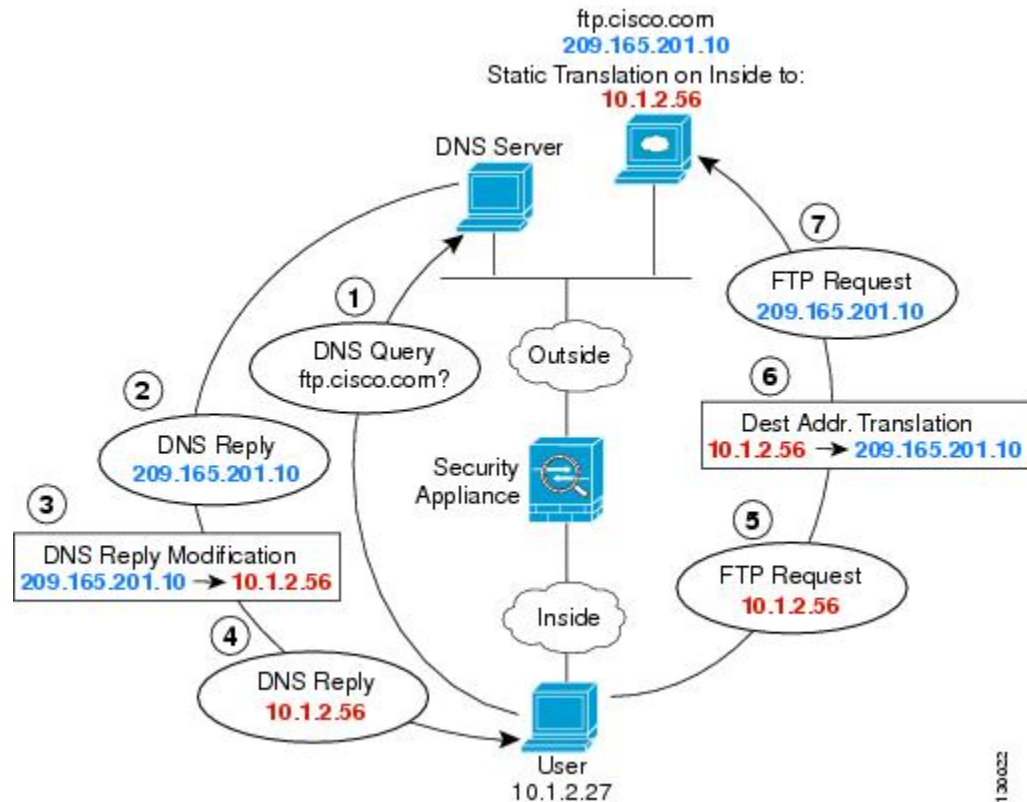
Packet Translation Advanced Options

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)] = [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

ORIGINAL PACKET

Source Interface

outside ▼

Original Address

ftp_server ▼

Original Port

Any ▼

TRANSLATED PACKET

Destination Interface

inside

Translated Address

ftp_server_transla ▼

Translated Port

Any

d) [OK] をクリックします。



第 **V** 部

バーチャル プライベート ネットワーク (VPN)

- [サイト間 VPN \(565 ページ\)](#)
- [リモート アクセス VPN \(605 ページ\)](#)



第 19 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](#)（565 ページ）
- [サイト間 VPN の管理](#)（572 ページ）
- [サイト間 VPN のモニタリング](#)（589 ページ）
- [サイト間 VPN の例](#)（589 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。

- 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。
- 15 : Diffie-Hellman グループ 15 (3072 ビット MODP グループ)。
- 16 : Diffie-Hellman グループ 16 (4096 ビット MODP グループ)。
- 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。

使用する認証方式の決定

次の方法を使用して、サイト間 VPN 接続でピアを認証することもできます。

事前共有キー

事前共有キーは、接続内のそれぞれのピアに設定されている秘密鍵の文字列です。これらのキーは、認証フェーズ中に IKE によって使用されます。IKEv1 の場合は、それぞれのピアで同じ事前共有キーを設定する必要があります。IKEv2 の場合は、各ピアに一意のキーを設定できます。

事前共有キーは証明書と比べて拡張性に劣ります。多数のサイト間 VPN 接続を設定する必要がある場合は、事前共有キー方式ではなく証明書方式を使用します。

証明書

デジタル証明書は IKE キー管理メッセージの署名や暗号化に RSA キー ペアを使用します。サイト間 VPN 接続の両端を設定するときに、リモートピアがローカルピアを認証できるように、ローカルデバイスのアイデンティティ証明書を選択します。

証明書方式を使用するには、次を実行する必要があります。

1. ローカルピアを認証局 (CA) に登録し、デバイスアイデンティティ証明書を取得します。この証明書をデバイスにアップロードします。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 \(173 ページ\)](#) を参照してください。

リモートピアも担当している場合、そのピアも登録してください。ピアに同じ CA を使用することは便利ですが、必須ではありません。

VPN 接続を確立するために自己署名証明書を使用することはできません。認証局でデバイスを登録する必要があります。

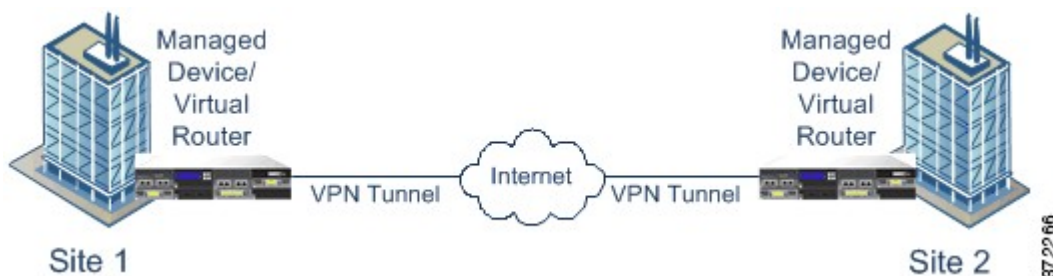
Windows 認証局 (CA) を使用してサイト間 VPN エンドポイントの証明書を作成する場合は、アプリケーションポリシー拡張に IP セキュリティ エンドシステムを指定する証明書を使用する必要があります。これは、[拡張 (Extensions)] タブ (Windows CA サーバ) の証明書の [プロパティ (Properties)] ダイアログボックスで確認できます。この拡張機能のデフォルトは、IP セキュリティ IKE 中間ですが、これは FDM を使用して設定されたサイト間 VPN では機能しません。

2. ローカルピアのアイデンティティ証明書に署名するために使用された、信頼できる CA 証明書をアップロードします。中間 CA が使用されていた場合は、ルートおよび中間証明書を含むチェーン全体をアップロードします。詳細については、[信頼できる CA 証明書のアップロード \(176 ページ\)](#) を参照してください。
3. リモートピアが異なる CA で登録されていた場合、リモートピアのアイデンティティ証明書に署名するために使用した信頼できる CA 証明書もアップロードします。リモートピアを制御する組織から証明書を取得します。中間 CA が使用されていた場合は、ルートおよび中間証明書を含むチェーン全体をアップロードします。
4. サイト間 VPN 接続を設定したら、証明書方式を選択し、ローカルピアのアイデンティティ証明書を選択します。接続の両端が、接続のローカルエンドの証明書を指定します。リモートピアの証明書は指定しません。

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。



動的にアドレス指定されたピアによるサイト間 VPN 接続の確立

ピアの IP アドレスがわからない場合でも、ピアにサイト間 VPN 接続を作成できます。これは、次の状況で役立ちます。

- ピアが DHCP を使用してそのアドレスを取得した場合は、特定の静的 IP アドレスを持つリモートエンドポイントに依存することはできません。
- 不特定多数のリモートピアが、ハブアンドスポークトポロジのハブとして機能するデバイスとの接続を確立できるようにする場合。

動的にアドレス指定したピア B にセキュアな接続を確立する必要がある場合、接続 A の終端に静的 IP アドレスがあることを確認する必要があります。次に、A で接続を作成する際に、ピアのアドレスが動的であることを指定します。ただし、ピア B で接続を設定する際は、リモートピアアドレスとして A の IP アドレスを入力します。

システムがサイト間 VPN 接続を確立する場合、ピアがダイナミックアドレスを持つすべての接続は応答のみとなります。つまり、リモートピアは接続を開始するものである必要があります。リモートピアが接続を確立しようとする、デバイスは事前共有キーまたは証明書（接続で定義されているいずれかの方式）を使用して接続を検証します。

VPN 接続はリモートピアが接続を開始した後にのみ確立されるため、VPN トンネルのトラフィックを許可するアクセス制御ルールに一致するすべての発信トラフィックは、接続が確立されるまでドロップされます。これにより、適切な暗号化と VPN 保護のないデータがネットワークから流出しないようになります。

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 \(573 ページ\)](#) 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 \(573 ページ\)](#) 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。

- [スタティック (Static)]/[ダイナミック (Dynamic)]: リモートピアの IP アドレスが静的または動的 (DHCP などを使用して) のどちらかで定義されるか。[スタティック (Static)] を選択した場合、リモートピアの IP アドレスも入力します。[ダイナミック (Dynamic)] を選択した場合、リモートピアのみがこの VPN 接続を開始できるようになります。

- [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 \(577 ページ\)](#) 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 \(583 ページ\)](#) を参照してください。
- [認証タイプ (Authentication Type)]: VPN 接続でピアを認証する方法 ([事前共有手動キー (Preshared Manual Key)] または [証明書 (Certificate)] のいずれか)。また、選択内容に基づいて、次のフィールドに入力する必要があります。IKEv1 の場合、接続用に設定された IKEv1 ポリシーオブジェクトで選択された認証方式と選択内容が一致する必要があります。これらのオプションの詳細については、[使用する認証方式の決定 \(570 ページ\)](#) 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。キーは1～127文字の英数字で指定できます。

- [証明書 (Certificate)] : ローカル ピアのデバイス アイデンティティ証明書。認証局 (CA) から取得した証明書である必要があります。自己署名証明書を使用することはできません。証明書をアップロードしていない場合は、[新しいオブジェクトの作成 (Create New Object)] リンクをクリックします。また、アイデンティティ証明書の署名に使用されたルート証明書および中間 CA 証明書をアップロードする必要があります。まだアップロードしていない場合は、このウィザードを完了した後に実行できます。
- [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 \(589 ページ\)](#) 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 \(569 ページ\)](#) 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。

[サイト間VPN経由によるトラフィックの許可 \(577ページ\)](#) で説明したように、追加の手順でVPN トンネル内のトラフィックを許可する必要があります。

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 \(586 ページ\)](#) を参照してください。

サイト間 VPN 経路によるトラフィックの許可

サイト間 VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

- **sysopt connection permit-vpn** コマンドを設定します。これにより、VPN 接続と一致するトラフィックがアクセスコントロールポリシーから免除されます。このコマンドのデフォルトは **no sysopt connection permit-vpn** で、VPN トラフィックをアクセスコントロールポリシーでも許可する必要があることを意味します。

これは、外部ユーザが保護されたリモートネットワーク内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。これは、トラフィックに対する接続イベントは発生せず、したがって統計ダッシュボードでは VPN 接続が反映されないことも意味します。

このコマンドを設定するのに適した方法は、リモートアクセス VPN 接続プロファイルを作成し、そこで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (Bypass Access Control policy for decrypted traffic)] オプションを選択することです。RA VPN を設定しない場合、または RA VPN を設定できない場合、FlexConfig を使用してコマンドを設定することができます。

- リモートネットワークからの接続を許可するアクセス制御ルールを作成します。この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

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 \(579 ページ\)](#)
- [IKEv2 ポリシーの設定 \(580 ページ\)](#)

- 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、これが最初に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、それが最初に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せん。

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。詳細については、[使用する認証方式の決定 \(570 ページ\)](#) を参照してください。
 - [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。
 - [証明書 (Certificate)] : ピアのデバイス ID 証明書を使用して相互に識別します。各ピアを認証局で登録することで、これらの証明書を取得する必要があります。また、各ピアでアイデンティティ証明書の署名に使用された、信頼できる CA ルート証明書および中間 CA 証明書もアップロードする必要があります。ピアは同じまたは別の CA に登録することができます。いずれのピアにも自己署名証明書を使用することはできません。
- [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 \(567ページ\)](#) 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 \(569 ページ\)](#) 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 \(568 ページ\)](#) 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 \(567 ページ\)](#) 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 \(569 ページ\)](#) 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 \(568 ページ\)](#) 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 \(568 ページ\)](#) 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 \(567 ページ\)](#) 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 \(568 ページ\)](#) 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 \(567 ページ\)](#) 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

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 \(568 ページ\)](#) 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が、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。

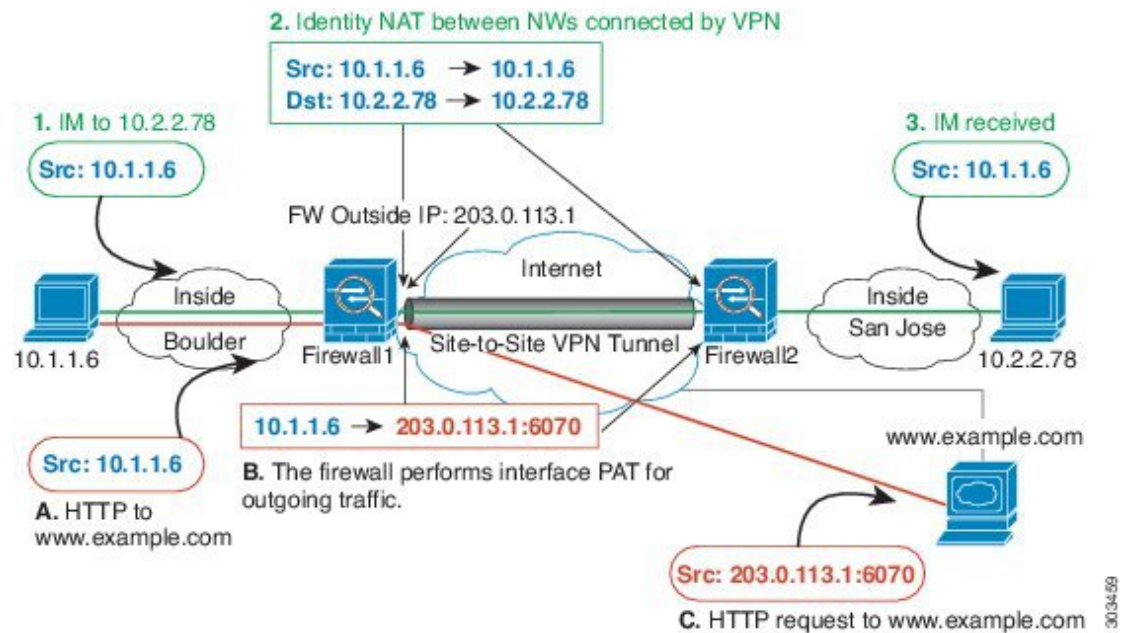
VPN 接続を作成するときに、[NATを除外 (NAT Exempt)] オプションを選択すると、ルールが自動的に作成されます。ただし、これはローカルで保護されたネットワークが単一のルーテッドインターフェイス (ブリッジグループメンバーではない) を介して接続されている場合のみ動作します。その代わりに、接続内のローカルネットワークが複数のルーテッドインターフェイス、または1つ以上のブリッジグループメンバーの背後に存在する場合、NAT 免除ルールを手動で設定する必要があります。

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 28: 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（ボルダー）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ダーを特定します。

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

- [OK] をクリックします。
- [+] 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。

f) [OK] をクリックします。

ステップ 2 Firewall1 (ボールドー) 上で VPN 経由でサンノゼに向かう場合、ボールドー 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。

- [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。
- [OK] をクリックします。
- 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) 。

Add NAT Rule

Title: inside1_2 interface PAT Create Rule for: Manual NAT Status:

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: Below a Specific Rule NAT Exempt 1_2 E Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside1_2	Destination Interface	outside
Source Address	boulder-network	Source Address	Interface
Source Port	Any	Source Port	Any
Destination Address	Any	Destination Address	Any
Destination Port	Any	Destination Port	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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

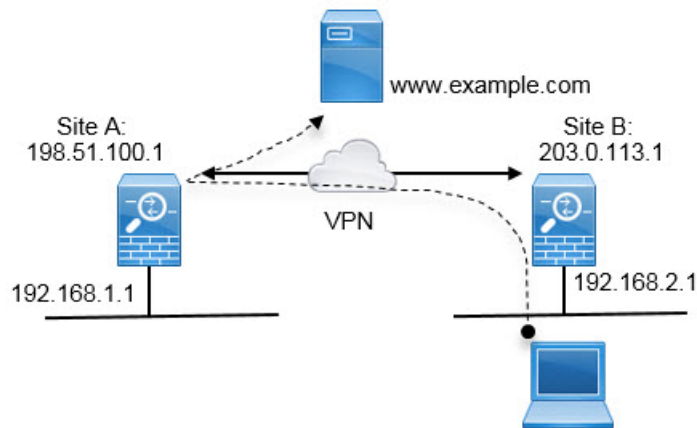
- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイスオブジェクトを作成します。

- 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。

始める前に

この手順では、VPNトラフィックをアクセスコントロールポリシーの対象とする、VPNトラフィックを許可するためのデフォルト設定を使用していると仮定します。実行中のコンフィギュレーションでは、これは **no sysopt connection permit-vpn** コマンドで表されます。代わりに FlexConfig を介して **sysopt connection permit-vpn** を有効にした場合、または RA VPN 接続プロファイルで [復号されたトラフィックでアクセス制御ポリシーをバイパスする (Bypass Access Control policy for decrypted traffic)] オプションを選択することで、アクセス制御ルールを設定する手順は不要になります。

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。

- 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、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	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
outside	Remote IP Address
Local Network	203.0.113.1
+ ANY	Remote Network
	+ 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。

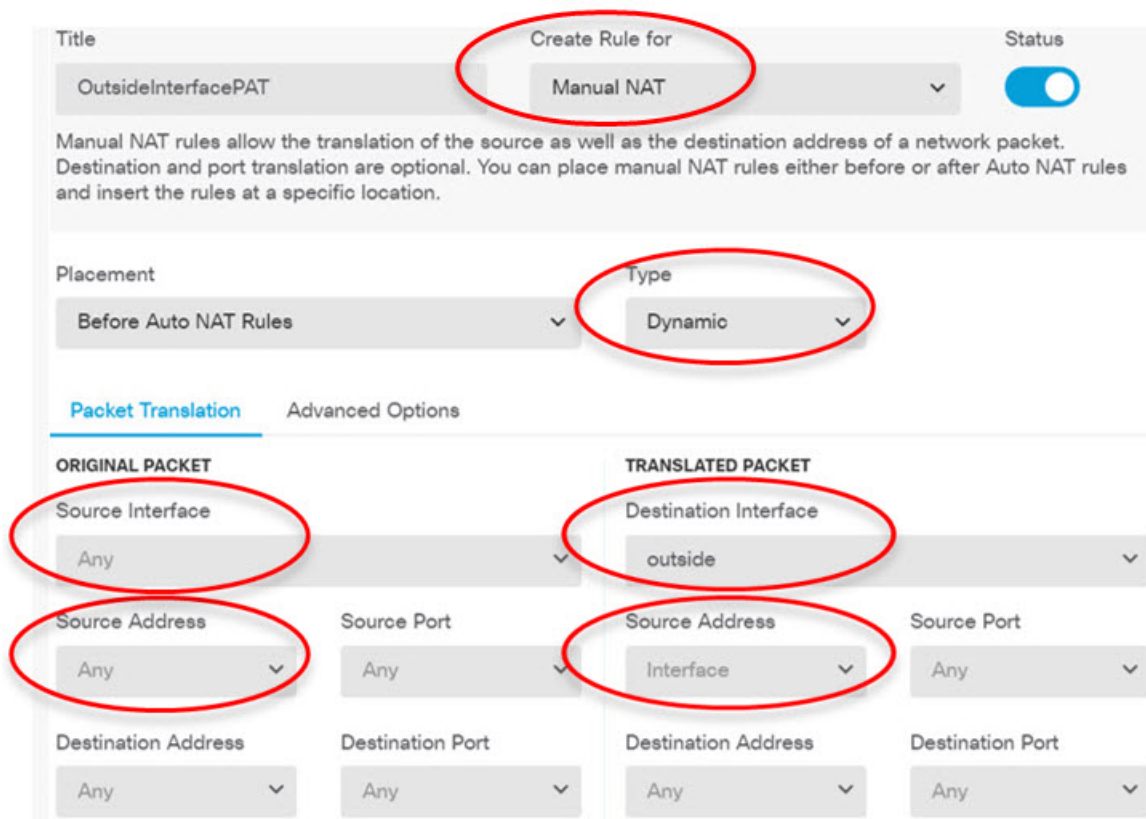
- c) 次のプロパティを使用してルールを設定します。

- [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。



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) サイト B の保護ネットワークへのアクセスを許可するアクセス制御ルールを設定します。

VPN 接続を作成するだけで、VPN 上のトラフィックが自動的に許可されるわけではありません。使用しているアクセス コントロール ポリシーがリモート ネットワークへのトラフィックを許可している必要があります。

次の手順では、リモート ネットワーク用の固有ルールの追加方法を示します。追加のルールが必要かどうかは、既存のルールによって異なります。

a) [ポリシー (Policies)] > [アクセス制御 (Access Control)] をクリックします。

- b) [+] をクリックして新しいルールを作成します。
- c) 次のプロパティを使用してルールを設定します。
- [順序 (Order)] : ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。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。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。
 - [タイトル (Title)] : スペースを含めずにわかりやすい名前を入力します。例、Site-B-Network。
 - [アクション (Action)] : [許可 (Allow)]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼 (Trust)] を選択できます。
 - [送信元または宛先 (Source/Destination)] タブ : [宛先 (Destination)] > [ネットワーク (Network)] で、リモートネットワークの VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先 (Source and Destination)] の他のすべてのオプションについては、デフォルトの [任意 (Any)] のままにします。

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ANY	ANY	ANY	Site-B-Network	ANY

- [アプリケーション (Application)]、[URL]、および [ユーザ (Users)] タブ : これらのタブではデフォルトの設定 (何も選択しない) のままにします。
- [侵入 (Intrusion)]、[ファイル (File)] タブ : オプションで、脅威またはマルウェアを検索する侵入またはファイルポリシーを選択できます。
- [ロギング (Logging)] タブ : オプションで接続のロギングを有効にできます。

d) [OK] をクリックします。

ステップ 4 (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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。ウィンドウをアクティブのままにすると、展開が正常に終了した後、保留中の変更はないことが表示されます。

ステップ 5 (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

Local VPN Access Interface

outside

Local Network

+

ANY

REMOTE SITE

Static Dynamic

Remote IP Address

198.51.100.1

Remote Network

i We don't recommend to use "ANY" for this option.

+

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 6 (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。

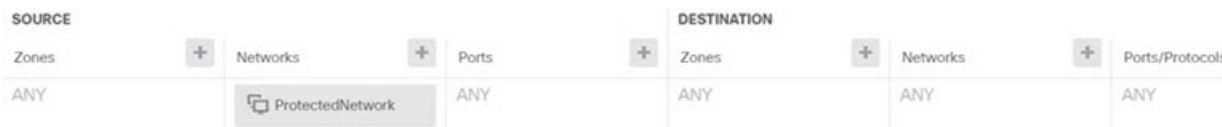
ステップ 7 (サイト B、リモート サイト) 保護ネットワークからインターネットへのアクセスを許可するアクセス制御ルールを設定します。

次の例では、保護ネットワークから任意の宛先へのトラフィックが許可されます。これは独自の要件に合わせて調整できます。不要なトラフィックを除外するブロックルールをルールの前に置くことができます。別のオプションとして、サイト A のデバイスにブロック ルールを設定することもできます。

- a) [ポリシー (Policies)] > [アクセス制御 (Access Control)] をクリックします。
- b) [+] をクリックして新しいルールを作成します。
- c) 次のプロパティを使用してルールを設定します。

- [順序 (Order)] : ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。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。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。

- [タイトル (Title)]: スペースを含めずにわかりやすい名前を入力します。例、Protected-Network-to-Any。
- [アクション (Action)]: [許可 (Allow)]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼 (Trust)]を選択できます。
- [送信元または宛先 (Source/Destination)] タブ: [送信元 (Source)] > [ネットワーク (Network)] で、ローカル ネットワークの VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先 (Source and Destination)] の他のすべてのオプションについては、デフォルトの [任意 (Any)] のままにします。



- [アプリケーション (Application)]、[URL]、および [ユーザ (Users)] タブ: これらのタブではデフォルトの設定 (何も選択しない) のままにします。
- [侵入 (Intrusion)]、[ファイル (File)] タブ: オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング (Logging)] タブ: オプションで接続のロギングを有効にできます。

d) [OK] をクリックします。

ステップ 8 (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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。ウィンドウをアクティブのままにすると、展開が正常に終了した後、保留中の変更はないことが表示されます。



第 20 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 \(605 ページ\)](#)
- [リモート アクセス VPN のライセンス要件 \(612 ページ\)](#)
- [リモート アクセス VPN に関する注意事項と制限事項 \(613 ページ\)](#)
- [リモート アクセス VPN の設定 \(613 ページ\)](#)
- [リモート アクセス VPN 設定の管理 \(619 ページ\)](#)
- [リモート アクセス VPN のモニタリング \(636 ページ\)](#)
- [リモート アクセス VPN のトラブルシューティング \(636 ページ\)](#)
- [リモート アクセス VPN の例 \(639 ページ\)](#)

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 5508-X	100
ASA 5516-X	300
ASA 5525-X	750
ASA 5545-X	2500
ASA 5555-X	5000
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Firepower 4100 シリーズ、すべてのモデル	10,000
Firepower 9300 アプライアンス、すべてのモデル	20,000
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。

RADIUS およびグループポリシーを使用したユーザの権限および属性の制御

外部 RADIUS サーバまたは Firepower Threat Defense デバイスで定義されているグループポリシーから、RA VPN 接続にユーザの認可属性（ユーザの権利または権限とも呼ばれる）を適用できます。Firepower Threat Defense デバイスがグループポリシーに設定されている属性と競合する外部 AAA サーバから属性を受信した場合は、AAA サーバからの属性が常に優先されます。

Firepower Threat Defense デバイスは次の順序で属性を適用します。

1. 外部 AAA サーバ上で定義されたユーザ属性：ユーザ認証または認可が成功すると、サーバからこの属性が返されます。
2. Firepower Threat Defense デバイス上で設定されているグループポリシー：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25 (OU=group-policy) の値が返された場合は、Firepower Threat Defense デバイスはそのユーザを同じ名前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバから返されないものを適用します。
3. 接続プロファイルによって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザに適用されるデフォルトのグループポリシーが含まれています。Firepower Threat Defense デバイスに接続するすべてのユーザは、最初にこのグループに所属します。このグループでは、AAA サーバから返されるユーザ属性、またはユーザに割り当てられたグループポリシーにはない属性が定義されています。

Firepower Threat Defense デバイスは、ベンダー ID 3076 の RADIUS 属性をサポートします。使用する RADIUS サーバでこれらの属性が定義されていない場合、手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダーコード (3076) を使用します。

次のトピックでは、サポートされている属性値について、値が RADIUS サーバで定義されるかどうか、または RADIUS サーバにシステムが送信する値であるかどうかに基づいて説明します。

RADIUS サーバに送信された属性

RADIUS 属性 146 および 150 は、認証および認可の要求の場合に FTD デバイスから RADIUS サーバに送信されます。次の属性はすべて、アカウント開始、中間アップデート、および終了の要求の場合に FTD デバイスから RADIUS サーバに送信されます。

表 12: FTD が RADIUS に送信する属性

属性	属性番号	構文、タイプ	シングルまたはマルチ値	説明または値
Client Type	150	整数	シングル	VPN に接続しているクライアントのタイプ： 2 = AnyConnect クライアント SSL VPN
Session Type	151	整数	シングル	接続の種類： 1 = AnyConnect クライアント SSL VPN
Tunnel Group Name	146	文字列	シングル	FTD デバイスで定義された、セッションの確立に使用された接続プロファイルの名前。名前には 1 ～ 253 文字を使用できます。

RADIUS サーバから受信した属性

次のユーザ認可属性が RADIUS サーバから FTD デバイスに送信されます。

表 13: 送信される RADIUS 属性 FTD

属性	属性番号	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	両方の Access-List 属性が、FTD デバイスで設定されている ACL の名前を使用します。スマート CLI 拡張アクセスリストのオブジェクトタイプを使用して、これらの ACL を作成します ([デバイス (Device)] > [詳細設定 (Advanced Configuration)] > [スマート CLI (Smart CLI)] > [オブジェクト (Object)] を選択します)。 これらの ACL は、着信 (FTD デバイスに入るトラフィック) または発信 (FTD デバイスから出るトラフィック) 方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	
Address-Pools	217	文字列	シングル	FTD デバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[オブジェクト (Objects)] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザがログインするときに表示されるバナー。

属性	属性番号	構文、タイプ	シングルまたはマルチ値	説明または値
Banner2	36	文字列	シングル	ユーザがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されません。
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の [グループポリシー (Group Policy)] ページでグループポリシーを作成する必要があります。次の形式のいずれかを使用できます。 <ul style="list-style-type: none"> • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
Simultaneous-Logins	2	整数	シングル	ユーザが確立を許可されている個別の同時接続の数 (0 ~ 2147483647)。
VLAN	140	整数	シングル	ユーザの接続を制限する VLAN (0 ~ 4094)。FTD デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

二要素認証

RA VPN に対して二要素認証を設定することができます。二要素認証を使用する場合、ユーザはユーザ名とスタティックパスワードに加えて、RSA トークンや Duo パスコードなどの追加項目を指定する必要があります。二要素認証が 2 番目の認証ソースを使用することと異なるのは、1 つの認証ソースで 2 つの要素が設定され、RSA/Duo サーバとの関係がプライマリ認証ソースに関連付けられている点です。ただし、Duo LDAP は例外で、この場合はセカンダリ認証ソースとして Duo LDAP サーバを設定します。

システムは、2 番目の要素のためにモバイルにプッシュされる RSA トークンと Duo パスコードを、二要素認証プロセスの最初の要素としての RADIUS サーバまたは AD サーバと組み合わせることでテストされています。

RSA 二要素認証

次の方法のいずれかを使用して RSA を設定することができます。RSA 側の設定については、RSA のドキュメントを参照してください。

- RSA サーバを RADIUS サーバとして直接 FDM で定義し、そのサーバを RA VPN のプライマリ認証ソースとして使用します。

この方法を使用する場合、ユーザは RSA RADIUS サーバで設定されているユーザ名を使用して認証し、パスワードと 1 回限りの一時的な RSA トークンを連結し、パスワードとトークンをコンマで区切る必要があります (*password,token*)。

この設定では、認証サービスを提供するために (Cisco ISE で供給されるような) 個別の RADIUS サーバを使用することが一般的です。2 番目の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウントングサーバとしても設定します。

- 直接統合をサポートする RADIUS または AD サーバと RSA サーバを統合し、RSA 以外の RADIUS または AD サーバをプライマリ認証ソースとして使用するよう RA VPN を設定します。この場合、RADIUS/AD サーバは RSA-SDI を使用して、クライアントと RSA サーバ間の二要素認証を委任して調整します。

この方法を使用する場合、ユーザは RSA 以外の RADIUS または AD サーバで設定されているユーザ名を使用して認証し、パスワードと 1 回限りの一時的な RSA トークンを連結し、パスワードとトークンをコンマで区切る必要があります (*password,token*)。

この設定では、RSA 以外の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウントングサーバとしても設定します。

RADIUS を使用した Duo 二要素認証

Duo RADIUS サーバはプライマリ認証ソースとして設定できます。この方法では、Duo RADIUS 認証プロキシを使用します

Duo の詳細な設定手順については、<https://duo.com/docs/cisco-firepower> を参照してください。

その後、最初の認証要素として別の RADIUS サーバ (または AD サーバ) を使用し、2 番目の要素として Duo クラウドサービスを使用するため、プロキシサーバ宛の認証要求を転送するように Duo を設定します。

この方法を使用する場合、ユーザは Duo 認証プロキシおよび関連する RADIUS/AD サーバの両方に設定されているユーザ名、RADIUS/AD サーバに設定されているユーザ名のパスワード、およびその後に次の Duo コードのいずれかを使用することで、認証を行う必要があります。

- *Duo-passcode. my-password,12345* など
- **push.** *my-password,push* など。push は、ユーザによるインストールと登録が完了している Duo モバイルアプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- **sms.** *my-password,sms* など。sms は、ユーザのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。sms を使用すると、ユーザの認証試行が失敗します。ユーザは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。
- **phone.** *my-password,phone* など。phone は、電話コールバック認証を実行するように Duo に指示する場合に使用します。

ユーザ名/パスワードが認証されると、Duo 認証プロキシは Duo クラウドサービスに接続し、Duo クラウドサービスは、その要求が設定されている有効なプロキシデバイスからのものであることを検証してから、指示に従ってユーザのモバイルデバイスに一時的なパスコードをプ

シユ送信します。ユーザがこのパスコードを受け入れると、セッションは Duo で認証済みとマークされ、RA VPN が確立されます。

LDAP を使用した Duo 二要素認証

プライマリ ソースとして Microsoft Active Directory (AD) または RADIUS サーバを使用し、それと組み合わせてセカンダリ認証ソースとして Duo LDAP サーバを使用できます。Duo LDAP を使用すると、セカンダリ認証において、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールによって検証されます。

FTD デバイスは、LDAPS を使用して、ポート TCP/636 経由で Duo LDAP と通信します。

Duo LDAP サーバは認証サービスのみを提供し、アイデンティティサービスを提供しないことに注意してください。そのため、プライマリ認証ソースとして Duo LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザ名は表示されず、これらのユーザに対してアクセス制御ルールを作成することはできません。

このアプローチを採用する場合は、RADIUS/AD サーバと Duo LDAP サーバの両方で設定されているユーザ名を使用してユーザを認証する必要があります。AnyConnect によるログインを求められた場合、ユーザは、[プライマリパスワード (Primary Password)] フィールドに RADIUS/AD のパスワードを入力し、[セカンダリパスワード (Secondary Password)] に次のいずれかを入力して、Duo での認証を行います。詳細については、<https://guide.duo.com/anyconnect> を参照してください。

- [Duo パスコード (Duo passcode)] : Duo Mobile で生成され、SMS を介して送信され、ハードウェアトークンによって生成されるパスコード、または管理者によって提供されるパスコードを使用して、認証します。1234567 などです。
- [プッシュ (push)] : Duo Mobile アプリをインストールしてアクティブにしている場合は、ログイン要求を電話機にプッシュします。要求を確認し、[承認 (Approve)] をタップしてログインします。
- [電話 (phone)] : 電話機のコールバックを使用して認証します。
- [sms] : Duo パスコードをテキストメッセージで要求します。ログイン試行は失敗します。新しいパスコードを使用して再度ログインします。

Duo LDAP の詳細な説明と例については、[Duo LDAP を使用した二要素認証の設定方法 \(649 ページ\)](#) を参照してください。

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 \(108 ページ\)](#) 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。
- RADIUS トークンと RSA トークンを使用して二要素認証を設定すると、ほとんどの場合、デフォルトの 12 秒の認証タイムアウトでは短すぎて正常な認証が行われません。[クライアントプロファイルの設定およびアップロード \(615 ページ\)](#) で説明しているように、カスタム AnyConnect クライアントプロファイルを作成し、それを RA VPN 接続プロファイルに適用することにより、認証タイムアウト値を増やすことができます。認証タイムアウトを 60 秒以上にすることをお勧めします。これにより、ユーザの認証および RSA トークンの貼り付けと、トークンのラウンドトリップ検証のための十分な時間が得られます。

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 \(107 ページ\)](#) 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 \(612 ページ\)](#) 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 \(108 ページ\)](#) 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 \(172 ページ\)](#) 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 (615 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ソースを設定します。

リモートアクセス VPN へのログインを許可するユーザアカウントに次のソースを使用できます。代わりに、クライアント証明書を単独で、またはアイデンティティソースと連携させて、認証を使用することができます。

- **Active Directory** アイデンティティレルム：プライマリ認証ソースとして。ユーザアカウントは Active Directory (AD) サーバで定義されます。[AD アイデンティティレルムの設定 \(183 ページ\)](#) を参照してください。
- **RADIUS** サーバグループ：プライマリまたはセカンダリ認証ソースとして。認可およびアカウントリングにも。[RADIUS サーバグループの設定 \(190 ページ\)](#) を参照してください。
- **LocalIdentitySource** (ローカルユーザデータベース)：プライマリソースまたはフォールバックソースとして。デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。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ユーザ名/パスワードを定義します。[ローカルユーザの設定 \(197 ページ\)](#) を参照してください。
- **Duo LDAP** サーバ：プライマリまたはセカンダリ認証ソースとして。Duo LDAP サーバをプライマリソースとして使用できますが、これは通常の設定ではありません。通常は、プライマリの Active Directory または RADIUS サーバと組み合わせて二要素認証を提供するために、セカンダリソースとして使用します。詳細については、[Duo LDAP を使用した二要素認証の設定方法 \(649 ページ\)](#) を参照してください。

ステップ5 (オプション) [RA VPN のグループポリシーの設定 \(628 ページ\)](#)

グループポリシーは、ユーザに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用することもできます。

ステップ6 [RA VPN 接続プロファイルの設定 \(620 ページ\)](#)。**ステップ7** [リモートアクセス VPN によるトラフィックの許可 \(617 ページ\)](#)。**ステップ8** [リモートアクセス VPN 設定の確認 \(617 ページ\)](#)。

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 \(636 ページ\)](#) を参照してください。

ステップ9 (オプション) アイデンティティポリシーを有効にして、パッシブ認証のルールを設定します。

パッシブユーザ認証を有効にすると、リモートアクセスVPN経由でログインするユーザがダッシュボードに表示され、ポリシー内のトラフィック一致基準としても使用できます。パッシブ認証を有効にしない場合、RA VPN ユーザはアクティブ認証ポリシーに一致する場合のみ使用できます。ダッシュボードのユーザ情報またはトラフィック照合用のユーザ情報を取得するには、アイデンティティポリシーを有効にする必要があります。

クライアントプロファイルの設定およびアップロード

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ー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ー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、外部インターフェー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 によるトラフィックの許可

リモートアクセス VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

- **sysopt connection permit-vpn** コマンドを設定します。これにより、VPN 接続と一致するトラフィックがアクセス コントロール ポリシーから免除されます。このコマンドのデフォルトは **no sysopt connection permit-vpn** で、VPN トラフィックをアクセス コントロール ポリシーでも許可する必要があることを意味します。

これは、外部ユーザがリモート アクセス VPN アドレス プール内の IP アドレスになりすまることができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。これは、トラフィックに対する接続イベントは発生せず、したがって統計ダッシュボードでは VPN 接続が反映されないことも意味します。

このコマンドを設定するには、RA VPN 接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (Bypass Access Control policy for decrypted traffic)] オプションを選択します。

- リモートアクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

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っています。[リモート アクセス VPN のトラブルシューティング \(636 ページ\)](#) 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://raypn-address> を開きます。*raypn-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 \(607 ページ\)](#) を参照してください。

グループ URL を設定した場合は、それらの URL も試みてください。

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 設定の管理

リモートアクセス VPN 接続プロファイルは、外部ユーザが AnyConnect クライアントを使用してシステムに VPN に接続することを許可するという接続特性を定義します。各プロファイルは、ユーザの認証に使用される AAA サーバと証明書、ユーザの IP アドレスを割り当てるためのアドレスプール、およびさまざまなユーザ向け属性を定義するグループポリシーを定義します。

異なるユーザグループに異なるサービスを提供する必要がある場合、または異なる認証ソースがある場合は、複数のプロファイルを作成します。たとえば、自分の組織が異なる認証サーバを使用する異なる組織と合併した場合、これらの認証サーバを使用する新しいグループのプロファイルを作成できます。

手順

ステップ 1 [デバイス (Device)] > [リモートアクセス VPN (Remote Access VPN)] グループで [設定の表示 (View Configuration)] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次の [接続プロファイル (Connection Profiles)] をクリックします (未選択の場合)。

ステップ 3 次のいずれかを実行します。

- 新しい接続プロファイルを作成するには、[+] ボタンをクリックします。詳細な手順については、[RA VPN 接続プロファイルの設定 \(620 ページ\)](#) を参照してください。

- 表示ボタン (👁️) をクリックして、接続プロファイルの概要と接続手順を開きます。概要内で [編集 (Edit)] をクリックすると変更が行えます。
- 削除ボタン (🗑️) をクリックすると、不要な接続プロファイルを削除できます。
- 接続プロファイルのユーザ向け属性を定義するには、目次の [グループポリシー (Group Policies)] を選択します。RA VPN のグループポリシーの設定 (628 ページ) を参照してください。

RA VPN 接続プロファイルの設定

リモートアクセス VPN 接続プロファイルを作成すると、ホームネットワークなどの外部ネットワークからでも、ユーザは内部ネットワークに接続できるようになります。異なる認証方式に対応するには、個別のプロファイルを作成します。

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。
- 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 (688 ページ) を参照してください。

手順

ステップ 1 [デバイス (Device)] > [リモートアクセスVPN (Remote Access VPN)] グループで [設定の表示 (View Configuration)] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次の [接続プロファイル (Connection Profiles)] をクリックします (未選択の場合)。

ステップ 3 次のいずれかを実行します。

- 新しい接続プロファイルを作成するには、[+] ボタンをクリックします。
- 表示ボタン (👁️) をクリックして、接続プロファイルの概要と接続手順を開きます。概要内で [編集 (Edit)] をクリックすると変更が行えます。

ステップ 4 基本的な接続属性を設定します。

- [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。ユーザにとって意味のある名前を選択します。

- [グループエイリアス (Group Alias)], [グループURL (Group URL)] : エイリアスには特定の接続プロファイルの代替名または URL を含めることができます。VPN ユーザは、FTD デバイスへの接続時に、AnyConnect クライアントの接続リストでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。

グループ URL のリストも設定できます。このリストは、リモートアクセス VPN 接続を開始するときにエンドポイントが選択できるリストです。ユーザがグループ URL を使用して接続する場合、システムは自動的に URL と一致する接続プロファイルを使用します。この URL は、まだ AnyConnect クライアントがインストールされていないクライアントによって使用されます。

グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意でなければなりません。グループ URL は **https://** で始める必要があります。

たとえば、「Contractor」というエイリアスとグループ URL

「<https://ravpn.example.com/contractor>」があるとします。AnyConnect クライアントをインストールすると、ユーザは単純に AnyConnect VPN の接続ドロップダウンリストでグループエイリアスを選択します。

ステップ 5 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。

これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザ認証方法が決定されます。最も簡単な方法は、AAA のみを使用し、次に AD レルムを選択するか、LocalIdentitySource を使用することです。[認証タイプ (Authentication Type)] には次の方法を使用できます。

- [AAAのみ (AAA Only)] : ユーザ名とパスワードに基づいてユーザを認証および認可します。詳細については、[接続プロファイルのための AAA の設定 \(624 ページ\)](#) を参照してください。
- [クライアント証明書のみ (Client Certificate Only)] : クライアントデバイスアイデンティティ証明書に基づいてユーザを認証します。詳細については、[接続プロファイルのための証明書認証の設定 \(627 ページ\)](#) を参照してください。
- [AAAおよびクライアント認証 (AAA and Client Certificate)] : ユーザ名/パスワードと、クライアントデバイスアイデンティティ証明書の両方を使用します。

ステップ 6 クライアントのアドレスプールを設定します。

アドレスプールは、リモートクライアントが VPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、[RA VPN のクライアントアドレス指定の設定 \(627 ページ\)](#) を参照してください。

ステップ 7 [次へ (Next)] をクリックします。

ステップ 8 このプロファイルを使用するには、[グループポリシー (Group Policy)] を選択します。

グループポリシーは、トンネル確立後のユーザ接続の期間を設定します。システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

グループポリシーを選択すると、グループの特性の概要が表示されます。変更するには概要内で [編集 (Edit)] をクリックします。

必要なグループポリシーが存在しない場合は、ドロップダウンリストの [新しいグループポリシーの作成 (Create New Group Policy)] をクリックします。

グループポリシーの詳細については、[RA VPN のグループポリシーの設定 \(628 ページ\)](#) を参照してください。

ステップ 9 [次へ (Next)] をクリックします。

ステップ 10 グローバル設定を行います。

これらのオプションは、各接続プロファイルに適用されます。最初の接続プロファイルを作成したら、これらのオプションは後続の各プロファイルに事前設定されます。変更すると、設定済みのすべての接続プロファイルが変更されます。

- [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。
- [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] : VPN トラフィックにアクセス制御ポリシーを適用するかどうか。復号された VPN トラフィックは、デフォルトでアクセスコントロールポリシーインスペクションの対象となります。[復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] を有効にすると、アクセス制御ポリシーはバイパスされますが、リモートアクセス VPN の場合、

VPN フィルタ ACL および AAA サーバからダウンロードされた認証 ACL は引き続き VPN トラフィックに適用されます。

このオプションを選択すると、システムによりグローバル設定である **sysopt connection permit-vpn** コマンドが設定されることに注意してください。これは、サイト間 VPN 接続の動作にも影響を与えます。また、接続プロファイル全体でこのオプションに異なる選択をすることはできません。この機能は、すべてのプロファイルでオンまたはオフのいずれかとなります。

このオプションを選択しない場合、外部ユーザがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。内部リソースへアクセスすることをアクセスプールに許可するアクセス制御ルールを作成する必要があるため、このような状況が発生します。アクセス制御ルールを使用する場合は、送信元 IP アドレス単独ではなく、ユーザ仕様を使用してアクセスを制御することを検討してください。

このオプションを選択する欠点は、VPN トラフィックが検査されないことです。つまり、侵入/ファイル保護、URL フィルタリング、またはその他の高度な機能がトラフィックに適用されません。これは、トラフィックに対する接続イベントは発生せず、したがって統計ダッシュボードでは VPN 接続が反映されないことも意味します。

- [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。

これはすべての接続プロファイルに適用されるグローバルオプションであることに注意してください。したがって、インターフェイスおよび内部ネットワークは追加するだけで、交換しないでください。そうでない場合、すでに定義済みのその他の接続プロファイルすべてに対する NAT 免除設定が変更されます。

- [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 パッケージ (AnyConnect Packages)] : RA VPN 接続でサポートする AnyConnect の完全インストール 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。ただし、異なる接続プロファイルで異なるパッケージを設定することはできません。別のプロファイルパッケージがすでに設定されている場合、そのパッケージが事前に選択されます。変更すると、すべてのプロファイルが変更されます。

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 11 [次へ (Next)] をクリックします。

ステップ 12 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 13 [終了 (Finish)] をクリックします。

次のタスク

[リモートアクセス VPN によるトラフィックの許可 \(617 ページ\)](#) で説明したように、トラフィックが VPN トンネルで許可されていることを確認します。

接続プロファイルのための AAA の設定

認証、認可、およびアカウントिंग (AAA) サーバは、ユーザがリモートアクセス VPN へのアクセスを許可されるかどうかを判断するためにユーザ名とパスワードを使用します。RADIUS サーバを使用する場合は、保護されたリソースへの差分アクセスを提供するために、認証されたユーザ間で認可レベルを区別できます。使用状況を追跡するために RADIUS アカウントングサービスを使用することもできます。

AAA を設定する際に、プライマリアイデンティティソースを設定する必要があります。セカンダリソースとフォールバックソースはオプションです。RSA トークンや DUO などを使用する二重認証を実装する場合は、セカンダリソースを使用します。

プライマリアイデンティティソースのオプション

- [ユーザ認証用のプライマリアイデンティティソース (Primary Identity Source for User Authentication)] : リモートユーザの認証に使用されるプライマリアイデンティティソース。VPN 接続を完了するには、エンドユーザがこのソースか任意のフォールバックソースで定義されている必要があります。次のいずれかを選択します。
 - Active Directory (AD) のアイデンティレルム。必要なレルムがまだ存在しない場合、[新規アイデンティレルムの作成 (Create New Identity Realm)] をクリックします。
 - RADIUS サーバグループ。
 - LocalIdentitySource (ローカルユーザデータベース) : デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。

- Duo LDAP サーバ。ただし、[Duo LDAP を使用した二要素認証の設定方法 \(649 ページ\)](#) の説明に従って、二要素認証を提供するためのセカンダリ認証ソースとして使用するのが最適です。プライマリ ソースとして使用する場合、ユーザ ID 情報は取得されません。ダッシュボードにユーザ情報が表示されず、ユーザベースのアクセス制御ルールを作成することもできません。
- [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。
- [削除オプション (Strip options)] : レルムとは管理ドメインのことです。次のオプションを有効にすると、ユーザ名だけに基づいて認証できます。これらのオプションを任意に組み合わせることで有効にできます。ただし、サーバが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
 - [ユーザ名からアイデンティティソースサーバを削除 (Strip Identity Source Server from Username)] : ユーザ名を AAA サーバに渡す前に、ユーザ名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザがユーザ名として domain\username を入力すると、ドメインがユーザ名から取り除かれ、認証用に AAA サーバに送信されます。デフォルトでは、このオプションはオフになっています。
 - [ユーザ名からグループを削除 (Strip Group from Username)] : ユーザ名を AAA サーバに渡す前に、ユーザ名からグループ名を削除するかどうか。このオプションは、username@domain 形式で指定された名前に適用され、ドメインと @ 記号が削除されます。デフォルトでは、このオプションはオフになっています。

セカンダリ アイデンティティ ソース

- [ユーザ認証用のセカンダリアイデンティティソース (Secondary Identity Source for User Authentication)] : オプションの 2 番目のアイデンティティ ソースです。ユーザがプライマリソースで正常に認証されると、セカンダリソースでの認証が求められます。AD レルム、RADIUSサーバグループ、DuoLDAPサーバ、またはローカルアイデンティティ ソースを選択することができます。
- [詳細オプション (Advanced options)] : [詳細 (Advanced)] リンクをクリックし、次のオプションを設定します。
 - [セカンダリ用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 for Secondary)] : セカンダリソースが外部サーバの場合、セカンダ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、必ずセカンダリ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。
 - [セカンダリログインにプライマリユーザ名を使用 (Use Primary Username for Secondary Login)] : デフォルトでは、セカンダリアイデンティティ ソースを使用する場合、セ

カンダリソースに対してユーザ名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリアイデンティティソースに対して認証されたものと同じユーザ名をセカンダリソースに対して使用します。プライマリおよびセカンダリアイデンティティソースの両方で同じユーザ名を設定する場合は、このオプションを選択します。

- [セッションサーバのユーザ名 (Username for Session Server)] : 認証に成功すると、ユーザ名はイベントと統計ダッシュボードに表示され、ユーザベースまたはグループベースのSSL復号化およびアクセス制御ルールに一致するものを判断するために使用され、アカウントングに使用されます。2つの認証ソースを使用しているため、ユーザアイデンティティとして、プライマリまたはセカンダリのどちらのユーザ名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。
- [パスワードタイプ (Password Type)] : セカンダリサーバのパスワードを取得する方法。デフォルトは[プロンプト (Prompt)]で、ユーザにパスワードの入力が求められることを意味します。

プライマリサーバへのユーザ認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード (Primary Identity Source Password)]を選択します。

すべてのユーザに同じパスワードを使用するには、[共通パスワード (Common Password)]を選択し、[共通パスワード (Common Password)]フィールドにそのパスワードを入力します。

その他のオプション

- [認証サーバ (Authorization Server)] : リモートアクセスVPNユーザを認証するように設定されたRADIUSサーバグループです。

認証の完了後、認可によって、認証済みの各ユーザが利用できるサービスおよびコマンドが制御されます。認可は、ユーザが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザに対して同じアクセス権を提供します。認証用のRADIUSの設定については、[RADIUS およびグループポリシーを使用したユーザの権限および属性の制御 \(608 ページ\)](#) を参照してください。

システムがグループポリシーで定義されているものと重複する認可属性をRADIUSサーバから取得した場合、RADIUS属性は、グループポリシー属性をオーバーライドすることに注意してください。

- [アカウントングサーバ (Accounting Server)] : (オプション) リモートアクセスVPNセッションへのアカウントングに使用するRADIUSサーバグループ。

アカウントングは、ユーザがアクセスしているサービスや、ユーザが消費しているネットワークリソース量を追跡します。FTDデバイスは、RADIUSサーバにユーザのアクティビティを報告します。アカウントング情報には、セッションの開始時刻と停止時刻、ユーザ名、セッションごとのデバイスを通じたバイト数、使用されたサービス、および

各セッションの時間が含まれています。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウントリングは、単独で使用するか、認証および認可とともに使用することができます。

接続プロファイルのための証明書認証の設定

リモートアクセス VPN 接続を認証するために、クライアントデバイスにインストールされた証明書を使用することができます。

クライアント証明書を使用しても、セカンダリ アイデンティティ ソース、フォールバックソース、および認証およびアカウントリングサーバを引き続き設定できます。これらは AAA オプションです。詳細については[接続プロファイルのための AAA の設定 \(624 ページ\)](#)を参照してください。

証明書固有の属性を次に示します。プライマリおよびセカンダリ アイデンティティ ソースに対して、個別にこれらの属性を設定することができます。セカンダリソースの設定はオプションです。

- [証明書のユーザ名 (Username from Certificate)] : 次のいずれかを選択します。
 - [マップ固有フィールド (Map Specific Field)] : 証明書の要素を [プライマリフィールド (Primary Field)] および [セカンダリフィールド (Secondary Field)] の順番で使用します。デフォルトは CN (共通名) および OU (組織単位) です。組織にとって有効なオプションを選択します。これらのフィールドを組み合わせてユーザ名が提供され、このユーザ名がイベント、ダッシュボード、さらに SSL 復号とアクセス制御ルールでのマッチング目的に使用されます。
 - [DN (識別名) 全体をユーザ名として使用 (Use entire DN (distinguished name) as username)] : システムが自動的に DN フィールドからユーザ名を導出します。
- [詳細オプション (Advanced options)] : [詳細 (Advanced)] リンクをクリックし、次のオプションを設定します。
 - [ユーザログインウィンドウの証明書からユーザ名を事前入力 (Prefill username from certificate on user login window)] : ユーザに認証を要求するときに、取得したユーザ名をユーザ名フィールドに入力するかどうか。
 - [ログインウィンドウでユーザ名を非表示にする (Hide username in login window)] : [事前入力 (Prefill)] オプションを選択すると、ユーザ名を非表示にできます。これは、ユーザがパスワードプロンプトでユーザ名を編集できないことを意味します。

RA VPN のクライアントアドレス指定の設定

リモートアクセス VPN に接続するエンドポイントにシステムが IP アドレスを提供するための方法が必要です。これらのアドレスは、AAA サーバ、DHCP サーバ、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールによって提供されます。システムは、この順序でこれらのリソースを試行し、使用可能なアドレ

スを取得すると停止し、次にアドレスをクライアントに割り当てます。このように、同時接続数が異常な場合のフェールセーフを作成するために複数のオプションを設定できます。

接続プロファイルのアドレスプールを設定するには、次の方法の1つ以上を使用します。

- [AAAサーバ (AAA Server)]: まず、アドレスプールのサブネットを指定する FTD デバイスのネットワークオブジェクトを設定します。次に、RADIUSサーバで、そのオブジェクト名を使用してユーザの Address-Pools (217) 属性を設定します。また、接続プロファイルで認証用の RADIUS サーバを指定します。
- [DHCP]: まず、1つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバを設定します (DHCP を使用して IPv6 プールを設定することはできません)。次に、DHCP サーバの IP アドレスでホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバ (DHCP Servers)] 属性で選択できます。複数の DHCP サーバを設定することができます。

DHCP サーバに複数のアドレスプールがある場合、[DHCPスコープ (DHCP Scope)] 属性を接続プロファイルにアタッチするグループポリシーで使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホスト ネットワーク オブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。

- [ローカルIPアドレスプール (Local IP address pools)]: まず、サブネットを指定する最大 6 つのネットワーク オブジェクトを作成します。IPv4 と IPv6 に個別のプールを設定できます。次に、グループポリシーまたは接続プロファイルの [IPv4アドレスプール (IPv4 Address Pool)] および [IPv6アドレスプール (IPv6 Address Pool)] オプションで、これらのオブジェクトを選択します。IPv4 と IPv6 の両方を設定する必要はなく、サポートするアドレス方式のみを設定します。

また、グループポリシーと接続プロファイルの両方でプールを設定する必要もありません。グループポリシーは接続プロファイル設定をオーバーライドします。そのため、グループポリシーでプールを設定する場合は、接続プロファイルのオプションを空白のままにしてください。

プールはリストの順序で使用されることに注意してください。

RA VPN のグループポリシーの設定

グループポリシーは、リモートアクセス VPN 接続のための一連のユーザ指向の属性と値のペアです。接続プロファイルでは、トンネル確立後、ユーザ接続の条件を設定するグループポリシーが使用されます。グループポリシーを使用すると、ユーザまたはユーザのグループに属性セット全体を適用できるので、ユーザごとに各属性を個別に指定する必要がありません。

システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

手順

ステップ 1 [デバイス (Device)] > [リモートアクセスVPN (Remote Access VPN)] グループで [設定の表示 (View Configuration)] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次で [グループポリシー (Group Policy)] 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。

- 新しいグループを作成するには、[+] ボタンをクリックします。グループポリシーのページの属性の説明については、次のトピックを参照してください。
 - [一般属性 \(629 ページ\)](#)
 - [セッション設定属性 \(630 ページ\)](#)
 - [アドレス割り当て属性 \(631 ページ\)](#)
 - [スプリット トンネリング属性 \(631 ページ\)](#)
 - [AnyConnect 属性 \(633 ページ\)](#)
 - [トラフィック フィルタ属性 \(634 ページ\)](#)
 - [Windows ブラウザ プロキシ属性 \(635 ページ\)](#)
- 既存のグループポリシーを編集するには、編集ボタン (🔍) をクリックします。
- 不要なグループを削除するには、削除ボタン (🗑️) をクリックします。現在、グループを接続プロファイルで使用することはできません。

一般属性

グループポリシーの全般的な属性では、グループの名前およびその他の基本設定を定義します。[名前 (Name)] 属性は唯一の必須属性です。

- [名前 (Name)] : グループ ポリシーの名前。名前には最大 64 文字の長さを使用でき、スペースも使用できます。
- [説明 (Description)] : デバイス グループの説明。説明には、最大 1,024 文字を使用できます。
- [DNSサーバ (DNS Servers)] : VPNに接続する際、クライアントがドメイン名の解決に使用する DNS サーバを定義する DNS サーバグループを選択します。必要なグループがまだ定義されていない場合は、[DNSグループの作成 (Create DNS Group)] をクリックしてすぐに作成します。

- **Banner** : ユーザのログイン時に表示するバナーテキストまたはウェルカムメッセージです。デフォルトでは、バナーは表示されません。最大文字数は496文字です。AnyConnectクライアントは、部分的なHTMLをサポートします。リモートユーザへバナーが適切に表示されることを確認するには、
 タグを使用して改行を示します。
- [デフォルトドメイン (Default Domain)] : RA VPN内のユーザのデフォルトドメインの名前。例、example.com。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。
- [AnyConnectクライアントプロファイル (AnyConnect Client Profiles)] : [+] をクリックし、このグループに使用する AnyConnect クライアントプロファイルを選択します。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（接続プロファイルで）、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。

セッション設定属性

グループポリシーのセッションの設定は、VPNを通じて接続できる時間と、接続を確立できる個別の接続数を制御します。

- [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。
- [接続時間のアラート間隔 (Connection Time Alert Interval)] : 最大接続時間を指定した場合、アラート間隔は、次の自動切断についてユーザに警告を表示する、最大時間に達するまでの時間を定義します。ユーザは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは1分です。1～30分を指定できます。
- [アイドル時間 (Idle Time)] : VPN 接続がアイドル状態のままの場合、自動的にクローズされるまでの時間の長さ（分単位）。1～35791394で指定します。この分単位での連続期間中に接続で通信アクティビティがない場合、接続は終了します。デフォルトは30分です。
- [アイドル時間のアラート間隔 (Idle Time Alert Interval)] : アイドルセッションが原因の次の自動切断について、ユーザにアラートを表示するアイドル時間に達するまでの時間。アクティビティがあるとタイマーがリセットされます。デフォルトは1分です。1～30分を指定できます。
- [ユーザあたり同時ログイン (Simultaneous Logins Per User)] : ユーザに許可する同時接続の最大数。デフォルトは3です。1～2147483647個の接続を指定できます。複数の同時接

続を許可するとセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

アドレス割り当て属性

グループポリシーのアドレスの割り当て属性は、グループのIPアドレスプールを定義します。ここで定義されているプールは、このグループを使用するすべての接続プロファイルで定義済みのプールをオーバーライドします。接続プロファイルで定義済みのプールを使用する場合は、これらの設定を空白のままにします。

- [IPv4アドレスプール (IPv4 Address Pool)]、[IPv6アドレスプール (IPv6 Address Pool)] : 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たくない場合は、リストを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。

ローカルアドレスの割り当てに使用する最大6個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムでは、プールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

- [DHCPスコープ (DHCP Scope)] : 接続プロファイルのアドレスプールにDHCPサーバを設定した場合、DHCPスコープはこのグループのプールに使用するサブネットを識別します。DHCPサーバには、スコープで識別される同じプールのアドレスも必要です。スコープを使用すると、この特定のグループに使用するDHCPサーバで定義されているアドレスプールのサブセットを選択できます。

ネットワークスコープを定義しない場合、DHCPサーバはアドレスプールの設定順にプール内を探してIPアドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

スコープを指定するには、ネットワーク番号のホストアドレスを含むネットワークオブジェクトを選択します。オブジェクトがまだ存在しない場合は、[新しいネットワークの作成 (Create New Network)]をクリックします。たとえば、192.168.5.0/24 サブネットプールのアドレスを使用するようにDHCPサーバに指示するには、ホストアドレスとして192.168.5.0を指定するネットワークオブジェクトを選択します。DHCPはIPv4アドレス指定にのみ使用することができます。

スプリット トンネリング属性

グループポリシーのスプリットトンネリング属性は、システムが内部ネットワーク用のトラフィックと外部方向トラフィックを処理する方法を定義します。スプリットトンネリングは、一部のネットワークトラフィックをVPNトンネルに誘導して通過させ（暗号化）、残りのネットワークトラフィックをVPNトンネルの外に誘導します（非暗号化、つまりクリアテキストの状態）。

- [IPv4スプリットトンネリング (IPv4 Split Tunneling)]、[IPv6スプリットトンネリング (IPv6 Split Tunneling)]: トラフィックが IPv4 または IPv6 アドレスを使用するかどうかによって、さまざまなオプションを指定できますが、それぞれのオプションは同じです。スプリットトンネリングを有効にする場合は、ネットワークオブジェクトの選択が必要となるオプションのいずれかを指定します。
 - [トンネル経由のトラフィックをすべて許可する (Allow all traffic over tunnel)]: スプリットトンネリングを行いません。ユーザが RA VPN 接続を行うと、ユーザのすべてのトラフィックは保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。
 - [トンネル経由で指定されたトラフィックを許可する (Allow specified traffic over the tunnel)]: 宛先ネットワークとホストアドレスを定義するネットワーク オブジェクトを選択します。これらの宛先へのトラフィックは保護されたトンネルを通過します。その他のすべての宛先へのトラフィックは、クライアントによって、トンネル外の接続 (ローカル Wi-Fi またはネットワーク接続など) にルーティングされます。
 - [以下に指定したネットワークを除外する (Exclude networks specified below)]: 宛先ネットワークまたは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選択します。これらの宛先へのトラフィックは、クライアントによって、トンネルの外の接続にルーティングされます。その他の宛先へのトラフィックは、トンネルを通過します。
- [スプリットDNS (Split DNS)]: クライアントが、クライアントで設定されている DNS サーバに他の DNS 要求を送信することを許可しながら、セキュアな接続を介していくつかの DNS 要求を送信するようにシステムを設定することができます。次の DNS の動作を設定することができます。
 - [スプリットトンネルポリシーに従ってDNS要求を送信する (Send DNS Request as per split tunnel policy)]: このオプションでは、スプリットトンネルオプションが定義されているのと同じ方法で DNS 要求が処理されます。スプリットトンネリングを有効にすると、DNS 要求は宛先アドレスに基づいて送信されます。スプリットトンネリングを有効にしていない場合、DNS 要求はすべて保護された接続を介します。
 - [常にトンネル経由でDNS要求を送信する (Always send DNS requests over tunnel)]: スプリットトンネリングを有効にするが、すべての DNS 要求をグループで定義された DNS サーバに保護された接続を介して送信する場合は、このオプションを選択します。
 - [指定したドメインのみをトンネル経由で送信 (Send only specified domains over tunnel)]: 保護された DNS サーバが特定のドメインのアドレスだけを解決するようにしたい場合は、このオプションを選択します。次に、これらのドメインを指定します。ドメイン名はコンマで区切ります。たとえば、example.com, example1.com のように指定します。内部 DNS サーバが内部ドメインの名前を解決し、外部 DNS サーバが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

AnyConnect 属性

グループポリシーの AnyConnect 属性は、AnyConnect クライアントでリモートアクセス VPN 接続に使用されるいくつかの SSL および接続設定を定義します。

SSL 設定

- [Datagram Transport Layer Security (DTLS) の有効化 (Enable Datagram Transport Layer Security (DTLS))] : AnyConnect クライアントが SSL トンネルおよび DTLS トンネルの 2 つのトンネルを同時に使用することを許可するかどうか。DTLS によって、一部の SSL 接続に関連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。DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアントユーザは SSL トンネルのみで接続します。
- [DTLS 圧縮 (DTLS Compression)] : LZS を使用してこのグループの Datagram Transport Layer Security (DTLS) 接続を圧縮するかどうか。[DTLS 圧縮 (DTLS Compression)] はデフォルトで無効になっています。
- [SSL 圧縮 (SSL Compression)] : データ圧縮を有効にするかどうか。有効にする場合は、使用するデータ圧縮の方法 ([圧縮 (Deflate)] または [LZS (LZS)])。[SSL 圧縮 (SSL Compression)] はデフォルトで無効になっています。データ圧縮は、伝送速度を上げますが、各ユーザセッションのメモリ要件と CPU 使用率も高めます。したがって、SSL 圧縮ではデバイスの全体的なスループットが低下します。
- [SSL キーの再生成方法 (SSL Rekey Method)]、[SSL キーの再生成間隔 (SSL Rekey Interval)] : クライアントは、暗号キーと初期化ベクトルを再ネゴシエートしながら VPN 接続キーを再生成して、接続のセキュリティを強化します。[なし (None)] を選択するとキーの再生成が無効になります。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル (New Tunnel)] を選択します ([既存トンネル (Existing Tunnel)] オプションを選択しても [新しいトンネル (New Tunnel)] と同じ動作になります)。キーの再生成を有効にする場合、キーの再生成間隔も設定します。これはデフォルトでは 4 分です。間隔は、4 ~ 10080 分 (1 週間) まで設定できます。

接続の設定

- [DF (フラグメント化しない) ビットを無視する (Ignore the DF (Don't Fragment) bit)] : フラグメント化が必要なパケットの Don't Fragment (DF) ビットを無視するかどうか。DF ビットがセットされたパケットの強制フラグメンテーションを許可し、これらのパケットがトンネルを通過できるようにするには、このオプションを選択します。
- [クライアントバイパスプロトコル (Client Bypass Protocol)] : セキュアゲートウェイによる (IPv6 トラフィックだけを予期しているときの) IPv4 トラフィックの管理方法や、(IPv4 トラフィックだけを予期しているときの) IPv6 トラフィックの管理方法を設定することができます。

AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に

IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合に、ヘッドエンドが IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアントプロトコルバイパスによってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できるようになりました。

たとえば、セキュアゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアントバイパスプロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアントバイパスプロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリアテキストとして送信されます。

- [MTU] : Cisco AnyConnect VPN クライアントによって確立された SSL VPN 接続の最大伝送単位 (MTU) サイズ。デフォルトは 1406 バイトです。576 ~ 1462 バイトの範囲を使用できます。
- [AnyConnect と VPN ゲートウェイ間のキープアライブメッセージ (Keepalive Messages Between AnyConnect and VPN Gateway)] : トンネルでのデータ送受信にピアを使用できることを示すために、ピア間でキープアライブメッセージを交換するかどうかを指定します。キープアライブメッセージは、設定された間隔で送信されます。デフォルトの間隔は 20 秒、有効な範囲は 15 ~ 600 秒です。
- [ゲートウェイ側の間隔での DPD (DPD on Gateway Side Interval)]、[クライアント側の間隔での DPD (DPD on Client Side Interval)] : ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection (DPD) を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。デフォルトの DPD メッセージの送信間隔は 30 秒です。間隔は、5 ~ 3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザに適用する制限を定義します。アクセスコントロールポリシールールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネットアドレスとプロトコル、または VLAN に基づいて、特定のリソースに RA VPN ユーザを制限することができます。

デフォルトでは、RA VPN ユーザは、保護されたネットワーク上の宛先へのアクセスがグループポリシーによって制限されることはありません。

- [アクセスリストのフィルタ (Access List Filter)] : 拡張アクセスコントロールリスト (ACL) を使用してアクセスを制限します。スマート CLI 拡張 ACL オブジェクトを選択するか、または [拡張アクセスリストの作成 (Create Extended Access List)] をクリックして作成します。

拡張 ACL では、送信元アドレス、宛先アドレス、およびプロトコル (IP TCP など) に基づいたフィルタリングが可能です。ACL は、トップダウン型の最初の一貫ベースで評価されるため、より一般的なルールの前に具体的なルールを配置するようにしてください。

ACL の末尾には、暗黙的な「deny any」があります。そのため、いくつかのサブネットへ

のアクセスだけを拒否しながら、他のすべてのアクセスを許可する場合は、ACLの最後に「permit any」ルールを含めるようにしてください。

拡張 ACL スマート CLI オブジェクトを編集しながらネットワークオブジェクトを作成することはできないため、グループポリシーを編集する前に、ACLを作成する必要があります。そうしないと、単純にオブジェクトを作成し、後でもう一度ネットワークオブジェクトを作成し、その後で必要なすべてのアクセス制御エントリを作成する必要があります。ACLを作成するには、[デバイス (Device)] > [詳細設定 (Advanced Configuration)] > [スマートCLI (Smart CLI)] > [オブジェクト (Object)] に移動し、オブジェクトを作成して、オブジェクトタイプとして [拡張アクセスリスト (Extended Access List)] を選択します。例については、[グループによってRA VPNアクセスを制御する方法 \(679 ページ\)](#) を参照してください。

- [VPNをVLANに制限 (Restrict Access to VLAN)] : (オプション) 「VLAN マッピング」とも呼ばれます。この属性により、このグループポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。システムは、このグループからのトラフィックすべてを、選択した VLAN に転送します。

この属性を使用して VLAN をグループポリシーに割り当て、アクセスコントロールを簡素化します。この属性に値を割り当てる方法は、ACLを使用してセッションのトラフィックをフィルタリングする方法の代替方法です。デバイスのサブインターフェイスで定義されている VLAN 番号を指定していることを確認します。値の範囲は 1 ~ 4094 です。

Windows ブラウザ プロキシ属性

グループポリシーの Windows のブラウザプロキシ属性は、ユーザのブラウザで定義されたプロキシが動作するかどうか、およびその動作方法を決定します。

[VPNセッション中のブラウザプロキシ (Browser Proxy During VPN Sessions)] には、次の値のいずれかを選択できます。

- [エンドポイント設定のまま (No change in endpoint settings)] : HTTP のブラウザプロキシを設定するかどうかをユーザが決定できます。設定されている場合、そのプロキシが使用されます。
- [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)] : クライアントデバイスの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。
- [カスタム設定を使用 (Use custom settings)] : HTTP トラフィックに対してすべてのクライアントデバイスで使用する必要があるプロキシを定義します。次を設定します。
 - [プロキシサーバのIPまたはホスト名 (Proxy Server IP or Hostname)]、[ポート (Port)] : プロキシサーバの IP アドレスまたはホスト名、およびプロキシサーバが使用するプロキシ接続のポート。ホストとポートの組み合わせは、100 文字を超えることはできません。

- [ブラウザ免除リスト (Browser Exemption List)]: 免除リストにあるホスト/ポートへの接続はプロキシを経由しません。プロキシを使用すべきでない宛先のすべてのホスト/ポート値を追加します。たとえば、`www.example.com` ポート 80 などです。[プロキシ例外の追加 (Add Proxy Exception)] をクリックしてリストに項目を追加します。項目を削除するには、ゴミ箱アイコンをクリックします。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。

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 \(663 ページ\)](#) 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。
 - VPN フィルタがトラフィックをブロックしています。接続プロファイルのグループポリシーで設定されている ACL トラフィック フィルタまたは VLAN フィルタを確認します。グループポリシーに基づいてトラフィックをフィルタリングしている場合、

またはその方法によっては、ACL で調整を行うか、VLAN を変更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過しており、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。

RADIUS 認可変更の実装方法

ダイナミック認証とも呼ばれる RADIUS 認可変更 (CoA) は、FTD リモートアクセス VPN にエンドポイントセキュリティを提供します。RA VPN の重要な課題は、侵害されたエンドポイントから内部ネットワークを保護し、ウイルスまたはマルウェアの影響を受けた場合はエンドポイントへの攻撃を修復することで、エンドポイント自体を保護することです。RA VPN セッションの前後だけでなく途中も含め、すべてのフェーズでエンドポイントおよび内部ネットワークを保護する必要があります。RADIUS CoA 機能は、この目的を達成するために役立ちます。

Cisco Identity Services Engine (ISE) RADIUS サーバを使用する場合は、認可変更ポリシーの適用を設定できます。

ISE 認可変更機能は、認証、認可、およびアカウントティング (AAA) セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザグループのポリシーが変更されると、ISE は CoA メッセージを FTD デバイスに送信して認証を再初期化し、新しいポリシーを適用します。Inline Posture Enforcement Point (IPEP) では、FTD デバイスによって確立された各 VPN セッションにアクセスコントロールリスト (ACL) を適用する必要はありません。

ここでは、CoA の動作とその設定方法について説明します。

認可変更へのシステムフロー

Cisco ISE には、プロセス、ファイル、レジストリエントリ、ウイルス対策保護、スパイウェア対策保護、およびホストにインストールされているファイアウォールソフトウェアなどの条件に対するエンドポイントの準拠状況を評価するクライアント ポスチャ エージェントがあります。管理者はその後、エンドポイントが条件に準拠するまでネットワークアクセスを制限したり、修復方法を確立できるようにローカルユーザの権限を昇格したりできます。ISE ポスチャは、クライアント側評価を実行します。クライアントは、ISE からポスチャ要件ポリシーを受信し、ポスチャデータ収集を実行し、結果をポリシーと比較し、評価結果を ISE に返します。

次に、認可変更 (CoA) 処理のための FTD デバイス、ISE、および RA VPN クライアントの間のシステムフローを示します。

1. リモートユーザは、AnyConnect クライアントを使用して、FTD デバイスとの RA VPN セッションを開始します。
2. FTD デバイスはそのユーザの RADIUS Access-Request メッセージを ISE サーバに送信します。
3. クライアントポスチャはこの時点で不明であるため、ISE は不明なポスチャに対して設定されている認証ポリシーにユーザを一致させます。このポリシーは、ISE が RADIUS Access-Accept の応答で FTD に送信する次の `cisco-av-pair` オプションを定義します。

- `url-redirect-acl=acl_name`。ここで `acl_name` は FTD デバイスで設定された拡張 ACL の名前です。この ACL は、どのユーザトラフィックを ISE サーバにリダイレクトすべきか (HTTP トラフィック) を定義します。次に例を示します。

```
url-redirect-acl=redirect
```

- `url-redirect=url` : トラフィックのリダイレクト先 URL。次に例を示します。

```
url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
```

ホスト名を解決できるように、データインターフェイスの DNS を設定する必要があります。接続プロファイルのグループポリシーにトラフィックフィルタリングも設定する場合は、クライアントプールがポート (この例では TCP/8443) 経由で ISE サーバに到達できることを確認します。

4. FTD デバイスは RADIUS Accounting-Request 開始パケットを送信し、ISE から応答を受信します。アカウントティング要求には、セッション ID、VPN クライアントの外部 IP アドレ

ス、FTD デバイスの IP アドレスを含む、セッションの詳細がすべて含まれます。ISE はセッション ID を使用してセッションを識別します。FTD デバイスはさらに、定期的な中間アカウント情報を送信します。この情報で最も重要な属性は、FTD デバイスによってクライアントに割り当てられている IP アドレスを持つ Framed-IP-Address です。

5. 不明なポスチャ状態では、FTD デバイスがリダイレクト ACL に一致するクライアントからのトラフィックを、リダイレクト URL へとリダイレクトします。ISE は、必要なポスチャコンプライアンスモジュールがクライアントにあるかどうかを判断し、必要に応じてユーザにインストールを指示します。
6. エージェントは、クライアントデバイスにインストールされると、ISE ポスチャポリシーで設定されたチェックを自動的に実行します。クライアントは ISE と直接通信します。クライアントは ISE にポスチャレポートを送信します。このレポートには、SWISS プロトコルおよびポート TCP/UDP 8905 を使用した複数の交換を含めることができます。
7. ISE がエージェントからポスチャレポートを受信すると、認証ルールをもう一度処理します。この時点でポスチャ結果が認識され、異なるルールがクライアントと一致するようになります。ISE は RADIUS CoA のパケットを送信します。このパケットには準拠または非準拠のいずれかのエンドポイント向けのダウンロード可能 ACL (DACL) が含まれます。たとえば、準拠 DACL はすべてのアクセスを許可しますが、非準拠 DACL はすべてのアクセスを拒否することがあります。DACL の内容は ISE 管理者によって決まります。
8. FTD デバイスはリダイレクションを削除します。このデバイスが DACL をキャッシュしていない場合、デバイスは ISE からダウンロードするために Access-Request を送信する必要があります。特定の DACL が VPN セッションに関連付けられますが、デバイス構成の一部にはなりません。
9. RA VPN ユーザがもう一度 Web ページにアクセスしようとする時、ユーザはそのセッション用に FTD にインストールされている DACL によって許可されたすべてのリソースにアクセスできます。



- (注) エンドポイントが必須要件を満たすことができず、手動修復が必要な場合は、AnyConnect クライアントで修復ウィンドウが開き、対応が必要な項目が表示されます。修復ウィンドウはバックグラウンドで実行されるため、ネットワークアクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。AnyConnect クライアントの ISE ポスチャタイトル部分で [詳細 (Details)] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。

FTD デバイスでの認可変更の設定

認可変更ポリシーのほとんどは、ISE サーバで設定されます。ただし、正しく ISE に接続するように FTD デバイスを設定する必要があります。次の手順では、FTD 側の設定方法について説明します。

始める前に

任意のオブジェクトでホスト名を使用する場合、[データと管理インターフェイスの DNS の設定 \(700 ページ\)](#) で説明したように、データインターフェイスに使用できるように DNS サーバが設定されていることを確認します。通常、システムが完全に機能するように DNS を設定する必要があります。

手順

ステップ 1 ISE への初期接続をリダイレクトするように、拡張アクセスコントロールリスト (ACL) を設定します。

リダイレクト ACL の目的は、ISE がクライアントポスタチャを評価できるように、初期トラフィックを ISE に送信することです。ACL は HTTPS トラフィックを ISE に送信する必要がありますが、すでに宛先が ISE に指定されているトラフィック、または名前解決のために DNS サーバに送信されるトラフィックは除きます。リダイレクト ACL のサンプルは、次のようになります。

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

ただし、ACL には最後のアクセス制御エントリ (ACE) として暗黙の「deny any any」があることに注意してください。この例では、TCP ポート www (つまりポート 80) に一致する最後の ACE は、最初の 3 つの ACE に一致するすべてのトラフィックと一致しないため、これらは冗長となります。最後の ACE で ACL を作成するだけで、同じ結果を取得することができます。

なお、リダイレクト ACL では、許可および拒否アクションはどのトラフィックが ACL に一致するかを決定するだけであり、一致するものは許可し、一致しないものは拒否します。実際にはどのトラフィックもドロップされず、拒否されたトラフィックは ISE にリダイレクトされただけです。

リダイレクト ACL を作成するには、スマート CLI オブジェクトを設定する必要があります。

- [**デバイス (Device)**] > [**詳細設定 (Advanced Configuration)**] > [**スマート CLI (Smart CLI)**] > [**オブジェクト (Objects)**] を選択します。
- [+] をクリックして新しいオブジェクトを作成します。
- ACL の名前を入力します。たとえば、**redirect** などと入力します。
- [**CLI テンプレート (CLI Template)**] には、[**拡張アクセスリスト (Extended Access List)**] を選択します。
- [**テンプレート (Template)**] の本文で、次を設定します。
 - `configure access-list-entry action = permit`
 - `source-network = any-ipv4`
 - `destination-network = any-ipv4`
 - `configure permit port = any-source`

- destination-port = HTTP
- configure logging = disabled

ACE は、次のようになります。

Name	Description
redirect	

CLI Template

Extended Access List

Template

```

1 access-list redirect extended
2 configure access-list-entry permit
3 permit network source [ any-ipv4 ] destination [ any-ipv4 ]
4 configure permit port any-source
5 permit port source ANY destination [ HTTP ]
6 configure logging disabled
7 disabled log set log-level INFORMATIONAL log-interval 300

```

f) [OK] をクリックします。

この ACL は、次回変更を展開すると設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

(注) この ACL は、IPv4 にのみ適用されます。IPv6 のサポートも追加したい場合、送信元ネットワークと宛先ネットワークに any-ipv6 を選択すること以外は、すべて IPv4 と同じ属性にして 2 つ目の ACE を追加します。ISE または DNS サーバへのトラフィックはリダイレクトされないようにするために、他の ACE を追加することもできます。まず、これらのサーバの IP アドレスを保持するためのホストネットワーク オブジェクトを作成する必要があります。

ステップ 2 RADIUS サーバグループをダイナミック認証用に設定します。

ダイナミック認証とも呼ばれる認可変更を有効にするには、RADIUS サーバとサーバグループオブジェクトでいくつかの重要なオプションを正確に選択する必要があります。次の手順では、これらのオブジェクトの属性に焦点を当てています。これらのオブジェクトの詳細については、[RADIUS サーバおよびグループ \(188 ページ\)](#) を参照してください。

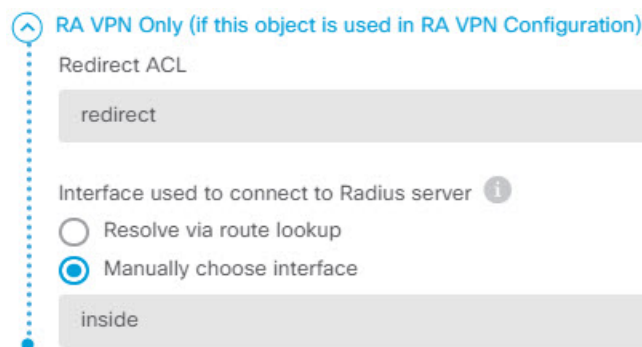
- [オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] を選択します。
- [+] > [RADIUSサーバ (RADIUS Server)] をクリックします。
- サーバの名前、ISE RADIUS サーバのホスト名/IP アドレス、認証ポート、およびサーバで設定されている秘密鍵を入力します。必要に応じてタイムアウトを調整します。これらのオプションはダイナミック認証に直接関係しません。
- [RA VPNのみ (RA VPN Only)] リンクをクリックし、次のオプションを設定します。

- [リダイレクトACL (Redirect ACL)]: リダイレクト用に作成した拡張 ACL を選択します。この例では、redirect と名付けられた ACL です。
- [RADIUSサーバに接続するために使用されるインターフェイス (Interface Used to Connect to RADIUS Server)]: [インターフェイスを手動で選択する (Manually Choose Interface)] を選択し、サーバに到達できるインターフェイスを選択します。システムがインターフェイスで CoA リスナーを適切に有効にできるように、特定のインターフェイスを選択する必要があります。

サーバが管理アドレスと同じネットワーク上にある場合（これは診断インターフェイスを選択することを意味します）、診断インターフェイスで IP アドレスを設定する必要もあります。管理 IP アドレスを設定するだけでは不十分です。[デバイス (Device)] > [インターフェイス (Interfaces)] に移動し、管理 IP アドレスと同じサブネット上にある診断インターフェイスで IP アドレスを設定します。

FDM 管理アクセスにもこのサーバを使用する場合、このインターフェイスは無視されます。管理アクセスの試行は、管理 IP アドレスを通じて常に認証されます。

次に、内部インターフェイスで設定するオプションの例を示します。



- e) [OK] をクリックしてサーバオブジェクトを保存します。
複数の重複する ISE RADIUS サーバによる冗長設定がある場合、これらのサーバそれぞれにサーバオブジェクトを作成します。
- f) [+] > [RADIUSサーバグループ (RADIUS Server Group)] をクリックします。
- g) サーバグループの名前を入力し、必要な場合は、デッドタイムと最大試行回数を調整します。
- h) [ダイナミック認証 (Dynamic Authorization)] オプションを選択し、ISE サーバが異なるポートを使用するように設定されている場合は、ポート番号を変更します。ポート 1700 は、CoA パケットをリッスンするために使用されるデフォルトのポートです。
- i) AD サーバを使用してユーザを認証するように RADIUS サーバが設定されている場合は、この RADIUS サーバと組み合わせて使用される AD サーバを指定する [RADIUSサーバをサポートするレルム (Realm that Supports the RADIUS Server)] を選択します。レルムが存在していない場合は、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。

- j) [RADIUSサーバ (RADIUS Server)] の下で[+]をクリックし、RA VPN用に作成したサーバオブジェクトを選択します。
- k) [OK] をクリックしてサーバグループオブジェクトを保存します。

ステップ3 [デバイス (Device)] > [RA VPN] > [接続プロファイル (Connection Profiles)] を選択し、この RADIUS サーバグループを使用する接続プロファイルを作成します。

[AAA認証 (AAA Authentication)] を使用し (単独または証明書と一緒に)、[ユーザ認証用のプライマリアイデンティティソース (Primary Identity Source for User Authentication)]、[認可 (Authorization)]、および[アカウンティング (Accounting)] オプションでサーバグループを選択します。

組織での要件に応じて、その他すべてのオプションを設定します。

(注) DNS サーバに VPN ネットワーク経由で到達する場合、接続プロファイルで使用されるグループポリシーを編集し、スプリット トンネリング属性ページで [スプリット DNS (Split DNS)] オプションを設定します。

ISE での認可変更の設定

認可変更設定のほとんどは、ISE サーバで行われます。ISE にはエンドポイントデバイス上で実行されるポスチャ アセスメント エージェントがあり、ISE はデバイスと直接通信してポスチャスタンスを決定します。FTD デバイスは基本的に、特定のエンドユーザの処理に関する ISE からの指示を待ちます。

ポスチャ アセスメント ポリシーの設定に関する詳細情報は、このマニュアルの範囲外です。ただし、次の手順で一部の基本情報を説明します。ISE の設定のスタート地点として活用してください。正確なコマンドパス、ページ名、および属性名は、リリースごとに変更される場合があります。使用している ISE のバージョンによっては、異なる用語または構成を使用する場合があります。

サポートされる最低限の ISE リリースは、2.2 パッチ 1 です。

始める前に

この手順では、ISE RADIUS サーバでユーザがすでに設定済みであると想定しています。

手順

ステップ1 [管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [ネットワークデバイス (Network Devices)] を選択し、FTD デバイスを ISE のネットワーク デバイス インベントリに追加し、RADIUS を設定します。

[RADIUS認証設定 (RADIUS Authentication Settings)] を選択し、FTD RADIUS サーバオブジェクトで設定されているものと同じ [共有秘密 (Shared Secret)] を設定します。必要な場合は、[CoAポート (CoA Port)] 番号を変更し、FTDRADIUS サーバグループオブジェクトで同じポートを設定していることを確認します。

ステップ 2 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [ダウンロード可能ACL (Downloadable ACLs)] を選択します。

ダウンロード可能 ACL (DACL) を 2 つ作成し、1 つは準拠エンドポイント用、もう 1 つは非準拠エンドポイント用とします。

たとえば、準拠エンドポイントではすべてのアクセスを許可し (permit ip any any)、非準拠エンドポイントではすべてのアクセスを拒否できます (deny ip any any)。ユーザに求められる正確なアクセスを準拠状態に基づいて提供するために、これらの DACL は必要なだけ複雑にすることができます。これらの DACL は認可プロファイルで使用します。

ステップ 3 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択し、必要なプロファイルを設定します。

次の状態のプロファイルが必要です。それぞれの最低限の属性を一覧表示します。

- [不明 (Unknown)] : 不明なポスチャプロファイルはデフォルトのポスチャプロファイルです。すべてのエンドポイントは、RA VPN 接続の最初の確立時にこのポリシーに一致します。このルールポイントには、リダイレクト ACL と URL を適用し、ポスチャエージェントがエンドポイント上に存在していない場合は、これをダウンロードすることです。エンドポイントは、エージェントがインストールされていない場合、またはインストールが失敗した場合、このプロファイルが適用されたままとなります。そうでない場合、エンドポイントはポスチャを評価した後に準拠または非準拠プロファイルに移行します。

最低限の属性には、次のものがあります。

- [名前 (Name)] : PRE_POSTURE など。
- [アクセスタイプ (Access Type)] : [ACCESS_ACCEPT] を選択します。
- [共通タスク (Common Tasks)] : [Webリダイレクション (CWA、DRW、MDM、NSP、CPP) (Web Redirection (CWA, DRW, MDM, NSP, CPP))] を選択し、次に [クライアントプロビジョニング (ポスチャ) (Client Provisioning (Posture))] を選択し、FTD デバイスで設定したリダイレクト ACL の名前を入力します。[値 (Value)] では、[クライアントプロビジョニングポータル (Client Provisioning Portal)] を選択します (まだ選択していない場合)。
- [属性の詳細 (Attribute Details)] には、url-redirect-acl および url-redirect の 2 つの cisco-av-pair 値が表示されている必要があります。ISE はこのデータを FTD デバイスに送信します。これにより、RA VPN ユーザセッションに条件が適用されます。
- [準拠 (Compliant)] : ポスチャアセスメントが完了した後、エンドポイントに設定されたすべての要件を満たしている場合、クライアントは準拠と見なされてこのプロファイルを取得します。通常、このクライアントにはフルアクセスを付与します。

最低限の属性には、次のものがあります。

- [名前 (Name)] : FULL_ACCESS など。
- [アクセスタイプ (Access Type)] : [ACCESS_ACCEPT] を選択します。

- [共通タスク (Common Tasks)] : [DACL名 (DACL Name)] を選択し、準拠ユーザ向けに PERMIT_ALL_TRAFFIC などのダウンロード可能 ACL を選択します。ISE は ACL を FTD デバイスに送信します。デバイスは、これをユーザセッションに適用します。この DACL は、ユーザセッションの初期のリダイレクト ACL を置き換えます。
- [非準拠 (Non-compliant)] : ポスチャアセスメントによってエンドポイントがすべての要件を満たしていないことが決定された場合、必要な更新プログラムをインストールするなどにより、クライアントがエンドポイントを準拠させることができるカウントダウンが存在します。AnyConnect クライアントは、準拠の問題をユーザに通知します。カウントダウンの間、エンドポイントは不明な準拠状態になります。カウントダウンの期限が切れた後もエンドポイントが非準拠のままだと、セッションは非準拠とマークされ、非準拠プロファイルを取得します。通常、このエンドポイントではすべてのアクセスを禁止するか、少なくとも何らかの方法でアクセスを制限します。

最低限の属性には、次のものがあります。

- [名前 (Name)] : Non_Compliant など。
- [アクセスタイプ (Access Type)] : [ACCESS_ACCEPT] を選択します。
- [共通タスク (Common Tasks)] : [DACL名 (DACL Name)] を選択し、非準拠ユーザ向けに DENY_ALL_TRAFFIC などのダウンロード可能 ACL を選択します。ISE は ACL を FTD デバイスに送信します。デバイスは、これをユーザセッションに適用します。この DACL は、ユーザセッションの初期のリダイレクト ACL を置き換えます。

ステップ 4 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択し、次のリソースを設定します。

- [AnyConnect パッケージ (AnyConnect package)] : software.cisco.com からダウンロードしたヘッドエンドパッケージファイル。サポートするクライアントプラットフォームごとに個別のパッケージが必要です。そのため、AnyConnectDesktopWindows などの複数のタイプを設定する必要があります。
- [ISE ポスチャ設定ファイル (タイプ : AnyConnectProfile) (ISE Posture Configuration File (Type: AnyConnectProfile))] : この設定ファイルは、コンプライアンス モジュールがエンドユーザのデバイスを評価するために使用する設定を定義します。このファイルはまた、ユーザが非準拠デバイスを準拠させるために使用できる時間の長さを定義します。
- [コンプライアンスモジュールパッケージ (タイプ : ComplianceModule) (Compliance Module Package (Type: ComplianceModule))] : AnyConnect コンプライアンス モジュールファイルは、エンドポイントのコンプライアンスを確認するためにインストールされた AnyConnect パッケージにプッシュされるファイルです。このファイルは、[Cisco サイトからリソースを追加 (Add Resources from Cisco Site)] コマンドを使用してダウンロードします。設定した AnyConnect パッケージに基づいて適切なモジュールをダウンロードしていることを確認します。そうでない場合、ダウンロードに失敗します。これらのファイルは、software.cisco.com 上の ISEComplianceModule フォルダの AnyConnect リストでも確認できます。

- [AnyConnect設定ファイル (タイプ: AnyConnectConfig) (AnyConnect Configuration File (Type: AnyConnectConfig))] : これらの AnyConnect リリース固有設定は、[AnyConnectパッケージ (AnyConnect Package)]、[コンプライアンスモジュール (Compliance Module)]、および適用する [ISEポスチャ (ISE Posture)] を定義します。パッケージは OS 固有であるため、サポートするクライアント OS (Windows、MAC、Linux など) ごとに個別の設定ファイルを作成します。

ステップ 5 [ポリシー (Policy)] > [クライアントプロビジョニング (Client Provisioning)] を選択し、クライアントプロビジョニングポリシーを設定します。

CoA を実装する必要があるオペレーティングシステムごとに、CoA_ClientProvisionWin などの名前を持つ新しいルールを作成します。ルールに適したオペレーティングシステムを選択し、[結果 (Results)] で、OS 用に作成した AnyConnect 設定ファイルを [エージェント (Agent)] として選択します。

置換対象のデフォルトの OS 固有ルールを無効にします。

ステップ 6 ポスチャポリシーを設定します。

この手順では、組織にとって合理的なポスチャ要件を設定します。

- [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] を選択し、満たす必要がある単純なポスチャ条件を定義します。たとえば、ユーザが特定のアプリケーションをインストールしている必要がある場合があります。
- [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [要件 (Requirements)] を選択し、エンドポイントのコンプライアンスモジュール要件を定義します。
- [ポリシー (Policy)] > [ポスチャ (Posture)] > [ポスチャポリシー (Posture Policy)] を選択し、サポートされるオペレーティングシステムのポリシーを設定します。

ステップ 7 [ポリシー (Policy)] > [ポリシーセット (Policy Sets)] > [デフォルト (Default)] > [許可ポリシー (Authorization Policy)] を選択し、ポリシーを作成します。

準拠条件それぞれのルールを追加します。これらの値の例は、前の手順の例に基づいています。

- [不明 (Unknown)] : pre-posture およびポスチャ ダウンロード用。
 - [名前 (Name)] : PRE_POSTURE など
 - [条件 (Conditions)] : "Session-PostureStatus EQUALS Unknown" および "Radius-NAS-Port-Type EQUALS Virtual"
 - [プロファイル (Profiles)] : PRE_POSTURE など
- [準拠 (Compliant)] : ポスチャ要件を満たすクライアント用。
 - [名前 (Name)] : FULL_ACCESS など

- [条件 (Conditions)] : "Session-PostureStatus EQUALS Compliant" および "Radius-NAS-Port-Type EQUALS Virtual"
- [プロファイル (Profiles)] : FULL_ACCESS など
- [非準拠 (Non-compliance)] : ポスチャ要件を満たさないクライアント用。
- [名前 (Name)] : Non_Compliant など。
- [条件 (Conditions)] : "Session-PostureStatus EQUALS NonCompliant" および "Radius-NAS-Port-Type EQUALS Virtual"
- [プロファイル (Profiles)] : Non_Compliant など

ステップ 8 (オプション) [管理 (Administration)] > [設定 (Settings)] > [ポスチャ (Posture)] > [再評価 (Reassessments)] を選択し、ポスチャの再評価を有効にします。

デフォルトでは、ポスチャは接続時にのみ評価されます。ポスチャ再評価を有効にすると、接続されたエンドポイントのポスチャを定期的に確認することができます。再評価間隔を設定して、発生頻度を決定できます。

システムが再評価に失敗する場合、システムがどのように応答するかを定義できます。ユーザの続行を許可する (接続したまま) 、ユーザをログオフさせる、またはユーザにシステムの修復を依頼することができます。

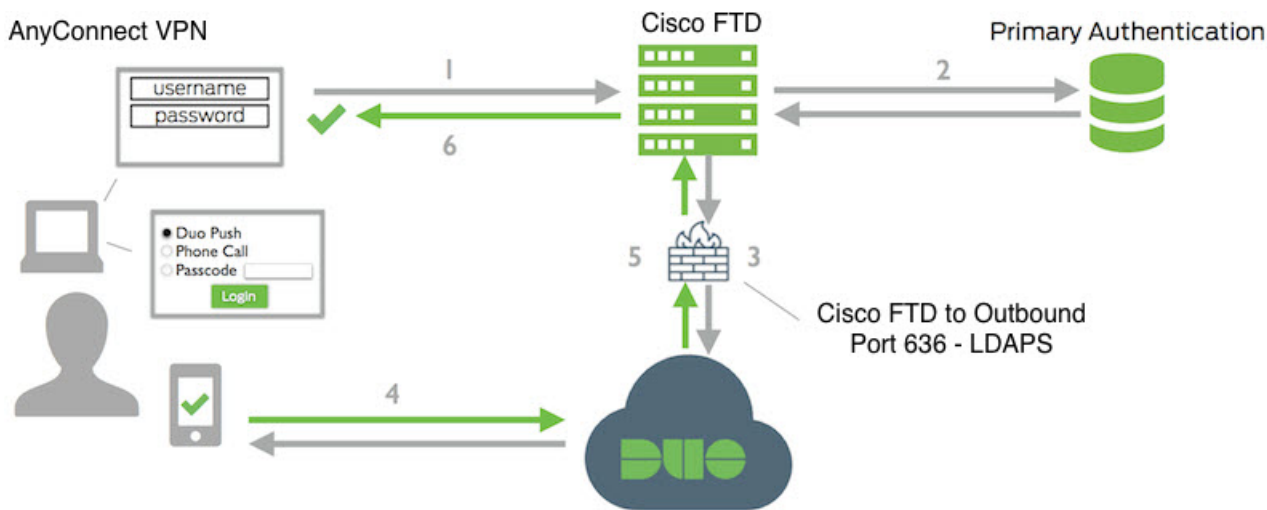
Duo LDAP を使用した二要素認証の設定方法

プライマリ ソースとして Microsoft Active Directory (AD) または RADIUS サーバを使用し、それと組み合わせてセカンダリ認証ソースとして Duo LDAP サーバを使用できます。Duo LDAP を使用すると、セカンダリ認証において、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールによって検証されます。

以降のトピックでは設定についてさらに詳しく説明します。

Duo LDAP セカンダリ認証のシステム フロー

次の図は、LDAP を使用した二要素認証を実現するために、FTD と Duo がどのように連携するかを示しています。



次に、システムフローについて説明します。

1. ユーザは、FTD デバイスへのリモート アクセス VPN 接続を確立し、ユーザ名とパスワードを提供します。
2. FTD は、プライマリ認証サーバを使用して、このプライマリ認証試行を認証します。プライマリ認証サーバは、Active Directory または RADIUS の場合があります。
3. プライマリ認証が成功すると、FTD は、セカンダリ認証の要求を Duo LDAP サーバに送信します。
4. 要求を受けた Duo は、プッシュ通知、パスコード付きのテキストメッセージ、または電話コールによって、ユーザを個別に認証します。ユーザはこの認証を正常に完了する必要があります。
5. Duo は FTD デバイスに応答し、ユーザが正常に認証されたかどうかを示します。
6. セカンダリ認証が成功すると、FTD デバイスは、ユーザの AnyConnect クライアントとのリモート アクセス VPN 接続を確立します。

Duo LDAP セカンダリ認証の設定

次の手順では、リモートアクセス VPN のセカンダリ認証ソースとして、Duo LDAP を使用して二要素認証を設定するエンドツーエンドのプロセスについて説明します。この設定を完了するには、Duo のアカウントが必要であり、また Duo からいくつかの情報を取得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 Duo アカウントを作成し、統合キー、秘密キー、および API ホスト名を取得します。

プロセスの概要を次に示します。詳細については、Duo の Web サイト <https://duo.com> を参照してください。

- a) Duo アカウントへのサインアップを行います。
- b) Duo Admin Panel にログインし、[アプリケーション (Applications)] に移動します。
- c) [アプリケーションの保護 (Protect An Application)] をクリックし、アプリケーションリストで Cisco SSL VPN を探します。[アプリケーションの保護 (Protect An Application)] をクリックし、統合キー、秘密キー、および API ホスト名を取得します。詳細については、Duo の『Getting Started』ガイド <https://duo.com/docs/getting-started> を参照してください。

ステップ 2 Duo LDAP サーバの Duo LDAP アイデンティティ ソースを作成します。

FTD API を使用して Duo LDAP オブジェクトを作成する必要があります。FDM を使用して作成することはできません。API エクスプローラを使用するか、または独自のクライアントアプリケーションを作成して、オブジェクトを作成することができます。次の手順では、API エクスプローラを使用してオブジェクトを作成する方法について説明します。

- a) FDM にログインし、[詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。

ブラウザの設定に応じて、API エクスプローラが別のタブまたはウィンドウで開きます。

- b) (オプション) Duo LDAP サーバへの接続に使用されるインターフェイスを識別するために必要な値を取得します。

インターフェイスを指定しない場合は、ルーティングテーブルが使用されます。必要に応じて、Duo LDAP サーバのスタティック ルートを作成できます。または、Duo LDAP オブジェクトで使用するインターフェイスを指定することもできます。インターフェイスを指定する場合は、Interfaces グループの各種 GET メソッドを使用して、必要な値を取得します。物理インターフェイス、サブインターフェイス、EtherChannel、または VLAN インターフェイスを使用できます。たとえば、物理インターフェイスの値を取得するには、GET /devices/default/interfaces メソッドを使用して、必要なインターフェイスのオブジェクトを検索します。インターフェイス オブジェクトから次の値を取得する必要があります。

- id
- type
- version
- name

- c) [DuoLDAPIdentitySource] 見出しをクリックして、グループを開きます。
- d) [POST /object/duoldapidentitiesources] メソッドをクリックします。
- e) [パラメータ (Parameters)] 見出しの [本文 (body)] 要素について、右側の [データタイプ (Data Type)] 列の [サンプル値表示 (Example Value display)] ボックスをクリックします。この操作により、例が [本文の値 (body value)] 編集ボックスにロードされます。
- f) [本文の値 (body value)] 編集ボックスで、次の手順を実行します。
 - 属性行の version、id を削除します (これらの属性は PUT 呼び出しには必要ですが POST には必要ありません)。
 - **name** で、オブジェクトの名前を入力します (Duo-LDAP-server など)。

- **description** で、後で参照できるようにオブジェクトのわかりやすい説明を入力するか、または属性行を削除します。
- **apiHostname** で、自分の Duo アカウントから取得した API ホスト名を入力します。ホスト名は API-XXXXXXXXX.DUOSEcurity.COM のような形式になります。X の部分を一意の値に置き換えます。大文字は必須ではありません。
- **port** で、LDAPS に使用する TCP ポートを入力します。別のポートを使用するよう Duo から指示された場合を除き、636 にします。アクセスコントロールリストで、必ずこのポートを介した Duo LDAP サーバへのトラフィックを許可してください。
- **timeout** で、Duo サーバに接続するためのタイムアウトを秒単位で入力します。1 ~ 300 秒の値を入力できます。デフォルトは 120 です。デフォルトを使用する場合は、120 を入力するか、または属性行を削除します。
- **integrationKey** で、自分の Duo アカウントから取得した統合キーを入力します。
- **secretKey** で、自分の Duo アカウントから取得した秘密キーを入力します。以降、このキーはマスクされます。
- **interface** で、Duo LDAP サーバへの接続に使用するインターフェイスの id、type、version、および name の値を入力するか、またはインターフェイス属性の定義に使用されている 6 行（末尾の閉じカッコを含む）を削除します。
- **type** では、値を duoldapidentitysource のままにしておきます。

たとえば、オブジェクトの本体は次のようになります。apiHostname と integrationKey は不明瞭にしてありますが、秘密キーは意図的に仮のものを示しています。

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXXX.DUOSEcurity.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

- g) [試してみる (Try It Out!)] ボタンをクリックします。

curl コマンドが発行され、オブジェクトがデバイス設定にポストされます。curl コマンド、応答本文、および応答コードが表示されます。有効な本文を作成した場合は、[応答コード (Response Code)] フィールドに **200** と表示されます。

エラーが発生した場合は、応答本文でエラーメッセージを確認します。本文の値を修正してから、もう一度試してください。

- h) トップメニューで [デバイス (Device)] をクリックして、FDM に戻ります。
- i) [オブジェクト (Objects)] をクリックし、目次の [アイデンティティソース (Identity Sources)] をクリックします。

DuoLDAP オブジェクトがリストに表示されます。表示されない場合は、API エクスプローラに戻ってオブジェクトを作成し直してください。GET メソッドを使用して、実際に作成されたかどうかを確認できます。

FDM を使用して、オブジェクトを削除することはできますが、編集したり、内容を表示したりすることはできません。これらの操作には API を使用する必要があります。関連するメソッドは [DuoLDAPIdentitySource] グループに表示されます。

ステップ 3 FDM に、Duo Web サイト用の信頼できる CA 証明書をアップロードします。

FTD システムには、Duo LDAP サーバへの接続の検証に必要な証明書が必要です。次の手順を使用して、証明書を取得してアップロードできます。下記の手順は Google Chrome ブラウザで実行したものです。具体的な手順はブラウザによって異なる場合があります。または、<https://www.digicert.com/digicert-root-certificates.htm> に直接アクセスして証明書をダウンロードすることもできますが、次の手順は汎用的であり、この手順では任意のサイト用の信頼できるルート CA 証明書を取得できます。

- a) ブラウザで <https://duo.com> を開きます。
- b) ブラウザの URL フィールドでサイト情報リンクをクリックし、[証明書 (Certificate)] リンクをクリックします。この操作により、[証明書の情報 (Certificate information)] ダイアログボックスが開きます。
- c) [証明のパス (Certificate path)] タブをクリックし、パスのルート (最上位) を選択します。この例では DigiCert です。
- d) DigiCert を選択した状態で、[証明書の表示 (View Certificate)] をクリックします。この操作により、新しい [証明書 (Certificate)] ダイアログボックスが開き、[全般 (General)] タブに、DigiCert High Assurance EV Root CA に発行されたことが示されます。このルート CA 証明書を FDM にアップロードする必要があります。
- e) [詳細 (Details)] タブをクリックし、[ファイルにコピー (Copy to File)] ボタンをクリックして、証明書のダウンロード ウィザードを起動します。
- f) ウィザードを使用して、証明書をワークステーションにダウンロードします。デフォルトの DER 形式を使用してダウンロードします。
- g) FDM で、[オブジェクト (Objects)] > [証明書 (Certificates)] を選択します。
- h) [+] > [信頼済みCAの証明書の追加 (Add Trusted CA Certificate)] をクリックします。
- i) 証明書の名前 (たとえば、DigiCert_High_Assurance_EV_Root_CA) を入力します (スペースは使用できません)。
- j) [証明書のアップロード (Upload Certificate)] をクリックし、ダウンロードしたファイルを選択します。

Add Trusted CA Certificate

Name

DigiCert_High_Assurance_EV_Root_CA

Paste certificate, or choose file:

UPLOAD CERTIFICATE

DigiCertHighAssuranceEVRootCA.cer

```
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIQAxqcJmoLQJuPC3nyrkYldzANBgkqhkiG9w0BAQUFADB3
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNoLnQuY29tMSswKQYDVQDEYjEaWdpQ2VydCBlaWdoIEFzc3VyYW5j
ZSBFViBSb290IENBMB4XDTA2MTEwMDAwMDAwMFoXDTEwMDAwMDAwMDAwMFowDEL
MAKGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2lDZXJ0IEluYzEZMBcGA1UECmQd3d3
-----
```

CANCEL

OK

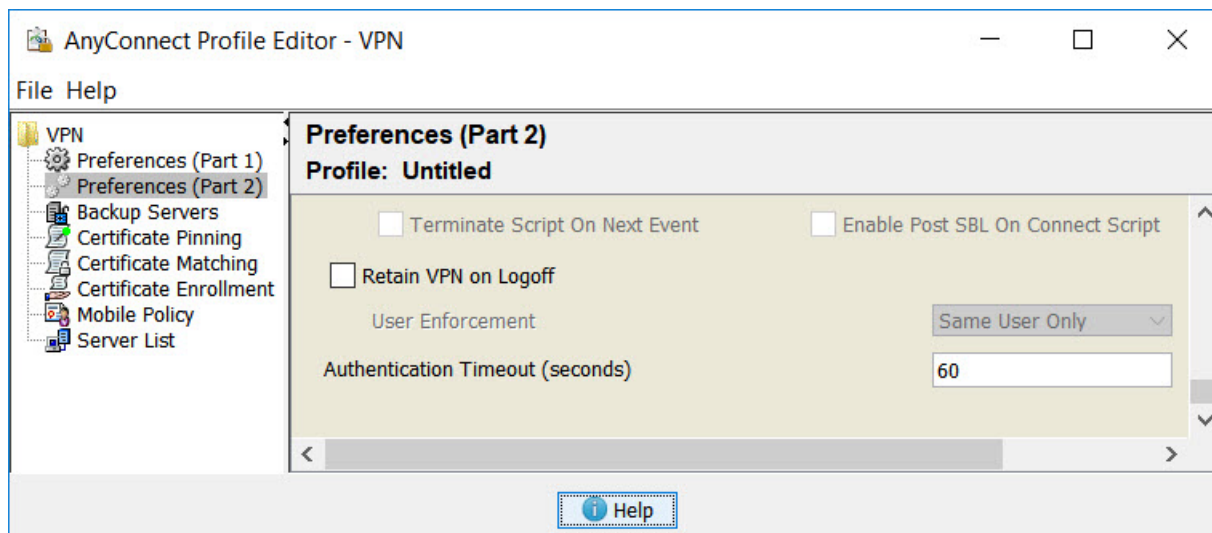
k) [OK] をクリックします。

ステップ 4 AnyConnect プロファイルエディタを使用して、認証タイムアウトに 60 秒以上を指定するプロファイルを作成します。

ユーザに対して、Duo パスコードを取得してセカンダリ認証を完了するまでの時間を別途提供する必要があります。60 秒以上を推奨します。

AnyConnect プロファイルの作成とアップロードの詳細については、[クライアント プロファイルの設定およびアップロード \(615 ページ\)](#) を参照してください。次の手順では、認証タイムアウトのみを設定してから FTD にプロファイルをアップロードする方法について説明します。他の設定を変更する場合は、ここで行うことができます。

- a) AnyConnect プロファイルエディタパッケージをダウンロードしてインストールします（まだ実行していない場合）。このパッケージは、AnyConnect バージョンのフォルダにある Cisco Software Central (software.cisco.com) で見つけることができます。このマニュアルの執筆時点におけるベースパスは、[ダウンロードホーム (Downloads Home)] > [セキュリティ (Security)] > [VPN およびエンドポイントセキュリティクライアント (VPN and Endpoint Security Clients)] > [Cisco VPN クライアント (Cisco VPN Clients)] > [AnyConnect セキュアモビリティクライアント (AnyConnect Secure Mobility Client)] です。
- b) [AnyConnect VPN プロファイルエディタ (AnyConnect VPN Profile Editor)] を開きます。
- c) 目次の [設定 (パート2) (Preferences (Part 2))] を選択し、ページの最後までスクロールして、[認証タイムアウト (Authentication Timeout)] を 60 以上に変更します。次の図は AnyConnect 4.7 VPN プロファイルエディタからの引用です。以前のバージョンとそれ以降のバージョンでは内容が異なる場合があります。



- d) [ファイル (File)] > [保存 (Save)] を選択し、適切な名前 (duo-ldap-profile.xml など) を使用してワークステーションにプロファイル XML ファイルを保存します。
これで、VPN プロファイルエディタ アプリケーションを閉じることができます。
- e) FDM で、[オブジェクト (Objects)] > [AnyConnect クライアントプロファイル (AnyConnect Client Profiles)] を選択します。
- f) [+] をクリックして新しいプロファイル オブジェクトを作成します。
- g) [名前 (Name)] に、オブジェクトの名前を入力します。たとえば、Duo-LDAP-profile と入力します。
- h) [アップロード (Upload)] をクリックし、作成した XML ファイルを選択します。

Add AnyConnect Client Profile

Name

Duo-LDAP-profile

Description

AnyConnect Client Profile

UPLOAD duo-ldap-profile.xml

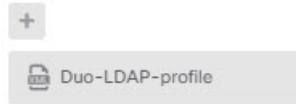
- i) [OK] をクリックします。

ステップ 5 グループ ポリシーを作成し、ポリシーで AnyConnect プロファイルを選択します。

ユーザに割り当てるグループポリシーは、接続のさまざまな側面を制御します。次の手順では、プロファイル XML ファイルをグループに割り当てる方法について説明します。グループポリシーで実行できる操作の詳細については、[RA VPN のグループポリシーの設定 \(628 ページ\)](#) を参照してください。

- a) [デバイス (Device)] > [リモートアクセスVPN (Remote Access VPN)] で [設定の表示 (View Configuration)] をクリックします。
- b) 目次の [グループポリシー (Group Policy)] をクリックします。
- c) DfltGrpPolicy を編集するか、[+] をクリックして新しいグループポリシーを作成します。たとえば、すべてのユーザに対して1つのリモートアクセスVPN 接続プロファイルが必要な場合は、デフォルトのグループポリシーを編集することが適切です。
- d) [一般 (General)] ページで、次のプロパティを設定します。
 - [名前 (Name)] : 新しいプロファイルの場合は、名前を入力します。たとえば、Duo-LDAP-group と入力します。
 - [AnyConnectクライアントプロファイル (AnyConnect Client Profiles)] : [+] をクリックし、作成した AnyConnect クライアントプロファイルを選択します。

AnyConnect client profiles



- e) [OK] をクリックしてグループプロファイルを保存します。

ステップ 6 Duo LDAP セカンダリ認証に使用するリモートアクセスVPN 接続プロファイルを作成または編集します。

接続プロファイルを設定するには数多くの手順があります。詳細については、[RA VPN 接続プロファイルの設定 \(620 ページ\)](#) を参照してください。次の手順では、Duo-LDAP をセカンダリ認証ソースとして有効にし、AnyConnect クライアントプロファイルを適用するための主な変更について説明します。新しい接続プロファイルの場合は、残りの必須フィールドを設定する必要があります。この手順では、既存の接続プロファイルを編集していることを前提としており、これら2つの設定を変更するだけで済みます。

- a) RA VPN ページで、目次の [接続プロファイル (Connection Profile)] を選択します。
- b) 既存のプロファイルを編集するか、新規に作成します。
- c) [プライマリアイデンティティソース (Primary Identity Source)] で、次のように設定します。
 - [認証タイプ (Authentication Type)] : [AAAのみ (AAA Only)] または [AAAとクライアント証明書 (AAA and Client Certificate)] のいずれかを選択します。AAA を使用しない限り、二要素認証を設定することはできません。
 - [ユーザ認証のプライマリアイデンティティソース (Primary Identity Source for User Authentication)] : プライマリ Active Directory または RADIUS サーバを選択します。プライマリソースとして Duo-LDAP アイデンティティソースを選択できます。ただし、Duo-LDAP は認証サービスのみを提供し、アイデンティティサービスは提供しな

いため、プライマリ認証ソースとして Duo-LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザ名は表示されず、これらのユーザに対してアクセス制御ルールを作成することはできません（必要に応じてローカルアイデンティティソースへのフォールバックを設定できます）。

- **[セカンダリアイデンティティソース (Secondary Identity Source)]** : Duo-LDAP のアイデンティティソースを選択します。

Primary Identity Source

Authentication Type

AAA Only
 Client Certificate Only
 AAA and Client Certificate

Primary Identity Source for User Authentication

AD ▼

Fallback Local Identity Source 

Please Select Local Identity Source ▼

Strip Identity Source server from username

Strip Group from Username

Secondary Identity Source

Secondary Identity Source for User Authentication

Duo-LDAP-server ▼

- [次へ (Next)] をクリックします。
- [リモートユーザエクスペリエンス (Remote User Experience)] ページで、作成または編集した [グループポリシー (Group Policy)] を選択します。

Group Policy

Duo-LDAP-group

- このページの [次へ (Next)] をクリックし、次のページの [グローバル設定 (Global Settings)] をクリックします。
- [完了 (Finish)] をクリックして、接続プロファイルへの変更を保存します。

ステップ7 変更を保存します。

- 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。



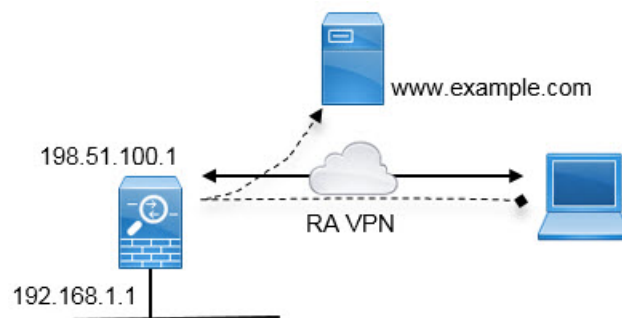
- [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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があります。

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alm 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 接続を設定します。

設定には、接続プロファイルだけでなく、カスタマイズされたグループポリシーが必要です。ヘアピニングは一般的な構成であり、グループポリシーでの必要な設定は全般的に適用できる

ため、この例では新しいグループポリシーを作成するのではなく、デフォルトグループポリシーを編集します。どちらのアプローチも選択できます。

- a) [デバイス (Device)] > [リモートアクセスVPN (Remote Access VPN)] グループで [設定の表示 (View Configuration)] をクリックします。
- b) 目次で [グループポリシー (Group Policies)] をクリックし、DfltGrpPolicy オブジェクトの編集アイコン (🔗) をクリックします。
- c) デフォルトグループポリシーに次の変更を加えます。
 - [全般 (General)] ページの [DNSサーバ (DNS Server)] で、VPN エンドポイントがドメイン名を解決するために使用する必要があるサーバを定義する DNS サーバグループを選択します。

DNS Server

CustomDNSServerGroup

- [スプリットトンネリング (Split Tunneling)] ページの [IPv4] および [IPv6スプリットトンネリング (IPv6 Split Tunneling)] の両方で、[トンネル経由のトラフィックをすべて許可する (Allow all traffic over tunnel)] オプションを選択します。これはデフォルト設定であるため、すでに正しく設定されている可能性があります。

IPv4 Split Tunneling

Allow all traffic over tunnel

IPv6 Split Tunneling

Allow all traffic over tunnel

(注) これはヘアピニングを有効にするための重要な設定です。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。

- d) [OK] をクリックして、デフォルトグループポリシーの変更を保存します。
- e) [接続プロファイル (Connection Profiles)] をクリックし、既存のプロファイルを編集するか、新規作成します。
- f) 接続プロファイルのウィザードを進め、その他の RA VPN 設定の場合と同様に、すべてのオプションを設定します。ただし、ヘアピニングを有効にするには、次のオプションを正しく設定する必要があります。
 - 手順2の [グループポリシー (Group Policy)]。ヘアピニング用にカスタマイズしたグループポリシーを選択します。

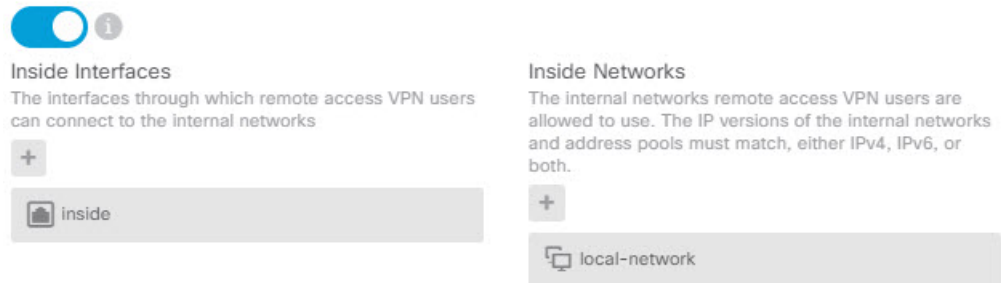
Group Policy

DfltGrpPolicy

- 手順3の [NAT免除 (NAT Exempt)]。この機能をイネーブルにします。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。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

NAT Exempt



(注) [NAT免除 (NAT Exempt)] オプションは、ヘア ピニング設定にとって重要なもう 1 つの設定です。

- g) (オプション) [グローバル設定 (Global Settings)] 手順で、[復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] オプションを選択します。

このオプションを選択すると、RA VPN プールアドレスからのトラフィックを許可するアクセス制御ルールを設定する必要がなくなります。このオプションはセキュリティを向上させますが (外部ユーザがプール内のアドレスをスプーフィングできません)、RA VPN トラフィックが、URL フィルタリングや侵入防御を含むインスペクションから除外されることを意味します。このオプションを決定する前に、長所と短所を考慮してください。

- 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. Key elements are circled in red:

- Title:** OutsideInterfacePAT
- Create Rule for:** Manual NAT
- Placement:** Before Auto NAT Rules
- Type:** Dynamic
- ORIGINAL PACKET:**
 - Source Interface: Any
 - Source Address: Any
- TRANSLATED PACKET:**
 - Destination Interface: outside
 - Source Address: Interface

d) [OK] をクリックします。

ステップ 3 (接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] を設定していない場合) リモートアクセス VPN アドレス プールからのアクセスを許可するアクセス制御ルールを設定します。

接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] を選択した場合、RA VPN プールアドレスからのトラフィックは、アクセス制御ポリシーをバイパスします。このトラフィックに適用されるアクセス制御ルールを作成することはできません。このオプションを無効にする場合にのみ、ルールを作成する必要があります。


次の例では、アドレスプールから任意の宛先へのトラフィックが許可されます。これは独自の要件に合わせて調整できます。不要なトラフィックを除外するブロックルールをルールの前に置くことができます。

a) [ポリシー (Policies)] > [アクセス制御 (Access Control)] をクリックします。

b) [+] をクリックして新しいルールを作成します。

c) 次のプロパティを使用してルールを設定します。

- [順序 (Order)] : ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。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。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。
- [タイトル (Title)] : スペースを含めずにわかりやすい名前を入力します。例、RAVPN-address-pool。
- [アクション (Action)] : [許可 (Allow)]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼 (Trust)] を選択できます。
- [送信元または宛先 (Source/Destination)] ブ : [送信元 (Source)] > [ネットワーク (Network)] で、アドレスプールの RA VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先 (Source and Destination)] の他のすべてのオプションについては、デフォルトの [任意 (Any)] のままにします。

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	 ravpn-pool	ANY	ANY	ANY	ANY

- [アプリケーション (Application)]、[URL]、および [ユーザ (Users)] タブ : これらのタブではデフォルトの設定 (何も選択しない) のままにします。
- [侵入 (Intrusion)]、[ファイル (File)] タブ : オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング (Logging)] タブ : オプションで接続のロギングを有効にできます。

d) [OK] 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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

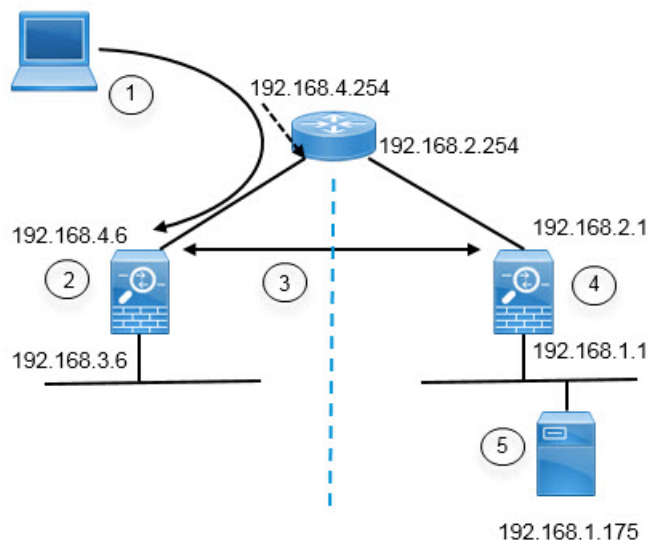
モバイルワーカーと在宅勤務者が内部ネットワークに安全に接続できるリモートアクセス VPN を設定できます。接続のセキュリティは、ユーザ接続を認証して、認可されたユーザだけがエントリを取得できるようにするディレクトリ サーバによって異なります。

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

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。

- 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 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

Local Network

+
Network192.168.1.0

REMOTE SITE

Static Dynamic

Remote IP Address

192.168.4.6

Remote Network

+
SiteAInside
SiteAInterface

- 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。

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-SHA] 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に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 Version 2

IKE Version 1

IKE Policy

Globally applied

IPsec Proposal

Default set selected

Authentication Type

Pre-shared Manual Key Certificate

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 \(589ページ\)](#) 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 \(569ページ\)](#) 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


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。
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	REMOTE SITE
Local VPN Access Interface outside	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Local Network + SiteAInside SiteAInterface	Remote IP Address 192.168.2.1 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 Version 2 <input checked="" type="checkbox"/>	IKE Version 1 <input type="checkbox"/>
IKE Policy Globally applied EDIT...	
IPSec Proposal Default set selected EDIT...	
Authentication Type <input checked="" type="radio"/> Pre-shared Manual Key <input type="radio"/> Certificate	
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 \(589 ページ\)](#) 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

inside

Diffie-Helman Group for Perfect Forward Secrecy

19

- [次へ (Next)] をクリックします。
- サマリーを確認し、[終了 (Finish)] をクリックします。
- 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。



- [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 接続の另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。

- [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。
- [+] > [AD] をクリックします。
- 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 \(182 ページ\)](#) 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。

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

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
192.168.1.175	389
<i>e.g. ad.example.com</i>	
Encryption	Trusted CA certificate
NONE	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 \(612 ページ\)](#) を参照してください。

RA VPN License

Type

PLUS ▾

DISABLE

✔ 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)] > [リモートアクセスVPN (Remote Access VPN)] グループで [設定の表示 (View Configuration)] をクリックします。[接続プロファイル (Connection Profiles)] ページを表示していることを確認します。
- b) 接続プロファイルを作成するか、編集します。
- c) ウィザードの最初のステップでプロファイル名を設定し、その後プライマリ認証ソースとして AD レルムを選択します。必要に応じて、フォールバックアイデンティティソースとしてローカルデータベースを選択できます。

Primary Identity Source

Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

Primary Identity Source for User Authentication

AD

Fallback Local Identity Source ⚠

LocalIdentitySource

- d) アドレスプールを設定します。

この例では、[+] をクリックしてから IPv4 アドレスプールで [新しい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、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。

Client Address Pool Assignment

<p>IPv4 Address Pool Endpoints are provided an address from this pool</p> <p><input type="button" value="+"/></p> <p><input type="button" value="+"/> ra-vpn-pool</p>	<p>IPv6 Address Pool Endpoints are provided an address from this pool</p> <p><input type="button" value="+"/></p>
<p>DHCP Servers</p> <p><input type="button" value="+"/></p>	

- e) [次へ (Next)] をクリックし、適切なグループポリシーを選択します。

選択したポリシーに関する概要情報を確認します。DNSサーバが設定されていることを確認します。設定されていない場合は、ここでポリシーを編集し、DNSを設定します。

- f) [次へ (Next)] をクリックし、[グローバル設定 (Global Settings)] で [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] オプションを選択し、[NAT免除 (NAT Exempt)] オプションを設定します。

[NAT免除 (NAT Exempt)] では、次のオプションを設定する必要があります。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

- [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。

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



SiteAInside

- g) サポートするプラットフォーム向けの AnyConnect パッケージをアップロードします。
h) [次へ (Next)] をクリックし、設定を確認します。

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。

グループによって RA VPN アクセスを制御する方法

リモートアクセス VPN 接続プロファイルを、グループポリシーに基づいて内部リソースへの差分アクセスを提供するように設定することができます。たとえば、従業員に無制限のアクセスを提供し、請負業者には単一の内部ネットワーク以外へのアクセスを提供したくない場合

は、グループポリシーを使用して、適切にアクセスを制限するための異なる ACL を定義できます。

次の例では、192.168.2.0/24 内部サブネットのみのアクセス権を取得する必要がある請負業者向けに、RA VPN 接続を設定する方法を示します。通常の従業員の場合、VPN に対してトラフィックフィルタが定義されていないデフォルトグループポリシーを使用できます。これらのユーザに制限を適用する場合は、デフォルトグループポリシーを編集して、次のように構築された ACL を適用することができます。

始める前に

次の手順では、請負業者に使用するアイデンティティソースがすでに作成されていると仮定します。通常の従業員に使用するソースとは異なるソースであるかもしれません。アイデンティティソースはアクセスの制限に厳密に関連するものではないため、この例からは省略します。

また、この例では、「inside2」インターフェイスが 192.168.2.0/24 サブネットを IP アドレス 192.168.2.1 でホストするように設定されていると想定します（サブネット上のその他のアドレスも許容されます）。

手順

ステップ 1 RA VPN トラフィックを制限するため、拡張アクセスコントロールリスト (ACL) を設定します。

まず、ターゲット 192.168.2.0/24 を定義するネットワークオブジェクトを設定し、次にアクセスリストを定義するスマート CLI オブジェクトを作成する必要があります。ACL の最後には暗黙の「deny」があるため、サブネットへのアクセスを許可することだけが必要となります。サブネット外の IP アドレスへのトラフィックは拒否されます。この例は IPv4 にのみ適用されます。特定のサブネットへの IPv6 アクセスを制限するためのオブジェクトを設定することもできます。ネットワークオブジェクトを作成し、同じ ACL に IPv6 ベースの ACE を追加するだけです。

a) **[オブジェクト (Objects)] > [ネットワーク (Networks)]** を選択し、必要なオブジェクトを作成します。

オブジェクトに ContractNetwork などの名前を付けます。オブジェクトは、次のようになります。

Name

ContractNetwork

Description

Type

Network Host

Network

192.168.2.0/24

e.g. 192.168.2.0/24

- b) [デバイス (Device)] > [詳細設定 (Advanced Configuration)] > [スマートCLI (Smart CLI)] > [オブジェクト (Objects)] を選択します。
- c) [+] をクリックして新しいオブジェクトを作成します。
- d) ACL の名前を入力します。 **ContractACL** などを入力します。
- e) [CLIテンプレート (CLI Template)] には、[拡張アクセスリスト (Extended Access List)] を選択します。
- f) [テンプレート (Template)] の本文で、次を設定します。
 - configure access-list-entry action = permit
 - source-network = any-ipv4
 - destination-network = ContractNetwork object
 - configure permit port = any
 - configure logging = default

ACE は、次のようになります。

Name	Description
ContractACL	

CLI Template

Extended Access List

Template

```

1 access-list ContractACL extended
2 configure access-list-entry permit
3 permit network source [any-ipv4] destination [ContractNetwork]
4 configure permit port any
5 permit port source ANY destination ANY
6 configure logging default
7 default log set log-level INFORMATIONAL log-interval 300
    
```

g) [OK] をクリックします。

この ACL は、次回変更を展開すると設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

ステップ 2 ACL を使用するグループポリシーを作成します。

最低限、グループポリシーの DNS サーバを設定する必要もあります。必要に応じて他のオプションを設定できます。次の手順では、この使用例に関する 1 つの設定について説明します。

- a) [デバイス (Device)] > [RA VPN] > [グループポリシー (Group Policy)] を選択します。
- b) [+] をクリックして新しいグループポリシーを作成します。
- c) [全般 (General)] ページで、ContractGroup などのポリシーの名前を入力します。
- d) 目次の [トラフィックフィルタ (Traffic Filters)] をクリックします。
- e) [アクセスリストフィルタ (Access List Filter)] では、ContractACL オブジェクトを選択します。

この例では、[VLAN] オプションは空白のままにします。別の方法として、フィルタリング用の VLAN を設定し、その VLAN にサブインターフェイスを設定することも可能です。

Access List Filter

ContractACL

Restrict VPN to VLAN

1-4094

f) [OK] をクリックして、グループポリシーを保存します。

ステップ 3 請負業者の接続プロファイルを設定します。

- a) RA VPN ページで、目次の [接続プロファイル (Connection Profile)] をクリックします。
- b) 新しい接続プロファイルを作成するには、[+] をクリックします。
- c) ウィザードの手順 1 を完了し、[次へ (Next)] をクリックします。

「Contractors」などのプロファイルの名前を入力します。

通常の方法で残りのオプションを設定します。これには、請負業者の適切な認証ソースの選択、アドレスプールの定義が含まれます。

- d) 請負業者用に設定されているグループポリシーを選択し、[次へ (Next)] をクリックします。

Group Policy

ContractGroup

- e) [グローバル設定 (Global Settings)] で、[復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] オプションを選択し、[NAT免除 (NAT Exempt)] オプションを設定します。

[NAT免除 (NAT Exempt)] では、次のオプションを設定する必要があります。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

- [内部インターフェイス (Inside Interfaces)] : **inside2** 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)] : **ContractNetwork** 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。

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside2

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



ContractNetwork

- f) サポートするプラットフォーム向けの AnyConnect パッケージをアップロードします。
- g) [次へ (Next)]をクリックし、設定を確認します。

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。

- h) [終了 (Finish)]をクリックします。
-



第 **VI** 部

システム管理

- システム設定 (687 ページ)
- システム管理 (713 ページ)



第 21 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。

- [管理アクセスの設定 \(687 ページ\)](#)
- [システム ロギングの設定 \(690 ページ\)](#)
- [DHCP サーバの設定 \(696 ページ\)](#)
- [DNS の設定 \(698 ページ\)](#)
- [管理インターフェイスの設定 \(703 ページ\)](#)
- [デバイスのホスト名の設定 \(705 ページ\)](#)
- [Network Time Protocol \(NTP\) の設定 \(706 ページ\)](#)
- [URL フィルタリングの設定 \(707 ページ\)](#)
- [クラウドサービスの設定 \(708 ページ\)](#)

管理アクセスの設定

管理アクセスとは、設定およびモニタ目的で FTD デバイスにログインする機能のことです。次の項目を設定できます。

- ユーザアクセス認証に使用するアイデンティティソースを特定するための AAA。ローカルユーザデータベースまたは外部 AAA サーバを使用することができます。管理ユーザの管理の詳細については、[FDM および FTD ユーザアクセスの管理 \(734 ページ\)](#) を参照してください。
- 管理インターフェイスおよびデータ インターフェイスへのアクセス制御。これらのインターフェイスには個別のアクセスリストがあります。どの IP アドレスが HTTPS (Firepower Device Manager で使用) および SSH (CLI で使用) で許可されるかを決定できます。[管理アクセス リストの設定 \(688 ページ\)](#) を参照してください。
- Firepower Device Manager に接続するためにユーザが受け入れる必要がある管理 Web サーバ証明書。Web ブラウザで信頼される証明書をアップロードすることにより、ユーザが不明な証明書を信頼するように求められるのを回避できます。[Firepower Device Manager Web サーバ証明書の設定 \(690 ページ\)](#) を参照してください。

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、[システム設定 (System Settings)] > [管理アクセス (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。


このページで AAA を設定して、外部 AAA サーバで定義されたユーザの管理アクセスを許可することもできます。詳細は、[FDM および FTD ユーザアクセスの管理 \(734 ページ\)](#) を参照してください。

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。

ルールのレストランは、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。

ルールのレストランには、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。

Firepower Device Manager Web サーバ証明書の設定

Web インターフェイスにログインするときに、システムはデジタル証明書を使用して HTTPS で通信を保護します。デフォルトの証明書はブラウザで信頼されていないため、Untrusted Authority という警告が表示され、証明書を信頼するかどうかを確認されます。ユーザは証明書を Trusted Root Certificate ストアに保存することもできますが、その代わりにブラウザが信頼するように設定されている新しい証明書をアップロード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、[システム設定 (System Settings)] > [管理アクセス (Management Access)] 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 [管理アクセス (Management Access)] をクリックします。

ステップ 2 [管理Webサーバ (Management Web Server)] タブをクリックします。

ステップ 3 [Webサーバ証明書 (Web Server Certificate)] で、Firepower Device Manager への HTTPS 接続をセキュリティ保護するために使用する内部証明書を選択します。

証明書をアップロードまたは作成していない場合、リストの下部にある [内部証明書の新規作成 (Create New Internal Certificate)] リンクをクリックして作成します。

デフォルトは、事前に定義された DefaultWebserverCertificate オブジェクトです。

ステップ 4 [保存 (Save)] をクリックします。

変更はすぐに適用され、システムが Web サーバを再起動します。設定を展開する必要はありません。

数分待つて再起動が完了してから、ブラウザを更新します。

システム ロギングの設定

FTD デバイスのシステムロギング (syslog) を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。syslog は、診断ロギング、およびアクセス制御、侵入防御、ファイルとマルウェアのロギングを含む接続関連ロギングのために有効にすることができます。

診断ロギングは、デバイスおよびシステムの状態に関するイベントと、接続とは関係のないネットワーク設定に関する 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。

診断ロギングでは、データプレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバ、NAT などの機能が含まれます。

これらのメッセージの詳細については、『Cisco Firepower Threat Defense Syslog Messages』 (https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_ftpd_syslog_guide.html) を参照してください。

次のトピックでは、さまざまな出力場所に対するの診断メッセージやファイル/マルウェアメッセージのロギングを設定する方法について説明します。

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 14: 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。

リモート syslog サーバのロギングの設定

システムを設定して、syslog のメッセージを外部 syslog サーバに送信できます。これはシステムロギングの最適なオプションです。外部サーバを使用することでメッセージを保持する容量が増え、メッセージの表示、分析、およびアーカイブにサーバの施設を使用できます。

さらに、アクセス制御ルールでトラフィックにファイルポリシーを適用してファイルへのアクセスまたはマルウェア、あるいはその両方を制御する場合、外部 syslog サーバにファイルイベントメッセージを送信するようにシステムを設定できます。syslog サーバを設定しない場合、イベントは FDM イベントビューアのみに表示されます。

次の手順では、診断（データ）ログギングおよびファイル/マルウェアのログギングのために syslog を有効にする方法について説明します。次のイベント用に外部ログギングを設定することもできます。

- 接続イベント：個々のアクセス制御ルール、SSL 復号ルール、またはセキュリティインテリジェンス ポリシー設定で syslog サーバを選択します。
- 侵入イベント：侵入ポリシー設定で syslog サーバを選択します。

始める前に

ファイル/マルウェアイベントの syslog 設定は、脅威ライセンスとマルウェアライセンスを必要とするファイルまたはマルウェアのポリシーを適用する場合にのみ該当します。

さらに、ポリシーを適用するアクセス制御ルールで、**[ファイルイベント (File Events)] > [ファイルのログギング (Log Files)]** オプションが選択されていることを確認する必要があります。そうでない場合、syslog でもイベントビューアでもイベントはまったく生成されません。

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)] > [ログ設定 (Logging Settings)]** 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 **[ログギングの設定 (Logging Settings)]** をクリックします。

ステップ 2 [リモートサーバ (Remote Server)] の下の **[データログギング (Data Logging)]** スライダを「オン」にして、データプレーンで生成された診断メッセージの外部 syslog サーバへのログギングを有効にします。次に、以下のオプションを設定します。

- [Syslogサーバ (Syslog Server)] : [+] をクリックし、1 つまたは複数の syslog サーバ オブジェクトを選択して、[OK] をクリックします。オブジェクトが存在しない場合は、**[Syslog サーバの追加 (Add Syslog Server)]** リンクをクリックして作成します。詳細については、[Syslog サーバの設定 \(166 ページ\)](#) を参照してください。
- [FXOSシャーシsyslogのフィルタリングの重大度レベル (Severity Level for Filtering FXOS Chassis Syslogs)] : FXOS を使用する特定のデバイス モデルの、基本の FXOS プラットフォームによって生成される syslog メッセージの重大度レベル。このオプションは、デバイスに該当する場合にのみ表示されます。重大度を選択します。このレベル以上のメッセージが syslog サーバに送信されます。
- [Firepower Threat Defenseのメッセージフィルタリング (Message Filtering for Firepower Threat Defense)] : Firepower Threat Defense のオペレーティングシステム用に生成されたメッセージを制御するには、次のオプションのいずれかを選択します。

- [すべてのイベントのフィルタリングの重大度レベル (Severity Level for Filtering All Events)]: 重大度レベルを選択します。このレベル以上のメッセージが syslog サーバに送信されます。
- [カスタムロギングフィルタ (Custom Logging Filter)]: 関心のあるメッセージのみを取得するために追加のメッセージフィルタリングを行う場合、生成させたいメッセージを定義するイベントリストフィルタを選択します。フィルタが存在しない場合は、[新しいイベントリストフィルタの作成 (Create New Event List Filter)]をクリックして作成します。詳細については、[イベントリストフィルタの設定 \(695 ページ\)](#) を参照してください。

ステップ 3 ファイルおよびマルウェアのイベントの外部 syslog サーバへのロギングを有効にするには、[ファイル/マルウェア (File/Malware)] スライダを「オン」にします。次に、ファイル/マルウェアロギングのオプションを設定します。

- [Syslogサーバ (Syslog Server)]: syslog サーバオブジェクトを選択します。オブジェクトが存在しない場合は、[Syslogサーバの追加 (Add Syslog Server)] リンクをクリックして作成します。
- [重大度レベルのログ (Log at Severity Level)]: ファイル/マルウェア イベントに割り当てる重大度レベルを選択します。すべてのファイル/マルウェア イベントが同じ重大度で生成されるため、フィルタリングは実行されません。選択したレベルに関係なく、すべてのイベントが表示されます。これがメッセージの重大度フィールドに表示されるレベルになります (つまり、FTD-x-<message_ID> の x)。ファイルイベントはメッセージ ID 430004 であり、マルウェアイベントは 430005 です。

ステップ 4 [保存 (Save)] をクリックします。

内部バッファへのロギングの設定

システムを設定して、内部ロギングバッファに syslog メッセージを保存できます。このバッファの内容を表示するには、CLI または CLI コンソールで **show logging** コマンドを使用します。

新しいメッセージは、バッファの最後に追加されます。バッファの空きがなくなると、システムはバッファをクリアしてから、メッセージの追加を続行します。ログバッファに空きがなくなると、システムは最も古いメッセージを削除して、バッファに新しいメッセージ用の領域を確保します。

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)] > [ログ設定 (Logging Settings)] 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 [ロギングの設定 (Logging Settings)] をクリックします。

ステップ 2 ロギングの宛先としてバッファを有効にするには、[内部バッファ (Internal Buffer)] スライダを「オン」にします。

ステップ 3 内部バッファロギングのオプションの設定。

- [すべてのイベントのフィルタリングの重大度レベル (Severity Level for Filtering All Events)] : 重大度レベルを選択します。このレベル以上のメッセージが内部バッファに送信されます。
- [カスタムロギングフィルタ (Custom Logging Filter)] : (オプション) 関心のあるメッセージのみを取得するために追加のメッセージフィルタリングを行う場合、生成するメッセージを定義するイベントリストフィルタを選択します。フィルタが存在しない場合は、[新しいイベントリストフィルタの作成 (Create New Event List Filter)] をクリックして作成します。詳細については、[イベントリストフィルタの設定 \(695 ページ\)](#) を参照してください。
- [バッファサイズ (Buffer Size)] : syslog メッセージを保存する内部ログ バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。指定できる範囲は 4096 ~ 52428800 です。

ステップ 4 [保存 (Save)] をクリックします。

コンソールへのロギングの設定

コンソールにメッセージを送信するようにシステムを設定することができます。コンソールポートの CLI にログインしたときにこれらのメッセージが表示されます。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。

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)] > [ログ設定 (Logging Settings)] 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 [ロギングの設定 (Logging Settings)] をクリックします。

ステップ 2 ロギングの宛先としてコンソールを有効にするには、[コンソールフィルタ (Console Filter)] スライダを「オン」にします。

ステップ 3 [重大度 (Severity)] レベルを選択します。このレベル以上のメッセージがコンソールに送信されます。

ステップ4 [保存 (Save)]をクリックします。

イベントリスト フィルタの設定

イベントリスト フィルタの設定は、宛先に送信されるメッセージを制御するためにロギング宛先に適用するカスタムフィルタです。通常、重大度のみに基づいて接続先へのメッセージをフィルタリングしますが、フィルタを使用して、イベントクラス、重大度、およびメッセージ識別子 (ID) の組み合わせに基づいて送信されるメッセージを微調整できます。

重大度レベル単独でメッセージを制限するだけでは目的を満たすのに不十分である場合は、フィルタを使用します。

次の手順では、[オブジェクト (Objects)]ページでフィルタを設定する方法について説明します。フィルタを使用できるロギング宛先の設定時にフィルタ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[イベントリストフィルタ (Event List 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 フィルタ プロパティを設定します。

- [名前 (Name)]: フィルタ オブジェクトの名前。
- [説明 (Description)]: (オプション) オブジェクトの説明。
- [重大度とログクラス (Severity and Log Class)]: メッセージクラスでフィルタリングする場合は、[+] をクリックしてクラスフィルタの重大度レベルを選択し、[OK] をクリックします。次に、重大度レベル内のドロップダウン矢印をクリックし、その重大度レベルでフィルタリングする1つまたは複数のクラスを選択し、[OK] をクリックします。

システムは、指定されたクラスのメッセージがその重大度レベル以上の場合のみ、syslog メッセージを送信します。重大度レベルごとに最大で1行を追加することができます。

特定の重大度レベルですべてのクラスをフィルタリングする場合は、重大度リストを空のままにし、その代わりに、ロギング宛先を有効にするときにそのロギング宛先のグローバル重大度レベルを選択します。

- [Syslog範囲/メッセージID (Syslog Range/Message ID)]: syslog メッセージ ID でフィルタリングする場合は、単独のメッセージ ID、またはメッセージを生成する ID 番号の範囲を

入力します。範囲の開始番号と終了番号は、100000-200000 のようにハイフンで区切ります。ID は 6 桁の数字です。特定のメッセージ ID および関連するメッセージについては、『Cisco Firepower Threat Defense Syslog Messages』 (https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html) を参照してください。

ステップ 4 [保存 (Save)] をクリックします。

それを許可するロギング宛先のカスタム フィルタリング オプションで、このオブジェクトを選択できるようになりました。[デバイス (Device)] > [システム設定 (System Settings)] > [ロギング設定 (Logging Settings)] に移動します。

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 デバイスでプールあたり 256 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。初期システムセットアップ時に DNS サーバを設定します。それにより、これらのサーバがデータインターフェイスと管理インターフェイスに適用されます。セットアップ後に変更することが可能です。また、データインターフェイスと管理インターフェイスに個別のサーバセットを使用できます。

少なくとも、管理インターフェイスの DNS を設定する必要があります。FQDN ベースのアクセス制御ルールを使用する場合や、**ping** などの CLI コマンドでホスト名を使用する場合は、データインターフェイスの DNS も設定する必要があります。

DNS の設定は、DNS グループを設定し、インターフェイスで DNS を設定するという 2 手順のプロセスです。

ここでは、このプロセスについて詳しく説明します。

DNS グループの設定

DNS グループは、DNS サーバおよび関連付けられているいくつかの属性のリストを定義します。管理インターフェイスとデータインターフェイスで別々に DNS を設定できます。

www.example.com などの完全修飾ドメイン名 (FQDN) を IP アドレスに解決するには、DNS サーバが必要です。



デバイスセットアップウィザードが完了した後、次のシステム定義 DNS グループの一方または両方を使用できます。


- **CiscoUmbrellaDNSServerGroup** : このグループには、Cisco Umbrella と使用できる DNS サーバの IP アドレスが含まれています。初期セットアップ時にこれらのサーバを選択した場合、これが唯一のシステム定義グループになります。このグループの名前またはサーバリストを変更することはできませんが、他のプロパティは編集できます。
- **CustomDNSServerGroup** : デバイスセットアップ時に Umbrella サーバを選択していない場合、システムはサーバリストを使用してこのグループを作成します。このグループのすべてのプロパティを編集できます。

手順


ステップ 1 [オブジェクト (Objects)] を選択して、目次から [DNSグループ (DNS Groups)] を選択します。

ステップ 2 次のいずれかを実行します。

- 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。
- グループを編集するには、そのグループの [編集 (edit)] 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 次のプロパティを設定します。

- [名前 (Name)] : DNS サーバグループの名前。DefaultDNS という名前は予約済みで使用できません。
- [DNS IPアドレス (DNS IP Addresses)] : DNS サーバの IP アドレスを入力します。複数のサーバを設定するには、[別のDNS IPアドレスを追加 (Add Another DNS IP Address)] をクリックします。サーバアドレスを削除する場合は、アドレスの [削除 (delete)] アイコン  をクリックします。

リストは優先順です。リストの最初のサーバが常に使用されます。後続のサーバは、上位のサーバから応答が受信されない場合のみ使用されます。最大6台のサーバを設定できます。ただし、6台のサーバはデータインターフェイスでのみサポートされます。管理インターフェイスでは、最初の3台のサーバのみが使用されます。

- [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。名前は、データ インターフェイスのグループを使用するために 63 文字以下にする必要があります。

- [再試行 (Retries)]: システムが応答を受信しない場合に DNS サーバのリストを再試行する回数 (0 ~ 10 の範囲)。デフォルトは 2 です。この設定は、データ インターフェイスのみで使用される DNS グループに適用されます。
- [タイムアウト (Timeout)]: 次の DNS サーバを試行する前に待機する秒数 (1 ~ 30)。デフォルトは 2 秒です。システムがサーバのリストを再試行するたびに、このタイムアウトは 2 倍になります。この設定は、データ インターフェイスのみで使用される DNS グループに適用されます。

ステップ 4 [OK] をクリックします。

データと管理インターフェイスの 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。まず、データおよび管理 DNS 設定は、デバイスセットアップウィザードで設定した DNS サーバに基づいています。次の手順を使用して、デフォルトを変更できます。

configure network dns servers および **configure network dns searchdomains** コマンドを使用して、CLI で管理 DNS の設定を変更することもできます。データ インターフェイスおよび管理インターフェイスが同じ DNS グループを使用していて、そのグループが更新され次の展開段階にある場合、データ インターフェイスにも変更が適用されます。

DNS 解決に関する問題が発生した場合は、次を参照してください。

- [DNS の一般的な問題のトラブルシューティング \(702 ページ\)](#)
- [管理インターフェイスの DNS のトラブルシューティング \(749 ページ\)](#)

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 [DNSサーバ (DNS Server)] をクリックします。

ステップ 2 データ インターフェイスの DNS を設定します。

- a) (オプション) [+] をクリックし、DNS ルックアップを実行するときに使用する [インターフェイス (Interfaces)] を選択します。

デフォルトおよび推奨される値は [任意 (Any)] であるため、ルックアップを任意のインターフェイス (ルーティング テーブルに基づいた) で実行できます。これらのインターフェイスを介して DNS サーバにアクセスする必要があることがわかっている場合にのみ、

特定のインターフェイスを選択します。診断インターフェイスの IP アドレスを設定している場合にのみ、診断インターフェイスを選択します。サーバにトラフィックを転送するには既存のルートが不十分である場合、DNS サーバのスタティック ルートを設定する必要があります。

- b) データ インターフェイスで使用するサーバを定義する [DNS グループ (DNS Group)] を選択します。グループが存在していない場合は、[DNS グループの新規作成 (Create New DNS Group)] をクリックし、すぐに作成します。データ インターフェイスでルックアップしないようにするには、[なし (None)] を選択します。
- c) (オプション) アクセス制御ルールで FQDN ネットワーク オブジェクトを使用する場合は、[FQDN DNS 設定 (FQDN DNS Settings)] を設定します。

これらのオプションは、FQDN オブジェクトのみを解決する場合に使用されます。その他のタイプの DNS 解決では無視されます。

- [ポーリング時間 (Poll Time)] : FQDN ネットワーク オブジェクトを IP アドレスに解決するために使用するポーリング サイクルの時間 (分単位)。FQDN オブジェクトは、アクセス コントロール ポリシーで使用されている場合にのみ解決されます。タイマーによって、解決間隔の最大時間が決定されます。また、DNS エントリの存続可能時間 (TTL) の値を使用しても、IP アドレス解決を更新するタイミングを決定できます。したがって、個々の FQDN がポーリング サイクルよりも頻繁に解決される可能性があります。デフォルトは 240 (4 時間) です。指定できる範囲は 1 ~ 65535 分です。
 - [有効期限 (Expiry)] : DNS エントリの期限が切れる (DNS サーバから取得した TTL が経過する) 分数。この分数が経過すると、エントリは DNS ルックアップ テーブルから削除されます。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNS エントリによっては TTL が極端に短い (3 秒程度) 場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です (つまり、TTL が経過してから 1 分後にエントリが削除されます)。指定できる範囲は 1 ~ 65535 分です。
- d) [保存 (Save)] をクリックします。設定を展開して、デバイスに変更を適用する必要もあります。

ステップ 3 管理インターフェイスの DNS を設定します。

- a) 管理インターフェイスで使用するサーバを定義する [DNS グループ (DNS Group)] を選択します。グループが存在していない場合は、[DNS グループの新規作成 (Create New DNS Group)] をクリックし、すぐに作成します。
- b) [保存 (Save)] をクリックします。変更はすぐにデバイスに適用されます。この変更を適用するために展開ジョブは実行しません。

DNS の一般的な問題のトラブルシューティング

管理インターフェイスおよびデータ インターフェイスに個別に DNS サーバを設定する必要があります。一部の機能では、両方ではなくどちらか片方のタイプのインターフェイスで名前解決を行います。所定の機能では、用途に応じて異なる解決方法を使用することもあります。

たとえば、**ping hostname** コマンドと **ping interface interface_name hostname** コマンドはデータ インターフェイス DNS サーバを使用して名前解決を行い、**ping system hostname** コマンドは管理インターフェイス DNS サーバを使用します。これにより、特定のインターフェイスおよびルーティング テーブルを介した接続をテストできます。

ホスト名ルックアップに関する問題をトラブルシューティングする場合は、このことに留意してください。

管理インターフェイスの DNS をトラブルシューティングする場合は、[管理インターフェイスの DNS のトラブルシューティング \(749 ページ\)](#) も参照してください。

名前解決しない場合

単純に名前解決が実行されない場合のトラブルシューティングに関するヒントは、次のとおりです。

- 管理インターフェイスとデータ インターフェイスの両方に DNS サーバを設定していることを確認します。データ インターフェイスでは、インターフェイスに [任意 (Any)] を使用します。これらのインターフェイス経由で DNS サーバにアクセスする必要がある場合にのみ、インターフェイスを明示的に指定します。
- データ インターフェイスでのルックアップに診断インターフェイスを使用している場合、そのインターフェイスで IP アドレスを設定していることを確認します。ルックアップでは、インターフェイスに IP アドレスがある必要があります。
- 各 DNS サーバの IP アドレスに ping を実行して、到達可能であることを確認します。system および interface キーワードを使用して、特定のインターフェイスをテストします。ping が失敗した場合は、スタティックルートとゲートウェイを確認します。サーバのスタティックルートを追加する必要がある場合があります。
- ping が成功して名前解決が失敗する場合は、アクセス制御ルールを確認します。サーバから到達可能なインターフェイスの DNS トラフィック (UDP/53) を許可していることを確認します。このトラフィックは、システムと DNS サーバの間にあるデバイスによってブロックされる可能性もあるため、別の DNS サーバを使用する必要がある場合があります。
- ping が機能する場合は適切なルートが存在し、アクセス制御ルールに問題はありません。DNS サーバに FQDN のマッピングが存在しない可能性を考えます。別のサーバを使用する必要がある場合があります。

名前解決が正しくない場合

名前解決は実行されるが名前の IP アドレスが最新のものではない場合、キャッシュに問題がある可能性があります。この問題は、アクセス制御ルールで使用される FQDN ネットワークオブジェクトなどのデータ インターフェイス ベースの機能にのみ影響します。

システムには、以前のルックアップで取得した DNS 情報のローカルキャッシュが存在します。新しいルックアップが要求されると、システムは最初にローカルキャッシュを調べます。ローカルキャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカルキャッシュで要求を解決できない場合、DNS サーバに DNS クエリが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカルキャッシュに格納されます。

各ルックアップには DNS サーバによって定義される存続可能時間値が設定されており、キャッシュからのルックアップは自動的に期限切れになります。また、システムはアクセス制御ルールで使用される FQDN の値を定期的に更新します。この更新は、少なくともポーリング間隔（デフォルトでは4時間ごと）で実行されますが、エントリの存続可能時間値に基づいて、より頻繁に実行できます。

show dns-hosts コマンドおよび **show dns** コマンドを使用して、ローカルキャッシュを確認します。FQDN の IP アドレスが正しくない場合は、**dns update[host hostname]** コマンドを使用して情報を強制的に更新できます。ホストを指定せずにコマンドを使用すると、すべてのホスト名が更新されます。

clear dns[host fqdn] コマンドおよび **clear dns-hosts cache** コマンドを使用して、キャッシュ情報を削除できます。

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ます、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。

ホスト名の変更は、いくつかのシステムプロセスにすぐに適用されます。ただし、すべてのシステムプロセスで同じ名前が使用されるため、更新を完了するには変更を展開する必要があります。

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 \(747 ページ\)](#) を参照してください。



(注) Firepower 4100/9300 では、FDM から NTP を設定しません。FXOS で NTP を設定します。

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)] > [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) (Cisco Talos Intelligence Group (Talos)) 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。
- [URL 存続可能時間 (URL Time to Live)] ([未知の URL 用 Cisco CSI のクエリ (Query Cisco CSI for Unknown URLs)] を選択している場合にのみ利用可能) : 指定された URL のカテゴリおよびレピュテーションルックアップ値を保持する時間。存続可能時間が経過すると、次に試行される URL のアクセスが新規のカテゴリ/レピュテーションルックアップになります。時間が短いほど URL フィルタリングが正確になり、時間が長いほど未知の URL に対するパフォーマンスが向上します。TTL は 2、4、8、12、24、または 48 時間、1 週間、または [使用しない (Never)] (デフォルト) に設定できます。

ステップ 3 必要に応じて、URL のカテゴリを確認できます。

特定の URL のカテゴリとレピュテーションをチェックすることができます。[確認する URL (URL to Check)] ボックスに URL を入力し、[移動 (Go)] をクリックします。結果を表示す

るには、外部の Web サイトに移動します。分類に同意しない場合は、[URLカテゴリの異議を送信する (Submit a URL Category Dispute)] リンクをクリックして弊社までお知らせください。

ステップ 4 [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。

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。シスコクラウドサービスのアカウントからキーを取得することもできます。

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 [スマートライセンシング (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。



- (注) 高可用性を設定する予定の場合、高可用性グループで使用する両方のデバイスを登録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、[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、クラウドサービス リージョンを選択し、[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 \(107 ページ\)](#) 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。クラウドから完全に切断する方法については、[シスコクラウドサービスの登録の無効化 \(710 ページ\)](#) を参照してください。

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。



- (注) 高可用性グループのアクティブ装置で Cisco Success Network を有効にする場合、スタンバイ装置での接続も有効にします。

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。

シスコクラウドサービスの登録の無効化

デバイスを Cisco Defense Orchestrator に登録するか、Cisco Success Network を有効にするか、Cisco Cloud にイベントを送信するか、または Cisco Smart Software Manager にデバイスを登録すると、デバイスがシスコクラウドサービスに登録されます。すべてのクラウドサービスを無効にしても、デバイスは登録されたままになります。

接続を有効にすると、デバイスがシスコクラウドサービスへのセキュアな接続を確立し、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なります。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。

場合によっては、別のスマート ライセンシング アカウントで登録できるように、またはサービスからデバイスを削除するために、デバイスのシスコクラウドサービスへの登録を削除する必要があります。

手順

-
- ステップ 1** [デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページで、すべてのクラウドサービスを無効にします。
- ステップ 2** [デバイス (Device)] > [スマートライセンス (Smart License)] を選択し、歯車ドロップダウンリストから [デバイスの登録解除 (Unregister Device)] を選択します。
- ステップ 3** デバイスをクラウドに再登録する場合は、次のいずれかを実行します。
- シスコ セキュリティ アカウントを使用する場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] を選択し、トークンを使用して Cisco Defense Orchestrator に再登録します。その後、[デバイス (Device)] > [スマートライセンス (Smart License)] に移動し、デバイスを再登録することができます。
 - スマート ライセンス アカウントを使用する場合は、[デバイス (Device)] > [スマートライセンス (Smart License)] ページでデバイスを登録します。これで、[クラウドサービス (Cloud Services)] ページに戻り、必要なサービスを再度有効にすることができます。
-

Web 分析の有効化と無効化

Web 分析を有効にすると、ページのヒット数に基づいて匿名の製品使用情報をシスコに提供できます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブ データは送信されません。

Web 分析はデフォルトで有効になっています。

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 [Web 分析 (Web Analytics)] 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。
-

Cisco Cloud へのイベントの送信

Cisco Cloud サーバにイベントを送信できます。このサーバから、各種のシスコクラウドサービスがイベントにアクセスできます。イベント送信後に、Cisco Threat Response などのクラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。このサービスを有効にすると、このデバイスから、接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントが Cisco Cloud に送信されます。

始める前に

このサービスを有効にするには、事前に Cisco Smart Software Manager にデバイスを登録する必要があります。

<https://visibility.amp.cisco.com/> 米国地域では https://visibility.eu.amp.cisco.com で、EU 地域では、Cisco Threat Response に接続できます。アプリケーションの使い方と利点についての動画は、YouTube でご視聴いただけます (<http://cs.co/CTRvideos>)。FTD での Cisco Threat Response の使い方の詳細については、『*Firepower And CTR Integration Guide*』を参照してください (<https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>)。

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 Cloud にイベントを送信 (Send Events to the Cisco Cloud)] オプションの [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。



第 22 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 \(713 ページ\)](#)
- [システムのバックアップと復元 \(720 ページ\)](#)
- [監査と変更管理 \(726 ページ\)](#)
- [デバイス設定のエクスポート \(733 ページ\)](#)
- [FDM および FTD ユーザ アクセスの管理 \(734 ページ\)](#)
- [システムの再起動またはシャットダウン \(741 ページ\)](#)
- [システムのトラブルシューティング \(742 ページ\)](#)
- [一般的でない管理タスク \(755 ページ\)](#)

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。ルールの更新では、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ルリング 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。

ハイ アベイラビリティ グループ内の 1 台の装置のフィードを手動で更新する場合は、その他の装置のフィードも手動で更新して一貫性を確保する必要があります。

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。

高可用性グループ内の装置をアップグレードする場合は、スタンバイデバイスをアップグレードし、モードを切り替えてアクティブ/スタンバイ装置を交換して、新しいスタンバイデバイスにアップグレードをインストールします。詳細については、[HA デバイスでのソフトウェアアップグレードのインストール \(251 ページ\)](#) を参照してください。

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のすべてのタスクが完了するまでお待ちください。また、スケジュールされたタスクがないかどうかを確認します。アップグレードタスクに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、アプリケーションフィルタ、アクセスルール、またはSSL復号ルールに非推奨のアプリケーションが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、以前に有効になっていたアプリケーションが廃止される可能性があります。この場合、アップグレードは失敗し、デバイスは使用不能状態のままになります。

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 Compatibility Guide』 (<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せんが、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** (ISA 3000 のみ) [バックアップファイルの場所 (Location of Backup Files)] を選択します。
- [ローカルハードディスク (Local Hard Disk)] または [SDカード (SD Card)] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。
- ステップ 5** [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** (ISA 3000 のみ) [バックアップファイルの場所 (Location of Backup Files)] を選択します。
- [ローカルハードディスク (Local Hard Disk)] または [SDカード (SD Card)] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。
- ステップ 6** [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 (ISA 3000 のみ) [バックアップファイルの場所 (Location of Backup Files)] を選択します。

[ローカルハードディスク (Local Hard Disk)] または [SD カード (SD Card)] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。

ステップ 6 [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。

ただし、このデバイスがハイアベイラビリティペアの一部である場合、バックアップは復元できません。まず、**[デバイス (Device)] > [ハイアベイラビリティ (High Availability)]** ページから HA を無効化することで、バックアップを復元できます。バックアップに HA の設定が含まれている場合、デバイスは HA グループに再度参加します。両方のユニットで同じバックアップを復元しないでください (両方のユニットがアクティブになってしまうため)。代わりに、まず、アクティブにする装置でバックアップを復元し、その後、別のユニットで同等のバックアップを復元してください。

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 (715 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。

ステップ 4 必要に応じて、[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、デバイスを再登録し、必要なオプションライセンスを再度有効にします。

元のデバイスと同じデバイスにバックアップを復元する場合、ライセンスの状態はバックアップ時に存在していたものに戻ります。ライセンスの有効化または無効化など、その後に変更を加えた場合は、これらの変更をやり直す必要があります。

デバイスを交換するなどの理由で別のデバイスでバックアップを復元する場合、新しいデバイスは未登録です。デバイスを再登録し、必要なオプションライセンスを有効にする必要があります。復元に HA の設定が含まれている場合、デバイスは HA グループへの参加を試みません。最初にデバイスを登録し、設定を手動で展開する必要があります。

ISA 3000 デバイスの交換

ISA 3000 の SD カードは、別の ISA 3000 デバイスとの間でやり取りできます。SD カード上にシステムバックアップを作成すれば、この機能を使用してデバイスを簡単に交換できます。その方法は、障害が発生したデバイスから SD カードを取り出して新しいデバイスに挿入するだけです。その後に、バックアップを使用して復元できます。

必要なバックアップを確実に用意するには、SD カードにバックアップを作成するバックアップジョブを設定します。

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。

監査と変更管理

システムイベントやユーザが実行したアクションに関するステータス情報を表示できます。この情報は、システムを監査し、システムが適切に管理されていることを確認するために役立ちます。

監査ログを表示するには、[デバイス (Device)] > [デバイス管理 (Device Administration)] > [監査ログ (Audit Log)] をクリックします。さらに、右上隅にある [タスクリスト (Task List)] アイコン ボタンまたは [展開 (Deployment)] アイコン ボタンをクリックすると、システム管理情報を確認できます。

ここでは、システム監査および変更管理のいくつかの主要な概念とタスクについて説明します。

監査イベント

監査ログには、次のタイプのイベントを含めることができます。

[カスタムフィードの更新イベント (Custom Feed Update Event)]、[カスタムフィードの更新に失敗 (Custom Feed Update Failed)]

これらのイベントは、カスタムのセキュリティ インテリジェンス フィードの更新が正常に完了したか失敗したことを示します。詳細には、更新を開始したユーザと、更新されたフィードに関する情報が含まれます。

Deployment Completed (展開完了)、Deployment Failed (展開失敗) : ジョブ名またはエンティティ名

これらのイベントは、正常に完了した展開ジョブまたは失敗した展開ジョブを示します。詳細には、ジョブを開始したユーザと、そのジョブエンティティに関する情報が含まれます。失敗したジョブには、その失敗に関連するエラーメッセージが含まれます。

詳細には[差異ビュー (Differences View)]タブもあります。このタブには、ジョブでデバイスに展開された変更が表示されます。これは、展開されたエンティティのすべてのエンティティ変更イベントの組み合わせです。

これらのイベントをフィルタリングするには、事前定義フィルタの[展開履歴 (Deployment History)]をクリックします。これらのイベントのイベントタイプはDeployment Event (展開イベント) であり、完了したイベントまたは失敗したイベントのみをフィルタリングすることはできないことに注意してください。

イベント名には、ユーザ定義のジョブ名 (定義している場合) または「User (*username*) Triggered Deployment (ユーザ (ユーザ名) トリガー イベント)」が含まれます。また、デバイスセットアップウィザードの実行時に発生する「Device Setup Automatic Deployment (デバイスセットアップ自動展開)」ジョブと「Device Setup Automatic Deployment (Final Step) (デバイスセットアップ自動展開 (最終手順))」ジョブもあります。

Entity Created (エンティティ作成)、Entity Updated (エンティティ更新)、Entity Deleted (エンティティ削除) : エンティティ名 (エンティティ型)

これらのイベントは、識別されたエンティティまたはオブジェクトに変更が加えられたことを示します。エンティティの詳細には、エンティティ名、タイプ、およびIDに加えて、変更を加えたユーザが含まれます。これらの項目に関してフィルタリングできます。詳細には[差異ビュー (Differences View)]タブもあります。このタブには、オブジェクトに加えられた変更が表示されます。

HA Action Event (HA アクション イベント)

これらのイベントは、高可用性設定でのアクション (ユーザが開始したアクションまたはシステムが開始したアクション) に関連したものです。HA Action Event はイベントタイプですが、イベント名は次のいずれかです。

- **HA Suspended (HA 一時停止)** : ユーザがシステムで HA を意図的に一時停止しました。
- **HA Resumed (HA 再開)** : ユーザがシステムで HA を意図的に再開しました。
- **HA Reset (HA リセット)** : ユーザがシステムで HA を意図的にリセットしました。
- **HA Failover: Unit Switched Modes (HA フェールオーバー: ユニットモード切り替え)** : ユーザがモードを意図的に切り替えたか、ヘルスメトリック違反のためにシステムがフェールオーバーしました。このメッセージは、アクティブピアがスタンバイになったか、スタンバイピアがアクティブになったことを示します。

Interface List Scanned (スキャンされたインターフェイス リスト)

このイベントは、インターフェイスインベントリの変更をスキャンしたことを示します。

Pending Changes Discarded（保留中の変更の破棄）

このイベントは、保留中のすべての変更をユーザが削除したことを示します。このイベントと以前の Deployment Completed イベントの間の Entity Created、Entity Updated、および Entity Deleted イベントで示されたすべての変更が削除され、影響を受けたオブジェクトの状態が、最後に展開されたバージョンに戻されています。

Task Started（タスク開始）、Task Completed（タスク完了）、Task Failed（タスク失敗）

タスクイベントは、システムまたはユーザによって開始されたジョブの開始および終了を示します。これらの2つのイベントは、タスクリストで1つのタスクに統合されます。このタスクリストは、右上隅にある [タスクリスト (Task List)] ボタンをクリックすると表示されます。



タスクには、展開ジョブや手動（またはスケジュールされた）データベース更新などのアクションが含まれます。タスクリスト内の任意の項目は、監査ログの2つのタスクイベント、タスクの開始の表示、正常な完了または失敗のいずれかに対応します。

User Logged In（ユーザ ログイン）、User Logged Out（ユーザ ログアウト）：ユーザ名

これらのイベントは、Firepower Device Manager のユーザ ログインおよびユーザ ログアウトの時間と送信元 IP アドレスを示します。User Logged Out イベントは、アクティブ ログアウトと、アイドル時間を超過したための自動ログアウトの両方で発生します。

これらのイベントは、デバイスとの接続を確立している RA VPN ユーザに関するものではありません。また、デバイス CLI のログイン/ログアウトも含まれません。

監査ログの表示および分析

監査ログには、展開ジョブ、データベースの更新、Firepower Device Manager のログインとログアウトなど、システムが開始したイベントやユーザが開始したイベントに関する情報が含まれています。

ログで確認できるイベントの種類の説明については、[監査イベント（726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、[デバイス管理 (Device Administration)] > [設定の表示 (View Configuration)] リンクをクリックします。

ステップ 2 目次の [監査ログ (Audit Log)] をクリックします (未選択の場合)。

イベントは日付別にグループ分けされ、1日の中では時間別にグループ分けされます。最新の日時がリストの一番上に表示されます。初めは、各イベントは折りたたまれているため、時間、イベント名、そのイベントを開始したユーザ、ユーザの送信元 IP アドレスのみ確認できます。ユーザと IP アドレスの「システム」は、デバイス自体がイベントを開始したことを意味しています。

次を実行できます。

- イベント名の横にある [>] をクリックしてイベントを開き、イベントの詳細を確認します。もう一度アイコンをクリックするとイベントが閉じます。多くのイベントには、イベント属性（イベントタイプ、ユーザ名、送信元IPアドレスなど）の簡単なリストがあります。ただし、エンティティイベントと展開イベントには次の2つのタブがあります。
 - [概要 (Summary)] : 基本的なイベント属性が示されます。
 - [差異ビュー (Differences View)] : 既存の「展開済み」設定とイベントの一部として行われた変更との比較が示されます。展開ジョブの場合、このビューは長く、スクロールする必要がある場合があります。このタブには、展開ジョブの一部だったエンティティ イベントの変更のすべての差異が要約されます。
- [フィルタ (Filter)] フィールドの右にあるドロップダウンリストから別の時間範囲を選択します。デフォルトでは、過去2週間のイベントが表示されますが、過去24時間、7日間、月、または6ヵ月に変更できます。[カスタム (Custom)] をクリックし、開始および終了日時を入力して、正確な範囲を指定します。
- ログ内で任意のリンクをクリックして、該当項目の検索フィルタを追加します。リストが更新されて、該当項目を含むイベントだけが表示されます。単純に [フィルタ (Filter)] ボックスをクリックして、フィルタを直接作成することもできます。フィルタボックスの下には事前定義済みのフィルタがいくつかあり、クリックして関連するフィルタ条件をロードできます。イベントのフィルタリングの詳細については、[監査ログのフィルタリング \(729 ページ\)](#) を参照してください。
- ブラウザ ページをリロードして、ログを最新のイベントで更新します。

監査ログのフィルタリング

監査ログにフィルタを適用して、特定のタイプのメッセージだけが表示されるように絞り込むことができます。フィルタの各要素は、正確な完全一致です。たとえば、「User = admin」では **admin** という名前のユーザが開始したイベントだけが表示されます。

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。このリストは、フィルタ要素を追加するたびに自動的に更新されます。

事前定義のフィルタをクリック

[フィルタ (Filter)] フィールドの下には事前定義のフィルタがあります。リンクをクリックするだけでフィルタがロードされます。確認を求められます。すでにフィルタが適用されている場合は、追加されず、置き換えられます。

強調表示された項目をクリック

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ログテーブルまたはイベント詳細情報内の項目をクリックすることです。項目をクリックすると、その値と要素の組み合わせに正しく定式化されている要素を使用して、[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。

項目に関するフィルタ要素を追加できる場合は、その項目にマウスカーソルを合わせると下線が引かれ、[クリックしてフィルタに追加 (Click to Add to Filter)] コマンドが表示されます。

アトミック要素を選択

[フィルタ (Filter)] フィールドをクリックして、ドロップダウンリストから必要なアトミック要素を選択し、等号の後に照合値を入力してから Enter キーを押すことでフィルタを作成することもできます。次の要素に関するフィルタリングを実行できます。すべての要素がすべてのイベントタイプに関連するわけではないことに注意してください。

- [イベントタイプ (Event Type)] : これは、通常、イベント名と同じですが、異なる場合もあります (エンティティ名やユーザのような可変修飾子はありません)。展開イベントの場合、イベントタイプは **Deployment Event** (展開イベント) です。イベントタイプの説明については、[監査イベント \(726 ページ\)](#) を参照してください。
- [ユーザ (User)] : イベントを開始したユーザの名前。システムユーザは **SYSTEM** (すべて大文字) です。
- [送信元IP (Source IP)] : ユーザがイベントを開始した IP アドレス。システムが開始したイベントの送信元 IP アドレスは **SYSTEM** です。
- [エンティティID (Entity ID)] : エンティティまたはオブジェクトの UUID。これは、理解できない長い文字列 (8e7021b4-2e1e-11e8-9e5d-0fc002c5f931 など) です。通常、このフィルタを使用するには、イベント詳細情報内のエンティティ ID をクリックするか、REST API を使用し、関連する GET コールによって必要な ID を取得する必要があります。
- [エンティティ名 (Entity Name)] : エンティティまたはオブジェクトの名前。ユーザが作成したエンティティの場合は、通常、ユーザがオブジェクトに付けた名前 (ネットワークオブジェクトの **InsideNetwork** など) です。システムが生成したエンティティの場合は (一部のユーザ定義のエンティティについても)、事前定義されていて理解できる名前です。たとえば、明示的に名前を付けない展開ジョブの場合は「**User(admin) Triggered Deployment**」です。
- [エンティティタイプ (Entity Type)] : エンティティまたはオブジェクトの種類。これらは、事前定義されていて理解できる名前 (**Network Object** など) です。API エクスプローラで「**type**」値の関連オブジェクトモデルを調べることによってエンティティタイプを確認できます。通常、API タイプはすべて小文字であり、スペースは含まれません。それらをモデルに表示されているとおりに正確に入力し、Enter キーを押すと、文字列が理解しやすい形式に変更されます。どちらの形式で入力しても機能します。API エクスプローラを開くには、[詳細オプション (More options)] ボタン (☰) をクリックし、[API エクスプローラ (API Explorer)] を選択します。

複雑な監査ログフィルタのルール

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、「User = admin」と「User = SYSTEM」が含まれている場合、いずれかのユーザによって開始されたイベントと一致します。
- 異なるタイプの要素には、AND 関係があります。たとえば、「Event Type = Entity Updated」と「User = SYSTEM」が含まれている場合、アクティブ ユーザではなくシステムがエンティティを更新したイベントだけが表示されます。
- ワイルドカード、正規表現、部分一致、または単純なテキスト文字列の一致は使用できません。

展開およびエンティティ変更履歴の確認

展開およびエンティティイベントの詳細には、[差異ビュー (Differences View)] タブが含まれています。このタブには、古い設定と変更の色分けされた比較が表示されます。

- 展開ジョブの場合は、展開前にデバイスで実行されていた設定と、実際に展開された変更との比較です。
- エンティティイベントの場合は、オブジェクトの以前のバージョンに行われた設定の変更です。エンティティイベントの場合は、オブジェクトの以前のバージョンに行われた設定の変更です。

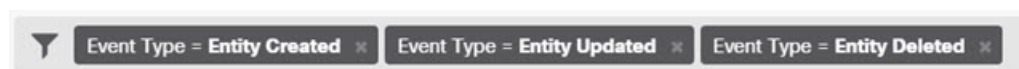
手順

ステップ 1 [デバイス (Device)] をクリックし、[デバイス管理 (Device Administration)] > [設定の表示 (View Configuration)] リンクをクリックします。

ステップ 2 目次の [監査ログ (Audit Log)] をクリックします (未選択の場合)。

ステップ 3 (オプション) メッセージのフィルタ処理：

- 展開イベント：フィルタ ボックスの下にある [展開履歴 (Deployment History)] 事前定義フィルタをクリックします。
- エンティティ変更イベント：関心のある変更の種類に対して、[イベントの種類 (Event Type)] 要素を使用してフィルタを手動で作成します。すべてのエンティティの変更を確認するには、[作成済みエンティティ (Entity Created)]、[更新済みエンティティ (Entity Updated)]、および [削除済みエンティティ (Entity Deleted)] の 3 つの仕様を含めます。フィルタは次のようになります。



ステップ 4 イベントを開き、[差異ビュー (Differences View)] タブをクリックします。

Deployment Completed: User (admin) Triggered Deployment

Summary Differences View

DEPLOYED VERSION	PENDING VERSION	Legend: Removed Added Edited
Syslog Server Removed		
Entity ID: 4a1605df-311d-11e8-893d-c15d8f450fd9		
syslogServerIpAddress: 192.168.1.25	-	
portNumber: 514	-	
deviceInterface:		
inside	-	
Network Object Added		
Entity ID: b64f4101-311d-11e8-893d-a302db0bc31e		
-	subType: Network	
-	value: 10.1.10.0/24	
-	isSystemDefined: false	
-	name: RemoteNetwork	
Network Object Edited		
Entity ID: ddb608e9-311c-11e8-893d-5588b92854ca		
value: 192.168.2.0/24	192.168.1.0/24	

変更は色分けされていて、見出しにはオブジェクトの種類と、Added（作成）、Removed（削除）、または Edited（更新）が表示されます。Edited オブジェクトには、変更された属性またはオブジェクトから削除された属性のみ表示されます。展開ジョブの場合、変更されたエンティティごとに個別の見出しがあります。見出しには、オブジェクトのエンティティタイプが表示されます。

保留中の全変更の廃棄

まだ展開されていない一連の設定の変更に納得していない場合は、すべての保留中の変更を破棄できます。破棄すると、すべての機能がデバイスに存在する状態に戻ります。その後、設定の変更をもう一度を開始できます。

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。

保留中の変更がある場合、アイコンがドット付きで強調表示されます。



ステップ2 [詳細オプション (More Options)] > [すべて破棄 (Discard All)] をクリックします。

ステップ3 確認ダイアログで [OK] をクリックします。

変更が破棄され、プロセスが完了すると、保留中の変更がないことを示すメッセージが表示されます。監査ログに [保留中の変更の破棄 (Pending Changes Discarded)] イベントが追加されます。

デバイス設定のエクスポート

現在展開されている設定のコピーを JSON 形式でエクスポートできます。このファイルは、アーカイブまたはレコードの保存目的で使用できます。パスワードや秘密キーなどのセンシティブデータはすべてマスク処理されます。

ファイルを当該デバイスや別のデバイスにインポートすることはできません。この機能は、システムバックアップの代替機能ではありません。

設定をダウンロードする前に、少なくとも1つの展開ジョブが正常に完了している必要があります。

手順

ステップ1 [デバイス (Device)] を選択し、[デバイス管理 (Device Administration)] グループで [設定の表示 (View Configuration)] をクリックします。

ステップ2 目次で [設定のダウンロード (Download Configuration)] をクリックします。

ステップ3 [デバイス設定の取得 (Get Device Configuration)] をクリックして、ファイルを作成するジョブを開始します。

ファイルを事前に作成している場合、ファイルの作成日とともに、[ダウンロード (Download)] ボタンと「File is ready to download」メッセージが表示されます。

設定のサイズによっては、ファイルの生成に数分かかることがあります。タスクリストや監査ログを確認したり、定期的にこのページに戻ったりして、Export Config ジョブが完了してファイルが生成されるのを待ちます。

ステップ4 ファイルが生成されたらこのページに戻り、[設定ファイルのダウンロード (Download the Configuration File)] ボタン (📄) をクリックして、ファイルをワークステーションに保存します。

FDM および FTD ユーザ アクセスの管理

ユーザが Firepower Device Manager にログインするための外部認証および認可ソースを設定できます (HTTPS アクセス)。ローカルユーザデータベースとシステム定義の**管理者**ユーザに加えて (またはその代わりに) 外部サーバを使用できます。FDM アクセスでは追加のローカルユーザアカウントは作成できないことに注意してください。

設定を変更できる複数の外部 FDM ユーザアカウントを用意できますが、それらの変更がユーザごとに追跡されることはありません。1 人のユーザが変更を展開すると、すべてのユーザが行った変更が展開されます。ロック機能はありません。つまり、複数のユーザが同じオブジェクトの更新を同時に試みることができます。その結果、1 人のユーザだけが変更を正常に保存できます。また、ユーザに基づいて変更を破棄することもできません。

Firepower Device Manager では、5 つの同時ユーザセッションが可能です。6 人目のユーザがログインすると、最も古いユーザセッションが自動的にログオフされます。また、アイドルタイムアウトがあり、非アクティブユーザは 20 分後にログアウトされます。

FTD CLI への SSH アクセスでは、外部認証および認可を設定することもできます。ローカルデータベースは外部ソースを使用する前に常にチェックされるため、フェールセーフアクセスでは追加のローカルユーザを作成することができます。ローカルソースと外部ソースの両方で重複するユーザを作成しないでください。**管理者**ユーザを除き、CLI ユーザと Firepower Device Manager ユーザが入れ替わることはありません。ユーザアカウントは完全に個別です。



- (注) 外部サーバを使用する場合、別の RADIUS サーバグループをセットアップするか、または特定の FTD デバイスの IP アドレスのみへのユーザアクセスを許可する RADIUS サーバ内で認証/認可ポリシーを作成することにより、デバイスのサブセットへのユーザアクセスを制御することができます。

ここでは、Firepower Device Manager のユーザアクセスの設定および管理方法と CLI ユーザアクセスについて説明します。

FDM (HTTPS) ユーザ用の外部認証 (AAA) 設定

Firepower Device Manager への HTTPS アクセスを外部 RADIUS サーバから提供できます。RADIUS 認証および認可を有効にすることにより、さまざまなレベルのアクセス権を付与でき、すべてのユーザがローカル**管理者**アカウントを使用してログインする必要がなくなります。

これらの外部ユーザは、Firepower Threat Defense API および API エクスプローラについても認証されます。

ロールベース アクセス コントロール (RBAC) を提供するには、RADIUS サーバ上のユーザアカウントを更新して、**cisco-av-pair** 属性を定義します (ISE の場合。ただし、FreeRADIUS での属性の綴りは **Cisco-AVPair** となります。システムで正しいスペルを確認してください)。ユーザアカウントでこの属性を正しく定義する必要があります。そうしなければ、ユーザは

Firepower Device Manager へのアクセスを拒否されます。 **cisco-av-pair** 属性のサポートされる値は、次のとおりです。

- **fdm.userrole.authority.admin** はフル管理者アクセスを提供します。これらのユーザは、ローカル管理者ユーザが実行できるすべてのアクションを実行できます。
- **fdm.userrole.authority.rw** は読み取り/書き込みアクセスを提供します。これらのユーザは、読み取り専用ユーザが実行できるすべてのアクションを実行でき、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、Firepower Device Manager ユーザのセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- **fdm.userrole.authority.ro** は読み取り専用アクセスを提供します。これらのユーザは、ダッシュボードと設定を表示できますが、変更できません。ユーザが変更しようとする、権限が不足していることを示すエラーメッセージが表示されます。

ユーザが Firepower Device Manager にログインすると、ページの右上隅にユーザ名とロール ([管理者 (Administrator)]、[読み取り/書き込みユーザ (Read-Write User)]、または[読み取り専用ユーザ (Read-Only User)]) が表示されます。

RADIUS サーバで正しくアカウントを設定すると、次の手順で管理アクセス用にそのアカウントを有効にできます。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [管理アクセス (Management Access)] 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 [管理アクセス (Management Access)] をクリックします。
- ステップ 2** まだ選択されていない場合は、[AAA設定 (AAA Configuration)] タブをクリックします。
- ステップ 3** [HTTPS接続 (HTTPS Connection)] のオプションを設定します。
 - [管理/REST API用のサーバグループ (Server Group for Management/REST API)] : プライマリ認証ソースとして使用する RADIUS サーバグループまたはローカルユーザデータベース (LocalIdentitySource) を選択します。外部認証を使用する RADIUS サーバグループを選択する必要があります。

サーバグループがまだ存在しない場合は、[新しいRADIUSサーバグループの作成 (Create New RADIUS Server Group)] リンクをクリックしてすぐに作成します。サーバごとに RADIUS サーバ オブジェクトを作成してグループに追加する必要がありますが、サーバグループを定義するときにこれを実行できます。RADIUS の詳細については、[RADIUS サーバおよびグループ \(188 ページ\)](#) を参照してください。

 - [ローカルによる認証 (Authentication with LOCAL)] : 外部サーバグループを選択する場合、ローカル [管理 (admin)] アカウントを含むローカルアイデンティティソースを使用する方法を指定できます。次のいずれかを選択します。

- [外部サーバの前 (Before External Server)] : システムは、まずローカルソースに対してユーザ名とパスワードを確認します。
- [外部サーバの後 (After External Server)] : 外部ソースが使用できない場合またはユーザアカウントが外部ソースで見つからなかった場合にのみ、ローカルソースが確認されます。
- [使用しない (Never)] : (非推奨) ローカルソースがまったく使用されないため、管理者ユーザとしてログインできません。

注意 [使用しない (Never)] を選択すると、[管理 (admin)] アカウントを使用して Firepower Device Manager にログインできなくなります。RADIUS サーバが使用できなくなった場合または RADIUS サーバのアカウント設定が間違っている場合は、システムがロックされます。

ステップ 4 [保存 (Save)] をクリックします。

FTD CLI (SSH) ユーザ用の外部認証 (AAA) 設定

外部 RADIUS サーバから FTD CLI への SSH アクセスを提供できます。RADIUS 認証および許可を有効にすることで、デバイスごとに個別のローカルユーザアカウントを定義するのではなく、単独の認証ソースからさまざまなレベルのアクセス権を提供することができます。

これらの SSH 外部ユーザは、Firepower Threat Defense API および API エクスプローラには認証されません。SSH の認証を定義するために使用するメカニズムは、HTTPS アクセスに必要なものとは異なります。ただし、SSH と HTTPS の両方の許可条件で同じ RADIUS ユーザを設定し、どちらのプロトコルでも特定のユーザがシステムにアクセスできるようにすることは可能です。

SSH アクセスにロールベースのアクセス制御 (RBAC) を提供するには、RADIUS サーバ上のユーザアカウントを更新して **Service-Type** 属性を定義します。この属性はユーザアカウントで定義されている必要があります。定義されていないと、ユーザの SSH へのアクセスが拒否されます。次に、**Service-Type** 属性でサポートされている値を示します。

- **Administrator (6)** : CLI への **config** アクセス認証を提供します。これらのユーザは、CLI ですべてのコマンドを使用できます。
- **NAS Prompt (7)** または 6 以外のレベル : CLI への **basic** アクセス認証を提供します。これらのユーザは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

RADIUS サーバで正しくアカウントを設定すると、次の手順で SSH 管理アクセス用にそのアカウントを有効にすることができます。



- (注) ローカルソースと外部ソースの両方で重複するユーザを作成しないでください。重複するユーザ名を作成した場合は、同じ許可権限があることを確認します。許可権限がローカルユーザアカウントで異なる場合、外部バージョンのユーザアカウントのパスワードを使用してログインすることはできません。ログインできるのはローカルのパスワードを使用した場合のみです。権限が同じ場合、パスワードが異なっていれば、使用するパスワードによって外部ユーザまたはローカルユーザのどちらでログインしているかが判断されます。最初にローカルデータベースが確認されますが、ユーザ名がローカルデータベースに存在するがパスワードが正しくない場合、外部サーバが確認され、外部ソースのパスワードが正しい場合、ログインが成功します。

始める前に

外部定義ユーザに次の動作を通知し、希望通りに設定できるようにしてください。

- 外部ユーザが初めてログインすると、FTD は必要な構造体を作成しますが、ユーザセッションを同時に作成することはできません。ユーザがセッションを開始するには、再度認証する必要があります。ユーザには次のようなメッセージが表示されます。「新しい外部ユーザ名が特定されました。(New external username identified.) セッションを開始するにはもう一度ログインしてください。(Please log in again to start a session.)」
- 同様に、最後のログイン以降に Service-Type で定義したユーザの認証が変更された場合は、ユーザは再認証する必要があります。ユーザには次のようなメッセージが表示されません。「認証権限が変更されています。(Your authorization privilege has changed.) セッションを開始するにはもう一度ログインしてください。(Please log in again to start a session.)」

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)] > [管理アクセス (Management Access)] 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 [管理アクセス (Management Access)] をクリックします。

ステップ 2 まだ選択されていない場合は、[AAA設定 (AAA Configuration)] タブをクリックします。

ステップ 3 [SSH接続 (SSH Connection)] のオプションを設定します。

- [サーバグループ (Server Group)]: プライマリ認証ソースとして使用する RADIUS サーバグループまたはローカルユーザデータベース (LocalIdentitySource) を選択します。外部認証を使用する RADIUS サーバグループを選択する必要があります。

サーバグループがまだ存在しない場合は、[新しいRADIUSサーバグループの作成 (Create New RADIUS Server Group)] リンクをクリックしてすぐに作成します。サーバごとに RADIUS サーバ オブジェクトを作成してグループに追加する必要もありますが、サーバグループを定義するときにこれを実行できます。RADIUS の詳細については、[RADIUS サーバおよびグループ \(188 ページ\)](#) を参照してください。

SSH 接続はグループ内の最初の 2 つのサーバのみ使用することに注意してください。3 つ以上のサーバがあるグループを使用する場合、追加のサーバが試行されることはありません。さらに、[デッドタイム (Dead Time)] と [最大失敗試行数 (Maximum Failed Attempts)] グループ属性は使用されません。

- [ローカルによる認証 (Authentication with LOCAL)] : 外部サーバグループを選択する場合、ローカルアイデンティティソースを使用する方法を指定できます。SSH アクセスでは、ローカルデータベースが常に外部サーバの前に確認されます。

ステップ 4 [保存 (Save)] をクリックします。

Firepower Device Manager ユーザセッションの管理

[モニタリング (Monitoring)] > [セッション (Sessions)] を選択すると、現在 Firepower Device Manager にログインしているユーザのリストが表示されます。このリストには、各ユーザが現在のセッションにログインしている時間が示されます。

同じユーザ名が複数回表示される場合は、ユーザが異なる送信元アドレスからセッションを開いたことを意味します。セッションは、ユーザ名と送信元アドレスに基づいて個別に追跡され、各セッションは固有のタイムスタンプを持ちます。

このシステムでは、5 つの同時ユーザセッションが可能です。6 人目のユーザがログインすると、最も古い現在のセッションが自動的にログアウトされます。また、アイドル状態のユーザは、アクティビティが 20 分間ないと自動的にログアウトされます。

FDM ユーザが、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、ユーザのアカウントは 5 分間ロックされます。ユーザは再度ログインを試みる前に待つ必要があります。FDM ユーザアカウントをロック解除する方法はありません。また、再試行回数やロックタイムアウトを調整することもできません (SSH ユーザの場合は、これらの設定を調整し、アカウントをロック解除することができます)。

必要に応じて、セッションの [削除 (delete)] アイコン (🗑️) をクリックすることにより、ユーザセッションを終了させることができます。自分自身のセッションを削除すると、自分もログアウトされます。セッションを終了させた場合、ロックアウト期間はなく、ユーザはすぐにログインしなおすことができます。

外部ユーザ用のスタンバイ HA ユニットでの FDM アクセスの有効化

FDM ユーザ用に外部認証を設定すると、これらのユーザはハイアベイラビリティペアのアクティブおよびスタンバイ装置の両方にログインできます。ただし、スタンバイ装置への最初のログインを正常に行うには、アクティブな装置にログインする場合と比較して、いくつかの追加手順が必要です。

外部ユーザがアクティブな装置に最初にログインした後、システムはユーザおよびユーザのアクセス権を定義するオブジェクトを作成します。管理者または読み取り/書き込みユーザはそ

の後、アクティブな装置からユーザオブジェクトの設定を展開し、スタンバイ装置で表示されるようにする必要があります。

展開および後続の設定同期が正常に終了した後にのみ、外部ユーザがスタンバイ装置にログインすることができます。

管理者および読み取り/書き込みユーザは、アクティブな装置にログインした後に変更を展開できます。ただし、読み取り専用ユーザは設定を展開できないため、適切な権限を持つユーザに設定を展開を依頼する必要があります。

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` 権限を持っていれば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 minpasswdlen** *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。

システムの再起動またはシャットダウン

必要に応じて、システムを再起動またはシャットダウンすることができます。

下記の手順以外に、**reboot** または **shutdown** コマンドを使用して、SSH セッションまたは FDM CLI コンソールからこれらのタスクを実行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、[システム設定 (System Settings)] > [再起動/シャットダウン (Reboot/Shutdown)] リンクをクリックします。

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 [再起動/シャットダウン (Reboot/Shutdown)] をクリックします。

ステップ 2 必要な機能を実行するボタンをクリックします。

- [再起動 (Reboot)] : システムが正常に動作しておらず、どうしても問題が解決できないと判断した場合に、デバイスを再起動できます。また、システムソフトウェアをリロードするためにデバイスを再起動するよう求める手順がいくつかあります。
- [シャットダウン (Shut Down)] : システムをシャットダウンし、制御された方法で電源をオフにします。ネットワークからデバイスを削除する場合 (デバイスの交換などの場合) は、シャットダウンを使用します。デバイスをシャットダウンした後は、ハードウェアのオン/オフ スイッチからのみ電源をオンにすることができます。

ステップ 3 操作が完了するまで待ちます。

システムの再起動またはシャットダウン中は、FDM または CLI で他の操作を実行することはできません。

再起動中、FDM のページが更新され、再起動が完了するとログイン ページに移動します。再起動が完了する前に Web ブラウザでページを更新しようとすると、その時点での FDM Web サーバの動作状態に基づいて、503 または 404 エラーを返すことがあります。

シャットダウンの場合、システムは最終的には応答できず、404 エラーが表示されます。システムを完全にオフにしようとしているため、これは想定される結果です。

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。コマンドは、**ping** CLI コンソールを開くかデバイスの CLI にログインすることにより使用できます。



- (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 ホスト

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) にできます。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 ホスト

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、を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 ww1.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
 1 10.83.194.1 0 msec 10 msec 0 msec
 2 10.83.193.65 0 msec 0 msec 0 msec
```

```

3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 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へ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。
 - 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、**Decrement_TTL**。
 - 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。

```
icmp unreachable rate-limit 50 burst-size 1
```

```
policy-map global_policy
  class class-default
    set connection decrement-ttl
```

- 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。

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
  class class-default
    no set connection decrement-ttl
```

- 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 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。

- 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。

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。[DNS の一般的な問題のトラブルシューティング \(702 ページ\)](#) も参照してください。

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。これは、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` を入力します。

- `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す。

```
> 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** を試行します。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-gwl.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 Command Reference』 (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     | br1.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な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 \(109 ページ\)](#) を参照してください。

デバイスがハイアベイラビリティ用に設定されている場合は、まず、デバイスマネージャ（可能な場合）または **configure high-availability disable** コマンドを使用して、ハイアベイラビリティ構成を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします。

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 \(108 ページ\)](#) を参照してください。

デバイスがハイアベイラビリティ用に設定されている場合は、まず、デバイスマネージャ (可能な場合) または **configure high-availability disable** コマンドを使用して、ハイアベイラビリティ構成を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

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。

- a) FMC からデバイスを登録解除します。
- b) 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 \(108 ページ\)](#) を参照してください。

デバイスがハイアベイラビリティ用に設定されている場合は、まず、デバイスマネージャ（可能な場合）または **configure high-availability disable** コマンドを使用して、ハイアベイラビリティ構成を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

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 \(765 ページ\)](#)
- [Smart CLI および FlexConfig に関する注意事項と制限事項 \(776 ページ\)](#)
- [Smart CLI オブジェクトの設定 \(776 ページ\)](#)
- [FlexConfig ポリシーの設定 \(779 ページ\)](#)
- [FlexConfig ポリシーのトラブルシューティング \(792 ページ\)](#)
- [FlexConfig の例 \(793 ページ\)](#)

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 Command References』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。

ソフトウェアのアップグレードが FlexConfig ポリシーに与える影響

新しいバージョンの Firepower Threat Defense ソフトウェアにはそれぞれ、Firepower Device Manager の機能を設定するためのサポートが追加されています。これらの新機能は、FlexConfig を使用して以前に設定した機能と重複する場合があります。

アップグレードの後に、FlexConfig ポリシーおよびオブジェクトを調べる必要があります。Firepower Device Manager またはスマート CLI 内の追加されたサポートのためにブラックリストに登録されたコマンドがある場合は、オブジェクトのアイコンとメッセージに問題が示されます。その場合は、設定をやりなおしてください。ブラックリストに登録されたコマンドのリストは、コマンドをどのように設定する必要があるのかを判断するために役立ちます。

FlexConfig ポリシーに添付されている FlexConfig オブジェクトに新しくブラックリストに登録されたコマンドが含まれていても、システムは変更の展開を妨げません。ただし、FlexConfig ポリシーに示されているすべての問題を解決するまでは、新しい Smart CLI オブジェクトを作成できません。

FlexConfig ポリシーから問題のあるオブジェクトを単に削除できます。これは、デバイス設定にアクティブに展開しているオブジェクトにのみ制限が適用されるためです。そのため、オブジェクトを削除してから、それらを、対応する Smart CLI または統合された Firepower Device Manager 設定を作成する際にリファレンスとして使用できます。新しい設定に不満がない場合は、単にオブジェクトを削除できます。削除されたオブジェクトに、ブラックリストに登録されていない要素が含まれている場合は、それらを編集してサポートされていないコマンドを削除してから、オブジェクトを FlexConfig ポリシーに再添付できます。

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。Smart CLI 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)] > [アイデンティティソース (Identity Sources)] を使用します。
aaa-server	[オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] 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。

禁止された CLI コマンド	説明
access-list	部分的にブロックされます。 <ul style="list-style-type: none"> • ethertype アクセス リストを作成できます。 • extended および standard アクセスリストは作成できません。Smart CLI 拡張アクセス リストまたは標準アクセス リストオブジェクトを使用してこれらの ACL を作成します。その後、それらは、サービスポリシートラフィッククラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド (match access-list など) で使用できます。 • 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。
as-path	Smart CLI AS パス オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、自律システムパスフィルタを設定します。
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	—
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	—

禁止された CLI コマンド	説明
command-alias	—
community-list	Smart CLI 拡張コミュニティ リストまたは標準コミュニティ リスト オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、コミュニティリストフィルタを設定します。
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	[オブジェクト (Objects)] > [DNS グループ (DNS Groups)] を使用して DNS グループを設定し、[デバイス (Device)] > [システム設定 (System Settings)] > [DNS サーバ (DNS Server)] を使用してそれらのグループを割り当てます。
dns-group	[オブジェクト (Objects)] > [DNS グループ (DNS Groups)] を使用して DNS グループを設定し、[デバイス (Device)] > [システム設定 (System Settings)] > [DNS サーバ (DNS Server)] を使用してグループを割り当てます。
domain-name	[オブジェクト (Objects)] > [DNS グループ (DNS Groups)] を使用して DNS グループを設定し、[デバイス (Device)] > [システム設定 (System Settings)] > [DNS サーバ (DNS Server)] を使用してグループを割り当てます。
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。

禁止された CLI コマンド	説明
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	—
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> <ul style="list-style-type: none"> cts ip address ip address dhcp ipv6 address ipv6 enable ipv6 nd dad ipv6 nd suppress-ra mode nameif security-level shutdown zone-member
vni、redundant、tunnel 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。

禁止された CLI コマンド	説明
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 ospf コマンドと ipv6 router ospf コマンドを設定することはできますが、その他のすべての ipv6 コマンドは禁止されています。 SmartCLI IPv6 プレフィックスリストオブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、IPv6 のプレフィックス リストフィルタを設定します。
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。
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。 ただし、FlexConfig で logging history コマンドを設定できません。
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	—

禁止された CLI コマンド	説明
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。
passwd password	—
password-policy	—
policy-list	スマート CLI ポリシーリストオブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシー リストを設定します。
policy-map sub-commands	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
prefix-list	Smart CLI IPv4 プレフィックスリストオブジェクトを作成し、それらを Smart CLI OSPF または BGP オブジェクトで使用して、IPv4 のプレフィックス リストフィルタを設定します。
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。

禁止された CLI コマンド	説明
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。
route-map	スマート CLI ルート マップ オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルート マップを設定します。
router bgp	BGP には Smart CLI テンプレートを使用します。
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。
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	—

禁止された CLI コマンド	説明
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
オブジェクト： AS パス	AS パス	ルーティング プロトコル オブジェクトで使用する AS パス オブジェクトを作成します。
オブジェクト：ア クセス リスト	拡張アクセス リ スト 標準アクセス リ スト	ルーティング オブジェクトで使用する拡張 ACL または標準 ACL を作成します。ACL を使用する許可コマンドを設定する FlexConfig オブジェクトからの名前によって、これらのオブジェクトを参照することもできます。
オブジェクト：コ ミュニティ リス ト	拡張コミュニティ リスト 標準コミュニティ リスト	ルーティング オブジェクトで使用する拡張コミュニティ リストまたは標準コミュニティ リストを作成します。
オブジェクト：プ レフィックス リ スト	IPv4 プレフィッ クス リスト IPv6 プレフィッ クス リスト	ルーティング オブジェクトで使用する IPv4 または IPv6 プレフィックス リストを作成します。
オブジェクト：ポ リシー リスト	ポリシー リスト	ルーティング オブジェクトで使用するポリシー リストを作成します。
オブジェクト： ルート マップ	ルート マップ	ルーティング オブジェクトで使用するルート マップを作成します。

機能	テンプレート	説明
ルーティング： BGP	BGP	BGP 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ます。
ルーティング： BGP の一般設定	BGP	BGP の一般設定テンプレートを使用して、すべての BGP プロセスに適用するグローバル設定を設定します。
ルーティング： OSPFv2	OSPF OSPF インターフェイス設定	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 Smart CLI 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、テーブルの上の [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 \(780 ページ\)](#)
- [FlexConfig オブジェクトの変数の作成 \(783 ページ\)](#)
- [秘密キー オブジェクトの設定 \(791 ページ\)](#)

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。

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、変数进行评估し、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 \(792 ページ\)](#) 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 \(783 ページ\)](#) 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 \(784 ページ\)](#) 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、二重括弧に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}} または {{{variable}}}](#) (784 ページ) を参照してください。
- **Smart CLI** オブジェクトを使用するには、オブジェクト名を入力します。**Smart CLI** に設定されているルーティングプロセスを参照する必要がある場合は、プロセス ID を入力します。[FlexConfig オブジェクト内の Smart CLI オブジェクトの参照 \(790 ページ\)](#) 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ゲートします。

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、ネゲ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、ネゲ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 (779 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 \(780 ページ\)](#) 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 \(791 ページ\)](#) 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}} または {{{variable}}}](#) (784 ページ)
- [セクション {{#key}} {/key}} と逆セクション {{^key}} {{/key}}](#) (788 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}} または {{{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}}
```

または

```
{{{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]。変数に & などの特殊文字が含まれている場合、三重カッコを使用します。または、すべての変数で常に三重カッコを使用できます。

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、[詳細オプション (More options)] ボタン (☰) をクリックし、[APIエクスプローラ (API Explorer)] を選択します。

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)	<p>変数 :</p> <p><code>{{variable_name}}</code></p> <p>セクション :</p> <p><code>{{#variable_name}}</code> <code>commands</code> <code>{{/variable_name}}</code></p> <p>反転セクション :</p> <p><code>{{^variable_name}}</code> <code>commands</code> <code>{{/variable_name}}</code></p>	<p>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。</p> <p>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。</p>

変数の型	参照モデル	説明
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>	<p>[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。</p> <p>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。</p> <p>次に、役に立つ主な属性をいくつか示します。</p> <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
<p>ネットワーク (オブジェクト変数：API モデルは NetworkObject です)</p>	<p>変数 (ネットワークオブジェクト) : <code>{{variable_name.attribute}}</code> 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>	<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。
<p>数値 (単純変数)</p>	<p>変数 : <code>{{variable_name}}</code></p>	<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>
<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)</p>	<p>変数 : <code>{{variable_name.attribute}}</code></p>	<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。
<p>秘密 (オブジェクト変数：API モデルは Secret です)</p>	<p>変数 : <code>{{variable_name.password}}</code> または <code>{{{variable_name.password}}}</code></p>	<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> <p>パスワードに <code>&</code> などの特殊文字が含まれる場合、三重カッコを使用します。</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内容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す。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、そ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}}
```

FlexConfig オブジェクト内の Smart CLI オブジェクトの参照

FlexConfig オブジェクトを作成する場合、変数を使用して、Firepower Device Manager 内で設定可能なオブジェクトを示すことができます。たとえば、インターフェイス要素やネットワークオブジェクトを示す変数を作成できます。

ただし、同じ方法で Smart CLI オブジェクトを示すことはできません。

代わりに、FlexConfig ポリシーで使用する必要がある Smart CLI オブジェクトを作成する場合は、適切な場所で Smart CLI オブジェクトの名前を単純に入力します。

たとえば、プロトコルインスペクションを設定する場合、トラフィック クラスとして、拡張アクセスリストを使用することがあります。これは、拡張アクセスリストのスマート CLI オブジェクトが存在するため、このスマート CLI オブジェクトを使用して ACL を作成する必要があります。FlexConfig オブジェクトで **access-list** コマンドを使用することはできません。

たとえば、192.168.1.0/24 および 192.168.2.0/24 ネットワーク間でグローバルに DCERPC インスペクションを有効化する場合は、次の手順を実行します。

手順

ステップ 1 2つのネットワークに個別のネットワークオブジェクトを作成します。たとえば、`InsideNetwork` と `dmz-network`。

ステップ 2 これらのオブジェクトを Smart CLI 拡張アクセス リスト オブジェクトで使用します。

Name	Description
<code>dcerpc_class</code>	

CLI Template

Extended Access List

Template

```

1 access-list dcerpc_class extended
2   configure access-list-entry permit
3     permit network source [ InsideNetwork ] destination [ dmz-network ]
4     configure permit port any
5     permit port source ANY destination ANY
6     configure logging default
7     default log set log-level INFORMATIONAL log-interval 300

```

ステップ 3 名前を Smart CLI オブジェクトを示す FlexConfig オブジェクトを作成します。

たとえば、オブジェクトの名前が「`dcerpc_class`」の場合、FlexConfig オブジェクトは次のようになります。ネゲートテンプレートでは、Smart CLI オブジェクトから作成したアクセスリス

トは無効にできない点に注意してください。そのオブジェクトは、実際には FlexConfig から作成されたオブジェクトではないためです。

Template

```
1 class-map dcerpc_inspection
2   match access-list dcerpc_class
3 policy-map global_policy
4   class dcerpc_inspection
5     inspect dcerpc
```

Negate Template

```
1 policy-map global_policy
2   no class dcerpc_inspection
3 no class-map dcerpc_inspection
```

ステップ 4 オブジェクトを FlexConfig ポリシーに追加します。


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 \(783 ページ\)](#) 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。[保留中の変更 (Pending Changes)] ダイアログボックスに「最後の展開は失敗しました (Last Deployment Failed)」というメッセージが表示された場合は、[詳細の表示 (See Details)] リンクをクリックします。リンクから監査ログが表示されます。このログで失敗した展開ジョブを確認できます。特定のエラーメッセージを検索するには、ジョブを開きます。

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 を介するものであり、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。

Deployment Failed: User (admin) Triggered Deployment

- "Template" field of `sysopt-connection-tcpms` caused an error. ERROR: [3] is smaller than minimum allowed MSS of 48 by RFC 791 Config Error - `sysopt connection tcpms 3`

```
sysopt connection tcpms 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。「Config Error」で始まるテキストが、エラーメッセージを生成した特定の行を示しています。
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。

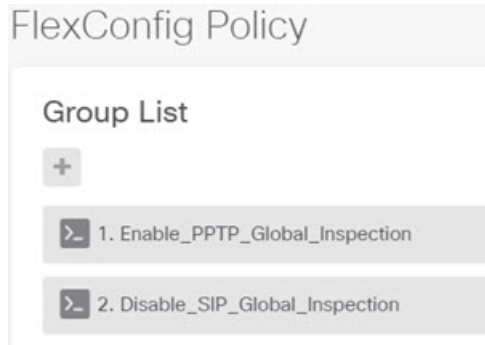
ステップ 5 オブジェクトを FlexConfig ポリシーに追加します。

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。

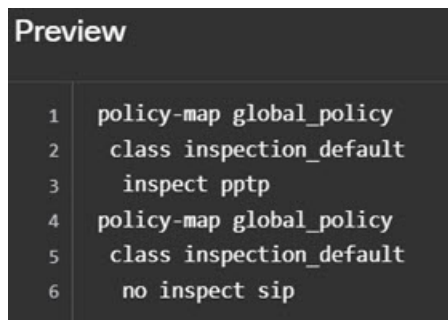
- 目次で [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。
- [グループリスト (Group List)] で [+] をクリックします。

- 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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 \(793 ページ\)](#) 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

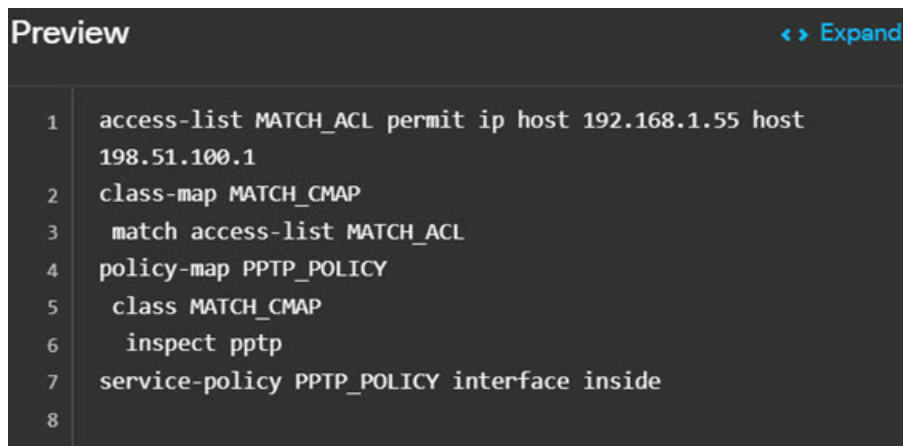
- a) 目次で [FlexConfigポリシー (FlexConfig Policy)] をクリックします。
- b) [グループリスト (Group List)] で [+] をクリックします。
- c) [Enable_PPTP_Inspection_on_Interface] オブジェクトを選択し、[OK] をクリックします。

グループリストは次のようになります。

FlexConfig Policy



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。



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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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** (ACL の確認用)。

- **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** (クラスおよびポリシーマップ設定の確認用)。
- **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
```

高精度時間プロトコルの設定方法 (ISA 3000)

高精度時間プロトコル (PTP) は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。これらのデバイスクロックは、一般に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせによる、分散型のネットワークシステムです。PTP デバイスには、オーディナリクック、境界クック、およびトランスペアレントクックが含まれます。非 PTP デバイスには、ネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

FTD デバイスは、トランスペアレントクックとして設定できます。FTD デバイスは、自身のクロックを PTP クロックと同期しません。FTD デバイスは、PTP クロックで定義されている PTP のデフォルト プロファイルを使用します。

PTP デバイスを設定するときは、連携させるデバイスのドメイン番号を定義します。したがって、複数の PTP ドメインを設定した後、1つの特定のドメインに PTP クロックを使用するように各非 PTP デバイスを設定できます。

始める前に

デバイスが使用する PTP クロックに設定されているドメイン番号を確認します。この例では、PTP ドメイン番号が 10 であることを前提としています。また、システムがドメイン内の PTP クロックに到達できるインターフェイスを決定します。

次に、PTP を設定する際のガイドラインを示します。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。
- PTP は IPv6 ネットワークではなく、IPv4 ネットワークでのみ使用できます。
- PTP 設定は、ルーテッドかブリッジグループメンバーかを問わず、物理イーサネットデータ インターフェイスでサポートされます。管理インターフェイス、サブインターフェイス、Etherchannel、ブリッジ仮想インターフェイス (BVI)、またはその他の仮想インターフェイスではサポートされません。
- VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。
- PTP パケットが確実にデバイスを通過できるようにする必要があります。PTP トラフィックは UDP 宛先ポート 319 と 320、および宛先 IP アドレス 224.0.1.129 によって識別されます。そのため、このトラフィックを許可するアクセス コントロール ルールはすべて動作します。
- ルーテッドファイアウォールモードでは、PTP マルチキャスト グループ用のマルチキャストルーティングを有効にする必要もあります。さらに、PTP をイネーブルにしたインターフェイスがブリッジグループに含まれていない場合は、IGMP マルチキャストグループ 224.0.1.129 に参加するようにインターフェイスを設定する必要があります。物理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は、IGMP マルチキャストグループに参加するように設定することはありません。

手順

ステップ 1 現在の PTP 設定を確認します。

CLI セッションでは、SSH かコンソール ポートのいずれか、または FDM CLI コンソールを使用して、**show ptp** コマンドで現在の PTP 設定を確認できます。PTP が設定されていない場合は、次の出力が表示されます。この手順の残りの部分では、PTP が設定されていないことを前提としています。

```
> show ptp clock
No clock information is available in PTP forwarding mode.
```

```
> show ptp port
No clock information is available in PTP forwarding mode.
```

ステップ 2 PTP クロック側インターフェイスの設定を確認します。

デフォルト設定では、すべてのインターフェイスが同じブリッジグループに配置されますが、ブリッジグループからインターフェイスを削除することができます。マルチキャストIGMPグループの場合とは異なる方法で設定する必要があるため、インターフェイスがルーテッドなのかブリッジグループメンバーなのかを決定することが重要です。

次の手順では、どのインターフェイスがブリッジグループに含まれているかを確認する方法について説明します。PTP用に設定するインターフェイスがブリッジグループメンバーかどうかを確認します。

- a) FDM で、[デバイス (Device)] > [インターフェイス (Interfaces)] の [すべてのインターフェイスを表示 (View All Interfaces)] をクリックします。
- b) リストでインターフェイスを検索し、[モード (Mode)] 列を確認します。BridgeGroupMember はブリッジグループの一部であることを意味します。それ以外の場合はルーテッドです。

ステップ 3 FDM で、[デバイス (Device)] > [詳細設定 (Advanced Configuration)] の [設定の表示 (View Configuration)] をクリックします。

ステップ 4 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 5 PTP を有効にして適切なインターフェイスに設定するために必要な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。たとえば、**Enable_PTP** と入力します。
- c) [テンプレート (Template)] エディタで、必要なコマンドをインデントを含めて入力します。

次の例では、PTP ドメイン 10 の GigabitEthernet1/2 で PTP を設定しています。これらの設定は、ネットワークに関連する設定に合わせて調整する必要があります。システムがネットワーク内の PTP クロックに接続できるインターフェイスで、PTP を有効にします。バックアップクロックを使用できる他のインターフェイスがある場合は、PTP を有効にするための行を追加し、ルーテッドインターフェイスの場合は、そのインターフェイスの IGMP グループをこの一連のコマンドに結合します。

この例では、GigabitEthernet1/2 はブリッジグループメンバーであるため、**igmp** コマンドを含めないでください。**igmp** コマンドはブリッジグループメンバーではサポートされていないため、コマンドを含めると、システムがコマンドを認識できないことを示す展開エラーが表示されます。

```
multicast-routing
ptp mode e2etransparent
ptp domain 10
interface GigabitEthernet1/2
  ptp enable
```

GigabitEthernet1/2 がルーテッドインターフェイスの場合は、224.0.1.129 IGMP グループ（すべてのネットワークの正しい IP アドレス）に参加するように **igmp** コマンドを含める必要があります。完成したオブジェクトは次のようになります。

```
multicast-routing
ptp mode e2etransparent
ptp domain 10
interface GigabitEthernet1/2
  ptp enable
  igmp join-group 224.0.1.129
```

- 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。

```
no multicast-routing
no ptp mode e2etransparent
no ptp domain 10
interface GigabitEthernet1/2
  no ptp enable
```

ルーテッドインターフェイスのネゲートテンプレートは、次のようになります。

```
no multicast-routing
no ptp mode e2etransparent
no ptp domain 10
interface GigabitEthernet1/2
  no ptp enable
  no igmp join-group 224.0.1.129
```

オブジェクトは次のようになります。

Name

Enable_PTP

Description

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

```

1 multicast-routing
2 ptp mode e2etransparent
3 ptp domain 10
4 interface GigabitEthernet1/2
5 ptp enable

```

Negate Template ⚠

```

1 no multicast-routing
2 no ptp mode e2etransparent
3 no ptp domain 10
4 interface GigabitEthernet1/2
5 no ptp enable

```

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 6 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_PTP 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。

Group List

+

> 1. Enable_PTP

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。

```

Preview
-----
1  multicast-routing
2  ptp mode e2transparent
3  ptp domain 10
4  interface GigabitEthernet1/2
5  ptp enable

```

- 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ8 PTP 設定を確認します。

FDM CLI コンソール、SSH セッション、またはコンソールセッションから、PTP の設定を確認します。

```

> show ptp clock
PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81

```

```
Port identity: Port Number: 4  
PTP version: 2  
Port state: Disabled
```
