



Cisco Firepower Threat Defense バージョン 6.2 コンフィギュレーションガイド（Firepower Device Manager 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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティングシステムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、<http://www.cisco.com/go/trademarks> でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2015-2017 Cisco Systems, Inc. All rights reserved.



目次

使用する前に 1

このガイドの目的 1

Firepower Device Manager/Firepower Threat Defense6.2 の新機能 2

システムへのログイン 6

Firepower Device Manager へのログイン 7

コマンドラインインターフェイス (CLI) へのログイン 8

パスワードの変更 8

ユーザプロファイル設定の設定 9

Firepower Threat Defenseの CLI ユーザアカウントの作成 9

システムの設定 11

インターフェイスの接続 12

ASA 5506-X、5506W-X、5506H-X のケーブル接続 13

ASA 5508-X および 5516-X のケーブル接続 14

ASA 5512-X、5515-X、5525-X、5545-X、5555-X のケーブル接続 15

初期設定の完了 16

外部サブネットが内部サブネットと競合する（セットアップウィザードがステップ
1 でハングする）場合の解決策 19

ワイヤレスアクセスポイント (ASA 5506W-X) の設定 21

初期セットアップ前のデフォルト設定 25

初期セットアップ後の設定 27

設定の基本 31

デバイスの設定 31

変更の展開 32

インスペクションエンジンを再起動させる設定変更 33

インターフェイスと管理ステータスの表示 34

システムタスクステータスの表示 35

FirePOWER Threat Defenseの使用例 37

ネットワーク トラフィックを調べる方法	37
脅威をブロックする方法	45
マルウェアをブロックする方法	49
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	53
アプリケーションの使用を制御する方法	58
サブネットの追加方法	62
システムのライセンス	71
Firepower システムのスマート ライセンス	71
Cisco Smart Software Manager	71
License Authority との定期通信	72
スマート ライセンスのタイプ	72
期限切れまたは無効なオプション ライセンスの影響	73
スマート ライセンスの管理	74
デバイスの登録	75
オプション ライセンスの有効化と無効化	76
Cisco Smart Software Manager との同期	77
デバイスの登録解除	77
デバイスのモニタリング	79
トラフィック統計情報を取得するためのロギングの有効化	79
トラフィックおよびシステム ダッシュボードのモニタリング	80
コマンドラインを使用した追加の統計のモニタリング	83
イベントの表示	83
イベント タイプ	85
カスタム ビューの設定	86
イベントのフィルタリング	87
イベント フィールドの説明	88
オブジェクト	99
オブジェクト タイプ	99
オブジェクトの管理	101
ネットワーク オブジェクトとグループの設定	102
ポート オブジェクトとグループの設定	103
セキュリティ ゾーンの設定	105

アプリケーションフィルタ オブジェクトの設定	106
URL オブジェクトとグループの設定	109
地理位置情報オブジェクトの設定	110
syslog サーバの設定	111
基本	113
インターフェイス	115
Firepower Threat Defenseインターフェイスについて	115
インターフェイス設定の制約	115
データ インターフェイス	116
IPv6 アドレッシング	117
管理/診断インターフェイス	118
個別の管理ネットワークを設定するための推奨事項	118
個別管理ネットワークの管理/診断インターフェイス設定の制限事項	119
セキュリティ ゾーン	119
Auto-MDI/MDIX 機能	120
MTU について	120
パス MTU ディスカバリ	120
MTU とフラグメンテーション	120
MTU とジャンボ フレーム	121
インターフェイスの設定	121
物理インターフェイスの設定	122
VLAN サブインターフェイスと 802.1Q トランキングの設定	125
ブリッジグループの設定	128
高度なインターフェイス オプションの設定	132
モニタリング インターフェイス	134
ルーティング	137
ルーティングの概要	137
NAT がルート選択に及ぼす影響	137
ルーティング テーブルとルートの選択	138
転送の決定方法	138
スタティック ルートの設定	139
ルーティングのモニタリング	140

セキュリティ ポリシー	143
アイデンティティ ポリシー	145
アイデンティティ ポリシーの概要	145
アクティブ認証によるユーザ アイデンティティの確立	146
ユーザ数の上限	146
サポートされるディレクトリ サーバ	146
ディレクトリ ベースの DN の決定	147
不明なユーザの処理	148
アイデンティティ ポリシーの設定	149
ディレクトリ サーバの設定	150
アクティブ認証キャプティブ ポータルの設定	151
アイデンティティ ルールの設定	153
トランスペアレント ユーザ認証のイネーブル化	157
トランスペアレント認証の要件	158
トランスペアレント認証用の Internet Explorer の設定	158
トランスペアレント認証用の Firefox の設定	160
アイデンティティ ポリシーのモニタリング	161
アクセス コントロール	163
アクセス コントロールの概要	163
アクセス コントロール ルールとデフォルト アクション	163
アプリケーション フィルタリング	164
URL フィルタリング	165
レピュテーションベースの URL フィルタリング	165
手動 URL フィルタリング	166
HTTPS トラフィックのフィルタリング	167
Web サイトをブロックしたときのユーザへの表示	167
侵入、ファイル、マルウェアのインスペクション	168
NAT とアクセス ルール	169
アクセス コントロール ポリシーの設定	169
デフォルト アクションの設定	170
アクセス コントロール ルールの設定	171
送信元/宛先条件	173

アプリケーション条件	175
URL の条件	177
ユーザの条件	178
侵入ポリシーの設定	180
ファイル ポリシーの設定	180
ロギングの設定	182
アクセス コントロール ポリシーのモニタリング	184
アクセス コントロールの制限事項	186
アプリケーション コントロールの制約	186
ユーザまたはグループ コントロールの制約	187
URL フィルタリングの制約事項	187
ネットワーク アドレス変換 (NAT)	189
NAT を使用する理由	189
NAT の基本	190
NAT の用語	190
NAT タイプ	191
ルーテッド モードの NAT	192
自動 NAT と 手動 NAT	192
自動 NAT	193
手動 NAT	193
自動 NAT および手動 NAT の比較	193
NAT ルールの順序	194
NAT インターフェイス	196
NAT のルーティングの設定	197
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	197
一意のネットワーク上のアドレス	197
実際のアドレスと同じアドレス (アイデンティティ NAT)	197
NAT のガイドライン	198
インターフェイスのガイドライン	198
IPv6 NAT のガイドライン	198
IPv6 NAT の推奨事項	199
インスペクション対象プロトコルに対する NAT サポート	199

NAT のその他のガイドライン	201
NAT の設定	203
ダイナミック NAT	204
ダイナミック NAT について	204
ダイナミック NAT の欠点と利点	205
ダイナミック自動 NAT の設定	206
ダイナミック手動 NAT の設定	207
ダイナミック PAT	210
ダイナミック PAT について	210
ダイナミック PAT の欠点と利点	211
ダイナミック自動 PAT の設定	211
ダイナミック手動 PAT の設定	213
スタティック NAT	216
スタティック NAT について	216
ポート変換を設定したスタティック NAT	217
1 対多のスタティック NAT	218
他のマッピング シナリオ (非推奨)	219
スタティック自動 NAT の設定	221
スタティック手動 NAT の設定	223
アイデンティティ NAT	227
アイデンティティ自動 NAT の設定	227
アイデンティティ手動 NAT の設定	229
Firepower Threat Defense の NAT ルールのプロパティ	232
自動 NAT のパケット変換プロパティ	233
手動 NAT のパケット変換プロパティ	235
高度な NAT のプロパティ	237
IPv6 ネットワークの変換	238
NAT64/46 : IPv6 アドレスから IPv4 への変換	239
NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット	239
NAT66 : IPv6 アドレスを別の IPv6 アドレスに変換	244
NAT66 の例 : ネットワーク間のスタティック変換	245
NAT66 の例 : 簡単な IPv6 インターフェイス PAT	247

NAT のモニタリング	251
NAT の例	251
内部 Web サーバへのアクセスの提供 (スタティック自動 NAT)	251
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)	254
宛先に応じて異なる変換 (ダイナミック手動 PAT)	261
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)	268
NAT による DNS クエリおよび応答のリライト	274
DNS 64 応答修正	275
DNS 応答修正 : Outside 上の DNS サーバ	281
DNS 応答修正 : ホスト ネットワーク上の DNS サーバ	285
バーチャル プライベート ネットワーク (VPN)	289
サイト間 VPN	291
VPN の基本	291
インターネット キー エクスチェンジ (IKE)	292
VPN 接続の安全性を確保する方法	293
使用する暗号化アルゴリズムの決定	293
使用するハッシュアルゴリズムの決定	294
使用する Diffie-Hellman 係数グループの決定	295
VPN トポロジ	296
サイト間 VPN の管理	297
サイト間 VPN 接続の設定	298
グローバル IKE ポリシーの設定	300
IKEv1 ポリシーの設定	302
IKEv2 ポリシーの設定	303
IPsec プロポーザルの設定	305
IKEv1 の IPsec プロポーザルの設定	306
IKEv2 の IPsec プロポーザルの設定	307
NAT からのサイト間 VPN トラフィックの除外	308
サイト間 VPN のモニタリング	314
システム管理	317
システム設定	319

管理アクセス リストの設定	319
診断ロギングの設定	321
重大度	322
DHCP サーバの設定	322
DNS の設定	324
管理インターフェイスの設定	325
デバイスのホスト名の設定	327
Network Time Protocol (NTP) の設定	327
Cisco Collective Security Intelligence (CSI) の URL フィルタリングの設定の設定	328
クラウド管理の設定	329
システム管理	331
ソフトウェア アップデートのインストール	331
システム データベースの更新	331
システム データベースの更新の概要	331
システム データベースの更新	333
FirePOWER Threat Defenseソフトウェアのアップグレード	334
デバイスの再イメージ化	335
システムのバックアップと復元	336
即時のシステム バックアップ	336
スケジュールされた時刻のシステム バックアップ	337
定期バックアップ スケジュールの設定	338
バックアップの復元	339
バックアップ ファイルの管理	339
システムの再起動	340
システムのトラブルシューティング	341
接続テストのためのアドレスの ping	341
ホストまでのルートの追跡	343
NTP のトラブルシューティング	345
CPU とメモリ使用率の分析	347
ログの表示	347
トラブルシューティング ファイルの作成	349

一般的でない管理タスク 349

- ローカル管理とリモート管理の切り替え 349
- ファイアウォールモードの変更 352
- 設定のリセット 355



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。

- [このガイドの目的, 1 ページ](#)
- [Firepower Device Manager/Firepower Threat Defense6.2 の新機能, 2 ページ](#)
- [システムへのログイン, 6 ページ](#)
- [システムの設定, 11 ページ](#)
- [設定の基本, 31 ページ](#)

このガイドの目的

このガイドは、FirePOWER Threat Defenseデバイスに組み込まれている Firepower デバイスマネージャの Web ベースの設定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 デバイスマネージャでは、小規模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を設定できます。特に、多数の FirePOWER Threat Defense デバイスを含む大規模ネットワークを制御するための強力なマルチデバイス マネージャの使用を避けたい、単一のデバイスまたは少数のデバイスを含むネットワーク向けに設計されています。

多数のデバイスを管理する場合、または FirePOWER Threat Defense が許容するより複雑な機能と設定を使用する場合は、統合された Firepower デバイスマネージャではなく、Firepower Management Center を使用してデバイスを設定してください。

Firepower デバイスマネージャは次のデバイスで使用できます。

表 1: Firepower デバイスマネージャがサポートするモデル

デバイス モデル	Firepower Threat Defense ソフトウェアの最小バージョン
ASA 5506-X、5506H-X、5506W-X、5508-X、5516-X	6.1

デバイス モデル	Firepower Threat Defense ソフトウェアの最小バージョン
ASA 5512-X、5515-X、5525-X、5545-X、5555-X	6.1

Firepower Device Manager/Firepower Threat Defense6.2 の新機能

次の表に、Firepower Device Manager を使用して設定した場合に Firepower Threat Defense6.2で利用できる新機能を示します。

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

機能	説明
<p>Firepower Threat Defenseのデフォルト設定の変更</p>	<p>新規デバイスまたは再イメージ化されたデバイスの場合、デフォルト設定には、次を含む重要な変更が含まれています。</p> <ul style="list-style-type: none"> • (ASA 5506-X、5506W-X、5506H-X)。最初のデータインターフェイス、およびASA 5506W-XのWi-Fiインターフェイスを除き、これらのデバイスモデルのその他すべてのデータインターフェイスは「内部」ブリッジグループ内に構築されて、有効になっています。内部ブリッジグループにはDHCPサーバがあります。エンドポイントまたはスイッチをブリッジされた任意のインターフェイスに接続し、エンドポイントで192.168.1.0/24ネットワークのアドレスを入手できます。 • 内部インターフェイスのIPアドレスは192.168.1.1になっており、DHCPサーバはアドレスプール(192.168.1.5～192.168.1.254)のインターフェイスで定義されています。 • HTTPSアクセスは内部インターフェイスで有効になっているため、デフォルトアドレス(192.168.1.1)で内部インターフェイスを介してFirepower Device Managerを開くことができます。ASA 5506-Xモデルの場合、任意の内部ブリッジグループメンバーインターフェイスを介して開くことができます。 • 管理ポートは、192.168.45.0/24ネットワークのDHCPサーバをホストします。ワークステーションを管理ポートに直接接続し、IPアドレスを取得して、Firepower Device Managerを開き、デバイスを設定できます。 • OpenDNSパブリックDNSサーバは、管理インターフェイス用のデフォルトのDNSサーバになっています。以前は、デフォルトのDNSサーバはありませんでした。デバイスの設定時に別のDNSサーバを設定できます。 • 管理IPアドレスのデフォルトゲートウェイは、データインターフェイスをインターネットにルーティングするために使用されます。そのため、管理用物理インターフェイスをネットワークに有線接続する必要はありません。

機能	説明
管理インターフェイスとアクセスの変更	<p>管理アドレス、およびFirepower Device Managerへのアクセス方法に対する複数の変更は次のように機能します。</p> <ul style="list-style-type: none"> • HTTPS (Firepower Device Managerの場合) 接続とSSH (CLIの場合) 接続に対してデータインターフェイスを開くことができるようになりました。デバイスを管理するための、別の管理ネットワークは不要で、管理/診断用物理ポートを内部ネットワークに接続する必要もありません。[デバイス (Device)]>[システム設定 (System Settings)]>[管理アクセスリスト (Management Access List)]を選択します。 • システムは、外部インターフェイスのゲートウェイを介してシステムデータベースの更新を取得できます。管理インターフェイスまたはネットワークからインターネットまでの明示的なルートを設定する必要はありません。デフォルトでは、データインターフェイスを経由する内部ルートが使用されます。ただし、別の管理ネットワークを使用したい場合は特定のゲートウェイを設定できます。[デバイス (Device)]>[システム設定 (System Settings)]>[管理インターフェイス (Management Interface)]を選択します。 • Firepower Device Manager を使用して管理インターフェイスを設定し、DHCPから管理インターフェイスのIPアドレスを入手できます。[デバイス (Device)]>[システム設定 (System Settings)]>[管理インターフェイス (Management Interface)]を選択します。 • スタティックアドレスを設定する場合、管理アドレス上にDHCP サーバを設定できます。[デバイス (Device)]>[システム設定 (System Settings)]>[管理インターフェイス (Management Interface)]を選択します。

機能	説明
<p>さまざまなユーザインターフェイスの変更</p>	<p>Firepower Device Manager ユーザインターフェイスの主な変更点は次のとおりです。</p> <ul style="list-style-type: none"> • [デバイス (Device)]のメインメニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは [デバイス ダッシュボード (Device Dashboard)]ではなく、[デバイス サマリ (Device Summary)]と呼ばれていました。 • デバイスの初期設定時に代替の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。 • [デバイス (Device)]>[システム設定 (System Settings)]>[クラウド設定 (Cloud Preferences)]は [デバイス (Device)]>[システム設定 (System Settings)]>[URL フィルタリング設定 (URL Filtering Preferences)]に変わりました。 • [システム設定 (System Settings)]>[DHCP サーバ (DHCP Server)]ページは2つのタブで編成されており、グローバルパラメータから切り離された DHCP サーバのテーブルが含まれています。
<p>サイト間 VPN の接続</p>	<p>事前共有キーを使用してサイト間バーチャルプライベートネットワーク (VPN) の接続を設定できます。IKEv1 接続と IKEv2 接続を設定できます。</p>

機能	説明
Integrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング) のサポート	<p>Integrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング) は、ブリッジグループとルーテッドインターフェイス間のルーティング機能を提供します。ブリッジグループは、Firepower Threat Defenseデバイスがルーティングの代わりにブリッジングするインターフェイスのグループです。Firepower Threat Defenseデバイスは、Firepower Threat Defense デバイスがファイアウォールとして機能し続けるという点において真のブリッジではなく、インターフェイス間のアクセスコントロールは管理され、通常のすべてのファイアウォールチェックが実施されます。</p> <p>この機能を使用すると、ブリッジグループを設定し、ブリッジグループ間、およびブリッジグループとルーテッドインターフェイス間のルートを設定できます。ブリッジグループは、ブリッジグループのゲートウェイとして機能するために、ブリッジ仮想インターフェイス (BVI) を使用してルーティングに参加します。Firepower Threat Defenseデバイスにブリッジグループに割り当てる追加のインターフェイスがある場合、Integrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング) では、外部のレイヤ 2 スイッチを使用するための代替案が提供されます。BVI は名前付きインターフェイスにでき、一部の機能 (ブリッジグループメンバーインターフェイスにその他の機能を設定する DHCP サーバ、NAT およびアクセスコントロールルールなど) にはメンバーインターフェイスから切り離して参加できます。</p> <p>[デバイス (Device)]>[インターフェイス (Interfaces)] を選択して、ブリッジグループを設定します。</p>

システムへのログイン

FirePOWER Threat Defenseデバイスへのインターフェイスは2つあります。

Firepower デバイス マネージャ Web インターフェイス

Firepower デバイス マネージャが Web ブラウザ内で実行されます。システムを設定、管理およびモニタするには、このインターフェイスを使用します。

コマンドライン インターフェイス (CLI、コンソール)

トラブルシューティングには、CLI を使用します。Firepower デバイス マネージャの代わりに、初期設定で使用することもできます。

以降のトピックでは、これらのインターフェイスにログインして、ユーザアカウントを管理する方法を説明します。

Firepower Device Manager へのログイン

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

最新バージョンの Firefox、Chrome、Safari、または Internet Explorer を使用してください。

はじめる前に

admin ユーザ名を使用することによってのみ Firepower Device Manager にログインできます。Firepower Device Manager アクセスの追加ユーザは作成できません。

手順

ステップ 1 ブラウザを使用して、システムのホームページ (<https://ftd.example.com> など) を開きます。次のいずれのアドレスも使用できます。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上の 192.168.45.45 です。
- HTTPS アクセスのために開いたデータ インターフェイスのアドレス。デフォルトでは、「内部」インターフェイスが HTTPS アクセスを許可するため、デフォルトの内部アドレスである 192.168.1.1 に接続できます。内部インターフェイスがブリッジグループであるデバイスモデルでは、任意のブリッジグループ メンバー インターフェイスを介してこのアドレスに接続できます。

ヒント ブラウザがサーバ証明書を認識するように設定されていない場合、信頼されてい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、または信頼されたルート証明書ストアのものを受け入れます。

ステップ 2 admin ユーザ名およびパスワードを入力して、[ログイン (Login)] をクリックします。デフォルトの admin パスワードは Admin123 です。

セッションは20分間操作しないと期限切れになり、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 アイコンのドロップダウン メニューから [ログアウト (Log Out)] を選択するとログアウトできます。



コマンドラインインターフェイス (CLI) へのログイン

システムの設定および基本的なシステムのトラブルシューティングを行うには、コマンドラインインターフェイス (CLI) を使用します。CLIセッションを通じて、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。

- 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端末エミュレータを使用しているコンソールに、デバイスに付属のコンソールケーブルを使用して PC を接続します。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。
- SSH クライアントを使用して、管理 IP アドレスへの接続を確立します。SSH 接続のインターフェイスを開く場合は、データインターフェイスのアドレスに接続することもできます ([管理アクセス リストの設定, \(319 ページ\)](#) を参照)。デフォルトでは、データインターフェイスへの SSH アクセスは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) 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。

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。使用方法の詳細については、http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html で『*Command Reference for Firepower Threat Defense*』を参照してください。



(注) **configure user add** コマンドを使用して、CLI にログイン可能なユーザ アカウントを作成できます。ただし、これらのユーザは、CLI のみにログイン可能で、Firepower デバイスマネージャ Web インターフェイスにはログインできません。

パスワードの変更

定期的にパスワードを変更する必要があります。以下の手順では、FirePOWER Device Manager へのログイン中にパスワードを変更する方法について説明します。



(注) CLI を使用してログインしている場合にパスワードを変更するには、**configure password** コマンドを使用します。別の CLI ユーザに対するパスワードを変更するには、**configure user passwordusername** コマンドを使用します。

手順

ステップ 1 メニュー右上のユーザ 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 プロファイル設定の設定

ユーザ インターフェイスの設定を設定し、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 アイコン ドロップダウンリストから [プロフィール (Profile)]を選択します。



- ステップ 2 [プロフィール (Profile)]タブで、次の項目を設定し、[保存 (Save)]をクリックします。
 - [タスクのスケジューリングのタイムゾーン (Time Zone for Scheduling Tasks)] : バックアップや更新などのタスクをスケジュールするために使用するタイムゾーンを選択します。別のゾーンを設定した場合、ダッシュボードとイベント用にはブラウザのタイムゾーンが使用されます。
 - [色のテーマ (Color Theme)] : ユーザ インターフェイスに使用する色の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。
-

Firepower Threat Defenseの CLI ユーザ アカウントの作成

Firepower Threat Defense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 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` コマンドを使用して Firepower Threat Defense 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 addusername {basic | config}
次の権限レベルを持つユーザを定義できます。

- **config** : ユーザに構成への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) **configure password** コマンドを使用して自分のパスワードを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、有効期限が近づく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してもらいます。
- **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。アカウントをロック解除するには、**configure user unlock** コマンドを使用します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

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

パスワードの最小長を 1~127 までで設定します。

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

パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用している場合は、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する必要があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

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

ユーザアカウントの権限を変更します。

- **configure user delete** *username*

指定したアカウントを削除します。

- **configure user disable** *username*

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

- **configure user enable** *username*

指定したアカウントを有効にします。

- **configure user password** *username*

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

- **configure user unlock** *username*

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

システムの設定

ネットワークでシステムが正しく動作するには、初期設定を完了する必要があります。導入を適切に完了するには、ケーブルを正しく接続し、デバイスをネットワークに追加してインターネット

トや上流に位置するほかのルータに接続するために必要なアドレスを設定します。次の手順では、このプロセスについて説明します。

はじめる前に

初期設定を開始する前に、デバイスにはデフォルト設定が含まれています。詳細は、[初期セットアップ前のデフォルト設定](#)、(25 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](#)、(12 ページ)
 - ステップ 2 [初期設定の完了](#)、(16 ページ)
完了後の設定の詳細については、[初期セットアップ後の設定](#)、(27 ページ) を参照してください。
 - ステップ 3 [ワイヤレス アクセス ポイント \(ASA 5506W-X\) の設定](#)、(21 ページ)
-

インターフェイスの接続

デフォルト設定では、内部および外部ネットワークにそれぞれ特定のインターフェイスが使用されることが前提となっています。この前提に基づいてネットワーク ケーブルで各インターフェイスを接続すると、初期設定の実行が容易になります。

のデフォルト設定は、ワークステーションを内部インターフェイスに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となっているデバイスモデルでは、任意のメンバーインターフェイスに接続できます。また、ワークステーションを管理ポートに直接接続することもできます。適切なネットワーク上のアドレスを取得するには、DHCP を使用します。各インターフェイスはさまざまなネットワークにつながっているため、内部インターフェイスと管理ポートとを同一ネットワークに接続しないように注意が必要です。

また、アクティブな DHCP サーバが設置されたネットワークには、内部インターフェイスまたは管理インターフェイスを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 サーバを使用するには、ワークステーションを管理ポートに直接接続し、初期設定を実行してから、不要な DHCP サーバを無効にします。これで、デバイスをネットワークに接続できる状態になります。

以下の各トピックでは、内部インターフェイスを使用してデバイスを設定する場合に、このようなトポロジにおいてシステムをケーブル接続する方法について説明します。

ASA 5506-X、5506W-X、5506H-X のケーブル接続

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

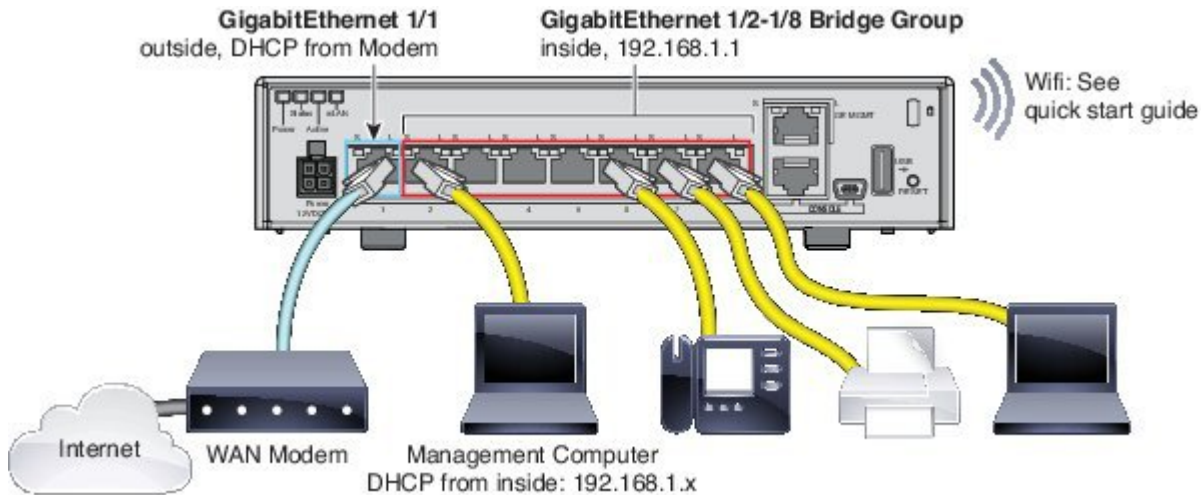
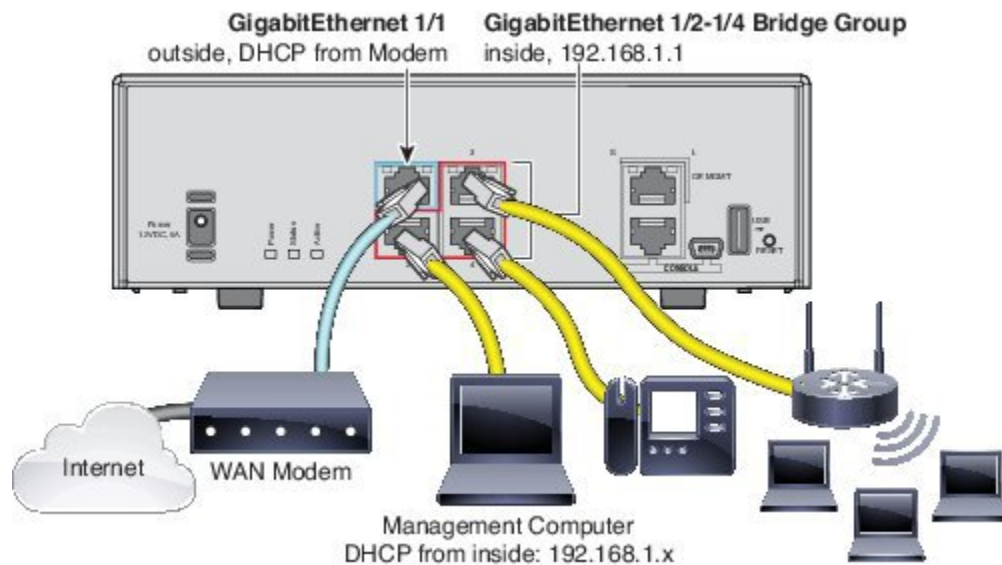


図 2 : ASA 5506H-X



- GigabitEthernet 1/1 は、ISP/WAN モデムまたは他の外部デバイスに接続します。デフォルトでは、IP アドレスは DHCP を使用して取得されますが、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 (または内部ブリッジグループの他のメンバーポート) を、デバイスの設定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

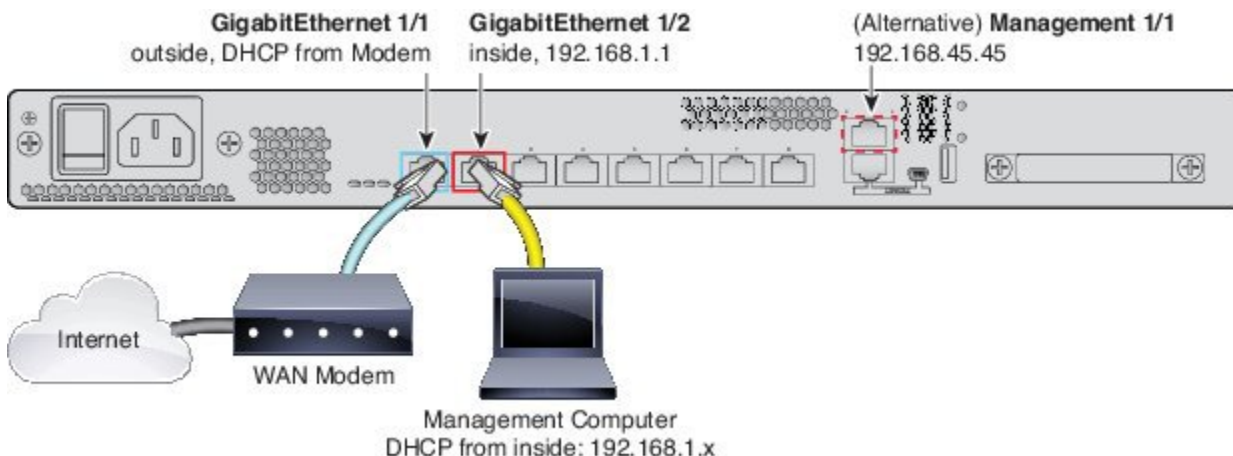
うに、ワークステーションを設定します。ワークステーションは、192.168.1.0/24 ネットワーク上のアドレスを取得します。



(注) 管理ワークステーションの接続方法には、この他にもいくつかのオプションがあります。管理ワークステーションを、管理ポートに直接接続することもできます。この場合、ワークステーションはDHCPを経由して、192.168.45.0/24 ネットワーク上のアドレスを取得します。もう1つの方法は、ワークステーションはスイッチに接続したままで、このスイッチを、GigabitEthernet 1/2 などのいずれかの内部ポートに接続します。ただし、スイッチのネットワーク上に、DHCPサーバを実行するデバイスが他に存在しないことを確認する必要があります。存在している場合、内部ブリッジグループ 192.168.1.1 で実行される DHCP サーバとの競合が生じます。

- 必要に応じて、内部ブリッジグループ内の他のポートに、他のエンドポイントまたはスイッチを接続します。エンドポイントの追加は、最初のデバイスのセットアップが完了してから行うようにしてください。スイッチを追加する場合は、これらのネットワーク上で他のDHCPサーバが実行されていないことを確認します。実行されている場合、内部ブリッジグループで実行される DHCP サーバとの競合が生じます。

ASA 5508-X および 5516-X のケーブル接続

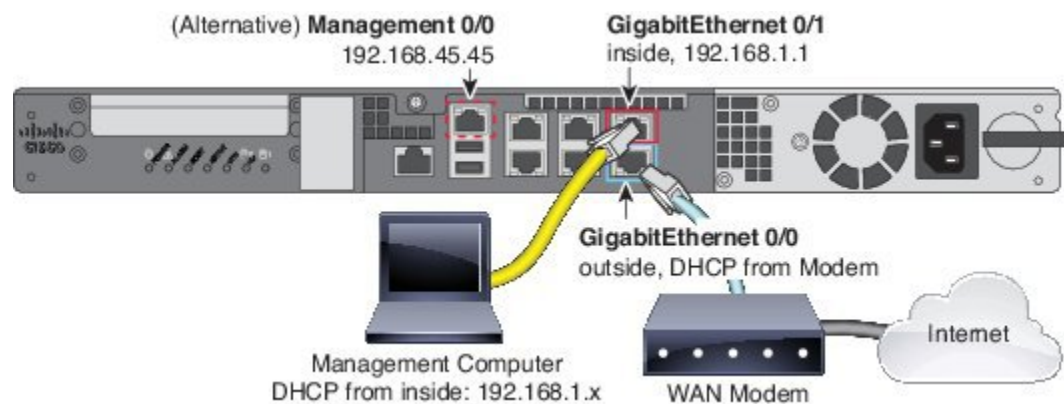


- GigabitEthernet 1/1 は、ISP/WAN モデムまたは他の外部デバイスに接続します。デフォルトでは、IP アドレスは DHCP を使用して取得されますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 1/2 を、デバイスの設定に使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するように、ワークステーションを設定します。ワークステーションは、192.168.1.0/24 ネットワーク上のアドレスを取得します。



- (注) 管理ワークステーションの接続方法には、この他にもいくつかのオプションがあります。管理ワークステーションを、管理ポートに直接接続することもできます。この場合、ワークステーションはDHCPを経由して、192.168.45.0/24 ネットワーク上のアドレスを取得します。もう1つの方法は、ワークステーションはスイッチに接続したままで、このスイッチを GigabitEthernet 1/2 に接続します。ただし、スイッチのネットワーク上に、DHCPサーバを実行するデバイスが他に存在しないことを確認する必要があります。存在している場合、内部インターフェイス 192.168.1.1 で実行される DHCP サーバとの競合が生じます。

ASA 5512-X、5515-X、5525-X、5545-X、5555-X のケーブル接続



- GigabitEthernet 0/0 は、ISP/WAN モデムまたは他の外部デバイスに接続します。デフォルトでは、IP アドレスは DHCP を使用して取得されますが、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、デバイスの設定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 ネットワーク上のアドレスを取得します。



- (注) 管理ワークステーションの接続方法には、この他にもいくつかのオプションがあります。管理ワークステーションを、管理ポートに直接接続することもできます。この場合、ワークステーションはDHCPを経由して、192.168.45.0/24ネットワーク上のアドレスを取得します。もう1つの方法は、ワークステーションはスイッチに接続したままで、このスイッチをGigabitEthernet 0/1に接続します。ただし、スイッチのネットワーク上に、DHCPサーバを実行するデバイスが他に存在しないことを確認する必要があります。存在している場合、内部インターフェイス 192.168.1.1 で実行されるDHCPサーバとの競合が生じます。

初期設定の完了

FirePOWER Device Manager に最初にログインすると、システムの初期設定を行うためのデバイスセットアップウィザードが開始されます。

はじめる前に

データインターフェイスが、ケーブルモデムやルータなどのゲートウェイデバイスに接続されていることを確認してください。エッジでの展開では、インターネット側のゲートウェイがこれに相当します。データセンターでの展開では、バックボーンルータです。使用するモデルでの、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](#)、[\(12 ページ\)](#) および [初期セットアップ前のデフォルト設定](#)、[\(25 ページ\)](#) を参照）。

次に、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となっているモデルでは、ブリッジグループの任意のメンバーインターフェイス（外部インターフェイス以外の任意のデータポート）に接続できます。または、管理用および診断用の物理インターフェイスに接続できます。

管理用および診断用の物理インターフェイスは、ネットワークに接続されている必要はありません。デフォルトでは、ライセンス設定、およびデータベースなどの更新は、インターネットに接続されているデータインターフェイス（通常は外部インターフェイス）から取得されます。そうではなく、個別の管理ネットワークを使用するには、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、個別の管理ゲートウェイを設定します。

手順

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

a) CLI から初期設定を完了していない場合は、FirePOWER Device Manager (<https://ip-address>) を開きます。アドレスは、次のいずれかとなります。

- 内部インターフェイスに接続しているか、またはデフォルトで内部ブリッジグループを持つモデルで、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> となります。

- 管理用の物理インターフェイスに接続している場合は、<https://192.168.45.45> となります。

b) ユーザ名 **admin** およびパスワード **Admin123** でログインします。

ステップ 2 これがシステムへの最初のログインであり、CLI によるセットアップ ウィザードも未実行の場合は、エンドユーザ ライセンス契約を読んで同意し、管理パスワードを変更するように促すメッセージが表示されます。

続行するには、この手順を実行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以下のオプションを設定し、[次へ (Next)] をクリックします。

注意 ここで[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。インターフェイスは「outside」という名前で、「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。内部インターフェイスと同じサブネットにある外部インターフェイスの IP アドレスを設定してしまい、内部アドレスの FirePOWER Device Manager に接続している状態になると、内部インターフェイスのアドレスは削除されるため、[次へ (Next)] をクリックした時点でウィザードが機能停止します。回復方法については、[外部サブネットが内部サブネットと競合する \(セットアップ ウィザードがステップ 1 でハングする\) 場合の解決策](#)、(19 ページ) を参照してください。

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の IPv4 アドレス。DHCP を使用することも、スタティックな IP アドレス、サブネット マスク、およびゲートウェイを手動で入力することもできます。IPv4 アドレスを設定しない場合は、[オフ (Off)] を選択します。スタティックに設定する場合も、DHCP を使用する場合も、デフォルトの内部アドレスと同じサブネットにある IP アドレスを設定しないようにしてください ([初期セットアップ前のデフォルト設定](#)、(25 ページ) を参照)。
- [IPv6 の設定 (Configure IPv6)]: 外部インターフェイスの IPv6 アドレス。DHCP を使用することも、スタティックな IP アドレス、プレフィックス、およびゲートウェイを手動で入力することもできます。IPv6 アドレスを設定しない場合は、[オフ (Off)] を選択します。

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に対する DNS サーバ。名前解決を行う DNS サーバのアドレスを 1 つ以上入力します。デフォルトでは、OpenDNS のパブリック DNS サーバです。各フィールドの編集後にデフォルトに戻すには、[OpenDNS を使用 (Use OpenDNS)] をクリックすると、適切な IP アドレスがフィールドに読み込まれます。
- [ファイアウォールのホスト名 (Firewall Hostname)]: システムの管理アドレスのホスト名。

ステップ 4 システム時刻を設定して、[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 サーバの使用を選択するか、または任意の NTP サーバのアドレスを手動で入力します。バックアップ用に、複数のサーバを追加できます。

ステップ 5 システムのスマート ライセンスを設定します。

システムに必要なライセンスを取得および適用するには、スマートライセンスアカウントが必要です。最初に、90 日間の評価ライセンスを使用してから、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、Smart Software Manager のアカウントにログインするリンクをクリックして、新しいトークンを作成し、このトークンを編集ボックスにコピーします。

評価ライセンスを使用するには、[登録せず、90 日間の評価期間を開始する (Start 90 day evaluation period without registration)]を選択します。後からデバイスを登録し、スマートライセンスを取得するには、デバイス、[スマート ライセンス (Smart Licenses)]グループ内の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。

次の作業

- カテゴリ ベースの URL フィルタリング、侵入検知、マルウェア防止など、オプション ライセンスで実現する機能を使用するには、必要なライセンスを有効化します。[オプションライセンスの有効化と無効化](#)、(76 ページ) を参照してください。
- 新しいシステムの場合、デフォルトで内部ブリッジグループが設定されているデバイス モデル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すぐに使用できます。各インターフェイスには、エンドポイントを直接接続できます。単一のデフォルト物理インターフェイスを備えたモデルの場合は、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、インターフェイスを設定できます。ブリッジグループのメンバーインターフェイスでは、各インターフェイスをブリッジグループから削除し、一意のネットワークを追加で設定することもできます。インターフェイスの設定の詳細については、[サブネットの追加方法](#)、(62 ページ) および [インターフェイスの設定](#)、(121 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のメンバー インターフェイス経由でデバイスを管理する場合に、内部インターフェイスから CLI セッションを開くには、内部インターフェイスまたはブリッジグループを開いて SSH 接続を開始します。[管理アクセスリストの設定](#)、(319 ページ) を参照してください。
- さまざまな使用例を参照することで、製品の使用方法を学習できます。[FirePOWER Threat Defenseの使用例](#)、(37 ページ) を参照してください。

外部サブネットが内部サブネットと競合する（セットアップウィザードがステップ1でハングする）場合の解決策

内部インターフェイスを介して Firepower Device Manager に接続した場合、ステップ1で外部インターフェイスを設定して [次へ (Next)] クリックすると、セットアップウィザードがハングする場合があります。通常、このステップは完了に時間がかかるため、ハングとはその状態が10分を超えて継続する場合を指します。ブラウザを更新すると、Firepower Device Manager との接続が切断されたことがわかります（管理IPアドレスから接続した場合、セットアップウィザードはハングしませんが、次の症状で説明する問題が存在する場合があります）。

この問題の最も可能性の高い原因は、内部インターフェイスと外部インターフェイスの両方に同じサブネットのアドレスが割り当てられているため、内部インターフェイスの設定が失われたことです。

デフォルト設定には、内部インターフェイスのスタティックアドレス、およびDHCPサーバが含まれています。これにより、セットアップウィザードが完了した直後からデバイスは正しく動作し、トラフィックを受け渡し、接続されているワークステーションをサポートできます。

しかし、デフォルトの内部アドレスが正しく機能するのは、同じサブネットに属するアドレスを外部インターフェイスに設定しない場合に限りです。これには、DHCP 経由で外部アドレスにアドレスを提供する ISP デバイスに接続する状況が含まれます。一部の ISP は、FirePOWER Threat Defenseが内部アドレス用に使用するサブネットと同じ192.168.1.0/24サブネットを（外部インターフェイスに接続する）内部インターフェイス用に使用します。

この問題を解決するには、内部インターフェイスのIPアドレスを変更する必要があります。



(注)

このトピックでは、ハードウェアモデルとそのデフォルトについて説明します。仮想モデルでは、デフォルトの内部IPアドレスは異なっており、管理IPアドレスと同じサブネットに属しています。その場合でも内部と外部のサブネット競合が発生する可能性はありますが、その確率はより低くなります。

内部と外部のサブネット競合の症状

ここでは、内部インターフェイスと外部インターフェイスのアドレスが同じサブネットに属する場合の症状について説明します。


- デバイスのセットアップウィザードの実行中、ステップ1で [次へ (Next)] をクリックするとウィザードがハングします。通常、このステップは完了に時間がかかるため、ハングとはその状態が10分を超えて継続する場合を指します。
- コンソールポートに接続されている場合、CLIで次のメッセージが表示されます。このメッセージは、Firepower Device Manager から（以降で変更することなく）設定を展開しようとする場合にも表示されます。

```
ERROR: Failed to apply IP address to interface GigabitEthernet1/1,  
as the network overlaps with interface GigabitEthernet1/2.  
Two interfaces cannot be in the same subnet.
```

外部サブネットが内部サブネットと競合する（セットアップウィザードがステップ1でハングする）場合の解決策

- 設定を終了すると、接続グラフィックに、外部サービス（ゲートウェイ、DNSサーバ、NTPサーバ、スマートライセンスなど）との接続が存在しないことが示されます。また、メニューの [導入 (Deploy)] アイコンに、導入が必要であることが示されます。
- CLIで、**show running-config** コマンドと **show startup-config** コマンドを使用して確認すると、内部インターフェイスと外部インターフェイスの **interface** および **dhcp** 設定が矛盾しています。

手順

- ステップ 1** デバイスの設定中に内部インターフェイスに接続されていた場合は、設定を完了します。
- a) 管理ポートに接続して、デバイスに再接続します。必要に応じて、管理ネットワーク (192.168.45.0/24) で新しいアドレスを取得するためにワークステーションの DHCP アドレスを解放して更新します。必要に応じて、192.168.45.1 ~ 192.168.45.44 の範囲でワークステーションのスタティックアドレスを設定します。
 - b) <https://192.168.45.45> で Firepower Device Manager を開きます。
 - c) 90 日間の評価ライセンスの開始を確認するプロンプトが表示されます。このオプションを選択し、[確認 (Confirm)] をクリックします。
 - d) [デバイス (Device)] > [システム設定 (System Settings)] > [NTP] を選択し、NTP サーバを設定して、[保存 (Save)] をクリックします。デフォルトのサーバが要件に適合する場合は、このステップをスキップできます。
 - e) メニューの右上にあるユーザアイコン ドロップダウンリストから [プロファイル (Profile)] を選択し、デバイスのタイムゾーンを選択して、[保存 (Save)] をクリックします。
- 
- f) 評価ライセンスを使用しない場合は、[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、[登録の要求 (Request Register)] をクリックして、指示に従ってデバイスを登録します。[デバイスの登録, \(75 ページ\)](#) を参照してください。（この時点で必要なオプションのライセンスを有効にすることもできます）。
- ステップ 2** 内部インターフェイスから DHCP サーバを削除します。
- a) [デバイス (Device)] > [システム設定 (System Settings)] > [DHCP サーバ (DHCP Server)] を選択します。
 - b) [DHCP サーバ (DHCP Server)] タブをクリックします。
 - c) 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、削除アイコン (🗑️) をクリックします。
- ステップ 3** 内部インターフェイスのアドレスを変更します。
- a) [デバイス (Device)] を選択します。
 - b) インターフェイス グループで、有効化されているインターフェイスの数を示すリンク ([3 個有効 (3 Enabled)] など) をクリックします。
 - c) 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、編集アイコン (✎) をクリックします。

- d) [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。また、内部ネットワークですでに DHCP サーバが実行されている場合は、DHCP を使用してアドレスを取得することもできます。
- e) [OK]をクリックします。

ステップ 4

- (オプション) 内部アドレスの DHCP サーバを設定します。
内部インターフェイスのスタティック アドレスを設定した場合は、内部ネットワークに接続するワークステーションにアドレスを提供するために DHCP サーバを設定できます。これは一般的な設定です。
- a) [デバイス (Device)]>[システム設定 (System Settings)]>[DHCP サーバ (DHCP Server)]を選択します。
 - b) [DHCP サーバ (DHCP Server)]タブをクリックします。
 - c) [+]をクリックします。
 - d) サーバを有効化するオプションを選択し、内部インターフェイスを選択します。
 - e) アドレス プールについては、内部アドレスと同じサブネットに属する範囲を入力します。たとえば、内部アドレスが 192.168.2.1/24 の場合は、192.168.2.5 ~ 192.168.2.254 を使用できません。ネットワーク上のノードにスタティックに割り当てられているアドレスを含めないでください。必要に応じてスタティックアドレスを割り当てることができるよう、数個のアドレスをプールから除外することを検討してください。
 - f) [OK]をクリックします。

ステップ 5

メニューの [導入 (Deploy)]ボタンをクリックします。



ステップ 6

[今すぐ導入 (Deploy Now)]をクリックします。
導入が完了すると、外部サービスの接続グラフィックが緑を示します。

ワイヤレス アクセス ポイント (ASA 5506W-X) の設定

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

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

次の手順では、アクセスポイントを設定する方法について説明します。手順は、デバイス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。代わりに手動でデバイスを設定した場合は、設定に基づいて手順を調整する必要があります。

詳細については、次のマニュアルを参照してください。

- ワイヤレス LAN コントローラの使用法の詳細については、[Cisco Wireless LAN Controller ソフトウェアのマニュアル](#)を参照してください。
- ワイヤレスアクセスポイントのハードウェアおよびソフトウェアの詳細については、[Cisco Aironet 700 シリーズのマニュアル](#)を参照してください。

はじめる前に

アクセスポイントに到達できないときに、Firepower Threat Defenseデバイスは推奨される設定であり、他にネットワーク問題は見つからない場合、アクセスポイントをデフォルト設定に復元することができます。Firepower Threat Defense CLI にアクセスする必要があります（コンソールポートに接続するか、またはSSHアクセスを設定します）。Firepower Threat Defense CLI から、次のコマンドを入力します。

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

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

アクセスポイントをさらにトラブルシューティングする必要がある場合は、**session wlan console** コマンドを使用してアクセスポイント CLI に接続します。

手順

ステップ 1 ワイヤレスインターフェイスの GigabitEthernet 1/9 を設定し、有効にします。

- デバイスをクリックし、[インターフェイス (Interfaces)] グループ内のリンクをクリックして、インターフェイスのリストを開きます。
- GigabitEthernet 1/9 インターフェイスの編集アイコン (🔗) をクリックします。
- 次のオプションを設定します。
 - インターフェイス名 (Interface Name) : インターフェイスの名前を入力します。たとえば、wifi。
 - ステータス (Status) : スライダをクリックして、インターフェイスを有効にします。
 - IPv4アドレス (IPv4 Address) : アドレスタイプに[スタティック (Static)]を選択してから、アドレスとサブネットマスクを入力します。たとえば、192.168.10.1/24 と入力します。
- [保存 (Save)] をクリックします。

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

デバイスセットアップウィザードは、`inside_zone`という名前のセキュリティゾーンに `inside` ブリッジグループのメンバーを配置します。アクセスポイント Web インターフェイスに到達するには、Wi-Fi インターフェイスが同じゾーンに存在する必要があります (デフォルトの `Inside_Inside_Rule` アクセス ルールによって実現可能)。

- a) メニューで [オブジェクト (Objects)] をクリックし、目次から [セキュリティゾーン (Security Zones)] を選択します。
- b) `inside_zone` の編集アイコン (🔗) をクリックします。
- c) [インターフェイス (Interfaces)] の下の [+] をクリックし、`wifi` インターフェイスを選択します。

ステップ 3 `inside_zone` セキュリティゾーン内のインターフェイス間のトラフィックを許可するためのアクセスコントロールルールが存在することを確認します。

デバイスセットアップウィザードは、トラフィックが `inside_zone` から `outside_zone` へ流れるのを許化する、つまり、内部ユーザのインターネットへのアクセスを許可するルールを作成します。

また、内部ホストが相互に到達できるように、トラフィックが `inside_zone` と `inside_zone` の間で流れるのを許可するルールを作成します。

`wifi` インターフェイスを `inside_zone` に追加すると、Wi-Fi ユーザもこれらの両方のルールに含まれ、インターネットと他の内部ユーザに到達できるようになります。

ウィザードを完了していない場合、これらのルールは存在していない可能性があります。デフォルトアクションがすべてのトラフィックのブロックであるため、これらのルールを作成する必要があります。次の手順は、`inside_zone` セキュリティゾーン内のインターフェイス間のトラフィックを有効にするルールを作成する方法を説明しています。

- a) メニューで [ポリシー (Policies)] をクリックします。
- b) [アクセスコントロール (Access Control)] テーブルの上にある [+] をクリックして、ルールを追加します。
- c) 少なくとも次のオプションをルールに設定します。
 - タイトル (Title) : ルールの名前を入力します。たとえば、`Inside_Inside` と入力します。
 - アクション (Action) : [許可 (Allow)] または [信頼 (Trust)] のいずれかを指定します。
 - [送信元/宛先 (Source/Destination)] > [送信元ゾーン (Source Zones)] : `inside_zone` を選択します。
 - [送信元/宛先 (Source/Destination)] > [宛先ゾーン (Destination Zones)] : `inside_zone` を選択します。
- d) [OK] をクリックします。

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

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

- a) デバイスをクリックします。
- b) [システム設定 (System Settings)] > [DHCP サーバ (DHCP Server)] をクリックします。
- c) [DHCP サーバ (DHCP Servers)] タブをクリックします。

- d) DHCP サーバ テーブルの上の [+]をクリックします。
- e) 次の DHCP 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) : スライダをクリックして、DHCP サーバを有効にします。
 - インターフェイス (Interface) : wifi インターフェイスを選択します。
 - アドレス プール (Address Pool) : DHCP クライアントのアドレス プールを入力します。たとえば、ワイヤレス インターフェイスのアドレス例を使用した場合、プールは 192.168.10.2 ~ 192.168.10.254 です。プールは、インターフェイスの IP アドレスと同じサブネット上に存在している必要があります。インターフェイスのアドレスまたはブロードキャスト アドレスを含めることはできません。
- f) [追加 (Add)]、[OK] の順にクリックします。

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



続行する前に展開が終了するまで待機します。

ステップ 6 ワイヤレス アクセス ポイントを設定します。
ワイヤレス アクセス ポイントは、ワイヤレス インターフェイスに定義されている DHCP プールからアドレスを取得します。プール内の最初のアドレスを取得する必要があります。アドレス例を使用した場合、これは 192.168.10.2 です (最初のアドレスが動作しない場合は、プール内の次のアドレスが試行されます)。

- a) 新しいブラウザ ウィンドウを使用して、ワイヤレス アクセス ポイントの IP アドレス、たとえば、<http://192.168.10.2> に移動します。
アクセス ポイント Web インターフェイスが表示されます。

このアドレスを開くには、内部ネットワーク上またはそれをルーティングできるネットワーク上にいる必要があります。
- b) ユーザ名 `cisco` およびパスワード `Cisco` でログインします。
- c) 左側の [簡易設定 (Easy Setup)] > [ネットワーク設定 (Network Configuration)] をクリックします。
- d) [無線設定 (Radio Configuration)] 領域で、[無線 2.4GHz (Radio 2.4GHz)] および [無線 5GHz (Radio 5GHz)] の各セクションに対して、少なくとも次のパラメータを設定し、セクションごとに [適用 (Apply)] をクリックします。
 - SSID : サービス セット 識別子。これは、ワイヤレス ネットワークの名前です。Wi-Fi 接続のワイヤレス ネットワークを選択すると、この名前が表示されます
 - ビーコンのブロードキャスト SSID (Broadcast SSID in Beacon) : このオプションを選択します。
 - Universal Admin Mode (ユニバーサル管理モード) : [無効 (Disable)]。

- セキュリティ (Security) : 使用するセキュリティ オプションを選択します。

- ステップ 7** ワイヤレス アクセス ポイントの Web インターフェイスでは、無線を有効にします。
- 左側の [サマリ (Summary)] をクリックし、メインページの [ネットワーク インターフェイス (Network Interfaces)] で、2.4 GHz 無線に対応するリンクをクリックします。
 - [Settings (設定)] タブをクリックします。
 - [Enable Radio] の設定では、[Enable] ラジオ ボタンをクリックし、ページ下部の [Apply] をクリックします。
 - 5 GHz 無線についてもプロセスを繰り返します。

初期セットアップ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は、デバイスには以下のデフォルト設定が適用されています。

この設定では、内部インターフェイス経由で Firepower Device Manager を開き (通常はコンピュータをインターフェイスに直接接続)、内部インターフェイス上で定義された DHCP サーバを使用して、コンピュータに IP アドレスを供給していることを前提としています。デバイスモデルごとのデフォルトの内部および外部インターフェイスについては、下の表を参照してください。また、物理的な管理インターフェイスまたは診断インターフェイスにコンピュータを接続して、DHCP を使用してアドレスを取得することもできます。デフォルトの内部および管理 IP アドレスについては、構成時の設定表を参照してください。この IP アドレスを使用して、ブラウザから Firepower Device Manager を開きます。

構成時のデフォルト設定

設定項目	デフォルト	初期設定時に変更できるか
管理者ユーザのパスワード	Admin123	可。デフォルト パスワードは変更する必要があります。
管理 IP アドレス	192.168.45.45	不可。
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。このゲートウェイは、 from-the-box (デバイスからの出力) トラフィックのみに対応して動作します。	いいえ。

設定項目	デフォルト	初期設定時に変更できるか
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 で有効化されています。	不可。
管理インターフェイスの DNS サーバ	OpenDNS パブリック DNS サーバ、208.67.220.220 および 208.67.222.222。	可。
内部インターフェイスの IP アドレス	192.168.1.1/24	不可。
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ~ 192.168.1.254 の内部インターフェイスで実行されます。	不可。
内部クライアントに対する DHCP 自動設定 (自動設定では、WINS および DNS サーバ用のアドレスがクライアントに供給されます)	外部インターフェイスに対して有効。	可 (ただし間接的に)。外部インターフェイスのスタティック IPv4 アドレスを設定すると、DHCP サーバ自動設定は無効になります。
外部インターフェイスの IP アドレス	DHCP を経由し、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取得。	可。

デバイス モデルごとのデフォルトのインターフェイス

初期設定時に、デフォルト以外の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割り当てを変更するには、インターフェイスおよび DHCP の設定を編集します。インターフェイスをスイッチ不可として設定するには、事前にこのインターフェイスをブリッジ グループから削除する必要があります。

FirePOWER Threat Defense デバイス	外部インターフェイス	内部インターフェイス
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet 1/1	BV11。外部インターフェイス以外の、他のすべてのデータインターフェイスが含まれます。5506W-X の場合はワイヤレス インターフェイス GigabitEthernet 1/9。

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 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet 0/0	GigabitEthernet 0/1

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」と示された項目は、すべて設定を確認し、必要に応じて修正してください。

設定項目	設定内容	明示的/暗黙的な設定、またはデフォルト設定
管理者ユーザのパスワード	任意の入力値	明示的
管理 IP アドレス	192.168.45.45	デフォルト
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。管理ゲートウェイは、 from-the-box （デバイスからの出力）トラフィックのみに対応して動作します。	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 で有効化されています。	デフォルト
管理インターフェイスの DNS サーバ	任意の入力値	明示的
管理ホスト名	firepower または任意の入力値	明示的

設定項目	設定内容	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	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。	暗黙的
システム時間	選択したタイムゾーンおよび NTP サーバ。	明示的
スマート ライセンス	基本ライセンスとともに登録したか、または評価期間を開始したか、いずれか選択した方法。サブスクリプションライセンスは有効化されていません。スマートライセンスのページに移動して、スマートライセンスを有効化してください。	明示的
内部インターフェイスの IP アドレス	192.168.1.1/24	デフォルト
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ~ 192.168.1.254 の内部インターフェイスで実行されます。	デフォルト
内部クライアントに対する DHCP 自動設定 (自動設定では、WINS および DNS サーバ用のアドレスがクライアントに供給されます)	DHCP を使用して外部インターフェイスの IPv4 アドレスを取得している場合、DHCP 自動設定は外部インターフェイスに対して有効化されます。 静的アドレッシングを使用している場合は、DHCP 自動設定は無効になります。	明示的 (ただし間接的)

設定項目	設定内容	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の設定	<p>(内部ブリッジグループがないモデル) 設定および有効化されるのは、外部インターフェイスと内部インターフェイスのみです。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> <p>(内部ブリッジグループを持つモデル) 外部インターフェイスを除くすべてのデータインターフェイス (GigabitEthernet 1/2 など) は有効化され、内部ブリッジグループの一部となります。これらのポートにエンドポイントまたはスイッチを接続すると、内部インターフェイスのアドレスを DHCP サーバから取得できます。</p>	デフォルト
外部の物理インターフェイスおよびIPアドレス	<p>デバイスモデルに基づくデフォルトの外部ポート。初期セットアップ前のデフォルト設定、(25 ページ) を参照してください。</p> <p>IPアドレスはDHCPによって取得されるか、入力したとおりのスタティックアドレスとなります (IPv4、IPv6、またはその両方)。</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。
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 <code>inside_zone</code>。内部ブリッジグループを持つモデルでは、内部ブリッジグループインターフェイスの全メンバーがゾーンに含まれます。</p> <p>外部インターフェイスを含む <code>outside_zone</code></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

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

設定の基本

以下の各トピックでは、デバイスを設定するための基本的な方法について説明します。

デバイスの設定

Firepower Device Manager に初めてログインする場合、セットアップウィザードに従い基本設定を行います。ウィザードを完了したら、次の手順を使用して、その他の機能を設定し、デバイス設定を管理します。

項目を視覚的に区別できない場合は、ユーザプロファイルに別のカラースキームを選択します。ページの右上にあるユーザアイコン 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、[デバイス サマリ (Device Summary)] [デバイス ダッシュボード (Device Dashboard)] にアクセスします。

ダッシュボードにデバイスのビジュアルステータスが表示されます。表示情報には、有効になっているインターフェイス、キー設定が設定されているか（緑色）、まだ未設定であるかが含まれます。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](#)、(34 ページ) を参照してください。

ステータスイメージの上に、デバイスモデル、ソフトウェアバージョン、VDB（システムおよび脆弱性のデータベース）バージョンの概要、および侵入ルールの最終更新時間が表示されます。

イメージの下には、設定可能なさまざまな機能のグループ、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実行できるアクションが表示されます。

ステップ 2 各グループのリンクをクリックして、設定を行うか、またはアクションを実行します。次に、グループのサマリを示します。

- [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](#)、(115 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。構成によってはその他のルートが必要な場合があります。 [ルーティング](#)、(137 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、脆弱性データベースの更新、システムソフトウェアの更新。これらの機能を使用する場合は、定期的な更新スケジュールを設定して、

最新のデータベース更新が適用されるようにします。定期的なスケジュール更新が行われる前に更新をダウンロードする必要がある場合は、このページにアクセスすることもできます。[システム データベースの更新](#), (331 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ています。一部は、デバイスの初期設定時に設定し、その後ほとんど変更することがない基本設定です。[システム設定](#), (319 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状態が表示されます。システムを使用するため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。一部の機能には追加ライセンスが必要です。[システムのライセンス](#), (71 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、または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](#), (336 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 の要求に従い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](#), (349 ページ) を参照してください。
- [サイト間 VPN (Site-to-Site VPN)]: このデバイスとリモートデバイス間のサイト間バーチャルプライベートネットワーク (VPN) 接続。[サイト間 VPN の管理](#), (297 ページ) を参照してください。

ステップ 3 メニューの [展開 (Deploy)] ボタンをクリックして、変更内容を展開します。



変更内容は、展開するまでデバイス上で有効になりません。[変更の展開](#), (32 ページ) を参照してください。

次の作業

メインメニューの [ポリシー (Policies)] をクリックして、システムのセキュリティポリシーを設定します。 [オブジェクト (Objects)] をクリックして、セキュリティ ポリシーに必要なオブジェクトを設定することもできます。

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。また、変更によってはインスペクションエンジンの再起動が必要であり、再起動中にトラフィックがドロップする場合がありますため、潜在的な分断の影響が最小限となるタイミングで変更を展開することを検討してください。

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させる設定変更](#)、（[33 ページ](#)）を参照してください。

手順

- ステップ 1** Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。このアイコンは、展開されていない変更がある場合にドットマークで強調表示されます。



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

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



- ステップ 2** [今すぐ展開 (Deploy Now)] をクリックします。

インスペクションエンジンを再起動させる設定変更

次の設定またはアクションはどれも、設定変更を導入するときにインスペクションエンジンが再起動します。

**注意**

展開時に、リソースの需要が高まった結果、いくつかの packets がインスペクションなしでドロップされる場合があります。さらに、一部の設定の導入ではインスペクションエンジンの再起動が必要です。これにより、トラフィックの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

導入によってインスペクション エンジンが再起動します。

システム アップデート

システムを再起動させないシステムアップデートまたはパッチをインストールする場合、それらにバイナリ変更が含まれているときは、インスペクションエンジンの再起動が必要になります。バイナリ変更には、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ます。バイナリ変更を含まないパッチが Snort の再起動を必要とする場合があることにも注意してください。

インターフェイスと管理ステータスの表示

デバイス概要には、デバイスおよび管理アドレスで選択する設定に関するグラフィカルビューが含まれます。デバイス概要を開くには、[デバイス (Device)] をクリックします。

このグラフィック上の要素は、要素のステータスに基づいて色が変わります。要素にカーソルを当てると、追加情報が表示されます。このグラフィックを使用して次の項目を監視できます。



(注) 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 ステータス情報を含めて、[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入手できます。

インターフェイス ステータス

ポートの上にマウスを合わせると、その IP アドレス、およびイネーブル ステータスやリンク ステータスが表示されます。IP アドレスは DHCP を使用してスタティックに割り当てたり、取得できます。ブリッジ仮想インターフェイス (BVI) 上にマウスを合わせた場合にも、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：インターフェイスが設定され、イネーブルで、リンクが稼働中です。
- 灰色：インターフェイスがイネーブルではありません。
- オレンジ/赤：インターフェイスが設定され、イネーブルですが、リンクがダウンしています。インターフェイスが有線接続である場合、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接続でない場合、これは予想される状態です。

内部、外部ネットワーク接続

グラフィックは、次の条件下でどのポートが外部（またはアップストリーム）および内部ネットワークに接続されるかを示します。

- 内部ネットワーク：内部ネットワークのポートは、「内部 (inside)」という名前のインターフェイスにのみ表示されます。さらなる内部ネットワークがある場合、それらは表示されま

せん。インターフェイスに「内部 (inside)」という名前を付けなければ、どのポートも内部ポートとしてマークされません。

- 外部ネットワーク：外部ネットワークのポートは、「外部 (outside)」という名前のインターフェイスにのみ表示されます。内部ネットワークと同様に、この名前は必須です。この名前を付けないと、ポートは外部ポートとしてマークされません。

管理設定ステータス

グラフィックは、管理アドレスにゲートウェイ、DNSサーバ、NTPサーバ、およびスマートライセンスが設定されているかどうか、および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。

緑色は機能が設定されて正常に動作していることを示し、灰色は設定されていないか、正しく動作していないことを示します。たとえば、サーバに到達できなければDNSボックスは灰色になります。要素にカーソルを当てると、詳細情報が表示されます。

問題が見つかった場合、次のように修正してください。

- 管理ポートとゲートウェイ：[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](#)、(345 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 グループで [設定を表示 (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更新の取得と適用など、ユーザが直接操作せずに発生する処理が含まれています。これらのシステムタスクとそのステータスを表示して、それらが正常に完了していることを確認できます。

手順

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




タスク リストが開き、システムタスクのステータスと詳細が表示されます。

- ステップ 2** タスクのステータスを評価します。

繰り返し発生する問題を発見した場合は、デバイス設定の修正が必要になる場合があります。たとえば、データベース更新を取得できない状態が続く場合は、デバイスの管理IPアドレスからイ

インターネットへのパスが存在しない可能性があります。タスクの説明で示される一部の問題については、Cisco Technical Assistance Center (TAC) に連絡する必要があります。

タスク リストでは、次の操作を実行できます。

- [成功 (Success)]または[失敗 (Failures)]ボタンをクリックして、ステータスに基づいてリストをフィルタリングする。
 - [削除 (Delete)]アイコン () をクリックして、タスクをリストから削除する。
 - [完了したタスクをすべて削除 (Remove All Completed Tasks)]をクリックして、進行中ではないタスクのリストを空にする。
-



第 2 章

FirePOWER Threat Defenseの使用例

ここでは、FirePOWER Threat Defenseで Firepower Device Manager を使用して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を完了し、その初期設定を維持していることを前提としています。初期設定を変更している場合でも、これらの例を参照することは、製品の使用方法を理解する上で役立つはずです。

- [ネットワーク トラフィックを調べる方法, 37 ページ](#)
- [脅威をブロックする方法, 45 ページ](#)
- [マルウェアをブロックする方法, 49 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, 53 ページ](#)
- [アプリケーションの使用を制御する方法, 58 ページ](#)
- [サブネットの追加方法, 62 ページ](#)

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、他のトラフィックすべてをブロックするデフォルトアクションが設定されます。付加的な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の状況を知ることが有益です。

ネットワーク トラフィックの分析には、FirePOWER デバイス マネージャのモニタリング機能を利用できます。FirePOWER デバイスマネージャのレポートは、次の質問の答えを得るのに役立ちます。

- 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ー
- ユーザの接続先
- ユーザが使用しているデバイス

- 最も多く適用されているアクセスコントロールルール（ポリシー）

最初のアクセスルールは、ポリシー、接続先、セキュリティゾーンを含むトラフィックに関するいくつかの情報を提供できます。しかし、ユーザ情報を取得するには、ユーザ自身を認証（特定）するよう求めるアイデンティティポリシーを設定する必要があります。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、いくつかの付加的な調整が必要です。

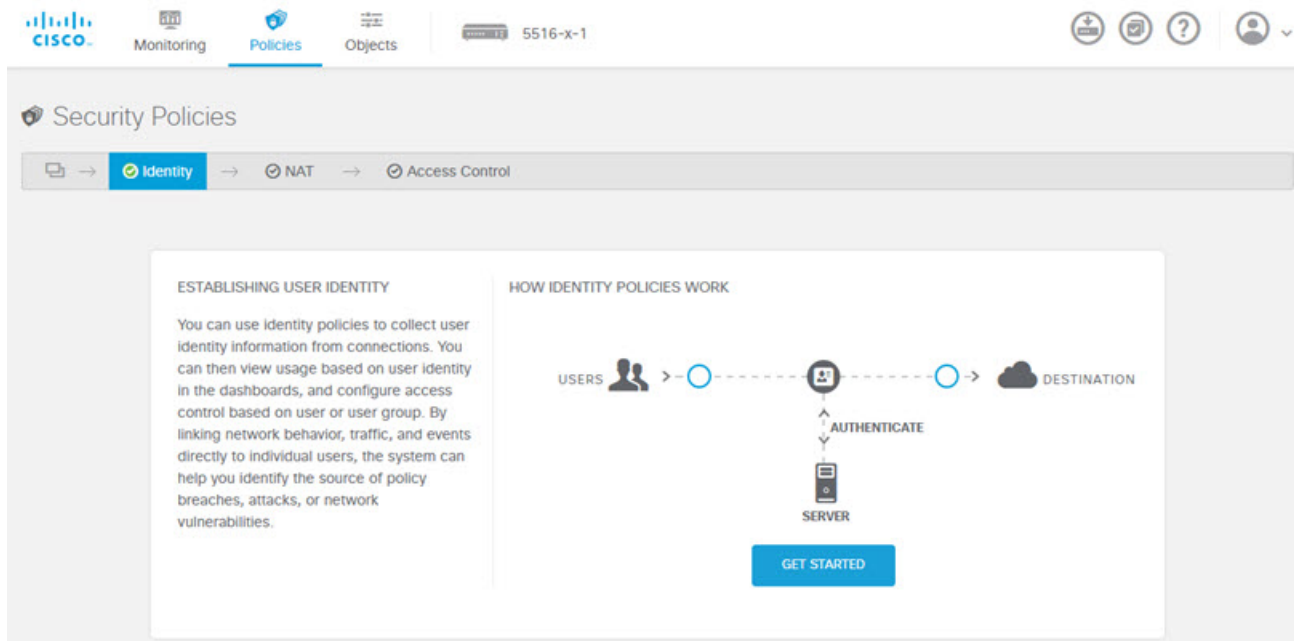
次の手順で、FirePOWER Threat Defenseデバイスがトラフィックをモニタするように設定する方法を説明し、設定ポリシーおよびモニタリングポリシーのエンドツーエンドプロセスの概要を示します。



- (注) この手順は、ユーザが参照するサイトの Web サイト カテゴリとレピュテーションについて理解する手がかりにはならないため、Web カテゴリ ダッシュボードで有意義な情報を得ることはできません。カテゴリおよびレピュテーション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行して、URL ライセンスを有効にする必要があります。この情報を取得するには、許容されるカテゴリ（[金融サービス (Financial Services)] など）へのアクセスを許可する新しいアクセスコントロールルールを追加し、このルールをアクセスコントロール ポリシーの最初のルールにします。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](#)、(53 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を設定する必要があります。
- アイデンティティポリシーを有効にすることにより、だれがネットワークを使用しているか、使用されているリソースは何かに関する情報を収集できます。この情報は、ユーザ監視ダッシュボードで入手できます。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使用できます。
- ユーザは、HTTP 接続のために Web ブラウザを使用する際に認証されます。
- 認証に失敗したユーザが Web 接続を阻止されることはありません。これは、単に接続のためのユーザ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)]をクリックしてから、[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、初期状態では無効になっています。アイデンティティポリシーは、アクティブディレクトリサーバを使用して、ユーザを認証し、使用中のワークステーションの IP アドレスにユーザを関連付けます。その後、システムは、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特定します。



b) [開始 (Get Started)]ボタンをクリックして、必要な要素を設定するウィザードを開始します。

c) アクティブ ディレクトリ サーバを特定します。

次の情報を入力します。

- 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。Active Directory が唯一サポートされているタイプであり、このフィールドは変更できません。
- 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する適切な権限を持つユーザの識別ユーザ名とパスワード。たとえば、admin@ad.example.com。
- ベース DN (Base DN) : ユーザおよびグループ情報を検索またはクエリするためのディレクトリ ツリー、つまり、ユーザとグループの共通の親。たとえば、dc=example、dc=com。ベース DN の検索方法の詳細については、[ディレクトリ ベースの DN の決定](#)、(147 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。
- 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している場合は、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されるポート番号。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情報をダウンロードするために暗号化された接続を使用するには、目的の方式 [STARTTLS] または [LDAPS] を選択します。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ることを意味します。

- [STARTTLS]は、暗号化方式をネゴシエートして、ディレクトリサーバによってサポートされている最強の方式を使用します。ポート 389 を使用します。
- [LDAPS]には、LDAP over SSL が必要です。ポート 636 を使用します。
- SSL証明書 (SSL Certificate) : 暗号化方式を選択する場合は、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するため、CA 証明書をアップロードします。証明書を使用して認証している場合は、証明書のサーバ名がサーバのホスト名/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、証明書内で ad.example.com を使用した場合は、接続が失敗します。

例 :

たとえば、次のイメージは、ad.example.com サーバへの非暗号化接続を作成する方法を示しています。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。すべてのユーザ情報とグループ情報は、識別名 (DN) ou=user、dc=example、dc=com の下にあります。

The screenshot shows a configuration window for a Directory Server. The fields are as follows:

Field	Value
Name	AD
Type	Active Directory (AD)
Directory Username	Administrator@ad.example.com
Directory Password
Base DN	ou=user,dc=example,dc=com
AD Primary Domain	example.com
Hostname / IP Address	ad.example.com
Port	389
Encryption	NONE
SSL Certificate	UPLOAD (button) No certificates uploaded yet.

At the bottom right, there are two buttons: CANCEL and NEXT.

d) [Next]をクリックします。

- e) アクティブ認証キャプティブ ポータルを設定します。
最も簡単なオプションは、すべてのフィールドをそのままにして[保存 (Save)]をクリックすることです。アクティブ認証のデフォルトポートを設定した場合、ユーザは、自分のユーザ名とパスワードを提供するために信頼する必要がある自己署名証明書を取得します。そうなることが予想されることと、ユーザは証明書を承認する必要があることをユーザに知らせてください。

とはいえ、ブラウザがすでに信頼した証明書をアップロードすることが理想的です。証明書が存在する場合、その証明書を使用するには、次のフィールドに入力します。

- サーバ証明書 (Server Certificate) : アクティブ認証時にユーザに提供される CA 証明書。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。証明書を貼り付けるか、または [証明書のアップロード (Upload Certificate)] をクリックして証明書ファイルを選択します。デフォルトでは、ユーザ認証時に自己署名証明書を提供します。
- 証明書キー (Certificate Key) : サーバ証明書のキー。キーを貼り付けるか、または [キーのアップロード (Upload Key)] をクリックしてキーファイルを選択します。
- 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。異なるポートを設定する場合は、1025 ~ 65535 の範囲内にする必要があります。

- f) [Save]をクリックします。
これにより、セットアップウィザードが実行されます。次に、アクティブ認証を必要とする特定のルールを作成します。
- g) [アイデンティティルールの作成 (Create Identity Rule)] ボタンをクリックするか、[+] ボタンをクリックします。
- h) アイデンティティルールのプロパティを入力します。
すべてにユーザに認証を要求する場合、次の設定を使用できます。

- [名前 (Name)] : 任意の名前。Require_Authentication など。
- [ユーザ認証 (User Authentication)] : [アクティブ (Active)] がすでに選択されている必要があります。変更しないでください。
- [タイプ (Type)] : [HTTP ネゴシエート (HTTP Negotiate)] を選択します。これは、ブラウザとディレクトリサーバが、まず NTLM、次に HTTP ベーシックの順序で、最も強力な認証プロトコルをネゴシエートすることを許可します。

(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 ネゴシエートの場合は、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は、DNS サーバも更新して、アクティブな認証が必要な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必要があります。そうしないと、リダイレクションが完了できず、ユーザは認証できません。認証が実行されない場合、または認証を実行しない場合には、DNS サーバを更新して、他の認証方法の 1 つを選択します。

- [送信元/接続先 (Source/Destination)] : すべてのフィールドをデフォルトから [任意 (Any)] にします。

トラフィックを一層制限された設定にすることがふさわしいと判断する場合、ポリシーを制限することもできます。とはいえ、アクティブ認証は HTTP トラフィックのみで試行されるため、非HTTPトラフィックが送信元/接続先条件に一致するかどうかは重要ではありません。アイデンティティポリシーのプロパティの詳細については、[アイデンティティルールの設定](#)、(153 ページ) を参照してください。

SOURCE		DESTINATION			
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ANY	ANY	ANY	ANY	ANY

- [OK]をクリックしてルールを追加します。

ウィンドウ右上の[展開 (Deploy)]アイコンボタンにはドットが表示されます。これは、展開されていない変更があることを示しています。ユーザインターフェイスでの変更だけでは、変更がデバイスに設定されないため、変更を展開する必要があります。そのため、部分的に設定された一連の変更がデバイス上で実行されるという潜在的な問題に直面せずにすむよう、変更を展開する前に関係する一連の変更を作成することができます。このプロセスの後の手順で変更を展開します。



- 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 [許可する (Allow)] に変更します。

Inside_Outside_Rule アクセスルールは、信頼済みのルールとして作成されます。ただし、信頼済みのトラフィックのインスペクションは実行されないため、トラフィックの一致条件に、アプリケーションや、ゾーン、IPアドレス、ポート以外の他の条件が含まれていない場合、システムは、信頼済みのトラフィックの特性の一部 (アプリケーションなど) について把握することができません。トラフィックを信頼するのではなく、トラフィックを許可するようにルールを変更すると、システムは、トラフィックのインスペクションを完全に実行します。

- (注) (ASA 5506-X モデル) Inside_Inside_Rule を [信頼する (Trust)] から [許可する (Allow)] に変更することも検討してください。このルールは、内部インターフェイス間のトラフィックを対象とします。

- [ポリシー (Policies)] ページの [アクセスコントロール (Access Control)] をクリックします。

- b) Inside_Outside_Rule の右側の [アクション (Actions)] セルにマウスオーバーして編集項目を表示してからアイコンを削除し、編集アイコン (🔗) をクリックしてルールを開きます。
- c) [アクション (Action)] の [許可する (Allow)] を選択します。

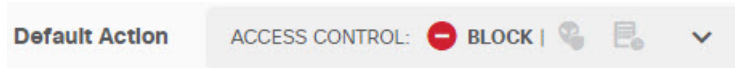
Order	Title	Action
1	Inside_Outside_Rule	🔗 Allow

- d) [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 アクションでのロギングを有効にします。ダッシュボードには、接続が、接続ロギングを有効にするアクセスコントロールルールに一致する場合にのみ、接続に関する情報が表示されます。Inside_Outside_Rule はロギングを有効にしますが、デフォルト アクションはロギングを無効にしています。したがって、ダッシュボードには Inside_Outside_Rule の情報のみが表示され、ルールに一致しない接続は反映されません。

- a) アクセス コントロール ポリシーのページ下部にあるデフォルト アクションの部分をクリックします。



- b) [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。
- c) [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、接続に使用するアプリケーションを特定できるアプリケーション デイテクトを含む VDB に定期的に更新を提供します。VDB は定期的に更新する必要があります。手動で更新をダウンロードすることもできれば、定期的なスケジュールを設定することもできます。次に、スケジュールを設定する方法を示します。デフォルトでは、VDB 更新が無効になっているため、更新された VDB を取得するアクションを実行する必要があります。

- a) デバイスをクリックします。
- b) [更新 (Updates)] グループの [設定の表示 (View Configuration)] をクリックします。

Updates

[View Configuration](#) >

- c) [VDB] グループの [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。

ネットワークを障害しない時間と頻度を選択します。また、更新のダウンロード後に、システムが更新を自動展開することに留意してください。これは新しいディテクタを有効にするために必要です。したがって、実行し保存したもののまだ展開していなかったいずれの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、毎週日曜日の AM 12:00（24時間表記を使用）に VDB データベースを更新します。

Set recurring VDB Update

Frequency

Weekly

Days of Week

Sundays ×

Time

at 00 : 00

(-07:00) America/Los_Angeles

e) [保存 (Save)]をクリックします。

ステップ 5 変更を保存します。

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



b) [すぐに展開する (Deploy Now)]ボタンをクリックして、展開が完了するまで待機します。展開の概要に変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)]になる必要があります。

Deployment Summary

DEPLOY NOW

You have successfully deployed.

Deployment History

Modified Objects	Initiated	Completed	Status
> AccessPolicy	11 May 2016	11 May 2016	✔ Deployed
> AccessRule	01:24:35 PM	01:27:06 PM	
> ActiveDirectoryRealm			
> IdentityPolicy			
> IdentityRule			

次の作業

この時点で、監視ダッシュボードとイベントに、ユーザとアプリケーションについての情報が表示され始める必要があります。望ましくないパターンの情報を評価し、許容されない使用を制約する新しいアクセスルールを作成することができます。

侵入とマルウェアに関する情報の収集を開始する場合、1つ以上のアクセスルールで侵入ポリシーとファイルポリシーを有効にする必要があります。これらの機能のライセンスを有効にする必要もあります。

Web 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

アクセスコントロールルールに侵入ポリシーを追加することで、次世代侵入防御システム (IPS) 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と既知の脅威を比較します。ある接続と監視中の脅威が一致する場合、システムはその接続をドロップすることにより攻撃を阻止します。

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。

侵入ポリシーの設定に使用できるルールは、トラフィックを [許可する (allow)] ルールのみです。インスペクションは、ルールがトラフィックを [信頼する (trust)] または [ブロックする (block)] ように設定されていると実行されません。さらに、デフォルトアクションが [許可する (allow)] になっている場合、侵入ポリシーをデフォルトアクションの一部として設定できます。

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、侵入ルールとプリプロセッサルールの状態を設定し、詳細設定を構成する Cisco Talos Security Intelligence and Research Group によって設計されています。

手順

ステップ 1 まだ有効にしていない場合には、[脅威 (Threat)] ライセンスを有効にします。侵入ポリシーを使用するには、[脅威 (Threat)] ライセンスを有効にする必要があります。現在評価ライセンスを使用している場合、このライセンスの評価版が有効になっています。デバイスが登録済みの場合、必要なライセンスを購入して、そのライセンスを Cisco.com の Smart Software Manager のアカウントに追加する必要があります。

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



- [脅威 (Threat)] グループで [有効にする (Enable)] をクリックします。システムは、ユーザのアカウントでライセンスを登録するか、必要に応じて評価ライセンスを有効にします。グループの表示は、ライセンスが有効になり、ボタンが [無効にする (Disable)] ボタンに変更されている必要があります。



ステップ 2 1 つ以上のアクセスルールに対して侵入ポリシーを選択します。脅威をスキャンするトラフィックを対象とするルールを決定します。この例では、侵入インスプレクションを Inside_Outside_Rule に追加します。ASA 5506-X モデルの場合、Inside_Inside_Rule にも追加できます。

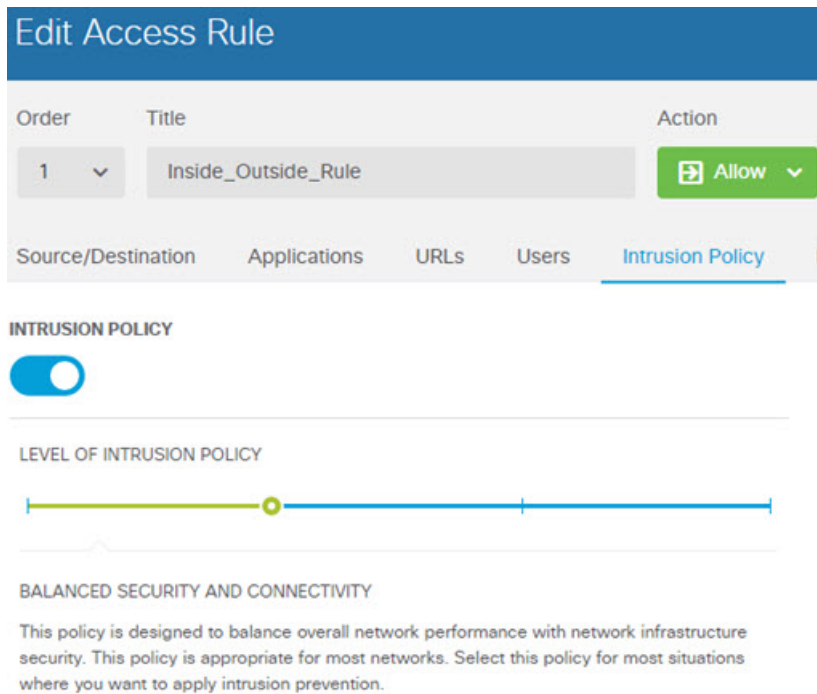
- メインメニューで [ポリシー (Policies)] をクリックします。
[アクセスコントロール (Access Control)] ポリシーが表示されていることを確認します。
- Inside_Outside_Rule の右側の [アクション (Actions)] セルにマウスオーバーして編集項目を表示してからアイコンを削除し、編集アイコン (🔧) をクリックしてルールを開きます。
- まだ実行していない場合、[アクション (Action)] を [許可する (Allow)] を選択します。

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有効にしてから、スライダで侵入ポリシーのレベルを選択します。

ポリシーは、安全性の小さいものから大きいものへの順序で表示されます。[バランスのとれた安全性と接続性 (Balanced Security and Connectivity)] は、ほとんどのネットワークに適しています。ユーザがドロップすることを望まないトラフィックをドロップする可能性のある過度に積極的な防御機能ではなく、適度な侵入防御機能を提供します。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、[安全性よりも接続性を優先する (Connectivity over Security)] ポリシーを選択することにより、侵入インスペクションを緩和できます。

セキュリティに関して積極的である必要がある場合には、[接続性よりも安全性を優先する (Security over Connectivity)] ポリシーを試行します。[最大限検出する (Maximum Detection)] 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にさらに重点を置いており、運用上の影響が一層大きくなる可能性があります。



- 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判断するために侵入ポリシーによって使用される侵入ルールデータベースの更新を定期的リリースします。ルールデータベースを定期的に更新する必要があります。手動で更新をダウンロードすることもできれば、定期的なスケジュールを設定

することもできます。次に、スケジュールを設定する方法を示します。デフォルトでは、データベース更新が無効になっているため、更新されたルールを取得するアクションを実行する必要があります。

- a) デバイスをクリックします。
- b) [更新 (Updates)] グループの [設定の表示 (View Configuration)] をクリックします。

Updates

[View Configuration](#) >

- c) [ルール (Rule)] グループの [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。
ネットワークを阻害しない時間と頻度を選択します。また、更新のダウンロード後に、システムが更新を自動展開することに留意してください。これは新しいルールを有効にするために必要です。したがって、実行し保存したもののまだ展開していなかったいずれの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、毎週月曜日の AM 12:00 (24 時間表記を使用) にルールデータベースを更新します。

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 変更を保存します。

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



b) [すぐに展開する (Deploy Now)] ボタンをクリックして、展開が完了するまで待機します。展開の概要に変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になる必要があります。

次の作業

この時点で、監視ダッシュボードとイベントが開始され、何らかの侵入が確認された場合、攻撃者、ターゲット、脅威に関する情報が表示されるようになる必要があります。この情報を評価して、ネットワークにより多くのセキュリティ対策が必要かどうか、または侵入ポリシーのレベルを下げる必要があるかどうかを判断できます。

マルウェアをブロックする方法

ユーザは、悪意のあるソフトウェアやマルウェアをインターネットサイトや電子メールなどの他の通信方法で取得するリスクに常にさらされています。信頼される Web サイトでも、ハイジャックされて、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、しばしば、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 用 Advanced Malware Protection (FirePOWER 用 AMP) を使用して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。

FirePOWER 用 AMP 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マルウェアの疑いのあるファイルの性質を把握します。管理インターフェイスには、AMP クラウドに到達し、マルウェア ルックアップを実行するためのインターネットへのパスが必要です。デバイスは、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、AMP クラウドにファイルの性質について問い合わせます。想定される性質には、[クリーン (clean)]、[マルウェア (malware)]、または [不明 (unknown)] (明確に判定できない) が含まれます。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、接続されている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。

ファイルポリシーの設定に使用できるルールは、トラフィックを [許可する (allow)] ルールのみです。インスペクションは、ルールがトラフィックを [信頼する (trust)] または [ブロックする (block)] ように設定されていると実行されません。

手順

ステップ 1 まだ有効にしていない場合には、[マルウェア (Malware)] ライセンスを有効にします。マルウェアの制御にファイルポリシーを使用するには、[マルウェア (Malware)] 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、このライセンスの評価版が有効になっています。デバイスが登録済みの場合、必要なライセンスを購入して、そのライセンスを Cisco.com の Smart Software Manager のアカウントに追加する必要があります。

a) デバイスをクリックします。

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 [有効にする (Enable)] をクリックします。システムは、ユーザのアカウントでライセンスを登録するか、必要に応じて評価ライセンスを有効にします。グループの表示は、ライセンスが有効になり、ボタンが [無効にする (Disable)] ボタンに変更されている必要があります。



ステップ 2 1 つ以上のアクセス ルールに対してファイル ポリシーを選択します。

マルウェアをスキャンするトラフィックを対象とするルールを決定します。この例では、ファイルインスペクションを `Inside_Outside_Rule` に追加します。ASA 5506-X モデルの場合、`Inside_Inside_Rule` にも追加できます。

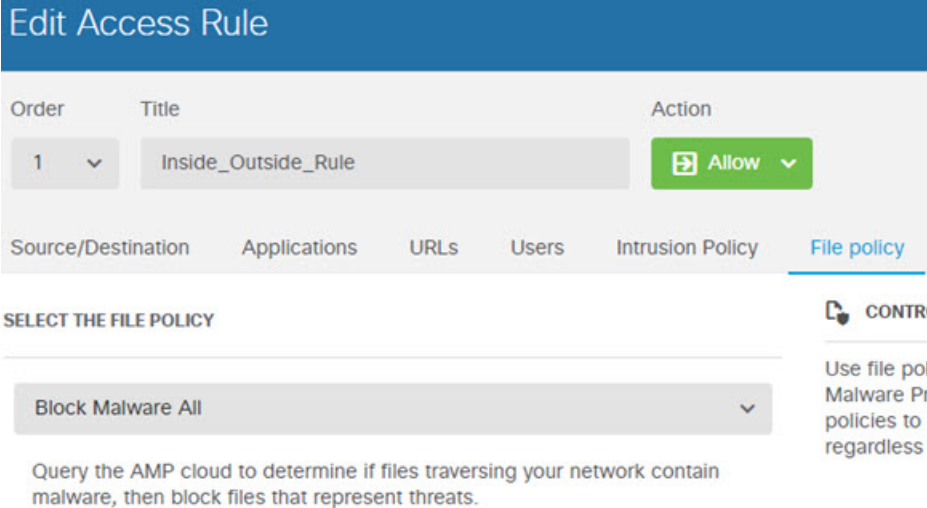
- a) メインメニューで [ポリシー (Policies)] をクリックします。
[アクセスコントロール (Access Control)] ポリシーが表示されていることを確認します。
- b) `Inside_Outside_Rule` の右側の [アクション (Actions)] セルにマウスオーバーして編集項目を表示してからアイコンを削除し、編集アイコン (🔗) をクリックしてルールを開きます。
- c) まだ実行していない場合、[アクション (Action)] を [許可する (Allow)] を選択します。

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。
マルウェアとみなされたすべてのファイルをドロップする [すべてのマルウェアをブロックする (Block Malware All)] と、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るもののブロックはしない [クラウドですべてをルックアップする (Cloud Lookup All)] のどちらを選択するかが主要な選択事項です。最初にファイルの評価方法を確認するには、クラウドルックアップを使用します。ファイルの評価方法に納得した後で、ブロッキングポリシーに切り替えることもできます。

マルウェアをブロックする使用可能な他のポリシーもあります。これらのポリシーは、Microsoft Office、または Office および PDF ドキュメントのアップロードをブロックするファイル制御と併用されます。つまり、これらのポリシーは、マルウェアをブロックするだけでなく、ユーザが他のネットワークにこれらのファイルタイプを送信することを防止します。必要に応じて、これらのポリシーを選択できます。

この例では、[すべてのマルウェアをブロックする (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)] 下の [ログファイル (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した場合にはいつでもファイルロギングが有効になります。イベントとダッシュボードのファイルとマルウェア情報を取得するには、ファイルロギングを有効にする必要があります。

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 [変更を展開する (Deploy Changes)] アイコンをクリックします。



- b) [すぐに展開する (Deploy Now)] ボタンをクリックして、展開が完了するまで待機します。展開の概要に変更が正常に展開されたことが示され、ジョブのタスクステータスが [展開済み (Deployed)] になる必要があります。

次の作業

この時点で、ダッシュボードおよびイベントの監視が開始され、ファイルまたはマルウェアが送信された場合には、ファイルタイプ、ファイルイベントおよびマルウェアイベントに関する情報が表示される必要があります。この情報を評価して、ネットワークが送信に関連したセキュリティ対策をさらに必要とするかどうかを判断できます。

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。カテゴリを一致させるため、サイトの相対的な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と、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、シスコの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。

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。例として、いくつかのカテゴリの任意の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、`badsite.example.com` をブロックします。

手順

ステップ 1

まだ有効にしていない場合には、[URL]ライセンスを有効にします。Webカテゴリとレピュテーション情報を使用したり、ダッシュボードとイベントの情報を表示したりするには、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、このライセンスの評価版が有効になっています。デバイスが登録済みの場合、必要なライセンスを購入して、そのライセンスをCisco.comのSmart Software Managerのアカウントに追加する必要があります。

- a) デバイスをクリックします。
- 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。

Smart License

Registered

View Configuration >

- c) [URL ライセンス]グループで [有効にする (Enable)] をクリックします。システムは、ユーザのアカウントでライセンスを登録するか、必要に応じて評価ライセンスを有効にします。グループの表示は、ライセンスが有効になり、ボタンが [無効にする (Disable)] ボタンに変更されている必要があります。

URL License

 Enabled

DISABLE

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を作成する前に、ユーザが閲覧しているサイトのカテゴリを最初に確認したいと思うかも知れません。その場合、許容されるカテゴリ ([金融サービス (Financial Services)] など) の [許可する (Allow)] アクションでルールを作成できます。すべての Web 接続を確認して URL がこのカテゴリに属しているかどうか判断する必要があるため、[金融サービス (Financial Services)] ではないサイトのカテゴリ情報を取得します。

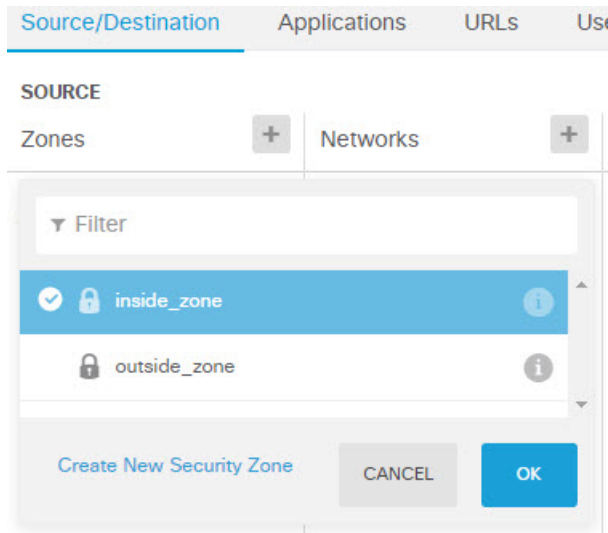
しかし、ブロックするつもりであることをすでに知っている Web カテゴリも存在します。ブロッキングポリシーはインスペクションを強制するため、ユーザは、ブロックされたカテゴリだけではなく、ブロックされなかったカテゴリへの接続に関する情報も取得します。

- メインメニューで [ポリシー (Policies)] をクリックします。
[アクセス コントロール (Access Control)] ポリシーが表示されていることを確認します。
- [+] をクリックして新しいルールを追加します。
- 順序、タイトル、アクションを設定します。
 - [順序 (Order)] : デフォルトでは、アクセス コントロール ポリシーの末尾に新しいルールを追加します。ただしこのルールは、同じ送信元/接続先その他の条件に一致するルールの前 (上) に配置する必要があります。そうしないと、このルールはどの接続とも一致しなくなります (1つの接続は1つのルール、つまりテーブル内で一致する最初のルールのみと一致します)。このルールの場合、デバイスの初期設定時に作成された `Inside_Outside_Rule` と同じ送信元/接続先を使用します。すでに他のルールが作成されている場合もあります。アクセス コントロールの効率を最大化するため、早期に特定のルールを作成して、接続を許可するか、またはドロップするかの決定を最大限迅速化することが最善です。例として、ルールの順序に [1] を選択します。
 - [タイトル (Title)] : ルールに意味のある名前を付けます (`Block_Web_Sites` など)。
 - [アクション (Action)] : [ブロックする (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。

どの条件を追加しても、同じ方法で動作します。[+]をクリックすると開く小さなダイアログボックスで、追加する項目をクリックします。複数の項目をクリックすることができ、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された項目を示します。しかし、[OK]ボタンをクリックしない限り、何もポリシーに追加されません。項目を選択するだけでは十分ではありません。

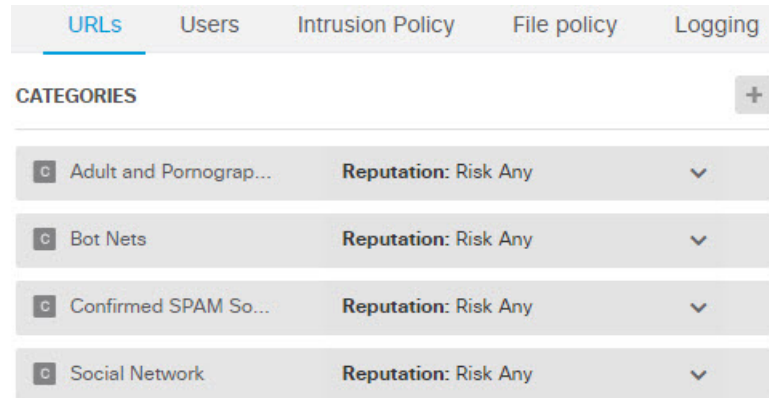


- e) 同じ技術を使用して、[接続先 (Destination)]>[ゾーン (Zones)]で[outside_zone] を選択します。

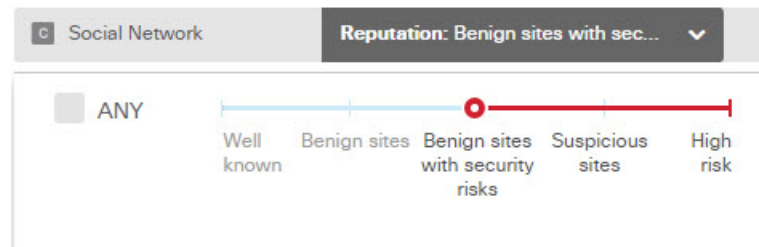
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
SOURCE						DESTINATION
Zones			Ports		Zones	
inside_zone	ANY		ANY		outside_zone	

- f) [URL]タブをクリックします。
g) [カテゴリ (Categories)]の[+]をクリックして、完全にまたは一部をブロックするカテゴリを選択します。

例として、[成人向けおよびポルノ (Adult and Pornography)]、[ボットネット (Bot Nets)]、[確認済みスパム ソース (Confirmed SPAM Sources)]、[ソーシャル ネットワーク (Social Network)] を選択します。ブロックする可能性の高い付加的なカテゴリもあります。



- h) [ソーシャル ネットワーク (Social Network)] カテゴリのレピュテーション依存ブロッキングを実装するには、このカテゴリの[レピュテーション: すべてのリスク (Reputation: Risk Any)] をクリックし、[すべて (Any)] を解除してから、スライダを[セキュリティ リスクのある無害なサイト (Benign sites with security risks)] に移動します。スライダから離れた部分をクリックしてスライダを閉じます。



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ます。この例では、[疑わしいサイト (Suspicious Sites)] と [高リスク (High Risk)] の範囲内のレピュテーションを持つソーシャル ネットワーキング サイトのみがブロックされます。このようにして、ユーザは、一般的に使用されているソーシャル ネットワーキング サイトにアクセスすることができます。

レピュテーションを使用して、許可するカテゴリ内のサイトを選択的にブロックすることもできます。

- i) カテゴリ一覧左の [URL (URLS)] 一覧横の [+] 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、[新しい 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] と入力してから、[追加 (Add)] [OK] をクリックしてオブジェクトを作成します。

オブジェクトを URL と同じ名前にすることもできますし、オブジェクトに別の名前を指定することもできます。URL には、URL のプロトコル部分を含めずに、サーバ名のみを追加してください。

New URL Object

Name

badsite.example.com

Description

URL

badsite.example.com

- l) 新しいオブジェクトを選択してから、[OK]をクリックします。ポリシーの編集時に新しいオブジェクトを追加すると、そのオブジェクトは一覧に追加されません。新しい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
<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">badsite.example.com</div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input checked="" type="checkbox"/> Adult and Pornograp... Reputation: Risk Any </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input checked="" type="checkbox"/> Bot Nets Reputation: Risk Any </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input checked="" type="checkbox"/> Confirmed SPAM So... Reputation: Risk Any </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input checked="" type="checkbox"/> Social Network Reputation: Benign sites with sec... </div>

- 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 ダッシュボードと接続イベントにカテゴリおよびレピュテーション情報を取得するには、ロギングを有効に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 ライセンスを有効にすると、システムは、Web カテゴリ データベースに対する更新を自動的に有効にします。システムは 30 分ごとに更新をチェックしますが、データは通常 1 日ごとに更新されます。何らかの理由で更新を必要としない場合には、更新を無効にすることもできます。

分析のために、シスコに分類されていない URL を選択し送信することもできます。そうすると、ユーザがカテゴリとレピュテーションのない新しいサイトに移動した場合、シスコはそのサイトを評価し、分類し、レピュテーションを付与し、将来の更新に含めることができます。サイトへのその後のアクセスは、新しい情報に基づいて許可されるか、またはブロックされる場合があります。

a) デバイスをクリックします。

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 (Query Cisco CSI for Unknown URLs)] を選択します。

d) [保存 (Save)] をクリックします。

ステップ 4 変更を保存します。

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



b) [すぐに展開する (Deploy Now)] ボタンをクリックして、展開が完了するまで待機します。

展開の概要に変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になる必要があります。

次の作業

この時点で、監視ダッシュボードとイベントに、Web カテゴリおよびレピュテーション、ドロップされた接続についての情報が表示されるようになる必要があります。この情報を評価して、URL フィルタリングで好ましくないサイトがドロップされているかどうか、または特定の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。

分類と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前に、ユーザに通知することを検討してください。

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、または企業ネットワークの内部および外部での転送に 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りました。

FirePOWER Threat Defense は、接続のインスペクションを実行して、使用されているアプリケーションを判別します。これにより、特定の TCP ポートや UDP ポートではなく、アプリケーション

ンを対象とするアクセスコントロールルールを記述することが可能になります。そのため、同じポートを使用している場合でも、Web ベース アプリケーションを選択的にブロックまたは許可することができます。

許可またはブロックする特定のアプリケーションを選択することもできますが、タイプ、カテゴリ、タグ、リスク、あるい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。ユーザがそれらのアプリケーションの1つを使用しようとする、セッションがブロックされます。

シスコは、システムおよび脆弱性データベース (VDB) の更新を通じて頻繁にアプリケーションを更新し追加します。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、新しいアプリケーションに自動的に適用され、ルールを手動で更新する必要はありません。

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

はじめる前に

この使用例は、使用例 [ネットワークトラフィックを調べる方法](#)、(37 ページ) が完了済みであることを前提としています。その使用例は、アプリケーションダッシュボードで分析可能なアプリケーション使用情報を収集する方法を説明しています。どのようなアプリケーションが実際に使用されているかを理解することは、有効なアプリケーションベースのルールを設計するのに役立つ場合があります。さらにこの使用例は、ここでは繰り返されない VDB 更新スケジュールの作成方法についても説明しています。VDB が定期的に更新され、アプリケーションが正しく特定されることを確認してください。

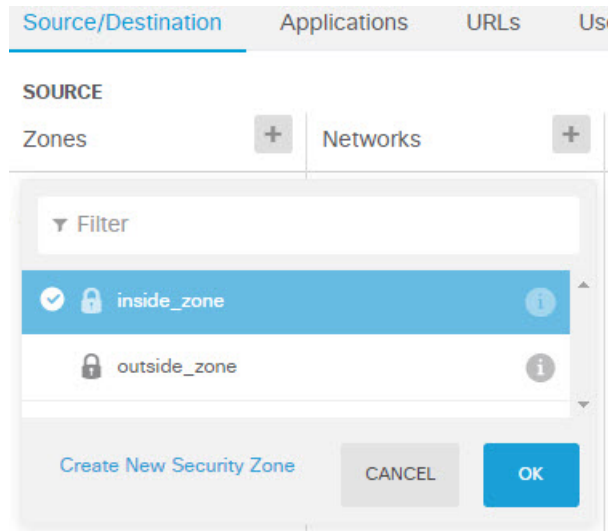
手順

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てい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、アクションを設定します。
 - [順序 (Order)]: デフォルトでは、アクセス コントロール ポリシーの末尾に新しいルールを追加します。ただしこのルールは、同じ送信元/接続先その他の条件に一致するルールの前 (上) に配置する必要があります。そうしないと、このルールはどの接続とも一致しなくなります (1 つの接続は 1 つのルール、つまりテーブル内で一致する最初のルールのみと一致します)。このルールの場合、デバイスの初期設定時に作成された `Inside_Outside_Rule` と同じ送信元/接続先を使用します。すでに他のルールが作成されている場合もあります。アクセス コントロールの効率を最大化するため、早期に特定のルールを作成して、接続を許可するか、またはドロップするかの決定を最大限迅速化することが最善です。例として、ルールの順序に [1] を選択します。
 - [タイトル (Title)]: ルールに意味のある名前を付けます (`Block_Anonymizers` など)。
 - [アクション (Action)]: [ブロックする (Block)] を選択します。

Order	Title	Action
1	Block_Anonymizers	Block

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



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

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

- f) [アプリケーション (Applications)]タブをクリックします。
- g) [アプリケーション (Applications)]の[+]をクリックしてから、ポップアップダイアログボックスの下部にある[詳細フィルタ (Advanced Filter)]リンクをクリックします。前もってアプリケーションフィルタオブジェクトを作成しておき、ここでアプリケーションフィルタリストに対して適用することも可能ですが、アクセスコントロールルールで直接条件を指定して、その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対してルールを記述する場合でない限り、[詳細フィルタ (Advanced Filter)]ダイアログボックスを使用してアプリケーションを選択し、適切な条件を構築する方が簡単です。

条件を選択すると、ダイアログボックス下のアプリケーションリストが更新され、どのアプリケーションが選択した条件と一致するかが表示されます。記述中のルールは、これらのアプリケーションに適用されます。

このリストを注意深く参照してください。たとえば、非常にリスクの高いアプリケーションすべてをブロックしたいと思うかもしれませんが、しかし、このルール記述の場合、Facebook と TFPT は非常にリスクが高いアプリケーションとして分類されます。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したいとは考えません。時間をかけてさまざまなフィルタ条件を試行し、どのアプリケーションが選択に一致するかを確認してください。これらのリストは、すべての VDB 更新で変更される場合があることに留意してください。

例として、[カテゴリ (Categories)] リストからアノマイザーまたはプロキシを選択します。

Filter Applications ? RESET FILTER

Risks

Any

Business Relevance

Any

Types

Any

Categories 1 selected x

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

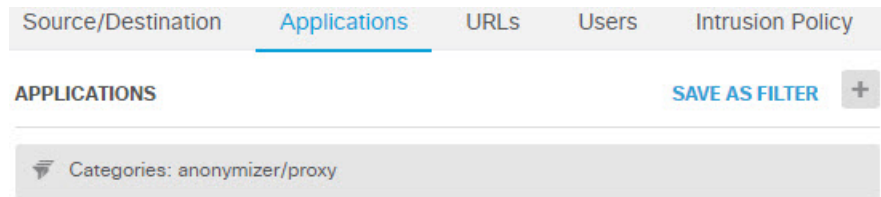
Tags Any selected

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

Filter the list of applications 33 Applications

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

- h) [詳細フィルタ (Advanced Filter)] ダイアログボックスで [Add (追加)] をクリックします。フィルタが [アプリケーション (Applications)] タブに追加され、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すべての接続についての情報を取得するには、ロギングを有効に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 [変更を展開する (Deploy Changes)] アイコンをクリックします。



- b) [すぐに展開する (Deploy Now)] ボタンをクリックして、展開が完了するまで待機します。
展開の概要に変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になる必要があります。

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

[ネットワークの概要 (Network Overview)] ダッシュボードに、アプリケーション ウィジェットでドロップされた接続が表示される場合があります。[すべて/拒否済み/許可済み (All/Denied/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にフォーカスします。

[アプリケーション (Applications)] ダッシュボードには、これらの結果も表示されます。あるユーザがこれらのアプリケーションを使用しようとする場合、アイデンティティ ポリシーが有効になっており認証が必要であると仮定すると、アプリケーションと接続を試行するそのユーザを関連付ける必要があります。

サブネットの追加方法

デバイスで使用可能なインターフェイスがあれば、それをスイッチ（または別のルータ）に配線して、異なるサブネットにサービスを提供することができます。

サブネットを追加する理由は数多くあります。この使用例では、次の一般的なシナリオについて説明します。

- サブネットは、プライベート ネットワーク 192.168.2.0/24 を使用してい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、ネットワークには物理インターフェイスが使用されています。別のオプションとして、すでに配線済みのインターフェイスを使用して、新しいネットワーク向けのサブインターフェイスを作成することができます。
- デバイスは、192.168.2.2 ~ 192.168.2.254 をアドレス プールとして使用し、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。
- 他の内部ネットワークと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す。外部ネットワークに向かうトラフィックは、パブリック アドレスを取得するために NAT を使用します。



- (注) この例では、未使用のインターフェイスがブリッジ グループの一部ではないと仮定します。もし現在ブリッジグループのメンバーであるならば、この手順を進める前に、ブリッジグループから削除する必要があります。

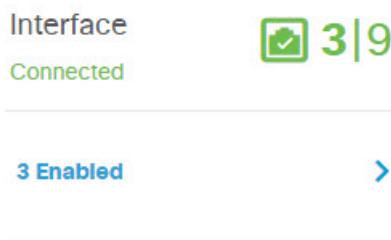
はじめる前に

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と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。

- デバイス。
- [インターフェイス (Interfaces)] グループで、有効なインターフェイスの数を表示するリンクをクリックします。
有効なインターフェイス数とデバイス上のインターフェイスの合計数 (モデルによって異なる) を比較した概要が表示されます。この例では、9 つのうち 3 つのインターフェイスが有効になっています。



- 配線したインターフェイスの行の右側にある [アクション (Actions)] セルの上にカーソルを移動し、編集アイコン (🔧) をクリックします。
- 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)] そのインターフェイスに固有の名前です。この例では、inside_2 です。

- [ステータス (Status)] : インターフェイスを有効にするには、ステータストグルをクリックします。
- [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、192.168.2.1/24 を入力します。

Edit Physical Interface

Interface Name Status

inside_2

Description

IPv4 Address IPv6 Address Advanced Options

Type IP Address and Subnet Mask

Static 192.168.2.1 / 24

- e) [保存 (Save)]をクリックします。
インターフェイスリストには、更新されたインターフェイスのステータスと設定された IP アドレスが表示されます。

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

- ステップ 2** インターフェイス向けに DHCP サーバを設定します。
- デバイス。
 - [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 Server)] 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向けにのサーバが 1 つ含まれています。
 - 表の上にある [+] をクリックします。
 - サーバのプロパティを設定します。
 - [DHCP サーバを有効にする (Enable DHCP Server)]サーバを有効にするには、このトグルをクリックします。

- [インターフェイス (Interface)] : DHCP サービスを提供す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)、ブロードキャストアドレス (.255) が含まれていないことを確認します。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、これらのアドレスをプールから除外します。プールは単一の連続した一連のアドレスである必要があるため、最初または最後の範囲からスタティック アドレスを選択します。

Add Server

Enabled DHCP Server

Interface

inside_2

Address Pool

192.168.2.2-192.168.2.254

e.g. 192.168.45.46-192.168.45.254

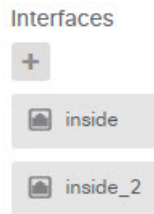
f) [追加 (Add)]をクリックします。

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

ステップ 3 セキュリティゾーンにインターフェイスを追加します。インターフェイスのポリシーを記述するには、そのインターフェイスが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ために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、自動的にインターフェイスに適用されたポリシーが変更されます。

- メインメニューの [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)]セルの上にカーソルを移動し、編集アイコン (🔍) をクリックします。

- d) [インターフェイス (Interfaces)]の下の [+] をクリックし、 **inside_2** インターフェイスを選択して、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。

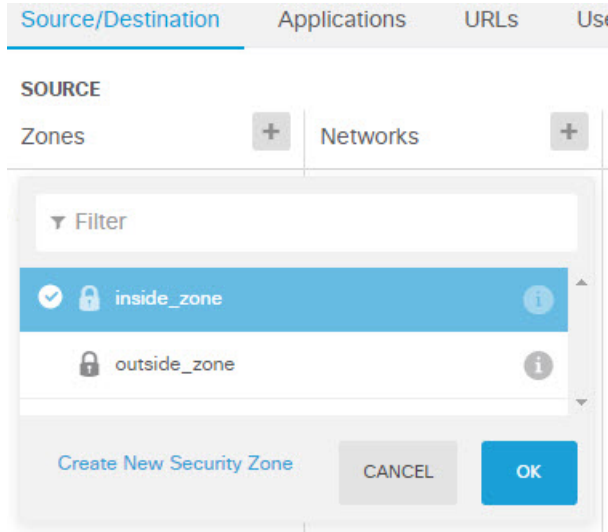
#	NAME	INTERFACES
1	inside_zone	inside, inside_2
2	outside_zone	outside

ステップ 4 内部ネットワーク間で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るわけではありません。必要な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する場合です。この例では、デバイスのセットアップウィザードで設定するブロックのデフォルトアクションを保持したと仮定します。そのため、内部インターフェイス間で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。すでにこのようなルールを作成している場合、この手順をスキップします。

- メインメニューの [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ていることを確認します。
- [+] をクリックして新しいルールを追加します。
- 順序、タイトル、およびアクションを設定します。
 - [順序 (Order)] : デフォルトでは、アクセス コントロール ポリシーの最後に新しいルールが追加されます。ただし、このルールは同じ送信元/接続先およびその他の条件に一致するルールの前に配置する必要があります。そうでない場合、ルールはいつまでも一致しなくなります (1つの接続で一致するのは1つのルールのみであり、それは表中で一致する最初のルールです)。このルールでは、固有の送信元/接続先条件を使用するため、リストの最後にルールを追加することは容認できません。
 - [タイトル (Title)] : ルールに **Allow_Inside_Inside** などのわかりやすい名前を付けます。
 - [アクション (Action)] : [許可 (Allow)] を選択します。

Order	Title	Action
4	Allow_Inside_Inside	

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



- e) 同じ方法を使用して、宛先[接続先 (Destination)]>[ゾーン (Zones)]に [inside_zone] を選択します。

送信元と接続先に同じゾーンを選択するには、セキュリティゾーンに少なくとも2つのインターフェイスが含まれている必要があります。

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

- 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されたゾーンにありますが、ユーザがラップトップをネットワークに接続することは一般的にあります。そのため、ユーザは知らずに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脅威をもたらす可能性があります。したがって、内部ネットワーク間で伝送されるトラフィックに対して、侵入およびマルウェアをスキャンすることができます。
次を行うことを検討します。

- [侵入ポリシー (Intrusion Policies)] タブをクリックして侵入ポリシーを有効にし、スライダを使用して [分散型のセキュリティと接続 (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、[マルウェアをすべてブロック (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、[ログアクションを選択 (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。
このルールに一致するすべての接続についての情報を取得するには、ロギングを有効にする必要があります。ロギングを行うと、ダッシュボードに統計情報が追加されるだけでなく、イベントビューアにイベントも表示されます。
- h) [OK] をクリックしてルールを保存します。

ステップ 5 必要なポリシーが新しいサブネットに定義されたことを確認します。
`inside_zone` セキュリティゾーンインターフェイスを追加すると、`inside_zone` のすべての既存ポリシーが新しいサブネットに自動的に適用されます。ただし、念のためポリシーのインスペクションを実行して、追加のポリシーが必要でないことを確認してください。

デバイスの初期設定が完了したら、次のポリシーがすでに適用されているはずです。

- [アクセス コントロール (Access Control)] : `Inside_Outside_Rule` は新しい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する必要があります。前の使用例に従うと、このポリシーでは侵入およびマルウェアのインスペクションも行います。新しいネットワークと外部ネットワーク間の幾つかのトラフィックを許可するルールを設定する必要があります。そうでないと、ユーザがインターネットまたはその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向かう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 を適用します。このルールを保持した場合、外部に向かう新しいネットワークからのトラフィックは、外部インターフェイスの IP アドレスの一意のポートに変換された IP アドレスを持つことになります。すべてのインターフェイス (または外部インターフェイスに向かう場合は `inside_zone` インターフェイス) に適用されるルールがない場合、もう 1 つルールを作成する必要があります。
- [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た場合、新しいネットワークの認証をすでに必要とするアイデンティティポリシーが存在す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、新しいネットワーク向けのユーザベースの情報が必要な場合は、ルールをもう 1 つ作成します。

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、展開が完了するまで待機します。

展開の概要には変更が正常に展開されたことが表示され、ジョブのタスクステータスは [展開済み (Deployed)] となります。

次の作業

新しい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、および内部ネットワークと外部ネットワークに相互に到達できることを確認します。ネットワークの使用状況を評価するには、モニタリング ダッシュボードとイベント ビューアを使用します。



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適用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, 71 ページ](#)
- [スマート ライセンスの管理, 74 ページ](#)

Firepower システムのスマート ライセンス

シスコスマートライセンスによって、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利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

加えて、スマートライセンスを使用しても、まだ購入していない製品機能を使用できなくなることはありません。Cisco Smart Software Managerに登録し、後でライセンスを購入する場合に限り、ライセンスの使用をすぐに開始できます。これにより、機能を展開して使用することができ、発注書の承認を待つ遅れることがなくなります。

Cisco Smart Software Manager

FirePOWER Threat Defenseデバイスに対する1つまたは複数のライセンスを購入する場合は、これらのライセンスを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、マスターアカウントの下位のデフォルトバーチャルアカウントにライセンスが割り当てられます。アカウントの管理者は、たとえば地域、部署、子会社などに対し、追加のバーチャルアカウントを作成できます。複数のバーチャルアカウントを使用することで、大量のライセンスおよびアプライアンスを管理しやすくなります。

ライセンスおよびアプライアンスは、バーチャルアカウントごとに管理されます。各バーチャルアカウントのアプライアンスは、それぞれのアカウントに割り当てられたライセンスのみを使用できます。追加のライセンスが必要になった場合は、未使用のライセンスを別のバーチャルア

ウントから転送できます。バーチャル アカウント間でアプライアンスを転送することもできます。

Cisco Smart Software Manager にデバイスを登録する際、製品インスタンスの登録トークンを作成し、このトークンを Firepower Device Manager に入力します。使用するトークンに基づき、登録したデバイスがバーチャル 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、オンライン ヘルプを参照してください。

License Authority との定期通信

製品インスタンス登録トークンを使用して FirePOWER Threat Defense デバイスを登録すると、そのデバイスは Cisco License Authority に登録されます。License Authority は、デバイスと License Authority の間の通信に使用する 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ると（通常、9 ヶ月または 1 年間通信がない場合）、デバイスは登録解除状態に戻り、ライセンス機能の使用は中断されます。

デバイスは License Authority と定期的に通信します。Cisco Smart Software Manager で変更を加えた場合は、デバイス上の認証を更新し、変更がすぐに反映されるようにします。あるいは、デバイスがスケジュールどおりに通信するのを待つこともできます。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、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 License Authority に連絡する必要があります。

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 2: 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	<p>オプションのタームライセンスでカバーされないすべての機能。</p> <p>[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）]かどうかも指定する必要があります。このオプションは、エクスポート制御基準に国が適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。</p>

ライセンス	期間	付与される機能
脅威 (Threat)	ターム ベース	<p>侵入検知および防御：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：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を必要とする AMP for Firepower は、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することができます。</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 AMP 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することができます。</p>
URL フィルタリング (URL Filtering)	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>

期限切れまたは無効なオプションライセンスの影響

オプションライセンスの期限が切れた場合でも、引き続きライセンスを必要とする機能を使用できます。ただし、ライセンスはコンプライアンス違反としてマークされるため、ライセンスを購入してアカウントに追加し、ライセンスをコンプライアンスの状態に戻す必要があります。

オプションライセンスを無効にすると、システムは次のように対応します。

- マルウェアライセンス (Malware license)：システムは AMP クラウドのクエリを停止し、AMP クラウドから送信されるレトロスペクティブ イベントの確認応答も停止します。既存のアクセスコントロールポリシーにマルウェアインスペクションを適用するファイルポリシーが含まれている場合、それら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化された後、ごく短時間のみ、システムが既存のキャッシュされた処理済みのファイル

を使用できる点に注意してください。その時間枠が経過すると、システムはそれらのファイルに使用不可 (Unavailable) の処理を割り当てます。

- 脅威 (Threat) : システムは侵入ポリシーまたはファイル制御ポリシーを適用しなくなります。ライセンスが必要な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 カテゴリ条件付きのアクセスコントロールルールは、即座に URL のフィルタリングを停止し、システムは URL データ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およびレピュテーションベースの URL 条件が含まれる場合、それらを再展開することはできません。

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確認するには、[スマートライセンス (Smart License)] ページを使用します。システムはライセンスされる必要があります。

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や、Cisco Smart Software Manager に登録している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と、各タイプのライセンスのステータスが表示されます。

[使用認証 (Usage Authorization)] では、Smart License Agent のステータスが識別されます。

- [承認済み (Authorized)] ([接続済み (Connected)], [十分なライセンス (Sufficient Licenses)]) : デバイスはライセンス認証局に正常にアクセスして登録されており、ライセンス認証局によってそのアプライアンスのライセンス付与が承認されています。デバイスは、現在、[コンプライアンス適合 (In-Compliance)] 状態です。
- [コンプライアンス不適合 (Out-of-Compliance)] : デバイスに使用可能なライセンス付与がありません。ライセンスされた機能は動作を継続します。ただし、コンプライアンス適合状態になるには追加の権限付与を購入するか解除する必要があります。
- [認証期限切れ (Authorization Expired)] : デバイスがライセンス認証局と通信せずに 90 日以上が経過しています。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、Smart License Agent は認証要求を再試行します。再試行に成功すると、エージェントはコンプライアンス不適合状態または承認済み状態になり、新しい認証期間が開始されます。デバイスの同期を手動で試みてください。



(注) [スマートライセンス (Smart License)] ステータスの横にある [i] ボタンをクリックして、仮想アカウントとエクスポート制御機能を表示し、Cisco Smart Software Manager を開くためのリンクを取得します。エクスポート規制機能により、国家安全保障、外交政策、および反テロリズムに関する法律と規制の対象となるソフトウェアが制御されます。

次の手順で、システムのライセンスを管理する方法の概要を示します。

手順

-
- ステップ 1** デバイスをクリックし、[スマート ライセンス (Smart License)] サマリの [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。
オプションのライセンスを割り当てるには、Cisco Smart Software Manager に登録する必要があります。評価期間が終了する前に登録してください。
[デバイスの登録, \(75 ページ\)](#) を参照してください。
- ステップ 3** オプションの機能ライセンスを要求して管理します。
ライセンスによって制御される機能を使用するには、オプションの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, \(76 ページ\)](#) を参照してください。
- ステップ 4** システムのライセンス付与を保持します。
次のタスクを実行できます。
- [Cisco Smart Software Manager との同期, \(77 ページ\)](#)
 - [デバイスの登録解除, \(77 ページ\)](#)
-

デバイスの登録

FirePOWER Threat Defense デバイスの購入には自動的に基本ライセンスが含まれます。基本ライセンスの対象は、オプションライセンスの対象になっていないすべての機能です。これは永久ライセンスです。

システムの初期セットアップ時に、Cisco Smart Software Manager によってデバイスを登録するように求められます。代わりに 90 日間の評価ライセンスの使用を選択した場合は、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、仮想アカウントによってライセンスがデバイスに割り当てられます。また、デバイスの登録により、有効にしたすべてのオプションライセンスも登録されます。

手順

-
- ステップ 1** デバイスをクリックし、[スマート ライセンス (Smart License)] サマリの [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** [登録の要求 (Request Register)] をクリックし、画面の指示に従います。
- a) リンクをクリックして [Cisco Smart Software Manager](#) を開き、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) 新しいトークンを作成します。

トークンを作成する際、トークンの有効な使用期間を指定します。推奨される有効期間は 30 日間です。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り、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。トークンを使用する前に期限切れになった場合は、単に新しいトークンを生成できます。

また、[このトークンで登録される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)] かどうかを指定する必要があります。このオプションは、製品を使用する国がエクスポート制御基準を満たしている場合にのみ選択できます。このオプションにより、高度な暗号化と高度な暗号化を必要とする機能の使用が制御されます。

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

オプションライセンスの有効化と無効化

オプションのライセンスを有効化 (登録) または無効化 (リリース) することができます。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することができます。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。

はじめる前に

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

手順

- ステップ 1** デバイスし、[スマートライセンス (Smart License)] サマリで [設定を表示 (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、展開できるようになります。

- [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を設定することも、その機能を使用するポリシーを展開することもできません。

Cisco Smart Software Manager との同期

ライセンス情報は、システムによって Cisco Smart Software Manager と定期的に同期されます。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。

ただし、Cisco Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、変更をすぐに反映させることができます。

同期では、ライセンスの現在のステータスを取得して、許可と ID 証明書を更新します。

手順

- ステップ1 デバイス[スマートライセンス (Smart License)] サマリの [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 [接続の再同期 (Resync Connection)] を選択します。

デバイスの登録解除

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

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

手順

- ステップ1 デバイス[スマートライセンス (Smart License)] サマリの [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 4 章

デバイスのモニタリング

システムには、デバイスおよび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のロギングの有効化](#), 79 ページ
- [トラフィックおよびシステムダッシュボードのモニタリング](#), 80 ページ
- [コマンドラインを使用した追加の統計のモニタリング](#), 83 ページ
- [イベントの表示](#), 83 ページ

トラフィック統計情報を取得するためのロギングの有効化

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、幅広い種類のトラフィック統計をモニタできます。これには、ロギングを有効にして、収集する統計の種類をシステムに指示する必要があります。

次のロギングタイプを個々のアクセスルールに対して有効化することで、オプションの統計情報が収集され、イベントが生成されます。

- **接続ロギング**：接続の終了時にロギングが行われるため、接続に関するほとんどの情報を取得できます。接続の開始時にロギングを行うこともできますが、これらのイベントで得られる情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡したいトラフィックを対象とする個々のルール（およびデフォルトアクション）に対し、接続ロギングを有効化する必要があります。
- **ファイルロギング**：検出されたファイルについての情報を収集するには、ファイルロギングを有効化する必要があります。アクセスルールでファイルポリシーを選択すると、ファイルロギングは自動的に有効化されますが、無効にすることもできます。

設定したロギングに加え、禁止されたファイルやマルウェアが検出された場合、または侵入が試みられた場合には、ほとんどの接続が自動的に記録されます（接続終了時）。ただし、デフォルト

トアクションによって対処される侵入イベントは例外です。これらの侵入イベントを確認するには、デフォルトアクションに対して接続ロギングを有効化する必要があります。

ヒント

ロギングの設定、および関連する統計情報の評価について検討する場合は、以下のヒントを参考にしてください。

- 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、さらにトラフィックをのインスペクションを実行し、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することができます。ただし、デフォルトでは、ファイルおよび侵入のインスペクションは暗号化されたペイロードでは無効になっていることに注意してください。侵入ポリシーまたはファイルポリシーに基づき、接続をブロックする根拠が得られた場合は、接続ログの設定にかかわらず、接続終了イベントがただちに記録されます。ロギングの許可された接続からは、ネットワーク内のトラフィックに関するほとんどの統計情報を収集できます。
- 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。しかし、信頼されている接続に対しては、ディスカバリ データ、侵入、禁止されたファイルやマルウェアのインスペクションは行われません。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したアクセス 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に対しては、接続開始イベントが自動的に記録されます。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）攻撃時にブロックされたTCP接続のロギングは、システムパフォーマンスに影響し、複数の類似のイベントでデータベースが圧倒される場合があります。ブロックルールに対してロギングを有効化する場合は、ルールによってインターネット側のインターフェイスを通過するトラフィックを監視するのか、またはDoS攻撃に対して脆弱な他のインターフェイスを監視するのかを事前に検討します。

トラフィックおよびシステムダッシュボードのモニタリング

システムには、デバイスを通過するトラフィックとセキュリティ ポリシーの結果を分析するために使用できるいくつかのダッシュボードが含まれています。この情報を使用して、設定の全体的な有効性を評価するとともに、ネットワークに関する問題を特定して解決します。



- (注) トラフィック関連のダッシュボードで使用されるデータは、接続またはファイル ロギングを可能にするアクセス コントロール ルールから収集されます。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に一致するトラフィックは反映されません。必ず、重要な情報がログに記録されるようにルールを設定してください。また、ユーザ情報は、ユーザ アイデンティティを収集するためのアイデンティティ ルールを設定する場合にのみ使用できます。最後に、侵入、ファイル、マルウェア、および Web カテゴリ情報は、それらの機能のライセンスがあり、それらの機能を使用するルールを設定する場合にのみ使用できます。

手順

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

定義済みの時間範囲 (過去 1 時間、過去 1 週間など) を選択するか、特定の開始時間と終了時間によるカスタム時間範囲を定義して、ダッシュボードのグラフとテーブルに表示されるデータを制御できます。

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あります。

- 上位 5 つの棒グラフ：これらは、[ネットワークの概要 (Network Overview)] ダッシュボードに表示され、ダッシュボードテーブルの項目をクリックすると表示される項目ごとの概要ダッシュボードにも表示されます。[トランザクション (Transactions)] の数と [データ使用量 (Data Usage)] (送受信された総バイト数) の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、拒否トランザクションの表示を切り替えることもできます。[詳細表示 (View More)] リンクをクリックすると、グラフに関連付けられたテーブルが表示されます。
- テーブル：テーブルには、特定タイプの項目 (アプリケーション、Web カテゴリなど) と、その項目の総トランザクション、許可トランザクション、ブロックトランザクション、データ使用量、および送受信されたバイト数が表示されます。未処理の [値 (Values)] と [パーセンテージ (Percentages)] パーセントの間で数値を切り替え、上位 10、100、または 1000 エントリを表示できます。項目がリンクの場合は、その項目をクリックすると、詳細情報を含む概要ダッシュボードが表示されます。

ステップ 2 コンテンツ テーブルの [ダッシュボード (Dashboard)] リンクをクリックすると、次のデータのダッシュボードが表示されます。

- [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概要情報 (一致したアクセスルール (ポリシー)、トラフィックを開始するユーザ、接続で使用されるアプリケーション、一致した侵入シグネチャ、アクセスされた URL の Web カテゴリ、接続の最も頻繁な宛先など) が表示されます。
- [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。

- [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 (Facebook など) が表示されます。この情報は、インスペクションが実行された接続についてのみ使用できます。接続は、それらが「許可」ルールや、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場合にインスペクションが実行されます。したがって、インスペクションが必要なルールに一致する前に接続が信頼されるかブロックされる場合は、アプリケーション情報を使用できません。
- [Web カテゴリ (Web Categories)] : アクセスした Web サイトの分類に基づいて、ネットワークで使用されている Web サイトの上位カテゴリ (ギャンブル、教育機関など) が表示されます。この情報を取得するには、トラフィック一致基準として Web カテゴリを使用する 1 つ以上のアクセスコントロールルールがある必要があります。この情報は、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が必要なトラフィックについて使用できます。最初の Web カテゴリ アクセスコントロールルールの前に照会されるルールに一致する接続のカテゴリ (またはレピュテーション) 情報は表示されません。
- [ポリシー (Policies)] : ネットワークトラフィックと一致した上位のアクセスルールが表示されます。
- [入力ゾーン (Ingress Zones)] : デバイスに入るトラフィックが通過した上位のセキュリティゾーンが表示されます。
- [出力ゾーン (Egress Zones)] : デバイスを出るトラフィックが通過した上位のセキュリティゾーンが表示されます。
- [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)] : 上位の攻撃者 (侵入イベントをトリガーする接続の送信元) が表示されます。この情報を表示するには、アクセスルールで侵入ポリシーを設定する必要があります。
- [ターゲット (Targets)] : 侵入イベントの上位のターゲット (攻撃の被害者) が表示されます。この情報を表示するには、アクセスルールで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、アクセスルールで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に見られる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、アクセスルールでファイルポリシーを設定する必要があります。
- [システム (System)] : システムの全体像 (インターフェイスとそのステータス (インターフェイスにマウスカーソルを合わせると IP アドレスが表示される) や全体的なシステムスループットに加え、システムイベント、CPU 使用率、メモリ使用率、およびディスク使用率に関する概要情報など) が表示されます。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が表示されるようにスループットのグラフを制限することができます。

(注) システム ダッシュボードに表示される情報は、システム全体のレベルです。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表示できます。たとえば、**show cpu** コマンドと **show memory** コマンドには追加の詳細情報を表示するためのパラメータがありますが、これらのダッシュボードには **show cpu system** コマンドと **show memory system** コマンドのデータが表示されます。

ステップ 3 コンテンツ テーブルの次のリンクをクリックすることもできます。

- [イベント (Events)]: 発生したイベントが表示されます。これらのルールに関連する接続イベントを表示するには、個々のアクセス ルールで接続ロギングを有効にする必要があります。これらのイベントは、ユーザの接続に関する問題を解決するために役立ちます。

コマンドラインを使用した追加の統計のモニタリング

Firepower デバイスマネージャのダッシュボードは、デバイスを経由するトラフィックと全般的なシステムの使用状況に関する広範な統計情報を提供します。ただし、デバイス CLI にログインすることで、ダッシュボードでカバーされていない領域の追加情報を取得できます ([コマンドライン インターフェイス \(CLI\) へのログイン](#), (8 ページ) を参照)。

CLI には、これらの統計情報を提供するためのさまざまな **show** コマンドが含まれています。また、**ping** や **traceroute** などのコマンドを含め、一般的なトラブルシューティングに CLI を使用することもできます。ほとんどの **show** コマンドには統計を 0 にリセットするための **clear** コマンドが付随しています。

コマンドの詳細については、『*Command Reference for Firepower Threat Defense*』 (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。

たとえば、次のコマンドは全般的に役立つ場合があります。

- **show nat** は、NAT ルールのヒット数を表示します。
- **show xlate** は、アクティブな実際の 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、インターフェイスに設定している 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

ロギングを有効化するアクセスルールから生成されたイベントを表示できます。また、イベントは、トリガーされた侵入ポリシーとファイル ポリシーから生成されます。

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

はじめる前に

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。
- 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：アクセスルールは、ファイル ポリシーを適用して、ファイル ロギングを有効化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](#)、(85 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。
 - 新しいイベントが表示される速さを制御するには、別の更新率 (5、10、20、または 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](#)、(86 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](#)、(88 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

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条件を作成することができます。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](#)、(87 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。

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。この情報に関連する統計情報をモニタリングダッシュボードに表示するには、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。接続イベントは、アクセスルールで接続のログギングを有効にしている場合のみに表示できます。

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のインスペクションを実行し、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。

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

ネットワークトラフィック内のマルウェア検出は、全体的なアクセスコントロール設定の一環として行われます。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。

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、イベントを表示すると目的の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、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 [カラムの追加または削除 (Add/Remove Columns)] リンクをクリックし、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](#)、(88 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

現在関心のあるイベントだけが表示されるように、複合的なフィルタを作成して、イベントテーブルの表示を制限できます。フィルタの作成には、以下の手法を単独で、またはいくつかを組み合わせることで使用できます。

列のクリック

最も簡単なフィルタ作成方法は、イベントテーブル内で、フィルタ処理の基準に使用したい値を持つセルをクリックすることです。セルをクリックすると、[フィルタ (Filter)] フィールドが更新され、この値とフィールドの組み合わせに対して適切に作成されたルールが入力されます。ただし、この手法は、既存のイベントリストに必要な値が含まれていることが前提となります。

すべての列をフィルタ処理することはできません。フィルタ処理可能なデータが含まれるセルでは、このセルにマウス オーバーすると、セルに下線が表示されます。

アトミック要素の選択

もう1つのフィルタ作成方法は、[フィルタ (Filter)] フィールド内をクリックして、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、一致する値を入力する方法です。これらの要素には、イベントテーブル内の列としては表示されないイベントフィールドが含まれます。また、入力した値と表示するイベントとの関係を定義するための演算子も含まれます。列をクリックする場合は、常に「等号 (=)」フィルタとなりますが、要素を選択する場合は、数値フィールドに対して「より大きい (>)」または「より小さい (<)」も選択できます。

どのような方法で要素を [フィルタ (Filter)] フィールドに追加する場合でも、フィールドに直接入力して、演算子や値を調整できます。[フィルタ (Filter)] をクリックすると、テーブルにフィルタが適用されます。

イベント フィルタの演算子

イベント フィルタには、以下の演算子を使用できます。

=	次の値と等しい。イベントは指定の値と一致します。ワイルドカードを使用することはできません。
!=	次の値と等しくない。イベントは指定の値と一致しません。不等号による式を作成するには、「! (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、指定の値より大きな値が含まれます。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、指定の値より小さな値が含まれます。この演算子は数値のみに使用できます。

複合イベント フィルタのルール

複数のアトミック要素を保持する複合フィルタを作成する場合は、以下のルールに注意します。

- 同じタイプの要素は、このタイプのすべての値が互いに「論理和 (OR)」の関係となります。たとえば、イニシエータ IP=10.100.10.10 とイニシエータ IP=10.100.10.11 を含めると、このどちらかのアドレスがトラフィック送信元となるイベントが適合します。
- 異なるタイプの要素は、「論理積 (AND)」の関係となります。たとえば、イニシエータ IP=10.100.10.10 と宛先ポート/ICMP タイプ=80 を含めると、この発信元アドレスを持ち、かつこの宛先ポートを持つイベントのみが適合します。10.100.10.10 から別の宛先ポートに向かうイベントは、表示されません。
- IPv4 および IPv6 アドレスなど、数値要素は範囲を指定できます。たとえば、宛先ポート=50-80 と指定すると、この範囲内のポートに送信されるすべてのトラフィックがキャプチャされます。範囲の開始値と終了値は、ハイフンでつなぎます。すべての数値フィールドで範囲を指定できるわけではありません。たとえば、送信元要素には、IP アドレス範囲を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

ここでは、各イベントに含めることのできる情報について説明します。この情報を読むには、イベントの詳細を表示します。また、関心の高い情報を表示する列をイベントビューアテーブルに追加することもできます。

以下に、使用可能なフィールドの一覧を示します。すべてのイベント タイプに対し、すべてのフィールドが適用されるわけではありません。それぞれのイベントで使用可能な情報は、システムが接続を記録する方法、理由、およびタイミングによって異なることに注意してください。

アクション (Action)

接続イベントにおいて、接続を記録したアクション コントロール ルールに関連付けられたアクション、またはデフォルトアクション。

許可 (Allow)

明示的に許可された接続。

信頼 (Trust)

信頼できる接続。信頼ルールによって最初のパケットで検出されたTCP接続は、接続終了イベントだけを生成します。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)

ブロックされた接続。以下の条件下で、ブロック (Block) アクションを許可 (Allow) アクセス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検出された接続。
- ファイル ポリシーによってファイルがブロックされた接続。

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状況。

ファイル イベントまたはマルウェア イベントの場合、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ているファイルルールアクションと、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付けられた、ビジネスとの関連性。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。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 (Application Categories)、アプリケーション タグ (Application Tag)

アプリケーションの機能を分かりやすくするため、アプリケーションの特徴付けに使用される基準。

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付けられたリスク。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。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。

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

接続で検出されたクライアント アプリケーションおよびクライアント 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付けられた、ビジネスとの関連性。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。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 (Client Category)、クライアント タグ (Client Tag)

アプリケーションの機能を分かりやすくするため、アプリケーションの特徴付けに使用される基準。

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付けられたリスク。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。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 (Destination IP)

受信ホストの IP アドレス。

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

セッション レスポンダによって使用されるポートまたは ICMP コード。

方向 (Direction)

ファイルの送信方向。

傾向 (Disposition)

ファイルの傾向。

マルウェア (Malware)

AMPクラウドによってファイルがマルウェアと分類されたか、またはファイルの脅威スコアがファイルポリシーに定義されたマルウェアのしきい値を超えたことを示します。

正常 (Clean)

AMPクラウドによってファイルが正常であると分類されたことを示します。

不明 (Unknown)

システムがAMPクラウドに問い合わせたが、ファイルに傾向が割り当てられていなかった（このファイルがAMPクラウドによって分類されていない）ことを意味します。

使用不可 (Unavailable)

システムによるAMPクラウドへの照会が失敗したことを示します。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

ファイル検出 (Detect Files) ルールまたはファイルブロック (Block Files) ルールによってこのファイルが処理され、AMPクラウドへの照会は行われませんでした。

出力インターフェイス (Egress Interface)、出力セキュリティゾーン (Egress Security Zone)

接続がデバイスを通る出口となるインターフェイスおよびゾーン。

イベント (Event)、イベントタイプ (Event Type)

イベントのタイプ。

イベントの秒数 (Event Seconds)、イベントのマイクロ秒数 (Event Microseconds)

イベントの検出時を表す秒単位またはマイクロ秒単位の値。

ファイルカテゴリ (File Category)

ファイルタイプの一般分類。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 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 ルールに関連付けられたアクション、および関連するすべてのファイル ルール アクション オプション。

ファイル SHA256 (File SHA256)

ファイルの SHA-256 ハッシュ値。

ファイル サイズ (KB) (File Size)

キロバイト単位のファイル サイズ。受信が完了する前にシステムによってブロックされたファイルの場合、ファイル サイズが空になることがあります。

ファイル タイプ (File Type)

ファイルの種類 (HTML、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。

ファイアウォール ポリシー ルール (Firewall Policy Rule) 、ファイアウォール ルール (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 URL のリファラを示す HTTP リファラ (他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど)。

HTTP 応答 (HTTP Response)

クライアントの HTTP 要求への応答として、接続上を送信された 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する分類。

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

接続がデバイスを通る入口となるインターフェイスおよびゾーン。

イニシエータのバイト数またはパケット数 (Initiator Bytes, Initiator Packets)

セッションイニシエータが送信したバイト数またはパケット数の合計。

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が属する国または大陸。イニシエータのIPアドレスがルーティング可能である場合にのみ使用可能です。

イニシエータ IP (Initiator IP)

セッションを開始したホストのIPアドレス (DNS解決が有効化されている場合はIPアドレスおよびホスト名)。

インライン結果 (Inline Result)

侵入イベントをトリガーさせたパケットが実際に破棄されたか、または、もしインラインモードで動作していたとしたら破棄されていたかどうか。空白の場合は、トリガーされたルールが「破棄およびイベント生成 (Drop and Generate Events)」に設定されていなかったことを意味します。

侵入ポリシー (Intrusion Policy)

イベントを生成させたルールが有効化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は、このイベントを説明するテキスト。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た何らかの補足情報。

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または大陸 (Original Client Country and Continent)

セッションを開始した元のクライアント ホストが属する国または大陸。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場合にのみ使用可能です。

元のクライアント IP (Original Client IP)

HTTP 接続を開始した元のクライアント IP アドレス。このアドレスは X-Forwarded-For (XFF) または True-Client-IP HTTP ヘッダー フィールド、またはこの同等フィールドから取得されます。

ポリシー (Policy) 、ポリシー リビジョン (Policy Revision)

イベントに関連付けられたアクセス (ファイアウォール) ルールが含まれるアクセス コントロールルールとそのリビジョン。

優先順位 (Priority)

Cisco Talos Security Intelligence and Research Group (Talos) によって決定されたイベントの優先順位。「高 (high)」、「中 (medium)」、「低 (low)」のいずれかとなります。

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。

理由 (Reason)

次の場合に接続がロギングされた 1 つまたは複数の原因。

理由	説明
ファイルブロック (File Block)	接続に、システムが送信を阻止するファイルまたはマルウェアファイルが含まれます。理由「ファイルブロック」は、常に「ブロック」アクションとペアになります。
ファイルモニタ (File Monitor)	接続内に特定のファイルタイプが検出されました。
ファイルの再開を許可 (File Resume Allow)	最初に、「ファイルまたはマルウェアファイルのブロック」ルールによってファイル伝送がブロックされました。このファイルを許可するアクセスコントロールポリシーが新たに展開された後、HTTPセッションが自動的に再開されました。
ファイルの再開をブロック (File Resume Block)	最初に、「ファイルまたはマルウェアクラウドルックアップファイルの検出」ルールによってファイル伝送が許可されました。このファイルをブロックするアクセスコントロールポリシーが新たに展開された後、HTTPセッションが自動的に停止されました。
侵入ブロック (Intrusion Block)	接続中に検出されたエクスプロイト (侵入ポリシー違反) が実際にブロックされたか、またはブロックされていたことが想定されるか。理由「侵入ブロック」は、エクスプロイトがブロックされた場合は「ブロック」、ブロックされていたことが想定される場合は「許可」アクションとペアになります。
侵入モニタ (Intrusion Monitor)	接続中のエクスプロイトが検出されましたが、ブロックされませんでした。これは、トリガーされた侵入ルールの状態が「イベントの生成 (Generate Events)」である場合です。

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)

接続に使用されたプロトコルが HTTP または HTTPS であれば、このフィールドには、それぞれのプロトコルが使用したホストの名前が表示されます。

レスポンドのバイト数またはパケット数 (Responder Bytes, Responder Packets)

セッション レスポンドが送信したバイト数またはパケット数の合計。

レスポンドの国または大陸 (Responder Country and Continent)

セッションに応答したホストが属する国または大陸。レスポンドの IP アドレスがルーティング可能である場合にのみ使用可能です。

レスポンド IP (Responder IP)

セッション レスポンドのホスト IP アドレス (DNS 解決が有効化されている場合は IP アドレスおよびホスト名)。

シグネチャ (Signature)

イベントのトラフィックと一致する侵入ルールのシグネチャ ID。

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

送信元ホストの国および大陸。送信元 IP アドレスがルーティング可能である場合にのみ使用可能です。

送信元 IP (Source IP)

侵入イベントで送信元ホストが使用する IP アドレス。

送信元のポート/ICMP タイプ (Source Port/ICMP Type) 、送信元ポート (Source Port) 、送信元ポート Itype (Source Port Itype)

セッション イニシエータに使用されるポートまたは ICMP タイプ。

TCP フラグ (TCP Flags)

接続で検出された TCP フラグ。

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

セッション中、モニタリングされているホストから要求された URL と、これに関連するカテゴリ、レピュテーション、レピュテーション スコア (ある場合)。

SSL アプリケーションが識別またはブロックされた場合は、要求された URL は暗号化トラフィックであり、このトラフィックは SSL 証明書に基づいて識別されます。したがって、SSL アプリケーションの場合は、URL は証明書内の共通名を表しています。

ユーザ (User)

イニシエータ 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付けられた、ビジネスとの関連性。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。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分かりやすくするため、Web アプリケーションの特徴付けに使用される基準。

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付けられたリスク。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。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 トラフィックに対応する、コンテンツまたは要求 URL を表す Web アプリケーション。

このイベントの URL に Web アプリケーションが一致しない場合は、このトラフィックは参照先トラフィック (広告トラフィックなど) を表していることが考えられます。参照先トラフィックが検出された場合は、参照元アプリケーション (存在する場合) が保管され、このアプリケーションが Web アプリケーションとしてリストされます。



第 5 章

オブジェクト

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

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

- [オブジェクトタイプ, 99 ページ](#)
- [オブジェクトの管理, 101 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、ポリシーや設定によりオブジェクトが許可されている場合は、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
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 オブジェクトでは、IP 接続で使用されるアプリケーション、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、ポリシーで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, (106 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
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では、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や大陸を定義します。IP アドレスを使用する代わりに、ポリシーで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, (110 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では、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の自動確立に使用される IKE プロポーザルを定義します。IKEv1 と IKEv2 には個別のオブジェクトがあります。 グローバルIKE ポリシーの設定, (300 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の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 には個別のオブジェクトがあります。 IPsec プロポーザルの設定, (305 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の設定。	ネットワークグループと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ぶ）では、ホストまたはネットワークのアドレスを定義します。 ネットワークオブジェクトとグループの設定, (102 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。	ポートグループとポートオブジェクト（総称してポートオブジェクトと呼ぶ）では、トラフィックのプロトコル、ポート、または ICMP サービスを定義します。 ポートオブジェクトとグループの設定, (103 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
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。ゾーンでネットワークを複数のセグメントに分割することで、トラフィックの管理と分類が容易になります。 セキュリティゾーンの設定, (105 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。	syslog サーバ 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特定します。 syslog サーバの設定, (111 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。	URL オブジェクトとグループ (総称して URL オブジェクトと呼ぶ) では、Web 要求の URL または IP アドレスを定義します。 URL オブジェクトとグループの設定, (109 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、ポリシーを編集するときに設定することもできます。どちらの方式でも同じ結果となり、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きにプロパティにオブジェクトが必要な場合は、すでに定義されているもののリストが表示されるため、適切なオブジェクトが選択してください。目的のオブジェクトがまだない場合は、リストに表示される [オブジェクトの新規作成 (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を示すコンテンツテーブルがあります。オブジェクトタイプを選択すると、既存のオブジェクトのリストが表示されます。

ここから新しいオブジェクトを作成することもできます。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 コンテンツ テーブルからオブジェクト 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。固有の情報については、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アイテムが含まれます。
- オブジェクトを編集するには、そのオブジェクトの編集アイコン () をクリックします。事前定義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アイコン () をクリックします。ポリシーまたは別のオブジェクトで現在使用中のオブジェクトを削除することはできません。また、事前定義オブジェクトも削除できません。

ネットワーク オブジェクトとグループの設定

ネットワーク グループとネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ぶ）を使用して、ホストまたはネットワークのアドレスを定義します。その後、オブジェクトは、トラフィックの一致基準を定義するためにセキュリティポリシーで使用したり、サーバやその他のリソースのアドレスを定義するための設定で使用したりできます。



ネットワーク オブジェクトで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 オブジェクトでは複数のアドレスを定義できます。

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。アドレスプロパティ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、[グループを追加 (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、オブジェクトのゴミ箱アイコン (🗑️) 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、任意で説明を入力して、オブジェクトの内容を定義します。

ネットワーク オブジェクト

オブジェクトの [タイプ (Type)] ([ネットワーク (Network)] または [ホスト (Host)]) を選択します。次に、ホストまたはネットワーク アドレスを入力します。次の形式を使用できます。

- IPv4 ホストアドレス (10.100.10.10 など)。
- 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)。
- IPv6 ホストアドレス (2001:DB8::0DB8:800:200C:417A、2001:DB8:0:0:0DB8:800:200C:417A 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)。

ネットワーク グループ

[+] ボタンをクリックして、グループに追加するネットワーク オブジェクトを選択します。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。

ポートオブジェクトとグループの設定

ポートグループとポートオブジェクト (総称してポートオブジェクトと呼ぶ) を使用して、トラフィックのプロトコル、ポート、または ICMP サービスを定義します。その後、オブジェクトは、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で使用したり、特定の TCP ポートへのトラフィックを許可するアクセスルールを使用するために使用したりできます。

ポートオブジェクトでは、単一のプロトコル、TCP/UDP ポートまたはポート範囲、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では複数のサービスを定義できます。

システムには共通サービスのための複数の定義済みオブジェクトが含まれています。それらのオブジェクトはユーザのポリシーで使用できます。ただし、システム定義オブジェクトの編集や削除はできません。





- (注) ポートグループオブジェクトを作成する場合は、意味のあるオブジェクトの組み合わせにしてください。たとえば、アクセスルールで送信元ポートと宛先ポートの両方を指定するために使用する場合、1つのオブジェクトにプロトコルを混在さ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。そのオブジェクトを使用するポリシーを無効にしてしまう可能性があります。


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。サービスプロパティを編集している間に、オブジェクトリストに表示される [ポートの新規作成 (Create New Port)] リンクをクリックして、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、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、[グループを追加 (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、オブジェクトのゴミ箱アイコン  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、任意で説明を入力して、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] : 単一ポートの番号またはポート範囲の番号を入力します。例、80 (HTTP の場合)、または 1 ~ 65535 (全ポートを対象にする場合)
- [ICMP]、[IPv6-ICMP] : ICMP [タイプ (Type)] を選択し、任意で [コード (Code)] を選択します。すべての ICMP メッセージに適用するタイプの場合は、[すべて (Any)] を選択します。タイプとコードの詳細については、次の各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

[+]ボタンをクリックして、グループに追加するポートオブジェクトを選択します。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は、インターフェイスのグループです。ゾーンでネットワークを複数のセグメントに分割することで、トラフィックの管理と分類が容易になります。複数のゾーンを定義できますが、特定のインターフェイスは1つのゾーンにのみ定義できます。

初期設定時に次のゾーンが作成されます。それらのゾーンを編集して、インターフェイスの追加や削除ができます。また、不要になったゾーンは削除できます。

- **[inside_zone]** : 内部インターフェイスが含まれています。内部インターフェイスがブリッジグループの場合、このゾーンには、内部の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。これは、内部ネットワークを表すためのゾーンです。
- **[outside_zone]** : 外部インターフェイスが含まれています。これは、ユーザの制御が及ばないネットワーク (インターネットなど) を表すためのゾーンです。

通常は、ネットワーク内での役割に応じてインターフェイスをグループ化します。たとえば、インターネットに接続するインターフェイスは **[outside_zone]** セキュリティゾーンに設定し、内部ネットワークのインターフェイスはすべて **[inside_zone]** セキュリティゾーンに設定します。次に、外部ゾーンから内部ゾーンに移動するトラフィックに対して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とその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設定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つのネットワークの扱いを他の3つのネットワークとは変えた場合は、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必要があ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は別のゾーンを使用することができます。

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。セキュリティゾーンプロパティを編集している間に、オブジェクトリストに表示される **[セキュリティゾーンの新規作成 (Create New Security Zone)]** リンクをクリックして、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、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、オブジェクトのゴミ箱アイコン (🗑️) 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、任意で説明を入力します。
- ステップ 4** [インターフェイス (Interfaces)] リストで [+] をクリックして、ゾーンに追加するインターフェイスを選択します。
- 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がリストに表示されます。インターフェイスはゾーンに追加する前に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含まれている場合、リストは空です。インターフェイスを別のゾーンに移動する場合は、まず現在のゾーンからそのインターフェイスを削除する必要があります。
- (注) ブリッジグループインターフェイス (BVI) をゾーンに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。メンバーは異なるゾーンに含めることができます。
- ステップ 5** [OK] をクリックして変更を保存します。

アプリケーションフィルタ オブジェクトの設定

アプリケーションフィルタオブジェクトは、IP接続で使用されるアプリケーション、または、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。ポート仕様を使用する代わりに、ポリシーで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。

個々のアプリケーションを指定することもできますが、アプリケーションフィルタを使用するとポリシーの作成と管理が簡素化されます。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。ユーザがそれらのアプリケーションの1つを使用しようとする、セッションがブロックされず。

アプリケーションフィルタオブジェクトを使用することなく、ポリシーで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、アプリケーションフィルタの同じグループに対して複数のポリシーを作成する場合は、オブジェクトを使用した方が便利です。システム

には、編集または削除できない複数の事前定義されたアプリケーションフィルタが含まれています。



(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、高リスクのアプリケーションをブロックするルールは、ルールを手動で更新する必要なく、新しいアプリケーションに自動的に適用できます。

次の手順では、[オブジェクト (Objects)] ページを通じて、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。[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)] をクリックすることで、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 オブジェクトを作成できます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [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、オブジェクトのゴミ箱アイコン (🗑️) 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、任意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+)] をクリックして、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。初期リストでは、絶えずスクロールしているリストにアプリケーションが表示されます。[高度なフィルタ (Advanced Filter)] をクリックして、フィルタ オプションを表示し、アプリケーションを選択するための見やすいビューを表示します。選択したら、[追加 (Add)] をクリックします。プロセスを繰り返して、アプリケーションまたはフィルタを追加します。

(注) 単一のフィルタ条件内で選択された複数の項目は、互いに「論理和 (OR)」の関係となります。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、条件を満たすものだけが表示されるように、画面のアプリケーションリストが更新されます。これらのフィルタを使用すると、個別に追加しようとするアプリケーションを特定したり、ルールに追加する必要のあるフィルタが選択されているか確認する場合に役立ちます。

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おそれのある目的で使用される可能性。「非常に低い (Very Low)」～「非常に高い (Very High)」。

ビジネスとの関連性

娯楽としてではなく、組織の事業運営のコンテキスト内でアプリケーションが使用される可能性。「非常に低い (Very Low)」～「非常に高い (Very High)」。

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：HTTP や SSH など、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：Web ブラウザや電子メールクライアントなど、ホスト上で実行され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：MPEG ビデオや Facebook など、HTTP トラフィックのコンテンツ、または要求された URL を表す 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

アプリケーションの補足情報。カテゴリに似ています。

暗号化トラフィックに対しては、SSL プロトコルのタグが付いたアプリケーションだけを使用するトラフィックが識別およびフィルタ処理されます。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（暗号化トラフィックまたは暗号化されていないトラフィックではなく）復号トラフィックのみで検出できるアプリケーションに対し、復号トラフィックタグを割り当てます。

アプリケーション リスト (画面下部)

このリストは、リスト上のオプションからフィルタを選択すると更新されます。したがって、現時点でフィルタに一致するアプリケーションを確認できます。このリストを使用すると、フィルタ条件をルールに追加する場合、必要なアプリケーションがフィルタのターゲットとなっているかどうかを確認できます。特定のアプリケーションを追加するには、このリストから選択します。

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 コントロール ポリシーで手動フィルタリングを実装することができます。

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。

- ネットワーク トラフィックが URL 条件に一致するかどうか判断するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の一部に一致すると、URL が一致したと見なされます。したがって、`example.com` は、`www.example.com` や `ads.example.com` など、そのネットワーク上の任意のホストに一致します。また、`badexample.com` と一致します。
- URL 条件を含むアクセス コントロールルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィック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。






(注) 特定のサイトをターゲットとする URL オブジェクトを設定する前に、アクセス コントロールの章に記載されている URL のフィルタリングに関する情報をよく確認してください。URL のマッチングは想定されるようには行われなため、意図せずにサイトをブロックしてしまう可能性があります。たとえば、ゲーム サイト `ign.com` を明示的にブロックしようとする、`verisign.com`、およびその他の「ign」で終わる任意のサイトもブロックしてしまいます。

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 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、[グループを追加 (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、オブジェクトのゴミ箱アイコン () をクリックします。

ステップ 3 オブジェクトの名前、さらに任意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では、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や大陸を定義します。IP アドレスを使用する代わりに、ポリシーで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。たとえば、地理的な場所を使用して、その国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。

通常は、地理位置情報オブジェクトを使用しなくても、ポリシーで地理的な場所を直接選択できます。ただし、同じグループの国や大陸に対して複数のポリシーを作成する場合はオブジェクトの使用が便利です。



(注) 最新の地理的な場所のデータを使用してトラフィックをフィルタ処理するためには、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。ネットワークプロパティを編集している間に、オブジェクトリストに表示される [地理位置情報の新規作成 (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、オブジェクトのゴミ箱アイコン (🗑️) 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、任意で説明を入力します。

ステップ 4 [大陸と国 (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と国を選択します。

大陸を選択すると、その大陸にある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特定します。ログ収集と分析用の syslog サーバをセットアップしている場合は、ログ収集と分析を定義するためのオブジェクトを作成し、アクセスルールまたは診断ロギングシステムの設定でそれらのオブジェクトを使用します。システムロギングの設定の詳細については、次のトピックを参照してください。

- [ロギングの設定, \(182 ページ\)](#)
- [診断ロギングの設定, \(321 ページ\)](#)

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。syslog サーバプロパティを編集している間に、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)] リンクをクリックして、syslog サーバ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 [syslog サーバ (Syslog Servers)] 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、オブジェクトのゴミ箱アイコン (🗑️) をクリックします。

ステップ 3 syslog サーバのプロパティを設定します。

- [デバイス インターフェイス (Device Interface)] : syslog サーバにアクセスするインターフェイスを選択します。ブリッジ グループ メンバー インターフェイスからサーバにアクセスできる場合は、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。
- [IP アドレス (IP Address)] : syslog サーバの IP アドレスを入力します。
- [ポート (Port)] : サーバが syslog メッセージの受信に使用する UDP ポートを入力します。デフォルトは 514 です。

ステップ 4 [OK] をクリックして変更を保存します。



第 **■** 部

基本

- [インターフェイス, 115 ページ](#)
- [ルーティング, 137 ページ](#)



第 6 章

インターフェイス

ここでは、Firepower Threat Defenseのインターフェイスを設定する方法について説明します。

- [Firepower Threat Defenseインターフェイスについて](#), 115 ページ
- [インターフェイスの設定](#), 121 ページ
- [モニタリングインターフェイス](#), 134 ページ

Firepower Threat Defenseインターフェイスについて

Firepower Threat Defenseデバイスには、データ インターフェイスの他、管理インターフェイスと診断インターフェイスが含まれます。以下の各トピックでは、Firepower Device Manager を使用してインターフェイスを設定する場合の制限事項、およびインターフェイス管理に関するその他の概念について説明します。

インターフェイス設定の制約

Firepower デバイスマネージャを使用してデバイスを設定する場合は、インターフェイスの設定に関するいくつかの制約があります。次の機能のいずれかが必要な場合は、Firepower Management Centerを使用してデバイスを設定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ています。トランスペアレントファイアウォールモードインターフェイスは設定できません。
- IPS専用モードはサポートされていません。IPS専用処理向けにインターフェイスをインライン、インラインタップ、パッシブまたはERSPANに設定することはできません。IPS専用モードインターフェイスは、多数のファイアウォール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。比較すると、ファイアウォールモードインターフェイスは、フローの維持、IP層とTCP層の両方でのフロー状態の追跡、IPの最適化、TCPの正規化などのファイアウォール機能の対象となるトラフィックを処理します。オプションで、このファイアウォールモードトラフィックのIPS機能をセキュリティポリシーに従って設定できます。

- EtherChannel または冗長インターフェイスは設定できません。
- IPv4 対応の PPPoE は設定できません。インターネットインターフェイスが DSL、ケーブルモデム、またはその他の接続を介して ISP に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、Firepower Management Center を使用してこれらの設定を行う必要があります。
- ASA 5512-X、5515-X、5525-X、5545-X および 5555-X の場合は、オプションのネットワークインターフェイスカード (EPM) を装着できます。カードはブートストラップの間にのみ検出されます (つまり、インストール中、ローカル/リモート管理の切り替え時、およびメジャー/マイナー リリース アップグレード中)。SFP インターフェイスが組み込まれたカードの場合、Firepower デバイスマネージャは、速度とデュプレックスを自動 (auto) に設定します。ただし、SFP インターフェイスは自動に設定された速度とデュプレックスをサポートしていません。速度とデュプレックスは、手動で設定する必要があります。速度を 1000、デュプレックスを Full に設定してから、設定を展開します。リンクが起動しない場合は、別の速度を試行します。

データ インターフェイス

以下のタイプのインターフェイスを設定できます。

ルーテッド

個々のレイヤ 3 ルーテッドインターフェイス (またはサブインターフェイス) には、一意のサブネットの IP アドレスが必要です。通常、このタイプのインターフェイスはスイッチ、別のルータのポート、または ISP/WAN ゲートウェイに接続します。

スタティック アドレスを割り当てることも、DHCP サーバからアドレスを取得することもできます。しかし、デバイス上で静的に定義されたインターフェイスと同じサブネットのアドレスが DHCP サーバによって提供された場合は、DHCP インターフェイスが無効になります。DHCP を使用してアドレスを取得しているインターフェイスがトラフィックの通過を停止している場合は、アドレスがデバイス上の別のインターフェイスのサブネットと重複していないかどうかを確認してください。

ブリッジ

ブリッジグループは、ルータではなく Firepower Threat Defense デバイスによってブリッジされるインターフェイスグループです。ブリッジされる各インターフェイスは1つのブリッジグループに属し、すべてのインターフェイスは同一ネットワークに属します。ブリッジグループは、ブリッジネットワーク上の単一の 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 を指定して、ルーテッドインターフェイスと BVI 間をルーティングできます。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 を指定しないと、ブリッジグループのメンバーインターフェイス上のトラフィックは、ブリッジグループの外に出ることができません。通常、メンバーインターフェイスをインターネットにルーティングすることのできるインターフェイスを指定します。

ルーテッドモードでブリッジグループを使用する例として、外部スイッチではなく、Firepower Threat Defense デバイスの予備のインターフェイスを使用できます。エンドポイントは、ブリッジグループのメンバーインターフェイスに直接接続できます。また、スイッチを接続して、BVI と同じネットワークにさらに多くのエンドポイントを追加することもできます。

ルーテッドインターフェイスと BVI のどちらにも、IPv6 および IPv4 アドレスを設定できます。IPv6 と IPv4 の両方で、デフォルトルートを設定してください。ブリッジグループのメンバーインターフェイスには、アドレスを設定しません。

IPv6 アドレッシング

IPv6 では、2 タイプ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できるパブリックアドレスです。ブリッジグループの場合は、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) にグローバルアドレスを設定します。グローバルアドレスとして次のいずれかを指定することはできません。
 - 内部的に予約された IPv6 アドレス：fd00:: - 未指定のアドレス：:: - ループバックアドレス：::1/128
 - マルチキャストアドレス：ff00:: - リンクローカルアドレス：fe80::
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークでのみ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しません。これらのアドレスは、特定の物理ネットワークセグメントでの通信専用です。アドレス設定、またはアドレス解決やネイバー探索などネットワーク検出機能で使用できます。ブリッジグループでは、BVI で IPv6 を有効にすると、各ブリッジグループメンバーの

インターフェイスのリンクローカルアドレスが自動的に設定されます。リンクローカルアドレスはセグメントでのみ使用可能であり、インターフェイス MAC アドレスに結合されているため、各インターフェイスは専用のアドレスを保持する必要があります。

IPv6 を動作させるには、少なくとも 1 つの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は自動的にインターフェイスに設定されます。そのため、特に、リンクローカルアドレスを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または手動のいずれかで設定する必要があります。

管理/診断インターフェイス

Management とラベル付けされた物理ポートには、実際は 2 つの個別のインターフェイスが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用に使用したり、データベース更新を取得するために使用したりするアドレスです。このアドレスへの管理セッションを開くことができます（Firepower デバイス マネージャまたは 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、Diagnostic という名前が付けられています。このインターフェイスは、外部 syslog サーバへの syslog メッセージを送信するために使用できます。診断物理インターフェイスの IP アドレスの設定はオプションです。このインターフェイスを syslog 用に使用する場合にはのみ、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、トラフィックの通過は許可しません。

管理/診断を設定するための推奨方法は、物理ポートをネットワークに配線しないことです。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を取得す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。その後、HTTPS/SSH トラフィックへの内部インターフェイス（デフォルトでは、HTTPS は有効）を開き、内部 IP アドレスを使用して Firepower デバイス マネージャを開きます（[管理アクセス リストの設定](#)、[319 ページ](#)）を参照）。

個別の管理ネットワークを設定するための推奨事項

個別の管理ネットワークを使用する場合は、管理/診断用物理インターフェイスをスイッチまたはルータに有線接続します。

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、接続されているネットワークに IPv4 または IPv6 アドレス（あるいは両方）を設定します。必要に応じて、ネットワーク上のその他のエンドポイントに IPv4 アドレスを提供するように DHCP サーバを設定できます。管理ネットワーク上

のインターネットへのルートがあるルータが存在する場合、そのルータをゲートウェイとして使用します。それ以外の場合は、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。

- インターフェイス経由で syslog サーバに syslog メッセージを送信する場合のみ、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)])。それ以外の場合は、不要なので診断インターフェイスのアドレスは設定しないでください。設定する IP アドレスはすべて、管理 IP アドレスと同じサブネット上のアドレスである必要があり、DHCP サーバプールのアドレスは指定できません。たとえば、デフォルト設定で 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場合、192.168.45.1 ~ 192.168.45.44 の任意のアドレスを使用して診断インターフェイスを設定できます。

個別管理ネットワークの管理/診断インターフェイス設定の制限事項

物理的な管理インターフェイスを配線する場合、以下の制限事項に注意してください。

- 管理ネットワークで DHCP サーバを使用する場合は、DHCP サーバを管理インターフェイスに設定します ([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)])。DHCP サーバを診断 (物理) インターフェイスに設定することはできません。
- 管理ネットワークに別の DHCP サーバが存在する場合は、この DHCP サーバ、または管理インターフェイス上で実行されている DHCP サーバを無効にします。規則として、1 つのサブネットでは 1 つの DHCP サーバしか使用できません。
- 管理インターフェイスおよび診断インターフェイスの両方にアドレスを設定する場合は、どちらも同じサブネット上にあることを確認します。
- 診断インターフェイスの IP アドレスを設定した場合であっても、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では、データインターフェイスはゲートウェイとして使用されません。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となる場合は、管理ネットワーク上の別のルータによって、診断 IP アドレスから送信された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)] 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。たとえば、内部から外部へのトラフィックは有効にして、外部から内部へは有効にしないアクセスコントロールポリシーを設定できます。

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。

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 機能も含まれます。Auto-MDI/MDIX 機能は、自動ネゴシエーション フェーズでストレート ケーブルが検出された場合に、内部クロスオーバーを実行します。したがって、クロスオーバー配線が不要になります。インターフェイスに対して Auto-MDI/MDIX 機能を有効にするには、速度またはデュプレックスのいずれかを自動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設定して、両方の設定の自動ネゴシエーションを無効にすると、Auto-MDI/MDIX も無効になります。ギガビット イーサネットの場合は、速度を 1000 に、デュプレックスを全二重に設定すると、インターフェイスでは常に自動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、無効にすることができなくなります。

MTU について

MTU は、Firepower Threat Defense デバイスがイーサネット インターフェイス上で送信可能な最大のフレーム ペイロード サイズを指定します。MTU 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む 1518 バイト、または VLAN を使用する場合は 1522 バイトとなります。これらのヘッダーも収容できるように、過度に大きな値を MTU に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、パス MTU ディスカバリ (RFC 1191 に規定) 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 とフラグメンテーション

IPv4 の場合、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。フラグメントは送信先 (場合によっては中継先) で組立て直されますが、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 の場合、通常、パケットのフラグメント化は許可されません。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、フラグメンテーションを回避するためにアプリケーションで MTU を考慮する必要があります。



(注) Firepower Threat Defense デバイスはメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

MTU とジャンボ フレーム

大きな MTU はより大きなパケットを送信できます。パケットが大きくなると、ネットワークの効率性が向上することがあります。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**：トラフィック パス内のすべての Firepower Threat Defense デバイス インターフェイスとその他のデバイスのインターフェイスの MTU を同じサイズ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 ヘッダーと 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、MTU は最大で 9198 バイトに設定できます。



(注) MTU のサイズを増やすと、ジャンボフレームに割り当てるメモリが増え、その他の機能（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 デバイスのデフォルト値の 1500 よりも MTU のサイズを大きくする場合は、システムを再起動する必要があります。

インターフェイスの設定

インターフェイスにケーブルを接続する場合は、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。このインターフェイスがブリッジグループのメンバーであれば、設定はこれで十分です。ブリッジグループのメンバーでない場合は、インターフェイスに IP アドレスも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を特定のポートに設定するのではなく、VLAN サブインターフェイスを作成する場合は、通常は物理インターフェイスではなくサブインターフェイスに 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、それぞれ異なる 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。

インターフェイスリストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。インターフェイスの状態（オンまたはオフ）は、インターフェイスリスト内で直接変更できます。リストには、設定に基づいたインターフェイス特性が表示されます。ブリッジグループ インターフェイスのオープン/クローズ矢印を使用すると、メンバー インターフェイスを表示できます。メンバー インターフェイスは、リスト内に単独でも表示されます。

ポート図を使用して、インターフェイスの現在の状態をモニタします。ポートの上にマウスを合わせると、そのIPアドレス、およびイネーブルステータスやリンクステータスが表示されます。IPアドレスはDHCPを使用してスタティックに割り当てたり、取得できます。

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：インターフェイスが設定され、イネーブルで、リンクが稼働中です。
- 灰色：インターフェイスがイネーブルではありません。
- オレンジ/赤：インターフェイスが設定され、イネーブルですが、リンクがダウンしています。インターフェイスが有線接続である場合、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接続でない場合、これは予想される状態です。

以下の各トピックでは、インターフェイスを設定する方法について説明します。

物理インターフェイスの設定

少なくとも、物理インターフェイスをイネーブルにし、使用できるようにする必要があります。また、通常は物理インターフェイスの名前を指定し、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作成する場合、またはブリッジグループにインターフェイスを追加する場合は、IPアドレッシングを設定しません。



(注) ブリッジグループのメンバーインターフェイスにはIPアドレスは設定できませんが、必要に応じて、詳細設定を変更できます。

インターフェイスをディセーブルにして、接続されたネットワークへの伝送を一時的に禁止することができます。インターフェイスの設定を削除する必要はありません。

手順

ステップ 1 デバイスをクリックし、[インターフェイス (Interfaces)] 概要ページのリンクをクリックします。インターフェイスリストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。

ステップ 2 編集する物理インターフェイスの編集アイコン (🔍) をクリックします。

ステップ 3 インターフェイスをイネーブルにするには、[ステータス (Status)] > [オン (On)] をクリックします。

この物理インターフェイスにサブインターフェイスを設定しようとする段階では、多くの場合、設定は完了です。[保存 (Save)] をクリックし、[VLANサブインターフェイスと802.1Qトランキングの設定 \(125 ページ\)](#) に進みます。それ以外の場合は、続行します。

(注) サブインターフェイスを設定する場合でも、インターフェイスに名前を付け、IPアドレスを割り当てることは有効です。これは一般的な設定ではありませんが、必要に応じて設定できます。

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。英字は小文字である必要があります。たとえば、「inside」や「outside」などの名前を使用します。名前を設定しない場合は、残りのインターフェイス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を設定する必要があります。

(注) 名前を変更すると、セキュリティゾーン、syslog サーバオブジェクト、および DHCP サーバの定義を含む、古い名前を使用したすべての場所にその変更が自動的に反映されます。ただし、一般に名前の付いていないインターフェイスをポリシーや設定に使用できないため、名前を削除するには、まず、その使用するすべての設定を削除する必要があります。

- (オプション) [説明 (Description)] : 説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 [IPv4 アドレス (IPv4 Address)] タブをクリックし、IPv4 アドレスを設定します。
[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [ダイナミック (Dynamic)] (DHCP) : ネットワーク上の DHCP サーバからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて次のオプションを変更します。

◦ [ルートメトリック (Route Metric)] : DHCP サーバからデフォルトルートを取得する場合、学習された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 です。デフォルトは 1 です。

◦ [デフォルトルートの取得 (Obtain Default Route)] : DHCP サーバからデフォルトルートを取得するかどうか。通常、このオプションをオン (デフォルト) にします。

- [スタティック (Static)] : 変更しないアドレスを割り当てる場合は、このオプションをオンにします。インターフェイスの IP アドレスと、インターフェイスに接続されるネットワークの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。そのアドレスがまだネットワークで使用されていないことを確認してください。

(注) 既存のインターフェイスの場合、そのインターフェイス用に DHCP サーバが設定されているときは、アドレスを変更する機能が制限されます。新しい IP アドレスは、DHCP アドレスプールと同じサブネット上にある必要があります。また、このアドレスをそのプールに含めることはできません。異なるサブネット上にアドレスを設定する必要がある場合は、最初に DHCP サーバの設定を削除します。 [DHCP サーバの設定](#), (322 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、IPv6 アドレスを設定します。

- [状態 (State)] : IPv6 処理を有効にして、グローバルアドレスを設定しないときにリンクローカルアドレスを自動設定するには、[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 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、IPv6 アドレスが明示的に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での IPv6 処理は無効になりません。

- [アドレス自動設定 (Address Auto Configuration)]: アドレスを自動的に設定させるには、このオプションをオンにします。IPv6 ステートレス自動設定は、デバイスが存在するリンクで使用するグローバルな IPv6 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 アドレスを生成します。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカルな IPv6 アドレスのみが取得され、そのデバイスが属すネットワーク リンクの外部に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に基づきます。

RFC 4862 では、ステートレスな自動設定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していますが、Firepower Threat Defense デバイスはこの場合、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、RFC に準拠させるには、[RA の抑制 (Suppress RA)] を選択します。

- [スタティック アドレス/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は、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 と指定します。IPv6 アドレッシングの詳細については、[IPv6 アドレッシング](#)、(117 ページ) を参照してください。

アドレスをリンクローカルとしてのみ使用する場合は、[リンクローカル (Link - Local)] オプションをオンにします。リンクローカルアドレスはローカル ネットワークの外部にはアクセスできません。ブリッジグループ インターフェイスではリンクローカルアドレスを設定できません。

(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。たとえば fe80::20d:88ff:feec:6a82 のようになります。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、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

- [RA の抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうか。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、各 IPv6 対応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送信要求メッセージに応答して送信されます (ICMPv6 Type 133)。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、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を行うことができます。

Firepower Threat Defense 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) [高度なインターフェイス オプションの設定](#)、(132 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。

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、それぞれ異なる 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。



(注) ブリッジグループのメンバーインターフェイスには IP アドレスは設定できませんが、必要に応じて、詳細設定を変更できます。

はじめる前に

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イネーブル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。

手順

ステップ 1 デバイスをクリックし、[インターフェイス (Interfaces)] 概要ページのリンクをクリックします。インターフェイスリストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。サブインターフェイスは、それぞれの物理インターフェイスの下位にグループ化されます。

ステップ 2 次のいずれかを実行します。

- 歯車のドロップダウンリストから [サブインターフェイスの追加 (Add Subinterface)] を選択し、サブインターフェイスを新規作成します。
- 編集するサブインターフェイスの編集アイコン (🔍) をクリックします。

サブインターフェイスが不要になった場合は、このサブインターフェイスの削除アイコン (🗑️) をクリックして削除します。

ステップ 3 インターフェイスをイネーブルにするには、[ステータス (Status)] > [オン (On)] をクリックします。

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。

- [親インターフェイス (Parent Interface)] : サブインターフェイスを追加する物理インターフェイスを選択します。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。
- [名前 (Name)] : 最大 48 文字のサブインターフェイスの名前。英字は小文字である必要があります。たとえば、「inside」や「outside」などの名前を使用します。名前を設定しない場合は、残りのインターフェイス設定は無視されます。
 - (注) 名前を変更すると、セキュリティゾーン、syslog サーバ オブジェクト、および DHCP サーバの定義を含む、古い名前を使用したすべての場所にその変更が自動的に反映されます。ただし、一般に名前の付いていないインターフェイスをポリシーや設定に使用できないため、名前を削除するには、まず、その使用するすべての設定を削除する必要があります。
- (オプション) [説明 (Description)] : 説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 サブインターフェイスの一般的な特性を設定します。

- [VLAN ID] : VLAN ID を 1 ~ 4094 の範囲で入力します。これは、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されます。
- [サブインターフェイス ID (Subinterface ID)] : 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。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。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 6 [IPv4 アドレス (IPv4 Address)] タブをクリックし、IPv4 アドレスを設定します。
[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [ダイナミック (Dynamic)] (DHCP) : ネットワーク上の DHCP サーバからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて次のオプションを変更します。
 - [ルート メトリック (Route Metric)] : DHCP サーバからデフォルト ルートを取得する場合、学習された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 です。デフォルトは 1 です。
 - [デフォルト ルートの取得 (Obtain Default Route)] : DHCP サーバからデフォルト ルートを取得するかどうか。通常、このオプションをオン (デフォルト) にします。
- [スタティック (Static)] : 変更しないアドレスを割り当てる場合は、このオプションをオンにします。インターフェイスの IP アドレスと、インターフェイスに接続されるネットワークのサブネット 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。そのアドレスがまだネットワークで使用されていないことを確認してください。

- (注) 既存のインターフェイスの場合、そのインターフェイス用に DHCP サーバが設定されているときは、アドレスを変更する機能が制限されます。新しい IP アドレスは、DHCP アドレス プールと同じサブネット上にある必要があります。また、このアドレスをそのプールに含めることはできません。異なるサブネット上にアドレスを設定する必要がある場合は、最初に DHCP サーバの設定を削除します。DHCP サーバの設定、(322 ページ) を参照してください。

ステップ 7 (オプション) [IPv6 アドレス (IPv6 Address)] タブをクリックし、IPv6 アドレスを設定します。

- [状態 (State)] : IPv6 処理を有効にして、グローバルアドレスを設定しないときにリンクローカルアドレスを自動設定するには、[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 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、IPv6 アドレスが明示的に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での IPv6 処理は無効になりません。

- [アドレス自動設定 (Address Auto Configuration)] : アドレスを自動的に設定させるには、このオプションをオンにします。IPv6 ステートレス自動設定は、デバイスが存在するリンクで使用するグローバルな IPv6 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 アドレスを生成しません。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカルな IPv6 アドレスのみが取得され、そのデバイスが属すネットワーク リンクの外部に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 に基づきます。

RFC 4862 では、ステートレスな自動設定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していますが、Firepower Threat Defense デバイスはこの場合、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、RFC に準拠させるには、[RA の抑制 (Suppress RA)] を選択します。

- [スタティック アドレス/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は、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 と指定します。IPv6 アドレッシングの詳細については、IPv6 アドレッシング、(117 ページ) を参照してください。

アドレスをリンクローカルとしてのみ使用する場合は、[リンクローカル (Link - Local)] オプションをオンにします。リンクローカルアドレスはローカル ネットワークの外部にはアクセスできません。ブリッジ グループ インターフェイスではリンクローカルアドレスを設定できません。

(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。たとえば fe80::20d:88ff:feec:6a82 のようになります。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、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

- [RA の抑制 (Suppress RA)] : ルータ アドバタイズメントを抑制するかどうか。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、各 IPv6 対応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送信要求メッセージに回答して送信されます (ICMPv6 Type 133)。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、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を行うことができます。

Firepower Threat Defense 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 8 (オプション) [高度なインターフェイス オプションの設定, \(132 ページ\)](#) .

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 9 [OK]をクリックします。

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した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です。これにより、ワークステーションまたは他のエンドポイントデバイスを、ブリッジグループ内のインターフェイスに直接接続できます。個別の物理スイッチを経由して接続する必要はありません。ただし、ブリッジグループメンバーにスイッチを接続することも可能です。

各グループメンバーは、IPアドレスを持ちません。代わりに、すべてのメンバーインターフェイスは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、各メンバーインターフェイスには自動的に、一意のリンクローカルアドレスが割り当てられます。

通常は、ブリッジグループ インターフェイス (BVI) には DHCP サーバを設定します。これにより、メンバーインターフェイスを介して接続されたすべてのエンドポイントに、IP アドレスが提供されます。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たエンドポイントにスタティックアドレスを設定することもできます。ブリッジグループ内のすべてのエンドポイントは、ブリッジグループの IP アドレスと同じサブネット上の IP アドレスを持つ必要があります。



- (注) すべてのASA 5506-Xモデルでは、新バージョンの6.2+システム、またはイメージを再作成した6.2+システムにおいて、デバイスにはあらかじめBVII「inside」と名前の付いたブリッジグループが設定されています。これには、「outside」インターフェイス以外のすべてのデータインターフェイスが含まれます。したがって、デバイスにはインターネット、またはその他のアップストリームネットワークへのリンクに使用される1つのポートが事前に設定されています。また、他のすべてのポートも有効であり、エンドポイントを直接接続できます。新しいサブネット内で内部インターフェイスを使用するには、まず、必要なインターフェイスをBVIIから削除する必要があります。

はじめる前に

ブリッジグループのメンバーと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す必要があります。

- インターフェイスには名前が必要です。
- スタティックアドレスであっても、DHCP経由であっても、インターフェイスに何らかのIPv4またはIPv6アドレスを定義することはできません。現在使用中の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、アドレスを保持するインターフェイスの種類に応じて、スタティックルート、DHCPサーバ、NATルールなど、インターフェイスの他の設定も削除しなければならない可能性があります。
- インターフェイスをブリッジグループに追加するには、このインターフェイスをセキュリティゾーンから削除し（ゾーンに属している場合）、インターフェイスに設定されていたすべてのNATルールを削除しておく必要があります。

また、各メンバーインターフェイスは個別に有効化および無効化します。これにより、未使用のインターフェイスを、ブリッジグループから削除することなく無効にできます。ブリッジグループ自体は常に有効です。

手順

- ステップ 1** [デバイス (Device)] をクリックして、[インターフェイス (Interfaces)] 概要ページのリンクをクリックします。
- インターフェイスリストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。ブリッジグループがすでに存在する場合は、フォルダとして表示されます。オープン/クローズ矢印をクリックすると、メンバーインターフェイスを表示できます。また、リストには個別のメンバーインターフェイスも表示されます。
- ステップ 2** 次のいずれかを実行します。
- BVIIブリッジグループの編集アイコン (🔗) をクリックします。
 - 歯車のドロップダウンリストから [ブリッジグループ インターフェイスの追加 (Add Bridge Group Interface)] を選択し、新規グループを作成します。

(注) 使用できるのは1つのブリッジグループのみです。すでにブリッジグループを定義している場合は、新たなグループを新規作成するのではなく、既存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、既存のブリッジグループを事前に削除しておく必要があります。

- 不要になったブリッジグループを削除する場合は、削除アイコン (🗑️) をクリックします。ブリッジグループを削除すると、このグループの各メンバーは標準的なルーテッドインターフェイスとなり、すべての NAT ルールまたはセキュリティゾーンメンバーシップは維持されます。各インターフェイスを編集して、それぞれの IP アドレスを指定できます。新しいブリッジグループにインターフェイスを追加するには、まず、NAT ルールを削除し、セキュリティゾーンからこのインターフェイスを削除する必要があります。

ステップ 3 以下を設定します。

- [インターフェイス名 (Interface Name)] : 最大 48 文字のブリッジグループの名前。英字は小文字である必要があります。たとえば、「inside」や「outside」などの名前を使用します。名前を設定しない場合は、残りのインターフェイス設定は無視されます。
 - (注) 名前を変更すると、セキュリティゾーン、syslog サーバオブジェクト、および DHCP サーバの定義を含む、古い名前を使用したすべての場所にその変更が自動的に反映されます。ただし、一般に名前の付いていないインターフェイスをポリシーや設定に使用できないため、名前を削除するには、まず、その使用するすべての設定を削除する必要があります。
- (オプション) [説明 (Description)] : 説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 4 ブリッジグループのメンバー リストを編集します。 1つのブリッジグループには、最大 64 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。

- [+]をクリックして、インターフェイスを追加します。
- インターフェイスを削除するには、インターフェイス上にマウス オーバーし、右側の [x] をクリックします。

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、次のオプションのいずれかを選択します。

- [スタティック (Static)] : 変更されることのないアドレスを割り当てるには、このオプションを選択します。ブリッジグループの IP アドレスおよびサブネット マスクを入力します。接続されるすべてのエンドポイントは、このネットワークに接続されます。ASA 5506-X モデルでは、BVII の inside ネットワークはデフォルトで 192.168.1.1/24 (つまり 255.255.255.0) となります。このアドレスが、ネットワーク上でまだ未使用であることを確認します。

(注) 既存のブリッジグループでは、グループに DHCP サーバを設定している場合、アドレスの変更に制限が生じます。新しい IP アドレスは、DHCP アドレスプールと同じサブネット上でなければならず、このプールの一部にすることはできません。別のサブネットにアドレスを設定する必要がある場合は、まず、DHCP サーバの設定を削除します。DHCP サーバの設定、(322 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場合は、このオプションを選択します。これはブリッジグループの一般的なオプションではありませんが、必要に応じて設定できます。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)] : デフォルトルートを DHCP サーバから取得する場合の、学習したルートまでのアドミニストレーティブディスタンス (1 ~ 255) 。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)] : DHCP サーバからデフォルトルートを取得するかどうか。デフォルトではオンであり、通常はこのオプションを選択します。

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、IPv6 アドレスを設定します。

- [状態 (State)] : IPv6 処理を有効にして、グローバルアドレスを設定しないときにリンクローカルアドレスを自動設定するには、[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 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、IPv6 アドレスが明示的に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での IPv6 処理は無効になりません。

- [スタティックアドレス/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は、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 と指定します。IPv6 アドレッシングの詳細については、IPv6 アドレッシング、(117 ページ) を参照してください。

アドレスをリンクローカルとしてのみ使用する場合は、[リンクローカル (Link - Local)] オプションをオンにします。リンクローカルアドレス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。ブリッジグループインターフェイスではリンクローカルアドレスを設定できません。

(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。たとえば fe80::20d:88ff:feec:6a82 のようになります。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、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

- [RA の抑制 (Suppress RA)] : ルータアドバタイズメントを抑制するかどうか。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、各 IPv6 対応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送信要求メッセージに応答して送信されます (ICMPv6 Type 133)。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、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を行うことができます。

Firepower Threat Defense 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) [高度なインターフェイス オプションの設定, \(132 ページ\)](#) .

ブリッジ グループのメンバー インターフェイスにはほとんどの詳細オプションを設定できますが、いくつかの詳細オプションはブリッジ グループ インターフェイスにも設定できます。

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。

次の作業

- 使用するすべてのメンバー インターフェイスが有効化され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, \(322 ページ\)](#) 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, \(105 ページ\)](#) を参照してください。
- アイデンティティ ポリシー、NAT ポリシー、アクセス ポリシーなどのポリシーが、ブリッジ グループおよびメンバー インターフェイスに必要なサービスを供給することを確認してください。

高度なインターフェイス オプションの設定

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する場合のみ設定を行います。

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。

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 の試行を除き、これらのオプションをブリッジ仮想インターフェイス (BVI) に設定することはできません。

手順

- ステップ 1** デバイスをクリックし、[インターフェイス (Interfaces)] 概要ページのリンクをクリックします。インターフェイスリストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。
- ステップ 2** 編集するインターフェイスの編集アイコン (🔗) をクリックします。
- ステップ 3** [詳細オプション (Advanced Options)] タブをクリックします。
- ステップ 4** データインターフェイスを管理専用指定する場合は、[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 5** [MTU] (最大伝送ユニット) を任意の値に設定します。
デフォルトの MTU は 1500 バイトです。64 ~ 9198 の値を指定できます (Firepower Threat Defense Virtual の場合は最大値が 9000)。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 に対して MTU を 1500 以上に設定した場合は、デバイスをリブートする必要があります。CLI にログインし、**reboot** コマンドを使用します。
- ステップ 6** (物理インターフェイスのみ) 速度およびデュプレックスの設定を変更します。
デフォルトでは、インターフェイスは接続相手のインターフェイスに対し、互いに最適なデュプレックスおよび速度をネゴシエートしますが、必要に応じて、特定のデュプレックスおよび速度を強制的に適用することもできます。
- [デュプレックス (Duplex)] : [全二重 (Full)]、[半二重 (Half)]、または [自動 (Auto)] のいずれかを選択します。デフォルトは [自動 (Auto)] です。
 - [速度 (Speed)] : [10]、[100]、[1000]、[10000] Mbps、または [自動 (Auto)] を選択します。デフォルトは [自動 (Auto)] です。
- ステップ 7** [IPv6 設定 (IPv6 Configuration)] を変更します。
- [IPv6 アドレス設定で DHCP を有効化する (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 のアドレス以外の設定で DHCP を有効化する (Enable DHCP for IPv6 non-address configuration)] : IPv6 ルータのアドバタイズメントパケットに、その他のアクセス設定フラグを設定するかどうか。このフラグは、DHCPv6 から DNS サーバアドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。
 - [DAD の試行 (DAD Attempts)] : インターネット上で重複アドレス検出 (DAD) を実行する頻度 (0 ~ 600)。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD はアドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性

を検証します。重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上でIPv6パケットの処理はディセーブルになります。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) プロセスをディセーブルにするには、この値を **0** に設定します。

ステップ 8 [OK]をクリックします。

モニタリングインターフェイス

次のエリアで、インターフェイスに関する基本情報を表示できます。

- [モニタリング (Monitoring)] > [システム (System)]。[スループット (Throughput)] ダッシュボードはシステムを経由するトラフィックに関する情報を表示します。すべてのインターフェイスに関する情報を表示することもできれば、特定のインターフェイスを選択して調べることもできます。
- [モニタリング (Monitoring)] > [入力ゾーン (Ingress Zones)] および [出力ゾーン (Egress Zones)]。これらのダッシュボードは、インターフェイスで構成されたゾーンに基づく統計情報を表示します。この情報はさらに詳細な情報へ掘り下げることができます。
- [デバイス (Device)]。[接続図 (Connection Diagram)] には、インターフェイスのステータスが表示されます。ポートをマウスオーバーすると、インターフェイスの IP アドレス、インターフェイスの状態およびリンクステートが表示されます。この情報を使用すると、稼働している必要があるときにダウンしているインターフェイスを識別するために役立ちます。

CLI でのインターフェイスのモニタリング

デバイス CLI にログインし、次のコマンドを使用して、インターフェイス関連の動作と統計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、必要な情報を取得するために使用できる多数のキーワードがあります。使用可能なオプションを確認するには、? 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、メンバー情報と IP アドレスを含む、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ます。
- **show conn** は、インターフェイスを通じて現在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経由するトラフィックに関する統計情報を表示します。
- **show ipv6 traffic** は、デバイスを經由する IPv6 トラフィック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、特に、インターフェイスに設定された DHCP サーバに関する統計情報とその他の情報を表示します。



第 7 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、ルーティングの概要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, 137 ページ](#)
- [スタティック ルートの設定, 139 ページ](#)
- [ルーティングのモニタリング, 140 ページ](#)

ルーティングの概要

次に、Firepower Threat Defenseデバイス内でルーティングがどのように動作するかを示します。ルーティングは、送信元から宛先にネットワーク経路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、インターネットワーク経路で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。

NAT がルート選択に及ぼす影響

Firepower Threat Defenseは、ルーティングを決定するために、ルーティングテーブルとネットワークアドレス変換 (NAT) XLATE (変換) テーブルの両方を使用します。宛先 IP 変換対象トラフィック、つまり、未変換のトラフィックを処理するために、システムは既存の XLATE またはスタティック変換を検索して、出力インターフェイスを選択します。

選択プロセスは、次の手順に従っています。

- 1 宛先 IP 変換 XLATE がすでに存在する場合、出力インターフェイスはルーティングテーブルではなく、XLATE テーブルから決定されます。
- 2 宛先 IP 変換 XLATE が存在しないが、一致するスタティック NAT 変換が存在する場合は、出力インターフェイスはスタティック NAT ルールから決定され、XLATE が作成され、ルーティングテーブルは使用されません。

- 3 宛先 IP 変換 XLATE が存在せず、一致するスタティック変換がない場合は、パケットの宛先 IP は変換されません。システムは、出力インターフェイスを選択するためにルートをルックアップしてこのパケットを処理し、その後、送信元 IP 変換が実行されます（必要な場合）。

正規のダイナミックアウトバウンド NAT の場合、初期発信パケットはルートテーブルを使用してルーティングされ、その後、XLATE が作成されます。着信リターンパケットは、既存の XLATE のみを使用して転送されます。スタティック NAT の場合、宛先変換済みの着信パケットは常に、既存の XLATE またはスタティック変換ルールを使用して転送されます。

出力インターフェイスの選択後、選択した出力インターフェイスに属する適切なネクストホップを見つけるために、追加のルートルックアップが実行されます。ルーティングテーブルに、選択したインターフェイスに明示的に属するルートがないと、異なる出力インターフェイスに属する所定の宛先ネットワークへの別のルートが存在する場合でも、パケットはドロップされ、レベル 6 診断 syslog メッセージ 110001（ホストへのルートがない）が生成されます。選択した出力インターフェイスに属するルートが見つかった場合は、パケットは対応するネクストホップに転送されます。

ルーティングテーブルとルートの選択

NAT XLATEs とルールによって出力インターフェイスが決定されない場合、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、特定のルートに相対的な優先順位を提供する、「アドミニストレーティブディスタンス」と呼ばれる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に一致する場合、ディスタンスが最小のものが使用されます。直接接続ネットワーク（インターフェイスで定義されるもの）のディスタンスは 0 であるため、常に優先されます。スタティックルートのデフォルトディスタンスは 1 ですが、1 ~ 254 までの任意のディスタンスでそれらを作成できます。

特定の宛先を識別するルートは、デフォルトルート（宛先が 0.0.0.0/0 である）よりも優先されません。

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たインターフェイスを介して転送されます。デフォルトルートが設定されていない場合、パケットは廃棄されます。
- 宛先がルーティングテーブル内の単一のエントリと一致する場合、パケットはそのルートに関連付けられたインターフェイスを介して転送されます。
- 宛先がルーティングテーブル内の複数のエントリに一致する場合、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た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内の次のルートのインターフェイスに到達したものとします。

- 192.168.32.0/24 ゲートウェイ 10.1.1.2
- 192.168.32.0/19 ゲートウェイ 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にダイレクトされます。ルーティングテーブル内の他のルートにも含まれますが、192.168.32.0/24がルーティングテーブル内で最長のプレフィックスを保持しています（24ビット対19ビット）。パケットを転送する場合は、より長いプレフィックスがより短いプレフィックスより常に優先されます。



(注) ルートの変更のために新しい類似の接続が異なる動作をする場合でも、既存の接続は継続して確立済みのインターフェイスを使用します。

スタティックルートの設定

スタティックルートを定義して、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にバインドされていないパケットの送信先をシステムに知らせます。

少なくとも1つのスタティックルートが必要です。ネットワークのデフォルトルートは0.0.0.0/0です。このルートで、既存のNAT Xlates（変換）、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決定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すべてのネットワークに到達できない場合は、他のスタティックルートが必要な場合があります。たとえば、通常、デフォルトルートは外部インターフェイスの上流に位置するルータを通過します。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、デフォルトゲートウェイを介してそれらのネットワークにアクセスできない場合、それらの各内部ネットワークのスタティックルートが必要です。

システム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スタティックルートは定義できません。それらのルートはシステムによって自動的に作成されます。

手順

ステップ1 デバイス、[ルーティング (Routing)] サマリでリンクをクリックします。

ステップ2 [スタティックルーティング (Static 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、[+] > [スタティックルートの追加 (Add Static Route)] 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場合は、削除するルートのごみ箱アイコンをクリックします。

ステップ 3 ルートのプロパティを設定します。

[プロトコル (Protocol)]

ルートが [IPv4] アドレス用か、 [IPv6] アドレス用かを選択します。

[ゲートウェイ (Gateway)]

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。

[インターフェイス (Interface)]

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できる必要があります。

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。

[メトリック (Metric)]

ルートのアドミニストレーティブ ディスタンス (1 ~ 254)。スタティック ルートのデフォルトは 1 です。インターフェイスとゲートウェイの間に追加のルータがある場合、アドミニストレーティブ ディスタンスとしてホップの数を入力します。

アドミニストレーティブ ディスタンスは、ルートの比較に使用されるパラメータです。低い番号の方がそのルートに与えられる優先順位が高くなります。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、常にスタティック ルートよりも優先されます。

[ネットワーク (Network)]

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、任意の定義済み ipv4 または ipv6 ネットワーク オブジェクトを使用するか、0.0.0.0/0 (IPv4) ネットワークまたは ::/0 (IPv6) ネットワークのオブジェクトを作成します。

ステップ 4 [OK] をクリックします。

ルーティングのモニタリング

ルーティングをモニタしてトラブルシューティングするには、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** : 直接接続ネットワークのルートを含む、データ インターフェイスのルーティング テーブルが表示されます。

- **show ipv6 route** : 直接接続ネットワークのルートを含む、データ インターフェイスの IPv6 ルーティング テーブルが表示されます。
- **show network** : 管理ゲートウェイを含む、仮想管理インターフェイスの設定が表示されます。仮想インターフェイス経由のルーティングは、データ インターフェイスを管理ゲートウェイとして指定している場合を除き、データ インターフェイスのルーティング テーブルでは処理されません。
- **show network-static-routes** : **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用に設定されているスタティックルートが表示されます。通常、ほとんどの場合のルーティングは管理ゲートウェイで管理できるため、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。



第 **II** 部

セキュリティポリシー

- [アイデンティティポリシー](#), 145 ページ
- [アクセスコントロール](#), 163 ページ
- [ネットワークアドレス変換 \(NAT\)](#), 189 ページ



第 8 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。

- [アイデンティティポリシーの概要, 145 ページ](#)
- [アイデンティティポリシーの設定, 149 ページ](#)
- [トランスペアレントユーザ認証のイネーブル化, 157 ページ](#)
- [アイデンティティポリシーのモニタリング, 161 ページ](#)

アイデンティティポリシーの概要

アイデンティティポリシーを使用して、接続に関連付けられているユーザを検出できます。ユーザを特定することで、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アイデンティティ情報に関連付けることができます。ネットワークの行動、トラフィックおよびイベントを直接個々のユーザにリンクすることで、システムは、ユーザがポリシー違反、攻撃またはネットワーク脆弱性の元を特定できるように助長します。

たとえば、誰が侵入イベントによって標的とされたホストを所有しているか、誰が内部攻撃またはポートスキャンを開始したかなどを特定できます。また、帯域幅使用率の高い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も特定できます。

ユーザ検出では、分析用のデータ収集以上のことができます。ユーザ名またはユーザグループ名に基づいてアクセスルールを記述し、ユーザ認証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することもできます。



(注) システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、特定のホストにログインするユーザは一度に1人だけであり、ホストの現在のユーザが最後の権限のあるユーザログインであると見なします。複数のユーザがリモートセッションを通じてログインしている場合は、サーバによってレポートされた最後のユーザがユーザとみなされます。

アクティブ認証によるユーザ アイデンティティの確立

認証は、ユーザのアイデンティティを確認する手段です。

アクティブな認証では、ユーザ アイデンティティのマッピングが確認できない IP アドレスから HTTP トラフィック フローが送信されてきた場合、システムに設定したディレクトリに照会して、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決定できます。このユーザが認証に成功すると、この IP アドレスは、認証したユーザのアイデンティティを持つとみなされます。

認証に失敗しただけでは、このユーザのネットワーク アクセスは禁止されません。このようなユーザに許可されるアクセスの種類は、事前に指定したアクセスルールによって最終的に決定されます。

ユーザ数の上限

Firepower デバイス マネージャは、最大 2000 ユーザに関する情報をディレクトリ サーバからダウンロードできます。

ディレクトリ サーバに 2000 を超えるユーザ アカウントが含まれており、アクセス ルールでユーザを選択したか、ユーザベースのダッシュボード情報を表示した場合、候補となるすべての名前は表示されません。ダウンロードされた名前に対してのみルールを記述できます。

2000 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。1つのグループに 2000 を超えるメンバーがいる場合、ダウンロードされた 2000 のみの名前をグループ メンバーシップに対して照合できます。

2000 ユーザを超える場合は、Firepower デバイス マネージャではなく、Firepower Management Center (リモート マネージャ) の使用を検討してください。Firepower Management Center は、極めて多数のユーザをサポートします。

サポートされるディレクトリ サーバ

Windows Server 2008 および 2012 の Microsoft Active Directory (AD) をアイデンティティ ポリシーに使用できます。

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。
- システムが該当するフィールドのサーバからユーザ メタデータを取得するには、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する必要があります。

メタデータ	Active Directory フィールド
LDAP user name	samaccountname
first name	givenname

メタデータ	Active Directory フィールド
last name	sn
email address	mail userprincipalname (mail に値が設定されていない場合)
department	department distinguishedname (department に値が設定されていない場合)
telephone number	telephonenumber

ディレクトリ ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名 (DN) を指定する必要があります。ベースはディレクトリ サーバ内で定義され、ネットワークごとに異なります。アイデンティティポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。



ヒント

正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory での正しいベースを確認するには、ドメイン管理者として Active Directory サーバにログインし、以下に示すようにコマンドプロンプトで **dsquery** コマンドを実行して、ベースを判断します。

ユーザ検索ベース

既知のユーザ名 (一部または完全) を使用して **dsquery user** コマンドを入力し、ベース識別名を判断します。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

既知のグループ名を使用して、**dsquery group** コマンドを入力し、ベース識別名を判断します。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]> [ファイル名を指定して実行]> [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。

不明なユーザの処理

アイデンティティ ポリシー用にディレクトリ サーバを設定すると、ユーザおよびグループメンバーシップの情報がディレクトリ サーバからダウンロードされます。この情報は午前 0 時から 24 時間ごと、またはディレクトリの設定を編集および保存する都度 (変更を何も加えなかった場合も同様) 更新されます。

アクティブな認証アイデンティティ ルールの要求する認証に成功したユーザであっても、ダウンロードされたユーザ アイデンティティ 情報内にこのユーザの名前が含まれていない場合は、このユーザは「不明」とマークされます。アイデンティティ 関連のダッシュボードにはこのユーザの ID は表示されず、このユーザはグループ ルールにも一致しません。

代わりに、不明ユーザを対象としたすべてのアクセスコントロールルールが適用されます。たとえば、不明ユーザの接続をブロックするように設定している場合は、認証に成功したユーザ (ディレクトリ サーバに認識され、パスワードも有効であるユーザ) であっても、不明ユーザとみなされればブロックされます。

したがって、ユーザの追加や削除、またはグループ メンバーシップの変更など、ディレクトリ サーバに何らかの変更を加えた場合は、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は反映されません。

毎日の午前0時の更新時まで待機することが難しい場合は、ディレクトリサーバ情報を編集することで、更新を強制的に適用できます（[ポリシー（Policies）]>[アイデンティティ（Identity）]を選択して[ディレクトリサーバ（Directory Server）]ボタンをクリック）。[保存（Save）]をクリックして、変更を展開します。更新情報がただちにダウンロードされます。





- (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。新規ユーザが表示されない場合、または削除したはずのユーザが表示される場合は、システム上の情報が古いことを意味します。



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からユーザアイデンティティを取得するために必要な要素の設定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。
まだアイデンティティポリシーを定義していない場合は、ウィザードを開始して設定するように求められます。[開始（Get Started）]をクリックしてウィザードを開始します。ウィザードでは次の手順を実行します。
- ディレクトリサーバの設定、（150 ページ）
 - アクティブ認証キャプティブポータルの設定、（151 ページ）
- ステップ2** アイデンティティポリシーを管理します。
アイデンティティの設定を行うと、このページにすべてのルールが順番に表示されます。ルールが上から下の順番でトラフィックと照合され、最初に一致したルールによって適用するアクションが決まります。このページから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。
 - ディレクトリサーバの設定を変更するには、[ディレクトリサーバ（Directory Server）]ボタン（) をクリックします。
 - アクティブ認証のキャプティブポータルの設定を変更するには、[アクティブ認証（Active Authentication）]ボタン（) をクリックします。
 - 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には、そのルールの編集アイコン () をクリックします。また、テーブルでプロパティをクリックしてルールのプロパティを選択的に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には、そのルールの削除アイコン () をクリックします。

アイデンティティルールの作成と編集の詳細については、[アイデンティティルールの設定](#)、(153 ページ) を参照してください。

ディレクトリ サーバの設定


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たユーザおよびユーザグループについての情報が保存されます。システムは毎日深夜11時 (UTC) に、すべてのユーザおよび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の各プロパティを設定するための必要な値については、ディレクトリの管理者に相談してください。



- (注) レルムを追加した後は、設定を確認し、接続をテストできます。これには、[ディレクトリサーバ (Directory Server)] ボタンをクリックし、[ディレクトリサーバ (Directory Server)] ダイアログボックスの[テスト (Test)] ボタンをクリックします。テストに失敗した場合は、すべてのフィールドを検証し、管理 IP アドレスとディレクトリサーバ間にネットワークパスが確立されていることを確認します。

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** 次のいずれかを実行します。
- ディレクトリまたはアイデンティティルールが未設定である場合は、[開始 (Get Started)] をクリックして、アイデンティティポリシー ウィザードを開始します。最初に、ディレクトリサーバを設定するように求められます。
 - [ディレクトリサーバ (Directory Server)] ボタン () をクリックします。
- ステップ 3** ディレクトリサーバについて、以下の情報を指定します。
- 名前 (Name) : ディレクトリレルムの名前。

- **タイプ (Type)** : ディレクトリ サーバのタイプ。Active Directory が唯一サポートされているタイプであり、このフィールドは変更できません。
- **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する適切な権限を持つユーザの識別ユーザ名とパスワード。たとえば、admin@ad.example.com。
- **ベース DN (Base DN)** : ユーザおよびグループ情報を検索またはクエリするためのディレクトリ ツリー、つまり、ユーザとグループの共通の親。たとえば、dc=example、dc=com。ベース DN の検索方法の詳細については、[ディレクトリ ベースの DN の決定](#)、(147 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。
- **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している場合は、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されるポート番号。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情報をダウンロードするために暗号化された接続を使用するには、目的の方式 [STARTTLS] または [LDAPS] を選択します。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ることを意味します。
 - [STARTTLS] は、暗号化方式をネゴシエートして、ディレクトリ サーバによってサポートされている最強の方式を使用します。ポート 389 を使用します。
 - [LDAPS] には、LDAP over SSL が必要です。ポート 636 を使用します。
- **SSL 証明書 (SSL Certificate)** : 暗号化方式を選択する場合は、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するため、CA 証明書をアップロードします。証明書を使用して認証している場合は、証明書のサーバ名がサーバのホスト名/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、証明書内で ad.example.com を使用した場合は、接続が失敗します。

ステップ 4 [次へ (Next)] (ウィザード内) または [保存 (Save)] をクリックします。

アクティブ認証キャプティブ ポータルの設定

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。証明書をアップロードしない場合、ユーザには自己署名証明書が提示されます。すでにユーザのブラウザが信頼している証明書がアップロードされていない場合、ユーザはその証明書を受け入れる必要があります。




- (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 ネゴシエートの場合は、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は、DNS サーバも更新して、アクティブな認証が必要な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必要があります。そうしないと、リダイレクションが完了できず、ユーザは認証できません。

はじめる前に

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るが、たとえば、10 AM PST = 1 PM EST など、時刻がそれらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

- ステップ 1** [ポリシー (Policies)] > [アイデンティティ (Identity)] を選択します。
- ステップ 2** 次のいずれかを実行します。
- 開始 (Get Started) ウィザードを使用する場合は、ディレクトリ サーバを設定後に、[次へ (Next)] をクリックします。
 - [アクティブ認証 (Active Authentication)] ボタン () をクリックします。
- ステップ 3** 次のオプションを設定します。
- サーバ証明書 (Server Certificate) : アクティブ認証時にユーザに提供される CA 証明書。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。証明書を貼り付けるか、または [証明書のアップロード (Upload Certificate)] をクリックして証明書ファイルを選択します。デフォルトでは、ユーザ認証時に自己署名証明書を提供します。
 - 証明書キー (Certificate Key) : サーバ証明書のキー。キーを貼り付けるか、または [キーのアップロード (Upload Key)] をクリックしてキーファイルを選択します。
 - 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。異なるポートを設定する場合は、1025 ~ 65535 の範囲内にする必要があります。
- ステップ 4** [保存 (Save)] をクリックします。

アイデンティティ ルールの設定

アイデンティティルールは、一致するトラフィックのユーザアイデンティティ情報を収集する必要があるかどうかを決定します。一致するトラフィックのユーザアイデンティティ情報を取得しない場合は、[認証なし (No Authentication)] を設定できます。

ルールの設定に関係なく、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点に注意してください。そのため、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 トラフィックに関するユーザアイデンティティ情報を取得する場合は、すべての送信元と宛先にアクティブ認証ルールを適用するだけで取得できます。



(注) また、認証の失敗は、ネットワークのアクセスには影響しない点にも注意してください。アイデンティティポリシーは、ユーザアイデンティティ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するのを阻止する場合は、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、ルールの順序付きリストにそのルールを挿入する場所を選択します。ルールは、最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用される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。ルールの位置を後から変更するには、このオプションを編集します。

ステップ 4 [ユーザ認証 (User Authentication)] のタイプを選択します。

- **アクティブ (Active)** : ユーザアイデンティティを判別するためにアクティブ認証を使用します。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) : ユーザアイデンティティを取得しません。アイデンティティベースのアクセスルールは、このトラフィックに適用されません。これらのユーザは[認証不要 (No Authentication Required)]としてマークされます。

ステップ 5 (アクティブ認証のみ) ディレクトリサーバによってサポートされる認証方式 ([タイプ (Type)]) を選択します。

- HTTP Basic : 暗号化されていない HTTP Basic 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 : NT LAN マネージャ (NTLM) 接続を使用してユーザを認証します。この選択は AD レルムを選択するときのみ使用できます。Windows ドメインログインを使用して透過的に認証するために IE や Firefox ブラウザを設定できますが、ユーザは自分の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イネーブル化, \(157 ページ\)](#) を参照)。
- 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) 方式か、または Active Directory サーバ方式かを、デバイスがネゴシエートできるようになります。ネゴシエーションの結果は、NTLM、Basic の順に、共通にサポートされ使用されている中で最強な方式になります。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 ページを使用して認証するように求められます。これは、HTTP Basic 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 ネゴシエートの場合は、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は、DNS サーバも更新して、アクティブな認証が必要な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必要があります。そうしないと、リダイレクションが完了できず、ユーザは認証できません。

ステップ 6 (アクティブ認証のみ) アクティブ認証に失敗したユーザをゲストユーザとしてラベル付けするかどうかを決めるには、[ゲストとしてフォールバック (Fall Back as Guest)]>[オン/オフ (On/Off)] を選択します。

ユーザには、正常に認証されるまで 3 回のチャンスがあります。失敗した場合に、このオプションを選択して、ユーザをマークする方法を決定します。これらの値に基づいてアクセスルールを記述できます。

- [ゲストとしてフォールバック (Fall Back as Guest)]>[オン (On)] : ユーザは [ゲスト (Guest)] としてマークされます。
- [ゲストとしてフォールバック (Fall Back as Guest)]>[オフ (Off)] : ユーザは [失敗した認証 (Failed Authentication)] としてマークされます。

ステップ7 [送信元/宛先 (Source/Destination)]タブのトラフィック一致基準を定義します。アクティブ認証が HTTP トラフィックのみに試行される点に注意してください。そのため、非 HTTP トラフィックに対して [認証なし (No Auth)]ルールを設定する必要はなく、非 HTTP トラフィックのアクティブ認証ルールを作成するポイントもありません。

アイデンティティルールの送信元/宛先基準は、トラフィックが通過するセキュリティゾーン (インターフェイス)、IP アドレスまたは IP アドレスの国か大陸 (地理的位置)、またはトラフィックに使用されるプロトコルとポートを定義します。デフォルトは、任意のゾーン、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、ポップアップダイアログボックスで、[OK] をクリックします。基準にオブジェクトが必要で、必要なオブジェクトが存在しない場合は、[オブジェクトの新規作成 (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 [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。一方または両方の基準を定義することもできれば、どちらも定義しないでおくこともできます。指定されていない基準は、あらゆる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入出力する場所に基づいてルールを適用する必要がある場合に、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するすべてのトラフィックからユーザアイデンティティが収集されるように確保するには、宛先ゾーンを空のままにして、内部ゾーンを [送信元ゾーン (Source Zones)] として選択します。

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です。

- 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。

この基準を追加する場合は、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の 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) : 送信元または宛先の国または大陸に基づいてトラフィックを制御するための地理的位置を選択します。大陸を選択すると、大陸内のすべての国が選択されます。ルールで地理的位置を直接選択するほか、作成した地理位置情報 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のある IP アドレスをすべて把握する必要なく、アクセスを特定の国へ容易に制限できます。

(注) 確実に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するために、地理的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 オブジェクトです。TCP/UDP の場合は、これにポートが含まれる場合があります。

- 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。送信元ポートに指定できるのは、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 ポートから発信されるトラフィックと、特定の TCP/UDP ポート宛での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は、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、TCP/80 から TCP/8080 へのトラフィックを対象にすることができます。

ステップ 8 [OK] をクリックします。

トランスペアレント ユーザ認証のイネーブル化

アクティブな認証を可能にするアイデンティティ ポリシーを設定する場合は、次のような認証方法を使用して、ユーザーのアイデンティティを取得できます。

HTTP 基本認証

HTTP 基本認証では、ユーザは常に、ディレクトリのユーザ名およびパスワードによる認証を促されます。パスワードはクリア テキストで送信されます。このため、基本認証は安全な認証形態とみなされません。

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

HTTP 基本認証の一種であり、ユーザにブラウザのログイン ページが表示されます。

NTLM、HTTP ネゴシエート (Active Directory 向けの統合 Windows 認証)

統合 Windows 認証では、ユーザがドメインにログインして、各自のワークステーションを使用することを利用します。アクティブ認証中、ブラウザはサーバにアクセスするとき (FirePOWER Threat Defense キャプティブ ポータルも含む)、このドメイン ログインを使用しようとしています。パスワードは送信されません。認証が成功すると、ユーザは透過的に認証されます。つまり、認証チャレンジが行われたことも、適合したことも、ユーザが意識することはありません。

ドメインのログイン クレデンシャルを使用した認証要求をブラウザが満たすことができなかった場合は、ユーザはユーザ名とパスワードを要求されます。これは、基本認証と同じユーザ エクスペリエンスです。このように、統合 Windows 認証を設定すると、同一ドメイン内のネットワークまたはサーバにアクセスしようとするユーザは、クレデンシャルを提示する必要がなくなります。

HTTP ネゴシエートでは、Active Directory サーバとユーザエージェントの両方でサポートされるものの中から、最強の認証方式が選択されることに注意してください。ネゴシエーションによって HTTP 基本認証が認証方式として選択された場合は、トランスペアレント認証は行われません。強度の順位は、NTLM、基本認証の順です。トランスペアレント認証を使用するには、ネゴシエーションで NTLM が選択される必要があります。

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。以下のセクションでは、一般的に使用され、統合 Windows 認証をサポートするいくつかのブラウザを対象に、統合 Windows 認証の一般的な要件および基本設定について説明します。ソフトウェアのリリースごとに方法が異なる可能性もあるため、使用するブラウザ (または他のユーザ エージェント) の詳細情報について、ヘルプで確認してください。

**ヒント**

Chrome や Safari など（本稿執筆時点のバージョンに基づく）、一部のブラウザでは統合 Windows 認証がサポートされません。ユーザはユーザ名とパスワードの入力を要求されます。使用するバージョンでサポートされるかどうかについては、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、ユーザ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、典型的には `*.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ーバを信頼することができます（独自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には、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 を使用する場合であって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

Internet Explorer を NTLM のトランスペアレント認証用に設定するには、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。
- a) [サイト (Sites)]ボタンをクリックして、信頼済みサイトのリストを開きます。
 - b) 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。
 - [イントラネットの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ディセーブルになります。
 - [プロキシサーバを使用しないサイトをすべて含める (Include all sites that bypass the proxy)]。
 - c) [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、信頼する URL を[サイトの追加 (Add Site)]ボックスに貼り付けて[追加 (Add)]をクリックします。
複数の URL が存在する場合は、このステップを繰り返します。ワイルドカードを使用して、`http://*.example.com` のように URL の一部を指定するか、または単に `*.example.com` と指定します。
このダイアログボックスを閉じて、[インターネット オプション (Internet Options)]ダイアログボックスに戻ります。
 - d) [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、[イントラネットゾーンでのみ自動的にログオンする (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)]タブをクリックして、[LAN の設定 (LAN Settings)]をクリックします。
[LAN に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、[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)]ボックスにアドレスを入力します。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 (NT LAN マネージャ) の透過的な認証のために 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プリファレンスを検索します。

ステップ 2 NTLM をサポートするには、次のプリファレンスを修正します (network.automatic でフィルタリング)。

- [network.automatic-ntlm-auth.trusted-uris] : プリファレンス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、ドメイン名のみを指定して、内部ネットワーク全体を含めることができます。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。
- [プロキシの手動設定 (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 [プロキシの対象なし (No Proxy For)] 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ていて使用可能な場合は、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基準がユーザに一致するように記述さ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。

アイデンティティルールは HTTP トラフィックのみに一致するため、ユーザはデバイス経由でそのタイプのトラフィックを送信する必要があります。



第 9 章

アクセスコントロール

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, 163 ページ](#)
- [アクセスコントロールポリシーの設定, 169 ページ](#)
- [アクセスコントロールポリシーのモニタリング, 184 ページ](#)
- [アクセスコントロールの制限事項, 186 ページ](#)

アクセスコントロールの概要

以下の各トピックでは、アクセスコントロールポリシーについて説明します。

アクセスコントロールルールとデフォルトアクション

アクセスポリシーを使用すると、ネットワークリソースへのアクセスを制御できます。ポリシーは、順序付けられた一連のルールで構成され、各ルールが上位から下位に向かって順に評価されます。すべてのトラフィック条件が一致したトラフィックに適用されるルールが、最初に使用されます。

アクセスは、以下に基づいて制御できます。

- 送信元および宛先の IP アドレス、プロトコル、ポート、インターフェイス（セキュリティゾーンとして）など、従来のネットワーク特性。
- 使用されるアプリケーション。特定のアプリケーションに基づいてアクセスを制御することもできますが、アプリケーションのカテゴリ、特定の特性をタグ付けら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評価に基づくルールを作成することもできます。

- 一般化した URL カテゴリを含む、Web 要求の接続先 URL。カテゴリとの一致を、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細かく絞り込むことができます。
- 要求を送信したユーザ、またはこのユーザが属するユーザ グループ。

通過を許可する非暗号化トラフィックに対しては、IPS インスペクションを適用して脅威の有無を調べ、攻撃の可能性のあるトラフィックをブロックできます。また、ファイルポリシーを使用すると、禁止したファイルまたはマルウェアの有無のインスペクションを実行できます。

アクセス ルールと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、トラフィックに IPS インスペクションを適用できます。しかし、デフォルト アクションによって処理されたトラフィックに対し、ファイルまたはマルウェアのインスペクションを実行することはできません。

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、接続に使用されるアプリケーションに基づきトラフィックをフィルタ処理できます。システムでは、幅広い種類のアプリケーションを認識できません。したがって、すべての Web アプリケーションをブロックすることなく、1 つの Web アプリケーションだけをどのようにブロックするのか、ユーザが理解している必要はありません。

広く使用されている一部のアプリケーションに対しては、アプリケーションのさまざまな側面に対してフィルタ処理できます。たとえば、Facebook をすべてブロックするのではなく、Facebook のゲームだけ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くルールを作成することもできます。リスク、ビジネスとの関連性、タイプ、カテゴリ、またはタグを選択することで、該当するアプリケーション グループ全体をブロックまたは許可できます。ただし、アプリケーション フィルタ内のカテゴリを選択する場合は、意図しないアプリケーションまで含まれてしまうことのないように、一致したアプリケーションのリストを十分に確認してください。可能なグループ化の詳細については、[アプリケーション条件](#)、(175 ページ) を参照してください。

アプリケーション フィルタリングで注意すべき制限事項については、[アプリケーション コントロールの制約](#)、(186 ページ) を参照してください。最も注意が必要な制限は、暗号化トラフィックの処理です。

HTTPS 接続など、暗号化を使用するアプリケーションは、システムによって識別されない可能性があります。アプリケーションに復号が必要かどうかを確認するには、アプリケーション フィルタのダイアログボックスで以下のタグを選択して、表示されたアプリケーション リストを検証します。

- [SSL プロトコル (SSL Protocol)] : 「SSL プロトコル」のタグが付いたトラフィックは、復号する必要はありません。このトラフィックはシステムによって認識され、指定したアクセス コントロール アクションが適用されます。リストされたアプリケーションに対するアクセス コントロール ルールは、予期された接続と一致します。
- [復号トラフィック (Decrypted Traffic)] : このトラフィックは、事前に復号しておかないとシステムによって認識されません。Firepower Device Manager を使用して SSL 復号を設定することはできないため、これらのアプリケーションに対するアクセス コントロール ルールは機能しません。たとえば、本稿執筆時点で、Dropbox にはこのタグが付けられています。し

たがって、Dropbox アプリケーションに対するアクセスルールは、Dropbox の接続と一致しません。

URL フィルタリング

URL 条件は、ネットワークのユーザがアクセスできる Web サイトを制御します。この機能は、URL フィルタリングと呼ばれます。

次の手法を使用して、URL フィルタリングを実装することができます。

- カテゴリと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 ライセンスを使用すると、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することができます。
- 手動 URL フィルタリング：任意のライセンスを使用して、手動で個別に URL および URL グループを指定し、きめ細かくカスタマイズした Web トラフィックの制御を実現することができます。

次のトピックでは、URL フィルタリングに関する詳細を説明します。

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 ライセンスでは、要求された URL のカテゴリと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 (Auctions)] カテゴリ、monster.com は [求職 (Job Search)] 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：URL が組織のセキュリティ ポリシーに反する目的で使用される可能性のレベル。レピュテーションの範囲は、[高リスク (High Risk)] (レベル 1) から [ウェルノウン (Well Known)] (レベル 5) まであります。



(注) イベントおよびアプリケーションの詳細で URL カテゴリおよびレピュテーション情報を確認するには、URL 条件を指定して少なくとも 1 つのルールを作成する必要があります。また、最新の脅威インテリジェンスを入手するためには、Cisco Collective Security Intelligence (CSI) との通信を有効にする必要があります。

レピュテーションベースの URL フィルタリングの利点

URL カテゴリとレピュテーションは、URL フィルタリングを迅速に設定するのに役立ちます。たとえば、アクセスコントロールを使用して、[乱用薬物 (Abused Drugs)] カテゴリの高リスクの URL をブロックできます。

カテゴリおよびレピュテーション データを使用すると、ポリシーの作成と管理が簡単になります。この方法により Web トラフィックが期待通りに制御されます。シスコでは、既存 URL の新

しいカテゴリとリスクだけでなく、脅威インテリジェンスと新しいURLを継続的に更新しているため、システムが最新の情報を使用して要求されたURLをフィルタ処理していることを保証できます。（たとえば）セキュリティに対する脅威を示しているサイトや望ましくない内容を提供しているサイトは、ユーザが新しいポリシーを更新して展開するよりも速く現れたり、消えたりすることがあります。

次に、システムの適応方法の例をいくつか示します。

- アクセスコントロールルールですべてのゲームサイトがブロックされる場合、新しいドメインが登録されて[ゲーム (Gaming)]に分類されると、これらのサイトを自動的にブロックできます。
- アクセスコントロールルールですべてのマルウェアサイトがブロックされ、あるブログページがマルウェアに感染すると、システムはそのURLを[ブログ (Blog)]から[マルウェア (Malware)]に再分類して、そのサイトをブロックできます。
- アクセスコントロールルールで高リスクのソーシャルネットワーキングサイトがブロックされ、それらのサイトのプロフィールページに悪意のあるペイロードへのリンクを含むリンクが掲載されると、システムはそのページのレピュテーションを[無害なサイト (Benign Sites)]から[高リスク (High Risk)]に変更してページをブロックできます。

手動 URL フィルタリング

アクセスコントロールルールでは、個々のURLまたはURLグループを手動でフィルタリングすることで、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足したり、選択的にオーバーライドしたりすることができます。このタイプのURLフィルタリングは、特別なライセンスなしで実行できます。

たとえば、アクセスコントロールを使用して、組織に適していないWebサイトのカテゴリをブロックできます。ただし、カテゴリに、アクセスの提供を希望する適切なWebサイトが含まれている場合は、そのサイトの手動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。

手動で特定のURLをフィルタリングする場合は、影響を受ける可能性のあるその他のトラフィックを慎重に考慮してください。ネットワークトラフィックがURL条件に一致するかどうか判断するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の一部と一致する場合、URLは一致するものと見なされます。

たとえばexample.comへのすべてのトラフィックを許可する場合、ユーザは次のURLを含むサイトを参照できます。

- <http://example.com/>
- <http://example.com/newexample>
- <http://www.example.com/>

別の例として、ign.com（ゲームサイト）を明示的にブロックする場合を考えてください。ただし、部分列の一致はign.comをブロックすることを意味していますが、意図していないverisign.comもブロックしてしまいます。

HTTPS トラフィックのフィルタリング

暗号化トラフィックをフィルタリングする場合、システムは SSL ハンドシェイクの実行時に渡された情報（トラフィックの暗号化に使用された公開キー証明書のサブジェクト共通名）に基づき、要求された URL を判断します。

HTTP フィルタリングでは、サブドメインを含むホスト名全体が考慮されます。しかし、HTTPS フィルタリングではサブジェクト共通名に含まれるサブドメインは無視されるため、内で HTTPS 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ようにしてください。たとえば、`www.example.com` ではなく `example.com` を使用します。

暗号化プロトコルによるトラフィックの制御

内で URL フィルタリングを実行する場合、暗号化プロトコル（HTTP に対する HTTPS）は無視されます。これは、手動、およびレピュテーションベースの URL 条件の両方で生じます。つまり、URL フィルタリングでは、次の 2 つの Web サイト宛てのトラフィックが同じものとみなされます。

- `http://example.com/`
- `https://example.com/`

HTTP、HTTPS トラフィックのどちらか一方だけに一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、サイトへの HTTPS アクセスを許可しつつ、HTTP アクセスは禁止するには、2 つのアクセスコントロールルールを作成し、それぞれでアプリケーションおよび URL 条件を指定します。

最初のルールでは、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
アプリケーション：HTTPS
URL：example.com
```

2 番目のルールでは、同じ Web サイトに対する HTTP アクセスをブロックします。

```
アクション：ブロック
アプリケーション：HTTP
URL：example.com
```

Web サイトをブロックしたときのユーザへの表示

URL フィルタリングルールを使用して Web サイトをブロックした場合にユーザに何が表示されるかは、サイトが暗号化されているかどうかによって異なります。

- HTTP 接続：タイムアウトまたは接続リセット時の通常のブラウザ 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。このページでは、接続が意図的にブロックされたことを明らかにする必要があります。
- 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、安全な接続に障害が発生した場合のブラウザのデフォルトページが表示されます。

エラーメッセージは、ポリシーによってサイトがブロックされたことを示しません。その代わりに、一般的な暗号化アルゴリズムがないことを示します。このメッセージからは、接続を意図的にブロックしたことは明らかになりません。

加えて、Web サイトは、明示的な URL フィルタリング ルールではない他のアクセス コントロール ルールによって、あるいはデフォルトアクションによってブロックされる可能性もあります。たとえば、ネットワークまたは地理位置情報全体をブロックすると、そのネットワーク上にある、またはその地理的な場所にある 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、次の制限事項に示すように、応答ページが表示される場合も、されない場合もあります。

URL フィルタリングを実行する際は、サイトが意図的にブロックされたときにユーザに何が表示され、どのようなサイトがブロックされるかをエンドユーザに説明することを検討してください。そうしないと、ユーザはブロックされた接続のトラブルシューティングに相当の時間を費やすおそれがあります。

HTTP 応答ページの制限事項

HTTP 応答ページは、システムが Web トラフィックをブロックしたときに常に表示されるわけではありません。

- 容易なアクセス コントロール ルール（シンプルなネットワーク条件を使用した、早い段階でのブロッキングルール）の結果として Web トラフィックがブロックされた場合、応答ページは表示されません。
- 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た場合、応答ページは表示されません。
- アクセス コントロール ルールによってブロックされた暗号化接続には、応答ページが表示されません。

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 Firepower 機能の AMP 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と関連付けることで、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受け渡す前に、まずは侵入ポリシー、ファイルポリシー、または両方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に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せん。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のインスペクションを実行しません。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。

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。

アクセスコントロールポリシーの設定

アクセスコントロールポリシーを使用すると、ネットワークリソースへのアクセスを制御できます。ポリシーは、順序付けられた一連のルールで構成され、各ルールが上位から下位に向かって順に評価されます。すべてのトラフィック条件が一致したトラフィックに適用されるルールが、最初に使用されます。トラフィックに一致するルールがまったく存在しない場合は、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テーブルに、順序付けられたすべてのルールが表示されます。各ルールに対し、以下を行えます。

- 最左列に表示されるルールメンバーの横にある [>] ボタンをクリックすると、ルールの図が開きます。この図は、各ルールがどのようにトラフィックを制御するかを分かりやすく示します。ボタンを再度クリックすると、図が閉じます。
- ほとんどのセルでは、インライン編集を行えます。たとえば、アクションを選択すると、別のアクションを選択できます。また、送信元ネットワークオブジェクトをクリックすると、送信元の条件を追加または変更できます。

- ルールを移動するには、ルール上にマウスオーバーして移動アイコン (✎) を表示します。この状態でルールをクリックすると、ドラッグアンドドロップによって別の場所に移動できます。また、ルールを編集し、[順序 (Order)] リスト内の任意の場所を選択して、ルールを移動することもできます。各ルールは、処理させたい順に配置することが重要です。特定のルール、特に汎用ルールに対する例外を定義するようなルールは、最上位の付近に配置する必要があります。
- 最右列は、ルールに対するアクションボタンです。このセル上をマウスオーバーすると、ボタンが表示されます。ルールは編集 (✎) または削除 (✖) することができます。

以下の各トピックでは、ポリシーを設定する方法について説明します。

デフォルトアクションの設定

ある接続が特定のアクセスルールと一致しない場合、その接続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 (Trust)] : 追加のインスペクションを行わずにトラフィックを許可します。
 - [許可 (Allow)] : 侵入ポリシーの対象であ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)] の場合は、[侵入ポリシー (Intrusion Policy)] の下で [ポリシーの有効化 (Enable Policy)] > [オン (On)] を選択して、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, \(180 ページ\)](#) 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。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、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有効にする必要があります。[ロギングの設定, \(182 ページ\)](#) 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できます。アクセスコントロールポリシーのルールは上から下へ順番に評価されます。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した最初のルールです。

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、ルールの順序付きリストにそのルールを挿入する場所を選択します。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る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。ルールの位置を後から変更するには、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。名前にスペースを含めることはできません。英数字と次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) : さらにどの種類のインスペクションも行うことなく、トラフィックを許可します。
 - 許可 (Allow) : ポリシーの侵入およびその他のインスペクションの設定に従って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、トラフィックの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 アドレスの国か大陸 (地理的位置)、またはトラフィックに使用されるプロトコルとポート。デフォルトは、任意のゾーン、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/宛先条件、(173 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。デフォルト

は任意のアプリケーションです。[アプリケーション条件](#)、(175 ページ) を参照してください。

- URL : Web 要求の URL または URL カテゴリ。デフォルトは任意の URL です。[URL の条件](#)、(177 ページ) を参照してください。
- ユーザ (Users) : ユーザまたはユーザグループ。アイデンティティポリシーは、トラフィックの照合にユーザおよびグループ情報が使用できるかどうかを決定します。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。[ユーザの条件](#)、(178 ページ) を参照してください。

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、ポップアップダイアログボックスで、[OK]をクリックします。基準にオブジェクトが必要で、必要なオブジェクトが存在しない場合は、[オブジェクトの新規作成 (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[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、次のヒントを考慮してください。

- 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、特定のホストの URL フィルタリングを実行する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およびアプリケーションフィルタの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、OR 関係は単一の条件内の項目間で生じますが、AND 関係は条件タイプ間で生じません (たとえば、送信元/宛先とアプリケーションの間)。
- 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は、暗号化されていないトラフィックに対するさらなる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) : 侵入とエクスプロイトに関してトラフィックのインスペクションを実行するには、[侵入ポリシー (Intrusion Policy)] > [オン (On)] を選択し、IPS 侵入インスペクションポリシーを選択します。[侵入ポリシーの設定](#)、(180 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およびブロックする必要があるファイルに関してトラフィックのインスペクションを実行するには、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](#)、(180 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。
ファイルポリシーを選択した場合、デフォルトでファイルイベントが生成されますが、デフォルトでは、ルールに一致するトラフィックに関する接続イベントは生成されません。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](#)、(182 ページ) を参照してください。

ステップ 9 [OK]をクリックします。

送信元/宛先条件

アクセス ルールの送信元/宛先条件は、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（地理的な場所）、あるいはトラフィックに使用されるプロトコルやポートを定義します。デフォルトは任意のゾーン、アドレス、地理的な場所、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、対象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。条件がオブジェクトを必要とする場合で、必要なオブジェクトが存在しない場合、[オブジェクトの新規作成 (Create New Object)] をクリックします。ポリシーからオブジェクトまたは要素を削除するには、[X]をクリックします。

次の条件を使用して、ルールに一致する送信元と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 ゾーンのオブジェクト。一方または両方の基準を定義することもできれば、どちらも定義しないでおくこともできます。指定されていない基準は、あらゆる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入出力する場所に基づいてルールを適用する必要がある場合に、この基準を使用します。たとえば、内部ホストに向かうすべてのトラフィックに IPS インспекションを受けさせるには、内部ゾーンを [送信元ゾーン (Destination Zones)] として選択し、宛先ゾーンを空にします。ルールに IPS フィルタリングを実装するには、ルールアクションは [許可 (Allow)] として、ルールの侵入ポリシーを選択する必要があります。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義するネットワーク オブジェクトまたは地理的位置です。

- 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。

この基準を追加する場合は、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。
- [地理位置情報置 (Geolocation)] : 送信元または宛先の国または大陸に基づいてトラフィックを制御するための地理的位置を選択します。ある大陸を選択すると、大陸内のすべての国が選択されます。ルールで地理的位置を直接選択するほか、作成した地理位置情報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のある IP アドレスをすべて把握する必要なく、アクセスを特定の国へ容易に制限できます。



(注) 常に最新の地理的位置データを使用してネットワーク トラフィックをフィルタ処理できるように、シスコでは、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 オブジェクトです。TCP/UDP の場合は、これにポートが含まれる場合があります。ICMP では、コードとタイプが含まれる場合があります。

- 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。送信元ポートに指定できるのは、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。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 仕様は宛先ポートのみで許可され、送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから発信されるトラフィックと、特定の TCP/UDP ポート宛での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は、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、TCP/80 から TCP/8080 へのトラフィックを対象にすることができます。

アプリケーション条件

アクセスルールのアプリケーション条件は、IP 接続またはフィルタで使用されるアプリケーションを定義します。アプリケーションの定義は、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基づいて行われます。デフォルトは、すべてのアプリケーションです。

ルール内に個々のアプリケーションを指定することもできますが、アプリケーションフィルタを使用することで、ポリシーを簡単に作成および管理できます。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。ユーザがそれらのアプリケーションの 1 つ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、シスコでは、システムおよび脆弱性データベース (VDB) の更新により、さらなるアプリケーション検出プログラムを高頻度で更新および追加しています。したがって、ルールを手動で更新しなくても、リスクの高いアプリケーションをブロックするルールが新規アプリケーションにも自動的に適用されます。

アプリケーションおよびフィルタをルール内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。どちらの指定方法も同機能ですが、オブジェクトを使用したほうが、複合ルールを作成する場合に、「1 条件につき 50 アイテム」というシステム制限に容易に準拠できます。

アプリケーションおよびフィルタ リストを変更するには、条件内の [+] ボタンをクリックし、必要な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 (個別のタブにリスト) を選択して、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。いずれかのタブで [高度なフィルタ (Advanced Filter)] をクリックすると、特定のアプリケーションの検索に役立つフィルタ条件を選択できます。ポリシーから削除するには、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。まだオブジェクト化されていない、複数の条件の組み合わせ

を1つの新規アプリケーションフィルタオブジェクトとして保存するには、[フィルタとして保存 (Save As Filter)] リンクをクリックします。

以下の[高度なフィルタ (Advanced Filter)]条件を使用すると、ルールと一致するアプリケーションまたはフィルタを識別できます。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要素と同じです。



(注) 単一のフィルタ条件内で選択された複数の項目は、互いに「論理和 (OR)」の関係となります。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、条件を満たすものだけが表示されるように、画面のアプリケーションリストが更新されます。これらのフィルタを使用すると、個別に追加しようとするアプリケーションを特定したり、ルールに追加する必要のあるフィルタが選択されているか確認する場合に役立ちます。

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おそれのある目的で使用される可能性。「非常に低い (Very Low)」～「非常に高い (Very High)」。

ビジネスとの関連性

娯楽としてではなく、組織の事業運営のコンテキスト内でアプリケーションが使用される可能性。「非常に低い (Very Low)」～「非常に高い (Very High)」。

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：HTTP や SSH など、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：Web ブラウザや電子メールクライアントなど、ホスト上で実行され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：MPEG ビデオや Facebook など、HTTP トラフィックのコンテンツ、または要求された URL を表す 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

アプリケーションの補足情報。カテゴリに似ています。

暗号化トラフィックに対しては、SSLプロトコルのタグが付いたアプリケーションだけを使用するトラフィックが識別およびフィルタ処理されます。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（暗号化トラフィックまたは暗号化されていないトラフィックではなく）復号トラフィックのみで検出できるアプリケーションに対し、復号トラフィックタグを割り当てます。

アプリケーション リスト（画面下部）

このリストは、リスト上のオプションからフィルタを選択すると更新されます。したがって、現時点でフィルタに一致するアプリケーションを確認できます。このリストを使用すると、フィルタ条件をルールに追加する場合、必要なアプリケーションがフィルタのターゲットとなっているかどうかを確認できます。特定のアプリケーションを追加するには、このリストから選択します。

URL の条件

アクセスルールの URL 条件は、Web リクエストで使用される URL を定義するか、または要求された URL が属するカテゴリを定義します。カテゴリを一致させるために、許可またはブロックするサイトの相対的なレピュテーションを指定することもできます。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 条件をすぐに作成することができます。たとえば、すべてのゲームサイトやリスクの高いすべてのソーシャルネットワーキングサイトを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、シスコの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、次の方式のいずれかを使用して、適切なカテゴリまたは 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、[X]をクリックします。

[URL] タブ

[+]をクリックし、URLの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なければ、[新規URLの作成 (Create New URL)]をクリックします。



(注) 特定のサイトを対象とする 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よくお読みください。URL のマッチングは想定されるようには行われられないため、意図せずにサイトをブロックしてしまう可能性があります。たとえば、ゲームサイト `ign.com` を明示的にブロックしようとする、`verisign.com`、およびその他の「ign」で終わる任意のサイトもブロックしてしまいます。

[カテゴリ (Categories)] タブ

[+]をクリックして必要なカテゴリを選択し、[OK] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した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、各カテゴリの下向き矢印をクリックし、[任意 (Any)] チェックボックスの選択を解除してから、[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。

- Web アクセスをブロックまたはモニタするルールの場合、あるレピュテーション 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が同様に選択されます。たとえば疑わしいサイト (レベル2) をブロックまたはモニタするようルールを設定した場合、高リスク (レベル1) のサイトも自動的にブロックまたはモニタされます。
- Web アクセスを許可するルールの場合、あるレピュテーション 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が同様に選択されます。たとえば無害なサイト (Benign sites) (レベル4) を許可するようルールを設定した場合、有名 (Well known) (レベル5) サイトもまた自動的に許可されます。

ユーザの条件

アクセスルールのユーザ条件は、IP接続のため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条件を含めるには、アイデンティティポリシー、および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、ユーザ ID が特定の接続のために収集されるかどうかを決定します。ID が確立されると、ホストの IP アドレスは指定されたユーザに関連付けられます。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るトラフィックは、そのユーザからのものと見なされます。IP パケット自体にユーザ ID 情報は含まれないため、この IP アドレスとユーザのマッピングが、使用できる最高の近似値となります。

ルールには最大50のユーザまたはグループを追加できるため、通常は個々のユーザを選択するよりもグループを選択した方が有意義です。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、ネットワークへのその他すべてのアクセスを拒否する後続のルールを作成することができます。次に、このルールを新しいエンジニアに適用するために必要なことは、ディレクトリサーバのエンジニアリンググループにエンジニアを追加するだけです。

ユーザリストを変更するには、条件内の[+]ボタンをクリックし、次の方式のいずれかを使用して、適切な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、[X]をクリックします。

- [ユーザおよびグループ (Users and Groups) タブ] : 目的のユーザまたはユーザグループを選択します。グループは、ディレクトリサーバでグループを設定している場合のみ利用できません。グループを選択すると、ルールは、サブグループを含むすべてのグループのメンバーに適用されます。サブグループで異なる処理を希望する場合、サブグループ用に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の親グループ用のルールの上に配置する必要があります。



(注) デフォルトでは、Active Directory サーバはセカンダリグループから報告するユーザの数を制限します。この制限は、セカンダリグループ内のすべてのユーザが報告され、ユーザ条件を含むアクセスコントロールルールでの使用に適するようにカスタマイズする必要があります。Firepower Device Manager では、ユーザの合計人数が 2000 人に制限されているため、ディレクトリに 2000 人以上のユーザがいる場合、使用可能なすべてのユーザ名が表示されません。

- [特別なエンティティ (Special Entities)]タブ : 次から選択してください。
 - [失敗した認証 (Failed Authentication)] : 認証を促されたユーザが、許容される最大試行回数以内で有効なユーザ名/パスワードのペアを入力できませんでした。認証の失敗それ自体によってユーザがネットワークにアクセスできなくなることはありませんが、これらのユーザのネットワークアクセスを制限するアクセスルールを記述することができます。
 - [ゲスト (Guest)] : これらのユーザをゲストと呼ぶアイデンティティルールが設定されていることを除き、ゲストユーザとは認証に失敗したユーザと同様です。ゲストユーザは認証を促されましたが、最大試行回数以内で認証できませんでした。
 - [認証の必要なし (No Authentication Required)] : ユーザの接続が認証を指定しないアイデンティティルールに一致するため、認証が促されませんでした。
 - [不明 (Unknown)] : IPアドレスのユーザマッピングがなく、認証の失敗記録がまだありません。

侵入ポリシーの設定

Firepower システムには、いくつかの侵入ポリシーが用意されています。これらのポリシーは、侵入およびプリプロセッサ ルールの状態と詳細設定を規定する Cisco Talos Security Intelligence and Research Group によって設計されています。これらのポリシーは変更できません。

トラフィックを許可するアクセスコントロールルールの場合、次の侵入ポリシーのいずれかを選択して、侵入およびエクスプロイトに関してトラフィックのインスペクションを実行できます。侵入ポリシーは、パターンに基づいて攻撃に関してデコードされたパケットを調べ、悪意のあるトラフィックをブロックまたは修正できます。

侵入インスペクションを有効にするには、[侵入ポリシー (Intrusion Policy)] > [オン (On)] を選択し、スライダを使用して目的のポリシーを選択します。ポリシーは、安全性が最低なものから最高なものへの順序で一覧されます。

- **セキュリティより接続を優先 (Connectivity over Security)** : このポリシーは、接続（すべてのリソースにアクセスできること）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優先される組織向けに作成されています。この侵入ポリシーは、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。ある程度の侵入保護の適用を希望するが、ネットワークのセキュリティにはかなり自信がある場合に、このポリシーを選択します。
- **バランスのとれたセキュリティと接続 (Balanced Security and Connectivity)** : 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と全体的なネットワークパフォーマンスとのバランスをとるように設計されています。このポリシーは、大半のネットワークに適しています。侵入防御の適用を希望する大半の状況では、このポリシーを選択します。
- **接続よりセキュリティを優先 (Security over Connectivity)** : 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がユーザの利便性より優先される組織向け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。セキュリティが最重要の場合、またはハイリスクなトラフィックの場合に、このポリシーを選択します。
- **最大限検出 (Maximum Detection)** : このポリシーは、操作性にさらに大きく影響する可能性があっても、[接続よりセキュリティを優先 (Security over Connectivity)] ポリシー以上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向けに作成されています。たとえば、侵入ポリシーは、マルウェア、エクスプロイトキット、古い脆弱性や共通の脆弱性、既知のインザワイルドエクスプロイトを含む多数の脅威カテゴリでルールを有効にします。このポリシーを選択する場合は、ドロップされる正当なトラフィックが過剰でないかどうか慎重に評価してください。

ファイルポリシーの設定

ファイルポリシーを使用すると、Advanced Malware Protection for FirePOWER (AMP for FirePOWER) を使用してマルウェア（悪意のあるソフトウェア）を検出できます。ファイルポリシーを使用してファイル制御を実行することもできます。この場合、ファイルにマルウェアが含まれるかどうかにかかわらず、特定の種類の全ファイルを制御できます。

AMP for FirePOWER では AMP クラウドを使用して、ネットワークトラフィック内で検出された潜在的なマルウェアの性質を取得します。また、ローカルなマルウェア分析、および分類前のファイル更新情報も取得します。管理インターフェイスには、AMPクラウドに到達し、マルウェア検索を実行できるように、インターネットへのパスが必要となります。デバイスは適格ファイルを検出すると、このファイルの SHA-256 ハッシュ値を使用して、AMPクラウドにファイルの性質を問い合わせます。ファイルの性質には、次のような種類があります。

- マルウェア：ファイルが AMP によってマルウェアと分類されました。アーカイブファイル（zip ファイルなど）の場合、アーカイブ内のいずれかのファイルにマルウェアが含まれていると、マルウェアとして識別されます。
- クリーン：ファイルが AMP によって、マルウェアを含まないクリーンファイルと分類されました。アーカイブファイルは、アーカイブ内の全ファイルがクリーンであった場合にクリーンとして識別されます。
- 不明：AMPクラウドによってファイルに性質が割り当てられていません。アーカイブファイルは、アーカイブ内のいずれかのファイルが不明であれば、不明として識別されます。
- 使用不可：システムは AMP クラウドに対し、このファイルの性質を問い合わせることができませんでした。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。多数の「使用不可」イベントが連続して出現した場合は、管理アドレス宛てのインターネット接続が正しく機能しているかどうか確認してください。

使用可能なファイルポリシー

以下のファイルポリシーのいずれか1つを選択できます。

- なし：送信されたファイルに対してマルウェアかどうかを評価せず、ファイル固有のブロックも行いません。このオプションは、ファイルの伝送が信頼されている状況、またはファイルが伝送される可能性が低い（または不可能な）状況でのルール、あるいは使用するアプリケーションまたは URL フィルタリングによってネットワークが適切に保護されることに確信が持てる場合の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)]：ネットワークに送信されたファイルにマルウェアが含まれるかどうか AMP クラウドに問い合わせ、脅威を意味するファイルをブロックします。
- [クラウドによってすべてを検索 (Cloud Lookup All)]：ネットワークに送信された各ファイルの性質を AMP クラウドに問い合わせて記録しますが、ファイルの伝送は許可します。
- [Office ドキュメントおよび PDF のアップロードをブロック、その他のマルウェアをブロック (Block Office Document and PDF Upload, Block Malware Others)]：ユーザに対し、Microsoft Office ドキュメントおよび PDF のアップロードをブロックします。さらに、ネットワークに送信されたファイルにマルウェアが含まれるかどうか AMP クラウドに問い合わせ、脅威を意味するファイルをブロックします。
- [Office ドキュメントのアップロードをブロック、その他のマルウェアをブロック (Block Office Documents Upload, Block Malware Others)]：ユーザに対し、Microsoft Office ドキュメントのアップロードを禁止します。さらに、ネットワークに送信されたファイルにマルウェア

が含まれるかどうか AMP クラウドに問い合わせ、脅威を意味するファイルをブロックします。

ロギングの設定

アクセス ルールのロギング設定は、ルールに一致するトラフィックで接続イベントが発生しているかどうかを判別します。イベントビューアでルールに関連するイベントを表示するには、ロギングを有効にする必要があります。また、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一致するトラフィックを反映させる場合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。目標が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。



注意

サービス妨害 (DoS) 攻撃時にブロックされた TCP 接続のロギングは、システム パフォーマンスに影響し、複数の類似のイベントでデータベースが圧倒される場合があります。ブロック ルールのロギングを有効にする前に、ルールがインターネットに面するインターフェイスに対応しているか、または DoS 攻撃に脆弱なその他のインターフェイスに対応しているかどうかを考慮してください。

次のロギングアクションを設定できます。

ログアクションの選択 (Select Log Action)

次のアクションのいずれかを選択できます。

- 接続の開始および終了時にロギング (Log at Beginning and End of Connection) : 接続の開始および終了時にイベントが発生します。接続の終了 (end-of-connection) イベントには、接続の開始 (start-of-connection) イベントに含まれるすべてのものと、接続中に収集できたすべての情報が含まれるため、許可しているトラフィックに対してこのオプションを選択しないことをお勧めします。両方のイベントをロギングすると、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たトラフィックに対して許可されている唯一のオプションです。
- 接続の終了時にロギング (Log at End of Connection) : 接続の終了時の接続のロギングを有効にする場合は、このオプションを選択します。これは、許可または信頼されるトラフィックの場合に推奨されます。
- 接続時にロギングなし (Log at End of Connection) : ルールに関する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、侵入イベントを生成した場合は、ルールのロギング設定に関係なく、システムは自動的に侵入の発生した接続の終了時にロギングします。侵入がブロックされた接続では、接続ログ内の接続のアクションは[ブロック (Block)]、理由は[侵入ブロック (Intrusion Block)]ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。
-

ファイル イベント

禁止されたファイルまたはマルウェア イベントのログギングを有効にするには、[ファイルのログギング (Log Files)] を選択します。このオプションを設定するには、ルール内でファイルポリシーを選択する必要があります。ルールのファイルポリシーを選択した場合、デフォルトでは、オプションは有効になっています。このオプションは有効なままにしておくことをお勧めします。

システムは、禁止されたファイルを検出すると、次のいずれかのタイプのイベントを自動的にログギングします。

- ファイル イベント：マルウェア ファイルを含むファイルが検出またはブロックされたことを表します。
- マルウェア イベント：マルウェア ファイルのみが検出またはブロックされたことを表します。
- 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のマルウェア ディスポジションが変更され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 [理由 (Reason)] 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場合)、[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場合) のいずれかです。

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場合は、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存在しない場合は、[Syslog サーバの新規作成 (Create New Syslog Server)] をクリックして、新たに作成します (syslog サーバへのログギングを無効にするには、サーバリストから [任意 (Any)] を選択します)。

デバイスのイベントストレージは限定されているため、外部 syslog サーバへイベントを送信することで、より長期的なストレージを提供し、イベント分析を強化できます。

アクセスコントロールポリシーのモニタリング

[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。トラフィックおよびシステム ダッシュボードのモニタリング、(80 ページ) を参照してください。

- [モニタリング (Monitoring)] > [ポリシー (Policies)] は、最もヒット数の多いアクセスコントロールルールと関連する統計情報を表示します。
- [ネットワーク概要 (Network Overview)]、[宛先 (Destinations)]、[入力ゾーン (Ingress Zones)] および [出力ゾーン (Egress Zones)] ダッシュボードで全般的な統計を確認できます。

- [Web カテゴリ (Web Categories)]および[宛先 (Destinations)] ダッシュボードでは、URL フィルタリングの結果を確認できます。[Web カテゴリ (Web Categories)] 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 URL フィルタリング ポリシーが存在する必要があります。
- [アプリケーション (Applications)]ダッシュボードでは、アプリケーションフィルタリングの結果を確認できます。
- [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。
- [ファイルのログ (File Logs)]ダッシュボードでは、ファイルポリシーおよびマルウェアフィルタリングの統計情報を確認できます。こ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ファイルポリシーを適用する必要があります。
- [モニタリング (Monitoring)]>[イベント (Events)]には、アクセスコントロールルールに関連する接続とデータのイベントも表示されます。

CLIでのアクセスコントロールポリシーのモニタリング

デバイスCLIにログインし、次のコマンドを使用して、アクセスコントロールポリシーと統計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、アクセスコントロールルールのサマリ情報とルールごとのヒット数を表示します。
- **show access-list** は、アクセスコントロールルールから生成されたアクセスコントロールリスト (ACL) を表示します。ACLは初期フィルタを提供し、できる限り迅速な決定を実現しようとするため、ドロップされる接続を調査する（および、そのために不必要にリソースを消費する）必要はありませんこの情報には、ヒット数が含まれます。
- **show snort statistics** は、メインのインスペクタである Snort インспек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、インターフェイスを通じて現在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経由するトラフィックに関する統計情報を表示します。
- **show ipv6 traffic** は、デバイスを經由するIPv6トラフィックに関する統計情報を表示します。

アクセスコントロールの制限事項

以下の各トピックでは、アクセスコントロールポリシーに関するいくつかの制限事項について説明します。

アプリケーションコントロールの制約

アプリケーション識別の速度

システムは、次の条件が満たされるまで、を含むアプリケーションコントロールを実行できません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムがセッションでアプリケーションを識別する。

この識別は3～5パケット以内で、またはトラフィックが暗号化されている場合は、SSLハンドシェイクのサーバ証明書交換の後に発生する必要があります。

早期のトラフィックが他のすべての条件と一致してもアプリケーションの識別が不完全な場合は、パケットの通過と接続の確立（またはSSLハンドシェイクの完了）が許可されます。システムによる識別が完了すると、残りのセッショントラフィックに適切なアクションが適用されます。

アクセスコントロールのために、これらの通過したパケットが、アクセスコントロールポリシーのデフォルトの侵入ポリシー（デフォルトアクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）によりインスペクションが実行されます。

暗号化トラフィックおよび復号トラフィックのアプリケーションコントロール

システムは、暗号化されたトラフィックと復号されたトラフィックを識別してフィルタリングできます。

- 暗号化されたトラフィック：システムはSMTP、POPS、FTPS、TelnetS、IMAPSを含むStartTLS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。また、TLSClientHello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。これらのアプリケーションは、SSLルールで[SSLプロトコル (SSL Protocol)]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。
- 復号されたトラフィック：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。

ペイロードのないアプリケーショントラフィック パケットの処理

アクセスコントロールの実行時には、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が適用されます。

参照されるアプリケーショントラフィックの処理

Web サーバによって参照されるトラフィック（アドバタイズメントトラフィックなど）を処理するには、参照す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。

複数のプロトコルを使用するアプリケーショントラフィックのコントロール（Skype）

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 のトラフィックをコントロールするには、個々のアプリケーションを選択するのではなく、[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コントロールできるようになります。

ユーザまたはグループコントロールの制約

Firepower デバイスマネージャは、最大 2000 ユーザに関する情報をディレクトリサーバからダウンロードできます。

ディレクトリサーバに 2000 を超えるユーザアカウントが含まれており、アクセスルールでユーザを選択したか、ユーザベースのダッシュボード情報を表示した場合、候補となるすべての名前は表示されません。ダウンロードされた名前に対してのみルールを記述できます。

2000 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。1つのグループに 2000 を超えるメンバーがいる場合、ダウンロードされた 2000 のみの名前をグループメンバーシップに対して照合できます。

2000 ユーザを超える場合は、Firepower デバイスマネージャではなく、Firepower Management Center（リモートマネージャ）の使用を検討してください。Firepower Management Center は、極めて多数のユーザをサポートします。

URL フィルタリングの制約事項

URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- セッション内の HTTP または HTTPS アプリケーションがシステムにより識別される。
- 要求された URL がシステムにより識別される（ClientHello メッセージまたはサーバ証明書から暗号化されたセッションの場合）。

この識別は 3～5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。

早期のトラフィックが他のすべてのルール条件と一致しても識別が不完全な場合は、パケットの通過と接続の確立（または SSL ハンドシェイクの完了）が許可されます。システムによる識別が完了すると、残りのセッショントラフィックに適切なルールアクションが適用されます。

アクセスコントロールのために、これらの通過したパケットが、アクセスコントロールポリシーのデフォルトの侵入ポリシー（デフォルトアクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）によりインスペクションが実行されます。

手動 URL フィルタリング

手動で特定の URL をフィルタリングする場合は、影響を受ける可能性のあるその他のトラフィックを慎重に考慮してください。ネットワークトラフィックが URL 条件に一致するかどうか判断するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の一部と一致する場合、URL は一致するものと見なされます。

暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングが実行される場合、システムのように動作します。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件はない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。

URL での検索クエリパラメータ

システムでは、URL 条件の照合に URL 内の検索クエリパラメータを使用しません。たとえば、すべてのショッピングトラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするするとブロックされません。

一部のデバイスモデルのメモリに関する制約事項

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 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、一部のデバイスでは、すべてのサブサイトに対して親 URL のデータが使用されます。具体的な例として、システムは google.com カテゴリとレピュテーションを使用して mail.google.com を評価します。影響を受けるデバイスには、ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、および ASA5525-X の各 ASA モデルが含まれます。



第 10 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, 189 ページ](#)
- [NAT の基本, 190 ページ](#)
- [NAT のガイドライン, 198 ページ](#)
- [NAT の設定, 203 ページ](#)
- [IPv6 ネットワークの変換, 238 ページ](#)
- [NAT のモニタリング, 251 ページ](#)
- [NAT の例, 251 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を設定できるからです。

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を行うことができます。



(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どおりに適用されます。

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。

- 実際アドレス/ホスト/ネットワーク/インターフェイス：実際アドレスとは、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

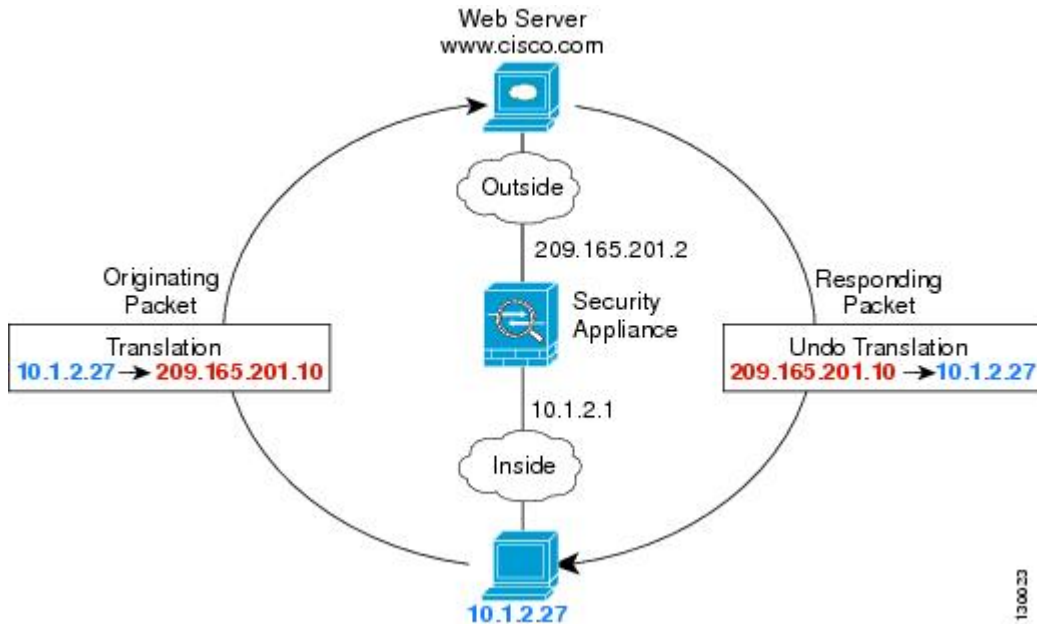
NAT は、次の方法を使用して実装できます。

- 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](#)、[\(204 ページ\)](#) 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 アドレスのポートが使用されます。[ダイナミック PAT](#)、[\(210 ページ\)](#) 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](#)、[\(216 ページ\)](#) 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](#)、[\(227 ページ\)](#) 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 3: NAT の例 : ルーテッドモード



- 1 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピングアドレス 209.165.201.10 に変換されます。
- 2 サーバが応答すると、マッピングアドレス 209.165.201.10 に応答を送信し、Firepower Threat Defense デバイスがそのパケットを受信します。これは、Firepower Threat Defense デバイスがプロキシ ARP を実行してパケットを要求するためです。
- 3 Firepower Threat Defense デバイスはその後、パケットをホストに送信する前に、マッピングアドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

自動 NAT と 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 IP アドレスと宛先 IP 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 および手動 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 : 実アドレスおよびマッピングアドレスの両方に対し、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 グループを特定します。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。実アドレスに対してネットワーク オブジェクト グループを使用できるため、手動 NAT はより高い拡張性を提供します。
- 送信元および宛先 NAT の実装方法。
 - 自動 NAT : 個々のルールは、パケットの送信元または宛先のどちらかに適用されます。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 : 単一のルールが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ていない場合でも、パケットは 1 つの手動 NAT ルールのみで一致します。送信元と宛先は 1 つに結合されるため、送信元/宛先ペアに応じて、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 テーブル内で自動的に順序が決まります。
 - 手動 NAT : NAT テーブル内で手動で順序を決定します（自動 NAT ルールの前または後）。

NAT ルールの順序

自動 NAT ルールおよび手動 NAT ルールは、3 つのセクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 3: 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	<p>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。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。</p>
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てします。

- 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。

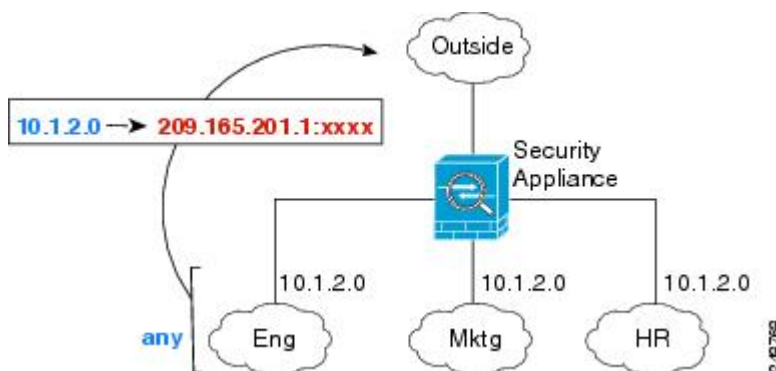
- 192.168.1.1/32 (スタティック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

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せん。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 4: 任意のインターフェイスの指定



ただし、「任意」のインターフェイスの概念は、ブリッジグループメンバー インターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジグループメ

ンバー インターフェイスが除外されます。そのため、ブリッジグループ メンバーに NAT を適用するには、メンバーインターフェイスを指定する必要があります。この結果、1つのインターフェイスのみが異なる同様のルールが多数作成されることとなります。ブリッジ仮想インターフェイス (BVI) 自体に NAT を設定することはできず、メンバー インターフェイスにのみ NAT を設定できます。

NAT のルーティングの設定

Firepower Threat Defense デバイスは、変換済み (マッピング) アドレスに送信されるすべての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。外部ネットワークに十分な数の空きアドレスがあれば、このソリューションは最適です。ダイナミック NAT またはスタティック NAT など、1対1の変換を使用する場合には使用を検討します。ダイナミック PAT を使用すると、少ない数のアドレスに対し、使用可能な変換アドレス数を大幅に増加できます。したがって、外部ネットワーク上で使用可能なアドレスが少ない場合でも、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。上流に位置するルータには、Firepower Threat Defense デバイスを指しているマッピングアドレスのスタティック ルートが必要です。

実際のアドレスと同じアドレス (アイデンティティ NAT)

アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、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 をディセーブルにできます。必要に応じて標準スタティック NAT のプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。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 をイネーブル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。次に、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サブインターフェイスでサポートされません。

ただし、ブリッジグループメンバーのインターフェイス（ブリッジ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）に NAT を設定する場合は、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。ブリッジグループ インターフェイス（BVI）自体に NAT を設定することはできません。
- ブリッジグループメンバーのインターフェイス間で NAT を実行する場合は、送信元と宛先の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 "any" は指定できません。
- 宛先インターフェイスがブリッジグループメンバーのインターフェイスの場合は、インターフェイスに接続された IP アドレスがないため、インターフェイス PAT は設定できません。
- 送信元と宛先の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は、IPv4 ネットワークと IPv6 ネットワーク間の変換（NAT64/46）は実行できません。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 のみが許可された方式です。ダイナミック PAT66 はサポートされていません。

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約が伴います。

- 標準のルーテッドモードインターフェイスの場合は、IPv4 と IPv6 の間の変換もできます。
- 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の場合は、IPv4 と IPv6 の間の変換はできません。2 つの IPv6 ネットワークまたは 2 つの IPv4 ネットワークの間でのみ変換

できます。この制約は、ブリッジグループメンバーと標準のルーティングインターフェイスの間には適用されません。

- 同じブリッジグループに含まれるインターフェイス間で変換する場合、IPv6のダイナミックPAT (NAT66) は使用できません。この制約は、ブリッジグループメンバーと標準のルーティングインターフェイスの間には適用されません。
- 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 の推奨事項

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます (ルーテッドモードのみ)。次のベストプラクティスを推奨します。

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます (混合表記で表示)。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。
- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するためにインスペクションが実行されます。

- ピンホールの作成：一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くため、ユーザはそれらを許可するアクセス コントロール ルールを作成する必要はありません。
- NAT の書き換え：プロトコルの一部としてのパケット データ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジン は、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制：一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用するインスペクション対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていないインスペクション対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。



(注) NAT の書き換えは、リストされているポートでのみサポートされます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 4: 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。	○
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。	×
ESMTP	TCP/25	NAT64 なし。	×
FTP	TCP/21	制限なし。	○
H.323 H.225 (コール シグナリング) H.323 RAS	TCP/1720 UDP/1718 For RAS、 UDP/1718-1719	NAT64 なし。	○

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。	×
IP オプション	RSVP	NAT64 なし。	×
NetBIOS Name Server over IP	UDP/137、138 (送信 元ポート)	NAT64 なし。	×
RSH	TCP/514	PAT なし。 NAT64 なし。	○
RTSP	TCP/554 (HTTP クローキング は処理しません)。	NAT64 なし。	○
SIP	TCP/5060 UDP/5060	拡張 PAT なし。 NAT64 または NAT46 はなし。	○
Skinny (SCCP)	TCP/2000	NAT64、NAT46、または NAT66 はなし。	○
SQL*Net (バージョン 1、2)	TCP/1521	NAT64 なし。	○
Sun RPC	UDP/111	NAT64 なし。	○
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	○
XDMCP	UDP/177	NAT64 なし。	○

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になっているインターフェイス用に、メンバー インターフェイスの NAT ルールを作成します。ブリッジ仮想インターフェイス (BVI) 自体の NAT ルールを作成することはできません。

- (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、インターフェイス上の着信 ESP トラフィックは NAT ルールの影響を受けません。確立された VPN トンネルについてのみ ESP トラフィックが許可され、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。この制限は ESP および UDP ポートの 500 および 4500 に適用されます。
- (手動 NAT のみ) 送信元 IP アドレスがサブネットの場合は、FTP またはセカンダリ接続を使用する他のアプリケーションに対し宛先ポート変換を設定することはできません。FTP データ チャネルの確立は成功しません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、デバイスの CLI で `clear xlate` コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。



(注) ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、`clear xlate` コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。


- 1つのオブジェクトグループに IPv4 と IPv6 の両方のアドレスを入れ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だけが含まれている必要があります。
- (手動 NAT のみ) 発信元アドレスとして **any** を NAT ルールで使用する場合、「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 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイス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 プールは、次のアドレスを含むことができません。
 - 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 がイネーブルの場合は、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。
 - 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 の設定

ネットワーク アドレス変換は、かなり複雑になる場合があります。変換問題や困難なトラブルシューティング状況を回避するため、ルールを可能なかぎりシンプルに保つことをお勧めします。NAT を実装する前に慎重に計画することが非常に重要です。次の手順は、基本的なアプローチを示しています。

手順

-
- ステップ 1** [ポリシー (Policies)] > [NAT] を選択します。
- ステップ 2** 必要なルールの種類を決定します。
ダイナミック NAT、ダイナミック PAT、スタティック NAT およびアイデンティティ NAT のルールを作成できます。概要については、[NAT タイプ](#)、[\(191 ページ\)](#) 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 と手動 NAT](#)、[\(192 ページ\)](#) を参照してください。
- ステップ 4** 以降で説明する手順に従って、ルールを作成します。
- [ダイナミック NAT](#)、[\(204 ページ\)](#)
 - [ダイナミック PAT](#)、[\(210 ページ\)](#)
 - [スタティック NAT](#)、[\(216 ページ\)](#)
 - [アイデンティティ NAT](#)、[\(227 ページ\)](#)
- ステップ 5** NAT ポリシーおよびルールを管理します。
ポリシーとルールを管理するには、次の手順を実行します。
- 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、ルールの削除アイコン (🗑️) をクリックします。

ダイナミック NAT

以下の各トピックでは、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

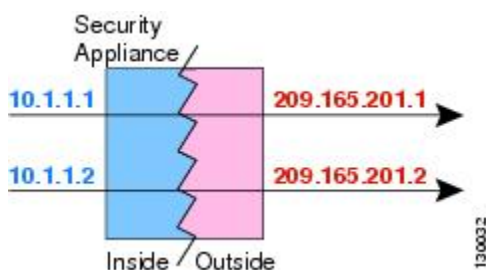
ダイナミック NAT は、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに、実アドレスのグループを変換する機能です。マッピングプールには通常、実際のグループより少ない数のアドレスが含まれます。変換しようとするホストが宛先ネットワークにアクセスすると、NAT はマッピングプール内の IP アドレスをこのホストに割り当てます。この変換は、実際のホストが接続を開始する時点のみに行われます。この接続が終了するまでの時間に限り、変換アドレスは有効であり、変換アドレスの有効時間が経過した後は、ユーザは同一の IP アドレスを維持することはありません。したがって、宛先ネットワーク上のユーザは、ダイナミック NAT を使用するホストへの安定した接続を開始することができません。これは、接続がアクセスルールによって許可されている場合でも同様です。



- (注) 変換の有効時間内であれば、アクセスルールによって許可されている場合、リモートホストは変換されたホストへの接続を開始できます。アドレスが予測できないため、ホストへの接続は成功しにくくなります。しかし、この場合でも、アクセスルールのセキュリティは信頼できます。

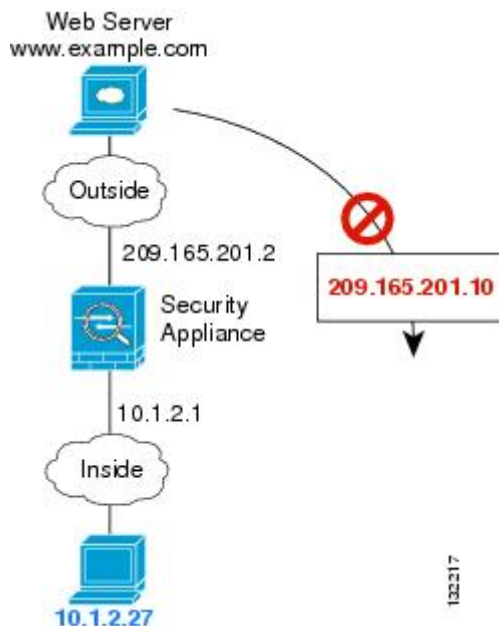
次の図は、ダイナミック NAT の一般的なシナリオを示します。実際のホストのみが NAT セッションを作成でき、応答トラフィックは送信元に戻ることを許可されます。

図 5: ダイナミック NAT



次の図は、マッピングアドレスに対して接続を開始しようとするリモートホストを示します。このアドレスは現時点で変換テーブルに存在しないため、パケットは破棄されます。

図 6: マッピングアドレスへの接続開始を試みるリモートホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、以下の欠点があります。

- マッピングプール内のアドレスの数が実際のグループより少ない場合は、トラフィック量が予想を上回るとアドレスが不足する可能性があります。
この現象が頻繁に発生する場合は、PAT または PAT フォールバック方式を使用します。PAT を使用すると、単一アドレスのポートを使用して 64,000 以上の変換を実行できます。
- ルーティング可能なアドレスをマッピングプールで大量に使用する必要がありますが、大量のルーティング可能なアドレスを使用できない場合があります。

ダイナミック NAT の利点は、PAT を使用できない一部のプロトコルにも対応可能であることです。PAT は、以下の状況では動作しません。

- オーバーロードポートを持たない IP プロトコル (GRE バージョン 0 など) での使用
- データストリームと制御パスを異なるポートで送受信する、非オープンスタンダードの一部のマルチメディアアプリケーションでの使用

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールは、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する機能です。

はじめる前に

[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 ルールを定義す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、以下の要件を満たしている必要があります。

- [元のアドレス (Original Address)] : ネットワーク オブジェクトである必要があります。(グループは不可)。ホストまたはサブネットを含めることができます。
- [変換済みアドレス (Translated Address)] : ネットワーク オブジェクトまたはグループ。サブネットを含めることはできません。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。

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。

- ルールを新規作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン (✎) をクリックします

(不要になったルールを削除するには、このルールのごみ箱アイコンをクリック)。

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。
- [作成するルールの適用対象 (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 以下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)] : (ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)])、ブリッジグループのメンバー インターフェイスは例外です。
- [元のアドレス (Original Address)] : 変換対象のアドレスを保持するネットワーク 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保持するネットワーク 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、必要な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)] : DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード (IPv4 では A レコード、IPv6 では 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されたインターフェイスへの DNS 応答の場合、この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定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、[NAT による DNS クエリおよび応答のリライト](#)、(274 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 (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : 相手のマッピングアドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか (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する場合のみに使用できます。

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、ダイナミックな手動 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行いたいような場合です。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する機能です。

はじめる前に

[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。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 ルールを定義す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、以下の要件も満たしている必要があります。

- [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。ここには、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換するには、この手順を省略し、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)] : ネットワーク オブジェクトまたはグループ。サブネットを含めることはできません。

宛先アドレスのスタティックな変換をルール内で設定する場合は、[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することもできます。

ダイナミック NAT の場合、接続先でポート変換を実行することもできます。Object Manager で、[元の宛先ポート (Original Destination Port)] と [変換済み宛先ポート (Translated Destination Port)] のそれぞれに使用可能なポート 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。

- ルールを新規作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン (✎) をクリックします (不要になったルールを削除するには、このルールのごみ箱アイコンをクリック)。

ステップ 3 基本的なルール オプションを設定します。

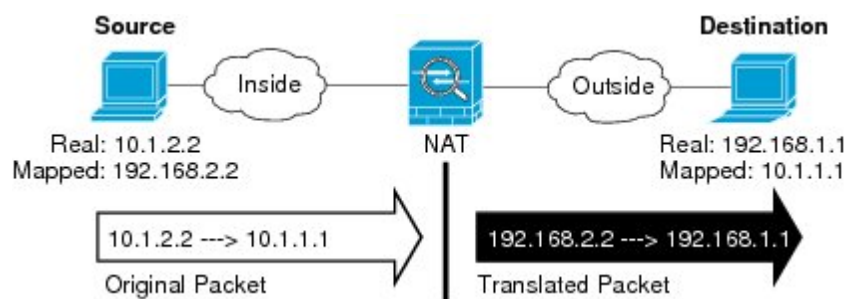
- [タイトル (Title)] : ルールの名前を入力します。
- [作成するルールの適用対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールを追加する位置。ルールはカテゴリ内に挿入することも (自動 NAT ルールの前または後)、選択したルールの前または後に挿入することもできます。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は、送信元アドレスのみに適用されます。宛先アドレスに変換を定義する場合は、変換のタイプは常にスタティックとなります。

ステップ 4 以下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)] : (ブリッジグループのメンバー インターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)])、ブリッジグループのメンバー インターフェイスは例外です。

ステップ 5 元のパケットアドレス (IPv4 または IPv6) を識別します。これは、元のパケットに表示されていたパケットアドレスです。

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。



- [元の発信元アドレス (Original Source Address)] : 変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)] : (オプション) 宛先の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、宛先にかかわらず、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する場合は、こ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 を使用します。

[インターフェイス (Interface)][送信元インターフェイス IP (Source Interface IP)]を選択すると、元の宛先を送信元インターフェイス ([すべて (Any)]以外) に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケットアドレス (IPv4またはIPv6) を識別します。これは、宛先インターフェイスのネットワークで表示されるパケットアドレスです。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保持するネットワーク 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) 変換済みパケットに使用される宛先アドレスを保持するネットワーク オブジェクトまたはグループ。[元の宛先アドレス (Original Destination Address)]にオブジェクトを選択している場合は、同じオブジェクトを選択してアイデンティティ NAT (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 ポートを識別します ([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ではポート変換はサポートされません。したがって、[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)]フィールドは空白のままにしておきます。しかし、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を同じにします (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、必要な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)] : DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード (IPv4 では A レコード、IPv6 では 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されたインターフェイスへの DNS 応答の場合、この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定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、[NAT による DNS クエリおよび応答のリライト](#)、(274 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 (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : 相手のマッピングアドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか (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する場合のみに使用できます。

ステップ 9 [OK] をクリックします。

ダイナミック PAT

以下の各トピックでは、ダイナミック PAT について説明します。

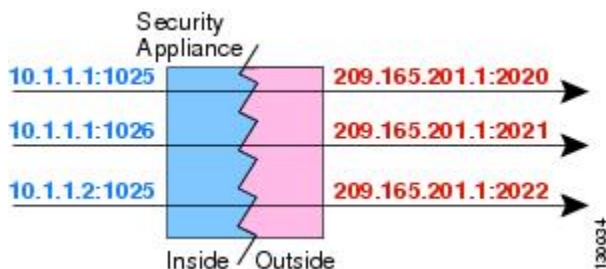
ダイナミック PAT について

ダイナミック PAT は、実アドレスと送信元ポートとを、マッピングアドレスおよび一意のポートに変換することで、複数の実アドレスを 1 つのマッピング IP アドレスに変換する機能です。使用可能である場合は、実際の送信元ポートの番号がマッピングポートにも使用されます。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。したがって、1024 以下のポートは、使用可能な PAT プールがごく小さくなります。

送信元ポートは接続ごとに異なるため、個々の接続に個別の変換セッションが必要となります。たとえば、10.1.1.1:1025 には 10.1.1.1:1026 とは異なる変換が必要です。

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。実際のホストのみが NAT セッションを作成でき、応答トラフィックは送信元に戻ることを許可されます。変換の都度、同じマッピングアドレスが使用されますが、ポートは動的に割り当てられます。

図 7: ダイナミック PAT



変換の有効時間内であれば、アクセスルールによって許可されている場合、宛先ネットワーク上のリモートホストは変換されたホストへの接続を開始できます。ポートアドレス（実際のアドレスおよびマッピングアドレス）が予測できないため、ホストへの接続は成功しにくくなります。しかし、この場合でも、アクセスルールのセキュリティは信頼できます。

接続が有効期限切れになると、ポート変換も期限切れとなります。

ダイナミック PAT の欠点と利点

ダイナミック PAT を使用すると、単一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を節約できます。Firepower Threat Defense デバイスのインターフェイス IP アドレスを PAT アドレスとして使用することもできます。ただし、インターフェイス上で、IPv6 アドレスに対するインターフェイス PAT を使用することはできません。

同じブリッジグループに含まれるインターフェイス間で変換する場合、IPv6 のダイナミック PAT (NAT66) は使用できません。この制約は、ブリッジグループメンバーと標準のルーティングインターフェイスの間には適用されません。

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無効になります。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](#)、(199 ページ) を参照してください。

ダイナミック PAT により、大量の接続が単一の IP アドレスから送信されているように見えることがあり、サーバがこのトラフィックを DoS 攻撃と解釈してしまう場合があります。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールは、アドレスを複数の IP アドレスのみに変換するのではなく、一意の IP アドレスおよびポートの組み合わせに変換する場合に使用します。アドレスは、単一のアドレス（宛先インターフェイスのアドレス、または別のアドレス）に変換できます。

はじめる前に

[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 ルールを定義す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、以下の要件を満たしている必要があります。

- [元のアドレス (Original Address)] : ネットワーク オブジェクトである必要があります。(グループは不可)。ホストまたはサブネットを含めることができます。
- [変換済みアドレス (Translated Address)] : 以下のオプションを使用して PAT アドレスを指定できます。
 - [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場合は、ネットワーク オブジェクトは不要です。IPv6 にインターフェイス PAT を使用することはできません。
 - [単一の PAT アドレス (Single PAT address)] : 単一ホストを保持するネットワーク 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。

- ルールを新規作成するには、[+] ボタンをクリックします。
 - 既存のルールを編集するには、このルールの編集アイコン (✎) をクリックします
- (不要になったルールを削除するには、このルールのごみ箱アイコンをクリック)。

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。
- [作成するルールの適用対象 (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 以下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)] : (ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)])、ブリッジグループのメンバー インターフェイスは例外です。

- [元のアドレス (Original Address)]: 変換対象のアドレスを保持するネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)]: 以下のいずれかを設定します。
 - (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には、[インターフェイス (Interface)]を選択します。また、特定の宛先インターフェイスを選択する必要があります。これには、ブリッジグループのメンバー インターフェイスは使用できません。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以外の単一アドレスを使用するには、この用途で作成したホスト 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、必要な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 (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))]: 相手のマッピングアドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか (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する場合のみに使用できます。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。また、IPv6 ネットワークでこのオプションを使用することはできません。

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 では要件を満たせない場合は、ダイナミックな手動 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行いたいような場合です。ダイナミック PAT では、アドレスを複数の IP アドレスのみに変換するのではなく、一意の IP アドレスおよびポートの組み合わせに変換します。アドレスは、単一のアドレス (宛先インターフェイスのアドレス、または別のアドレス) に変換できます。

はじめる前に

[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。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 ルールを定義す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、以下の要件も満たしている必要があります。

- [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。ここには、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換するには、この手順を省略し、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)] : 以下のオプションを使用して PAT アドレスを指定できます。
 - [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場合は、ネットワーク オブジェクトは不要です。IPv6 にインターフェイス PAT を使用することはできません。
 - [単一の PAT アドレス (Single PAT address)] : 単一ホストを保持するネットワーク オブジェクトを作成します。

宛先アドレスのスタティックな変換をルール内で設定する場合は、[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することもできます。

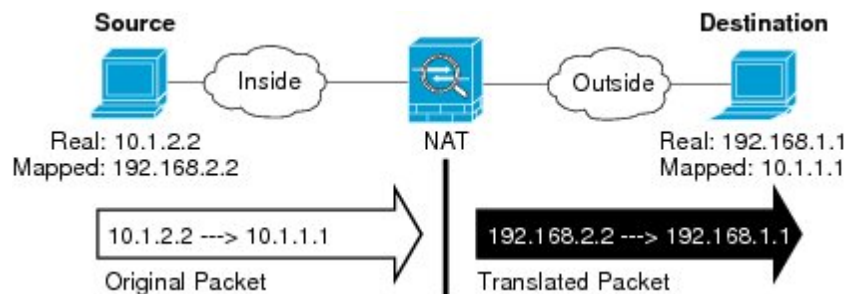
ダイナミック PAT の場合、接続先でポート変換を実行することもできます。Object Manager で、[元の宛先ポート (Original Destination Port)]と [変換済み宛先ポート (Translated Destination Port)]のそれぞれに使用可能なポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

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。
- ルールを新規作成するには、[+] ボタンをクリックします。
 - 既存のルールを編集するには、このルールの編集アイコン (✎) をクリックします
- (不要になったルールを削除するには、このルールのごみ箱アイコンをクリック)。
- 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。
 - [作成するルールの適用対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
 - [ルールの配置 (Rule Placement)] : ルールを追加する位置。ルールはカテゴリ内に挿入することも (自動 NAT ルールの前または後)、選択したルールの前または後に挿入することもできます。
 - [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は、送信元アドレスのみに適用されます。宛先アドレスに変換を定義する場合は、変換のタイプは常にスタティックとなります。
- ステップ 4** 以下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 グループのメンバー インターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実

際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)])、ブリッジグループのメンバーインターフェイスは例外です。

- ステップ 5** 元の packet アドレス (IPv4 または IPv6) を識別します。これは、元の packet に表示されていた packet アドレスです。
元の packet と変換済み packet の例については、次の図を参照してください。



- [元の発信元アドレス (Original Source Address)] : 変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)] : (オプション) 宛先の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、宛先にかかわらず、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する場合は、こ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 を使用します。

[インターフェイス (Interface)] [送信元インターフェイス IP (Source Interface IP)] を選択すると、元の宛先を送信元インターフェイス ([すべて (Any)] 以外) に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

- ステップ 6** 変換済み packet アドレス (IPv4 または IPv6) を識別します。これは、宛先インターフェイスのネットワークで表示される packet アドレスです。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)] : 以下のいずれかを設定します。
 - (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には、[インターフェイス (Interface)] を選択します。また、特定の宛先インターフェイスを選択する必要があります。これには、ブリッジグループのメンバーインターフェイスは使用できません。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以外の単一アドレスを使用するには、この用途で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) 変換済みパケットに使用される宛先アドレスを保持するネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)]にオブジェクトを選択している場合は、同じオブジェクトを選択してアイデンティティ NAT (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 ポートを識別します ([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 ではポート変換はサポートされません。したがって、[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)]フィールドは空白のままにしておきます。しかし、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を同じにします (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、必要な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 (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))]: 相手のマッピングアドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか (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する場合のみに使用できます。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。また、IPv6 ネットワークでこのオプションを使用することはできません。

ステップ 9 [OK]をクリックします。

スタティック NAT

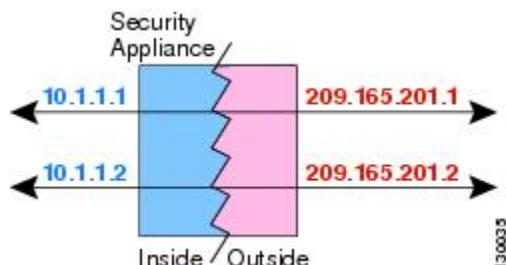
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT は、実際のアドレスをマッピングアドレスに固定的に変換します。スタティック NAT を使用する場合、以降のどの接続でもマッピング アドレスが同じであるため、ホスト宛て、またはホストからの双方向接続を開始できます (これ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 の場合は、変換の都度、ホストは異なるアドレスまたはポートを使用するため、双方向接続の開始はサポートされません。

次の図は、スタティック NAT の一般的なシナリオを示します。変換は常にアクティブなため、実際のホスト、リモートホストのいずれも接続を開始できます。

図 8: 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 9: 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



(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することができます。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。

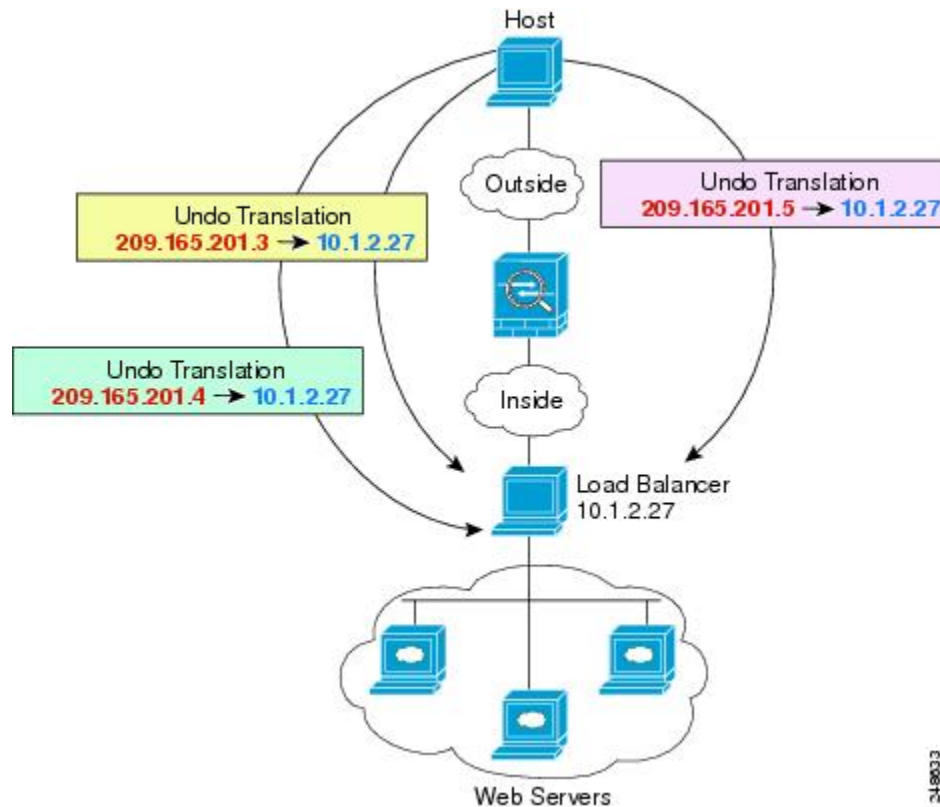
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 10：1 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 11: 1対多のスタティック NAT の例



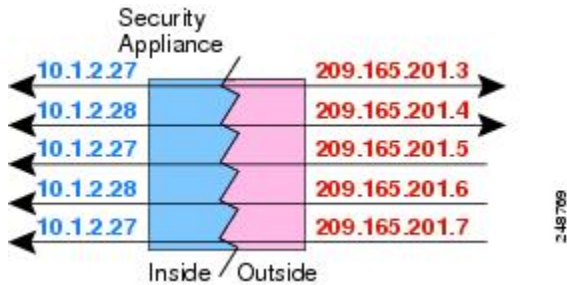
他のマッピング シナリオ (非推奨)

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。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対して1対多のコンフィギュレーションを作成することを推奨します。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、次にマッピングされるアドレスは、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対多のコンフィギュレーションのように、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 12: 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されたプールの中でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。



(注) 多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5 つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 13: 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

アドレスを宛先ネットワーク上でルーティング可能な異なるIPアドレスに変換するには、スタティック自動 NAT ルールを使用します。また、スタティック NAT ルールを使用してポート変換を実行することもできます。

はじめる前に

[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。代わりに、NAT ルールを定義する一方で、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) を指定する必要があります。ホストまたはサブネットを指定できます。
- 変換済みアドレス (Translated Address) : 変換済みアドレスを指定するための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ために、ネットワーク オブジェクトは必要ありません。これはポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスと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 の場合、インターフェイス PAT は使用できません。
 - アドレス (Address) : ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの編集アイコン (✎) をクリックします。

(不要になったルールを削除するには、ルールのごみ箱アイコンをクリックします。)

ステップ 3 基本ルール 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) : (ブリッジグループのメンバー インターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)]) 、ブリッジグループのメンバー インターフェイスは例外です。
- 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) : 次のいずれかを指定します。
 - アドレスの設定グループを使用するには、マッピング 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。
 - (ポート変換でのスタティック 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、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ができ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。IPv6 の場合はインターフェイス PAT を使用できません。これは、ポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスと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) 、変換済みポート (Translated Port) : TCP または UDP ポートを変換する必要がある場合は、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に対応している必要があります。オブジェクトが存在しない場合は、[オブジェクトの新規作成 (Create New Object)] リンクをクリックします。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 応答を変換する (Translate DNS replies that match this rule) : DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード (IPv4 では A レコード、IPv6 では 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されたインターフェイスへの DNS 応答の場合、この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定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、[NAT による DNS クエリおよび応答のリライト、\(274 ページ\)](#) を参照してください。ポート変換を実行する場合、このオプションは使用できません。

- 宛先インターフェイスでプロキシ ARP を実行しない (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 をディセーブルにします。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によって、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。この方法では、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。必要に応じて、プロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

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 ではニーズが満たされない場合は、スタティック手動 NAT ルールを使用します。たとえば、宛先に基づいて異なる変換を実行する場合などです。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異なる IP アドレスに変換します。また、スタティック NAT ルールを使用してポート変換を実行することもできます。

はじめる前に

[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 つのタイプのみを含める必要があります。代わりに、NAT ルールを定義する一方で、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も満たす必要があります。

- 元の送信元アドレス (Original Source Address) : ネットワーク オブジェクトまたはグループを指定できます。ホストまたはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合は、この手順をスキップして、ルールで [すべて (Any)] を指定できます。
- 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ための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ために、ネットワーク オブジェクトは必要ありません。これはポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスと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 の場合、インターフェイス PAT は使用できません。
 - アドレス (Address) : ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで [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)] のスタティック変換を設定している場合は、それらのアドレスのネットワークオブジェクトを作成することもできます。ポート変換を設定した宛先のスタティックインターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップして、ルールでインターフェイスを指定できます。

送信元、宛先または両方のポート変換を実行できます。オブジェクトマネージャで、元のポートと変換済みポート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。

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、ルールのごみ箱アイコンをクリックします。)

ステップ 3 基本ルール オプションを設定します。

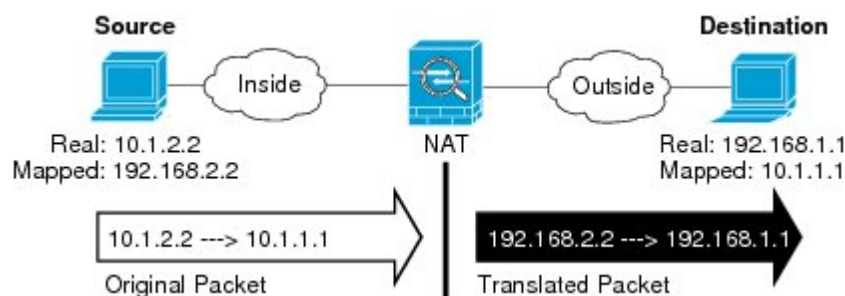
- タイトル (Title) : ルールの名前を入力します。
- ルールの作成対象 (Create Rule For) : [手動 NAT (Manual NAT)] を選択します。
- ルールの配置 (Rule Placement) : ルールを追加する位置。ルールはカテゴリ内に挿入することも (自動 NAT ルールの前または後) 、選択したルールの前または後に挿入することもできます。
- タイプ (Type) : [スタティック (Static)] を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義する場合は、変換は常にスタティックです。

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) : (ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)]) 、ブリッジグループのメンバーインターフェイスは例外です。

ステップ 5 元のパケットアドレス (IPv4 または IPv6) を識別します。これは、元のパケットに表示されていたパケットアドレスです。

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。



- [元の発信元アドレス (Original Source Address)] : 変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)] : (オプション) 宛先の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、宛先にかかわらず、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する場合は、こ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 を使用します。

[インターフェイス (Interface)] [送信元インターフェイス IP (Source Interface IP)] を選択すると、元の宛先を送信元インターフェイス ([すべて (Any)] 以外) に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケットアドレスが、IPv4 または IPv6 のいずれであるか、つまり、宛先ネットワーク インターフェイス上に現れたときのパケットアドレスを特定します。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) : 次のいずれかを指定します。
 - 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。
 - (ポート変換でのスタティック インターフェイス NAT) 宛先インターフェイスの IPv4 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、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ができ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。これはポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスと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 の場合、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) : (任意) 変換済み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です。[元の宛先 (Original Destination)] のオブジェクトを選択した場合は、同じオブジェクトを選択することでアイデンティティ 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。

ポート変換でのスタティック NAT を設定する場合は、送信元、宛先または両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 の間で変換できます。

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を同じにします（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 応答を変換する (Translate DNS replies that match this rule)：DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード (IPv4 では A レコード、IPv6 では 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されたインターフェイスへの DNS 応答の場合、この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定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、[NAT による DNS クエリおよび応答のリライト](#)、(274 ページ) を参照してください。ポート変換を実行する場合、このオプションは使用できません。
- 宛先インターフェイスでプロキシ ARP を実行しない (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 をディセーブルにします。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によって、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。この方法では、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。必要に応じて、プロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

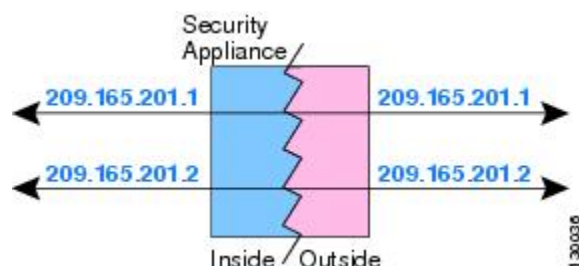
ステップ 9 [OK] をクリックします。

アイデンティティ NAT

IP アドレスをそれ自体に変換する必要がある NAT 設定が存在する場合があります。たとえば、NAT をすべてのネットワークに適用する広範なルールを作成するが、1つのネットワークを NAT から除外する場合は、アドレスをそれ自体に変換するスタティック NAT ルールを作成できます。

次の図は、典型的なアイデンティティ NAT のシナリオを示しています。

図 14: アイデンティティ NAT



以降のトピックでは、アイデンティティ NAT の設定方法を説明します。

アイデンティティ自動 NAT の設定

スタティックなアイデンティティ自動 NAT ルールは、アドレスを変換させたくない場合に使用します。つまり、アドレスを自分自身に変換します。

はじめる前に

[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 ルールを定義す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、以下の要件を満たしている必要があります。

- [元のアドレス (Original Address)]: ネットワーク オブジェクトである必要があります。(グループは不可)。ホストまたはサブネットを含めることができます。
- {変換済みアドレス (Translated Address)}: 元の送信元オブジェクトとまったく同じ内容のネットワーク 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。

- ルールを新規作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン (🔧) をクリックします

(不要になったルールを削除するには、このルールのごみ箱アイコンをクリック)。

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。
- [作成するルールの適用対象 (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 以下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)] : (ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)])、ブリッジグループのメンバーインターフェイスは例外です。
- [元のアドレス (Original Address)] : 変換対象のアドレスを保持するネットワーク 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。オプションとして、まったく同じ内容を持つ、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 [元のポート (Original Port)] および [変換済みポート (Translated Port)] オプションは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、必要な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 をディセーブルにします。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によって、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。この方法では、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。必要に応じて、プロキシ ARP をディセーブルにできます。その場合は、アップストリームルータの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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [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、変換後の送信元アドレスと同じオブジェクトを選択する場合に、送信元インターフェイスおよび宛先インターフェイスを選択するとき、このオプションを選択すると、NAT ルールに設定された宛先インターフェイスを使用するのではな

く、ルーティング テーブルに基づく宛先インターフェイスがシステムによって決定されます。

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 では要件を満たせない場合は、スタティックな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行いたいような場合です。スタティックなアイデンティティ NAT ルールは、アドレスを変換させたくない場合に使用します。つまり、アドレスを自分自身に変換します。

はじめる前に

[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。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 ルールを定義す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、以下の要件も満たしている必要があります。

- [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。ここには、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換するには、この手順を省略し、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)] : 元の送信元と同じオブジェクト。オプションとして、まったく同じ内容を持つ、別のオブジェクトを選択できます。

宛先アドレスのスタティックな変換をルール内で設定する場合は、[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することもできます。ポート変換のみを使用するスタティックな宛先インターフェイスを設定する場合は、宛先をマッピングしたアドレスに対するオブジェクトの追加を省略して、ルール内でインターフェイスを指定できます。

送信元または宛先、またはその両方に対してポート変換を実行できます。Object Manager で、元のポートと変換済みポートのそれぞれに使用可能なポート 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、同一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。

- ルールを新規作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン (🔧) をクリックします

(不要になったルールを削除するには、このルールのごみ箱アイコンをクリック)。

ステップ 3 基本的なルール オプションを設定します。

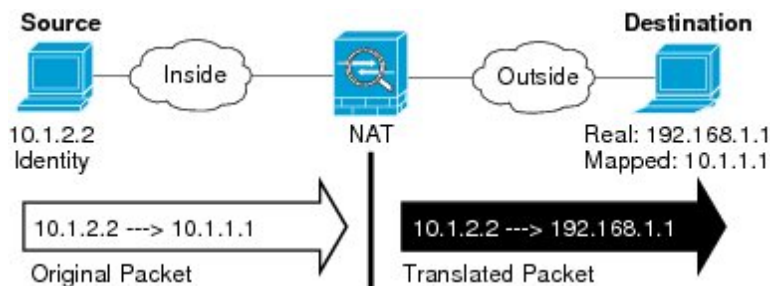
- [タイトル (Title)] : ルールの名前を入力します。
- [作成するルールの適用対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールを追加する位置。ルールはカテゴリ内に挿入することも (自動 NAT ルールの前または後) 、選択したルールの前または後に挿入することもできます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は、送信元アドレスのみに適用されます。宛先アドレスに変換を定義する場合は、変換のタイプは常にスタティックとなります。

ステップ 4 以下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)] : (ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)]) 、ブリッジグループのメンバーインターフェイスは例外です。

ステップ 5 元の packet アドレス (IPv4 または IPv6) を識別します。これは、元の packet に表示されていた packet アドレスです。

元の packet と変換済み packet の例については、次の図を参照してください。ここでは、内部ホストにはアイデンティティ NAT を実行しますが、外部ホストは変換します。



- [元の発信元アドレス (Original Source Address)] : 変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)] : (オプション) 宛先の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、宛先にかかわらず、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する場合は、こ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 を使用します。

[インターフェイス (Interface)] を選択すると、元の接続先を送信元インターフェイス ([すべて (Any)] 以外) に基づいて決定できます。このオプションを選択した場合は、変換済み

接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケットアドレス (IPv4 または IPv6) を識別します。これは、宛先インターフェイスのネットワークで表示されるパケット アドレスです。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。オプションとして、まったく同じ内容を持つ、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) 変換済みパケットに使用される宛先アドレスを保持するネットワーク オブジェクトまたはグループ。[元の宛先アドレス (Original Destination Address)] にオブジェクトを選択している場合は、同じオブジェクトを選択してアイデンティティ NAT (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。ポート変換を行うスタティック NAT を設定する場合は、送信元または宛先、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 間で変換できます。

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を同じにします (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、必要な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 をディセーブルにします。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によって、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。この方法では、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。必要に応じて、プロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

- [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、変換後の送信元アドレスと同じオブジェクトを選択する場合には、送信元インターフェイスおよび宛先インターフェイスを選択するとき、このオプションを選択すると、NAT ルールに設定された宛先インターフェイスを使用するのではなく、ルーティングテーブルに基づく宛先インターフェイスがシステムによって決定されます。

ステップ 9 [OK]をクリックします。

Firepower Threat Defense の NAT ルールのプロパティ

ネットワーク アドレス変換 (NAT) のルールを使用して、IP アドレスを別の 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可能なアドレスに変換します。変換は1つのアドレスから別のアドレスに行うことができ、ポートアドレス変換 (PAT) を使用して、複数のアドレスを1つのアドレスに変換することもできます。送信元アドレス間で区別するためにはポート番号を使用します。

NAT ルールには、次の基本プロパティが含まれます。別途示されている場合を除き、自動 NAT ルールと手動 NAT ルールのプロパティは同じです。

[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)]

変換ルールが [自動 NAT (Auto NAT)]か、[手動 NAT (Manual NAT)]であるかを指定します。自動 NAT は手動 NAT よりシンプルですが、手動 NAT では、宛先アドレスに基づいて送信元アドレス用に異なる変換を作成することができます。

[ステータス (Status)]

ルールをアクティブするか、無効にするかを指定します。

[配置 (Placement)] (手動 NAT のみ)

ルールを追加する位置。ルールはカテゴリ内に挿入することも (自動 NAT ルールの前または後)、選択したルールの前または後に挿入することもできます。

[タイプ (Type)]

変換ルールが [ダイナミック (Dynamic)]か、[スタティック (Static)]であるかを指定します。ダイナミック変換では、アドレスのプールからマッピングアドレス、またはアドレスとポートの組み合わせ (PAT を実装している場合) が自動的に選択されます。マッピングアドレスとポートを正確に定義したい場合は、スタティック変換を使用します。

次のトピックでは、NAT ルールの残りのプロパティについて説明します。

自動 NAT のパケット変換プロパティ

送信元アドレスと変換されたマッピングアドレスを定義するには、[パケット変換 (Packet Translation)]オプションを使用します。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)]

(ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)]) 、ブリッジグループのメンバーインターフェイスは例外です。

[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。これは (グループではなく) ネットワーク オブジェクトである必要があり、ホストまたはサブネットを指定できます。

[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。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。
- [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には、[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も選択する必要があります。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。インターフェイス PAT は IPv6 には使用できません。
 - 宛先インターフェイス以外の単一アドレスを使用するには、この用途で作成したホスト 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)] : 次のいずれかを実行します。
 - 一連のアドレスのグループを使用するには、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を選択します。オブジェクトまたはグループには、ホストや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。特定の宛先インターフェイスも選択する必要があります。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。これで、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 が設定されます。送信元アドレスとポートは、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。インターフェイス PAT は IPv6 には使用できません。
- [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。オプションとして、まったく同じ内容を持つ、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は、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のものである必要があります。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

送信元アドレスと変換されたマッピングアドレスを定義するには、[パケット変換 (Packet Translation)] オプションを使用します。次のプロパティは、手動 NAT にのみ適用されます。指定されている場合を除き、すべて任意選択です。

[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)]

(ブリッジグループのメンバーインターフェイスに必要) この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通じたトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが ([すべて (Any)])、ブリッジグループのメンバーインターフェイスは例外です。

[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。これは、ネットワーク オブジェクトまたはグループを指定でき、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールで [すべて (Any)] を指定できます。

[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。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。
- [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。特定の宛先インターフェイスも選択する必要があります。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。インターフェイス PAT は IPv6 には使用できません。
 - 宛先インターフェイス以外の単一アドレスを使用するには、この用途で作成したホスト 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)] : 次のいずれかを実行します。
 - 一連のアドレスのグループを使用するには、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。特定の宛先インターフェイスも選択する必要があります。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。これで、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 が設定されます。送信元アドレスとポートは、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。インターフェイス PAT は IPv6 には使用できません。
- [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。オプションとして、まったく同じ内容を持つ、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)]

宛先の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、宛先にかかわらず、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する場合は、こ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 を使用します。

[インターフェイス (Interface)] を選択すると、元の接続先を送信元インターフェイス ([すべて (Any)] 以外) に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート 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)]

変換済み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)]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)。

[元の送信元ポート (Original Source Port)]、[変換済み送信元ポート (Translated Source Port)]、[元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]

元のパケットと変換済みパケットの送信元と宛先のサービスを定義するポート オブジェクト。ポートを変換するか、または同じオブジェクトを選択して、ポートを変換せずにルールをサービスに依存させることができます。サービスを設定するときは、次の点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)]と [変換済み送信元ポート (Translated Source Port)]で変換を実行することはできません。宛先ポートでのみ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を同じにします (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。

高度な NAT のプロパティ

NAT を設定する際、[詳細 (Advanced)] オプションを使用すると、特殊なサービスを実現する各種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 応答を変換 (Translate DNS replies that match this rule)]

DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード (IPv4 では A レコード、IPv6 では 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されたインターフェイスへの DNS 応答の場合、この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定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、[NAT による DNS クエリおよび応答のリライト](#)、(274 ページ) を参照してください。スタティック NAT ルールでポート変換を行っている場合には、このオプションは使用できません。

[インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] (ダイナミック NAT のみ)

相手のマッピングアドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスのIPアドレスを使用するかどうか (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する場合のみに使用できます。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)] (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 をディセーブルにします。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によって、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。この方法では、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。必要に応じて、プロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

宛先インターフェイスに対し、ルートルックアップを実行します (スタティックなアイデンティティ NAT のみ、ルーテッドモードのみ)。

元の送信元アドレス、変換後の送信元アドレスと同じオブジェクトを選択する場合に、送信元インターフェイスおよび宛先インターフェイスを選択するとき、このオプションを選択すると、NAT ルールに設定された宛先インターフェイスを使用するのではなく、ルーティングテーブルに基づく宛先インターフェイスがシステムによって決定されます。

IPv6 ネットワークの変換

IPv6 のみ、および IPv4 のみのネットワーク間でトラフィックを渡す必要がある場合、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 ネットワークであっても、外部ネットワークから内部アドレスを隠したい場合もあります。

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 パケットに (またはその逆に) 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。DNS サーバが外部ネットワーク上にあり、DNS 応答を書き換える必要がある場合、1 つの手動 NAT ルールで同じことを実現できます。宛先を指定している場合、手動 NAT ルールでは DNS の書き換えを有効にできないため、2 つの自動 NAT ルールを作成することを推奨します。



(注) NAT46 はスタティック マッピングのみをサポートします。

- NAT66 : IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。



(注) NAT64 および NAT 46 は、標準的なルーテッドインターフェイスでのみ使用できます。NAT66 は、ルーテッドインターフェイスとブリッジグループメンバーインターフェイスの両方で使用できます。

NAT64/46 : IPv6 アドレスから IPv4 への変換

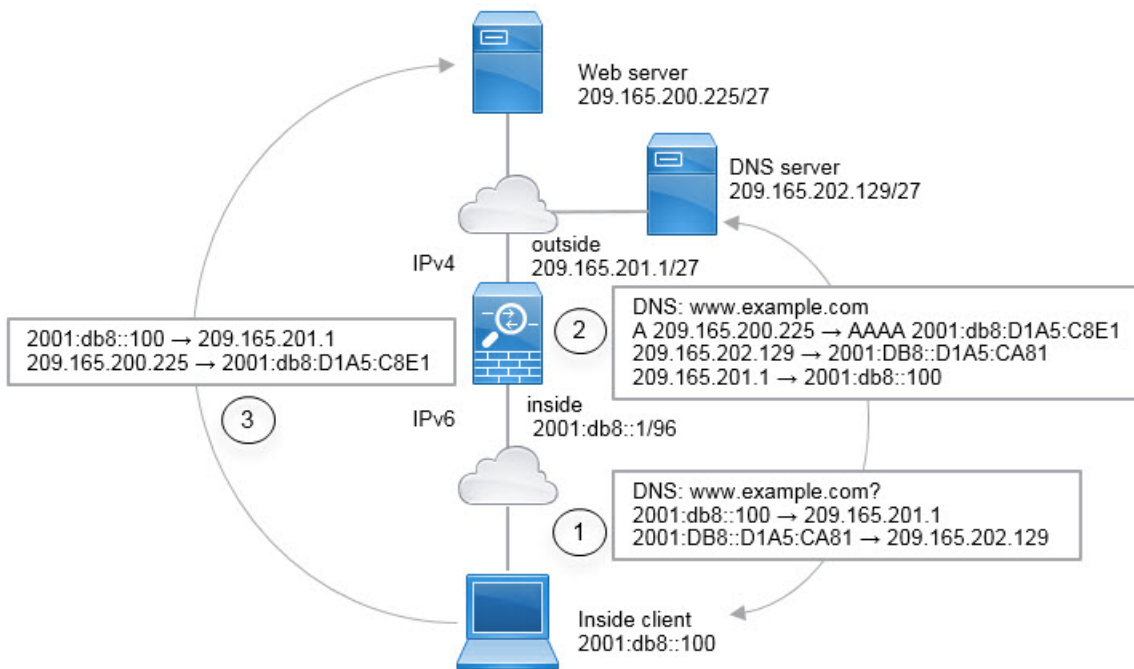
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 アドレスに変換して、IPv4 から IPv6 にトラフィックを戻す必要があります。2つのアドレスプール (IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレスプールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレスプール) を定義する必要があります。

- NAT64 ルールの IPv4 アドレスプールは一般的に小さく、通常、IPv6 クライアントアドレスと 1 対 1 でマッピングするだけの十分なアドレスが含まれていません。ダイナミック PAT は、ダイナミックまたはスタティック NAT と比較すると、想定される大量の IPv6 クライアントアドレスをより簡単に満たすことができます。
- NAT46 ルールの IPv6 アドレスプールは、マッピングする IPv4 アドレスの数以上のサイズにできます。そのため、各 IPv4 アドレスを異なる IPv6 アドレスにマッピングできます。NAT46 はスタティック マッピングのみサポートしているため、ダイナミック PAT は使用できません。

2つのポリシー (1つは送信元 IPv6 ネットワーク用、もう1つは宛先 IPv4 ネットワーク用) を定義する必要があります。DNSサーバが外部ネットワーク上にあり、DNS応答を書き換える必要がある場合、1つの手動 NAT ルールで同じことを実現できます。宛先を指定している場合、手動 NAT ルールでは DNS の書き換えを有効にできないため、2つの自動 NAT ルールを作成することを推奨します。

NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット

以下に、IPv6 専用の内部ネットワークを使用しているにもかかわらず内部ユーザが外部インターネット上のいくつかの IPv4 専用サービスを必要とする一般的な例を示します。



この例では、ダイナミック インターフェイス PAT と外部インターフェイスの IP アドレスを使用して、内部 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 ネットワーク上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。外部 DNS サーバからの応答を A (IPv4) レコードから AAAA (IPv6) レコードに変換し、アドレスを IPv4 から IPv6 に変換できるように、NAT46 ルールで DNS リライトを有効にします。

以下に、内部 IPv6 ネットワーク上の 2001:DB8::100 のクライアントが www.example.com を開こうとする Web 要求の一般的なシーケンスを示します。

- 1 クライアントのコンピュータが、2001:DB8::D1A5:CA81 の 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に対して次の変換が実行されます。
 - 2001:DB8::100 から 209.165.201.1 上の一意のポート (NAT64 インターフェイス PAT ルール)
 - 2001:DB8::D1A5:CA81 から 209.165.202.129 (NAT46 ルール。D1A5:CA81 は 209.165.202.129 の IPv6 の相当物)
- 2 DNS サーバは、www.example.com が 209.165.200.225 にあることを示す A レコードで応答します。NAT46 ルールは、DNS リライトが有効になっている場合、A レコードを IPv6 の相当物の AAAA レコードに変換し、AAAA レコードで 209.165.200.225 を 2001:db8:D1A5:C8E1 に変換します。また、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 から 2001:DB8::D1A5:CA81
 - 209.165.201.1 から 2001:db8::100

- 3 この時点で、IPv6 クライアントは Web サーバの IP アドレスを取得しており、2001:db8:D1A5:C8E1 の www.example.com に HTTP 要求を送信します (D1A5:C8E1 は 209.165.200.225 の IPv6 の相当物)。HTTP 要求の送信元と宛先が変換されます。
- 2001:DB8::100 から 209.156.101.54 上の一意的ポート (NAT64 インターフェイス PAT ルール)
 - 2001:db8:D1A5:C8E1 から 209.165.200.225 (NAT46 ルール)

次の手順では、この例を設定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 の場合は、各メンバー インターフェイスに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 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) コンテンツ テーブルから [ネットワーク (Network)] を選択し、[+] 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 アドレスとして 2001:db8::/96 を入力します。

Add Network Object

Name

Description

Type

Network Host

Network

- d) [OK] をクリックします。

- e) [+]をクリックし、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を付け (outside_v4_any など)、[ネットワーク (Network)]
 を選択して、ネットワーク アドレスとして 0.0.0.0/0 を入力します。

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 (または任意の別の名前)。
 - [ルール作成目的 (Create Rule For)]= Auto NAT。
 - [タイプ (Type)]= Dynamic。
 - [送信元インターフェイス (Source Interface)]= inside。
 - [宛先インターフェイス (Destination Interface)]= outside。
 - [元のアドレス (Original Address)]= inside_v6 ネットワーク オブジェクト。
 - [変換されたアドレス (Translated Address)]= Interface。このオプションは、宛先インターフェイスの IPv4 アドレスを PAT アドレスとして使用します。

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::/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 変換を取得します。

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 (または任意の別の名前)。
- [ルール作成目的 (Create Rule For)] = Auto NAT。
- [タイプ (Type)] = Static。
- [送信元インターフェイス (Source Interface)] = outside。
- [宛先インターフェイス (Destination Interface)] = inside。
- [元のアドレス (Original Address)] = outside_v4_any ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] = inside_v6 ネットワーク オブジェクト。
- [詳細オプション (Advanced Options)] タブで、[このルールと一致する DNS 応答を変換する (Translate DNS replies that match this rule)] をオンにします。

Add NAT Rule ?

Title	Create Rule for	Status
NAT46Rule	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation

Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface		Destination Interface	
outside ▼		inside	
Original Address	Original Port	Translated Address	Translated Port
outside_v4_any ▼	Any ▼	inside_v6 ▼	Any

c) [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に向かう外部ネットワーク上のすべての IPv4 アドレスが、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。

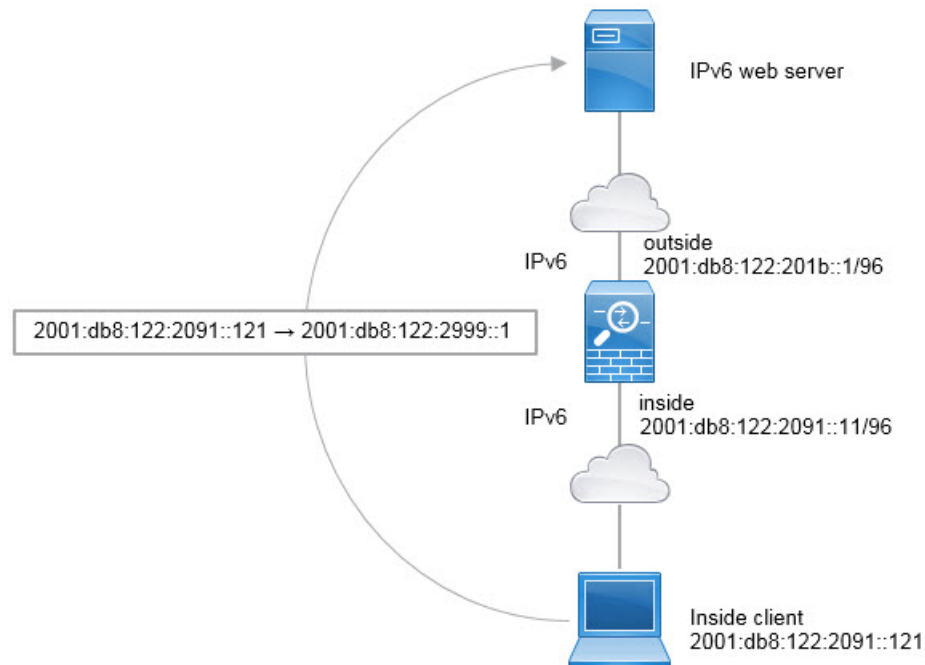
NAT66 : IPv6 アドレスを別の IPv6 アドレスに変換

ある 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、外部ネットワークの別の IPv6 アドレスにアドレスを変換できます。この場合、スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

異なるアドレスタイプ間で変換しているわけではないため、NAT66 変換用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リングできます。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 ルールを単方向にすることができます。

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な変換を設定できます。次の例で、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 の場合は、各メンバーインターフェイスに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。
 - コンテンツ テーブルから [ネットワーク (Network)] を選択し、[+] 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 アドレスとして 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、外部 IPv6 NAT 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 (outside_nat_v6 など)、[ネットワーク (Network)]
を選択して、ネットワーク アドレスとして 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 (または任意の別の名前)。
- [ルール作成目的 (Create Rule For)] = Auto NAT。
- [タイプ (Type)] = Static。
- [送信元インターフェイス (Source Interface)] = inside。
- [宛先インターフェイス (Destination Interface)] = outside。
- [元のアドレス (Original Address)] = inside_v6 ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] = outside_nat_v6 ネットワーク オブジェクト。

Add NAT Rule

Title: NAT66Rule 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	inside_v6	Translated Address	outside_nat_v6
Original Port	Any	Translated Port	Any

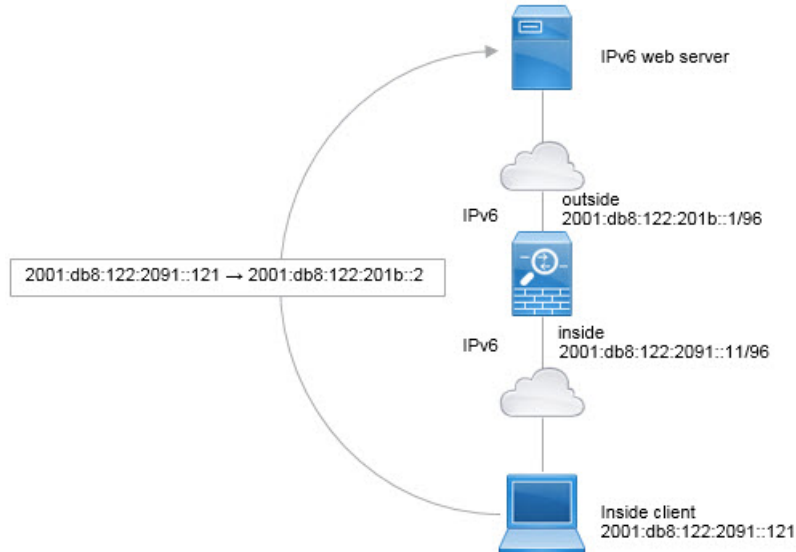
d) [OK]をクリックします。

このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスへのスタティック NAT66 変換を取得します。

NAT66 の例 : 簡単な 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 IPv6 アドレスの異なるポートに内部アドレスをダイナミックに割り当てることです。

ただし、Firepower Device Manager によりインターフェイスの IPv6 アドレスを使用してインターフェイス PAT を設定することはできません。代わりに、ダイナミック PAT プールと同じネットワーク上の 1 つの空きアドレスを使用します。



(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 の場合は、各メンバー インターフェイスに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 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。
 - コンテンツ テーブルから [ネットワーク (Network)] を選択し、[+] 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 アドレスとして 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) [OK] をクリックします。
- e) [+]をクリックし、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を付け (ipv6_pat など)、[ホスト (Host)] を選択して、ホスト アドレスとして 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 (または任意の別の名前)。
- [ルール作成目的 (Create Rule For)] = Auto NAT。
- [タイプ (Type)] = Dynamic。
- [送信元インターフェイス (Source Interface)] = inside。
- [宛先インターフェイス (Destination Interface)] = outside。
- [元のアドレス (Original Address)] = inside_v6 ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] = ipv6_pat ネットワーク オブジェクト。

Add NAT Rule ?

Title	Create Rule for	Status
PAT66Rule	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 ▼	ipv6_pat ▼	Any

- d) [OK]をクリックします。
このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:201b::2 上のポートへのダイナミック PAT66 変換を取得します。

NAT のモニタリング

NAT 接続をモニタしてトラブルシュートするには、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 nat** : NAT ルールとルールごとのヒット カウントが表示されます。NAT のその他のアスペクトを表示するための追加キーワードがあります。
- **show xlate** : 現在アクティブになっている実際の NAT 変換が表示されます。
- **clear xlate** : アクティブな NAT 変換を削除できます。既存の接続ではその接続が終了するまで古い変換スロットが使用されるため、NAT ルールを変更すると、アクティブな変換の削除が必要になることがあります。変換を削除することで、システムは新しいルールに基づき、次にクライアントの接続が試行されるときにそのクライアントに対する新しい変換を作成できます。

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。

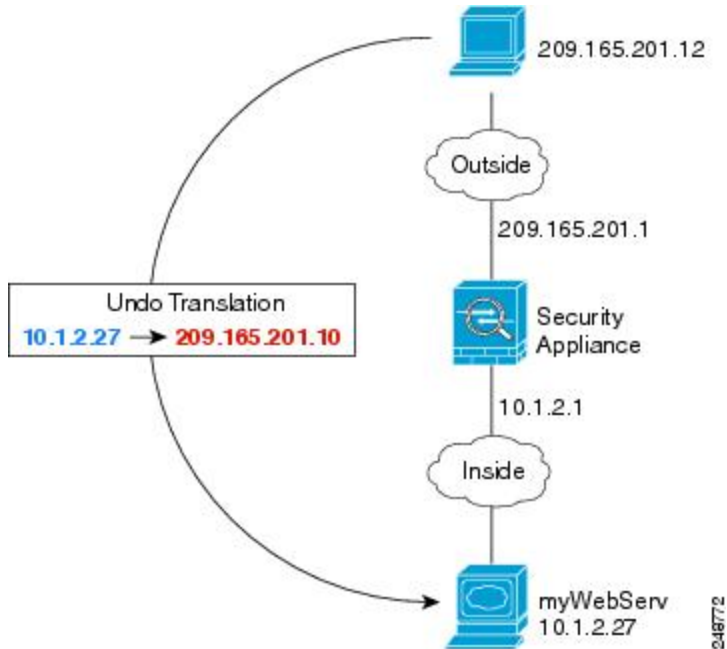
内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

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 の場合は、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 15: 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。
 - コンテンツ テーブルから [ネットワーク (Network)] を選択し、[+] 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を付け (WebServerPrivate など)、[ホスト (Host)] を選択して、実際のホスト IP アドレスとして 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、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を付け (WebServerPublic など)、[ホスト (Host)]を選択して、ホストアドレスとして 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 (または任意の別の名前)。
- [ルール作成目的 (Create Rule For)] = Auto NAT。
- [タイプ (Type)] = Static。
- [送信元インターフェイス (Source Interface)] = inside。
- [宛先インターフェイス (Destination Interface)] = outside。
- [元のアドレス (Original Address)] = WebServerPrivate ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] = WebServerPublic ネットワーク オブジェクト。

The screenshot shows the 'Add NAT Rule' configuration page. At the top, the title is 'Add NAT Rule'. Below this, there are two main sections: 'Title' and 'Create Rule for'. The 'Title' field is set to 'WebServer'. The 'Create Rule for' dropdown is set to 'Auto NAT'. There is a toggle switch to the right of the 'Create Rule for' dropdown, which is currently turned on. Below this, there is a descriptive text: '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.' Below this, there are two more sections: 'Placement' and 'Type'. The 'Placement' dropdown is set to 'Automatically placed in Auto NAT rules'. The 'Type' dropdown is set to 'Static'. Below these, there are two tabs: 'Packet Translation' and 'Advanced Options'. The 'Packet Translation' tab is active. It shows two columns: 'Original Packet' and 'Translated Packet'. Under 'Original Packet', there are four fields: 'Source Interface' (inside), 'Original Address' (WebServerPrivate), 'Original Port' (Any), and 'Translated Packet' (outside). Under 'Translated Packet', there are four fields: 'Destination Interface' (outside), 'Translated Address' (WebServerPublic), and '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）

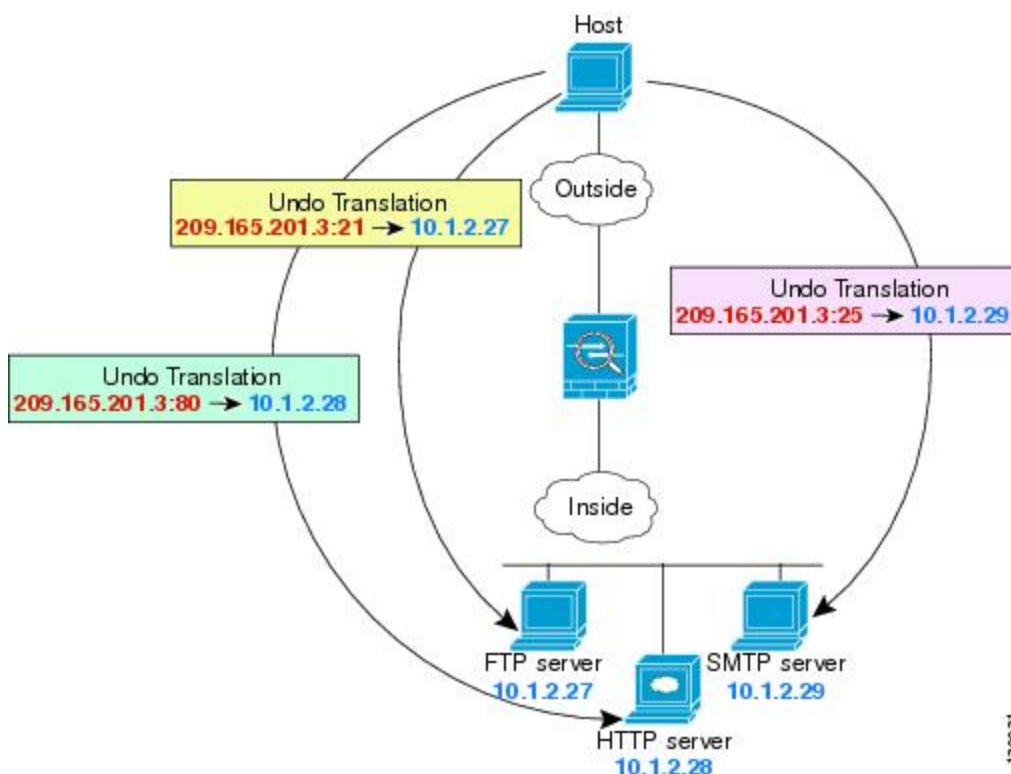
次のポート変換を設定したスタティック NAT の例では、リモートユーザは単一のアドレスで FTP、HTTP、および SMTP にアクセスできるようになります。これらのサーバは実際には、それ

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することができます。



(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ている標準のルーテッドインターフェイスであり、サーバはそのスイッチに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、各サーバが別個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は、各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て対応するルールを設定します。たとえば、ルールでは送信元インターフェイスとして `inside` ではなく `inside1_2`、`inside1_3`、および `inside1_4` を設定します。

図 16: 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。
 - コンテンツのテーブルから [ネットワーク (Network)] を選択し、[+] をクリックします。

- c) ネットワーク オブジェクトの名前（たとえば FTPserver）を入力し、[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。

The screenshot shows the 'New Network Object' configuration window. The title bar is blue with the text 'New Network Object'. Below the title bar, there are four sections: 'Name' with a text input field containing 'FTPServer'; 'Description' with a large empty text area; 'Type' with two radio buttons, 'Network' (unselected) and 'Host' (selected); and 'Host' with a text input field containing '10.1.2.27'.

- d) [追加（Add）]、[OK] の順にクリックします。

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 オブジェクトの名前（たとえば HTTPserver）を入力し、[ホスト（Host）] を選択し、ホストのアドレス（10.1.2.28）を入力します。

The screenshot shows the 'New Network Object' configuration window. The title bar is blue with the text 'New Network Object'. Below the title bar, there are four sections: 'Name' with a text input field containing 'HTTPServer'; 'Description' with a large empty text area; 'Type' with two radio buttons, 'Network' (unselected) and 'Host' (selected); and 'Host' with a text input field containing '10.1.2.28'.

c) [追加 (Add)], [OK] の順にクリックします。

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 オブジェクトの名前 (たとえば SMTPserver) を入力し、[ホスト (Host)]を選択し、ホストのアドレス (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] の順にクリックします。

ステップ 4 3つのサーバに使用するパブリック 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 オブジェクトの名前 (たとえば ServerPublicIP) を入力し、[ホスト (Host)]を選択し、ホストのアドレス (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] の順にクリックします。

ステップ 5 FTP サーバ用に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プします。

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 (または選択した別の名前) 。
- [作成するルールの対象 (Create Rule For)] : Auto NAT。
- [タイプ (Type)] : Static。
- [送信元インターフェイス (Source Interface)] : inside。
- [宛先インターフェイス : (Destination Interface)] : outside。
- [元のアドレス (Original Address)] : FTPserver ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] : ServerPublicIP ネットワーク オブジェクト。
- [元のポート (Original Port)] : FTP ポート オブジェクト。
- [変換されたポート (Translated Port)] : FTP ポート オブジェクト。

d) [OK]をクリックします。

ステップ 6 HTTP サーバ用に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プします。

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 (または選択した別の名前)。
- [作成するルールの対象 (Create Rule For)] : Auto NAT。
- [タイプ (Type)] : Static。
- [送信元インターフェイス (Source Interface)] : inside。
- [宛先インターフェイス : (Destination Interface)] : outside。
- [元のアドレス (Original Address)] : HTTPserver ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] : ServerPublicIP ネットワーク オブジェクト。
- [元のポート (Original Port)] : HTTP ポート オブジェクト。
- [変換されたポート (Translated Port)] : HTTP ポート オブジェクト。

c) [OK]をクリックします。

ステップ 7 SMTP サーバ用に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プします。

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)] : SMTPServer (または選択した別の名前)。
- [作成するルールの対象 (Create Rule For)] : Auto NAT。
- [タイプ (Type)] : Static。
- [送信元インターフェイス (Source Interface)] : inside。
- [宛先インターフェイス : (Destination Interface)] : outside。
- [元のアドレス (Original Address)] : SMTPServer ネットワーク オブジェクト。
- [変換されたアドレス (Translated Address)] : ServerPublicIP ネットワーク オブジェクト。
- [元のポート (Original Port)] : SMTP ポート オブジェクト。
- [変換されたポート (Translated Port)] : SMTP ポート オブジェクト。

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

Source Interface: inside

Original Address: SMTPServer

Original Port: SMTP

Translated Packet

Destination Interface: outside

Translated Address: ServerPublicIP

Translated Port: SMTP

c) [OK]をクリックします。

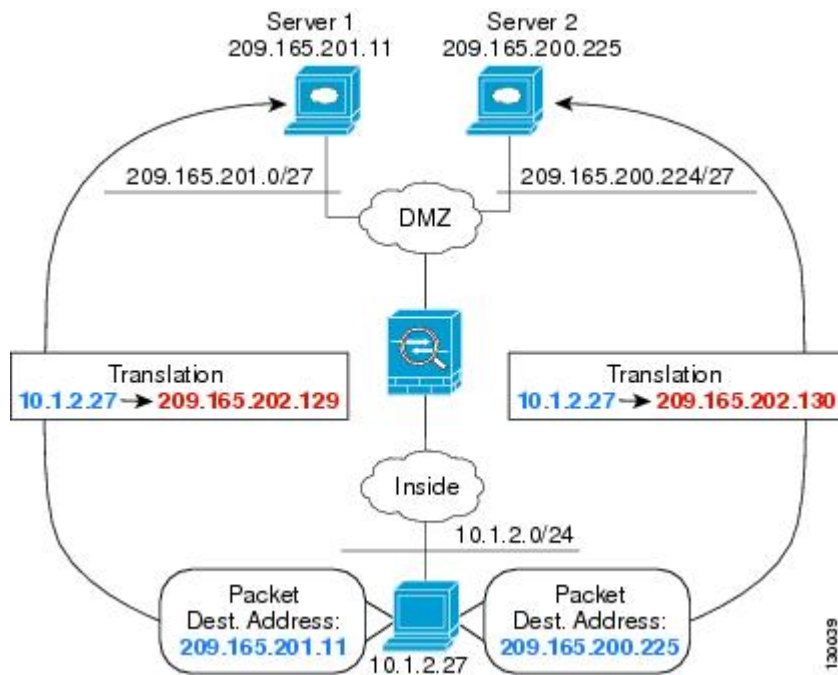
宛先に応じて異なる変換（ダイナミック手動 PAT）

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 17: 異なる宛先アドレスを使用する手動 NAT



手順

- ステップ 1** 内部ネットワークのネットワーク オブジェクトを作成します。
- [オブジェクト (Objects)] を選択します。
 - 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
 - ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、[ネットワーク (Network)] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Object

Name
myInsideNetwork

Description

Type
 Network Host

Network
10.1.2.0/24

d) [追加 (Add)] [OK] をクリックします。

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け (DMZnetwork1 など)、[ネットワーク (Network)] を選択し、ネットワーク アドレス 209.165.201.0/27 を入力します (255.255.255.224 のサブネットマスク)。

New Network Object

Name
DMZnetwork1

Description

Type
 Network Host

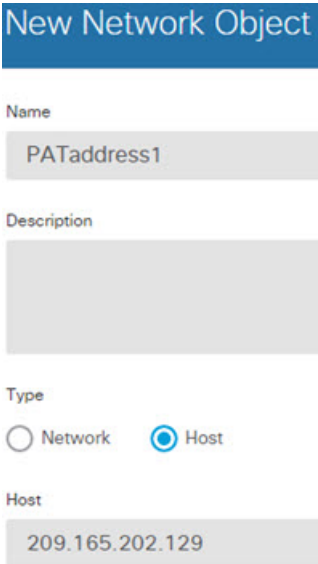
Network
209.165.201.0/27

c) [追加 (Add)] [OK] をクリックします。

ステップ 3 DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

- b) ネットワーク オブジェクトに名前を付け (PATaddress1 など) 、[ホスト (Host)]を選択して、ホストアドレス 209.165.202.129 を入力します。



New Network Object

Name
PATaddress1

Description

Type
 Network Host

Host
209.165.202.129

- c) [追加 (Add)][OK] をクリックします。

ステップ 4 DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

- a) [+] をクリックします。
- b) ネットワーク オブジェクトに名前を付け (DMZnetwork2 など) 、[ネットワーク (Network)] を選択し、ネットワークアドレス 209.165.200.224/27 を入力します (255.255.255.224 のサブネットマスク) 。

New Network Object

Name
DMZnetwork2

Description

Type
 Network Host

Network
209.165.200.224/27

c) [追加 (Add)] [OK] をクリックします。

ステップ 5 DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け (PATaddress2 など)、[ホスト (Host)] を選択して、ホスト アドレス 209.165.202.130 を入力します。

New Network Object

Name
PATaddress2

Description

Type
 Network Host

Host
209.165.202.130

c) [追加 (Add)][OK] をクリックします。

ステップ 6 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

a) [ポリシー (Policies)] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- タイトル (Title) = DMZNetwork1 (または任意の別の名前)。
- ルールの作成先 (Create Rule For) = Manual NAT。
- タイプ (Type) = Dynamic。
- 送信元インターフェイス (Source Interface) = 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。
- 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。
- 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。
- 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。

(注) 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート (Port)] フィールドはすべて空白のままにします。

Add NAT Rule

Title: DMZNetwork1

Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules

Type: Dynamic

Packet Translation | Advanced Options

Original Packet				Translated Packet							
Source Interface		Source Address		Source Port		Destination Interface		Source Address		Source Port	
inside		myInsideNetwork		Any		dmz		PATaddress1		Any	
Destination Address		Destination Port		Destination Address		Destination Port		Destination Address		Destination Port	
DMZnetwork1		Any		DMZnetwork1		Any		DMZnetwork1		Any	

d) [OK]をクリックします。

ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- タイトル (Title) = DMZNetwork2 (または任意の別の名前)。
- ルールの作成先 (Create Rule For) = Manual NAT。
- タイプ (Type) = Dynamic。
- 送信元インターフェイス (Source Interface) = 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。
- 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。
- 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。

- 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。

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。

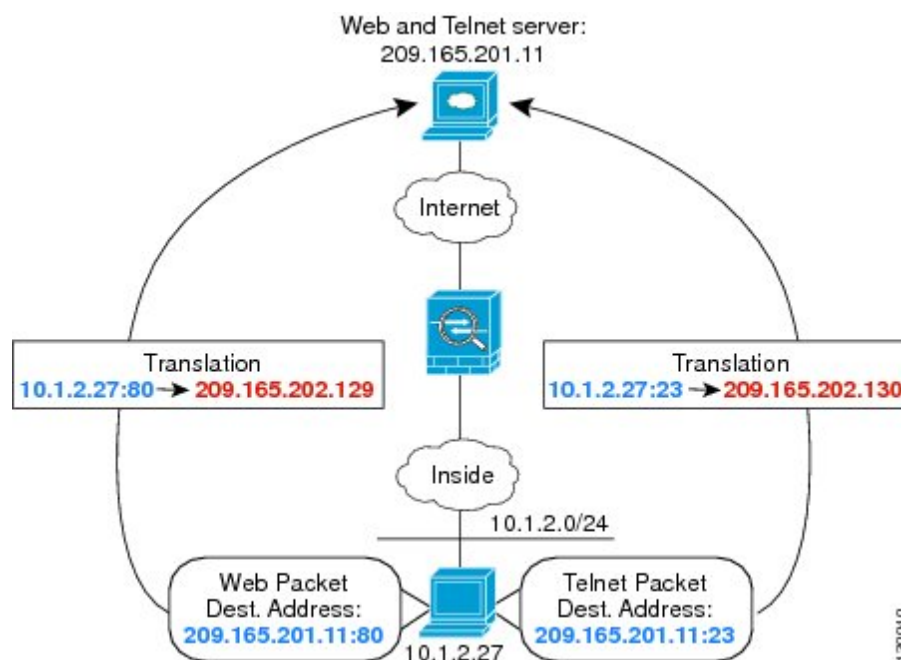
宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

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 18 : 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

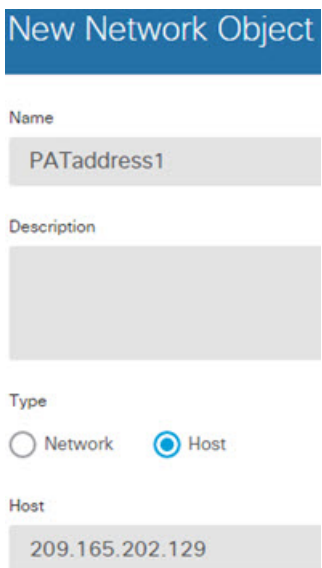
Host
209.165.201.11

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。

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

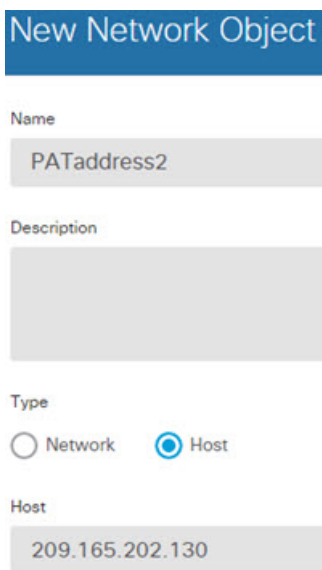
Type
 Network Host

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。

- 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 5 Telnet アクセス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) = TelnetServer (または任意の別の名前)。
- ルールの作成先 (Create Rule For) = Manual NAT。
- タイプ (Type) = Dynamic。
- 送信元インターフェイス (Source Interface) = 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。
- 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。
- 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。
- 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。
- 元の宛先ポート (Original Destination Port) = TELNET ポート オブジェクト。
- 変換済みの宛先ポート (Translated Destination Port) = TELNET ポート オブジェクト。

(注) 宛先アドレスまたはポートを変換しないため、元の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 (または任意の別の名前)。
- ルールの作成先 (Create Rule For) = Manual NAT。
- タイプ (Type) = Dynamic。
- 送信元インターフェイス (Source Interface) = 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。
- 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。
- 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。

- 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。
- 元の宛先ポート (Original Destination Port) = HTTP ポート オブジェクト。
- 変換済みの宛先ポート (Translated Destination Port) = HTTP ポート オブジェクト。

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 による DNS クエリおよび応答のリライト

DNS 応答を修正して、応答内のアドレスを、NAT 設定に適合するアドレスに置換できるように、Firepower Threat Defense デバイスを設定しなければならない場合があります。DNS 修正は、各トランスレーションルールの設定時に設定できます。

これは、NAT ルールに一致する DNS クエリおよび応答内のアドレスをリライトする機能です (たとえば、IPv4 の場合は A レコード、IPv6 の場合は AAAA、逆引き DNS クエリの場合は 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リライトされます。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リライトされます。

NAT ルールに対して DNS リライトを設定しなければならないのは、次のような状況です。

- ルールが NAT64 または NAT46 であり、DNS サーバが外部ネットワーク上にある場合。DNS A レコード (IPv4 用) と AAAA レコード (IPv6) とを変換するため、DNS リライトが必要になります。
- DNS サーバは外部に、クライアントは内部にあり、クライアントが使用する完全修飾ドメイン名の一部が、他の内部ホストとして解決される場合。
- 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ているのに対し、クライアントが外部にあり、これらのクライアントが、内部でホストされているサーバを指す完全修飾ドメイン名にアクセスする場合。

DNS リライトの制限事項

DNS リライトには、次のようないくつかの制限事項があります。

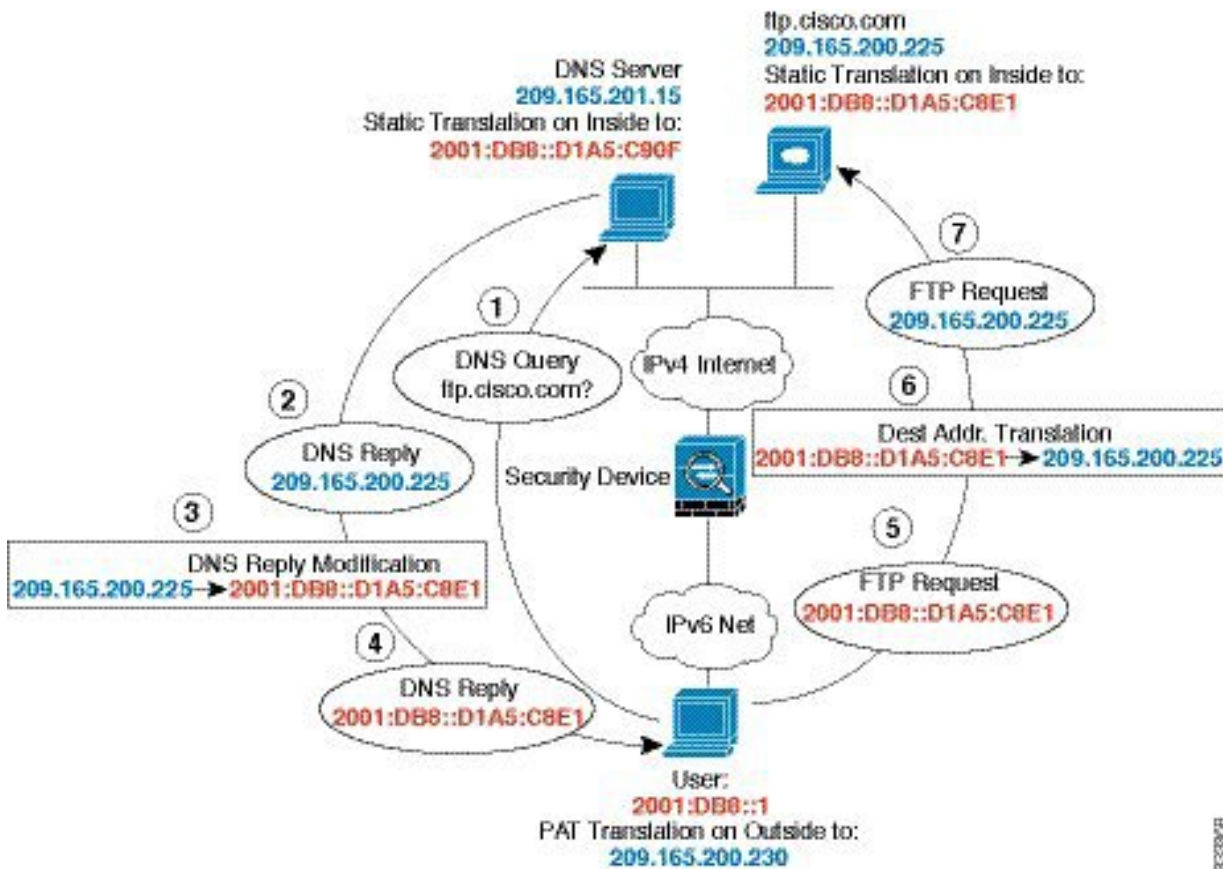
- DNS リライトは PAT には適用されません。個々の A レコードまたは AAAA レコードには複数の PAT ルールが適用可能であり、どの PAT ルールが使用されるかはあいまいであるためです。
- 手動 NAT ルールを設定し、宛先アドレスと発信元アドレスの両方を指定する場合は、DNS 修正を設定することはできません。このようなルールでは、A に送信する場合、B に送信する場合とで、単一アドレスが異なるアドレスに変換される可能性があります。この場合、Firepower Threat Defense デバイスでは、DNS 応答内の IP アドレスを適切な Twice NAT ルールに正確に適合させることができません。DNS 応答には、DNS 要求を促すパケット内に、どのような送信元/宛先アドレスの組み合わせが含まれていたかを示す情報は含まれません。
- DNS リライトは実際には、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 が存在しない場合は、リライトは正しく実行されません。スタティック NAT の場合は、この問題が生じることはありません。
- DNS リライトでは、DNS 動的更新メッセージはリライトされません (opcode 5)。

以下の各トピックでは、NAT ルールにおける DNS リライトのさまざまな例を示します。

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。この場合に、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 サーバは応答として実際のアドレス 209.165.200.225 を返します。

ftp.cisco.com のマッピングアドレス (2001:DB8::D1A5:C8E1、ここで D1A5:C8E1 は 209.165.200.225 の IPv6 の相当物) が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック 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) この例では、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 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)。
- ルールの作成先 (Create Rule For) = Auto NAT。
- タイプ (Type) = Static。
- 送信元インターフェイス (Source Interface) = outside。
- 宛先インターフェイス (Destination Interface) = inside。
- 元のアドレス (Original Address) = ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス (Translated Address) = inside_v6 のネットワーク オブジェクト。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。

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)。
- ルールの作成先 (Create Rule For) = Auto NAT。
- タイプ (Type) = Static。
- 送信元インターフェイス (Source Interface) = outside。
- 宛先インターフェイス (Destination Interface) = inside。
- 元のアドレス (Original Address) = dns_server のネットワーク オブジェクト。
- 変換済みのアドレス (Translated Address) = inside_v6 のネットワーク オブジェクト。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 (または任意の別の名前)。

- ルールの作成先 (Create Rule For) = Auto NAT。
- タイプ (Type) = Dynamic。
- 送信元インターフェイス (Source Interface) = inside。
- 宛先インターフェイス (Destination Interface) = outside。
- 元のアドレス (Original Address) = inside_v6 のネットワーク オブジェクト。
- 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。

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	ipv4_pat
Original Port	Any	Translated Port	Any

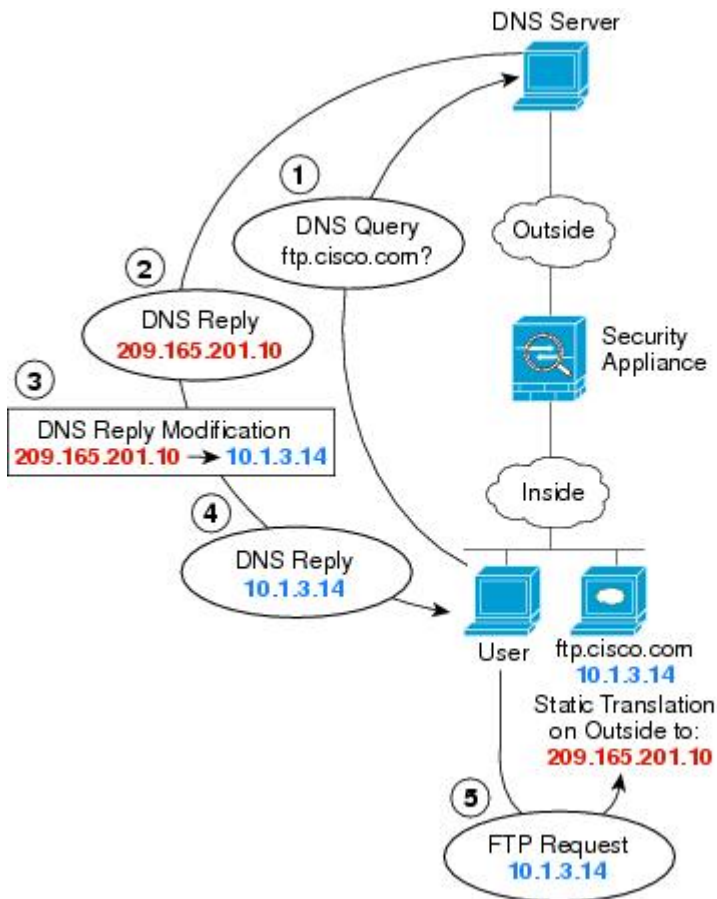
d) [OK]をクリックします。

DNS 応答修正 : Outside 上の 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可視の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。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、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 サーバは応答でマッピングアドレス (209.165.201.10) を示します。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 にトラフィックを送信することを試みます。



(注) この例では、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 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

Description

Type

Network Host

Host

- 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

Description

Type

Network Host

Host

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)。
 - ルールの作成先 (Create Rule For) = Auto NAT。
 - タイプ (Type) = Static。
 - 送信元インターフェイス (Source Interface) = inside。
 - 宛先インターフェイス (Destination Interface) = outside。
 - 元のアドレス (Original Address) = ftp_server のネットワーク オブジェクト。
 - 変換済みのアドレス (Translated Address) = ftp_server_outside 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: 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

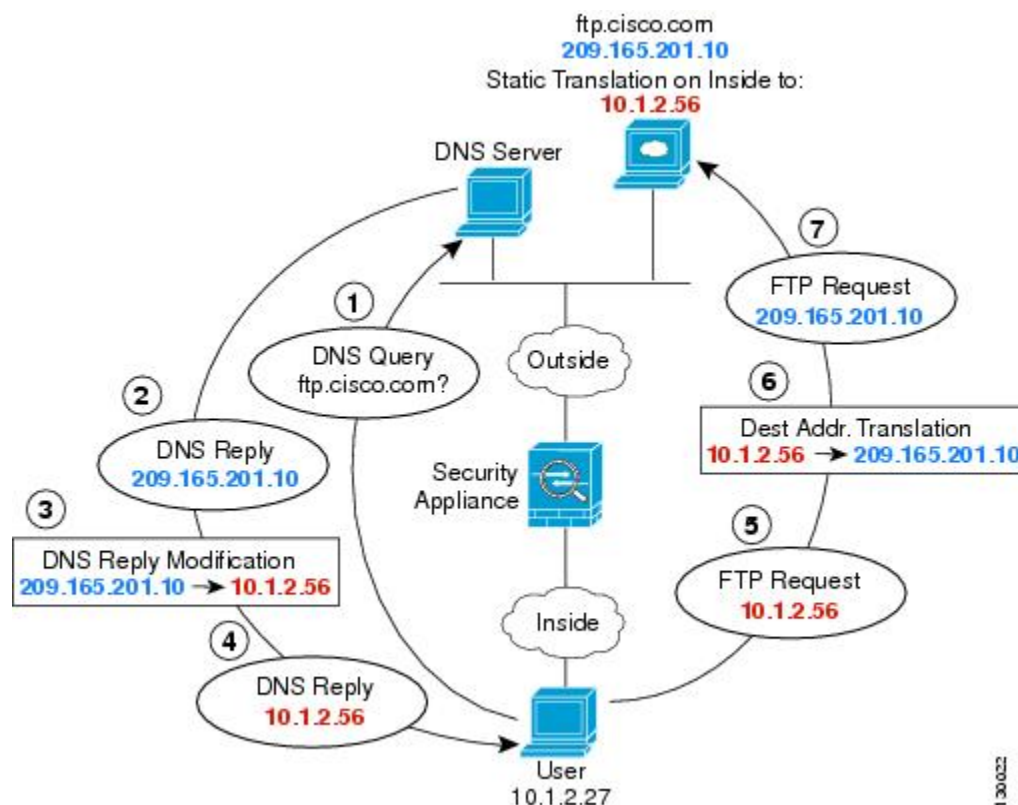
Packet Translation Advanced Options

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、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.201.10 を示します。ftp.cisco.com のマッピングアドレス (10.1.2.56) が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。



(注) この例では、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 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。

- 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 209.165.201.10 を入力します。

Add Network Object

Name
ftp_server

Description

Type
 Network Host

Host
209.165.201.10

- d) [追加 (Add)][OK] をクリックします。
- e) [+]をクリックして FTP サーバの変換済みアドレスを定義します。
ネットワーク オブジェクトに名前を付け (ftp_server_translated など)、[ホスト (Host)]を選択して、ホストアドレス 10.1.2.56 を入力します。

Add Network Object

Name
ftp_server_translated

Description

Type
 Network Host

Host
10.1.2.56

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
 - タイトル (Title) = FTPServer (または任意の別の名前)。
 - ルールの作成先 (Create Rule For) = Auto NAT。
 - タイプ (Type) = Static。
 - 送信元インターフェイス (Source Interface) = outside。
 - 宛先インターフェイス (Destination Interface) = inside。
 - 元のアドレス (Original Address) = ftp_server のネットワーク オブジェクト。
 - 変換済みのアドレス (Translated Address) = ftp_server_translated のネットワーク オブジェクト。
 - [詳細オプション (Advanced Options)] タブで、[このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] を選択します。

Add NAT Rule

Title: 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	ftp_server_transla
Original Port	Any	Translated Port	Any

- d) [OK] をクリックします。



第 **III** 部

バーチャル プライベート ネットワーク (VPN)

• [サイト間 VPN, 291 ページ](#)



第 11 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、公共の送信元（インターネット、またはその他のネットワーク）を使用するリモートピア間に、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 パケット内にデータ パケットをカプセル化し、IP ベースのネットワーク上を転送します。VPN では暗号化を使用することでプライバシーを保証し、認証によってデータ整合性を保証します。

- [VPN の基本, 291 ページ](#)
- [サイト間 VPN の管理, 297 ページ](#)
- [サイト間 VPN のモニタリング, 314 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することができます。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。

Firepower Threat Defense では、システムは、VPN トラフィックがアクセス コントロール ポリシーを通じて受け渡されるまで、VPN トラフィックを送信しません。着信トンネルパケットは復号されてから、Snort プロセスへ送信されます。発信パケットは、Snort によって処理されてから、暗号化されます。VPN トンネルのエンドポイントノードごとに保護されたネットワークを特定すると、どのトラフィックに Firepower Threat Defense デバイスをパススルーして内部ホストへ到達することが許可されるかが決まります。さらに、システムは、トンネルがダウンしている場合は、トンネルトラフィックをパブリックなソースに送信しません。

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 フェーズで構成されています。フェーズ 1 では、2つの IKE ピア間でセキュリティ 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 で安全に通信できます。フェーズ 2 のネゴシエーションでは、IKE は IPsec などの他のアプリケーションの SA を確立します。どちらのフェーズも、接続をネゴシエートするときにプロポーザルを使用します。

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、各ピアが共通 (共有) IKE ポリシーに同意することで始まります。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。



(注) 認証には事前共有キーのみが使用されます。

- 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 プロポーサルを使用して、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い出します。

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 プロポーサルに対して使用する暗号化アルゴリズムを決定する場合は、VPN 内のデバイスによってサポートされるアルゴリズムに限定されます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。各設定が、安全性の高い順に順序付けられ、ピアとのネゴシエーションにはこの順序が使用されます。IKEv1 では、1つのオプションしか選択できません。

IPsec プロポーザルでは、このアルゴリズムは Encapsulating Security Protocol (ESP) によって使用されます。これにより、認証、暗号化、およびアンチリプレイサービスが実現します。ESP の IP プロトコルタイプは 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の接頭辞が「ESP-」となります。

使用するデバイス ライセンスが強力な暗号化に対応している場合は、以下の暗号化アルゴリズムを選択できます。ライセンスが強力な暗号化に対応していない場合は、DESのみを選択できます。

- AES-GCM (IKEv2 のみ) : Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) は、機密性とデータ発信元認証を可能にするブロック暗号動作モードであり、AES より強力なセキュリティを実現します。AES-GCM では、128、192、および 256 ビットの 3 種類の強度を持つキーを使用できます。長いキーほどセキュリティに優れますが、その分パフォーマンスが低くなります。GCM は AES モードの 1 つであり、NSA Suite B をサポートする必要があります。NSA Suite B は、暗号強度の米国連邦標準規格に適合するために各デバイスがサポートする必要のある、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 Galois Message Authentication Code (AES-GMAC) はブロック暗号動作モードであり、発信元認証のみを実現します。これは、データを暗号化せずにデータ認証を可能にする、AES-GCM の一形態です。AES-GMAC では、128、192、および 256 ビットの 3 種類の強度を持つキーを使用できます。
- AES : Advanced Encryption Standard (AES) は対称暗号アルゴリズムであり、DES より強力なセキュリティを実現し、3DES より効率的な計算方式です。AES では、128、192、および 256 ビットの 3 種類の強度を持つキーを使用できます。長いキーほどセキュリティに優れますが、その分パフォーマンスが低くなります。
- 3DES : トリプル DES と呼ばれ、56 ビットのキーを用い、暗号化を 3 回繰り返します。個々のデータ ブロックをそれぞれ異なるキーで 3 回ずつ処理するため、DES より強力なセキュリティを実現できます。ただし、DES より多くのシステムリソースを消費し、パフォーマンスも低速です。
- DES : DES (データ暗号化標準) は 56 ビットのキーによる暗号化を行う、対称的な秘密キー ブロック アルゴリズムです。3DES より高速で、消費リソースも少なく済みますが、安全性は劣ります。強力なデータ機密性が不要であり、システムリソースまたは速度を重視する場合は、DES を選択します。
- Null : Null 暗号化アルゴリズムは、暗号化を使用しない認証を実現します。一般的には、テスト目的のみで使用します。

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 Encapsulating Security Protocol (ESP) による認証に使用されます。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、アルゴリズム名の接頭辞が「ESP-」となり、「-HMAC」 (Hash Method Authentication Code) という接尾辞も使用されます。

IKEv2 では、複数のハッシュアルゴリズムを設定できます。各設定が、安全性の高い順に順序付けられ、ピアとのネゴシエーションにはこの順序が使用されます。IKEv1 では、1 つのオプションしか選択できません。

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)] : 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。

Standard SHA (SHA1) は 160 ビットのダイジェストを生成します。

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することができます。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。しかし、暗号化オプションとしていずれかの AES-GCM/GMAC オプションを選択した場合は、NULL 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

以下の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec セキュリティ アソシエーション (SA) キーを生成できます。各グループは、それぞれ係数のサイズが異なります。係数のサイズが大きいほど、セキュリティは高まりますが、より多くの処理時間が必要となります。両方のピアが、一致する係数グループを使用する必要があります。

AES 暗号化を選択する場合、AES に必要となる大きなキー サイズをサポートするには、Diffie-Hellman (DH) グループ 5 以上を使用する必要があります。IKEv1 ポリシーでは、グループ 1、2、および 5 のみが許可されます。

NSA Suite B 暗号化仕様を実装するには、IKEv2 を使用し、楕円曲線 Diffie-Hellman (ECDH) オプション 19、20、または 21 のいずれか 1 つを選択します。2048 ビットの係数を使用する楕円曲線オプションおよびグループは、Logjam などの攻撃にさらされる可能性は低くなります。

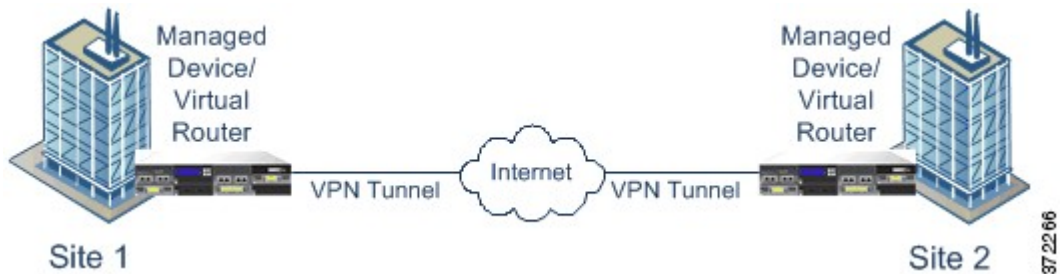
IKEv2 では、複数のグループを設定できます。各設定が、安全性の高い順に順序付けられ、ピアとのネゴシエーションにはこの順序が使用されます。IKEv1 では、1 つのオプションしか選択できません。

- 1 : Diffie-Hellman グループ 1 (768 ビット係数)
- 2 : Diffie-Hellman グループ 2 (1024 ビット係数)
- 5 : Diffie-Hellman グループ 5 (1536 ビット係数) 128 ビット キーに対して最適な保護強度とみなされます。
- 14 : Diffie-Hellman グループ 14 (2048 ビット係数)。192 ビット キーに対して最適な保護強度とみなされます。
- 19 : Diffie-Hellman グループ 19 (256 ビット楕円曲線)
- 20 : Diffie-Hellman グループ 20 (384 ビット楕円曲線)
- 21 : Diffie-Hellman グループ 21 (521 ビット楕円曲線)
- 24 : Diffie-Hellman グループ 24 (2048 ビット係数および 256 ビット素数位数サブグループ)

VPN トポロジ

Firepower Device Manager を使用して設定できるのは、ポイントツーポイント VPN 接続のみです。すべての接続はポイントツーポイントですが、デバイスが参加する各トンネルを定義することで、より大規模なハブアンドスポーク VPN、またはメッシュ VPN にリンクできます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。ポイントツーポイントの VPN トポロジでは、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピア デバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。



サイト間 VPN の管理

バーチャルプライベートネットワーク (VPN) は、インターネットや他のネットワークなどのパブリックソース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 は、トンネルを使用して、IP ベースのネットワークを介して転送するために通常の IP パケット内にデータパケットをカプセル化します。VPN では、プライバシーを確保するために暗号化が使用され、データの整合性を確保するために認証が使用されます。

ピアデバイスへの VPN 接続を作成できます。すべての接続はポイントツーポイントですが、すべての関連接続を設定することにより、デバイスをより大きなハブアンドスポーク VPN またはメッシュ VPN にリンクさせることができます。



- (注) VPN 接続は、暗号化を使用してネットワークのプライバシーを保護します。使用できる暗号化アルゴリズムは、基本ライセンスが強力な暗号化を許可するかどうかによって異なります。これは、Cisco Smart License Manager に登録するときにデバイス上でエクスポート制御機能を許可するオプションを選択した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エクスポート制御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** デバイスをクリックし、[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。
これにより [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, \(298 ページ\)](#) を参照してください。
まだ接続がない場合は、[サイト間接続の作成 (Create Site-to-Site Connection)] ボタンをクリックすることもできます。
 - 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, \(298 ページ\)](#) を参照してください。
 - 接続設定の概要をクリップボードにコピーするには、その接続のコピーアイコン (📄) をクリックします。この情報をドキュメントに貼り付けて、リモートデバイスの管理者に送信し、接続の他方の端を設定するために役立てることができます。
 - 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があることを前提に、デバイスを別のデバイスにリンクするためのポイントツーポイント VPN 接続を作成できます。すべての接続が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 へリンクできます。



(注) ローカルネットワークとリモートネットワークの組み合わせごとに単一の 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内で一意の場合は、ローカルネットワークに対応する複数の接続を作成できます。

手順

ステップ 1 デバイスをクリックし、[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。

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は、[サイト間接続の作成 (Create Site-to-Site Connection)] ボタンをクリックすることもできます。
- 既存の接続を編集するには、接続の編集アイコン (🔗) 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。スペースなしで最大 64 文字です。たとえば、MainOffice と入力します。名前として IP アドレスを使用することはできません。
- ローカル サイト (Local Site) : これらのオプションはローカル 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) : 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することはできません。
 - 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。これらのネットワーク上のユーザは、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では IPv4 または IPv6 アドレスを使用できますが、接続の各側でアドレスタイプを一致させる必要があります。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。単一の接続の両側で、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をオーバーラップさせ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は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 アドレスを入力します。
 - リモートネットワーク (Remote Network) : [+] をクリックし、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、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 [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) ライセンスによって、選択可能な暗号化プロトコルが決まります。最も基本的なオプション以外にもあらゆるオプションを選択するには、強力な暗号化、つまり十分なエクスポート制御を行うために適したライセンスが必要です。

- 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) の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。デバイスが別のピアとの接続のネゴシエーションを試行する場合は、許可されたバージョンか、他のピアが受け入れるバージョンのどちらも使用できます。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に、デバイスは他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は、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。これはグローバルポリシーです。有効にしたオブジェクトは、すべての VPN に適用されます。IKE バージョンごとに現在グローバルで有効なポリシーを調べたり、新しいポリシーの有効化や作成を行ったりするには、[編集 (Edit)] をクリックします。詳細については、[グローバル IKE ポリシーの設定](#)、(300 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 トンネル内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、各 IKE バージョンのプロポーザルを選択します。許可するプロポーザルをすべて選択します。エクスポートコンプライアンスに基づいて異なるシステムデフォルトを選択するだけの場合は、[デフォルトに設定 (Set Default)] をクリックします。システムは、ピアと合意が得られるまで、最強なプロポーザルから最弱なプロポーザルまで順次ネ

ゴシエートします。詳細については、[IPsec プロポーザルの設定](#)、(305 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) : このデバイスと VPN 接続のリモートデバイスで定義されたキーです。IKEv2 では、これらのキーは異なります。キーには、1 ~ 127 文字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ているキーです。キーには、1 ~ 127 文字の英数字を指定できます。
- NAT 免除 (NAT Exempt) : ローカル VPN アクセス インターフェイスの NAT ポリシーから VPN トラフィックを除外するかどうかを指定します。ローカル ネットワークに NAT ルールを適用しない場合は、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 (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動作します。ローカル ネットワークが複数のルーテッド インターフェイスの背後に存在する場合は、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](#)、(308 ページ) を参照してください。
- Perfect Forward Secrecy 用の Diffie-Hellman グループ (Diffie-Hellman Group for Perfect Forward Secrecy) : 暗号化された交換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に、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、以降の復号から交換が保護されます。このことは、交換全体が記録され、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 を有効にするには、[モジュールグループ (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 キー派生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、オプションが IKEv1 でサポートされているオプションに限定されます。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](#)、(295 ページ) を参照してください。

ステップ 6 [Next] をクリックします。

ステップ 7 サマリを確認し、[完了 (Finish)] をクリックします。
サマリ情報はクリップボードにコピーされます。ドキュメントに情報を貼り付け、それを使用してリモートピアの設定に役立てたり、ピアの設定担当者にそれを送信したりすることができます。

グローバル IKE ポリシーの設定

Internet Key Exchange (IKE; インターネット キー エクスチェンジ) は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association (SA; セキュリティ アソシエーション) の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの

他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKE ポリシー オブジェクトはこれらのネゴシエーションに対して IKE プロポーザルを定義します。有効にするオブジェクトは、ピアが VPN 接続をネゴシエートするときに使用するものであり、接続ごとに異なる IKE ポリシーを指定することはできません。各オブジェクトの相対的な優先順位は、これらの中でどのポリシーを最初に試すかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKE グローバル ポリシーを定義するには、各 IKE バージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティ ポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト ページでグローバル ポリシーを設定する方法について説明します。VPN 接続を編集しているときに IKE ポリシー設定の [編集 (Edit)] をクリックすることで、ポリシーの有効化、無効化および作成が行えます。

手順

-
- ステップ 1** [オブジェクト (Objects)] を選択し、次に目次から [IKE ポリシー (IKE Policies)] を選択します。IKEv1 と IKEv2 のポリシーが別のリストに表示されます。
- ステップ 2** 各 IKE バージョンで許可する IKE ポリシーを有効にします。
- a) オブジェクトテーブル上部の [IKEv1] または [IKEv2] を選択すると、そのバージョンのポリシーが表示されます。
 - b) 適切なオブジェクトを有効にし、要件を満たしていないオブジェクトを無効にするには、[状態 (State)] トグルをクリックします。
セキュリティ要件の一部が既存のオブジェクトに反映されていない場合、要件に合う新しい要件を定義します。詳細については、次のトピックを参照してください。
 - [IKEv1 ポリシーの設定, \(302 ページ\)](#)
 - [IKEv2 ポリシーの設定, \(303 ページ\)](#)
 - 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、それを編集します。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 接続を定義するときに IKEv1 ポリシーに必要なパラメータが含まれています。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。

定義済みの複数の IKEv1 ポリシーがあります。自分のニーズに適したポリシーがある場合は、[状態 (State)] トグルをクリックして有効にできます。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ポリシー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 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 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 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 [IKE ポリシー (IKE Policies)] 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 ポリシーを表示します。
- ステップ 3** 自分の要件を満たすシステム定義ポリシーが存在する場合は、[状態 (State)] トグルをクリックして有効にします。
[状態 (State)] トグルを使用して、不要なポリシーを無効にすることもできます。相対的な優先順位に基づき、最初に試されるポリシーが決まります。低い数字の方が優先順位が高くなります。
- 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、オブジェクトのゴミ箱アイコン (🗑️) をクリックします。
- ステップ 5** IKEv1 の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順位 (1 ~ 65,535)。この優先順位によって、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、最高の優先順位を持つ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は、次に低い優先順位で定義されているパラメータの使用が試行されます。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。状態を変更するにはトグルをクリックします。有効になっているポリシーのみが IKE ネゴシエーション時に使用されます。
- [認証 (Authentication)] : 2つのピア間で使用する認証方式。事前共有キーを選択します。事前共有キーを使用すると、秘密鍵を2つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。ピアに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
- [暗号化 (Encryption)] : フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティアソシエーション (SA) の確立に使用される暗号化アルゴリズム。オプションの説明については、[使用する暗号化アルゴリズムの決定](#)、(293 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](#)、(295 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](#)、(294 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 (秒単位、120 – 2147483647) 。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。

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 接続を定義するときに IKEv2 ポリシーに必要なパラメータが含まれています。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。

定義済みの複数の IKEv2 ポリシーがあります。自分のニーズに適したポリシーがある場合は、[状態 (State)] トグルをクリックして有効にできます。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ポリシー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 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 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 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 [IKE ポリシー (IKE Policies)] 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 ポリシーを表示します。
- ステップ 3** 自分の要件を満たすシステム定義ポリシーが存在する場合は、[状態 (State)] トグルをクリックして有効にします。
- [状態 (State)] トグルを使用して、不要なポリシーを無効にすることもできます。相対的な優先順位に基づき、最初に試されるポリシーが決まります。低い数字の方が優先順位が高くなります。
- 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、オブジェクトのゴミ箱アイコン (🗑️) をクリックします。

- ステップ 5** IKEv2 の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順位 (1 ~ 65,535)。この優先順位によって、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、最高の優先順位を持つ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は、次に低い優先順位で定義されているパラメータの使用が試行されます。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。状態を変更するにはトグルをクリックします。有効になっているポリシーのみが IKE ネゴシエーション時に使用されます。
 - [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。許可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) オプションと通常モードオプションの両方を含めることはできません (通常モードでは整合性ハッシュを選択する必要がありますが、混合モードでは個別の整合性ハッシュの選択は禁止されています)。システムは、一致が得られるまで、最も強いアルゴリズムから最も弱いアルゴリズムの順に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](#)、(293 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、一致が得られるまで、最も強いグループから最も弱いグループの順に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](#)、(295 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、一致が得られるまで、最も強いアルゴリズムから最も弱いアルゴリズムの順に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](#)、(294 ページ) を参照してください。
- [擬似乱数関数 (PRF) ハッシュ (Pseudo Random Function (PRF) Hash)]: ハッシュアルゴリズムの擬似乱数関数 (PRF) 部分であり、IKEv2 トンネル暗号化に必要なキー材料とハッシュ操作を取得するためのアルゴリズムとして使用されます。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、一致が得られるまで、最も強いアルゴリズムから最も弱いアルゴリズムの順に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](#)、(294 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 (秒単位、120 – 2147483647)。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。

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 を設定するための最も安全な手法の 1 つです。IPsec は IP パケットレベルのデータ暗号化を実現し、各種の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を提供します。IPsec を使用すると、データはトンネルを経由し、パブリック ネットワーク上を送信されます。このトンネルは、2つのピア間をつなぐ、セキュアで論理的な通信パスです。IPsec トンネル内に入るトラフィックは、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およびアルゴリズムの組み合わせによってセキュリティ保護されます。IPsec のセキュリティアソシエーション (SA) ネゴシエーションの実施中、各ピアは、2つのピアの両方に共通のトランスフォームセットを検索します。

IKE のバージョン (IKEv1 または IKEv2) ごとに、それぞれ異なる IPsec プロポーザルオブジェクトが使用されます。

- IKEv1 IPsec プロポーザルを作成する場合は、IPsec が動作するモードを選択し、必要となる暗号化および認証のタイプを定義します。アルゴリズムに対して選択できるのは、1つのオプションのみです。VPN で複数の組み合わせがサポートされるようにするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成して選択する必要があります。

- IKEv2 IPsec プロポーザルを作成する場合は、VPN で許可されるすべての暗号化およびハッシュアルゴリズムを選択できます。各設定が、安全性の高い順に順序付けられ、一致する設定が見つかるまで、ピアとのネゴシエーションにはこの順序が使用されます。これにより、IKEv1 のように、許可された組み合わせを 1 つずつ送信する必要がなく、許可されたすべての組み合わせを 1 回のプロポーザルで伝送できる場合もあります。

IKEv1 および IKEv2 IPsec プロポーザルの両方に、Encapsulating Security Protocol (ESP) が使用されます。このプロトコルにより、認証、暗号化、およびアンチリプレイ サービスが実現します。ESP の IP プロトコル タイプは 50 です。



(注) IPsec トンネルに対しては、暗号化と認証の両方を使用することを推奨します。

以下の各トピックでは、各 IKE バージョンごとの IPsec プロポーザルの設定方法について説明します。

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、オブジェクトのゴミ箱アイコン (🗑️) 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](#)、(293 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](#)、(294 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、オブジェクトのゴミ箱アイコン (🗑️) 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、一致が得られるまで、最も強いアルゴリズムから最も弱いアルゴリズムの順に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](#), (293 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、一致が得られるまで、最も強いアルゴリズムから最も弱いアルゴリズムの順に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](#), (294 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。

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

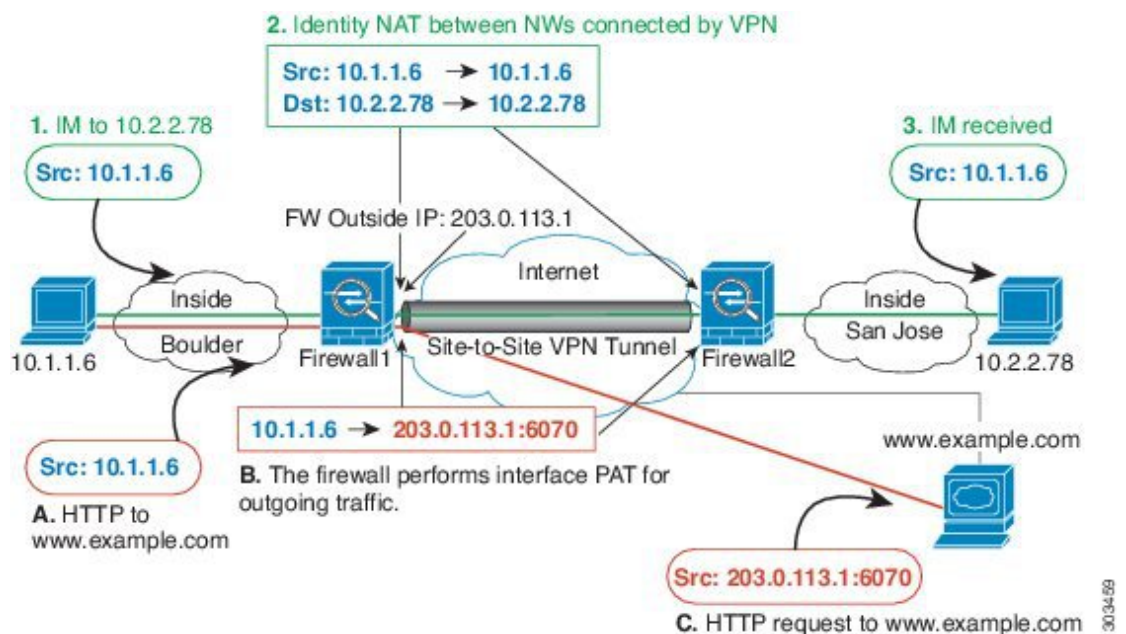
ます。その代わりに、接続内のローカルネットワークが複数のルーテッドインターフェイス、または1つ以上のブリッジグループメンバーの背後に存在する場合、NAT 除外ルールを手動で設定する必要があります。

NAT ルールから VPN トラフィックを除外するには、宛先がリモートネットワークのときにローカルトラフィックの手動アイデンティティ NAT ルールを作成します。次に、任意の宛先（インターネットなど）のトラフィックに NAT を適用します。ローカルネットワークに複数のインターフェイスがある場合、各インターフェイスにルールを作成します。次の点も考慮してください。

- 接続内に複数のローカルネットワークがある場合、ネットワークを定義するオブジェクトを保持するネットワーク オブジェクトグループを作成します。
- VPN に IPv4 ネットワークと IPv6 ネットワークの両方を含める場合、それぞれに個別のアイデンティティ NAT ルールを作成します。

次の例では、ボールドーとサンノゼのオフィスを接続するサイトツーサイトトンネルを示します。インターネットに渡すトラフィックについて（たとえばボールドーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールドーの 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 19: サイトツーサイト VPN のためのインターフェイス PAT およびアイデンティティ NAT



次の例は、Firewall1（ボールドー）の設定を示します。例では、内部インターフェイスがブリッジグループであると仮定するため、各メンバーインターフェイスにルールを記述する必要があります。

ます。ルーティングされた内部インターフェイスが 1 つある場合も複数ある場合も、プロセスは同じです。



- (注) この例では、IPv4 のみと仮定します。VPN に IPv6 ネットワークも含まれる場合、IPv6 にはパラレルルールを作成します。IPv6 インターフェイス PAT は実装できないため、PAT を使用するには固有の IPv6 アドレスを持つホスト オブジェクトを作成する必要があることに注意してください。

手順

- ステップ 1** さまざまなネットワークを定義するには、オブジェクトを作成します。
- [オブジェクト (Objects)]を選択します。
 - 目次から [ネットワーク (Network)]を選択し、[+] をクリックします。
 - ネットワーク内でボールドーを特定します。
ネットワーク オブジェクトに名前を付け (boulder-network など)、[ネットワーク (Network)] を選択して、ネットワーク アドレス 10.1.1.0/24 を入力します。

Add Network Object

Name

boulder-network

Description

Type

Network Host

Network

10.1.1.0/24

- [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。

Add Network Object

Name
sanjose-network

Description

Type
 Network Host

Network
10.2.2.0/24

f) [OK]をクリックします。

ステップ 2 Firewall1 (ボールドー) 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)。
- ルールの作成先 (Create Rule For) = Manual NAT。
- 配置 (Placement) = 特定のルールの上 (Above a SpecificRule) 。 [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) = 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) = 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。
- 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。
- 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。

- 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。
 (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)。
 - ルールの作成先 (Create Rule For) = Manual NAT。
 - 配置 (Placement) = 特定のルールの下 (Below a SpecificRule)。[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) = 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) = 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。
 - 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) = any。
 - 変換済みの宛先アドレス (Original Destination Address) = 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 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` 向けとなります。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 `any` の場合は `sanjose-network` 向けとなります。

サイト間 VPN のモニタリング

サイト間 VPN 接続をモニタしてトラブルシュートするには、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` : IPsec の運用データと統計が表示されます。

- **show ipsec sa** : VPNセッション（セキュリティアソシエーション）が表示されます。これらの統計は **clear ipsec sa counters** コマンドを使用してリセットできます。
- **show isakmp** : ISAKMP の運用データと統計が表示されます。



第 **IV** 部

システム管理

- [システム設定, 319 ページ](#)
- [システム管理, 331 ページ](#)



第 12 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を指定する方法について説明します。この設定は、システム機能全体が対象となります。

- [管理アクセス リストの設定, 319 ページ](#)
- [診断ロギングの設定, 321 ページ](#)
- [DHCP サーバの設定, 322 ページ](#)
- [DNS の設定, 324 ページ](#)
- [管理インターフェイスの設定, 325 ページ](#)
- [デバイスのホスト名の設定, 327 ページ](#)
- [Network Time Protocol \(NTP\) の設定, 327 ページ](#)
- [Cisco Collective Security Intelligence \(CSI\) の URL フィルタリングの設定の設定, 328 ページ](#)
- [クラウド管理の設定, 329 ページ](#)

管理アクセス リストの設定

デフォルトでは、任意の IP アドレスから、管理アドレス上のデバイスの Firepower デバイスマネージャ Web インターフェイスまたは CLI インターフェイスに到達できます。システム アクセスは、ユーザ名とパスワードのみによって保護されています。ただし、別のレベルの保護を提供するために、特定の IP アドレスまたはサブネットからの接続のみを許可するアクセスリストを設定できます。

また、データ インターフェイスを開いて、Firepower デバイスマネージャまたは CLI への SSH 接続を許可することもできます。その後、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、デバイスをリモートで設定できるように、外部インターフェイスへの管理アクセスを許可できます。ユーザ名とパスワードは、望ましくない接続を阻止します。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。これは、デフォルトの "inside" ブリッジグルー

ブを持つデバイス モデルの場合には、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の IP アドレス（デフォルトは 192.168.1.1）に達する Firepower デバイスマネージャ接続を確立できることを意味しています。デバイスに入力する際に経由するインターフェイスでのみ管理接続を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約すると、自分自身を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、さらに "any" アドレスのエントリが存在しない場合は、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ことに決めた場合は十分に注意してください。

手順

ステップ 1 デバイスをクリックし、[システム設定 (System Settings)] > [管理アクセス リスト (Management Access List)] リンクをクリックします。

すでに [システム設定 (System Settings)] ページ上の場合、目次の [管理アクセス リスト (Management Access List)] をクリックするだけです。

ルールのリストは、どのアドレスに指定されたポートへのアクセスを許可するかを定義します。ポートは、Firepower デバイスマネージャの場合は 443 (HTTPS Web インターフェイス)、SSH CLI の場合は 22 です。

ルールは順序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ルールに一致する場合、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、ルールのごみ箱アイコン (🗑️) をクリックします。

ステップ 2 管理アドレスのルールを作成するには、次の手順を実行します。

- a) [管理インターフェイス (Management Interface)] タブを選択します。
- 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) 用か、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なければならない IPv4 または IPv6 ネットワークもしく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。"any" 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 インターフェイスのルールを作成するには、次の手順を実行します。

- a) [データ インターフェイス (Data Interfaces)] タブを選択します。
- 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 (Protocol) : ルールが HTTPS (ポート 443) 用か、SSH (ポート 22) 用か、または両方に対応しているかを選択します。
- 許可されるネットワーク (Allowed Networks) : システムにアクセスできなければならぬ IPv4 または IPv6 ネットワークもしく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。"any" アドレスを指定するには、any-ipv4 (0.0.0.0/0) および any-ipv6 (::/0) を選択します。

c) [OK]をクリックします。

診断ロギングの設定

診断ロギングは、接続に関係していないイベントの syslog メッセージを提供します。接続ロギングは、個々のアクセスコントロールルール内に設定します。次の手順では、診断メッセージのロギングの設定方法について説明します。

手順

- ステップ 1** デバイス、[システム設定 (System Settings)] > [ロギング設定 (Logging Settings)] リンクをクリックします。
すでに [システム設定 (System Settings)] ページが表示されている場合は、目次の [ロギング設定 (Logging Settings)] をクリックします。
- ステップ 2** [診断ログの設定 (Diagnostic Log Settings)] > [オン (On)] をクリックします。
このページの残りのフィールドを設定しても、この設定を有効にしなければ診断ログメッセージは生成されません。
- ステップ 3** 診断ログメッセージを確認したい各場所のスライダを [オン (On)] に切り替えて、最低の重大度レベルを選択します。
メッセージは次の場所に記録できます。
- [コンソール (Console)] : メッセージは、コンソールポートの CLI にログインすると表示されます。これらのログは、**show console-output** コマンドを使用して、その他のインターフェイス (管理アドレスを含む) の SSH セッションでも確認できます。
 - [Syslog] : メッセージは、指定する外部の syslog サーバに送信されます。[+]をクリックして syslog サーバ オブジェクトを選択し、ポップアップ ダイアログボックスで [OK] をクリックします。サーバのオブジェクトがまだ存在していない場合は、[syslog サーバの追加 (Add Syslog Server)] をクリックして作成します。
- ステップ 4** [保存 (Save)] をクリックします。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。

表 5 : *syslog* メッセージの重大度

レベル番号	重大度	説明
0	emergencies	システムが使用不可能な状態。
1	alert	すぐに措置する必要があります。
2	critical	深刻な状況です。
3	error	エラー状態です。
4	warning	警告状態。
5	notification	正常ですが、注意を必要とする状況です。
6	informational	情報メッセージです。
7	debugging	デバッグ メッセージです。



(注) Firepower Threat Defenseは、重大度 0 (emergencies) の syslog メッセージを生成しません。

DHCP サーバの設定

DHCP サーバは、IP アドレスなどのネットワーク コンフィギュレーション 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上の DHCP クライアントに設定パラメータを提供するために、インターフェイス上に 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ではなく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上に存在する必要があります。つまり、サーバとクライアント間に仲介ルータを置くことはできません。スイッチは置くことができます。



- (注) すでに DHCP サーバが稼働しているネットワーク上に DHCP サーバを設定しないでください。2 台のサーバが競合し、結果が予測不能になります。

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)] > [DHCP サーバ (DHCP Server)] リンクをクリックします。
すでに [システム設定 (System Settings)] ページが表示されている場合は、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。最初は、[構成 (Configuration)] タブに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、サーバが有効になっているかどうか、およびサーバのアドレス プールが表示されます。
- ステップ 2** [構成 (Configuration)] タブで、自動設定と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の DHCP を使用してアドレスを取得している場合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は、必要なオプションを手動で定義できます。
- 自動設定を使用する場合は、[自動設定の有効化 (Enable Auto Configuration)] > [オン (On)] (スライダは右側に位置) をクリックして、DHCP を介してアドレスを取得しているインターフェイスを [取得元インターフェイス (From Interface)] で選択します。
 - 自動設定を有効にしない、または自動的に設定される設定をすべてオーバーライドする場合は、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上の 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) サーバのクライアントのアドレスを NetBIOS 名前解決で使用する必要があります。
 - [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)] : ドメインネームシステム (DNS) サーバのクライアントのアドレスをドメインの名前解決で使用する必要があります。OpenDNS パブリック DNS サーバを設定する場合は、[OpenDNS を使用 (Use OpenDNS)] をクリックします。ボタンをクリックすると、フィールドに適切な IP アドレスがロードされます。
 - [保存 (Save)] をクリックします。
- ステップ 3** [DHCP サーバ (DHCP Servers)] タブをクリックして、サーバを設定します。
- 次のいずれかを実行します。

- まだリストに含ま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、そのサーバのゴミ箱アイコン (🗑️) をクリックします。

b) 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)]: サーバを有効にするかどうかを指定します。サーバを設定し、使用可能になるまで無効にしておくことができます。
- [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。そのインターフェイスには静的 IP アドレスが設定されている必要があります。そのインターフェイスで DHCP サーバを実行する場合、DHCP を使用してインターフェイスアドレスを取得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) に DHCP サーバを設定すると、そのサーバはすべてのメンバー インターフェイスで動作します。

[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)]ページでは、管理インターフェイスに DHCP サーバを設定する代わりに、診断インターフェイスに設定することはできません。

- [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。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るため、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、サブネット ネットワークのアドレスを含めることはできません。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。例、10.100.10.12-10.100.10.250。

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、ホスト名を IP アドレスに解決するために使用されます。DNS サーバは管理インターフェイスによって使用されます。DNS サーバは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。

configure network dns servers および **configure network dns searchdomains** コマンドを使用して、CLI で DNS 設定を変更することもできます。

手順

-
- ステップ 1** デバイス、[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。
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 [DNS サーバ (DNS Server)] をクリックします。
- ステップ 2** [プライマリ、セカンダリ、ターシャリ DNS IP アドレス (Primary, Secondary, Tertiary DNS IP address)] に、設定順に最大 3 台の DNS サーバの IP アドレスを入力します。
プライマリ DNS サーバが使用されますが、接続できない場合はセカンダリが試され、最後にターシャリが試されます。

OpenDNS パブリック DNS サーバを設定する場合は、[OpenDNS を使用 (Use OpenDNS)] をクリックします。ボタンをクリックすると、フィールドに適切な IP アドレスがロードされます。
- ステップ 3** [ドメイン検索名 (Domain Search Name)] に、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。
- ステップ 4** [保存 (Save)] をクリックします。
-

管理インターフェイスの設定

管理インターフェイスは物理的な管理ポートに接続されている仮想インターフェイスです。物理ポートは診断インターフェイスと呼ばれ、他の物理ポートとともにインターフェイス ページで設定できます。

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。また、CLI で **configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用することで、管理アドレスと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 サーバはポートで動作します（DHCP サーバを持たない 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、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。
 - [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 サーバを設定しません。
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。

- a) [DHCP サーバを有効化 (Enable DHCP Server)]>[オン (On)]をクリックします。
- b) サーバの [アドレス プール (Address Pool)]を入力します。
アドレスプールとは、アドレスを要求するクライアントに対してサーバが提供できる、最小から最大までの IP アドレスの範囲です。IP アドレスの範囲は管理アドレスと同じサブネット上にある必要があり、次のものを含めることはできません：インターフェイスの自体の 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

デバイスのホスト名を変更できます。

configure network hostname コマンドを使用して、CLI の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そのホスト名を変更し、その変更を保存すると、変更はすぐに適用されるため、Firepower Device Manager へのアクセスは失われます。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、[システム設定 (System Settings)]>[ホスト名 (Hostname)]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[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)]をクリックして警告を読み、[続行 (Proceed)]をクリックします。

Network Time Protocol (NTP) の設定

システムの時刻を定義するには、Network Time Protocol (NTP) サーバを設定する必要があります。NTP サーバはシステムの初期設定時に設定しますが、次の手順を使用して変更できます。NTP 通信に関する問題が発生した場合は、[NTP のトラブルシューティング](#)、(345 ページ) を参照してください。

手順

- ステップ 1** デバイス、[システム設定 (System Settings)] > [NTP] 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 (手動) を使用するか、シスコのタイム サーバを使用するかを選択します。
- [Cisco NTP タイム サーバ (Cisco NTP Time Server)] [[デフォルトの NTP タイム サーバ (Default NTP Time Server)]: このオプションを選択した場合、NTP で使用され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)]: このオプションを選択した場合、使用する NTP サーバの完全修飾名または 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。

Cisco Collective Security Intelligence (CSI) の URL フィルタリングの設定の設定

システムでは、レピュテーション、リスク、脅威インテリジェンスのために Cisco Collective Security Intelligence (CSI) が使用されます。

(マルウェア ファイルのポリシーに使用する) FirePOWER の URL フィルタリングおよび AMP に必要なライセンスを保有している場合、それらの機能は自動的に有効になり、Cisco CSI から必要な情報を取得するための通信が可能になります。また、通信を制御するいくつかのオプションを設定できます。

手順

- ステップ 1** デバイス、[システム設定 (System Settings)] > [URL フィルタリング設定 (URL Filtering Preferences)] リンクをクリックします。すでに [システム設定 (System Settings)] ページが表示されている場合は、目次の [クラウド設定 (Cloud Preferences)] [[URL フィルタリング設定 (URL 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)]: 更新された URL データ (カテゴリおよびレピュテーション情報を含む) の自動チェックとダウンロードをシステムに許可します。データは通常 1 日 1 回更新されますが、更新は 30 分ごとにチェックされます。デフォルト

では、更新が有効になります。このオプションを選択解除し、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は、定期的に有効にして新しい URL データを取得します。

- [不明 URL に関する Cisco CSI へのクエリ (Query Cisco CSI for Unknown URLs)] : ローカルの URL フィルタリングデータベースにカテゴリおよびレピュテーションデータが含まれていない URL の更新情報について Cisco CSI に確認するかどうかを指定します。ルックアップから妥当な制限時間内にこの情報が返される場合、URL の条件に基づきアクセスルールを選択するときに使用されます。それ以外の場合、その URL は [未分類 (Uncategorized)] カテゴリに一致します。

ステップ 3 [保存 (Save)]をクリックします。

クラウド管理の設定

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 を使用し、次の技術を使用して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 を使用してローカルでデバイスを設定します。



(注) Firepower Device Manager を使用してデバイスを設定後、クラウド経由でデバイスを管理することに決めた場合は、クラウドベースの設定でローカルでの変更を繰り返していることを確認してください。

- クラウド経由のリモート構成管理 : 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して更新します。このアプローチを使用する場合、ローカルで設定に変更を加えないでください。これは、各クラウドの導入において、クラウドに定義されている設定でデバイスのローカル設定が置き換えられたためです。ローカルで変更を加える場合、その変更を維持するには、クラウドベースの設定でもその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、担当の再販業者またはパートナーに確認してください。

はじめる前に

Cisco Defense Orchestrator の登録キーを取得します。

また、デバイスにインターネットへのルートが設定されていることを確認します。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [クラウド管理 (Cloud Management)] リンクをクリックします。
すでに [システム設定 (System Settings)] ページが表示されている場合は、目次の [クラウド管理 (Cloud Management)] をクリックします。
- ステップ 2** [開始 (Get Started)] をクリックします。
- ステップ 3** [登録キー (Registration Key)] にキーを貼り付けて、[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ます。その後、ポータルを使用してデバイスの管理を開始できます。
- クラウド管理の使用をやめることにした場合は、[ギア (gear)] ドロップダウンリストから [登録解除 (Unregister)] を選択できます。
-



第 13 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/復元といったシステム管理タスクを実行する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, 331 ページ](#)
- [システムのバックアップと復元, 336 ページ](#)
- [システムの再起動, 340 ページ](#)
- [システムのトラブルシューティング, 341 ページ](#)
- [一般的でない管理タスク, 349 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およびシステムソフトウェアにアップデートをインストールできます。ここでは、それらのアップデートをインストールする方法について説明します。

システム データベースの更新

システムは、高度なサービスを提供するために複数のデータベースを使用しています。シスコでは、セキュリティポリシーが利用可能な最新情報を使用できるように、これらのデータベースに更新プログラムを提供しています。

システム データベースの更新の概要

Firepower Threat Defense は次のデータベースを使用して、アドバンスド サービスを提供します。

侵入ルール

Cisco Talos セキュリティ インテリジェンス & リサーチ グループ (Talos) は、新たな脆弱性が確認されると、インポート可能な侵入ルールの更新をリリースします。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ためには、設定を再度展開する必要があります。

侵入ルールの更新はサイズが大き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使用率が低い時間帯に行ってください。

地理位置情報データベース (GeoDB)

シスコ地理位置情報データベース (GeoDB) は、ルーティング可能な IP アドレスと関連付けられた地理的データ (国、都市、座標など) および接続関連のデータ (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 の更新によって他のシステム機能 (進行中の位置情報収集など) が中断されることはありませんが、更新が完了するまでシステム リソースが消費されます。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、特定のホストによるネットワーク侵害リスクの増大の有無を判断できるようにします。Cisco Talos セキュリティ インテリジェンス & リサーチ グループ (Talos) は、VDB の更新を定期的に発行しています。

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 を更新したら、設定を再度展開して、更新されたアプリケーションディテクタおよびオペレーティング システムのフィンガープリントを有効にする必要があります。

システム データベースの更新

システムデータベースの更新は、いつでも手動で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できます。そのため、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必要です。

また、定期スケジュールを設定してデータベース更新を取得および適用することもできます。これらの更新は大規模である可能性があるため、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ます。



(注) データベースの更新中は、操作に対するユーザ インターフェイスの応答が遅くなる場合があります。

はじめる前に

保留中の変更に影響を与える可能性を避けるため、手動でこれらのデータベースを更新する前にデバイスに設定を導入しておきます。

手順

- ステップ 1** デバイス[更新 (Updates)] サマリの [設定の表示 (View Configuration)] をクリックします。[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と、各データベースの最終更新日時が示されます。
- 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。
更新をダウンロードして適用すると、ポリシーがデバイスに自動的に再導入され、システムが更新された情報を使用できるようになります。
- ステップ 3** (オプション) データベース更新の定期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存在する場合は、[編集 (Edit)] をクリックします。
更新スケジュールはデータベースごとに異なります。更新スケジュールは個別に定義する必要があります。
 - b) 開始時刻を設定します。
 - 更新の頻度 (毎日、毎週、または毎月)。
 - 毎週または毎月の場合は、更新を実行する曜日または日付。
 - 更新を開始する時刻。
 - c) [保存 (Save)] をクリックします。
- (注) 定期スケジュールを削除する場合は、[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、次に [削除 (Remove)] ボタンをクリックします。

FirePOWER Threat Defense ソフトウェアのアップグレード

FirePOWER Threat Defense ソフトウェアのアップグレードが公開されたら、アップグレードをインストールできます。次の手順では、ご使用のシステムですでに FirePOWER Threat Defense バージョン 6.2.0 以降が実行されており、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、および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では再起動が不要の場合もありますが、メジャーアップグレードとマイナーアップグレードでは再起動が必要です。再起動が必要な場合は、インストール後にシステムが自動的に再起動します。更新のインストール中はトラフィックが中断する可能性があるため、インストールは営業時間外に行ってください。

この手順では、デバイスのイメージ再作成も、ASA ソフトウェアから FirePOWER Threat Defense ソフトウェアへの移行もできません。



- (注) 更新をインストールする前に、保留中の変更をすべて導入したことを確認します。また、バックアップを実行して、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。

はじめる前に

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。

- ファイルタイプが .sh である適切なアップグレードファイルを手にしたことを確認します。システムソフトウェアパッケージや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リリースノートを確認します。リリースノートは、<http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html> で参照できます。

手順

- ステップ 1** [デバイス (Device)] を選択し、[更新 (Updates)] サマリで [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、現在実行されているソフトウェアバージョンとすでにアップロードし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。
- まだアップグレードファイルをアップロードしていない場合は、[参照 (Browse)] をクリックしてファイルを選択します。

- アップロードされたファイルが存在し、別のファイルをアップロードする場合は、[別のファイルをアップロード (Upload Another File)] をクリックします。アップロードできるファイルは1つだけです。新しい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。システムに再度ログインできるまで待機します。デバイスサマリ、またはシステムモニタリングダッシュボードが新しいバージョンになっています。問題が発生した場合は、インストールのログを確認します。ログファイルは、`/var/log/upgrade file name` フォルダに保存されています。フォルダ名は、ビルド番号を除いたアップグレードファイルの名前です。最も役立つログファイルは、`main_upgrade_script.log` です。ログを表示するには、デバイス CLI で `system support view-logs` コマンドを使用します。インストールに失敗し、アップグレードを再インストールしても問題を修正できない場合は、シスコテクニカルサポートにお問い合わせください。

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、および脆弱性 (VDB) データベース用の自動更新ジョブを設定していない場合は、ここでそれらを更新します。

デバイスの再イメージ化

デバイスの再イメージ化には、デバイス設定の削除と新しいソフトウェアイメージのインストールが含まれます。再イメージ化とは、工場出荷時のデフォルト設定でクリーンインストールを行うことを意味します。

デバイスの再イメージ化は次のような場合に行います。

- 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。
- デバイスで実行している 6.1.0 以前のイメージを 6.1 以降のイメージにアップグレードして、Firepower Device Manager を使用してデバイスを設定する場合。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、ローカル管理に切り替えることはできません。
- デバイスが正しく機能しておらず、設定を修正するすべての試みが失敗した場合。

デバイスの再イメージ化方法の詳細については、使用しているデバイス モデルの *Cisco ASA* または *Firepower Threat Defense* デバイスの再イメージ化 [英語] または *Firepower Threat Defense* クイック

ク スタート ガイド [英語] 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

システム設定をバックアップしておくことで、将来的に設定ミスや物理的な災害が生じて設定が破損したとしても、デバイスを復元することができます。

交換用のデバイス上にバックアップを復元できるのは、2つのデバイスが同じモデルであり、同じバージョンのソフトウェアを実行している場合に限りです。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てはいけません。バックアップファイルには、アプライアンスを一意に識別するための情報が含まれているため、このような方法で共有することはできません。



(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 ファイルを回復しても、管理アドレスはバックアップ コピーの情報によって置換されません。これにより、アドレスに加えた変更はすべて維持され、別のネットワーク セグメント上の別のデバイスにも設定を復元できます。

バックアップにはシステム ソフトウェアは含まれず、設定のみが含まれます。デバイスのイメージを完全に再作成するには、ソフトウェアを再インストールする必要があります。その後、バックアップをアップロードし、設定を回復します。

バックアップ中、設定データベースはロックされます。バックアップ中は、ポリシーやダッシュボードなどを閲覧することはできますが、設定を変更することはできません。復元中、システムは一切使用できなくなります。

[バックアップおよび復元 (Backup and Restore)] ページの表には、システムで使用可能な既存のすべてのバックアップ コピーが表示され、バックアップのファイル名、バックアップ作成日時、およびファイルサイズを確認できます。バックアップのタイプ (手動、スケジュール設定、定期的) は、システムに指示したバックアップ コピー作成方法に基づきます。



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 リカバリ用に必要なバックアップ コピーが確保されるように、システム上のバックアップ コピーを手動でダウンロードして、安全なサーバ上に保管しておく必要があります。

以下の各トピックでは、バックアップの管理方法、および復元の実行方法について説明します。

即時のシステム バックアップ

バックアップはいつでも開始できます。

手順

- ステップ 1** デバイスをクリックし、[バックアップと復元 (Backup and Restore)]サマリの[設定の表示 (View Configuration)]をクリックします。
[バックアップと復元 (Backup and Restore)]ページが表示されます。この表には、システムで使用可能なすべての既存バックアップ コピーが示されます。
- 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。
すぐにバックアップするのではなく、将来の特定の時点でバックアップを実行する場合は、代わりに[スケジュール (Schedule)]をクリックします。
- ステップ 4** [今すぐバックアップ (Back Up Now)]をクリックします。
バックアッププロセスが開始されます。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。その後、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、別の場所に保存できます。
バックアップを開始した後は、[バックアップと復元 (Backup and Restore)]ページから移動できます。

スケジュールされた時刻のシステム バックアップ

スケジュールバックアップを設定して、将来の特定の日にシステムをバックアップできます。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実行するバックアップスケジュールを作成する場合は、スケジュールバックアップの代わりに定期的な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場合は、スケジュールを編集し、[削除 (Remove)]をクリックします。

手順

- ステップ 1** デバイスをクリックし、[バックアップと復元 (Backup and Restore)]サマリの[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)]>[バックアップのスケジュール (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選択します。
- ステップ 5** [スケジュール (Schedule)]をクリックします。
 選択した日時になると、バックアップが実行されます。完了すると、バックアップ コピーがバックアップの表に示されます。

定期バックアップ スケジュールの設定

定期バックアップを設定して、システムを定期的にバックアップできます。たとえば、毎週金曜日の深夜 0 時にバックアップを実行できます。定期バックアップ スケジュールを使用すると、常に一連の最近のバックアップを保持できます。



- (注) 定期スケジュールを削除するには、スケジュールを編集し、[削除 (Remove)]をクリックします。

手順

- ステップ 1** デバイス[バックアップと復元 (Backup and Restore)]サマリの [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)]と関連するスケジュールを選択します。
- [毎日 (Daily)]: 時刻を選択します。バックアップはスケジュールされた時刻に毎日実行されます。
 - [毎週 (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実行されます。たとえば、月曜日、水曜日、金曜日の 23:00 (午後 11 時) にバックアップをスケジュールできます。
 - [毎月 (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実行されます。たとえば、毎月 1 日、15 日、28 日の 23:00 (午後 11 時) にバックアップをスケジュールできます。
- ステップ 5** [保存 (Save)]をクリックします。
 選択した日付と時刻になると、バックアップが実行されます。完了すると、バックアップ コピーがバックアップのテーブルに表示されます。
- 定期スケジュールは、変更または削除しない限りバックアップを継続します。

バックアップの復元

必要に応じてバックアップを復元できます。復元するバックアップコピーがまだデバイス上にならない場合は、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。

復元中は、システムが完全に使用できなくなります。



- (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、管理アドレスはバックアップコピーから置き換えられません。これにより、アドレスに加えた変更が保持され、異なるネットワーク セグメント上の異なるデバイスで設定を復元することも可能になります。

手順

- ステップ 1** デバイスをクリックし、[バックアップと復元 (Backup and Restore)]サマリの[設定の表示 (View Configuration)]をクリックします。
[バックアップと復元 (Backup and Restore)]ページが表示されます。この表には、システムで使用可能なすべての既存バックアップ コピーが示されます。
- ステップ 2** 復元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含まれていない場合は、[アップロード (Upload)]>[参照 (Browse)]をクリックして、バックアップコピーをアップロードします。
- ステップ 3** そのファイルの復元アイコン (🔄) をクリックします。
復元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が削除されますが、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)]を選択してバックアップコピーを保持することができます。
復元が完了するとシステムが再起動します。
- (注) システムが再起動すると、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、必要に応じてそれらがダウンロードされます。システムはポリシーも再導入します。

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は、[バックアップと復元 (Backup and Restore)]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持されるわけではありません：デバイスのディスク容量の使用率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スペースを空けるために、より古いバックアップコピーが削除されます。したがって、最も必

重要な特定のバックアップコピーを確保するために、定期的にバックアップファイルを管理する必要があります。

バックアップ コピーを管理するには、次の手順を実行します。

- ファイルをセキュアなストレージにダウンロードする：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アイコン (📄) をクリックします。その後、ファイルをセキュアなファイルストレージに移動できます。
- 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、それを復元できます。



(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、システムにすでに 10 を超えるバックアップ コピーがある場合は、アップロードされたファイル用のスペースを空けるために、最も古いファイルが削除されます。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はアップロードできません。

- 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、ファイルの復元アイコン (🔄) をクリックします。復元中はシステムを使用できません。復元が完了すると、システムは再起動されます。システムが稼働した後に、設定を展開する必要があります。
- 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不要になった場合は、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。削除後に、バックアップ ファイルを回復することはできません。

システムの再起動

システムが正常に動作していないと思われる場合、問題を解決するための他の取り組みが失敗したときは、デバイスを再起動することができます。デバイスは CLI を使用して再起動する必要があります。Firepower Device Manager を使用してデバイスを再起動することはできません。

手順

- ステップ 1 SSH クライアントを使用して、管理 IP アドレスへの接続を開き、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、admin ユーザ名を使用します。
- ステップ 2 `reboot` コマンドを入力します。

例：

```
> reboot
```

システムのトラブルシューティング

次に、システムレベルのトラブルシューティングのタスクと機能の一部を示します。アクセスコントロールなどの特定の機能のトラブルシューティングについては、その機能に関する章を参照してください。

接続テストのためのアドレスの ping

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その他のポリシーにより、特定のタイプのトラフィックがデバイスを正常に通過できないことがあります。ping はデバイスの CLI にログインすることで使用できます。



(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。重要な接続をテストするために、適切なコマンドを使用していることを確認する必要があります。たとえば、システムが仮想管理インターフェイスを介してシスコライセンス サーバに接続できる必要がある場合、**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、データ インターフェイスからアドレスにアクセスできるかどうかをテストしていることになり、同じ結果が得られないことがあります。

通常の ping では、ICMP パケットを使用して接続がテストされます。使用しているネットワークで 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 ping の場合のみ）。

ネットワーク アドレスの ping に関する主なオプションは次のとおりです。

仮想管理インターフェイス経由のアドレスの ping

ping system コマンドを使用します。

ping system host

host には IP アドレス、または **www.example.com** などの完全修飾ドメイン名 (FQDN) を指定できます。データ インターフェイス経由の ping とは異なり、システム ping のデフォルトカウントはありません。ping は、Ctrl+C を使用して停止するまで続行されます。

```
> 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 テーブルを使用したデータ インターフェイス経由のアドレスの ping

ping コマンドを使用します。インターフェイスを指定しない場合、システムがホストへの一般的なルートを検出できるかどうかをテストします。これは、標準的なトラフィックのルーティング方法であるため、通常はこのテストを行います。

ping host

ホストの IP アドレスを指定します。FQDN のみわかっている場合は、**nslookup fqdn-name** コマンドを使用して IP アドレスを確認します。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、リポートカウント、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確認するには、CLI のヘルプ インジケータ (?) を使用します。

特定のデータ インターフェイス経由のアドレスの ping

特定のデータ インターフェイス経由で接続をテストする場合は、**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 のみわかっている場合は、**nslookup fqdn-name** コマンドを使用して IP アドレスを確認します。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 を使用したデータ インターフェイス経由のアドレスの 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 [interfaceif_name] hostport

ホストと TCP ポートを指定する必要があります。FQDN のみわかっている場合は、**nslookup fqdn-name** コマンドを使用して IP アドレスを確認します。

必要に応じて、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。ping を送信するインターフェイスではありません。この ping タイプでは、常にルーティングテーブルが使用されます。

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、リポート カウント、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確認するには、CLI のヘルプ インジケータ (?) 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。tracert は、無効なポート上で UDP パケットまたは ICMPv6 エコーを宛先に送信することで動作します。宛先までの間にあるルータから ICMP Time Exceeded メッセージが返され、tracert に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、ノードあたり3回参考結果が得られる可能性があります。tracertoute はデバイス CLI にログインして使用できます。



(注) データ インターフェイスを通じて (**tracertoute**)、または仮想管理インターフェイスを通じて (**tracertoute system**) 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。必ず適切なコマンドを使用してください。

次の表に、パケットごとの結果を出力で表示されるとおりに示します。

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。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間 (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 が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

仮想管理インターフェイスを通じたルートの追跡

tracertoute system コマンドを使用します。

tracertoute systemdestination

ホストは IPv4/IPv6 アドレスまたは `www.example.com` などの完全修飾ドメイン名 (FQDN) とすることができます。次に例を示します。

```
> tracertoute system www.example.com
tracertoute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.213 ms 0.310 ms 0.328 ms
 2 10.88.127.1 (10.88.127.1) 0.677 ms 0.739 ms 0.899 ms
 3 lab-gw1.example.com (10.89.128.25) 0.638 ms 0.856 ms 0.864 ms
 4 04-bb-gw1.example.com (10.152.240.65) 1.169 ms 1.355 ms 1.409 ms
 5 wan-gw1.example.com (10.152.240.33) 0.712 ms 0.722 ms 0.790 ms
 6 wag-gw1.example.com (10.152.240.73) 13.868 ms 10.760 ms 11.187 ms
 7 rbb-gw2.example.com (172.30.4.85) 7.202 ms 7.301 ms 7.101 ms
 8 rbb-gw1.example.com (172.30.4.77) 8.162 ms 8.225 ms 8.373 ms
 9 sbb-gw1.example.com (172.16.16.210) 7.396 ms 7.548 ms 7.653 ms
10 corp-gw2.example.com (172.16.16.58) 7.413 ms 7.310 ms 7.431 ms
11 dmzbb-gw2.example.com (172.16.0.78) 7.835 ms 7.705 ms 7.702 ms
12 dmzdcc-gw2.example.com (172.16.0.190) 8.126 ms 8.193 ms 11.559 ms
13 dcz05n-gw1.example.com (172.16.2.106) 11.729 ms 11.728 ms 11.939 ms
14 www1.example.com (172.16.4.161) 11.645 ms 7.958 ms 7.936 ms
```

データ インターフェイスを通じたルートの追跡

traceroute コマンドを使用します。

traceroutedestination

ホストの IP アドレスを指定します。FQDN のみわかっている場合は、**nslookupfqdn-name** コマンドを使用して IP アドレスを確認します。次に例を示します。

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 0 10.83.194.1 0 msec 10 msec 0 msec
 1 10.83.193.65 0 msec 0 msec 0 msec
 2 10.88.193.101 0 msec 10 msec 0 msec
 3 10.88.193.97 0 msec 0 msec 10 msec
 4 10.88.239.9 0 msec 10 msec 0 msec
 5 10.88.238.65 10 msec 10 msec 0 msec
 6 172.16.7.221 70 msec 70 msec 80 msec
 7 209.165.200.225 70 msec 70 msec 70 msec
```



(注) タイムアウト、パケット存続時間、ノードあたりのパケット数、さらには IP アドレスやインターフェイスを指定して、**traceroute** のソースとして使用できます。使用可能なオプションを確認するには、CLI のヘルプインジケータ (?) を使用します。

NTP のトラブルシューティング

システムが正常に機能し、イベントその他のデータポイントを正確に処理するには、正確かつ一貫した時間が不可欠です。システムが常に信頼できる時間情報を備えるには、少なくとも1つ（理想的には3つ）のネットワーク タイム プロトコル (NTP) サーバを設定する必要があります。

デバイス概要接続図（メインメニューで [デバイス (Device)] をクリック）は、NTP サーバへの接続ステータスを示します。ステータスが黄色またはオレンジの場合、設定済みサーバに接続の問題があります。接続の問題が解消されない（単なる一時的な問題ではない）場合、次を実行します。

- 最初に、[デバイス (Device)] > [システム設定 (System Settings)] > [NTP] で、NTP サーバが少なくとも3つ設定されていることを確認します。これは必須要件ではありませんが、少なくとも3つの NTP サーバがあると信頼性は格段に高まります。
- 管理インターフェイスの 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)] で定義されている) 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る場合、デフォルトルートが不適切であれば、[デバイス (Device)] > [ルーティング (Routing)] で NTP サーバへのスタティック 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した場合、デバイス CLI にログインして、`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をテストします。
- デバイス CLI にログインして、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 サーバに関する基本情報と、その可用性を示します。ただし、**Firepower Device Manager** の接続ステータスは、ステータスを示す追加情報を使用しているため、このコマンドで表示される情報と、接続ステータスの図に示される情報が一致しない場合があります。

- **system support ntp** : このコマンドには、**show ntp** の出力に加えて、NTP プロトコルと一緒に記載される標準の NTP コマンドである **ntpq** の出力が含まれます。このコマンドは、NTP の同期を確認する必要がない場合に使用します。

「Results of 'ntpq -pn.」セクションを探します。たとえば、次のような出力が表示されます。

```
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 サーバアドレスの前の「+」は、それが潜在的な候補であることを示します。次のアスタリスク (*) は、現在の時刻源のピアを示します。

NTP daemon (NTPD) は、ピアのそれぞれから 8 つのサンプルのスライディングウィンドウを使用してサンプルを 1 つ選択し、次にクロックを選択して、True chimer と False ticker を決定します。次に、NTPD はラウンドトリップの距離を決定します (候補のオフセットは、ラウンドトリップ遅延の 2 分の 1 を超えてはいけません)。接続が遅延すると、パケット損失により、またはサーバの問題によって候補の □ つまたはすべてが拒否され、同期に長時間の遅延が発生します。さらに、調整にも非常に長い時間がかかります。クロック オフセットとオシレーターのエラーはクロック規律アルゴリズムによって解決する必要があり、これには数時間かかる場合があります。



(注) refid が .LOCL. である場合、ピアが規律のないローカルクロックであること、つまり、そのローカルクロックを時間設定にのみ使用していることを意味します。Firepower Device Manager は、選択したピアが .LOCL. である場合、NTP 接続は常に黄色くマークします (未同期)。通常、NTP はより優れた候補があれば .LOCL. 候補を選びません。少なくとも 3 つのサーバを設定する必要があるのはこのためです。

CPU と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。これらのグラフには、CLI で **show cpu system** および **show memory system** コマンドを使用して収集した情報が表示されます。

CLI にログインすると、これらのコマンドのその他のバージョンを使用して、その他の情報を表示できます。このような情報が必要になるのは通常、使用率に関する問題が長引いている場合、または Cisco Technical Assistance Center (TAC) からの指示があった場合です。詳細情報の多くは複雑で、TAC による解釈が必要です。

以下に、ユーザが個人で検証可能なくつかの箇所を紹介합니다。これらのコマンドの詳細情報については、*Firepower Threat Defense* コマンドリファレンス (http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) を参照してください。

- **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 コアの使用率を個別に表示します。
- **show cpu detailed** は、コア単位、または全体的なデータプレーンの CPU 使用率に関する追加情報を表示します。
- **show memory** は、データプレーンのメモリ使用率を表示します。



(注) 一部のキーワード（上記以外）の場合は、**cpu** または **memory** コマンドを使用して、最初にプロファイリングまたは他の機能をセットアップ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にのみ使用します。

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記録します。**system support view-files** コマンドを使用すると、システム ログを開くことができます。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、Enter キーを押します。
- 表示するファイルを選択するには、プロンプトで **s** を入力します。次に、ファイル名の入力を求められます。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。ファイルリストはログのサイズを示します。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 エントリを表示するには Enter キーを押します。ログの最後に到達すると、メインメニューに移動します。「--More--」の行は、ログのサイズと表示した量を示します。**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、コマンドを終了するには、Ctrl+C キーを使用します。**
- メニューまでの構造のレベルを 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るたびに確認できるようにするには、**tail-logs** コマンドを **system support view-files** コマンドの代わりに使用します。

次の例は、システムへのログイン試行を追跡する `cisco/audit.log` ファイルの表示方法を示します。ファイルリストの上部はディレクトリで始まり、次に現在のディレクトリにあるファイルのリストが表示されます。

```
> system support view-files

===View Logs===

=====
Directory: /ngfw/var/log
-----sub-dirs-----
cisco
mojo
removed_packages
setup
seshat
connector
sf
scripts
packages
removed_scripts
httpd
-----files-----
2016-10-14 18:12:04.514783 | 5371      | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353      | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517   | action_queue.log
2016-10-06 16:00:56.620019 | 1018     | brl.down.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

=====
Directory: /ngfw/var/log/cisco
-----files-----
2017-02-13 22:44:42.394907 | 472      | audit.log
2017-02-13 23:40:30.858198 | 903615   | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0        | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338  | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338  | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218  | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848    | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160  | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,
2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,
```



```

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,
<remaining log truncated>

```

トラブルシューティング ファイルの作成

問題レポートを提出した際に、Cisco Technical Assistance Center (TAC) の担当者により、システム ログ情報の提出を求められることがあります。この情報は、問題の診断に役立ちます。診断ファイルの提出は、求められた場合だけでかまいません。

次の手順では、ログ レベルを設定して診断ファイルを作成する方法について説明します。

手順

-
- ステップ 1** デバイス。
 - 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することができます。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

デバイスの設定と管理は、デバイスで直接ホストされるローカル Firepower Device Manager を使用して行うか、Firepower Management Center マルチ デバイス マネージャを使用してリモートで行います。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 のパワーと分析機能が必要な場合は、リモート管理を使用することをお勧めします。

また、デバイスをトランスペアレントファイアウォールモードで実行する場合も、Firepower Management Centerを使用する必要があります。

ローカル管理とリモート管理の切り替えは、ソフトウェアを再インストールせずに行うことができます。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 が設定要件をすべて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、デバイスの設定が消去され、システムが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。

はじめる前に

デバイスを登録した場合（特にフィーチャライセンスを有効化した場合）は、リモート管理に切り替える前に、Firepower Device Manager を使用してデバイスの登録を解除する必要があります。デバイスの登録を解除すると、基本ライセンスおよびすべてのフィーチャライセンスが解放されます。デバイスの登録を解除しないと、こ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。[デバイスの登録解除](#)、(77 ページ) を参照してください。

手順

ステップ 1

SSH クライアントを使用して、管理 IP アドレスへの接続を開き、設定 CLI アクセス権を持つユーザ名でデバイス CLI にログインします。たとえば、admin ユーザ名を使用します。

管理 IP アドレスに接続されている間、このプロセスに従うことが重要です。Firepower Device Manager を使用するときには、データインターフェイスの IP アドレスを使用してデバイスを制御するオプションを選択できます。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は、次の事項を確認します。

- 管理物理ポートが正しく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 IP アドレスとゲートウェイが管理ネットワーク用に設定されていることを確認します。Firepower Device Manager 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)] を選択してアドレスと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 アドレス用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は、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に切り替えるには、次の手順に従います。

a) 現在ローカル管理モードであ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**} は、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 または IPv6) を表します。Firepower Management Center を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、英数字の一意的登録キーです。
- *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** を使用して 192.168.0.123 でマネージャを使用するには、次のように入力します。

```
> 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) 登録がまだ保留中であれば、**configure manager delete** を使用して登録をキャンセルし、次に **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 にログインして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 リモート管理からローカル管理に切り替えるには、次の手順に従います。

- a) 現在リモート管理モードであ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 マネージャを削除し、マネージャなしモードに移行します。

リモート管理からローカル管理に直接切り替えることはできません。 **configure manager delete** コマンドを使用してマネージャを削除します。

```
> 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 ブラウザを使用して **https://management-IP-address** でローカルマネージャを開くことができます。

ファイアウォールモードの変更

FirePOWER Threat Defenseの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、保護された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。これに対し、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」のように動作するレイヤ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 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、ファイアウォールのモードを変更して、Firepower Management Centerでのデバイス管理を開始できます。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こともできます。この場合は、ローカルマネージャを使用してデバイスを設定できます（Firepower Management Centerを使用してルーテッドモードデバイスを管理することも可能）。

ローカル管理、リモート管理にかかわらず、モードを変更するにはデバイスの CLI を使用する必要があります。

以下の手順では、ローカルマネージャの使用中にモードを変更する方法、またはローカルマネージャを使用するためにモードを変更する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、デバイス設定が消去され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスおよびホスト名は保持されます。

はじめる前に

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。

有効化された機能ライセンスが存在する場合は、FirePOWER Device Manager でこのライセンスを無効にしてから、ローカルマネージャを削除し、リモート管理に切り替えます。そうしないと、Cisco Smart Software Manager でこれらのライセンスがデバイスに割り当てられたままの状態となります。オプションライセンスの有効化と無効化、(76 ページ) を参照してください。

手順**ステップ 1**

SSH クライアントを使用して、管理 IP アドレスへの接続を開き、設定用 CLI へのアクセスが許可されたユーザ名でデバイス CLI にログインします。たとえば、admin ユーザ名を使用します。管理 IP アドレスとの接続中は、このプロセスに従うことが重要です。FirePOWER Device Manager を使用する場合は、データインターフェイスの IP アドレス経由でデバイスを管理することができます。しかし、デバイスをリモートに管理する場合は、管理用の物理ポートと管理 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は、以下を確認します。

- 管理用の物理ポートが、正しく機能す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 IP アドレスおよびゲートウェイが、管理ネットワーク用に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)。

(注) 管理 IP アドレスには、外部のゲートウェイを使用するようにしてください。リモートマネージャを使用する場合は、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できません。

ステップ 2

ルーテッドモードをトランスペアレントモードに変更して、リモート管理を使用するには、以下を行います。

- ローカル管理を無効にし、マネージャなしのモードに切り替えます。
アクティブなマネージャが存在する状態では、ファイアウォールモードを変更できません。
`configure manager delete` コマンドを使用して、マネージャを削除します。

```
> 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 firewalltransparent

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**} は、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 または IPv6) を表します。Firepower Management Center を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 に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、192.168.0.123 にあるマネージャ、および登録キー **secret** を使用するには、次のように入力します。

```
> 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 トランスペアレントモードからルーテッドモードに変更し、ローカル管理に切り替えるには、以下を行います。

- a) デバイスを Management Centerから登録解除します。
- b) 可能であればコンソールポートから、Firepower Threat Defenseデバイスの CLI にアクセスします。
モードの変更によって設定が消去されるため、管理 IP アドレスはデフォルトに戻ります。したがって、モードの変更後に、管理 IP アドレスとの SSH 接続が失われる可能性があります。
- 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 firewallrouted

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 ブラウザを使用して、**https://management-IP-address** のローカル マネージャを起動できるようになります。

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。

はじめる前に

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 でそれらが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](#)、(76 ページ) を参照してください。

手順

ステップ 1 SSH クライアントを使用して、管理 IP アドレスへの接続を開き、設定 CLI アクセス権を持つユーザ名でデバイスの CLI にログインします。たとえば、**admin** ユーザ名を使用します。

ステップ 2 **configure manager delete** コマンドを使用してマネージャを削除します。

```
> 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 ブラウザを使用して **https://management-IP-address** でローカル 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。