Cisco Firepower Threat Defense バージョン 6.1 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。

目 次

第 1 章

使用する前に

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

このガイドの対象読者

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

Firepower Device Manager を使用すると、小規模ネットワークで最もよく使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defenseデバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

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

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

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

デバイス モデル	Firepower Threat Defense の最小ソフトウェア バージョン
ASA 5506-X、5506H-X、5506W-X、5508-X、5516-X	6.1
ASA 5512-X、5515-X、5525-X、5545-X、5555-X	6.1

システムへのログイン

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

Firepower Device Manager Web インターフェイス

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

コマンドライン インターフェイス（CLI、コンソール）

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

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

Firepower Device Manager へのログイン

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

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

はじめる前に

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

手順

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

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

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

セッションは非アクティブの状態が20分間続くと期限切れになり、再度ログインするように求められます。ページの右上にあるユーザ アイコン ドロップダウン リストから [ログアウト（Log Out）]を選択するとログアウトできます。

CLI（コマンドライン インターフェイス）へのログイン

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

CLI にログインするには、次のいずれかを実行します。

- デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。
- SSH クライアントを使用して、管理 IP アドレスに接続します。**admin** ユーザ名（デフォルトのパスワードは Admin123 です）または別の CLI のユーザ アカウントを使用してログインします。

ログインした後、CLI で使用可能なコマンドを確認するには、**help** または **?** を入力してください。使い方については、http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html で *Firepower Threat Defense* のコマンド リファレンス [英語] を参照してください。

（注） **configure user add** コマンドを使用して、CLI にログインできるユーザ アカウントを作成できます。ただし、これらのユーザは CLI のみにログインできます。Firepower Device Manager の Web インターフェイスにはログインできません。

パスワードの変更

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

（注） CLI にログインしている場合は、**configure password** コマンドを使用してパスワードを変更できます。**configure user password** *username* コマンドを使用すると、別の CLI ユーザの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 [プロファイル（Profile）]を選択します。

ステップ 2 [パスワード（Password）]タブをクリックします。

ステップ 3 現在のパスワードを入力します。

ステップ 4 新しいパスワードを入力して確認します。

ステップ 5 [変更（Change）]をクリックします。

ユーザ プロファイルの設定

ユーザ インターフェイスの設定を行い、パスワードを変更することができます。

手順

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

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

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

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

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 add*username* {**basic** | **config**}

次の権限レベルを持つユーザを定義できます。

- **config**：ユーザに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、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どち

らの値も 1 ~ 9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

  次回ログイン時にユーザにパスワードを強制的に変更してもらいます。

- **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 minpasswdlen** *username number*

  パスワードの最小長を 1 ~ 127 までで設定します。

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

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

ステップ 4 必要に応じてユーザ アカウントを管理します。
ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したり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機能するためには、初期設定を完了する必要があります。展開を成功させるには、ケーブルを正しく接続し、デバイスをネットワークに挿入し、インターネットや他のアップストリーム ルータに接続するために必要なアドレスを設定する必要があります。次の手順で、このプロセスについて説明します。

はじめる前に

初期設定を開始する前に、デバイスにはいくつかのデフォルト設定が含まれています。詳細は、初期設定前のデフォルト設定, （15 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, （7 ページ）

ステップ 2 初期設定の完了, （9 ページ）
設定の結果の詳細については、初期展開後の設定, （16 ページ）を参照してください。

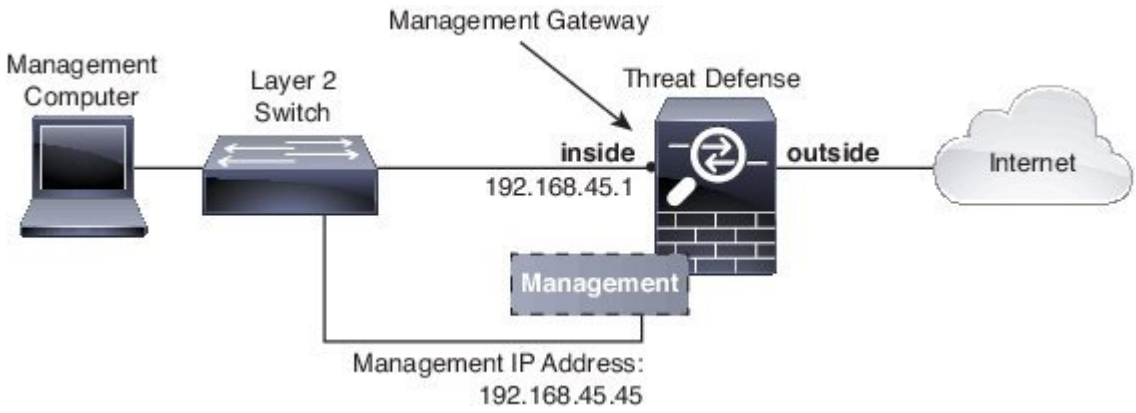
ステップ 3 ワイヤレス アクセス ポイント（ASA 5506W-X）の設定, （11 ページ）

インターフェイスの接続

デフォルト設定は、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの想定に基づいてインターフェイスにネットワーク ケーブルを接続していると、初期設定がしやすくなります。

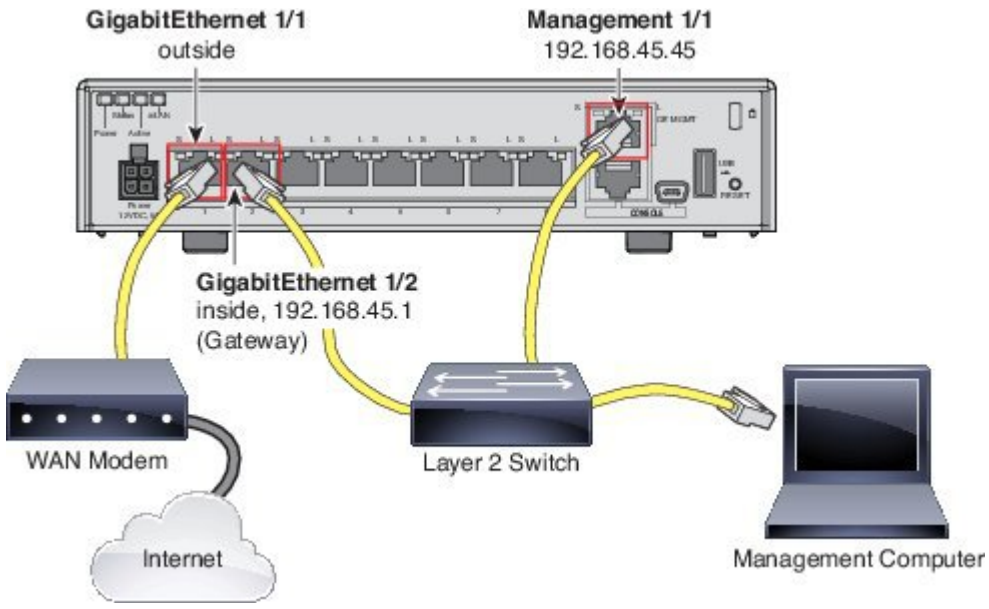
デフォルト設定は、スイッチを使用して同じネットワークに管理インターフェイスおよび内部インターフェイスに接続すると仮定しています。内部インターフェイスが DHCP サーバとして設定されているため、同じスイッチに管理ワークステーションを接続し、同じネットワーク上の DHCP を介してアドレスを取得して、Firepower Device Manager の Web インターフェイスを開くことができます。

次の図は、想定されるネットワーク トポロジを示しています。



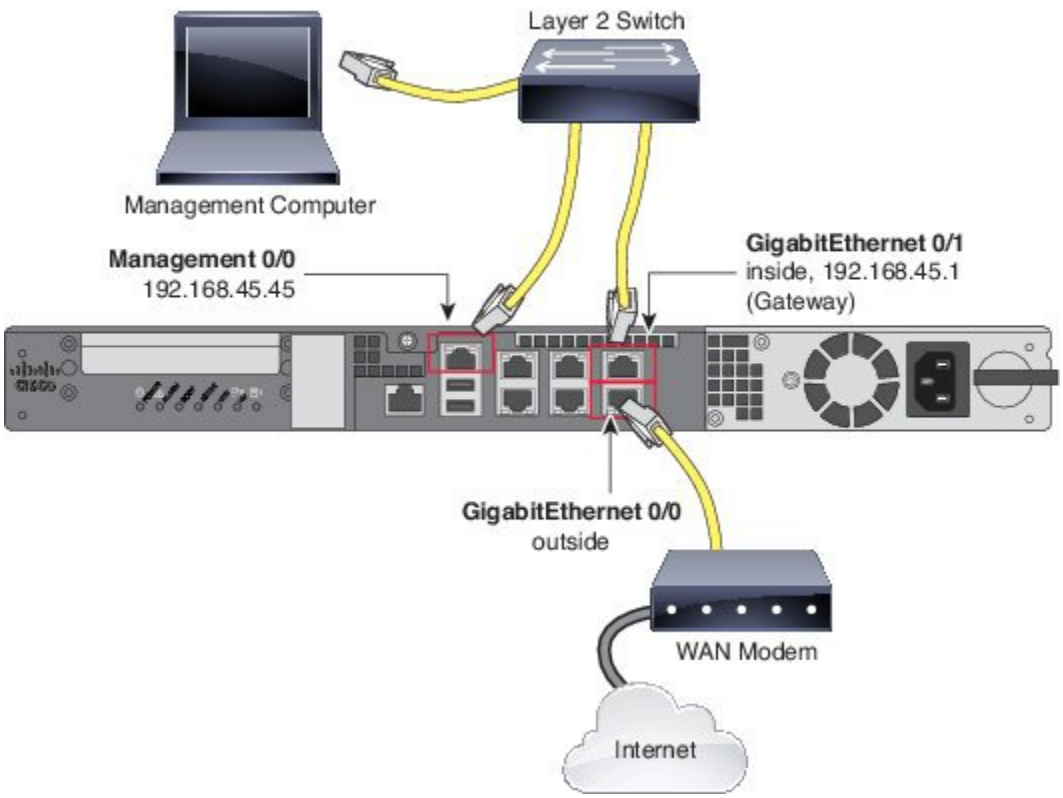
次の図は、このトポロジでのシステムの配線方法を示します。内部ルータを使用して異なるネットワークに管理ネットワークと内部ネットワークを接続するには、ルーテッド モードの導入, （105 ページ）を参照してください。

ASA 5506-X、5508-X、5516-X の配線



- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 1/2 をレイヤ 2 スイッチに接続します。IP アドレスは 192.168.45.1 であり、これが内部ネットワークのゲートウェイとして機能します。
- Management 1/1 をレイヤ 2 スイッチに接続します。IP アドレスは 192.168.45.45 です。
- ワークステーションがレイヤ 2 スイッチに接続し、DHCP を使用してアドレスを取得するように設定します。

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



- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 0/0 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 0/1 をレイヤ 2 スイッチに接続します。IP アドレスは 192.168.45.1 であり、これが内部ネットワークのゲートウェイとして機能します。
- Management 0/0 をレイヤ 2 スイッチに接続します。IP アドレスは 192.168.45.45 です。
- ワークステーションがレイヤ 2 スイッチに接続し、DHCP を使用してアドレスを取得するように設定します。

初期設定の完了

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

はじめる前に

データインターフェイスをゲートウェイのデバイス（ケーブルモデムやルータなど）に接続していることを確認します。エッジの導入では、これはインターネット向けのゲートウェイになります。データセンターの導入では、バックボーン ルータになります。使用モデルのデフォルトの

「外部」インターフェイスを使用します（インターフェイスの接続，（7 ページ）および初期設定前のデフォルト設定，（15 ページ）を参照）。

管理インターフェイスは、インターネットにアクセスできるゲートウェイにも接続する必要があります。システムのライセンススシングおよびデータベースの更新には、インターネット アクセスが必要です。

手順

ステップ 1 これがシステムへの初めてのログインであり、CLI セットアップ ウィザードを使用していない場合、エンドユーザ ライセンス契約を読んで承認し、管理パスワードを変更するように求められます。
続行するには、以下の手順を完了する必要があります。

ステップ 2 外部インターフェイスを選択し、[次へ（Next）]をクリックします。
これは、ゲートウェイのモデムまたはルータに接続されているデータ ポートです。

（注） デフォルト設定で内部インターフェイスとして設定されているインターフェイスは選択できません。デフォルトの内部インターフェイスを外部インターフェイスとして使用する場合は、デバイス設定をスキップして、手動で設定を行うことができます。また、別のインターフェイスを一時的な外部インターフェイスとして選択して設定を完了し、その後設定を手動で編集して、実際の外部インターフェイスを反映させることができます。

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

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

[外部インターフェイス（Outside Interface）]

- [IPv4 の設定（Configure IPv4）]：外部インターフェイスの IPv4 アドレス。DHCP を使用するか、または手動で静的 IP アドレス、サブネット マスク、およびゲートウェイを入力できます。また、[オフ（Off）]を選択して、IPv4 アドレスを設定しないこともできます。デフォルトの内部アドレスと同じサブネットに（静的に、または DHCP を介して）IP アドレスを設定しないでください（初期設定前のデフォルト設定，（15 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 を使用するか、または手動で静的 IP アドレス、プレフィックス、およびゲートウェイを入力できます。また、[オフ（Off）]を選択して、IPv6 アドレスを設定しないこともできます。

管理インターフェイス

- [DNS サーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。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。
- [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 システム時刻の設定を行い、[次へ（Next）]をクリックします。

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

ステップ 5 システムのスマート ライセンスを設定します。
スマート ライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマート ライセンスを設定することができます。

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

評価ライセンスを使用するには、[登録せずに 90 日の評価期間を開始する（Start 90 day evaluation period without registration）]を選択します。後でデバイスを登録して、スマート ライセンスを取得するには、[デバイス（Device）]メニューのデバイス名、[スマート ライセンス（Smart Licenses）]グループ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

- オプション ライセンスでカバーされている機能（カテゴリベースの URL フィルタリング、侵入インスペクション、マルウェア対策など）を使用する場合は、必要なライセンスを有効にします。オプション ライセンスの有効化と無効化，（64 ページ）を参照してください。
- 他のインターフェイスをネットワークに接続している場合は、各接続インターフェイスを設定します。サブネットを追加する方法，（50 ページ）およびインターフェイスの設定，（109 ページ）を参照してください。
- 製品の使用方法については、使用例で学習してください。Firepower Threat Defenseの使用例，（25 ページ）を参照してください。

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。このワイヤレスアクセスポイントは、デフォルトで無効化されています。ワイヤレス無線を有効化し、SSID およびセキュリティの設定を行うには、アクセス ポイント Web インターフェイスに接続してください。

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

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

詳細については、次のマニュアルを参照してください。

- ワイヤレス LAN コントローラの使用の詳細については、『Cisco Wireless LAN Controller 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デバイスは推奨設定になっていて、他のネットワーク問題が見つからない場合、アクセス ポイントをデフォルト設定に復元することができます。Firepower Threat DefenseCLI にアクセス（コンソール ポートに接続、または SSH アクセスを設定）する必要があります。Firepower Threat DefenseCLI から、次のコマンドを入力します。

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

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

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

手順

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

a) インターフェイスのリストを開くには、[デバイス（Device）]メニューのデバイス名をクリックし、[インターフェイス（Interfaces）] グループのリンクをクリックします。

b) GigabitEthernet 1/9 インターフェイスの [編集（edit）] アイコン（  ）をクリックします。

c) 次のオプションを設定します。

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

d) [保存（Save）]をクリックします。

ステップ 2 内部インターフェイスと同じセキュリティ ゾーンに Wi-Fi インターフェイスを追加します。
デバイスのセットアップ ウィザードでは、[inside_zone]というセキュリティ ゾーンの[内部（inside）] インターフェイスを設定します。Wi-Fi インターフェイスは、アクセスポイントの Web インターフェイスに到達できるよう、同じゾーンに存在する必要があります。

a) メニューの[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（edit）] アイコン（  ）をクリックします。
c) [インターフェイス（Interfaces）]の下の [+] をクリックし、[wifi] インターフェイスを選択します。

ステップ 3 [inside_zone] セキュリティ ゾーン内のインターフェイス間のトラフィックを許可するため、アクセス コントロール ルールを設定します。
デバイスのセットアップ ウィザードでは、トラフィックが [inside_zone]から [outside_zone] に流れるようにするためのルールを作成します。これにより、内部ユーザがインターネットにアクセスできます。[Wifi]インターフェイスを [inside_zone] に追加することにより、Wi-Fi ユーザもインターネット アクセスを許可するルールに含まれます。

ただし、デフォルトのアクションはすべてのトラフィックをブロックするため、[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必要があります。

a) メニューで [ポリシー（Policies）]をクリックします。
b) ルールを追加するには、[アクセス コントロール（Access Control）]テーブルの上の [+] をクリックします。
c) ルールで少なくとも次のオプションを設定します。

- [タイトル（Title）] : ルールの名前を入力します。たとえば、「Inside_Inside」と入力します。
- [アクション（Action）] : Allow または Trust。
- [送信元/宛先（Source/Destination）] > [送信元ゾーン（Source Zones）] : inside_zone を選択します。
- [送信元/宛先（Source/Destination）] > [宛先ゾーン（Destination Zones）] : inside_zone を選択します。

d) [OK]をクリックします。

ステップ 4 ワイヤレス インターフェイスで、DHCP サーバを設定します。
DHCP サーバは、アクセス ポイントに接続するデバイスに IP アドレスを提供します。また、アクセス ポイント自体にアドレスを提供します。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
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 テーブルの上の [+]をクリックします。
d) 次の DHCP 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）]：DHCP サーバを有効にするには、スライダをクリックします。
- [インターフェイス（Interface）]：[wifi] インターフェイスを選択します。
- [アドレス プール（Address Pool）]：DHCP クライアントのアドレス プールを入力します。たとえば、ワイヤレス インターフェイスにアドレスの例を使用した場合、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なければならず、またインターフェイス アドレスまたはブロードキャスト アドレスを含むことはできません。

e) [追加（Add）] [OK] をクリックします。

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

展開が完了するまで待ってから続行します。

ステップ 6 ワイヤレス アクセス ポイントを設定します。
ワイヤレス アクセス ポイントは、ワイヤレス インターフェイス用に定義された DHCP プールからアドレスを取得します。プール内の最初のアドレスを取得する必要があります。アドレスの例を使用した場合、これは「192.168.10.2」です。（最初のアドレスが機能しない場合は、プール内の次のアドレスを試します）。

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

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

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

- [SSID]：サービス セット識別子。これはワイヤレス ネットワークの名前です。Wi-Fi 接続用のワイヤレス 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。
- [ユニバーサル管理モード（Universal Admin Mode）]：無効。
- [セキュリティ（Security）]：どのセキュリティ オプションを使用するかを選択します。

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

a) 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。
b) [設定（Settings）] タブをクリックします。
c) [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。
d) 5 GHz 無線についても、この手順を繰り返します。

初期設定前のデフォルト設定

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

この設定では、管理インターフェイス、内部インターフェイスおよびコンピュータを同じスイッチに有線接続し、内部インターフェイスで定義されている DHCP サーバを使用して IP アドレスをコンピュータに提供しているものと仮定します。次の表で、デバイス モデル別のデフォルトの内部および外部インターフェイスを参照してください。

デフォルト設定

設定	デフォルト	初期設定時に変更できるか
管理者ユーザのパスワード	Admin123	可。デフォルト パスワードを変更する必要があります。
管理 IP アドレス	192.168.45.45	不可。
管理ゲートウェイ	192.168.45.1	不可。
内部インターフェイスの IP アドレス	192.168.45.1	不可。
内部クライアントの DHCP サーバ	アドレス プール 192.168.45.46 ～ 192.168.45.254 の内部インターフェイスで実行されます。	不可。
内部クライアントの DHCP 自動設定（自動設定では、WINS サーバおよび DNS サーバのアドレスをクライアントに提供します）	外部インターフェイスで有効です。	可（ただし間接的）。外部インターフェイスにスタティック IPv4 アドレスを設定した場合、DHCP サーバの自動設定が無効になります。

設定	デフォルト	初期設定時に変更できるか
外部インターフェイスの IP アドレス。	インターネット サービス プロバイダー（ISP）または上流に位置するルータから DHCP 経由で取得されます。	可。

デバイス モデル別のデフォルト インターフェイス

初期設定時に異なる外部インターフェイスを選択できます。ただし、異なる内部インターフェイスを選択することはできません。設定後に内部インターフェイスを変更するには、インターフェイス設定と DHCP 設定を編集します。

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	GigabitEthernet 1/2
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

初期展開後の設定

セットアップ ウィザードを完了すると、デバイス設定には次の設定が含まれます。表は、特定の設定が明示的に選択したものであるか、または他の選択に基づいて自動的に定義されたものかどうかを示します。「暗黙的」な設定を検証し、ニーズに合わない場合は編集します。

設定	構成	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	入力した任意の内容	明示的
管理 IP アドレス	192.168.45.45	デフォルト

設定	構成	明示的/暗黙的な設定、またはデフォルト設定
管理ゲートウェイ	192.168.45.1	デフォルト
管理インターフェイスの DNS サーバ	入力した任意の内容	明示的
管理ホスト名	firepower または入力した任意の内容	明示的
システム時刻	選択したタイム ゾーンと NTP サーバ	明示的
スマート ライセンス	基本ライセンスで登録したもの、または評価期間が有効なもの（選択した方）。 サブスクリプション ライセンスは有効ではありません。これらを有効化するには、スマート ライセンスのページに移動します。	明示的
内部インターフェイスの IP アドレス	192.168.45.1	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 192.168.45.46 ～ 192.168.45.254 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 サーバおよびDNS サーバ用のアドレスがクライアントに提供されます）	外部インターフェイスの IPv4 アドレスを取得するために DHCP を使用している場合、DHCP 自動設定は外部インターフェイスで有効になります。 スタティック アドレッシングを使用する場合、DHCP 自動設定は無効になります。	明示的だが間接
外部物理インターフェイスと IP アドレス	選択した物理ポート IP アドレスは DHCP によって取得するか、入力したスタティック アドレスです（IPv4、IPv6、またはその両方）。	明示的。

設定	構成	明示的/暗黙的な設定、またはデフォルト設定
スタティック ルート	外部インターフェイスにスタティック IPv4 または IPv6 アドレスを設定すると、スタティック デフォルト ルートが必要に応じて IPv4/IPv6 用に設定され、そのアドレス タイプに定義したゲートウェイを指定します。DHCP を選択すると、デフォルト ルートが DHCP サーバから取得されます。 ネットワーク オブジェクトもそのゲートウェイおよび任意のアドレス向けに作成されます（つまり IPv4 では 0.0.0.0/0、IPv6 では ::/0）。	暗黙的
セキュリティ ゾーン	内部インターフェイスを含む inside_zone 外部インターフェイスを含む outside_zone （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したり、独自のゾーンを作成したりできます）	暗黙的
アクセス コントロール ポリシー	inside_zone から outside_zone へのすべてのトラフィックを信頼するルール。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。 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。これにより、外部から発信されたトラフィックがネットワークに入らないようにしています。	暗黙的
NAT	インターフェイス ダイナミック PAT ルールは、外部インターフェイスに宛てられたすべての トラフィックの発信元アドレスを、外部インターフェイスの IP アドレスの一意のポートに変換します。 （注） このルールは、外部 IPv6 アドレスへの接続を防止します。IPv6 の使用時に PAT ルールをバイパスするには、そのルールを編集して、内部 IPv4 ネットワークを送信元アドレスとしてネットワーク オブジェクトを選択します。	暗黙的

設定の基本

ここでは、デバイスの設定に関する基本的な手順について説明します。

デバイスの設定

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

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

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名、[デバイス ダッシュボード（Device Dashboard）] に移動します。
たとえば、以下のリンクが 5516-x-1 という名前のデバイスに表示されます。

ダッシュボードには、有効なインターフェイスやキー設定が設定されているか（緑色）またはまだ設定が必要であるかなど、デバイスの視覚的なステータスが表示されます。詳細については、インターフェイスと管理ステータスの表示，（22 ページ）を参照してください。

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

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

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

- [インターフェイス（Interface）]：管理インターフェイスに加えて、少なくとも 2 つのデータインターフェイスを設定する必要があります。インターフェイス，（103 ページ）を参照してください。
- [ルーティング（Routing）]：ルーティングの設定。デフォルト ルートを定義する必要があります。他のルートは設定に応じて必要になります。ルーティング，（119 ページ）を参照してください。

- [更新（Updates）]：地理位置情報、侵入ルールと脆弱性のデータベースの更新、および。これらの機能を使用する場合、最新のデータベースの更新情報を確実にするため、定期的な更新スケジュールを設定します。定期的なスケジュールの更新が発生する前に更新をダウンロードする必要がある場合にも、このページにアクセスできます。システムデータベースの更新，（281 ページ）を参照してください。
- [システム設定（System Settings）]：このグループにはさまざまな設定が含まれます。デバイスの初期設定時に構成し、その後めったに変更しない基本設定などがあります。システム設定，（271 ページ）を参照してください。
- [スマート ライセンス（Smart License）]：システム ライセンスの現在のステータスを示します。システムを使用するには、適切なライセンスをインストールする必要があります。一部の機能では追加のライセンスが必要です。システムのライセンス，（59 ページ）を参照してください。
- [バックアップと復元（Backup and Restore）]：システム設定をバックアップするか、以前のバックアップを復元します。システムのバックアップと復元，（286ページ）を参照してください。
- [トラブルシューティング（Troubleshoot）]：Cisco Technical Assistance Center の依頼により、トラブルシューティング ファイルを生成します。トラブルシューティング ファイルの作成，（300 ページ）を参照してください。

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

変更は、それらを展開するまでデバイスで有効になりません。変更の展開，（20 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、システムのセキュリティ ポリシーを設定します。また、これらのポリシーで必要なオブジェクトを設定するには、[オブジェクト（Objects）]をクリックします。

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るため、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 エンジンを再起動する設定の変更，（21 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）]アイコンリンクをクリックします。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 エンジンを再起動する設定の変更

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

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

展開

展開はすべて、インスペクション エンジンが再起動されます。

システムの更新プログラム

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

インターフェイスと管理ステータスの表示

[デバイス ダッシュボード（Device Dashboard）] には、デバイスのグラフィカル ビューと管理アドレス用の設定が含まれています。[デバイス ダッシュボード（Device Dashboard）] を開くには、メニューでデバイスの名前をクリックします。

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

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

インターフェイス ステータス

ポートをマウス オーバーすると、その IP アドレスと有効なリンク ステータスが表示されます。IP アドレスはスタティックに割り当てることもできれば、DHCP を使用して取得することもできます。

インターフェイス ポートは、次のカラー コーディングを使用します。

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

内部、外部ネットワーク接続

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

- 内部ネットワーク：“inside” という名前のインターフェイスの場合のみ、内部ネットワークのポートが表示されます。その他に内部ネットワークが存在する場合、それらは表示されません。いずれのインターフェイスにも “inside” と命名していない場合は、ポートは内部ポートとしてマークされません。

- 外部ネットワーク：“outside” という名前のインターフェイスの場合のみ、外部ネットワークのポートが表示されます。内部ネットワークと同様に、この名前は必須であり、存在しない場合は、ポートは外部ポートとしてマークされません。

管理設定のステータス

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

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

問題が見つかった場合は、次のように修正します。

- 管理ポートおよびゲートウェイ：[システム設定（System Settings）]>[デバイス管理IP（Device Management IP）] 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，（296 ページ）も参照してください。
- スマート ライセンス：[スマート ライセンス（Smart License）] グループ内の [設定の表示（View Configuration）]リンクをクリックします。

システム タスク ステータスの表示

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

手順

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

タスク リストが開き、システム タスクのステータスと詳細が表示されます。

ステップ 2 タスクのステータスを評価します。
永続的な問題がある場合は、デバイス設定を修正する必要があります。たとえば、データベースの更新を永続的に取得できない場合、デバイスの管理IPアドレスにインターネットへのパスがないと示される場合があります。タスクの説明に挙げられている問題については、Cisco Technical Assistance Center（TAC）に問い合わせる必要があります。

タスク リストでは、次の操作を実行できます。

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

第 2 章

Firepower Threat Defenseの使用例

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

ネットワーク トラフィックを調べる方法

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

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

- ネットワークの用途
- 最も多くネットワークを使用しているユーザ
- ユーザの接続先
- ユーザが使用しているデバイス

- ヒット数が最も多いアクセス コントロール ルール（ポリシー）

初期のアクセスルールでは、ポリシー、宛先、セキュリティゾーンなどのトラフィックについての情報が明らかになります。しかし、ユーザ情報を取得するには、ユーザを認証（識別）する必要があるアイデンティティ ポリシー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、追加でいくつかの調整を行う必要があります。

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

（注） この手順では、ユーザがアクセスしたサイトの Web サイト カテゴリおよびレピュテーションに関する情報は提供されないため、Web カテゴリ ダッシュボードに有意義な情報は表示されません。カテゴリおよびレピュテーションのデータを取得するには、カテゴリベースの URL フィルタリングを実装し、URL ライセンスを有効化する必要があります。この情報のみを取得する場合は、許容するカテゴリ（金融サービスなど）へのアクセスを許可する新規のアクセス コントロール ルールを追加して、アクセス コントロール ポリシーで最初のルールに設定することができます。URL フィルタリングの実装の詳細については、アクセプタブル ユース ポリシー（URL フィルタリング）の実装方法, （41 ページ）を参照してください。

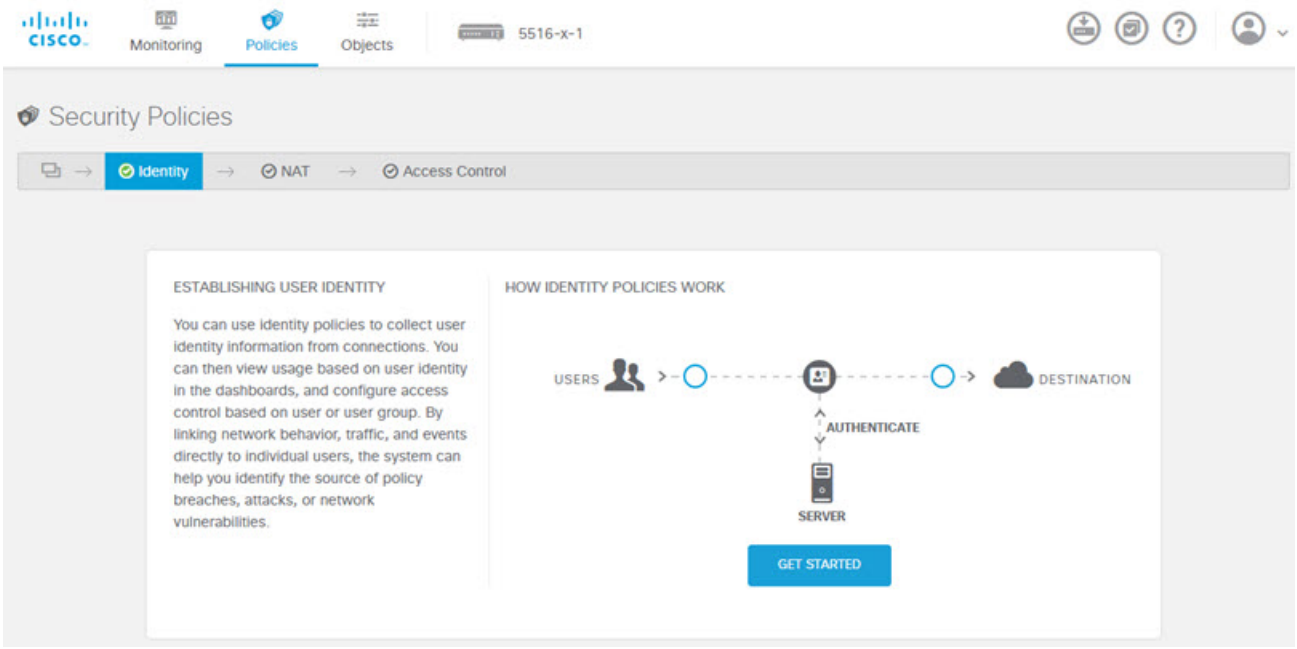
手順

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

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

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

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



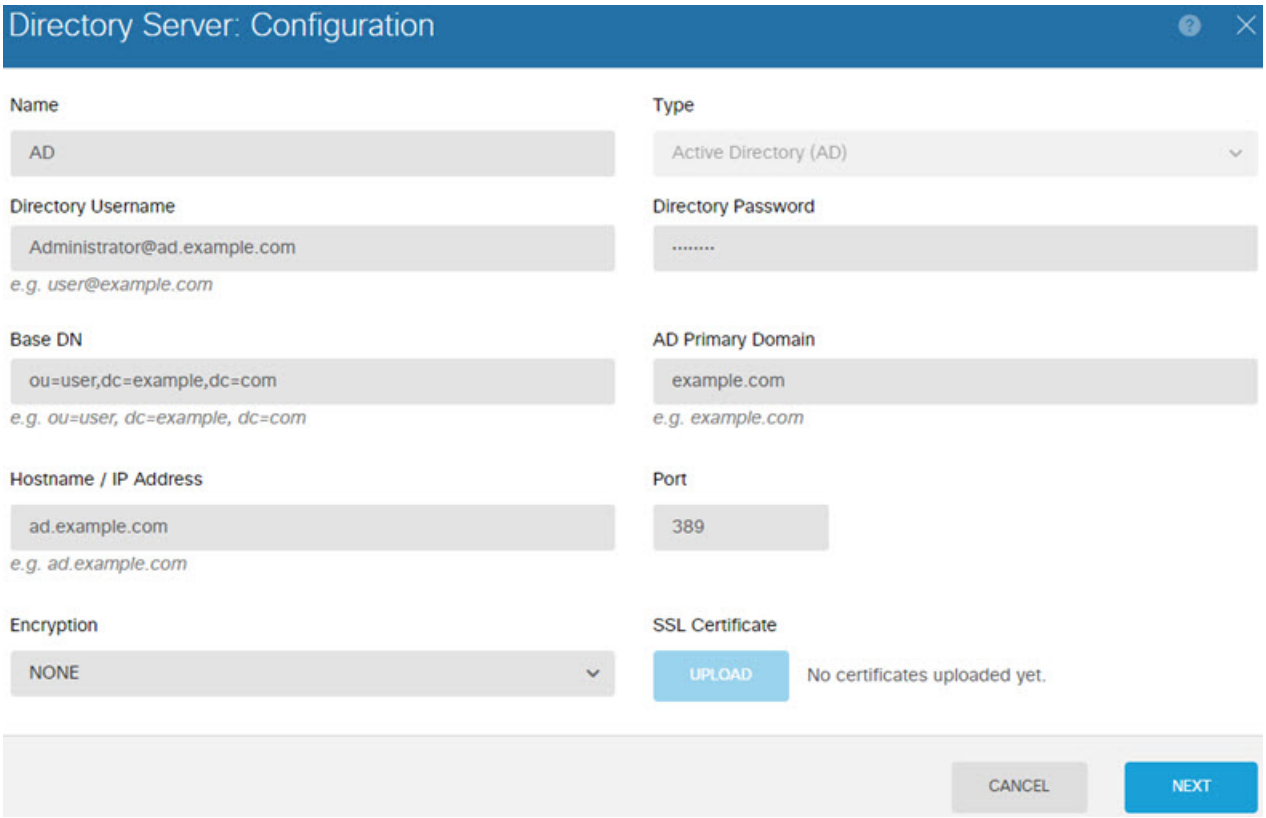
b) [スタート（Get Started）] ボタンをクリックし、ウィザードを起動して必要な要素を設定します。

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 がサポートされている唯一のタイプであり、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適切な権限を持っているユーザの識別用のユーザ名とパスワード。たとえば、admin@ad.example.com などです。
- [ベース DN（Base DN）]：ユーザおよびグループの共通の親である、ユーザおよびグループ情報を検索、または問い合わせるためのディレクトリ ツリー。たとえば、dc=example,dc=com などです。ベース DN の検索についての詳細は、ディレクトリ ベース DN の決定，（129 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のある、完全修飾 Active Directory ドメイン名。たとえば、example.com などです。
- [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。サーバへ暗号化接続を使用している場合、IP アドレスではなく完全修飾ドメイン名を入力する必要があります。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合はポート 636 を使用します。

- [暗号化（Encryption）]：ユーザおよびグループ情報をダウンロードするために暗号化接続を使用するには、希望する方法、STARTTLS または LDAPSを選択します。デフォルトは [なし（None）]であり、ユーザおよびグループ情報はクリア テキストに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、ディレクトリ サーバでサポートされている最も強力な方式を使用します。ポート 389 を使用します。
  - LDAPSでは LDAP over SSL が必要です。ポート 636 を使用します。
- [SSL 証明書（SSL Certificate）]：暗号化方式を選択したら、CA 証明書をアップロードしてシステムとディレクトリ サーバ間の信頼されている接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用し、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、次のイメージには、ad.example.com サーバの暗号化されていない接続の作成方法が示されています。プライマリ ドメインは example.com で、ディレクトリ ユーザ名は Administrator@ad.example.com です。すべてのユーザおよびグループの情報は、識別名（DN）ou=user,dc=example,dc=com の下にあります。



d) [Next]をクリックします。

e) アクティブ認証のキャプティブ ポータルを設定します。
最もシンプルな方法は、すべてのフィールドをそのままにして[保存（Save）]をクリックします。アクティブ認証のデフォルトポートを設定します。ユーザは、ユーザ名とパスワードを提供するための信頼に必要な自己署名証明書を取得します。証明書を受け入れるようユーザに伝えます。

ただし、理想としては、ブラウザが信頼している証明書をアップロードします。証明書を持っている場合は、次のフィールドに入力して使用します。

- [サーバ証明書（Server Certificate）]：アクティブ認証の間にユーザに表示する 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。証明書に貼り付けるか、[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、ユーザ認証時の自己署名証明書が表示されます。
- [証明書キー（Certificate Key）]：サーバ証明書のキー。キーに貼り付けるか、[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 ポータルのポート。デフォルトは 885（TCP）です。異なるポートを設定する場合、1025 ～ 65535 の範囲内とする必要があります。

f) [保存（Save）]をクリックします。
これで、セットアップ ウィザードが終了します。次に、アクティブ認証に必要なアイデンティティ 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、または [+] ボタンをクリックします。

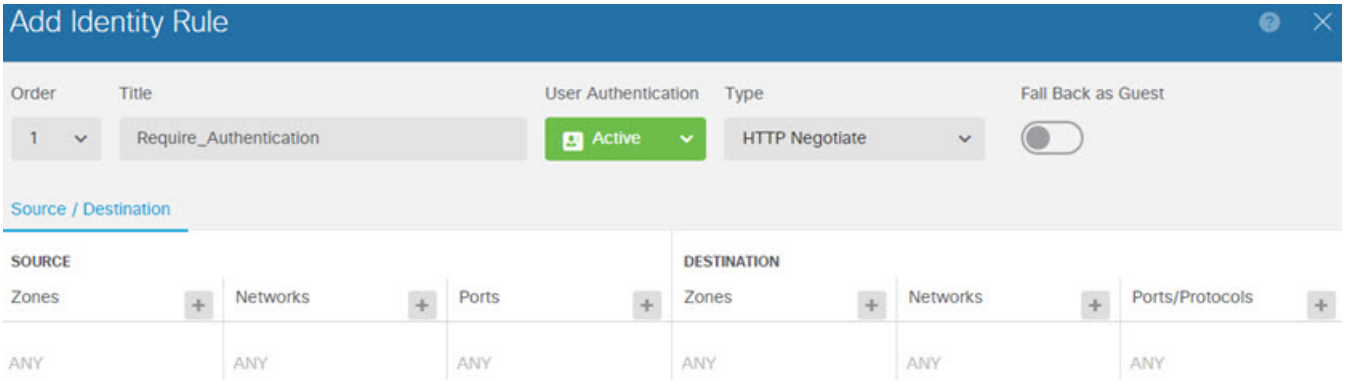
h) アイデンティティ ルールのプロパティを入力します。
全員を認証する必要があることを前提として、次の設定を使用できます。

- [名前（Name）]：任意の選択（Require_Authenticationなど）。
- [ユーザ認証（UserAuthentication）]：[アクティブ（Active）] が選択されているため、そのままにします。
- [タイプ（Type）]：[HTTPネゴシエート（HTTP Negotiate）]を選択します。これにより、ブラウザおよびディレクトリ サーバは最も強力な認証プロトコルを、NTLM、HTTP ベーシックの順にネゴシエートできます。

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

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

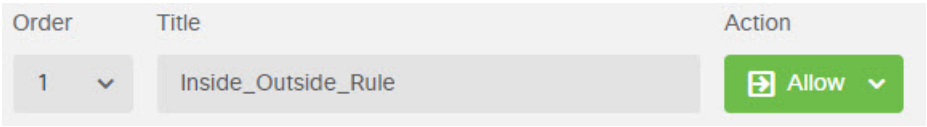
より制限されているトラフィックに合わせて、ポリシーに制約を加えることができます。ただし、アクティブ認証はHTTPトラフィックに対してのみ試行されるため、非HTTPトラフィックが送信元/宛先条件に一致していることは重要ではありません。アイデンティティ ポリシーのプロパティの詳細については、アイデンティティ ルールの設定, （135 ページ）を参照してください。



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

ステップ 2 Inside_Outside_Rule アクセス コントロール ルールのアクションを[許可（Allow）]に変更します。Inside_Outside_Rule アクセス ルールは、信頼できるルールとして作成されます。ただし、信頼できるトラフィックのインスペクションは実行されないため、トラフィック一致基準にアプリケーションやその他の条件（ゾーン、IP アドレス、およびポートを除く）が含まれない場合、システムは信頼できるトラフィックの一部の特性（アプリケーションなど）を学習できません。信頼できるトラフィックではなく許可にルールを変更すると、システムはすべてのトラフィックのインスペクションを実行します。

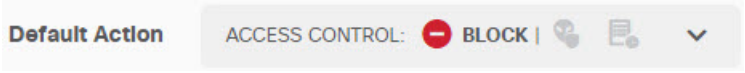
a) [ポリシー（Policies）]ページの[アクセス コントロール（Access Control）]をクリックします。
b) Inside_Outside_Rule 行の右側にある [アクション（Actions）]セルにマウスを合わせると、編集アイコンと削除アイコンが表示されます。ルールを開くには、編集アイコン（）をクリックします。
c) [アクション（Action）]の [許可（Allow）] を選択します。



d) [OK（OK）]をクリックして変更を保存します。

ステップ 3 アクセス コントロール ポリシーのデフォルト アクションでロギングを有効化します。
接続のロギングが有効なアクセス コントロール ルールと接続が一致する場合にのみ、ダッシュボードに接続情報が表示されます。Inside_Outside_Rule ではロギングが有効ですが、デフォルト アクションのロギングは無効化されています。そのため、ダッシュボードにはInside_Outside_Rule の情報のみが表示され、ルールと一致しない接続は反映されません。

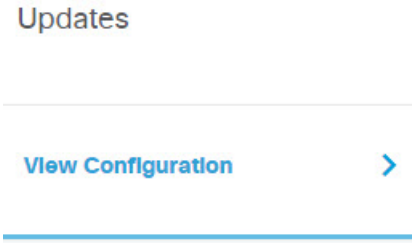
a) アクセス コントロール ポリシー ページの下部のデフォルト アクションで、任意の場所をクリックします。



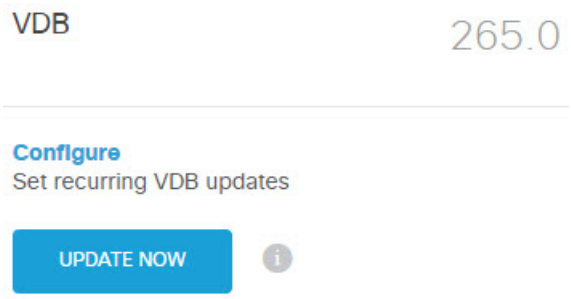
b) [ログ アクションの選択（Select Log Action）＞[接続の開始時および終了時（At Beginning and End of Connection）] を選択します。
c) [OK]をクリックします。

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

a) [デバイス（Device）]メニューのデバイス名をクリックします。
b) [更新（Updates）] グループで [設定の表示（View Configuration）] をクリックします。

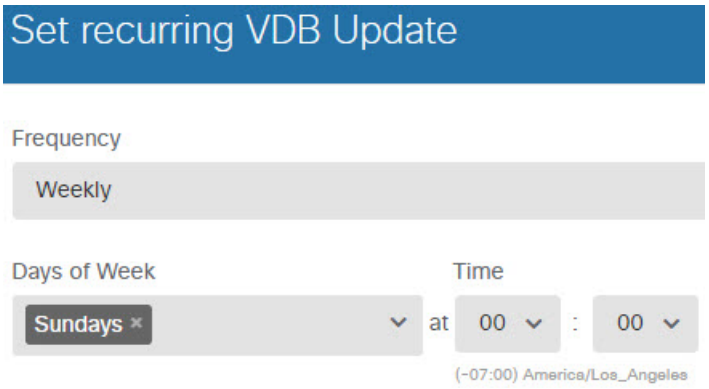


c) [VDB（VDB）] グループで [設定（Configure）]をクリックします。



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

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

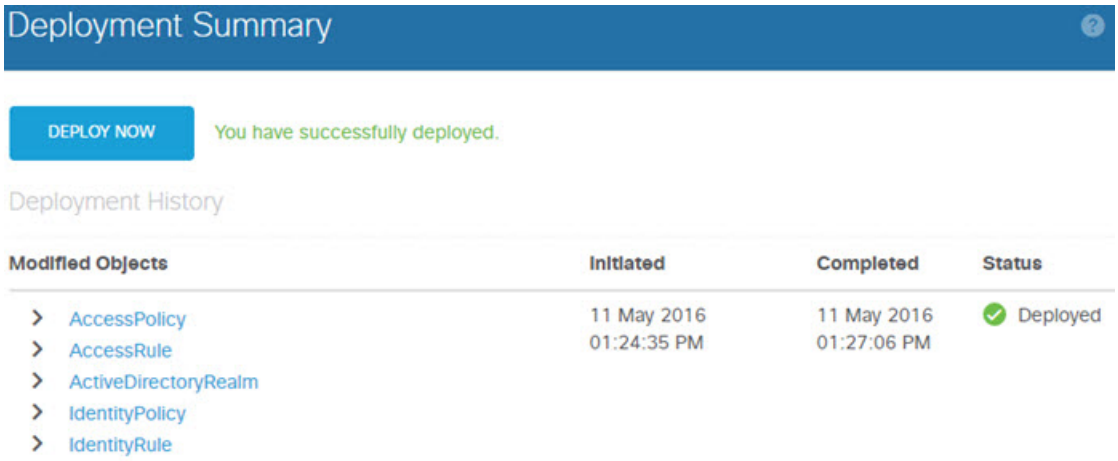


e) [保存（Save）]をクリックします。

ステップ 5 変更を保存します。

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

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。



次の作業

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

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

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

脅威をブロックする方法

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

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

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

Firepower システムでは、複数の侵入ポリシーが提供されています。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 まだ有効化していない場合は、[脅威（Threat）]ライセンスを有効化します。
侵入ポリシーを使用するには、脅威ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイスアイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイスダッシュボードが開きます。

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。

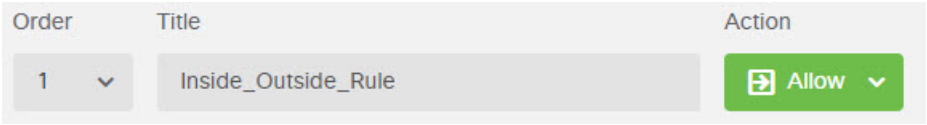
c) [脅威（Threat）]グループで [有効化（Enable）] をクリックします。
必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化（Disable）] ボタンに変わります。

ステップ 2 1 つまたは複数のアクセス ルールの侵入ポリシーを選択します。
脅威がないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule に侵入インスペクションを追加します。

a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されることを確認します。

b) Inside_Outside_Rule 行の右側にある [アクション（Actions）]セルにマウスを合わせると、編集アイコンと削除アイコンが表示されます。ルールを開くには、編集アイコン（）をクリックします。

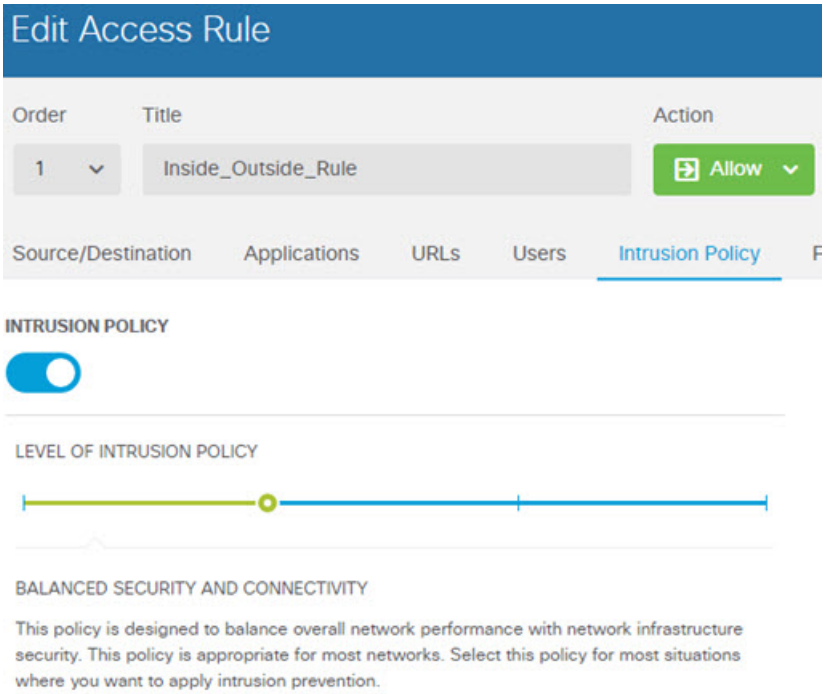
c) まだ選択していない場合は、[アクション（Action）]の [許可（Allow）] を選択します。



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

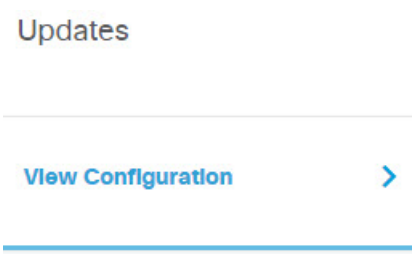
セキュリティを強力にする必要がある場合は、[接続よりセキュリティを優先する（Security over Connectivity）] ポリシーを試します。[最大検出（Maximum Detection）]ポリシーでは、ネットワークインフラストラクチャのセキュリティがよりいっそう重視され、動作にさらに大きな影響を及ぼす可能性があります。



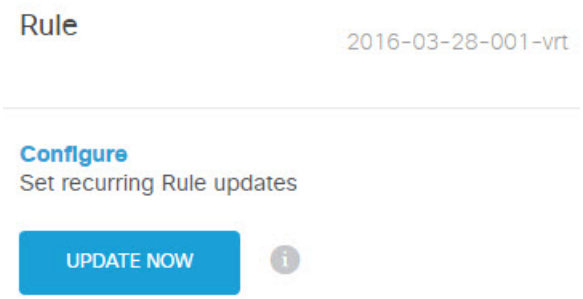
f) [OK（OK）]をクリックして変更を保存します。

ステップ 3 侵入ルール データベースの更新スケジュールを設定します。
シスコは、接続をドロップするかどうかを決定する侵入ポリシーで使用される、侵入ルール データベースの更新を定期的にリリースしています。定期的にルール データベースを更新する必要があります。更新を手動でダウンロードするか、または定期的なスケジュールを設定することができます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、データベースの更新は無効化されているため、更新されたルールを取得するには操作を実行する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
b) [更新（Updates）] グループで [設定の表示（View Configuration）]をクリックします。

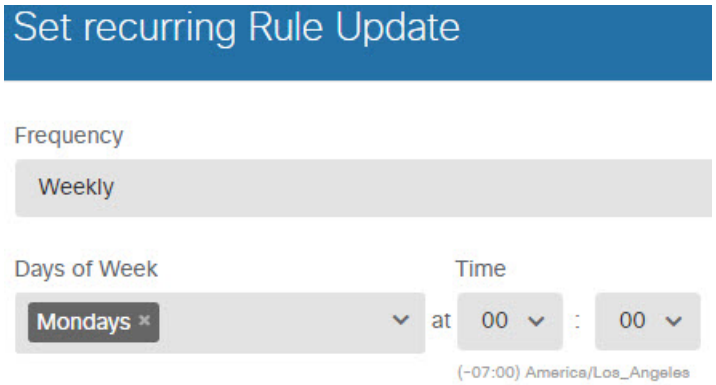


c) [ルール（Rule）] グループで [設定（Configure）]をクリックします。



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

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



e) [保存（Save）] をクリックします。

ステップ 4 変更を保存します。

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

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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

マルウェアをブロックする方法

ユーザは、インターネット サイトまたは電子メールなどのその他の通信方法から、悪意のあるソフトウェア（マルウェア）を取得する危険に常にさらされています。信頼できる Web サイトでも、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 の高度なマルウェア防御（Firepower の AMP）を使用してマルウェアを検出するには、ファイルポリシーを使用します。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

Firepower の AMP では、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る可能性のあるマルウェアの性質を取得します。AMP クラウドに到達してマルウェア ルックアップを実行するには、管理インターフェイスにインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドにクエリーします。可能性のある性質は、[クリーン（clean）]、[マルウェア（malware）]、または [不明（unknown）]（明確な判定を下せない）になります。 AMP クラウドに到達できない場合、性質は [不明（unknown）]になります。

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

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

手順

ステップ 1 まだ有効化していない場合は、[マルウェア（Malware）]ライセンスを有効化します。
マルウェア制御にファイルポリシーを使用するには、マルウェア ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイス アイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイス ダッシュボードが開きます。

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。

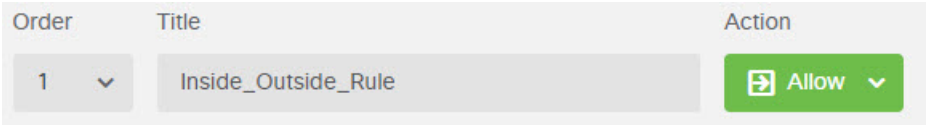
c) [マルウェア（Malware）]グループで [有効化（Enable）] をクリックします。
必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化（Disable）]ボタンに変わります。

ステップ 2 1 つまたは複数のアクセス ルールのファイル ポリシーを選択します。
マルウェアがないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule にファイル インスペクションを追加します。

a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されることを確認します。

b) Inside_Outside_Rule 行の右側にある [アクション（Actions）]セルにマウスを合わせると、編集アイコンと削除アイコンが表示されます。ルールを開くには、編集アイコン（）をクリックします。

c) まだ選択していない場合は、[アクション（Action）]の [許可（Allow）] を選択します。

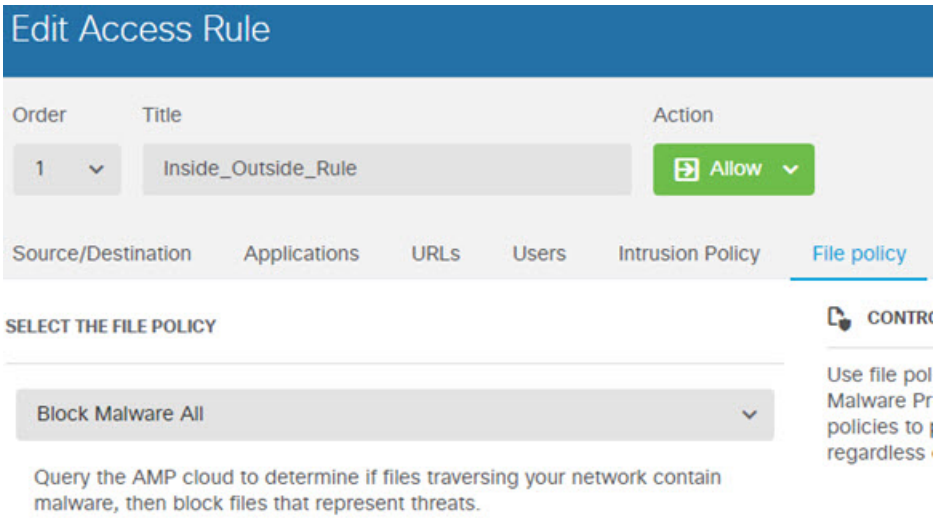


d) [ファイル ポリシー（File Policy）]タブをクリックします。

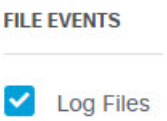
e) 使用するファイル ポリシーをクリックします。
主な選択は、マルウェアと見なされるすべてのファイルをドロップする [すべてのマルウェアをブロックする（Block Malware All）]、または AMP クラウドにクエリーしてファイルの性質を判断するけれどもブロックはしない [すべてのクラウド ルックアップを実行する（Cloud Lookup All）] です。ファイルがどのように評価されるかを確認する場合は、クラウド ルックアップを使用します。ファイルが評価される方法に納得したら、後でブロッキング ポリシーに切り替えることができます。

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

この例では、[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）] の下にある [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 ポリシーを選択するとファイル ロギングは有効化されます。イベントおよびダッシュボードにファイルおよびマルウェア情報を表示するには、ファイル ロギングを有効化する必要があります。



g) [OK（OK）]をクリックして変更を保存します。

ステップ 3 変更を保存します。

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

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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

アクセプタブルユースポリシー（URLフィルタリング）の実装方法

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

URL フィルタリングを使用して、アクセス ポリシーと共にアクセプタブル ユース ポリシーを定義できます。広範なカテゴリ（ギャンブルなど）でフィルタリングできるため、ブロックするWebサイトを個別に識別する必要はありません。カテゴリの照合では、サイトの関連レピュテーションを指定して、許可またはブロックすることもできます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、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、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。この例では、複数のカテゴリのあらゆるレピュテーションのサイト、高リスクのソーシャル ネットワーキング サイト、および未分類サイトである badsite.example.com をブロックします。

手順

ステップ 1 まだ有効化していない場合は、[URL（URL）]ライセンスを有効化します。
Web カテゴリおよびレピュテーションの情報を使用するには、またはダッシュボードおよびイベントで情報を表示するには、URL ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイスアイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイスダッシュボードが開きます。

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

ステップ 2 URL フィルタリングのアクセス コントロール ルールを作成します。
ブロッキング ルールの作成前に、ユーザがアクセスしているサイトのカテゴリを最初に確認できます。その場合、許可するカテゴリ（金融サービスなど）に [許可（Allow）] アクションを設定したルールを作成できます。すべての Web 接続のインスペクションを実行して、URL がこのカテゴリに属しているかどうかを判断する必要があるため、金融サービス以外のサイトのカテゴリ情報も取得します。

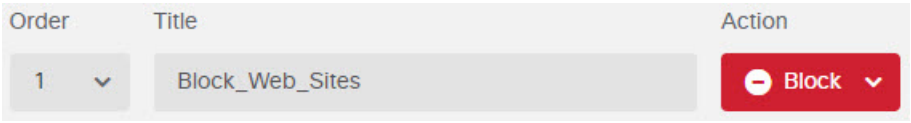
しかし、ブロックする必要があるとすでにわかっている Web カテゴリもあります。ブロッキング ポリシーでもインスペクションが強制されるため、ブロックされるカテゴリだけでなく、ブロックされないカテゴリへの接続に関するカテゴリ情報も取得します。

a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されることを確認します。

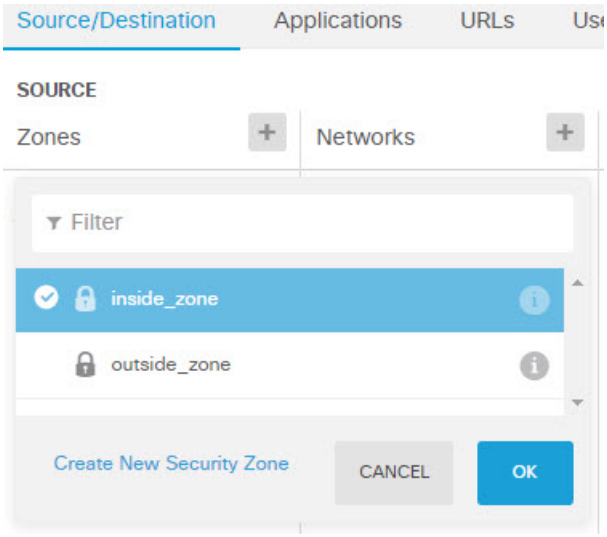
b) [+]をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

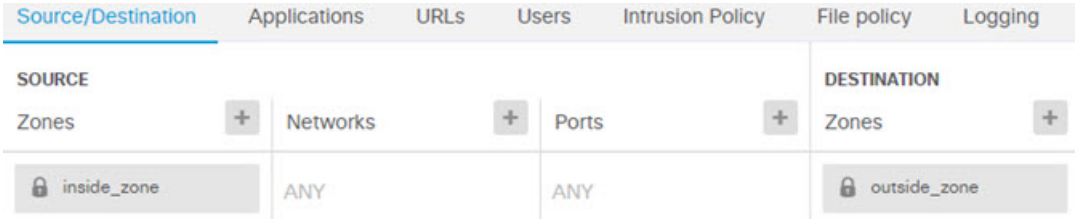
- [順序（Order）] : デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセス コントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを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



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



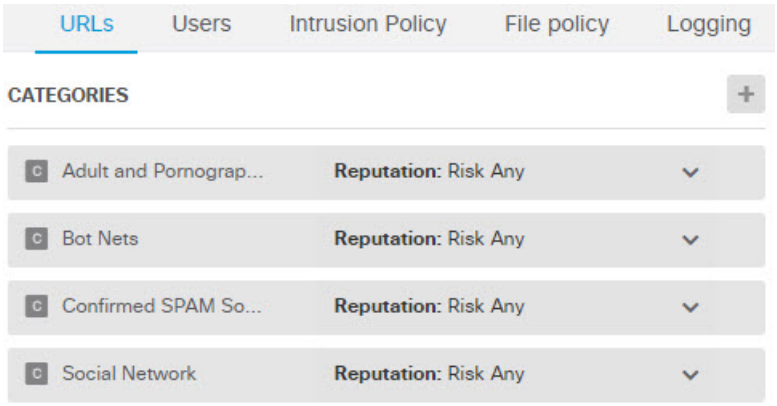
e) 同じ方法で、[宛先（Destination）] > [Zones（ゾーン）] の [outside_zone（outside_zone）] を選択します。



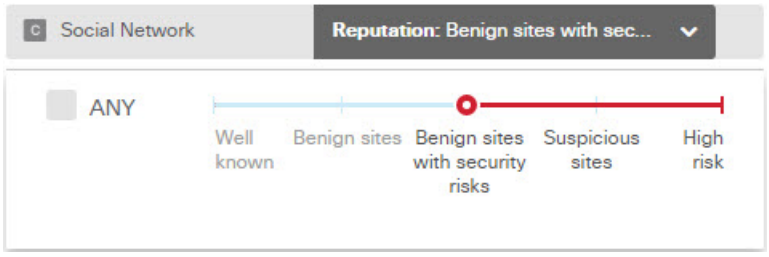
f) [URL（URLs）]タブをクリックします。

g) [カテゴリ（Categories）]の [+] をクリックして、完全または部分的にブロックするカテゴリを選択します。
この例では、[アダルトおよびポルノ（Adult and Pornography）]、[ボットネット（Bot Nets）]、[確認済みのスパム送信元（Confirmed SPAM Sources）]、および [ソーシャル ネットワーク

（Social Network）] を選択します。ブロックすることが必要な可能性が高い追加カテゴリがあります。



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



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

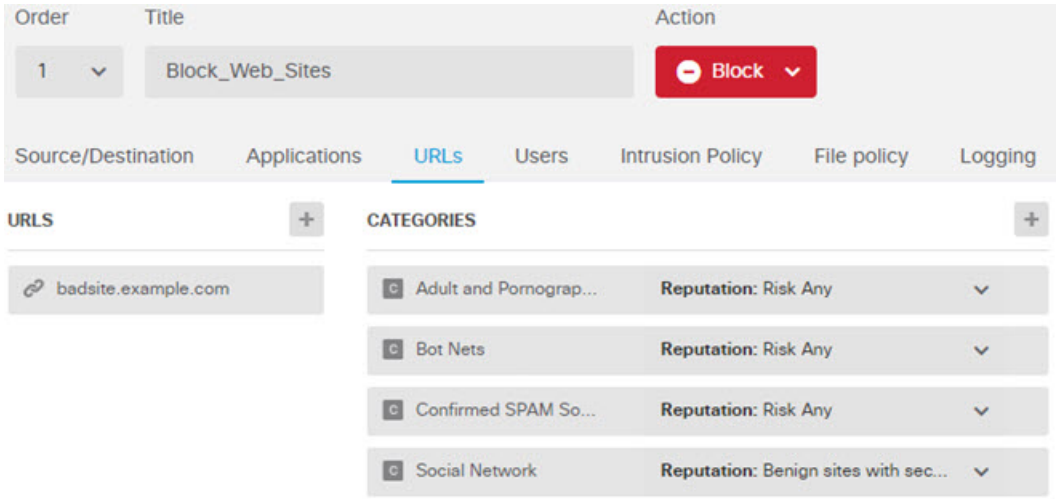
レピュテーションを使用すると、別の方法で許可したカテゴリ内のサイトを選択的にブロックできます。

i) カテゴリ リストの左側にある [URL（URLS）] リストの横の [+] をクリックします。

j) ポップアップ ダイアログ ボックスの下部で、[新規 URL の作成（Create New URL）] リンクをクリックします。

k) 名前とURL の両方に「badsite.example.com」と入力して、[追加（Add）]、[OK（OK）] の順にクリックしてオブジェクトを作成します。
オブジェクトに URL と同じ名前を付けるか、またはオブジェクトに別の名前を付けることができます。URL には、URL のプロトコル部分を含めず、サーバ名のみを追加します。

l) 新規オブジェクトを選択して、[OK（OK）]をクリックします。
ポリシーの編集時に新規オブジェクトを追加するだけで、リストにオブジェクトが追加されます。新規オブジェクトは、自動的に選択されません。



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）] > [接続の開始時および終了時（At Beginning and End of Connection）] を選択します。
Web カテゴリ ダッシュボードおよび接続イベントにカテゴリおよびレピュテーションの情報を表示するには、ロギングを有効化する必要があります。

n) [OK（OK）]をクリックしてルールを保存します。

ステップ 3 （オプション）URL フィルタリングを設定します。

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

また、分類されていないURLを分析のためにシスコに送信するよう選択することもできます。これによって、ユーザがカテゴリおよびレピュテーションのない新しいサイトにアクセスすると、シスコはサイトを評価して分類し、レピュテーションを指定し、今後の更新に含めることができます。その後、新しい情報に基づいて、今後のサイトへのアクセスを許可またはブロックすることができます。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
b) [システム設定（System Settings）] > [トラフィック設定（Traffic Settings）] > [クラウド設定）Cloud Preferences] をクリックします。
c) [未知の URL 用 Cisco CSI のクエリー（Query Cisco CSI for Unknown URLs）]を選択します。
d) [保存（Save）]をクリックします。

ステップ 4 変更を保存します。

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

b) [今すぐ展開（Deploy Now）] ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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

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

アプリケーションの使用を制御する方法

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

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

特定のアプリケーションを許可またはブロックするよう選択できますが、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性に基づいてルールを記述することもできます。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

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

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

はじめる前に

この使用例では、使用例ネットワーク トラフィックを調べる方法, （25 ページ）を完了していることを前提としています。その使用例では、[アプリケーション（Applications）] ダッシュボードで分析できる、アプリケーションの使用状況に関する情報を取得する方法について説明しています。実際に使用されているアプリケーションを理解することで、効率的なアプリケーションベースのルールを設計できます。また、その使用例では、VDB の更新をスケジュールする方法についても説明しています（ここでは繰り返しません）。アプリケーションを正しく識別できるように、定期的に VDB を更新してください。

手順

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

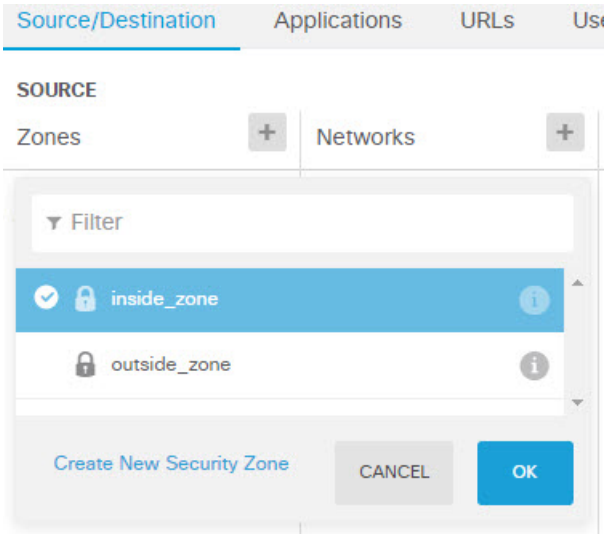
a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されることを確認します。

b) [+]をクリックして新しいルールを追加します。

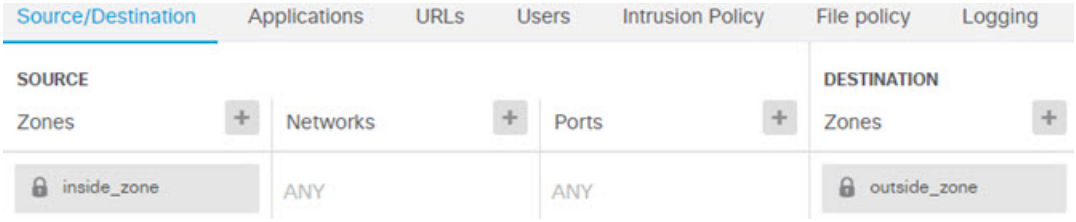
c) 順序、タイトル、およびアクションを設定します。

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

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



e) 同じ方法で、[宛先（Destination）]>[Zones（ゾーン）] の [outside_zone（outside_zone）] を選択します。



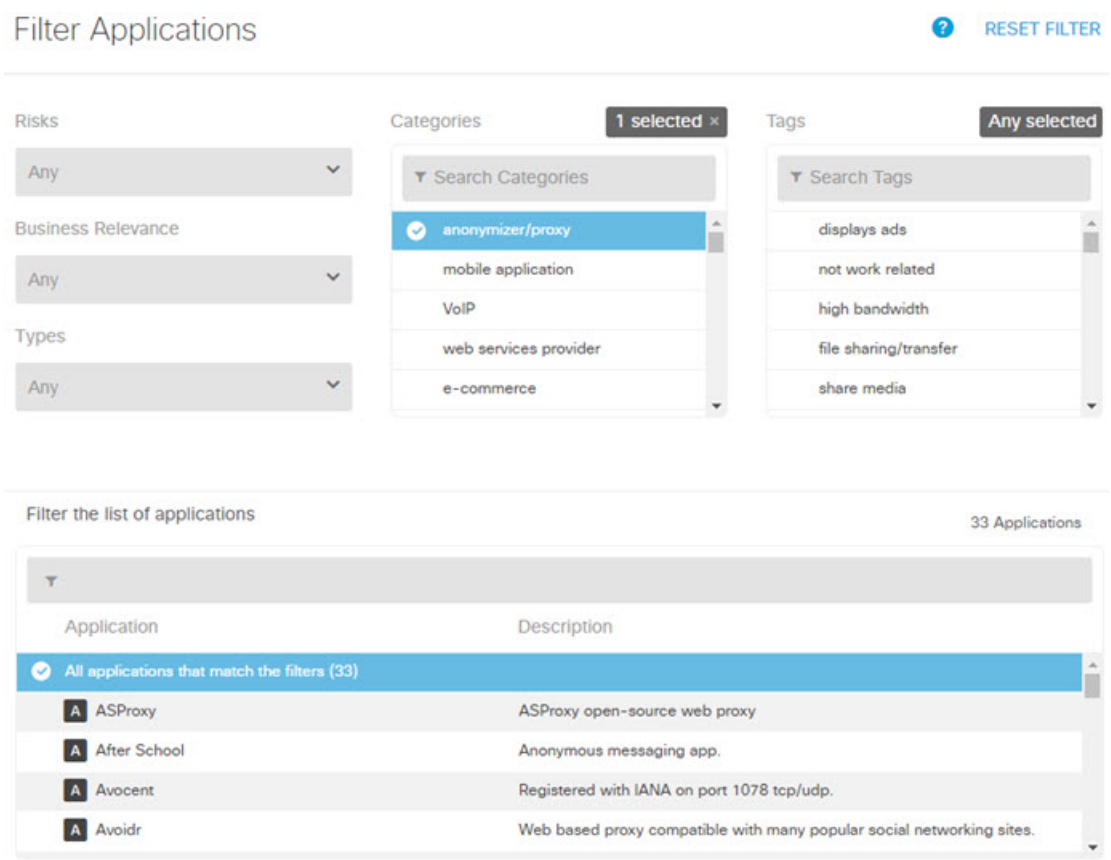
f) [アプリケーション（Applications）]タブをクリックします。

g) [アプリケーション（Applications）] の [+] をクリックして、ポップアップ ダイアログ ボックスの下部にある [高度なフィルタ（Advanced Filter）] リンクをクリックします。
事前にアプリケーション フィルタ オブジェクトを作成して、ここの [アプリケーション フィルタ（Application Filters）] リストで選択できますが、アクセス コントロール ルールで条件を直接指定して、オプションで条件をフィルタ オブジェクトとして保存することもできます。単一のアプリケーションにルールを記述していない場合は、[高度なフィルタ（Advanced Filter）] ダイアログ ボックスを使用して、より簡単にアプリケーションを検索して適切な条件を生成することができます。

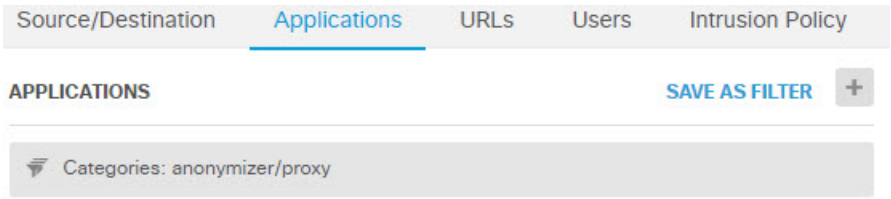
条件を選択すると、ダイアログ ボックスの下部にある [アプリケーション（Applications）] リストが更新され、条件に一致するアプリケーションが表示されます。記述したルールは、これらのアプリケーションに適用されます。

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

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



h) [高度なフィルタ（ Advanced Filters）] ダイアログ ボックスで、[追加（Add）]をクリックします。
フィルタが追加され、[アプリケーション（Applications）] タブに表示されます。



i) [ロギング（Logging）]タブをクリックして、[ログ アクションの選択（Select Log Action）] > [接続の開始時および終了時（At Beginning and End of Connection）] を選択します。
このルールによってブロックされる接続の情報を取得するには、ロギングを有効化する必要があります。

j) [OK（OK）]をクリックしてルールを保存します。

ステップ 2 変更を保存します。

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

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

ステップ 3 [モニタリング（Monitoring）]をクリックして、結果を評価します。
これで、[ネットワークの概要（Network Overview）] ダッシュボードのアプリケーション ウィジェットにドロップされた接続が表示されます。[すべて（All）]/[拒否（Denied）]/[許可（Allowed）] ドロップダウン オプションを使用して、ドロップされたアプリケーションのみに焦点を当てます。

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

サブネットを追加する方法

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

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

- サブネットは、プライベート ネットワーク 192.168.2.0/24 を使用する内部ネットワークです。

- ネットワークのインターフェイスには、スタティック アドレス 192.168.2.1 があります。この例では、物理インターフェイスはこのネットワーク専用です。別の方法では、すでに接続されているインターフェイスを使用して、新しいネットワークのサブインターフェイスを作成します。
- デバイスは、DHCP を使用してネットワーク上のワークステーションにアドレスを提供します。アドレス プールとして 192.168.2.2 ～ 192.168.2.254 を使用します。
- 他の内部ネットワークおよび外部ネットワークへのネットワーク アクセスは、許可されます。外部ネットワークに移動するトラフィックでは、NAT を使用してパブリック アドレスを取得します。

はじめる前に

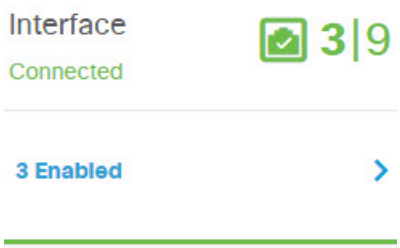
ネットワーク ケーブルを新しいサブネットのインターフェイスおよびスイッチに物理的に接続します。

手順

ステップ 1 インターフェイスを設定します。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイス アイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイス ダッシュボードが開きます。

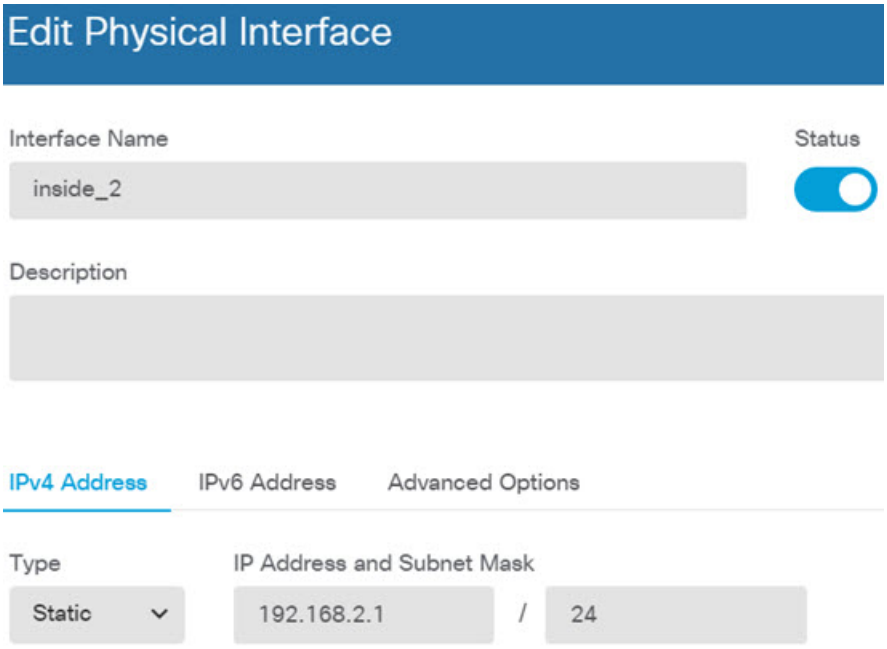
b) 有効なインターフェイスの数を示す[インターフェイス（Interfaces）]グループで、リンクをクリックします。
デバイス上のインターフェイスの合計数に対する有効なインターフェイスの数の概要が示されます。これは、モデルごとに異なります。この例では、9 個のうち 3 個のインターフェイスが有効です。



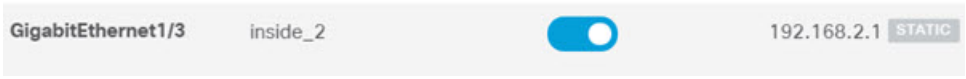
c) 接続しているインターフェイスの行の右側にある[アクション（Actions）]セルにマウスを合わせて、編集アイコン（）をクリックします。
d) 基本的なインターフェイスのプロパティを設定します。

- [名前（Name）]：インターフェイスに固有の名前（inside_2 など）。

- [ステータス（Status）]：ステータストグルをクリックして、インターフェイスを有効化します。
- [IPv4 アドレス（IPv4 Address）]タブ：[タイプ（Type）] に [スタティック（Static）] を選択して、192.168.2.1/24 を入力します。



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

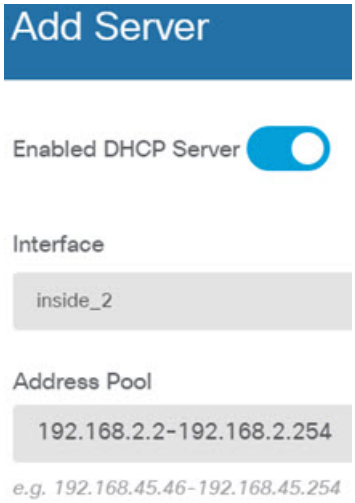


ステップ 2 インターフェイスの DHCP サーバを設定します。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
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 サーバの表までスクロール ダウンして、表の上部の [+]をクリックします。
d) サーバのプロパティを設定します。

- [DHCP サーバの有効化（Enable DHCP Server）]：このトグルをクリックして、サーバを有効化します。
- [インターフェイス（Interface）]：DHCPサービスを提供しているインターフェイスを選択します。この例では、inside_2 を選択します。

- [アドレス プール（AddressPool）]：サーバがネットワーク上のデバイスに供給できるアドレス。192.168.2.2 ～ 192.168.2.254 を入力します。ネットワーク アドレス（.0）、インターフェイス アドレス（.1）、またはブロードキャスト アドレス（.255）が含まれないようにしてください。また、ネットワーク上のデバイスにスタティック アドレスが必要な場合は、プールからそれらのアドレスを除外します。プールは単一の連続したアドレスである必要があるため、範囲の最初または最後からスタティック アドレスを選択します。

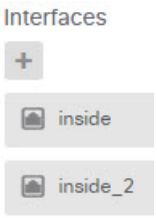


e) [追加（Add）]をクリックします。

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

ステップ 3 内部セキュリティ ゾーンにインターフェイスを追加します。
インターフェイスにポリシーを記述するには、インターフェイスはセキュリティ ゾーンに属している必要があります。セキュリティ ゾーンのポリシーを記述します。そのため、ゾーンでインターフェイスを追加および削除すると、インターフェイスに適用されたポリシーは自動的に変更されます。

a) メイン メニューで [オブジェクト（Objects）]をクリックします。
b) 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。
c) [inside_zone（inside_zone）]オブジェクトの行の右側にある [アクション（Actions）] セルにマウスを合わせて、編集アイコン（）をクリックします。
d) [インターフェイス（Interfaces）]の下にある [+] をクリックして、inside_2 インターフェイスを選択し、インターフェイス リストで [OK（OK）] をクリックします。



e) [保存（Save）] をクリックします。

ステップ 4 内部ネットワーク間のトラフィックを許可するアクセス コントロール ルールを作成します。トラフィックは、すべてのインターフェイス間で自動的には許可されません。希望のトラフィックを許可するには、アクセスコントロールルールを作成する必要があります。唯一の例外は、アクセス コントロール ルールのデフォルト アクションでトラフィックを許可している場合です。この例では、デバイスのセットアップ ウィザードで設定したブロックのデフォルトアクションを保持していることを前提としています。したがって、内部インターフェイス間のトラフィックを許可するルールを作成する必要があります。このようなルールをすでに作成している場合は、この手順をスキップします。

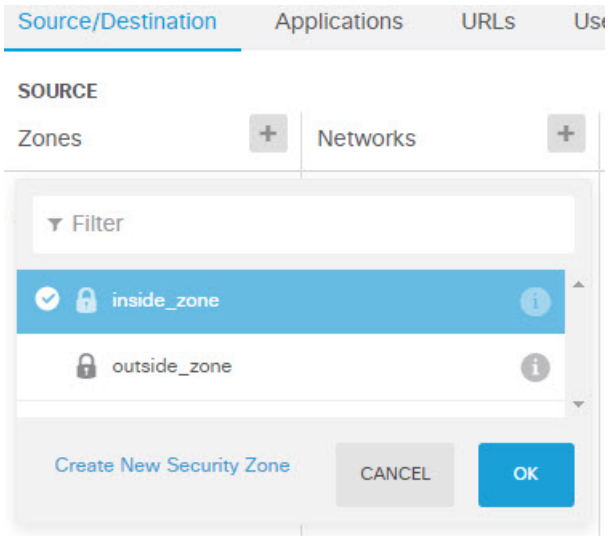
a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されることを確認します。

b) [+]をクリックして新しいルールを追加します。

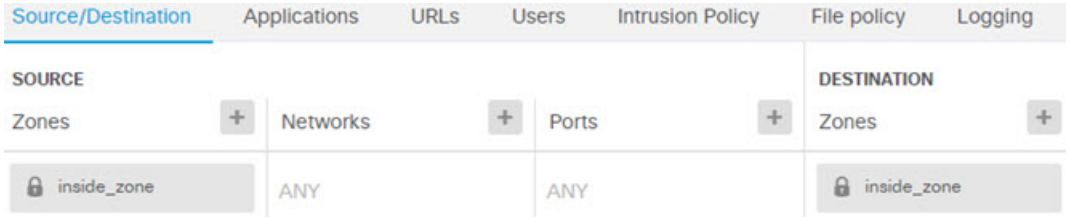
c) 順序、タイトル、およびアクションを設定します。

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

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



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



f) （オプション）侵入およびマルウェアのインスペクションを設定します。
内部インターフェイスは信頼できるゾーン内にありますが、一般的に、ユーザはラップトップをネットワークに接続します。そのため、ユーザは、外部ネットワークまたはWi-Fiホットスポットからネットワーク内に知らないうちに脅威を持ち込んでいます。したがって、内部ネットワーク間を移動するトラフィックに侵入やマルウェアの形跡がないかスキャンする必要がある場合があります。

次の操作の実行を検討します。

- [侵入ポリシー（Intrusion Policy）]タブをクリックして侵入ポリシーを有効化し、スライダを使用して[セキュリティと接続のバランスをとる（Balanced Security and Connectivity）]ポリシーを選択します。
- [ファイル ポリシー（File Policy）]タブをクリックして、[すべてのマルウェアをブロックする（Block Malware All）] ポリシーを選択します。

g) [ロギング（Logging）]タブをクリックして、[ログ アクションの選択（Select Log Action）] > [接続の開始時および終了時（At Beginning and End of Connection）] を選択します。
このルールに一致する接続に関する情報を取得するには、ロギングを有効化する必要があります。ロギングによってダッシュボードにスタティックが追加され、イベント ビューアにイベントが表示されます。

h) [OK（OK）]をクリックしてルールを保存します。

ステップ 5 新規サブネットに必要なポリシーが定義されていることを確認します。
inside_zone セキュリティ ゾーンにインターフェイスを追加することによって、inside_zone の既存のポリシーが自動的に新規サブネットに適用されます。ただし、ポリシーのインスペクションには時間がかかるため、ポリシーの追加が必要ないことを確認します。

デバイスの初期設定を完了すると、次のポリシーがすでに適用されています。

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

ステップ 6 変更を保存します。

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

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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

第 3 章

システムのライセンス

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

Firepower システムのスマート ライセンス

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

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

Cisco Smart Software Manager

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

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

ライセンスとアプライアンスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのアプライアンスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加

のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

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

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

ライセンス認証局との定期通信

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

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

スマート ライセンスのタイプ

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

Firepower Threat Defenseデバイスを購入すると、自動的に基本ライセンスが含まれています。その他すべての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	オプションのターム ライセンスに含まれないすべての機能。 [このトークンに登録された製品で輸出管理機能を許可する（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。国が輸出管理標準を満たしている場合にのみ、このオプションを選択できます。このオプションは、高度な暗号化および高度な暗号化を必要とする機能の使用を制御します。

ライセンス	期間	付与される機能
脅威	期間ベース	侵入検知および防御（Intrusion detection andprevention）：侵入ポリシーが、侵入およびエクスプロイトのネットワーク トラフィックを分析します。また、オプションで違反パケットをドロップします。 ファイル制御（Filecontrol）：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）をブロックします。マルウェア ライセンスが必要な Firepower の AMP を使用すると、マルウェアを含むファイルのインスペクションを実行してブロックすることができます。
マルウェア	期間ベース	マルウェアを確認するファイルポリシー。Cisco Advanced Malware Protection（AMP）を Firepower の AMP（ネットワークベースの高度なマルウェア防御）および AMP Threat Gridとともに使用します。 ファイルポリシーは、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックすることができます。
URL フィルタリング（URL Filtering）	期間ベース	カテゴリとレピュテーションに基づく URL フィルタリング。 このライセンスなしで、個々の URL で URL フィルタリングを実行できます。

期限切れまたは無効なオプション ライセンスの影響

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

オプションのライセンスを無効にすると、システムは次のように反応します。

- [マルウェア ライセンス（Malware license）]：システムは AMP クラウドへの問い合わせを停止し、AMP レトロスペクション クラウドから送信されたレトロスペクティブ イベントの認証も停止します。既存のアクセス コントロール ポリシーにマルウェア検出を適応ファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再展開することはできません。マルウェア ライセンスが無効にされた後、システムが既存のキャッシュ ファイ

ルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは Unavailable という性質をこれらのファイルに割り当てます。

- [脅威（Threat）]：システムは侵入またはファイル制御ポリシーを適用しなくなります。ライセンスを必要とする既存のポリシーを再展開することはできません。
- [URL フィルタリング（URL Filtering）]：URL カテゴリ条件が指定されたアクセス コントロール ルールは URL のフィルタリングをただちに停止し、システムは URL データへの更新をダウンロードしなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

スマート ライセンスの管理

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

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

使用認証により、スマート ライセンス エージェントのステータスが特定されます。

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

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

次の手順では、システム ライセンスの管理方法の概要について説明します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名、[スマート ライセンス（Smart License）] サマリで [設定の表示（View Configuration）] をクリックします。

ステップ 2 デバイスを登録します。
オプション ライセンスを割り当てる前に、Cisco Smart Software Manager に登録する必要があります。評価期間の終了前に登録してください。

デバイスの登録, （63 ページ）を参照してください。

ステップ 3 オプション機能のライセンスをリクエストして管理します。
ライセンスによって制御される機能を使用するためには、オプション ライセンスを登録する必要があります。オプション ライセンスの有効化と無効化, （64 ページ）を参照してください。

ステップ 4 システム ライセンスを維持します。
次の作業を実行できます。

- Cisco Smart Software Manager との同期, （65 ページ）
- デバイスの登録解除, （65 ページ）

デバイスの登録

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

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

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

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名、[スマート ライセンス（Smart License）] サマリで [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）]をクリックして、手順に従います。

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

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

[このトークンを使用して登録した製品で輸出管理機能を許可（Allow export-controlled functionality on the products registered with this token）]を選択するかどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化および高度な暗号化を必要とする機能の使用を制御します。

c) トークンをコピーして、[スマート ライセンスの登録（Smart License Registration）] ダイアログボックスの編集ボックスに貼り付けます。

d) [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（Device）]メニューのデバイス名し、[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、定期的に Cisco Smart Software Manager と同期されます。通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、アプライアンスはホームをコールすることなく最大で 90 日間は動作します。

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

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

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックし、[スマート ライセンス サマリ（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 ギア 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、そのデバイスを Cisco Smart Software Manager から登録解除できます。登録解除すると、基本ライセンス、およびデバイスに関連付けられたすべてのオプション ライセンスがバーチャル アカウントで解放されます。オプション ライセンスは他のデバイスに割り当てることができます。

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

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックし、[スマート ライセンス サマリ（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 ギア 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 実際にデバイスの登録を解除するには、警告を読み、[登録解除（Unregister）]をクリックします。

第 4 章

デバイスのモニタリング

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

トラフィック統計情報を取得するためにロギングを有効にする

モニタリング ダッシュボードおよびイベント ビューアを使用して、幅広いトラフィック統計をモニタできます。ただし、どの統計情報を収集すべきかシステムに知らせるためにロギングを有効にする必要があります。

オプションの統計情報を収集し、イベントを生成するには、個別のアクセス ルール上で次のロギング タイプを有効にします。

- 接続ロギング：接続の最後でロギングを行うと、接続に関するほとんどの情報が提供されます。接続の開始も記録できますが、これらのイベントの情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡するトラフィックを対象とする各ルール（およびデフォルトのアクション）でこれを有効にする必要があります。
- ファイル ロギング：検出されたファイルに関する情報を収集するには、ファイル ロギングを有効にする必要があります。ファイル ロギングは、アクセス ルールでファイル ポリシーを選択すると自動的に有効になりますが、それを無効にすることもできます。

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続（および接続の終了）を自動的にログに記録します。例外は、

デフォルト アクションによって処理される侵入イベントです。これらの侵入イベントを確認するには、デフォルト アクションで接続ロギングを有効にする必要があります。

ヒント

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

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

トラフィックのモニタリングおよびシステム ダッシュボード

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

（注） トラフィック関連のダッシュボードに使用されるデータは、接続またはファイル ロギングを有効にするアクセス 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と一致するトラフィックは反映されません。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザ情報はユーザ ID を収集するアイデンティティ ルールを設定している場合にのみ利用できます。さらに、侵入、ファイル、マルウェア、および Web カテゴリの情報は、それらの機能のライセンスがあり、機能を使用するルールを設定している場合のみ使用できます。

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

トラフィック関連のダッシュボードには、次のタイプの表示が含まれます。

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

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

- [ネットワークの概要（Network Overview）]：ネットワークのトラフィックに関する概要情報が表示されます。情報には、一致したアクセス ルール（ポリシー）、ユーザが送信側のトラフィック、接続で使用されてい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、最も頻繁に接続されている宛先が含まれます。
- [ユーザ（Users）]：ネットワークの上位ユーザが表示されます。ユーザ情報を表示するには、アイデンティティ ポリシーを設定する必要があります。

- [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、インスペクションを実行済みの接続にのみ提供されます。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロックルールと一致するかどうかのインスペクションが実行されます。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Webカテゴリ（Web Categories）]：訪問したWebサイトのカテゴリに基づいて、ネットワークで使用されているWebサイトの上位カテゴリ（ギャンブルや教育機関など）が表示されます。この情報を取得するためには、トラフィックの一致基準としてWebカテゴリを使用するアクセス コントロール ルールが少なくとも1つ必要です。情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判断するためにインスペクションを実行する必要があるトラフィックに関してのみ提供されます。最初のWebカテゴリのアクセス コントロールルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。
- [ポリシー（Policies）]：一致する上位のアクセスルールがネットワーク トラフィック別に表示されます。
- [入力ゾーン（Ingress Zones）]：デバイスに入るトラフィックが通過する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）]：デバイスから出るトラフィックが通過する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）]：侵入イベントをトリガーする接続の送信元である上位の攻撃者が表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [ターゲット（Targets）]：攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [脅威（Threats）]トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ファイル ログ（File Logs）]：ネットワーク トラフィックで確認された上位のファイル タイプが表示されます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
- [システム（System）]：インターフェイスとインターフェイスのステータス（IPアドレスを確認するには、そのインターフェイスにマウスオーバーします）、システムの全体的なスループット、およびシステムイベント、CPU使用率、メモリ使用率、ディスク使用率に関する概要情報など、システムの全体的情報が表示されます。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を表示するように、スループット グラフを制限できます。

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

ステップ 3 目次でこれらのリンクをクリックすることもできます。

- [イベント（Events）]：イベント発生時にイベントが表示する場合に選択します。個々のアクセス ルールに関連する接続イベントを表示するには、それぞれのアクセス ルールで接続のロギングを有効にする必要があります。これらのイベントは、ユーザの接続の問題を解決するのに役立ちます。

コマンドラインを使用したその他の統計情報のモニタリング

Firepower Device Manager ダッシュボードには、デバイスを介して移動するトラフィックや一般的なシステム使用状況に関連するさまざまな統計情報が表示されます。ただし、デバイス CLI にログインすることによって、ダッシュボードには表示されていない領域のその他の情報を取得できます（CLI（コマンドライン インターフェイス）へのログイン，（3 ページ）を参照）。

CLI には、これらの統計情報を表示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対になった **clear** コマンドがあります。

コマンドについては、『*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、次のコマンドが役に立ちます。

- **show nat** は、NAT ルールのヒット数を表示します。
- **show xlate** は、アクティブな実際の NAT 変換を表示します。
- **show conn** は、デバイスを介して行われる現在の接続に関する情報を表示します。
- **show dhcpd** は、インターフェイスで設定した DHCP サーバに関する情報を表示します。
- **show interface** は、各インターフェイスの使用状況の統計を表示します。

イベントの表示

ロギングを有効にしたアクセス ルールから生成されたイベントを表示できます。イベントはまた、トリガーされた侵入ポリシーとファイル ポリシーについても生成されます。

イベント ビューアテーブルには、生成されたイベントがリアルタイムで表示されます。新しいイベントが生成されると、古いイベントはテーブルからロール アウトされます。

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、次のことに依存します。

- 接続イベント：アクセス ルールは接続ロギングを有効に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、ファイル ロギングを有効にする必要があります。

手順

ステップ 1 メイン メニューの [監視（Monitoring）]をクリックします。

ステップ 2 目次から [イベント（Events）]を選択します。
イベント ビューアは、イベント タイプに基づいて、タブ上のイベントを整理します。詳細については、イベント タイプ, （73 ページ）を参照してください。

ステップ 3 表示するイベント タイプのタブをクリックします。
イベント リストでは、次の操作を実行できます。

- イベントをより簡単に検索、分析できるようにするために、新しいイベントの追加を停止するには、[一時停止（Pause）]をクリックします。新しいイベントが表示されるようにするには、[再開（Resume）]をクリックします。
- 新しいイベントの表示速度を制御するには、別のリフレッシュ レート（5、10、20、60 秒）を選択します。
- 必要なカラムを含むカスタム ビューを作成します。カスタム ビューを作成するには、タブバーの [+]ボタンをクリックするか、[カラムの追加/削除（Add/Remove Columns）] をクリックします。事前設定された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, （74 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、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，（76 ページ）を参照してください。

ステップ 4 必要に応じてテーブルにフィルタを適用すると、さまざまなイベント属性に基づき目的のイベントを見つけることができます。
新規フィルタを作成するには、ドロップダウンリストからアトミック要素を選択してフィルタを手動で入力し、フィルタの値を入力するか、フィルタリングの基準となる値を含むイベント テーブルのセルをクリックしてフィルタを作成します。同じカラムにある複数のセルをクリックして値の間に OR 条件を作成するか、異なるカラムにあるセルをクリックしてカラムの間に AND 条件を作成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 ルールの作成の詳細については、イベントのフィルタリング，（75 ページ）を参照してください。

フィルタを作成したら、次のいずれかを実行します。

- 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。さらに [フィルタ（Filter）]ボタンをクリックします。

イベント タイプ

システムは次の種類のイベントを生成できます。モニタリング ダッシュボードでこの情報に関連する統計情報を確認するには、次のイベントを生成する必要があります。

接続イベント

ユーザがシステムを通過するトラフィックを生成するときの接続イベントを生成できます。アクセス ルールで接続のロギングを有効化している場合のみ、接続イベントを確認できます。

接続イベントには、送信元および宛先 IP アドレスとポート、使用される URL およびアプリケーション、送信されるバイト数またはパケット数など、接続に関するさまざま情報が含まれています。この情報には、実行したアクション（たとえば接続の許可またはブロック）、接続に適用されるポリシーなども含まれます。

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、侵入の可能性を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時刻、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報の記録です。

ファイル イベント

ファイル イベントは、ファイル ポリシーに基づいてシステムがネットワーク トラフィック内で検出した（およびオプションでブロックした）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 ルールでファイルのロギングを有効にする必要があります。

システムがファイル イベントを生成するときは、呼び出しを行うアクセス コントロール ルールのロギング設定に関係なく、関連する接続の終了も記録します。

マルウェア イベント

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データを含むマルウェア イベントを生成できます。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールでファイルの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、イベントの表示に必要なカラムが簡単に表示されるようにすることができます。また、事前定義ビューは編集または削除できませんが、カスタム ビューは編集または削除できます。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 右側のイベント テーブルの上にある [追加/削除カラム（Add/Remove Columns）]アイコン ボタンをクリックし、選択したリストに、ビューに含めるカラムのみが含まれるようになるまで、カラムを選択または選択解除します。
使用可能な（ただし使用されていない）リストと選択されているリストの間で、カラムをクリックしてドラッグします。選択されているリスト内でカラムをクリックしてドラッグし、左から右に向かうテーブル内でのカラムの順番を変更することもできます。カラムについては、イベントフィールドの説明，（76 ページ）を参照してください。

完了したら [OK]をクリックして、カラムの変更を保存します。

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

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

イベントのフィルタリング

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

カラムのクリック

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

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

アトミック要素の選択

[フィルタ（Filter）]フィールドをクリックして、ドロップダウンから目的のアトミック要素を選択した後、照合値を入力することでフィルタを作成することもできます。これらの要素には、イベント テーブルのカラムとして表示されないイベント フィールドが含まれます。また、表示するイベントと入力された値との関係を定義するオペレータが含まれます。カラムをクリックすると必ず、「equals (=)」フィルタが表示されますが、要素を選択すると、数値フィールドに「greater than (>)」または「less than (<)」も選択できるようになります。

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

イベント フィルタの演算子

イベント フィルタには、次の演算子を使用できます。

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

複雑なイベント フィルタのルール

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

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

イベント フィールドの説明

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

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

操作

接続イベントの場合、接続をロギングしたアクセス コントロール ルールまたはデフォルト アクションに関連付けられたアクション。

許可（Allow）

明示的に許可された接続。

信頼（Trust）

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

ブロック（Block）

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

- 侵入ポリシーによってエクスプロイトが検出された接続。
- ファイルがファイル ポリシーによってブロックされている接続。

デフォルト アクション（Default Action）

接続はデフォルト アクションによって処理されました。

ファイル イベントまたはマルウェア イベントの場合、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するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

アプリケーション カテゴリ、アプリケーション タグ（Application Categories、Application Tag）

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

アプリケーションのリスク（Application Risk）

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

ブロック タイプ（Block Type）

イベントのトラフィック 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のクライアント アプリケーションとバージョン。

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

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

クライアント カテゴリ、クライアント タグ（Client Category、Client Tag）

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

クライアント リスク（Client Risk）

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

接続（Connection）

内部的に生成されたトラフィック フローの固有 ID。

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

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

接続バイト（Connection Bytes）

接続の合計バイト数。

接続時間（Connection Time）

接続の開始時刻。

接続タイムスタンプ（Connection Timestamp）

接続が検出された時刻。

拒否された接続（Denied Connection）

システムがイベントのトラフィック フローを拒否したかどうか。

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

受信ホストの国および大陸。

宛先 IP（Destination IP）

受信ホストの IP アドレス。

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

セッション レスポンダが使用するポートまたは ICMP コード。

方向（Direction）

ファイルの送信方向。

傾向（Disposition）

ファイルの性質。

マルウェア（Malware）

AMP クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。

正常（Clean）

AMP クラウドがファイルを正常に分類したことを示します。

不明（Unknown）

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

応対不可（Unavailable）

システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかであ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）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、システムが AMP クラウドに問い合わせなかったことを示します。

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

接続がデバイスを通り抜けたゾーンとインターフェイス。

イベント、イベント タイプ（Event、Event Type）

イベントのタイプ。

イベント秒、イベント マイクロ秒（Event Seconds、Event Microseconds）

イベントが検出された時刻（秒またはマイクロ秒単位）。

ファイル カテゴリ（File Category）

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

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

ファイルまたはマルウェア ファイルが作成された日時。

ファイル名（File Name）

ファイルの名前です。

ファイル ルールのアクション（File Rule Action）

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

ファイル SHA256（File SHA256）

ファイルの SHA-256 ハッシュ値。

ファイル サイズ（File Size）（KB）

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

ファイル タイプ（File Type）

ファイルのタイプ（HTML や MSEXE など）。

ファイル/マルウェア ポリシー（File/Malware Policy）

イベントの生成に関連付けられているファイル ポリシー。

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

イベントのトラフィック 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、ファイアウォール ルール（Firewall Policy Rule、Firewall Rule）

接続を処理したアクセス コントロール ルールまたはデフォルト アクション。

最初のパケット（First Packet）

セッションの最初のパケットが検出された日時。

HTTP リファラ（HTTP Referrer）

接続で検出された HTTP トラフィックの要求 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 レスポンス（HTTP Response）

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

IDS の分類（IDS Classification）

イベントを生成したルールが属する分類。

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

接続がデバイスに入ったゾーンとインターフェイス。

イニシエータ バイト、イニシエータ パケット（Initiator Bytes、Initiator Packets）

セッション イニシエータが送信した合計バイト数またはパケット数。

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

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

イニシエータ IP（Initiator IP）

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

インライン結果（Inline Result）

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

侵入ポリシー（Intrusion Policy）

イベントを生成したルールが有効にされた侵入ポリシー。

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

イベントのトラフィック フローと一致する侵入ルールのアクション。

最後のパケット（Last Packet）

セッションの最後のパケットが検出された日時。

MPLSラベル（MPLS Label）

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

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

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

メッセージ（Message）

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

NetBIOS ドメイン（NetBIOS Domain）

セッションで使用された NetBIOS ドメイン。

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

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

クライアントのオリジナル IP（Original Client IP）

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

ポリシー、ポリシーの改訂（Policy、Policy Revision）

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

プライオリティ（Priority）

Cisco Talos Security Intelligence and Research Group（Talos）によって決定されたイベント優先順位：High、Medium、または Low。

プロトコル（Protocol）

接続に使用されるトランスポート プロトコルです。

理由（Reason）

次の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）	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
ファイルモニタ（File Monitor）	システムが接続において特定のファイルの種類を検出しました。
ファイル復帰許可（File Resume Allow）	ファイル送信がはじめに [ファイルブロック（Block Files）] ルールまたは [マルウェア ブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。
ファイル復帰ブロック（File Resume Block）	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。
侵入ブロック（Intrusion Block）	接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の原因は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
侵入モニタ（Intrusion Monitor）	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。

受信時間（Receive Times）

イベントが生成された日時。

参照ホスト（Referenced Host）

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

レスポンダ バイト、レスポンダ パケット（Responder Bytes、Responder Packets）

セッション レスポンダが送信した合計バイト数またはパケット数。

レスポンダの国または大陸（Responder Country and Continent）

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

レスポンダ IP（Responder IP）

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

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ときにのみ使用できます。

ソース IP

侵入イベントで送信元ホストが使用する IP アドレス。

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

セッション イニシエータが使用するポートまたは ICMP タイプ。

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

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

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

ユーザ（User）

イニシエータの IP アドレスに関連付けられたユーザ。

VLAN

イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

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

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

Web アプリケーション カテゴリ、Web アプリケーション タグ（Web App Categories、Web App Tag）

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

Web アプリケーションのリスク（Web App Risk）

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

Web アプリケーション（Web Application）

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

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

第 5 章

オブジェクト

オブジェクトは、ポリシーまたはその他の設定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

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

オブジェクトタイプ	主な用途	説明
アプリケーション フィルタ	アクセス コントロール ルール	アプリケーション フィルタ オブジェクトは、IP接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネス関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使うのではなく、ポリシーにこれらのオブジェクトを使用してトラフィックを制御できます。 アプリケーション フィルタ オブジェクトの設定，（93 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は、トラフィックの送信元または宛先であるデバイスをホストする国および大陸を定義します。IP アドレスを使用するのではなく、ポリシーにこれらのオブジェクトを使用してトラフィックを制御できます。 地理位置情報オブジェクトの設定, （98 ページ）を参照してください。
ネットワーク	セキュリティ ポリシーおよびさまざまなデバイス設定	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。 ネットワーク オブジェクトとグループの設定, （89 ページ）を参照してください。
ポート	セキュリティ ポリシー	トラフィックのプロトコル、ポート、または ICMP サービスを定義するポート グループおよびポート オブジェクト（総称してポート オブジェクトと呼ばれます）。 ポート オブジェクトとグループの設定, （91 ページ）を参照してください。
セキュリティ ゾーン	セキュリティ ポリシー	セキュリティ ゾーンは、インターフェイスのグループです。ゾーンによって、ネットワークがトラフィックの管理や分類に役立つセグメントに分割されます。 セキュリティ ゾーンの設定, （92 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識別します。 syslog サーバの設定, （99 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	Web リクエストの URL または IP アドレスを定義する URL オブジェクトおよびグループ（総称して URLオブジェクトと呼ばれます）。 URL オブジェクトとグループの設定, （96 ページ）を参照してください。

オブジェクトの管理

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

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

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

手順

ステップ 1 [オブジェクト（Objects）]を選択します。
[オブジェクト（Objects）] ページには、使用可能なオブジェクト タイプが一覧表示される目次があります。オブジェクト タイプを選択すると、既存オブジェクトのリストが表示され、新しいオブジェクトを作成できます。オブジェクトの内容とタイプも確認できます。

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

- オブジェクトを作成するには、[+]ボタンをクリックします。オブジェクトの内容はタイプによって異なります。具体的な情報については、各オブジェクト タイプの設定トピックを参照してください。
- グループ オブジェクトを作成するには、[グループの追加（Add Group）]（）ボタンをクリックします。グループ オブジェクトには複数の項目が含まれます。
- オブジェクトを編集するには、そのオブジェクトの編集（）アイコンをクリックします。定義済みオブジェクトの内容は編集できません。
- オブジェクトを削除するには、そのオブジェクトの削除（）アイコンをクリックします。ポリシーや別のオブジェクトで現在使用されているオブジェクト、または定義済みのオブジェクトは削除できません。

ネットワーク オブジェクトとグループの設定

ホストまたはネットワークのアドレスを定義するには、ネットワーク グループとネットワーク オブジェクト（ネットワーク オブジェクトと総称される）を使用します。これらのオブジェクト

は、トラフィックの一致条件を定義するためにセキュリティ ポリシーで使用するか、サーバその他のリソースのアドレスを定義するために設定で使用することができます。

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

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

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

ネットワーク オブジェクト

オブジェクトの [タイプ（Type）]を、[ネットワーク（Network）] と [ホスト（Host）]のいずれかから選択します。次に、ホストまたはネットワークの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 または 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

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

ステップ 4 （新しいオブジェクトの）[追加（Add）]をクリックするか、（オブジェクトの編集時に）[保存（Save）] をクリックして変更を保存します。

ポート オブジェクトとグループの設定

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

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

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

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

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 オブジェクトの名前、さらに任意で説明を入力し、オブジェクトの内容を定義します。

ポート オブジェクト

[プロトコル（Protocol）]を選択し、次のようにプロトコルを設定します。

- TCP、UDP：単一のポートまたはポート範囲の番号を入力します（たとえば80（HTTPの場合）または 1-65535（すべてのポートをカバー））。
- ICMP、IPv6 ICMP：ICMPの[タイプ（Type）]を選択し、オプションで[コード（Code）]を選択します。タイプをすべての ICMP メッセージに適用するには、[任意（Any）]を選択します。タイプとコードについての詳細は、次のページを参照してください。
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- [その他（Other）]：目的のプロトコルを選択します。

ポート グループ

[+]ボタンは、グループに追加するポート オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 4 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。

セキュリティ ゾーンの設定

セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

システムは初期設定時に次のゾーンを作成します。これらのゾーンを編集してインターフェイスを追加または削除したり、使用しなくなったゾーンを削除したりすることができます。

- inside_zone：内部インターフェイスが含まれます。このゾーンは内部ネットワークを表すことを目的としています。
- outside_zone：外部インターフェイスが含まれます。このゾーンは、インターネットなどの制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターフェイスに接続するインターフェイスを outside_zone セキュリティ ゾーンに配置し、内部ネットワークに接続するすべてのインターフェイスを inside_zone セキュリティ ゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセス コントロール ルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセス ルールや他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。4つの内部ネットワークがあり、1つだけ他の3つとは異なる処理をしたい場合、1つではなく2つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用することができます。

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [新規セキュリティ ゾーンの作成（Create New Security Zone）]リンクをクリックすることで、セキュリティ ゾーンのプロパティを編集しながらセキュリティ ゾーンを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、次に目次から [セキュリティ ゾーン（Security Zones）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

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

ステップ 3 オブジェクトの名前、さらに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、ゾーンに追加するインターフェイスを選択します。
このリストは、現在ゾーンに含まれていないすべての名前付きインターフェイスを表示します。インターフェイスをゾーンに追加するには、インターフェイスを設定して名前を付ける必要があります。

すべての名前付きインターフェイスがすでにゾーンにある場合、リストは空になります。別のゾーンにインターフェイスを移動しようとする場合、最初に現在のゾーンから削除する必要があります。

ステップ 5 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）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 オブジェクトでは、IP接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性ごとにアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーション フィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

アプリケーション フィルタ オブジェクトを使用せず、ポリシーのアプリケーションとアプリケーション フィルタを直接選択することができます。ただし、同じアプリケーションまたはフィルタ グループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーション フィルタが含まれていて、これらは編集または削除できません。

（注） シスコでは、システムおよび脆弱性データベース（VDB）の更新を通じて、アプリケーション ディテクタを頻繁に更新し、追加します。したがって、リスクの高いアプリケーションをブロックするルールは、手動でルールを更新しなくても、新しいアプリケーションに自動的に適用されます。

次の手順では、[オブジェクト（Objects）] ページから直接オブジェクトを作成および編集する方法について説明します。[アプリケーション（Applications）] タブにアプリケーション基準を追加した後、[フィルタとして保存（Save As Filter）]リンクをクリックして、アクセス コントロール ルールを編集しながら、アプリケーション フィルタ オブジェクトも作成できます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、目次から [アプリケーション フィルタ（Application Filters）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

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

ステップ 3 オブジェクトの名前を入力し、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、オブジェクトに追加するアプリケーションとフィルタを選択します。
最初のリストには、継続的にスクロールするリストでアプリケーションが表示されます。[フィルタの詳細設定（[フィルタの詳細設定]）]をクリックすると、フィルタ オプションが表示され、アプリケーションを容易に選択できます。選択したら、[追加（Add）]をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

（注） 1 つのフィルタ条件内での複数の選択は OR 関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりすることができます。

リスク

アプリケーションが組織のセキュリティ ポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーション プロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル。
- [クライアント プロトコル（Client Protocol）]：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Web アプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も不可欠な機能を表す一般的な分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは [SSL プロトコル（SSL Protocol）]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）]タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

ステップ 5 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトの編集の場合）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、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別するために、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と、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、[グループの追加（Add Group）]ボタン（  ）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

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

ステップ 3 オブジェクトの名前、さらに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 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。

地理位置情報オブジェクトの設定

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。たとえば、地理的な場所を使用して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。

（注） 常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

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

手順

ステップ 1 [オブジェクト（Objects）]を選択し、目次から [地理位置情報（Geolocation）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

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

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 [大陸または国（Continents/Countries）]リストで[+ を追加（Add+）] をクリックして、オブジェクトに追加する大陸や国を選択します。
大陸を選択すると、大陸内のすべての国が選択されます。

ステップ 5 （新しいオブジェクトの）[追加（Add）]をクリックするか、（オブジェクトの編集時に） [保存（Save）] をクリックして変更を保存します。

syslog サーバの設定

syslog サーバのオブジェクトはコネクション型メッセージまたは診断システム ログ（syslog）メッセージを受信できるサーバを指定します。ログのコレクションと分析用に設定された syslog サーバがある場合、それらを定義するオブジェクトを作成し、そのオブジェクトをアクセス ルールまたは診断ロギング システム設定で使用します。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，（164 ページ）
- 診断ロギングの設定，（272 ページ）

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 [syslog サーバの追加（Add Syslog Server）] リンクをクリックすることで、syslog サーバのプロパティを編集しながら syslog サーバを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、次に目次から [Syslog サーバ（Syslog Server）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

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

ステップ 3 syslog サーバのプロパティを設定します。

- [デバイス インターフェイス（Device Interface）]：syslog サーバにアクセスするインターフェイスを選択します。
- [IP アドレス（IP Address）]：syslog サーバの IP アドレスを入力します。
- [ポート（Port）]：サーバが syslog メッセージを受信するために使用する UDP ポートを入力します。デフォルトは 514 です。

ステップ 4 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。

第 I 部

基本

第 6 章

インターフェイス

ここでは、Firepower Threat Defenseデバイスでのインターフェイスの設定方法について説明します。

Firepower Threat Defenseインターフェイスについて

Firepower Threat Defenseデバイスは、データ インターフェイスに加えて管理/診断インターフェイスが含まれています。次のトピックでは、Firepower Device Manager、および他のインターフェイス管理概念を通じたインターフェイス設定に関する制限事項について説明します。

インターフェイス設定の制限事項

Firepower Device Manager を使用してデバイスを設定する場合、インターフェイス設定に関するいくつかの制限があります。次の機能のいずれかが必要である場合、デバイスを設定するためにFirepower Management Centerを使用する必要があります。

- ルーテッド ファイアウォール モードのみがサポートされます。トランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- IPS 専用モードはサポートされていません。IPS 専用処理では、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 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティ ポリシーのみをサポートします。対照的に、ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよびTCP レイヤの両方でのフロー状態の追跡、TCP の標準化などのファイアウォール機能の対象となります。また、任意で、セキュリティ ポリシーに従ってファイアウォール モードのトラフィックにIPS 機能を設定することもできます。

- 冗長インターフェイスでは EtherChannel を設定できません。
- IPv4 の PPPoE を設定することはできません。インターネット インターフェイスが DSL、ケーブル モデム、または ISP へのその他の接続に接続されていて、ISP が PPPoE を使用して IP アドレスを提供している場合、これらの構成を設定するには、Firepower Management Center を使用する必要があります。
- ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X では、オプションのネットワーク インターフェイス カード（EPM）を設置できます。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、インストールの間にローカルまたはリモート管理を切り替えるとき、およびメジャー/マイナー リリース アップグレードの間）。SFP インターフェイスを含むカードでは、Firepower Device Manager が速度とデュプレックスを「自動」に設定しますが、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は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 に設定し、デュプレックスを [フル（Full）] に設定してから設定を展開します。リンクが機能しない場合、異なる速度を試行します。

ルーテッド インターフェイス

ルーテッド ファイアウォール モードでは、各インターフェイスは、一意のサブネットで IP アドレスを設定する必要があるレイヤ 3 ルーテッド インターフェイスになります。

1 つのインターフェイスに IPv6 アドレスと IPv4 アドレスの両方を設定できます。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。次のいずれかをグローバル アドレスとして指定することはできません。
  - 内部で予約済みの IPv6 アドレス：fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - 未指定のアドレス（::/128 など）
  - ループバック アドレス（::1/128）
  - マルチキャスト アドレス（ff00::/8）
  - リンクローカル アドレス（fe80::/10）
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などのネットワーク検出機能に使用できます。

最低限、IPv6が動作するようにリンクローカルアドレスを設定する必要があります。グローバルアドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカルアドレスを個別に設定する必要はありません。グローバルアドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

管理/診断インターフェイスとネットワーク配置

物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有できます。

管理インターフェイス

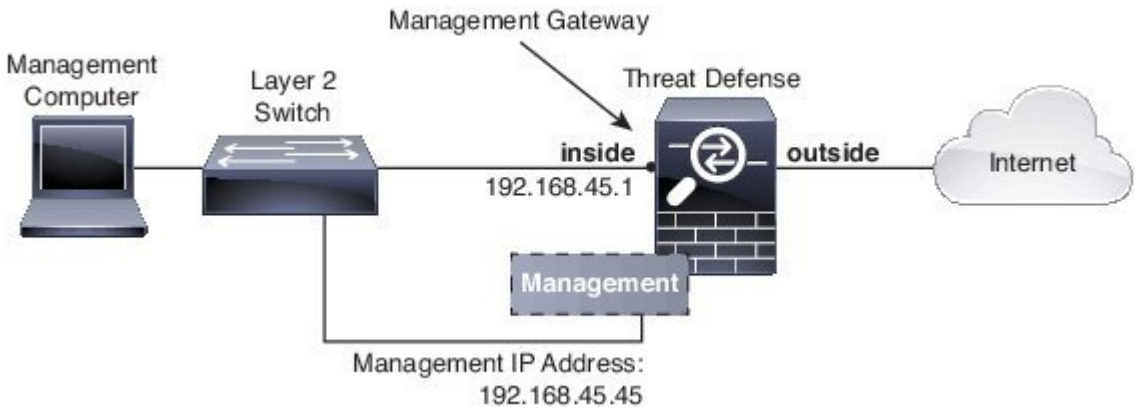
管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これはコンフィギュレーション インターフェイス を実行し、デバイスのコマンドライン インターフェイス（CLI）にアクセスしてさまざまな機能の更新情報を取得するために使用されます。アドレスは [システム設定（System Settings）] > [デバイス管理 IP（Device Management IP）] ページで設定します。**configure network** コマンドを使用して、CLIに追加の設定を構成できます。

診断インターフェイス

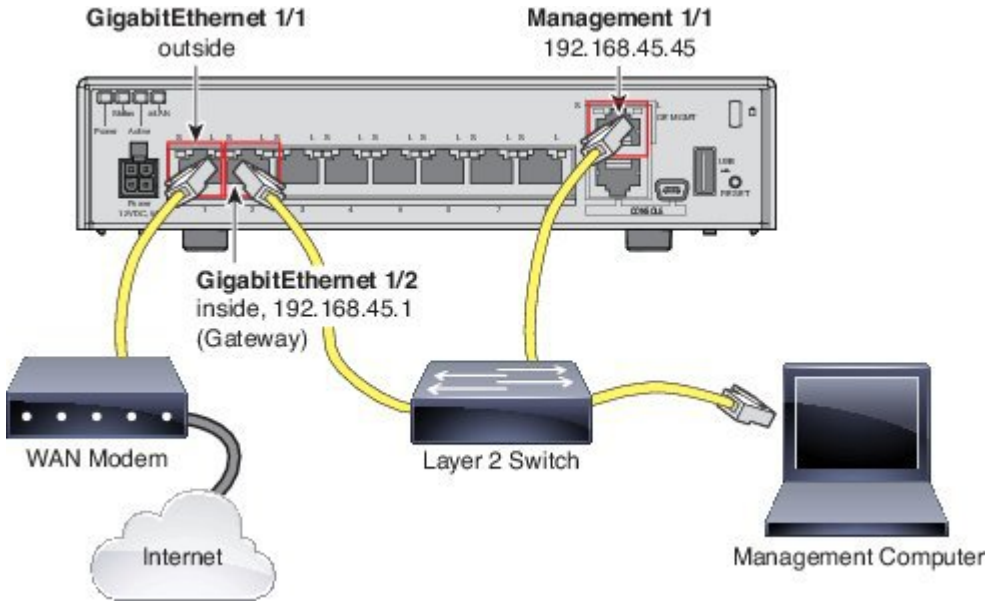
診断論理インターフェイスは、他のデータ インターフェイスと一緒に設定できます。診断インターフェイスの使用はオプションです。たとえば、データ インターフェイスを介してリモート syslog サーバにログ メッセージを送信する必要がない場合は、IP アドレスを設定します。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。

ルーテッド モードの導入

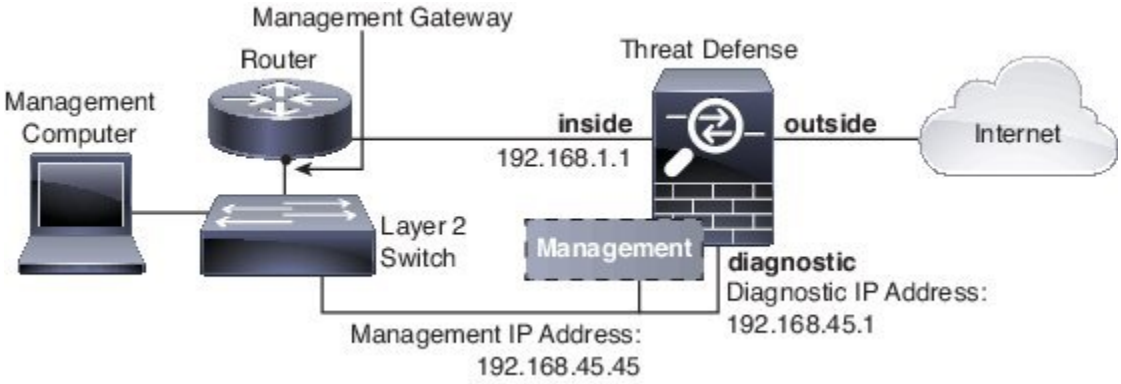
内部ルータがない場合は診断インターフェイスのIPアドレスを設定しないことをお勧めします。診断インターフェイスのIPアドレスを設定しなければ、他のデータインターフェイスと同じネットワーク上に管理インターフェイスを配置できます。診断インターフェイスを設定すると、一般的にその IP アドレスは管理 IP アドレスと同じネットワークになり、他のデータ インターフェイスと同じネットワーク上に存在できない標準インターフェイスと見なされます。管理インターフェイスは更新のためにインターネットにアクセスする必要があるため、管理インターフェイスを内部インターフェイスと同じネットワーク上に置くと、内部にスイッチのみを持つFirepower Threat Defenseデバイスを導入して、そのゲートウェイとして内部インターフェイスを指定することができます。内部スイッチを使用する次の導入を参照してください。



ASA 5506-X、ASA 5508-X、または ASA 5516-X で上記のシナリオをケーブル接続するには、次を参照してください。



診断 IP アドレスを設定する場合は、内部ルータが必要です。



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。その後、ゾーンに基づいてセキュリティ ポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、外部から内部に向けては設定できません。

診断/管理インターフェイスはゾーンに含まれません。ゾーンは、データインターフェイスにのみ適用されます。

[オブジェクト（Objects）]ページで、セキュリティ ゾーンを作成できます。

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 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビット イーサネットの速度と二重通信をそれぞれ1000と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

MTU について

MTU は、Firepower Threat Defense デバイス が特定のイーサネット インターフェイスで送信する最大フレーム ペイロード サイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば MTU を 1500 に設定した場合、想定されるフレーム サイズはヘッダーを含めて 1518 バイト、VLAN を使用する場合は 1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

パス MTU ディスカバリ

Firepower Threat Defense デバイス は、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 およびフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

UDP または ICMP の場合、アプリケーションではフラグメント化を避けるために MTU を考慮する必要があります。

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

MTU とジャンボ フレーム

MTUが大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての Firepower Threat Defense デバイス インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することをお勧めします。MTUの一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応：ジャンボ フレームとは、標準的な最大値 1522 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネット パケットのことです。ジャンボ フレームに対応するために、9198 バイトまでの MTU を設定できます。

（注） MTU を増やすとジャンボ フレームに割り当てられるメモリが増加し、他の機能（アクセス ルールなど）の最大使用量が制限される場合があります。ASA 5500-X シリーズ デバイスで、MTU をデフォルトの 1500 以上に増やす場合、システムを再起動する必要があります。

インターフェイスの設定

インターフェイス接続のためにケーブルを接続するとき、インターフェイスを設定する必要があります。最小限の作業として、物理インターフェイスを有効にし、このインターフェイスにIPアドレスを割り当てる必要があります。単一の物理インターフェイスではなく、VLANサブインターフェイスを特定のポートで作成する場合、通常、物理インターフェイスではなくサブインターフェイス上でIPアドレスを設定します。VLANサブインターフェイスを使用すると、物理インターフェイスを異なるVLAN ID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 リストは、利用可能なインターフェイス、その名前、アドレスおよびステータスを表示します。インターフェイスのステータスは、インターフェイスのリストで直接オン/オフを変更できます。このリストは、設定に基づいたインターフェイス特性を示します。

インターフェイスの現在の状態をモニタするには、ポート グラフィックを使用します。マウスオーバーでそのIPアドレス、有効なステータスとリンク ステータスを確認します。IPアドレスはDHCPを使用して静的に割り当てたり取得したりできます。

インターフェイス ポートは、次のカラー コーディングを使用します。

- 緑：インターフェイスが設定され、イネーブルであり、リンクが稼働中です。
- グレー：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されている場合、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されていない場合、これは予想される状態です。

次に、インターフェイスの設定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、使用する物理インターフェイスは有効にする必要があります。通常は名前も付けて、IPアドレッシングを設定します。VLANサブインターフェイスを作成する予定の場合、、IPアドレッシングを設定する必要はありません。

接続されたネットワークでの送信を一時的に防ぐために、インターフェイスを無効に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（Device）]メニューのデバイス名クリックして、[インターフェイス（Interfaces）]サマリのリンクをクリックします。
インターフェイス リストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。

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有効にするには、[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のサブインターフェイスを設定する予定の場合、すでに設定している可能性が高いです。[保存（Save）]をクリックして、VLAN サブインターフェイスと 802.1Q トランキングの設定, （112 ページ）に進みます。保存しない場合は、次に進みます。

（注） サブインターフェイスを設定している場合でも、インターフェイスに名前を付けて、IP アドレスを指定することができます。これは一般的な設定ではありませんが、必要だとわかっている場合は設定できます。

ステップ 4 以下を設定します。

- [インターフェイス名（Interface Name）]：最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。例、inside または outside。名前を設定しないと、インターフェイスの残りの設定は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。

  （注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

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

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

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

  - [ルート メトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。

  - [デフォルト ルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトであるこのオプションを選択します。

- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  （注） 既存のインターフェイスの場合、そのインターフェイスに対して DHCP サーバを設定していると、アドレスの変更機能は制限されます。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存在する必要があり、そのプールの一部にすることはできません。別のサブネットの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, （274 ページ）を参照してください。

ステップ 6 （オプション）[IPv6 アドレス（IPv6 Address）]タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）]を選択します。リンクローカルアドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

  （注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属すネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、Firepower Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）]を選択します。

- [スタティック アドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定，（104 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）]オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注） リンクローカルアドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカル アドレスによりパケットがドロップされることがあります。

- [RA を抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。Firepower Threat Defense デバイス は、ネイバー デバイスがデフォルトのルータ アドレスを動的に学習できるように、ルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホスト

は、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定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）詳細インターフェイス オプションの設定, （115 ページ）
詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 8 [保存（Save）]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、1 つの物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスやデバイスを追加しなくても、ネットワーク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。

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、通常は、物理インターフェイスをトラフィックが通過しないようにします。これは、物理インターフェイスはタグなしパケットを通過させるためです。トラフィックがサブインターフェイスを通過するためには物理インターフェイスを有効にする必要があるため、物理インターフェイスに名前を付けないことで、物理インターフェイスをトラフィックが通過しないようにします。物理インターフェイスにタグなしパケットを通過させる場合は、通常どおり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（Device）]メニューのデバイス名クリックして、[インターフェイス（Interfaces）]サマリのリンクをクリックします。
インターフェイス リストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。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。

- [+]ボタンをクリックして、新しいサブインターフェイスを作成します。
- 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、削除するサブインターフェイスの削除アイコン（）をクリックします。

ステップ 3 インターフェイスを有効にするには、[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、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。サブインターフェイスを作成後に、親インターフェイスを変更することはできません。
- [名前（Name）]：最大 48 文字のサブインターフェイスの名前。英字は小文字にする必要があります。例、inside または outside。名前を設定しないと、インターフェイスの残りの設定は無視されます。

  （注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

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

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]：このサブインターフェイス上のパケットにタグ付けするために使用される VLAN ID（1 ～ 4094）を入力します。
- [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数は、プラットフォームによって異なります。サブインターフェイスを作成後に、ID を変更することはできません。

ステップ 6 [IPv4 アドレス（IPv4 Address）]タブをクリックして、IPv4 アドレスを設定します。
[タイプ（Type）]フィールドから次のいずれかのオプションを選択します。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて、次のオプションを変更します。
  - [ルート メトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルト ルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトであるこのオプションを選択します。
- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワーク

を接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

（注） 既存のインターフェイスの場合、そのインターフェイスに対して DHCP サーバを設定していると、アドレスの変更機能は制限されます。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存在する必要があり、そのプールの一部にすることはできません。別のサブネットの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, （274 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）]タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカル アドレスを自動的に設定するには、[有効（Enabled）]を選択します。リンクローカル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

  （注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属すネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、Firepower Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）]を選択します。

- [スタティック アドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定, （104 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）]オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注） リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカル アドレスによりパケットがドロップされることがあります。

- [RA を抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。Firepower Threat Defense デバイス は、ネイバー デバイスがデフォルトのルータ アドレスを動的に学習できるように、ルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定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）詳細インターフェイス オプションの設定, （115 ページ）
詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 9 [保存（Save）]をクリックします。

詳細インターフェイス オプションの設定

詳細インターフェイス オプションには、ほとんどのネットワークに適しているデフォルト設定があります。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。

次の手順は、インターフェイスがすでに定義されていることを前提としています。これらの設定は、インターフェイスの初期編集時または作成時にも編集できます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックして、[インターフェイス（Interfaces）]サマリのリンクをクリックします。
インターフェイス リストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。

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 インターフェイスの管理のみを行うには、[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として設定する価値はあまりありません。常に管理専用の管理/診断インターフェイスの場合、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）を目的の値に変更します。

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 9000）。ネットワーク上にジャンボ フレームが多い場合は、高い値を設定します。

（注） ASA 5500-X シリーズ デバイスの MTU を 1500 より上の値にする場合、デバイスを再起動する必要があります。CLI にログインして、**reboot** コマンドを使用します。

ステップ 6 （物理インターフェイスのみ）速度とデュプレックスの設定を変更します。
デフォルトでは、インターフェイスがネットワークの反対側にあるインターフェイスと最適なデュプレックスと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または速度を強制することができます。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）]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）]の設定を変更します。

- [IPv6 アドレス設定での DHCP の有効化（Enable DHCP for IPv6 address configuration）] : IPv6 ルータ アドバタイズメント パケットに管理対象アドレス設定フラグを設定するかどうかを指定します。このフラグは、取得されるステートレス自動設定アドレス以外のアドレスを取得するために 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 以外のアドレス設定での DHCP の有効化（Enable DHCP for IPv6 non-address configuration）] : IPv6 ルータ アドバタイズメント パケットにその他のアドレス設定フラグを設定するかどうかを指定します。このフラグは、DNS サーバ アドレスなどの追加情報を DHCPv6 から取得するために 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 試行（DAD Attempts）] : インターフェイスが重複アドレス検出（DAD）を実行する頻度（0 ～ 600）を指定します。デフォルトは 1 です。ステートレス自動設定プロセスの間、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る場合、インターフェイス上での IPv6 パケットの処理は無効になります。重複アドレスがグローバルアドレスである場合、そのアドレスは使用されません。インターフェイスは、ネイバー要請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）処理を無効にするには、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

次の領域に、インターフェイスに関する一部の基本情報を表示できます。

- [モニタリング（Monitoring）] > [システム（System）]。[スループット（Throughput）]ダッシュボードには、システムを介して移動するトラフィックに関する情報が表示されます。すべてのインターフェイスに関する情報を表示できます。または、調査する特定のインターフェイスを選択できます。
- [モニタリング（Monitoring）] > [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には、インターフェイスで構成されるゾーンに基づいた統計情報が表示されます。詳細について、この情報を掘り下げることができます。
- [デバイス（Device）]。接続図にインターフェイスのステータスが表示されます。ポートの上にマウスを移動すると、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、起動している必要がある場合にダウンしているインターフェイスを特定できます。

CLI でのインターフェイスのモニタリング

デバイス CLI にログインして次のコマンドを使用すると、インターフェイス関連の動作および統計情報に関するより詳細な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および設定情報を表示します。このコマンドには多数のキーワードがあり、必要な情報を取得するために使用できます。使用可能なオプションを表示するには、「?」をキーワードとして使用します。
- **show ipv6 interface** は、インターフェイスに関する IPv6 設定情報を表示します。
- **show bridge-group** は、メンバー情報や 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介し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介して移動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、デバイスを介して移動する IPv6 トラフィックに関する統計情報を表示します。
- **show dhcpd** は、インターフェイスでの DHCP の使用状況、特にインターフェイスで設定されている DHCP サーバに関する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、システムに入力されるパケットの出力インターフェイスを決定します。ここでは、ルーティングの基本とデバイスでのルーティングの設定方法について説明します。

ルーティングの概要

ここでは、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のかを説明します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも 1 つの中間ノードがあります。ルーティングには、最適なルーティング パスの決定と、ネットワーク経由のパケットの転送という 2 つの基本的なアクティビティが含まれます。

NAT がルート選択に与える影響

Firepower Threat Defenseは、ルーティング テーブルおよび Network Address Translations（NAT）XLATE（変換）テーブルの両方を使用してルーティングを決定します。宛先 IP 変換トラフィック、つまり、変換されていない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とおりです。

1. 宛先 IP を変換する XLATE がすでに存在する場合は、パケットの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 を変換する XLATE が存在せず、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て 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 を変換する XLATE が存在せず、一致するスタティック変換も存在しない場合は、パケットの宛先IP変換は実行されません。システムは、ルートをルックアップして出力インターフェイスを選択することでこのパケットを処理し、次に発信元 IP 変換が（必要に応じて）実行されます。

通常のダイナミック発信 NAT では、最初の発信パケットがルート テーブルを使用してルーティングされた後、XLATE が作成されます。着信返送パケットは、既存の XLATE だけを使用して転送されます。スタティック NAT では、宛先変換された着信パケットは、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を選択した後、さらにルート ルックアップが実行され、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 ホップが検出されます。選択されたインターフェイスに明示的に属するルートがルーティング テーブルにない場合は、パケットがドロップされてレベル 6 の診断 syslog メッセージ 110001（ホストへのルートなし）が生成されます（別の出力インターフェイスに属する、指定の宛先ネットワークへの別のルートがあるかどうかにかかわらず）。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ると、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 テーブルおよびルートの選択

NAT XLATE およびルールによって外部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、指定ルートに相対的な優先順位を定める「アドミニストレーティブディスタンス」というメトリックが含まれています。パケットが複数のルートエントリと一致する場合、最短距離のルート エントリが使用されます。直接接続されたネットワーク（インターフェイス上で定義されたネットワーク）の距離は0のため、これが常に優先されます。スタティック ルートのデフォルトの距離は 1 ですが、1 ～ 254 の距離で作成できます。

特定の宛先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 のルート）よりも優先されます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティングテーブル内のエントリと一致しない場合、パケットはデフォルト ルートに指定されているインターフェイスを通して転送されます。デフォルト ルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

（注） ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

スタティック ルートの設定

システムのインターフェイスに直接接続されているネットワークに向かわないパケットの送信先をシステムに伝えるため、スタティック ルートを定義します。

少なくとも 1 つのスタティック ルート、ネットワーク 0.0.0.0/0 のデフォルト ルートが必要になります。このルートは、既存の NAT xlates（変換）またはスタティック NAT ルール、またはその他のスタティック ルートでは出力インターフェイスを判別できないパケットの送信先を定義します。

デフォルト ゲートウェイを使用してもすべてのネットワークに到達できない場合、他のスタティック ルートが必要になる可能性があります。たとえば、デフォルト ルートは通常、外部インターフェイスの上流に位置するルータです。デバイスに直接接続されていない追加の内部ネットワークがあり、それらにデフォルト ゲートウェイを介してアクセスできない場合、これらそれぞれの内部ネットワークに対してスタティック ルートが必要です。

システムのインターフェイスに直接接続されたネットワークのスタティック ルートを定義することはできません。システムは自動でこれらのルートを作成します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名し、[ルーティング（Routing）] の概要のリンクをクリックします。

ステップ 2 [ルーティングの選択（Select Routing）]ページで、次のいずれかを実行します。

- 新しいルートを追加するには、[+] > [スタティック ルートを追加（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ら、ルートのゴミ箱アイコンをクリックして削除します。

ステップ 3 ルート プロパティの設定

プロトコル

[IPv4]または [IPv6] アドレスのどちらのルートであるかを選択します。

ゲートウェイ

ゲートウェイの IP アドレスを特定するホスト ネットワーク オブジェクトを選択します。トラフィックはこのアドレスに送信されます。

インターフェイス

トラフィックの送信を行うインターフェイスを選択します。ゲートウェイ アドレスは、このインターフェイスを介してアクセス可能である必要があります。

メトリック

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

アドミニストレーティブ ディスタンスは、ルートを比較するために使用されるパラメータです。番号が低いほど、ルートに高い優先順位が与えられます。接続されたルート（デバイスのインターフェイスに直接接続されているネットワーク）は、スタティック ルートよりも常に優先されます。

ネットワーク

このルートのゲートウェイを使用する必要がある、宛先ネットワークまたはホストを特定するネットワーク オブジェクトを選択します。

デフォルト ルートを定義するには、事前定義された any-ipv4 または any-ipv6set ネットワーク オブジェクトを使用するか、または 0.0.0.0/0（IPv4）または ::/0（IPv6）ネットワークのオブジェクトを作成します。

ステップ 4 必要に応じて、[追加（Add）]または [保存（Save）] 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を実行するには、デバイス CLI にログインして次のコマンドを使用します。

- **show route** は、直接接続されたネットワークのルートを含め、データ インターフェイスのルーティング テーブルを表示します。

- **show ipv6 route** は、直接接続されたネットワークのルートを含め、データ インターフェイスの IPv6 ルーティング テーブルを表示します。
- **show network** は、管理ゲートウェイを含め、仮想管理インターフェイスの設定を表示します。仮想インターフェイスを介したルーティングは、データ インターフェイスを管理ゲートウェイに指定しなければ、データ インターフェイス ルーティング テーブルによって処理されません。
- **show network-static-routes** は、**configure network static-routes** コマンドを使用して仮想管理インターフェイス用に設定されたスタティック ルートを表示します。通常、ほとんどの場合、管理ゲートウェイは管理ルーティングに対して十分機能するため、スタティック ルートは存在しません。これらのルートは、データ インターフェイス上のトラフィックには使用できません。

第 II 部

セキュリティ ポリシー

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、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

接続に関連付けられているユーザを検出するためにアイデンティティ ポリシーを使用できます。ユーザを識別することで、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。

たとえば、侵入イベントのターゲットとされたホストを誰が所有し、誰が内部攻撃やポート スキャンを開始したかを確認できます。また、高帯域幅のユーザや、望ましくない Web サイトまたはアプリケーションにアクセスしているユーザを確認することもできます。

ユーザの検出は、分析用のデータを収集するだけではありません。ユーザ名またはユーザ グループの名前に基づいてアクセス ルールを書き込み、ユーザの権限に基づいて選択的にリソースへのアクセスを有効化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 セッション経由でログインしている場合は、サーバによって報告された最後のユーザがユーザであると見なされます。

アクティブ認証によるユーザ ID の確立

認証は、ユーザのアイデンティティを確認する動作です。

アクティブ認証を使用すると、HTTP トラフィック フローがユーザ ID のマッピングがないシステムの IP アドレスから送られてきたときに、ネットワークに設定されたディレクトリを使用して、トラフィック フローを開始したユーザを認証するかどうかを決定できます。ユーザが正常に認証された場合、IP アドレスは、認証されたユーザのアイデンティティがあると見なされます。

認証が失敗しても、ユーザのネットワーク アクセスは妨げられません。アクセス ルールは最終的に、これらのユーザにどのアクセスを提供するか決定します。

ユーザ数の制限

Firepower Device Manager は、ディレクトリ サーバから最大 2000 人のユーザに関する情報をダウンロードできます。

ディレクトリ サーバに 2000 人以上のユーザ アカウントが含まれる場合、アクセス ルールでユーザを選択するとき、またはユーザ ベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

2000 までの制限は、グループに関連付けられた名前に適用されます。グループに 2000 人以上のメンバーがいる場合、ダウンロードされた 2000 の名前のみをグループ メンバーシップと一致させることができます。

2000 人以上のユーザがいる場合、Firepower Device Manager ではなく Firepower Management Center（リモート マネージャ）の使用を検討してください。Firepower Management Center では、はるかに多くのユーザをサポートします。

サポートされるディレクトリ サーバ

アイデンティティ ポリシーとともに Windows Server 2008 および 2012 で Microsoft Active Directory（AD）を使用できます。

サーバの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行する場合、ディレクトリ サーバでユーザ グループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザ グループ制御を実行できません。
- ディレクトリ サーバは、次の表に示すフィールド名を使用して、システムがそのフィールドのサーバからユーザ メタデータを取得できるようにする必要があります。

メタデータ	Active Directory フィールド
LDAP 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 DN の決定

ディレクトリのプロパティを設定する際は、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。このベースは、ディレクトリ サーバで定義され、ネットワークごとに異なります。アイデンティティ ポリシーが動作するためには、正しいベースを入力する必要があります。ベースが誤っている場合、システムがユーザやグループ名を判別できないため、アイデンティティ ベースのポリシーが動作不能になります。

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問い合わせてください。

Active Directory の場合、ドメイン管理者として Active Directory サーバにログインし、コマンド プロンプトで **dsquery** のコマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べたい既知のユーザ名（一部または全部）を指定します。たとえば、次のコマンドでは、「John*」という部分名を使用して、「John」から始まるすべてのユーザの情報を返します。

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名（一部または全部）を指定します。たとえば、次のコマンドは、Employees グループ名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。

また、ADSI Edit プログラムを使用して、Active Directory 構造をブラウズすることもできます（[スタート（Start）]>[ファイル名を指定して実行（Run）]>[adsiedit.msc]）。ADSI Edit で組織ユニット（OU）、グループ、ユーザなど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できます。

ベースが正しいことを確認するには、次のように操作します。

1. ディレクトリ プロパティの [接続テスト（Test Connection）] ボタンをクリックして、接続を確認します。問題を解決し、ディレクトリ プロパティを保存します。
2. デバイスに対する変更をコミットします。
3. アクセス ルールを作成し、[ユーザ（Users）]タブを選択して、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。ディレクトリが含まれるレルム内のユーザおよびグループに入力が一致すると、自動コンプリートによる候補が表示されます。これらの候補がドロップダウン リストに表示された場合、システムがディレクトリを正常にクエリーできたことが分かります。候補が表示されず、入力した文字列は確実にユーザ名またはグループ名に含まれることが既知である場合には、対応する検索ベースを修正する必要があります。

不明なユーザの対処

アイデンティティ ポリシーのディレクトリ サーバを設定すると、システムはディレクトリ サーバからユーザおよびグループ メンバーシップ情報をダウンロードします。この情報は、24 時間ごとに夜中に更新されるか、またはディレクトリ設定を編集して保存するたびに（変更がなくても）更新されます。

アクティブな認証アイデンティティ ルールによって求められた認証に成功したにも関わらず、ユーザ名がダウンロードしたユーザ ID 情報の中に存在しない場合、不明なユーザとしてマークされます。ID 関連のダッシュボードにそのユーザの ID は表示されず、ユーザ一致グループ ルールにも検出されません。

ただし、不明なユーザに対するアクセス コントロール ルールが適用されます。たとえば、不明なユーザの接続をブロックすると、これらのユーザは、たとえ認証に成功（ディレクトリ サーバがユーザとパスワードが有効であると認識したことを意味する）してもブロックされます。

そのため、ユーザの追加や削除、グループ メンバーシップの変更などの変更をディレクトリ サーバに加えた場合、システムがディレクトリから更新情報をダウンロードするまで、これらの変更はポリシーの適用に反映されません。

毎日の深夜の更新まで待てない場合、ディレクトリ サーバ情報を編集することで強制的に更新を実行できます（[ポリシー（Policies）] > [アイデンティティ（Identity）] から [ディレクトリ サーバ（Directory Server）]ボタンをクリックする）。[保存（Save）]をクリックして変更を展開します。システムはただちに更新情報をダウンロードします。

（注） 新規または削除されたユーザ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）] に移動して [ルールを追加（Add Rule (+)）] ボタンをクリックし、[ユーザ（Users）]タブのユーザ リストを確認します。新規ユーザを検出できないか、または削除されたユーザが検出される場合、システムには古い情報があります。

アイデンティティ ポリシーの設定

アイデンティティ ポリシーを使用して、接続からユーザ アイデンティティ情報を収集できます。その後で、ダッシュボードにユーザ アイデンティティに基づく使用状況を表示し、ユーザまたはユーザ グループに基づくアクセス コントロールを設定できます。

次に、アイデンティティ ポリシーでユーザ アイデンティティを取得するために必要な要素を設定する方法の概要を示します。

手順

ステップ 1 [ポリシー（Policies）] > [アイデンティティ（Identity）] を選択します。
アイデンティティ ポリシーをまだ定義していない場合、ウィザードを開始してアイデンティティ ポリシーを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。

a) ディレクトリ サーバの設定, （132 ページ）
b) アクティブ認証キャプティブ ポータルの設定, （133 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。
アイデンティティ設定を設定すると、このページにすべてのルールが順番にリストアップされます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- アイデンティティ ポリシーを有効または無効にするには、[アイデンティティ ポリシー（Identity Policy）]トグルをクリックします。
- 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。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
- 不要になったルールを削除するには、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 ルールの作成と変更の詳細については、アイデンティティ ルールの設定, （135 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が許可されているユーザおよびユーザ グループに関する情報が含まれています。毎日、一日の最後の時間（UTC）にすべてのユーザとグループに関する更新情報がダウンロードされます。

ディレクトリ管理者と協力して、ディレクトリ サーバのプロパティの設定に必要な値を入手します。

（注） レルムを追加したら、設定を確認し、[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て接続をテストします。テストが失敗した場合は、すべてのフィールドを確認し、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 パスが存在す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 ルールまたはアイデンティティ ルールを設定していない場合は、[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（）

ステップ 3 ディレクトリ サーバに関する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 がサポートされている唯一のタイプであり、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適切な権限を持っているユーザの識別用のユーザ名とパスワード。たとえば、admin@ad.example.com などです。
- [ベース DN（Base DN）]：ユーザおよびグループの共通の親である、ユーザおよびグループ情報を検索、または問い合わせるためのディレクトリ ツリー。たとえば、dc=example,dc=com などです。ベース DN の検索についての詳細は、ディレクトリ ベース DN の決定, （129 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のある、完全修飾 Active Directory ドメイン名。たとえば、example.com などです。
- [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。サーバへ暗号化接続を使用している場合、IP アドレスではなく完全修飾ドメイン名を入力する必要があります。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合はポート 636 を使用します。
- [暗号化（Encryption）]：ユーザおよびグループ情報をダウンロードするために暗号化接続を使用するには、希望する方法、STARTTLS または LDAPSを選択します。デフォルトは [なし（None）]であり、ユーザおよびグループ情報はクリア テキストに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、ディレクトリ サーバでサポートされている最も強力な方式を使用します。ポート 389 を使用します。
  - LDAPSでは LDAP over SSL が必要です。ポート 636 を使用します。
- [SSL 証明書（SSL Certificate）]：暗号化方式を選択したら、CA 証明書をアップロードしてシステムとディレクトリ サーバ間の信頼されている接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用し、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 （ウィザードで）[次へ（Next）]をクリックするか、[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 ルールで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、認証を求めるプロンプトが表示されます。証明書をアップロードしないと、ユーザには自己署名証明書が提示されます。ブラウザがすでに信頼している証明書をアップロードしない場合、ユーザは証明書を承認する必要があります。

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

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

手順

ステップ 1 [ポリシー（Policies）] > [アイデンティティ（Identity）] を選択します。

ステップ 2 次のいずれかを実行します。

- [開始する（Get Started）]ウィザードを使用している場合、ディレクトリ サーバを設定した後、[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）] : アクティブ認証の間にユーザに表示する 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。証明書に貼り付けるか、[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、ユーザ認証時の自己署名証明書が表示されます。
- [証明書キー（Certificate Key）] : サーバ証明書のキー。キーに貼り付けるか、[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 ポータルのポート。デフォルトは 885（TCP）です。異なるポートを設定する場合、1025 ～ 65535 の範囲内と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に対してユーザ識別情報を収集する必要があるかどうかを定義します。一致するトラフィックのユーザ識別情報を取得しない場合は、「No Authentication」を設定します。

ルール設定に関係なく、アクティブ認証は HTTP トラフィックに対してのみ実行されることに注意してください。したがって、HTTP 以外のトラフィックをアクティブ認証から除外するルールを作成する必要はありません。すべての HTTP トラフィックに対してユーザ識別情報を取得する場合は、アクティブ認証ルールをすべての送信元および宛先に適用するだけで済みます。

（注） また、認証に失敗してもネットワークアクセスには影響しません。アイデンティティポリシーは、ユーザ識別情報のみを収集します。認証に失敗したユーザがネットワークにアクセスできないようにするには、アクセス ルールを使用する必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アイデンティティ（Identity）] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（  ）をクリックします。

ステップ 3 [順序（Order）]で、ルールの番号付きリストのどこにルールを挿入するかを選択します。ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

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

- [アクティブ（Active）] : ユーザを識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）]：ユーザ識別情報を取得しません。このトラフィックに、アイデンティティベースのアクセス ルールは適用されません。これらのユーザは、[認証不要（No Authentication Required）]とマークが付けられます。

ステップ 5 （アクティブ認証のみ）。ディレクトリ サーバでサポートする認証方法（[タイプ（Type）]）を選択します。

- [HTTP 基本（HTTP Basic）]：暗号化されていない HTTP 基本認証（BA）接続を使用して、ユーザを認証します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。これがデフォルトです。
- [NTLM]：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にのみ使用できます。Windows ドメインのログインを使って透過的に認証するよう、IE と Firefox ブラウザを設定することはできますが、ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします（透過的なユーザ認証のイネーブル化, （139 ページ）を参照してください）。
- [HTTP ネゴシエート（HTTP Negotiate）]：ユーザ エージェント（トラフィック フローを開始するためにユーザが使用しているアプリケーション）方式と Active Directory サーバ方式の間でデバイスがネゴシエーションできるようになります。ネゴシエーションの結果は、NTLM、ベーシックの順に、共通にサポートされ、使用されている最も強力な方式になります。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- [HTTP 応答ページ（HTTP Response Page）]：システムが提供する Web ページを使用して、ユーザに認証を求めるプロンプトを表示します。これは、HTTP 基本認証の 1 つの形式です。

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

ステップ 6 （アクティブ認証のみ）。アクティブ認証に失敗したユーザがゲスト ユーザとしてラベル付けされているかどうかを確認するには、[ゲストとしてフォールバックする（Fall Back as Guest）]>[オン/オフ（On/Off）] を選択します。
ユーザは、正常に認証する 3 つの機会が得られます。失敗した場合、このオプションの選択により、ユーザがどのようにマーク付けされるかが決まります。これらの値に基づき、アクセス ルールを書き込みできます。

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

ステップ 7 [送信元/宛先（Source/Destination）]タブで、トラフィック一致基準を定義します。
アクティブ認証は、HTTP トラフィックに対してのみ試されることに注意してください。したがって、HTTP 以外のトラフィックに対して「No Auth」ルールを設定する必要はなく、また HTTP 以外のトラフィックに対してアクティブ認証ルールを作成するポイントもありません。

アイデンティティ ルールの送信元/宛先基準は、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレス、または IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートを定義します。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、条件内の [+]ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New *Object*）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x]をクリックします。

次のトラフィック一致基準を設定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）]に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）]に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、内部ネットワークから発信されるすべてのトラフィックからユーザ識別情報を収集する場合、内部ゾーンを [送信元ゾーン（Source Zones）]として選択し、宛先ゾーンを空のままにします。

送信元ネットワーク、宛先ネットワーク

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

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）]を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）]を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。
- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限することができます。

  （注） 確実に最新の位置情報データを使用してトラフィックをフィルタ処理するため、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、これにポートを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）]を設定します。送信元ポートは TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル（Destination Ports/Protocols）]を設定します。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にすることができます。

ステップ 8 [OK]をクリックします。

透過的なユーザ認証のイネーブル化

アクティブ認証を有効にするためにアイデンティティ ポリシーを設定する場合、ユーザ ID を取得するために次の認証方式を使用できます。

HTTP Basic

HTTP 基本認証では、ユーザは常に自分のディレクトリ ユーザ名とパスワードを認証するように要求されます。パスワードはクリア テキストで送信されます。そのため、基本認証はセキュアな認証形式とは見なされません。

基本認証は、デフォルトの認証メカニズムです。

HTTP 応答ページ

これは、HTTP 基本認証の一種であり、ユーザがログイン ブラウザ ページに表示されます。

NTLM、HTTP ネゴシエート（Active Directory のための統合 Windows s認証）

統合 Windows 認証では、ユーザがドメインにログインしてワークステーションを使用するという事実が利用されます。ブラウザは、アクティブ認証中のFirepower Threat Defenseキャプティブ ポータルを含め、サーバへのアクセス時にこのドメイン ログインの使用を試みます。パスワードは送信されません。認証が成功すると、ユーザは透過的に認証されます。ユーザは、何らかの認証チャレンジが実行され、それが満たされたことを意識しません。

ブラウザがドメイン ログイン クレデンシャルを使用して認証要求を満足できない場合、ユーザは、ユーザ名とパスワードの入力を要求されますが、これは基本認証と同じユーザ エクスペリエンスとなります。したがって、統合 Windows 認証を設定した場合、同じドメイン内のネットワークまたはサーバにアクセスするときに、ユーザがクレデンシャルを入力する必要性を減らすことができます。

なお、HTTP ネゴシエートは、アクティブ ディレクトリ サーバとユーザ エージェントの両方がサポートする、最も強力な方式を選択することに注意してください。ネゴシエーションが認証方式として HTTP 基本認証を選択した場合、トランスペアレント認証は行われません。強度の順序は、NTLM、次に基本認証です。トランスペアレント認証を可能にするには、ネゴシエーションが NTLM を選択する必要があります。

透過的な認証をイネーブルにするには、統合 Windows 認証をサポートするようにクライアント ブラウザを設定する必要があります。以下に、統合 Windows 認証をサポートする、広く使用されている一部のブラウザに関して、一般的な要件と基本設定について説明します。ソフトウェア リリースごとに技術が変更される場合があるため、詳細情報についてはブラウザ（または他のユーザ エージェント）のヘルプを参照してください。

ヒント Chrome および Safari など、すべてのブラウザが統合 Windows 認証をサポートするとは限りません（これが書かれたときに使用可能なバージョンに基づく）。ユーザはユーザ名とパスワードの入力を要求されます。使用しているバージョンでサポートが使用可能かどうかを確認するには、ブラウザのマニュアルを参照してください。

トランスペアレント認証の要件

トランスペアレント認証を実装するには、ブラウザまたはユーザ エージェントを設定する必要があります。これは、個別に実行することも、そのための設定を作成し、ソフトウェア配布ツールを使用してその設定をクライアント ワークステーションにプッシュすることもできます。この作業をユーザが自分で実行する場合は、ネットワークで機能する具体的な設定パラメータを提供する必要があります。

ブラウザまたはユーザ エージェントに関係なく、次の一般的な設定を実装する必要があります。

- ユーザがネットワークへの接続に使用する Firepower Threat Defense インターフェイスを [信頼済みサイト（Trusted Sites）] リストに追加します。IP アドレスか、使用可能な場合は完全修飾ドメイン名（たとえば、inside.example.com）を使用できます。また、ワイルドカードまたはアドレスの一部を使用して、汎用化された信頼済みサイトを作成できます。たとえば、一般的には *.example.com または単に example.com を使用してすべて内部サイトを網羅し、ネットワーク内のすべてのサイトを信頼することができます（自身のドメイン名を使用）。インターフェイスの特定アドレスを追加する場合は、信頼済みサイトに複数のアドレスを追加して、ネットワークへのすべてのユーザ アクセス ポイントに対処することが必要な場合があります。
- 統合 Windows 認証は、プロキシ サーバ経由で機能しません。したがって、プロキシを使用しないか、またはプロキシを通過しないアドレスにFirepower Threat Defenseインターフェイスを追加する必要があります。プロキシを使用する必要がある場合、ユーザはNTLMを使用する場合でも認証を要求されます。

ヒント トランスペアレント認証の設定は必須ではありませんが、エンド ユーザにとって便利です。トランスペアレント認証を設定しなかった場合、ユーザはすべての認証方式に対するログイン チャレンジを提示されます。

トランスペアレント認証用の Internet Explorer の設定

NTLM トランスペアレント認証を有効にするよう Internet Explorer を設定するには、次の手順を実行します。

手順

ステップ 1 [ツール（Tools）] > [インターネット オプション（Internet Options）]を選択します。

ステップ 2 [セキュリティ（Security）]タブを選択し、[ローカル イントラネット（Local Intranet）] ゾーンを選択した後、次の手順を実行します。

a) [サイト（Sites）]ボタンをクリックして、信頼できるサイトのリストを開きます。

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 ネットワークを自動的に検出する（Automatically detect intranet network）]。このオプションを選択すると、他のすべてのオプションが無効になります。
- [プロキシをバイパスするすべてのサイトを含める（Include all sites that bypass the proxy）]。

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、次に信頼する URL を [サイトの追加（Add Site）] ボックスに貼り付けて [追加（Add）] をクリックします。
複数の URL が存在する場合は、このステップを繰り返します。ワイルドカードを使用して、http://*.example.com のように URL の一部を指定するか、または単に *.example.com と指定します。

このダイアログボックスを閉じて、[インターネット オプション（Internet Options）] ダイアログボックスに戻ります。

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で、[カスタム レベル（Custom Level）]をクリックして [セキュリティ設定（Security Settings）] ダイアログボックスを開きます。[ユーザ認証（User Authentication）] > [ログオン（Logon）] 設定を探して、[自動ログオンをイントラネット ゾーンのみで有効にする（Automatic logon only in Intranet zone）]を選択します。[OK]をクリックします。

ステップ 3 [インターネットオプション（Internet Options）] ダイアログボックスで [接続（Connections）]タブをクリックし、次に [LAN 設定（LAN Settings）] をクリックします。
[LAN でプロキシ サーバを使用する（Use a proxy server for your LAN）]が選択されている場合、Firepower Threat Defense インターフェイスがプロキシをバイパスすることを確認する必要があります。必要に応じて、次のいずれかを実行します。

- [ローカル アドレスにはプロキシ サーバを使用しない（Bypass proxy server for local addresses）] を選択します。
- [詳細（Advanced）]をクリックして、アドレスを [次で始まるアドレスにはプロキシ サーバを使用しない（Do not use proxy server for addresses beginning with）]ボックスに入力します。たとえば、*.example.com のようにワイルドカードを使用できます。

トランスペアレント認証用の Firefox の設定

NTLM トランスペアレント認証を有効にするよう Firefox を設定するには、次の手順を実行します。

手順

ステップ 1 [about:config]を開きます。フィルタ バーを使用して、修正する必要のある設定を検索します。

ステップ 2 NTLM をサポートするには、次の設定を修正します（network.automatic でフィルタリング）。

- [network.automatic-ntlm-auth.trusted-uris]：設定をダブルクリックし、URL を入力して [OK]をクリックします。カンマで区切って複数の URL を入力できます。プロトコルを含めるかどうかは任意です。次に例を示します。

  ```
  http://host.example.com, http://hostname, myhost.example.com
  ```

  URL の一部を使用することもできます。Firefox は、ランダムに部分文字列と照合するのではなく、文字列の末尾と照合します。したがって、ドメイン名のみを指定することにより、内部ネットワーク全体を包含することができます。次に例を示します。

  ```
  example.com
  ```

- [network.automatic-ntlm-auth.allow-proxies]：値が、デフォルトの [true]であることを確認します。値が [false] になっている場合は、ダブルクリックして変更します。

ステップ 3 HTTP プロキシ設定を確認します。これは、[ツール（Tools）] > [オプション（Options）] を選択し、次に [オプション（Options）] ダイアログボックスで [ネットワーク（Network）]タブをクリックすると見つかります。[接続（Connection）] グループで、[設定（Settings）]ボタンをクリックします。

- [プロキシなし（No Proxy）]が選択されている場合は、何も設定する必要がありません。
- [システムのプロキシ設定を使用（Use System Proxy Settings）]が選択されている場合、[about:config] 内の [network.proxy.no_proxies_on] プロパティを修正して、[network.automatic-ntlm-auth.trusted-uris] に含めた信頼済み URI を追加する必要があります。
- [手動プロキシ設定（Manual Proxy Configuration）]が選択されている場合、これらの信頼済み URI を包含するように [プロキシなし（No Proxy For）] リストを更新します。
- 他のオプションの 1 つが選択されている場合、これらの設定で使用するプロパティから同一の信頼済み URI が除外されていることを確認します。

アイデンティティ ポリシーのモニタリング

認証が必要なアイデンティティ ポリシーが正しく機能している場合、[モニタリング（Monitoring）] > [ユーザ（Users）] ダッシュボード、および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。

また、[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 サーバが正しく機能していることを確認します。ディレクトリ サーバの設定ダイアログ ボックスにある [テスト（Test）]ボタンを使用して、接続を確認します。

ディレクトリ サーバが機能していて使用可能な場合、認証が必要なアイデンティティ ルールのトラフィック一致条件がユーザを照合する方法で記述されていることを確認します。たとえば、ユーザ トラフィックがデバイスに入るインターフェイスが送信元ゾーンに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 トラフィックのみを照合するため、ユーザはそのタイプのトラフィックをデバイス経由で送信している必要があります。

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。これらのルールは、どのトラフィックにデバイスの通過を許可するかを制御し、侵入検知などのアドバンスド サービスをトラフィックに適用します。

アクセス コントロールの概要

次に、アクセス コントロール ポリシーを説明します。

アクセス コントロール ルールとデフォルト アクション

ネットワーク リソースへのアクセスを制御するには、アクセス ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。

アクセスの制御は次に基づいて行われます。

- 送信元と宛先の IP アドレス、プロトコル、ポート、インターフェイスなど従来のネットワーク特性（セキュリティ ゾーンの形式で）。
- 使用されているアプリケーション。アクセス コントロールは特定のアプリケーションに基づいて行うことも、アプリケーションのカテゴリ、特定の特性がタグ付けされたアプリケーション、アプリケーションのタイプ（クライアント、サーバ、Web）、またはアプリケーションのリスクやビジネスとの関連性の格付けを対象とするルールを作成できます。
- 汎用的な URL のカテゴリが含まれる Web 要求の宛先 URL。ターゲット サイトのパブリック レピュテーションに基づいて、カテゴリの一致を絞り込むことができます。

- 要求を作成したユーザ、またはユーザが所属するユーザ グループ。

ユーザが許可する暗号化トラフィックの場合、IPS インスペクションを適用して脅威をチェックし、攻撃だと思われるトラフィックをブロックすることができます。また、禁止されたファイルやマルウェアをチェックするためにファイル ポリシーも使用できます。

アクセス ルールに一致しないすべてのトラフィックは、アクセス コントロールの [デフォルト アクション（Default Action）]によって処理されます。デフォルトでトラフィックを許可する場合、トラフィックに IPS インスペクションを適用できます。ただし、デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。

アプリケーション フィルタリング

アクセスコントロールルールを使用すると、接続で使用されるアプリケーションに基づいてトラフィックをフィルタリングできます。このシステムはさまざまアプリケーションを認識できるため、すべての Web アプリケーションをブロックせずに 1 つの Web アプリケーションをブロックする方法を探す必要はありません。

人気のあるアプリケーションでは、アプリケーションのさまざまな要素にフィルタ処理を行えます。たとえば、Facebook をブロックせずに、Facebook Games をブロックするルールを作成できます。

一般的なアプリケーション特性に基づいて、リスクまたはビジネス関連性、タイプ、タグを選択することでアプリケーション グループ全体をブロックまたは許可するルールを作成できます。**ただし、アプリケーション フィルタでカテゴリを選択するときは、目的のアプリケーション以外を含まないように一致するアプリケーションのリストをよく確認してください。**可能なグループ処理の詳細については、アプリケーション基準, （157 ページ）を参照してください。

アプリケーションのフィルタリングについて特に注意すべき点については、アプリケーション制御の制限, （168 ページ）で言及されています。最も注意すべき制限は暗号化トラフィックについてです。

アプリケーションがHTTPS接続などの暗号化を使用する場合、システムがアプリケーションを特定できない可能性があります。アプリケーション フィルタのダイアログボックスを使用し、次のタグを選択することでアプリケーションに復号が必要かどうかを決定してから、アプリケーションのリストを確認します。

- [SSL プロトコル（SSL Protocol）]：SSL プロトコルとしてタグ付けされたトラフィックを解釈する必要はありません。システムはこのトラフィックを認識し、アクセス コントロール操作を適用できます。リストされたアプリケーションのアクセス コントロール ルールは、想定される接続に一致する必要があります。
- [復号されたトラフィック（Decrypted Traffic）]：最初にトラフィックを復号する場合のみ、システムがこのトラフィックを特定できます。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のアクセス コントロール ルールは機能しません。たとえば、この書き込み時に、Dropbox にこのタグが付けられているとします。この場合、Dropbox アプリケーションのアクセス ルールは Dropbox 接続に一致しません。

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できます。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリング ライセンスでは、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：任意のライセンスで、個々の URL および URL のグループを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。

ここでは、URL フィルタリングについてさらに詳しく説明します。

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 のカテゴリおよびレピュテーションに基づいて、Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、高リスク（レベル 1）からウェルノウン（レベル 5）の範囲です。

（注） イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。また、Cisco Collective Security Intelligence（CSI）との通信を有効にして、最新の脅威インテリジェンスを取得する必要もあります。

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によって、URL フィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、乱用薬物カテゴリの高リスク URL をブロックできます。

カテゴリ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より簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。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 をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザが新しいポリシーを更新したり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。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで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 サイトをブロックし、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をブログからマルウェアに再分類して、そのサイトをブロックすることができます。
- アクセス コントロール ルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、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から高リスクに変更してブロックすることができます。

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のグループを手動でフィルタリングすることで、カテゴリとレピュテーション ベースのURLの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できます。特殊なライセンスなしでこのタイプのURLフィルタリングを実行することができます。

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、カテゴリに適切なWebサイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で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。

特定のURLを手動でフィルタリングする場合、影響を受ける可能性のある他のトラフィックについて慎重に検討してください。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別するために、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。

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。部分文字列マッチングによりign.com自体だけでなくverisign.comもブロックされることになり、意図しない動作が生じる可能性があります。

HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムはSSLハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求されたURLを決定します。

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を検討します。しかし、HTTPS フィルタリングではサブジェクト共通名内のサブドメインを無視するため、HTTPS URL を手動でフィルタリングする場合はにサブドメインを含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

暗号化プロトコルによるトラフィックの制御

でURL フィルタリングを実行する場合、システムは暗号化プロトコル（HTTP と HTTPS）を無視します。これは、手動およびレピュテーション ベース両方の URL 条件で発生します。つまり、URL フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

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

HTTP または HTTPS トラフィックのみ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、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

Action: Allow
Application: HTTPS
URL: example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

Action: Block
Application: HTTP
URL: example.com

Web サイトのブロック時にユーザに表示される内容

URL フィルタリング ルールで Web サイトをブロックした場合、ユーザに表示される内容は、サイトが暗号化されているかどうかに基づいて異なります。

- HTTP 接続：タイムアウトまたはリセットされた接続の場合、通常のブラウザ ページの代わりにシステムのデフォルトのブロック応答ページが表示されます。このページには、故意に接続がブロックされたことが明確に示されます。
- HTTPS（暗号化）接続：システムのデフォルトのブロック応答ページは表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルト ページが表示されます。エラー メッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

さらに、Web サイトは、明示的な URL フィルタリング ルールではないその他のアクセス コントロール ルールまたはデフォルトのアクションによってブロックされている場合があります。たとえば、ネットワーク全体または地理位置情報をブロックしている場合、ネットワーク上またはそ

の地理的な位置にあるWebサイトもブロックされます。これらのルールによってブロックされたユーザには、以下の制限で説明するとおり、応答ページが表示されることもあれば、表示されないこともあります。

URLフィルタリングを実装している場合、サイトが意図的にブロックされているときに表示されることがある内容と、どのタイプのサイトをブロックしているかについてエンドユーザに説明することを検討してください。そうでないと、エンドユーザがブロックされた接続のトラブルシューティングにかなりの時間を費やしてしまう場合があります。

HTTP応答ページの制限

システムがWebトラフィックをブロックする場合に、常に、HTTP応答ページが表示されるわけではありません。

- Webトラフィックがプロモートされたアクセス コントロール ルール（単純なネットワーク条件のみの早期に適用されたブロッキング ルール）の結果としてブロックされている場合、システムは応答ページを表示しません。
- システムが要求されたURLを特定する前に、Webトラフィックがブロックされている場合、システムは応答ページを表示しません。
- アクセス コントロール ルールによってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。

侵入、ファイル、マルウェアのインスペクション

侵入ポリシーとファイル ポリシーは、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- 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制御とAMP for Firepowerの機能を管理します。

他のトラフィック処理はすべて、侵入、禁止されたファイル、およびマルウェアについて、ネットワーク トラフィックが調べられる前に実行されます。侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを[許可（allow）]する侵入ポリシーとファイル ポリシーをルールに設定できます。インスペクションは、[信頼（trust）]または[ブロック（block）]トラフィックに設定されているルールでは実施されません。また、アクセス コントロール ポリシーのデフォルト アクションが、[許可（allow）]の場合、侵入ポリシーは設定できますが、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、暗号化ペイロードの侵入およびファイル インスペクションは無効化されます。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。インスペクションは暗号化トラフィックのみで機能します。

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

アクセス コントロール ポリシーを設定する

ネットワーク リソースへのアクセスを制御するには、アクセス コントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。トラフィックに一致するルールがない場合、ページ下部に表示されるデフォルト アクションが適用されます。

アクセス コントロール ポリシーを設定するには、[ポリシー（Policies）] > [アクセス コントロール（Access Control）] を選択します。

アクセス コントロール表には、すべてのルールが順番に表示されます。各ルールで以下を実行します。

- 左側の列にあるルール番号の隣の > ボタンをクリックし、ルール図を開きます。この図は、ルールがトラフィックをどのように制御するかを視覚的に示します。ボタンを再度クリックして図を閉じます。
- ほとんどのセルはインライン編集が可能です。たとえば、アクションをクリックして別のものを選択したり、送信元ネットワーク オブジェクトをクリックして送信元の条件を追加または変更したりできます。
- 右側の列には、ルールのアクション ボタンが含まれます。セルにマウスを当てるとボタンが表示されます。ルールを編集（）したり削除（）したりできます。

次に、ポリシーの設定方法について説明します。

デフォルト アクションの設定

接続が特定のアクセス ルールに一致しない場合、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] を選択します。

ステップ 2 [デフォルト アクション（Default Action）]フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [信頼性（Trust）]：いかなる種類の追加インスペクションもなしでトラフィックを許可します。
- [許可（Allow）]：侵入ポリシーの対象となるトラフィックを許可します。
- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 4 アクションが [許可（Allow）]の場合、[侵入ポリシー（Intrusion Policy）] の下で [ポリシーの有効化（Enable Policy）] > [オン（On）] を選択し、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, （162 ページ）を参照してください。

ステップ 5 （オプション）デフォルト アクションのロギングを設定します。
デフォルト アクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベント ビューアに記載されるようにするには、トラフィックのロギングを必要があります。ロギングの設定, （164 ページ）を参照してください。

ステップ 6 [OK]をクリックします。

アクセス コントロール ルールの設定

アクセス コントロール ルールを使用して、ネットワーク リソースへのアクセスを制御します。アクセス コントロール ポリシーのルールは、上から下に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。

- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（  ）をクリックします。

ステップ 3 [順序（Order）]で、ルールの番号付きリストのどこにルールを挿入するかを選択します。
ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。
この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+ ._ -

ステップ 5 一致するトラフィックに適用するアクションを選択します。

- [信頼（Trust）]：どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可（Allow）]：ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。
- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/宛先（Source/Destination）]：トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレス、または IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポート。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。送信元/宛先基準，（154 ページ）を参照してください。
- [アプリケーション（Application）]：アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトはすべてのアプリケーションです。アプリケーション基準，（157 ページ）を参照してください。
- [URL]：Web リクエストの URL または URL カテゴリ。デフォルトはすべての URL です。URL 基準，（159 ページ）を参照してください。
- [ユーザ（Users）]：ユーザとユーザ グループ。アイデンティティ ポリシーは、ユーザとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。ユーザ基準，（160 ページ）を参照してください。

条件を変更するには、条件内の [+]ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New *Object*）] をクリック

します。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の[x]をクリックします。

条件をアクセス コントロール ルールに追加する場合は、次のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、特定のホストの 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またはアプリケーションフィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。
- 一部の機能では、適切なライセンスを有効にする必要があります。

ステップ 7 （オプション）[許可（Allow）]アクションを使用するポリシーの場合、暗号化されていないトラフィックについてさらにインスペクションを設定できます。次のいずれかのリンクをクリックします。

- [侵入ポリシー（Intrusion Policy）]：[侵入ポリシー（Intrusion Policy）]>[オン（On）]を選択し、トラフィックへの侵入と弱点をインスペクションのする IPS 侵入インスペクションのポリシーを選択します。侵入ポリシーの設定, （162 ページ）を参照してください。
- [ファイルポリシー（File Policy）]：マルウェアを含むファイルやブロックすべきファイルのトラフィックのインスペクションを実行するファイル ポリシーを選択します。ファイル ポリシーの設定, （162 ページ）を参照してください。

ステップ 8 （オプション）ルールのロギングを設定します。
デフォルトでは、ルールに一致するトラフィックに対して接続イベントは生成されませんが、ファイルポリシーを選択した場合、ファイルイベントはデフォルトで生成されます。この動作は変更できます。ダッシュボード データまたはイベント ビューアに含まれるポリシーに一致するトラフィックのロギングを有効にする必要があります。ロギングの設定, （164 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/宛先基準

アクセス ルールの送信元/宛先基準によって、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスや IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートが定義されます。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、その条件内の[+]ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK（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、[Create New *Object*（新規オブジェクトの作成）]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、それらの [x]をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。片方または両方の基準を定義できます。両方とも定義しないことも可能です。指定されていない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）]に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）]に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスを出入りする場所に基づいてルールを適用する場合は、この基準を使用します。たとえば、内部ホストに移動するすべてのトラフィックが IPS インスペクションを必ず受けるようにするには、[宛先ゾーン（Destination Zones）]として内部ゾーンを選択し、送信元ゾーンを空のままにします。ルールに IPS フィルタリングを実装するには、ルール アクションを [許可（Allow）]にして、ルールで侵入ポリシーを選択する必要があります。

送信元ネットワーク、宛先ネットワーク

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

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）]を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）]を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この基準を追加する場合、次のタブから選択します。

- ネットワーク（Network）：制御するトラフィックの送信元または宛先IPアドレスを定義するネットワーク オブジェクトまたはグループを選択します。
- 地理位置情報（Geolocation）：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地理的位置を選択します。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。ルールで地理的位置を直接選択する以外に、場所を定義するために作成した地理位置情報オブジェクトを選択することもできます。地理的位置を使用すると、そこで使用される可能性があるすべての IP アドレスを知らなくても、特定の国へのアクセスを簡単に制限できます。

（注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、ポートを含めることができます。ICMP では、コードとタイプを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）]を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート]（Destination Ports）/[宛先プロトコル]（Destination Protocols）] を設定します。宛先ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。ICMP およびその他の非 TCP/UDP 仕様は、宛先ポートでのみ許可されます。送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから送信されるトラフィックと特定の TCP/UDP ポートに向かうトラフィックの両方を照合するには、両方を設定します。送信元ポートと宛先ポートの両方を条件に追加する場合は、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、ポート TCP/80 からポート TCP/8080 へのトラフィックをターゲットにすることができます。

アプリケーション基準

アクセス ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネス関連性によってアプリケーションを定義するフィルタが規定されます。デフォルトは任意のアプリケーションです。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

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

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーション フィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタ リストを変更するには、条件内の [+]ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーション フィルタ オブジェクトを選択してから、ポップアップ表示されるダイアログボックスで[OK]をクリックします。いずれかのタブで [詳細フィルタ（Advanced Filte）]をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x]をクリックします。[フィルタとして保存（Save As Filter）]リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーション フィルタ オブジェクトとして保存します。

次の [詳細フィルタ（Advanced Filter）]基準を使用すると、ルールに一致するアプリケーションまたはフィルタを特定できます。これらはアプリケーション フィルタ オブジェクトで使用されるものと同じ要素です。

（注） 1つのフィルタ条件内での複数の選択はOR関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりすることができます。

リスク

アプリケーションが組織のセキュリティ ポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーション プロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル。
- [クライアント プロトコル（Client Protocol）]：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Web アプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も不可欠な機能を表す一般的な分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは [SSL プロトコル（SSL Protocol）]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）]タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

URL 基準

アクセス ルールの URL 基準は、Web 要求で使用される URL または要求された URL が属するカテゴリを定義します。カテゴリが一致する場合は、許可またはブロックするためのサイトの相対レピュテーションも指定できます。デフォルトでは、すべての URL が許可されます。

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成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ができます。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 および既存の URL に対する新たな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 をフィルタ処理します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と現れては消える可能性があります。

URL リストを変更するには、条件内の [+]ボタンをクリックし、次の手法のいずれかを使用して、目的のカテゴリまたは URL を選択します。ポリシーからカテゴリまたはオブジェクトを削除するには、対応する [x]をクリックします。

[URL] タブ

[+]をクリックし、URL オブジェクトまたはグループを選択して、[OK] をクリックします。必要なオブジェクトが存在しない場合は、[URL の新規作成（Create New URL）]をクリックします。

（注） 特定のサイトをターゲットにするように URL オブジェクトを設定する前に、手動URLフィルタリングに関する情報を注意深く読みます。URL マッチングが予期したとおりに動作せず、意図せずにサイトをブロックしてしまうことがよくあります。たとえば、明示的にゲームサイト ign.com をブロックしようとすると、verisign.com や “ign.” で終わる他のサイトもブロックされてしまいます。

[カテゴリ（Categories）] タブ

[+]をクリックし、目的のカテゴリを選択して、[OK] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべての URL にルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意（Any）]チェックボックスを選択解除し、[レピュテーション（Reputation）] スライダを使用してレピュテーション レベルを選択します。レピュテーション スライダの左側は許可されるサイトを、右側はブロックされるサイトを示しています。レピュテーションがどのように使用されるかは、ルール アクションによって異なります。

- ルールによって Web アクセスをブロックまたは監視する場合は、レピュテーション レベルを選択することで、そのレベルより深刻なすべてのレピュテーションも選択されます。たとえば疑わしいサイト（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。
- ルールが Web アクセスを許可する場合は、レピュテーション レベルを選択すると、そのレベルより深刻でないすべてのレピュテーションも選択されます。たとえば無害なサイト（Benign sites）（レベル 4）を許可する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。

ユーザ基準

アクセス ルールのユーザ基準は、IP 接続のユーザまたはユーザ グループを定義します。アクセス ルールにユーザまたはユーザ グループの基準を含めるには、アイデンティティ ポリシーと関連付けられたディレクトリ サーバを設定する必要があります。

アイデンティティ ポリシーは、特定の接続に関してユーザ アイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストの IP アドレスに識別されたユーザが関連付けられます。したがって、送信元 IP アドレスがユーザにマッピングされているトラフィックは、そのユーザからのものとみなされます。IP パケット自体にはユーザ アイデンティティ情報は

含まれていないため、このIPアドレスとユーザ間のマッピングが使用可能な中での最良近似となります。

1つのルールに最大50のユーザまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザを選択するより有意義です。たとえば、エンジニアリング グループに開発ネットワークへのアクセスを許可するルールを作成し、それに続くルールとして、そのネットワークへの他のすべてのアクセスを拒否するルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバのエンジニアリング グループに追加する必要があるだけです。

ユーザ リストを変更するには、条件内の [+]ボタンをクリックし、次の手法のいずれかを使用して、目的のユーザまたはユーザ グループを選択します。ポリシーからユーザまたはグループを削除するには、対応する [x]をクリックします。

- [ユーザおよびグループ（Users and Groups）]タブ：目的のユーザまたはユーザ グループを選択します。グループは、ディレクトリ サーバにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセス ルールを作成し、それをアクセス コントロール ポリシー内で親グループのルールの上に配置する必要があります。

  （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、全体で2000ユーザまでに制限されています。そのため、ディレクトリに2000を超えるユーザが存在する場合は、存在するすべてのユーザ名は表示されません。

- [特別なエンティティ（Special Entities）]：次から選択します。
  - [認証失敗（Failed Authentication）]：ユーザは認証を求められましたが、最大許容試行回数内に有効なユーザ名/パスワード ペアを入力できませんでした。認証の失敗は、それ自体ではユーザのネットワークへのアクセスは妨げられませんが、これらのユーザのネットワーク アクセスを制限するためのアクセス ルールを記述することができます。
  - [ゲスト（Guest）]：ゲスト ユーザは、これらのユーザをゲストと呼ぶようにアイデンティティ ルールが設定されている点を除き、認証失敗ユーザと同様です。ゲスト ユーザは認証を求められましたが、最大試行回数内に認証されることができませんでした。
  - [認証不要（No Authentication Required）]：ユーザの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザは認証を求められませんでした。
  - [不明（Unknown）]：IPアドレスのユーザ マッピングがなく、認証失敗の記録もありません。

侵入ポリシーの設定

シスコではFirepower Systemを使用して複数の侵入ポリシーを提供しています。これらのポリシーは、侵入ルールやプリプロセッサルールの状態や詳細設定を定める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では、次の侵入ポリシーのいずれかを選択して、トラフィックの侵入やエクスプロイトのインスペクションを実行できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。

侵入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低いものから高いものへとリストされます。

- [セキュリティよりも接続を重視（Connectivity over Security）]：このポリシーは、ネットワークインフラストラクチャのセキュリティよりも接続性（すべてのリソースにアクセスできること）が優先される組織のために作成されています。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。このポリシーは、侵入からの保護を適用する必要があるが、ネットワークのセキュリティにかなり自信がある場合に選択します。
- [セキュリティと接続のバランス型（Balanced Security and Connectivity）]：このポリシーは、全体的なネットワークパフォーマンスとネットワークインフラストラクチャのセキュリティのバランスを取るように設計されています。このポリシーは大部分のネットワークに適しています。このポリシーは、侵入防御を適用したい大部分の状況で選択できます。
- [接続よりもセキュリティを重視（Security over Connectivity）]：このポリシーは、ユーザの利便性よりもネットワークインフラストラクチャのセキュリティが優先される組織のために作成されています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。このポリシーは、セキュリティが特に重要であるか、トラフィックのリスクが高い場合に選択します。
- [最大検出（Maximum Detection）]：このポリシーは、接続よりもセキュリティを重視（Security over Connectivity）するポリシーよりもさらに、ネットワークインフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。このポリシーを選択する場合、正当なトラフィックが過剰にドロップされていないか慎重に評価してください。

ファイル ポリシーの設定

Advanced Malware Protection for Firepower（AMP for Firepower）を使用して悪意のあるソフトウェア、つまり、マルウェアを検出するファイル ポリシーを使用します。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

AMP for Firepower は、ネットワーク トラフィックで検出された潜在的なマルウェアの性質を取得し、ローカル マルウェア ファイル分析と事前分類の更新を取得するために AMP クラウドを使用します。AMP クラウドにアクセスし、マルウェア ルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドに問い合わせます。可能な性質を次に示します。

- マルウェア（Malware）：AMP クラウドはファイルをマルウェア クラウドとして分類しました。ファイル内のいずれかのファイルがマルウェアである場合、アーカイブ ファイル（たとえば zip ファイル）はマルウェアとしてマークされます。
- クリーン（Clean）：AMP クラウドはファイルをマルウェアが含まれないクリーンな状態であると分類しました。その中のすべてのファイルがクリーンであれば、アーカイブ ファイルはクリーンであるとマークされます。
- 不明（Unknown）：AMP クラウドがまだファイルの性質を指定していません。その中のすべてのファイルが不明であれば、アーカイブ ファイルは不明であるとマークされます。
- 利用不可（Unavailable）：システムは、ファイルの性質を判断するために AMP クラウドに問い合わせできませんでした。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。複数の「利用不可」イベントが連続して発生している場合、管理アドレスのインターネット接続が正常に機能していることを確認します。

使用可能なファイル ポリシー

次のいずれかのファイル ポリシーを選択できます。

- [なし（None）]は、送信したファイルでマルウェアの評価を行わず、特定のファイルをブロックしません。このオプションは、ファイル送信が信頼されている、またはファイル送信の可能性が低い（または不可能である）、あるいはアプリケーションを信頼している、または URL フィルタリングがネットワークを適切に保護しているルールに対して選択します。
- [マルウェアをすべてブロック（Block Malware All）]は、AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [クラウドをすべてルックアップ（Cloud Lookup All）]は、AMPクラウドに問い合わせてネットワークを通過するファイルの傾向を取得して記録したうえでその伝送を許可します。
- [オフライン ドキュメントとアップロードされた PDF をブロック、その他のマルウェアをブロック（Block Office Document and PDF Upload, Block Malware Others）]は、ユーザによる Microsoft Office のドキュメントと PDF のアップロードをブロックします。AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [オフライン ドキュメントのアップロードをブロック、その他のマルウェアをブロック（Block Office Documents Upload, Block Malware Others）]は、ユーザによる Microsoft Office のドキュメントのアップロードをブロックします。AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。

ロギングの設定

アクセス ルールのロギング設定は、接続イベントがルールに一致するトラフィックに対して発行されるかどうかを決定します。イベント ビューアでルールに関連するイベントを確認するには、ロギングを有効にする必要があります。また、一致するトラフィックがシステムをモニタするために使用できるさまざまなダッシュボードに反映されるようにするためにも、ロギングを有効にする必要があります。

組織のセキュリティ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）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイスを対象としているかどうかを検討します。

次のロギング オプションを設定できます。

ログ アクションの選択

次のいずれかのアクションを選択できます。

- [接続の開始時と終了時にログを記録する（Log at Beginning and End of Connection）]：接続の開始時と終了時にイベントを発行します。接続終了イベントには接続開始イベントに含まれるすべての情報と、接続中に拾うことができるすべての情報が含まれているため、許可しようとしているトラフィックではこのオプションを選択しないことをお勧めします。両方のイベントのロギングは、システム パフォーマンスに影響する可能性があります。ただし、これはブロックされているトラフィックに許可されている唯一のオプションです。
- [接続終了時にログを記録する（Log at End of Connection）]：接続の終了時に接続ログの記録を許可する場合は、このオプションを選択します。これは許可されている、または信頼されているトラフィックに推奨されます。
- [接続のロギングなし（No Logging at Connection）]：ルールのロギングを無効にするには、このオプションを選択します。これがデフォルトです。

（注） アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。侵入がブロックされた接続では、接続ログ内の接続のアクションは[ブロック（Block）]、理由は[侵入ブロック（Intrusion Block）]ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ファイル イベント

禁止されたファイルまたはマルウェア イベントのロギングを有効にするには、[ファイルのロギング（Log Files）]を選択します。このオプションを設定するには、ルールでファイル ポリシーを選択する必要があります。ルールにファイル ポリシーを選択している場合、このオプションはデフォルトで有効になっています。シスコ は、このオプションを有効のままにすることを推奨します。

システムが禁止されたファイルを検出すると、次のタイプのイベントの1つを自動的にロギングします。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

ファイルがブロックされた接続の場合、接続ログにおける接続のアクションは [ブロック（Block）]ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイル モニタ（FileMonitor）]（ファイル タイプまたはマルウェアが検出された）、あるいは [マルウェア ブロック（Malware Block）] または [ファイル ブロック（File Block）]（ファイルがブロックされた）です。

接続イベントの送信先

外部 syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslog サーバの新規作成（Create New Syslog Server）]をクリックして作成します（syslog サーバへのロギングを無効にするには、サーバ リストから [任意（Any）]を選択します）。

デバイスのイベント ストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化することができます。

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）]ダッシュボードのデータの大半は、アクセス コントロール ポリシーに直接関連しています。トラフィックのモニタリングおよびシステム ダッシュボード, （68 ページ）を参照してください。

- [モニタリング（Monitoring）] > [ポリシー（Policies）] には、ヒット数が最も多いアクセス コントロール ルールと関連の統計情報が表示されます。
- [ネットワークの概要（Network Overview）]、[宛先（Destinations）]、[入力ゾーン（Ingress Zones）]、および[出力ゾーン（Egress Zones）] ダッシュボードには、一般的な統計情報が表示されます。

- [Web カテゴリ（Web Categories）] および [宛先（Destinations）] ダッシュボードには、URL フィルタリングの結果が表示されます。[Web カテゴリ（Web Categories）] ダッシュボードに情報を表示するには、少なくとも 1 つの URL フィルタリング ポリシーが必要です。
- [アプリケーション（Applications）]ダッシュボードには、アプリケーション フィルタリングの結果が表示されます。
- [ユーザ（Users）]ダッシュボードには、ユーザベースの統計情報が表示されます。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）] ダッシュボードには、侵入ポリシーの統計情報が表示されます。これらのダッシュボードに情報を表示するには、少なくとも 1 つのアクセス 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 ログ（File Logs）] ダッシュボードには、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が表示されます。このダッシュボードに情報を表示するには、少なくとも 1 つのアクセス 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）] にも、接続のイベントとアクセス コントロール ルールに関連するデータが表示されます。

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 にログインして次のコマンドを使用すると、アクセス コントロール ポリシーと統計情報に関するより詳細な情報を取得することもできます。

- **show access-control-config** は、ルールごとのヒット数とともにアクセス コントロール ルールに関するサマリ情報を表示します。
- **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、主要なインスペクタである Snort インスペクション エンジンに関する情報を表示します。Snort は、アプリケーション フィルタリング、URL フィルタリング、侵入からの保護、およびファイルとマルウェアのフィルタリングを実装しています。
- **show conn** は、インターフェイスを介し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介して移動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、デバイスを介して移動する 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

次に、アクセス コントロール ポリシーの制限の一部を説明します。

アプリケーション制御の制限

アプリケーション識別の速度

システムは、次が実行されるまで、アプリケーション制御を実行できません。

- 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、
- 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行われる必要があります。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、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。

暗号化および復号トラフィックのアプリケーション制御

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、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。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションに `SSL Protocol` タグが付けられます。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。
- 復号トラフィック：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 `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 コントロールを実行している場合、システムは、アプリケーションが識別された接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるアプリケーション トラフィックの処理

アドバタイズメント トラフィックなどの Web サーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（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 のトラフィックを制御するには、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制御できるようになります。

ユーザまたはグループ制御の制限

Firepower Device Manager は、ディレクトリ サーバから最大 2000 人のユーザに関する情報をダウンロードできます。

ディレクトリ サーバに 2000 人以上のユーザ アカウントが含まれる場合、アクセス ルールでユーザを選択するとき、またはユーザ ベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

2000 までの制限は、グループに関連付けられた名前に適用されます。グループに 2000 人以上のメンバーがいる場合、ダウンロードされた 2000 の名前のみをグループ メンバーシップと一致させることができます。

2000 人以上のユーザがいる場合、Firepower Device Manager ではなく Firepower Management Center（リモート マネージャ）の使用を検討してください。Firepower Management Center では、はるかに多くのユーザをサポートします。

URL フィルタリングの制限

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。
- システムがセッションで HTTP または HTTPS アプリケーションを識別する
- システムが要求された URL を識別する（ClientHello メッセージまたはサーバ証明書からの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行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なルール アクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、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く、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

特定のURLを手動でフィルタリングする場合は、影響を受ける可能性のある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別するために、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が文字列の任意の部分に一致する場合、URL は一致するとみなされます。

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 フィルタリングを実行すると、システムは次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がない場合、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とブロックされます。

選択したデバイス モデルのメモリ制限

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、次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X および ASA5525-X。

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

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通りに適用されます。

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに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を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に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/変換解除することができます。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

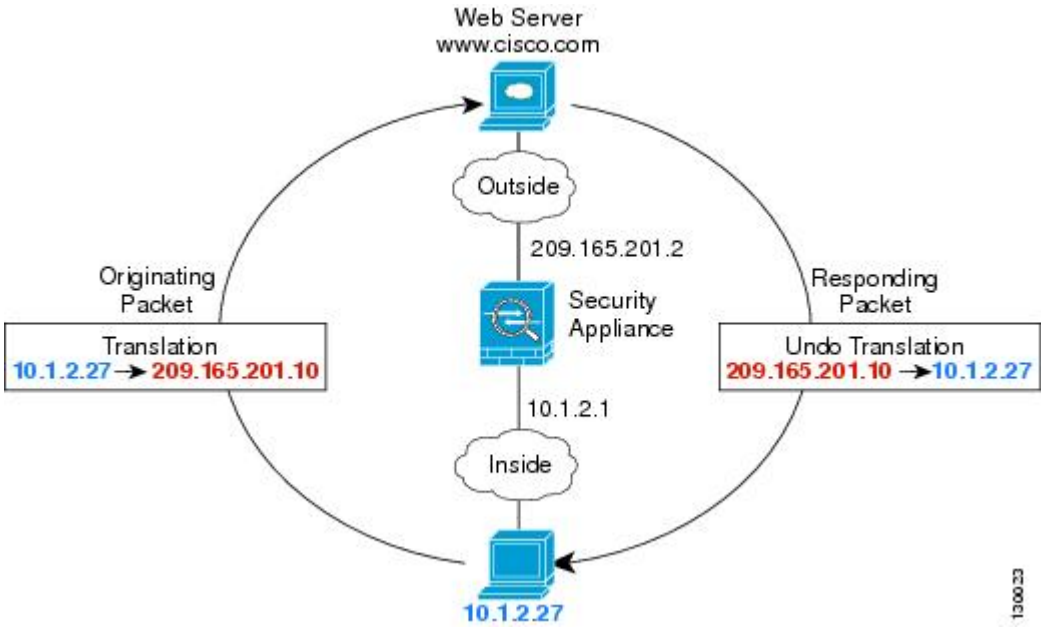
NAT は、次の方法を使用して実装できます。

- 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, （185 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。ダイナミック PAT, （191 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, （197 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, （208 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 *1*：*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アドレスと宛先アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないため、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、/手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

/手動 NAT

/手動 NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポート アドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

/自動 NATと /手動 NAT の比較

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際のアドレスの定義方法
  - 自動 NAT：NAT ルールは、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（実際の）アドレスとして機能します。

- /手動 NAT：実際のアドレスとマッピング アドレスの両方のネットワーク オブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト グループを使用できることは、/手動 NAT がよりスケーラブルであることを意味します。

- 送信元および宛先 NAT の実装方法
  - /自動 NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。つまり、送信元 IP アドレスに 1 つ、宛先 IP アドレスに 1 つと、2 つのルールが使用されることがあります。これらの 2 つのルールを相互に結び付けて、送信先と宛先の組み合わせに特定の変換を適用することはできません。
  - /手動 NAT：1 つのルールが送信元と宛先の両方を変換します。パケットは 1 つのルールにのみ一致し、それ以上のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、一致するパケットは、1 つの /手動 NAT ルールのみに一致します。送信元および宛先は相互に結び付けられるため、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。

- NAT ルールの順序
  - /自動 NAT：NAT テーブルで自動的に順序付けされます。
  - /手動 NAT：NAT テーブルで手動で順序付けされます（/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 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	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、/手動 NATルールはセクション 1 に追加されます。
セクション 2	/自動 NAT	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。 **1** スタティック ルール **2** ダイナミック ルール **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。** **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	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。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）

- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

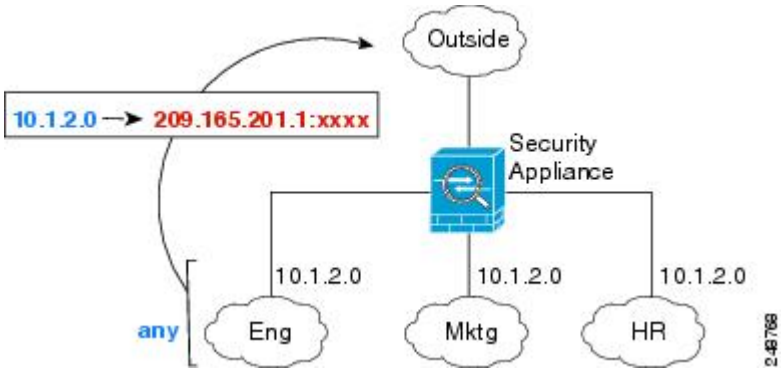
- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用できるように NAT ルールを設定することも、特定の実際のインターフェイスおよびマッピング インターフェイスを識別することもできます。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 アドレスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベート アドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバル プールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスには外部インターフェイスを指定します。

図 *2*：任意のインターフェイスの指定



NAT のルーティング設定

Firepower Threat Defenseデバイスは、変換された（マッピング）アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際の出力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 では、宛先インターフェイスを指定していてもルート ルックアップを使用するオプションがあります。

必要なルート設定のタイプは、次のトピックで説明するように、マッピング アドレスのタイプによって異なります。

マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、Firepower Threat Defense デバイスはプロキシ ARP を使用してマッピング アドレスの ARP 要求に応答し、マッピングアドレス宛てのトラフィックを代行受信します。この方法では、Firepower Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリー アドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるため、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

固有のネットワーク上のアドレス

宛先（マッピングされた）インターフェイス ネットワークで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを識別できます。アップストリーム ルータには、Firepower Threat Defense デバイスをポイントするマッピング アドレスのスタティック ルートが必要です。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効化され、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 を無効にできます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリーム ルータに適切なルートがあることを確認する必要があります。

アイデンティティ NAT の場合、通常はプロキシ ARP 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 を有効のままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（「任意」のアドレスと一致する）NAT ルールと一致します。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。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッド モードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 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。

（注） 初期設定時に作成された Inside_Outside_Rule は、外部 IPv6 アドレスへの接続を阻止します。IPv6 を使用するときに PAT ルールをバイパスするには、それを編集して、内部 IPv4 ネットワークのネットワーク オブジェクトを送信元アドレスとして選択します。

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ため、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（/手動 NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング ア

ドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。

- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するためにインスペクションが実行されます。

- ピンホールの作成：一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くため、ユーザはそれらを許可するアクセス コントロール ルールを作成する必要はありません。
- NAT の書き換え：プロトコルの一部としてのパケット データ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制：一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用するインスペクション対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていないインスペクション対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。

（注） NAT の書き換えは、リストされているポートでのみサポートされます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 *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。	あり
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	なし
ESMTP	TCP/25	NAT64 なし。	なし
FTP	TCP/21	制限なし。	あり
H.323 H.225（コールシグナリング） H.323 RAS	TCP/1720 UDP/1718 RAS の場合、 UDP/1718 ～ 1719	NAT64 なし。	あり
ICMP ICMP エラー	ICMP （デバイス インターフェイスに送信される ICMP トラフィックのインスペクションは実行されません。）	制限なし。	なし
IP オプション	RSVP	NAT64 なし。	なし
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	NAT64 なし。	なし
RSH	TCP/514	PAT なし。 NAT64 なし。	あり
RTSP	TCP/554 （HTTP クローキングは処理しません。）	NAT64 なし。	あり
SIP	TCP/5060 UDP/5060	拡張 PAT なし。 NAT64 または NAT46 なし。	あり
Skinny（SCCP）	TCP/2000	NAT64、NAT46、または NAT66 なし。	あり
SQL*Net （バージョン 1、2）	TCP/1521	NAT64 なし。	あり

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
Sun RPC	UDP/111	NAT64 なし。	あり
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	あり
XDMCP	UDP/177	NAT64 なし。	あり

NAT のその他のガイドライン

- （/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。
- （/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て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 設定を変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT 設定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確保できます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを含めることはできません。オブジェクト グループには、1 つのタイプのアドレスのみを含める必要があります。
- （/手動NATのみ）NATルールで送信元アドレスとして **any** を使用する場合、"any" トラフィックの定義（IPv4 と IPv6）はルールによって異なります。Firepower Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firepower Threat Defense デバイスが、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 インターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。

- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。
  - マッピング インターフェイスの IP アドレス。ルールに "any" インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合は、インターフェイス アドレスの代わりにインターフェイス名を指定します。
  - フェールオーバー インターフェイスの IP アドレス。
- 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 アドレス変換は非常に複雑な場合があります。変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。次の手順では、基本的なアプローチを示します。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 必要なルールを決定します。
ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールを作成できます。概要については、「NAT タイプ, （173 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 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, （174 ページ）」を参照してください。

ステップ 4 次のセクションで説明するルールを作成します。

- ダイナミック NAT, （185 ページ）
- ダイナミック PAT, （191 ページ）
- スタティック NAT, （197 ページ）

- アイデンティティ NAT, （208 ページ）

ステップ 5 NAT ポリシーとルールを管理します。
ポリシーとそのルールを管理するには、次のことを行います。

- ルールを編集するには、ルールの [編集（edit）] アイコン（）をクリックします。
- ルールを削除するには、ルールの [削除（delete）] アイコン（）をクリックします。

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

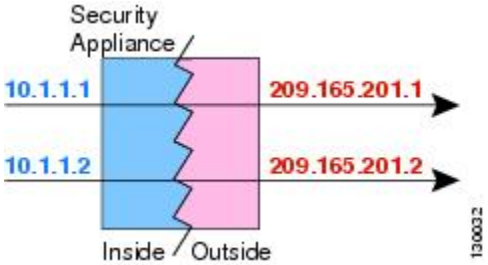
ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス ルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

（注） 変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

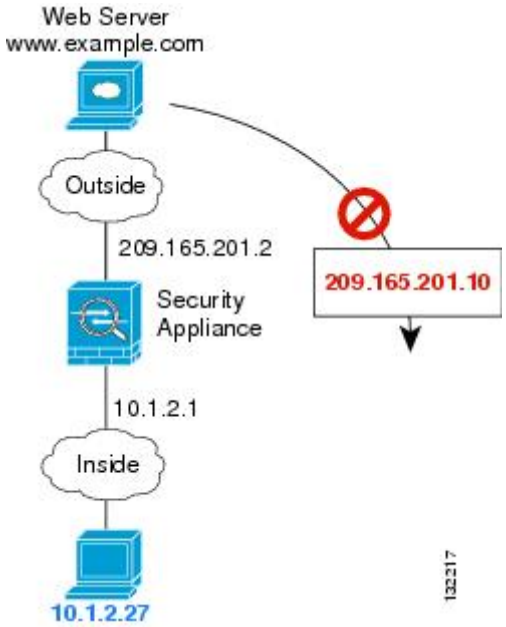
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 *3*：ダイナミック *NAT*



次の図に、マッピングアドレスへの接続開始を試みているリモートホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 *4*：マッピング アドレスへの接続開始を試みているリモート ホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  PAT では、1 つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールを使用して、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

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。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たしている必要があります。

- [元のアドレス（Original Address）]：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、ホストやサブネットを指定できます。
- [変換済みアドレス（Translated Address）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、そ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、そのルールのゴミ箱アイコンをクリックします）。

ステップ 3 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [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）]：[動的（Dynamic）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original Address）]：変換しているアドレスを含むネットワーク オブジェクト。

- [変換済みアドレス（Translated Address）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックして、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答,（255 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））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 6 [OK]をクリックします。

ダイナミック手動 NAT の設定

自動 NAT がお客様のニーズを満たしていない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

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。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけが含まれている必要があります。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件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を指定でき、ホストや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、この手順をスキップして、ルールで [すべて（Any）]を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス（Original Destination Address）]と [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトも作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクト マネージャで、[元の宛先ポート（Original Destination Port）]と [変換済み宛先ポート（Translated Destination Port）]に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、そ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、そのルールのゴミ箱アイコンをクリックします）。

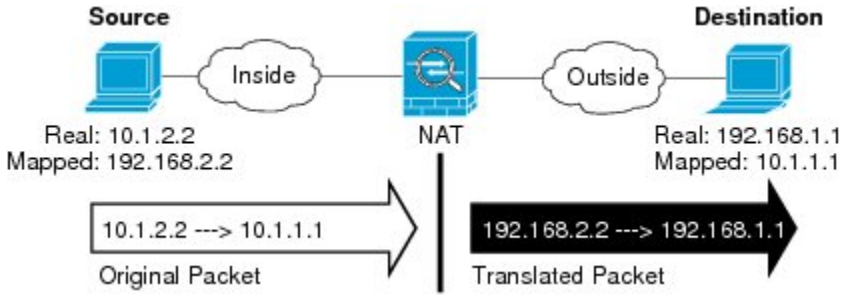
ステップ 3 基本ルールのオプションを設定します。

- [タイトル（Title）] : ルールの名前を入力します。
- [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）] : ルールを追加する場所を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）] : [動的（Dynamic）]を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）] : この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。
元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス（Original Source Address）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（任意）。宛先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、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。
- [変換済み宛先アドレス（Translated Destination Address）]：（任意）。変換済みパケットで使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）]のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。
ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）]フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（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て、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答,（255 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））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 9 [OK]をクリックします。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

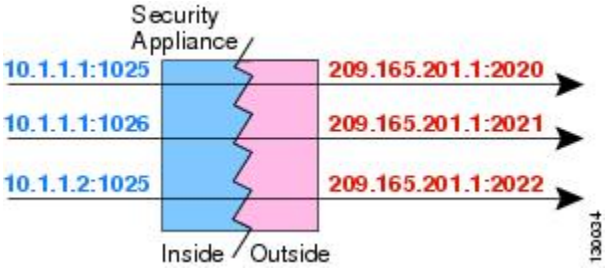
ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピング アドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 *5*：ダイナミック *PAT*



変換が継続している間、アクセスルールで許可されていれば、宛先ネットワーク上のリモートホストは変換済みホストへの接続を開始できます。実際のポートアドレスおよびマッピングポートアドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、Firepower Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用することもできます。ただし、インターフェイス PAT をインターフェイスの IPv6 アドレスのために使用することはできません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、インスペクション対象プロトコルに対する NAT サポート，（181 ページ） を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

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。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たしている必要があります。

- [元のアドレス（Original Address）]：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、ホストやサブネットを指定できます。
- [変換済みアドレス（Translated Address）]：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
  - [単一の PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、そ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、そのルールのゴミ箱アイコンをクリックします）。

ステップ 3 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [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）]：[動的（Dynamic）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original Address）]：変換しているアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスを選択することもできます。。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のアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックして、目的のオプションを選択します。

- [インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT（Destination Interface））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。インターフェイス PAT を変換済みアドレスとしてすでに設定している場合、このオプションは選択できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 6 [OK]をクリックします。

ダイナミック手動 PAT の設定

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

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。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけが含まれている必要があります。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件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を指定でき、ホストや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、この手順をスキップして、ルールで [すべて（Any）]を指定します。
- [変換済み送信元アドレス（Translated Source Address）：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
  - [単一の PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス（Original Destination Address）]と [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトも作成できます。

ダイナミック PAT の場合、宛先でポート変換を実行することもできます。オブジェクト マネージャで、[元の宛先ポート（Original Destination Port）]と [変換済み宛先ポート（Translated Destination Port）]に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、そ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、そのルールのゴミ箱アイコンをクリックします）。

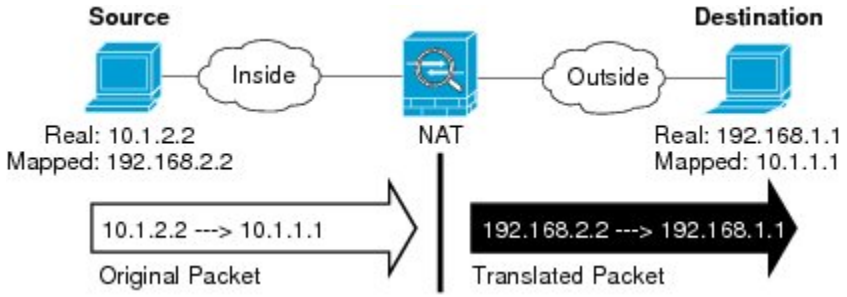
ステップ 3 基本ルールのオプションを設定します。

- [タイトル（Title）] : ルールの名前を入力します。
- [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）] : ルールを追加する場所を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）] : [動的（Dynamic）]を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）] : この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。
元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス（Original Source Address）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（任意）。宛先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、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスを選択することもできます。。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のアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- [変換済み宛先アドレス（Translated Destination Address）]：（任意）。変換済みパケットで使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（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）。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。
ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）]フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空白のままに

する必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（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て、目的のオプションを選択します。

- [インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT（Destination Interface））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。インターフェイス PAT を変換済みアドレスとしてすでに設定している場合、このオプションは選択できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 9 [OK]をクリックします。

スタティック NAT

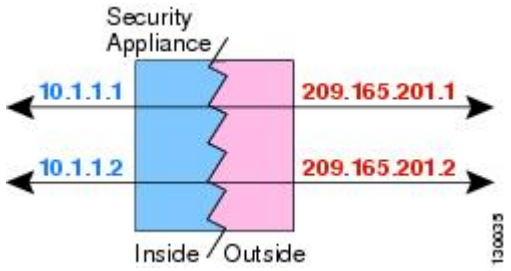
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じであるため、スタティック NAT では、双方向の接続（ホストへの接続とホストから接続の両方）を開始できます（接続を許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブであるため、実際のホストとリモート ホストの両方が接続を開始できます。

図 *6*：スタティック *NAT*



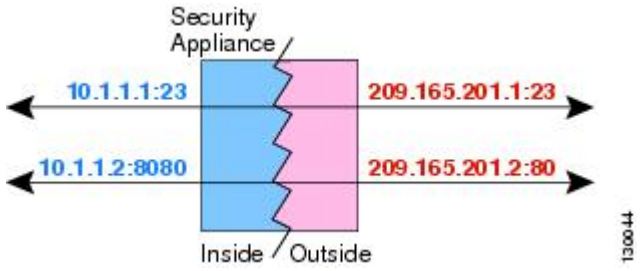
ポート変換を設定したスタティック *NAT*

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 *7*：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

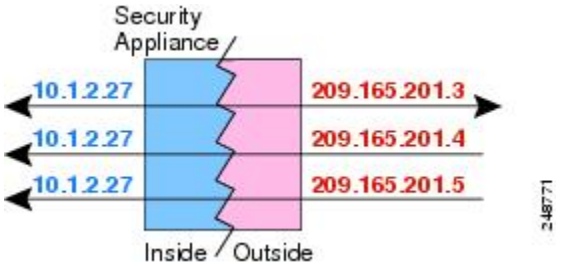
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

一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。

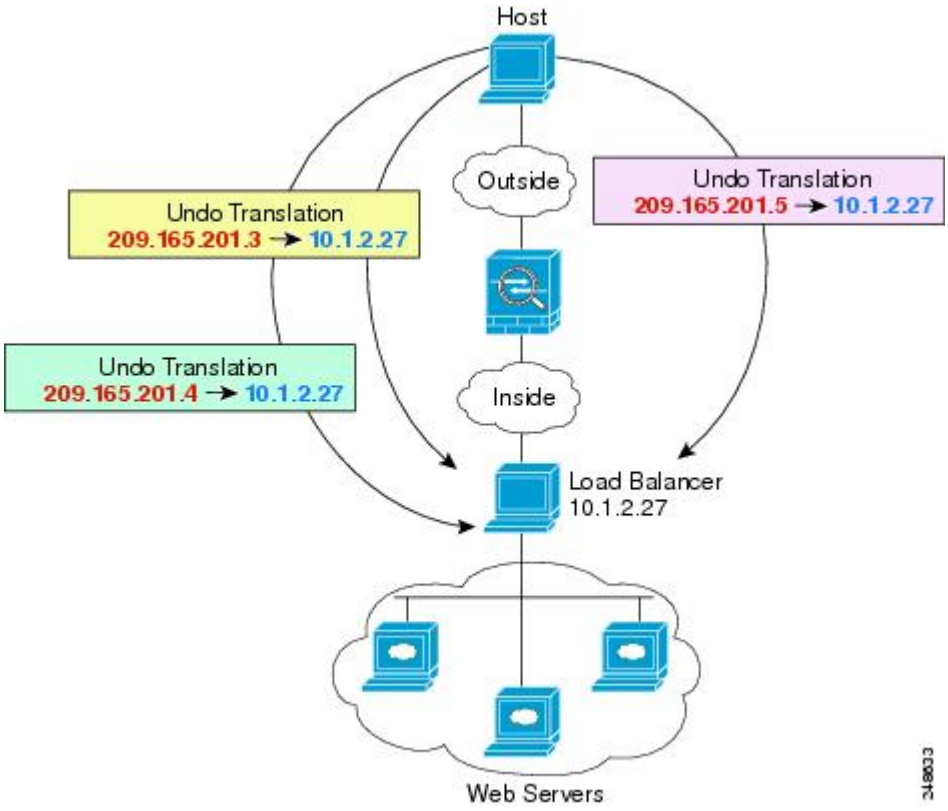
次の図に、一般的な一対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *8*：一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 *9*：一対多のスタティック *NAT* の例



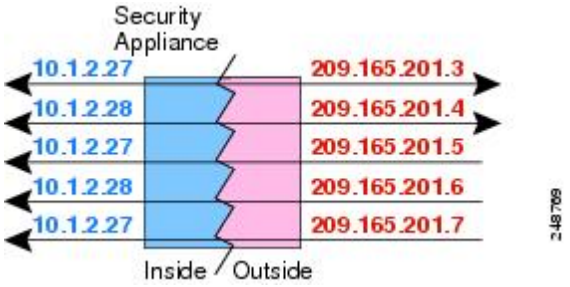
他のマッピング シナリオ（非推奨）

NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は 1 対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して 1 対多の設定を作成することをお勧めします。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次のマッピング アドレスが最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1 対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 *10*：少対多のスタティック *NAT*



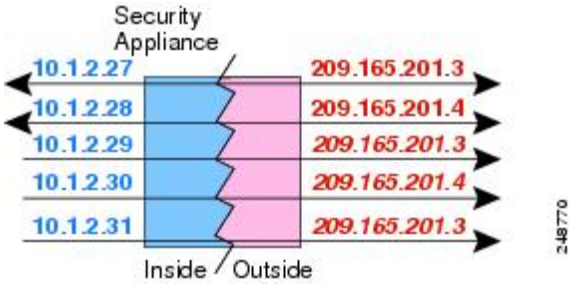
多対少または多対 1 の設定では、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピング プールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターン トラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注）

多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5 つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *11*：多対少のスタティック *NAT*



このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

スタティック自動 NAT の設定

スタティック 自動 NAT ルールを使用して、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

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 ルールを定義しながら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）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホストまたはサブネットも可能です。
- [変換済みアドレス（Translated Address）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（destination interface）]：宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
  - [アドレス（Address）]：ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。

- [タイプ（Type）]：[スタティック（Static）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original Address）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）。宛先のアドレスのインターフェイスを使用するには、[インターフェイス（Interface）]を選択します。また、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 にインターフェイス PAT は使用できません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- （オプション）[元のポート（Original Port）]、[Translated Port（変換済みポート）]：TCP または UDP ポートを変換する必要がある場合、元のポートと変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコル用でなければなりません。そのオブジェクトがまだ存在しない場合、[新規オブジェクトの作成（Create New Object）]をクリックします。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、希望する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 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答, （255 ページ）を参照してください。 ポート変換している場合、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 ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ 6 [OK]をクリックします。

スタティック手動 NAT の設定

自動 NAT がニーズを満たさない場合、スタティック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

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 ルールを定義しながらオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [送信元アドレス（Original Address）]：これはネットワーク オブジェクトまたはグループで、ホストまたはサブネットを含むことができます。すべての元のトラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）]を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（destination interface）]：宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
  - [アドレス（Address）]：ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス（Original Destination Address）]および [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。Object Managerでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

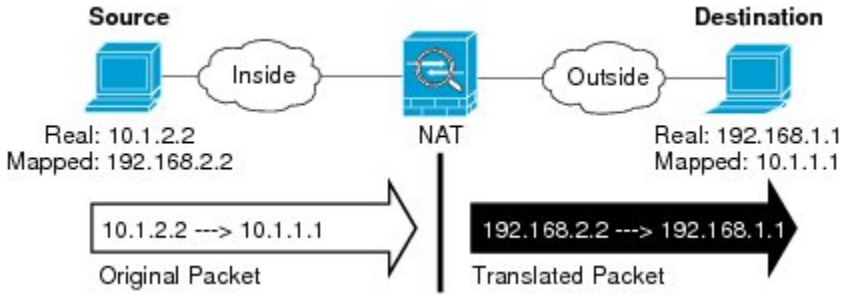
ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）] ：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）] : [手動 NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）] : ルールを追加する場所を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）] : [スタティック（Static）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義すると、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）] : この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。
元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス（Original Source Address）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（任意）。宛先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、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換されたパケット アドレス（IPv4 または IPv6）、すなわちそれが宛先インターフェイス ネットワーク上に現れるときのパケット アドレスを識別します。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）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）。宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の

宛先（Original Destination）]を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換された送信元ポート（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）]、[変換された宛先ポート（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、希望する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 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答, （255 ページ）を参照してください。 ポート変換している場合、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 ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

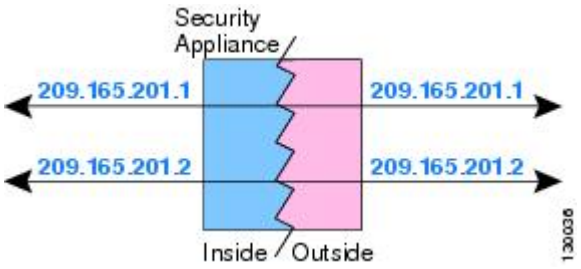
ステップ 9 [OK]をクリックします。

アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適するものの、1 つのネットワークを NAT から除外するという広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 *12*：アイデンティティ *NAT*



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

スタティック アイデンティティ自動 NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

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。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たしている必要があります。

- [元のアドレス（Original Address）]：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、ホストやサブネットを指定できます。
- [変換済みアドレス（Translated Address）]：元の送信元オブジェクトとコンテンツが全く同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、そ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、そのルールのゴミ箱アイコンをクリックします）。

ステップ 3 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [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）]：[静的（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）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original Address）]：変換しているアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

アイデンティティ NAT には、[元のポート（Original Port）]オプションと [変換済みポート（Translated Port）] オプションを設定しないでください。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックして、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルート ルックアップを実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択している場合に、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わ

りに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 6 [OK]をクリックします。

アイデンティティ手動 NAT の設定

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

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。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけが含まれている必要があります。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件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を指定でき、ホストや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、この手順をスキップして、ルールで [すべて（Any）]を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス（Original Destination Address）]と [変換済み宛先アドレス（Translated Destination Address）]のネットワーク オブジェクトも作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、ルールにインターフェイスを指定できます。

送信元、宛先、または両方でポート変換を実行することもできます。オブジェクト マネージャで、元のポートと変換済みポートで使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT には同じオブジェクトを使用できます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、そ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、そのルールのゴミ箱アイコンをクリックします）。

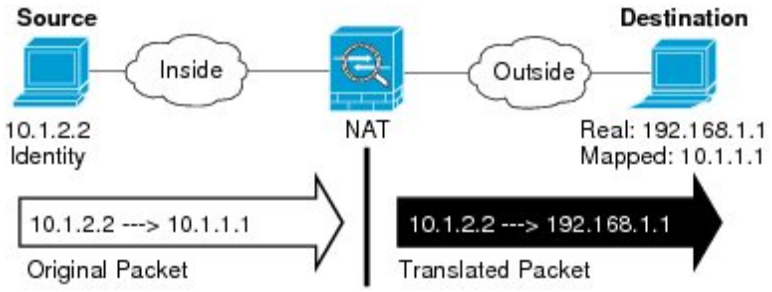
ステップ 3 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [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）]：ルールを追加する場所を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）]：[静的（Static）]を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。
元のパケットと変換済みパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



- [元の送信元アドレス（Original Source Address）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（任意）。宛先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、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

  [インターフェイス（Interface）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）]は選択不可）をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。
- [変換済み宛先アドレス（Translated Destination Address）]：（任意）。変換済みパケットで使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）]のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。ポート変換を設定したスタティック NAT を設定している場合、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て、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルート ルックアップを実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択している場合に、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わ

りに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 9 [OK]をクリックします。

Firepower Threat Defense の NAT ルールのプロパティ

ネットワークアドレス変換（NAT）ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、NAT ルールを使用してプライベートアドレスをパブリックにルーティングできるアドレスに変換します。1つのアドレスから別のアドレスに変換するか、ポートアドレス変換（PAT）を使用して多数のアドレスを 1 つに変換し、ポート番号を使用して送信元アドレスを識別することができます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

役職（Title）

ルールの名前を入力します。名前にスペースを含めることはできません。

ルールの作成

変換ルールを [自動 NAT（Auto NAT）]にするか、[手動 NAT（Manual NAT）]にするか。自動 NAT は手動 NAT よりシンプルですが、手動 NAT を使用すると、宛先アドレスに基づいて送信元アドレスの個別の変換を作成できます。

ステータス（Status）

ルールをアクティブにするか無効にするか。

配置（Placement）（手動NAT のみ）

ルールを追加する場所を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。

タイプ（Type）

変換ルールを [ダイナミック（Dynamic）]にするか、[スタティック（Static）]にするか。ダイナミック変換では、アドレス プールからマッピング アドレスが自動的に選択されるか、または、PAT の実装時にはアドレス/ポートの組み合わせが自動的に選択されます。マッピングアドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

次に、残りの NAT ルール プロパティを説明します。

自動 NAT のパケット変換プロパティ

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスと変換済みマッピング アドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

送信元インターフェイス（SourceInterface）、宛先インターフェイス（Destination Interface）

このNATルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

元のアドレス（OriginalAddress）（常に必須）

変換している送信元アドレスを含むネットワーク オブジェクト。グループではなくネットワーク オブジェクトにする必要があり、ホストまたはサブネットを含めることができます。

変換済みアドレス（TranslatedAddress）（通常は必須）

変換先のマッピング アドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- ダイナミックNAT（Dynamic NAT）：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。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）：次のいずれかになります。
  - （インターフェイス PAT）宛先インターフェイスの IPv4 アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。IPv6 にインターフェイス PAT を使用することはできません。
  - 宛先インターフェイス アドレス以外の単一アドレスを使用するには、この目的のために作成したホスト ネットワーク オブジェクトを選択します。
- スタティックNAT（Static NAT）：次のいずれかになります。
  - アドレスのセット 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、ホストまたはサブネットを含めることができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイスNAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。これによって、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/ポートは、インターフェイスのアドレスおよび同一ポート番号に変換されます。IPv6 にインターフェイス PAT を使用することはできません。
- アイデンティティNAT（Identity NAT）：元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

元のポート（OriginalPort）、変換済みポート（Translated Port）（スタティック NAT のみ）

TCP または UDP ポートを変換する必要がある場合、元のポートおよび変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコル向けにする必要があります。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

手動 NAT のパケット変換プロパティ

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスと変換済みマッピング アドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

送信元インターフェイス（SourceInterface）、宛先インターフェイス（Destination Interface）

このNATルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

元の送信元アドレス（Original Source Address）（常に必須）

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることが可能で、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールに[すべて（Any）]を指定します。

変換済み送信元アドレス（Translated Source Address）（通常は必須）

変換先のマッピング アドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- ダイナミックNAT（Dynamic NAT）：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。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）：次のいずれかになります。
  - （インターフェイス PAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。IPv6 にインターフェイス PAT を使用することはできません。
  - 宛先インターフェイス アドレス以外の単一アドレスを使用するには、この目的のために作成したホスト ネットワーク オブジェクトを選択します。
- スタティックNAT（Static NAT）：次のいずれかになります。
  - アドレスのセット 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 IP アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。これによって、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/ポートは、インターフェイスのアドレスおよび同一ポート番号に変換されます。IPv6 にインターフェイス PAT を使用することはできません。
- アイデンティティNAT（Identity NAT）：元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

元の宛先アドレス

宛先アドレスを含むネットワーク オブジェクト。これを空白のままにすると、送信元アドレスの変換が宛先に関係なく適用されます。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。

[インターフェイス（Interface）]を選択し、送信元インターフェイスを元の宛先のベースにすることができます（[すべて（Any）] をベースにすることはできません）。このオプションを使用するには、変換済み宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

変換済み宛先アドレス

変換済みパケットで使用される宛先アドレスが含まれるネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] 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することによってアイデンティティ NAT（変換されていない NAT）を設定できます。

元の送信元ポート（Original Source Port）、変換済み送信ポート（Translated Source Port）、元の宛先ポート（Original Destination Port）、変換済み宛先ポート（Translated Destination Port）

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポート オブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上することができます。サービスを設定するときは、次のルールに注意してください。

- （ダイナミック NAT または PAT）[元の送信元ポート（Original Source Port）]および [変換済み送信元ポート（Translated Source Port）]では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（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。

詳細 NAT プロパティ

NAT を設定するとき、[詳細（Advanced）]オプションで特別なサービスを提供するプロパティを設定できます。これらすべてのプロパティはオプションであり、サービスを必要としている場合のみ設定します。

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答, （255 ページ）を参照してください。このオプションは、スタティック NAT ルールでポート変換を行っているときは利用できません。

[インターフェイス PAT（宛先インターフェイス）へのフォールスルー（Fallthrough to Interface PAT (Destination Interface)）]（ダイナミック NAT のみ）

その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。IPv6 ネットワークでは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 なし（スタティック NATのみ）

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

宛先インターフェイスでルート ルックアップを実行します（スタティック ID NAT のみ。ルーテッド モードのみ）。

元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択している場合に、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

IPv6 ネットワークの変換

IPv6 専用ネットワークと IPv4 専用ネットワークの間でトラフィックを通過させる必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークから内部アドレスを隠す必要がある場合があります。

IPv6 ネットワークとともに次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4（およびその反対）に変換します。IPv6 から IPv4 への変換と IPv4 から IPv6 への変換に対する 2 つのポリシーを定義する必要があります。1 つの/手動 NAT ルールでこれを実現できますが、DNS サーバが外部ネットワークにある場合は、DNS 応答を書き換える必要がある可能性があります。宛先を指定するときに/手動 NAT ルールで DNS の書き換えを有効にすることはできないため、2 つの/自動 NATルールを作成する方法が適しています。

（注） NAT46 がサポートするのは、スタティック マッピングのみです。

- NAT66：IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用をお勧めします。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

（注） NAT64 および NAT 46 は、標準的なルーテッドインターフェイスでのみ使用できます。NAT66 は、ルーテッドインターフェイスとブリッジ グループ メンバー インターフェイスの両方で使用できます。

NAT64/46：IPv6 アドレスから IPv4 への変換

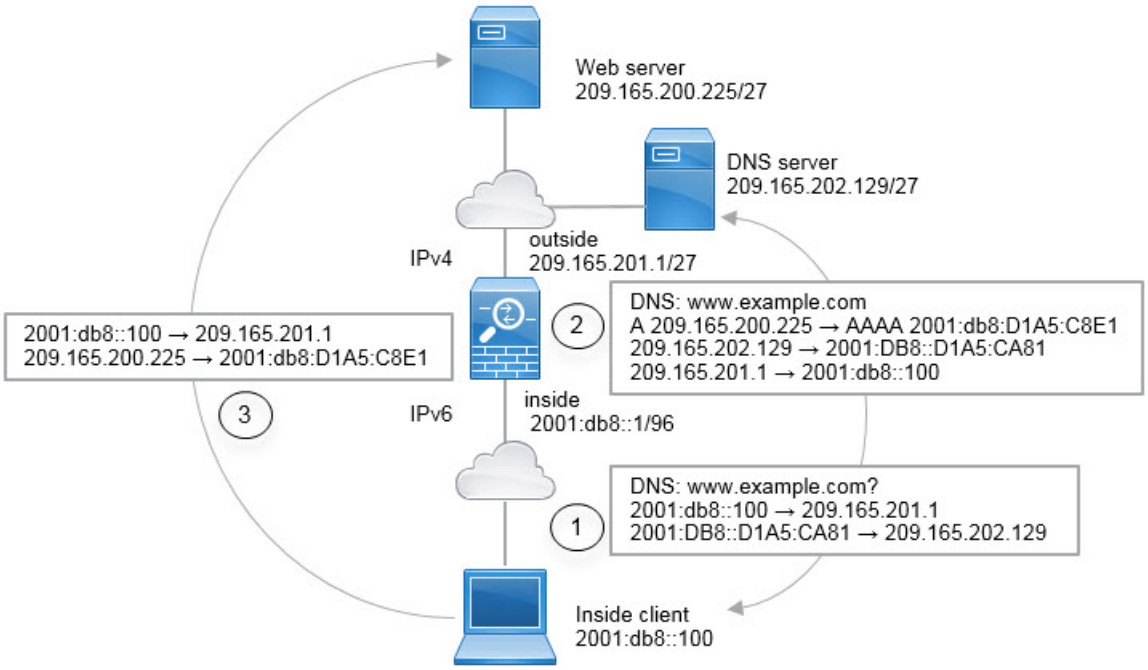
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。IPv4 ネットワークで IPv6 アドレスをバインドするための IPv4 アドレス プールと、IPv6 ネットワークで IPv4 アドレスをバインドするための IPv6 アドレス プールの 2 つを定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは通常は小さく、一般的に IPv6 クライアント アドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT またはスタティック NAT と比較して、できる限り多数の IPv6 クライアント アドレスにより容易に対応します。
- NAT 46 ルールの IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティック マッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。1 つの/手動 NAT ルールでこれを実現できますが、DNS サーバが外部ネットワークにある場合は、DNS 応答を書き換える必要がある可能性があります。宛先を指定するときに /手動 NAT ルールで DNS の書き換えを有効にすることはできないため、2 つの/自動 NAT ルールを作成する方法が適しています。

NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザが必要とするいくつかの IPv4 専用サービスが外部のインターネット上に存在する一般的な例です。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバからの応答を A（IPv4）レコードから AAAA（IPv6）レコードに変換でき、アドレスが IPv4 から IPv6 に変換されます。

次は、内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとしている場合の Web 要求の一般的なシーケンスです。

1. クライアントのコンピュータが 2001:DB8::D1A5:CA81 にある DNS サーバに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先が次のように変換されます。
   - 2001:DB8::100 を 209.165.201.1 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
   - 2001:DB8::D1A5:CA81 を 209.165.202.129 に変換（NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 に相当します）。
2. DNS サーバが、www.example.com が 209.165.200.225 であることを示す A レコードに応答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
   - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
   - 209.165.201.1 を 2001:db8::100 に変換

3 これで、IPv6 クライアントが Web サーバの IP アドレスを取得し、www.example.com（2001:db8:D1A5:C8E1）に HTTP 要求を送信できます。（D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します）。HTTP 要求の送信元と宛先が変換されます。

- 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
- 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換（NAT46 ルール）。

次の手順では、この例の設定方法について説明します。

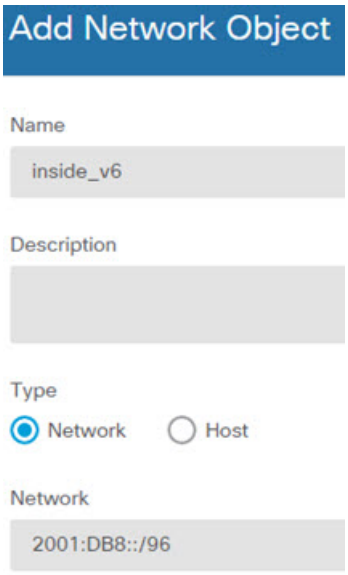
手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

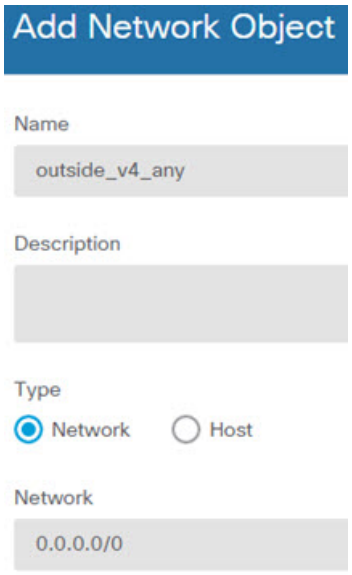
b) 目次から [ネットワーク（Network）]を選択して、[+] をクリックします。

c) 内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）]を選択して、ネットワーク アドレス（2001:db8::/96）を入力します。



d) [追加（Add）]、[OK]をクリックします。

e) [+]をクリックして、外部 IPv4 ネットワークを定義します。
ネットワーク オブジェクトに名前（outside_v4_any など）を付け、[ネットワーク（Network）]を選択して、ネットワーク アドレス（0.0.0.0/0）を入力します。



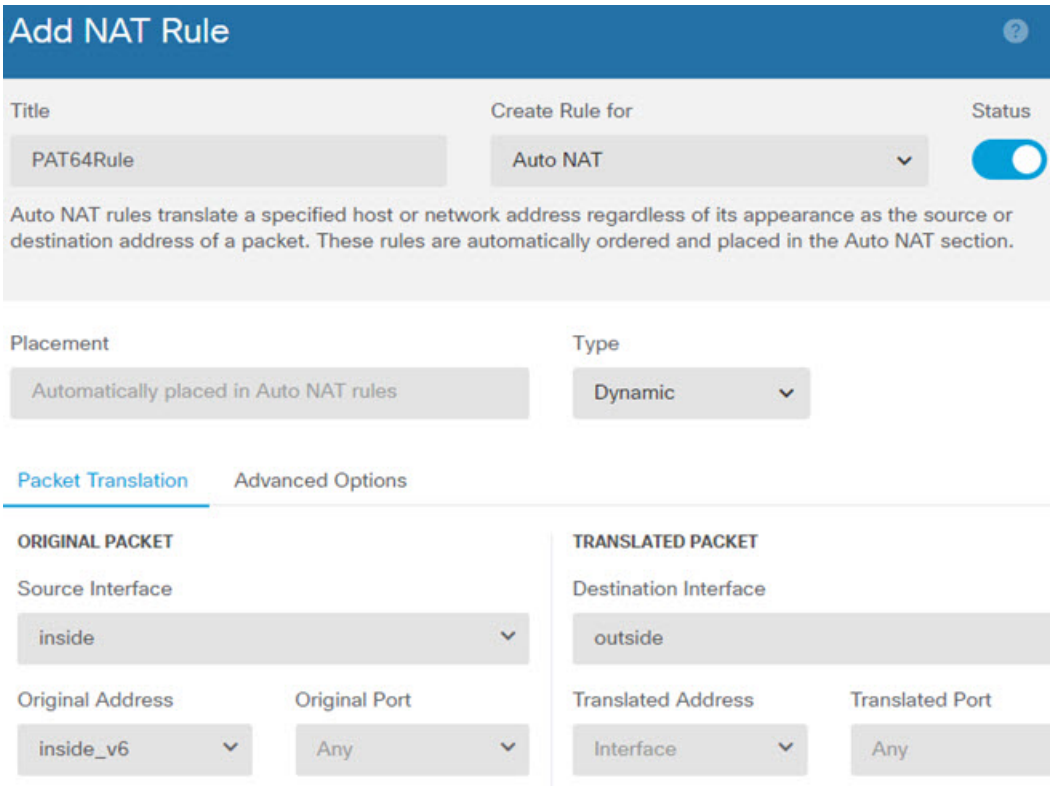
ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）]：PAT64Rule（またはユーザが選択する別の名前）。
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）]。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：[インターフェイス（Interface）]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。



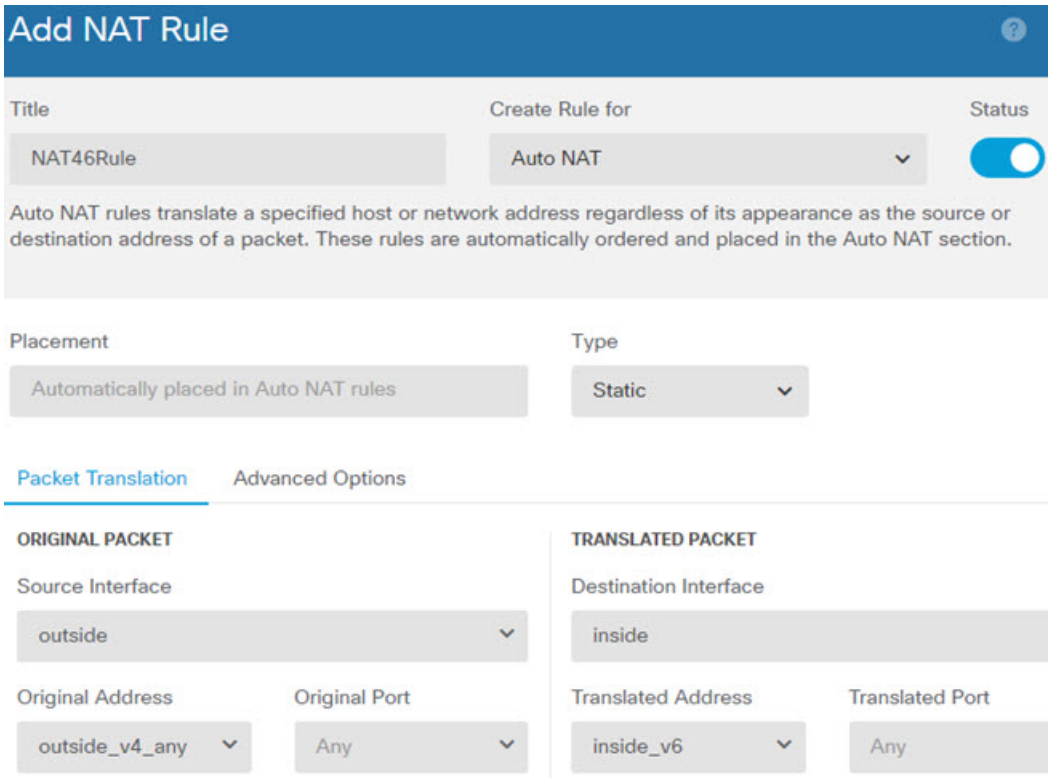
d) [OK]をクリックします。
このルールを使用すると、内部インターフェイスの2001:db8::/96サブネットから外部インターフェイスに移動するすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）] : NAT46Rule（またはユーザが選択する別の名前）。
- [ルールの作成対象（Create Rule For）] : [自動 NAT（Auto NAT）]。
- [タイプ（Type）] : [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）] : 外部。
- [宛先インターフェイス（Destination Interface）] : 内部。
- [元のアドレス（Original Address）] : outside_v4_any ネットワーク オブジェクト。
- [変換済みアドレス（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（Translate DNS replies that match this rule）] を選択します。



c) [OK]をクリックします。
このルールを使用すると、内部インターフェイスに届く外部ネットワークのすべての IPv4 アドレスが、組み込みの IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答が A（IPv4）レコードから AAAA（IPv6）レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

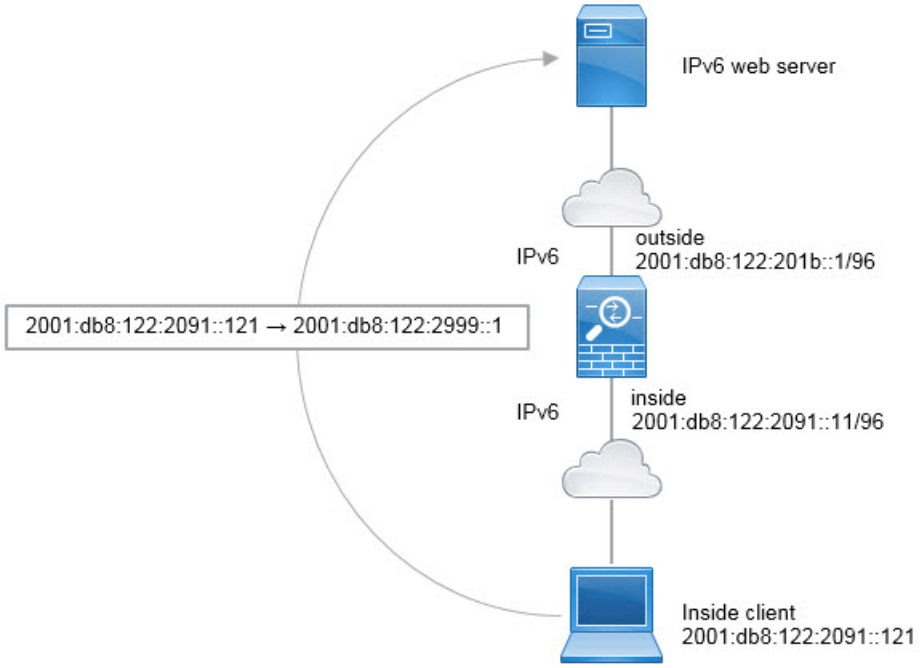
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用をお勧めします。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。/自動 NATを使用すると、これらのルールを容易にモデル化できます。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 ルールを単一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変換を設定できます。次の例では、2001:db8:122:2091::/96 ネットワークの内部アドレスを 2001:db8:122:2999::/96 ネットワークの外部アドレスに変換する方法について説明します。



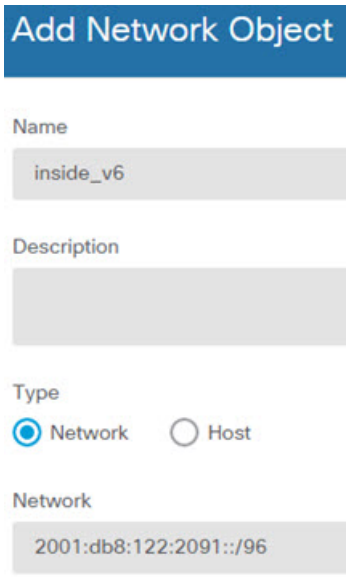
手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

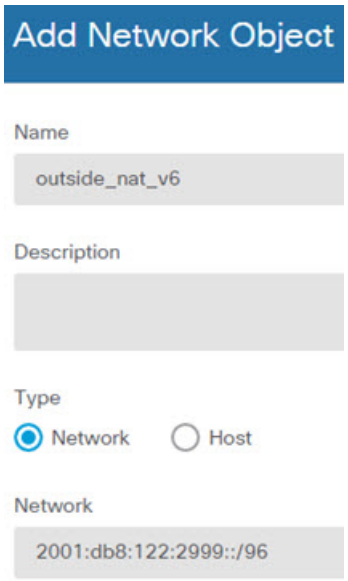
b) 目次から [ネットワーク（Network）]を選択して、[+] をクリックします。

c) 内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）]を選択して、ネットワーク アドレス（2001:db8:122:2091::/96）を入力します。



d) [追加（Add）]、[OK]をクリックします。

e) [+]をクリックして、外部 IPv6 PAT ネットワークを定義します。
ネットワーク オブジェクトに名前（outside_nat_v6 など）を付け、[ネットワーク（Network）]を選択して、ネットワーク アドレス（2001:db8:122:2999::/96）を入力します。



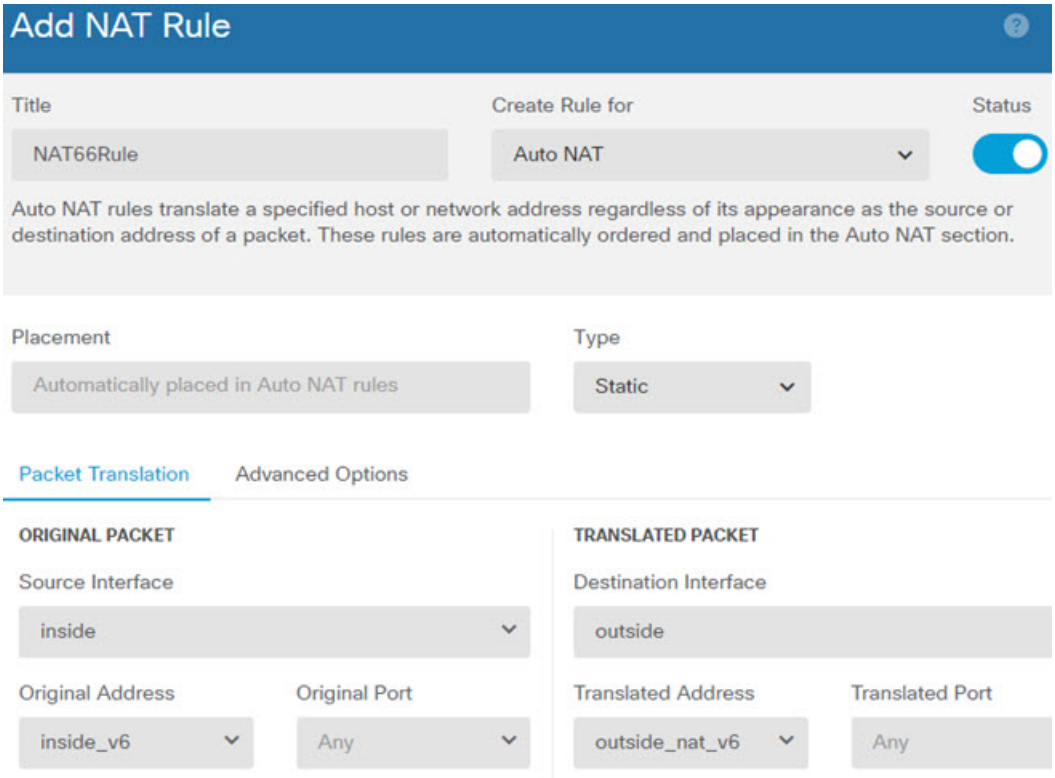
ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）]：NAT66Rule（またはユーザが選択する別の名前）
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）]。
- [タイプ（Type）]：[スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：outside_nat_v6 ネットワーク オブジェクト。

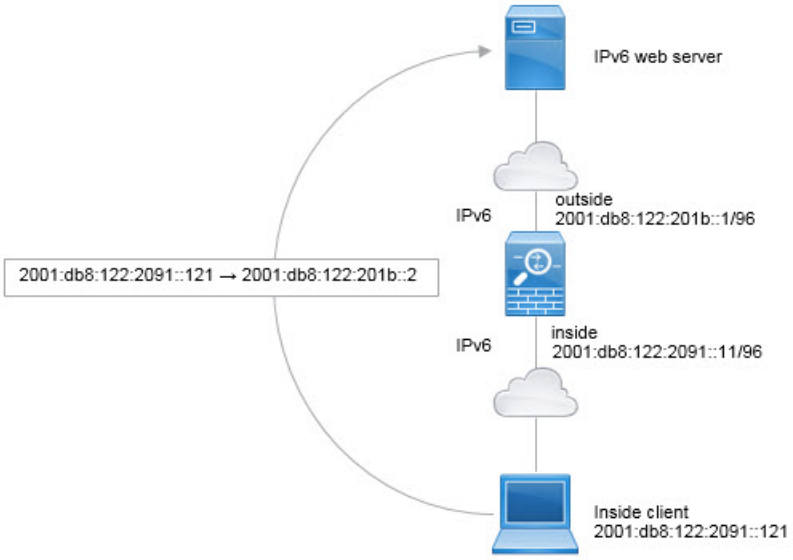


d) [OK]をクリックします。
このルールを使用すると、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:2999::/96 ネットワークのアドレスにスタティック NAT66 変換されます。

NAT66 の例、シンプルな IPv6 インターフェイス PAT

NAT66 を実装するための簡単なアプローチは、外部インターフェイスの IPv6 アドレス上の異なるポートに内部アドレスを動的に割り当てる方法です。

ただし、Firepower Device Manager を使用して、インターフェイスの IPv6 アドレスを使用するインターフェイス PAT は設定できません。代わりに、同じネットワーク上の 1 つの空きアドレスをダイナミック PAT プールとして使用します。



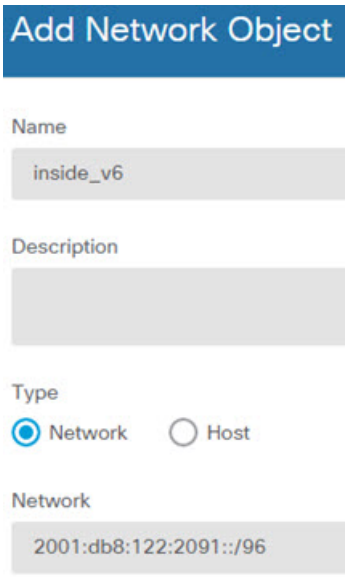
手順

ステップ 1 内部 IPv6 ネットワークと IPv6 PAT アドレスを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

b) 目次から [ネットワーク（Network）]を選択して、[+] をクリックします。

c) 内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）]を選択して、ネットワーク アドレス（2001:db8:122:2091::/96）を入力します。



d) [追加（Add）]、[OK]をクリックします。

e) [+]をクリックして、外部 IPv6 PAT アドレスを定義します。
ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ホスト（Host）]を選択して、ホスト アドレス（2001:db8:122:201b::2）を入力します。

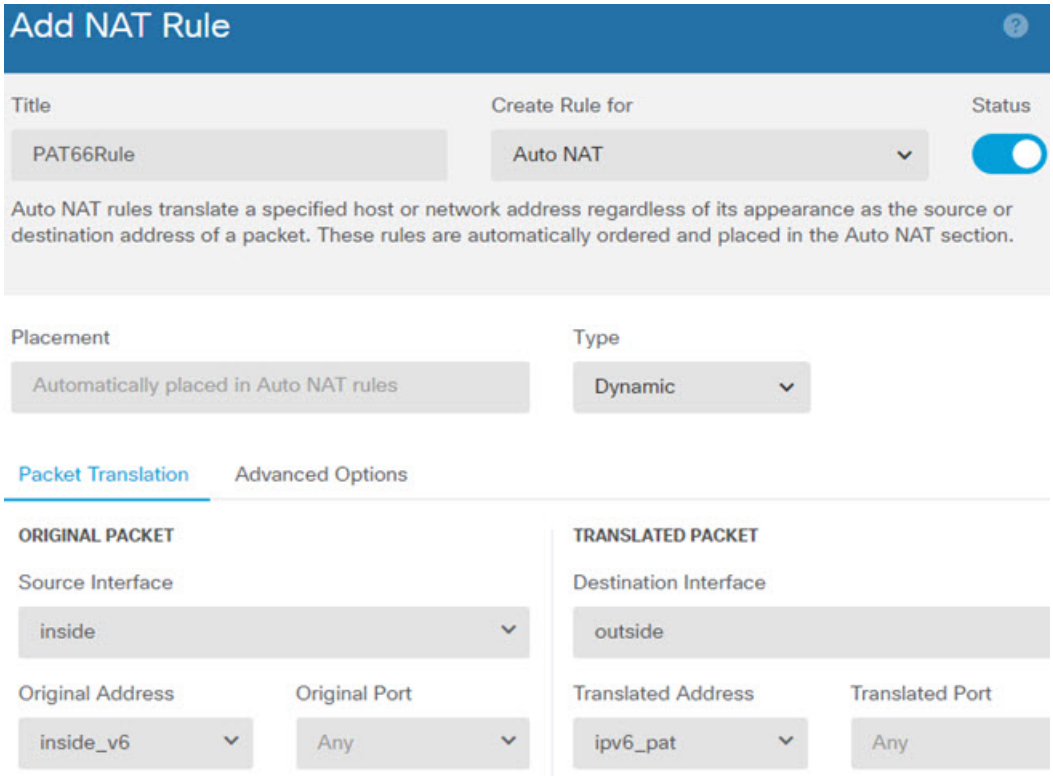
ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）]：PAT66Rule（またはユーザが選択する別の名前）
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）]。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：ipv6_pat ネットワーク オブジェクト。



d) [OK]をクリックします。
このルールを使用すると、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:201b::2 のポートにダイナミック PAT66 変換されます。

NAT のモニタリング

NAT 接続をモニタしてトラブルシューティングを実行するには、デバイス CLI にログインして次のコマンドを使用します。

- **show nat** は、NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** は、現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** を使用すると、アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換をクリアすると、システムは、新しいルールに基づいたクライアントの次の接続試行でクライアントの新しい変換を作成できます。

NAT の例

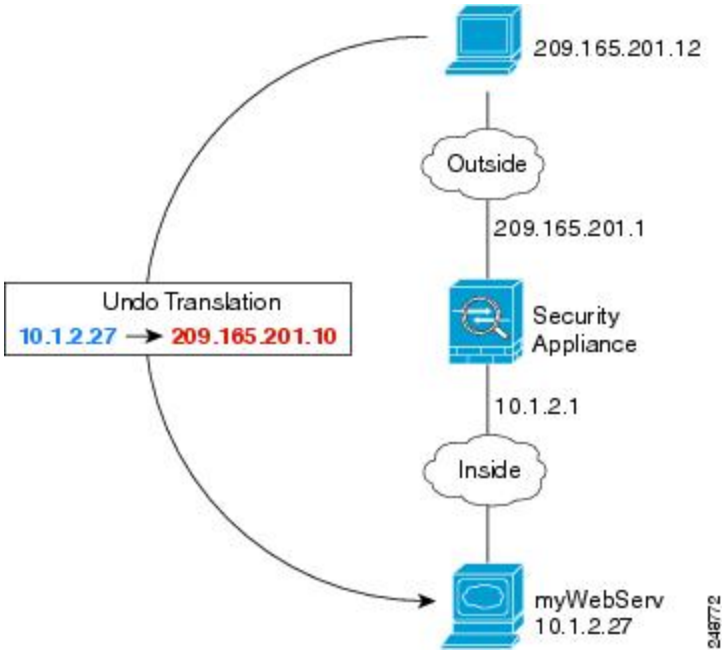
次に、脅威に対する防御デバイスでの NAT の設定例を示します。

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。

図 *13*：内部 *Web* サーバのスタティック *NAT*



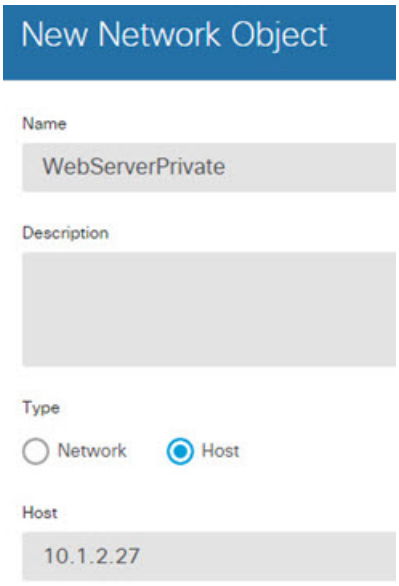
手順

ステップ 1 サーバのプライベートおよびパブリック 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。

a) [オブジェクト（Objects）]を選択します。

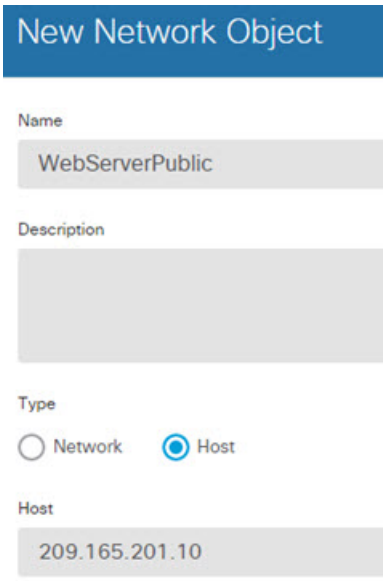
b) 目次から [ネットワーク（Network）]を選択して、[+] をクリックします。

c) Web サーバのプライベート アドレスを定義します。
ネットワーク オブジェクトに名前（WebServerPrivate など）を付け、[ホスト（Host）]を選択して、実際のホスト IP アドレス（10.1.2.27）を入力します。



d) [追加（Add）]、[OK]をクリックします。

e) [+]をクリックして、パブリック アドレスを定義します。
ネットワーク オブジェクトに名前（WebServerPublic など）を付け、[ホスト（Host）]を選択して、ホスト アドレス（209.165.201.10）を入力します。



f) [追加（Add）]、[OK]をクリックします。

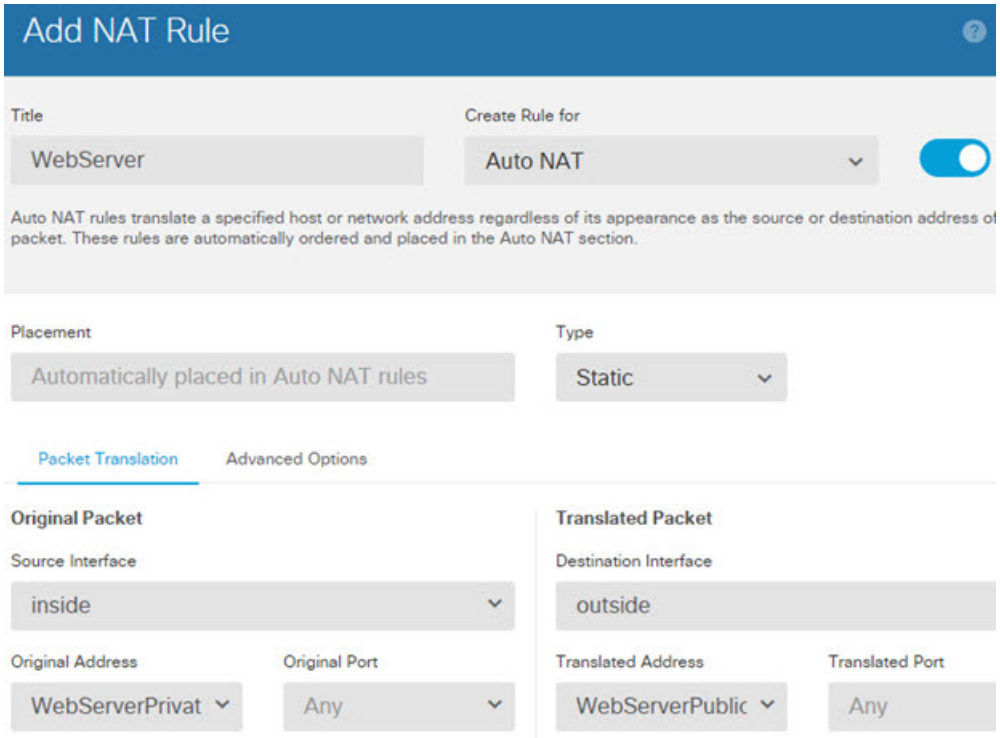
ステップ 2 オブジェクトのスタティック NAT を設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）]：WebServer（またはユーザが選択する別の名前）。
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）]。
- [タイプ（Type）]：[スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [元のアドレス（Original Address）]：WebServerPrivate ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：WebServerPublic ネットワーク オブジェクト。



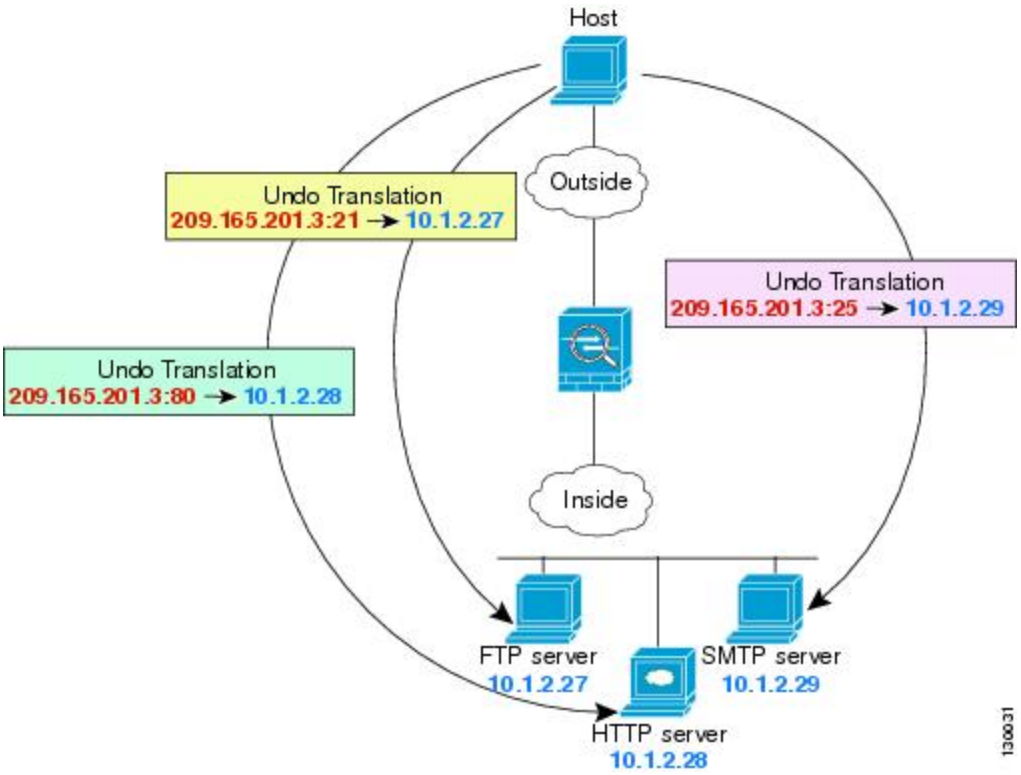
d) [OK]をクリックします。

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック自動 NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティッ

ク NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。

図 *14*：ポート変換を設定したスタティック *NAT*



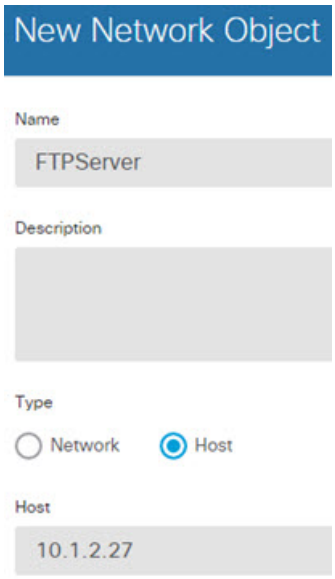
手順

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。

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) ネットワーク オブジェクトに名前を付け（たとえばFTPserver）、[ホスト（Host）]を選択し、FTP サーバの実際の IP アドレス（10.1.2.27）を入力します。

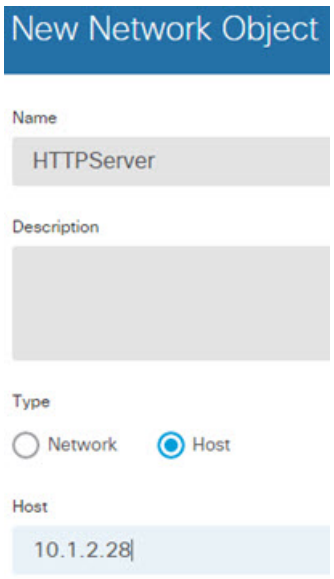


d) [追加（Add）] [OK] をクリックします。

ステップ 2 HTTP サーバのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば HTTPserver）、[ホスト（Host）]を選択し、ホストアドレス（10.1.2.28）を入力します。

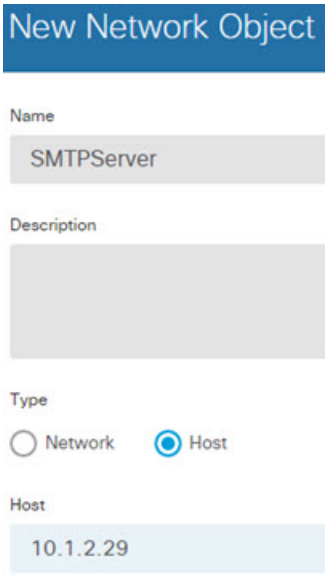


c) [追加（Add）] [OK] をクリックします。

ステップ 3 SMTP サーバのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば SMTPserver）、[ホスト（Host）]を選択し、ホストアドレス（10.1.2.29）を入力します。

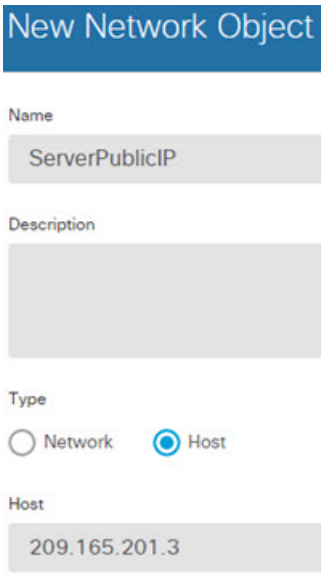


c) [追加（Add）] [OK] をクリックします。

ステップ 4 3 つのサーバに使用されるパブリック IP アドレスのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえばServerPublicIP）、[ホスト（Host）]を選択し、ホストアドレス（209.165.201.3）を入力します。



c) [追加（Add）] [OK] をクリックします。

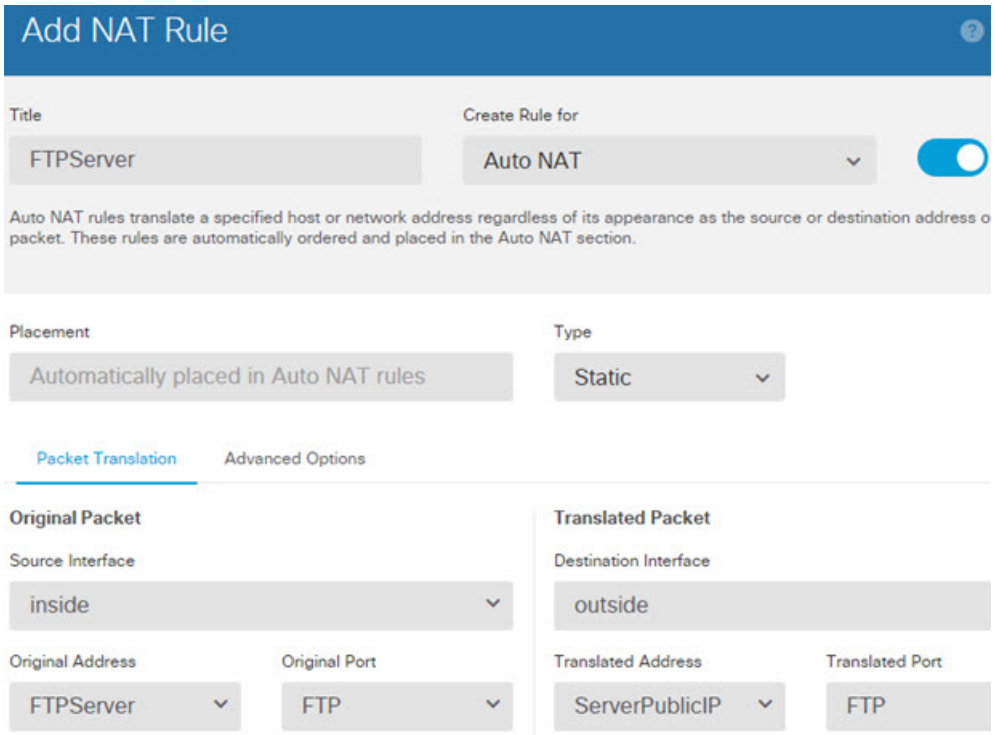
ステップ 5 FTP サーバのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）]= [FTPServer]（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）]= [自動 NAT（Auto NAT）]。
- [タイプ（Type）]= [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]= [内部（inside）]。
- [宛先インターフェイス（Destination Interface）]= [外部（outside）]。
- [元のアドレス（Original Address）]= [FTPServer ネットワーク オブジェクト（FTPserver network object）]。
- [変換済みアドレス（Translated Address）]= [ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）]。
- [元のポート（Original Port）]= [FTP ポート オブジェクト（FTP port object）]。
- [変換済みポート（Translated Port）]= [FTP ポート オブジェクト（FTP port object）]。



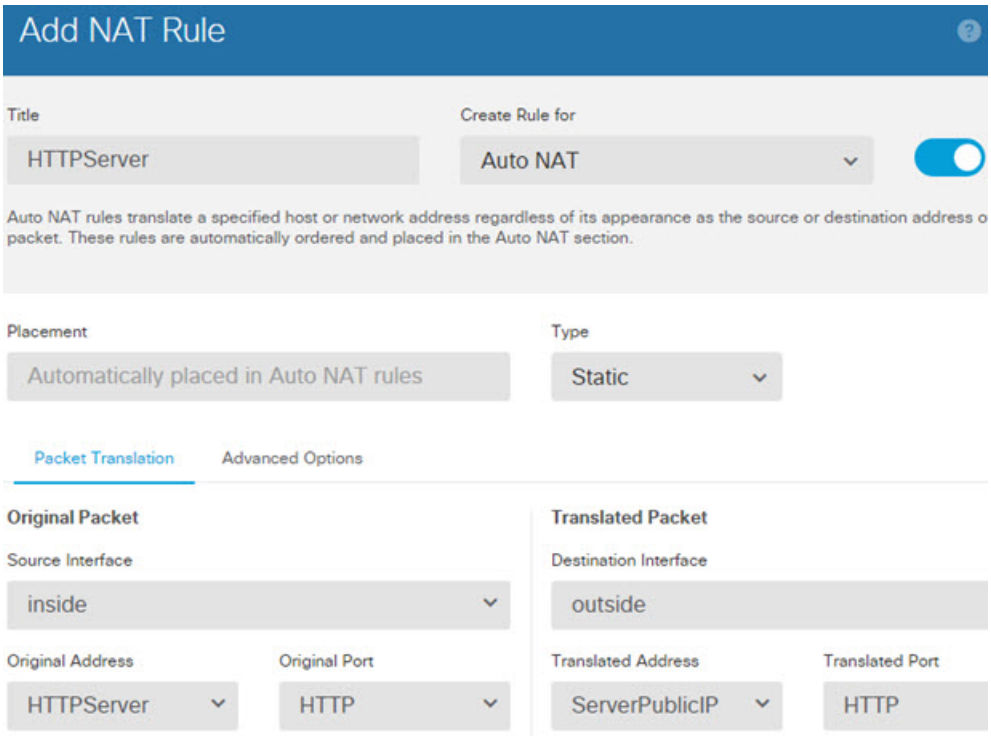
d) [OK]をクリックします。

ステップ 6 HTTP サーバのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）]= [HTTPServer]（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）]= [自動 NAT（Auto NAT）]。
- [タイプ（Type）]= [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]= [内部（inside）]。
- [宛先インターフェイス（Destination Interface）]= [外部（outside）]。
- [元のアドレス（Original Address）]= [HTTPserver ネットワーク オブジェクト（HTTPserver network object）]。
- [変換済みアドレス（Translated Address）]= [ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）]。
- [元のポート（Original Port）]= [HTTP ポート オブジェクト（FTP port object）]。
- [変換済みポート（Translated Port）]= [HTTP ポート オブジェクト（HTTP port object）]。



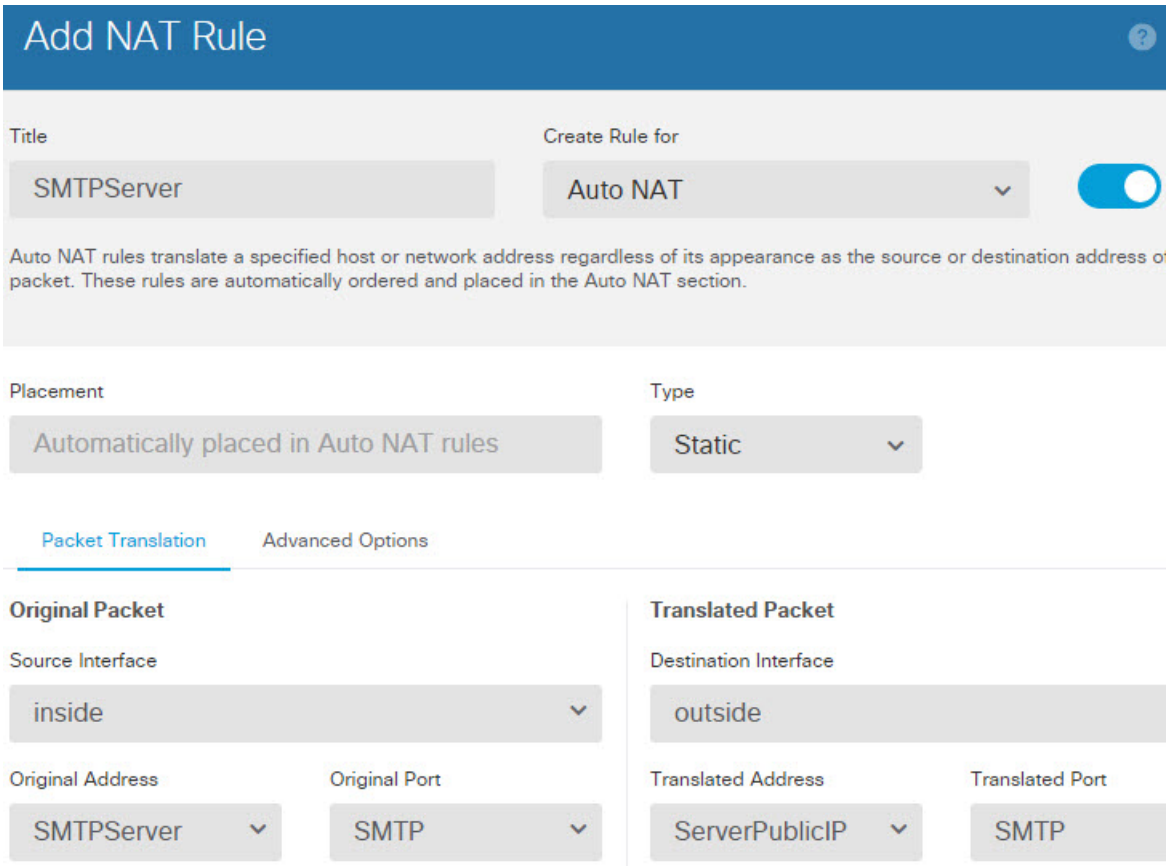
c) [OK]をクリックします。

ステップ 7 SMTP サーバのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

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]（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）]= [自動 NAT（Auto NAT）] 。
- [タイプ（Type）]= [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]= [内部（inside）]。
- [宛先インターフェイス（Destination Interface）]= [外部（outside）]。
- [元のアドレス（Original Address）]= [SMTPserver ネットワーク オブジェクト（SMTPserver network object）]。
- [変換済みアドレス（Translated Address）]= [ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）]。
- [元のポート（Original Port）]= [SMTP ポート オブジェクト（SMTP port object）]。
- [変換済みポート（Translated Port）]= [SMTP ポート オブジェクト（SMTP port object）]。



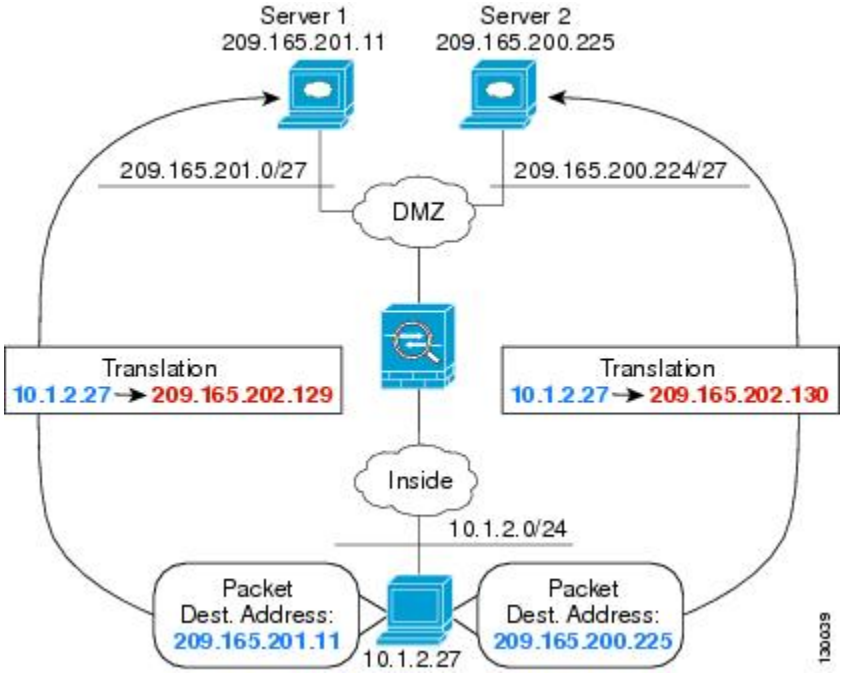
c) [OK]をクリックします。

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。

図 *15*：異なる宛先アドレスを使用する手動 *NAT*



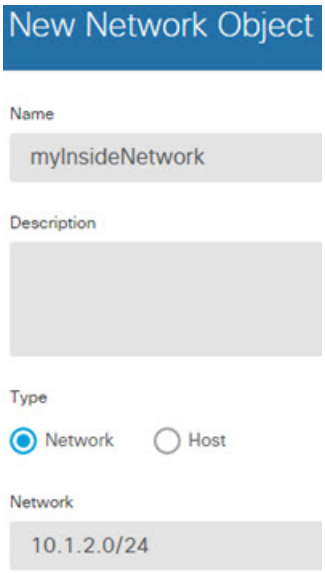
手順

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。

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) 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。

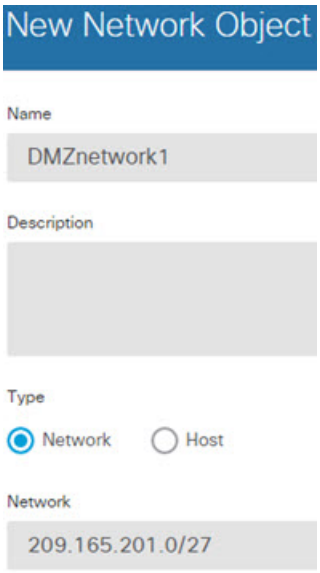


d) [追加（Add）][OK]をクリックします。

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）。

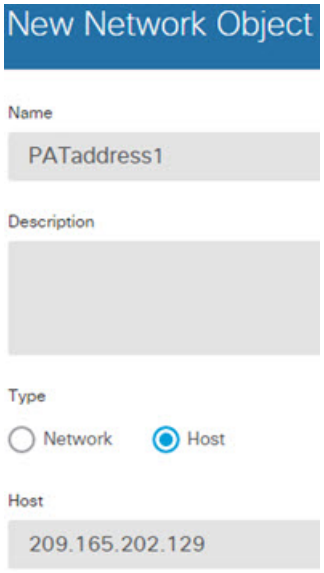


c) [追加（Add）][OK]をクリックします。

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。

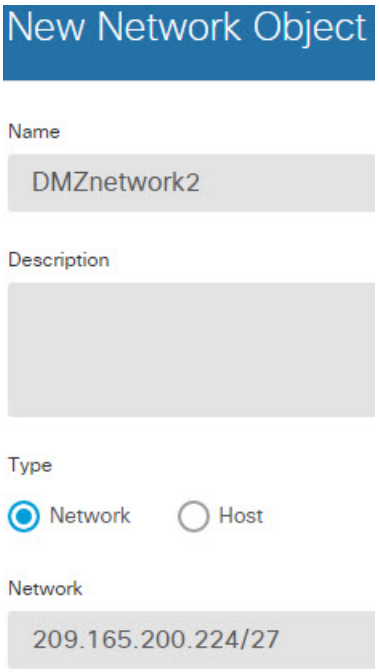


c) [追加（Add）][OK]をクリックします。

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）。

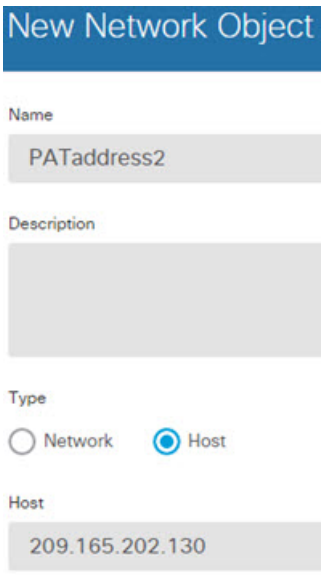


c) [追加（Add）][OK]をクリックします。

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。



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。

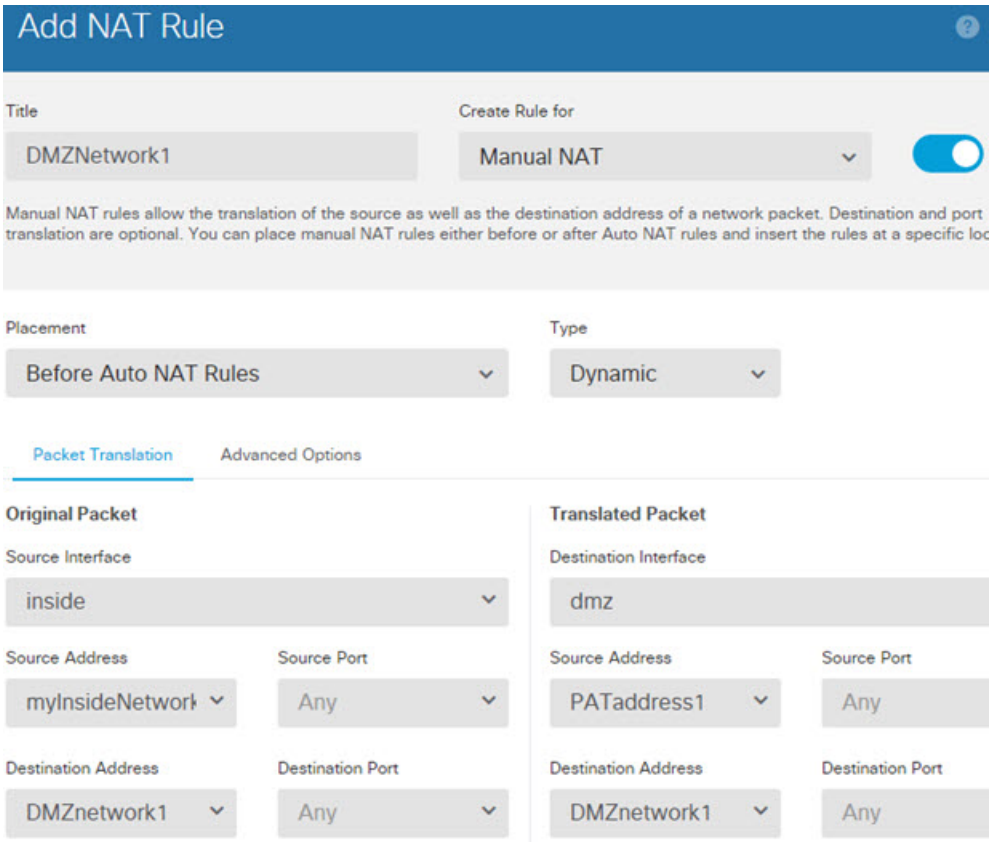
a) [ポリシー（Policies）] > [NAT] を選択します。

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。



d) [OK]をクリックします。

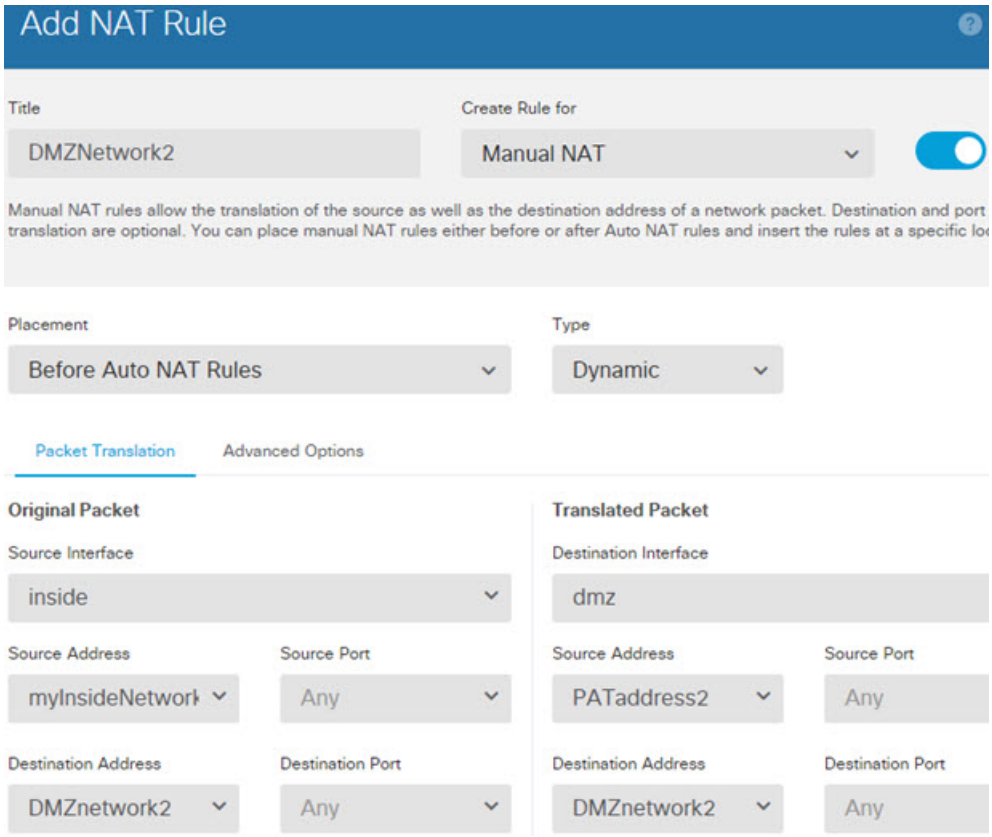
ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

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。



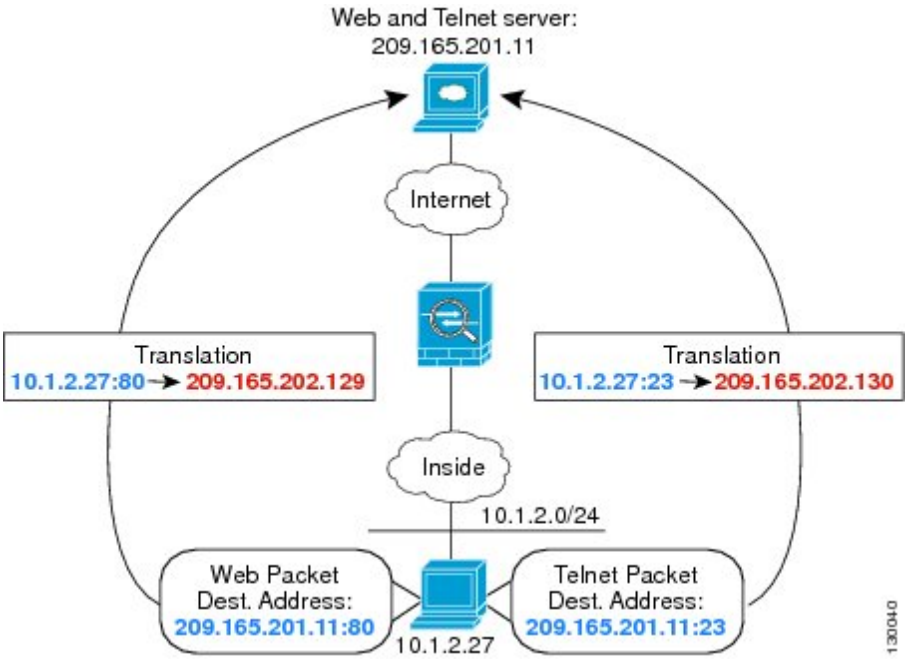
c) [OK]をクリックします。

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。

図 *16* : 異なる宛先ポートを使用する手動 *NAT*



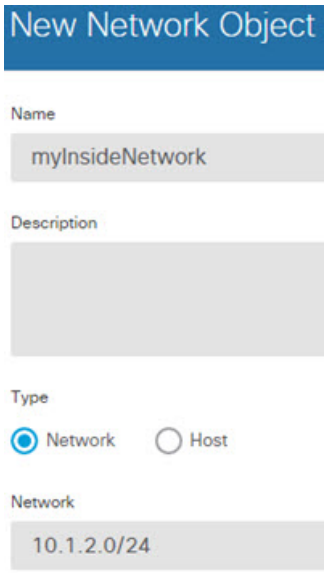
手順

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。

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) 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。

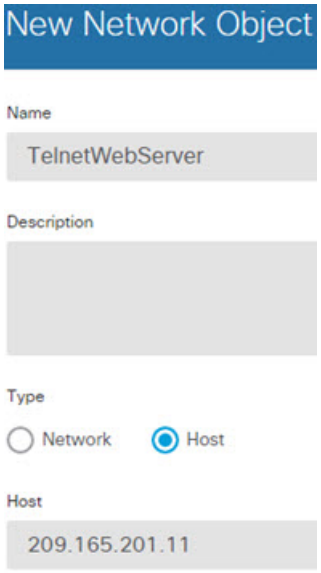


d) [追加（Add）][OK]をクリックします。

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。

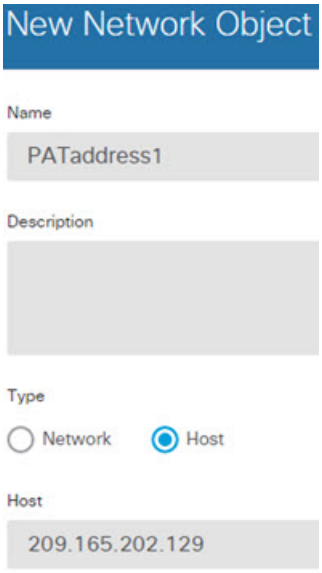


c) [追加（Add）][OK]をクリックします。

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.202.129 を入力します。

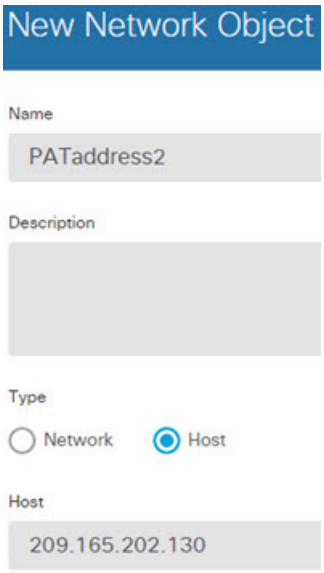


c) [追加（Add）][OK]をクリックします。

ステップ 4 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

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。



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。

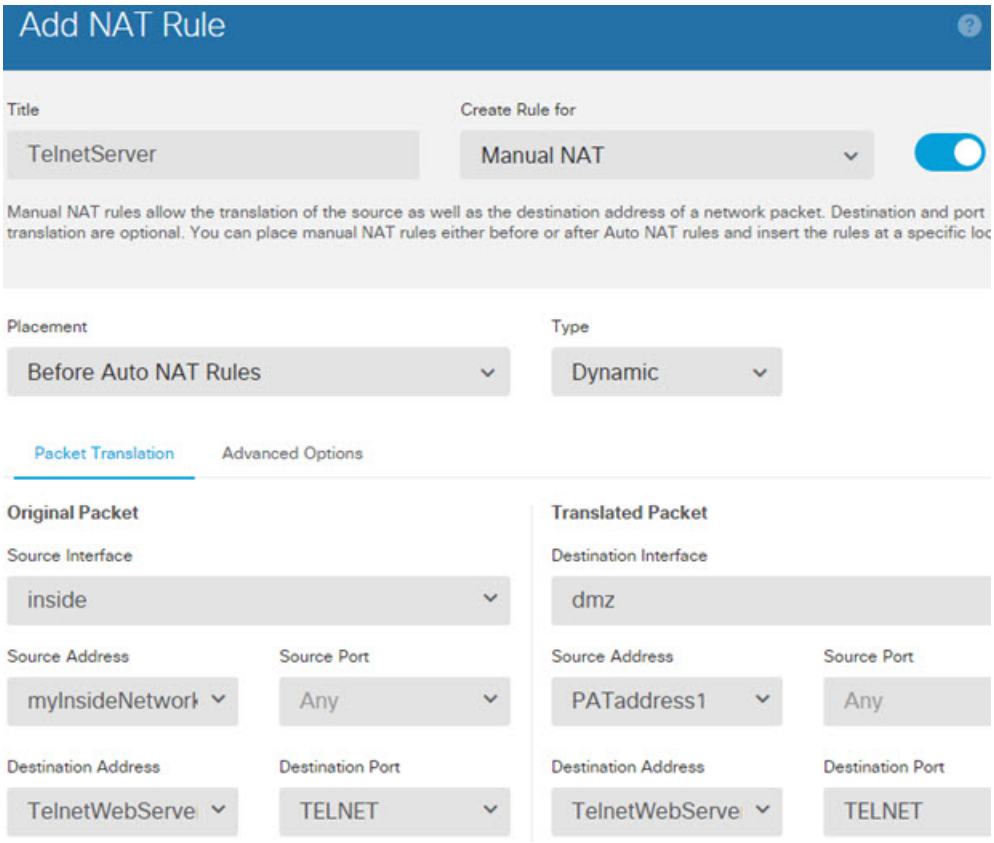
a) [ポリシー（Policies）] > [NAT] を選択します。

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。



d) [OK]をクリックします。

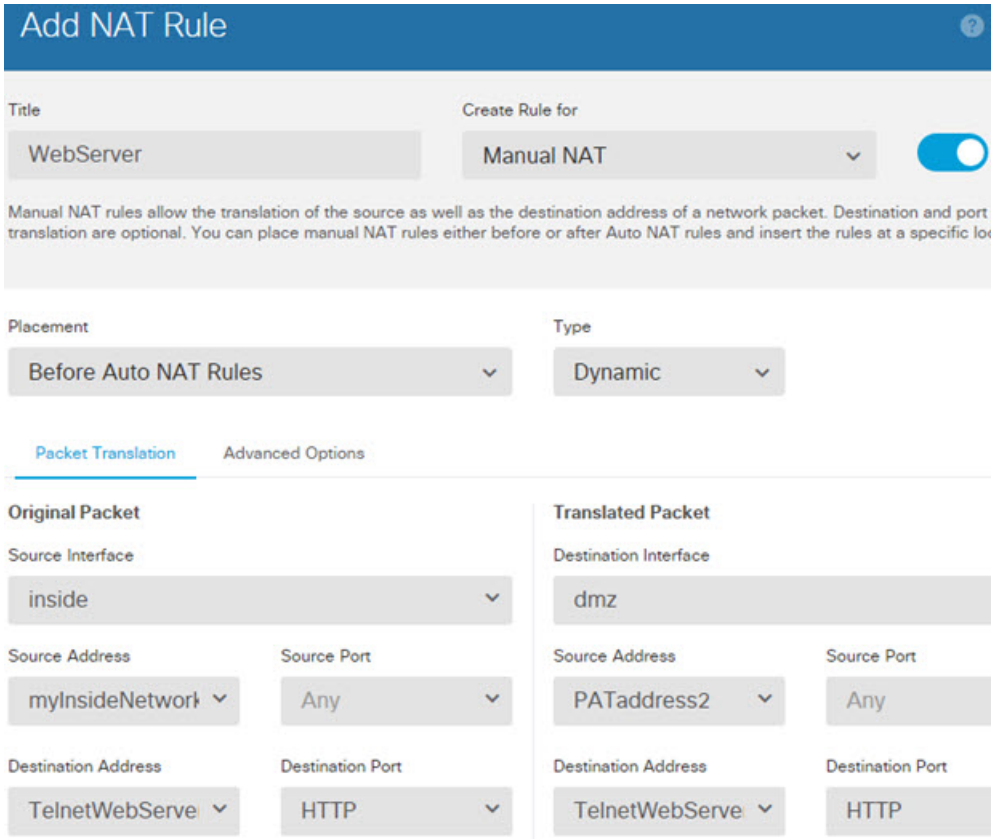
ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

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。



c) [OK]をクリックします。

NAT を使用した DNS クエリーのリライトと応答

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにFirepower Threat Defenseデバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーション ルールを設定するときに設定できます。

この機能は、NAT ルールに一致する DNS クエリーと応答のアドレスをリライトします（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリーの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。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。

以下に、NAT ルールで DNS のリライトを設定する必要が生じる主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード（IPv4 用）と AAAA レコード（IPv6 用）を変換するために DNS のリライトが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS リライトに関する制限事項

次に DNS リライトの制限事項を示します。

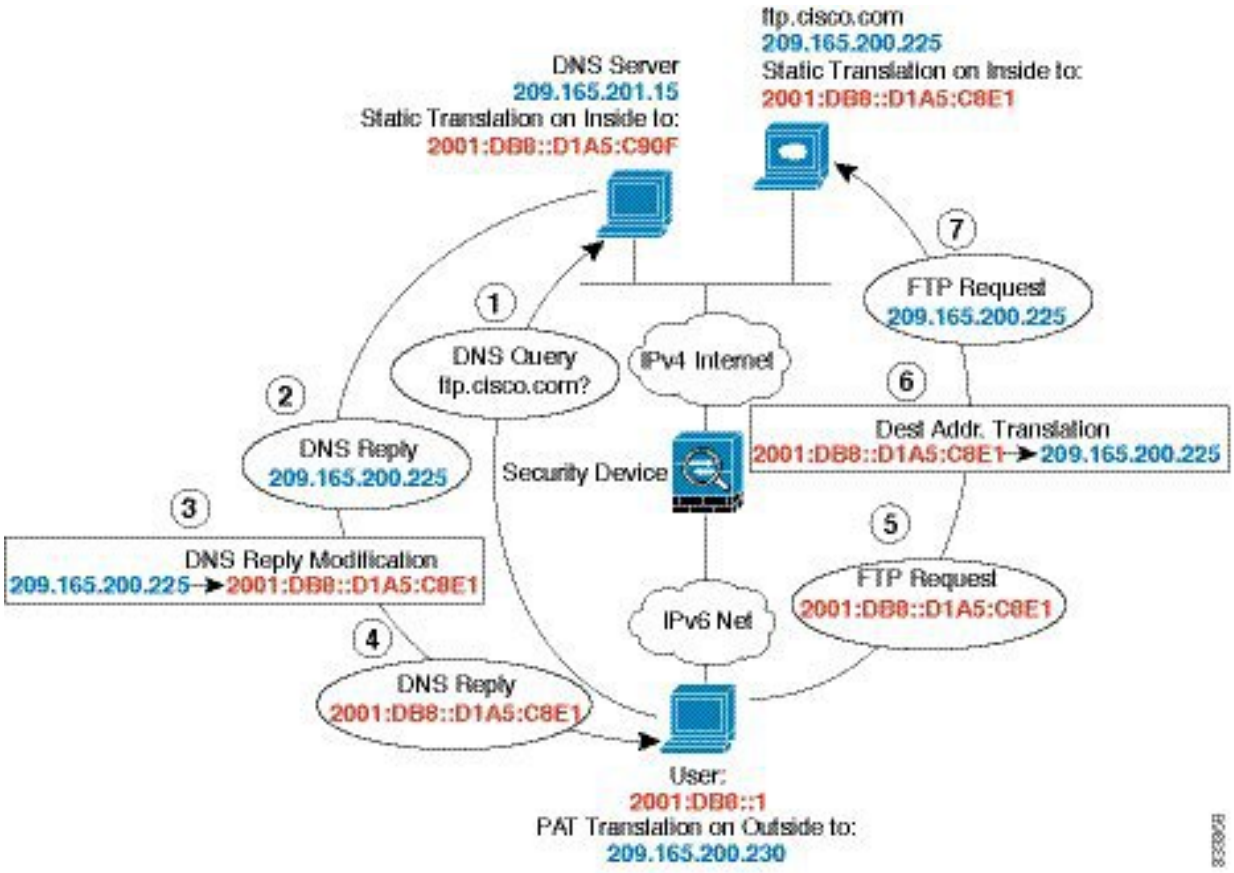
- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- /手動 NATルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、Firepower Threat Defense デバイスは、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- 実際には、DNS リライトは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、リライトが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS のリライトによって、DNS ダイナミック アップデートのメッセージ（オペレーション コード 5）は書き換えられません。

次のトピックで、NAT ルールでの DNS リライトの例を示します。

DNS 64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス（209.165.200.225）を応答します。

内部ユーザに ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1：D1A5:C8E1 は IPv6 の 209.165.200.225 に相当）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。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。



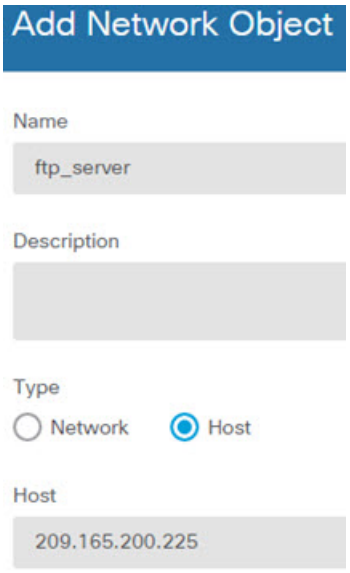
手順

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。

a) [オブジェクト（Objects）]を選択します。

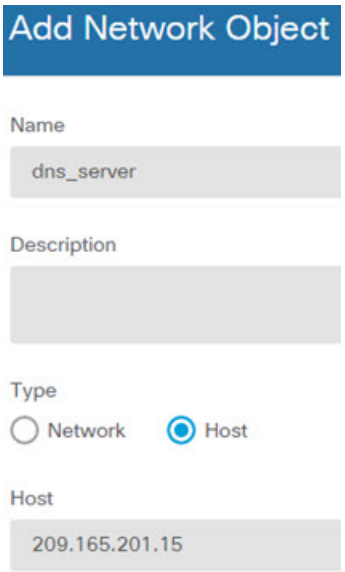
b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。

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 209.165.200.225 を入力します。



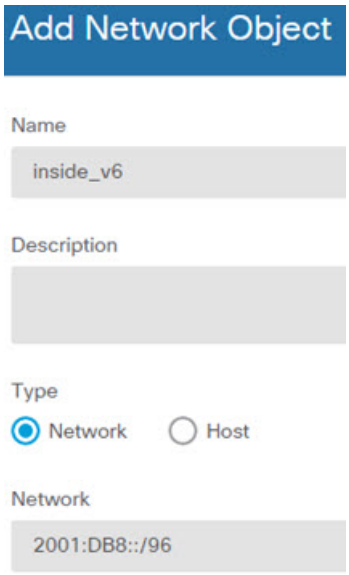
d) [追加（Add）][OK]をクリックします。

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。



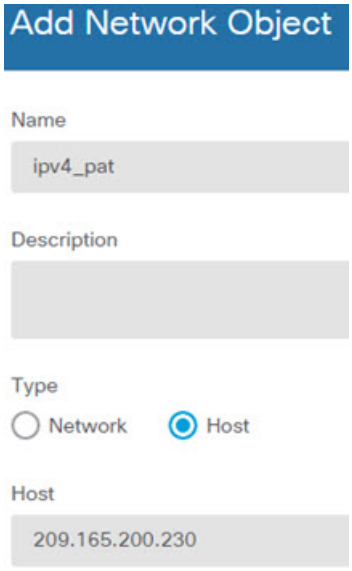
f) [追加（Add）][OK]をクリックします。

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。



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。



j) [追加（Add）][OK]をクリックします。

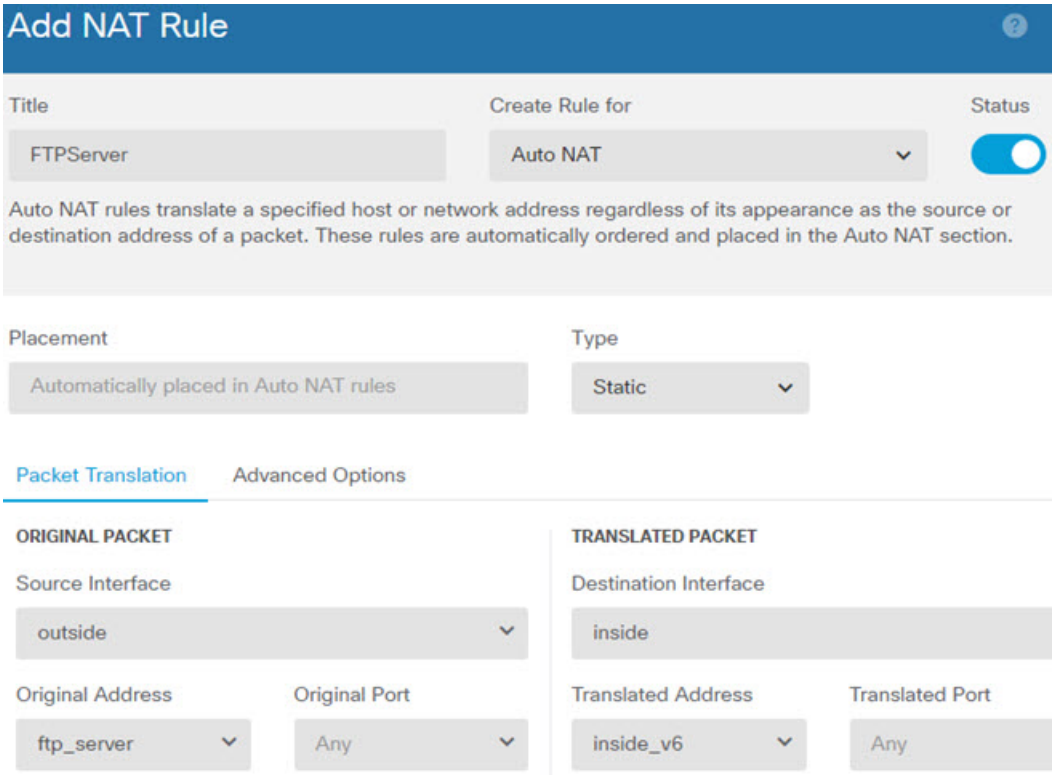
ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

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。

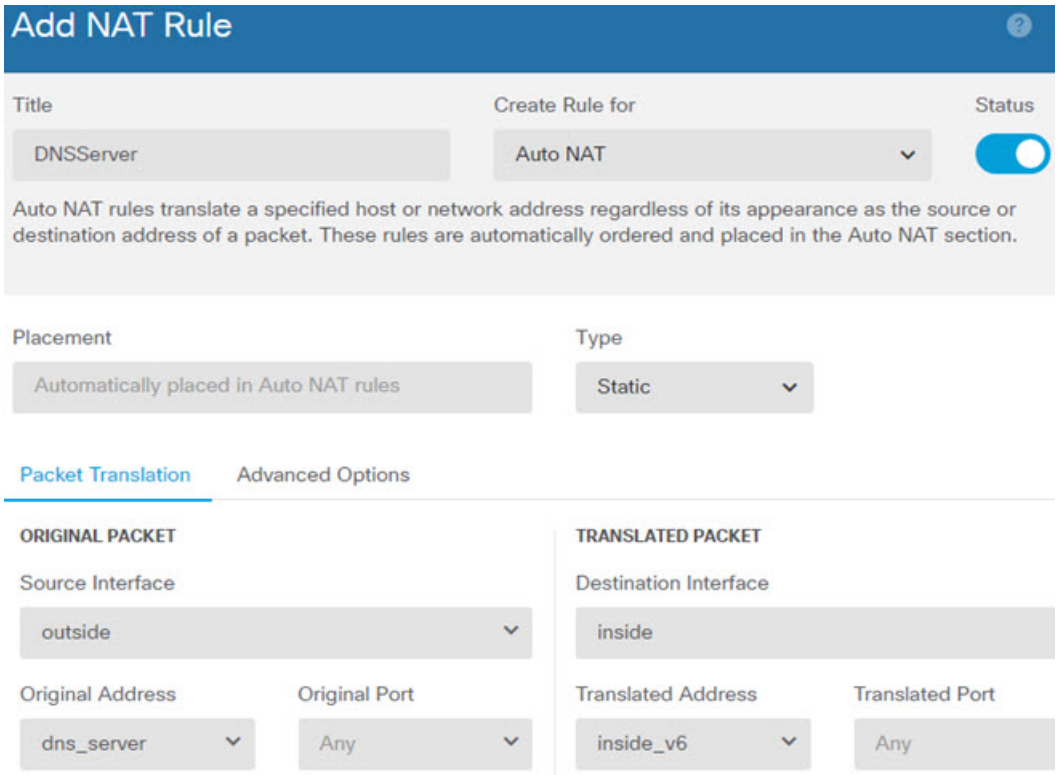
ステップ 3 DNS サーバのためのスタティック NAT ルールを設定します。

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）= 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。



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。

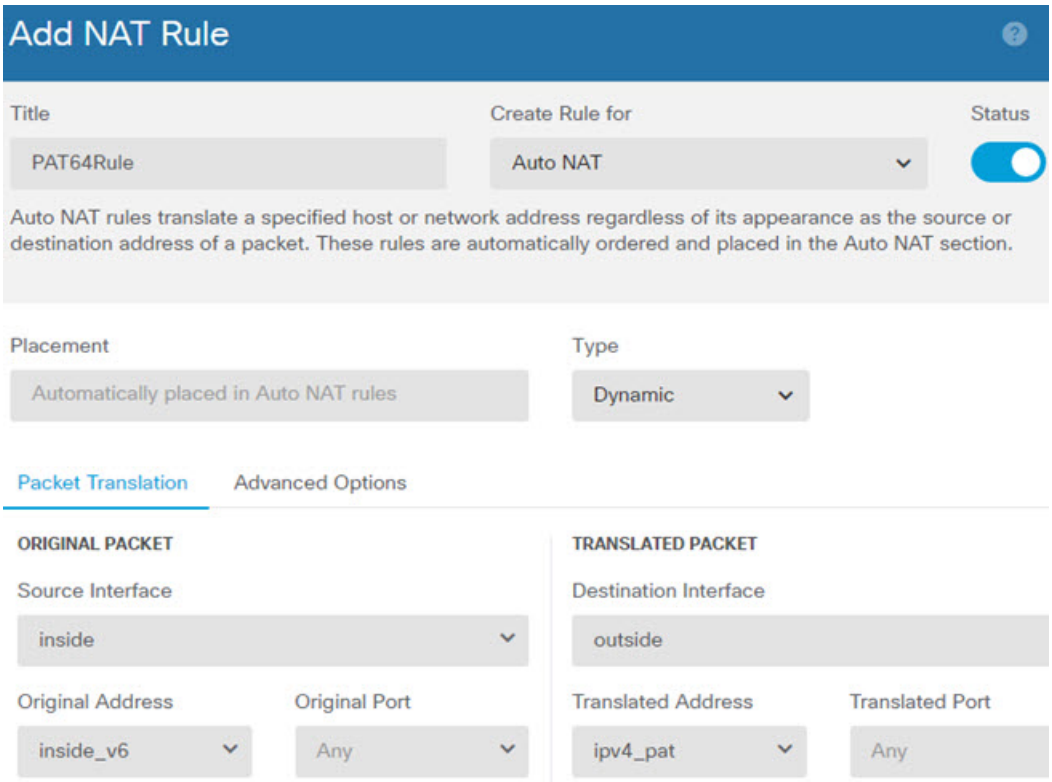
a) [ポリシー（Policies）] > [NAT] を選択します。

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。



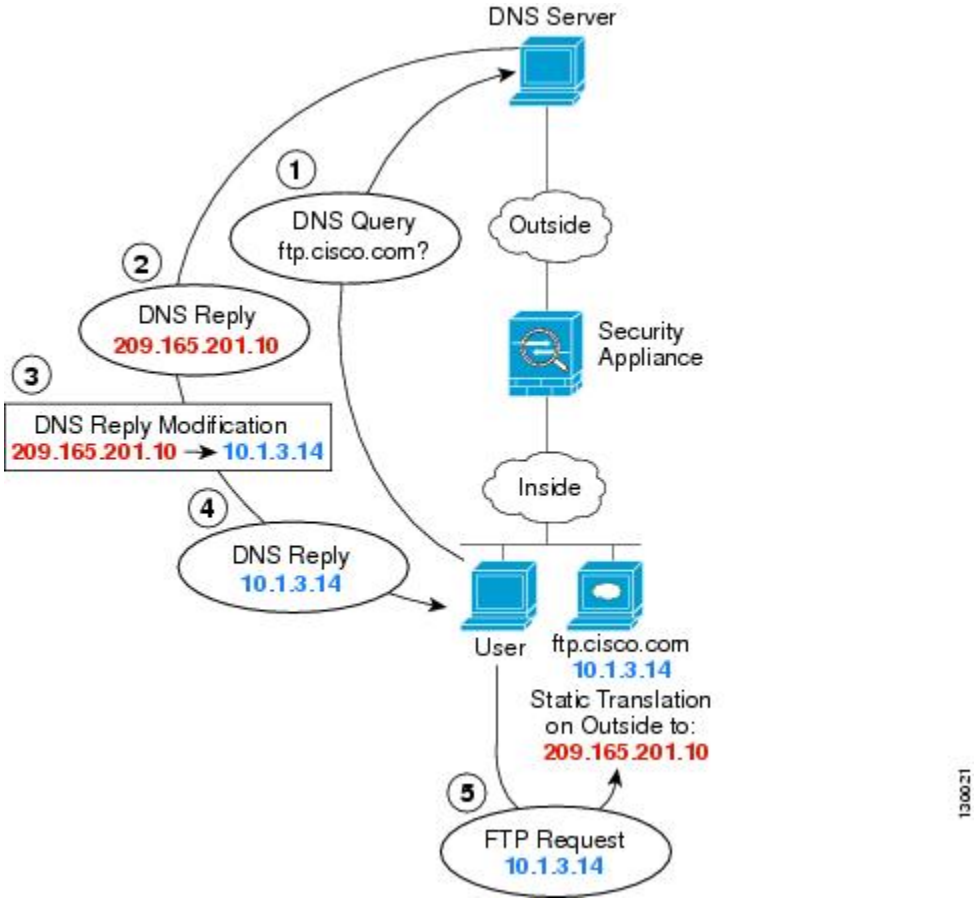
d) [OK]をクリックします。

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確認できるマッピング アドレス（209.165.201.10）にスタティックに変換するように NAT を設定します。

この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバはマッピング アドレス（209.165.201.10）を応答します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



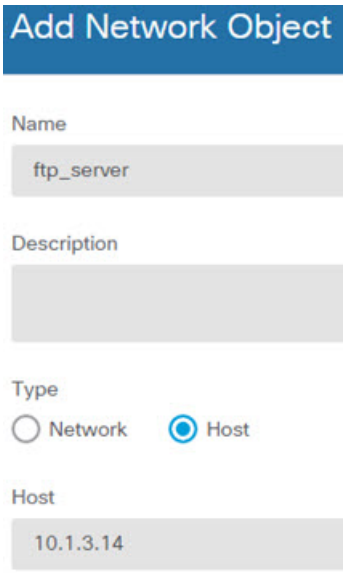
手順

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。

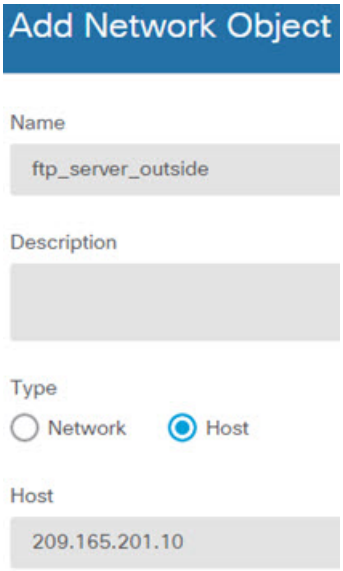
b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。

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。



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。



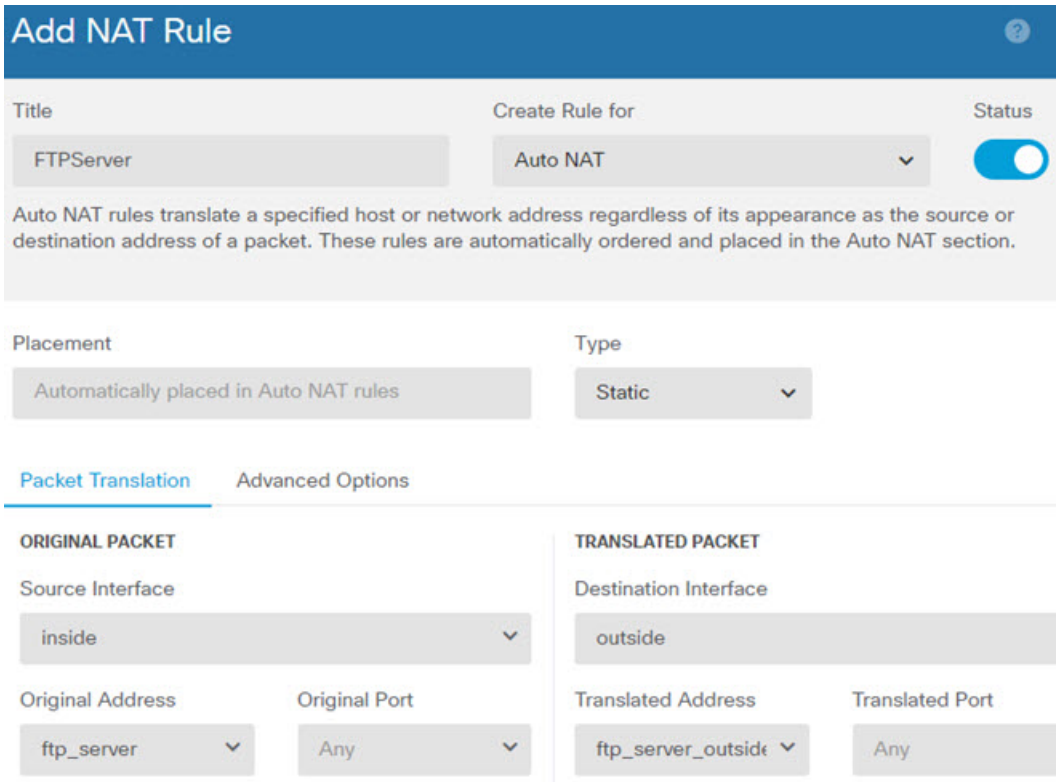
ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

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。

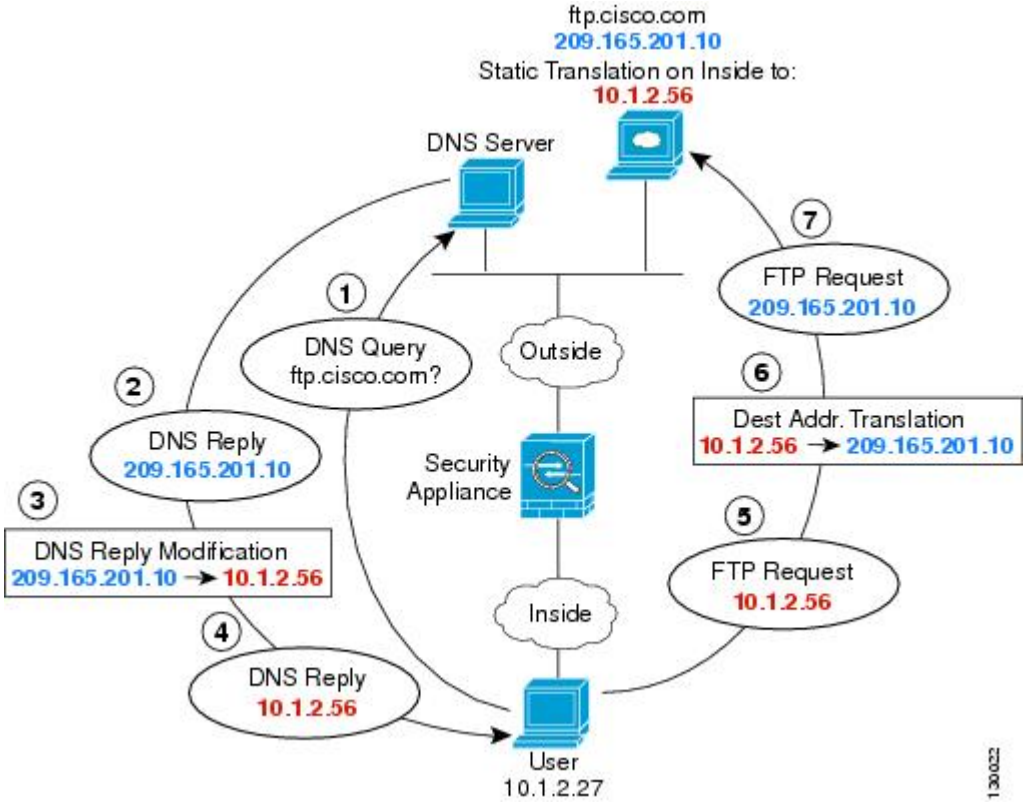
- タイトル（Title）= FTPServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Static。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= outside。
- 元のアドレス（Original Address）= ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= ftp_server_outside のネットワーク オブジェクト。
- [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。



d) [OK]をクリックします。

DNS 応答修正：ホスト ネットワーク上の DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス（209.165.20.10）を応答します。内部ユーザに ftp.cisco.com のマッピング アドレス（10.1.2.56）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



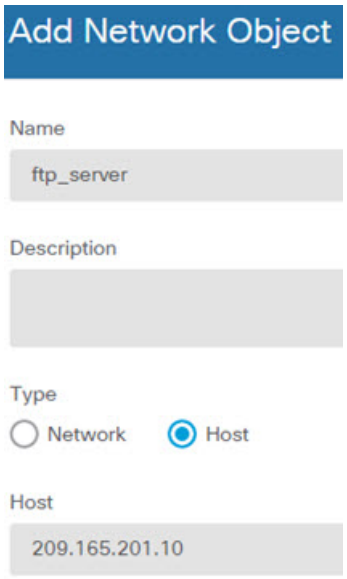
手順

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。

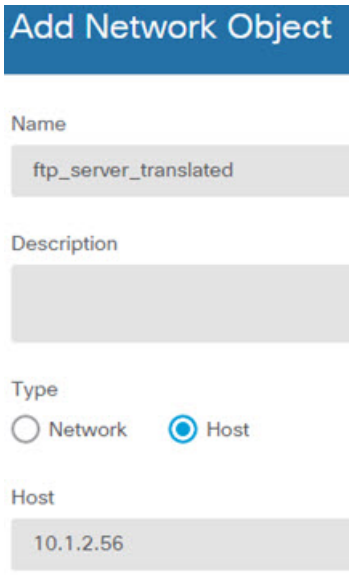
a) [オブジェクト（Objects）]を選択します。

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 209.165.201.10 を入力します。

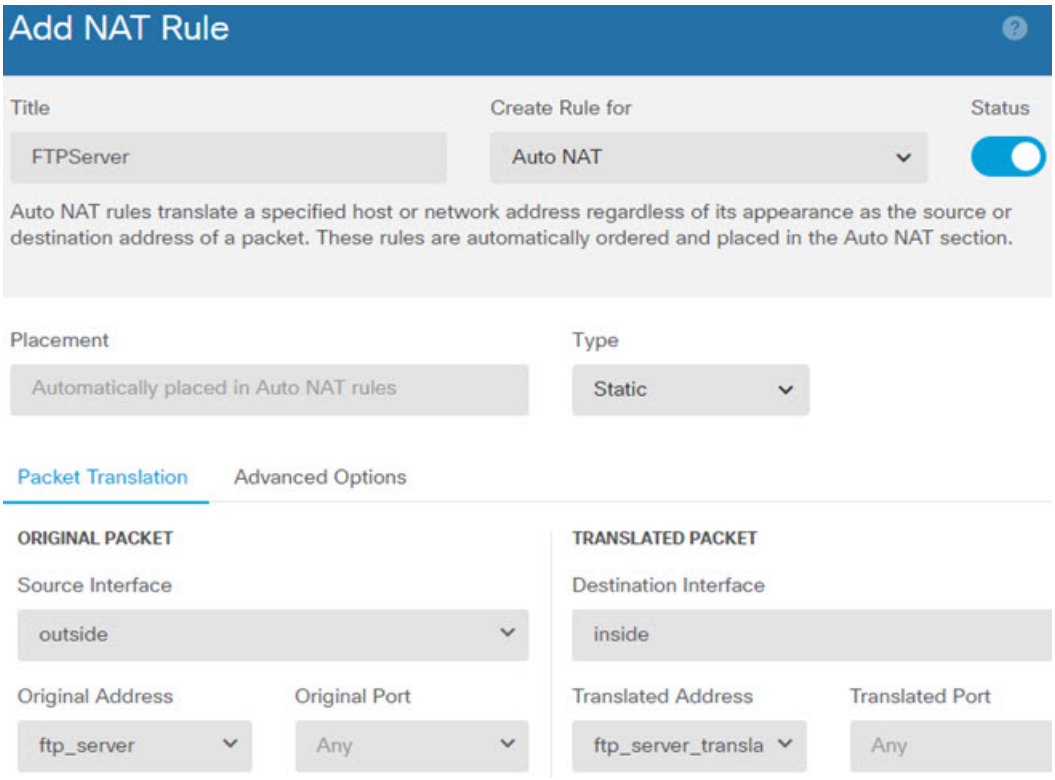


d) [追加（Add）][OK]をクリックします。
e) [+]をクリックして FTP サーバの変換済みアドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server_translated など）、[ホスト（Host）]を選択して、ホスト アドレス 10.1.2.56 を入力します。



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。



d) [OK]をクリックします。

第 III 部

システム管理

第 11 章

システム設定

ここでは、[システム設定（System Settings）] ページでグループ化されているさまざまなシステム設定の設定方法について説明します。設定は、システムの機能全体を網羅しています。

管理アクセス リストの設定

デフォルトでは、任意の IP アドレスから、デバイスの Firepower Device Manager ウェブまたは管理アドレスの CLI インターフェイスにアクセスできます。システム アクセスは、ユーザ名/パスワードのみで保護されています。ただし、特定の IP アドレスまたはサブネットのみからの接続を許可するようアクセス リストを設定し、さらにレベルの高い保護を提供することができます。

注意 特定のアドレスへのアクセスを制限すると、システムから簡単にロックアウトできます。現在使用している IP アドレスへのアクセスを削除し、「任意」のアドレスへのエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。アクセス リストを設定する場合は、特に注意してください。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックし、[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ページにアクセスしている場合、目次の [管理アクセス リスト（Management Access List）]をクリックします。

ルールのリストは、指定したポートへのアクセスが許可されるアドレスを定義します。Firepower Device Manager（HTTPS Web インターフェイス）の場合は 443、SSH CLI の場合は 22 です。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

（注） ルールを削除するには、ルールの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 2 管理アドレスのルールを作成するには、以下の手順に従います。

a) [+]をクリックし、次のオプションを入力します。

- [プロトコル（Protocol）] : ルールが HTTPS（ポート 443）または SSH（ポート 22）用かを選択します。
- [IP アドレス（IP Address）] : システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4](0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

b) [追加（Add）]をクリックします。

診断ロギングの設定

診断ロギングは、接続に関係していないイベントの syslog メッセージを提供します。個々のアクセス コントロール ルール内に接続ロギングを設定します。次に、診断メッセージのロギングを設定する方法について説明します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [ロギングの設定（Logging Settings）] リンクをクリックします。
[システム設定（System Settings）]ページをすでに開いている場合、目次の[ロギングの設定（Logging Settings）]をクリックします。

ステップ 2 [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い限り、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 メッセージを表示する各々の場所のスライダを[オン（On）]にしてから、最小重大度レベルを選択します。
次の場所にメッセージをロギングすることができます。

- [コンソール（Console）]：コンソール ポートの CLI にログインすると診断ログ メッセージが表示されます。**show console-output** コマンドを使用して、他のインターフェイス（管理アドレスを含む）への SSH セッションでこれらのログを表示することもできます。
- [Syslog]：診断ログ メッセージは、指定した外部 syslog サーバに送信されます。[+]をクリックして、syslog サーバの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すでに存在しなくなっている場合、[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です。
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**	警告状態です。
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（緊急）の syslog メッセージを生成しません。

DHCP サーバの設定

DHCP サーバは、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。Firepower Threat Defenseデバイスは、インターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。DHCP サーバは、ネットワーク構成パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャスト アドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。DHCP サーバは、BOOTP 要求をサポートしていません。

DHCP クライアントは、サーバが有効になっているインターフェイスと同じネットワークに属している必要があります。つまり、スイッチがあるとしても、サーバとクライアントの間にルータを介在させることはできません。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [DHCP サーバ（DHCP Server）] リンクをクリックします。
[システム設定（System Settings）]ページをすでに開いている場合、目次の [DHCP サーバ（DHCP Server）]をクリックします。

リストには、DHCP サーバを設定したインターフェイスと、サーバが有効にされているかどうか、そしてサーバのアドレス プールが表示されます。

（注） サーバを削除するには、サーバのごみ箱アイコン（）をクリックします。

ステップ 2 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で DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

a) 自動設定を利用する場合、[自動設定を有効にする（Enable Auto Configuration）]>[オン（On）] をクリックしてから（スライダは右側に移動）、は、DHCP を介してアドレスを取得するインターフェイスを [次のインターフェイスから取得（From Interface）] で選択します。
b) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、次のグローバル オプションを設定します。これらの設定は、DHCP サーバをホストするすべてのインターフェイスで DHCP クライアントに送信されます。

- [プライマリ WINS IP アドレス（Primary WINS IP Address）]、[セカンダリ WINS IP アドレス（Secondary WINS IP Address）] ：Windows インターネット ネーム サービス（WINS）サーバ クライアントのアドレスは、NetBIOS の名前解決に使用されます。

- [プライマリDNS IP アドレス（Primary DNS IP Address）]、[セカンダリ DNS IP アドレス（Secondary DNS IP Address）]：ドメイン ネーム サーバ（DNS）のサーバ クライアントのアドレスは、ドメインの名前解決に使用されます。OpenDNS パブリック DNS サーバを設定するには、[OpenDNS を使用する（Use OpenDNS）]をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

c) [保存（Save）]をクリックします。

ステップ 3 次のいずれかを実行します。

- まだリストされていないインターフェイスのDHCPサーバを設定するには、[+]をクリックします。
- 既存のDHCPサーバを編集するには、そのサーバの編集アイコン（  ）をクリックします。

ステップ 4 サーバ プロパティを設定します。

- [DHCP サーバを有効にする（Enable DHCP Server）]：サーバを有効にするかどうかを決定します。サーバを設定することができますが、使用する準備が整うまでサーバは無効にしておきます。
- [インターフェイス（Interface）]：クライアントにDHCPアドレスを提供するインターフェイスを選択します。インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバを実行する場合、インターフェイス アドレスの取得に DHCP を使用することはできません。
- [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り、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。プールの開始アドレスと終了アドレスをハイフンで区切って指定します。たとえば、10.100.10.12-10.100.10.250 のように指定します。

ステップ 5 新しいサーバの [追加（Add）]と、既存のサーバの [保存（Save）] をクリックします。

DNS の設定

ドメインネームシステム（DNS）サーバは、IPアドレスのホスト名の解決に使用されます。これらのサーバは管理インターフェイスによって使用されます。DNS サーバは初期システム設定の際に設定しますが、次のプロシージャを使用して設定を変更することができます。

configure network dns servers コマンドと **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可能です。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [DNS サーバ（DNS Server）] リンクをクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [DNS サーバ（DNS Server）]をクリックします。

ステップ 2 [プライマリ、セカンダリ、ターシャリ DNS IP アドレス（Primary, Secondary, Tertiary DNS IP address）]に、DNS サーバの IP アドレスを優先順位に従って 3 つまで入力します。
使用していたプライマリ DNS サーバからの応答がなくなると、セカンダリが使用され、最後にターシャリが使用されます。

OpenDNS パブリック DNS サーバを設定するには、[OpenDNS を使用する（Use OpenDNS）]をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

ステップ 3 [ドメイン検索名（Domain Search Name）]に、example.com などのネットワークのドメイン名を入力します。
このドメインは、完全修飾されていないホスト名に追加されます（たとえば serverA.example.com ではなく serverA のようなホスト名）。

ステップ 4 [保存（Save）]をクリックします。

管理 IP アドレスの設定

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。これは、Firepower Device Manager の Web インターフェイス および CLI にアクセスするアドレスです。

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。または、CLIから設定する場合は、DHCP または IPv6 自動設定を使用するように管理インターフェイスを設定できます。

⚠

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 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 メニューでデバイスの名前をクリックし、[システム設定（System Settings）] > [デバイス管理 IP（Device Management IP）] 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 [デバイス管理 IP（Device Management IP）] をクリックします。

ステップ 2 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。

ステップ 3 [保存（Save）]をクリックして警告を読み、[OK] をクリックします。

デバイスのホスト名の設定

デバイス ホスト名を変更できます。

CLI で **configure network hostname** コマンドを使用してホスト名を変更することもできます。

注意 ホスト名を使用してシステムに接続しているときにホスト名を変更すると、変更はただちに適用されるため、変更を保存するときに Firepower Device Manager へのアクセスが失われます。デバイスに接続し直す必要があります。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名、[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 サーバは初期システム設定の際に設定しますが、次のプロシージャを使用して設定を変

更することができます。NTP 接続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，（296 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックしてから、[システム設定（System Settings）] > [NTP] リンクをクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [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、独自のサーバを（手動で）使用するか、シスコのタイム サーバを使用するかどうかを選択します。

- [Cisco NTP タイム サーバ（Cisco NTP Time Server）][デフォルト NTP タイム サーバ（Default NTP Time Server）]：このオプションを選択すると、NTP で使用されるサーバ名がサーバ一覧に表示されます。
- [手動入力（Manually Input）]：このオプションを選択する場合、使用する NTP の完全修飾ドメイン名または IP アドレスを入力します。たとえば、ntp1.example.com または 10.100.10.10 と入力します。複数の NTP サーバが存在する場合、[別の NTP タイム サーバを追加する（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 集合型セキュリティ インテリジェンス （CSI）の クラウド の基本設定の設定

システムは、レピュテーション、リスク、脅威インテリジェンスに関して Cisco 集合型セキュリティ インテリジェンス（CSI）を使用します。

URL フィルタリングと FirePOWER の AMP（マルウェア ファイル ポリシーに使用）に必要なライセンスを保有している場合、システムは、これらの機能を自動的に有効にし、Cisco CSI から必要な情報を取得するための通信を有効にします。とはいえ、通信を制御するためのオプションの一部はユーザが設定できます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックしてから、[システム設定（System Settings）] > [クラウドの基本設定（Cloud Preferences）] の順にクリックします。
[システム設定（System Settings）] ページをすでに開いている場合、目次の [クラウドの基本設定（Cloud Preferences）]と [URL フィルタリングの基本設定（Filtering Preferences）]をクリックします。

ステップ 2 次のオプションを設定します。

- [自動更新の有効化（Enable Automatic Updates）]：カテゴリとレピュテーションを含む更新された URL データをチェックしてダウンロードすることをシステムに許可します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。デフォルトでは、更新が有効になっています。このオプションを選択解除した状態でカテゴリとレピュテーションのフィルタリングを使用している場合、このオプションを周期的に有効にして新しい URL データを取得してください。
- [不明な URL に対する Cisco CSI のクエリ （Query Cisco CSI for Unknown URLs）]：ローカル URL フィルタリング データベースのカテゴリおよびレピュテーションのデータを含まない URL の更新情報を Cisco CSI でチェックするかどうかを切り替えます。ルックアップが適度な制限時間内に更新情報を返した場合、その情報は、URL の状況に基づいてアクセス ルールを選択する際に使用されます。それ以外の場合、URL は分類されていないカテゴリと照合されます。

ステップ 3 [保存（Save）]をクリックします。

第 12 章

システム管理

ここでは、システム データベースの更新やシステムのバックアップおよび復元などの、システム管理タスクの実行方法について説明します。

ソフトウェア アップデートのインストール

システムデータベースとシステム ソフトウェアの更新プログラムをインストールできます。ここでは、これらの更新プログラムのインストール方法について説明します。

システム データベースの更新

システムは複数のデータベースを使用して高度なサービスを提供しています。シスコは、セキュリティ ポリシーが利用可能な最新の情報を使用できるように、これらのデータベースの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

新しい脆弱性が出現すると、Cisco Talos Security Intelligence and Research Group（Talos）は、ユーザがインポートできる侵入ルールの更新をリリースします。この更新は、侵入ルール、プリプロセッサ ルール、およびそのルールを使用するポリシーに影響します。

侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。

侵入ルールの更新によって行われた変更を有効にするには、設定を再展開する必要があります。

侵入ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに実行してください。

位置情報データベース（GeoDB）

シスコの位置情報データベース（GeoDB）は、ルート可能な IP アドレスに関連する位置情報データ（国、都市、緯度と経度の座標など）、および接続関係のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。

GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセス コントロール ルールとして使用できます。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30～40 分かかります。GeoDB の更新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）

シスコの脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。Firepower システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco Talos Security Intelligence and Research Group（Talos）は、VDB に定期的な更新を発行します。

脆弱性のマッピングを更新するのにかかる時間は、ネットワーク マップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、更新されたアプリケーション ディテクタとオペレーティング システム フィンガープリントを有効にするために、設定を再展開する必要があります。

システム データベースの更新

必要に応じて、手動でシステム データベースの更新を取得して適用することができます。更新はシスコサポート サイトから取得されます。したがって、システムの管理アドレスからインターネットへのパスが存在する必要があります。

またデータベースの更新を取得して適用するよう、定期的なスケジュールを設定することもできます。これらの更新はサイズが大きい場合があるため、ネットワーク アクティビティが少ない時間帯にスケジュールしてください。

（注） データベース更新が進行中の場合、ユーザ インターフェイスのアクションへの応答が遅くなる場合があります。

はじめる前に

保留中の変更に対して潜在的な影響を与えることを避けるため、これらのデータベースを手動で更新する前に、デバイスに設定を展開します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックし、[更新サマリ（Updates summary）] の [設定の表示（View Configuration）] をクリックします。
これによって、[更新（Updates）] ページが開きます。このページの情報には、各データベースの現在のバージョン、および各データベースの最終更新日時が表示されます。

ステップ 2 手動でデータベースを更新するには、そのデータベースのセクションで [今すぐ更新（Update Now）]をクリックします。
更新をダウンロードして適用した後、更新された情報を使用できるよう、ポリシーがデバイスに自動的に再展開されます。

ステップ 3 （オプション）定期的なデータベース更新スケジュールを設定するには、次の手順に従います。

a) 目的のデータベースのセクションで[設定（Configure）]リンクをクリックします。すでにスケジュールが設定されている場合、[編集（Edit）]をクリックします。
データベースの更新スケジュールは独立しています。スケジュールは別途定義する必要があります。

b) 更新開始時刻を設定します。

- 更新の頻度（日次、週次、または月次）。
- 週次または月次の場合、更新が必要な曜日または日付。
- 更新を開始する時刻。

c) [保存（Save）]をクリックします。

（注） 定期的なスケジュールを削除する場合、[編集（Edit）]リンクをクリックしてスケジューリング ダイアログボックスを開き、[削除（Remove）] ボタンをクリックします。

Firepower Threat Defenseソフトウェアのアップグレード

Firepower Threat Defenseソフトウェア アップグレードが使用可能になると、インストールできます。次の手順は、システム上ですでに Firepower Threat Defenseソフトウェアが稼働していて、正常に動作していることを前提としています。

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。

はじめる前に

保留中の変更を展開し、展開が完了するまで待ちます（確認するには、タスク リストを参照してください）。保留中の変更があると、アップグレードを適用することはできません。

次に、Firepower Device Manager をログアウトします。ソフトウェアのアップグレード中、設定の変更は行わないでください。

アップグレード中、すべてのイベントが消去されます。

手順

ステップ 1 アップグレード イメージを取得し、インストールの準備をします。

a) 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 の適切なアップグレード ファイルを取得します。システム ソフトウェア パッケージまたはブート イメージをダウンロードしないでください。
- アップグレード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。

b) 管理 IP アドレスからアクセスできる HTTP サーバにイメージを置きます。
または、TFTP または SCP を使用してファイルをダウンロードすることもできます。これらのオプションのいずれかを選択する場合、これらのファイル転送プロトコルをサポートするサーバにファイルを置きます。

ステップ 2 SSH クライアントを使用し、[管理者（admin）]ユーザ アカウントとパスワードを使用して管理 IP アドレスにログインします。
または、コンソール ポートに接続することもできます。

ステップ 3 エキスパート モードにアクセスするには、**expert** コマンドを入力します。

```
> expert
admin@firepower:~$
```

ステップ 4 作業ディレクトリ（**cd**）を /var/sf/updates/ に変更します。

```
admin@firepower:~$ cd /var/sf/updates/
```

```
admin@firepower:/var/sf/updates$
```

ステップ 5 HTTP サーバからアップグレード ファイルをダウンロードします。
sudo wget*url*

たとえば次のコマンドは、架空の Cisco_FTD_Upgrade-6.2.0-181.sh アップグレード ファイルを files.example.com HTTP サーバの ftd フォルダからダウンロードします。**sudo** コマンドは root ユーザの下で動作するため、ストック警告が表示されます。このコマンドを実行する前に、[管理者（admin）] パスワードを再入力する必要があります。ダウンロードが完了するまで待ちます。

```
admin@firepower:/var/sf/updates$ sudo wget
http://files.example.com/ftd/Cisco_FTD_Upgrade-6.2.0-181.sh

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password: (enter admin password)
Connecting to files.example.com
|***********************************************
***********************************************
***********************************************
***********************************************
*********************************|

...(remaining output omitted)
```

HTTP サーバを使用していない場合、代わりに **tftp** または **scp** コマンドを使用します。

ステップ 6 アップグレード ファイルをインストールします。
sudo install_update.pl/var/sf/updates/*filename*

コマンドにアップグレードファイルへのフルパスを含める必要があります。次に例を示します。

```
admin@firepower:/var/sf/updates$ sudo
install_update.pl /var/sf/updates/Cisco_FTD_Upgrade-6.2.0-181.sh
(output omitted)
```

ステップ 7 インストールが完了するまで待機します。インストールが完了したら再起動されます。
インストールには 30 分以上かかることがあります。

ステップ 8 インストールが完了したことを確認します。
SSH クライアントを使用し、[管理者（admin）]ユーザ アカウントとパスワードを使用して管理 IP アドレスにログインします。バナー情報には、新しいビルド番号が表示される行（強調表示される）が含まれます。たとえば次の出力は、現在のFirepower Threat Defenseのバージョンが 6.2.0-181

であり、例の更新ファイルと一致していることを示しています。**show version** コマンドでもソフトウェア バージョン情報が表示されます。

```
Password:

Last login: Fri May 6 14:42:18 2016 from 10.152.242.234

Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 22)
Cisco ASA5512-X Threat Defense v6.2.0 (build 181)

>
```

デバイスの再イメージ化

デバイスを再イメージ化すると、デバイス設定が消去され、新しいソフトウェア イメージがインストールされます。再イメージ化の目的は、工場出荷時のデフォルト設定でクリーン インストールすることです。

次の場合に、デバイスを再イメージ化します。

- ASA ソフトウェアからFirepower Threat Defenseソフトウェアにシステムを変換する場合。ASA イメージを実行しているデバイスを Firepower Threat Defenseイメージを実行しているデバイスにアップグレードすることはできません。
- デバイスが 6.1.0 以前のイメージを実行していて、6.1 以降のイメージにアップグレードし、Firepower Device Manager を使用してデバイスを設定したい場合。Firepower Management Center を使用して、6.1 以前のデバイスをアップグレードしてからローカル管理を切り替えることはできません。
- デバイスが正しく機能せず、設定の修正ですべての試行が失敗した場合。

デバイスの再イメージ化の詳細については、ご使用のデバイス モデルの『*Reimage the Cisco ASA or Firepower Threat Defense Device*』または *Firepower Threat Defense* のクイック スタート ガイドを参照してください。これらのガイドは、http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html で入手できます。

システムのバックアップと復元

後の設定ミスまたは物理的な事故が原因で設定が損なわれた場合にデバイスを復元できるように、システム設定をバックアップできます。

代替のデバイスにバックアップを復元できるのは、2台のデバイスが同じモデルで、同じバージョンのソフトウェアを実行している場合です。アプライアンス間でコンフィギュレーションをコピーする目的で、バックアップと復元のプロセスを使用しないでください。バックアップ ファイルには、この方法で共有することができないようにアプライアンスを一意に特定する情報が含まれます。

（注） バックアップには管理 IP アドレス設定は含まれません。そのため、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 コピーから置換されません。これにより、アドレスに行ったいかなる変更も保持され、別のネットワーク セグメント上のさまざまなデバイスの設定を復元することも可能になります。

バックアップには設定だけが含まれ、システム ソフトウェアは含まれません。デバイスを完全に最イメージングする必要がある場合、ソフトウェアを再インストールしてからバックアップをアップロードして、設定を回復する必要があります。

バックアップ中は設定データベースがロックされます。バックアップの間はポリシー、ダッシュボードなどを表示できますが、設定を変更することはできません。復元を行っている間、システムは完全に使用できません。

「バックアップと復元」ページの表は、バックアップのファイル名、作成日時、ファイル サイズを含む、システムで使用できる既存のすべてのバックアップ コピーを示します。バックアップのタイプ（手動、スケジュール、繰り返し）は、システムに指示したバックアップ コピーの作成方法に基づいています。

ヒント バックアップ コピーはシステム自体に作成されます。ディザスタ リカバリのために必要なバックアップ コピーを確保するため、バックアップ コピーは手動でダウンロードし、安全なサーバに保存する必要があります。

次に、バックアップの管理と復元操作について説明します。

システムの即時バックアップ

希望する場合はいつでもバックアップを開始できます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックして、[バックアップと復元（Backup and Restore）] の概要ページで [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）] ページが開きます。表に、システムで使用可能なすべての既存のバックアップ コピーが一覧されます。

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。

今すぐではなく、将来のある時刻にバックアップする場合は、代わりに[スケジュール（Schedule）]をクリックすることができます。

ステップ 4 [今すぐバックアップ（Back Up Now）]をクリックします。
システムがバックアップ プロセスを開始します。バックアップが完了すると、バックアップ ファイルが表に表示されます。必要に応じて、バックアップ コピーをシステムにダウンロードして、他の場所に保存することができます。

バックアップが開始されたら、[バックアップと復元（Backup and Restore）] ページを閉じてもかまいません。

スケジュールされた時間でのシステムのバックアップ

システムを将来の特定の日時にバックアップするために、スケジュール バックアップを設定できます。スケジュール バックアップは、1 回だけ実行されます。定期的にバックアップを作成するようにバックアップ スケジュールを作成するには、スケジュール バックアップではなく、繰り返しバックアップを設定します。

（注） 将来のバックアップのスケジュールを削除するには、スケジュールを編集して、[削除（Remove）]をクリックします。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名をクリックして、[バックアップと復元（Backup and Restore）] の概要ページで [設定の表示（View Configuration）] をクリックします。

ステップ 2 [スケジュール バックアップ（Scheduled Backup）] > [バックアップをスケジュール（Schedule a Backup）] をクリックします。
すでにスケジュール バックアップがある場合は、[スケジュール バックアップ（Scheduled Backup）] > [編集（Edit）] をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 バックアップの日時を入力します。

ステップ 5 [スケジュール（Schedule）]をクリックします。
選択した日時に達すると、システムがバックアップされます。完了すると、バックアップ コピーがバックアップの表に一覧されます。

定期的なバックアップ スケジュールの設定

定期的なバックアップを設定し、システムを定期的にバックアップすることができます。たとえば、毎週金曜日の真夜中にバックアップをとることもできます。定期的なバックアップ スケジュールにより、常に最新のバックアップ セットを保持できます。

（注） 定期的なスケジュールを削除する場合、スケジュールを編集し、[削除（Delete）]をクリックします。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックし、[バックアップおよび復元サマリ（Backup and Restore summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 [定期的なバックアップ（Recurring Backup）] > [設定（Configure）] をクリックします。
すでに定期的なバックアップが設定されている場合、[定期的なバックアップ（Recurring Backup）] > [編集（Edit）] をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 [頻度（Frequency）]と関連スケジュールを選択します。

- [日次（Daily）] : 時刻を選択します。バックアップは毎日、スケジュールされた時刻に取得されます。
- [週次（Weekly）] : 曜日と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、毎週月曜日、水曜日、金曜日の 23 時（午後 11 時）にバックアップをスケジュールすることもできます。
- [月次（Monthly）] : 日付と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、1 日、15 日、28 日の 23 時（午後 11 時）にバックアップをスケジュールすることもできます。

ステップ 5 [保存（Save）]をクリックします。
選択した日付と時刻になると、バックアップが取得されます。完了すると、バックアップ コピーがバックアップ テーブルにリストされます。

定期的なスケジュールを変更または削除するまで、バックアップを取得し続けます。

バックアップの復元

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に存在しない場合、復元する前にまずバックアップをアップロードする必要があります。

復元している間、システムは全く使用できません。

（注） バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワーク セグメント上の別のデバイスに設定を復元することもできます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックし、[バックアップおよび復元サマリ（Backup and Restore summary）] の [設定の表示（View Configuration）] をクリックします。
これにより、[バックアップおよび復元（Backup and Restore）] ページが開きます。使用可能なすべての既存のバックアップ コピーが表にリストされています。

ステップ 2 復元しようとするバックアップ コピーが、使用可能なバックアップのリストにない場合、[アップロード（Upload）] > [検索（Browse）] をクリックし、バックアップ コピーをアップロードします。

ステップ 3 ファイルの [復元（restore）] アイコン（）をクリックします。
復元するかどうかの確認が求められます。デフォルトでは、復元後にバックアップ コピーは削除されますが、これを保持するには、復元を続行する前に、[復元後にバックアップを削除しない（Do not remove the backup after restoring）]を選択します。

復元が完了すると、システムは再起動します。

ステップ 4 システムが起動して稼働したら、[展開（Deploy）]ボタンをクリックし、設定を再展開します。

バックアップ ファイルの管理

新しいバックアップを作成すると、バックアップ ファイルがバックアップと復元ページに表示されます。バックアップ コピーは無期限に保たれません。デバイスのディスク領域の利用量が最大しきい値に達すると、新しいバックアップコピー用の場所を空けるために、古いバックアップコピーが削除されます。したがって、定期的にバックアップ ファイルを管理し、最も保持したい特定のバックアップ コピーが削除されていないことを確認してください。

バックアップ コピーを管理するには、次の操作を行うことができます。

- ファイルを安全なストレージにダウンロード：バックアップファイルをワークステーションにダウンロードするには、ファイルのダウンロードアイコン（）をクリックします。その後、安全なファイル ストレージにファイルを移動できます。
- システムにバックアップ ファイルをアップロードする：デバイスで使用できなくなったバックアップ コピーを復元するには、[アップロード（Upload）] > [ファイルを参照（Browse

File）] をクリックしてワークステーションからアップロードします。その後、復元できます。

（注） アップロードされたファイルは、元のファイル名と一致するように名前が変更される場合があります。また、システムに 10 以上のバックアップ コピーがすでに存在する場合、アップロードされたファイル用の場所を空けるために最も古いものは削除されます。古いソフトウェア バージョンによって作成されたファイルをアップロードすることはできません。

- バックアップを復元する：バックアップ コピーを復元するには、ファイルの復元アイコン（）をクリックします。復元の間システムは使用できなくなり、復元が完了するとリブートします。システムが稼働していて、動作中になってから設定を展開してください。
- バックアップ ファイルを削除する：特定のバックアップが必要でなくなったら、ファイルの削除アイコン（）をクリックします。削除の確認が求められます。削除すると、バックアップ ファイルを回復することはできません。

システムの再起動

システムが正常に動作していないときに、他の問題解決手段では解決しない場合は、デバイスを再起動できます。デバイスは CLI から再起動する必要があります。Firepower Device Manager からは再起動できません。

手順

ステップ 1 SSH クライアントを使用して管理 IP アドレスへの接続を開き、Configuration CLI 権限があるユーザ名でデバイスの CLI にログインします。たとえば、admin ユーザ名を使用します。

ステップ 2 **reboot** コマンドを入力します。

例：

```
> reboot
```

システムのトラブルシューティング

ここでは、いくつかのシステムレベルのトラブルシューティングのタスクおよび機能について説明します。特定の機能（アクセス コントロールなど）のトラブルシューティングの詳細については、その機能に関する章を参照してください。

接続をテストするための ping アドレス

pingは、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。これは基本接続が機能していることを意味します。ただし、デバイスで実行されている他のポリシーにより、特定のタイプのトラフィックは正常にデバイスを通過できないことがあります。デバイス CLI にログインすることで ping を使用できます。

（注） システムには複数のインターフェイスがあるため、アドレスのpingに使用されるインターフェイスを制御できます。接続をテストすることが重要であるため、確実に正しいコマンドを使用する必要があります。たとえば、システムは仮想管理インターフェイスを介してシスコ ライセンス サーバに到達できる必要があるため、**ping system** コマンドを使用して接続をテストする必要があります。**ping** を使用すると、データ インターフェイスを介してアドレスに到達できるかどうかをテストしており、同じ結果にならない可能性があります。

通常の ping は、ICMP パケットを使用して接続をテストします。ネットワークで ICMP が禁止されている場合は、代わりに TCP ping を使用できます（データ インターフェイスの ping のみ）。

次に、ネットワーク アドレスを ping するための主なオプションを示します。

仮想管理インターフェイスを介したアドレスの ping

ping system コマンドを使用します。

ping system*host*

ホストは IP アドレスまたは完全修飾ドメイン名（FQDN）（www.example.com など）にすることができます。データ インターフェイスを介した ping とは違い、システム ping のデフォルト数はありません。pingはCtrl+cを使用して停止するまで続けられます。次に例を示します。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

ルーティング テーブルを使用するデータ インターフェイスを介したアドレスの ping

ping コマンドを使用します。インターフェイスを指定せずに、システムが一般的にホストへのルートを検索できるかどうかをテストします。システムは通常このようにしてトラフィックをルーティングするため、一般的に実行する必要があるのはこのテストです。

ping*host*

ホストの IP アドレスを指定します。FQDN しかわからない場合は、**nslookup***fqdn-name* コマンドを使用して IP アドレスを特定します。次に例を示します。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

（注） タイムアウト、繰り返し回数、パケット サイズ、さらには送信するデータ パターンを指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

特定のデータ インターフェイスを介したアドレスの ping

特定のデータ インターフェイスを介して接続をテストするには、**pinginterface***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。

pinginterface*if_namehost*

ホストの IP アドレスを指定します。FQDN しかわからない場合は、**nslookup***fqdn-name* コマンドを使用して IP アドレスを特定します。次に例を示します。

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping を使用するデータ インターフェイスを介したアドレスの ping

ping tcp コマンドを使用します。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。

ping tcp [**interface***if_name*] *hostport*

ホストと TCP ポートを指定する必要があります。FQDN しかわからない場合は、**nslookup***fqdn-name* コマンドを使用して IP アドレスを特定します。

オプションで、ping を送信するインターフェイスではなく、ping の送信元インターフェイスであるインターフェイスを指定できます。このタイプの ping では、必ずルーティング テーブルを使用します。

TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。次に例を示します。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

（注） タイムアウト、繰り返し回数、および TCP ping の送信元アドレスも指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワーク パスに問題がないかどうかを確認できます。トレースルートでは、宛先に対して、無効なポートで UDP パケットを送信したり、ICMPv6 エコーを送信したりします。宛先までの途中にあるルータから ICMP Time Exceeded メッセージが返され、トレースルートにそのエラーが報告されます。各ノードは 3 つのパケットを受信するため、有益な結果を得る機会が 1 台のノードにつき 3 回あります。デバイス CLI にログインすることで、トレースルートを使用できます。

（注） データ インターフェイスを介してルートを追跡するためのコマンド（**traceroute**）、または仮想管理インターフェイスを介してルートを追跡するためのコマンド（**traceroute system**）があります。適切なコマンドを使用するようにしてください。

次の表に、パケットによって出力に表示される可能性のある結果を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。

出力記号	説明
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 が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

仮想管理インターフェイスを介したルートの追跡

traceroute system コマンドを使用します。

traceroute system*destination*

ホストには、IPv4/IPv6 アドレスまたは完全修飾ドメイン名（FQDN）（www.example.com など）を使用できます。次に例を示します。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

データ インターフェイスを介したルートの追跡

traceroute コマンドを使用します。

traceroute*destination*

ホストの IP アドレスを指定します。FQDN しかわからない場合は、**nslookup***fqdn-name* コマンドを使用して IP アドレスを特定します。次に例を示します。

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

（注） タイムアウト、パケット存続時間、1 ノードあたりのパケット数、およびトレースルートの送信元として使用する IP アドレスまたはインターフェイスを指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

NTP のトラブルシューティング

システムは、正確で一貫性のある時間に基づいて正しく動作し、イベントやその他のデータ ポイントを正確に処理します。少なくとも 1 つ、理想的には 3 つの Network Time Protocol（NTP）サーバで、システムが常に信頼できる時間情報を取得できるようにする必要があります。

デバイスの接続概要図（メイン メニューで [デバイス（Device）]をクリック）に、NTP サーバへの接続ステータスが示されます。ステータスが黄色またはオレンジ色の場合、設定したサーバへの接続に問題があります。接続の問題が解消されない（一時的な問題ではない）場合は、次の操作を試します。

- まず、[デバイス（Device）] > [システム設定（System Settings）] > [NTP（NTP）] で 3 つ以上の NTP サーバが設定されていることを確認します。これは要件になっていませんが、NTP サーバが 3 つ以上あると信頼性が大幅に向上します。
- 管理インターフェイス IP アドレス（[デバイス（Device）]>[システム設定（System Settings）] >[管理インターフェイス（Management Interface）] で定義される）と NTP サーバの間にネットワーク パスがあることを確認します。

  デバイス CLI にログインし、ping system コマンドを使用して、各 NTP サーバへのネットワーク パスがあるかどうかテストします。
- デバイス CLI にログインし、次のコマンドを使用して NTP サーバのステータスを確認します。

- **show ntp**：このコマンドは、NTP サーバの基本情報とその可用性を表示します。ただし、Firepower Device Manager の接続ステータスではその他の情報を使用してステータスを示すため、このコマンドが示す内容や接続ステータス図が示す内容と一致しないことがあります。
- **system support ntp**：このコマンドには、**show ntp** の出力と、NTP プロトコルによってドキュメント化される標準の NTP コマンド **ntpq** の出力が含まれます。NTP 同期を確認する必要がある場合は、このコマンドを使用します。

  「Results of 'ntpq -pn」の部分を探します。たとえば、次のように表示されます。

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

  この例では、NTP サーバアドレスの前にある + は潜在的な候補であることを示します。アスタリスク * は、現在の時刻源のピアを示します。

  NTP デーモン（NTPD）は、各ピアの 8 つのスライディング ウィンドウ サンプルを使用して 1 つのサンプルを選択します。その後、クロックの選択によって正しいチャイマーと不正なチッカーが特定されます。次に、NTPD がラウンドトリップ距離を特定します（候補のオフセットをラウンドトリップ遅延の半分以上にすることはできません）。接続の遅延、パケットの損失、またはサーバの問題が発生して 1 つまたはすべての候補が拒否されると、同期中に長い遅延が生じます。また、調整にも非常に長い時間がかかります。クロック規律アルゴリズムによって、クロック オフセットおよびオシレータ エラーを解決する必要がありますが、これには数時間かかる可能性があります。

  （注） refid が .LOCL. の場合は、ピアが無規律のローカル クロックであることを示します。つまり、時間設定にそのローカル クロックのみを使用します。選択したピアが .LOCL. の場合、Firepower Device Manager は NTP 接続を常に黄色（非同期）にマークします。通常 NTP は、より適切な候補を利用できる場合、.LOCL. 候補を選択しません。そのため、サーバを 3 つ以上設定する必要があります。

CPU およびメモリ使用率の分析

CPU およびメモリの使用率に関するシステム 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、CPU とメモリの棒グラフを検索します。これらのグラフは、**show cpu system** および **show memory system** コマンドを使用して CLI から収集した情報を示します。

CLI にログインすると、これらのコマンドの追加バージョンを使用して他の情報を見ることができます。通常、この情報を確認するのは使用状況に関する永続的な問題がある場合や、Cisco Technical Assistance Center（TAC）の指示があった場合に限られます。詳細情報の多くは複雑で、TAC の解釈が必要です。

以下に、調べることができるいくつかのポイントを示します。これらのコマンドについての詳細情報は、http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.htmlの「*Firepower Threat Defense* のコマンド リファレンス」[英語]をご覧ください。

- **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、追加のコアごと、および全体的なデータ プレーン CPU の使用率を表示します。
- **show memory** は、データ プレーンのメモリ使用率を表示します。

（注） キーワード（上述されていない）の中には、**cpu** または **memory** コマンドを使用して最初にプロファイルその他の機能の設定が必要な場合があります。これらの機能は、TAC の指示があった場合のみ使用します。

ログの表示

システムはさまざまなアクションに関する情報をログに記録します。システム ログを開くには、**system support view-files** コマンドを使用します。Cisco Technical Assistance Center（TAC）への問い合わせ時にこのコマンドを使用すると、出力を解釈して、適切なログを表示できるようになります。

コマンドは、ログを選択するためのメニューを表示します。ウィザードに移動するには、次のコマンドを使用します。

- サブディレクトリに変更するには、ディレクトリの名前を入力して、Enter を押します。
- 表示するファイルを選択するには、プロンプトで **s** と入力します。その後、ファイル名の入力が求められます。完全な名前を入力する必要があります。大文字と小文字は区別されます。ファイル リストにはログのサイズが示されます。非常に大きいログを開く前には検討が必要な場合があります。
- 「--More--」が表示されたら Space キーを押してログ エントリの次のページを表示します。次のログ エントリのみを表示するには Enter を押します。ログの最後に到達すると、メインメニューに戻ります。「--More--」の行には、ログのサイズと表示した量が示されます。**ログのすべてのページを表示する必要がなく、ログを閉じて、コマンドを終了するには、Ctrl+C を使用します。**
- メニューまでの構造内で 1 つ上のレベルに移動するには、**b** を入力します。

新しいメッセージが追加されたときにそれらを確認できるように、ログを開いたままにするには、**system support view-files** ではなく **tail-logs** コマンドを使用します。

次の例は、システムへのログイン試行を追跡する cisco/audit.log ファイルがどのように表示されるかを示しています。ファイル リストは、最上位のディレクトリで始まり、その後、現在のディレクトリ内のファイル リストが続きます。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
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       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,


<remaining log truncated>
```

トラブルシューティング ファイルの作成

問題レポートを提出した際に、Cisco Technical Assistance Center（TAC）の担当者により、システム ログ情報の提出を求められることがあります。この情報は、問題の診断に役立ちます。診断ファイルの提出は、求められた場合だけでかまいません。

次の手順では、ログ レベルを設定して診断ファイルを作成する方法について説明します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名。

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

ここでは、皆無ではありませんが、頻繁には実行しないアクションについて取り上げます。これらのアクションはすべて、デバイス設定を消去します。これらの変更を行う前に、デバイスが現在、実稼働ネットワークに重要なサービスを提供していないことを確認してください。

ローカル管理とリモート管理の切り替え

デバイスに直接ホストされているローカルの Firepower Device Manager を使用し、またはリモートでFirepower Management Centerの複数のデバイス マネージャを使用して、デバイスを設定および管理できます。Firepower Device Manager でサポートされていない機能を設定する場合、または Firepower Management Centerで使用可能な電力と分析機能が必要な場合、リモート マネージャを使用できます。

トランスペアレント ファイアウォール モードでデバイスを実行する場合、Firepower Management Centerも使用する必要があります。

ソフトウェアを再インストールすることなく、ローカル管理とリモートの管理を切り替えることができます。リモート管理からローカル管理に切り替える前に、Firepower Device Manager がすべての設定要件を満たしていることを確認します。

注意 マネージャを切り替えると、デバイス設定は削除され、デフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

はじめる前に

デバイスを登録した場合、特に機能ライセンスを有効にした場合、リモート管理に切り替える前に、Firepower Device Manager を介してデバイスを登録解除する必要があります。デバイスを登録解除すると、基本ライセンスとすべての機能ライセンスが解放されます。デバイスを登録解除しない場合、これらのライセンスは Cisco Smart Software Manager のデバイスに割り当てられたままになります。デバイスの登録解除, （65 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 アクセスを持つユーザ名でデバイス CLI にログインします。たとえば、[管理者（admin）]ユーザ名など。

ステップ 2 ローカル管理からリモート管理へ切り替えるには、次の手順に従います。

a) 現在ローカル管理モードになっていることを確認します。

```
> show managers
Managed locally.
```

b) リモート マネージャを設定します。
configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

ここで、

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} 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 のマネージャを登録キー **[秘密（secret）]** で使用する場合、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） 登録がまだ保留中の場合、**configure manager delete** を使用して登録を取り消し、**configure manager local** を使用してローカル管理に戻すことができます。

c) Firepower Management Centerにログインし、デバイスを追加します。
詳細については、Firepower Management Centerオンライン ヘルプを参照してください。

ステップ 3 リモート管理からローカル管理へ切り替えるには、次の手順に従います。

a) 現在リモート管理モードになっていることを確認します。

```
> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

b) リモート マネージャを削除し、マネージャなしのモードになります。
リモート管理からローカル管理に直接移行することはできません。マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

c) ローカル マネージャを設定します。
configure manager local

次に例を示します。

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Web ブラウザを使用して、**https://***management-IP-address* のローカル マネージャを開くことができるようになります。

ファイアウォール モードの変更

Firepower Threat Defenseファイアウォールは、ルーテッド モードまたはトランスペアレント モードで実行できます。ルーテッドモードのファイアウォールはルーテッドホップであり、スクリーンサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ローカルの Firepower Device Manager はルーテッド モードのみをサポートします。ただし、トランスペアレント モードですぐに実行する必要がある場合、ファイアウォール モードに変更し、Firepower Management Center を使用してデバイスの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 モードに変換すると、ローカル マネージャでそのデバイスを設定することができ、Firepower Management Centerを使用してルーテッド モードのデバイスを管理することもできます。

ローカル管理であるか、リモート管理であるかに関係なく、モードを変更するためにはデバイスの CLI を使用する必要があります。

次の手順では、ローカルマネージャを使用している場合、またはローカルマネージャを使用予定の場合のモードの変更方法について説明します。

注意 ファイアウォール モードを変更すると、デバイス設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

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。

いずれかの機能ライセンスを有効にしている場合、ローカル マネージャを削除してリモート管理に切り替える前に、Firepower Device Manager でそれらのライセンスを無効にする必要があります。無効にしないと、それらのライセンスは Cisco Smart Software Manager でデバイスに割り当てられたままになります。オプション ライセンスの有効化と無効化, （64 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、コンフィギュレーション CLI アクセス権があるユーザ名でデバイスの CLI にログインします。たとえば、admin ユーザ名を使用します。

ステップ 2 モードをルーテッドからトランスペアレントに変更して、リモート管理を使用するには、次の手順を実行します。

a) ローカル管理を無効にし、ノー マネージャ モードを開始します。
アクティブなマネージャが存在する間は、ファイアウォールモードを変更できません。**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 firewall transparent

例：

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) リモート マネージャを設定します。
configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

ここで、

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} では、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）を指定します。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 に登録するために必要な一意の英数字の登録キーです。
- *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任意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 で登録キーが **secret** である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
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 モードをトランスペアレントからルーテッドに変更して、ローカル管理に変換するには、次の手順を実行します。

a) Management Centerからデバイスを登録解除します。

b) Firepower Threat Defenseデバイスの CLI にアクセスします。可能ならばコンソール ポートからアクセスします。
これは、モードを変更すると設定が削除され、管理 IP アドレスはデフォルトに戻ってしまうため、モード変更後に管理 IP アドレスへの SSH 接続が失われることがあるためです。

c) ファイアウォール モードをルーテッドに変更します。
configure firewall routed

例：

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) ローカル マネージャを有効にします。
configure manager local

次に例を示します。

```
> configure manager local
Deleting task list
```

```
> show managers
Managed locally.
```

これで、Web ブラウザを使用し、**https://***management-IP-address* でローカル マネージャを開くことができます。

設定のリセット

最初からやり直したい場合は、システム設定を工場出荷時の設定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、マネージャの削除および追加を行うと設定がクリアされます。

設定を削除してバックアップを回復したい場合は、復元するバックアップ コピーをすで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ている場合、ローカルマネージャを削除する前に、Firepower Device Manager でそれらのライセンスを無効にする必要があります。無効にしないと、それらのライセンスは Cisco Smart Software Manager でデバイスに割り当てられたままになります。オプション ライセンスの有効化と無効化, （64 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、Configuration CLI 権限があるユーザ名でデバイスの CLI にログインします。たとえば、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ます。設定をクリアすると、デバイスのセットアップ ウィザードを完了するように求められます。