基本ポリシーの設定

次の設定を使用して基本的なセキュリティポリシーを設定します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスにスタティック IP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバー：クライアントの内部インターフェイスで DHCP サーバーを使用します。
- デフォルトルート：外部インターフェイスを介してデフォルトルートを追加します。
- NAT：外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール：内部から外部へのトラフィックを許可します。

セキュリティポリシーをカスタマイズして、より高度な検査を含めることもできます。

インターフェイスの設定

ゼロタッチプロビジョニングまたは初期設定に Device Manager を使用する場合、次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- イーサネット 1/2：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

Management Center に登録する前に Device Manager 内で追加のインターフェイス固有の設定を実行した場合、その設定は保持されます。

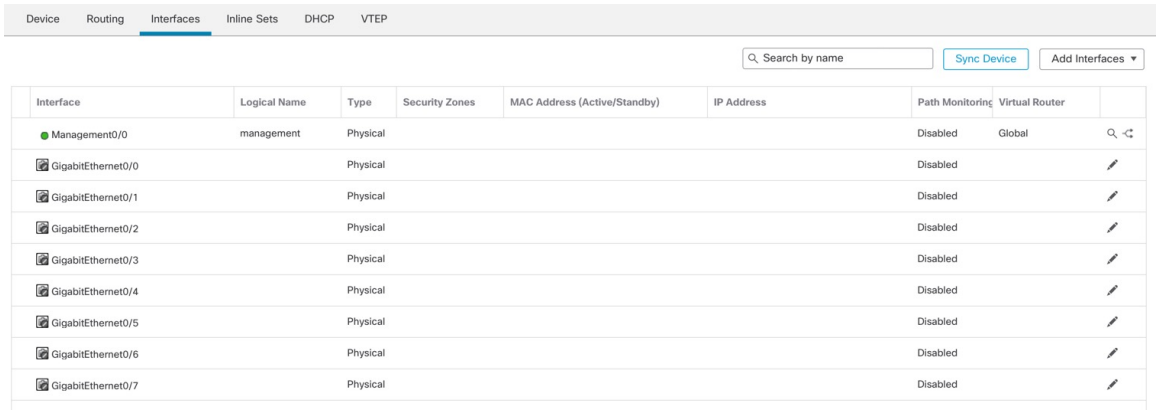
次の例では、静的アドレスを持つルーテッドモードの内部インターフェイスと、DHCPを使用するルーテッドモードの外部インターフェイスを設定します。また、内部 Web サーバー用の DMZ インターフェイスも追加します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、ファイアウォールの [編集（Edit）]（） をクリックします。 >

ステップ 2 [インターフェイス（Interfaces）] をクリックします。

図 *1*: インターフェイス

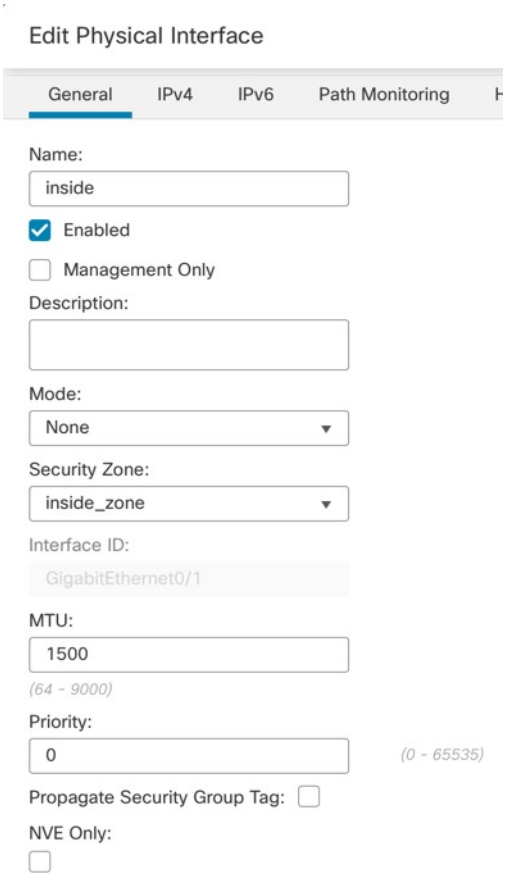


ステップ 3 40 Gb 以上のインターフェイスからブレークアウトポートを作成するには、インターフェイスの **[ブレーク（Break）]** アイコンをクリックします。

設定でフルインターフェイスをすでに使用している場合は、ブレークアウトを続行する前に設定を削除する必要があります。

ステップ 4 内部に使用するインターフェイスの [編集（Edit）]（） をクリックします。

図 *2 : [General]* タブ



a) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。ゾーンまたはグループ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、内部ゾーンから外部ゾーンへのトラフィックは有効にするが外部ゾーンから内部ゾーンへのトラフィックは有効にしないアクセス コントロール ポリシーを設定します。

内部インターフェイスが事前に設定されている場合、これらのフィールドの残りの部分はオプションです。

b) 48 文字までの [名前（Name）] を入力します。

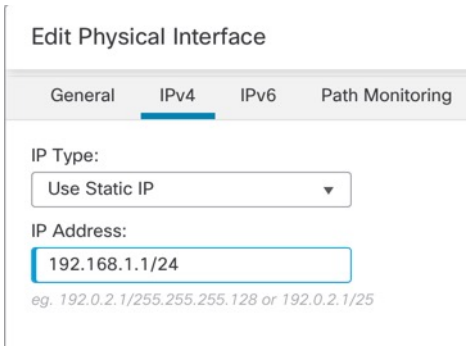
たとえば、インターフェイスに **inside** という名前を付けます。

c) [有効（Enabled）] チェックボックスをオンにします。
d) [モード（Mode）] は [なし（None）] に設定したままにします。
e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

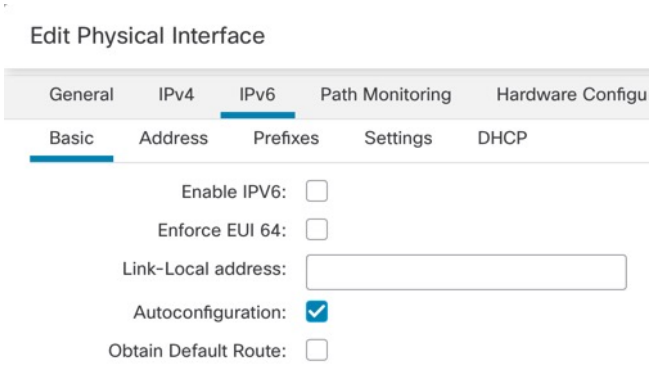
たとえば、**192.168.1.1/24** などと入力します。

図 *3 : [IPv4]* タブ



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

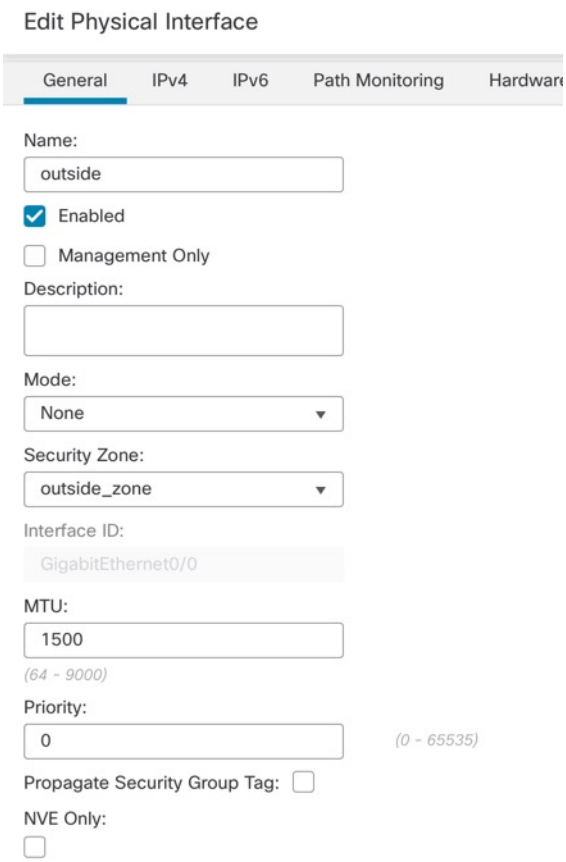
図 *4 : [IPv6]* タブ



f) [OK] をクリックします。

ステップ 5 外部に使用するインターフェイスの [編集（Edit）]（） をクリックします。

図 *5 : [General]* タブ



a) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、「outside_zone」という名前のゾーンを追加します。

他の基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。

b) [OK] をクリックします。

ステップ 6 たとえば、Web サーバーをホストするように DMZ インターフェイスを設定します。

a) 使用するインターフェイスの [編集（Edit）] （） をクリックします。

b) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の DMZ セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**dmz_zone** という名前のゾーンを追加します。

c) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **dmz** という名前を付けます。

d) [有効（Enabled）] チェックボックスをオンにします。

e) [モード（Mode）] は [なし（None）] に設定したままにします。

f) 必要に応じて、[IPv4] タブと [IPv6] タブのいずれかまたは両方をクリックし、IP アドレスを設定します。
g) [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

DHCP サーバーの設定

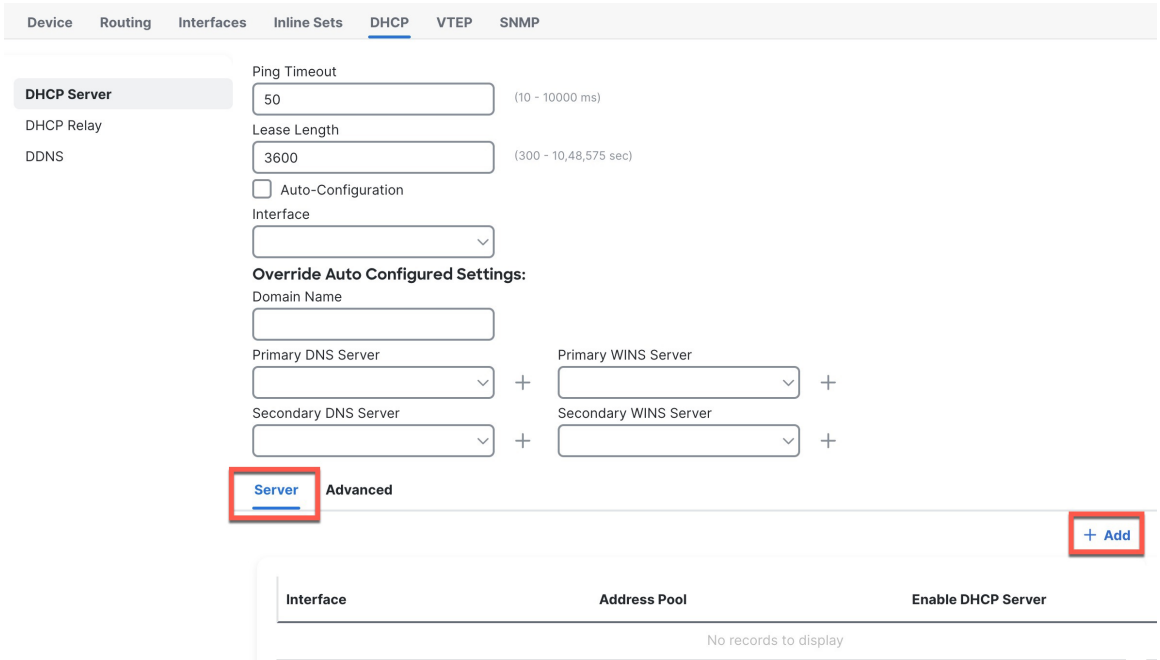
クライアントで DHCP を使用してファイアウォールから IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 [デバイス（Devices）]、[デバイス管理（Device Management）] の順に選択し、デバイスの [編集（Edit）]（） をクリックします。 >

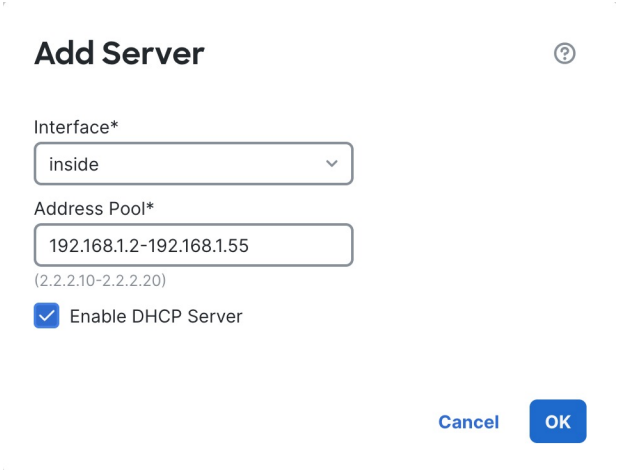
ステップ 2 **[DHCP]** > **[DHCPサーバー（DHCP Server）]** を選択します。

図 *6 : DHCP* サーバー



ステップ 3 [サーバー（Server）] エリアで、[追加（Add）] をクリックし、以下のオプションを設定します。

図 *7*:サーバーの追加



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイス名を選択します。
- [アドレスプール（Address Pool）]：IP アドレスの範囲を設定します。IP アドレスは、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身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

NAT の設定

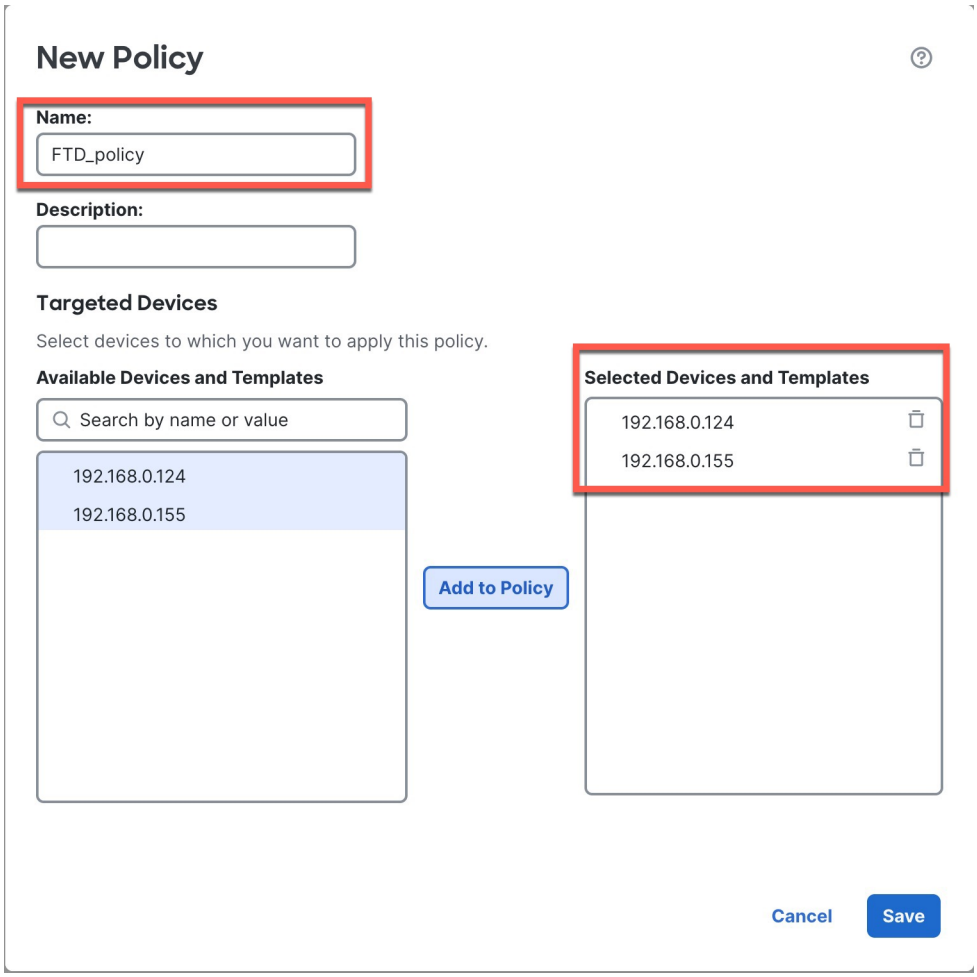
この手順では、内部クライアントが内部アドレスを外部インターフェイスの IP アドレスのポートに変換する NAT ルールを作成します。このタイプの NAT ルールのことをインターフェイスポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** の順に選択し、**[新しいポリシー（New Policy）]** をクリックします。

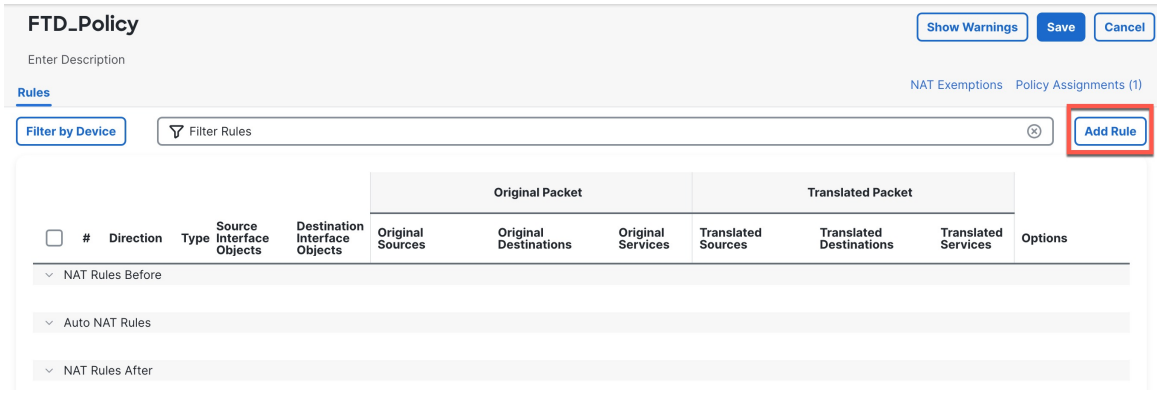
ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。

図 *8* : 新しいポリシー



ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

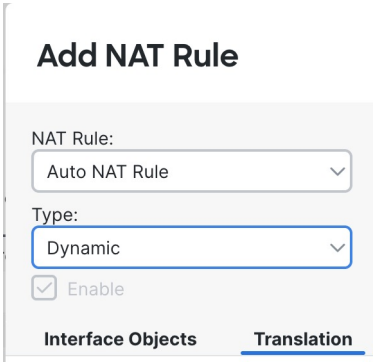
図 *9* : *NAT* ポリシー



ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 基本ルールのオプションを設定します。

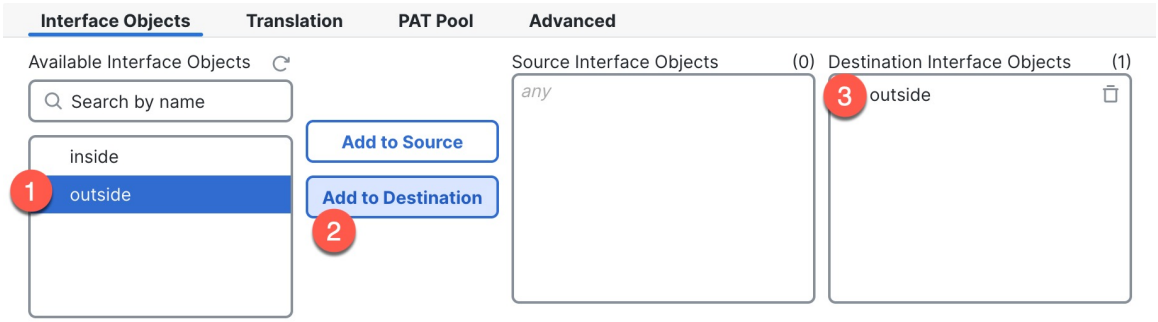
図 *10* : 基本ルールのオプション



- [NATルール（NAT Rule）]：[自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

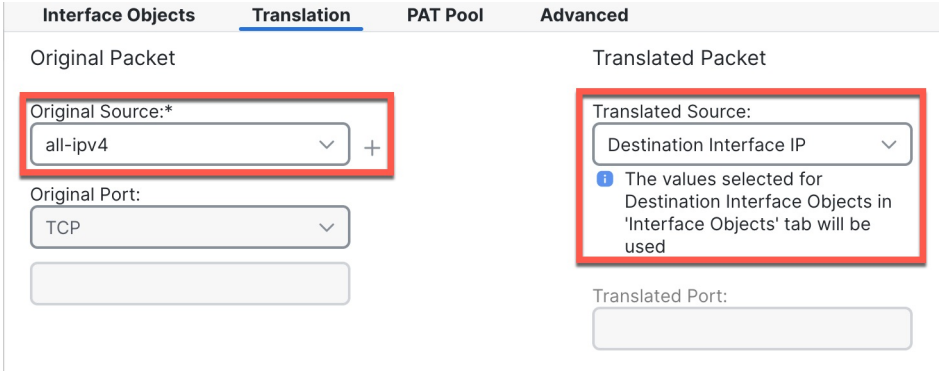
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。

図 *11* : インターフェイス オブジェクト



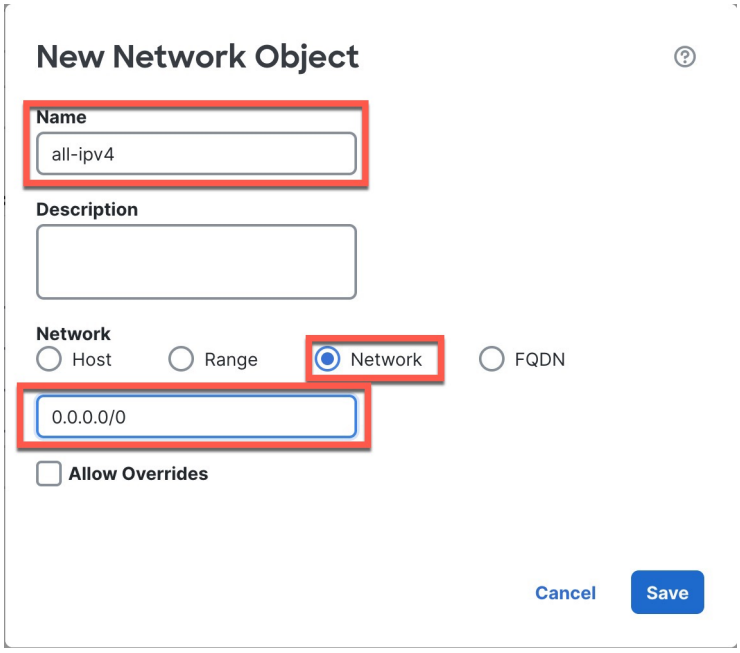
ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。

図 *12* : 変換



- **[元の送信元（Original Source）]**：[追加（Add）]（＋）をクリックして、すべての IPv4 トラフィック（**0.0.0.0/0**）のネットワークオブジェクトを追加します。

  図 *13* : 新しいネットワークオブジェクト



（注）
自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

アクセス制御ルールの設定

デバイスを登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。アクセス コントロール ポリシーには、順番に評価される複数のルールを含めることができます。

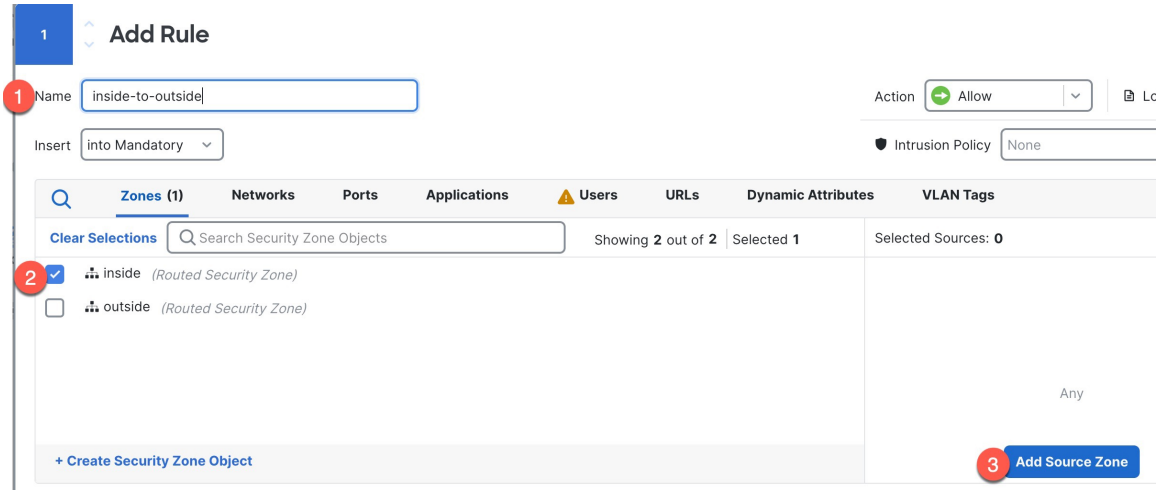
次の手順では、内部ゾーンから外部ゾーンへのすべてのトラフィックを許可するアクセス制御ルールを作成します。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]** の順に選択し、デバイスに割り当てられているアクセス コントロール ポリシーの [編集（Edit）]（） をクリックします。

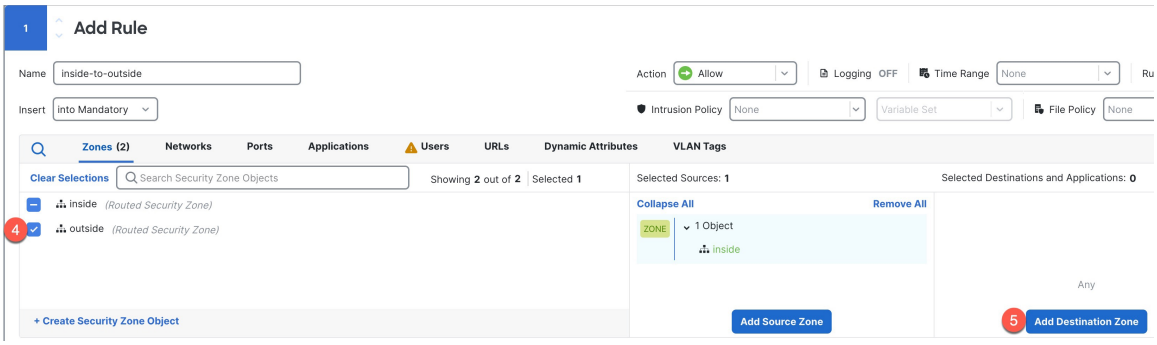
ステップ 2 [ルールを追加（Add Rule）] をクリックし、次のパラメータを設定します。

図 *14 :* 送信元ゾーン（*Source Zone*）



1. このルールに名前を付けます（たとえば、**inside-to-outside**）。
2. [ゾーン（Zones）] から内部ゾーンを選択します。
3. [送信元ゾーンの追加（Add Source Zone）] をクリックします。

図 *15*：宛先ゾーン（*Destination Zone*）



4. [ゾーン（Zones）] から外部ゾーンを選択します。

5. [宛先ゾーンを追加（Add Destination Zone）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 （任意）パケットフロー図でポリシータイプをクリックして、関連付けられたポリシーをカスタマイズします。

[プレフィルタ（Prefilter）]、[復号（Decryption）]、[セキュリティインテリジェンス（Security Intelligence）]、および [アイデンティティ（Identity）] ポリシーは、アクセス制御ルールの前に適用されます。これらのポリシーをカスタマイズする必要はありませんが、ネットワークのニーズを把握した後、信頼できるトラフィックに fastpath を適用（処理をバイパス）したりトラフィックをブロックしてその後の処理が不要になるようにすることで、ネットワークのパフォーマンスを向上させることができます。

図 *16*：アクセス制御の前に適用されるポリシー

- [プレフィルタルール（Prefilter Rules）]：デフォルトのプレフィルタポリシーは、他のルールが適用される（分析する）すべてのトラフィックを通過させます。デフォルトポリシーに加えることができる唯一の変更は、トンネルトラフィックを「ブロックする」ことです。それ以外では、新しいプレフィルタポリシーを作成して、分析（通過）、fastpath 処理（以降のチェックをバイパス）、またはブロックできるアクセス コントロール ポリシーに関連付けることができます。

  プレフィルタを使用すると、ブロックまたは fastpath 処理のいずれかによって、トラフィックがさらに進む前に処理することで、パフォーマンスを向上させることができます。新しいポリシーでは、「トンネル」ルールと「プレフィルタ」ルールを追加できます。トンネルルールを使用すると、プレーンテキスト（非暗号化）のパススルートンネルを fastpath 処理、ブロック、または再ゾーン化できます。プレフィルタルールを使用すると、IP アドレス、ポート、およびプロトコルで識別される非トンネルトラフィックを fastpath 処理またはブロックできます。

  たとえば、ネットワーク上のすべての FTP トラフィックをブロックし、管理者からの SSH トラフィックを高速パスする場合は、新しいプレフィルタ ポリシーを追加できます。

- [復号（Decryption）]：デフォルトでは、復号は適用されません。復号は、ネットワークトラフィックをディープインスペクションに公開する方法です。ほとんどの場合、トラフィックを復号する必要はなく、法的に許可されている場合にのみ復号できます。ネットワークを最大限に保護するために、重

要なサーバーへのトラフィックや、信頼できないネットワークセグメントからのトラフィックには、復号ポリシーを使用することをお勧めします。

- [セキュリティ インテリジェンス（Security Intelligence）]：（IPS ライセンスが必要）セキュリティ インテリジェンスはデフォルトで有効になっています。セキュリティ インテリジェンスは、悪意のあるアクティビティに対するもう 1 つの早期防御で、さらなる処理のために接続をアクセス コントロール ポリシーに渡す前に適用されます。セキュリティ インテリジェンスは、レピュテーション インテリジェンスを使用して、シスコの脅威インテリジェンス組織である Talos が提供する IP アドレス、URL、およびドメイン名との接続を迅速にブロックします。必要に応じて、IP アドレス、URL、ドメインを追加または削除できます。

  （注）
  IPS ライセンスがない場合、このポリシーは、アクセス コントロール ポリシーで有効と表示されていても展開されません。

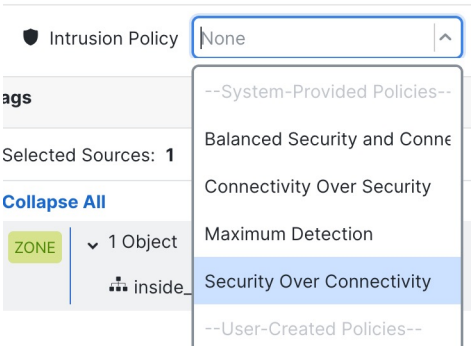
- [アイデンティティ（Identity）]：アイデンティティはデフォルトでは適用されません。アクセス コントロール ポリシーによるトラフィックの処理を許可する前に、ユーザーに認証を要求できます。

ステップ 4 （任意） アクセス制御ルールの後に適用される侵入ポリシーを追加します。

侵入ポリシーは、トラフィックのセキュリティ違反を検査する定義済みの一連の侵入検出および侵入防止設定です。Management Center には、多数のシステム提供のポリシーが含まれており、そのまま有効にすることもカスタマイズすることもできます。この手順では、システム提供のポリシーを有効にします。

a) [侵入ポリシー（Intrusion Policy）] ドロップダウンリストをクリックします。

図 *17*：システム提供の侵入ポリシー

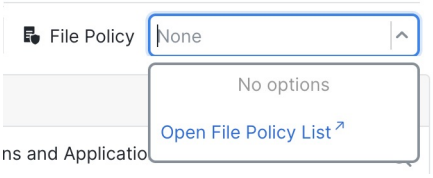


b) リストからシステム提供のポリシーを 1 つ選択します。

ステップ 5 （任意） アクセス制御ルールの後に適用されるファイルポリシーを追加します。

a) [ファイルポリシー（File Policy）] ドロップダウンリストをクリックし、既存のポリシーを選択するか、[ファイルポリシーリストを開く（Open File Policy List）] を選択してポリシーを追加します。

図 *18* : ファイルポリシー（*File Policy*）



新しいポリシーの場合は、**[ポリシー（Policies）]** > **[マルウェア&ファイル（Malware & File）]** ページが別のタブで開きます。

b) ポリシーの作成の詳細については、Cisco Secure Firewall Device Manager Configuration Guideを参照してください。

c) [ルールの追加（Add Rule）]ページに戻り、ドロップダウンリストから新しく作成したポリシーを選択します。

ステップ 6 [Apply] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。

ステップ 7 [保存（Save）] をクリックします。

外部インターフェイスでの SSH の有効化

ここでは、外部インターフェイスへの SSH 接続を有効にする方法について説明します。

デフォルトでは、初期設定時にパスワードを設定した **admin** ユーザーを使用できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシーを作成または編集します。

ステップ 2 [SSHアクセス（SSH Access）] を選択します。

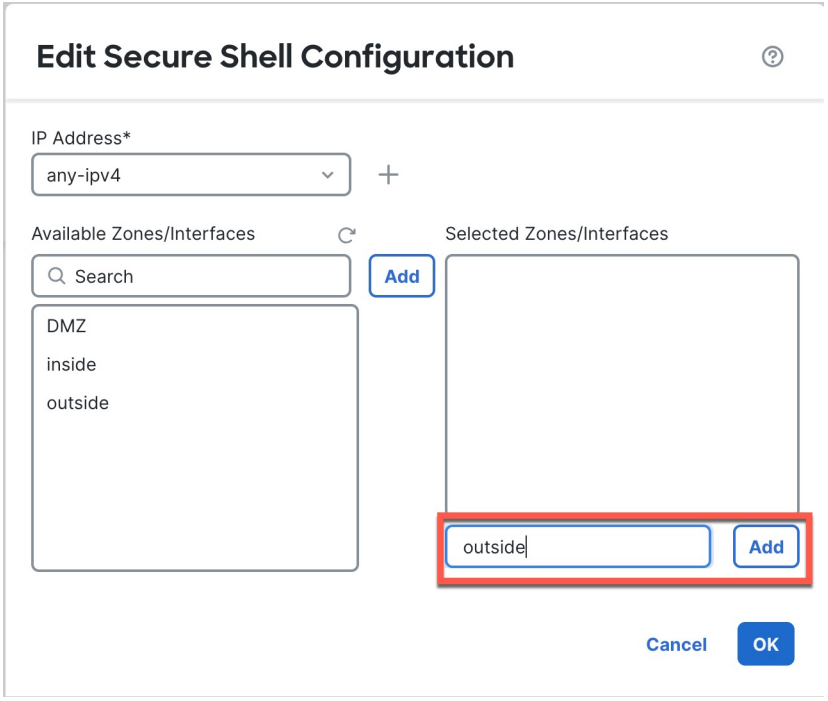
ステップ 3 SSH 接続を許可する外部インターフェイスと IP アドレスを指定します。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IP Address]：SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または[+]をクリックして新しいネットワークオブジェクトを追加します。
- [使用可能なゾーン/インターフェイス（Available Zones/Interfaces）]：[選択したゾーン/インターフェイス（Selected Zones/Interfaces）] リストの下のフィールドに外部ゾーンを追加するか「外部」インターフェイス名を入力し、[追加（Add）] をクリックします。

図 *19* : 外部インターフェイスでの *SSH* の有効化



c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

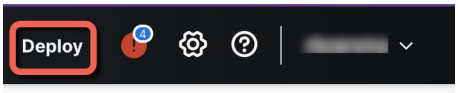
設定の展開

設定の変更をデバイスに展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

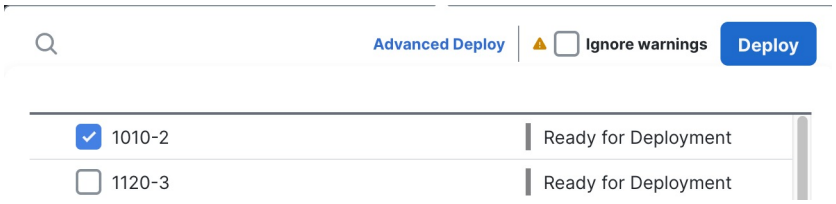
ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *20* : 展開



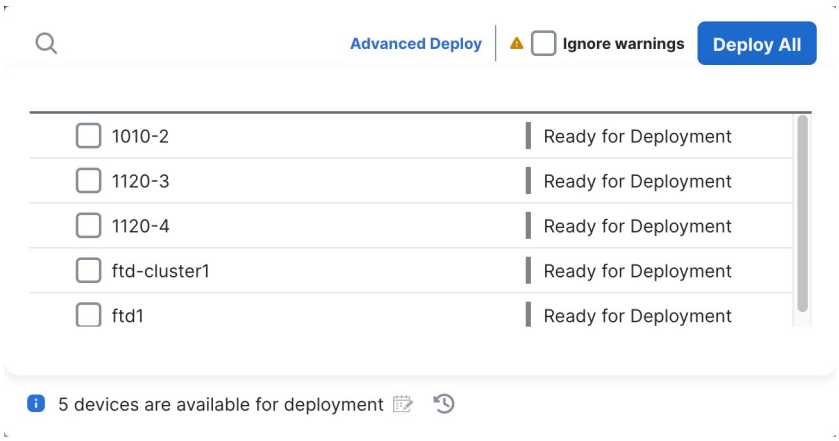
ステップ 2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開（Deploy）] をクリックします。

図 *21* : 選択したものを展開



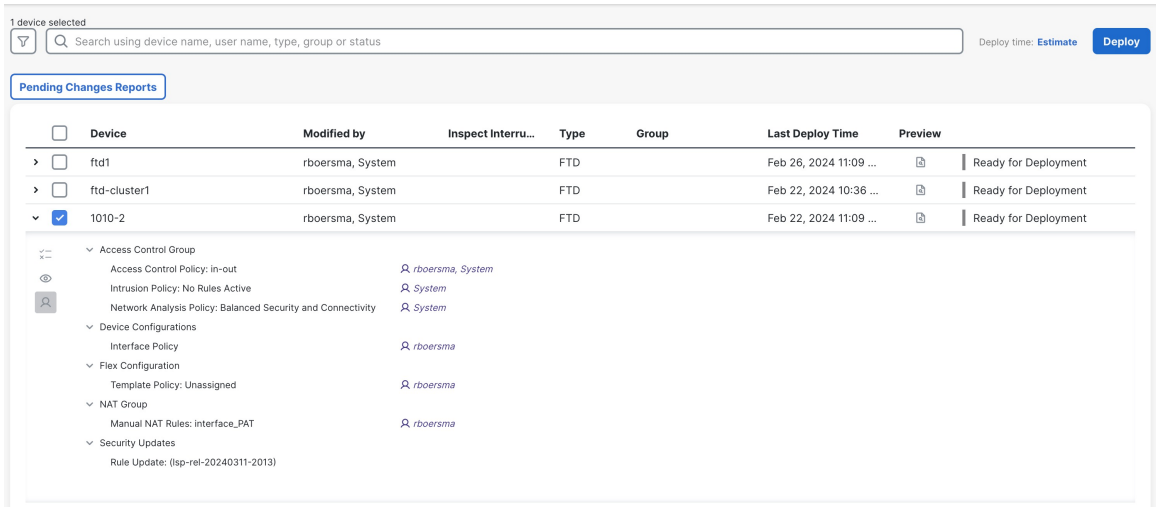
または、[すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開します。

図 *22* : すべて展開



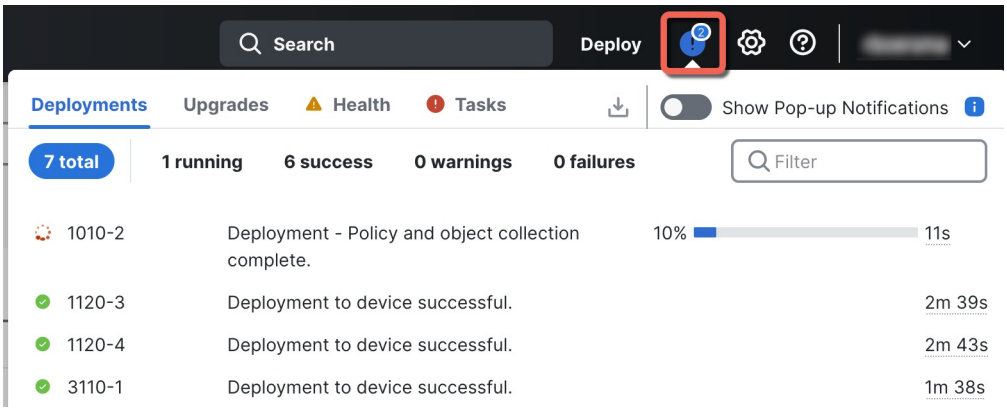
それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

図 *23* : 高度な展開



ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。

図 *24* : 展開ステータス



翻訳について
このドキュメントは、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。