



## 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イ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ができます。

- インターフェイスの設定 (1 ページ)
- DHCP サーバーの設定 (7 ページ)
- デフォルトルートの追加 (8 ページ)
- NAT の設定 (11 ページ)
- アクセス制御ルールの設定 (15 ページ)
- 設定の展開 (18 ページ)

## インターフェイスの設定

初期設定に Firewall 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

Firewall Management Center に登録する前に Firewall 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。

## ■ インターフェイスの設定

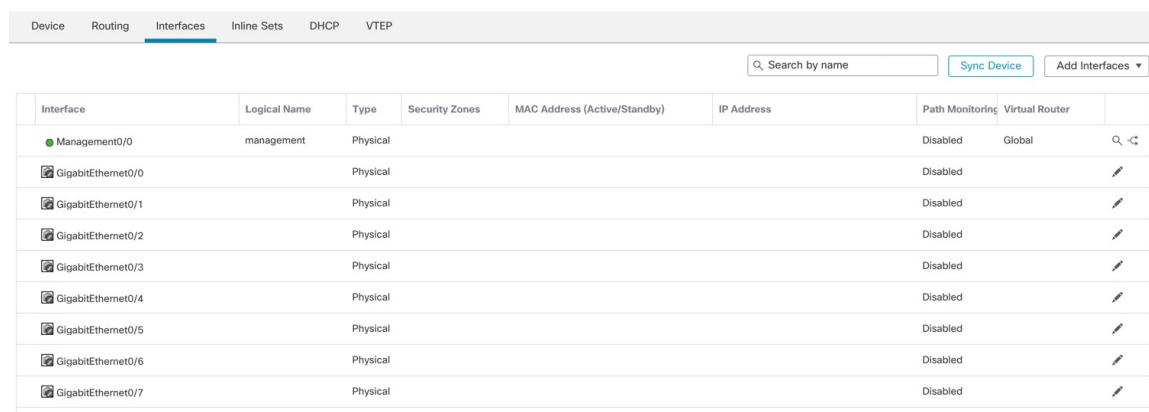
次の例では、静的アドレスを持つルーテッドモードの内部インターフェイスと、DHCPを使用するルーテッドモードの外部インターフェイスを設定します。また、内部 Web サーバー用の DMZ インターフェイスも追加します。

### 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)] (Ø) 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



Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	Actions
Management0/0	management	Physical				Disabled	Global	🔗
GigabitEthernet0/0		Physical				Disabled		🔗
GigabitEthernet0/1		Physical				Disabled		🔗
GigabitEthernet0/2		Physical				Disabled		🔗
GigabitEthernet0/3		Physical				Disabled		🔗
GigabitEthernet0/4		Physical				Disabled		🔗
GigabitEthernet0/5		Physical				Disabled		🔗
GigabitEthernet0/6		Physical				Disabled		🔗
GigabitEthernet0/7		Physical				Disabled		🔗

**ステップ3** 40Gb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)] (Ø) をクリックします。

図 2:[General] タブ

Edit Physical Interface

General    IPv4    IPv6    Path Monitoring

Name:

Enabled

Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:

(0 - 65535)

Propagate Security Group Tag:

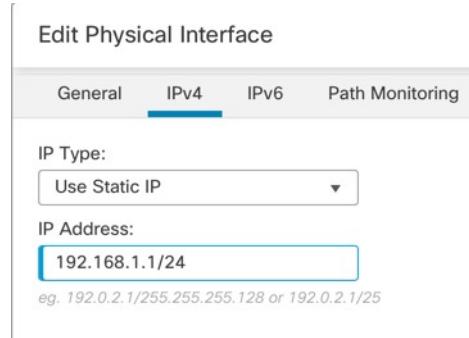
NVE Only:

- [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イ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イ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。
- 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。
- [有効 (Enabled) ] チェックボックスをオンにします。
- [モード (Mode) ] は [なし (None) ] に設定したままにします。
- [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。

## ■ インターフェイスの設定

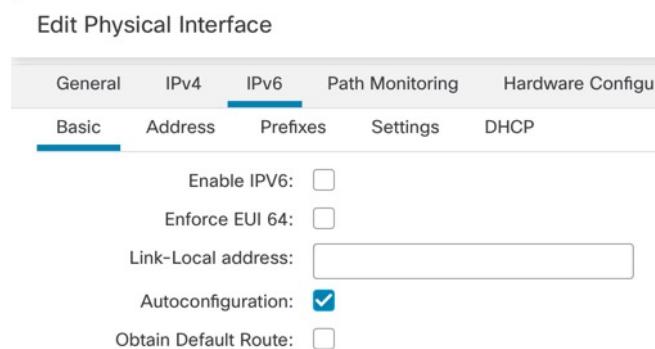
たとえば、**192.168.1.1/24** などと入力します。

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

## Edit Physical Interface

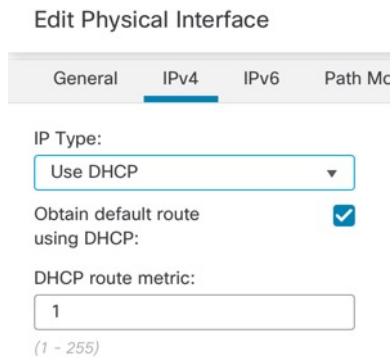
General	IPv4	IPv6	Path Monitoring	Hardware
Name: <input type="text" value="outside"/>				
<input checked="" type="checkbox"/> Enabled				
<input type="checkbox"/> Management Only				
Description: <input type="text"/>				
Mode: <input type="text" value="None"/>				
Security Zone: <input type="text" value="outside_zone"/>				
Interface ID: <input type="text" value="GigabitEthernet0/0"/>				
MTU: <input type="text" value="1500"/>				
(64 - 9000)				
Priority: <input type="text" value="0"/>				
(0 - 65535)				
Propagate Security Group Tag: <input type="checkbox"/>				
NVE Only: <input type="checkbox"/>				

- [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。  
外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。
- 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「outside」という名前を付けます。
- [有効 (Enabled) ] チェックボックスをオンにします。
- [モード (Mode) ] は [なし (None) ] に設定したままにします。
- [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。
  - [IPv4] : [DHCP の使用 (Use DHCP) ] を選択し、次のオプションのパラメータを設定します。
    - [DHCP を使用してデフォルトルートを取得 (Obtain default route using DHCP) ] : DHCP サーバーからデフォルトルートを取得します。

## ■ インターフェイスの設定

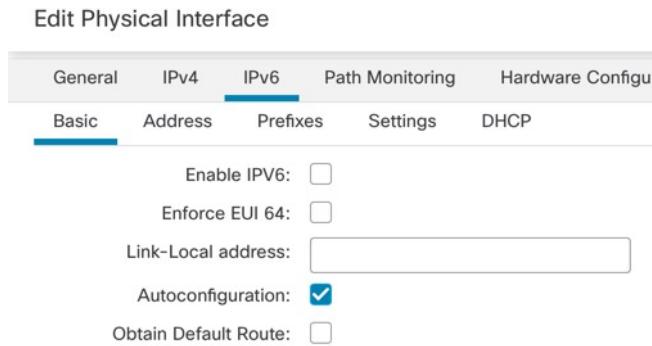
- [DHCPルートメトリック (DHCP route metric) ] : アドミニスト레이ティブディスタンスを学習したルートに割り当てます (1 ~ 255)。学習したルートのデフォルトのアドミニストレイティブディスタンスは 1 です。

図 6: [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 7: [IPv6] タブ



f) [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。

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

- 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。
- [有効 (Enabled)] チェックボックスをオンにします。
- [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

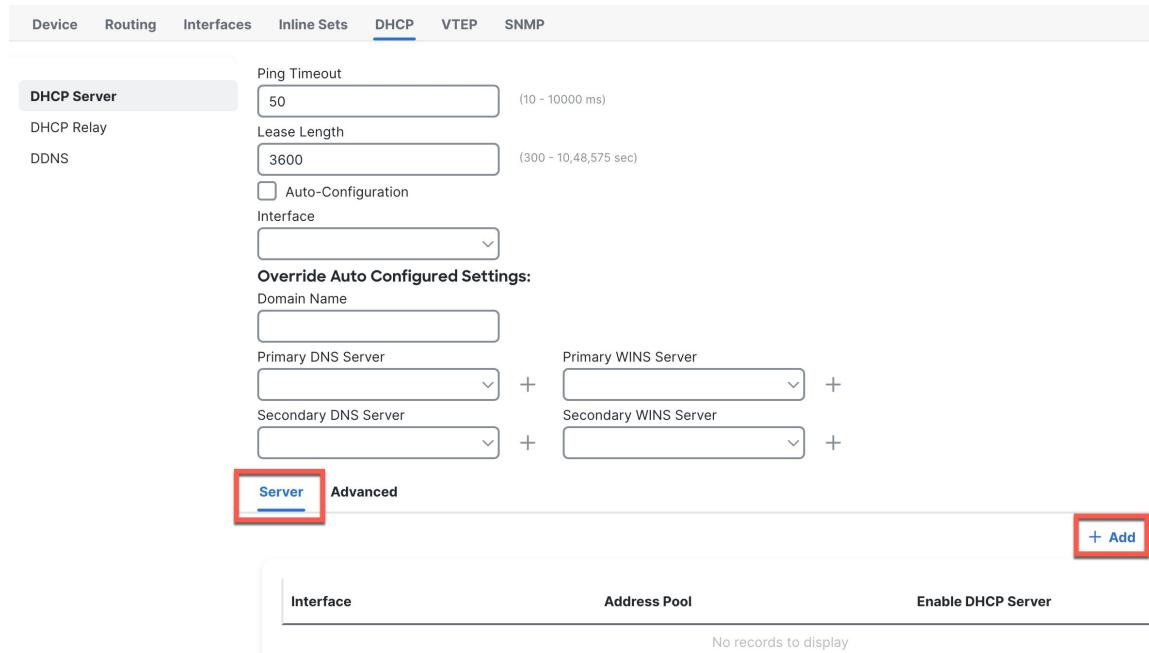
クライアントで DHCP を使用してファイアウォールから IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

### 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) ] (Ø) 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。

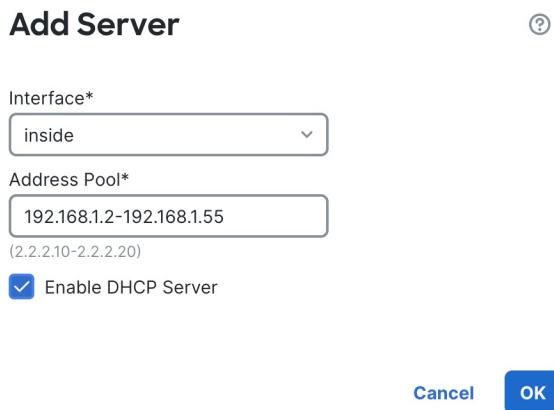
図 8: DHCP サーバー



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。

## ■ デフォルトルートの追加

図 9: 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ます、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。

## デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指示します。DHCPから外部アドレスを取得した場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。

### 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 [ルーティング (Routing) ] > [静的ルート (Static Routes) ] を選択します。

図 10: 静的ルート

The screenshot shows the 'Manage Virtual Routers' interface with the 'Global' tab selected. On the left, a sidebar lists various routing protocols: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing (with BGP, IPv4, and IPv6 sub-options), and Static Route. The 'Static Route' option is highlighted with a red box. On the right, a table lists routes categorized by 'Network' (IPv4 and IPv6) and 'Interface'. A red box highlights the '+ Add Route' button in the top right corner of the table area.

DHCP サーバーからデフォルトルートを受信した場合は、このテーブルに表示されます。

**ステップ3** [ルートを追加 (Add route) ] をクリックして、次のオプションを設定します。

## ■ デフォルトルートの追加

図 11: 静的ルート追加の設定

Add Static Route Configuration

Type:  IPv4  IPv6

Interface\*: outside

(Interface starting with this icon  signifies it is available for route leak)

Available Network:  Search +

Selected Network: any-ipv4

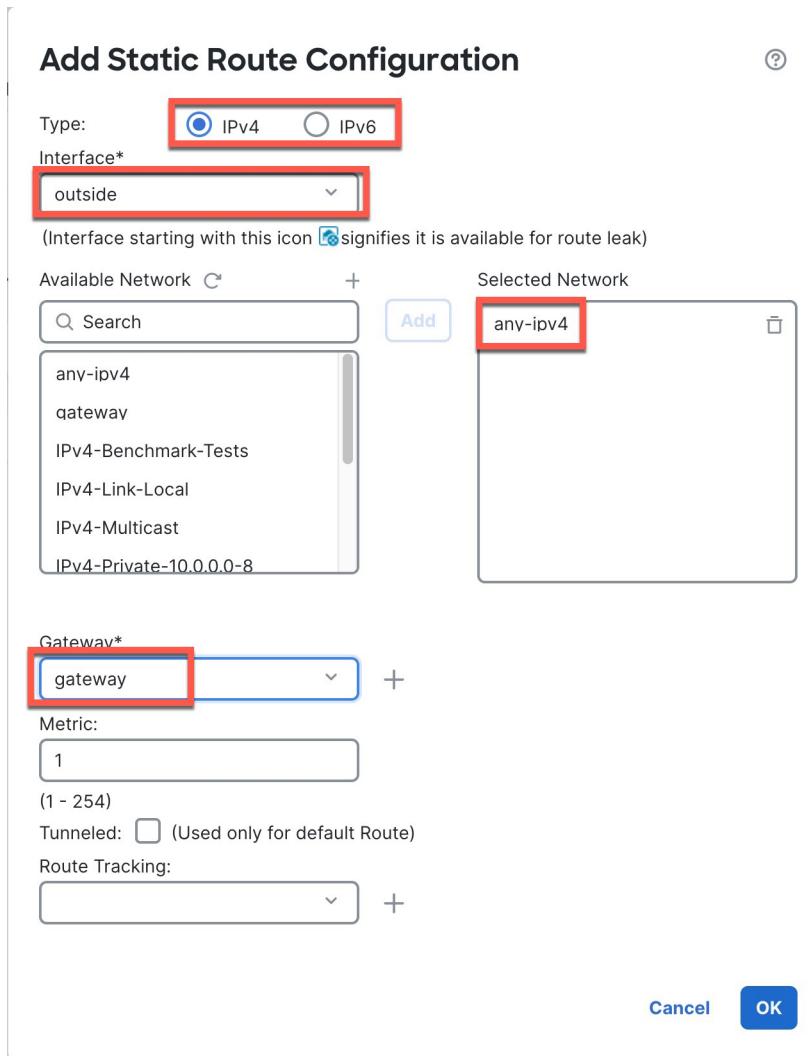
Gateway\*: gateway

Metric: 1

Tunneled:  (Used only for default Route)

Route Tracking: +

Cancel OK



- ・[タイプ (Type) ] : 追加するスタティックルートのタイプに応じて、[IPv4] または[IPv6] オプションボタンをクリックします。
- ・[インターフェイス (Interface) ] : 出力インターフェイスを選択します。通常は外部インターフェイスです。
- ・[可能なネットワーク (Available Network) ] : IPv4 デフォルトルートの場合は[any-ipv4] を選択し、IPv6 デフォルトルートの場合は [any-ipv6] を選択し、[追加 (Add) ] をクリックして [選択したネットワーク (Selected Network) ] リストに移動させます。
- ・[ゲートウェイ (Gateway) ] または [IPv6ゲートウェイ (IPv6 Gateway) ] : このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。

ステップ4 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。

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。

## NAT の設定

図 12:新しいポリシー

**New Policy**

**Name:** FTD\_policy

**Description:**

**Targeted Devices**  
Select devices to which you want to apply this policy.

**Available Devices and Templates**

Search by name or value

192.168.0.124  
192.168.0.155

**Selected Devices and Templates**

192.168.0.124  
192.168.0.155

Add to Policy

Cancel Save

ポリシーが Firewall 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 13: NAT ポリシー

**FTD\_Policy**

Enter Description

**Rules**

Filter by Device Filter Rules Add Rule

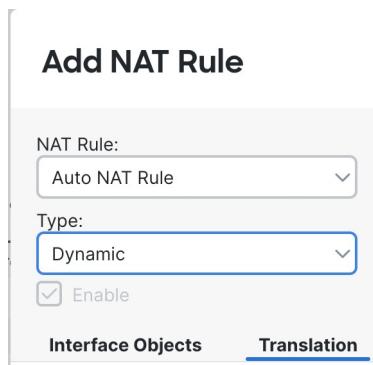
Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
		Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before								
Auto NAT Rules								
NAT Rules After								

Show Warnings Save Cancel

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。

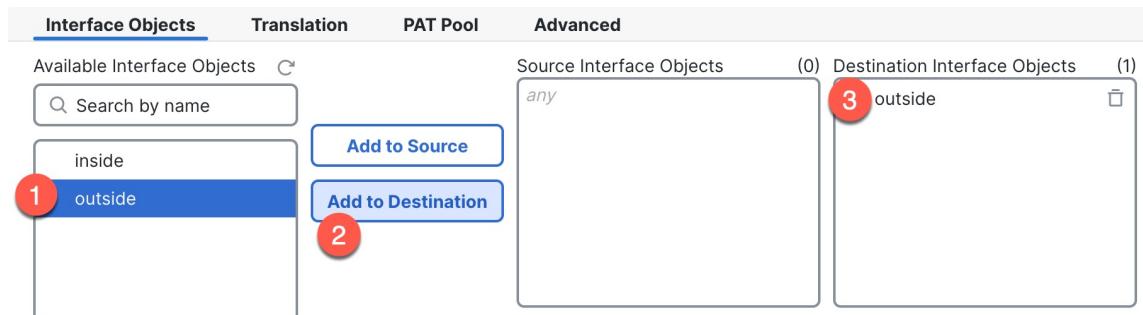
図 14: 基本ルールのオプション



- [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。

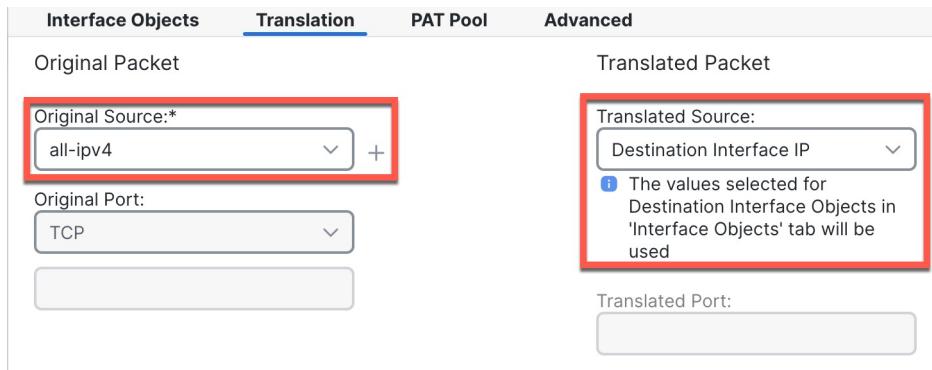
図 15:インターフェイス オブジェクト



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。

## ■ NAT の設定

図 16: 変換



- ・[元の送信元 (Original Source) ] : [追加 (Add) ] (+) をクリックして、すべての IPv4 トライフィック (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 17: 新しいネットワークオブジェクト

New Network Object

Name: all-ipv4

Description:

Network

Host  Range  Network  FQDN

Address: 0.0.0.0/0

Allow Overrides

Cancel Save

(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。

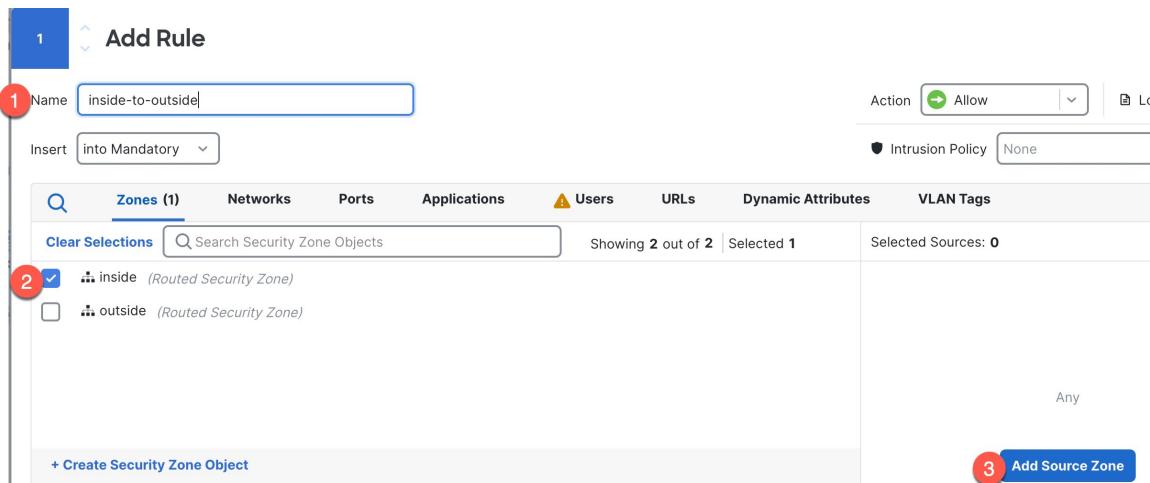
次の手順では、内部ゾーンから外部ゾーンへのすべてのトラフィックを許可するアクセス制御ルールを作成します。

### 手順

ステップ1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [アクセス制御 (Access Control)] を選択し、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。

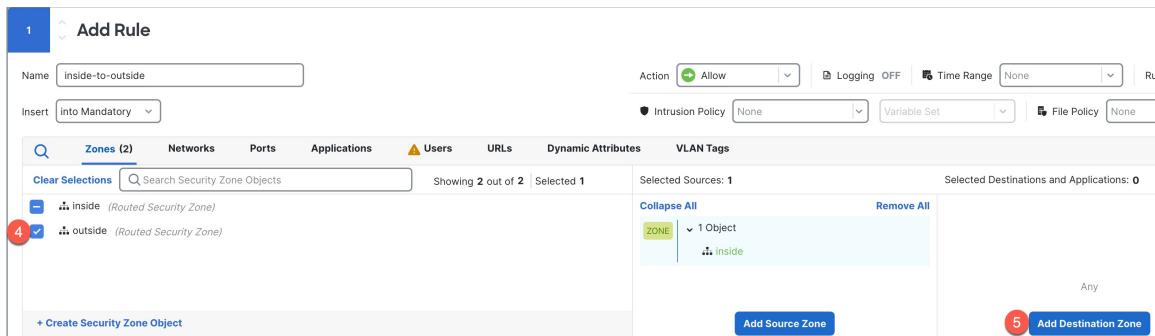
図 18: 送信元ゾーン (Source Zone)



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。

## ■ アクセス制御ルールの設定

図 19: 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、信頼できるトライフィックに fastpath を適用 (処理をバイパス) したりトライ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 20: 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) すべてのトライ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、トンネルトライフィックを「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、トライ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イフィックを 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 トライフィックをブロックし、管理者からのSSH トライ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、ネットワークトライ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、トライ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

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。

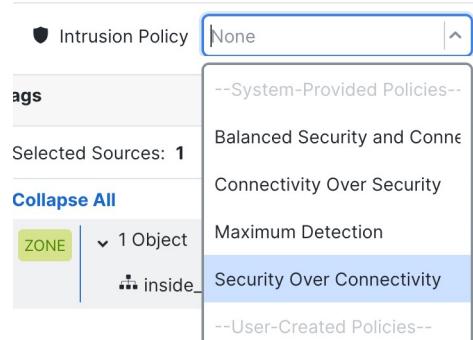
- [アイデンティティ (Identity) ]: アイデンティティはデフォルトでは適用されません。アクセスコントロールポリシーによるトラフィックの処理を許可する前に、ユーザーに認証を要求できます。

#### 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。Firewall 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。

- [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 21: システム提供の侵入ポリシー



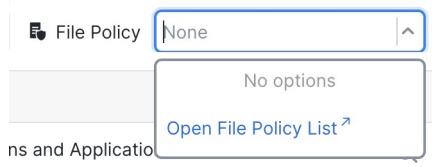
- リストからシステム提供のポリシーを 1 つ選択します。

#### 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。

- [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。

## 設定の展開

図 22: 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) ]>[アクセス制御 (Access Control) ]見出し>[マルウェアとファイル (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。

## 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

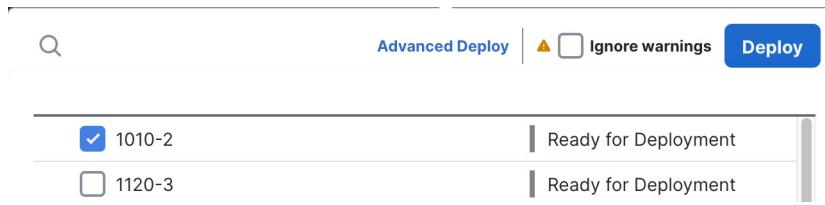
ステップ1 右上の [展開 (Deploy) ] をクリックします。

図 23: 展開



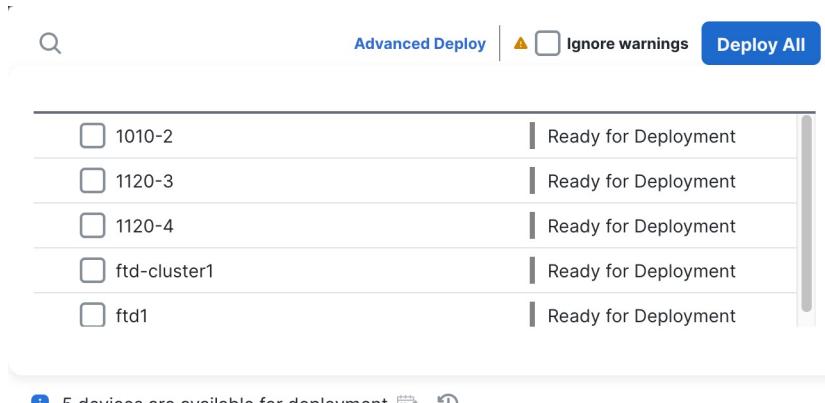
ステップ2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開 (Deploy) ] をクリックします。

図 24:選択したもの展開



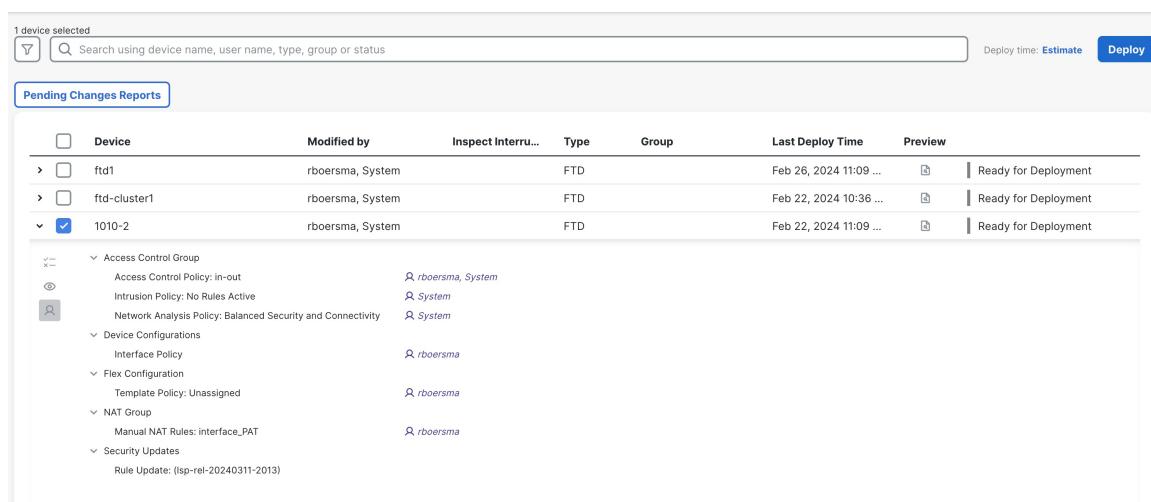
または、[すべて展開 (Deploy All) ] をクリックしてすべてのデバイスに展開します。

図 25: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。

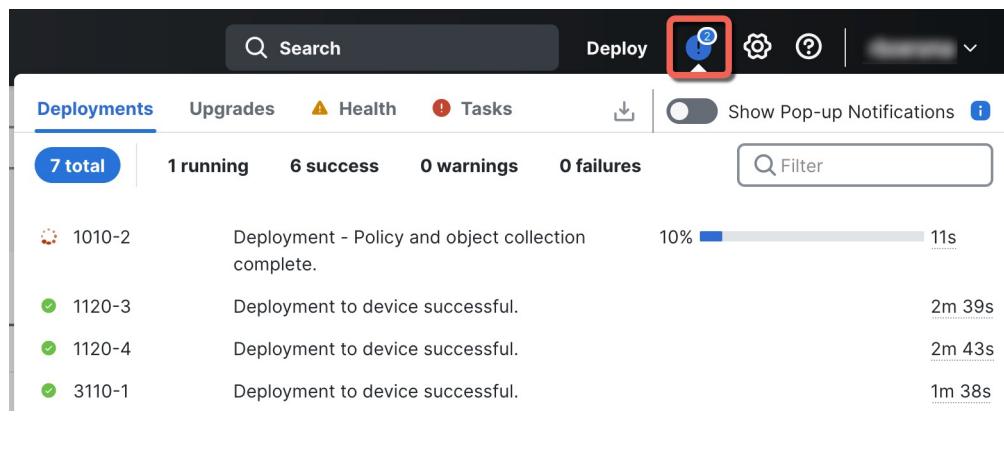
図 26:高度な展開



**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。

## 設定の展開

図 27: 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。