



# Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理

この章では、Management Center を使用して管理されるスタンドアロンの Threat Defense Virtual デバイスを展開する方法について説明します。



(注) このドキュメントでは、最新の Threat Defense Virtual バージョンの機能について説明します。古いバージョンのソフトウェアを使用している場合は、お使いのバージョンの Management Center コンフィギュレーションガイドの手順を参照してください。

- [Secure Firewall Management Center を備えた Secure Firewall Threat Defense Virtual について \(1 ページ\)](#)
- [Secure Firewall Management Center へのログイン \(2 ページ\)](#)
- [Secure Firewall Management Center へのデバイス登録 \(2 ページ\)](#)
- [基本的なセキュリティポリシーの設定 \(5 ページ\)](#)
- [Secure Firewall Threat Defense CLI へのアクセス \(18 ページ\)](#)

## Secure Firewall Management Center を備えた Secure Firewall Threat Defense Virtual について

Secure Firewall Threat Defense Virtual は、Cisco NGFW ソリューションの仮想化コンポーネントです。Threat Defense Virtual は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System (NGIPS)、Application Visibility and Control (AVC)、URL フィルタリング、マルウェア防御などの次世代ファイアウォールサービスを提供します。

Threat Defense Virtual を管理するには、別のサーバー上で実行されるフル機能のマルチデバイススマネージャである Management Center を使用します。Threat Defense Virtual は、Threat Defense

Virtual マシンに割り当てた管理インターフェイス上の Management Center を登録して通信します。

Threat Defense Virtual は、Threat Defense Virtual マシンに割り当てた管理インターフェイス上の Management Center を登録して通信します。

トラブルシューティングの目的で、管理インターフェイス上の SSH を使用して Threat Defense CLI にアクセスすることも、Management Center の CLI から Threat Defense に接続することもできます。

このガイドでは、Management Center を使用して管理されるスタンドアロンの Threat Defense Virtual デバイスの展開方法について説明します。Management Center での設定の詳細については、[Management Center アドミニストレーションガイド \[英語\]](#) および [Management Center デバイス コンフィギュレーションガイド \[英語\]](#) を参照してください。

Management Center のインストールの詳細については、『[Cisco Firepower Management Center 1600、2600、4600 ハードウェア設置ガイド](#)』または『[Cisco Firepower Management Center Virtual スタートアップガイド](#)』を参照してください。

## Secure Firewall Management Center へのログイン

Management Center を使用して、Threat Defense を設定および監視します。

### 始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート (<https://www.cisco.com/go/firepower-notes>) を参照してください。

---

**ステップ 1** サポートされているブラウザを使用して、次の URL を入力します。

**`https://fmcv_ip_address`**

`fmcv_ip_address` で Management Center の IP アドレスまたはホスト名を指定します。

(注) IPv6 固有の `https://[fmcv_ipv6_public_address]`

**ステップ 2** ユーザー名とパスワードを入力します。

**ステップ 3** [ログイン (Log In) ] をクリックします。

---

## Secure Firewall Management Center へのデバイス登録

### 始める前に

Threat Defense Virtual マシンが正常に展開されていて、電源がオンになっており、最初のブート手順を実行済みであることを確認してください。



- (注) この手順では、day0/bootstrap スクリプトを使用して、Management Center の登録情報が指定されていることを前提としています。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。[Cisco Secure Firewall Threat Defense コマンドリファレンス](#)を参照してください。

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 [追加 (Add)] ドロップダウンリストから、[デバイスの追加 (Add Device)] を選択し、次のパラメータを入力します。

### Add Device

Host:†

Display Name:

Registration Key: \*

Group:

Access Control Policy: \*

Smart Licensing  
Note: All virtual FTDs require a performance tier license.  
Make sure your Smart Licensing account contains the available licenses you need.  
It's important to choose the tier that matches the license you have in your account.  
Click [here](#) for information about the FTD performance-tiered licensing.  
Until you choose a tier, your FTDv defaults to the FTDv50 selection.

Performance Tier (only for FTDv 7.0 and above):

Malware  
 Threat  
 URL Filtering

Advanced  
Unique NAT ID:†

Transfer Packets

- [ホスト (Host)] : 追加するデバイスの IP アドレス (IPv4 および IPv6) を入力します。IPv6 が有効になっている場合は、ホスト名に IPv4 または IPv6 を使用できます。

- [表示名 (Display Name)] : Management Center に表示するデバイスの名前を入力します。
- [登録キー (Registration key)] : Threat Defense Virtual ブートストラップ設定で指定したものと同一登録キーを入力します。
- [ドメイン (Domain)] : マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。
- [グループ (Group)] : グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー (Access Control Policy)] : 初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成 (Create new policy)] を選択し、[すべてのトラフィックをブロック (Block all traffic)] を選択します。後でこれを変更してトラフィックを許可することができます。「[アクセス制御の設定 \(16 ページ\)](#)」を参照してください。

The screenshot shows the 'New Policy' configuration interface. It includes the following elements:

- Name:** A text input field containing 'ftd-ac\_policy'.
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently set to 'None'.
- Default Action:** Three radio button options: 'Block all traffic' (selected), 'Intrusion Prevention', and 'Network Discovery'.
- Targeted Devices:** A section titled 'Select devices to which you want to apply this policy.' It contains two columns: 'Available Devices' and 'Selected Devices'.
  - Available Devices:** A search box with the text '192.168.0.12' and an 'Add to Policy' button.
  - Selected Devices:** An empty list box.

- [スマートライセンス (Smart Licensing)] : 展開する機能に必要なスマートライセンスとして、[マルウェア (Malware)] (マルウェア防御インスペクションを使用する予定の場合)、[脅威 (Threat)] (侵入防御を使用する予定の場合)、および[URL] (カテゴリベースのURLフィルタリングを実行する予定の場合) を割り当てます。
- [一意の NAT ID (Unique NAT ID)] : Threat Defense Virtual ブートストラップ設定で指定した NAT ID を指定します。
- [パケットの転送 (Transfer Packets)] : デバイスから Management Center へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Management Center に送信します。このオプ

ションを無効にした場合は、イベント情報だけが Management Center に送信され、パケットデータは送信されません。

**ステップ 3** [登録 (Register)] をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されません。Threat Defense Virtual が登録に失敗した場合は、次の項目を確認してください。

- ping : Threat Defense CLI (「[Secure Firewall Threat Defense CLI へのアクセス \(18 ページ\)](#)」) にアクセスし、次のコマンドを使用して Management Center IP アドレスへの ping を実行します。

```
ping system ip_address
```

ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。Threat Defense IP アドレスを変更する必要がある場合は、**configure network {ipv4 | ipv6} manual or DHCP** コマンドを実行します。

- NTP : NTP サーバーが[システム (System)] > [設定 (Configuration)] > [時刻の同期 (Time Synchronization)] ページで設定した Management Center サーバーと一致していることを確認します。
- 登録キー、NAT ID、および Management Center IP アドレス : 両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add DONTRESOLVE<registrationkey> <NATID>** コマンドを使用して、Threat Defense Virtual で登録キーと NAT ID を設定することができます。また、このコマンドで Management Center IP アドレスを変更することもできます。

---

## 基本的なセキュリティポリシーの設定

ここでは、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する方法について説明します。

- 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。

---

**ステップ 1** [インターフェイスの設定 \(6 ページ\)](#)

**ステップ 2** [DHCP サーバーの設定 \(9 ページ\)](#)

**ステップ 3** [デフォルトルートの追加 \(10 ページ\)](#)

ステップ4 NAT の設定 (12 ページ)

ステップ5 アクセス制御の設定 (16 ページ)

ステップ6 設定の展開 (17 ページ)

## インターフェイスの設定

Threat Defense Virtual インターフェイスを有効にし、それらをセキュリティゾーンに割り当てて IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも2つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの1つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」(DMZ) となる場合があります。

一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCPによるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイス[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。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	Virtual Router
Diagnostic0/0	diagnostic	Physical			Global

ステップ3 「内部」に使用するインターフェイス[編集 (Edit)] (✎) をクリックします。  
[全般 (General)] タブが表示されます。

The screenshot shows the 'Edit Physical Interface' dialog box. The 'General' tab is selected. The 'Name' field contains 'Inside'. The 'Enabled' checkbox is checked. The 'Management Only' checkbox is unchecked. The 'Description' field is empty. The 'Mode' dropdown is set to 'None'. The 'Security Zone' dropdown is set to 'inside-zone'. The 'Interface ID' is 'GigabitEthernet0/2'. The 'MTU' is '1500'. The 'Priority' is '0'. The 'Propagate Security Group Tag' checkbox is unchecked. The 'Cancel' and 'OK' buttons are at the bottom right.

- a) 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。
- b) [有効 (Enabled)] チェックボックスをオンにします。
- c) [モード (Mode)] は [なし (None)] に設定したままにします。
- d) [セキュリティゾーン (SecurityZone)] 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。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てする必要があります。インターフェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。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。この場合、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。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

- e) [IPv4] タブ、または [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または DHCP オプションで入力します。  
たとえば、**192.168.1.1/24** などと入力します。



**Edit Physical Interface**

General IPv4 IPv6 **Advanced** Hardware Configuration FMC Access

IP Type:  
Use Static IP

IP Address:  
192.168.1.1/24  
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- [IPv6] : ステートレス自動設定を使用し、かつインターフェイスを有効にするために IPv6 DHCP または静的設定を使用する場合は、[自動設定 (Autoconfiguration)] チェックボックスをオンにします。

f) [OK] をクリックします。

**ステップ 4** 「外部」に使用するインターフェイス[編集 (Edit)] (✎) をクリックします。

[全般 (General)] タブが表示されます。

**Edit Physical Interface**

General **IPv4** IPv6 Advanced Hardware Configuration FMC Access

Name:  
Outside

Enabled  
 Management Only

Description:

Mode:  
None

Security Zone:  
outside-zone

Interface ID:  
GigabitEthernet0/2

MTU:  
1500  
(64 - 9000)

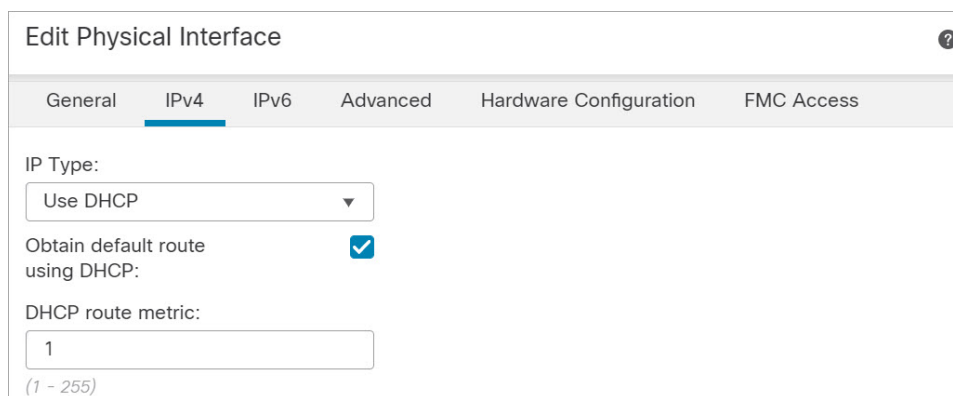
Priority:  
0  
(0 - 65535)

Propagate Security Group Tag:

Cancel OK



- a) 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。
- b) [有効 (Enabled)] チェックボックスをオンにします。
- c) [モード (Mode)] は [なし (None)] に設定したままにします。
- d) [セキュリティゾーン (SecurityZone)] 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。
- e) [IPv4] タブ、または [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。
    - [DHCPルートメトリック (DHCP route metric)] : アドミニストレーティブ 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ーティブ ディスタンスは 1 です。



The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown menu is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1', with a range of '(1 - 255)' indicated below the input field.

- [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。

f) [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。

## DHCP サーバーの設定



(注) AWS、Azure、GCP、OCIなどのパブリッククラウド環境に展開する場合は、この手順をスキップします。

クライアントで DHCP を使用して Threat Defense Virtual から IP アドレスを取得するようになる場合は、DHCP サーバーを有効にします。

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイス[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。

ステップ 3 [サーバー (Server)] ページで、[追加 (Add)] をクリックして、次のオプションを設定します。

- [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を選択します。
- [アドレスプール (Address Pool)] : DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の 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し示します。外部インターフェイスに DHCP を使用する場合は、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。DHCP サーバーからデフォルトルートを受信した場合は、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [ルーティング (Routing)] > [スタティックルート (Static Route)] ページの [IPv4ルート (IPv4 Routes)] または [IPv6ルート (IPv6 Routes)] テーブルに表示されます。

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

ステップ2 [ルーティング (Routing)] > [スタティックルート (Static route)] を選択し、[ルートを追加 (Add route)] をクリックして、次のように設定します。

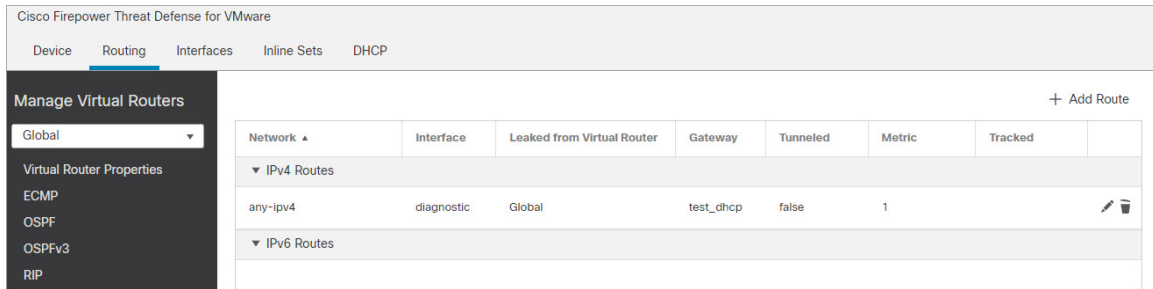
The screenshot shows the 'Add Static Route Configuration' dialog box. It has a title bar with a question mark icon. The 'Type' section has radio buttons for 'IPv4' (selected) and 'IPv6'. The 'Interface\*' dropdown is set to 'Outside'. Below it is a note: '(Interface starting with this icon [lock icon] signifies it is available for route leak)'. The 'Available Network' section has a search box and a list of networks: 'any-ipv4' (highlighted), 'any-IPv4-10.0.0.1', 'IPv4-Benchmark-Tests', 'IPv4-Link-Local', 'IPv4-Multicast', and 'IPv4-Private-10.0.0.0-8'. An 'Add' button is next to the search box. The 'Selected Network' section contains 'any-ipv4' with a trash icon. Below this is a note: 'Ensure that egress virtualrouter has route to that destination'. The 'Gateway' dropdown is set to 'any-IPv4-10.0.0.1'. The 'Metric' input field contains '1'. Below it is '(1 - 254)'. The 'Tunneled' checkbox is unchecked with the text '(Used only for default Route)'. The 'Route Tracking' dropdown is empty. At the bottom are 'Cancel' and 'OK' buttons.

- [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。
- [使用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]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。
- [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。
- [メトリック (Metric)] : 宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ~ 255 で、デフォルト値は 1 です。

## NAT の設定

ステップ3 [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4 [保存 (Save) ] をクリックします。

## NAT の設定

一般的な NAT ルールでは、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。

ステップ1 [デバイス (Devices) ] > [NAT] をクリックし、[新しいポリシー (New Policy) ] > [Threat Defense NAT] 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。

New Policy

Name:  
Interface\_PAT

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

FTDv 7.1.0 Build 1...

Add to Policy

Selected Devices

FTDv 7.1.0 Build 1...

Cancel Save

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。

**ステップ 3** [ルール の追加 (Add Rule) ] をクリックします。

[NAT ルール の追加 (Add NAT Rule) ] ダイアログ ボックス が表示 されます。

**ステップ 4** 基本ルール のオプション を設定 します。

Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

- [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。

**Add NAT Rule**

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects   Source Interface Objects (0)   Destination Interface Objects (1)

Search by name

outside-zone

Add to Source

Add to Destination

any

outside-zone

Cancel   OK

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。

**Add NAT Rule**

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet   Translated Packet

Original Source:\*  
any-IPv4-10.0.0.1

Original Port:  
TCP

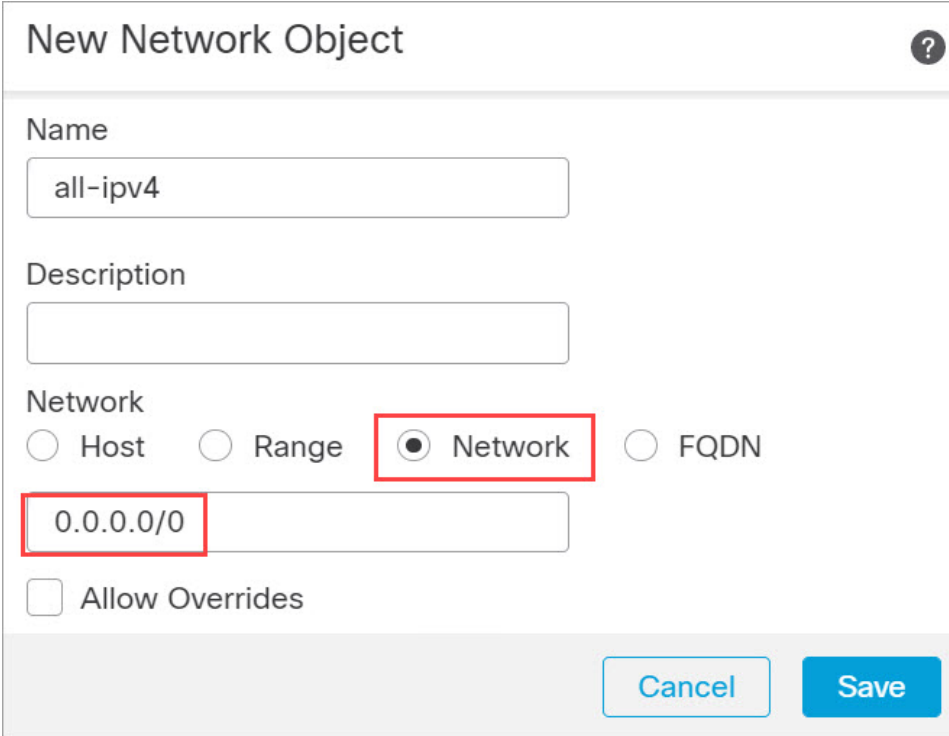
Translated Source:  
Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

Cancel   OK

- [元の送信元 (Original Source)] : 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。



New Network Object

Name  
all-ipv4

Description

Network  
 Host  Range  Network  FQDN

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。

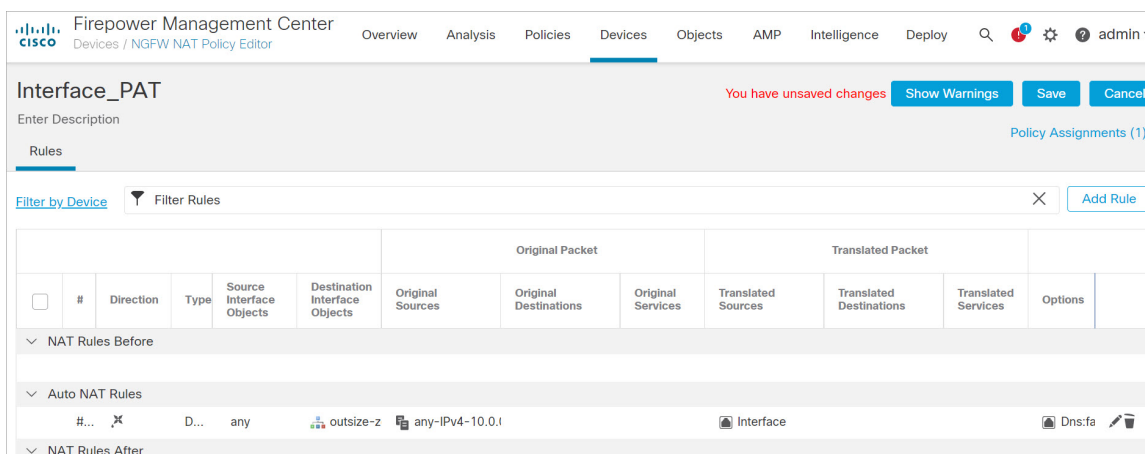
同様に、すべての IPv6 トラフィックに対してデフォルトのホストネットワーク `:::/0` を使用して NAT ポリシーを作成できます。

- [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。

## アクセス制御の設定

Threat Defense Virtual を Management Center に登録したときに、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。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

より高度なセキュリティ設定とルールを設定する場合は、[Firepower Management Center コンフィギュレーションガイド](#)のコンフィギュレーションガイドを参照してください。

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)] を選択し、Threat Defense 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。

The screenshot shows the 'Add Rule' configuration interface. The 'Name' field contains 'inside\_to\_outside' and is checked as 'Enabled'. The 'Insert' dropdown is set to 'into Mandatory'. The 'Action' is 'Allow' and 'Time Range' is 'None'. Below, the 'Available Zones' list includes 'inside-zone' and 'outside-zone'. 'inside-zone' is added to the 'Source Zones (1)' list, and 'outside-zone' is added to the 'Destination Zones (1)' list.

- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside\_to\_outside**) 。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] 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** [追加 (Add)] 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。

The screenshot shows the 'Initial AC Policy' configuration page. The 'Rules' tab is selected, displaying a table of rules. The table has columns for Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applications, Source Ports, Dest Ports, URLs, Source Dynamic Attributes, Dest Dynamic Attributes, and Action. One rule is listed: 'inside\_to\_outside' with action 'Allow'. The 'Default Action' is set to 'Access Control:Block all traffic'.

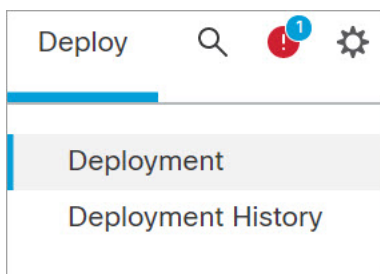
#	Name	Source Zones	Dest Zones	Source Netw...	Dest Netw...	VLAN Tags	Users	Appli...	Source Ports	Dest Ports	URLs	Source Dyna... Attr...	Desti... Dyna... Attr...	Act...
1	inside_to_outside	inside-zone	outside-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

**ステップ 4** [保存 (Save)] をクリックします。

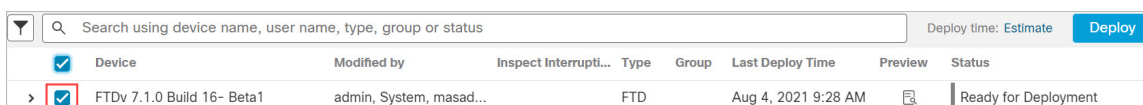
## 設定の展開

設定の変更を Threat Defense Virtual 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。

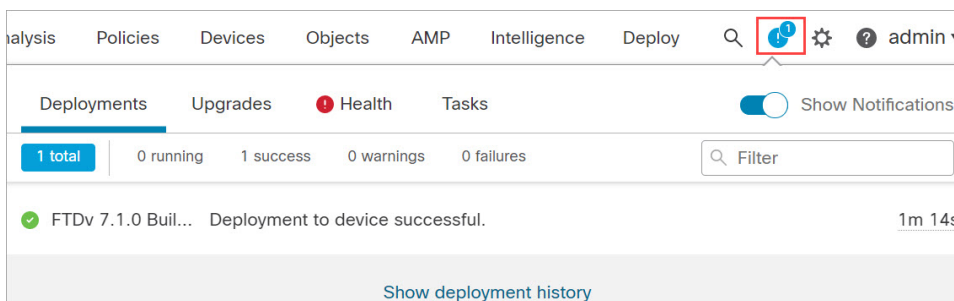
ステップ1 右上の [展開 (Deploy)] をクリックします。



ステップ2 [ポリシーの展開 (Deploy Policies)] ダイアログボックスでデバイスを選択し、[展開 (Deploy)] をクリックします。



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。



## Secure Firewall Threat Defense CLI へのアクセス

Threat Defense Virtual CLI を使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLIにアクセスするには、管理インターフェイスへの SSH を使用するか、VMware コンソールから接続します。

ステップ1 (オプション1) Threat Defense Virtual 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、仮想マシンを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して Threat Defense Virtual にログインします。

ステップ2 (オプション2) VMware コンソールを開き、初期展開時に設定したデフォルトのユーザー名「admin」アカウントとパスワードを使用してログインします。

## 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。