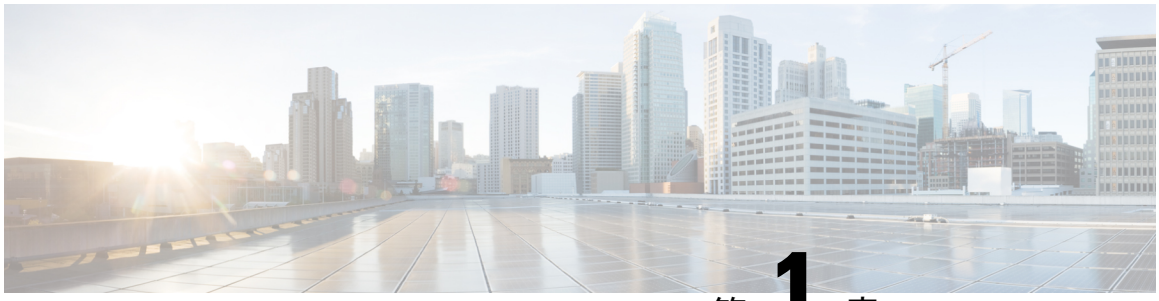
Cisco Firepower Threat Defense Virtual スタートアップガイド（KVM 向け）

初版：2019 年 4 月 24 日

最終更新：2020 年 11 月 2 日

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/



第 1 章

Firepower Threat Defense Virtual と KVM の利用開始

Cisco Firepower Threat Defense 仮想（FTDv）は、シスコの Firepower 次世代ファイアウォール機能を仮想化環境にもたらし、一貫性のあるセキュリティポリシーを実現して、物理、仮想、クラウドの各環境にわたって、またクラウド間で、ワークロードを実行します。

この章では、カーネルベース仮想マシン（KVM）のハイパーバイザ環境で FTDv が機能する仕組みについて説明します。機能のサポート、システム要件、ガイドライン、および制限事項について取り上げます。また、FTDv を管理する際のオプションについても説明します。

展開を開始する前に、管理オプションを理解しておくことが重要です。FTDv の管理と監視には Firepower Management Center または Firepower Device Manager を使用できます。その他の管理オプションを使用できる場合もあります。

KVM を使用した FTDv の展開について

KVM は、仮想化拡張機能（Intel VT など）を搭載した x86 ハードウェア上の Linux 向け完全仮想化ソリューションです。KVM は、コア仮想化インフラストラクチャを提供するロード可能なカーネル モジュール（kvm.ko）と kvm-intel.ko などのプロセッサ固有のモジュールで構成されています。

KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワーク カード、ディスク、グラフィック アダプタなどのプライベートな仮想化ハードウェアが搭載されています。

Firepower デバイスの管理方法

Firepower Threat Defense デバイスの管理には次の 2 つのオプションを選択できます。

Firepower Device Manager

Firepower Device Manager（FDM）オンボード統合マネージャ。

FDM は、一部の Firepower Threat Defense デバイスに組み込まれている Web ベースの設定インターフェイスです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。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。

（注） FDM をサポートしている Firepower Threat Defense デバイスのリストについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』を参照してください。

Firepower Management Center

Cisco Firepower Management Center（FMC）。

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は、組み込みの FDM の代わりに FMC を使用してデバイスを設定します。

重要 FDM と FMC の両方を使用して Firepower デバイスを管理することはできません。いったん FDM の統合管理を有効にすると、ローカル管理を無効にして、FMC を使用するように管理を再設定しない限り、FMC を使用して Firepower デバイスを管理することはできなくなります。一方、Firepower を FMC に登録すると、FDM のオンボード管理サービスは無効になります。

注意 現在、シスコには FDM Firepower 設定を FMC に移行するオプションはありません。その逆も同様です。Firepower デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

システム要件

Firepower Threat Defense 仮想のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

メモリ、vCPU、およびディスクのサイジング

Firepower Threat Defense 仮想 の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。FTDv の各インスタンスには、サーバ上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

（注） FTDv は、調整可能な vCPU およびメモリリソースを使用して展開されます。

表 *1*：バージョン *6.4* 以降の *FTDv* アプライアンスの設定

設定	デフォルト	設定調整の可否
メモリ	8 GB	はい（最大 32GB）
cCPU	4	はい（最大 16 個の vCPU）
ハードディスク プロビジョニング サイズ	50 GB	はい。virtio ブロック デバイスをサポート

次の 3 つの推奨/サポートされている vCPU/メモリ値があります。

- 4 vCPU/8 GB（デフォルト）
- 8 vCPU/16 GB
- 12 vCPU/24 GB

重要 その他の vCPU/メモリ値を設定できますが、上記の 3 つの組み合わせのみがサポートされています。vCPU/メモリの値を変更するには、最初に FTDv デバイスの電源をオフにする必要があります。

表 *2*：バージョン *6.3* 以前の *FTDv* アプライアンスの設定

設定	デフォルト	設定調整の可否
メモリ	8 GB	なし
vCPU	4	なし

設定	デフォルト	設定調整の可否
ハード ディスク プロビジョニング サイズ	50 GB	はい。virtio ブロック デバイスをサポート

（注） FTDv は固定構成 4vCPU/8GB デバイスとして展開されます。バージョン 6.3 以前では、vCPU とメモリの調整はサポートされていません。

ネットワーキング ガイドラインとベストプラクティス

- ブートするには 2 つの管理インターフェイスと 2 つのデータ インターフェイスが必要

（注） FTDv のデフォルト設定では、管理インターフェイス、診断インターフェイス、および内部インターフェイスは同じサブネットに配置されます。

  - virtio ドライバをサポート
  - SR-IOV の ixgbe-vf ドライバをサポート
  - 合計 10 個のインターフェイスをサポート

- FTDv のデフォルト設定では、管理インターフェイス（管理と診断）および内部インターフェイスが**同じサブネット**上にあり、管理アドレスはインターネットへのゲートウェイとして内部アドレスを使用すると仮定します（外部インターフェイス経由）。
- FTDv は、少なくとも 4 つのインターフェイスを備え、firstboot で電源がオンになる必要があります。4 つのインターフェイスがなければ展開は実行されません。
- FTDv では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワーク インターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。
  - 1. 管理インターフェイス（必須）
  - 2. 診断インターフェイス（必須）
  - 3. 外部インターフェイス（必須）
  - 4. 内部インターフェイス（必須）
  - 5 ～ 10. データ インターフェイス（オプション）

FTDv インターフェイスのネットワーク アダプタ、送信元ネットワーク、宛先ネットワークに関する以下の用語索引を参照してください。

表 *3*: 送信元から宛先ネットワークへのマッピング

ネットワーク アダプタ	送信元ネットワーク	宛先ネットワーク	機能
vnic0*	Management0-0	Management0/0	管理
vnic1	診断	診断	診断
vnic2*	GigabitEthernet0-0	GigabitEthernet 0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet 0/1	内部
* 重要同じサブネットに接続します。			

- OpenStack 環境に FTDv を導入する場合は、無差別モードで実行し、ポート セキュリティ（パケット フィルタリング）を無効にする必要があります。この操作を行うときに、セキュリティ グループまたは許可されたアドレス ペアがインターフェイスに割り当てられていると、ポート セキュリティを無効にできないことに注意してください。ポート レベルのセキュリティを無効にすると、すべてのトラフィック（イングレスとイーグレス）が許可されます。
- 仮想マシンの複製はサポートされません。
- コンソールアクセスでは、Telnet を介したターミナルサーバをサポートします。

SR-IOV のサポート

SR-IOV 仮想機能には特定のシステムリソースが必要です。SR-IOV 対応 PCIe アダプタに加えて、SR-IOV をサポートするサーバが必要です。以下のハードウェア検討事項に留意する必要があります。

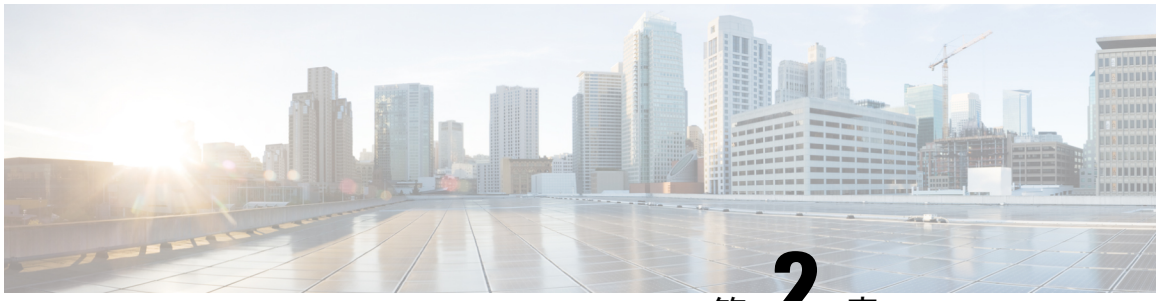
- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。次の NIC がサポートされています。
  - Intel Ethernet Server Adapter X710
  - Intel Ethernet Server Adapter X520 - DA2
- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。
- x86_64 マルチコア CPU：Intel Sandy Bridge 以降（推奨）。

（注） シスコでは、FTDv を 2.3GHz の Intel Broadwell CPU（E5-2699-v4）でテストしました。

- コア
  - CPU ソケットあたり 8 個以上の物理コア。
  - 単一のソケット上で 8 コアにする必要があります。

（注） CPU ピンニングは、フルスループットを実現するために推奨されています。

- メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。KVM の場合は、SR-IOV サポートの CPU の互換性を確認できます。KVM 上の FTDv では、x86 ハードウェアしかサポートされないことに注意してください。



第 2 章

Firepower Threat Defense Virtual の展開

この章では、Firepower Threat Defense 仮想 を KVM 環境に展開する手順について説明します。

KVM を使用した導入の前提条件

- Cisco.com から Firepower Threat Defense Virtual の qcow2 ファイルをダウンロードし、Linux ホストに格納します。

  https://software.cisco.com/download/navigator.html

  （注） Cisco.com のログインおよびシスコ サービス契約が必要です。

- このマニュアルの導入例では、ユーザが Ubuntu 18.04 LTS を使用していることを前提としています。Ubuntu 18.04 LTS ホストの最上部に次のパッケージをインストールします。
  - qemu-kvm
  - libvirt bin
  - bridge-utils
  - Virt-Manager
  - virtinst
  - virsh tools
  - genisoimage

- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での Firepower Threat Defense Virtual のスループットを最大化できます。一般的なホスト調

整の概念については、『Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture』を参照してください。

- 以下の機能は Ubuntu 18.04 LTS の最適化に役立ちます。
  - macvtap：高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
  - Transparent Huge Pages：メモリ ページ サイズを増加させます。Ubuntu 18.04 では、デフォルトでオンになっています。
  - Hyperthread disabled：2 つの vCPUを 1 つのシングル コアに削減します。
  - txqueuelength：デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップ レートを低減します。
  - pinning：qemu および vhost プロセスを特定のCPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。
- RHEL ベースのディストリビューションの最適化については、『Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide』を参照してください。
- KVM と Firepower System の互換性については、「Cisco Firepower Threat Defense Virtual Compatibility」を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

FTDv を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキストファイルです。この初期設定は、「day0-config」というテキストファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。

重要 day0.iso ファイルは、最初のブート時に使用できる必要があります。

第 0 日のコンフィギュレーション ファイルを使用して展開する場合、プロセスで、FTDv アプライアンスの初期設定全体を実行できます。次を指定することができます。

- エンド ユーザ ライセンス契約書（EULA）の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- 管理モード。Firepower デバイスの管理方法 （2 ページ）を参照してください。

[ローカルに管理（ManageLocally）] を [はい（Yes）] に設定するか、または Firepower Management Center フィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に情報を入力することができます。使用していない管理モードでは、フィールドを空のままにします。

- 最初のファイアウォール モード。最初のファイアウォール モード（**ルーテッド**または**トランスペアレント**）を設定します。

  ローカルの Firepower Device Manager（FDM）を使用して展開を管理する予定の場合は、ファイアウォール モードに**ルーテッド**のみ入力できます。FDM を使用して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。

- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。

第 0 日のコンフィギュレーション ファイルを使用せずに展開する場合は、起動後に Firepower システムの必須設定を指定する必要があります。詳細については、「第 0 日のコンフィギュレーション ファイルを使用しない起動 （15 ページ）」を参照してください。

（注） この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

手順の概要

1. 「day0-config」というテキストファイルに Firepower Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Firepower Management Center の管理に関する情報を追加します。
2. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。
3. 手順を繰り返して、導入する FTDv ごとに一意のデフォルト設定ファイルを作成します。

手順の詳細

ステップ 1 「day0-config」というテキストファイルに Firepower Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Firepower Management Center の管理に関する情報を追加します。

例：

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
```

```
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"Yes"

}
```

ローカルの Firepower Device Manager（FDM）を使用するには、第 0 日のコンフィギュレーション ファイル内で [ローカルに管理（ManageLocally）] に対して [はい（Yes）] と入力します。または、Firepower Management Center のフィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に入力します。使用していない管理オプションの場合は、これらのフィールドを空白のままにします。

ステップ 2 テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

または

例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

ステップ 3 手順を繰り返して、導入する FTDv ごとに一意のデフォルト設定ファイルを作成します。

次のタスク

- virt-install を使用している場合は、virt-install コマンドに次の行を追加します。

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- virt-manager を使用している場合、virt-manager の GUI を使用して仮想 CD-ROM を作成できます。「Virtual Machine Manager を使用した起動 （13 ページ）」を参照してください。

Firepower Threat Defense Virtual の起動

導入スクリプトを使用した起動

virt-install ベースの導入スクリプトを使用して FTDv を起動できます。

環境に最適なゲスト キャッシング モードを選択してパフォーマンスを最適化できることに注意してください。使用中のキャッシュ モードは、データ損失が発生するかどうかに影響を与え、キャッシュ モードはディスクのパフォーマンスにも影響します。

各 KVM ゲスト ディスク インターフェイスで、指定されたいずれかのキャッシュモード（*writethrough*、*writeback*、*none*、*directsync*、または *unsafe*）を指定できます。*writethrough* モードは読み取りキャッシュを提供します。*writeback* は読み取り/書き込みキャッシュを提供しま

す。*directsync* はホストページキャッシュをバイパスします。*unsafe* はすべてのコンテンツをキャッシュし、ゲストからのフラッシュ要求を無視する可能性があります。

- *cache=writethrough* は、ホストで突然の停電が発生した場合の KVM ゲスト マシン上のファイル破損を低減できます。*writethrough* モードの使用をお勧めします。
- ただし、*cache=writethrough* は、*cache=none* よりディスク I/O 書き込みが多いため、ディスク パフォーマンスに影響する可能性もあります。
- *--disk* オプションの cache パラメータを削除する場合、デフォルトは *writethrough* になります。
- キャッシュ オプションを指定しないと、VM を作成するために必要な時間も大幅に短縮される場合もあります。これは、古いRAID コントローラにはディスク キャッシング能力が低いものがあることが原因です。そのため、ディスク キャッシングを無効にして（*ache=none*）、*writethrough* をデフォルトに設定すると、データの整合性を確保できます。
- バージョン 6.4 以降では、FTDv は、調整可能な vCPU およびメモリ リソースを使用して展開されます。バージョン 6.4 より前のバージョンでは、FTDv は、固定構成 4vCPU/8GB デバイスとして展開されていました。各 FTDv プラットフォームサイズの --vcpus および --ram パラメータでサポートされている値については、次の表を参照してください。

表 *4 : virt-install* でサポートされる *vCPU* およびメモリ パラメータ

--vcpus	**--ram**	**FTDv プラットフォームのサイズ**
4	8192	4vCPU/8GB（デフォルト）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

ステップ 1 「virt_install_ftdv.sh」という virt-install スクリプトを作成します。

FTDv VM の名前は、この KVM ホスト上の他の仮想マシン（VM）全体において一意であることが必要です。FTDv は最大 10 個のネットワーク インターフェイスをサポートできます。この例では、4 つのインターフェイスを使用しています。仮想 NIC は Virtio でなければなりません。

（注） FTDv のデフォルト設定では、管理インターフェイス、診断インターフェイス、および内部インターフェイスは**同じサブネット**上に配置すると仮定します。システムでは、少なくとも 4 つのインターフェイスが正常に起動する必要があります。仮想 NIC は Virtio でなければなりません。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

- 1. 管理インターフェイス（必須）
- 2. 診断インターフェイス（必須）
- 3. 外部インターフェイス（必須）
- 4. 内部インターフェイス（必須）

- 5. （オプション）データインターフェイス：最大6

例：

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --disk path==<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet
   --force
```

ステップ 2 virt_install スクリプトを実行します。

例：

```
/usr/bin/virt_install_ftdv.sh

Starting install...
Creating domain...
```

ウィンドウが開き、VMのコンソールが表示されます。VMが起動中であることを確認できます。VMが起動するまでに数分かかります。VM が起動したら、コンソール画面から CLI コマンドを実行できます。

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルに管理（ManageLocally）] で [いいえ（No）] を選択した場合は、Firepower Management Center を使用して FTDv を管理します。「Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 （29 ページ）」を参照してください。
- [ローカルに管理（ManageLocally）] で [はい（Yes）] を選択した場合は、統合された Firepower Device Manager を使用して FTDv を管理します。「Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理 （19 ページ）」を参照してください。

管理オプションの選択方法の概要については、「Firepowerデバイスの管理方法 （2ページ）」を参照してください。

Virtual Machine Manager を使用した起動

virt-manager（Virtual Machine Manager とも呼ばれる）を使用して FTDv を起動します。virt-manager は、ゲスト仮想マシンを作成および管理するためのグラフィカル ツールです。

ステップ 1 virt-manager を起動します（**[アプリケーション（Applications）] > [システムツール（System Tools）] > [仮想マシンマネージャ（Virtual Machine Manager）]**）。

ハイパーバイザの選択、およびルート パスワードの入力を求められる可能性があります。

ステップ 2 左上隅のボタンをクリックし、[VMの新規作成（New VM）] ウィザードを開きます。

ステップ 3 仮想マシンの詳細を入力します。

a) オペレーティング システムの場合、[既存のディスクイメージをインポート（Import existing disk image）] を選択します。

この方法でディスク イメージ（事前にインストールされた、ブート可能なオペレーティング システムを含んでいるもの）をインポートできます。

b) [次へ（Forward）] をクリックして続行します。

ステップ 4 ディスク イメージをロードします。

a) [参照...（Browse...）] をクリックしてイメージ ファイルを選択します。
b) [OSタイプ（OS type）] には [汎用（Generic）] を選択します。
c) [次へ（Forward）] をクリックして続行します。

ステップ 5 メモリおよび CPU オプションを設定します。

バージョン 6.4 以降では、FTDv は、調整可能な vCPU およびメモリリソースを使用して展開されます。バージョン 6.4 より前のバージョンでは、FTDv は、固定構成 4vCPU/8GB デバイスとして展開されていました。各 FTDv プラットフォームサイズの --vcpus および --ram パラメータでサポートされている値については、次の表を参照してください。

表 *5*：仮想マシンマネージャでサポートされる *vCPU* およびメモリパラメータ

CPU	メモリ	FTDv プラットフォームのサイズ
4	8192	4vCPU/8GB（デフォルト）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

a) FTDv プラットフォームサイズに対応する**メモリ（RAM）**パラメータを設定します。
b) FTDv プラットフォーム サイズに対応する **CPU** パラメータを設定します。
c) [次へ（Forward）] をクリックして続行します。

ステップ 6 [インストール前に設定をカスタマイズする（Customize configuration before install）] チェックボックスをオンにして、[名前（Name）] を指定してから [完了（Finish）] をクリックします。

この操作を行うと、別のウィザードが開き、仮想マシンのハードウェア設定を追加、削除、設定することができます。

ステップ 7 CPU 構成を次のように変更します。

左側のパネルから [プロセッサ（Processor）] を選択し、**[設定（Configuration）] > [ホストCPU構成のコピー（Copy host CPU configuration）]** を選択します。

これによって、物理ホストの CPU モデルと設定が仮想マシンに適用されます。

ステップ 8 仮想ディスクを設定します。

a) 左側のパネルから [ディスク1（Disk 1）] を選択します。
b) [詳細オプション（Advanced Options）] をクリックします。
c) [ディスクバス（Disk bus）] を [Virtio] に設定します。
d) [ストレージ形式（Storage format）] を [qcow2] に設定します。

ステップ 9 シリアル コンソールを設定します。

a) 左側のパネルから [コンソール（Console）] を選択します。
b) [削除（Remove）] を選択してデフォルト コンソールを削除します。
c) [ハードウェアを追加（Add Hardware）] をクリックしてシリアル デバイスを追加します。
d) [デバイスタイプ（Device Type）] で、[TCP net console (tcp)] を選択します。
e) [モード（Mode）] で、[サーバモード（バインド）（Server mode (bind)）] を選択します。
f) [ホスト（Host）] には「**0.0.0.0**」と入力し、IP アドレスと一意の**ポート**番号を入力します。
g) [Telnetを使用（Use Telnet）] ボックスをオンにします。
h) デバイス パラメータを設定します。

ステップ 10 KVMゲストがハングまたはクラッシュしたときに何らかのアクションが自動でトリガーされるようウォッチドッグ デバイスを設定します。

a) [ハードウェアを追加（Add Hardware）] をクリックしてウォッチドック デバイスを追加します。
b) [モデル（Model）] で、[デフォルト（default）] を選択します。
c) [アクション（Action）] で、[ゲストを強制的にリセット（Forcefully reset the guest）] を選択します。

ステップ 11 少なくとも 4 つの仮想ネットワーク インターフェイスを設定します。

[ハードウェアの追加（Add Hardware）] をクリックしてインターフェイスを追加し、**macvtap** を選択するか、共有デバイス名を指定します（ブリッジ名を使用）。

（注） KVM 上の FTDv では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データ トラフィック用ネットワーク インターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

vnic0：管理インターフェイス（必須）

vnic1：診断インターフェイス（必須）

vnic2：外部インターフェイス（必須）

vnic3：内部インターフェイス（必須）

vnic4-9：データ インターフェイス（オプション）

重要　vnic0、vnic1、および vnic3 は、必ず同じサブネットにマップするようにしてください。

ステップ 12　第 0 日のコンフィギュレーション ファイルを使用して展開する場合、ISO の仮想 CD-ROM を作成します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) [ストレージ（Storage）] を選択します。
c) [管理対象またはその他既存のストレージを選択（Select managed or other existing storage）] をクリックし、ISO ファイルの場所を参照します。
d) [デバイスタイプ（Device type）] で、[IDE CDROM] を選択します。

ステップ 13　仮想マシンのハードウェアを設定した後、[適用（Apply）] をクリックします。

ステップ 14　virt-manager の [インストールの開始（Begin installation）] をクリックして、指定したハードウェア設定で仮想マシンを作成します。

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルに管理（ManageLocally）] で [いいえ（No）] を選択した場合は、Firepower Management Center を使用して FTDv を管理します。「Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 （29 ページ）」を参照してください。
- [ローカルに管理（ManageLocally）] で [はい（Yes）] を選択した場合は、統合された Firepower Device Manager を使用して FTDv を管理します。「Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理 （19 ページ）」を参照してください。

管理オプションの選択方法の概要については、「Firepower デバイスの管理方法 （2 ページ）」を参照してください。

第 0 日のコンフィギュレーション ファイルを使用しない起動

FTDv アプライアンスには Web インターフェイスがないため、第 0 日のコンフィギュレーション ファイルを使用せずに展開した場合には、CLI を使用して仮想デバイスを設定する必要があります。

新しく展開されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアッププロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定およびファイアウォールモードを設定します。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が (*y*/*n*) のように括弧で囲まれて示されます。デフォルト値は、[*y*] のように大カッコ内に列挙されます。選択を確定するには、Enter キーを押します。

（注） 初期セットアップの完了後に仮想デバイスに関するこれらの設定を変更するには、CLI を使用する必要があります。

ステップ 1 FTDv でコンソールを開きます。

ステップ 2 [firepower ログイン（firepower login）] プロンプトで、ユーザ名 *admin* とパスワード *Admin123* のデフォルトのクレデンシャルでログインします。

ステップ 3 Firepower Threat Defense システムが起動すると、セットアップ ウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス
- システム名
- デフォルトゲートウェイ
- DNS セットアップ
- HTTP プロキシ
- 管理モード（ローカル管理が必要）

ステップ 4 セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

ステップ 5 プロンプトに従ってシステム設定を行います。

ステップ 6 コンソールが firepower # プロンプトに戻るときに、設定が正常に行われたことを確認します。

ステップ 7 CLI を閉じます。

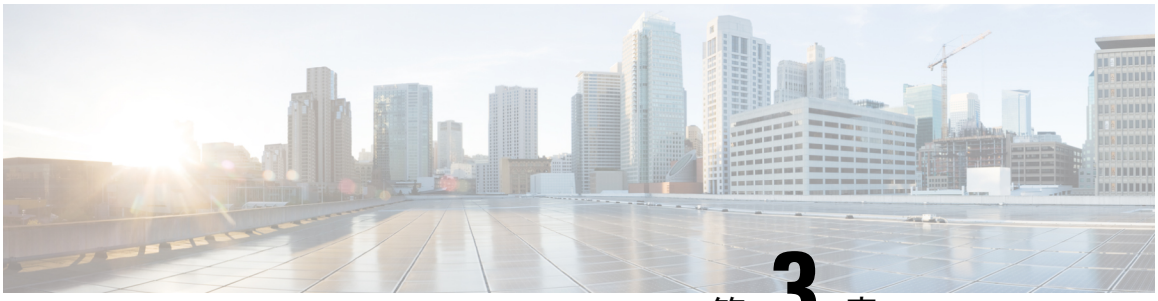
次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Firepower Management Center を使用して FTDv を管理します。「Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 （29 ページ）」を参照してください。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、統合されている Firepower Device Manager を使用して FTDv を管理します。「Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理 （19 ページ）」を参照してください。

管理オプションの選択方法の概要については、「Firepowerデバイスの管理方法 （2ページ）」を参照してください。



第 3 章

Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理

この章では、FDM を使用して管理されるスタンドアロンの FTDv デバイスを展開する方法について説明します。高可用性ペアを展開する場合は、FDM の設定ガイドを参照してください。

Firepower Device Manager を使用した Firepower Threat Defense Virtual について

Firepower Threat Defense 仮想（FTDv）は、Cisco NGFW ソリューションの仮想化コンポーネントです。FTDv 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、高度なマルウェア防御（AMP）などの次世代ファイアウォールサービスを提供します。

FTDv の管理には Firepower Device Manager（FDM）を使用できます。これは、一部の Firepower Threat Defense モデルに組み込まれている Web ベースのデバイス セットアップ ウィザードです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。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は、組み込みの Firepower Device Manager の代わりに Firepower Management Center を使用してデバイスを設定します。詳細については、「Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 （29 ページ）」を参照してください。

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 FTD CLI にアクセスすることも、Firepower CLI から FTD に接続することもできます。

デフォルト設定

FTDv のデフォルト設定では、管理インターフェイスと内部インターフェイスは同じサブネットに配置されます。スマートライセンスを使用する場合やシステムデータベースへの更新プログラムを取得する場合は、管理インターフェイスにインターネット接続が必要です。

そのため、デフォルト設定は、Management 0-0 と GigabitEthernet 0-1（内部）の両方を仮想スイッチ上の同じネットワークに接続できるように設計されています。デフォルトの管理アドレスは、内部 IP アドレスをゲートウェイとして使用します。したがって、管理インターフェイスは内部インターフェイスを介してルーティングし、その後、外部インターフェイスを介してルーティングして、インターネットに到達します。

また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに Management 0-0 を接続することもできます。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

FTDv は、初回起動時に少なくとも 4 つのインターフェイスで電源がオンになる必要があります。

- 仮想マシン上の 1 番目のインターフェイス（Management 0-0）は、管理インターフェイスです。
- 仮想マシン上の 2 番目のインターフェイス（Diagnostic 0-0）は、診断インターフェイスです。
- 仮想マシン上の 3 番目のインターフェイス（GigabitEthernet 0-0）は、外部インターフェイスです。
- 仮想マシン上の 4 番目のインターフェイス（GigabitEthernet 0-1）は、内部インターフェイスです。

データ トラフィック用に最大 6 つのインターフェイスを追加し、合計で 8 つのデータ インターフェイスを使用できます。追加のデータ インターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データ インターフェイスが一意のサブネットまたは VLAN にマッピングされていることを確認します。「VMware インターフェイスの設定」を参照してください。

初期設定

FTDv の機能をネットワークで正しく動作させるには、初期設定を完了する必要があります。これには、セキュリティアプライアンスをネットワークに挿入して、インターネットまたは他の上流に位置するルータに接続するために必要なアドレスの設定が含まれます。2 つの方法のいずれかでシステムの初期設定を行うことができます。

- FDM Web インターフェイスの使用（推奨）。FDM は Web ブラウザで実行します。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）セットアップウィザードを使用します（オプション）。FDM の代わりに CLI のセットアップウィザードを初期設定に使用できます。またトラブルシューティングに CLI を使用できます。システムの設定、管理、監視には引き続き FDM 使用します。「Firepower Threat Defense CLI ウィザードの起動（オプション）」を参照してください。

次のトピックでは、これらのインターフェイスを使用してシステムの初期設定を行う方法について説明します。

Firepower Device Manager の起動

Firepower Device Manager（FDM）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。

ステップ 1 ブラウザを開き、FDM にログインします。CLI での初期設定を完了していない場合は、Firepower Device Manager を **https://***ip-address* で開きます。このアドレスは次のいずれかになります。

- 内部のブリッジ グループ インターフェイスに接続されている場合は **https://192.168.1.1**。
- Management 物理インターフェイスに接続されている場合は **https://192.168.45.45**。

ステップ 2 ユーザ名 **admin**、およびパスワード **Admin123** を使用してログインします。

ステップ 3 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、これらの手順を完了する必要があります。

ステップ 4 外部インターフェイスおよび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） [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。設定値が正しいことを確認します。

a) [外部インターフェイス（Outside Interface）]：これは、ゲートウェイモードまたはルータに接続するためのデータポートです。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

[IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック 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。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。

[IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック 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。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

b) **[管理インターフェイス（Management Interface）]**

[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。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

（注） デバイス セットアップ ウィザードを使用して Firepower Threat Defense デバイスを設定する場合は、アウトバウンドとインバウンドのトラフィックに対してシステムから 2 つのデフォルトアクセスルールが提供されます。初期セットアップ後に、これらのアクセスルールに戻って編集できます。

ステップ 5 システム時刻を設定し、[次へ（Next）] をクリックします。

a) [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。

b) [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 6 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日間の評価期間を開始する（Start 90 day evaluation period without registration）] を選択します。後でデバイスを登録し、スマートライセンスを取得するには、メニューからデバイスの名前をクリックして [デバイスダッシュボード（Device Dashboard）] に進み、[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 7 [終了（Finish）] をクリックします。

次のタスク

- Firepower Device Manage を使用してデバイスを設定します。「Firepower Device Manager でデバイスを設定する方法 （22 ページ）」を参照してください。

Firepower Device Manager でデバイスを設定する方法

セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。

- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスまたはブリッジグループで実行されている DHCP サーバ。

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン（**?**）をクリックしてください。

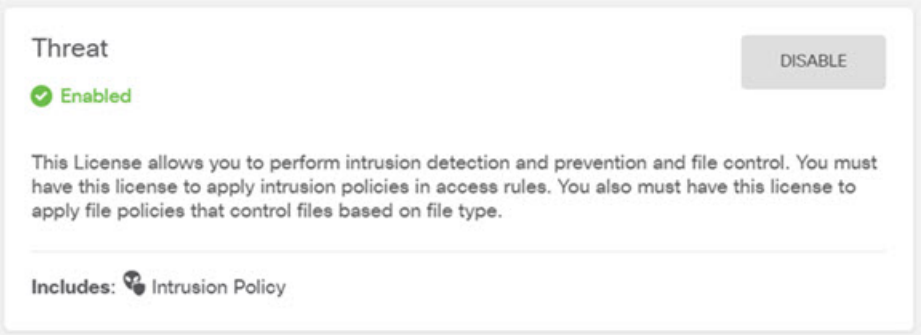
ステップ 1 [デバイス（Device）] を選択してから、[スマートライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

使用するオプションのライセンス（[脅威（Threat）]、[マルウェア（Malware）]、[URL]）でそれぞれ [有効化（Enable）] をクリックします。セットアップ中にデバイスを登録した場合は、必要な RA VPN ライセンスも有効にできます。必要かどうかわからない場合は、各ライセンスの説明を確認します。

登録していない場合は、このページから登録できます。[登録の要求（Request Register）] をクリックして、手順に従います。評価ライセンスの有効期限が切れる前に登録してください。

たとえば、有効な脅威ライセンスは次のようになります。

図 *1*：有効な脅威ライセンス

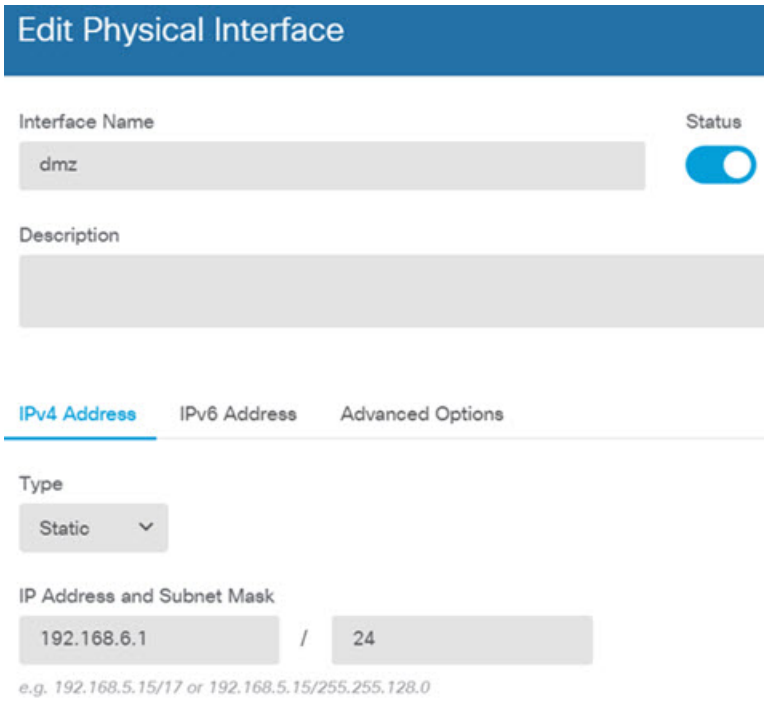


ステップ 2 他のインターフェイスを設定した場合は、[デバイス（Device）] を選択してから、[インターフェイス（Interfaces）] グループの [設定の表示（View Configuration）] をクリックして、各インターフェイスを設定します。

他のインターフェイスのブリッジグループを作成するか、別々のネットワークを設定するか、または両方の組み合わせを設定できます。各インターフェイスの [編集（Edit）] アイコン（）をクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。完了したら [保存（Save）] をクリックします。

図 *2:* インターフェイスの編集



ステップ 3 新しいインターフェイスを構成する場合は、[オブジェクト（Objects）] を選択し、目次から[セキュリティゾーン（Security Zones）] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティ ゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後には常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZ インターフェイスのために新しい DMZ ゾーンを作成する方法を示します。

図 *3*:セキュリティ ゾーン オブジェクト

ステップ 4 内部クライアントでDHCPを使用してデバイスからIPアドレスを取得する場合は、**[デバイス（Device）]**>**[システム設定（System Settings）]** > **[DHCPサーバ（DHCP Server）]** を選択してから、**[DHCPサーバ（DHCP Servers）]** タブを選択します。

すでに内部インターフェイス用に構成されているDHCPサーバがありますが、アドレス プールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上にDHCP サーバをセットアップするのがごく一般的です。[+] をクリックして各内部インターフェイスのサーバとアドレスプールを構成します。

[構成（Configuration）] タブでクライアントに提供されるWINSおよびDNSのリストを微調整することもできます。次の例では、アドレス プールの 192.168.4.50 ～ 192.168.4.240 で inside2 インターフェイス上のDHCP サーバを設定する方法を示しています。

図 *4*:*DHCP* サーバ

ステップ 5 [デバイス（Device）] を選択してから、[ルーティング（Routing）] グループで [設定の表示（View Configuration）]（または [最初のスタティックルートを作成（Create First Static Route）]）をクリックし、デフォルトルートを構成します。

デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4（0.0.0.0/0）、デフォルトの IPv6 ルートは任意の ipv6（::0/0）です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

（注） このページで定義したルートは、データ インターフェイス用のみです。管理インターフェイスには影響しません。**[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）]** で管理ゲートウェイを設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです（アドレスは ISP から取得する必要があります）。[ゲートウェイ（Gateway）] の下部の [新しいネットワークを作成する（Create New Network）] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

図 *5:* デフォルトルート

ステップ 6 [ポリシー（Policies）] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間のトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーン オブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

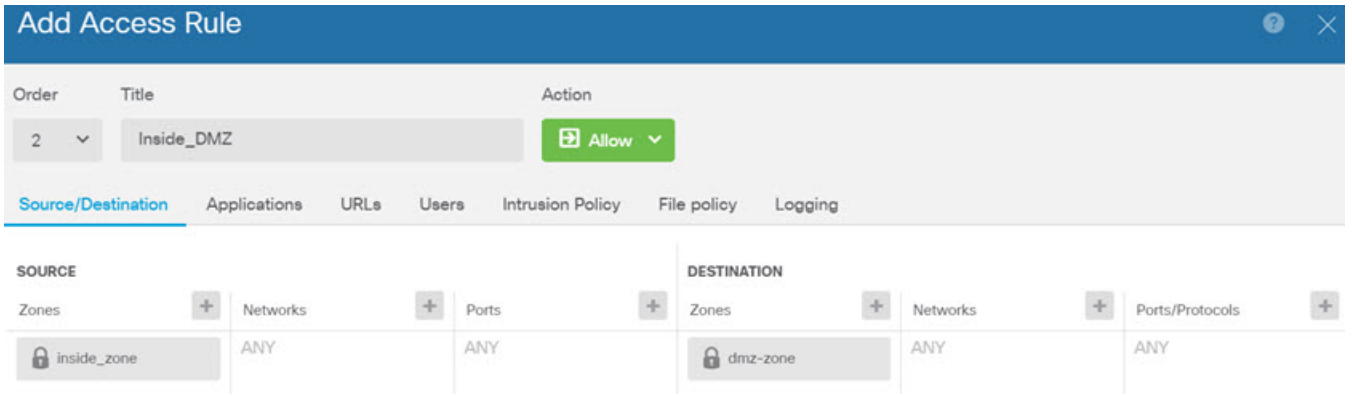
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ（Identity）]：個々のユーザにネットワーク アクティビティを関連付ける、またはユーザまたはユーザ グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティ ポリシーを使用します。
- [セキュリティインテリジェンス（Security Intelligence）]：ブラックリスト登録済みの IP アドレスまたはURL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセス コントロール ポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスやURL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT]（ネットワークアドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザ グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用してURL フィルタリングを実装します。
- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間のトラフィックを許可する方法を示します。この例では、[接続の最後で（At End of Connection）]が選択されている場合、[ロギング（Logging）]を除いて他のいずれのタブでもオプションは設定されません。

図 *6:* アクセス コントロール ポリシー



ステップ 7 [デバイス（Device）] を選択してから、[更新（Updates）] グループで [設定の表示（View Configuration）] をクリックし、システムデータベースの更新スケジュールを設定します。

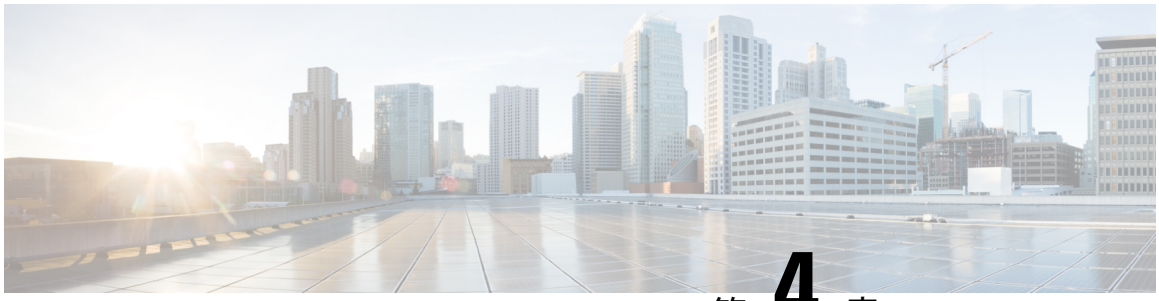
侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 8 メニューの [導入（Deploy）] ボタンをクリックし、[今すぐ導入する（Deploy Now）] ボタン（  ）をクリックして、変更内容をデバイスに展開します。

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。

次のタスク

Firepower Device Manager による Firepower Threat Defense 仮想 の管理の詳細については、『『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』』または Firepower Device Manager のオンラインヘルプを参照してください。



第 4 章

Firepower Management Center を使用した Firepower Threat Defense Virtual の管理

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

（注） 本書では、最新の FTDv バージョンの機能を取り上げています。機能の変更の詳細については、「Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴 （44 ページ）」を参照してください。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 FMC 設定ガイドの手順を参照してください。

Firepower Management Center を使用した Firepower Threat Defense Virtual について

Firepower Threat Defense 仮想（FTDv）は、Cisco NGFW ソリューションの仮想化コンポーネントです。FTDv 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、高度なマルウェア防御（AMP）などの次世代ファイアウォールサービスを提供します。

FTDv を管理するには、別のサーバ上で実行されるフル機能のマルチデバイスマネージャである Firepower Management Center（FMC）を使用します。FMC のインストールの詳細については、『FMCgetting started guide』を参照してください。

FTDv は、FTDv 仮想マシンに割り当てた管理インターフェイス上の FMC 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 FTD CLI にアクセスすることも、Firepower CLI から FTD に接続することもできます。

Firepower Management Center へのログイン

FMC を使用して、 FTD 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://*fmc_ip_address*

- *fmc_ip_address*：FMC の IP アドレスまたはホスト名を指定します。

ステップ 2 ユーザ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。

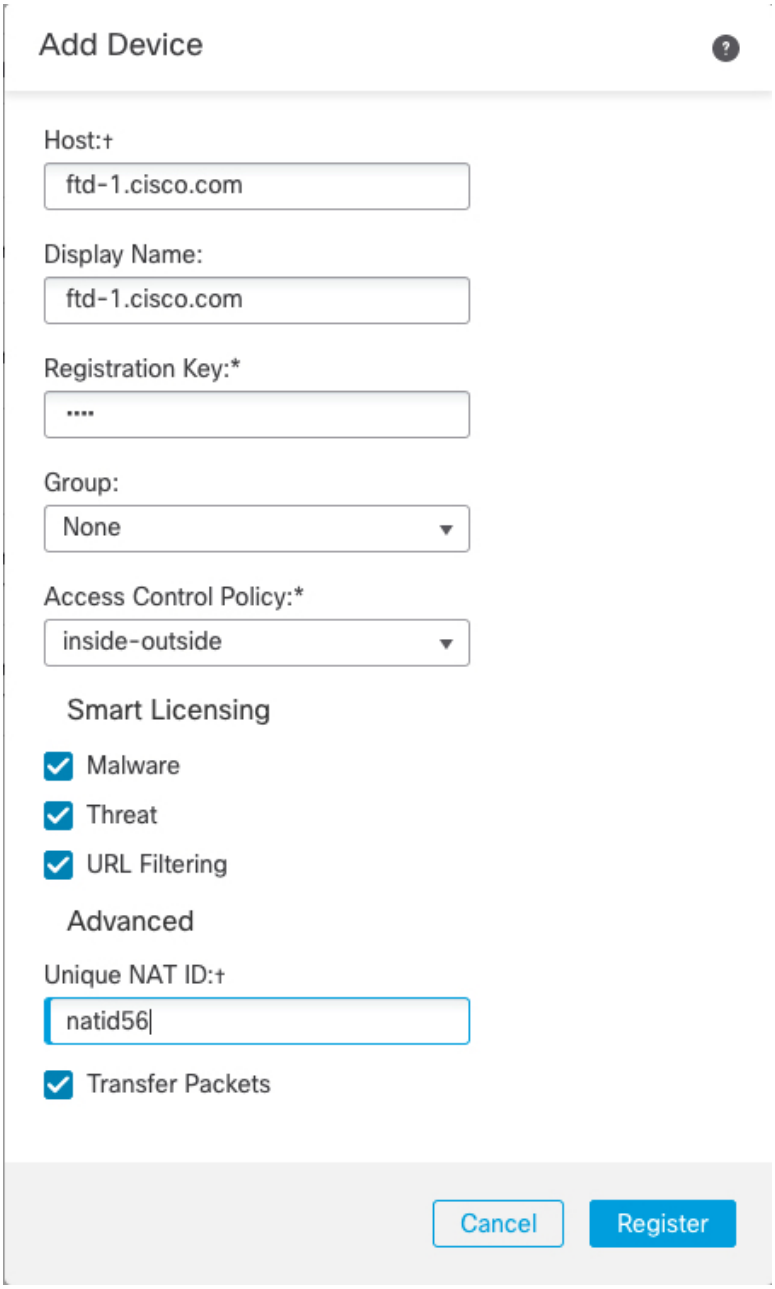
Firepower Management Center へのデバイスの登録

始める前に

FTDv 仮想マシンが、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。

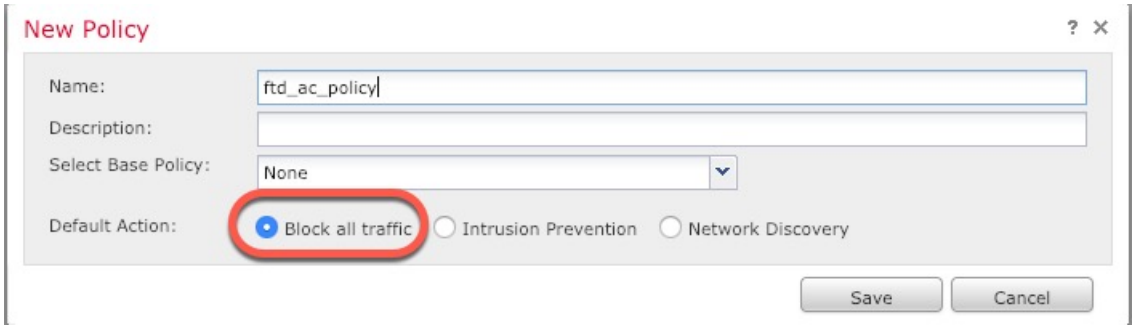
ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

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。



- [ホスト（Host）]：追加する論理デバイスの IP アドレスを入力します。FTD ブートストラップ設定で FMC の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。
- [表示名（Display Name）]：FMC に表示する論理デバイスの名前を入力します。
- [登録キー（Registration key）]：FTDv ブートストラップ設定で指定したものと同じ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 （42 ページ）」を参照してください。



- [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）]（AMP マルウェア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装する予定の場合）を割り当てます。
- [一意の NAT ID（Unique NAT ID）]：FTDv 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 FMC 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 FMC 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 FMC 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す。FTDv 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：FTD CLI（「Firepower Threat Defense CLI へのアクセス （44 ページ）」）にアクセスし、次のコマンドを使用して FMC 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。FTD IP アドレスを変更する必要がある場合は、**configure network {ipv4 | ipv6} manual** コマンドを実行します。

- NTP：NTP サーバが **[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]** ページの FMC サーバセットと一致することを確認します。
- 登録キー、NAT ID、および FMC 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** コマ

ンドを使用して、FTDv 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 FMC 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：クライアントの内部インターフェイスで DHCP サーバを使用します。
- 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 （33 ページ）
ステップ 2 DHCP サーバの設定 （37 ページ）
ステップ 3 デフォルトルートの追加 （38 ページ）
ステップ 4 NAT の設定 （39 ページ）
ステップ 5 アクセス制御の設定 （42 ページ）
ステップ 6 設定の展開 （43 ページ）

インターフェイスの設定

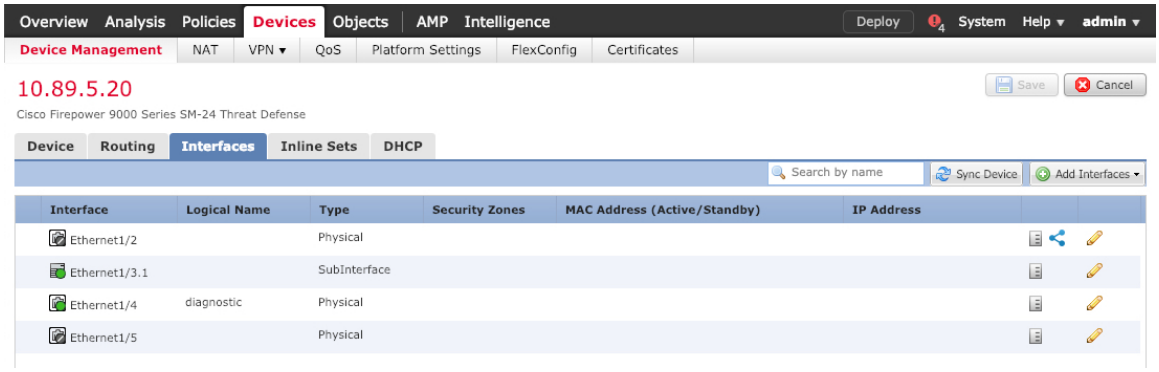
FTDv インターフェイスを有効にし、それらをセキュリティゾーンに割り当て、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

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。

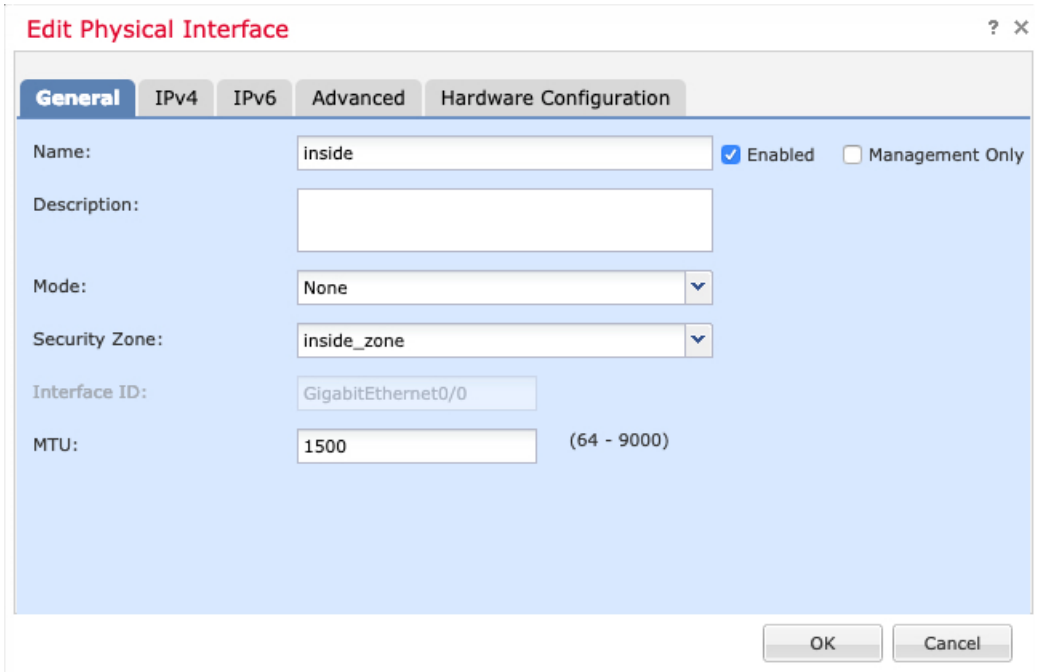
ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]** を選択し、デバイスの をクリックします。

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



ステップ 3 「内部」に使用するインターフェイスの をクリックします。

[全般（General）] タブが表示されます。



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。

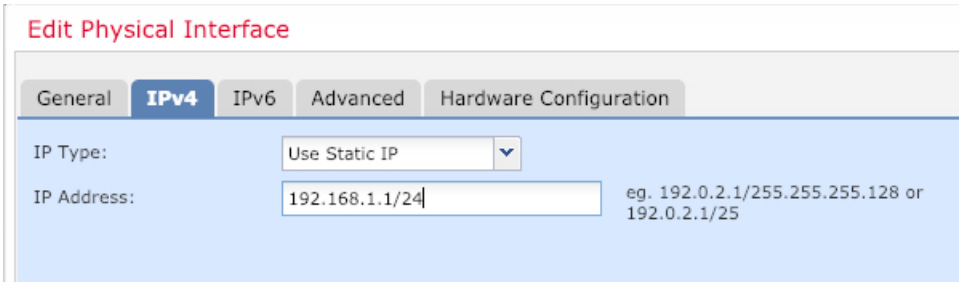
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。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、[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。

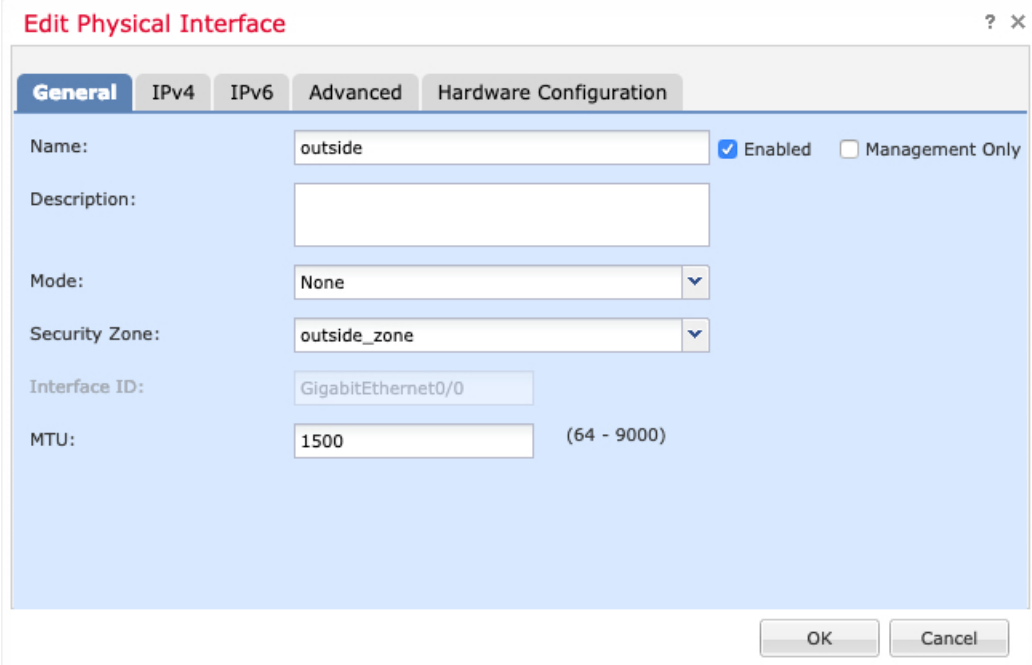


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスの をクリックします。

[全般（General）] タブが表示されます。



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。

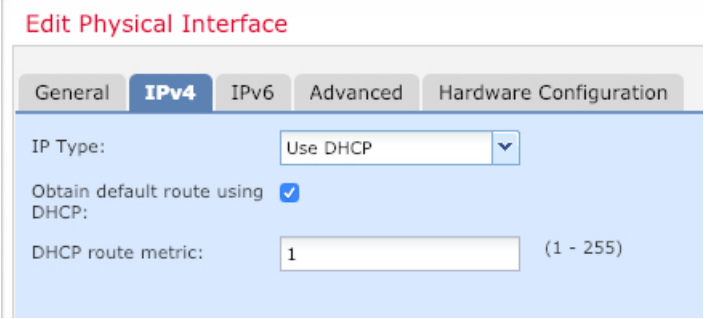
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（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。

e) [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。



- [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。

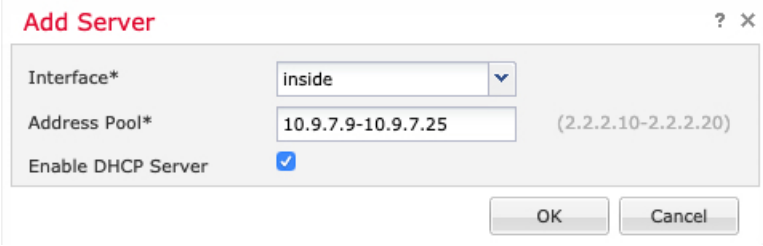
DHCP サーバの設定

クライアントで DHCP を使用して FTDv から IP アドレスを取得するようにする場合は、DHCP サーバを有効にします。

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

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

ステップ 3 **[サーバ（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。

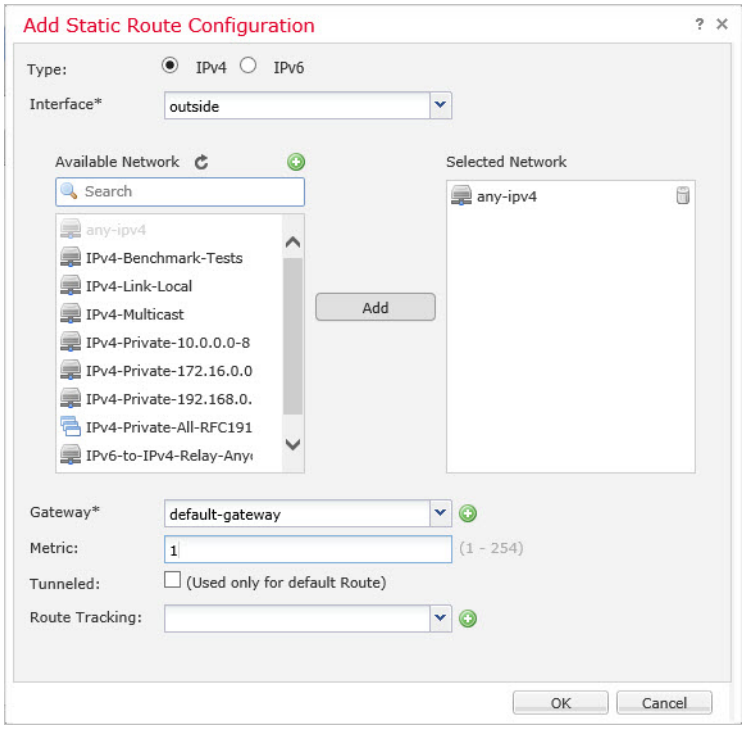
ステップ 5 [保存（Save）] をクリックします。

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、デバイスの 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。

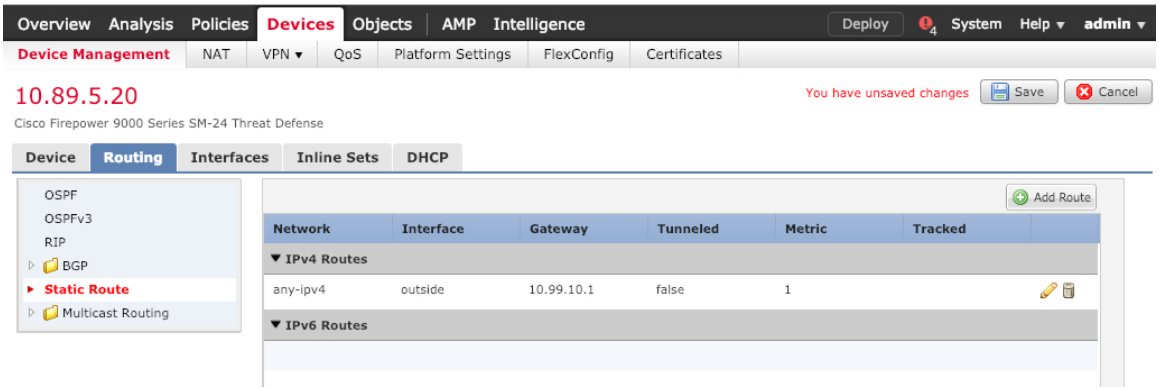


- [タイプ（Type）]：追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス（Interface）]：出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク（Available Network）]：IPv4 デフォルト ルートの場合は [any-ipv4]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。

- [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。

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。



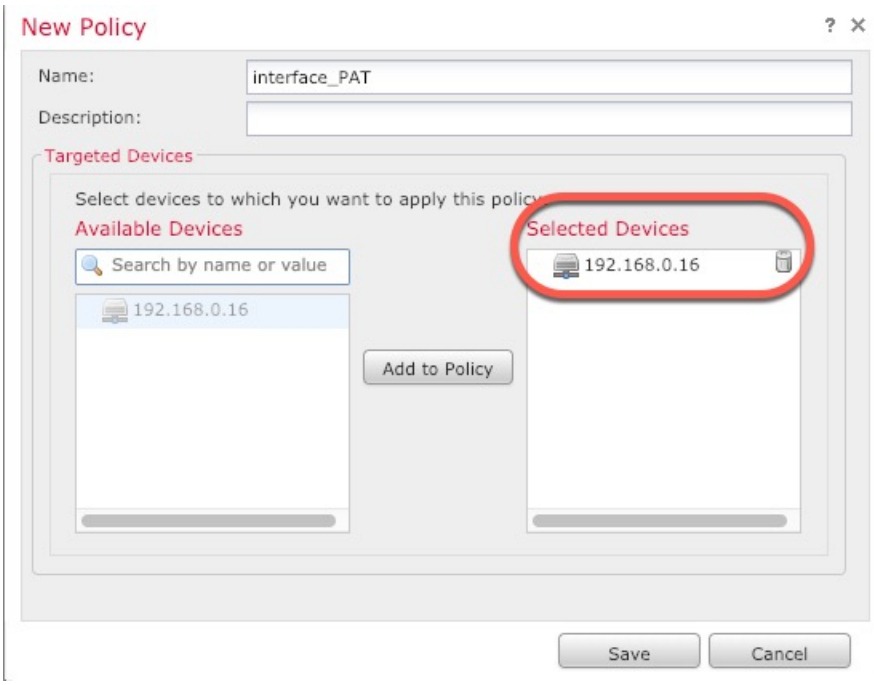
ステップ 4 [保存（Save）] をクリックします。

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。



ポリシーが FMC 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。

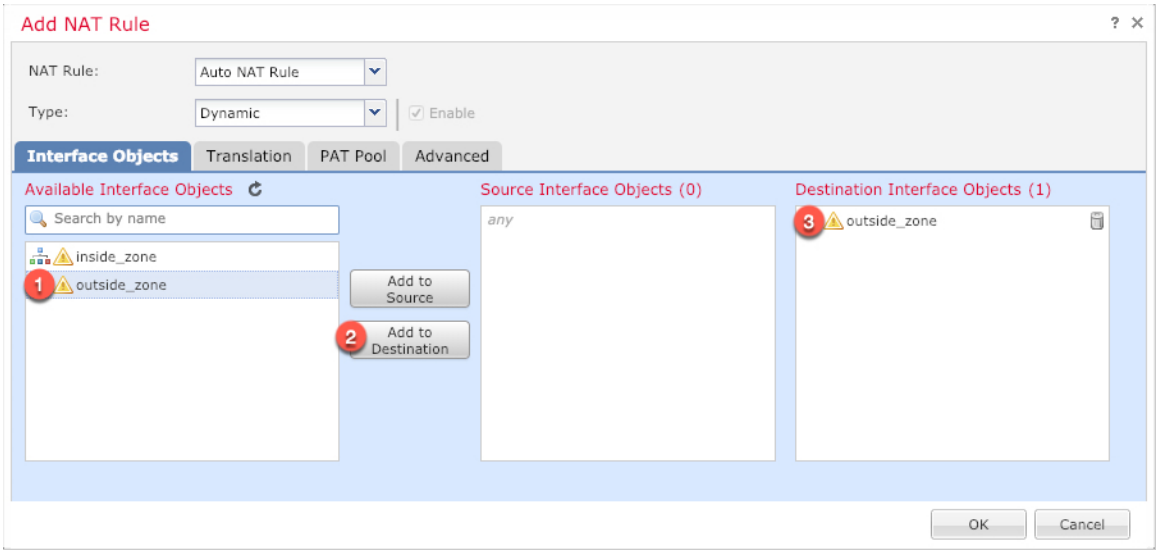
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[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。

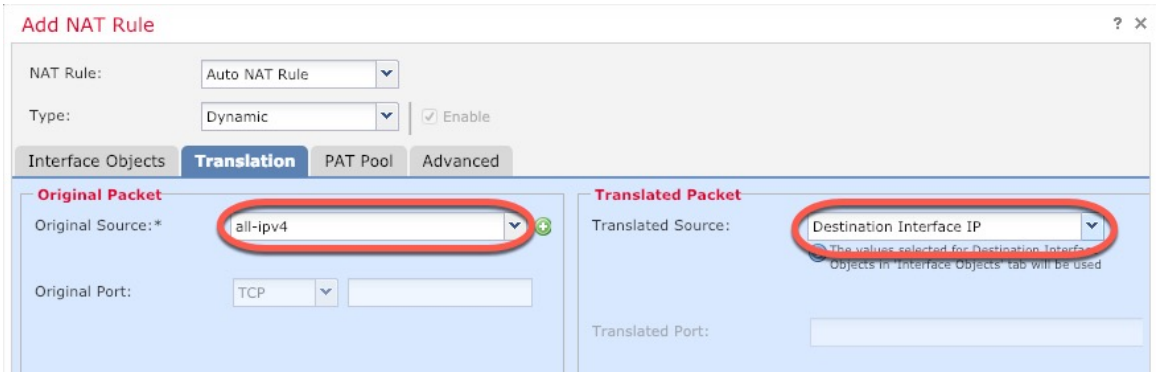
ステップ 4 基本ルールのオプションを設定します。

- [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。

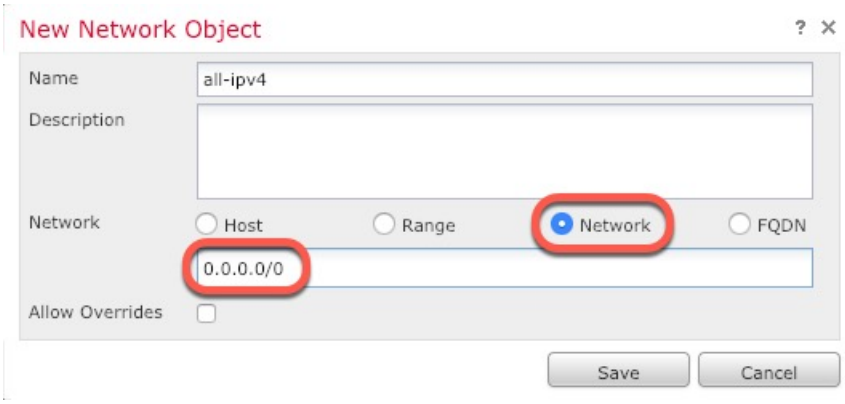
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



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。



- [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。

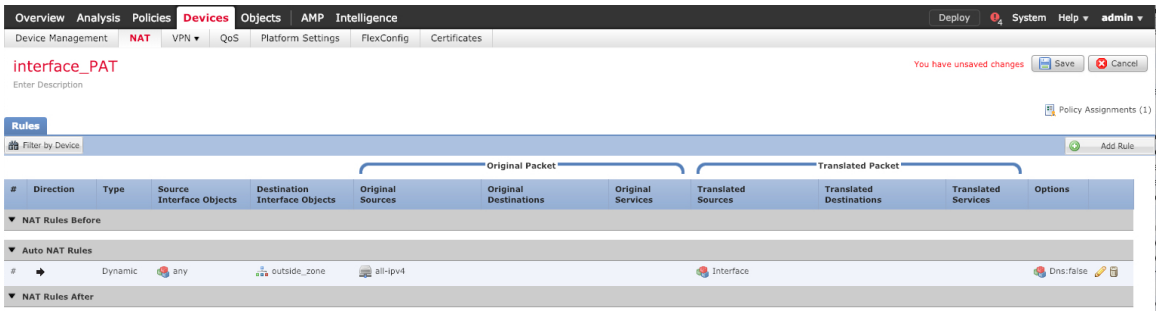


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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。

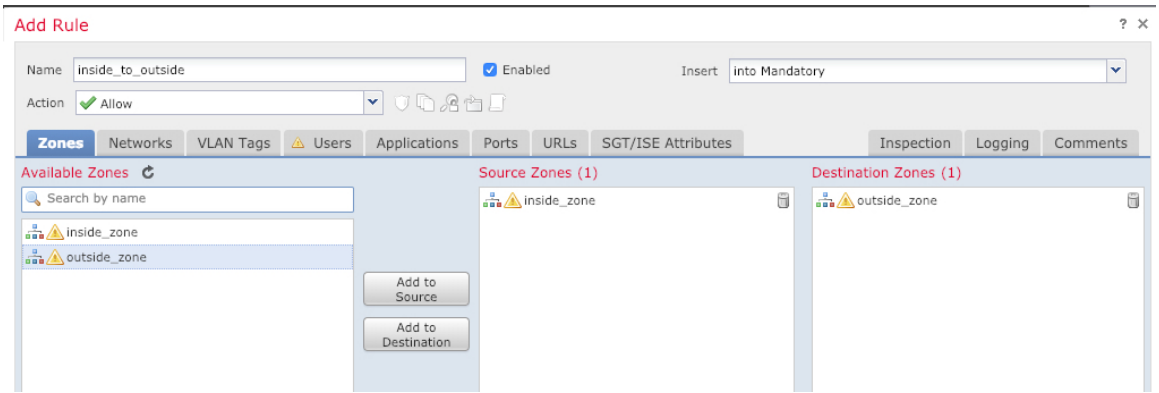
アクセス制御の設定

FTDv を FMC 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。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、FMC の設定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、FTD 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 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。

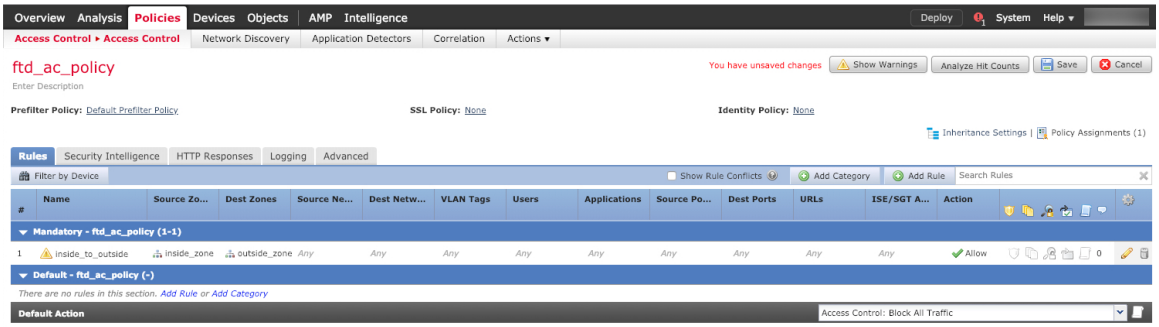


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

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。

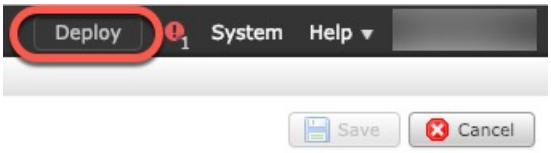


ステップ 4 [保存（Save）] をクリックします。

設定の展開

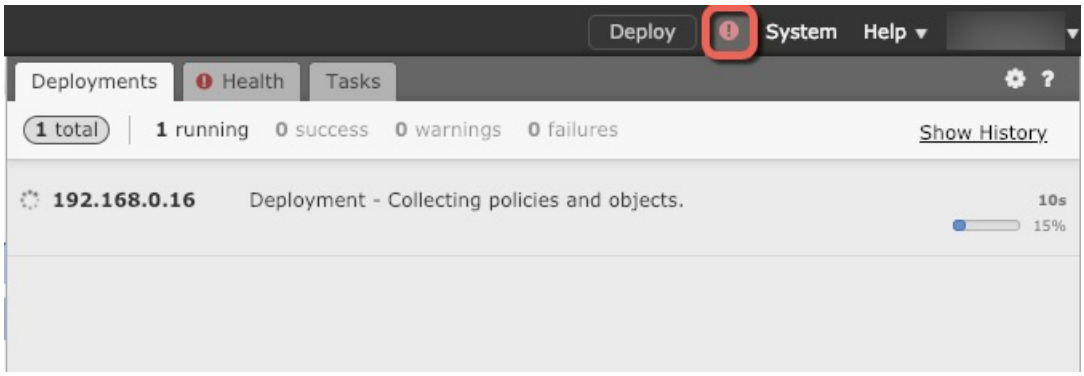
設定の変更を FTDv に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

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。



Firepower Threat Defense CLI へのアクセス

FTDv 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）FTDv 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 FTDv 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。

Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴

機能名	プラットフォームリリース	機能情報
FMC 管理	6.0	初期サポート。

© 2019–2020 Cisco Systems, Inc. All rights reserved.