



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

初版：2016年7月10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 VMware 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、VMware ESXi 環境内における Firepower Threat Defense 仮想の機能について解説し、機能のサポート、システム要件、ガイドライン、制限事項などを説明します。また、この章では FTDv を管理するため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。

- [Firepower Threat Defense Virtual と VMware について \(1 ページ\)](#)
- [VMware の機能における Firepower Threat Defense Virtual のサポート \(2 ページ\)](#)
- [Firepower デバイスの管理方法 \(3 ページ\)](#)
- [システム要件 \(4 ページ\)](#)
- [FTDv と VMware のガイドライン、制限事項、および既知の問題 \(9 ページ\)](#)
- [インターフェイスの計画 \(14 ページ\)](#)

Firepower Threat Defense Virtual と VMware について

シスコでは、VMware vSphere vCenter および ESXi ホスティング環境向けに 64 ビットの Firepower Threat Defense 仮想 (FTDv) デバイスをパッケージ化しています。FTDv は、Cisco.com から入手可能なオープン仮想化フォーマット (OVF) パッケージで配布されます。OVF は、仮想マシン (VM) 向けのソフトウェアアプリケーションをパッケージ化して配布するためのオープンソースの標準規格です。OVF パッケージでは 1 つのディレクトリに複数のファイルが含まれています。

FTDv は、VMware ESXi を実行できる任意の x86 デバイスに展開できます。FTDv を展開するには、vSphere のネットワーキング、ESXi ホストのセットアップと設定、仮想マシンのゲスト展開など、VMware と vSphere についての詳しい知識が必要です。

VMware の機能における Firepower Threat Defense Virtual のサポート

次の表に、Firepower Threat Defense 仮想 の VMware 機能のサポートを示します。

表 1: の VMware 機能のサポート FTDv

機能	説明	サポート (あり/なし)	コメント
コールドクローン	クローニング中に VM の電源がオフになります。	なし	–
VMotion	VM のライブ マイグレーションに使用されます。	あり	共有ストレージを使用します。「FTDv と VMware のガイドライン、制限事項、および既知の問題」を参照してください。
ホット追加	追加時に VM が動作しています。	なし	–
ホットクローン	クローニング中に VM が動作しています。	なし	–
ホットリムーブ	取り外し中に VM が動作していません。	なし	–
スナップショット	VM が数秒間フリーズします。	なし	FMC と管理対象デバイス間で同期されていない状況のリスク。
一時停止と再開	VM が一時停止され、その後再開します。	あり	–
vCloud Director	VM の自動配置が可能になります。	なし	–
VMware FT	VM の HA に使用されます。	なし	Firepower Threat Defense Virtual の VM のフェールオーバーには、Firepower のフェールオーバー機能を使用します。

機能	説明	サポート（あり/なし）	コメント
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	Firepower Threat Defense Virtual の VM のフェールオーバーには、Firepower のフェールオーバー機能を使用します。
VMware vSphere スタンドアロン Windows クライアント	VM を導入するために使用されます。	あり	—
VMware vSphere Web Client	VM を導入するために使用されます。	あり	—

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스에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。

FTDv 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。

VMware vCenter Server と ESXi のインスタンスを実行するシステムは、特定のハードウェアおよびオペレーティングシステム要件を満たす必要があります。サポートされるプラットフォームのリストについては、オンラインの『[VMware Compatibility Guide](#)』を参照してください。

表 2: Firepower Threat Defense Virtual アプライアンスのリソース

設定	値
コアおよびメモリの数	<p>バージョン 6.4 以降</p> <p>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。サポートされている vCPU/メモリのペアの値は、次の 3 つです。</p> <ul style="list-style-type: none"> • 4 vCPU/8 GB (デフォルト) • 8 vCPU/16 GB • 12 vCPU/24 GB <p>(注) 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。上記の 3 つの組み合わせだけがサポートされます。</p>
	<p>バージョン 6.3 以前</p> <p>FTDv は、固定の vCPU およびメモリリソースを使用して展開されます。サポートされている vCPU/メモリのペアの値は次の 1 つだけです。</p> <ul style="list-style-type: none"> • 4 vCPU/8 GB <p>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。</p> <p>(注) vCPU とメモリの調整はサポートされていません。</p>
ストレージ	<p>ディスク形式の選択に基づきます。</p> <ul style="list-style-type: none"> • シンプロビジョニングのディスクサイズは 48.24 GB です。

設定	値
vNIC	<p>FTDv は次の仮想ネットワークアダプタをサポートしています。</p> <ul style="list-style-type: none"> VMXNET3 : VMware 上の FTDv では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。vmxnet3 ドライバは、2つの管理インターフェイスを使用します。最初の2つのイーサネットアダプタは、管理インターフェイスとして設定する必要があります。1つはデバイス管理/登録用で、もう1つは診断用です。 IXGBE : ixgbe ドライバは、2つの管理インターフェイスを使用します。最初の2つの PCI デバイスは、管理インターフェイスとして設定する必要があります。1つはデバイス管理/登録用で、もう1つは診断用です。ixgbe ドライバは、FTDv のフェールオーバー (HA) の展開をサポートしていません。 E1000 : e1000 インターフェイスを使用する場合、e1000 ドライバ用の FTDv 管理インターフェイス (br1) は、2つの MAC アドレス (1つは管理用で、もう1つは診断用) とのブリッジインターフェイスです。 <p>重要 6.4 よりも前のバージョンの Firepower では、VMware 上の FTDv のデフォルトインターフェイスは e1000 でした。リリース 6.4 以降では、VMware 上の FTDv のデフォルトが vmxnet3 インターフェイスになります。仮想デバイスで現在 e1000 インターフェイスを使用している場合は、インターフェイス vmxnet3 を変更することを強く推奨します。詳細については、「VMXNET3 インターフェイスの設定 (18 ページ)」 を参照してください。</p> <ul style="list-style-type: none"> IXGBE-VF : ixgbe-vf (10 ギガビット/秒) ドライバは、SR-IOV をサポートするカーネルでのみアクティブ化できる仮想関数デバイスをサポートしています。SR-IOV には適切なプラットフォームおよび OS のサポートが必要です。詳細については、「SR-IOV のサポート」を参照してください。

仮想化テクノロジーのサポート

- 仮想化テクノロジー (VT) は、動作中の仮想マシンのパフォーマンスを向上させる新しいプロセッサの機能拡張セットです。システムには、ハードウェア仮想化用のインテル

VT または AMD-V の拡張機能をサポートする CPU が必要です。Intel と AMD はどちらも、CPU を識別して機能を確認するために役立つオンラインプロセッサ識別ユーティリティを提供しています。

- VT をサポートする CPU を搭載する多くのサーバでは、VT がデフォルトで無効になっている可能性があります。その場合は、VT を手動で有効にする必要があります。システムで VT のサポートを有効にする手順については、製造元のマニュアルを参照してください。



(注) CPU が VT をサポートしているにもかかわらず BIOS にこのオプションが表示されない場合は、ベンダーに連絡して、VT のサポートを有効にすることができるバージョンの BIOS を要求してください。

ハイパースレッディングの無効化

FTDv を実行するシステムでは、ハイパースレッディングを無効にすることを推奨します。[ハイパースレッディングは非推奨 \(11 ページ\)](#) を参照してください。次のプロセッサはハイパースレッディングをサポートし、コアごとに 2 つのスレッドがあります。

- Intel Xeon 5500 プロセッサのマイクロアーキテクチャに基づくプロセッサ。
- Intel Pentium 4 (HT 対応)
- Intel Pentium EE 840 (HT 対応)

ハイパースレッディングを無効にするには、初めにシステムの BIOS 設定でこれを無効にしてから、vSphere クライアントでオフにします (vSphere ではデフォルトでハイパースレッディングが有効になっています)。CPU がハイパースレッディングをサポートしているかどうかを確認するには、システムのマニュアルを参照してください。

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 X520 - DA2](#)
 - [Intel Ethernet Server Adapter X540](#)
- 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。オンラインの『[VMware Compatibility Guide](#)』で、SR-IOV のサポートを含む推奨システムを検索できます。

SSSE3 のサポート

- Firepower Threat Defense Virtual には、Intel によって作成された単一命令複数データ (SIMD) 命令セットである Supplemental Streaming SIMD Extensions 3 (SSSE3 または SSE3S) のサポートが必要です。
- システムは SSSE3 をサポートする CPU (インテル Core 2 Duo、インテル Core i7/i5/i3、インテル Atom、AMD Bulldozer、AMD Bobcat およびそれ以降のプロセッサなど) を搭載している必要があります。
- SSSE3 命令セットと SSSE3 をサポートする CPU の詳細については、この [リファレンスページ](#) を参照してください。

CPU のサポートの確認

Linux コマンドラインを使用して、CPU ハードウェアに関する情報を取得できます。たとえば、`/proc/cpuinfo` ファイルには個々の CPU コアに関する詳細情報が含まれています。less または cat により、その内容を出力できます。

フラグセクションで次の値を確認できます。

- vmx : インテル VT 拡張機能
- svm : AMD-V 拡張機能
- ssse3 : SSSE3 拡張機能

grep を使用すると、次のコマンドを実行して、ファイルにこれらの値が存在するかどうかを素早く確認することができます。

```
egrep "vmx|svm|ssse3" /proc/cpuinfo
```

システムが VT または SSSE3 をサポートしている場合は、フラグのリストに **vmx**、**svm**、または **ssse3** が表示されます。次の例は、2 つの CPU を搭載しているシステムからの出力を示しています。

```
flags      : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

```
flags      : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

FTDv と VMware のガイドライン、制限事項、および既知の問題

管理モード

- 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 (FDM) オンボード統合マネージャ。



(注) Cisco Firepower ソフトウェアバージョン 6.2.2 以降、VMware 上の FTDv は Firepower Device Manager をサポートしています。バージョン 6.2.2 よりも前の Firepower ソフトウェアを実行している VMware 上の FTDv は、Firepower Management Center を使用してのみ管理できます。「[Firepower デバイスの管理方法 \(3 ページ\)](#)」を参照してください。

- Firepower Management Center (FMC)
- Firepower Device Manager を使用するには、新しいイメージ (バージョン 6.2.2 以降) をインストールする必要があります。既存の FTDv 仮想マシンを古いバージョン (バージョン 6.2.2 よりも前) からアップグレードして Firepower Device Manager に切り替えることはできません。
- Firepower Device Manager (ローカルマネージャ) はデフォルトで有効になっています。



(注) [ローカルマネージャを有効にする (Enable Local Manager)]の[はい (Yes)]を選択すると、ファイアウォールモードが「ルーテッド」に変更されます。Firepower Device Manager を使用する場合は、これが唯一のサポート モードになります。

OVF ファイルのガイドライン

Firepower Threat Defense Virtual アプライアンスをインストールする際は次のインストールオプションを選択できます。

```
Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

ここで、X.X.X-xxx は、使用するファイルのバージョンとビルド番号を表します。

- VIOVFテンプレートをを使用して展開する場合、インストールプロセスで、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。
 - 管理者アカウントの新しいパスワード。
 - 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。
 - Firepower Device Manager を使用するローカル管理 (デフォルト) 、または Firepower Management Center を使用するリモート管理のいずれかの管理。
 - ファイアウォールモード。[ローカルマネージャを有効にする (Enable Local Manager)]の[はい (Yes)]を選択すると、ファイアウォールモードがルーテッドに変更されます。これは Firepower Device Manager を使用する場合のみサポートされるモードです。



(注) VMware vCenter を使用してこの仮想アプライアンスを管理する必要があります。

- ESXi OVF テンプレートをを使用して導入する場合、インストール後に Firepower システムの必須設定を構成する必要があります。この FTDv は ESXi でスタンドアロンのアプライアンスとして管理します。詳細については、「[vSphere ESXi ホストへの Firepower Threat Defense Virtual の展開 \(26 ページ\)](#)」を参照してください。

vMotion のサポート

vMotion を使用する場合、共有ストレージのみを使用することをお勧めします。導入時に、ホストクラスタがある場合は、ストレージをローカルに (特定のホスト上) または共有ホスト上でプロビジョニングできます。ただし、vMotion を使用して Firepower Management Center Virtual を別のホストに移行する場合、ローカルストレージを使用するとエラーが発生します。

ハイパースレッディングは非推奨

ハイパースレッディングテクノロジーにより、単一の物理プロセッサコアを2つの論理プロセッサのように動作させることができます。FTDv を実行するシステムでは、ハイパースレッディングを無効にすることを推奨します。Snort プロセスにより、CPU コアの処理リソースがすでに最大化されています。各 CPU に2つの CPU 使用スレッドをプッシュしても、パフォーマンスの向上は見込まれません。実際には、ハイパースレッディングプロセスに必要となるオーバーヘッドのためにパフォーマンスが低下することがあります。

INIT Respanning エラーメッセージの症状

ESXi 6 および ESXi 6.5 で実行されている FTDv コンソールに次のエラーメッセージが表示される場合があります。

```
"INIT: Id "ftdv" respawning too fast: disabled for 5 minutes"
```

回避策：デバイスの電源がオフになっているときに、vSphere で仮想マシンの設定を編集してシリアルポートを追加します。

1. 仮想マシンを右クリックして、[設定の編集 (Edit Settings)] をクリックします。
2. [仮想ハードウェア (Virtual Hardware)] タブで、[新規デバイス (New device)] ドロップダウンメニューから [シリアルポート (Serial port)] を選択し、[追加 (Add)] をクリックします。

シリアルポートがバーチャルデバイスリストの一番下に表示されます。

3. [仮想ハードウェア (Virtual Hardware)] タブで、[シリアルポート (Serial Port)] を展開し、接続タイプとして [物理シリアルポートを使用 (Use physical serial port)] を選択します。
4. [パワーオン時に接続 (Connect at power on)] チェックボックスをオフにします。
[OK] をクリックして設定を保存します。

ファイアウォール保護からの仮想マシンの除外

vCenter Server が VMware NSX Manager と統合されている vSphere 環境では、分散ファイアウォール (DFW) が、NSX 用に準備されたすべての ESXi ホストクラスタで、VIB パッケージとしてカーネルで実行されます。ホストの準備により、ESXi ホストクラスタで DFW が自動的にアクティブ化されます。

FTDv は無差別モードを使用して動作します。無差別モードを必要とする仮想マシンのパフォーマンスは、これらの仮想マシンが分散ファイアウォールで保護されている場合、悪影響を受ける可能性があります。VMware では、無差別モードを必要とする仮想マシンは分散ファイアウォール保護から除外することを推奨しています。

1. [除外リスト (Exclusion List)] の設定に移動します。
 - NSX 6.4.1 以降で、[ネットワークとセキュリティ (Networking & Security)] > [セキュリティ (Security)] > [ファイアウォール (Firewall)] > [除外リスト (Exclusion List)] に移動します。

- NSX 6.4.0 で、[ネットワークとセキュリティ (Networking & Security)] > [セキュリティ (Security)] > [ファイアウォール (Firewall)] > [除外リスト (Exclusion List)] に移動します。

2. [追加 (Add)] をクリックします。
3. 除外する VM を [選択されたオブジェクト (Selected Objects)] に移動します。
4. [OK] をクリックします。

仮想マシンに複数の vNIC がある場合、それらはすべて保護から除外されます。除外リストに追加されている仮想マシンに vNIC を追加すると、新しく追加された vNIC にファイアウォールが自動的に展開されます。新しい vNIC をファイアウォール保護から除外するには、仮想マシンを除外リストから削除してから、除外リストに再度追加する必要があります。別の回避策として、仮想マシンの電源を再投入（電源をオフにしてからオン）する方法がありますが、最初のオプションの方が中断が少なく済みます。

vSphere 標準スイッチのセキュリティポリシー設定の変更

vSphere 標準スイッチの場合、レイヤ2セキュリティポリシーには、無差別モード、MAC アドレスの変更、不正送信という 3 つの要素があります。Firepower Threat Defense Virtual は無差別モードを使用して稼働します。また、Firepower Threat Defense Virtual の高可用性は、正常に稼働するために MAC アドレスをアクティブとスタンバイの間で切り替えるかどうか依存します。

デフォルトの設定では、Firepower Threat Defense Virtual の正常な動作が妨げられます。以下の必須の設定を参照してください。

表 3: vSphere 標準スイッチのセキュリティポリシーオプション

オプション	必須の設定	アクション
無差別モード (Promiscuous Mode)	承認 (Accept)	vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを編集し、[無差別モード (Promiscuous mode)] オプションを [承認 (Accept)] に設定する必要があります。 ファイアウォール、ポートスキャナ、侵入検知システムなどは無差別モードで実行する必要があります。

オプション	必須の設定	アクション
MAC アドレスの変更 (MAC Address Changes)	承認 (Accept)	vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[MAC アドレスの変更 (MAC address changes)] オプションが [承認 (Accept)] に設定されていることを確認する必要があります。
不正送信 (Forged Transmits)	承認 (Accept)	vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[不正転送 (Forged transmits)] オプションが [承認 (Accept)] に設定されていることを確認する必要があります。

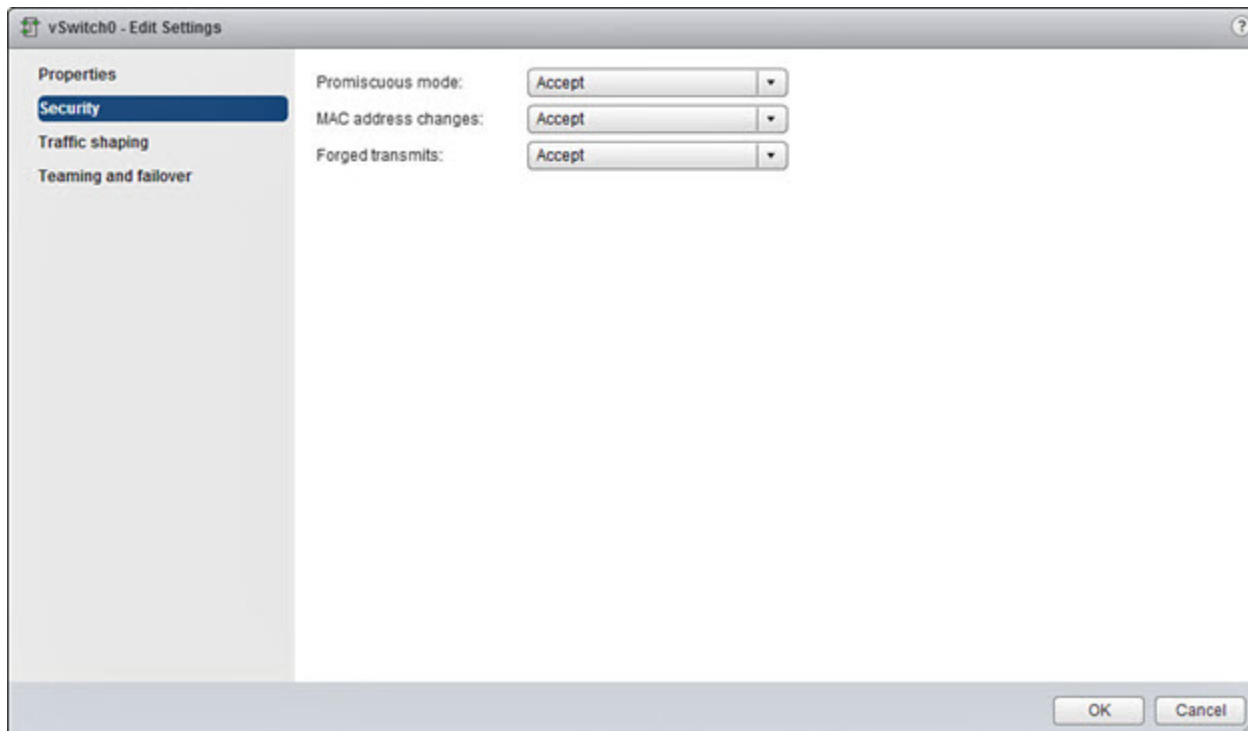
vSphere 標準スイッチのセキュリティポリシー設定の変更

デフォルトの設定は、FTDv の適切な動作をブロックします。

手順

- ステップ 1 vSphere Web Client で、ホストに移動します。
- ステップ 2 [管理 (Manage)] タブで、[ネットワーク (Networking)] をクリックし、[仮想スイッチ (Virtual switches)] を選択します。
- ステップ 3 リストから標準スイッチを選択し、[設定の編集 (Edit settings)] をクリックします。
- ステップ 4 [セキュリティ (Security)] を選択し、現在の設定を表示します。
- ステップ 5 標準スイッチに接続された仮想マシンのゲスト オペレーティング システムで無差別モードの有効化、MAC アドレスの変更、および不正送信の [承認 (Accept)] を選択します。

図 1: vSwitch の編集設定



ステップ 6 [OK] をクリックします。

次のタスク

- これらの設定が、FTDv デバイスの管理インターフェイスおよびフェールオーバー (HA) インターフェイスに設定されているすべてのネットワーク上で同じであることを確認します。

インターフェイスの計画

展開の前に、Firepower Threat Defense 仮想の vNIC とインターフェイスのマッピングを計画することで、リブートと設定の問題を回避できます。FTDv は 10 個のインターフェイスで展開され、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。

FTDv は、vmxnet3 (デフォルト)、ixgbe、および e1000 の仮想ネットワークアダプタをサポートしています。また、適切に設定されたシステムでは、FTDv は SR-IOV 用の ixgbe-vf ドライバもサポートしています。詳細については、「[システム要件 \(4 ページ\)](#)」を参照してください。



重要 FTDv VMware では、仮想デバイスを作成するときに、デフォルトが `vmxnet3` インターフェイスになりました。以前は、デフォルトは `e1000` でした。`e1000` インターフェイスを使用している場合は、切り替えることを強く推奨します。`Vmxnet3` のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

インターフェイスに関するガイドラインと制限事項

ここでは、VMware 上の FTDv で使用されるサポート対象の仮想ネットワークアダプタに関するガイドラインと制約事項について説明します。展開を計画する際は、これらのガイドラインに留意しておくことが重要です。

一般的なガイドライン

- 前述のように、FTDv は 10 個のインターフェイスで展開され、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。少なくとも 4 つのインターフェイスにネットワークを割り当てる必要があります。
- 10 個の FTDv インターフェイスをすべて使用する必要はありません。使用しないインターフェイスの場合は、FTDv の設定内でそのインターフェイスを無効のままにしておいて構いません。
- 展開後に仮想マシンに仮想インターフェイスを追加することはできないので注意してください。一部のインターフェイスを削除してから、さらにインターフェイスが必要になった場合は、仮想マシンを削除してからやり直す必要があります。

デフォルトの VMXNET3 インターフェイス



重要 FTDv VMware では、仮想デバイスを作成するときに、デフォルトが `vmxnet3` インターフェイスになりました。以前は、デフォルトは `e1000` でした。`e1000` インターフェイスを使用している場合は、切り替えることを強く推奨します。`Vmxnet3` のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

- `vmxnet3` ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つのイーサネットアダプタは、管理インターフェイスとして設定する必要があります。1 つはデバイス管理/登録用で、もう 1 つは診断用です。
- `vmxnet3` では、4 つを超える `vmxnet3` ネットワークインターフェイスを使用する場合、VMware vCenter によって管理されるホストを使用することを推奨します。スタンドアロンの ESXi に展開する場合、連続する PCI バスアドレスを持つ仮想マシンに対してさらに多くのネットワークインターフェイスは追加されません。ホストを VMware vCenter で管理

する場合は、設定 CD-ROM の XML から正しい順序を取得できます。ホストでスタンドアロンの ESXi を実行している場合、ネットワークインターフェイスの順序を判断する唯一の方法は、FTDv に表示される MAC アドレスと、VMware 構成ツールから表示される MAC アドレスとを手動で比較することです。

次の表に、vmxnet3 および ixgbe インターフェイスの FTDv 用のネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を示します。

表 4: 送信元から宛先ネットワークへのマッピング : vmxnet3 と ixgbe

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
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部日付
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データトラフィック (オプション)
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データトラフィック (オプション)
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データトラフィック (オプション)
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データトラフィック (オプション)
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データトラフィック (オプション)
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データトラフィック (オプション)

IXGBE インターフェイス

- ixgbe ドライバは、2つの管理インターフェイスを使用します。最初の2つの PCI デバイスは、管理インターフェイスとして設定する必要があります。1つはデバイス管理/登録用で、もう1つは診断用です。
- ixgbe の場合は、ESXi プラットフォームで ixgbe PCI デバイスをサポートするために ixgbe NIC が必要です。また、ESXi プラットフォームには、ixgbe PCI デバイスをサポートする

ために必要な固有の BIOS 要件と設定要件があります。詳細については、[Intel の技術概要](#)を参照してください。

- サポートされる唯一の ixgbe トラフィックインターフェイスのタイプは、ルーテッドと ERSPAN パッシブです。これは、MAC アドレスフィルタリングに関する VMware の制限によるものです。
- ixgbe ドライバは、Firepower Threat Defense Virtual のフェールオーバー（HA）展開をサポートしていません。

e1000 インターフェイス



重要

FTDv VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

- e1000 ドライバ用の管理インターフェイス（br1）は、2 つの MAC アドレス（1 つは管理用で、もう 1 つは診断用）とのブリッジインターフェイスです。
- e1000 インターフェイスを使用していて、FTDv を 6.4 にアップグレードする場合は、ネットワークスループットを向上させるために、e1000 インターフェイスを vmxnet3 または ixgbe インターフェイスのいずれかに置き換えてください。

次の表に、デフォルトの e1000 インターフェイスにおける FTDv 用のネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を示します。

表 5: 送信元から宛先ネットワークへのマッピング：e1000 インターフェイス

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
Network adapter 1	Management0-0	Diagnostic0/0	管理と診断
Network adapter 2	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 3	GigabitEthernet0-1	GigabitEthernet 0/1	内部日付
ネットワークアダプタ 4	GigabitEthernet0-2	GigabitEthernet 0/2	データトラフィック (必須)
ネットワークアダプタ 5	GigabitEthernet0-3	GigabitEthernet 0/3	データトラフィック (オプション)
ネットワークアダプタ 6	GigabitEthernet0-4	GigabitEthernet 0/4	データトラフィック (オプション)

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
ネットワークアダプタ 7	GigabitEthernet0-5	GigabitEthernet 0/5	データトラフィック (オプション)
ネットワークアダプタ 8	GigabitEthernet0-6	GigabitEthernet 0/6	データトラフィック (オプション)
ネットワークアダプタ 9	GigabitEthernet0-7	GigabitEthernet 0/7	データトラフィック (オプション)
ネットワークアダプタ 10	GigabitEthernet0-8	GigabitEthernet 0/8	データトラフィック (オプション)

VMXNET3 インターフェイスの設定



重要 6.4のリリース以降、VMware上のFTDvでは、仮想デバイスを作成するときに、デフォルトがvmxnet3インターフェイスになりました。以前は、デフォルトはe1000でした。e1000インターフェイスを使用している場合は、切り替えることを強く推奨します。Vmxnet3のデバイスドライバとネットワーク処理はESXiハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

e1000インターフェイスをvmxnet3に変更するには、「すべての」インターフェイスを削除し、vmxnet3ドライバを使用してそれらを再インストールする必要があります。

展開内でインターフェイスを混在させる（仮想 Firepower Management Center で e1000 インターフェイス、およびその管理対象仮想デバイスで vmxnet3 インターフェイスを混在させるなど）ことはできますが、同じ仮想アプライアンス上でインターフェイスを混在させることはできません。仮想アプライアンス上のすべてのセンサーインターフェイスと管理インターフェイスは同じタイプである必要があります。

手順

ステップ 1 FTDv 仮想マシンの電源をオフにします。

インターフェイスを変更するには、アプライアンスの電源をオフにする必要があります。

ステップ 2 インベントリ内のFTDv仮想マシンを右クリックして、[設定の編集 (Edit Settings)] をクリックします。

ステップ 3 該当するネットワークアダプタを選択し、[削除 (Remove)] を選択します。

ステップ 4 [追加 (Add)] をクリックして、[ハードウェアの追加ウィザード (Add Hardware Wizard)] を開きます。

ステップ 5 [イーサネットアダプタ (Ethernet Adapter)] を選択し、[次へ (Next)] をクリックします。

ステップ 6 vmxnet3 アダプタを選択し、ネットワークラベルを選択します。

ステップ 7 FTDv のすべてのインターフェイスについて手順を繰り返します。

次のタスク

- VMware コンソールから FTDv の電源をオンにします。

インターフェイスの追加

FTDv デバイスを展開する場合、合計 10 のインターフェイス（管理 1、診断 1、データ 8 のインターフェイス）を設けることができます。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。



注意

仮想マシンにさらに仮想インターフェイスを追加して、FTDv にそれらを自動的に認識させることはできません。仮想マシンにインターフェイスを追加する場合は、完全に FTDv 設定を消去する必要があります。設定でそのまま残しておく唯一の部分は、管理アドレスとゲートウェイ設定です。

FTDv デバイス向けに追加の物理インターフェイスが必要な場合は、基本的にもう一度やり直す必要があります。新しい仮想マシンを展開するか、または『[Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#)』の「Add Interfaces to Firepower Threat Defense Virtual」の手順を使用できます。



第 2 章

Firepower Threat Defense Virtual の展開

この章では、Firepower Threat Defense 仮想を VMware vSphere 環境（vSphere vCenter またはスタンドアロンの ESXi ホストのどちらか）に展開する手順について説明します。

- [VMware の展開について](#)（21 ページ）
- [vSphere vCenter への Firepower Threat Defense Virtual の展開](#)（22 ページ）
- [vSphere ESXi ホストへの Firepower Threat Defense Virtual の展開](#)（26 ページ）
- [CLI を使用した Firepower Threat Defense Virtual のセットアップの実行](#)（31 ページ）

VMware の展開について

Firepower Threat Defense 仮想（FTDv）は、スタンドアロンの ESXi サーバに展開でき、vCenter vSphere を使用している場合は、vSphere Client または vSphere Web Client を使用して展開できます。FTDv を正常に展開するには、vSphere のネットワーキング、ESXi ホストのセットアップと設定、仮想マシンのゲスト展開など、VMware と vSphere についての詳しい知識が必要です。

FTDv VMware 用の FTDv はオープン仮想化フォーマット（OVF）を使用して配布されます。OVF は、仮想マシンをパッケージ化して展開する標準的な方法です。VMware では、vSphere 仮想マシンをプロビジョニングするための方法がいくつか用意されています。お使いの環境に最適な方法は、インフラストラクチャの規模やタイプ、達成目標などの要因によって異なります。

VMware vSphere Web Client と vSphere Client は、vCenter Server、ESXi ホスト、および仮想マシンへのインターフェイスです。vSphere Web Client と vSphere Client を使用して、vCenter Server にリモート接続できます。vSphere Client では、任意の Windows システムから ESXi に直接接続することもできます。vSphere Web Client と vSphere Client は、vSphere 環境のすべての側面を管理するための主要なインターフェイスです。これらはコンソールによる仮想マシンへのアクセスも提供します。

vSphere Web Client では、すべての管理機能を使用できます。vSphere Client では、これらの機能の一部を使用できます。

vSphere vCenter への Firepower Threat Defense Virtual の展開

この手順を使用して、Firepower Threat Defense 仮想 (FTDv) アプライアンスを VMware vSphere vCenter に展開します。vSphere Web Client (または vSphere Client) を使用して、FTDv 仮想マシンを展開し、設定できます。

始める前に

- FTDv を導入する前に、vSphere (管理用) で少なくとも 1 つのネットワークを設定しておく必要があります。

手順

-
- ステップ 1** vSphere Web Client (または vSphere Client) にログインします。
- ステップ 2** vSphere Web Client (または vSphere Client) を使用し、[ファイル (File)] > [OVF テンプレートの展開 (Deploy OVF Template)] をクリックして、以前にダウンロードした OVF テンプレート ファイルを展開します。
- [OVF テンプレートの導入 (Deploy OVF Template)] ウィザードが表示されます。
- ステップ 3** ファイルシステムで OVF テンプレートソースの場所を参照し、[次へ (Next)] をクリックします。
- 次の Firepower Threat Defense Virtual VI OVF テンプレートを選択します。
- Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*
- ここで、X.X.X-xxx は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。
- ステップ 4** [OVF テンプレートの詳細 (OVF Template Details)] ページを確認し、OVF テンプレートの情報 (製品名、バージョン、ベンダー、ダウンロードサイズ、ディスク上のサイズ、説明) を確認して、[次へ (Next)] をクリックします。
- ステップ 5** [エンドユーザライセンス契約書 (End User License Agreement)] ページが表示されます。OVF テンプレート (VI テンプレートのみ) でパッケージ化されたライセンス契約書を確認し、[承認 (Accept)] をクリックしてライセンスの条件に同意し、[次へ (Next)] をクリックします。
- ステップ 6** [名前と場所 (Name and Location)] ページで、この展開の名前を入力し、FTDv を展開するインベントリ内の場所 (ホストまたはクラスター) を選択して、[次へ (Next)] をクリックします。名前はインベントリフォルダ内で一意である必要があります。最大 80 文字を使用できます。
- VSphere Web Client では、インベントリビューに管理対象オブジェクトの組織階層が表示されます。インベントリは、vCenter Server またはホストが管理対象オブジェクトを整理する目的で使用される階層構造です。この階層には、vCenter Server にあるすべての監視対象オブジェクトが含まれています。

- ステップ 7** Firepower Threat Defense Virtual を実行するリソースプールに移動して選択し、[次へ (Next)] をクリックします。
- (注) このページは、クラスタにリソースプールが含まれている場合にのみ表示されます。
- ステップ 8** [導入設定 (Deployment Configuration)] を選択します。[設定 (Configuration)] ドロップダウンリストから、サポートされている 3 つの vCPU/メモリ値のいずれかを選択し、[次へ (Next)] をクリックします。
- 重要** 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。6.4 より前のバージョンでは、FTDv は、固定構成の 4 vCPU/8 GB デバイスとして展開されていました。「[システム要件 \(4 ページ\)](#)」を参照してください。
- ステップ 9** 仮想マシンファイルを保存する [保存 (Storage)] 場所を選択し、[次へ (Next)] をクリックします。
- このページで、宛先クラスタまたはホストですでに設定されているデータストアから選択します。仮想マシン コンフィギュレーション ファイルおよび仮想ディスク ファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスクファイルを保存できる十分なサイズのデータストアを選択してください。
- ステップ 10** 仮想マシンの仮想ディスクを保存するための「ディスク形式」を選択し、[次へ (Next)] をクリックします。
- [シックプロビジョン (Thick Provisioned)] を選択すると、すべてのストレージは、ただちに割り当てられます。[シンプロビジョン (Thin Provisioned)] を選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。
- ステップ 11** [ネットワークマッピング (Network Mapping)] ページで、OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ (Next)] をクリックします。
- Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Firepower Management Center または Firepower Device Manager から設定できます。
- 重要** FTDv VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。
- ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集 (Edit Settings)] ダイアログボックスからネットワークを変更できます。展開後、FTDv インスタンスを右クリックして [設定の編集 (Edit Settings)] を選択します。ただし、この画面には FTDv の ID は表示されません (ネットワークアダプタ ID のみ)。

以下に示す、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、宛先ネットワークの対応を参照してください（これらは vmxnet3 デフォルトのインターフェイスです）。

表 6: 送信元から宛先ネットワークへのマッピング : *vmxnet3*

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
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部日付
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データトラフィック (オプション)
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データトラフィック (オプション)
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データトラフィック (オプション)
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データトラフィック (オプション)
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データトラフィック (オプション)
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データトラフィック (オプション)

FTDv を展開する際には、合計 10 個のインターフェイスを指定できます。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。すべての FTDv インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、FTDv 設定内でそのインターフェイスを無効のままにしておいて構いません。

ステップ 12 [プロパティ (Properties)] ページで、OVF テンプレート (VI テンプレートのみ) でパッケージ化された、ユーザ設定可能なプロパティを設定します。

a) パスワード

FTDv 管理アクセス用のパスワードを設定します。

b) ネットワーク

完全修飾ドメイン名 (FQDN)、DNS、検索ドメイン、ネットワークプロトコル (IPv4 または IPv6) などのネットワーク情報を設定します。

c) 管理

管理モードを設定します。[ローカルマネージャを有効にする (Enable Local Manager)] のドロップダウン矢印をクリックし、Web ベースの Firepower Device Manager 統合設定ツールを使用する場合は [はい (Yes)] を選択します。Firepower Management Center を使用してこのデバイスを管理する場合は、[いいえ (No)] を選択します。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 \(3 ページ\)](#)」を参照してください。

d) ファイアウォールモード

初期ファイアウォールモードを設定します。[ファイアウォールモード (Firewall Mode)] のドロップダウン矢印をクリックし、サポートされている 2 つのモードである [ルーテッド (Routed)] または [トランスペアレント (Transparent)] のどちらかを選択します。

[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、[ルーテッド (Routed)] ファイアウォールモードのみを選択できます。ローカルの Firepower Device Manager 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を設定することはできません。

e) 登録

[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、管理を行う Firepower Management Center にこのデバイスを登録するのに必要なクレデンシャルを指定する必要があります。次の情報を入力します。

- [管理を行う Defense Center (Managing Defense Center)] : FMC のホスト名または IP アドレスを入力します。
- [登録キー (Registration Key)] : 登録キーは、ユーザが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。デバイスを FMC に追加するときに、この登録キーを思い出す必要があります。
- [NAT ID] : FTDv と FMC がネットワーク アドレス変換 (NAT) デバイスによって分離されていて、Firepower Management Center が NAT デバイスの背後にある場合は、一意の NAT ID を入力します。これは、ユーザが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。

f) [次へ (Next)] をクリックします。

ステップ 13 [準備完了 (Ready To Complete)] セクションで、表示された情報を確認します。これらの設定を使用して展開を開始するには、[終了 (Finish)] をクリックします。変更を加えるには、[戻る (Back)] をクリックして前の各画面に戻ります。

オプションで、[展開後に電源をオン (Power on after deployment)] オプションにチェックマークを付けて、FTDv の電源をオンにし、[終了 (Finish)] をクリックします。

ウィザードが完了すると、vSphere Web Client によって仮想マシンが処理されます。[グローバル情報 (Global Information)] 領域の [最近使用したタスク (Recent Tasks)] ペインで [OVF 展開の初期設定 (Initialize OVF deployment)] ステータスを確認できます。

この手順が終了すると、[OVF テンプレートの展開 (Deploy OVF Template)] 完了ステータスが表示されます。

FTDv 仮想インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。新しい VM の起動には、最大 30 分かかることがあります。

(注) Cisco Licensing Authority に FTDv を正常に登録するには、FTDv にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

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 \(33 ページ\)](#)」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 \(51 ページ\)](#)」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 \(3 ページ\)](#)」を参照してください。

vSphere ESXi ホストへの Firepower Threat Defense Virtual の展開

この手順を使用して、Firepower Threat Defense 仮想 (FTDv) アプライアンスを単一の ESXi ホストに展開します。VMware Host Client (または vSphere Client) を使用して、単一の ESXi ホストを管理でき、FTDv 仮想マシンの展開や設定といった仮想化の基本的な操作などの管理タスクを実行できます。



- (注) VMware Host Client は vSphere Web Client とユーザインターフェイスが似ていますが、まったく異なるものであることに注意してください。vSphere Web Client は、vCenter Server に接続して複数の ESXi ホストを管理する場合に使用します。一方、VMware Host Client は単一の ESXi ホストを管理する場合に使用します。

vCenter 環境に Firepower Threat Defense 仮想 アプライアンスを展開する方法については、「[vSphere vCenter への Firepower Threat Defense Virtual の展開 \(22 ページ\)](#)」参照してください。

始める前に

- FTDv を展開する前に、vSphere (管理用) で少なくとも 1 つのネットワークを設定しておく必要があります。

手順

- ステップ 1** Cisco.com から VMware ESXi 用の Firepower Threat Defense 仮想 インストールパッケージをダウンロードして、ローカル管理コンピュータに保存します。

<https://www.cisco.com/go/ftd-software>

Cisco.com のログインおよびシスコサービス契約が必要です。

- ステップ 2** tar ファイルを作業ディレクトリに解凍します。ディレクトリからファイルを削除しないでください。次のファイルが含まれています。

- Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xx.ovf : vCenter 展開用
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf : ESXi 展開用
- Cisco_Firepower_Threat_Defense_Virtual-X.X.X-xx.vmdk : VMware 仮想ディスク ファイル
- Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xx.mf : vCenter 展開用マニフェストファイル
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.mf : ESXi 展開用マニフェストファイル

ここで、X.X.X-xx は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。

- ステップ 3** ブラウザで、[http:// \(ホスト名\) /ui](http://(ホスト名)/ui) または [http:// \(ホスト IP アドレス\) /ui](http://(ホスト IP アドレス)/ui) という形式を使用して、ESXi ターゲットのホスト名または IP アドレスを入力します。

ログイン画面が表示されます。

- ステップ 4** 管理者のユーザ名とパスワードを入力します。

- ステップ 5** [ログイン (Login)] をクリックして続行します。
これで、ターゲットの ESXi ホストにログインしました。
- ステップ 6** VMware Host Client のインベントリで、[ホスト (Host)] を右クリックし、[VMの作成/登録 (Create/Register VM)] を選択します。
[新規仮想マシンウィザード (New Virtual Machine Wizard)] が開きます。
- ステップ 7** [作成タイプの選択 (Select creation type)] ページで、[OVFまたはOVAファイルから仮想マシンを導入 (Deploy a virtual machine from an OVF or OVA file)] を選択し、[次へ (Next)] をクリックします。
- ステップ 8** ウィザードの [OVFおよびVMDKファイルの選択 (Select OVF and VMDK files)] ページで次の操作を行います。
- FTDv 仮想マシンの名前を入力します。
仮想マシン名には 80 文字まで含めることができます。マシン名は各 ESXi インスタンスの中で一意にする必要があります。
 - 青いペインをクリックし、FTDv tar ファイルを解凍したディレクトリを参照して、ESXi OVF テンプレートと付随する VMDK ファイルを選択します。
`Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf`
`Cisco_Firepower_Threat_Defense_Virtual-X.X.X-xx.vmdk`
ここで、X.X.X-xx は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。
注目 必ず ESXi OVF を選択してください。
- ステップ 9** [次へ (Next)] をクリックします。
使用しているローカルシステムストレージが開きます。
- ステップ 10** ウィザードの [ストレージの選択 (Select storage)] ページで、アクセス可能なデータストアのリストからデータストアを選択します。
仮想マシンの設定ファイルとすべての仮想ディスクが、このデータストアに保存されます。データストアはそれぞれ、サイズ、速度、可用性などのプロパティが異なる場合があります。
- ステップ 11** [次へ (Next)] をクリックします。
- ステップ 12** FTDv の ESXi OVF と一緒にパッケージ化されている [展開オプション (Deployment options)] を設定します。
- [ネットワークマッピング (Network Mapping)] : OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ (Next)] をクリックします。
Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Firepower Management Center または Firepower Device Manager から設定できます。

重要 FTDv VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集 (Edit Settings)] ダイアログボックスからネットワークを変更できます。展開後、FTDv インスタンスを右クリックして [設定の編集 (Edit Settings)] を選択します。ただし、この画面には FTDv の ID は表示されません (ネットワークアダプタ ID のみ)。

以下に示す、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、宛先ネットワークの対応を参照してください (これらは vmxnet3 デフォルトのインターフェイスです)。

表 7: 送信元から宛先ネットワークへのマッピング : *vmxnet3*

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
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部日付
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データトラフィック (オプション)
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データトラフィック (オプション)
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データトラフィック (オプション)
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データトラフィック (オプション)
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データトラフィック (オプション)
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データトラフィック (オプション)

FTDv を展開する際には、合計 10 個のインターフェイスを指定できます。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的なサブネットまたは VLAN にマッピングされていることを確認します。すべての FTDv インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、FTDv 設定内でそのインターフェイスを無効のままにしておいて構いません。

- b) [ディスクプロビジョニング (Disk provisioning)] : 仮想マシンの仮想ディスクを保存するためのディスク形式を選択します。

[シック (Thick)] プロビジョニングを選択すると、すべてのストレージがただちに割り当てられます。[シン (Thin)] プロビジョニングを選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。

ステップ 13 新規仮想マシンウィザードの [準備完了 (Ready To Complete)] ページで、仮想マシンの設定を確認します。

- (任意) ウィザードの設定を確認または変更するには、[戻る (back)] をクリックして戻ります。
- (任意) 作成タスクを破棄してウィザードを閉じるには、[キャンセル (Cancel)] をクリックします。
- [終了 (Finish)] をクリックして作成タスクを完了し、ウィザードを終了します。

ウィザードが完了すると、ESXi ホストによって VM が処理されます。展開のステータスは [最近使用したタスク (Recent Tasks)] で確認できます。展開が成功すると、[結果 (Results)] 列に [正常に完了 (Completed successfully)] が表示されます。

新しい FTDv 仮想マシンインスタンスが、ESXi ホストの仮想マシンインベントリの下に表示されます。新しい仮想マシンの起動には、最大 30 分かかることがあります。

(注) Cisco Licensing Authority に FTDv を正常に登録するには、FTDv にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

次のタスク

- CLI を使用して仮想デバイスのセットアップを完了します。これは、ESXi OVF テンプレートを使用して FTDv を展開する場合の次の手順になります。「[CLI を使用した Firepower Threat Defense Virtual のセットアップの実行 \(31 ページ\)](#)」を参照してください。

CLI を使用した Firepower Threat Defense Virtual のセットアップの実行

ESXi OVF テンプレートをを使用して展開した場合は、CLI を使用して FTDv をセットアップする必要があります。Firepower Threat Defense 仮想 アプライアンスには Web インターフェイスがありません。また、VIOVF テンプレートをを使用して展開し、かつ展開時にセットアップウィザードを使用しなかった場合は、CLI を使用して、Firepower システムに必要な設定を行うことができます。



- (注) VIOVF テンプレートをを使用して展開し、かつセットアップウィザードを使用した場合は、仮想デバイスが設定済みであり、それ以上のデバイス設定は必要ありません。以降の手順は、選択する管理モードによって異なります。

新しく設定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。

手順

- ステップ 1 VMware 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を求められます。
 - 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 Firepower Device Manager を使用）

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。

設定が実装されたときに、VMware コンソールにメッセージが表示される場合があります。

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。

(注) Cisco Licensing Authority に FTDv を正常に登録するには、FTDv にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

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 \(33 ページ\)](#)」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 \(51 ページ\)](#)」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 \(3 ページ\)](#)」を参照してください。



第 3 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 \(50 ページ\)](#)」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 \(33 ページ\)](#)
- [Firepower Management Center へのログイン \(34 ページ\)](#)
- [Firepower Management Center へのデバイスの登録 \(34 ページ\)](#)
- [基本的なセキュリティポリシーの設定 \(37 ページ\)](#)
- [Firepower Threat Defense CLI へのアクセス \(49 ページ\)](#)
- [Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴 \(50 ページ\)](#)

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。

手順

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。

手順

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

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

- [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 \(47 ページ\)](#)」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 \(49 ページ\)](#)」) 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。

手順

- ステップ 1 [インターフェイスの設定 \(37 ページ\)](#)
- ステップ 2 [DHCP サーバの設定 \(41 ページ\)](#)
- ステップ 3 [デフォルトルートの追加 \(42 ページ\)](#)
- ステップ 4 [NAT の設定 \(44 ページ\)](#)
- ステップ 5 [アクセス制御の設定 \(47 ページ\)](#)
- ステップ 6 [設定の展開 \(48 ページ\)](#)

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。

手順

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。

The screenshot shows the 'Interfaces' configuration page in the Cisco Firepower Management Center. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (selected), 'Objects', 'AMP', and 'Intelligence'. Below the navigation bar, there are tabs for 'Device Management', 'NAT', 'VPN', 'QoS', 'Platform Settings', 'FlexConfig', and 'Certificates'. The main content area shows the IP address '10.89.5.20' and a 'Save' button. Below this, there are tabs for 'Device', 'Routing', 'Interfaces' (selected), 'Inline Sets', and 'DHCP'. A search bar and 'Add Interfaces' button are also present. The main table lists the following interfaces:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			
Ethernet1/3.1		SubInterface			
Ethernet1/4	diagnostic	Physical			
Ethernet1/5		Physical			

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。

The screenshot shows the 'Edit Physical Interface' configuration window. The 'General' tab is selected. The 'Name' field contains 'inside'. The 'Enabled' checkbox is checked, and 'Management Only' 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' field contains 'GigabitEthernet0/0'. The 'MTU' field contains '1500', with a range '(64 - 9000)' indicated to its right. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 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せんが、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。

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

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。

Edit Physical Interface ? x

General **IPv4** IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone: outside_zone

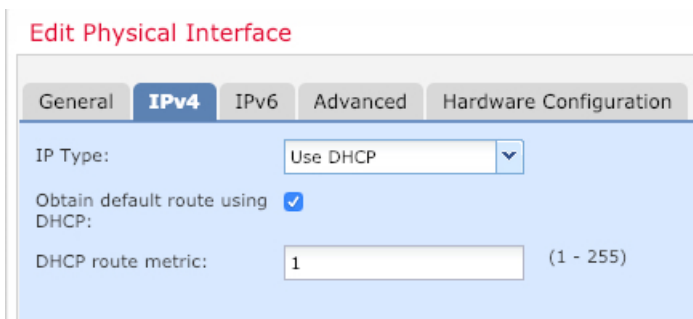
Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

OK Cancel

- 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。
- [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。
- [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。

手順

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るため、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。

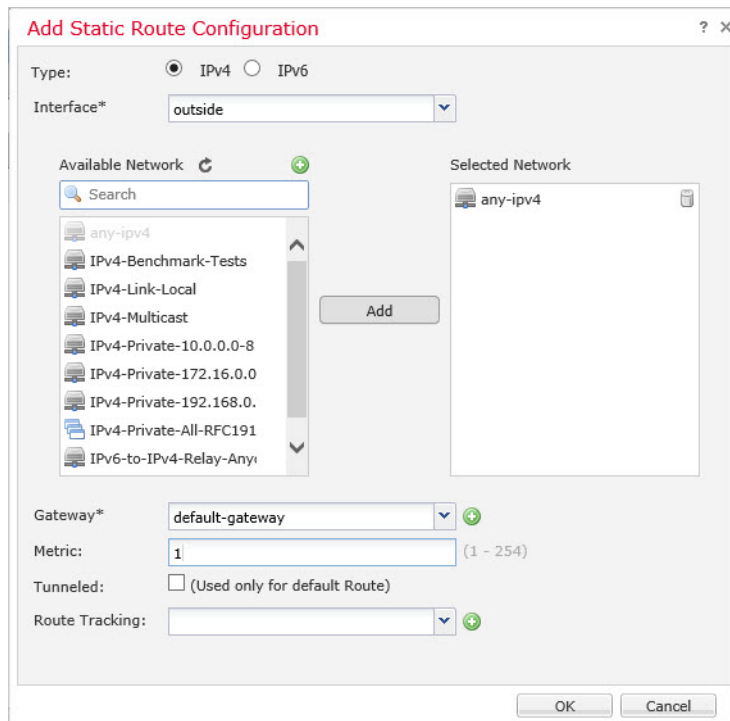
デフォルトルートの追加

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。

手順

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。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

10.99.5.20 You have unsaved changes Save Cancel

Cisco Firepower 9000 Series SM-24 Threat Defense

Device Routing Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
Static Route
Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

Add Route

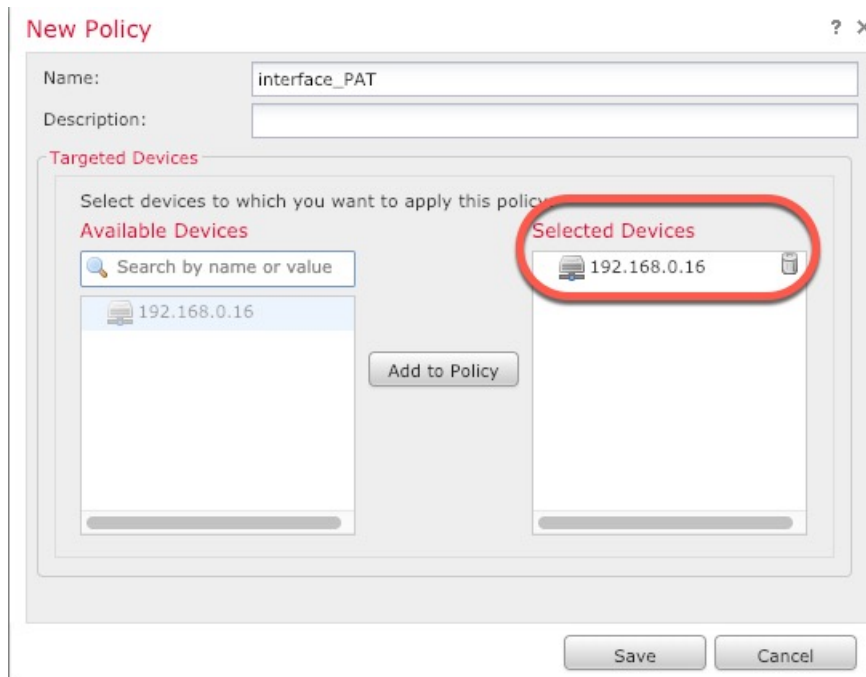
ステップ4 [保存 (Save)]をクリックします。

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。

手順

- 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。

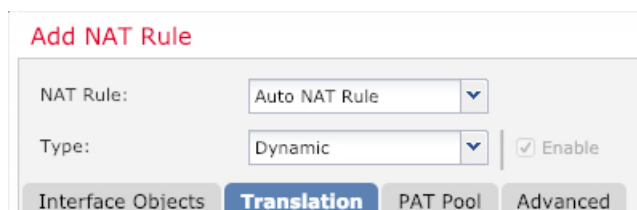


ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

ステップ 3 [ルール (Add Rule)] をクリックします。

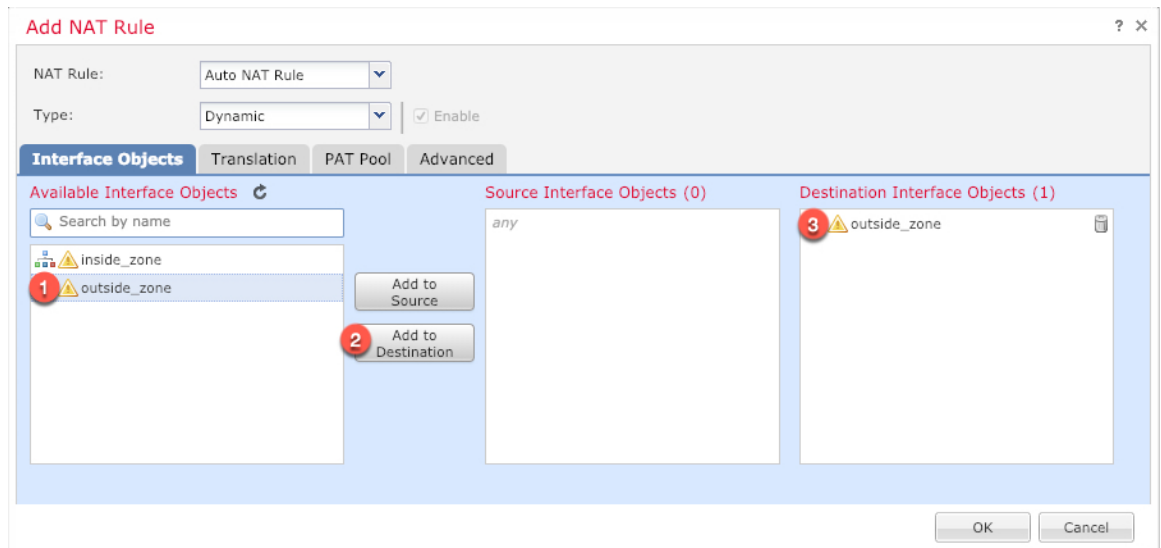
[NATルールの追加 (Add NAT Rule)] ダイアログボックスが表示されます。

ステップ 4 基本ルールのオプションを設定します。

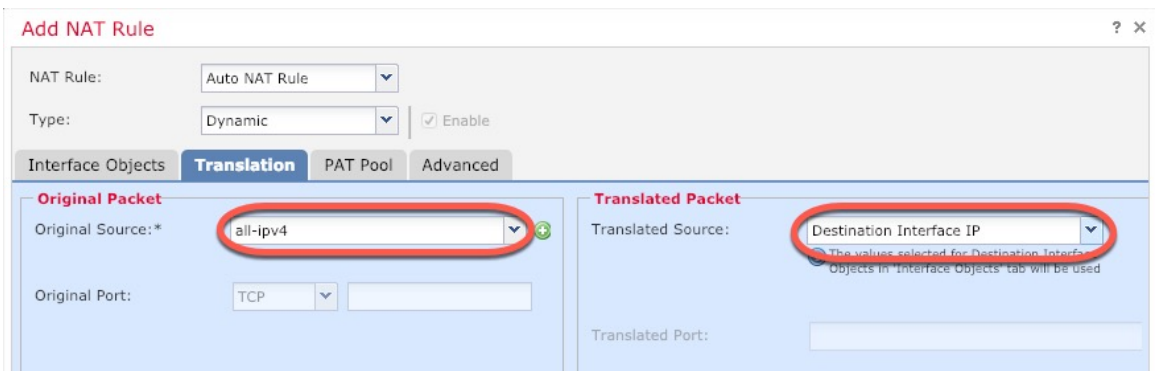


- [NATルール (NAT Rule)] : [自動NATルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

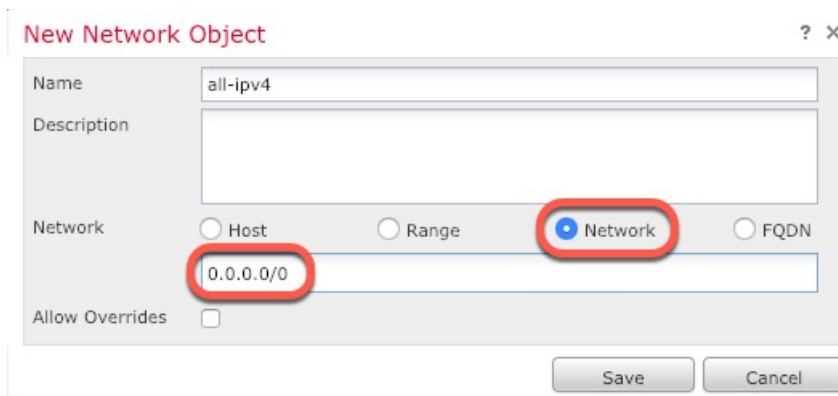
ステップ 5 [インターフェイスオブジェクト (Interface objects)] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects)] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects)] 領域に外部ゾーンを追加します。



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。

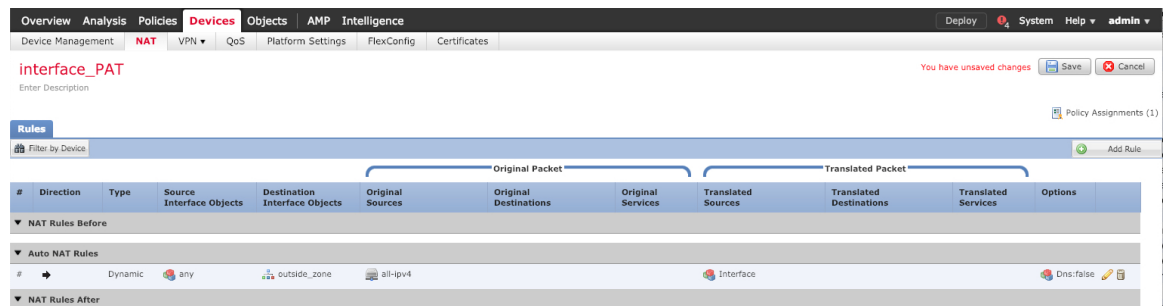


- (注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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

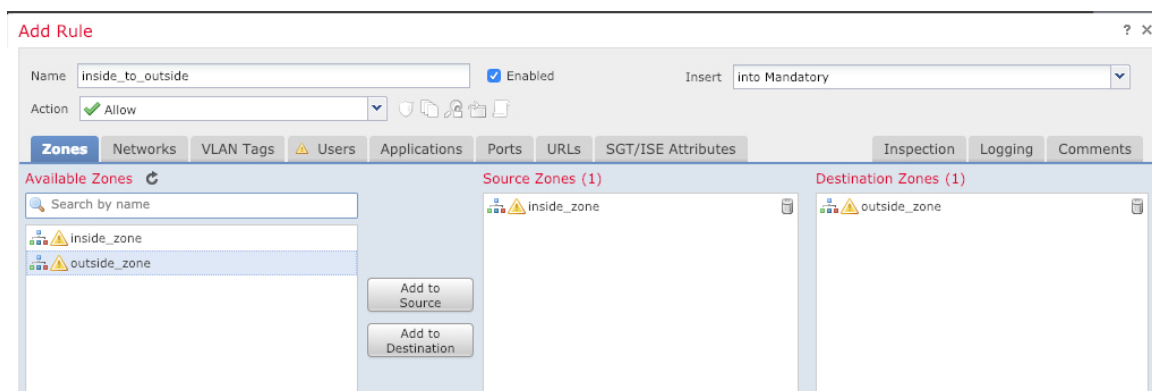
FTDv を FMC に登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセス コントロール ポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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。

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)] 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。

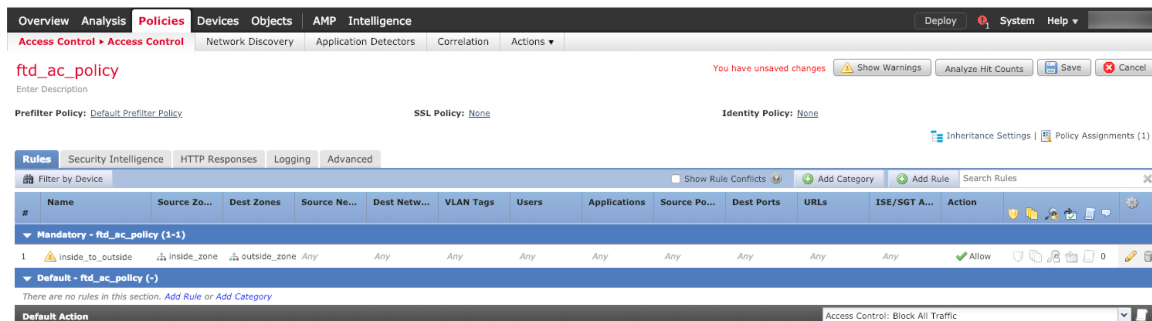


- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside_to_outside**) 。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] をクリックします。

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。



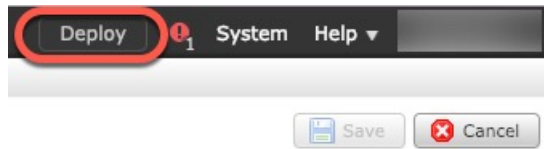
ステップ 4 [保存 (Save)] をクリックします。

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。

手順

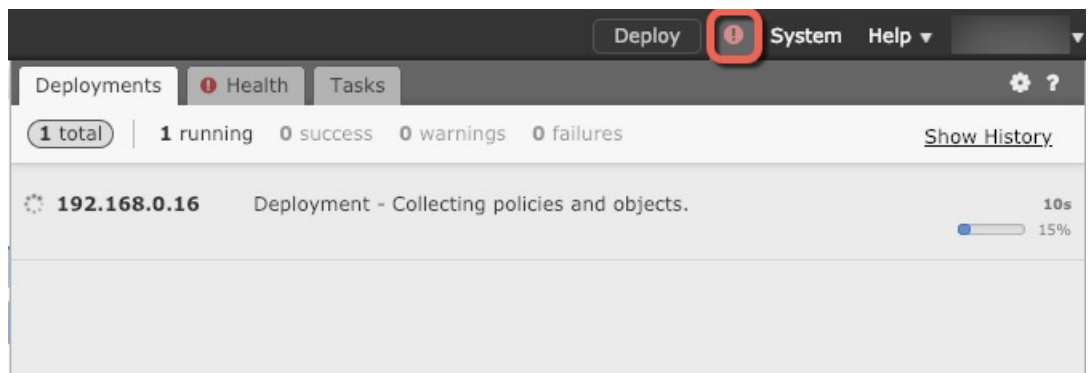
ステップ 1 右上の [展開 (Deploy)] をクリックします。



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。

手順

- 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。



第 4 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 \(51 ページ\)](#)
- [初期設定 \(52 ページ\)](#)
- [Firepower Device Manager でデバイスを設定する方法 \(55 ページ\)](#)

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 \(33 ページ\)](#)」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。

手順

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 Manager 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 \(55 ページ\)](#)」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。

手順

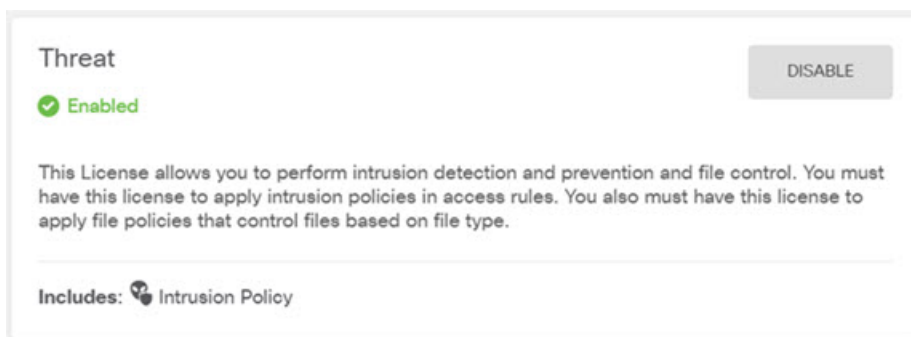
ステップ 1 [デバイス (Device)] を選択してから、[スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。

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 RAVPN 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 2: 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 3: インターフェイスの編集

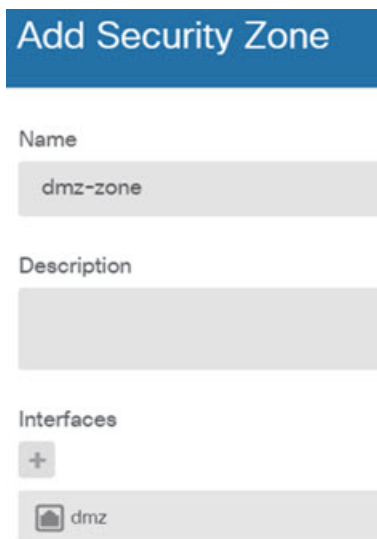
The screenshot displays the 'Edit Physical Interface' configuration interface. At the top, there is a blue header with the text 'Edit Physical Interface'. Below the header, the 'Interface Name' is set to 'dmz' and the 'Status' is turned on. A 'Description' field is present but empty. At the bottom, the 'IPv4 Address' tab is selected, showing the 'Type' as 'Static' and the 'IP Address and Subnet Mask' as '192.168.6.1 / 24'. A note below the field reads 'e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0'.

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 4: セキュリティゾーンオブジェクト



Add Security Zone

Name

dmz-zone

Description

Interfaces

+

dmz

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 5: DHCP サーバ



Add Server

Enabled DHCP Server

Interface

inside2

Address Pool

192.168.4.50-192.168.4.240

e.g. 192.168.45.46-192.168.45.254

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 6: デフォルトルート

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text field containing 'isp-gateway'.
- Interface:** A text field containing 'outside'.
- Metric:** A text field containing '1'.
- Networks:** A dropdown menu showing a plus sign and a selected option 'any-ipv4'.

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でのトラフィック 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。どの接続を復号化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せん。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 7: アクセス コントロール ポリシー

Order	Title	Action
2	Inside_DMZ	Allow


SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
inside_zone	ANY	ANY	dmz-zone	ANY	ANY

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 5 章

VMware のパフォーマンス調整 : Firepower Threat Defense Virtual のベストプラクティス

Firepower Threat Defense 仮想 は高性能のアプライアンスですが、最適な結果を得るにはハイパーバイザの調整が必要になる場合があります。

この章では、VMware vSphere 環境で Firepower Threat Defense 仮想 の最高のパフォーマンスを得るためのベストプラクティスと推奨事項について説明します。



(注) 最高のパフォーマンスを得るには、ESXi 6.0.0.0 以降を推奨します。

- [SR-IOV インターフェイスのプロビジョニング \(61 ページ\)](#)

SR-IOV インターフェイスのプロビジョニング

Single Root I/O Virtualization (SR-IOV) により、さまざまなゲストオペレーティングシステムを実行している複数の VM が、ホストサーバ内の単一の PCIe ネットワークアダプタを共有できるようになります。SR-IOV では、VM がネットワーク アダプタとの間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバの CPU 負荷が低下します。最近の x86 サーバプロセッサには、SR-IOV に必要なダイレクトメモリの転送やその他の操作を容易にする Intel VT-d テクノロジーなど、チップセットの拡張機能が搭載されています。

SR-IOV 仕様では、次の 2 つのデバイス タイプが定義されています。

- 物理機能 (PF) : 基本的にスタティック NIC です。PF は、SR-IOV 機能を含む完全な PCIe デバイスです。PF は、通常の PCIe デバイスとして検出、管理、設定されます。単一 PF は、一連の仮想関数 (VF) の管理および設定を提供できます。
- Virtual Function (VF) : ダイナミック vNIC に似ています。VF は、データ移動に必要な最低限のリソースを提供する、完全または軽量の仮想 PCIe デバイスです。VF は直接的には

管理されず、PF を介して配信および管理されます。1 つ以上の VF を 1 つの VM に割り当てることができます。

VF は、仮想化されたオペレーティング システム フレームワーク内の Firepower Threat Defense Virtual 仮想マシンに最大 10 Gbps の接続を提供できます。このセクションでは、VMware 環境で VF を設定する方法について説明します。

SR-IOV インターフェイスのベストプラクティス

SR-IOV インターフェイスに関するガイドライン

VMware vSphere 5.1 以降のリリースは、特定の設定の環境でしか SR-IOV をサポートしません。vSphere の一部の機能は、SR-IOV が有効になっていると機能しません。

Firepower Threat Defense 仮想 と SR-IOV に関する [システム要件](#) に加えて、VMware と SR-IOV に関する要件、サポートされている NIC、機能の可用性、およびアップグレード要件の詳細については、VMware マニュアル内の「[Supported Configurations for Using SR-IOV](#)」で確認する必要があります。

このセクションでは、VMware システム上の SR-IOV インターフェイスのプロビジョニングに関するさまざまなセットアップ手順と設定手順を示します。このセクション内の情報は、VMware ESXi 6.0 と vSphere Web Client、Cisco UCS C シリーズ サーバ、および Intel Ethernet Server Adapter X520 - DA2 を使用した特定のラボ環境内のデバイスから作成されたものです。

SR-IOV インターフェイスに関する制限事項

Firepower Threat Defense 仮想 を起動すると、ESXi で表示される順序とは逆の順序で、SR-IOV インターフェイスが表示される場合があります。これにより、インターフェイス設定エラーが発生し、特定の FTDv 仮想マシンへのネットワーク接続が切断する場合があります。



注意 FTDv で SR-IOV ネットワーク インターフェイスの設定を開始する前に、インターフェイスのマッピングを確認することが重要です。これにより、ネットワーク インターフェイスの設定が、VM ホストの正しい物理 MAC アドレスインターフェイスに適用されます。

FTDv が起動したら、MAC アドレスとインターフェイスのマッピングを確認できます。**show interface** コマンドを使用して、インターフェイスの MAC アドレスなど、インターフェイスの詳細情報を確認します。インターフェイス割り当てが正しいことを確認するには、**show kernel ifconfig** コマンドの結果と MAC アドレスを比較します。

ESXi ホスト BIOS の確認

始める前に

VMware に SR-IOV インターフェイスを備えた FTDv を導入するには、仮想化をサポートして有効にする必要があります。VMware では、SR-IOV サポートに関するオンラインの

『[Compatibility Guide](#)』だけでなく、仮想化が有効か無効かを検出するダウンロード可能な『[CPU Identification Utility](#)』も含めて、仮想化サポートの各種確認手段を提供しています。

また、ESXi ホストにログインすることによって、BIOS 内で仮想化が有効になっているかどうかを判断することもできます。

手順

ステップ 1 次のいずれかの方法を使用して、ESXi シェルにログインします。

- ホストへの直接アクセスがある場合は、Alt+F2 を押して、マシンの物理コンソールのログインページを開きます。
- ホストにリモートで接続している場合は、SSH または別のリモート コンソール接続を使用して、ホスト上のセッションを開始します。

ステップ 2 ホストによって認識されるユーザ名とパスワードを入力します。

ステップ 3 次のコマンドを実行します。

例 :

```
esxcfg-info|grep "\----\HV Support"
```

HV Support コマンドの出力は、使用可能なハイパーバイザサポートのタイプを示します。可能性のある値の説明を以下に示します。

0 : VT/AMD-V は、サポートがこのハードウェアでは使用できないことを示します。

1 : VT/AMD-V は、VT または AMD-V を使用できますが、このハードウェアではサポートされないことを示します。

2 : VT/AMD-V は、VT または AMD-V を使用できますが、現在、BIOS 内で有効になっていないことを示します。

3 : VT/AMD-V は、VT または AMD-V が BIOS 内で有効になっており、使用できることを示します。

例 :

```
~ # esxcfg-info|grep "\----\HV Support"
      |----HV Support.....3
```

値の 3 は、仮想化がサポートされており、有効になっていることを示します。

次のタスク

- ホスト物理アダプタ上で SR-IOV を有効にします。

ホスト物理アダプタ上での SR-IOV の有効化

仮想マシンを仮想機能に接続する前に、vSphere Web Client を使用して、SR-IOV を有効にし、ホスト上の仮想機能の数を設定します。

始める前に

- SR-IOV 互換ネットワーク インターフェイス カード (NIC) がインストールされていることを確認します。「[システム要件 \(4 ページ\)](#)」を参照してください。

手順

ステップ 1 vSphere Web Client で、SR-IOV を有効にする ESXi ホストに移動します。

ステップ 2 [Manage] タブで、[Networking] をクリックし、[Physical adapters] を選択します。

SR-IOV プロパティを調査することにより、物理アダプタが SR-IOV をサポートしているかどうかを確認できます。

ステップ 3 物理アダプタを選択し、[Edit adapter settings] をクリックします。

ステップ 4 SR-IOV の下で、[Status] ドロップダウン メニューから [Enabled] を選択します。

ステップ 5 [Number of virtual functions] テキストボックスに、アダプタに設定する仮想機能の数を入力します。

(注) インターフェイスあたり 2 つ以上の VF を使用しないことをお勧めします。物理インターフェイスを複数の仮想機能で共有すると、パフォーマンスが低下する可能性があります。

ステップ 6 [OK] をクリックします。

ステップ 7 ESXi ホストを再起動します。

物理アダプタ エントリで表現された NIC ポートで仮想機能がアクティブになります。これらは、ホストの [Settings] タブの [PCI Devices] リストに表示されます。

次のタスク

- SR-IOV 機能と設定を管理するための標準 vSwitch を作成します。

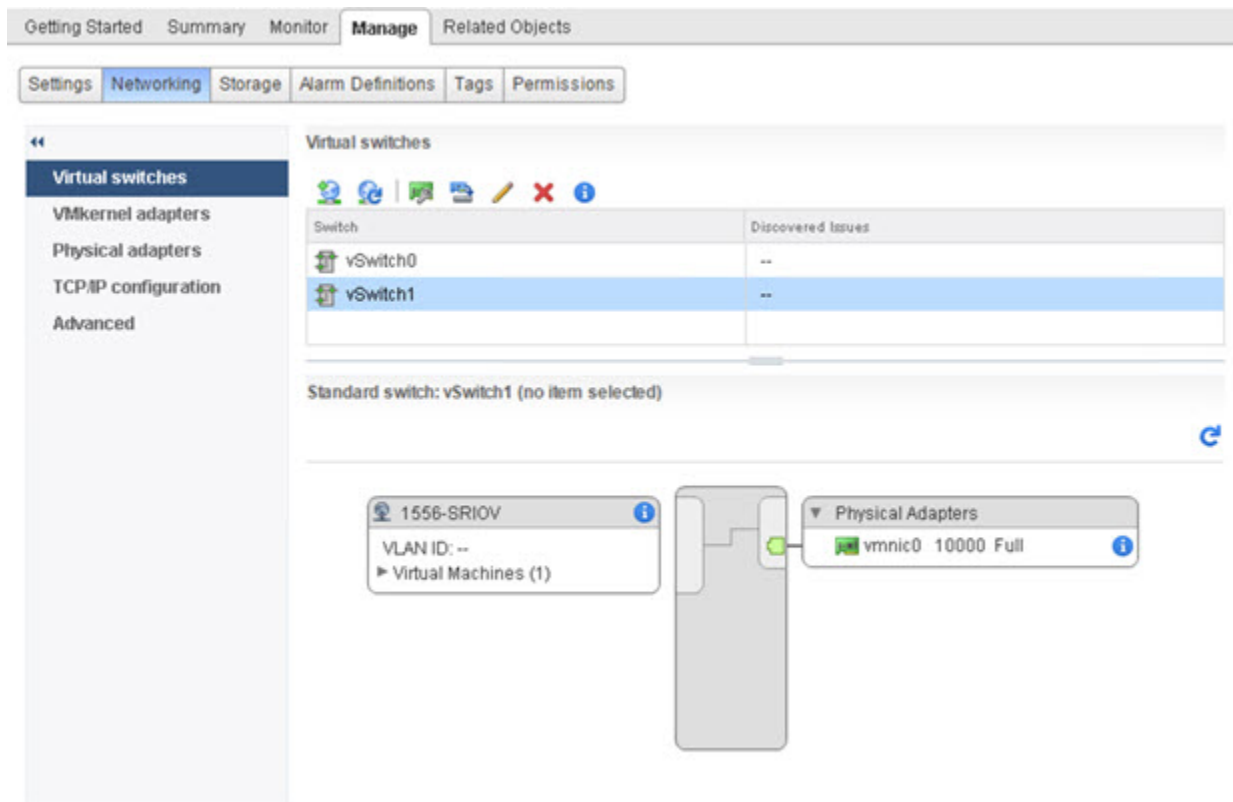
vSphere スイッチの作成

SR-IOV インターフェイスを管理するための vSphere スイッチを作成します。

手順

- ステップ 1** vSphere Web Client で、ESXi ホストに移動します。
- ステップ 2** [Manage] で、[Networking] を選択してから、[Virtual switches] を選択します。
- ステップ 3** プラス (+) 記号付きの緑色の地球アイコンである [Add host networking] アイコンをクリックします。
- ステップ 4** [標準スイッチ用仮想マシンポートグループ (Virtual Machine Port Group for a Standard Switch)] 接続タイプを選択して、[次へ (Next)] をクリックします。
- ステップ 5** [New standard switch] を選択して、[Next] をクリックします。
- ステップ 6** 物理ネットワーク アダプタを新しい標準スイッチに追加します。
- 割り当てられたアダプタの下で、緑色のプラス (+) 記号をクリックしてアダプタを追加します。
 - リストから SR-IOV に対応するネットワーク インターフェイスを選択します。たとえば、Intel(R) 82599 10 Gigabit Dual Port Network Connection を選択します。
 - [Failover order group] ドロップダウンメニューで、[Active adapters] から選択します。
 - [OK] をクリックします。
- ステップ 7** SR-IOV vSwitch の [Network label] を入力して、[Next] をクリックします。
- ステップ 8** [Ready to complete] ページで選択を確認してから、[Finish] をクリックします。
-

図 8: SR-IOV インターフェイスがアタッチされた新しい vSwitch



次のタスク

- 仮想マシンの互換性レベルを確認します。

仮想マシンの互換性レベルのアップグレード

互換性レベルは、ホストマシンで使用可能な物理ハードウェアに対応する仮想マシンで使用可能な仮想ハードウェアを決定します。FTDv VM は、ハードウェアレベルを 10 以上にする必要があります。これにより、SR-IOV のパススルー機能が FTDv に公開されます。この手順では、FTDv を短時間で最新のサポートされている仮想ハードウェアバージョンにアップグレードします。

仮想マシンのハードウェアバージョンと互換性については、vSphere 仮想マシン管理マニュアルを参照してください。

手順

- ステップ 1** vSphere Web Client から vCenter Server にログインします。
- ステップ 2** 変更する FTDv 仮想マシンを特定します。

- a) データセンター、フォルダ、クラスタ、リソースプール、またはホストを選択して、[関連オブジェクト (Related Objects)] タブをクリックします。
- b) [仮想マシン (Virtual Machines)] をクリックして、リストから FTDv 仮想マシンを選択します。

ステップ 3 選択した仮想マシンの電源をオフにします。

ステップ 4 FTDv を右クリックして、[アクション (Actions)] > [すべての vCenter アクション (All vCenter Actions)] > [互換性 (Compatibility)] > [VM アップグレードの互換性 (Upgrade VM Compatibility)] を選択します。

ステップ 5 [はい (Yes)] をクリックして、アップグレードを確認します。

ステップ 6 仮想マシンの互換性で [ESXi 5.5以降 (ESXi 5.5 and later)] オプションを選択します。

ステップ 7 (オプション) [通常のゲスト OS のシャットダウン後のみアップグレード (Only upgrade after normal guest OS shutdown)] を選択します。

選択された仮想マシンが、選択された [互換性 (Compatibility)] 設定の対応するハードウェアバージョンにアップグレードされ、仮想マシンの [概要 (Summary)] タブで新しいハードウェアバージョンが更新されます。

次のタスク

- SR-IOV パススルー ネットワーク アダプタを介して FTDv と仮想機能を関連付けます。

Firepower Threat Defense Virtual への SR-IOV NIC の割り当て

FTDv 仮想マシンと物理 NIC がデータを交換可能なことを保証するには、FTDv を SR-IOV パススルー ネットワーク アダプタとして 1 つ以上の仮想機能に関連付ける必要があります。次の手順では、vSphere Web Client を使用して、SR-IOV NIC を FTDv 仮想マシンに割り当てる方法について説明します。

手順

ステップ 1 vSphere Web Client から vCenter Server にログインします。

ステップ 2 変更する FTDv 仮想マシンを特定します。

- a) データセンター、フォルダ、クラスタ、リソースプール、またはホストを選択して、[関連オブジェクト (Related Objects)] タブをクリックします。
- b) [仮想マシン (Virtual Machines)] をクリックして、リストから FTDv 仮想マシンを選択します。

ステップ 3 仮想マシンの [Manage] タブで、[Settings] > [VM Hardware] を選択します。

ステップ 4 [Edit] をクリックして、[Virtual Hardware] タブを選択します。

ステップ 5 [New device] ドロップダウンメニューで、[Network] を選択して、[Add] をクリックします。

[New Network] インターフェイスが表示されます。

ステップ 6 [New Network] セクションを展開して、使用可能な SRIOV オプションを選択します。

ステップ 7 [Adapter Type] ドロップダウンメニューで、[SR-IOV passthrough] を選択します。

ステップ 8 [Physical function] ドロップダウンメニューで、パススルー仮想マシンアダプタに対応する物理アダプタを選択します。

ステップ 9 仮想マシンの電源をオンにします。

仮想マシンの電源をオンにすると、ESXi ホストが物理アダプタから空いている仮想機能を選択して、それを SR-IOV パススルーアダプタにマップします。ホストが仮想マシンアダプタと基礎となる仮想機能のすべてのプロパティを確認します。

