



Firepower Device Manager を使用して VMware 上で Cisco Firepower Threat Defense Virtual を導入するためのクイック スタート ガイド

バージョン **6.2.2** 以降

初版:2017 年 9 月 5 日

最終更新日:2018 年 12 月 3 日

Cisco Firepower Threat Defense Virtual Firepower Device Manager を使用して VMware 上で展開できます。システム要件およびハイパーバイザのサポートについては『[Cisco Firepower Compatibility Guide](#)』を参照してください。

- [Firepower Threat Defense Virtual の VMware 機能のサポート \(1 ページ\)](#)
- [Firepower Threat Defense Virtual Firepower Device Manager、および VMware の前提条件 \(2 ページ\)](#)
- [システム要件 \(4 ページ\)](#)
- [Firepower Threat Defense Virtual および Firepower Device Manager のガイドライン \(6 ページ\)](#)
- [Firepower Threat Defense Virtual と VMware の制限事項および既知の問題点 \(7 ページ\)](#)
- [OVF ファイルのガイドライン \(8 ページ\)](#)
- [VMware vSphere Web クライアントまたは vSphere ハイパーバイザを使用した Firepower Threat Defense Virtual の展開 \(9 ページ\)](#)
- [インストール後の設定 \(12 ページ\)](#)
- [仮想アプライアンスの電源投入 \(14 ページ\)](#)
- [初期設定 \(15 ページ\)](#)
- [Firepower Device Manager のデバイスを構成する方法 \(18 ページ\)](#)
- [SR-IOV インターフェイスのプロビジョニング \(22 ページ\)](#)

Firepower Threat Defense Virtual の VMware 機能のサポート

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

Firepower Threat Defense Virtual Firepower Device Manager、および VMware の前提条件

表 1 Firepower Threat Defense Virtual の VMware 機能のサポート

| 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。 vMotion に関するガイドライン(7 ページ) 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 が動作しています。 | なし | — |
| スナップショット | VM が数秒間フリーズします。 | なし | — |
| 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 VM の障害に対して Firepower のフェールオーバー機能を使用します。 |
| 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 VM の障害に対して 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 Threat Defense Virtual Firepower Device Manager、および VMware の前提条件

- 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。既存の仮想マシンを以前のバージョン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、デフォルトで有効です。
(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。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。
- ESXi 上で VMware vSphere Web クライアントまたは vSphere スタンドアロン クライアントを使用して Firepower Threat Defense Virtual を展開し、Firepower Device Manager を使用して仮想マシンを構成します。
- VMware 上の仮想マシンは、e1000(1 Gbit/s)インターフェイスをデフォルトで使用します。デフォルトのインターフェイスを vmxnet3 または ixgbe(10 Gbit/s)インターフェイスに置き換えることができます。

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にかかわらず依存します。

デフォルトの設定は、Firepower Threat Defense Virtual の適切な動作をブロックします。以下の必須の設定を参照してください。

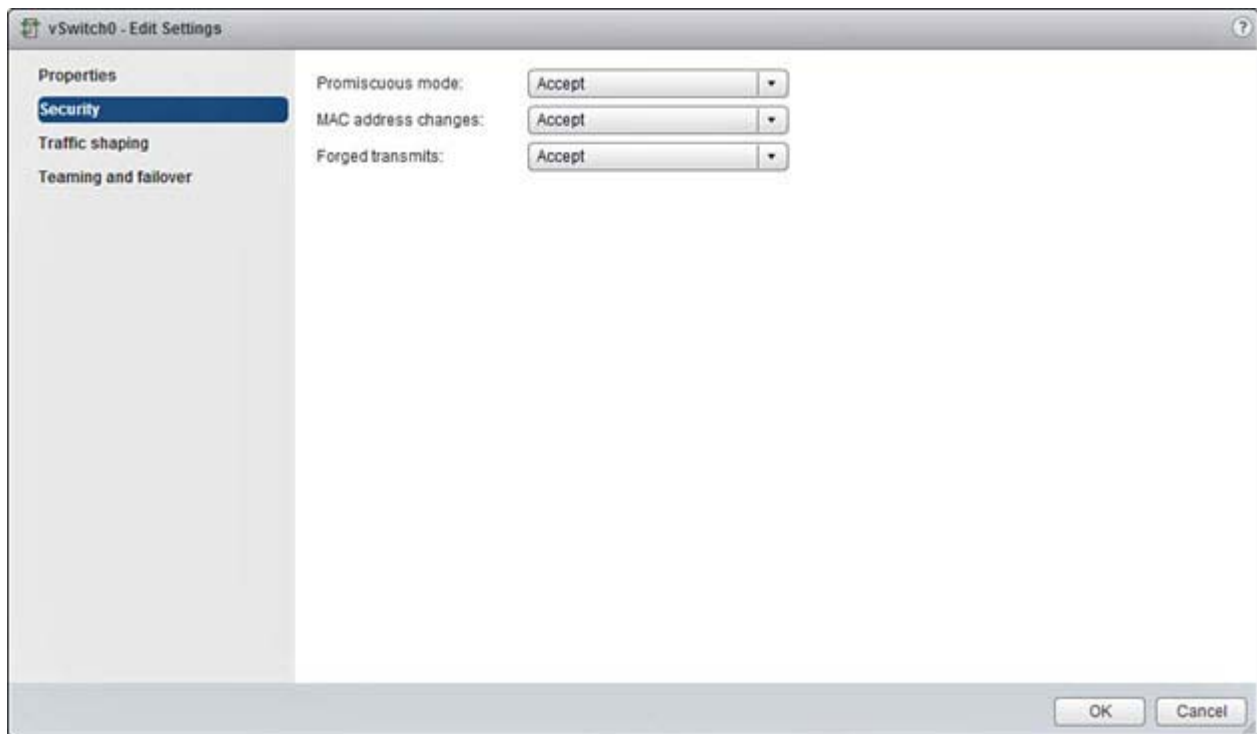
表 2 vSphere 標準スイッチのセキュリティ ポリシー オプション

| 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 クライアントの 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。 |
| MAC アドレスの変更 (MAC Address Changes) | 承認 (Accept) | vSphere Web クライアントの 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 クライアントの 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。 |

手順

1. vSphere Web クライアントで、ホストに移動します。
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。
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。
4. [セキュリティ (Security)] を選択し、現在の設定を表示します。
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。

システム要件



6. [OK] をクリックします。

次の作業

これらの設定が、Firepower Threat Defense Virtual 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。

システム要件

Firepower Threat Defense Virtual 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。Firepower Threat Defense Virtual 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。

次の表に、デフォルトのアプライアンス設定を示します。

表 3 Firepower Threat Defense Virtual アプライアンスのデフォルト設定

| 設定 | デフォルト | 設定調整の可否 |
|-----------------------------|---------|--|
| メモリ | 8GB | No |
| 仮想 CPU | 4 | No |
| ハード ディスク プロビジョニング サイズ | 48.24GB | No。[ディスク形式 (Disk Format)] の選択に基づく (シン プロビ ジョニングでは 48.24 GB) |

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、VMware のオンライン[互換性ガイド](#)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。

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、Firepower Threat Defense Virtual 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。VMware の場合は、オンラインの『[Compatibility Guide](#)』で SR-IOV サポートを検索できます。

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。

Linux コマンドラインによる CPU 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。

Firepower Threat Defense Virtual および Firepower Device Manager のガイドライン

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** が表示されません。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
```

Firepower Threat Defense Virtual および Firepower Device Manager のガイドライン

サポート対象のネットワーク アダプタ タイプ

Firepower Threat Defense Virtual は次の 3 つの仮想ネットワーク アダプタをサポートしています。

- **e1000**:仮想マシンの作成時に、VMware はデフォルトの **e1000**(1 Gbit/s) インターフェイスを設定します。**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。
- **VMXNET3**:**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。

(注)このリリースでは、**ixgbe** ドライバは、Firepower Threat Defense Virtual のフェールオーバー(HA)の展開をサポートしていません。

- **IXGBE-VF**:**ixgbe-vf** 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、[システム要件\(4 ページ\)](#)を参照してください。

デフォルト設定

Firepower Threat Defense Virtual 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、**Management0-0** と **GigabitEthernet0-1**(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。

(注) 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 **Management0-0** 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。

Firepower Threat Defense Virtual 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。**

- 仮想マシン上の 1 番目のインターフェイス (**Management0-0**) 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 (**GigabitEthernet0-0**) は、外部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 (**GigabitEthernet0-1**) は、内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 (**GigabitEthernet0-2**) は、データ インターフェイスです。使用しないインターフェイスについては、インターフェイスを無効のままにしておくことができます。4 番目のインターフェイスを削除しないでください。

(注) 仮想マシンの作成時に、VMware はデフォルトの **e1000 (1 Gbit/s)** インターフェイスを設定しています。仮想マシンの作成が終了し、**Firepower Threat Defense Virtual** が完全にインストールされたら、デフォルトの **e1000** インターフェイスをすべて削除して **vmxnet3 (10 Gbit/s)** または **ixgbe (10 Gbit/s)** インターフェイスに置き換え、ネットワークスループットを向上させることができます。

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。** **VMware インターフェイスの設定 (13 ページ)** を参照してください。

Firepower Threat Defense Virtual と VMware の制限事項および既知の問題点

- Cisco では、**5 つ以上の vmxnet3 ネットワーク カードを使用する場合、VMware vCenter** によって管理されるホストを使用することが推奨されます。スタンドアロン 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 カードは追加されません。 **VMware インターフェイスの設定 (13 ページ)** を参照してください。
- 仮想マシンの複製はサポートされません。
- スナップショットによる仮想マシンの復元はサポートされません。
- バックアップの復元はサポートされません。 **Firepower Threat Defense Virtual** 管理対象デバイスのバックアップ ファイルを作成または復元することはできません。 イベント データをバックアップするには、管理用の **Firepower Management Center** のバックアップを実行します。

vMotion に関するガイドライン

- **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。 **Firepower Threat Defense Virtual** の導入時に、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、**Firepower Threat Defense Virtual** を **vMotion** を使用して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。共有ストレージを使用しない場合は、**VM** の電源を切らないと移行が行われません。

INIT Respanning エラー メッセージ

症状: ESXi 6 および ESXi 6.5 で実行されている **Firepower Threat Defense Virtual** 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 "ftd1" respawning too fast: disabled for 5 minutes"
```

OVF ファイルのガイドライン

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。
5. [OK] をクリックして設定を保存します。

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場合、以下のインストール オプションがあります。

```
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。

- **VI OVF** テンプレートを 사용하여展開する場合、インストール プロセスで、Firepower Threat Defense Virtual 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 を使用するのみサポートされるモードです。
- (注) この仮想アプライアンスは、VMware vCenter を使用して管理する必要があります。
- **ESXi OVF** テンプレートを 사용하여展開する場合、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。この仮想アプライアンスは、VMware vCenter を使用して管理することも、スタンドアロン アプライアンスとして使用することもできます。詳細については、[初期設定 \(15 ページ\)](#) を参照してください。

OVF テンプレートを展開する際に、以下の情報を指定します。

表 4 VMware OVF テンプレート

| 設定 | ESXi または VI | 操作 |
|---------------------|-------------|---|
| OVF テンプレートのインポート/展開 | 両方 | 前の手順でダウンロードした、使用する OVF テンプレートを参照します。 |
| OVF テンプレートの詳細 | 両方 | インストールするアプライアンス (Cisco Firepower Threat Defense Virtual) と展開オプション (VI または ESXi) を確認します。 |
| 使用許諾契約の同意 | VI のみ | OVF テンプレートに含まれるライセンス条項を受け入れることに同意します。 |
| 名前と場所 | 両方 | 仮想アプライアンスの一意のわかりやすい名前を入力し、アプライアンスのインベントリの場所を選択します。 |

VMware vSphere Web クライアントまたは vSphere ハイパーバイザを使用した Firepower Threat Defense Virtual の展開

表 4 VMware OVF テンプレート (続き)

| 設定 | ESXi または VI | 操作 |
|--------------|-------------|---|
| ホスト/クラスタ | 両方 | 仮想アプライアンスを展開するホストまたはクラスタを選択します。 |
| リソース プール | 両方 | ホストやクラスタ内のコンピューティング リソースを、わかりやすい階層を設定して管理します。仮想マシンと子リソース プールは親リソース プールのリソースを共有します。 |
| ストレージ | 両方 | 仮想マシンに関連付けられているすべてのファイルを保存します。 |
| ディスクの書式設定 | 両方 | 仮想ディスクを保存する形式を、シック プロビジョニング (Lazy Zeroed)、シック プロビジョニング (Eager Zeroed)、シン プロビジョニングの中から選択します。 |
| ネットワーク マッピング | 両方 | 仮想アプライアンスの管理インターフェイスを選択します。 |
| プロパティ | VI のみ | <p>管理モードを含む、仮想マシンの初期設定セットアップをカスタマイズします。</p> <p>(注) Firepower Device Manager を使用して Firepower Threat Defense Virtual デバイスを管理するには、[ローカル マネージャを有効にする (Enable Local Manager)] の [はい(Yes)] を選択します。Firepower Device Manager を使用する場合のみルーティング モードで Firepower Threat Defense Virtual デバイスを展開できます。</p> <p>Firepower Device Manager のセットアップについては「初期設定」(15 ページ)を参照してください。</p> <p>(注) Firepower Management Center (リモート マネージャ) の登録 (Registration) プロパティは、[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、システムによって無視されます。</p> |

VMware vSphere Web クライアントまたは vSphere ハイパーバイザを使用した Firepower Threat Defense Virtual の展開

VMware vSphere Web クライアントを使用して、Firepower Threat Defense Virtual を展開できます。Web クライアントには、vCenter が必要です。また、スタンドアロンの ESXi の展開には、vSphere ハイパーバイザを使用できます。vSphere を使用して、VI OVF テンプレートまたは ESXi OVF テンプレートのいずれかによる展開が可能です。

- VI OVF テンプレートを使用して展開する場合、アプライアンスは VMware vCenter によって管理する必要があります。
- ESXi OVF テンプレートを使用して展開する場合、アプライアンスは VMware vCenter によって管理するか、またはスタンドアロン ホストに展開できます。いずれの場合も、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。

VMware vSphere Web クライアントまたは vSphere ハイパーバイザを使用した Firepower Threat Defense Virtual の展開

はじめる前に

- シスコのサポート サイト (<https://software.cisco.com/download/navigator.html> [英語]) の [ダウンロード (Downloads)] エリアから Firepower Threat Defense Virtual のアーカイブ ファイルをダウンロードします。
(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。
- アーカイブ 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。

手順

1. vSphere Client を使用して、[ファイル (File)] > [OVF テンプレートの展開 (Deploy OVF Template)] をクリックし、以前にダウンロードした OVF テンプレートを展開します。
2. ドロップダウン リストから、Firepower Threat Defense Virtual デバイス用に展開する OVF テンプレートを 1 つ 選択します。
`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、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。
3. [OVF テンプレートの詳細 (OVF Template Details)] ページが表示されるので [次へ (Next)] をクリックします。
4. ライセンス契約書が OVF テンプレート (VI テンプレートのみ) に含まれている場合は、エンドユーザ ライセンス契約のページが表示されます。ライセンス条項に同意し、[次へ (Next)] をクリックすることに同意します。
5. オプションで、名前を編集し、Firepower Threat Defense Virtual を配置するインベントリ内のフォルダの場所を選択して、[次へ (Next)] をクリックすることもできます。
(注) vSphere クライアントが ESXi ホストに直接接続されている場合、フォルダの場所を選択するオプションは表示されません。
6. Firepower Threat Defense Virtual を展開するホストまたはクラスタを選択して、[次へ (Next)] をクリックします。
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。
8. 仮想マシン ファイルを保存する場所を選択し、[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。
9. 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。
10. OVF テンプレートで使用されるネットワークを自分のインベントリのネットワークにマップします。インフラストラクチャの [宛先ネットワーク (Destination Networks)] 列を右クリックしてネットワークを選択し、各 Firepower Threat Defense Virtual インターフェイスのネットワーク マッピングを設定して [次へ (Next)] をクリックします。
(注) Firepower Threat Defense Virtual では、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。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。
インターネットから到達可能な VM ネットワークに管理 0-0 インターフェイスが関連付けられていることを確認します。

VMware vSphere Web クライアントまたは vSphere ハイパーバイザを使用した Firepower Threat Defense Virtual の展開

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、[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後で変更できます。展開後、**Firepower Threat Defense Virtual** 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 **Firepower Threat Defense Virtual** インターフェイス ID は表示されません (ネットワーク アダプタ ID のみ)。

Firepower Threat Defense Virtual 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 5 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 |
|-------------------|--------------------|--------------------|------------|
| Network adapter 1 | Management0-0 | Diagnostic0/0 | 管理と診断 |
| Network adapter 2 | GigabitEthernet0-0 | GigabitEthernet0/0 | 外部データ |
| Network adapter 3 | GigabitEthernet0-1 | GigabitEthernet0/1 | 内部データ |
| Network adapter 4 | GigabitEthernet0-2 | GigabitEthernet0/2 | データ トラフィック |

(注) **vSphere Client** では、少なくとも 4 つのネットワークにインターフェイスを割り当てる必要があります。すべての **Firepower Threat Defense Virtual** 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、**Firepower Threat Defense Virtual** 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。

Firepower Threat Defense Virtual デバイスを展開する際には、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。詳細については、**vSphere Client** オンライン ヘルプを参照してください。

(注) **Firepower Threat Defense Virtual** デバイスの展開後にさらにインターフェイスの追加が必要な場合は、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Add Interfaces to Firepower Threat Defense Virtual」のセクションを参照してください。

- ユーザ設定可能なプロパティが OVF テンプレート (VI テンプレートのみ) に含まれている場合は、設定可能なプロパティを設定し、[次へ (Next)] をクリックします。

(注) **Firepower Device Manager** を使用して **Firepower Threat Defense Virtual** を設定するために、ローカル管理を有効にします。**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 1 つの管理モードのみ使用できます。

- [終了準備の完了 (Ready to Complete)] ウィンドウで設定を見直し、確認します。オプションで、[展開後に電源を入れる (Power on after deployment)] オプションにチェック マークを付けて、**Firepower Threat Defense Virtual** に電源を入れ、[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** は VM を処理します。[最近使用したタスク (Recent Tasks)] ペインの [グローバル情報 (Global Information)] 領域で [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、[Deploy OVF Template] 完了ステータスが表示されます。

その後、**Firepower Threat Defense Virtual VM** 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 **Firepower Threat Defense Virtual** を正常に登録するには、**Firepower Threat Defense Virtual** 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。

インストール後の設定

次の作業

- 仮想アプライアンスのハードウェアおよびメモリ設定の変更、またはインターフェイスの設定が必要かどうかを確認します。[インストール後の設定\(12 ページ\)](#)を参照してください。
- **Firepower Device Manager** を使用してデバイスを設定します。[Firepower Device Manager のデバイスを構成する方法\(18 ページ\)](#)を参照してください。

インストール後の設定

仮想アプライアンスの展開後に、仮想アプライアンスのハードウェアおよびメモリの設定が展開の要件を満たしていることを確認します。デフォルトの設定は、システム ソフトウェアの実行の最小要件であるため、**減らさない**でください。次の表に、デフォルトのアプライアンス設定を示します。

表 6 デフォルトの仮想アプライアンス設定

| 設定 | デフォルト | 設定調整の可否 |
|-----------------------------|----------|---|
| メモリ | 8 GB | なし |
| 仮想 CPU | 4 | なし |
| ハード ディスク プロビジョニング サイズ | 48.24 GB | なし。[ディスク形式(Disk Format)] の選択に基づきます(シンプル プロビジョニングでは 48.24 GB) |

仮想マシンのプロパティの確認

[Vmware 仮想マシンプロパティ (VMware Virtual Machine Properties)] ダイアログボックスを使用して、選択した仮想マシンのホスト リソースの割り当てを調整できます。このタブで、CPU、メモリ、ディスク、および拡張 CPU リソースを変更できます。また、仮想マシンの仮想イーサネット アダプタ設定の電源接続設定、MAC アドレス、およびネットワーク接続を変更できます。

手順

1. 新しい仮想アプライアンスの名前を右クリックし、コンテキスト メニューから **[Edit Settings]** を選択するか、メイン ウィンドウの **[Getting Started]** タブから **[Edit virtual machine settings]** をクリックします。

2. [表 6 デフォルトの仮想アプライアンス設定\(12 ページ\)](#) に示すように、**[メモリ (Memory)]**、**[CPU (CPUs)]**、および **[ハード ディスク 1 (Hard disk 1)]** の設定がデフォルトに設定されていることを確認します。

アプライアンスのメモリ設定および仮想 CPU の数は、ウィンドウの左側に表示されます。ハード ディスクの **プロビジョニング サイズ** を表示するには、**[ハード ディスク 1 (Hard disk 1)]** をクリックします。

3. **[ネットワークアダプタ 1 (Network adapter 1)]** 設定が次のようになっていることを確認し、必要に応じて変更します。

- a. **[デバイスのステータス (Device Status)]** の下で、**[パワーオン時に接続 (Connect at power on)]** チェックボックスを有効にします。

- b. **[MAC アドレス (MAC Address)]** の下で、仮想アプライアンスの管理インターフェイスの MAC アドレスを手動で設定します。

仮想アプライアンスに手動で MAC アドレスを割り当て、ダイナミック プール内の他のシステムによる MAC アドレスの変更または競合を回避します。

また、仮想 **Cisco Firepower Management Center** の場合、MAC アドレスを手動で設定することにより、アプライアンスの再イメージ化が必要になった場合に、Cisco からライセンスを再要求しなくて済みます。

- c. **[ネットワーク接続 (Network Connection)]** の下で、**[ネットワークラベル (Network label)]** に仮想アプライアンスの管理ネットワーク名を設定します。

4. [OK] をクリックします。

次の作業

- 仮想アプライアンスを初期化します。[仮想アプライアンスの電源投入\(14 ページ\)](#)を参照してください。
- オプションで、アプライアンスの電源を入れる前に、デフォルトの e1000 インターフェイスを vmxnet3 インターフェイスに置き換えるか、追加の管理インターフェイスを作成するか、またはその両方を実行することもできます。[VMware インターフェイスの設定\(13 ページ\)](#)を参照してください。

VMware インターフェイスの設定

仮想マシンの作成時に、VMware はデフォルトの e1000(1 Gbit/s)インターフェイスを設定しています。仮想マシンの作成が終了し、Firepower Threat Defense Virtual が完全にインストールされたら、ネットワーク スループットを向上させるために、e1000 から vmxnet3(10 Gbit/s)または ixgbe(10 Gbit/s)インターフェイスに切り替えることができます。デフォルトの e1000 インターフェイスを交換する際は、次の重要なガイドラインを考慮してください。

VMXNET3 インターフェイス

- vmxnet3 の場合、Cisco では、5 つ以上の vmxnet3 ネットワーク インターフェイスを使用する際に、VMware vCenter によって管理されるホストを使用することが推奨されます。スタンドアロン 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。ホストが VMware vCenter で管理される場合、正しい順序は設定 CD-ROM の XML から取得できます。ホストがスタンドアロン ESXi で実行している場合、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、Firepower Threat Defense Virtual に表示されている MAC アドレスを、VMware 構成ツールから表示されている MAC アドレスと手動で比較することです。
- 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。

IXGBE インターフェイス

- ixgbe の場合、ESXi プラットフォームでは ixgbe NIC が ixgbe PCI デバイスをサポートする必要があります。さらに、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 要件と構成要件があります。詳細については、Intel Technical Brief の『[How to Configure Intel® Ethernet Converged Network Adapter-Enabled Virtual Functions on VMware* ESXi* 5.1](#)』を参照してください。
- 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。
- 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) の展開をサポートしていません。

インターフェイスの置き換え

デフォルトの e1000 インターフェイスを置き換えるには、すべての e1000 インターフェイスを削除し、それを vmxnet3 または ixgbe インターフェイスに置き換えます。

展開内でインターフェイスを混在させる (仮想 Cisco 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。

仮想アプライアンスの電源投入

E1000 インターフェイスを置き換えるには、vSphere Client を使用して次の操作を行います。

- 既存の e1000 インターフェイスの削除
- 新しいインターフェイスの追加
- 適切なアダプタ タイプとネットワーク接続の選択
- 仮想アプライアンスの電源投入

また、同じ仮想 Firepower Management Center に 2 つ目の管理インターフェイスを追加して、2 つの異なるネットワーク上でトラフィックを別々に管理することもできます。2 つ目の管理インターフェイスを 2 つ目のネットワーク上の管理対象デバイスに接続するように、追加の仮想スイッチを構成します。vSphere Client を使用して、仮想アプライアンスに 2 つ目の管理インターフェイスを追加します。

(注) アプライアンスの電源を入れる前に、インターフェイスに対するすべての変更を実行します。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して、インターフェイスを削除し、新しいインターフェイスを追加してから、アプライアンスの電源をオンにします。

vSphere Client の使用に関する詳細については、VMware の Web サイト (<http://vmware.com> [英語]) を参照してください。複数の管理インターフェイスの詳細については、『Firepower Management Center Configuration Guide』の「Managing Devices」を参照してください。

インターフェイスの追加

Firepower Threat Defense Virtual 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。

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、Firepower Device Manager 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 Firepower Threat Defense Virtual 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。

Firepower Threat Defense Virtual 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。

仮想アプライアンスの電源投入

仮想アプライアンスをインストールした後、仮想アプライアンスに初めて電源を入れると初期化が自動的に開始されます。

注意: 起動時間は、サーバリソースの可用性など、さまざまな要因によって異なります。初期化が完了するまでに最大で 40 分かかることがあります。初期化は中断しないでください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

仮想アプライアンスを初期化するには、次の手順を使用します。

手順

1. アプライアンスの電源をオンにします。vSphere Client で、インベントリ リストからインポートした仮想アプライアンスの名前を右クリックし、コンテキスト メニューで [電源 (Power)] > [電源オン (Power On)] を選択します。
2. VMware コンソール タブで初期化を監視します。

次の作業

- VI OVF テンプレートを使用し、展開中に Firepower システムの必須設定を行った場合は、これ以上の設定は必要ありません。Firepower Device Manager にログインして追加のデバイス設定を実行できます。Firepower Device Manager の起動(15 ページ)を参照してください。
- ESXi OVF テンプレートを使用した場合、または VI OVF テンプレートで展開したときに Firepower システム の必須設定を行わなかった場合は、初期設定(15 ページ)に進みます。

初期設定

ネットワークで Firepower Threat Defense Virtual が正しく機能するためには、初期設定を完了する必要があります。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。

- Firepower Device Manager の Web インターフェイスを使用します(推奨)。

Firepower Device Manager はお使いの Web ブラウザで実行されます。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)。

Firepower Device Manager の代わりに CLI のセットアップ ウィザードを初期設定のために使用できます。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、およびモニタに Firepower Device Manager を使用する場合は、(オプション) Firepower Threat Defense CLI ウィザードを起動します(16 ページ)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 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

1. Firepower Threat Defense Virtual と同じサブネット上のクライアントから、ブラウザを開きます。
2. Firepower Device Manager 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 **https://192.168.45.45** になります。
3. ユーザー名 **admin** およびパスワード **Admin123** を使用してログインします。
4. 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、エンドユーザー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。
5. 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、または手動で静的 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。

初期設定

[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、または手動で静的 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

[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。

6. 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。

7. 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。

8. [終了 (Finish)] をクリックします。

次の作業

デバイスセットアップウィザードが完了したら、ポップアップに次のオプションが表示されます。

- 他のインターフェイスをネットワークに接続している場合は、[インターフェイスの設定 (Configure Interfaces)] を選択して、接続されているインターフェイスをそれぞれ設定します。
- デフォルトのアクセスルールを変更する場合は、[ポリシーの設定 (Configure Policy)] を選択して、トラフィックポリシーの設定および管理を行います。

いずれかのオプションを選択するか、またはポップアップを閉じて [デバイスダッシュボード (Device Dashboard)] に戻ることができます。

(オプション) Firepower Threat Defense CLI ウィザードを起動します

ESXi OVF テンプレートで展開している場合、CLI を使用して Firepower Threat Defense Virtual デバイスをセットアップすることができます。VI OVF テンプレートを使用して展開し、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、CLI を使用して Firepower システムで必要な設定を行うことができます。

(注) VI OVF テンプレートで展開しており、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されているため、これ以上の処理は必要ありません。

システムをセットアップするために CLI を使用する場合、デバイスのネットワーク設定、ファイアウォール モード、および管理モードのみ設定します。ただし、CLI セッションからポリシーを設定することはできません。システムの設定、管理、およびモニタに Firepower Device Manager を使用する場合は、[Firepower Device Manager の起動 \(15 ページ\)](#) を参照してください。

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。

手順

1. VMware コンソールを開きます。
2. [firepower ログイン (firepower login)] プロンプトで、ユーザー名 **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。
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)

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。

5. プロンプトに従ってシステム設定を行います。

VMware コンソールには、設定が実装されるときにメッセージが表示されることがあります。完了したら、このデバイスを **Cisco Firepower Management Center** に登録するよう要求され、CLI プロンプトが表示されます。

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 Firepower Threat Defense Virtual を正常に登録するには、Firepower Threat Defense Virtual 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。

次の作業

Firepower Device Manager を使用して、システムを設定、管理、およびモニタします。ブラウザで設定可能な機能を、CLI で設定することはできません。セキュリティ ポリシーを実装するには、**Web** インターフェイスを使用する必要があります。

Firepower Device Manager のデバイスを構成する方法

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。
- 内部の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

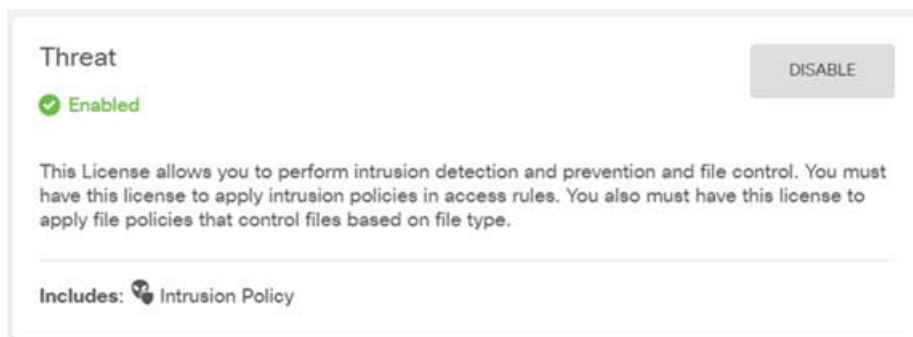
1. [デバイス (Device)] を選択してから、[スマート ライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。

Firepower Threat Defense Virtual 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。

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 [有効にする (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。



2. Firepower Threat Defense Virtual のデフォルト設定では、Management0/0 および GigabitEthernet0/1 (内部) 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。[デバイス (Device)] を選択し、[インターフェイス (Interface)] グループ内で [設定の表示 (View Configuration)] をクリックして、追加のインターフェイスを設定します。

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。

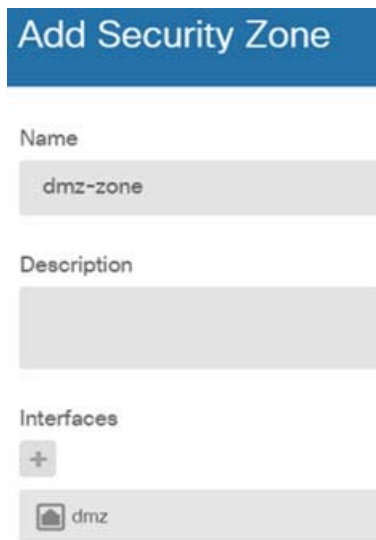
(注) また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに Management0/0 を接続するオプションもあります。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

管理インターフェイスの IP 設定は、[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)] で定義されている点に注意してください。[デバイス (Device)] > [インターフェイス (Interfaces)] > [設定の表示 (View Configuration)] に一覧されている Management0/0 (診断) インターフェイスの IP アドレスと同じではありません。

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)] を選択してから、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。



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。

Firepower Device Manager のデバイスを構成する方法

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

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 [最初の静的ルートを作成 (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。

Add Static Route

Protocol
 IPv4 IPv6

Gateway
isp-gateway

Interface
outside

Metric
1

Networks
+
any-ipv4

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。

The screenshot shows the 'Add Access Rule' configuration interface. At the top, the rule name is 'Inside_DMZ' and the action is 'Allow'. Below this, there are several tabs: 'Source/Destination', 'Applications', 'URLs', 'Users', 'Intrusion Policy', 'File policy', and 'Logging'. The 'Source/Destination' tab is active, showing a table with columns for 'SOURCE' and 'DESTINATION'. Under 'SOURCE', there is a row for 'Zones' with 'inside_zone' selected. Under 'DESTINATION', there is a row for 'Zones' with 'dmz-zone' selected. Both 'inside_zone' and 'dmz-zone' have a lock icon next to them. The 'Networks' and 'Ports/Protocols' columns are set to 'ANY'.

SR-IOV インターフェイスのプロビジョニング

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。

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。

次の作業

- Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理に関する完全な情報については、『[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。

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せん。
- 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。

注意事項と制約事項

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 Virtual と SR-IOV に関する [システム要件 \(4 ページ\)](#) 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 Virtual 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 Firepower Threat Defense Virtual 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) Firepower Threat Defense Virtual 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。

Firepower Threat Defense Virtual 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

VMware に SR-IOV インターフェイスを備えた Firepower Threat Defense Virtual 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 [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、仮想化サポートの確認手段をいくつか提供しています。

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

- 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。
- 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。
- 次のコマンドを実行します。

```
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。

次に例を示します。

```
~ # 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。

次の作業

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。

SR-IOV インターフェイスのプロビジョニング

はじめる前に

- 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。[SR-IOV のサポート \(5 ページ\)](#) を参照してください。

手順

1. vSphere Web Client で、SR-IOV を有効にする ESXi ホストに移動します。
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。
3. 物理アダプタを選択し、[Edit adapter settings] をクリックします。
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。
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。
6. [OK] をクリックします。
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。

次の作業

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

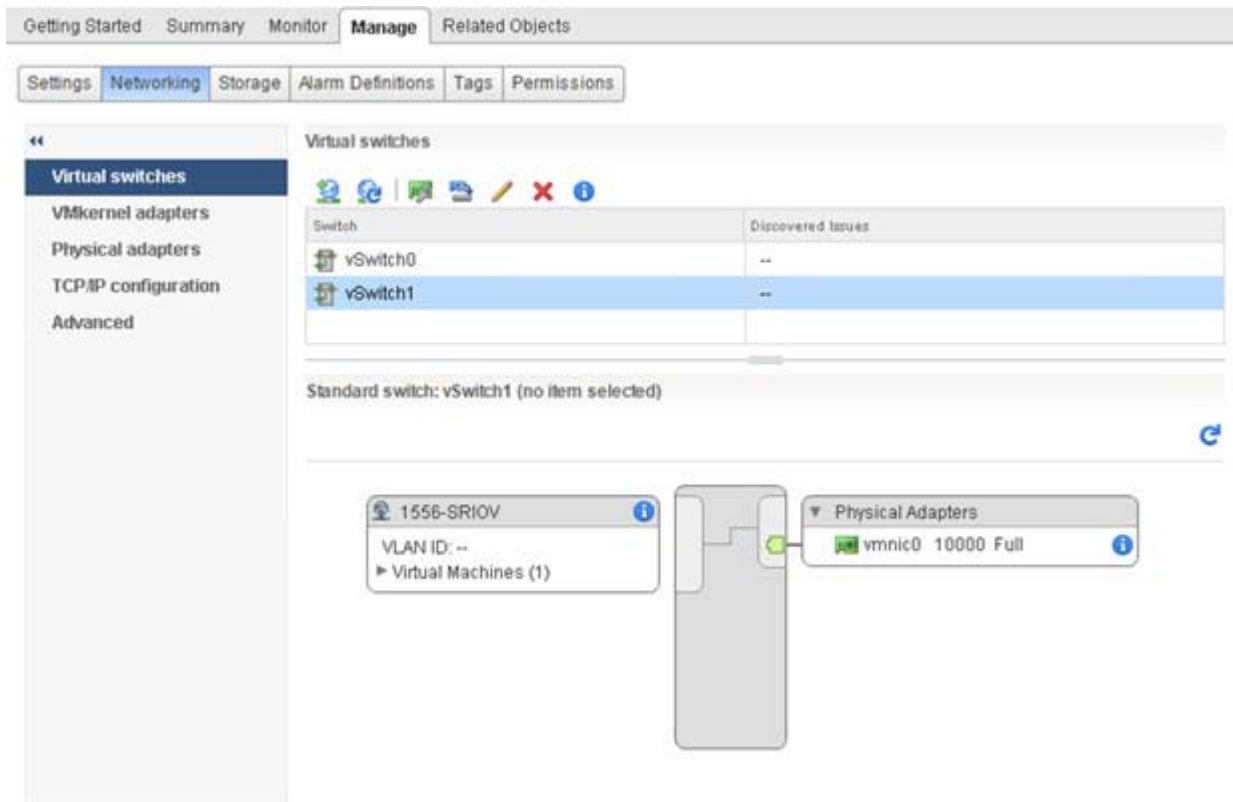
vSphere スイッチの作成

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

1. vSphere Web Client で、ESXi ホストに移動します。
2. [Manage] で、[Networking] を選択してから、[Virtual switches] を選択します。
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。
4. [Virtual Machine Port Group for a Standard Switch] 接続タイプを選択して、[Next] をクリックします。
5. [New standard switch] を選択して、[Next] をクリックします。
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。
 - a. 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。
 - b. 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。
 - c. [Failover order group] ドロップダウン メニューで、[Active adapters] から選択します。
 - d. [OK] をクリックします。
7. SR-IOV vSwitch の [Network label] を入力して、[Next] をクリックします。
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 1 SR-IOV インターフェイスがアタッチされた新しい vSwitch



次の作業

- 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。Firepower Threat Defense Virtual 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 Firepower Threat Defense Virtual に公開されます。この手順では、Firepower Threat Defense Virtual 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

1. vSphere Web Client から vCenter Server にログインします。
2. 変更する Firepower Threat Defense Virtual VM 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、[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 Firepower Threat Defense Virtual VM を選択します。
3. 選択した仮想マシンの電源をオフにします。

SR-IOV インターフェイスのプロビジョニング

4. Firepower Threat Defense Virtual 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。
5. [Yes] をクリックして、アップグレードを確認します。
6. 互換性を持たせる仮想マシンの [ESXi 5.5 and later] オプションを選択します。
7. (オプション)[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 [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 [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。

次の作業

SR-IOV パススルー ネットワーク アダプタを介して Firepower Threat Defense Virtual 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

Firepower Threat Defense Virtual VM と物理 NIC がデータを交換可能なことを保証するには、Firepower Threat Defense Virtual 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 Firepower Threat Defense Virtual VM に割り当てる方法について説明します。

手順

1. vSphere Web Client から vCenter Server にログインします。
2. 変更する Firepower Threat Defense Virtual VM 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、[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 Firepower Threat Defense Virtual VM を選択します。
3. 仮想マシンの [Manage] タブで、[Settings] > [VM Hardware] を選択します。
4. [Edit] をクリックして、[Virtual Hardware] タブを選択します。
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。
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。
7. [Adapter Type] ドロップダウン メニューで、[SR-IOV passthrough] を選択します。
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。
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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 - 2018 Cisco Systems, Inc. All rights reserved.