Firepower Device Manager を使用して KVM 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 **6.2.3** 以降

初版:2018 年 3 月 29 日

最終更新日:2018 年 12 月 12 日

カーネルベース仮想マシン(KVM)ハイパーバイザを使用して、Firepower Device Manager を備えた Firepower Threat Defense Virtual を導入できます。

KVM を使用した導入について

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

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

KVM 上の Firepower Threat Defense Virtual は次をサポートします。

- プロセッサ
  - 4 個の vCPU が必要
- メモリ
  - 8 GB RAM が必要

- ネットワーキング
  - ブートするには 2 つの管理インターフェイスと 2 つのデータ インターフェイスが必要

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

  - virtio ドライバをサポート
  - SR-IOV の ixgbe-vf ドライバをサポート
  - 合計 10 個のインターフェイスをサポート
- 仮想マシンあたりのホスト ストレージ
  - Firepower Threat Defense Virtual には 50 GB 必要
  - virtio ブロック デバイスをサポート
- コンソール
  - Telnet を介したターミナル サーバをサポート

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。KVM の場合は、SR-IOV サポートの CPU の互換性を確認できます。KVM 上の Firepower Threat Defense Virtual では、x86 ハードウェアしかサポートされないことに注意してください。

注意事項と制約事項

- Firepower Threat Defense Virtual のデフォルト設定では、管理インターフェイス(管理と診断)および内部インターフェイスが**同じサブネット**上にあり、管理アドレスはインターネットへのゲートウェイとして内部アドレスを使用すると仮定します(外部インターフェイス経由)。
- 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。**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。

- KVM 上の Firepower Threat Defense Virtual では、合計で 10 個のインターフェイスをサポートします(管理インターフェイス X 1 個、診断インターフェイス X 1 個、データ トラフィック用ネットワーク インターフェイス X 最大 8 個)。ネットワークへのインターフェイスの割り当ては、次の順番である必要があります。
  - 1. 管理インターフェイス(必須)
  - 2. 診断インターフェイス(必須)
  - 3. 外部インターフェイス(必須)
  - 4. 内部インターフェイス(必須)
  - 5 ～ 10. データ インターフェイス(オプション)

  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 1　送信元から宛先ネットワークへのマッピング

ネットワーク アダプタ	送信元ネットワーク	宛先ネットワーク	機能
vnic0[1]	Management0-0	Management0/0	管理
vnic1[1]	Diagnostic	Diagnostic	診断
vnic2	GigabitEthernet0-0	GigabitEthernet0/0	外部データ
vnic3[1]	GigabitEthernet0-1	GigabitEthernet0/1	内部トラフィック

1. 同じサブネットに接続します。

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

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

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

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

  (注)Cisco.com のログインおよびシスコ サービス契約が必要です。
- Firepower Device Manager を使用するには、新しいイメージ(バージョン 6.2.3 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古い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。

- このマニュアルの導入例では、ユーザが Ubuntu 14.04 LTS を使用していることを前提としています。Ubuntu 14.04 LTS ホストの最上部に次のパッケージをインストールします。
  - qemu-kvm
  - libvirt bin
  - bridge-utils
  - Virt-Manager
  - virtinst
  - virsh（通常、このコマンドライン インターフェイスは libvirt bin パッケージの一部）
  - genisoimage
- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での Firepower Threat Defense Virtual のスループットを最大化できます。一般的なホスト調整の概念については、「Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture.」を参照してください。
- 以下の機能は Ubuntu 14.04 LTS の最適化に役立ちます。
  - macvtap：高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。

    (注) ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
  - Transparent Huge Pages：メモリ ページ サイズを増加させます。Ubuntu 14.04 では、デフォルトでオンになっています。
  - Hyperthread disabled：2 つの vCPU を 1 つのシングル コアに削減します。
  - txqueuelength：デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップ レートを低減します。
  - pinning：qemu および vhost プロセスを特定の CPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。
- RHEL ベースのディストリビューションの最適化については、『Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide』を参照してください。
- KVM と Firepower System の互換性については、「Cisco Firepower Threat Defense Virtual Compatibility」を参照してください。

ライセンス要件

Firepower Threat Defense デバイスや Firepower Threat Defense Virtual を購入すると、自動的に基本ライセンスが含まれます。すべての追加ライセンス（Threat、Malware、URL Filtering）はオプションです。Firepower Threat Defense のライセンスに関する詳細については、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Licensing the System」の章を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

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

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

第 0 日のコンフィギュレーション ファイルを使用して展開する場合、プロセスで、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。

- EULA への同意
- システムのホスト名
- 管理者アカウントの新しい管理者パスワード
- 初期ファイアウォール モード
- 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
- 管理 Cisco Firepower Management Center

第 0 日のコンフィギュレーション ファイルを使用せずに展開する場合は、起動後に Firepower システム の必須設定を指定する必要があります。詳細については、第 0 日のコンフィギュレーション ファイルを使用しない起動（12 ページ）を参照してください。

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

手順

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

   例:

   ```
   #Firepower Threat Defense on KVM
   {
       "EULA": "accept",
       "Hostname": "ftdv-kvm-production",
       "AdminPassword": "Admin123",
       "FirewallMode": "routed",
       "DNS1": "1.1.1.1",
       "DNS2": "1.1.1.2",
       "DNS3": "",
       "IPv4Mode": "manual",
       "IPv4Addr": "10.12.129.44",
       "IPv4Mask": "255.255.0.0",
       "IPv4Gw": "10.12.0.1",
       "IPv6Mode": "disabled",
       "IPv6Addr": "",
       "IPv6Mask": "",
       "IPv6Gw": "",
       "FmcIp": "",
       "FmcRegKey": "",
       "FmcNatId": "",
       "ManageLocally":"Yes"
   }
   ```

   (注) 第 0 日のコンフィギュレーション ファイル内で [ローカルに管理（ManageLocally）] に対して [はい（Yes）] と入力し、Firepower Management Center のフィールド（**FmcIp**、**FmcRegKey**、および **FmcNatId**）を空欄のままにします。

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

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

   または

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

3. 手順を繰り返して、導入する Firepower Threat Defense Virtual ごとに一意のデフォルト設定ファイルを作成します。

次の作業

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

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

- virt-manager を使用している場合、virt-manager の GUI を使用して仮想 CD-ROM を作成できます。Virtual Machine Manager を使用した起動（7 ページ）を参照してください。

Firepower Threat Defense Virtual の起動

導入スクリプトを使用した起動

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

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

各 KVM ゲスト ディスク インターフェイスで、指定されたいずれかのキャッシュ モード（*writethrough*、*writeback*、*none*、*directsync*、または *unsafe*）を指定できます。*writethrough* は読み取りキャッシングを提供します。*writeback* は読み取りと書き込みキャッシングを提供します。*directsync* はホスト ページ キャッシュをバイパスします。*unsafe* はすべてのコンテンツをキャッシュし、ゲストからのフラッシュ要求を無視できます。

キャッシュ モードのガイドライン

- *cache=writethrough* は、ホストで突然の停電が発生した場合の KVM ゲスト マシン上のファイル破損を低減できます。*writethrough* モードの使用をお勧めします。
- ただし、*cache=writethrough* は、*cache=none* よりディスク I/O 書き込みが多いため、ディスク パフォーマンスに影響する可能性もあります。
- *--disk* オプションの *cache* パラメータを削除する場合、デフォルトは *writethrough* になります。
- キャッシュ オプションを指定しないと、VM を作成するために必要な時間も大幅に短縮される場合もあります。これは、古い RAID コントローラにはディスク キャッシング能力が低いものがあることが原因です。そのため、ディスク キャッシングを無効にして（ *ache=none*）、*writethrough* をデフォルトに設定すると、データの整合性を確保できます。

手順

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

   Firepower Threat Defense Virtual VM の名前は、この KVM ホスト上の他の仮想マシン（VM）全体において一意であることが必要です。

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

   - 1. 管理インターフェイス（必須）
   - 2. 診断インターフェイス（必須）
   - 3. 外部インターフェイス（必須）
   - 4. 内部インターフェイス（必須）
   - 5 ～ 10. データ インターフェイス（オプション）

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=4 \
   --ram=8192 \
   --os-type=linux \
   --os-variant=virtio26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset \
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,
     cache=writethrough \
   --disk path=<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
   --force
```

2. virt_install スクリプトを実行します。

```
/usr/bin/virt_install_ftdv.sh

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

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

次の作業

- Firepower Device Manage 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（13 ページ）を参照してください。

Virtual Machine Manager を使用した起動

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

1. virt-manager を起動します（[アプリケーション（Applications）] > [システムツール（System Tools）] > [Virtual Machine Manager]）。

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

2. 左上隅のボタンをクリックし、[VM の新規作成（New VM）] ウィザードを開きます。
3. 仮想マシンの詳細を入力します。
   a. [名前（Name）] を指定します。
   b. オペレーティング システムの場合、[既存のディスクイメージをインポート（Import existing disk image）] を選択します。

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

   c. [次へ（Forward）] をクリックして続行します。

4. ディスク イメージをロードします。
   a. [参照...(Browse...)] をクリックしてイメージ ファイルを選択します。
   b. [OS タイプ(OS type)] に [Linux] を選択します。
   c. [バージョン(Version)] に [virtio を含む汎用 2.6.25 以降のカーネル(Generic 2.6.25 or later kernel with virtio)] を選択します 。
   d. [次へ(Forward)] をクリックして続行します。
5. メモリおよび CPU オプションを設定します。
   a. [メモリ(RAM)(Memory (RAM))] を *8192* に設定します。
   b. [CPU(CPUs)] を *4* に設定します。
   c. [次へ(Forward)] をクリックして続行します。
6. [完了(Finish)] をクリックする前に [インストール前に設定をカスタマイズする(Customize configuration before install)] ボックスをオンにします。

   この操作を行うと、別のウィザードが開き、仮想マシンのハードウェア設定を追加、削除、設定することができます。
7. CPU 構成を次のように変更します。

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

   これによって、物理ホストの CPU モデルと設定が仮想マシンに適用されます。
8. 仮想ディスクを設定します。
   a. 左側のパネルから [ディスク 1(Disk 1)] を選択します。
   b. [詳細オプション(Advanced Options)] をクリックします。
   c. [ディスクバス(Disk bus)] を [Virtio] に設定します。
   d. [ストレージ形式(Storage format)] を [qcow2] に設定します。
9. シリアル コンソールを設定します。
   a. 左側のパネルから [コンソール(Console)] を選択します。
   b. [削除(Remove)] を選択してデフォルト コンソールを削除します。
   c. [ハードウェアを追加(Add Hardware)] をクリックしてシリアル デバイスを追加します。
   d. [デバイスタイプ(Device Type)] で、[TCP net console (tcp)(TCP net console (tcp)] を選択します。
   e. [モード(Mode)] で、[サーバモード(バインド)(Server mode (bind))] を選択します。
   f. [ホスト(Host)] には IP アドレスとポート 番号を入力します。
   g. [Telnet を使用(Use Telnet)] ボックスをオンにします。
   h. デバイス パラメータを設定します。
10. KVM ゲストがハングまたはクラッシュしたときに何らかのアクションが自動でトリガーされるようウォッチドッグ デバイスを設定します。
    a. [ハードウェアを追加(Add Hardware)] をクリックしてウォッチドック デバイスを追加します。
    b. [モデル(Model)] で、[デフォルト(default)] を選択します。
    c. [アクション(Action)] で、[ゲストを強制的にリセット(Forcefully reset the guest)] を選択します。

11. 少なくとも 4 つの仮想ネットワーク インターフェイスを設定します。
    a. [ハードウェアを追加(Add Hardware)] をクリックしてインターフェイスを追加します。
    b. [送信元デバイス(Source device)] で、[macvtap] を選択します。
    c. [デバイスモデル(Device model)] で、[virtio] を選択します。
    d. [送信元モード(Source mode)] で、[ブリッジ(Bridge)] を選択します。

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

    – vnic0:管理インターフェイス(必須)
    – vnic1:診断インターフェイス(必須)
    – vnic2:外部インターフェイス(必須)
    – vnic3:内部インターフェイス(必須)
    – vnic4-9:データ インターフェイス(オプション)

    (注) vnic0、vnic1、および vnic3 は、必ず同じサブネットにマップするようにしてください。
12. 第 0 日のコンフィギュレーション ファイルを使用して展開する場合、ISO の仮想 CD-ROM を作成します。
    a. [ハードウェアを追加(Add Hardware)] をクリックします。
    b. [ストレージ(Storage)] を選択します。
    c. [管理対象またはその他既存のストレージを選択(Select managed or other existing storage)] をクリックし、ISO ファイルの場所を参照します。
    d. [デバイスタイプ(Device type)] で、[IDE CDROM] を選択します。
13. 仮想マシンのハードウェアを設定した後、[適用(Apply)] をクリックします。
14. virt-manager の [インストールの開始(Begin installation)] をクリックして、指定したハードウェア設定で仮想マシンを作成します。

次の作業

- Firepower Device Manage 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(13 ページ)を参照してください。

OpenStack を使用した起動

OpenStack 環境に Firepower Threat Defense Virtual を展開できます。OpenStack は、パブリック クラウドとプライベート クラウドの、クラウド コンピューティング プラットフォームを構築および管理するための一連のソフトウェア ツールで、KVM ハイパーバイザと緊密に統合されています。

(注) OpenStack 環境に Firepower Threat Defense Virtual を導入する場合は、無差別モードで実行し、ポート セキュリティ(パケット フィルタリング)を無効にする必要があります。この操作を行うときに、セキュリティ グループまたは許可されたアドレス ペアがインターフェイスに割り当てられていると、ポート セキュリティを無効にできないことに注意してください。ポート レベルのセキュリティを無効にすると、すべてのトラフィック(イングレスとイーグレス)が許可されます。

OpenStack での 第 0 日のコンフィギュレーション ファイルについて

OpenStack では、ブート時にインスタンスに接続される特殊な設定ドライブ（config-drive）を使った設定データの提供をサポートしています。第 0 日のコンフィギュレーション ファイルを含む Firepower Threat Defense Virtual インスタンスを nova boot コマンドを使用して展開するには、次の行を含めます。

```
--config-drive true --file day0-config=/home/user/day0-config \
```

--config-drive コマンドが有効な場合、nova クライアントが呼び出される Linux ファイルシステムにあるファイル *=/home/user/day0-config* が仮想 CDROM の仮想マシンに渡されます。

（注）VM はこのファイルを *day0-config* という名前で認識しますが、OpenStack では通常このファイルの内容を /openstack/content/xxxx として保存します。この xxxx は、割り当てられた 4 桁の数字（/openstack/content/0000 など）です。これは、OpenStack ディストリビューションによって異なる場合があります。

コマンドラインを使用した起動

nova boot コマンドを使用して Firepower Threat Defense Virtual インスタンスを作成およびブートします。

手順

1. イメージ、フレーバー、インターフェイス、および第 0 日の設定情報を使用して Firepower Threat Defense Virtual インスタンスをブートします。

   Firepower Threat Defense Virtual は最大 10 個のネットワーク インターフェイスをサポートできます。この例では、4 つのインターフェイスを使用しています。

   （注）Firepower Threat Defense Virtual のデフォルト設定では、管理インターフェイス、診断インターフェイス、および内部インターフェイスは同じサブネットに配置されます。システムでは、少なくとも 4 つのインターフェイス（管理インターフェイス、診断インターフェイス、外部インターフェイス、内部インターフェイス）が正常に起動する必要があります。

```
local@maas:~$ nova boot \
  --image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \
  --flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \
  --nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \
  --nic net-id=ae638375-d0d1-4f1e-a93d-6e621e5fabd2 \
  --nic net-id=e9cedefd-178e-41a8-9c47-4e1feaa48477
  --nic net-id=f8b8dd2d-c8cc-452e-98f3-9542dddc7965 \
  --config-drive true --file day0-config=/home/local/day0-config \
```

OpenStack ダッシュボードを使用した起動

Horizon は、OpenStack のダッシュボードであり、Nova、Swift、Keystone などの OpenStack サービスへの Web ベース ユーザ インターフェイスを提供します。

はじめる前に

- Cisco.com から Firepower Threat Defense Virtual qcow2 ファイルをダウンロードし、ローカル MAAS サーバに格納します。

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

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

手順

1. [Log In] ページで、ユーザ名とパスワードを入力し、[Sign In] をクリックします。

   ダッシュボードに表示されるタグと機能は、ログインしているユーザのアクセス権限(権限)によって異なります。

2. メニューから [Admin] > [System Panel] > [Flavor] を選択します。

   仮想ハードウェアのテンプレートは OpenStack でフレーバーと呼ばれ、RAM、ディスクのサイズ、コア数を定義します。この手順では、Firepower 導入用のフレーバーを作成します。

3. [Flavor Info] ウィンドウに必要な情報を入力します。

   a. [名前(Name)]:インスタンスを簡単に識別するわかりやすい名前を入力します。たとえば、FTD-FMC-4vCPU-8GB とします。

   b. [VCPUs]:[VCPUs] を 4 に設定します。

   c. [RAM MB]:RAM を 8192 に設定します。

4. [Create Flavor] を選択します。

5. メニューから [Admin] > [System Panel] > [Images] を選択します。

6. [Create An Image] ウィンドウに必要な情報を入力します。

   a. [Name]:イメージを簡単に識別する名前を入力します。たとえば、FTD-Version-Build とします。

   b. [Description]:(オプション)イメージ ファイルの説明を入力します。

   c. [Browse]:前に Cisco.com からダウンロードした Firepower Threat Defense Virtual qcow2 ファイルを選択します。

   d. [Format]:形式タイプとして [QCOW2-QEMU Emulator] を選択します。

   e. [Public] ボックスをオンにします。

7. [Create Image] を選択します。

   新しく作成されたイメージを表示します。

8. メニューから [Project] > [Compute] > [Instances] を選択します。

9. [Launch Instance] をクリックします。

10. [Launch Instance] > [Details] タブに必要な情報を入力します。

    a. [Instance Name]:インスタンスを簡単に識別する名前を入力します。たとえば、FTD-Version-Build とします。

    b. [Flavor]:手順 3. で前に作成したフレーバーを選択します。このイメージ ファイルの説明を入力します。

    c. [Instance Boot Source]:[Boot from image] を選択します。

    d. [Image Name]:手順 6. で作成したイメージを選択します。

11. [Launch Instance] > [Networking] タブから、Firepower Threat Defense Virtual インスタンスの管理ネットワークとデータ ネットワークを選択します。

    (注)Firepower Threat Defense Virtual を起動するには、少なくとも 4 つのインターフェイス(2 つの管理インターフェイスと 2 つのトラフィック インターフェイス)が必要です。

12. [作成(Launch)] をクリックします。

    インスタンスはクラウド内のコンピューティング ノードから開始します。[インスタンス(Instances)] ウィンドウから新しく作成したインスタンスを表示します。

13. Firepower Threat Defense Virtual インスタンスを選択します。
14. [コンソール(Console)] タブを選択します。
15. コンソールで仮想アプライアンスにログインします。

次の作業

- Firepower Device Manage 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(13 ページ)を参照してください。

第 0 日のコンフィギュレーション ファイルを使用しない起動

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

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

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

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

手順

1. Firepower Threat Defense Virtual で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が求められます。
   - 使用許諾契約の同意
   - 新しい管理者パスワード
   - IPv4 または IPv6 の構成
   - IPv4 または IPv6 の DHCP 設定
   - 管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
   - システム名
   - デフォルト ゲートウェイ
   - DNS セットアップ
   - HTTP プロキシ
   - 管理モード(ローカル管理が必要)
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。
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。
7. CLI を閉じます。

```
> exit
```

次の作業

- Firepower Device Manage 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（13 ページ）を参照してください。

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、管理インターフェイス、診断インターフェイス、および内部インターフェイスを、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。

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 アドレスとその他の設定を定義します。完了したら [保存(Save)] をクリックします。

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には常にゾーン オブジェクトを編集する必要があります。

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

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。

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。

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

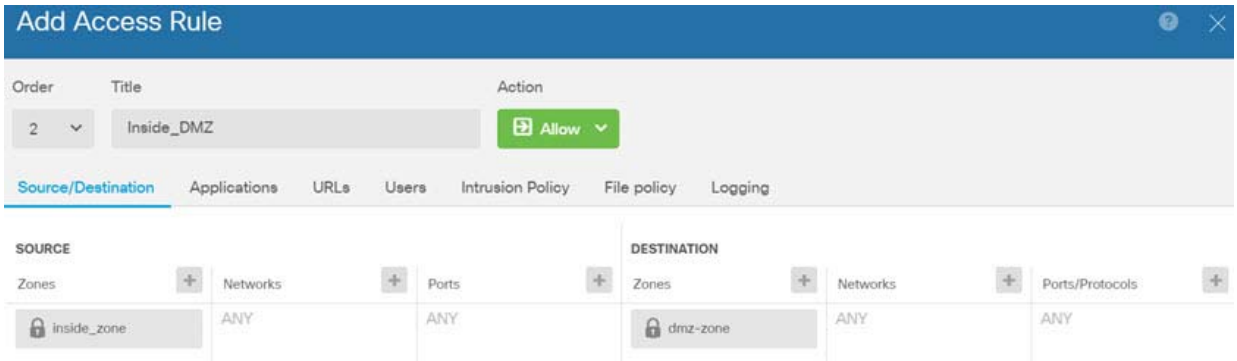
デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間のトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーン オブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

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

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

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

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



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。

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

SR-IOV をサポートする物理 NIC があれば、SR-IOV 対応 VF または仮想 NIC(vNIC)を ASAv インスタンスにアタッチできます。SR-IOV は、BIOS だけでなく、ハードウェア上で実行しているオペレーティング システム インスタンスまたはハイパーバイザでのサポートも必要です。KVM 環境で実行中の ASAv 用の SR-IOV インターフェイスのプロビジョニングに関する一般的なガイドラインのリストを以下に示します。

- ホスト サーバには SR-IOV 対応物理 NIC が必要です。SR-IOV のサポート(2 ページ)を参照してください。
- ホスト サーバの BIOS で仮想化が有効になっている必要があります。詳細については、ベンダーのマニュアルを参照してください。
- ホスト サーバの BIOS で IOMMU グローバル サポートが SR-IOV に対して有効になっている必要があります。詳細については、ベンダーのマニュアルを参照してください。

KVM ホスト BIOS とホスト OS の変更

このセクションでは、KVM 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、Intel Ethernet Server Adapter X520 - DA2 を使用した Cisco UCS C シリーズ サーバ上の Ubuntu 14.04 を使用して、特定のラボ環境内のデバイスから作成されたものです。

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)が取り付けられていることを確認します。
- Intel 仮想化テクノロジー(VT-x)機能と VT-d 機能が有効になっていることを確認します。

  (注)システム メーカーによっては、これらの拡張機能がデフォルトで無効になっている場合があります。システムごとに BIOS 設定にアクセスして変更する方法が異なるため、ベンダーのマニュアルでプロセスを確認することをお勧めします。
- オペレーティング システムのインストール中に、Linux KVM モジュール、ライブラリ、ユーザ ツール、およびユーティリティのすべてがインストールされていることを確認します。Firepower Threat Defense Virtual、Firepower Device Manager、および KVM の前提条件(3 ページ)を参照してください。
- 物理インターフェイスが稼働状態であることを確認します。**ifconfig *<ethname>*** を使用して確認します。

手順

1. " root" ユーザ アカウントとパスワードを使用してシステムにログインします。
2. Intel VT-d が有効になっていることを確認します。

   次に例を示します。

   ```
   kvmuser@kvm-host:/$ dmesg | grep -e DMAR -e IOMMU
   [    0.000000] ACPI: DMAR 0x000000006F9A4C68 000140 (v01 Cisco0 CiscoUCS 00000001 INTL 20091013)
   [    0.000000] DMAR: IOMMU enabled
   ```

   最後の行は、VT-d が有効になっていることを示しています。
3. */etc/default/grub* 設定ファイル内の *GRUB_CMDLINE_LINUX* エントリに ***intel_iommu=on*** パラメータを付加することによって、カーネル内の Intel VT-d をアクティブにします。

   次に例を示します。

   ```
   # vi /etc/default/grub
   ...
   GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on"
   ...
   ```

   (注)AMD プロセッサを使用している場合は、代わりに、***amd_iommu=on*** をブート パラメータに付加する必要があります。
4. iommu の変更を有効にするためにサーバをリブートします。

   次に例を示します。

   ```
   > shutdown -r now
   ```
5. 次の形式を使用して sysfs インターフェイス経由で *sriov_numvfs* パラメータに適切な値を書き込むことによって VF を作成します。

   ```
   #echo n > /sys/class/net/device name/device/sriov_numvfs
   ```

   サーバの電源を入れ直すたびに必要な数の VF が作成されることを保証するには、*/etc/rc.d/* ディレクトリに配置されている **rc.local** ファイルに上記コマンドを付加します。Linux OS は、ブート プロセスの最後で rc.local スクリプトを実行します。

   たとえば、ポートあたり 1 つの VF を作成するケースを以下に示します。お使いのセットアップではインターフェイスが異なる可能性があります。

```
echo '1' > /sys/class/net/eth4/device/sriov_numvfs
echo '1' > /sys/class/net/eth5/device/sriov_numvfs
echo '1' > /sys/class/net/eth6/device/sriov_numvfs
echo '1' > /sys/class/net/eth7/device/sriov_numvfs
```

6. サーバをリブートします。

   次に例を示します。

```
> shutdown -r now
```

7. ***lspci*** を使用して、VF が作成されたことを確認します。

   次に例を示します。

```
 > lspci | grep -i "Virtual Function"
kvmuser@kvm-racetrack:~$ lspci | grep -i "Virtual Function"
0a:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.2 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.3 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

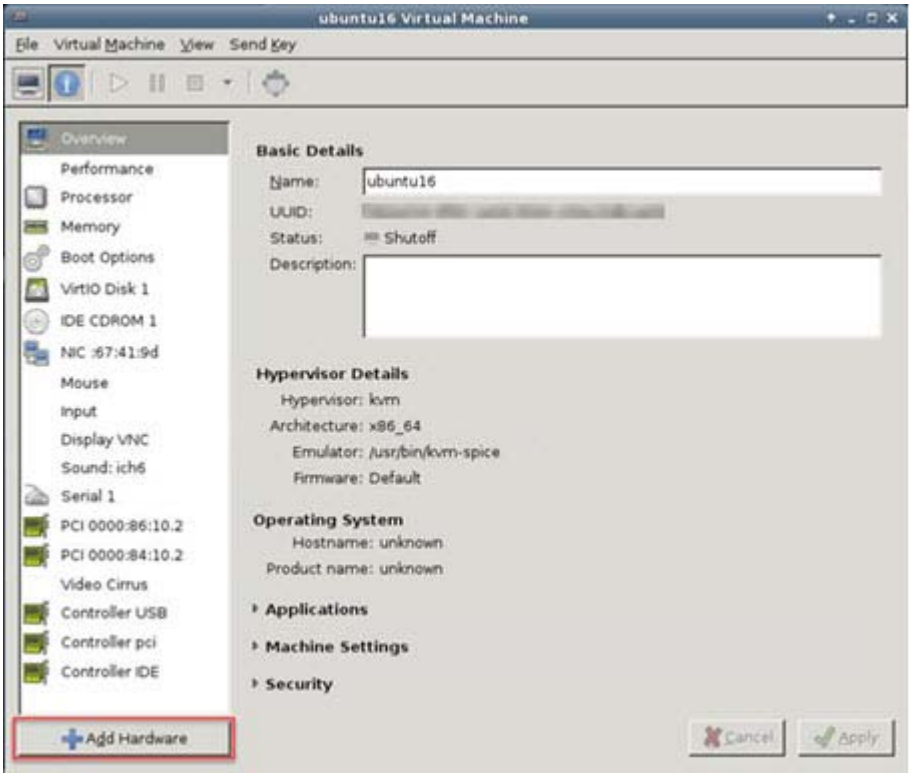
   (注) **ifconfig** コマンドを使用して、新しいインターフェイスを表示します。

Firepower Threat Defense Virtual への PCI デバイスの割り当て

VF を作成したら、PCI デバイスを追加するのと同様に、VF を Firepower Threat Defense Virtual に追加できます。次の例では、グラフィカル **virt-manager** ツールを使用して、イーサネット VF コントローラを Firepower Threat Defense Virtual に追加する方法について説明します。

1. Firepower Threat Defense Virtual を開いて、[Add Hardware] ボタンをクリックし、新しいデバイスを仮想マシンに追加します。

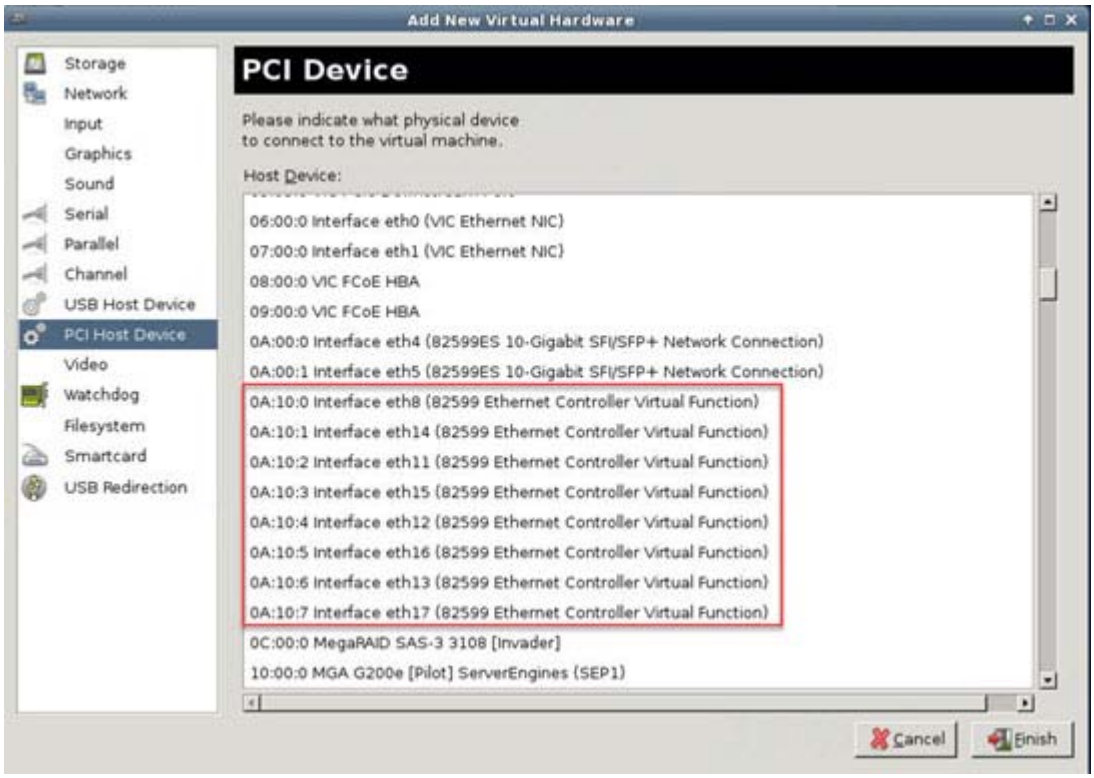
図 1　ハードウェアの追加



2. 左ペインの [Hardware] リストで [PCI Host Device] をクリックします。

   VF を含む PCI デバイスのリストが中央ペインに表示されます。

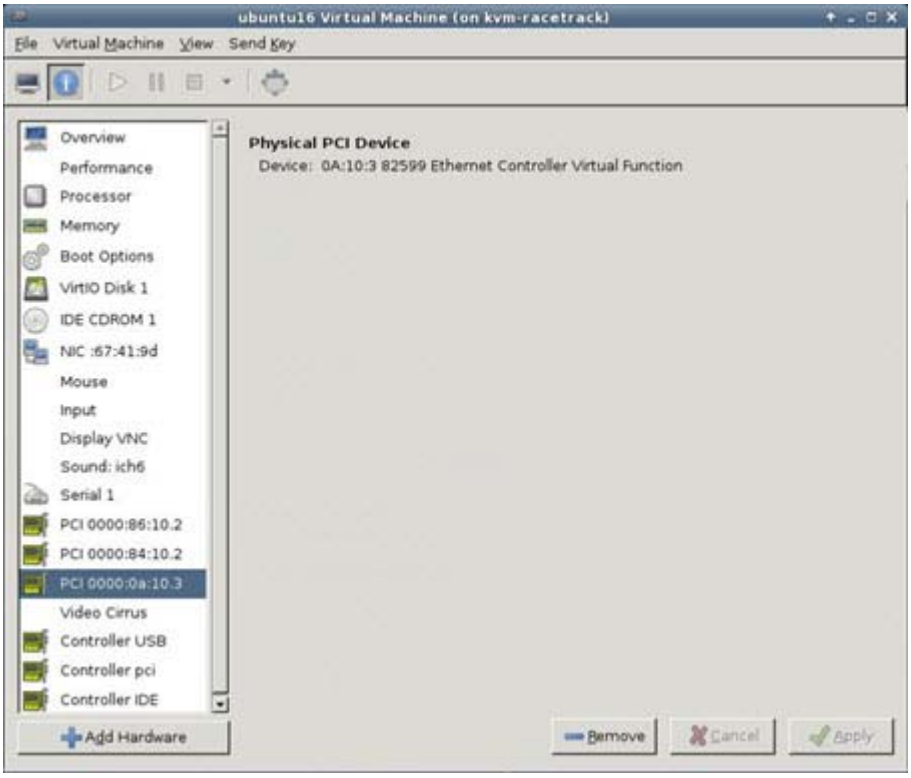
図 2　仮想機能のリスト



3. 使用可能な仮想機能のいずれかを選択して、[Finish] をクリックします。

   PCI デバイスがハードウェア リストに表示されます。デバイスの記述が Ethernet Controller Virtual Function になっていることに注意してください。

図 3　追加された仮想機能



次の作業

- Firepower Threat Defense Virtual コマンド ラインから、**show interface** コマンドを使用して、新しく設定したインターフェイスを確認します。
- Firepower Device Manager を使用したインターフェイスの設定、およびその他のインターフェイス管理の概念については、『Firepower Device Manager コンフィギュレーション ガイド』を参照してください。