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

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	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 デバイスに組み込まれている Web ベースの設定インターフェイスです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

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

Firepower Management Center

Cisco Firepower Management Center（FMC）。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの FDM の代わりに FMC を使用してデバイスを設定します。

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

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

システム要件

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

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	**バージョン 6.4 以降** 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。 • 4 vCPU/8 GB（デフォルト） • 8 vCPU/16 GB • 12 vCPU/24 GB （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。
	バージョン 6.3 以前 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。 • 4 vCPU/8 GB 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。 （注） vCPU とメモリの調整はサポートされていません。
ストレージ	ディスク形式の選択に基づきます。 • 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	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。 • **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。 **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。 • **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。

- VI OVF テンプレート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」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 Respawning 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 devide）] 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て済みます。

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に依存します。

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。

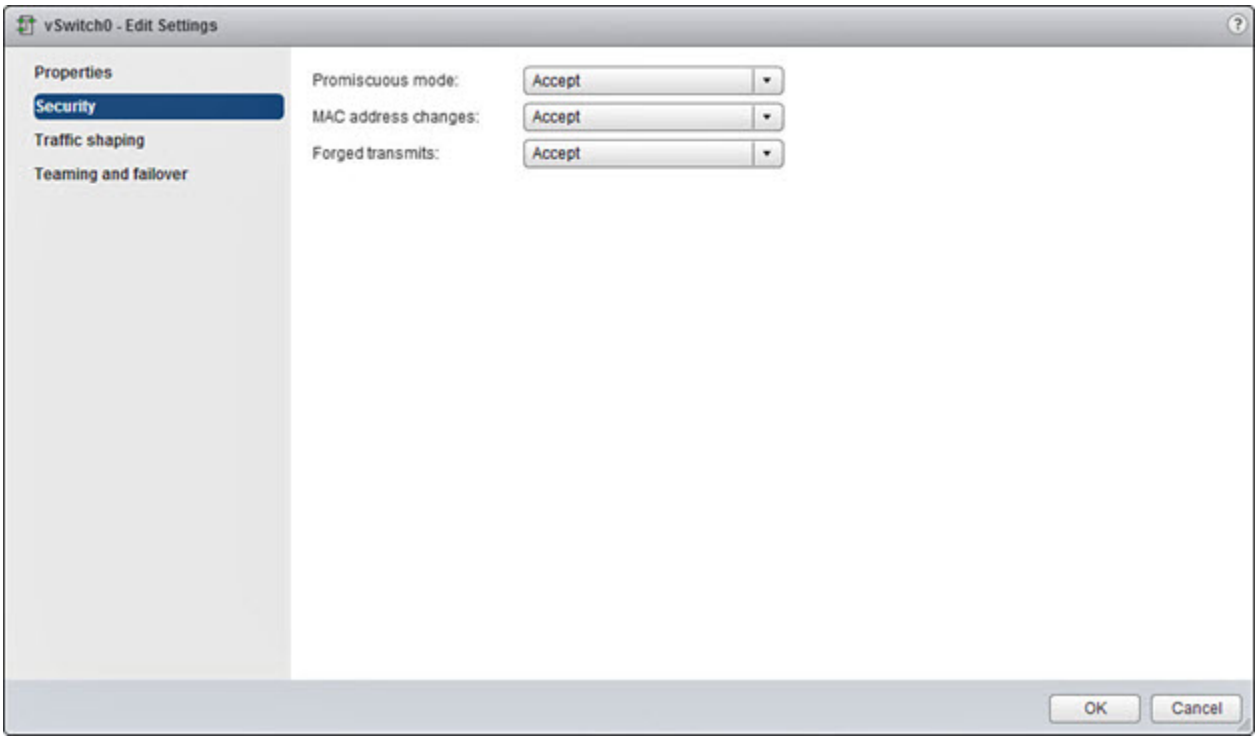
ステップ 2 [管理（Manage）] タブで、[ネットワーク（Networking）] をクリックし、[仮想スイッチ（Virtual switches）] を選択します。

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ける唯一の部分は、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。