



Cisco Firepower Threat Defense Virtual for VMware Deployment

改訂:2018 年 2 月 12 日

VMware を使用して Cisco Firepower Threat Defense Virtual を導入できます。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 と VMware の前提条件 \(2 ページ\)](#)
- [システム要件 \(3 ページ\)](#)
- [Firepower Threat Defense Virtual と VMware のガイドライン \(5 ページ\)](#)
- [Firepower Threat Defense Virtual と VMware の制限事項および既知の問題点 \(5 ページ\)](#)
- [OVF ファイルのガイドライン \(6 ページ\)](#)
- [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 \(7 ページ\)](#)
- [インストール後の設定 \(9 ページ\)](#)
- [CLI を使用した Firepower Threat Defense Virtual デバイスの設定 \(12 ページ\)](#)
- [Firepower Threat Defense Virtual の Firepower Management Center への登録 \(13 ページ\)](#)

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。

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 (5 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	—

Firepower Threat Defense Virtual と VMware の前提条件

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

機能	説明	サポート (あり/なし)	コメント
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 と VMware の前提条件

Firepower Threat Defense Virtual は、VMware vSphere Web クライアントまたは ESXi 上の vSphere スタンドアロン クライアントを使用して展開できます。システム要件については、『[Cisco Firepower Threat Defense Compatibility](#)』を参照してください。

仮想アプライアンスは、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は依存します。

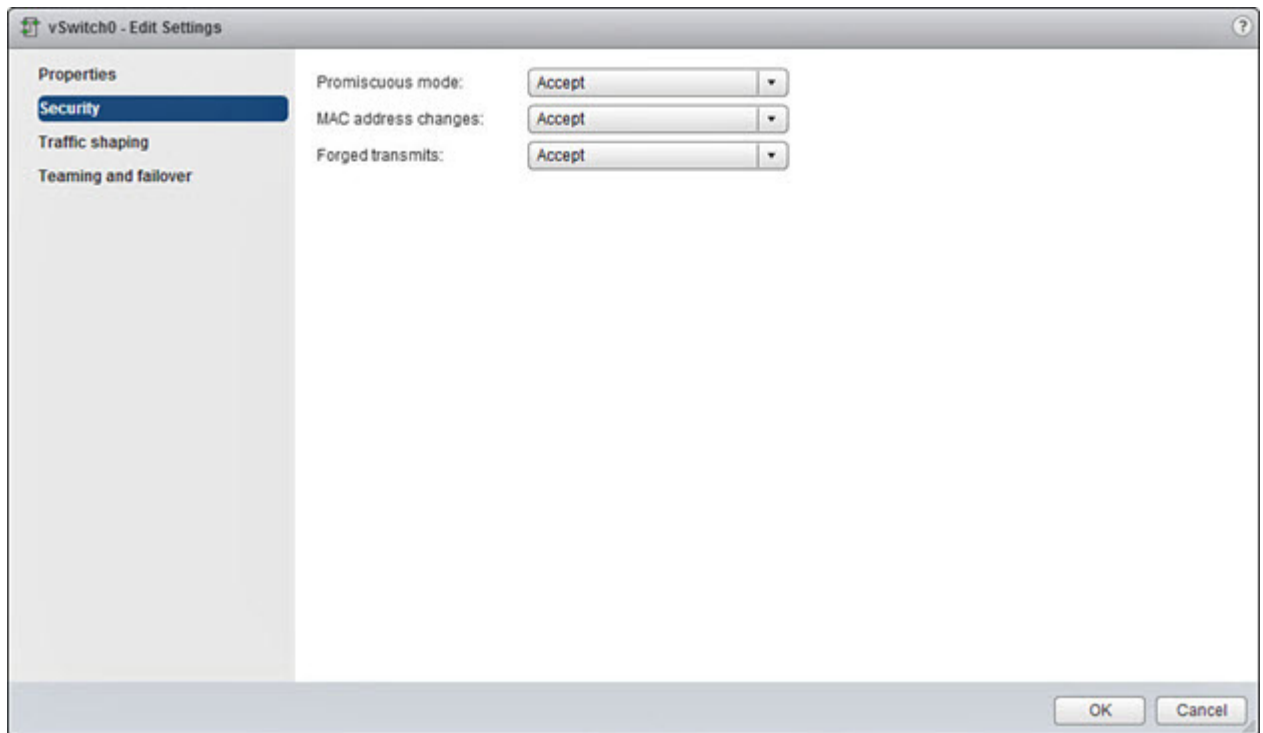
デフォルトの設定は、Firepower Threat Defense Virtual の適切な動作をブロックします。以下の必須の設定を参照してください。

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。



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 センサー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。

システム要件

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。

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) を搭載する必要があります。
- 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。

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
```

Firepower Threat Defense Virtual と VMware のガイドライン

- 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。
 - 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 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 (eth0) で、もう 1 つは診断用 (eth1) です。
 - 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 (eth0) で、もう 1 つは診断用 (eth1) です。
 - Version 6.0 で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。
- (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。
- 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追加と構成 \(10 ページ\)](#) 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

- 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。

OVF ファイルのガイドライン

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"
```

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 テンプレートを使用して展開する場合、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
 - 初期ファイアウォール モード
 - 管理 Cisco Firepower Management Center

(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 テンプレートを使用して展開する場合、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、[CLI を使用した Firepower Threat Defense Virtual デバイスの設定 \(12 ページ\)](#)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。

表 4 VMware OVF テンプレート (続き)

設定	ESXi または VI	操作
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。
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 (Properties)	VI のみ	仮想マシンの初期設定をカスタマイズします。

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

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。

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 テンプレートで指定されたネットワークごとに、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、Firepower Threat Defense Virtual インターフェイスごとにネットワーク マッピングを設定して、[次へ(Next)] をクリックします。

(注) 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 Firepower Threat Defense Virtual **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。

Firepower Management Center から到達可能な VM ネットワークに Management0-0 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。非管理インターフェイスは Firepower Management Center から設定できます。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、[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、[設定の編集 (Edit Settings)] を選択して、[設定の編集 (Edit Settings)] ダイアログボックスにアクセスします。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**送信元ネットワーク**と**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

送信元ネットワーク	宛先ネットワーク	機能
Management0-0	Diagnostic0/0	診断および管理
GigabitEthernet0-0	GigabitEthernet0/0	データ トラフィック
GigabitEthernet0-1	GigabitEthernet0/1	データ トラフィック
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 を展開した後、オプションで、vSphere Client に戻り、**[Edit Settings]** ダイアログボックスから他のインターフェイスをさらに追加できます。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。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。

11. 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。
12. **[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。

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 \(9 ページ\)](#) を参照してください。
- Firepower Threat Defense Virtual を Firepower Management Center に登録します。[Firepower Threat Defense Virtual の Firepower Management Center への登録 \(13 ページ\)](#) 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 ([システム要件 \(3 ページ\)](#) を参照)。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。

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確認できます。このタブで、CPU、メモリ、ディスク、および拡張 CPU リソースを確認できます。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 3 Firepower Threat Defense Virtual アプライアンスのデフォルト設定 \(4 ページ\)](#) 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。

インストール後の設定

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初期化\(11 ページ\)](#)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追加と構成\(10 ページ\)](#)を参照してください。

VMware インターフェイスの追加と構成

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 e1000 インターフェイスを置き換える際には、以下のガイドラインが重要です。

- 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 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。

(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。

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ことはできますが(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 インターフェイスなど)、同じ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。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が同じタイプである必要があります。

e1000 インターフェイスを置き換えるには、vSphere Client を使用して、まず既存の e1000 インターフェイスを削除して新しいインターフェイスを追加し、その後で適切なアダプタ タイプとネットワーク接続を選択します。

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。

仮想アプライアンスの初期化

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 Threat Defense Virtual の Firepower Management Center への登録 \(13 ページ\)](#) を参照してください。
- ESXi OVF テンプレート使用した場合、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、[CLI を使用した Firepower Threat Defense Virtual デバイスの設定 \(12 ページ\)](#) に進みます。

CLI を使用した Firepower Threat Defense Virtual デバイスの設定

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、ESXi OVF テンプレートで展開した場合には、CLI を使用して仮想デバイスを設定する必要があります。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。

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

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

CLI では、物理デバイスのセットアップ Web ページで要求される設定情報とほぼ同じ情報が要求されます。詳細については、『Firepower システム Installation Guide』を参照してください。

(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。詳細については、『Firepower Management Center Configuration Guide』の「Command Line Reference」の章を参照してください。

手順

1. VMware コンソールを開きます。
2. VMware コンソールで、ユーザ名として `admin`、および展開のセットアップ ウィザードで指定した新しい `admin` アカウント パスワードを使用して、仮想アプライアンスにログインします。

ウィザードを使用してパスワードを変更していない場合、または ESXi OVF テンプレートを使用して展開している場合は、パスワードとして `Admin123` を使用します。

直後に、デバイスから EULA を読むようにプロンプトが表示されます。

3. EULA を読んで同意します。
4. `admin` アカウントのパスワードを変更します。このアカウントには Configuration CLI アクセス レベルが付与されており、削除することはできません。

(注) Cisco では、大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することを推奨しています。辞書に掲載されている単語の使用は避けてください。

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 Threat Defense Virtual を Firepower Management Center に登録します。[Firepower Threat Defense Virtual の Firepower Management Center への登録\(13 ページ\)](#)を参照してください。

Firepower Threat Defense Virtual の Firepower Management Center への登録

仮想デバイスには Web インターフェイスがないため、CLI を使用して仮想デバイスを Cisco Firepower Management Center に登録する必要があります（物理でも仮想でも可）。初期設定プロセス中にデバイスを Firepower Management Center に登録する方が簡単です。これは、すでにデバイスの CLI にログインしているためです。

デバイスを登録するには、`configure manager add` コマンドを使用します。デバイスを Firepower Management Center へ登録するには、自己生成の一意の英数字登録キーが必ず必要です。これはユーザが指定する簡単なキーで、ライセンスキーとは異なります。

ほとんどの場合は、登録キーと一緒に Firepower Management Center の IP アドレスを指定する必要があります。たとえば次のようにします。

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

XXX.XXX.XXX.XXX は、管理している Firepower Management Center の IP アドレスで、`my_reg_key` は、仮想デバイスに入力した登録キーです。

(注) ESXi プラットフォームでは、vSphere Client を使用して仮想デバイスを Firepower Management Center に登録する場合、設定時に DNS 情報が提供されていない場合は、管理している Firepower Management Center の IP アドレス（ホスト名ではない）を使用する必要があります。

ただし、デバイスと Firepower Management Center がネットワーク アドレス変換 (NAT) デバイスによって分けられており、Firepower Management Center が NAT デバイスの背後にある場合は、登録キーと共に一意の NAT ID を入力し、IP アドレスの代わりに `DONTRESOLVE` を指定します。次に例を示します。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

`my_reg_key` は仮想デバイスに入力した登録キーで、`my_nat_id` は NAT デバイスの NAT ID です。

デバイス (Firepower Management Center ではない) が NAT デバイスの背後にある場合は、一意の NAT ID を登録キーと共に入力し、Firepower Management Center のホスト名または IP アドレスを指定します。次に例を示します。

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

`my_reg_key` は仮想デバイスに入力した登録キーで、`my_nat_id` は NAT デバイスの NAT ID です。

手順

1. CLI 設定 (管理者) の権限を持つユーザとして仮想デバイスにログインします。
 - VMware コンソールから初期設定を実行している場合は、`admin` ユーザとしてすでにログインしています。このユーザは必要なアクセス レベルを持っています。
 - そうでない場合は、VMware コンソールを使用してデバイスにログインします。または、デバイスのネットワーク設定が完了している場合は、SSH を使用してデバイスの管理 IP アドレスまたはホスト名にログインします。
2. プロンプトで、次のような構文の `configure manager add` コマンドを使用してデバイスを Cisco Firepower Management Center に登録します。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

値は次のとおりです。

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` は、Firepower Management Center の IP アドレスを表します。Firepower Management Center が直接アドレス指定できない場合は、`DONTRESOLVE` を使用します。
- `reg_key` は、デバイスを Firepower Management Center へ登録するのに必要な一意の英数字による登録キーです。

(注) 登録キーは、ユーザが生成した 1 回限り使用できる一意のキーで、37 文字を超えてはなりません。有効な文字には、英数字 (A～Z、a～z、0～9)、およびハイフン (-) などがあります。Firepower Management Center にデバイスを追加するときは、この登録キーを覚えておく必要があります。

- `nat_id` は、Cisco Firepower Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。ホスト名が DONTRESOLVE に設定されている場合に必須です。

(注) `show managers` コマンドを使用して、デバイス登録の状態をモニタします。

3. アプライアンスからログアウトします。

次の作業

- Firepower Management Center をすでに設定している場合は、Web インターフェイスにログインし、[デバイス管理 (Device Management) ページ ([デバイス (Device)] > [デバイス管理 (Device Management)]) を使用してデバイスを追加します。詳細については、『*Firepower Management Center Configuration Guide*』の「Managing Devices」の章を参照してください。

シスコおよびシスコのロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks ご確認いただけます。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

© 2018 Cisco Systems, Inc. All rights reserved.