VMware への Threat Defense Virtual の展開

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

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 Threat Defense Virtual デバイスをパッケージ化しています。Threat Defense Virtual 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。

Threat Defense Virtual は、VMware ESXi を実行できる任意の x86 デバイスに展開できます。Threat Defense Virtual 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。

Threat Defense Virtual の VMware 機能のサポート

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

表 *1 : 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。「Threat Defense Virtual 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	Management Center 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	Threat Defense Virtual VM の障害に対して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	Threat Defense Virtual VM の障害に対して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	–

システム要件

Threat Defense Virtual 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。

Threat Defense Virtual 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。Threat Defense Virtual の各インスタンスには、サーバー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 : Threat Defense Virtual* アプライアンスのリソース要件

設定	値
パフォーマンス階層	**バージョン 7.0 以降** Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。 • FTDv5 4vCPU/8GB（100 Mbps） • FTDv10 4vCPU/8GB（1 Gbps） • FTDv20 4vCPU/8GB（3 Gbps） • FTDv30 8vCPU/16GB（5 Gbps） • FTDv50 12vCPU/24GB（10 Gbps） • FTDv100 16vCPU/32GB（16 Gbps） Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Licensing」の章を参照してください。 （注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。

設定	値
コアおよびメモリの数	**バージョン 6.4 からバージョン 6.7** Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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 （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	Threat Defense Virtual 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 Threat Defense Virtual 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、もう 1 つは診断用です。ixgbe ドライバは、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。 • **E1000**：e1000 インターフェイスを使用する場合、e1000 ドライバ用の Threat Defense Virtual 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では、VMware 上の Threat Defense Virtual 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 Threat Defense Virtual 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 （20 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」の項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ーでは、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

Threat Defense Virtual 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 （12 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ーが必要です。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、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。

（注） Threat Defense Virtual は、複数の Non-uniform Memory Access（NUMA）ノードおよび物理コア用の複数の CPU ソケットをサポートしません。

  - 割り当てられたすべての物理コアを 1 つのソケットに割り当てるようにしてください。

（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

- 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確認できます。

```
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
```

Threat Defense Virtual と VMware のガイドライン、制限事項、および既知の問題

Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。

表 *3 : Threat Defense Virtual* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Licensing」の章を参照してください。

パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「ESXi 構成でのパフォーマンスの向上 （35 ページ）」、「NUMA のガイドライン （36 ページ）」、および「SR-IOV インターフェイスのプロビジョニング （36 ページ）」を参照してください。

Receive Side Scaling：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。RSS はバージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

クラスタリング

バージョン 7.2 以降、クラスタリングは VMware で展開された Threat Defense Virtual インスタンスでサポートされます。詳細については、『プライベートクラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。

管理モード

- Secure Firewall Threat Defense（旧称 Firepower Threat Defense） デバイスの管理には次の 2 つのオプションがあります。
  - Device Manager オンボード統合マネージャ。

（注） VMware 上の Threat Defense Virtual は、シスコ ソフトウェア バージョン 6.2.2 以降で Device Manager をサポートしています。バージョン 6.2.2 よりも前のソフトウェアを実行している VMware 上の Threat Defense Virtual は、Management Center を使用してのみ管理できます。「Secure Firewall Threat Defense Virtual デバイスの管理方法」を参照してください。

  - Management Center。

- 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 Threat Defense Virtual 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 Device Manager に切り替えることはできません。
- 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。Device Manager を使用する場合は、これが唯一のサポートモードです。

OVF ファイルのガイドライン

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、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。
  - Device Manager を使用するローカル管理（デフォルト）、または 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）] で [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。Device Manager を使用する場合は、これが唯一のサポートモードです。

（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、インストール後にシステムの必須設定を行う必要があります。この Threat Defense Virtual 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 Threat Defense Virtual の展開 （30 ページ）」を参照してください。

vSphere 7.0.2 で仮想マシン（VM）の設定を保存できない

vSphere 7.0.2 を使用している場合、VM の設定を保存できない場合があります。

（注） この問題は、VMware ナレッジベースの記事 https://kb.vmware.com/s/article/83898 の手順に従って解決できます。

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。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、vMotion を使用して Secure Firewall Management Center Virtual（旧称 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。Threat Defense Virtual 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 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 "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。

Threat Defense Virtual 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の 3 つの要素は、無差別モード、MAC アドレスの変更、および不正送信です。Threat Defense Virtual は無差別モードで動作し、Threat Defense Virtual の高可用性が正しく機能するかは、アクティブとスタンバイ間の MAC アドレスの切り替えにかかっています。

デフォルト設定では、Threat Defense Virtual の適切な動作が阻止されます。以下の必須の設定を参照してください。

表 *4 : 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。
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。

（注） NSX-T を使用する VMware は認定されていないため、vSphere 標準スイッチのセキュリティポリシー設定の NSX-T 構成に関する推奨事項はありません。

Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。

- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

vSphere 標準スイッチのセキュリティポリシー設定の変更

デフォルト設定では、Threat Defense Virtual の適切な動作が阻止されます。

ステップ 1 vSphere Web Client で、ホストに移動します。

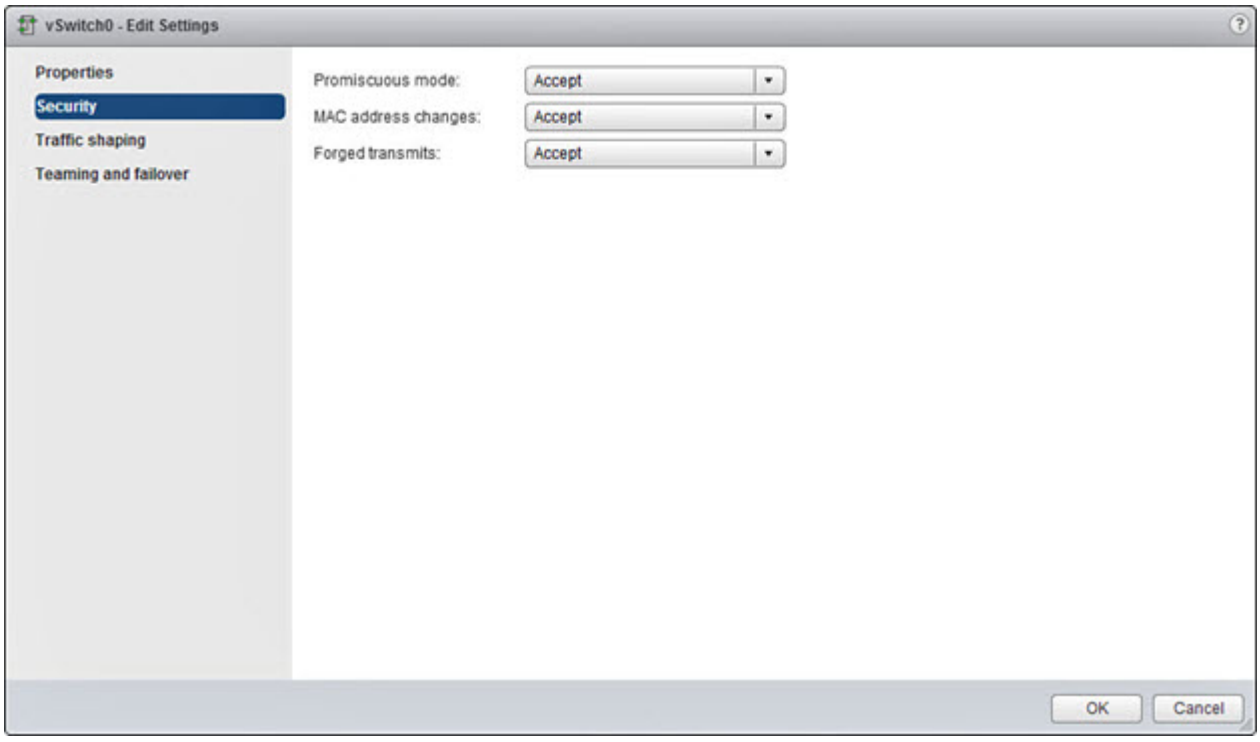
ステップ 2 [管理（Manage）] タブで、[ネットワーク（Networking）] をクリックし、[仮想スイッチ（Virtual switches）] を選択します。

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、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。

インターフェイスの計画

展開の前に、Threat Defense Virtual 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。Threat Defense Virtual 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。

Threat Defense Virtual 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、Threat Defense Virtual 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（3 ページ）」を参照してください。

重要 Threat Defense Virtual 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 Threat Defense Virtual 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、Threat Defense Virtual 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。
- Threat Defense Virtual インターフェイスに HOLDING ポートグループを使用しないことをお勧めします。vSphere からの HOLDING ポートグループは、インターフェイス接続の一貫性が失われる原因になります。これにより、セカンダリ Threat Defense Virtual デバイスとの HA 形成中に問題が発生する可能性があります。
- 10 個の Threat Defense Virtual 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、Threat Defense Virtual 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。
- 6.7 以降では、必要に応じて、管理インターフェイスの代わりにデータインターフェイスを Management Center に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center にアクセスするためのデータインターフェイスの設定に関する詳細については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』の **configure network management-data-interface** コマンドを参照してください。
- Threat Defense Virtual の内部インターフェイスまたはフェールオーバーの高可用性リンクに使用される ESX ポートグループ用に 2 つの仮想 NIC をもつフェールオーバーの順序は、1 つはアクティブアップリンク、もう 1 つはスタンバイアップリンクとなるよう構成されていなければなりません。この設定は、2 つの VM が相互に ping を実行したり、Threat Defense Virtual の高可用性リンクを稼働させたりするために必要です。

デフォルトの VMXNET3 インターフェイス

重要 Threat Defense Virtual 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、 Threat Defense Virtual 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 Threat Defense Virtual 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：*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	Diagnostic0/0	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、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。

e1000 インターフェイス

重要 Threat Defense Virtual 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、Threat Defense Virtual 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 Threat Defense Virtual 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 *6 :* 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 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	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 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 Threat Defense Virtual と Management Center Virtual では、仮想デバイスを作成する際のデフォルトインターフェイスが vmxnet3 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ことはできますが（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。

ステップ 1 Threat Defense Virtual または Management Center Virtual 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 Threat Defense Virtual または Management Center Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual または Management Center Virtual の電源をオンにします。

インターフェイスの追加

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 X 1、診断 X 1、データ X 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、Threat Defense Virtual 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 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。

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、『Cisco Secure Firewall Device Manager Configuration Guide』の「インターフェイスの変更のスキャンとインターフェイスの移行」の手順を使用できます。

VMware の展開について

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

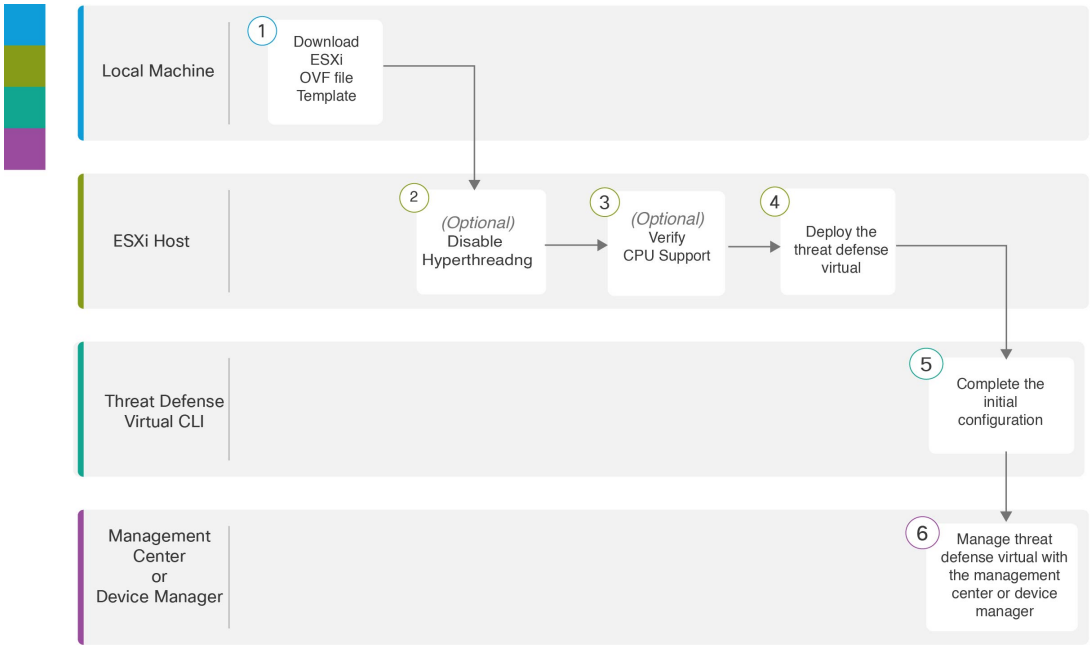
Threat Defense Virtual VMware 用の FTDv はオープン仮想化フォーマット（OVF）を使用して配布されます。OVF は、仮想マシンをパッケージ化して展開する標準的な方法です。VMware では、vSphere 仮想マシンをプロビジョニングするための方法がいくつか用意されています。お使いの環境に最適な方法は、インフラストラクチャの規模やタイプ、達成目標などの要因によって異なります。

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

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

エンドツーエンドの手順

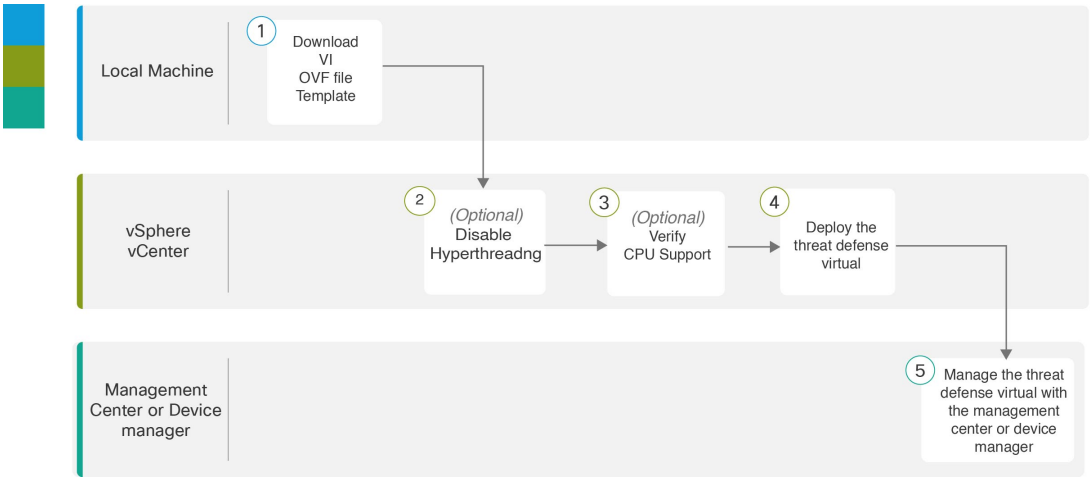
次のフローチャートは、ESXi ホストに Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	Local Machine	ESXi OVF テンプレートのダウンロード：Cisco.com から入手可能なオープン仮想フォーマット（OVF）パッケージをダウンロードします。
2	ESXi ホスト（ESXi Host）	（任意）システム要件：Threat Defense Virtual を実行するシステムのハイパースレッディングを無効にします。
3	ESXi ホスト（ESXi Host）	システム要件：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。
4	ESXi ホスト（ESXi Host）	vSphere ESXi ホストへの Threat Defense Virtual の展開：Threat Defense Virtual アプライアンスを単一の ESXi ホストに展開します。
5	Threat Defense Virtual CLI	CLI を使用した Threat Defense Virtual のセットアップ：ESXi OVF テンプレートを使用して展開した場合は、CLI を使用して Threat Defense Virtual を設定する必要があります。

	ワークスペース	手順
6	Management CenterまたはDevice Manager	Threat Defense Virtual を管理します。 • Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 • Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理

次のフローチャートは、vSphere vCenter に Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	Local Machine	VI OVF テンプレートのダウンロード：Cisco.com から入手可能なオープン仮想フォーマット（OVF）パッケージをダウンロードします。
2	vSphere vCenter	（任意）システム要件：Threat Defense Virtual を実行するシステムのハイパースレッディングを無効にします。
3	vSphere vCenter	システム要件：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。
4	vSphere vCenter	vSphere ESXi ホストへの Threat Defense Virtual の展開：Threat Defense Virtual アプライアンスを単一の ESXi ホストに展開します。

	ワークスペース	手順
5	Management CenterまたはDevice Manager	Threat Defense Virtual を管理します。 • Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 • Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理

vSphere vCenter への Threat Defense Virtual の展開

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

始める前に

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

ステップ 1 vSphere Web Client（または vSphere Client）にログインします。

ステップ 2 vSphere Web Client（または vSphere Client）を使用し、**[ファイル（File）]** > **[OVFテンプレートの展開（Deploy OVF Template）]** をクリックして、以前にダウンロードした OVF テンプレートファイルを展開します。

[OVFテンプレートの導入（Deploy OVF Template）] ウィザードが表示されます。

ステップ 3 ファイルシステムで OVF テンプレートソースの場所を参照し、[次へ（Next）] をクリックします。

次の Threat Defense Virtual VI OVF テンプレートを選択します。

Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf

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

ステップ 4 [OVFテンプレートの詳細（OVF Template Details）] ページを確認し、OVF テンプレートの情報（製品名、バージョン、ベンダー、ダウンロードサイズ、ディスク上のサイズ、説明）を確認して、[次へ（Next）] をクリックします。

ステップ 5 [エンドユーザーライセンス契約書（End User License Agreement）] ページが表示されます。OVF テンプレート（VI テンプレートのみ）でパッケージ化されたライセンス契約書を確認し、[承認（Accept）] をクリックしてライセンスの条件に同意し、[次へ（Next）] をクリックします。

ステップ 6 [名前と場所（Name and Location）] ページで、この展開の名前を入力し、Threat Defense Virtual を展開するインベントリ内の場所（ホストまたはクラスタ）を選択して、[次へ（Next）] をクリックします。名前はインベントリフォルダ内で一意である必要があり、最大 80 文字を使用できます。

VSphere Web Client では、インベントリビューに管理対象オブジェクトの組織階層が表示されます。インベントリは、vCenter Server またはホストが管理対象オブジェクトを整理する目的で使用する階層構造です。この階層には、vCenter Server にあるすべての監視対象オブジェクトが含まれています。

ステップ 7 Threat Defense Virtual を実行するリソース プールに移動して選択し、[次へ（Next）] をクリックします。

（注） このページは、クラスタにリソースプールが含まれている場合にのみ表示されます。

ステップ 8 [導入設定（Deployment Configuration）] を選択します。[設定（Configuration）] ドロップダウンリストから、サポートされている 3 つの vCPU/メモリ値のいずれかを選択し、[次へ（Next）] をクリックします。

重要 バージョン 6.4 以降、Threat Defense Virtual は、調整可能な vCPU およびメモリリソースを使用して展開されます。6.4 より前のバージョンでは、Threat Defense Virtual は、固定構成の 4vCPU/8GB デバイスとして展開されていました。「システム要件 （3 ページ）」を参照してください。

ステップ 9 仮想マシンファイルを保存する [保存（Storage）] 場所を選択し、[次へ（Next）] をクリックします。

このページで、宛先クラスタまたはホストですでに設定されているデータストアから選択します。仮想マシン コンフィギュレーション ファイルおよび仮想ディスク ファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスクファイルを保存できる十分なサイズのデータストアを選択してください。

ステップ 10 仮想マシンの仮想ディスクを保存するための「ディスク形式」を選択し、[次へ（Next）] をクリックします。

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

ステップ 11 [ネットワークマッピング（Network Mapping）] ページで、OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ（Next）] をクリックします。

Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Management Center または Device Manager から設定できます。

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

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集（Edit Settings）] ダイアログボックスからネットワークを変更できます。展開後、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 Threat Defense Virtual の ID は表示されません（ネットワークアダプタ ID のみ）。

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

表 7 : 送信元から宛先ネットワークへのマッピング：*vmxnet3*

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic0/0	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）

Threat Defense Virtual を展開する際には、合計 10 個のインターフェイスを指定できます。データインターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データインターフェイスが一意のサブネットまたは VLAN にマッピングされていることを確認します。すべての 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、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。

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

a) **パスワード**

Threat Defense Virtual 管理アクセス用のパスワードを設定します。

b) **ネットワーク**

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

c) **管理**

管理モードを設定します。[ローカルマネージャを有効にする（Enable Local Manager）] のドロップダウン矢印をクリックし、Web ベースの Device Manager 統合設定ツールを使用する場合は [はい（Yes）] を選択します。Management Center を使用してこのデバイスを管理するには、[いいえ（No）] を選択します。管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法」を参照してください。

d) **ファイアウォールモード**

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

[ローカルマネージャを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、[ルーテッド（Routed）] ファイアウォール モードのみを選択できます。ローカルの Device Manager を使用してトランスペアレント ファイアウォール モードのインターフェイスは設定できません。

e) **導入タイプ**

導入タイプを [スタンドアロン（Standalone）] または [クラスタ（Cluster）] に設定します。[クラスタ（Cluster）] を選択して、クラスタ制御リンクに必要なジャンボフレームの予約を有効にします。スタンドアロンまたは高可用性の展開には、[スタンドアロン（Standalone）] を選択します。スタンドアロンデバイスとして展開した場合でもクラスタで使用できますが、展開後にクラスタリング用のジャンボフレームを有効にすると、再起動が必要になることに注意してください。

f) **登録**

[ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、管理を行う Firepower Management Center にこのデバイスを登録するのに必要なクレデンシャルを指定する必要があります。次の情報を入力します。

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

g) [次へ（Next）] をクリックします。

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

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

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

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

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

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法」を参照してください。

クラスタ展開用の Day 0 構成ファイルの準備

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。

重要 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。

導入時に Day 0 の構成ファイルを使用すると、導入プロセスで Threat Defense Virtual アプライアンスの初期設定をすべて実行できます。次を指定することができます。

- エンド ユーザー ライセンス契約書（EULA）の承認。
- 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。
- 管理モード。Secure Firewall Threat Defense Virtual デバイスの管理方法を参照してください。

  Management Center フィールド（[FmcIp]、[FmcRegKey]、[FmcNatId]）に情報を入力します。使用していない管理モードでは、フィールドを空のままにします。
- 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。
- Threat Defense Virtual をクラスタとして展開するかスタンドアロンで展開するかを指定できる展開タイプ。

（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。

手順の概要

1. Threat Defense Virtual を展開する Linux ホストにログインします。
2. Threat Defense Virtual 用に「day0-config」というテキストファイルを作成します。このテキストファイルには、クラスタ展開の設定、ネットワーク設定、および Management Center の管理に関する情報を追加する必要があります。
3. 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。
4. ターゲットの ESXi ホストにログインします。
5. クラスタモードで Threat Defense Virtual を展開する仮想マシンインスタンスを開きます。
6. 仮想マシンの電源をオンにする前に、作成した day0 の ISO イメージファイルを参照して、[ハードウェア構成（Hardware Configuration）] の設定の下にある [CD/DVD ドライブ1（CD/DVD drive 1）] フィールドにアタッチします。
7. 仮想マシンの電源をオンにして、クラスタモードで Threat Defense Virtual を展開します。

手順の詳細

ステップ 1 Threat Defense Virtual を展開する Linux ホストにログインします。

ステップ 2 Threat Defense Virtual 用に「day0-config」というテキストファイルを作成します。このテキストファイルには、クラスタ展開の設定、ネットワーク設定、および Management Center の管理に関する情報を追加する必要があります。

例：

```
#Firepower Threat Defense
{

     "DeploymentType": "Cluster"

}
```

Management Center フィールド（[FmcIp]、[FmcRegKey]、[FmcNatId]）に情報を入力します。使用していない管理オプションの場合は、これらのフィールドを空白のままにします。

ステップ 3 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。

例：

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

ステップ 4 ターゲットの ESXi ホストにログインします。

ステップ 5 クラスタモードで Threat Defense Virtual を展開する仮想マシンインスタンスを開きます。

ステップ 6 仮想マシンの電源をオンにする前に、作成した day0 の ISO イメージファイルを参照して、[ハードウェア構成（Hardware Configuration）] の設定の下にある [CD/DVD ドライブ1（CD/DVD drive 1）] フィールドにアタッチします。

ステップ 7 仮想マシンの電源をオンにして、クラスタモードで Threat Defense Virtual を展開します。

vSphere ESXi ホストへの Threat Defense Virtual の展開

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

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

vCenter 環境に Threat Defense Virtual アプライアンスを展開する方法については、「vSphere vCenter への Threat Defense Virtual の展開 （24 ページ）」参照してください。

始める前に

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

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

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

Cisco.com へのログインとシスコサービス契約が必要です。

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

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

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

ステップ 3 ブラウザで、*http://host-name/ui* または *http://host-IP-address/ui* の形式で、対象の ESXi ホスト名または IP アドレスを入力します。

ログイン画面が表示されます。

ステップ 4 管理者のユーザー名とパスワードを入力します。

ステップ 5 [ログイン（Login）] をクリックして続行します。

これで、ターゲットの ESXi ホストにログインしました。

ステップ 6 VMware Host Client のインベントリで、[ホスト（Host）] を右クリックし、[VMの作成/登録（Create/Register VM）] を選択します。

[新規仮想マシンウィザード（New Virtual Machine Wizard）] が開きます。

ステップ 7 [作成タイプの選択（Select creation type）] ページで、[OVFまたはOVAファイルから仮想マシンを導入（Deploy a virtual machine from an OVF or OVA file）] を選択し、[次へ（Next）] をクリックします。

ステップ 8 ウィザードの [OVFおよびVMDKファイルの選択（Select OVF and VMDK files）] ページで次の操作を行います。

a) Threat Defense Virtual マシンの名前を入力します。

仮想マシン名には 80 文字まで含めることができます。マシン名は各 ESXi インスタンスの中で一意にする必要があります。

b) 青いペインをクリックし、 Threat Defense Virtual tar ファイルを解凍したディレクトリを参照して、ESXi OVF テンプレートと付随する VMDK ファイルを選択します。

Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.ovf

Cisco_Firepower_Threat_Defense_Virtual-*X.X.X-xx*.vmdk

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

注目 必ず ESXi OVF を選択してください。

ステップ 9 [次へ（Next）] をクリックします。

使用しているローカルシステムストレージが開きます。

ステップ 10 ウィザードの [ストレージの選択（Select storage）] ページで、アクセス可能なデータストアのリストからデータストアを選択します。

仮想マシンの設定ファイルとすべての仮想ディスクが、このデータストアに保存されます。データストアはそれぞれ、サイズ、速度、可用性などのプロパティが異なる場合があります。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 Threat Defense Virtual の ESXi OVF と一緒にパッケージ化されている [展開オプション（Deployment options）] を設定します。

a) [ネットワークマッピング（Network Mapping）] : OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ（Next）] をクリックします。

Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Management Center または Device Manager から設定できます。

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

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集（Edit Settings）] ダイアログボックスからネットワークを変更できます。展開後、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 Threat Defense Virtual の ID は表示されません（ネットワークアダプタ ID のみ）。

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

表 *8 :* 送信元から宛先ネットワークへのマッピング：*vmxnet3*

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic0/0	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	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 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）

Threat Defense Virtual を展開する際には、合計 10 個のインターフェイスを指定できます。データインターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データインターフェイスが一意のサブネットまたは VLAN にマッピングされていることを確認します。すべての 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、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。

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

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

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

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

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

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

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、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。

次のタスク

- CLI を使用して仮想デバイスのセットアップを完了します。これは、ESXi OVF テンプレートを使用して Threat Defense Virtual を展開する場合の次の手順になります。「CLI を使用した Threat Defense Virtual のセットアップ （34 ページ）」を参照してください。

CLI を使用した Threat Defense Virtual のセットアップ

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

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

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

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

ステップ 1 VMware コンソールを開きます。

ステップ 2 [firepowerログイン（firepower login）] プロンプトで、ユーザー名 **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。

ステップ 3 Threat Defense Virtual 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 の構成

- IPv4 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク
- 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（ローカル管理で Device Manager を使用）

ステップ 4 セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

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

ステップ 5 プロンプトに従ってシステム設定を行います。

ステップ 6 コンソールが firepower # プロンプトに戻るときに、設定が正常に行われたことを確認します。

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、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。

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法」を参照してください。

ESXi 構成でのパフォーマンスの向上

ESXi ホストの CPU 構成時の設定を調整することによって、ESXi 環境内の Threat Defense Virtual のパフォーマンスを向上させることができます。[Scheduling Affinity] オプションによって、仮想マシンの CPU をホストの物理コア（およびハイパースレッディングが有効になっている場合のハイパースレッド）にどのように分散させるかを制御できます。この機能を使用すれば、各仮想マシンを、指定したアフィニティセット内のプロセッサに割り当てることができます。

詳細については、以下の VMware ドキュメントを参照してください。

- 「*Administering CPU Resources*」の章（『vSphere Resource Management』）。
- 『Performance Best Practices for VMware vSphere』
- vSphere Client のオンライン ヘルプ。

NUMA のガイドライン

Non-uniform Memory Access（NUMA）は、マルチプロセッサシステムのプロセッサに対するメインメモリモジュールの配置について記述する共有メモリアーキテクチャです。プロセッサが自身のノード（リモートメモリ）内に存在しないメモリにアクセスする場合は、ローカルメモリにアクセスする場合よりも低速の速度で、NUMA 接続を介してデータを転送する必要があります。

X86 サーバーアーキテクチャは、複数のソケットおよびソケット内の複数のコアで構成されています。各 CPU ソケットとそのメモリおよび I/O が、NUMA ノードと呼ばれます。メモリからパケットを効率的に読み取るには、ゲストアプリケーションおよび関連付けられている周辺機器（NIC など）が同じノード内に存在する必要があります。

最適な Threat Defense Virtual パフォーマンスを実現するには：

- Threat Defense Virtual VM は、1 つの NUMA ノード上で実行する必要があります。1 つの Threat Defense Virtual が 2 つのソケットで実行されるように展開されている場合、パフォーマンスは大幅に低下します。
- 8 コア Threat Defense Virtual では、ホスト CPU の各ソケットが、それぞれ 8 個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- 16 コア Threat Defense Virtual では、ホスト CPU 上の各ソケットが、それぞれ 16 個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- NIC は、Threat Defense Virtual VM と同じ NUMA ノード上にある必要があります。

NUMA システムと ESXi の使用に関する詳細については、VMware ドキュメント『*vSphere Resource Management*』で、お使いの VMware ESXi バージョンを参照してください。このドキュメントおよびその他の関連ドキュメントの最新エディションを確認するには、http://www.vmware.com/support/pubs 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、ホストサーバー内の単一の 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

バーの CPU 負荷が低下します。最近の x86 サーバー 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 Threat Defense Virtual 仮想マシンに最大 10 Gbps の接続を提供できます。このセクションでは、VMware 環境で VF を設定する方法について説明します。

SR-IOV インターフェイスのベストプラクティス

SR-IOV インターフェイスに関するガイドライン

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

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

このセクションでは、VMware システム上の SR-IOV インターフェイスのプロビジョニングに関するさまざまなセットアップ手順と設定手順を示します。このセクション内の情報は、VMware ESXi 6.0 と vSphere Web Client、Cisco UCS C シリーズ サーバー、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

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 Threat Defense Virtual マシンへのネットワーク接続が切断する場合があります。

注意 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。

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。

ixgbe-vf インターフェイスの使用の制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の Threat Defense Virtual プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている Threat Defense Virtual（プライマリ装置）に障害が発生すると、スタンバイ Threat Defense Virtual 装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ Threat Defense Virtual 装置の新しい MAC アドレスで更新されます。その後、Threat Defense Virtual は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更を同じネットワーク上の他のデバイスに通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

ESXi ホスト BIOS の確認

始める前に

VMware に SR-IOV インターフェイスを備えた 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の『Compatibility Guide』だけでなく、仮想化が有効か無効かを検出するダウンロード可能な『CPU Identification Utility』も含めて、仮想化サポートの各種確認手段を提供しています。

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

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

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

ステップ 2 ホストによって認識されるユーザ名とパスワードを入力します。

ステップ 3 Run the following commands:

```
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。

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

値の 3 は、仮想化がサポートされており、有効になっていることを示します。

次のタスク

ホスト物理アダプタ上で SR-IOV を有効にします。

ホスト物理アダプタ上での SR-IOV の有効化

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

始める前に

- SR-IOV 互換ネットワーク インターフェイス カード（NIC）がインストールされていることを確認します。「システム要件 （3 ページ）」を参照してください。

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

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

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

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

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

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

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

ステップ 6 [OK] をクリックします。

ステップ 7 ESXi ホストを再起動します。

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

次のタスク

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

vSphere スイッチの作成

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

ステップ 1 vSphere Web Client で、ESXi ホストに移動します。

ステップ 2 [Manage] で、[Networking] を選択してから、[Virtual switches] を選択します。

ステップ 3 プラス（+）記号付きの緑色の地球アイコンである [Add host networking] アイコンをクリックします。

ステップ 4 [標準スイッチ用仮想マシンポートグループ（Virtual Machine Port Group for a Standard Switch）] 接続タイプを選択して、[次へ（Next）] をクリックします。

ステップ 5 [New standard switch] を選択して、[Next] をクリックします。

ステップ 6 物理ネットワーク アダプタを新しい標準スイッチに追加します。

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。

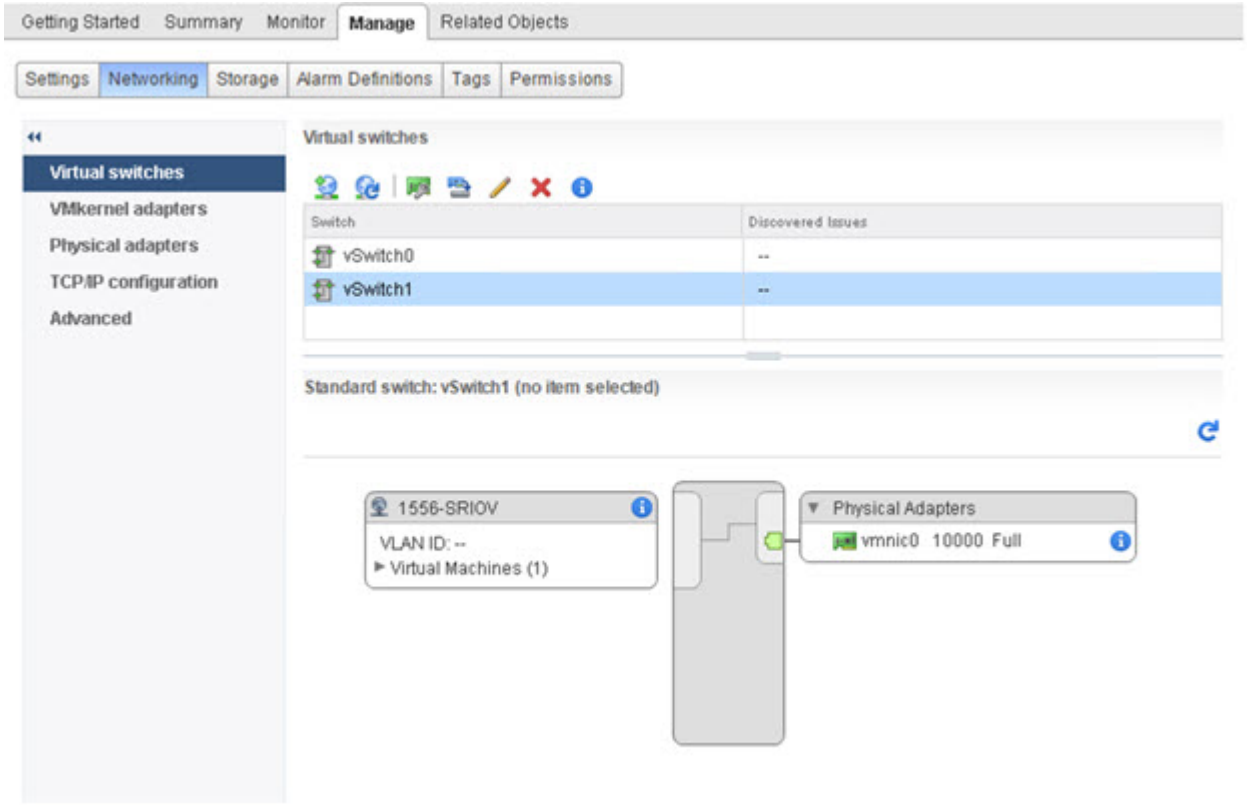
c) [Failover order group] ドロップダウン メニューで、[Active adapters] から選択します。

d) [OK] をクリックします。

ステップ 7 SR-IOV vSwitch の [Network label] を入力して、[Next] をクリックします。

ステップ 8 [Ready to complete] ページで選択を確認してから、[Finish] をクリックします。

図 *2 : SR-IOV* インターフェイスがアタッチされた新しい *vSwitch*



次のタスク

- 仮想マシンの互換性レベルを確認します。

仮想マシンの互換性レベルのアップグレード

互換性レベルは、ホストマシンで使用可能な物理ハードウェアに対応する仮想マシンで使用可能な仮想ハードウェアを決定します。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 Threat Defense Virtual に公開されます。この手順では、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。

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

ステップ 2 変更する Threat Defense Virtual マシンを見つけます。

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 Threat Defense Virtual マシンを選択します。

ステップ 3 選択した仮想マシンの電源をオフにします。

ステップ 4 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。

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

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

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

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

次のタスク

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

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

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

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

ステップ 2 変更する Threat Defense Virtual マシンを特定します。

a) データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択して、[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 Threat Defense Virtual マシンを選択します。

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

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

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

[New Network] インターフェイスが表示されます。

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

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

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

ステップ 9 仮想マシンの電源をオンにします。

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

（注） 無差別モードの制限により、SR-IOV ドライバを使用する一部の Intel ネットワークアダプタ（Intel X710 や 82599 など）では、SR-IOV インターフェイスを Threat Defense Virtual のパッシブインターフェイスとして使用することはできません。このような場合は、この機能をサポートするネットワークアダプタを使用してください。Intel ネットワークアダプタの詳細については、『Intel Ethernet Products』[英語] を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。