VMware 向け Cisco Firepower NGIPSv クイック スタート ガイド

バージョン 6.0

発行日:2015 年 11 月 10 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

VMware 向け Cisco Firepower 仮想アプライアンスの概要

シスコは、VMware vSphere と VMware vCloud Director のホスティング環境用に 64 ビット仮想 Firepower Management Center および仮想デバイスをパッケージ化しています。VMware vCenter または VMware vCloud Director を使用して、64 ビット Cisco Firepower Management Center Virtual および 64 ビット Cisco Firepower NGIPSv 管理対象デバイスを ESXi ホストに展開できます。仮想アプライアンスは e1000（1 Gbit/s）インターフェイスを使用します。また、デフォルトのインターフェイスを vmxnet3（10 Gbit/s）インターフェイスに置き換えることもできます。仮想アプライアンスのパフォーマンスと管理を向上させるために VMware ツールを使用することもできます。

Cisco Firepower Management Center Virtual は物理デバイスおよび Cisco ASA with FirePOWER Services（ASA FirePOWER）を管理でき、物理 Cisco Firepower Management Center は仮想デバイスを管理できます。ただし、仮想アプライアンスはシステムのハードウェア ベースの機能をサポートしません。具体的には、Cisco Firepower Management Center Virtual では高可用性がサポートされず、仮想デバイスではクラスタリング、スタッキング、スイッチング、ルーティングなどがサポートされません。物理 Firepower System アプライアンスの詳細については、『*Firepower System Installation Guide*』を参照してください。

このガイドでは、仮想 Firepower System アプライアンス（Firepower NGIPSv デバイスおよび Firepower Management Center Virtual）の展開、インストール、セットアップに関する情報を提供します。また、vSphere クライアント、VMware vCloud Director Web ポータル、VMware ツール（オプション）を含む VMware 製品の機能と名称について精通していることを想定しています。

動作環境の前提条件

次のホスティング環境で 64 ビットの仮想アプライアンスをホストできます。

- VMware ESXi 5.5（vSphere 5.5）
- VMware ESXi 5.1（vSphere 5.1）
- VMware vCloud Director 5.1

サポート対象のすべての ESXi バージョンで VMware ツールを有効化できます。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。ホスティング環境の構築については、VMware vCloud Director と VMware vCenter を含む VMware ESXi のドキュメントを参照してください。

仮想アプライアンスは Open Virtual Format（OVF）パッケージを使用します。VMware Workstation、Player、Server、および Fusion は OVF パッケージを認識しないため、サポートされません。また、仮想アプライアンスは、仮想ハードウェアのバージョン 7 の仮想マシンとしてパッケージ化されます。

ESXi ホストとして動作するコンピュータは、次の要件を満たす必要があります。

- 仮想化サポートとして、Intel® Virtualization Technology（VT）または AMD Virtualization™（AMD-V™）テクノロジのいずれかを実現する 64 ビット CPU が必要
- 仮想化は、BIOS 設定で有効化する必要がある
- 仮想デバイスをホストするために、コンピュータには Intel e1000 ドライバと互換性があるネットワーク インターフェイスが必要（PRO 1000MT デュアル ポート サーバ アダプタまたは PRO 1000GT デスクトップ アダプタなど）

詳細については、VMware の Web サイト http://www.vmware.com/resources/guides.html を参照してください。

作成する各仮想アプライアンスでは、ESXi ホストに一定量のメモリ、CPU、およびハードディスク スペースが必要です。デフォルトの設定は、システム ソフトウェアの実行の最小要件であるため、**減らさない**でください。ただし、使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。次の表に、デフォルトのアプライアンス設定を示します。

表 1 デフォルトの仮想アプライアンス設定

設定	デフォルト	設定調整の可否
メモリ	8GB	可
仮想 CPU	4	可。最大 8
ハード ディスク プロビジョニング サイズ	40GB（NGIPSv） 250GB（Firepower Management Center Virtual）	不可

仮想アプライアンスのパフォーマンス

仮想アプライアンスのスループットおよび処理能力を正確に予測することは不可能です。次のように、多数の要因がパフォーマンスに大きく影響します。

- ESXi ホストのメモリと CPU の容量
- ESXi ホストで実行されている仮想マシンの総数
- センシング インターフェイスの数、ネットワーク パフォーマンス、およびインターフェイス速度
- 各仮想アプライアンスに割り当てられたリソースの量
- ホストを共有する他の仮想アプライアンスのアクティビティのレベル
- 仮想デバイスに適用されるポリシーの複雑さ

（注） VMware は複数のパフォーマンス測定ツールとリソース割り当てツールを備えています。仮想アプライアンスを実行しながら、ESXi ホストでこれらのツールを使用し、トラフィックの監視とスループットの測定を行います。スループットに満足できない場合は、ESXi ホストを共有する仮想アプライアンスに割り当てられたリソースを調整します。

また、仮想アプライアンスのパフォーマンスと管理を向上させるために VMware ツールを有効にできます。あるいは、ホスト上、または仮想パフォーマンスを調べる ESXi ホストの仮想化管理レイヤ（ゲスト レイヤではなく）に、ツール（`esxtop` または VMware/サードパーティのアドオンなど）をインストールできます。VMware ツールを有効にするには、『*Firepower System Configuration Guide*』を参照してください。

注意事項と制約事項

VMware 向け Firepower NGIPSv の展開には次の制限事項があります。

- vMotion はサポートされません。
- 仮想マシンのクローニング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。

VMware 向け仮想アプライアンスのインストール パッケージ

シスコ は VMware ESXi ホスト環境用にパッケージ化した仮想アプライアンスを、圧縮アーカイブ（.tar.gz）ファイルとしてサポート サイトで提供します。シスコ 仮想アプライアンスは、仮想ハードウェアのバージョン 7 の仮想マシンとしてパッケージ化されています。各アーカイブには次のファイルが含まれています。

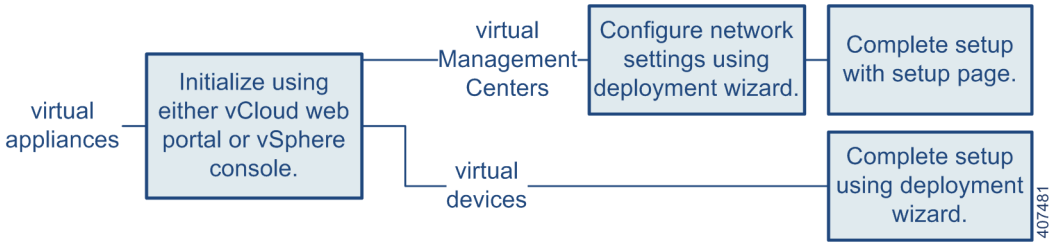
- ファイル名に -ESXi- が含まれている Open Virtual Format（.ovf）テンプレート
- ファイル名に -VI- が含まれている Open Virtual Format（.ovf）テンプレート
- ファイル名に -ESXi- が含まれているマニフェスト ファイル（.mf）
- ファイル名に -VI- が含まれているマニフェスト ファイル（.mf）
- 仮想マシン ディスク形式（.vmdk）

仮想アプライアンスは、仮想インフラストラクチャ（VI）または ESXi Open Virtual Format（OVF）テンプレートを使用して展開します。

- VI OVF テンプレートを使用して展開する場合、展開時にセットアップ ウィザードを使用して、Firepower Systemの必須設定（管理者アカウントのパスワードおよびアプライアンスをネットワーク上で通信可能にする設定など）を構成できます。VMware vCloud Director または VMware vCenter のいずれかの管理プラットフォームを使用して展開する必要があります。

VI OVF テンプレートの展開

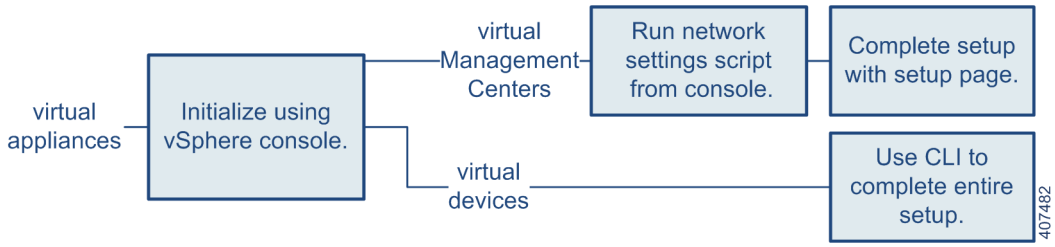
次の図は、VI OVF テンプレートを使用して展開する場合の、Firepower System 仮想アプライアンスの一般的な設定プロセスについて示しています。



- ESXi OVF テンプレートを使用して展開する場合、インストール後に仮想アプライアンスの VMware コンソールでコマンド ライン インターフェイス（CLI）を使用して設定を構成する必要があります。管理プラットフォーム（VMware vCloud Director または VMware vCenter）を使用して展開するか、スタンドアロン アプライアンスとして展開できます。

ESXi OVF テンプレートの展開

次の図は、ESXi OVF テンプレートを使用して展開する場合の、Firepower System 仮想アプライアンスの一般的な設定プロセスについて示しています。



インストール ファイルの取得

VMware 向けの Firepower System仮想アプライアンスをインストールする前に、サポート サイトから正しいアーカイブ ファイルを取得してください。シスコは、常に最新のパッケージを使用することを推奨します。仮想アプライアンスのパッケージは、通常、システム ソフト ウェアのメジャー バージョンに関連付けられています(たとえば 5.4 または 6.0 など)。

仮想アプライアンスのアーカイブ ファイルを取得するには:

1. Web ブラウザを使用して、シスコ サポート サイトの [Downloads] 領域(https://software.cisco.com/download/navigator.html)に移動します。
2. [Products] 領域でソフトウェアを参照するか、インストールするシステム ソフトウェアの名前を [Find] フィールドに入力します。

   たとえば Firepower のアーカイブ ファイルを検索するには、**Firepower** と入力します。
3. 次の命名規則を使用して、ダウンロードする Firepower System仮想アプライアンスのアーカイブ ファイルを検索します。

   `Cisco_Firepower_NGIPSv_VMware-X.X.X-xxx.tar.gz`
   `Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx.tar.gz`

   ここで、*X.X.X-xxx* は、ダウンロードするアーカイブ ファイルのバージョンとビルド番号を表します。
4. ダウンロードするアーカイブをクリックします。

   (注) サポート サイトにログインしている間、シスコ は、仮想アプライアンスの使用可能なすべての更新をダウンロードすることを推奨します。こうすることで、仮想アプライアンスをメジャー バージョンにインストールした後で、システム ソフトウェアを更新できるようになります。アプライアンスによってサポートされるシステム ソフトウェアの最新バージョンを常に実行する必要があります。Cisco Firepower Management Center Virtual の場合は、新しい侵入ルールと脆弱性データベース(VDB)の更新もダウンロードする必要があります。
5. vSphere クライアントまたは VMware vCloud Director Web ポータルを実行中のワークステーションまたはサーバからアクセス可能な場所に、アーカイブ ファイルをコピーします。

注意: アーカイブ ファイルを電子メールで転送しないでください。ファイルが破損することがあります。

6. 任意のツールを使用してアーカイブ ファイルの圧縮を解除し、インストール ファイルを抽出します。

   Cisco Firepower NGIPSv 仮想デバイスの場合:

   `Cisco_Firepower_NGIPSv_VMware-X.X.X-xxx-disk1.vmdk`
   `Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf`
   `Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.mf`
   `Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf`
   `Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.mf`

   Cisco Firepower Management Center Virtual の場合:

   `Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk`
   `Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf`
   `Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf`
   `Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf`
   `Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.mf`

   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。

   (注) 必ずすべてのファイルを同じディレクトリ内に保持してください。

次の作業

- Cisco Firepower NGIPSv：VMware 向け Cisco Firepower NGIPSv 展開（9 ページ）に進んで、仮想 Firepower System管理対象デバイスを展開します。
- Cisco Firepower Management Center Virtual：仮想 Firepower Management Center を展開する方法については、『*Cisco Firepower Management Center Virtual Quick Start Guide for VMware*』を参照してください。

VMware 向け仮想アプライアンスのインストール パッケージ

VMware 向け Cisco Firepower NGIPSv 展開

Cisco Firepower NGIPSv 仮想デバイスをインストールするには、プラットフォーム インターフェイス（VMware vCloud Director Web ポータルまたは vSphere クライアント）を使用して、管理プラットフォーム（VMware vCloud Director または VMware vCenter）に OVF（VI または ESXi）テンプレートを展開します。

- VI OVF テンプレートを使用して展開する場合、インストール時に Firepower Systemの必須設定を構成できます。この仮想アプライアンスは VMware vCloud Director または 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 System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 vCloud Director または VMware vCenter のどちらかを使用して管理するか、スタンドアロン アプライアンスとして使用できます。

計画した展開が前提条件（動作環境の前提条件（3 ページ）を参照）を満たしていることを確認し、必要なアーカイブ ファイルをダウンロードしたら、VMware vCloud Director Web ポータルまたは vSphere クライアントを使用して仮想アプライアンスをインストールします。

Cisco Firepower NGIPSv 仮想デバイスのインストールには、次のインストール オプションがあります。

```
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
Cisco_Firepower_NGIPSv_VMware-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。

OVF テンプレートの展開時に次の情報を指定します。

表 1 VMware OVF テンプレート

設定	ESXi または VI	操作
Import/Deploy OVF Template	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 Template Details	両方	インストールするアプライアンス（Cisco Firepower Threat Defense 仮想アプライアンス）と展開オプション（`VI` または `ESXi`）を確認します。
Accept EULA	VI のみ	OVF テンプレートに含まれるライセンス契約に同意します。
Name and Location	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。
Host / Cluster	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。
Resource Pool	両方	ホストまたはクラスタ内のコンピューティング リソースを有効な階層に設定して管理します。仮想マシンおよび子リソース プールは親リソース プールのリソースを共有します。
Storage	両方	仮想マシンに関連付けられたすべてのファイルを格納するデータストアを選択します。
Disk Format	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。
Network Mapping	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。
Properties	VI のみ	仮想マシンの初期設定をカスタマイズします。

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、Cisco Firepower NGIPSv 仮想デバイ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
- 初期検出モード
- 管理 Cisco Firepower Management Center

ESXi OVF テンプレートを使用して展開する場合、またはセットアップ ウィザードを使用する構成を選択しない場合、VMware コンソールを使用して仮想アプライアンスの初期設定を実行する必要があります。指定する構成に関するガイダンスなど、初期設定の実行の詳細については、VMware 向け Cisco Firepower Virtual の設定（17 ページ）を参照してください。

次のオプションのいずれかを使用して、仮想アプライアンスをインストールします。

- Cisco Firepower NGIPSv 仮想デバイスを VMware vCloud Director に展開する（VMware vCloud Director を使用した展開（10 ページ）を参照）。
- Cisco Firepower NGIPSv 仮想デバイスを VMware vCenter に展開する（VMware vSphere を使用した展開（11 ページ）を参照）。

VMware vCloud Director を使用した展開

VMware vCloud Director Web ポータルを使用すると、vApp テンプレートを使って Cisco Firepower NGIPSv 仮想デバイスを展開できます。展開に VMware vCloud Director を使用するには、組織とカタログを作成し、Cisco.com から取得した OVF パッケージをアップロードして、vApp テンプレートを使って Cisco Firepower NGIPSv を作成します。

仮想アプライアンス OVF パッケージのアップロード

Cisco Firepower NGIPSv 仮想デバイスの OVF パッケージを VMware vCloud Director 組織カタログにアップロードできます。

はじめる前に

- vApp テンプレートを含める組織とカタログを作成します。詳細については、『*VMware vCloud DirectorUser's Guide*』を参照してください。
- Cisco.com から OVF テンプレートをダウンロードします。インストール ファイルの取得（6 ページ）を参照してください。

手順

1. VMware vCloud Director Web ポータルで、[Catalogs] > *Organization* > [vApp Templates] を選択します。*Organization* は、vApp テンプレートを含める組織の名前です。
2. [vApp Templates media] タブで、アップロード アイコン（  ）をクリックします。
3. [OVF package] フィールドに、OVF パッケージの場所を入力するか、[Browse] をクリックして Cisco Firepower NGIPSv 仮想デバイスの OVF パッケージを参照します。

   `Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf`

   ここで、*X.X.X-xxx* は、アップロードする OVF パッケージのバージョンとビルド番号を表します。
4. 名前およびオプションで OVF パッケージの説明を入力します。
5. ドロップダウン リストから、vApp テンプレートを含める、仮想データセンター、ストレージ プロファイル、およびカタログを選択します。
6. [Upload] をクリックします。

次の作業

- vApp テンプレートから仮想デバイスを作成します。vApp テンプレートの使用（11 ページ）を参照してください。

vApp テンプレートの使用

vApp テンプレートを使用して Cisco Firepower NGIPSv 仮想デバイスを作成し、セットアップ ウィザードを使用したインストール時に Firepower Systemの必須設定を構成できます。

手順

1. VMware vCloud Director Web ポータルで、[My Cloud] > [vApps] を選択します。
2. [vApps media] タブで、追加アイコン（➕）をクリックし、カタログから vApp を追加します。
3. テンプレートのメニュー バーの [All Templates] をクリックします。
4. 追加する vApp テンプレートを選択し、Cisco Firepower NGIPSv 仮想デバイスの説明を表示します。

   `Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf`

   ここで、*X.X.X-xxx* は、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。
5. EULA を読んで同意します。
6. 名前およびオプションで vApp の説明を入力します。
7. [Configure Resources] 画面で、仮想データセンターを選択し、システム名を入力して（またはデフォルトのシステム名を使用して）、ストレージ プロファイルを選択します。
8. 外部、管理、および内部の送信元に対する宛先と IP の割り当てを選択することにより、OVF テンプレートで使用されるネットワークをインベントリのネットワークにマッピングします。
9. オプションで、セットアップ ウィザードで Firepower System の必須設定を入力し、[Custom Properties] 画面でアプライアンスの初期設定を実行します。初期設定をすぐに実行しない場合、VMware 向け Cisco Firepower Virtual の設定（17 ページ）の手順を使用して、後で行うことができます。
10. 設定を確認し、[Finish] をクリックします。

    （注） 仮想デバイスの [Power on after deployment] オプションを有効化**しない**でください。センシング インターフェイスをマッピングする必要があります。必ず、アプライアンスの電源を投入する前にセンシング インターフェイスが接続するように設定してください。詳細については、仮想アプライアンスの初期化（17 ページ）を参照してください。

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（13 ページ）を参照してください。

VMware vSphere を使用した展開

VMware vSphere vCenter、vSphere クライアント、vSphere Web クライアント、または vSphere Hypervisor（スタンドアロン ESXi 展開の場合）を使用して、Cisco Firepower NGIPSv 仮想デバイスを展開できます。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 または VMware vCloud Director で管理する必要があります。
- OVF ESXi テンプレートを使用して展開する場合、アプライアンスを VMware vCenter または VMware vCloud Director で管理するか、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 Systemの必須設定を構成する必要があります。

はじめる前に

- Cisco.com から OVF テンプレートをダウンロードします。インストール ファイルの取得（6 ページ）を参照してください。

手順

1. vSphere クライアントを使用して、[File] > [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 ファイルを展開します。
2. ドロップダウン リストから、Cisco Firepower NGIPSv 仮想デバイスに展開する OVF テンプレートを 1 つ選択します。

   ```
   Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
   Cisco_Firepower_NGIPSv_VMware-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 Template Details] ページを確認して、[Next] をクリックします。
4. ライセンス契約書が OVF テンプレートにパッケージ化されている場合（VI テンプレートのみ）、[End User License Agreement] ページが表示されます。ライセンス契約に同意して [Next] をクリックします。
5. 名前を編集し、Firepower Threat Defense 仮想アプライアンス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、[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 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て、[Next] をクリックします。
7. Firepower Threat Defense 仮想アプライアンスを実行するリソース プールに移動して選択し、[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ストレージの場所を選択し、[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ディスク形式を選択し、[Next] をクリックします。

   [Thick Provisioned] を選択すると、すべてのストレージがすぐに割り当てられます。[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。
10. [Network Mapping] 画面で、NGIPSv 管理インターフェイスと 2 つのセンシング インターフェイス（内部および外部）を VMware ネットワークに関連付けます。

    OVF テンプレートで指定される各ネットワークに対して、インフラストラクチャの [Destination Networks] 列を右クリックしてネットワークを選択し、Cisco Firepower NGIPSv の各インターフェイスにネットワーク マッピングを設定して [Next] をクリックします。

    Firepower Management Center から到達可能な VM ネットワークに管理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。
11. 管理 Firepower Management Center の [Detection Mode] や [Registration] 情報など、ユーザ設定可能なプロパティが OVF テンプレートにパッケージ化されている場合（VI テンプレートのみ）、設定可能なプロパティを設定して [Next] をクリックします。
12. [Ready to Complete] ウィンドウで設定を確認します。
13. 設定を確認したら [Finish] をクリックします。

(注) 仮想アプライアンスの [Power on after deployment] オプションを有効にしないでください。センシング インターフェイスをマッピングする必要があります。必ず、アプライアンスの電源を投入する前にセンシング インターフェイスが接続するように設定してください。詳細については、仮想アプライアンスの初期化(17 ページ)を参照してください。

14. インストールが完了したら、ステータス ウィンドウを閉じます。
15. ウィザードが完了すると、vSphere Web Client は VM を処理します。[Recent Tasks] ペインの [Global Information] 領域で [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 Cisco Firepower NGIPSv 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、最長で 30 分かかる場合があります。

    (注) Cisco Licensing Authority に Cisco Firepower NGIPSv を正常に登録するために、Cisco Firepower NGIPSv はインターネット アクセスを必要とします。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(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。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。ただし、使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。次の表に、デフォルトのアプライアンス設定を示します。

図 1 デフォルトの仮想アプライアンス設定

設定	デフォルト	設定調整の可否
メモリ	8GB	可
仮想 CPU	4	可。最大 8
ハード ディスク プロビジョニング サイズ	40GB (NGIPSv)	不可

仮想マシンのプロパティの確認

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
いずれか(Any)	いずれか(Any)	いずれか(Any)	いずれか(Any)	Admin

選択した仮想マシンのホスト リソース割り当てを調整するには、[VMware Virtual Machine Properties] ダイアログボックスを使用します。このタブでは、CPU、メモリ、ディスク、および拡張 CPU リソースを変更できます。仮想マシンの仮想イーサネット アダプタ設定については、電源投入接続設定、MAC アドレス、およびネットワーク接続を変更することもできます。

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. デフォルトの仮想アプライアンス設定（13 ページ）に示すように、[Memory]、[CPUs]、および [Hard disk 1] の設定がデフォルト値以上になっていることを確認します。

   アプライアンスのメモリ設定および仮想 CPU の数は、ウィンドウの左側に表示されます。ハード ディスクの**プロビジョニング サイズ**を表示するには、[Hard disk 1] をクリックします。
3. オプションで、ウィンドウの左側の適切な設定をクリックしてメモリと仮想 CPU の数を増やし、ウィンドウの右側で変更します。
4. [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. [Device Status] の下で、[Connect at power on] チェック ボックスを有効にします。
   b. [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、シスコからのライセンスを再要求する必要がなくなります。
   c. [Network Connection] の下で、[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。
5. [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（17 ページ）を参照してください。
- 必要に応じて、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。インターフェイスの追加と構成（14 ページ）を参照してください。

インターフェイスの追加と構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
いずれか（Any）	いずれか（Any）	NGIPSv	いずれか（Any）	Admin

デフォルトの e1000（1 Gbit/s）インターフェイスを vmxnet3（10 Gbit/s）インターフェイスに置き換えるには、e1000 インターフェイスのすべてを削除して、vmxnet3 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シング インターフェイスと管理インターフェイスは同じである必要があります（e1000 または vmxnet3 のいずれか）。**

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には、まず、vSphere クライアントを使用して既存の e1000 インターフェイスを削除した後、新しい vmxnet3 インターフェイスを追加し、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。

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の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。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するには、vSphere クライアントを使用します。

vSphere クライアントの使用に関する詳細については、VMware の Web サイト（http://vmware.com）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 System Configuration Guide*』の「Managing Devices」を参照してください。

（注） アプライアンスをオンにする前に、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、Firepower Management Center から登録解除し、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ます。その後、新しいインターフェイスを追加してアプライアンスの電源をオンにしてから、Firepower Management Center に再登録します。

仮想デバイスのセンシング インターフェイスの設定

Cisco Firepower NGIPSv 仮想デバイスのセンシング ンターフェイスは、無差別モードを受け入れる ESXi ホスト仮想スイッチ上のポートにネットワーク接続する必要があります。

（注） 仮想スイッチにポート グループを追加し、無差別モードの仮想ネットワーク接続を実稼動トラフィックから分離します。ポート グループの追加とセキュリティ属性の設定の詳細については、VMware のマニュアルを参照してください。

手順

1. vSphere クライアント を使用してサーバにログインし、サーバの [Configuration] タブをクリックします。

   [Hardware] 選択リストと [Software] 選択リストが表示されます。
2. [Hardware] リストで、[Networking] をクリックします。
3. 仮想デバイスのセンシング インターフェイスを接続するスイッチおよびポート グループの [Properties] をクリックします。
4. [Switch Properties] ポップアップ ウィンドウで、[Edit] をクリックします。
5. [Detailed Properties] ポップアップ ウィンドウで、[Security] タブを選択します。

   [Policy Exceptions] > [Promiscuous Mode] の下で、無差別モードが [Accept] に設定されていることを確認します。

   （注） 仮想環境で VLAN トラフィックを監視するには、無差別ポートの VLAN ID を 4095 に設定します。
6. 変更を保存します。

   仮想アプライアンスが初期化できる状態になります。

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（17 ページ）を参照してください。

インストール後の設定

VMware 向け Cisco Firepower Virtual の設定

シスコ Firepower System仮想アプライアンスをインストールしたら、設定プロセスを完了する必要があります。これにより、新しいアプライアンスは信頼された管理ネットワーク上で通信できるようになります。また、管理者パスワードを変更し、エンドユーザ ライセンス契約書(EULA)に同意する必要もあります。

設定プロセスにより、時間の設定、デバイスの登録とライセンシング、更新のスケジューリングなど、管理レベルの多数の初期タスクを実行することもできます。設定と登録中に選択されたオプションによって、システムで作成され、適用されるデフォルト インターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

これらの初期設定およびポリシーの目的は、オプションを制限することなく、優れたユーザ体験を提供し、迅速に展開できるようにすることです。仮想アプライアンスをどのように初期設定したかに関係なく、設定は Cisco Firepower Management Center を使用することでいつでも変更できます。つまり、たとえば、設定中に検出モード またはアクセス制御ポリシーを選択しても、特定のデバイス、ゾーン、またはポリシー設定に固定されません。

どのように展開する場合でも、最初に、初期化するアプライアンスの電源を入れてください。初期化が完了したら、VMware コンソールを使用してログインし、アプライアンスのタイプに応じて次のいずれかの方法で設定を完了します。

Cisco Firepower NGIPSv

Cisco Firepower NGIPSv 仮想アプライアンスには Web インターフェイスがありません。VI OVF テンプレートで展開すると、展開ウィザードを使用して初期設定(アプライアンスの Firepower Management Center への登録など)を実行できます。ESXi OVF テンプレートで展開する場合は、対話式のコマンドライン インターフェイス(CLI)を使用して初期設定を実行する必要があります。

Cisco Firepower Management Center Virtual

VI OVF テンプレートで展開すると、展開でウィザードを使用してネットワークを設定することができます。セットアップ ウィザードを使用しない、または ESXi OVF テンプレートを使用して展開することを選択した場合は、スクリプトを使用してネットワークを設定します。ネットワークを設定した後で、管理ネットワーク上のコンピュータを使用して、Cisco Firepower Management Center の Web インターフェイスを参照するための設定プロセスを完了します。

(注) 複数のアプライアンスを展開している場合は、先に Firepower NGIPSv アプライアンスを設定してから、管理元の Firepower Management Center を設定します。デバイスの初期設定プロセスを使用すれば、デバイスを Firepower Management Center に事前登録できます。Firepower Management Center の設定プロセスを使用すれば、事前登録した管理対象デバイスを追加してライセンス認証できます。

仮想アプライアンスの初期化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
いずれか(Any)	いずれか(Any)	いずれか(Any)	いずれか(Any)	Admin

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. 以下のようにして、アプライアンスの電源をオンにします。
   - VMware vCloud Director の Web ポータルで、ディスプレイから [vApp] を選択して [Start] をクリックします。
   - vSphere クライアントで、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 [Power] > [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 System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。

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 Systemの必須設定を行わなかった場合は、CLI を使用した Firepower NGIPSv デバイスの設定（18 ページ）に進みます。

CLI を使用した Firepower NGIPSv デバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
いずれか（Any）	いずれか（Any）	NGIPSv	いずれか（Any）	Admin

Firepower NGIPSv デバイスには 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 テンプレートでの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は、CLI を使用して Firepower Systemの必須設定を行うこともできます。

（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検出モードを設定します。

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

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 System Installation Guide*』を参照してください。

（注） 初期設定の完了後の仮想デバイスのこれらの設定を変更するには、CLI を使用します。詳細については、『*Firepower System Configuration Guide*』の「Command Line Reference」の章を参照してください。

デバイス ネットワークの設定について

Firepower Systemは、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。ユーザは IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィクスの長さ、およびデフォルトのゲートウェイを設定する必要があります。また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。デバイスを再起動するまで、ホスト名は syslog に反映されないので注意してください。

検出モードについて

仮想デバイスに対して検出モードを選択すると、システムが最初にデバイス インターフェイスをどのように設定するか、およびこれらのインターフェイスがインライン セットとセキュリティ ゾーンのどちらに属するかが決定されます。検出モードはユーザが後から変更できない設定で、設定時にユーザが選択するだけのオプションです。このオプションの選択により、システムはデバイスの初期設定を調整して行うことができます。一般的には、デバイスがどのように展開されているかに基づいて検出モードを選択する必要があります。

パッシブ

デバイスがパッシブ展開されている場合は、このモードを侵入検知システム（IDS）として選択します。パッシブ展開では、仮想デバイスは、ネットワーク ベース ファイルとマルウェアの検出、セキュリティ インテリジェンス モニタリング、およびネットワーク検出を実行できます。

インライン

デバイスがインラインで展開されている場合は、このモードを侵入防御システム（IPS）として選択します。

（注） IPS 展開の一般的な方法はフェール オープンにし、一致しないトラフィックを許可することですが、仮想デバイスのインライン セットにはバイパス機能がありません。

アクセス コントロール

デバイスがアクセス制御展開の一部としてインライン展開されている場合、つまり、アプリケーション、ユーザ、および URL 制御を実行する場合に、このモードを選択します。アクセス制御を実行するように設定されているデバイスは、通常、フェールクローズであり、一致しないトラフィックをブロックします。ルールで、通過させるトラフィックが明示的に指定されます。

アクセス制御の展開では、高度なマルウェア対策、ファイル制御、セキュリティ インテリジェンス フィルタリング、およびネットワーク検出も実行できます。

ネットワーク ディスカバリ

デバイスがパッシブ展開されている場合は、ホスト、アプリケーション、およびユーザ ディスカバリのみを実行するためにこのモードを選択します。

次の表に、選択された検出モードに基づいてシステムが作成するインターフェイス、インライン セット、およびゾーンを示します。

表 1　検出モードに基づく初期設定

検出モード	セキュリティ ゾーン	インライン セット	インターフェイス
インライン	内部と外部	デフォルト インライン セット	デフォルト インライン セットに追加された最初のペア：内部ゾーン向けの 1 つと外部ゾーン向けの 1 つ
パッシブ	パッシブ	none	パッシブ ゾーンに割り当てられた最初のペア
アクセス コントロール	none	none	none
ネットワーク ディスカバリ	パッシブ	none	パッシブ ゾーンに割り当てられた最初のペア

セキュリティ ゾーンは Firepower Management Center レベルの設定であり、ユーザが実際にデバイスをFirepower Management Center に追加するまで作成されないことに注意してください。その時点で、Firepower Management Center 上に適切なゾーン（内部、外部、またはパッシブ）がすでに存在している場合、システムは一覧で示されたインターフェイスを既存のゾーンに追加します。ゾーンが存在しない場合は、システムがそれを作成してインターフェイスを追加します。インターフェイス、インライン セット、およびセキュリティ ゾーンの詳細については、『*Firepower System Configuration Guide*』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、仮想デバイ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 を読むように要求されます。
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） シスコ 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. デバイスのネットワーク設定を構成します。最初に IPv4 管理設定を構成（または無効に）してから、IPv6 に移ります。ネットワーク設定を手動で指定する場合は、次の手順を実行する必要があります。
   - ネットマスクを含む IPv4 アドレスをドット付き 10 進形式で入力します。たとえば、`255.255.0.0` のネットマスクを指定できます。
   - IPv6 アドレスをコロン区切りの 16 進形式で入力します。IPv6 プレフィックスの場合、ビット数を指定します（たとえば、`112` のプレフィックス長）。

   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。
6. デバイスの展開方法に基づいて検出モードを指定します。

   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。

次の作業

- 次のCisco Firepower Management Centerへの仮想デバイスの登録（20 ページ）へ進み、CLI を使用してデバイスをその管理元となる Cisco Firepower Management Center に登録します。デバイスは Cisco Firepower Management Center を使用して管理する必要があります。今すぐデバイスを登録しない場合は、後でデバイスにログインしてそれを登録するまで Cisco Firepower Management Center に追加できません。

Cisco Firepower Management Centerへの仮想デバイスの登録

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
いずれか（Any）	いずれか（Any）	NGIPSv	いずれか（Any）	Admin CLI Configuration

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(物理または仮想の両方)。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) vSphere クライアントを使用して仮想デバイスを Firepower Management Center へ登録する場合は、管理元の Firepower Management Center の(ホスト名ではなく)IP アドレス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いる場合は、登録キーと一緒に一意の NAT ID を入力し、IP アドレスの代わりに `DONTRESOLVE` を指定します。たとえば次のようにします。

```
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 を登録キーと一緒に入力し、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、デバイスの管理 IP アドレスまたはホスト名に対する SSH を使用してログインします。
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。
- *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。

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、[Device Management] ページ（[Devices] > [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 System Configuration Guide*』の「Managing Devices」の章を参照してください。
- Firepower Management Center をまだ設定していない場合、仮想 Firepower Management Center については『*Cisco Firepower Management Center Virtual Quick Start Guide for VMware*』、物理 Firepower Management Center については『*Cisco Firepower Management Center Installation Guide*』を参照してください。

VMware ツールの有効化

VMware ツールは仮想マシンのオペレーティング システム上にインストールされるユーティリティのスイートで、仮想マシンのパフォーマンスを向上させ、VMware 製品で使い勝手のよい多数の機能を実現します。システムはすべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールのサポートされるプラグインおよびすべての機能の詳細については、VMware Web サイト（http://www.vmware.com/）を参照してください。

仮想アプライアンスを設定した後、管理対象デバイスでコマンド ライン インターフェイス（CLI）を使用して、仮想アプライアンスの VMware ツールを有効化できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
いずれか（Any）	いずれか（Any）	NGIPSv	いずれか（Any）	Admin

仮想デバイスにログインし、次のコマンドの 1 つ以上を入力できます。

- `show vmware-tools` は、VMware ツールがシステム上で実行されているかどうかを表示します。
- `configure vmware-tools enable` </code> は、仮想デバイスで VMware ツールを有効にします。
- `configure vmware-tools disable` は、仮想デバイスで VMware ツールを無効にします。

仮想デバイスで VMware ツールを有効にするには：

1. コンソールで仮想デバイスにログインし、CLI プロンプトで、VMware ツールを有効または無効にするコマンド、あるいは、VMware ツールが有効であるかどうかを表示するコマンドを入力して、**Enter** を押します。

次の手順

仮想アプライアンスの初期設定プロセスが完了し、正常に終了したことが確認できたら、シスコ では、展開での管理を容易にするためのさまざまな管理タスクを完了することを推奨しています。また、デバイスの登録やライセンスの取得など、初期設定で省略したタスクも完了する必要があります。以降の項で説明するタスクの詳細と、展開の設定を開始する方法については、『*Firepower System Configuration Guide*』を参照してください。

個々のユーザ アカウント

初期セットアップを完了した時点で、システム上には管理者ロールおよびアクセス権を持つ admin ユーザしか存在しません。このロールを持つユーザには、すべてのメニューが表示され、システムへの設定アクセス（シェルまたは CLI の使用も含む）が可能です。シスコでは、セキュリティ上および監査上の理由で、admin アカウント（および管理者ロール）の使用を制限することを推奨します。

システムを使用するユーザごとに個別のアカウントを作成することで、各ユーザが行う操作および変更を監査するだけでなく、各ユーザに関連付けるユーザ アクセス ロールを制限することができます。これは、設定と分析タスクのほとんどを実行する Cisco Firepower Management Center では特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベント データにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。

システムには、さまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。また、特別なアクセス権限を持つカスタム ユーザ ロールを作成することもできます。

ヘルス ポリシーとシステム ポリシー

デフォルトでは、すべてのアプライアンスにシステムの初期ポリシーが適用されます。システム ポリシーは、メール リレー ホストのプリファレンスや時間同期の設定など、展開内の複数のアプライアンスで共通している可能性が高い設定を管理します。シスコ では、Firepower Management Center を使用して、防御センター自身およびその管理対象デバイスすべてに同じシステム ポリシーを適用することを推奨しています。

デフォルトで、Firepower Management Center にはヘルス ポリシーも適用されます。ヘルス ポリシーは、ヘルス モニタリング機能の一部として、システムが展開環境内でアプライアンスのパフォーマンスを継続して監視するための基準を提供します。シスコ では、Firepower Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアおよびデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。シスコ では、展開環境内のすべてのアプライアンスが Firepower System の最新のバージョンを実行することを推奨しています。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。

注意：Firepower System のいずれかの部分を更新する前に、更新に付属のリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。リリース ノートには、サポートされるプラットフォーム、互換性、前提条件、警告、および特定のインストールとアンインストールの手順などの重要な情報が記載されています。

次の手順

VMware 向け Cisco Firepower 仮想アプライアンスの展開例

仮想デバイスと仮想 Cisco Firepower Management Center を使用することによって、物理アセットおよび仮想アセット両方の保護機能を強化するために、仮想環境内にセキュリティ ソリューションを展開できます。仮想デバイスと仮想 Cisco Firepower Management Center によって、VMware プラットフォームにセキュリティ ソリューションを簡単に実装することができます。また仮想デバイスによって、リソースが制限されることのあるリモート サイトでのデバイスの展開および管理が行いやすくなります。

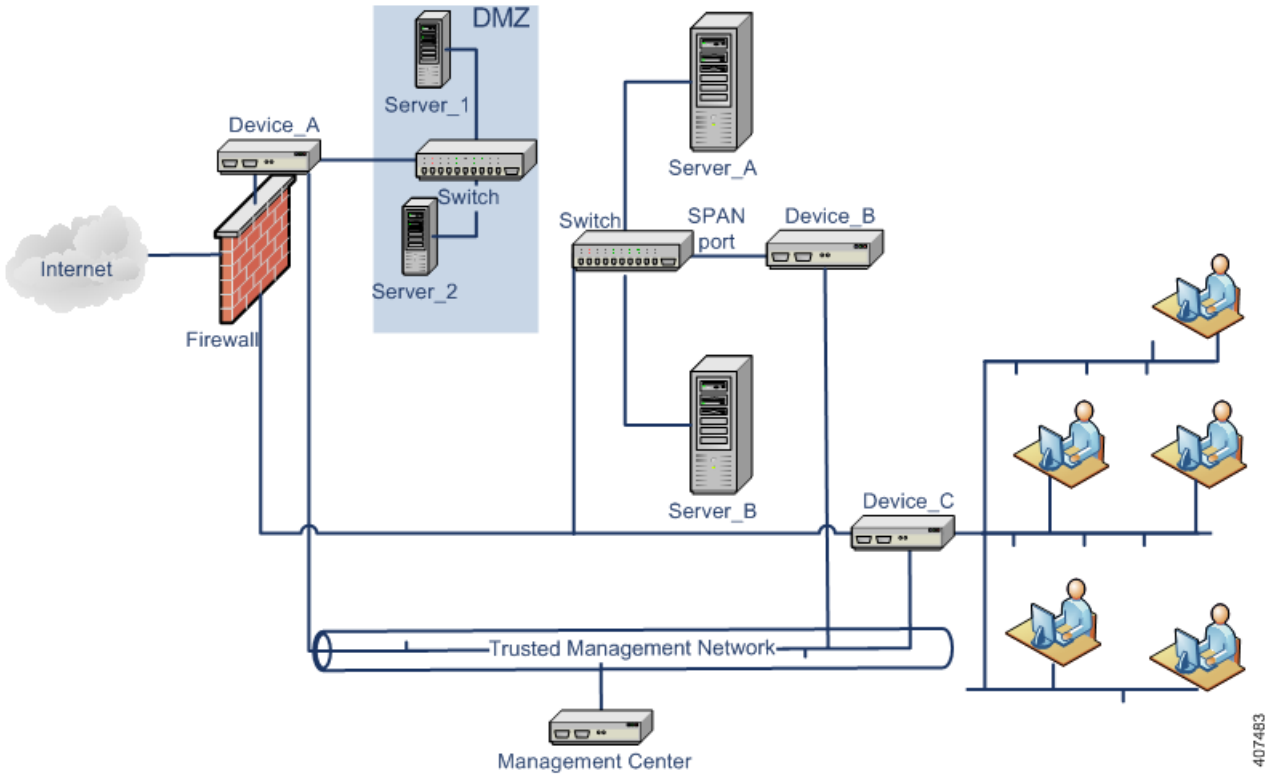
以下に示す例では、物理または仮想デバイスを管理するために物理または仮想 Cisco Firepower Management Center を使用できます。IPv4 または IPv6 ネットワーク上に展開できます。また、Cisco Firepower Management Center に複数の管理インターフェイスを設定することにより、2 つの異なるネットワークを分離して監視したり、単一ネットワークの内部トラフィックとイベント トラフィックを分離することもできます。仮想デバイスは複数の管理インターフェイスをサポートしていないことに注意してください。

パフォーマンスを向上するため、または 2 つの異なるネットワーク上のトラフィックを別個に管理するため、仮想 Cisco Firepower Management Center に 2 つ目の管理インターフェイスを設定できます。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、追加のインターフェイスおよび追加の仮想スイッチを設定します。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する方法については、VMware vSphere（http://vmware.com）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 System Configuration Guide*』の「Managing Devices」を参照してください。

注意: シスコでは、異なるネットワーク セグメントに、実稼働ネットワーク トラフィックおよび信頼できる管理ネットワーク トラフィックを保持することを強く推奨します。予防措置を講じて、アプライアンスおよび管理トラフィックのデータ ストリームのセキュリティを確保する必要があります。

一般的な Firepower System の展開

物理アプライアンス環境では、一般的な Firepower System の展開では、物理デバイス、物理 Cisco Firepower Management Center が使用されます。次の図に、展開例を示します。次に示すように、Device_A および Device_C をインライン構成で、Device_B をパッシブ構成で展開できます。



1 個のスイッチ ポート（または VLAN 全体）に表示されるネットワーク パケットのコピーをネットワーク モニタリング接続に送信するように、ほとんどのネットワーク スイッチでポート ミラーリングを構成できます。また、ポート ミラーリング（ネットワーク機器の大手プロバイダーでは「スイッチ ポート アナライザ（SPAN）」とも呼ばれる）によって、ネットワーク トラフィックを監視することができます。Device_B が Server_A と Server_B の間のトラフィックを、Server_A と Server_B の間のスイッチ上の SPAN ポートを介して監視することに注意してください。

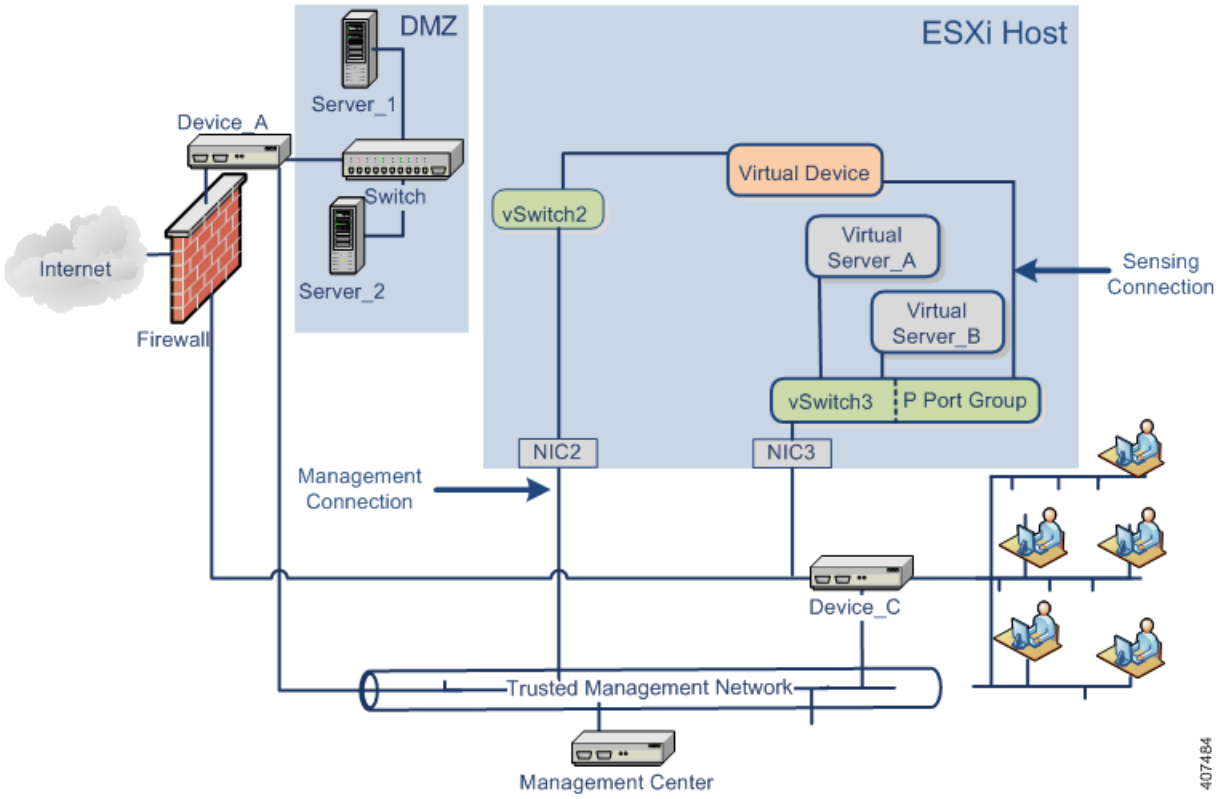
VMware での仮想 Firepower アプライアンスの展開

仮想化と仮想デバイスの追加

仮想インフラストラクチャを使用して、一般的な Firepower System の展開（25 ページ）の物理内部サーバを置き換えることができます。以下の例では、ESXi ホストを使用して、Server_A と Server_B を仮想化できます。

仮想デバイスを使用して、Server_A と Server_B の間のトラフィックを監視することができます。

仮想デバイスのセンシング インターフェイスは、次のように、無差別モードのトラフィックを受け入れるスイッチまたはポート グループに接続する必要があります。



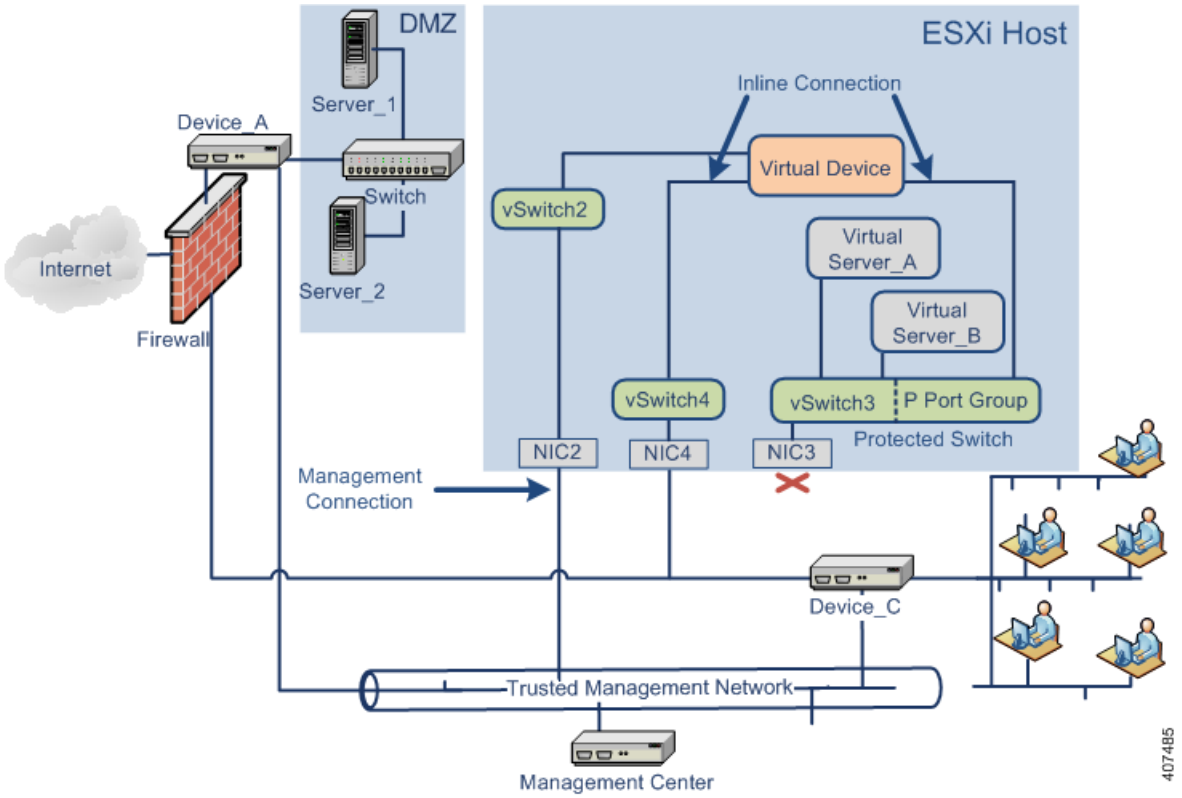
(注) すべてのトラフィックを検知するには、デバイスのセンシング インターフェイスが接続される仮想スイッチまたはポート グループで無差別モードのトラフィックを許可します。仮想デバイスのセンシング インターフェイスの設定 (15 ページ) を参照してください。

この例では、1 つのセンシング インターフェイスしか示されていませんが、デフォルトで 2 つのセンシング インターフェイスを仮想デバイスで使用できます。仮想デバイスの管理インターフェイスは、信頼できる管理ネットワークと Cisco Firepower Management Center に接続します。

インライン検出用の仮想デバイスの使用

仮想デバイスのインライン インターフェイス セットを介してトラフィックを渡すことによって、仮想サーバの周りに安全な境界を設けることができます。このシナリオは、一般的な Firepower System の展開 (25 ページ) および仮想化と仮想デバイスの追加 (26 ページ) で示された例に基づいています。

まず、保護された仮想スイッチを作成し、そのスイッチを仮想サーバに接続します。次に、仮想デバイスを通じて保護されているスイッチを外部ネットワークに接続します。詳細については、『*Firepower System Configuration Guide*』を参照してください。



(注) すべてのトラフィックを検知するには、デバイスのセンシング インターフェイスが接続される仮想スイッチまたはポート グループで無差別モードのトラフィックを許可します。仮想デバイスのセンシング インターフェイスの設定 (15 ページ) を参照してください。

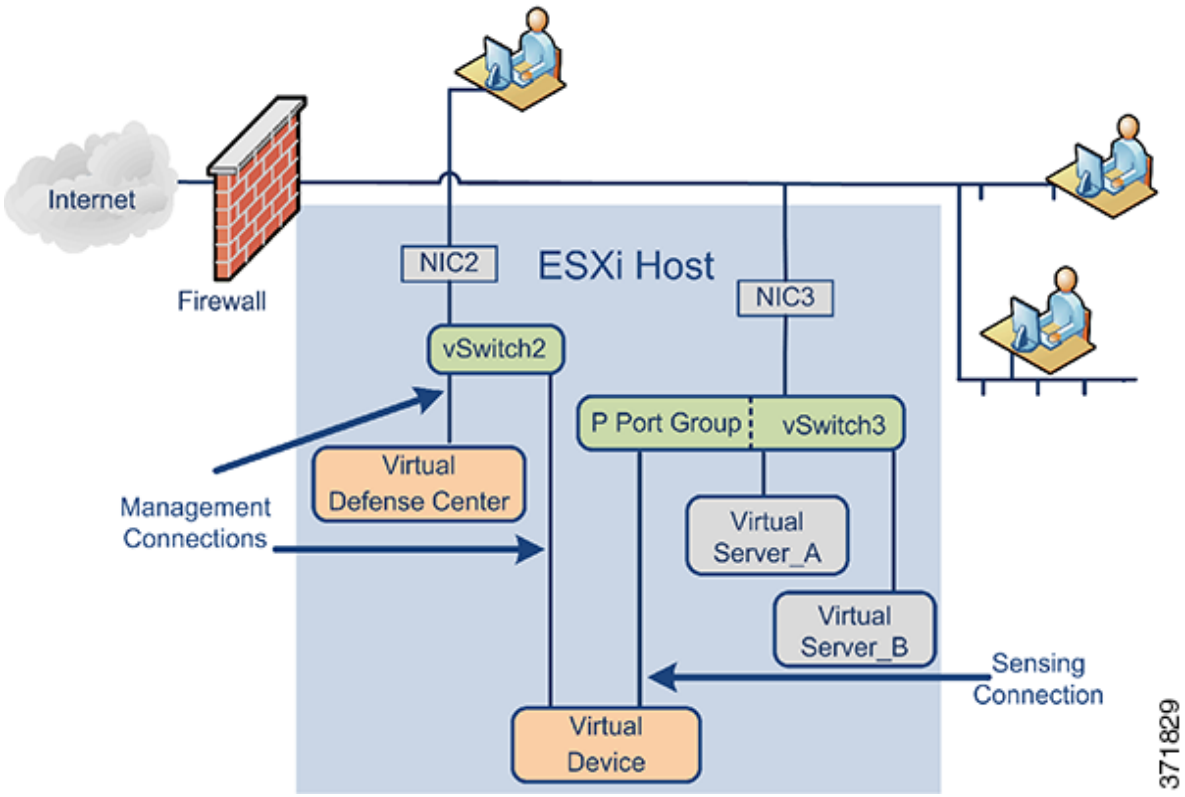
仮想デバイスは、侵入ポリシーに応じて、Server_A および Server_B への悪意のあるトラフィックを監視し、ドロップします。

Cisco Firepower Management Center Virtual の追加

次に示すように、ESXi ホストに Cisco Firepower Management Center Virtual を展開し、仮想ネットワークおよび物理ネットワークに接続できます。このシナリオは、一般的な Firepower System の展開 (25 ページ) および インライン検出用の仮想デバイスの使用 (27 ページ) で示された例に基づいています。

Firepower Management Center Virtual から NIC2 を経由した信頼できる管理ネットワークへの接続により、Firepower Management Center Virtual は物理デバイスと仮想デバイスの両方を管理できます。

シスコの仮想アプライアンスは必要なアプリケーション ソフトウェアで事前に構成されているため、ESXi ホストに展開したら、すぐに実行できます。これにより、ハードウェアとソフトウェアの複雑な互換性の問題は軽減され、展開を迅速化し、Firepower System のメリットに集中できます。次に示すように、ESXi ホスト上に仮想サーバ、Firepower Management Center Virtual、および仮想デバイスを展開し、Firepower Management Center Virtual からその展開を管理することができます。

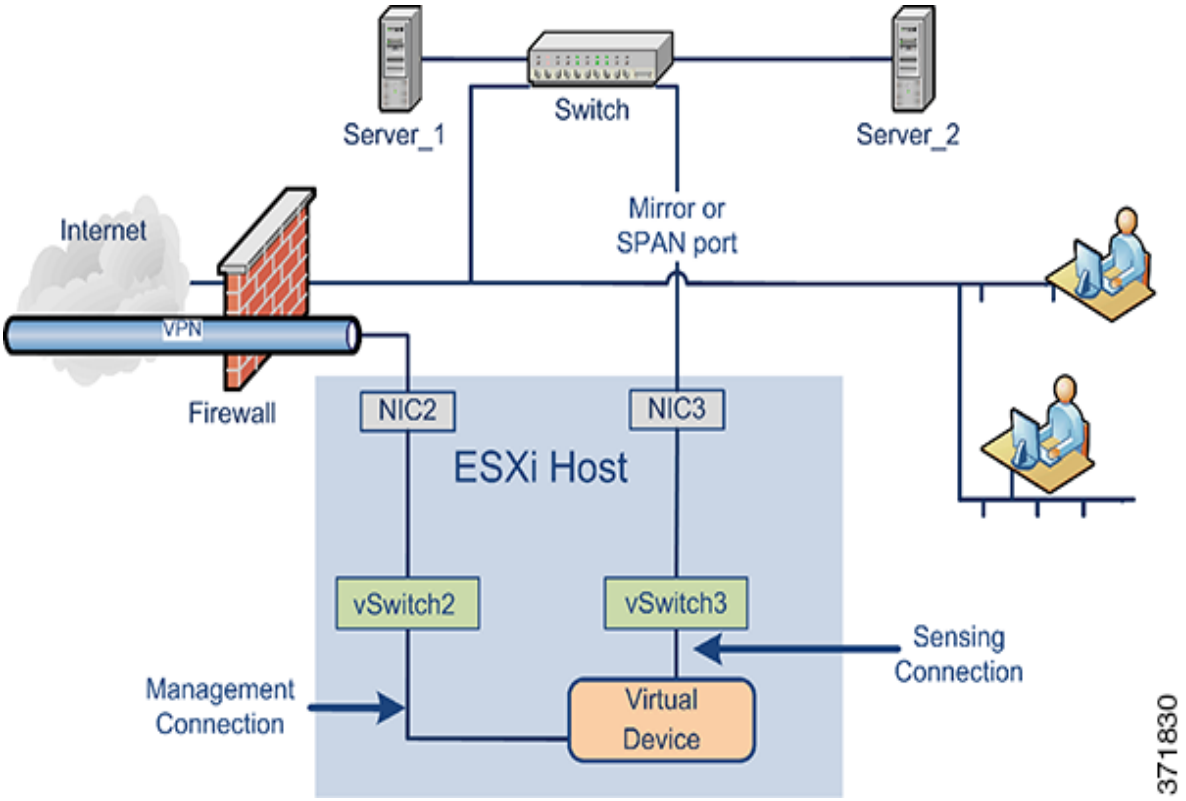


仮想デバイスのセンシング接続でのネットワーク トラフィックの監視を許可する必要があります。仮想インターフェイスを接続する仮想スイッチ、またはそのスイッチ上のポート グループは、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスに、他のマシンまたはネットワーク デバイス宛のパケットの読み取りを許可します。この例では、P ポート グループが、無差別モードのトラフィックを受け入れるように設定されています。仮想デバイスのセンシング インターフェイスの設定（15 ページ）を参照してください。

仮想アプライアンスの管理接続のほうがより一般的な差別モード接続です。仮想 Firepower Management Center によって、仮想デバイスのコマンドと制御が提供されます。ESXi ホストのネットワーク インタフェース カード（この例の NIC2）による接続によって、仮想 Firepower Management Center にアクセスできます。Firepower Management Center Virtual および仮想デバイスの管理接続のセットアップについては『*Cisco Firepower Management Center Virtual Quick Start Guide for VMware*』とCLI を使用した Firepower NGIPSv デバイスの設定（18 ページ）を参照してください。

リモート オフィス展開の使用

仮想デバイスでは、リソースが限られているリモート オフィスを監視するのが理想的です。次に示すように、ESXi ホストに仮想デバイスを展開し、ローカル トラフィックを監視できます。



仮想デバイスのセンシング接続でのネットワーク トラフィックの監視を許可する必要があります。これを実行するには、センシング インターフェイスを接続する仮想スイッチ、またはそのスイッチ上のポート グループで、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスに、他のマシンまたはネットワーク デバイス宛のパケットの読み取りを許可します。この例では、vSwitch3 のすべてが、無差別モードのトラフィックを受け入れるように設定されています。また、VSwitch3 は、トラフィックがリモート オフィスのスイッチを通過する際に、そのトラフィックを監視できるように、NIC3 を経由して SPAN ポートに接続されます。仮想デバイスのセンシング インターフェイスの設定（15 ページ）を参照してください。

仮想デバイスは、Firepower Management Center によって管理される必要があります。ESXi ホストのネットワーク インタフェース カード（この例の NIC2）による接続によって、リモート Firepower Management Center を使用する仮想デバイスにアクセスできます。

さまざまな地理的位置にデバイスを展開する場合、デバイスおよびデータ ストリームのセキュリティを確保するため、保護されていないネットワークからデバイスを隔離することによって、予防措置を講じる必要があります。これは、VPN または別のセキュアなトンネリング プロトコル上で、デバイスからデータ ストリームを送信することによって実現できます。仮想デバイスの管理接続の設定の詳細については、CLI を使用した Firepower NGIPSv デバイスの設定（18 ページ）を参照してください。

VMware 向け Cisco Firepower 仮想アプライアンスのトラブルシューティング

ここでは、最も一般的な設定に関する問題、および質問の送り先とサポートを受けるための連絡先について説明します。

時刻の同期

仮想アプライアンスのクロック設定が同期されていないことがヘルス モニタに示された場合は、システム ポリシーの時間の同期設定を確認してください。シスコ では、仮想アプライアンスを物理 NTP サーバに同期することを推奨しています。(仮想または物理)管理対象デバイスを仮想 Cisco Firepower Management Center と同期しないでください。時間の同期が正しく設定されていることを確認するには、『*Firepower System Configuration Guide*』の「Synchronizing Time」を参照してください。仮想アプライアンスのクロック設定が正しいことが確認できたら、ESXi のホスト管理者に連絡して、サーバの時間設定が正しいことを確認します。

パフォーマンスの問題

パフォーマンスに問題がある場合は、仮想アプライアンスに影響を与える要因があることに注意してください。パフォーマンスに影響を与える可能性がある要因については、仮想アプライアンスのパフォーマンス (4 ページ) を参照してください。ESXi のホスト パフォーマンスを監視するには、vSphere クライアント および [Performance] タブで示されている情報を使用できます。

接続性の問題

VMware vCloud Director Web Portal および vSphere クライアント を使用して、管理インターフェイスおよびセンシング インターフェイスの接続性を表示し、確認することができます。

VMware vCloud Director Web Portal の使用

VMware vCloud Director Web Portal を使用して、管理接続およびセンシング インターフェイスが正しく接続されていることを表示および確認することができます。

接続を確認するには:

1. [My Cloud] > [VMs] を選択し、表示する仮想アプライアンスにカーソルを合わせて右クリックします。
2. [Actions] ウィンドウで、[Properties] をクリックします。
3. [Hardware] タブで管理インターフェイスとセンシング インターフェイスの NIC を表示し、接続を確認します。

vSphere クライアント の使用

vSphere クライアント を使用して、管理接続およびセンシング インターフェイスが正しく接続されていることを確認することができます。

管理接続

初期設定時には、電源をオンにした状態でネットワーク アダプタを接続することが重要です。このようにしないと、最初の管理接続設定を正常に完了できず、次のようなメッセージで終了します。

```
ADDRCONF (NETDEV_UP): eth0: link is not ready
```

管理接続が接続されていることを確認するには:

1. vSphere クライアントで仮想アプライアンスの名前を右クリックし、[Edit Settings] を選択します。[Hardware] リストの [Network adapter 1] を選択し、[Connect at power on] チェックボックスがオンになっていることを確認します。

   最初の管理接続が正常に完了したら、このメッセージの `/var/log/messages` ディレクトリを確認します。

   ```
   ADDRCONF (NETDEV_CHANGE): eth0: link becomes ready
   ```

センシング インターフェイス

初期設定時には、電源をオンにした状態でセンシング インターフェイスを接続することが重要です。

電源がオンの状態でセンシング インターフェイスを接続されていることを確認するには:

1. vSphere クライアントで仮想デバイスの名前を右クリックし、[Edit Settings] を選択します。[Hardware] リストで [Network adapter 2] および [Network adapter 3] を選択します。使用中の各アダプタについて、[Connect at power on] チェックボックスがオンになっていることを確認します。

   仮想デバイスのセンシング インターフェイスは、無差別モードのトラフィックを受け入れる仮想スイッチまたは仮想スイッチ グループに接続する必要があります。このようにしないと、デバイスはブロードキャスト トラフィックしか検出できません。

次の作業

- 仮想デバイスのセンシング インターフェイスの設定（15 ページ）を参照して、センシング インターフェイスがすべてのエクスプロイトを検出するように設定します。

インライン インターフェイスの設定

インライン インターフェイスがシンメトリックで、トラフィックが相互に入出していることを確認できます。自身の仮想デバイスに対して VMware コンソールを開くには、VMware vCloud Director の Web ポータルまたは vSphere クライアント のいずれかを使用します。

インライン センシング インターフェイスが正しく設定されていることを確認するには:

1. コンソールで、CLI Configuration（Administrator）権限を持つユーザとしてログインします。
2. `expert` と入力してシェル プロンプトを表示します。
3. `cat /proc/sf/sfe1000.*` というコマンドを入力します。

   次のような情報が示されたテキスト ファイルが表示されます。

```
SFE1000 driver for eth1 is Fast, has link, is bridging, not MAC filtering, MAC timeout 7500,
Max Latency 0.
```

```
  39625470 packets received.
         0 packets dropped by user.
  13075508 packets sent.
0 Mode 1 LB Total 0 Bit 000...
.
.
SFE1000 driver for eth2 is Fast, has link, is bridging, not MAC filtering, MAC timeout 7500,
Max Latency 0.
  13075508 packets received.
         0 packets dropped by user.
  39625470 packets sent.
0 Mode 1 LB Total 0 Bit 00
```

eth1 で受信したパケット数は、eth2 から送信されたパケット数と一致すること、および eth1 から送信されたパケット数は、eth2 で受信したパケット数と一致することに注意してください。

4. 仮想デバイスからログアウトします。
5. 保護されているドメインに対してダイレクト ルーティングがサポートされている場合は、オプションとして、仮想デバイスのインライン インターフェイスが接続されている、保護されている仮想アプライアンスを ping します。

   ping が戻り、仮想デバイスのインライン インターフェイス セットを介して接続が存在していることが示されます。

支援が必要な場合

シスコ の製品をご利用いただきありがとうございます。

シスコ サポート

ご質問がある場合、またはシスコ ASA アプライアンスに関するサポートが必要な場合は、シスコ サポートにお問い合わせください。

- シスコ サポート サイト（http://www.cisco.com/cisco/web/support/index.html）にアクセスしてください。
- シスコ サポートの電子メール アドレス：tac@cisco.com。
- シスコ サポートの電話番号：1-408-526-7209 または 1-800-553-2447。

支援が必要な場合