



Cisco Firepower NGIPSv (VMware 向け) ク イック スタート

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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェアライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハードコピーおよびソフトコピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/go/offices) をご覧ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.



Vmware 向け仮想 Cisco Firepower アプライアンスの概要

Cisco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 ビット仮想 Cisco Firepower Management Center と 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。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 ツールを使用することもできます。

仮想 Cisco Firepower Management Center は物理デバイスおよび Cisco ASA with FirePOWER Services (ASA FirePOWER) を管理することができ、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。仮想 Cisco Firepower Management Center は高可用性をサポートせず、仮想デバイスはクラスタリング、スタッキング、スイッチング、ルーティングなどをサポートしません。物理 Firepower システム アプライアンスの詳細については、『Firepower 7000 and 8000 Series Installation Guide』および『Firepower Management Center Installation Guide』を参照してください。

このガイドは、仮想 Firepower システム アプライアンス (Firepower NGIPSv デバイスおよび Firepower Management Center) 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 Client、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 ツール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作成については、VMware vCloud Director および VMware vCenter を含む VMware ESXi のマニュアル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™) テクノロジー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。

仮想アプライアンスのパフォーマンス

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	8 GB	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	40 GB (NGIPSv) 250 GB (仮想 Firepower Management Center)	否

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方法については、『*Firepower Management Center Configuration Guide*』を参照してください。

注意事項と制約事項

Vmware 向けに Firepower NGIPSv を展開する際には次の制約があります。

- vMotion はサポートされません。
- 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。

VMware 向け仮想アプライアンスのインストールパッケージ

Cisco 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。Cisco 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。

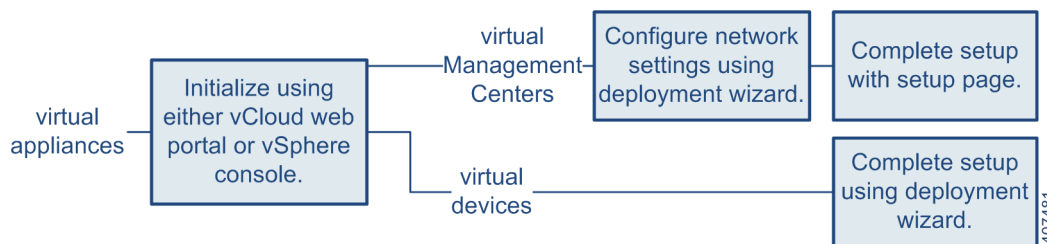
- ファイル名に **-ESXi-** が含まれている Open Virtual Format (.ovf) テンプレート
- ファイル名に **-vI-** が含まれている Open Virtual Format (.ovf) テンプレート
- ファイル名に **-ESXi-** が含まれているマニフェスト ファイル (.mf)
- ファイル名に **-vI-** が含まれているマニフェスト ファイル (.mf)
- 仮想マシン ディスク形式 (.vmdk)

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。

- VIOVF 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 システムの必須設定 (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。管理プラットフォームを使用して、VMware vCloud Director または VMware vCenter を展開する必要があります。

VIOVF テンプレートの展開

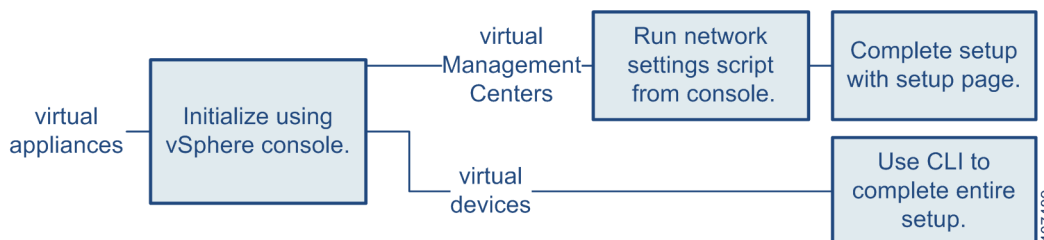
次の図は、VIOVF テンプレートを使用して展開する場合の、仮想 Firepower システム アプライアンスの設定の一般的なプロセスについて示しています。



- 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、または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、仮想 Firepower システム アプライアンスの設定の一般的な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

仮想 Firepower システム 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。Cisco 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、シスコのサポート サイト (<https://software.cisco.com/download/navigator.html>) の [ダウンロード (Downloads)] 領域に移動します。
2. [製品 (Products)] 領域のソフトウェアを参照するか、または、インストールするシステム ソフトウェアの [検索 (Find)] フィールドに名前を入力します。
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、ダウンロードする仮想 Firepower システム 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、Cisco 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。仮想 Cisco Firepower Management Center 向けに、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 Client 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。

仮想 Cisco Firepower NGIPSv 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
```

仮想 Cisco Firepower Management Center 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 \(7 ページ\)](#) に進んで、仮想 Firepower システム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 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 Client) 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 システム 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 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 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 Client 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
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 NGIPSv) 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。
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る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。
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	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 \(15 ページ\)](#) 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 \(8 ページ\)](#) 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 \(9 ページ\)](#) 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 Director User'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するには、『[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、[カタログ (Catalogs)] > [組織 (Organization)] > [vApp テンプレート (vApp Templates)] を選択します。ここで、[組織 (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 \(9 ページ\)](#) 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 システムの必須設定を構成できます。

手順

1. VMware vCloud Director Web ポータルで、[個人用クラウド(My Cloud)] > [vApps] を選択します。
2. [vApp メディア(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. [リソースの設定(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、[Custom Properties] 画面で、セットアップ ウィザードの Firepower システム の必須設定を入力し、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 \(15 ページ\)](#) 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、[完了(Finish)] をクリックします。
(注) 仮想デバイスの [展開後に電源を入れる (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 \(15 ページ\)](#) 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 \(11 ページ\)](#) を参照してください。

VMware vSphere を使用した展開

VMware vSphere vCenter、vSphere Client、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 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 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

- Cisco.com から OVF テンプレートをダウンロードするには、「[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 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、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 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. 名前を編集し、Cisco Firepower NGIPSv 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. Cisco Firepower NGIPSv 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. Cisco Firepower NGIPSv 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。
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、Cisco Firepower NGIPSv 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。
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\(15 ページ\)](#)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。[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、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、最大 30 分かかることがあります。

(注) Cisco Licensing Authority に Cisco Firepower NGIPSv を正常に登録するには、Cisco Firepower NGIPSv 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\(11 ページ\)](#)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	8 GB	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	40 GB (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 (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

[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調整できます。このタブで、CPU、メモリ、ディスク、および拡張 CPU リソースを変更できます。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。

インストール後の設定

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 (11 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、[ハードディスク 1 (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. [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。
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 \(15 ページ\)](#) 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。[インターフェイスの追加と構成 \(12 ページ\)](#) 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 (Access)
任意 (Any)	任意 (Any)	NGIPSv	任意 (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 Client 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。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。

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>) 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。

(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 インターフェイスには、無差別モードを受け入れる ESXi ホストの仮想スイッチ上のポートへのネットワーク接続が必要です。

(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 Client を使用してサーバにログインし、サーバの [設定 (Configuration)] タブをクリックします。
[ハードウェア (Hardware)] 選択リストと [ソフトウェア (Software)] 選択リストが表示されます。
2. [ハードウェア (Hardware)] リストで、[ネットワーキング (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\(15 ページ\)](#)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

Cisco Firepower システム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) に同意する必要があります。

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ス、スケジュールの更新など、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。設定および登録時に選択したオプションにより、システムが作成および適用するデフォルトのインターフェイス、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、すぐに使用できるエクスペリエンスを提供し、オプションを制限せずにユーザが展開を迅速に設定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、その設定はいつでも Cisco Firepower Management Center を使用して変更できます。つまり、設定中に、たとえば検出モードや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ることはありません。

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アプライアンスを Firepower Management Center へ登録するなど、初期設定を行うことができます。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。

仮想 Cisco Firepower Management Center

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場合、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 (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (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。

CLI を使用した Firepower NGIPSv デバイスの設定

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 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。

ESXi OVF テンプレートを使用した場合、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 NGIPSv デバイスの設定 \(16 ページ\)](#)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 (Access)
任意 (Any)	任意 (Any)	NGIPSv	任意 (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者パスワードを変更し、デバイスのネットワーク設定と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せん。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 7000 and 8000 Series 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。

デバイス ネットワークの設定について

Firepower システム 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ックスの長さ、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。検出モードの設定を後で変更することはできません。これは、システムによるデバイス初期設定の調整を容易にするために、セットアップ中にユーザが選択するオプションに過ぎません。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	デフォルトのインラインセット	デフォルトのインラインセットに追加された最初のペア (内部ゾーンに1つと外部ゾーンに1つ)
パッシブ	パッシブ	なし	パッシブゾーンに割り当てられた最初のペア
アクセス制御	なし	なし	なし
ネットワーク ディスカバリ	パッシブ	なし	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 Management Center 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. デバイスのネットワーク設定を構成します。最初に IPv4 の管理設定を行い(または無効にして)、次に IPv6 を設定します。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. デバイスをどのように展開したかに基づいて、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\(18 ページ\)](#) 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 (Access)
任意 (Any)	任意 (Any)	NGIPSv	任意 (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 に登録の方が簡単です。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 Client 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。
- 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、[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。
- 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 Tools 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強化し、VMware 製品で使い勝手のよい多数の機能を実現します。このシステムは、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 (Access)
任意 (Any)	任意 (Any)	NGIPsv	任意 (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` 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、Cisco 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。以下のセクションで説明するタスクの詳細、および展開の設定を開始する方法の詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

個別のユーザ アカウント

初期セットアップが完了した時点で、システム上の唯一のユーザは、管理者ロールとアクセス権を持つ `admin` ユーザです。このロールを所有しているユーザは、シェルまたは CLI を介したアクセスを含め、システムのすべてのメニューおよび設定にアクセスできます。セキュリティおよび監査上の理由から、Cisco では、`admin` アカウント (および `Administrator` ロール) の使用を制限することを推奨しています。

システムを使用する各ユーザに対して個別のアカウントを作成すると、各ユーザによって行われたアクションと変更を組織で監査できるほか、各ユーザに関連付けられたユーザ アクセス ロールを制限することができます。これは、ほとんどの設定および分析タスクを実行する Cisco Firepower Management Center で特に重要です。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。Cisco 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。Cisco 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。

ソフトウェアと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。Cisco では、展開環境内のすべてのアプライアンスが Firepower システム 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 システム 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 ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

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 を使用して、仮想環境内にセキュリティソリューションを展開し、物理資産と仮想資産の両方の保護を向上させることができます。仮想デバイスと仮想 Cisco Firepower Management Center により、VMware プラットフォームでセキュリティソリューションを容易に実装できます。仮想デバイスはまた、リソースが制限されることがあるリモートサイトのデバイスの展開および管理を容易にします。

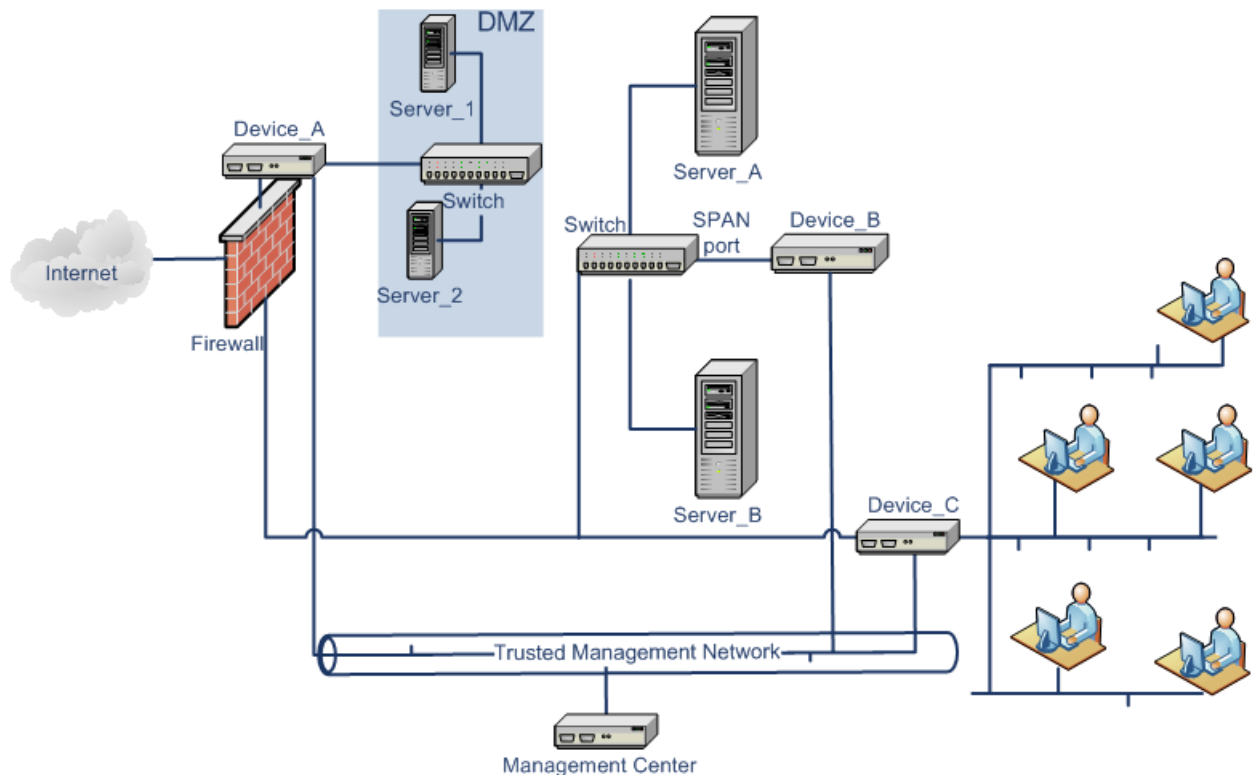
次の例では、物理デバイスまたは仮想デバイスを管理するために物理または仮想の Cisco Firepower Management Center を使用できます。IPv4 または IPv6 のネットワークに展開できます。また、Cisco Firepower Management Center に複数の管理インターフェイスを設定することにより、2 つの異なるネットワークを分離して監視したり、単一ネットワークの内部トラフィックとイベントトラフィックを分離することもできます。仮想デバイスは複数の管理インターフェイスをサポートしていないことに注意してください。

パフォーマンスを向上させるため、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 で 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 Management Center Configuration Guide*』の「Managing Devices」を参照してください。

注意: 実稼働ネットワークトラフィックと信頼される管理ネットワークトラフィックを、異なるネットワークセグメントに保持することを Cisco 強く推奨します。アプライアンスと管理トラフィックデータストリームのセキュリティを保証するための対策を実施する必要があります。

一般的な Firepower システムの展開

物理アプライアンス環境で、一般的な Firepower システムの展開には、物理デバイスと物理 Cisco Firepower Management Center を使用します。次の図は展開の例を表します。以下に示すように、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。



ほとんどのネットワーク スイッチでポート ミラーリングを設定して、1つのスイッチ ポート(または VLAN 全体)で発生するネットワーク パケットのコピーをネットワーク 監視接続に送信できます。主要なネットワーク 機器プロバイダーでは SPAN(スイッチ ポート アナライザ)とも呼ばれるポート ミラーリングを使用することで、ネットワーク トラフィックを監視できます。Device_B は、Server_A と Server_B の間のスイッチの SPAN ポートを経由して、Server_A と Server_B の間のトラフィックを監視することに注意してください。

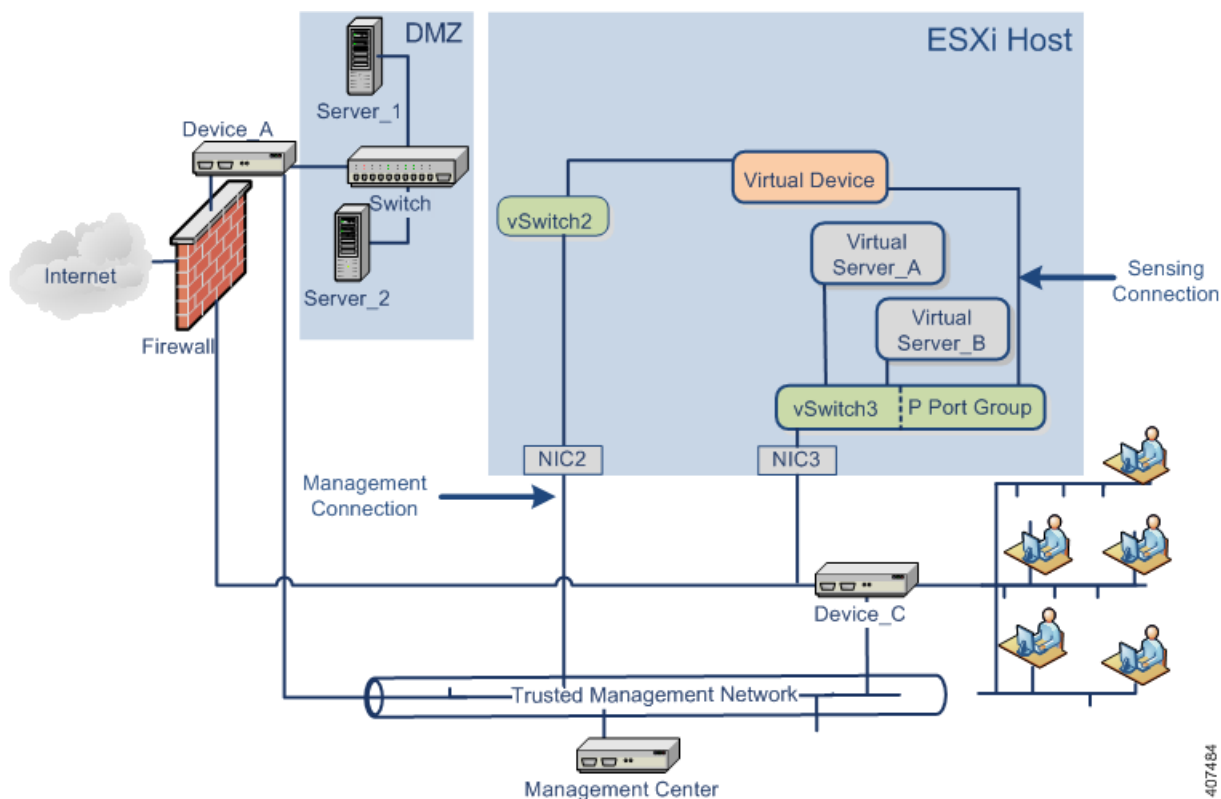
仮想 Firepower アプライアンスの導入 VMware

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することにより、一般的な Firepower システム の展開 (23 ページ) で物理的な内部サーバを置き換えることができます。次の例では、ESXi ホストを使用して、Server_A および 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できます。

下図のように、仮想デバイスセンシング インターフェイスは、無差別モード 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。



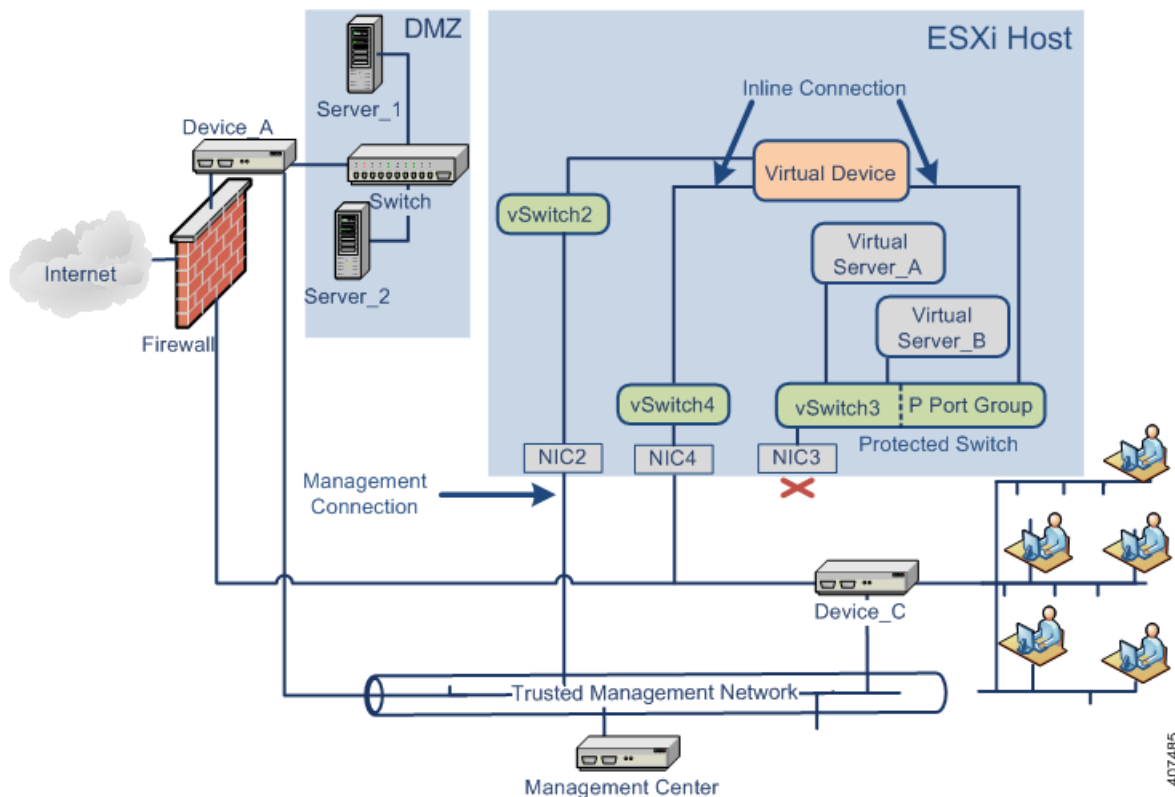
(注)すべてのトラフィックを検知するには、デバイスセンシングインターフェイスが接続する仮想スイッチまたはポートグループで無差別モードトラフィックを許可します。[仮想デバイスのセンシングインターフェイスの設定 \(13 ページ\)](#)を参照してください。

この例で示しているセンシングインターフェイスは1つのみですが、仮想デバイスではデフォルトで2つのセンシングインターフェイスを使用できます。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。

インライン検出のため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り、仮想サーバの周囲にセキュアな境界を実現できます。このシナリオは[一般的な Firepower システム の展開 \(23 ページ\)](#)と[仮想化と仮想デバイスの追加 \(24 ページ\)](#)に示す例の上に構築します。

はじめに、保護された仮想スイッチを作成し、それを仮想サーバに接続します。次に、保護されたスイッチを、仮想デバイスを通じて外部ネットワークに接続します。詳細については、『[Firepower Management Center 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 センシング インターフェイスが接続する仮想スイッチまたはポート グループで無差別モード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 \(13 ページ\)](#)を参照してください。

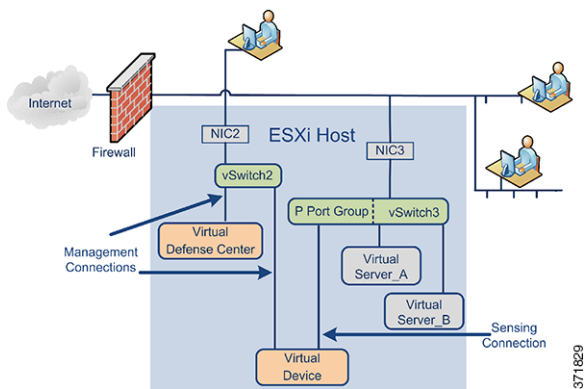
仮想デバイスは、侵入ポリシーに応じて、Server_A および Server_B への悪意のある任意のトラフィックを監視およびドロップします。

仮想 Cisco Firepower Management Center の追加

次に示すように、ESXi ホストに仮想 Cisco Firepower Management Center 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 システム の展開 \(23 ページ\)](#)と[インライン検出のための仮想デバイスの使用 \(25 ページ\)](#)に示す例の上に構築します。

仮想 Firepower Management Center 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、仮想 Firepower Management Center は物理デバイスと仮想デバイスの両方を管理できます。

Cisco 仮想アプライアンスは必須のアプリケーション ソフトウェアとともに事前に構成されているので、ESXi ホストに展開後すぐに動作可能です。このことにより、ハードウェアとソフトウェアの複雑な互換性問題が減り、展開時間が短縮されて、Firepower システム の機能を最大限に活用できます。次に示すように、ESXi ホスト上に仮想サーバ、仮想 Firepower Management Center、および仮想デバイスを展開し、仮想 Firepower Management Center からその展開を管理することができます。

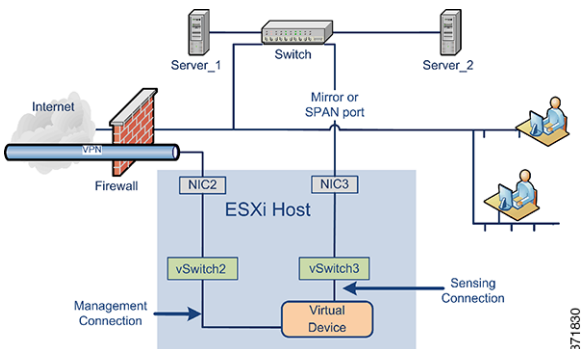


仮想デバイスの検知接続は、ネットワークトラフィックを監視できるようにする必要があります。仮想スイッチまたは仮想インターフェイスが接続するスイッチ上のポートグループは、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワークデバイス向けの packets を読み取ることができます。例では、Pポートグループが無差別モードトラフィックを受け入れるように設定されています。[仮想デバイスのセンシングインターフェイスの設定\(13ページ\)](#)を参照してください。

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ーフェイスカード(この例では NIC2)を経由した接続により、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(16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ための理想的な方法です。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。



仮想デバイスの検知接続は、ネットワークトラフィックを監視できるようにする必要があります。これを行うには、仮想スイッチまたはセンシングインターフェイスが接続するスイッチのポートグループが、無差別モードトラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワークデバイス向けの packets を読み取ることができます。この例では、vSwitch3 のすべてが無差別モードトラフィックを受け入れるように設定されています。vSwitch3 は、NIC3 を経由して SPAN ポートにも接続されているため、リモートオフィスのスイッチを通過するトラフィックも監視できます。[仮想デバイスのセンシングインターフェイスの設定\(13ページ\)](#)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ーフェイスカード(この例では NIC2)を経由した接続により、リモート Firepower Management Center を使用して、仮想デバイスにアクセスできます。

仮想 Firepower アプライアンスの導入 VMware

さまざまな地理的位置にデバイスを展開する場合、保護されていないネットワークからデバイスを隔離して、デバイスおよびデータストリームのセキュリティを保証するための対策を実施する必要があります。デバイスから VPN または別のセキュアなトンネリングプロトコルを使用してデータストリームを送信することによりこれを実現できます。仮想デバイスの管理接続のセットアップの詳細については、[CLI を使用した Firepower NGIPSv デバイスの設定 \(16 ページ\)](#) を参照してください。



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

このセクションでは、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。Cisco 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 Management Center 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 Client および [パフォーマンス (Performance)] タブで示されている情報を使用できます。

接続の問題

VMware vCloud Director Web Portal および vSphere Client 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 ポータルを使用して、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. [個人用クラウド (My Cloud)] > [VM] を選択し、表示する仮想アプライアンスにマウスを合わせて右クリックします。
2. [アクション (Actions)] ウィンドウで、[プロパティ (Properties)] をクリックします。
3. [ハードウェア (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 Client の使用

vSphere Client 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 Client の仮想アプライアンスの名前を右クリックし、[設定の編集 (Edit Settings)] を選択します。[ハードウェア (Hardware)] リストの [ネットワークアダプタ 1 (Network adapter 1)] を選択し、[パワーオン時に接続 (Connect at power on)] チェックボックスが選択され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 Client の仮想デバイスの名前を右クリックし、[設定の編集 (Edit Settings)] を選択します。[ハードウェア (Hardware)] リストで [ネットワークアダプタ 2 (Network adapter 2)] および [ネットワークアダプタ 3 (Network adapter 3)] を選択します。使用中の各アダプタについて、[パワーオン時に接続 (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 \(13 ページ\)](#) を参照して、センシング インターフェイスがすべてのエキ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。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 Client 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 の設定 (管理者) 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

Cisco の製品をご利用いただきありがとうございます。

Cisco のサポート

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

- Cisco 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。
- Cisco サポートの電子メールアドレス: tac@cisco.com。
- Cisco 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