Cisco Firepower Management Center Virtual（VMware 向け）導入クイック スタート ガイド

発行日:2015 年 11 月 10 日
更新日:2018 年 6 月 29 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、および推奨事項は、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 ライセンスおよび限定保証は、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およびソフトウェアは、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、およびその他の図は、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)

© 2018 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 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 ESXi ハイパーバイザーを使用して、64 ビットの Cisco Firepower Management Center Virtual 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、Cisco FirePOWER NGFW データシートを参照してください 。

このガイドは、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、vSphere Client、（オプション）VMware ツールを含む 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

仮想 Firepower Management Center は VMware ESXi と vSphere でホストできます。詳細については、『Cisco Firepower Compatibility Guide』を参照してください。このガイドでは、サポート対象の各 FirePOWER バージョンについて、オペレーティング システムとホスティング環境の要件を含めた Cisco FirePOWER ソフトウェアとハードウェアの互換性を提供します。

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 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、次の VMware Web サイトを参照してください。http://www.vmware.com/resources/guides.html

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

注意事項と制約事項

VMware 向けに展開する際には次のガイドラインがあります。

- 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。導入時に、ホスト クラスタがある場合は、ストレージをローカルに（特定のホスト上）または共有ホスト上でプロビジョニングできます。ただし、vMotion を使用して Firepower Management Center Virtual を別のホストに移行する場合、ローカル ストレージを使用するとエラーが発生します。

VMware 向けに展開する際には次の制約があります。

- 仮想 Cisco Firepower Management Center のアプライアンスにシリアル番号はありません。[システム（System）] の [設定（Configuration）] ページには、仮想プラットフォームに応じて、[なし（None）] または [未指定（Not Specified）] のいずれかが表示されます。
- 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。

INIT Respawning エラー メッセージ

症状:ESXi 6 および ESXi 6.5 で実行されている Firepower Management Center 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  "fmcv1" 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。
5. [OK] をクリックして設定を保存します。

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。

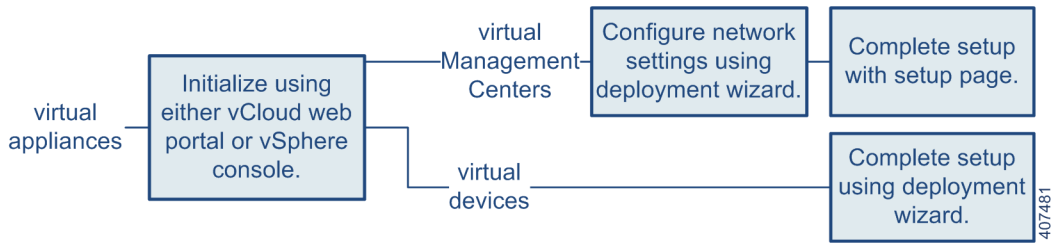
- ファイル名に `-ESXi-` が含まれている Open Virtual Format(`.ovf`)テンプレート
- ファイル名に `-VI-` が含まれている Open Virtual Format(`.ovf`)テンプレート
- ファイル名に `-ESXi-` が含まれているマニフェスト ファイル(`.mf`)
- ファイル名に `-VI` が含まれているマニフェスト ファイル(`.mf`)
- 仮想マシン ディスク形式(`.vmdk`)

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。

- 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 システム必須設定(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 vCenter など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

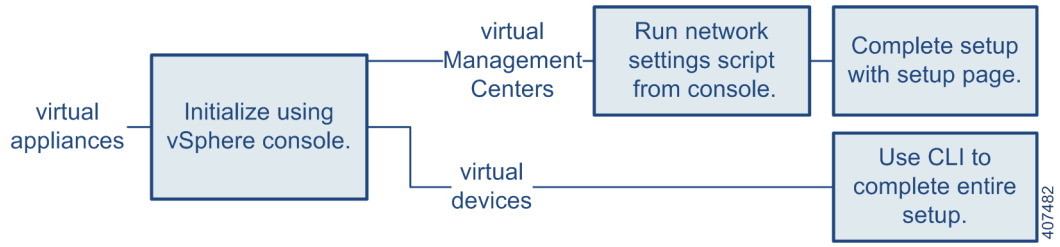
次の図は、VI OVF テンプレートを使用して展開する場合の、仮想 Firepower システム アプライアンスの設定の一般的なプロセスについて示しています。



- 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。VMware vCenter などの管理プラットフォーム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_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 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 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

- Vmware 向け仮想 Cisco Firepower Management Center の展開 (9 ページ) に進み、仮想 Firepower Management Center を展開します。

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 向け仮想 Cisco Firepower Management Center の展開

仮想 Cisco Firepower Management Center 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（vSphere Client）を使用して、管理プラットフォーム（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 vCenter を使用して管理する必要があります。
- ESXi OVF テンプレートを使用して展開する場合、インストール後に Firepower システム の必須設定を構成する必要があります。この仮想アプライアンスは VMware vCenter を使用して管理するか、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、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 Management Center Virtual 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_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
Cisco_Firepower_Management_Center_Virtual_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。

次の表に、展開に必要な情報を示します。

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 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。
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。

表 1　VMware OVF テンプレート（続き）

設定	ESXi または VI	操作
ディスクの書式設定	両方	仮想ディスクを保存する形式を、シック プロビジョニング（Lazy Zeroed）、シック プロビジョニング（Eager Zeroed）、シン プロビジョニングの中から選択します。
ネットワーク マッピング	両方	仮想アプライアンスの管理インターフェイスを選択します。
プロパティ（Properties）	VI のみ	仮想マシンの初期設定をカスタマイズします。

VI OVF テンプレートを展開する場合、インストール プロセスで仮想 Cisco Firepower Management Center の基本設定を実行できます。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

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。指定する構成内容に関するガイダンスを含む、初期設定の実行の詳細については、仮想 Cisco Firepower Management Center の設定（16 ページ）を参照してください。

VMware vSphere を使用した展開（10 ページ）では、Firepower Management Center 仮想アプライアンスを VMware vCenter に展開する方法について説明します。

ネットワークの設定については、ネットワーク設定（18 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、仮想 Firepower Management Center を展開できます。vSphere を使用して、VI 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 によって管理する必要があります。
- ESXi OVF テンプレートを使用して展開する場合、アプライアンスは VMware vCenter によって管理するか、またはスタンドアロン ホストに展開できます。いずれの場合も、インストール後に Firepower システム の必須設定を構成する必要があります。

はじめる前に

- 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」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、展開する OVF テンプレートを選択します。

   仮想 Cisco Firepower Management Center の場合：

   ```
   Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
   Cisco_Firepower_Management_Center_Virtual_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. オプションで、仮想 Firepower Management Center を置くインベントリ内のフォルダの名前を編集し、場所を選択して [次へ（Next）] をクリックします。

   （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. 仮想 Firepower Management Center 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. 仮想 Firepower Management Center を実行するリソース プールに移動してこれを選択し、[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. [ネットワークマッピング（Network Mapping）] 画面で、仮想 Firepower Management Center 管理インターフェイスを Vmware ネットワークと関連付けます。

    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、ネットワーク マッピングをセットアップして、[次へ（Next）] をクリックします。
11. ユーザ設定可能なプロパティが OVF テンプレート（VI テンプレートのみ）に含まれている場合は、設定可能なプロパティを設定し、[次へ（Next）] をクリックします。
12. [終了準備の完了（Ready to Complete）] ウィンドウで設定を見直し、確認します。
13. オプションで [展開後に電源を入れる（Power on after deployment）] オプションをオンにして、仮想 Firepower Management Center に電源を入れ、[完了（Finish）] をクリックします。

    （注）展開後に電源を入れないことを選択した場合は、後で VMware コンソールから電源を入れることができます（仮想アプライアンスの初期化（15 ページ）を参照）。
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、[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。

    その後、仮想 Cisco Firepower Management Center 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 に仮想 Firepower Management Center を正常に登録するためには、Firepower Management Center 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を変更する必要があるかを確認するには、インストール後の設定（12 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をインストールしたら、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 仮想 Firepower Management Center の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	250 GB（Cisco Firepower Management Center）	否

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）	管理者

[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。

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 [設定の編集（Edit Settings）] を選択するか、メイン ウィンドウの [作業の開始（Getting Started）] タブから [仮想マシン設定の編集（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（4 ページ）に示すように、[メモリ（Memory）]、[CPU（CPUs）]、および [ハード ディスク 1（Hard disk 1）] の設定がデフォルト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の初期設定の方法については、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。
- オプションで、アプライアンスの電源を入れる前に、他の管理インターフェイスを作成できます(『*Cisco Firepower NGIPSv Quick Start Guide for VMware*』を参照)。

インストール後の設定

VMware 向け仮想 Cisco Firepower Management Center のセットアップ

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。このプロセスにより、信頼された管理ネットワーク上で新しいアプライアンスが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。

設定プロセスを使用すると、時間の設定、デバイスの登録とライセンス認証、更新のスケジューリングなどのさまざまな管理レベル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。

これらの初期設定とポリシーの目的は、オプションを制限することではなく、すぐに使用できるエクスペリエンスを提供し、短時間で展開を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、設定を完了します。

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)	管理者

仮想アプライアンスをインストールした後、仮想アプライアンスに初めて電源を入れると初期化が自動的に開始されます。

注意: 起動時間は、サーバ リソースの可用性など、さまざまな要因によって異なります。初期化が完了するまでに最大で 40 分かかることがあります。初期化は中断しないでください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

仮想アプライアンスを初期化するには、次の手順を使用します。

手順

1. アプライアンスの電源をオンにします。

   vSphere Client で、インベントリ リストからインポートした仮想アプライアンスの名前を右クリックし、コンテキスト メニューで [電源(Power)] > [電源オン(Power On)] を選択します。

2. VMware コンソール タブで初期化を監視します。

次の作業

- 設定を完了するには、仮想 Cisco Firepower Management Center の設定(16 ページ)を参照してください。

仮想 Cisco Firepower Management Center の設定

仮想 Cisco Firepower Management Center の設定に必要な手順は、VI OVF テンプレートまたは ESXi OVF テンプレートのいずれを使用して展開したかによって異なります。

- VI OVF テンプレートを使用して展開し、セットアップ ウィザードを使用した場合は、Firepower システム の必須設定を行ったときに指定したパスワードを使用して、仮想 Firepower Management Center にログインし、Firepower システム を使用してローカル アプライアンスの設定、ライセンスとデバイスの追加、トラフィックを監視および管理するためのポリシーの適用を行います。詳細については、『*Firepower System Configuration Guide*』を参照してください。
- ESXi OVF テンプレートを使用して展開した場合、または VI OVF テンプレートを使用して展開したときに Firepower システム の必須設定を行っていない場合は、仮想 Firepower Management Center の設定は 2 段階のプロセスになります。仮想 Firepower Management Center を初期化した後で、VMware コンソールでスクリプトを実行します。これにより、管理ネットワーク上で通信するアプライアンスを設定できます。次に、管理ネットワーク上のコンピュータを使用して、アプライアンスの 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。
- ESXi OVF テンプレートを使用して仮想 Firepower Management Center を展開し、VI OVF テンプレートを使用してすべての仮想デバイスを展開する場合は、1 ページのセットアップ ウィザードを使用して仮想 Firepower Management Center へすべてのデバイスを同時に登録できます。詳細については、初期設定ページ:Cisco Firepower Management Center Virtual(17 ページ)を参照してください。

仮想 Firepower Management Center ネットワーク設定の自動化

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)	Management Center	グローバルのみ	管理者

新しい仮想 Cisco Firepower Management Center を初期化した後で、管理ネットワーク上でアプライアンスが通信できるようにするための設定を行う必要があります。VMware コンソールでスクリプトを実行して、この手順を完了します。

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。最初に、スクリプトから IPv4 管理設定を構成(または無効に)するように要求されてから、IPv6 に移ります。IPv6 展開では、ローカル ルータから設定値を取得できます。IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを指定する必要があります。

スクリプトの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。

はじめる前に

仮想アプライアンスの初期化(15 ページ)に示すように、デバイスを初期化します。

手順

1. ユーザ名 `admin` と、VI OVF テンプレートを使用して展開したときにセットアップ ウィザードで指定した管理者アカウントのパスワードを使用して、VMware コンソールで仮想 Firepower Management Center 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。

2. admin プロンプトで、次のスクリプトを実行します。

   ```
   sudo /usr/local/sf/bin/configure-network
   ```

3. スクリプトのプロンプトに従ってください。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）。

4. 設定値が正しいことを確認します。

   設定値を誤って入力した場合は、プロンプトで「`n`」と入力して、Enter キーを押します。その後、正しい情報を入力できます。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。

5. アプライアンスからログアウトします。

次の作業

- Cisco Firepower Management Center の Web インターフェイスを使用して設定を完了するには、初期設定ページ：Cisco Firepower Management Center Virtual（17 ページ）に進みます。

初期設定ページ：Cisco Firepower Management Center Virtual

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）	Management Center	グローバルだけ	管理者

仮想 Cisco Firepower Management Center では、アプライアンスの Web インターフェイスにログインして、設定ページで初期設定オプションを指定することによって、設定プロセスを完了する必要があります。管理者パスワードを変更して、まだの場合はネットワーク設定を指定し、EULA に同意します。

設定プロセスでは、デバイスの登録およびライセンス付与を行うこともできます。デバイスを登録する前に、Firepower Management Center をリモート マネージャとして追加するだけでなく、そのデバイス自体の設定プロセスを完了する必要があります。完了していない場合、デバイスの登録が失敗します。

手順

1. 管理ネットワーク上のコンピュータから、サポートされているブラウザで `https://`*`MC_name`*`/` にアクセスします。ここで *`MC_name`* は、前の手順で Firepower Management Center の管理インターフェイスに割り当てたホスト名または IP アドレスです。

2. ユーザ名 `admin` と、VI OVF テンプレートによる展開でセットアップ ウィザードに指定した管理者アカウントのパスワードを使用してログインします。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は、パスワードとして `Admin123` を使用します。

設定ページが表示されます。設定の完了方法については、次の項を参照してください。

パスワードの変更(Change Password)(18 ページ)

ネットワーク設定(18 ページ)

時刻設定(19 ページ)

ルール更新の定期インポート(19 ページ)

地理情報の定期的な更新(19 ページ)

自動バックアップ(20 ページ)

ライセンス設定(20 ページ)

ライセンス設定(20 ページ)

エンド ユーザ ライセンス契約(21 ページ)

3. 完了したら、[適用(Apply)] をクリックします。

   仮想 Firepower Management Center が選択内容に従って設定されます。

4. 初期設定が正常に終了したことを確認するには、[タスクステータス(Task Status)] ページ([システム(System)] > [モニタリング(Monitoring)] > [タスクステータス(Task Status)])を使用します。

   ページは 10 秒ごとに自動的に更新されます。最初のデバイス登録およびポリシーの適用のタスクについて、[完了(Completed)] ステータスが表示されるまでページを監視します。設定の一部として、侵入ルールまたは位置情報の更新を設定した場合は、これらのタスクも監視することができます。

Cisco Firepower Management Center を使用する準備が整いました。展開の設定の詳細については、『*Firepower System Configuration Guide*』を参照してください。

次の作業

- 次のステップ(22 ページ)に進みます。

パスワードの変更(Change Password)

admin アカウントのパスワードを変更する必要があります。このアカウントは管理者特権が付与されているため、削除できません。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。

ネットワーク設定

Cisco Firepower Management Center のネットワーク設定によって、それが管理ネットワーク上で通信できるようになります。スクリプトを使用してすでにネットワークを設定しているため、ページのこの項には情報が設定されています。

事前入力された設定を変更する場合は、Firepower システム によって IPv4 と IPv6 の両方の管理環境にデュアル スタック実装が提供されることに注意してください。管理ネットワーク プロトコル([IPv4]、[IPv6]、または [両方(Both)])を指定する必要があります。選択した内容に応じて、設定のページにはさまざまなフィールドが表示されます。ここで 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。

- IPv4 の場合、ドット付き 10 進表記でアドレスおよびネットマスクを設定する必要があります(例:255.255.0.0 のネットマスク)。
- IPv6 ネットワークの場合は、[ルータ自動設定を使用してIPv6アドレスを割り当てる(Assign the IPv6 address using router autoconfiguration)] チェックボックスをオンにして IPv6 のネットワーク設定を自動的に割り当てることができます。このチェックボックスを選択しない場合は、コロンで区切られた 16 進表記のアドレスおよびプレフィックス内のビット数(たとえば、112 のプレフィックス長)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。

時刻設定

Firepower Management Center の時刻は、手動で設定することも、ネットワーク タイム プロトコル（NTP）サーバから NTP 経由で設定することもできます。

また、**admin** アカウント用のローカル Web インターフェイスで使用されるタイム ゾーンを指定することもできます。現在のタイム ゾーンをクリックし、ポップアップ ウィンドウを使用してそのタイム ゾーンを変更します。Firepower Management Center

管理対象デバイスの時刻が、管理している Firepower Management Center と同期している必要があります。Firepower Management Center は NTP ソースとしてサポートされていないため、物理 NTP サーバを使用して時刻を設定することをお勧めします。

注意：Firepower Management Center Virtual を手動時刻で VMware に設定すると、（デフォルトでは）ホストからの実行に時間がかかります。ESX/ESXi ホストを NTP サーバとして設定できますが、この方法は VMware のベスト プラクティスではありません。VMware では、ESX/ESXi ホストを正式な時刻（NTP）サーバに設定することをベスト プラクティスと見なします。

ルール更新の定期インポート

新しい脆弱性が発見された場合、Cisco の脆弱性調査チーム（VRT）は侵入ルールの更新を公開します。ルールの更新では、新規および更新された侵入ルールおよびプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が提供されます。ルールの更新では、ルールを削除して、新しいルール カテゴリおよびシステム変数を提供する場合もあります。

展開で侵入検知および防御を実行するよう計画している場合、Cisco は、[ルール更新の定期インポートを有効にする（Enable Recurring Rule Update Imports）] を選択することを推奨しています。

それぞれのルール更新の後で、システムが侵入についての [ポリシーの再適用（Policy Reapply）] を実行するよう設定するだけでなく、[インポート頻度（Import Frequency）] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[今すぐインストール（Install Now）] を選択します。

（注） ルールの更新には、新しいバイナリが含まれている場合があります。ルール更新のダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認します。加えて、ルール更新のサイズが大きい場合があるため、ネットワーク使用率の低い時間帯にルールをインポートするようにしてください。

地理情報の定期的な更新

仮想 Cisco Firepower Management Center を使用して、ダッシュボードおよび Context Explorer の地理情報統計を監視するだけでなく、システムで生成されたイベントに関連付けられているルーテッド IP アドレスの地理情報を表示することができます。

Cisco Firepower Management Center の地理情報データベース（GeoDB）には、IP アドレスに関連するインターネット サービス プロバイダ（ISP）、接続タイプ、プロキシ情報、正確な位置情報などの情報が含まれています。定期的な GeoDB の更新を有効にすることで、システムが常に最新の地理情報を使用するようにすることができます。展開で地理情報システムに関連する分析の実行を計画する場合、Cisco は [定期的な週次更新を有効にする（Enable Recurring Weekly Updates）] を選択することを推奨しています。

GeoDB について、週次の更新頻度を指定できます。ポップアップ ウィンドウを使用してタイム ゾーンを変更するには、そのタイム ゾーンをクリックします。初期設定プロセスの一部としてデータベースをダウンロードするには、[今すぐインストール（Install Now）] を選択します。

（注） GeoDB の更新はサイズが大きくなることがあるため、ダウンロードの後のインストールに最大で 45 分かかることがあります。GeoDB は、ネットワークの使用量が少ないときに更新してください。

自動バックアップ

Firepower Management Center には、障害時に設定を復元できるように、データをアーカイブするためのしくみが用意されています。初期設定の一部として、[自動バックアップを有効にする（Enable Automatic Backups）] を選択することができます。

この設定を有効にすると、スケジュールされたタスクが作成され、このタスクによって Firepower Management Center の設定のバックアップが週次に作成されます。

ライセンス設定

組織にとって最適な Firepower システム の展開を実現するために、さまざまな機能のライセンスを取得することができます。Firepower Management Center を使用して、それ自体およびその管理対象のデバイスを管理できます。Firepower システム によって提供されるライセンスのタイプは、管理するデバイスのタイプによって異なります。

- Firepower、ASA FirePOWER、および NGIPSv の各デバイスの場合は、従来のライセンスを使用する必要があります。

デフォルトで、Firepower Management Center はドメイン制御、ホスト、アプリケーション、ユーザ ディスカバリの実行と、SSL および TLS で暗号化されたトラフィックの復号化と検査を行うことができます。機能別の従来のライセンスを取得すると、管理対象デバイスでさまざまな機能を実行することができます。ライセンスに関する完全な情報については、*Firepower System Configuration Guide* または Firepower Management Center のオンライン ヘルプを参照してください。

デバイスの登録（Device Registration）

仮想 Cisco Firepower Management Center は、Firepower システム が現在サポートしているすべての物理的および仮想的なデバイスを管理することができます。初期設定のプロセス中に、事前に登録したほとんどのデバイスを Firepower Management Center に追加できます。ただし、デバイスと Firepower Management Center が NAT デバイスによって分離されている場合は、設定プロセスが完了した後で、デバイスを追加する必要があります。

Firepower Management Center に管理対象デバイスを登録する際、登録時にアクセス制御ポリシーを自動的にデバイスに適用する場合は、[デフォルトのアクセス制御ポリシーを適用する（Apply Default Access Control Policies）] チェックボックスをオンのままにしておきます。Firepower Management Center が各デバイスに対してどのポリシーを適用するかは、選択できません。選択できるのはポリシーを適用するかどうかのみであることに注意してください。各デバイスに適用されるポリシーは、デバイスの設定時に選択した検出モードによって異なります。これを次の表に示します。

表 1　検出モードごとに適用されるデフォルトのアクセス制御ポリシー

検出モード	デフォルトのアクセス コントロール ポリシー
インライン	[デフォルト侵入防御（Default Intrusion Prevention）]
パッシブ	[デフォルト侵入防御（Default Intrusion Prevention）]
アクセス制御	[デフォルト アクセス制御（Default Access Control）]
ネットワーク ディスカバリ	[デフォルト ネットワーク ディスカバリ（Default Network Discovery）]

Firepower Management Center を使用して以前にデバイスを管理しており、そのデバイスの最初のインターフェイス設定を変更すると、例外が発生します。このような場合、新しい Firepower Management Center のページによって適用されるポリシーは、変更した（現在の）デバイスの設定によって異なります。設定されたインターフェイスがある場合、Firepower Management Center は Default Intrusion Prevention ポリシーを適用します。そうでない場合、Firepower Management Center は Default Access Control ポリシーを適用します。

仮想デバイスの検出モードの詳細については、『*Cisco NGIPSv Quick Start Guide for Vmware*』を参照してください。物理デバイスについては、『*Firepower システム Installation Guide*』を参照してください。

(注) デバイスがアクセス制御ポリシーに適合していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス コントロール ポリシーの適用が失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス コントロール ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、*Firepower System Configuration Guide* を参照してください。

デバイスを追加するには、デバイスの登録時に指定した**登録キー**のほかに、**ホスト名**または **IP アドレス**を入力します。これは、ユーザが指定した単純なキーで、ライセンス キーとは異なりますので注意してください。

次に、チェックボックスを使用して、ライセンスが付与された機能をデバイスに追加します。すでに Cisco Firepower Management Center に追加したライセンスしか選択できないので注意してください。また、いくつかのライセンスについては、他の機能を有効にするまで、有効にできません。たとえば、最初に Protection を有効にするまで、デバイス上で Control を有効にすることはできません。

アーキテクチャとリソースの制限のために、すべての管理対象デバイスですべてのライセンスがサポートされるわけではありません。ただし、セットアップ ページでは、管理対象デバイスでサポートされていないライセンスの有効化は**可能な**状態です。これは、後にならないと Cisco Firepower Management Center がデバイス モデルを判別できないためです。システムは無効なライセンスを有効にすることはできません。また、無効なライセンスを有効にしようとしても、ユーザが使用できるライセンス数は減少しません。

ライセンスを有効にした後で [追加(Add)] をクリックしてデバイスの登録設定を保存します。必要に応じてデバイスを追加します。間違ったオプションを選択した場合、またはデバイス名を誤って入力した場合は、[削除(Delete)] をクリックして削除します。その後で、デバイスをもう一度追加できます。

エンド ユーザ ライセンス契約

EULA をよく読んで、規定に従う場合はチェックボックスをオンにします。指定した情報がすべて正しいことを確認して、[適用(Apply)] をクリックします。

Cisco Firepower Management Center が選択内容に従って設定されます。管理者ロールを持つ `admin` ユーザとして Web インターフェイスにログインします。Firepower Management Center の初期設定を完了するには、初期設定ページ:Cisco Firepower Management Center Virtual(17 ページ)の手順 3. に進みます。

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
- スナップショット

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セットアップした後、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）を使用するか、または仮想 Firepower Management Center でブラウザを使用して、仮想アプライアンスの VMware ツールを有効にできます。詳細については、仮想 Firepower Management Center での VMware ツールの設定（22 ページ）を参照してください。

仮想 Firepower Management Center での VMware ツールの設定

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）	仮想 Management Center	任意（Any）	管理者

Web インターフェイスを使用して [設定（Configuration）] メニューのチェックボックスをオンまたはオフにできます。CLI を使用して仮想 Cisco Firepower Management Center で VMware ツールを有効にすることはできません。

仮想 Cisco Firepower Management Center で VMware ツールを有効または無効にするには、次の手順に従います。

1. Web ブラウザを使用して、Cisco Firepower Management Center にログインし、[システム（System）] > [設定（Configuration）] > [VMware ツール（VMware Tools）] を選択します。それから、[VMware ツールの有効化（Enable VMware Tools）] チェックボックスをオンまたはオフにし、[保存（Save）] をクリックします。

次のステップ

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 System 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。

次のステップ

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。

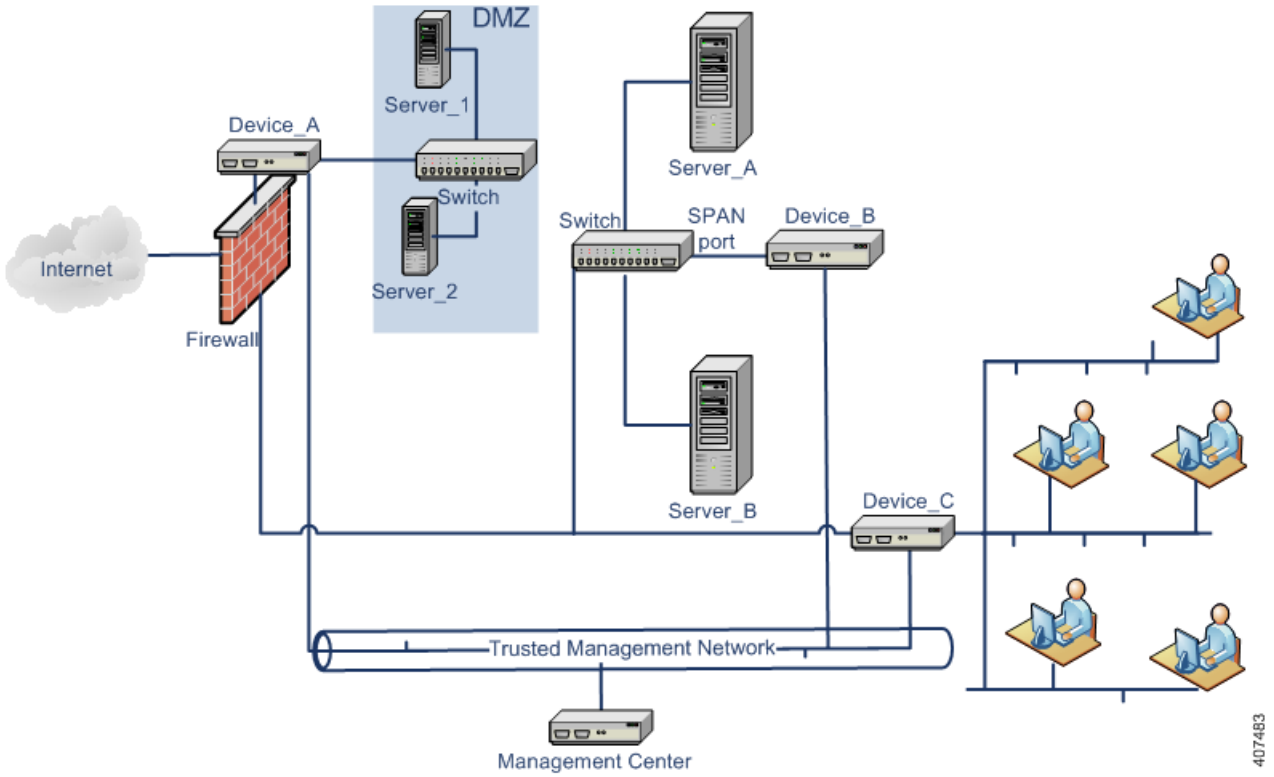
次の例では、物理デバイスまたは仮想デバイスを管理するために物理または仮想の Cisco Firepower Management Center を使用できます。IPv4 または IPv6 のネットワークに展開できます。また、Cisco Firepower Management Center に複数の管理インターフェイスを設定することにより、2 つの異なるネットワークを分離して監視したり、単一ネットワークの内部トラフィックとイベント トラフィックを分離することもできます。仮想デバイスは複数の管理インターフェイスをサポートしていないことに注意してください。

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 System Configuration Guide*』の「Managing Devices」を参照してください。

注意 : Cisco 実稼動ネットワーク 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。

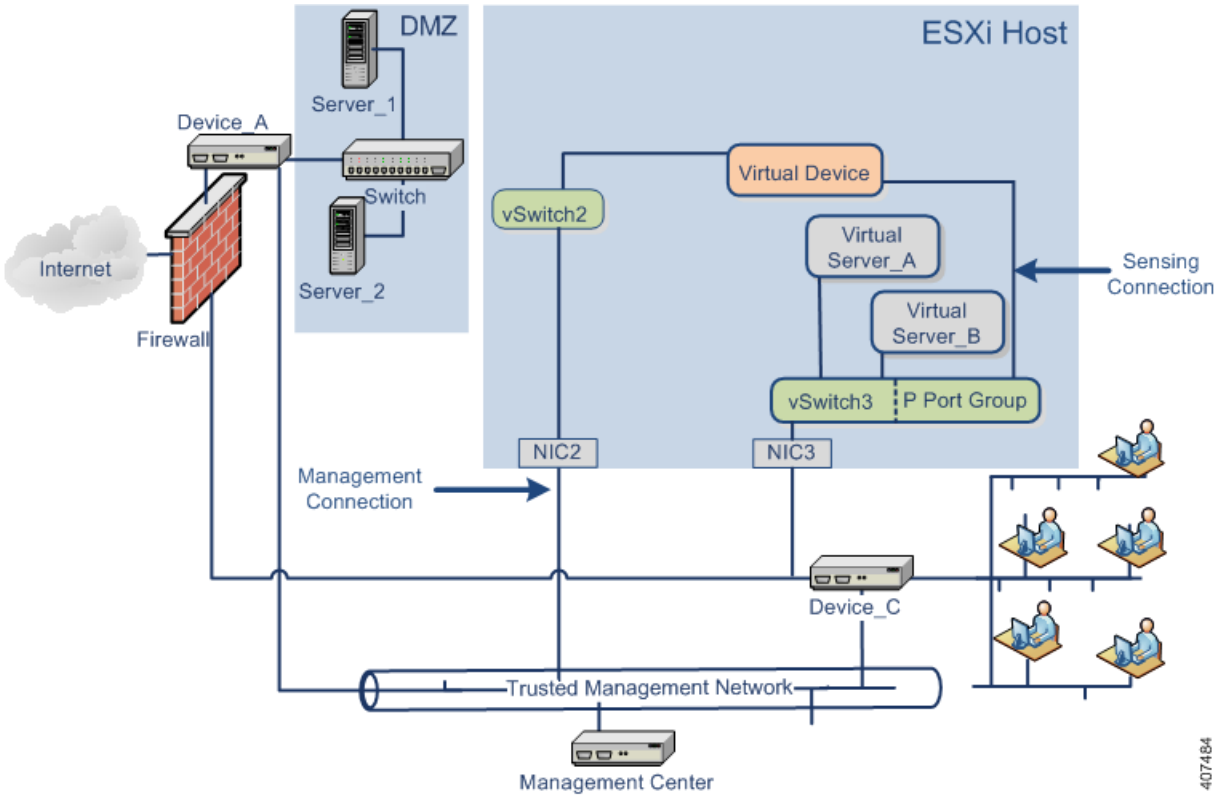
仮想 Firepower アプライアンスの導入VMware

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（25 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。



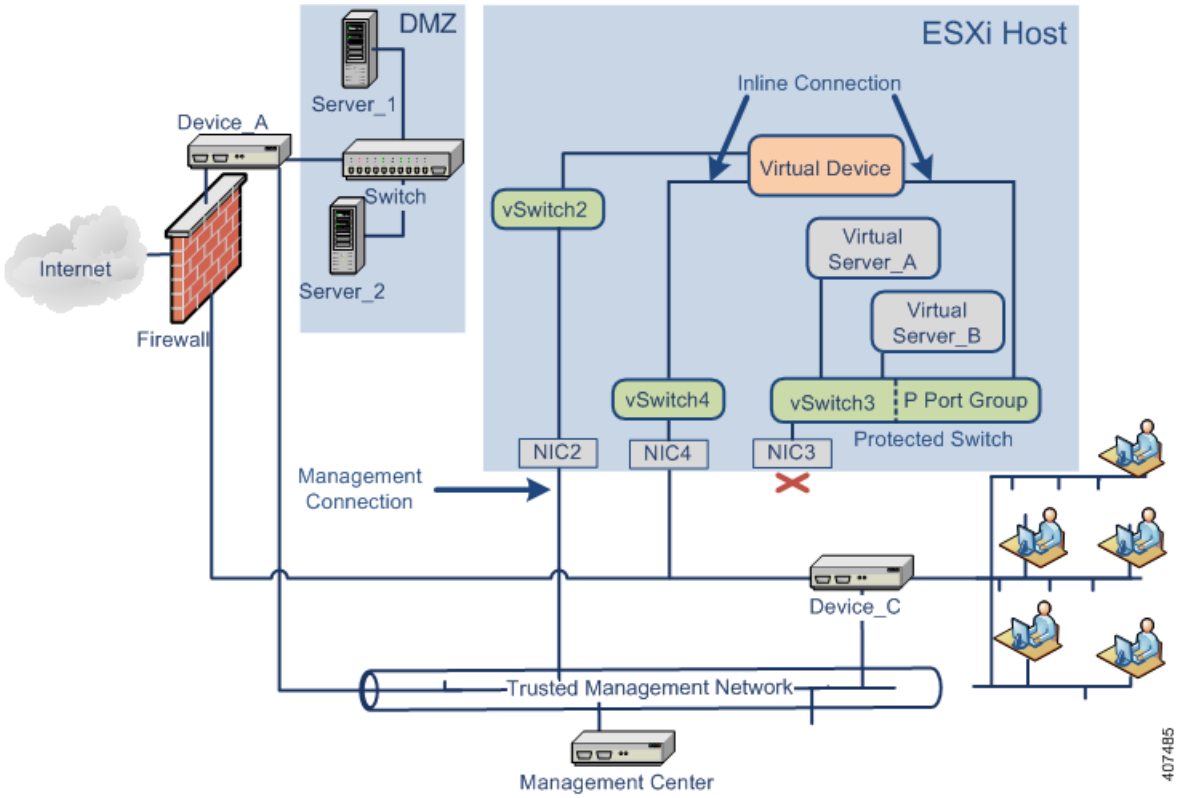
(注) すべてのトラフィックを検知するには、デバイス センシング インターフェイスが接続する仮想スイッチまたはポート グループで無差別モード トラフィックを許可します。

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 (25 ページ)と仮想化と仮想デバイスの追加 (26 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 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 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。

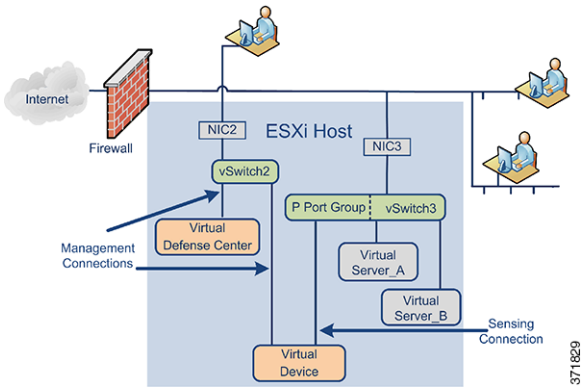
仮想デバイスは、侵入ポリシーに応じて、Server_A および Server_B への悪意のある任意のトラフィックを監視およびドロップします。

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 (25 ページ)とインライン検出のための仮想デバイスの使用 (27 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。

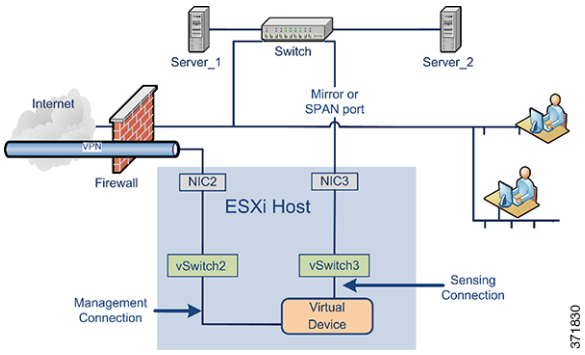


仮想デバイスの検知接続は、ネットワーク トラフィックを監視できるようにする必要があります。仮想スイッチまたは仮想インターフェイスが接続するスイッチ上のポート グループは、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワーク デバイス向けのパケットを読み取ることができます。例では、P ポート グループが無差別モード トラフィックを受け入れるように設定されています。

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。仮想 Firepower Management Center 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、『仮想 Firepower Management Center ネットワーク設定の自動化（16 ページ）と *Cisco NGIPSv Quick Start Guide for VMware*』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 デバイス向けのパケット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。

仮想デバイスは Firepower Management Center で管理する必要があります。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。

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。

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 System Configuration Guide User 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。

注意: **Firepower Management Center Virtual を手動時刻で VMware に設定すると、(デフォルトでは)ホストからの実行に時間がかかります。ESX/ESXi ホストを NTP サーバとして設定できますが、この方法は VMware のベスト プラクティスではありません。VMware では、ESX/ESXi ホストを正式な時刻(NTP)サーバに設定することをベスト プラクティスと見なします。**

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

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。

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

- 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方法については、『*Cisco NGIPSv Quick Start Guide for VMware*』を参照してください。

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、vSphere Client 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 [英語]）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