FireSIGHT 仮想インストレーション ガイド

バージョン 5.4.1
2015 年 1 月 22 日

Cisco Systems, Inc.
www.cisco.com
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 サイトをご覧ください
www.cisco.com/go/offices

【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。

CONTENTS

仮想アプライアンスの概要

Cisco FireSIGHT® システムは、検出されたアプリケーション、ユーザ、および URL に基づいてネットワークへのアクセスを制御する機能と、業界トップのネットワーク侵入防御システムのセキュリティを統合したものです。

シスコは、VMware vSphere と VMware vCloud Director のホスティング環境用に 64 ビット仮想防御センターおよびバーチャル デバイスをパッケージ化しています。vCenter または VMware vCloud Director を使用して、64 ビット仮想防御センターと 64 ビット仮想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。

防御センターによって、システムの一元管理コンソールとデータベース リポジトリが提供されます。仮想デバイスは次のように、パッシブ展開またはインライン展開の仮想ネットワークまたは物理ネットワークのトラフィックを検査できます。

- パッシブ展開の仮想デバイスは、ネットワーク上を流れるトラフィックを単純に監視します。
- パッシブ センシング インターフェイスはすべてのトラフィックを無条件で受信し、これらのインターフェイスで受信されたトラフィックは再送信されません。
- インライン展開の仮想デバイスでは、ネットワーク上のホストの可用性、整合性、または機密性に影響を及ぼす可能性がある攻撃からネットワークを保護できます。インライン デバイスは単純な侵入防御システムとして展開できます。インライン デバイスを設定して、アクセス制御を実行したり、他の方法でネットワーク トラフィックを管理したりすることができます。
- インライン インターフェイスはすべてのトラフィックを無条件で受信し、展開環境での設定によって明示的に廃棄されている場合を除き、これらのインターフェイスで受信されたトラフィックは再送信されます。

仮想防御センターは物理デバイス、Blue Coat X-Series 向け Cisco NGIPS、および Cisco ASA with FirePOWER Services（ASA FirePOWER）を管理することができ、物理防御センターはバーチャル 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。仮想防御センター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 FireSIGHT システム アプライアンスの詳細については、『*FireSIGHT System Installation Guide*』を参照してください。

このインストール ガイドは、仮想 FireSIGHT システム アプライアンス（デバイスおよび防御センター）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。

次のトピックで FireSIGHT システム 仮想アプライアンスについて説明します。

FireSIGHT システム 仮想アプライアンス

FireSIGHT システム *仮想アプライアンス*は、トラフィック検知の管理対象 *バーチャル デバイス*か、または管理 *仮想*防御センターのいずれかになります。詳細については、次の項を参照してください。

仮想防御センター

防御センターは、FireSIGHT システム配置環境の集中管理ポイントとイベント データベースを提供します。仮想防御センターは、侵入、ファイル、マルウェア、検出、接続、およびパフォーマンス データを集約し、相互に関連付けます。これには、特定のホストにおけるイベントの影響を評価し、ホストにセキュリティ侵害をマークするタグ付けをすることが含まれます。これにより、デバイス間で交わされる情報の監視、ネットワーク上で発生するアクティビティ全体の評価や制御が可能になります。

仮想防御センターの主な機能は次のとおりです。

- デバイス、ライセンス、およびポリシーの管理
- 表、グラフ、図に表示されるイベント情報と状況情報
- ヘルスとパフォーマンスのモニタリング
- 外部通知とアラート
- リアルタイムに脅威に対処するための関連付け、侵害の痕跡、および修復機能
- カスタムもしくはテンプレートベースのレポート作成

仮想管理対象デバイス

組織内のネットワーク セグメントに展開されたバーチャル デバイスは、分析用にトラフィックをモニタします。パッシブに展開されたバーチャル デバイスは、ネットワーク トラフィック情報を把握するのに役立ちます。インライン展開の場合、仮想デバイスを使用して、複数の基準に基づいてトラフィック フローに影響を与えることができます。各デバイスには、モデルとライセンスに応じて次のような特徴があります。

- 組織のホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、および脆弱性に関する詳細情報を収集する

- ネットワークベースのさまざまな基準、およびアプリケーション、ユーザ、URL、IP アドレスの評価、および侵入やマルウェアの調査結果を含めた他の基準によって、ネットワーク トラフィックをブロックまたは許可する

仮想デバイスには Web インターフェイスが**ありません**。仮想デバイスはコンソールとコマンドラインを使用して設定し、防御センターで管理する必要があります。

仮想アプライアンスの機能について

仮想アプライアンスは物理アプライアンスの機能の多くを備えています。

- 仮想防御センターは、仮想防御センターの高可用性ペアを作成できないことを除き、物理防御センターと同じ機能を持っています。FireSIGHT ライセンスがある場合、仮想防御センターは 50,000 件のホストおよびユーザを監視できます。
- 仮想デバイスは物理デバイスのトラフィックおよびブロッキング分析機能を持っています。ただし、スイッチング、ルーティング、VPN、および他のハードウェア ベース、冗長性、およびリソース共有の機能は実行できません。

仮想防御センターの機能について

「表 1-1 仮想防御センターでサポートされる機能」(P.1-3)に、システムの主要な機能と仮想防御センターの比較を示します。ここでは、ユーザがそれらの機能をサポートするデバイスを管理し、適切なライセンスがインストールされ適用されていることを想定しています。

仮想アプライアンスでサポートされる機能およびライセンスの要約については、「FireSIGHT システム のコンポーネント」(P.1-7)および「仮想アプライアンスのライセンス」(P.1-12)を参照してください。

仮想防御センターは、シリーズ 2、シリーズ 3、ASA FirePOWER、およびX-シリーズ デバイスを管理できることに留意しておいてください。同様に、シリーズ 2 およびシリーズ 3 の防御センターは仮想デバイスを管理できます。デバイス ベース機能（スタック構成、スイッチング、ルーティングなど）に関する防御センターの列は、仮想防御センターがそれらの機能を実行するためにデバイスを管理および設定できるかどうかを示します。たとえば、仮想デバイスで VPN の設定はできませんが、仮想防御センターを使用すれば VPN 展開でシリーズ 3 デバイスを管理できます。

表 1-1　　仮想防御センターでサポートされる機能

特徴または機能	仮想防御センター
管理対象デバイスによって報告されるディスカバリ データ（ホスト、アプリケーション、およびユーザ）を収集し、組織のネットワーク マップを作成する	yes
ネットワーク トラフィックの位置情報データを表示する	yes
侵入検知と防御（IPS）の配置を管理する	yes
セキュリティ インテリジェンスのフィルタリングを実行するデバイスを管理する	yes
位置情報ベースのフィルタリングを含む単純なネットワークベース制御を実行するデバイスを管理する	yes
アプリケーション制御を実行するデバイスを管理する	yes
ユーザ制御を実行するデバイスを管理する	yes

表 1-1　仮想防御センターでサポートされる機能（続き）

特徴または機能	仮想防御センター
リテラル URL によってネットワーク トラフィックをフィルタリングするデバイスを管理する	yes
カテゴリおよびレピュテーション別の URL フィルタリングを実行するデバイスを管理する	yes
ファイル タイプによる単純なファイル制御を実行するデバイスを管理する	yes
ネットワークベースの高度なマルウェア対策（AMP）を実行するデバイスを管理する	yes
FireAMP 配置環境からエンドポイントベースのマルウェア（FireAMP）イベントを受信する	yes
デバイスベースのハードウェアベース機能を管理する • 高速パス ルール • 厳密な TCP の適用 • 設定可能バイパス インターフェイス • タップ モード • スイッチングとルーティング • NAT ポリシー • VPN	yes
デバイスベースの冗長性とリソース共有を管理する • デバイス スタック • デバイス クラスタ • Blue Coat X-Series 向け Cisco NGIPSの VAP グループ • クラスタ化スタック	yes
トラフィック チャネルを使用して、内部トラフィックとイベント トラフィックを分離して管理する	yes
複数の管理インターフェイスを使用して、異なるネットワーク上のトラフィックを分離して管理する	yes
ハイ アベイラビリティを確立する	no
マルウェア ストレージ パックをインストールする	no
eStreamer、ホスト入力、またはデータベース クライアントへの接続	yes

仮想管理対象デバイスの機能について

「表 1-2 仮想管理対象デバイスでサポートされる機能」（P.1-5）に、システムの主要な機能と管理対象デバイスの比較を示します。ここでは、管理防御センターから適切なライセンスがインストールされ適用されていることを想定しています。

バージョン 5.4.1 のシステムを実行する防御センターの任意のモデルを使用してバージョン 5.4.1 の仮想デバイスを管理できますが、いくつかのシステム機能は防御センターのモデルによって制限されることに留意してください。たとえば、仮想管理対象デバイスがセキュリティ

インテリジェンス フィルタリング機能をサポートしている場合でも、シリーズ 2 DC500 を使用してその機能を実行する仮想管理対象デバイスを管理することはできません。詳細については、「 仮想防御センターの機能について」(P.1-3)を参照してください。

表 1-2　仮想管理対象デバイスでサポートされる機能

特徴または機能	仮想管理対象デバイス
管理対象デバイスによって報告されるディスカバリ データ(ホスト、アプリケーション、およびユーザ)を収集し、組織のネットワーク マップを作成する	yes
ネットワーク トラフィックの位置情報データを表示する	yes
ネットワーク ディスカバリ:ホスト、アプリケーション、およびユーザ	yes
侵入検知および防御(IPS)	yes
セキュリティ インテリジェンス フィルタリング	yes
アクセス制御:基本的なネットワーク制御	yes
アクセス制御:位置情報ベースのフィルタリング	yes
アクセス制御:アプリケーション制御	yes
アクセス制御:ユーザ制御	yes
アクセス制御:リテラル URL	yes
アクセス制御:カテゴリとレピュテーションによる URL フィルタリング	yes
ファイル制御:ファイル タイプ別	yes
ネットワーク ベースの高度マルウェア防御(AMP)	yes
Automatic Application Bypass	yes
高速パス ルール	no
厳密な TCP の適用	no
設定可能バイパス インターフェイス	no
タップ モード	no
スイッチングとルーティング	no
NAT ポリシー	no
VPN	no
デバイス スタッキング	no
デバイス クラスタリング	no
クラスタ化スタック	no
トラフィック チャネル	no
複数の管理インターフェイス	no
マルウェア ストレージ パック	no
FireSIGHT システム固有のインタラクティブ CLI	yes
eStreamer クライアントへの接続	no

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 Tools 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作成については、VMware vCloud Director および VMware vCenter を含む VMwareESXi 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、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 1-3　　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	4 GB	可。仮想デバイスに対して次の量を割り当てる**必要**があります。 • 4 GB 以上 • カテゴリとレピュテーションに基づく URL フィルタリングを使用する場合は 5 GB • 大規模なダイナミック フィードを使用してセキュリティ インテリジェンスのフィルタリングを実行する場合は 6 GB • URL フィルタリングおよびセキュリティ インテリジェンスを実行する場合は 7 GB
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（デバイス） 250 GB（防御センター）	no

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

ヒント　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、『*FireSIGHT System User Guide*』を参照してください。

FireSIGHT システム のコンポーネント

続くセクションでは、組織のセキュリティ、アクセプタブル ユース ポリシー、およびトラフィック管理戦略に貢献する仮想防御センターおよびバーチャル デバイスの主要機能の一部について説明します。シリーズ 2 およびシリーズ 3 アプライアンスでサポートされる追加機能の詳細については、『*FireSIGHT System Installation Guide*』および『*FireSIGHT System User Guide*』を参照してください。

ヒント　仮想アプライアンス機能の多くは、ライセンスとユーザ ロールに依存します。必要に応じて、FireSIGHT システム のマニュアルに機能とタスクごとの要件が記載されています。

以下のトピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な FireSIGHT システム の主な機能について説明します。

- 「FireSIGHT」（P.1-8）
- 「アクセス コントロール」（P.1-8）
- 「侵入検知と侵入防御」（P.1-9）
- 「ファイルの追跡、コントロール、マルウェア防御」（P.1-9）
- 「アプリケーション プログラミング インターフェイス」（P.1-10）

FireSIGHT

FireSIGHT™ は、ネットワークの全体像を提供するためにホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、位置情報、および脆弱性に関する情報を収集するシスコのディスカバリおよび認識テクノロジーです。

防御センターの Web インターフェイスを使用して、FireSIGHT で収集したデータを表示および分析することができます。また、このデータを使用することで、アクセス コントロールを実施し、侵入ルールの状態を修正できます。また、ホストの相関イベント データに基づいて、ネットワーク上のホストの侵害の痕跡を生成し、追跡できます。

アクセス コントロール

*アクセス制御*はポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録することが可能です。*アクセス制御ポリシー*は、ネットワーク上のトラフィックをシステムがどのように処理するかを決定します。*アクセス制御ルール*が含まれていないポリシーを使用して、*デフォルト アクション*と呼ばれる以下のいずれかの方法でトラフィックを処理することができます。

- すべてのトラフィックをブロックして、ネットワークに入れない
- すべてのトラフィックを信頼してネットワークに入ることを許可し、検査は行わない
- すべてのトラフィックがネットワークに入ることを許可し、ネットワーク ディスカバリ ポリシーのみを使用してトラフィックを検査する
- すべてのトラフィックがネットワークに入ることを許可し、侵入ポリシーとネットワーク ディスカバリ ポリシーを使用してトラフィックを検査する

アクセス制御ポリシーにアクセス制御ルールを含めて、対象のデバイスがトラフィックをどのように処理するか(簡単な IP アドレスのマッチングから、異なるユーザ、アプリケーション、ポート、および URL が関与する複雑なシナリオまで)、より詳しく定義することができます。それぞれのルールについて、ユーザはルールの *アクション*、つまり侵入またはファイル ポリシーと一致するトラフィックを信頼、監視、ブロック、または検査するかどうかを指定します。

それぞれのアクセス制御ポリシーについてカスタム HTML ページを作成することができます。このページは、システムが HTTP 要求をブロックするときに表示されます。オプションで、ユーザに警告するページを表示することができますが、ユーザはボタンをクリックして最初に要求されたサイトの表示を継続できるようにすることも可能です。

アクセス制御の一部として、セキュリティ インテリジェンス機能により、トラフィックがアクセス制御ルールによって分析される前に特定の IP アドレスをブラックリストに登録(トラフィックの入出を拒否)することができます。システムで地理情報をサポートしている場合は、検出された送信元および宛先の国および大陸に基づいて、トラフィックをフィルタすることもできます。

アクセス制御には、侵入の検知および防御、ファイル コントロール、および高度なマルウェア防御が含まれています。詳細については、次の項を参照してください。

侵入検知と侵入防御

侵入検知および防御により、ユーザはセキュリティ違反のネットワーク トラフィックを監視し、インラインの展開で、悪意のあるトラフィックをブロックまたは改正することができます。

侵入防御はアクセス制御に組み込まれており、ユーザは侵入ポリシーと特定のアクセス制御ルールを関連付けることができます。ネットワーク トラフィックがルールの条件と一致する場合、一致するトラフィックを、侵入ポリシーを使用して分析できます。また、侵入ポリシーをアクセス制御ポリシーのデフォルト アクションに関連付けることもできます。

侵入ポリシーは次のようなさまざまな要素で構成されます。

- プロトコル ヘッダー値、ペイロードの内容、および特定のパケット サイズの特性を検査するルール
- FireSIGHT の推奨事項に基づくルール状態設定
- プリプロセッサやその他の検出およびパフォーマンス機能などの高度な設定
- 関連するプリプロセッサとプリプロセッサ オプション用のイベントを生成可能なプリプロセッサ ルール

ファイルの追跡、コントロール、マルウェア防御

マルウェアの影響を特定し、軽減することを容易にするために、FireSIGHT システム のファイル制御、ネットワーク ファイルのトラジェクトリ、および高度なマルウェア防御のコンポーネントはネットワーク トラフィック内のファイルの伝送を（マルウェア ファイルも含めて）検出、追跡、取得、分析、およびオプションでブロックすることができます。

ファイル制御

*ファイル制御*により、管理対象デバイスは、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。ファイル制御は、全体的なアクセス制御設定の一部として設定します。アクセス制御ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

ネットワークベースの高度なマルウェア防御（AMP）

ネットワークベースの*高度なマルウェア対策*（AMP）によって、複数のファイル タイプのマルウェアに関してネットワーク トラフィックを検査できます。バーチャル デバイスは、詳細な分析を行うために、検出されたファイルをハード ドライブに保存できます。

検出されたファイルは、保存済みかどうかに関係なく、ファイルの SHA-256 ハッシュ値を使用して単純な既知の性質の検索を行うために Collective Security Intelligence クラウド に送信できます。また、脅威のスコアを生成する*動的分析*を行うためにファイルを送信することもできます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

マルウェア防御をアクセス制御設定全体の一部として設定することができます。アクセス制御ルールに関連付けられているファイル ポリシーは、ルールの条件に一致するネットワーク トラフィックを検査します。

FireAMP の統合

FireAMP はシスコのエンタープライズクラスの高度なマルウェア分析および防御ソリューションで、高度なマルウェアの発生、高度で継続的な脅威、および標的型攻撃を検出、認識、ブロックします。

組織に FireAMP のサブスクリプションがある場合は、個々のユーザが自分のコンピュータやモバイル デバイス（*エンドポイント*とも呼ばれる）に*FireAMP コネクタ*をインストールします。これらの軽量エージェントが Collective Security Intelligence クラウドと通信し、次に Collective Security Intelligence クラウドが防御センターと通信します。

防御センターをクラウドに接続するように設定した後で防御センターの Web インターフェイスを使用して、組織のエンドポイントでのスキャン、検出、および検疫の結果として生成されたエンドポイントベースのマルウェア イベントを表示することができます。また、防御センターは FireAMP のデータを使用して、ホストに対する侵害の痕跡を生成および追跡するとともに、ネットワーク ファイルのトラジェクトリを表示します。

FireAMP 展開を構成するには、*FireAMP* ポータルを使用します。ポータルは、マルウェアをすばやく特定および検疫するうえで有用です。ユーザはマルウェアを発生時に特定し、それらのトラジェクトリを追跡して影響を把握し、正常にリカバリする方法を学習することができます。FireAMP を使用してカスタム保護を作成する、グループ ポリシーに基づいて特定のアプリケーションの実行をブロックする、カスタム ホワイトリストを作成する、といったことも可能です。

詳細については、http://amp.sourcefire.com/を参照してください。

ネットワーク ファイルのトラジェクトリ

ネットワーク ファイル トラジェクトリ機能を使用すれば、ネットワーク全体のファイルの伝送パスを追跡することができます。システムは SHA-256 ハッシュ値を使用してファイルを追跡するため、ファイルを追跡するには、システムで以下のいずれかの処理を行う必要があります。

- ファイルの SHA-256 ハッシュ値を計算し、その値を使用してマルウェアのクラウド ルックアップを実行する
- 防御センターと組織の FireAMP サブスクリプションとの統合を使用して、ファイルについてエンドポイントベースの脅威および検疫データを受け取る

各ファイルには、関連するトラジェクトリ マップが付随しており、これには、一定期間のファイルの転送を視覚的に表したものや、ファイルに関する追加情報が含まれています。

アプリケーション プログラミング インターフェイス

アプリケーション プログラミング インターフェイス（API）を使用してシステムと対話する方法がいくつかあります。詳細については、サポート サイトから追加のドキュメントをダウンロードできます。

eStreamer

Event Streamer（eStreamer）を使用すれば、シスコ アプライアンスからの数種類のイベント データをカスタム開発されたクライアント アプリケーションにストリーム配信できます。クライアント アプリケーションを作成したら、ユーザはそれを eStreamer サーバ（防御センターまたは管理対象デバイス）に接続し、eStreamer サービスを開始して、データのやりとりを始めることができます。

eStreamer の統合ではカスタム プログラミングが必要ですが、これによりユーザはアプライアンスの特定のデータを要求することができます。たとえば、ネットワーク管理アプリケーションの 1 つにネットワーク ホスト データを表示する場合、防御センターからホストの重要度または脆弱性のデータを取得し、その情報を表示に追加するためのプログラムを記述することができます。

外部データベースのアクセス

データベース アクセス機能によって、JDBC SSL 接続をサポートするサードパーティ製クライアントを使用して防御センター上の複数のデータベース テーブルを照会できます。

Crystal Reports、Actuate BIRT、JasperSoft iReport などの業界標準のレポート作成ツールを使用してクエリを作成し、送信することができます。また、独自のカスタム アプリケーションを設定してシスコ データをクエリすることもできます。たとえば、侵入およびディスカバリ イベント データについて定期的にレポートしたり、アラート ダッシュボードをリフレッシュしたりするサーブレットを構築することが可能です。

ホスト入力

ホスト入力機能では、スクリプトまたはコマンドライン ファイルを使用してサードパーティのソースからデータをインポートすることにより、ネットワーク マップの情報を増やすことができます。

Web インターフェイスにもいくつかのホスト入力機能があります。これらの機能では、オペレーティング システムまたはアプリケーション プロトコルの識別情報を変更し、脆弱性を有効化または無効化し、ネットワーク マップからさまざまな項目（クライアントやサーバ ポーとなど）を削除することができます。

修復

システムには、ネットワークの状況が関連する相関ポリシーやコンプライアンス ホワイトリストに違反したときに、防御センターが自動的に起動できる修復の作成を可能にする API が含まれます。これにより、ユーザが攻撃に即時に対処できない場合でも攻撃の影響を自動的に緩和でき、またシステムが組織のセキュリティ ポリシーに準拠し続けるようにすることができます。お客様が作成する修復のほかに、防御センターにはいくつかの事前定義された修復モジュールが付属しています。

複数の管理インターフェイス

シリーズ 3 アプライアンスおよび仮想防御センターで *複数の管理インターフェイス*を使用して、2 つのトラフィック チャネル（デバイス間通信を行う *管理トラフィック チャネル*および Web アクセスなどの外部トラフィックを伝送する *イベント トラフィック チャネル*）にトラフィックを分離することによって、パフォーマンスを向上できます。両方のトラフィック チャネルを同じ管理インターフェイス上で伝送することも、2 つの管理インターフェイスに分割して各インターフェイスで 1 つずつトラフィック チャネルを伝送することもできます。

防御センター上の特定の管理インターフェイスから別のネットワークまでのルートを作成することにより、あるネットワーク上のデバイスからのトラフィックと別のネットワーク上のデバイスからのトラフィックを、防御センターで別々に管理することができます。

追加の管理インターフェイスは、次の例外を除いて、デフォルトの管理インターフェイスと同じように機能（防御センター間でのハイ アベイラビリティを使用など）します。

- DHCP は、デフォルト（`eth0`）管理インターフェイスにのみ設定できます。追加のインターフェイス（`eth1` など）には、固有の静的 IP アドレスとホスト名が必要です。
- デフォルト以外の管理インターフェイスを使用して防御センターと管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。
- 70xx ファミリでは、2 つのチャネルにトラフィックを分離し、それらのチャネルが仮想防御センターの 1 つ以上の管理インターフェイスにトラフィックを送信するように設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上で防御センターから送信されたトラフィックを受信します。

アプライアンスを設置した後、Web ブラウザを使用して複数の管理インターフェイスを設定します。管理インターフェイスを仮想防御センターに追加する方法については、「インターフェイスの追加と構成」(P.4-10)を参照してください。詳細については、『*FireSIGHT System User Guide*』の「Multiple Management Interfaces」を参照してください。

仮想アプライアンスのライセンス

組織に対して FireSIGHT システム の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。防御センターを使用して、それ自身と管理対象デバイスのライセンスを管理する必要があります。

シスコ は、防御センターの初期設定時に、購入したライセンスを追加することを推奨します。そうしない場合、初期設定時に登録するデバイスは、未ライセンスとして防御センターに追加されます。この場合、初期設定プロセスが終了した後で、各デバイスで個別にライセンスを有効化する必要があります。詳細については、「仮想アプライアンスの設定」(P.5-1)を参照してください。

FireSIGHT ライセンスは、防御センターの各購入に含まれており、ホスト、アプリケーション、およびユーザ ディスカバリを実行するために必要です。防御センター上の FireSIGHT ライセンスにより、防御センターおよびその管理対象デバイスで監視可能なホスト数とユーザ数と、ユーザ制御を許可するユーザ数も決定されます。仮想防御センターの場合、この制限は 50,000 の個別のホストおよびユーザです。

防御センターが以前バージョン 4.10.x を実行していた場合は、FireSIGHT ライセンスの代わりに、従来の RNA ホスト ライセンスと RUA ユーザ ライセンスを使用できる場合があります。詳細については、「ライセンス設定」(P.5-11)を参照してください。

モデル固有ライセンスを追加すれば、管理対象デバイスは、次のように、さまざまな機能を実行できます。

保護

保護ライセンスにより、仮想デバイスは侵入検知と防御、ファイル管理、およびセキュリティ インテリジェンス フィルタリングを実行できます。

Control

Control ライセンスにより、仮想デバイスはユーザおよびアプリケーションの制御を実行できます。仮想デバイスは、Control ライセンスによって シリーズ 2 デバイスおよび シリーズ 3 デバイスに付与されるハードウェア ベースのいずれの機能（スイッチングまたはルーティングなど）もサポートしませんが、仮想防御センターは物理デバイスでそうした機能を管理できます。Control ライセンスには保護ライセンスが必要です。

URL フィルタリング

URL フィルタリング ライセンスにより、仮想デバイスは定期的に更新されるクラウドベースのカテゴリとレピュテーションのデータを使用して、監視対象ホストが要求した URL に基づいて、ネットワークを通過できるトラフィックを判別できます。URL フィルタリング ライセンスには保護ライセンスが必要です。

マルウェア

マルウェア ライセンスにより、仮想デバイスはネットワークベースの高度なマルウェア防御（AMP）を実行できます。これはネットワーク上で転送されるファイルに含まれるマルウェアを検出し、ブロックする機能です。また、ネットワーク上で転送されるファイルを追跡するトラジェクトリを表示することもできます。マルウェア ライセンスには保護ライセンスが必要です。

VPN

VPN ライセンスにより、仮想防御センターを使用して、シリーズ 3 デバイス上の仮想ルータ間、または シリーズ 3 デバイスからリモート デバイスまたは他のサードパーティ製 VPN エンドポイントへセキュアな VPN トンネルを構築できます。VPN ライセンスには、保護ライセンスとControlライセンスが必要です。

アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではありません。一般に、デバイスがサポートしていない機能のライセンスは付与できません。「 仮想アプライアンスの機能について」(P.1-3) を参照してください。

次の表に、防御センターに追加して、各デバイス モデルに適用可能なライセンスの概要を示します。防御センターの行(FireSIGHT を除くすべてのライセンス)は、防御センターがそれらのライセンスを使用してデバイスを管理できるかどうかを示します。たとえば、シリーズ 3 デバイスを使用した VPN 展開を構築するために シリーズ 2 DC1000 を使用できますが、カテゴリおよびレピュテーション ベースの URL フィルタリングを実行するために DC500 を使用することはできません(管理されるデバイスとは無関係に)。なお、n/a は、管理対象デバイスとは関係のない防御センター ベースのライセンスを示します。

表 1-4　　各モデルによってサポートされるライセンス

モデル	FireSIGHT	保護	Control	URL フィルタリング	マルウェア	VPN
シリーズ 2 デバイス: • 3D500、3D1000、3D2000 • 3D2100、3D2500、3D3500、3D4500 • 3D6500 • 3D9900	n/a	自動、セキュリティ インテリジェンスなし	no	no	no	no
シリーズ 3 デバイス: • 7000 シリーズ • 8000 シリーズ	n/a	yes	yes	yes	yes	yes
仮想デバイス	n/a	yes	はい、ただしハードウェア機能のサポートなし	yes	yes	no
Cisco ASA with FirePOWER Services	n/a	yes	はい、ただしハードウェア機能のサポートなし	yes	yes	no
Blue Coat X-Series 向け Cisco NGIPS	n/a	yes	はい、ただしハードウェア機能のサポートなし	yes	yes	no
シリーズ 2 防御センター: • DC500	yes	はい、ただしセキュリティ インテリジェンスなし	はい、ただしユーザ制御なし	no	no	yes
シリーズ 2 防御センター: • DC1000、DC3000	yes	yes	yes	yes	yes	yes

表 1-4　各モデルによってサポートされるライセンス（続き）

モデル	FireSIGHT	保護	Control	URL フィルタリング	マルウェア	VPN
シリーズ 3 防御センター: • DC750、DC1500、DC3500、DC2000、DC4000	yes	yes	yes	yes	yes	yes
仮想の防御センター	yes	yes	yes	yes	yes	yes

ライセンスの詳細については、『*FireSIGHT System User Guide*』の章「FireSIGHT システム のライセンス」を参照してください。

セキュリティ、インターネット アクセス、および通信ポート

防御センターを保護するには、保護された内部ネットワークに防御センターをインストールする必要があります。防御センターは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

防御センターとその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、防御センターと同じ保護された内部ネットワークに接続できます。これにより、防御センターからデバイスを安全に制御することができます。また、防御センターでその他のネットワーク上にあるデバイスからのトラフィックを管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法とは無関係に、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

また、FireSIGHT システムの機能によってはインターネット接続が必要となることにも注意してください。デフォルトで、すべてのアプライアンスはインターネットに直接接続するよう設定されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的は基本的なアプライアンス間通信、セキュアなアプライアンス アクセス、および特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にすることです。

ヒント　Blue Coat X-Series 向け Cisco NGIPS と Cisco ASA with FirePOWER Services を除いて、FireSIGHT システム アプライアンスではプロキシ サーバを使用できます。詳細については、『*FireSIGHT System User Guide*』を参照してください。

詳細については、以下を参照してください。

- 「 インターネット アクセス要件」（P.1-15）
- 「 通信ポートの要件」（P.1-16）

インターネット アクセス要件

仮想防御センターは、デフォルトでオープンしているポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに直接接続するように設定されます。バーチャル デバイスでは、マルウェア ライセンスを有効にしている場合のみ、ポート 443 がオープンします。このポートがオープンしていると、デバイスは動的分析のためにファイルを送信できます。詳細については、「通信ポートの要件」（P.1-16）を参照してください。FireSIGHT 仮想アプライアンスはプロキシ サーバの使用をサポートしています。詳細については、『*FireSIGHT System User Guide*』を参照してください。プロキシ サーバは whois アクセスに使用できない点にも注意が必要です。

次の表に、FireSIGHT システムの特定の機能におけるインターネット アクセス要件を示します。

表 1-5　FireSIGHT システム機能のインターネット アクセス要件

機能	インターネット アクセスが必要な動作	アプライアンス
動的分析：照会	動的分析のために、提出済みファイルの脅威スコアを Collective Security Intelligence クラウドに照会します。	防御センター
動的分析：送信	動的分析のためにファイルを Collective Security Intelligence クラウドに提出します。	管理対象デバイス
FireAMP 統合	エンドポイント ベースの（FireAMP）マルウェア イベントを Collective Security Intelligence クラウドから受信します。	防御センター
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	防御センター
ネットワークベースの AMP	マルウェア クラウド検索を実行します。	防御センター
RSS フィード ダッシュボード ウィジェット	シスコ を含む外部ソースから RSS フィード データをダウンロードします。	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）
セキュリティ インテリジェンス フィルタリング	FireSIGHT システム インテリジェンス フィードを含む外部ソースからのセキュリティ インテリジェンス フィード データをダウンロードします。	防御センター
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）
URL フィルタリング	クラウドベースの URL カテゴリおよびレピュテーション データをアクセス制御用にダウンロードし、カテゴライズされていない URL に対してルックアップを実行します。	防御センター
whois	外部ホストの whois 情報を要求します。	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）

通信ポートの要件

FireSIGHT システム アプライアンスは、(デフォルトでポート 8305/tcp を使用する)双方向 SSL 暗号化通信チャネルを使って通信します。基本的なアプライアンス間通信用にこのポートを開いたままにする**必要があります**。他のオープン ポートの役割は次のとおりです。

- アプライアンスの Web インターフェイスにアクセスする
- アプライアンスへのリモート接続を保護する
- 特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にする

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。たとえば、ユーザ エージェントに防御センターを接続するまで、エージェントの通信ポート(3306/tcp)は閉じられたままです。別の例としては、LOM を有効にするまで、シリーズ 3 アプライアンスのポート 623/udp は閉じられたままです。

注意　オープンしているポートを閉じると展開にどのような影響が生じるかを理解するまで、オープンしているポートを閉じないでください。

たとえば、管理デバイスのポート 25/tcp(SMTP)アウトバウンドを閉じると、デバイスによる個々の侵入イベントに関する電子メール通知の送信がブロックされます(『*FireSIGHT System User Guide*』を参照)。別の例としては、ポート 443/tcp(HTTPS)を閉じることによって、物理管理対象デバイスの Web インターフェイスへのアクセスを無効にできますが、これにより、デバイスはマルウェアと疑われるファイルを動的分析のために Collective Security Intelligence クラウドに送信することもできなくなります。

次のように、システムのいくつかの通信ポートを変更できることに注意してください。

- システムと認証サーバの間の接続を設定する場合に、LDAP および RADIUS 認証用にカスタム ポートを指定できます。『*FireSIGHT System User Guide*』を参照してください。
- 管理ポート(8305/tcp)は変更できます。『*FireSIGHT System User Guide*』を参照してください。ただし、シスコでは、デフォルト設定を維持することを**強く**推奨しています。管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。
- アップグレードした防御センターが Collective Security Intelligence クラウドと通信できるようにするため、ポート 32137/tcp を使用できます。ただし、シスコでは、バージョン 5.3 以降の新規インストールのデフォルトであるポート 443 に切り替えることを推奨しています。詳細については、『*FireSIGHT System User Guide*』を参照してください。

次の表は、FireSIGHT システムの機能を最大限に活用できるように、各アプライアンス タイプで必要なオープン ポートを示しています。

表 1-6　FireSIGHT システムの機能と操作のデフォルト通信ポート

ポート	説明	方向	開いているアプライアンス	目的
22/tcp	SSH/SSL	双方向	すべて	アプライアンスへのセキュアなリモート接続を許可します。
25/tcp	SMTP	発信	すべて	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	すべて	DNS を使用します。

表 1-6　FireSIGHT システムの機能と操作のデフォルト通信ポート （続き）

ポート	説明	方向	開いているアプライアンス	目的
67/udp 68/udp	DHCP	発信	すべて（X-シリーズ を除く）	DHCP を使用します。 **（注）** これらのポートはデフォルトで**閉じられています**。
80/tcp	HTTP	発信	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）	RSS フィード ダッシュボード ウィジェットからリモート Web サーバに接続できるようにします。
		双方向	防御センター	HTTP 経由でカスタムおよびサードパーティのセキュリティ インテリジェンス フィードを更新します。 URL カテゴリおよびレピュテーション データをダウンロードします（さらにポート 443 も必要）。
161/udp	SNMP	双方向	X-シリーズ と ASA FirePOWER を除くすべて	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	すべて	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	すべて（仮想デバイスと X-シリーズ を除く）	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	防御センター	検出された LDAP ユーザに関するメタデータを取得します。
443/tcp	HTTPS	着信	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）	アプライアンスの Web インターフェイスへのアクセス。

表 1-6　FireSIGHT システムの機能と操作のデフォルト通信ポート （続き）

ポート	説明	方向	開いているアプライアンス	目的
443/tcp	HTTPS AMQP クラウド通信	双方向	防御センター	次のものを取得します。 • ソフトウェア、侵入ルール、VDB、および GeoDB の更新 • URL カテゴリおよびレピュテーション データ（さらにポート 80 も必要） • 共有されたセキュリティ インテリジェンス フィードと他のセキュアなセキュリティ インテリジェンス フィード • エンドポイント ベース（FireAMP）のマルウェア イベント • ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質 • 送信されたファイルに関する動的分析情報
			シリーズ 2 デバイスと シリーズ 3 デバイス	デバイスのローカル Web インターフェイスを使用してソフトウェア更新をダウンロードします。
			シリーズ 3、仮想デバイス、X-シリーズ、および ASA FirePOWER	動的分析のためにファイルを送信します。
514/udp	syslog	発信	すべて	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	双方向	シリーズ 3	Serial Over LAN（SOL）接続を使用して Lights-Out Management を実行できるようにします。
1500/tcp 2000/tcp	着信	TCP	防御センター	サードパーティ クライアントによるデータベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	双方向	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）	外部認証とアカウンティングのために RADIUS サーバと通信します。
3306/tcp	User Agent	着信	防御センター	ユーザ エージェントと通信します。
8302/tcp	eStreamer	双方向	すべて（仮想デバイスと X-シリーズ を除く）	eStreamer クライアントと通信します。
8305/tcp	デバイス管理	双方向	すべて	展開におけるアプライアンス間で安全に通信します。**必須です**。
8307/tcp	ホスト入力クライアント	双方向	防御センター	ホスト入力クライアントと通信します。
32137/tcp	クラウド通信	双方向	防御センター	アップグレード対象の防御センター とCollective Security Intelligence クラウド クラウドの通信を可能にします。

CHAPTER 2

管理ネットワークでの展開

FireSIGHT システム は、それぞれ固有のネットワーク アーキテクチャのニーズに応じて展開することができます。防御センターが、FireSIGHT システム の集中管理コンソールおよびデータベース リポジトリとなります。トラフィック接続を収集して分析するために、複数のネットワーク セグメントにデバイスを設置します。

防御センターは管理インターフェイスを使用して、*信頼できる管理ネットワーク*(つまり、公開されている外部トラフィックではない安全な内部ネットワーク)に接続します。次にデバイスは、管理インターフェイスを使用して防御センターに接続します。

(注) ASA FirePOWER のデバイスの展開シナリオについて詳しくは、ASA のマニュアルを参照してください。

インターフェイス オプションの詳細については、以下の項を参照してください。

管理展開に関する考慮事項

管理展開の決定は、さまざまな要因に基づいて行われます。以下の質問に答えることは、最も効率的かつ効果的なシステムを構成するための展開オプションの理解に役立ちます。

- デフォルトの単一の管理インターフェイスを使用してデバイスを防御センターに接続しますか? パフォーマンスを向上したり、防御センターで受信した別のネットワークからのトラフィックを分離するために、追加の管理インターフェイスを有効化しますか? 詳細については、「管理インターフェイスについて」(P.2-2) を参照してください。
- パフォーマンスを向上するために、トラフィック チャネルを有効化して防御センターと管理対象デバイスの間に 2 つの接続を作成しますか? 防御センターと管理対象デバイスの間のスループット容量をさらに増加するために、複数の管理インターフェイスを使用しますか? 詳細については、「複数のトラフィック チャネルを持つ場合の展開」(P.2-3) を参照してください。
- 単一の防御センターを使用して、別のネットワーク デバイスからのトラフィックを管理および分離しますか? 詳細については、「ネットワーク ルートを持つ場合の展開」(P.2-5) を参照してください。

- 保護された環境に管理インターフェイスを展開しますか? アプライアンスのアクセスは、特定のワークステーション IP アドレスに制限されますか?「セキュリティの考慮事項」(P.2-6) には、管理インターフェイスを安全に展開するための考慮事項が説明されています。

管理インターフェイスについて

管理インターフェイスは、防御センターが管理するすべてのデバイスと防御センターの間の通信手段を提供します。アプライアンス間のトラフィック制御を正常に維持することが、展開の成功に不可欠です。

シリーズ 3 アプライアンスおよび仮想防御センター上では、防御センターまたはデバイス上、あるいは両方の管理インターフェイスを使用して、アプライアンス間のトラフィックを 2 種類のトラフィック チャネルに分類できます。管理トラフィック チャネルは、すべての内部トラフィック(アプライアンスおよびシステムの管理専用のデバイス間トラフィックなど)を伝送し、イベント トラフィック チャネルは、すべてのイベント トラフィック(Web イベントなど)を伝送します。トラフィックを 2 つのチャネルに分割することにより、アプライアンス間に 2 つの接続ポイントが作成されてスループットが増大するために、パフォーマンスが向上します。また、*複数の管理インターフェイス*を有効化して、アプライアンス間のスループットをさらに向上させたり、異なるネットワーク上のデバイス間のトラフィックの管理と分離を行うこともできます。

デバイスを防御センターに登録した後、各アプライアンスの Web ブラウザを使用してデフォルト設定を変更し、トラフィック チャネルや複数の管理インターフェイスの有効化ができます。設定については、『*FireSIGHT System User Guide*』の「Configuring Appliance Settings」を参照してください。

管理インターフェイスの使用に関する詳細については、以下の項を参照してください。

- 「単一の管理インターフェイス」(P.2-2)
- 「複数の管理インターフェイス」(P.2-3)

単一の管理インターフェイス

ライセンス:すべて

サポートされる防御センター:すべて

サポートされるデバイス:すべて

デバイスを防御センターに登録すると、防御センター上の管理インターフェイスとデバイス上の管理インターフェイス間のすべてのトラフィックを伝送する単一通信チャネルが確立されます。

以下の図に、デフォルトの単一通信チャネルを示します。1 つのインターフェイスにより、管理トラフィックとイベント トラフィックの両方が 1 つの通信チャネルで伝送されます。

複数の管理インターフェイス

ライセンス:すべて

サポートされる防御センター:シリーズ 3、仮想

サポートされるデバイス:シリーズ 3

複数の管理インターフェイスを有効化および設定し、それぞれに固有の IPv4 または IPv6 アドレス(および必要に応じて固有のホスト名)を割り当て、各 トラフィック チャネルを異なる管理インターフェイスに送信することよに、トラフィック スループットを大幅に向上できます。負荷が軽い管理トラフィックの搬送用には小さなインターフェイスを構成し、負荷が大きいイベント トラフィックの搬送用には大きなインターフェイスを構成します。デバイスを別々の管理インターフェイスに登録し、同一のインターフェイスに対して両方のトラフィック チャネルを構成したり、防御センターによって管理されるすべてのデバイスのイベント トラフィック チャネルを専用の管理インターフェイスで伝送することができます。

また、防御センター 上の特定の管理インターフェイスから別のネットワークへのルートを作成することにより、防御センター で、あるネットワーク上のデバイスからのトラフィックと別のネットワーク上のデバイスからのトラフィックを別々に管理することもできます。

追加の管理インターフェイスは、次の例外を除いて、デフォルトの管理インターフェイスと同じように機能(防御センター間でのハイ アベイラビリティを使用など)します。

- DHCP は、デフォルト(`eth0`)管理インターフェイスにのみ設定できます。追加のインターフェイス(`eth1` など)には、固有の静的 IP アドレスとホスト名が必要です。
- デフォルト以外の管理インターフェイスを使用して防御センターと管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。
- 70xx ファミリでは、2 つのチャネルにトラフィックを分離し、それらのチャネルが仮想防御センターの 1 つ以上の管理インターフェイスにトラフィックを送信するように設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上で防御センターから送信されたトラフィックを受信します。

展開オプション

トラフィック チャネルを使用してトラフィック フローを管理することで、1 つ以上の管理インターフェイスを使用してシステムのパフォーマンスを向上させることができます。さらに、防御センターおよびその管理対象デバイス上の専用の管理インターフェイスを使用して別のネットワークまでのルートを作成することにより、異なるネットワーク上のデバイス間のトラフィックを分離することもできます。詳細については、次の項を参照してください。

複数のトラフィック チャネルを持つ場合の展開

ライセンス:すべて

サポートされる防御センター:シリーズ 3、仮想

サポートされるデバイス:シリーズ 3

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、防御センターと管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。

次の例は、同じインターフェイス上に 2 つの独立したトラフィック チャネルを持つ通信チャネルを示しています。

複数の管理インターフェイスを使用する場合、トラフィック チャネルを 2 つの管理インターフェイスに分割することによりパフォーマンスを向上できます。それによって両方のインターフェイス容量が増し、トラフィック フローが増加します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

次の図は、2 つの管理インターフェイス上にある管理トラフィック チャネルとイベント トラフィック チャネルを示しています。

専用の管理インターフェイスを使用して、複数のデバイスからのイベント トラフィックのみを伝送することができます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、防御センター上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

以下の図では、2 台のデバイスが別々の管理チャネル トラフィック インターフェイスを使用し、イベント トラフィック チャネルに対しては同じ専用インターフェイスを共有しています。

ネットワーク ルートを持つ場合の展開

ライセンス:すべて

サポートされる防御センター:シリーズ 3、仮想

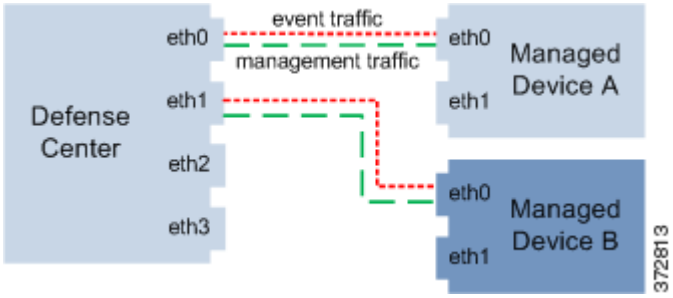
サポートされるデバイス:シリーズ 3

防御センター上の特定の管理インターフェイスから別のネットワークまでのルートを作成できます。そのネットワークのデバイスを防御センター上の指定された管理インターフェイスに登録すると、別のネットワーク上のデバイスと防御センターの間で独立した接続が実現されます。両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定することで、そのデバイスからのトラフィックが他のネットワーク上のデバイス トラフィックから確実に分離された状態を維持できます。ルーテッド インターフェイスは防御センター上の他のすべてのインターフェイスから分離されているため、ルーテッド管理インターフェイスに障害が発生した場合、接続が失われます。

ヒント デバイスを、デフォルト（`eth0`）の管理インターフェイス以外の管理インターフェイスの静的 IP アドレスに登録する必要があります。DHCP は、デフォルトの管理インターフェイスだけでサポートされています。

防御センターをインストールした後、Web インターフェイスを使用して、複数の管理インターフェイスを設定します。詳しくは、『*FireSIGHT System User Guide*』の「Configuring Appliance Settings」を参照してください。

次の図では、2 つのデバイスですべてのトラフィックに対して別々の管理インターフェイスを使用することにより、ネットワーク トラフィックを分離しています。さらに管理インターフェイスを追加して、デバイスごとに独立した管理トラフィック チャネル インターフェイスとイベント トラフィック チャネル インターフェイスを構成できます。



防御センターに 8000 シリーズ の管理対象デバイスを登録するときは、接続の両側で自動ネゴシエーションするか、または両側を同じ固定速度に設定して安定したネットワーク リンクを確保する必要があります。8000 シリーズ 管理対象デバイスは、半二重ネットワーク リンクをサポートしません。また、接続の反対側と異なる速度またはデュプレックス コンフィギュレーションもサポートしません。

セキュリティの考慮事項

管理インターフェイスを安全な環境に展開するために、シスコでは次の事項を考慮することを推奨しています。

- 管理インターフェイスは、必ず、不正アクセスから保護された信頼できる内部管理ネットワークに接続します。
- アプライアンスへのアクセスを許可可能な特定のワークステーションの IP アドレスを特定します。アプライアンスのシステム ポリシー内のアクセス リストを使用している特定のホストにアプライアンスへのアクセスを限定します。詳細については、『*FireSIGHT System User Guide*』を参照してください。

仮想アプライアンスの展開

仮想デバイスと仮想防御センターを使用して、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防御センターにより、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防御センターを使用できます。IPv4 または IPv6 のネットワークに展開できます。また、防御センター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、仮想防御センターで 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。複数の管理インターフェイスの詳細については、『FireSIGHT System User Guide』の「Managing Devices」を参照してください。

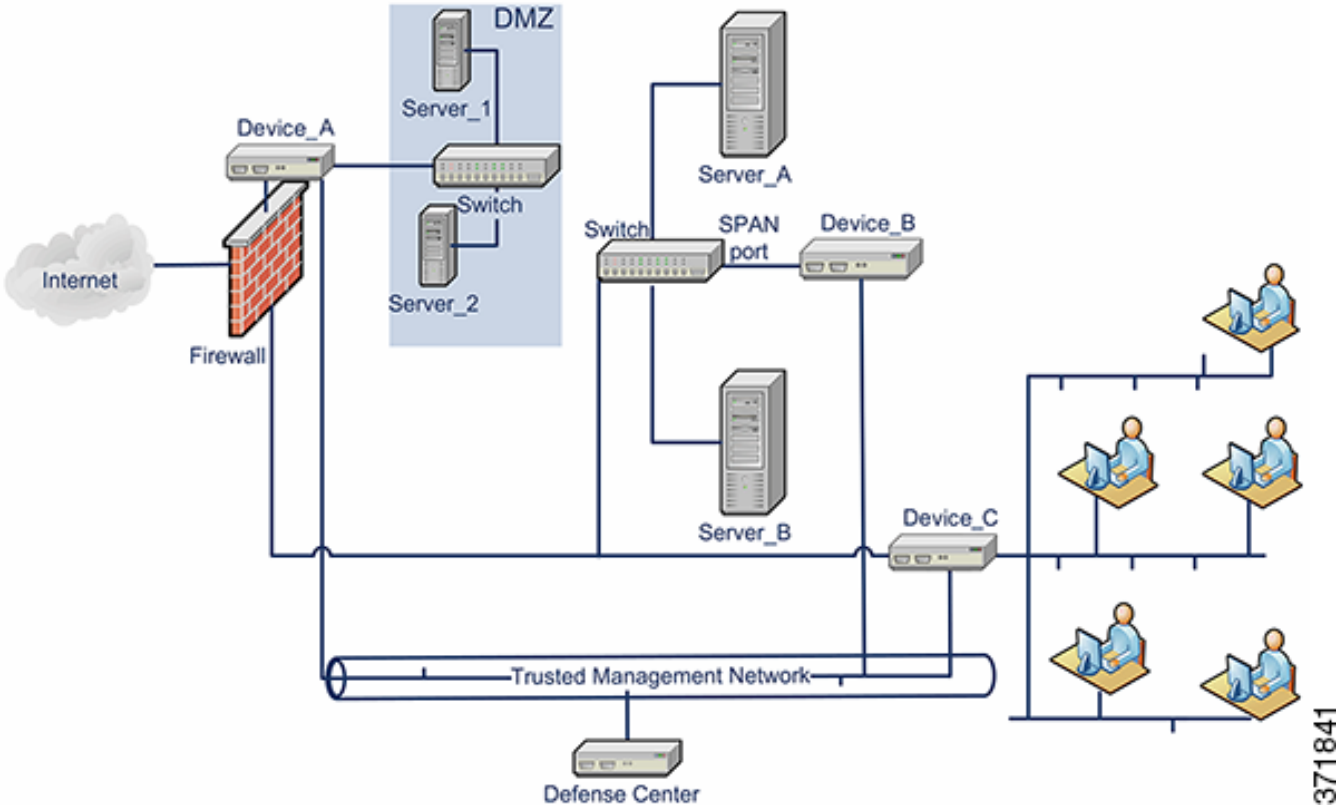
仮想アプライアンスに 2 つ目の管理インターフェイスを追加する方法については、VMware vSphere（http://vmware.com）を参照してください。

注意 シスコは、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。

この章では、展開に関する事例を示します。

一般的な FireSIGHT システム の展開

物理アプライアンス環境で、一般的な FireSIGHT システム の展開には、物理デバイスと物理防御センターを使用します。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。

VMware 仮想アプライアンスの展開

一般的な展開例について、次の仮想アプライアンス展開シナリオを参照してください。

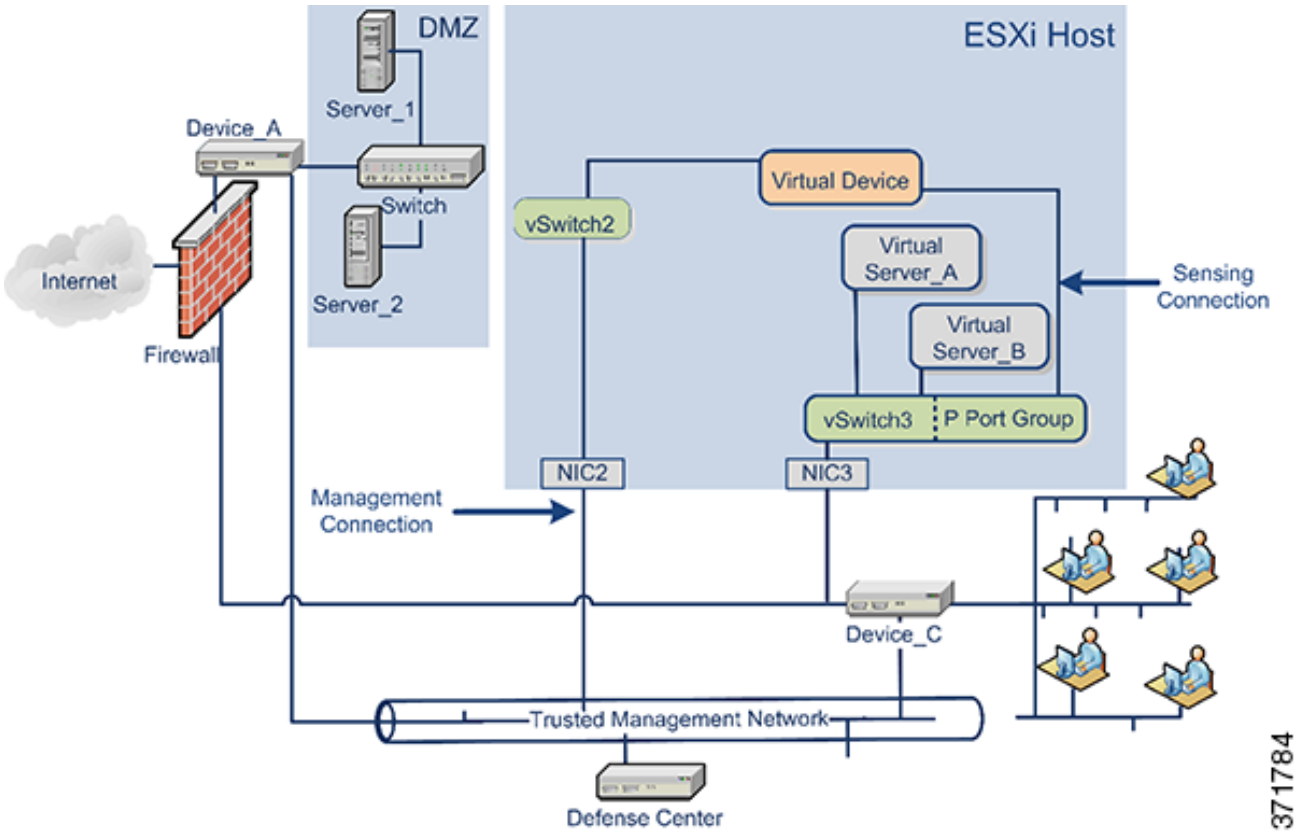
- 「仮想化と仮想デバイスの追加」(P.3-3)
- 「インライン検出のための仮想デバイスの使用」(P.3-4)
- 「仮想防御センターの追加」(P.3-5)
- 「リモート オフィス展開の使用」(P.3-6)

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 FireSIGHT システム の展開」(P.3-2)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。



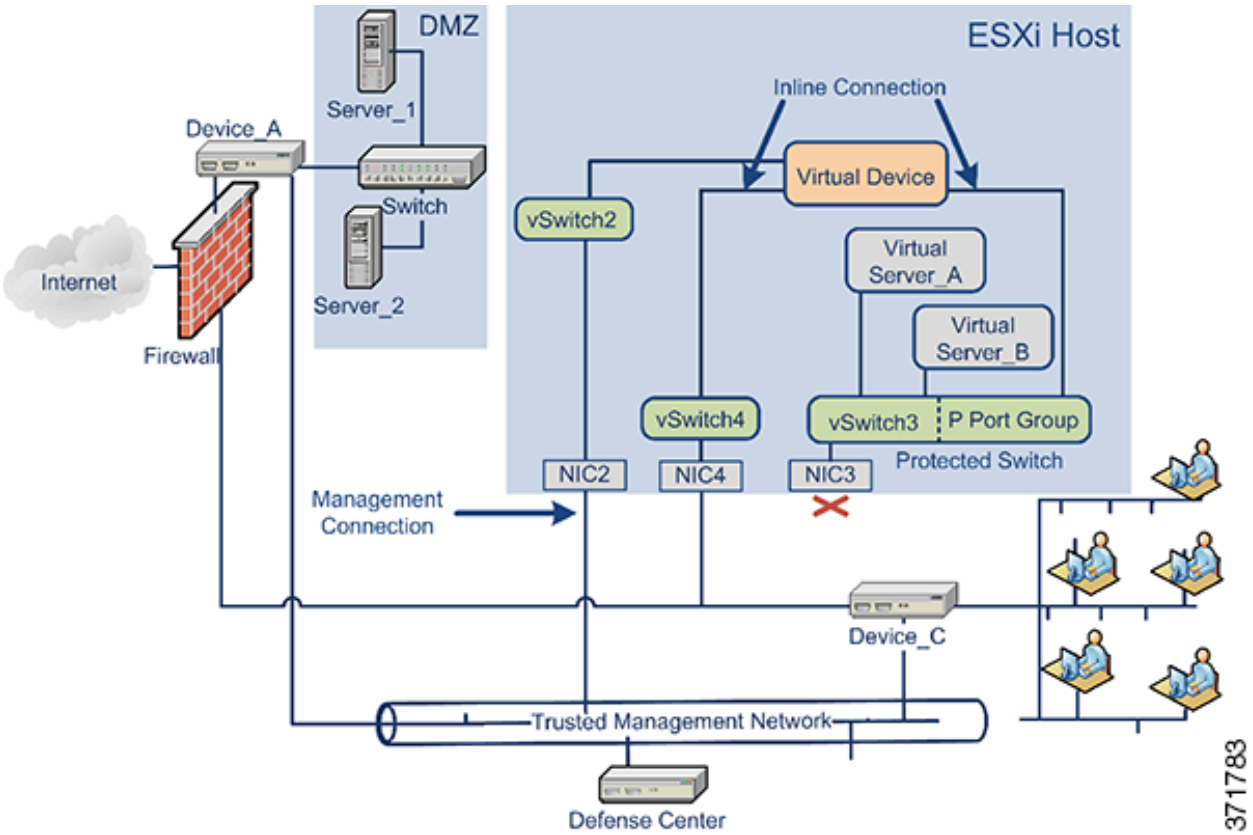
（注）　すべてのトラフィックを検知するには、デバイス センシング インターフェイスが接続する仮想スイッチまたはポート グループで無差別モード トラフィックを許可します。「仮想デバイスのセンシング インターフェイスの設定」(P.4-11)を参照してください。

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防御センターに接続します。

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 FireSIGHT システム の展開」(P.3-2) と「仮想化と仮想デバイスの追加」(P.3-3) 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、『*FireSIGHT System User 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」(P.4-11) を参照してください。

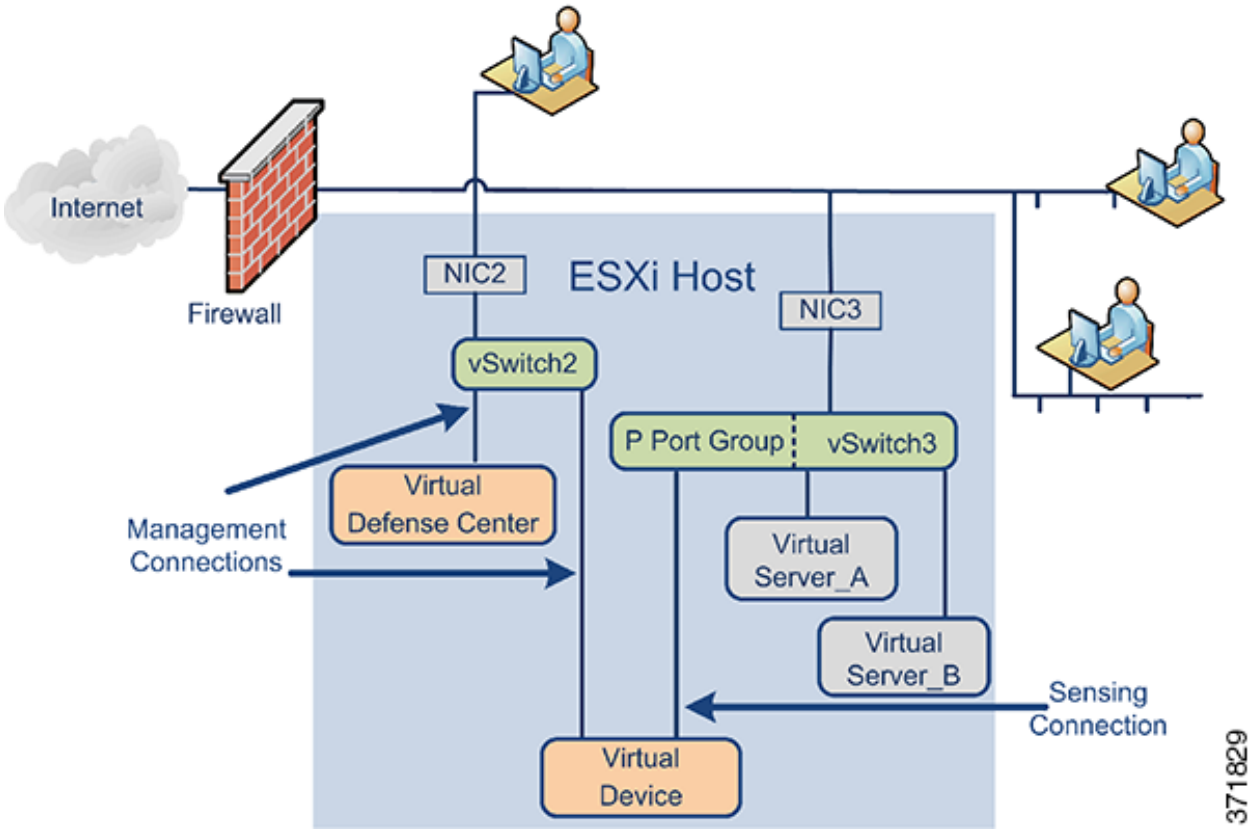
仮想デバイスは、侵入ポリシーに応じて、Server_A および Server_B への悪意のある任意のトラフィックを監視およびドロップします。

仮想防御センターの追加

次に示すように、ESXi ホストに仮想防御センターを展開し、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 FireSIGHT システム の展開」(P.3-2) と「インライン検出のための仮想デバイスの使用」(P.3-4) に示す例の上に構築します。

仮想防御センターから 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、仮想防御センター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 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、FireSIGHT 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、仮想防御センター、および仮想デバイスを展開し、仮想防御センターからその展開を管理することができます。

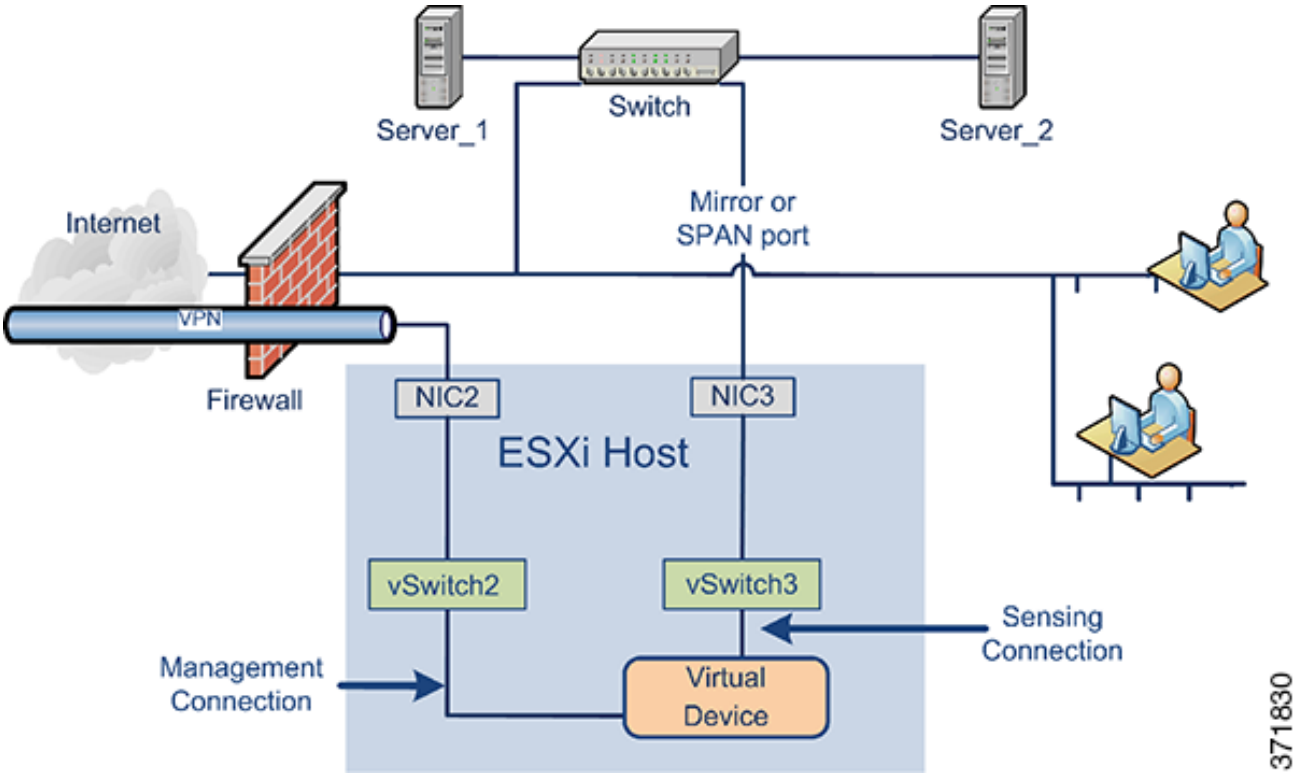


仮想デバイスの検知接続は、ネットワーク トラフィックを監視できるようにする必要があります。仮想スイッチまたは仮想インターフェイスが接続するスイッチ上のポート グループは、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワーク デバイス向けのパケットを読み取ることができます。例では、P ポート グループが無差別モード トラフィックを受け入れるように設定されています。「仮想デバイスのセンシング インターフェイスの設定」(P.4-11) を参照してください。

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。仮想防御センターによって、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、仮想防御センターにアクセスできます。仮想防御センター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「仮想防御センター ネットワーク設定の自動化」(P.5-7) と「CLI を使用した仮想デバイスの設定」(P.5-3) 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。「仮想デバイスのセンシング インターフェイスの設定」(P.4-11) を参照してください。

仮想デバイスは防御センター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、リモート防御センターを使用して、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。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 を使用した仮想デバイスの設定」(P.5-3) を参照してください。

仮想アプライアンスのインストール

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。

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、FireSIGHT 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。
- 管理プラットフォーム（VMware vCloud Director または VMware vCenter のいずれか）に展開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）に展開するか、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。

（注） シスコ 仮想アプライアンスの VMware スナップショットはサポートされて**いません**。

この章の手順を使用して、シスコ 仮想アプライアンスのダウンロード、インストール、および設定を行います。仮想ホスト環境の作成については、VMware ESXi のマニュアルを参照してください。

次の手順に従って仮想アプライアンスをインストールして構成したら、電源を入れて初期設定し、次の章で説明するように、初期設定プロセスを開始します。仮想アプライアンスのアンインストールの詳細については、「仮想アプライアンスのアンインストール」（P.4-12）を参照してください。

シスコ 仮想アプライアンスのインストールと展開を行うには：

ステップ 1 計画した展開が「動作環境の前提条件」（P.1-6）で説明されている前提条件を満たしていることを確認します。

ステップ 2 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、適切なストレージ メディアにコピーして、圧縮解除します。「インストール ファイルの取得」（P.4-2）を参照してください。

ステップ 3 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が、電源をオンにしないでください。「仮想アプライアンスのインストール」（P.4-4）を参照してください。

ステップ 4　ネットワーク、ハードウェア、およびメモリの設定を確認して調整します。「インストール後の重要な設定の更新」(P.4-9) を参照してください。

ステップ 5　任意で、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。詳細については、「インターフェイスの追加と構成」(P.4-10) を参照してください。

ステップ 6　仮想デバイス上のセンシング インターフェイスが ESXi ホスト仮想スイッチに正しく接続されていることを確認します。「仮想デバイスのセンシング インターフェイスの設定」(P.4-11) を参照してください。

インストール ファイルの取得

シスコ は仮想アプライアンスをインストールするために圧縮アーカイブ（.tar.gz）ファイルを提供します。1 つは防御センター用で、1 つはデバイス用です。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 5.3 または 5.4 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：

ステップ 1　サポート アカウントのユーザ名とパスワードを使用して、サポート サイト（ https://support.sourcefire.com/）にログインします。

ステップ 2　[Downloads] をクリックし、表示されるページの [3D System] タブを選択し、インストールするシステム ソフトウェアのメジャー バージョンをクリックします。

たとえば、バージョン 5.4.1 アーカイブ ファイルをダウンロードするには、[Downloads] > [3D] > [5.4.1] をクリックします。

ステップ 3　次の命名規則を使用して、仮想デバイスまたは仮想防御センターのいずれかに対してダウンロードするアーカイブ ファイルを検索します。

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx.tar.gz
Sourcefire_Defense_Center_Virtual64_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。

ページの左側にあるリンクの 1 つをクリックして、ページの該当するセクションを表示します。たとえば、[**5.4.1** Virtual Appliances] をクリックすると、FireSIGHT システムのバージョン 5.4.1 用のアーカイブ ファイルが表示されます。

ステップ 4　ダウンロードするアーカイブをクリックします。

ファイルのダウンロードが開始されます。

ヒント　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。防御センター向けに、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。

ステップ 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。

ステップ 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。

仮想デバイスの場合：

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.mf
```

仮想防御センターの場合：

```
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_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。

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。

ステップ 7　仮想アプライアンスのインストールに進み、仮想アプライアンスを展開します。

仮想アプライアンスのインストール

仮想アプライアン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 FireSIGHT 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 FireSIGHT 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」（P.1-6）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。

仮想アプライアンスをインストールするために、次のインストール オプションがあります。

- 仮想防御センターの場合：

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`
  `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf`

- 仮想デバイスの場合：

  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`
  `Sourcefire_3D_Device_Virtual64_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 4-1　　VMware OVF テンプレート

設定	操作
Import/Deploy OVF Template	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	インストールするアプライアンス（仮想防御センターまたは仮想デバイス）と展開オプション（VI または ESXi）を確認します。
Name and Location	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	仮想デバイス用のみ。デバイスを展開するホストまたはクラスタを選択します。
Disk Format	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	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。

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、仮想防御センターの基本設定、および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
- 仮想デバイスについてのみ、最初の検出モード
- 仮想デバイスについてのみ、管理元の防御センター

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、「仮想アプライアンスの設定」(P.5-1) 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。

- 「VMware vCloud Director Web ポータルを使用したインストール」(P.4-5) では、仮想アプライアンスを VMware vCloud Director に展開する方法について説明します。
- 「vSphere クライアント を使用したインストール」(P.4-7) では、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。

ネットワーク設定と検出モードの詳細については、「CLI を使用した仮想デバイスの設定」(P.5-3) と「仮想防御センターの設定」(P.5-7) を参照してください。

VMware vCloud Director Web ポータルを使用したインストール

次の手順により、VMware vCloud Director Web ポータルを使用して仮想アプライアンスを展開できます。

- vApp テンプレートを含めるための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。
- FireSIGHT システム 仮想アプライアンス OVF パッケージを vApp テンプレートとしてカタログにアップロードします。詳細については、「仮想アプライアンス OVF パッケージのアップロード」(P.4-5) を参照してください。
- vApp テンプレートを使用して、仮想アプライアンスを作成します。詳細については、「vApp テンプレートの使用」(P.4-6) を参照してください。

仮想アプライアンス OVF パッケージのアップロード

次の 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。

仮想防御センターの場合:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-   xxx.ovf
```

仮想デバイスの場合:

```
Sourcefire_3D_Device_Virtual64_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。

仮想アプライアンス OVF パッケージをアップロードするには:

ステップ 1　VMware vCloud Director Web ポータルで、[Catalogs] > [*Organization*] > [vApp Templates] を選択します。ここで、[*Organization*] は、vApp テンプレートを含める組織の名前です。

ステップ 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。

[Upload OVF package as a vApp Template] ポップアップ ウィンドウが表示されます。

ステップ 3　[OVF package] フィールドに、OVF パッケージの場所を入力するか、OVF パッケージを参照するために [Browse] をクリックします。

- 仮想防御センターの場合:

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 仮想デバイスの場合:

  `Sourcefire_3D_Device_Virtual64_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。

ステップ 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。

ステップ 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。

ステップ 6　[Upload] をクリックして、OVF パッケージを vApp テンプレートとしてカタログにアップロードします。

OVF パッケージは組織のカタログにアップロードされます。

ステップ 7　vApp テンプレートの使用に進み、vApp テンプレートから仮想アプライアンスを作成します。

vApp テンプレートの使用

vApp テンプレートを使用して仮想アプライアンスを作成し、セットアップ ウィザードを使用したインストール時に FireSIGHT システム の必須設定を構成できます。ウィザードの各ページで設定を指定してから、[Next] をクリックして続行します。ユーザの利便性のために、ウィザードの最終ページでは、手順を完了する前に、設定を確認することができます。

vApp テンプレートを使用して仮想アプライアンスを作成するには:

ステップ 1　VMware vCloud Director Web ポータルで、[My Cloud] > [vApps] を選択します。

ステップ 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。

[Add vApp from Catalog] ポップアップ ウィンドウが表示されます。

ステップ 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。

使用可能なすべての vApp テンプレートのリストが表示されます。

ステップ 4　追加する vApp テンプレートを選択し、仮想アプライアンスの説明を表示します。

- 仮想防御センターの場合:

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 仮想デバイスの場合:

  `Sourcefire_3D_Device_Virtual64_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。

エンドユーザ ライセンス契約(EULA)が表示されます。

ステップ 5　EULA を読んで同意します。

[Name this vApp] 画面が表示されます。

ステップ 6　名前およびオプションで vApp の説明を入力します。

[Configure Resources] 画面が表示されます。

ステップ 7　[Configure Resources] 画面で、仮想データセンターを選択し、コンピュータ名を入力して（またはデフォルトのコンピュータ名を使用して）、ストレージ プロファイルを選択します。

[Network Mapping] 画面が表示されます。

ステップ 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。

[Custom Properties] 画面が表示されます。

ステップ 9　オプションで、[Custom Properties] 画面で、セットアップ ウィザードの FireSIGHT 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、「仮想アプライアンスの設定」（P.5-1）の手順を使用して、後で行うことができます。

仮想アプライアンスの設定を示す [Ready to Complete] 画面が表示されます。

ステップ 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」（P.5-2）を参照してください。

ステップ 11　「インストール後の重要な設定の更新」（P.4-9）に進みます。

vSphere クライアント を使用したインストール

vSphere クライアント 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 FireSIGHT システム の必須設定を構成する必要があります。

ウィザードの各ページで設定を指定してから、[Next] をクリックして続行します。ユーザの利便性のために、ウィザードの最終ページでは、手順を完了する前に、設定を確認することができます。

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するには:

ステップ 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 テンプレートを展開します。

[Source] 画面が表示されます。この画面では、展開するテンプレートをドロップダウン リストから参照できます。

ステップ 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。

- 仮想防御センターの場合:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- 仮想デバイスの場合:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_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。

[OVF Template Details] 画面が表示されます。

ステップ 3　以下のように、適切な仮想マシンを選択したことを確認します。

- ESXi OVF テンプレートの場合:
- [Name and Location] 画面が表示されます。
- VI OVF テンプレートの場合:
- [End User License Agreement (EULA)] 画面が表示されます。
- EULA を読み、承認します。次に、[Name and Location] 画面が表示されます。

ステップ 4　テキスト フィールドに仮想アプライアンスの名前を入力し、アプライアンスを展開するインベントリの場所を選択します。

[Host/Cluster] 画面が表示されます。

ステップ 5　テンプレートを展開するホストまたはクラスタを選択します。

[Specific Host] 画面が表示されます。

ステップ 6　テンプレートを展開するクラスタ内の特定のホストを選択します。

[Storage] 画面が表示されます。

ステップ 7　仮想マシンの宛先ストレージを選択します。

[Disk Format] 画面が表示されます。

ステップ 8　次の選択肢から、仮想ディスクを保存する形式を選択します。

- シック プロビジョニング（Lazy Zeroed）
- シン プロビジョニング（Eager Zeroed）
- シン プロビジョニング

[Network Mapping] 画面が表示されます。

ステップ 9　以下のように、テンプレートを展開するネットワークを選択します。

- ESXi OVF テンプレートの場合:
- [ESXi Finish] 画面が表示されます。
- VI OVF テンプレートの場合:
- [Properties] 画面が表示されます。
- アプライアンス用に FireSIGHT システム の必須設定を入力するか、後でセットアップを完了するためにそのままクリックし、設定を確認して、[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」(P.5-2) を参照してください。

ステップ 10　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。

ステップ 11　インストール後の重要な設定の更新に進みます。

インストール後の重要な設定の更新

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する必要があります。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。

表 4-2　　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	4 GB	可。仮想デバイスに対して次の量を割り当てる**必要**があります。 • 4 GB 以上 • カテゴリとレピュテーション ベースの URL フィルタリングを追加するには 5 GB • 大規模なダイナミック フィードを使用してセキュリティ インテリジェンス フィルタリングを追加するには 6 GB • URL フィルタリングおよびセキュリティ インテリジェンスを追加するには 7 GB
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（デバイス） 250 GB（防御センター）	不可

次の手順は、仮想アプライアンスのハードウェアとメモリの設定を確認して調整する方法を説明しています。

仮想アプライアンスの設定を確認するには：

ステップ 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。

[Virtual Machine Properties] ポップアップ ウィンドウが表示され、[Hardware] タブが表示されます。

ステップ 2　「表 4-2デフォルトの仮想アプライアンス設定」(P.4-9) 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。

ステップ 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。

ステップ 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。

- [Device Status] の下で、[Connect at power on] チェック ボックスを有効にします。
- [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。
- 仮想デバイスに手動で 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、仮想防御センターの場合、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 からライセンスを再要求しなくて済みます。
- [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。

ステップ 5　[OK] をクリックします。

変更が保存されます。

ステップ 6　任意で、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。詳細については、「インターフェイスの追加と構成」(P.4-10) を参照してください。

ステップ 7　次の手順は、インストールしたアプライアンスのタイプにより異なります。

- 仮想防御センターの場合、初期化する準備が整っています。「仮想アプライアンスの設定」(P.5-1) に進みます。
- 仮想デバイスの場合、いくつかの追加の構成が必要になります。仮想デバイスのセンシング インターフェイスの設定に進みます。

インターフェイスの追加と構成

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（仮想防御センターで e1000 インターフェイス、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。

同じ仮想防御センターに 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 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、『FireSIGHT System User Guide』の「Managing Devices」を参照してください。

ヒント　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、アプライアンスの電源をオフにして、インターフェイスを削除し、新しいインターフェイスを追加してから、アプライアンスの電源をオンにします。

仮想デバイスのセンシング インターフェイスの設定

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へネットワーク接続が可能である必要があります。

ヒント　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。

無差別モードを許可するには:

ステップ 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。

ステップ 2　[Hardware] リストで、[Networking] をクリックします。

仮想スイッチの図が表示されます。

ステップ 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。

[Switch Properties] ポップアップ ウィンドウが表示されます。

ステップ 4　[Switch Properties] ポップアップ ウィンドウで、[Edit] をクリックします。

[Detailed Properties] ポップアップ ウィンドウが表示されます。

ステップ 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。

ヒント　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。

ステップ 6　変更を保存します。

デバイスが初期化できる状態になります。

ステップ 7　次の章の「仮想アプライアンスの設定」(P.5-1) に進みます。

仮想アプライアンスのアンインストール

仮想アプライアンスをアンインストールまたは削除する必要が生じることがあります。仮想アプライアンスをシャット ダウンし、削除することにより、仮想アプライアンスをアンインストールします。

ヒント　仮想デバイスを削除した後、必ず検知接続の仮想スイッチ ポート グループをデフォルトの設定である、[Promiscuous Mode]: [Reject] に戻してください。詳細については、「仮想デバイスのセンシング インターフェイスの設定」(P.4-11) を参照してください。

仮想アプライアンスのシャット ダウン

次の手順を使用して、仮想アプライアンスを適切にシャット ダウンします。

仮想アプライアンスをシャット ダウンするには:

ステップ 1　VMware コンソールで、管理者（または仮想デバイス用、CLI 設定用）権限を持つユーザとしてログインします。仮想デバイスを使用している場合は、`expert` と入力して、シェル プロンプトを表示します。

アプライアンスのプロンプトが表示されます。

ステップ 2　次のように、仮想アプライアンスをシャット ダウンします。

- 仮想防御センターで、`sudo shutdown -h now` と入力します。
- 仮想デバイスで、`system shutdown` と入力します。

仮想アプライアンスがシャット ダウンします。

仮想アプライアンスの削除

仮想アプライアンスの電源が切れたら、仮想アプライアンスを削除できます。

次の手順を使用して、VMware vCloud Director に展開された仮想アプライアンスを削除します。

VMware vCloud Director Web ポータルを使用して仮想アプライアンスを削除するには:

ステップ 1　[My Cloud] > [vApps] を選択し、削除する vApp を右クリックして、メニューから [Delete] をクリックし、確認ポップアップ ウィンドウで [Yes] をクリックします。

仮想アプライアンスがアンインストールされます。

次の手順を使用して、VMware vCenter に展開された仮想アプライアンスを削除します。

vSphere クライアント を使用して仮想アプライアンス削除するには:

ステップ 1　vSphere クライアント コンテキスト メニューのアプライアンス名をクリックし、[Inventory] メニューを使用して [Delete] をクリックし、確認ダイアログ ボックスで [Yes] をクリックします。

仮想アプライアンスがアンインストールされます。

仮想アプライアンスの設定

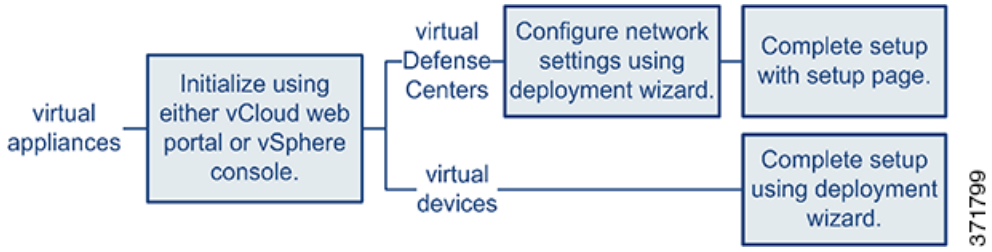
仮想アプライアンスをインストールしたら、設定プロセスを完了する必要があります。このプロセスにより、信頼された管理ネットワーク上で新しいアプライアンスが通信できるようになります。また、管理者パスワードを変更し、エンドユーザ ライセンス契約書(EULA)に同意する必要もあります。

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 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、アウトオブザボックス 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。デバイ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防御センターを使用して変更できます。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。

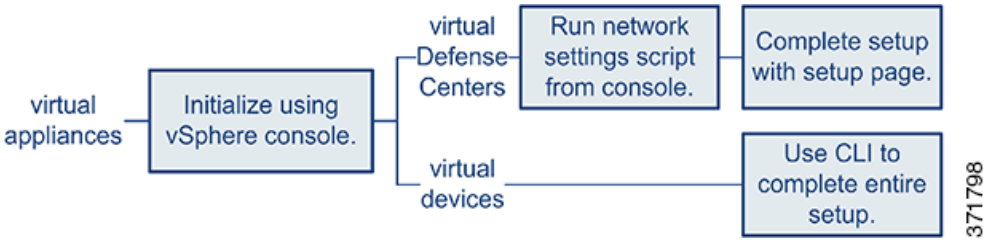
VI OVF テンプレートの展開

次の図は、VI OVF テンプレートを使用して展開する場合の、仮想防御センターおよび管理対象デバイ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、仮想防御センターおよび管理対象デバイスの設定の一般的なプロセスについて示しています。



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。

仮想デバイス

Web インターフェイスを持たない仮想デバイス。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デバイスを防御センターへ登録するなど、デバイスの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。

仮想防御センター

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、防御センターの 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。

ヒント　複数のアプライアンスを展開している場合は、先にデバイスを設定してから、管理元の防御センターを設定します。デバイスの初期設定プロセスを使用すれば、デバイスを防御センターに事前登録できます。防御センター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。

詳細については、以下を参照してください。

- 「仮想アプライアンスの初期化」（P.5-2）
- 「CLI を使用した仮想デバイスの設定」（P.5-3）
- 「仮想防御センターの設定」（P.5-7）
- 「VMware ツールの有効化」（P.5-13）
- 「次の手順」（P.5-14）

仮想アプライアンスの初期化

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

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

仮想アプライアンスを初期化するには、次の手順を使用します。

仮想アプライアンスを初期化するには：

ステップ 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。

ステップ 2　VMware コンソール タブで初期化を監視します。

プロセスの最も長い 2 つの部分でメッセージが表示されます。プロセスが完了すると、ログイン プロンプトが表示されます。

次の手順は、アプライアンスのタイプと展開によって異なります。

VI OVF テンプレートを使用し、FireSIGHT システム の必須設定を展開中に行った場合:

- 仮想防御センターについて、「仮想防御センターの設定」(P.5-7)に進んで設定を完了します。
- 仮想デバイスについては、これ以上設定することはありません。

ESXi OVF テンプレート使用している場合、または VI OVF テンプレートで展開したときに FireSIGHT システム の必須設定を行っていない場合:

- 仮想防御センターについて、「仮想防御センターの設定」(P.5-7)に進み、スクリプトを使用してネットワークを設定し、仮想防御センターを設定します。
- 仮想デバイスについては、「CLI を使用した仮想デバイスの設定」(P.5-3)に進み、CLI を使用して仮想デバイスを設定します。

CLI を使用した仮想デバイスの設定

仮想デバイスには 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 FireSIGHT システムで必要な設定を行うことができます。

ヒント　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、『*FireSIGHT System Installation Guide*』を参照してください。

ヒント　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、『*FireSIGHT System User Guide*』の「コマンド ライン リファレンス」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

FireSIGHT 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。

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 5-1　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	なし	パッシブ ゾーンに割り当てられた最初のペア
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 ゾーンは防御センターレベルの設定であり、ユーザが実際にデバイスを防御センター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、防御センター上に適切なゾーン（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、『*FireSIGHT System User Guide*』を参照してください。

CLI を使用して仮想デバイスを設定するには:

アクセス: Admin

ステップ 1　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 Cisco 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。

ステップ 2　EULA を読んで同意します。

ステップ 3　`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。

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。

ステップ 4　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。

ステップ 5　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、このデバイスを防御センターに登録するよう要求され、CLI プロンプトが表示されます。

ステップ 6　CLI を使用して、デバイスを管理元の防御センターに登録するには、次の項（「防御センターへの仮想デバイスの登録」（P.5-5））に進みます。

デバイスは防御センター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防御センターに追加できません。

防御センターへの仮想デバイスの登録

仮想デバイスには Web インターフェイスがないため、CLI を使用して仮想デバイスを防御センター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防御センター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。デバイスを防御センターへ登録するには、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、登録キーと一緒に防御センターの 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、管理している防御センターの 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防御センターへ登録する場合は、管理元の防御センターの（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、デバイスと防御センターがネットワーク 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。

仮想デバイスを防御センターに登録するには:

アクセス:CLI Configuration

ステップ 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。

ステップ 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防御センターに登録します。

```
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、防御センターの IP アドレスを表します。防御センター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、デバイスを防御センター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、防御センター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。

ステップ 3　アプライアンスからログアウトします。

ステップ 4　管理元の防御センターをすでに設定しているかどうか、および防御センターのモデルによって、次の手順が異なります。

- 防御センター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、『*FireSIGHT System User Guide*』の「デバイスの管理」の章を参照してください。
- 防御センターをまだ設定していない場合、仮想防御センターについては、「仮想防御センターの設定」（P.5-7）を参照してください。物理防御センターについては、『*FireSIGHT System Installation Guide*』を参照してください。

仮想防御センターの設定

仮想防御センター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、FireSIGHT 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、仮想防御センターにログインし、FireSIGHT 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、『*FireSIGHT System User 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 FireSIGHT システム の必須設定を行っていない場合は、仮想防御センターの設定は 2 段階のプロセスになります。仮想防御センターを初期化した後で、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防御センターを展開し、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防御センター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：仮想防御センター」（P.5-8）を参照してください。

詳細については、以下を参照してください。

- 「仮想防御センター ネットワーク設定の自動化」（P.5-7）
- 「初期設定ページ：仮想防御センター」（P.5-8）

仮想防御センター ネットワーク設定の自動化

新しい仮想防御センターを初期化した後で、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。

FireSIGHT 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。

スクリプトを使用して防御センターのネットワークを設定するには：

アクセス：Admin

ステップ 1　初期化プロセスが完了した後で、ユーザ名として `admin`、および 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 admin アカウントのパスワードを使用して、VMware コンソールで仮想防御センターにログインします。

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 Cisco を使用します。

ステップ 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
```

ステップ 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）。

ステップ 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。

ステップ 5　アプライアンスからログアウトします。

ステップ 6　防御センターの 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：仮想防御センター」（P.5-8）に進みます。

初期設定ページ：仮想防御センター

仮想防御センターについて、防御センターの Web インターフェイスにログインし、セットアップページで初期設定のオプションを指定して、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、防御センターをリモート 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。

Web インターフェイスを使用して防御センター上で初期設定を完了するには：

アクセス：Admin

ステップ 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://DC_name/` にアクセスします。ここで *`DC_name`* は、前の手順で防御センター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。

ログイン ページが表示されます。

ステップ 2　ユーザ名として `admin`、および 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 admin 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 Cisco 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」（P.5-9）
- 「ネットワーク設定」（P.5-9）
- 「時間設定」（P.5-10）
- 「ルール更新の定期インポート」（P.5-10）
- 「地理情報の定期的な更新」（P.5-10）

- 「自動バックアップ」(P.5-11)
- 「ライセンス設定」(P.5-11)
- 「デバイス登録」(P.5-11)
- 「VMware ツールの有効化」(P.5-13)
- 「End User License Agreement」(P.5-13)

ステップ 3　完了したら、[Apply] をクリックします。

防御センターが選択内容に従って設定されます。中間ページが表示されたら、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。

ステップ 4　初期設定が正常に終了したことを確認するには、[Task Status] ページ([System] > [Monitoring] > [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、[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。

防御センター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、『*FireSIGHT System User Guide*』を参照してください。

ステップ 5　「次の手順」(P.5-14) に進みます。

パスワードの変更

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。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。

ネットワーク設定

防御センター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、FireSIGHT 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 [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、[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。

時間設定

防御センターの時刻は、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て、ポップアップ ウィンドウを使用してそれを変更します。

シスコ では、物理的な NTP サーバを使用して時間を設定することを推奨しています。

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、新しく見つかった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。

侵入検知および防御を実行するよう計画している場合、シスコ は、[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 [Policy Reapply] を実行するよう設定するだけでなく、[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、[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。また、ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

地理情報の定期的な更新

仮想防御センターを使用して、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。

防御センター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、シスコ は [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、[Install Now] を選択します。

（注） GeoDB の更新は量が多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

防御センターには、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**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防御センター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

組織に対して FireSIGHT システム の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。ホスト、アプリケーション、およびユーザ ディスカバリを行うには、防御センターに FireSIGHT のライセンスが必要です。モデル固有の追加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。アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではありません。「仮想アプライアンスの機能について」(P.1-3)および「仮想アプライアンスのライセンス」(P.1-12)を参照してください。

シスコでは、初期設定ページを使用して、組織で購入したライセンスを追加することを推奨しています。この時点でライセンスを追加しない場合、初期設定で登録するすべてのデバイスは、ライセンス未登録として防御センターに追加されるため、初期設定プロセスが終了した後で、個別にライセンスを付与する必要があります。

ヒント　仮想防御センターを再作成した場合、および管理インターフェイスについて、削除したアプライアンスと同じ MAC アドレスを使用した場合は、以前のライセンスを使用できます。同じ MAC アドレスを使用できない(たとえば、動的に割り当てられた)場合、新しいライセンスについてサポートにお問い合わせください。

まだライセンスを取得していない場合は、リンクをクリックして `https://keyserver.sourcefire.com/` にナビゲートし、画面上の指示に従ってください。サポート契約に関連付けられている連絡先にメールで送信されたアクティベーション キーのほかに、(初期設定のページに示されている)ライセンス キーが必要です。

テキスト ボックスにライセンス キーをコピーし、[Submit License] をクリックしてライセンスを追加します。有効なライセンスを追加するとページが更新され、どのライセンスを追加したかを追跡することができます。ライセンスは一度に 1 つずつ追加します。

デバイス登録

仮想防御センターは、FireSIGHT 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防御センターに追加できます。ただし、デバイスと防御センターが 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。

防御センター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、[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。防御センター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 5-2　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制御ポリシー
インライン	Default Intrusion Prevention
パッシブ	Default Intrusion Prevention
アクセス コントロール	Default Access Control
ネットワーク ディスカバリ	Default Network Discovery

防御センター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、新しい防御センター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、防御センターは Default Intrusion Prevention ポリシーを適用します。そうでない場合、防御センターは 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、「CLI を使用した仮想デバイスの設定」（P.5-3）を参照してください。物理デバイスについては、『*FireSIGHT System 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。最初のアクセス制御ポリシーが失敗すると、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、アクセス制御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。アクセス制御ポリシー適用失敗の原因となる可能性のある問題についての詳細は、『*FireSIGHT System User 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。すでに防御センター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、最初に保護を有効にするまで、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により、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、防御センターはこの時点ではデバイス モデルを決定していないためです。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。詳細については、「仮想アプライアンスの機能について」（P.1-3）および「仮想アプライアンスのライセンス」（P.1-12）を参照してください。

ライセンスを有効にした後で [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、[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。

End User License Agreement

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、[Apply] をクリックします。

防御センターが選択内容に従って設定されます。中間ページが表示されたら、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。防御センターの初期設定を完了するには、「初期設定ページ：仮想防御センター」（P.5-8）の手順 3 に進みます。

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、または仮想防御センター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、次の項を参照してください。

- 「仮想デバイスでの VMware ツールの設定」（P.5-13）
- 「仮想防御センターでの VMware ツールの設定」（P.5-14）

仮想デバイスでの VMware ツールの設定

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：

アクセス：Admin

ステップ 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。

VMware ツールが実行中、有効、無効のいずれであるかを示すメッセージが、コンソールに表示されます。

仮想防御センターでの VMware ツールの設定

Web インターフェイスを使用して [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 を使用して仮想防御センターで VMware ツールを有効にすることはできません。

仮想防御センターで VMware ツールを有効または無効にするには:

アクセス: Admin

ステップ 1　Web ブラウザを使用して、防御センターにログインし、[System] > [Local] > [Configuration] > [VMware Tools] を選択します。それから、[VMware Tools] チェック ボックスをオンまたはオフにし、[Save] をクリックします。

変更が正常に実行されたことを示すメッセージが表示されます。

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、『*FireSIGHT System User 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、シスコ 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防御センターで特に重要です。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。シスコ では、防御センターを使用して、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、防御センターにはヘルス 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、防御センターを使用して、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。シスコ では、展開環境内のすべてのアプライアンスが FireSIGHT 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　FireSIGHT 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

仮想アプライアンスの展開のトラブルシューティング

この章では、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防御センター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、『*FireSIGHT System 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。

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」(P.1-7)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:

ステップ 1　[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。

[Actions] ウィンドウが表示されます。

ステップ 2　[Actions] ウィンドウで、[Properties] をクリックします。

[Virtual Machine Properties] ウィンドウが表示されます。

ステップ 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。

接続の管理

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:

ステップ 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、表示されるコンテキスト メニューの [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:

ステップ 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、表示されるコンテキスト メニューの [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。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ことを確認するには、「仮想デバイスのセンシング インターフェイスの設定」(P.4-11) 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。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:

アクセス:CLI Configuration

ステップ 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。

CLI プロンプトが表示されます。

ステップ 2　`expert` と入力してシェル プロンプトを表示します。

ステップ 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。

ステップ 4　仮想デバイスからログアウトします。

ステップ 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。

Sourcefire サポート

ご質問がある場合、または FireSIGHT 仮想デバイスや仮想防御センターに関するサポートが必要な場合は、Sourcefire サポートにお問い合わせください。

- Sourcefire サポート サイト（https://support.sourcefire.com/）にアクセスしてください。
- Sourcefire サポート（support@sourcefire.com）に電子メールをお送りください。
- Sourcefire サポート（1.410.423.1901 または 1.800.917.4134）にお電話ください。

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。