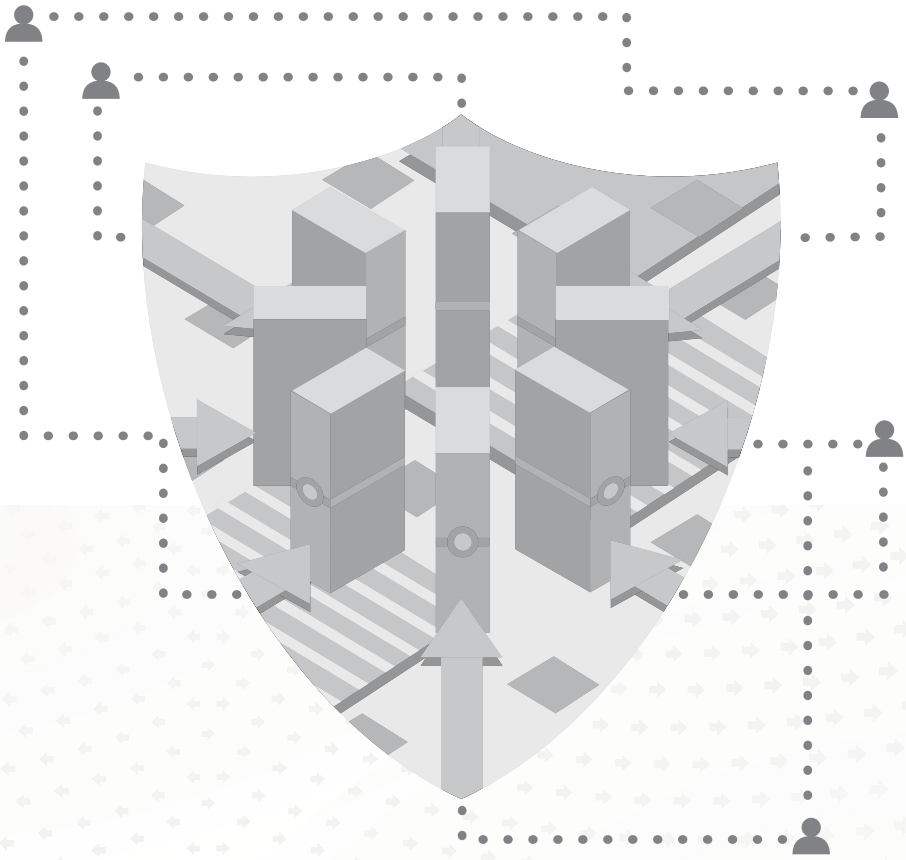
Sourcefire 3D システム
仮想インストール ガイド

バージョン 5.3



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

法律上の通知

Cisco、Cisco のロゴ、Sourcefire、Sourcefire のロゴ、Snort、Snort and Pig のロゴ、およびその他の商標とロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。

特記事項、免責事項、ご利用条件、および本書に含まれるその他の情報（「ご利用条件」）は、このドキュメント（「本書」）に記載されている情報、および読者によるその使用にのみ適用されます。これらのご利用条件は、シスコまたはシスコ支社（以下、「シスコ」）が管理する Web サイト、および Sourcefire またはシスコが提供する製品の使用には適用されず、また、それらを管理するものでもありません。Sourcefire およびシスコ製品は購入可能であり、個々のライセンス使用許諾契約またはさまざまな条件を含むご利用条件が適用されます。

本書の著作権はシスコが所有し、米国およびその他の国々の著作権およびその他の知的所有権に関する法律により保護されます。本書は非商用目的の使用の場合にのみ、使用、印刷、検索システムへの保存、その他複製や配布を行うことができます。ただし、以下の条件が満たされる場合に限ります。（i）いかなる方法においても本書を変更しないこと（ii）シスコの著作権情報、商標、その他の所有権通知、および本ページおよびその条件の全内容へのリンク、またはその印刷を必ず含めること。

本書のいかなる部分もシスコの明確な書面による事前の許可なく、編集することはできず、また、その他別の著作物や任意のドキュメント、ユーザ マニュアルに加えることも、派生的な著作物の作成に使用することもできません。シスコは条件を随時変更する権利を留保し、本書の継続的な使用はこれらの条項に同意したものと見なされます。

© 2004 - 2014 Cisco and/or its affiliates. All rights reserved.

免責事項

本書およびそこから入手できるすべての情報には正確ではないものや誤植が含まれていることがあります。シスコは随時本書を変更できます。シスコが管理するすべての Web サイト、ドキュメント、および/またはすべての製品情報の正確性や的確性について、シスコは一切の表明または保証を行いません。シスコが管理する Web サイト、ドキュメント、およびすべての製品情報は「現状のまま」提供され、シスコはすべての明示および暗黙の保証を否認します。これには権原の保証および特定目的に対する商品性および/または適合性が含まれますが、これらに限定されるものではありません。シスコはいかなる場合でも、シスコが管理する Web サイトまたは文書から発生、またはそれらに関連した任意の方法において生じた、直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、または結果的損害（代替商品または代替サービスの調達、データの損失、利益の損失、および/または事業の中断を含むが、これらに限定されない）に対して、それがどのように発生したか、あるいは契約、厳密な法的責任、過失あるいはその他の行為またはその他の任意の法的責任の理論に基づくものであるか否かにかかわらず、かつ、シスコがそうした損害の可能性を通知されていたとしても、一切責任を負いません。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が適用されない場合があります。

2015 年 3 月 23 日 17:57

Table of Contents

Chapter 1: 仮想アプライアンスの概要 4

Sourcefire 3D System 仮想アプライアンス 5
- 仮想防御センター 6
- 仮想管理対象デバイス 6

仮想アプライアンスの機能について 6
- 動作環境の前提条件 7
- 仮想アプライアンスのパフォーマンス 8

Sourcefire 仮想アプライアンスのライセンス 9

次のステップ 12

Chapter 2: Sourcefire 3D System の概要 13

Sourcefire 3D System のアプライアンス 14
- 防御センター 15
- 管理対象デバイス 16
- NO MDC THIS TIMEs 16
- アプライアンスのシリーズ、モデル、および機能について 16

Sourcefire 3D System のコンポーネント 22
- 冗長性およびリソース共有 22
- ネットワーク トラフィックの管理 23
- FireSIGHT 25
- アクセス制御 25
- 侵入検知と侵入防御 26
- ファイルの追跡、コントロール、マルウェア防御 26
- アプリケーション プログラミング インターフェース 28

目次

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 29
インターネット アクセスの要件 30
オープンな通信ポートの要件 32
ドキュメント リソース 34
ドキュメントの表記規則 35
ライセンスの表記規則 35
サポートされるデバイスと防御センターの表記規則 37
アクセスの表記規則 37
IP アドレスの表記規則 38
アプライアンスへのログイン 39
アプライアンスにログインしてアカウントを設定する 42
アプライアンスからのログアウト 44
コンテキスト メニューの使用 45

Chapter 3: 仮想アプライアンスの展開 48
一般的な Sourcefire 3D System の展開 49
VMware 仮想アプライアンスの展開 50
仮想化と仮想デバイスの追加 50
インライン検出のための仮想デバイスの使用 52
仮想防御センターの追加 53
パイロット展開の使用 53
リモート オフィス展開の使用 54

Chapter 4: 仮想アプライアンスのインストール 56
インストール ファイルの取得 57
仮想アプライアンスのインストール 60
VMware vCloud Director Web ポータルを使用したインストール 62
vSphere Client を使用したインストール 65
インストール後の重要な設定の更新 67
仮想デバイスのセンシング インターフェイスの設定 69
仮想アプライアンスのアンインストール 70
仮想アプライアンスのシャット ダウン 70
仮想アプライアンスの削除 70

Chapter 5: 仮想アプライアンスの設定 72
仮想アプライアンスの初期化 74
CLI を使用した仮想デバイスの設定 75
防御センターへの仮想デバイスの登録 79

目次

仮想防御センターの設定 81
スクリプトを使用した仮想防御センター ネットワークの設定 81
初期設定ページ：仮想防御センター 83
次の手順 92

Chapter 6: 仮想アプライアンスの展開のトラブルシューティング 94

時刻の同期 94
パフォーマンスの問題 95
接続性の問題 95
VMware vCloud Director Web Portal の使用 95
vSphere Client の使用 95
インライン インターフェイスの設定 96
サポート 97

CHAPTER 1
仮想アプライアンスの概要

Sourcefire 3D® システムは、業界トップ レベルのネットワーク侵入防御システムのセキュリティに、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を組み合わせたものです。

Sourcefire は64 ビット仮想防御センター® と VMwareESXi および VMware vCloud Director ホスティング環境用の仮想仮想デバイスをパッケージ化しています。防御センター はシステムの集中管理コンソールとデータベース リポジトリを提供します。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および X-シリーズの Sourcefire ソフトウェアを管理でき、物理防御センター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 Sourcefire アプライアンスの詳細については、『*Sourcefire 3D 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 Sourcefire 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、このガイドは、vSphere Client および VMware vCloud Director Web ポータルなど、VMware 製品の機能と専門用語について習熟している読者を対象としています。

次のトピックで Sourcefire 3D System 仮想アプライアンスについて説明します。

- 「Sourcefire 3D System 仮想アプライアンス」（P.5）
- 「仮想アプライアンスの機能について」（P.6）
- 「Sourcefire 仮想アプライアンスのライセンス」（P.9）
- 「次のステップ」（P.12）

Sourcefire 3D System 仮想アプライアンス

Sourcefire *仮想アプライアンス*は、トラフィック検知の管理対象の*仮想デバイス*または管理を実行する*仮想防御センター*のいずれかです。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」（P.6）
- 「仮想管理対象デバイス」（P.6）
- 「仮想アプライアンスの機能について」（P.6）
- 「動作環境の前提条件」（P.7）
- 「仮想アプライアンスのパフォーマンス」（P.8）

仮想防御センター

防御センターは Sourcefire 3D System 展開環境に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、ディスカバリ、接続、およびパフォーマンスのデータを集約し、相互に関連付けます。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、および図を使用したイベントとコンテキスト情報の表示
- 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
- 相関機能と修復機能を使用したリアルタイムの脅威への対応
- レポート

仮想管理対象デバイス

パッシブ展開された仮想 Sourcefire はネットワーク トラフィックに関する情報を取得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。

仮想デバイスは、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、ネットワーク、および脆弱性に関する詳細情報を収集できます。追加のライセンス機能により、さまざまなネットワーク ベースの基準のほか、アプリケーション、ユーザ、URL、IP アドレスのレピュテーション、ファイル、および侵入またはマルウェア インスペクションの結果など、他の基準に基づいて、ネットワーク トラフィックをブロックまたは許可することができます。

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。

Sourcefire 3D System の主な機能は、正しいライセンスをインストールおよび適用している場合、「Sourcefire 3D System の概要」の章の表「アプライアンスのモデル別のサポートされる機能」（P.20）で説明している機能をサポートするアプライアンスに匹敵します。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、「Sourcefire 3D System のコンポーネント」（P.22）および「Sourcefire 仮想アプライアンスのライセンス」（P.9）を参照してください。

動作環境の前提条件

次のホスティング環境で 64 ビット仮想 Sourcefire 仮想アプライアンスをホストできます。

- VMware vSphere Hypervisor 5.1
- VMware vSphere Hypervisor 5.0
- VMware vCloud Director 5.1

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。

Sourcefire 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、Sourcefire 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 に仮想マシンとしてパッケージ化されています。

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。

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）	不可

仮想アプライアンスのパフォーマンス

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

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

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。

Sourcefire では、ゲスト レイヤでのツール（VMware ツールを含む）のインストールがサポートされませんが、ESXi ホストにツール（`esxtop` または VMware/サードパーティ製のアドオンなど）をインストールして、仮想パフォーマンスを調べることができます。ただし、これらのツールはホストまたは仮想化管理レイヤのいずれかにインストールする必要があり、ゲスト レイヤにはインストールできません。

Sourcefire 仮想アプライアンスのライセンス

組織にとって最適な Sourcefire 3D System 展開を作成するためにさまざまな機能のライセンスを付与できます。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。

Sourcefire 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.72）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。防御センターでの FireSIGHT のライセンスは、防御センターとその管理対象デバイスで監視可能な個別のホストとユーザの数のほか、ユーザ制御を実行するために使用可能なユーザの数も決定します。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。

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。

制御

制御ライセンスにより、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、制御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。制御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および制御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を適用することはできません。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」（P6）を参照してください。次の表に、仮想防御センターに追加して、各デバイス モデルに適用できるライセンスを要約します。

- デバイスの行は、防御センターを含め、管理元の防御センターを使用して、そのライセンスをデバイスに適用可能かどうかを示します。
- 防御センターの行（FireSIGHT を除くすべてのライセンスが対象）は、防御センターがライセンスをデバイス（仮想デバイスを含む）に適用可能かどうかを示します。たとえば、DC500 は URL フィルタリング ライセンスを仮想デバイスに適用できません。

たとえば、仮想防御センターを使用して、シリーズ 3 デバイスを使用する VPN 展開を作成できますが、DC500を使用して、仮想デバイスを使用する、カテゴリとレピュテーション ベースの URL フィルタリングを実行することはできません。また、空のセルはライセンスがサポートされていないことを意味し、n/a は管理対象デバイスに関係のない防御センターベースのライセンスを意味します。

各モデルでサポートされるライセンス

モデル	FIRESIGHT	保護	制御	URL フィルタリング	マルウェア	VPN
シリーズ 2 デバイス： • 3D500/1000/2000 • 3D2100/2500/3500/4500 • 3D6500 • 3D9900	n/a	自動、セキュリティ インテリジェンスなし	なし	なし	なし	なし
シリーズ 3 デバイス： • 7000 シリーズ • 8000 シリーズ	n/a	あり	あり	あり	あり	あり
仮想デバイス	n/a	あり	ハードウェア機能のサポートなし	あり	あり	なし
X-シリーズの Sourcefire ソフトウェア	n/a	あり	ハードウェア機能のサポートなし	あり	あり	なし
DC500 シリーズ 2 防御センター	あり	セキュリティ インテリジェンスなし	ユーザ制御なし	なし	なし	あり
DC1000/3000 シリーズ 2 防御センター	あり	あり	あり	あり	あり	あり
DC750/1500/3500 シリーズ 3 防御センター	あり	あり	あり	あり	あり	あり
仮想防御センター	あり	あり	あり	あり	あり	あり

ライセンスの詳細については、『*Sourcefire 3D System User Guide*』のSourcefire 3D System に関する章を参照してください。

次のステップ

Sourcefire 3D System を使用した仮想アプライアンスの展開、インストール、および管理の詳細については、次の章を参照してください。

- Sourcefire 3D System については「Sourcefire 3D System の概要」（P.13）
- パッシブ展開およびインライン展開への仮想化の追加については「仮想アプライアンスの展開」（P.48）
- VMware vCloud Director Web ポータルと vSphere Client を使用したインストールについては「仮想アプライアンスのインストール」（P.56）
- 仮想デバイスおよび防御センターの初期設定とセットアップについては「仮想アプライアンスの設定」（P.72）
- 時刻同期、パフォーマンスの問題、管理接続、センシング インターフェイス、インライン インターフェイスの設定といったセットアップに共通の問題については「仮想アプライアンスの展開のトラブルシューティング」（P.93）

CHAPTER 2
SOURCEFIRE 3D SYSTEM の概要

Sourcefire 3D® システムは、業界トップ レベルのネットワーク侵入防御システムのセキュリティに、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を組み合わせたものです。ユーザは Sourcefire のアプライアンスを、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で使用することで、ネットワーク アドレス変換（NAT）を実行することができます。また、管理対象デバイスの Sourcefire の仮想ルータ間で安全な仮想プライベート ネットワーク（VPN）トンネルを構築することができます。

Sourcefire 防御センター® は、Sourcefire 3D System に集中管理コンソールとデータベース リポジトリを提供します。ネットワーク セグメントにインストールされている管理対象デバイスは、分析用のトラフィックを監視します。

パッシブな展開のデバイスは、ネットワークを流れるトラフィックを、スイッチ SPAN、仮想スイッチ、ミラー ポートなどを使用して監視します。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 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。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。

物理アプライアンスのほかに、ソフトウェア ベースの以下の Sourcefire アプライアンスを展開することができます。

- 64 ビット仮想防御センター® （VMware ESXi および VMware VMware vCloud Director ホスティング環境用）
- 同じ VMware 環境を使用した 64 ビットの仮想デバイス、および Crossbeam プラットフォーム上のホスティング X-シリーズの Sourcefire ソフトウェア

このガイドでは、Sourcefire 3D System の機能に関する情報を提供します。各章の説明、図、および手順には、ユーザ インターフェイスをナビゲートする、システム パフォーマンスを最大にする、問題をトラブルシューティングする、といったことに役に立つ詳細な情報が記載されています。

以下のトピックでは Sourcefire 3D System の概要、主なコンポーネント、Sourcefire アプライアンスに対するログインとログアウトの方法について説明します。また、システムの Web インターフェイスの使用に関する基本的な情報が含まれており、このガイドの使用法について理解するうえで有用です。

- 「Sourcefire 3D System のアプライアンス」（P.14）
- 「Sourcefire 3D System のコンポーネント」（P.22）
- 「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」（P.29）
- 「ドキュメント リソース」（P.34）
- 「ドキュメントの表記規則」（P.35）
- 「IP アドレスの表記規則」（P.38）
- 「アプライアンスへのログイン」（P.40）
- 「アプライアンスにログインしてアカウントを設定する」（P.42）
- 「アプライアンスからのログアウト」（P.44）
- 「コンテキスト メニューの使用」（P.45）

Sourcefire 3D System のアプライアンス

Sourcefire *アプライアンス*は、トラフィック検知の管理対象の *デバイス*または管理を実行する*防御センター*のいずれかです。

物理的なデバイスはフォールトトレラントで、特定の目的に特化したネットワークアプライアンスであり、ある範囲のスループットおよび機能で使用することができます。防御センターはこれらのデバイスの集中管理ポイントとして機能し、生成されたイベントを自動的に集約し、関連付けます。それぞれの物理アプライアンスのタイプには、いくつかの *モデル*があります。これらのモデルはさらに*シリーズ*と *ファミリ*に分類されます。

また、64 ビットの仮想防御センターとデバイスを、VMware ESXi および VMware vCloud Director ホスティング環境でホストすることもできます。仮想防御センターは物理デバイスを管理することが可能で、物理防御センターは仮想デバイスを管理することが可能です。また、X-シリーズの Sourcefire ソフトウェア を Crossbeam プラットフォームでホストすることができます。

Sourcefire 3D System の多くの機能は、アプライアンスによって異なります。詳細については、次の項を参照してください。

- 「防御センター」（P.15）
- 「管理対象デバイス」（P.16）
- 「アプライアンスのシリーズ、モデル、および機能について」（P.16）

防御センター

防御センターは Sourcefire 3D System 展開環境に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。（物理および仮想両方の）防御センターは侵入、ファイル、マルウェア、ディスカバリ、接続、およびパフォーマンスのデータを集約して関連付け、特定のホストにおけるイベントの影響を評価し、ホストに侵害の痕跡のタグを付けます。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。

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、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
- 脅威へリアルタイムに対応するための相関付け、侵害の痕跡、および修復の機能
- カスタムもしくはテンプレートベースのレポート作成

多くの物理防御センターでは、高可用性（冗長）機能により操作の継続性が保証されています。

管理対象デバイス

物理 Sourcefire デバイスはフォールトトレラントで、特定の目的に特化したネットワークアプライアンスであり、ある範囲のスループットで使用することができます。仮想デバイスまたは X-シリーズの Sourcefire ソフトウェア をホストすることもできます。パッシブに展開されたデバイスは、ネットワーク トラフィックについて理解するうえで有用です。インラインで展開されている場合は、Sourcefire デバイスを使用し、複数の基準に基づいてトラフィックのフローに影響を及ぼすことができます。防御センターを使用して Sourcefire デバイスを管理する必要があります。

モデルおよびライセンスによって、管理対象デバイスの機能は次のように異なります。

- 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
- 設定可能なバイパス インターフェイス、高速パス ルール、および厳密な TCP の適用の他に、スイッチング、ルーティング、DHCP、NAT、VPN の機能を備えている
- クラスタリング（冗長性）により操作の継続性を保証する、スタッキングにより複数のデバイスのリソースを組み合わせることができる

アプライアンスのシリーズ、モデル、および機能について

Sourcefire 3D System のバージョン 5.3 は、物理アプライアンスの 2 つのシリーズ、および仮想アプライアンスと X-シリーズの Sourcefire ソフトウェア で使用することができます。Sourcefire 3D System の多くの機能は、アプライアンスによって異なります。詳細については、以下を参照してください。

- 「シリーズ 2 のアプライアンス」（P.16）
- 「シリーズ 3 のアプライアンス」（P.17）
- 「仮想アプライアンス」（P.17）
- 「X-シリーズの Sourcefire ソフトウェア」（P.18）
- 「バージョン 5.3 で配布されるアプライアンス」（P.18）
- 「アプライアンスのモデル別のサポートされる機能」（P.19）

シリーズ 2 のアプライアンス

シリーズ 2 は Sourcefire の物理アプライアンスの 2 番目のシリーズです。リソースとアーキテクチャの制限により、シリーズ 2 のデバイスは、Sourcefire 3D System の一部の機能セットしかサポートしていません。

Sourcefire では新しい シリーズ 2 のアプライアンスを出荷していませんが、シリーズ 2 デバイスおよび防御センターをバージョン 5.3 に再イメージングすることができます。再イメージングを実行すると、アプライアンス上の**すべての**設定およびイベント データが失われます。詳細については、『*Sourcefire 3D System Installation Guide*』を参照してください。

警告! また、防御センター バージョン 4.10.3 または 3D Sensor の特定の設定とイベント データを、防御センター バージョン 5.2 へ移行し、その後でバージョン 5.3 にアップグレードすることができます。詳細については、『*Sourcefire 3D System Migration Guide*』でバージョン 5.2 を参照してください。

バージョン 5.3 を実行している場合、シリーズ 2 のデバイスは 保護ライセンスに関連付けられているほとんどの機能（侵入検知および防御、ファイル制御、基本的なアクセス制御など）を自動的に備えています。ただし、シリーズ 2 のデバイスはセキュリティ インテリジェンス フィルタリング、高度なアクセス制御、または高度なマルウェア対策は実行できません。また、シリーズ 2 のデバイスでライセンスを取得した他の機能を有効にすることもできません。高速パス ルール、スタッキング、およびタップ モードをサポートしている 3D9900 を除いて、シリーズ 2 のデバイスは、シリーズ 3 のデバイスに関連付けられているハードウェアベースの機能（スイッチング、ルーティング、NAT など）をサポートしていません。

バージョン 5.3、DC1000、および DC3000 シリーズ 2 防御センターは、Sourcefire 3D System のすべての機能をサポートしていますが、DC500 には、制限された機能のみ付随しています。

シリーズ 3 のアプライアンス

シリーズ 3 はSourcefire の物理アプライアンスの 3 番目のシリーズです。すべての 7000 シリーズ および8000 シリーズ のデバイスはシリーズ 3 のアプライアンスです。8000 シリーズ のデバイスはより強力で、7000 シリーズ のデバイスがサポートしていない機能をサポートしています。

仮想アプライアンス

64 ビットの仮想防御センターとデバイスを、VMware ESXi および VMware vCloud Director ホスティング環境でホストすることができます。仮想防御センターは最大 25 個の物理または仮想デバイスを管理することが可能で、物理防御センターは仮想デバイスを管理することが可能です。

インストールおよび適用されているライセンスに関係なく、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（冗長性、リソース共有、スイッチング、ルーティングなど）をサポートしません。また、仮想デバイスには Web インターフェイスがありません。

X-シリーズの Sourcefire ソフトウェア

Crossbeam プラットフォーム上でソフトウェアベースの X-シリーズの Sourcefire ソフトウェア をホストすることができます。これは仮想デバイスと類似の機能を備えています。仮想デバイスと同様に、X-シリーズの Sourcefire ソフトウェア には Web インターフェイスがありません。

インストールおよび適用されているライセンスに関係なく、X-シリーズの Sourcefire ソフトウェア はハードウェアベースの機能（冗長性、リソースの共有、スタッキング、クラスタリング、スイッチング、ルーティング、VPN、NAT など）をサポートしません。

Sourcefire 3D System を使用して冗長性を設定することはできませんが、X-シリーズの Sourcefire ソフトウェアのパッケージをインストールするときに冗長性を設定することができます。詳細については、『*Sourcefire Software for X-Series Installation Guide*』を参照してください。

バージョン 5.3 で配布されるアプライアンス

以下の表は、Sourcefire が Sourcefire 3D System のバージョン 5.3 で配布するアプライアンスについて示しています。

バージョン 5.3 の Sourcefire アプライアンス

モデル/ファミリ	シリーズ	タイプ
70xx ファミリ： • 3D7010/7020/7030	シリーズ 3（7000 シリーズ）	デバイス
71xx ファミリ： • 3D7110/7120 • 3D7115/7125 • AMP7150	シリーズ 3（7000 シリーズ）	デバイス
81xx ファミリ： • 3D8120/8130/8140 • AMP8150	シリーズ 3（8000 シリーズ）	デバイス
82xx ファミリ： • 3D8250 • 3D8260/8270/8290	シリーズ 3（8000 シリーズ）	デバイス
83xx ファミリ： • 3D8350 • 3D8360/8370/8390	シリーズ 3（8000 シリーズ）	デバイス

バージョン 5.3 の Sourcefire アプライアンス（続き）

モデル/ファミリ	シリーズ	タイプ
仮想デバイス	n/a	デバイス
X-シリーズの Sourcefire ソフトウェア	n/a	デバイス
シリーズ 3 防御センター： • DC750/1500/3500	シリーズ 3	防御センター
仮想防御センター	n/a	防御センター

Sourcefire では新しい シリーズ 2 のアプライアンスを出荷していませんが、シリーズ 2 デバイスおよび防御センターをバージョン 5.3 に再イメージングすることができます。再イメージングを実行すると、アプライアンス上の**すべての**設定およびイベント データが失われます。詳細については、『*Sourcefire 3D System Installation Guide*』を参照してください。

防御センター バージョン 4.10.3 または 3D Sensor の特定の設定とイベント データを、防御センター バージョン 5.2 へ移行し、その後でバージョン 5.3 にアップグレードすることができます。詳細については、『*Sourcefire 3D System Migration Guide*』でバージョン 5.2 を参照してください。ガイドおよび移行スクリプトの入手については、Sourcefire のサポートへお問い合わせください。

アプライアンスのモデル別のサポートされる機能

Sourcefire 3D System の多くの機能は、アプライアンスによって異なります。次の表は、正しいライセンスがインストールおよび適用されている場合の、システムの主な機能と、それらの機能をサポートするアプライアンスを対応付けたものです。

デバイスベースの機能（スタッキング、スイッチング、ルーティングなど）の防御センターの列は、防御センターがこ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ています。たとえば、シリーズ 2 DC1000 を使用して、シリーズ 3 のデバイス上で NAT を管理することができます。

アプライアンスのモデル別のサポートされる機能

機能	シリーズ 2 のデバイス	シリーズ 2 防御センター	シリーズ 3 のデバイス	シリーズ 3 防御センター	仮想デバイス	仮想防御センター	X-シリーズ
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	可	可	可	可	可	可	可
地理情報データ	可	DC1000 DC3000	可	可	可	可	可
侵入検知および防御（IPS）	可	可	可	可	可	可	可
セキュリティ インテリジェンス フィルタリング	不可	DC1000、DC3000	可	可	可	可	可
アクセス制御：基本的なネットワーク制御	可	可	可	可	可	可	可
アクセス制御：アプリケーション	不可	可	可	可	可	可	可
アクセス制御：ユーザ	不可	DC1000、DC3000	可	可	可	可	可
アクセス制御：リテラル URL	不可	可	可	可	可	可	可
アクセス制御：カテゴリおよびレピュテーションによる URL のフィルタリング	不可	DC1000、DC3000	可	可	可	可	可
ファイルの制御：ファイル タイプによる	可	可	可	可	可	可	可
ネットワークベースの高度なマルウェア防御（AMP）	不可	DC1000、DC3000	可	可	可	可	可
FireAMP の統合	n/a	可	n/a	可	n/a	可	n/a

アプライアンスのモデル別のサポートされる機能（続き）

機能	シリーズ 2 のデバイス	シリーズ 2 防御センター	シリーズ 3 のデバイス	シリーズ 3 防御センター	仮想デバイス	仮想防御センター	X-シリーズ
高速パス ルール	3D9900	可	8000 シリーズ	可	不可	可	不可
厳密な TCP の適用	不可	可	可	可	不可	可	不可
設定可能なバイパス インターフェイス	可	可	ハードウェアが制限されている場合を除く	可	不可	可	不可
タップ モード	3D9900	可	可	可	不可	可	不可
スイッチングおよびルーティング	不可	可	可	可	不可	可	不可
NAT ポリシー	不可	可	可	可	不可	可	不可
VPN	不可	可	可	可	不可	可	不可
高可用性	n/a	DC1000、DC3000	n/a	DC1500、DC3500	n/a	不可	n/a
デバイスのスタッキング	3D9900	可	3D8140、82xx ファミリ、83xx ファミリ	可	不可	可	不可
デバイスのクラスタリング	不可	可	可	可	不可	可	不可
クラスタ化されたスタック	不可	可	3D8140、82xx ファミリ、83xx ファミリ	可	不可	可	不可
マルウェア ストレージ パック	不可	DC1000、DC3000	可	可	不可	不可	不可
インタラクティブ CLI	不可	不可	可	不可	可	不可	不可

X-シリーズの Sourcefire ソフトウェア には、Crossbeam プラットフォームに固有のコマンド ライン インターフェイスがあります。ユーザはこれを使用して冗長性やロードバランシング、あるいはその両方を設定することができます。詳細については、『*Sourcefire Software for X-Series Installation Guide*』を参照してください。

Sourcefire 3D System のコンポーネント

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 Sourcefire 3D System の主な機能について説明します。

- 「冗長性およびリソース共有」（P.22）
- 「ネットワーク トラフィックの管理」（P.23）
- 「FireSIGHT」（P.25）
- 「アクセス制御」（P.25）
- 「侵入検知と侵入防御」（P.26）
- 「ファイルの追跡、コントロール、マルウェア防御」（P.26）
- 「アプリケーション プログラミング インターフェース」（P.28）

ヒント! Sourcefire 3D System の多くの機能はアプライアンス モデル、ライセンス、およびユーザ ロールによって異なります。このドキュメントには、各機能に対して Sourcefire 3D System のどのライセンスとデバイスが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、「ドキュメントの表記規則」（P.35）を参照してください。

冗長性およびリソース共有

Sourcefire 3D System の冗長性およびリソース共有の機能により、操作の継続性が保証され、複数の物理デバイスのリソースの処理を組み合わせることが可能になります。

防御センター高可用性

操作の継続性を確保するために、防御センターの*高可用性*機能を使用して、冗長な DC1000、DC1500、DC3000、または DC3500 の防御センターでデバイスを管理するよう指定することができます。イベント データは、管理対象デバイスから両方の防御センターへストリームされます。いくつかの設定要素は、両方の防御センターで保持されます。一方の防御センターで障害が発生した場合、他方の防御センターの使用を中断せずにネットワークを監視することができます。

デバイスのスタッキング

*デバイスのスタッキング*では、1 つのスタック構成内で 2 ～ 4 個の物理デバイスを接続することにより、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。スタック型の構成を確立する場合は、スタックされている各デバイスのリソースを、共有している 1 つの構成に統合します。

デバイスのクラスタリング

デバイスのクラスタリング（デバイスの高可用性とも呼ばれる）では、2 つ以上の シリーズ 3 デバイスまたはスタック間でのネットワーキング機能および設定データの冗長性を確立することができます。2 つ以上のピア デバイスまたはスタックをクラスタリングすると、ポリシーの適用、システムの更新、および登録について 1 つの論理システムが生成されます。デバイスのクラスタリングを使用して、システムは手動または自動でフェイルオーバーを実現することが可能です。

ほとんどの場合には、Sourcefire Redundancy Protocol（SFRP）を使用することによって、デバイスをクラスタリングせずにレイヤ 3 の冗長性を実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つ以上のデバイスまたはスタックが同じネットワーク接続を提供し、ネットワーク上の他のホストに対する接続性を保証するよう設定することができます。

X-シリーズの Sourcefire ソフトウェア の冗長性

Sourcefire 3D System を使用して X-シリーズの Sourcefire ソフトウェア をクラスタ化することはできませんが、X-シリーズの Sourcefire ソフトウェア パッケージをインストールするときに冗長性を設定することができます。詳細については、『*Sourcefire Software for X-Series Installation Guide*』を参照してください。

ネットワーク トラフィックの管理

Sourcefire 3D System のネットワーク トラフィック管理機能では、管理対象デバイスを組織のネットワーク インフラストラクチャの一部として機能させることができます。ユーザは、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で機能するよう シリーズ 3 のデバイスを設定し、ネットワーク アドレス変換（NAT）を実行することができます。また、安全な仮想プライベート ネットワーク（VPN）トンネルを構築することができます。

スイッチング

複数のネットワーク セグメントの間でパケットのスイッチングが可能になるように、レイヤ 2 の展開で Sourcefire 3D System を設定することができます。レイヤ 2 の展開では、スタンドアロンのブロードキャスト ドメインとして動作するよう、管理対象デバイス上でスイッチド インターフェイスおよび仮想スイッチを設定します。仮想スイッチは、ホストの MAC アドレスを使用してパケットの送信先を決定します。

ルーティング

複数のインターフェイス間でトラフィックをルーティングするように、レイヤ 3 の展開で、Sourcefire 3D System を設定することができます。レイヤ 3 の展開では、トラフィックを受信および転送するように、管理対象デバイス上でルーテッド インターフェイスと仮想ルータを設定します。システムは宛先の IP アドレスに従ってパケットの転送を判断することによって、パケットをルーティングします。ルータは転送基準に基づいて発信インターフェイスから宛先を取得し、アクセス コントロール ルールは、適用するセキュリティ ポリシーを指定します。

仮想ルータを設定するときに、スタティック ルートを定義できます。また、Routing Information Protocol（RIP）およびOpen Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定することができます。スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。ユーザは、設定するそれぞれの仮想ルータに対して DHCP リレーを設定できます。

Sourcefire アプライアンスの設定で仮想スイッチと仮想ルータの両方を使用する場合は、それらの 2 つの間でトラフィックをブリッジするように関連付けられているハイブリッド インターフェイスを設定できます。これらのユーティリティはトラフィックを分析し、そのタイプと適切な応答（ルート、スイッチ、またはそれ以外）を判断します。

NAT

レイヤ 3 の展開で、ネットワーク アドレス変換（NAT）を設定できます。内部サーバを外部ネットワークに公開することも、内部ホストまたはサーバを外部アプリケーションに接続できるようにすることも可能です。また、IP アドレスのブロックを使用するか、IP アドレスおよびポート変換の制限付きのブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すよう、NAT を設定することもできます。

VPN

バーチャル プライベート ネットワーク（VPN）は、インターネットや他のネットワークなどのパブリック ソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。シリーズ 3 デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、Sourcefire 3D System を設定することができます。

FireSIGHT

FireSIGHT™ は Sourcefire のディスカバリおよび認識テクノロジーで、ユーザがネットワークの全容を理解できるようにするために、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、地理情報、および脆弱性に関する情報を収集します。

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、アクセス制御を実行し、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。

アクセス制御

*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ネットワークに入ることができないようにブロックする
- ネットワークに入るすべてのトラフィックを詳細な検査なしで信頼する
- 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、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、侵入およびネットワーク 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。

侵入ポリシーには、次のようなさまざまなコンポーネントが含まれています。

- プロトコル ヘッダー値、ペイロードの内容、特定のパケット サイズの特性を検査するルール
- FireSIGHT の推奨事項に基づいたルール状態の設定
- プリプロセッサやその他の検出、パフォーマンス機能などの詳細設定
- プリプロセッサのルール（これにより、関連付けられているプリプロセッサおよびプリプロセッサのオプションについてイベントを生成できる）

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、Sourcefire 3D System 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。

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*高度なマルウェア防御*（AMP）を使用して、システムはネットワーク トラフィックでいくつかのファイル タイプ（PDF、Microsoft Office の多数のドキュメント、その他のタイプなど）でマルウェアを検査することができます。マルウェアが検出されると、管理対象デバイスはこれらのファイルを手動で分析するためにハード ドライブまたはマルウェアのストレージ パックに保存することができます。デバイスがファイルを保存するかどうかに関係なく、デバイスは*動的分析*のためにファイルを Sourcefire のクラウドへ送信することが可能です。また、防御センターは以下の結果に基づいて、ファイルの性質を割り当てます。

- マルウェアのクラウド ルックアップ、または*動的分析*の結果（脅威スコア）
- ファイルの *クリーン リスト*
- ファイルの *カスタム検出リスト*

管理対象デバイスはこの情報を使用してファイルをブロックまたは許可します。

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 Sourcefire 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、個々のユーザが自身のコンピュータおよびモバイル デバイス（*エンドポイント*とも呼ばれる）に *FireAMP Connector* をインストールします。これらの軽量なエージェントは Sourcefire クラウドと通信し、これ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。

FireAMP ポータル（http://amp.sourcefire.com/）を使用して、FireAMP の展開を設定します。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。

ネットワーク ファイルのトラジェクトリ

ネットワーク ファイルのトラジェクトリ機能により、ネットワークにおけるファイルの伝送経路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 インターフェース

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）では、Sourcefire のアプライアンスからカスタム開発のクライアント アプリケーションへ、いくつかの種類のイベント データをストリームすることができます。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 アクセス機能により、JDBC SSL 接続をサポートしているサードパーティのクライアントを使用して、Sourcefire 防御センターのいくつかのデータベース テーブルに対しクエリを実行することができます。

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 Sourcefire 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 API が含まれており、ユーザはこれを使用して*修復*を作成することができます。ネットワークの条件が、関連付けられている相関ポリシーまたはコンプライアンス 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修復を起動できます。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。ユーザ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。

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ためには、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、使用可能なサービスとポートのうち必要なもののみを持つように設定されていますが、攻撃がファイアウォールの外から侵入して、ここまで到達できないことを確認する必要があります。

防御センターと管理対象デバイスが同じネットワーク上に存在している場合は、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することができます。これにより、ユーザは防御センターからデバイスを安全に制御し、管理対象デバイスのネットワーク セグメント上で生成されたイベント データを集約することができます。防御センターのフィルタリング機能を使用して、ネットワーク全体で攻撃のデータを分析して相関付け、セキュリティ ポリシーが適切に実装されているかを評価することができます。

ただし、Sourcefire 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に設定されていることに注意してください。Sourcefire 3D System の機能には、この直接接続が必要なものと、プロキシ サーバの使用をサポートするものとがあります。またシステムでは、アプライアンスの Web インターフェイスにアクセスできるようにするため、および基本的なアプライアンス内通信のために、特定のポートをオープンなままにしておく必要があります。デフォルトでは、システムが追加の機能を利用できるようにするために、他のいくつかのポートがオープンになっています。

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 アクセスの要件」（P.30）
- 「オープンな通信ポートの要件」（P.32）

インターネット アクセスの要件

デフォルトでは、Sourcefire 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に設定されています。Sourcefire 3D System の一部の機能では、この直接接続が必要です。ただし、このような機能はすべてプロキシ サーバの使用をサポートしています。『*Sourcefire 3D SystemUser Guide*』の「Configuring Network Setting」を参照してください。

ヒント! ユーザは、システム ソフトウェア、侵入ルール、GeoDB、VDB の更新をアプライアンスへ手動でアップロードすることができます。

操作の継続性を確保するために、高可用性ペアの両方の防御センターがインターネットにアクセスできる必要があります。特定の機能については、プライマリ防御センターがインターネットにアクセスし、同期プロセスでセカンダリと情報を共有します。このためプライマリで障害が発生した場合は、『*Sourcefire 3D System User Guide*』の「Monitoring and Changing High Availability Status」に記載されているように、セカンダリをプライマリにプロモートする必要があります。

次の表では、Sourcefire 3D System のインターネット アクセスの要件について説明します。

Sourcefire 3D System インターネット アクセスの要件

対象	インターネット アクセスの目的	高可用性の考慮事項	プロキシを使用するか
RSS フィードのダッシュボード ウィジェット	Sourcefire などの外部のソースから RSS フィード データをダウンロードする。	フィード データは同期されない。	はい
セキュリティ インテリジェンスのフィード	Sourcefire Intelligence Feed などの外部ソースから、セキュリティ インテリジェンスのフィード データをダウンロードする。	プライマリ防御センターはフィード データをダウンロードして、セカンダリと共有する。プライマリに障害が発生した場合はロールを切り替える必要がある。	はい
URL フィルタリング データ	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する。	プライマリ防御センターは URL フィルタリング データをダウンロードして、セカンダリと共有する。プライマリに障害が発生した場合はロールを切り替える必要がある。	はい
マルウェアのクラウド ルックアップ（マルウェア ライセンス取得済み）	クラウド ルックアップを実行して、ネットワーク トラフィックで検出されたファイルにマルウェアが含まれているかどうかを判断する。	ペアの防御センターはクラウド ルックアップを個別に実行するが、ファイル ポリシーは同期化されている。	はい
動的分析	マルウェア分析のためにクラウドへファイルを送信する。	ファイル ポリシーは同期化されているが、ペアの防御センターは、クラウドに対してマルウェア分析のために送信されたファイルを個別に問い合わせする。	はい

Sourcefire 3D System インターネット アクセスの要件（続き）

対象	インターネット アクセスの目的	高可用性の考慮事項	プロキシを使用するか
FireAMP の統合（FireAMP のサブスクリプション）	Sourcefire のクラウドからエンドポイントベースのマルウェア イベントを受信する。	クラウドの接続は同期されない。両方の防御センターでクラウド接続を設定する。	はい
システム、侵入ルール、GeoDB および VDB の更新	侵入ルール、GeoDB、VDB、またはシステムの更新をアプライアンスへ直接ダウンロードするか、またはダウンロードをスケジュールする。	ルール、GeoDB および VDB の更新は同期化されているが、システムの更新は同期化されていない。更新をダウンロードするすべてのアプライアンスは、インターネットにアクセスできる必要がある。	はい
IP アドレスのコンテキスト メニューを使用した whois 情報の取得	whois 情報を取得する。	whois 情報を要求するすべてのアプライアンスがインターネットにアクセスできる必要がある。	はい

オープンな通信ポートの要件

Sourcefire 3D System では、ユーザがアプライアンスの Web インターフェイスへアクセスできるようにするため、および基本的なアプライアンス内通信のためにポート 443（受信）および 8305（受信および送信）をオープンにしておく必要があります。

デフォルトでは、システムが追加の機能を利用できるようにするために、他のいくつかのポートがオープンになっています。次の表に、これらのポートを示します。ポート 67 と 68 では DHCP がデフォルトで無効になっていることに注意してください。

Sourcefire 3D System のオープンな通信ポートの要件

ポート	説明	プロトコル	方向	ポートをオープンにする目的
22	SSH/SSL	TCP	双方向	アプライアンスに対するセキュアなリモート接続を可能にする。
25	SMTP	TCP	発信	アプライアンスから電子メール通知とアラートを送信する。
53	DNS	TCP	発信	DNS を使用する。
67、68	DHCP	UDP	発信	DHCP を使用する。**デフォルトでは無効です。**

Sourcefire 3D System のオープンな通信ポートの要件（続き）

ポート	説明	プロトコル	方向	ポートをオープンにする目的
80	HTTP	TCP	送信または双方向	RSS Feed ダッシュボード ウィジェットがリモート Web サーバ（発信）に接続できるようにする。 受信アクセスを追加することにより、防御センターは HTTP を介して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、URL のフィルタリング情報をダウンロードできるようにする。
161、162	SNMP	UDP	双方向（161）、送信（162）	SNMP ポーリング（受信）および SNMP トラップ（送信）を有効にした場合に、アクセスを提供する。
389、636	LDAP	TCP	発信	認証のためにユーザ アクティビティを追跡する。
443	HTTPS/AMQP、クラウド ルックアップ	TCP	受信または双方向	アプライアンスにアクセスする。**必須**。 送信アクセスを追加することにより、防御センターでソフトウェアの更新、VDB および GeoDB の更新、URL のフィルタリング情報、安全なセキュリティ インテリジェンス フィード、およびエンドポイントベースの（FireAMP の）マルウェア イベントをダウンロードまたは受信できるようにする。 ポート 443 を介した接続により、防御センターはクラウド ルックアップを実行して、ネットワーク トラフィックで検出されたファイルにマルウェアが含まれているかを判断する、クラウドに対して動的な分析情報を問い合わせる、ファイルのトラジェクトリを追跡する、などの処理を実行できる。 ポート 443 を介した接続により、管理対象デバイスが動的な分析のためにクラウドへファイルを送信できるようにする。
514	syslog	UDP	発信	リモート syslog サーバへアラートを送信する。
623	SOL/LOM	UDP	双方向	シリーズ 3 のアプライアンス上で Serial Over LAN（SOL）接続を使用して Lights-Out Management（LOM）を実行できるようにする。
1500、2000	データベース アクセス	TCP	受信	外部データベースへのアクセスが有効になっている場合に防御センターにアクセスする。

Sourcefire 3D System のオープンな通信ポートの要件（続き）

ポート	説明	プロトコル	方向	ポートをオープンにする目的
1812、1813	RADIUS	UDP	送信または双方向	RADIUS を使用する。受信アクセスを追加することにより、RADIUS の認証およびアカウンティングが正しく機能することが保証される。 ポート 1812 および 1813 はデフォルトであるが、他のポートを使用するよう RADIUS を設定することができる。『*Sourcefire 3D System User Guide*』の「Configuring RADIUS Connection Setting」を参照。
3306	Sourcefire ユーザ エージェント	TCP	受信	防御センターと Sourcefire ユーザ エージェント間の通信を可能にする。
8302	eStreamer	TCP	双方向	eStreamer クライアントを使用する。
8305	デバイス管理	TCP	双方向	防御センターと管理対象デバイス間で通信する。**必須**。
8307	ホスト入力クライアント	TCP	双方向	防御センターとホスト入力クライアント間の通信を可能にする。
32137	マルウェアのクラウド ルックアップ（レガシー、オプション）	TCP	双方向	防御センターでクラウド ルックアップを実行して、ネットワーク トラフィックで検出されたファイルにマルウェアが含まれているかどうかを判断し、ファイルのトラジェクトリを追跡することができるようにする。

ドキュメント リソース

Sourcefire 3D System のドキュメント セットには、オンライン ヘルプと PDF ファイルが含まれています。ユーザは次の 2 つの方法でオンライン ヘルプを使用できます。

- 各ページで状況依存ヘルプのリンクをクリックする
- [Help] > [Online] を選択する

オンライン ヘルプには、Web インターフェイスで完了できるタスクに関する情報（ユーザ管理、システム管理、イベント分析の手順や概念的な情報など）が含まれています。

ドキュメントの CD には、以下の内容の PDF が含まれています。

- *Sourcefire 3D System User Guide*（オンライン ヘルプと同じ内容が含まれていますが、印刷が簡単な形式）
- *Sourcefire 3D System Installation Guide*（Sourcefire のアプライアンスをインストールするための情報、およびハードウェア仕様特有の情報と安全に関する情報が含まれる）
- *Sourcefire 3D システム仮想インストール ガイド*（仮想デバイスおよび仮想防御センターのインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- *Sourcefire Software for X-Series Installation Guide*（X-シリーズの Sourcefire ソフトウェア のインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- 各種の API ガイドおよび補足資料

Sourcefire のサポート サイト（https://support.sourcefire.com/）で PDF ドキュメントマニュアルの最新バージョンを入手できます。

ドキュメントの表記規則

このドキュメントには、各機能に対して Sourcefire 3D System のどのライセンスとアプライアンス モデルが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、次の項を参照してください。

- 「ライセンスの表記規則」（P.35）
- 「サポートされるデバイスと防御センターの表記規則」（P.37）
- 「アクセスの表記規則」（P.37）

ライセンスの表記規則

項の先頭に記載されているライセンス文は、この項に記載されている機能を使用するのに必要なライセンスを示しています。具体的なライセンスは次のとおりです。

FireSIGHT

FireSIGHT ライセンスは防御センターに含まれており、ホスト、アプリケーション、およびユーザ ディスカバリの実行に必要です。防御センターでの FireSIGHT ライセンスは、防御センターとその管理対象デバイスで監視可能なホストおよびユーザの数、ユーザ制御を実行ために使用可能なユーザの数を決定します。

防御センターが以前にバージョン 4.10.x を実行していた場合は、FireSIGHT ライセンスの代わりに古い RNA Host および RUA User ライセンスを使用できる可能性があります。

保護

保護ライセンスでは、管理対象デバイスで侵入の検出および防御、ファイル制御、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ことができます。

制御

制御ライセンスでは、管理対象デバイスでユーザおよびアプリケーションの制御を実行することができます。また、デバイスがスイッチングおよびルーティング（DHCP リレーを含む）や NAT を実行したり、デバイスおよびスタックをクラスタ化したりできます。制御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 ライセンスでは、管理対象デバイスが定期的に更新されるクラウドベースのカテゴリおよびレピュテーション 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、ネットワークを通貨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 ライセンスでは、管理対象デバイスが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、取得、およびブロックし、動的な分析のためにこれらのファイルを送信することができる機能です。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 ライセンスでは、Sourcefire の管理対象デバイスの仮想ルータ間で安全な VPN トンネルを構築することができます。VPN ライセンスには保護および制御ライセンスが必要です。

ライセンス付きの機能の多くは追加機能であるため、このドキュメントでは、各機能で最も必要なライセンスについてのみ記載しています。たとえば、ある機能で FireSIGHT、保護、および制御のライセンスが必要な場合、制御のみが記載されています。

ライセンス文の "または" という語は、この項に記載されている機能を使用するには特定のライセンスが必要であるが、追加のライセンスで機能を追加することができることを示しています。たとえば、あるファイル ポリシーで、一部のファイル ルール アクションには保護ライセンスが必要であり、その他のファイル ルール アクションではマルウェア ライセンスが必要であるとします。この場合、そのファイル ルールの説明のライセンス文には、"保護またはマルウェア" と示されます。

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ないことに注意してください。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。「アプライアンスのモデル別のサポートされる機能」（P.19）を参照してください。ユーザが使用できる機能に対してライセンスがどのような影響を与えるかについて、および古い RNA Host および RUA User ライセンスの使用についての詳細は、『*Sourcefire 3D System User Guide*』の「Understanding Licensing」を参照してください。

サポートされるデバイスと防御センターの表記規則

項の先頭に記載されているサポートされるデバイス文は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、スタッキングは シリーズ 3 のデバイスでのみサポートされています。項にサポートされるデバイス文が記載されていない場合は、機能がすべてのデバイスでサポートされているか、またはその項が管理対象デバイスに適用されないことを表しています。

このリリースでサポートされているプラットフォームの詳細については、「アプライアンスのシリーズ、モデル、および機能について」（P.16）を参照してください。

アクセスの表記規則

このドキュメントの各手順の先頭に記載されているアクセス文は、手順の実行に必要な事前定義のユーザ ロールを示しています。複数のロールを区切るスラッシュは、記載されているどのロールでも手順を実行できることを示しています。次の表は、アクセス文で使用される共通の用語について定義しています。

アクセスの表記規則

アクセスの用語	意味
Access Admin	ユーザは Access Control Admin ロールを持っている必要がある
Admin	ユーザは Administrator ロールを持っている必要がある
Any	ユーザはいずれのロールを持っていてもよい

アクセスの表記規則（続き）

アクセスの用語	意味
Any/Admin	ユーザはいずれのロールを持っていてもよいが、Administrator ロールのみが無制限のアクセス権を持つ（プライベートとして保存された他のユーザのデータを参照できるなど）
Any Security Analyst	ユーザは、Security Analyst または Security Analyst（読み取り専用）のロールのいずれかを持つことができる
Database	ユーザは External Database ロールを持っている必要がある
Discovery Admin	ユーザは Discovery Admin ロールを持っている必要がある
Intrusion Admin	ユーザは Intrusion Admin ロールを持っている必要がある
Maint	ユーザは Maintenance User ロールを持っている必要がある
Network Admin	ユーザは Network Admin ロールを持っている必要がある
Security Analyst	ユーザは Security Analyst ロールを持っている必要がある
Security Approver	ユーザは Security Approver ロールを持っている必要がある

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義のロールを使用して、ある手順に対するアクセス要件を示す場合は、類似の権限を持つカスタム ロールもアクセス権限を持っています。カスタム ユーザ ロールの詳細については、『*Sourcefire 3D System User Guide*』の「Managing Custom User roles」を参照してください。

IP アドレスの表記規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、Sourcefire 3D System の多数の個所におけるアドレス ブロックを定義することができます。

CIDR 表記は、ネットワーク IP アドレスとビット マスクを組み合わせて使用し、指定されたアドレス ブロック内の IP アドレスを定義します。たとえば次の表に、プライベート IPv4 アドレス空間を CIDR 表記で示します。

CIDR 表記の構文例

CIDR ブロック	CIDR ブロックの IP アドレス	サブネット マスク	ポート グループ IP アドレス
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同様に、IPv6 はネットワーク IP アドレスとプレフィックス長を組み合わせて使用し、指定されたブロック内の IP アドレスを定義します。たとえば 2001:db8::/32 は、プレフィックス長が 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレスを表します。つまり、2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を表します。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Sourcefire 3D System は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、Sourcefire 3D System では 10.0.0.0/8 が使用されます。

つまり Sourcefire は、CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、Sourcefire 3D System ではこれは必要ありません。

アプライアンスへのログイン

ライセンス: 任意

防御センターには Web ベースのインターフェイスが用意されており、これを使用して管理および分析のタスクを実行することができます。物理管理対象デバイスは Web ベースの制限されたインターフェイスを備えており、これによって、初期設定および基本的な分析と設定のタスクを実行できます。仮想管理対象デバイスおよび X-シリーズの Sourcefire ソフトウェア には Web インターフェイスがありません。ユーザは Web ブラウザを使用してアプライアンスにログインして、Web インターフェイスにアクセスすることができます。ブラウザ要件の詳細については、リリース ノートで Sourcefire 3D System のこのバージョンについて参照してください。

インストール後にアプライアンスに最初にログインするユーザは、管理ユーザ アカウント（admin）を使用してログインし、初期設定プロセスを完了する必要があります。これについては、『*Sourcefire 3D System Installation Guide*』に記載されています。『*Sourcefire 3D System User Guide*』の「Adding New User Accounts」に記載されているとおりに他のユーザ アカウントを作成した後は、自分自身と他のユーザはこれらのアカウントを使用して Web インターフェイスにログインする必要があります。

重要! Sourcefire のアプライアンスはユーザ アカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることが保証されます。

アプライアンスにログインすると、ユーザがアクセスできる機能は、対象のユーザ アカウントに付与されている権限によって制御されます。ただし、アプライアンスに対するログインおよびログアウトの手順は変わりません。ログイン時に組織で SecurID® トークンを使用している場合は、SecurID PIN にトークンが付加され、ログインするためのパスワードとして使用されます。たとえば、PIN が 1111 で SecurID トークンが 222222 の場合は、1111222222 と入力します。

警告! 誤った資格情報を複数回指定すると、シェルのアクセス アカウントがロックされることがあります。アカウントがロックされている場合でも、資格情報を再度入力するよう促されます。正しい資格情報を入力しているのにログインが拒否される場合は、ログインを繰り返さずに、システム管理者に連絡してください。

Web セッションでアプライアンスのホーム ページに初めてアクセスするユーザは、そのアプライアンスの最後のログイン セッション情報を表示することができます。最後のログインについて、次の情報を表示できます。

- ログインの年、月、日、曜日
- ログイン時のアプライアンスのローカル時間（24 時間表記）
- アプライアンスにアクセスするために最後に使用されたホストとドメイン名

デフォルトでは、ユーザがセッションからタイムアウトされないと設定されていない限り、非活動の状態が 1 時間経過した後で、自動的にセッションからユーザがログアウトされます。Administrator ロールを持つユーザは、システム ポリシーでセッションのタイムアウト間隔を変更できます。詳細については、『*Sourcefire 3D System User Guide*』の「Managing User Login Settings and Configuring User Interface Settings」を参照してください。

プロセスの中には長時間かかるものがあります。このため、Web ブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このような場合は、プロセスが完了してからスクリプトを続行するようにしてください。

Web インターフェイスを使用してアプライアンスにログインするには：

アクセス：Any

1. ブラウザで `https://`*`hostname`*`/` にアクセスします。ここで *`hostname`* はアプライアンスのホスト名を表します。

   ログイン ページが表示されます。

2. [Username] および [Password] フィールドで、ユーザ名とパスワードを入力します。ユーザ名では、大文字と小文字が区別されます。

   企業で SecurID を使用している場合、SecurID トークンが SecurID PIN の末尾に付加され、ログイン時にパスワードとして使用されます。Sourcefire 3D System にログインする前に、自身の SecurID PIN を生成しておく必要があります。

3. [Login] をクリックします。

   デフォルトの開始ページが表示されます。ユーザ アカウントに対して新しいホーム ページを選択した場合は、代わりにそのページが表示されます。詳細については、『*Sourcefire 3D System User Guide*』の「Specifying Your Home Page」を参照してください。

   ページの上部に表示されるメニューおよびメニュー オプションは、ユーザ アカウントの権限によって異なります。ただし、デフォルト ホームページのリンクには、ユーザ アカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、次の警告メッセージが表示されます。

```
You are attempting to view an unauthorized page.This
activity has been logged.
```

提供されるメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックします。

コマンド ラインを介して シリーズ 3 または仮想デバイスにログインするには :

アクセス：CLI の基本設定

1. *hostname* でアプライアンスに対する SSH 接続を開きます。ここで *hostname* はアプライアンスのホスト名を表します。

   `login as:` コマンド プロンプトが表示されます。

2. ユーザ名を入力して Enter キーを押します。

   [Password:] プロンプトが表示されます。

3. パスワードを入力して Enter キーを押します。

   ログイン バナーが表示され、その後に > プロンプトが示されます。

   コマンド ライン アクセスのレベルで許可されている任意のコマンドを使用できます。使用できる CLI コマンドの詳細については、『*Sourcefire 3D System User Guide*』の「Command Line Reference」を参照してください。

アプライアンスにログインしてアカウントを設定する

ライセンス: Any

ユーザ アカウントの中には、外部の認証サーバを介して認証されるものもあります。LDAP または RADIUS 資格情報を使用して Sourcefire 3D System にログオンすることを組織で許可している場合、外部のユーザ資格情報を使用してアプライアンスに初めてログインすると、アプライアンスではローカル ユーザ レコードを作成し、これらの資格情報を権限セットに関連付けます。ローカル ユーザ レコードの権限は、以下のようにグループまたはリストのメンバーシップ全体に付与されている場合を除いて、変更することができます。

- 外部認証されているユーザ アカウントのデフォルト ロールが特定のアクセス ロールに設定されている場合、ユーザは（システム管理者による追加の設定なしで）外部のアカウント資格情報を使用してアプライアンスにログインすることができます。
- アカウントが外部で認証されており、デフォルトではアクセス権が付与されない場合、ログインはできますが機能にはアクセスできません。ユーザ（またはシステム管理者）は、ユーザ機能へ適切なアクセス権を付与する権限を変更することができます。

シェル アクセス ユーザの場合、システムはアプライアンス上にローカル ユーザ アカウントを作成しません。シェル アクセスは、シェル アクセス フィルタ、または LDAP サーバに設定されている PAM ログイン属性、あるいは RADIUS サーバ上のシェル アクセスリストによってすべて制御されます。

シェル ユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。LDAP ユーザ名には、下線（_）、ピリオド（.）、ハイフン（-）を使用することができますが、それ以外では英数字しかサポートされていません。

ログイン時に組織で SecurID トークンを使用している場合は、SecurID PIN にトークンが付加され、ログインするためのパスワードとして使用されます。たとえば、PIN が 1111 で SecurID トークンが 222222 の場合は、1111222222 と入力します。

重要! Web インターフェイスにアクセスする権限を持っていない場合は、システム管理者に連絡してアカウントの権限を変更してもらうか、Administrator のアクセス権を持つユーザとしてログインし、対象のアカウントの権限を変更します。詳細については、『*Sourcefire 3D System User Guide*』の「Modifying User Privileges and Options」を参照してください。

外部で認証されたアカウントをアプライアンスに作成するには：

アクセス：Any

1. ブラウザで `https://`*`hostname`*`/` にアクセスします。ここで *hostname* はアプライアンスのホスト名を表します。

   ログイン ページが表示されます。

2. [Username] と [Password] のフィールドに値を入力します。

   重要! 企業で SecurID を使用している場合、SecurID トークンが SecurID PIN に付加され、ログイン時にパスワードとして使用されます。

3. [Login] をクリックします。

   表示されるページは、外部認証のデフォルト アクセス ロールによって異なります。

   - 認証オブジェクトまたはシステム ポリシーでデフォルトのアクセス ロールを選択した場合は、デフォルトの開始ページが表示されます。ユーザ アカウントに対して新しいホーム ページを選択した場合は、代わりにそのページが表示されます。詳細については、『*Sourcefire 3D System User Guide*』の「Specifying Your Home Page」を参照してください。

     ページの上部に表示される使用可能なメニューおよびメニュー オプションは、ユーザ アカウントの権限によって異なります。ただし、デフォルト ホームページのリンクには、ユーザ アカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、次の警告メッセージが表示されます。

     ```
     You are attempting to view an unauthorized page. This
     activity has been logged.
     ```

     提供されるメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックします。

   - デフォルトのアクセス ロールを選択していない場合は、[Login] ページが再表示され、次のエラー メッセージが示されます。

     ```
     Unable to authorize access. If you continue to have
     difficulty accessing this device, please contact the system
     administrator.
     ```

   認証方法として、属性の一致を使用する RADIUS サーバを使用する場合、ユーザ アカウントが作成されているため、最初のログインは拒否されます。もう一度ログインする必要があります。

アプライアンスからのログアウト

ライセンス: Any

Web インターフェイスをアクティブに使用しなくなった場合、Sourcefire では、少しの間 Web ブラウザから離れるだけであっても、ログアウトすることを推奨しています。ログアウトによって Web セッションが終了し、自分の資格情報を使用して他のユーザがアプライアンスを使用できないようになります。

デフォルトでは、ユーザがセッションからタイムアウトされないと設定されていない限り、非活動の状態が 1 時間経過した後で、自動的にセッションからユーザがログアウトされます。Administrator ロールを持つユーザは、システム ポリシーでセッションのタイムアウト間隔を変更できます。詳細については、『*Sourcefire 3D System User Guide*』の「Managing User Login Settings and Configuring User Interface Settings」を参照してください。

アプライアンスからログアウトするには：

アクセス： Any

▶ ツールバーの [Logout] をクリックします。

コンテキスト メニューの使用

ライセンス: 機能によって異なる

操作の利便性を高めるため、Web インターフェイスのいくつかのページではポップアップ コンテキスト メニューをサポートしています。これを使用して、Sourcefire 3D System の他の機能へショートカットでアクセスすることができます。メニューの内容は*ホットスポット*によって異なり、ユーザはページだけでなく特定のデータにアクセスすることもできます。

たとえば、イベント ビューの *IP アドレス ホットスポット*、侵入イベントのパケット ビュー、ダッシュボード、および Context Explorer には追加のオプションがあります。アドレスに関連付けられているホストの詳細（使用可能な whois やホスト プロファイルの情報など）を知るには、ホットスポットを右クリックして [IP address] コンテキスト メニューを使用します。（セキュリティ インテリジェンスのフィルタリングをサポートしていない）DC500 防御センターを除いては、セキュリティ インテリジェンスのグローバル ホワイトリストまたはブラックリストに個別の IP アドレスを追加することもできます。

別の例として、イベント ビューおよびダッシュボードの *SHA-256 値のホットスポット*では、ファイルの SHA-256 ハッシュ値をクリーン リストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。この機能は、DC500 防御センターではサポートされていないことに注意してください。

次の一覧では、Web インターフェイスのさまざまなページのコンテキスト メニューで使用できるオプションについて説明しています。Sourcefire コンテキスト メニューがサポートされていないページまたは場所では、ブラウザの標準のコンテキスト メニューが表示されます。

アクセス制御ポリシー エディタ

アクセス制御ポリシー エディタには、各アクセス制御ルールのホットスポットが含まれます。コンテキスト メニューを使用して、新しいルールとカテゴリの挿入、ルールのカット、コピー、および貼り付け、ルール状態の設定、およびルールの編集を行うことができます。

NAT ポリシー エディタ

NAT ポリシー エディタには、各 NAT ルールのホットスポットが含まれます。コンテキスト メニューを使用して、新しいルールの挿入、ルールのカット、コピー、および貼り付け、ルール状態の設定、およびルールの編集を行うことができます。

侵入ルール エディタ

侵入ルール エディタには、各侵入ルールのホットスポットが含まれます。コンテキスト メニューを使用して、ルールの編集、ルール状態の設定（ルールの無効化を含む）、しきい値と抑制のオプションの設定、およびルールのドキュメントの表示を行うことができます。

イベント ビューア

イベント ページ（ドリルダウン ページとテーブル ビュー）には、各イベント、IP アドレス、および特定の検出ファイルの SHA-256 ハッシュ値のホットスポットが含まれます。ほとんどのイベント タイプでは、コンテキスト メニューを使用して、Context Explorer で関連情報を表示したり、イベントの情報について新しいウィンドウでドリルダウンしたりできます。ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL などの、イベント フィールドに含まれているテキストが長すぎて、イベント ビューですべて表示できない場合、コンテキスト メニューを使用してテキスト全体を表示することができます。

取得されたファイル、ファイル イベント、およびマルウェア イベントに対して、コンテキスト メニューを使用してファイルをクリーン リストまたはカスタム検出リストに追加する、クリーン リストまたはカスタム検出リストからファイルを削除する、ファイルのコピーをダウンロードする、動的分析のためにファイルをクラウドへ送信する、などの処理を実行できます。

侵入イベントに対しても、コンテキスト メニューを使用して、侵入ルール エディタまたは侵入ポリシーで実行できるものと類似のタスクを実行できます。これには、ルール状態を設定する（ルールの無効化を含む）、しきい値と抑制のオプションを設定する、ルールのドキュメントを表示するなどのタスクがあります。

パケット ビュー

侵入イベントのパケット ビューには、IP アドレスのホットスポットが含まれます。パケット ビューでは、右クリック メニューではなく、左クリックのコンテキスト メニューを使用することに注意してください。

ダッシュボード

多くのダッシュボード ウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれます。ダッシュボード ウィジェットには、IP アドレスと SHA-256 の値のホットスポットを含めることができます。

Context Explorer

Context Explorer には、図、表、およびグラフのホットスポットが含まれます。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブル ビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールの情報を表示できます。

Context Explorer でも左クリックのコンテキスト メニューを使用することに注意してください。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。詳細については、『*Sourcefire 3D System User Guide*』の「Drilling Down on Context Explorer Data」を参照してください。

コンテキスト メニューにアクセスするには：

アクセス：Any

1. Web インターフェイスのホットスポット対応ページで、ポインタをホットスポットに合わせます。

   Context Explorer を除いて、「`Right-click for menu`」というメッセージが表示されます。

2. コンテキスト メニューを起動します。
   - Context Explorer またはパケット ビューでは、ポインティング デバイスを左クリックします。
   - ホットスポット対応の他のすべてのページでは、ポインティング デバイスを右クリックします。

   ポップアップ コンテキスト メニューが表示され、ホットスポットに適したオプションが示されます。

3. オプションの名前を左クリックして、いずれかのオプションを選択します。

   アクセス制御ポリシー エディタまたは NAT ポリシー エディタを使用している場合は、ルールが変更されます。それ以外の場合は、選択したオプションに基づいて新しいブラウザ ウィンドウが開きます。

CHAPTER 3
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。

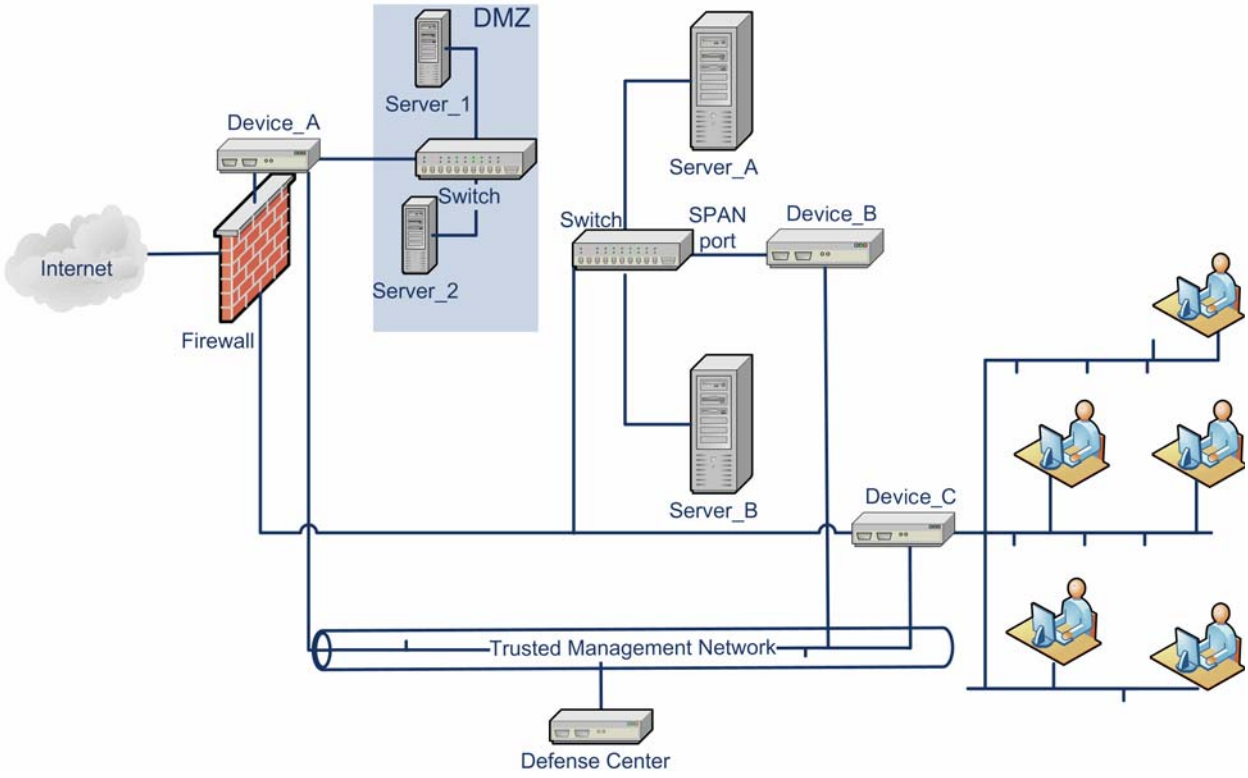
警告! Sourcefire は、実稼動ネットワーク トラフィックと信頼される管理ネットワーク トラフィックを、異なるネットワーク セグメントに保持することを**強く**推奨します。アプライアンスと管理トラフィック データ ストリームのセキュリティを保証するための対策を実施する必要があります。

この章では、展開に関する事例を示します。

- 「一般的な Sourcefire 3D System の展開」（P.49）
- 「VMware 仮想アプライアンスの展開」（P.50）

一般的な Sourcefire 3D System の展開

物理アプライアンス環境で、一般的な Sourcefire 3D System 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。

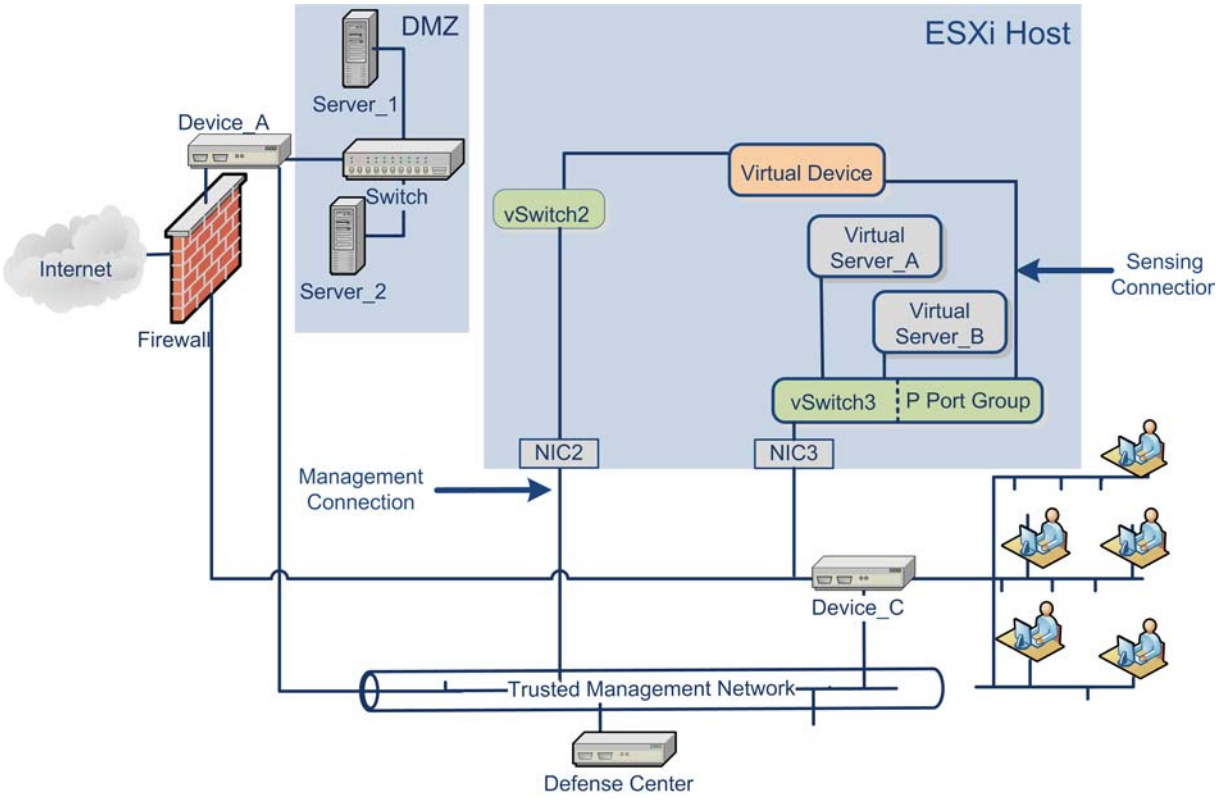
- 「仮想化と仮想デバイスの追加」（P.50）
- 「インライン検出のための仮想デバイスの使用」（P.52）
- 「仮想防御センターの追加」（P.53）
- 「パイロット展開の使用」（P.53）
- 「リモート オフィス展開の使用」（P.54）

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 Sourcefire 3D System の展開」（P.49）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。



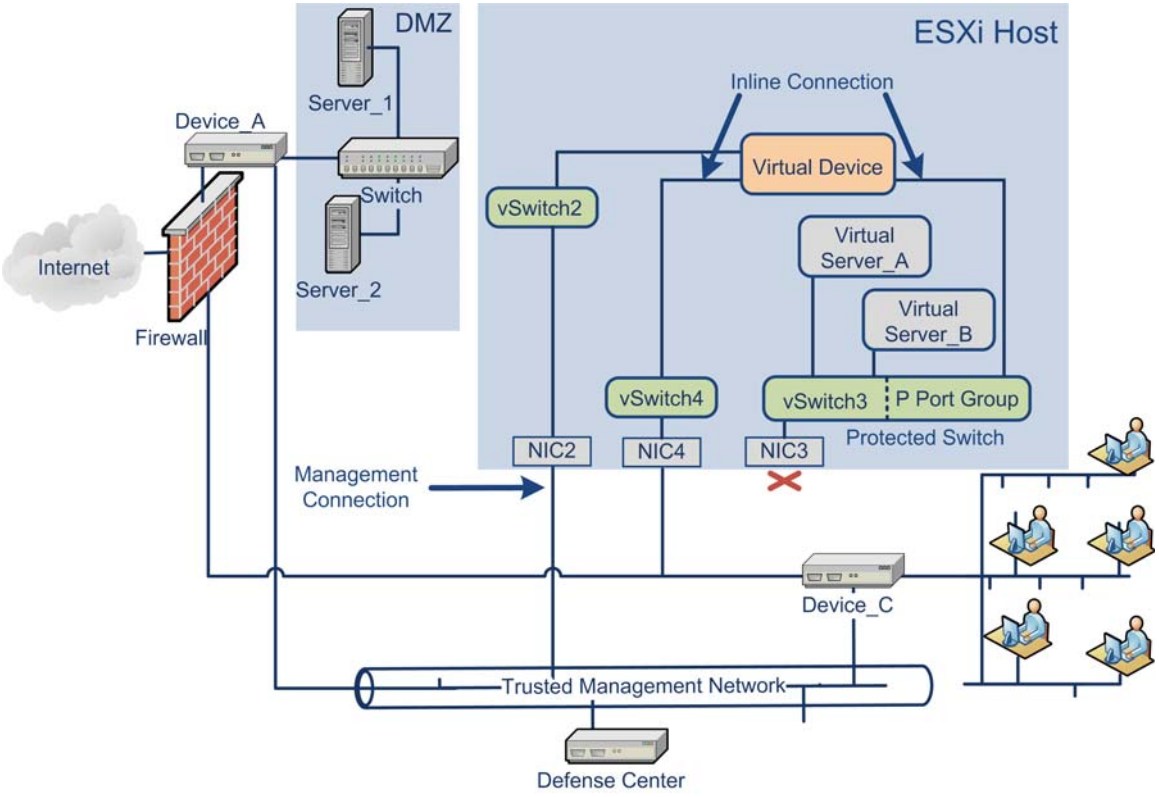
重要! すべてのトラフィックを検知するには、デバイス センシング インターフェイスが接続する仮想スイッチまたはポート グループで無差別モード トラフィックを許可します。「仮想デバイスのセンシング インターフェイスの設定」（P.69）を参照してください。

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 Sourcefire 3D System の展開」（P.49）と「仮想化と仮想デバイスの追加」（P.50）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、『*Sourcefire 3D System User Guide*』を参照してください。



重要! 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.69）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。

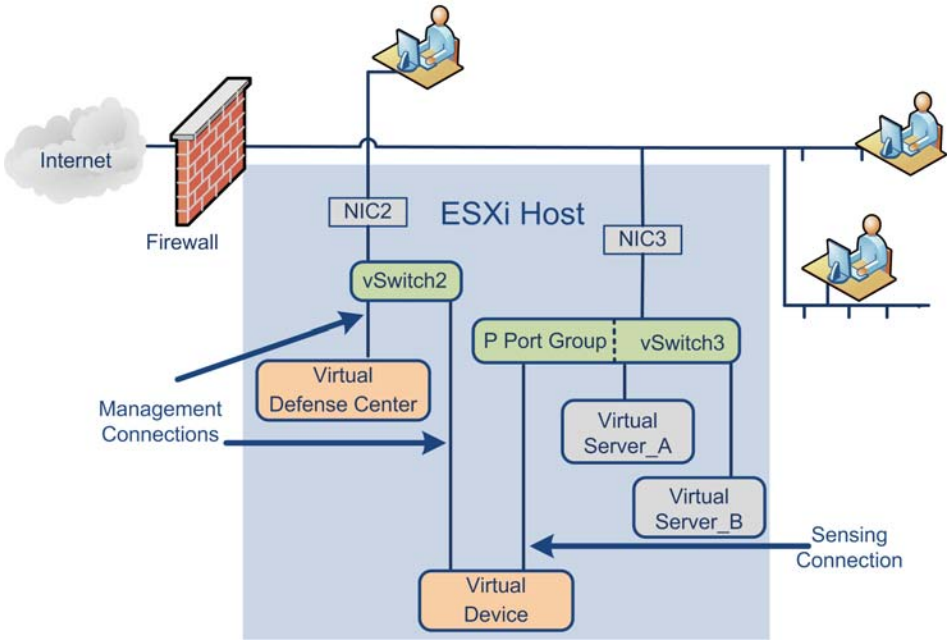
仮想防御センターの追加

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 Sourcefire 3D System の展開」（P.49）と「インライン検出のための仮想デバイスの使用」（P.52）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。

パイロット展開の使用

Sourcefire 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、Sourcefire 3D System の機能を最大限に活用できます。以下に示すように、テストまたはパイロットとして、ESXi ホストに仮想サーバ、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展開環境を管理できます。

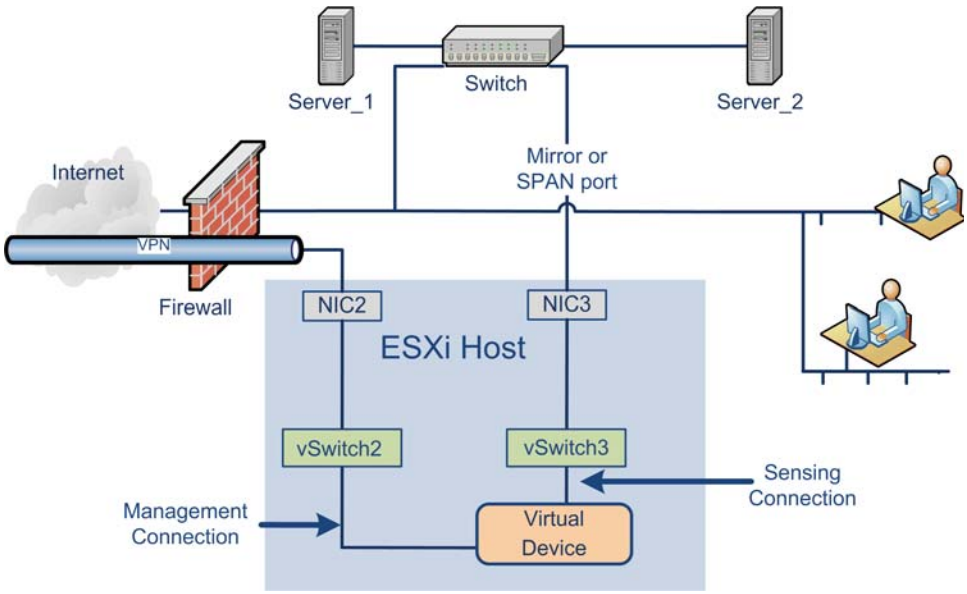


仮想デバイスの検知接続は、ネットワーク トラフィックを監視できるようにする必要があります。仮想スイッチまたは仮想インターフェイスが接続するスイッチ上のポート グループは、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワーク デバイス向けのパケットを読み取ることができます。例では、P ポート グループが無差別モード トラフィックを受け入れるように設定されています。「仮想デバイスのセンシング インターフェイスの設定」（P.69）を参照してください。

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。仮想防御センターは、仮想デバイス用のコマンドと制御を提供します。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「スクリプトを使用した仮想防御センター ネットワークの設定」（P.81）と「CLI を使用した仮想デバイスの設定」（P.75）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.69）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.75）を参照してください。

CHAPTER 4
仮想アプライアンスのインストール

Sourcefire 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。Sourcefire 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、Sourcefire 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。

重要! Sourcefire 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、Sourcefire 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.70）を参照してください。

Sourcefire 仮想アプライアンスのインストールと展開を行うには：

1. 計画した展開が「動作環境の前提条件」（P.7）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。
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.57）を参照してください。
3. VMware vCloud Director Web ポータルまたは vSphere Client を使用して、仮想アプライアンスをインストールしますが、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.60）を参照してください。
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.67）を参照してください。
5. 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.69）を参照してください。

インストール ファイルの取得

Sourcefire 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、Sourcefire サポート サイトから正しいアーカイブ ファイルを取得します。Sourcefire 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、一般にシステム ソフトウェアのメジャー バージョンに関連付けられます（たとえば 5.2 または 5.3 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. 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、Sourcefire サポート サイト（https://support.sourcefire.com/）にログインします。
2. [Downloads] をクリックして、表示されるページで [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 5.3 アーカイブ ファイルをダウンロードするには、[Downloads] > [3D System] > [5.3] をクリックします。
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です。

   ページの左側にあるリンクの 1 つをクリックして、ページの適切なセクションを表示できます。たとえば、[5.3 Virtual Appliances] をクリックして、Sourcefire 3D System のバージョン 5.3 に対するアーカイブを表示します。
4. ダウンロードするアーカイブをクリックします。

   ファイルのダウンロードが始まります。

ヒント! サポート サイトにログインしている間、Sourcefire 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。

5. vSphere Client または VMware vCloud Director Web ポータルを実行中のワークステーションまたはサーバからアクセス可能な場所に、アーカイブ ファイルをコピーします。

   警告! 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です。

   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。

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 Client）を使用して、OVF（VI または ESXi）テンプレートを管理プラットフォーム（VMware vCloud Director または VMware vCenter）に展開します。

- 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 Sourcefire 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 Sourcefire 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.7）を参照）を満たしていることを確認し、必要なアーカイブ ファイルをダウンロードしたら、VMware vCloud Director Web ポータルまたは vSphere Client を使用して仮想アプライアンスをインストールします。

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です。

次の表に、展開に必要な情報を示します。

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。

VMware OVF テンプレート（続き）

設定	操作
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。指定する構成に関するガイダンスなど、初期設定の実行の詳細については、「仮想アプライアンスの設定」（P.72）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.62）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 Client を使用したインストール」（P.65）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.75）と「仮想防御センターの設定」（P.80）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 Director User's Guide*』を参照してください。
- Sourcefire 3D System 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.62）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.63）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です。

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：

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。
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。

3. [OVF package] フィールドに OVF パッケージの場所を入力するか、または [Browse] をクリックして OVF パッケージを参照します。
   - 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です。
4. 名前およびオプションで OVF パッケージの説明を入力します。
5. ドロップダウン リストから、vApp テンプレートを含める、仮想データセンター、ストレージ プロファイル、およびカタログを選択します。
6. [Upload] をクリックして、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。
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 Sourcefire 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：

1. VMware vCloud Director Web ポータルで、[My Cloud] > [vApps] を選択します。
2. [vApps media] タブで、追加アイコン（➕）をクリックし、カタログから vApp を追加します。

   [Add vApp from Catalog] ポップアップ ウィンドウが表示されます。
3. テンプレートのメニュー バーで、[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。

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です。

   エンドユーザ ライセンス契約（EULA）が表示されます。
5. EULA を読み、承認します。

   [Name this vApp] 画面が表示されます。
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。
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。
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。
9. オプションで、[Custom Properties] 画面で、セットアップ ウィザードの Sourcefire 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.72）の手順を使用して、後で行うことができます。

   [Ready to Complete] 画面が表示され、仮想アプライアンスの設定が表示されます。
10. 設定を確認し、[Finish] をクリックします。

重要! 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.74）を参照してください。

---

11. 「インストール後の重要な設定の更新」（P.67）に進みます。

vSphere Client を使用したインストール

vSphere Client 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 Sourcefire 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 Client 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：

1. vSphere Client 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、展開するテンプレートをドロップダウン リストで参照できます。

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です。

   [OVF Template Details] 画面が表示されます。

3. 正しい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。

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。
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。
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。
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。
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。
9. 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 Sourcefire 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。

   重要! 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.74）を参照してください。
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。
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。

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：

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。

2. 表「デフォルトの仮想アプライアンス設定」（P.67）に示すように、[Memory] 、[CPUs] 、および [Hard disk 1] の設定がデフォルト値以上になっていることを確認します。

   アプライアンスのメモリ設定および仮想 CPU の数は、ウィンドウの左側に表示されます。ハード ディスクの**プロビジョニング サイズ**を表示するには、[Hard disk 1] をクリックします。

3. オプションで、ウィンドウの左側の適切な設定をクリックしてメモリと仮想 CPU の数を増やし、ウィンドウの右側で変更します。

4. [Network adapter 1] 設定が次のようになっていることを確認し、必要に応じて変更します。
   - [Device Status] の下で、[Connect at power on] チェックボックスをオンにします。
   - [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、Sourcefire 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] を仮想アプライアンスの管理ネットワーク名に設定します。

5. [OK] をクリックします。

   変更が保存されます。

6. 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。
   - 仮想防御センターは初期設定できる状態です。「仮想アプライアンスの設定」（P.72）に進みます。
   - 仮想デバイスは追加設定が必要です。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。

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：

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

   [Hardware] 選択リストと [Software] 選択リストが表示されます。

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

   仮想スイッチの図が表示されます。

3. 仮想デバイスのセンシング インターフェイスを接続するスイッチおよびポート グループの [Properties] をクリックします。

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

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

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

5. [Detailed Properties] ポップアップ ウィンドウで、[Security] タブを選択します。

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

   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。

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。

7. 次の章「仮想アプライアンスの設定」（P.72）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.69）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：

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。

   アプライアンスのプロンプトが表示されます。

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 su -` と入力し、パスワードを再入力します。root プロンプトで `shutdown -h now` と入力し、アプライアンスをシャット ダウンします。
   - 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：

▶ [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 Client を使用して仮想アプライアンス削除するには :

▶ vSphere Client 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。

CHAPTER 5
仮想アプライアンスの設定

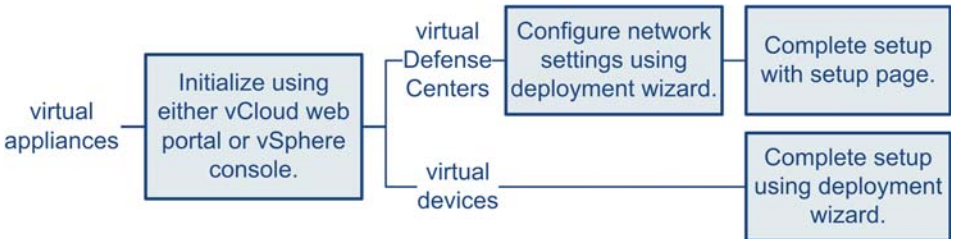
仮想アプライアンスをインストールしたら、設定プロセスを完了する必要があります。このプロセスにより、信頼された管理ネットワーク上で新しいアプライアンスが通信できるようになります。また、管理者パスワードを変更し、エンド ユーザ ライセンス契約（EULA）を承認する必要もあります。

設定プロセスにより、時間の設定、デバイスの登録とライセンシング、スケジュールの更新など、管理レベルの多数の初期タスクを実行することもできます。設定および登録時に選択したオプションにより、システムが作成および適用するデフォルトのインターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

これらの初期設定およびポリシーの目的は、すぐに使用できるエクスペリエンスを提供し、オプションを制限せずにユーザが展開を迅速に設定できるようにすることです。最初にデバイスをどのように設定するかに関係なく、防御センターを使用して設定を随時に変更することができます。つまり、設定時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、ユーザが特定のデバイス ゾーンまたはポリシー設定には固定されることはありません。

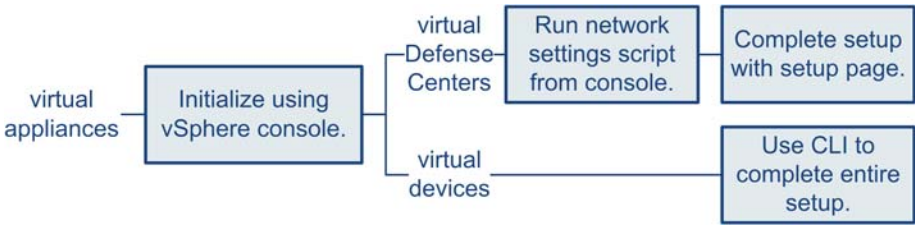
VI OVF テンプレートの展開

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する場合は、自身のデバイスを最初に設定し、次にそのデバイスを管理する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により、デバイスを事前に防御センターに登録することができ、防御センターの設定プロセスにより、事前に登録されていた管理対象デバイスを追加およびライセンス登録することができます。

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.74）
- 「CLI を使用した仮想デバイスの設定」（P.75）
- 「仮想防御センターの設定」（P.80）
- 「次の手順」（P.91）

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。

警告! 起動時間は、使用可能なサーバ リソース量など、いくつかの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：

1. アプライアンスの電源をオンにします。
   - VMware vCloud Director の Web ポータルで、ディスプレイから [vApp] を選択して [Start] をクリックします。
   - vSphere Client で、インベントリ リストからインポートした仮想アプライアンスの名前を右クリックし、コンテキスト メニューで [Power] > [Power On] を選択します。

2. VMware コンソール タブで初期化を監視します。

   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、Sourcefire 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.80）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 Sourcefire 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.80）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.75）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 テンプレートで展開しており、展開時にセットアップ ウィザードを使用しなかった場合は、CLI を使用して、Sourcefire の必須設定を行うこともできます。

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。デフォルトでは、[y] のように角括弧で囲まれています。選択を確定するには、Enter キーを押します。

CLI では、物理デバイスのセットアップ Web ページで要求される設定情報とほぼ同じ情報が要求されます。詳細については、『*Sourcefire 3D 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、『*Sourcefire 3D System User Guide*』の「Command Line Reference」の章を参照してください。

デバイス ネットワークの設定について

Sourcefire 3D System には、IPv4 と IPv6 の両方の管理環境に対するデュアル スタックの実装が用意されています。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、侵入検知システム（IDS）としてパッシブに展開されている場合は、このモードを選択します。パッシブな展開では、仮想デバイスはネットワーク ディスカバリのほかに、ネットワークベースのファイルおよびマルウェアの検出、セキュリティ インテリジェンスの監視を行うことができます。

インライン

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

重要! 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、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行うようパッシブに展開されている場合は、このモードを選択します。

次の表は、選択した検出モードごとに、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ています。

検出モードに基づいた初期設定

検出モード	セキュリティ ゾーン	インライン セット	インターフェイス
インライン	内部と外部	デフォルトのインライン セット	最初のペアはデフォルト インライン セットへ追加される（1 つは内部ゾーン、もう 1 つは外部ゾーンへ追加される）
パッシブ	パッシブ	なし	最初のペアはパッシブ ゾーンへ割り当てられる
ネットワーク ディスカバリ	パッシブ	なし	最初のペアはパッシブ ゾーンへ割り当てられる

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、システムはゾーン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、『*Sourcefire 3D 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

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 `Sourcefire` を使用します。

   デバイスでは、EULA を読むようすぐにプロンプトを表示します。

2. EULA を読んで同意します。

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。

   Sourcefire は、大文字と小文字の両方、および少なくとも 1 つの数字を含む 8 文字以上の英数字の強力なパスワードを使用することを推奨しています。辞書に記載されている単語は使用しないでください。

4. デバイスのネットワーク設定を行います。

   最初に IPv4 の管理設定を行い（または無効にして）、次に IPv6 を設定します。手動でネットワークの設定を指定する場合は、次のようにする必要があります。

   - IPv4 のアドレスを、ドット付き 10 進法形式でネットマスクを含めて入力します。たとえば、255.255.0.0 のネットマスクを指定できます。
   - IPv6 のアドレスを、コロンで区切った 16 進数の形式で入力します。IPv6 プレフィックスについては、（プレフィックスの長さ 112 のように）ビットの数を指定します。

   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。

5. デバイスをどのように展開したかに基づいて、検出モードを指定します。

   VMware コンソールには、設定が実装されるときにメッセージが表示されることがあります。完了すると、このデバイスを防御センターに登録するように要求され、CLI プロンプトが表示されます。

6. CLI を使用して、デバイスを管理する防御センターにそのデバイスを登録するには、次の項防御センターへの仮想デバイスの登録に進みます。

   防御センターを使用してデバイスを管理する必要があります。今はデバイスを登録しない場合は、デバイスを防御センターに追加する前に、後でログインしてデバイスを登録する必要があります。

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）。デバイスの CLI にすでにログインしているため、初期設定のプロセスでデバイスを防御センターへ登録するのが最も簡単な方法です。

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。

重要! vSphere Client 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。

防御センターへ仮想デバイスを登録するには：

アクセス：CLI の設定

1. CLI 設定（管理者）の権限を持つユーザとして仮想デバイスにログインします。
   - VMware コンソールから初期設定を実行している場合は、admin ユーザとしてすでにログインしています。このユーザは必要なアクセス レベルを持っています。
   - そうでない場合は、VMware コンソールを使用してデバイスにログインします。または、デバイスのネットワーク設定が完了している場合は、デバイスの管理 IP アドレスまたはホスト名に対する SSH を使用してログインします。
2. プロンプトで configure manager add コマンドを使用してデバイスを防御センターへ登録します。このコマンドの構文は次のとおりです。

   ```
   configure manager add {hostname | IPv4_address |
   IPv6_address | DONTRESOLVE} reg_key [nat_id]
   ```

   ここで、
   - {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE} は、防御センターの IP アドレスを表します。防御センターを直接アドレス指定できない場合は、DONTRESOLVE を使用してください。
   - *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* はオプションの英数字による文字列で、防御センターとデバイス間の登録プロセスで使用されます。hostname が DONTRESOLVE に設定されている場合、これが必要です。
3. アプライアンスからログアウトします。

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、『*Sourcefire 3D System User Guide*』の「Managing Devices」の章を参照してください。
   - まだ防御センターを設定していない場合は、「仮想防御センターの設定」（P.80）で、仮想防御センターに関する説明を参照するか、または『*Sourcefire 3D System Installation Guide*』で、物理防御センターに関する説明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、Sourcefire 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、Sourcefire 3D System 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、『*Sourcefire 3D 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 Sourcefire 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。

> **ヒント!** 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.82）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。

- 「スクリプトを使用した仮想防御センター ネットワークの設定」（P.81）
- 「初期設定ページ：仮想防御センター」（P.82）

スクリプトを使用した仮想防御センター ネットワークの設定

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。

Sourcefire 3D System には、IPv4 と IPv6 の両方の管理環境に対するデュアル スタックの実装が用意されています。最初に、スクリプトでは IPv4 の管理設定を行う（または無効にする）よう要求し、次に IPv6 について設定するよう要求します。IPv6 の展開については、ローカル ルータから設定を取得することができます。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。

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。デフォルトでは、[y] のように角括弧で囲まれています。選択を確定するには、Enter キーを押します。

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

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 Sourcefire を使用します。

2. admin プロンプトで sudo su - と入力してルート ユーザに切り替えて、要求された場合はもう一度パスワードを入力します。

3. root プロンプトで次のスクリプトを実行します。

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

4. スクリプトのプロンプトに従います。

   最初に IPv4 の管理設定を行い（または無効にして）、次に IPv6 を設定します。手動でネットワークの設定を指定する場合は、次のようにする必要があります。

   - IPv4 のアドレスを、ドット付き 10 進法形式でネットマスクを含めて入力します。たとえば、255.255.0.0 のネットマスクを指定できます。
   - IPv6 のアドレスを、コロンで区切った 16 進数の形式で入力します。IPv6 プレフィックスについては、（プレフィックスの長さ 112 のように）ビットの数を指定します。

5. 設定が正しいことを確認します。

   設定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。ここで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。

6. アプライアンスからログアウトします。

7. 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.82）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。管理者のパスワード変更と、ネットワーク設定の指定をまだ行っていない場合はこれらの 2 つを実行し、EULA に同意する必要があります。

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で初期設定を完了するには：

アクセス：Admin

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。

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 Sourcefire を使用します。

   設定ページが表示されます。設定方法の詳細は、以下の項を参照してください。

   - 「パスワードの変更」（P.83）
   - 「ネットワーク設定」（P.84）
   - 「時間の設定」（P.85）
   - 「ルール更新の再帰的なインポート」（P.85）
   - 「地理情報の再帰的な更新」（P.86）
   - 「自動バックアップ」（P.87）
   - 「ライセンスの設定」（P.87）
   - 「デバイス登録」（P.89）
   - 「エンド ユーザ ライセンス契約」（P.91）

3. 完了したら、[Apply] をクリックします。

   選択した内容に従って防御センターが設定されます。中間のページが表示された後で、Administrator 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。

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。

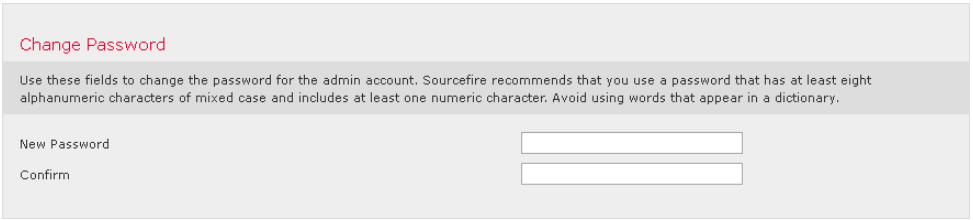
   ページは 10 秒ごとに自動的に更新されます。最初のデバイス登録およびポリシーの適用のタスクについて、[Completed] ステータスが表示されるまでページを監視します。設定の一部として、侵入ルールまたは位置情報の更新を設定した場合は、これらのタスクも監視することができます。

   これで防御センターを使用することができます。展開の設定についての詳細は、『*Sourcefire 3D System User Guide*』を参照してください。

5. 「次の手順」（P.91）に進みます。

パスワードの変更

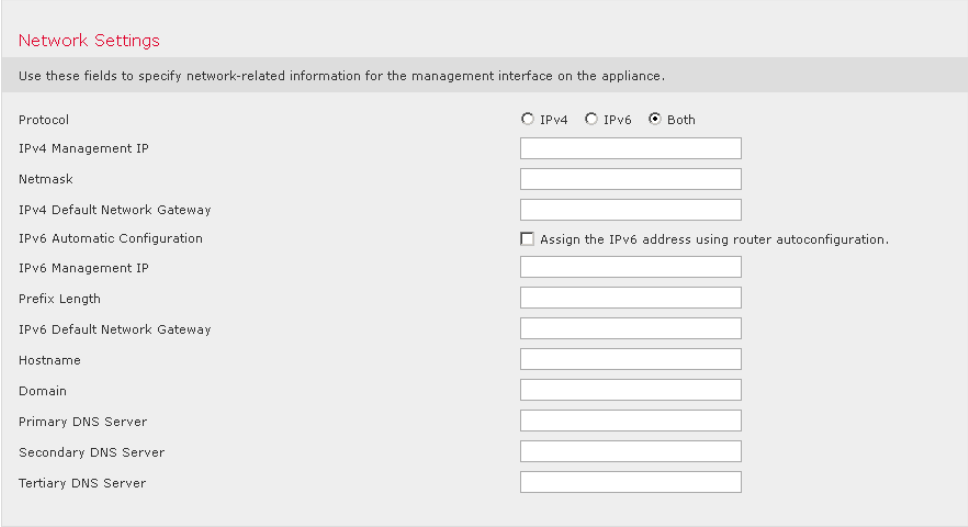
admin アカウントのパスワードを変更する必要があります。このアカウントには Administrator 権限が付与されており、削除することはできません。



Sourcefire は、大文字と小文字の両方、および少なくとも 1 つの数字を含む 8 文字以上の英数字の強力なパスワードを使用することを推奨しています。辞書に記載されている単語は使用しないでください。

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り、管理ネットワーク上で通信が可能になります。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。



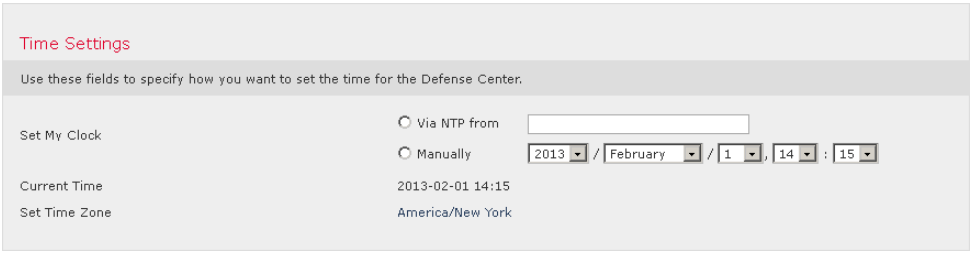
事前に指定されている設定を変更する場合は、Sourcefire 3D System には IPv4 と IPv6 の両方の管理環境についてデュアル スタックの実装が用意されていることに注意してください。管理ネットワーク プロトコル（[IPv4]、[IPv6]、または [Both] ）を指定する必要があります。選択した内容に応じて、設定のページにはさまざまなフィールドが表示されます。ここで IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィックスの長さ、およびデフォルトのゲートウェイを設定する必要があります。

- IPv4 の場合は、アドレスとネットマスクをドット付き 10 進法の形式（255.255.0.0 のネットマスクなど）で設定する必要があります。
- 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オンにしない場合は、コロンで区切った 16 進形式のアドレスと、プレフィックスのビット数を設定する必要があります（プレフィックスの長さ 112 など）。

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。

時間の設定

防御センターに対して、手動で、またはネットワーク タイム プロトコル（NTP）を介して NTP サーバから時間を設定することができます。



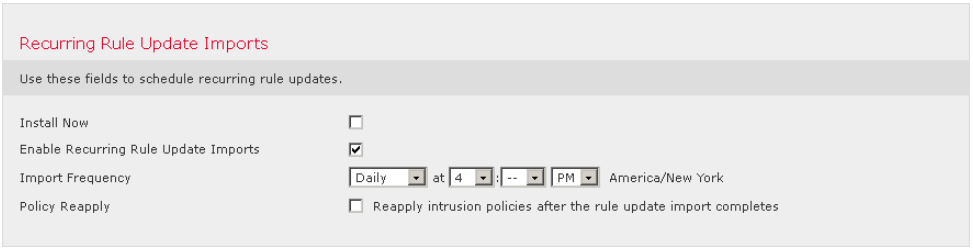
ローカル Web インターフェイスで admin アカウントに対して使用されるタイム ゾーンを指定することもできます。ポップアップ ウィンドウを使用してタイム ゾーンを変更するには、現在のタイム ゾーンをクリックします。

Sourcefire 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。

ルール更新の再帰的なインポート

新しい脆弱性が発見された場合、Sourcefire Vulnerability Research Team（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、Sourcefire は、[Enable Recurring Rule Update Imports] を選択することを推奨しています。



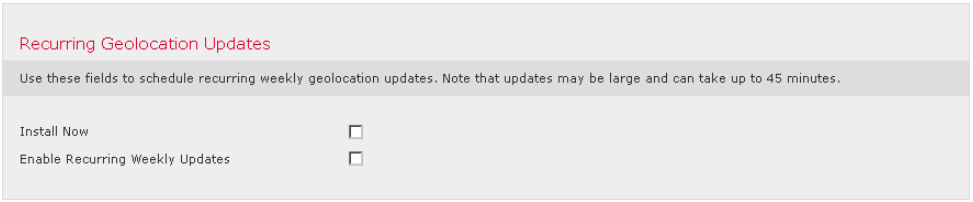
それぞれのルール更新の後で、システムが侵入についての [Policy Reapply] を実行するよう設定するだけでなく、[Import Frequency] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[Install Now] を選択します。

重要! 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。

地理情報の再帰的な更新

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、Sourcefire 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。

重要! 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、[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。

ライセンスの設定

組織に対して Sourcefire 3D System 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.6）および「Sourcefire 仮想アプライアンスのライセンス」（P.9）を参照してください。

Sourcefire では、初期設定のページを使用して、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。（動的に割り当てられたものなど）同じ MAC アドレスを使用できなかった場合は、新しいライセンスについて Sourcefire の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。

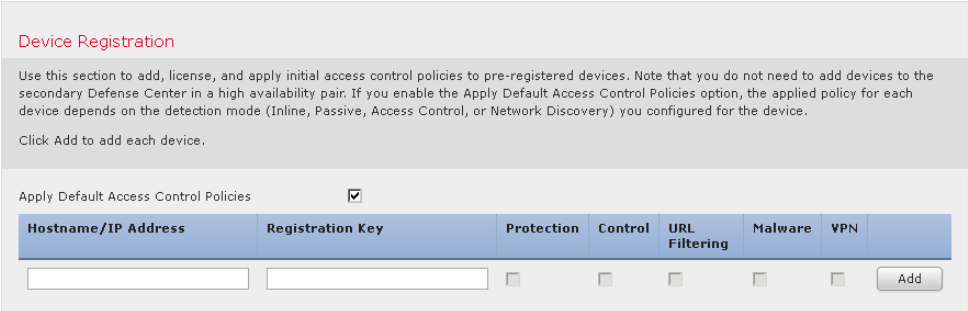
テキスト ボックスにライセンス キーをコピーし、[Submit License] をクリックしてライセンスを追加します。有効なライセンスを追加するとページが更新され、どのライセンスを追加したかを追跡することができます。ライセンスは一度に 1 つずつ追加します。

Maximum 3D8250 Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	0	5
Maximum Virtual Device 64bit Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	5	0
Maximum Virtual DC 64bit Licenses				
FireSIGHT Host	FireSIGHT User			
50000	50000			

Type	Description	Expires
3D8250	5 Protection License(s)	Never
3D8250	5 Control License(s)	Never
3D8250	5 VPN License(s)	Never
Virtual Device 64bit	5 Malware License(s)	2013-09-16 18:58:01
Virtual Device 64bit	5 Control License(s)	Never
Virtual Device 64bit	5 Protection License(s)	Never
Virtual DC 64bit	50000 FireSIGHT Host, 50000 FireSIGHT User License(s)	Never

デバイス登録

仮想防御センターは、Sourcefire 3D System 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。



アクセス制御ポリシーを登録時にデバイスに適用する場合は、デバイスを登録するときに、[Apply Default Access Control Policies] チェックボックスをオンのままにします。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。

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
アクセス制御	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に関する詳細は、「CLI を使用した仮想デバイスの設定」（P.75）を参照してください。物理デバイスについては、『*Sourcefire 3D System Installation 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、デバイス上で制御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。ただし、管理対象デバイスでサポートされていないライセンスを有効にしないようにする、モデル固有のライセンスを所有していない機能を有効にしないようにする、といったことは設定ページでは制御**できません**。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.6）および「Sourcefire 仮想アプライアンスのライセンス」（P.9）を参照してください。

重要! [Apply Default Access Control Policies] を有効にした場合は、[Inline] または [Passive] 検出モードを選択したデバイス上で保護ライセンスを有効にする必要があります。また、設定されたインターフェイスを備えている、以前に管理していたデバイス上で保護を有効にする必要があります。有効にしない場合は、デフォルトのポリシー（この場合は保護が必要）の適用が失敗します。

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。

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
		☐	☐	☐	☐	☐	Add
bodhi.example.com	buddha	Enabled	Disabled	Disabled	Enabled	Disabled	Delete
yggdrasil.example.com	loki	Enabled	Enabled	Disabled	Disabled	Enabled	Delete

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。

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、[Apply] をクリックします。

選択した内容に従って防御センターが設定されます。中間のページが表示された後で、Administrator 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.82）の手順 3 に進みます。

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、Sourcefire 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。展開の設定をどのように始めるかについて、および以降の項に記載されているタスクの詳細については、『*Sourcefire 3D SystemUser Guide*』を参照してください。

個別のユーザ アカウント

初期設定を完了した状態では、システム上のユーザは admin ユーザのみです。このユーザは Administrator のロールおよびアクセス権を所有しています。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、Sourcefire 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。Sourcefire 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。Sourcefire 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。

ソフトウェアおよびデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。Sourcefire では、展開環境内のすべてのアプライアンスが Sourcefire 3D System の最新のバージョンを実行することを推奨しています。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。

警告! Sourcefire 3D System のいずれかの部分を更新する前に、更新に付属のリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。リリース ノートには、サポートされるプラットフォーム、互換性、前提条件、警告、および特定のインストールとアンインストールの手順などの重要な情報が記載されています。

CHAPTER 6
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」（P.93）
- 「パフォーマンスの問題」（P.94）
- 「接続性の問題」（P.94）
- 「インライン インターフェイスの設定」（P.95）
- 「サポート」（P.96）

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。Sourcefire 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、『*Sourcefire 3D 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.8）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 [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 Client を使用して、管理インターフェイスおよびセンシング インターフェイスの接続性を表示し、確認することができます。

VMware vCloud Director Web Portal の使用

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

接続を確認するには：

1. [My Cloud] > [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。

2. [Action] 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。

3. [Hardware] タブで、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 NIC を表示して接続を確認します。

vSphere Client の使用

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

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：

- vSphere Client 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] リストで [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：

- vSphere Client 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.69）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 Client のいずれかを使用します。

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

アクセス：CLI の設定

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。

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。

サポート

Sourcefire の仮想デバイスまたは仮想防御センターについて質問がある場合、またはサポートが必要な場合は、Sourcefire のサポートへ連絡してください。

- Sourcefire のサポート サイト（https://support.sourcefire.com/）にアクセスしてください。
- Sourcefire のサポートにメールで連絡してください（support@sourcefire.com）。
- Sourcefire のサポートまで電話でご連絡ください（410.423.1901 または 1.800.917.4134）。

Sourcefire の製品をご利用いただきありがとうございます。