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

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

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」（P.6）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）