Firepower の概要

Cisco Firepowerは、専用プラットフォームで展開されるか、ソフトウェア ソリューションとして展開される、ネットワーク セキュリティおよびトラフィック管理製品の統合スイートです。このシステムは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワーク トラフィックを処理できるように設計されています。

標準的な展開では、ネットワーク セグメントにインストールされた複数のトラフィック検知管理対象デバイスが分析対象のトラフィックをモニタし、マネージャにレポートします。

- Firepower Management Center
- Firepower Device Manager
- Adaptive Security Device Manager（ASDM）

マネージャでは、集中管理コンソールのグラフィカル ユーザ インターフェイスを使用して管理、分析、およびレポート タスクを実行できます。

このガイドでは、*Firepower Management Center* 管理アプライアンスについて説明します。ASDMを介して管理される Firepower Device Manager または ASA with FirePOWER Services については、これらの管理手法のガイドを参照してください。

- *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*
- *ASA with FirePOWER Services Local Management Configuration Guide*

管理対象デバイスの概要

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、分析のためにトラフィックを監視します。パッシブな展開の場合、管理対象デバイスは、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、送信されたファイル（マルウェアを含む）、脆弱

性など、組織の資産に関する詳細情報を収集します。Firepower システムがこの情報を分析用に関連付けることで、ユーザがアクセスする Web サイトと使用するアプリケーションをモニタし、トラフィック パターンを評価して、侵入や他の攻撃の通知を受信できます。

インラインで展開されたシステムは、アクセス コントロールを使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークを出入りしたり通過したりするトラフィックを処理する方法を詳細に指定できます。ネットワーク トラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックのフィルタ処理や制御ができます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織の Microsoft Active Directory および LDAP ユーザ（ユーザごとに異なるアクセス レベルを付与できます）
- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号化されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入イベントが存在するかどうか

（注） システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、またはトランスペアレント インターフェイスあるいはインライン インターフェイス ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブラックリストはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

7000 および 8000 シリーズ デバイスでネットワーク管理機能を使用すると、スイッチドおよびルーテッド環境での対応、ネットワーク アドレス変換（NAT）の実行が可能になります。また、設定した仮想ルータ間でセキュアなバーチャル プライベート ネットワーク（VPN）トンネルを構築できます。バイパス インターフェイス、集約インターフェイス、8000 シリーズ 高速パス ルール、厳密な TCP の適用を設定することもできます。

7000 および 8000 シリーズ 管理対象デバイス

Cisco Firepower 7000 および 8000 シリーズ アプライアンスは、Firepower システム用に作られた物理デバイスです。7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多数の同じ機能を共有します。一般に、8000 シリーズ デバイスは 7000 シリーズ よりも高性能

で、8000 シリーズ 高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。

NGIPSv

NGIPSv（ESXi ホストとしての 64 ビット仮想デバイス）は、VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して展開できます。サポート対象のすべての ESXi バージョンで VMware ツールを有効化できます。

既定では、NGIPSv は e1000（1 ギガビット/秒）インターフェイスを使用します。また、VMware vSphere クライアントを使用して、既定のセンシングおよび管理インターフェイスを、vmxnet3（10 ギガビット/秒）インターフェイスで置き換えることもできます。

ライセンスに関係なく、NGIPSv では、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）のいずれもサポートされません。

Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services（または *ASA FirePOWER* モジュール）には、NGIPSv に類似した機能.があります。ASA FirePOWER 展開においては、ASA デバイスにより第 1 回線システム ポリシーが提供され、トラフィックが Firepower システムに渡されて、検出とアクセス制御が実行されます。

インストールされ適用されているライセンスに関係なく、ASA FirePOWER は次の Firepower システム機能をサポートしません。

- ASA FirePOWER は、Firepower システムの 7000 および 8000 シリーズ ハードウェアベースの機能（デバイス高可用性、スタッキング、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。ただし、これらの機能は ASA プラットフォームによって提供され、ASA CLI および ASDM を使用して設定できます。詳細については、ASA のマニュアルを参照してください。
- Firepower Management Center の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。
- Firepower Management Center を使用して ASA FirePOWER のシャットダウン、再起動、その他の管理を行うことはできません。

ASA FirePOWER には ASA プラットフォームに固有のソフトウェアとコマンドライン インターフェイス（CLI）があります。ASA 専用のこれらのツールを使用して、システムのインストールおよびプラットフォーム固有のその他の管理タスクを実行します。

（注） ASA FirePOWER を編集して、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、デバイスはそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての Firepower System セキュリティ ゾーン、相関ルール、関連する設定を再設定する**必要があります**。

Firepower Threat Defense

Firepower Threat Defense アプライアンスは、統合された次世代ファイアウォールと次世代の IPS デバイスを提供します。Firepower ソフトウェアのモデルで使用可能な IPS 機能に加えて、ファイアウォールおよびプラットフォーム機能には、サイト間 VPN、堅牢なルーティング、NAT、クラスタリング（Firepower 9300 の場合）、およびアプリケーション インスペクションとアクセス制御におけるその他の最適化が含まれています。

Firepower Threat Defense ソフトウェアは、次のプラットフォームでサポートされます。

- Firepower 9300
- Firepower 4100 シリーズ
- ASA 5512-X から 5555-X まで
- ASA 5508-X および 5516-X
- ASA 5506-X シリーズ

Firepower Threat Defense Virtual

Firepower Threat Defense Virtual（64 ビット仮想アプライアンス）は、仮想化環境に対して、統一された次世代ファイアウォールおよび次世代 IPS 機能を提供します。Firepower Threat Defense Virtual は、複数のハイパーバイザー環境で動作するように設計されており、管理作業のオーバーヘッドを削減し、操作効率を向上させます。

Firepower Threat Defense Virtual は、VMware vSphere ハイパーバイザーや KVM（カーネル ベースの仮想マシン）ハイパーバイザー環境を使用して展開できます。また Firepower Threat Defense Virtual は、Amazon Web Services（AWS）クラウド プラットフォームによって展開することもできます。

仮想アプライアンスと物理 Firepower Threat Defense アプライアンスについての、包括的なマルチ デバイスの展開と管理のため、Firepower Management Center を使用することができます。

Firepower Management Center の概要

Firepower Management Center は、Firepower システム展開の一元的な管理コンソールとデータベース リポジトリを提供するフォールト トレラントな専用ネットワーク アプライアンスです。また、VMware vSphere と KVM（カーネル ベースの仮想マシン）ハイパーバイザ環境を使用し

て、また Amazon Web Services（AWS）クラウド プラットフォームを使用して、64 ビットの仮想 Firepower Management Center を展開することもできます。Firepower Management Center は、さまざまなデバイス管理、イベント保存、ホスト モニタリング、およびユーザ モニタリング機能を備えています。どの Firepower Management Center でも、任意の種類の Firepower システム デバイスを管理することができます。

Firepower Management Center は、ネットワーク トラフィック情報とパフォーマンス データを集約して相互に関連付け、特定のホストに対するイベントの影響を評価します。デバイスから報告される情報を監視することができ、ネットワーク上で発生する活動全体を制御できます。Firepower Management Center は、デバイスのネットワーク管理機能（スイッチング、ルーティング、NAT、VPN など）も制御します。

Firepower Management Center の主な機能は次のとおりです。

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

Firepower Management Center の機能

このバージョンを実行している場合、すべての Firepower Management Center には同様の機能がありますが、容量と速度が主な違いとなります。Firepower Management Center のモデルによって、管理できるデバイス数、保存できるイベント数、およびモニタできるホスト数とユーザ数が異なります。

Firepower Management Center Web インターフェイスで利用可能な機能の構成は、管理しているデバイスのライセンスやモデルによって制限されていることがあります。

MC4000 では、シスコのユニファイド コンピューティング システム（UCS）プラットフォームが Firepower システムに導入されます。MC4000 は、ベースボード管理コントローラ（BMC）上で UCS Manager や Cisco Integrated Management Controller（CIMC）などのツールを使用するシスコの機能をサポートしないことに注意してください。

関連トピック

デバイス管理
データベース イベント数の制限の設定

Firepower システムのコンポーネント

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 Firepower システムの主な機能について説明します。

ヒント Firepower システム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、それぞれの機能用に Firepower システム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。

冗長性およびリソース共有

Firepower システムの冗長性とリソース共有機能を使用すれば、運用継続性を保証し、複数の 7000 および 8000 シリーズ デバイスの処理リソースを統合することができます。

デバイス 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。スタック構成を確立するときに、各スタック構成デバイスのリソースを 1 つの共有構成に統合します。

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

7000 および 8000 シリーズ デバイス ハイ アベイラビリティを使用すれば、複数の 7000 または 8000 シリーズ デバイスまたはスタック間のネットワーキング機能と設定データの冗長性を構築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ハイ アベイラビリティ ペアとして構成すると、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。デバイスのハイアベイラビリティにより、システムは手動または自動でフェールオーバーを実現することが可能です。

ほとんどの場合、SFRP を使用することによって、ハイ アベイラビリティ ペアを構成することなくレイヤ 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。

7000 & 8000 シリーズ デバイスのためのネットワーク トラフィック管理

Firepower システムのネットワーク トラフィック管理機能を使用すれば、7000 および 8000 シリーズ 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 7000 および 8000 シリーズ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（Switching）

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 Firepower システム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、7000 および 8000 シリーズ 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。複数の物理インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でパケット スイッチングが可能になります。エンドポイントは、2 台の 7000 および 8000 シリーズ デバイス、またはサードパーティ アクセス スイッチに接続している 1 台の管理対象デバイスである場合があります。

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、Firepower システムを設定できます。レイヤ 3 配置では、トラフィックを受信および転送するため、7000 および 8000 シリーズ デバイスでルーテッド 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 IP アドレスに従ってパケット転送を決定し、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（静的）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 プロトコルを設定できます。さらに、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。

展開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。複数の物理インターフェイスを単一の論理リンクにグループ化することで、ネットワークの2つのエンドポイント間でトラフィックがルーティングされます。エンドポイントは、2 台の 7000 および 8000 シリーズ デバイス、またはサードパーティ ルータに接続している 1 台の管理対象デバイスである場合があります。

NAT

レイヤ 3 の展開で、7000 および 8000 シリーズ デバイスを使用してネットワーク 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。7000 および 8000 シリーズ 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、Firepower システムを設定することができます。

マルチテナント機能

ドメイン機能では、管理対象デバイス、設定、イベントへのユーザアクセスをセグメント化することによって、Firepower システム展開内にマルチテナンシーを実装できます。

ユーザ ロールによる制限に加えて、現在のドメイン レベルによって設定の変更が制限される場合もあります。システム ソフトウェア アップデートなどのほとんどの管理タスクは、グローバル ドメインに制限されます。

検出とアイデンティティ

Cisco の検出およびアイデンティティ テクノロジーは、ネットワークの全体像を提供するためにホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、位置情報、および脆弱性に関する情報を収集します。

- ネットワーク検出ポリシーは、ネットワーク上のトラフィックを監視し、ホスト、アプリケーション、および権限のないユーザのデータを収集します。
- アイデンティティ ポリシーは、権限のあるユーザのデータを収集するため、ネットワーク上のユーザを、レルムおよび認証方式と関連付けます。

LDAP または AD サーバへの接続を確立し、ユーザ データのダウンロードを実行するため、アイデンティティ ポリシーと共にレルムを構成します。

特定のタイプの検出およびアイデンティティ データを使用すると、ネットワーク アセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

また、Firepower Management Center の Web インターフェイスを使用して、収集されたデータを表示および分析することもできます。

アクセス制御

アクセス コントロール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、および記録できます。アクセス コントロール ポリシーは、システムがネットワーク上のトラフィックを処理する方法を決定します。

最も単純なアクセス コントロール ポリシーでは、デフォルト アクションを使用してすべてのトラフィックを処理するターゲット デバイスを指定します。追加のインスペクションなしですべてのトラフィックをブロックまたは信頼するか、または侵入および検出データがないかトラフィックを検査するようにこのデフォルト アクションを設定できます。

より複雑なアクセス コントロール ポリシーは、IP、URL、および DNS のセキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録することができます。さらに、アクセス コントロール ルールを使用して、ネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照合および検査します。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザ別にトラフィックを制御できます。アクセス コントロールの詳細オプションには、復号化、前処理、およびパフォーマンスが含まれます。

各アクセス コントロール ルールにはアクションも含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

SSL インスペクション

SSL インスペクション（検査）はポリシーベースの機能です。暗号化されたトラフィックを復号化せずに処理したり、暗号化されたトラフィックを復号化して詳細なアクセス制御検査を行ったりすることができます。トラフィックの復号化や詳細な分析を行わずに信頼できない暗号化トラフィックの送信元をブロックすることも、暗号化されたトラフィックを復号化する代わりにアクセス制御を使用して検査することもできます。

暗号化トラフィックをさらに調査するために、システムにアップロードされた公開キー証明書とペア化された秘密キーを使用して、ネットワークを通過する暗号化トラフィックを復号化し、非暗号化の場合と同じ方法で復号化トラフィックをアクセス制御によって検査できます。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。システムは、暗号化された接続を処理する際にその詳細をログに記録できます。

侵入検知と防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。侵入ルールおよびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

Firepower システムには複数の侵入ポリシーが付属しています。システム付属のポリシーを使用することで、Cisco Talos Security Intelligence and Research Group（Talos）の経験を活用できます。これらのポリシーに対して、Talos は侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。

システムが提供するポリシーが組織のセキュリティのニーズに十分に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネット

ワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

Cisco Advanced Malware Protection およびファイル制御

マルウェアの影響を特定して軽減しやすくするため、Firepowerシステムのファイル制御、ネットワーク ファイル トラジェクトリ、およびAdvanced Malware Protection（AMP）の各コンポーネントによって、ネットワーク トラフィック内のファイル（マルウェア ファイルとアーカイブ ファイル内にネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析、および必要に応じてブロックできます。

ファイル制御

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

AMP for Firepower

AMP for Firepower は、ネットワーク トラフィックにいくつかのファイル タイプのマルウェアが出現するかどうかをシステムが検査できるようにするためのネットワーク ベース AMP ソリューションです。アプライアンスでは、検出されたファイルをさらに分析するためにハードドライブまたは（一部のモデルで）マルウェア ストレージ パックに保存できます。

ローカルマルウェア分析を使用してデバイス上でローカルにファイルを分析し、マルウェアを事前に分類できます。検出されたファイルを手元に保存するかどうかに関わらず、ファイルのSHA-256 ハッシュ値を使用して単純な既知ディスポジション ルックアップ用に AMP クラウドにそれを送信することができます。また、脅威のスコアを生成する動的分析を行うためにファイルを AMP Threat Grid クラウドに送信することもできます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

AMP for Firepower は、総合的なアクセス コントロール設定の一部として設定することができます。アクセス コントロール 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。

AMP for Endpoint の統合

AMP for Endpoints は、エンタープライズ クラスのエンドポイント ベース AMP ソリューションです。ユーザはそれぞれ、AMP クラウドと通信するコンピュータやモバイル デバイスに軽量コネクタをインストールします。次に Firepower Management Center により、スキャン、マルウェア検出、隔離、および侵害の兆候（IOC）のレコードをインポートし、検出された脅威のトラジェクトリを表示することが可能です。

AMP for Endpoints の展開を構成するには、AMP for Endpoints 管理コンソールを使用します。このコンソールは、マルウェアをすばやく識別し、検疫するのに役立ちます。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。AMP for Endpoints を使用すると、カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行のブロック、カスタム ホワイトリストの作成も可能です。

ネットワーク ファイル トラジェクトリ

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

- ファイルの SHA-256 ハッシュ値を計算し、その値を使用して AMP クラウドに対するクエリを実行する
- Firepower Management Center と組織の AMP for Endpoints 展開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

各ファイルにはトラジェクトリ マップが関連付けられています。このマップには、経時的なファイルの転送を視覚化した情報と、ファイルに関する追加情報が含まれています。

Cisco AMP プライベート クラウド仮想アプライアンス

AMP for Firepower と AMP for Endpoints のどちらについても、AMP クラウドにシステムから直接接続することが組織のセキュリティ ポリシーで許可されていない場合は、Cisco AMP プライベート クラウド仮想アプライアンス（AMPv）を構成できます。

AMPv は、AMP クラウドの圧縮されたオンプレミス バージョン、または匿名プロキシとして機能する仮想マシンです。通常は AMP クラウドとの直接接続が必要になるデータやアクション（AMP for Endpoints からのイベント、ファイル性質ルックアップ、レトロスペクティブ イベントなど）が、AMPv とのローカル接続によって処理されるようになります。AMPv では、エンドポイント イベント データは外部接続で共有されません。

（ファイルの性質ルックアップなどのために）AMP クラウドへの接続が必要になったとき、AMPv は、Firepower Management Center と AMP クラウドとの間の匿名化されたプロキシとして機能します。

Cisco AMP Threat Grid オンプレミス アプライアンス

組織にパブリックの AMP Threat Grid クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの AMP Threat Grid アプライアンスを展開することができます。このオンプレミス アプライアンスは、パブリック クラウドと同様に適格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを Firepower システムに返します。ただし、このオンプレミスアプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

アプリケーション プログラミング インターフェイス

アプリケーションプログラミングインターフェイス（API）を使用してシステムと対話する方法がいくつか用意されています。

eStreamer

Event Streamer（eStreamer）を使用すると、Firepower Management Center からの数種類のイベントデータを、カスタム開発されたクライアントアプリケーションにストリーム配信できます。クライアントアプリケーションを作成したら、ユーザはそれを Firepower Management Center 上の eStreamer サーバに接続し、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、Firepower Management Center 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 アクセス

データベース アクセス機能を使用すれば、JDBC SSL 接続をサポートするサードパーティ製クライアントを使用して、Firepower Management Center 上の複数のデータベース テーブルに対して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 Cisco 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のインポート 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、ディスカバリ データ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 ポートなど）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（修正）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 Firepower Management Center が自動的に修復を起動できます。ユーザが攻撃に即時に対処できない場合でも、修正により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、Firepower Management Center 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。

Firepower のオンライン ヘルプとドキュメンテーション

オンライン ヘルプには、Web インターフェイスからアクセスできます。

- 各ページで状況依存ヘルプのリンクをクリックする。
- **[ヘルプ（Help）]** > **[オンライン（Online）]** を選択する。

ドキュメンテーション ロードマップを使用して、Firepowerに関連する追加ドキュメンテーションを見つけることができます（http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html）。

ドキュメンテーションのライセンス ステートメント

項の先頭に記載されているライセンス ステートメントは、項で説明される機能を有効にするために Firepower システムの管理対象デバイスに割り当てる必要があるのは従来のライセンスかスマート ライセンスかを示します。

ライセンス付きの機能の多くは追加的であるため、ライセンス ステートメントでは、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。

ライセンス文の「または」という語は、その項に記載されている機能を有効にするには特定のライセンスを管理対象デバイスに指定する必要があることを示していますが、追加のライセンスで機能を追加できます。たとえば、ファイル ポリシー内では、一部のファイル ルール アクションではデバイスに保護ライセンスを指定する必要がありますが、他方ではマルウェア ライセンスを指定する必要があります。

ライセンスの詳細については、Firepower の機能ライセンスについてを参照してください。

関連トピック

Firepower の機能ライセンスについて

ドキュメント内のサポート対象デバイスに関する記述

章または項目の先頭に記載されているサポート対象デバイスに関する記述は、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 8000 シリーズ のデバイスでのみサポートされています。

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、リリース ノートを参照してください。

ドキュメント内のアクセス ステートメント

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 ステートメントは、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。記載されている任意のロールを使用して手順を実行することができます。

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。事前定義されたロールを使用して手順のアクセス要件が示されている場合は、同様の権限を持つカスタム ロールにもアクセス権があります。カスタム ロールを持っているユーザは、設定ページにアクセスするために使用するメニュー パスが若干異なる場合があります。たとえば、侵入ポリシー権限のみが付与されているカスタム ロールを持つユーザは、アクセス コントロール ポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。

ユーザ ロールの詳細については、定義済みのユーザ ロールおよびカスタム ユーザ ロールを参照してください。

Firepower システムの IP アドレス表記法

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 と同様のプレフィックス長の表記を使用して、Firepower システムのさまざまな場所でアドレス ブロックを定義することができます。

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、Firepower システムは、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、Firepower システムでは 10.0.0.0/8 が使用されます。

つまり、Cisco では 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、Firepower システムではこれは必要ありません。