Firepower Management Center の基礎

以下のトピックでは、Firepower Management Center の基礎について説明します。

Firepower Management Center

Firepower Management Center を使用して、Firepower システムを構成するすべてのデバイスを管理できます。デバイスを管理するには、Firepower Management Center とデバイスの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Firepower Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Firepower Management Center に送信します。

デバイス管理

Firepower Management Center は、Firepower システムのキー コンポーネントです。Firepower システムを構成するあらゆるデバイスを管理したり、ネットワーク上で検出された脅威を集約し、分析して対処するために、Firepower Management Center を使用できます。

Firepower Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを単一の場所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Firepower Management Center からデバイスのヘルス ステータスをモニタできます。

Firepower Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firepower Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

（注） Firepower Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で使用可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは新しい機能は利用できません。

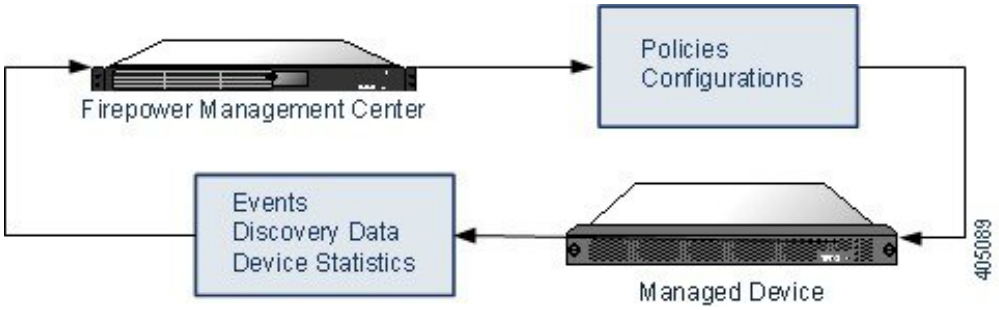
Firepower Management Center で管理できるデバイス

Firepower Management Center を Firepower システムの展開環境における中央の管理ポイントとして使用して、次の各デバイスを管理することができます。

- 7000 および 8000 シリーズ デバイス
- ASA FirePOWER モジュール
- NGIPSv デバイス
- Firepower Threat Defense および Firepower Threat Defense Virtual

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TCP トンネルを介して、Firepower Management Center とデバイスの間で送信されます。

次の図に、Firepower Management Center と管理対象デバイスの間で送信される情報をリストします。アプライアンス間で送信されるイベントとポリシーのタイプは、デバイス タイプに基づくことに注意してください。



ポリシーとイベント以外の機能

Firepower Management Center では、ポリシーをデバイスに展開したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

NGIPSv デバイスや ASA FirePOWER モジュールのバックアップ ファイルを作成、復元することは**できません**。

物理的な管理対象デバイス自体からそのバックアップを実行する場合は、デバイス設定**のみ**をバックアップできます。設定データと統合ファイル（任意）をバックアップするには、管理 Firepower Management Center を使用してデバイスのバックアップを実行します。

イベント データをバックアップするには、管理 Firepower Management Center のバックアップを実行します。

デバイスの更新

シスコは適宜、Firepower システムの更新プログラムをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベースの更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

Firepower Management Center を使用して、管理対象デバイスに更新プログラムをインストールできます。

関連トピック

バックアップ ファイル

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベート ネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Firepower Management Center 通信に支障はありませんが、ポート アドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。Firepower Management Center がデバイスの IP アドレスを指定し、デバイスが Firepower

Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Firepower Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを Firepower Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを指定します。デバイス上で、Firepower Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Firepower Management Center の IP アドレスに登録されます。この時点で、Firepower Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Firepower Management Center に追加することができます。Firepower Management Center で、追加するデバイスごとに一意の NAT ID を指定し、次に各デバイスで、Firepower Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。