はじめに

概要

このガイドでは、ファイアウォールのイベントデータを保存し、より長い保存期間でストレージを増やすようにシスコのセキュリティ分析とロギング（オンプレミス）を設定する方法について説明します。Cisco Secure Network Analytics（旧 Stealthwatch）アプライアンスを展開し、Firewall 展開に統合することで、イベントデータを Secure Network Analytics アプライアンスにエクスポートできます。

その後、次の操作を実行できます。

- Firepower Management Center にイベントを保存し、Secure Network Analytics 展開にイベントを保存します。
- このリモートデータソースを指定して、Firepower Management Center でこれらのイベントを表示します。
- イベントビューアを使用して、Cisco Secure Network Analytics Manager（旧 Stealthwatch 管理コンソール）Web アプリケーション UI からイベントデータを確認します。
- Firepower Management Center UI からイベントビューアに相互起動して、相互起動元の情報に関する追加のコンテキストを表示します。

（注） オンプレミスではなく Cisco Cloud にファイアウォール イベント データを保存する場合、詳細については Cisco Security Analytics and Logging (SaaS) documentation を参照してください。

サポートされるイベント タイプ

- FTD セキュリティイベント
  - 接続

- 侵入（Intrusion）
- ファイルおよびマルウェア

- FTD データプレーンイベント
- ASA イベント

概念とアーキテクチャ

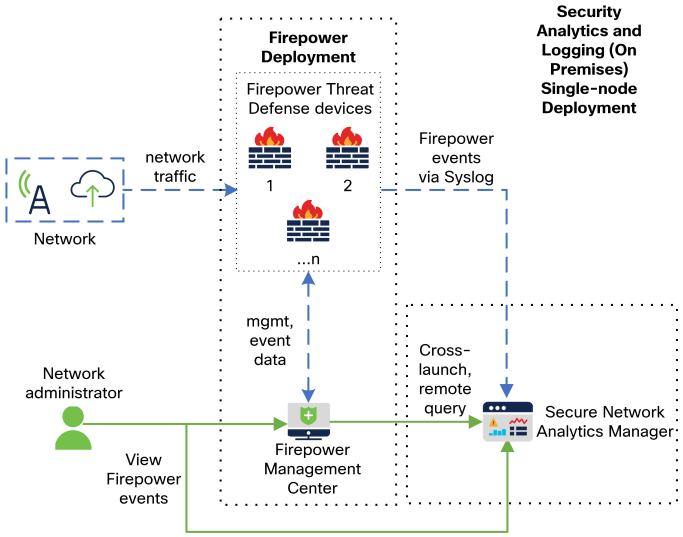
セキュリティ分析とロギング（オンプレミス）の展開では、Secure Network Analytics アプライアンスを使用して別のシスコ製品の展開環境（Firepower アプライアンス展開など）からのデータを保存します。Firepower 展開の場合、Firepower セキュリティイベントおよびデータプレーンイベントを UDP を介した syslog として Firepower Management Center が管理する Firepower Threat Defense デバイスから マネージャ にエクスポートして、その情報を保存します。セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0 では、syslog を介して ASA デバイスから マネージャ にイベントをエクスポートする機能が追加されました。

Secure Network Analytics の展開には次の 2 つのオプションがあります。

- 単一ノード：スタンドアロンの Manager を展開してイベントを受信および保存し、そこからイベントを確認および照会します。
- マルチノード：イベントを受信する Cisco Secure Network Analytics フローコレクタ、イベントを保存する Cisco Secure Network Analytics データストア（Cisco Secure Network Analytics データノード X 3 を装備）、イベントを確認および照会できる Manager を展開します。

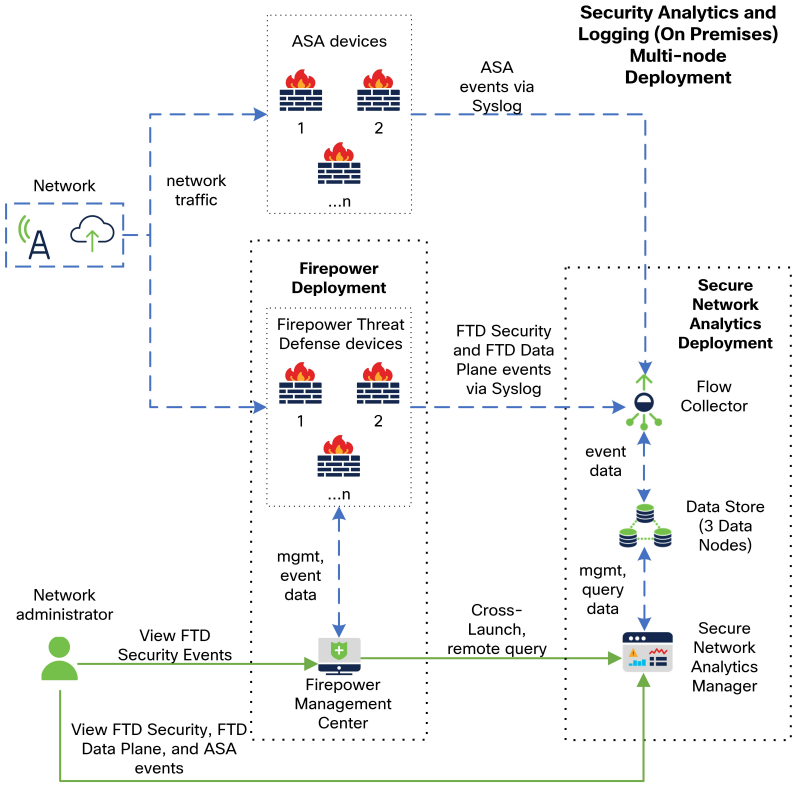
（注） スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと 3 つのデータノード（マルチノード）を管理する マネージャ のインストールがサポートされています。3 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャ にアプリケーションをインストールすることはできません。詳細については、トラブルシューティングを参照してください。

マネージャ を使用した 単一ノード の展開の例については、次の図を参照してください。



この展開では、Firepower Threat Defense デバイスは Firepower のイベントを マネージャ に送信し、Manager がこれらのイベントを保存します。ユーザは Firepower Management Center の UI からマネージャを相互起動して保存されたイベントに関する詳細情報を表示できます。また、Firepower Management Center からリモートでイベントを照会することもできます。

マネージャ、3 つのデータノード、およびフローコレクタを使用したマルチノードの展開の例については、次の図を参照してください。



この展開では、Firepower Threat Defense デバイスおよび ASA デバイスはファイアウォールのイベントをフローコレクタに送信します。フローコレクタは、保存のためにデータストア（データノード X 3）にイベントを送信します。ユーザは Firepower Management Center の UI から マネージャを相互起動して保存されたイベントに関する詳細情報を表示できます。また、Firepower Management Center からリモートでイベントを照会することもできます。