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。

- Secure Firewall 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、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。
- 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。

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） 展開では、Secure Network Analytics アプライアンスを使用して、別のシスコ製品展開からのデータを保存できます。Secure Firewall 展開の場

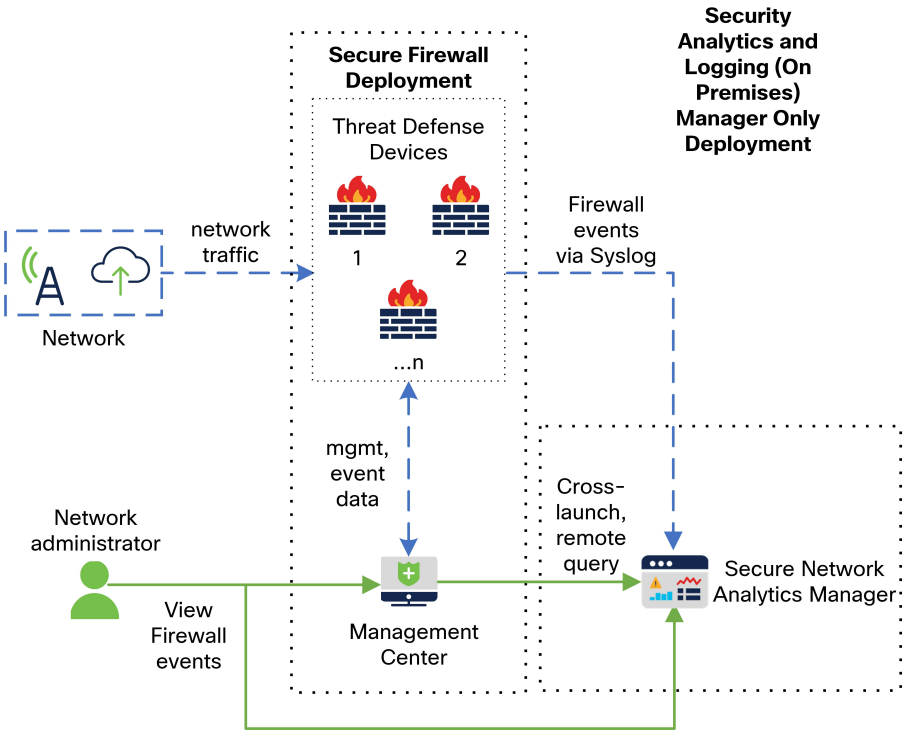
合、セキュリティイベントおよびデータプレーンイベントを Management Center が管理する Secure Firewall Threat Defense デバイスから マネージャ にエクスポートして、その情報を保存します。

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

- マネージャのみ：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。
- データストア：イベントを受信する Cisco Secure Network Analytics フローコレクタ（最大 5 つ）、イベントを保存する Cisco Secure Network Analytics データストア（3 つの Cisco Secure Network Analytics データノードのセットのうち 1 つ、3 つ、またはそれ以上を装備）、イベントを確認および照会できる Manager を展開します。

マネージャのみ

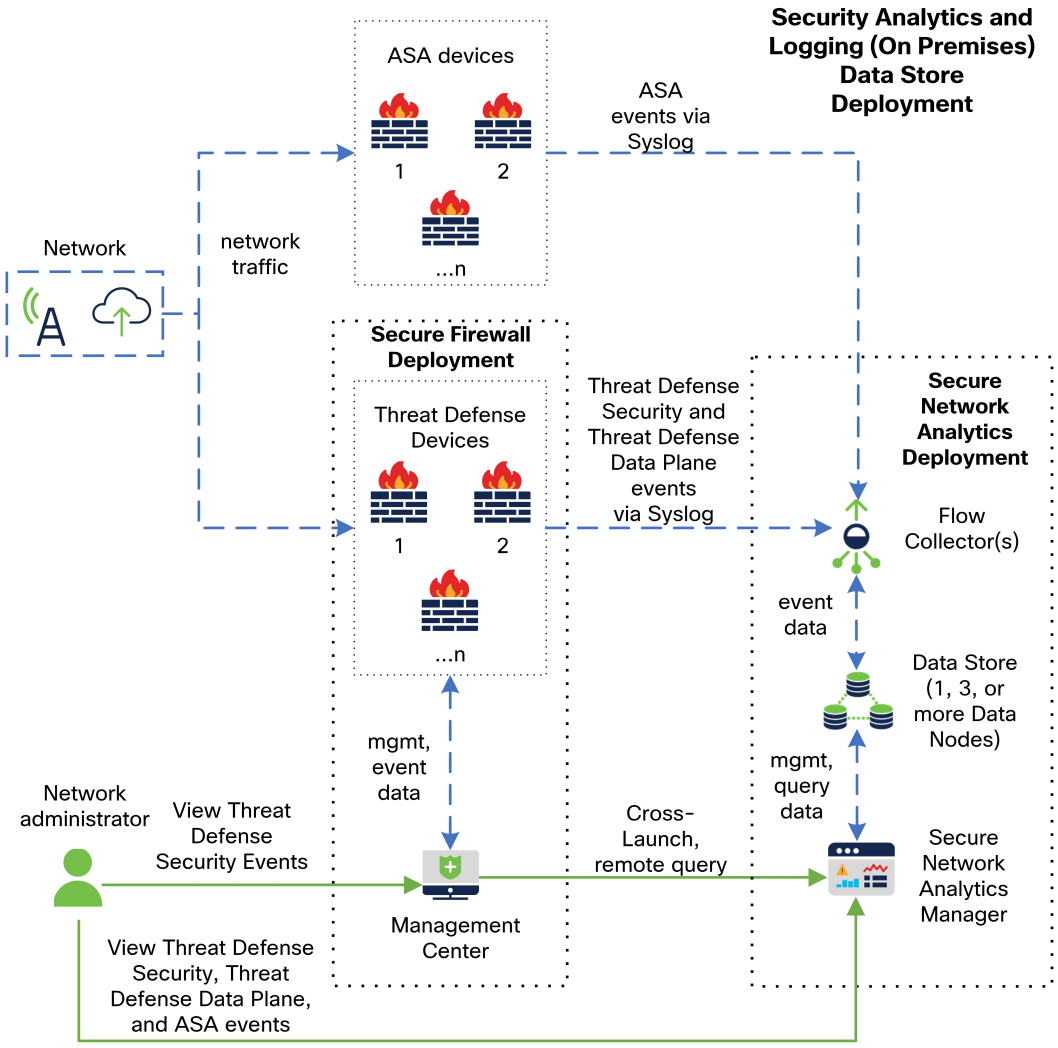
マネージャのみ の展開の例については、次の図を参照してください。



この展開では、脅威に対する防御 デバイスは Secure Firewall 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 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、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。

データストア

マネージャ、データノード、およびフローコレクタを使用した データストア 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、脅威に対する防御 および Secure Firewall 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にイベントを送信します。ユーザは 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、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。

サポートされるイベント タイプ

- Threat Defense セキュリティイベント
  - 接続
  - 侵入
  - ファイルおよびマルウェア

- Threat Defense データプレーンイベント（データストア 展開のみ）
- ASA イベント（データストア 展開のみ）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。