

Web ユーザ インターフェイスを使ったパケットデータ (PCAP ファイル) のダウンロード

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[PCAP ファイルのダウンロード手順](#)

概要

この記事では、Sourcefire FireSIGHT Management SystemのWebユーザインターフェイスを使用してパケットキャプチャデータ (PCAPファイル) をダウンロードする手順について説明します。

前提条件

要件

Sourcefire FirePOWER デバイスとバーチャル デバイスのモデルに関する知識があることが推奨されます。

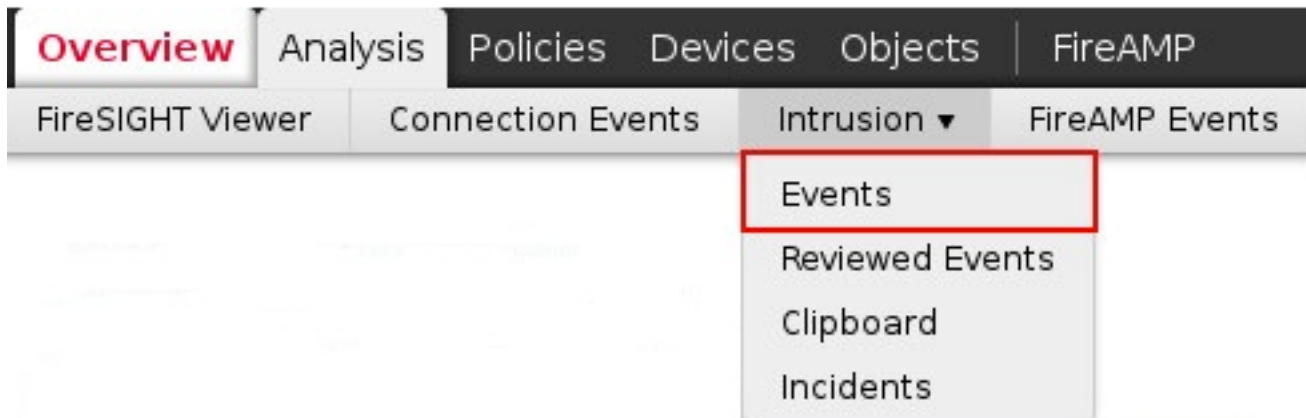
使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 5.2 以降が稼働する Sourcefire FireSIGHT Management Center (Defense Center と呼ばれる) に基づくものです。

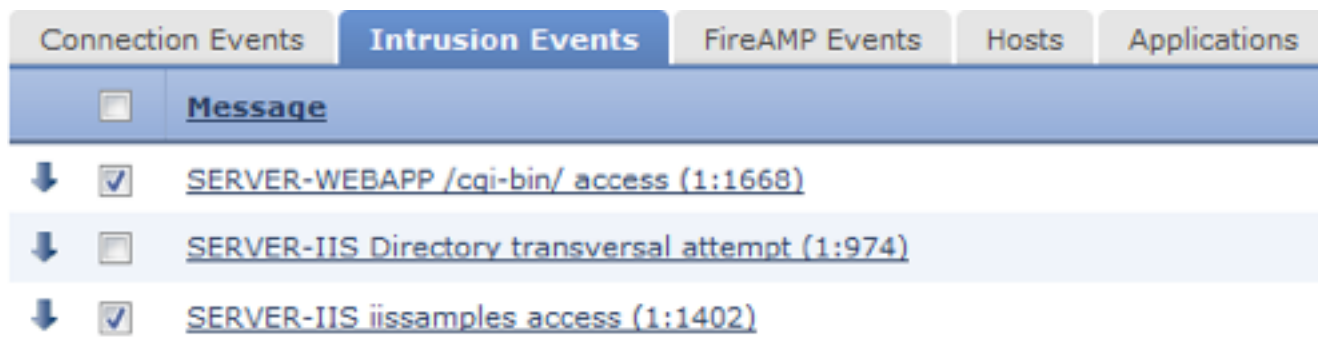
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

PCAP ファイルのダウンロード手順

ステップ 1 : Sourcefire Defense Center または Management Center にログインし、次に示すように [Intrusion Events] ページに移動します。



ステップ 2 : チェックボックスを使用して、パケット キャプチャ データ (PCAP ファイル) をダウンロードするイベントを選択します。



ステップ 3 : ページの下部までスクロールし、次のいずれかを実行します。

- [Download Packet] をクリックし、選択されている侵入イベントをトリガーしたパケットをダウンロードします。
- [Download All Packets] をクリックし、現在の制限ビューに示されている侵入イベントをトリガーしたすべてのパケットをダウンロードします。

注 : ダウンロードしたパケットは PCAP として保存されます。 パケット キャプチャを分析するには、PCAP ファイルを読み取ることができるソフトウェアをダウンロードしてインストールする必要があります。

ステップ 4 : プロンプトが表示されたら、ハード ドライブに PCAP ファイルを保存します。