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

目次

概要

Web ユーザ インターフェイスを使用して、Snort ルールをトリガーしたパケットをダウンロードできます。この記事では、Sourcefire FireSIGHT 管理システムの Web ユーザ インターフェイスを使用したパケット キャプチャ データ（PCAP ファイル）のダウンロード手順を説明します。

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。

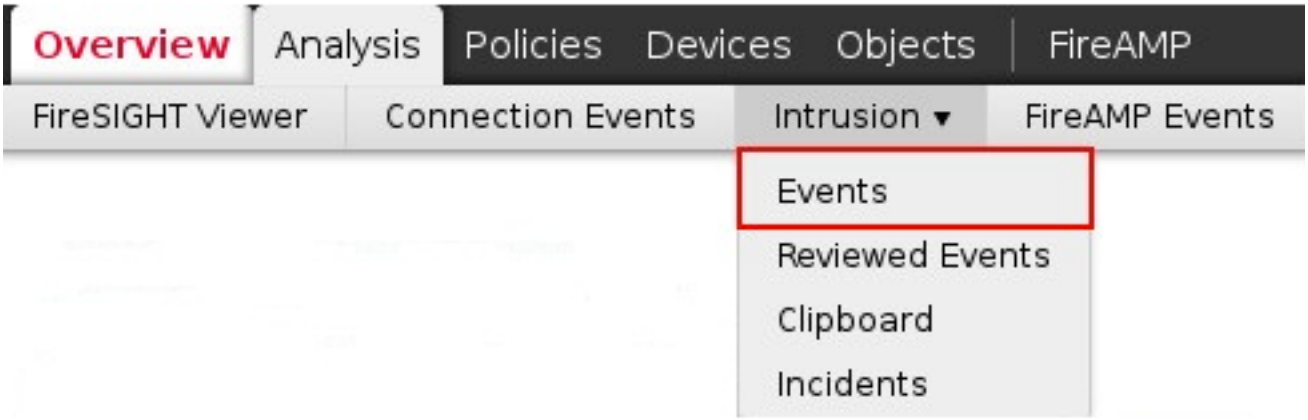
使用するコンポーネント

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 とも呼ばれる）に基づくものです。

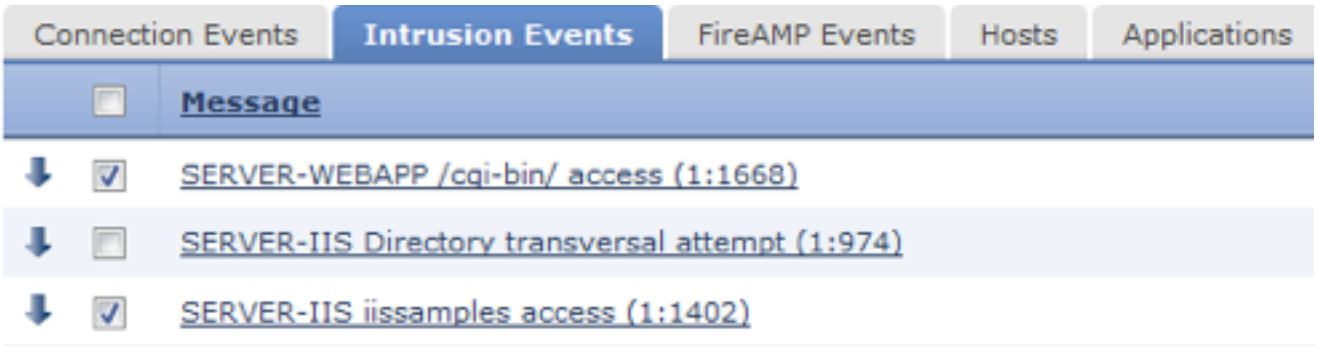
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。