

Download de dados de pacote (arquivo PCAP) usando a interface de usuário da Web

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Etapas para o download do arquivo PCAP](#)

Introduction

Usando a Interface de Usuário da Web, você pode baixar os pacotes que dispararam a regra Snort. O artigo fornece as etapas para baixar dados de captura de pacotes (arquivo PCAP) usando a Interface de Usuário da Web de um Sourcefire FireSIGHT Management System.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre os modelos de dispositivos virtuais e do Sourcefire FirePOWER.

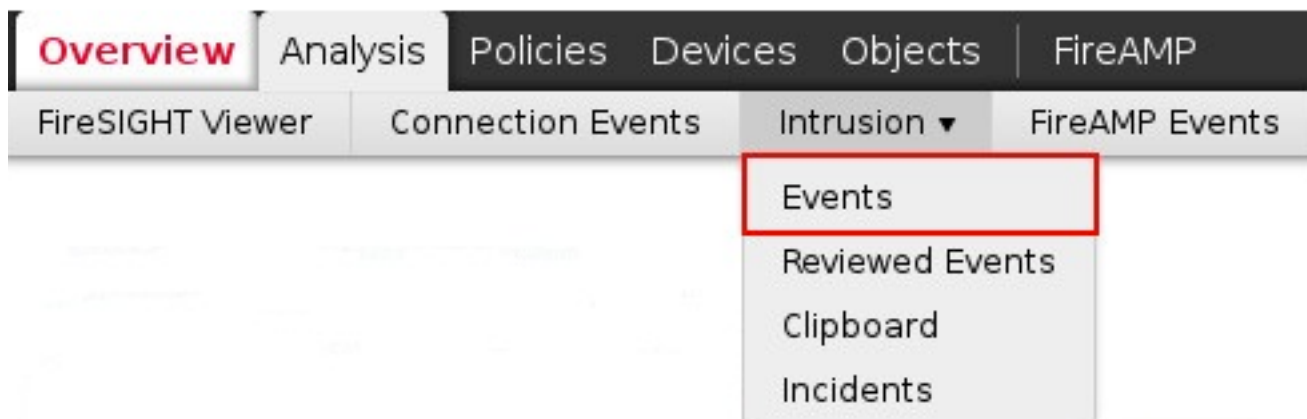
Componentes Utilizados

As informações neste documento são baseadas no Sourcefire FireSIGHT Management Center, também conhecido como Defense Center, executando a versão de software 5.2 ou posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Etapas para o download do arquivo PCAP

Passo 1: Faça login em um Sourcefire Defense Center ou Management Center e navegue até a página Eventos de intrusão como abaixo:



Passo 2: Usando a caixa de seleção, selecione o(s) evento(s) que deseja baixar os dados de captura de pacote (arquivo PCAP).



Passo 3: Role até a parte inferior da página e:

- Clique em Baixar pacote para baixar os pacotes que dispararam os eventos de intrusão selecionados
- Clique em Baixar todos os pacotes para baixar todos os pacotes que dispararam os eventos de intrusão na exibição restrita atual

Note: Os pacotes baixados serão salvos como PCAP. Se quiser analisar a captura de pacotes, será necessário baixar e instalar um software capaz de ler um arquivo PCAP.

Passo 4: Quando solicitado, salve o arquivo PCAP no disco rígido.