

Datos del paquete de la descarga (archivo PCAP) usando la interfaz del Web User

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Pasos para descargar el archivo PCAP](#)

Introducción

Usando la interfaz del Web User, usted puede descargar los paquetes que accionaron la regla del Snort. El artículo proporciona los pasos para descargar los datos de la captura de paquetes (archivo PCAP) usando la interfaz del Web User de un sistema de administración de Sourcefire FireSIGHT.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento en el dispositivo de Sourcefire FirePOWER y los modelos del dispositivo virtual.

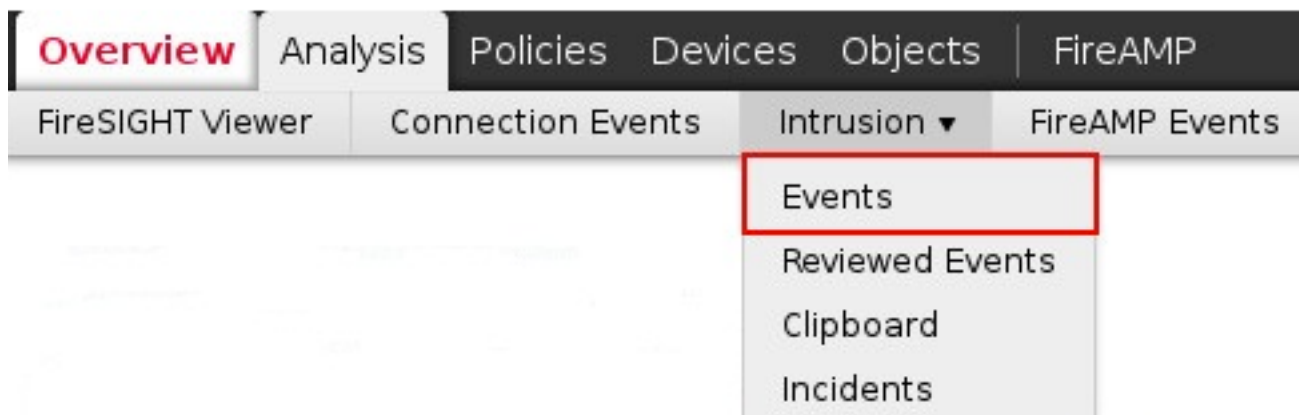
Componentes Utilizados

La información sobre este documento se basa en el centro de administración de Sourcefire FireSIGHT, también conocido como el centro de la defensa, versión de software corriente 5.2 o mayor.

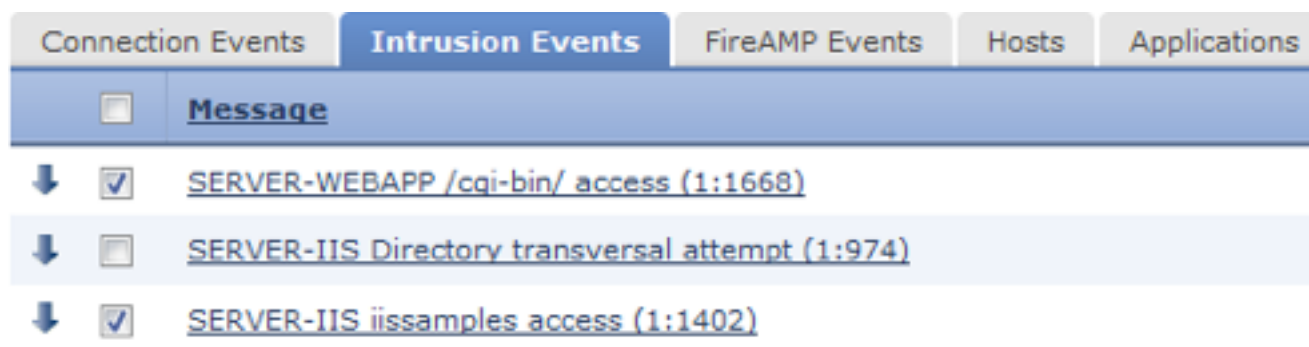
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Pasos para descargar el archivo PCAP

Paso 1: El login a un centro o a un centro de administración de la defensa de Sourcefire, y navega a la página de los eventos de la intrusión como abajo:



Paso 2: Usando la casilla de verificación, seleccione los eventos que usted quisiera que descargaran los datos de la captura de paquetes (archivo PCAP).



Paso 3: Navegue a la parte inferior de la página y de cualquiera:

- Haga clic el paquete de la descarga para descargar los paquetes que accionaron los eventos seleccionados de la intrusión
- Haga clic la descarga todos los paquetes para descargar todos los paquetes que accionaron los eventos de la intrusión en la visión obligada corriente

Note: Los paquetes descargados serán guardados como PCAP. Si usted quiere analizar a la captura de paquetes, usted necesitará descargar y instalar el software que es capaz de leer un archivo PCAP.

Paso 4: Cuando se le pregunte, salve el archivo PCAP a su unidad de disco duro.