Cómo determinar el tráfico manejado por un caso específico del Snort

Contenido

Introducción

Este documento describe cómo determinar el tráfico que está siendo manejado por un caso específico del snort. Este detalle es muy útil mientras que resuelve problemas CPU elevada la utilización en un snort específico cita como ejemplo.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología de FirePOWER

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Centro de administración 6.X de FirePOWER y arriba
- Aplicable a todos los dispositivos administrados que incluyen la defensa de la amenaza de FirePOWER, los módulos de FirePOWER, y los sensores de FirePOWER

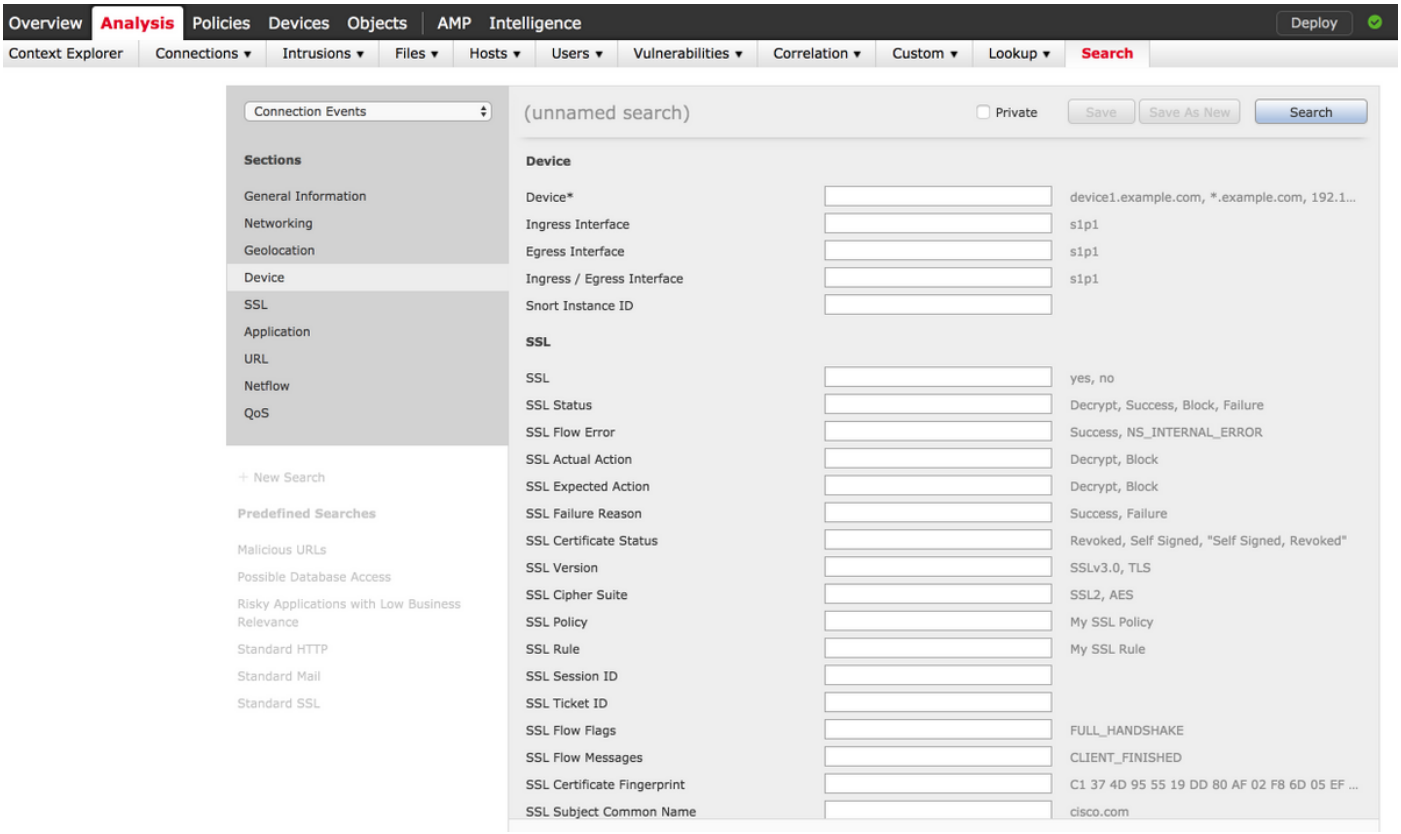
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de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

Configurar

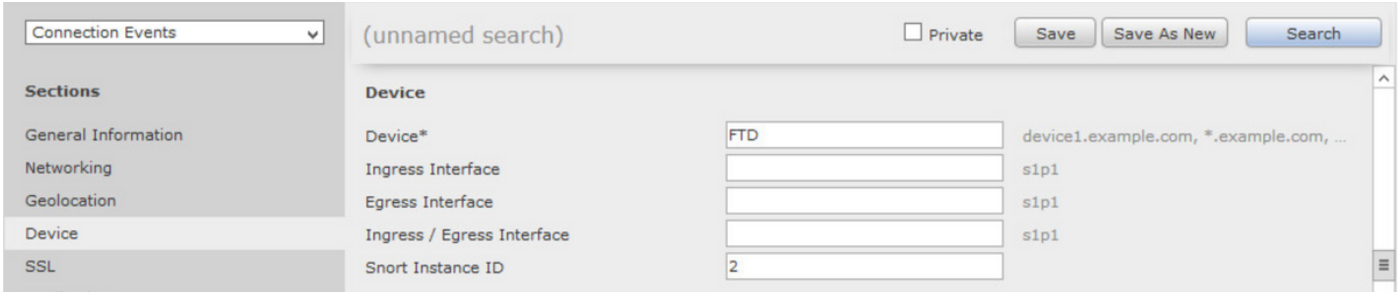
Configuraciones

Inicie sesión al centro de administración de FirePOWER con los privilegios de la administración.

El login es una vez acertado, navega al **análisis > a la búsqueda,** tal y como se muestra en de la imagen:



Asegúrese de que los **eventos de conexión que la** tabla se elige del descenso abajo y entonces seleccione el **dispositivo de la** sección. Ingrese los valores para el campo del dispositivo y resople el caso ID (0 a N, el número de casos del snort depende del dispositivo administrado), tal y como se muestra en de la imagen:



Una vez que se ingresan los valores, la **búsqueda del** tecleo y el resultado serían los eventos de conexión que son accionados por el caso específico del snort.

Note: Si el dispositivo administrado es defensa de la amenaza de FirePOWER, usted puede determinar los casos del snort usando el modo FTD CLISH.

```
> show asp inspect-dp snort
SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- --
--- ---------------- ---------- ---------- ---------- 0 5266 0% ( 0%| 0%) 0 0 READY 1 5268 0% (
0%| 0%) 0 0 READY 2 5267 0% ( 0%| 0%) 0 0 READY 3 5270 0% ( 0%| 0%) 0 0 READY 4 5269 0% ( 0%|
0%) 0 0 READY
```

Note: Si el dispositivo administrado es módulo de FirePOWER o sensor de FirePOWER, usted puede determinar los casos del snort usando el Modo experto y el **comando top** basado Linux.

```
admin@firepower:~$ top
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 5247 root      20   0 15248 1272  932 S    0  0.0   0:03.05 top
 5264 root       1 -19 1685m 461m  17m S    0  2.9   1:05.26 snort
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.