Cómo determinar el tráfico manejado por una instancia de Snort específica

Contenido

Introducción

Este documento describe cómo determinar el tráfico que está siendo manejado por una instancia de snort específica. Este detalle es muy útil mientras se resuelve el problema del uso elevado de la CPU en una instancia de snort específica.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower

Componentes Utilizados

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

- Firepower Management Center 6.X y posterior
- Aplicable a todos los dispositivos administrados que incluyen Firepower Threat Defense, Firepower Modules y Firepower Sensors

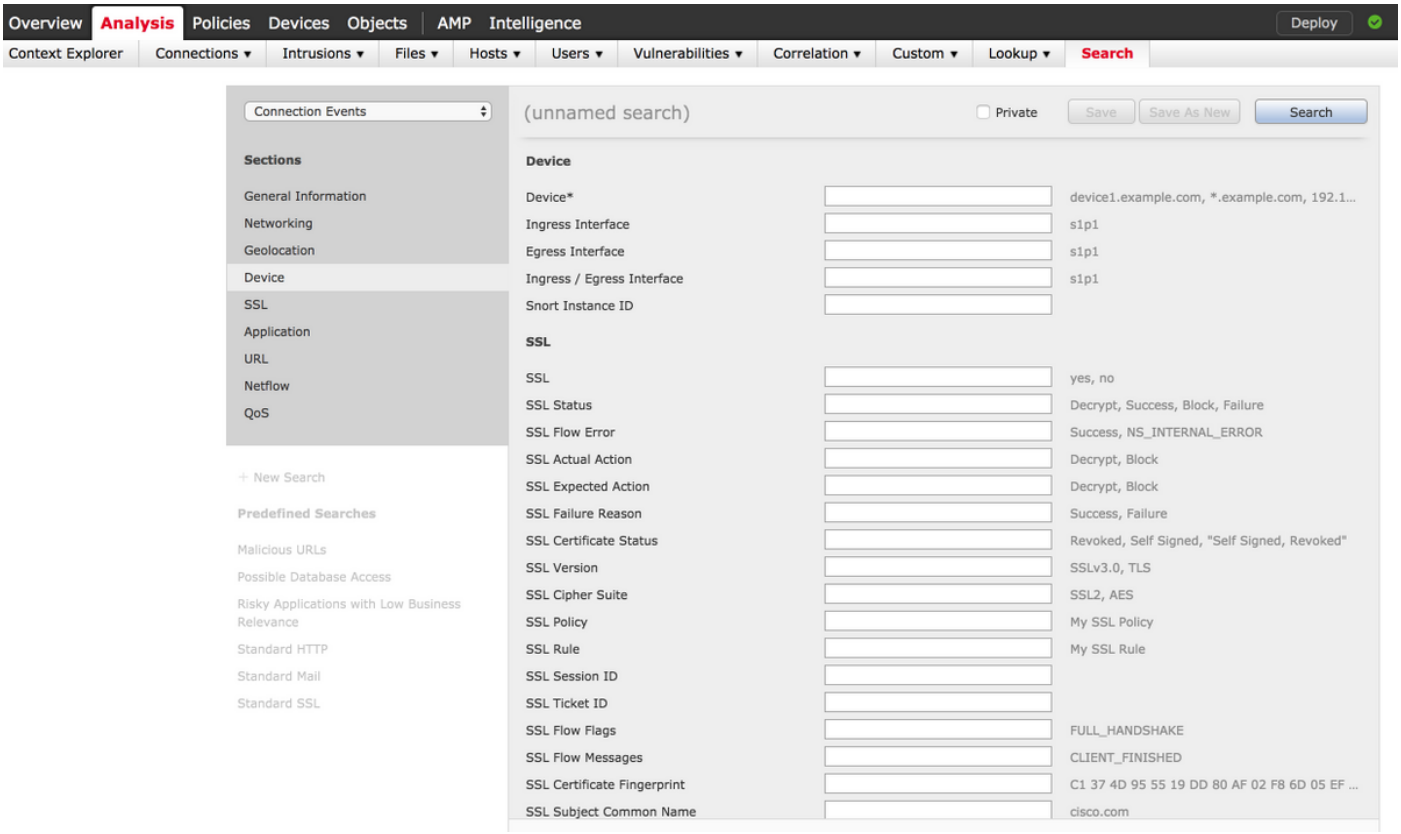
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Configuraciones

Inicie sesión en Firepower Management Center con privilegios de administración.

Una vez que el login se realiza correctamente, navegue hasta **Analysis > Search,** como se muestra en la imagen:



Asegúrese de que la tabla **Eventos de conexión** se elija en el menú desplegable y, a continuación, seleccione el **Dispositivo** en la sección. Introduzca los valores para el campo Dispositivo y la ID de instancia de Snort (0 a N, el número de instancias de Snort depende del dispositivo administrado), como se muestra en la imagen:

Una vez introducidos los valores, haga clic en **Buscar** y el resultado serían los eventos de conexión que se activan por la instancia de sondeo específica.

Nota: Si el dispositivo administrado es Firepower Threat Defense, puede determinar las instancias de sondeo utilizando 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
```

Nota: Si el dispositivo administrado es Firepower Module o Firepower Sensor, puede determinar las instancias de snort usando el modo experto y el **comando** superior basado en 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.

Troubleshoot

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