Como determinar o tráfego tratado por uma instância específica do Snort

Contents

Introduction

Este documento descreve como determinar o tráfego que está sendo tratado por uma instância de snort específica. Esse detalhe é muito útil ao solucionar problemas de alta utilização da CPU em uma instância de snort específica.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center 6.X e superior
- Aplicável a todos os dispositivos gerenciados que incluem Firepower Threat Defense, Firepower Modules e Firepower Sensors

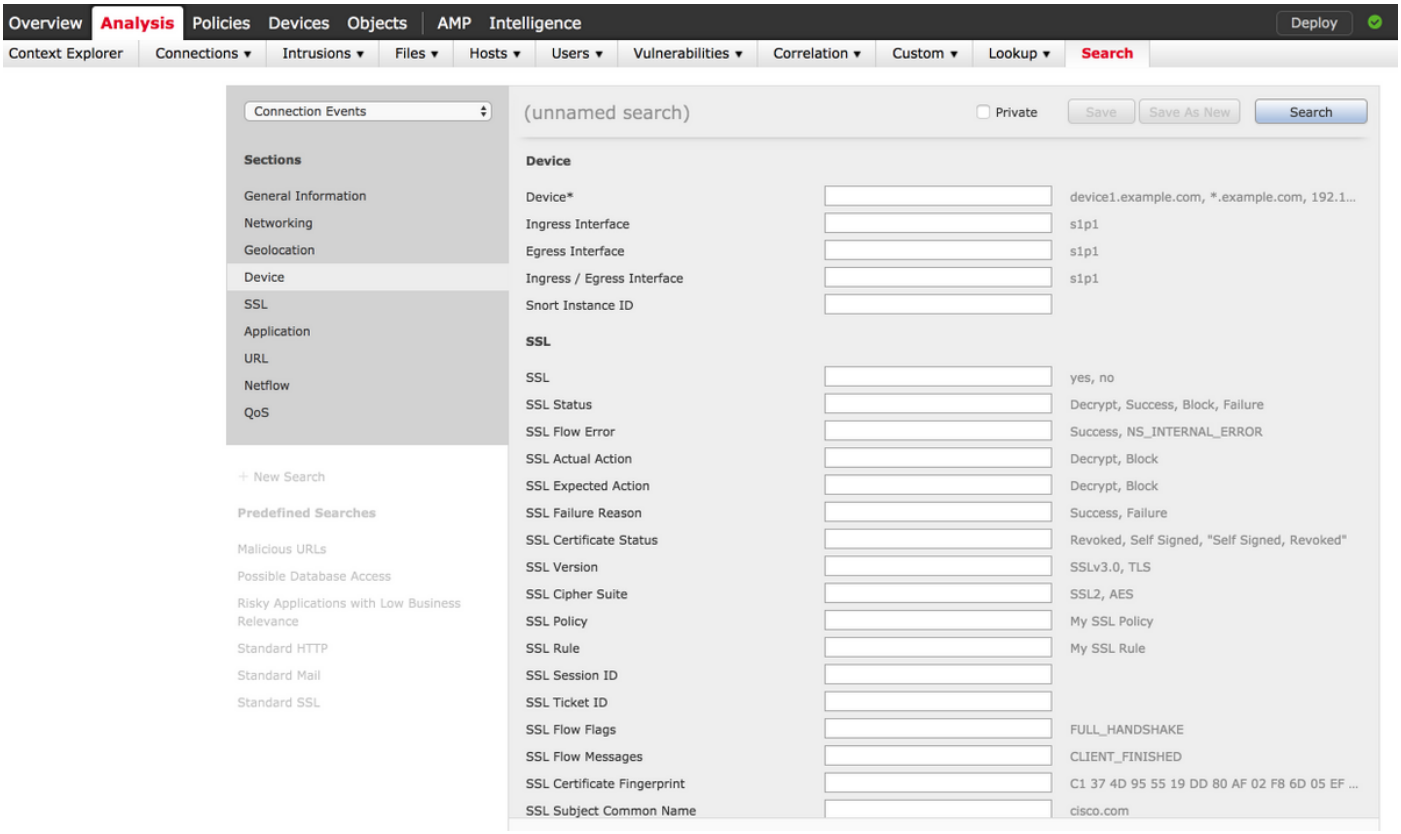
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

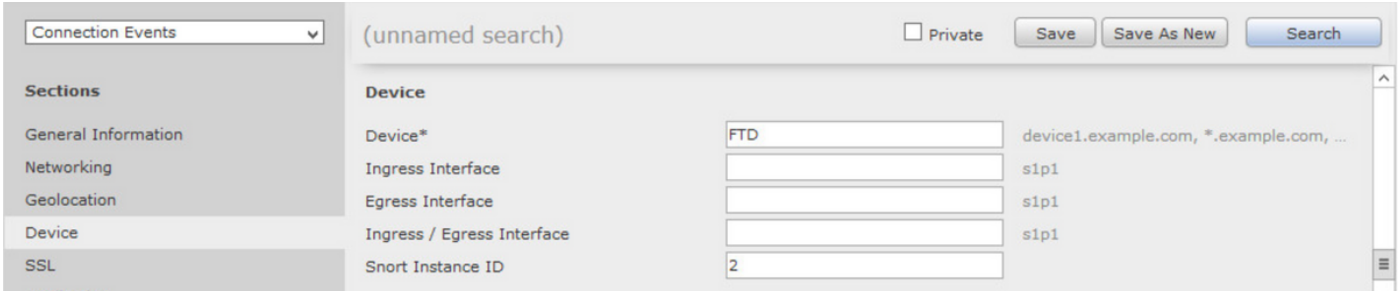
Configurações

Faça login no Firepower Management Center com privilégios de administração.

Quando o login for bem-sucedido, navegue para **Analysis > Search,** como mostrado na imagem:



Verifique se a tabela **Eventos de Conexão** está selecionada na lista suspensa e selecione o **Dispositivo** na seção. Insira os valores para o campo Dispositivo e a ID da instância de Snort (0 a N, o número de instâncias de snort depende do dispositivo gerenciado), como mostrado na imagem:



Quando os valores forem inseridos, clique em **Pesquisar** e o resultado serão eventos de conexão que são disparados pela instância de snort específica.

Note: Se o dispositivo gerenciado for Firepower Threat Defense, você poderá determinar as instâncias de snort usando o 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: Se o dispositivo gerenciado for Firepower Module ou Firepower Sensor, você poderá determinar as instâncias de snort usando o modo especialista e o comando **top** baseado em 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.