

Como determinar o tráfego segurado por um exemplo específico do Snort

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como determinar o tráfego que está sendo segurado por um exemplo específico do snort. Este detalhe é muito útil ao pesquisar defeitos a utilização elevada da CPU em um exemplo específico do snort.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia da potência de fogo

Componentes Utilizados

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

- Centro de gerenciamento 6.X da potência de fogo e acima
- Aplicável a todos os dispositivos gerenciado que incluem a defesa da ameaça da potência de fogo, os módulos da potência de fogo, e os sensores da potência de fogo

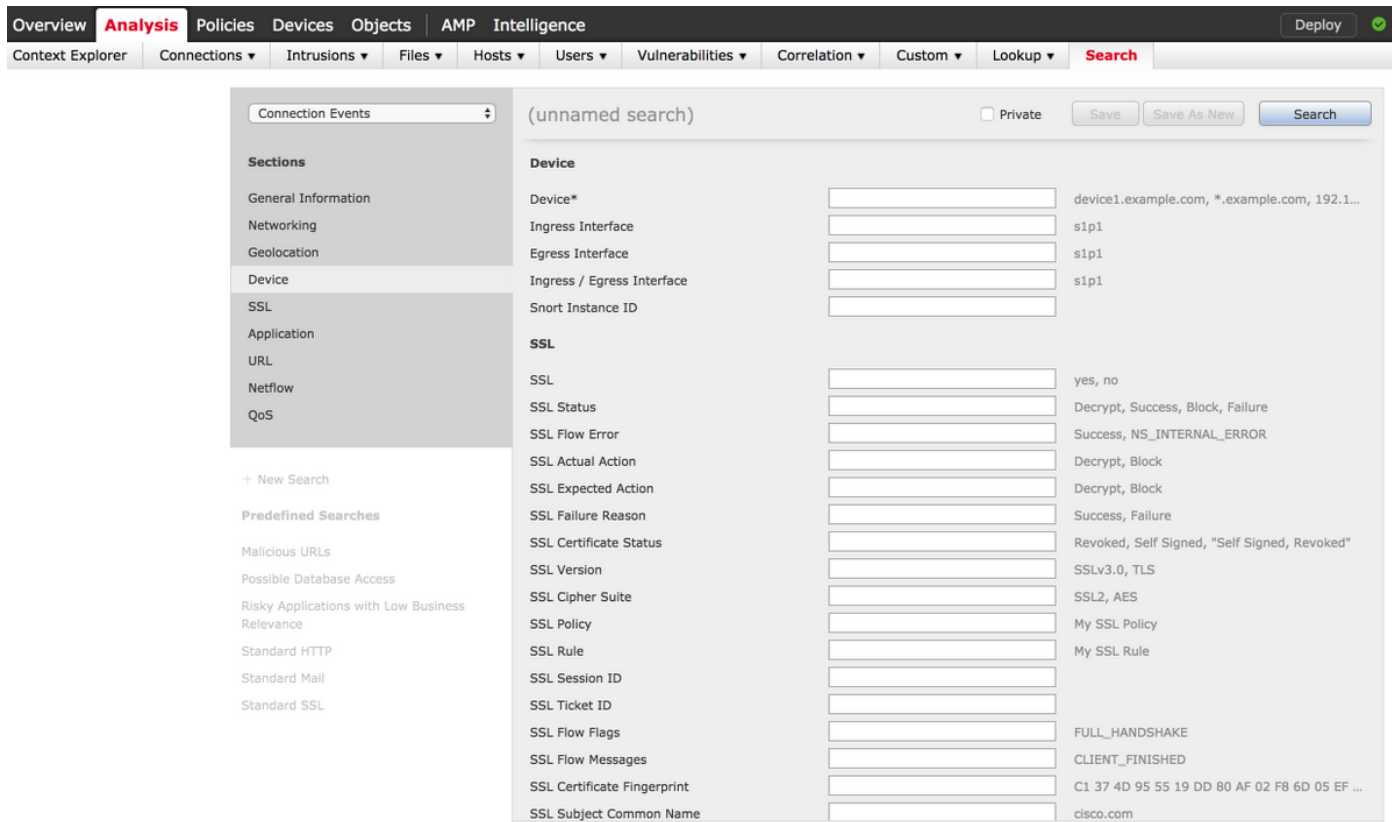
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configurações

Entre ao centro de gerenciamento da potência de fogo com privilégios da administração.

Uma vez que o início de uma sessão é bem sucedido, navegue à **análise > à busca**, segundo as indicações da imagem:



Assegure-se de que os **eventos de conexão** que a tabela é escolhida da gota para baixo e seleccione então o **dispositivo** da seção. Incorpore valores para o campo de dispositivo e ronque o exemplo ID (0 a N, o número de exemplos do snort dependem do dispositivo gerenciado), segundo as indicações da imagem:



Uma vez que os valores são incorporados, a **busca** do clique e o resultado seriam os eventos de conexão que são provocados pelo exemplo específico do snort.

Nota: Se o dispositivo gerenciado é defesa da ameaça da potência de fogo, você pode determinar os exemplos do 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
```

Nota: Se o dispositivo gerenciado é módulo da potência de fogo ou sensor da potência de fogo, você pode determinar os exemplos do snort usando o modo de especialista e o comando **top** baseado 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.

Troubleshooting

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