如何确定由特定Snort实例处理的流量

目录

简介

本文档介绍如何确定由特定snort实例处理的流量。在排除特定snort实例上的高CPU利用率故障时，此详细信息非常有用。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower管理中心6.X及更高版本
- 适用于包括Firepower威胁防御、Firepower模块和Firepower传感器的所有受管设备

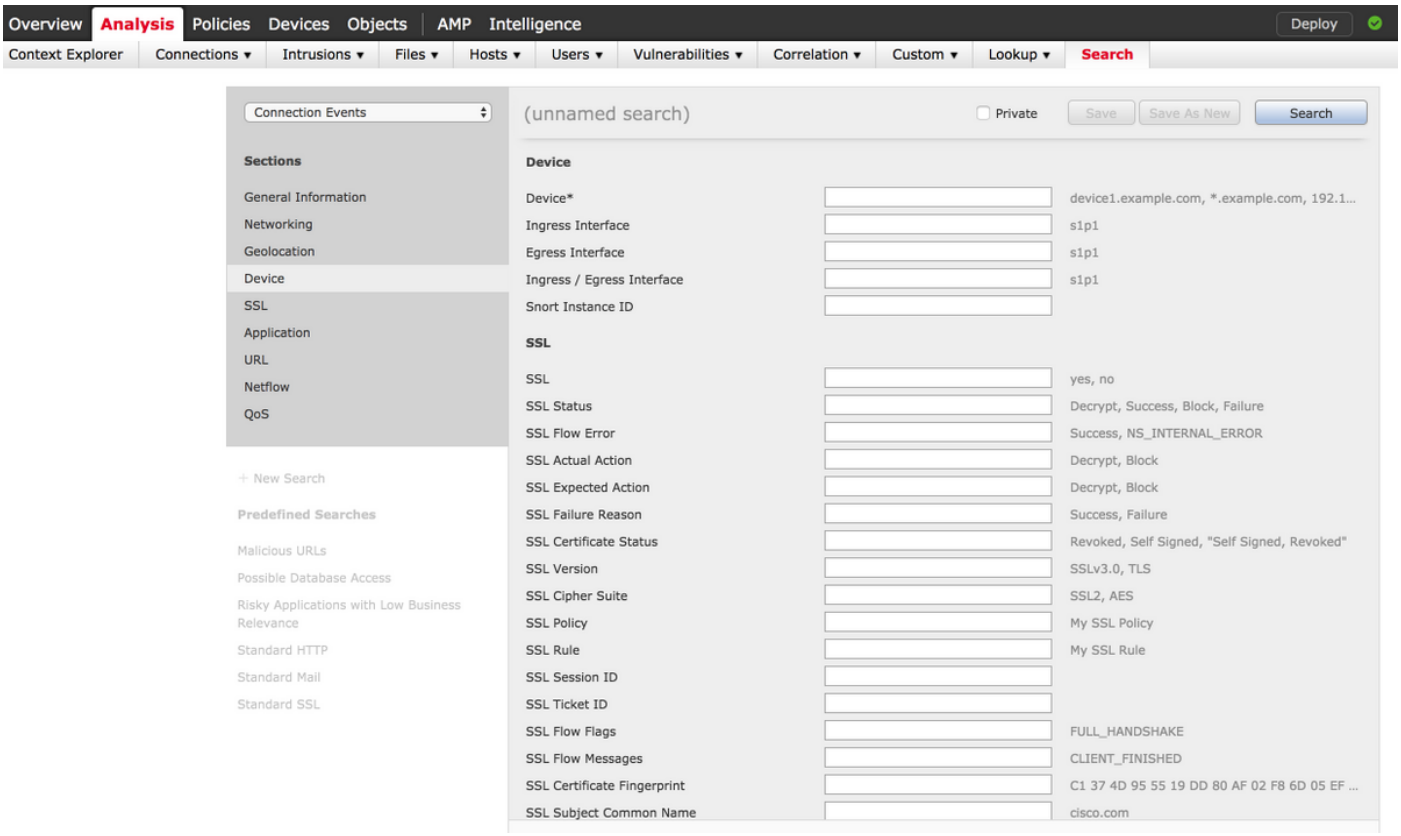
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

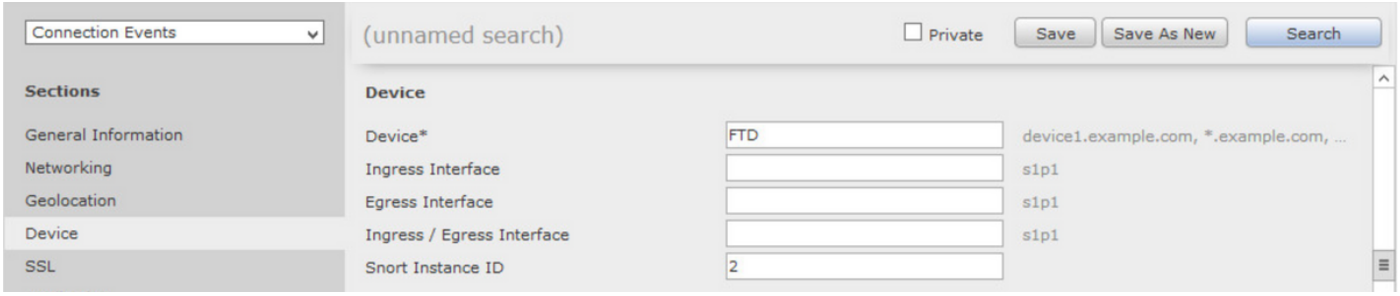
配置

使用管理权限登录Firepower管理中心。

登录成功后，导航至**Analysis > Search**，如图所示：



确保从下**拉列**表中选择“连接事件”表，然后从部分**中**选择“设备”。输入Device字段和Snort实例ID的值（0到N，Snort实例数取决于受管设备），如图所示：



输入值后，单击**Search**，结果将是特定snort实例触发的连接事件。

注意：如果受管设备是Firepower威胁防御，则可以使用FTD CLISH模式确定Snort实例。

```
> 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
```

注意：如果受管设备是Firepower模块或Firepower传感器，则可以使用专家模式和基于Linux的顶部命令确定Snort实例。

```
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
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。