Как определить трафик, с рукояткой определенным экземпляром фырканья

Содержание

Введение

Этот документ описывает, как определить трафик, который обрабатывается определенным экземпляром фырканья. Эта подробность очень полезна при устранении проблем высокой загрузки ЦП на определенном экземпляре фырканья.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание технологии огневой мощи

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Центр управления огневой мощи 6. X и выше
- Применимый ко всем управляемым устройствам, которые включают Защиту Угрозы Огневой мощи, Модули Огневой мощи и Датчики Огневой мощи

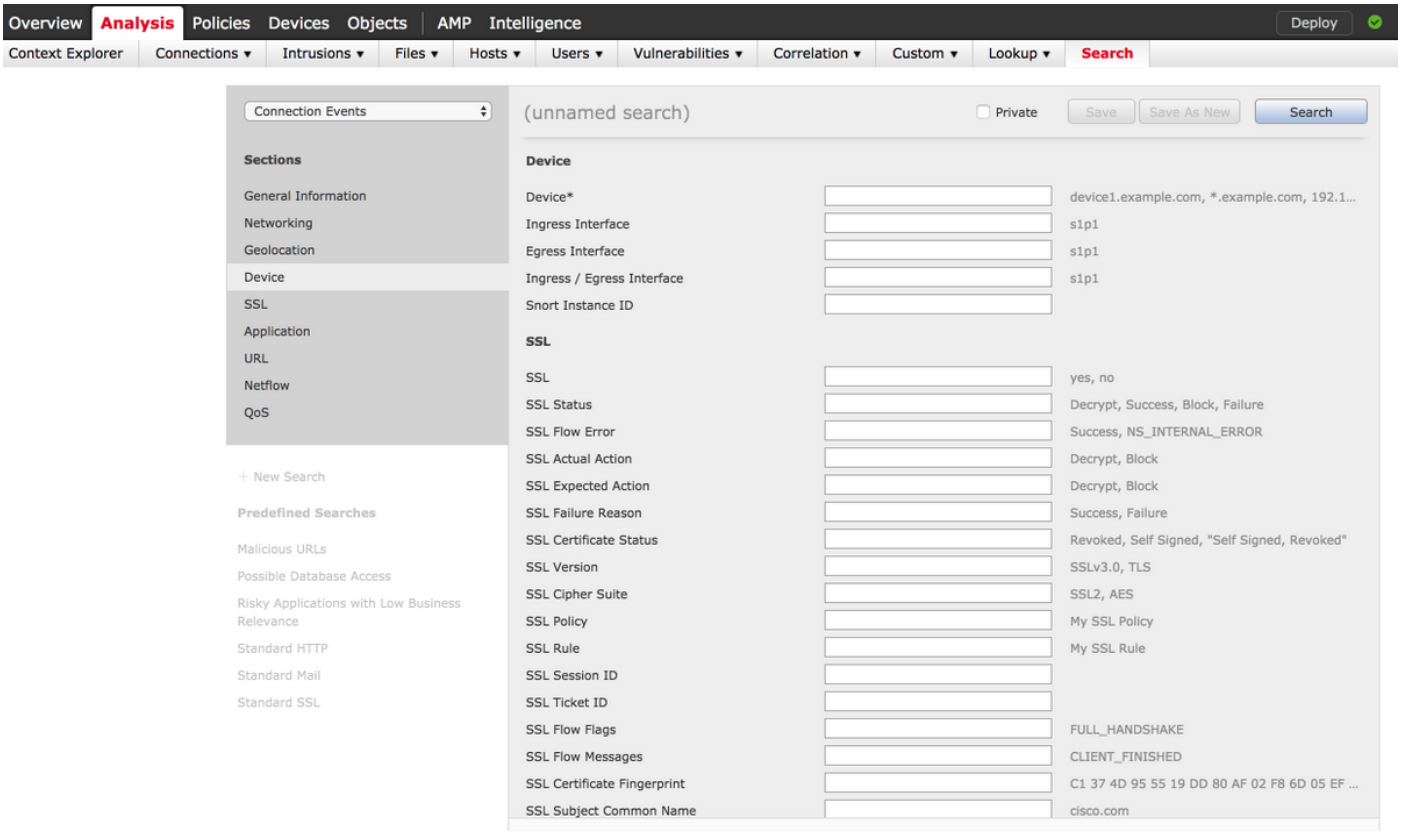
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

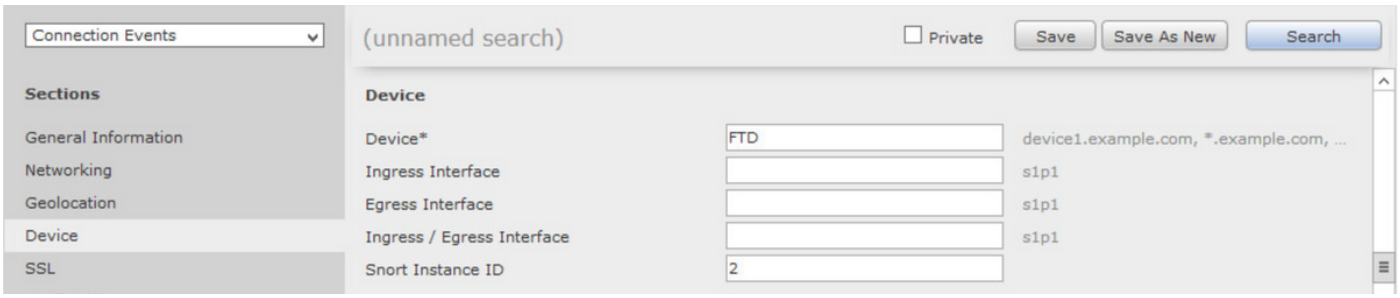
Конфигурации

Вход в систему к Центру управления Огневой мощи с полномочиями администрирования.

Как только вход в систему успешен, перейдите к **Анализу> Поиск,** как показано в образе:



Гарантируйте, что таблица **Событий подключения** выбрана из выпадающего , и затем выберите **Device** от раздела. Введите значения для ID Экземпляра Поля устройства и Фырканья (0 к N, количество экземпляров фырканья зависят от управляемого устройства), как показано в образе:



Как только значения введены, нажимают **Search**, и результатом были бы события подключения, которые инициированы определенным экземпляром фырканья.

Примечание: Если управляемое устройство является Защитой Угрозы Огневой мощи, можно определить экземпляры фырканья с помощью FTD CLISH режим.

```
> 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
```

Примечание: Если управляемое устройство является Датчиком Модуля или Огневой мощи Огневой мощи, можно определить экземпляры фырканья с помощью экспертного режима, и Linux базировал **главную** команду.

```
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
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.