Festlegen des Datenverkehrs, der von einer bestimmten Snort-Instanz verarbeitet wird

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Datenverkehr, der von einer bestimmten Snort-Instanz verarbeitet wird, bestimmt wird. Dieses Detail ist bei der Fehlerbehebung für eine hohe CPU-Auslastung einer bestimmten Snort-Instanz sehr nützlich.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der FirePOWER-Technologie

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Firepower Management Center 6.X und höher
- Gilt für alle verwalteten Geräte, darunter FirePOWER Threat Defense, FirePOWER-Module und FirePOWER-Sensoren

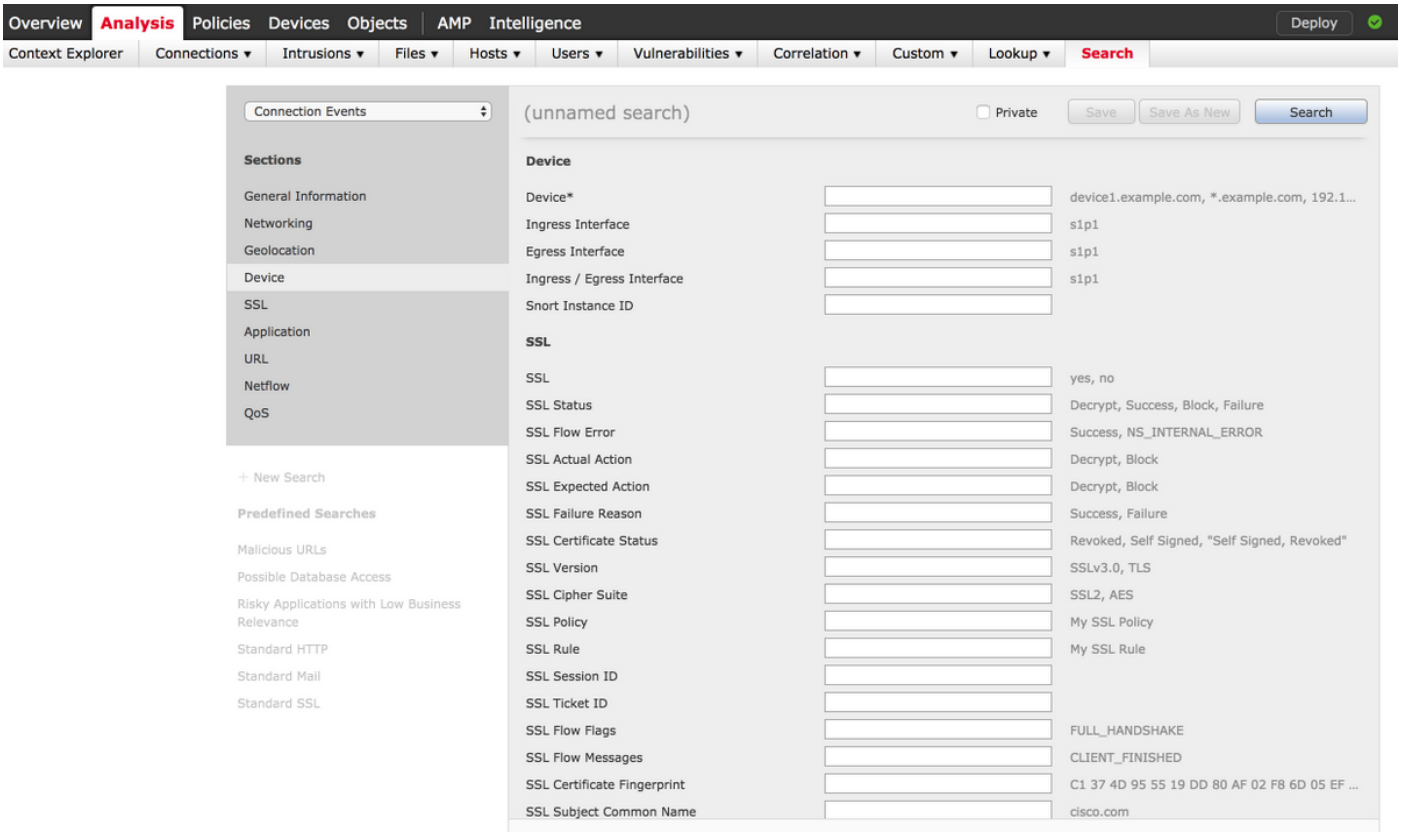
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

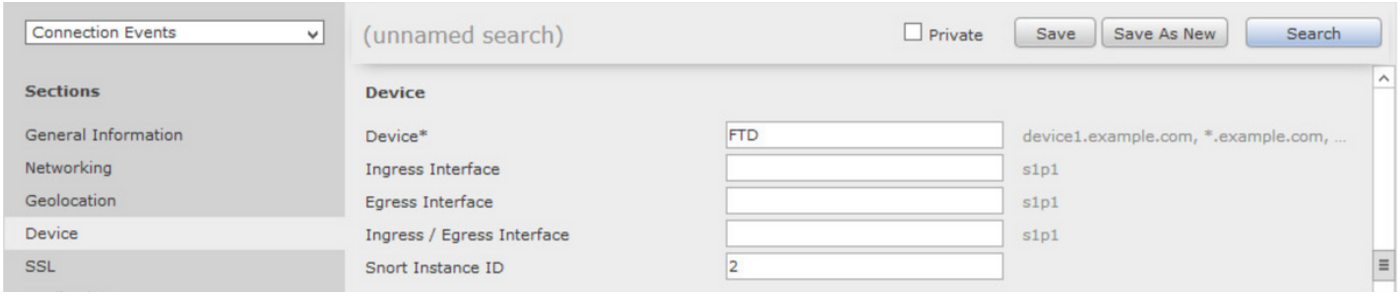
Konfigurationen

Melden Sie sich mit Administratorrechten beim FirePOWER Management Center an.

Wenn die Anmeldung erfolgreich war, navigieren Sie zu **Analysis > Search (Analyse > Suchen)**, wie im Bild gezeigt:



Stellen Sie sicher, dass die Tabelle **Connection Events** (Verbindungsereignisse) aus dem Dropdown-Menü ausgewählt wird, und wählen Sie dann das **Gerät** aus dem Abschnitt aus. Geben Sie Werte für das Device-Feld und die Snort Instance-ID (0 bis N, die Anzahl der Snort-Instanzen hängt vom verwalteten Gerät ab) ein, wie im Bild gezeigt:



Sobald die Werte eingegeben sind, klicken Sie auf **Suchen**, und das Ergebnis sind Verbindungsereignisse, die von der jeweiligen Snort-Instanz ausgelöst werden.

Hinweis: Wenn es sich bei dem verwalteten Gerät um FirePOWER Threat Defense handelt, können Sie die Snort-Instanzen im FTD CLISH-Modus bestimmen.

```
> 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
```

Hinweis: Wenn es sich bei dem verwalteten Gerät um das FirePOWER-Modul oder den FirePOWER-Sensor handelt, können Sie die Snort-Instanzen mithilfe des Expertenmodus und des Linux-basierten **Top-**Befehls bestimmen.

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.