

Hoe kunt u verkeer definiëren dat door een specifieke instantie wordt verwerkt

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u het verkeer kunt bepalen dat door een bepaalde instantie wordt verwerkt. Dit detail is zeer nuttig bij het oplossen van een probleem met een hoog CPU-gebruik op een specifiek gekleurd voorbeeld.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van technologie voor vuurkracht

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center 6.X en hoger
- Van toepassing op alle beheerde apparaten die FireSIGHT Threat Defense, FirePOWER-modules en FirePOWER-sensoren bevatten

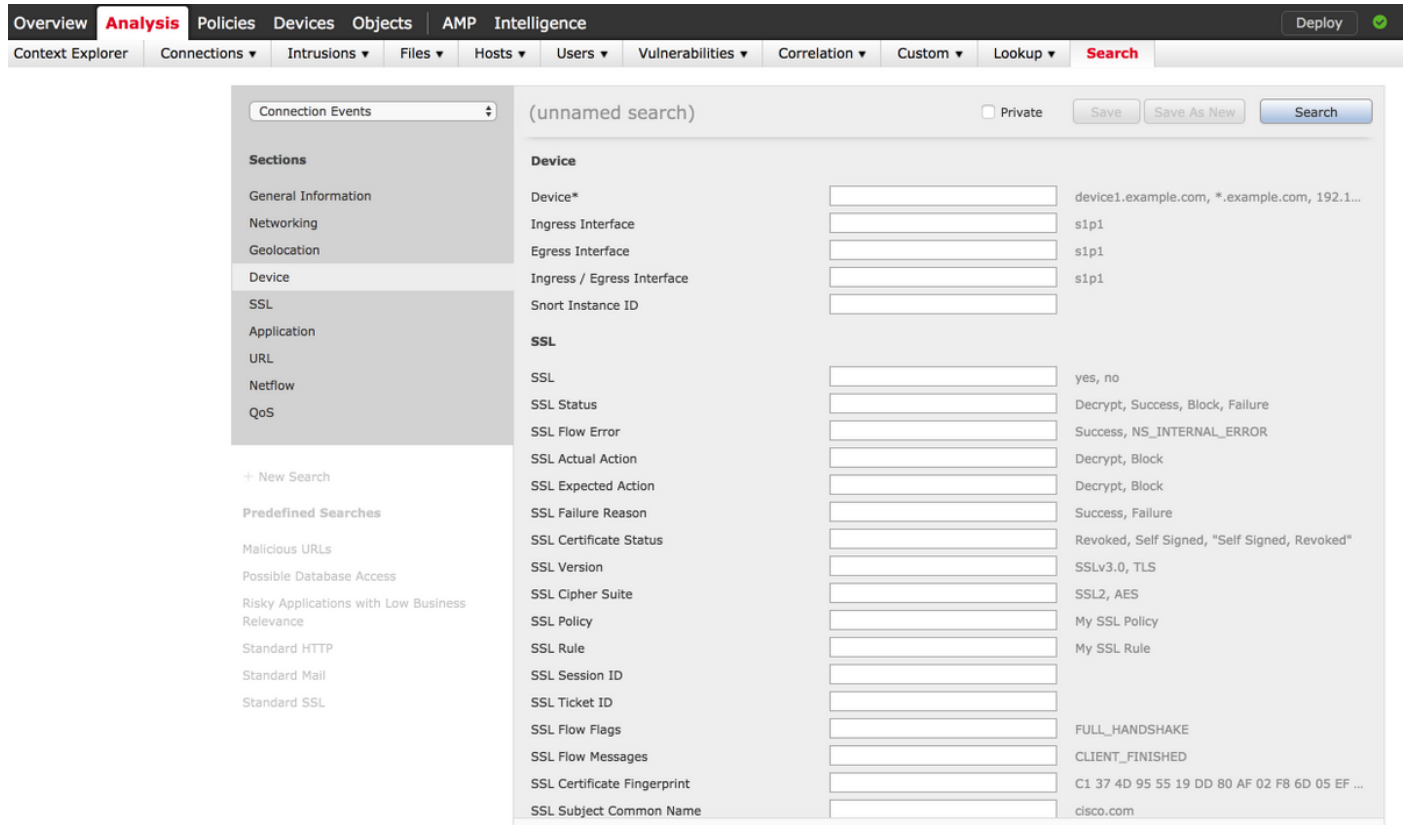
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

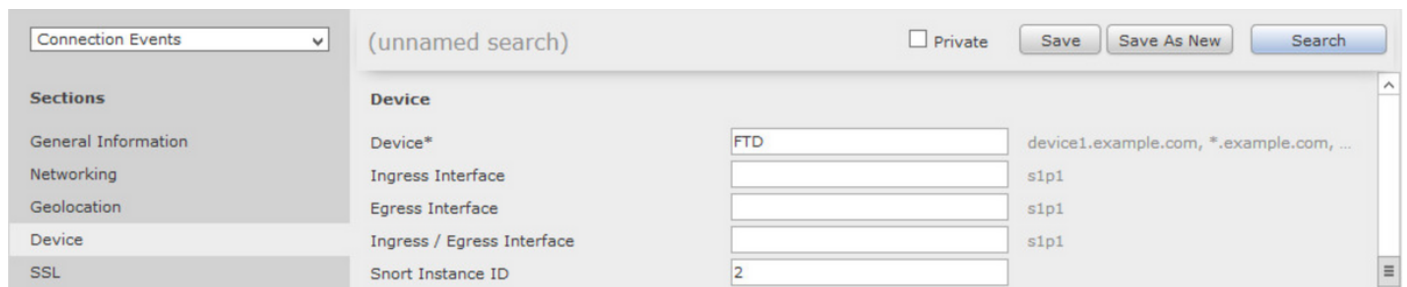
Configuraties

Aanmelden bij het FireSIGHT Management Center met beheerrechten.

Nadat de inlognaam is voltooid, navigeer dan naar **Analyse > Zoeken**, zoals in de afbeelding:



Zorg ervoor dat de tabel **met** verbindingsgebeurtenissen uit de vervolgkeuzelijst is geselecteerd en selecteer vervolgens het **apparaat** uit de sectie. Voer waarden in voor het veld Apparaat en Instantie-ID (0 tot N, het aantal gekleurde instanties is afhankelijk van het beheerde apparaat), zoals in de afbeelding:



Zodra de waarden zijn ingevoerd, klikt u op **Zoeken** en het resultaat is verbindingsgebeurtenissen die worden geactiveerd door de specifieke instantie.

Opmerking: Als het beheerde apparaat Firepower Threat Defense is, kunt u de gekleurde instanties bepalen met behulp van de FTD CLISH-modus.

```
> 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
```

Opmerking: Als het beheerde apparaat Firepower Module of Firepower Sensor is, kunt u de gekleurde instanties bepalen met behulp van de expertmodus en de Linux-gebaseerde **top** opdracht.

```
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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.