Comment déterminer le trafic traité par une particularité reniflez l'exemple

Contenu

Introduction

Ce document décrit comment déterminer le trafic qui est traité par une particularité reniflent l'exemple. Ce détail est très utile tandis que les dépannages de l'utilisation du CPU élevé sur une particularité reniflent l'exemple.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la technologie de FirePOWER

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre 6.X de Gestion de FirePOWER et en haut
- Applicable à tous les périphériques gérés qui incluent la défense contre des menaces de FirePOWER, les modules de FirePOWER, et les capteurs de FirePOWER

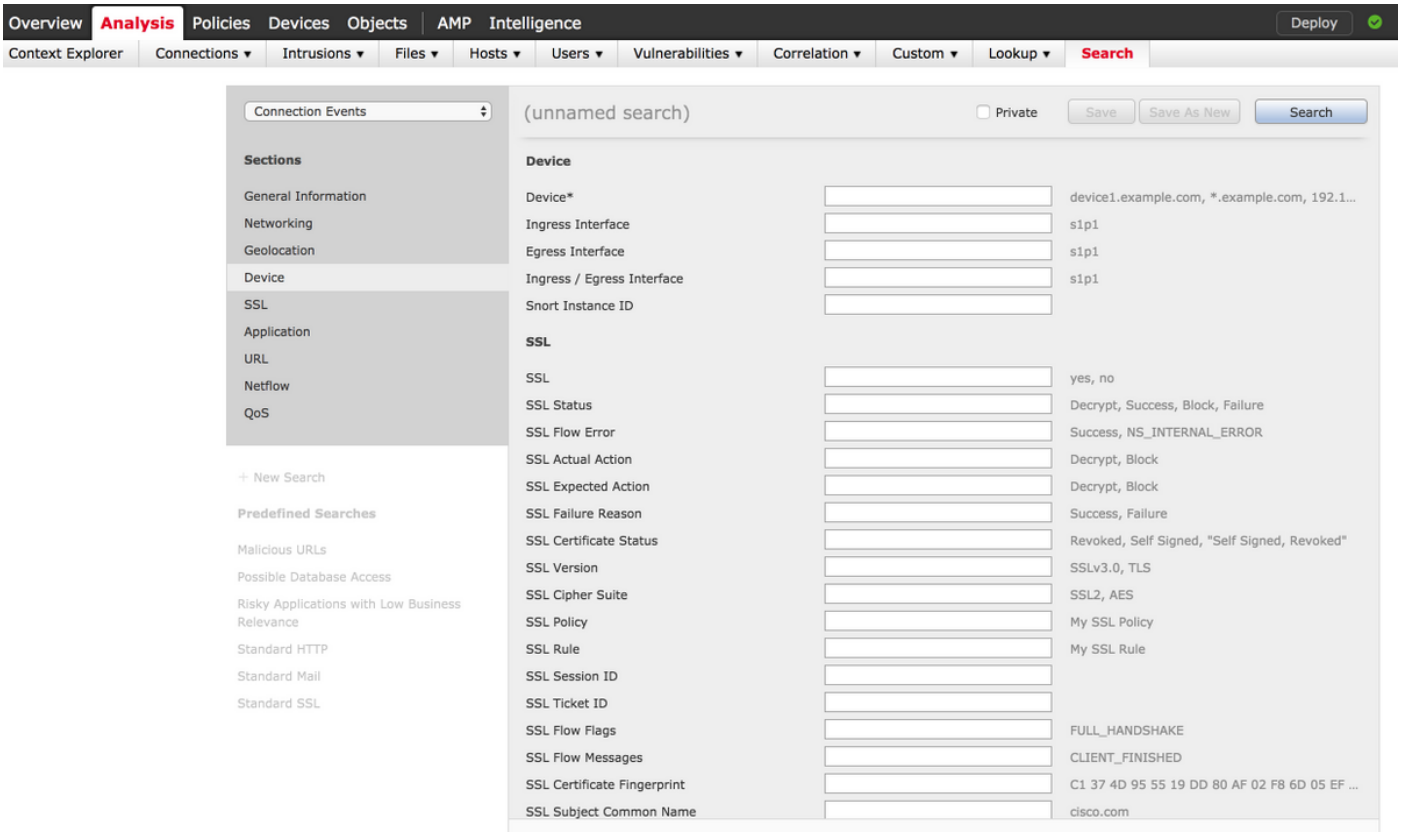
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

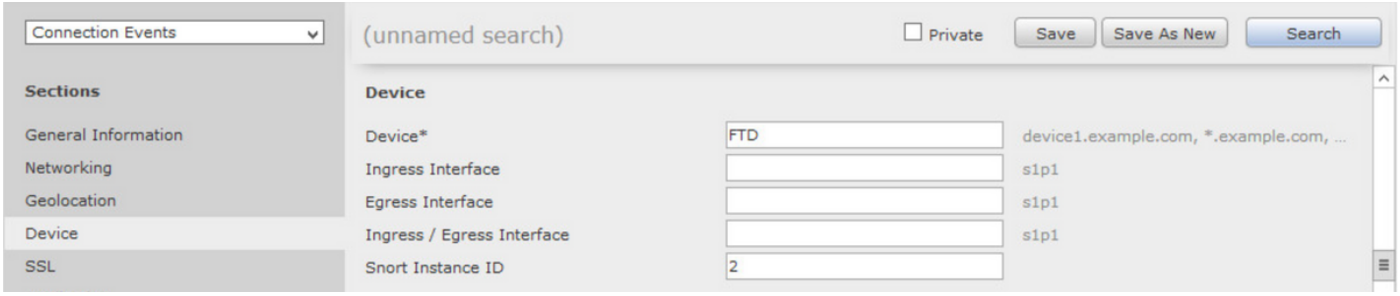
Configurations

Ouvrez une session au centre de Gestion de FirePOWER avec des privilèges de gestion.

Une fois que la procédure de connexion est réussie, naviguez vers l'**analyse > la recherche,** suivant les indications de l'image :



Assurez-vous que la table d'**événements de connexion** est choisie de la baisse vers le bas et sélectionne alors le **périphérique de la** section. Écrivez les valeurs pour le gisement de périphérique et reniflez l'ID d'exemple (0 à N, le nombre de reniflent des exemples dépendent du périphérique géré), suivant les indications de l'image :



Une fois que les valeurs sont écrites, la **recherche de** clic et le résultat seraient des événements de connexion qui sont déclenchés par la particularité reniflent l'exemple.

Note: Si le périphérique géré est défense contre des menaces de FirePOWER, vous pouvez déterminer les exemples de renifler utilisant le mode 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
```

Note: Si le périphérique géré est module de FirePOWER ou capteur de FirePOWER, vous pouvez déterminer les exemples de renifler utilisant le mode expert et la commande **supérieure** basée par 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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.