Comment déterminer le trafic traité par une instance Snort spécifique

Contenu

Introduction

Ce document décrit comment déterminer le trafic qui est traité par une instance de snort spécifique. Ce détail est très utile lors du dépannage d'une utilisation élevée du CPU sur une instance Snort spécifique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower

Components Used

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

- Firepower Management Center 6.X et versions ultérieures
- Applicable à tous les périphériques gérés, notamment Firepower Threat Defense, les modules Firepower et les capteurs Firepower

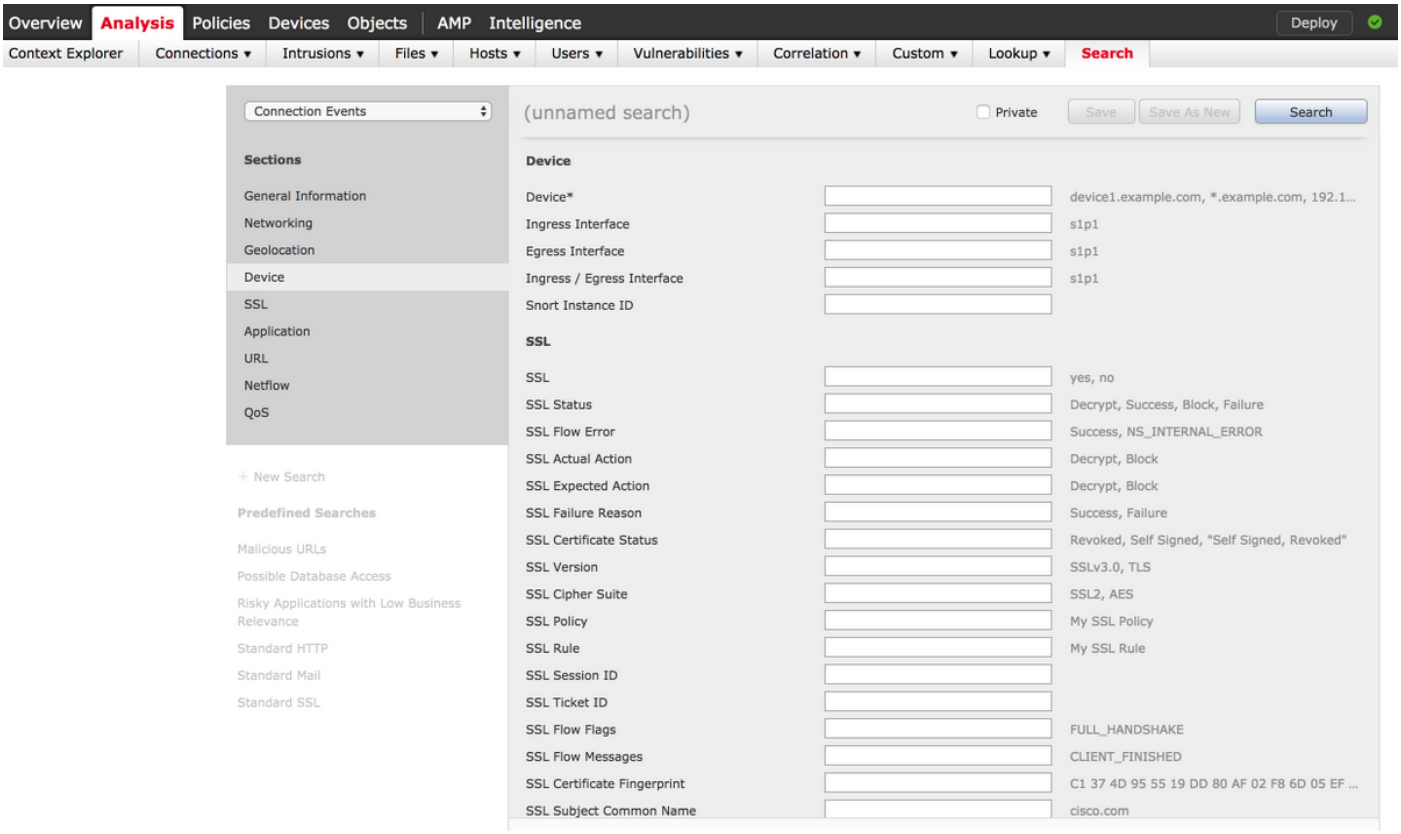
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

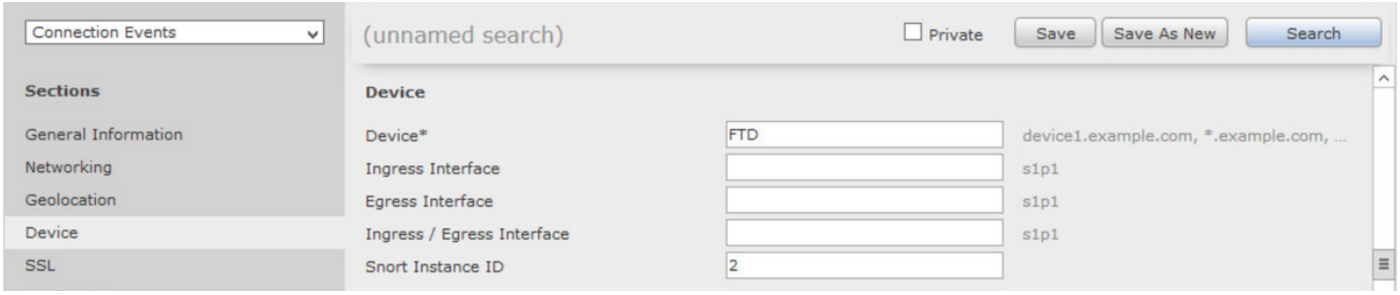
Configurations

Connectez-vous au Centre de gestion Firepower avec des privilèges d'administration.

Une fois la connexion établie, accédez à **Analysis > Search,** comme indiqué dans l'image :



Assurez-vous que le tableau **Événements de connexion** est sélectionné dans la liste déroulante, puis sélectionnez le **périphérique** dans la section. Saisissez les valeurs du champ Device et de l'ID d'instance Snort (0 à N, le nombre d'instances Snort dépend du périphérique géré), comme indiqué dans l'image :



Une fois les valeurs entrées, cliquez sur **Rechercher** et le résultat sera des événements de connexion déclenchés par l'instance de snort spécifique.

Note: Si le périphérique géré est Firepower Threat Defense, vous pouvez déterminer les instances de snort à l'aide du mode CLISH FTD.

```
> 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 Firepower Module ou Firepower Sensor, vous pouvez déterminer les instances de snort à l'aide de la commande **top** du mode expert et basée sur 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
```

Vérification

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

Dépannage

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