特定のSnortインスタンスによって処理されるトラフィックの判別方法

内容

概要

このドキュメントでは、特定のSnortインスタンスによって処理されるトラフィックを判別する方法について説明します。この詳細は、特定のSnortインスタンスでCPU使用率が高い場合のトラブルシューティングに非常に役立ちます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Center 6.X以降
- Firepower Threat Defense、Firepowerモジュール、およびFirepowerセンサーを含むすべての管理対象デバイスに適用可能

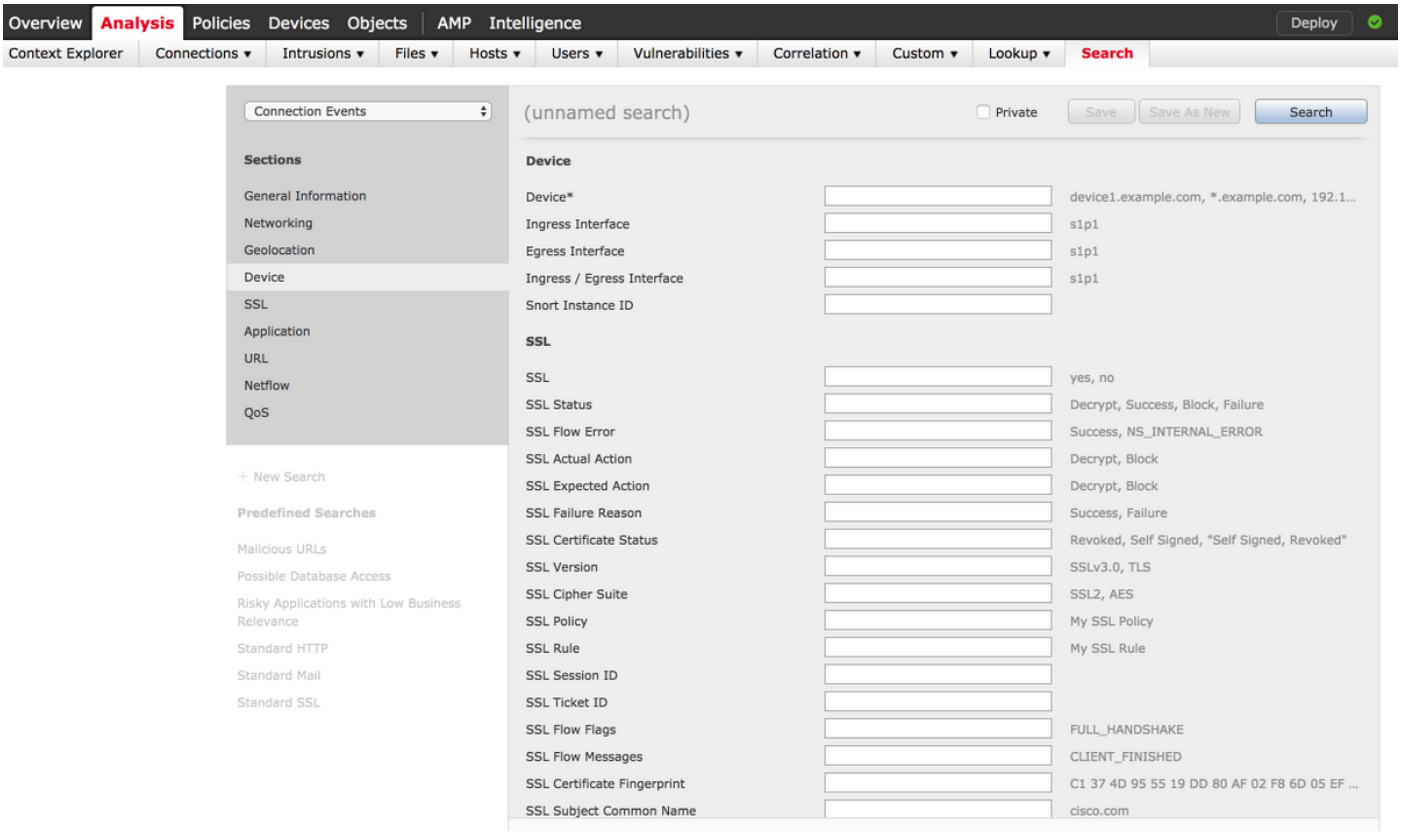
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

設定

管理者権限でFirepower Management Centerにログインします。

ログインが成功したら、図に示すように**[Analysis] > [Search]**に移動します。



ドロップダウンから**[Connection Events]**テーブルが選択されていることを確認し、セクションから**[Device]**を選択します。図に示すように、[Device]フィールドと[Snort Instance ID]（0 ~ N、Snortインスタンスの数は管理対象デバイスによって異なる）の値を入力します。

値を入力したら、**[Search]**をクリックします。その結果、特定のSnortインスタンスによってトリガーされる接続イベントが発生します。

注：管理対象デバイスがFirepower Threat Defense(FTD)の場合、FTD CLISHモードを使用してSnortインスタンスを判別できます。

```
> 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
```

注：管理対象デバイスがFirepowerモジュールまたはFirepowerセンサーの場合は、エキスパートモードとLinuxベースのtopコマンドを使用してSnortインスタンスを判別できます。

```
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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。