方法トラフィックを判別する特定の Snort 例によって処理しました

目次

概要

この資料に特定の snort 例によって処理されているトラフィックを判別する方法を記述されています。 この詳細は特定の snort 例の CPU使用率が高い状態をトラブルシューティング中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推奨されます。

- Firepower テクノロジーのナレッジ

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くものです。

- Firepower Management Center 6.X 以上に
- 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装置に適当

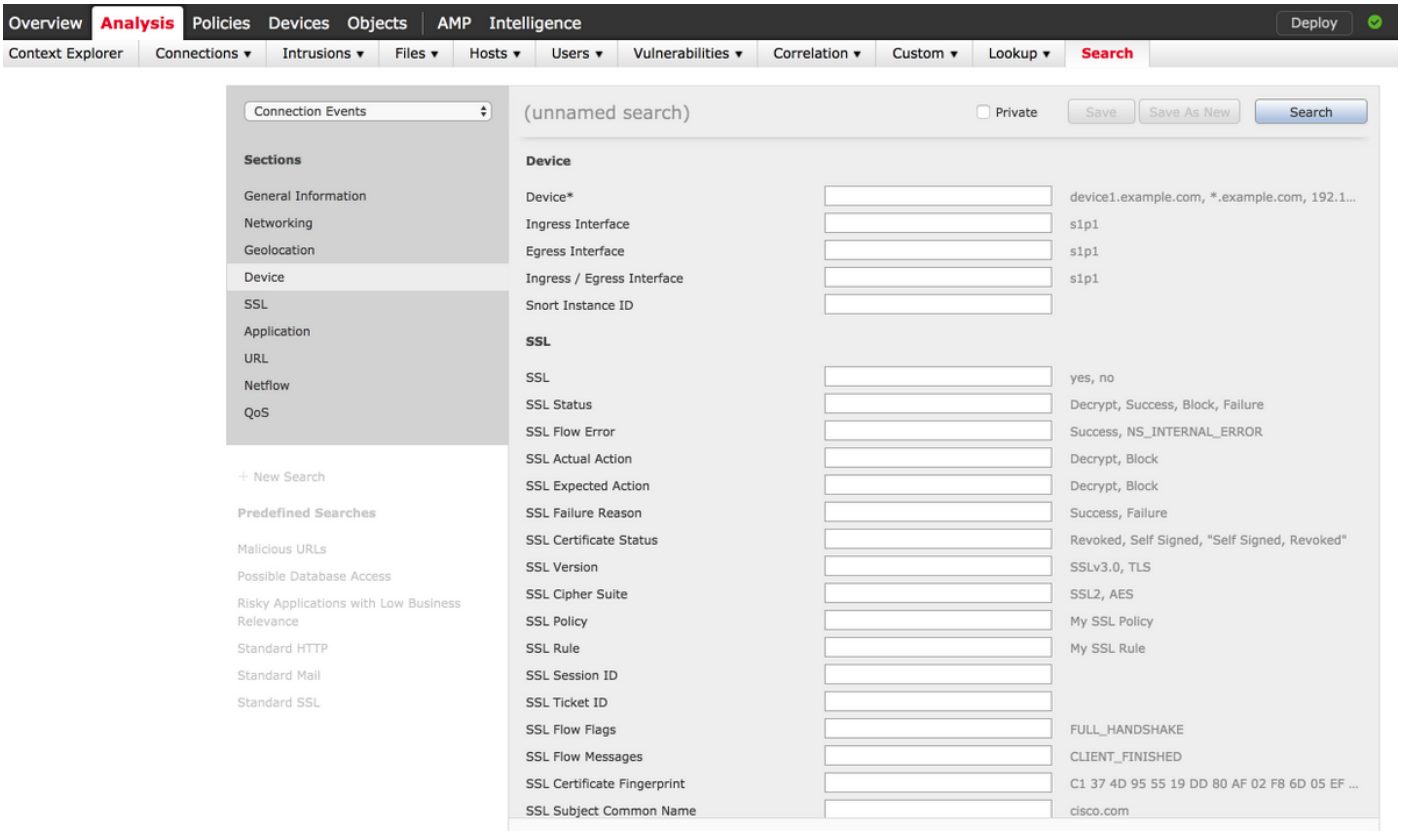
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

設定

管理特権の Firepower Management Center へのログオン。

ログオンが正常なら、**分析 >** イメージに示すように**検索**へのナビゲート、:



ようにそれからセクションから**デバイスを**選択しなさいことを表がドロップするから選択される**接続イベント**すれば。 Device フィールドの値を入力し、例 ID イメージに示すように (N への 0 は管理対象装置によって、snort 例の数決まります) 、鼻を鳴らして下さい:

値が入ったら、『Search』 をクリック すれば結果は特定の snort 例によって引き起こされる 接続イベントです。

注: 管理対象装置が Firepower Threat Defense である場合、FTD CLISH モードを使用して snort 例を判別できます。

```
> 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: 管理対象装置が Firepower モジュールまたは Firepower センサーである場合、巧妙なモードおよび Linux によって基づく上コマンドを使用して snort 例を判別できます。

```
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。

トラブルシューティング

現在のところ、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。