Come determinare il traffico gestito da una specifica istanza di snort

Sommario

Introduzione

Questo documento descrive come determinare il traffico gestito da una specifica istanza di snort. Questo dettaglio è molto utile durante la risoluzione dei problemi di utilizzo elevato della CPU in una specifica istanza di snort.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della tecnologia Firepower

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Management Center 6.X e versioni successive
- Applicabile a tutti i dispositivi gestiti che includono Firepower Threat Defense, Firepower Module e Firepower Sensor

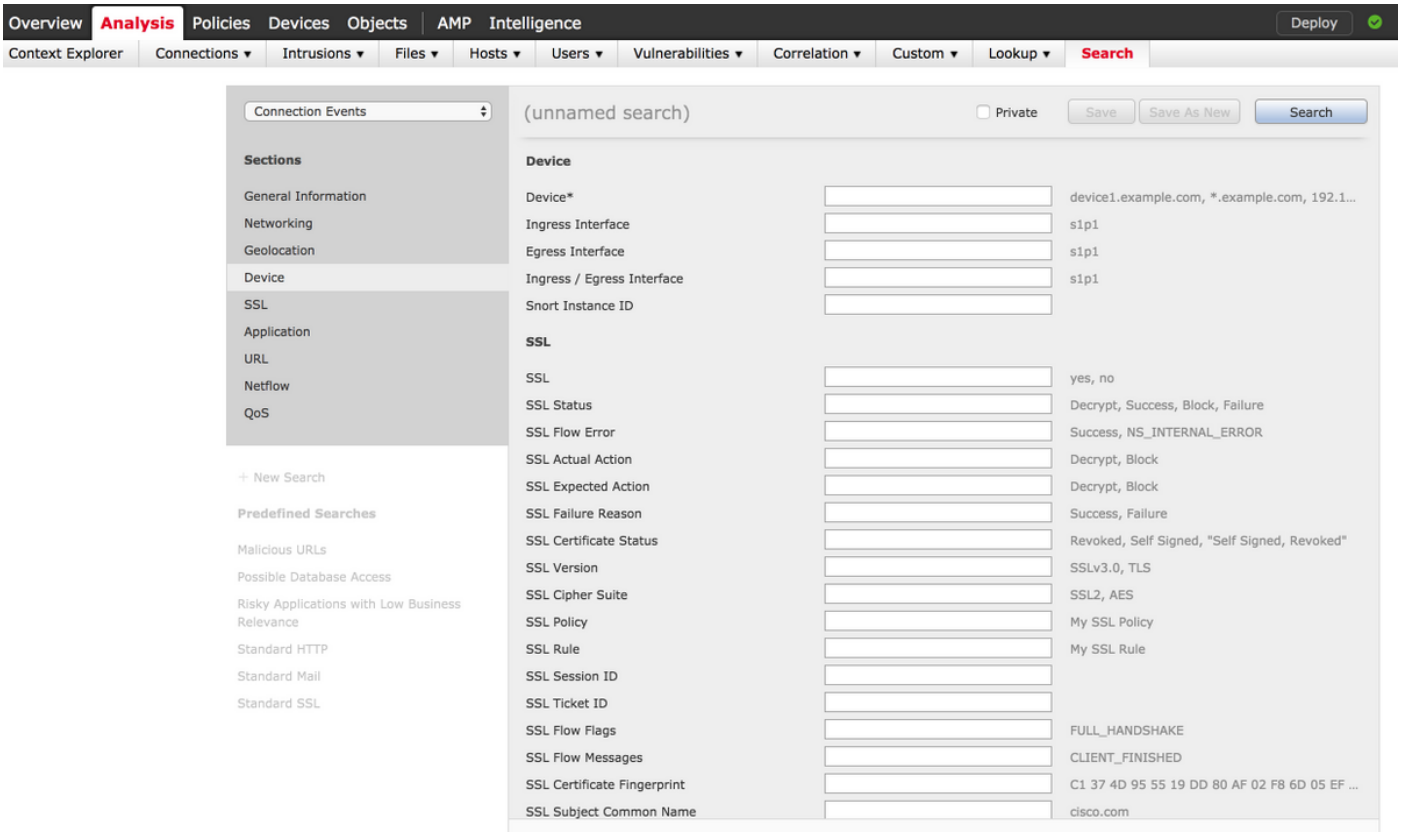
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

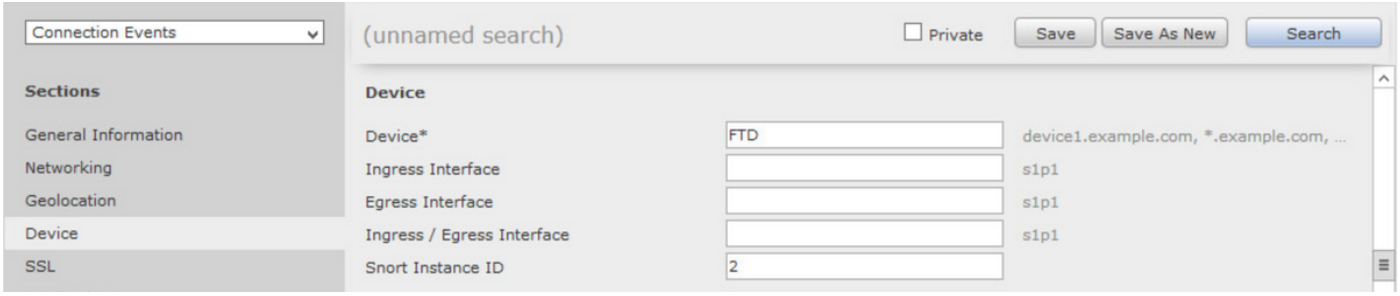
Configurazioni

Accedere a Firepower Management Center con privilegi di amministrazione.

Una volta eseguito correttamente il login, selezionare **Analisi > Ricerca,** come mostrato nell'immagine:



Verificare che la tabella **Eventi di connessione** sia selezionata dall'elenco a discesa, quindi selezionare la **periferica** dalla sezione. Immettere i valori per il campo Dispositivo e ID istanza snort (da 0 a N, il numero di istanze snort dipende dal dispositivo gestito), come mostrato nell'immagine:



Una volta immessi i valori, fare clic su **Search** per visualizzare gli eventi di connessione attivati dall'istanza snort specifica.

Nota: Se il dispositivo gestito è Firepower Threat Defense, è possibile determinare le istanze di snort utilizzando la modalità 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
```

Nota: Se il dispositivo gestito è il modulo Firepower o il sensore Firepower, è possibile determinare le istanze di snort utilizzando la modalità Expert e il comando **top** basato su 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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.