Instructies voor het indienen van regels voor FireSIGHT System

Inhoud

Inleiding

Als een FirePOWER-apparaat of NGIPS virtueel apparaat is overschreden, moet u extra gegevens verzamelen om te bepalen welke component van het apparaat het systeem vertraagt. Regelprofielen stellen een FireSIGHT-systeem in staat om verdere gegevens te genereren over welke regels en subsystemen van de detectiemachine de meeste CPU-cycli gebruiken. Dit artikel bevat de instructies voor het uitvoeren van regelprofielen van FireSIGHT-apparaat en NGIPS virtuele applicatie.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over FirePOWER-apparaat en de modellen van virtuele apparaten.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- FirePOWER 7000 Series-applicaties, 8000 Series applicaties en NGIPS virtuele applicaties
- Software, versie 5.2 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Waarschuwing: Het uitvoeren van regel profileren opdracht kan netwerkprestaties

beïnvloeden. Daarom dient u deze opdracht alleen uit te voeren als Cisco Technical Support om gegevens voor regelprofielen vraagt.

Stappen om regelprofielen uit te voeren

Stap 1: Toegang tot de CLI van het beheerde apparaat.

Stap 2: Start de volgende regel profileren opdracht voor een bepaalde tijd. De tijd moet tussen 15 en 120 minuten liggen. In het volgende voorbeeld, wordt het script 15 minuten uitgevoerd.

```
> system support run-rule-profiling 15
```

Stap 3: Bevestig de uitvoering van de opdracht. Typ **y** en druk op **ENTER**.

> **Waarschuwing**: De regel het profileren opdracht herstart de detectiemachine, die detectiefunctionaliteit kan beïnvloeden, en het gebruik van CPU's kan verhogen.

```
> system support run-rule-profiling 15

You are about to profile
 DE    Primary Detection Engine (94854a60-cb17-11e3-a2f5-8de07680f9f3)
 Time  15 minutes

WARNING!!  Detection Engine will be restarted.
Intrusion Detection / Prevention will be affected

Please confirm by entering 'y': y
```

Na het bevestigen van de executie, begint de regel profilering. De tijd om het profileren te voltooien telt terug tot nul minuten.

```
Restarting DE for profiling...done
Profiling for 15 more minutes...
```

Zodra de shell prompt is voltooid, komt hij terug.

```
Restarting DE for profiling...done
Profiling...done
Restarting DE with original configuration...in progress
>
```

Stap 4: De regel het profileren opdracht genereert een .tgz bestand. U kunt het bestand vinden door de volgende opdracht in de shell uit te voeren.

```
> system file list
May 12 15:53 99364308 profiling.94854a60-cb17-11e3-a2f5-8de07680f9f3.1399909945.tgz
```

Stap 5: Geef het bestand op aan Cisco Technical Support voor verdere analyse.