Istruzioni per la profilatura delle regole sul sistema FireSIGHT

Sommario

Introduzione

In caso di sottoscrizione eccessiva di un accessorio FirePOWER o di un dispositivo virtuale NGIPS, è necessario raccogliere alcuni dati aggiuntivi per determinare quale componente del dispositivo sta rallentando il sistema. La profilatura delle regole consente a un sistema FireSIGHT di generare ulteriori dati sulle regole e sui sottosistemi del motore di rilevamento che utilizzano la maggior parte dei cicli della CPU. In questo documento viene spiegato come eseguire la profilatura delle regole sull'appliance FireSIGHT e su NGIPS Virtual Appliance.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei modelli di appliance FirePOWER e virtuali.

Componenti usati

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

- Appliance FirePOWER serie 7000, appliance serie 8000 e NGIPS Virtual Appliance
- Software versione 5.2 o successive

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.

> **Avviso:** L'esecuzione del comando di profilatura delle regole può influire sulle prestazioni della rete. È pertanto consigliabile eseguire questo comando solo se il supporto tecnico

Cisco richiede i dati di profilatura delle regole.

Passi per eseguire la profilatura delle regole

Passaggio 1: Accedere alla CLI del dispositivo gestito.

Passaggio 2: Eseguire il seguente comando di profilatura delle regole per un determinato periodo di tempo. L'ora deve essere compresa tra 15 e 120 minuti. Nell'esempio seguente, lo script viene eseguito per 15 minuti.

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

Passaggio 3: Confermare l'esecuzione del comando. Digitare **y** e premere **Invio**.

> **Avviso:** Il comando di profilatura delle regole consente di riavviare il motore di rilevamento, con possibili effetti sulla funzionalità di rilevamento, e di aumentare l'utilizzo della CPU.

```
> 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
```

Dopo la conferma dell'esecuzione, inizia la profilatura della regola. Il tempo necessario per completare il profiling è di zero minuti.

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

Al termine, viene visualizzato il prompt della shell.

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

Passaggio 4: Il comando di profilatura delle regole genera un file .tgz. per trovare il file, eseguire il comando seguente nella shell.

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

Passaggio 5: Fornire il file al supporto tecnico Cisco per ulteriori analisi.