

Anweisungen zur Erstellung von Regelprofilen auf FireSIGHT-Systemen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Schritte zum Ausführen von Regelprofilen](#)

Einführung

Wenn eine FirePOWER-Appliance oder NGIPS Virtual Appliance überbelegt ist, müssen Sie einige zusätzliche Daten sammeln, um festzustellen, welche Komponente des Geräts das System verlangsamt. Die Erstellung von Regelprofilen ermöglicht es einem FireSIGHT-System, weitere Daten darüber zu generieren, welche Regeln und Subsysteme der Erkennungs-Engine die meisten CPU-Zyklen verwenden. Dieser Artikel enthält Anweisungen zum Ausführen der Erstellung von Regelprofilen auf der FireSIGHT-Appliance und der NGIPS Virtual Appliance.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der FirePOWER-Appliance und der virtuellen Appliance-Modelle verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Appliances der Serie FirePOWER 7000, Appliances der Serie 8000 und virtuelle NGIPS-Appliances
- Softwareversion 5.2 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Warnung: Die Ausführung eines Befehls zur Erstellung von Regelprofilen kann die Netzwerkleistung beeinträchtigen. Daher sollten Sie diesen Befehl nur ausführen, wenn der technische Support von Cisco Daten zur Erstellung von Regelprofilen anfordert.

Schritte zum Ausführen von Regelprofilen

Schritt 1: Zugreifen auf die CLI des verwalteten Geräts

Schritt 2: Führen Sie den folgenden Befehl zur Erstellung von Regelprofilen für eine bestimmte Zeit aus. Die Zeit muss zwischen 15 und 120 Minuten liegen. Im folgenden Beispiel wird das Skript 15 Minuten lang ausgeführt.

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

Schritt 3: Bestätigen Sie die Ausführung des Befehls. Geben Sie **y** ein, und drücken Sie die **Enter**-Taste.

Warnung: Der Befehl zur Erstellung von Regelprofilen startet die Erkennungs-Engine neu, was die Erkennungsfunktionalität beeinträchtigen und die CPU-Auslastung erhöhen kann.

```
> 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
```

Nach Bestätigung der Ausführung beginnt die Erstellung von Regelprofilen. Die Zeit für die Erstellung der Profilerstellung beträgt bis auf null Minuten.

```
Restarting DE for profiling...done
```

```
Profiling for 15 more minutes...
```

Wenn der Vorgang abgeschlossen ist, wird die Shell-Eingabeaufforderung wieder angezeigt.

```
Restarting DE for profiling...done
```

```
Profiling...done
```

```
Restarting DE with original configuration...in progress
```

```
>
```

Schritt 4: Der Befehl zur Erstellung von Regelprofilen generiert eine .tgz-Datei. Sie können die Datei finden, indem Sie den folgenden Befehl in der Shell ausführen.

```
> system file list
```

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

Schritt 5: Senden Sie die Datei zur weiteren Analyse an den technischen Support von Cisco.