FireSIGHT系統上的規則分析說明

目錄

簡介

如果FirePOWER裝置或NGIPS虛擬裝置超額訂閱，則需要收集一些其他資料以確定裝置的哪個元件正在降低系統速度。規則分析使FireSIGHT系統能夠生成檢測引擎的規則和子系統使用最多CPU週期的其他資料。本文提供有關如何在FireSIGHT裝置和NGIPS虛擬裝置上運行規則分析的說明。

必要條件

需求

思科建議您瞭解FirePOWER裝置和虛擬裝置型號。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- FirePOWER 7000系列裝置、8000系列裝置和NGIPS虛擬裝置
- 軟體版本5.2或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

> **警告**：運行規則分析命令可能會影響網路效能。因此，只有在思科技術支援請求規則分析資料時，才應運行此命令。

運行規則分析的步驟

第1步：訪問受管裝置的CLI。

第2步：在特定時間運行以下規則分析命令。時間必須介於15到120分鐘之間。在以下示例中，指令碼運行15分鐘。

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

步驟3:確認命令的執行。輸入**y**，然後按**Enter**。

警告： rule profiling命令重新啟動檢測引擎，這可能會影響檢測功能並增加CPU利用率。

```
> 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
```

確認執行後，規則分析開始。完成效能分析的時間將計為零分鐘。

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

完成後，Shell提示符會返回。

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

第4步：規則分析命令生成.tgz文件。您可以在外殼中運行以下命令來查詢檔案。

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

第5步：將檔案提供給思科技術支援以作進一步分析。