檢視Snort中的活動流

目錄

簡介

本文說明如何使用show snort flows命令檢視Snort中的活動流。

與此版本之前的版本相比

In Secure Firewall 7.4 and Below		New to Secure Firewall 7.6
• No way to look at active flows in Snort		• New CLI `show snort flows` can be used to view active flows in Snort

功能概述

- 新的CLI show snort flows用於檢視Snort 3流快取中的活動流。
- 其中提供了運行Snort 3進程時的活動流的詳細資訊。
- 輸出提供Snort流量的狀態、來源和目的地IP以及連線埠。
- 它有助於隔離和調試生產環境中的問題。

擾流器（突出顯示讀取）

附註：引入此功能是為了能夠檢視活動Snort流量和客戶端、伺服器流狀態、超時等。

附註：引入此功能是為了能夠檢視活動Snort流量和客戶端、伺服器流狀態、超時等。

最低軟體和硬體平台

Manager(s) and Version (s)	Application (FTD) and Minimum Version of Application	Supported Platforms
• (CLI only)	FTD 7.6.0	All platforms running FTD and Snort 3

Snort 3、IPv6、多例項和HA/群集支援

- 可同時與IPv4和IPv6配合使用。
- 要求Snort 3成為檢測引擎

FTD	
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes

支援的其他方面

Platforms	
FTD	
Licenses Required	Essentials
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

功能說明和演練

本節提供演練，包括流量逾時，以及有關更多功能的詳細資訊。

新建Show Snort Flows CLI

<#root>

```
> show snort flows
```

```
TCP 0: x1.x1.x1.2/38148 x1.x1.x1.1/22 pkts/bytes client 9/2323 server 6/2105 idle 7s, uptime 7s, timeout
ICMP 0: x1.x1.x1.2 type 8 x1.x1.x1.1 pkts/bytes client 1/98 server 1/98 idle 0s, uptime 0s, timeout 3m0
UDP 0: x1.x1.x1.1/40101 x1.x1.x1.1/12345 pkts/bytes client 3/141 server 0/0 idle 19s, uptime 58s, timeou
```

此範例顯示三個流量：TCP、ICMP和UDP。

對於TCP流，值如下：

- 通訊協定 — TCP/ICMP/UDP/IP
- 地址空間ID — 介面的VRF ID
- 源IP/埠：x1.x1.x1.2/38148
- 目的地IP/連線埠：x1.x1.x1.1/22
- 客戶端Pkts/bytes - 9/2323
- 伺服器Pkts/bytes - 6/2105
- Idle — 自流中最後一個資料包以來的時間
- Uptime — 自流設定以來的時間
- Timeout — 流超時
- 客戶端狀態（僅限TCP流） — EST
- 伺服器狀態（僅限TCP流） — EST

客戶端和伺服器流狀態

- 僅當協定是TCP時，輸出中才會顯示「客戶端狀態」和「伺服器狀態」。
- 以下是可能的值，以及每個縮寫詞對各狀態的含義：

State Acronym	Description
LST	Listen
SYS	SYN Sent
SYR	SYN received
EST	Established
MDS	Midstream Sent
MDR	Midstream Received
FW1	Final Wait 1
FW2	Final Wait 2
CLW	Close Wait
CLG	Closing
LAK	Last ACK
TWT	Time wait
CLD	Closed

篩選選項

show snort flows命令支援過濾選項，其中僅輸出與過濾器匹配的流。 語法是

show snort flows <filter option> <value>

過濾器選項包括：

- proto -TCP/UDP/IP/ICMP
- src_ip -按來源ip過濾流量
- dst_ip — 按目標ip過濾流
- src_port — 按源埠過濾流
- dst_port — 按目的地埠過濾流

> show snort flows proto TCP命令僅列出TCP流：

```
TCP 0: x1.x1.x1.2/45508 x1.x1.x1.1/22 pkts/bytes client 10/2389 server 7/2171 idle
30s, uptime 150s, timeout 59m30s state client CLW server FW2
```

擾流器（突出顯示讀取）

附註：您也可以在命令中使用多個過濾器。 例如，

show snort flows proto TCP src_ip x1.x1.x1.2 — 輸出具有src ip x1.x1.x1.2的TCP流

附註：您也可以在命令中使用多個過濾器。 例如， > show snort flows proto TCP src_ip x1.x1.x1.2 — 輸出具有src ip x1.x1.x1.2的TCP流

潛在錯誤響應

- CLI使用者可能收到「無法處理命令，請稍後再試」的回應。
- 例如，當Snort 3關閉、Snort 3繁忙或Snort 3未處理控制套接字命令（例如執行緒處於停滯狀態）時，就會發生這種情況。
- CLI成功運行的條件：
  - Snort 3正在運行。
  - Snort 3正在對UNIX域套接字上的控制命令做出響應。

停止CLI/輸出

- 與任何CLI命令一樣，您可以通過按CTRL +C獲得命令提示符，但該命令已傳遞給所有資料包執行緒，並且在Snort中運行至完成。
- 同時滿足以下兩個條件時，命令即完成：
  - 已檢視流快取中的所有流
  - 與CLI命令中的過濾器匹配的所有流都已寫入檔案，這些檔案用作命令在CLI中輸出的輸入。

效能影響

- 這是調試CLI。對於我們運行的每個資料包，我們會檢視來自流表的約100個流，並列印符合條件的流。
- 運行show snort flows會影響效能。

參考資料

常見問題

Q:我們是否可在「show snort flows」中使用多個過濾器

A:是，CLI支援一次提供多個過濾器，並輸出匹配兩個過濾器的流。

Q:支援哪些協定？

A:IP/TCP/UDP/ICMP

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。