Aktive Flows in Snort anzeigen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie mit dem Befehl show snort flows aktive Flows in Snort anzeigen.

Vergleich mit Vorgängerversion

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

Funktionsüberblick

- Die neue CLI zum Anzeigen von Snort-Flows wird zum Anzeigen der aktiven Flows im Snort 3-Flow-Cache verwendet.
- Hier finden Sie Details zu den aktiven Flows im laufenden Snort 3-Prozess.
- Die Ausgabe gibt den Status des Snort-Datenflusses, der Quell- und Ziel-IP-Adresse und des Ports an.

- Es hilft, Probleme in Produktionsumgebungen zu isolieren und zu beheben.

Spoiler (Zum Lesen markieren)

HINWEIS: Diese Funktion wurde eingeführt, um aktive Snort-Flows und Clients, Serverzustände des Flows, Timeouts und mehr zu untersuchen.

HINWEIS: Diese Funktion wurde eingeführt, um aktive Snort-Flows und Clients, Serverzustände des Flows, Timeouts und mehr zu untersuchen.

Software- und Hardware-Mindestanforderungen

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

Unterstützung von Snort 3, IPv6, Multi-Instance und HA/Clustering

- Kompatibel mit IPv4 und IPv6.
- Erfordert, dass Snort 3 die Erkennungs-Engine ist

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

Weitere Aspekte der Unterstützung

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

Funktionsbeschreibung und exemplarische Vorgehensweise

In diesem Abschnitt finden Sie eine exemplarische Vorgehensweise, einschließlich Ablauf-Timeout und Details zu weiteren Funktionen.

Neu 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, timeou
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, timeo
```

Dieses Beispiel zeigt drei Datenflüsse:TCP, ICMP und UDP.

Für den TCP-Fluss sind die Werte wie folgt:

- Protokoll - TCP/ICMP/UDP/IP
- Adressraum-ID - VRF-ID der Schnittstelle
- Quell-IP/Port: x1.x1.x1.2/38148
- Ziel-IP/Port: x1,x1,x1,1/22
- Client-Pakete/Byte - 23.09.2023
- Server-Pakete/Byte - 6/2015
- Inaktivität - Zeit seit dem letzten fließenden Paket
- Betriebszeit - Zeit seit Einrichtung des Ablaufs
- Timeout - Flow-Timeout
- Client-Status (nur TCP-Flows) - EST

- Serverstatus (nur TCP-Flows) - EST

Client- und Server-Flow-Status

- Der Client-Status und der Server-Status in der Ausgabe werden nur angezeigt, wenn das Protokoll TCP ist.
- Dies sind mögliche Werte und was jedes Akronym für jeden Zustand bedeutet:

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

Filteroptionen

Der Befehl show snort flows unterstützt Filteroptionen, bei denen nur die Flows ausgegeben werden, die mit den Filtern übereinstimmen. Die Syntax lautet

show snort flows <Filteroption> <Wert>

Die Filteroptionen sind:

- proto - TCP/UDP/IP/ICMP

- src_ip - Filtert Datenflüsse nach Quell-IP
- dst_ip - Filter-Flows nach Ziel-IP
- src_port - Filtert Datenflüsse nach Quellport
- dst_port - Filtert Datenflüsse nach Zielport

Der Befehl > show snort flows proto TCP listet nur TCP-Flows auf:

```
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
```

Spoiler (Zum Lesen markieren)

HINWEIS: können Sie auch mehr als einen Filter im Befehl verwenden. Beispiele,

> show snort flows proto TCP src_ip x1.x1.x1.2 - Ausgabe von TCP-Flows mit dem src ip x1.x1.x1.2

HINWEIS: können Sie auch mehr als einen Filter im Befehl verwenden. Beispiel: > show snort flows proto TCP src_ip x1.x1.x1.2 - Ausgabe von TCP-Flows mit dem src ip x1.x1.x1.2

Potenzielle Fehlerantwort

- CLI-Benutzer konnte die Antwort "Der Befehl kann nicht verarbeitet werden. Versuchen Sie es später erneut" erhalten.
- Dies geschieht beispielsweise, wenn Snort 3 ausgefallen ist, wenn Snort 3 ausgelastet ist oder wenn Snort 3 keine Control-Socket-Befehle verarbeitet (z. B. Threads im Steck-Zustand).
- Bedingungen für die erfolgreiche Ausführung der CLI:
  - Snort 3 wird ausgeführt.
  - Snort 3 reagiert auf Kontrollbefehle über den UNIX-Domänensockel.

Beenden der CLI/Ausgabe

- Wie bei allen CLI-Befehlen können Sie die Eingabeaufforderung durch Drücken von STRG + C aufrufen, aber der Befehl wurde bereits an alle Paket-Threads übergeben und wird in Snort vollständig ausgeführt.
- Der Befehl ist abgeschlossen, wenn beide Bedingungen zutreffen:
  - Alle Datenflüsse im Datenfluss-Cache wurden angezeigt
  - Alle Flows, die mit den Filtern im CLI-Befehl übereinstimmen, wurden in die Dateien geschrieben, die als Eingabe für den Befehl zur Ausgabe in der CLI dienen.

Leistungsbezogene Auswirkungen

- Dies ist eine Debug-CLI. Für jedes Paket, das wir durchlaufen, betrachten wir etwa 100 Flows aus der Flow-Tabelle und drucken die Flows aus, die den Kriterien entsprechen.
- Das Ausführen von show snort flows hat Auswirkungen auf die Leistung.

Referenzen

Häufig gestellte Fragen

F: Können bei "show snort flows" mehrere Filter verwendet werden?

A : Ja, die CLI unterstützt die gleichzeitige Bereitstellung von mehr als einem Filter und die Ausgabe von Flows, die mit beiden Filtern übereinstimmen.

F: Welche Protokolle werden unterstützt?

A : IP/TCP/UDP/ICMP

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.