View Active Flows in Snort

Contents

Introduction

Contrasting Previous to This Release

Feature Overview

Minimum Software and Hardware Platforms

Snort 3, IPv6, Multi-Instance and HA/Clustering Support

- Other Aspects of Support

Feature Description and Walkthrough

- New Show Snort Flows CLI
- Client and Server Flow States
- Filter Options
- Potential Error Response
- Stopping CLI/Output
- Performance Impact

References

- FAQs

Introduction

This document describes how to use the **show snort flows** command to view active flows in Snort.

Contrasting Previous to This Release

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

Feature Overview

- The new CLI show snort flows is used to view the active flows in the Snort 3 flow cache.
- This provides details of the active flows in running Snort 3 process.
- The output provides the state of the Snort flow, source and destination IP and port.
- It helps isolate and debug problems in production environments.

Spoiler (Highlight to read)

NOTE: This feature is introduced to have an ability to look at active Snort flows and client, server states of

flow, timeout, and more.

NOTE: This feature is introduced to have an ability to look at active Snort flows and client, server states of flow, timeout, and more.

Minimum Software and Hardware Platforms

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, Multi-Instance and HA/Clustering Support

- Works with both IPv4 and IPv6.
- Requires that Snort 3 be the detection engine

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

Other Aspects of Support

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

Feature Description and Walkthrough

This section provides a walkthrough, including flow timeout, and details about more features.

New 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
```

This example shows three flows:TCP, ICMP, and UDP.

For the TCP flow, the values are:

- Protocol - TCP/ICMP/UDP/IP
- Address Space Id - VRF id of the interface
- SourceIP / Port: x1.x1.x1.2/38148
- Destination IP/Port: x1.x1.x1.1/22
- Client Pkts/bytes - 9/2323
- Server Pkts/bytes - 6/2105
- Idle - Time since last packet in flow
- Uptime – Time since flow was set up
- Timeout – Flow timeout
- Client state (TCP flows only) - EST
- Server state (TCP flows only) - EST

Client and Server Flow States

- Client State and Server State in the output only appear if the protocol is TCP.
- These are possible values and what each acronym means, for each state:

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

Filter Options

The **show snort flows** command supports filtering options where only the flows which match the filters are output. The syntax is

show snort flows <filter option> <value>

The filter options are:

- **proto** -TCP/UDP/IP/ICMP
- **src_ip** - filter flows by source ip
- **dst_ip** - filter flows by destination ip
- **src_port** - filter flows by source port
- **dst_port** - filter flows by destination port

The > **show snort flows proto TCP** command only lists TCP flows:

```
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 (Highlight to read)

NOTE: you can also use more than one filter in the command. For example,

> **show snort flows proto TCP src_ip x1.x1.x1.2** – outputs TCP flows which have the src ip x1.x1.x1.2

NOTE: you can also use more than one filter in the command. For example, > show snort flows proto TCP src_ip x1.x1.x1.2 – outputs TCP flows which have the src ip x1.x1.x1.2

Potential Error Response

- CLI user could get a response **“unable to process the command, please try again later”**.
- This happens when, for example, Snort 3 is down, when Snort 3 is busy, or when Snort 3 is not processing control socket commands (such as threads in stuck state).
- Conditions for CLI to run successfully:
  - Snort 3 is running.
  - Snort 3 is responding to control commands over UNIX domain socket.

Stopping CLI/Output

- Like any CLI command, you can get the command prompt by pressing **CTRL +C** , but the command has already been passed to all packet threads and it runs to completion in Snort.
- The command completes when both conditions apply:
  - All flows in the flow cache have been viewed
  - All flows that match the filters in the CLI command have been written to the files which serve as input for the command to output in the CLI.

Performance Impact

- This is a debug CLI. For every packet we run through, we look at about 100 flows from the flow table and print the flows which match the criteria.
- Running **show snort flows** has a performance impact.

References

FAQs

Q: Can we use more than one filter in "show snort flows

A: Yes, The CLI supports providing more than one filter at a time and outputs flows matching both filters.

Q: What protocols are supported?

A: IP/TCP/UDP/ICMP