查看Snort中的活动流

目录

简介

本文档介绍如何使用show snort flows命令查看Snort中的活动流。

与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用于查看Snort 3流缓存中的活动流。
- 这提供了运行Snort 3进程的活动流的详细信息。
- 输出提供Snort流的状态、源IP和目标IP以及端口。
- 它有助于隔离和调试生产环境中的问题。

Spoiler（突出显示以便阅读）

NOTE:引入此功能是为了能够查看活动的Snort流量和客户端、流量的服务器状态、超时等。

NOTE:引入此功能是为了能够查看活动的Snort流量和客户端、流量的服务器状态、超时等。

最低软件和硬件平台

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、多实例和HA/群集支持

- 同时适用于IPv4和IPv6。
- 要求Snort 3作为检测引擎

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

支持的其他方面

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

功能说明和演练

本部分提供演练，包括流超时和有关更多功能的详细信息。

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, timeo
```

此示例显示了三个流：TCP、ICMP和UDP。

对于TCP流，值如下：

- 协议 — TCP/ICMP/UDP/IP
- 地址空间ID — 接口的VRF ID
- 源IP/端口：x1.x1.x1.2/38148
- 目的IP/端口：x1.x1.x1.1/22
- 客户端Pkts/bytes - 9/2323
- 服务器数据包/字节 — 6/2105
- 空闲 — 自流中最后一个数据包以来的时间
- Uptime — 设置流后的时间
- 超时 — 流超时
- 客户端状态（仅限TCP流量） — EST
- 服务器状态（仅限TCP流量） — EST

客户端和服务器流状态

- 仅当协议为TCP时，输出中才会显示Client State和Server State。
- 以下是可能的值以及每个缩写词对各状态的含义：

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

过滤器选项

show snort flows命令支持仅输出与过滤器匹配的流的过滤选项。 语法为

show snort flows <filter option> <value>

过滤器选项：

- proto -TCP/UDP/IP/ICMP
- src_ip -按源ip过滤流
- dst_ip — 按目标ip过滤流
- src_port — 按源端口过滤流量
- dst_port — 按目标端口过滤流量

> show snort flows proto TCP命令仅列出TCP流量：

```
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（突出显示以便阅读）

NOTE:还可以在命令中使用多个过滤器。 例如，

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

NOTE:还可以在命令中使用多个过滤器。 例如，> show snort flows proto TCP src_ip x1.x1.x1.2 — 输出具有src ip x1.x1.x1.2的TCP流

潜在错误响应

- CLI用户可能会收到“无法处理命令，请稍后重试”的响应。
- 例如，当Snort 3关闭、Snort 3繁忙或Snort 3未处理控制套接字命令（例如线程处于停滞状态）时，就会发生这种情况。
- CLI成功运行的条件：
  - Snort 3正在运行。
  - Snort 3正在对UNIX域套接字上的控制命令做出响应。

停止CLI/输出

- 与任何CLI命令一样，您可以通过按CTRL +C获得命令提示符，但该命令已传递到所有数据包线程，并在Snort中运行至完成。
- 当以下两种情况都适用时，命令完成：
  - 已查看流缓存中的所有流
  - 与CLI命令中的过滤器匹配的所有流已写入作为命令输入的文件中，以便在CLI中输出。

性能影响

- 这是调试CLI。对于我们通过的每个数据包，我们查看流表中的大约100个流，并打印符合条件的流。
- 运行show snort flows会对性能产生影响。

参考

常见问题解答

问:在“show snort flows”中是否可以使用多个过滤器

A：是，CLI支持一次提供多个过滤器，并输出匹配两个过滤器的流。

问:支持哪些协议？

A：IP/TCP/UDP/ICMP

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。