Ver flujos activos en Snort

Contenido

Introducción

Este documento describe cómo utilizar el comando show snort flows para ver los flujos activos en Snort.

Comparación con versiones anteriores a esta versión

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

Descripción general de características

- La nueva CLI show snort flows se utiliza para ver los flujos activos en la caché de flujos de Snort 3.
- Esto proporciona detalles de los flujos activos en la ejecución del proceso Snort 3.
- El resultado proporciona el estado del flujo de Snort, la IP de origen y destino y el puerto.
- Ayuda a aislar y depurar problemas en entornos de producción.

Deflector (Destaque para leer)

NOTE: Esta función se introduce para tener la capacidad de observar los flujos de Snort activos y el cliente, los estados de flujo del servidor, el tiempo de espera, etc.

NOTE: Esta función se introduce para tener la capacidad de observar los flujos de Snort activos y el cliente, los estados de flujo del servidor, el tiempo de espera, etc.

Plataformas mínimas de software y hardware

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

Compatibilidad con Snort 3, IPv6, varias instancias y HA/agrupación en clústeres

- Funciona con IPv4 e IPv6.
- Requiere que Snort 3 sea el motor de detección

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

Otros aspectos de la asistencia

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

Descripción de características y tutorial

En esta sección se proporciona un tutorial, que incluye el tiempo de espera del flujo, y detalles sobre más funciones.

Nuevo 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
```

Este ejemplo muestra tres flujos:TCP, ICMP y UDP.

Para el flujo TCP, los valores son:

- Protocolo: TCP/ICMP/UDP/IP
- ID del espacio de dirección: ID de VRF de la interfaz
- IP de origen/Puerto: x1.x1.x1.2/38148
- IP/puerto de destino: x1.x1.x1.1/22
- Paquetes/bytes de clientes: 9/2323
- Paquetes/bytes de servidor: 6/2015
- Inactivo - Tiempo desde el último paquete en flujo
- Tiempo de actividad: tiempo desde que se configuró el flujo
- Tiempo de espera - Tiempo de espera de flujo
- Estado del cliente (sólo flujos TCP): EST

- Estado del servidor (sólo flujos TCP): EST

Estados de flujo de cliente y servidor

- Client State (Estado del cliente) y Server State (Estado del servidor) en la salida sólo aparecen si el protocolo es TCP.
- Estos son valores posibles y lo que cada acrónimo significa, para cada estado:

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

Opciones de filtro

El comando show snort flows admite opciones de filtrado en las que sólo se generan los flujos que coinciden con los filtros. La sintaxis es la siguiente

show snort flows <filter option> <value>

Las opciones de filtro son:

- proto -TCP/UDP/IP/ICMP

- src_ip - filtrar flujos por ip de origen
- dst_ip - filtrar flujos por ip de destino
- src_port - filtrar flujos por puerto de origen
- dst_port - filtrar flujos por puerto de destino

El comando > show snort flows proto TCP sólo enumera los flujos TCP:

```
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
```

Deflector (Destaque para leer)

NOTE: también puede utilizar más de un filtro en el comando. Por ejemplo,

> show snort flows proto TCP src_ip x1.x1.x1.2 - salidas flujos TCP que tienen el src ip x1.x1.x1.2

NOTE: también puede utilizar más de un filtro en el comando. Por ejemplo, > show snort flows proto TCP src_ip x1.x1.x1.2 - output TCP flows which have the src ip x1.x1.x1.2

Posible respuesta de error

- El usuario de CLI pudo obtener una respuesta "no se puede procesar el comando, vuelva a intentarlo más tarde".
- Esto sucede cuando, por ejemplo, Snort 3 está inactivo, cuando Snort 3 está ocupado o cuando Snort 3 no está procesando comandos de socket de control (como subprocesos en estado bloqueado).
- Condiciones para que CLI se ejecute correctamente:
    - El Snort 3 se está ejecutando.
    - Snort 3 responde a los comandos de control sobre el socket de dominio UNIX.

Detención de CLI/salida

- Como cualquier comando CLI, puede obtener el símbolo del sistema presionando CTRL +C , pero el comando ya se ha pasado a todos los subprocesos de paquete y se ejecuta hasta su finalización en Snort.
- El comando se completa cuando se aplican ambas condiciones:
    - Se han visto todos los flujos de la caché de flujo
    - Todos los flujos que coinciden con los filtros del comando CLI se han escrito en los archivos que sirven como entrada para que el comando genere resultados en la CLI.

Impacto en el rendimiento

- Esta es una CLI de depuración. Por cada paquete que atravesamos, observamos unos 100 flujos de la tabla de flujo e imprimimos los flujos que coinciden con los criterios.
- La ejecución de show snort flows tiene un impacto en el rendimiento.

Referencias

Preguntas más Frecuentes

A: ¿Podemos utilizar más de un filtro en "show snort flows"?

R: Sí, la CLI admite el suministro de más de un filtro a la vez y genera flujos que coinciden con ambos filtros.

A: ¿Qué protocolos se admiten?

R: IP/TCP/UDP/ICMP

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).