Exibir Fluxos Ativos no Snort

Contents

Introdução

Este documento descreve como usar o comando show snort flows para visualizar fluxos ativos no Snort.

Comparando com anterior a esta versão

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

Visão geral do recurso

- O novo comando CLI show snort flows é usado para exibir os fluxos ativos no cache de fluxo do Snort 3.
- Isso fornece detalhes dos fluxos ativos na execução do processo do Snort 3.
- A saída fornece o estado do fluxo do Snort, o IP origem e destino e a porta.
- Ele ajuda a isolar e depurar problemas em ambientes de produção.

Spoiler (Realce para ler)

NOTE: Esse recurso é apresentado para ter a capacidade de observar os fluxos e o cliente do Snort ativos, os estados de fluxo do servidor, o tempo limite e muito mais.

NOTE: Esse recurso é apresentado para ter a capacidade de observar os fluxos e o cliente do Snort ativos, os estados de fluxo do servidor, o tempo limite e muito mais.

Plataformas mínimas de software e 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

Suporte a Snort 3, IPv6, várias instâncias e HA/clustering

- Funciona com IPv4 e IPv6.
- Requer que o Snort 3 seja o mecanismo de detecção

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

Outros aspectos do suporte

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

Descrição do recurso e passo a passo

Esta seção fornece um passo a passo, incluindo o tempo limite do fluxo e detalhes sobre mais recursos.

Novo CLI Show Snort Flows

<#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 exemplo mostra três fluxos:TCP, ICMP e UDP.

Para o fluxo TCP, os valores são:

- Protocolo - TCP/ICMP/UDP/IP
- ID do espaço de endereço - ID do VRF da interface
- IP/Porta de origem: x1.x1.x1.2/38148
- IP/Porta de Destino: x1.x1.x1.1/22
- Pacotes/bytes do cliente - 9/2323
- Pacotes/bytes de servidor - 6/2105
- Ocioso - Tempo desde o último pacote no fluxo
- Tempo de atividade - Tempo desde a configuração do fluxo
- Tempo limite - Tempo limite do fluxo
- Estado do cliente (somente fluxos TCP) - EST

- Estado do servidor (somente fluxos TCP) - EST

Estados de Fluxo do Cliente e do Servidor

- O estado do cliente e o estado do servidor na saída só aparecem se o protocolo for TCP.
- Estes são valores possíveis e o que cada acrônimo 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

Opções de filtro

O comando show snort flows suporta opções de filtragem em que apenas os fluxos correspondentes aos filtros são de saída. A sintaxe é

show snort flows <opção de filtro> <valor>

As opções de filtro são:

- proto -TCP/UDP/IP/ICMP
- src_ip - filtrar fluxos por ip de origem

- dst_ip - filtrar fluxos por ip de destino
- src_port - filtrar fluxos por porta de origem
- dst_port - filtrar fluxos por porta de destino

O comando > show snort flows proto TCP lista apenas os fluxos 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
```

Spoiler (Realce para ler)

NOTE: você também pode usar mais de um filtro no comando. Por exemplo,

> show snort flows proto TCP src_ip x1.x1.x1.2 - gera fluxos TCP que têm o src ip x1.x1.x1.2

NOTE: você também pode usar mais de um filtro no comando. Por exemplo, > show snort flows proto TCP src_ip x1.x1.x1.2 - gera fluxos TCP que têm o src ip x1.x1.x1.2

Possível Resposta a Erros

- O usuário CLI pode obter uma resposta "não é possível processar o comando, tente novamente mais tarde".
- Isso acontece quando, por exemplo, o Snort 3 está inoperante, quando o Snort 3 está ocupado ou quando o Snort 3 não está processando comandos de soquete de controle (como threads em estado de travamento).
- Condições para a execução bem-sucedida do CLI:
  - O Snort 3 está em execução.
  - O Snort 3 está respondendo aos comandos de controle sobre o soquete de domínio UNIX.

Parando CLI/Saída

- Como qualquer comando CLI, você pode obter o prompt de comando pressionando CTRL +C , mas o comando já foi passado para todos os threads de pacote e é executado até a conclusão no Snort.
- O comando é concluído quando ambas as condições se aplicam:
  - Todos os fluxos no cache de fluxo foram exibidos
  - Todos os fluxos que correspondem aos filtros no comando CLI foram gravados nos arquivos que servem como entrada para o comando exibir na CLI.

Impacto de desempenho

- Esta é uma CLI de depuração. Para cada pacote que executamos, observamos cerca de 100 fluxos da tabela de fluxo e imprimimos os fluxos que correspondem aos critérios.
- A execução de show snort flows tem um impacto no desempenho.

Referências

Perguntas freqüentes

P: Podemos usar mais de um filtro em "show snort flows

R: Sim, o CLI oferece suporte ao fornecimento de mais de um filtro por vez e gera fluxos de saída correspondentes a ambos os filtros.

P: Que protocolos são suportados?

R: IP/TCP/UDP/ICMP

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.