Snort의 활성 플로우 보기

목차

소개

이 문서에서는 show snort flows 명령을 사용하여 Snort의 활성 흐름을 보는 방법을 설명합니다.

이번 릴리스에 대한 이전 버전 대비

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

기능 개요

- 새로운 CLI show snort flow는 Snort 3 흐름 캐시에서 활성 흐름을 확인하는 데 사용됩니다.
- Snort 3 프로세스 실행의 활성 플로우에 대한 세부 정보를 제공합니다.
- 출력은 Snort 흐름의 상태, 소스 및 목적지 IP 및 포트를 제공합니다.
- 프로덕션 환경에서 문제를 격리하고 디버깅하는 데 도움이 됩니다.

스포일러 (읽으려면 강조 표시)

참고: 이 기능은 활성 Snort 흐름 및 클라이언트, 서버 흐름 상태, 시간 초과 등을 확인할 수 있도록 도입되었습니다.

참고: 이 기능은 활성 Snort 흐름 및 클라이언트, 서버 흐름 상태, 시간 초과 등을 확인할 수 있도록 도입되었습니다.

최소 소프트웨어 및 하드웨어 플랫폼

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, 다중 인스턴스 및 HA/클러스터링 지원

- IPv4 및 IPv6에서 모두 작동합니다.
- Snort 3이 탐지 엔진이어야 함

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

기타 지원 측면

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

기능 설명 및 연습

이 단원에서는 흐름 시간 제한을 비롯한 연습 및 추가 기능에 대한 세부 정보를 제공합니다.

새로운 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
```

이 예에서는 TCP, ICMP 및 UDP의 세 가지 플로우를 보여 줍니다.

TCP 흐름의 값은 다음과 같습니다.

- 프로토콜 - TCP/ICMP/UDP/IP
- 주소 공간 ID - 인터페이스의 VRF ID
- 소스 IP/포트: x1.x1.x1.2/38148
- 대상 IP/포트: x1.x1.x1.1/22
- 클라이언트 패킷/바이트 - 9/2323
- 서버 패킷/바이트 - 6/2105
- Idle(유휴) - 흐름의 마지막 패킷 이후 시간
- Uptime(가동 시간) - 플로우가 설정된 이후의 시간
- 시간 초과 - 흐름 시간 초과
- 클라이언트 상태(TCP 흐름만) - EST
- 서버 상태(TCP 흐름만) - EST

클라이언트 및 서버 플로우 상태

- Client State(클라이언트 상태) 및 Server State(서버 상태)는 프로토콜이 TCP인 경우에만 나타납니다.
- 각 상태에 대해 가능한 값 및 각 약어가 의미하는 것은 다음과 같습니다.

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

필터 옵션

show snort flows 명령은 필터와 일치하는 플로우만 출력되는 필터링 옵션을 지원합니다. 구문은 다음과 같습니다

show snort flows <filter option> <value>

필터 옵션은 다음과 같습니다.

- proto -TCP/UDP/IP/ICMP
- src_ip - 소스 ip로 플로우 필터링
- dst_ip - 목적지 ip로 플로우 필터링

- src_port - 소스 포트별로 흐름 필터링
- dst_port - 목적지 포트별 플로우 필터링

> show snort flows proto TCP 명령은 TCP 플로우만 나열합니다.

```
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
```

스포일러 (읽으려면 강조 표시)

참고: 명령에서 둘 이상의 필터를 사용할 수도 있습니다. 예를 들면 다음과 같습니다.

> show snort flows proto TCP src_ip x1.x1.x1.2 - src ip x1.x1.x1.2가 있는 TCP 플로우를 출력합니다.

참고: 명령에서 둘 이상의 필터를 사용할 수도 있습니다. 예를 들어 > show snort flows proto TCP src_ip x1.x1.x1.2 - src ip x1.x1.x1.2가 있는 TCP 플로우를 출력합니다

잠재적 오류 응답

- CLI 사용자가 "명령을 처리할 수 없습니다. 나중에 다시 시도하십시오."라는 응답을 받을 수 있습니다.
- 예를 들어, Snort 3이 다운되거나, Snort 3이 사용 중이거나, Snort 3이 제어 소켓 명령(예: 스레드 고정 상태)을 처리하지 않는 경우 이러한 현상이 발생합니다.
- CLI가 성공적으로 실행되기 위한 조건:
  - Snort 3이 실행되고 있습니다.
  - Snort 3은 UNIX 도메인 소켓에서 제어 명령에 응답합니다.

CLI/출력 중지

- 다른 CLI 명령과 마찬가지로 CTRL +C를 눌러 명령 프롬프트를 가져올 수 있지만 이 명령은 이미 모든 패킷 스레드에 전달되었으며 Snort에서 완료될 때까지 실행됩니다.
- 두 조건이 모두 적용되면 명령이 완료됩니다.
  - 플로우 캐시의 모든 플로우가 표시됨
  - CLI 명령의 필터와 일치하는 모든 플로우는 CLI에서 출력할 명령의 입력으로 사용되는 파일에 기록되었습니다.

성능에 미치는 영향

- 디버그 CLI입니다. 패킷을 실행할 때마다 플로우 테이블에서 약 100개의 플로우를 살펴보고 기준에 맞는 플로우를 인쇄합니다.
- show snort flow를 실행하면 성능에 영향을 줍니다.

참조

FAQ

Q: "show snort flows"에 두 개 이상의 필터를 사용할 수 있습니까?

A : 예. CLI는 한 번에 둘 이상의 필터를 제공하도록 지원하며 두 필터와 일치하는 플로우를 출력합니다.

Q: 어떤 프로토콜이 지원됩니까?

A : IP/TCP/UDP/ICMP

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.