firepower 디바이스에서 패킷 캡처 절차 사용

목차

소개

이 문서에서는 Firepower 디바이스의 네트워크 인터페이스에서 표시되는 패킷을 캡처하기 위해 tcpdump 명령을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco Firepower 디바이스 및 가상 디바이스 모델에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. BPF(Berkeley Packet Filter) 구문을 사용합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

경고: 프로덕션 시스템에서 tcpdump 명령을 실행하면 네트워크 성능에 영향을 줄 수 있습니다.

패킷 캡처 단계

firepower 디바이스의 CLI에 로그인합니다.

버전 6.1 이상에서 capture-traffic을 입력합니다. 예를 들면 다음과 같습니다.

<#root>

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

버전 6.0.x.x 및 이전 버전에서는 system support capture-traffic을 입력합니다. 예를 들면 다음과 같습니다.

<#root>

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

선택한 후에는 다음 옵션을 입력하라는 프롬프트가 표시됩니다.

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

패킷에서 충분한 데이터를 캡처하려면 -s 옵션을 사용하여 맞춤법을 올바르게 설정해야 합니다. Interface Set 컨피그레이션의 구성된 MTU(Maximum Transmission Unit) 값과 일치하는 값으로 맞춤을 설정할 수 있으며, 기본값은 1518입니다.

⚠ 경고: 화면으로 트래픽을 캡처하면 시스템 및 네트워크의 성능이 저하될 수 있습니다. tcpdump 명령에서 -w <filename> 옵션을 사용하는 것이 좋습니다. 패킷을 파일에 캡처합니다. -w 옵션 없이 명령을 실행할 경우 Ctrl-C 키 조합을 눌러 종료합니다.

-w <filename> 옵션 예:

<#root>

```
-w capture.pcap -s 1518
```

⚠ 주의: 패킷 캡처(pcap) 파일 이름을 지정할 때는 경로 요소를 사용하지 마십시오. 어플라이언스에서 생성할 pcap 파일 이름만 지정해야 합니다.

제한된 수의 패킷을 캡처하는 것이 좋으면 캡처할 패킷의 수를 지정하기 위해 -c <packets> 플래그를 사용할 수 있습니다. 예를 들어, 정확히 5000개의 패킷을 캡처하려면

<#root>

```
-w capture.pcap -s 1518 -c 5000
```

또한 캡처할 패킷을 제한하기 위해 명령의 끝에 BPF 필터를 추가할 수 있습니다. 예를 들어 소스 또는 목적지 IP 주소가 192.0.2.1인 패킷 5000개로 패킷 캡처를 제한하려면 다음 옵션을 사용할 수 있습니다.

<#root>

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

VLAN(Virtual LAN) 태그가 지정된 트래픽을 캡처할 경우 BPF 구문으로 VLAN을 지정해야 합니다. 그렇지 않으면 pcap에 VLAN 태그가 지정된 패킷이 포함되지 않습니다. 예를 들어 다음 예에서는 192.0.2.1에서 VLAN 태그가 지정된 트래픽으로 캡처를 제한합니다.

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

트래픽이 VLAN 태깅인지 확실하지 않은 경우 VLAN 태깅이 아닌 192.0.2.1에서 트래픽을 캡처하기 위해 다음 구문을 사용할 수 있습니다.

<#root>

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

참고: 앞의 예에서는 'or'가 'vlan'에만 적용되지 않도록 괄호가 필요합니다. 그런 다음 셸에 의해 괄호가 잘못 해석되는 것을 방지하기 위해 작은 따옴표가 필요합니다.

VLAN 태그 지정은 나머지 BPF와 일치하는 모든 VLAN 트래픽을 캡처합니다. 그러나 특정 VLAN 태그를 캡처하려는 경우 다음과 같이 캡처할 VLAN 태그를 지정할 수 있습니다.

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

원하는 옵션을 지정하고 Enter 키를 누르면 tcpdump가 트래픽 캡처를 시작합니다.

 팁: -c 옵션을 사용하지 않은 경우 캡처를 중지하려면 Ctrl-C 키 조합을 누릅니다.

캡처를 중지하면 확인 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

<#root>

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

-w capture.pcap -s 1518 -c 5000 host 192.0.2.1

```
Cleaning up.
Done.
```

Pcap 파일 복사

firepower 어플라이언스에서 인바운드 SSH 연결을 수락하는 다른 시스템으로 pcap 파일을 복사하려면 다음 명령을 사용합니다.

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Enter를 누르면 원격 시스템에 대한 비밀번호를 입력하라는 프롬프트가 표시됩니다. 네트워크 전체에서 파일을 복사할 수 있습니다.

 참고: 이 예에서 호스트 이름은 대상 원격 호스트의 이름 또는 IP 주소를 참조하고, 사용자 이름은 원격 호스트의 사용자 이름을 지정하며, destination_directory는 원격 호스트의 대상 경로를 지정하고, pcap_file은 전송할 로컬 pcap 파일을 지정합니다.

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.