Cisco Firepower 디바이스의 패킷 캡처 절차

목차

소개

이 문서에서는 **tcpdump** 명령을 사용하여 Firepower 디바이스의 네트워크 인터페이스에서 보이는 패킷을 캡처하는 방법에 대해 설명합니다.BPF(Berkeley Packet Filter) 구문을 사용합니다.

사전 요구 사항

요구 사항

Cisco는 Cisco Firepower 디바이스 및 가상 디바이스 모델에 대한 지식을 보유하고 있는 것을 권장합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

> **경고:**프로덕션 시스템**에서 tcpdump** 명령을 실행하면 네트워크 성능에 영향을 미칠 수 있습니다.

패킷 캡처 단계

Firepower 디바이스의 CLI에 로그인합니다.

버전 6.1 이상에서는 **capture-traffic을 입력합니다**.예를 들어

```
> capture-traffic

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

버전 6.0.x.x 이하 버전에서는 **system support capture-traffic을 입력합니다**.예를 들어

```
> system support capture-traffic

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

선택 후 다음 옵션을 묻는 메시지가 표시됩니다.

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

패킷에서 충분한 데이터를 캡처하려면 snaplength를 올바르게 설정하려면 -s 옵션을 사용해야 합니다.snaplength는 Interface Set 컨피그레이션의 구성된 MTU(Maximum Transmission Unit) 값과 일치하는 값으로 설정해야 합니다. 기본값은 1518입니다.

> **경고:**화면으로 트래픽을 캡처하면 시스템 및 네트워크의 성능이 저하될 수 있으므로 tcpdump 명령과 함께 -w <filename> 옵션을 사용하는 것이 좋습니다.파일을 캡처합니다.-w 옵션 없이 명령을 실행하는 경우 종료하려면 **Ctrl-C** 키 조합을 누릅니다.

-w <filename> 옵션 예:

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

> **주의:**pcap(packet capture) 파일 이름을 지정할 때 경로 요소를 사용하지 마십시오.어플라이언스에서 생성할 pcap 파일 이름만 지정해야 합니다.

제한된 수의 패킷을 캡처해야 하는 경우 캡처할 패킷 수를 지정하기 위해 -c <packets> 플래그를 사용할 수 있습니다.예를 들어 정확히 5000개의 패킷을 캡처하려면

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

또한 BPF 필터를 명령 끝에 추가하여 캡처되는 패킷을 제한할 수 있습니다.예를 들어, 소스 또는 목적지 IP 주소가 192.0.2.1인 패킷 캡처를 5,000개의 패킷으로 제한하려면 다음 옵션을 사용할 수 있습니다.

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

VLAN(Virtual LAN) 태그가 지정된 트래픽을 캡처할 때 BPF 구문으로 VLAN을 지정해야 합니다.그렇지 않으면 pcap에 VLAN 태그 패킷이 포함되지 않습니다.예를 들어, 이 예에서는 캡처를 192.0.2.1에서 태그가 지정된 VLAN으로 제한합니다.

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

트래픽이 VLAN 태그인지 확실하지 않은 경우 이 구문을 사용하여 VLAN 태그가 지정되지 않은 192.0.2.1의 트래픽을 캡처할 수 있습니다.

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

> **참고:**이전 예에서 괄호는 'or'가 'vlan'에만 적용되지 않도록 필요합니다. 그런 다음 셸에서 괄

호를 잘못 해석하지 않도록 하려면 단일 따옴표가 필요합니다.

VLAN 태그의 사양은 나머지 BPF와 일치하는 모든 VLAN 트래픽을 캡처합니다.그러나 특정 VLAN 태그를 캡처하려면 다음과 같이 캡처할 VLAN 태그를 지정할 수 있습니다.

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

원하는 옵션을 지정하고 **Enter**를 누르면 tcpdump가 트래픽을 캡처하기 시작합니다.

팁:-c 옵션을 사용하지 않은 경우 **Ctrl-C** 키 조합을 눌러 캡처를 중지합니다.

캡처를 중지하면 확인 메시지가 표시됩니다.예:

```
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 허용하는 다른 시스템으로 pcap 파일을 복사하려면 다음 명령을 사용합니다.

```
> system file secure-copy hostname username destination_directory pcap_file
```

Enter를 누르면 원격 시스템에 대한 비밀번호를 입력하라는 메시지가 표시됩니다.파일이 네트워크를 통해 복사됩니다.

참고:이 예에서 호스트 이름**은** 대상 원격 호스트의 이름 또는 IP 주소를, **username은** 원격 호스트의 사용자 이름을, destination_directory는 원격 호스트의 대상 경로를, pcap_file은 전송할 로컬 pcap 파일을 지정합니다.