소프트웨어에 포함된 패킷 구성 및 캡처

목차

소개

이 문서에서는 Cisco IOS® 소프트웨어의 EPC(Embedded Packet Capture) 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS 릴리스 12.4(20)T 이상
- Cisco IOS XE® 릴리스 15.2(4)S - 3.7.0 이상

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.

배경 정보

활성화된 경우 라우터는 전송 및 수신된 패킷을 캡처합니다. 패킷은 DRAM의 버퍼 내에 저장되며 다시 로드를 통해 유지되지 않습니다. 데이터가 캡처되면 라우터에서 요약 또는 상세 보기로 검사할 수 있습니다.

또한 추가 검사를 위해 데이터를 PCAP(패킷 캡처) 파일로 내보낼 수 있습니다. 이 도구는 EXEC 모드로 구성되어 있으며 임시 지원 도구로 간주됩니다. 따라서 도구 구성은 라우터 구성에 저장되지 않으며 시스템 다시 로드 후에도 그대로 유지되지 않습니다.

Cisco 고객은 패킷 캡처 구성 생성기 및 분석기 툴을 사용하여 패킷 캡처를 구성, 캡처 및 추출할 수 있습니다.

Cisco IOS 컨피그레이션 예

기본 EPC 컨피그레이션

1. 캡처된 패킷이 저장되는 임시 버퍼인 '캡처 버퍼'를 정의합니다.
2. 버퍼를 정의할 때 선택할 수 있는 옵션은 다양합니다. 크기, 최대 패킷 크기, 원형/선형 등의

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. 원하는 트래픽으로 캡처를 제한하려면 필터를 적용할 수 있습니다. 컨피그레이션 모드에서 ACL(Access Control List)을 정의하고 필터를 버퍼에 적용합니다.

```
ip access-list extended BUF-FILTER
permit ip host 192.168.1.1 host 172.16.1.1
permit ip host 172.16.1.1 host 192.168.1.1

monitor capture buffer BUF filter access-list BUF-FILTER
```

4. 캡처가 발생하는 위치를 정의하는 캡처 지점을 정의합니다.
5. 또한 캡처 포인트는 IPv4 또는 IPv6에 대한 캡처 여부 및 어떤 스위칭 경로(프로세스 대 cef)를 사용하는지 정의합니다.

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. 버퍼를 캡처 지점에 연결합니다.

```
monitor capture point associate POINT BUF
```

7. 캡처를 시작합니다.

```
monitor capture point start POINT
```

8. 이제 캡처가 활성화됩니다. 필요한 데이터의 수집을 허용합니다.

9. 캡처를 중지합니다.

```
monitor capture point stop POINT
```

10. 장치의 버퍼를 검사합니다.

```
show monitor capture buffer BUF dump
```

참고: 이 출력은 패킷 캡처의 16진수 덤프만 표시합니다. 사람이 읽을 수 있는 상태로 그들을 보기 위해서는 두 가지 방법이 있다.추가 분석을 위해 라우터에서 버퍼를 내보냅니다.

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

이전 방법은 라우터에 T/FTP 액세스가 필요했기 때문에 항상 실용적이지 않습니다. 그러한 경우, 16진수 덤프의 복사본을 가지고 온라인 hex-pcap 변환기를 사용하여 파일을 봅니다.

11. 필요한 데이터가 수집되면 'capture point' 및 'capture buffer'를 삭제합니다.

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

추가 Cisco IOS 컨피그레이션 정보

- Cisco IOS® 릴리스 15.0(1)M 이전 릴리스에서는 버퍼 크기가 512K로 제한되었습니다.
- Cisco IOS® 릴리스 15.0(1)M 이전의 릴리스에서는 캡처된 패킷 크기가 1024바이트로 제한되었습니다.
- 패킷 버퍼는 DRAM에 저장되며 다시 로드하는 동안 유지되지 않습니다.
- 캡처 컨피그레이션은 NVRAM에 저장되지 않으며 다시 로드할 때 유지되지 않습니다.
- 캡처 포인트는 cef 또는 프로세스 스위칭 경로에서 캡처하도록 정의할 수 있습니다.
- 캡처 포인트는 인터페이스 또는 전역에서만 캡처하도록 정의할 수 있습니다.
- 캡처 버퍼를 PCAP 형식으로 내보내면 L2 정보(예: 이더넷 캡슐화)가 보존되지 않습니다.
- 이 섹션에서 사용되는 명령에 대한 자세한 내용은 검색 명령에 대한 모범 사례를 참조하십시오.

기본 IP 트래픽 내보내기 컨피그레이션

IP 트래픽 내보내기는 여러 동시 WAN 또는 LAN 인터페이스에서 수신된 IP 패킷을 내보내는 다른 방법입니다.

1. 컨피그레이션 모드에서 IP 트래픽 내보내기 프로필을 정의합니다.

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2. 프로파일에서 양방향 트래픽을 구성합니다.

```
Device(config-rite)# bidirectional
```

3. 종료

4. 내보낸 트래픽에 대한 인터페이스를 지정합니다.

```
Device(config-if)# interface GigabitEthernet 0/1
```

5. 인터페이스에서 IP 트래픽 내보내기를 활성화합니다.

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6. 종료

7. 캡처를 시작합니다. 이제 캡처가 활성화됩니다. 필요한 데이터의 수집을 허용합니다.

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8. 캡처를 중지합니다.

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9. 외부 TFTP 서버로 캡처를 내보냅니다.

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10. 필요한 데이터가 수집되면 프로파일을 삭제합니다.

```
Device(config)# no ip traffic-export profile mypcap
```

IP 트래픽 내보내기의 단점

IP 트래픽 내보내기는 EPC 방법과 비교할 때 다음과 같은 단점이 있습니다.

- 캡처된 트래픽을 내보내는 인터페이스는 이더넷 인터페이스여야 합니다.
- IPv6를 지원하지 않습니다.
- 레이어 2 정보는 없고 레이어 3 이상만 가능합니다.

Cisco IOS-XE 컨피그레이션의 예

Embedded Packet Capture 기능은 Cisco IOS-XE® Release 3.7 - 15.2(4)S에 도입되었습니다. 캡처 구성은 Cisco IOS®와 다릅니다. 더 많은 기능이 추가되기 때문입니다.

기본 EPC 컨피그레이션

1. 캡처가 발생하는 위치를 정의합니다.

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. 필터를 연결합니다. 필터가 인라인으로 지정되었거나 ACL 또는 클래스 맵을 참조할 수 있습니다.

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. 캡처를 시작합니다.

```
monitor capture CAP start
```

4. 이제 캡처가 활성화됩니다. 필요한 데이터를 수집하도록 허용합니다.

5. 캡처를 중지합니다.

```
monitor capture CAP stop
```

6. 요약 보기에서 캡처를 검토합니다.

```
show monitor capture CAP buffer brief
```

7. 자세한 보기에서 캡처를 검토합니다.

```
show monitor capture CAP buffer detailed
```

8. 또한 추가 분석을 위해 캡처를 PCAP 형식으로 내보냅니다.

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. 필요한 데이터가 수집되면 캡처를 제거합니다.

```
no monitor capture CAP
```

추가 정보

- 물리적 인터페이스, 하위 인터페이스 및 터널 인터페이스에서 캡처가 수행됩니다.
- NBAR(Network Based Application Recognition) 기반 필터 **match protocol** class-map 아래의 명령은 현재 지원되지 않습니다.
- 이 섹션에서 사용되는 명령에 대한 자세한 내용은 검색 명령에 대한 모범 사례를 참조하십시오.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

Cisco IOS-XE®에서 실행되는 EPC의 경우 이 debug 명령을 사용하여 EPC가 제대로 설정되었는지 확인합니다.

```
debug epc provision
debug epc capture-point
```

관련 정보

- 내장형 패킷 캡처 - Cisco IOS-XE
- 내장형 패킷 캡처 - Cisco IOS
- 기술 지원 및 문서 – Cisco Systems

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.