CLI 모드에서 vManage/vSmart/vEdge TCPDUMP 패킷 캡처 구성

목차

소개

이 문서에서는 CLI 모드에서 vManage/vSmart/vEdge TCPDUMP 패킷 캡처를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)

사용되는 구성 요소

이 문서의 정보는 Cisco vManage 버전 20.9.4를 기반으로 합니다

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Cisco SD-WAN 아키텍처에서는 vManage, vSmart 및 vEdge가 각각 관리, 제어 및 데이터 전달의 핵심 역할을 수행합니다. 네트워크의 안정성과 보안을 보장하고 네트워크 결함을 트러블슈팅하기 위해 네트워크 엔지니어는 종종 이러한 디바이스를 통해 흐르는 트래픽에 대해 패킷 캡처 및 분석

을 수행해야 합니다. TCPDUMP는 인터페이스를 통과하는 데이터 패킷을 캡처하고 분석하는 데 사용할 수 있는 가볍고 강력한 명령줄 도구입니다.

CLI 모드에서 TCPDUMP를 구성하고 사용하면 추가 툴 또는 중간 프록시 디바이스 없이 디바이스에서 실시간 트래픽을 직접 캡처할 수 있습니다. 이는 라우팅 이상, 제어 연결 실패, 패킷 손실 및 트래픽 경로 확인과 같은 문제를 찾는 데 매우 중요합니다. Cisco SD-WAN 디바이스(예: vEdge)는 맞춤형 운영 체제(예: Viptela OS)를 실행하므로, TCPDUMP의 사용은 일부 측면에서 기존 Linux 환경과 약간 다를 수 있습니다. 따라서 기본 명령 구조 및 사용 제한을 이해하는 것이 특히 중요합니다.

이 섹션에서는 사용자가 효과적인 네트워크 트래픽 분석 및 문제 진단을 수행할 수 있도록 vManage, vSmart 및 vEdge 디바이스의 CLI 모드에서 TCPDUMP를 구성하고 실행하는 방법에 대해 설명합니다.

TCPDUMP(컨트롤러) 핵심 사항 설명

```
tcpdump [vpn x | interface x | vpn x interface x] options " "
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUv] [ -B size ] [ -c count ]
               [ -E algo:secret ] [ -j tstamptype ] [ -M secret ]
               [ -T type ] [ -y datalinktype ] [ expression ]
```

- 인터페이스 지정(vpn만 지정하는 출력을 가져올 수 없음)
- 따옴표 사이에 옵션을 넣습니다("). ctrl c를 사용하여 중지합니다.
- ip를 호스트 이름으로 변환하는 것을 방지하려면 -n을 사용하고, 이름과 포트를 방지하려면-nn을 사용합니다.
- -v 더 자세한 정보 표시 (IP 헤더 정보, tos, ttl, offset, flags, protocol)
- -vv 및 -vvv는 특정 패킷 유형에 대한 자세한 내용을 보여 줍니다.
- 프록시 ex - udp, tcp icmp pim igmp vrrp esp arp
- 부정하다! 또는 아님, &&or and, | | 또는 ()와 함께 사용하지 않음(udp 또는 icmp)

TCPDUMP(계속)

- Linux tcpdump 명령에서 조정되지만 사용 가능한 모든 옵션을 지원하지는 않습니다. 버퍼에 저장된 패킷의 스냅샷은 PCAP로 내보낼 수 없습니다.
- -p 플래그('no-promiscuous mode'를 의미함)로 실행됩니다. 컨트롤러는 제어 패킷 또는 브로드캐스트 패킷을 포함하여 컨트롤러 인터페이스로 향하는 패킷만 캡처합니다. 데이터 플레인 트래픽을 캡처할 수 없습니다.
- -s 128, 스냅샷 길이(바이트)로 실행됩니다. 패킷의 처음 x바이트가 캡처됩니다.

TCPDUMP 명령 사용

이 절에서는 tcpdumpcommand가 사용되는 방법을 보여 주는 예를 제공합니다.

```
vmanage# tcpdump ?
Possible completions:
interface  Interface on which tcpdump listens
vpn        VPN ID
```

show interface description 명령의 출력은 현재 사용 중인 vpn/인터페이스 이름 및 번호에 대한 정확한 정보를 제공합니다.

```
vmanage# tcpdump vpn 0 interface eth0 ?
Possible completions:
help       tcpdump help
options    tcpdump options or expression
|          Output modifiers
<cr>
```

"options" 키워드를 통해 패킷 캡처 필터링에 대한 조건을 더 추가할 수 있습니다.

```
vmanage# tcpdump vpn 0 interface eth0 help

Tcpdump options:
help               Show usage
vpn                VPN or namespace
interface          Interface name
options            Tcpdump options like -v, -vvv, t,-A etc or expressions like port 25 and not host 10.0

e.g., tcpdump vpn 1 interface ge0/4 options "icmp or udp"

Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUv] [ -B size ] [ -c count ] [ -E algo:secret ] [ -j tstamptype ]
               [ -T type ] [ -y datalinktype ] [ expression ]
```

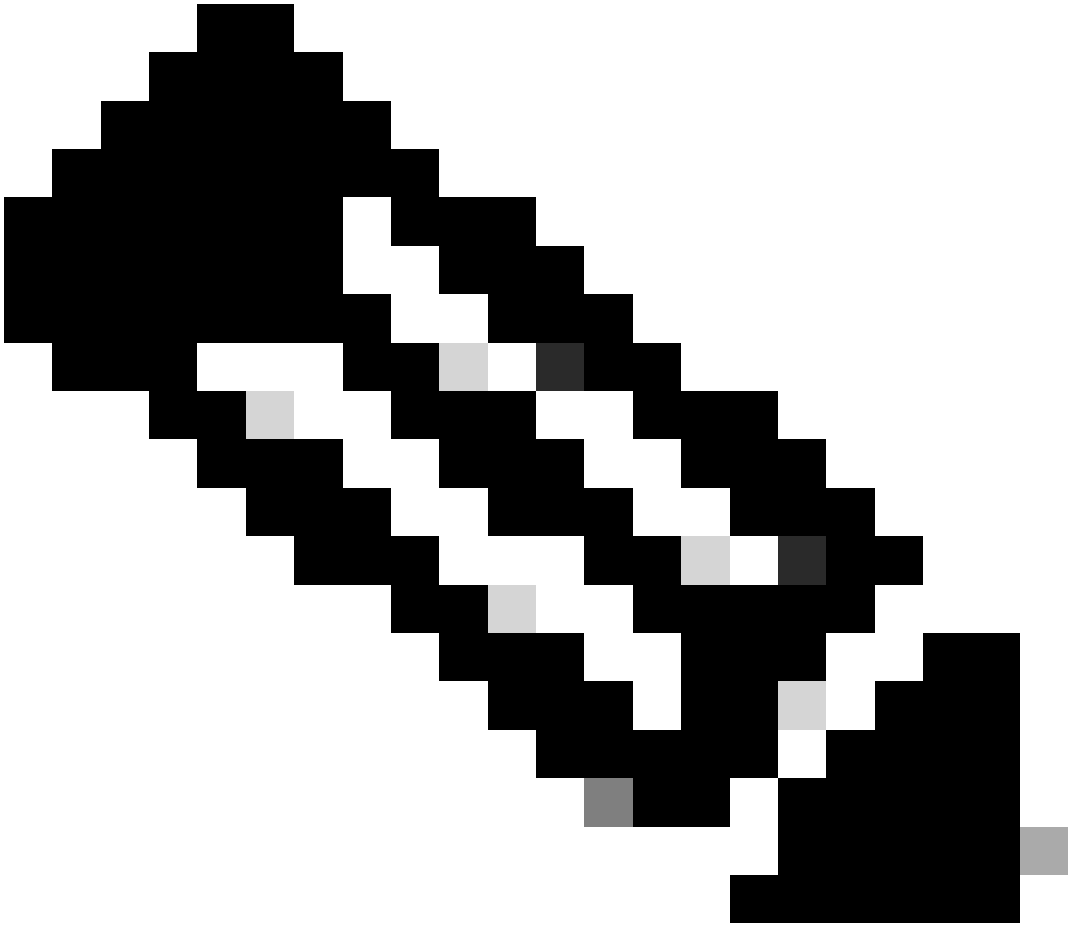
옵션 "-c count" 명령을 사용하여 특정 패키지 수를 지정할 수 있습니다. 특정 패키지 수를 지정하지 않으면 연속 캡처가 제한 없이 실행됩니다.

```
vmanage# tcpdump vpn 0 interface eth0 options "-c 10 "
tcpdump -p -i eth0 -s 128 -c 10 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
04:56:55.797308 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 237
04:56:55.797371 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 205
04:56:55.797554 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.797580 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.808036 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.917567 ARP, Request who-has 50.128.76.31 (Broadcast) tell 50.128.76.1, length 46
04:56:55.979071 IP 50.128.76.22.12346 > 50.128.76.25.12346: UDP, length 182
04:56:55.979621 IP 50.128.76.25.12346 > 50.128.76.22.12346: UDP, length 146
04:56:56.014054 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 237
04:56:56.135636 IP 50.128.76.32.12426 > 50.128.76.22.12546: UDP, length 140
10 packets captured
1296 packets received by filter
```

```
0 packets dropped by kernel
```

옵션에 호스트 주소 및 프로토콜 유형에 대한 필터 조건을 추가할 수도 있습니다.

```
vmanage# tcpdump vpn 0 interface eth0 options "-n host 50.128.76.27 and icmp"
tcpdump -p -i eth0 -s 128 -n host 50.128.76.27 and icmp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
05:21:31.855189 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 34351, seq 29515, length 28
05:21:34.832871 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 44520, seq 29516, length 28
05:21:34.859655 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 44520, seq 29516, length 28
05:21:37.837244 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 39089, seq 29517, length 28
05:21:37.866201 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 39089, seq 29517, length 28
05:21:40.842214 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 24601, seq 29518, length 28
05:21:40.870203 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 24601, seq 29518, length 28
05:21:43.847548 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 42968, seq 29519, length 28
05:21:43.873016 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 42968, seq 29519, length 28
05:21:46.852305 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 23619, seq 29520, length 28
05:21:46.880557 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 23619, seq 29520, length 28
^C                                                                                <<<< Ctrl + c can inter
11 packets captured
11 packets received by filter
0 packets dropped by kernel
```

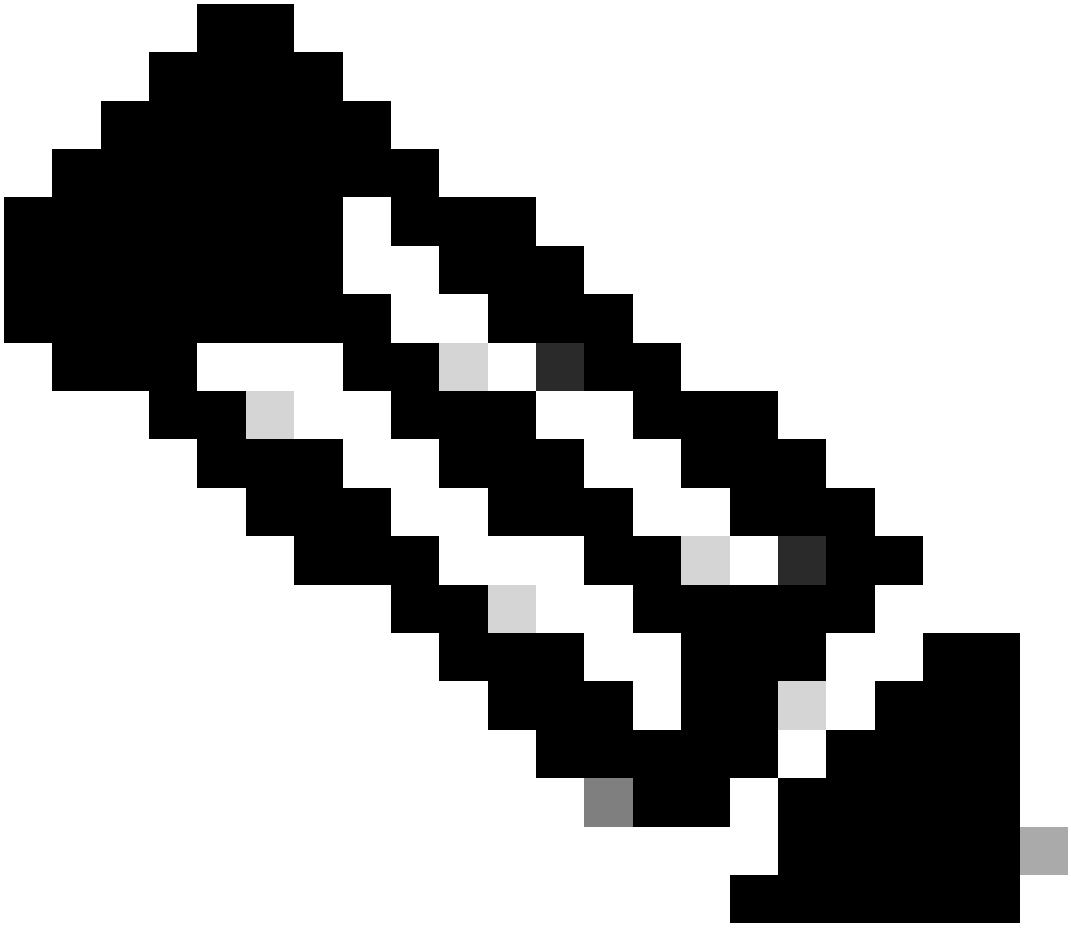


참고: Cisco IOS XE SD-WAN 소프트웨어에서 TCPDUMP 대신 EPC(Embedded Packet Capture)를 사용할 수 있습니다.

TCPDUMP 예

수신 대기 일반 UDP 패킷:

tcpdump vpn 0 옵션 "-vv -nnn udp"



참고: 다른 프로토콜에도 적용할 수 있습니다. 예: icmp, arp 등

ICMP 및 UDP를 사용하는 특정 포트 수신:
tcpdump vpn 0 인터페이스 ge0/4 옵션 "icmp 또는 udp"

특정 포트 번호에서 수신(TLS 포트에서 수신):
tcpdump vpn 0 인터페이스 ge0/4 옵션 "-vv -nn port 23456"

특정 포트 번호에서 수신(DTLS 포트에서 수신):
tcpdump vpn 0 인터페이스 ge0/4 옵션 "-vv -nn port 12346"

특정 호스트 수신(해당 호스트에서 수신/발신): -e 링크 레벨 헤더를 인쇄합니다.
tcpdump vpn 0 인터페이스 ge0/4 옵션 "host 64.100.103.2 -vvv -nn -e"

ICMP만 있는 특정 호스트 수신

tcpdump vpn 0 인터페이스 ge0/4 옵션 "host 64.100.103.2 && icmp"

소스 및/또는 대상별 필터링
tcpdump vpn 0 인터페이스 ge0/4 옵션 "src 64.100.103.2 && dst 64.100.100.75"

GRE 캡슐화된 트래픽 필터링
tcpdump vpn 0 인터페이스 ge0/4 옵션 "-v -n proto 47 "

관련 문서

- SD-WAN 제어 연결 문제 해결
- Cisco SD-WAN: 평소의 용의자들
- TCPDUMP 매뉴얼 페이지

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.