빠른 시작 가이드 - 다양한 SD-WAN 문제에 대한 데이터 수집

목차

소개

이 문서에서는 문제 해결 속도 및/또는 문제 해결 속도를 개선하기 위해 TAC 케이스를 열기 전에 미리 수집해야 하는 관련 데이터와 함께 몇 가지 SD-WAN 문제에 대해 설명합니다.이 문서는 두 가지 주요 기술 섹션으로 구분됩니다.vManage 및 Edge 라우터관련 출력 및 명령 구문은 해당 디바이스에 따라 제공됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco의 SDWAN 아키텍처
- vManage 컨트롤러와 cEdge(IOS-XE SD-WAN 라우터) 및 vEdge 디바이스(ViptelaOS 라우터)를 비롯한 솔루션에 대한 일반적인 이해

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.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

기본 정보 요청됨

- 네트워크 및 사용자에게 미치는 문제와 그 영향에 대해 설명하십시오. 예상 동작을 설명합니다.관찰된 동작에 대해 자세히 설명합니다.가능한 경우 주소를 지정하여 토폴로지 다이어그램을 준비합니다(수동 그린 경우에도).
- 언제 문제가 시작되었습니까? 문제가 처음 발견되거나 발견된 날짜와 시간을 확인합니다.
- 문제의 잠재적인 트리거가 될 수 있는 것은 무엇입니까? 문제가 시작되기 전에 변경한 내용을 문서화합니다.문제가 시작되도록 트리거할 수 있는 특정 작업 또는 이벤트를 확인합니다.이 문제가 다른 네트워크 이벤트 또는 작업과 관련이 있습니까?
- 문제의 빈도는 얼마입니까? 일회성 사건이었나요?그렇지 않으면 얼마나 자주 문제가 발생합니까?
- 해당 장치에 대한 정보 제공: 특정 장치가 영향을 받는 경우(무작위가 아님), 공통적인 사항은 무엇입니까?각 디바이스의 System-IP 및 Site-ID입니다.문제가 vManage 클러스터에 있는 경우 노드 세부 정보를 제공합니다(클러스터의 모든 노드에서 동일하지 않은 경우).vManage GUI의 일반적인 문제에 대해서는 모든 스크린샷을 파일로 캡처하여 오류 메시지 또는 조사해야 하는 기타 이상/사체를 표시합니다.
- TAC에서 원하는 결과와 우선 순위에 대한 정보를 제공합니다. 가능한 한 빨리 오류를 복구하시겠습니까? 아니면 실패의 근본 원인을 파악하시겠습니까?

vManage

여기서 문제는 vManage에 대해 보고된 일반적인 문제 조건과 관리 **기술** 파일 외에 수집해야 하는 각 문제에 대한 유용한 출력입니다. 클라우드 호스티드 컨트롤러의 경우, TAC(Technical Assistance Center) 엔지니어가 이에 대한 명시적 동의를 제공하는 경우 Base Information Requested 섹션의 피드백에 따라 디바이스에 대한 필수 **관리자 기술** 출력을 수집할 수 있습니다.그러나 여기에 설명된 단계에서 포함된 데이터가 문제 시간과 관련되는지 확인하기 위해 **admin-tech** 출력을 캡처하는 것이 좋습니다.문제가 지속되지 않는 경우 특히 그렇습니다. 즉, TAC가 참여할 때 문제가 사라질 수 있습니다. 온프레미스 컨트롤러의 경우 **관리자** 기술**을** 각 데이터 세트에 포함해야 합니다.vManage 클러스터의 경우 클러스터의 각 노드 또는 영향을 받는 노드만 **admin-tech**를 캡처해야 합니다.

느림/느림

문제 보고서:vManage GUI 액세스 속도 저하, GUI 내에서 작업을 수행할 때의 지연 시간, vManage 내에서 나타나는 일반적인 느림 또는 장진 현상

1단계. 스레드 인쇄의 2-3개 인스턴스를 캡처하고 각 스레드 **인쇄** 파일의 이름을 각각 숫자 지정으로 바꿉니다(파일 경로에서 vManage에 로그인하는 사용자 이름을 사용합니다). 예를 들면 다음과 같습니다.

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.1
```

2단계. vshell에 **로그인하고** 아래와 **같이 vmstat**를 실행합니다.

```
vManage# vshell
vManage:~$ vmstat 1 10
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
1 0 0 316172 1242608 5867144 0 0 1 22 3 5 6 1 93 0 0
0 0 0 316692 1242608 5867336 0 0 0 8 2365 4136 6 1 93 0 0
0 0 0 316204 1242608 5867344 0 0 0 396 2273 4009 6 1 93 0 0
0 0 0 316780 1242608 5867344 0 0 0 0 2322 4108 5 2 93 0 0
0 0 0 318136 1242608 5867344 0 0 0 0 2209 3957 9 1 90 0 0
0 0 0 318300 1242608 5867344 0 0 0 0 2523 4649 5 1 94 0 0
1 0 0 318632 1242608 5867344 0 0 0 44 2174 3983 5 2 93 0 0
0 0 0 318144 1242608 5867344 0 0 0 64 2182 3951 5 2 94 0 0
0 0 0 317812 1242608 5867344 0 0 0 0 2516 4289 6 1 93 0 0
0 0 0 318036 1242608 5867344 0 0 0 0 2600 4421 8 1 91 0 0
vManage:~$
```

3단계. vshell에서 추가 세부 정보를 **수집합니다**.

```
vManage:~$ top (press '1' to get CPU counts)
vManage:~$ free -h
vManage:~$ df -kh
```

4단계. 모든 NMS 서비스 진단을 캡처합니다.

```
vManage# request nms application-server diagnostics
vManage# request nms configuration-db diagnostics
vManage# request nms messaging-server diagnostics
vManage# request nms coordination-server diagnostics
vManage# request nms statistics-db diagnostics
```

API 실패/문제

문제 보고서:API 호출에서 데이터 또는 올바른 데이터를 반환하지 못함, 쿼리 실행 일반 문제

1단계. 사용 가능한 메모리를 확인합니다.

```
vManage:~$ free -h
total used free shared buff/cache available
Mem: 31Gi 24Gi 280Mi 60Mi 6.8Gi 6.9Gi
Swap: 0B 0B 0B
vManage:~$
```

2단계. 5초 간격의 스레드 인쇄 인스턴스를 캡처하고 각 **스레드 인쇄** 파일의 이름을 각 명령 실행 후 숫자 지정으로 바꿉니다(파일 경로에서 vManage에 로그인하는 사용자 이름을 사용합니다).

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.1
<WAIT 5 SECONDS>
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.2
```

3단계. 활성 HTTP 세션에 대한 세부 정보를 수집합니다.

```
vManage# request nms application-server jcmd gc-class-histo | i
io.undertow.server.protocol.http.HttpServerConnection
```

4단계. 다음 세부 정보를 제공합니다.

1. 실행된 API 호출

2. 호출 빈도

3. 로그인 방법(예: 후속 API 호출을 실행하는 단일 토큰 사용 또는 통화를 실행한 다음 로그아웃하는 기본 인증 사용)

4. JSESSIONID를 다시 사용하고 있습니까?

> **참고** 19.2 vManage 소프트웨어부터 API 호출에는 토큰 기반 인증만 지원됩니다.토큰 생성, 시간 초과 및 만료에 대한 자세한 내용은 이 링크를 참조하십시오.

DPI(Deep Packet Inspection) 통계/느림

문제 보고서:DPI를 활성화하면 통계 처리 속도가 느려지거나 vManage GUI 내에서 속도가 느려질 수 있습니다.

1단계. Administration(관리) > Settings(설정) > Statistics Database(통계 데이터베이스) > **Configuration(컨피그레이션)**으로 이동하여 vManage 내부**에서 DPI에 할당된** 디스크 크기를 **확인합니다**.

2단계. vManage에서 다음 CLI 명령을 실행하여 인덱스 상태를 확인합니다.

```
vManage# request nms statistics-db diagnostics
```

3단계. DPI 통계와 관련된 API 호출이 외부에서 실행되는지 확인합니다.

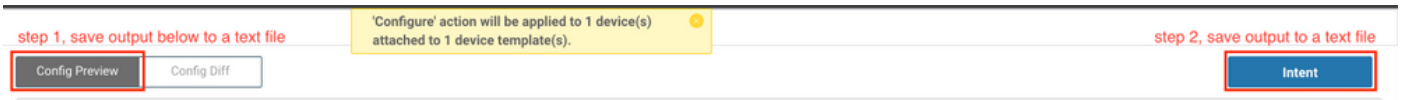
4단계. vManage에서 이 CLI 명령의 도움을 받아 디스크 I/O 통계를 확인합니다.

```
vManage# request nms application-server diagnostics
```

템플릿 푸시 실패

문제 보고서:템플릿 푸시 또는 디바이스 템플릿 업데이트에 실패하거나 시간 초과됩니다.

1단계. Configure Devices(디바이스 구성) 버튼을 클릭하기 전에 vManage에서 **Config Preview** 및 **Intent** 컨피그레이션을 캡처합니다(여기에 제공된 탐색 예).



2단계. logsettings 페이지에서 **viptella.enable.rest.log를 활성화합니다**(필수 정보를 캡처한 후 비활성화해야 함).

```
https://<vManage IP>:8443/logsettings.html
```

3단계. 템플릿 푸시 실패가 NETCONF 문제 또는 오류와 관련된 경우 1단계**의 REST** 로그 외에 viptela.enable.device.netconf**.log를** 활성화합니다. 3단계 및 4단계의 출력을 캡처한 후에도 이 로그를 비활성화해야 합니다.

4단계. vManage에서 실패한 템플릿을 다시 연결하고 이 CLI를 사용하여 **admin-tech**를 캡처합니다(클러스터의 각 노드에 대해 이 캡처).

```
vManage# request admin-tech
```

5단계. vManage 및 Config Diff의 작업에서 스크린샷을 제공하여 실패 세부사항과 템플릿에 사용된 CSV 파일을 확인합니다.

6단계. 실패한 푸시 시간, 실패한 디바이스의 **시스템** IP, vManage GUI에 표시되는 오류 메시지 등 오류 및 작업에 대한 세부 정보를 포함합니다.

7단계. 디바이스 자체에서 컨피그레이션에 대해 보고된 오류 메시지와 함께 템플릿 푸시 오류가 발생하는 경우 디바이스에서도 **admin-tech**를 수집합니다.

클러스터 관련 문제

문제 보고서:클러스터 불안정으로 인해 GUI 시간 초과, 장진 현상 또는 기타 이상 현상이 발생합니다.

1단계. 클러스터의 각 vManage 노드**에서 server_configs.json**의 출력을 캡처합니다.예를 들면 다음과 같습니다.

```
vmanage# vshell
vmanage:~$ cd /opt/web-app/etc/
vmanage:/opt/web-app/etc$ more server_configs.json | python -m json.tool
{
"clusterid": "",
"domain": "",
"hostsEntryVersion": 12,
"mode": "SingleTenant",
"services": {
"cloudAgent": {
"clients": {
"0": "localhost:8553"
},
"deviceIP": "localhost:8553",
"hosts": {
"0": "localhost:8553"
},
"server": true,
"standalone": false
},
"container-manager": {
"clients": {
"0": "169.254.100.227:10502"
},
"deviceIP": "169.254.100.227:10502",
"hosts": {
"0": "169.254.100.227:10502"
},
"server": true,
"standalone": false
},
"elasticsearch": {
"clients": {
"0": "169.254.100.227:9300",
"1": "169.254.100.254:9300",
"2": "169.254.100.253:9300"
},
"deviceIP": "169.254.100.227:9300",
"hosts": {
```

```
"0": "169.254.100.227:9300",
"1": "169.254.100.254:9300",
"2": "169.254.100.253:9300"
},
"server": true,
"standalone": false
},
"kafka": {
"clients": {
"0": "169.254.100.227:9092",
"1": "169.254.100.254:9092",
"2": "169.254.100.253:9092"
},
"deviceIP": "169.254.100.227:9092",
"hosts": {
"0": "169.254.100.227:9092",
"1": "169.254.100.254:9092",
"2": "169.254.100.253:9092"
},
"server": true,
"standalone": false
},
"neo4j": {
"clients": {
"0": "169.254.100.227:7687",
"1": "169.254.100.254:7687",
"2": "169.254.100.253:7687"
},
"deviceIP": "169.254.100.227:7687",
"hosts": {
"0": "169.254.100.227:5000",
"1": "169.254.100.254:5000",
"2": "169.254.100.253:5000"
},
"server": true,
"standalone": false
},
"orientdb": {
"clients": {},
"deviceIP": "localhost:2424",
"hosts": {},
"server": false,
"standalone": false
},
"wildfly": {
"clients": {
"0": "169.254.100.227:8443",
"1": "169.254.100.254:8443",
"2": "169.254.100.253:8443"
},
"deviceIP": "169.254.100.227:8443",
"hosts": {
"0": "169.254.100.227:7600",
"1": "169.254.100.254:7600",
"2": "169.254.100.253:7600"
},
"server": true,
"standalone": false
},
"zookeeper": {
"clients": {
"0": "169.254.100.227:2181",
"1": "169.254.100.254:2181",
"2": "169.254.100.253:2181"
```

```
},
"deviceIP": "169.254.100.227:2181",
"hosts": {
"0": "169.254.100.227:2888:3888",
"1": "169.254.100.254:2888:3888",
"2": "169.254.100.253:2888:3888"
},
"server": true,
"standalone": false
}
},
"vmanageID": "0"
}
```


2단계. 각 노드에 대해 활성화되거나 비활성화된 서비스에 대한 세부 정보를 캡처합니다.이를 위해 vManage GUI에서 **Administration > Cluster Management**로 이동합니다.

3단계. 클러스터 인터페이스의 언더레이 도달 가능성을 확인합니다.이를 위해 VPN 0**의** 각 vManage 노드에서 다른 노드의 클러스터 인터페이스 IP에 ping **<ip-address>**를 실행합니다.

4단계. 클러스터의 각 vManage 노드에 대한 모든 NMS 서비스에서 진단을 수집합니다.

```
vManage# request nms application-server diagnostics
vManage# request nms configuration-db diagnostics
vManage# request nms messaging-server diagnostics
vManage# request nms coordination-server diagnostics
vManage# request nms statistics-db diagnostics
```

에지(vEdge/cEdge)

이 문제는 Edge 장치에 대해 보고된 일반적인 문제 조건과 수집해야 하는 각 항목에 대한 유용한 출력입니다.각 문제에 대해 **관리자 기술**이 필요한 모든 에지 장치에 대해 수집되었는지 확인합니다 .클라우드 호스팅 컨트롤러의 경우, TAC에서 **Base Information Requested** 섹션의 피드백에 따라 디바이스에 필요한 관리자-기술 출력을 수집할 수 있는 액세스 권한이 **있습니다**.그러나 vManage와 마찬가지로, TAC 케이스를 열기 전에 이러한 데이터를 캡처하여 포함된 데이터가 문제의 시점과 관련되는지 확인해야 합니다.이는 문제가 지속되지 않을 경우 특히 사실입니다. 즉 TAC가 참여할 때 문제가 사라질 수 있습니다.

장치와 컨트롤러 간에 연결되지 않는 제어 연결

문제 보고서:vEdge/cEdge에서 하나 이상의 컨트롤러로의 제어 연결이 형성되지 않음

1단계. 제어 연결 실패의 로컬/원격 오류를 식별합니다.

- vEdge의 경우:show control connections-**history** 명령**의** 출력입니다.
- cEdge의 경우:show sdwan **control connection-history** 명령 출력

2단계. TLOC의 상태와 모든 상태가 'up'으로 표시되는지 확인합니다.

- vEdge의 경우:show control local-**properties** 명령**의** 출력입니다.
- cEdge의 경우:show sdwan control local-**properties** 명령**의** 출력입니다.

3단계. 시간 초과 또는 연결 실패(예: DCONFAIL 또는 VM_TMO)와 관련된 오류가 발생하면 에지 디바이스와 해당 컨트롤러에서 모두 컨트롤 플레인 캡처를 수행합니다.

- 컨트롤러:

```
vManage# tcpdump vpn 0 interface eth1 options "-vvvvvv host 192.168.44.6"
tcpdump -p -i eth1 -s 128 -vvvvvv host 192.168.44.6 in VPN 0
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 128 bytes
20:02:07.427064 IP (tos 0xc0, ttl 61, id 50139, offset 0, flags [DF], proto UDP (17), length
168)
192.168.44.6.12346 > 192.168.40.1.12346: UDP, length 140
20:02:07.427401 IP (tos 0xc0, ttl 64, id 37220, offset 0, flags [DF], proto UDP (17), length
210)
192.168.40.1.12346 > 192.168.44.6.12346: UDP, length 182
```

- vEdge의 경우:

```
vEdge-INET-Branch2# tcpdump vpn 0 interface ge0/2 options "-vvvvvv host 192.168.40.1"
tcpdump -p -i ge0_2 -vvvvvv host 192.168.40.1 in VPN 0
tcpdump: listening on ge0_2, link-type EN10MB (Ethernet), capture size 262144 bytes
20:14:16.136276 IP (tos 0xc0, ttl 64, id 55858, offset 0, flags [DF], proto UDP (17), length
277)
10.10.10.1 > 192.168.40.1.12446: [udp sum ok] UDP, length 249
20:14:16.136735 IP (tos 0xc0, ttl 63, id 2907, offset 0, flags [DF], proto UDP (17), length 129)
192.168.40.1.12446 > 10.10.10.1.12346: [udp sum ok] UDP, length 101
```

- cEdge의 경우(아래 캡처는 디바이스가 CLI 모드로 이동되었고 **CTRL-CAP**라는 ACL(Access Control List)이 필터링을 위해 생성되었다고 가정합니다. **애플리케이션/네트워크 성능** 시나리오의 EPC 캡처 예에서 자세한 내용을 참조하십시오).

```
cEdge-Branch1#config-transaction
cEdge-Branch1(config)# ip access-list extended CTRL-CAP
cEdge-Branch1(config-ext-nacl)# 10 permit ip host 10.10.10.1 host 192.168.40.1
cEdge-Branch1(config-ext-nacl)# 20 permit ip host 192.168.40.1 host 10.10.10.1
cEdge-Branch1(config-ext-nacl)# commit
cEdge-Branch1(config-ext-nacl)# end

cEdge-Branch1#monitor capture CAP control-plane both access-list CTRL-CAP buffer size 10
cEdge-Branch1#monitor capture CAP start

cEdge-Branch1#show monitor capture CAP buffer brief
------------------------------------------------------------------------
# size timestamp source destination dscp protocol
------------------------------------------------------------------------
0 202 0.000000 192.168.20.1 -> 50.50.50.3 48 CS6 UDP
1 202 0.000000 192.168.20.1 -> 50.50.50.4 48 CS6 UDP
2 220 0.000000 50.50.50.3 -> 192.168.20.1 48 CS6 UDP
3 66 0.000992 192.168.20.1 -> 50.50.50.3 48 CS6 UDP
4 220 0.000992 50.50.50.4 -> 192.168.20.1 48 CS6 UDP
5 66 0.000992 192.168.20.1 -> 50.50.50.4 48 CS6 UDP
6 207 0.015991 50.50.50.1 -> 12.12.12.1 48 CS6 UDP
```

4단계. 제어 연결 기록 출력에서 관찰된 다른 오류와 설명된 문제에 대한 자세한 내용은 다음 가이드를 참조하십시오.

에지 디바이스와 컨트롤러 간의 연결 플랩 제어

문제 보고서:vEdge/cEdge와 하나 이상의 컨트롤러 간에 하나 이상의 제어 연결 플랩.이는 자연에서 자주, 간헐적으로 또는 무작위일 수 있습니다.

- 제어 연결 플랩은 일반적으로 디바이스와 컨트롤러 간의 패킷 손실 또는 전달 문제의 결과입니다.이 오류는 실패의 방향에 따라 **TMO** 오류와 연결되는 경우가 많습니다.이를 자세히 확인하려면 먼저 플랩의 원인을 확인합니다. vEdge/컨트롤러:show control connections-**history** 명령

출력cEdge의 경우:show sdwan **control connection-history** 명령 출력
- 플랩이 발생할 때 TLOC의 상태와 모든 상태가 'up'으로 표시되는지 확인합니다. vEdge의 경우:show control local-**properties** 명령**의** 출력입니다.cEdge의 경우:show sdwan control local-**properties** 명령**의** 출력입니다.
- 컨트롤러와 에지 디바이스 모두에서 패킷 캡처를 수집합니다.각 측의 캡처 매개 변수에 대한 자세한 내용은 **Control Connections Not Forming Between Device and Controller** 섹션을 참조하십시오.

에지 디바이스 간에 BFD(Bidirectional Forwarding Detection) 세션이 형성되지 않거나 플래핑되지 않음

문제 보고서:BFD 세션이 다운되었거나 두 에지 디바이스 간에 업/다운되었습니다.

1단계. 각 디바이스에서 BFD 세션의 상태를 수집합니다.

- vEdge의 경우:show bfd sessions 명령**의** 출력입니다.
- cEdge의 경우:show sdwan bfd sessions 명령**의** 출력입니다.

2단계. 각 에지 라우터에서 Rx 및 Tx 패킷 수를 수집합니다.

- vEdge의 경우:show tunnel statistics bfd 명령**의** 출력입니다.
- cEdge의 경우:show platform **hardware qfp active feature bfd datapath sdwan summary** 명령 출력

3단계. 위의 출력에서 터널의 한쪽 끝에서 BFD 세션에 대한 카운터가 증가하지 않으면 ACL을 사용하여 패킷을 캡처하여 패킷이 로컬로 수신되는지 확인할 수 있습니다.이에 대한 자세한 내용과 함께 수행할 수 있는 다른 검증도 여기에서 확인할 수 있습니다.

디바이스 충돌

문제 보고서:장치가 예기치 않게 다시 로드되고 전원 문제가 발생하지 않습니다.디바이스의 징후는 잠재적으로 충돌이 발생했음을 나타냅니다.

1단계. 디바이스에서 충돌 또는 예기치 않은 다시 로드가 관찰되었는지 확인합니다.

- vEdge의 경우:show reboot history 명령**의** 출력입니다.
- cEdge의 경우:show sdwan reboot history 명령**의** 출력입니다.
- 또는 Monitor(**모니터) > Network(네트워크**)로 이동하여 디바이스를 선택한 다음 **System Status(시스템 상태) > Reboot(재부팅)로 이동하여** 예기치 않은 재로드가 있는지 확인합니다.

2단계. 확인된 경우, Tools(툴) > Operational Commands(운영 명령)로 이동하여 vManage를 통해 디바이스에서 admin-tech**를 캡처합니다**.그런 다음 장치의 **Options** 버튼을 선택하고 **Admin Tech**를 선택합니다.디바이스의 모든 로그 및 코어 파일을 포함하는 모든 확인란을 선택합니다.

사이트 간의 애플리케이션/네트워크 성능 저하 또는 실패

문제 보고서:애플리케이션이 작동하지 않음/HTTP 페이지가 로드되지 않음, 성능 저하/레이턴시, 정책 또는 컨피그레이션 변경 후 장애 발생

1단계. 문제를 나타내는 애플리케이션 또는 플로우의 소스/대상 IP 쌍을 식별합니다.

2단계. 경로에 있는 모든 에지 디바이스를 확인하고 vManage를 통해 각**에서 관리자 기술**을 수집합

니다.

3단계. 문제가 표시되면 각 사이트의 에지 디바이스에서 이 플로우에 대한 패킷 캡처를 수행합니다.

- vEdge의 경우: Administration(관리) **> Settings(설정)** For Hostname(호스트 이름에 대한 **설정)** 필드에서 Data Stream을 활성화하려면 vManage의 시스템 IP를 입력합니다.**VPN**의 경우 **0**을 입력합니다.vManage VPN 0 인터페이스의 **allow-service** 컨피그레이션 아래에서 HTTPS가 활성화되었는지 확인합니다.서비스 측 VPN 인터페이스에서 트래픽을 캡처하려면 여기의 단계를 따릅니다.
- cEdge의 경우: Configuration(컨피그레이션) > Devices(디바이스) > Change Mode(**모드 변경) > CLI mode(CLI 모드)를** 통해 cEdge를 CLI 모드로 **이동합니다.**cEdge에서 트래픽을 양방향으로 매칭하도록 확장 ACL을 구성합니다.캡처에서 크기와 데이터를 제한하기 위해 프로토콜 및 포트를 포함하도록 최대한 구체적으로 지정합니다.
- (b)에서 생성한 ACL을 사용하여 서비스 측 인터페이스에 대해 EPC(Embedded Packet Capture)를 양방향 구성합니다.캡처를 PCAP 형식으로 내보내고 상자에서 복사할 수 있습니다.BROKEN-**FLOW**라는 ACL을 사용하는 라우터의 GigabitEthernet0/0/0에 대한 샘플 컨피그레이션이 여기에 **제공됩니다**.

```
monitor capture CAP interface GigabitEthernet0/0/0 both access-list BROKEN-FLOW buffer size 10
monitor capture CAP start

show monitor capture CAP parameter
show monitor capture CAP buffer [brief]

monitor capture CAP export bootflash:cEdge1-Broken-Flow.pcap
```

- 트래픽을 필터링하기 위해 (b)에 생성된 ACL을 사용하여 양방향으로 트래픽에 대한 패킷 추적을 구성합니다.다음은 샘플 컨피그레이션입니다.

```
debug platform packet-trace packet 2048 fia-trace
debug platform packet-trace copy packet input l3 size 2048
debug platform condition ipv4 access-list BROKEN-FLOW both
debug platform condition start

show platform packet-trace summary
show platform packet-trace packet all | redirect bootflash:cEdge1-PT-OUTPUT.txt
```

4단계. 가능한 경우 비교 작업 시나리오에서 3단계를 반복합니다.

> **팁**: cEdge에서 해당 파일을 직접 복사하는 다른 방법이 없는 경우 여기에 설명된 방법을 사용하여 먼저 파일을 vManage에 복사할 수 있습니다. vManage에서 명령을 실행합니다. **scp -P 830 <username>@<cEdge system-IP>:/bootflash/<filename> 요청 실행** 이 파일은 vManage에 로그인하는 데 사용한 사용자 이름**에** 대한**/home/<username>/** 디렉토리에 저장됩니다.여기에서 SFTP(Secure File Transfer Protocol)의 SCP(Secure Copy Protocol)를 사용하여 타사 SCP/SFTP 클라이언트 또는 OpenSSH 유틸리티와 함께 Linux/Unix 시스템 CLI를 사용하여 vManage에서 파일을 복사할 수 있습니다.