

Snelle startgids - Gegevensverzameling voor verschillende SD-WAN problemen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Vereiste basisinformatie](#)

[vManager](#)

[Laagheid/verzwakking](#)

[API-fouten/problemen](#)

[Deep Packet Inspection \(DPI\) Status/Langzaamheid](#)

[Sjabloonruppelfouten](#)

[Cluster-gerelateerde problemen](#)

[Edge \(vEdge/cEdge\)](#)

[Control-verbindingen die niet bestaan tussen apparaten en controllers](#)

[Control-verbindingen tussen randapparatuur en controllers](#)

[BFD-sessies \(Bidirectional Forwarding Detection\) \(BFD\) die niet ontstaan of flappen tussen Edge-apparaten](#)

[Apparaatcrashes](#)

[Toepassings-/netwerkprestaties die achteruitgaan of falen tussen locaties](#)

Inleiding

Dit document beschrijft meerdere SD-WAN problemen langs relevante gegevens die vooraf moeten worden verzameld voordat u een TAC-case opent om de snelheid van de probleemoplossing en/of probleemoplossing te verbeteren. Dit document bestaat uit twee belangrijke technische onderdelen: vEdge-routers beheren. Relevante output en syntax van commando's zijn afhankelijk van het betrokken apparaat.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco's SDWAN-architectuur
- Algemeen begrip van oplossing, inclusief vManager-controller en cEdge (IOS-XE SD-WAN routers) en vEdge-apparaten (ViptelaOS-routers)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Vereiste basisinformatie

- Beschrijf het probleem en zijn impact op uw netwerk en gebruikers: Beschrijf een verwacht gedrag. Beschrijf in details waargenomen gedrag. Bereid een topologiediagram voor met het richten indien mogelijk, zelfs als dit met de hand wordt getekend.
- Wanneer is het probleem begonnen? Let op de dag en het tijdstip dat het probleem voor het eerst werd waargenomen/opgemerkt.
- Wat zou een mogelijke oorzaak van het probleem kunnen zijn? Document alle recente wijzigingen die zijn aangebracht voordat het probleem is begonnen. Let op alle specifieke acties of gebeurtenissen die zijn opgetreden en die het probleem hebben geactiveerd om te starten. Komt dit probleem overeen met andere netwerkgebeurtenissen of acties?
- Wat is de frequentie van het probleem? Was dit een eenmalige gebeurtenis? Zo niet, hoe vaak gebeurt dit probleem dan?
- Verstrek informatie over de betrokken inrichting(en): Als specifieke apparatuur wordt aangetast (niet willekeurig), wat hebben ze dan gemeen? System-IP en Site-ID voor elk apparaat. Als het probleem zich in een vManager-cluster voordoet, specificereert u de knooppunt details (als dit niet hetzelfde is voor alle knooppunten in het cluster). Voor algemene kwesties binnen de vManager GUI, neem alle screenshots op een bestand dat foutmeldingen of andere anomalieën/onevenwichtigheden toont die moeten worden onderzocht.
- Geef informatie over het gewenste resultaat van de TAC en uw prioriteiten: Wilt u zo snel mogelijk van de mislukking herstellen of de oorzaak van de mislukking ontdekken?

vManager

De hier besproken problemen zijn gebruikelijke probleemomstandigheden die voor vManager zijn gemeld, samen met nuttige output voor elk probleem dat moet worden verzameld naast een **admin-tech** bestand(en). Voor wolkenverschuilde controllers kan de TAC-ingenieur (Technical Assistance Center) toegang hebben tot het verzamelen van de vereiste **admin-tech**-uitgangen voor de apparaten op basis van de feedback in de gevraagde sectie voor basisinformatie als u hiervoor expliciet toestemming geeft. We raden echter aan om **admin-tech**-outputs op te nemen als de stappen die hier worden beschreven om ervoor te zorgen dat de gegevens die erin staan relevant zijn voor het moment van het probleem. Dit is specifiek waar als het probleem niet aanhoudend is, wat betekent dat het probleem kan verdwijnen tegen de tijd dat TAC is aangedaan. Voor controllers ter plaatse moet bij elke set gegevens ook een **admin-technologie** worden opgenomen. Zorg er bij een vManager-cluster voor dat u voor elk knooppunt in het cluster of alleen de getroffen knooppunt(s) een **admin-technologie** opneemt.

Laagheid/verzwakking

Probleemrapport: Langzaamheid bij de toegang tot de vManager GUI, vertraging bij het uitvoeren van bewerkingen binnen de GUI, algemene traagheid of traagheid die in vManager wordt gezien

Stap 1. Capture 2-3 instanties van een thread print, geef elk **thread-print** bestand een andere naam met een numerieke aanduiding na elk van deze exemplaren (let op het gebruik van de gebruikersnaam waarmee u in vManager in het bestandspad inlogt), bijvoorbeeld:

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

Stap 2. Meld u aan bij **vshell** en voer **vmstat** als volgt uit:

```
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:~$
```

Stap 3. Verzamel extra informatie uit de **vshell**:

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

Stap 4. Leg alle diagnostiek voor NMS-services vast:

```
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-fouten/problemen

Probleemrapport: API-oproepen leveren geen gegevens of de juiste gegevens op, algemene problemen bij het uitvoeren van vragen

Stap 1. Controleer het beschikbare geheugen:

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

Stap 2. Capture 2-3 instanties van een thread print met een tussenruimte van 5 seconden, hernoemen elk **thread-print** bestand met een numerieke aanduiding na elke run van de opdracht (let op het gebruik van de gebruikersnaam waarmee u in vManager inlogt in het bestandspad):

```
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
```

Stap 3. Verzamel details voor elke actieve HTTP-sessie:

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

Stap 4. Geef deze gegevens op:

1. Uitgevoerde API-oproepen
2. Inroepingsfrequentie
3. Inlogmethode (d.w.z. gebruik van één token om volgende API-oproepen of gebruik van basisauthenticatie uit te voeren om de oproep en dan uitlogging uit te voeren)
4. Wordt JSESSIONID opnieuw gebruikt?

Opmerking Vanaf 19.2 vManager software wordt alleen token-gebaseerde verificatie ondersteund voor API-oproepen. Zie deze [link](#) voor meer informatie over het genereren, tijdelijke versie en verlopen van een token.

Deep Packet Inspection (DPI) Status/Langzaamheid

Probleemrapport: Als DPI is ingeschakeld, kan de verwerking van statistieken traag zijn of traagheid veroorzaken in de vManager GUI.

Stap 1. Controleer de disk grootte die voor DPI binnen vManager is toegewezen door naar **Administratie > Instellingen > Statistische gegevensbank > Configuratie** te navigeren.

Stap 2. Controleer de indexstatus door de volgende CLI-opdracht van vManager uit te voeren:

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

Stap 3. Controleer of API-oproepen met betrekking tot DPI-stats extern worden uitgevoerd.

Stap 4. Controleer de I/O-status van de schijf met behulp van deze CLI-opdracht van vManager:

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

Sjabloondruppelfouten

Probleemrapport: Sjabloondruk of de update van de apparaatsjabloon mislukt of tijden.

Stap 1. Leg de knop **Config** en **Voorbeeld** vanaf vManager op voordat u op de knop **Apparaten** configureert (hier weergegeven navigatievoorbeeld) klikt:



Stap 2. Schakel `viptela.enabled.rest.log` in van de pagina met **logininstellingen** (dit moet worden

uitgeschakeld nadat u de vereiste informatie hebt opgenomen):

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

Stap 3. Als de sjabloon op het uitvoeren van een fout betrekking heeft op een NETCONF-probleem of een fout, schakelt u **viptela.enabled.device.netconf.log** in aanvulling op het logbestand REST in Stap 1. Let op dat dit logbestand ook uitgeschakeld moet worden nadat de resultaten uit Stap 3 en Stap 4 zijn opgenomen.

Stap 4. Probeer de mislukte sjabloon opnieuw toe te voegen via vManager en een **admin-technologie** op te nemen met deze CLI (leg dit voor elk knooppunt van een cluster vast):

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

Stap 5. Geef screenshots van de taak in vManager en de configuratie Diff om de misluktingsdetails te bevestigen, samen met alle CSV-bestanden die voor de sjabloon zijn gebruikt.

Stap 6. Neem details op over de fout en taak, inclusief de tijd van de mislukte druk, **systeem-ip** van het apparaat dat is mislukt, en foutmelding die u in de vManager GUI ziet.

Stap 7. Als een sjabloon op de drukfout optreedt met een foutbericht dat voor de configuratie door het apparaat zelf is gerapporteerd, verzamelt u ook een **admin-technologie** van het apparaat.

Cluster-gerelateerde problemen

Probleemrapport: Cluster instabiliteit die leidt tot tijdelijke instellingen, traagheid of andere anomalieën.

Stap 1. Leg de output van **server_configuraties.json** op van elk vManager knooppunt in de cluster. Bijvoorbeeld:

```
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"
}

```

Stap 2. Leg gegevens vast over welke services voor elk knooppunt is ingeschakeld of uitgeschakeld. Raadpleeg hiervoor **Beheer > Cluster Management** in de vManager GUI.

Stap 3. Bevestig onderligging bereikbaarheid op de clusterinterface. Hiervoor **ping <ip-adres>** van elk vManager-knooppunt in VPN 0 naar het IP-adres van de clusterinterface van de andere knooppunten.

Stap 4. Verzamel diagnostiek van alle NMS-services voor elk vManager-knooppunt in het cluster:

```

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

```

Edge (vEdge/cEdge)

De hier aan de orde zijnde kwesties zijn gemeenschappelijke problematische omstandigheden die voor de apparaten van de Rand samen met bruikbare output voor elk die moeten worden verzameld. Zorg ervoor dat voor elk probleem een **beheertechnologie** is verzameld voor alle benodigde en relevante Edge-apparaten. Voor wolkenverschuilde controllers kan TAC toegang hebben tot de vereiste admin-tech-uitgangen voor de apparaten, gebaseerd op de feedback in het **gevraagde** gedeelte van de **basisinformatie**. Maar net als met vManager moet u deze eerst vastleggen voordat u een TAC-case opent om er zeker van te zijn dat de gegevens die erin zitten relevant zijn voor het tijdstip van het probleem. Dit is specifiek waar als het probleem niet aanhoudend is, wat betekent dat het probleem kan verdwijnen tegen de tijd dat TAC wordt gebruikt.

Control-verbindingen die niet bestaan tussen apparaten en controllers

Probleemrapport: Controle-aansluiting die niet bestaat uit een vEdge/cEdge naar een of meer controllers

Stap 1. Identificeer de lokale/externe fout van de besturingsverbinding:

- Voor vEdge: uitvoer van **show control connecties-history** opdracht.
- Voor cEdge: output van **show sdwan control connectie-geschiedenis** opdracht.

Stap 2. Bevestig de status van de TLOC(en) en dat alle TLOC(s)'omhoog' komen:

- Voor vEdge: uitvoer van **show control local-Properties** opdracht.
- Voor cEdge: output van **show sdwan control local-Properties** opdracht.

Stap 3. Neem voor fouten rond tijdelijke uitgangen of aansluitingsfouten (d.w.z. DCONFAIL of VM_TMO) zowel op het randapparaat als op de controller in kwestie de besturingsplane op:

- Voor luchtverkeersleiders:

```
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
```

- Voor vEdge:

```
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
```

- Voor cEdge (opname hieronder veronderstelt dat het apparaat naar de CLI-modus is verplaatst en er is een toegangscontrolelijst (ACL) met de naam **CTRL-CAP** gemaakt om te filteren - zie meer details in het voorbeeld van de EPC-opname in het scenario **Application/Network Performance**):

```
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
```

Stap 4. Voor andere fouten die zijn waargenomen in de uitvoer van de verbindingsgeschiedenis en voor meer details over de beschreven kwesties, zie de volgende [handleiding](#).

Control-verbindingen tussen randapparatuur en controllers

Probleemrapport: Een of meer regelaansluitingen tussen een vEdge/cEdge en een of meer controllers. Dit kan frequent, intermitterend of willekeurig in de natuur zijn.

- De lijnkaarten van de controle zijn over het algemeen het resultaat van pakketverlies of het verzenden van kwesties tussen een apparaat en een controller. Vaak is dit gekoppeld aan **TMO-fouten**, afhankelijk van de richting van de mislukking. Controleer eerst de oorzaak van de flap om dit verder te controleren: Voor vEdge/controllers: uitvoer van **show control connecties-geschiedenis** opdracht. Voor cEdge: output van **show sdwan control connectie-geschiedenis** opdracht.
- Bevestig de toestand van de TLOC(s) en dat alle TLOC's opstaan wanneer de flakking plaatsvindt: Voor vEdge: uitvoer van **show control local-Properties** opdracht. Voor cEdge: output van **show sdwan control local-Properties** opdracht.
- Verzamel pakketvastlegging voor zowel de controller(s) als het randapparaat. Raadpleeg het gedeelte **Control-verbindingen die niet overeenkomen met het gedeelte Apparaat en controller** voor meer informatie over opnamparameters voor elke kant.

BFD-sessies (Bidirectional Forwarding Detection) (BFD) die niet ontstaan of flappen tussen Edge-apparaten

Probleemrapport: De BFD sessie is beneden of knippert op en neer tussen twee scherpste apparaten.

Stap 1. Verzamel de status van de BFD-sessie op elk apparaat:

- Voor vEdge: output van **show bfd sessieopdracht**.
- Voor cEdge: output van **show sdwan bfd sessieopdracht**.

Stap 2. Verzamel de tellingen van Rx en Tx van het pakket op elke randrouter:

- Voor vEdge: output van **show tunnel statistics bfd** opdracht.
- Voor cEdge: output van **show platform hardware qfp actieve optie bfd datapath sdwan summary** opdracht.

Stap 3. Als de tellers voor BFD zitting op één eind van de tunnel in de output hierboven niet verhogen, kunnen de opnamen met ACLs worden genomen om te bevestigen of pakketten lokaal worden ontvangen. Meer informatie hierover en andere validaties die kunnen worden uitgevoerd, kunt u [hier](#) vinden.

Apparaatcrashes

Probleemrapport: Apparatuur onverwacht opnieuw geladen en problemen met de stroom worden uitgesloten. Indicaties van het apparaat zijn dat het potentieel crasht.

Stap 1. Controleer het apparaat om te bevestigen dat er een crash of onverwachte herlading is waargenomen:

- Voor vEdge: uitvoer van de opdracht **reboogeschiedenis**.
- Voor cEdge: uitvoer van **show sdwan reboohistory** opdracht.
- In plaats hiervan kunt u ook **navigeren** naar **monitor > Network**, selecteert u het apparaat en vervolgens navigeer naar **systeemstatus > Opnieuw opstarten** om te bevestigen of er onverwachte herladingen zijn gezien.

Stap 2. Indien bevestigd, vang een adminetechnologie van het apparaat door vManager door in **Gereedschappen > Operationele Opdrachten** te navigeren. Selecteer eerst de knop **Opties** voor het apparaat en selecteer **Admin Tech**. Zorg ervoor dat alle vinkjes zijn ingeschakeld, die alle logbestanden en kernbestanden op het apparaat bevatten.

Toepassings-/netwerkprestaties die achteruitgaan of falen tussen locaties

Probleemrapport: De toepassing werkt niet/HTTP pagina's laden niet, traagheid/vertraging in prestaties, mislukkingen na het maken van beleid of configuratie veranderingen

Stap 1. Identificeer het bron/bestemming IP paar voor een toepassing of stroom die het probleem toont.

Stap 2. Bepaal alle apparaten van de Rand in het pad en verzamel een **admin-technologie** van elk tot vManager.

Stap 3. Neem een pakketvastlegging op de rand-apparaten op elke plaats voor deze stroom wanneer het probleem wordt gezien:

- Voor vEdge: Data Stream inschakelen onder **Beheer > Instellingen** voor het veld **Hostname**, voert u het systeem IP van vManager in. Voer voor **VPN 0** inZorg ervoor dat HTTPS is ingeschakeld onder de **allow-service** configuratie van de vManager VPN 0-interface. Volg de stappen [hier](#) om verkeer op de service-zijde VPN-interface op te nemen.
- Voor cEdge: Verplaats de cEdge(s) naar CLI-modus via **Configuratie > Apparaten > Wijzigen mode > CLI-modus** Specificeer in de cEdge(s) een uitgebreide ACL-modus om verkeer bidirectioneel aan te passen. Maak dit zo specifiek mogelijk om protocol en poort op te nemen om de grootte en gegevens in de opname te beperken.
- Configureer de [ingesloten pakketvastlegging](#) (EPC) voor de service-zijinterface in beide richtingen, met behulp van de ACL die onder b) is gemaakt om het verkeer te filteren. De opname kan worden geëxporteerd naar de PCAP-indeling en uit het vak worden gekopieerd. Er wordt hier een voorbeeldconfiguratie geboden voor Gigabit Ethernet0/0/0 op een router die gebruik maakt van een ACL met de naam **BROKEN-FLOW**:

```
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
```

- Configureer [Packet Trace](#) voor het verkeer in beide richtingen met behulp van de ACL die onder b) is gemaakt om het verkeer te filteren. Hieronder vindt u een voorbeeldconfiguratie:

```
debug platform packet-trace packet 2048 fia-trace
debug platform packet-trace copy packet input 13 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
```

Stap 4. Indien mogelijk, herhaal Stap 3 in een werkscenario voor vergelijking.

Tip: Als er geen andere manieren zijn om de corresponderende bestanden rechtstreeks van de cEdge te kopiëren, kunnen de bestanden eerst naar vManager worden gekopieerd met de hier beschreven methode. Start de opdracht op vManager:

aanvraag om SCP -P 830 <gebruikersnaam>@<cEdge systeem-IP>:/bootflash/<filename> uit te voeren.

Dit bestand wordt vervolgens opgeslagen in **/home/<gebruikersnaam>/<folder voor de gebruikersnaam die u hebt gebruikt om in te loggen op vManager.** Van daaruit kunt u Secure Copyright Protocol (SCP) of Secure File Transfer Protocol (SFTP) gebruiken om bestand te kopiëren van een vManager met behulp van een SCP/SFTP-client van derden of een Linux/Unix machine CLI met OpenSSH-hulpprogramma's.