Troubleshoot Common SD-WAN Control and Data Plane Issues

Contents

Introduction

This document describes how to start troubleshooting common Software Defined Wide Area Network (SD-WAN) control and data plane issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Catalyst solution.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

This article is designed as a runbook to provide a start place for debugging challenges seen in across production environments. Each section provides common use cases and probable data points to collect or look for when you are debugging these commonly seen issues.

Basic Configurations

Make sure the basic configurations are present on the router and that the device-specifc values are unique for each device in overlay:

System Configurations

<#root>

```
system
 system-ip <system –ip>
 site-id <site-id>
 admin-tech-on-failure
 organization-name <organization name>
 vbond <vbond-ip>
!
```

Example:

```
system
 system-ip 10.2.2.1
 site-id 2
 admin-tech-on-failure
 organization-name "TAC - 22201"
 vbond 10.106.50.235
!
```

Interface Configurations

```
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit

sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec
   color blue restrict
   no allow-service all
   no allow-service bgp
   no allow-service dhcp
   no allow-service dns
   no allow-service icmp
   allow-service sshd
   allow-service netconf
```

```
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
exit
```

Make sure that the router has aroute is available in the routing table to establish a control connection with the controllers (vBond, vManage and vSmart). You can use this command to see all routes installed in the routing table:

```
show ip route
```

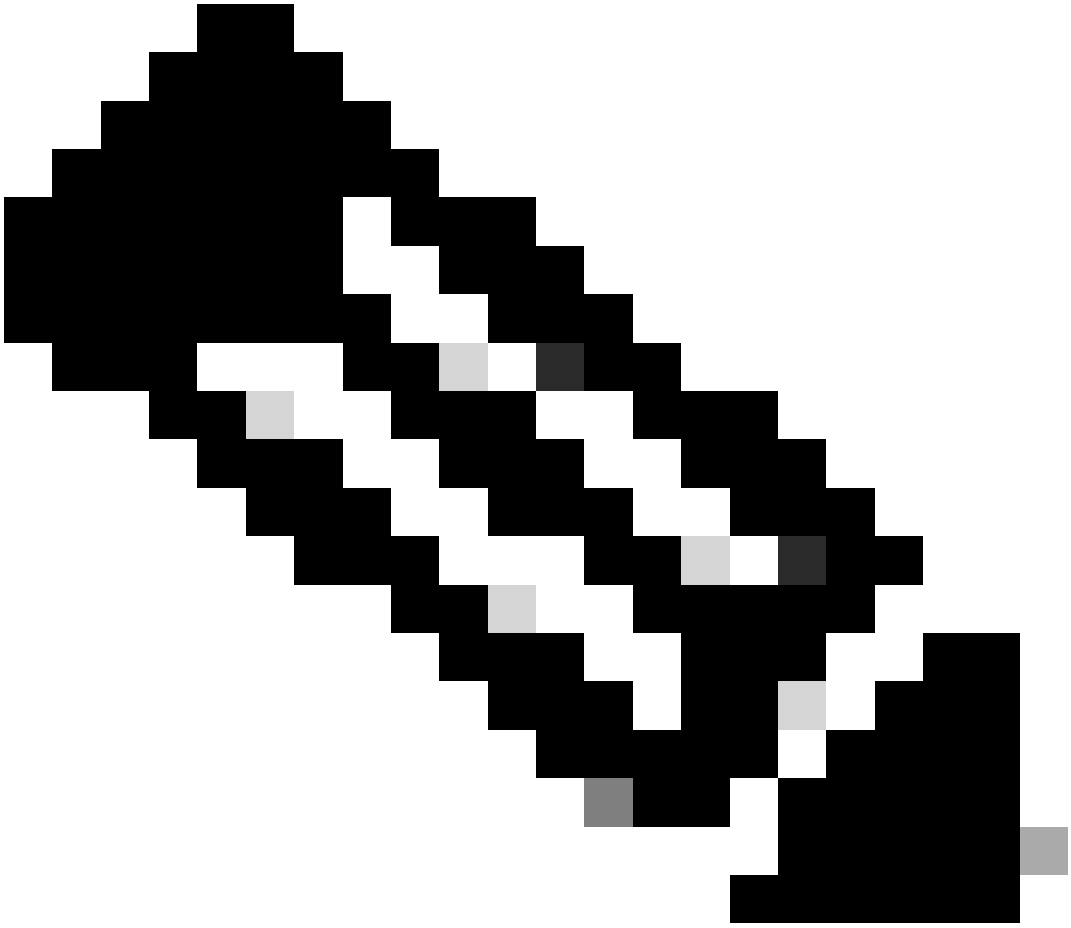
If you are using vBond FQDN, make sure DNS server or name server configured has an entry to resolve vBond hostname. You can check to see which DNS server or name-server is configured with this command:

```
show run | in ip name-server
```

Certificate

Verify that the certificate is installed on the router using this command:

```
show sdwan certificate installed
```



Note:If you are not using Enterprise certificates, the certificate is already available on the routers. For hardware platforms, the device certificates are built-in to the router hardware. For virtual routers, vManage acts as a certificate authority and generates the certificates for cloud routers.

If you are using Enterprise certificates on the controllers, make sure the root certificate of the Enterprise CA is installed on the router.

Verify the root certificates are installed on the router using these commands:

```
show sdwan certificate root-ca-cert
show sdwan certificate root-ca-cert | inc Issuer
```

Check the output of **show sdwan control local-properties** to make sure the required configurations and certificates are in place.

```
SD-WAN-Router#show sdwan control local-properties
```

```
personality                         vedge
sp-organization-name                TAC - 22201
organization-name                   TAC - 22201
root-ca-chain-status                Installed

certificate-status                  Installed
certificate-validity                Valid
certificate-not-valid-before        Nov 23 07:21:37 2015 GMT
certificate-not-valid-after         Nov 23 07:21:37 2025 GMT



enterprise-cert-status              Not-Applicable
enterprise-cert-validity            Not Applicable
enterprise-cert-not-valid-before    Not Applicable
enterprise-cert-not-valid-after     Not Applicable

dns-name                            10.106.50.235
site-id                             2
domain-id                           1
protocol                            dtls
tls-port                            0
system-ip                           10.2.2.1
chassis-num/unique-id               ASR1001-X-JAE194707HJ
serial-num                          983558
subject-serial-num                  JAE194707HJ
enterprise-serial-num               No certificate installed
token                               -NA-
keygen-interval                     1:00:00:00
retry-interval                      0:00:00:18
no-activity-exp-interval            0:00:00:20
dns-cache-ttl                       0:00:02:00
port-hopped                         TRUE
time-since-last-port-hop            0:00:01:26
embargo-check                       success
number-vbond-peers                  1

INDEX   IP                                      PORT
------------------------------------------------------
0       10.106.50.235                           12346

number-active-wan-interfaces        2


 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                           PUBLIC          PUBLIC PRIVATE         PRIVATE

INTERFACE                  IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0          10.197.240.4    12426  10.197.240.4    ::
GigabitEthernet0/0/1          10.197.242.10   12406  10.197.242.10   ::
```

When checking the output of **show sdwan control local-properties**, ensure that all of these criteria are met:

- The organization-name is reflected correctly.
- The certificate validity is valid at the time you are checking the output.

- The vBond FQDN/IP address is correct.

- System-ip/Site-id is correct.

- The vBond IP address is seen in the entry for “number-vbond-peers”. If the vBond IP address is not seen, then check that DNS is resolving for the vBond URL using the command **ping <vBond FQDN>**.

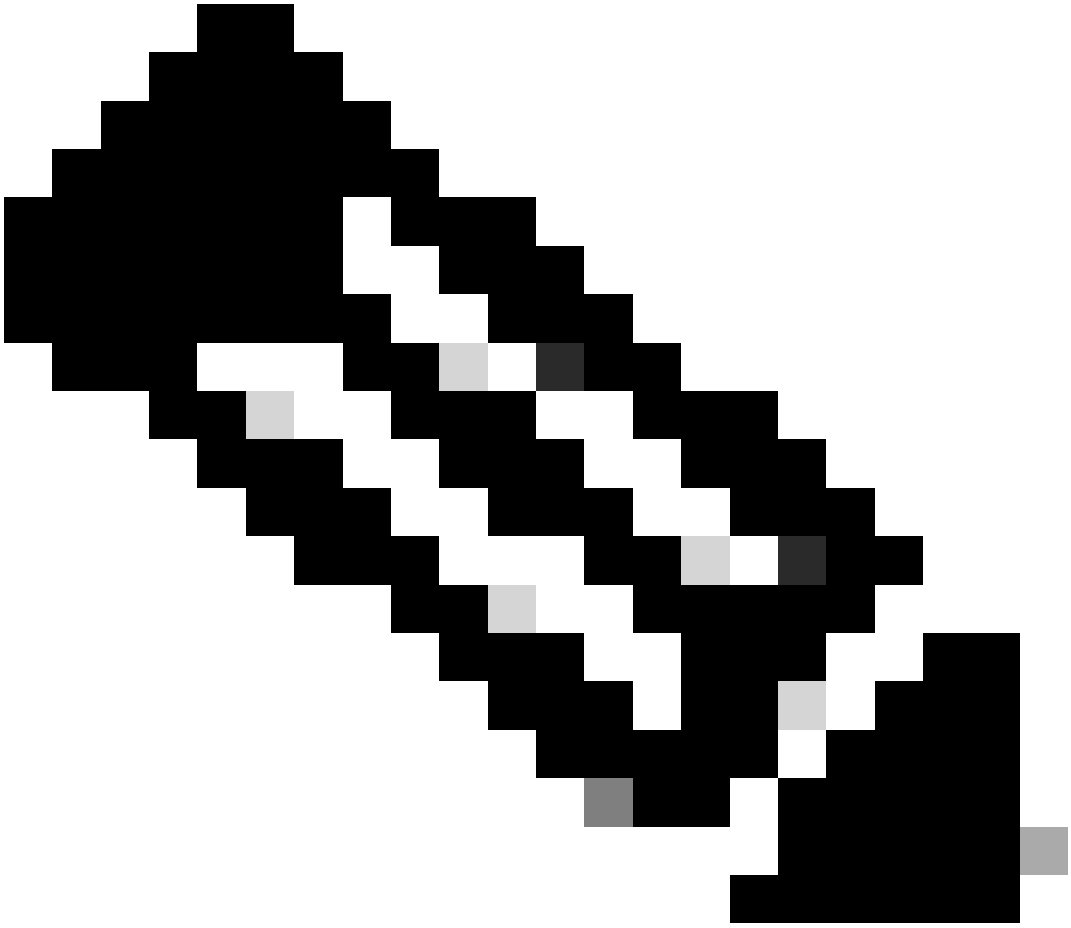
- The interfaces are mapped with correct color, IP address and the status of the interface is **UP**.
- The **MAX CNTRL** for the required interface to form control connection is not **0**.

Status of Control Connections

Check the status of control connection is using this command:

```
show sdwan control connection
```

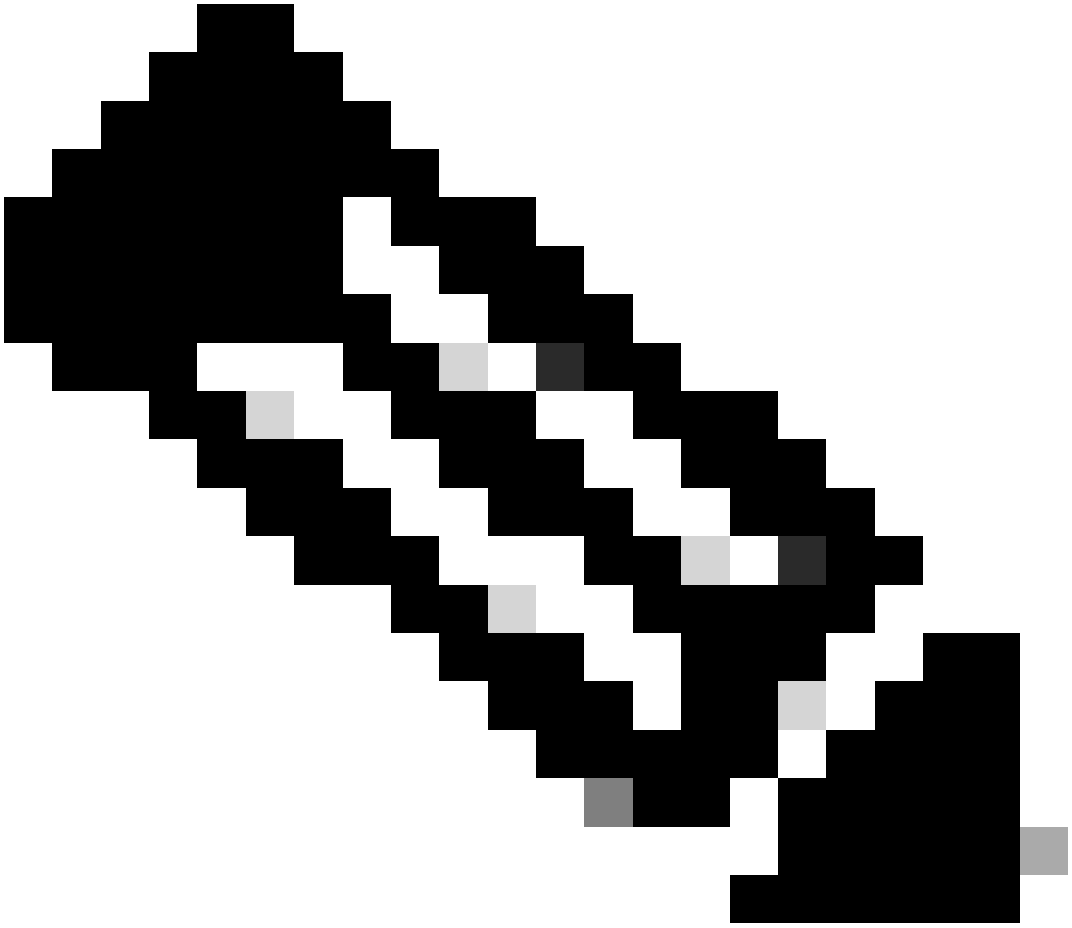
If all control connection are up, the device has a control connection formed to vBond, vManage and vSmart. Once the required vSmart and vManage connections are established, the vBond control connection is torn down.



Note: If there is only one vSmart in the overlay and **max-control connections** is set to the default value of **2**, a persistant control connection is maintained to vBond in addition to the expected connection to vManage and vSmart.

This configuration is available under the tunnel-interface configuration of the sdwan interface section. You can verify it using the command **show sdwan run sdwan**. If **max-control-connection** is configured to **0** on the interface, the router does not form control connection on that interface.

If there are 2 vSmarts in the overlay, the router forms a control connection to each vSmart on every Transport Locator (TLOC) color configured for control connections.



Note: The control connection to vManage is formed only on one interface color of the router in a scenario where router has multiple interfaces configured to form control connections.

```
SD-WAN-Router#show sdwan control connections
                                                                                                PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                            PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                                      PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------------------
vsmart  dtls 10.1.1.3        1          1      10.106.50.254                                   12346 10.106.50.
vbond   dtls  0.0.0.0        0          0      10.106.50.235                                   12346 10.106.50.
vmanage dtls 10.1.1.2        1          0      10.106.65.182                                   12346 10.106.65.
```

Troubleshooting Control Connections

In the output of **show sdwan control connections**, if all the required control connections are not up, verify the output of **show sdwan control connection-history**.

```
SD-WAN-Router#show sdwan control connection-history

Legend for Errors

ACSRREJ     - Challenge rejected by peer.              NOVMCFG    - No cfg in vmanage for device.
BDSGVERFL   - Board ID Signature Verify Failure.       NOZTPEN    - No/Bad chassis-number entry in ZTP.
BIDNTPR     - Board ID not Initialized.                OPERDOWN   - Interface went oper down.
BIDNTVRFD   - Peer Board ID Cert not verified.         ORPTMO     - Server's peer timed out.
BIDSIG     - Board ID signing failure.                 RMGSPR     - Remove Global saved peer.
CERTEXPRD   - Certificate Expired                      RXTRDWN    - Received Teardown.
CRTREJSER   - Challenge response rejected by peer.     RDSIGFBD   - Read Signature from Board ID failed.
CRTVERFL    - Fail to verify Peer Certificate.         SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch.            SSLNFAIL   - Failure to create new SSL context.
DCONFAIL    - DTLS connection failure.                 STNMODETD - Teardown extra vBond in STUN server 
DEVALC      - Device memory Alloc failures.            SYSIPCHNG - System-IP changed.
DHSTMO      - DTLS HandShake Timeout.                  SYSPRCH    - System property changed
DISCVBD     - Disconnect vBond after register reply.   TMRALC     - Timer Object Memory Failure.
DISTLOC     - TLOC Disabled.                           TUNALC     - Tunnel Object Memory Failure.
DUPCLHELO   - Recd a Dup Client Hello, Reset Gl Peer.  TXCHTOBD   - Failed to send challenge to BoardID.
DUPSER      - Duplicate Serial Number.                 UNMSGBDRG - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                      UNAUTHEL   - Recd Hello from Unauthenticated peer
HAFAIL      - SSL Handshake failure.                   VBDEST     - vDaemon process terminated.
IP_TOS      - Socket Options failure.                  VECRTREV   - vEdge Certification revoked.
LISFD       - Listener Socket FD Error.                VSCRTREV   - vSmart Certificate revoked.
MGRTBLCKD   - Migration blocked. Wait for local TMO.   VB_TMO     - Peer vBond Timed out.
MEMALCFL    - Memory Allocation Failure.               VM_TMO     - Peer vManage Timed out.
NOACTVB     - No Active vBond found to connect.        VP_TMO     - Peer vEdge Timed out.
NOERR       - No Error.                                VS_TMO     - Peer vSmart Timed out.
NOSLPRCRT   - Unable to get peer's certificate.        XTVMTRDN   - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections.       XTVSTRDN   - Teardown extra vSmart.
NTPRVMINT   - Not preferred interface to vManage.      STENTRY     - Delete same tloc stale entry.
HWCERTREN   - Hardware vEdge Enterprise Cert Renewed   HWCERTREV - Hardware vEdge Enterprise Cert Revok
EMBARGOFAIL - Embargo check failed

                                                                           PEER                        PEER
PEER     PEER      PEER              SITE        DOMAIN PEER              PRIVATE  PEER              PUBLIC
TYPE     PROTOCOL  SYSTEM IP         ID          ID     PRIVATE IP        PORT     PUBLIC IP         PORT
-------------------------------------------------------------------------------------------------------------
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vmanage  dtls     10.1.1.2           1           0      10.106.65.182     12346    10.106.65.182     12346
vsmart   dtls     10.1.1.3           1           1      10.106.50.254     12346    10.106.50.254     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
vbond    dtls      0.0.0.0           0           0      10.106.50.235     12346    10.106.50.235     12346
```

In the **show sdwan control connection-history** output, check these items:

- The type of controller to which the control connection is failing at a given timestamp.
- The error seen when the control connection failed. There are 2 columns for errors, Local Error, and Remote Error. Local error indicates the error generated by the router. Remote Error indicates the error generated by the respective controller. There is a legend of errors at the beginning of the output.

- Repeat count, indicates the number of times, the connection failed with the same reason.

Common Error Code Failures

- **DCONFAIL (DTLS connection Failure)**: This error indicates that there is a loss of DTLS packets which are exchanged between router and the respective controller due to which the DTLS handshake cannot be completed. To understand this better, you can setup simultaneous packet captures on router and respective controller. Different methods of setting up packet captures are shared in the Embedded Packet Capture section. While analyzing the packet captures, it is important to make sure the packets sent from one end are received at the other end without any modifications. If the packet sent from one end is not received at the other end, this indicates there is packet loss in the underlay circuit which needs to be verified with the service provider. More details on how to take a packet capture can be found in the Underlay Issues section.

- **BIDNTVRFD (Board ID Not Verified):** This error indicates the UUID and certificate serial number is not a valid entry in the controller vEdge list. You can check the output of the valid vedge list on the controllers using these commannds:

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

Usually, **BIDNTVRFD** is a remote error on the router because it is generated on the controller. On the respective controller, you can verify the log in the vdebug file located in the /var/log/tmplog directory using these commands:

```
vmanage# vshell
vmanage:~$ cd /var/log/tmplog/
vmanage:/var/log/tmplog$ tail -f vdebug
```

- **CRTVERFL (Certificate Verification Failed):** This error indicates the certificate sent by the peer could not be verified.

- If this is a local error on the router, then it indicates the certificate of the controller sent as a part of DTLS handshake could not be verified by the router. One of the common reasons for this is router does not have the root certificate of the certificate authority which signed the controller certificate. Verify the status of the certificate with these commands to ensure the requirerequired root certificate is present on the router.

```
show sdwan certificate root-ca-cert
show sdwan certificate root-ca-cert | inc Issuer
```

- If this error is a remote error on the router, check the vdebug log file on the respective controller to understand the cause using these commands:

```
vmanage# vshell
vmanage:~$ cd /var/log/tmplog/
vmanage:/var/log/tmplog$ tail -f vdebug
```

- **VB_TMO (vBond Timeout) / VM_TMO (vManage Timeout) / VP_TMO (vPeer Timeout) / VS_TMO (vSmart Timeout)**: These errors indicate that there was packet loss between the devices, which cause the control connection to time out. To understand this better, you can setup simultaneous packet captures on the router and respective controller. Different methods of setting up packet captures are shared in the Embedded Packet Capture section. While analyzing the packet captures, it is important to make sure the packets sent from one end are received at the other end without any modifications. If the packet sent from one end is not received at the other end,this indicates there is packet loss in the underlay circuit which needs to be verified with the service provider

For guidance on how to troubleshoot other control connection failure error codes, you can refer to this document:

Troubleshoot SD-WAN Control Connections

Underlay Issues

The tools used to troubleshoot packet loss in the underlay differs across different devices. For SD-WAN Controllers and vEdges router, you can use the tcpdump command. For Catalyst IOS® XE Edges, use Embedded Packet Capture (EPC) and Feature Invocation Array (FIA) trace.

To understand why control connections are failing and understand where the problem lies, you need to understand where the packet loss is happening. For example, if you have a vBond and Edge router not forming a control connection, this guide illustrates how to isolate the problem.

TCP Dump

```
tcpdump vpn 0 interface ge0/0 options "host 10.1.1.x -vv"
```

Based on the request and response of the packets the user can understand the device responsible for the drops. The tcpdump command can be used on all controllers and vEdge devices.

Embedded Packet Capture

Create an ACL on the device.

```
ip access-list extended TAC
10 permit ip host <edge-private-ip> host <controller-public-ip>
20 permit ip host <controller-public-ip> host <edge-private-ip>
```

Configure and start the monitor capture.

```
monitor capture CAP access-list TAC bidirectional
monitor capture CAP start
```

Stop the capture and export the capture file.

```
monitor capture CAP stop
monitor capture CAP export bootflash:<filename>
```

View the contents of the file in wireshark to understand the drops. You can find additional details at Configure and Capture Embedded Packet on Software .

FIA Trace

Configure the FIA trace.

```
debug platform condition ipv4 <ip> both
debug platform packet-trace packet 2048 fia-trace data-size 4096
debug platform condition start
```

View the fia phrase packet outputs.

```
debug platform condition stop
show platform packet-trace summary
show platform packet-trace summary | i DROP
```

If there is a drop, parse the FIA trace output for the dropped packet.

```
show platform packet-trace packet <packet-no> decode
```

To understand addtional FIA trace options, view this document: Troubleshoot with the IOS-XE Datapath Packet Trace Feature

The Determine Policy Drops on Catalyst SD-WAN Edge with FIA Trace video provides an example of

using FIA trace.

Generating Admin-Tech

Refer to Collect an Admin-Tech in SD-WAN Environment and Upload to TAC Case - Cisco

Related Information

Technical Support & Documentation - Cisco Systems