cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Cisco SD-WAN: The Usual Suspects

Common Culprits in WAN Edge Onboarding

Gina Cornett, Technical Marketing Engineer Technical Leader

BRKENT-2183

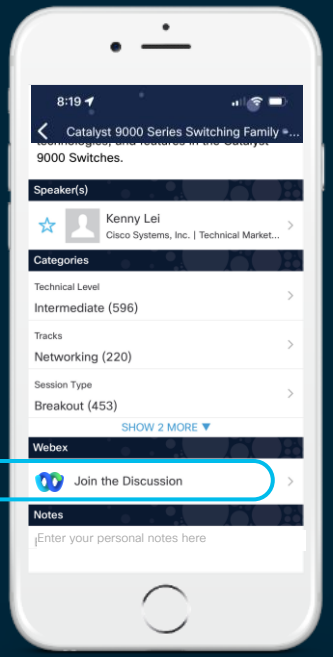
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2183

Webex spaces will be moderated by the speaker until June 17, 2022.

Agenda

- Introduction
- Onboarding stages
  - vBond control connections
  - vManage/vSmart control connections
  - WAN Edge data plane connections
- In what areas are the usual suspects lurking?
  - Reachability
  - Authentication
  - Authorization
- Conclusion

Introduction

Introduction

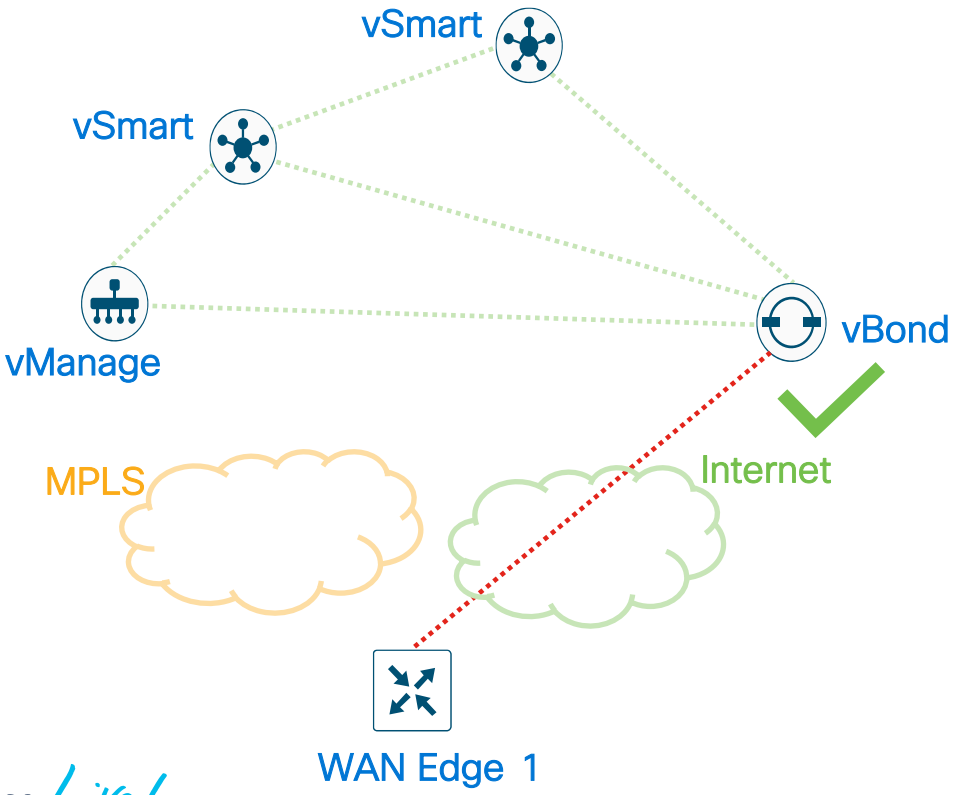
What's covered

- Focus on onboarding physical WAN Edge routers running IOS XE SD-WAN
- Help give a strategic and focused approach to identifying the usual suspects
- Recognize common pitfalls
- Reduce time for triaging of issues in onboarding
- Give tools to help troubleshoot common issues

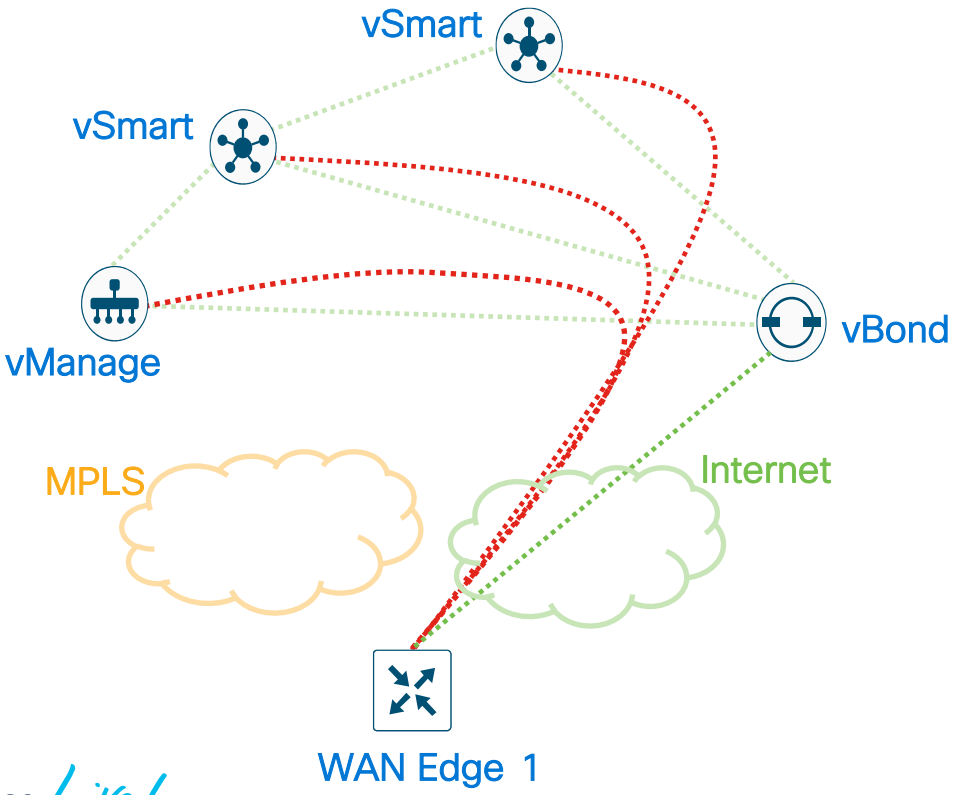
What's not covered

- Most SD-WAN design and foundational topics
- All onboarding issues - just addressing most common
- Tools for other troubleshooting/SD-WAN problem areas

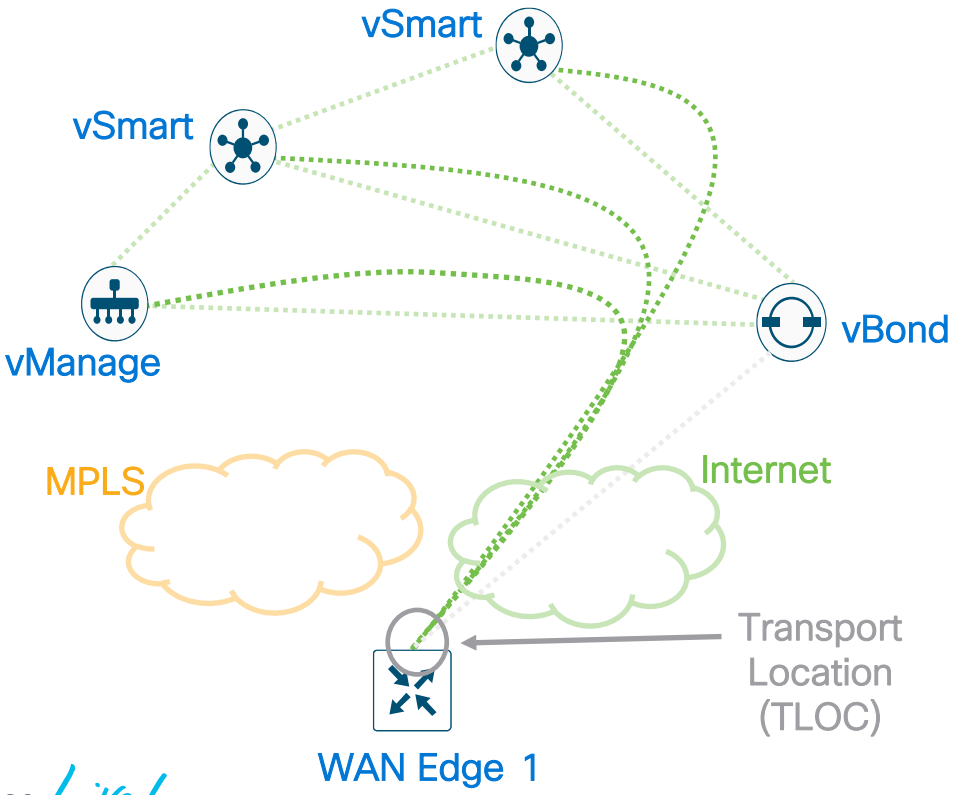
WAN Edge Onboarding



WAN Edge Onboarding



WAN Edge Onboarding

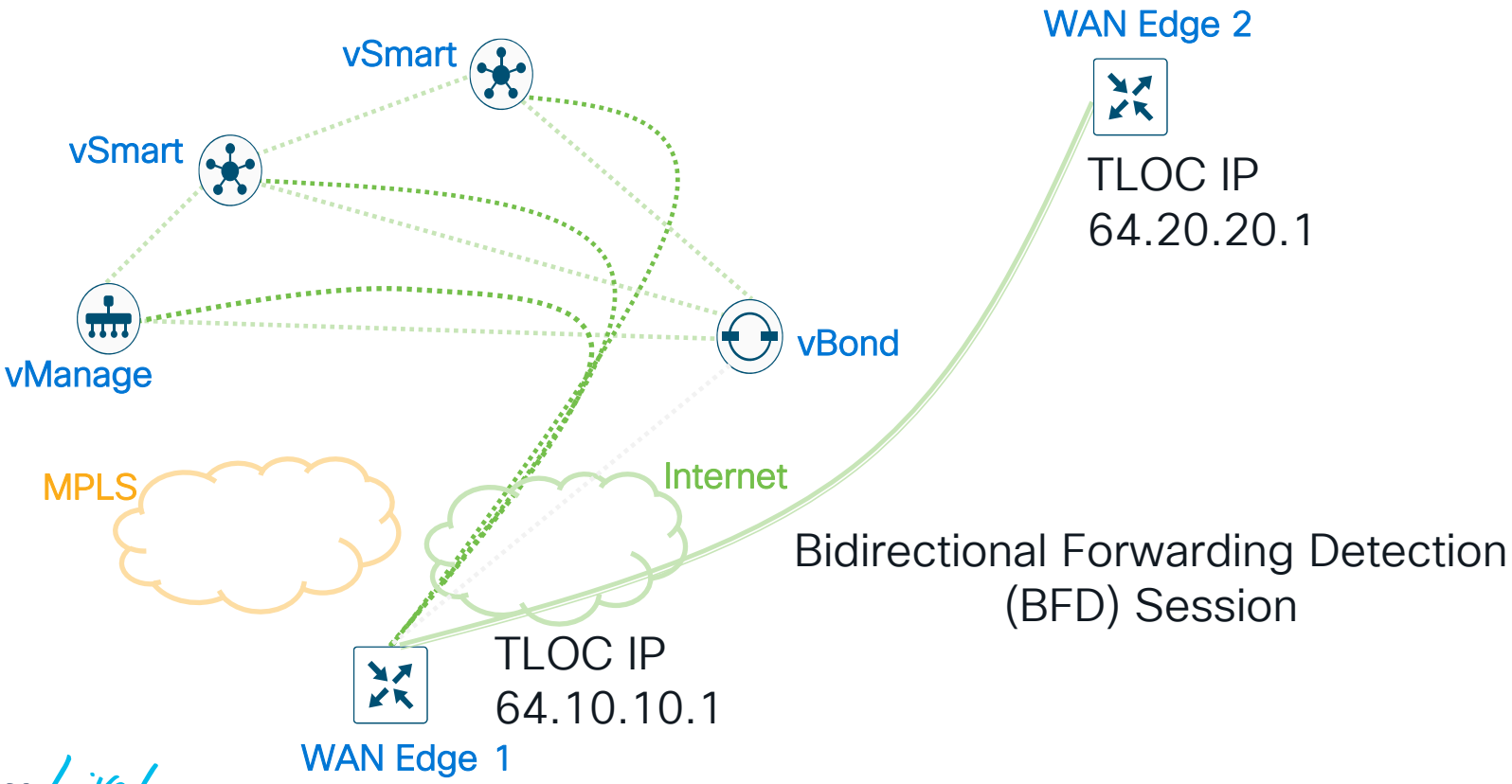


TLOC Information

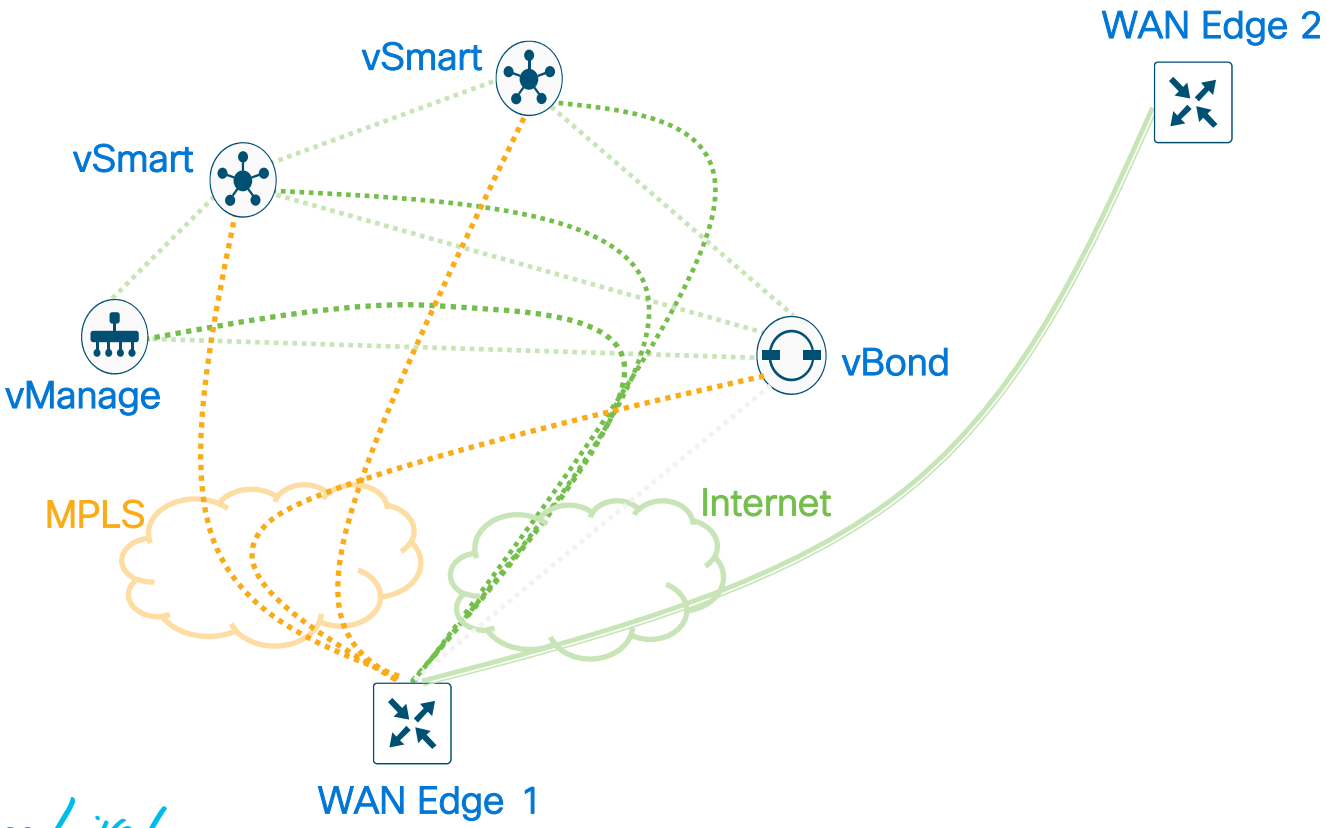
Routes

Encryption Keys

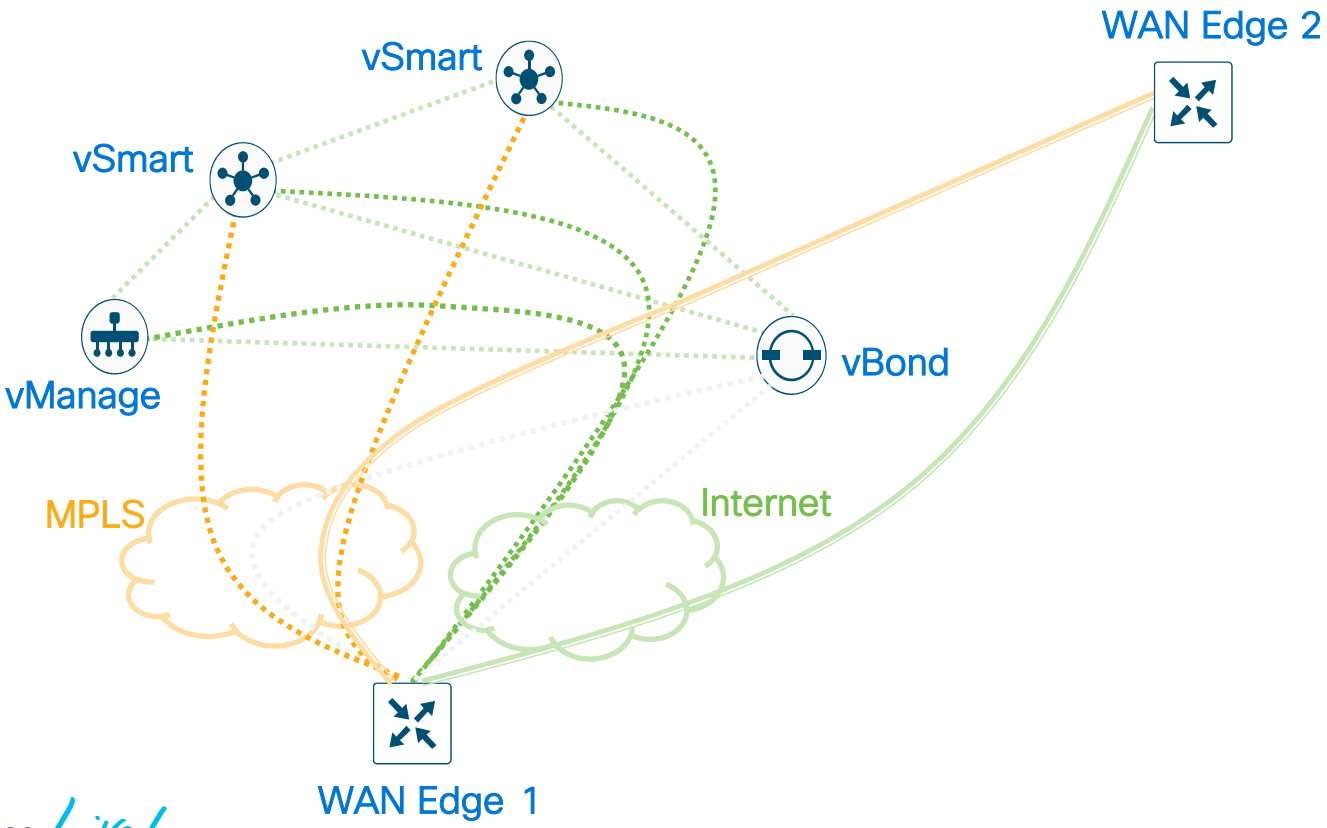
WAN Edge Onboarding



WAN Edge Onboarding



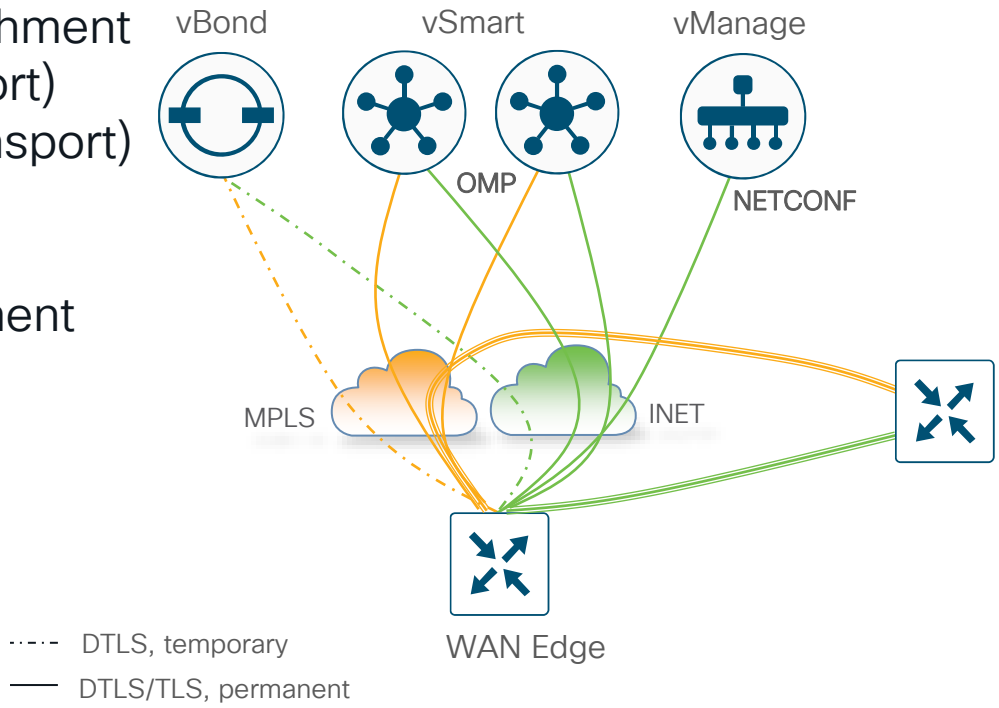
WAN Edge Onboarding



What Does Successful Onboarding Mean?

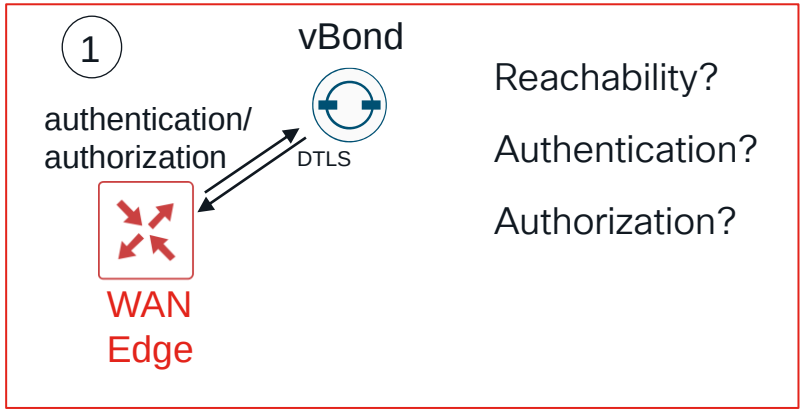
- Successful control plane establishment
  - vBond (transient per transport)
  - vManage (one over one transport)
  - vSmart (two per transport)

- Successful data plane establishment



vBond Control Connections

Bringing the SD-WAN Device into the Overlay



Where do the Usual Suspects Hide?

- Reachability
  - Is control traffic being initiated?
  - Is control traffic reaching the controller from the WAN Edge router?
  - Is control traffic returning to the WAN Edge router from the controller?
- Authentication?
  - Is authentication succeeding?
- Authorization?
  - Is authorization succeeding?

Show Sdwan Control Connections | Connection-History

WAN Edge (IOS XE SD-WAN)

```
WAN_EdgeG# show sdwan control connections
                                                                                PEER                          PEER
PEER     PEER PEER            SITE       DOMAIN PEER                 PRIV  PEER                  PUB
TYPE     PROT SYSTEM IP       ID         ID     PRIVATE IP           PORT  PUBLIC IP            PORT  LOCAL COLOR     PROXY STATE
-----------------------------------------------------------------------------------------------------------------------------------
vsmart   dtls 10.255.255.78   2          1      64.100.100.78        12346 64.100.100.78        12346 mpls            No    up
vsmart   dtls 10.255.255.79   2          1      64.100.100.79        12346 64.100.100.79        12346 mpls            No    up
vsmart   dtls 10.255.255.78   2          1      64.100.100.78        12346 64.100.100.78        12346 biz-internet    No    up
vsmart   dtls 10.255.255.79   2          1      64.100.100.79        12346 64.100.100.79        12346 biz-internet    No    up
vmanage dtls 10.255.255.74    2          0      64.100.100.74        12746 64.100.100.74        12746 mpls            No    up
```

```
WAN_EdgeG# show sdwan control connection-history

                                                                                PEER                  PEER
PEER PEER     PEER      DOMAIN SITE PEER            PRIVATE PEER              PUBLIC                                  LOCAL    REMOTE
TYPE PROTOCOL SYSTEM IP ID     ID   PRIVATE IP       PORT    PUBLIC IP         PORT    LOCAL COLOR    STATE       ERROR    ERROR
-----------------------------------------------------------------------------------------------------------------------------------
vbond   dtls   0.0.0.0   0    0   64.100.100.76    12346   64.100.100.76     12346   biz-internet   tear_down   DISCVBD  NOERR
vbond   dtls   0.0.0.0   0    0   64.100.100.76    12346   64.100.100.76     12346   mpls           tear_down   DISCVBD  NOERR
```

*vBond:

show **orchestrator** connections

Show **orchestrator** connections-history

*vManage/vSmart

show control connections

show control connections-history

Reachability: Is Control Traffic Being Initiated?

show sdwan control connections - WAN Edge (IOS XE SD-WAN)

```
WAN_EdgeG#show sdwan control connections

WAN_EdgeG#show sdwan control connections

WAN_EdgeG#show sdwan control connections

WAN_EdgeG#show sdwan control connections
```

NO!

```
WAN_EdgeG#show sdwan control connections

WAN_EdgeG#show sdwan control connections
                                                        PEER                    PEER
PEER     PEER PEER         SITE    DOMAIN PEER          PRIV  PEER              PUB
TYPE     PROT SYSTEM IP    ID      ID     PRIVATE IP    PORT  PUBLIC IP         PORT  LOCAL COLOR    PROXY STATE
-----------------------------------------------------------------------------------------------------------------
-
vbond    dtls 0.0.0.0      0       0      64.100.100.113  12346 64.100.100.113  12346 biz-internet    -    connect
```

YES!

Missing Configuration Parameters

For Control Traffic to be initiated from the WAN Edge Router:

- Is a vBond <domain name or IP address> configured?
- Is a DNS server or static host defined for vBond domain name?
- Is a tunnel interface is configured under the transport interface along with an IP address?
- Is a valid certificate and root-ca-chain certificate installed?
- Is an organization name is configured?
- Is a site-id is configured?
- Is a system IP address is configured?

Usual Suspects

Show Sdwan Control Local-Properties

WAN Edge (IOS XE SD-WAN)

```
WAN_EdgeG#show sdwan control local properties
personality                          vedge
sp-organization-name                 ENB-Solutions - 216151
organization-name                    ENB-Solutions - 216151
root-ca-chain-status                 Installed

certificate-status                   Installed
certificate-validity                 Valid
certificate-not-valid-before         Feb 15 19:08:30 2021 GMT
certificate-not-valid-after          Aug  9 20:58:26 2099 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                             vbond.cisco.net
site-id                              217
domain-id                            1
protocol                             dtls
tls-port                             0
system-ip                            10.255.255.217
chassis-num/unique-id                C8300-1N1S-6T-FLM250810CA
serial-num                           034300773184141193 1F
subject-serial-num                   FLM250810CA
```

*vManage/vSmart/vEdge:

```
show control local-properties
```

*vBond

```
show orchestrator local-properties
```

*DNS or Static Host Defined

```
WAN_EdgeG#show run | include name-server
ip name-server 208.67.222.222
```

```
WAN_EdgeE#show run | include host
hostname WAN_EdgeE
ip host vbond.cisco.net 64.100.100.113
```

*Tunnel Defined

```
WAN_EdgeE#show sdwan run
sdwan
<snip>
!
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec weight 1
   color biz-internet
```

Reachability: Is Traffic Reaching the Controller?

*WAN-Edge:

```
WAN_EdgeG# show sdwan control connections-history

PEER     PEER     PEER        SITE  PEER           PRIVATE  PEER           PUBLIC                                LOCAL     REMOTE
TYPE     PROTOCOL SYSTEM IP   ID    PRIVATE IP     PORT     PUBLIC IP      PORT    LOCAL COLOR   STATE   ERROR     ERROR
-----------------------------------------------------------------------------------------------------------------------------
vbond    dtls     0.0.0.0     0     64.100.100.76  12346    64.100.100.76  12346   biz-internet  connect DCONFAIL  NOERR
```

DCONFAIL - DTLS Connection Failure

*vBond:

YES!

```
vbond# show orchestrator connections-history

PEER  PEER     PEER       SITE PEER       PRIVATE PEER       PUBLIC                                    REPEAT
TYPE  PROTOCOL SYSTEM IP  ID   PRIVATE IP PORT    PUBLIC IP   PORT  REMOTE COLOR STATE  LOCAL/REMOTE    COUNT DOWNTIME
-----------------------------------------------------------------------------------------------------------------------------
unknown dtls   -          0    ::         0      64.100.1.34 48289 default   tear_down BIDNTVRFD/NOERR 8419  2022-05-22T22:40:07
```

MAYBE?

```
vbond# show orchestrator connections-history

PEER  PEER     PEER       SITE PEER       PRIVATE PEER       PUBLIC                                    REPEAT
TYPE  PROTOCOL SYSTEM IP  ID   PRIVATE IP PORT    PUBLIC IP   PORT  REMOTE COLOR STATE  LOCAL/REMOTE    COUNT DOWNTIME
-----------------------------------------------------------------------------------------------------------------------------
```

Reachability Problems – To/From the Controller

<u>On the WAN Edge Router</u>:

- Is the DNS server or IP static host defined correctly?
- Is the default route to the transport defined correctly?
- Is the default route next hop, DNS server, and vBond all reachable?
- If firewalls are present in the path, do firewall rules allow for the communication to succeed?
- Are TLOC subnets/IP addresses advertised properly into the underlay?

Usual Suspects

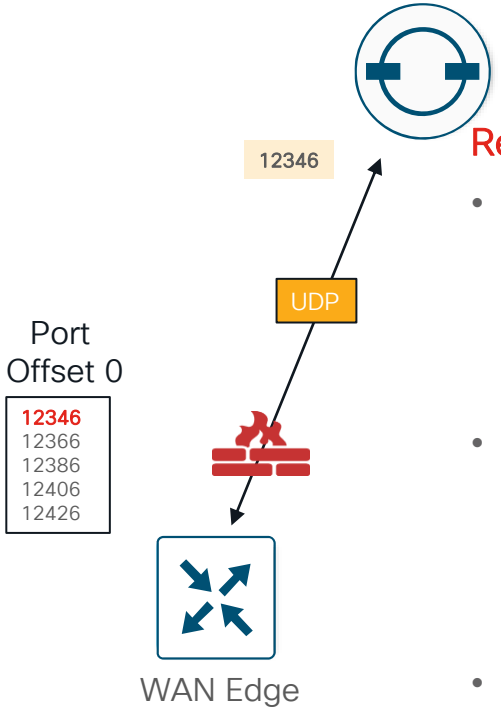
Firewalls Ports

vBond

vBond orchestrators always use DTLS tunnels to establish control connections with other devices, so they always use UDP. The UDP source and destination port for vBond is 12346. The port is configurable, but not recommended to be changed.

Ports 12346-12445

Port Offset 1	Port Offset 2	Port Offset 3		Port Offset 19
12347	12348	12349		12365
12367	12368	12369		12385
12387	12388	12389		12405
12407	12408	12409	...	12425
12427	12428	12429		12445



Default WAN Edge settings:
- No Port Offset
- DTLS

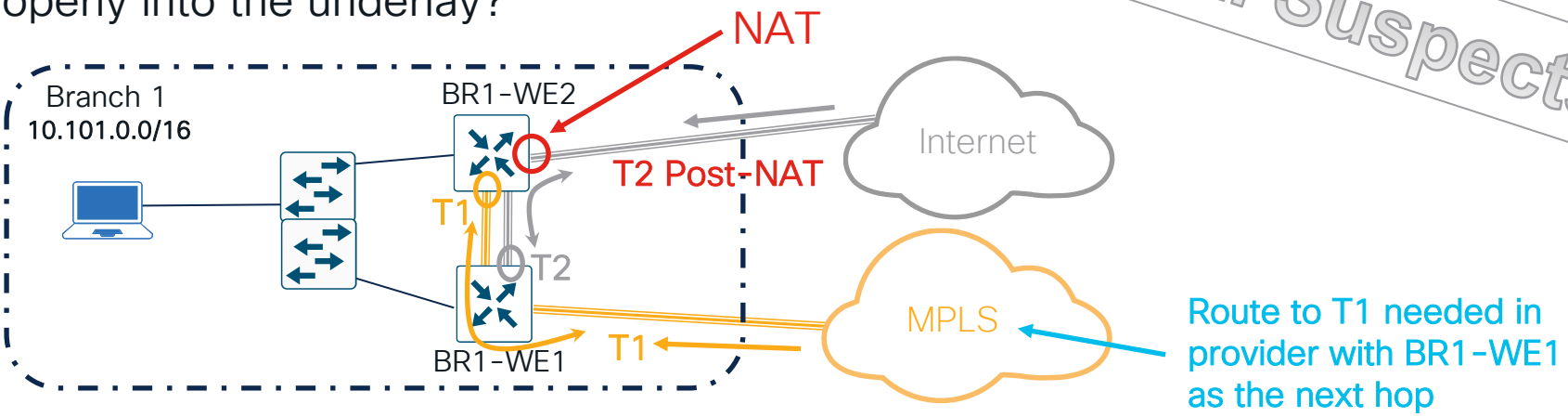
Red signifies first port used

- vBond IPs and port are static, It is recommended to permit UDP destination port 12346 to vBond and permit UDP source port 12346 from vBond.
- WAN Edges can port hop to establish a connection, its recommended to permit all 5 UDP ports to/from all WAN Edges. Additional ports are needed depending on the port offset used.
- For WAN Edge routers behind IOS XE SD-WAN routers using NAT on the outgoing interface, permit source UDP ports 5062-6085

Reachability - Is Control Traffic Returning?

*TLOCs on TLOC Extension Interfaces:
Are TLOC subnets/IP addresses advertised properly into the underlay?

Usual Suspects



T1: Static Route Needed in Provider Cloud or Routing Protocol between provider and WAN Edge to advertise T1 to provider
T2: NAT should be enabled on BR1-WE2 so T2 is reachable from the Internet provider

Troubleshooting Reachability (IOS XE SD-WAN)

- show ip route, show arp to verify default-route/next-hop
- Use ping to verify DNS, connectivity to vBond and default gateway (*ICMP needs to be allowed under the tunnel interface of the vBond in order to work)

```
WAN_EdgeE#ping vbond.cisco.net
Sending 5, 100-byte ICMP Echos to 64.100.100.113, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 29/30/31 ms
```

- Ping/extended ping option to generate diff size packets with options

```
WAN_EdgeJ2#ping ip 64.100.100.113 size 1500 dscp af41 source GigabitEthernet0/0/0
Sending 5, 1500-byte ICMP Echos to 64.100.100.113, timeout is 2 seconds:
Packet sent with a source address of 64.102.254.146
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/30/30 ms
```

- Traceroute to generate UDP port number with options

```
WAN_EdgeJ2#traceroute ip 64.100.100.113 port 12346 source GigabitEthernet0/0/0
Tracing the route to 64.100.100.113
VRF info: (vrf in name/id, vrf out name/id)
1 64.102.254.151 1 msec 2 msec 1 msec
2 64.100.100.113 3 msec 3 msec 4 msec
```

- Can utilize Embedded Packet Capture to view incoming control packets

Troubleshooting Reachability (Controllers)

- Verify connectivity to the WAN Edge router

```
vbond# ping source ge0/0 count 1 size 512 wait 1 64.100.217.2
Ping in VPN 0
PING 64.100.217.2 (64.100.217.2) from 64.100.100.113 : 512(540) bytes of data.
520 bytes from 64.100.217.2: icmp_seq=1 ttl=254 time=18.3 ms
```

- Nping can generate diff size packets and set port numbers on the packet

```
vbond# tools nping vpn 0 64.100.217.2 options "--udp -g 12346 --source-ip 64.100.100.113
Nping in VPN 0

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2022-06-09 02:18 UTC
SENT (0.0161s) UDP 64.100.100.113:12346 > 64.100.217.2:40125 ttl=64 id=26119 iplen=28
RCVD (0.0406s) ICMP [64.100.100.1 > 64.100.100.113 Communication administratively
   prohibited by filtering (type=3/code=13) ] IP [ttl=255 id=45588 iplen=56 ]
```

(see https://man7.org/linux/man-pages/man1/nping.1.html for information on options)

- Can utilize TCPDUMP to view incoming control packets

For Your Reference

Embedded Packet Capture (IOS XE SD-WAN)

https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-embedded-packet-capture/116045-productconfig-epc-00.html

- monitor capture CAP interface GigabitEthernet0/0/0 both (define capture location)
- monitor capture CAP match ipv4 protocol udp any eq 12346 any (associate a filter)
- monitor capture CAP start (start capture)
- monitor capture CAP stop (stop capture)
- show monitor capture CAP buffer [brief | detailed] (examine capture)
- monitor capture CAP export ftp://x.x.x.x/CAP.pcap (export capture)
- no monitor capture CAP (remove capture)

```
WAN_EdgeE#Show monitor capture CAP buffer brief
 ----------------------------------------------------------------------------
 #   size   timestamp     source             destination      dscp    protocol
 ----------------------------------------------------------------------------
   0   90    0.000000   64.100.100.113   ->  64.102.254.147   0  BE   UDP
   1 1066    0.100993   64.100.100.113   ->  64.102.254.147   0  BE   UDP
   2 1046    0.103998   64.100.100.113   ->  64.102.254.147   0  BE   UDP
```

For Your Reference

TCPDUMP (Controllers)

```
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 ]
```

- Specify an interface (may not get output specifying vpn only)
- Put options in “” , use ctrl c to stop
- Use –n to prevent converting ip to hostname and –nn to prevent name and port?
- -v shows more detail (IP header information, tos, ttl, offset, flags, protocol)
- -vv and –vvv show more detail in certain packet types
- Proto ex – udp, tcp icmp pim igmp vrrp esp arp
- Negate ! or not, && or and, || or or, use with () not (udp or icmp)
- https://www.tcpdump.org/manpages/tcpdump.1.html

For Your Reference

TCPDUMP (cont)

- Adapted from linux tcpdump command but does not support all available options. Snapshots of packets saved to a buffer, cannot export to a PCAP.
- Executes with -p flag, meaning 'no-promiscuous mode' - controller will only capture packets destined for the controller interface, including control packets, or broadcast pkts. Cannot capture data plane traffic.
- Executed with -s 128, snapshot length in Bytes. First x bytes of packet is captured.

TCPDUMP Examples

For Your Reference

tcpdump vpn 0 interface ge0/4 options "icmp or udp"

Listening on a specific port number:
tcpdump vpn 0 interface ge0/4 options “-vvv -nn port 12346”

Listening for a specific host (to/from that host): -e prints link-level header
tcpdump vpn 0 interface ge0/4 options “host 64.100.103.2 -vvv -nn -e”

Listening for a specific host with ICMP only
tcpdump vpn 0 interface ge0/4 options “host 64.100.103.2 && icmp”

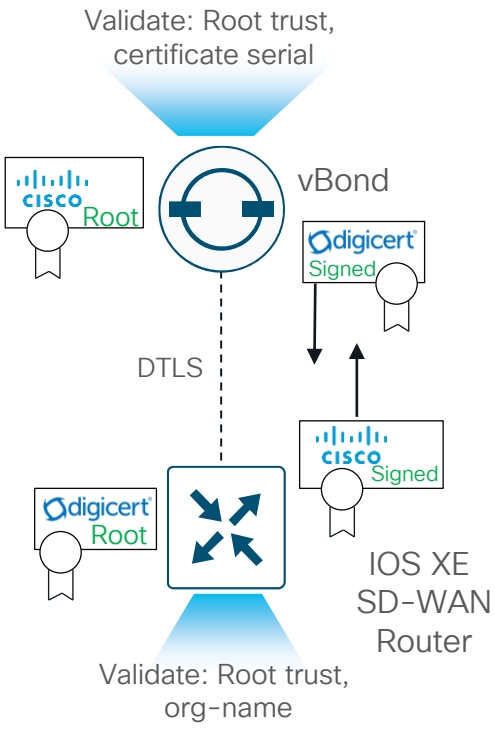
Filtering by Source and/or Destination
tcpdump vpn 0 interface ge0/4 options “src 64.100.103.2 && dst 64.100.100.75”

Filter on GRE-encapsulated traffic
tcpdump vpn 0 interface ge0/4 options “-v -n proto 47 "

Authentication/Authorization of WAN Edge Routers

vBond
- Validates the **trust for the certificate root** Certificate Authority (CA)
- Compares serial numbers against **authorized serial number list** distributed from vManage

WAN Edge Router
- Validates the **trust for the certificate root** Certificate Authority (CA)
- Compares the **Organization Name** of the received Certificate OU against the locally configured one.



Clock Time Off

Usual Suspects

```
vbond# show orchestrator connections-history

PEER      PEER     PEER         SITE   DOMAIN  PEER         PRIVATE PEER         PUBLIC
TYPE      PROTOCOL SYSTEM IP    ID     ID      PRIVATE IP   PORT    PUBLIC IP    PORT    REMOTE COLOR  STATE       LOCAL/REMOTE
-----------------------------------------------------------------------------------------------------------------------------------
unknown   dtls     -           0       0      ::            0      64.100.217.2 12386   default       challenge   RXTRDWN/CRTVERFL
```

CRTVERFL - Fail to verify Peer Certificate

*If time is outside certificate validity date, **Fail to Verify Peer Certificate Error** occurs

*Use **NTP** or **clock set** to set time on WAN Edge router

Root Certificate Missing

Usual Suspects

```
vbond# show orchestrator connections-history

PEER     PEER     PEER        SITE   DOMAIN  PEER        PRIVATE  PEER          PUBLIC
TYPE     PROTOCOL SYSTEM IP   ID     ID      PRIVATE IP  PORT     PUBLIC IP     PORT    REMOTE COLOR STATE      LOCAL/REMOTE
-----------------------------------------------------------------------------------------------------------------------------
unknown  dtls     -           0      0       ::          0        64.100.1.23   12386   default      tear_down  CRTVERFL/CRTVERFL
```

CRTVERFL - Fail to verify Peer Certificate

*Check for root certificate:

```
ios-xe-sdwan#show sdwan cert root-ca-cert | inc Subject:
```

*Extract root certificate chain from controller:

```
vbond# vshell
vbond:~$ cp /usr/share/viptela/root-ca.crt /home/admin/root-ca.crt
vbond:~$ exit
vbond# request upload vpn 512 ftp://admin:c1sco123@192.168.254.51/root-ca.crt root-ca.crt
```

*Copy and install root certificate chain on WAN Edge router:

```
ios-xe-sdwan#copy ftp://admin:c1sco123@192.168.254.51/root-ca.crt bootflash: vrf Mgmt-intf
ios-xe-sdwan#request platform software sdwan root-cert-chain install bootflash:root-ca.crt
```

Certificate Org Name Mismatch

Usual Suspects

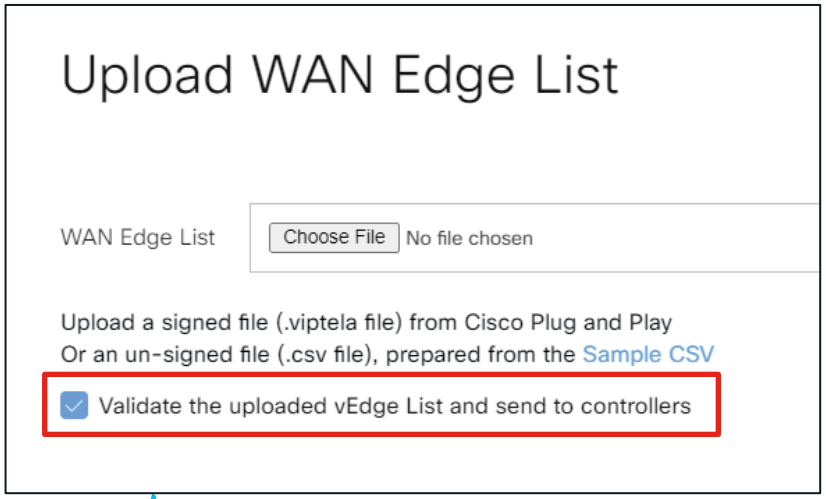
```
vEdge# show orchestrator connections-history

PEER      PEER      PEER         SITE   DOMAIN  PEER        PRIVATE  PEER            PUBLIC
TYPE      PROTOCOL  SYSTEM IP    ID     ID      PRIVATE IP  PORT     PUBLIC IP       PORT   REMOTE COLOR STATE      LOCAL/REMOTE
-----------------------------------------------------------------------------------------------------------------------------------
unknown   dtls      -            0      0       ::           0       64.102.254.147 12367  default      tear_down  BIDNTVRFD/NOERR
```

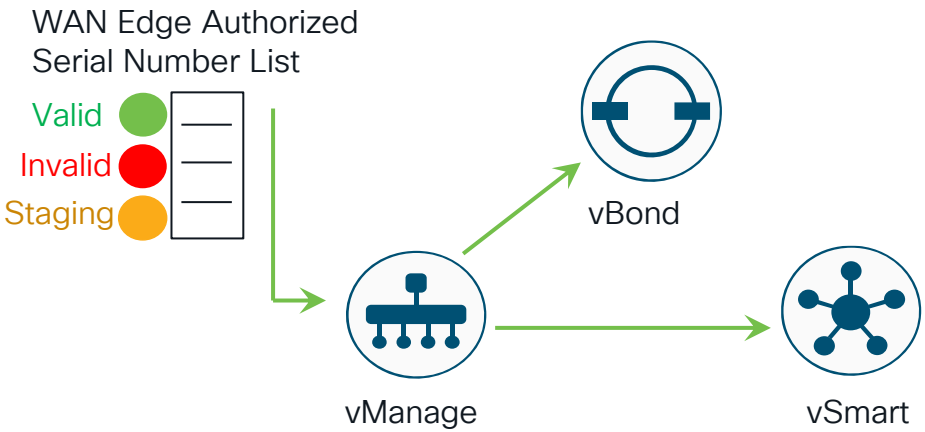
BIDNTVRFD - Peer Board ID Cert not verified

*WAN Edge compares the OU in the certificate of the controller to the locally configured Organization Name

Authorization of SD-WAN WAN Edge Routers

- Digitally-signed authorized serial number list file can be modified and retrieved from the Plug and Play Connect portal at http://software.cisco.com.
- Unsigned .csv file also now an option





Certificate Marked Invalid or Device Not in Authorized Serial Number List

Usual Suspects

```
vbond# show orchestrator connections-history

PEER      PEER     PEER                 SITE DOMAIN PEER        PRIVATE  PEER          PUBLIC
INSTANCE  TYPE     PROTOCOL SYSTEM IP   ID    ID    PRIVATE IP PORT     PUBLIC IP     PORT    REMOTE COLOR STATE     LOCAL/REMOTE
-----------------------------------------------------------------------------------------------------------------------------------
0         unknown  dtls     -           0      0       ::      0       64.100.217.2  5984    default     tear_down    BIDNTVRFD/NOERR
```

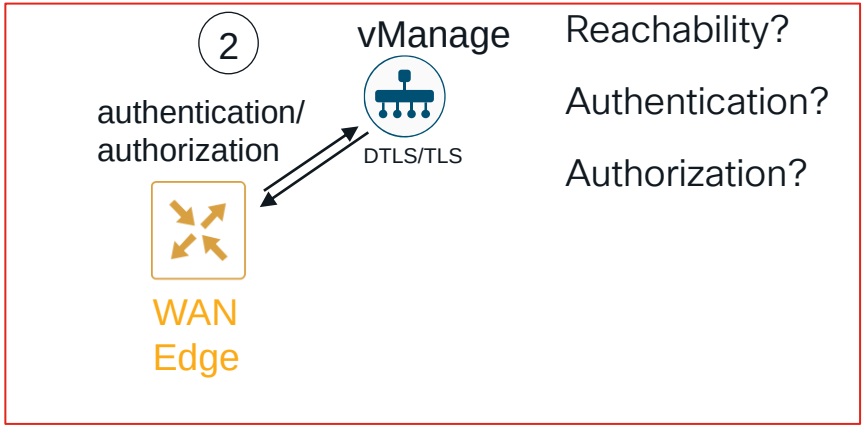
BIDNTVRFD - Peer Board ID Cert not verified

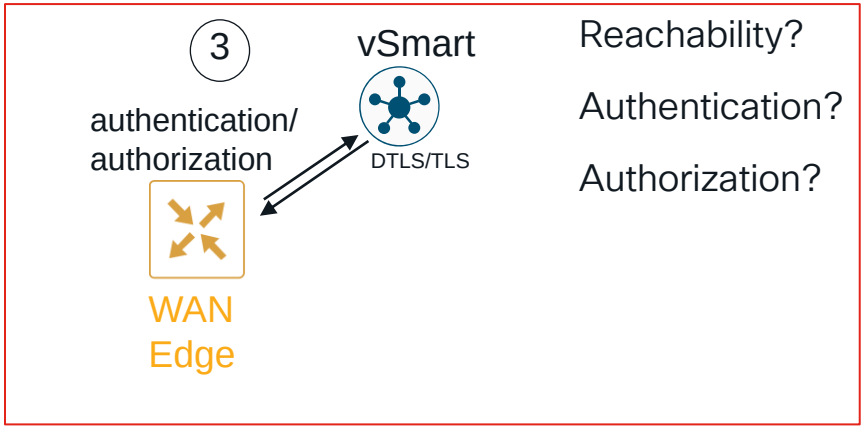
```
vbond# show orchestrator valid-vedges

CHASSIS NUMBER                          SERIAL NUMBER                     VALIDITY  ORG
-----------------------------------------------------------------------------------------------------------------------
11OG403180462                           100070F6                          valid     ENB-Solutions - 21615  N/A
11OG408180011                           10006E32                          valid     ENB-Solutions - 21615  N/A
```

```
IOS-XE-SDWAN#show sdwan control local-properties | include chassis-num|serial-num
chassis-num/unique-id C1111-4PLTEEA-FGL223911LK serial-num 016E9999
```

vManage/vSmart Control Connections

Bringing the SD-WAN Device into the Overlay





Public vs Private IP address

- Applies to WAN Edge routers and controllers (except for vBond):

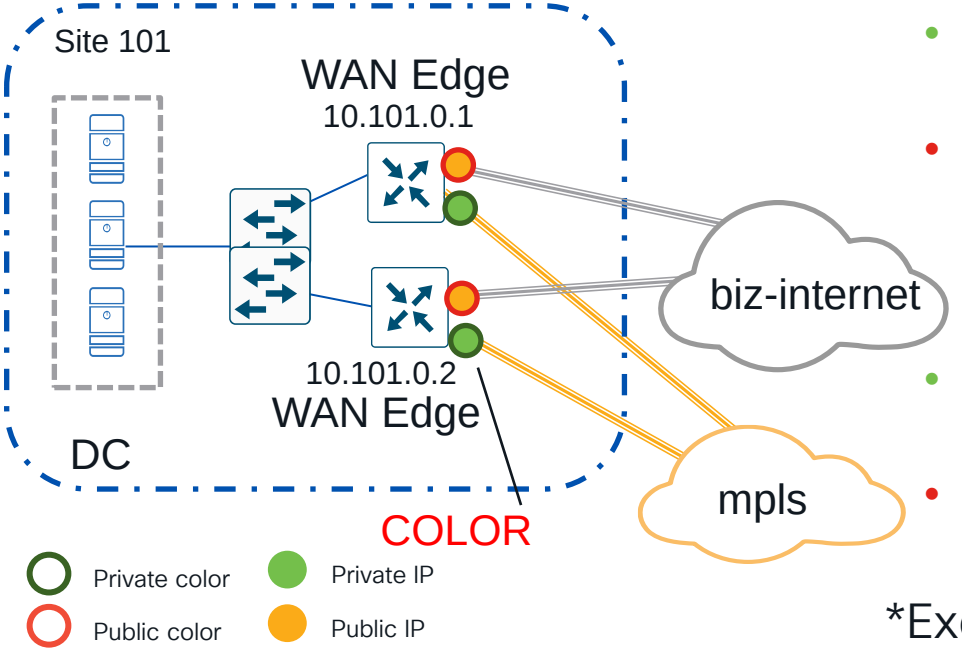
- Every TLOC has both public and private IP address attributes:
  - Private IP Address:
    IP address assigned to the interface of the SD-WAN device. This is the pre-NAT address and can be a publicly routable IP address or private (RFC 1918) IP address

  - Public IP Address:
    Post-NAT IP address that can be either a publicly routable IP address or a private (RFC 1918) IP address. Public IP address is from perspective of vBond.

*In absence of NAT, private and public IP addresses are the same

Role of Color on WAN Transport Interfaces

- Colors identify a transport as private or public
- Dictates the use of either private or public IP address for communicating



- Private colors are used in places with no NAT addressing
- Public colors used for public networks or where you use public IP addressing, either natively or through NAT

- Private to private color uses private IP address for communication
- Public to private or public uses public IP address for communication

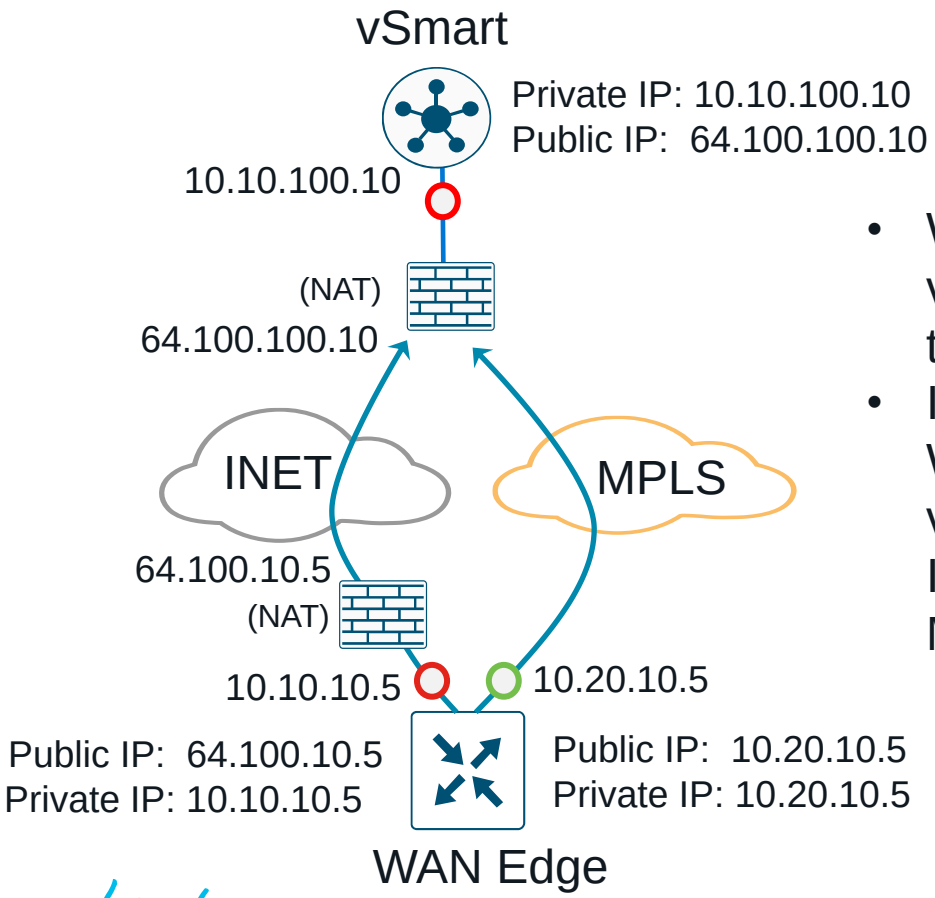
*Exception: Devices with the same site-ID use private IP addresses to communicate

Public vs Private Color

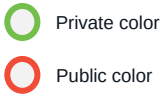
- Private Colors: metro-ethernet, mpls, private1, private2, private3, private4, private5, and private6

- Public Colors: 3g, biz-internet, public-internet, gold, green, red, silver, blue, bronze, lte, custom1, custom2, custom3, default

Public/Private IP Address Example



- WAN Edge reaches vSmart through vSmart public IP address on both transports
- If vSmart used a private color, then WAN Edge reaches vSmart through vSmart public IP address on Internet and private IP address on MPLS



Reachability

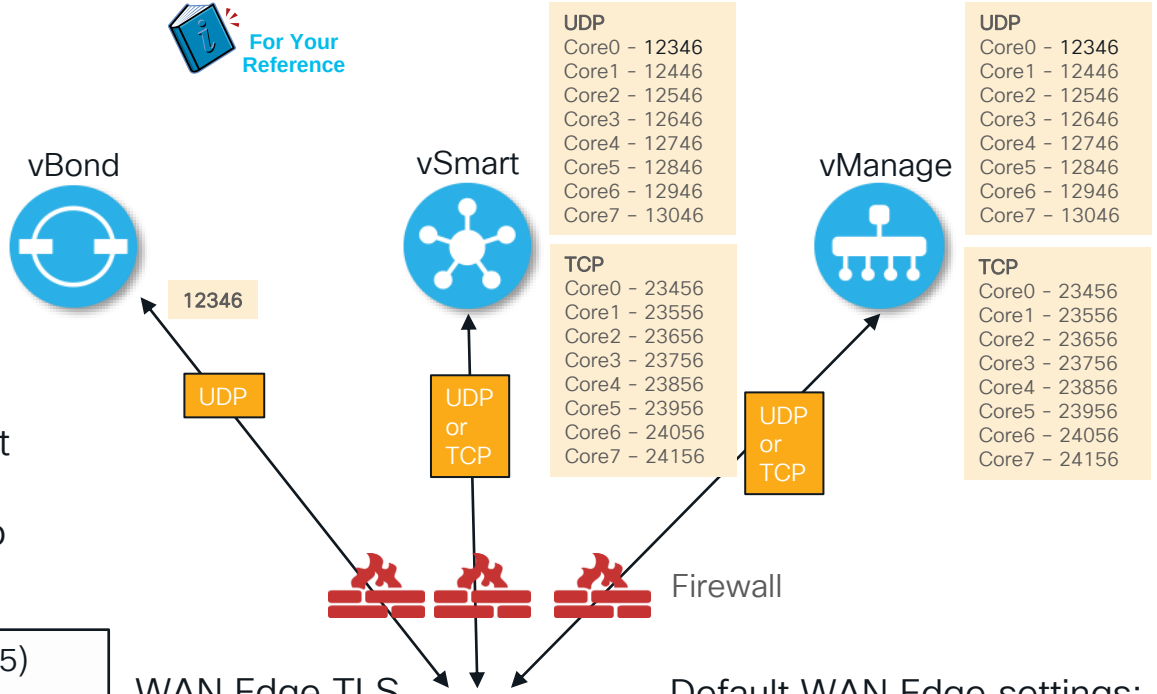
- Is the WAN Edge router trying to reach the vManage or vSmart controllers using the correct IP address?
- If firewalls are present in the path, do firewall rules allow for the communication to succeed?

Usual Suspects

Firewalls Ports

Controllers – DTLS or TLS

The vManage NMS and vSmart controllers can run on a virtual machine (VM) with up to eight cores. The cores are designated as Core0 through Core7. Each core is allocated separate base ports for control connections. Default setting is DTLS (using UDP), but TLS (using TCP) can be configured. WAN Edge router connection hashes to one of the control ports.



WAN Edge DTLS (UDP Ports 12346-12445)

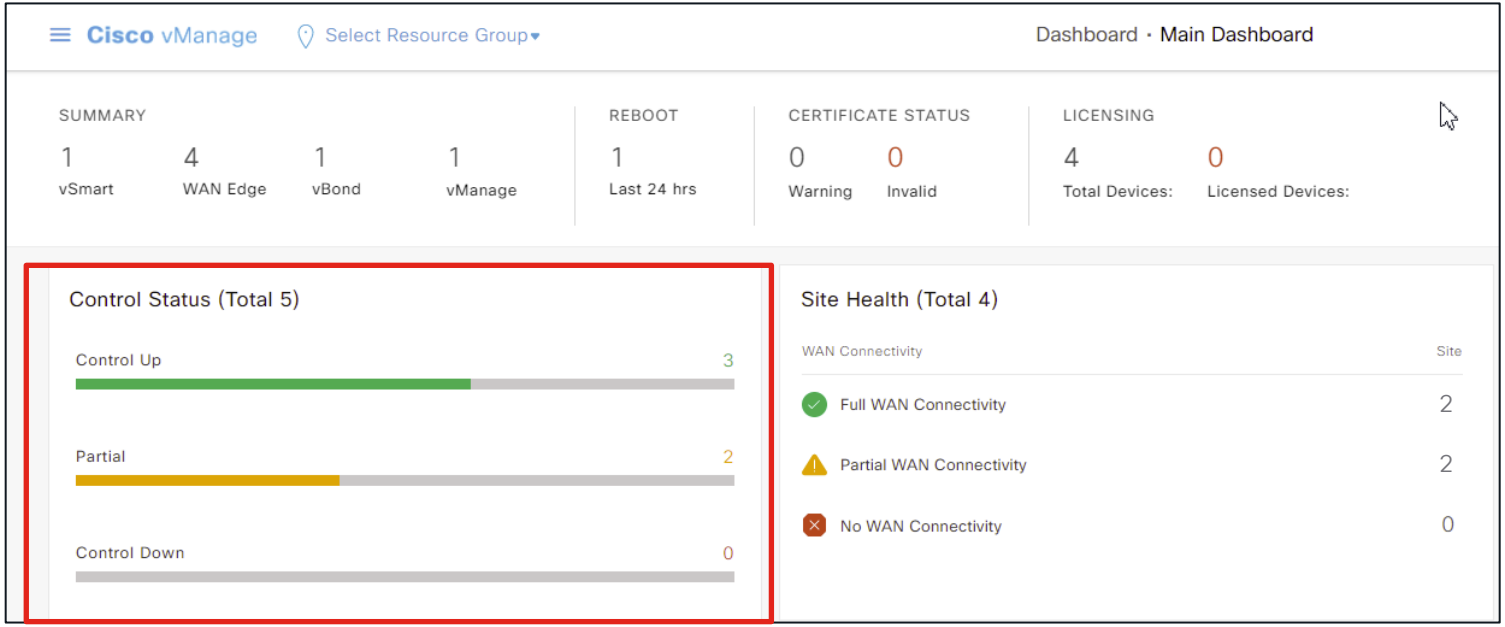
Port Offset 0	Port Offset 1	Port Offset 2	Port Offset 3		Port Offset 19
12346	12347	12348	12349		12365
12366	12367	12368	12369		12385
12386	12387	12388	12389		12405
12406	12407	12408	12409	...	12425
12426	12427	12428	12429		12445

WAN Edge TLS
TCP random port > 1024 (ephemeral port numbers)

Default WAN Edge settings:
- No Port Offset
- DTLS

*If only one side is TLS, TLS is used for the connection

vManage Status



Indicates vSmart control plane connections

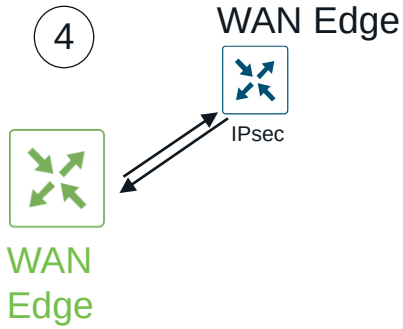
Control up (all required vSmart control connections up)

Partial (some required vSmart control connections up)

Control Down (all vSmart connections are down or no connection to vManage)

WAN Edge Data Plane Connections

Bringing the SD-WAN Device into the Overlay



Reachability?

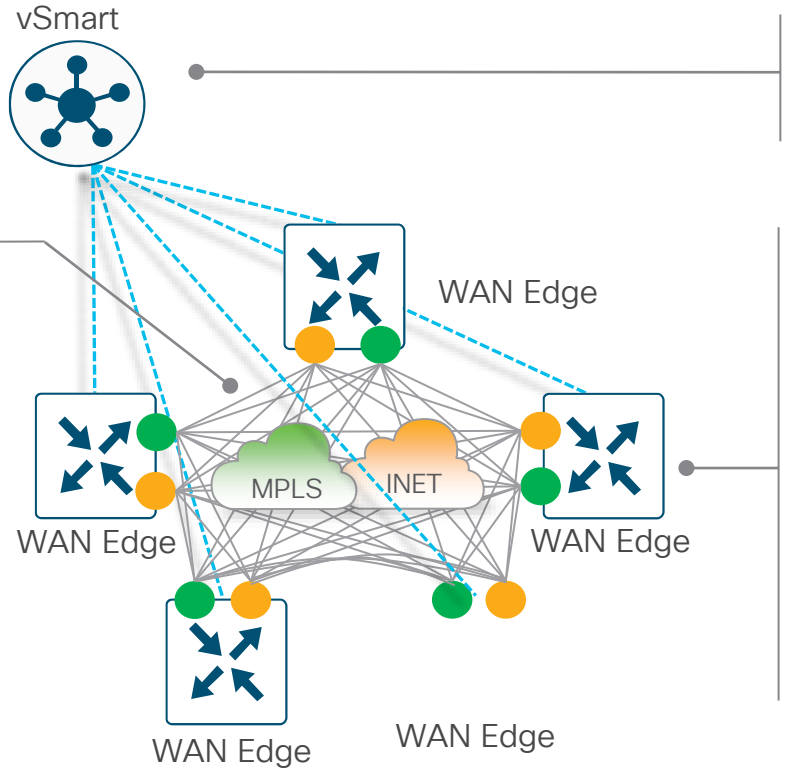
~~Authentication?~~

~~Authorization?~~

Data Plane Establishment

SD-WAN fabric between tunnel endpoints

*Note that TLOCs try to connect to all other TLOCs regardless of color unless the **restrict** keyword in used



vSmarts advertise TLOC routes and encryption keys to WAN Edges in OMP updates

TLOC Routes and encryption keys are advertised to vSmarts in OMP updates

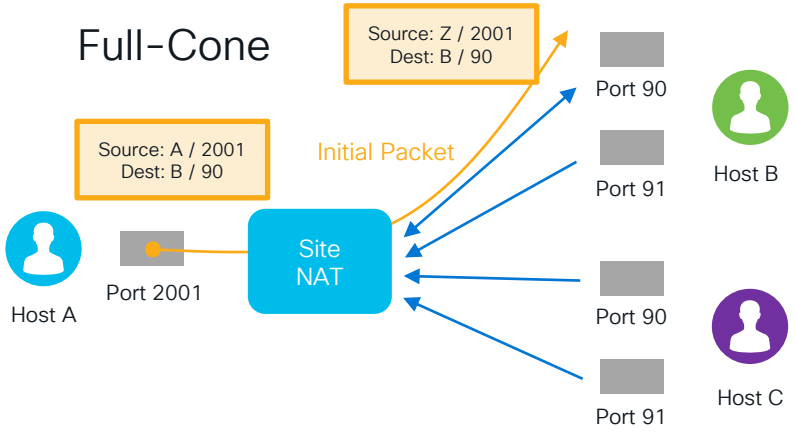
Local Routes
- TLOCs (SD-WAN tunnel endpoints)

Security Context
- IPSec Encryption Keys

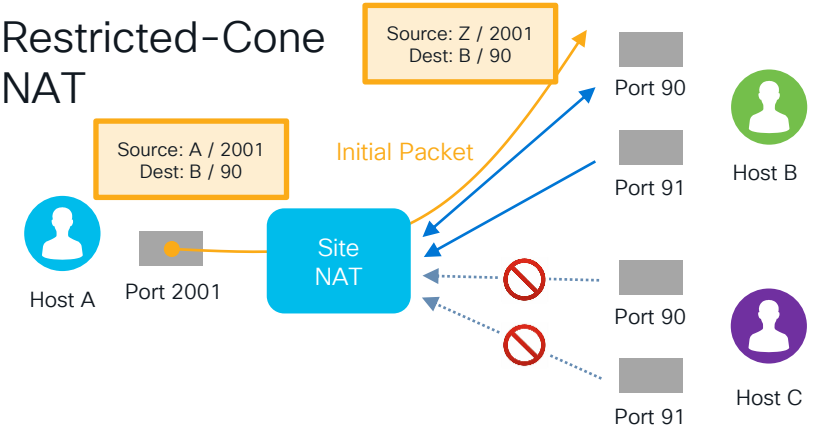
Transport Locator (TLOC) — OMP — IPSec Tunnel

NAT Considerations

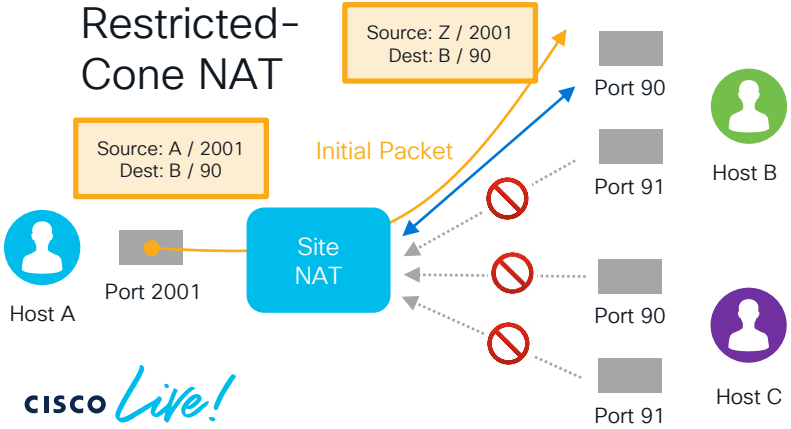
Full-Cone



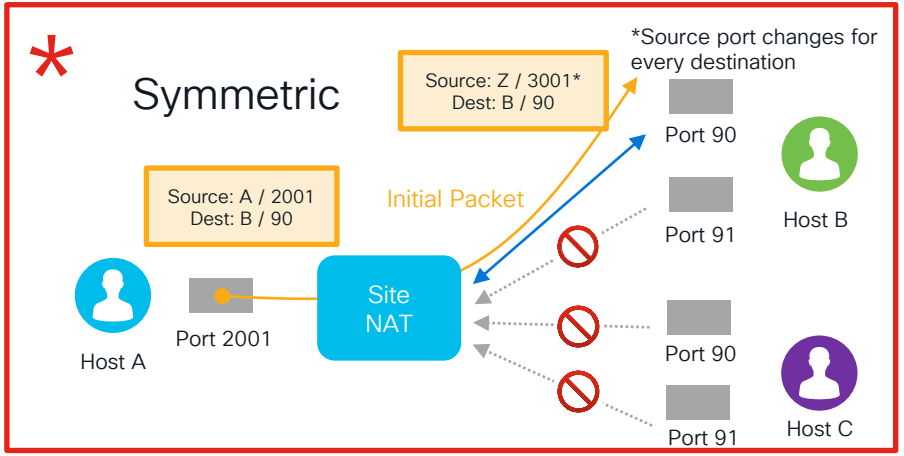
Restricted-Cone NAT



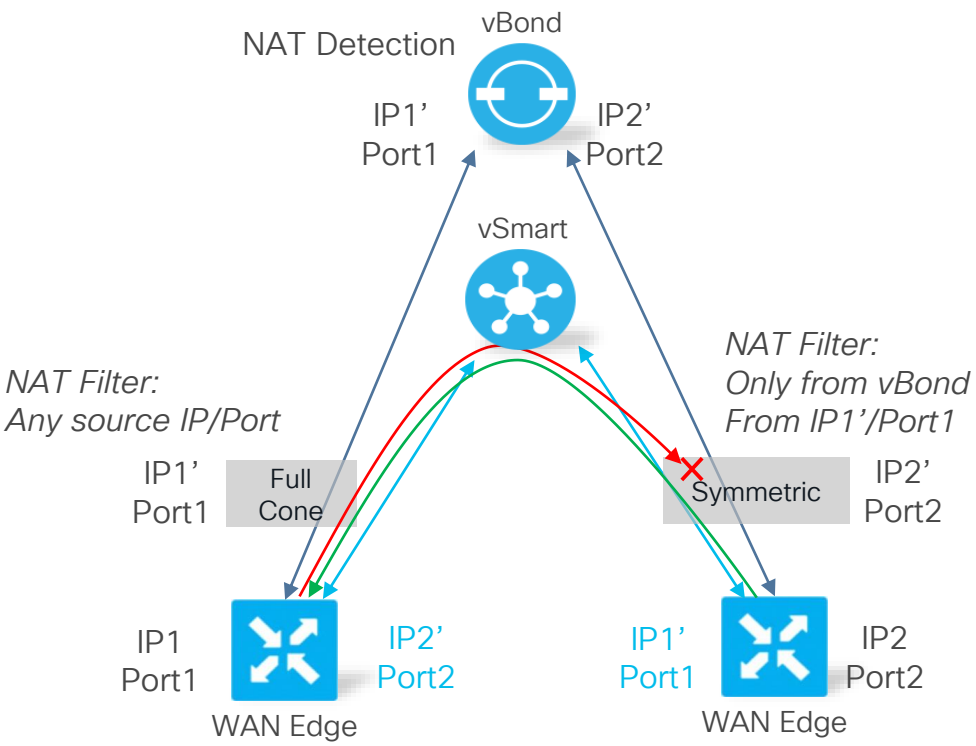
Port-Restricted-Cone NAT



Symmetric



NAT Traversal – Full Cone and Symmetric



Successful IPSec connection

- vBond discovers post-NAT public IP and communicates back to WAN Edge routers
- WAN Edge routers notify vSmart of their post-NAT public IP address
- Symmetric NAT devices enforce filter
  - Only allows traffic from vBond
- WAN Edge behind symmetric NAT reaches out to remote WAN Edge behind Full Cone NAT
  - NAT entry created with filter to allow remote WAN Edge return traffic
  - Remote WAN Edge will learn new symmetric NAT source port (data plane learning)

NAT Traversal Combinations

WAN Edge A	WAN Edge B	IPSec Tunnel Status	
Public IP (No NAT)	Public IP (No NAT)	●	★
Full Cone	Full Cone	●	★
Full Cone	Port/Address Restricted	●	
Port/Address Restricted	Port/Address Restricted	●	
Public	Symmetric	●	
Full Cone	Symmetric	●	★
Symmetric	Port/Address Restricted	●	
Symmetric	Symmetric	●	★

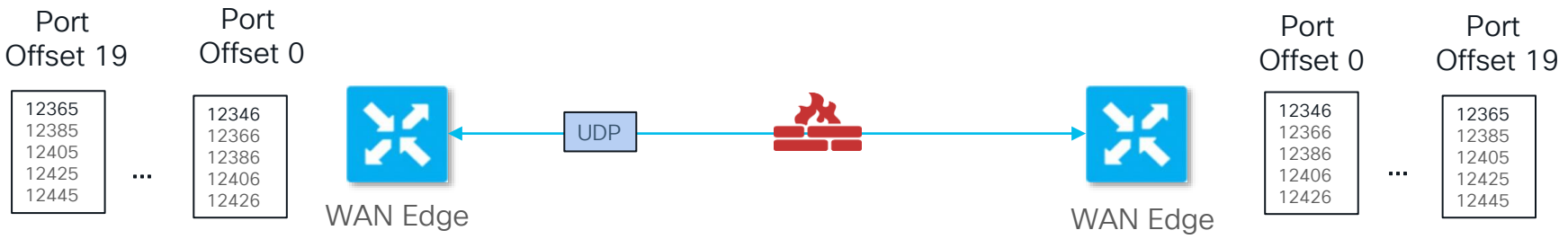
● Direct IPSec Tunnel

● No Direct IPSec Tunnel (traffic traverses hub, hub should be using Full Cone NAT)

★ Mostly Encountered

Firewall Ports

WAN Edge Router



Use **show [sdwan] bfd sessions** or **show [sdwan] tunnel statistics [table]** to view source and destination port numbers

```
WAN_EdgeE#  show sdwan tunnel statistics table


TUNNEL     SOURCE                SOURCE  DEST                                                TUNNEL
PROTOCOL   IP       DEST IP      PORT    PORT    SYSTEM IP    LOCAL COLOR REMOTE COLOR  MTU    tx-pkts   tx-octets rx-pkts rx-octets
-----------------------------------------------------------------------------------------------------------------------------------------
ipsec    10.4.1.2  10.101.1.2  12366   12426  10.255.241.12  mpls      mpls         1442  44848    6102981   44847   6427822  1362
ipsec    10.4.1.2  10.105.1.2  12366   12406  10.255.242.51  mpls      mpls         1434  42445    6104890   42318   5896768  1354
```

Reachability

Usual Suspects

- Does the NAT design allow BFD sessions to form between WAN Edge routers?
- If firewalls are present in the path, do firewall rules allow for the communication to succeed?
- Are all control connections established? Without this, BFD peers won't be established
- Is there any policy in place preventing TLOCs from being learned and thus prevent BFD sessions from forming?

Troubleshooting BFD Sessions

No MPLS BFD sessions

```
WAN_EdgeG# show sdwan bfd sessions
                                SOURCE TLOC   REMOTE TLOC              DST PUBLIC DST PUBLIC      DETECT TX
SYSTEM IP      SITE ID   STATE  COLOR         COLOR         SOURCE IP IP         PORT      ENCAP MULTIPLIER INTERVAL UPTIME TRANSITION
-----------------------------------------------------------------------------------------------------------------------------------
10.255.241.11  112001    up     biz-internet  biz-internet  10.4.1.6  64.100.101.2 5062    ipsec  7         1000   0:00:33:54   3
10.255.241.12  112001    up     biz-internet  biz-internet  10.4.1.6  64.100.101.2 12426   ipsec  7         1000   0:00:33:54   2
10.255.241.21  111002    up     biz-internet  biz-internet  10.4.1.6  64.100.102.2 12406   ipsec  7         1000   0:00:33:54   2
10.255.241.31  113003    up     biz-internet  biz-internet  10.4.1.6  64.100.103.2 12426   ipsec  7         1000   0:00:33:54   1
```

Router not advertising MPLS TLOC

```
WAN_EdgeG#show sdwan omp tloc-paths
tloc-paths entries 10.255.255.217 biz-internet ipsec
<snip>
```

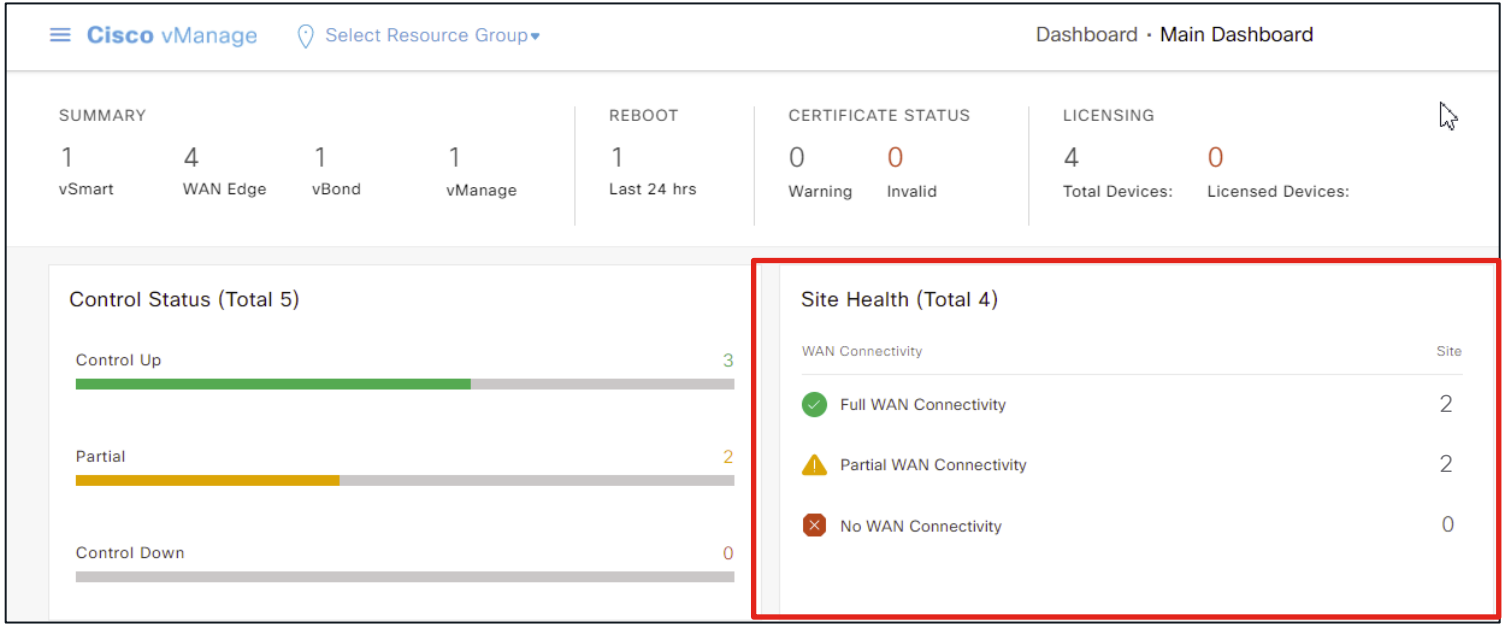
Missing MPLS Control Connections –
*Always troubleshoot control connections first

```
WAN_EgeG# show sdwan control connections
                                                                PEER                    PEER
PEER     PEER PEER            SITE    DOMAIN PEER             PRIV  PEER              PUB
TYPE     PROT SYSTEM IP       ID      ID     PRIVATE IP       PORT  PUBLIC IP         PORT  LOCAL COLOR     PROXY STATE UPTIME
-----------------------------------------------------------------------------------------------------------------------------------
vsmart   dtls 10.255.255.78   2       1      64.100.100.78    12346 64.100.100.78     12346 biz-internet    No    up     0:01:11:55
vsmart   dtls 10.255.255.79   2       1      64.100.100.79    12346 64.100.100.79     12346 biz-internet    No    up     0:01:11:52
vmanage dtls 10.255.255.74   2       0      64.100.100.74    12746 64.100.100.74     12746 biz-internet    No    up     0:01:10:06
```

Troubleshooting BFD Sessions (cont)

- show [sdwan] tunnel statistics bfd
- show [sdwan] bfd history
- BFD packets are marked CS6 (48 decimal) by default – use extended ping (IOS XE SD-WAN) to mark ICMP with the same DSCP to ensure all packets are making it through

vManage – Monitor BFD Sessions



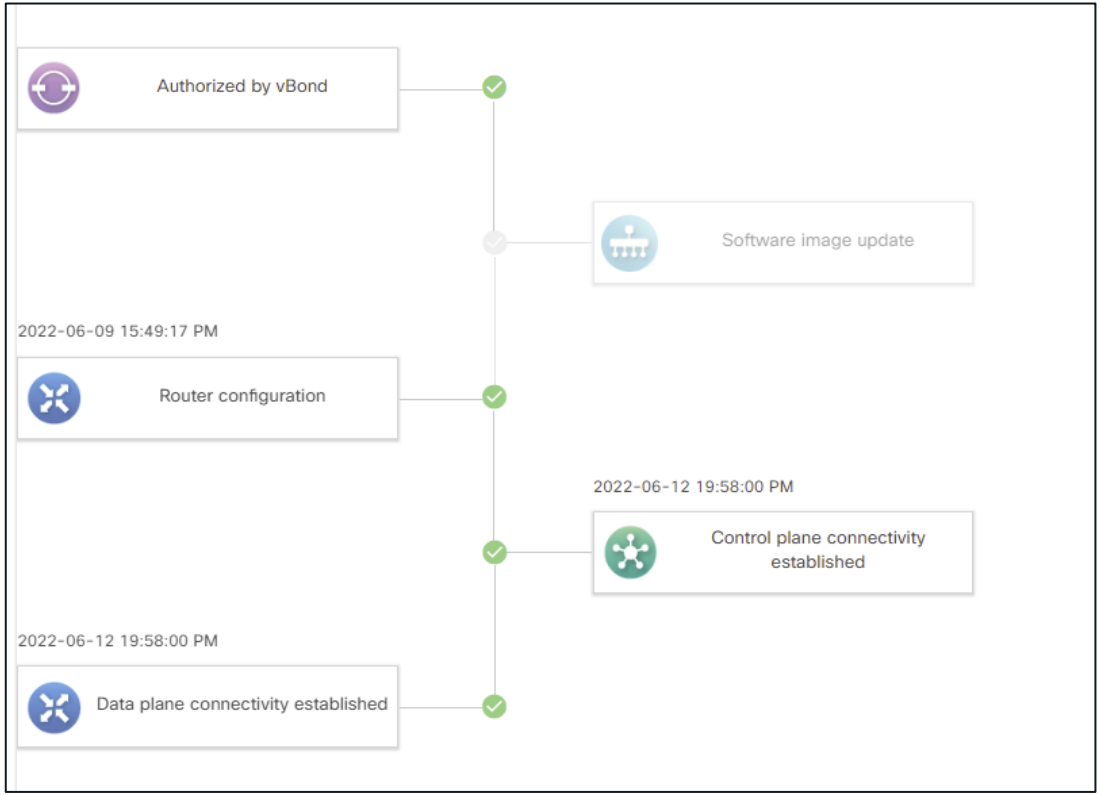
Indicates BFD data plane connections

Full WAN Connectivity (all required BFD connections up)

Partial WAN Connectivity (some required BFD connections up)

No WAN Connectivity (all BFD connections are down or no connection to vManage)

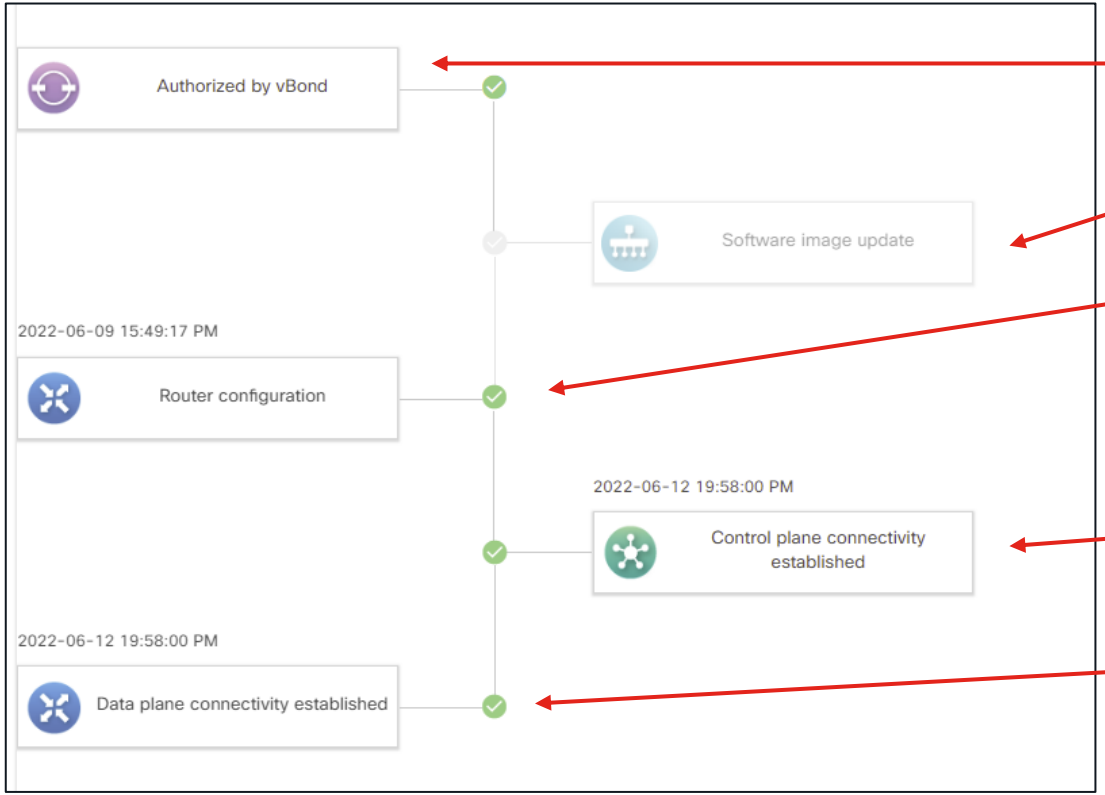
Device Bringup



Can go to **Configuration>Devices**, select **...** to the right of the device and choose **Device Bringup**

or go to **Monitor>Network**, select device, select **Troubleshooting**, then **Device Bringup** under **Connectivity**.

Device Bringup



vBond authorization

Software upgrade

Router configuration received from vManage

Control plane established

Data plane established

Conclusion

Summary

- In the onboarding process, the usual suspects hide in the following areas:
  - Reachability
    - Missing parameters prevent control traffic from initiating
    - Connectivity problems to other SD-WAN devices (including DNS configurations, default route, firewall ports, TLOC extension subnets not reachable, incompatible NAT types, configured policy, etc)
  - Authentication (organization name mismatch, missing root certificates, clock time off)
  - Authorization (certificate marked invalid, device missing from authorized serial number list)

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco SD-WAN @ CL WoS: Demo Highlights

- ITO-01: Cisco SD-WAN Management and Analytics (10 mins)
  - UX 2.0: Rapid Site Configuration Workflow (3-click Deployment)
  - Cloud onRamp Multi-Cloud
    - ✓ Support for various clouds: AWS, Azure, GCP, AWS Gov, Azure Gov
    - ✓ Cloud audit and 1-click self-healing
  - vAnalytics
- SDW-03: SD-WAN Remote Access and Remote Workers Solution (15-20 mins)
  - SD-WAN Remote Access
  - Identify-based ZBFW
  - SIG Integration
- SDW-02: Cisco SD-WAN Multicloud & Analytics (20-25 mins)
  - MSP Co-management (5-7 mins)
  - Cloud onRamp SDCI: Equinix (10 mins)
  - Cloud onRamp SaaS: Custom Apps (5-7 mins)

DEMSDW-02: SD-WAN Multicloud & Analytics
DEMSDW-03: SD-WAN for Remote Users

Platforms

SD-WAN Remote Access

Intuitive Experience

UX 2.0 Rapid Site Config

App Experience

SaaS Optimization M365, Webex, and Custom Apps

Multicloud

Multicloud Access (AWS/Azure/GCP)

Google Cloud

Megaport

EQUINIX

SDCI / Cloud Backbone

Security

Unified Policy and Unified Logging

Identity-based ZBFW

SIG Integration

AIOps

vAnalytics v3

MSP

Multi-tenant Controllers (Control Plane)

Co-managed SD-WAN Service

Thank you

cisco Live!

ALL IN

#CiscoLive