
cisco
You make possible

3 Steps to Design Cisco SD-WAN On-Prem

Andraz Piletic, Consulting Engineer / Instructor
Prashant Tripathi, Global Technical Solutions Architect

BRKRST-2559

cisco Live!
Barcelona | January 27-31, 2020

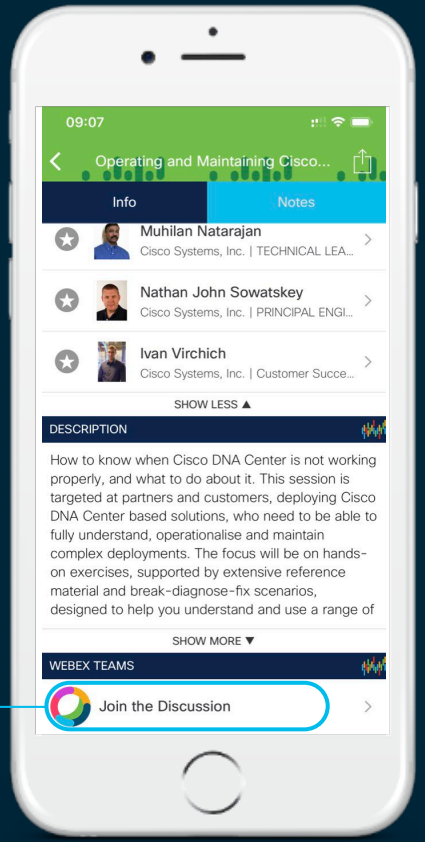
Cisco Webex Teams

Questions?

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

How

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



Agenda

- Designing controllers connectivity
- Deployment requirements
- Managing SA/VA
- Certificate Authority Options
- Zero Touch Provisioning
- vManage Cluster
- Designing high availability and scale

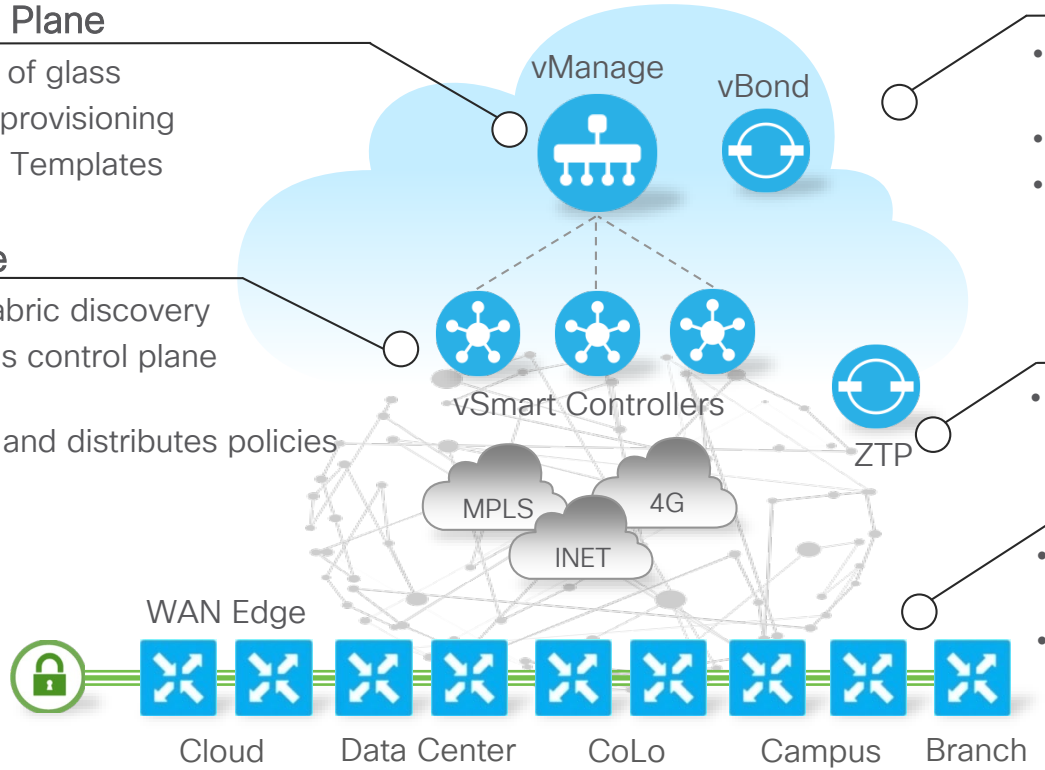
Architecture

Management Plane

- Single pane of glass
- Centralized provisioning
- Policies and Templates

Control Plane

- Facilitates fabric discovery
- Disseminates control plane information
- Implements and distributes policies



Orchestrator

- Orchestrates control and management plane
- First point of authentication
- Facilitates NAT traversal

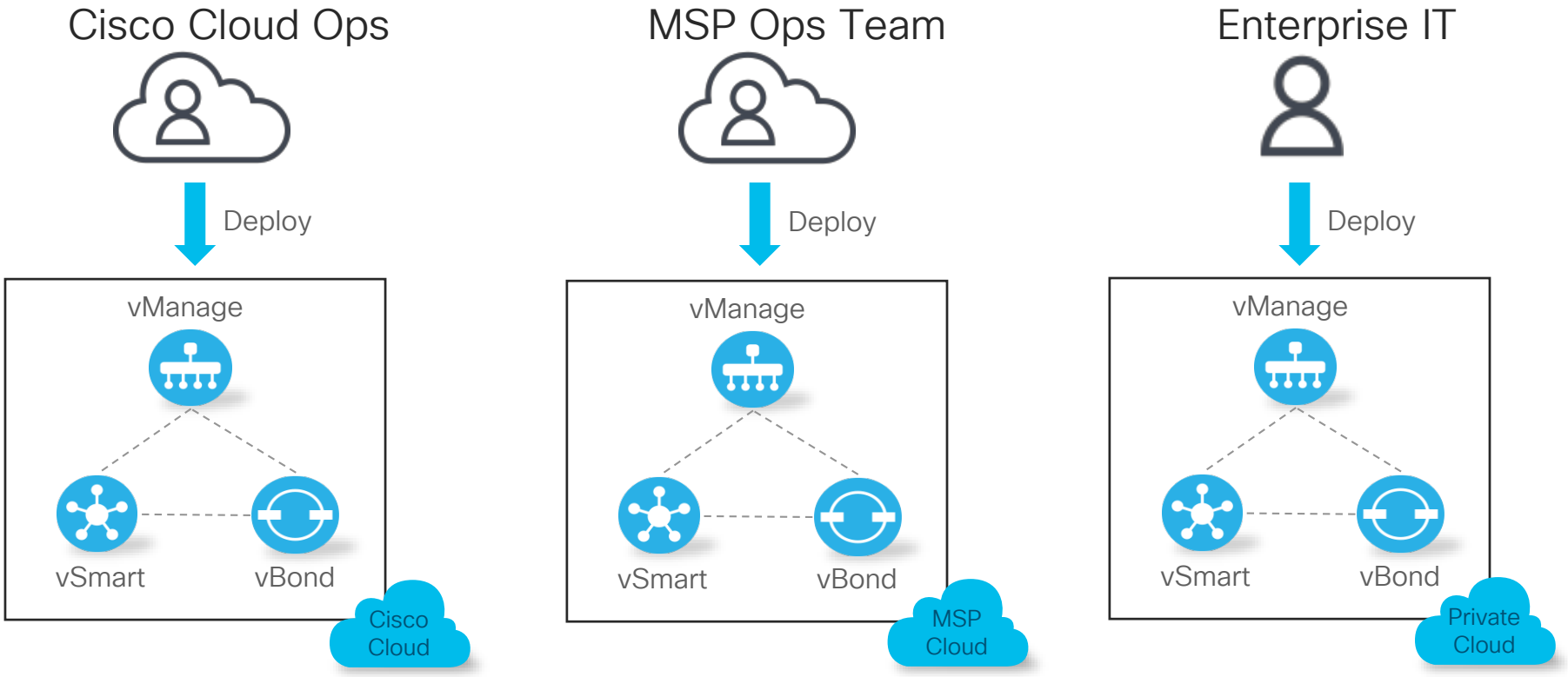
Zero Touch Provisioning

- Facilitates device onboarding

Data Plane

- Diversity of Physical or Virtual appliances
- Builds IPsec tunnels and exchanges user traffic

Controllers Deployment Options



Colors, Address Assignments, and Connectivity

On-Prem Design Consideration

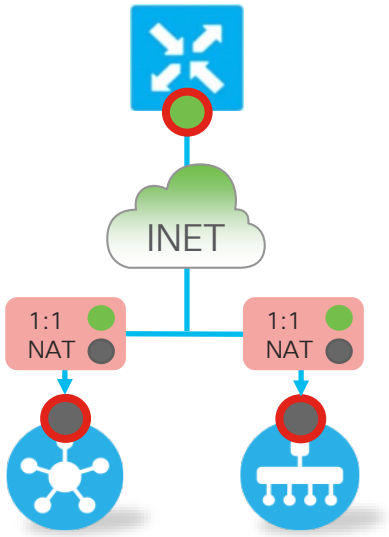
- How to connect WAN Edge devices to controllers?
  - Internet
  - MPLS
  - Multiple Transports
- Should I use private IPs, NAT, public IPs?
- What transport colors should I assign to my controllers?
- Where to place controllers in on-prem environment?

Transport Colors

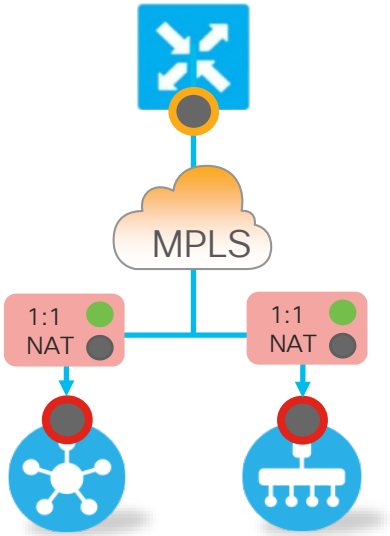
- Color attribute is used to identify:
  - Individual WAN transport tunnel – TLOC Interface
  - Underlay network attachment
- The specific color is categorized as Private or Public
  - Private Colors [mpls, private1-6, metro-ethernet]
  - All other colors are public [default, red, blue,..., public-internet,...]
- Private vs Public color is highly significant
- Color setting applies to:
  - WAN Edge to Controller Communication
  - WAN Edge to WAN Edge Communication

Transport Colors and Control Connections

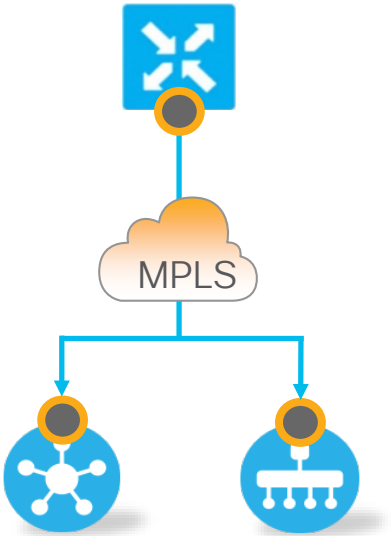
Local Color: Public
Controller Color: Public
Use: Public IP



Local Color: Private
Controller Color: Public
Use: Public IP

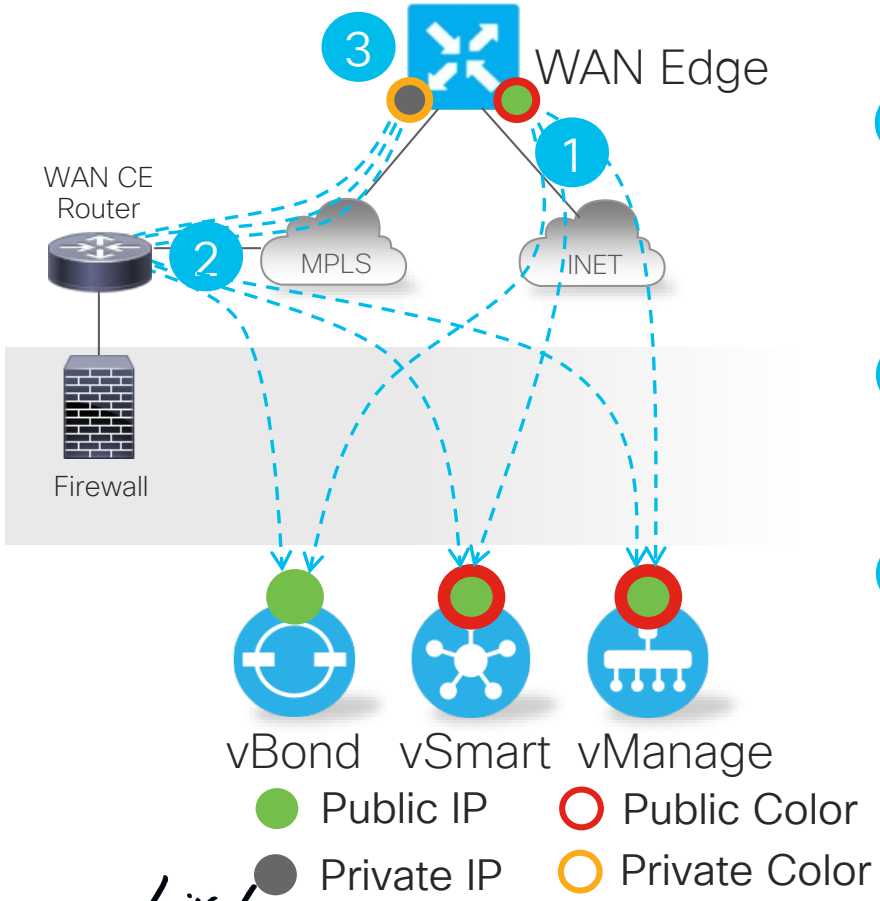


Local Color: Private
Controller Color: Private
Use: Private IP



Public IP
Private IP
Public Color
Private Color

Option A) Assigning Public IPs to Controllers

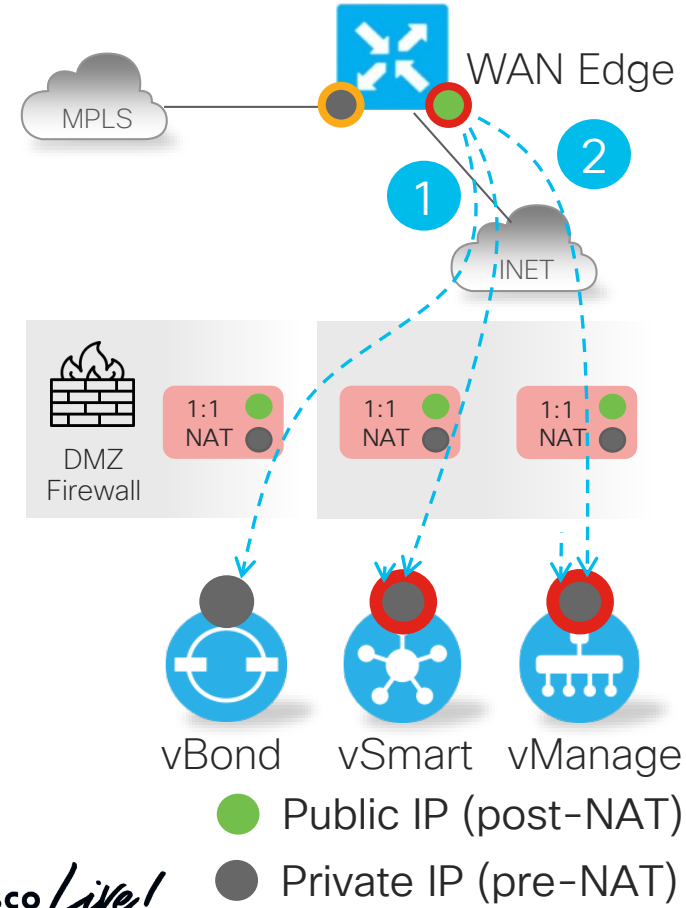


1 WAN Edge points to the vBond public IP and learns about vManage and vSmart public IPs

2 Optionally advertise controllers' public IPs also into private transport.

3 WAN Edge establishes control connections also via private transport using same controllers' public IPs

Option B) Assigning NATed Public IPs to Controllers

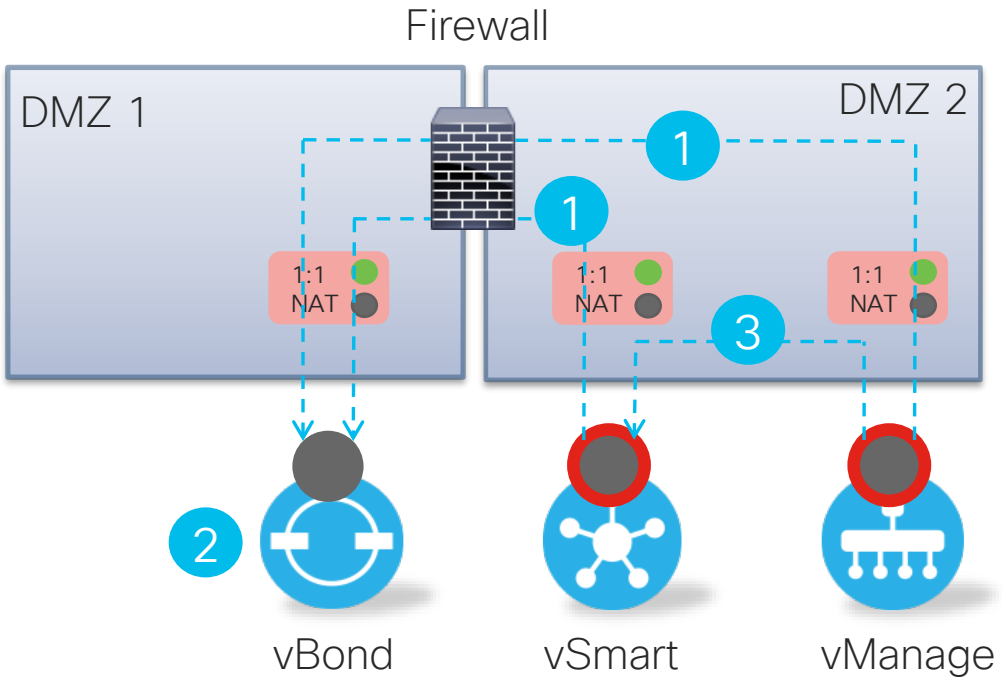


1 WAN Edge points to the vBond FQDN that resolves to NATed IP.

2 WAN Edge communicates with vSmart and vManage NATed public IP over the Internet only.

- Same design option as used in cloud-hosted scenario.

Option B) Assigning NATed Public IPs to Controllers



1 vSmart and vManage point to the vBond NATed public IP.

2 vBond learns interface private and NATed IP address of vSmart and vManage.

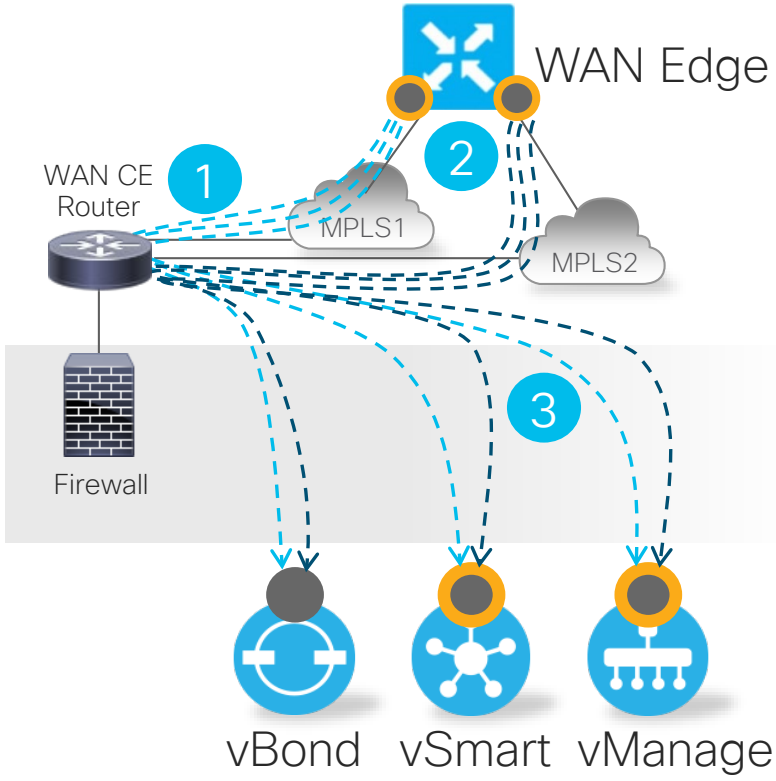
3 vSmart and vManage use private IPs for communication

- Same Site-ID must be used

Public IP (post-NAT) Public Color

Private IP (pre-NAT)

Option C) Assigning Private IPs to Controllers



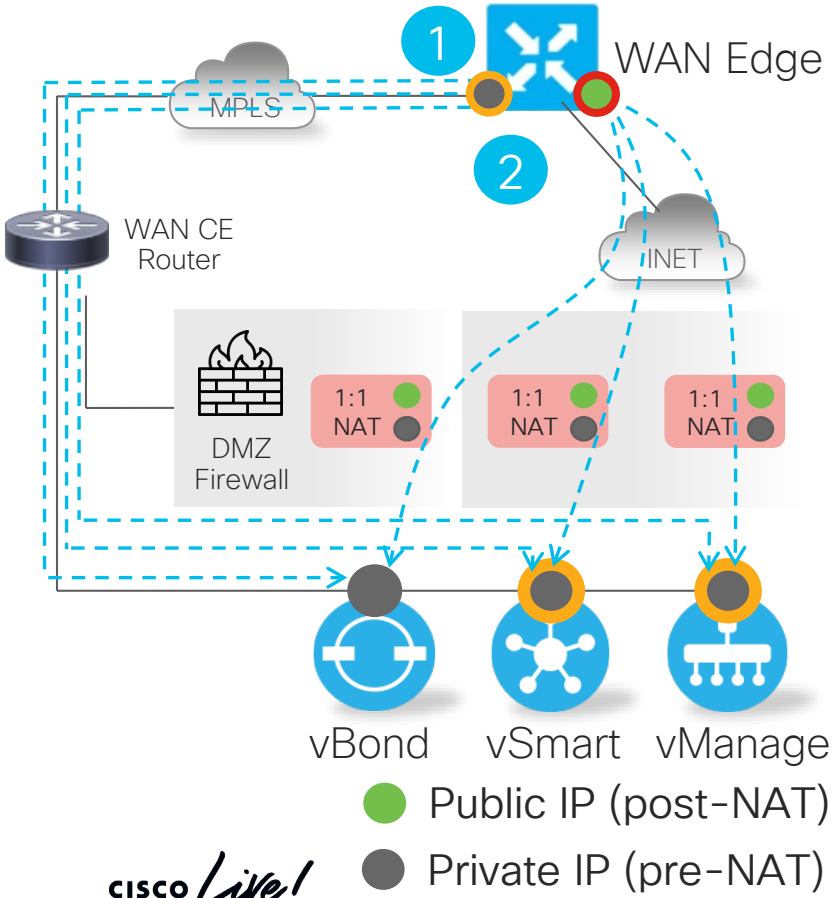
1 Controllers' private IPs are advertised across private transports.

2 WAN Edge points to the vBond private IP address.

- vBond private IP address is reachable through all private transports.

3 WAN Edge communicates with vSmart and vManage by connecting to their private IP address.

Option D) Assigning NATed Public IPs to Controllers



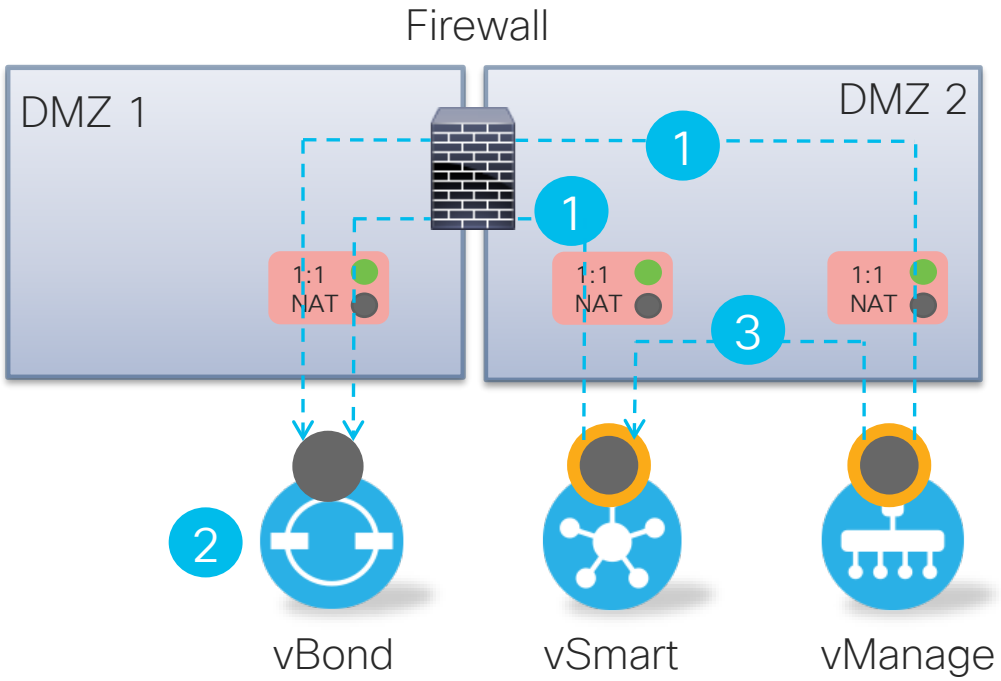
1 WAN Edge points to the vBond FQDN that resolves both public and private IP.

	Private IP	Public IP
MPLS	✓	✗
Internet	✗	✓

2 WAN Edge communicates with vSmart and vManage NATed public IP over Internet and use private IPs over MPLS

- Private color to private color uses private IP, public color to public color uses public IP.

Option D) Assigning NATed Public IPs to Controllers



1 vSmart and vManage point to the vBond NATed public IP.

2 vBond learns interface private and NATed IP address of vSmart and vManage.

3 vSmart and vManage use private IPs for communication

- vSmart and vManage use private color (non-default).

Public IP (post-NAT) Private Color

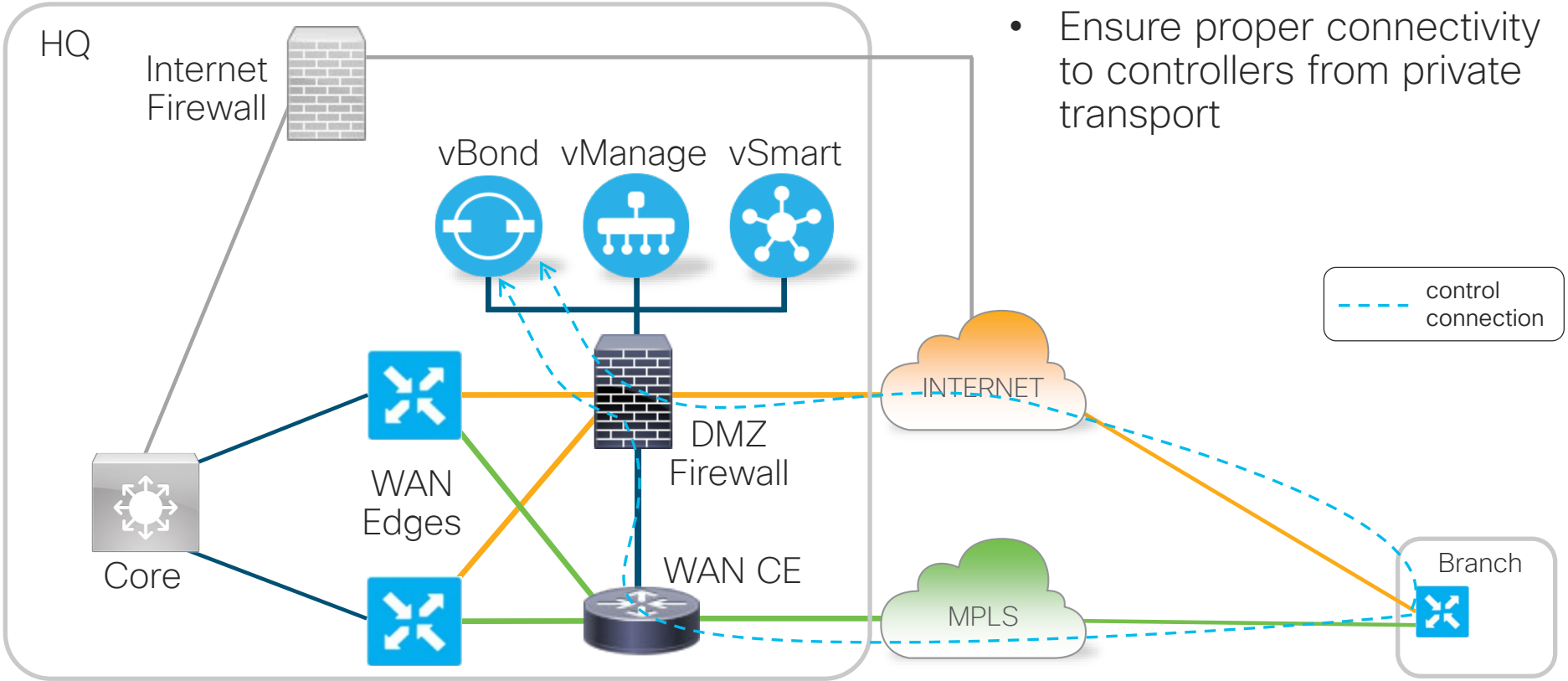
Private IP (pre-NAT)

Review of Design Options

Option	Controller's IPs	Behind NAT	Color Type	Reachable from INET	Reachable from MPLS
A	Public	No	Public	Yes	Only if advertised
B	Private	Yes	Public	Yes (NAT)	No
C	Private	No	Private	No	Yes
D	Private	Yes	Private	Yes (NAT)	Yes

- Prefer designs with control connections over multiple transports for better resiliency
- Option A) is the cleanest/simplest

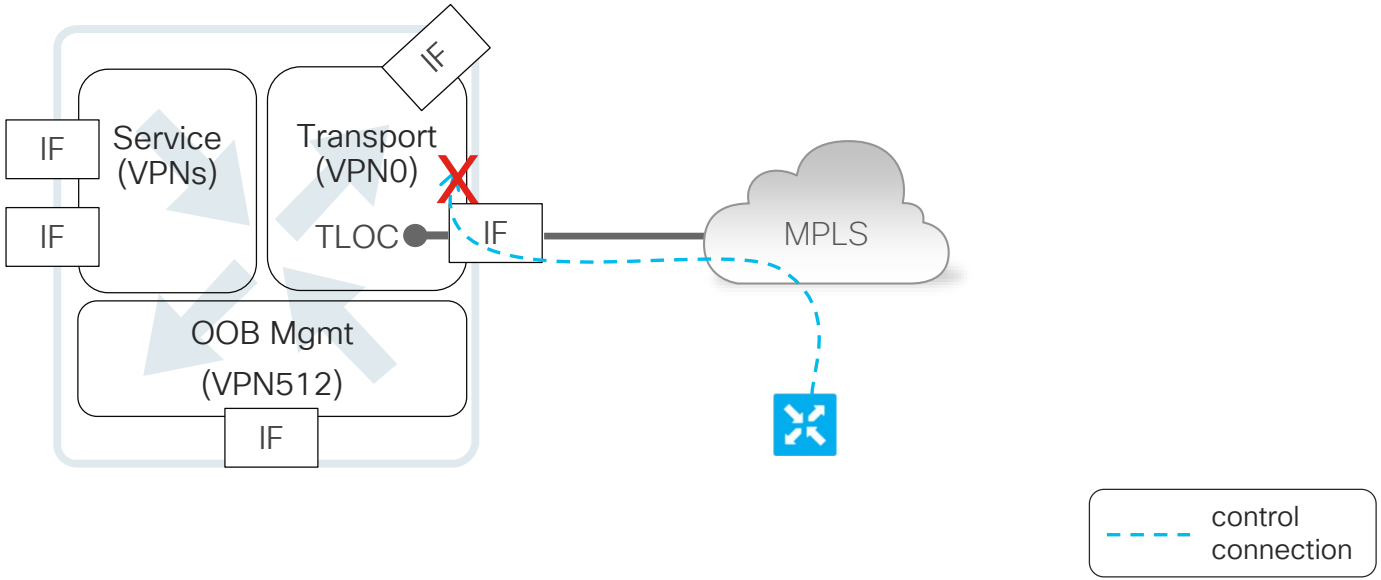
Controllers Placement in On-Prem Environment



- Ensure proper connectivity to controllers from private transport

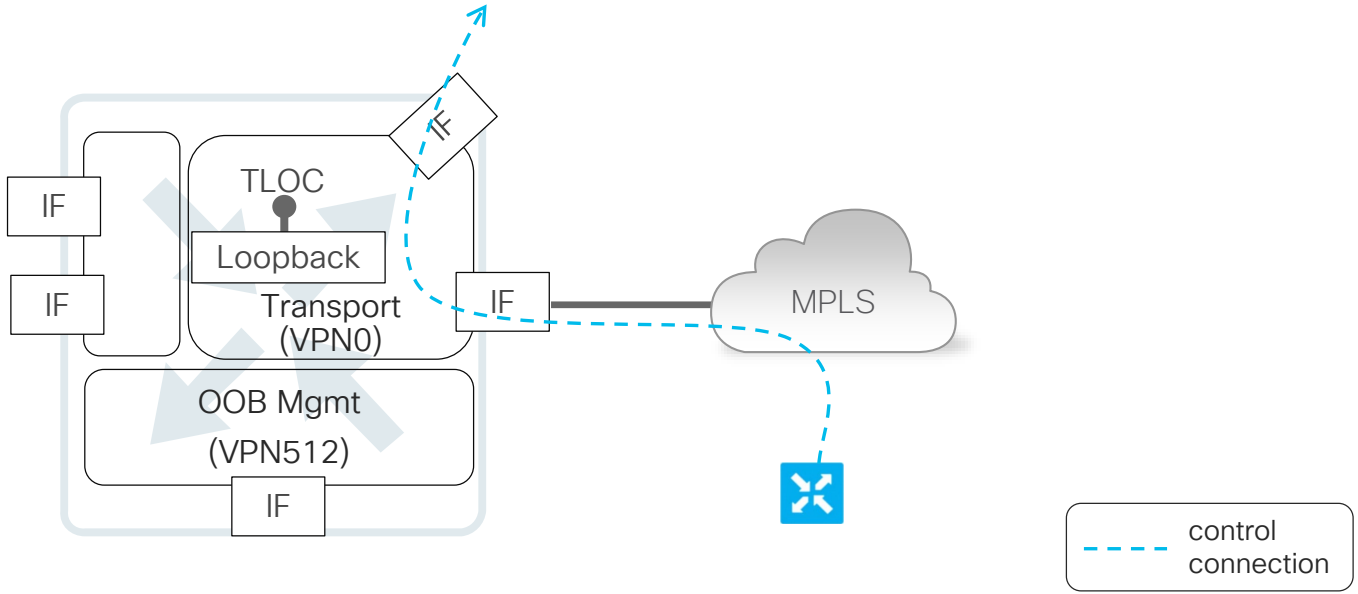
Using Loopback for TLOC Termination

- Problem: TLOC configuration on WAN interface locks down the interface – control connections are not routed through.

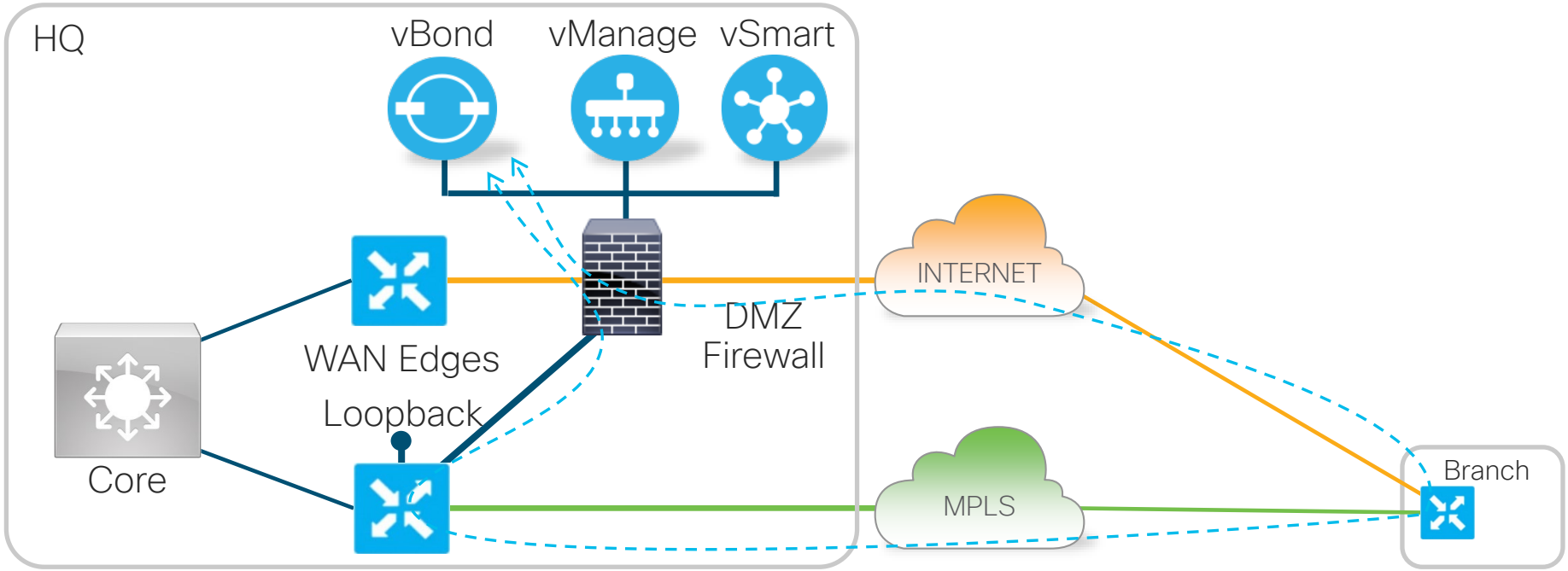


Using Loopback for TLOC Termination

- Problem: TLOC configuration on WAN interface locks down the interface – control connections are not passed through
- Solution: Configure TLOC interface on loopback



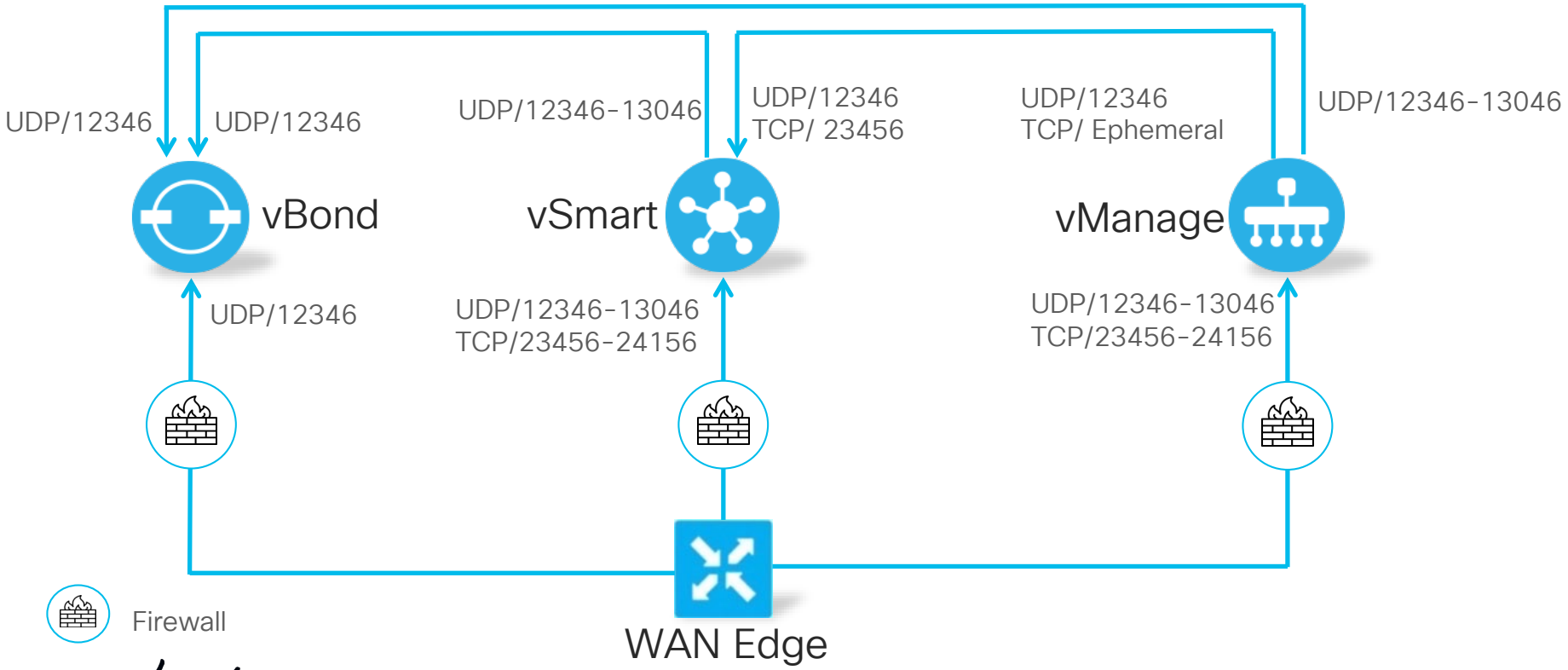
Connecting Controllers Without WAN CE Router



- Configure TLOC on Loopback to allow control connections passing through the WAN Edge towards controllers.

control connection

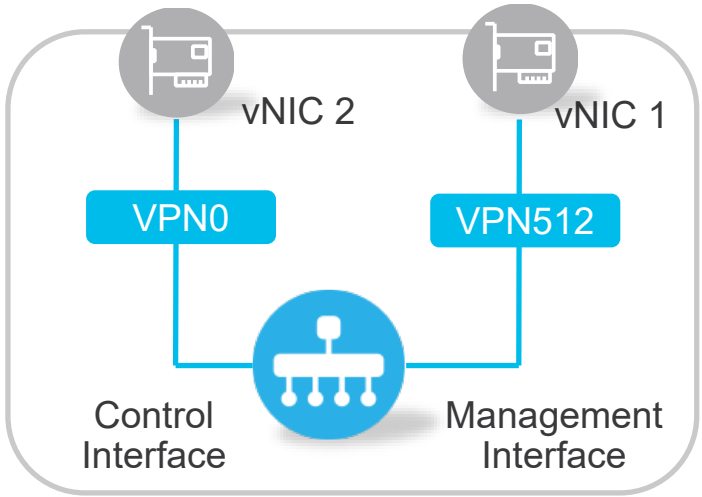
Firewall Rules for On-Prem Controllers



Deployment Requirements

Controllers' Requirements

- All controllers are deployed as virtual machines
- Supported Hypervisors in on-prem deployment
  - KVM
  - VMware ESXi (5.5 – 6.5)
- SSD-based storage required for all controllers
- One underlay (VPN0) interface is supported on each controller, optional additional interface for out-of-band management (VPN512)



Verifying vManage System Requirements

Devices	vCPUs	RAM	OS Volume	Database Volume	Bandwidth	vNICs
1-250	16	32 GB	20 GB	500 GB, 1500 IOPS	25 Mbps	2
251-1000	32	64 GB	20 GB	1 TB, 3072 IOPS	100 Mbps	2
1000+	32	64 GB	20 GB	1 TB, 3072 IOPS	150 Mbps	3*

- Private lab setup for learning purposes will work with less resources.
- * vManage Cluster requires dedicated interface for message bus.

Verifying vBond System Requirements

Devices	vCPUs	RAM	OS Volume	Bandwidth	vNICs
1-50	2	4 GB	10 GB	1 Mbps	2
51-250	2	4 GB	10 GB	2 Mbps	2
251-1000	2	4 GB	10 GB	5 Mbps	2
1001+	4	8 GB	10 GB	10 Mbps	2

- vBond is installed using vEdgeCloud OVA.
- OVA is preconfigured with four vCPUs.

Verifying vSmart System Requirements

Devices	vCPUs	RAM	OS Volume	Bandwidth	vNICs
1-50	2	4 GB	16 GB	2 Mbps	2
51-250	4	6 GB	16 GB	5 Mbps	2
251-1000	4	16 GB	16 GB	7 Mbps	2
1001+	8	16 GB	16 GB	10 Mbps	2

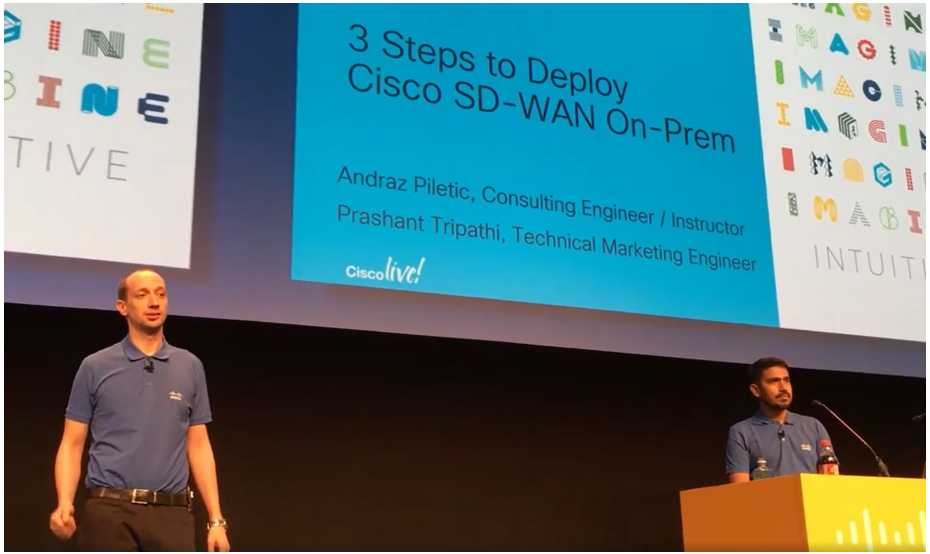
- vSmart controller can run also as container instance in vContainer

Performing Controller Installation

- Detailed step by step procedure covered at CiscoLive San Diego & Barcelona 2019:

BRKRST-2559 - 3 Steps to **Deploy** Cisco SD-WAN On-Prem

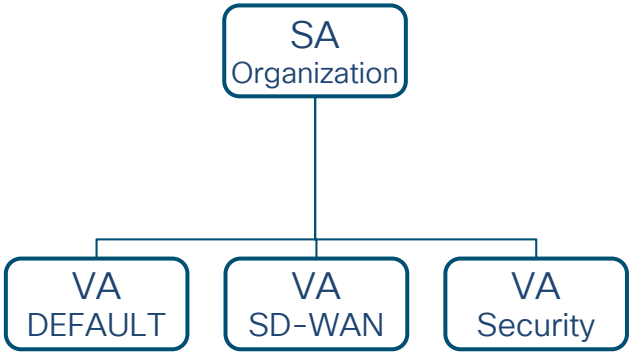
- Recordings and slides are available in the Cisco Live On-Demand Library



Managing Smart Account & Virtual Accounts

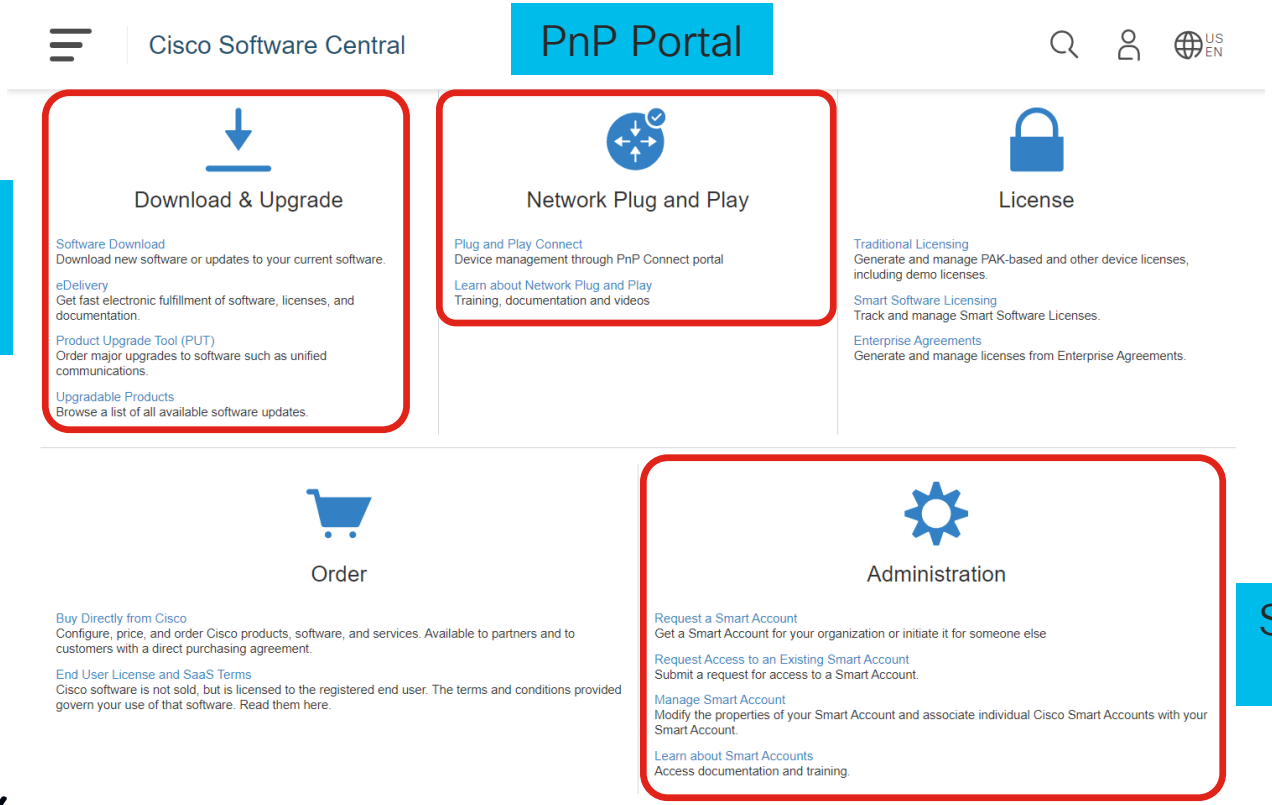
Cisco Smart and Virtual Accounts

- Smart Account (SA) – central repository where you can view, store, and manage licenses across the entire organization.
- Virtual Account (VA) – subaccount to organize and manage licenses based company needs.
  - Created and maintained by the customer
  - Individual SD-WAN overlay is mapped to a single VA
- Recommendation: create dedicated VA for SD-WAN needs
- Find SA Admin to accept PnP Agreement



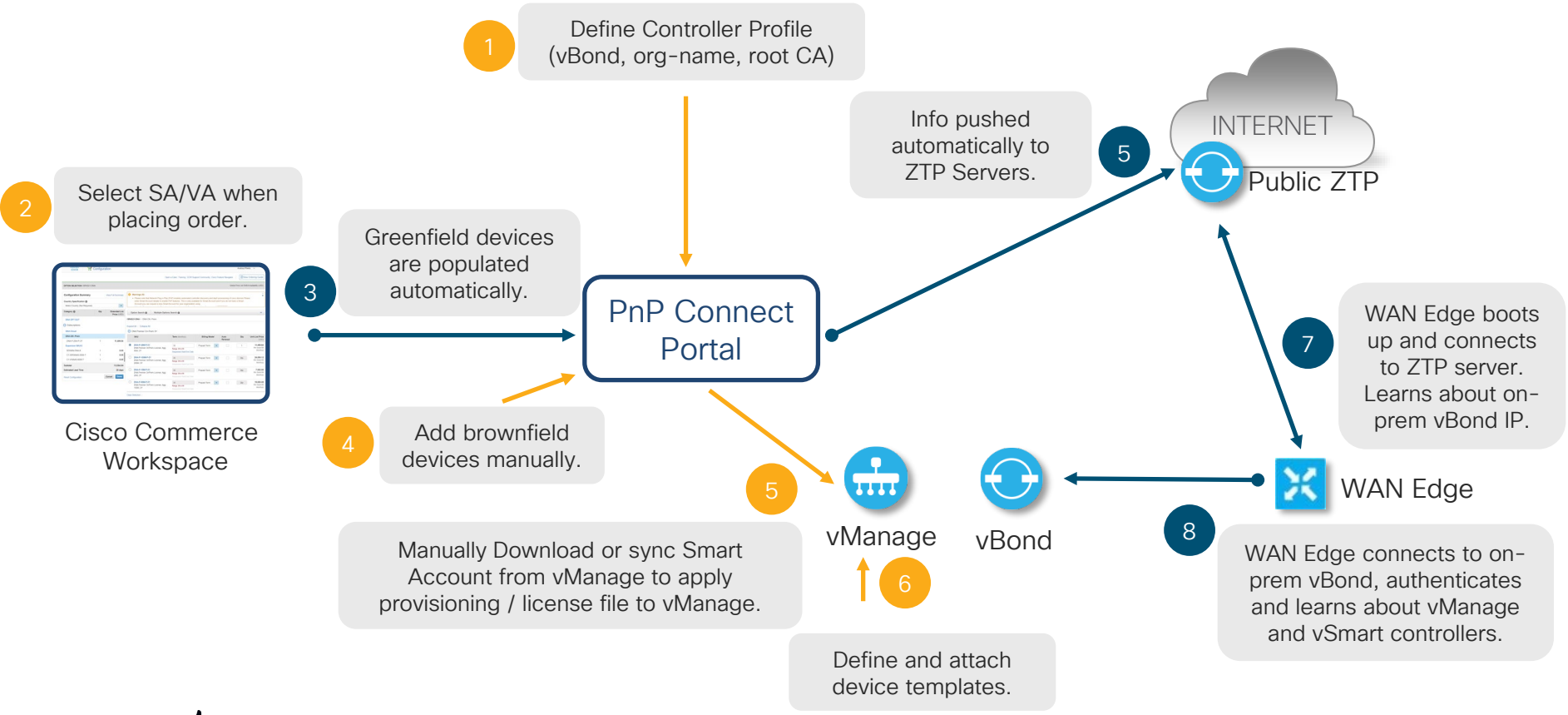
Cisco Software Central – software.cisco.com

Obtain SD-WAN Software

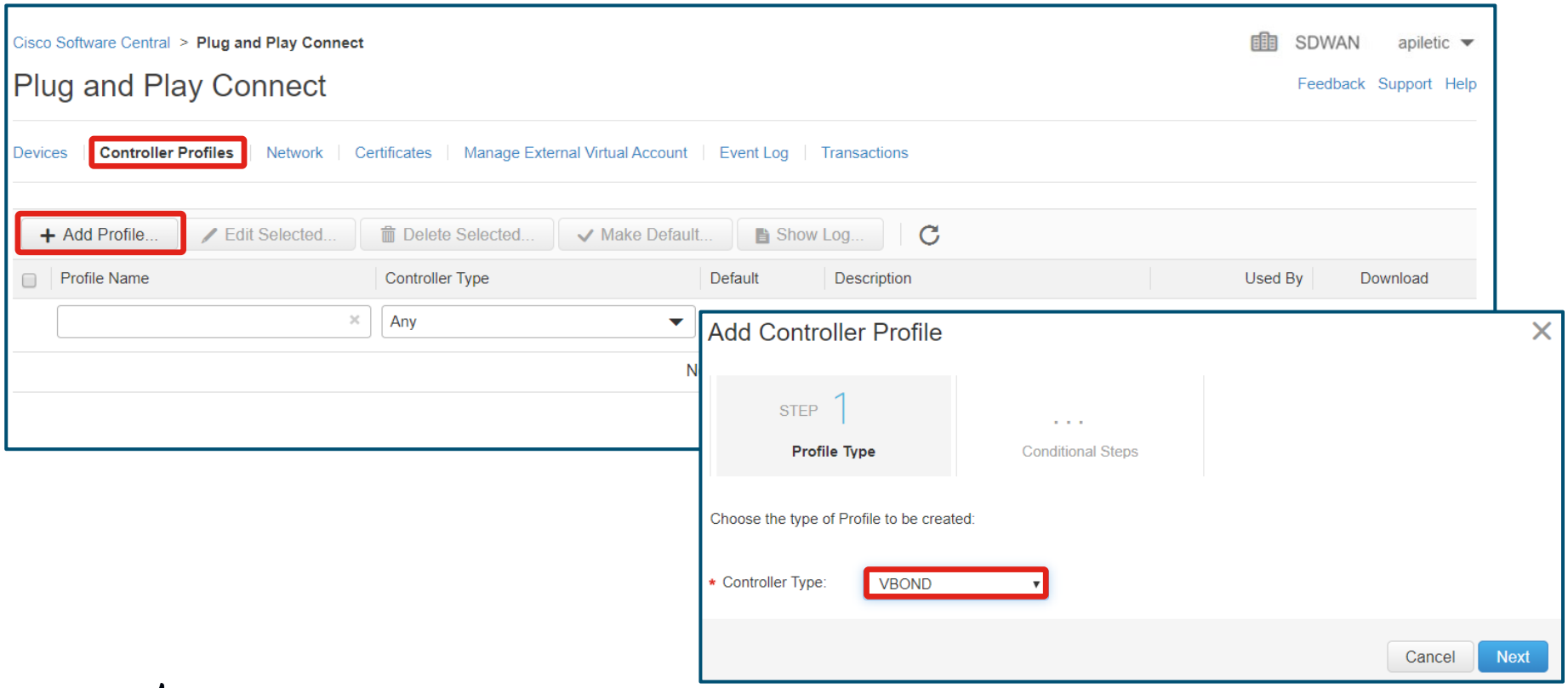


Smart Account Management

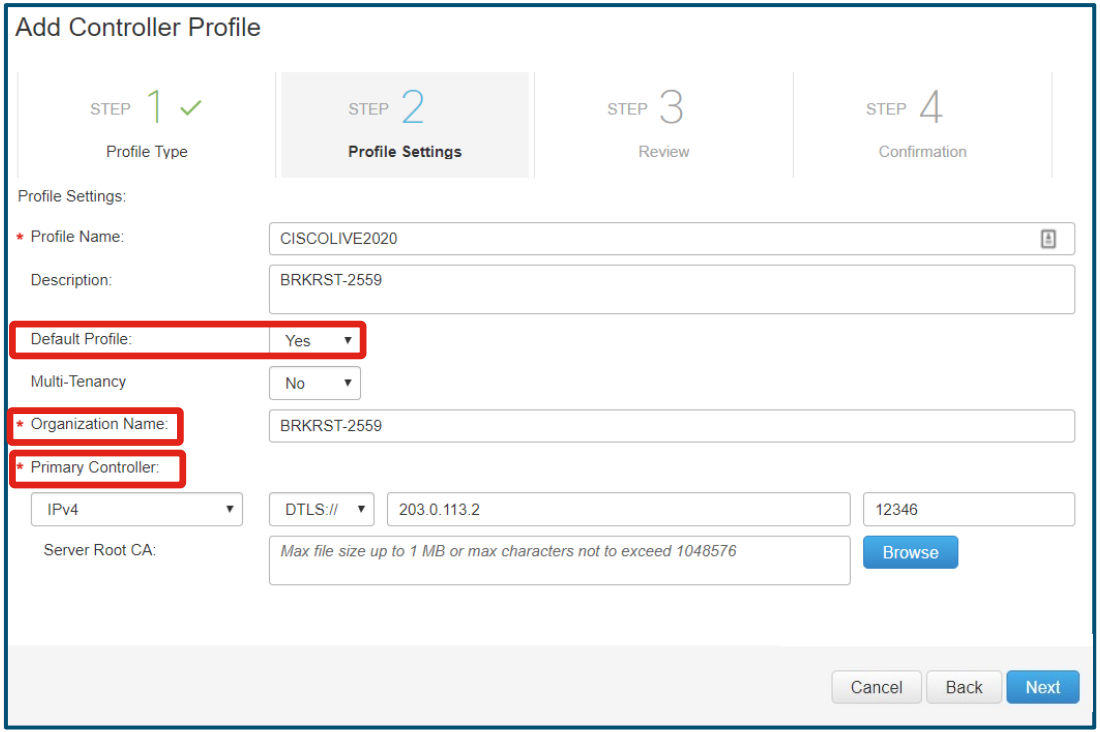
Workflow Overview



Defining Controller Profile



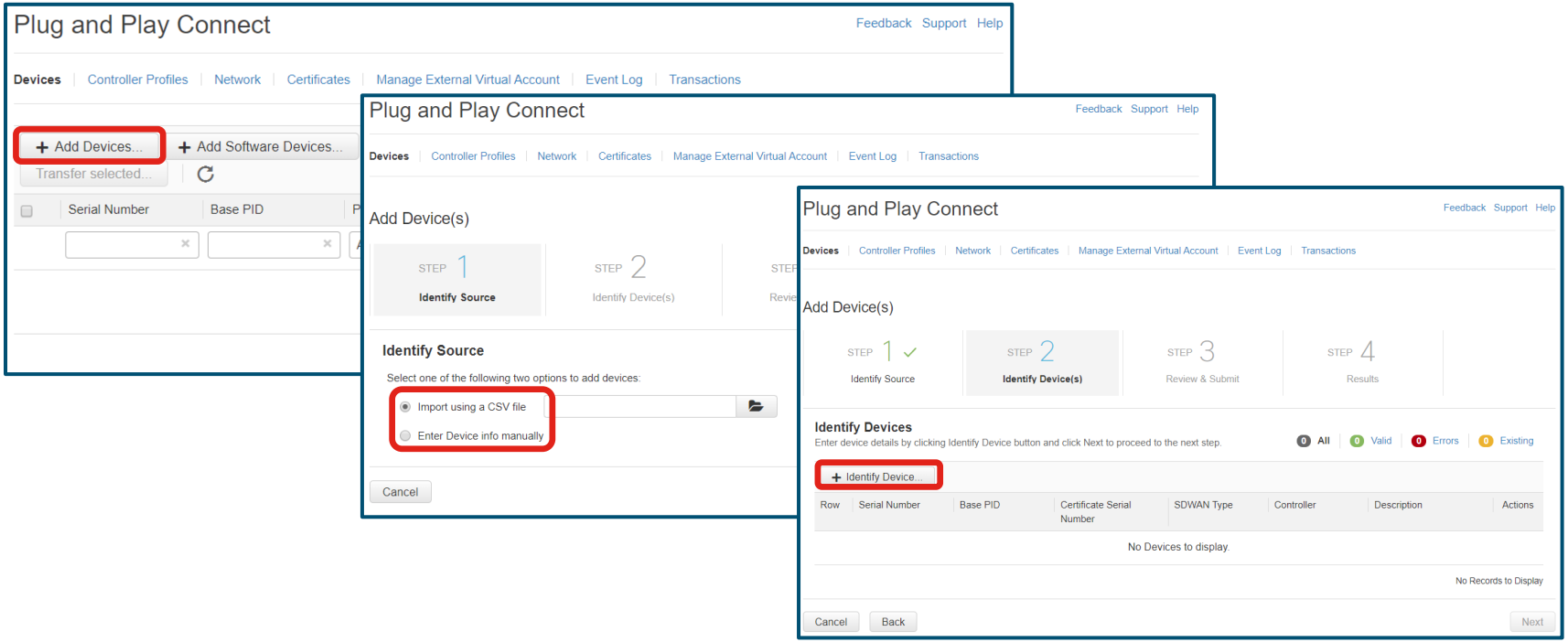
Controller Profile Details



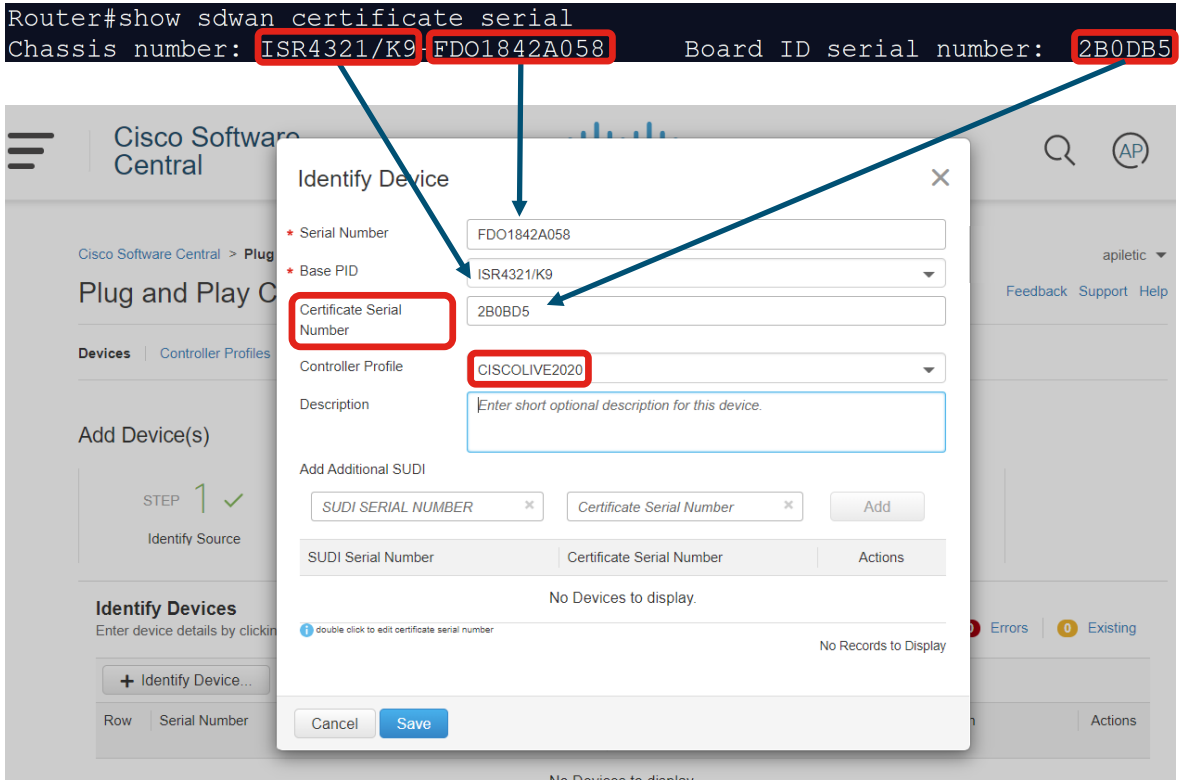
- Defined Organizational Name must match on all SD-WAN components.
- First profile must be marked as default

- Specify Domain or IP of on-prem vBond controller.
- Optionally upload Enterprise Root CA.

Adding Brownfield Devices to PnP Portal

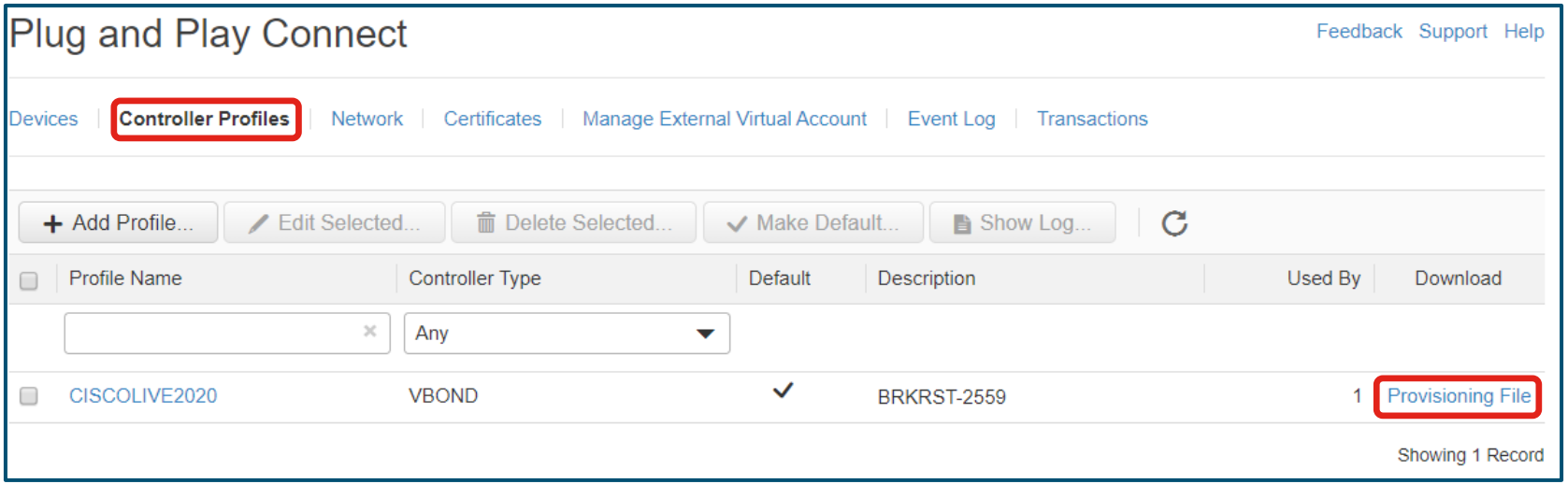


Adding Brownfield Devices to PnP Portal (Cont.)



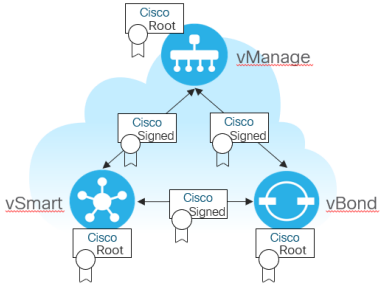
- Certificate Serial Number is required field for SD-WAN deployments
- On IOS-XE platforms running 16.6.1 or more use: **show crypto pki certificates**

Obtaining License / Provisioning File

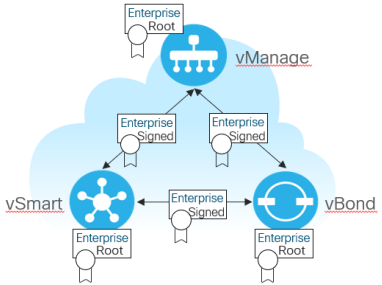


Certificate Authorities

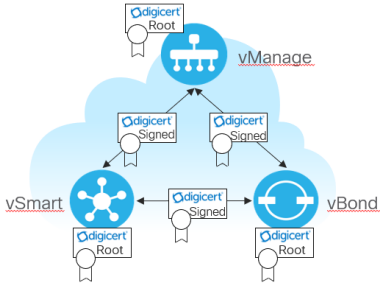
Certificate Authority Options



- Cisco PKI can be used for on-prem controllers deployment.
- CSRs can be automatically signed using configured Smart account and internet connectivity from vManage.
- Manual signing is supported via PnP portal.

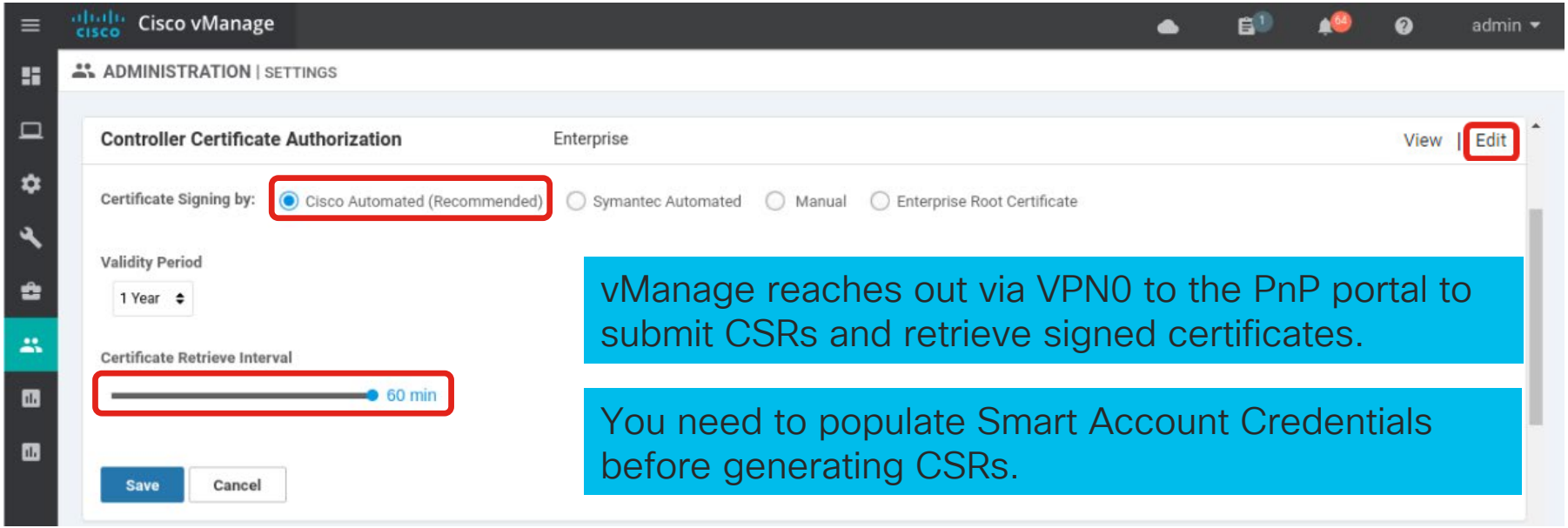


- Enterprise certificates can be used for on-prem controllers deployment.
- Need to install root certificate chain and sign all CSRs manually.



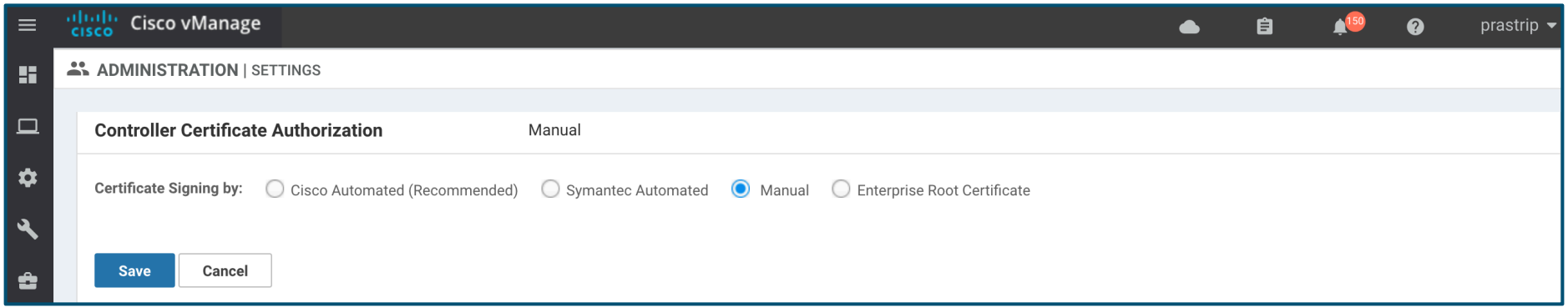
- DigiCert certificates can also be used also in on-prem deployment.
- Need to contact CloudOps for approval.
- Root certificate is preinstalled in the software.

Utilizing Cisco PKI



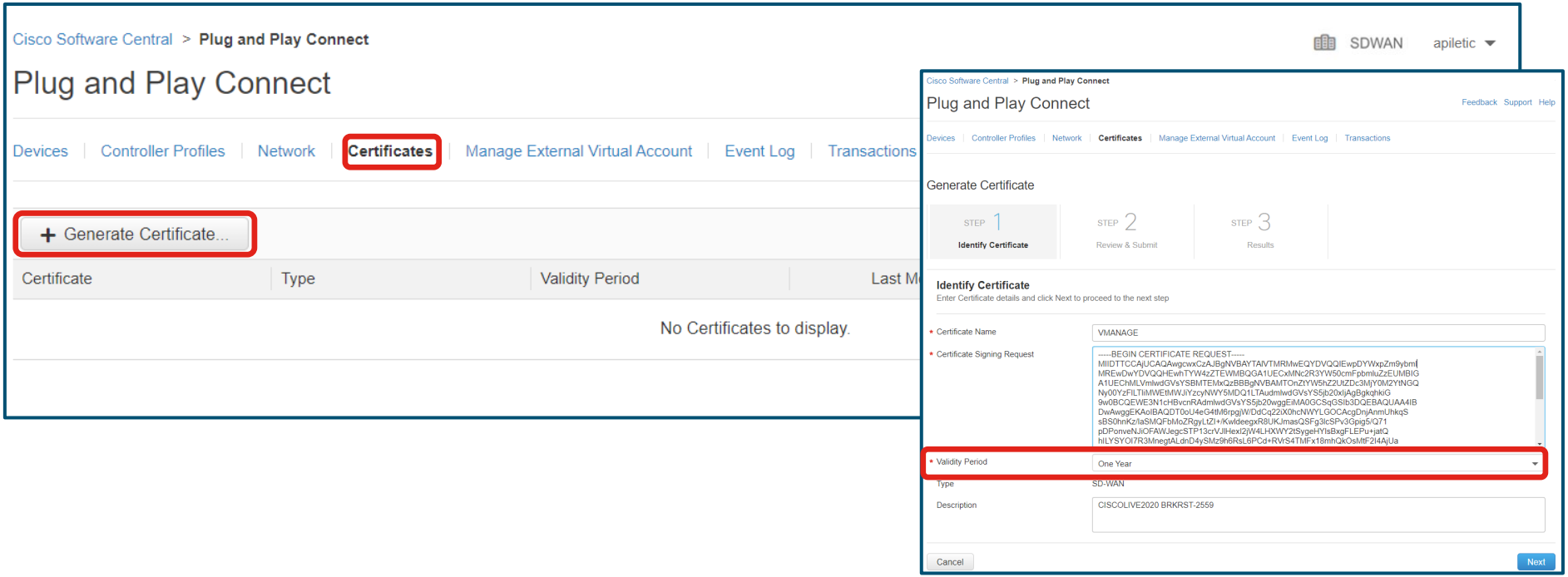
- Cisco PKI is supported since 19.1 software release

Utilizing Cisco PKI – Manual Method

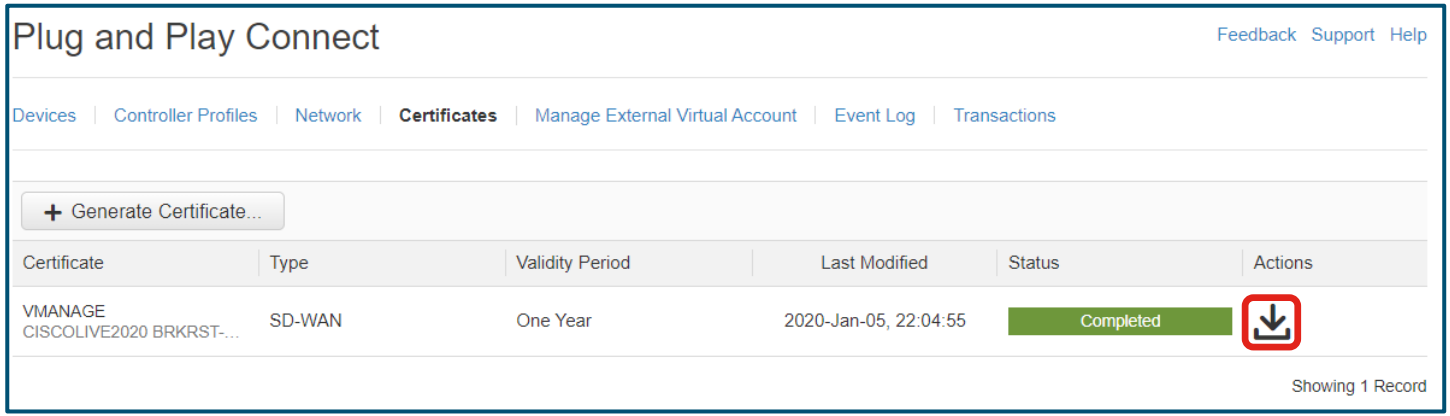


- For environments where vManage cannot connect to the PnP portal
- Manually generate CSRs for all controllers and submit them to the PnP Portal

Manually Submiting CSR to Cisco PKI



Utilizing Cisco PKI – Downloading Signed Cert

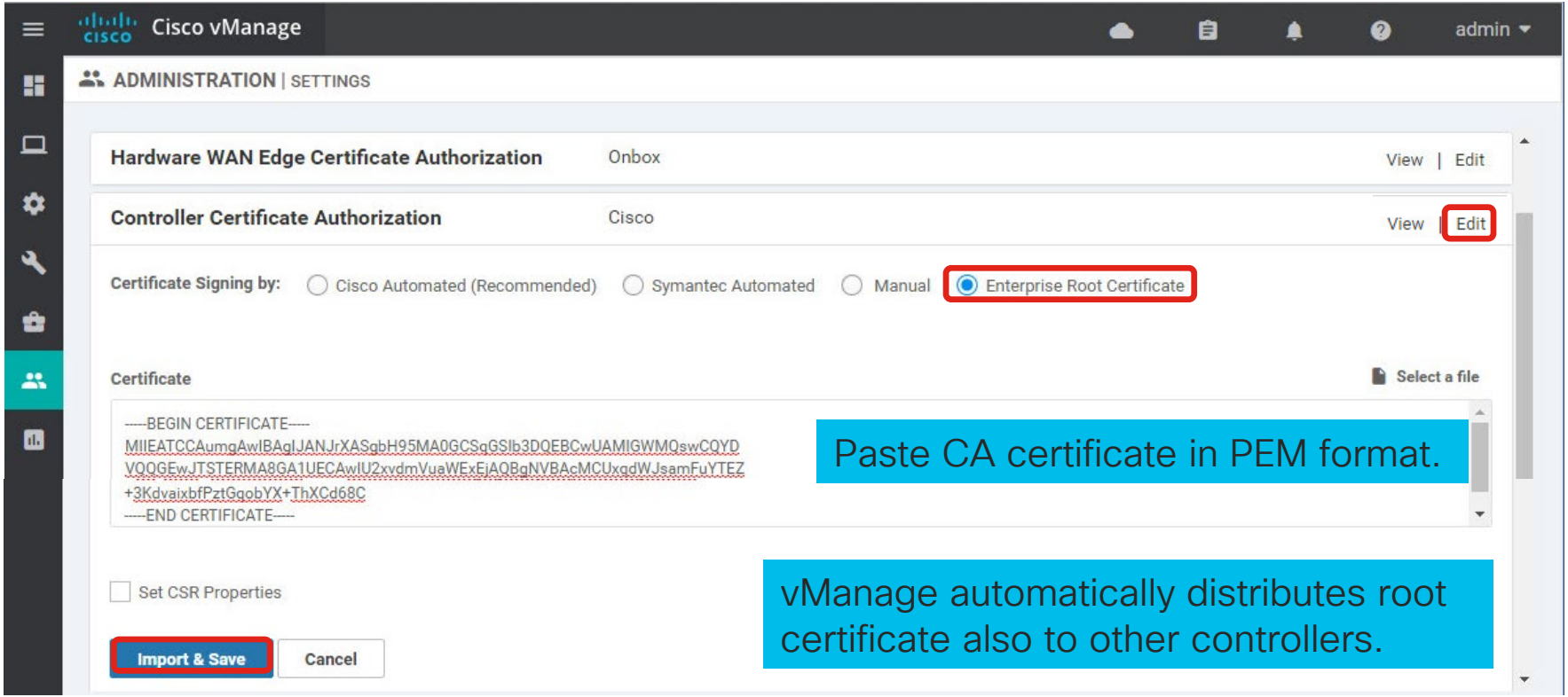


- When approaching expiration date, make sure new CSRs are generate and new certificates obtained and installed.

Using Enterprise CA

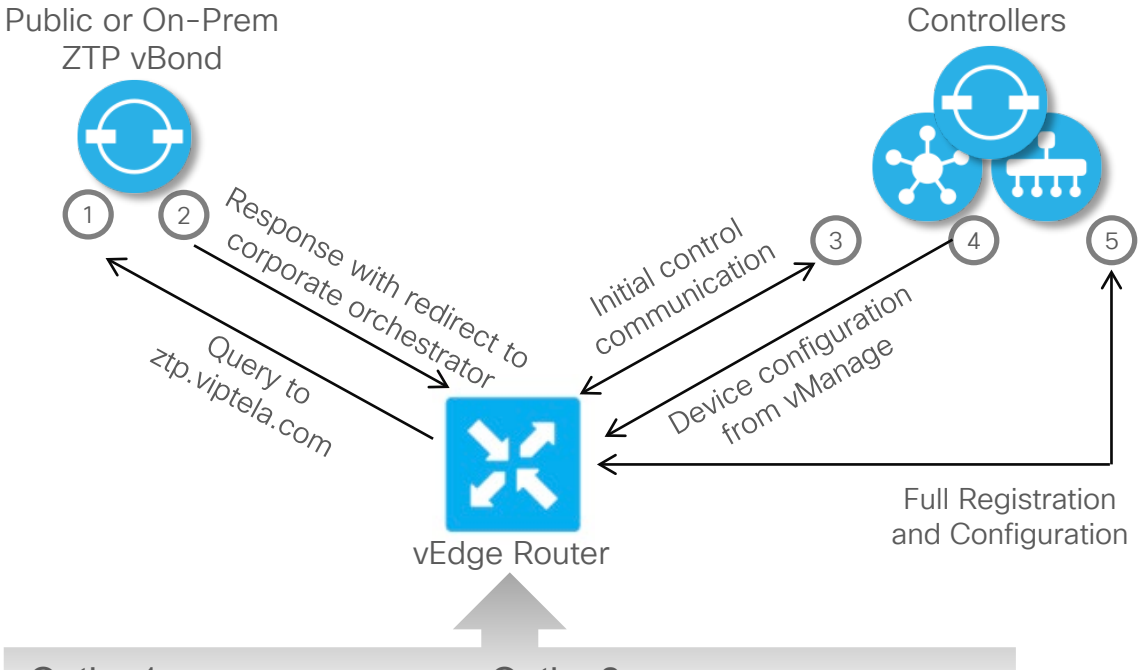
- Customer‘s existing CA infrastructure:
  - Microsoft CA is commonly used within enterprise environments.
- Convenient CA setups for lab testing and PoCs:
  - XCA
  - TinyCA
  - OpenSSL
    - The OpenSSL library is part of most Linux distributions by default.
    - Can be used for simple certificate generation, signing CSRs, etc.
- If using subordinate servers, make sure you export/import the full root-ca chain.

Utilizing Enterprise CA



Zero Touch Provisioning

Zero Touch Provisioning – vEdge HW Appliance



Option1:
- DHCP on WAN interface
- DNS to resolve ztp.viptela.com

Option2:
- Discover local addressing via ARP
- Google DNS: resolve ztp.viptela.com

- Public ZTP vBond can redirect to cloud hosted or On-Prem controllers.
- New devices are linked to organization using the Smart Account when placing order.
- Additional devices can be associated with the customer using the PnP Connect portal
- ZTP for vEdges can be deployed also On-Prem

Configuring On-Prem ZTP vBond Server

Dedicated vBond server can act as a ZTP server. Required steps:

1. Activate the ZTP role.

```
vBondZTP(config)# system vbond ip-address local ztp-server
```

2. Obtain a signed certificate by a trusted CA (Symantec / Digicert).
3. Define and upload the whitelist file.
4. Configure a local DNS server to resolve ztp.viptela.com with ZTP vBond IP.
5. Define device templates.

Obtaining Signed Certificate by Trusted CA

```
vBondZTP# request csr upload /home/admin/ztp.csr
Uploading CSR via VPN 0
Enter organization-unit name                  : ZTPvBond
Re-enter organization-unit name               : ZTPvBond
Generating private/public pair and CSR for this vbond device
Generating CSR for this vbond device    .........[DONE]
Copying ... /home/admin/ztp.csr via VPN 0
CSR upload successful
```

- Generate and submit CSR to Symantec Certificate Enrollment portal

Obtaining Signed Certificate by Trusted CA (Cont.)

```
vBondZTP# request certificate install /home/admin/ztp.pem
Installing certificate via VPN 0
Copying ... /home/admin/ztp.pem via VPN 0
Successfully installed the certificate
```

```
vBondZTP# show certificate installed
    Data:
        Version: 3 (0x2) Serial Number: 6f:3a:61:cd:a8:de:3e:b1:b9
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
        CN=Symantec Class 3 Secure Server CA - G4
        Validity
            Not Before: Nov 29 00:00:00 2019 GMT
            Not After : Nov 30 23:59:59 2020 GMT
        Subject: C=US, ST=California, L=San Jose, O=vIPtela Inc,
        OU=ZTPvBond, CN=vbond-088b7cc2-a905-2f4ee1729bf9-0.viptela.com
```

Uploading The ZTP Whitelist Chassis File

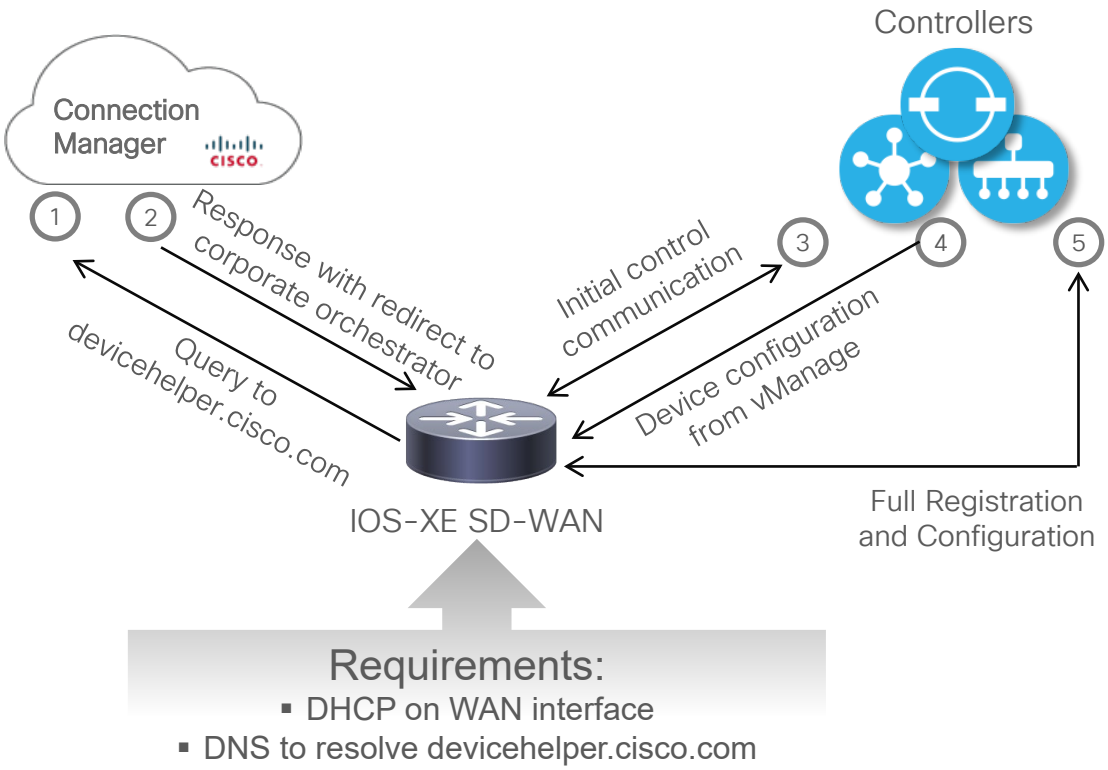
```
vBondZTP# vshell
vBondZTP~$ cat ztp-chassis-file
12345,6789,valid,10.0.0.22,12346,CLEUR 2020 BRKRST - 2559,/home/admin/ca.crt

vBondZTP# request device-upload chassis-file /home/admin/ztp-chassis-file
Uploading chassis numbers via VPN 0
Copying ... /home/admin/ztp-chassis-file via VPN 0
Successfully loaded the chassis numbers file to the database.
Uploading the serial numbers to the vedge-list ...
Uploading serial numbers via VPN 0
Copying ... /home/admin/ztp-chassis-file via VPN 0
Successfully loaded the vEdge serial numbers
```

Define and verify chassis file

Apply chassis file

```
vBondZTP# show ztp entries
       CHASSIS  SERIAL                                VBOND  ORGANIZATION                ROOT CERT
INDEX  NUMBER   NUMBER  VALIDITY  VBOND IP   PORT    NAME                        PATH
-------------------------------------------------------------------------------------------------
1      12345    6789    valid     10.0.0.22  12346   CLEUR 2020 BRKRST - 2559    /home/admin/ca.crt
```

Zero Touch Provisioning – WAN Edge Appliance



- The PnP Connection Manager can redirect to cloud-hosted or On-Prem controllers.
- New devices are linked to organization using the Smart Account when placing order.
- Additional devices can be associated with the customer using the PnP Connect portal
- No on-prem ZTP server support for IOS-XE SDWAN devices at the moment.

ZTP – Bootstraping With Configuration File

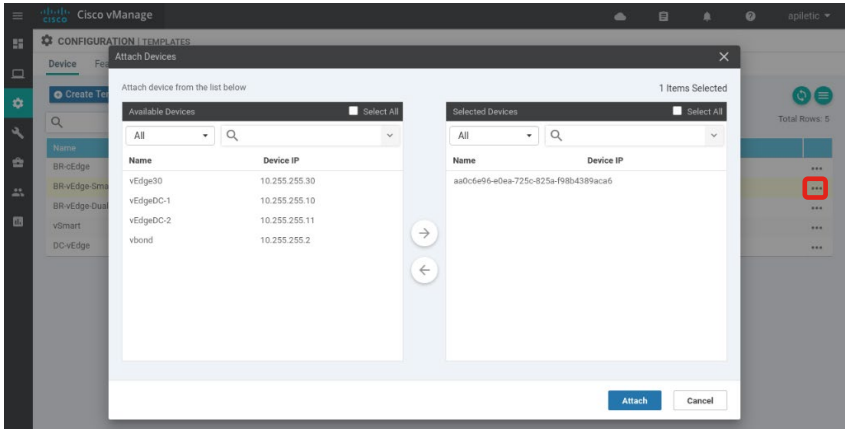
```
<… output omitted …>
#cloud-boothook
  system
   personality           vedge
   device-model          vedge-ISR-4321
   host-name             WanEdge
   system-ip             10.255.255.121
   site-id               21
   organization-name     "CLEUR 2020 BRKRST - 2559"
   console-baud-rate     9600
   vbond 203.0.113.3 port 12346
   !
   !
interface GigabitEthernet0/0/0
   no shutdown
   ip address 198.0.51.10 255.255.255.0
  exit
  !
ip route 0.0.0.0 0.0.0.0 198.0.51.1
<… output omitted …>
```

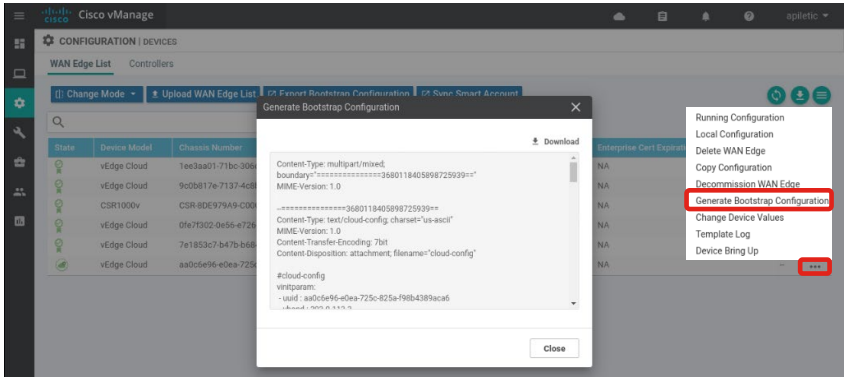
- Upon bootup, the router searches bootflash: or usbflash: for filename ciscosdwan.cfg.
- The config file with interface configuration, Root CA, Organization Name, vBond information, is fed into the PnP process.
- Supported only on SD-WAN IOS-XE (since 16.10).

cisco Live!

Generating Bootstrap Configuration File

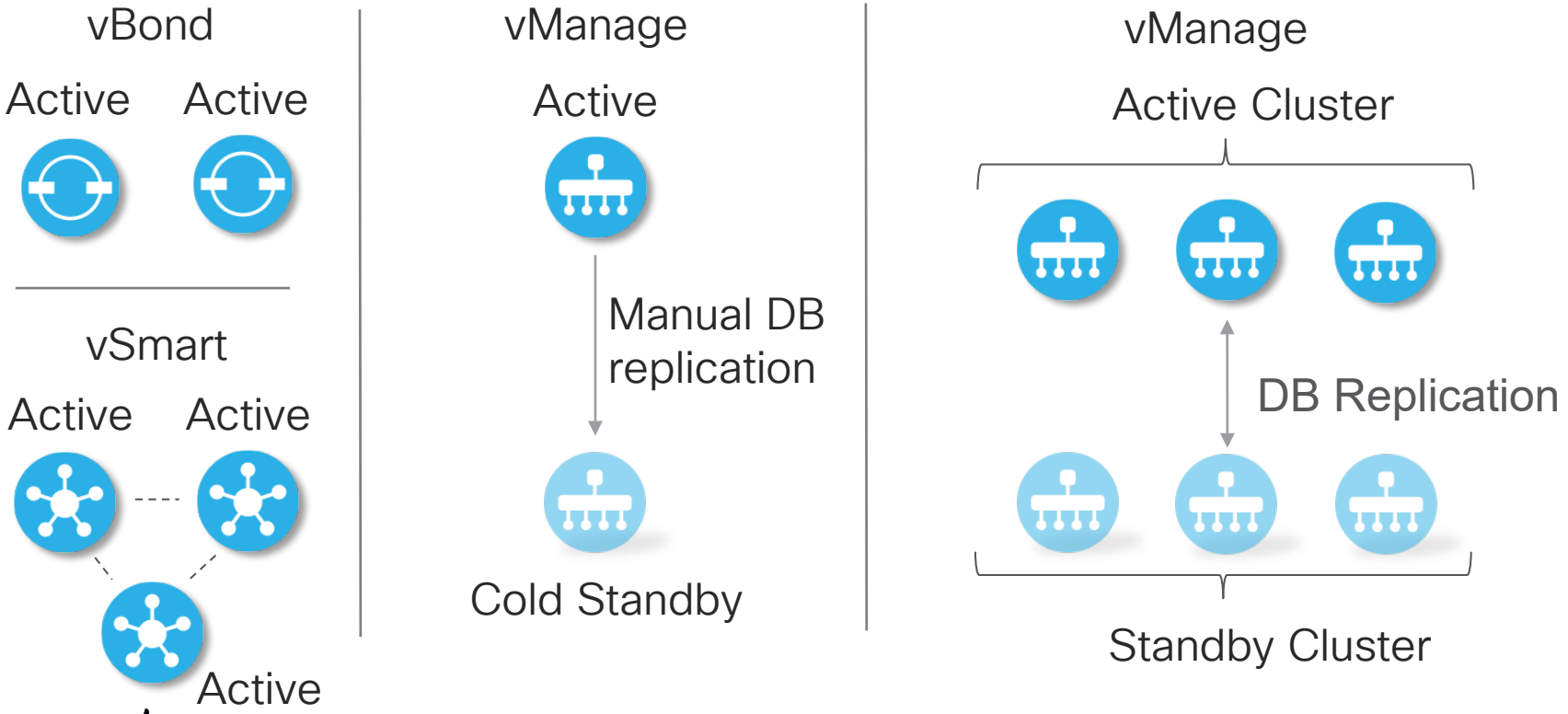
- Attach template to device placeholder
- Specify device specific variable values
- Generate bootstrap config
- Store it on bootflash: or usbflash: as ciscosdwan.cfg





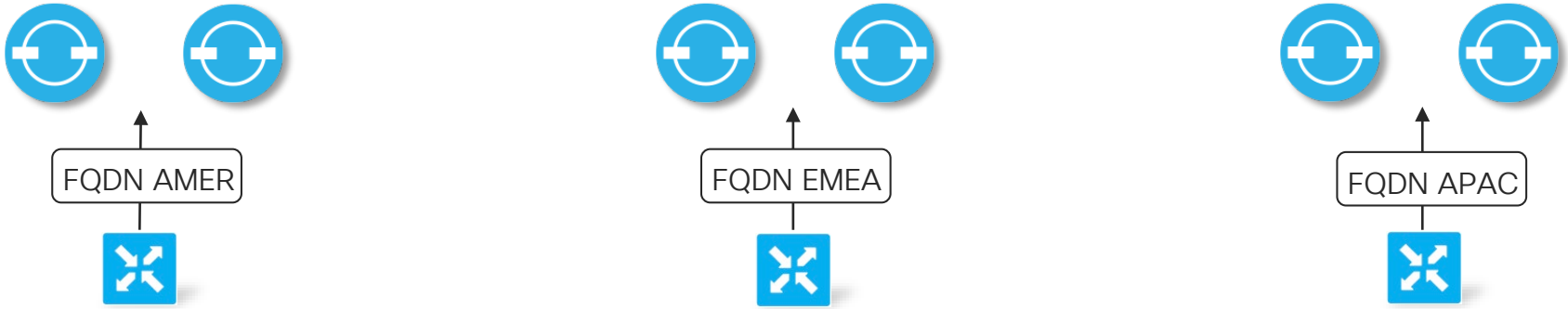
Designing for High Availability and Scale

Controllers High Availability Overview



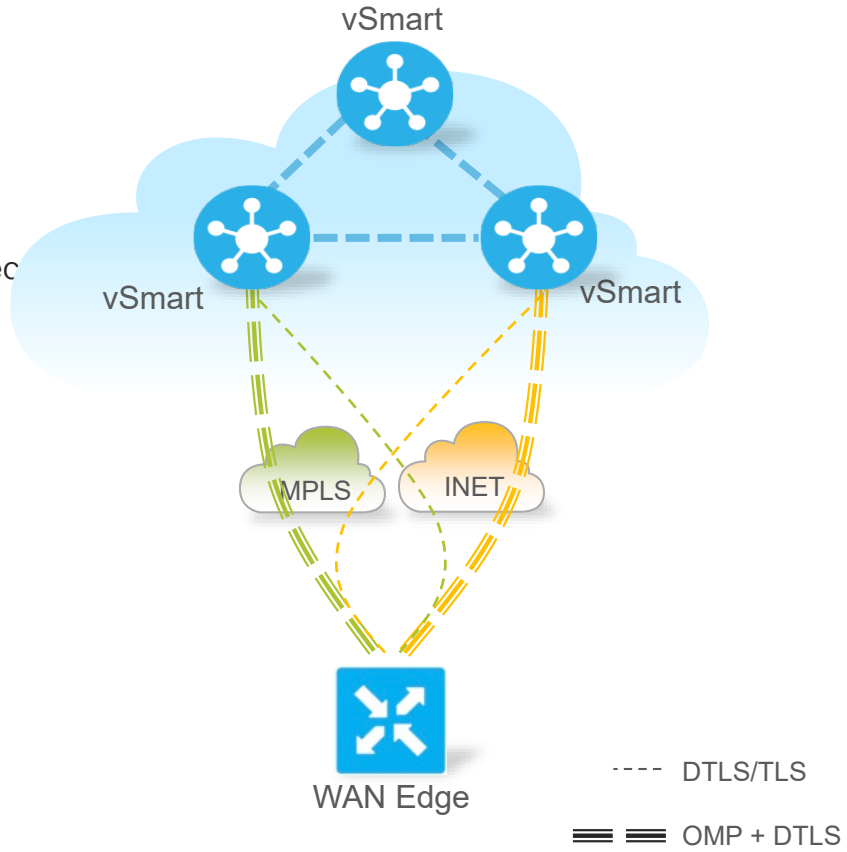
vBond High Availability and Scale

- Default behavior: WAN Edge tries to resolve and connect to all known vBond IPs on all WAN interfaces. Connection is transient.
- Scale approach:
  - Configure regional domain name to point to specific regional vBond pair
  - Rely on DNS A records or define manual host entry

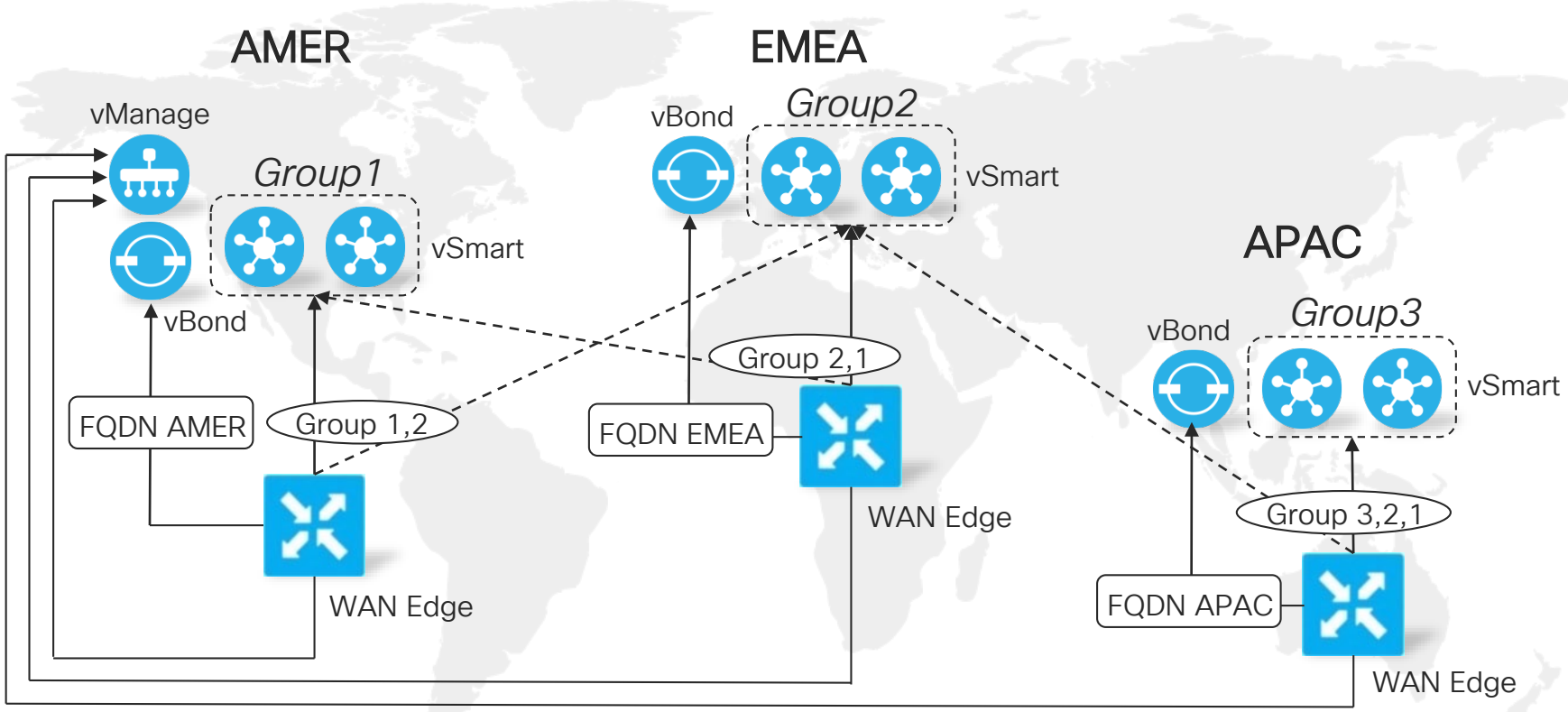


vSmart High Availability and Scale

- Default behavior:
  - WAN Edge connects up to two vSmarts on each transport
  - Example: WAN Edge with two transports == 2 control connec
  - No control over vSmart preference
- Scaling approach:
  - Leverage controller groups and affinity values

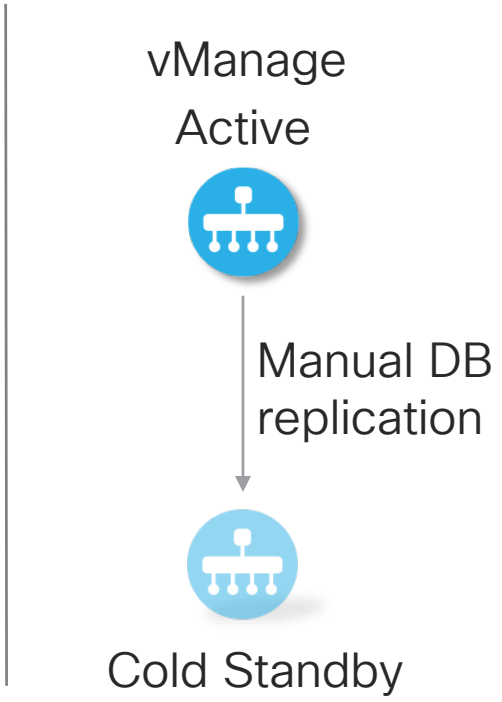


Controller Groups



Standalone vManage – Disaster Recovery

- Prerequisites:
  - Same SW version
  - Signed certificate on standby vManage
  - Synchronized clock
  - Reachable vBond
  - Disabled tunnel-interface on standby vManage



Managing Backup of Active vManage Controller

- Manually creating vManage backup

```
vmanage# request nms configuration-db backup path /home/admin/db_backup
Starting backup of configuration-db
Creating staging directory for backup.
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /home/admin/db_backup.tar.gz
```

- Transporting backup to external location

```
vmanage# vshell
vmanage:~$ scp db_backup.tar.gz admin@192.168.0.100:/home/admin
admin@192.168.0.100's password:
db_backup.tar.gz                              100%  703KB 351.3KB/s   00:02
```

- Caveat: configuration-db does not include local users and repository
- Tip: utilize a script to automate regular backups and exports

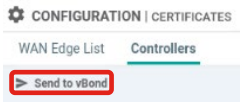
Activating Standby vManage Controller

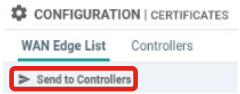
- Import backup to standby vManage

```
Standby-vManage# request nms configuration-db restore /home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

- Check all services are running using `#request nms all status`
- Under *Configuration>Certificates>Controllers* edit existing vBond entries by retyping mgmt IPs and credentials.
- Bring up vManage tunnel-interface
- Send the updated device list to vBond controllers
- Under *Configuration>Certificates>WAN Edge List*

  select *Send to Controllers*
- Invalidate failed vManage controller





Taking VM Level Snapshots

- Taking VM level snapshots for vManage controller is heavily recommended
  - Quick recovery
  - Rollback on controller upgrades
- Similar method is used by Cisco for Cloud hosted environment
  - Daily snapshots kept for 10 day
- Snapshots do not preclude the need for configuration database backups

Designing vManage Cluster with High Availability

vManage Cluster

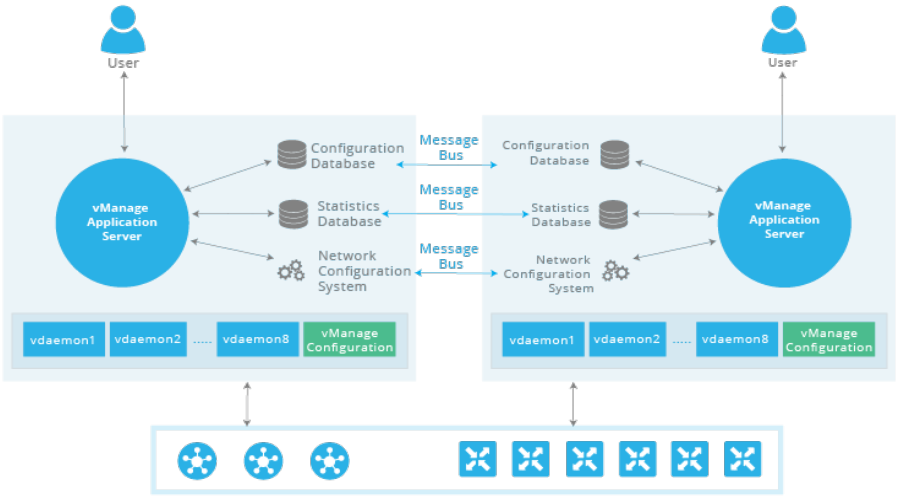
- Why cluster:
  - Managing large number of devices
  - Distributing NMS service load
  - Providing HA and redundancy for FT

vManage Cluster

- Main vManage services:
  - Application Server (GUI)
  - Statistics DB (statistics, logs, alarms, events)
  - Configuration DB (policies, templates, certificates)
  - Messaging Server (used by cluster)

Understanding the vManage Cluster

- Dedicated interface in VPN0 is used for synchronization (10G recommended)
- Required latency below 5ms (same DC)
- Databases run on odd number of members – quorum required
- Control connections are by default load-balanced between all members
- By default all services run on all members in a cluster



vManage Cluster Design – Basic Deployment

- 3 nodes, all services run on all nodes
- In case of single node failure:
  - Remaining nodes can support up to 4000 devices.
  - Configuration and statistics DBs are replicated, no data is lost

	vManage 1	vManage 2	vManage 3
Application Server	✓	✓	✓
Statistics Database	✓	✓	✓
Configuration Database	✓	✓	✓
Messaging Server	✓	✓	✓
Control Connections	✓	✓	✓

vManage Cluster Design – Increasing Stats DB Performance and Scale

- When improved performance and scale of Statistics DB is required
- Configuration DB redundancy is not provided
- Failure of first node will prevent management until recovery
- In case of other node failure, cluster can support up to 6000 devices

	vManage 1	vManage 2	vManage 3	vManage 4
Application Server	✓	✓	✓	✓
Statistics Database		✓	✓	✓
Configuration Database	✓			
Messaging Server	✓			
Control Connections	✓	✓	✓	✓

vManage Cluster Design – Large Deployment

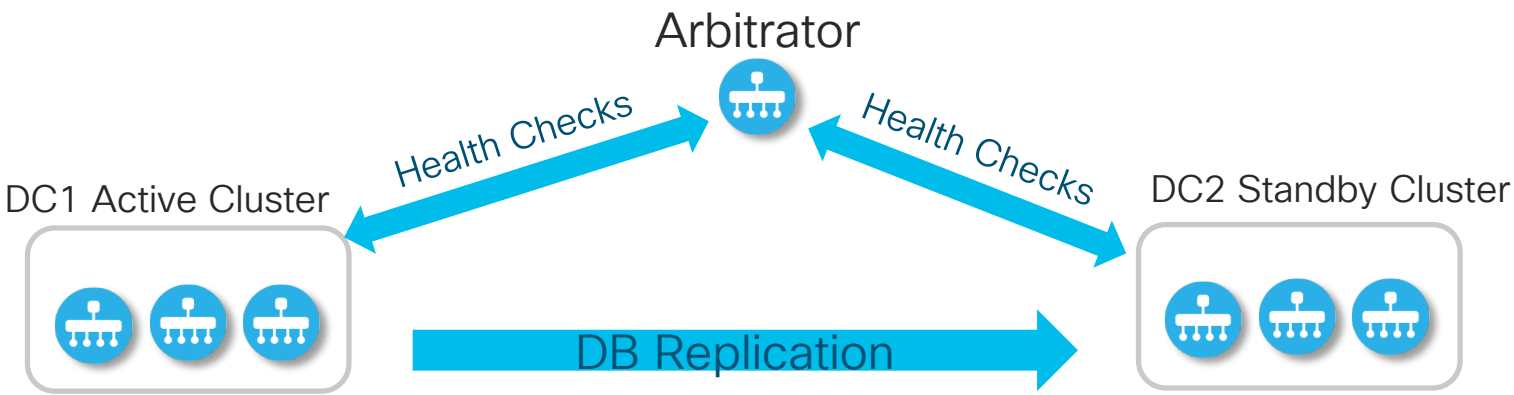
- Improved performance with redundancy
- Nodes 1-3 host everything except Statistics DB. In single node failure scenario can support up to 4000 devices.
- Nodes 4-6 host Statistics DB and no control connections for max performance.

	vManage 1	vManage 2	vManage 3	vManage 4	vManage 5	vManage 6
Application Server	✓	✓	✓	✓	✓	✓
Statistics DB				✓	✓	✓
Configuration DB	✓	✓	✓			
Messaging Server	✓	✓	✓			
Control Conn	✓	✓	✓			

vManage Cluster Disaster Recovery

vManage Cluster Disaster Recovery

- Problem: Cluster nodes must be part of same DC due to low latency requirements. Single cluster does not fulfill DR requirements. Need for automatic failover.
- Solution: Primary cluster, standby cluster, and arbitrator instance, which performs automatic failover in case of failure



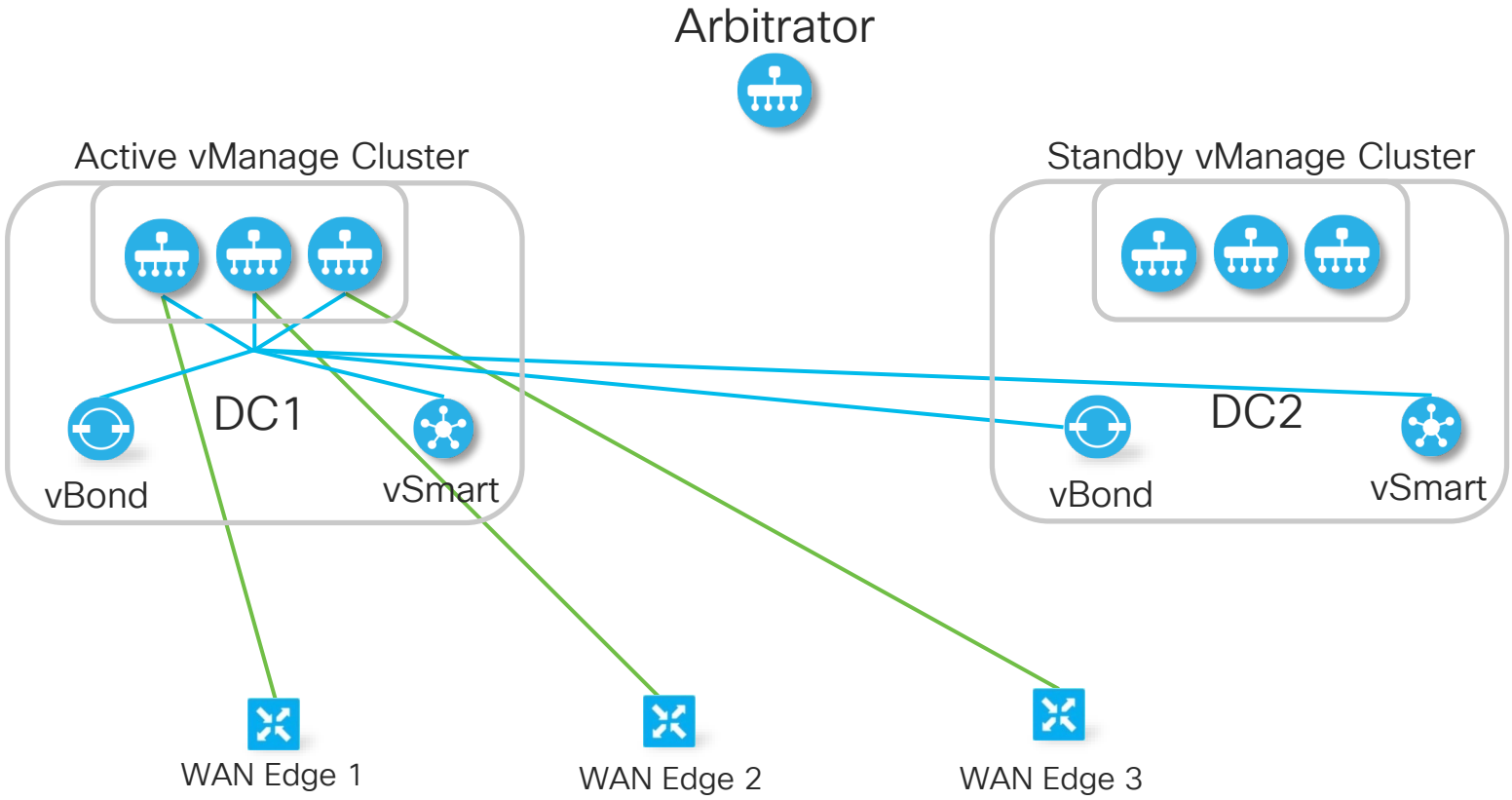
Understanding DR Arbitrator

- Installed as dedicated vManage instance (low resource profile).
- Tracks health state of the cluster.
- Prevents split-brain scenarios.

- Triggers activation of standby cluster in case of disaster (all nodes down).
  - No configuration changes is needed on WAN edge devices.

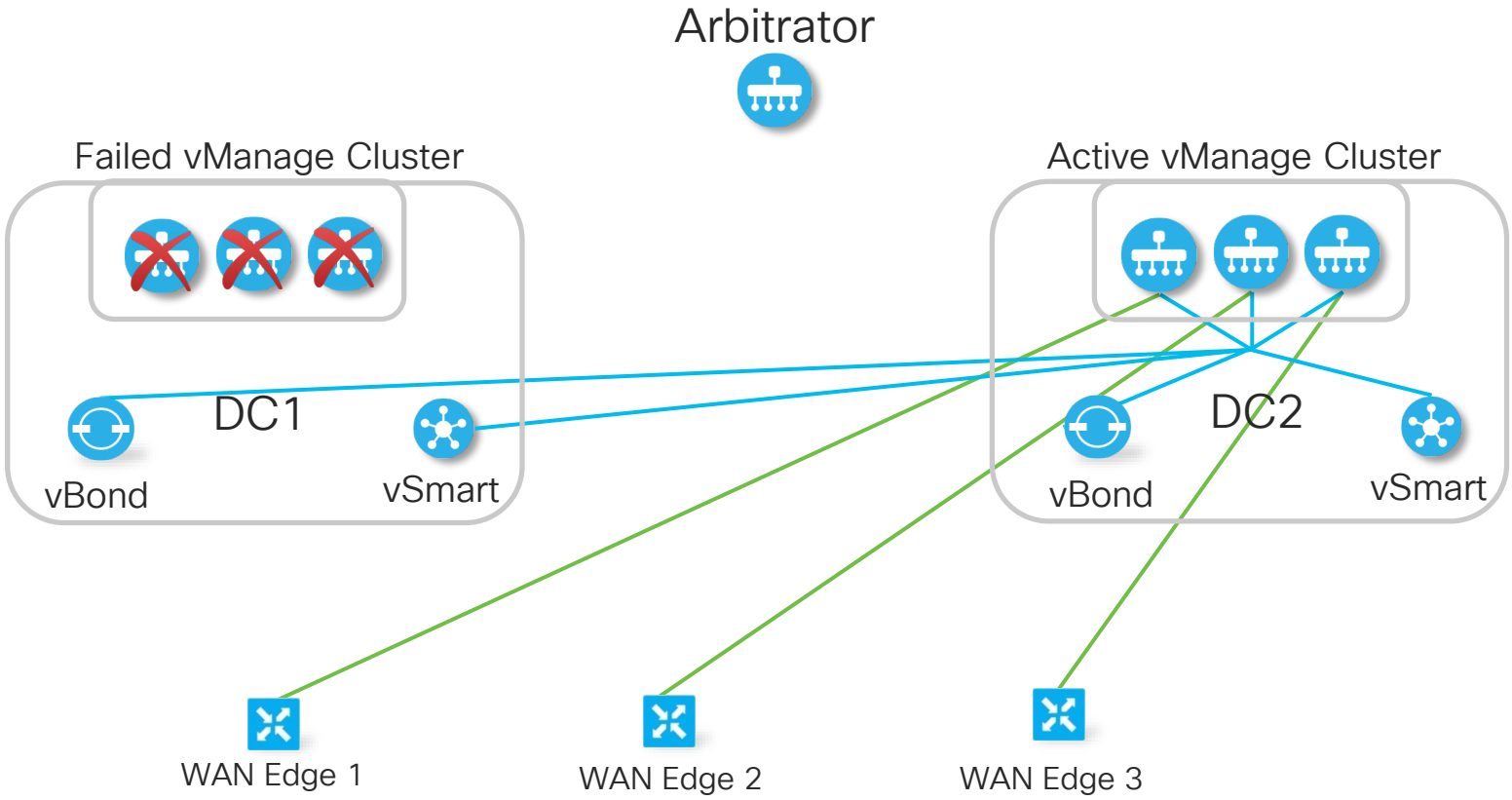
- Arbitrator and cluster members need IP connectivity over enterprise network.

Primary vManage Cluster Active



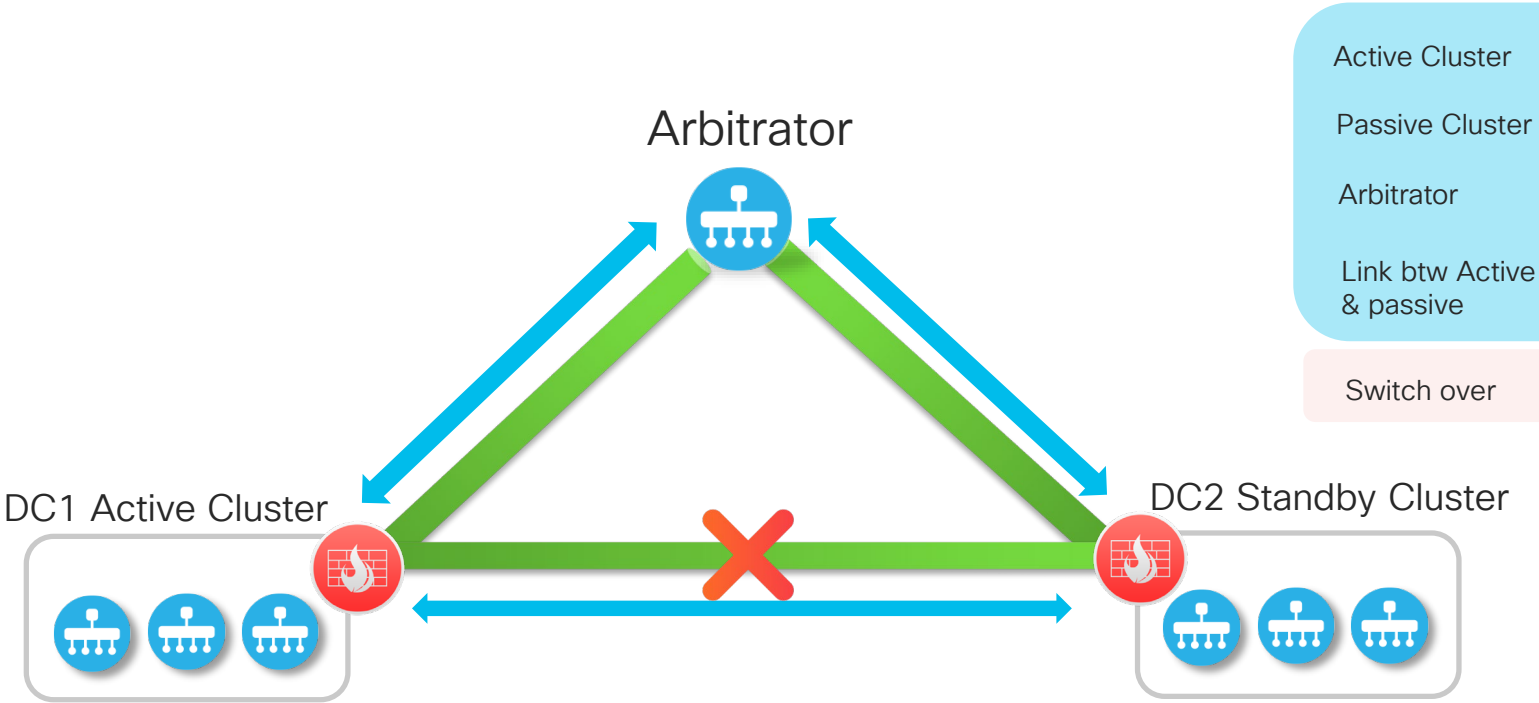
* Control connections between WAN Edges and vBonds/vSmarts not shown

Secondary vManage Cluster Active After Failover

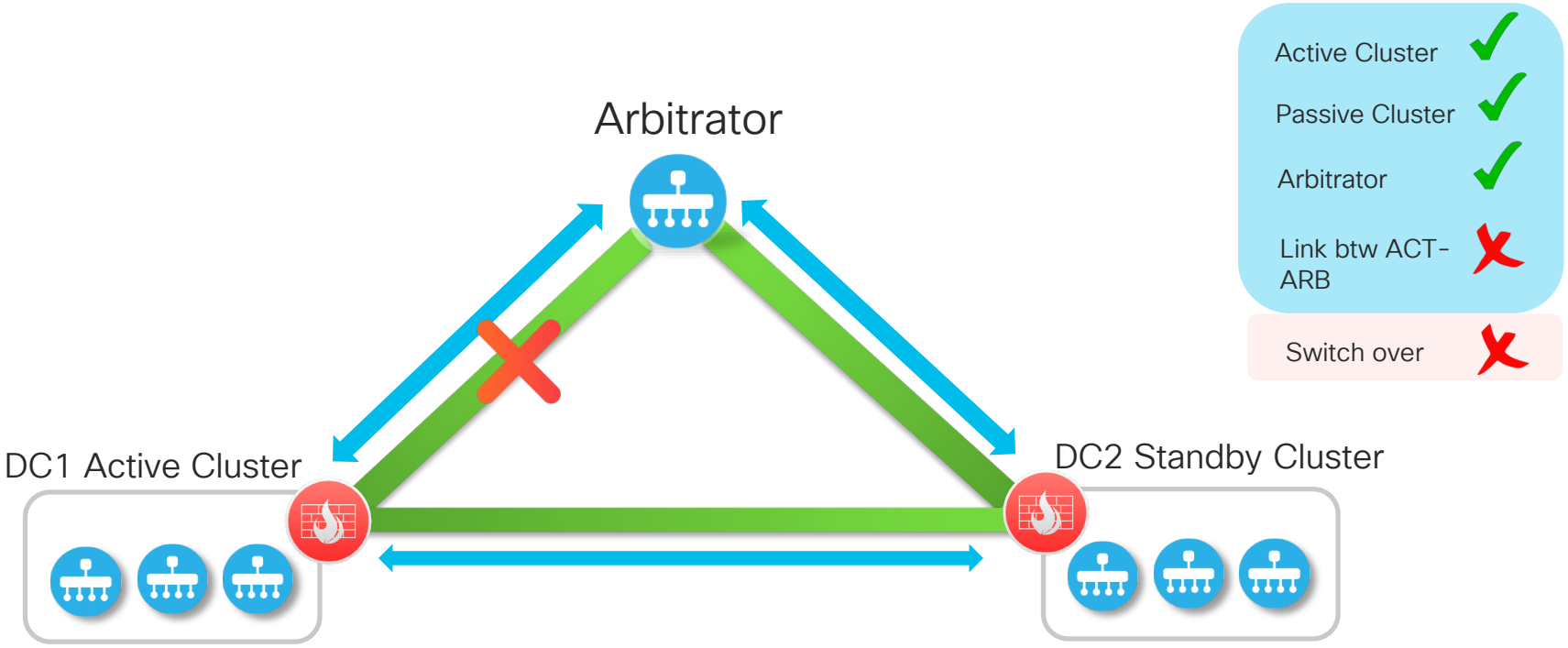


* Control connections between WAN Edges and vBonds/vSmarts not shown

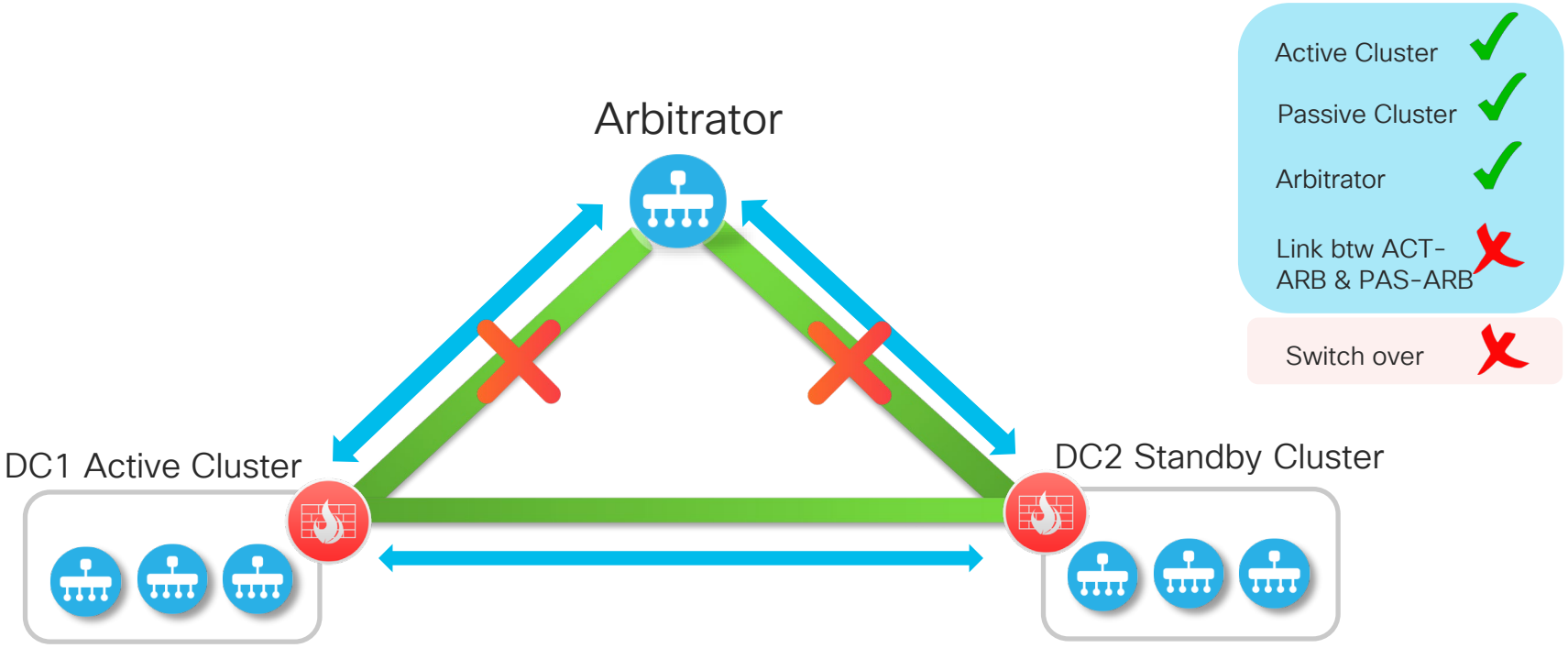
Scenario A) Failed DCI Link Between Clusters



Scenario 2) Failed Connectivity With Arbitrator



Scenario 3) Failed Connectivity With Arbitrator or Failed Arbitrator



Next Steps

- Documentation:

Cisco Documentation

https://sdwan-docs.cisco.com

- Cisco Live On-Demand Library

BRKRST-2559

- Webex Teams room

- SD-WAN Guides (CVDs)

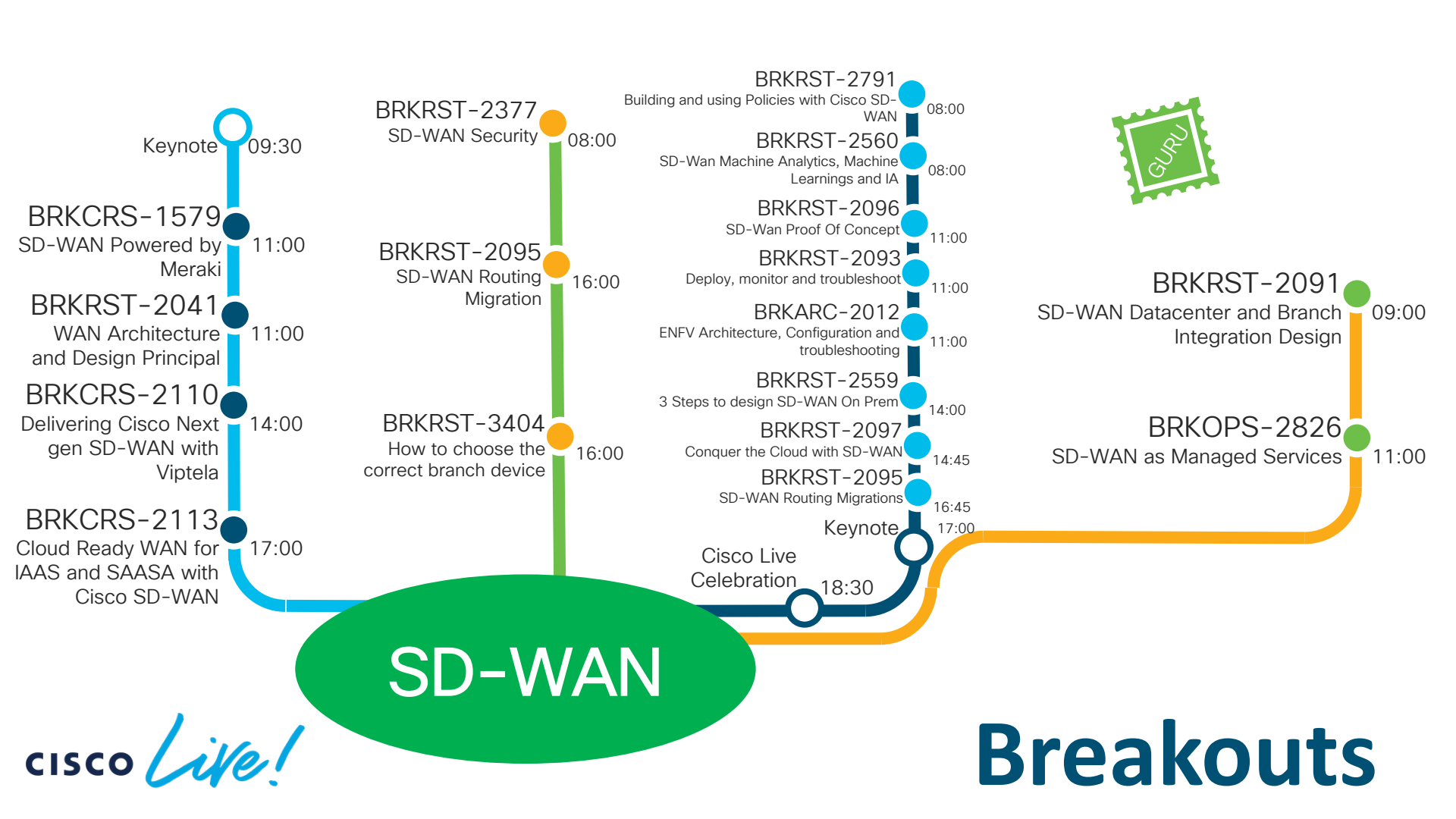
Design Guide, Deployment Guide

vManage Cluster White paper

- SD-WAN TechNotes

Disaster Recovery

cisco Live!


Keynote 09:30
BRKCRS-1579
SD-WAN Powered by Meraki
11:00
BRKRST-2041
WAN Architecture and Design Principal
11:00
BRKCRS-2110
Delivering Cisco Next gen SD-WAN with Viptela
14:00
BRKCRS-2113
Cloud Ready WAN for IAAS and SAASA with Cisco SD-WAN
17:00
BRKRST-2377
SD-WAN Security
08:00
BRKRST-2095
SD-WAN Routing Migration
16:00
BRKRST-3404
How to choose the correct branch device
16:00
BRKRST-2791
Building and using Policies with Cisco SD-WAN
08:00
BRKRST-2560
SD-Wan Machine Analytics, Machine Learnings and IA
08:00
BRKRST-2096
SD-Wan Proof Of Concept
11:00
BRKRST-2093
Deploy, monitor and troubleshoot
11:00
BRKARC-2012
ENFV Architecture, Configuration and troubleshooting
11:00
BRKRST-2559
3 Steps to design SD-WAN On Prem
14:00
BRKRST-2097
Conquer the Cloud with SD-WAN
14:45
BRKRST-2095
SD-WAN Routing Migrations
16:45
Keynote
17:00
Cisco Live Celebration
18:30
GURU
BRKRST-2091
SD-WAN Datacenter and Branch Integration Design
09:00
BRKOPS-2826
SD-WAN as Managed Services
11:00
SD-WAN
cisco Live!
Breakouts

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

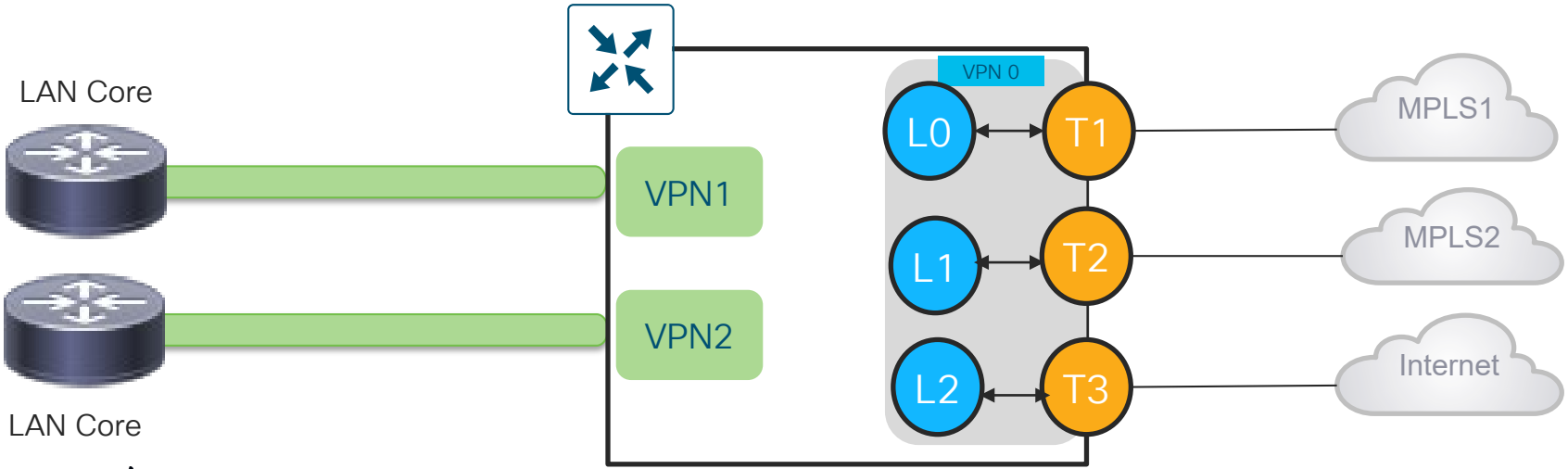
Thank you

cisco Live!

You make **possible**

Loopback Interface – Bind mode

- In case of bind mode, each loopback is bound to a physical interface
- Traffic destinated to loopback will be carried to and from mapped physical interface
- This can be used when customers have connected subnets on transport side, and can use loopback to form control connections and data tunnels.



Loopback Interface – Unbind Mode

- In case of unbind mode, loopback interface is not bound to any physical interface
- Traffic destinated to loopback can go through any physical interface (Based on hash lookup)
- This can be used when there are multiple transports available to same provider