The bridge to possible

Designing On-Prem SD-WAN Controllers

Chandra Balaji Rajaram, Technical Marketing Leader, Cisco SD-WAN

Cisco Webex App

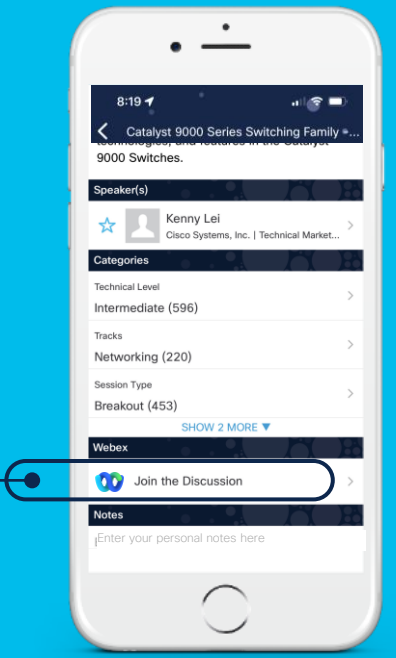
Questions?

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

Webex spaces will be moderated until February 24, 2023.

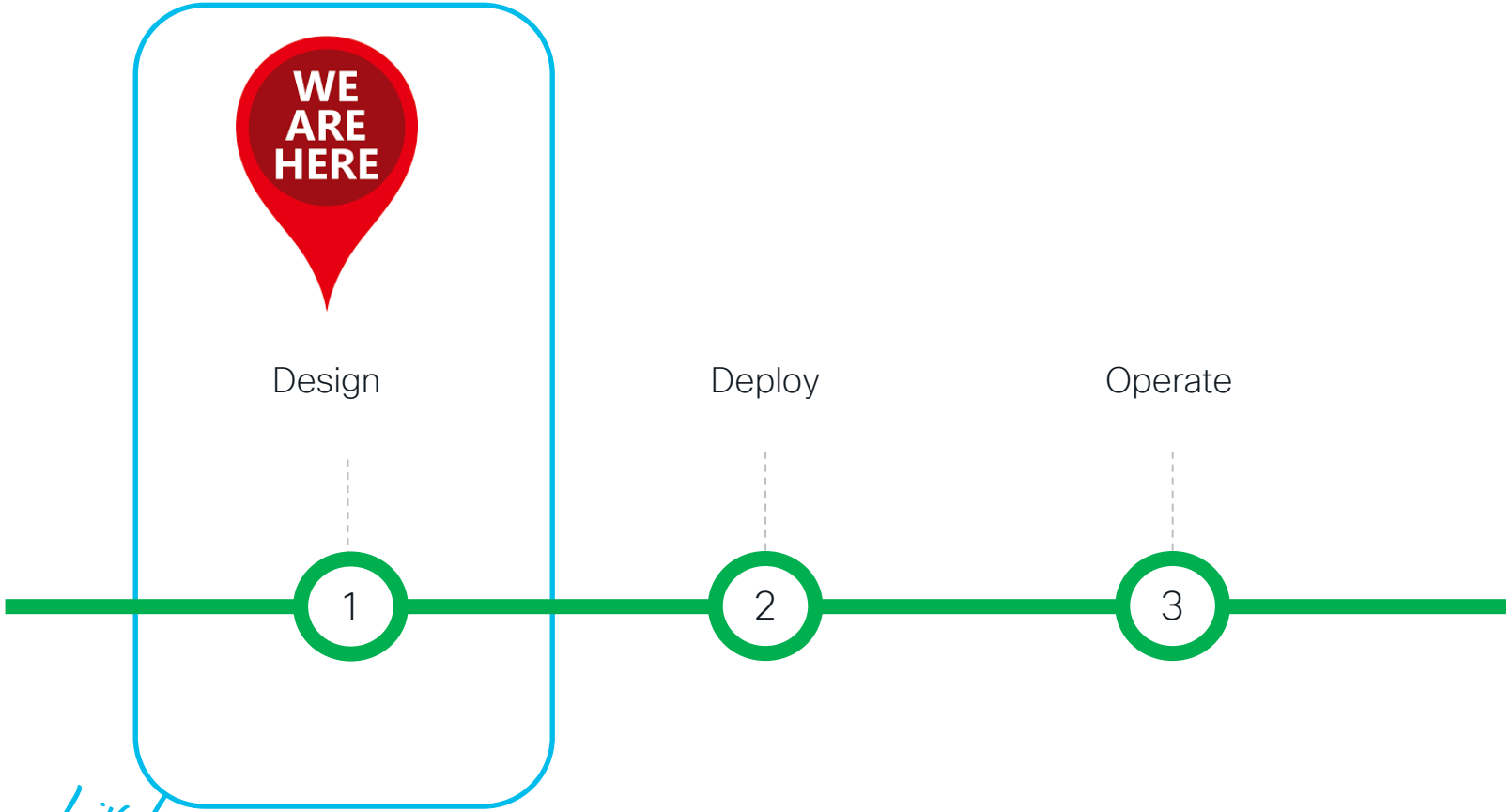


Agenda

- Introduction
- The Design Phase
- The Deployment Phase
- The Operational Phase
- Conclusion

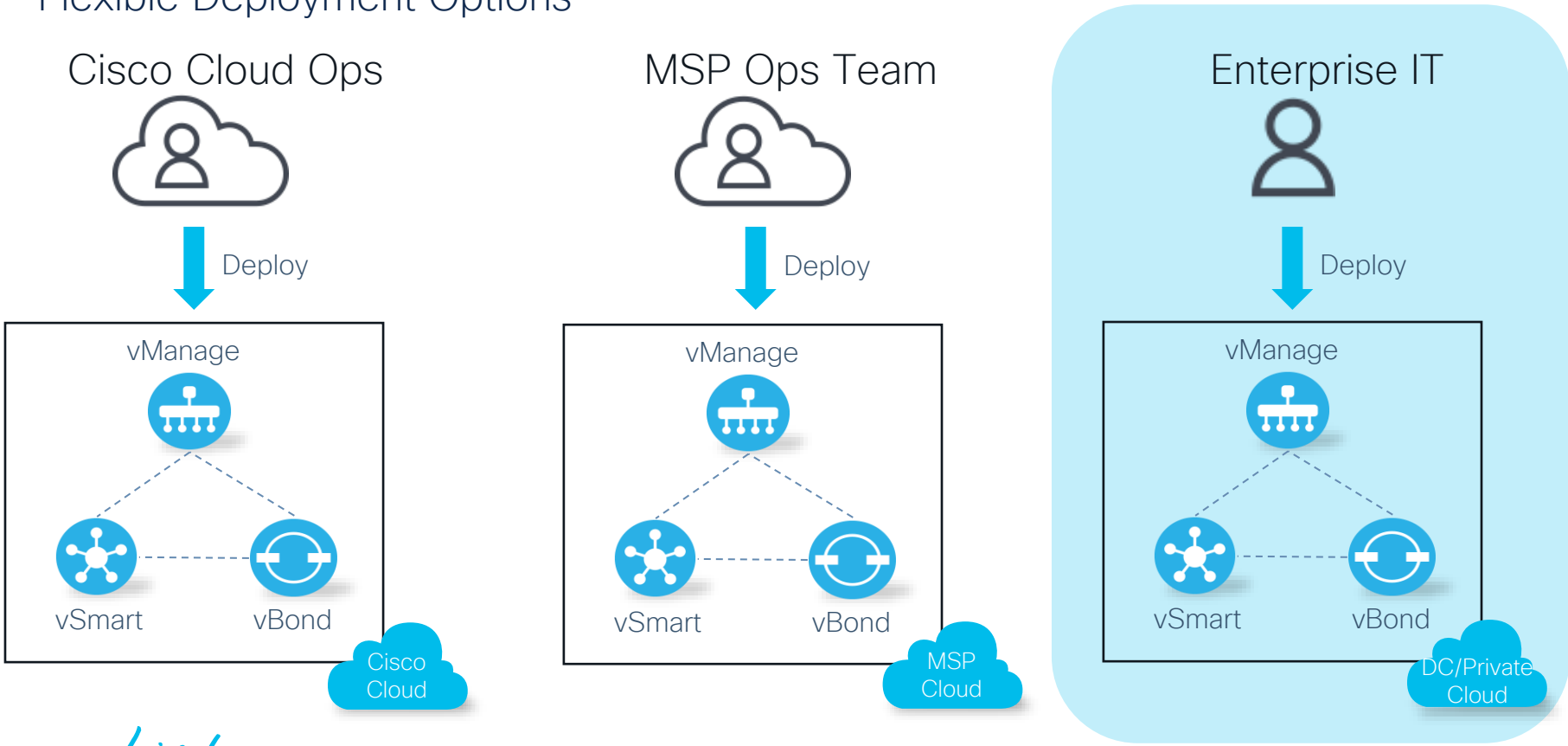
Introduction

1, 2, 3 … On-prem controller design & deployment

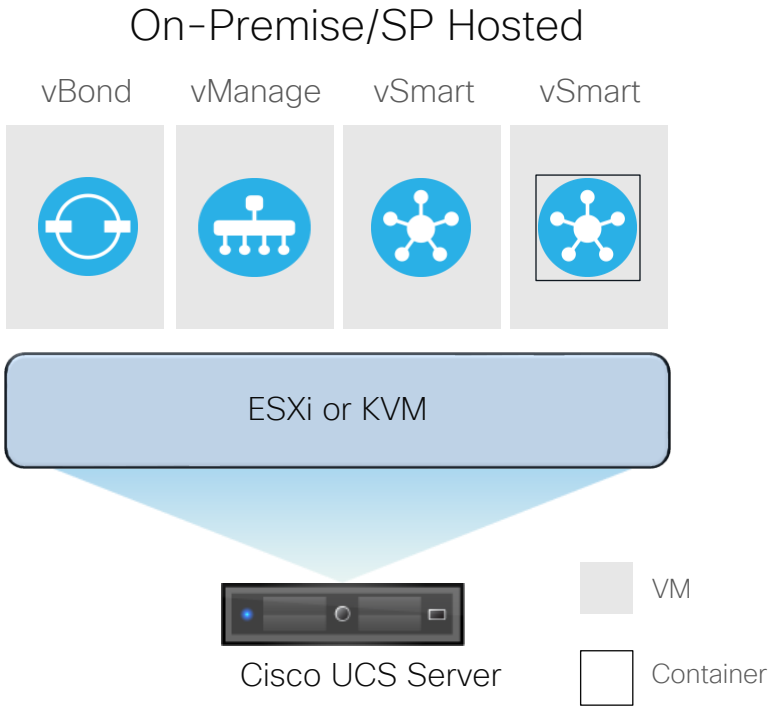


Cisco SD-WAN Controllers

Flexible Deployment Options



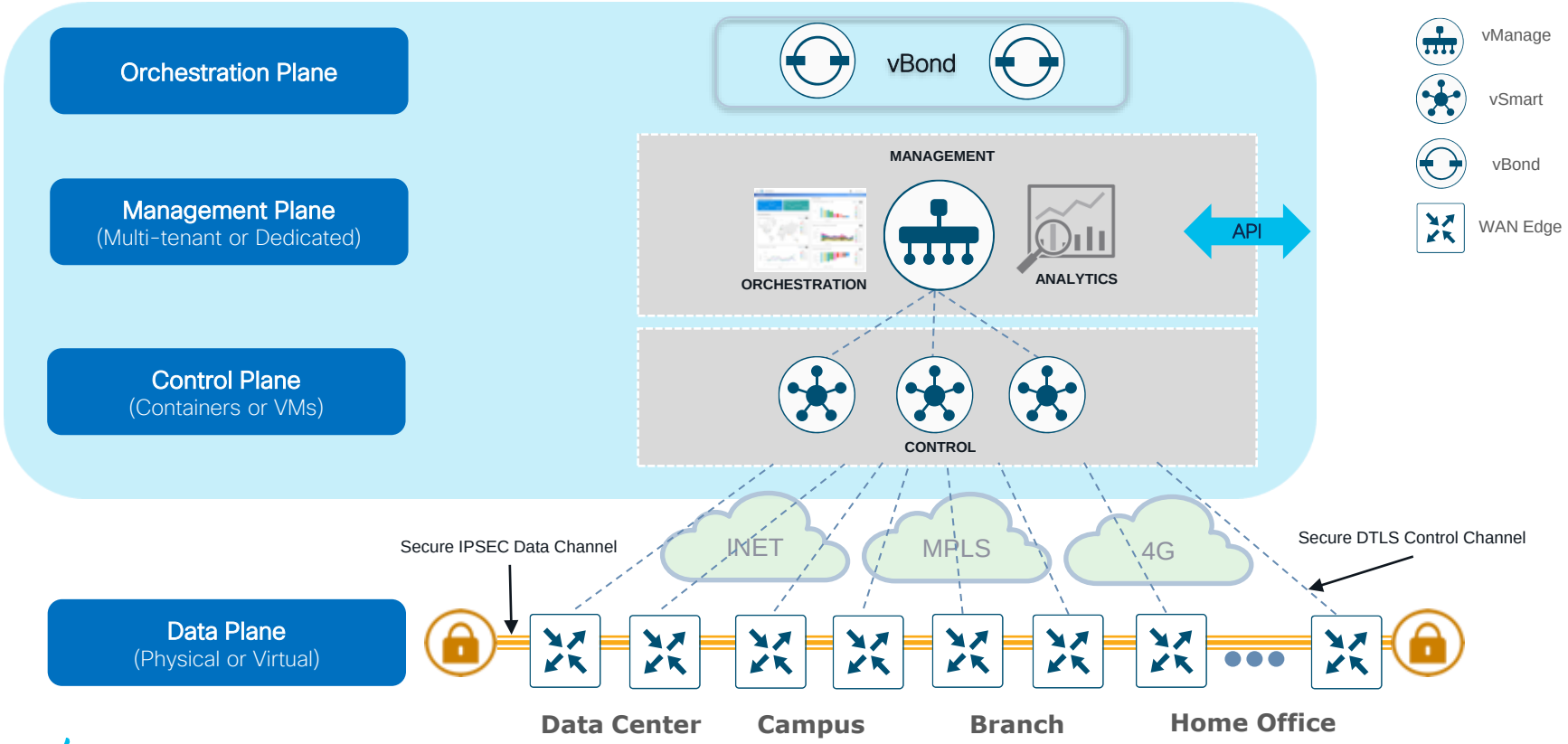
Controllers Deployment Methodology



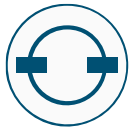
Controller Architecture Overview

Controller Architecture Overview

Applying SDN Principles To The Wide Area Network



Cisco SD-WAN Controllers



vBond

- Orchestrates control and management plane
- First point of authentication
- Distributes list of vSmarts/ vManage to all Edge routers
- Facilitates NAT traversal
- Requires public IP Address [could sit behind 1:1 NAT]
- Highly resilient
- Multitenant or single tenant

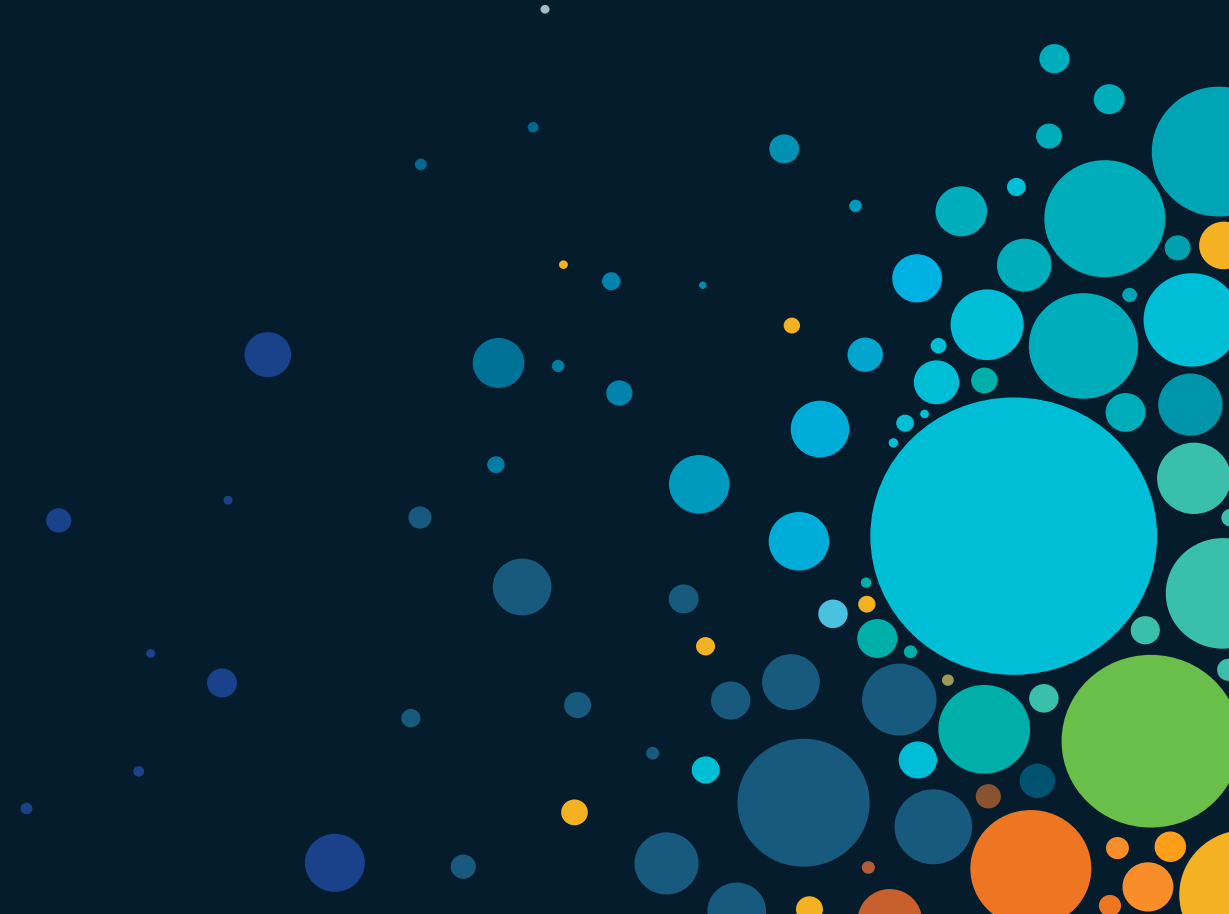
vManage

- Single pane of glass for Day0, Day1 and Day2 operations
- Centralized provisioning
- Multitenant or single tenant
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC
- Programmatic interfaces (REST, NETCONF)
- Highly resilient

vSmart

- Facilitates fabric discovery
- Disseminates control plane information between Edge routers
- Distributes data plane and app-aware routing policies to the Edge routers
- Implements control plane policies
- Dramatically reduces control plane complexity
- Highly resilient & supports Multitenancy

The Design Phase



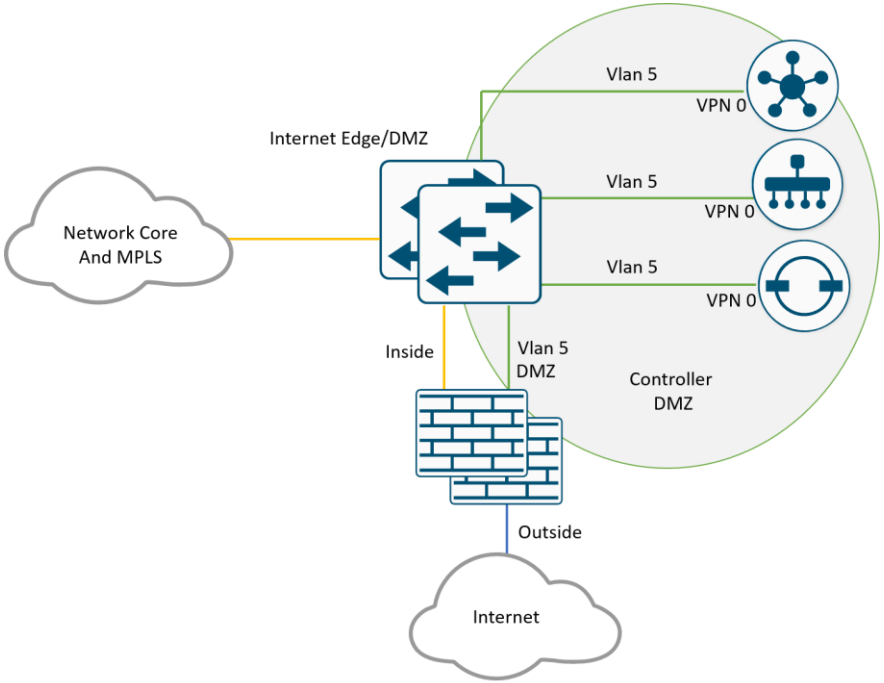
Controller Placement Options

Key Points

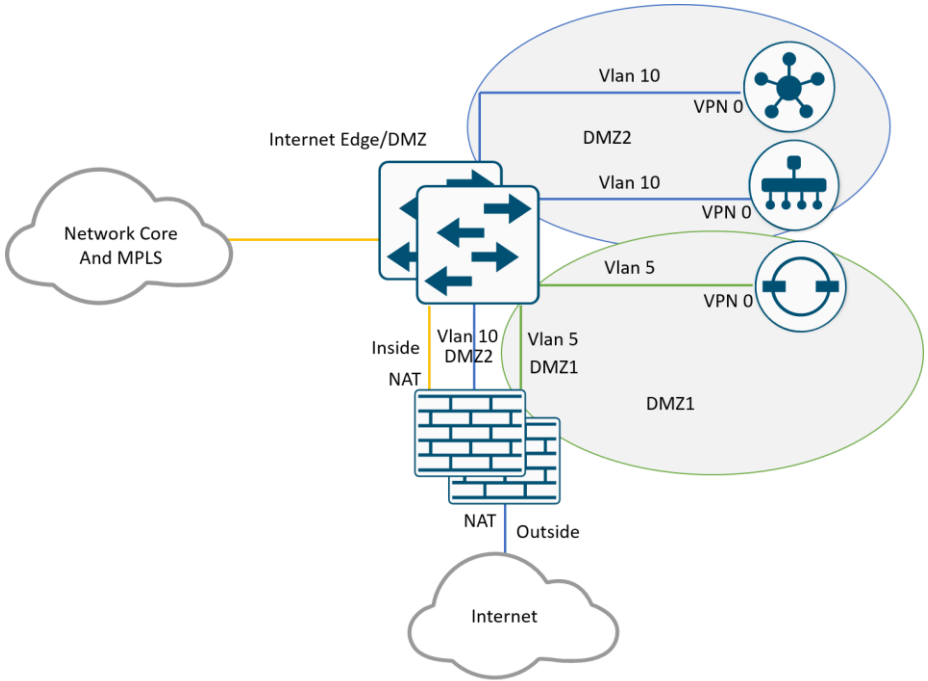
Regardless of the placement of the controllers in DataCentre, please keep the following rules in mind:

- All controllers must be reachable to each other via their VPN 0 interface.
- If available, vManage and vSmart controllers communicate to the vBond orchestrator using their publicly routable IP addresses. The vBond learns about both private and public addresses of the vSmart and vManage controllers and send this information to WAN Edge routers sitting outside the datacenter.
- The combination of transport colors on the interface tunnels of the vSmart and vManage controllers the same on the WAN Edge routers decides whether public (Post-NAT) or private (Pre-NAT) addressing of the controllers will be used by the WAN Edge routers while making control connections.
- Ensure any firewall in the path has the appropriate ports open for proper communication between controllers, as well as between WAN Edge routers and the controllers.

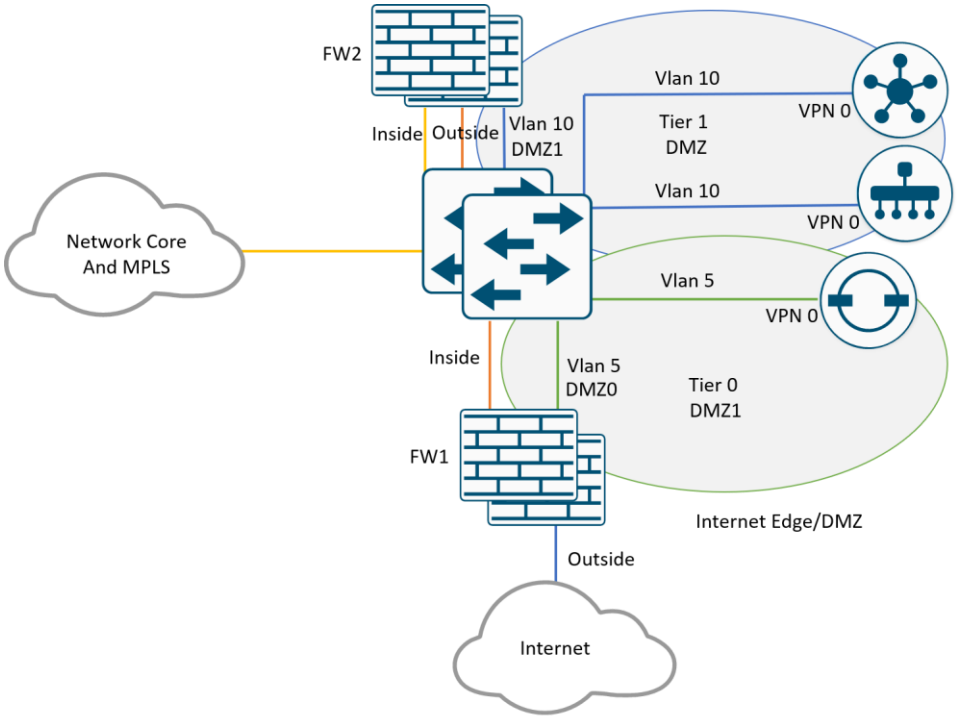
Controllers within same DMZ



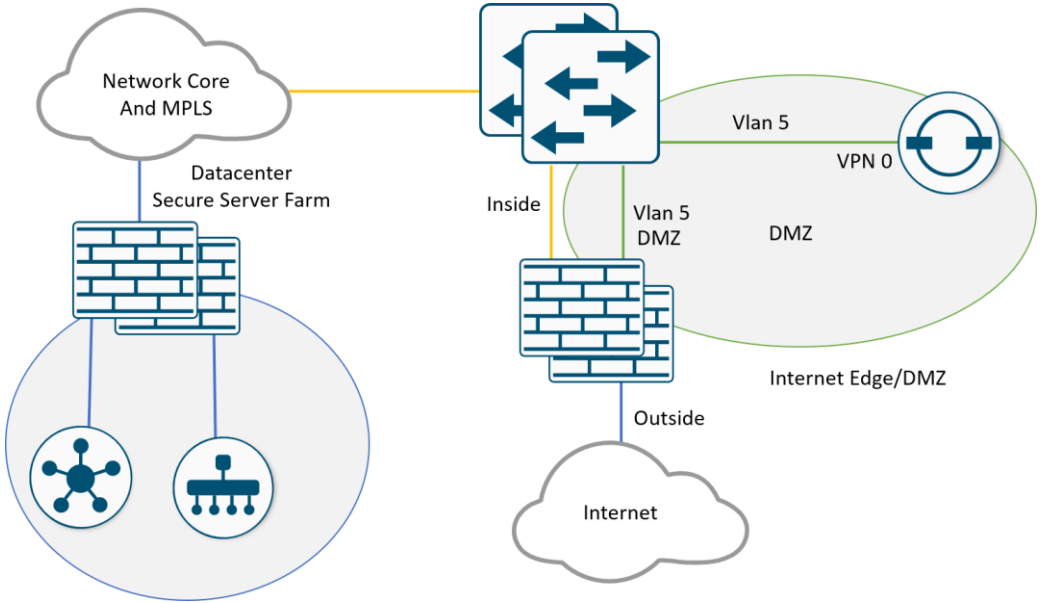
Controllers split between Multiple DMZs



Controllers split between Tiered DMZs



Controllers behind a Secure Datacenter Server Farm



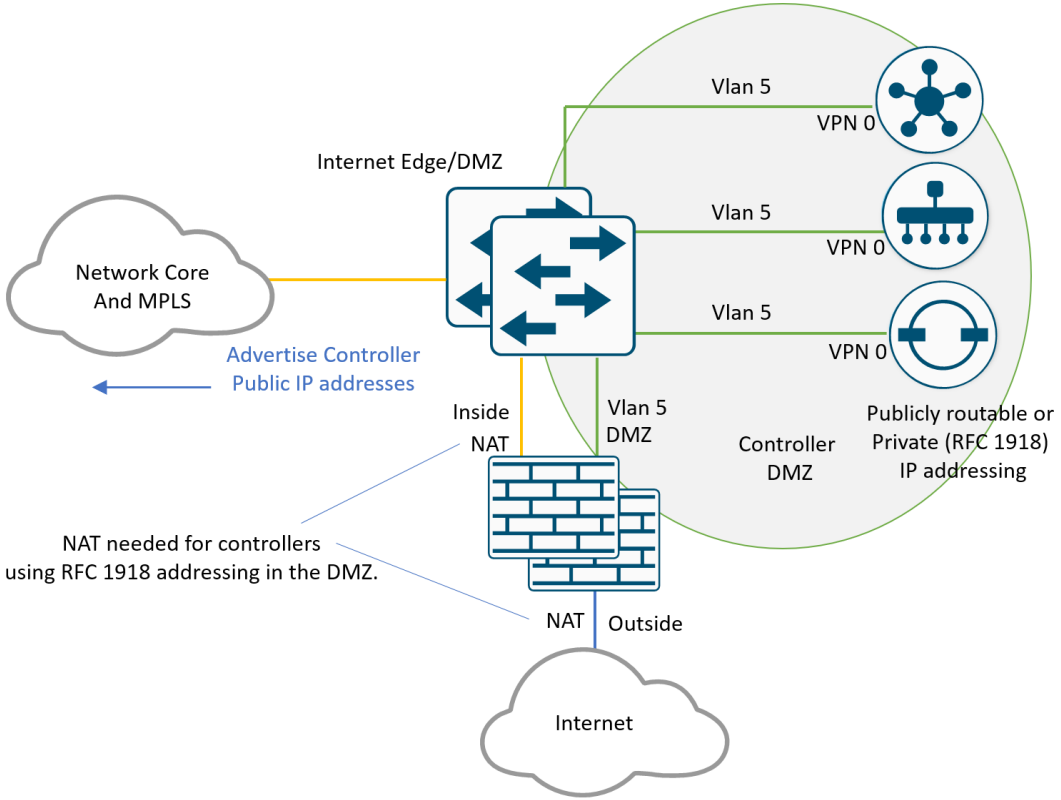
Controller Configuration

Once placed in the datacenter, there are multiple ways to arrange and configure the controllers using NAT, color, public IPs, and/or private IPs. This section outlines public/private IP addressing, NAT, color, and site-ID requirements for the different use cases. Though the diagrams show controllers residing in one or two DMZs, note that controllers can be positioned in other places within the physical network.

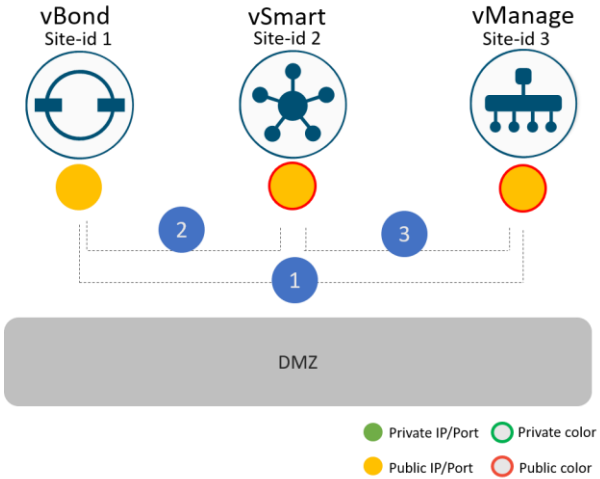
The following major options are covered for on-premise deployments:

- Public IP: Control connections are established through both the Internet and MPLS transports using publicly routable or post-NATed IP addresses.
- Public/Private IP: Control connections are established through the MPLS transport using private IP or Pre-NATed IP addresses and established through the Internet using publicly routable or Post-NATed IP addresses.
- MPLS only with vBond STUN server: Controllers are deployed on the private MPLS network, and control connections are established only through the MPLS network. An additional vBond is set up on the Internet so that Internet-connected devices can form data plane (IPSec and BFD sessions) with other devices over that transport

Controller Publicly Routable IP Address for MPLS and Internet Transports

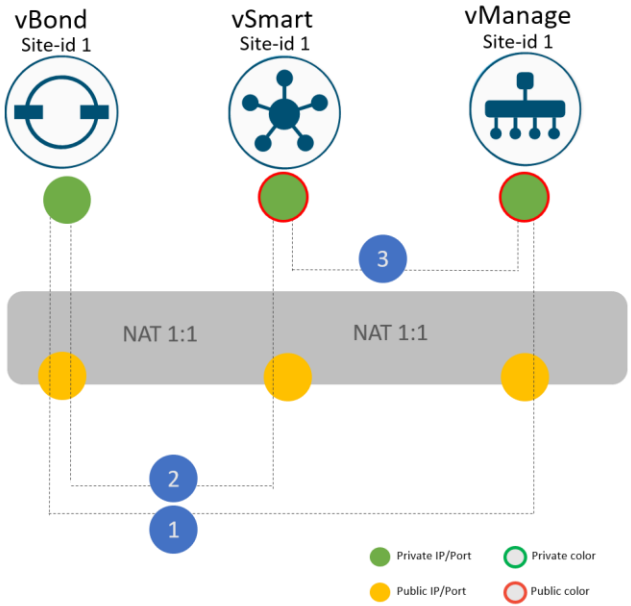


Controllers configured with Publicly routable IP addresses



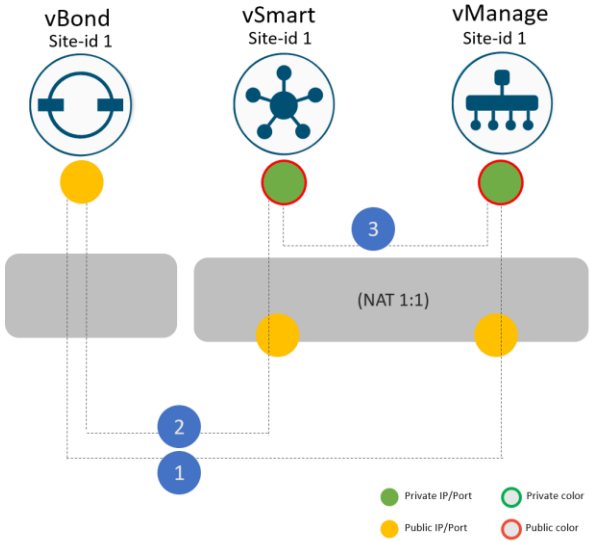
- **(1) (2)** vSmart and vManage point to the vBond publicly routable IP address
- Traffic between controllers need not traverse the firewall. The vBond orchestrator learns the publicly routable IP addresses of both the vManage and vSmart controllers. The private and public IP addresses of the controllers are the same.
- **(3)** vManage and vSmart controllers use their publicly routable IP addresses for communication.

Controllers configured with Private addresses & 1:1 NAT



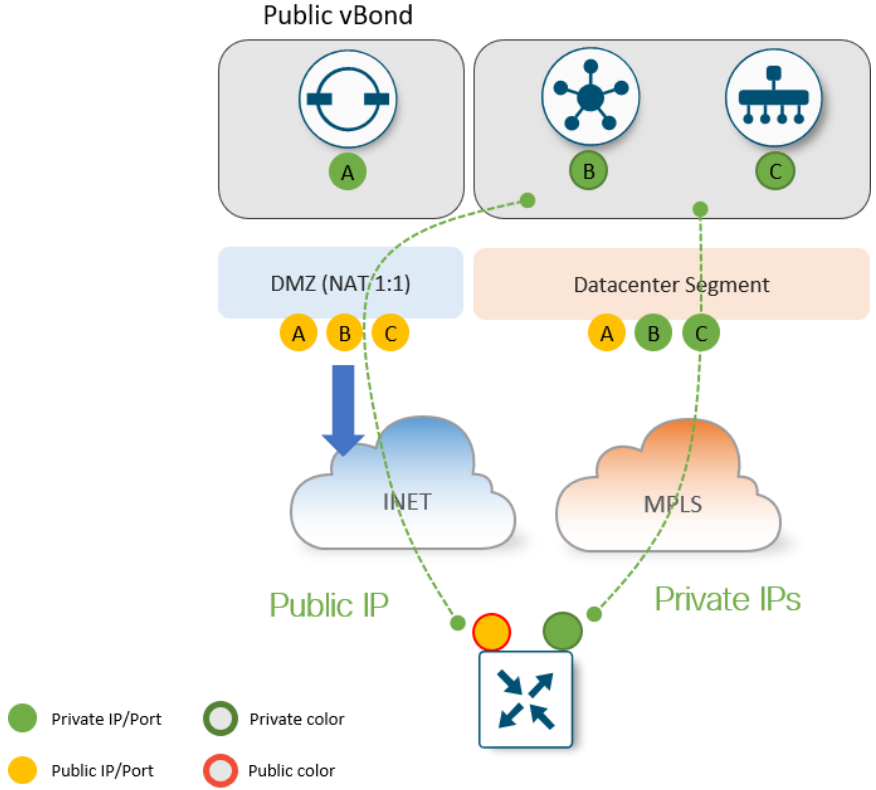
- Public color is used on the controllers so post-NAT IP addresses are used in communication with WAN Edge routers
- **(1) (2)** vSmart and vManage point to the vBond NATed public IP address
- Firewall is configured with hairpin NAT and each controller's source private IP address is NATed when traffic traverses the firewall
- vBond learns the private and NATed public IP address of the vSmart and vManage (private is pre-NAT, public is post-NAT)
- **(3)** vSmart and vManage use private IP addresses for communication because both are configured for public color and the site-ids are the same.

vBond with a Publicly routable IP address, vSmart & vManage with Private addresses

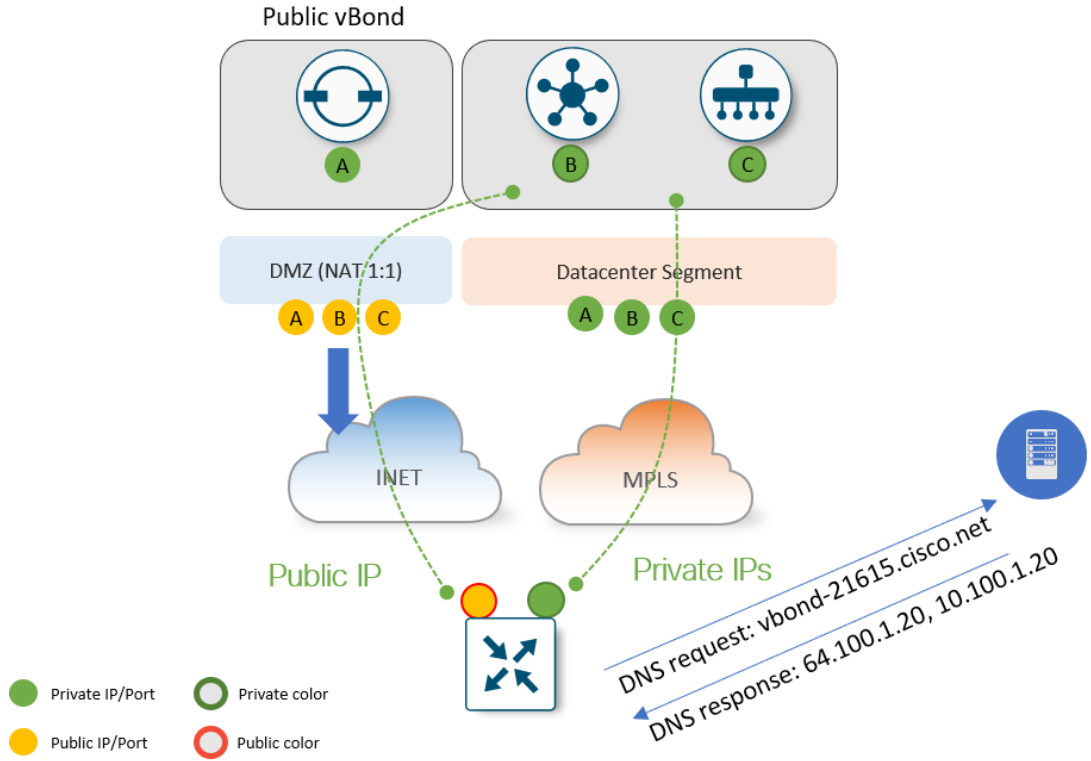


- Public color is used on the controllers so post-NAT IP addresses are used in communication with WAN Edge routers
- **(1) (2)** vSmart and vManage point to the vBond public IP address
- Firewall is configured with one-to-one NAT and each controller's source private IP address is NATed when traffic traverses the firewall
- vBond learns the private and NATed public IP address of the vSmart and vManage (private is pre-NAT, public is post-NAT)
- **(3)** vSmart and vManage use private IP addresses for communication because both are configured for public color and the site-ids are the same

Reachability to vBond via a Publicly Routable IP Address on MPLS and Internet (Recommended)

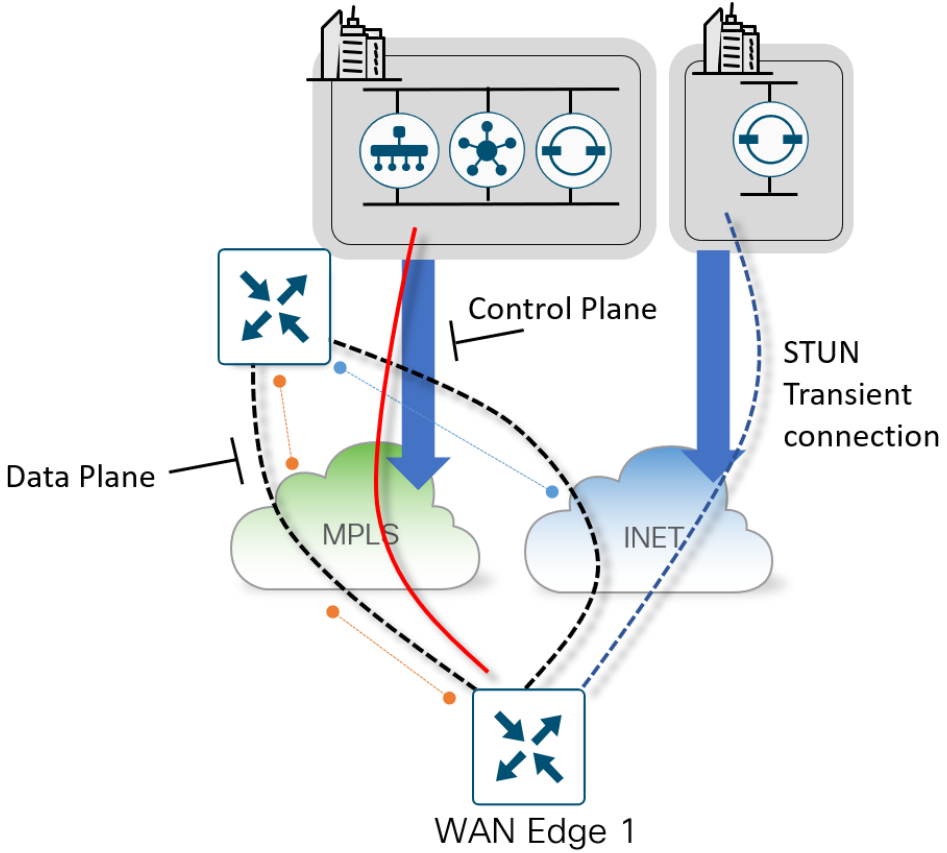


Reachability to vBond via its Private (RFC 1918) IP Address on MPLS and its Publicly Routable IP Address on Internet



MPLS Only With vBond STUN Server

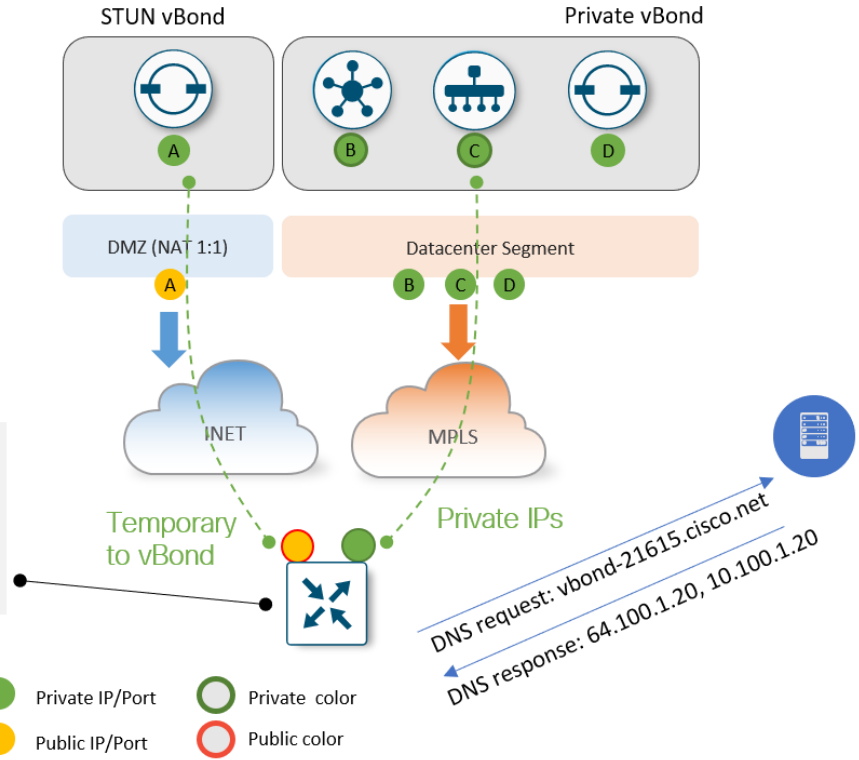
Control Connections Only on MPLS with Internet STUN Server



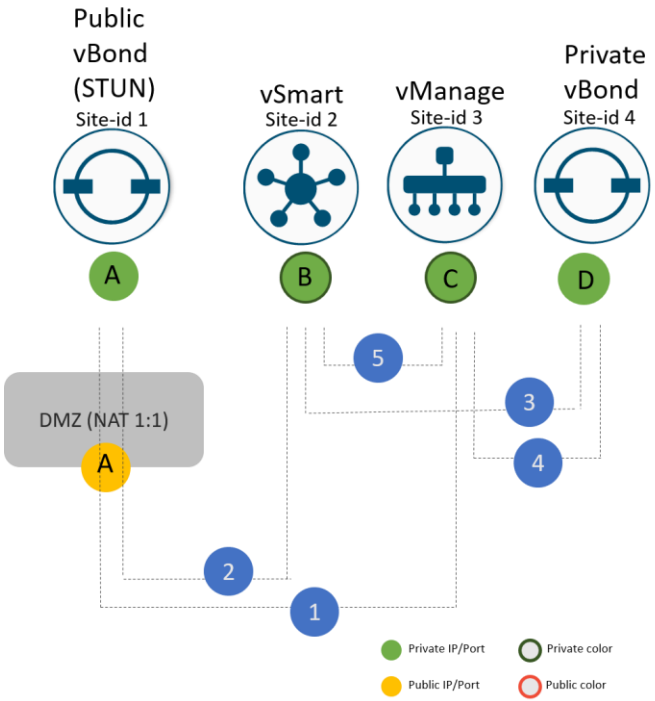
MPLS Only With vBond STUN Server

Control Connections Only on MPLS with Internet STUN Server

```
vpn 0
 interface ge0/0
  tunnel-interface
   vbond-as-stun-server
   color public-internet
```

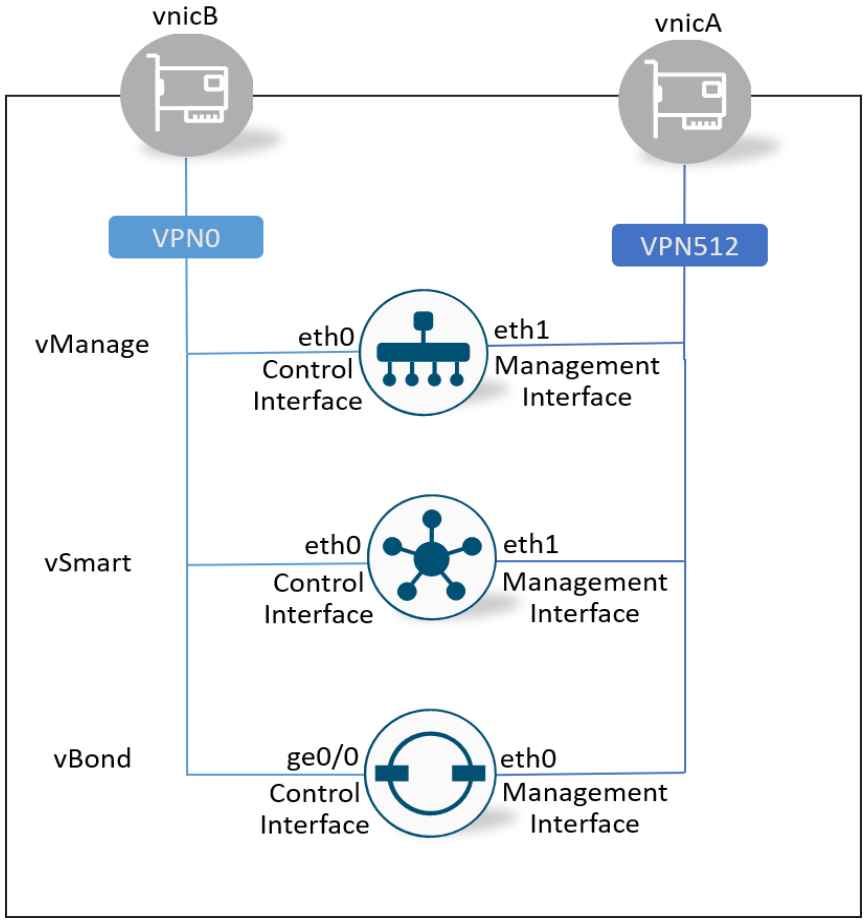


MPLS Only With vBond STUN Server



- Private color is used on the controllers so pre-NAT IP addresses are used in communication with WAN Edge routers on the private MPLS transport
- **(1) (2) (3) (4)** vSmart and vManage point to the vBond domain name, which resolves to the public IP address of the public vBond and the private address of the private vBond. There are no control connections on the Internet transport, hence there is no NAT applied to the vSmart or vManage servers
- The private vBond learns the private IP address of the vSmart and vManage so WAN Edge routers can make control connections on the MPLS transport.
- **(5)** vSmart and vManage use pre-NAT private IP addresses for communication because their tunnel transport color is private

Controller Virtual Interfaces



vManage Clustering

vManage Clustering

- A vManage cluster is a set of independent processing vManage instances where are all are simultaneously active and connected through a high-speed, cluster interface.
- Distributes the various NMS service loads and provide high availability and scalability
- Control connections from the WAN Edge routers are load-balanced to different vManage server instances within the cluster. Controller connections (from each vManage core to each vSmart and each vBond) are fully meshed
- Should be designed to tolerate failure of a single vManage instance failure, while the cluster remains operational. For HA, a standby cluster should be deployed in a different geographical location in the event of a cluster failure or connectivity failure to the site where the vManage cluster resides.

vManage Personas

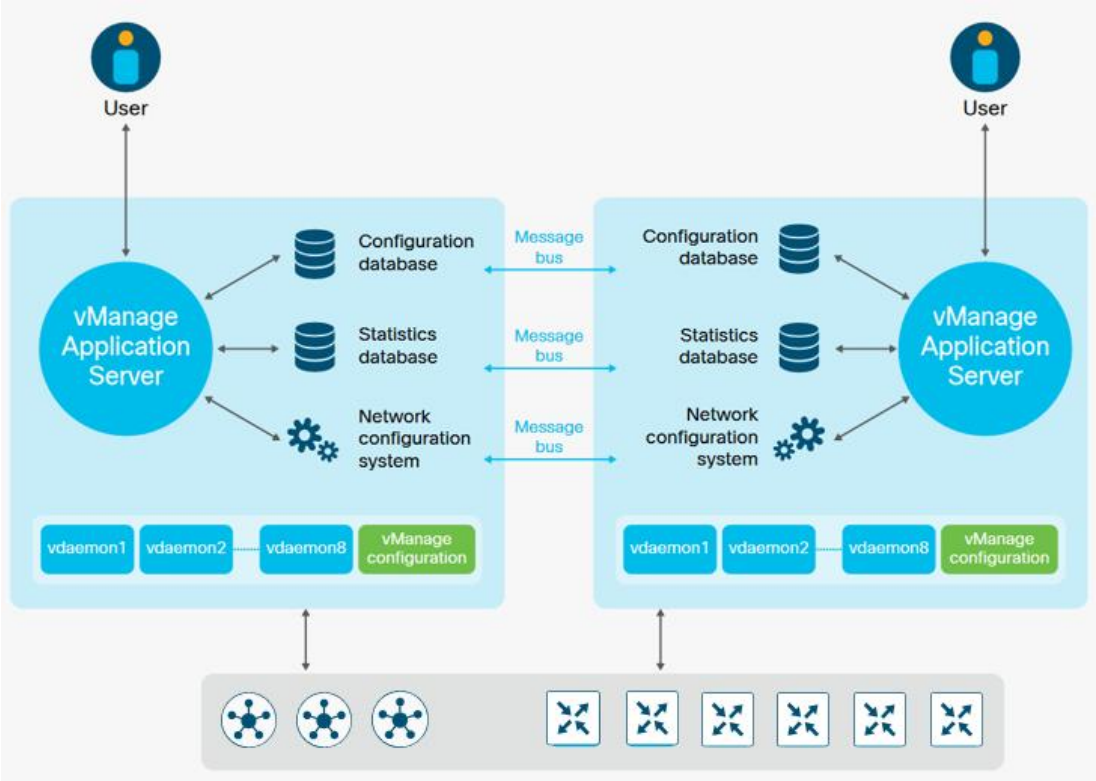
Simplifies adding Cisco vManage servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

A Cisco vManage server can have any of the following personas:

- Compute+Data: Includes all services that are required for Cisco vManage, including services that are used for the application, statistics, configuration, messaging, and coordination
- Compute: Includes services that are used for the application, configuration, messaging, and coordination
- Data: Includes services that are used for the application and statistics

Each Cisco vManage server has a storage device assigned to it. A storage device is a hard drive that contains the /opt/data partition on which the database and other configuration information is saved.

vManage Clustering



vManage Clustering – Key design considerations

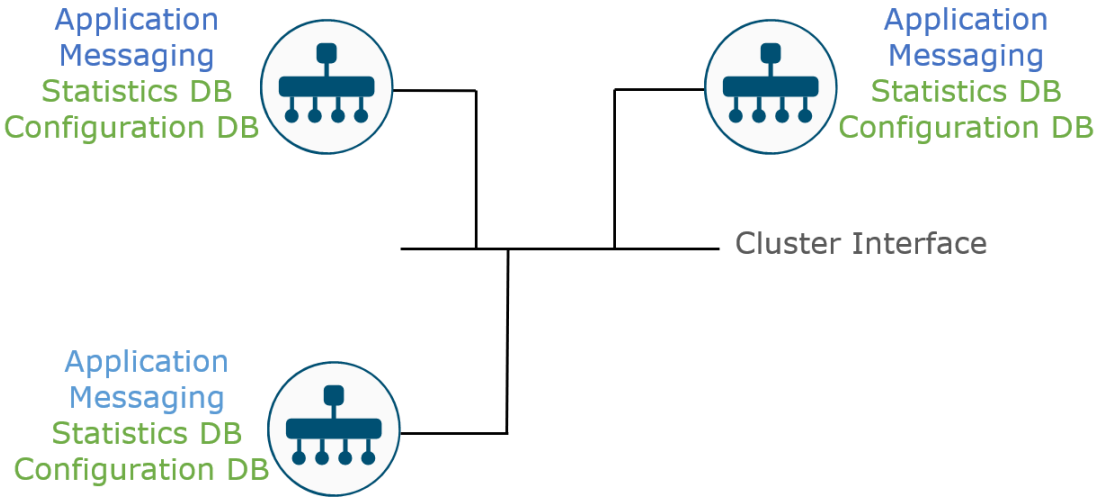
- All vManage instances should be located at same DC and have the same & recommended server resources (vCPU, memory, and hard disk space).
- Ensure that time is synced between servers and that each vManage server has the same admin password set.
- For clustering purposes, a third interface is required besides the interfaces used for VPN 0 (transport) and VPN 512 (management). This interface resides in VPN 0 is used for communication and syncing between the vManage servers within the cluster. This interface should be at least 1 Gbps, and have latency of 4 ms or less. A 10Gbps interface, however, is recommended.

➢ Tip: In ESXi, the VMXNET3 NIC interface supports 10G, but the vManage OVA does not allow you to select it by default. To be able to select this, you should change the Guest OS type to a 64-bit Linux version, such as RHEL 6.

vManage Clustering – Key design considerations

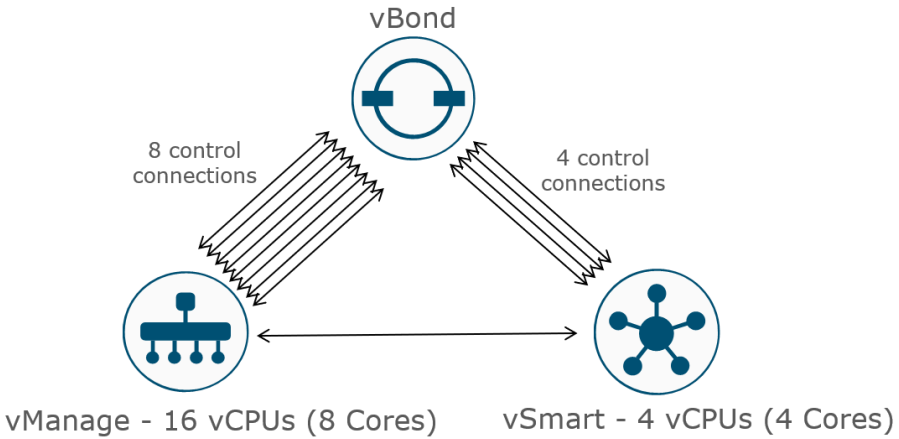
- A standalone vManage can be turned into a cluster at any time but enabling multitenancy on a vManage cluster is NOT possible, if it was initially deployed as a single tenant. Hence, a single tenant vManage needs to be deployed with multitenancy enabled, and additional vManage servers can be added to it to form a cluster.
- Changes to a cluster may require services to reload or servers to reboot. Any cluster configuration changes should be done during a maintenance window.
- The application and messaging services should run on all vManage servers.
- The configuration and statistics service must be run on an odd number of devices. For sufficient redundancy, these services should be run on at least three vManage instances, and they do not have to run together on the same nodes.

Example of a 3 Node vManage Cluster



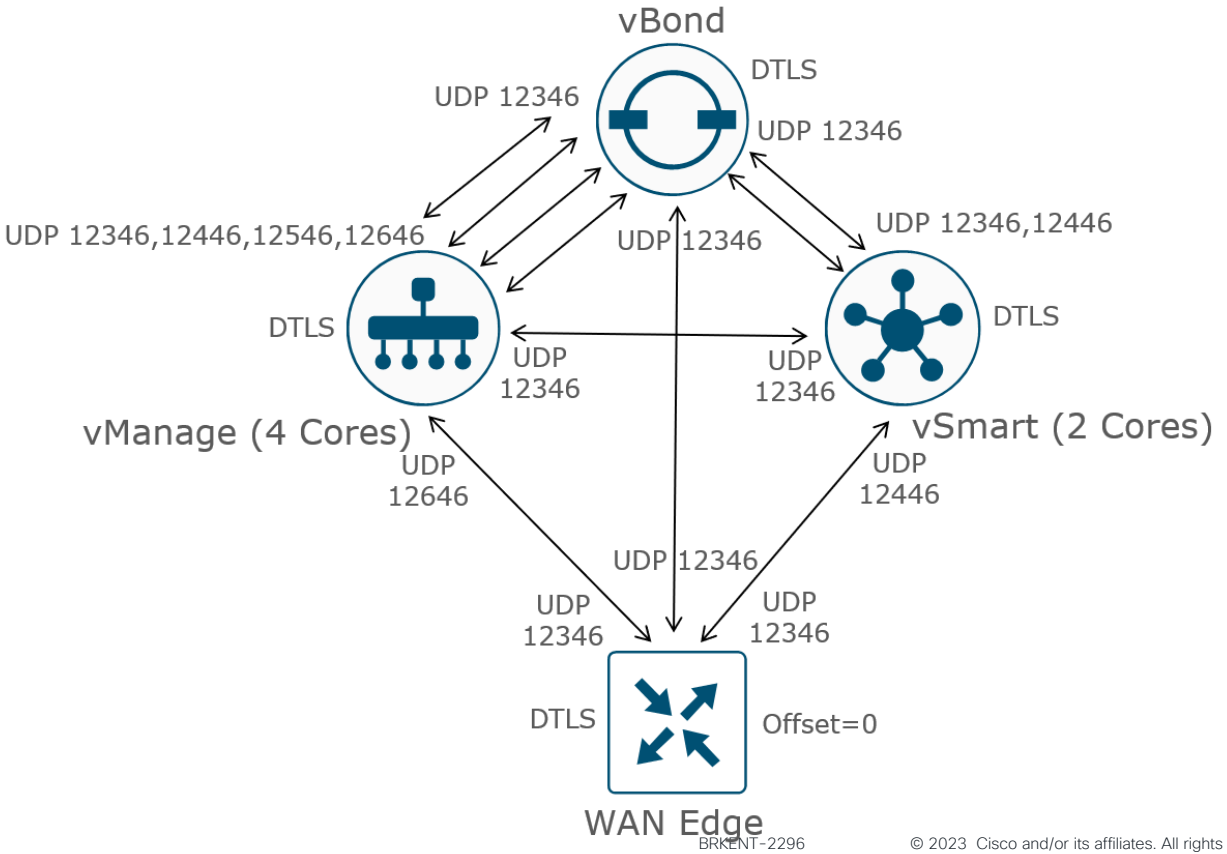
Port Management

Multiple core connections to vBond



Core Number	DTLS (UDP)	TLS (TCP)
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

Example Source and Destination Ports for Control Connections (DTLS)



Port Management – Key Points

- The letter “n” represents any configured port offset, 0-19.
- The communication to the vBond always happens over DTLS. For other SD-WAN devices, if one side is configured for TLS, the communication occurs over TLS.
- All cores for vManage and vSmart may not be deployed, so communication to those ports are not used.
- All cores deployed for both vManage and vSmart establish a permanent control connection with the vBond.
- WAN Edge devices make a transient control connection to vBond. Each WAN Edge device makes permanent control connections to each vSmart over each transport, and a control connection to a vManage over one transport. When a control connection is made to vManage or vSmart, the connection is hashed to one core.

Summary of Ports for SD-WAN Control Plane Communication

For Your Reference

The table below shows one direction for the communication for simplicity, even through traffic is bi-directional

Source Device	Source Port	Destination Device	Destination Port
vManage/vSmart (DTLS)	Core 1 = UDP 12346+n Core 2 = UDP 12446+n Core 3 = UDP 12546+n Core 4 = UDP 12646+n Core 5 = UDP 12746+n Core 6 = UDP 12846+n Core 7 = UDP 12946+n Core 8 = UDP 13046+n	vBond	UDP 12346
vManage/vSmart (DTLS)	UDP 12346+n	vManage/vSmart	UDP 12346+n
WAN Edge (DTLS)	UDP 12346+n UDP 12366+n UDP 12386+n UDP 12406+n UDP 12436+n	vBond	UDP 12346
WAN Edge (DTLS)	UDP 12346+n UDP 12366+n UDP 12386+n UDP 12406+n UDP 12436+n	vManage/vSmart	Core 1 = UDP 12346+n Core 2 = UDP 12446+n Core 3 = UDP 12546+n Core 4 = UDP 12646+n Core 5 = UDP 12746+n Core 6 = UDP 12846+n Core 7 = UDP 12946+n Core 8 = UDP 13046+n

Ports for Controller Management

Additional management protocols may be used on the VPN 512 interface of the controllers. Below is the summary

Service	Protocol/Port	Direction
NETCONF	TCP 830	bidirectional
SSH	TCP 22	incoming
SNMP Query	UDP 161	incoming
Radius	UDP 1812	outgoing
SNMP trap	UDP 162	outgoing
Syslog	UDP 514	outgoing
TACACS	TCP 49	outgoing
HTTPS (vManage)	TCP 443, 8443, 80	incoming

For Your Reference

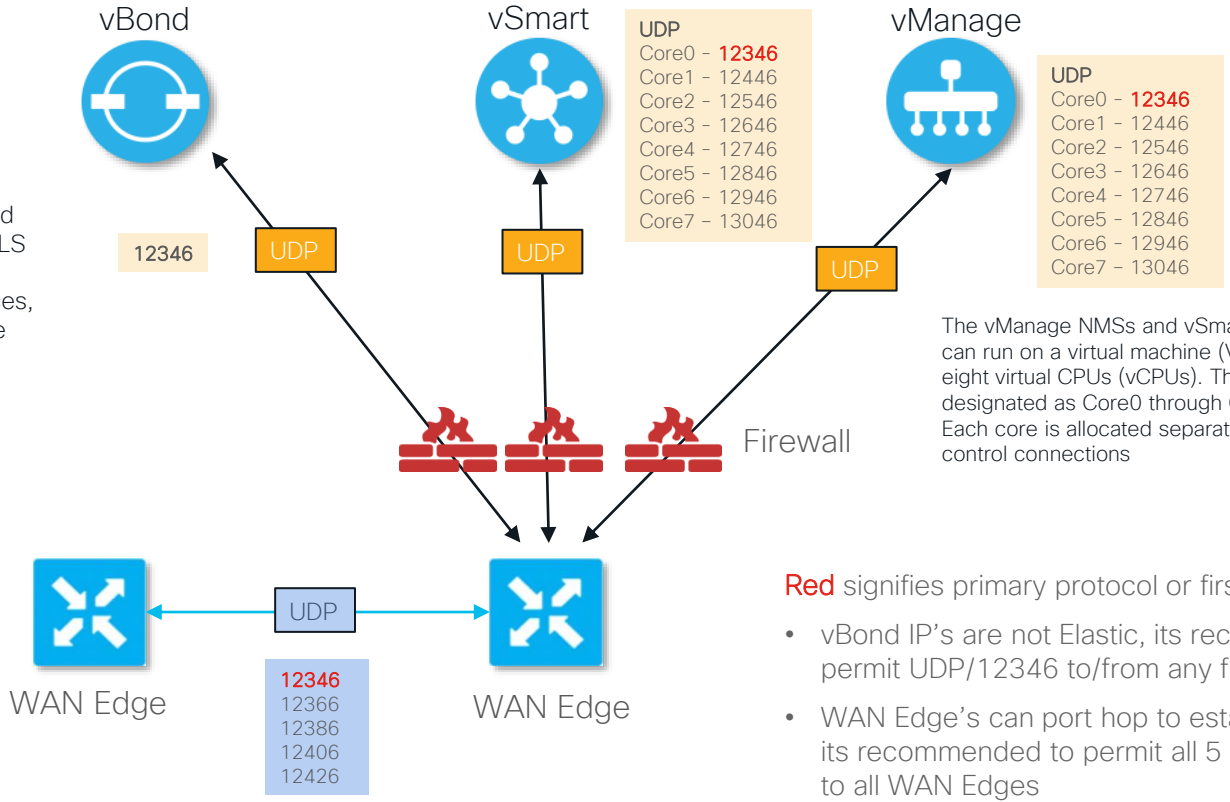
Ports for vManage Clustering

vManage Service	Protocol/Port Number	Direction
Application Server	TCP 80, 443, 7600, 8080, 8443, 57600	bidirectional
Configuration Database	TCP 2424, 2434	bidirectional
Coordination Server	TCP 2181, 3888	bidirectional
Message Bus	TCP 9092	bidirectional
Statistics Database	TCP 9200, 9300	bidirectional
Tracking of device configurations (NCS and NETCONF)	TCP 830	bidirectional

Firewalls Ports – DTLS

For Your Reference

vBond orchestrators do not support multiple cores. vBond orchestrators always use DTLS tunnels to establish control connections with other devices, so they always use UDP. The UDP port is 12346



The vManage NMSs and vSmart controllers can run on a virtual machine (VM) with up to eight virtual CPUs (vCPUs). The vCPUs are designated as Core0 through Core7.
Each core is allocated separate base ports for control connections

Default settings:
- No Port Offset
- DTLS

Red signifies primary protocol or first port used

- vBond IP's are not Elastic, its recommended to permit UDP/12346 to/from any from the WAN Edge
- WAN Edge's can port hop to establish a connection, its recommended to permit all 5 UDP ports inbound to all WAN Edges

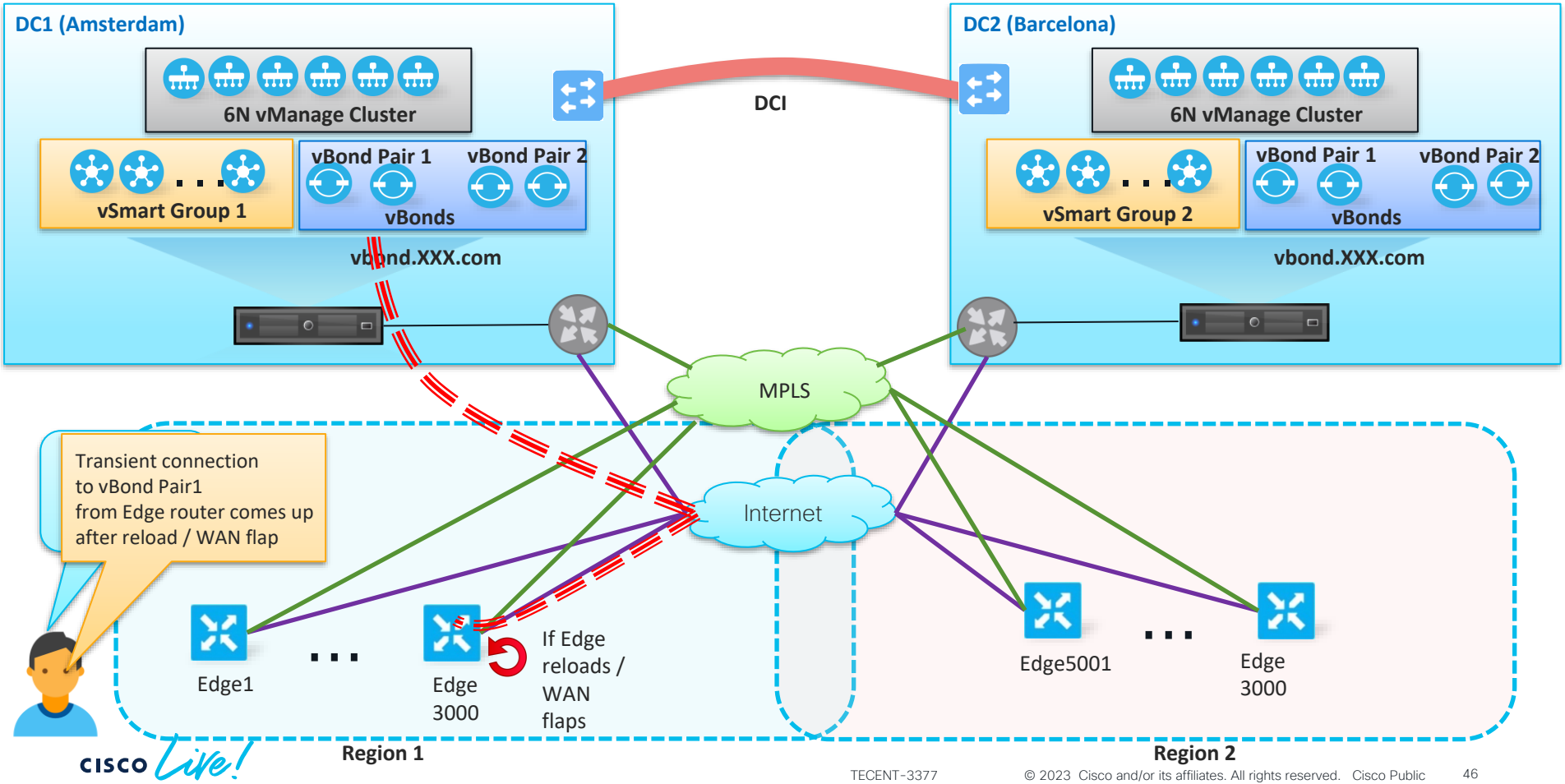
Recommended Computing resources

Please refer to the below link for recommended computing resources for Cisco SD-WAN Controllers – release 20.10.x

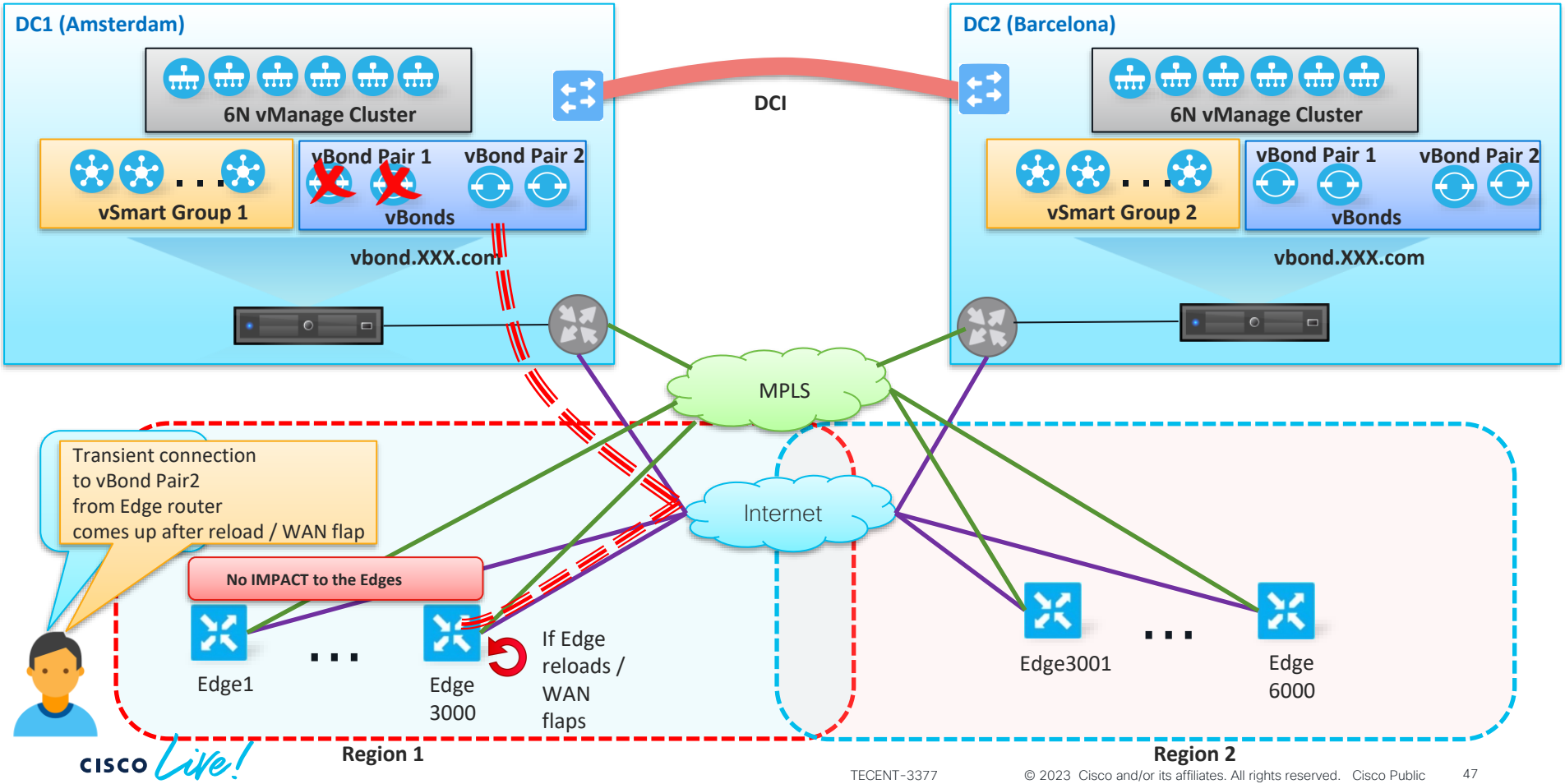
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/compatibility-and-server-recommendations/ch-server-recs-20-10-combined.html

On-prem Controllers- Failover Scenario

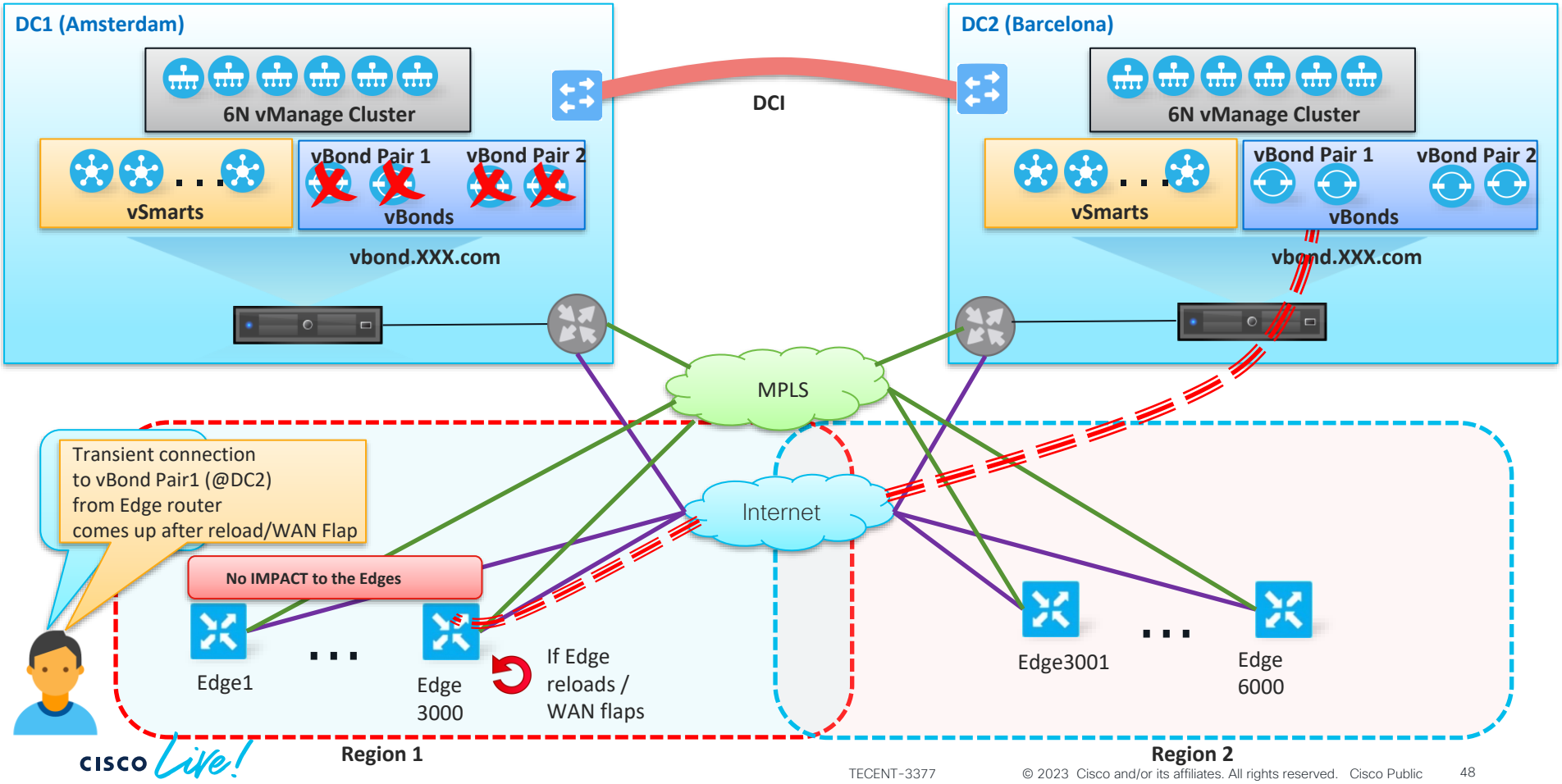
Case 1



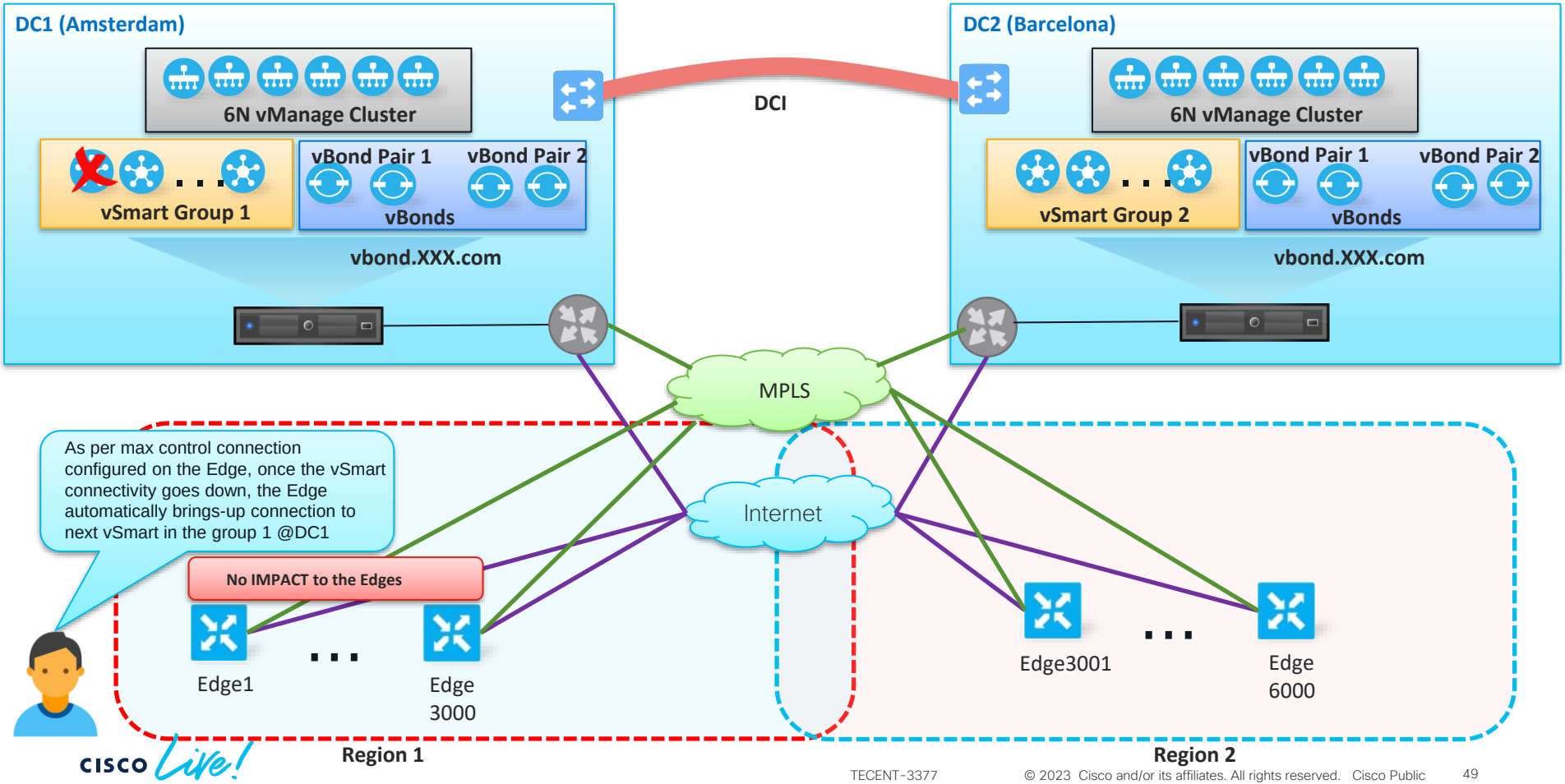
Case 2



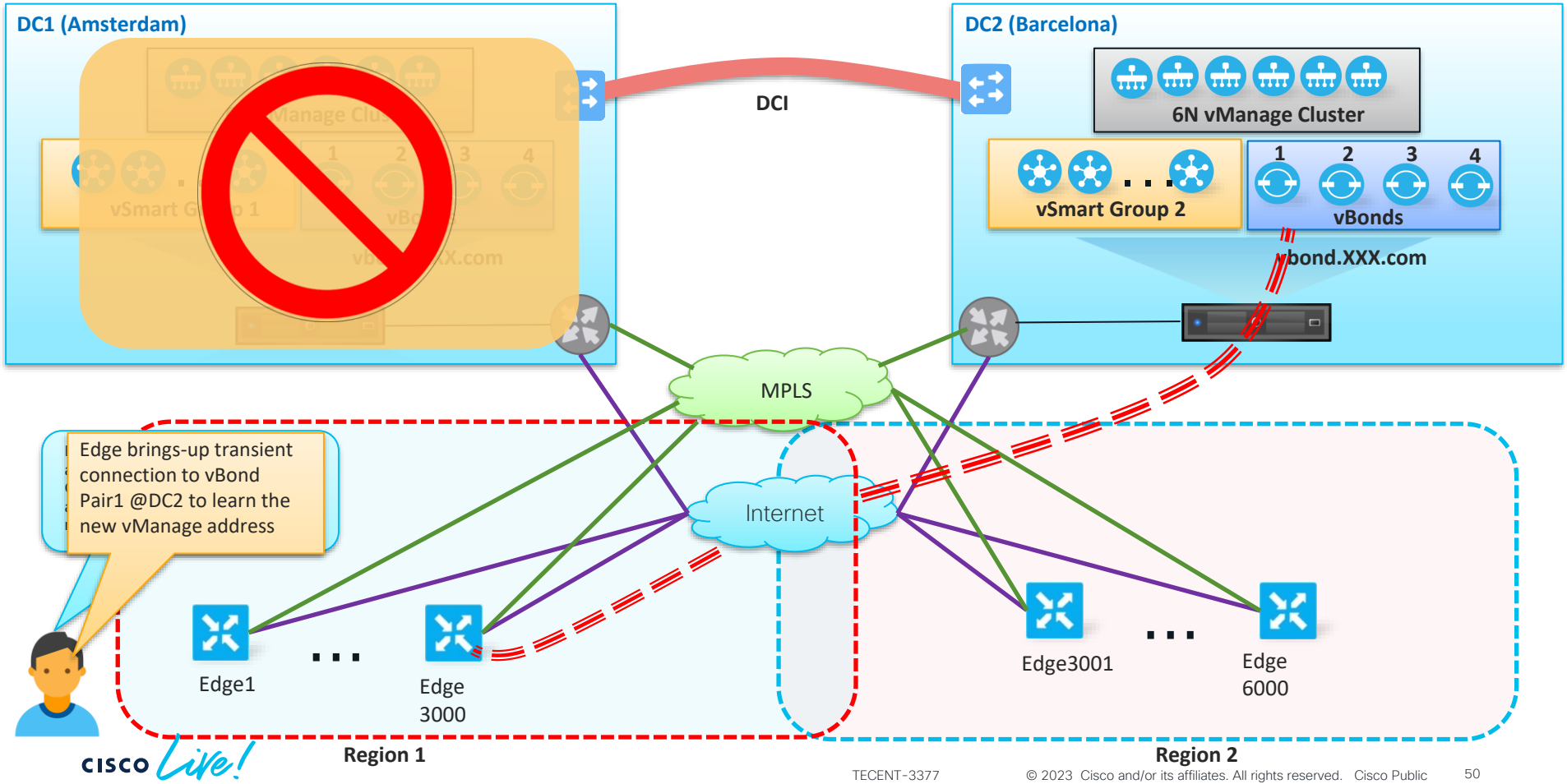
Case 3



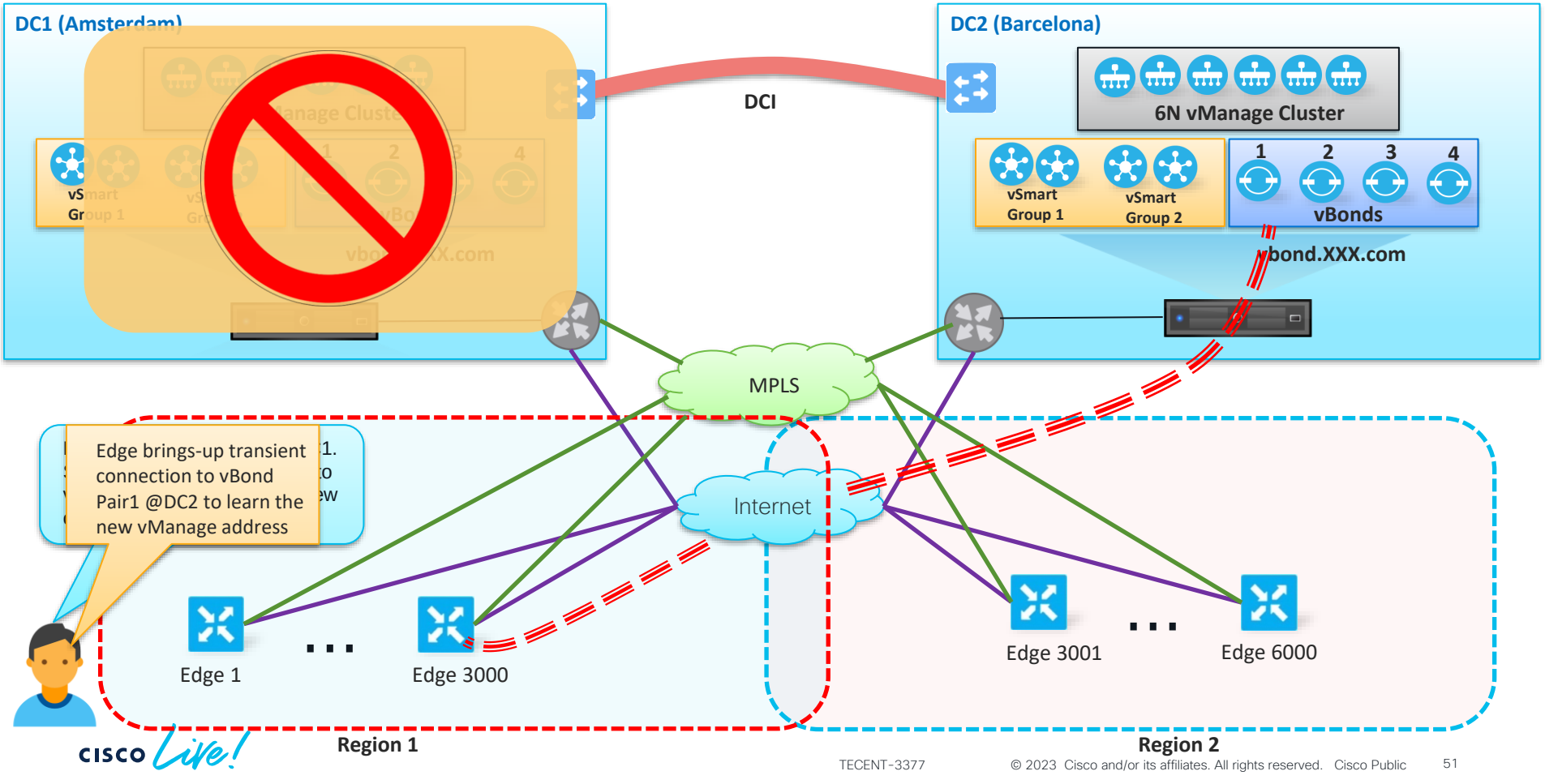
Case 4



Case 5



Case 6



Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from 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 Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN