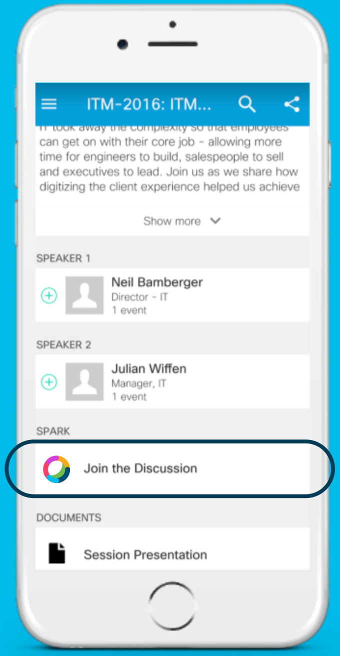
Cisco live!

January 28 - February 1, 2019 · Barcelona

cisco

IMAGINE

INTUITIVE



cs.co/ciscolivebot#BRKCRS-2117

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark)
to chat with the speaker after the session

How

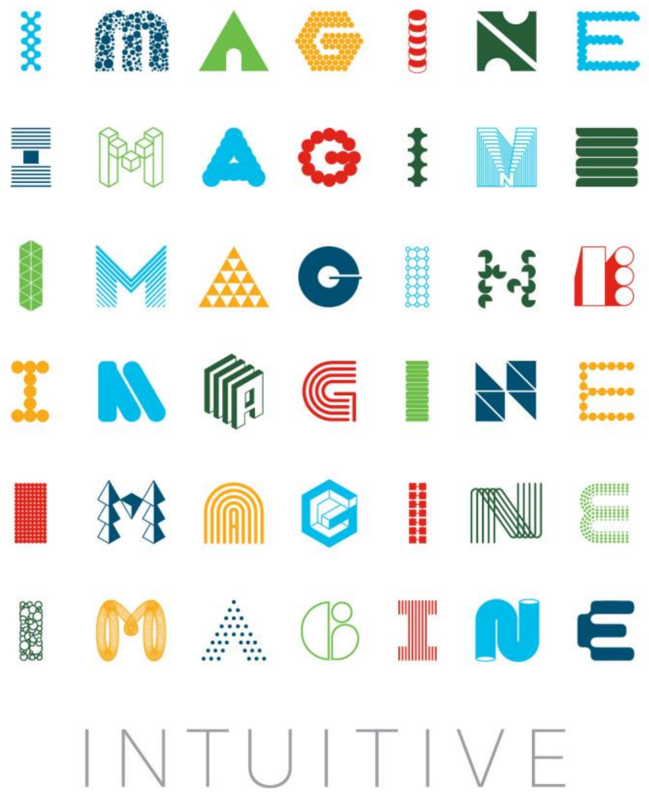
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

BRKCRS-2117

Cisco SDWAN Design & Deployment

Steven Wood - Principal Engineer – Enterprise Networks

David Prall – Principal Systems Engineer – Enterprise Networks



Agenda

- Introduction
- Network Architecture
- Controller Design
- Routing & Site Design
- Policy Design
- Resiliency Considerations
- Summary

About the jargon…

vEdge – vEdge Router

cEdge – ISR/ASR Router

i.e. an SDWAN router

vSmart – controller

vBond – orchestrator

vManage – Management Application

Cisco SD-WAN Solution Overview

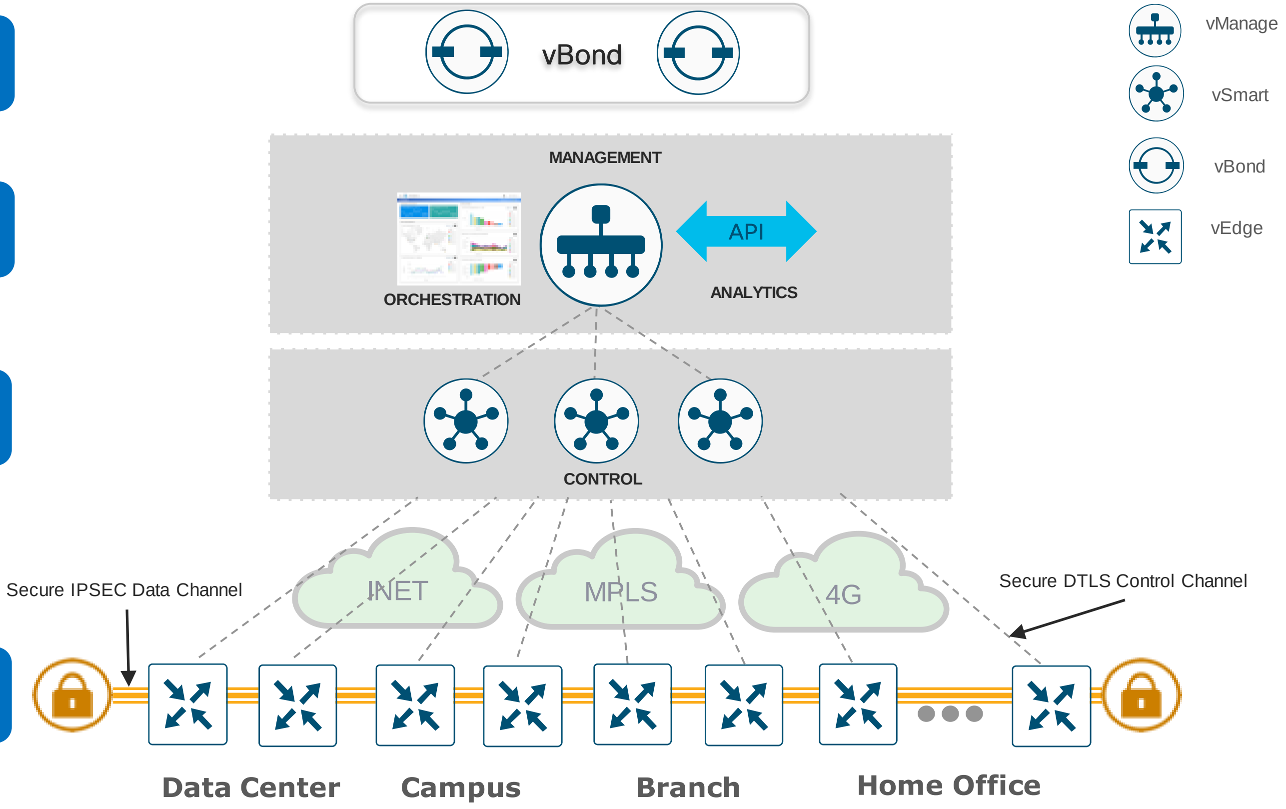
Applying SDN Principles To The Wide Area Network

Orchestration Plane

Management Plane
(Multi-tenant or Dedicated)

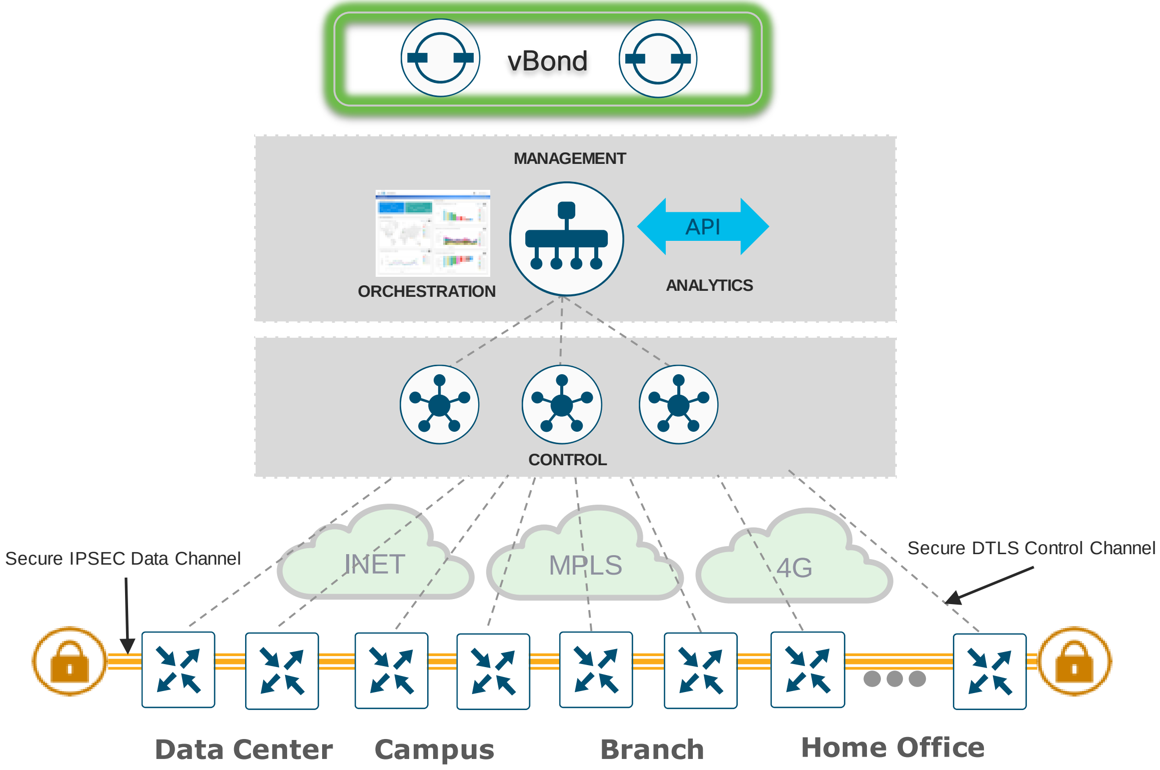
Control Plane
(Containers or VMs)

Data Plane
(Physical or Virtual)



Orchestration Plane

vBond Orchestrator

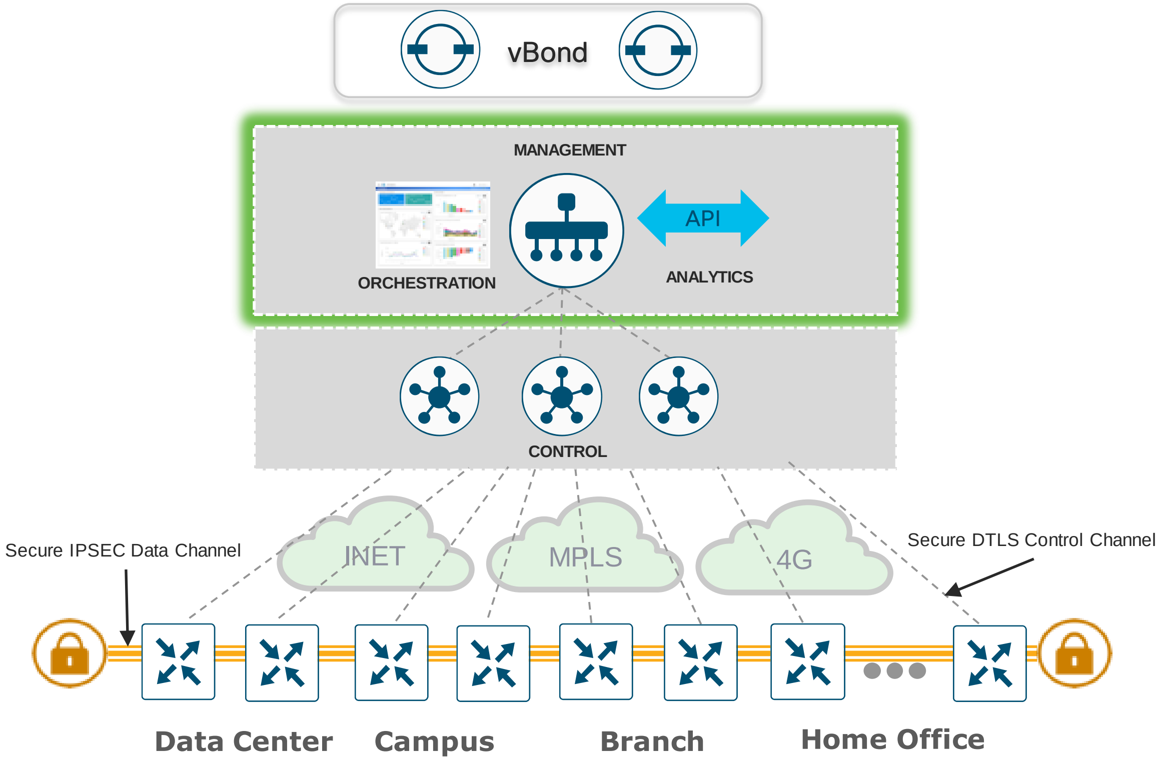


Main Characteristics

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

Management Plane

vManage

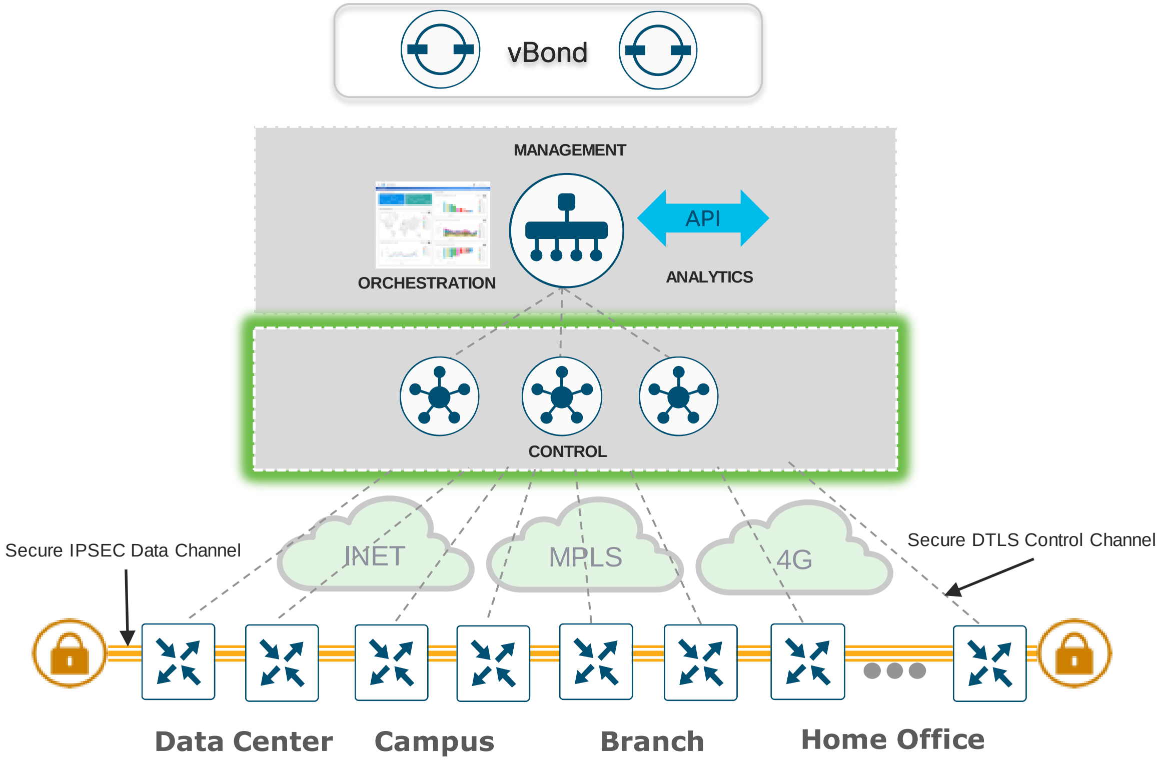


Main Characteristics

- 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

Control Plane

vSmart Controller

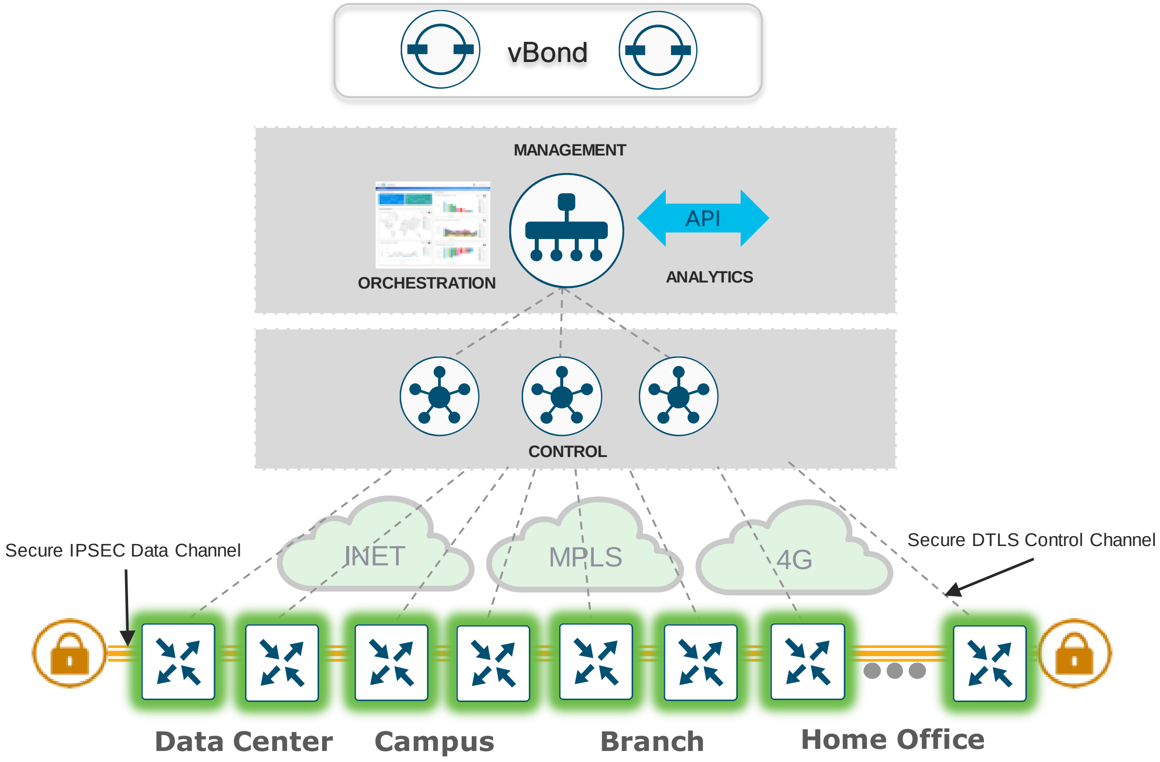


Main Characteristics

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

Data Plane

vEdge Router

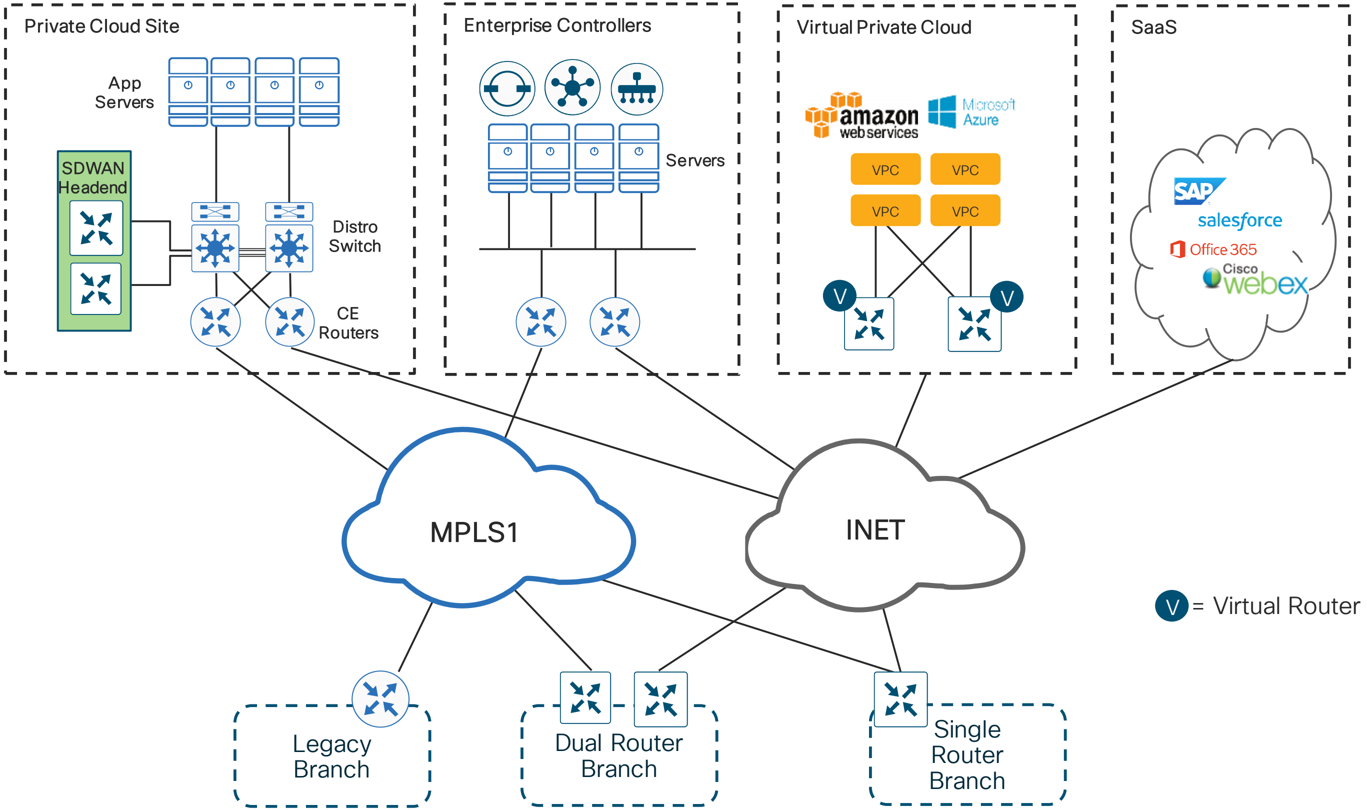


Main Characteristics

- WAN edge router
- Provides secure data plane with remote vEdge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP and VRRP
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mb, 1Gb, 10Gb, 20Gb+)

Network Architecture

Typical SDWAN Deployment Architecture

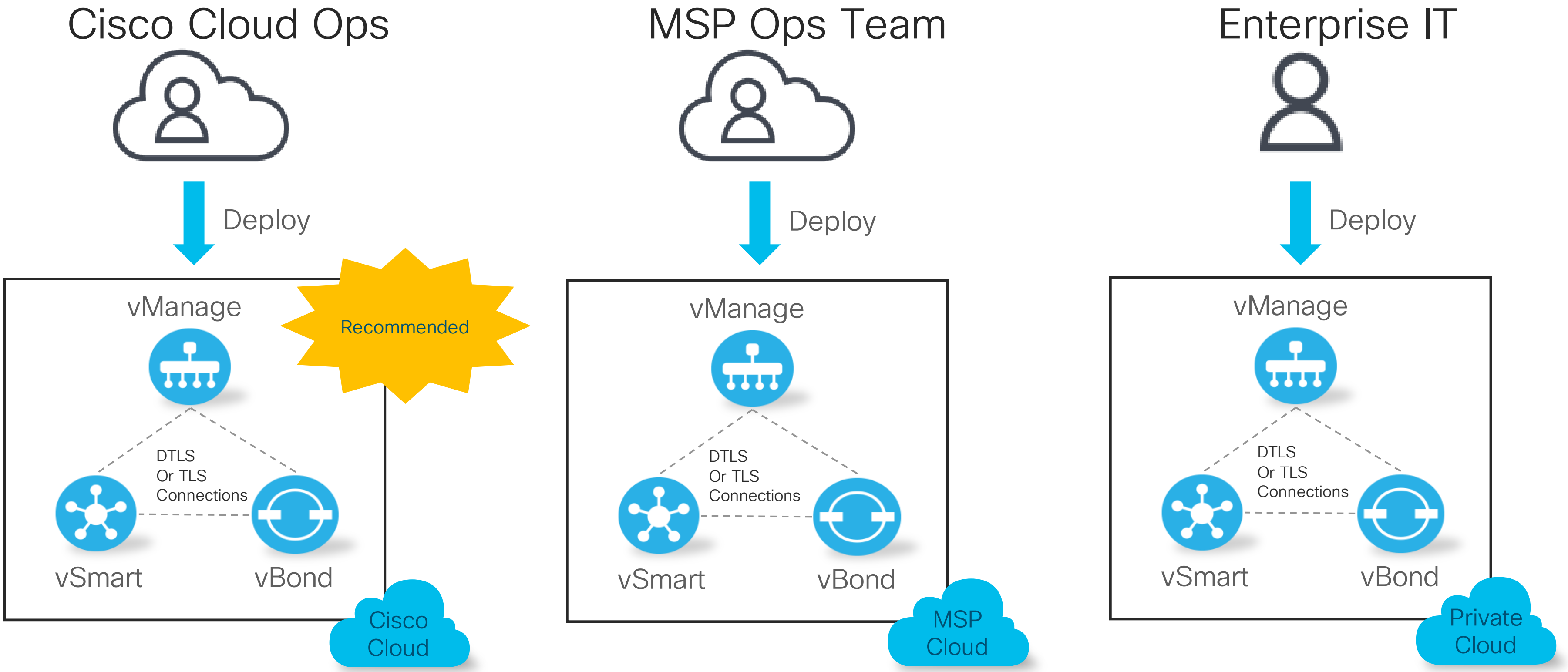


Controller Deployment

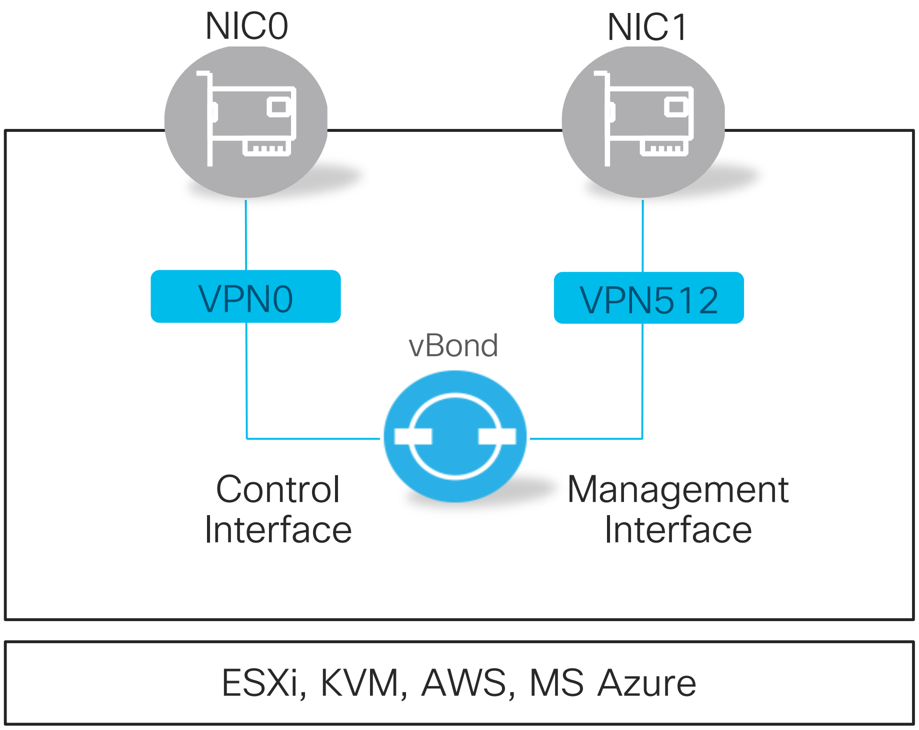
Cisco live!

Cloud-Delivered Control

Flexible Deployment Options

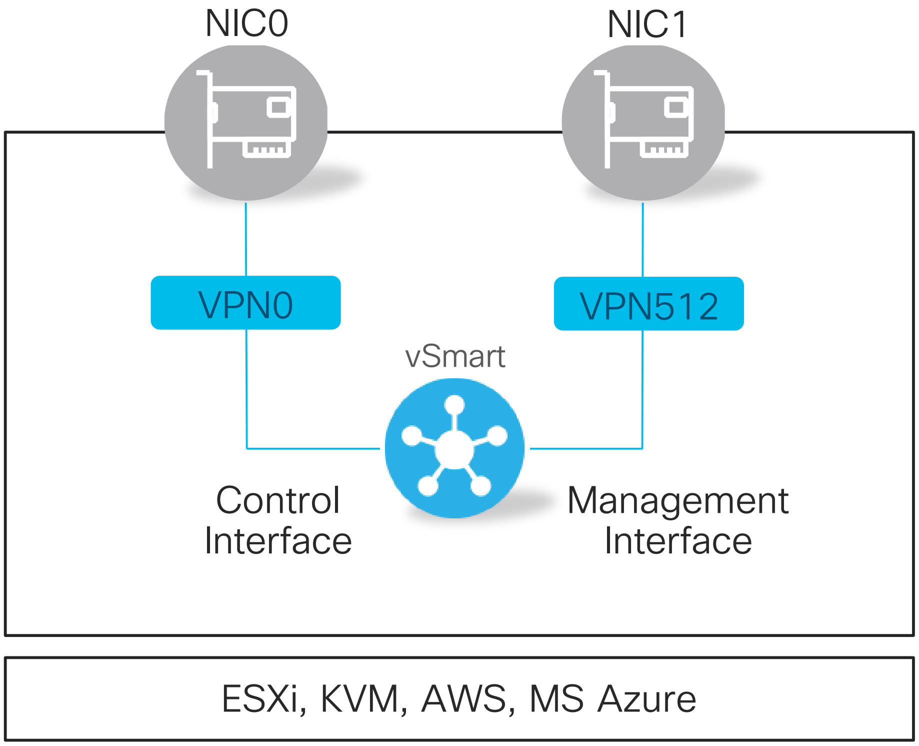


Controller Deployment



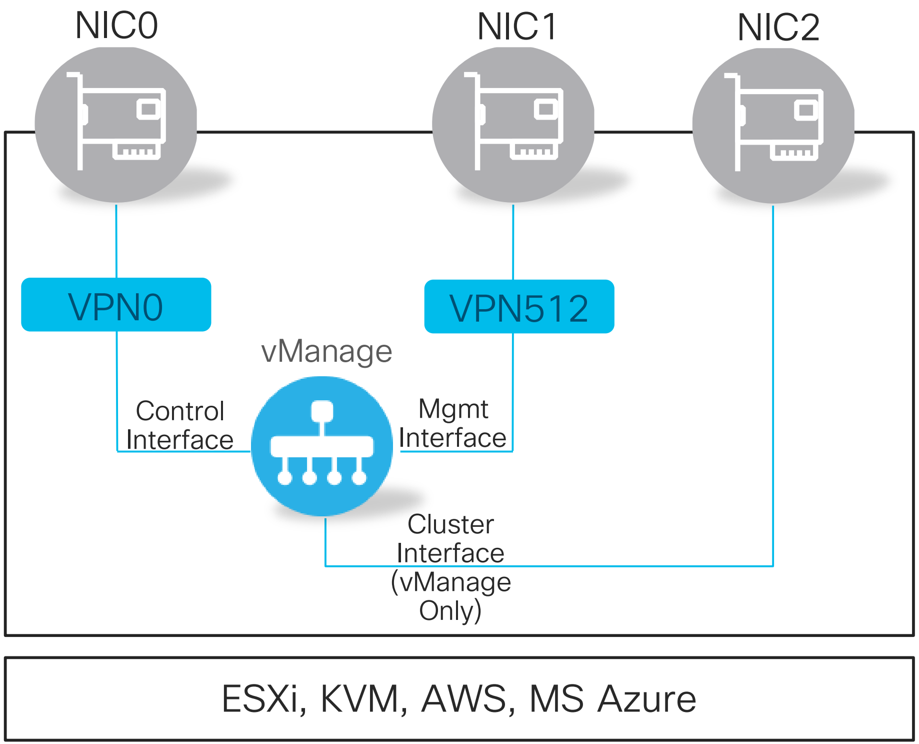
- Cloud or on premise deployment
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP (local)

Controller Deployment



- Cloud or on premise deployment
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP

Typical Controller Deployment



- Cloud or on premise deployment
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Internal Cluster I/F for vManage instance clustering
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP (local)

Controller Communication Principles

- The vBond is a special control element because it acts as a STUN server for the network to allow vEdges to sit behind NAT devices
- To work properly, the other control elements (vManage, vSmart) need to communicate to vBond through NAT as well.
- vSmarts and vManages can communicate with each other either through NAT or un-NATed connections
- NAT must be 1:1 with no PAT
- The choice of deployment model is dependent on security posture vs network complexity tradeoff.

Significance of Interface (TLOC) Color

- Color is an abstraction used to identify individual WAN transport as PUBLIC or PRIVATE
- Colors are KEYWORDS not free form LABELS
- Used for automation and policy writing
- "Color" dictates the use of private-ip vs public-ip (dest) for Tunnel Establishment when there is NAT present
  - Example:
    - If two ends have a private color: private IP address/port used for DTLS/TLS or IPSec
    - If endpoint has public color: Public IP is used for DTLS/TLS or IPSec

Private Colors

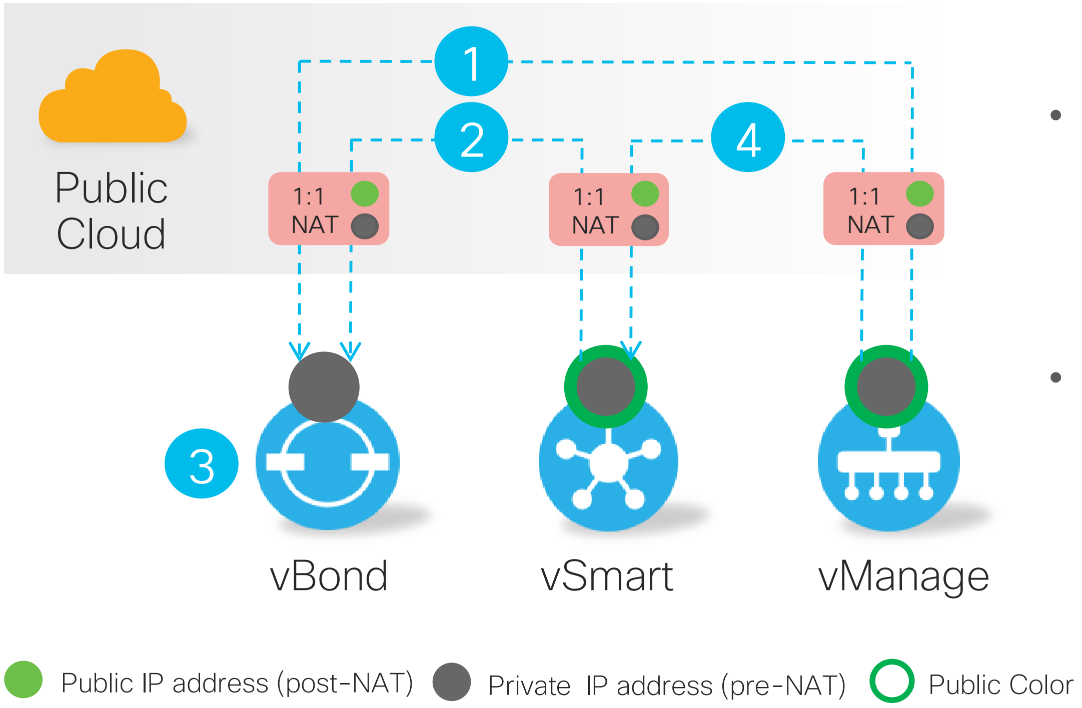
Metro-ethernet
mpls
private1
private2
private3
private4
private5
private6

Public Colors

3g
lte
biz-internet
public-internet
blue
green
red
gold
silver
bronze

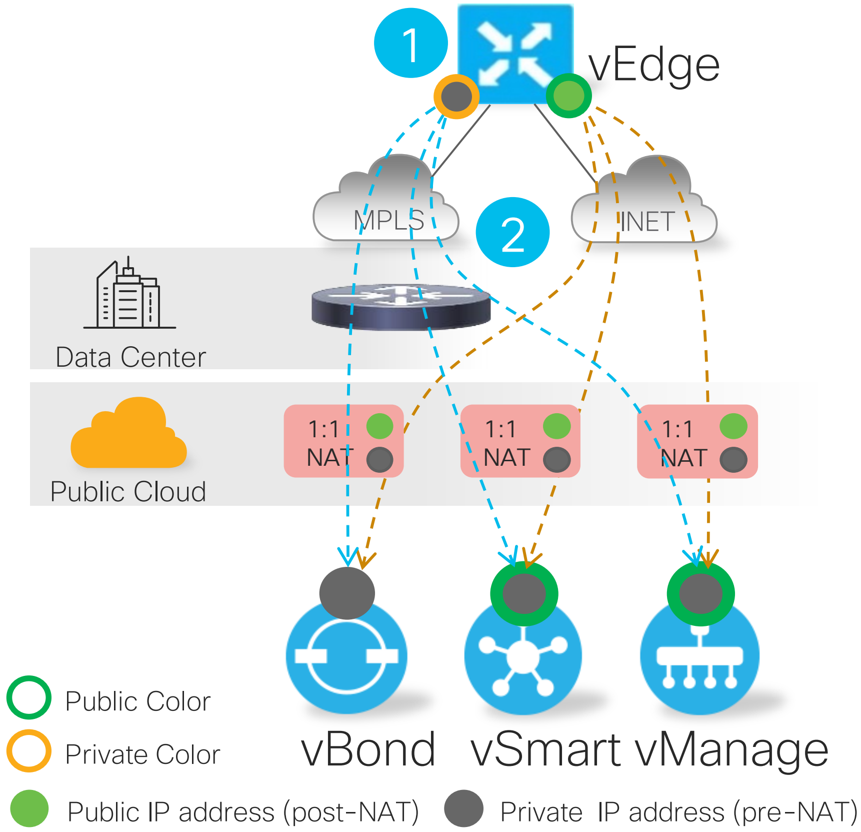
Controllers Public Cloud Deployment

Controllers Communication



- 1 2 vSmart and vManage point to the vBond IP address
  - NATed public IP address
- 3 vBond learns interface private and NATed public IP address of vSmart and vManage
  - Private is pre-NAT, public is post-NAT
- 4 vSmart and vManage use NATed public IP addresses for communication
  - vSmart and vManage use public color (default)
  - Public color to public color uses public IP address

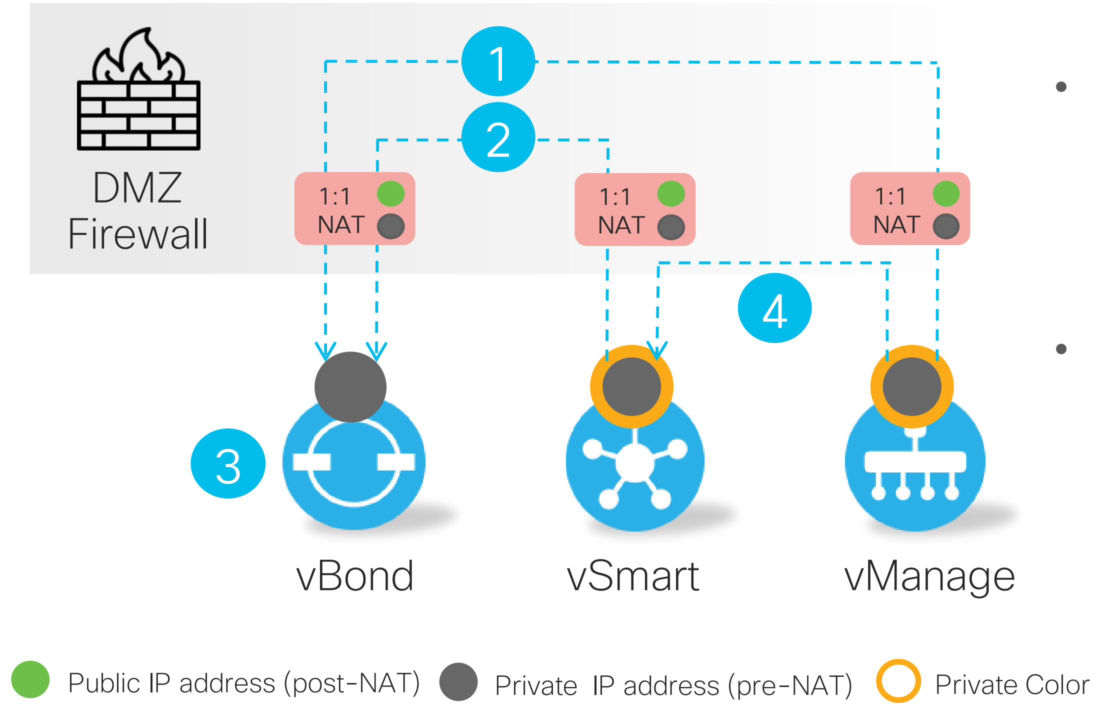
Controllers Public Cloud Deployment



- 1 vEdge points to the vBond NATed public IP
  - vBond NATed public IP address is reachable through MPLS (direct or via Data Center) and Internet transports
- 2 vEdge communicates with vSmart and vManage using NATed public IP address
  - Private color to public color uses public IP address, public color to public color uses public IP address
  - vSmart and vManage NATed public IP addresses are reachable through MPLS (direct or via Data Center) and Internet transports

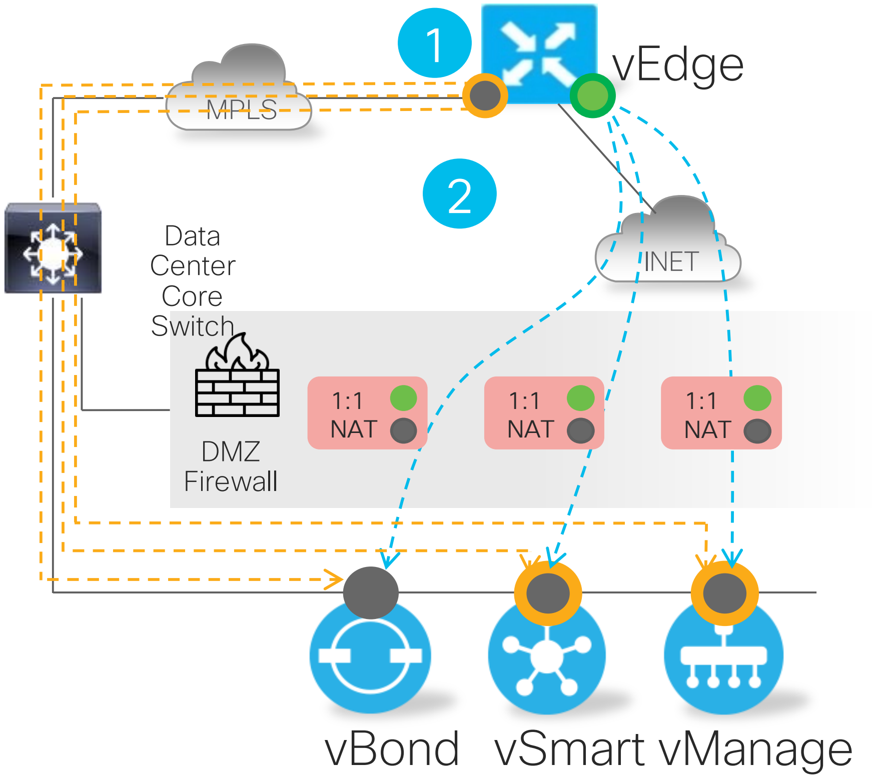
On-Prem Controllers Hybrid Deployment

Controllers Communication



- 1 2 vSmart and vManage point to the vBond IP address
  - NATed public IP address
- 3 vBond learns interface private and NATed public IP address of vSmart and vManage
  - Private is pre-NAT, public is post-NAT
- 4 vSmart and vManage use interface private IP addresses for communication
  - vSmart and vManage use private color (non-default)
  - Private color to private color uses private IP address

On-Prem Controllers Hybrid Deployment



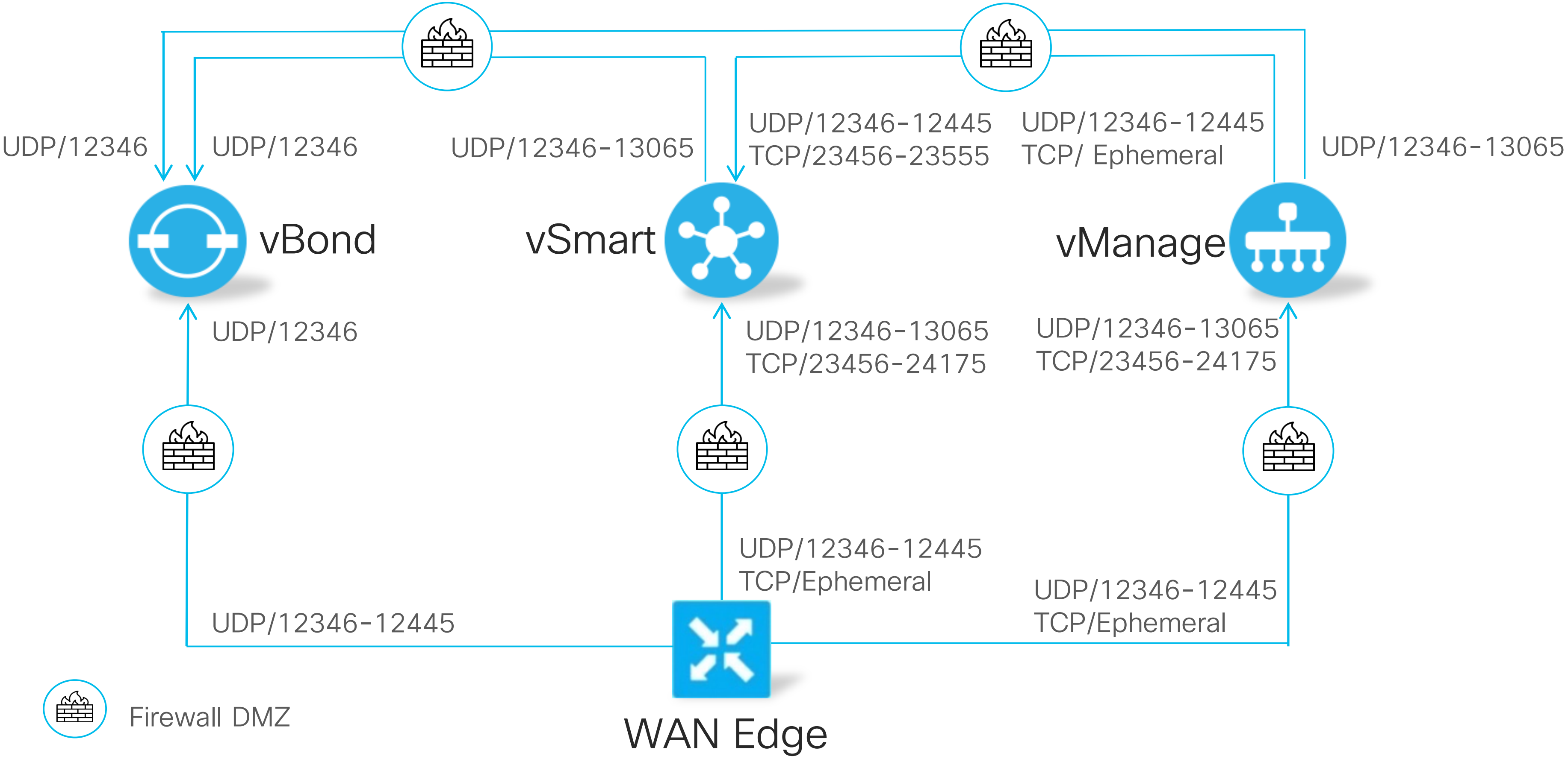
- 1 vEdge points to the vBond FQDN that resolves to both public and private IP addresses

	Private IP	Public IP
MPLS		
Internet		

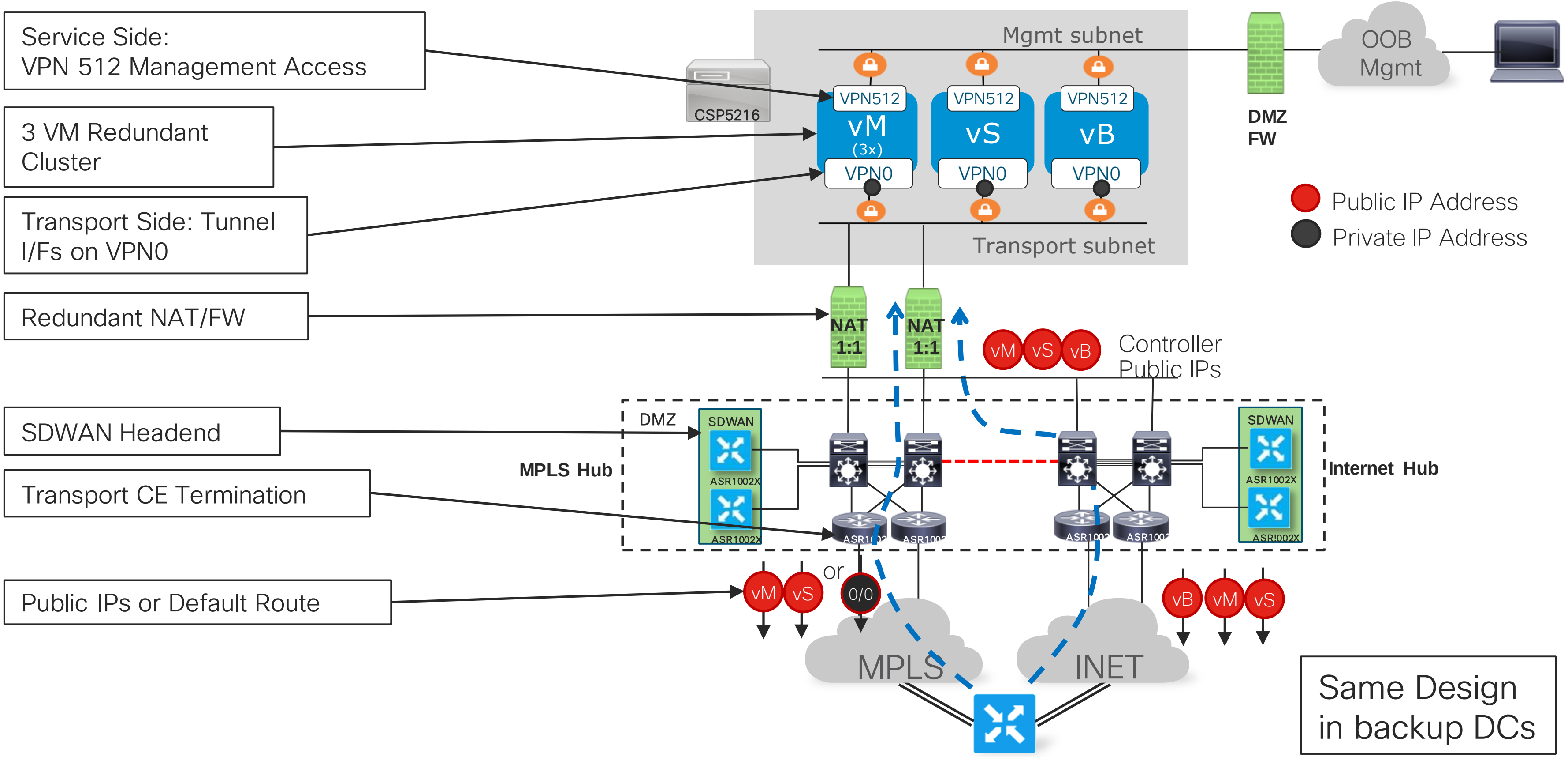
- 2 vEdge communicates with vSmart and vManage NATed public IP addresses over Internet and interface private IP addresses over MPLS
  - Private color to private color uses private IP address, private color to public color uses public IP address

Public IP address (post-NAT) Private IP address (pre-NAT) Public Color Private Color

Firewall Rules for On-Prem Controllers

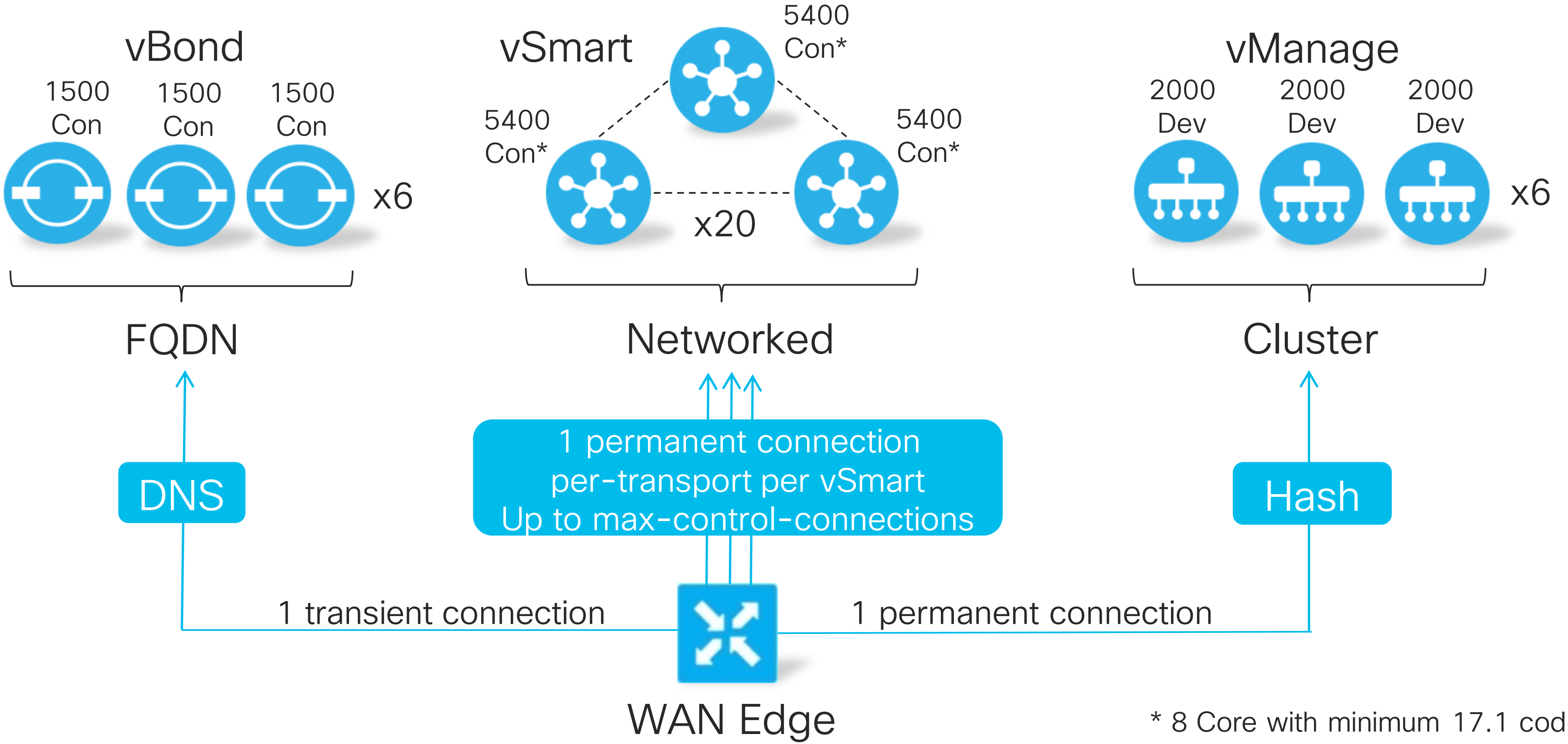


Example Controller System Deployment



Same Design in backup DCs

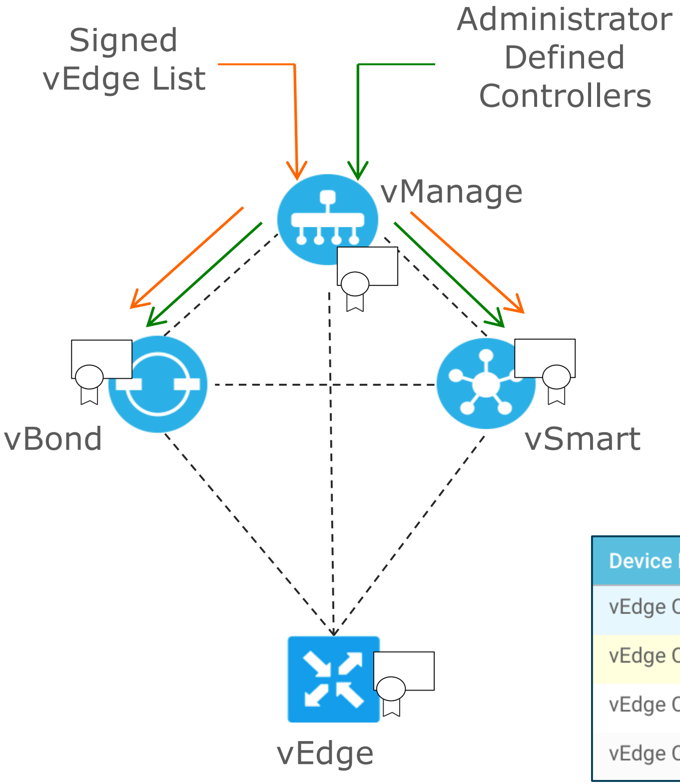
Controllers Connectivity and Scale



* 8 Core with minimum 17.1 code

Onboarding

Certificate-Based Trust

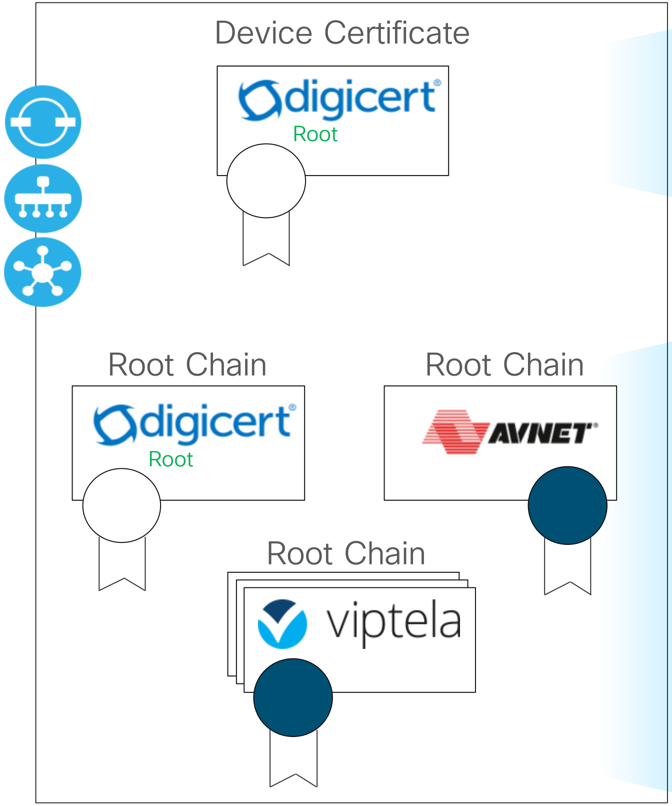


- Bi-directional certificate-based trust between all elements
  - Public or Enterprise PKI
- White-list of valid vEdges and controllers
  - Certificate serial number as unique identification

Controller Type ↑	Hostname	System IP	Certificate Serial
vBond	vBond1	1.1.1.2	46FD1AC2B1465B8E2EB5D7F7E10E1FEC
vBond	vBond2	1.1.1.11	64DAABDD54F3918EE30EA1CA13A97F06
vManage	vManage	1.1.1.1	074B7AE1DEA4F9678FA42C5A766845EF
vSmart	vSmart1	1.1.1.3	10CC1C0B71C3775885BF8B0F3E79ECC7
vSmart	vSmart2	1.1.1.10	0E4782A4EBCFA2DA47EB0DD9AE097C9A

Device Model	Serial No./Token	Hostname ↓	IP Address	Validate
vEdge Cloud	19EB7510F570D6BD235C10E576230...	RemoteSite2	1.1.1.8	Invalid | Staging | Valid
vEdge Cloud	585A0084DEA8396DD77BB66F22BAE...	RemoteSite1	1.1.1.4	Invalid | Staging | Valid
vEdge Cloud	368EDA9249E64F2C5ADF6BC430F7E...	RegionalHub	1.1.1.7	Invalid | Staging | Valid
vEdge Cloud	0334D73E5EC036F87ABE132FE1CE4...	DataCenter	1.1.1.5	Invalid | Staging | Valid

Controllers Identity and Trust



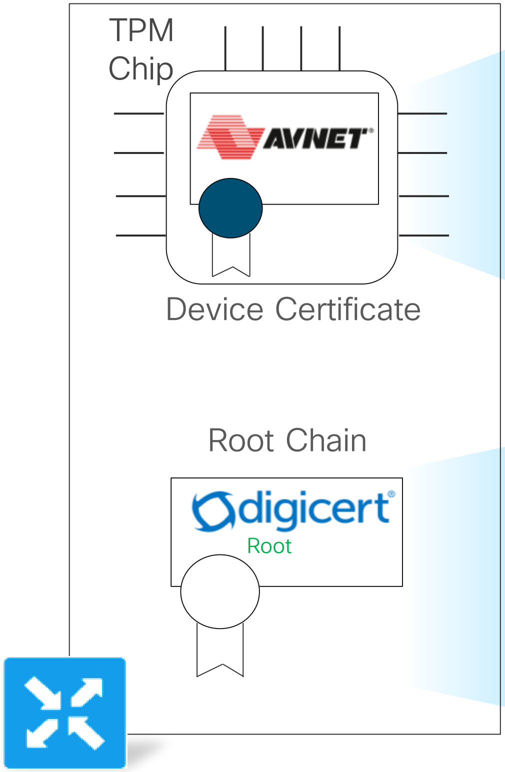
Identity

- Controller identity is provided by the digicert signed certificate (1-2 yr lifetime)
  - Alternatively can use Enterprise CA. Requires Enterprise Root cert on all other controllers and vEdge routers

Trust

- Avnet Root chain to authenticate vEdge routers
  - Embedded into Viptela software
- Viptela Root chain to authenticate vEdge Cloud routers
  - Provided by vManage. Multiple if cluster.
- digicert Root chain to authenticate other controllers
  - Embedded into Viptela software
  - Alternatively can use Enterprise Root chain

vEdge Router Identity and Trust



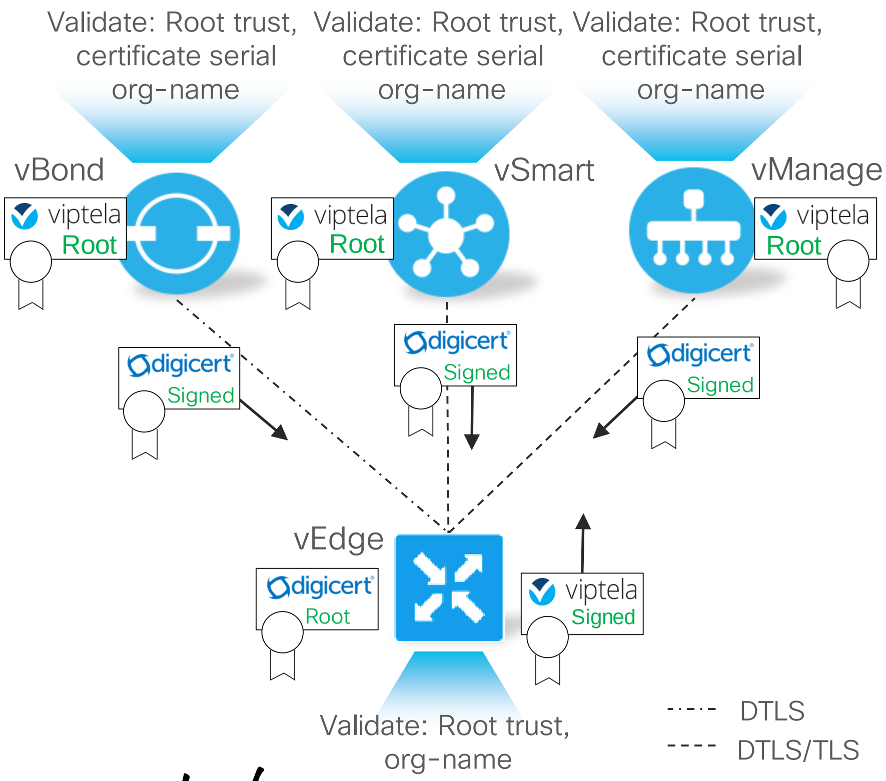
Identity

- Each physical vEdge router is uniquely identified by the chassis ID and certificate serial number
- Certificate is stored in on-board Tamper Proof Module (TPM)
  - Installed during manufacturing (25 year lifetime)
- Certificate is signed by Avnet root CA

Trust

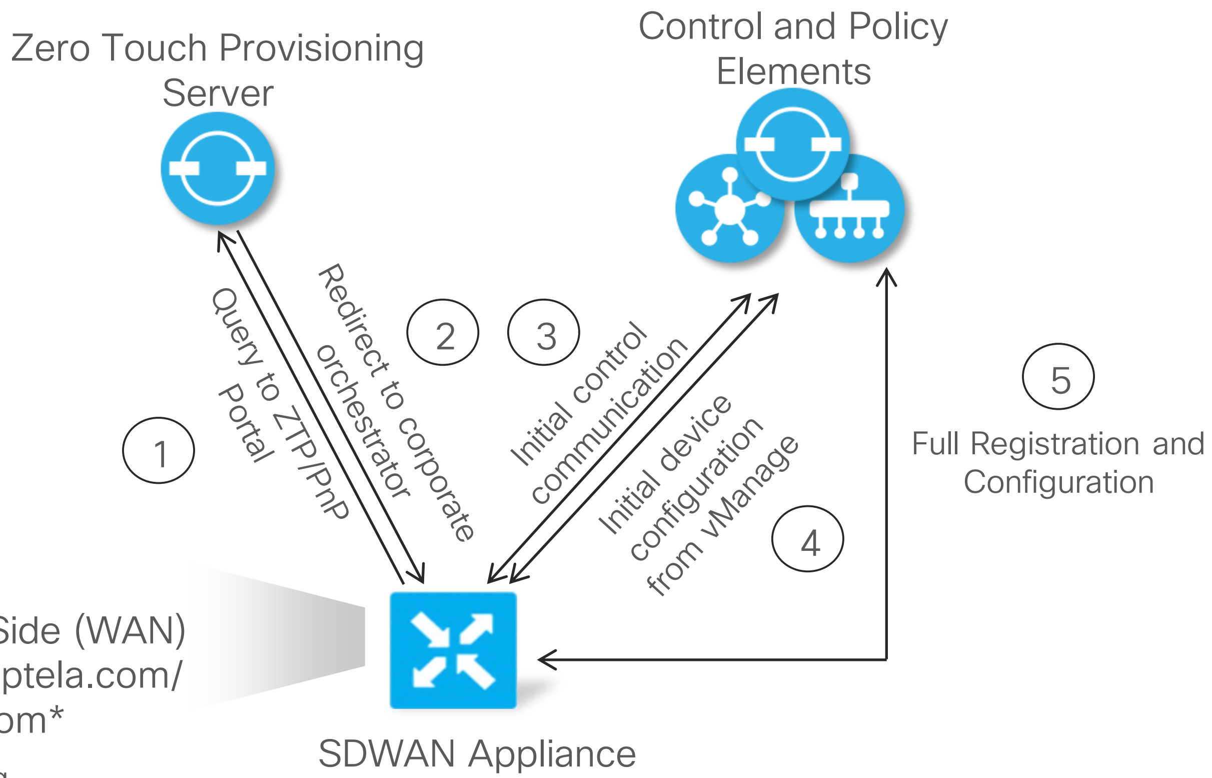
- digicert root chain of trust is used to validate Control Plane elements
  - Embedded into Viptela software
- Alternatively, Enterprise root chain of trust can be used to validate Control Plane elements
  - Can be automatically installed during ZTP

vEdge Cloud ⇔ vBond, vSmart, vManage



- vManage root cert is distributed to controllers
- vManage issues certificate identity
- vBond, vSmart and vManage validate:
  - Trust for vEdge certificate root CA
  - Certificate serial numbers against authorized white-list (from vManage)
  - Organization name (received certificate OU) against locally configured one
- vEdge validates:
  - Trust for vBond, vSmart and vManage certificate root CA
  - Organization name (received certificate OU) against locally configured one
- Persistent DTLS/TLS connection comes up between vEdge and vSmart/vManage
  - vEdge is a client

Zero Touch Provisioning – SDWAN Router

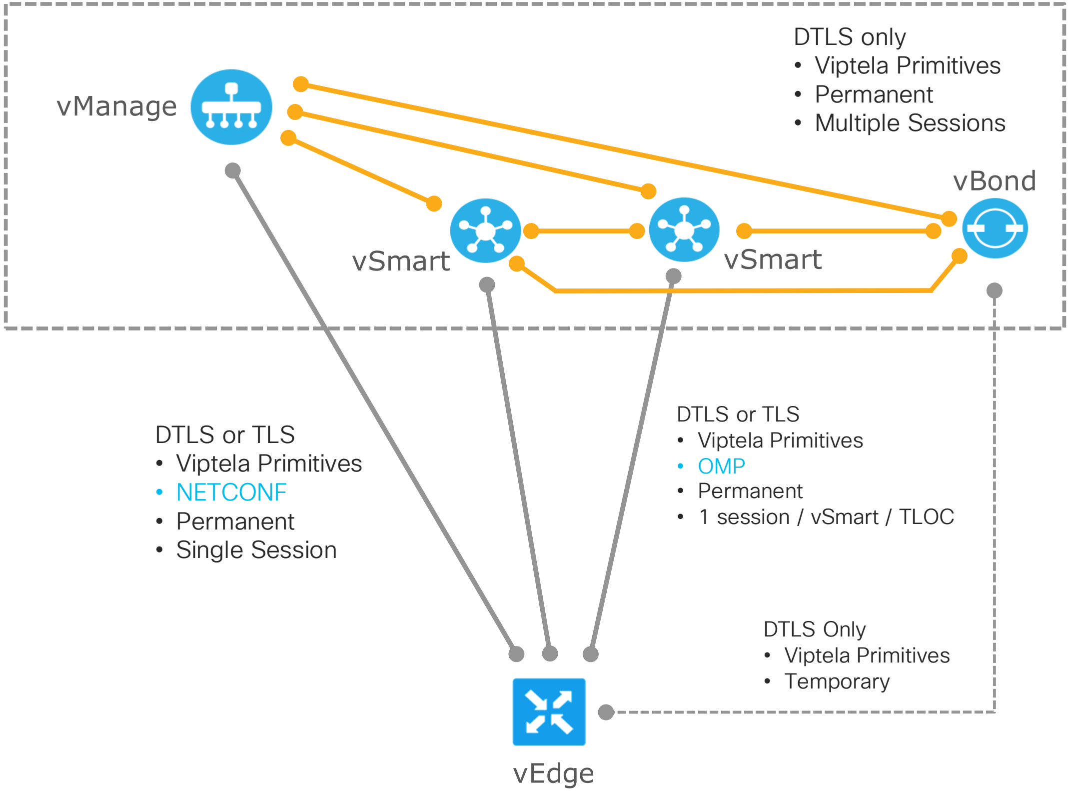


Assumption:
- DHCP on Transport Side (WAN)
- DNS to resolve ztp.viptela.com/ devicehelper.cisco.com*

* Factory default config

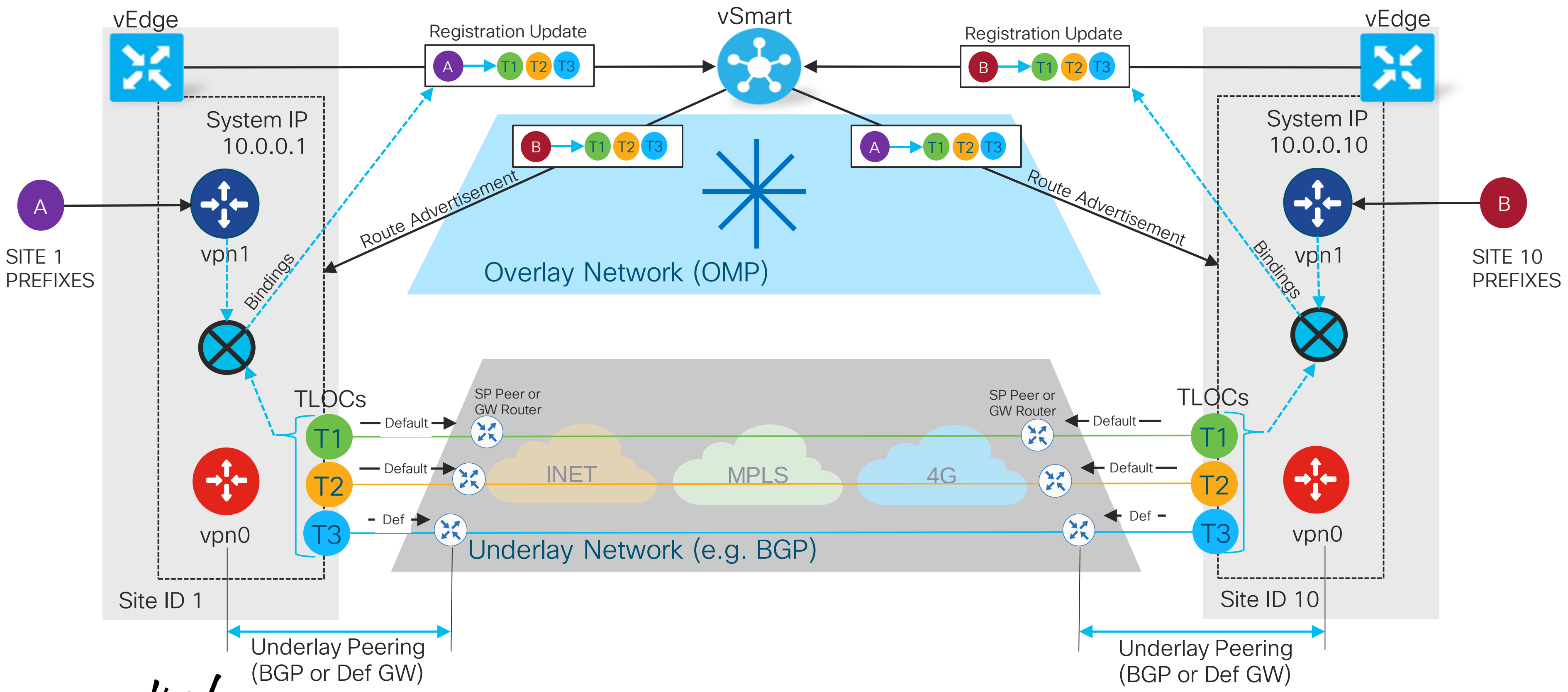
Control Plane Sessions

- Secure Channel to SD-WAN Controllers.
- Operates over DTLS/TLS authenticated and secured tunnels
- OMP - between vEdge routers and vSmart controllers and between the vSmart controllers
- NETCONF – Provisioning from vManage. Access via admin credentials over authenticated tunnel.
- Internal control connections do not carry HTTP/HTTPS primitives
- No need for reverse proxy protection. SDN Controllers are not webservers
- vManage is the exception, but HTTP access can be restricted to private access under RBAC



Routing Design

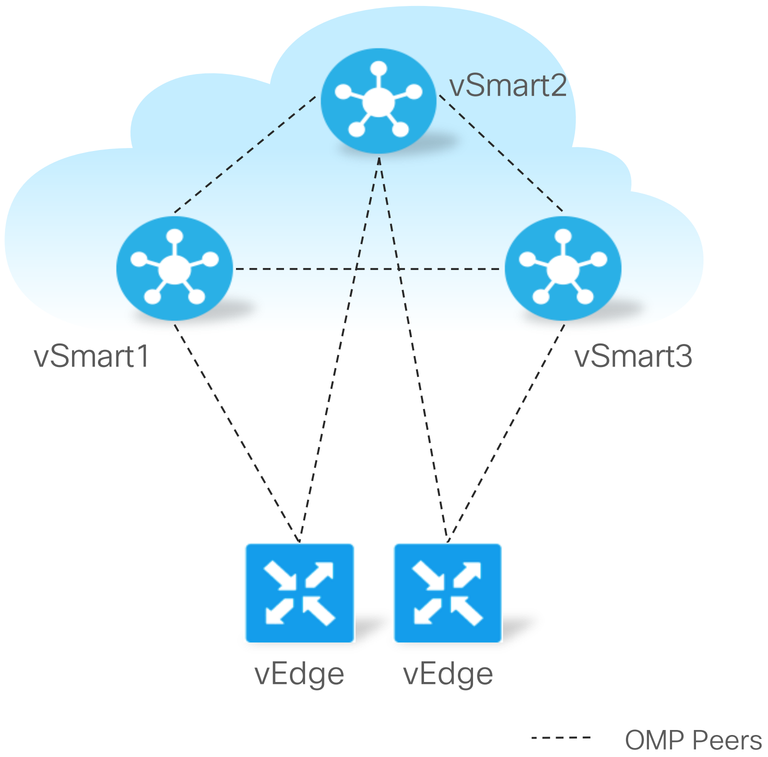
Understanding SDWAN Routing



SDWAN Fabric Terminology

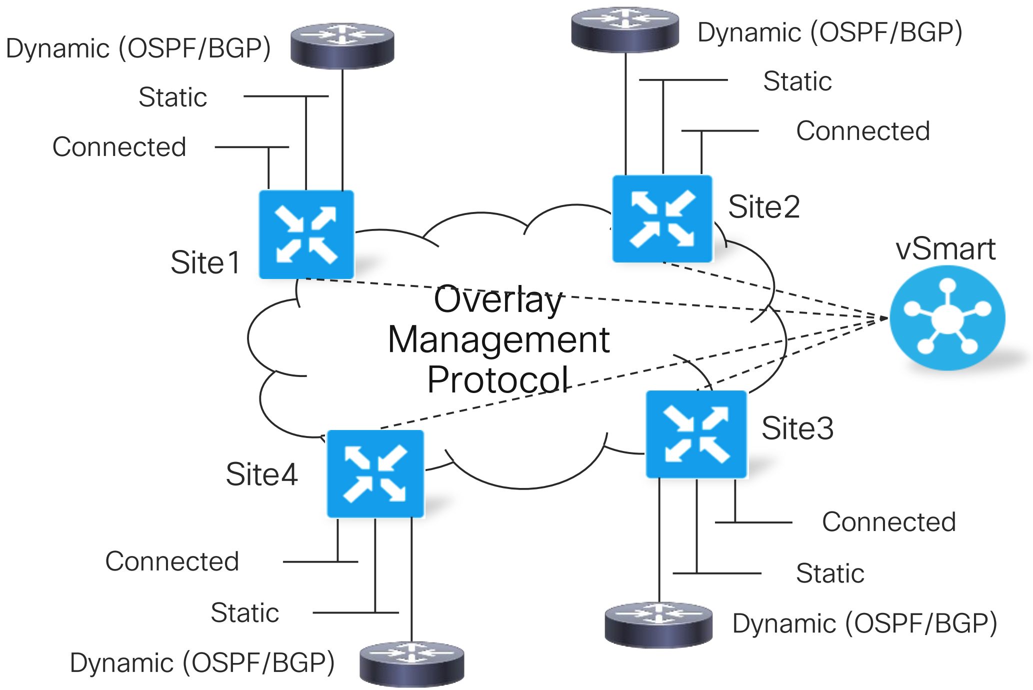
- Overlay Management Protocol – Control plane protocol distributing reachability, security and policies throughout the fabric
- Transport Locator (TLOC) – Transport attachment point and next hop route attribute
- Color – Control plane tag used for IPSec tunnel establishment logic
- Site ID – Unique per-site numeric identifier used in policy application
- System IP – Unique per-device (vEdge and controllers) IPv4 notation identifier. Also used as Router ID for BGP and OSPF.
- Organization Name – Overlay identifier common to all elements of the fabric
- VPN – Device-level and network-level segmentation

Overlay Management Protocol Overview



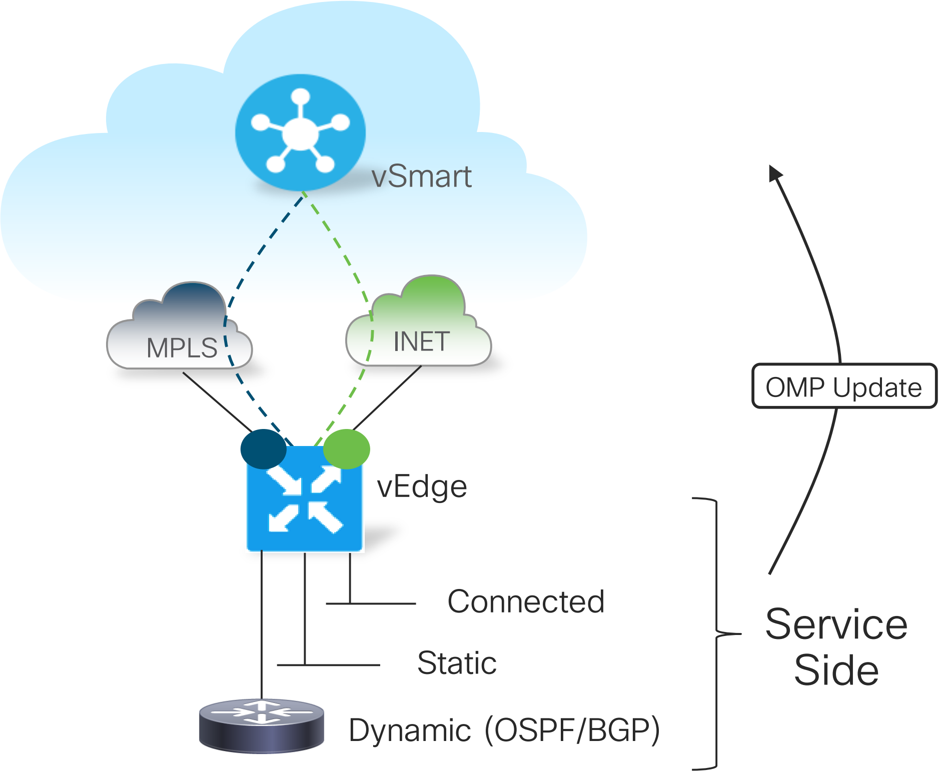
- TCP based extensible control plane protocol
- Runs between vEdge routers and vSmart controllers and between the vSmart controllers
  - Inside permanent TLS/DTLS connections
  - Automatically enabled on bringup
- vSmarts create full mesh of OMP peers
- Distribution of data-plane security parameters and policies
- Implementation of control (routing) and VPN membership policies

Overlay Routing: Service Routes



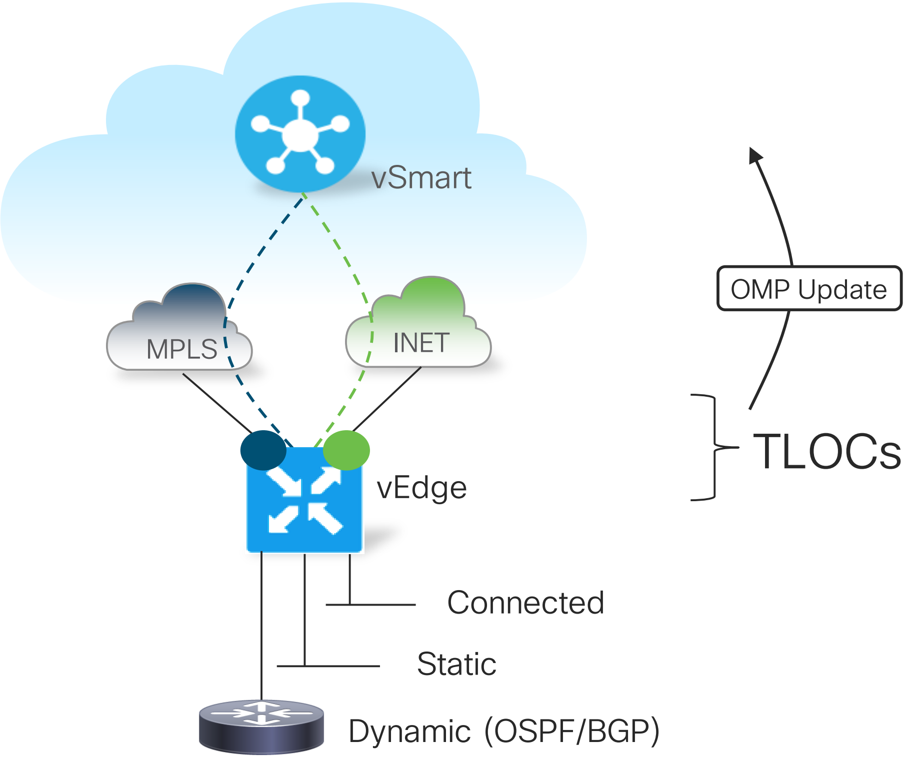
- Service routes are routes originating from outside the SDWAN
- i.e. "LAN" routes
- Redistributed to/from OMP
- OMP learns and translates routing information across the overlay
  - OMP routes, TLOC routes, network service routes
  - Unicast and multicast address families
  - IPv4 and IPv6 (March 2019)

Overlay Routing: OMP Routes



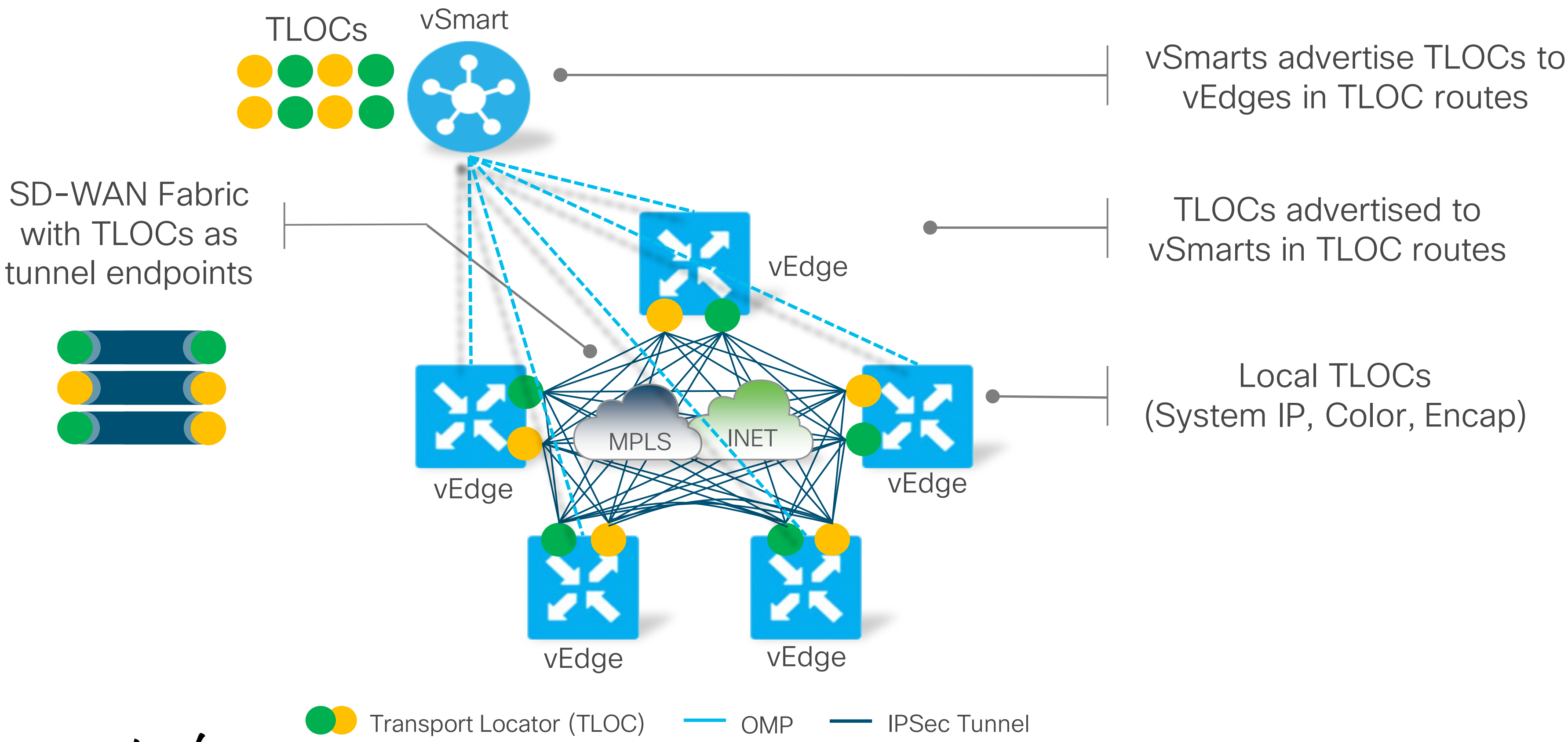
- Routes learnt from local service side
- Advertised to vSmart controllers
- Most prominent attributes:
  - TLOC
  - Site-ID
  - Label
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric
  - AS PATH

Overlay Routing: TLOC Routes

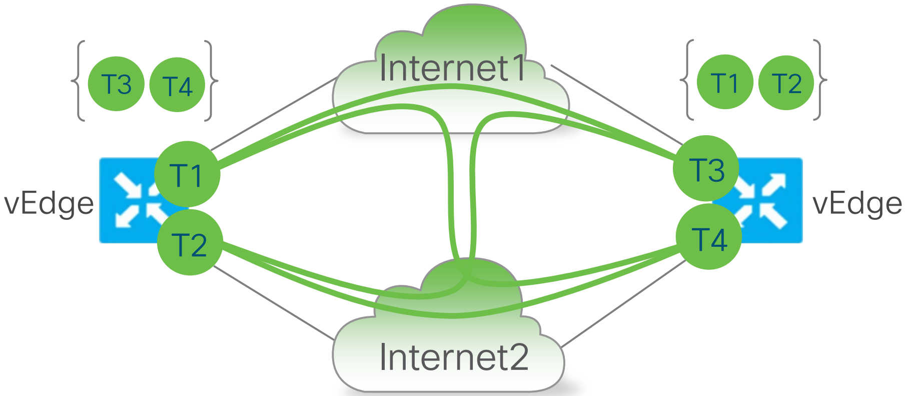


- Routes connecting locations to physical networks
- Advertised to vSmart controllers
- Most prominent attributes:
  - Site-ID
  - Encap-SPI
  - Encap-Authentication
  - Encap-Encryption
  - Public IP
  - Public Port
  - Private IP
  - Private Port
  - BFD-Status
  - Tag
  - Weight

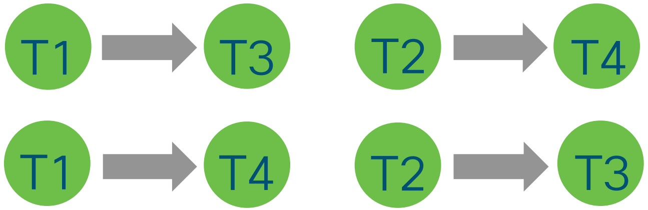
Transport Locators (TLOCs)

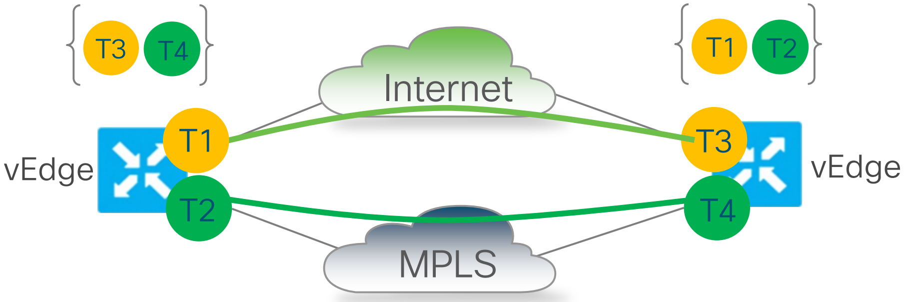


Transport Colors

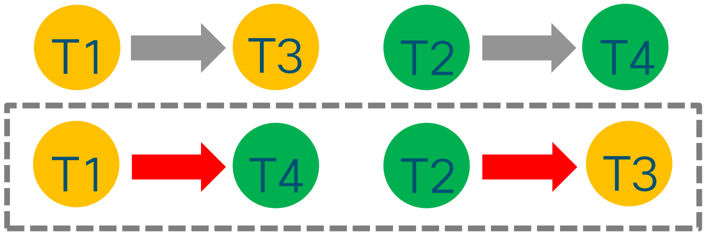


T1, T3 – Internet1 Color T2, T4 – Internet2 Color





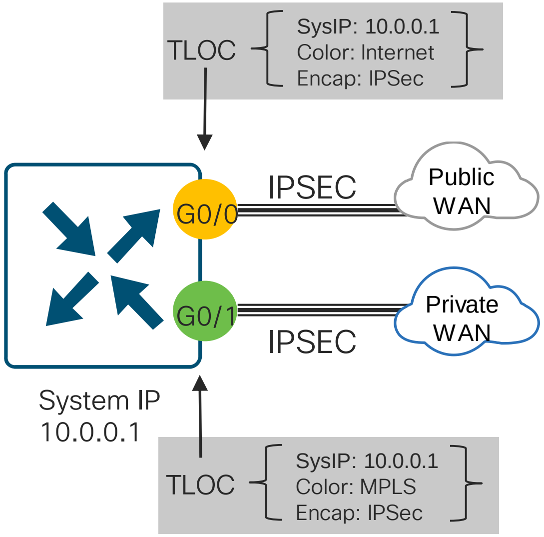
T1, T3 – Internet Color T2, T4 – MPLS Color



Color restrict will prevent attempt to establish IPSec tunnel to TLOCs with different color

Significance of TLOC Color

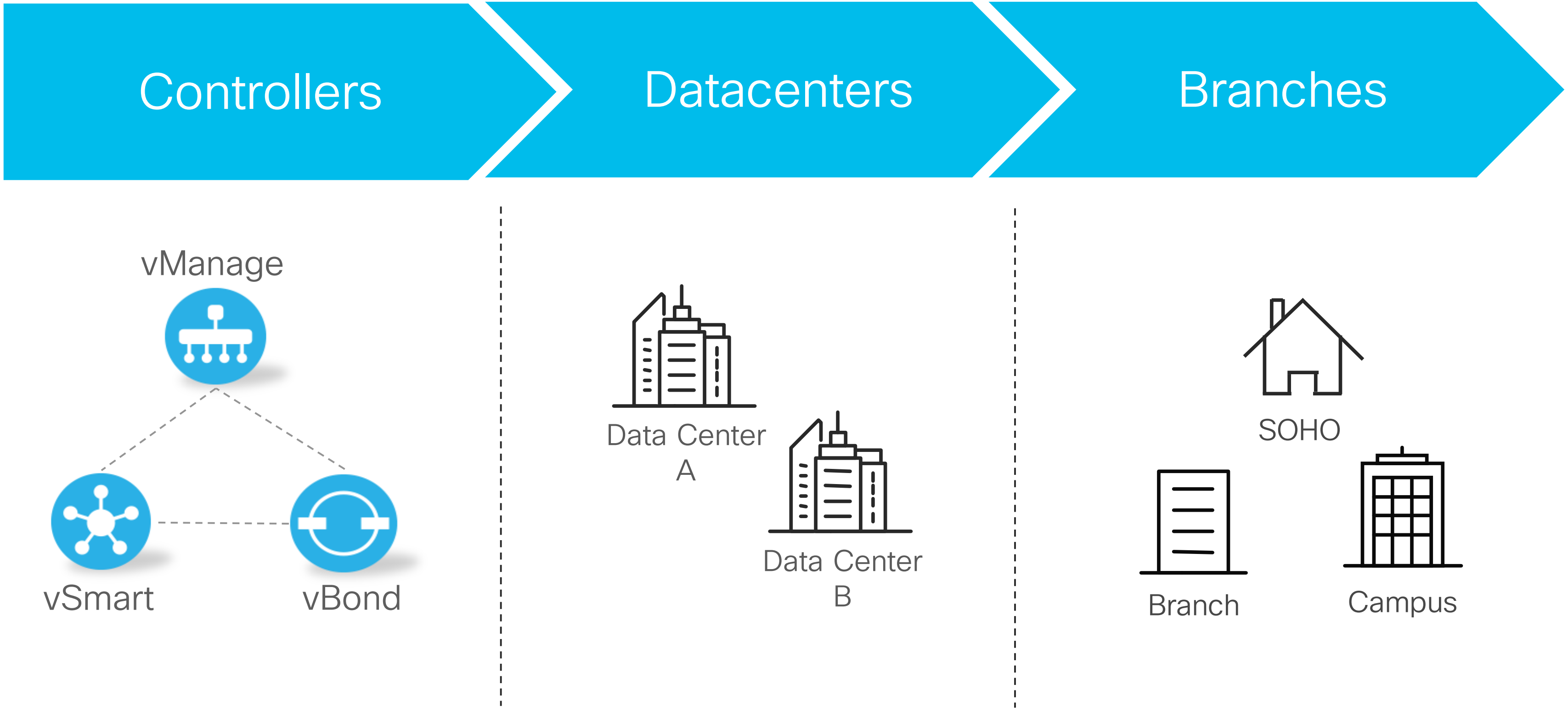
- Color is an abstraction used to identify individual WAN transport
- Colors are KEYWORDS not just LABELS
- Policy is written based on these
- TLOC maps to a physical WAN interfaces
- “Color” dictates the use of private-ip vs public-ip (dest) for Tunnel Establishment when there is NAT present
  - Example:
    - If two ends have a private color: private IP address/port used for DTLS/TLS or IPSec
    - If endpoint has public color: Public IP is used for DTLS/TLS or IPSec



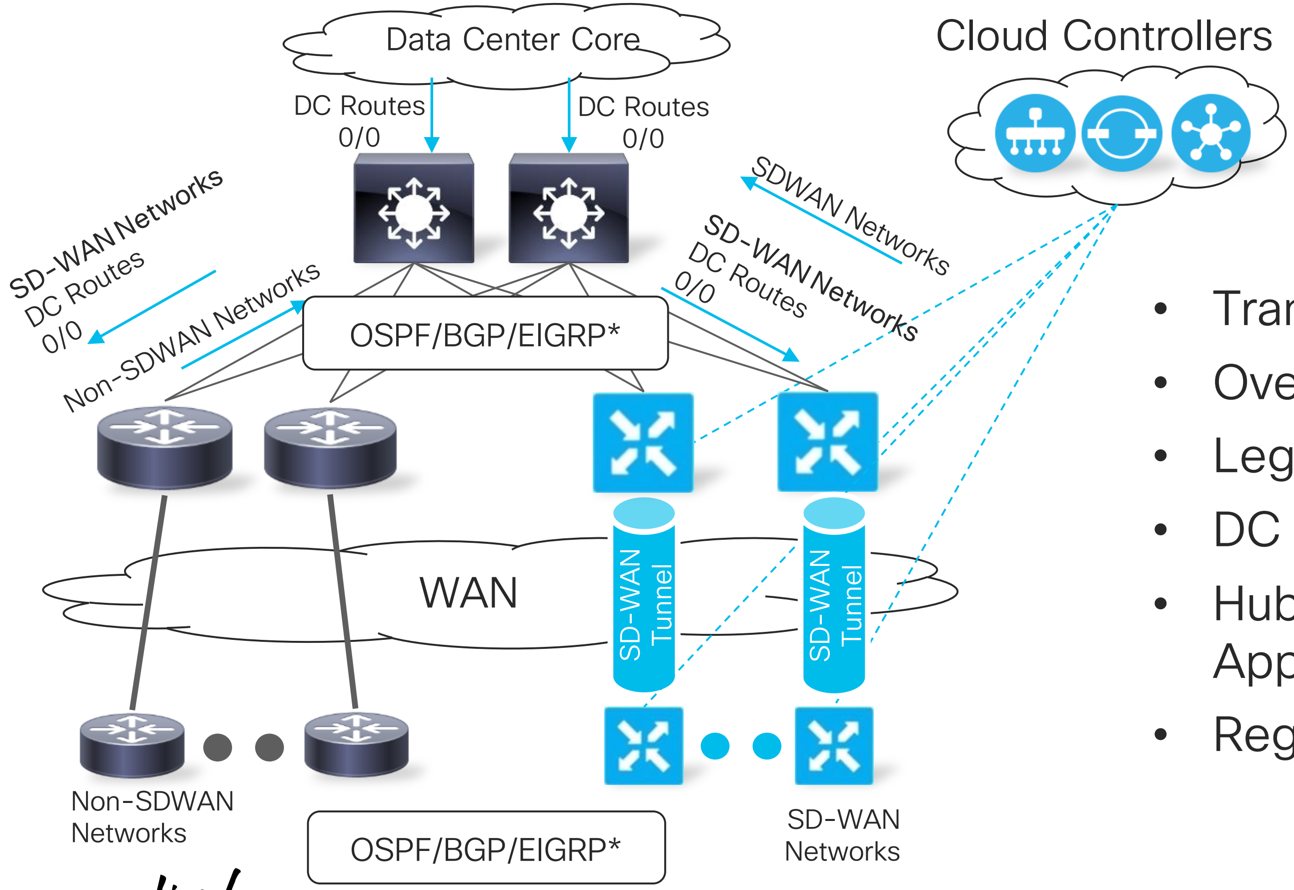
Private Colors	Public Colors
Metro-ethernet	3g
mpls	lte
private1	biz-internet
private2	public-internet
private3	blue
private4	green
private5	red
private6	gold
	silver
	bronze

Site Design & Deployment

Deployment Sequence



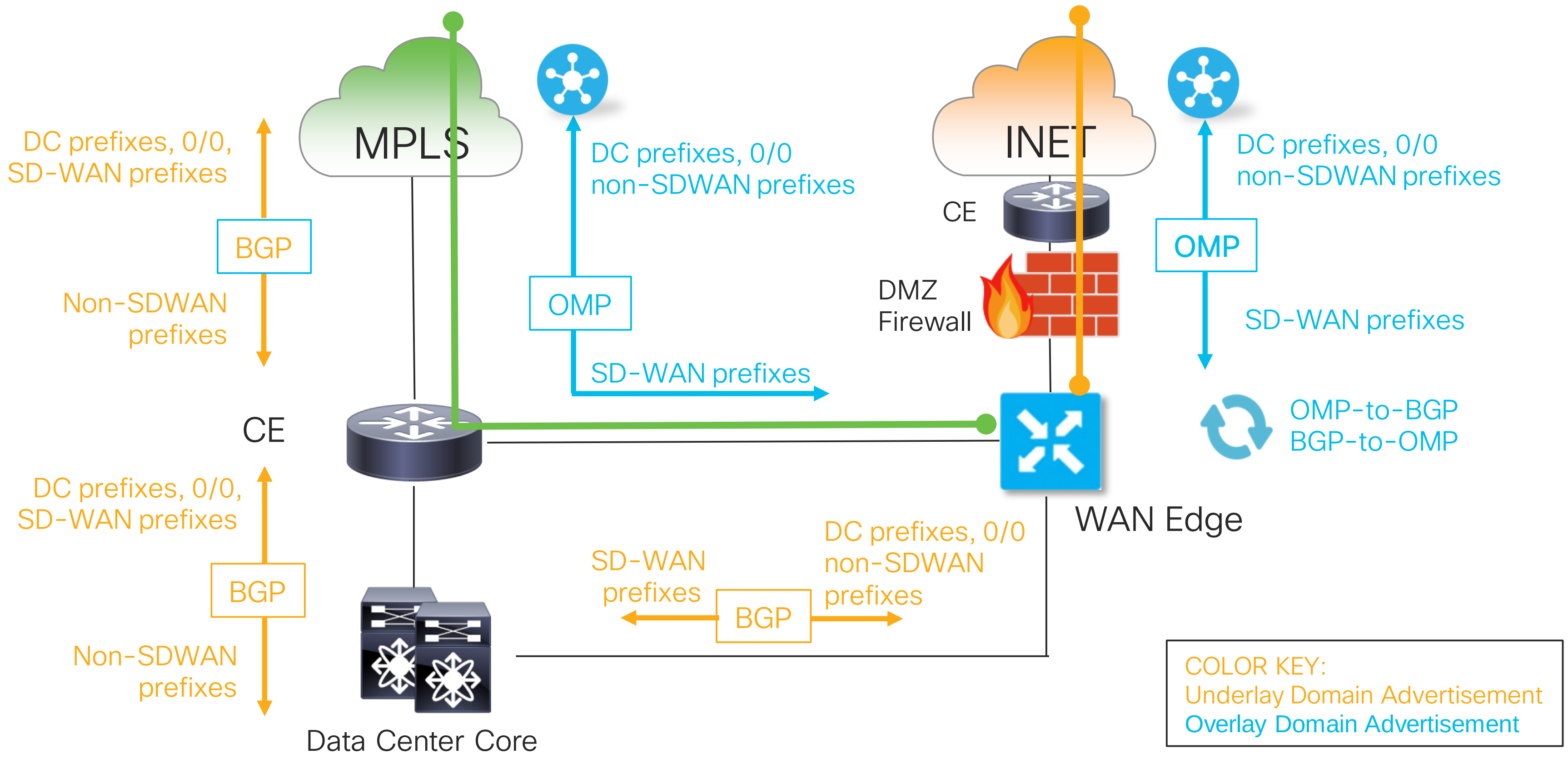
Deploying SDWAN – Routing Overview



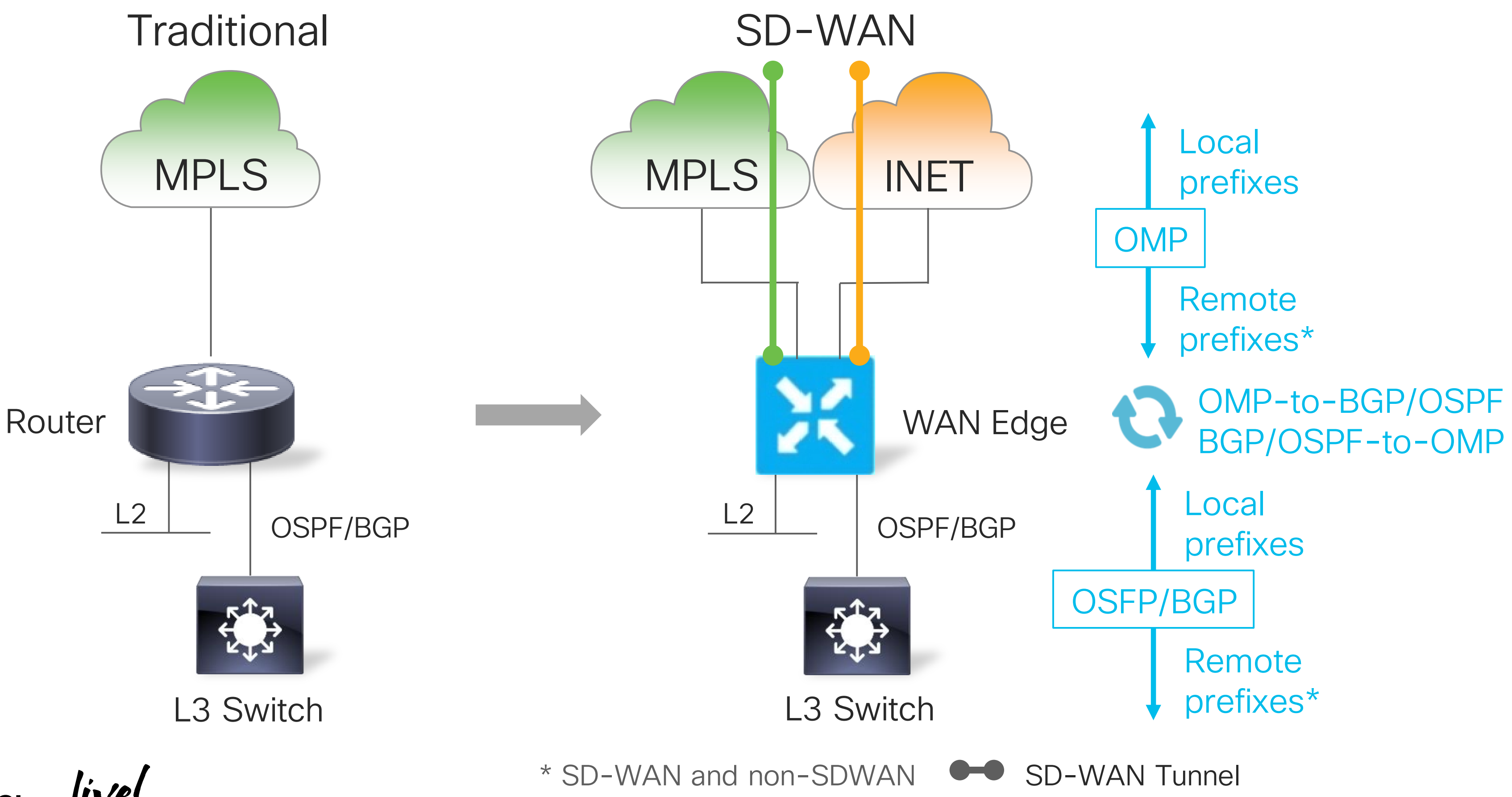
- Transition hubs
- Overlay Site Routing
- Legacy Site Routing
- DC Access
- Hub & Spoke Migration Approach
- Regionalization

*EIGRP support available March 2019

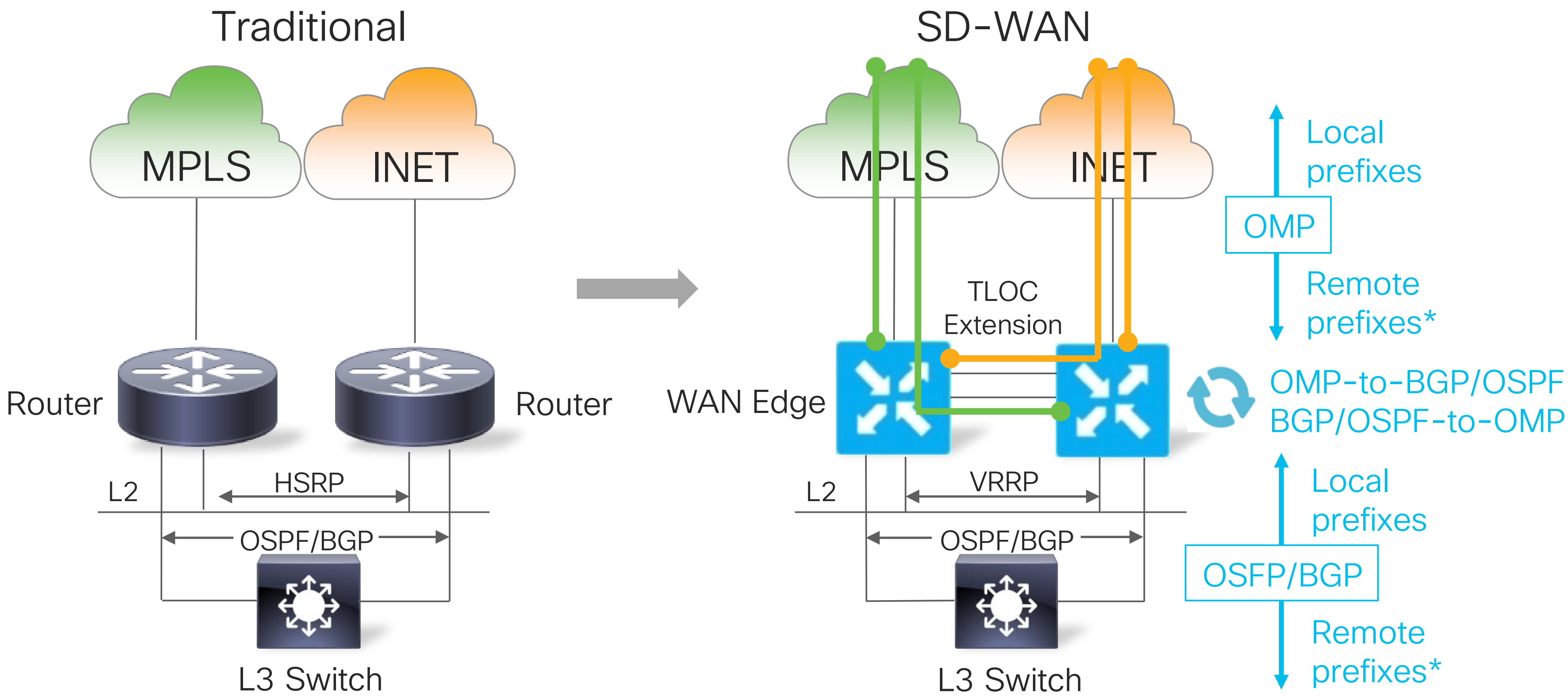
Data Center Routing



Branch Migration – In place

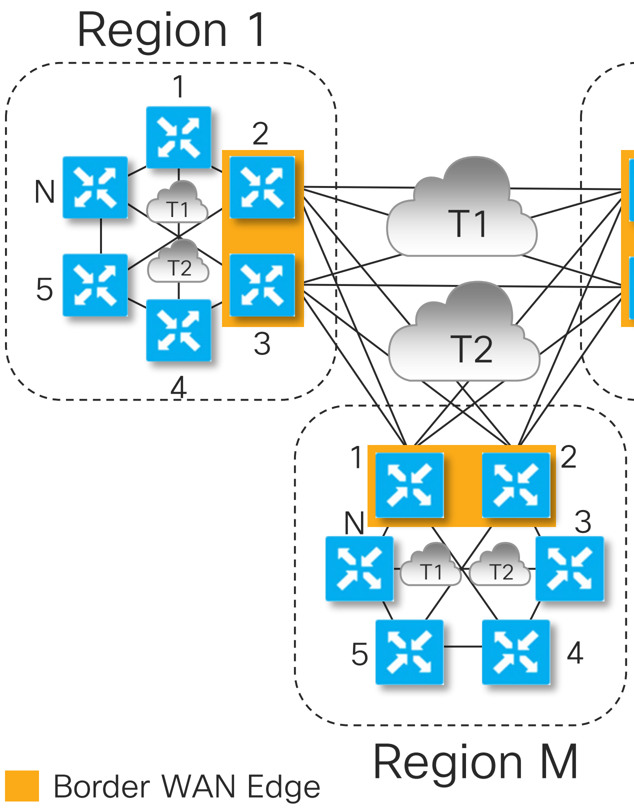


In Place Migration - Redundant



* SD-WAN and non-SDWAN
SD-WAN Tunnel

Topology – Regional Mesh



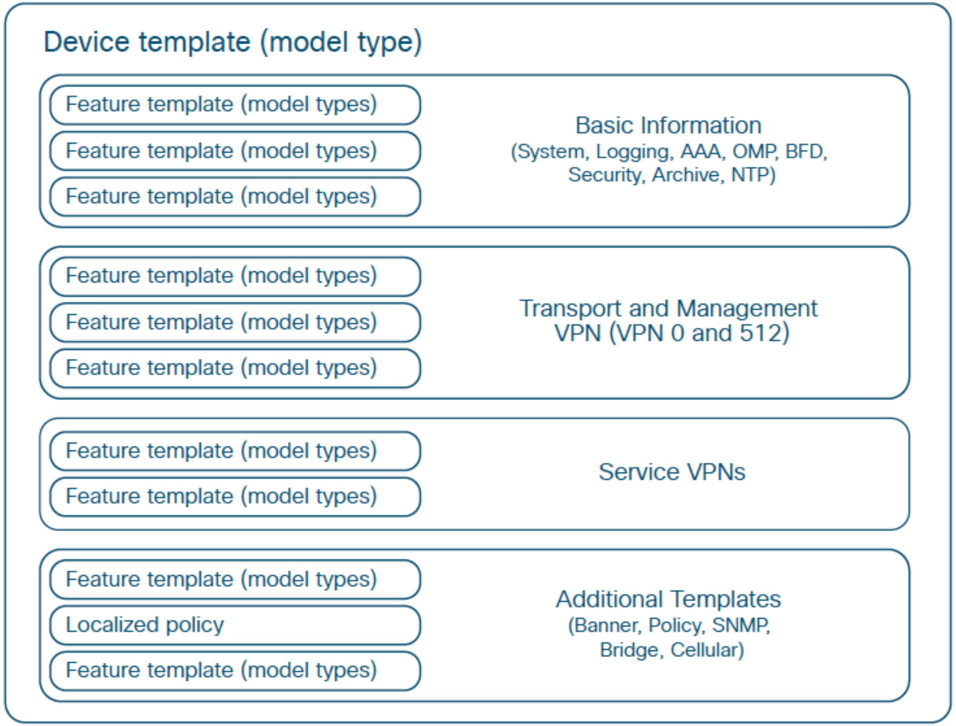
- M x Regions, N x Edges
- (N-1)[1] tunnel scale for intra-region WAN Edge
- 2*(M-1)[2] tunnel scale for border WAN Edge
- Doubled tunnel scale in case of dual transports
- Deny regional TLOCs in WAN core
- Permit regional edge routes through borders.
    - Set next-hop to Border TLOC

[1] Assumes single WAN Edge per-site
[2] Assumes dual border WAN Edges per-region

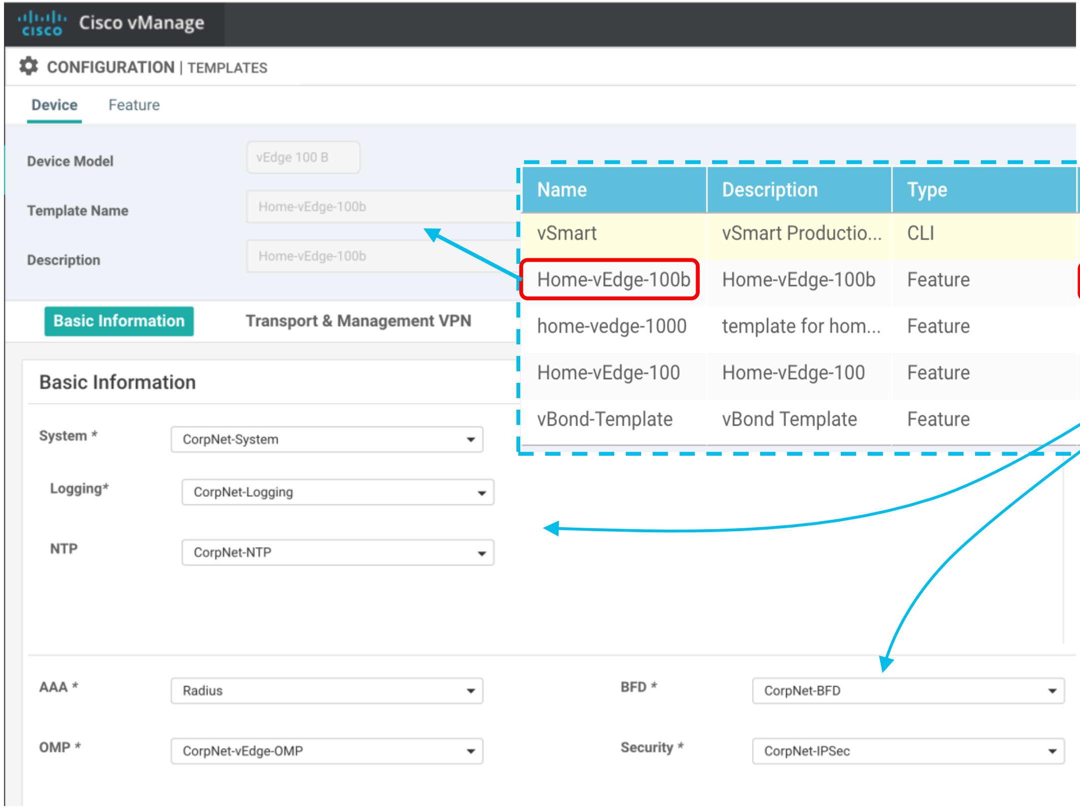
Device Template Structure

Site Router Configuration

- Specific to one device-type.
  (e.g. vEdge100, ISR4321)
- Basic Information
- Transport & Management (WAN side)
  - Transport VPN & Interfaces
  - Management VPN & Interface
  - Underlay BGP & OSPF configurations
- Service Side Configuration (LAN side)
  - Routing – BGP, OSPF, PIM, NAT, DHCP
  - Encaps – GRE, IPSec
  - VPNs (i.e. VRFs)
- Additional Templates
  - Housekeeping, logging servers, localized policy



Centralized Device Configuration via Templates



Name	Description	Type	Device Model	Feature Templates	Devices Attached
vSmart	vSmart Productio...	CLI	vSmart	0	1
Home-vEdge-100b	Home-vEdge-100b	Feature	vEdge 100 B	16	16
home-vedge-1000	template for hom...	Feature	vEdge 1000	17	3
Home-vEdge-100	Home-vEdge-100	Feature	vEdge 100	16	1
vBond-Template	vBond Template	Feature	vEdge Cloud	12	1

- Centralized Feature Templates
- Configuration with variables
- Self-recover on misconfiguration

https://www.youtube.com/watch?v=4hMMfM8OsoY

Frequently-used Feature Templates

For Your Reference

- **System** - Configure basic system information, site ID, system IP, time zone, hostname, device groups, GPS coordinates, port hopping, and port offset.
- **Logging** - Configure logging to disk and/or to a remote logging server.
- **AAA** - Specify authentication method, order. Configure Radius, TACACs, or local authentication, including local user groups with different read/write permissions.
- **BFD** - Specify BFD app-route multiplier and poll interval and specify the hello and BFD multiplier for each transport.
- **OMP** - Change graceful restart timers, advertisement and hold timers; change number of paths advertised; configure AS overlay number; set local redistribution into OMP; and change the number of equal-cost paths installed in the router.
- **Security** - Change the rekey time, anti-replay window, and authentication types for IPSec.
- **Archive** (optional) - Archive the full running configuration onto a file server within a time period specified.
- **NTP** (optional) - Configure NTP servers and authentication if required.
- **VPN** - Change ECMP hash, add DNS servers, advertise protocols (BGP, static, connected, OSPF external) from the VPN into OMP, add IPv4 or v6 static routes, service routes, and GRE routes.
- **BGP** (optional) - Configure the AS number, router ID, distance, maximum paths, neighbors, redistribution of protocols into BGP, hold time, and keepalive timers.
- **OSPF** (optional) - Configure router ID, distance, areas, OSPF interfaces, reference bandwidth, default information originate, metrics, metric type, and SPF timers.
- **VPN Interface configuration** - Configure interface name and status, static or dynamic IPv4 and v6 address, DHCP helper, NAT, VRRP, shaping, QoS, ingress/egress Access Control List (ACL) for IPv4 and 6, policing, static Address Resolution Protocol (ARP), 802.1x, duplex, MAC address, IP Maximum Transmission Unit (MTU), Transmission Control Protocol Maximum Segment Size (TCP MSS), TLOC extension, and more. In the case of the transport VPN, configure tunnel, transport color, allowed protocols for the interface, encapsulation, preference, weight, and more.
- **VPN interface bridge** (optional) - Configure layer 3 characteristics of a bridge interface, including IPv4 address, DHCP helper, ACLs, VRRP, MTU, and TCP MSS.
- **DHCP server** (optional) - Configure DHCP server characteristics, such as address pool, lease time, static leases, domain name, default gateway, DNS servers, and TFTP servers.
- **Banner** (optional) - Configure the login banner or message-of-the-day banner.
- **Policy** (optional) - Attach a localized policy.
- **SNMP** (optional) - Configure SNMP parameters, including SNMP device name and location, SNMP version, views, and communities, and trap groups.
- **Bridge** (optional) - Define layer 2 characteristics of a bridge, including the VLAN ID, MAC address aging, maximum MAC addresses, and physical interfaces for the bridge

Deployment Planning

Port Numbering, System IP

- Have a consistent Port Numbering scheme throughout the network
  - Factory config specifies certain ports in VPN 0 for DHCP to drive ZTP
  - Be sure this port has reachability to DHCP and DNS servers
- System IP – Persistent IPv4 Address
  - Uniquely identifies the device independently of interface addresses
  - Choose a hierarchy that follows Site ID or other logical scheme
  - Does not need to routable or advertised but…
  - Used as a marker for control policy
  - Best practice: advertise System IP as a source IP for SNMP/Logging correlation

Deployment Planning

Site ID

- Site ID is a unique identifier for the SITE location
  - Value from 1 – 4294967295.
  - Carried in OMP updates.
  - Same ID for all vEdges residing in the same site
  - Site could be a branch, campus, DC etc.
  - Required attribute to join the overlay
- Choose Site ID allocation schema carefully
  - Critical attribute use to scope Policy application (site, range of sites, etc)
  - No wild card support!

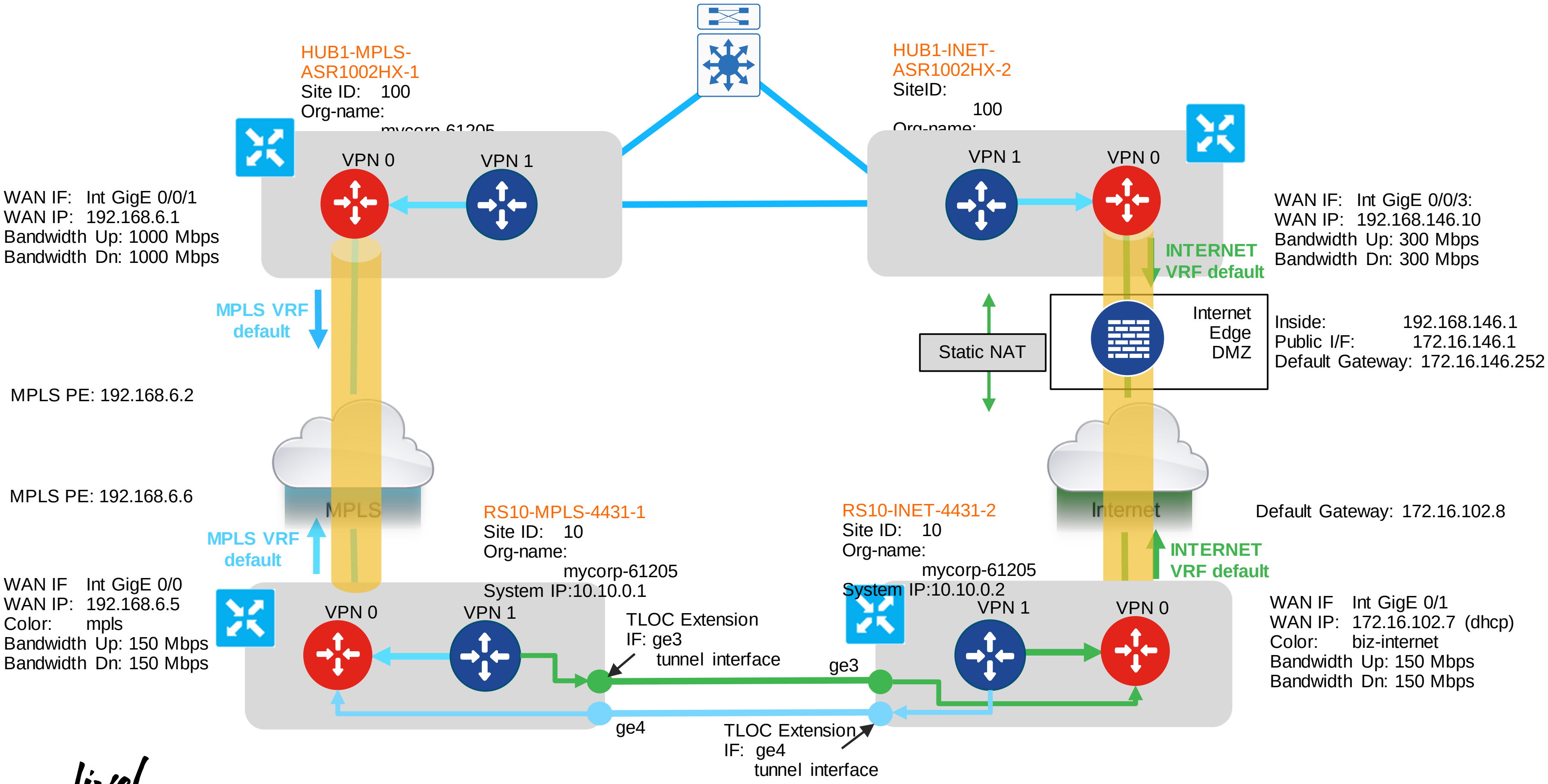
Digit	Representation	Examples
1	Country/continent	1=North America, 2=Europe, 3=APAC
2	Region	1=US West, 2=US East, 3=Canada West, 4=Canada East
3-6	Site type	0000-0099=Hub locations, 1000-1999=Type 1 sites, 2000-2999=Type 2 sites, 3000-3999 = Type 3 sites, 4000-4999=Type 4 sites, 5000-9999 = future use
7-9	Store/site/branch number, or any other ID specifier	001, 002, 003

Site Types Definition	
Service-sites – eg. Firewall	Type 1
Sites with Direct Internet Access	Type 2
Lower BW Sites	Type 3
Higher BW Sites	Type 4
Hub sites	Type 5

Cisco live!

Example Design

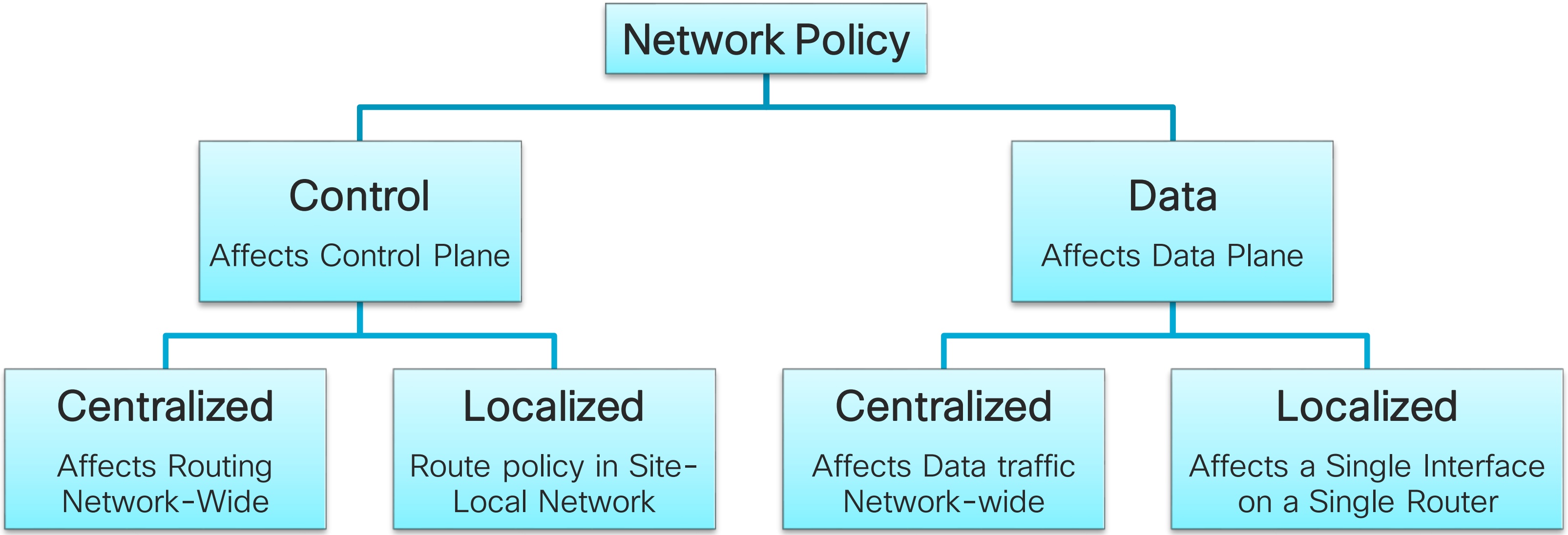
For Your Reference



Policy Design

Cisco SDWAN Policy Framework

Centralized Authoring – Globally or Locally Significant



Centralized Policy

Centralized Policy refers to policy provisioned on vSmart controllers. There are two types:

- **Control Policy**: Affects the routing in the overlay network-wide
  - Filter or modify information that is stored in the vSmart controller routing table
  - Filter advertisements made by the vSmart controller to the dataplane elements.
  - Control Policy is always on the vSmart controller. Never pushed to the vEdge routers
- **Data Policy**: Affects the flow of traffic throughout the VPN segments in the network
  - Apply to the flow of data traffic
  - Permit or restrict access based either on a 6-tuple match or on VPN membership
  - These policies are pushed to the affected vEdge routers

Localized Policy

Localized Policy refers to policy provisioned on dataplane routers. There are two types:

— **Local Control Policy**: underlay route policies on the service or transport networks

Implement traditional BGP or OSPF routing behaviours required to interface to the service or transport networks at the local site.

— **Local Data Policy**: Affects the flow of traffic throughout the VPN segments in the network

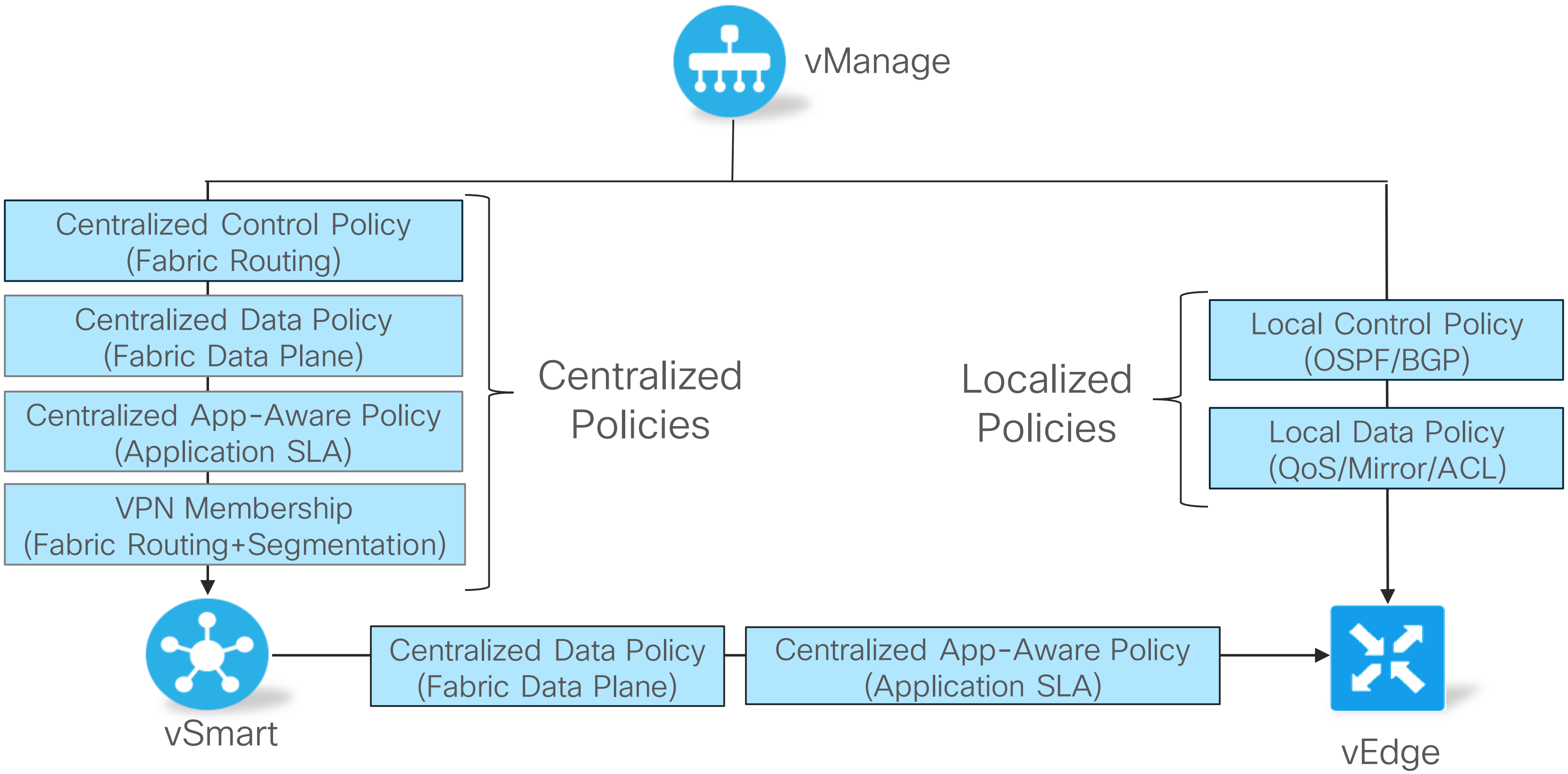
Access lists applied to a specific interface(s) on the router.

Simple access lists permit and restrict access based on a 6-tuple match.

Access lists for class of service (CoS) marking, queuing, policing, route-mapping and SPANning,

Control how data traffic flows out of and in to the router's interfaces and interface queues

Policy Distribution



vSmart Policy Construction

Lists

- **data-prefix-list** – list of prefixes for use with a data-policy
- **Prefix-list** – list of prefixes for use with any other policy
- **Site-list** – list of site-ids for use in policy and apply-policy
- **Tloc-list** – list of tlocs for use in policy
- **Vpn-list** – list of vpns for use in policy

+

Policy Definition

- **App-route-policy** is used together with sla-classes for application-aware-routing
- **Cflowd-template** configures the cflowd agents on the vEdge nodes
- **Control-policy** expresses OMP routing control
- **Data-policy** provides vpn-wide policy-based routing
- **Vpn-membership-policy** controls vpn membership across nodes

+

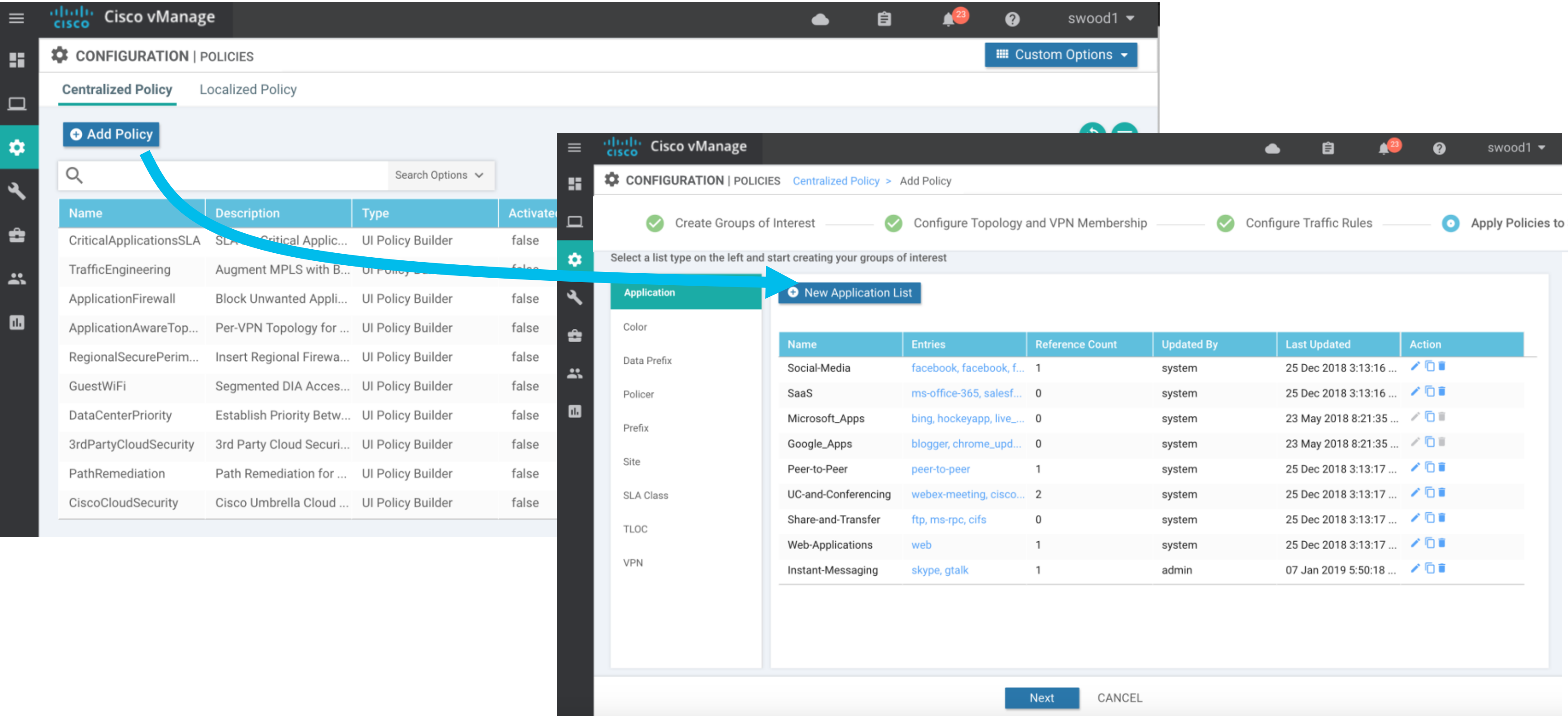
Policy Application

- **Apply-policy** is used in conjunction with a site-list to determine where policies are applied

=

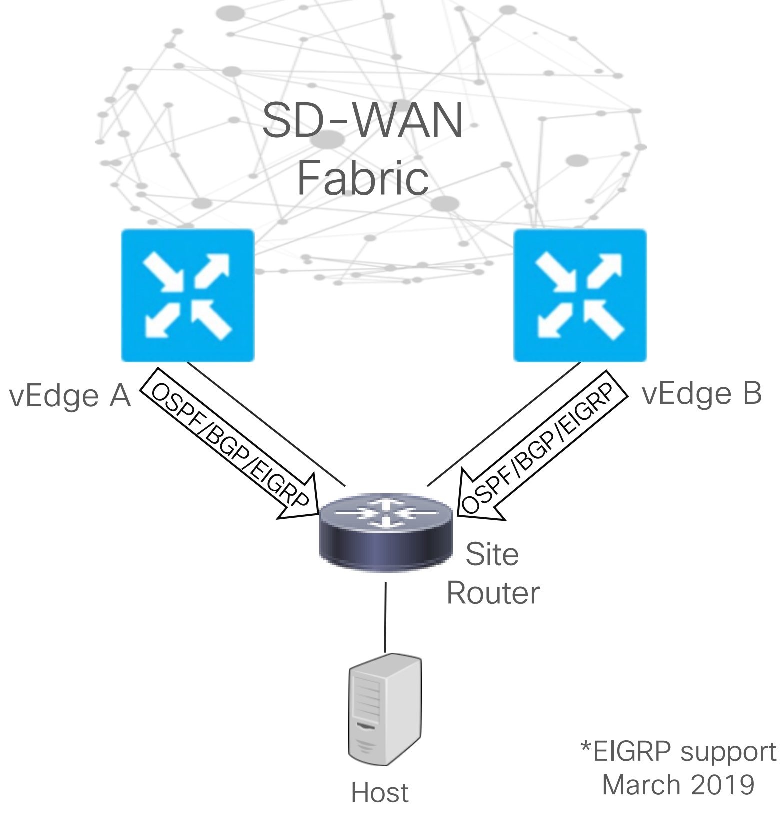
Complete policy definition configured on vSmart and enforced either on vSmart or on vEdge

Policy Creation Workflow in vManage



High Availability and Redundancy

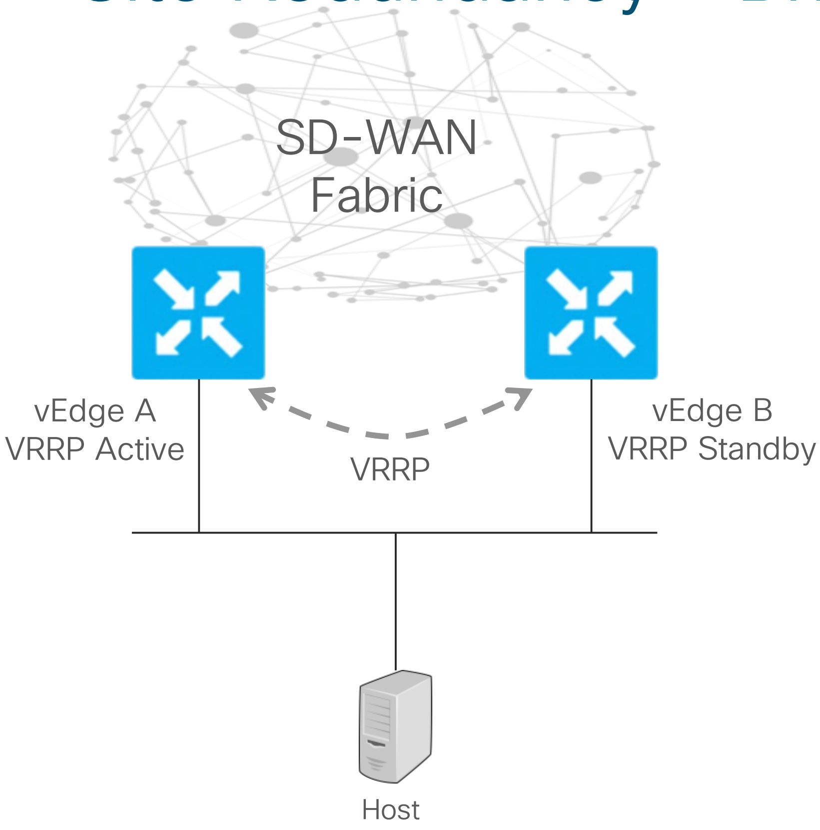
Site Redundancy - Routed



*EIGRP support
March 2019

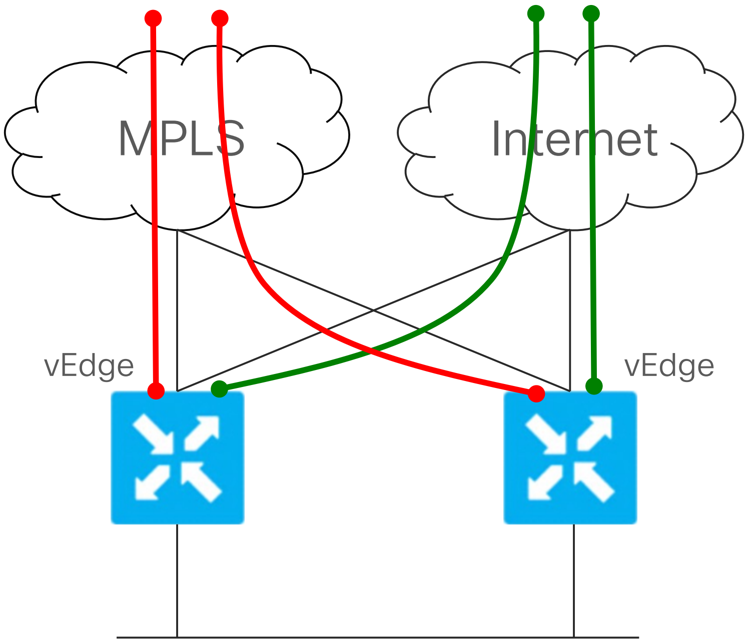
- Redundant pair of vEdge routers operate in active/active mode
- vEdge routers are one or more Layer 3 hops away from the hosts
- Standard OSPF/BGP/EIGRP* routing protocols are running between the redundant pair vEdge routers and the site router
- Bi-directional redistribution between OMP and OSPF/BGP and vice-versa on the vEdge routers
  - OSPF DN bit, BGP SoO community
- Site router performs equal cost multipathing for remote destinations across SD-WAN Fabric
  - Can manipulate OSPF/BGP to prefer one vEdge router over the other

Site Redundancy - Bridged



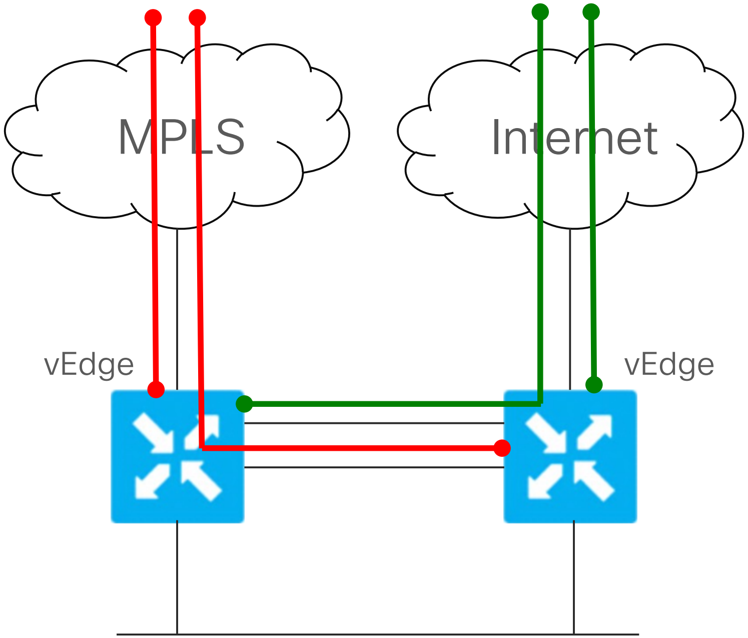
- vEdge routers are Layer 2 adjacent to the hosts
  - Default gateway for the hosts
- Virtual Router Redundancy Protocol (VRRP) runs between the two redundant vEdge routers
  - Active/active when using multi-group (per-VLAN)
- VRRP Active vEdge responds to ARP requests for the virtual IP with its physical interface MAC address
  - No virtual MAC
- In case of failover, new VRRP Active vEdge router sends out gratuitous ARP to update ARP table on the hosts and mac address table on the intermediate L2 switches

Transport Redundancy - Meshed



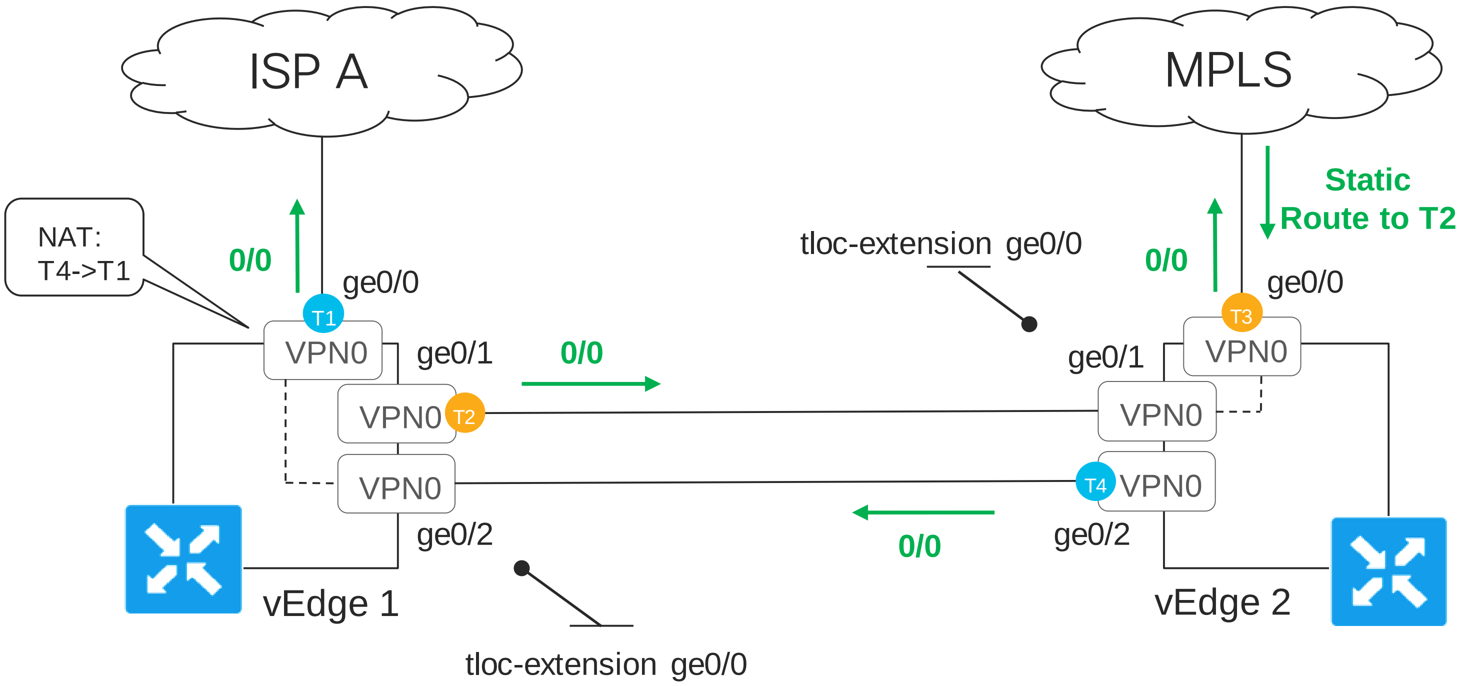
- vEdge routers are directly connected to all the transports
  - No need for L2 switches front-ending the vEdge routers
- When transport goes down, vEdge routers detect the condition and bring down the tunnels built across the failed transport
  - BFD times out across tunnels
- Both vEdge routers still draw the traffic for the prefixes available through the SD-WAN fabric
- If one of the vEdge routers fails (dual failure), second vEdge router takes over forwarding the traffic in and out of site
  - Both transport are still available

Transport Redundancy – TLOC Extension



- vEdge routers are connected only to their respective transports
- vEdge routers build IPSec tunnels across directly connected transports and across the transports connected to the neighboring vEdge router
  - Neighboring vEdge router acts as an underlay router for tunnels initiated from the other vEdge
- If one of the vEdge routers fails (dual failure), second vEdge router takes over forwarding the traffic in and out of site
  - Only transport connected to the remaining vEdge router can be used

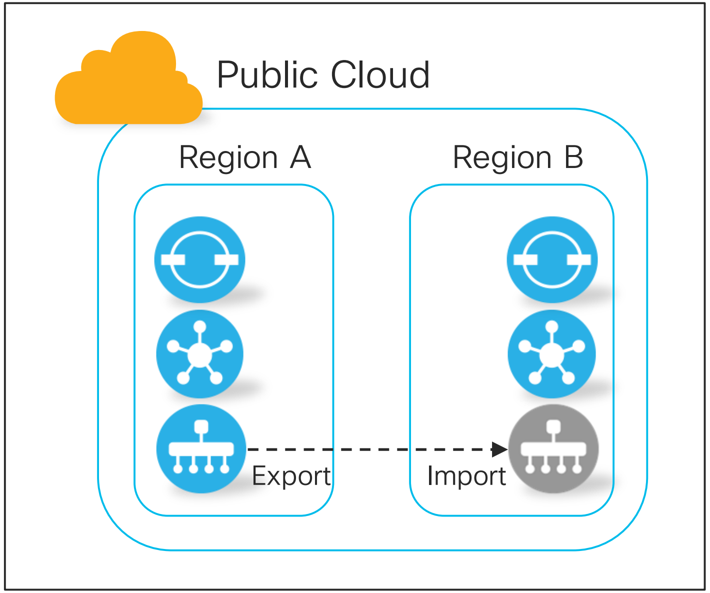
Internet and MPLS TLOC-Extension (Static)



Note: vEdge router connected to ISP will perform NAT on the traffic from the TLOC-extended interface

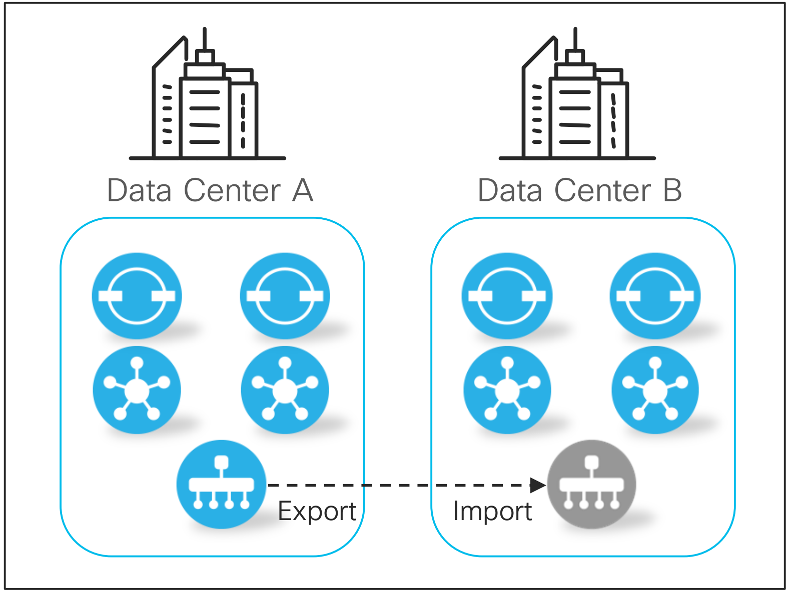
Color biz-internet
Color mpls

Controllers Redundant Deployment

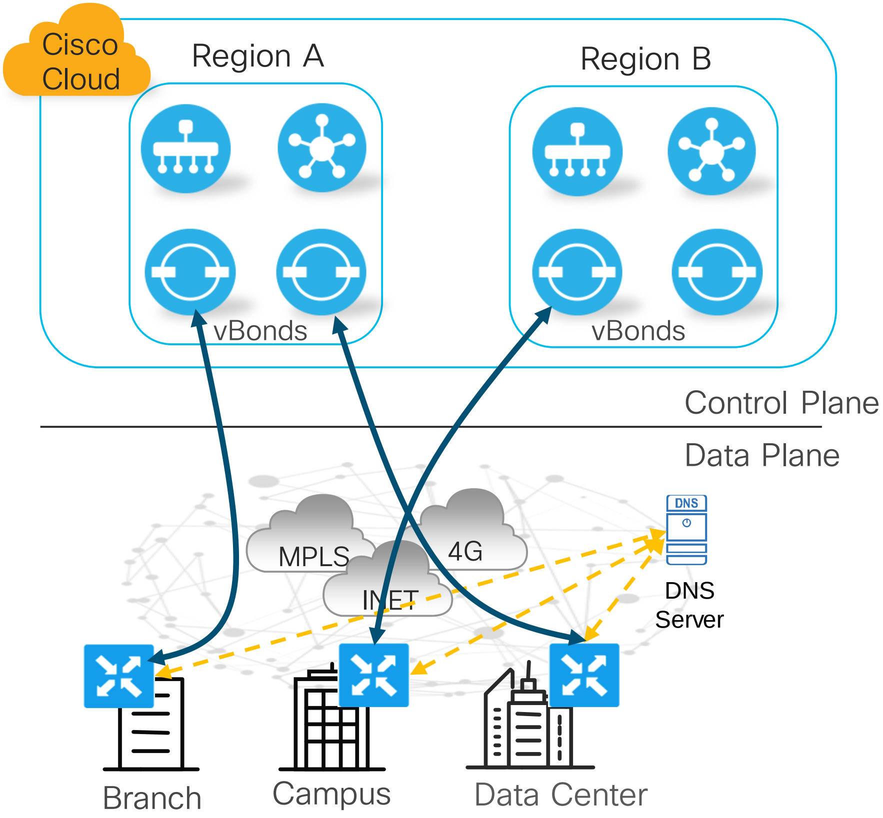


- Controllers are distributed across multiple public cloud regions
- Active-active, vManage is cold-standby

- Controllers are distributed across multiple private data centers
- Active-active, vManage is cold-standby

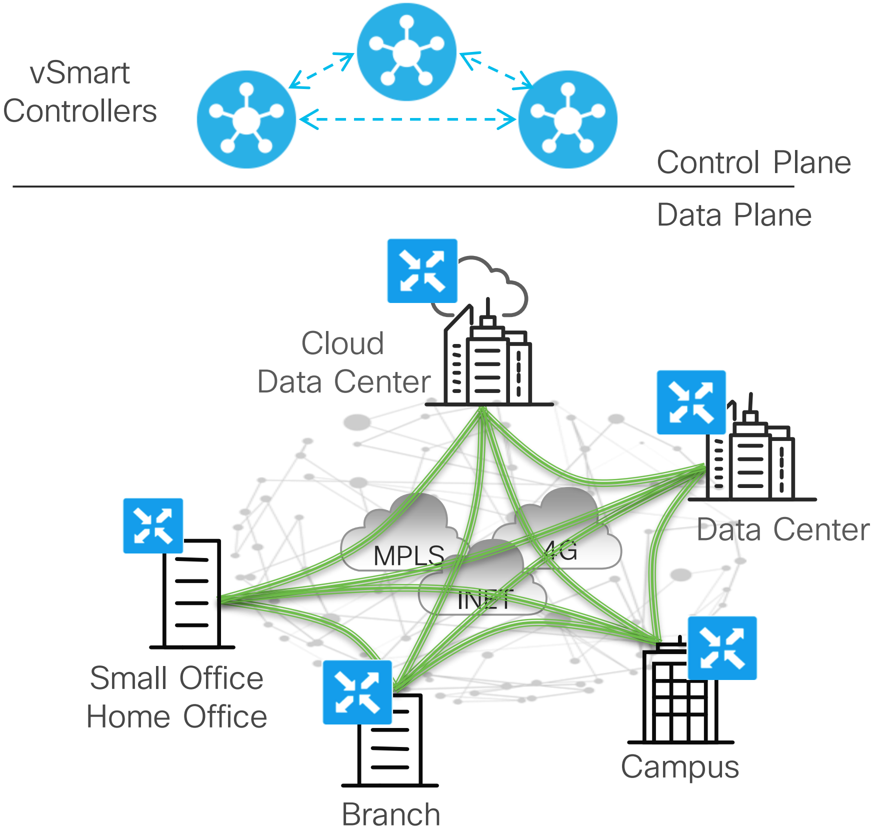


Control Redundancy - vBond



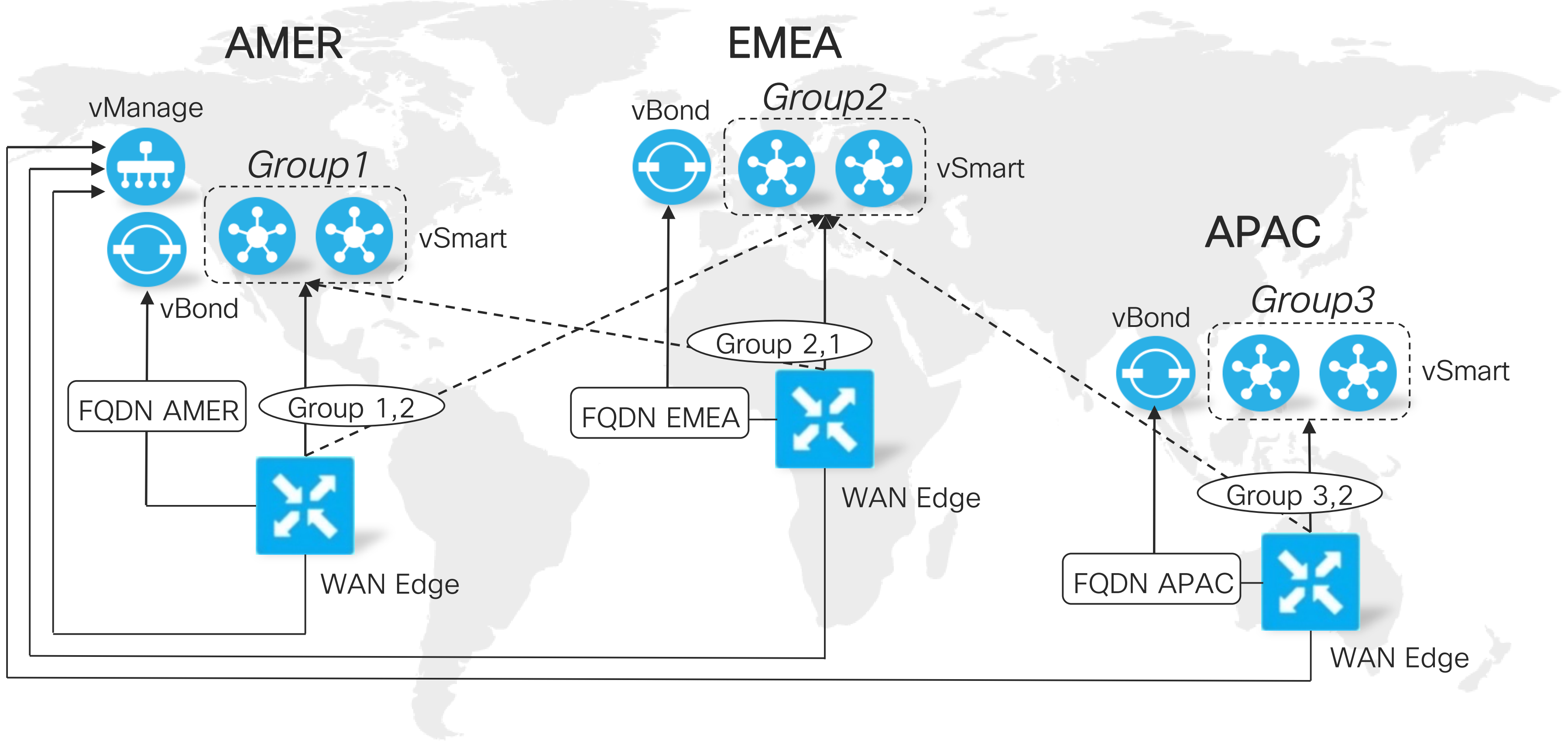
- vBond orchestrators have a whole view of the devices allowed on the network
- Multiple vBonds can be deployed for Function and Geographic redundancy
- vEdges pick vBond via DNS
- DNS round-robin is utilized
- vEdge will try first entry, then second, and so on
- vEdge to vBond connection
  - Temporary
  - Stateless
- vBonds maintain view of load on vSmarts
  - Delivers list of vSmart's to use

Control Redundancy - vSmart

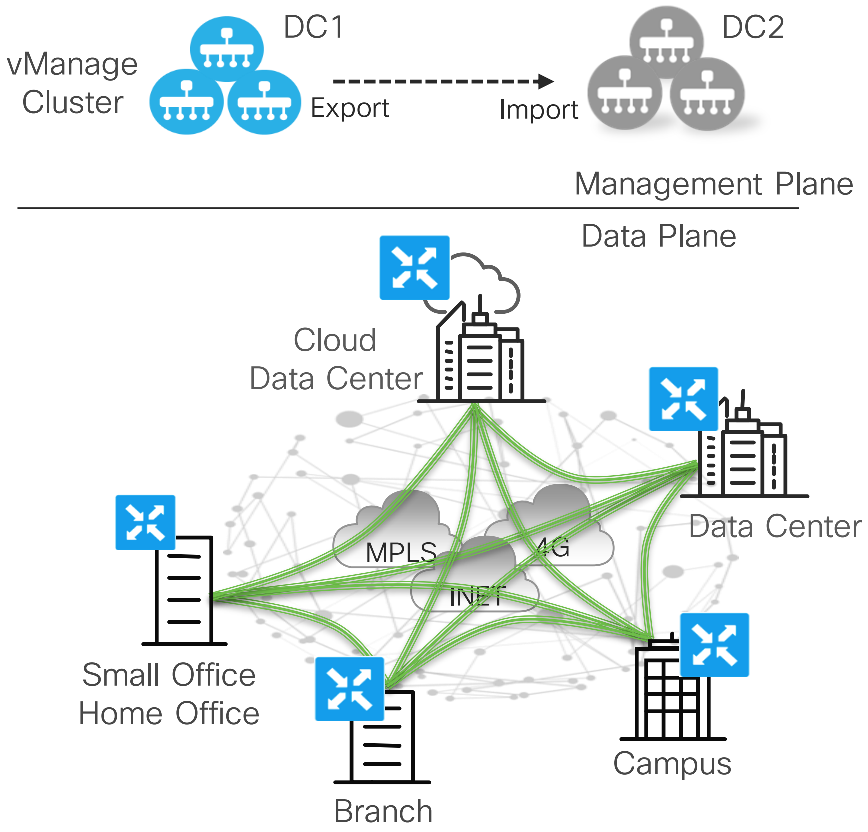


- vSmart controllers exchange OMP messages and have identical view of the SD-WAN fabric
- vEdge routers connect to up to three vSmart controllers for redundancy
- Single vSmart controller failure has no impact, other registered vSmart still available
- If all vSmart controllers fail or become unreachable, vEdge routers will continue operating on a last known good state for a configurable amount of time (min of re-key timer and GR timer)
  - No updates to reachability
  - No IPSec rekey
  - No policy changes propagation

Controllers Regional Affinity (Optional)



Control Redundancy - vManage



- vManage servers form a cluster for redundancy and high availability
- All servers in the cluster act as active/active nodes
  - All members of the cluster must be in the same DC / metro area
- For geo-redundancy, vManage servers operate in active/standby mode
  - Not clustered
  - Database replication between sites is needed
- Loss of all vManage servers has no impact on fabric operation
  - No administrative changes
  - No statistics collection

vManage Snapshots and Recovery

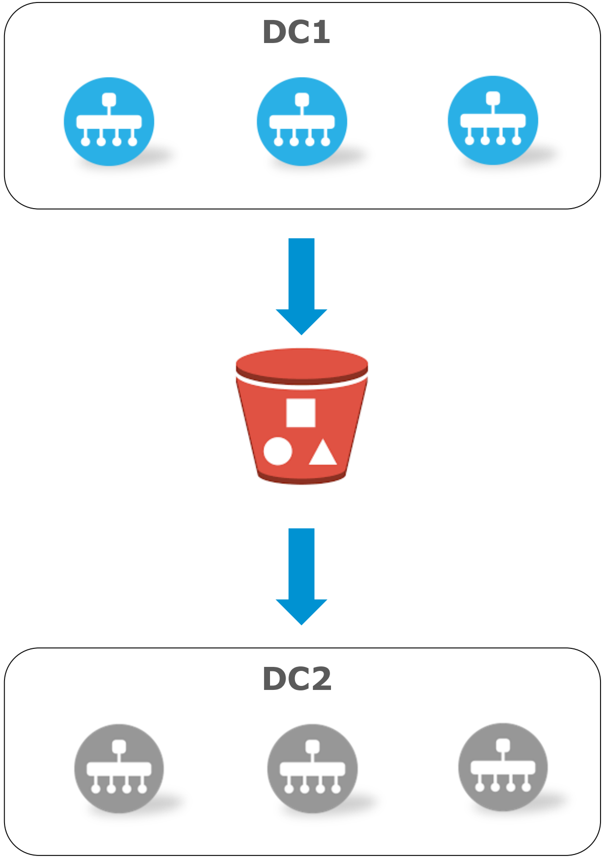
Best Practices

Snapshots

- vManage data volume periodically backed-up in active DC. Period is based on change frequency.
- vSmart and vBond are stateless (state can be re-created). No need to snapshot.

Recovery

- New volumes created from backed-up data volume
- New vManage instances created and attached to new volume (can be in cold standby – loaded and ready to start)



Closing

Cisco SD-WAN Platform Options

SD-WAN + Branch Services

ISR 1000

- 200 Mbps
- Next-gen connectivity
- Performance flexibility

ISR 4000

- Up to 2 Gbps
- Modular
- Integrated service containers
- Compute with UCS E

ASR 1000

- 2.5-200Gbps
- High-performance service w/hardware assist
- Hardware & software redundancy

SD-WAN

vEdge 100

- 100 Mbps
- 4G LTE & Wireless

vEdge 1000

- Up to 1 Gbps
- Fixed

vEdge 2000

- 10 Gbps
- Modular

Virtualization

ENCS 5100

- Up to 250Mbps

ENCS 5400

- 250Mbps – 2GB

Public Cloud

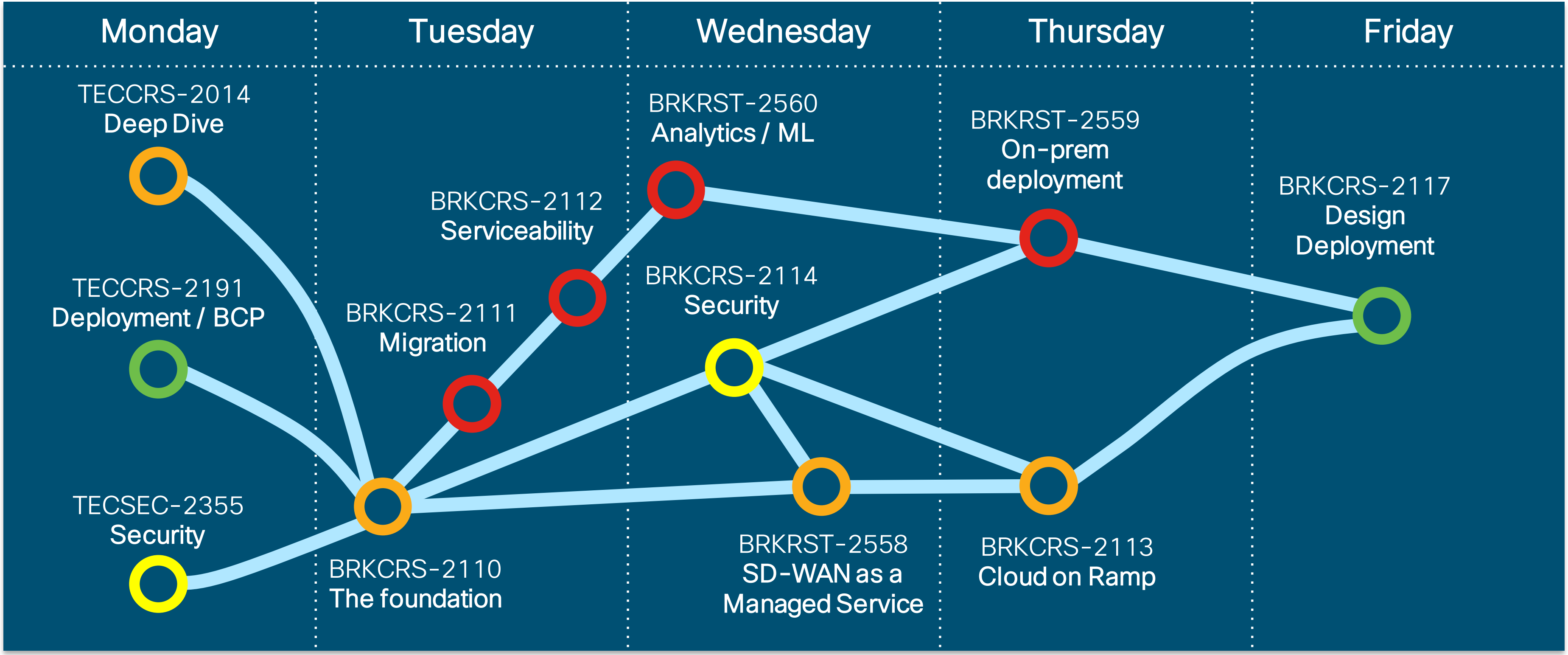
Microsoft Azure

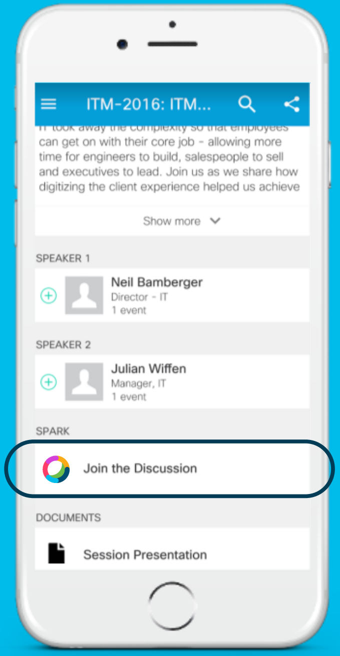
amazon web services

Summary

- Plan, Prepare, Educate
- Leverage Cloud Controllers
- Follow Migration Best Practice
- Simplify the routing design
- Embrace the flexible architecture

Your SD-WAN learning map at CLEUR





cs.co/ciscolivebot#BRKCRS-2117

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

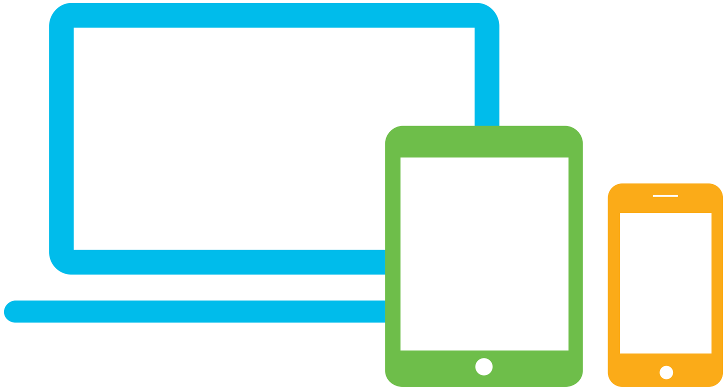
How

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

Complete your online session survey

- Please complete your Online Session Survey after each session
- Complete 4 Session Surveys & the Overall Conference Survey (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Events Mobile App or the Communication Stations

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com



Continue Your Education

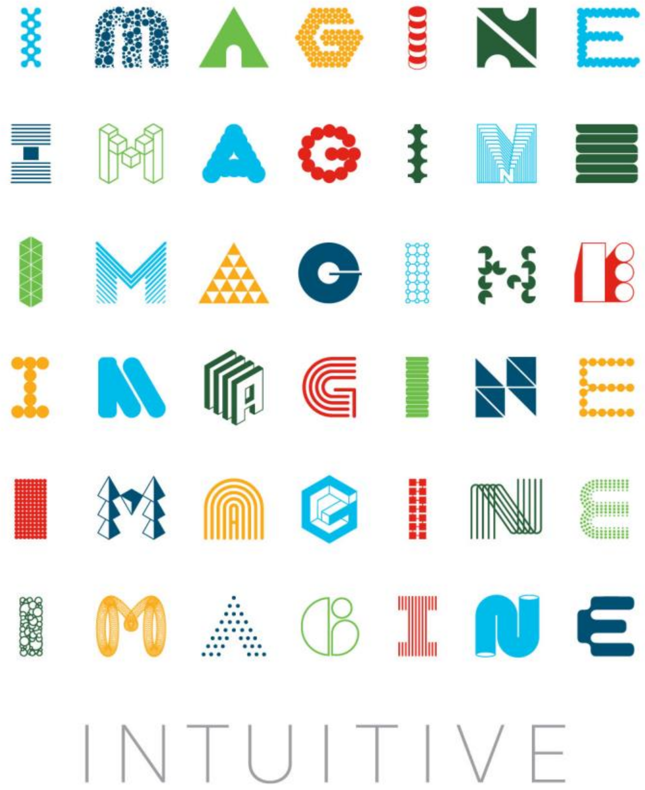
Demos in the Cisco Showcase

Walk-in self-paced labs

Meet the engineer 1:1 meetings

Related sessions

Thank you


IMAGINE
IMAGINE
IMAGINE
IMAGINE
IMAGINE
IMAGINE
INTUITIVE

IMAGINE

INTUITIVE