



The bridge to possible

From Zero to SD-WAN Hero

Planning, Designing and Implementing Cisco SD-WAN

Tomasz Zarski, Customer Delivery Architect – Enterprise Networks

Manuel Alvarez, Technical Solutions Specialist – Enterprise Networks



Agenda

- Introduction and Cisco SD-WAN Solution Overview
- SD-WAN Control Plane and Data Plane
- Configuration Templates and Policies
- SD-WAN Deployment Strategy
- Controllers and WAN Edge Platforms
- DC and Branch Deployment
- Conclusion

Cisco Webex App

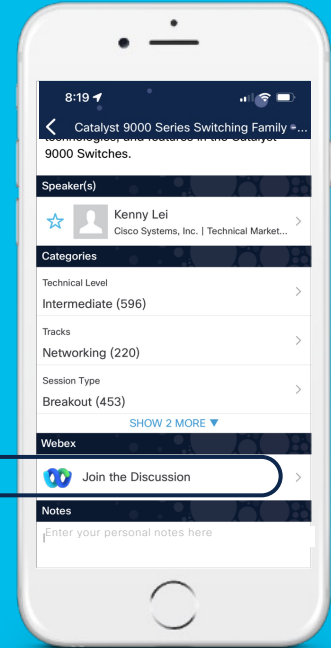
Questions?

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.



Why Cisco SD-WAN

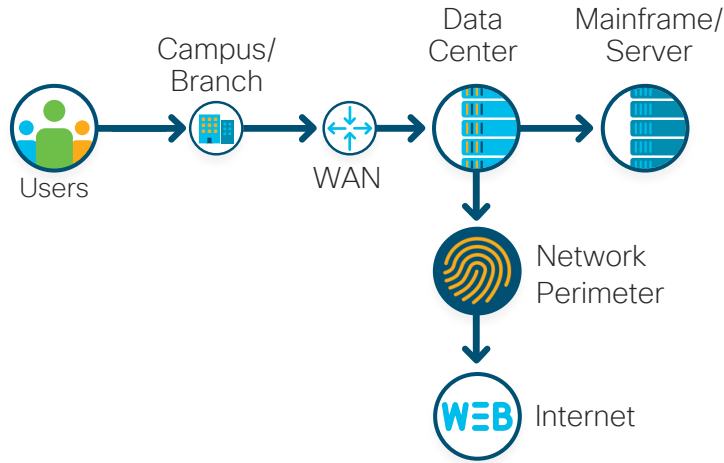
What is SD-WAN?

The **software-defined wide area network (SD-WAN)** is a technology for configuring and implementing an **enterprise WAN** based on software-defined networking (SDN) decoupling the **Control Plane, Data Plane** and **Management Plane**.

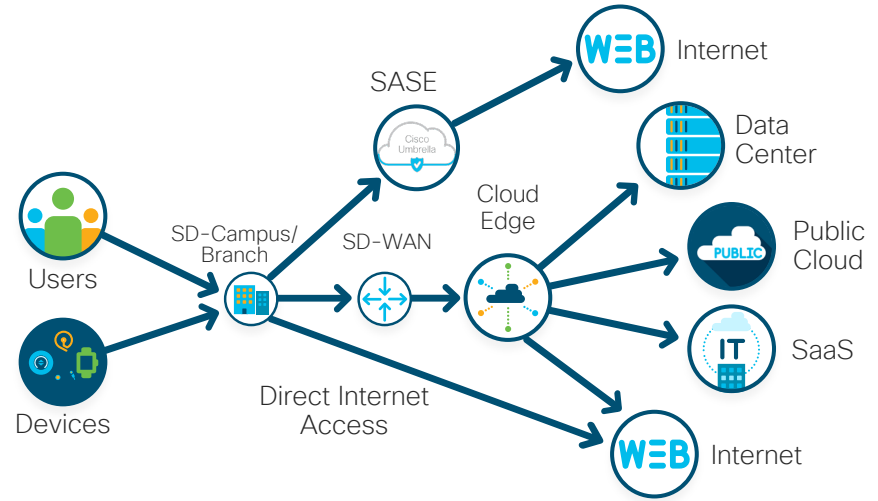


Hybrid Cloud Ready Network Topology

As-is Topology



To Be Topology



Secure Cloud Scale SD-WAN Architecture

Any Deployment

**Management
& Analytics**

On-premise | Cloud | Multi-tenant
Automation | Network Insights | Machine Learning | AI
Open | Programmable | Scalable

Any Service



Multi-Cloud
Optimization



Multi-Layer
Security



Multi-Domain
IBN Policy



Voice



Analytics

Any Transport



Satellite



Internet



MPLS



LTE/5G

Any Location



DC/Branch



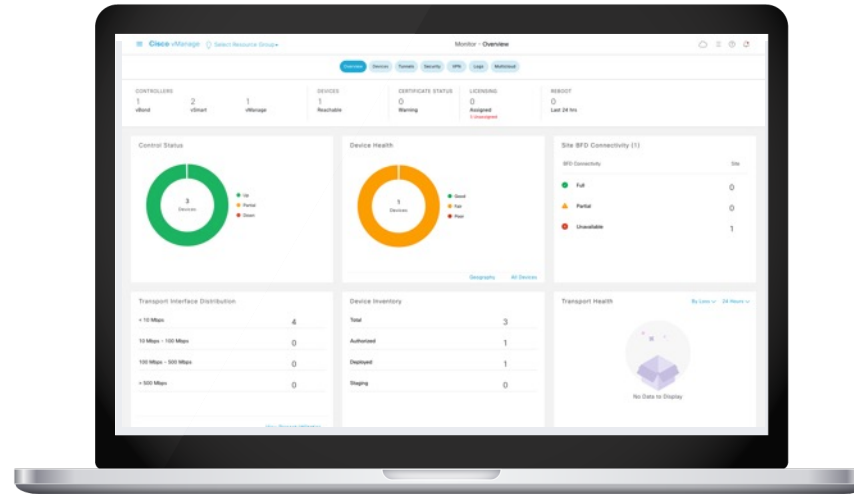
Colocation



Cloud

SD-WAN Controller for Simplified Management

Cisco vManage



Single monitoring dashboard

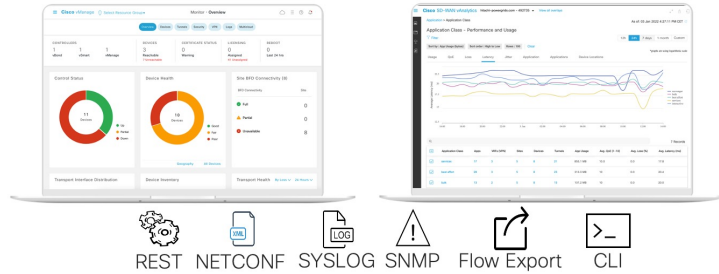
Configuration: OnRamp, security, devices, policies, templates

Lifecycle management

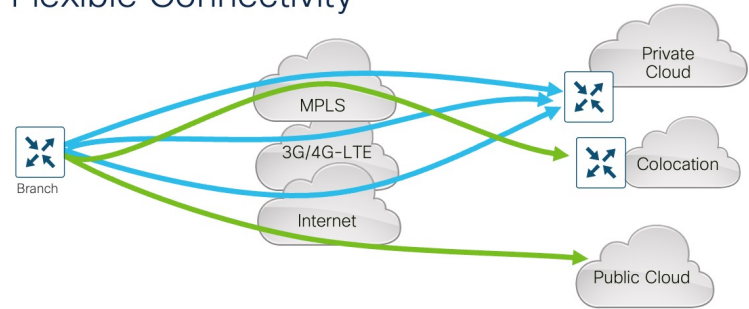
Role based access/
multi-tenant

SD-WAN Use Cases

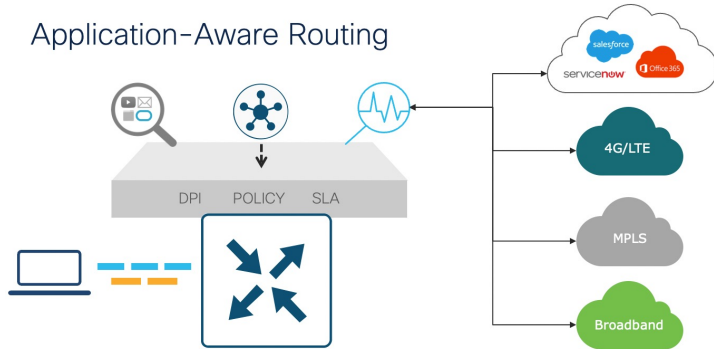
Simplify WAN Management



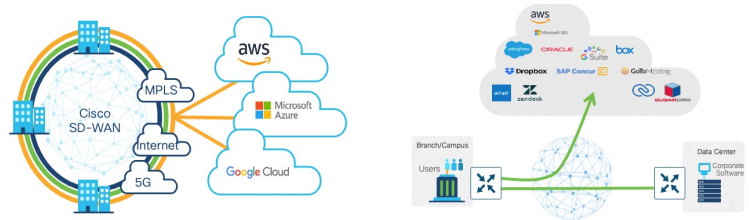
Flexible Connectivity



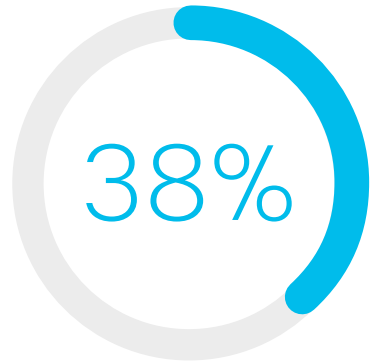
Application-Aware Routing



Cloud Ready WAN



Business value of Cisco SD-WAN



Lower five-year cost of WAN operations

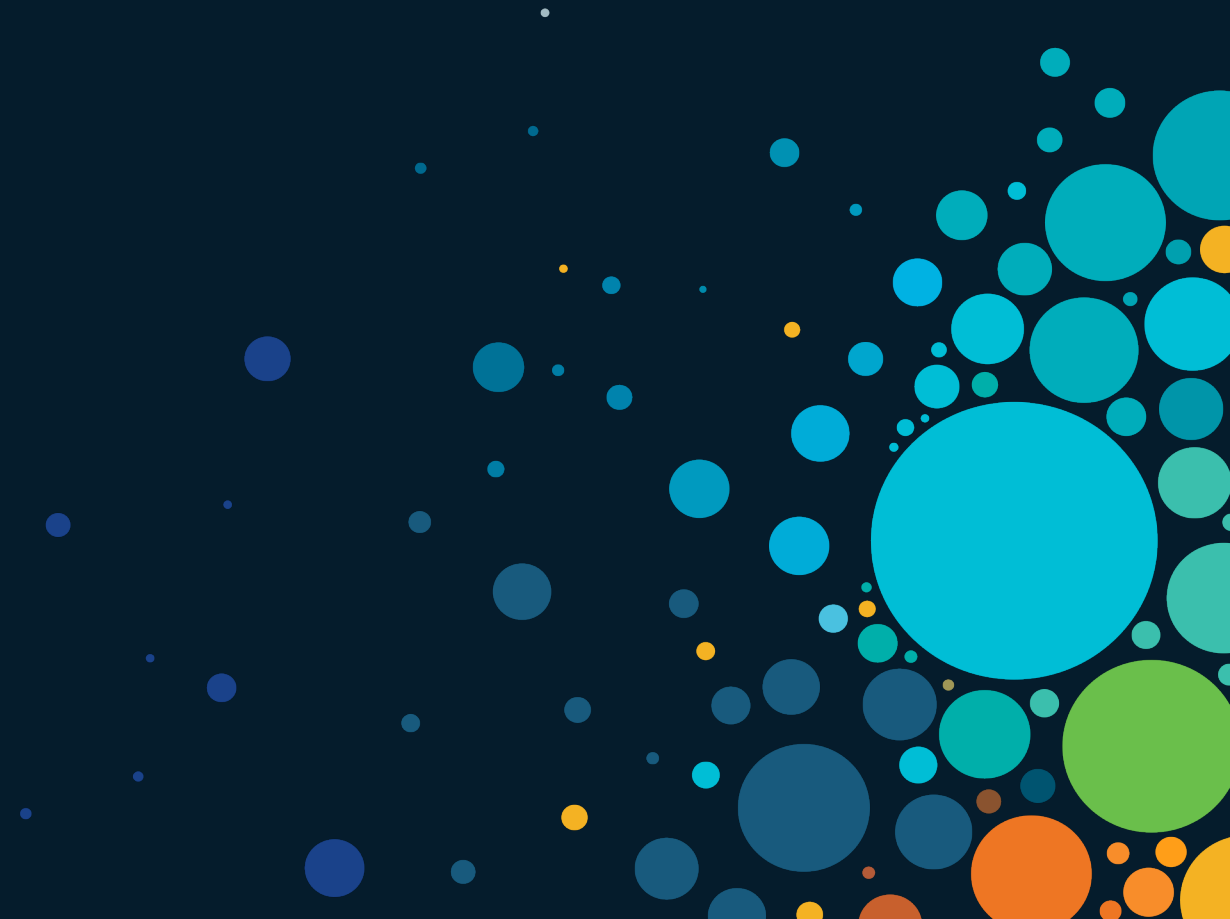


Faster to implement policy/ configuration changes



Less unplanned downtime

Solution Overview



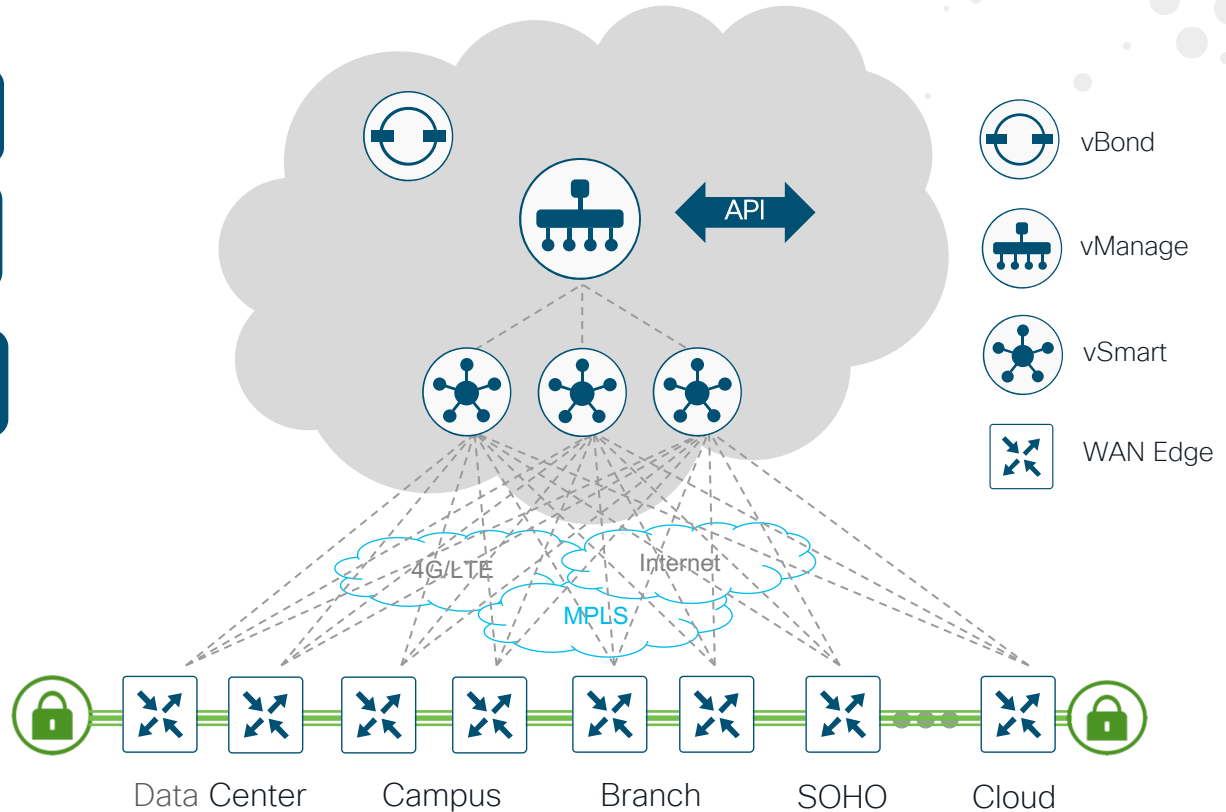
Cisco SD-WAN architecture overview

Orchestration = vBond

Management = vManage

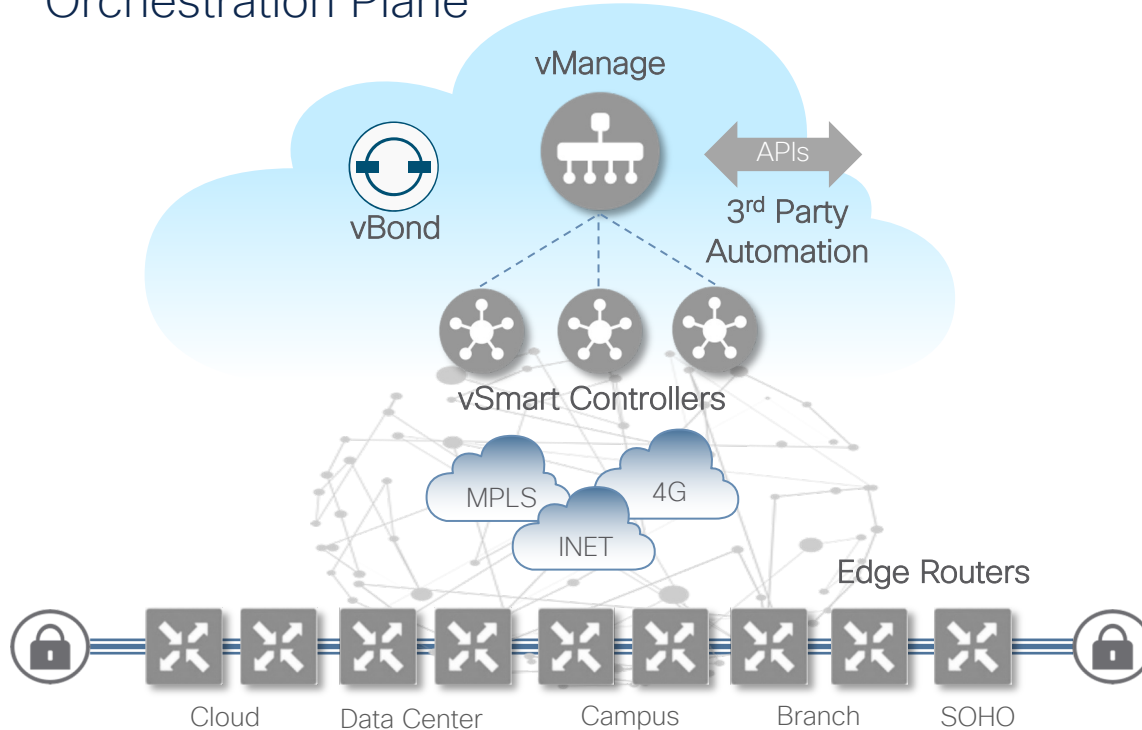
Control Plane = vSmart

Data Plane = WAN Edge



Cisco SD-WAN Solution Elements

Orchestration Plane



Orchestration Plane

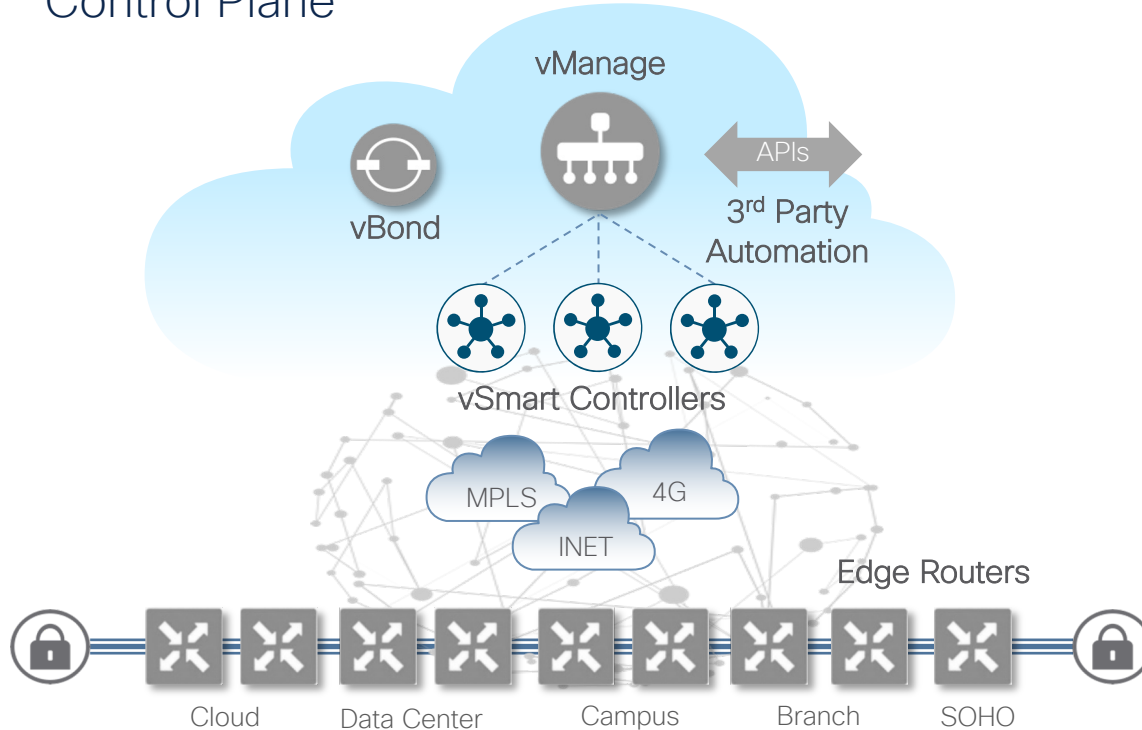


Cisco vBond

- Orchestrates control and management plane
- First point of authentication (white-list model)
- Distributes list of vSmarts/ vManage to all WAN Edge routers
- Facilitates NAT traversal
- Highly resilient

Cisco SD-WAN Solution Elements

Control Plane



Control Plane

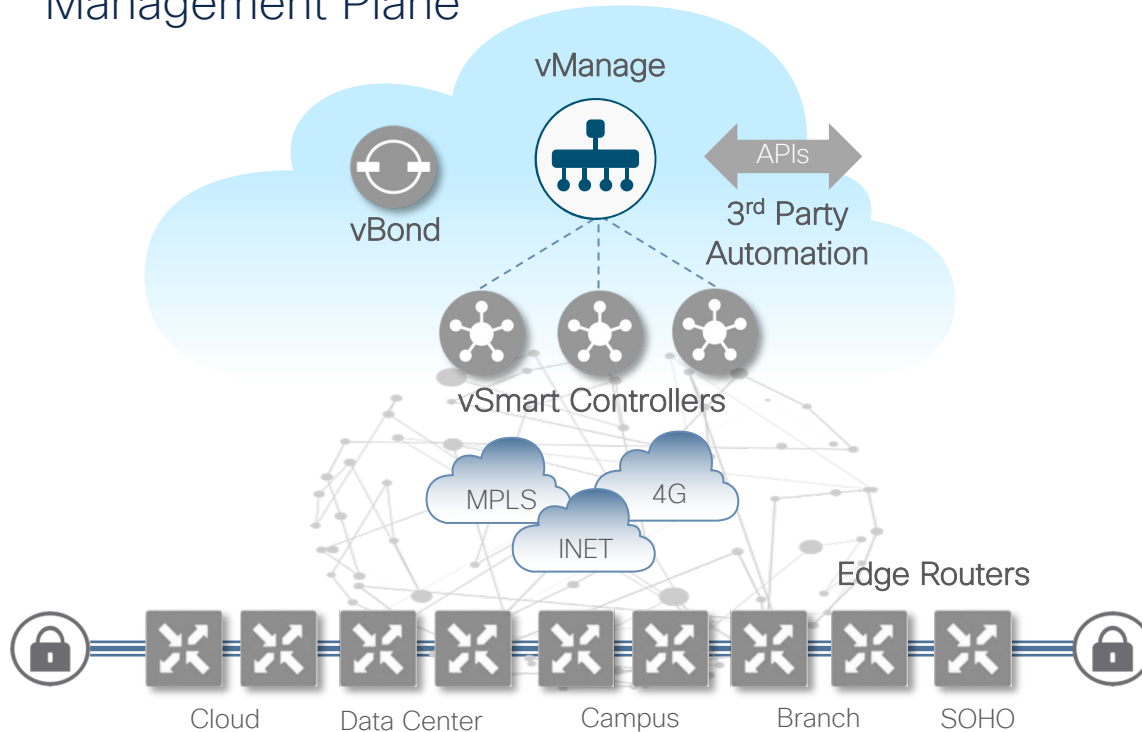


Cisco vSmart

- Facilitates fabric discovery
- Distributes control plane information between WAN Edges
- Distributes data plane and app-aware routing policies to the WAN Edge routers
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

Cisco SD-WAN Solution Elements

Management Plane



Management Plane

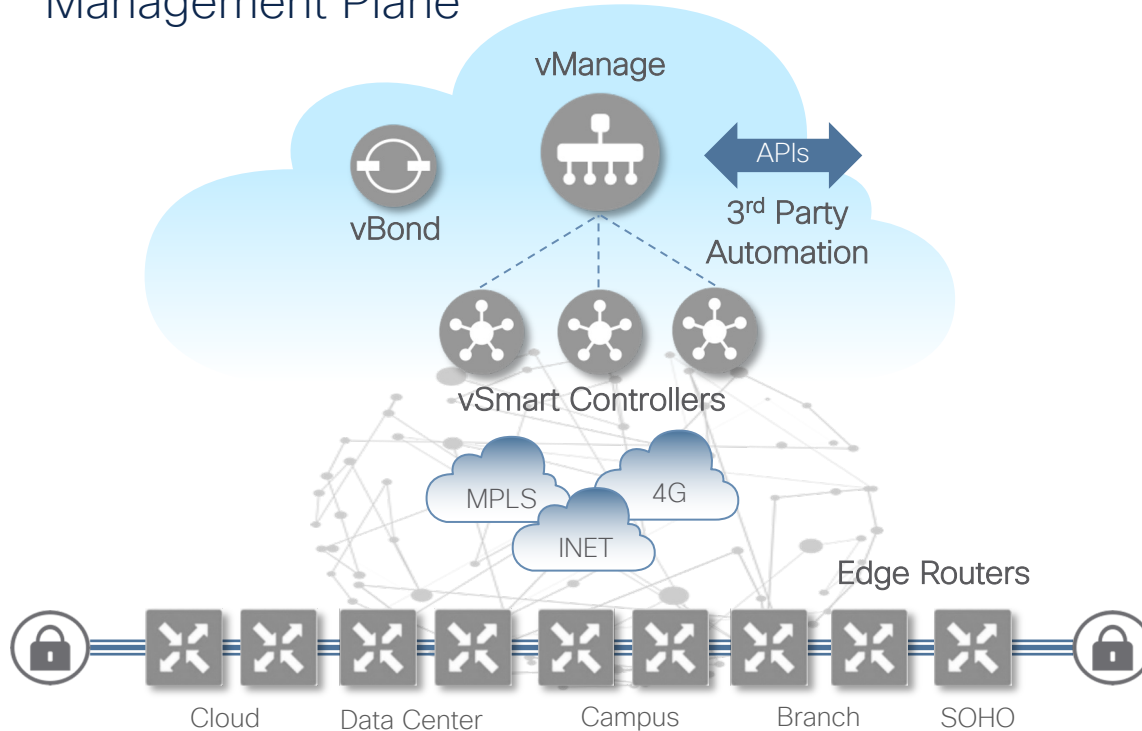


Cisco vManage

- Single pane of glass for Day0, Day1 and Day2 operations
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC
- Highly resilient

Cisco SD-WAN Solution Elements

Management Plane



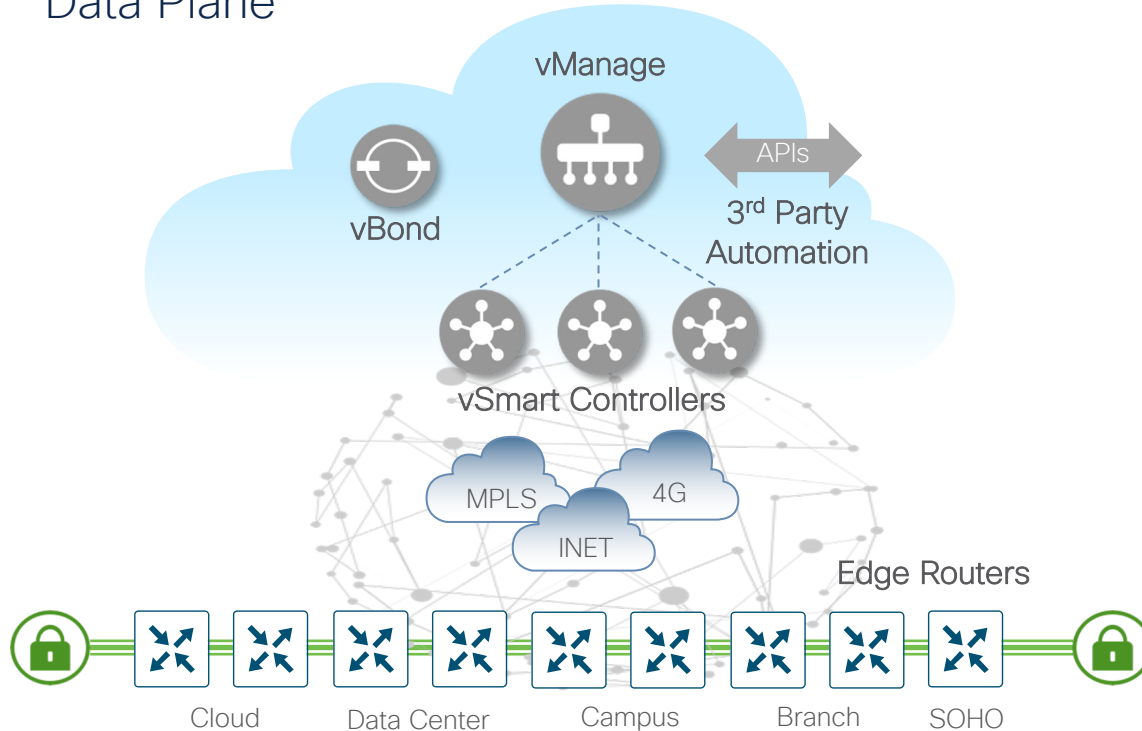
Management Plane



- Programmatic control over all aspects of vManage administration
- Secure HTTPS interface
- GET, PUT, POST, DELETE methods
- Python scripting

Cisco SD-WAN Solution Elements

Data Plane



Data Plane

Physical/Virtual

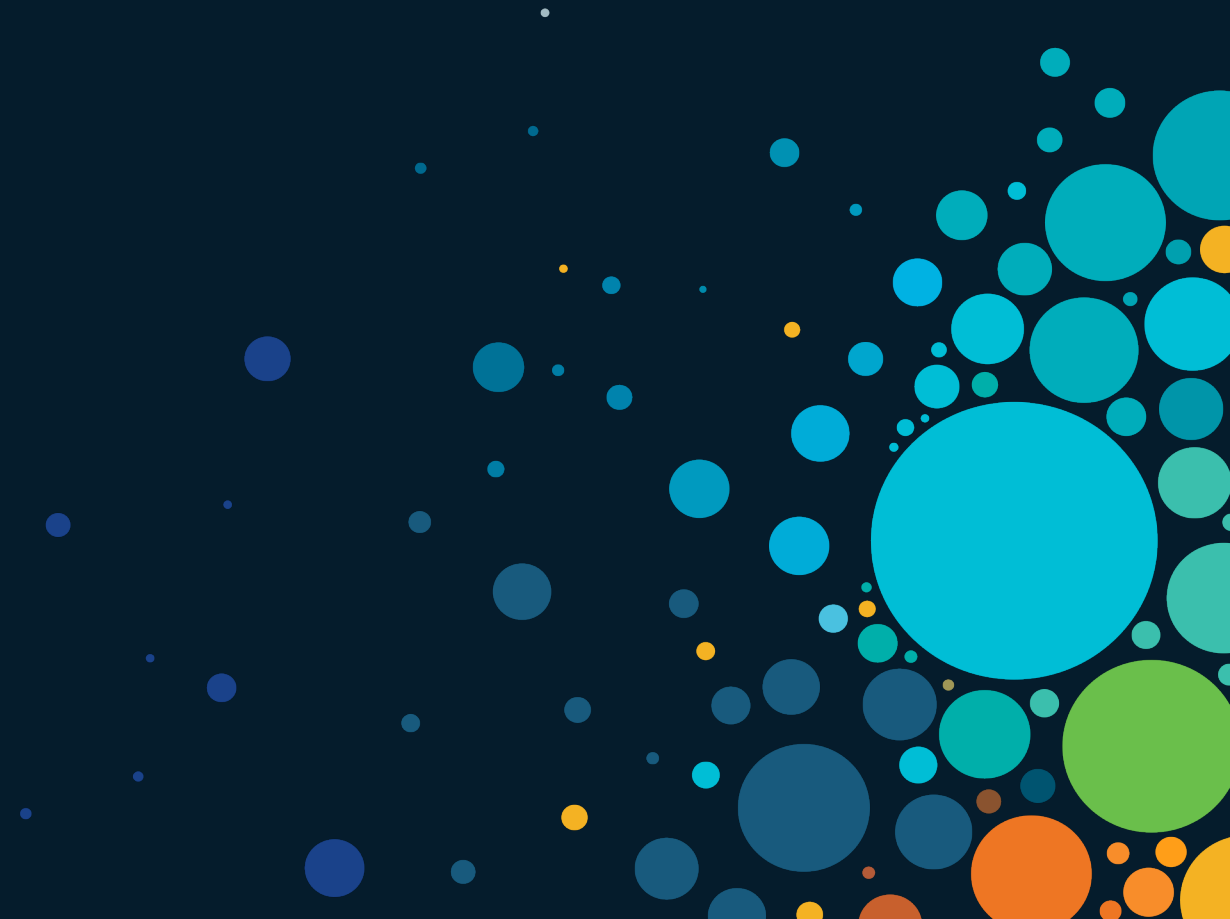


Cisco WAN Edge

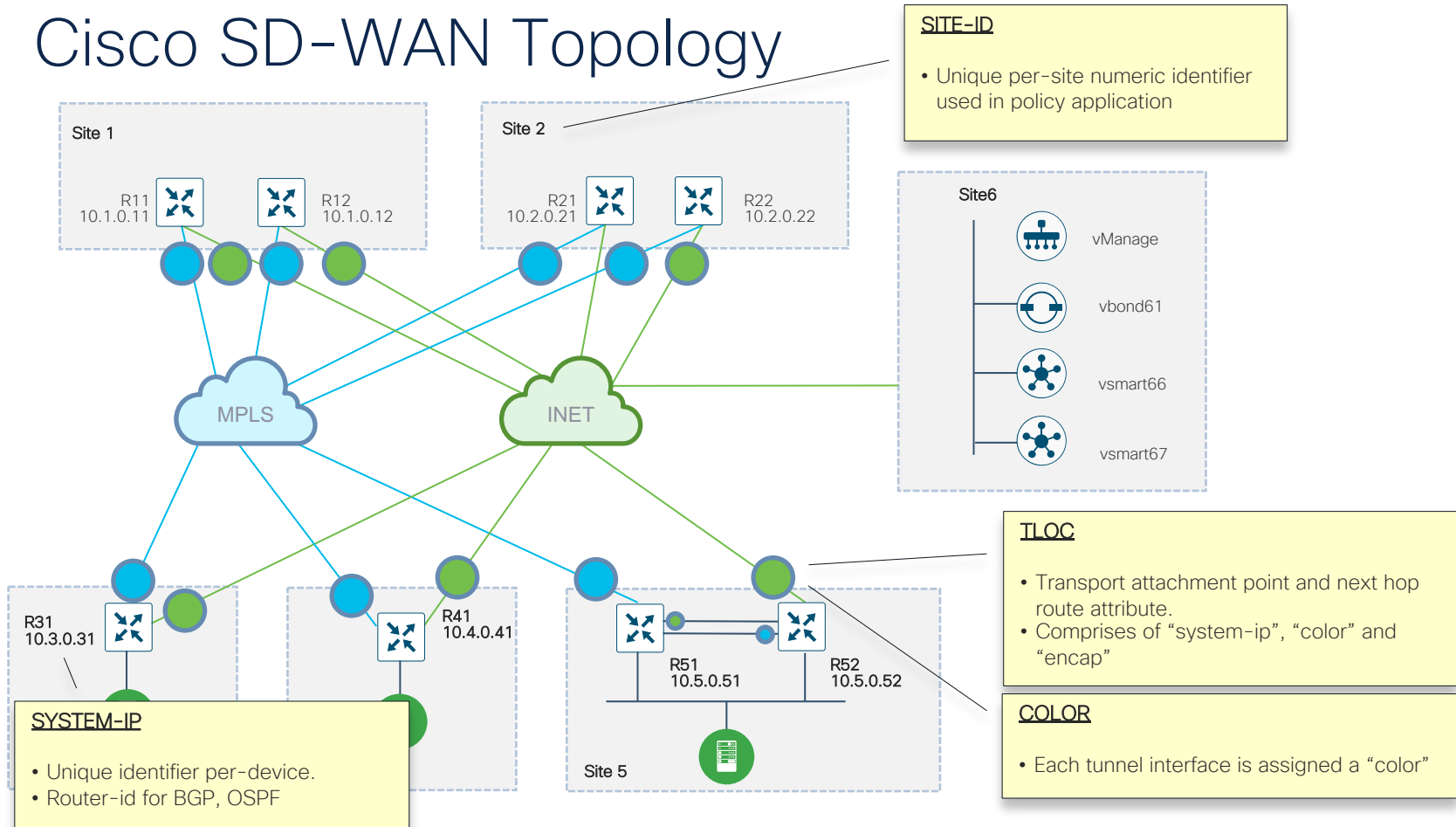
- Establishes secure control plane with vSmart controllers (OMP)
- Provides secure data plane with remote WAN Edge routers
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, EIGRP, BGP and VRRP
- Support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

vManage demo overview

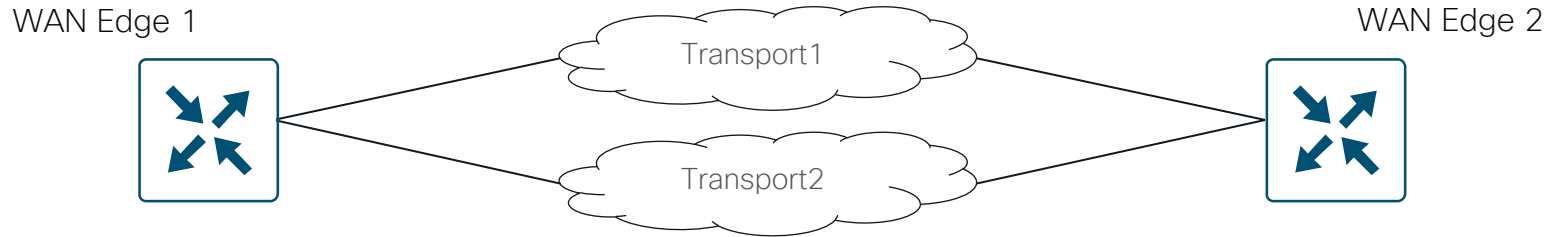
Fabric Operations



Cisco SD-WAN Topology

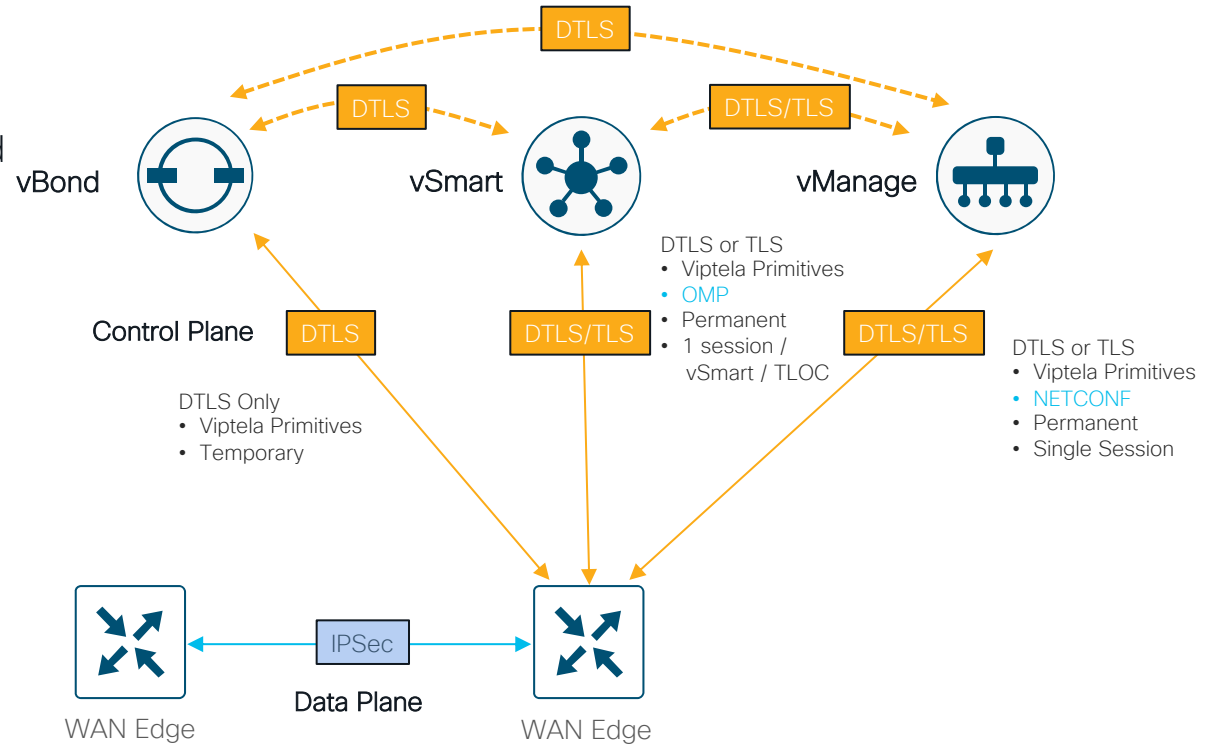


Fabric Operation



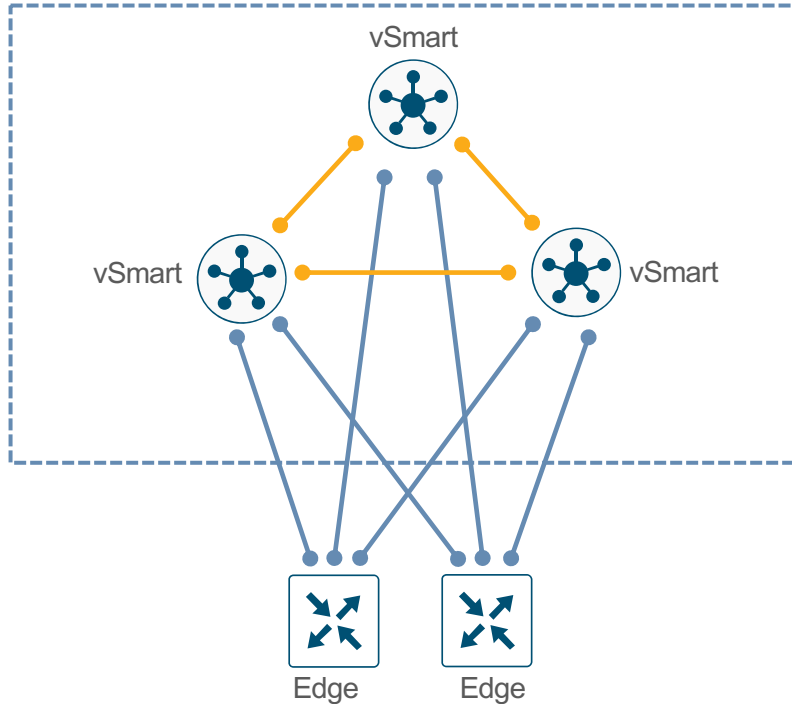
Control Plane Sessions

- **Control Connection** – authenticated and secured channel, operates over DTLS/TLS
- **OMP** – between Edge routers and vSmart controllers and between the vSmart controllers.
- **NETCONF** – Provisioning from vManage.



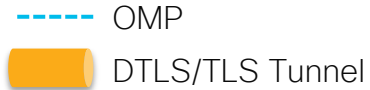
Overlay Management Protocol (OMP)

Unified Control Plane



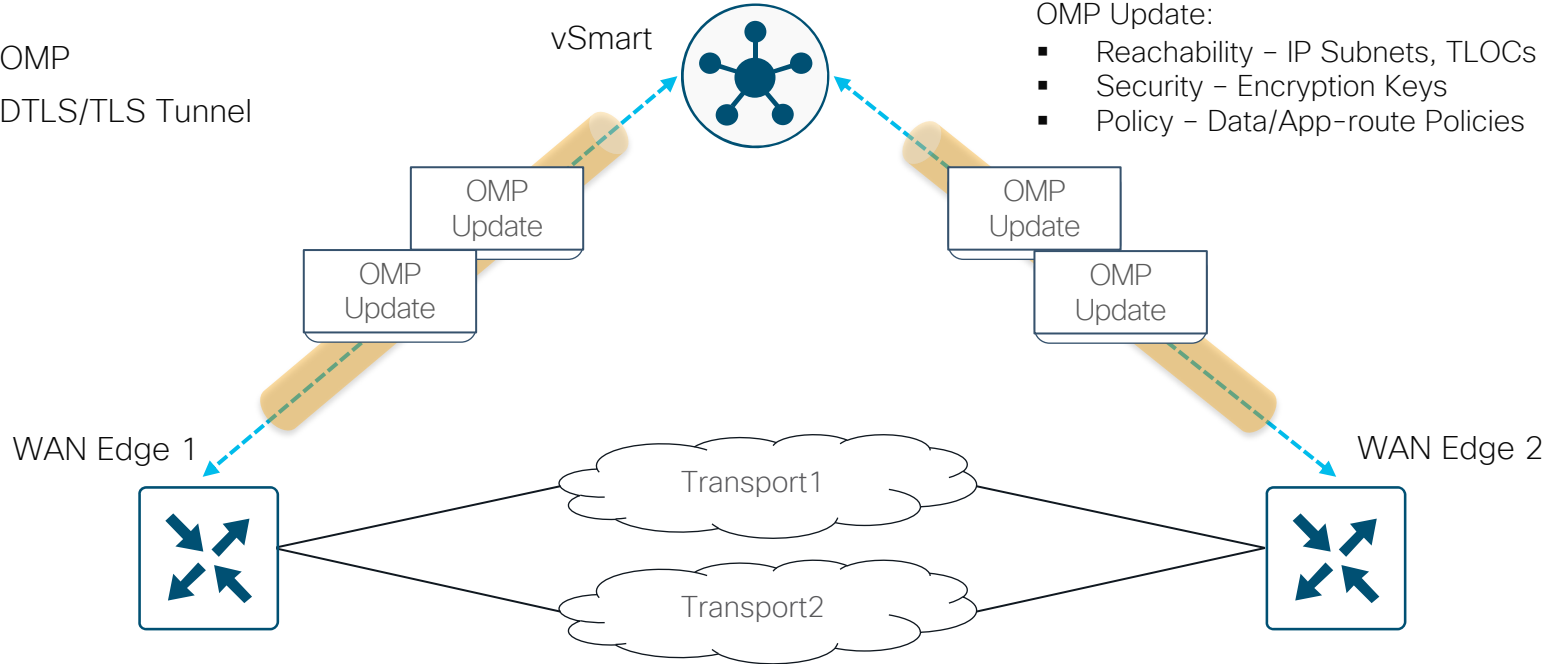
- TCP based extensible control plane protocol.
- Runs between Edge routers and vSmart controllers and between the vSmart controllers:
 - Inside TLS/DTLS connections.
- Leverages address families to advertise:
 - reachability for TLOCs,
 - unicast/multicast destinations (statically/dynamically learnt service side routes),
 - service routes (L4-L7)/service insertion
 - BFD stats (TE and H-SDWAN) and Cloud onRamp for SaaS probe stats (gateway)
- Distributes IPsec encryption keys, and data and app-aware policies.

Fabric Operation

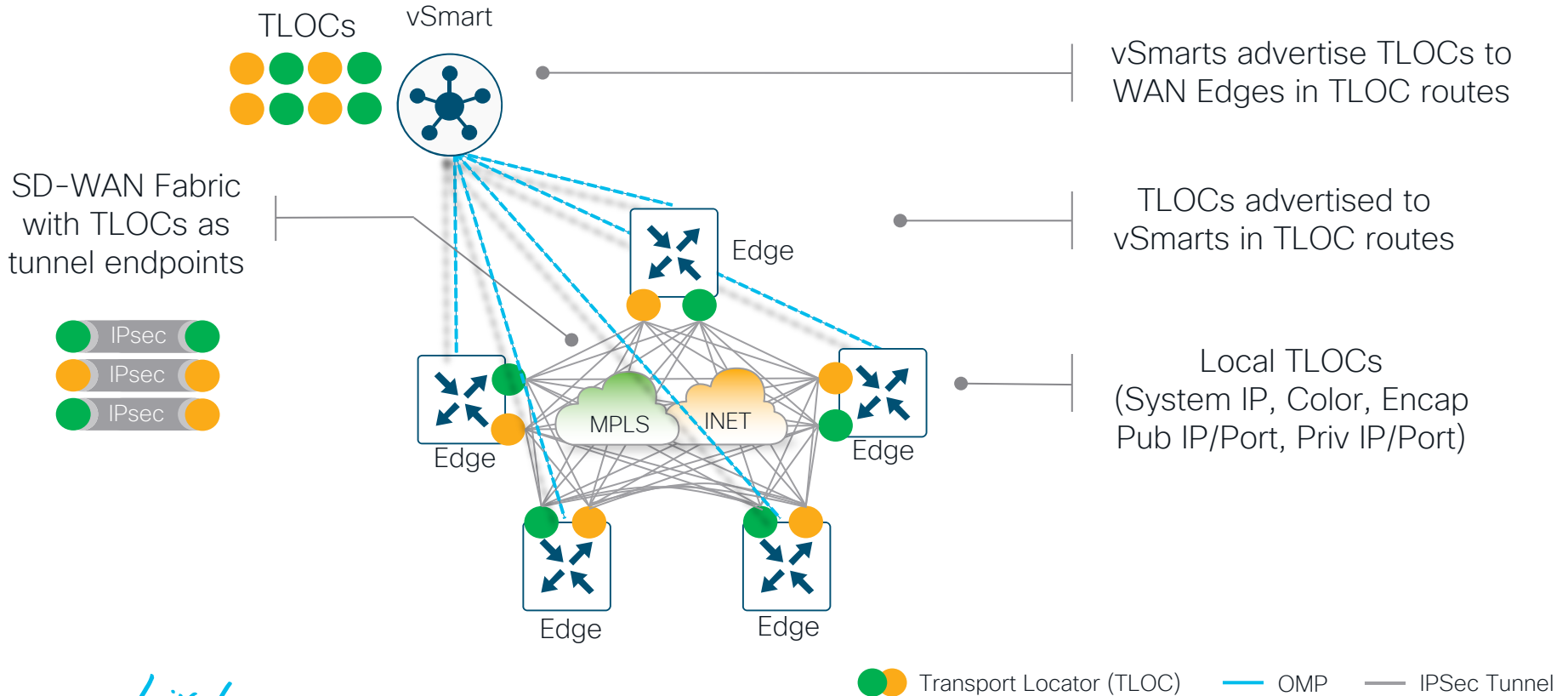


OMP Update:

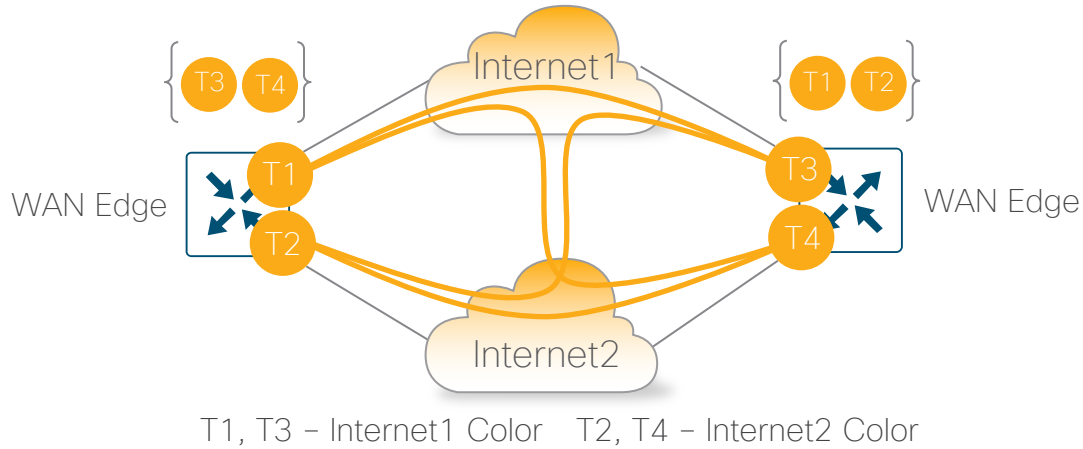
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies



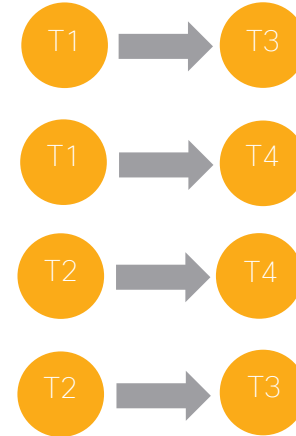
Transport Locators (TLOCs)



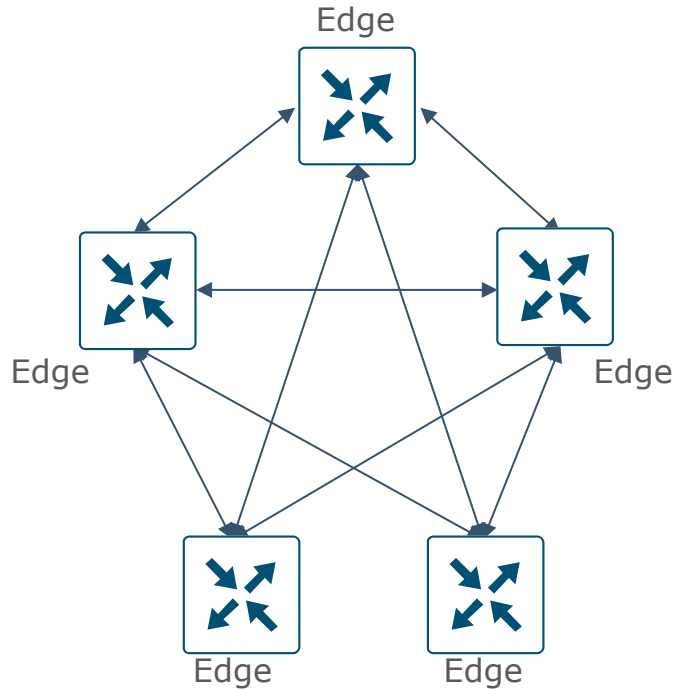
Transport Colors



We have a total of 4 IPSEC tunnels:



Bidirectional Forwarding Detection (BFD)



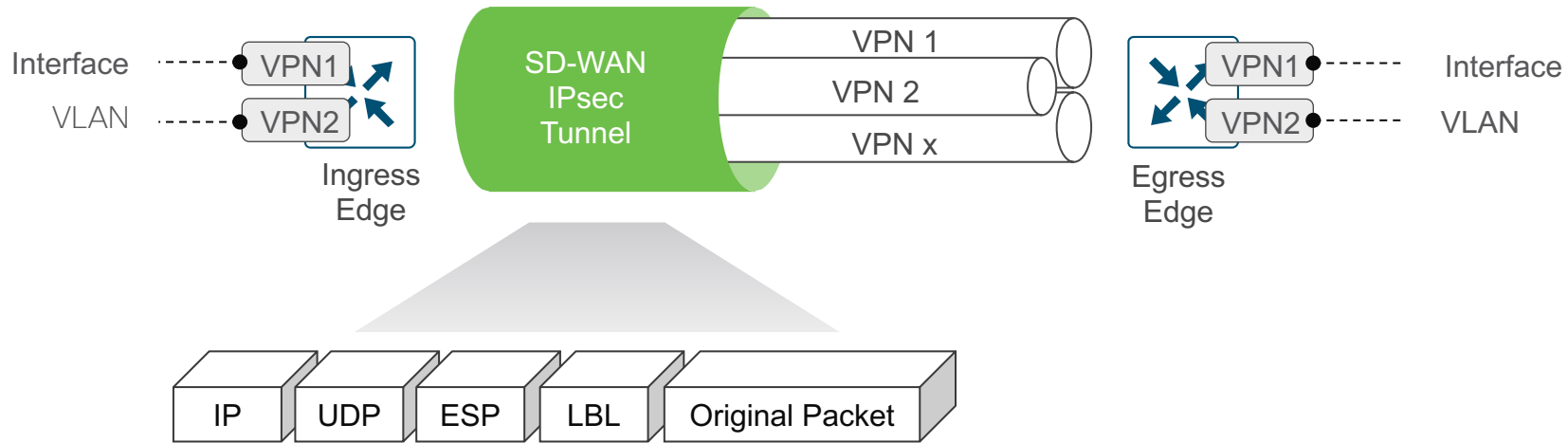
Path liveliness and quality measurement detection protocol:

- up/down
- loss/latency/jitter, IPsec tunnel MTU

Runs between all WAN Edge routers in the topology:

- Inside IPsec tunnels
- Automatically invoked after each IPsec tunnel establishment
- Cannot be disabled

End to End Segmentation



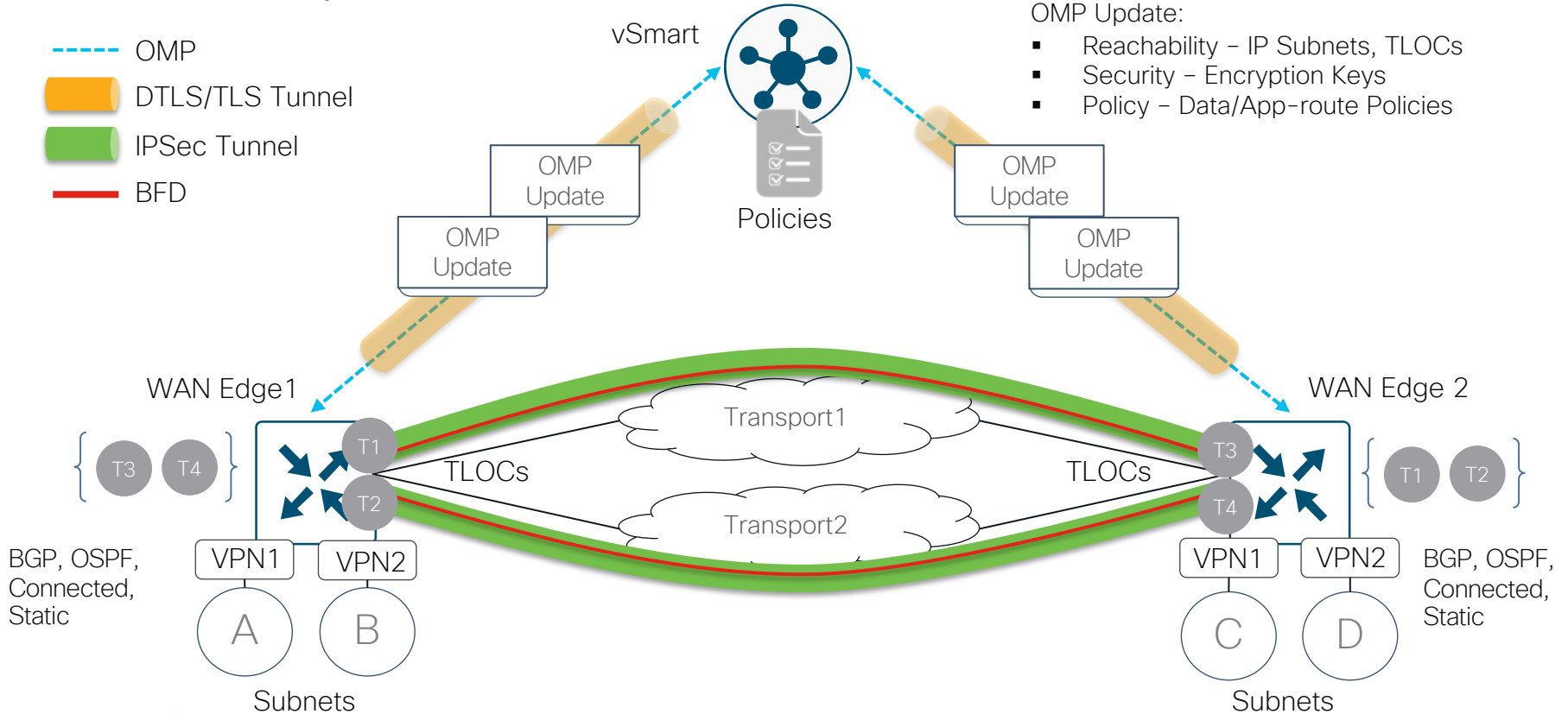
- Segment connectivity across fabric w/o reliance on underlay transport
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs
- WAN Edge routers maintain per-VPN routing table for complete control plane separation
- Labels are used to map packets into VPNs for complete data plane separation

Fabric Operation

- OMP
- DTLS/TLS Tunnel
- IPSec Tunnel
- BFD

OMP Update:

- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies





Fabric operation demo

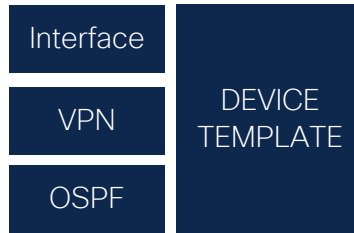
Edge configuration

Device configuration

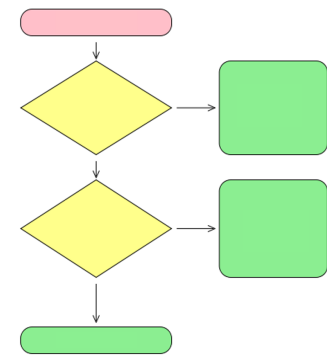
CLI Templates

```
interface GigabitEthernet5
no shutdown
arp timeout 1200
vrf forwarding 20
ip address 10.3.20.2 255.255.255.0
no ip redirects
ip mtu 1500
ip nbar protocol-discovery
load-interval 30
mtu 1500
negotiation auto
exit
```

Feature Templates



Configuration workflow

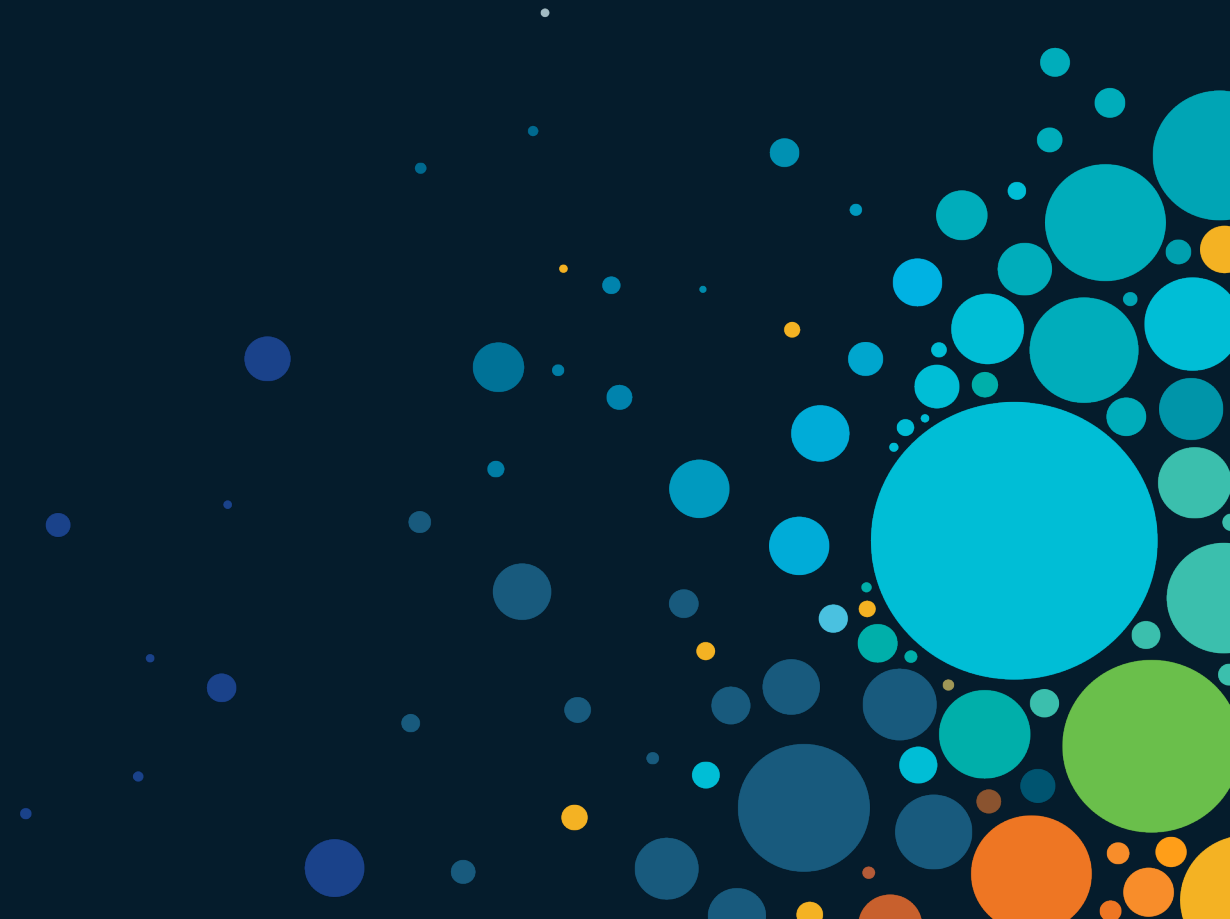


Bulk Device configuration provisioning using template variables

Enforcing of Device configuration consistency across the network

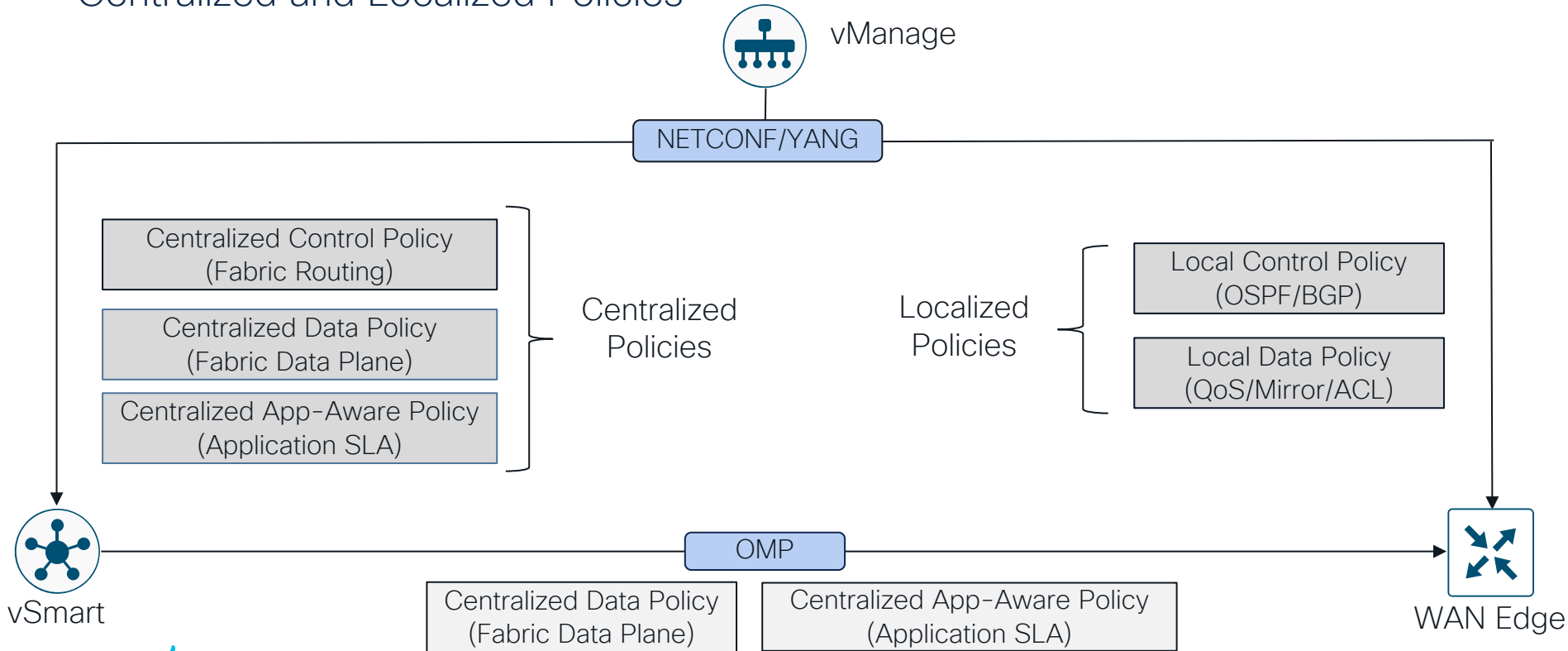
Central provisioning from vManage GUI

Policies

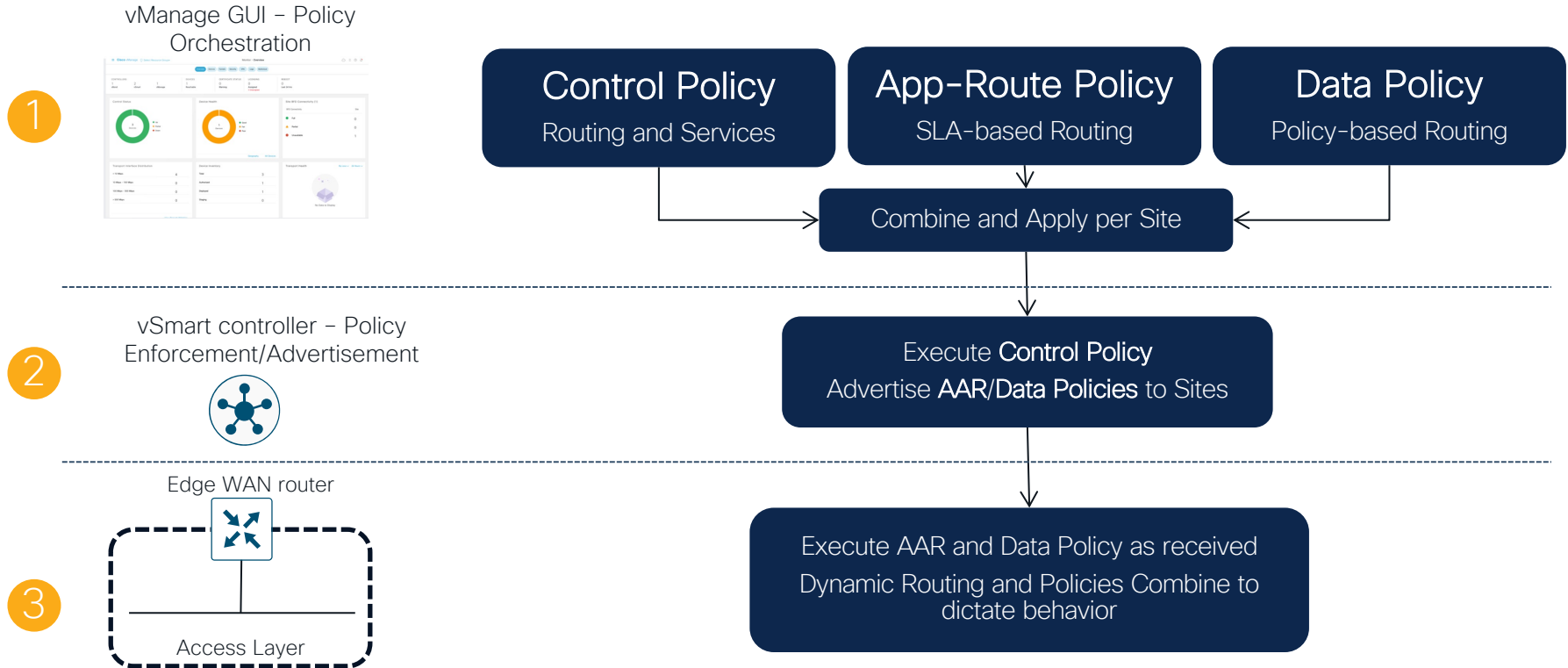


Policy Framework

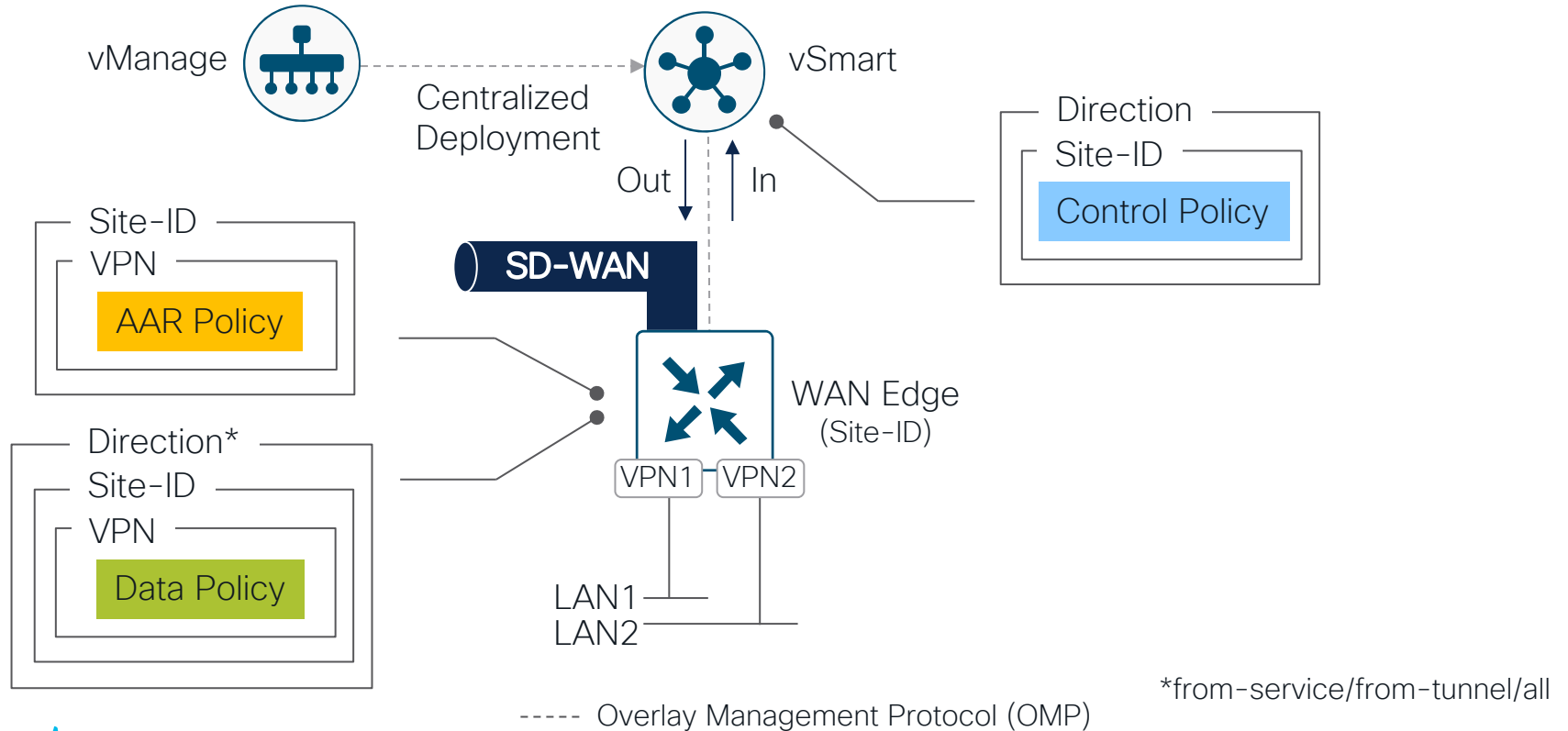
Centralized and Localized Policies



Centralized Policy Framework



Policy Deployment



vSmart Policy Construction

Lists

```
policy
  lists
    app-list social-media
      app facebook
      app twitter
    !
    prefix-list CORP
      ip-prefix 10.0.0.0/8
    !
    site-list eu-sites
      site-id 100-500
    !
    vpn-list internal-vpns
      vpn 1, 10-15
    !
  !
```

Policy Definition

```
policy
  policy-type <name>
    sequence <n>
      match <route|tloc|vpn|other>
      action <accept|reject|drop>
      set
        <attribute> <value>
      !
    sequence <n+1>
      <...>
    default-action <reject|accept>
  !
```

Policy Application

```
apply-policy
  site-list <name>
    control-policy <name>
  !
  site-list <name>
    data-policy <name>
    control-policy <name>
  !
  !
```

Centralized policy definition configured on vManage and enforced across entire network

vSmart Policy Example

```
apply-policy
  site-list EU-BRANCHES
  control-policy PREFER-EU-DC out
!
```

Apply the defined policy towards the sites in site-list

```
policy
  lists
    site-list EU-BRANCHES
      site-id 100-199
    site-list EU-DC
      site-id 200
!
```

Define the lists required for apply-policy and for use within the policy

```
control-policy PREFER-EU-DC
  sequence 10
  match route
    site-list EU-DC
  !
  action accept
  set
    preference 200
  !
  !
  !
  default-action accept
!
```

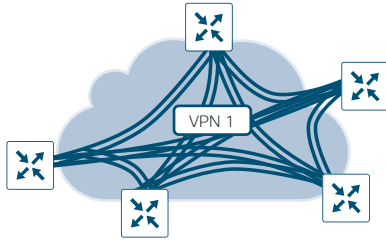
Define the actual policy to be applied

Lists previously defined used within policy

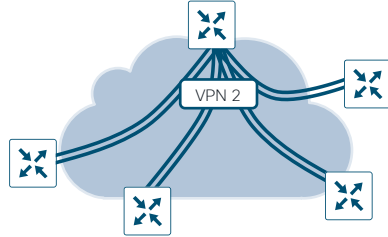
Note: Items listed as presented in node configuration. The order in which elements are configured should be lists, control-policy then apply-policy

Arbitrary VPN Topologies

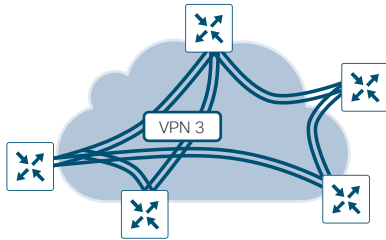
Full mesh



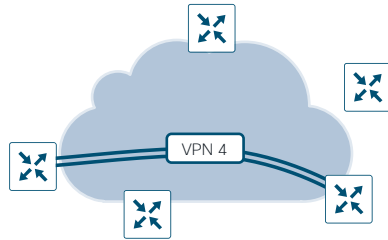
Hub and Spoke



Partial Mesh



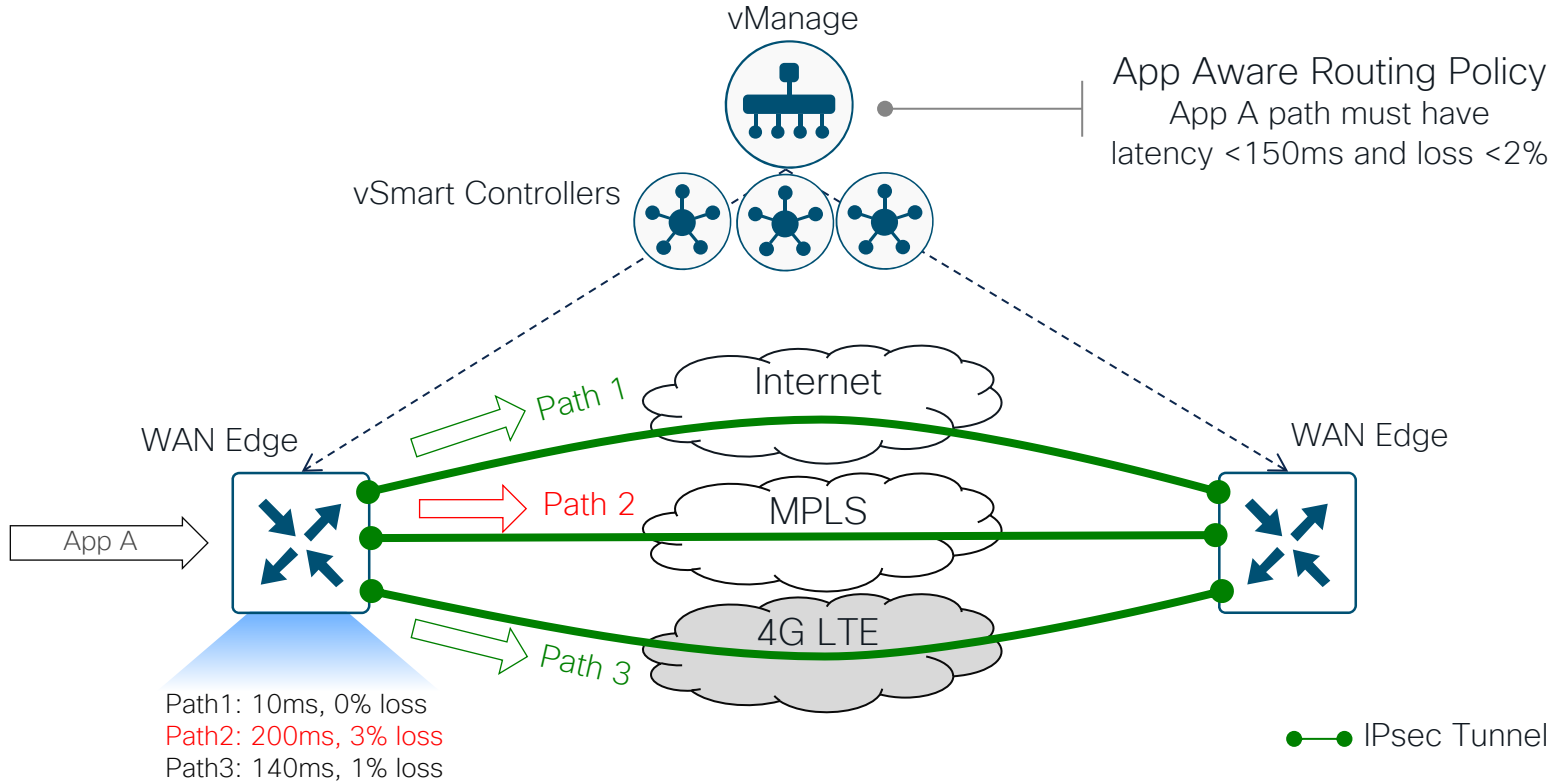
Point to Point



- Each VPN can have its own topology
 - Full-mesh, hub-and-spoke, partial-mesh, point-to-point, etc...
- VPN topology can be influenced by leveraging control policies
 - Filtering TLOCs or modifying next-hop TLOC attribute for OMP routes
- Applications can benefit from shortest path, e.g. voice takes full-mesh topology
- Security compliance can benefit from controlled connectivity topology, e.g. PCI data takes hub-and-spoke topology

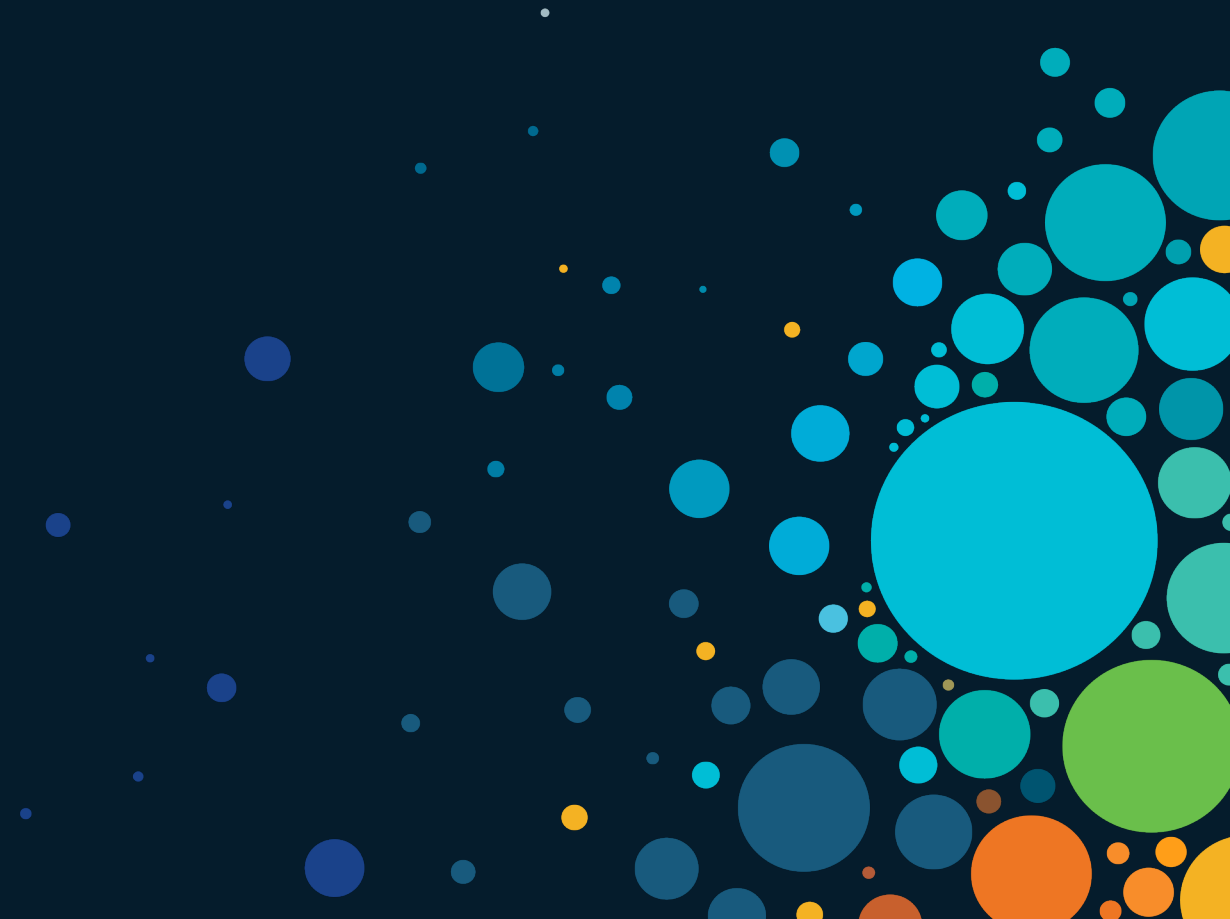
Critical Applications SLA

Application Aware Routing

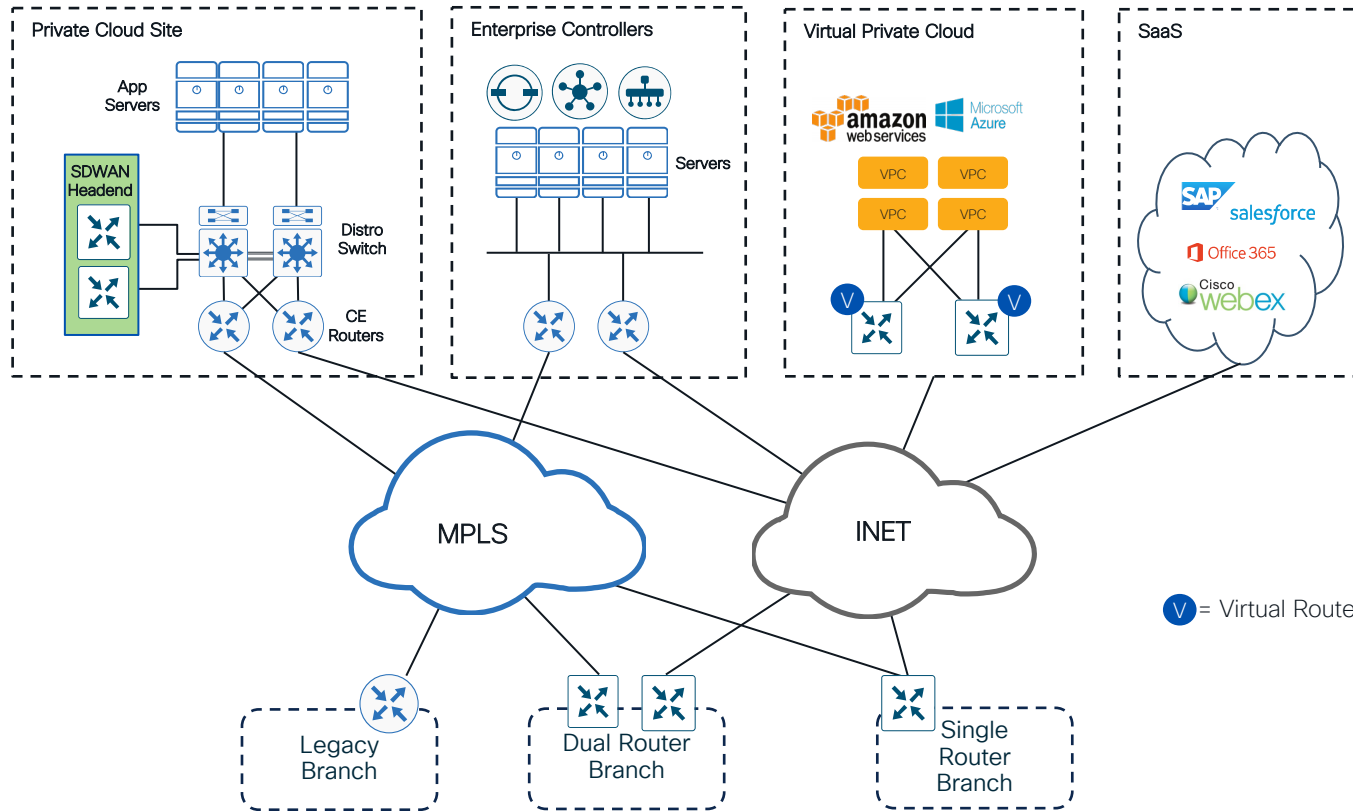


Policies demo

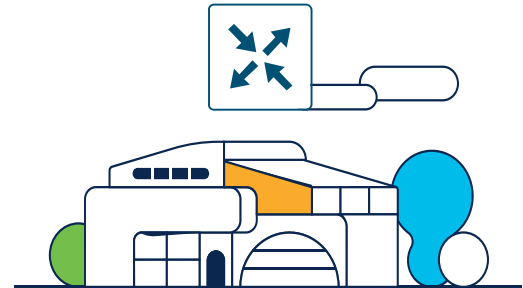
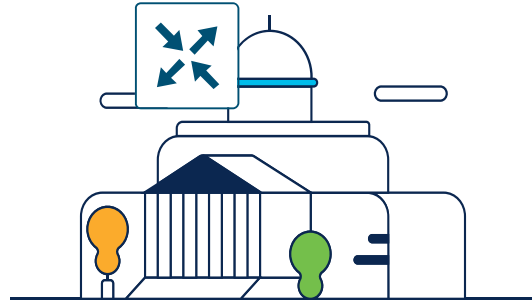
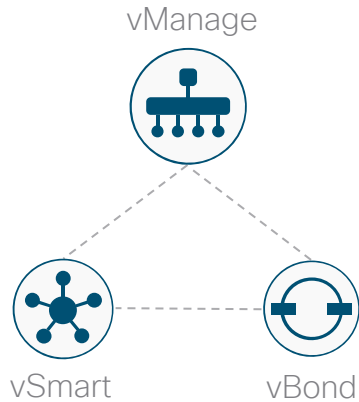
SD-WAN Deployment Strategy



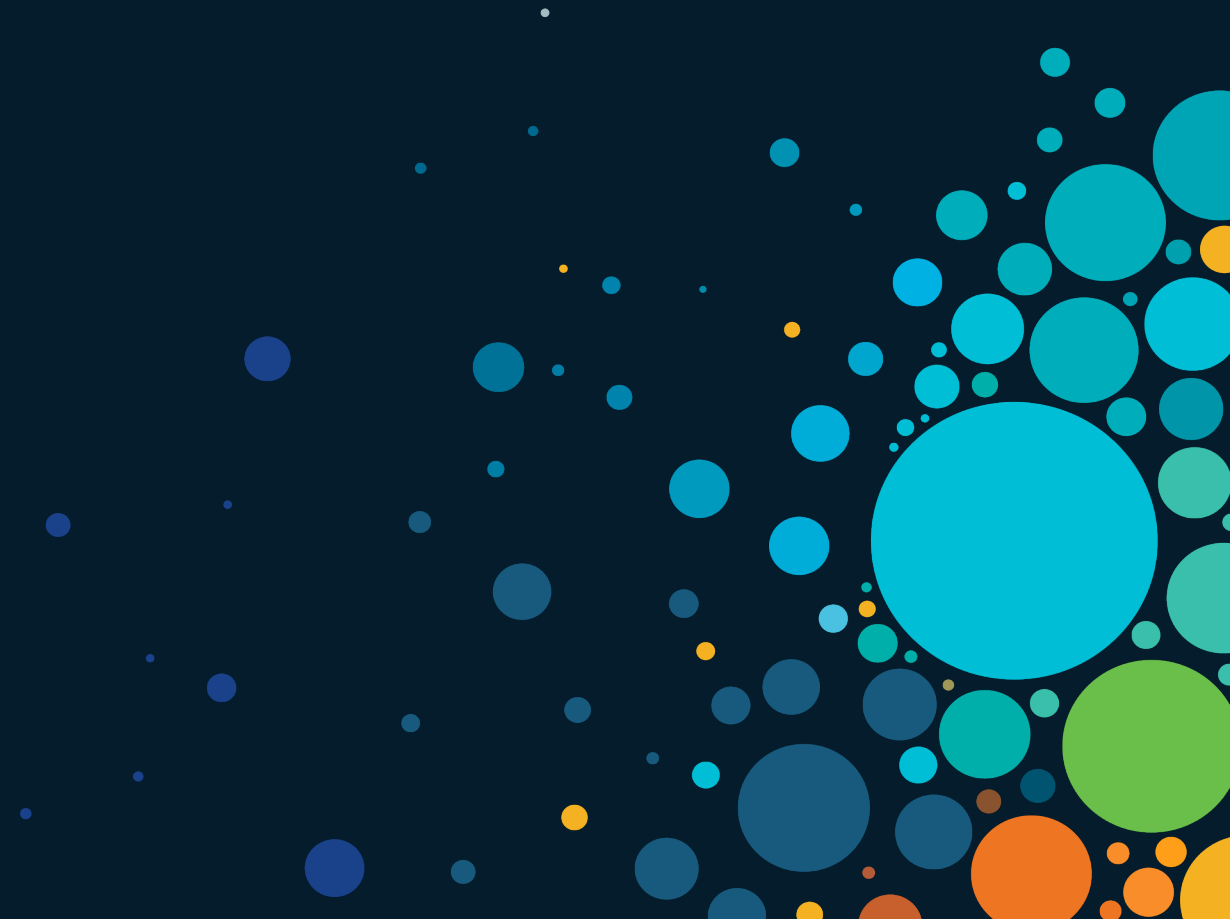
Typical SD-WAN Deployment Architecture



Deployment/Migration Sequence



Controllers



SD-WAN Controllers

Cisco Cloud Hosted

vBond vManage vSmart

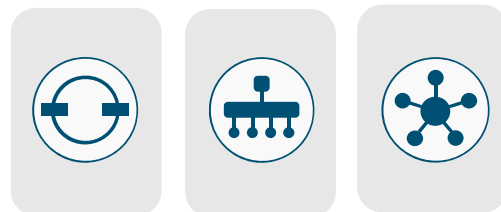


Public Cloud



On-Premises

vBond vManage vSmart



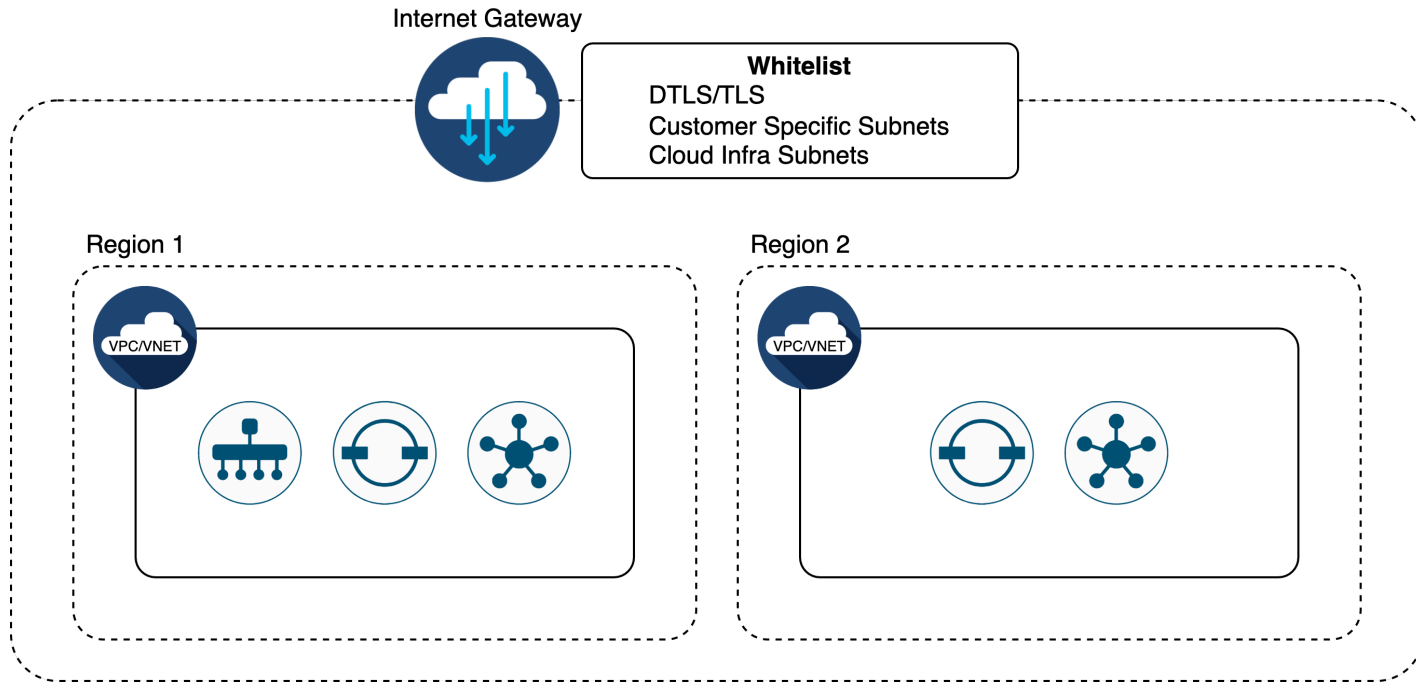
ESXi or KVM



Physical Server

Cloud-Hosted Controllers

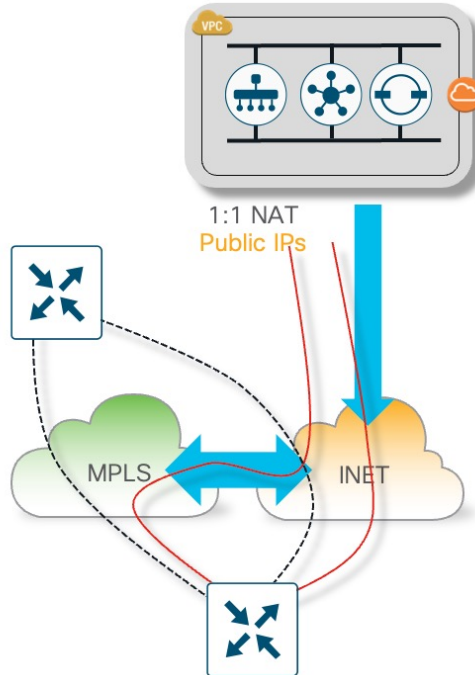
High-Level Design



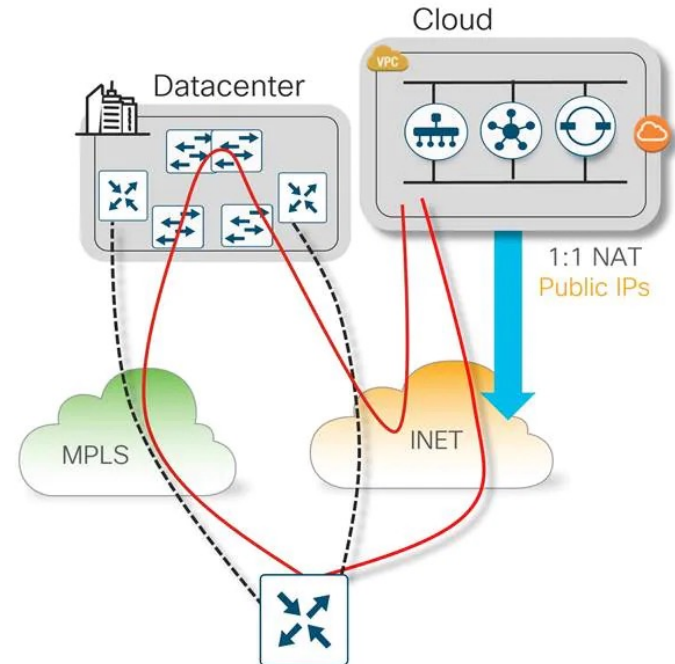
Cloud-Hosted Controllers

Reachability

MPLS Breakout by SP



Via Multihomed Datacenter

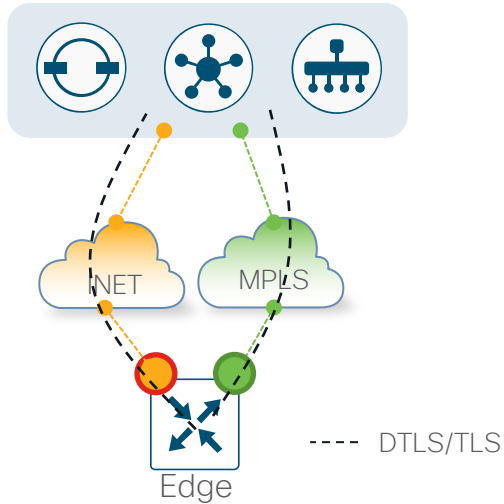


----- Data Plane
----- Control Plane

Cloud-Hosted Controllers

Reachability

Internet and MPLS



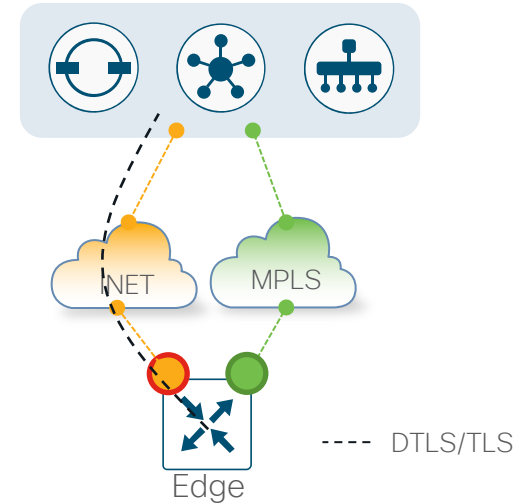
Maximum Control Connections



Maximum Control Connections



Only Internet



Maximum Control Connections



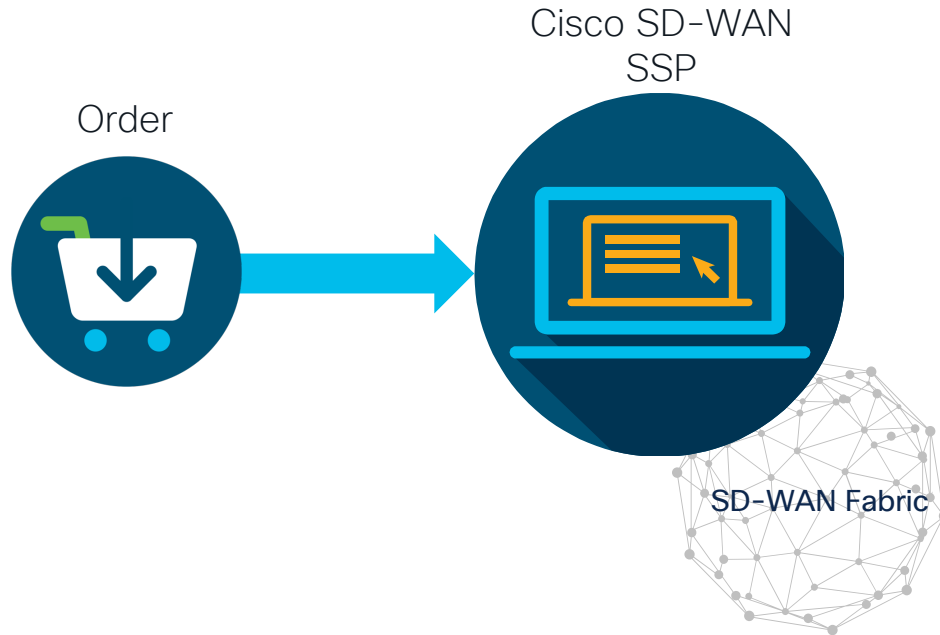
Maximum Control Connections



0

Cloud-Hosted Controllers

Self-Service Portal



Controller Lifecycle Mgmt:

- Cloud Provider selection
- Region selection



Deployment Accelerator:

- No delay in provisioning
- Simple day 0 cloud operation



Visibility:

- Cloud infra monitoring & auditing
- Holistic device status



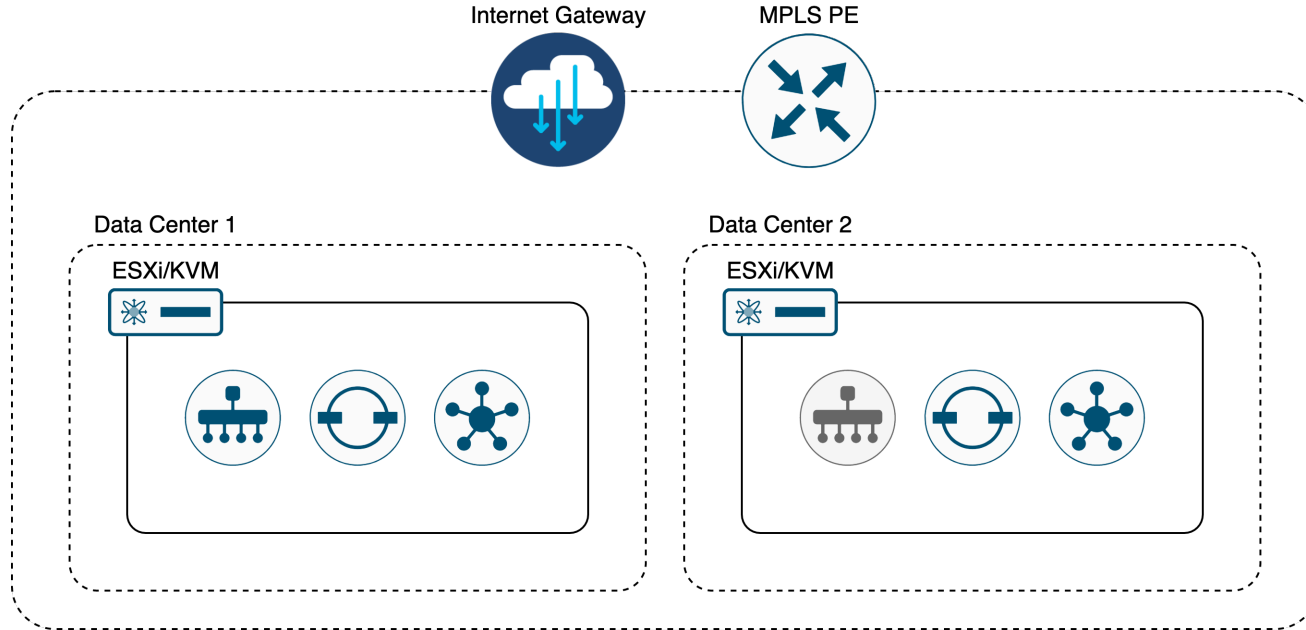
Operation Services:

- Whitelist updates
- Backup

Self-Service Portal Demo

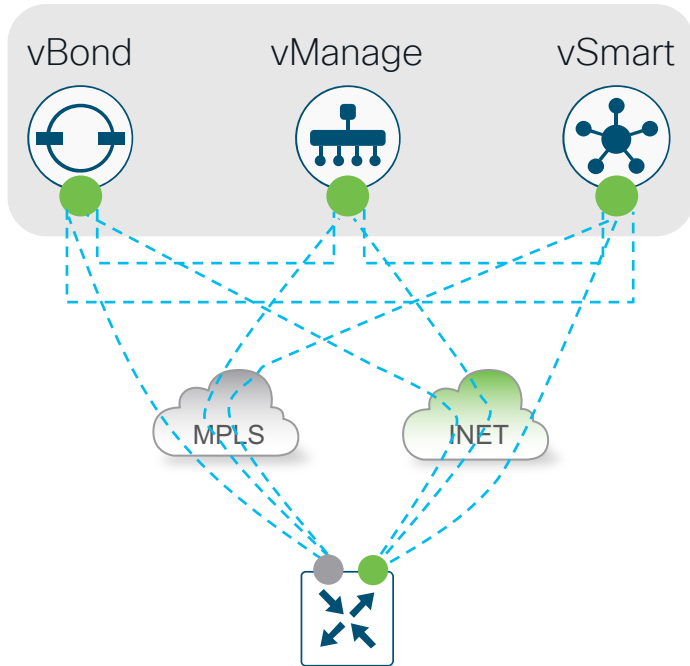
On-Prem Controllers

High-Level Design



On-Prem Controllers

Low-Level Design with Public IPs



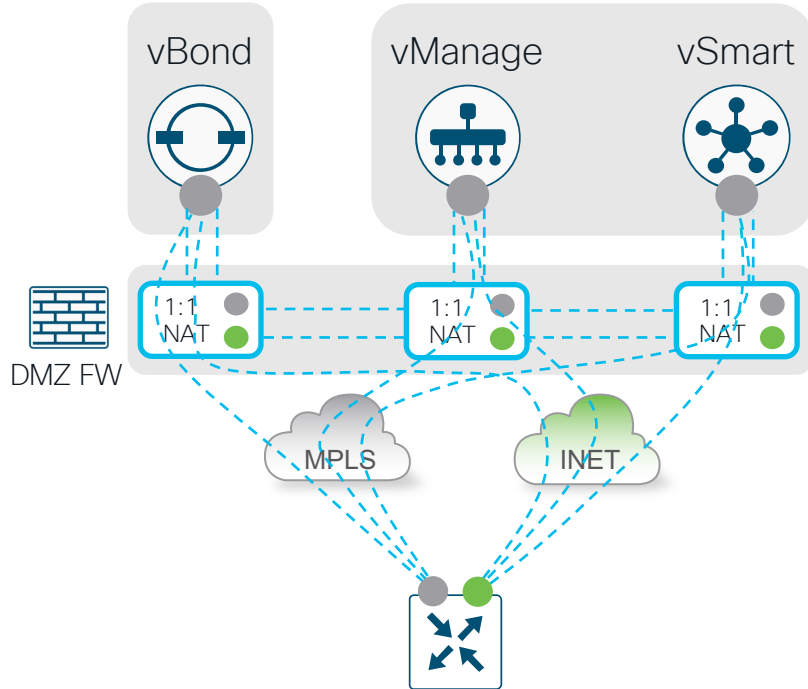
All control connections built using controllers' public IPs

Controllers' public IPs advertised to all transports

- Public IP
- Private IP

On-Prem Controllers

Low-Level Design with 1:1 NAT



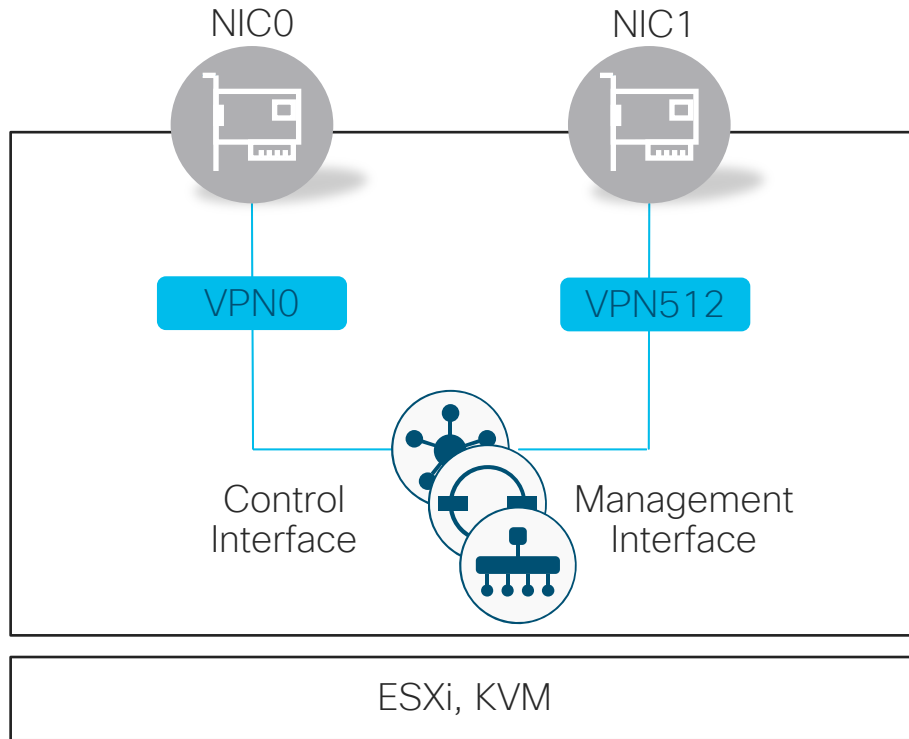
All control connections built using controllers' NATed IPs

Controllers' NATed IPs advertised to all transports

- Public IP
- Private IP

On-Prem Controllers

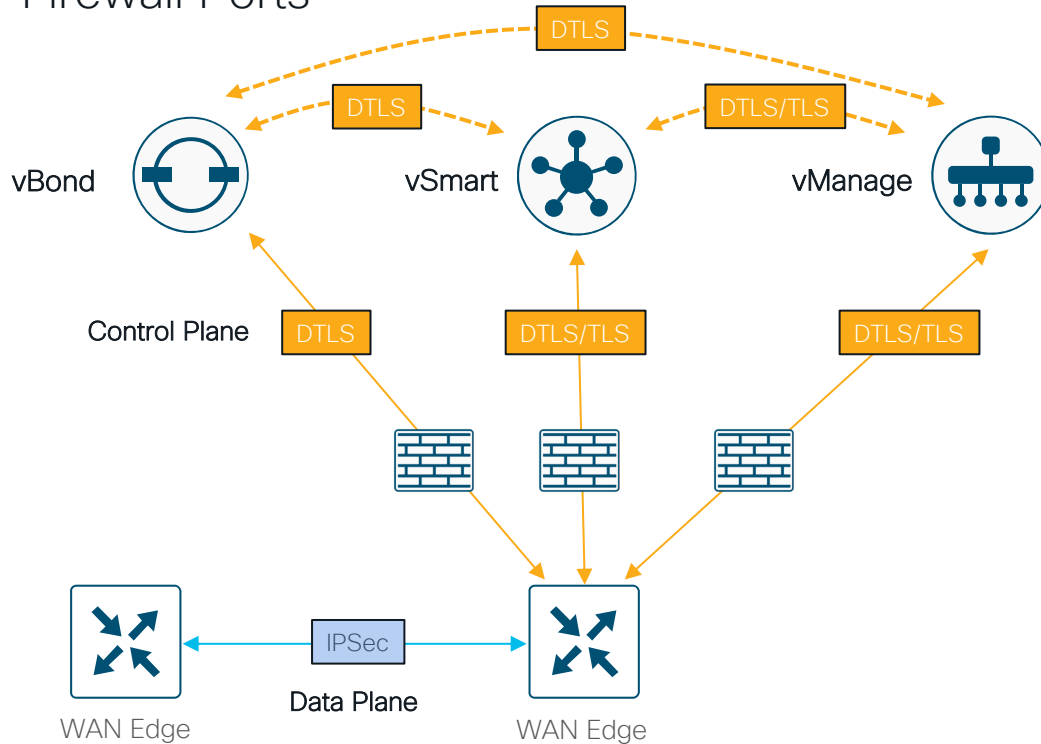
Controllers deployment



- 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

On-Prem Controllers

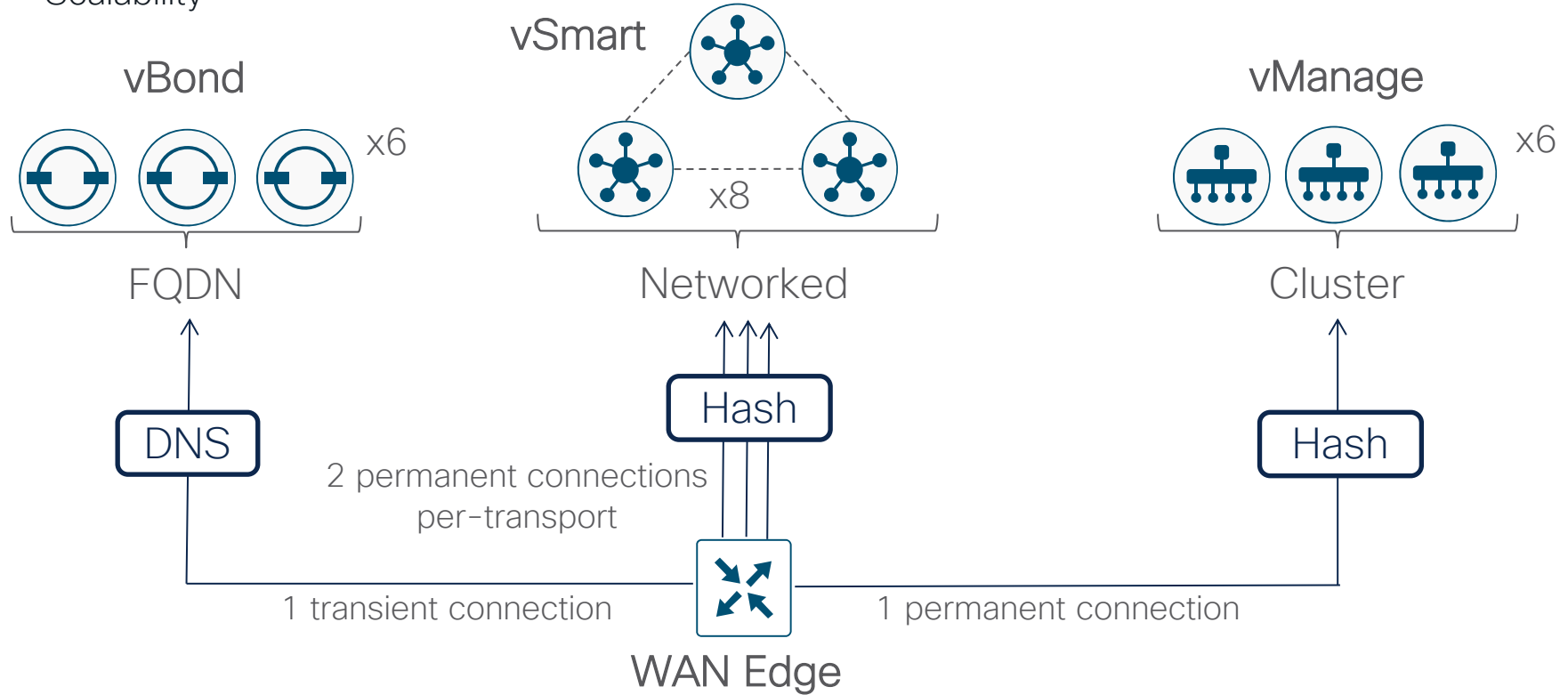
Firewall Ports



- If Firewall is present, remember to open respective ports to allow control connections.
- All required ports are documented in the [Firewall Port Considerations](#) document.

Controllers

Scalability



SD-WAN Controller Redundancy

Controllers Failure



Same Principles Apply for Cloud and On-Prem

All vBonds Fail



- New or rebooted edge devices will be able to join the overlay
- Edge devices continues forwarding traffic and updating routes

All vSmarts Fail



- No updates for routing table
- Edge devices continues forwarding traffic with the last known routes

All vManages Fail



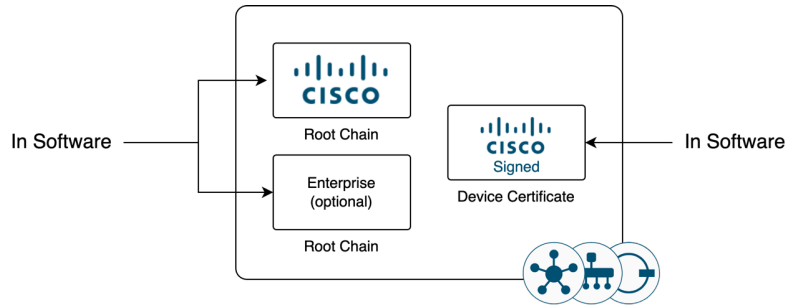
- No possible to monitor devices, change configuration or policies from the UI
- Edge devices continues forwarding traffic and updating routes



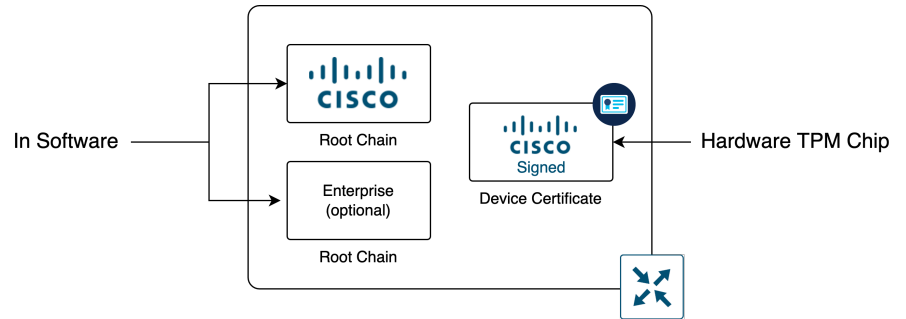
Controllers compatibility & recommendations

Certificates present for authentication purposes

Controllers' Identity

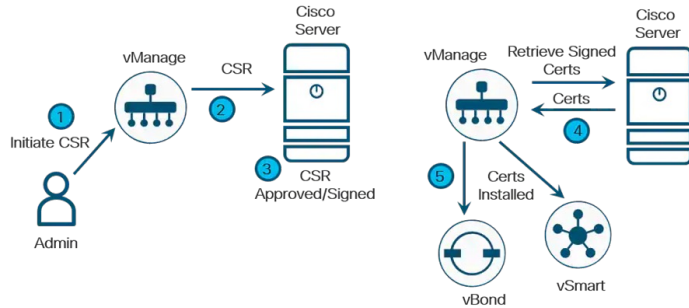


Routers' Identity



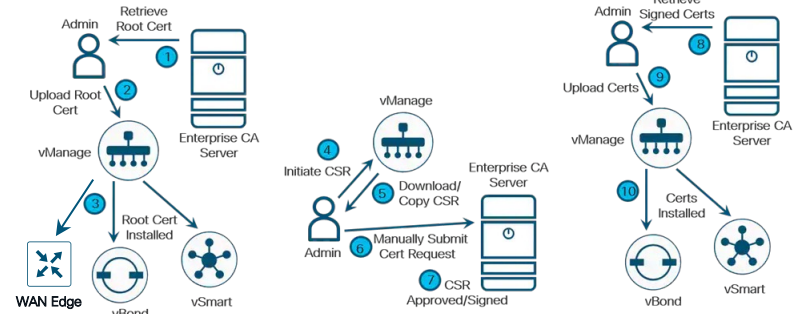
Controllers' Certificates Signing Process

Cisco PKI (recommended)

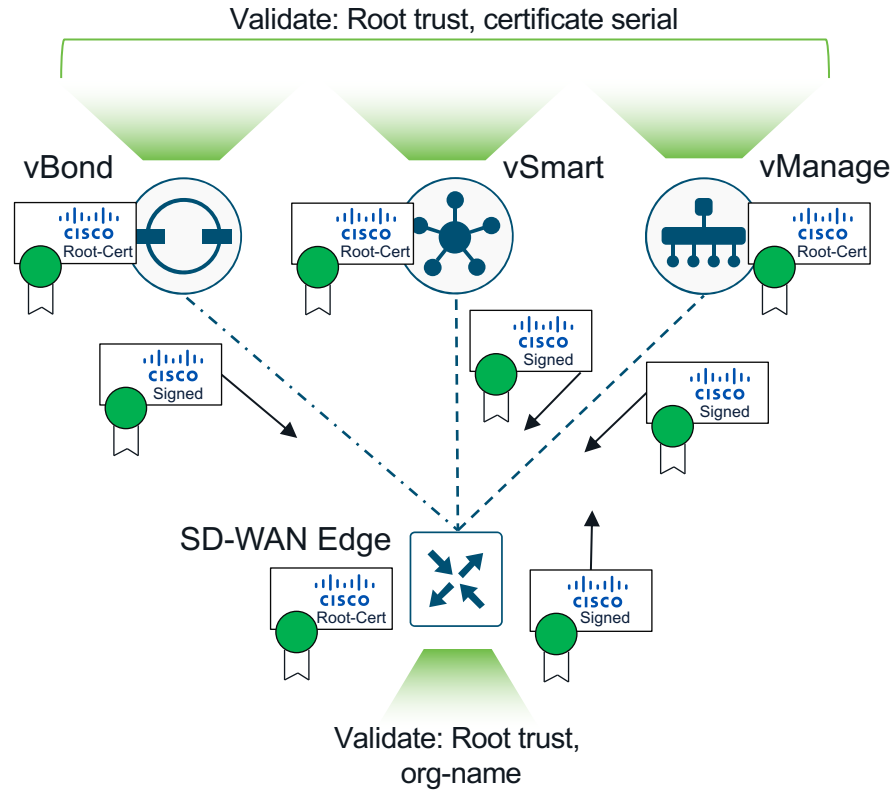


Fully automated from vManage

Enterprise CA

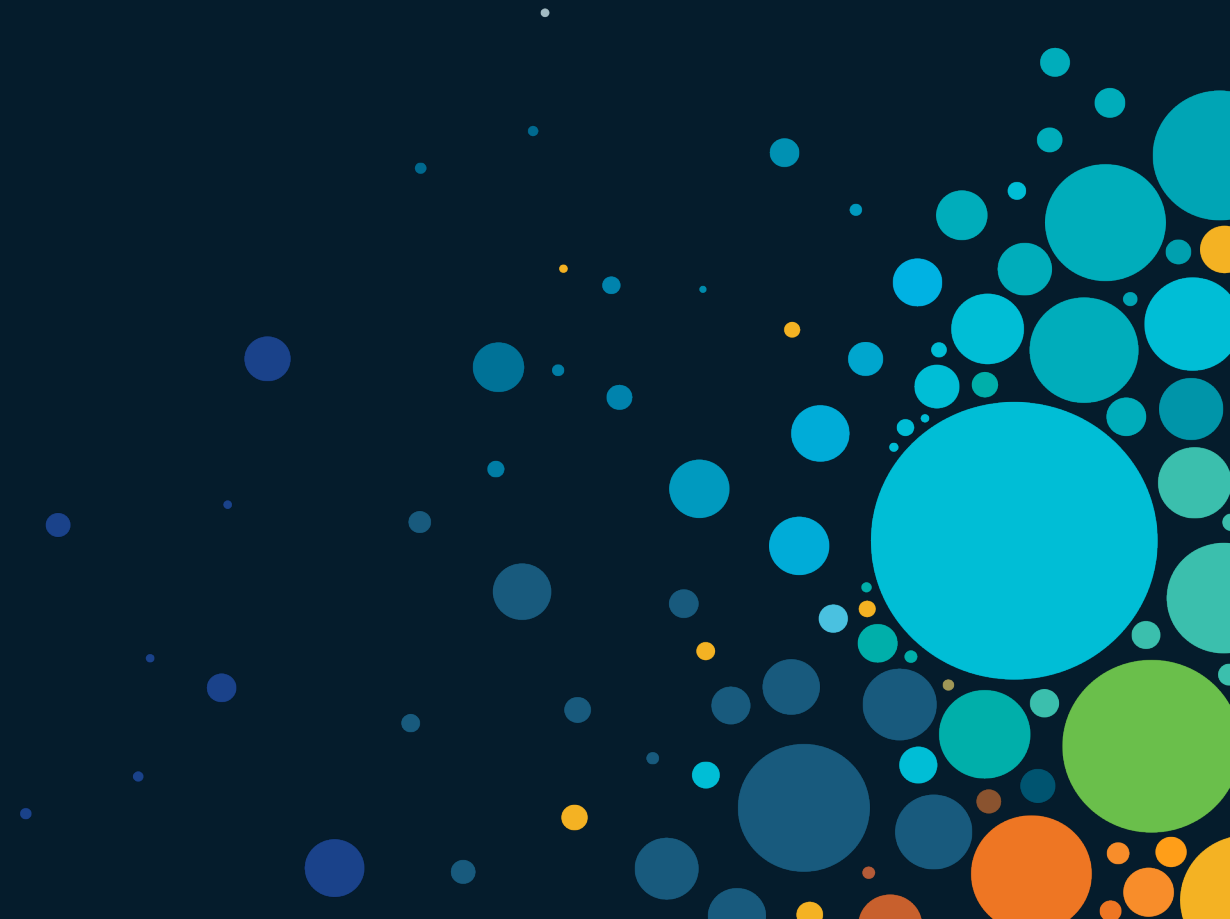


Control Plane Authentication

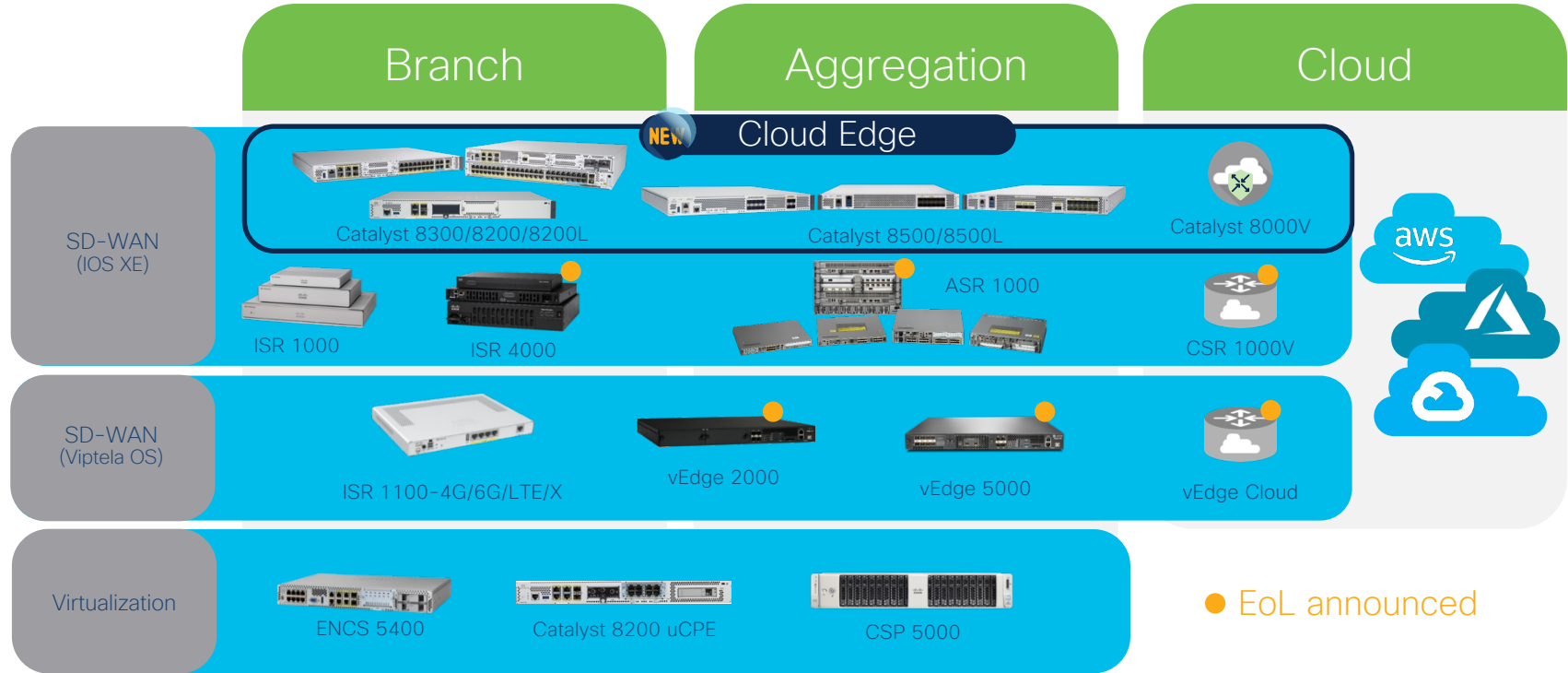


vSmart Deployment Demo

WAN Edge platforms

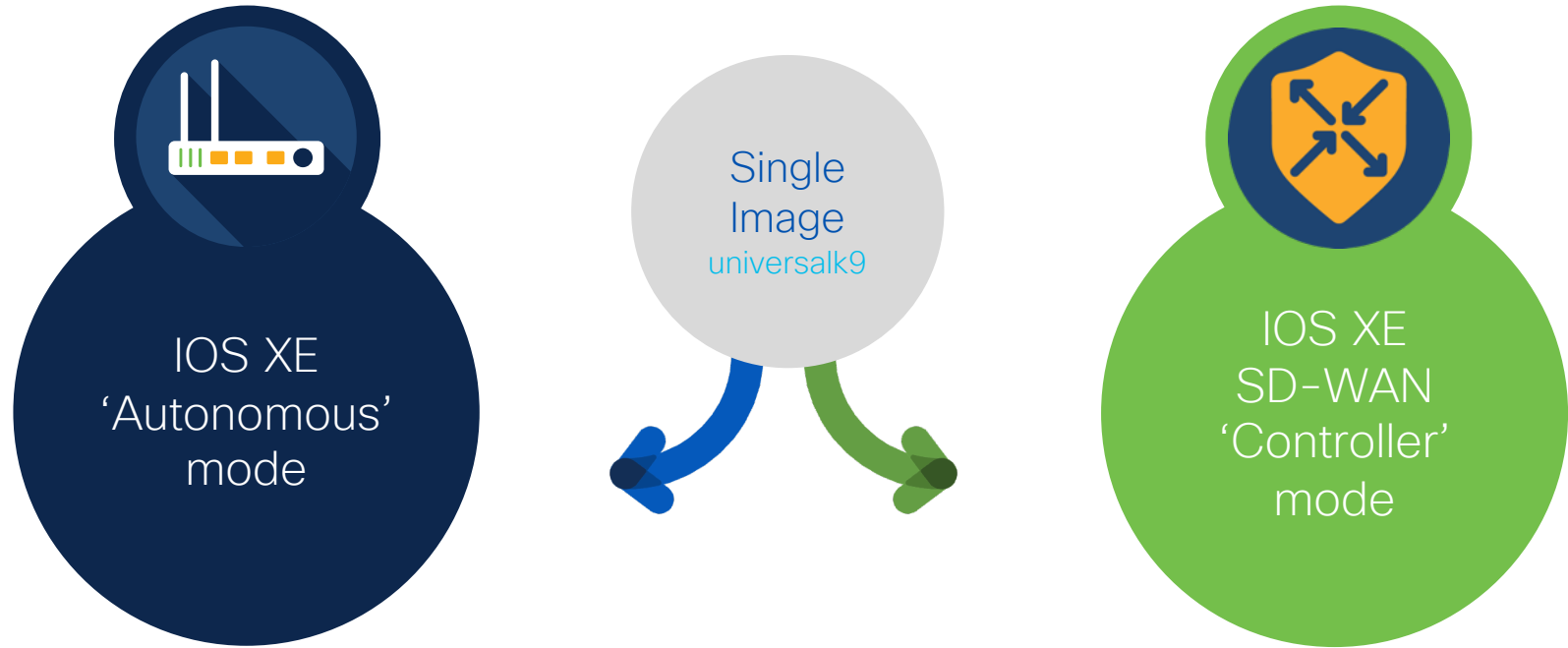


SD-WAN Platforms



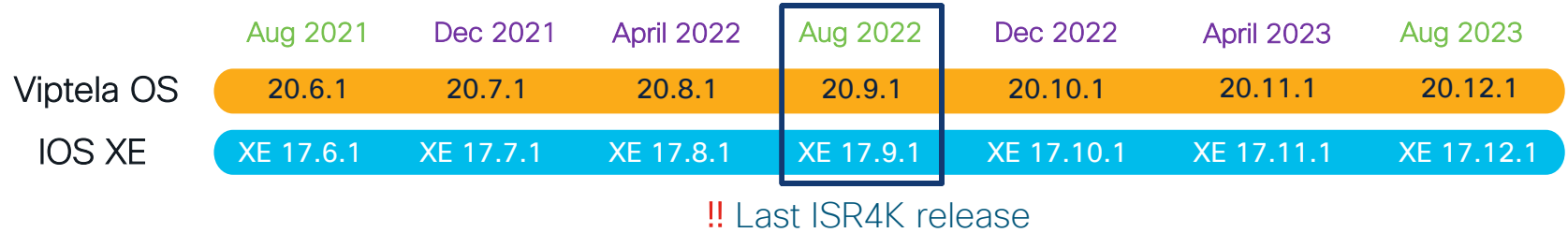
Cisco offers a broadest portfolio for WAN transformation

Easy operations with Single Image



Accelerate SD-WAN Journey | Simplify Deployments | Cloud-scale Application Support

Release Trains



Extended maintenance release

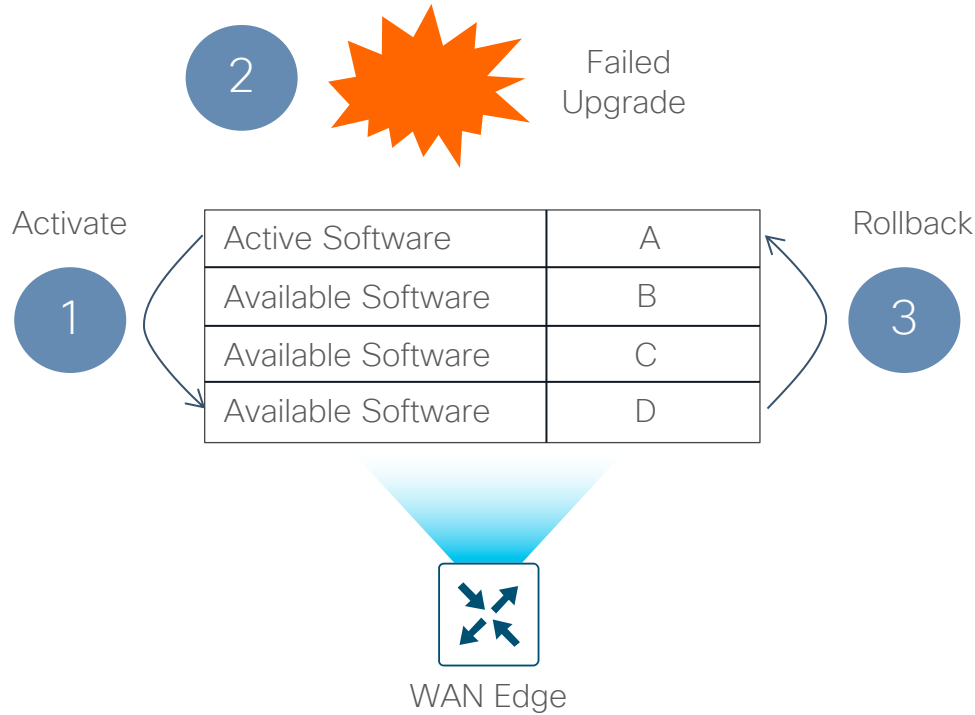
- 36 months of engineering support
- Seven scheduled rebuilds

Standard maintenance release

- 12 months of engineering support
- Two scheduled rebuilds

Software demo

Centralized Software Upgrades



- All software upgrades are performed centrally from vManage
- One or two stage upgrade
 - Load software and reboot now
 - Load software and reboot later
- Self-healing on upgrade failure
 - Device will revert to the last good image
- There is no requirement to run the same software version on all elements
 - Controllers should have higher software version than routers

Upgrade devices from vManage

Know your scale

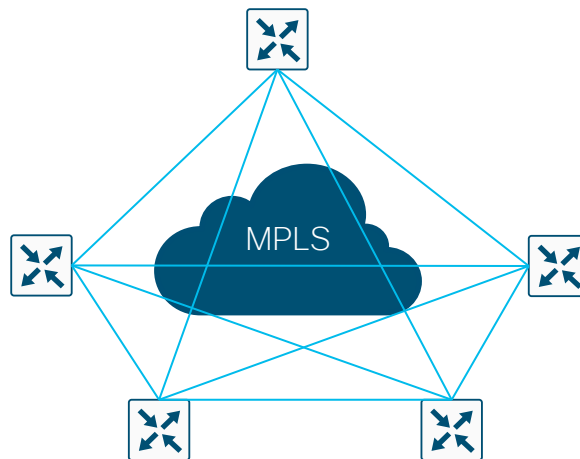
- Before choosing the right hardware platform for your deployment, identify the needs:
 - How many SD-WAN **overlay tunnels** per device are needed to build your desired topology?
 - What **features** would you like to run in your network?
 - How much **bandwidth** is required to carry the traffic?

Calculating number of tunnels

Full mesh: single transport, 1 Edge per site

- Each Edge builds tunnel to any other Edge
- Number of tunnels on Edge = number of Edges - 1
- If all Edge nodes are same platform, then max number of Edges in single overlay is:

Platform	Max number of IPSEC Tunnels	Max number of devices in full mesh
ISR1K	200 tunnels	201
Catalyst 8000v (2vCPUs)	500 tunnels	501
Catalyst 8200L	1500 tunnels	1501
Catalyst 8200	2500 tunnels	2501
Catalyst 8300	6000 tunnels	6001
Catalyst 8500	8000 tunnels	8001



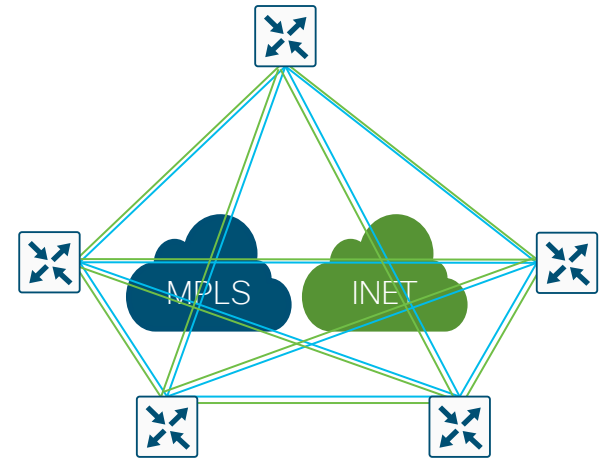
- If network has mix of different Edge platforms, then the **smallest platform** defines the limit!

Calculating number of tunnels

Full mesh: dual transport (colors restricted), 1 Edge per site

- Each Edge builds tunnel to any other Edge
- Number of tunnels on Edge = $2 * (\text{number of Edges} - 1)$
- If all Edge nodes are same platform, then max number of Edges in single overlay is:

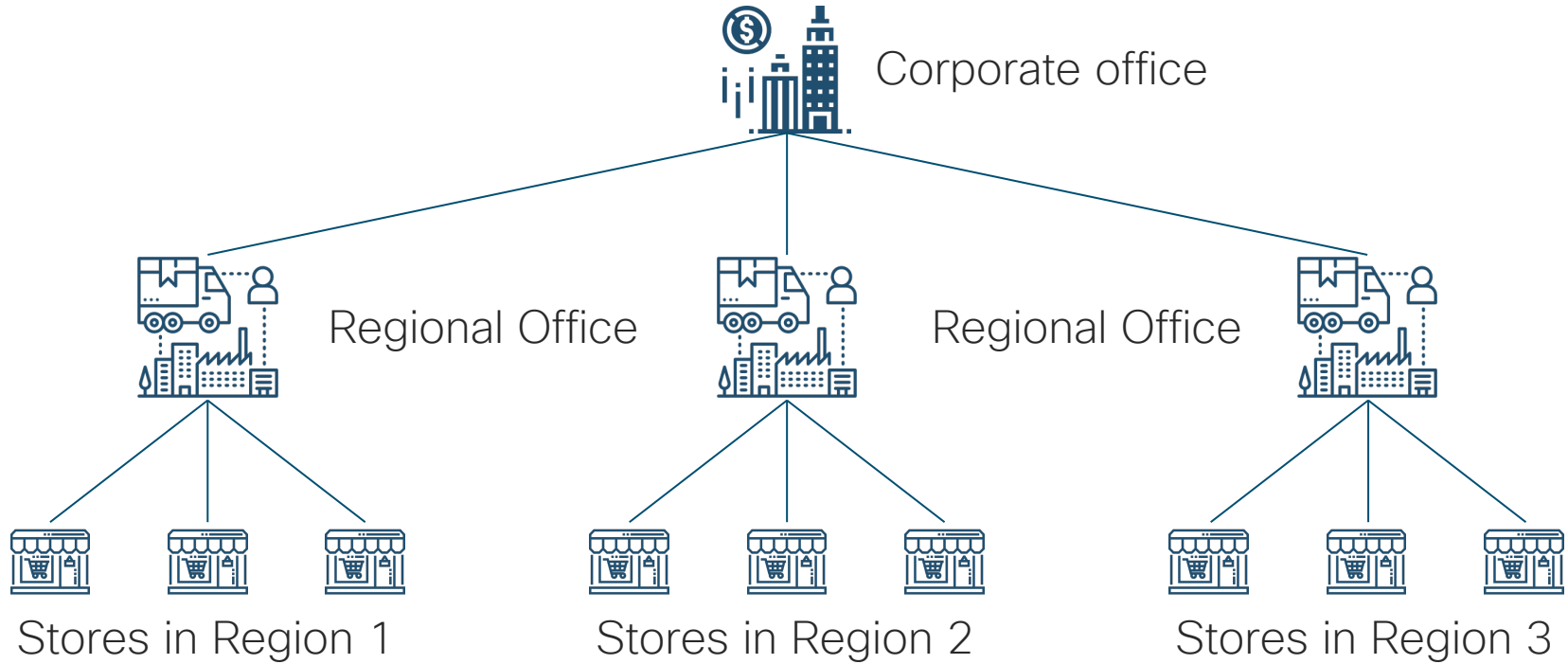
Platform	Max number of IPSEC Tunnels	Max number of devices in full mesh
ISR1K	200 tunnels	101
Catalyst 8000v (2vCPUs)	500 tunnels	251
Catalyst 8200L	1500 tunnels	751
Catalyst 8200	2500 tunnels	1251
Catalyst 8300	6000 tunnels	3001
Catalyst 8500	8000 tunnels	4001



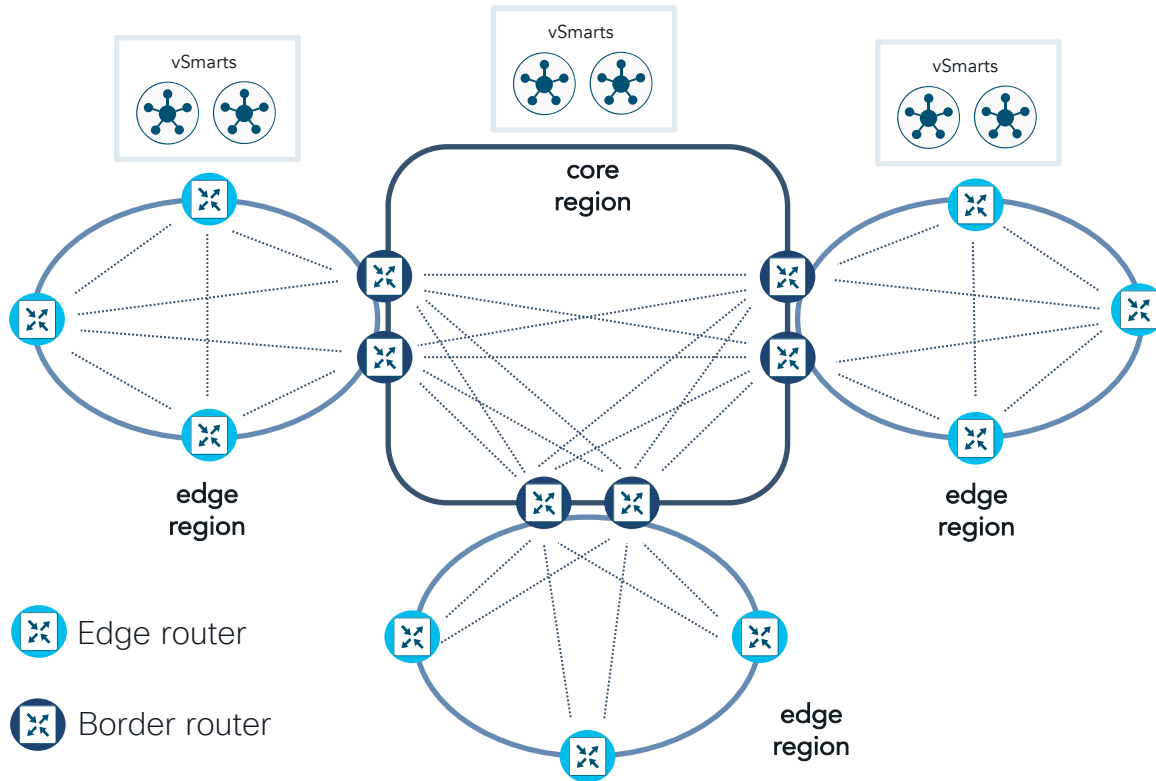
- If network has mix of different Edge platforms, then the **smallest platform** defines the limit!

Administrative regions

Company structure



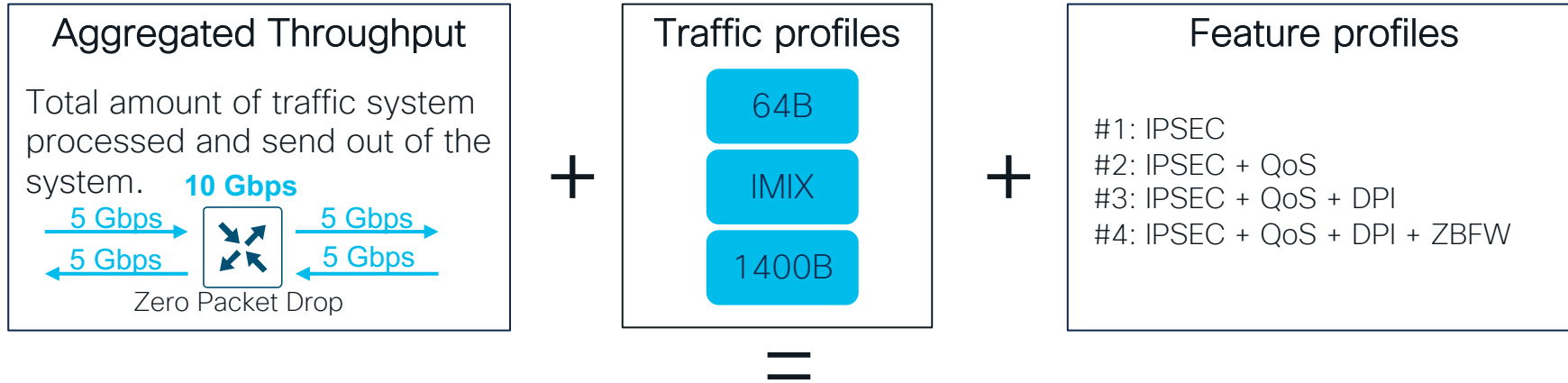
Multi-Region SD-WAN



Topology

- SD-WAN 2-Layer Architecture
- Fabric organized in Regions
- Edge Regions can be full mesh, partial mesh or hub and spoke
- OMP and vSmart region aware
- Regions have Border Routers in multiple POPs Connected to Core
- Global reachability via multiple Border Routers in every Region
- Simplified Configuration (No Control Plane Policy required)

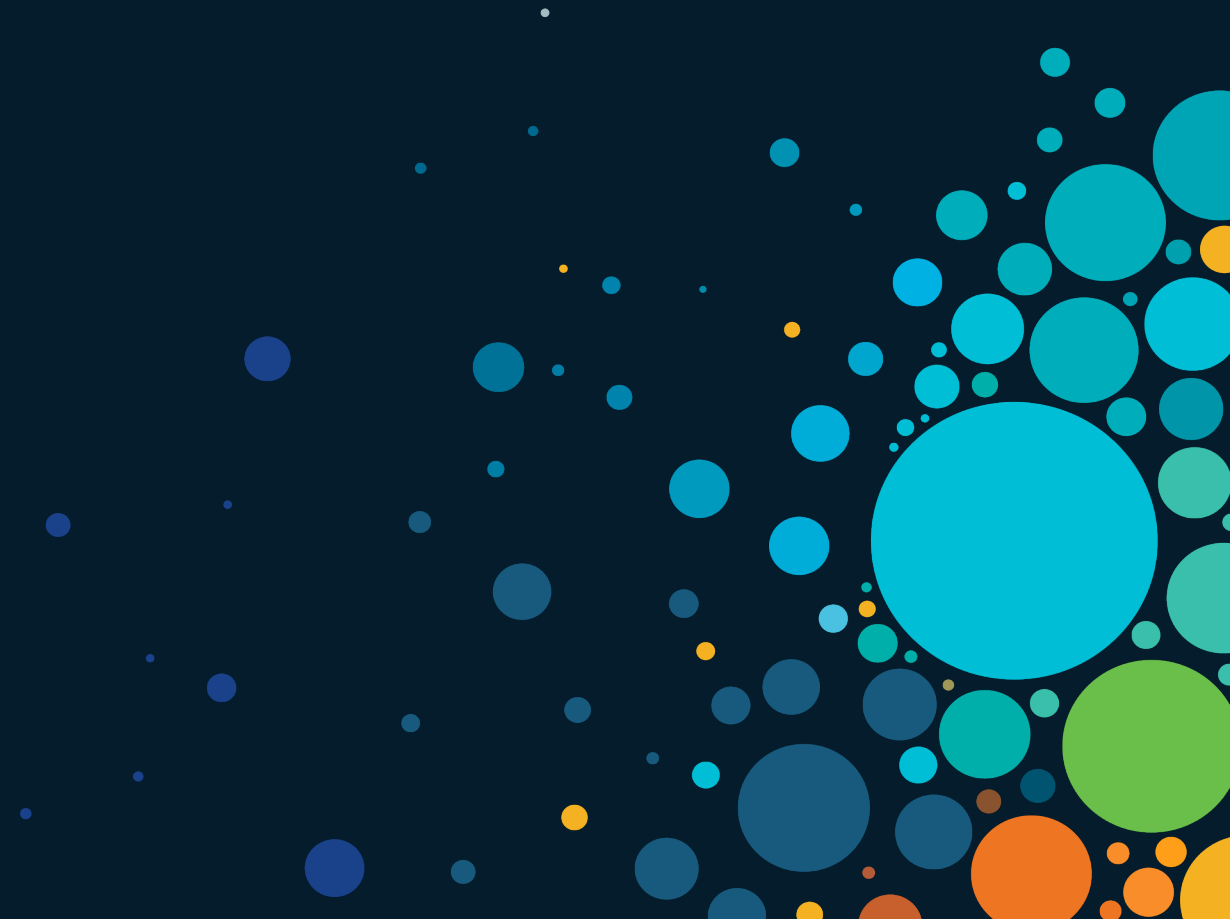
Performance – How do we do it at Cisco



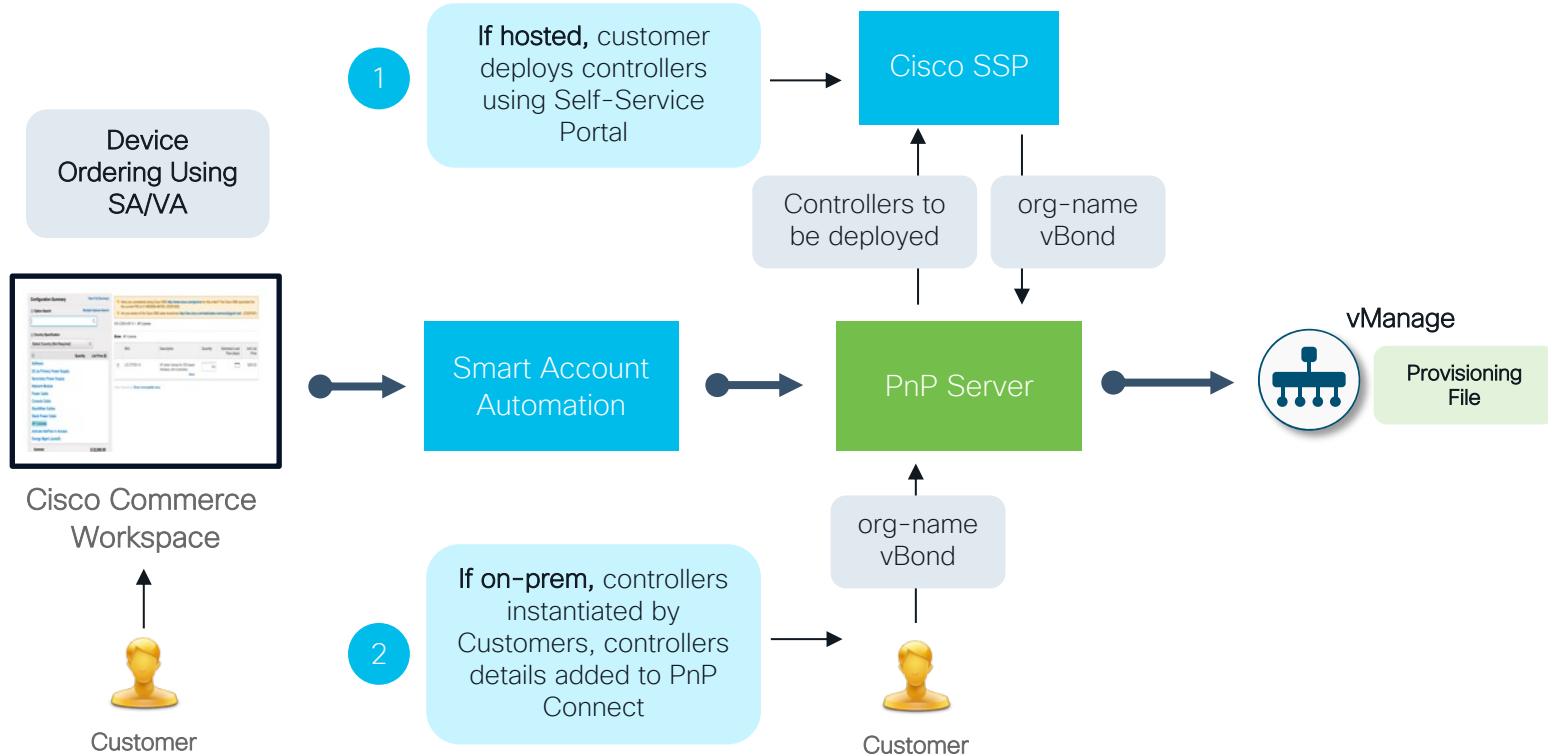
	C8500-12X4QC	C8500-12X	C8500L-8S4X
SD-WAN (IPSec)			
IMIX	21 Gbps	24,0 Gbps	10 Gbps
1400B	64,3 Gbps	63,8 Gbps	18,7 Gbps

RFC2544 – Benchmarking Methodology for Network Interconnect Devices

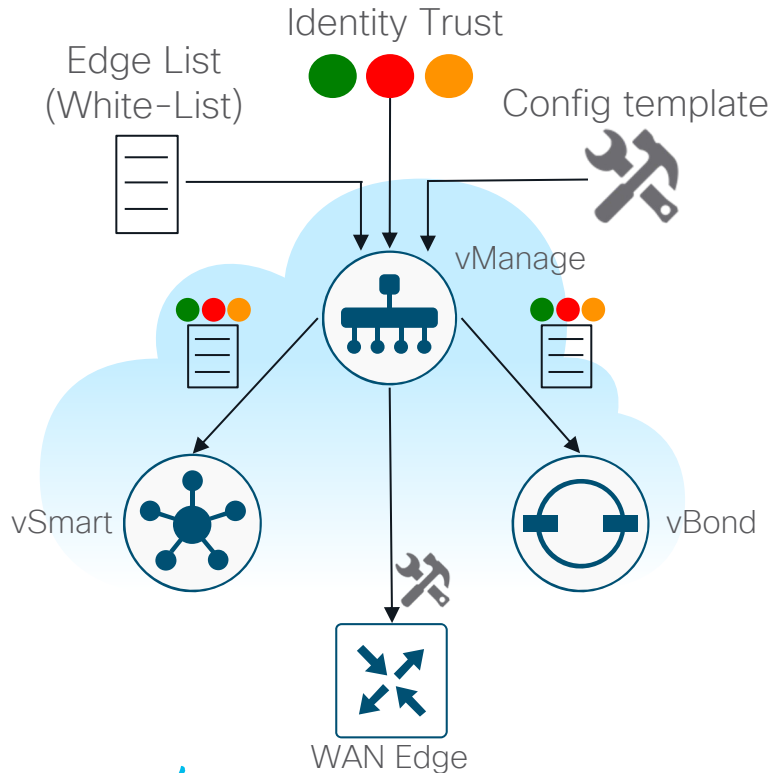
Onboarding



Global PnP Process Overview



Control Plane Whitelisting – Edge



- Digitally signed Edge white-list from PnP:

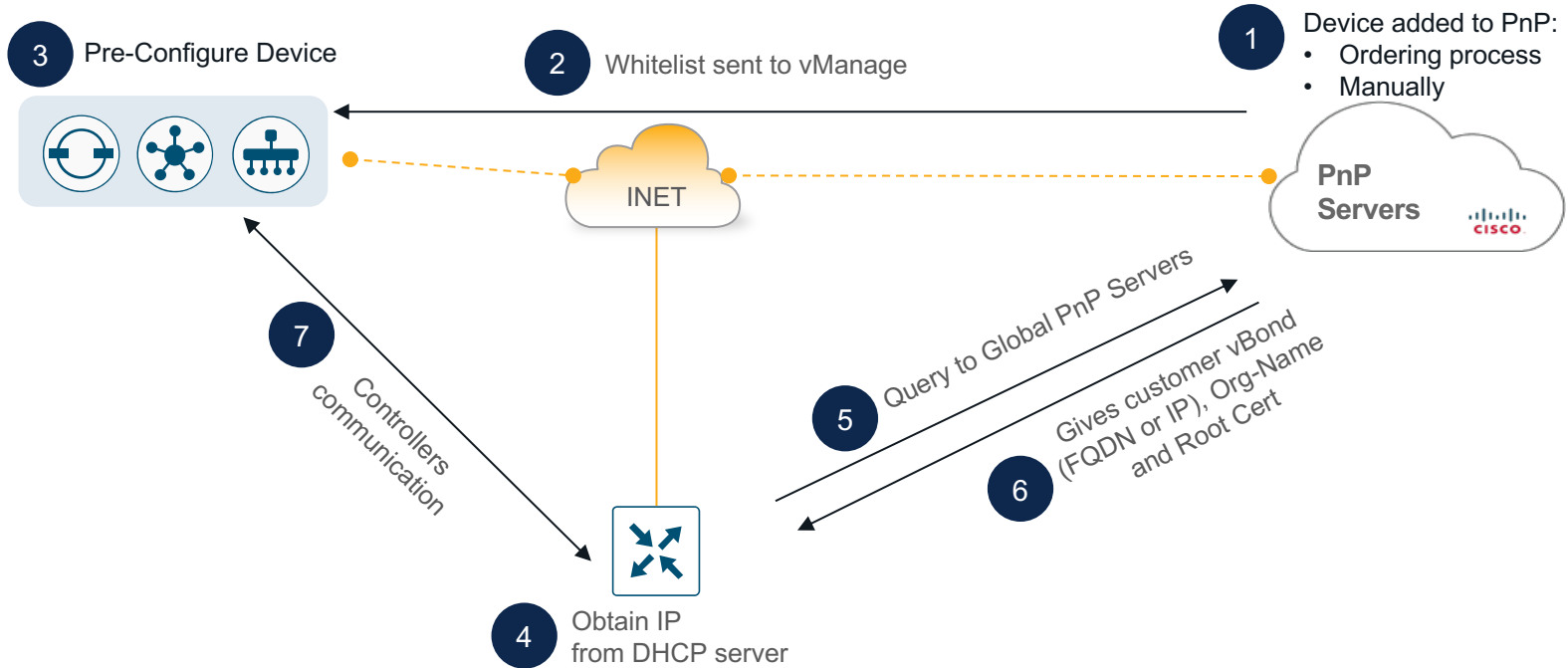
Chassis Number	Tags	Hostname	Site ID	Region ID	Mode
ISR4331/K9-FDO2347151E	Add Tag	MAD_SDWAN	81	-	vManage
ISR4331/K9-FDO23130B84	Add Tag	ISR4331_CORUNA	20	-	vManage
ISR4331/K9-FDO231300JW	Add Tag	ISR4331_SANTIAGO	20	-	vManage

- Administrator decides on identity trust:

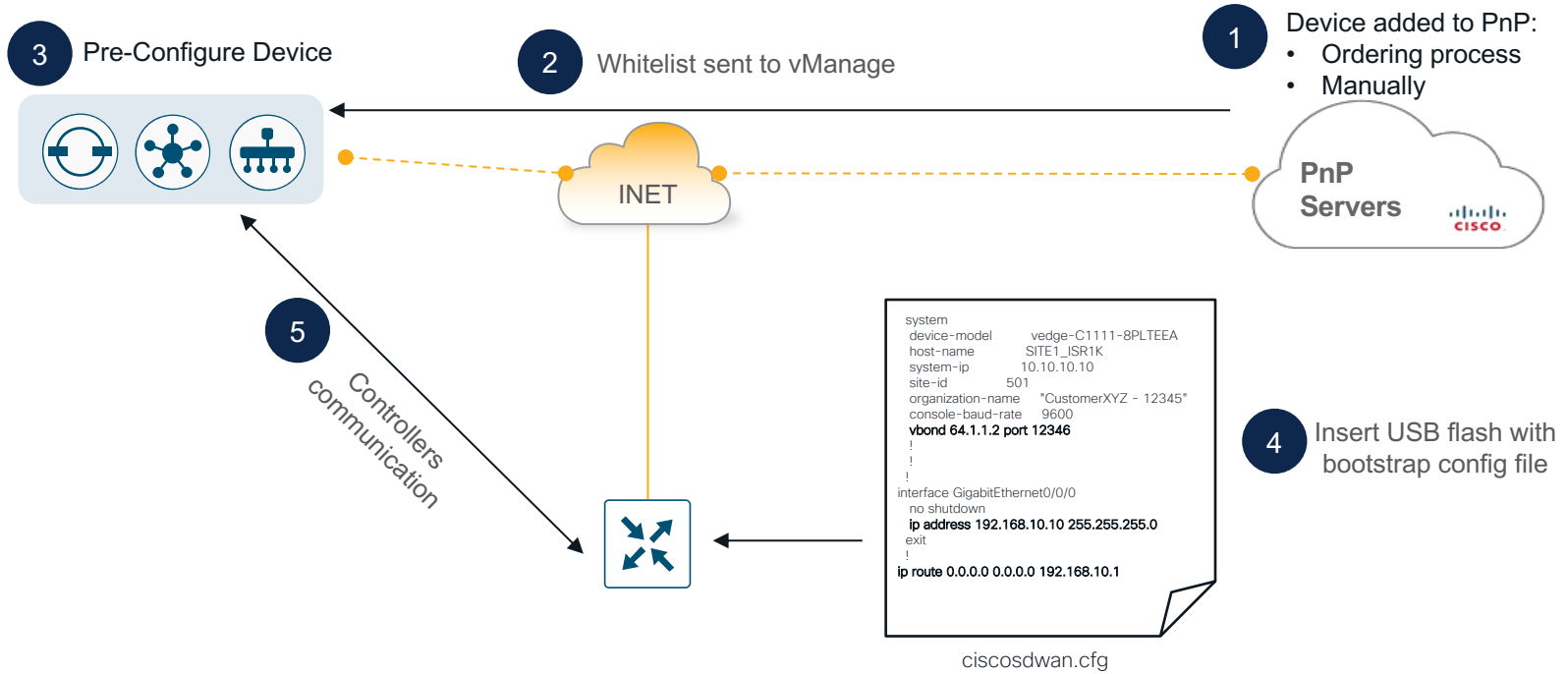
Subject SUDI serial #	Hostname	System IP	Validate
FDO2347151E	MAD_SDWAN	10.10.10.81	Invalid Staging Valid
FDO23130B84	ISR4331_CORUNA	10.0.0.20	Invalid Staging Valid
FDO231300JW	ISR4331_SANTIAGO	10.0.0.21	Invalid Staging Valid

- Edge list and identity trust are distributed by vManage to vSmart and vBond.
- Administrator assign config template to WAN Edge to be pushed when it becomes online.

Option 1 - Zero Touch Provisioning



Option 2 – Static IP Provisioning

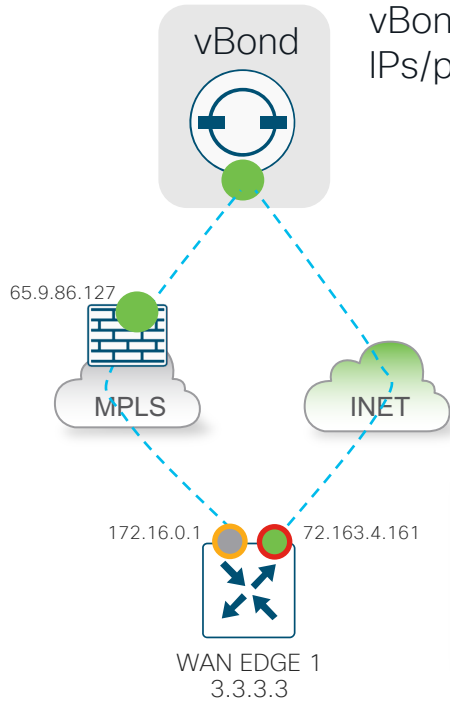


A decorative graphic in the top right corner consisting of a dense cluster of circles in various sizes and colors, including shades of blue, green, orange, red, and yellow. The circles are arranged in a way that suggests a sunburst or a cluster of data points. The colors transition from light blues and greys on the left to more vibrant colors like red and orange on the right.

Onboarding demo

Control plane & Data plane Tunnels

IPs discovery



vBond acts as STUN server and discover Private IPs/ports and Public IPs/ports

TLOC ROUTES

System IP	Color	Private IP	Private Port	Public IP	Public Port
3.3.3.3	MPLS	172.16.0.1	12346	65.9.86.127	1459
3.3.3.3	BIZ-INTERNET	72.163.4.162	12346	72.163.4.162	12346

PRIVATE COLORS

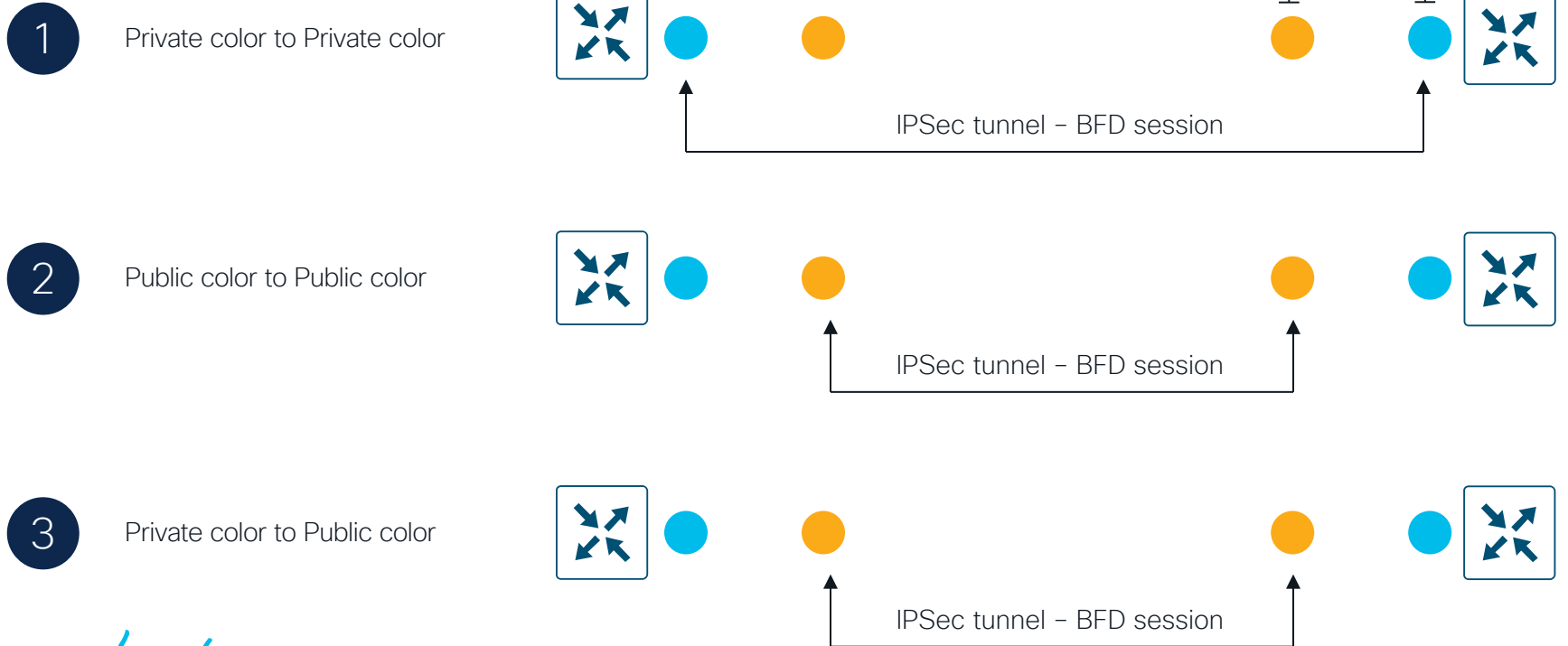
mpls
metro-ethernet
private1
private2
private3

PUBLIC COLORS

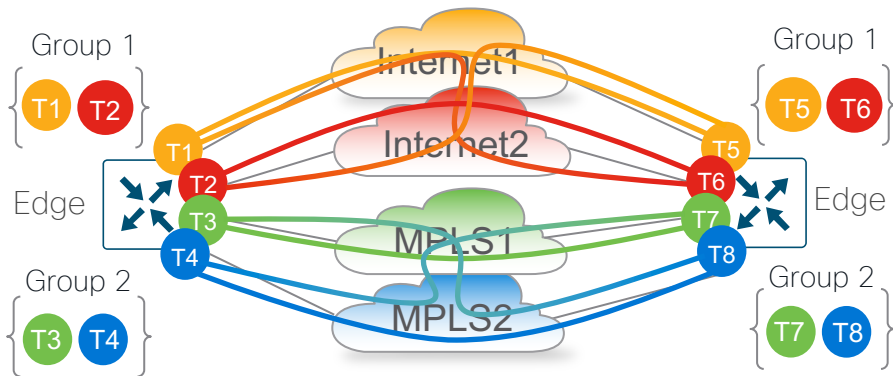
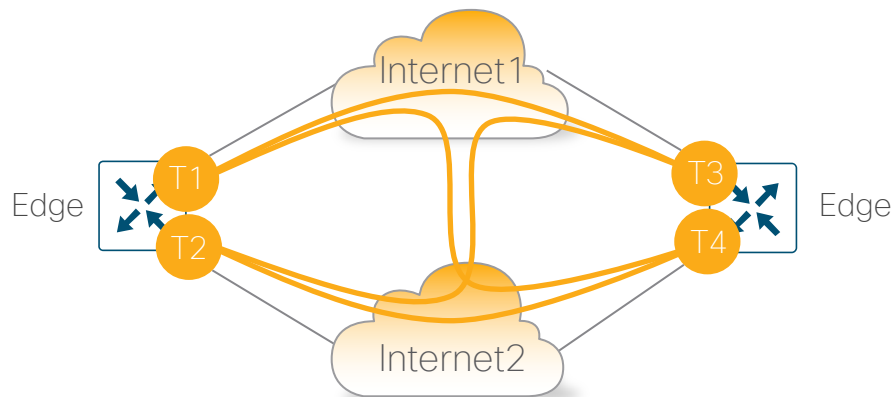
biz-internet
public-internet
custom1
custom2
custom3



TLOCs, Colors, Site-IDs and Carriers



Transport Colors

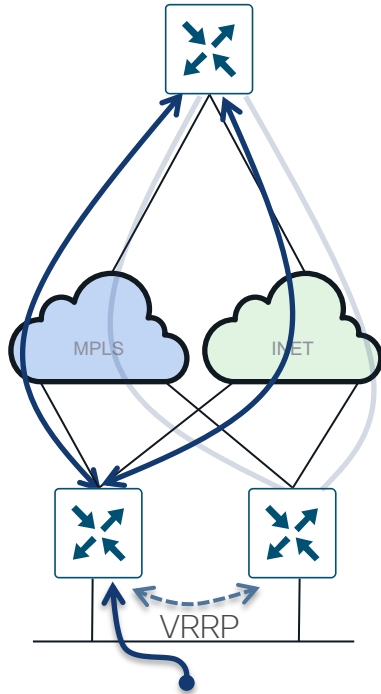


High Availability



Site Redundancy

VRRP



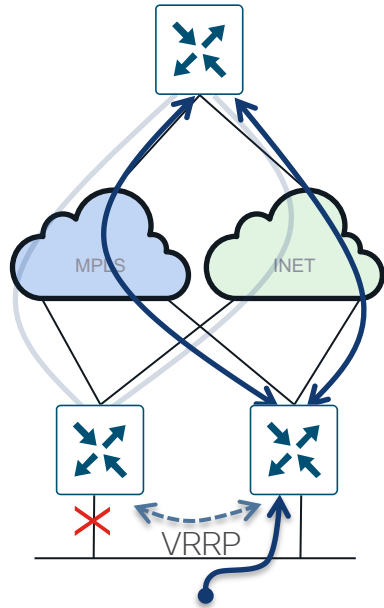
- WAN Edge routers are Layer 2 adjacent to the hosts
 - Default gateway for the hosts
- Virtual Router Redundancy Protocol (VRRP) runs between the two redundant WAN Edge routers



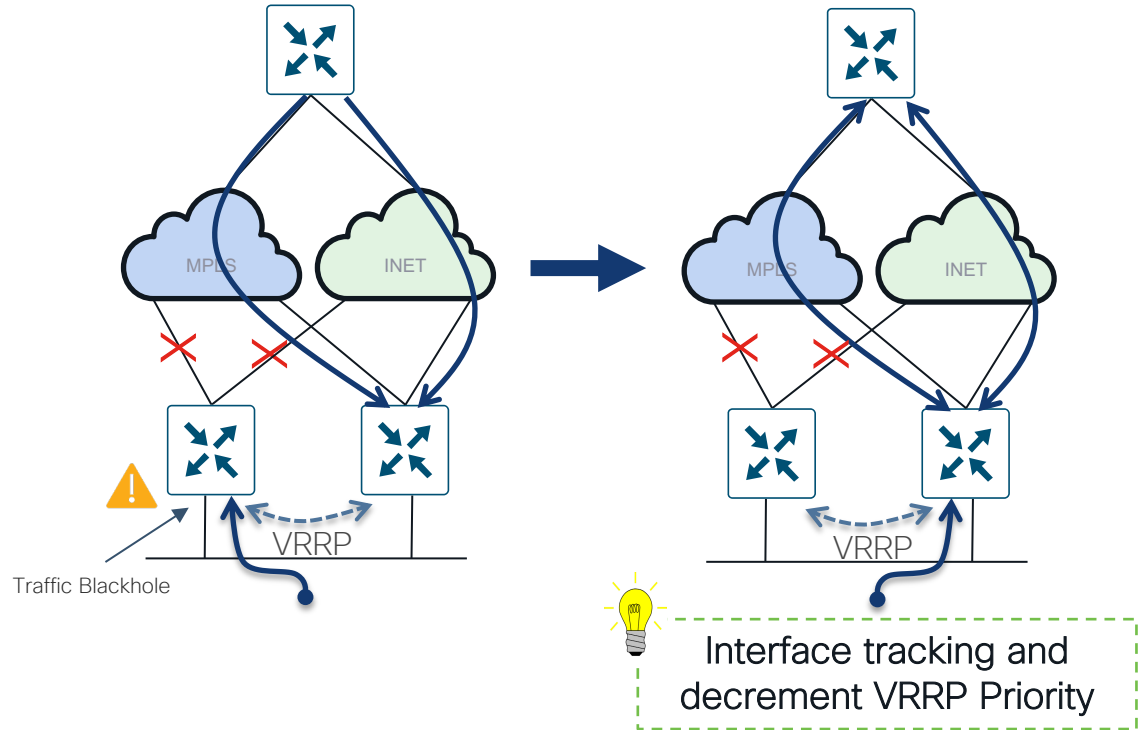
VRRP priority higher on primary device
TLOC preference higher on primary device

Site Redundancy

LAN Failure

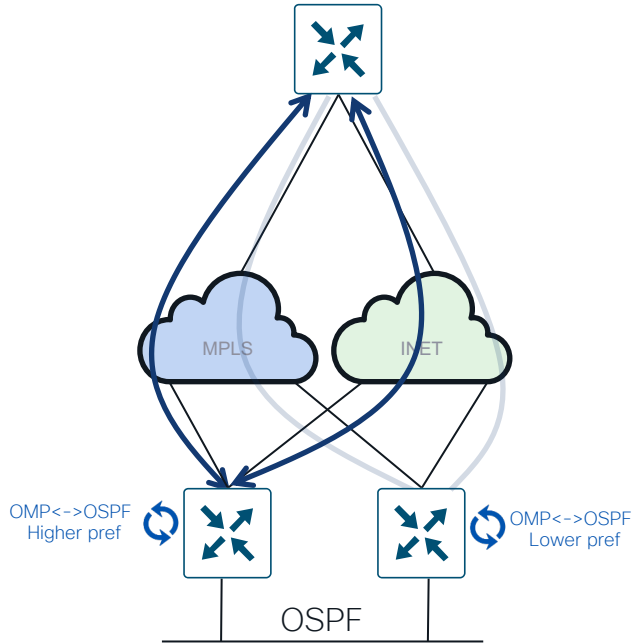


WAN Failure



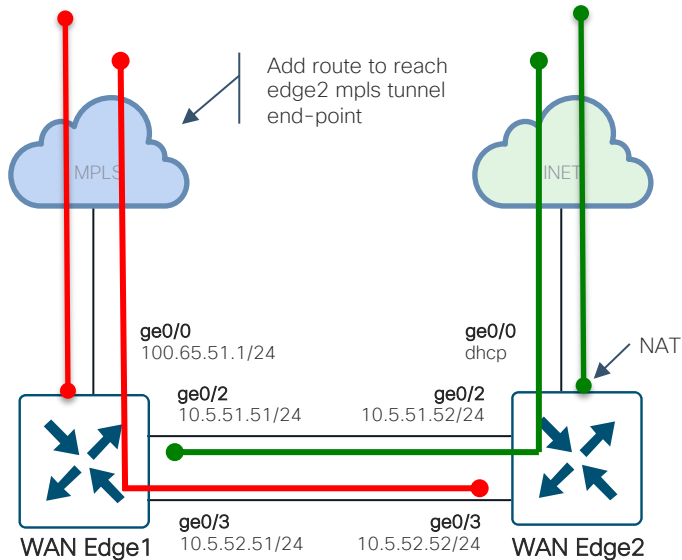
Site Redundancy

L3 Routing



- Routing protocols are running between the redundant pair Edge routers and the site router
- Bi-directional redistribution between OMP and OSPF/BGP and vice versa on the Edge routers
 - OSPF DN bit, BGP SoO community
- Site router performs equal cost multipathing for remote destinations across SD-WA Fabric
 - Can manipulate OSPF/BGP to prefer one Edge router over the other

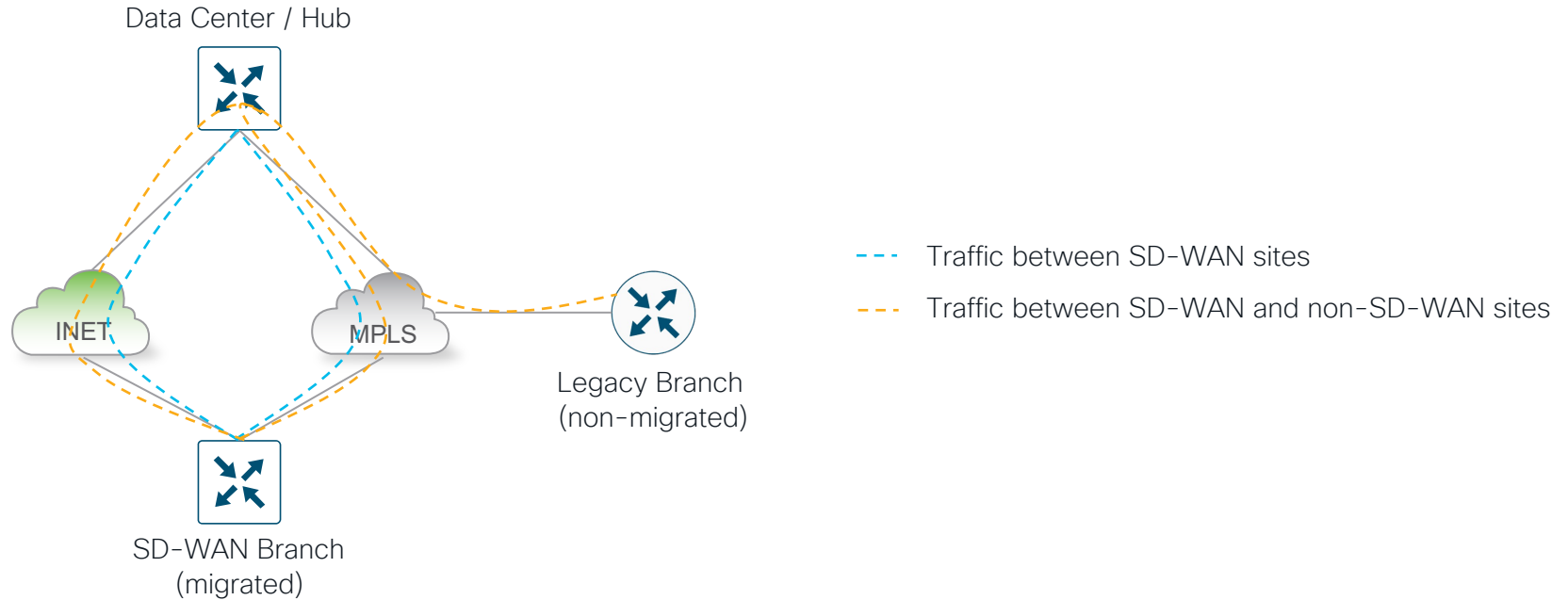
TLOC Extension



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

Data Center Edge

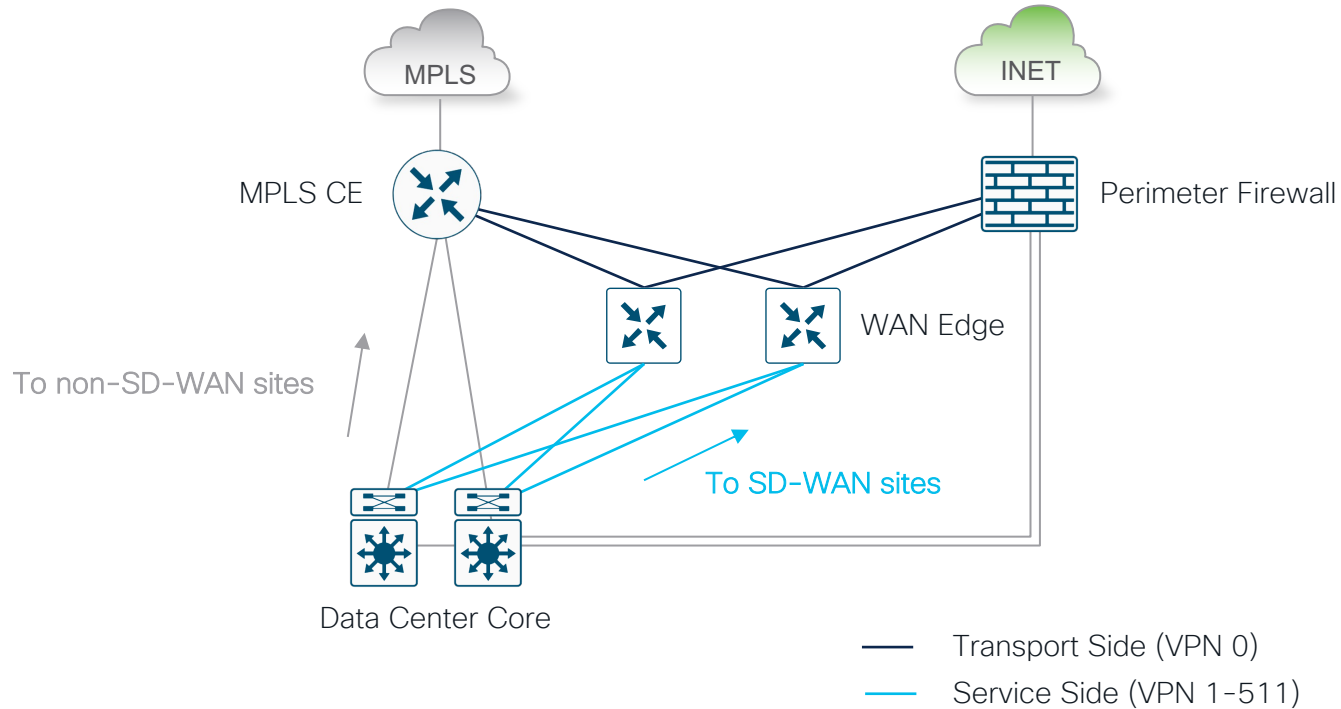
Why to start with Data Center?



SD-WAN to non-SDWAN interoperability in the Data Center

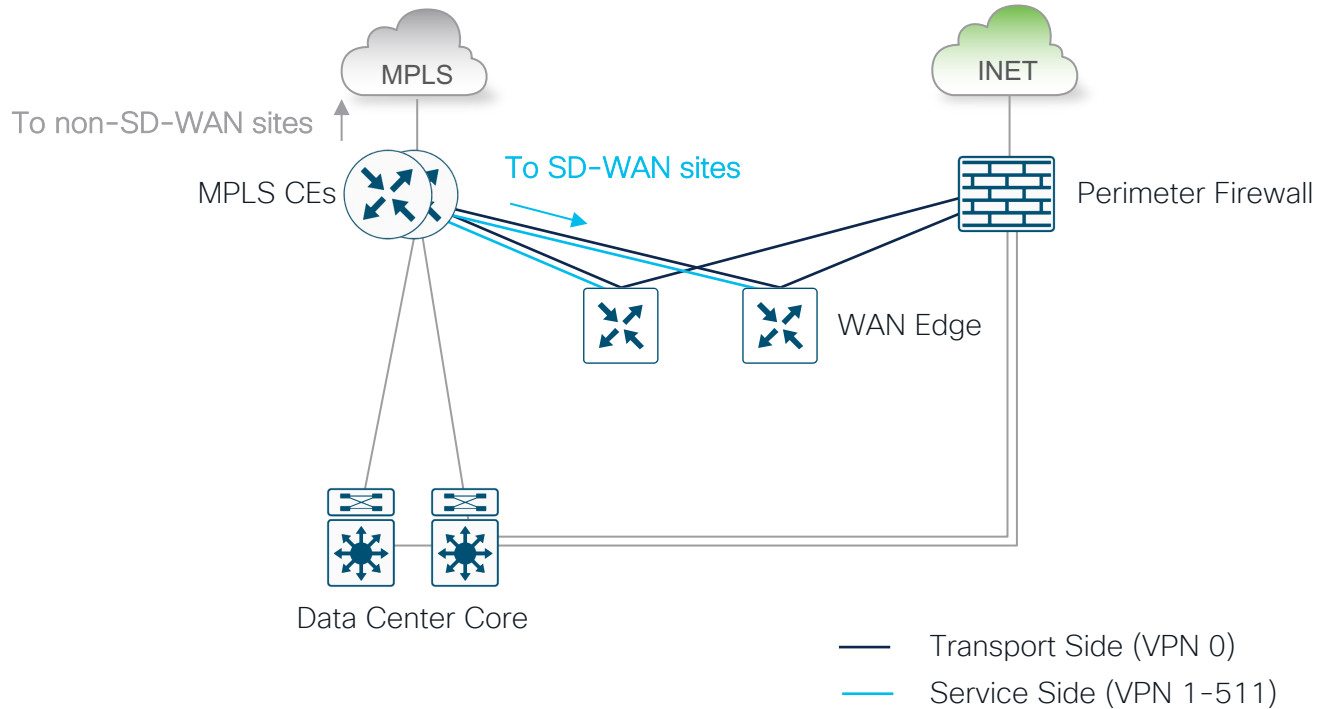
Data Center Topology

Option 1 – Integration with DC Core

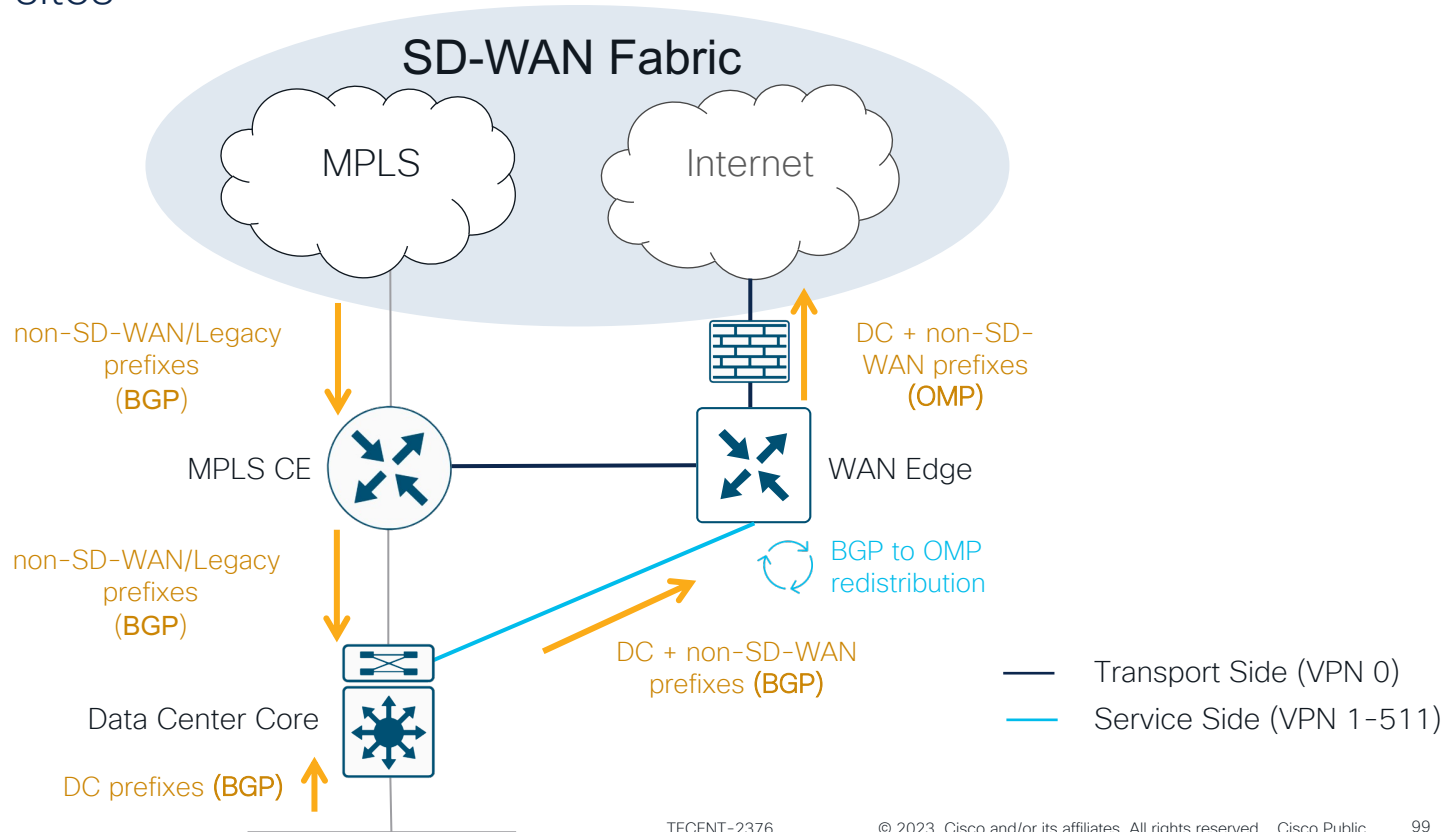


Data Center Topology

Option 2 – Integration with MPLS CEs

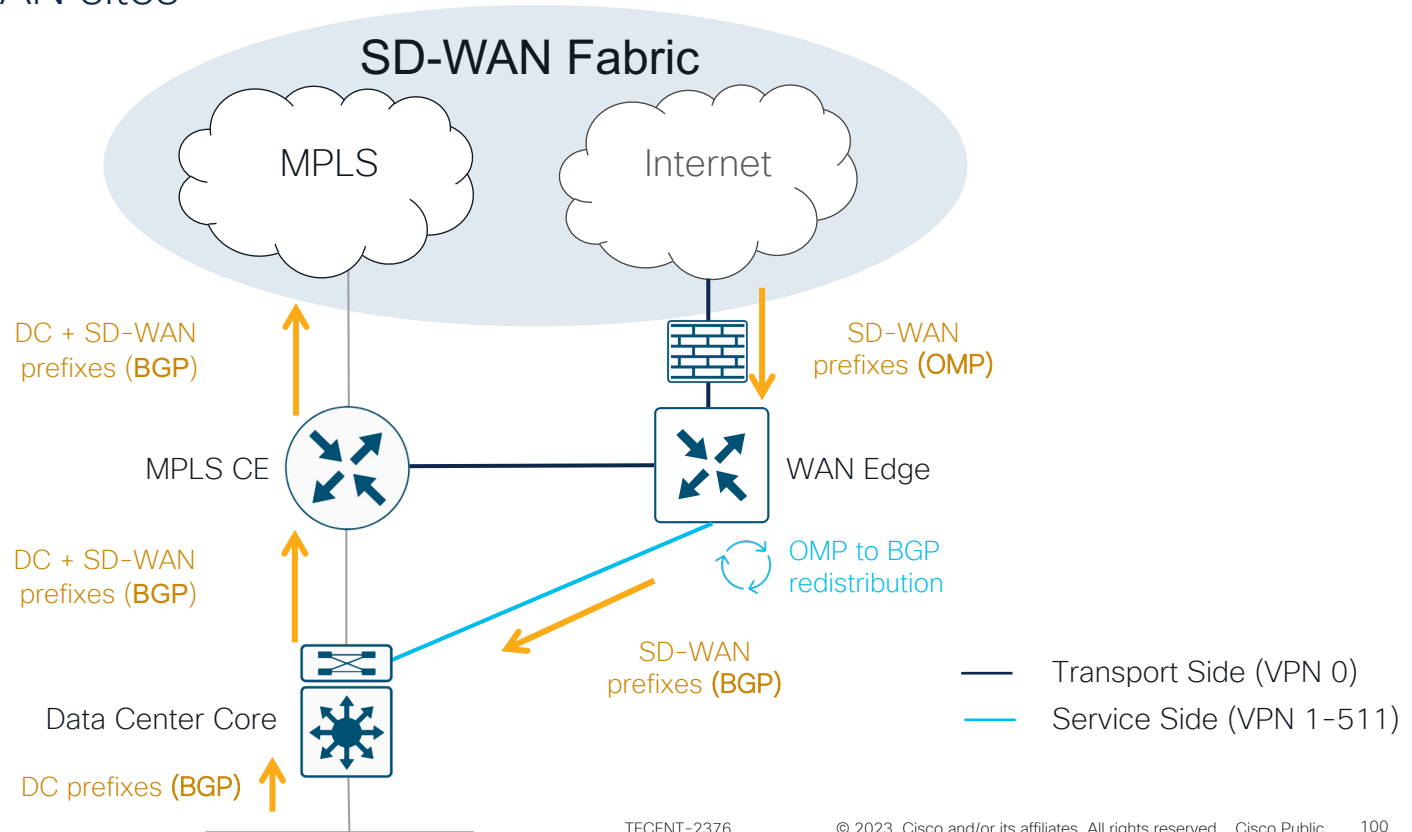


Data Center Route Advertisement To SD-WAN sites

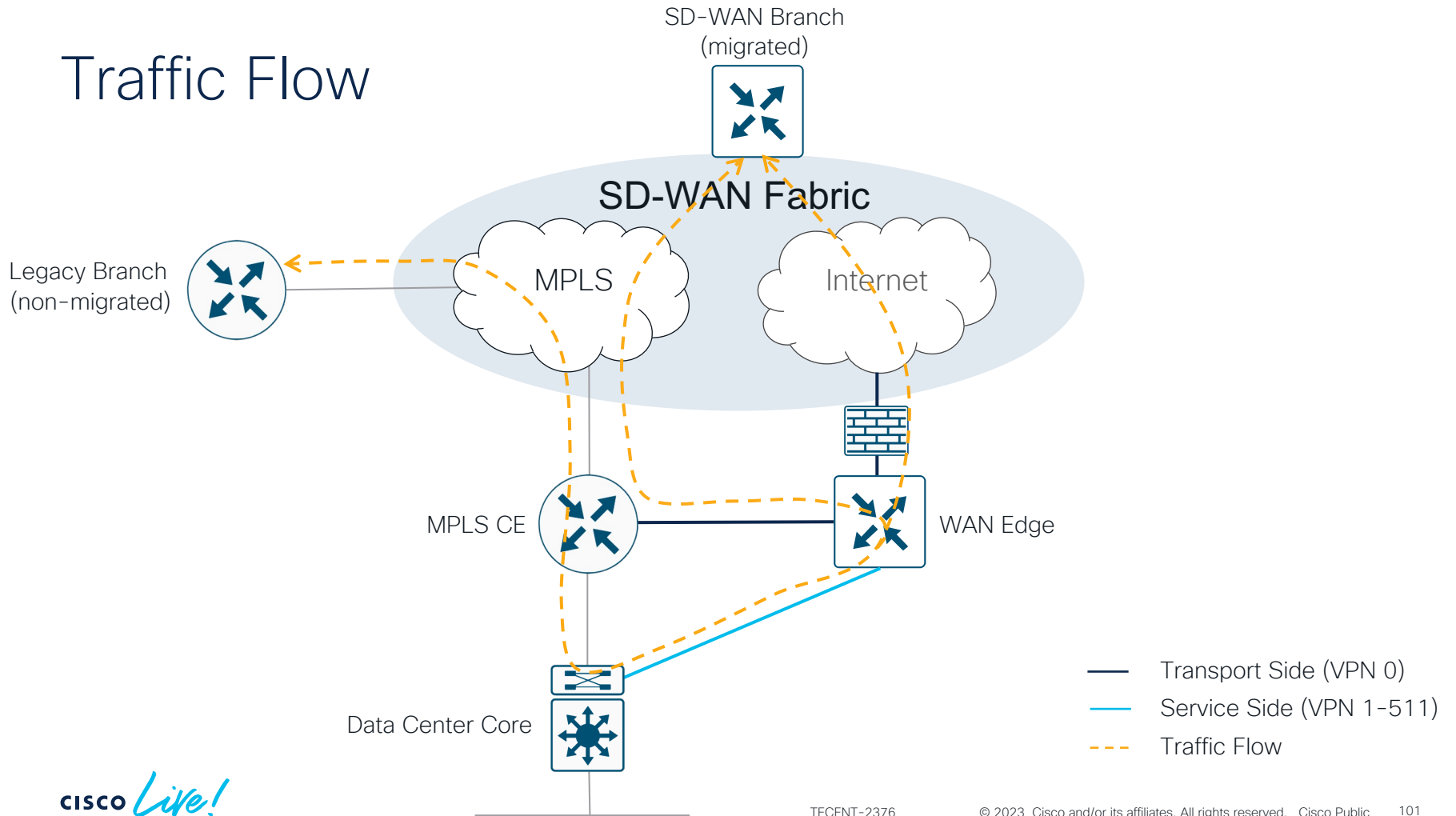


Data Center Route Advertisement

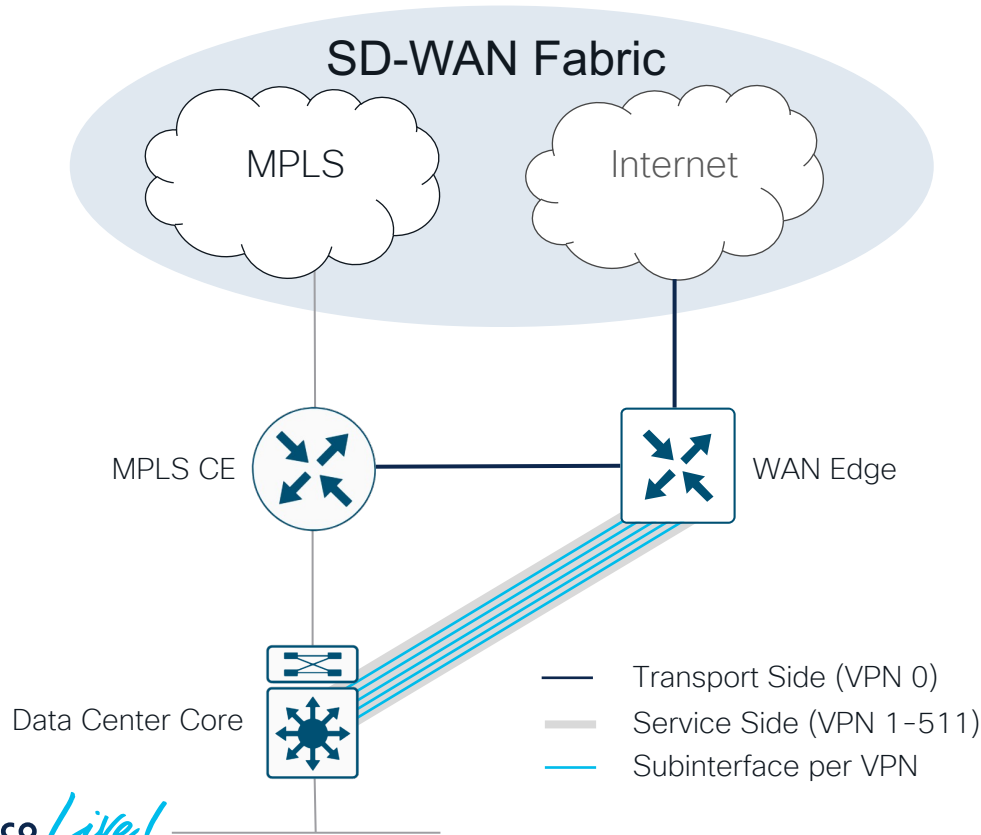
To non-SD-WAN sites



Traffic Flow



Data Center Segmentation

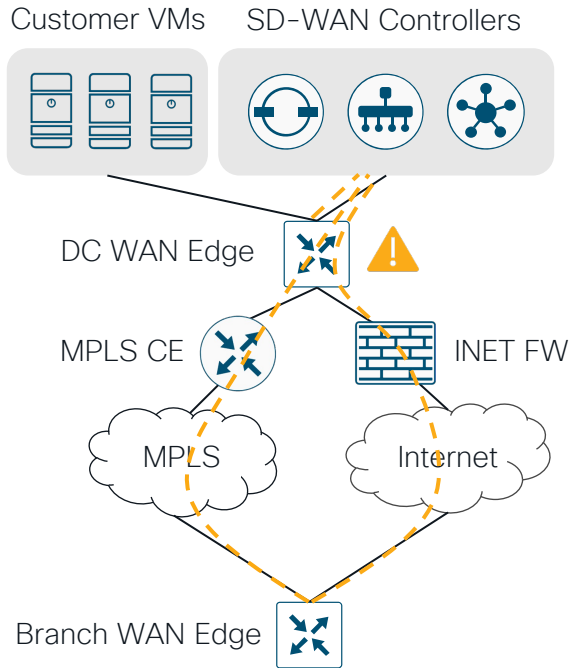


Per VPN:

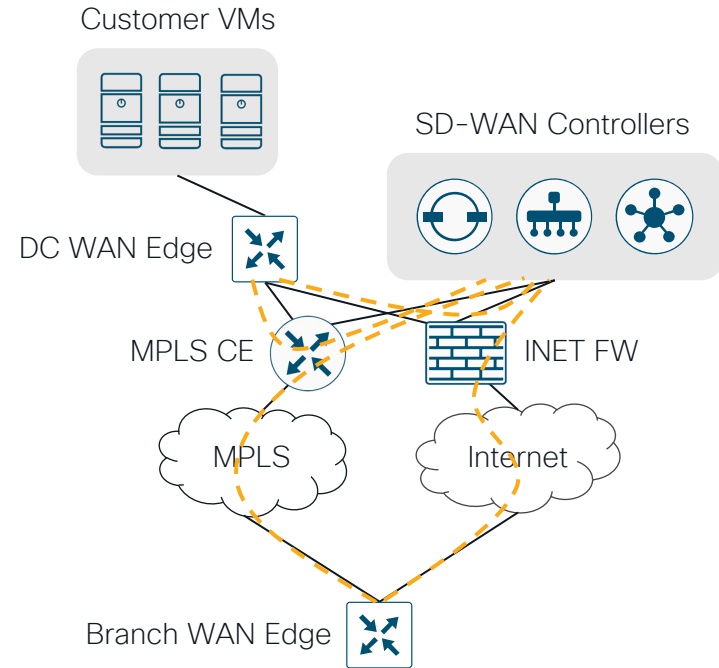
- VLAN
- Subinterface
- BGP session

Data Center Design with On-Prem Controllers

Option 1: Controllers part of LAN block
Complex Design - Avoid

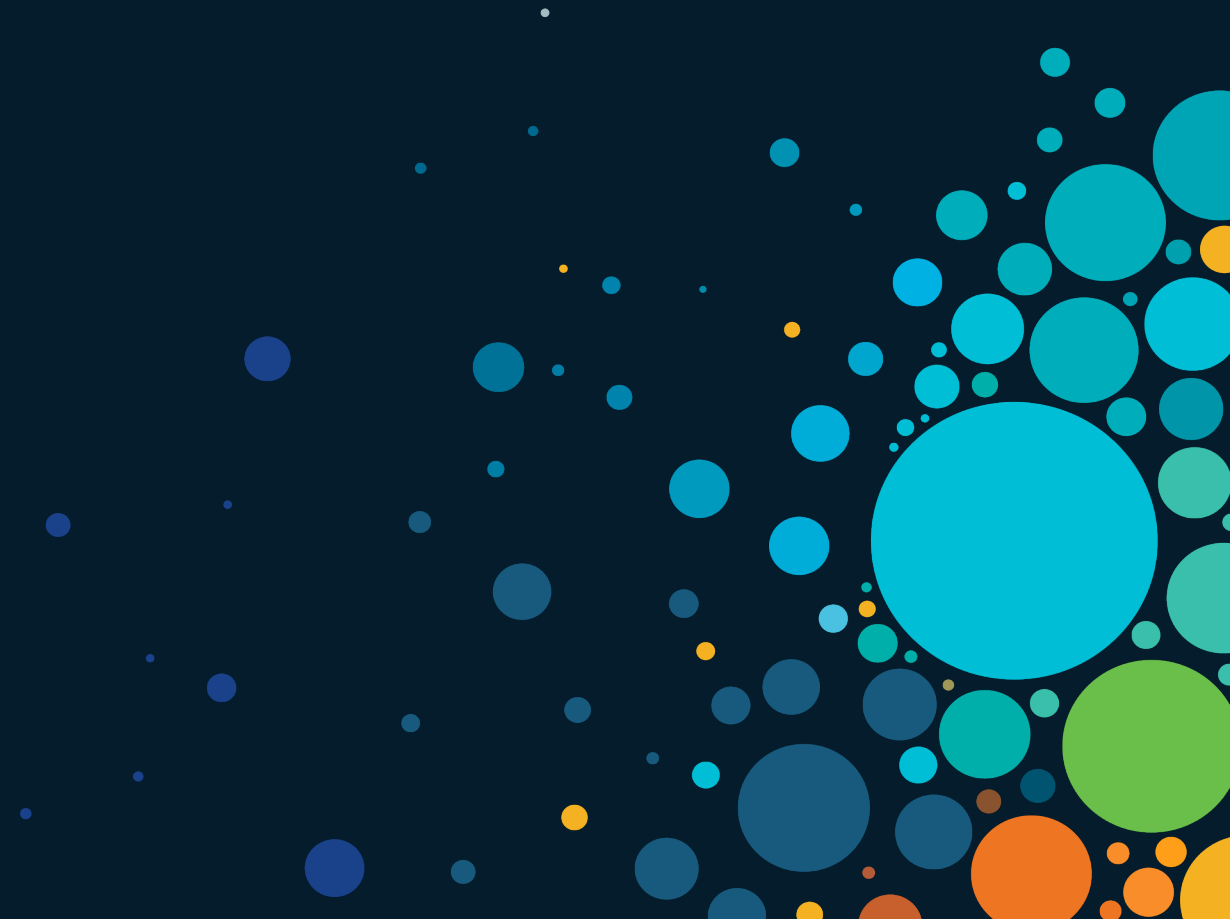


Option 2: Controllers part of WAN block
Simple Design - Recommended



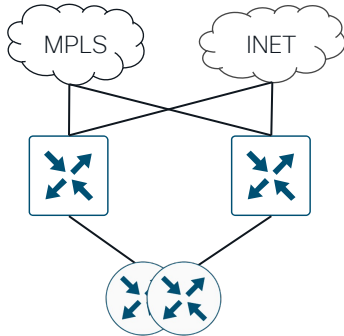
--- Control Connections

Branch Edge

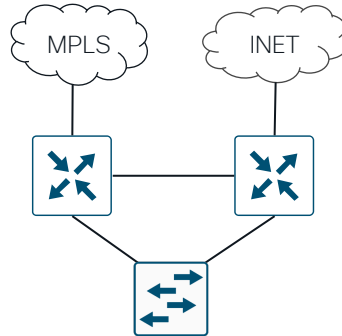


Defining Branch Types

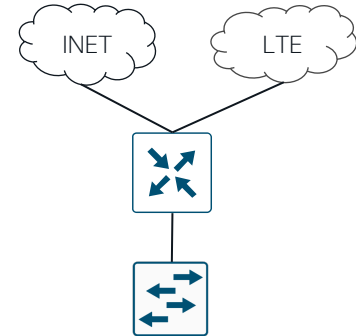
Branch Type 1



Branch Type 2



Branch Type 3

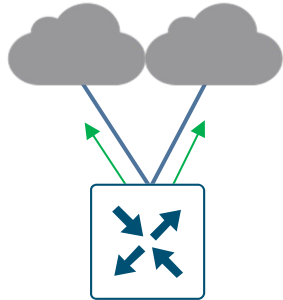


Unify the branch design to few types. Avoid exceptions.

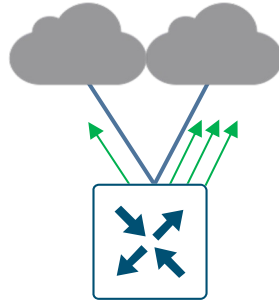
WAN Communication

Traffic Forwarding

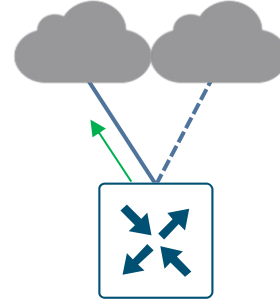
Per-Session Loadsharing
Active/Active



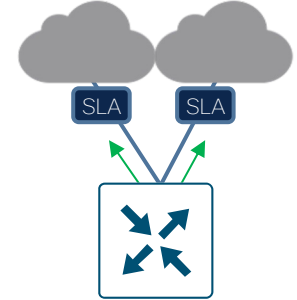
Per-Session Weighted
Active/Active



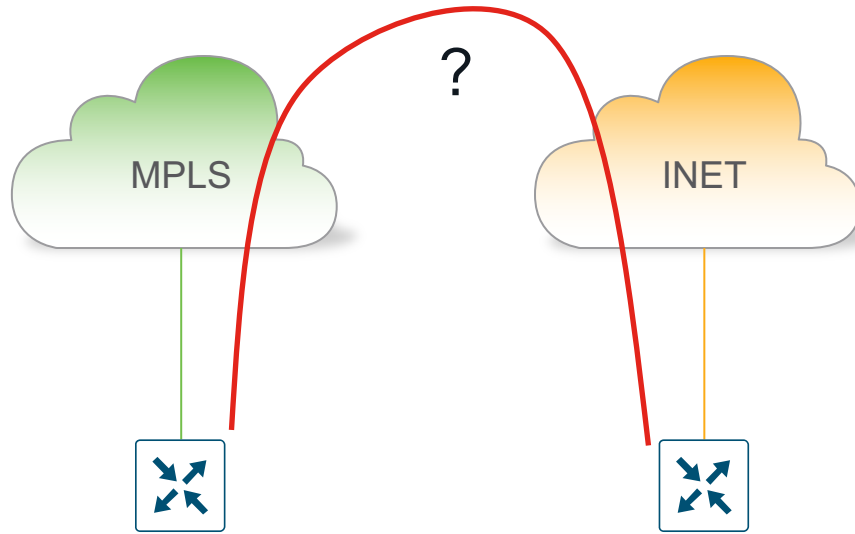
Application Pinning
Active/Standby



Application Aware Routing
SLA Compliant



INET WAN Edge Only to MPLS WAN Edge Only



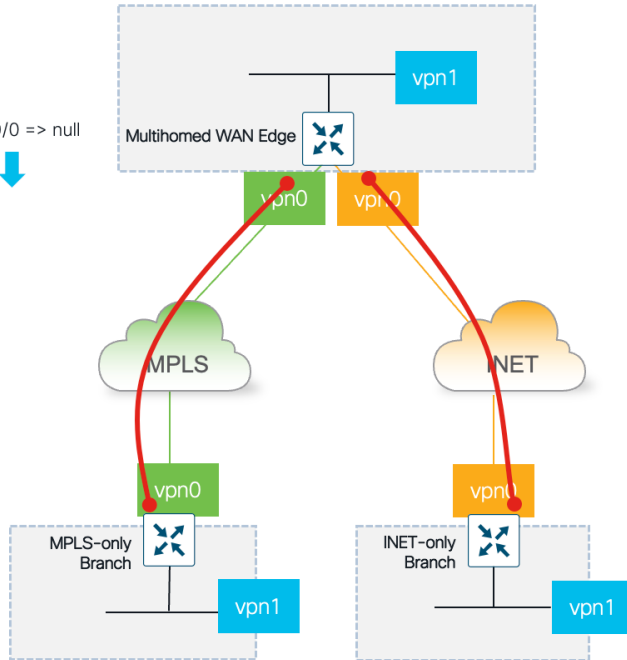
WAN Edge
single transport
MPLS

WAN Edge
single transport
INET

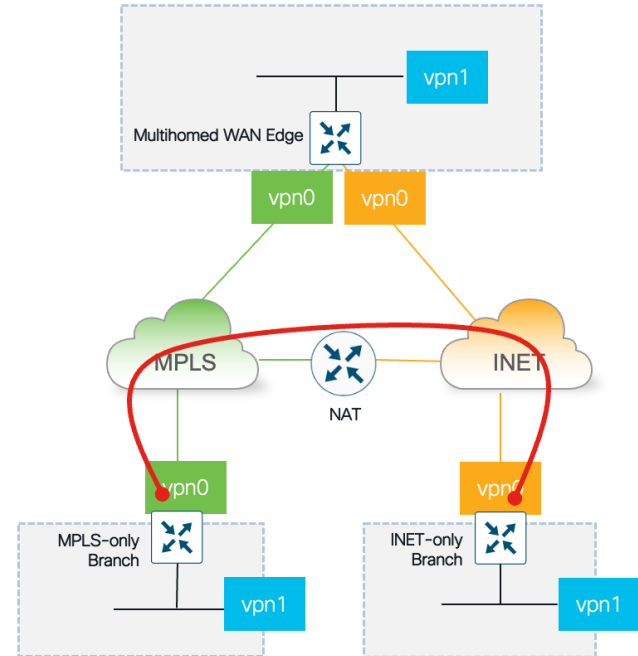
INET WAN Edge Only to MPLS WAN Edge Only

Multihomed WAN Edge
Recommended

0.0.0.0/0 => null
OMP ↓

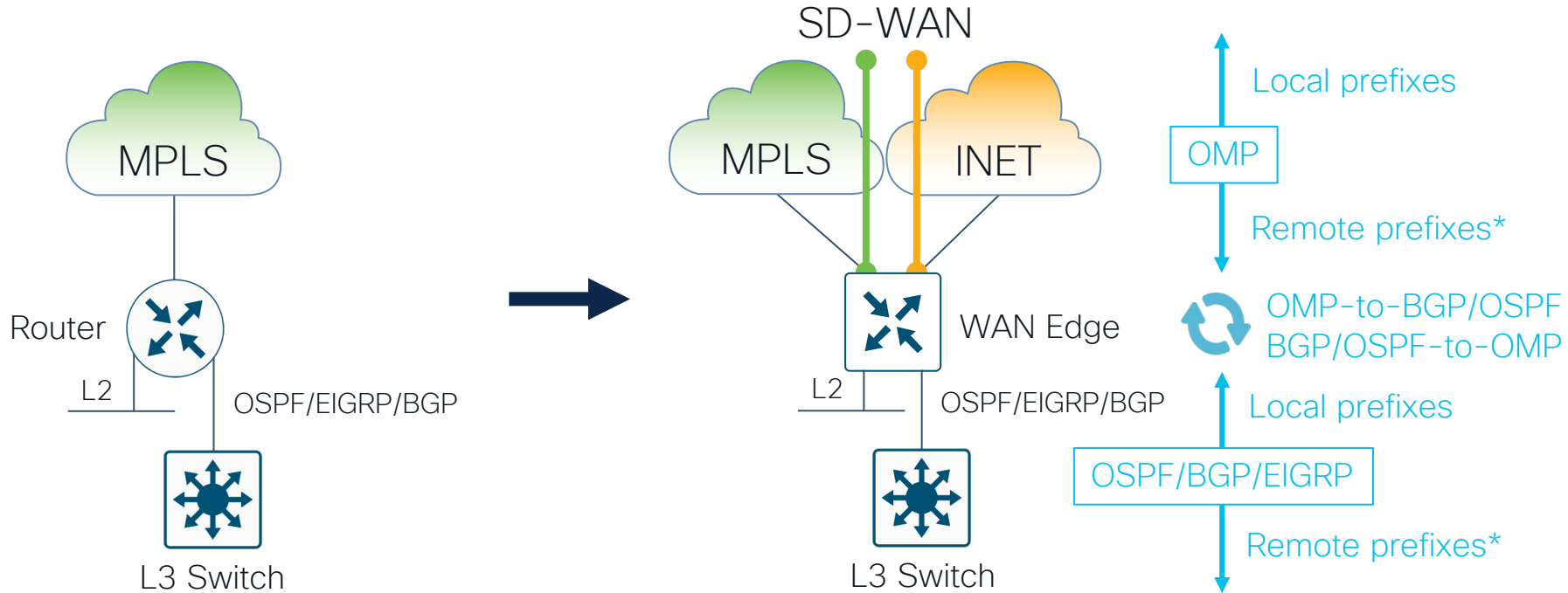


MPLS NAT
Complex - Avoid



Migration

Replace CE

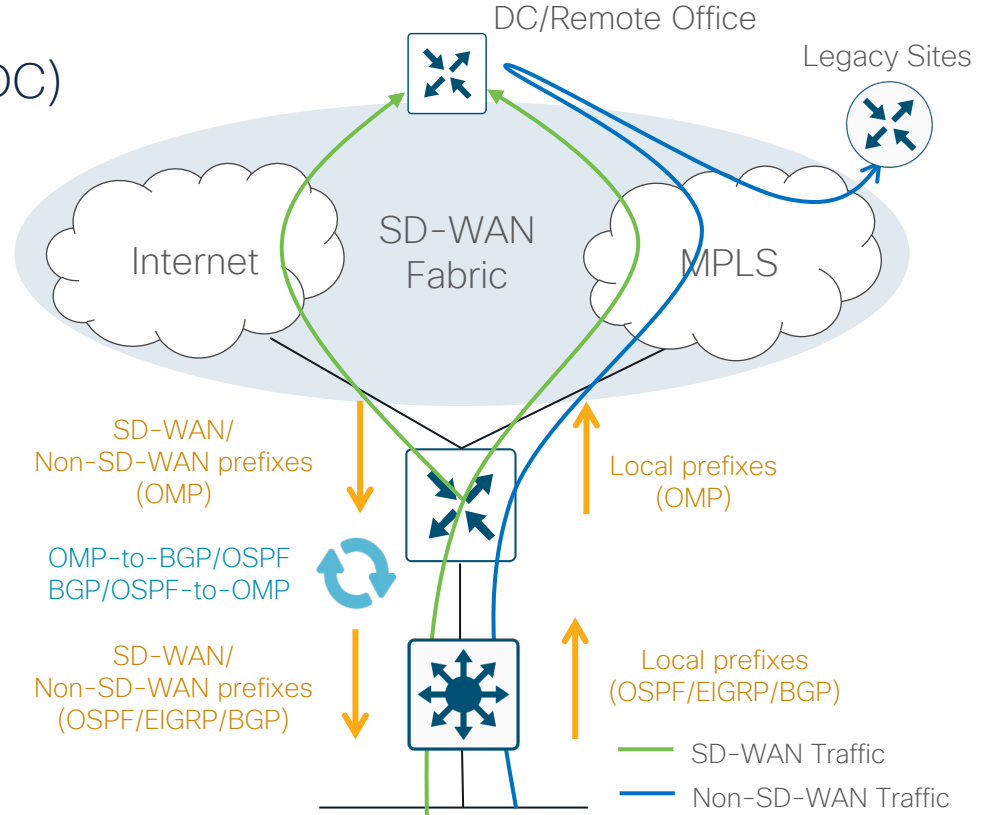


* SD-WAN and non-SDWAN  SD-WAN Tunnel

Traffic Flow

Option 1 - Replace CE (legacy via DC)

- Direct SD-WAN to SD-WAN sites communication
- SD-WAN to Legacy communication via DC/hub

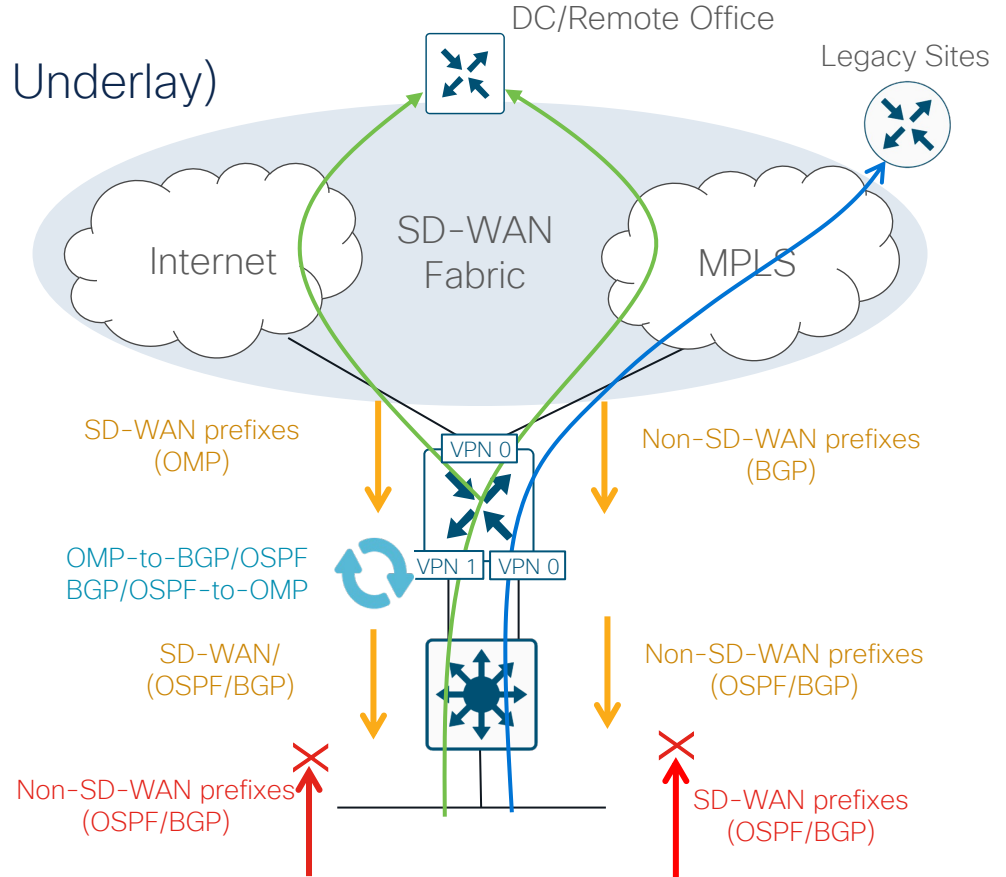


Traffic Flow

Option 2 - Replace CE (legacy via Underlay)

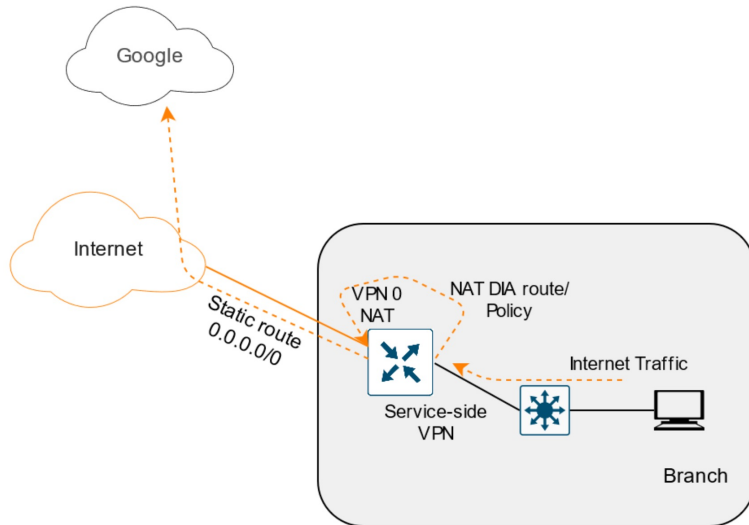
- Direct SD-WAN to SD-WAN sites communication
- SD-WAN to Legacy communication direct via underlay

— SD-WAN Traffic
— Non-SDWAN Traffic

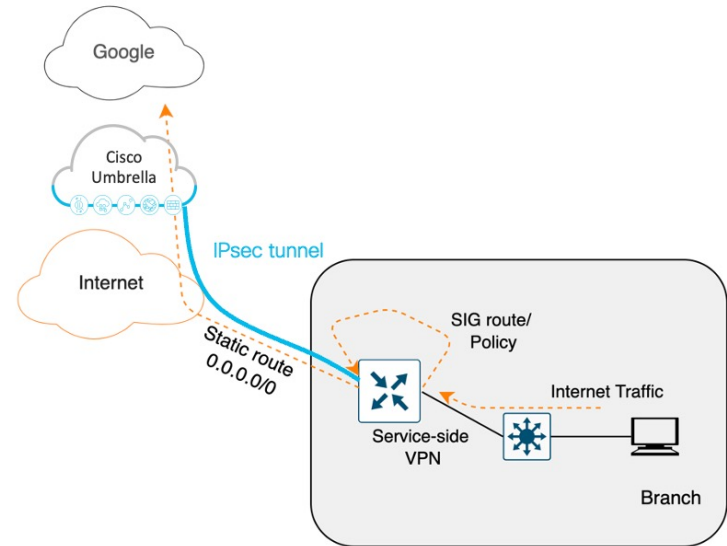


Direct Internet Access

NAT Direct Internet Access Route



Secure Internet Gateway



Monitoring and Troubleshooting



Troubleshooting

Basic troubleshooting with ping, trace, speed test, packet capture and more


Expert troubleshooting with full featured CLI real-time queries against WAN edge routers and more

Devices > Troubleshooting > Ping

Select Device **Branch** | 10.0.0.100 Site ID: 100 Device Model: C1111-8PLTEEA ⓘ


Destination IP* 10.0.0.1 VPN VPN - 10 Source/Interface for VPN - 10 Choose/Reset selections

Probes ICMP TCP UDP

 Packet Capture In Progress

Packet Capture will stop:

- In 4:56 Minutes, or
- 5-MB file is downloaded, or

 [Click to stop packet capture](#)

Device Group 10.0.0.100 x

All

Search

Sort by Reachability

DC vEdge Cloud

10.0.0.1 | Site ID: 1

Reachable

Branch C1111-8PLTEEA

10.0.0.100 | Site ID: 100

Reachable

```
10.0.0.100 login: admin
admin@10.0.0.100's password:
Password:
Branch#
```

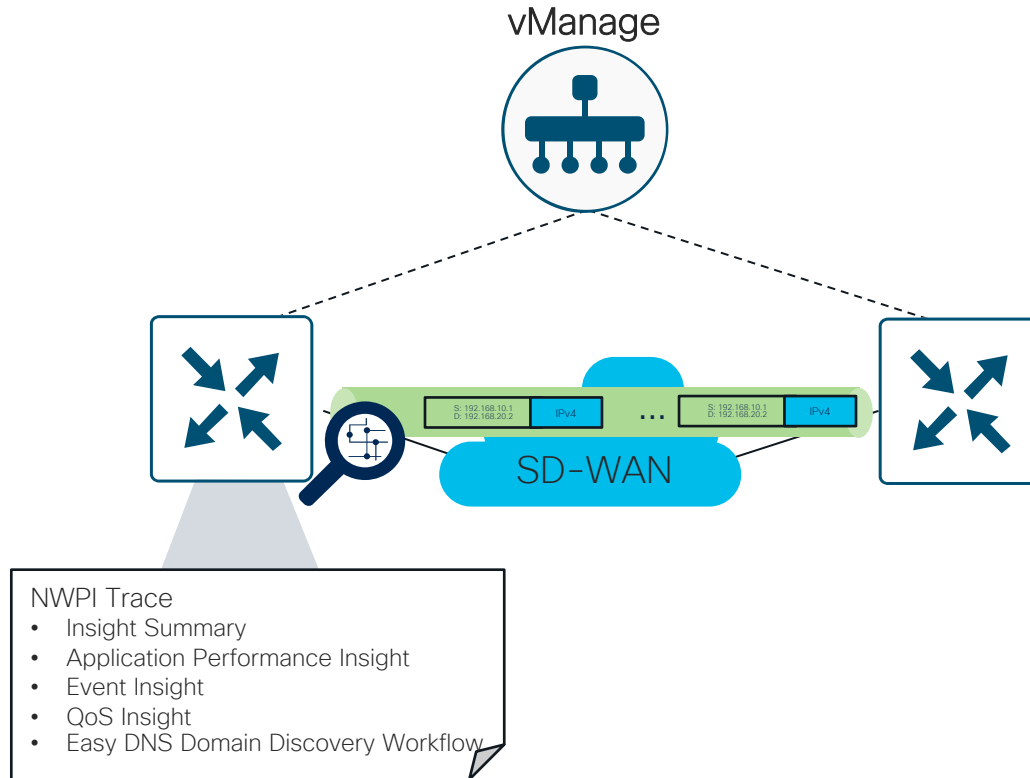
Branch | 10.0.0.100 Site ID: 100 Device Model: C1111-8PLTEEA ⓘ

Device Options:

- Appqoe Expired Flows Summary
- Appqoe Active Flow details
- Appqoe Expired Flow details
- ARP Table
- BFD History
- BFD Sessions**
- BFD Summary
- BFD TLOC Summary List
- BGP Neighbors
- BGP Routes
- BGP Summary
- Bridge Interface
- Bridge MAC
- Bridge Table
- Cellular Connection
- Cellular Hardware

System IP 10.0.0.1

Network Wide Path Insight (NWPI)

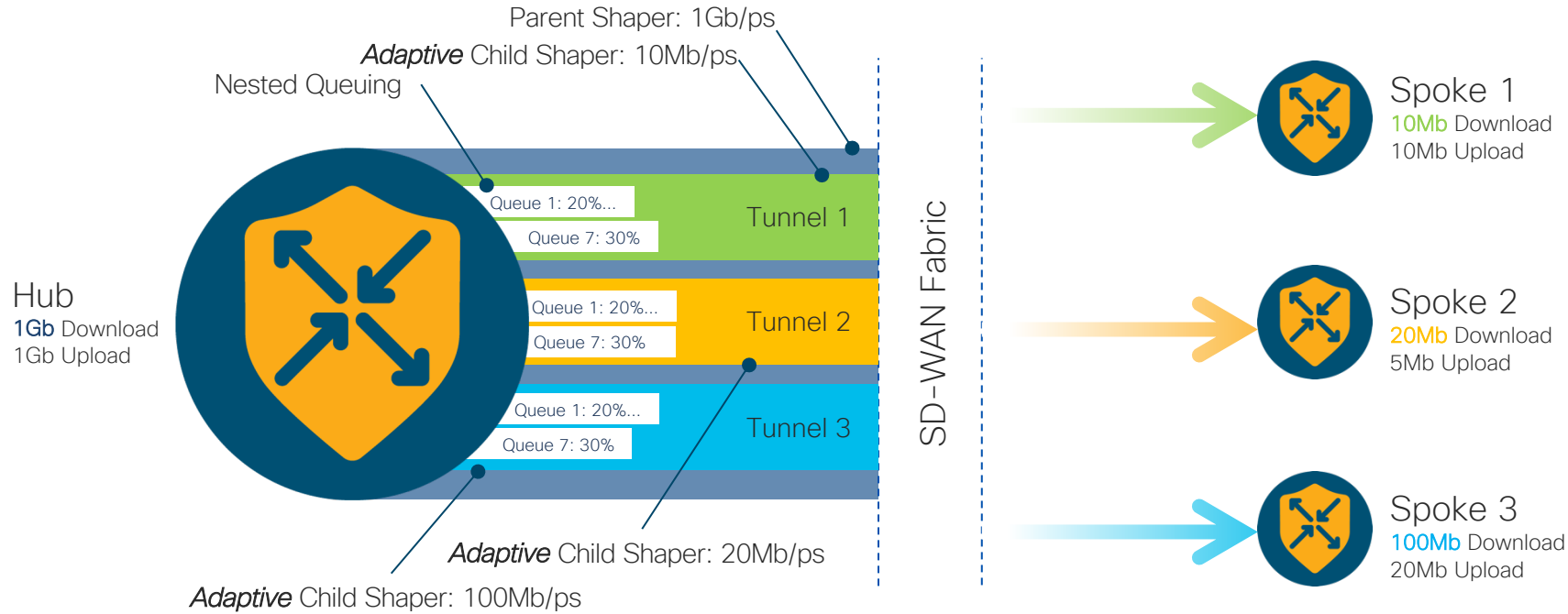


Network Wide Path Insight Demo

Additional SD-WAN Features



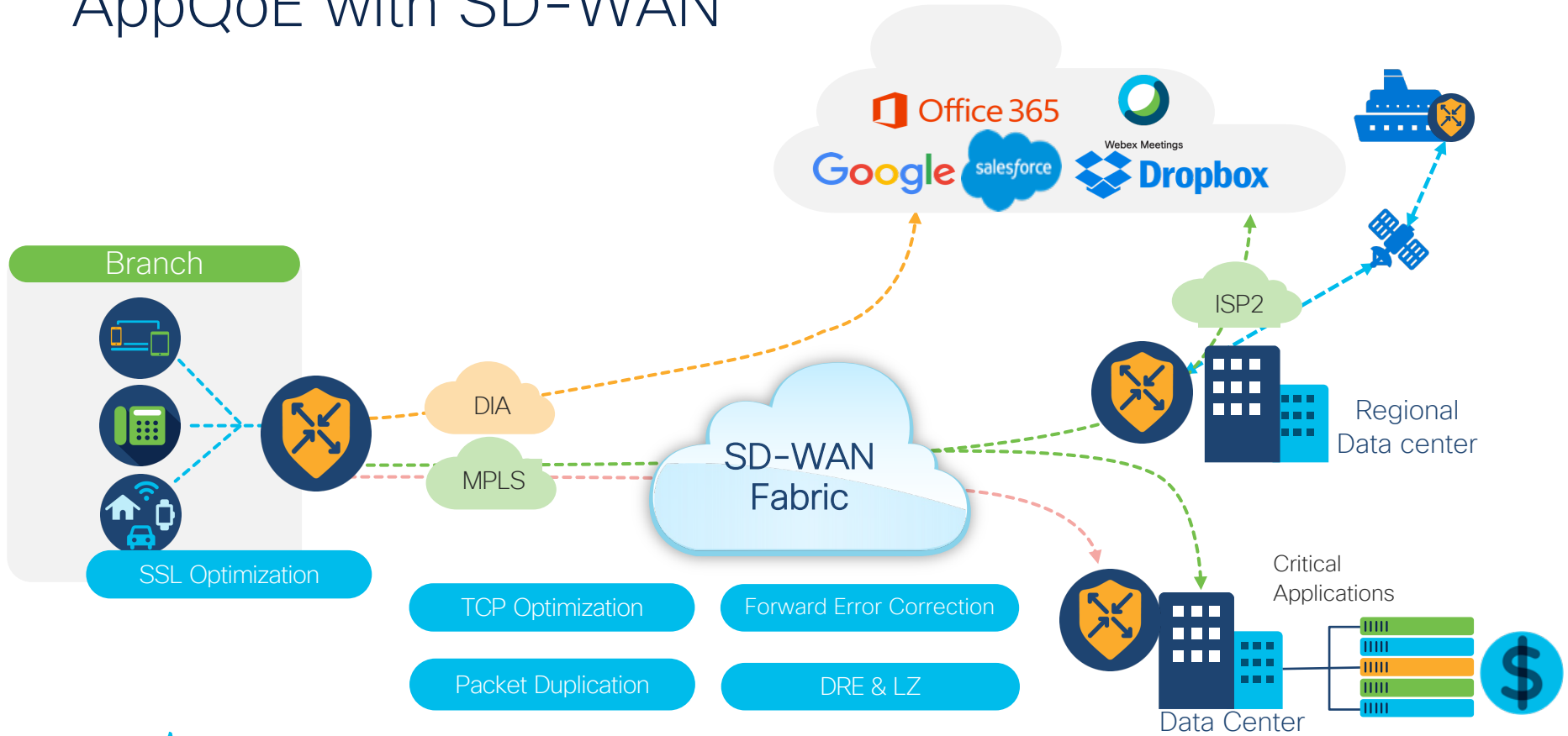
Per-Tunnel QoS with Adaptive Shaping





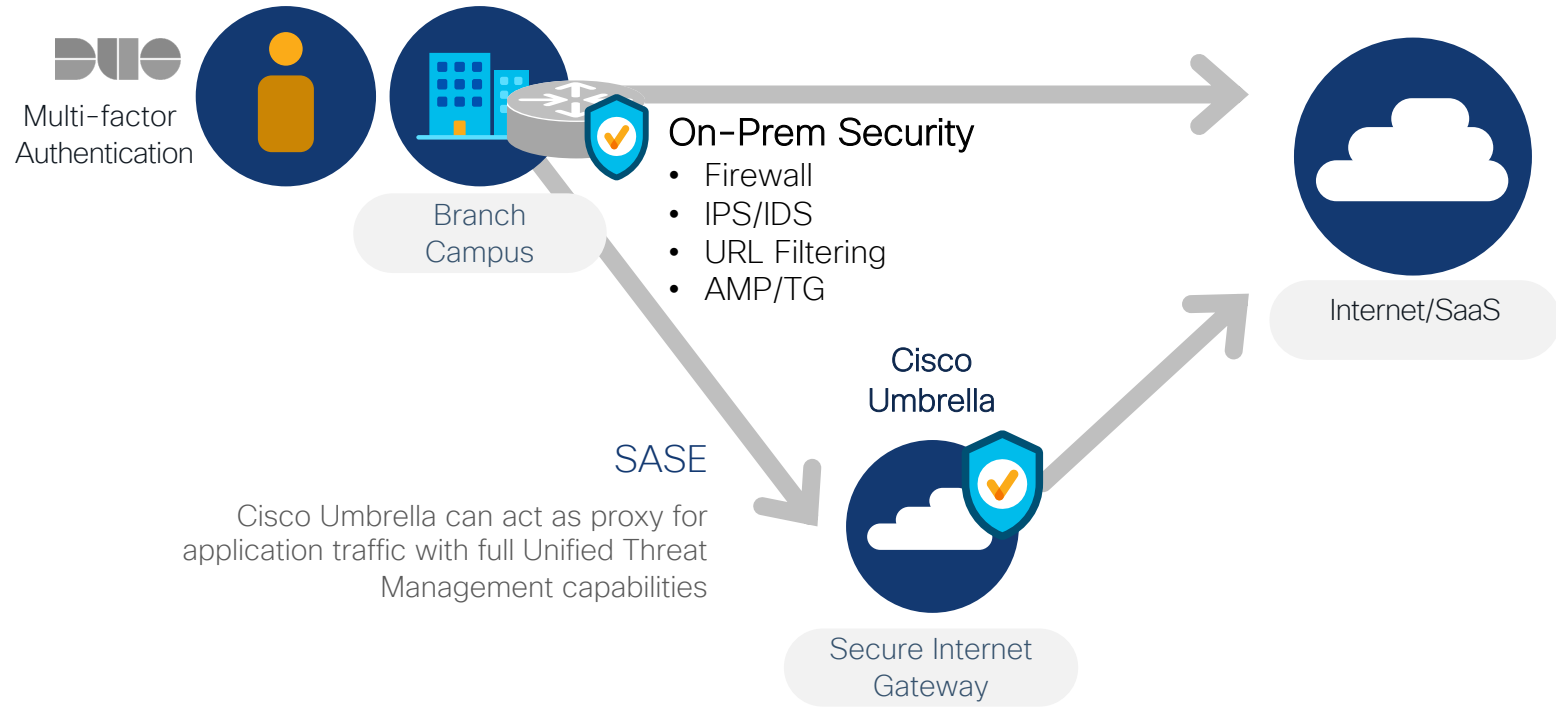
For Your Reference

AppQoE with SD-WAN



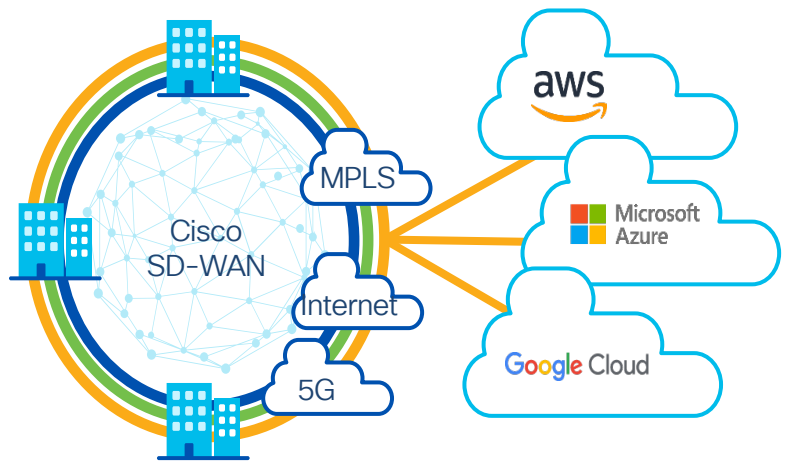


SD-WAN Security

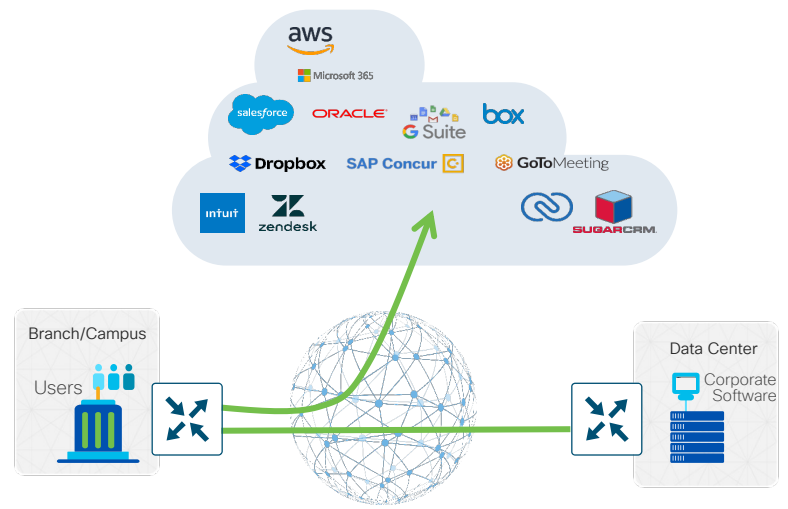




Cloud Ready WAN



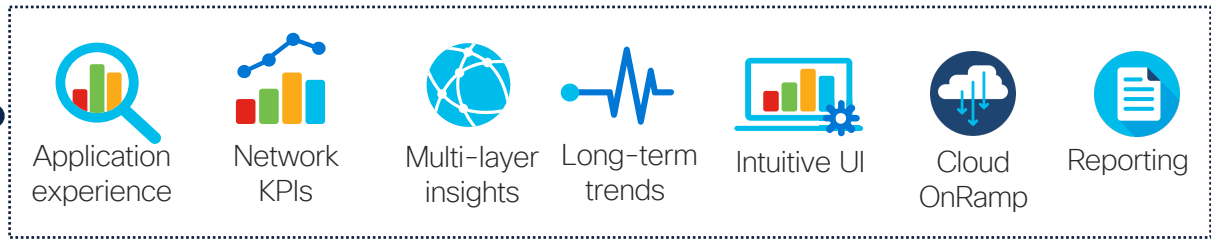
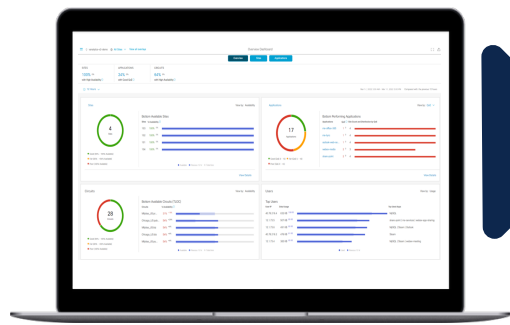
Secure and resilient
IaaS cloud-networking.



Optimized SaaS access and
performance visibility from all
branches.



vAnalytics: Translate Raw Data into Intelligent Insights



Intuitive Visualization of application experience and historical trends

Correlated Insights to expedite root cause isolation

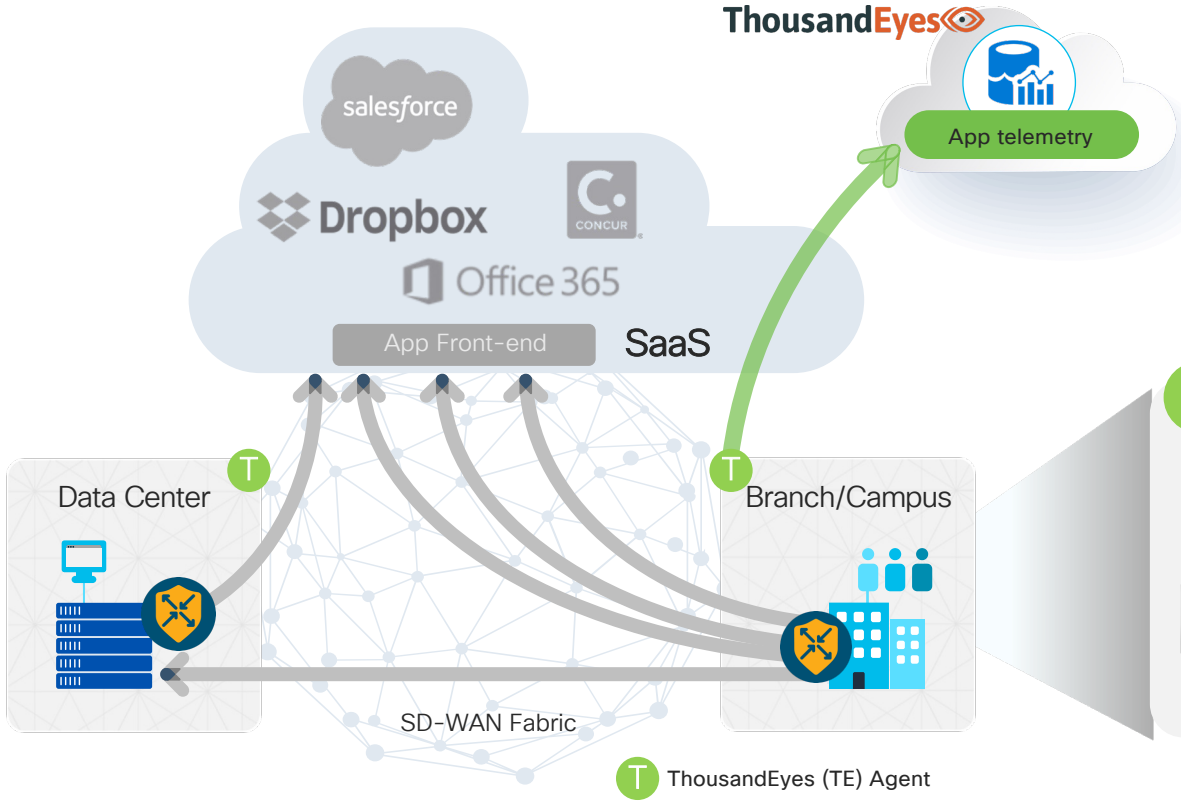
Leverage Insights for better planning

Robust, Scalable, Cloud-hosted SaaS Service



Cisco SD-WAN Enhanced Visibility

ThousandEyes



- 1 Cisco SD-WAN measures network path telemetry
- 2 Cisco ThousandEyes measures application telemetry
- 3 Cisco SD-WAN can adjust traffic based on either

T

ISR/C8K Native (Container)

ISR4K with UCSE/SSD

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.

SD-WAN at Cisco Live

START

● **Monday-Thursday**
LABENT-2490
Understanding SD-WAN Overlay Management Protocol (OMP)

● **LABENT-2570**
Unified Security Policy in Cisco SD-WAN

● **LABENT-2581**
Adaptive QoS in Cisco SD-WAN

● **LABENT-2203**
Cisco SD-WAN and ThousandEyes

● **LABENT-1348**
Cisco SD-WAN vAnalytics & WAN Insights Operations

● **Tuesday | 08:30**
BRKENT-1656
Beginner's Guide to Enterprise Network Monitoring with TE

● **Tuesday | 15:30**
BRKENT-2139
How to Choose the Correct Branch Router

● **Wednesday | 08:30**
LTRENT-2496
SD-WAN Migration Lab

● **Wednesday | 14:00**
LTRENT-2314
SD-WAN Advanced Lab

● **Wednesday | 16:45**
BRKENT-2060
Cisco SD-WAN Cloud OnRamp for Multicloud

● **Thursday | 12:00**
BRKENT-2312
Evolution of Cisco SD-WAN Security and Journey Towards SASE

● **Thursday | 12:30**
BRKENT-2296
Designing On-Prem SD-WAN Controllers

● **Thursday | 14:15**
BRKENT-3412
How to Optimize SaaS Applications using Cisco SD-WAN

● **Thursday | 15:45**
BRKENT-2126
Three Steps to Gain Actionable Visibility in the Cisco SD-WAN Using ThousandEyes

FINISH

Complete your 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 (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>





The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN