You make **possible**

Cisco SDWAN

Technical Deep-dive

Chandra Balaji
Hamzah Kardame
Marty Ma
Steve Wood

TECCRS-2014

Barcelona | January 27-31, 2020

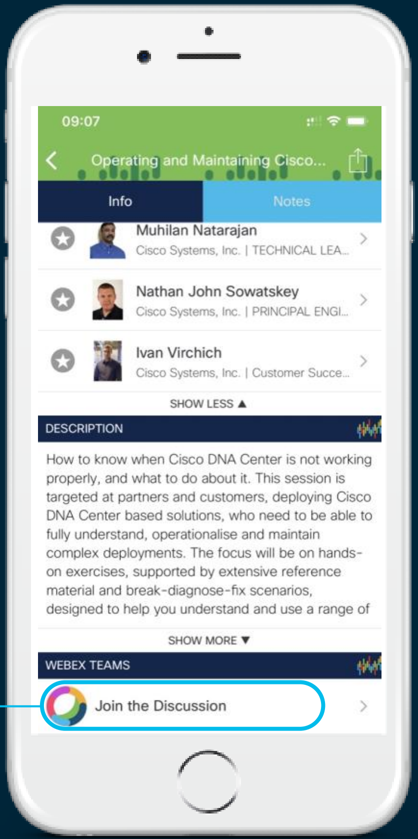
Cisco Webex Teams

Questions?

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

How

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



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

Agenda

Time	Duration	Topic	Presenter
8:30-8:40	0:10	Kick-Off / Presenters Intro	All
8:40-10:30	1:50	Introduction and Background	Steve Wood
		Solution Architecture Overview	Steve Wood
		The Fabric	Steve Wood
10:30-10:45	0:15	Break	
10:45-12:45	2:00	Overlay Management Protocol	Marty
		Policies	Marty
12:45-14:30	1:45	Lunch	
14:30-16:30	2:00	Security	Chandra
		Cloud	Chandra
		Colocations	Chandra
		Application Quality of Experience	Chandra
16:30-16:45	0:15	Break	
16:45-18:35	1:50	Management and Operations	Hamzah
		Deployment Use Cases	Hamzah
		Demo	Hamzah
18:35-18:45	0:10	Wrap-up	All

Introduction and Background

About the jargon...

vEdge – Viptela vEdge Router

cEdge – ISR/ASR/Virtual Router

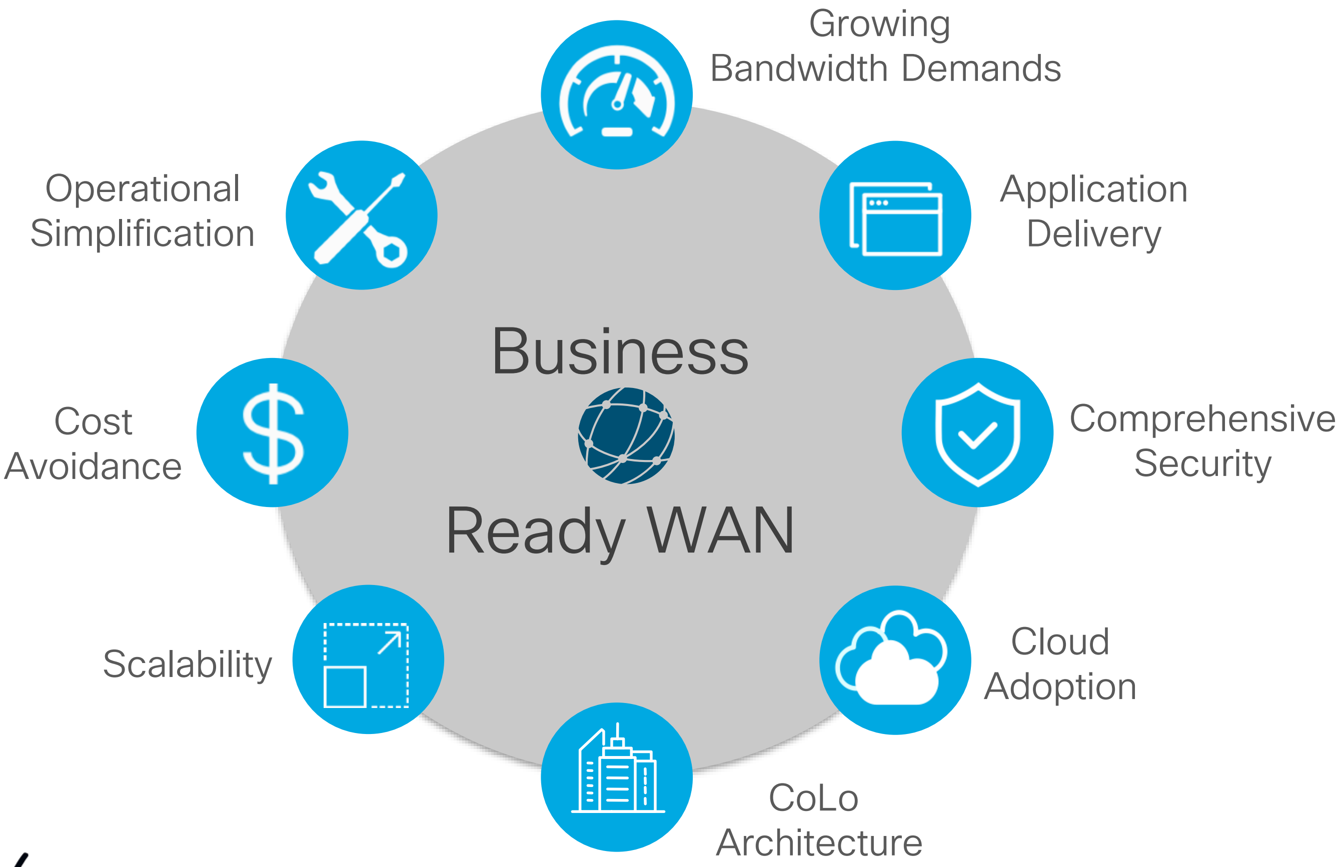
i.e. an SDWAN router

vSmart - controller

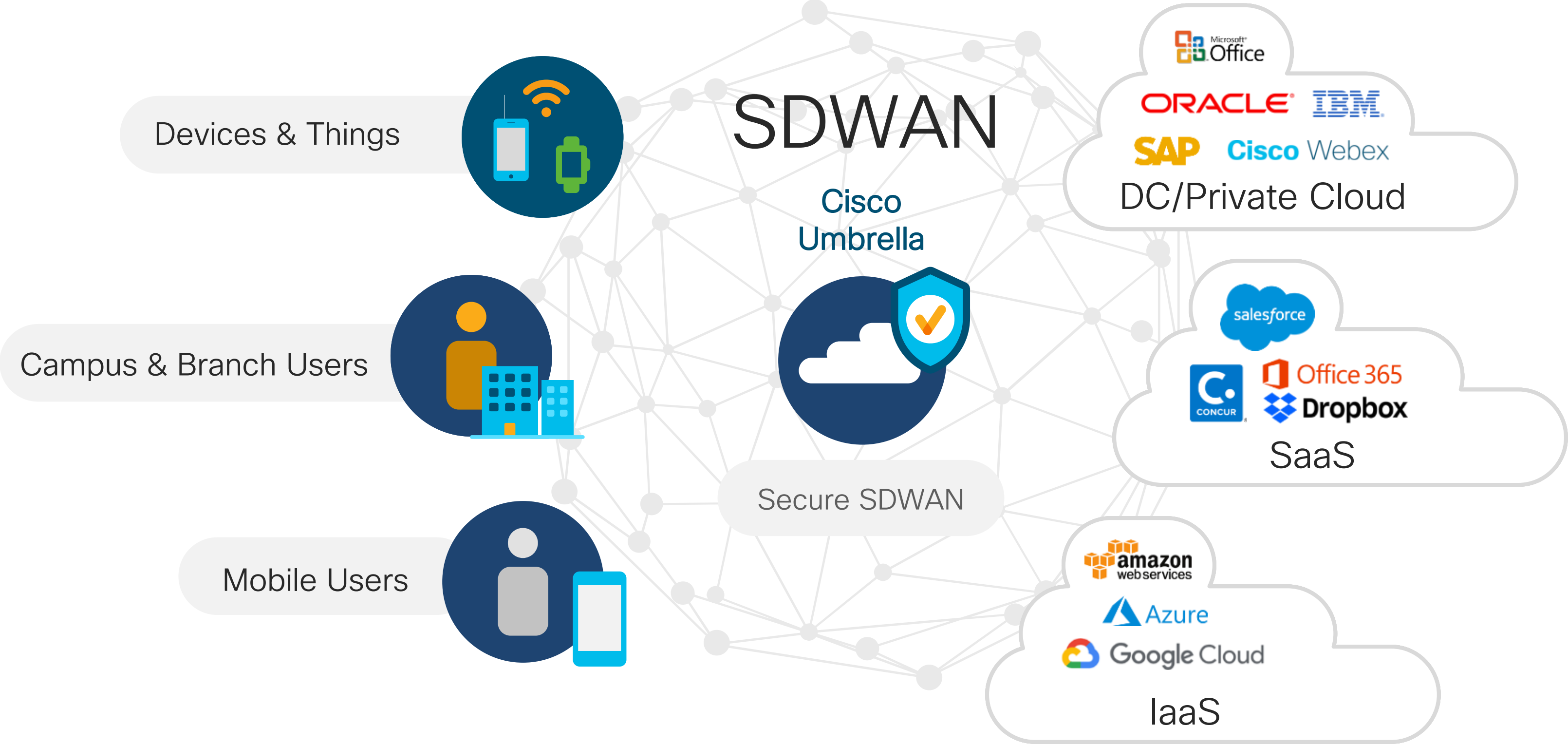
vBond - orchestrator

vManage – Management Application

Trends Driving WAN Transformation



Applications Moving to Not One Cloud, But Many



Devices & Things

Campus & Branch Users

Mobile Users

SDWAN

Cisco Umbrella

Secure SDWAN

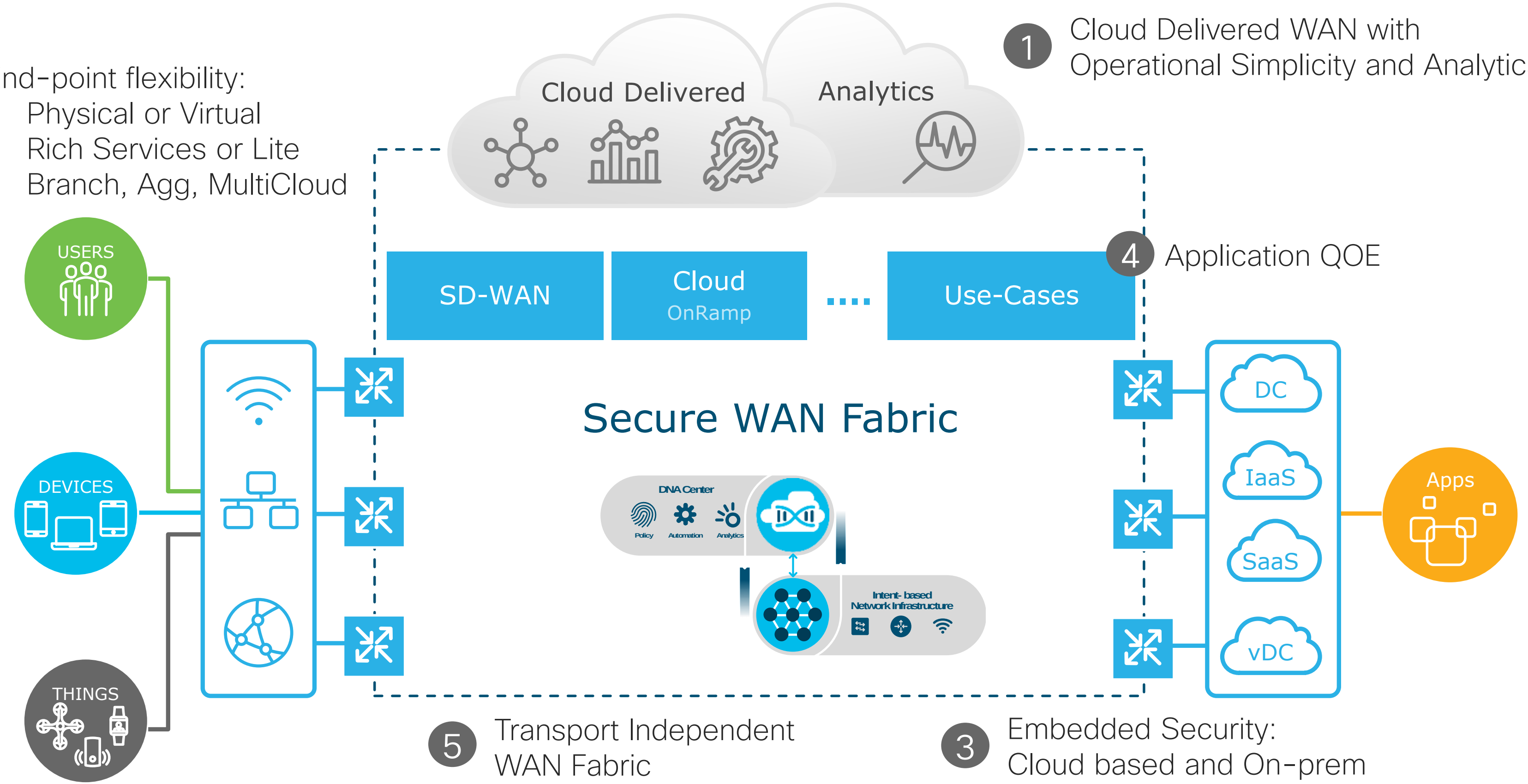
DC/Private Cloud

SaaS

IaaS

More user, things and applications, everywhere

Cisco SD-WAN



1 Cloud Delivered WAN with Operational Simplicity and Analytics

2 End-point flexibility:

- Physical or Virtual
- Rich Services or Lite
- Branch, Agg, MultiCloud

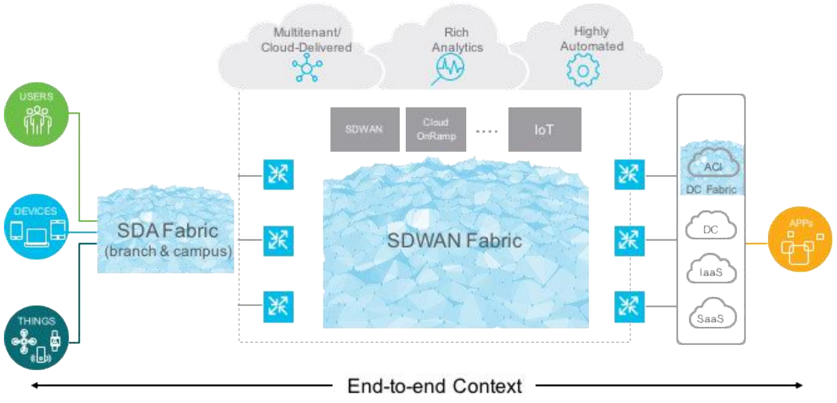
3 Embedded Security: Cloud based and On-prem

4 Application QOE

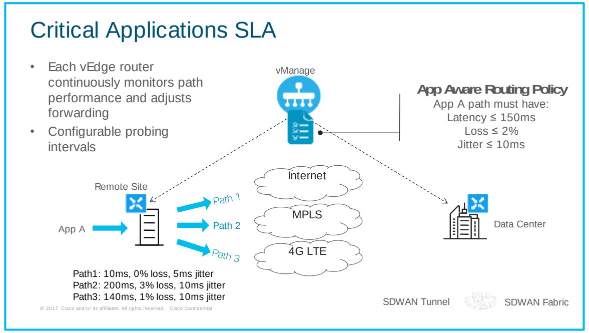
5 Transport Independent WAN Fabric

Why Fabric Architectures

- Single Hop, Input to Output
- Overlay any transport
- Consistent Policy Enforcement Points
- Carry New and Useful Context
- Multidomain User / Device Identity
- Policy control at Fabric Edge
- Simplicity
- Mobility
- Automation



Deployed Use Cases - Sample

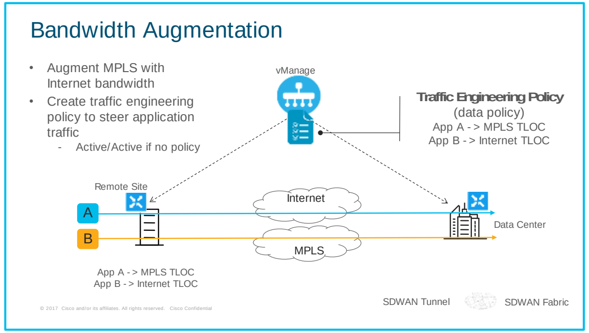


Critical Applications SLA

- Each vEdge router continuously monitors path performance and adjusts forwarding
- Configurable probing intervals

App Aware Routing Policy
App A path must have:
Latency ≤ 150ms
Loss ≤ 2%
Jitter ≤ 10ms

Path1: 10ms, 0% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

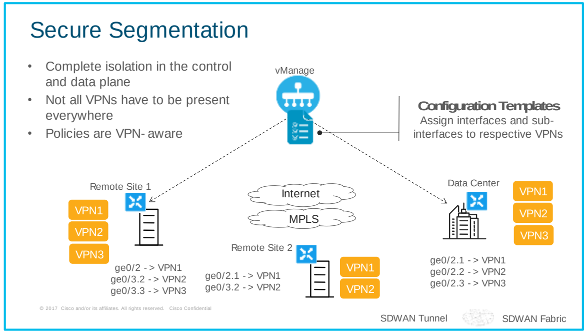


Bandwidth Augmentation

- Augment MPLS with Internet bandwidth
- Create traffic engineering policy to steer application traffic
  - Active/Active if no policy

Traffic Engineering Policy
(data policy)
App A -> MPLS TLOC
App B -> Internet TLOC

App A -> MPLS TLOC
App B -> Internet TLOC



Secure Segmentation

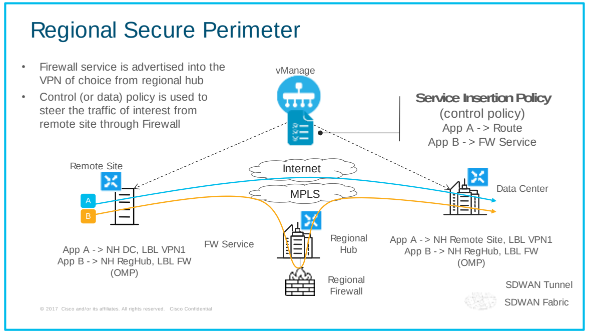
- Complete isolation in the control and data plane
- Not all VPNs have to be present everywhere
- Policies are VPN- aware

Configuration Templates
Assign interfaces and sub-interfaces to respective VPNs

ge0/2 -> VPN1
ge0/3.2 -> VPN2
ge0/3.3 -> VPN3

ge0/2.1 -> VPN1
ge0/3.2 -> VPN2

ge0/2.1 -> VPN1
ge0/2.2 -> VPN2
ge0/2.3 -> VPN3



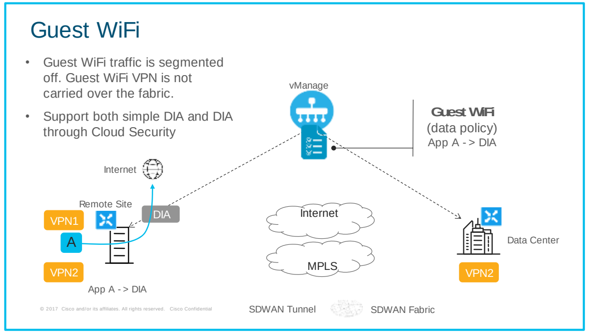
Regional Secure Perimeter

- Firewall service is advertised into the VPN of choice from regional hub
- Control (or data) policy is used to steer the traffic of interest from remote site through Firewall

Service Insertion Policy
(control policy)
App A -> Route
App B -> FW Service

App A -> NH DC, LBL VPN1
App B -> NH RegHub, LBL FW
(OMP)

App A -> NH Remote Site, LBL VPN1
App B -> NH RegHub, LBL FW
(OMP)

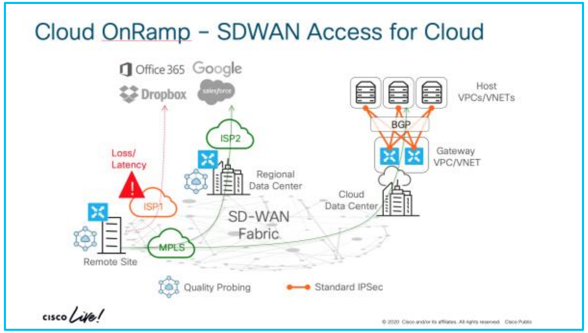


Guest WiFi

- Guest WiFi traffic is segmented off. Guest WiFi VPN is not carried over the fabric.
- Support both simple DIA and DIA through Cloud Security

Guest WiFi
(data policy)
App A -> DIA

App A -> DIA

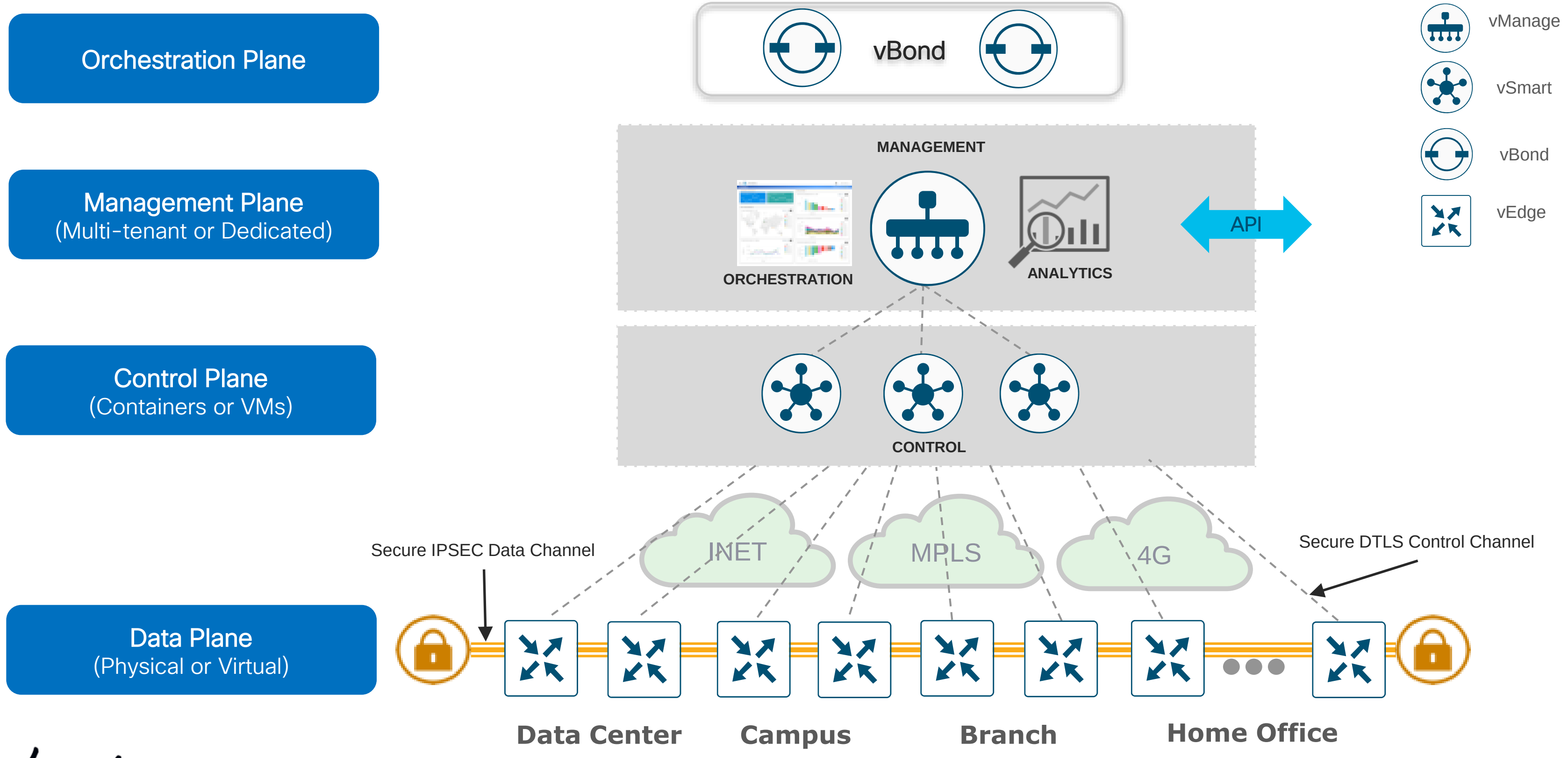


Cloud OnRamp - SDWAN Access for Cloud

Solution Architecture Overview

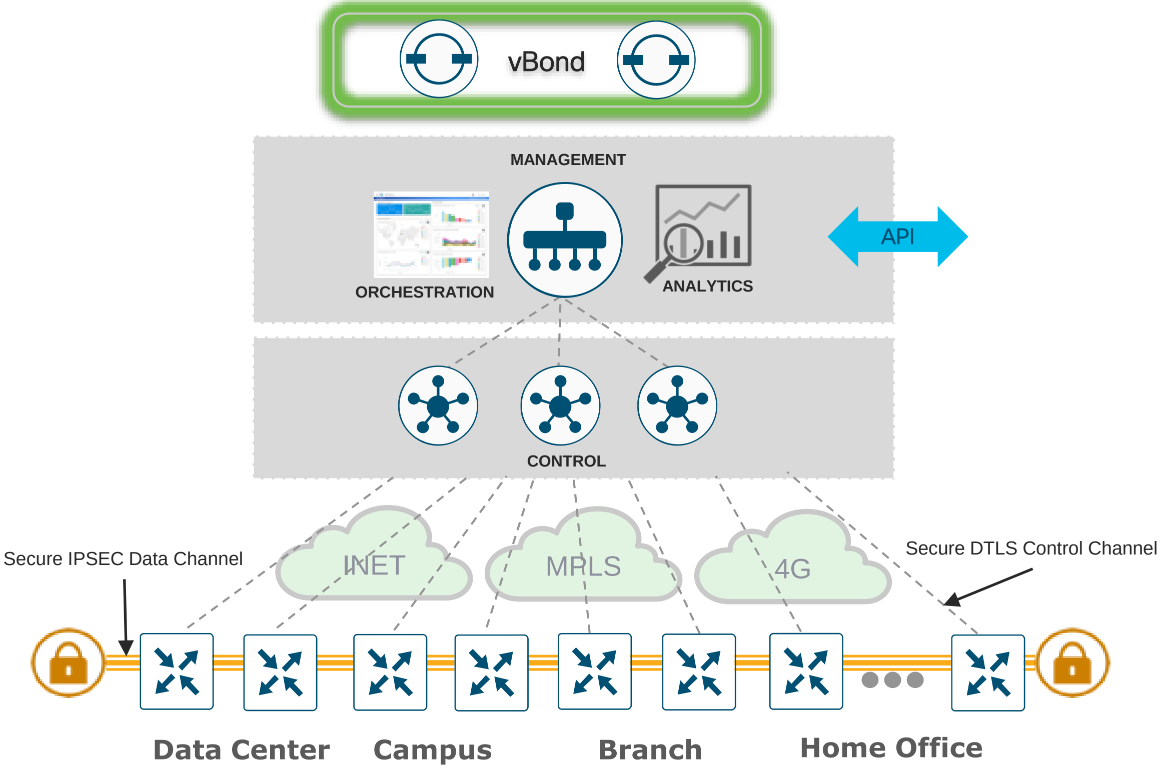
Cisco SD-WAN Solution Overview

Applying SDN Principles To The Wide Area Network



Orchestration Plane

vBond Orchestrator

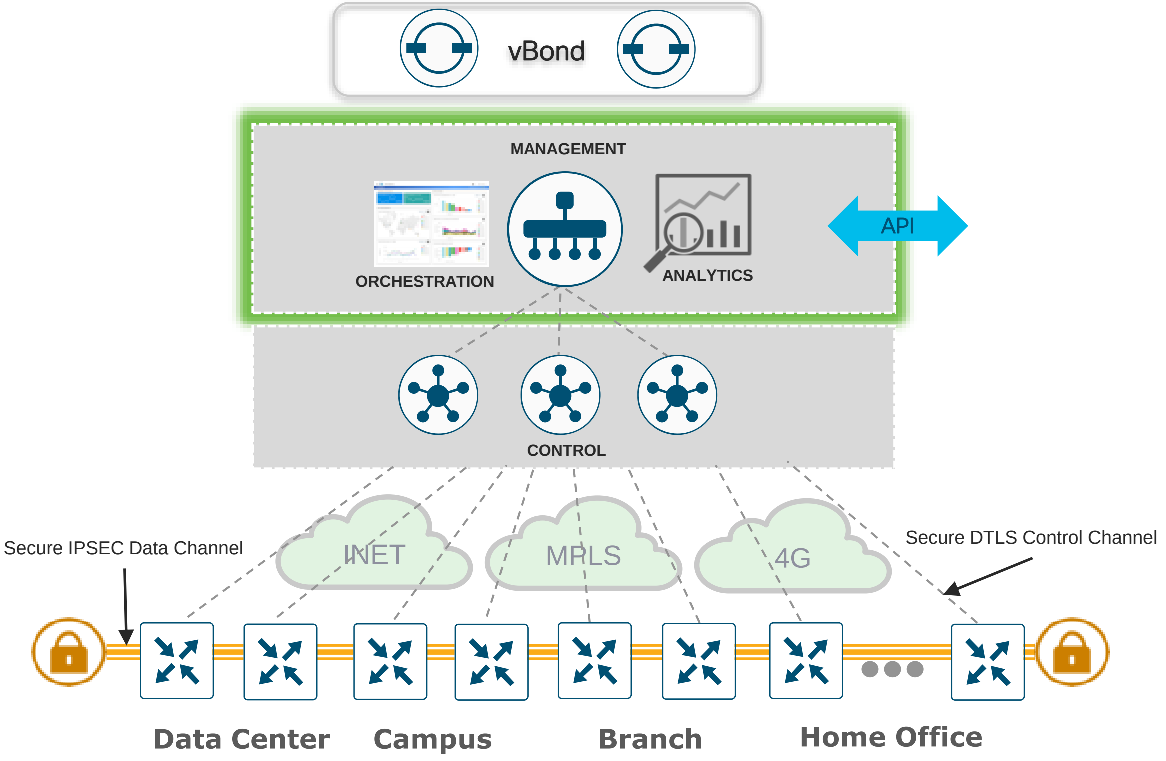


Main Characteristics

- 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

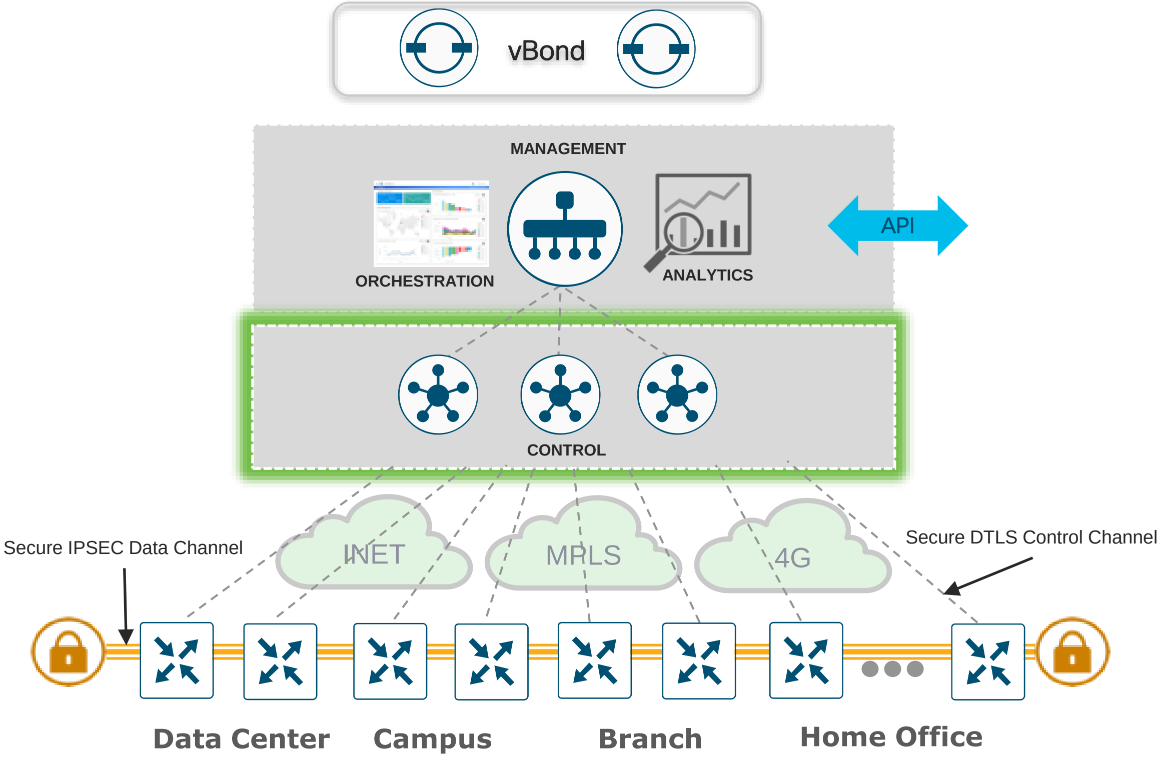


Main Characteristics

- 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



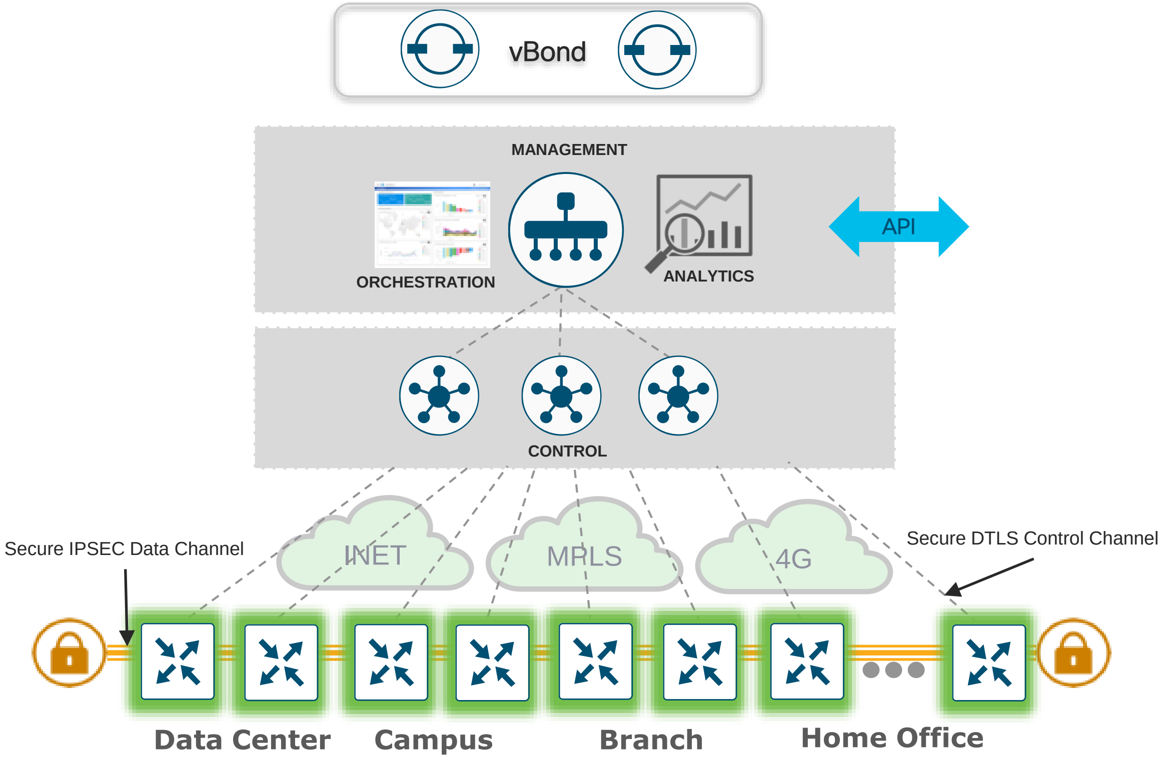
Main Characteristics

- 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

cisco Live!

Data Plane

vEdge Router



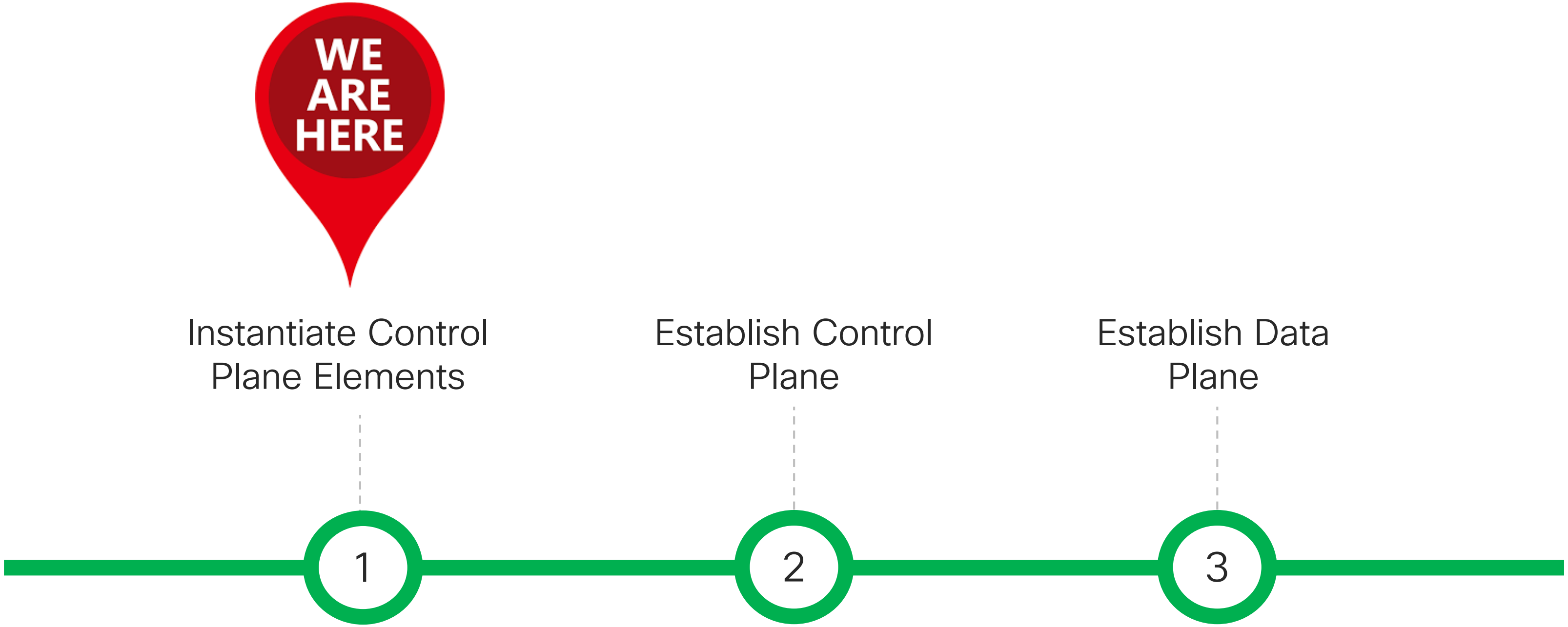
Main Characteristics

- WAN edge router
- Provides secure data plane with remote vEdge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Enforce Policies for Data plane and application aware routing.
- 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+)

The Fabric

Deploying Fabric Control Plane

1, 2, 3 … Fabric



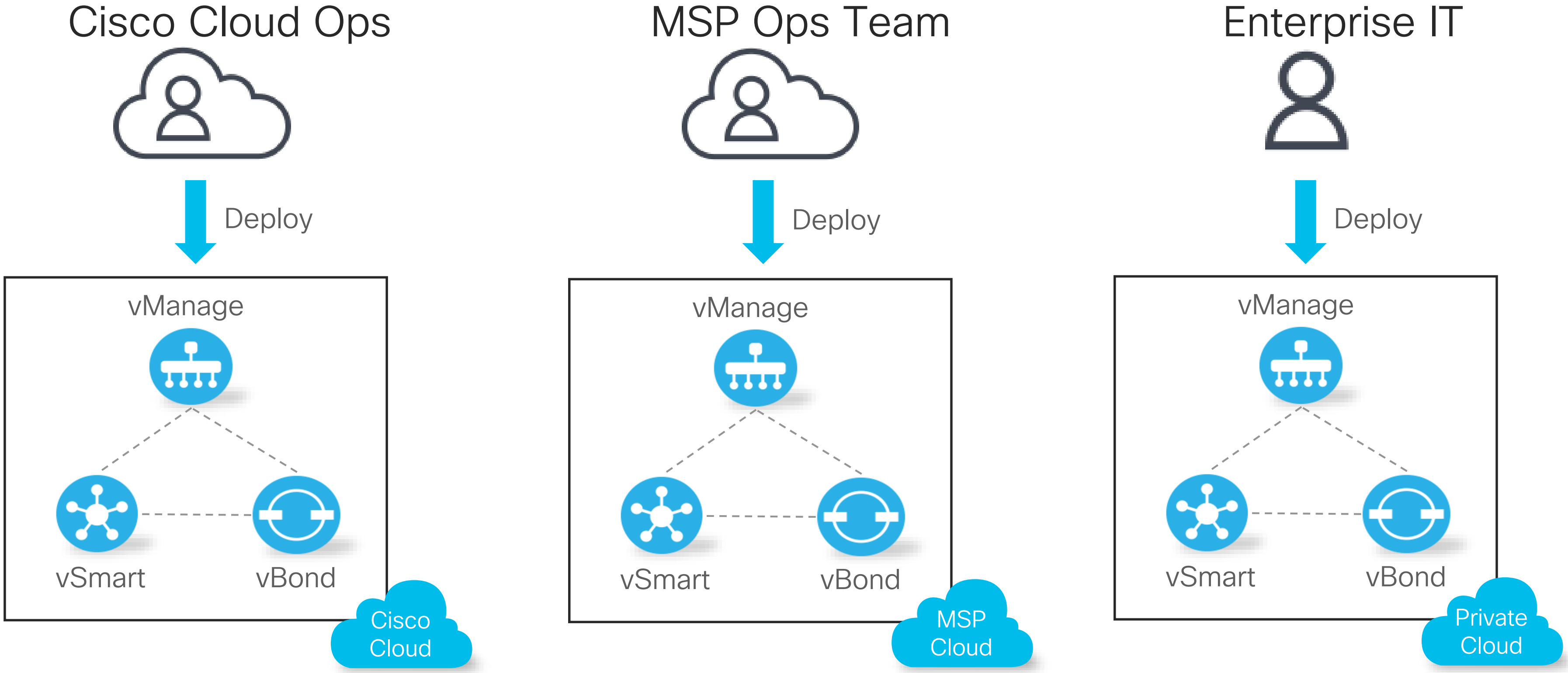
Instantiate Control Plane Elements

Establish Control Plane

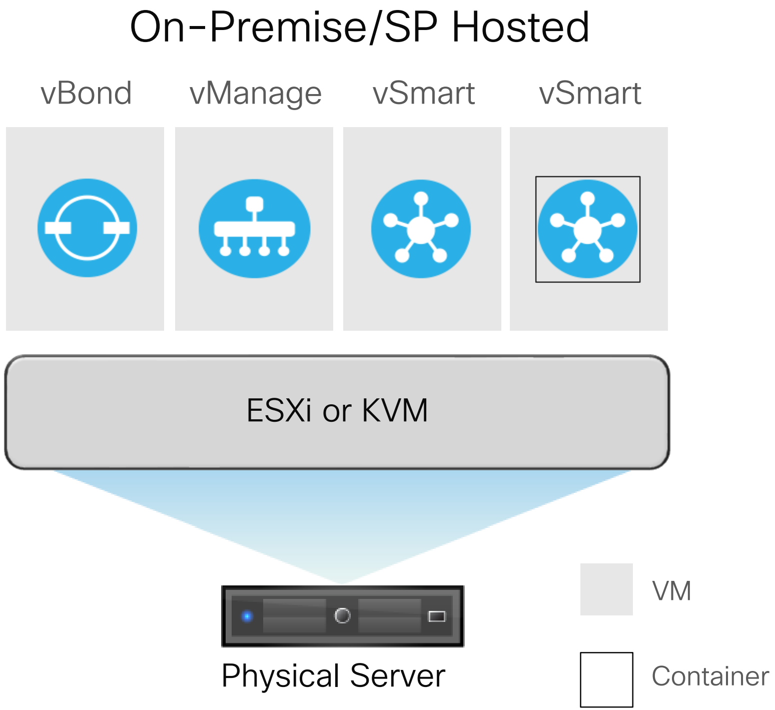
Establish Data Plane

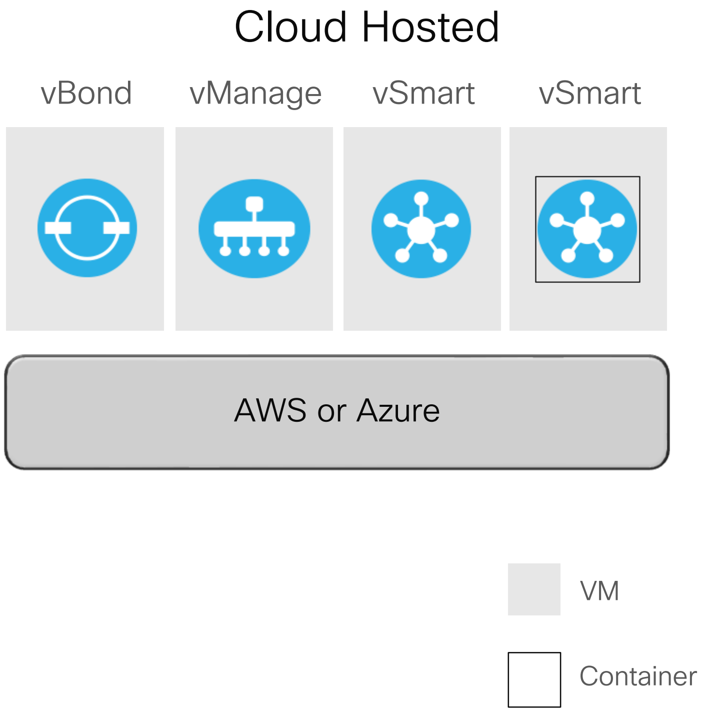
Cloud-Delivered Control

Flexible Deployment Options

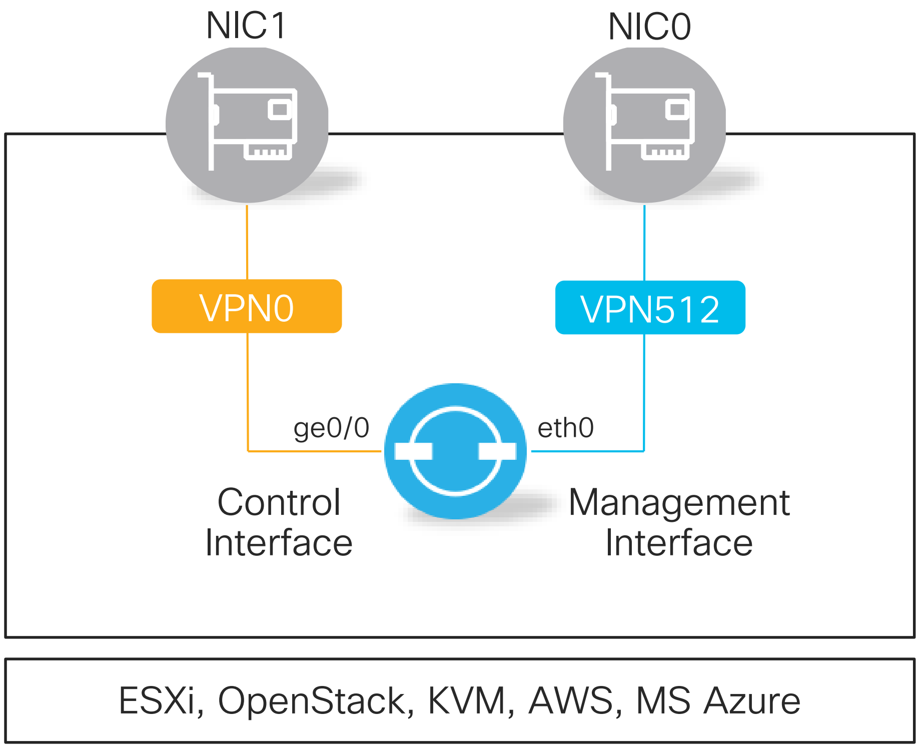


Controllers Deployment Methodology



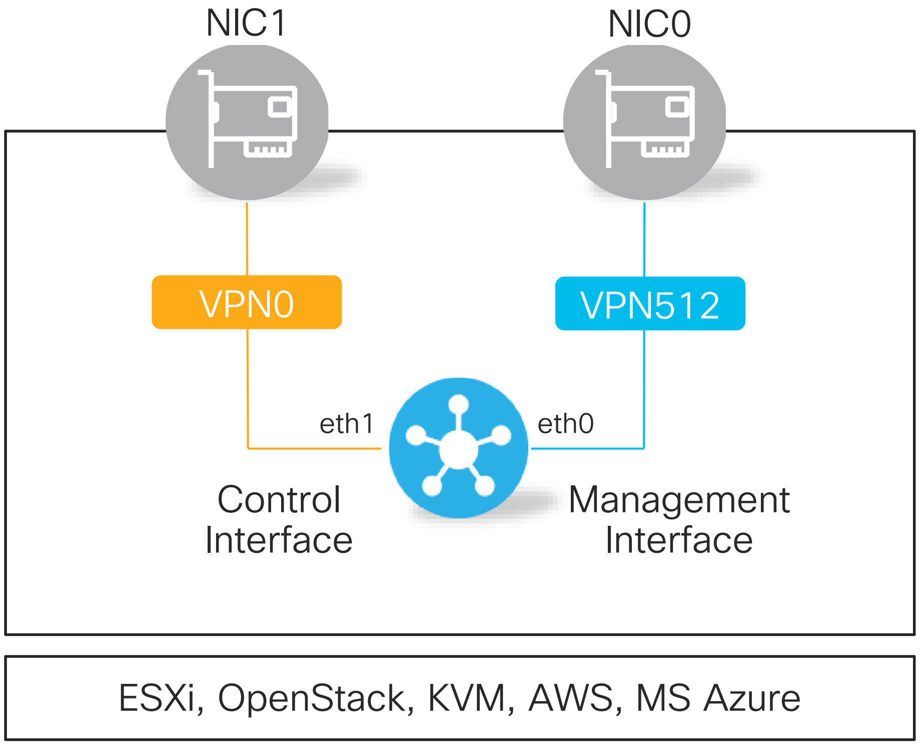


vBond Deployment



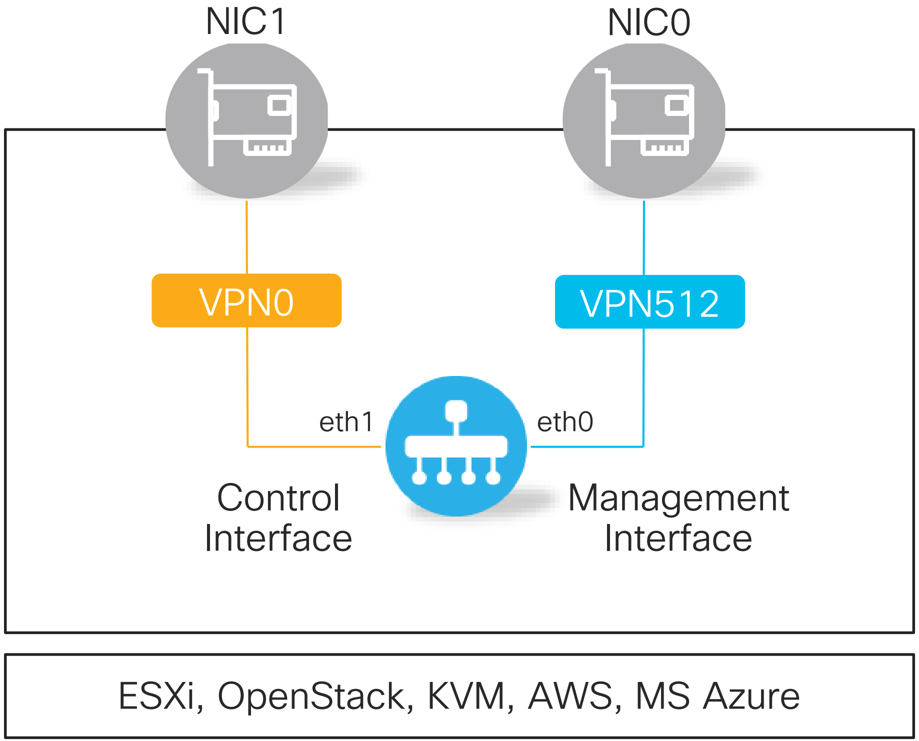
- Virtual machine
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP (local)

vSmart Deployment



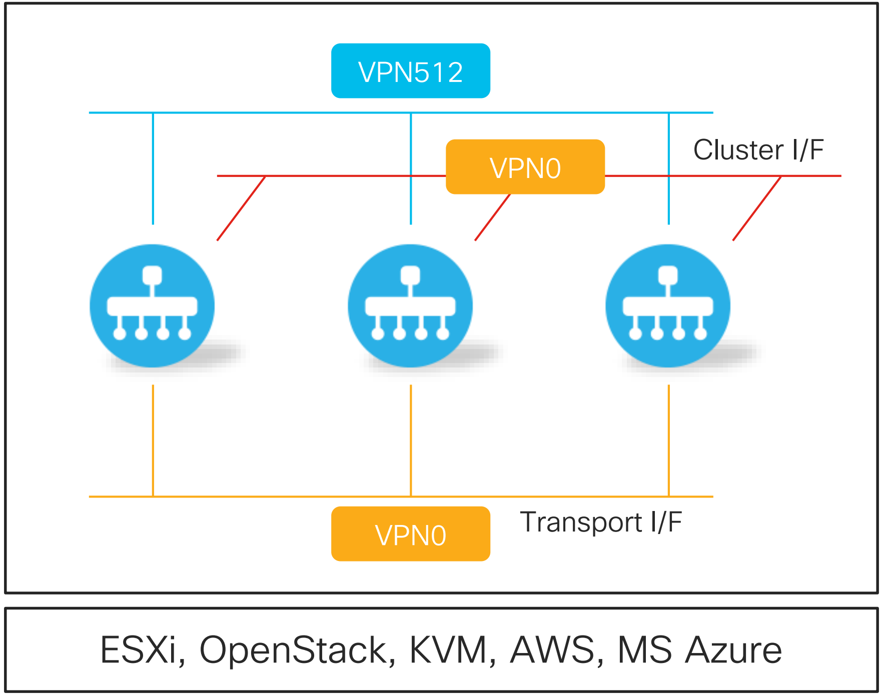
- Virtual machine or container
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP

vManage Deployment



- Virtual machine
- 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

vManage Cluster

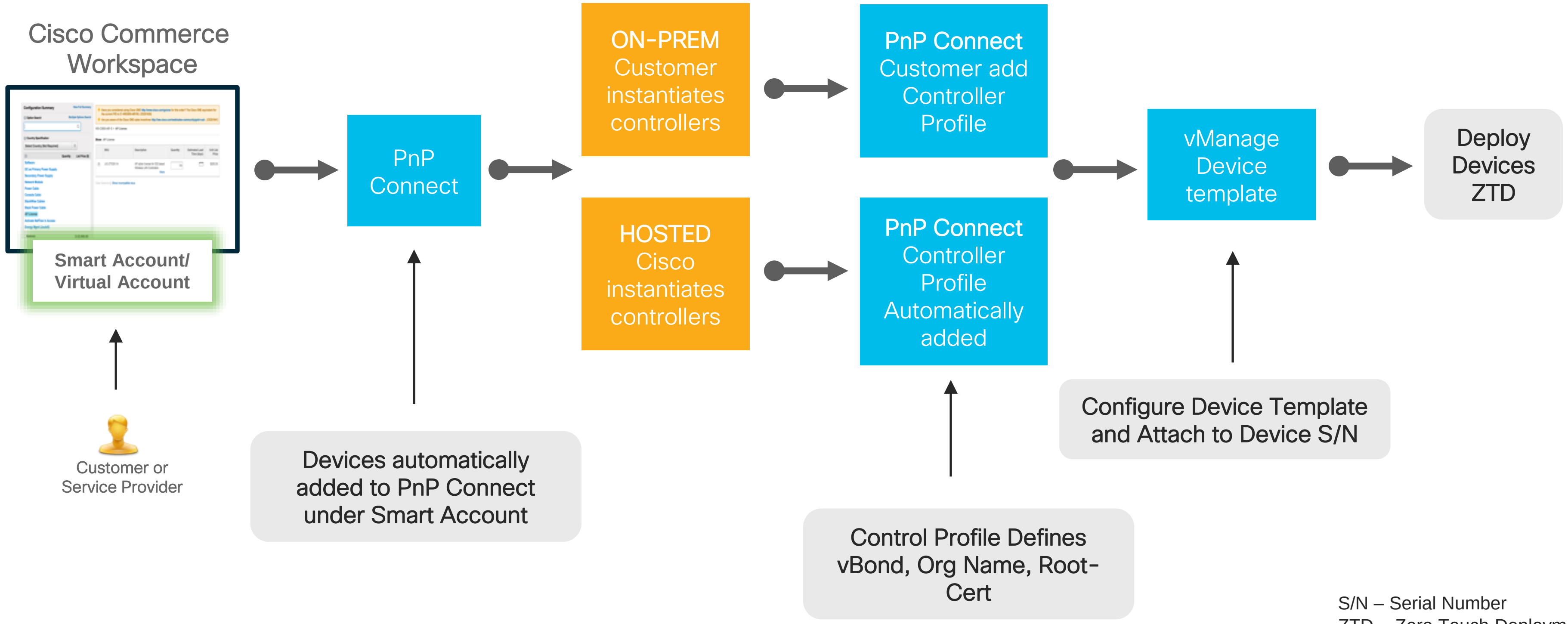


- Reasons to deploy a vManage cluster
  - High availability and redundancy for fault tolerance
  - Managing greater than 2000 WAN Edge routers
  - Distributing NMS service loads
- Not for geo-redundancy!
- The vManage cluster consists of at least three vManage devices
- Dedicated interface in VPN0 for cluster communication
- 1Gb bandwidth between cluster members
- <5ms latency between cluster members

https://techzone.cisco.com/t5/Viptela/vManage-Cluster-Creation-and-Troubleshooting/ta-p/1239794/message-revision/1239794:7

From Order to Zero-Touch Deployment

Overview



Cisco Commerce Workspace

Smart Account/ Virtual Account

Customer or Service Provider

PnP Connect

Devices automatically added to PnP Connect under Smart Account

ON-PREM Customer instantiates controllers

HOSTED Cisco instantiates controllers

PnP Connect Customer add Controller Profile

PnP Connect Controller Profile Automatically added

Control Profile Defines vBond, Org Name, Root-Cert

vManage Device template

Configure Device Template and Attach to Device S/N

Deploy Devices ZTD

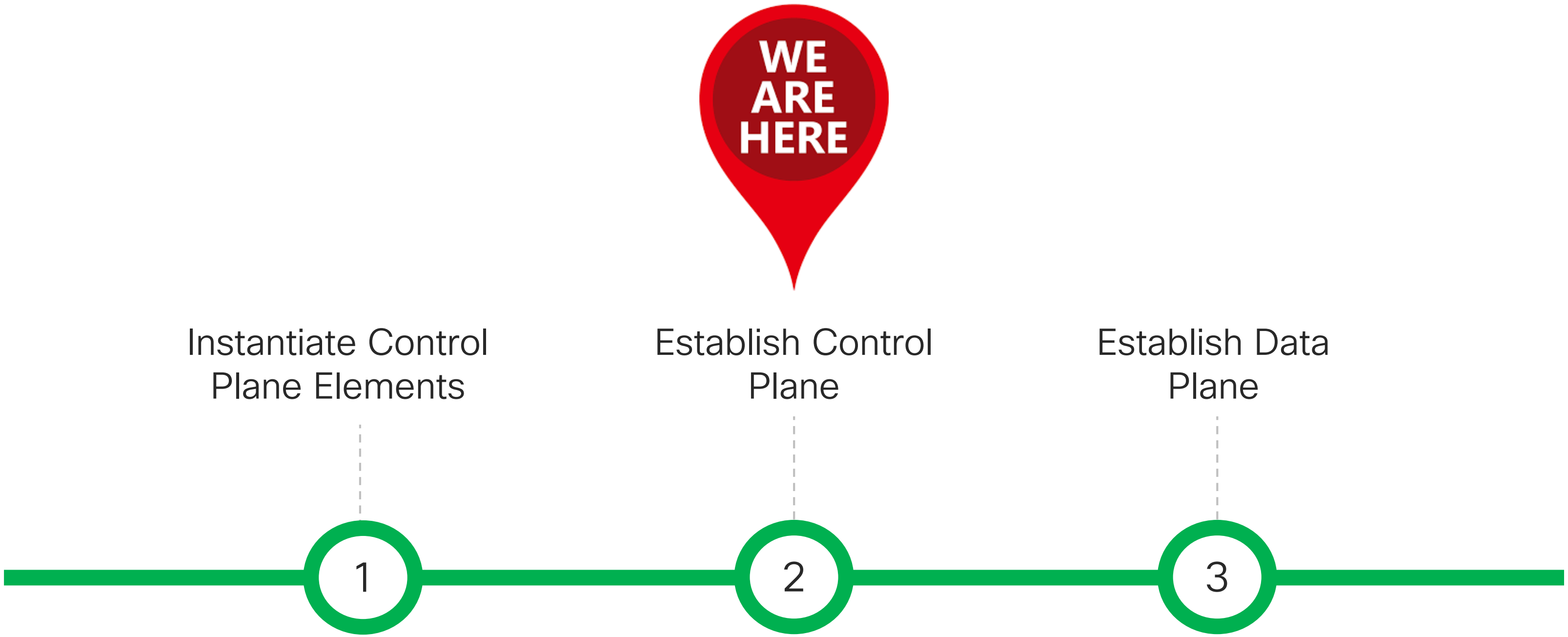
S/N – Serial Number
ZTD - Zero Touch Deployment

cisco Live!

The Fabric

Establishing Control Plane

1, 2, 3 ... Fabric



Instantiate Control Plane Elements

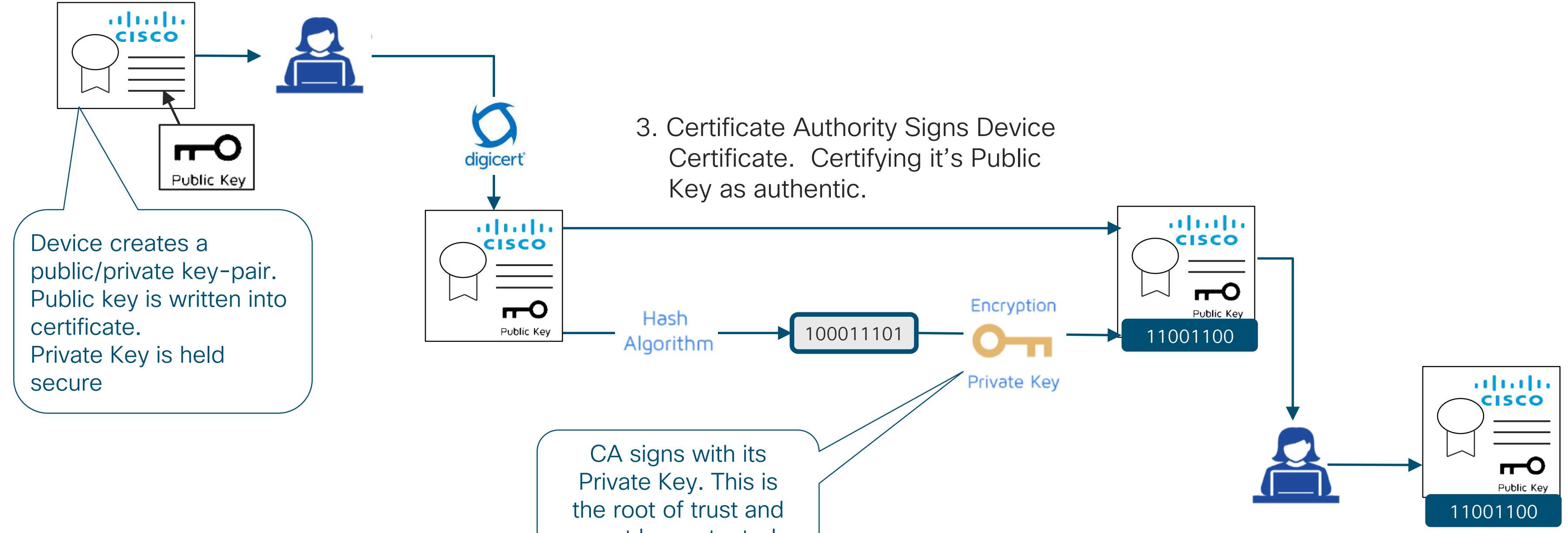
Establish Control Plane

Establish Data Plane

PKI 101: Establishing Device Identity via Certificates

1. Generate Device Certificate (establishes Identity)

2. Owner generates a Certificate Signing Request (CSR)



Device creates a public/private key-pair. Public key is written into certificate. Private Key is held secure

3. Certificate Authority Signs Device Certificate. Certifying it's Public Key as authentic.

CA signs with its Private Key. This is the root of trust and must be protected

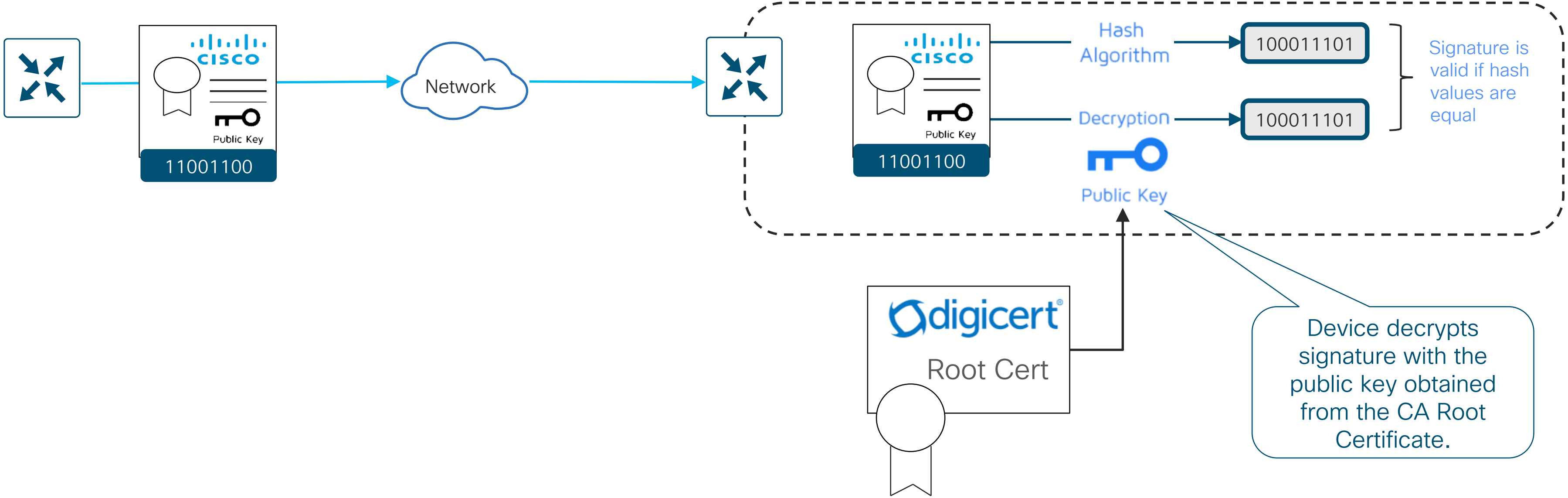
4. Owner installs signed Certificate into Device.

PKI 101: Validating Device Identity via Certificates

1. Client Device Provides Signed Certificate to Server Device

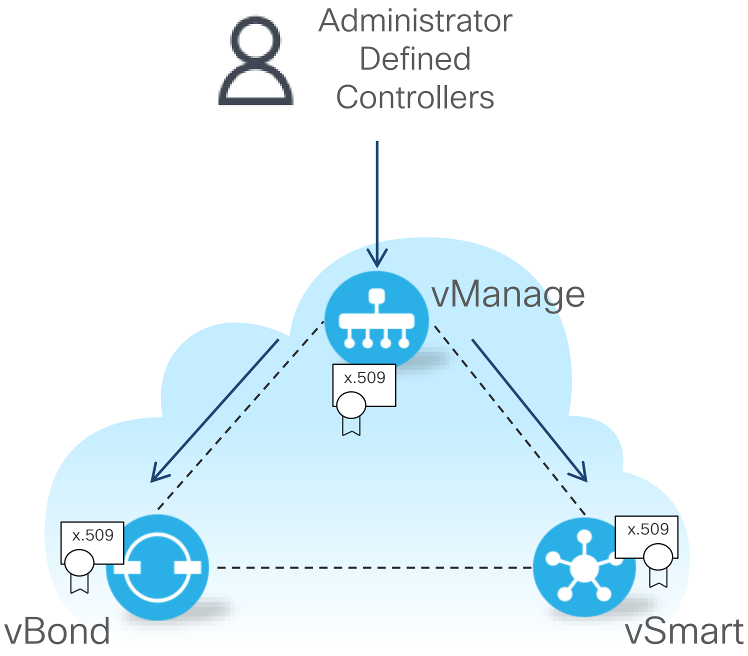
2. Server Device Validates Certificate Signature

3. Client Device now trusted. Client public key can be trusted for use in encryption

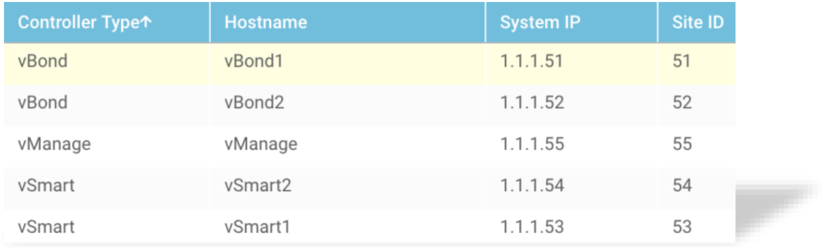


Device decrypts signature with the public key obtained from the CA Root Certificate.

Control Plane Whitelisting



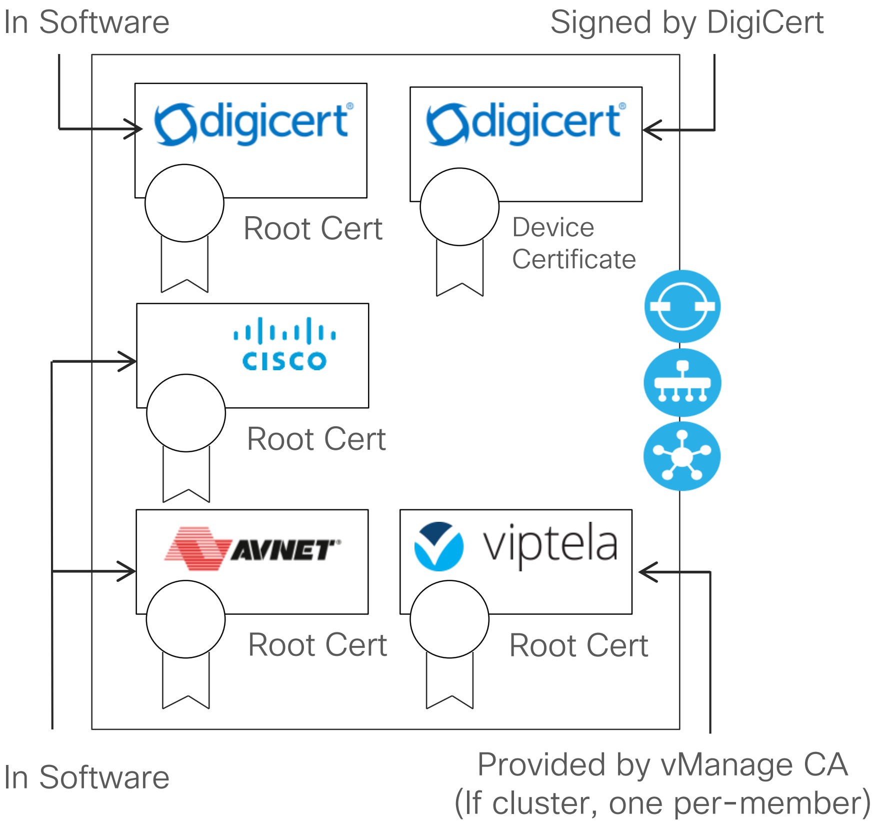
- Administrator adds controllers in the vManage GUI



Controller Type↑	Hostname	System IP	Site ID
vBond	vBond1	1.1.1.51	51
vBond	vBond2	1.1.1.52	52
vManage	vManage	1.1.1.55	55
vSmart	vSmart2	1.1.1.54	54
vSmart	vSmart1	1.1.1.53	53

- Automated certificate signing through DigiCert
  - Can use Enterprise CA
- Controllers list is distributed by vManage to all the controllers
  - Controllers’ certificates serial numbers

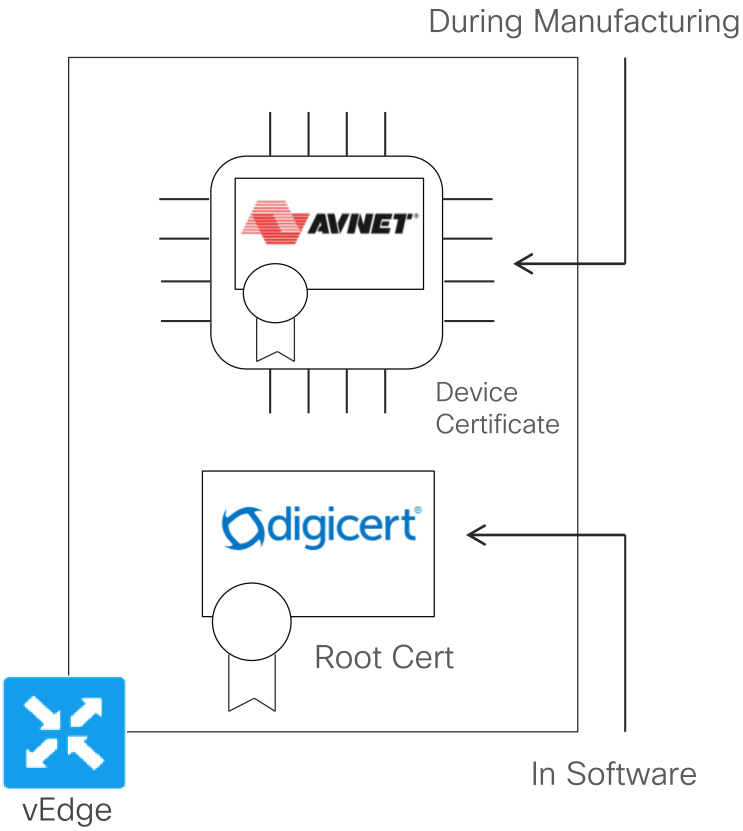
Controllers Identity



- **Device Certificate*** – Own identity (SHA256)
- **DigiCert** Root Chain** – Trust for other controllers' certificates
- **Avnet Root Chain** – Trust for vEdge routers' certificates
- **Cisco Root Chain** – Trust for Cisco routers' certificates (with SUDI)
- **Viptela Root Chain (vManage)** – Trust for vEdge Cloud routers' and Cisco routers' (without SUDI) certificates

* Can use Enterprise CA Certificate
** Can use Enterprise CA Root Chain

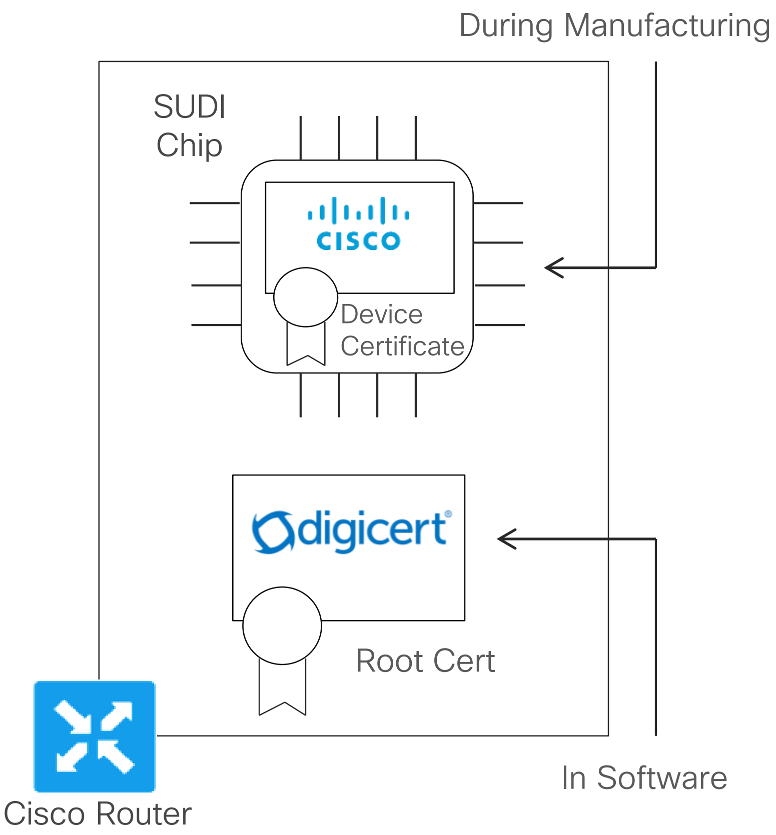
vEdge Router Identity



- **Device Certificate** – Own identity (SHA1)
- **DigiCert* Root Chain** – Trust for controllers' certificates

* Can use Enterprise CA Root Chain. Can be loaded during ZTP.

Cisco Router Identity (with SUDI)

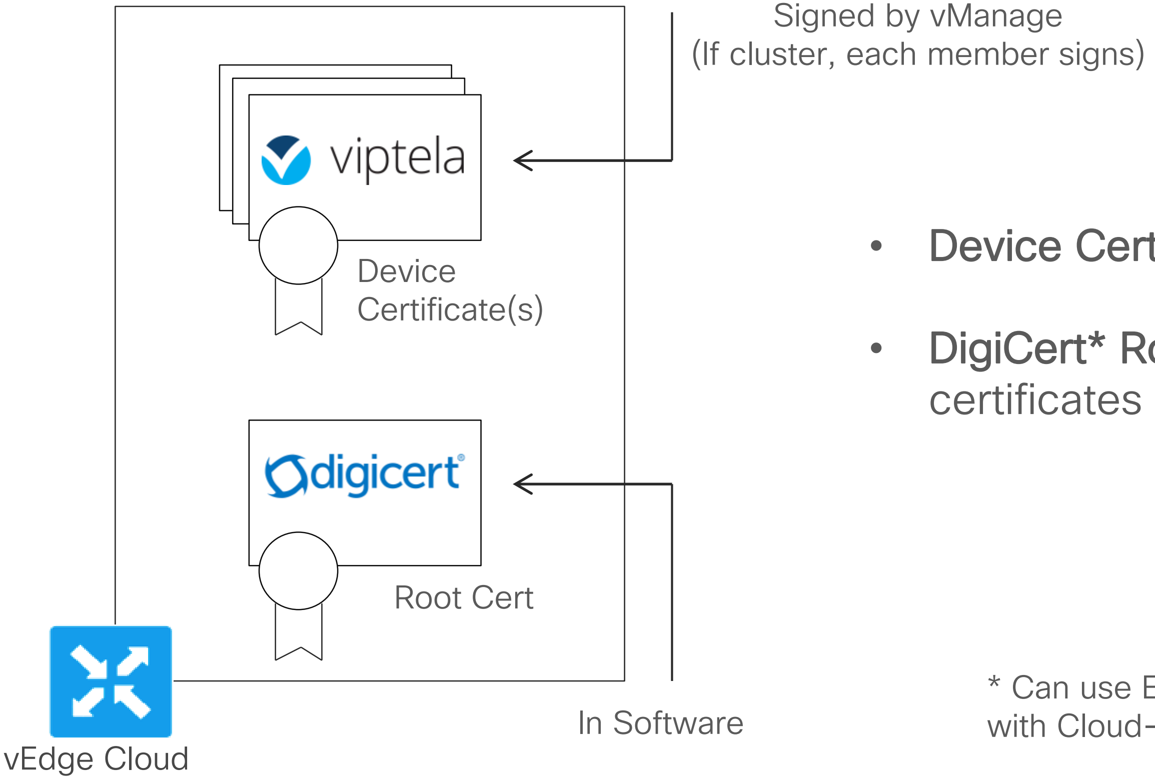


- **Device Certificate** – Own identity (SHA256)
- **DigiCert* Root Chain** – Trust for controllers' certificates

* SUDI = Secure Unique Device Identifier

* Can use Enterprise CA Root Chain. Can be loaded during PnP.

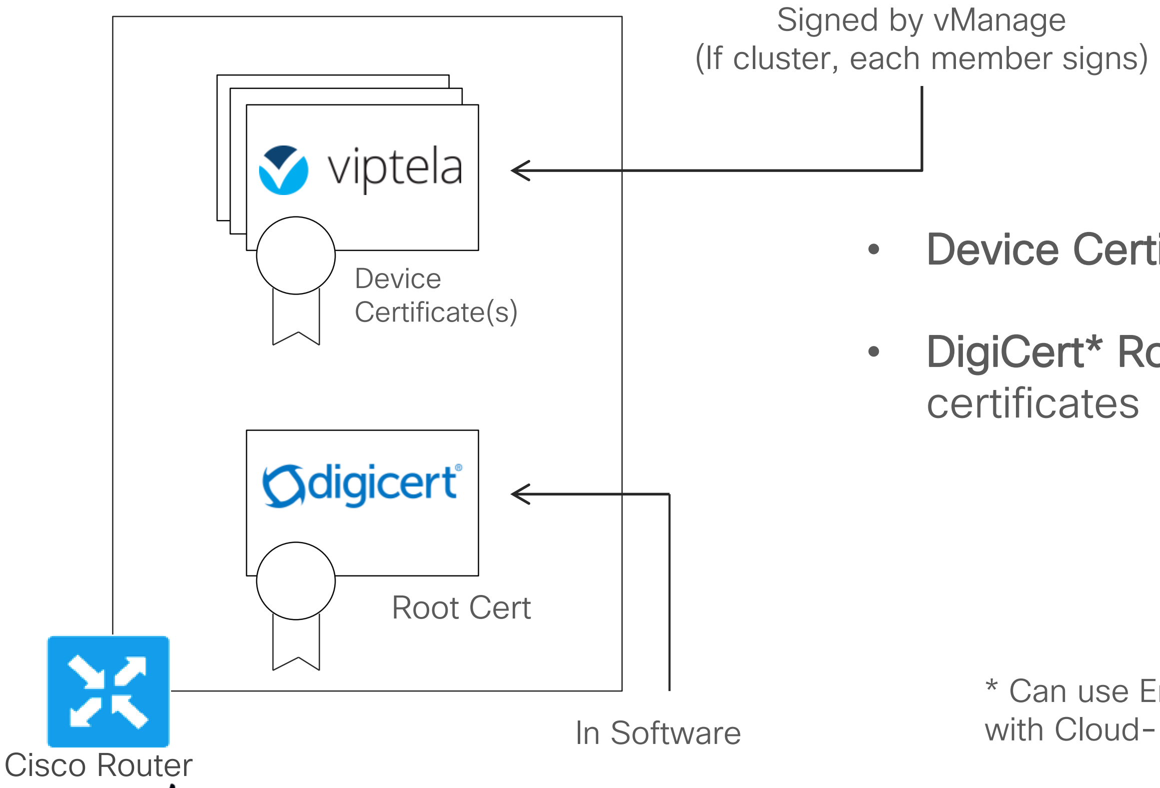
vEdge Cloud, CSR1000v Router Identity



- **Device Certificate** – Own identity (SHA256)
- **DigiCert* Root Chain** – Trust for controllers' certificates

* Can use Enterprise CA Root Chain. Can be loaded with Cloud-Init.

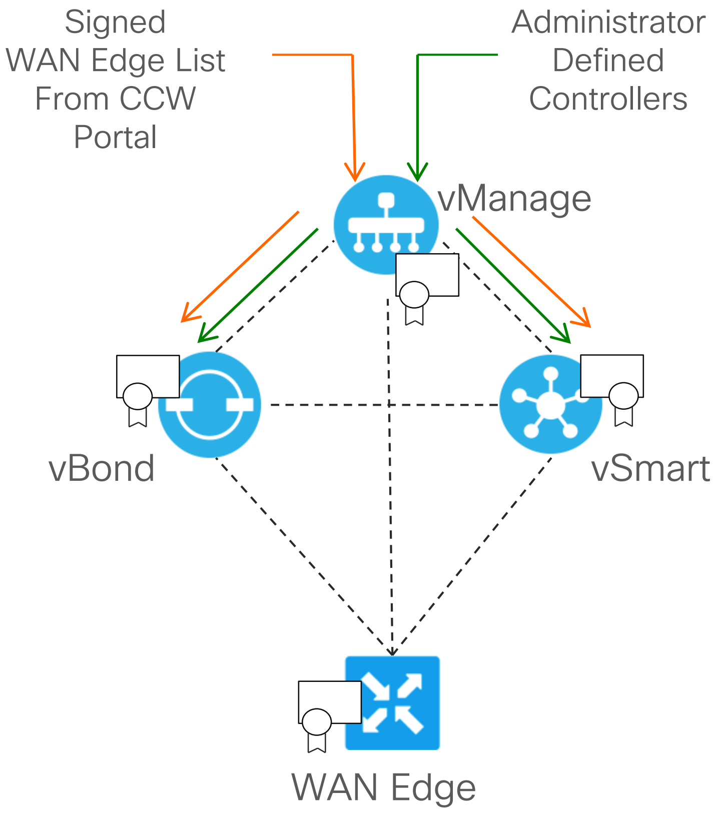
Cisco Router Identity (without SUDI)



- **Device Certificate** – Own identity (SHA256)
- **DigiCert* Root Chain** – Trust for controllers' certificates

* Can use Enterprise CA Root Chain. Can be loaded with Cloud-Init.

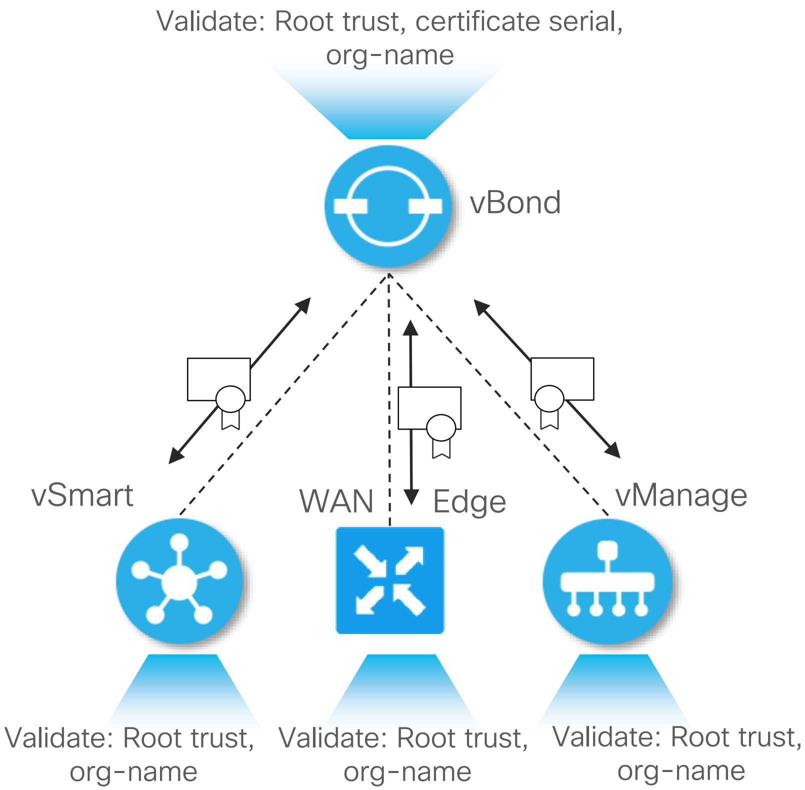
WAN Edge and Controllers White-List



- Administrator defined controllers
- Signed WAN Edge list (whitelist) from CCW Smart Account
- Distributed by vManage to all the controllers

Mutual Trust

WAN Edge, vSmart, vManage to vBond

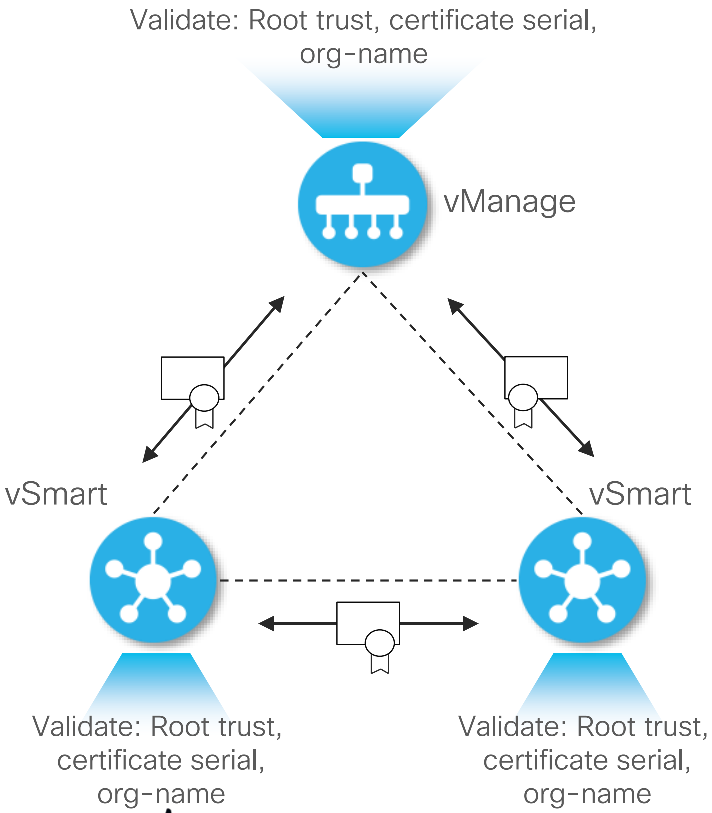

Validate: Root trust, certificate serial, org-name
vBond
vSmart
WAN Edge
vManage
Validate: Root trust, org-name
Validate: Root trust, org-name
Validate: Root trust, org-name

- Certificates are exchanged and mutual authentication takes place
- vBond validates:
  - Root of trust for vSmart, vManage and Edge
  - Certificate serial* numbers against authorized white-list (from vManage)
  - Organization name against locally configured one
- vSmarts, vManage and Edge validate:
  - Root of trust for vBond
  - Organization name against locally configured one

* Also OTP/Token in case of vEdge/cEdge-Cloud and Cisco non-SUDI routers

Mutual Trust

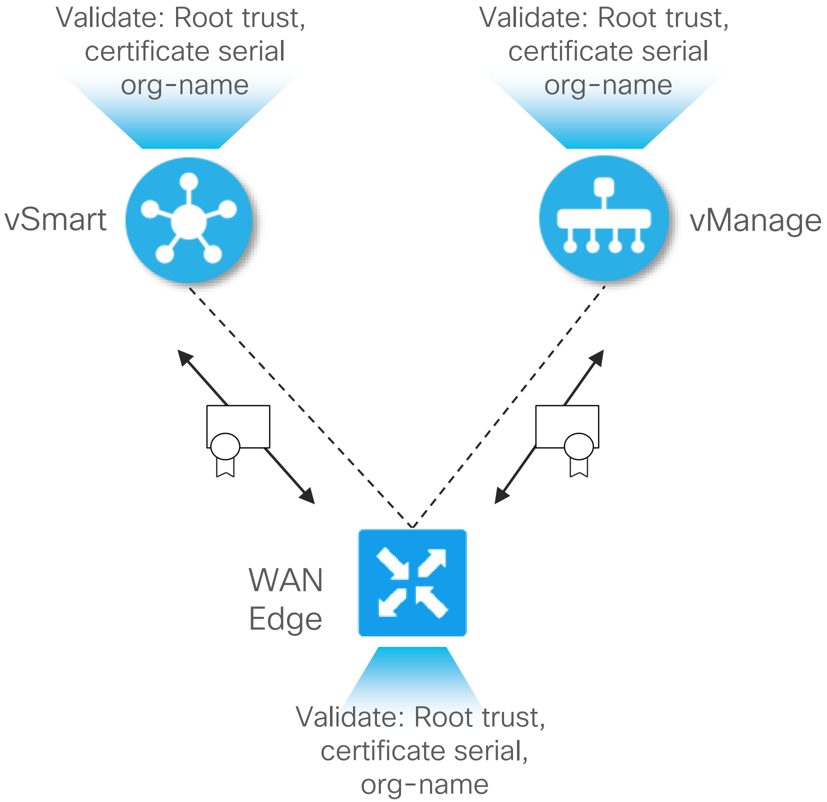
vSmart to vSmart, vManage to vSmart


Validate: Root trust, certificate serial, org-name
vManage
vSmart
vSmart
Validate: Root trust, certificate serial, org-name
Validate: Root trust, certificate serial, org-name

- Certificates are exchanged and mutual authentication takes place
- vSmart validates:
  - Trust for other vSmart and vManage
  - Certificate serial numbers against authorized white-list (from vManage)
  - Organization name against locally configured one
- vManage validates:
  - Trust for vSmart
  - Certificate serial numbers against authorized white-list (from vManage)
  - Organization name against locally configured one

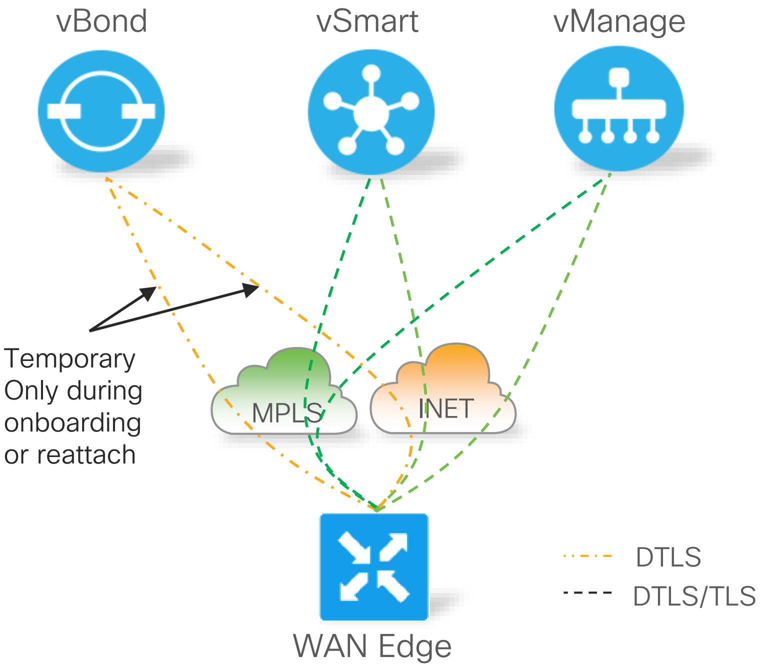
Mutual Trust

WAN Edge to vSmart, vManage

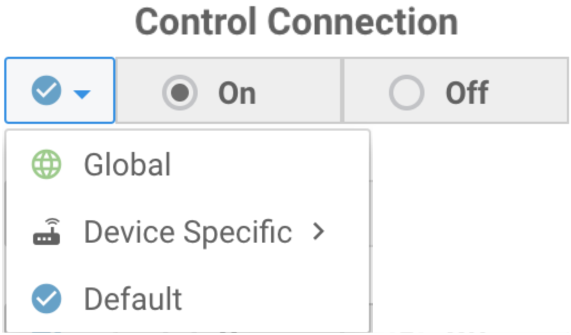


- Certificates are exchanged and mutual authentication takes place
- vSmart and vManage validate:
  - Trust for WAN Edge
  - WAN Edge Certificate serial numbers against authorized white-list (from vManage)
  - Organization name against locally configured one
- WAN Edge validates:
  - Trust for vSmart and vManage
  - Controllers' Certificate serial numbers against authorized white-list (from vManage)
  - Organization name against locally configured one

vEdge Control Plane Transport Establishment



- WAN Edge router will by default try to establish control connections over all provisioned transports
- Administrator can control which transports WAN Edge router uses for establishing control connections



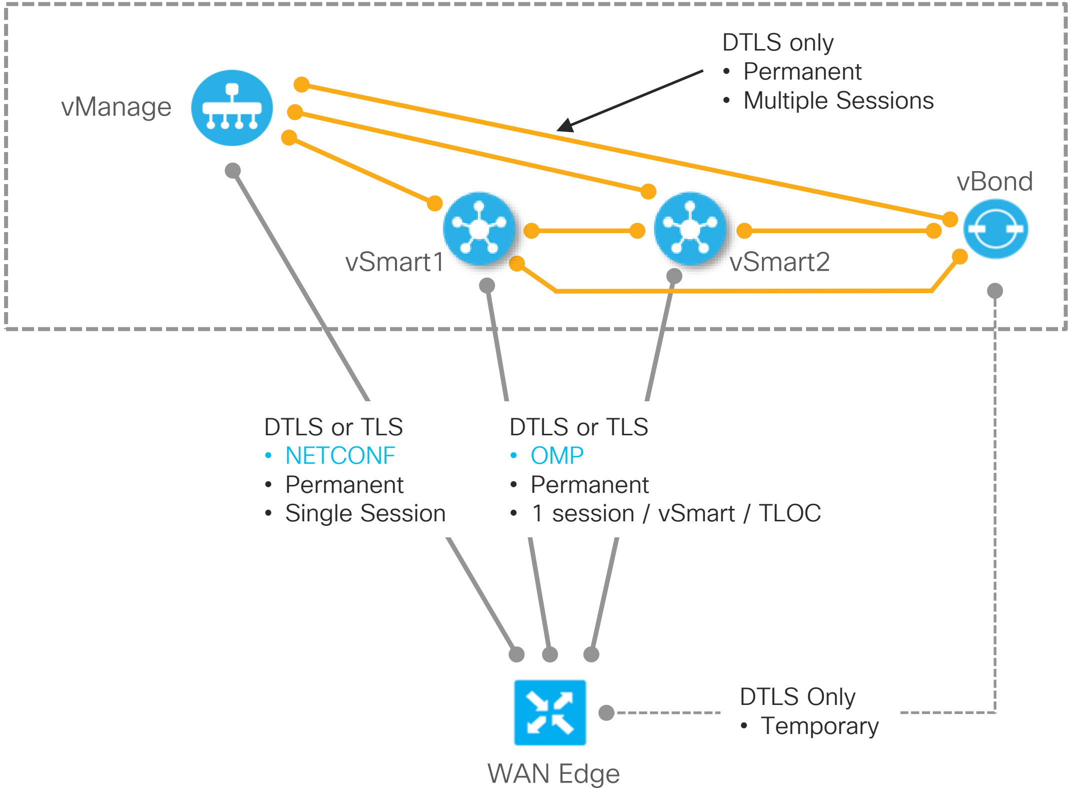
Control Connection

✓ ▾ | ● On | ○ Off

- Global
- Device Specific ›
- ✓ Default

Control Plane Sessions - Summary

- Secure Channel to SD-WAN Controllers
- Automatically extended over all transports by default
- Operates over DTLS/TLS authenticated and secured tunnels
- OMP - between WAN Edge routers and vSmart controllers and between the vSmart controllers
- NETCONF – Provisioning from vManage



DTLS only
- Permanent
- Multiple Sessions

DTLS or TLS
- NETCONF
- Permanent
- Single Session

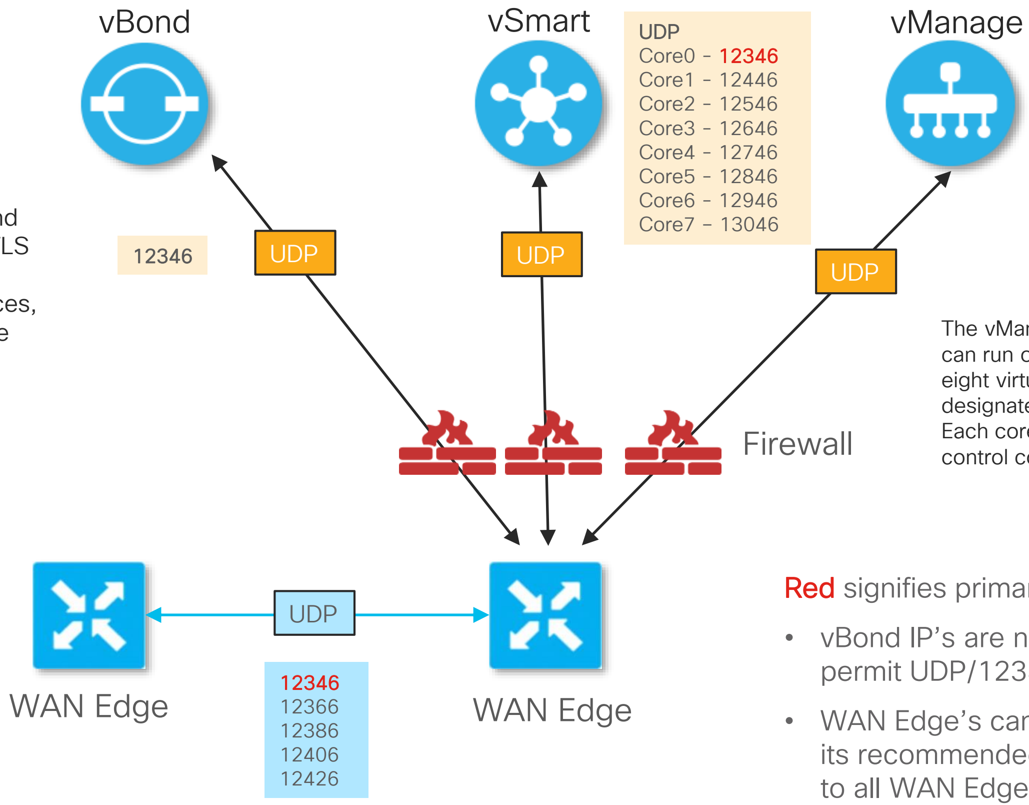
DTLS or TLS
- OMP
- Permanent
- 1 session / vSmart / TLOC

DTLS Only
- Temporary

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



12346

vSmart:

UDP	
Core0	12346
Core1	12446
Core2	12546
Core3	12646
Core4	12746
Core5	12846
Core6	12946
Core7	13046

vManage:

UDP	
Core0	12346
Core1	12446
Core2	12546
Core3	12646
Core4	12746
Core5	12846
Core6	12946
Core7	13046

12346
12366
12386
12406
12426

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

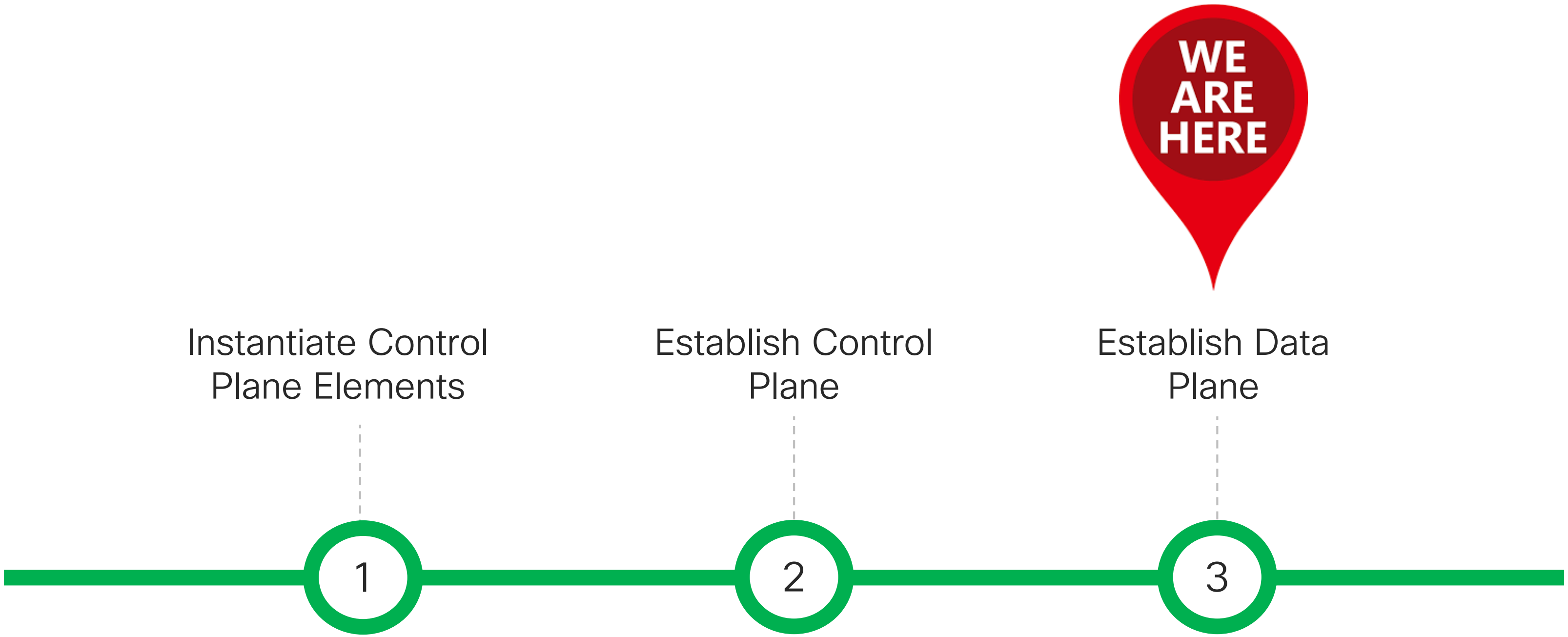
Red signifies primary protocol or first port used

- 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

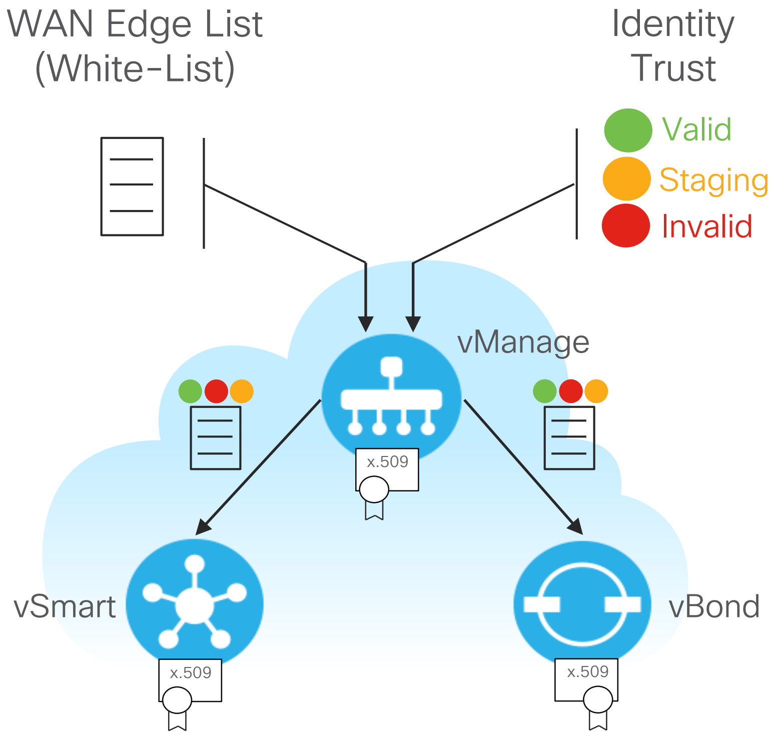
The Fabric

Establishing Data Plane

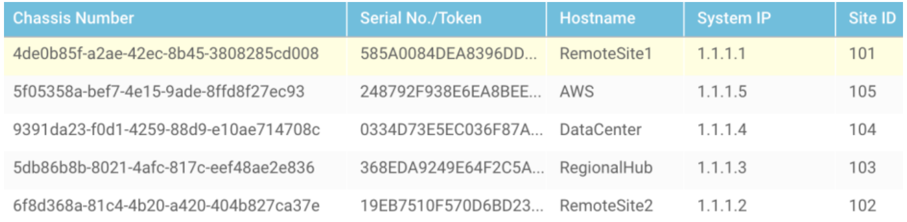
1, 2, 3 … Fabric


WE ARE HERE
Instantiate Control Plane Elements
Establish Control Plane
Establish Data Plane
1
2
3

Data Plane Whitelisting and Identity Trust



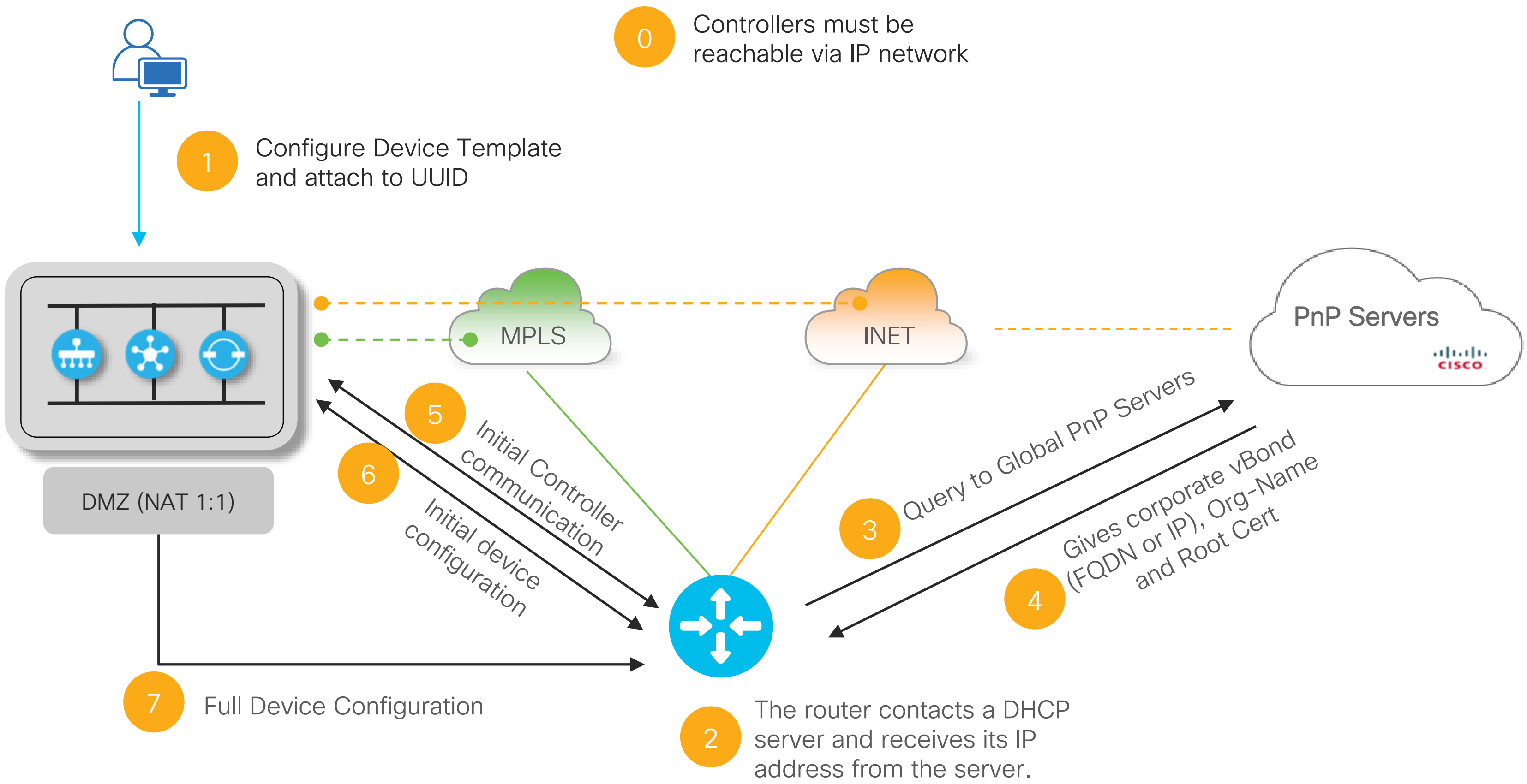
- Administrator uploads digitally signed WAN Edge list in the vManage GUI
  - White-list for WAN Edge routers
  - Manual upload or Smart Account sync



Chassis Number	Serial No./Token	Hostname	System IP	Site ID
4de0b85f-a2ae-42ec-8b45-3808285cd008	585A0084DEA8396DD...	RemoteSite1	1.1.1.1	101
5f05358a-bef7-4e15-9ade-8ffd8f27ec93	248792F938E6EA8BEE...	AWS	1.1.1.5	105
9391da23-f0d1-4259-88d9-e10ae714708c	0334D73E5EC036F87A...	DataCenter	1.1.1.4	104
5db86b8b-8021-4afc-817c-eef48ae2e836	368EDA9249E64F2C5A...	RegionalHub	1.1.1.3	103
6f8d368a-81c4-4b20-a420-404b827ca37e	19EB7510F570D6BD23...	RemoteSite2	1.1.1.2	102

- Administrator decides on identity trust
  - Valid, invalid, staging
- WAN Edge list and identity trust are distributed by vManage to vSmart and vBond

On-Boarding Using Global PnP



0 Controllers must be reachable via IP network

1 Configure Device Template and attach to UUID

2 The router contacts a DHCP server and receives its IP address from the server.

3 Query to Global PnP Servers

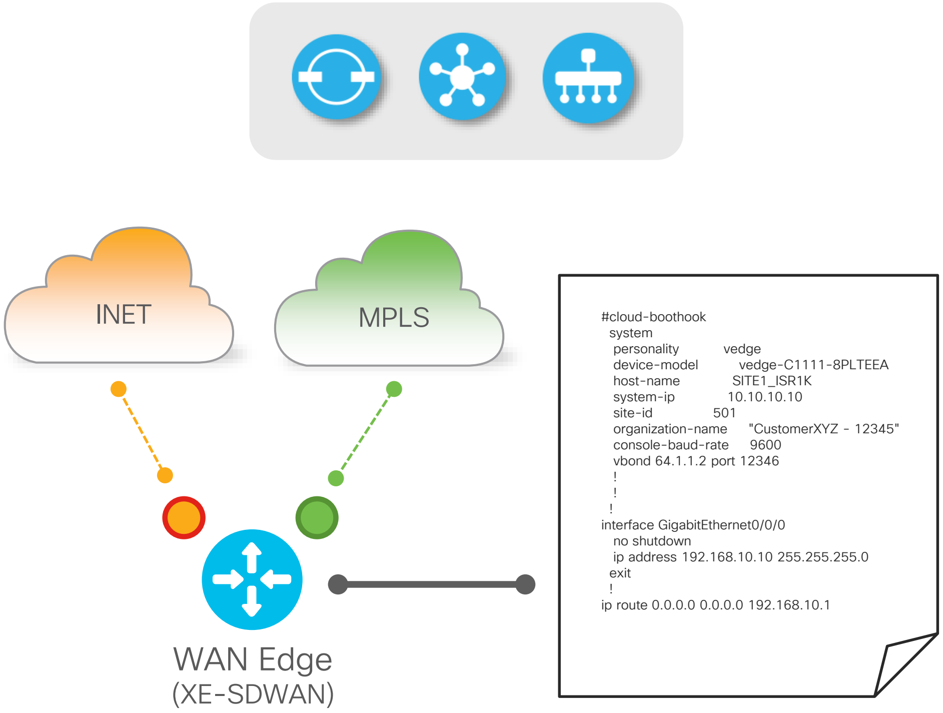
4 Gives corporate vBond (FQDN or IP), Org-Name and Root Cert

5 Initial Controller communication

6 Initial device configuration

7 Full Device Configuration

On Boarding on MPLS with Static IP

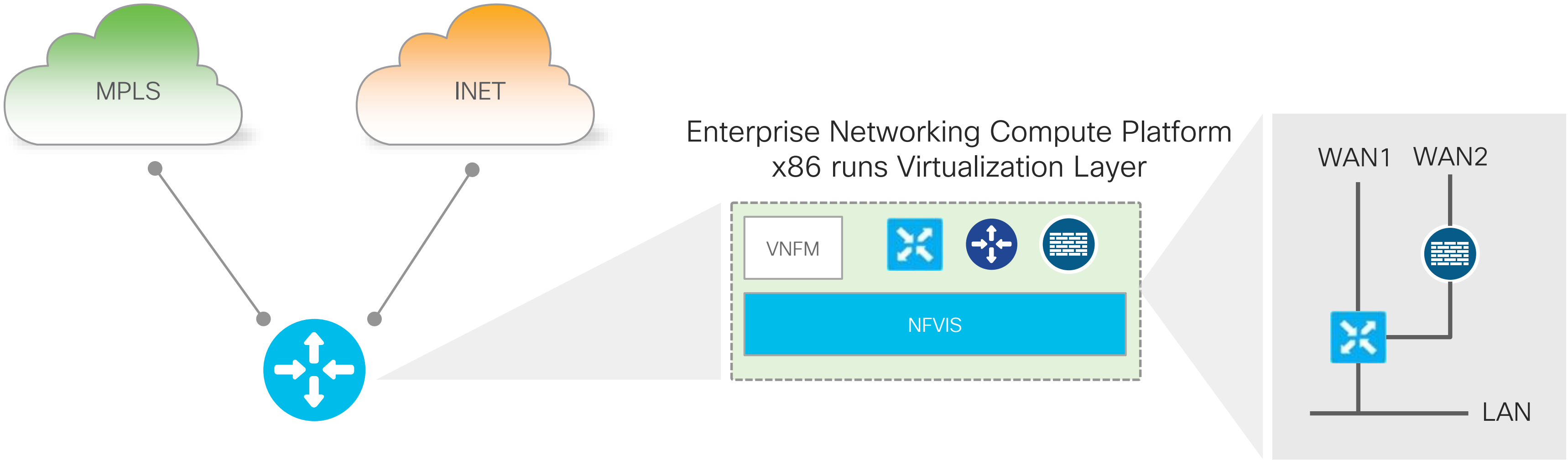


```
#cloud-boothook
  system
   personality          vedge
   device-model          vedge-C1111-8PLTEEA
   host-name            SITE1_ISR1K
   system-ip           10.10.10.10
   site-id             501
   organization-name     "CustomerXYZ - 12345"
   console-baud-rate     9600
   vbond 64.1.1.2 port 12346
   !
   !
  !
interface GigabitEthernet0/0/0
   no shutdown
   ip address 192.168.10.10 255.255.255.0
  exit
  !
ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

- Supported on SD-WAN XE only!
- DHCP is not enabled on CE to PE link (MPLS transport)
- Upon bootup, SD-WAN XE router will search bootflash: or usbflash: for filename ciscosdwan.cfg (case sensitive)
- Config file (which includes basic interface configuration, Root CA, Organization Name, vBond information, etc.) is fed into the PnP process
- Router has all required information to connect to vBond

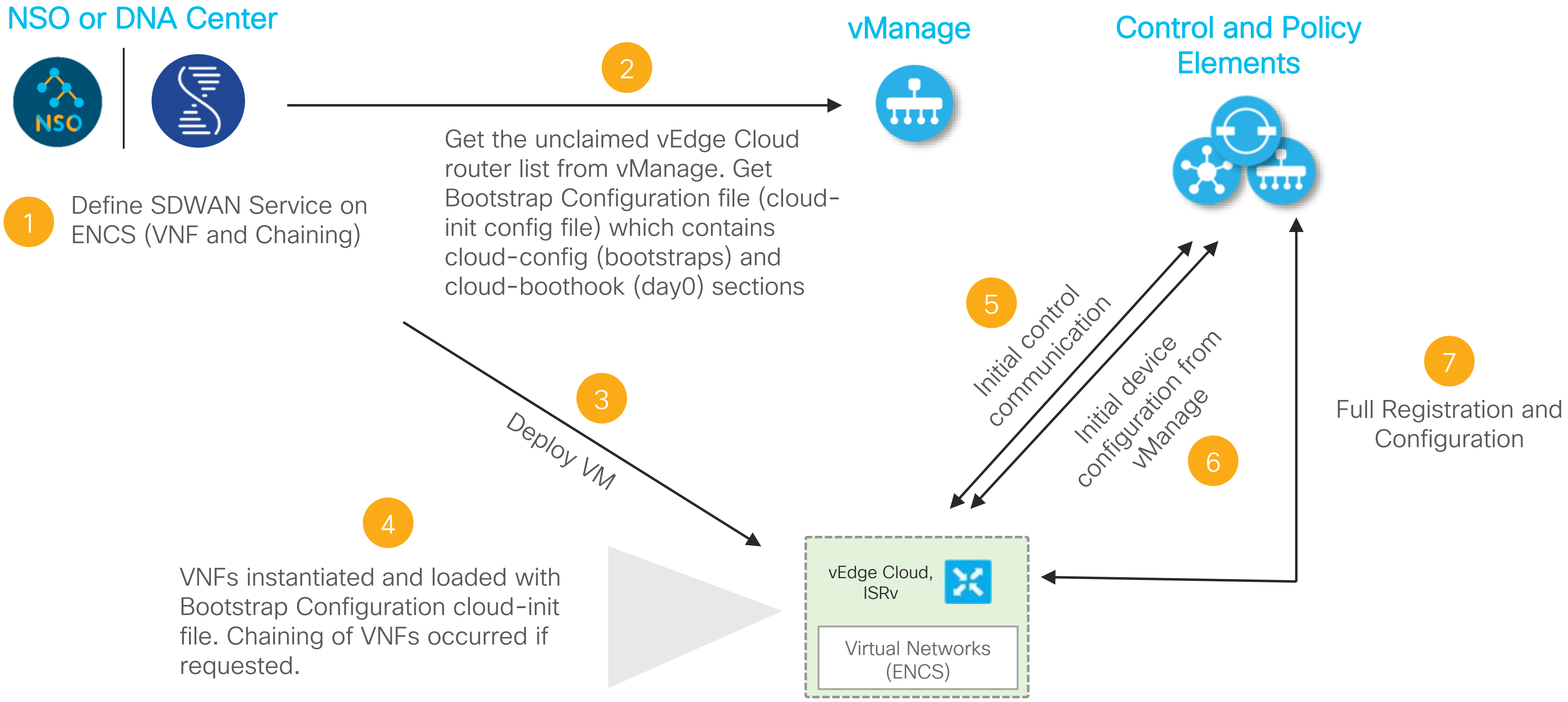
https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/On-Site_Bootstrap_Process_for_SD-WAN_Devices

On Boarding Universal CPE (uCPE)


MPLS
INET
Enterprise Networking Compute Platform
x86 runs Virtualization Layer
VNFM
NFVIS
WAN1
WAN2
LAN

Quickly roll out new services and location
Ability to run Cisco and 3rd party VNF on NFVIS

On-Boarding – vEdge Cloud, ISRv



NSO or DNA Center

1 Define SDWAN Service on ENCS (VNF and Chaining)

2 Get the unclaimed vEdge Cloud router list from vManage. Get Bootstrap Configuration file (cloud-init config file) which contains cloud-config (bootstraps) and cloud-boothook (day0) sections

vManage

Control and Policy Elements

3 Deploy VM

4 VNFs instantiated and loaded with Bootstrap Configuration cloud-init file. Chaining of VNFs occurred if requested.

vEdge Cloud, ISRv

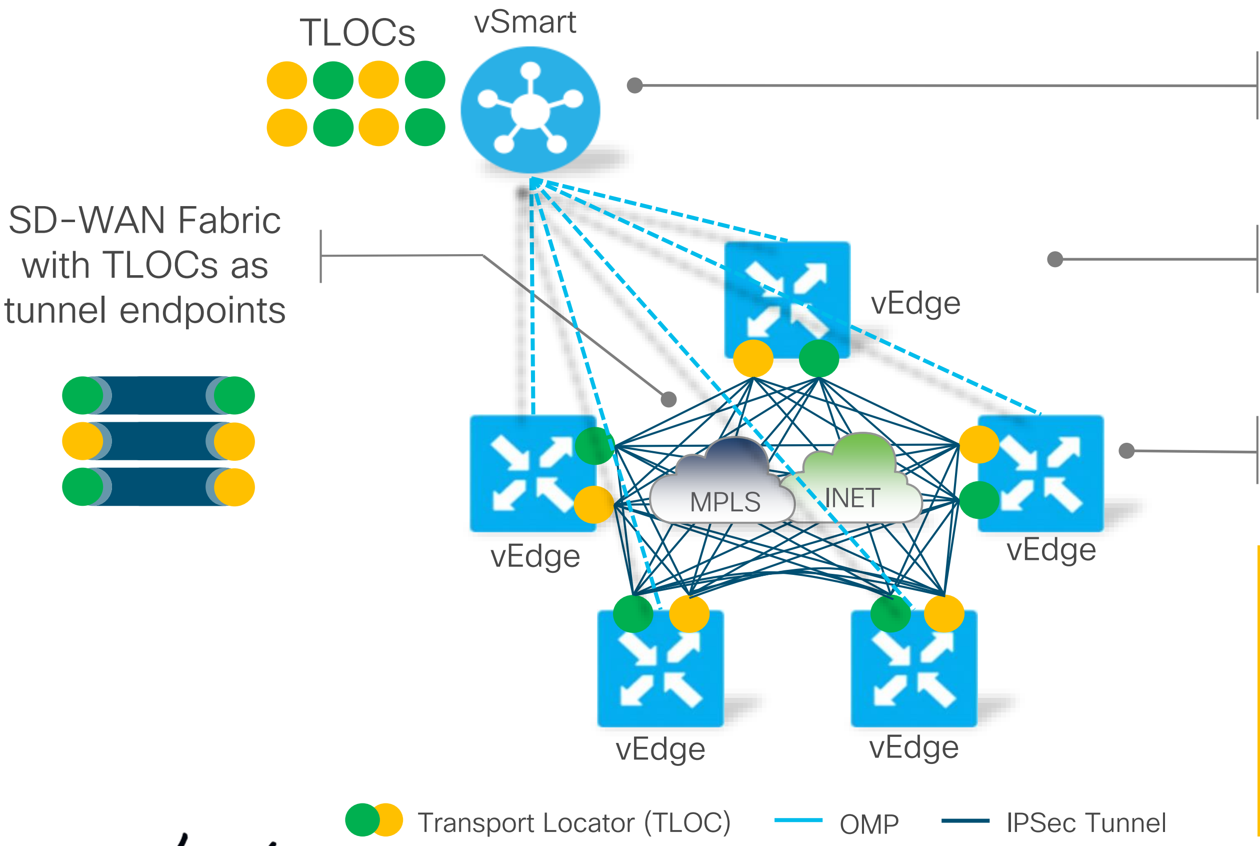
Virtual Networks (ENCS)

5 Initial control communication

6 Initial device configuration from vManage

7 Full Registration and Configuration

Transport Locators (TLOCs)



vSmarts advertise TLOCs to vEdges in TLOC routes

TLOCs advertised to vSmarts in TLOC routes

Local TLOCs (System IP, Color, Encap)

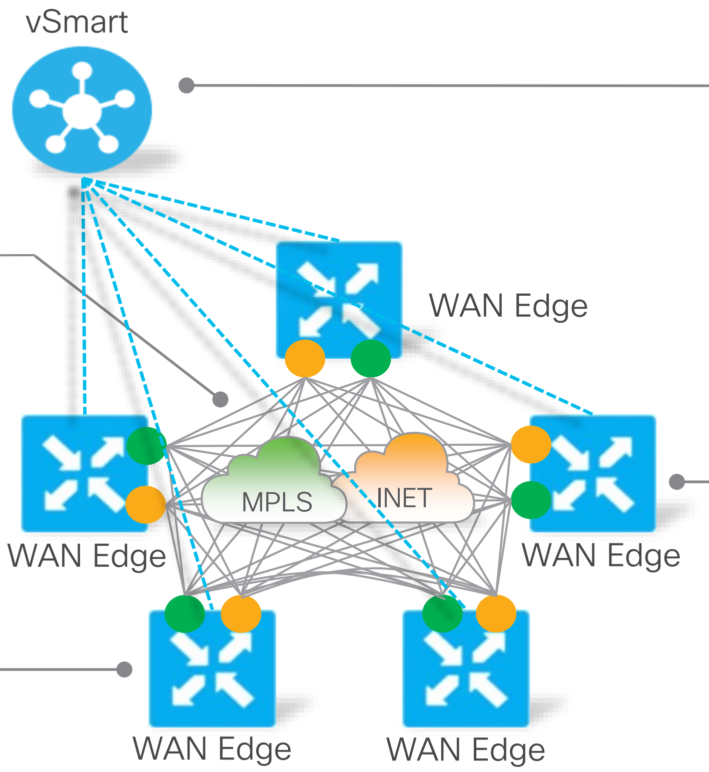
TLOC is an abstraction representing a WAN Interface

Color is label used to identify a WAN interface. It can be Public or Private.

Data Plane Establishment

SD-WAN fabric between tunnel endpoints

● IPsec ●
● IPsec ●
● IPsec ●



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

Routes and encryption keys are advertised to vSmarts in OMP updates

Local Routes

- Site prefixes (OSPF/BGP)
- TLOCs (SD-WAN tunnel endpoints)

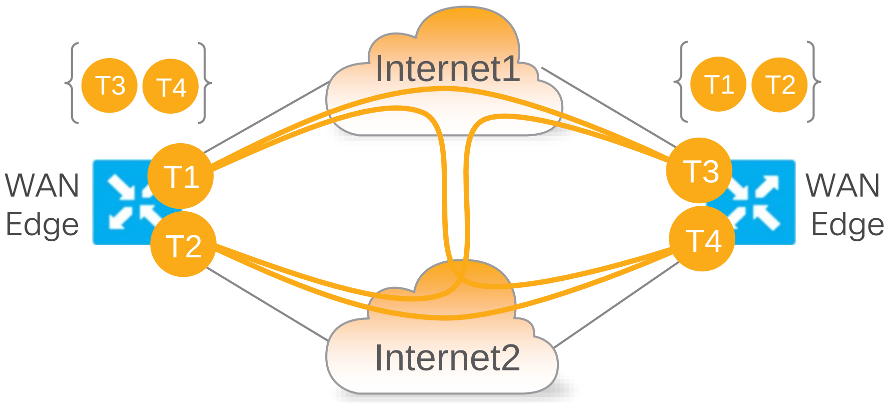
Security Context

- IPSec Encryption Keys

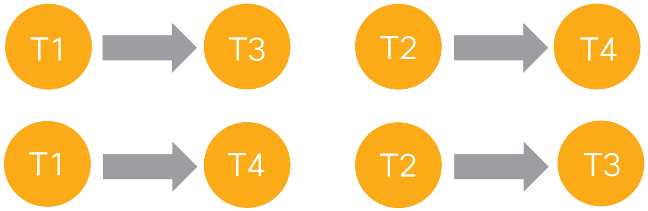
Fabric Routing:
<prefix> via ● ●

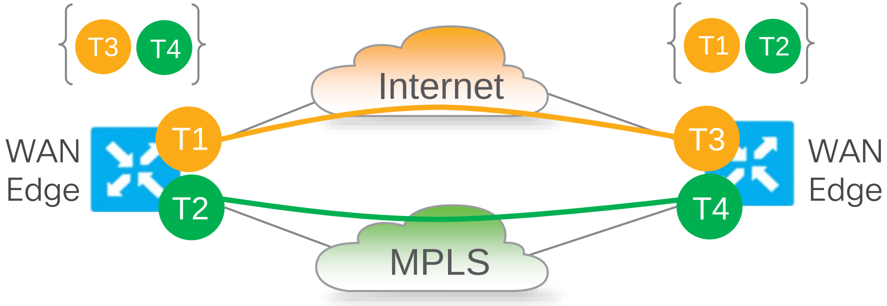
●● Transport Locator (TLOC)   - - OMP   — IPSec Tunnel

Transport Colors affect system behaviour…

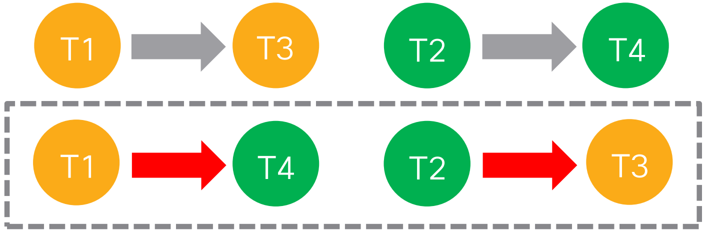


T1, T3 – Internet1 Color T2, T4 – Internet2 Color





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



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

Significance of 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
- Facilitiates NAT Traversal
- “Color” dictates the use of private-ip vs public-ip for Tunnel Establishment when there is NAT present
- Example:
    - If tunnel endpoints both have a private color: private IP address/port used for DTLS/TLS or IPSec
    - If any tunnel 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

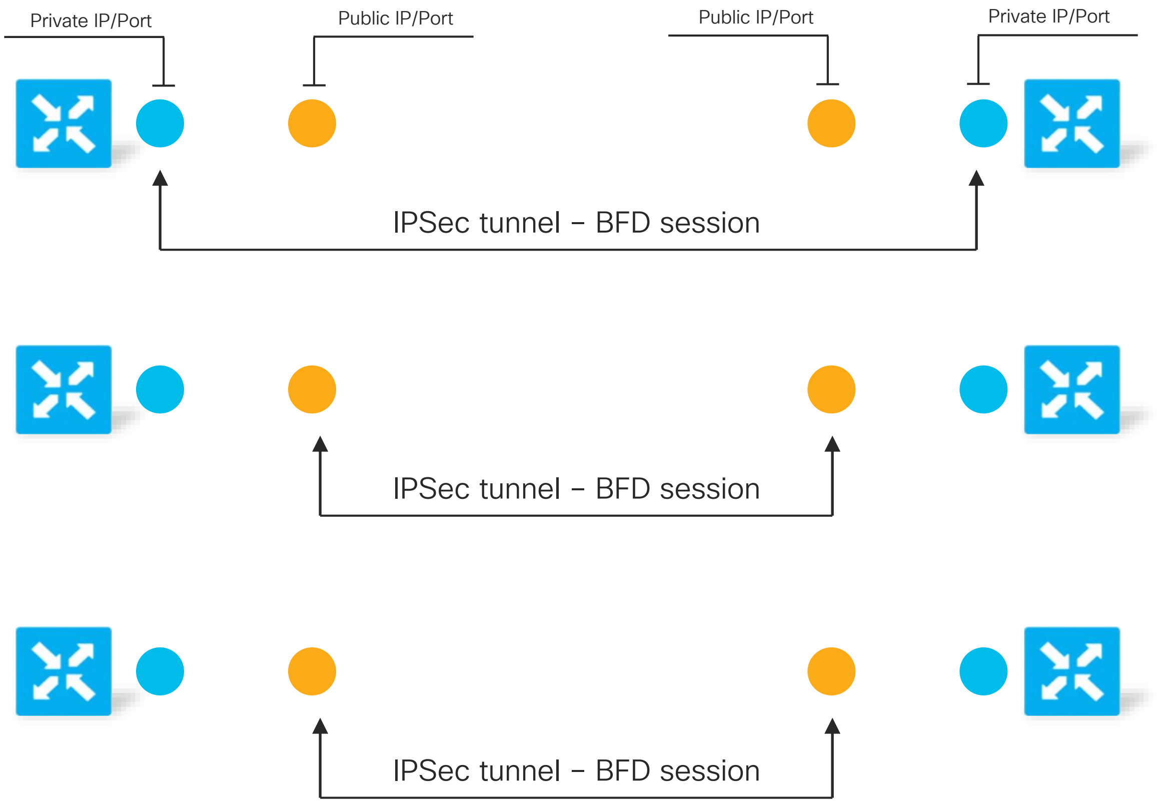
3g
lte
biz-internet
public-internet
blue
green
red
gold
silver
bronze

Significance of TLOC Color Illustrated

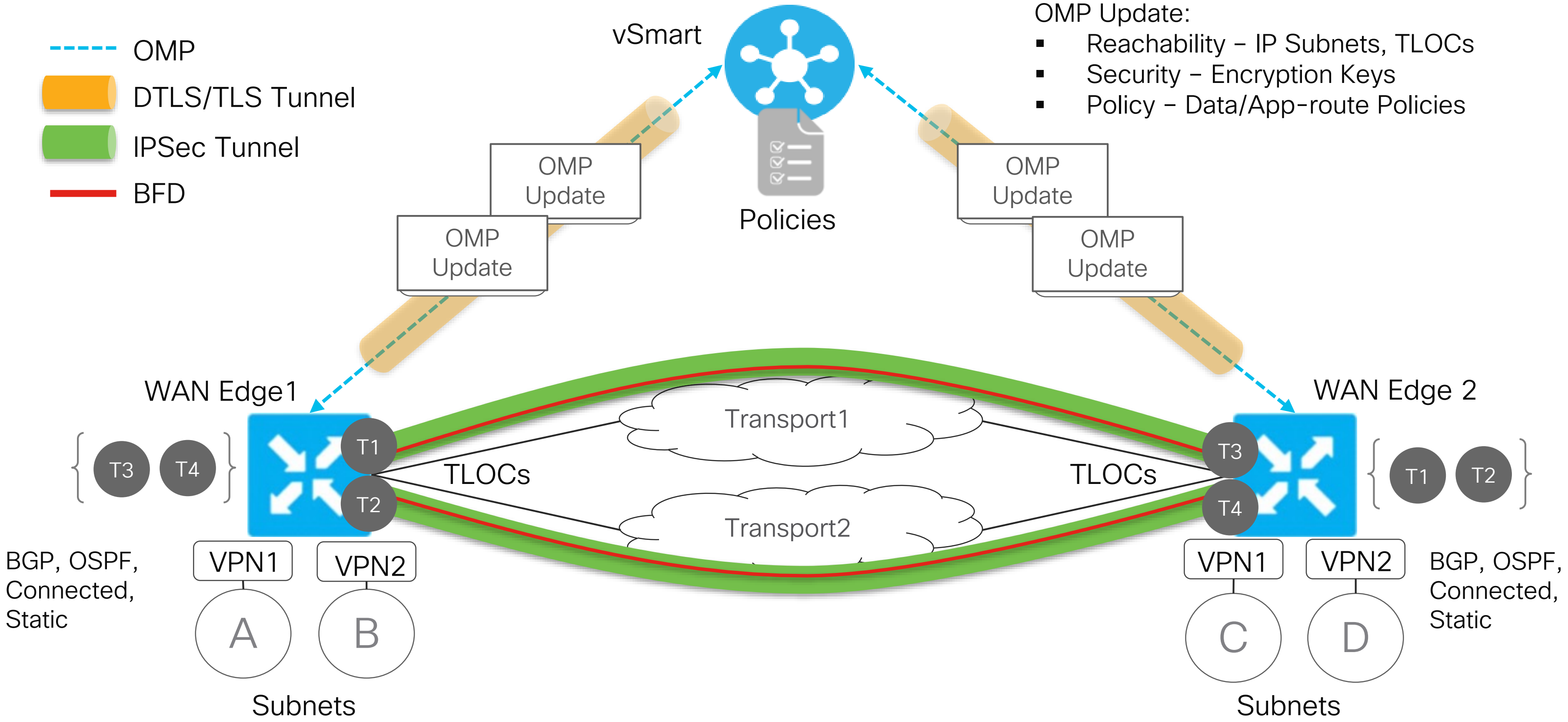
1 Private color to Private color

2 Private color to Public color

3 Public color to Public color


Private IP/Port
Public IP/Port
Public IP/Port
Private IP/Port
IPSec tunnel – BFD session
IPSec tunnel – BFD session
IPSec tunnel – BFD session

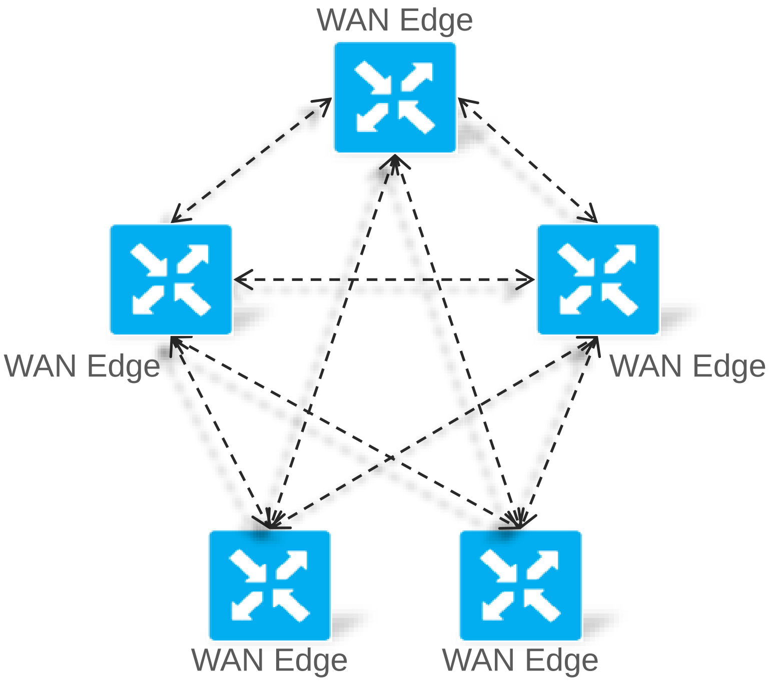
Fabric Operation



OMP Update:

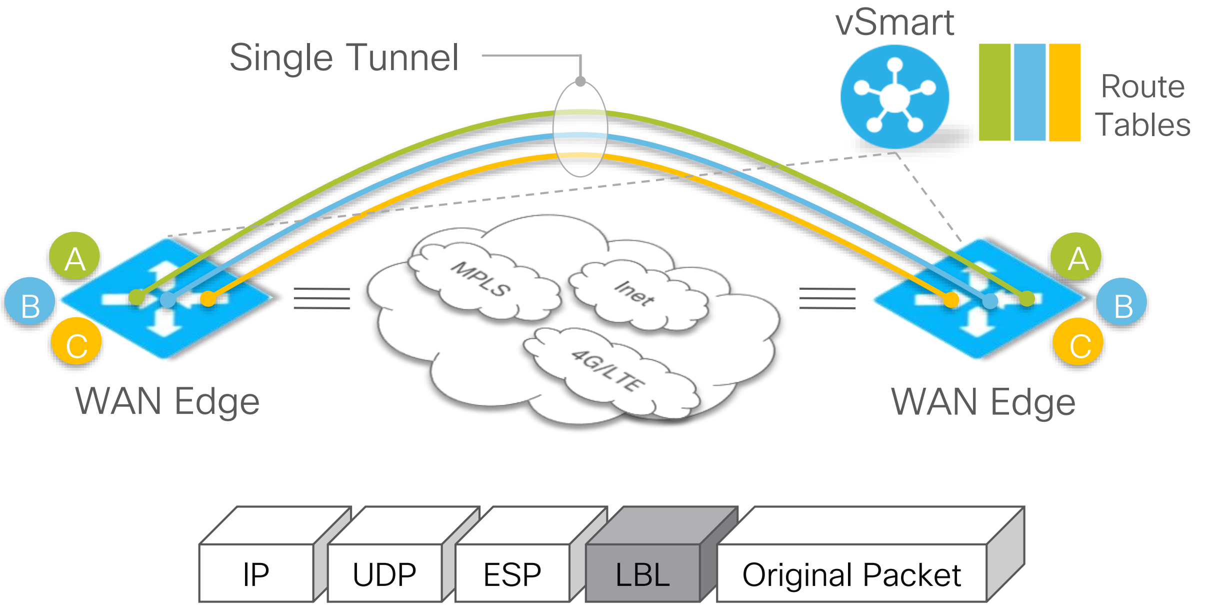
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies

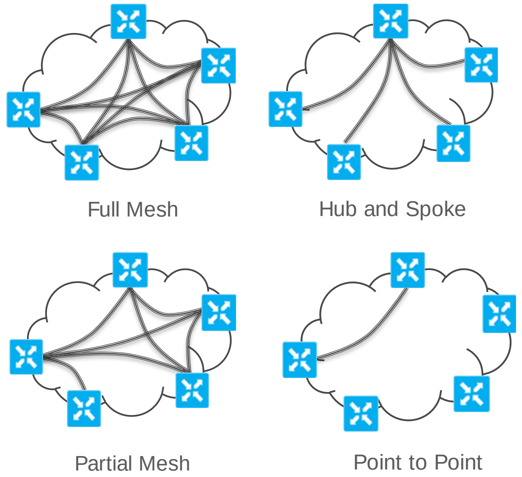
Data Plane Liveliness and Quality



- Bidirectional Forwarding Detection (BFD)
- Path liveliness and quality measurement
  - Up/Down, loss/latency/jitter, IPSec tunnel MTU
- Runs between all WAN Edge routers in the topology
  - Inside SD-WAN tunnels
  - Across all transports
  - Operates in echo mode
  - Automatically invoked at SD-WAN tunnel establishment
  - Cannot be disabled
- Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection
  - Fully customizable per-WAN Edge, per-transport

End-to-End Segmentation with Multi-Topology



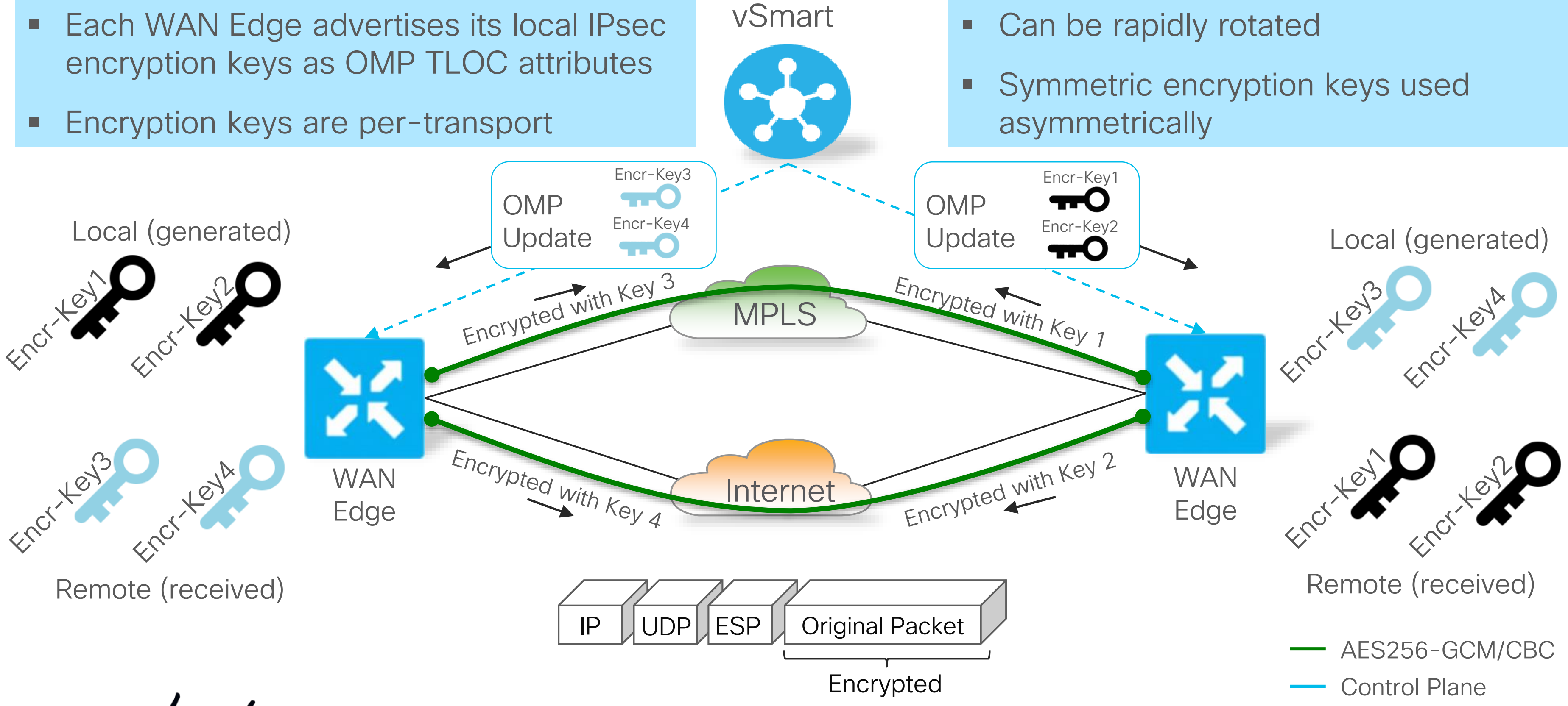


- Segment connectivity across fabric w/o reliance on underlay transport
- WAN Edge routers maintain per-VPN routing table for complete control plane separation

Data Plane Privacy and Encryption

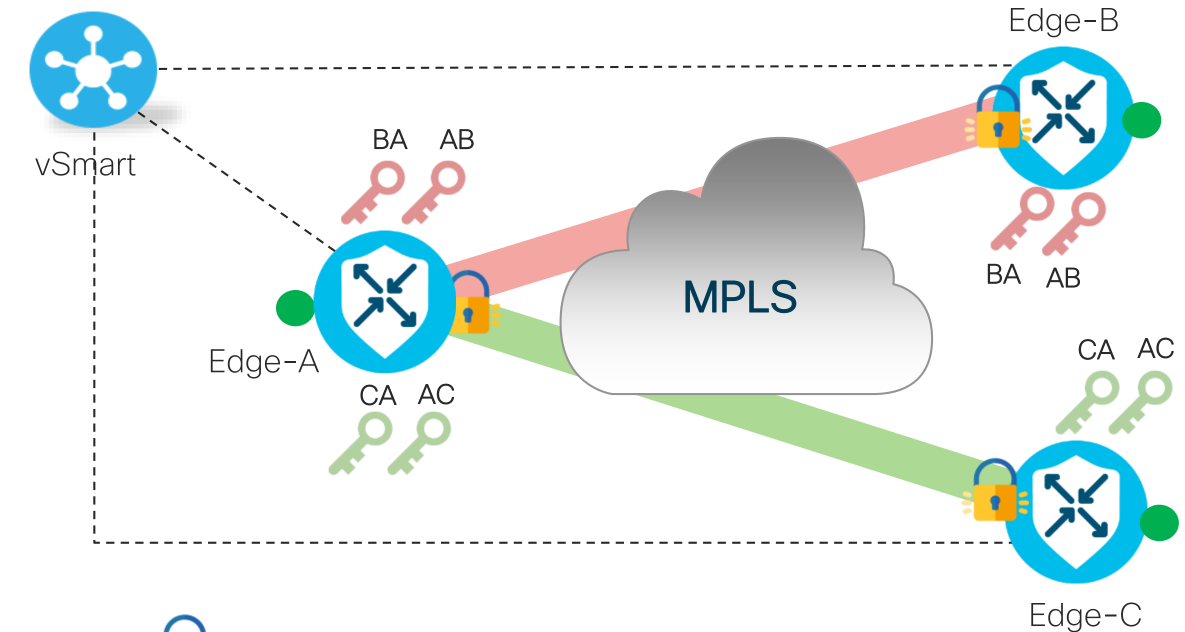
- Each WAN Edge advertises its local IPsec encryption keys as OMP TLOC attributes
- Encryption keys are per-transport

- Can be rapidly rotated
- Symmetric encryption keys used asymmetrically



cisco Live!

IPSec PairWise Key Management – New Feature



● LAN   🔒 IPSec/GRE   ---------- DTLS

AB – AB- A's Encryption Key for B

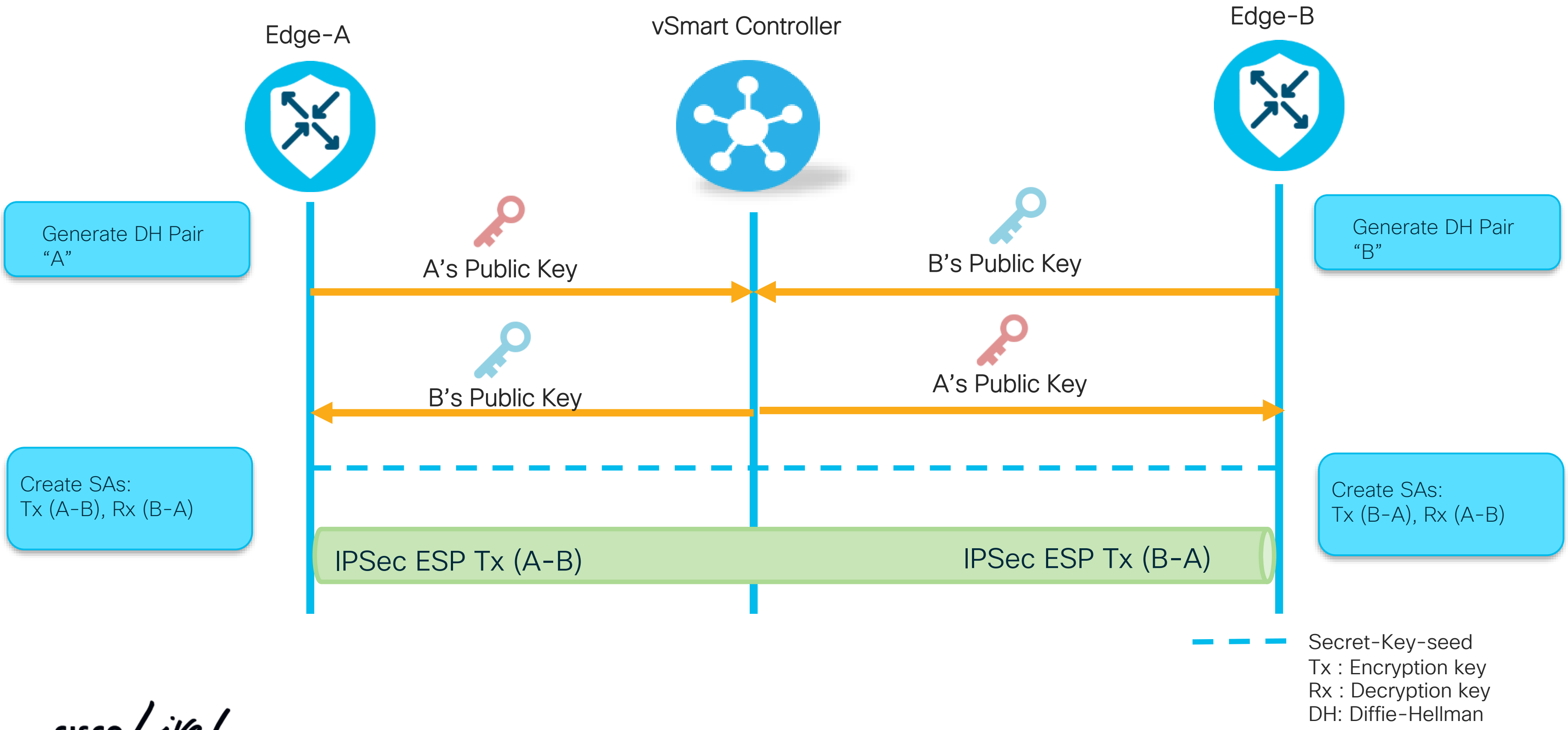
BA – BA - B's Encryption Key for A

AC – AC- A's Encryption Key for C

CA – CA - C's Encryption Key for A

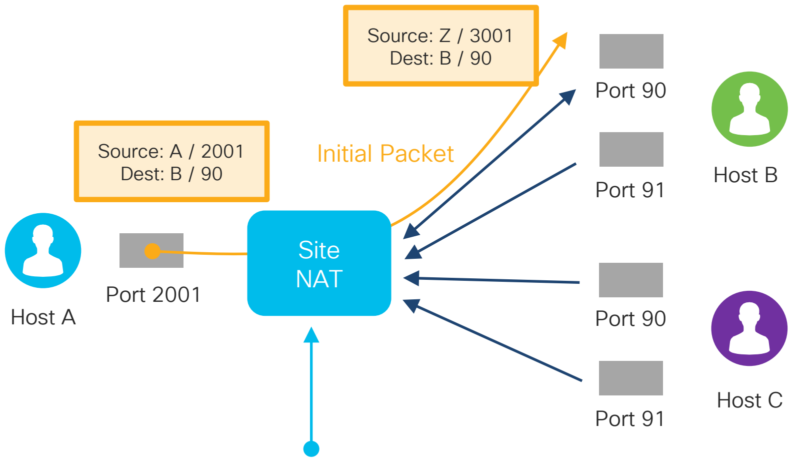
- Each WAN edge will create separate session key for each transport and for each peer
- Session keys will be advertised through vSmart using OMP
- Edge-A needs to send traffic to Edge-B, it will use session key "AB" (B will use key "BA")
- **Backward compatible** with non PWK devices
- PWK is disabled by **default**

IPSec Pairwise Keying Session Establishment



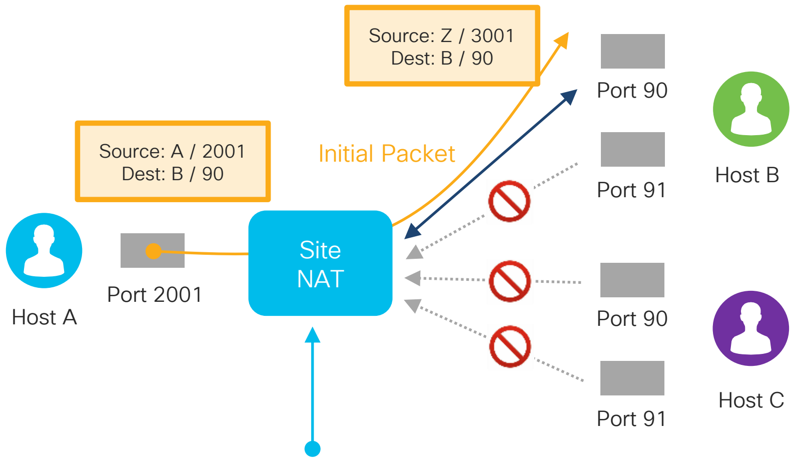
Understanding NAT Types (1/2)

Full-Cone



NAT Binding	NAT Filter
Local Addr / Port <-> External Addr / Port	External Address mask
A / 2001 <-> Z / 3001	* / *

Symmetric

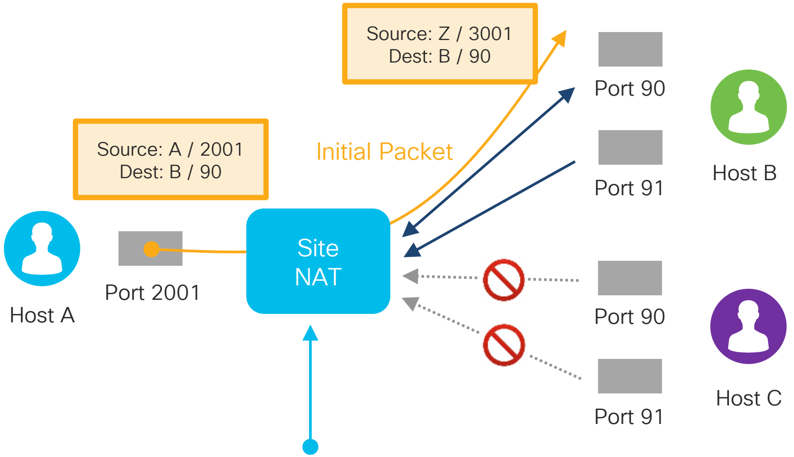


NAT Binding	NAT Filter
Local Addr / Port <-> External Addr / Port	External Address mask
A / 2001 <-> Z / 3001	B / 90

Source: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-29/anatomy.html

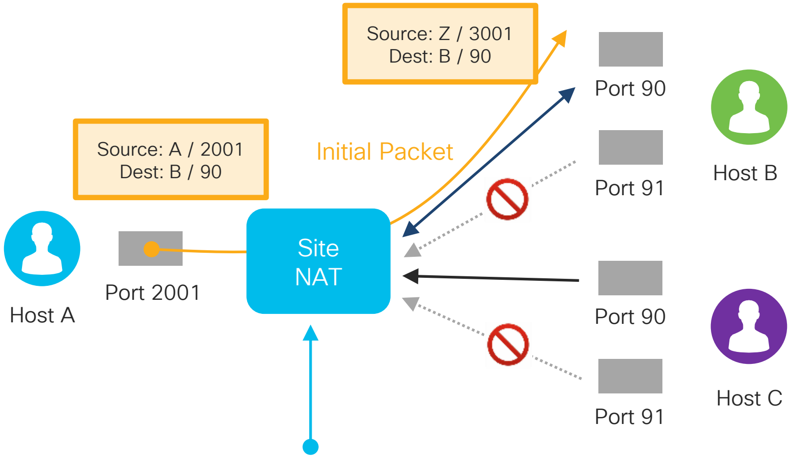
Understanding NAT Types (2/2)

Restricted-Cone NAT



NAT Binding	NAT Filter
Local Addr / Port <-> External Addr / Port	External Address mask
A / 2001 <-> Z / 3001	B / *

Port-Restricted-Cone NAT



NAT Binding	NAT Filter
Local Addr / Port <-> External Addr / Port	External Address mask
A / 2001 <-> Z / 3001	* / 90

Source: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-29/anatomy.html

NAT Traversal Combinations

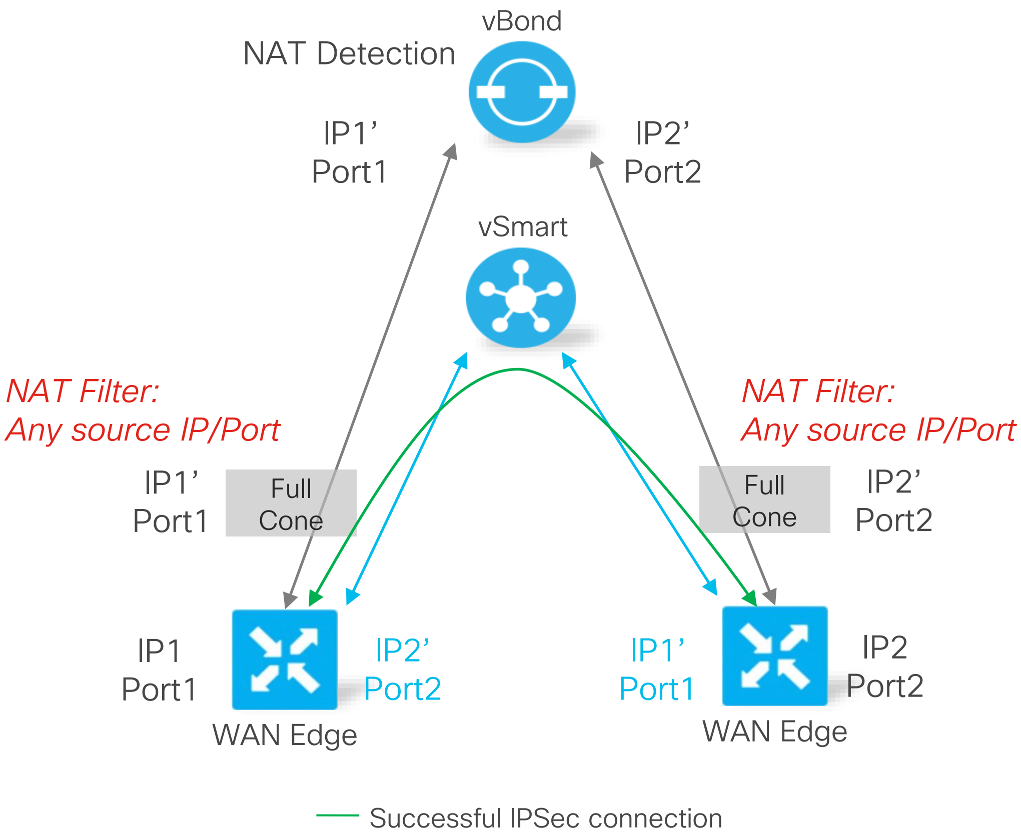
Side A	Side B	IPSec Tunnel Status	
Public	Public	🟢	★
Full Cone	Full Cone	🟢	★
Full Cone	Port/Address Restricted	🟢	
Port/Address Restricted	Port/Address Restricted	🟢	
Public	Symmetric	🟢	
Full Cone	Symmetric	🟢	★
Symmetric	Port/Address Restricted	🔴	
Symmetric	Symmetric	🔴	★

🟢 Direct IPSec Tunnel

🔴 No Direct IPSec Tunnel (traffic traverses hub)

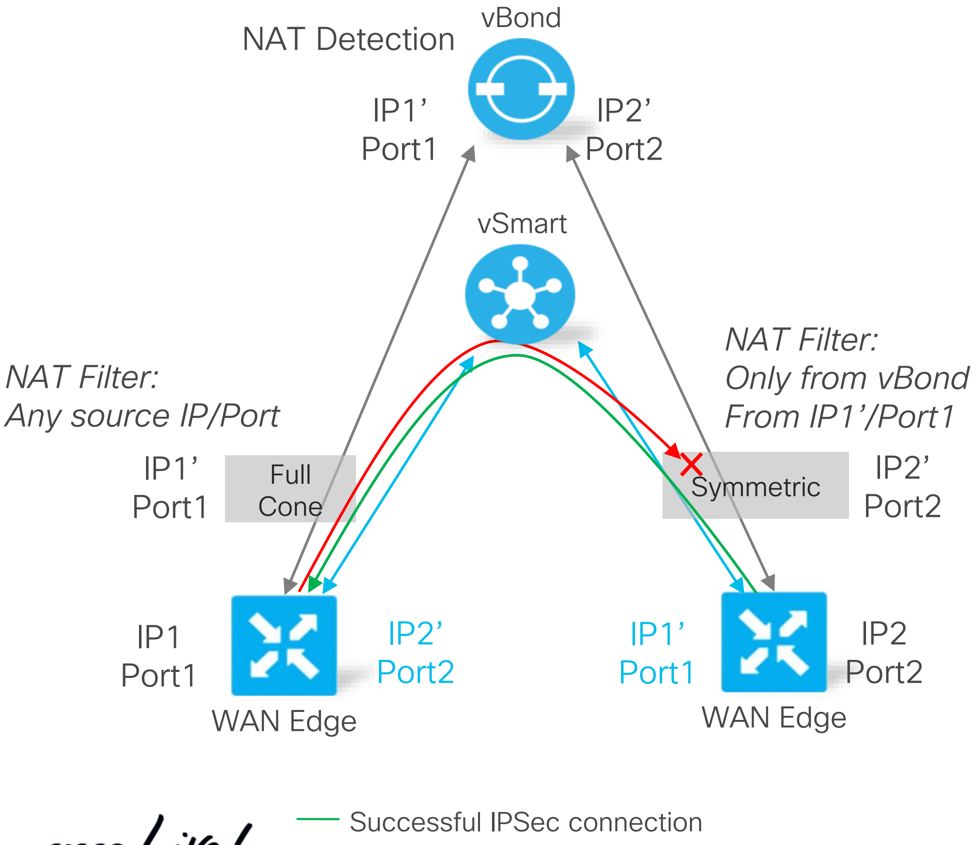
★ Mostly Encountered

NAT Traversal – Dual Sided Full Cone



- vBond discovers post-NAT public IP and communicates back to vEdges
  - STUN Server
- WAN Edge routers notify vSmart of their post-NAT public IP address
- vSmart Advertises both Post and Pre-NAT addresses to other vEdges
- NAT devices enforce no filter
  - Full-cone NAT

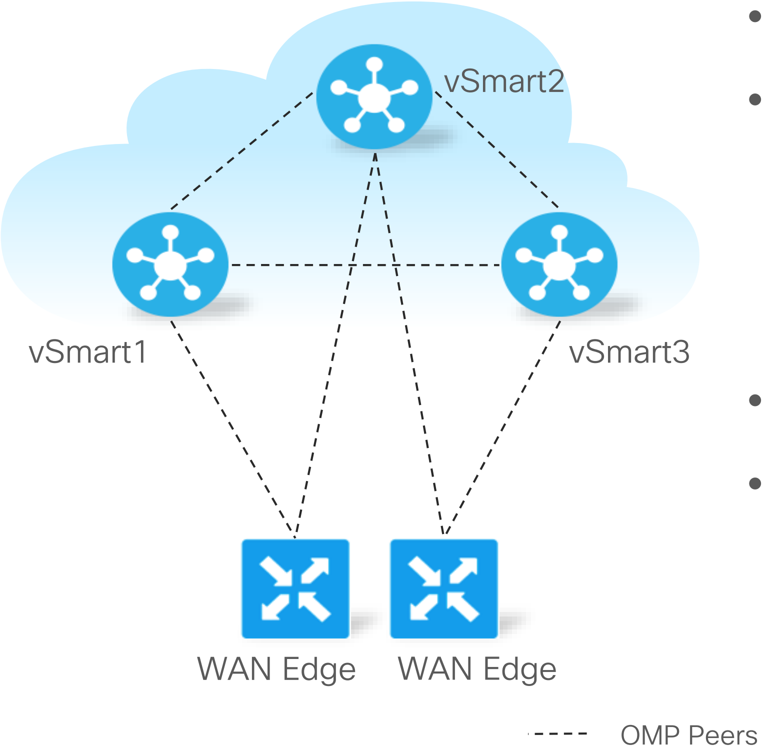
NAT Traversal – Full Cone and Symmetric



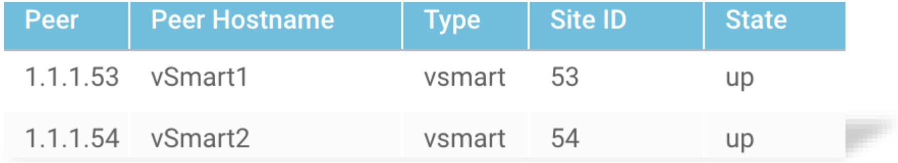
- vBond discovers post-NAT public IP and communicates back to WAN Edge routers
  - STUN Server
- WAN Edge routers notify vSmart of their post-NAT public IP address
- Symmetric NAT devices enforce filter
  - Only allows traffic from vBond
- WAN Edge behind symmetric NAT reaches out to remote WAN Edge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

Overlay Management Protocol (OMP)

Overlay Management Protocol Overview



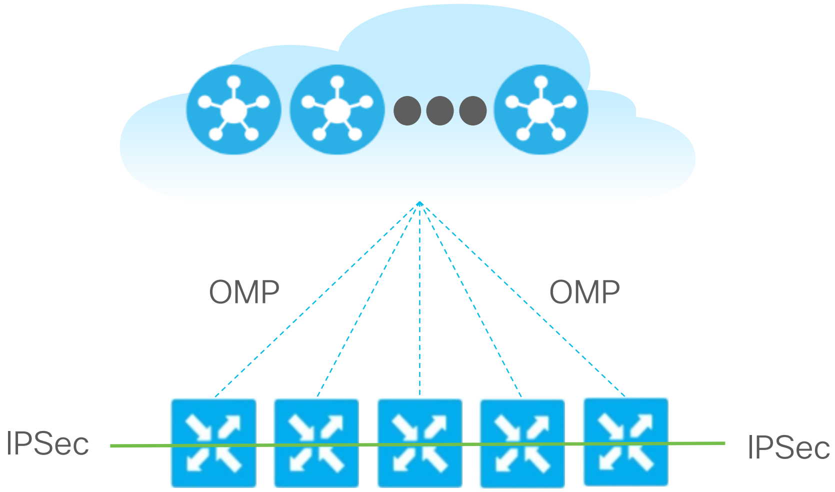
- TCP based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside permanent TLS/DTLS connections
  - Automatically enabled on bring-up
- vSmarts create full mesh of OMP peers
- WAN Edge routers need not peer with all vSmarts



Peer	Peer Hostname	Type	Site ID	State
1.1.1.53	vSmart1	vsmart	53	up
1.1.1.54	vSmart2	vsmart	54	up

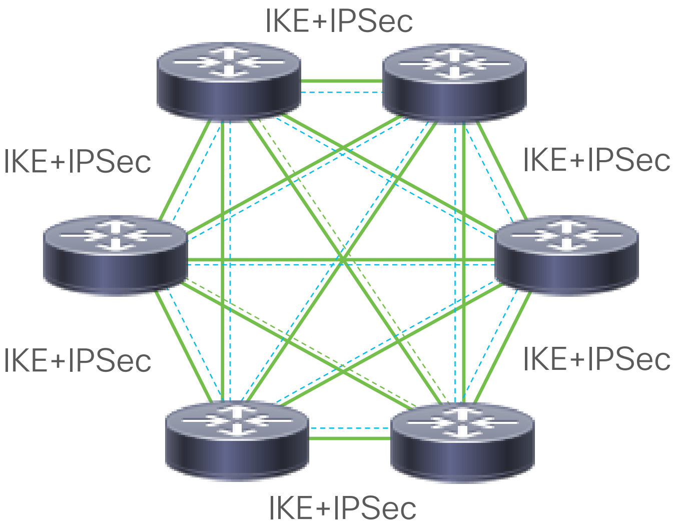
Control Plane Complexity

SD-WAN



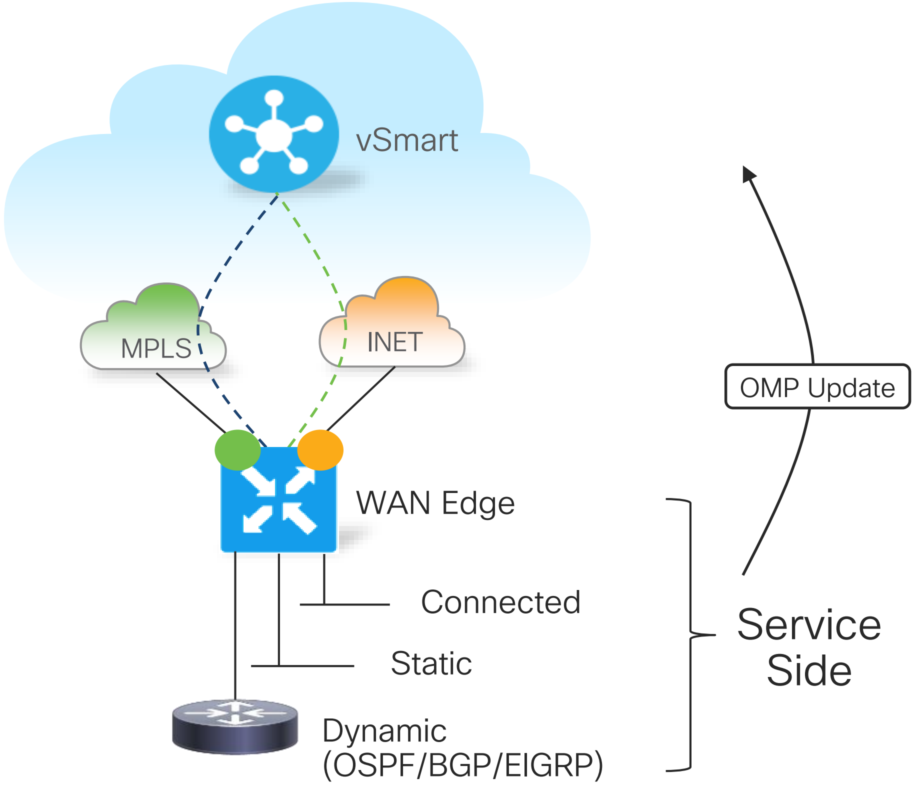
Linear Control Plane Complexity
O(n)

Traditional IPSec networks



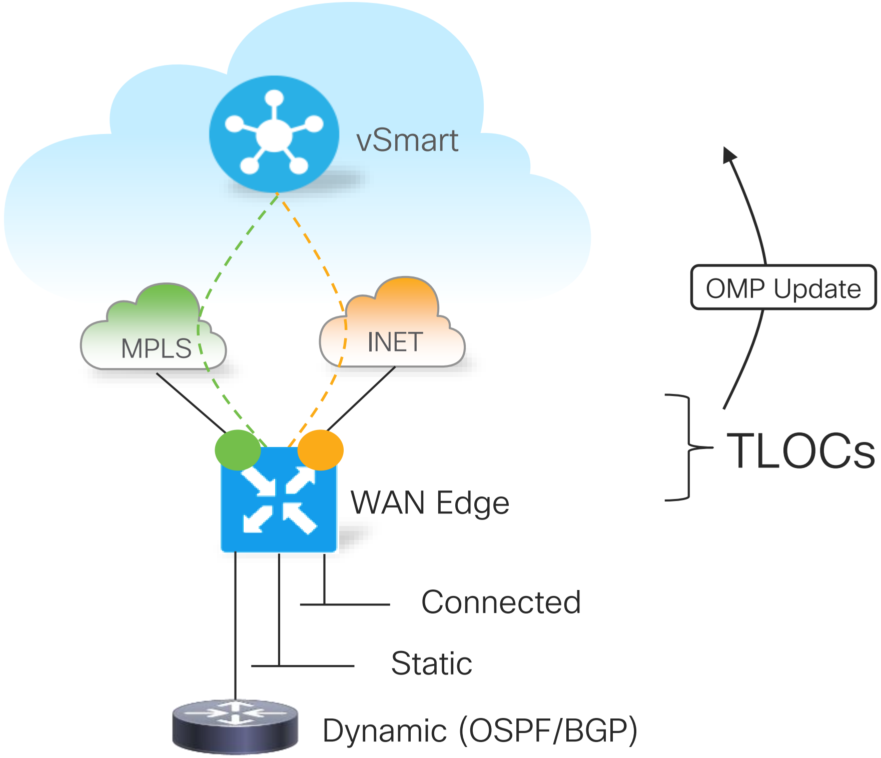
Quadratic Control Plane Complexity
O(n^2)

Overlay Routing: OMP Routes



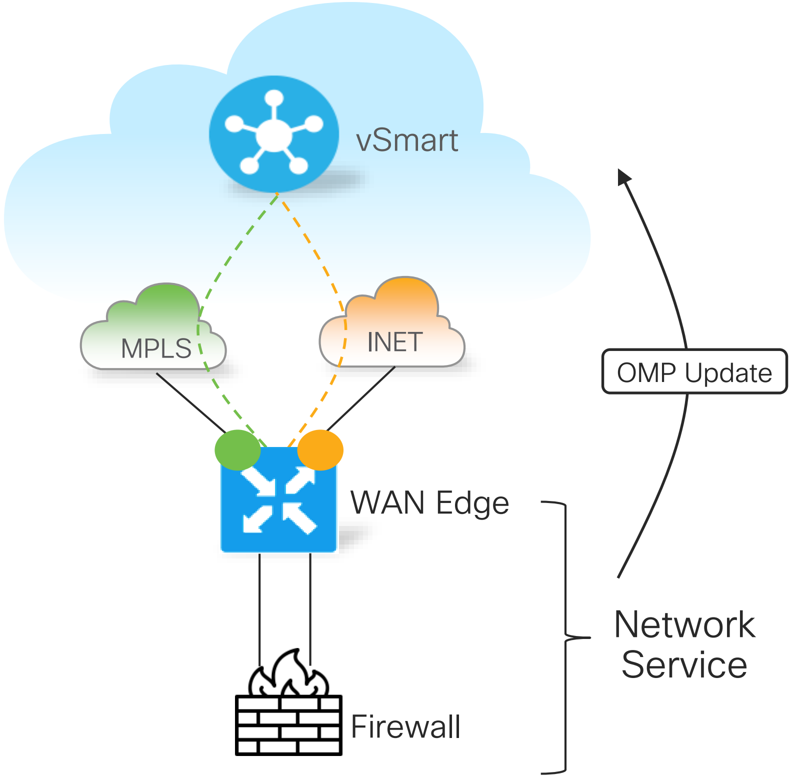
- Routes learnt from local service side
- Advertised to vSmart controllers
- Most prominent attributes:
  - TLOC
  - Site-ID
  - Label
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric
  - AS PATH

Overlay Routing: TLOC Routes



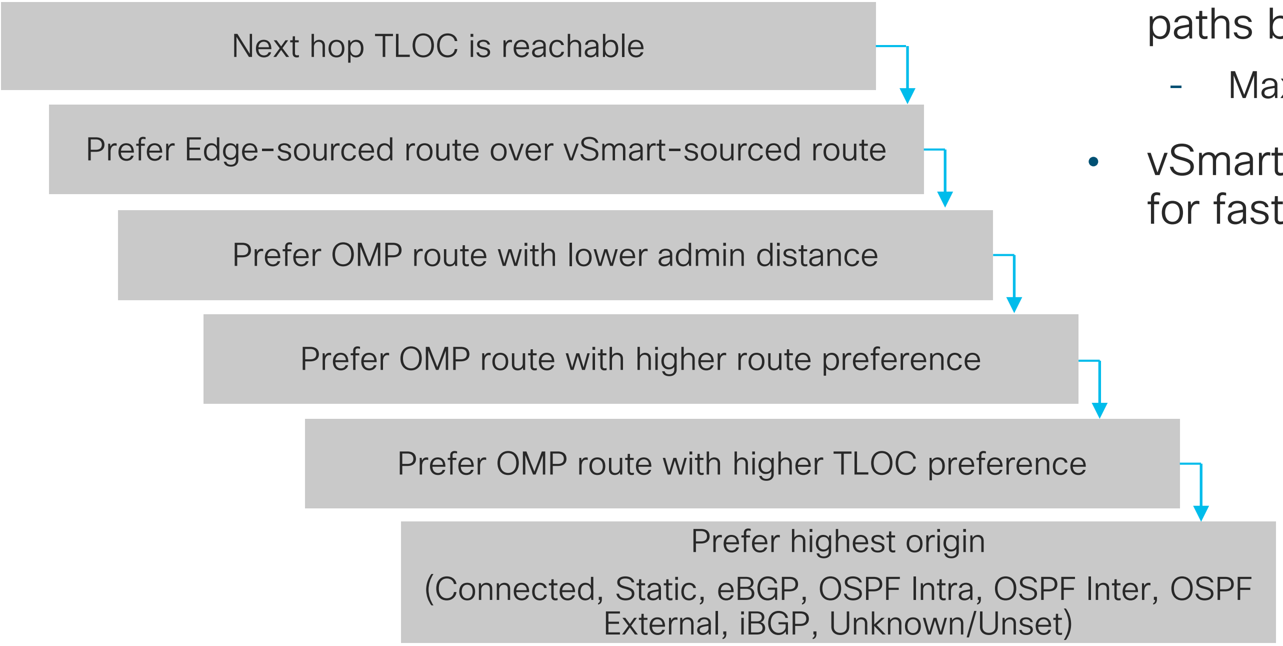
- Routes connecting locations to physical networks
- Advertised to vSmart controllers
- Most prominent attributes:
  - Site-ID
  - Encap-SPI
  - Encap-Authentication
  - Encap-Encryption
  - Public IP
  - Public Port
  - Private IP
  - Private Port
  - BFD-Status
  - Tag
  - Weight

Overlay Routing: Network Service Routes



- Routes for advertised network services, i.e. Firewall, IDS, IPS, generic
- Advertised to vSmart controllers
- Most prominent attributes:
  - VPN-ID
  - Service-ID
  - Originator System IP
  - TLOC

OMP Best-Path Algorithm and Loop Avoidance



Next hop TLOC is reachable

Prefer Edge-sourced route over vSmart-sourced route

Prefer OMP route with lower admin distance

Prefer OMP route with higher route preference

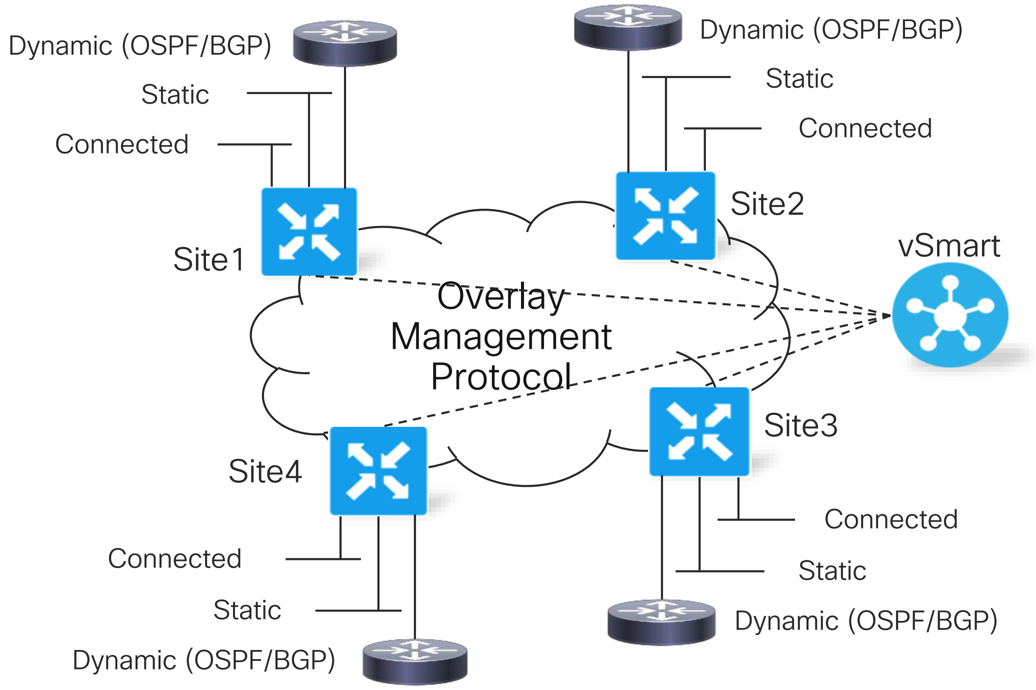
Prefer OMP route with higher TLOC preference

Prefer highest origin

(Connected, Static, eBGP, OSPF Intra, OSPF Inter, OSPF External, iBGP, Unknown/Unset)

- vSmart will advertise 4 ECMP paths by default
  - Max 16 paths
- vSmart can send backup path for faster reroute on WAN Edge

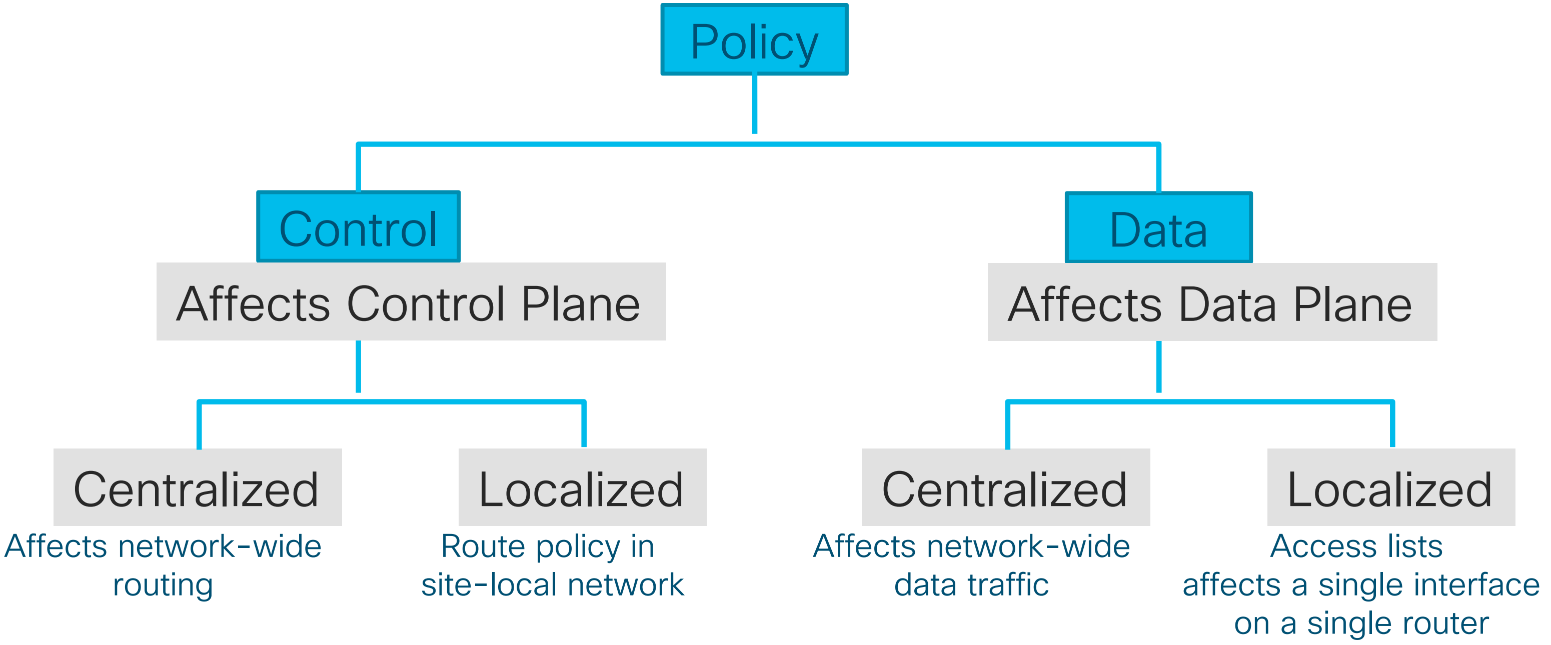
Overlay Routing



- Uniform control plane protocol
- OMP learns and translates routing information across the overlay
  - OMP routes, TLOC routes, network service routes
  - Unicast and multicast address families
  - IPv4 and IPv6
- Distribution of data-plane security parameters and policies
- Implementation of control (routing) and VPN membership policies

Policy Framework

Policy Configuration Overview



Policy

Control

Affects Control Plane

Data

Affects Data Plane

Centralized

Affects network-wide routing

Localized

Route policy in site-local network

Centralized

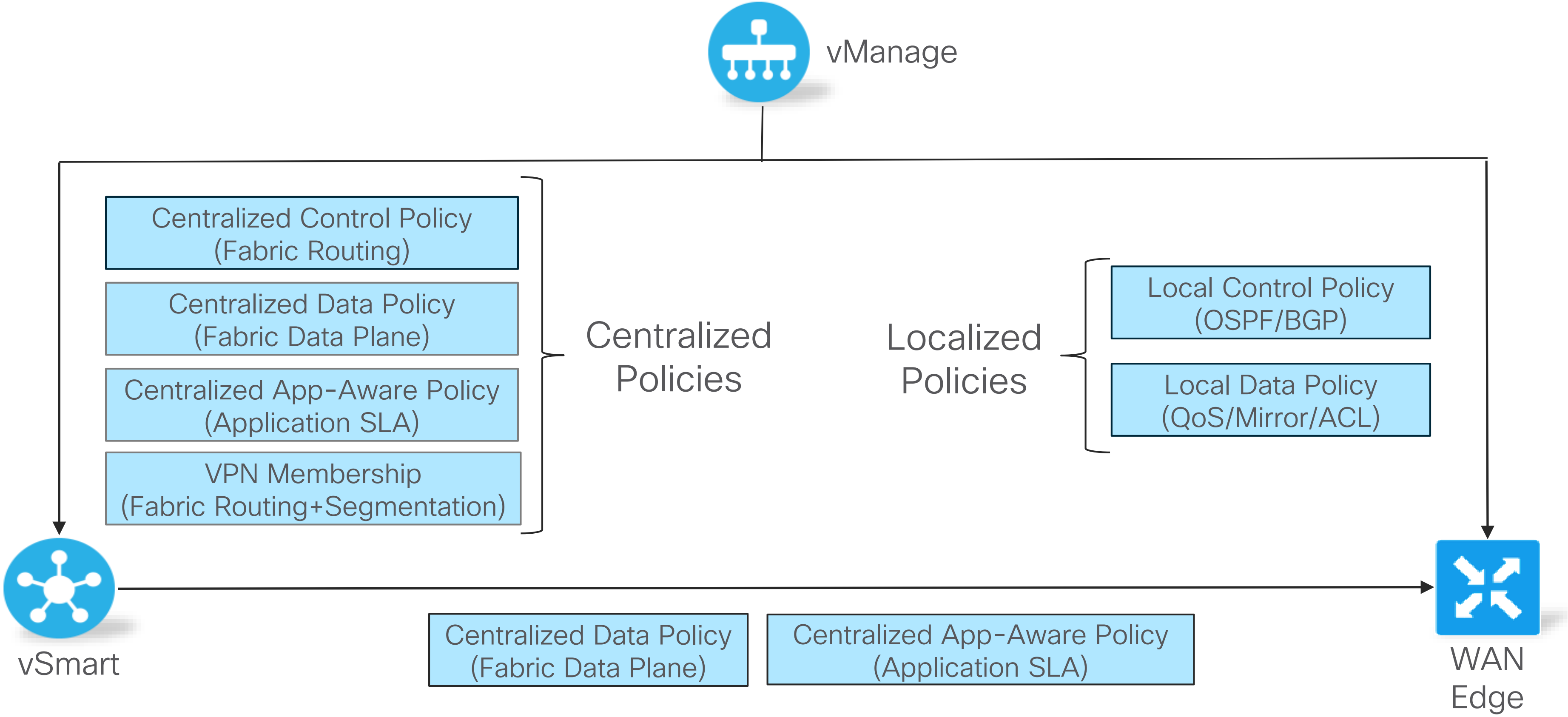
Affects network-wide data traffic

Localized

Access lists affects a single interface on a single router

- Clear separation exists between control plane and data plane policies
- Clear separation exists between centralized and localized functions

Policy Framework



vManage

Centralized Control Policy
(Fabric Routing)

Centralized Data Policy
(Fabric Data Plane)

Centralized App-Aware Policy
(Application SLA)

VPN Membership
(Fabric Routing+Segmentation)

Centralized
Policies

Localized
Policies

Local Control Policy
(OSPF/BGP)

Local Data Policy
(QoS/Mirror/ACL)

vSmart

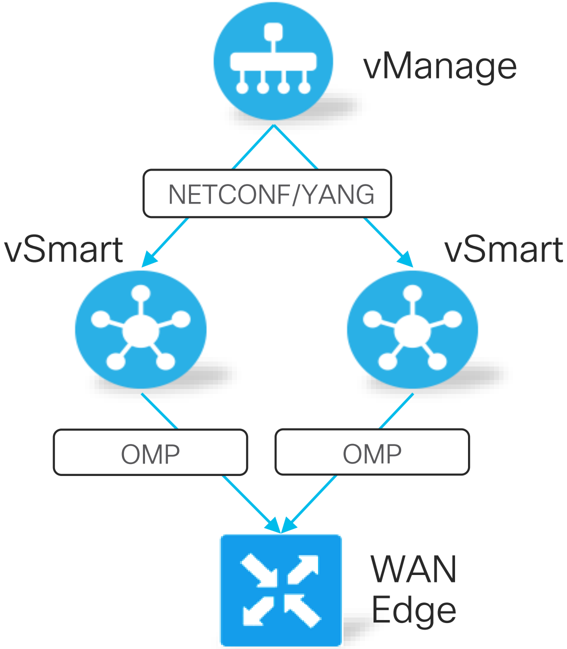
Centralized Data Policy
(Fabric Data Plane)

Centralized App-Aware Policy
(Application SLA)

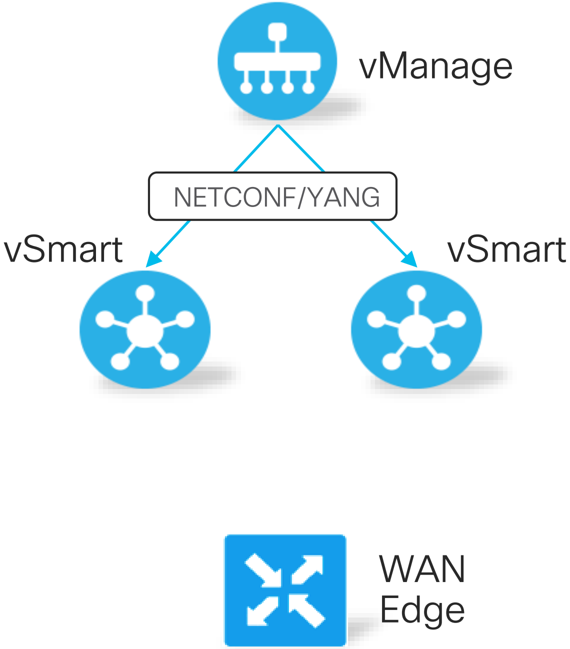
WAN
Edge

Policy Distribution

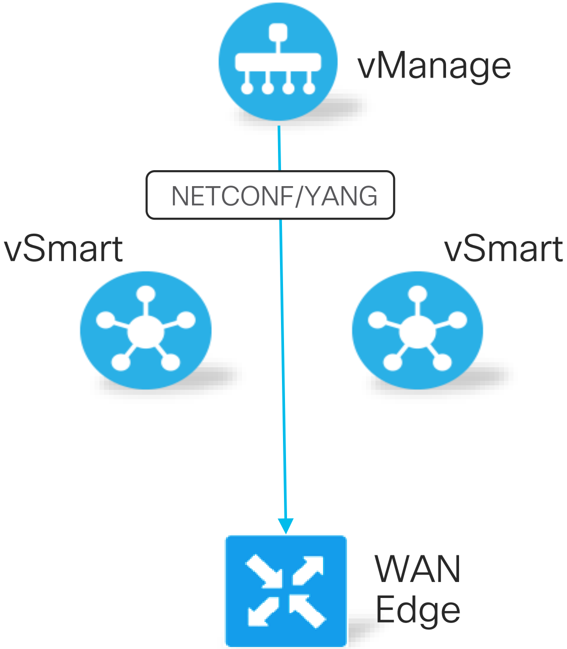
Data Policy
App Aware Routing Policy



Control Policy
VPN Membership Policy

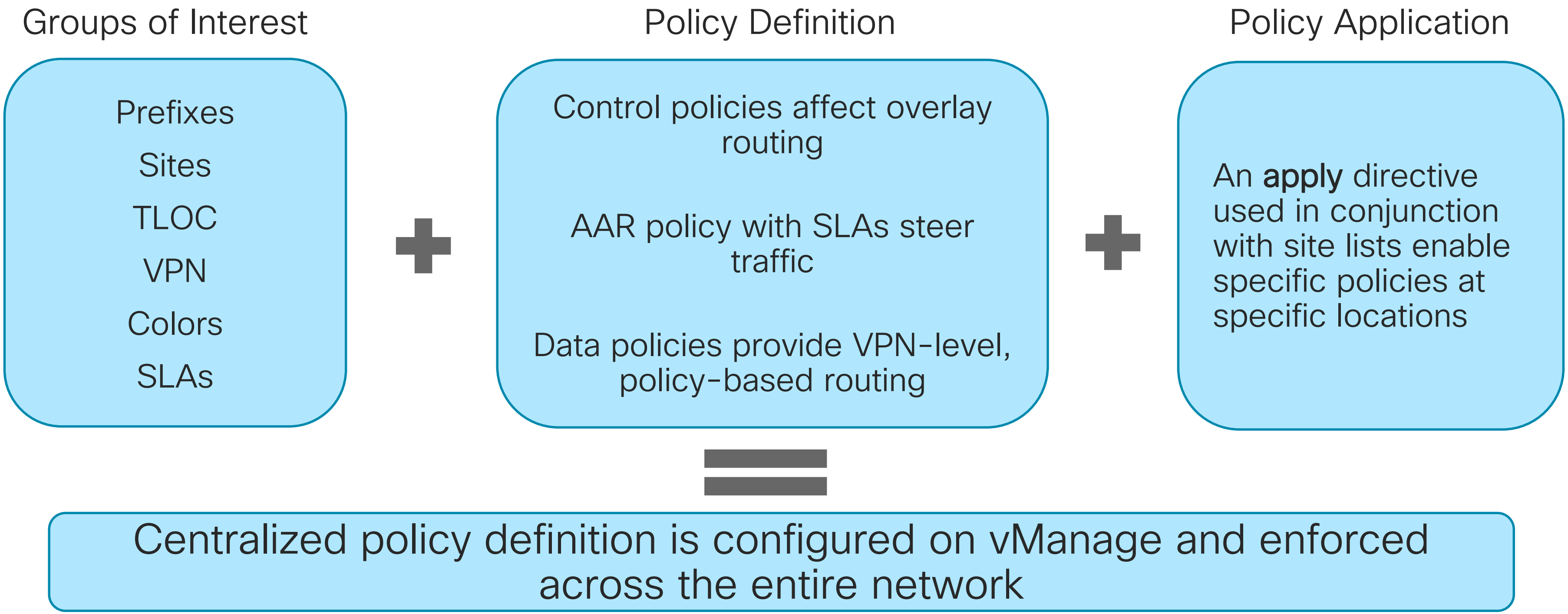


Local Policies



Building Blocks of Centralized Policies

- Assemble the three building blocks to configure vSmart policies: Groups of Interest, Policy Definition, and Policy Application.



Groups of Interest

Prefixes

Sites

TLOC

VPN

Colors

SLAs

Policy Definition

Control policies affect overlay routing

AAR policy with SLAs steer traffic

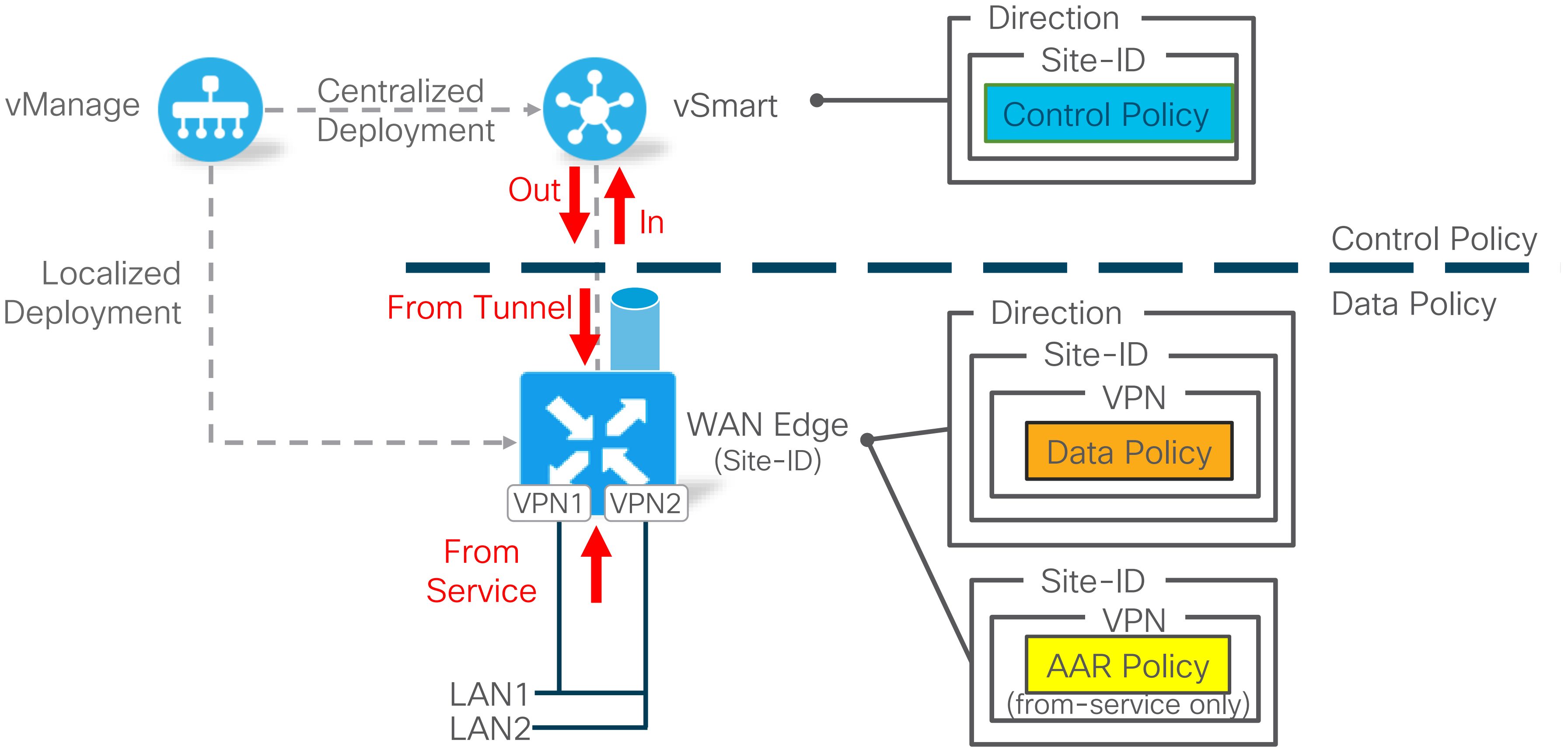
Data policies provide VPN-level, policy-based routing

Policy Application

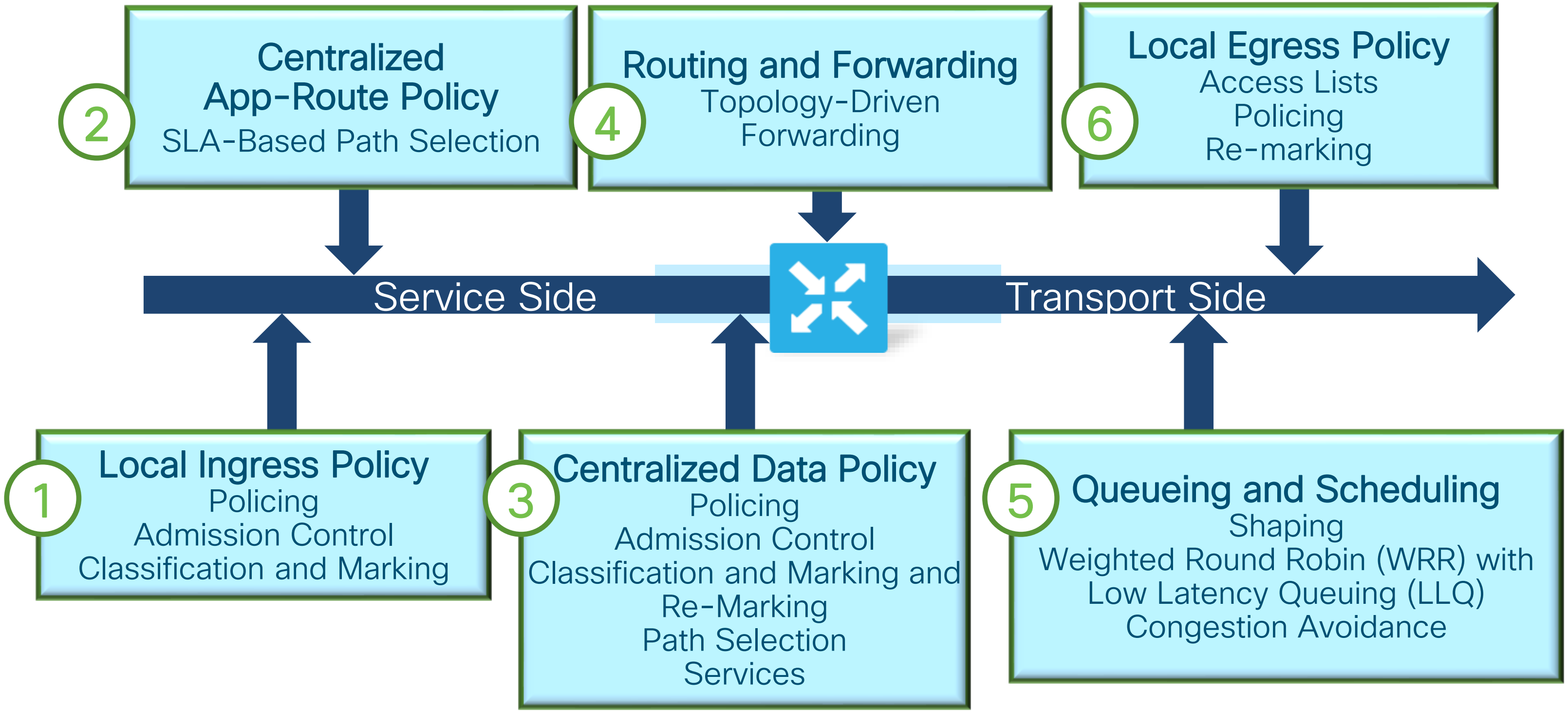
An **apply** directive used in conjunction with site lists enable specific policies at specific locations

Centralized policy definition is configured on vManage and enforced across the entire network

Where Policies are Attached



Order of Operation on WAN Edge



2 Centralized App-Route Policy
SLA-Based Path Selection

4 Routing and Forwarding
Topology-Driven Forwarding

6 Local Egress Policy
Access Lists
Policing
Re-marking

Service Side

Transport Side

1 Local Ingress Policy
Policing
Admission Control
Classification and Marking

3 Centralized Data Policy
Policing
Admission Control
Classification and Marking and Re-Marking
Path Selection
Services

5 Queueing and Scheduling
Shaping
Weighted Round Robin (WRR) with Low Latency Queuing (LLQ)
Congestion Avoidance

Policy Examples

Control Policies

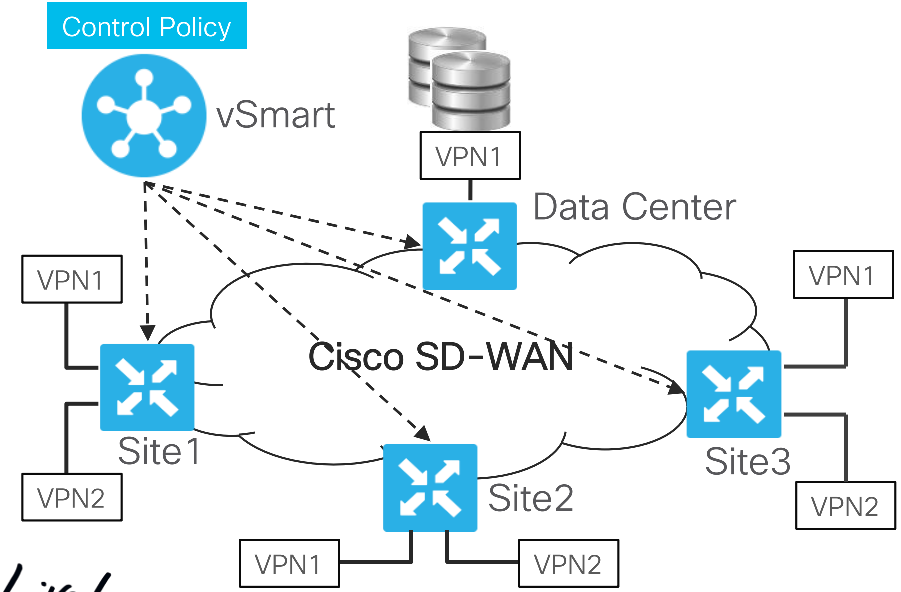
- Configured on vManage. Enabled and enforced on vSmart controllers. They **do not** get forwarded to WAN Edge routers.
- Control policies operate on OMP routing information received from or sent to WAN Edge routers. They can filter OMP updates or modify various attributes.
- Control policies can be very powerful tool changing routing behavior of the entire SD-WAN fabric
- Control policies are used to enable many services, such as:
    - Service Chaining
    - Traffic Engineering
    - Extranet VPNs
    - Service and Path affinity
    - Arbitrary VPN Topologies
    - and more …

Control Policy – Arbitrary VPN Topologies

- **Problem:** Different VPNs must be provided with different connectivity based on applications being serviced in each VPN

  VPN 1: CRM System = Hub and Spoke, VPN 2: Voice = Full Mesh

- **Solution:** Deploy control policy to control VPN topology



Policy Details:

VPN1 – vSmart advertises just the DC prefixes to Spokes and denies everything else on VPN1.

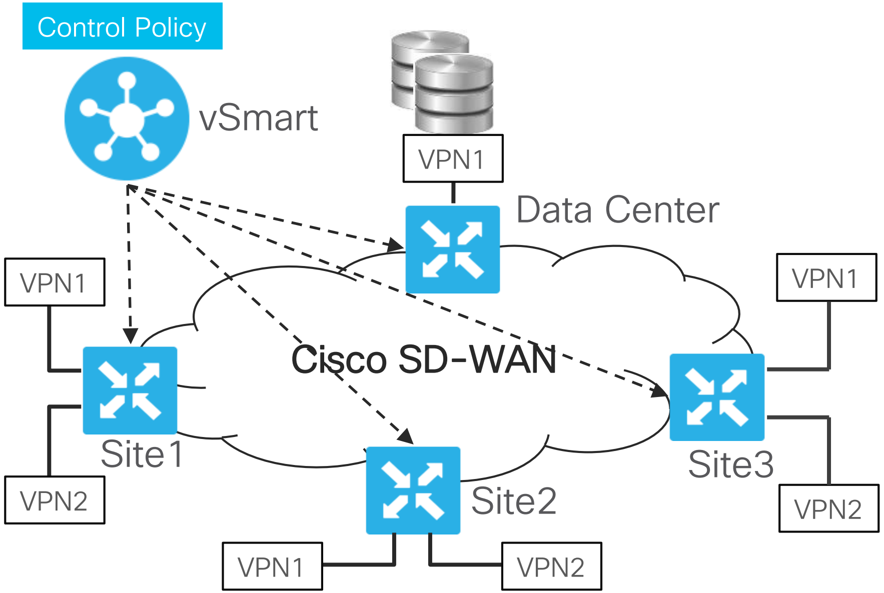
VPN2 – No filter all the prefixes are advertised to every node on VPN2

Control Policy – Arbitrary VPN Topologies

```
policy
 lists
  site-list Branches
   site-id 1-3
 !
  vpn-list CRM
   vpn 1
 !
```

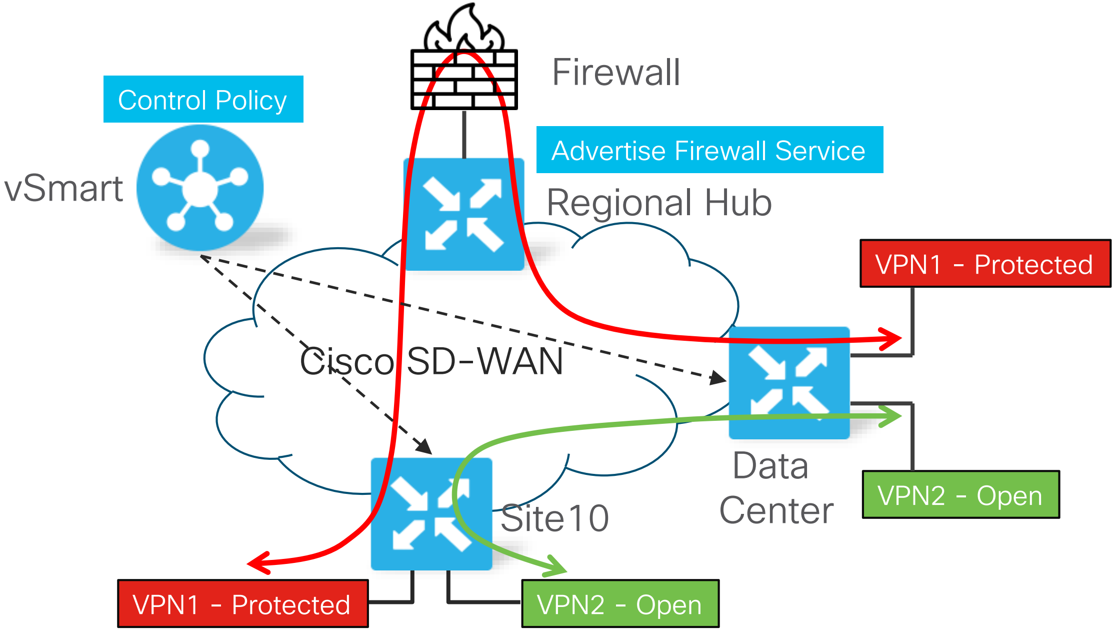
```
apply-policy
 site-list Branches
  control-policy ArbitraryTopology out
```

```
control-policy ArbitraryTopology
  sequence 10
   match route
    vpn-list CRM
    site-list Branches
   !
   action reject
  !
!
default-action accept
```



Control Policy Example – Service Insertion

- **Problem:** Certain departments require Firewall protection when interacting with data center networks, while other departments do not
- **Solution:** Deploy a service chained Firewall service per-VPN



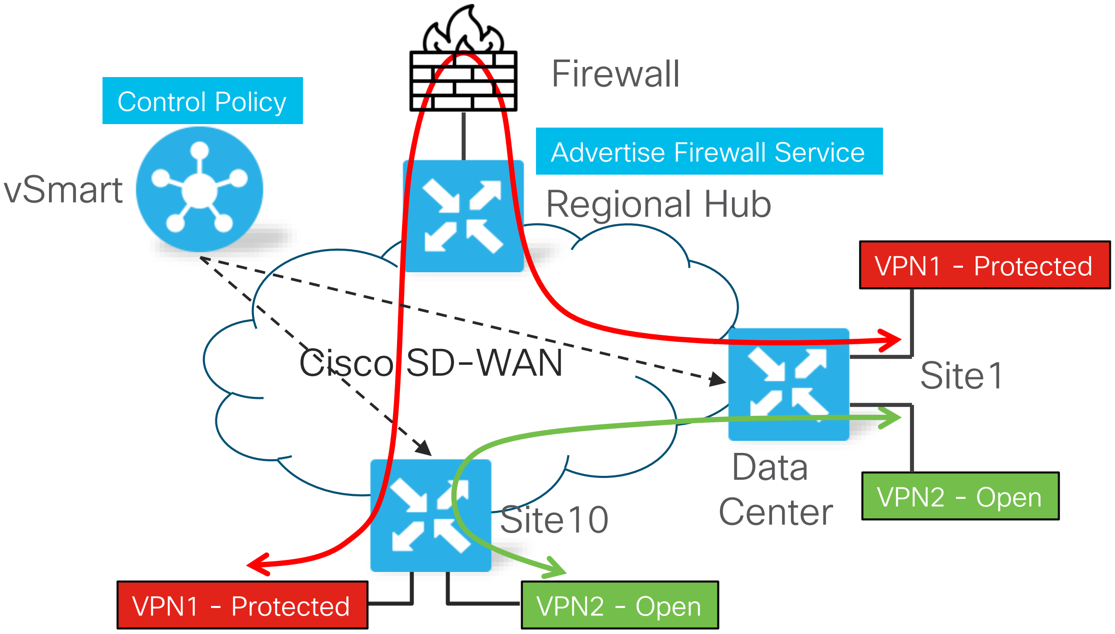
Policy Details:

Regional hub advertises availability of Firewall service

Bi-directionally modify TLOC next hop attribute for VPN1 traffic between Site1 and Data Center to point at regional hub TLOCs

Control Policy Example – Service Insertion

```
! Applied on Regional Hub
  vpn 1
    service netsvc1 address 10.0.1.1
```



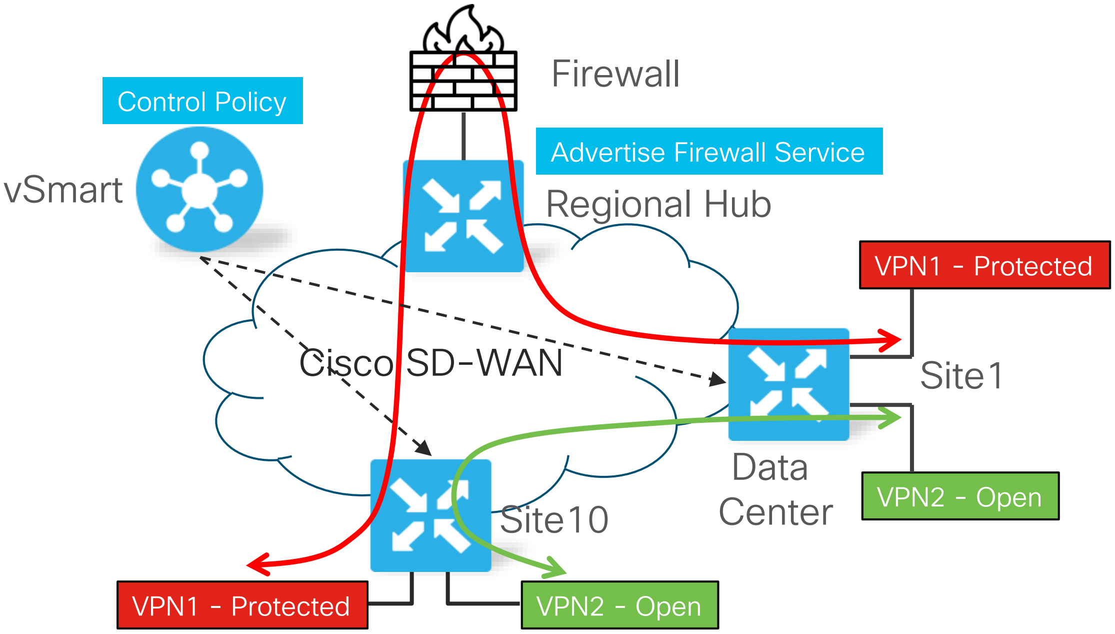
```
policy
 lists
   site-list fw-inspected
     site-id 10
   !
```

```
control-policy fw-service
    sequence 10
     match route
      vpn 1
      site-id 1
     action accept
      set service netsvc1 vpn 1
   !
   default-action accept
  !
```

```
apply-policy
 site-list fw-inspected
  control-policy fw-service out
 !
```

Control Policy Example – Service Insertion

```
! Applied on Regional Hub
  vpn 1
    service netsvc1 address 10.0.1.1
```



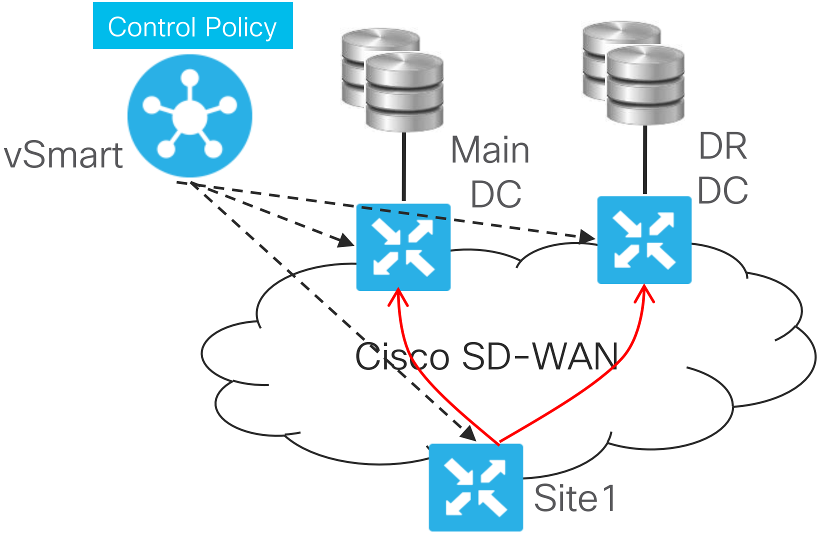
```
policy
  lists
    site-list dc
      site-id 1
    !
```

```
control-policy fw-service-return
    sequence 10
     match route
      vpn 1
      site-id 10
     action accept
      set service netsvc2 vpn 1
    !
    default-action accept
   !
```

```
apply-policy
 site-list dc
  control-policy fw-service-return out
 !
```

Control Policy Example – Data Center Priority

- **Problem:** Prefer main data center over DR data center. If main data center fails, traffic should reroute to DR data center.
- **Solution:** Deploy control policy to influence TLOC priority



Policy Details:

Set higher preference on main data center TLOCs than on DR data center TLOCs

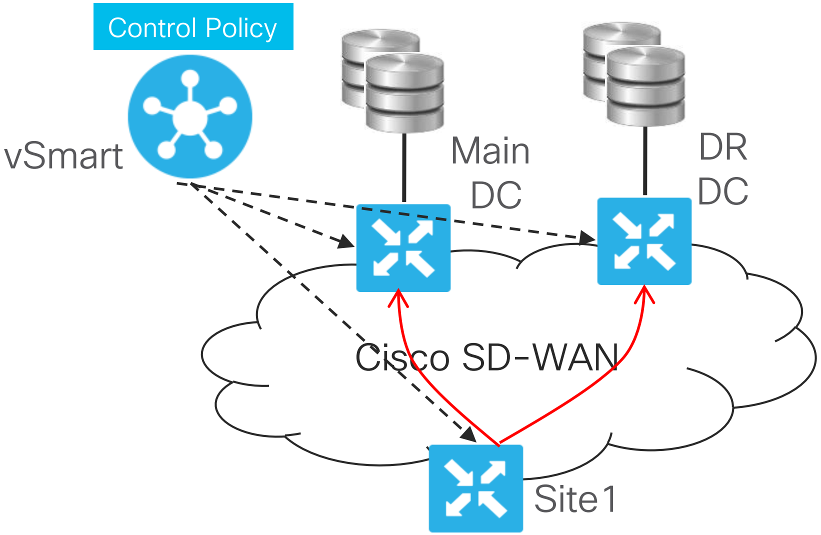
Preference is set on all TLOC colors using TLOC list

Control Policy Example – Data Center Priority

```
policy
 lists
  site-list Branches
   site-id 3-10
  tloc-list Main-DC-tlocs
   tloc-id 10.1.1.1 biz-internet
   tloc-id 10.1.1.1 mpls
```

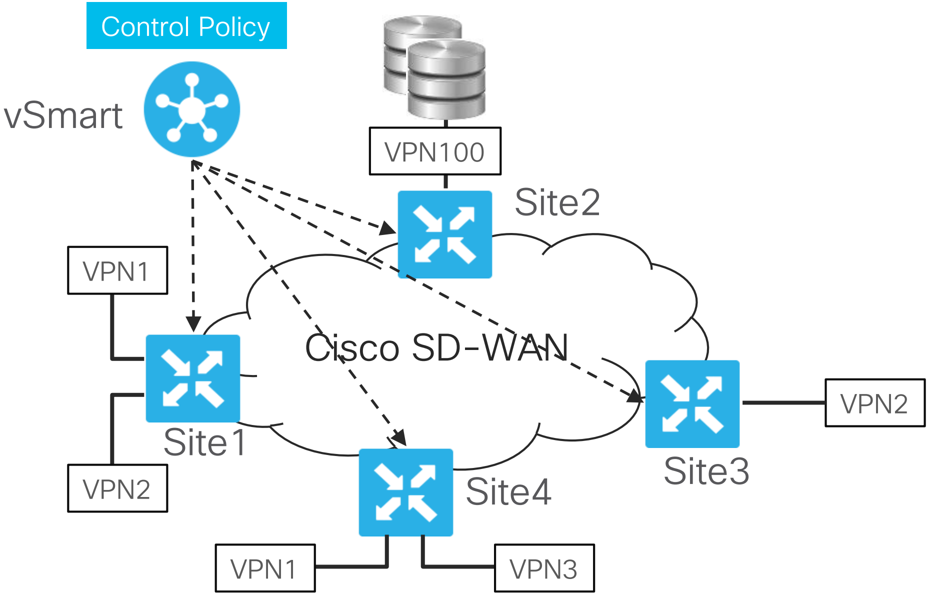
```
control-policy prefer-Main-DC
  sequence 10
   match tloc
    tloc-list Main-DC-tlocs
   action accept
    set preference 50
 default-action accept
```

```
apply-policy
 site Branches
  control-policy prefer-Main-DC out
```



Control Policy Example – Shared Services

- **Problem:** Services residing in a VPN must be shared across users residing in multiple other VPNs. Some VPNs don't need access to shared services.
- **Solution:** Deploy control policy with route exports



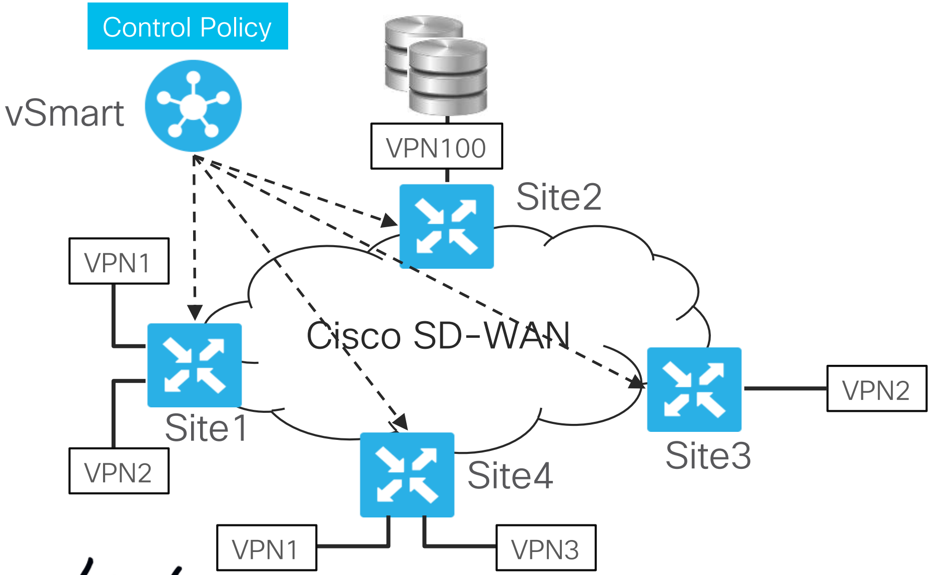
Policy Details:

Export VPN2 and VPN3 routes into shared service VPN100, and vice versa

VPN1 cannot communicate with VPN2, VPN3 or VPN100

Control Policy Example – Shared Services

```
policy
 lists
  site-list all-extranet-sites
   site-id 1-4
  vpn-list extranet-clients
   vpn-id 2-3
  prefix-list extranet-srv-prefix
   ip-prefix 10.1.1.1/32
```



```
control-policy extranet
    sequence 10
     match route
      vpn-list extranet-clients
     action accept
      export-to vpn 100
    !
    sequence 20
     match route
      vpn 100
      prefix-list extranet-srv-prefix
     action accept
      export-to vpn-list extranet-clients
      !
     !
    default-action accept
   !
```

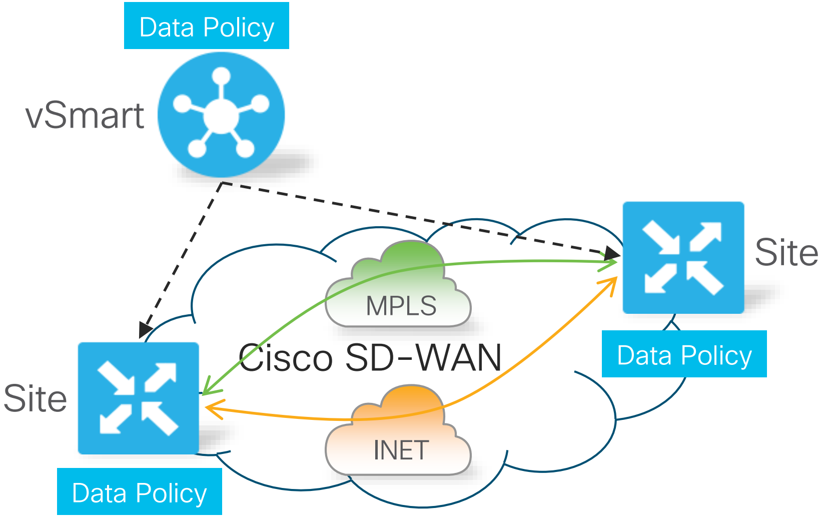
```
apply-policy
 site-list all-extranet-sites
  control-policy extranet in
 !
```

Data Policies

- Data policies are configured on vManage, enabled on vSmart controllers and enforced on WAN Edge routers
- Data policies allow easier fine-grain traffic controls when compared to control policies
- Certain objectives can be equally achieved by both control and data policies. Control policies act on OMP routing advertisements, data policies act on application traffic characteristics.
- Data policies are used to enable many services, such as:
  - Service Chaining
  - Cflowd
  - NAT
  - Traffic Policing and Counting
  - Transport Selection, TE

Data Policy Example – Path Preference

- **Problem:** Send critical applications over MPLS transport and non-critical applications over Internet transport
- **Solution:** Deploy data policy to set transport for relevant traffic



Policy Details:

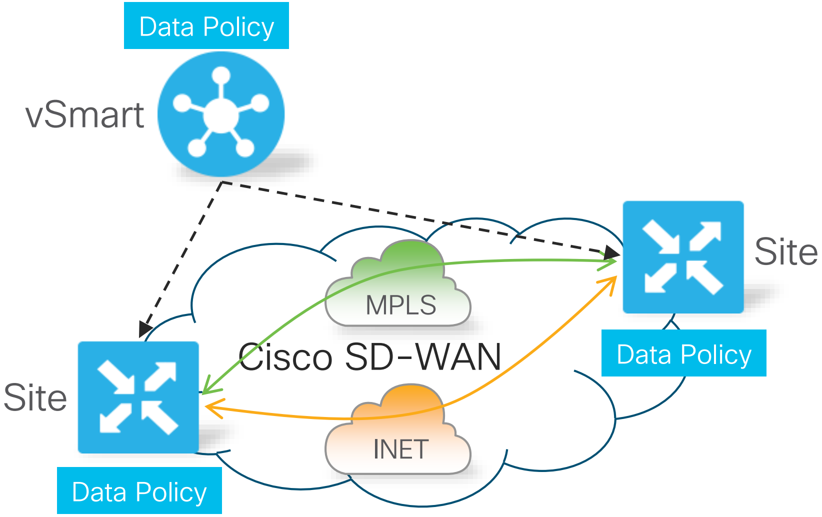
Bi-directionally set local TLOC for desired traffic

Override OMP routing decision

Fallback on overlay routing if transport fails

Data Policy Example – Path Preference

```
apply-policy
 site-list Site1-2
  data-policy prefer_mpls from-service
```

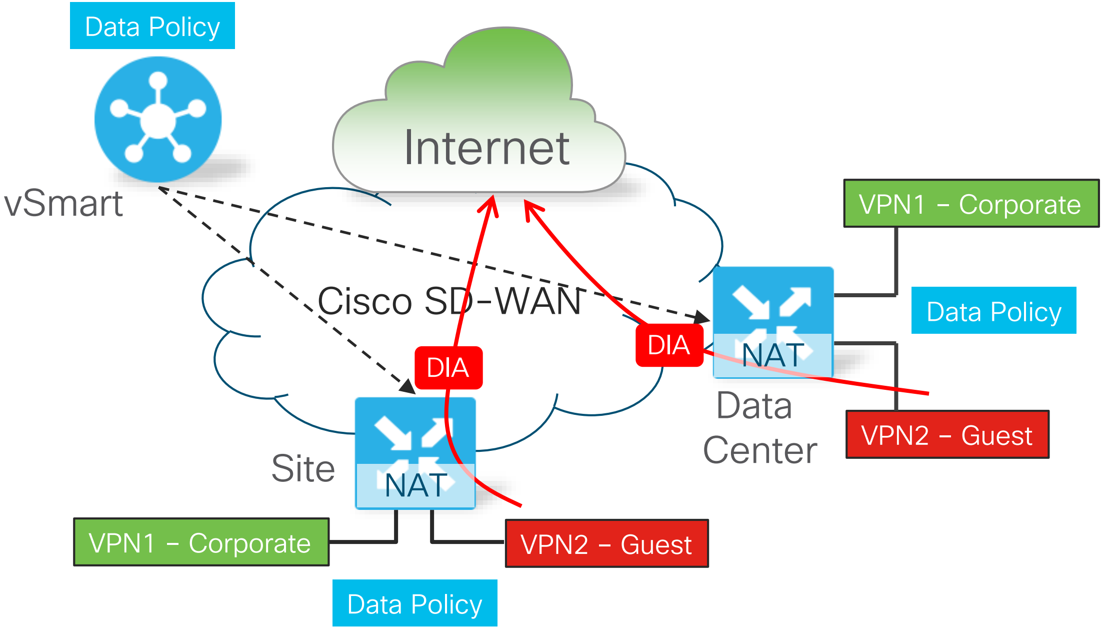


```
lists
  data-prefix-list DC-Servers
   ip-prefix 10.1.1.0/24
!
  site-list Site1-2
   site-id 1-2
  !
  vpn-list vpn10
   vpn 10
```

```
data-policy prefer_mpls
  vpn-list vpn10
   sequence 5
    match
      destination-data-prefix-list DC-Servers
      source-data-prefix-list Clients
     !
    action accept
      set
       local-tloc-list
        color mpls
       !
default-action accept
```

Data Policy Example – DIA with NAT

- **Problem:** Local Internet exit needs to be provided to guest WiFi users. Guest WiFi users need to be isolated from corporate users.
- **Solution:** Deploy a data policy in guest VPN with a network address translation

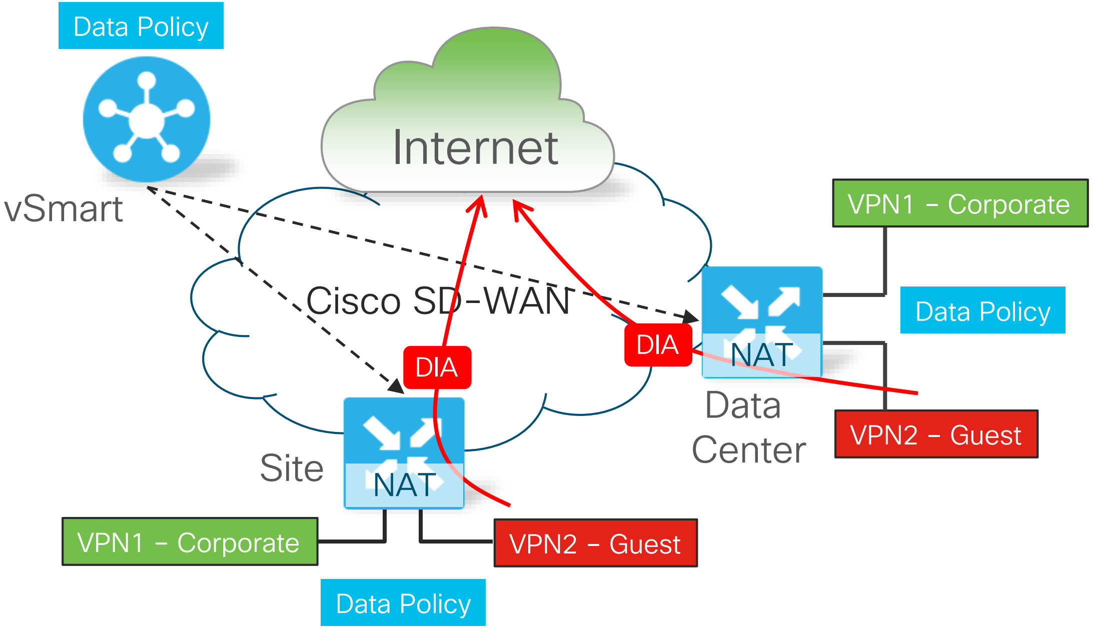


Policy Details:

Define NAT on transport side interface

Force matching traffic in guest WiFi VPN through a locally defined NAT on transport side interface

Data Policy Example – DIA with NAT



```
apply-policy
 site-list Site1-2
  data-policy guest-wifi from-service
```

```
site-list Site1-2
   site-id 1-2
  !
  vpn-list guest-vpn
   vpn 100
```

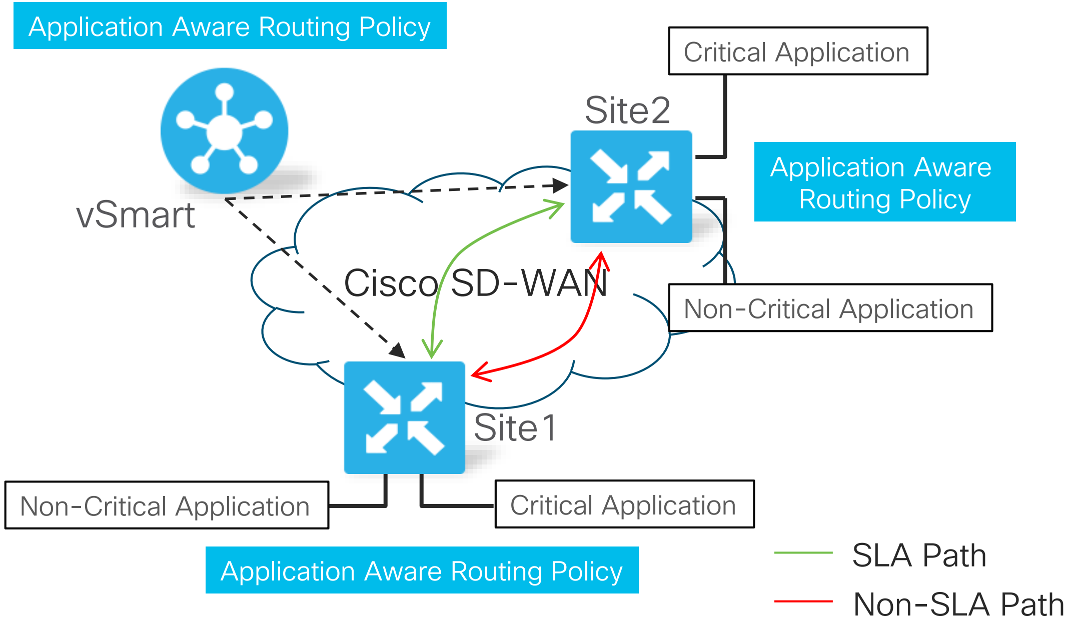
```
policy data-policy guest-wifi
  vpn-list guest-vpn
    sequence 10
      action accept
         nat use-vpn 0
      !
    !
    default-action drop
  !
```

Application Aware Routing Policies

- Application Aware Routing policies are configured on vManage, enabled on vSmart controllers and enforced on WAN Edge routers
- Application Aware Routing policies ensure SLA compliant path through the SD-WAN fabric
- The SLA class defines loss, latency and jitter thresholds
- Application Aware Routing policy matches on the application traffic of interest. Match can be based on 6-tuple matching or DPI signature.
- Application Aware Routing policy is enforced in VPNs and sites of interest

Application Aware Routing Policy Example

- **Problem:** Critical applications traffic needs to take SLA compliant path through the network to achieve better user quality of experience
- **Solution:** Deploy Application Aware Routing policy for critical application traffic



Policy Details:

Define SLA class for acceptable SLA thresholds for loss, latency and jitter

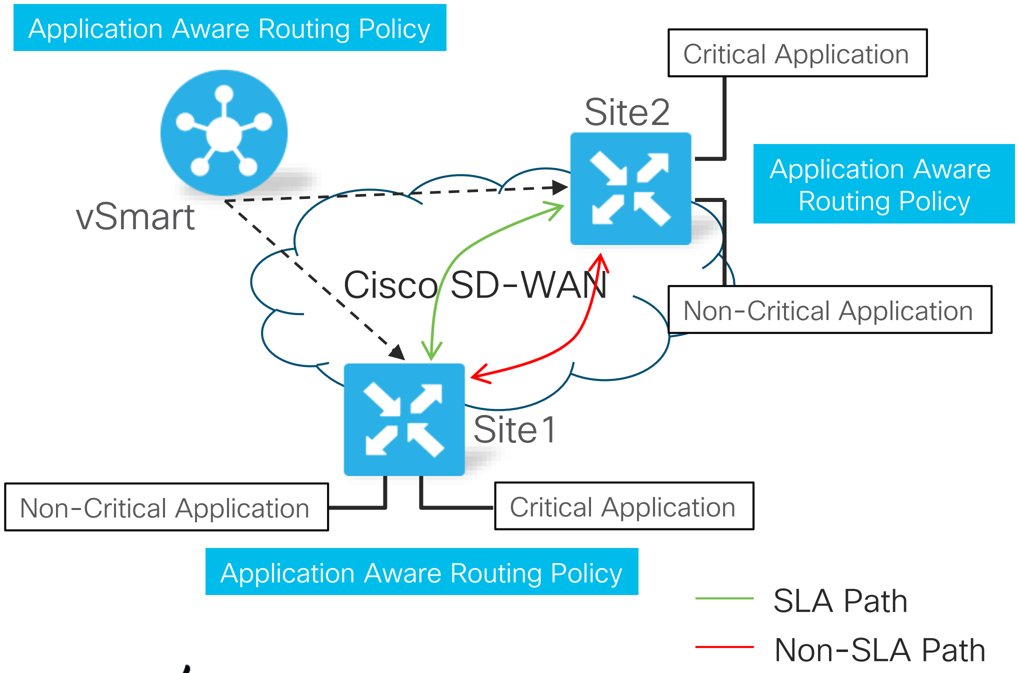
Apply SLA class to the application aware routing policy matching on the application traffic of interest

Bi-directionally apply application aware routing policy in the VPNs of choice

Application Aware Routing Policy Example

```
apply-policy
 site-list spokes
  app-route-policy voice-priority
```

```
lists
  app-list voice
   app-family audio_video
  site-list spokes
   site-id 3-5
  vpn-list vpn10
   vpn 10
```



Application Aware Routing Policy

vSmart

Cisco SD-WAN

Site2

Critical Application

Application Aware Routing Policy

Non-Critical Application

Site1

Non-Critical Application

Critical Application

Application Aware Routing Policy

SLA Path

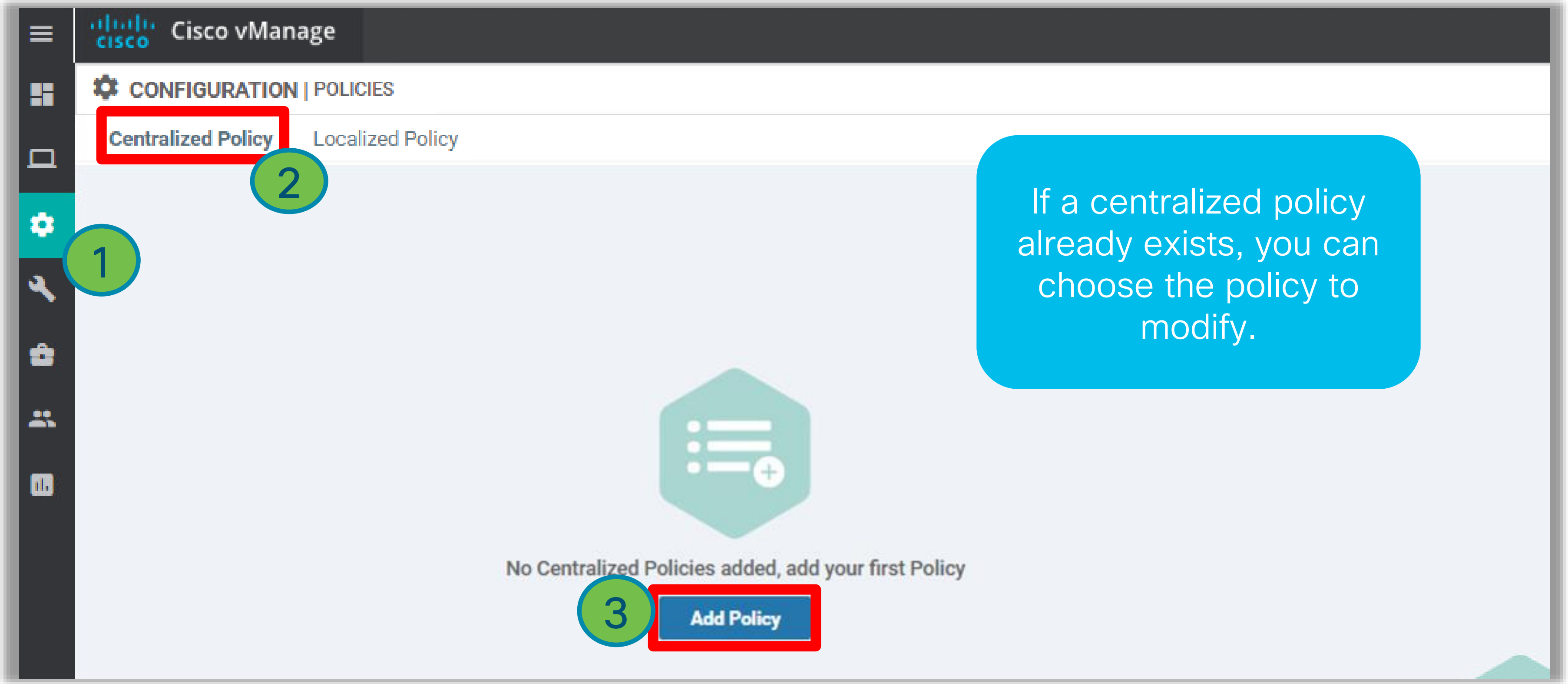
Non-SLA Path

```
policy
  sla-class sla-voice
   latency 150
   loss 1
  !
 app-route-policy voice-priority
  vpn-list vpn10
    sequence 1
     match
      app-list voice
     !
     action
      sla-class sla-web  preferred-color mpls
      backup-sla-preferred-color mpls
```

Policy Definition

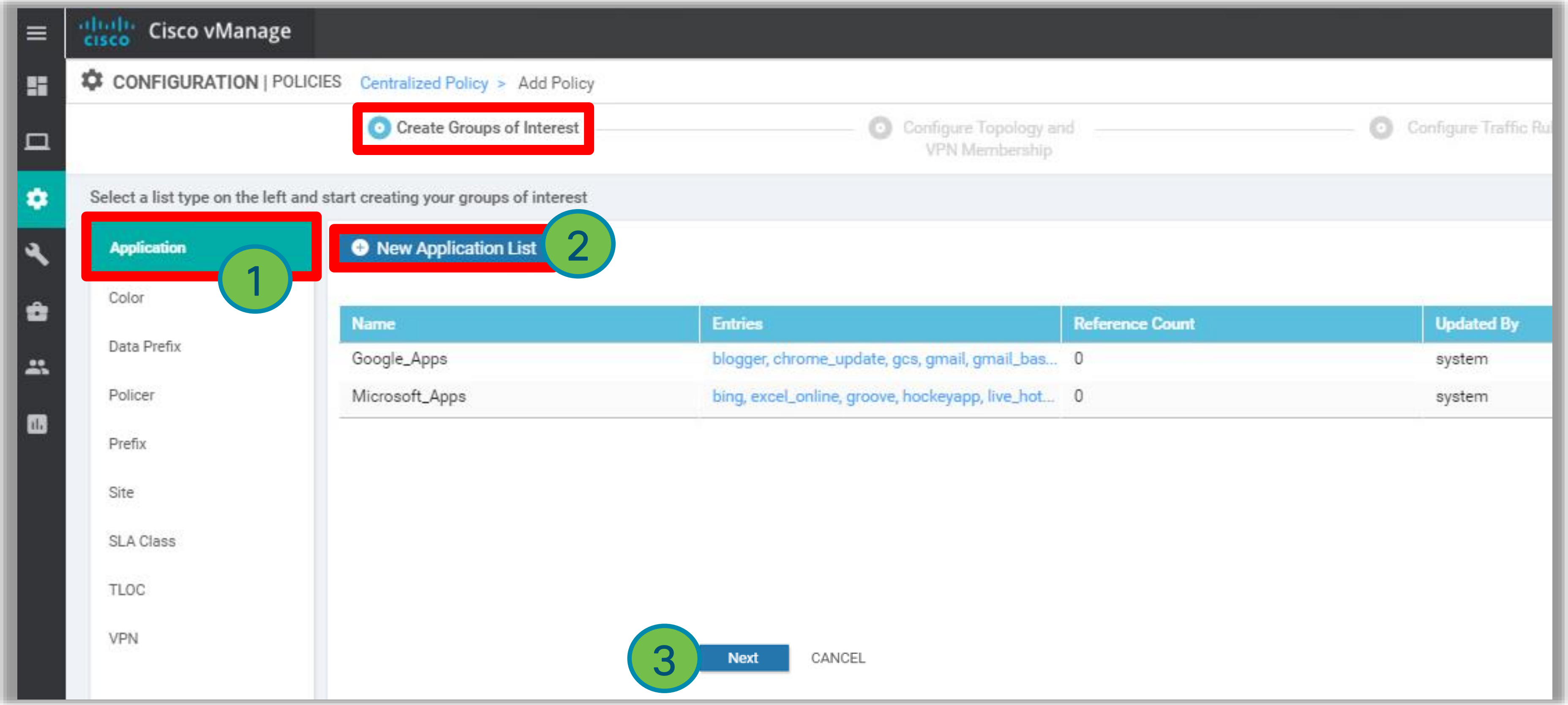
Adding a Centralized Policy

- Click **Centralized Policy** on the Cisco vManage Configuration | Policies screen.



If a centralized policy already exists, you can choose the policy to modify.

Step1a: Create Groups of Interest



Cisco vManage

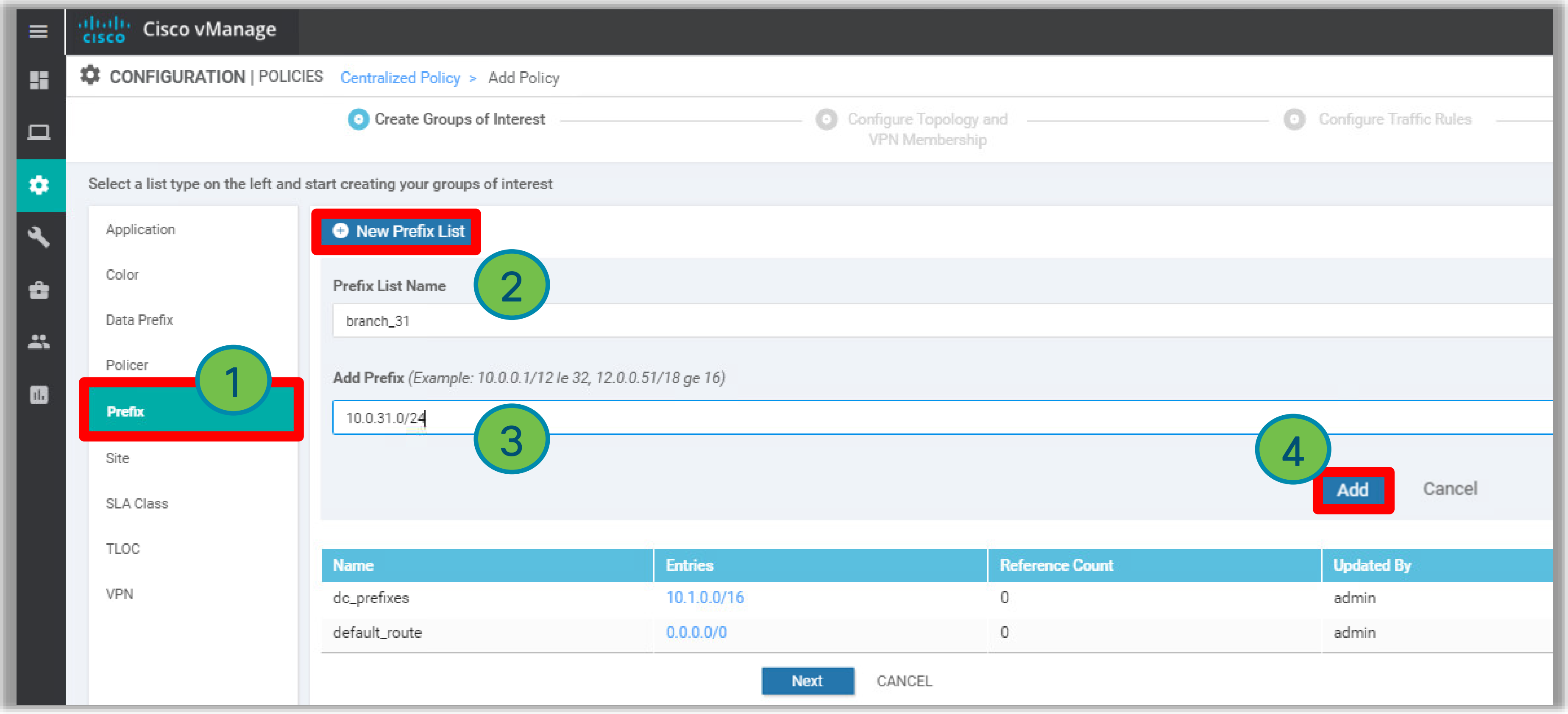
CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest — Configure Topology and VPN Membership — Configure Traffic Ru

Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Updated By
Google_Apps	blogger, chrome_update, gcs, gmail, gmail_bas...	0	system
Microsoft_Apps	bing, excel_online, groove, hockeyapp, live_hot...	0	system

Step1b: Create Groups of Interest – Prefix Lists



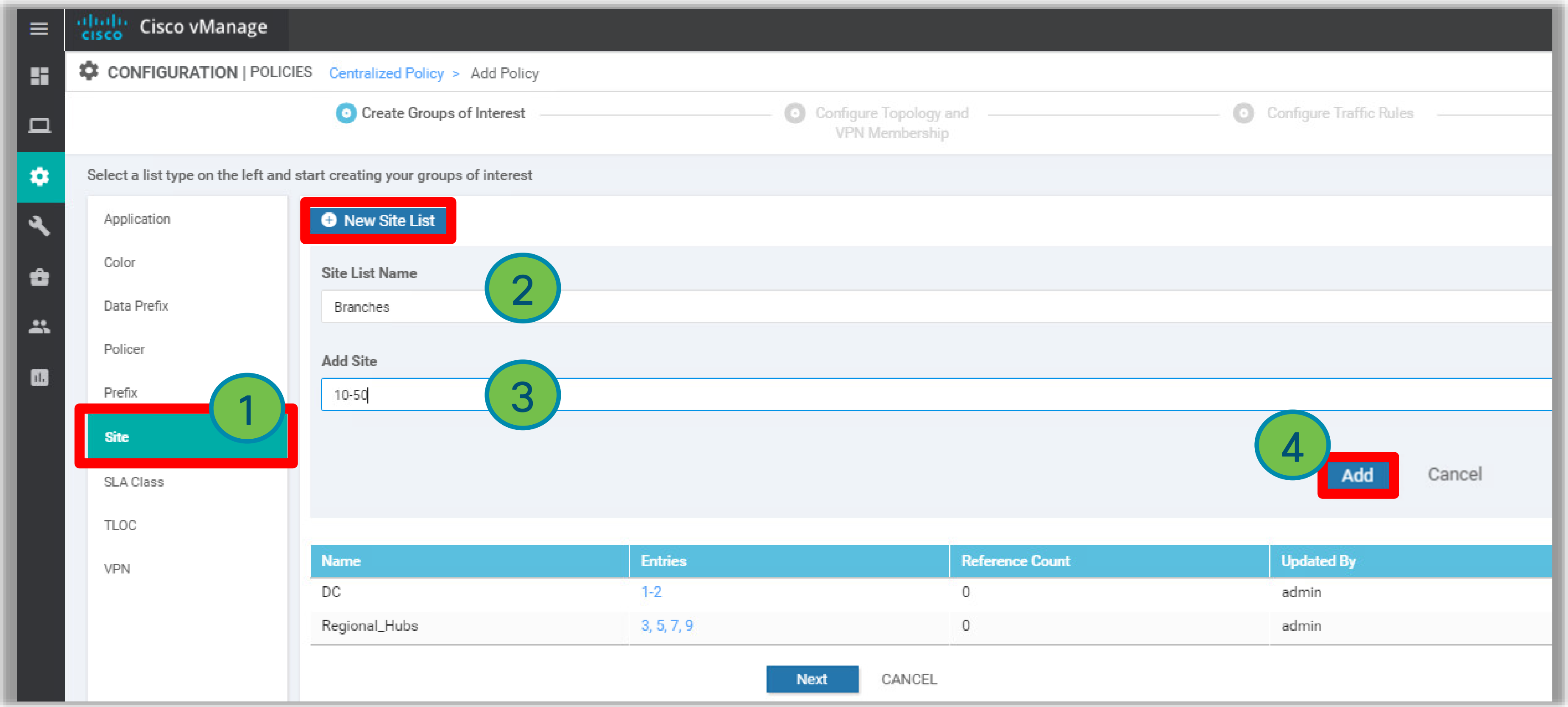
Select a list type on the left and start creating your groups of interest

Prefix List Name: branch_31

Add Prefix *(Example: 10.0.0.1/12 le 32, 12.0.0.51/18 ge 16)*: 10.0.31.0/24

Name	Entries	Reference Count	Updated By
dc_prefixes	10.1.0.0/16	0	admin
default_route	0.0.0.0/0	0	admin

Step1c: Create Groups of Interest – Site Lists



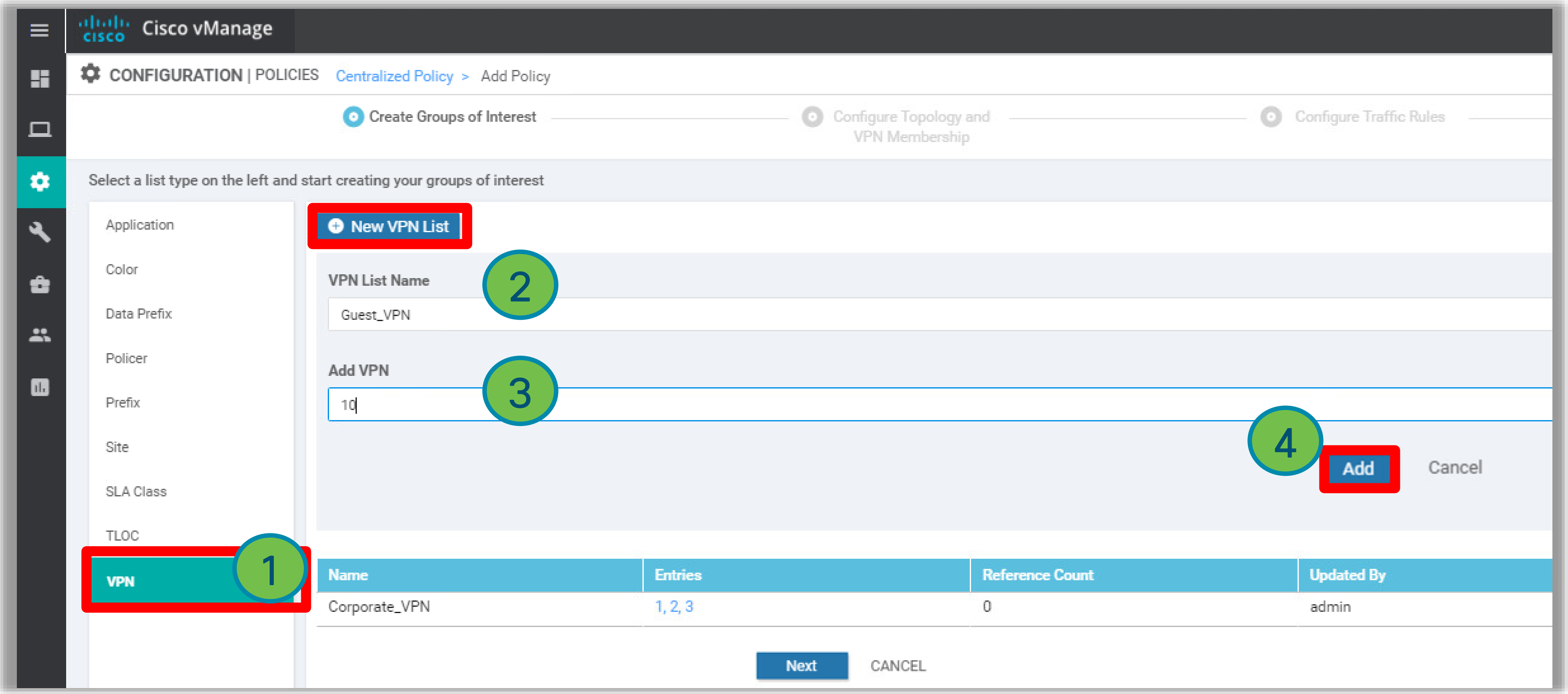
Select a list type on the left and start creating your groups of interest

Site List Name: Branches

Add Site: 10-50

Name	Entries	Reference Count	Updated By
DC	1-2	0	admin
Regional_Hubs	3, 5, 7, 9	0	admin

Step1d: Create Groups of Interest – VPN Lists



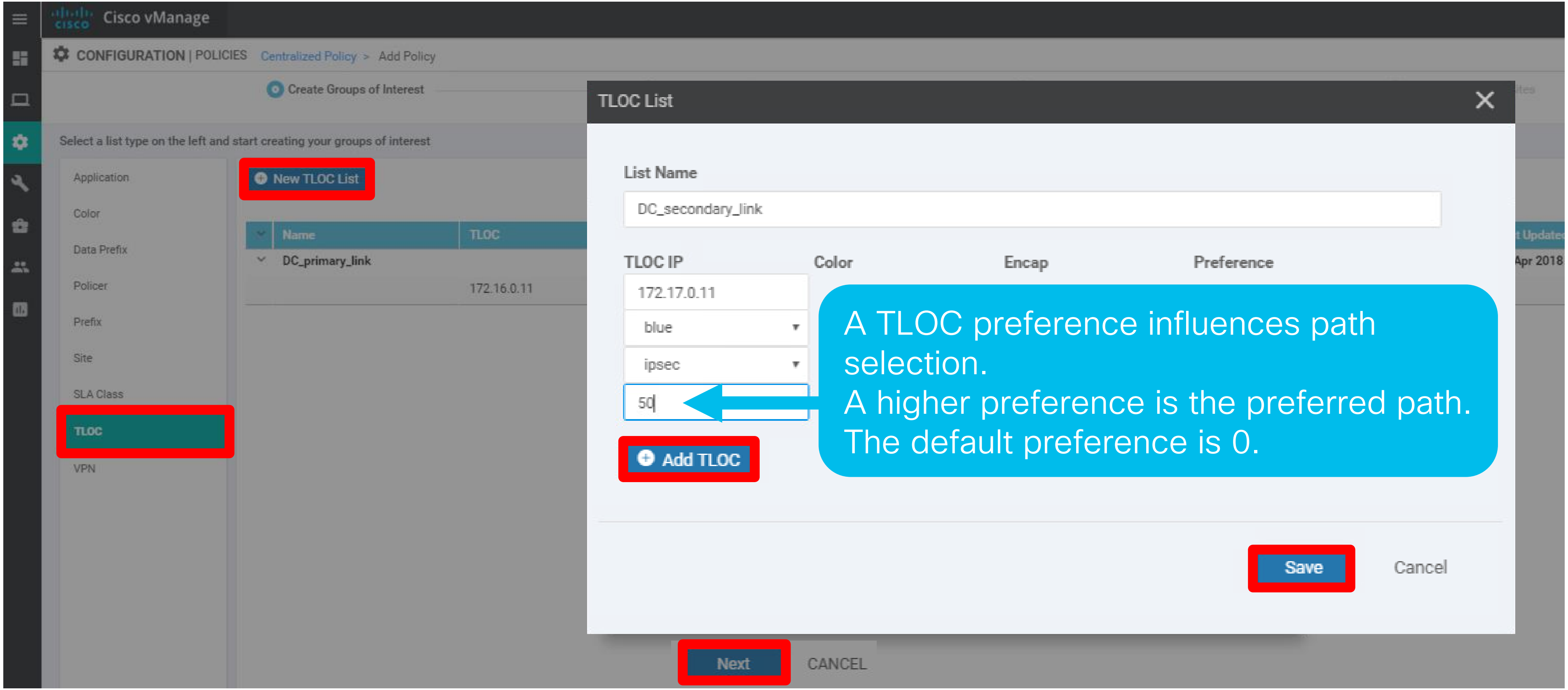
Select a list type on the left and start creating your groups of interest

VPN List Name: Guest_VPN

Add VPN: 10

Name	Entries	Reference Count	Updated By
Corporate_VPN	1, 2, 3	0	admin

Step1e: Create Groups of Interest – TLOC Lists



Select a list type on the left and start creating your groups of interest

Name	TLOC
DC_primary_link	
	172.16.0.11

List Name: DC_secondary_link

TLOC IP: 172.17.0.11

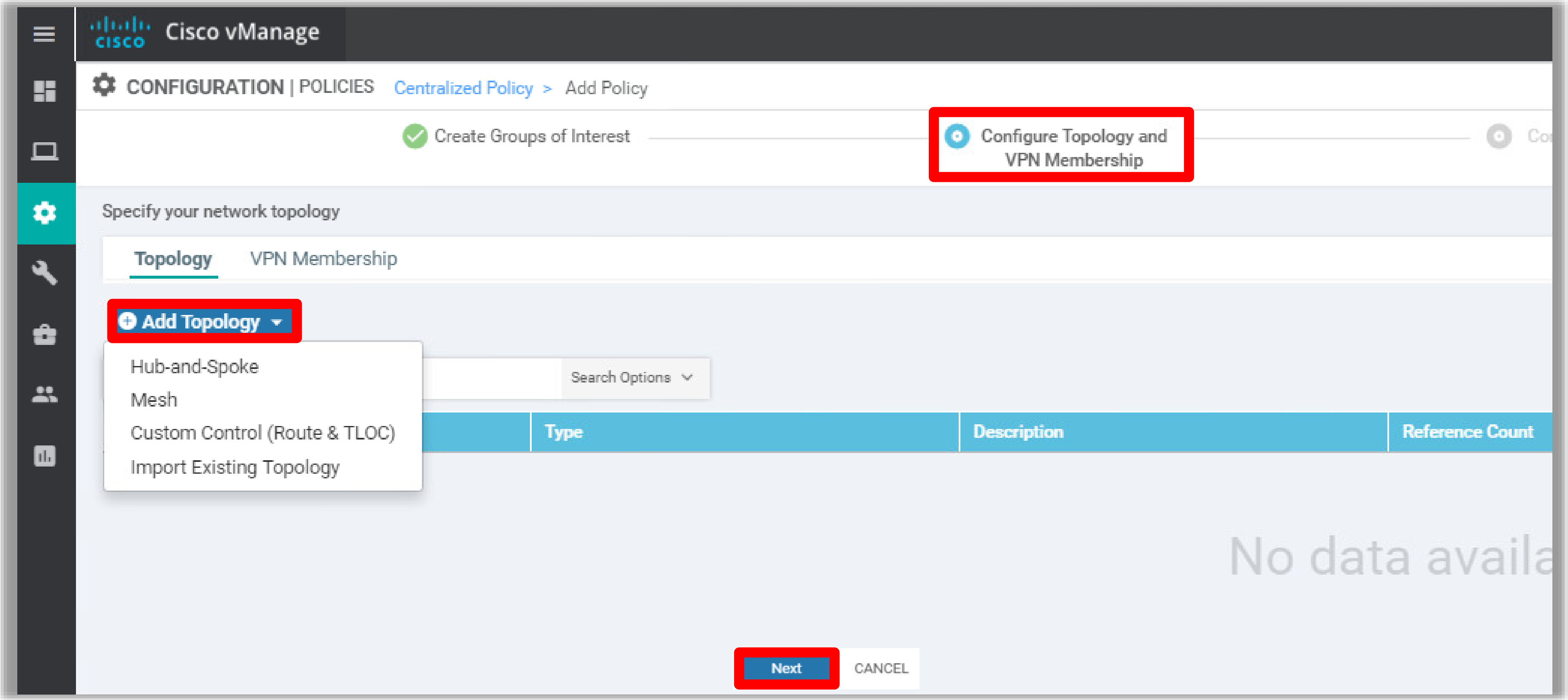
Color: blue

Encap: ipsec

Preference: 50

A TLOC preference influences path selection.
A higher preference is the preferred path.
The default preference is 0.

Step2a: Define a Topology (Control Policy)



Cisco vManage

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest

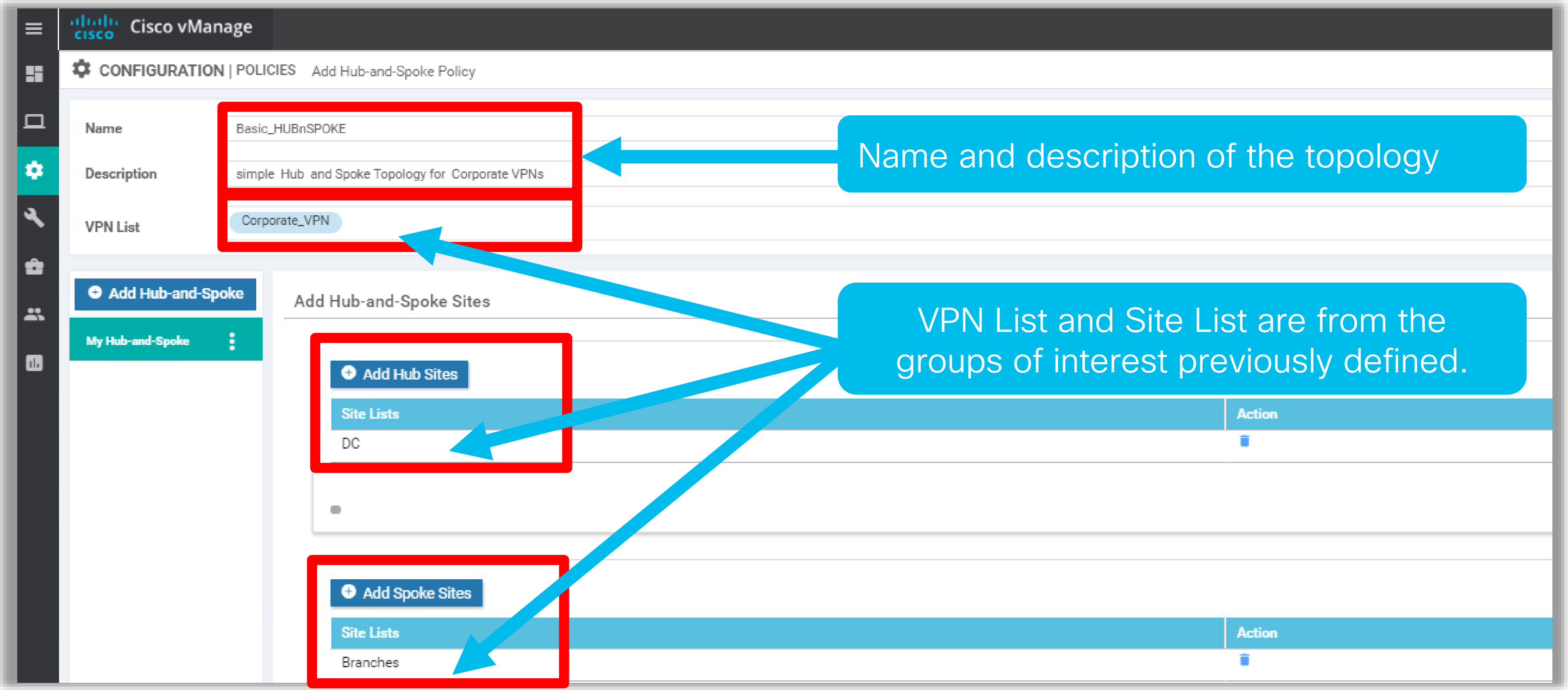
Configure Topology and VPN Membership

Co

Specify your network topology

Topology VPN Membership

Step2b: Define a Topology – Simple Hub and Spoke



Name: Basic_HUBnSPOKE

Description: simple Hub and Spoke Topology for Corporate VPNs

VPN List: Corporate_VPN

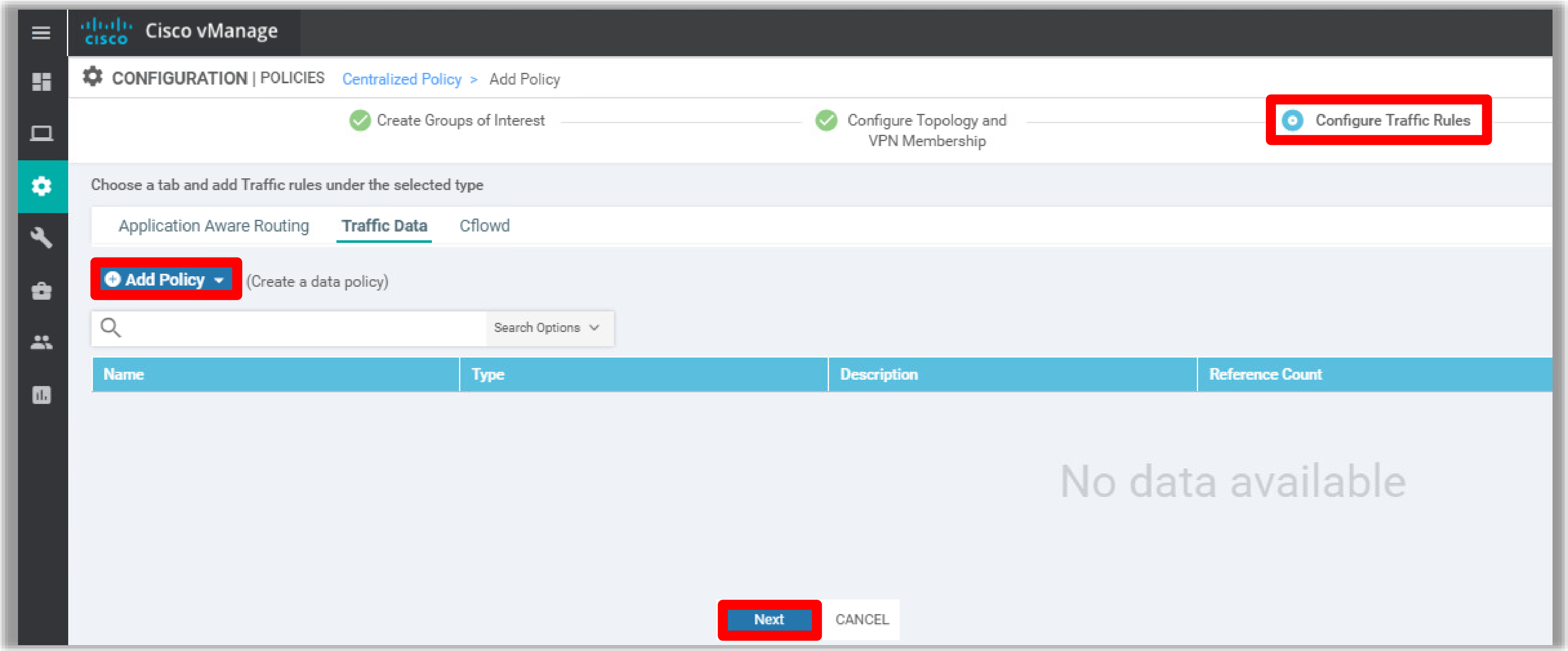
Site Lists	Action
DC	🗑

Site Lists	Action
Branches	🗑

Name and description of the topology

VPN List and Site List are from the groups of interest previously defined.

Step3a: Configure Traffic Rules (Data Policy)



Cisco vManage

CONFIGURATION | POLICIES Centralized Policy > Add Policy

✓ Create Groups of Interest ✓ Configure Topology and VPN Membership ○ Configure Traffic Rules

Choose a tab and add Traffic rules under the selected type

Application Aware Routing | **Traffic Data** | Cflowd

⊕ Add Policy ▾ (Create a data policy)

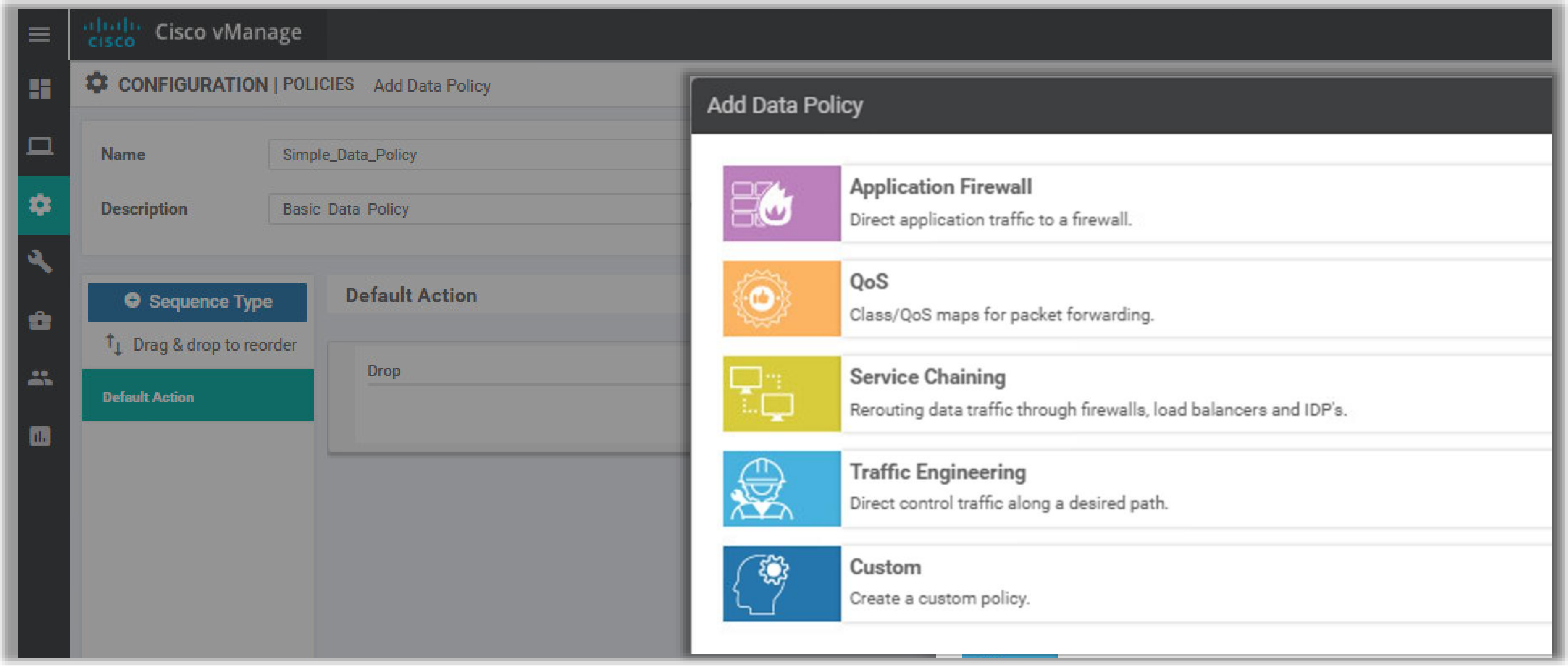
Search Options

Name	Type	Description	Reference Count

No data available

Next CANCEL

Step3b: Configure Traffic Rules (Data Policy)



CONFIGURATION | POLICIES Add Data Policy

Name: Simple_Data_Policy

Description: Basic Data Policy

Sequence Type

Drag & drop to reorder

Default Action

Default Action

Drop

Add Data Policy

Application Firewall
Direct application traffic to a firewall.

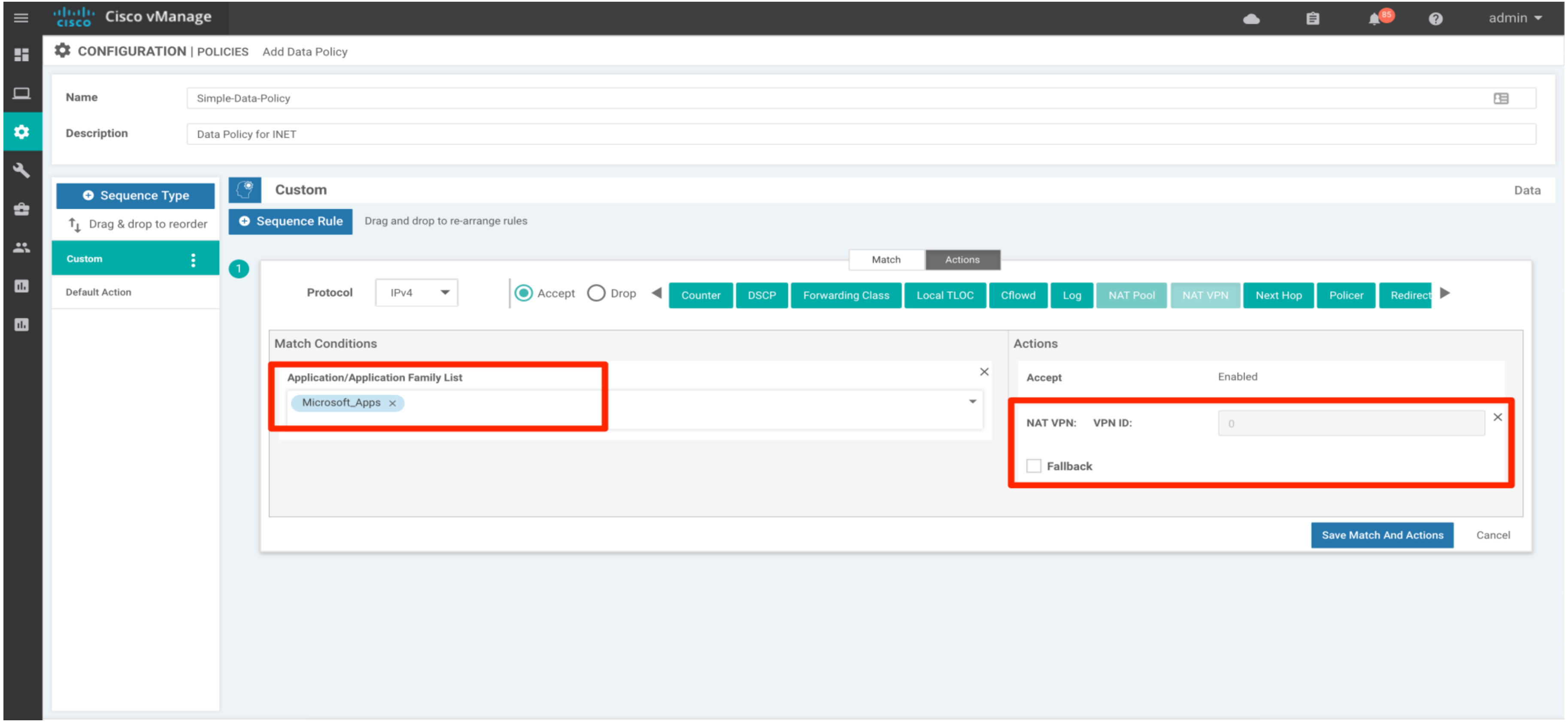
QoS
Class/QoS maps for packet forwarding.

Service Chaining
Rerouting data traffic through firewalls, load balancers and IDP's.

Traffic Engineering
Direct control traffic along a desired path.

Custom
Create a custom policy.

Step3c: Configure Traffic Rules (Data Policy)



Name: Simple-Data-Policy

Description: Data Policy for INET

Protocol: IPv4

● Accept ○ Drop

Match Conditions

Application/Application Family List: Microsoft_Apps

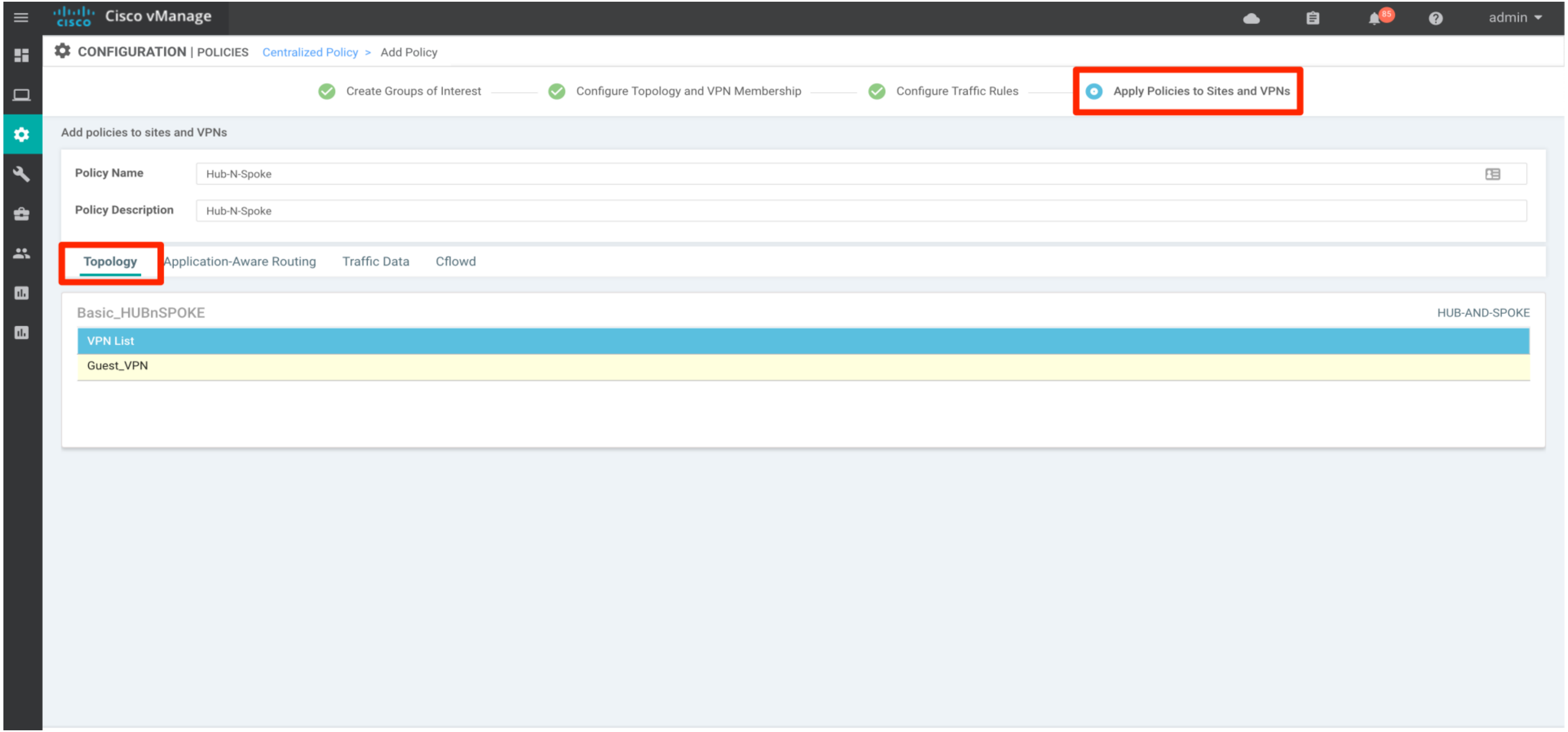
Actions

Accept: Enabled

NAT VPN: VPN ID: 0

□ Fallback

Step4a: Applying Control Policy



Cisco vManage

admin

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest — Configure Topology and VPN Membership — Configure Traffic Rules — Apply Policies to Sites and VPNs

Add policies to sites and VPNs

Policy Name: Hub-N-Spoke

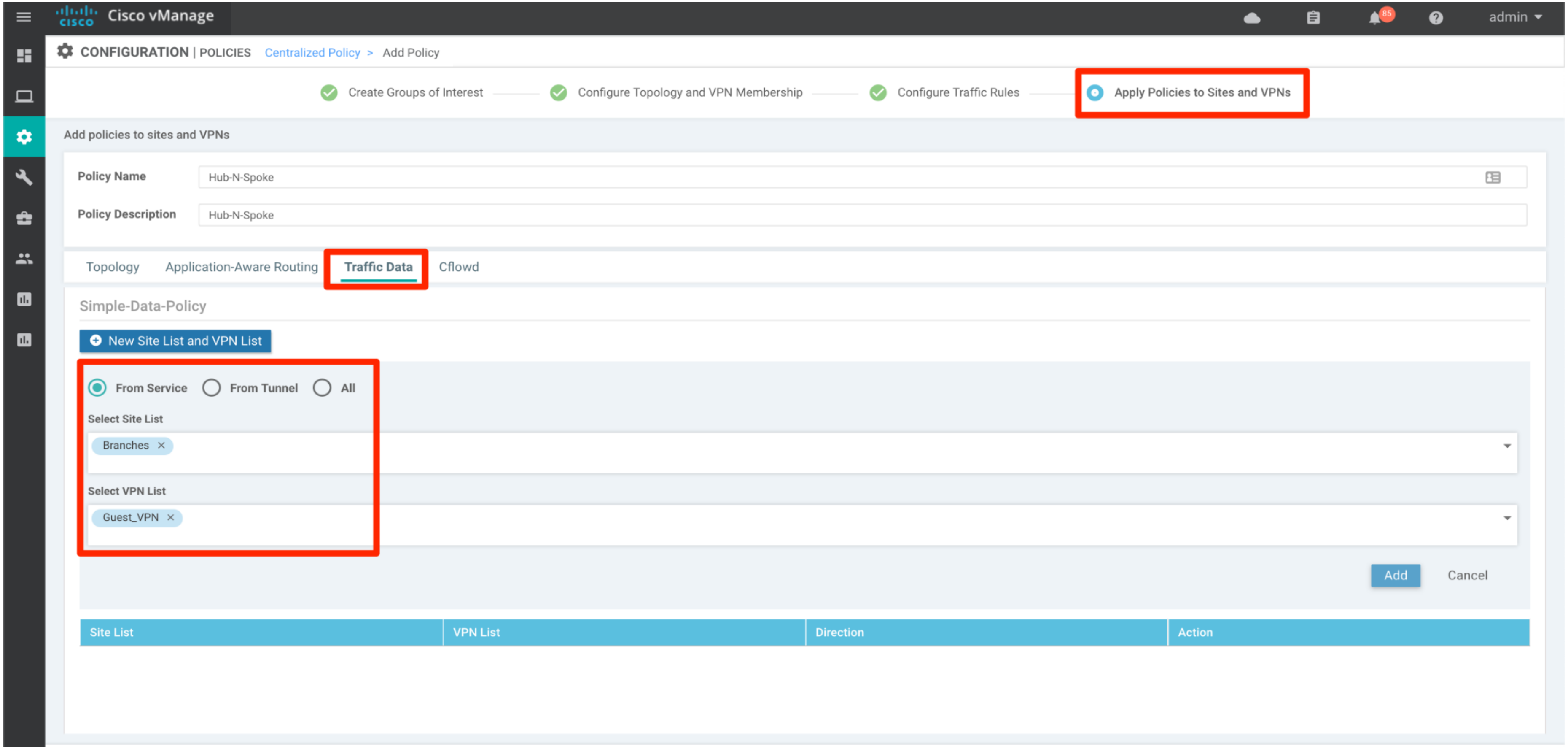
Policy Description: Hub-N-Spoke

Topology | Application-Aware Routing | Traffic Data | Cflowd

Basic_HUBnSPOKE HUB-AND-SPOKE

VPN List
Guest_VPN

Step4b: Applying Data Policy



Cisco vManage
admin
CONFIGURATION | POLICIES Centralized Policy > Add Policy
Create Groups of Interest
Configure Topology and VPN Membership
Configure Traffic Rules
Apply Policies to Sites and VPNs

Add policies to sites and VPNs

Policy Name	Hub-N-Spoke
Policy Description	Hub-N-Spoke

Topology
Application-Aware Routing
Traffic Data
Cflowd

Simple-Data-Policy

New Site List and VPN List

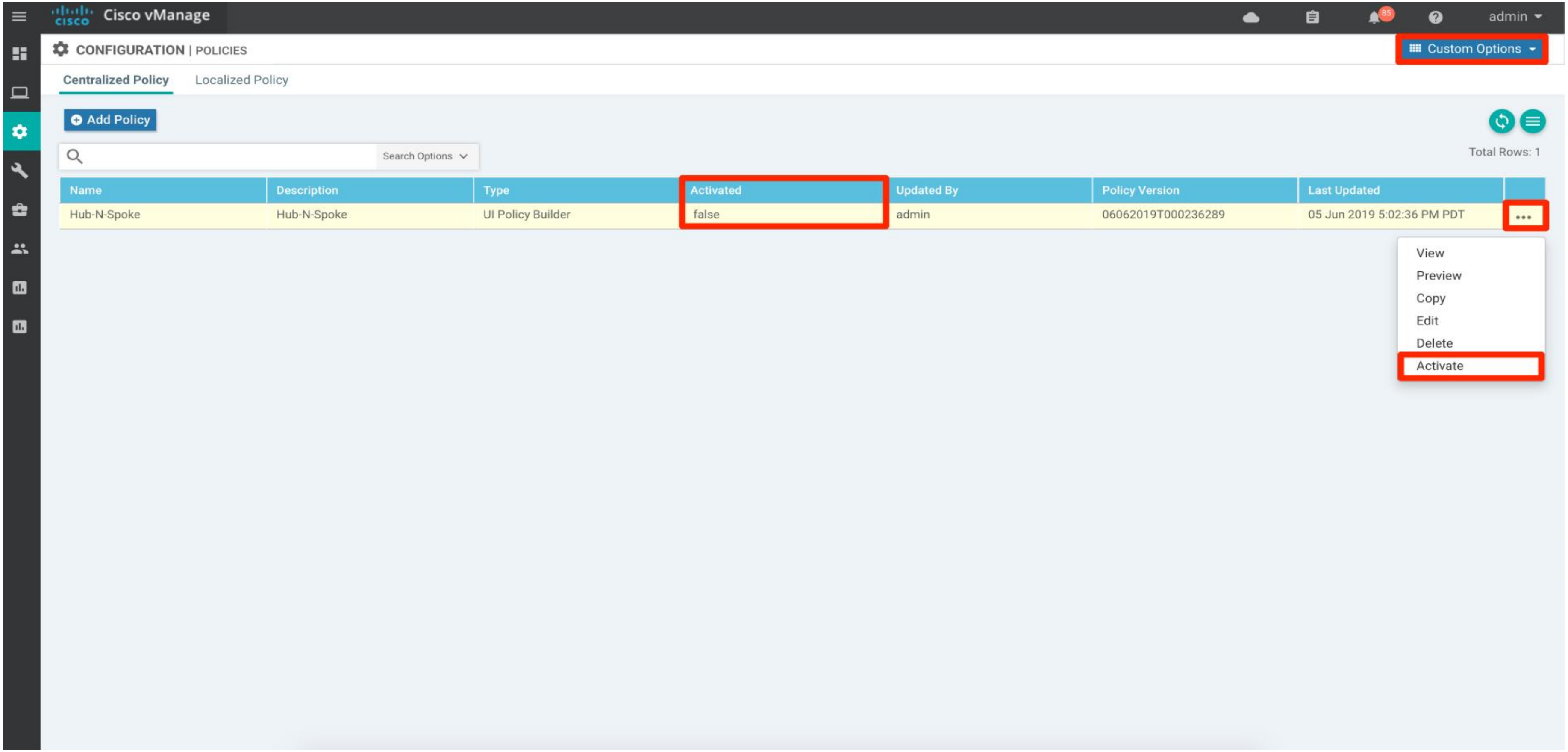
● From Service ○ From Tunnel ○ All

Select Site List: Branches ×

Select VPN List: Guest_VPN ×

Site List	VPN List	Direction	Action

Activating and Editing Policies



Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Hub-N-Spoke	Hub-N-Spoke	UI Policy Builder	false	admin	06062019T000236289	05 Jun 2019 5:02:36 PM PDT

Local Control Policy

- WAN Edge routers can establish standards base routing protocols adjacencies using OSPF and BGP
- Adjacencies are supported on both service and transport side interfaces
- Adjacencies on the LAN side are used to exchange routing information with traditional non-SDWAN routers
    - Redistribution of OMP overlay routing to OSPF/BGP, redistribution of OSPF/BGP into OMP
- Adjacencies on the WAN side are used to interact with underlay networks, when required
- Loop prevention mechanisms are used to prevent routing information feedback in case of multiple protocol redistribution points, such as redundant WAN Edge deployment

Local Data Policy

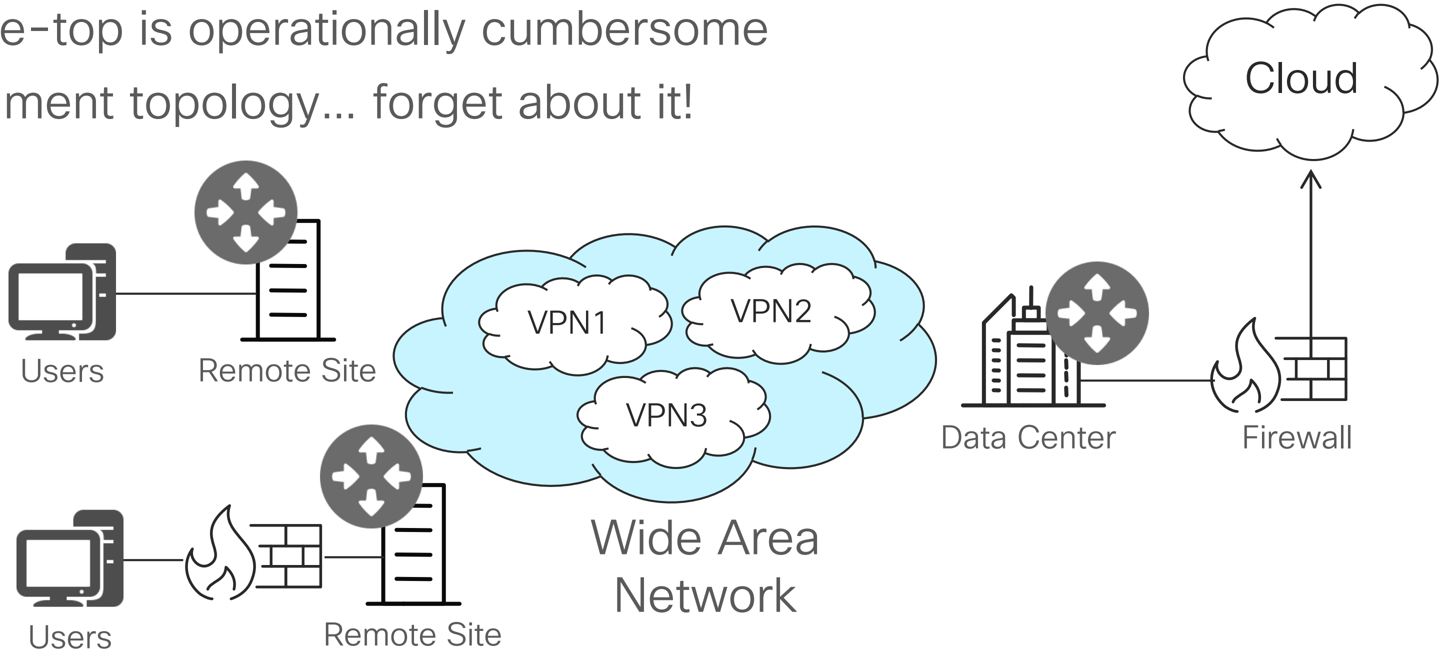
- Local WAN Edge router data policies allow device specific behavior
- Local WAN Edge router data policies cover wide range of functionalities
- Most commonly local data policies are used for:
  - Device QoS (queuing, policing, shaping, marking, remarking)
  - Local ACLs
  - Traffic mirroring
  - Deep Packet Inspection
  - Flow records
- Local data policies are centrally provisioned through vManage

DEMO

Security

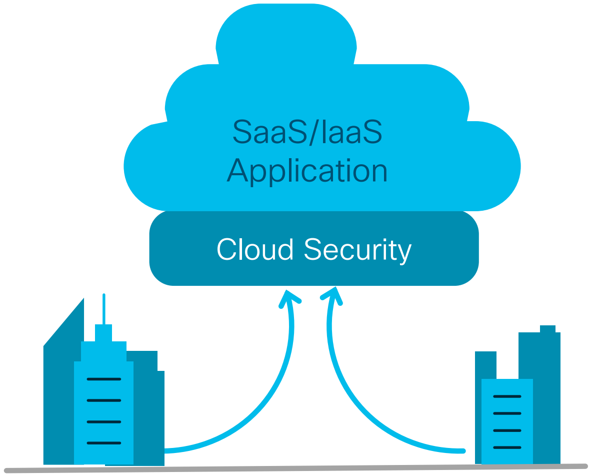
Traditional Branch Security

- Security enforcement at the branch is too costly, security enforcement at the data center is too inefficient (for cloud)
- Segmentation over MPLS is underlay specific, segmentation over-the-top is operationally cumbersome
- Per segment topology… forget about it!



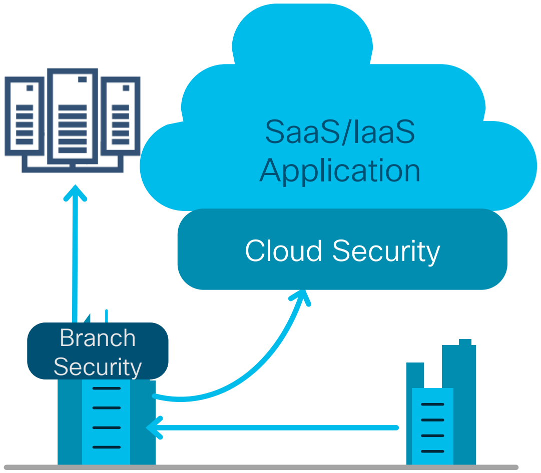
Cisco SD-WAN Security Overview

Flexible Security based on customer needs



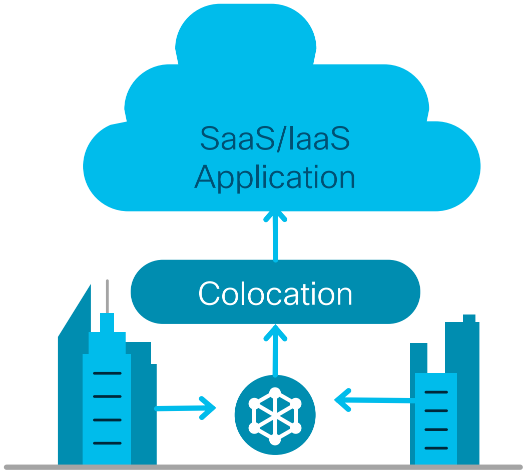
Cloud Security

Lean branch with security in the cloud



Integrated Security

Single platform for Routing and Branch Security at the branch

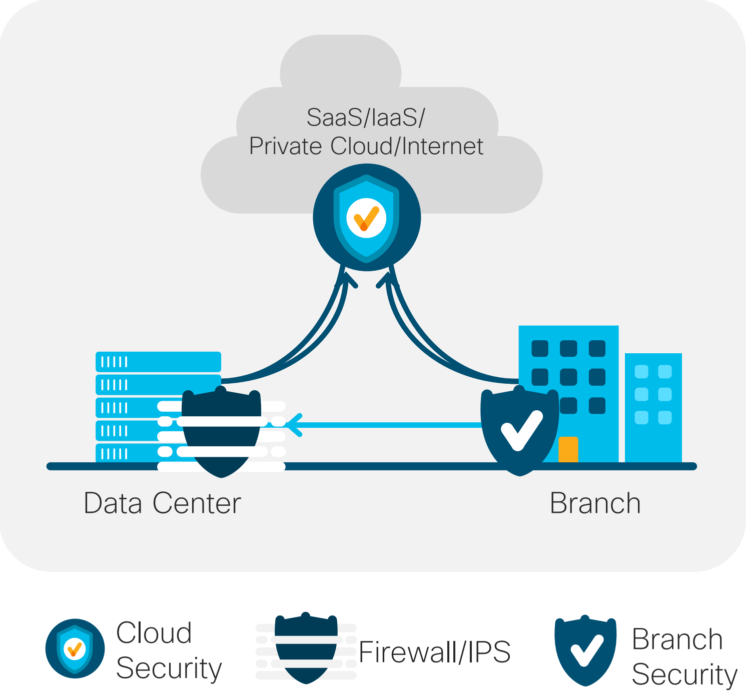


@Regional Hub

Security Services as VNF at Regional Colocation Hub

cisco Live!

Why Cisco SD-WAN Integrated Security?



1. Avoid Backhauling

Benefit: Better use of WAN bandwidth

2. Benefit Regional SaaS PoP

Benefit: Improves application performance

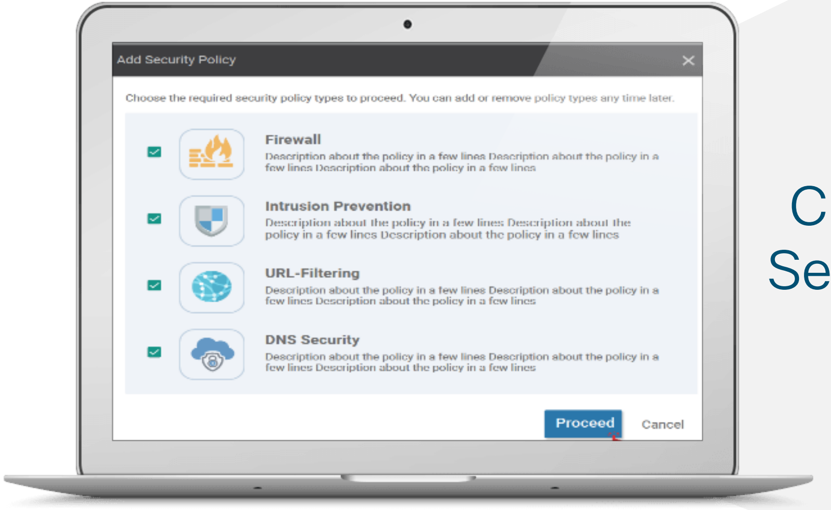
3. Enable DIA

Benefit: Improves user experience

4. Centralized Policy/Monitoring

Benefit: Consistent Security Policy & monitoring

Combining Best of Breed in Security and SD-WAN



Add Security Policy ×

Choose the required security policy types to proceed. You can add or remove policy types any time later.

☑ **Firewall**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **Intrusion Prevention**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **URL-Filtering**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **DNS Security**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

Cisco SD-WAN

Cisco Security

Enterprise Firewall
+1400 layer 7 apps classified

Intrusion Protection System
Most widely deployed IPS engine in the world

URL-Filtering
Web reputation score using 82+ web categories

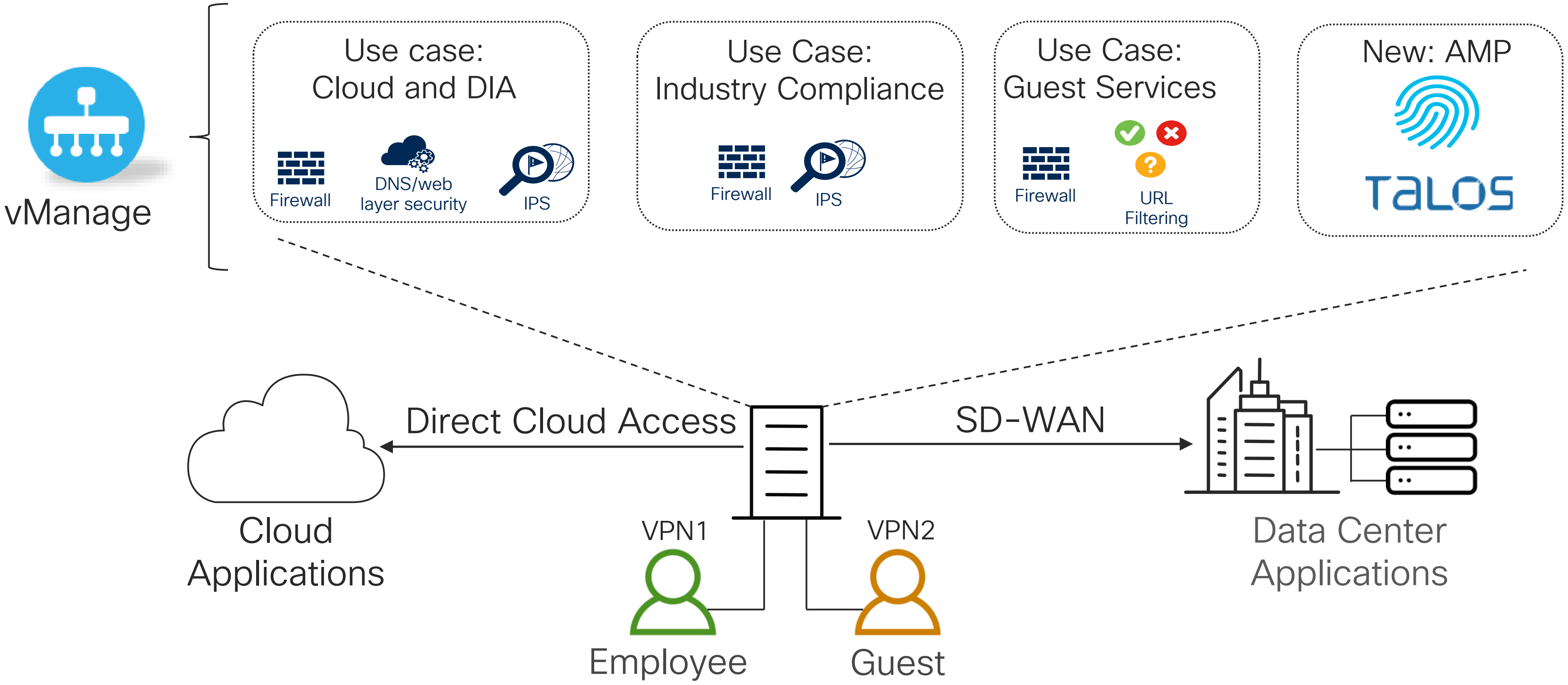
Adv. Malware Protection
With File Reputation and Sandboxing (TG)

COMING SOON!
Secure Internet Gateway
DNS Security/Cloud FW with Cisco Umbrella

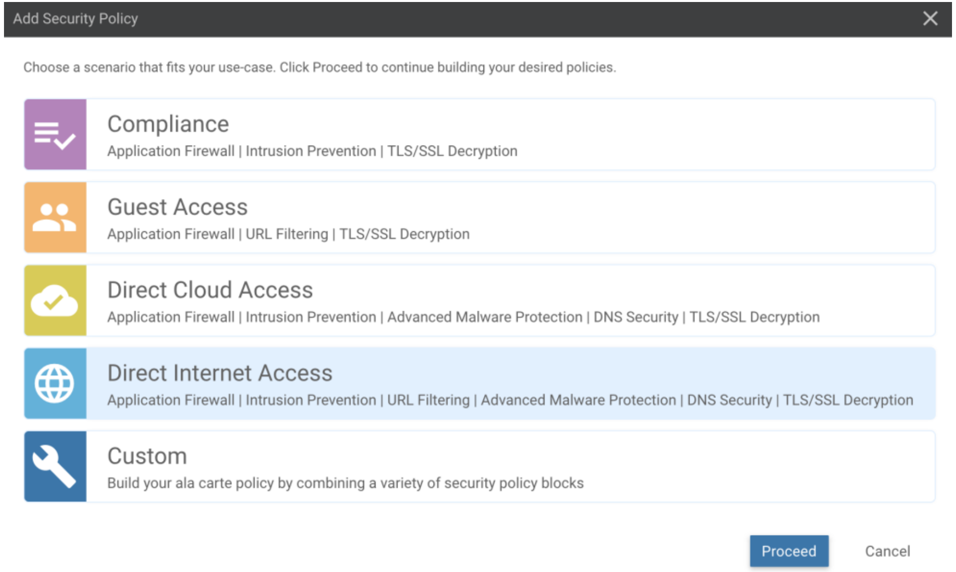
COMING SOON!
TLS/SSL Proxy
Detect Threats in Encrypted Traffic

Hours instead of weeks and months

SD-WAN Integrated Security Overview



SD-WAN Security: vManage Provisioning Wizard



Add Security Policy

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention | TLS/SSL Decryption

Guest Access
Application Firewall | URL Filtering | TLS/SSL Decryption

Direct Cloud Access
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption

Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption

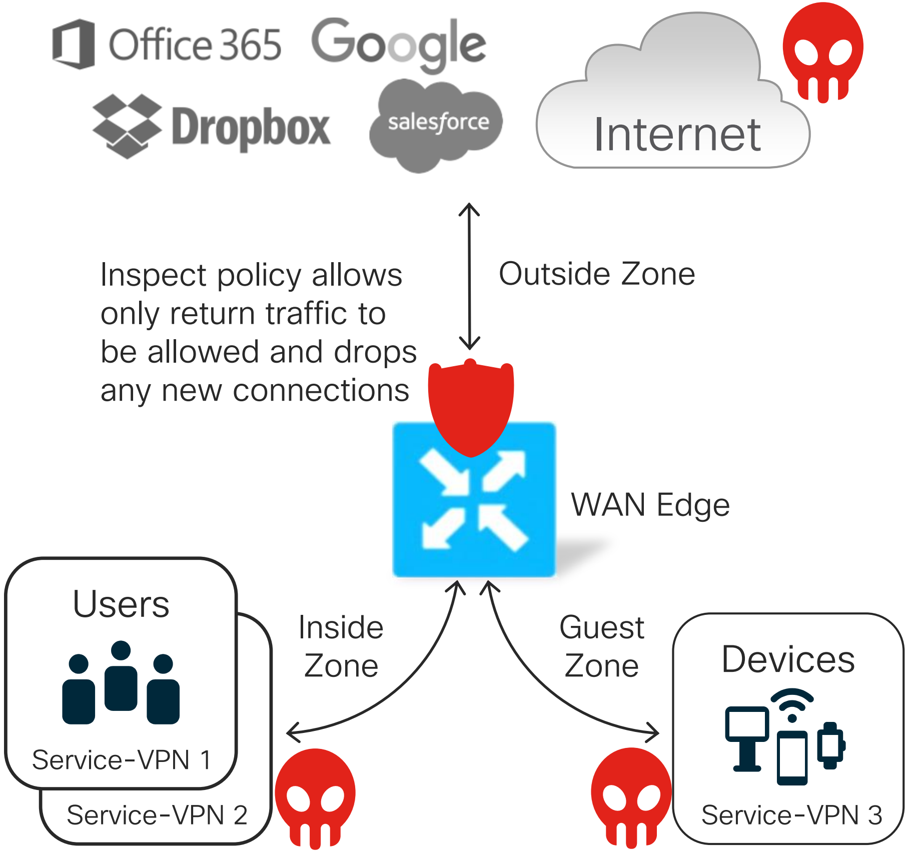
Custom
Build your ala carte policy by combining a variety of security policy blocks

Configuration > Security

⊕ Add Security Policy

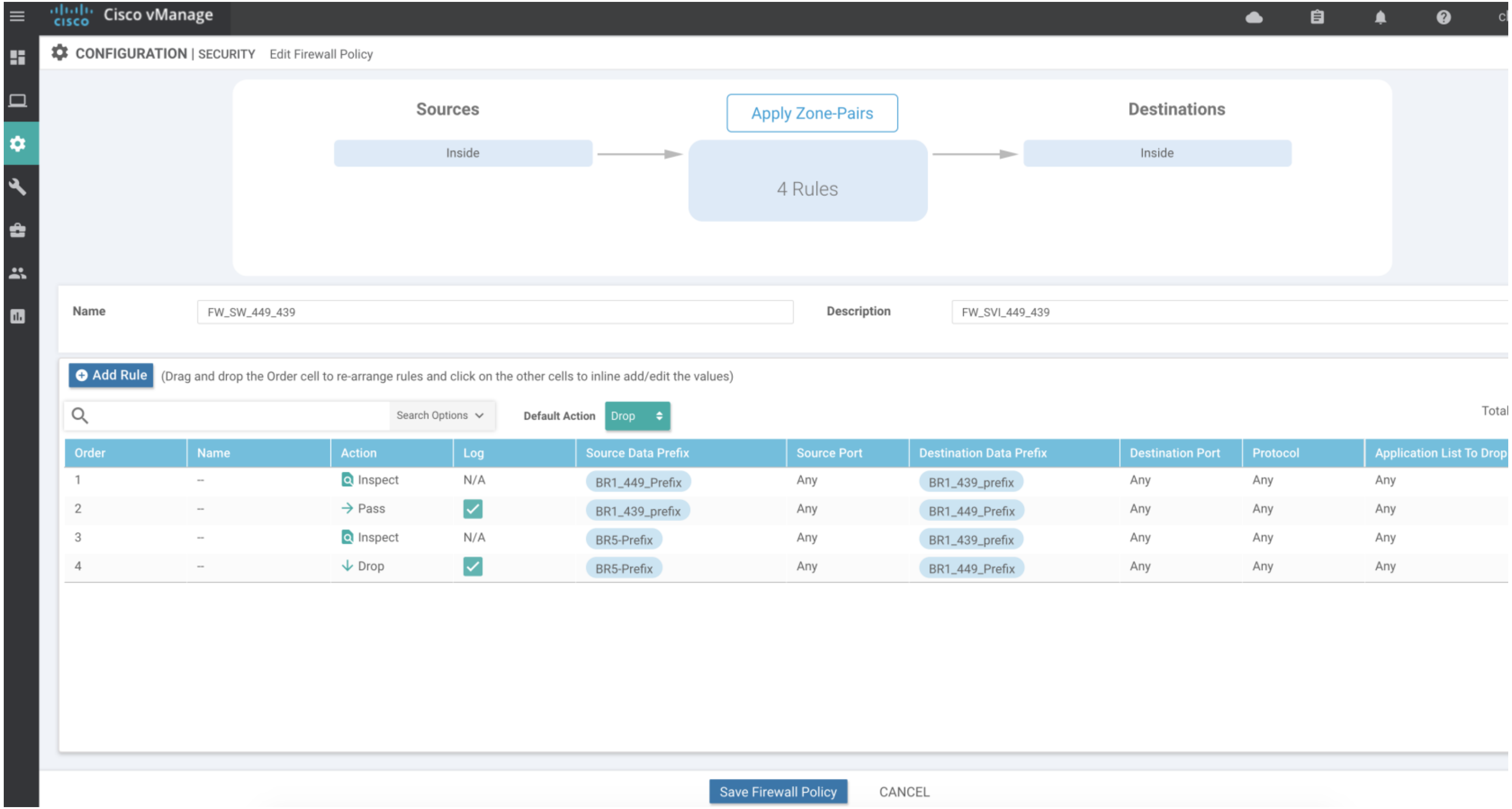
Application Aware Firewall

- VPN(s) are mapped to a zone
- Intra-zone, inter-zone and zone to DIA traffic policies
- Block, pass or inspect traffic
- Block 1400+ Layer 7 Applications
- HSL Logging (16.12 onwards)
- Self Zone Policy (16.12 onwards)
- FQDN support for configuring Src/Dstn (17.2 Onwards)



Inspect policy allows only return traffic to be allowed and drops any new connections

Application Aware Firewall Provisioning



CONFIGURATION | SECURITY   Edit Firewall Policy

Name: FW_SW_449_439

Description: FW_SVI_449_439

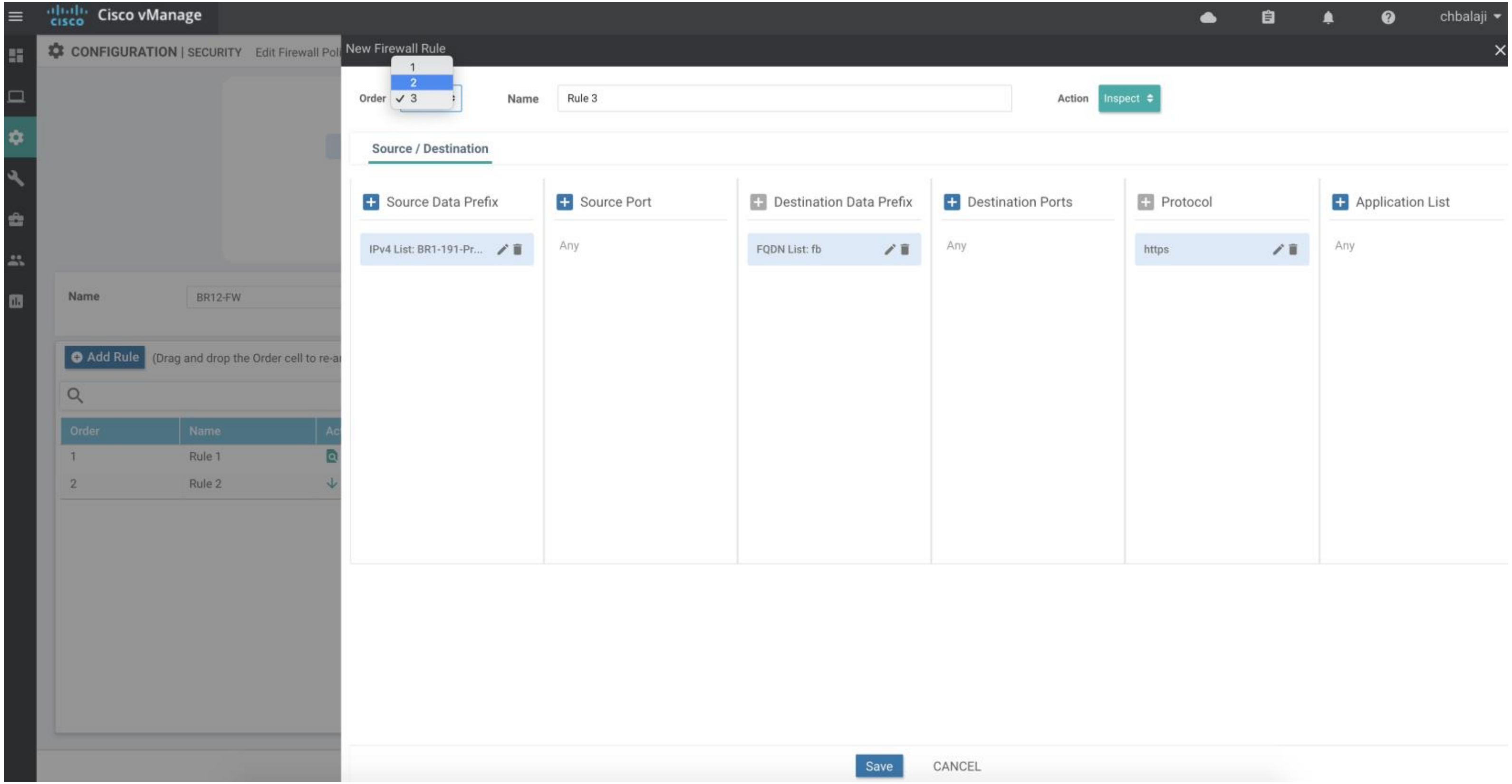
(Drag and drop the Order cell to re-arrange rules and click on the other cells to inline add/edit the values)

Default Action: Drop

Total

Order	Name	Action	Log	Source Data Prefix	Source Port	Destination Data Prefix	Destination Port	Protocol	Application List To Drop
1	--	Inspect	N/A	BR1_449_Prefix	Any	BR1_439_prefix	Any	Any	Any
2	--	→ Pass	☑	BR1_439_prefix	Any	BR1_449_Prefix	Any	Any	Any
3	--	Inspect	N/A	BR5-Prefix	Any	BR1_439_prefix	Any	Any	Any
4	--	↓ Drop	☑	BR5-Prefix	Any	BR1_449_Prefix	Any	Any	Any

Application Aware Firewall Provisioning



Name: BR12-FW

Order	Name
1	Rule 1
2	Rule 2

New Firewall Rule

Order: 1 / 2 / ✓ 3

Name: Rule 3

Action: Inspect

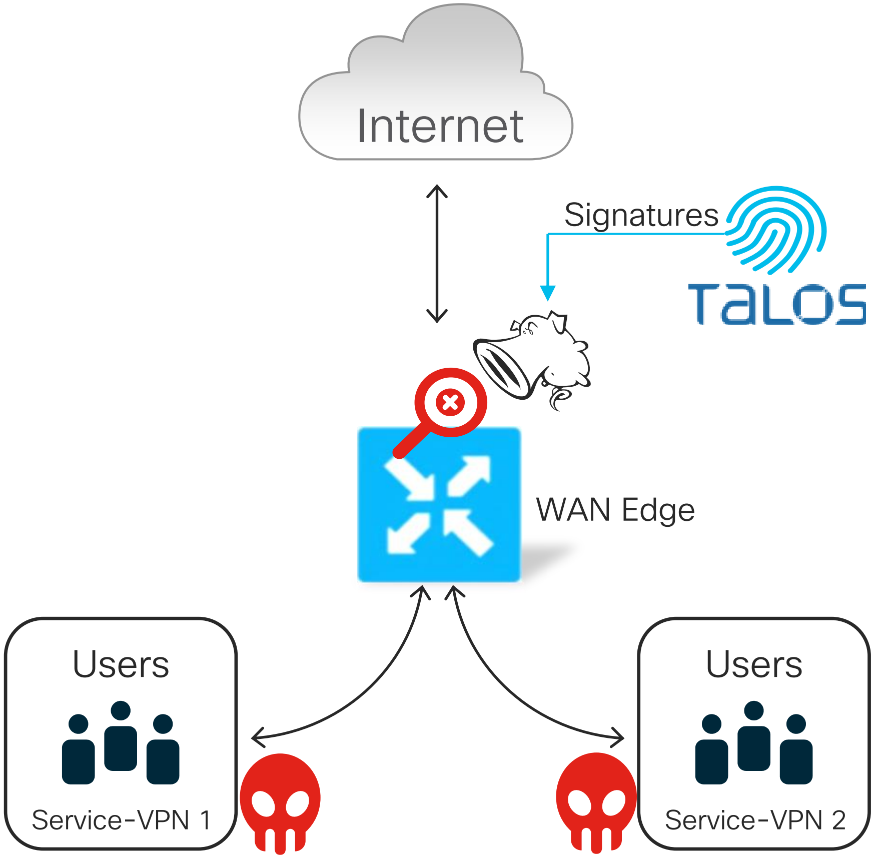
Source / Destination

Source Data Prefix	Source Port	Destination Data Prefix	Destination Ports	Protocol	Application List
IPv4 List: BR1-191-Pr...	Any	FQDN List: fb	Any	https	Any

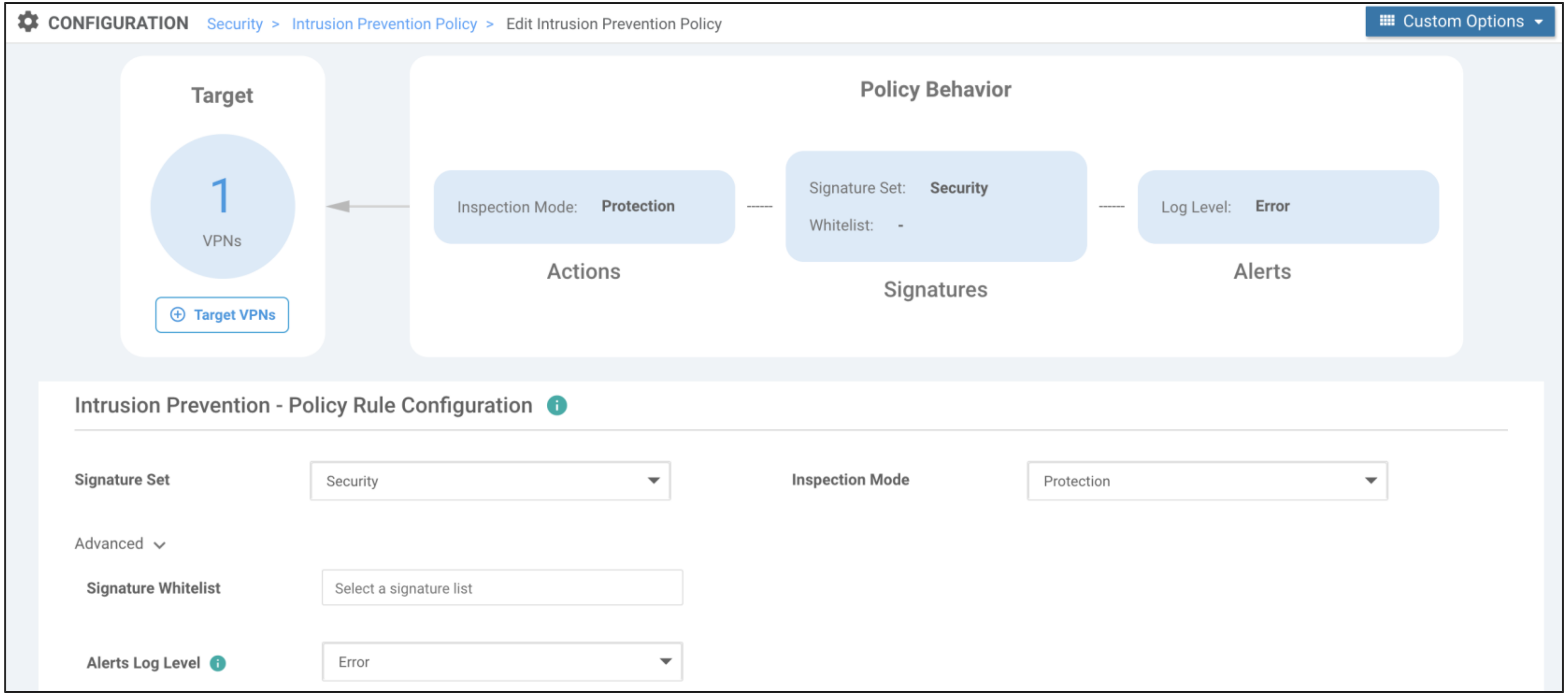
Save CANCEL

Intrusion Prevention and Detection

- Snort IPS engine
- Runs in a service container on Cisco SD-WAN Edge routers (ISR1K*/ISR4K/CSR1K)
- Backed by global Threat Intelligence (TALOS) signatures updated automatically
- Inspects traffic in VPNs of interest
- Supports three levels of signature sets
- Signature whitelist support
- Can run in detection mode



Intrusion Prevention and Detection Provisioning



CONFIGURATION Security > Intrusion Prevention Policy > Edit Intrusion Prevention Policy

Inspection Mode: Protection

Signature Set: Security

Whitelist: -

Log Level: Error

Intrusion Prevention - Policy Rule Configuration

Signature Set: Security

Inspection Mode: Protection

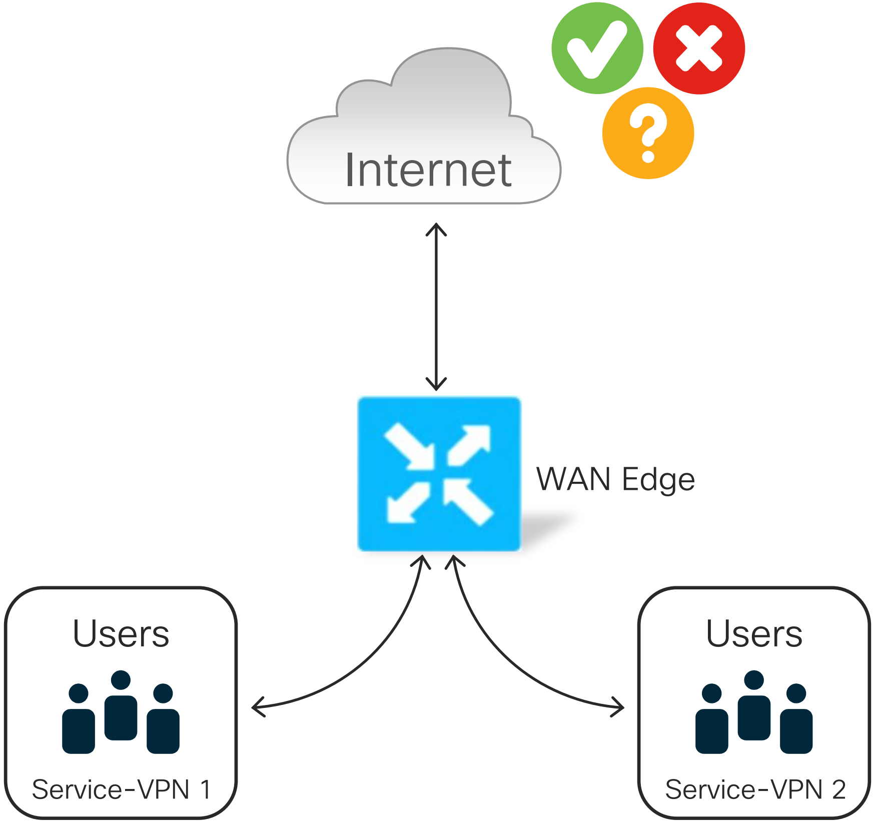
Advanced

Signature Whitelist: Select a signature list

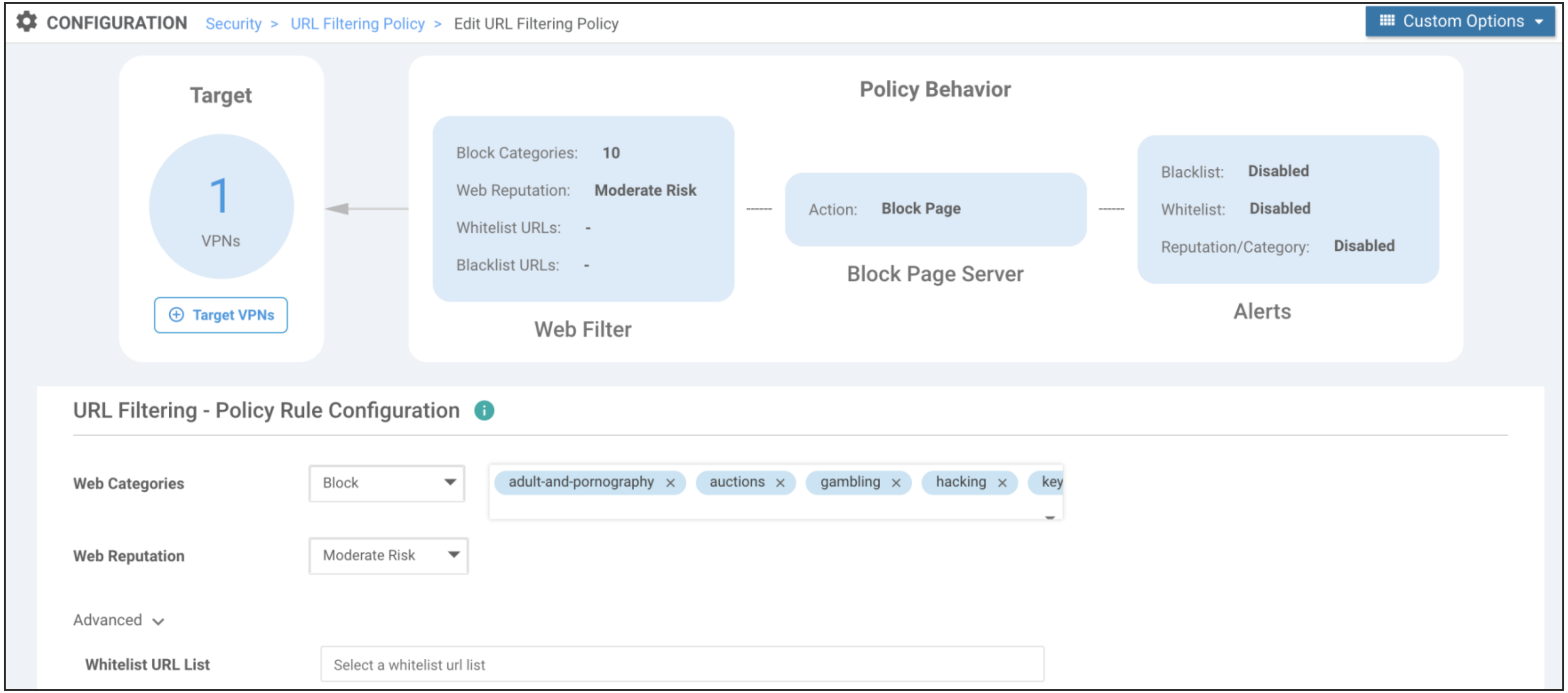
Alerts Log Level: Error

URL Filtering

- Runs in a service container on Cisco SD-WAN Edge Routers (ISR1K*/ISR4K/CSR1K)
- Cloud lookup with local caching or local lookup
  - Local lookup downloads URL database to the router
- 82+ Web Categories with dynamic updates
- Inspects traffic in VPNs of interest
- Block based on Web Reputation score
- Create custom Black and White Lists
- Customizable end-user notifications



URL Filtering Provisioning



CONFIGURATION Security > URL Filtering Policy > Edit URL Filtering Policy

Target

1 VPNs

Policy Behavior

Web Filter

Block Categories: 10

Web Reputation: Moderate Risk

Whitelist URLs: -

Blacklist URLs: -

Block Page Server

Action: Block Page

Alerts

Blacklist: Disabled

Whitelist: Disabled

Reputation/Category: Disabled

URL Filtering - Policy Rule Configuration

Web Categories: Block — adult-and-pornography ×, auctions ×, gambling ×, hacking ×, key

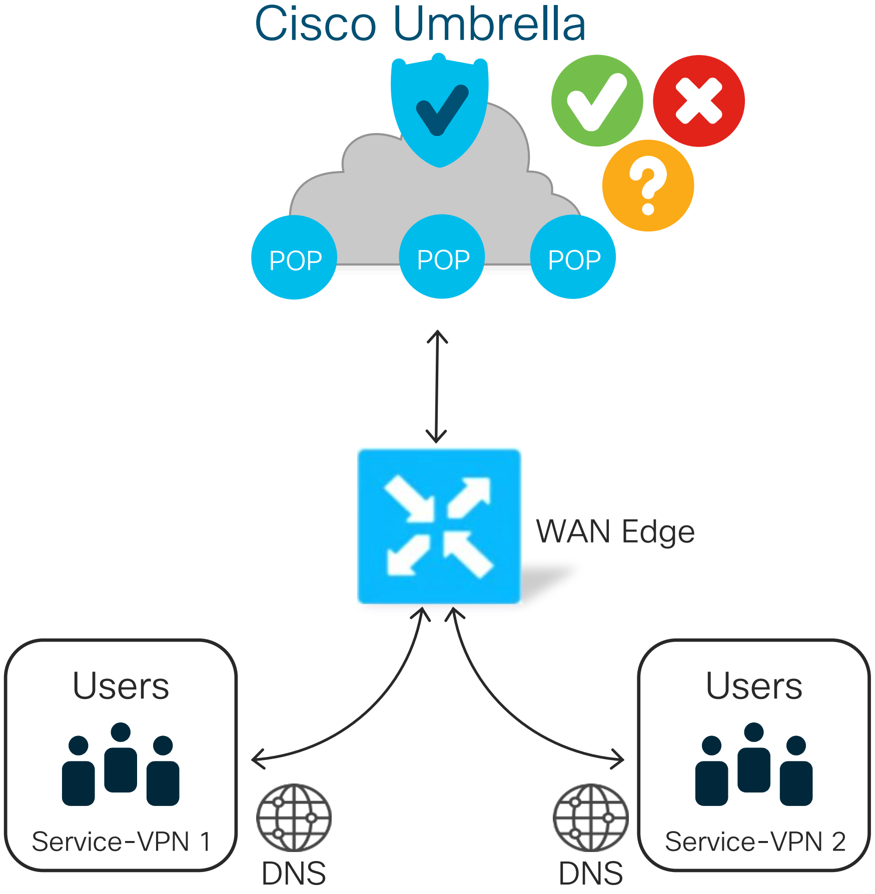
Web Reputation: Moderate Risk

Advanced

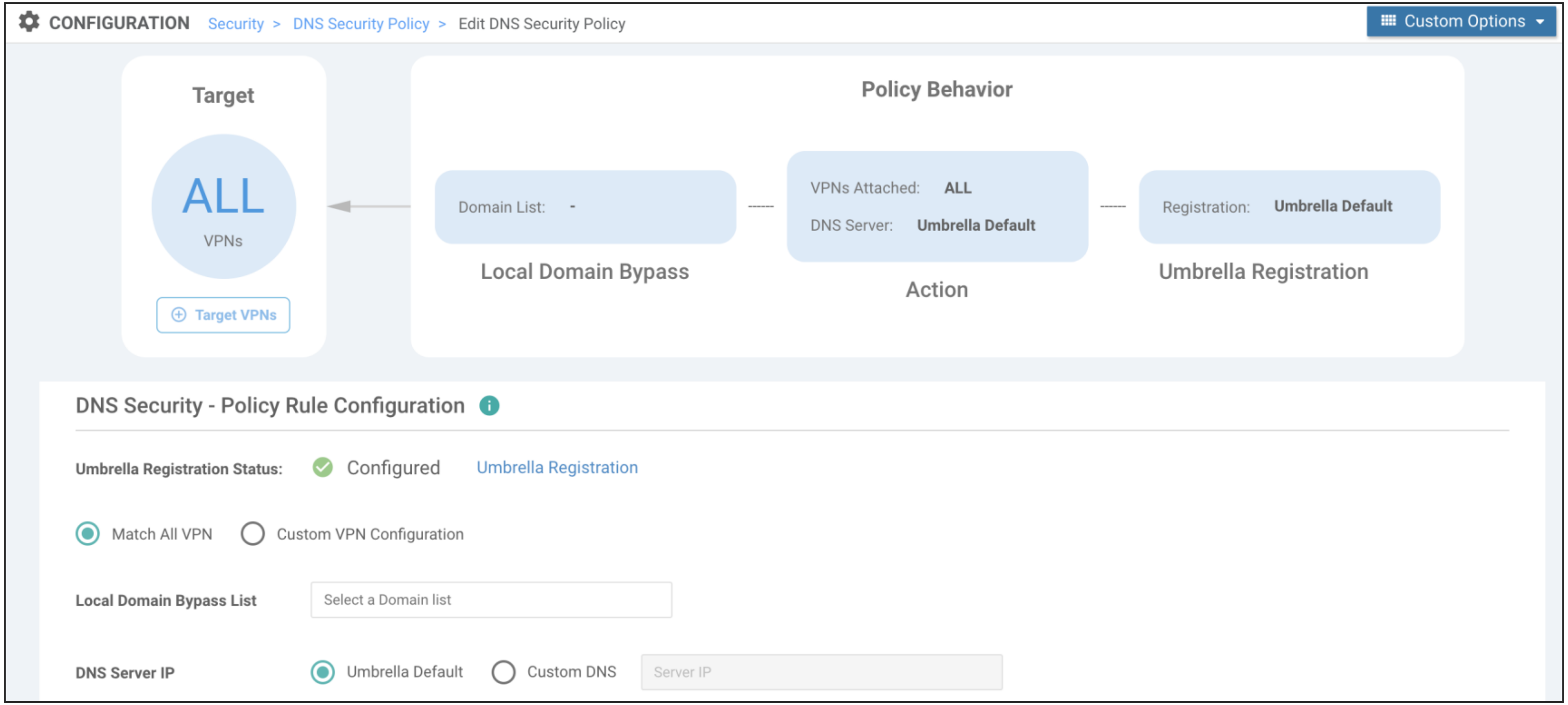
Whitelist URL List: Select a whitelist url list

DNS/Web-layer Security

- Cloud-only DNS based inspection API Key registration
- VPN-aware policies
- Global points of presence and anycast IP for fastest response and high availability
- DNScrypt
- Local domain-bypass
- Intelligent Proxy
- Auto Org Onboarding (March 2020)



DNS/Web-Layer Security Provisioning



Domain List: -

Local Domain Bypass

VPNs Attached: ALL

DNS Server: Umbrella Default

Action

Registration: Umbrella Default

Umbrella Registration

DNS Security - Policy Rule Configuration

Umbrella Registration Status: ✓ Configured Umbrella Registration

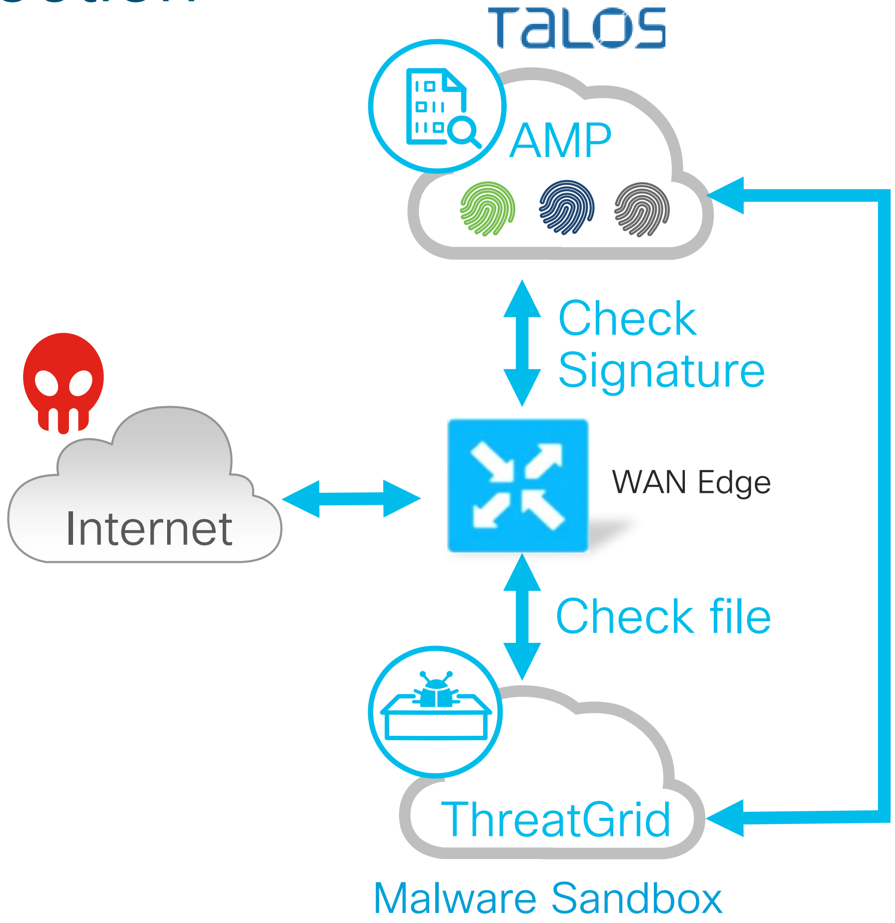
● Match All VPN ○ Custom VPN Configuration

Local Domain Bypass List: Select a Domain list

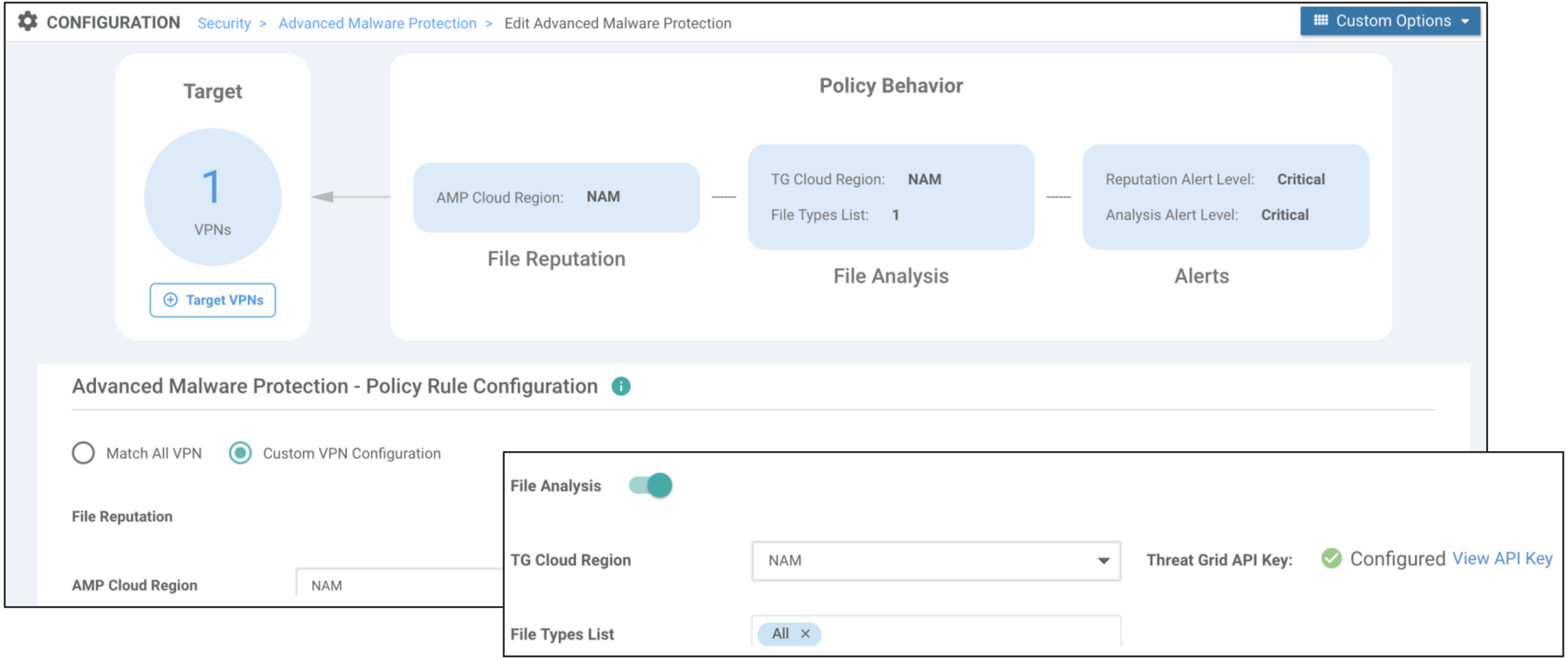
DNS Server IP: ● Umbrella Default ○ Custom DNS Server IP

Advanced Malware Protection

- Runs in a service container on Cisco SD-WAN Edge routers (ISR1K*/ISR4K/CSR1K)
- File reputation check powered by Talos
- Sandboxing and file analysis for unknown signatures powered by ThreatGrid
- Automated signature update from ThreatGrid to Talos
- Inspects traffic in VPNs of interest
- Leverages Snort engine to identify file transfers



Advanced Malware Protection Provisioning



CONFIGURATION Security > Advanced Malware Protection > Edit Advanced Malware Protection

Custom Options

Target

1 VPNs

Target VPNs

Policy Behavior

File Reputation
AMP Cloud Region: NAM

File Analysis
TG Cloud Region: NAM
File Types List: 1

Alerts
Reputation Alert Level: Critical
Analysis Alert Level: Critical

Advanced Malware Protection - Policy Rule Configuration

○ Match All VPN ● Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

File Analysis: On

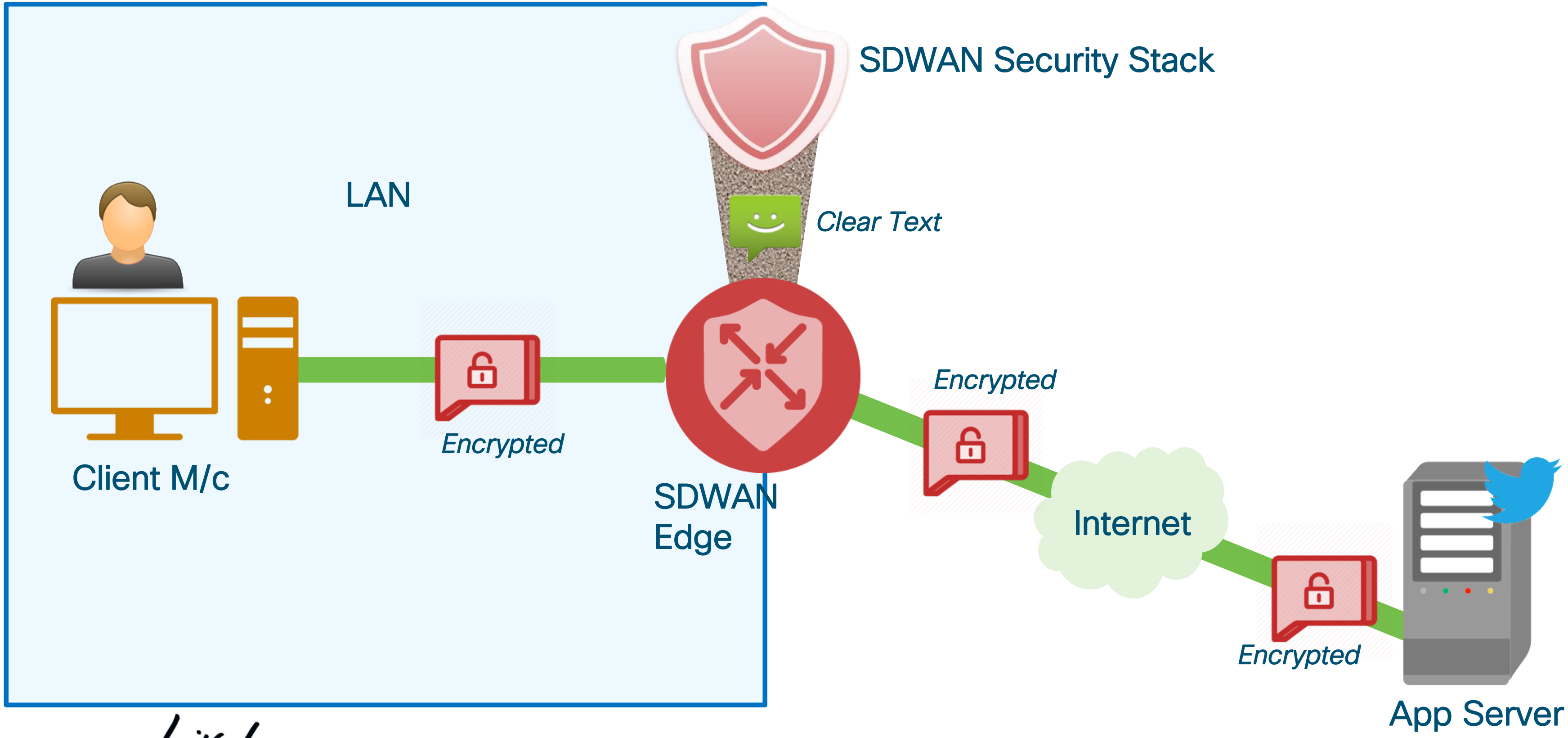
TG Cloud Region: NAM

Threat Grid API Key: ✓ Configured View API Key

File Types List: All ×

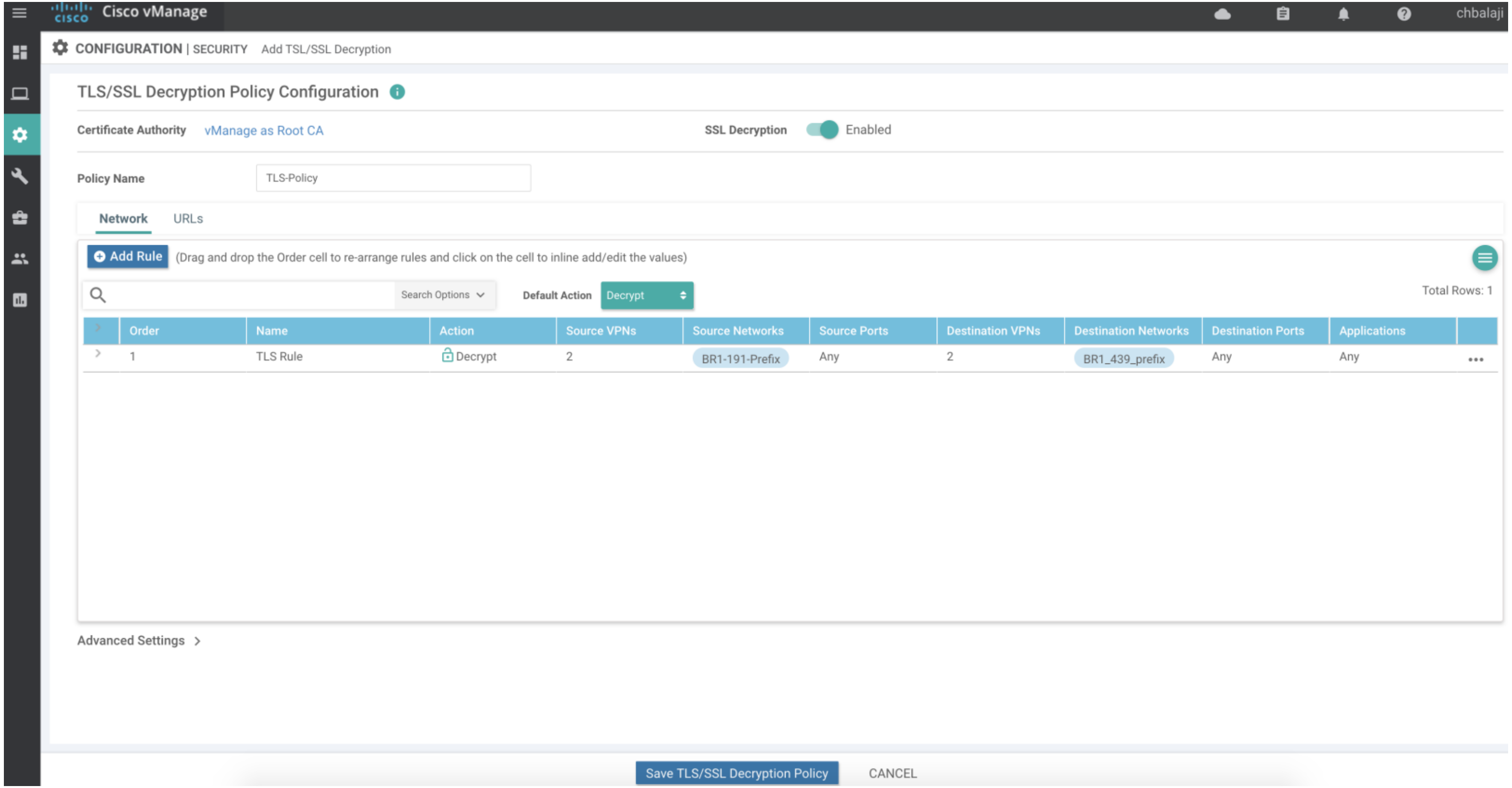
TLS/SSL Proxy

COMING SOON!



TLS/SSL Proxy Provisioning

COMING SOON!



CONFIGURATION | SECURITY Add TSL/SSL Decryption

TLS/SSL Decryption Policy Configuration

Certificate Authority: vManage as Root CA

SSL Decryption: Enabled

Policy Name: TLS-Policy

(Drag and drop the Order cell to re-arrange rules and click on the cell to inline add/edit the values)

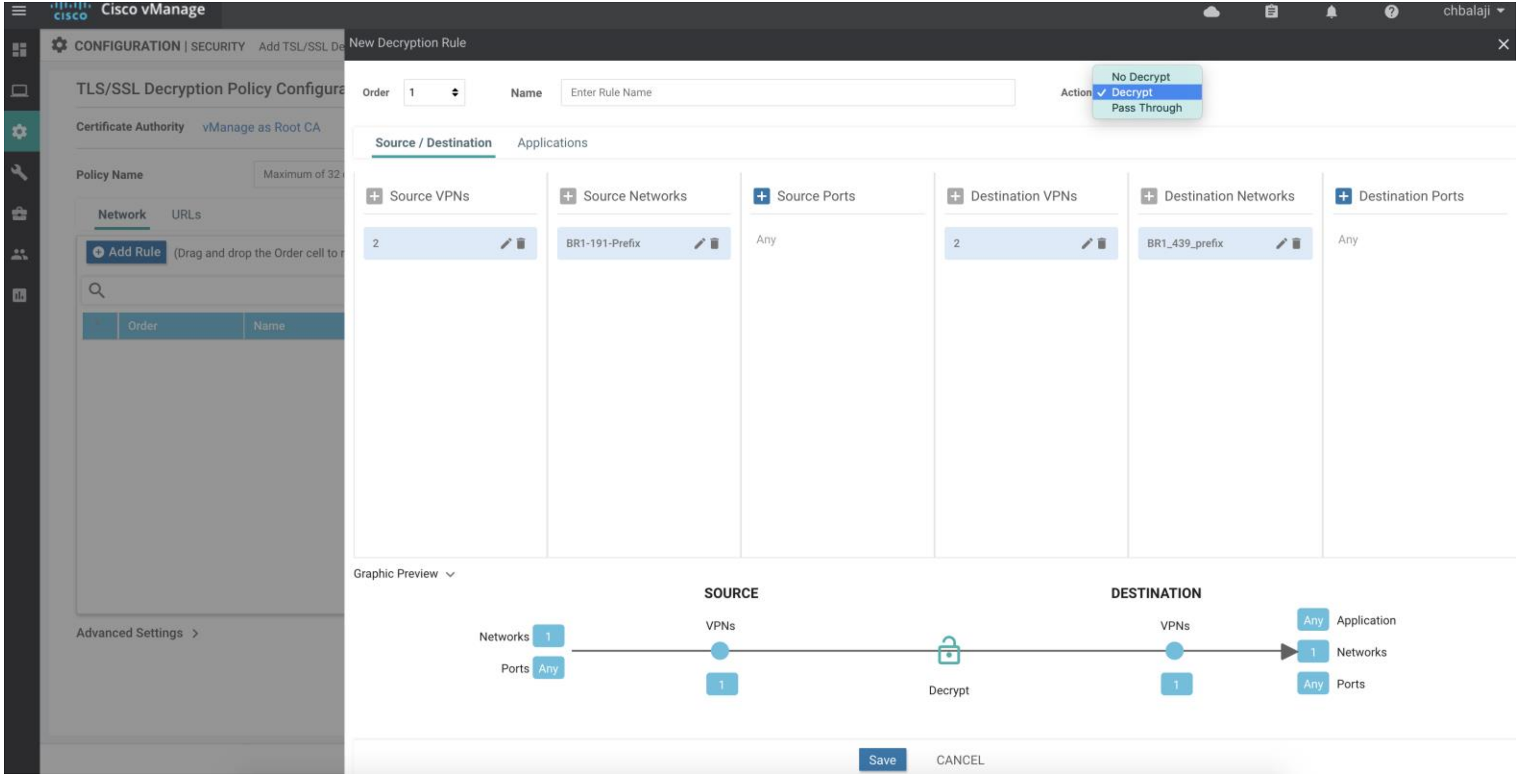
Default Action: Decrypt

Total Rows: 1

Order	Name	Action	Source VPNs	Source Networks	Source Ports	Destination VPNs	Destination Networks	Destination Ports	Applications
1	TLS Rule	Decrypt	2	BR1-191-Prefix	Any	2	BR1_439_prefix	Any	Any

TLS/SSL Proxy Provisioning

COMING SOON!



Cisco vManage

CONFIGURATION | SECURITY Add TSL/SSL De

TLS/SSL Decryption Policy Configura

Certificate Authority: vManage as Root CA

Policy Name: Maximum of 32

Network | URLs

Add Rule (Drag and drop the Order cell to r

Order	Name

Advanced Settings

New Decryption Rule

Order: 1

Name: Enter Rule Name

Action:
- No Decrypt
- ✓ Decrypt
- Pass Through

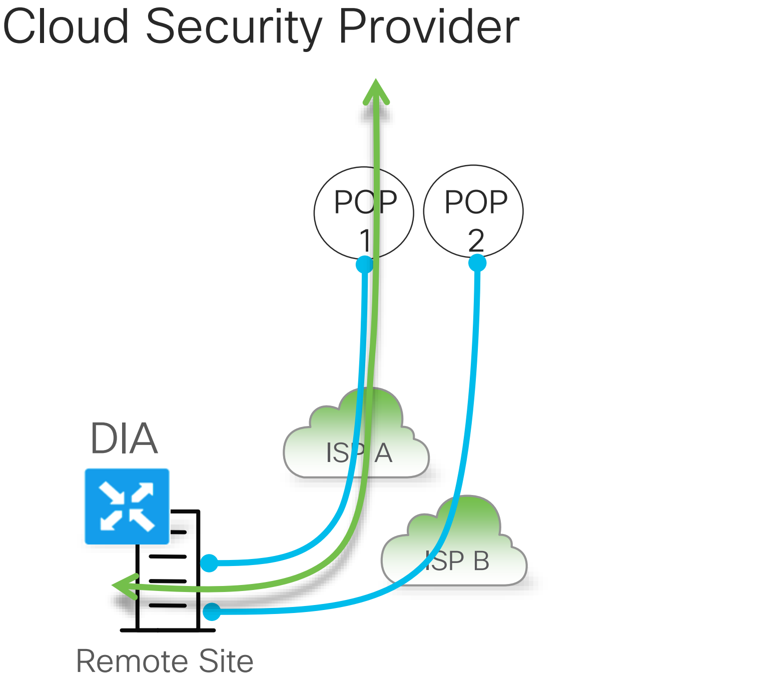
Source / Destination | Applications

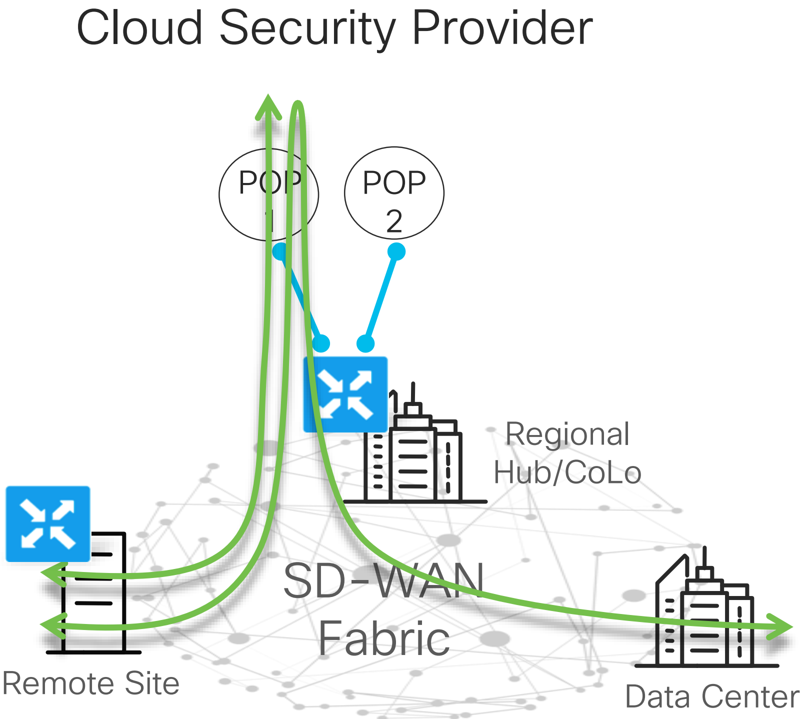
Source VPNs	Source Networks	Source Ports	Destination VPNs	Destination Networks	Destination Ports
2	BR1-191-Prefix	Any	2	BR1_439_prefix	Any

Graphic Preview

Save | CANCEL

3rd Party Cloud Security





●—● GRE/IPSec Tunnels

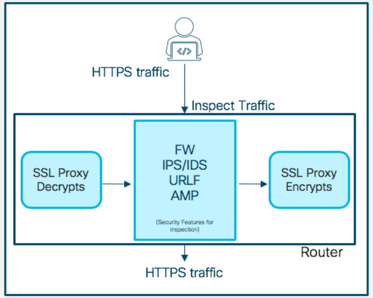
— Data Traffic

●—● IPSec Tunnels

SD-WAN Security Features - Overview

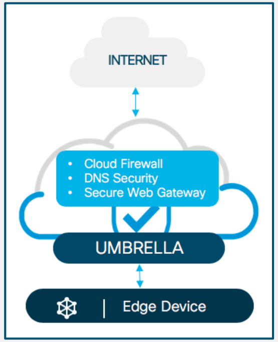
COMING SOON!

TLS/SSL Proxy Support with SD-WAN



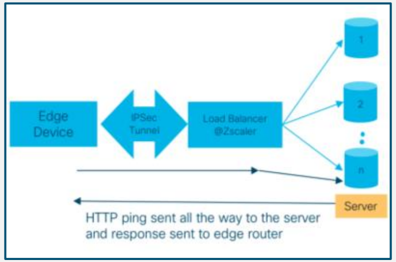
SSL Proxy helps to decrypt and inspect network traffic for malware
(XE-SDWAN only)

IPSec Auto-Tunnel to Cisco Umbrella



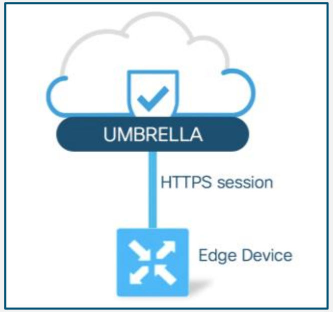
Push SIG feature template and setup IPSec tunnel to Umbrella SIG
(XE-SDWAN and vEdges)

Layer 7 Health Check to ZScaler SIG


Edge Device
IPSec Tunnel
Load Balancer @Zscaler
1
2
n
Server
HTTP ping sent all the way to the server and response sent to edge router

Deterministic way to ensure the network traffic to Zscaler SIG is not blackholed
(vEdges only)

Auto-Registration to Cisco Umbrella

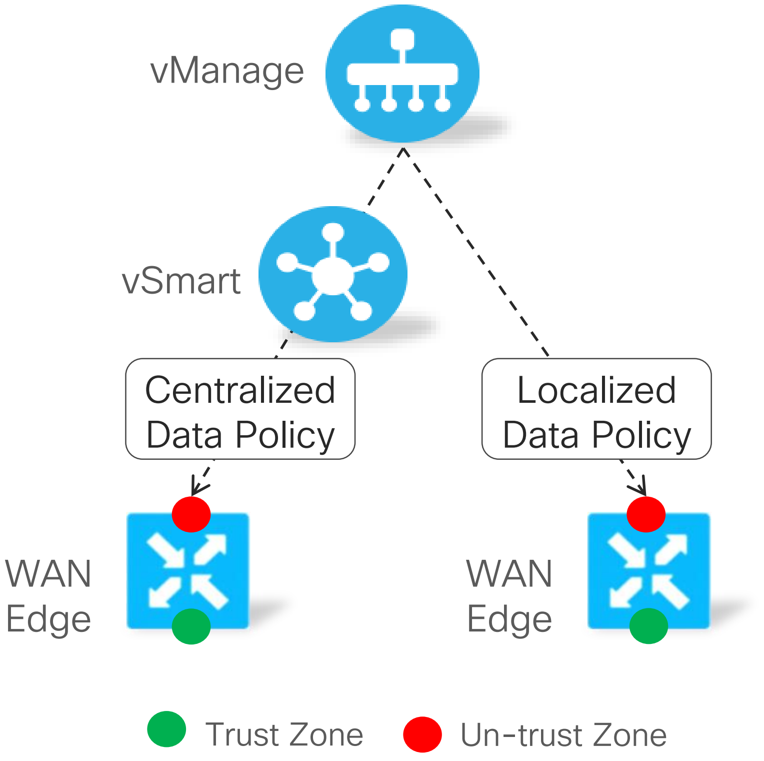


Smart Account enables Auto Registration & Provisioning between SD-WAN and Umbrella
(XE-SDWAN and vEdges)

SD-WAN Security: Platform Support

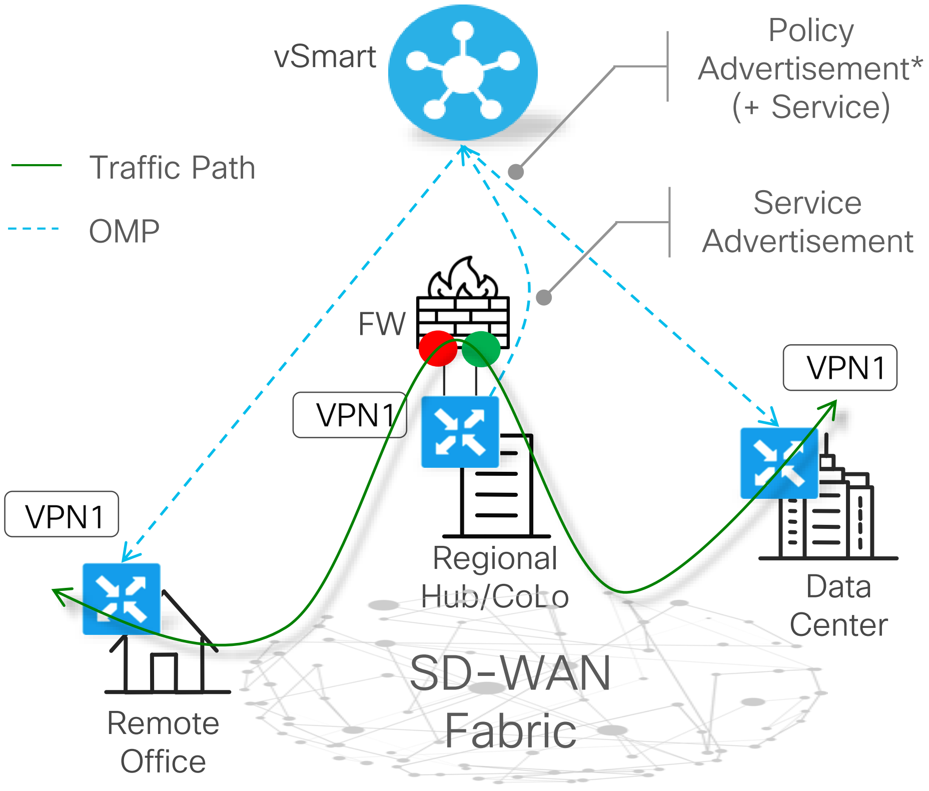
Platforms/Features	Firewall	App Aware Firewall	AMP/TG	IPS	URL Filtering	DNS/web-layer Security
vEdge (100, 1000, 2000 and 5000)	Y	N	N/A	N/A	N/A	N
Cisco CSR1Kv	Y	Y	Y	Y	Y	Y
Cisco ENCS (ISRv)	Y	Y	Y	Y	Y	Y
Cisco ISR4K	Y	Y	Y	Y	Y	Y
Cisco ISR1K (1111X-8P)	Y	Y	Y	Y	Y	Y
Cisco ASR1K (1001-HX, 1002-HX, 1001-X, 1002-X)	Y	Y	N/A	N/A	N/A	Y

Basic Application Filtering



- Centralized data policy is defined on vManage and distributed by vSmart controllers
- Centralized data policy match on application traffic of interest
  - DPI or 6 tuple matching
- Centralized data policy takes drop action to block unwanted traffic
  - Can log
- Localized data policy works similarly to centralized data policy, but it is distributed directly from vManage

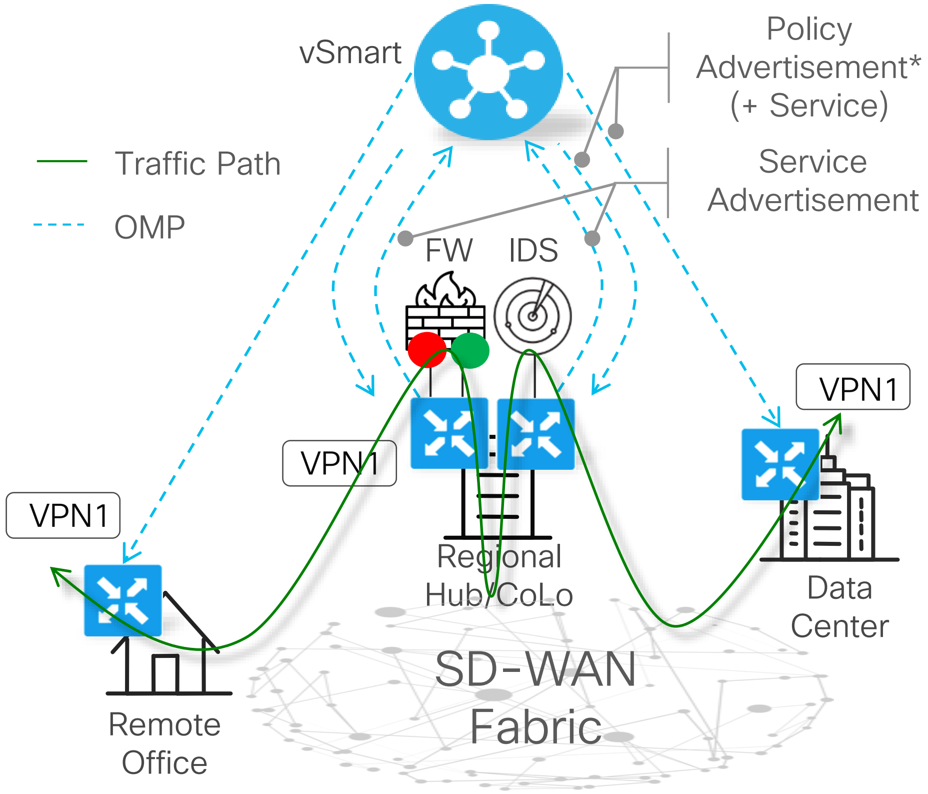
Dedicated Regional Security



* For data policy only. Control policy enforced on vSmart.

- Service node is connected to vEdge
  - Directly or IPSec IKE v1/v2
  - Routed or bridged
- vEdge router advertises service
  - Service route + Service label
  - Specific VPN
- Observe Firewall trust and untrust zones
- Control or data policies are used to insert the service node

Dedicated Regional Security: Multiple Services



* For data policy only, control policy is enforced on vSmart.

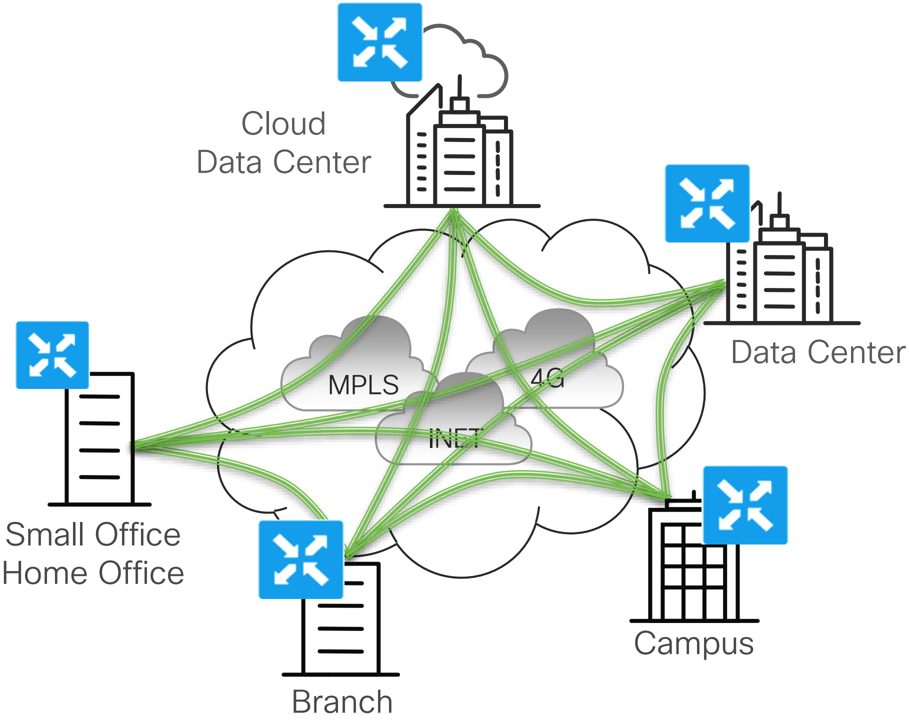
- Service nodes are connected to vEdge
  - Directly or IPSec IKE v1/v2
  - Routed or bridged
- Service nodes can be connected to different vEdge routers
  - Can be in different sites
- vEdge routers advertise service
  - Service route + Service label
  - Specific VPN
- Control or data policies are used to insert the service nodes

Application Quality of Experience

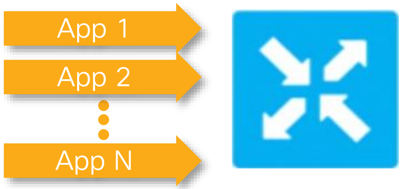
Multidimensional Application Quality of Experience

- Application Visibility and Recognition
- Device QoS
- DSCP/COS Re-Marking
- Application Aware Routing
- Path Remediation
- TCP Optimization
- Fragmentation Avoidance

Application Visibility and Recognition

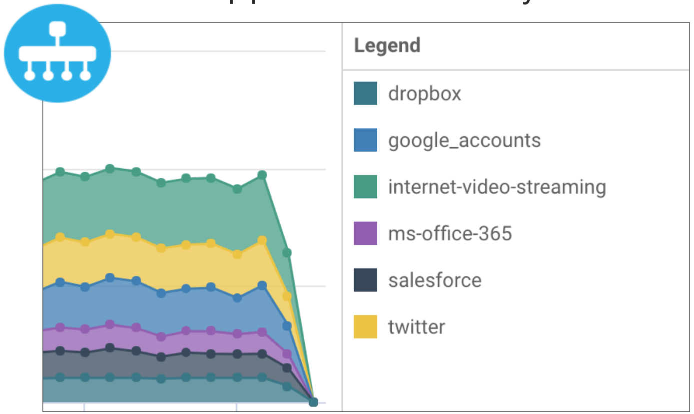


NBAR2: XE-SDWAN, DPI: vEdge

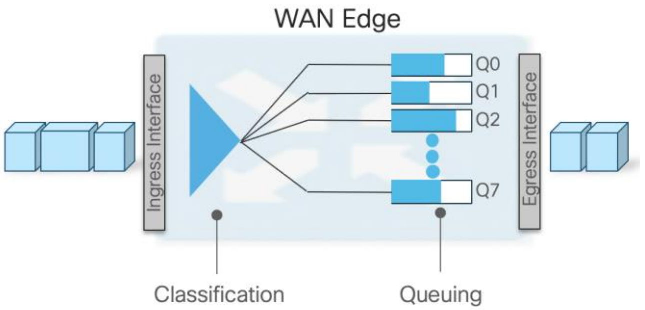


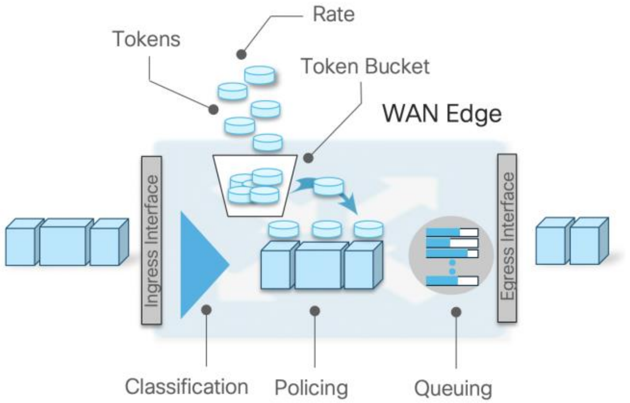
Application Recognition

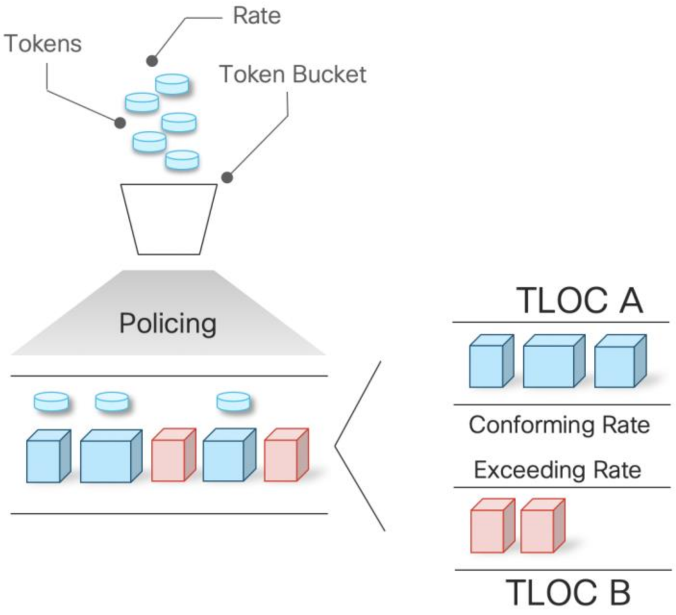
Application Visibility



Device QoS: (Queuing/Shaping/Policing/PLP)

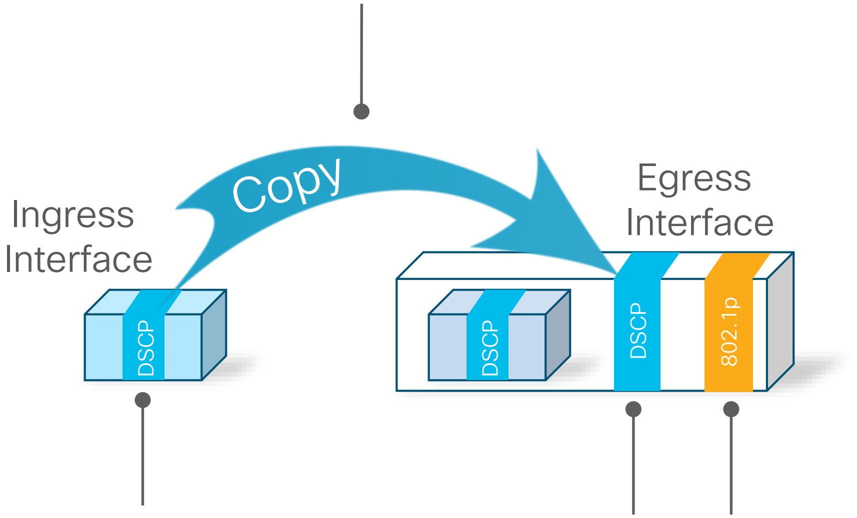






DSCP and COS (802.1p) Re-marking

Copy original DSCP markings into outer DSCP markings

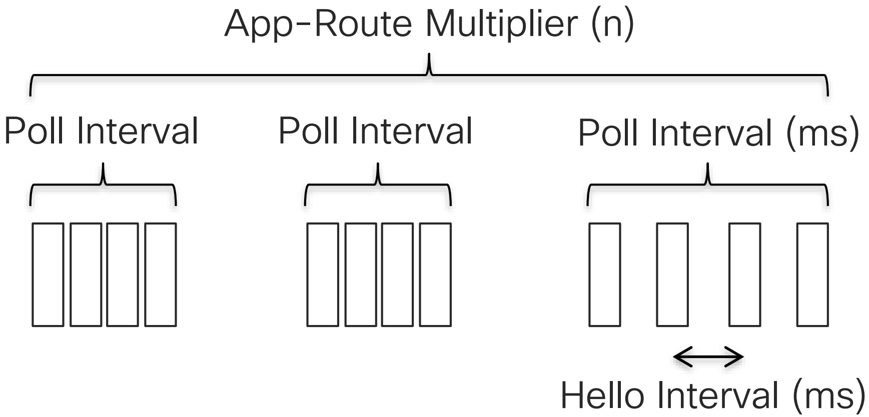


Classify: 6 tuple or DPI
Action: set DSCP, map into forwarding class (FC)

Modify with re-write rules (per-FC)

- Comply with service provider provisioned classes of service
- (Optional) Original DSCP rewrite
  - Classification: 6 tuple or DPI
  - Action: Local or central data policy
- (Default) Original DSCP marking is copied to the outer DSCP marking
- (Optional) Egress outer DSCP rewrite
  - Re-write rules based on forwarding class mapping on ingress
- (Optional) Egress COS rewrite
  - Re-write rules based on forwarding class mapping on ingress

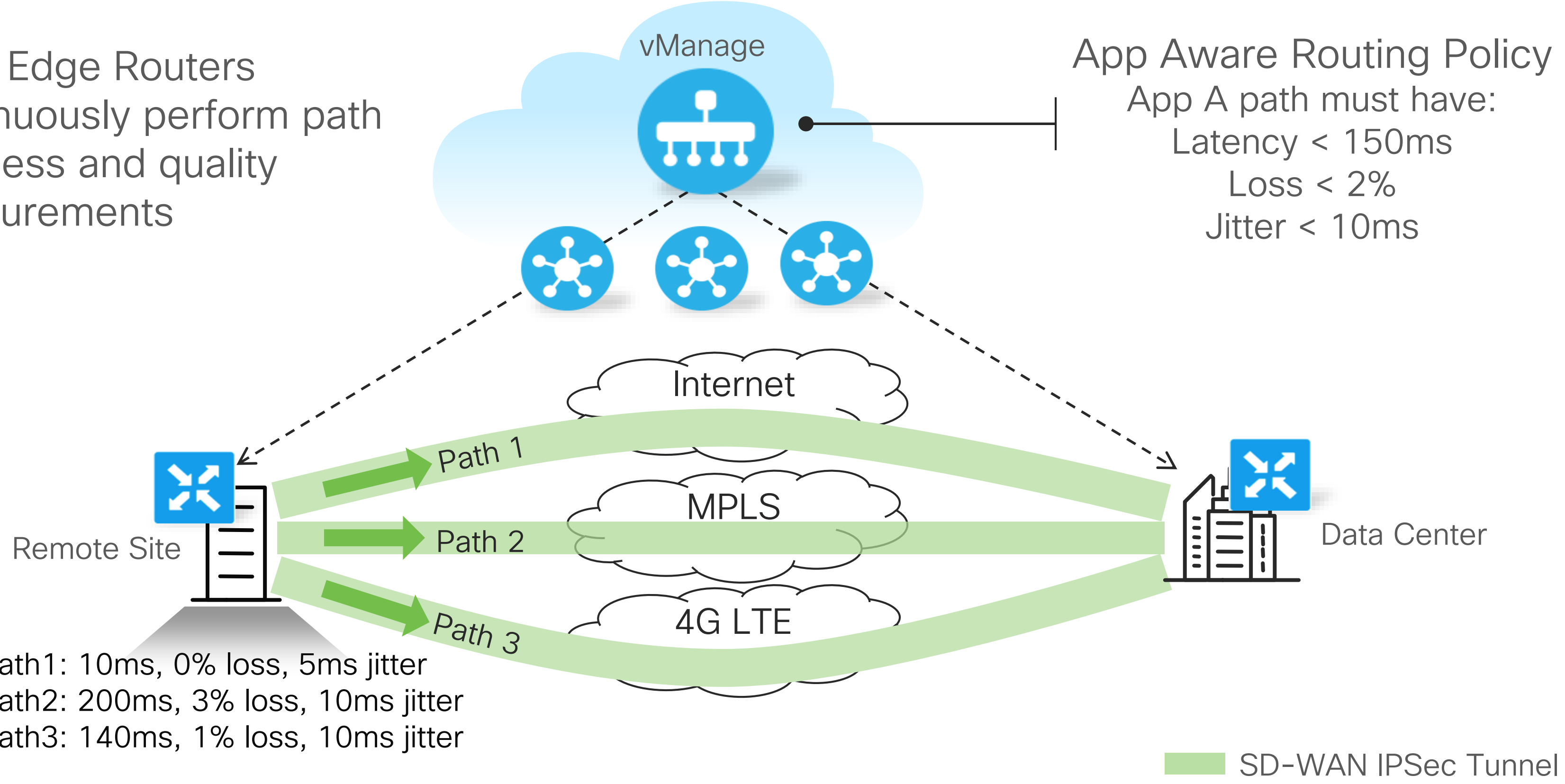
Path Quality Detection



- Each WAN Edge router initiates BFD packet every hello interval
  - Echo mode, no neighbors
  - Tunable to sub-second level
- Poll interval determines the window for calculating path quality
  - Averaged
  - Tunable to sub-second level
- App-route multiplier determines number of poll intervals for establishing overall average path quality
  - Compared against application aware routing thresholds

Critical Applications SLA

- WAN Edge Routers continuously perform path liveliness and quality measurements



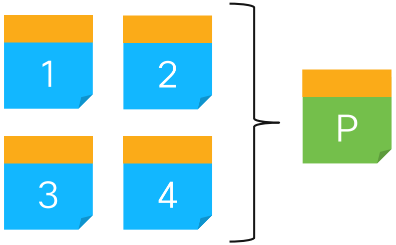
App Aware Routing Policy
App A path must have:
Latency < 150ms
Loss < 2%
Jitter < 10ms

Path1: 10ms, 0% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

🟩 SD-WAN IPSec Tunnel

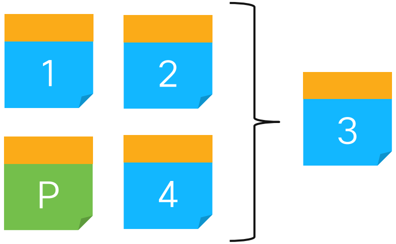
Forward Error Correction (FEC)

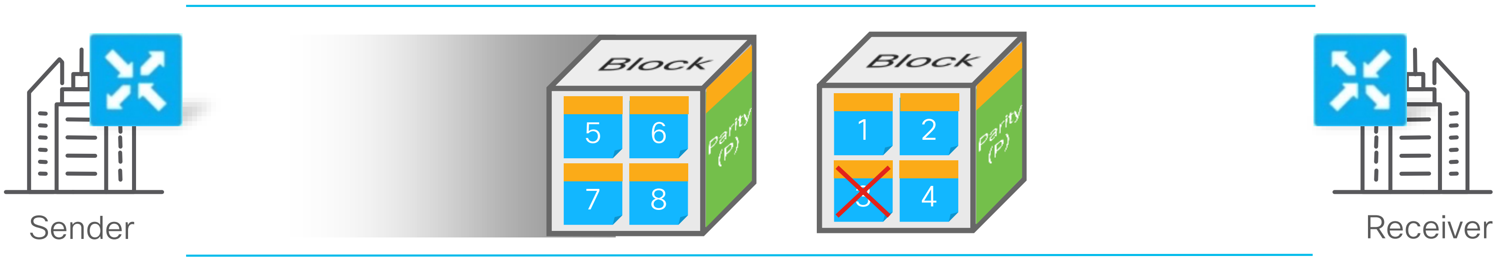
- Protects against packet loss
- Protocol (TCP/UDP) agnostic
- Operates per-tunnel
- Supports multiple transports
- Can be invoked dynamically
- Applied with data policy



Notes:

- Application traffic only, not BFD
- Parity packet matches the transport and DSCP value of the last packet in the block
- Parity packet size is the max size of the packet in the block





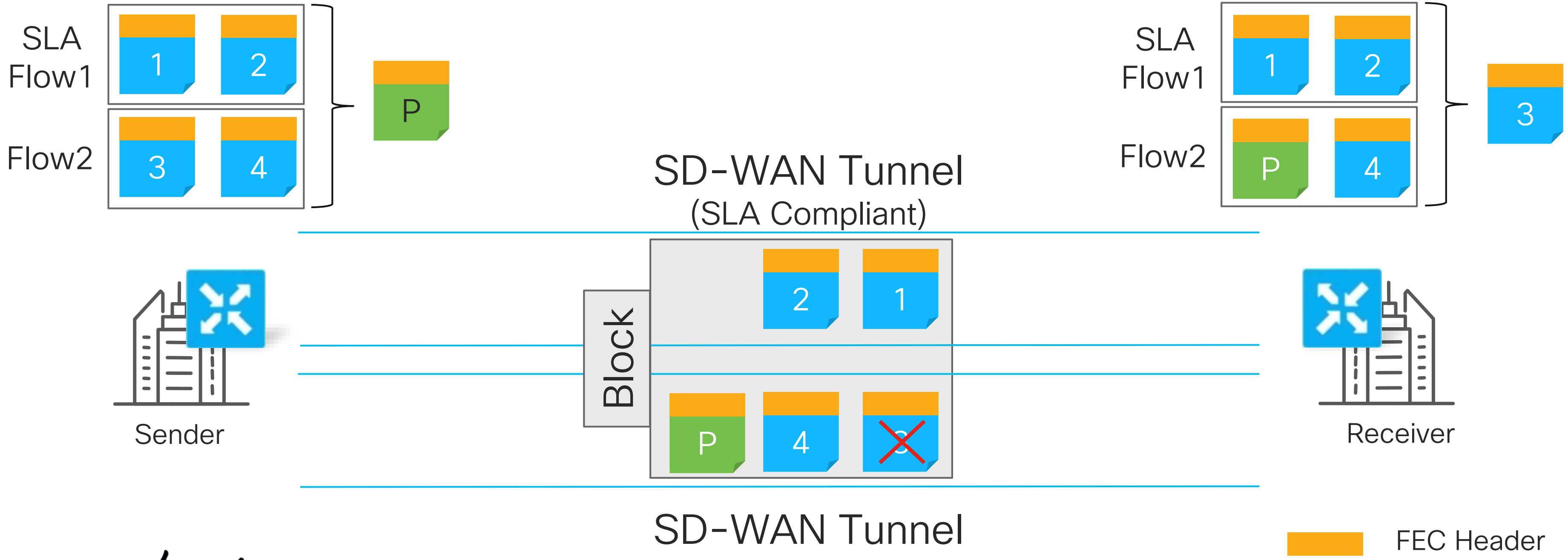
SD-WAN Tunnel

🟧 FEC Header

FEC and Application Aware Routing

- Works independently
- AppAware first, data policy next

- AppAware chooses SLA tunnel(s)
- Data policy applies FEC



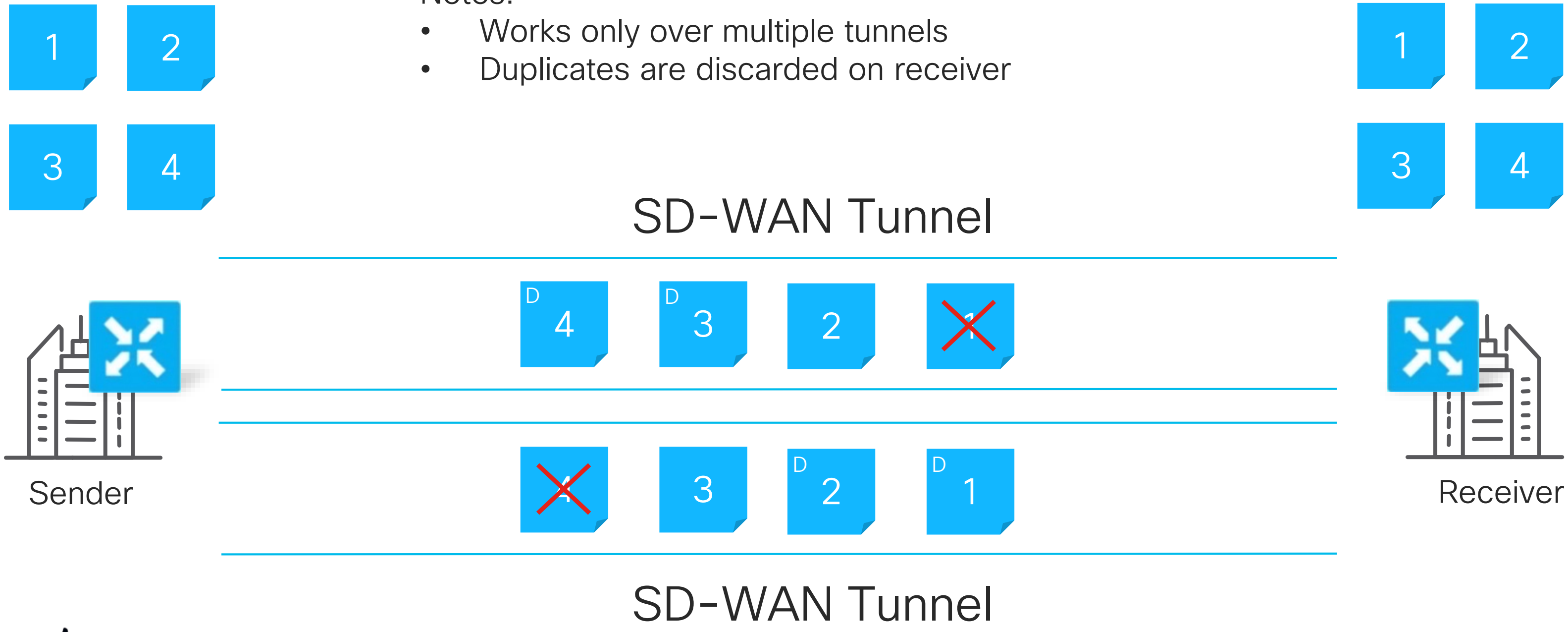
Packet Duplication

- Protects against packet loss
- Protocol (TCP/UDP) agnostic

- Operates over multiple tunnels
- Applied with data policy

Notes:

- Works only over multiple tunnels
- Duplicates are discarded on receiver



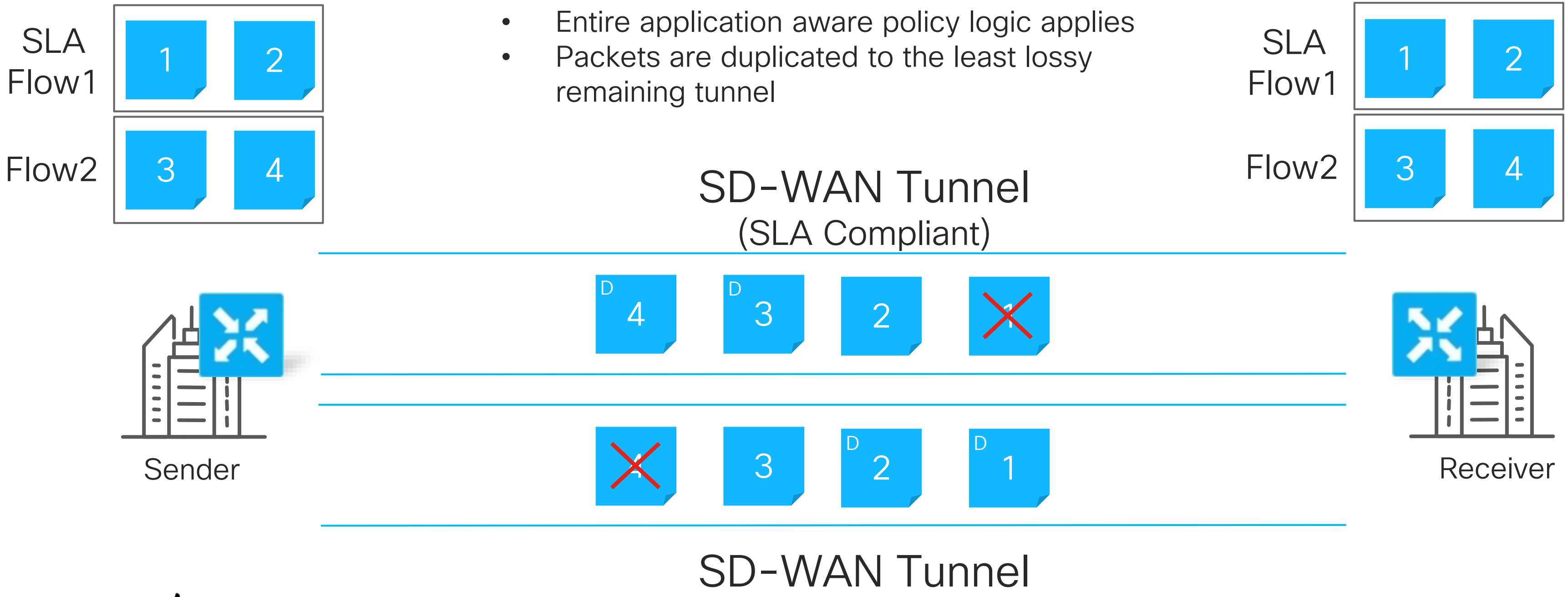
Packet Duplication and Application Aware Routing

- Works independently
- AppAware first, data policy next

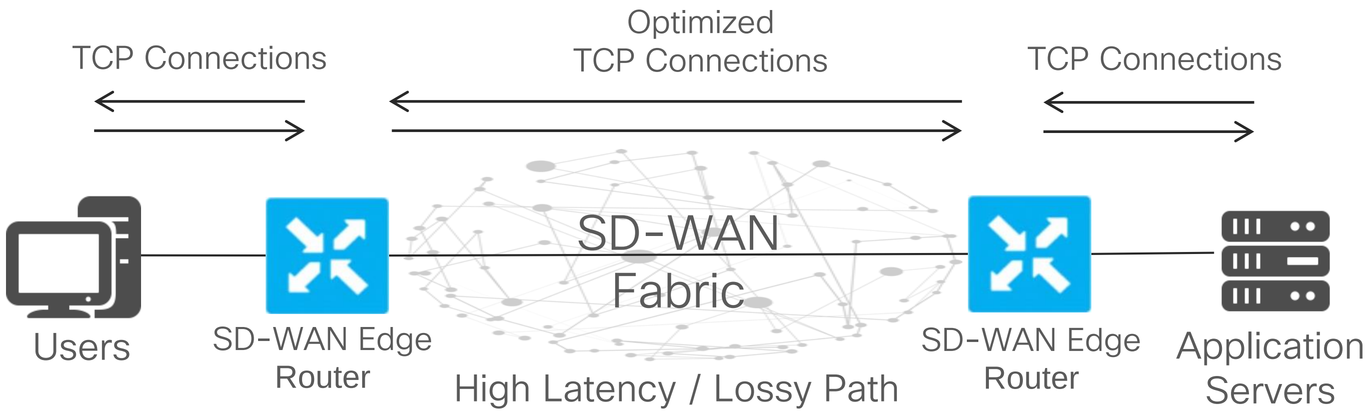
- AppAware chooses SLA tunnel(s)
- Data Policy applies duplication

Notes:

- Entire application aware policy logic applies
- Packets are duplicated to the least lossy remaining tunnel

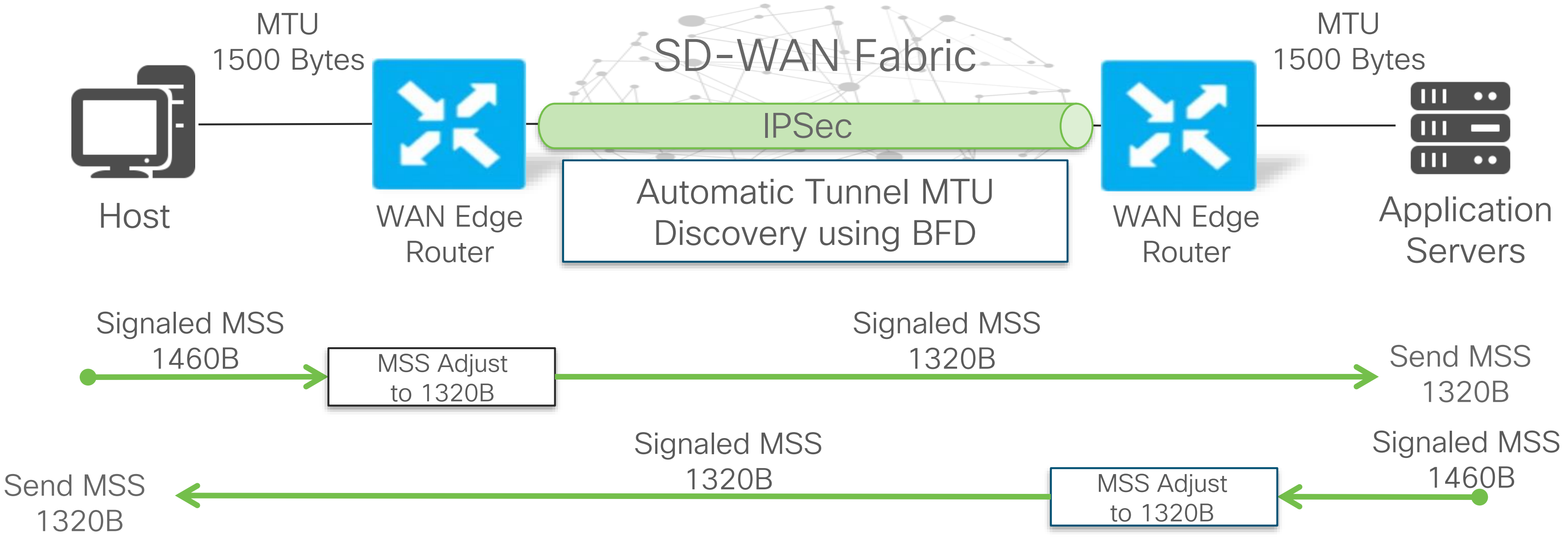


TCP Optimization



- High latency or/and lossy path between users and applications, i.e. geo-distances
- SD-WAN Edge routers terminate TCP sessions and provide local acknowledgements
  - Hosts don’t have to wait for end-to-end TCP ACKs and pause TCP transmission
- Optimized TCP connections use selective acknowledgements to prevent unnecessary retransmissions of received segments
- Hosts using older TCP/IP stacks will see the most benefit

Optimal MTU with TCP MSS Adjust

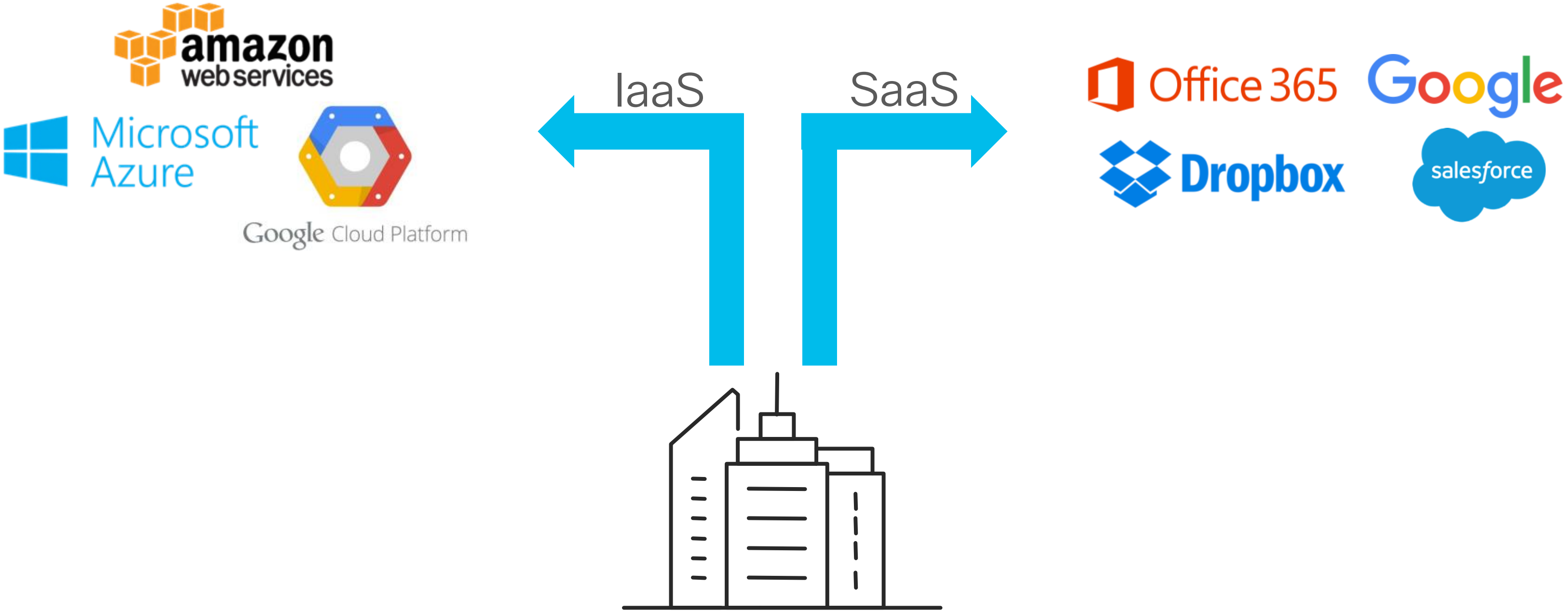


- Send TCP MSS is *min (local link IP MTU - 40B, signaled MSS value)*
  - Signaled in SYN packets
- Can manually set TCP MSS value on WAN Edge router
  - Per-interface

Cloud Adoption

Cloud onRamp for SaaS

Shifts in Enterprise Workloads



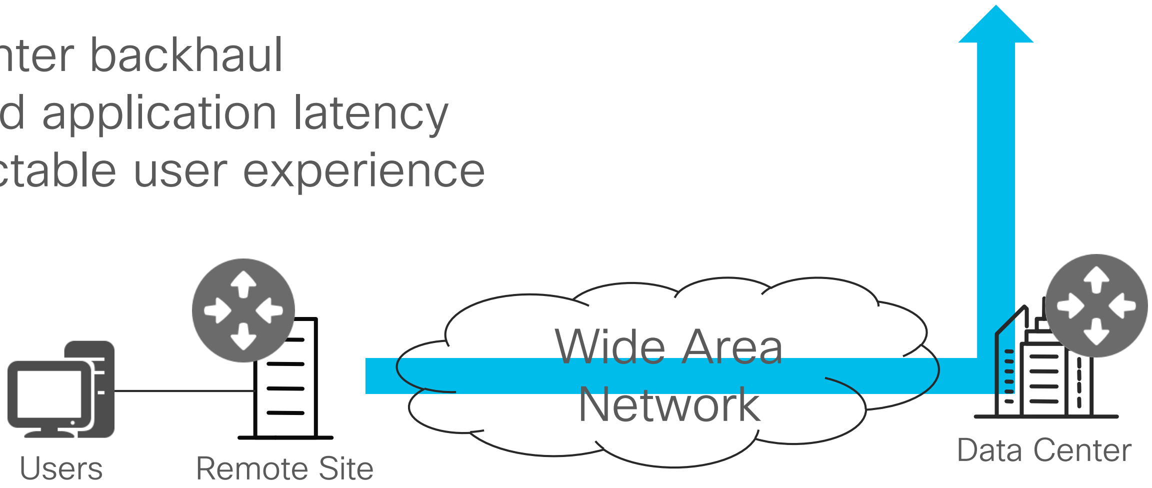
IaaS

SaaS

Traditional On-Premise Data Centers

Traditional Cloud Applications Access

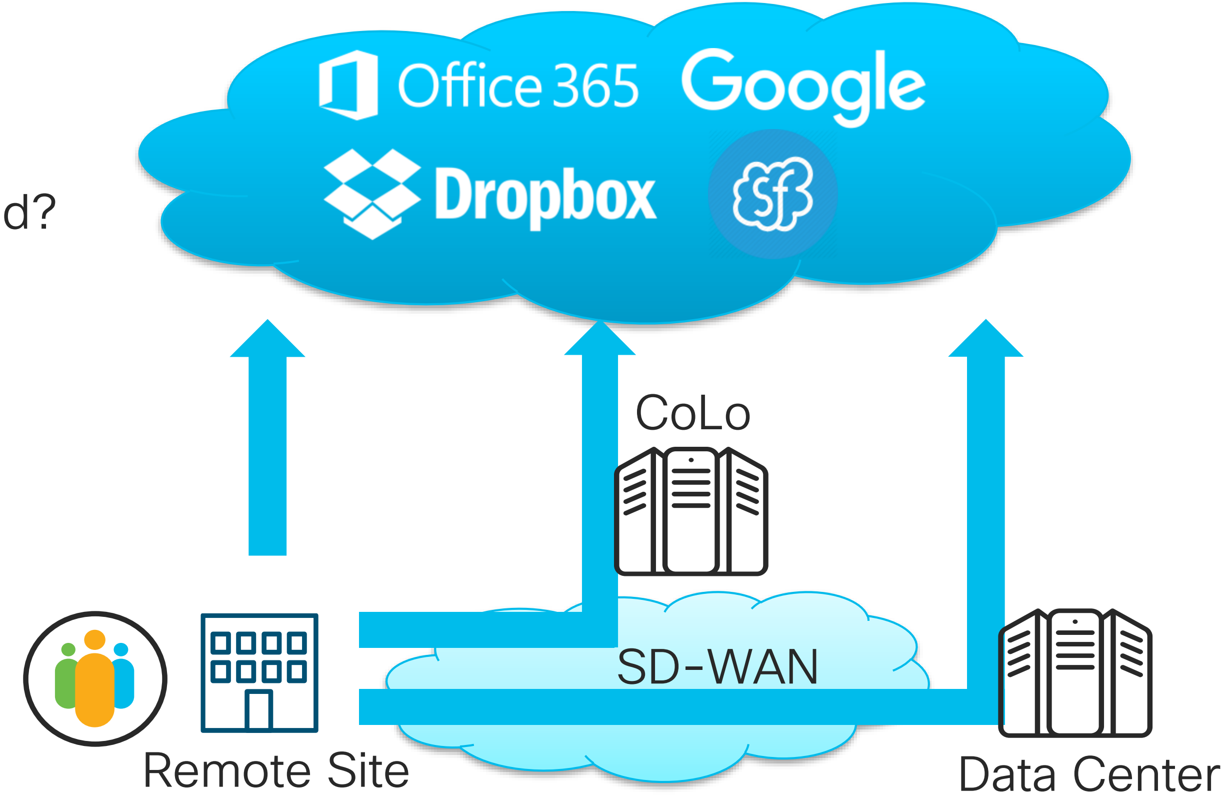
- Data Center backhaul
- Increased application latency
- Unpredictable user experience



Evolutionary SaaS Cloud Adoption with SD-WAN

Problems:

- Which way is cloud?
- Performance?
- Security?



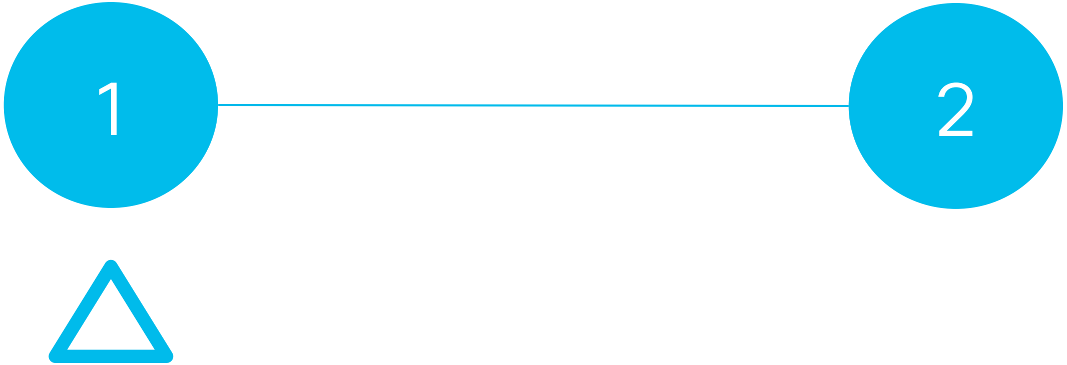
SD-WAN Cloud Applications Multipathing

Cloud Application Access without SLA

Recreational Browsing
Guest Access
Generic Cloud Applications

Cloud Application Access with SLA

Business Critical Applications



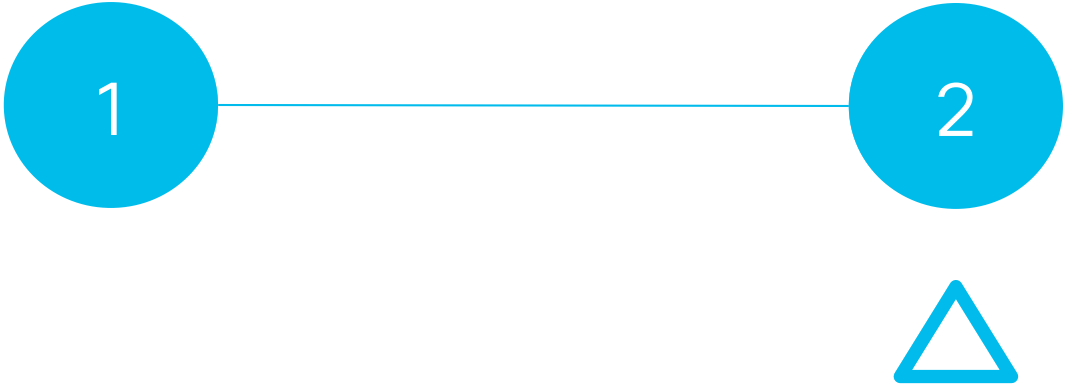
SD-WAN Cloud Applications Multipathing

Cloud Application Access without SLA

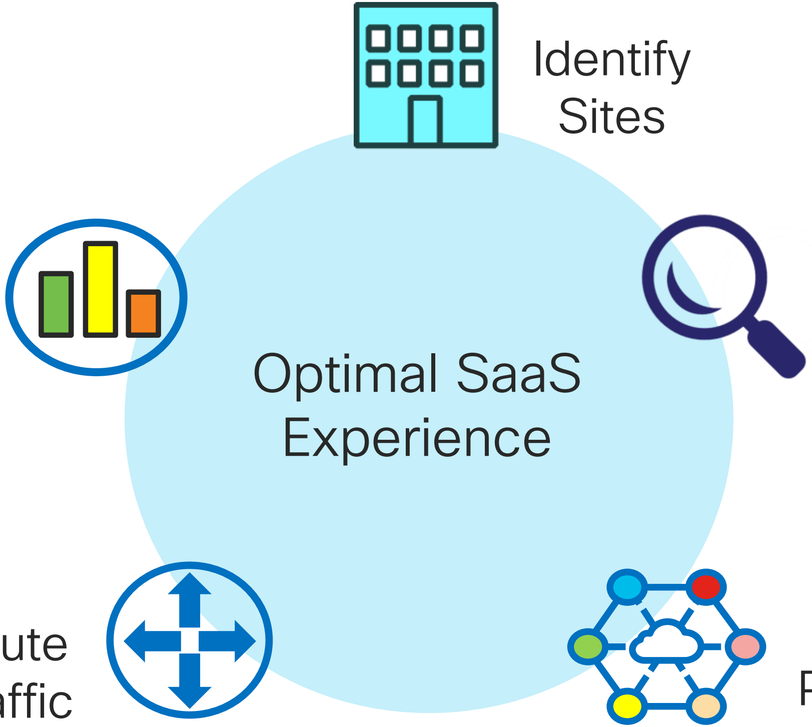
Recreational Browsing
Guest Access
Generic Cloud Applications

Cloud Application Access with SLA

Business Critical Applications



Cloud onRamp for SaaS



Identify Sites

Discover Cloud Applications

Determine Performance

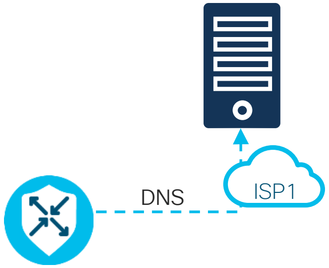
Route Traffic

Report on QoE metric

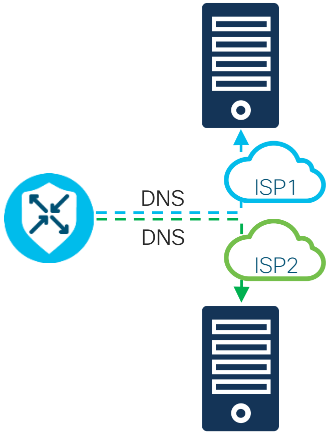
Optimal SaaS Experience

How does it work?

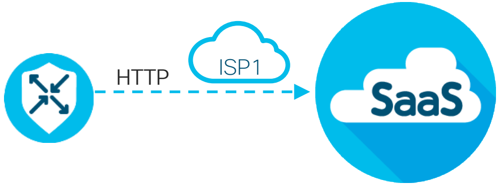
Configured WAN Edge router uses DNS address defined in VPN0 to send a DNS request for pre-configured SaaS application



HTTP ping packets are sent to probe (loss/latency) SaaS performance across all Internet egress points. A Quality of Experience score is then calculated



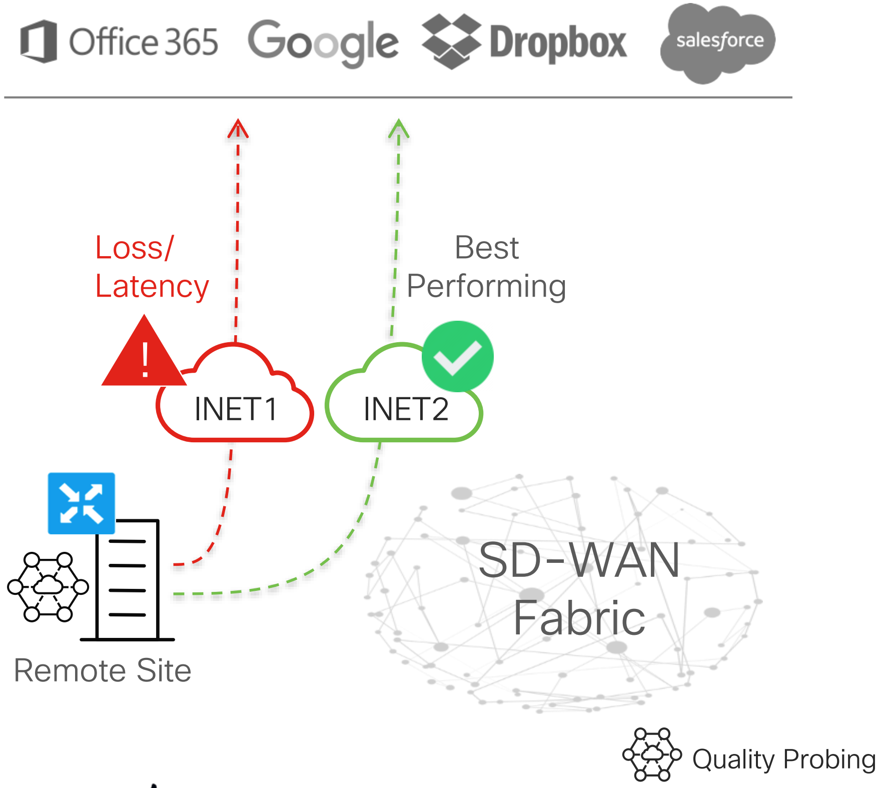
DNS requests are duplicated across all available Internet egress points or Gateway sites



	ISP	Score
✓	1	10
	2	8

Cloud onRamp for SaaS – Multiple DIA

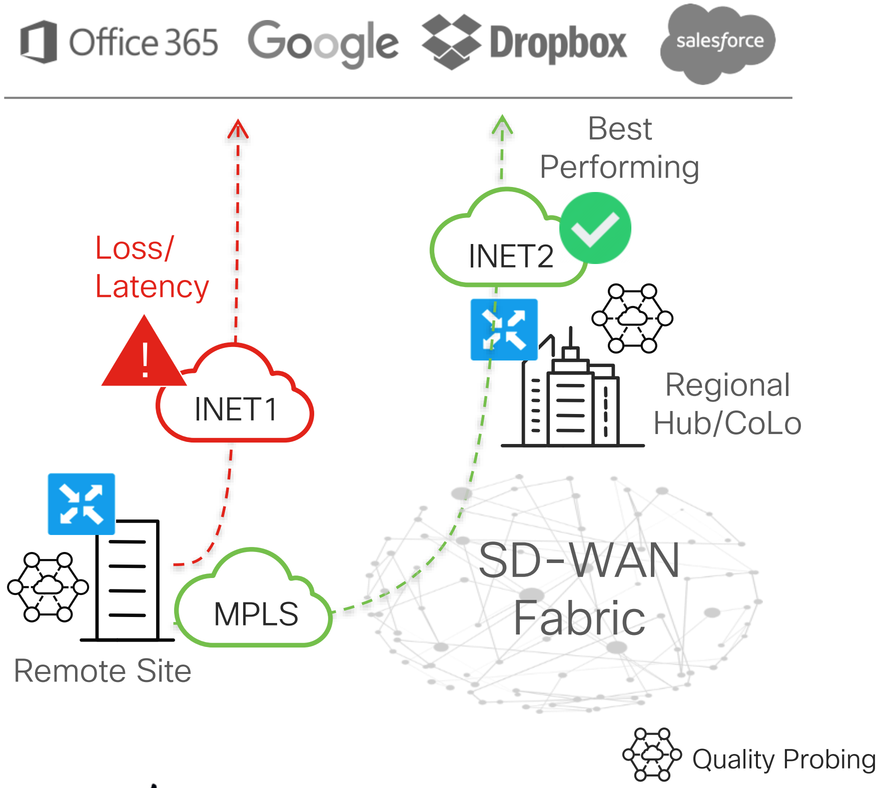
Overview



- Detect application performance through one or more Direct Internet Access circuits
- vEdge routers chose best performing path
  - Per-Application, Per-VPN
- Automatic failover in case of performance degradation
- Fully automated

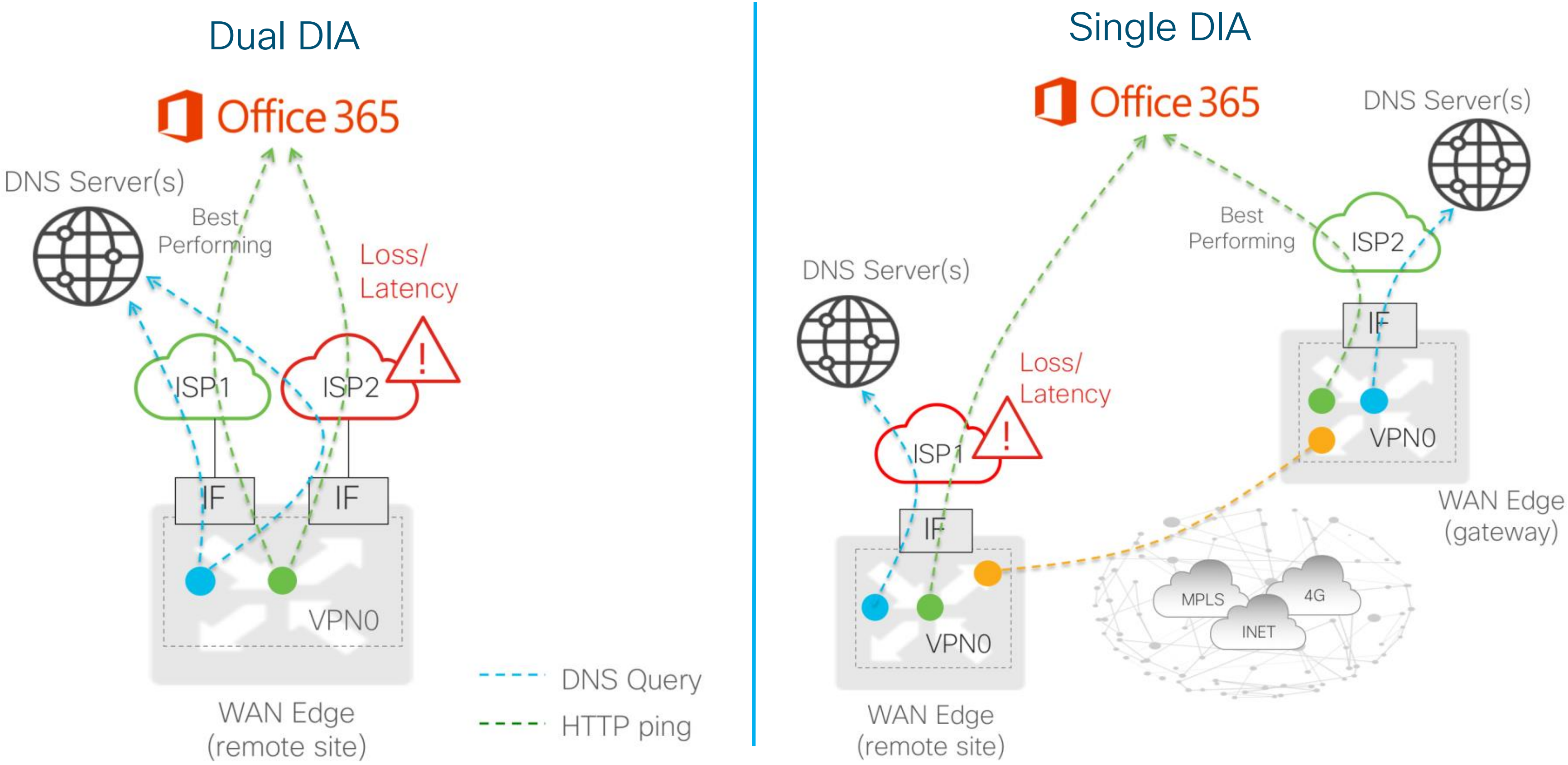
Cloud onRamp for SaaS – DIA(s) and Gateway(s)

Overview



- Detect application performance through DIAs and gateways
  - Customer/SP owned and operated
  - Security, performance, reliability
- vEdge routers chose best performing path
  - Per-Application, Per-VPN
- Automatic failover in case of performance degradation
- Fully automated

Quality Probing



vQoE Scores

Dual DIA

Office 365

App	Path	Score
O365	ISP1 (DIA)	10
O365	ISP2 (DIA)	8

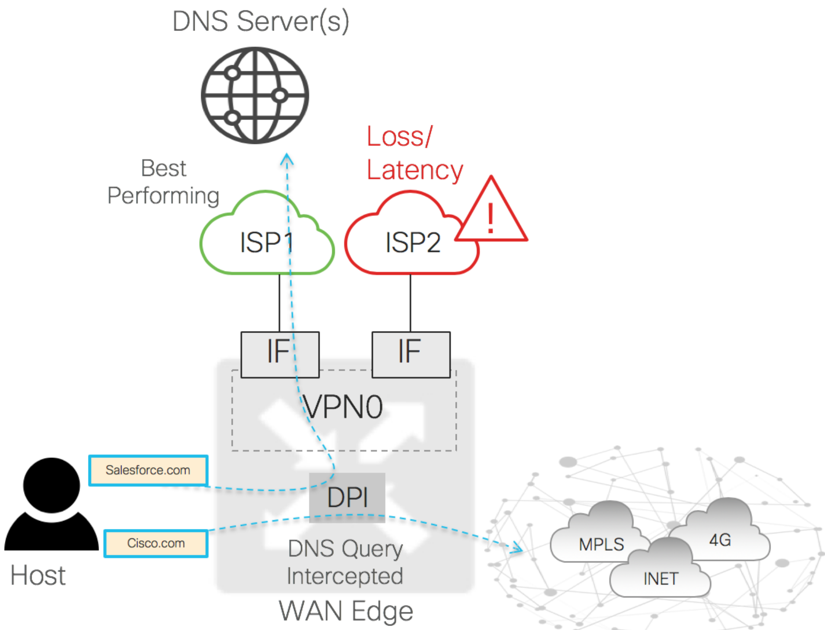
Single DIA

Office 365

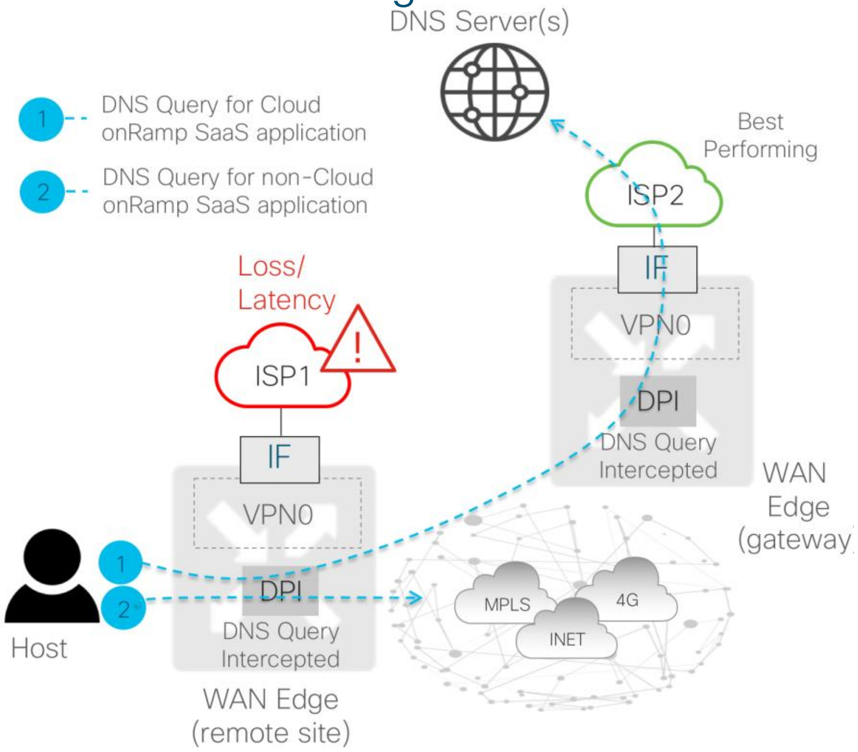
App	Path	Score
O365	ISP1 (DIA)	9
O365	Via Gateway	4

DNS Resolution

Dual DIA

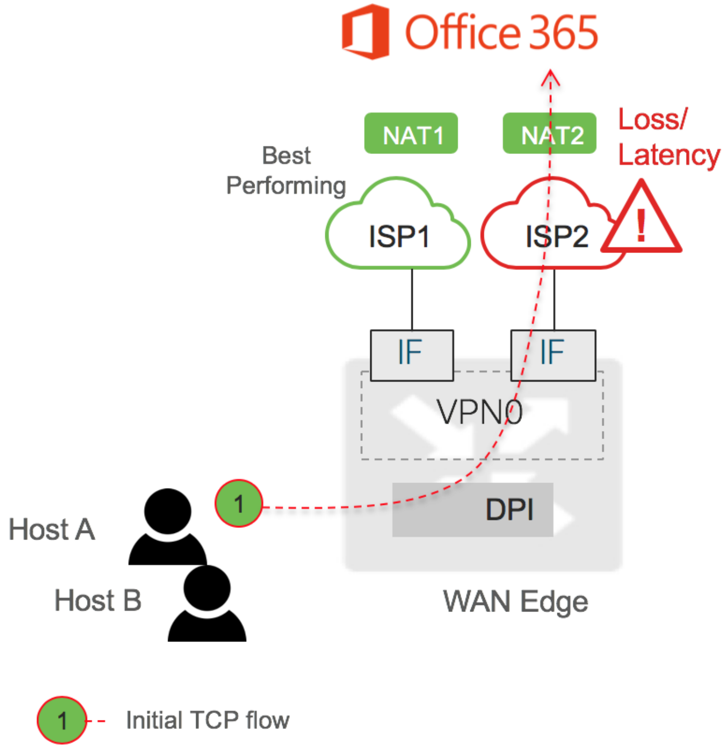


Single DIA

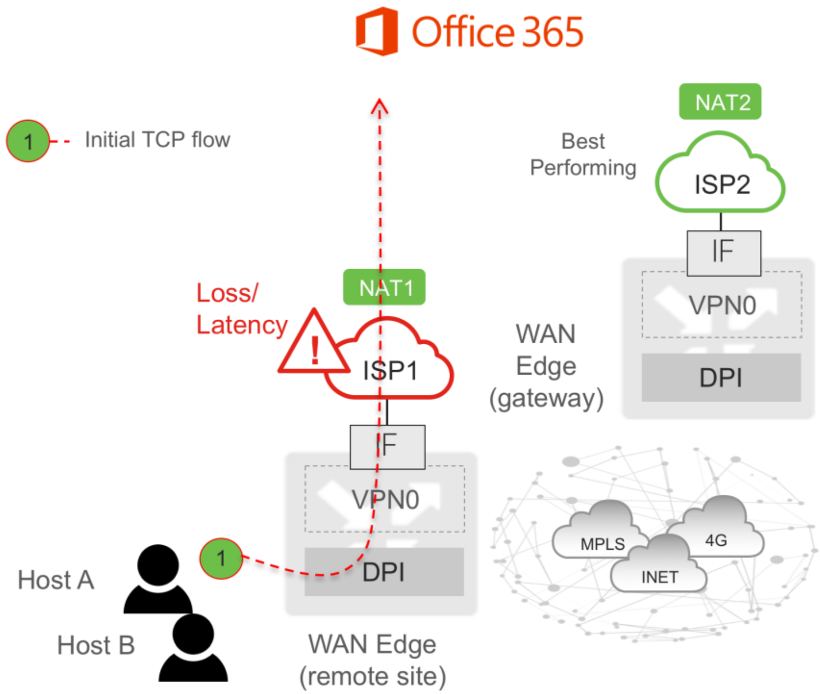


Path Selection – first flow

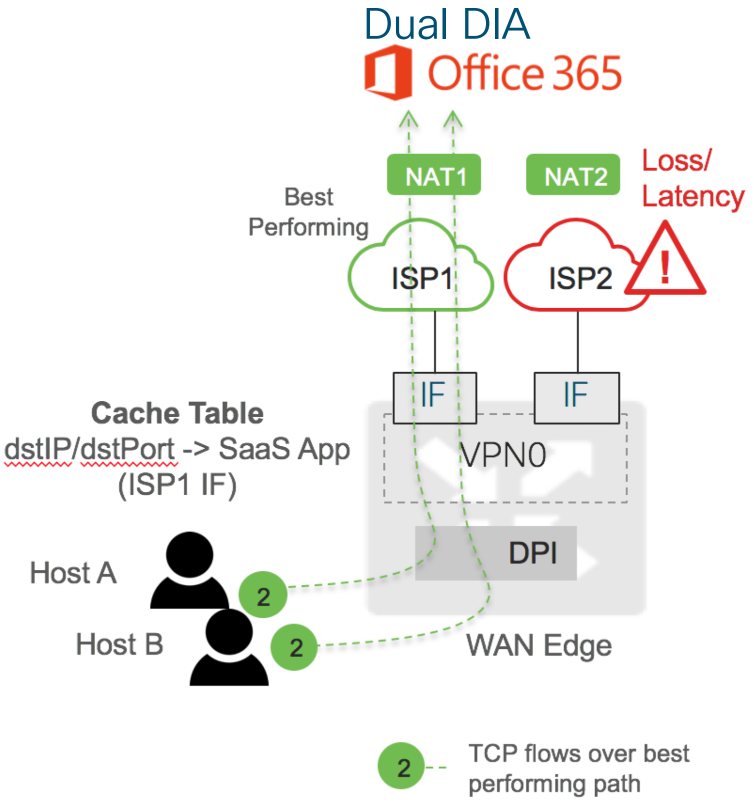
Dual DIA

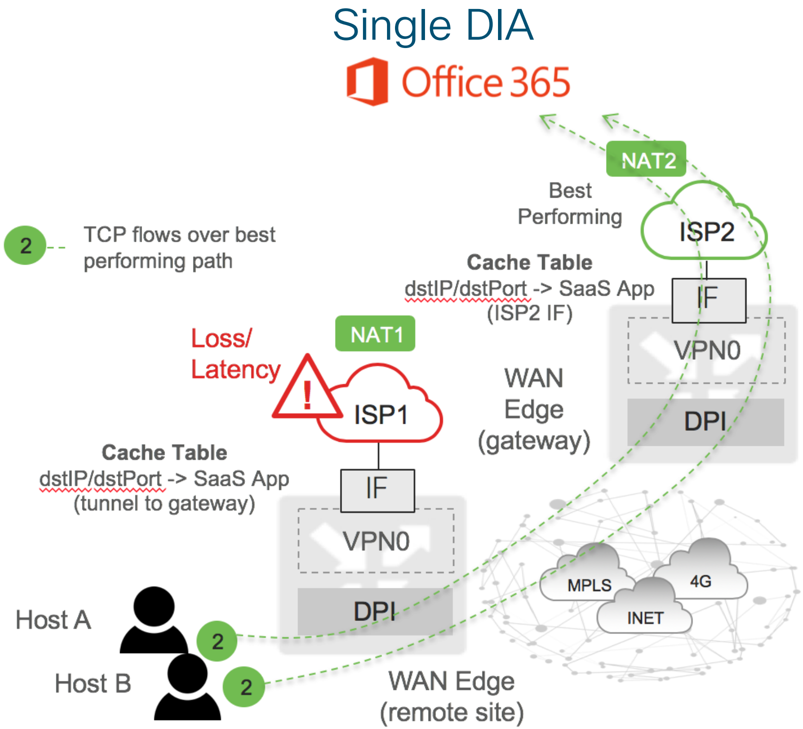


Single DIA

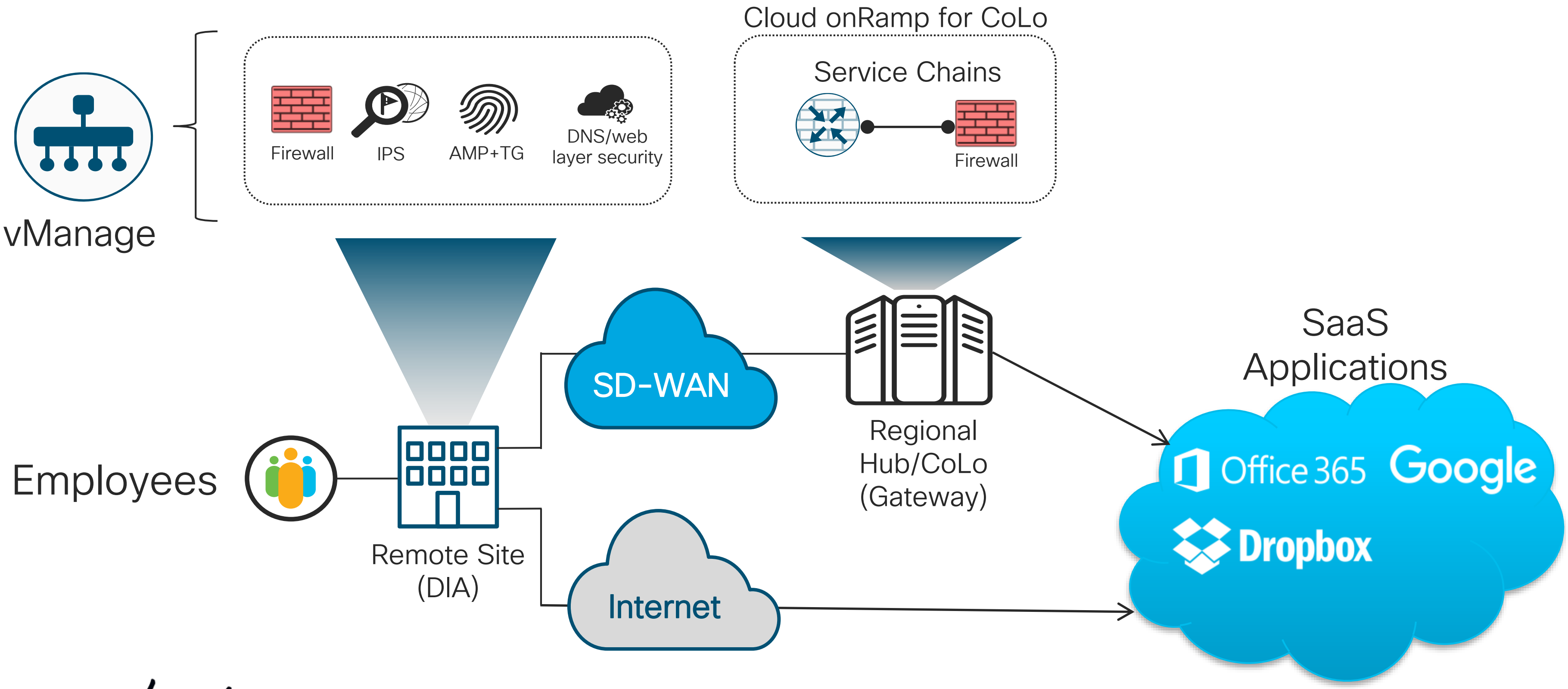


Path Selection – subsequent flow





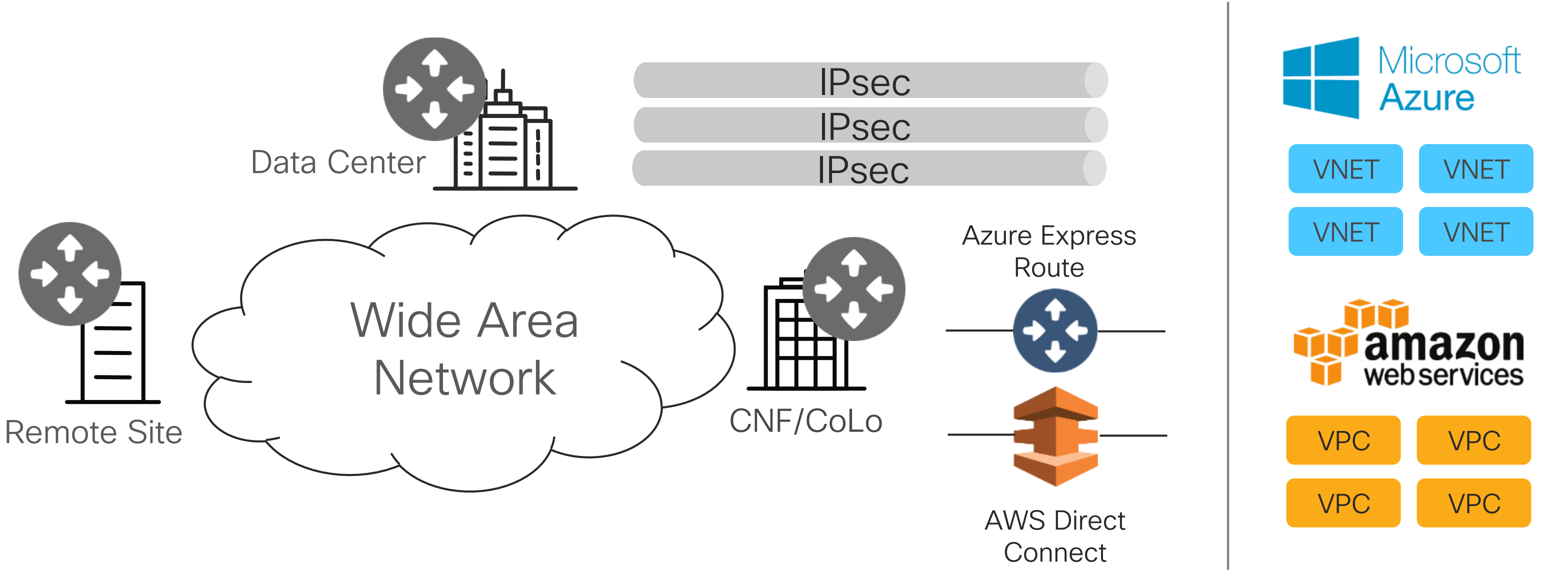
Securing Cloud onRamp for SaaS



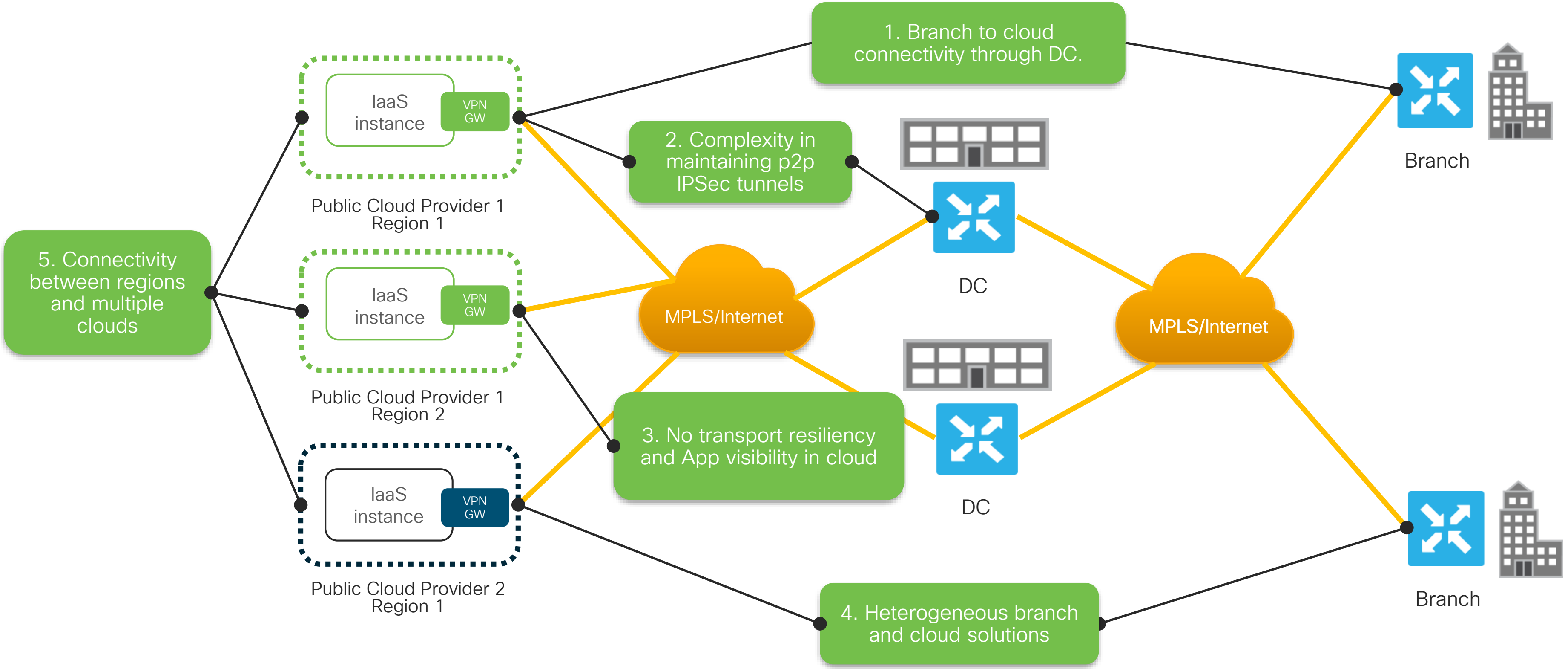
Cloud onRamp for IaaS

Traditional IaaS Access

- No Direct to Cloud access
- Limited segmentation and QoS
- Dependent on underlying technology

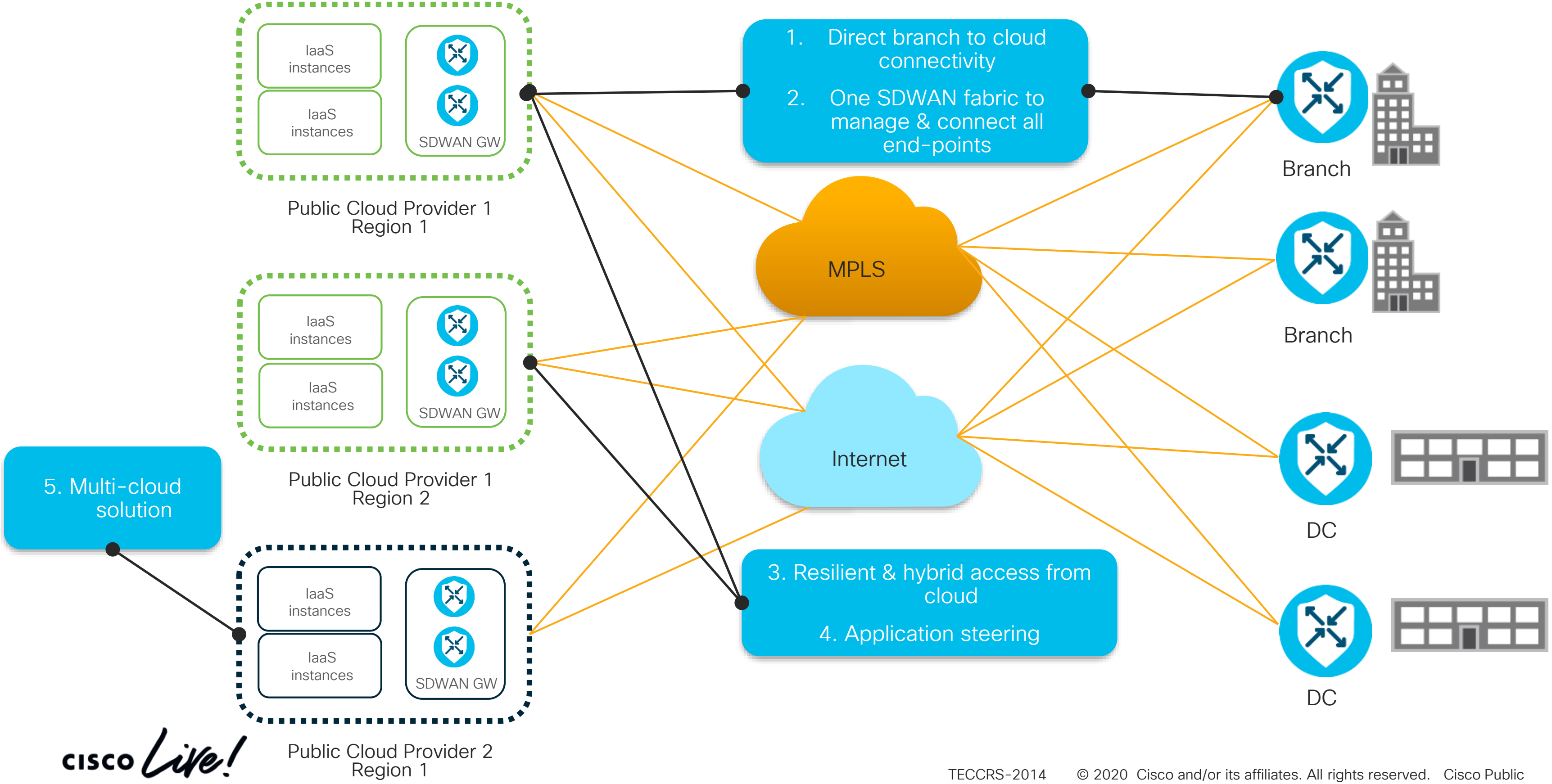


Challenges with Hybrid Cloud Today



1. Branch to cloud connectivity through DC.
2. Complexity in maintaining p2p IPSec tunnels
3. No transport resiliency and App visibility in cloud
4. Heterogeneous branch and cloud solutions
5. Connectivity between regions and multiple clouds
IaaS instance
VPN GW
Public Cloud Provider 1 Region 1
IaaS instance
VPN GW
Public Cloud Provider 1 Region 2
IaaS instance
VPN GW
Public Cloud Provider 2 Region 1
MPLS/Internet
DC
DC
MPLS/Internet
Branch
Branch

Cloud onRamp IaaS: Value Proposition



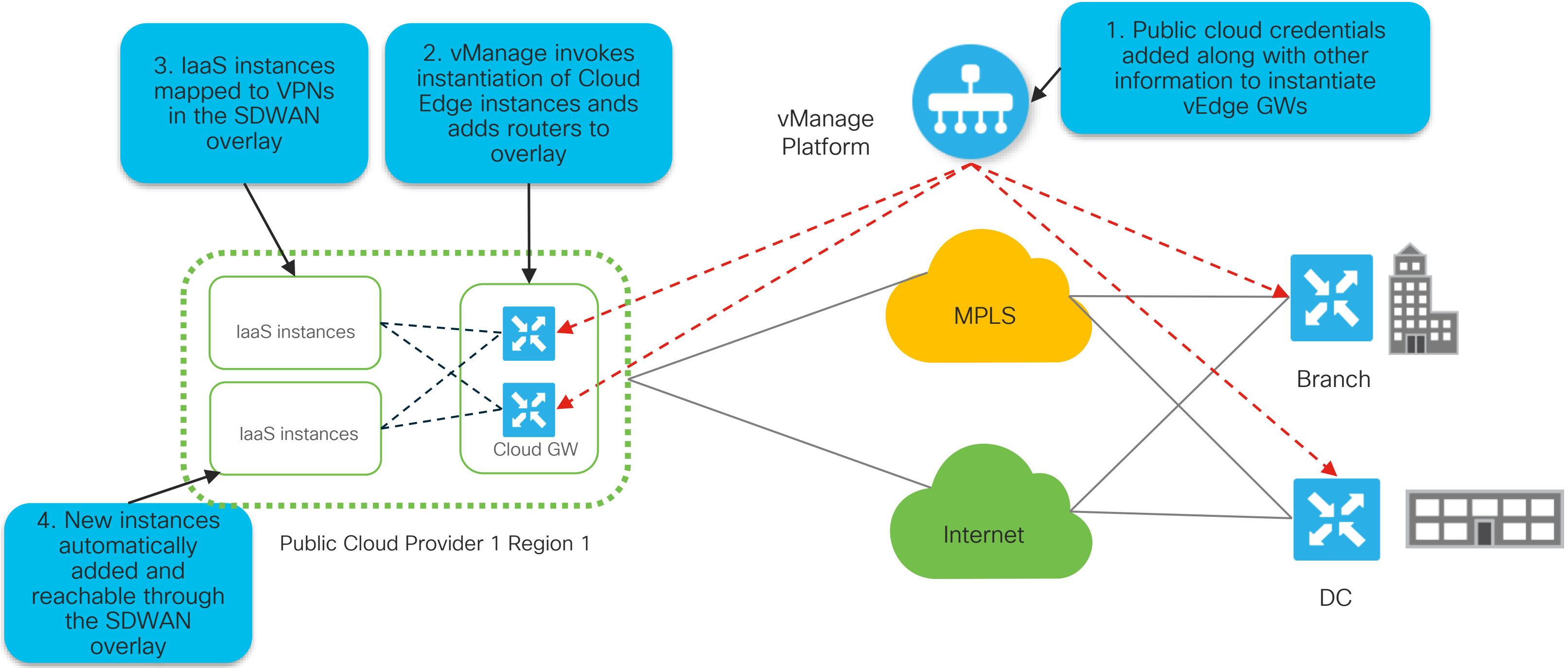
1. Direct branch to cloud connectivity
2. One SDWAN fabric to manage & connect all end-points

3. Resilient & hybrid access from cloud
4. Application steering

5. Multi-cloud solution

Cisco SDWAN Cloud onRamp for IaaS

- Public Cloud (AWS & Azure) connectivity solution consumable through the vManage platform



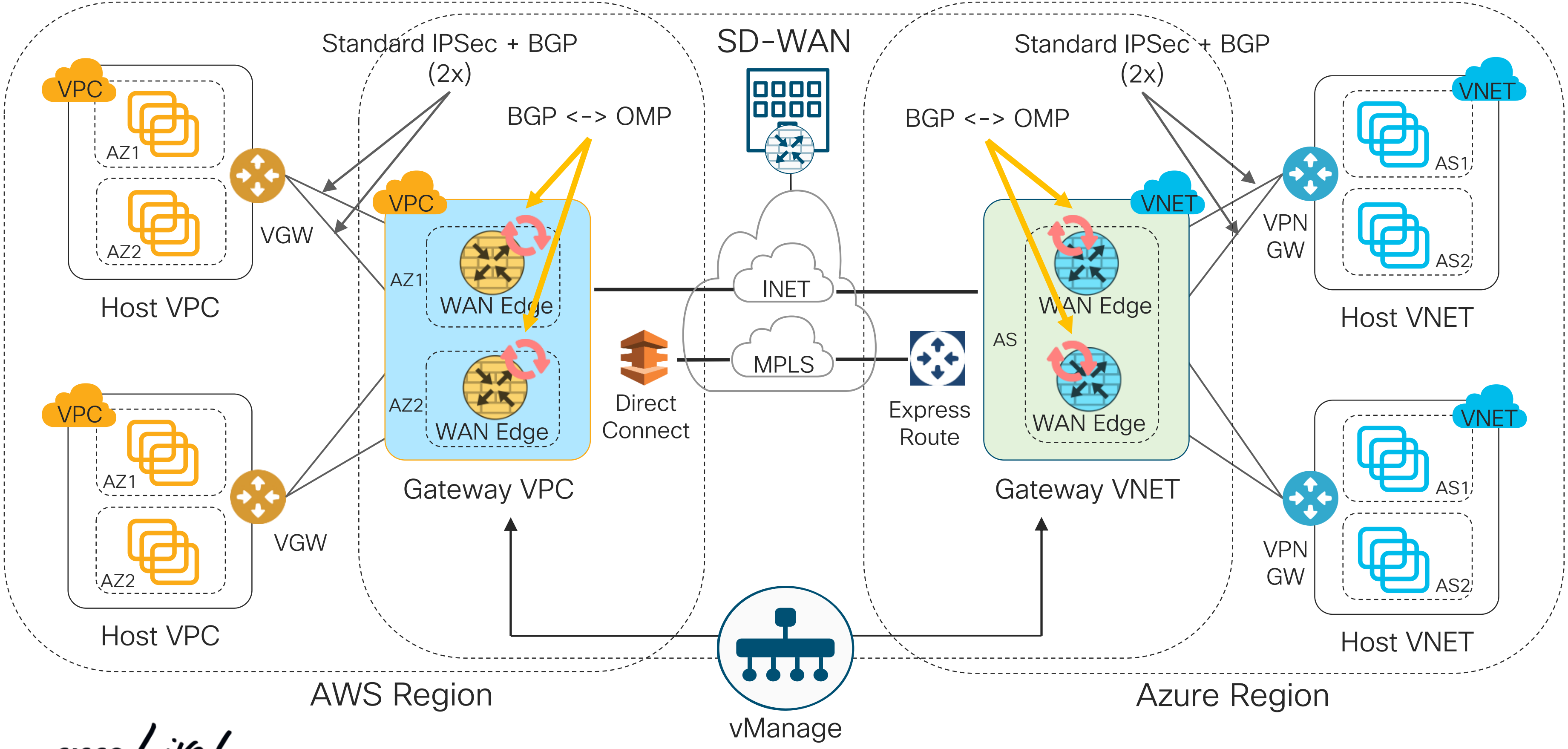
1. Public cloud credentials added along with other information to instantiate vEdge GWs

2. vManage invokes instantiation of Cloud Edge instances ands adds routers to overlay

3. IaaS instances mapped to VPNs in the SDWAN overlay

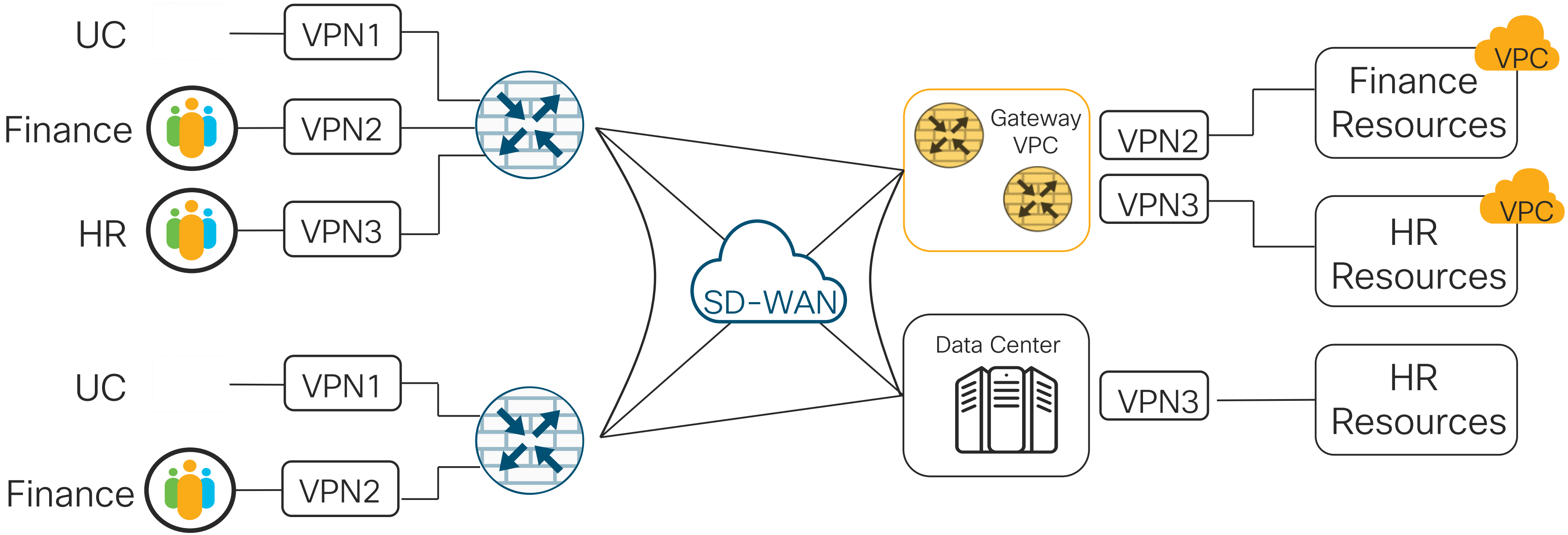
4. New instances automatically added and reachable through the SDWAN overlay

MultiCloud onRamp for IaaS - Explained

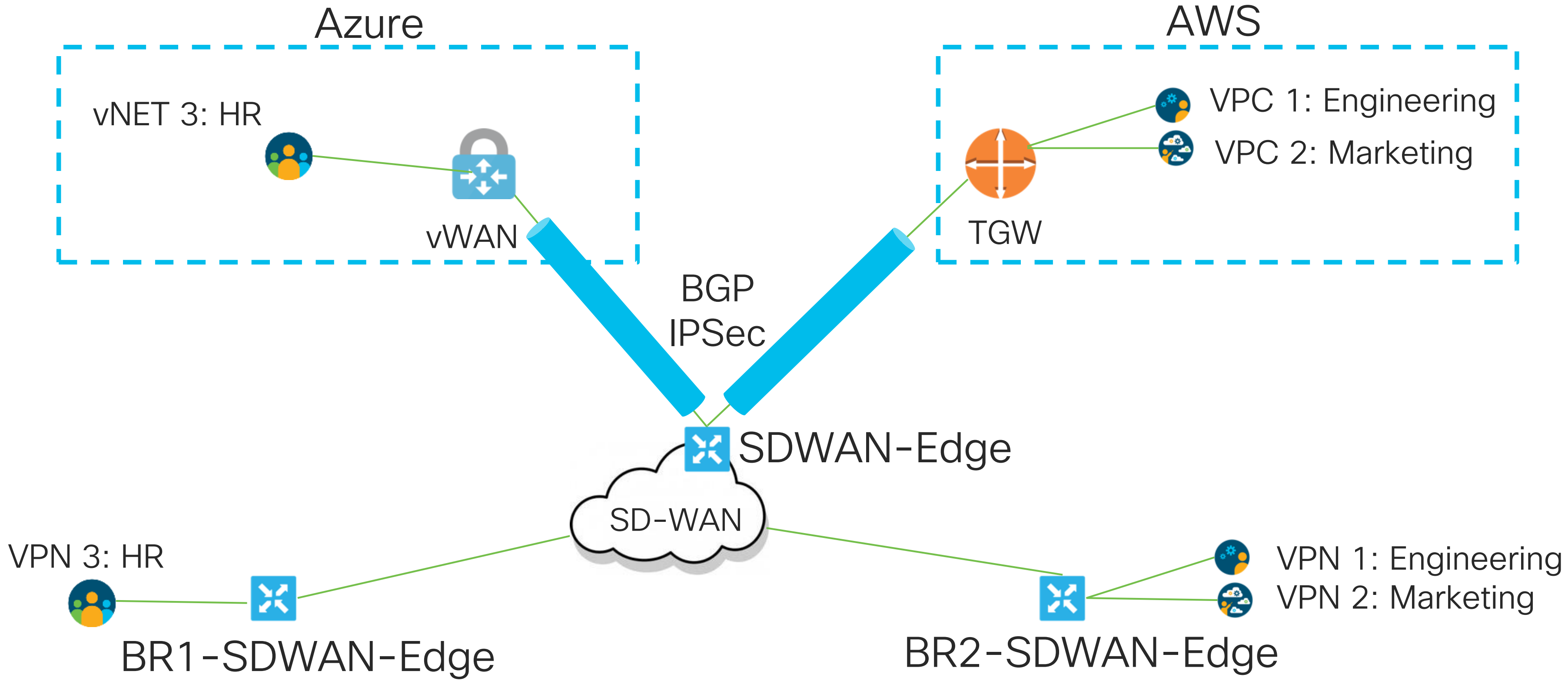


Segmentation and Optimal Topology

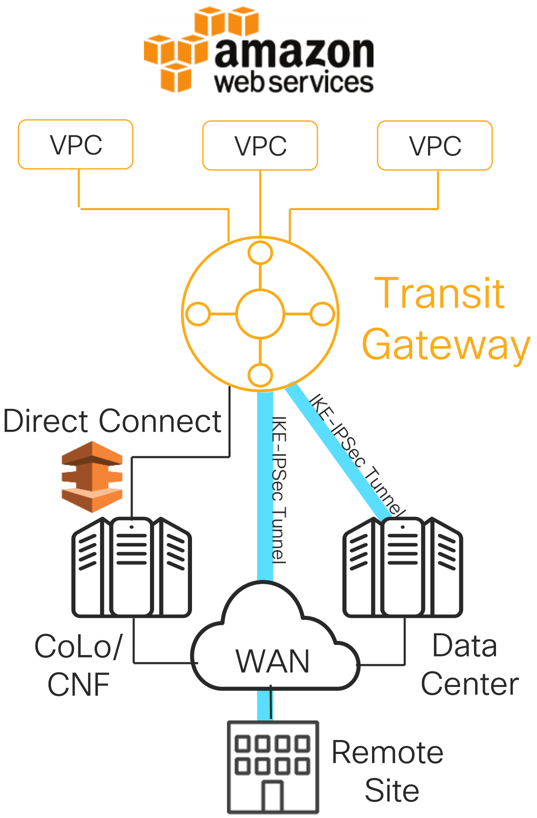
- End-to-end segmentation across public and private Data Centers
- Optimal application topology for best performance



Multicloud Interconnection with Cisco SD-WAN



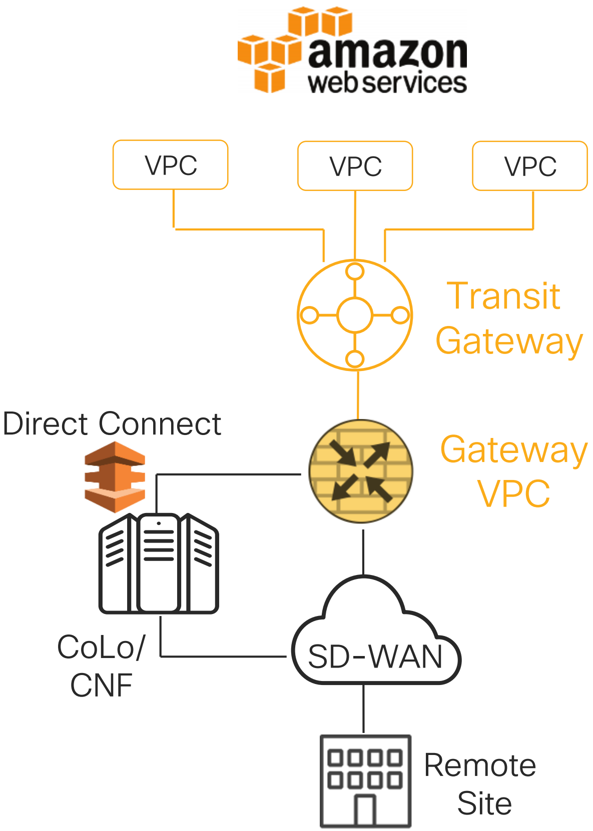
Integrating with AWS Transit Gateway



Disjoined WAN and Cloud

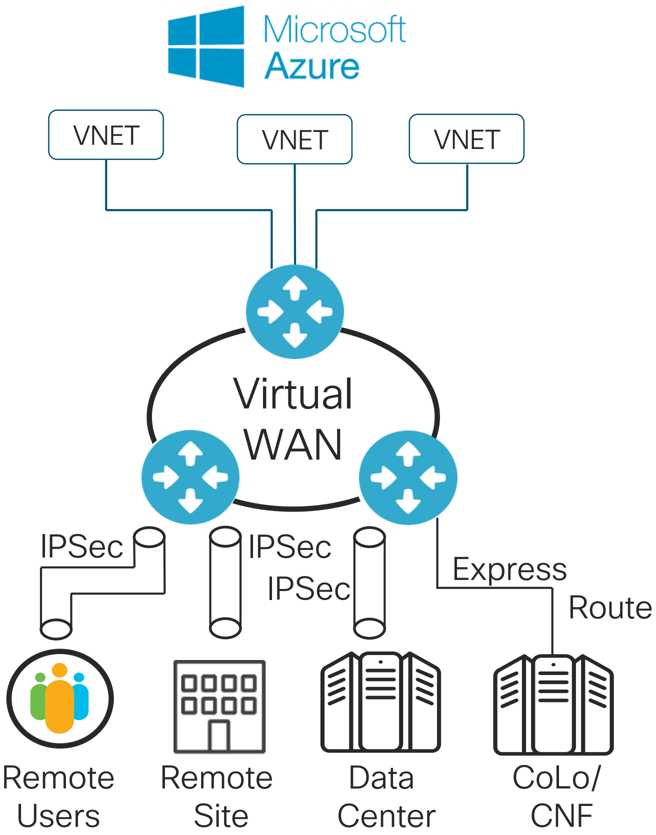
Manual Provisioning

No Direct to Cloud



Automated Direct to Cloud

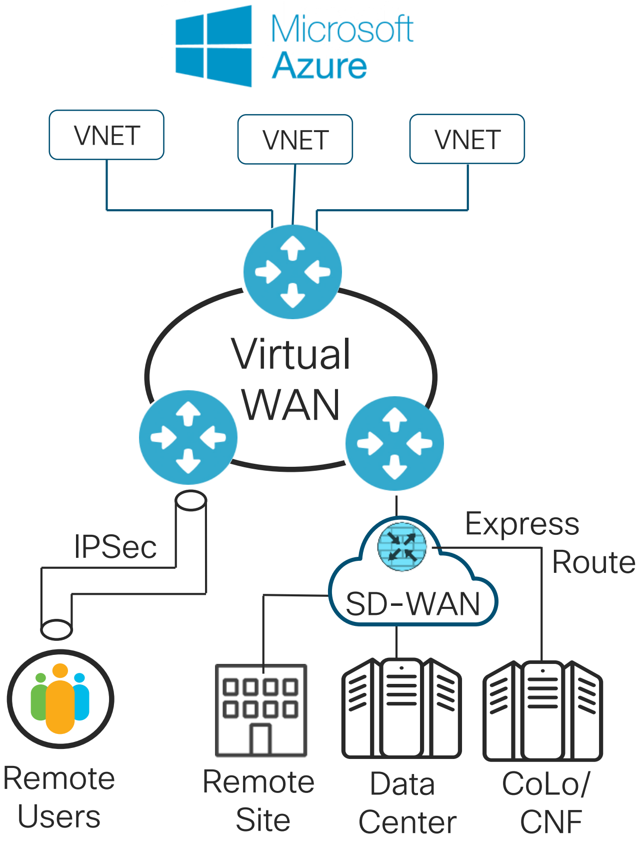
Integrating with Azure vWAN



Disjoined WAN and Cloud

Transport Dependent

Rudimentary, Manual Provisioning

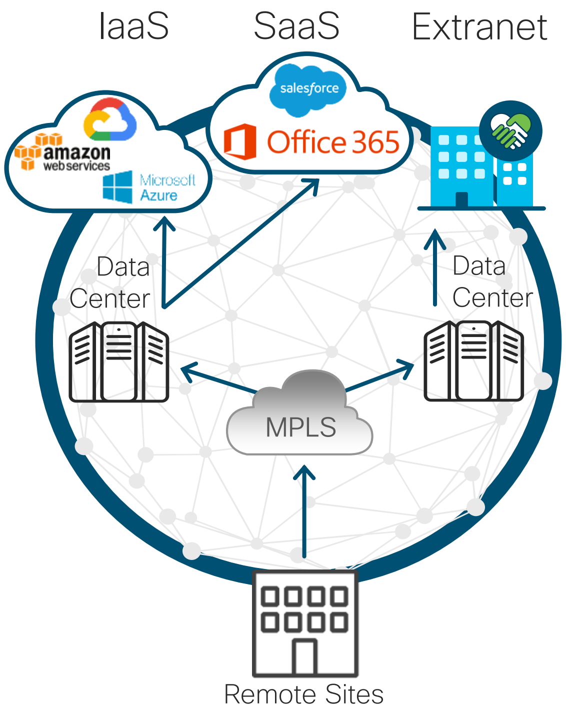


Automated Direct to Cloud

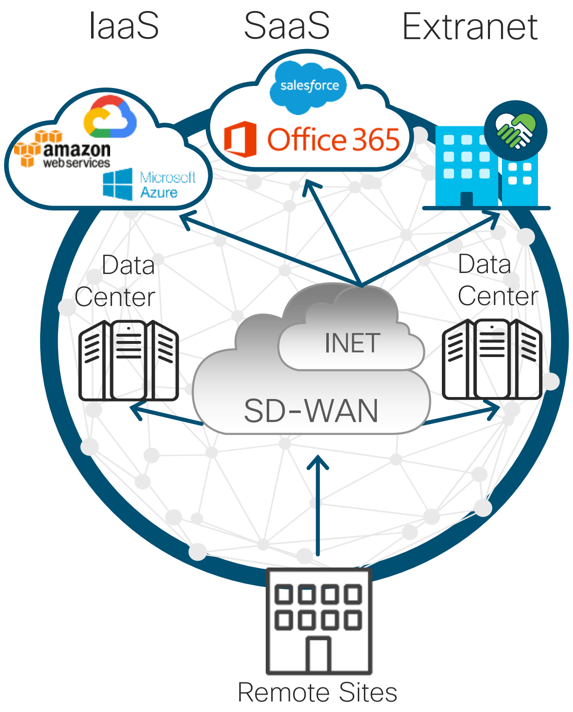
Colocations

Transformation of WAN Requirements

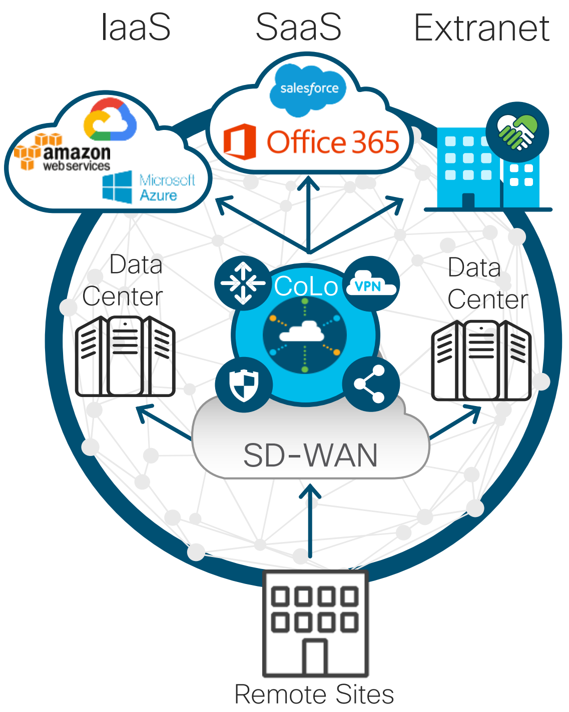
Backhauled Access



Distributed Access



Regional Access

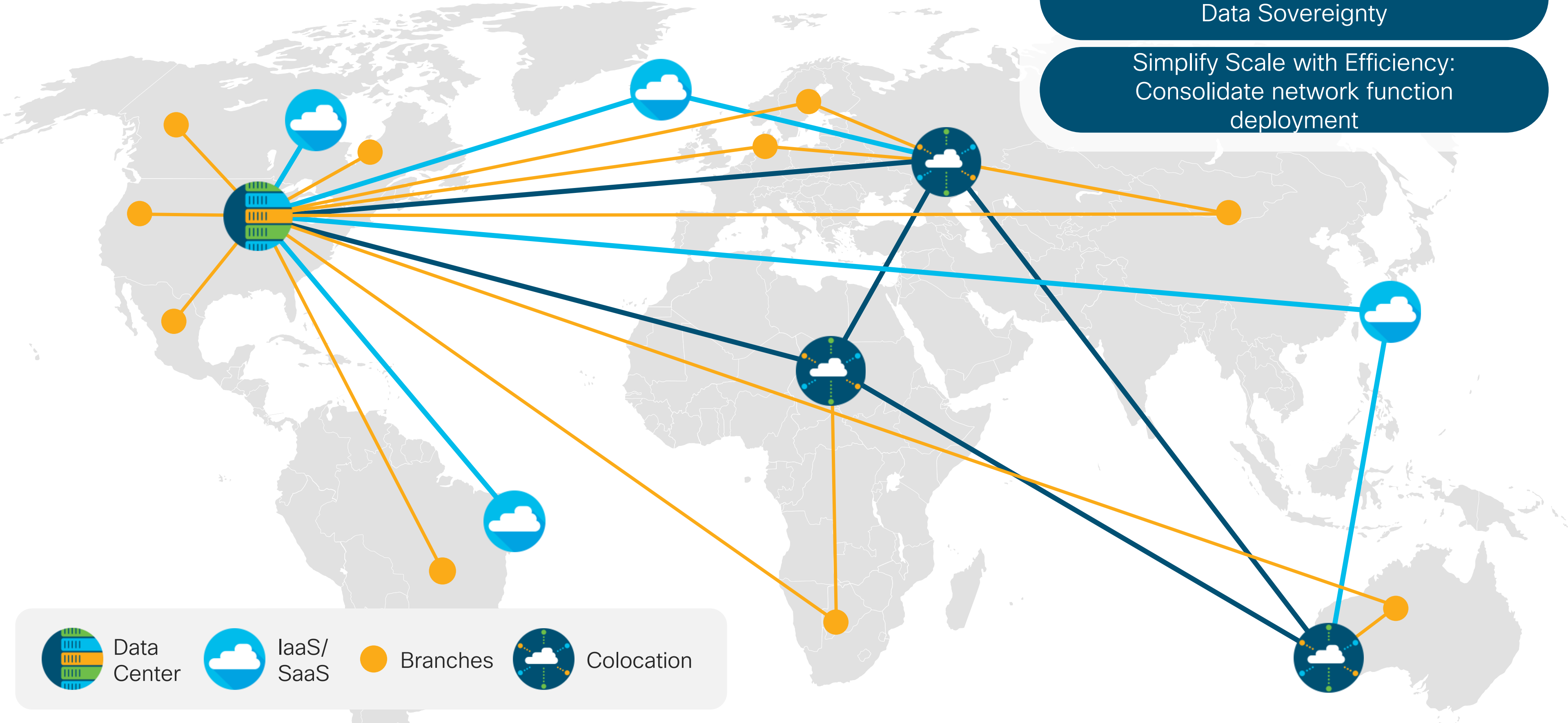


Introducing Cisco SD-WAN Cloud onRamp for Colocation

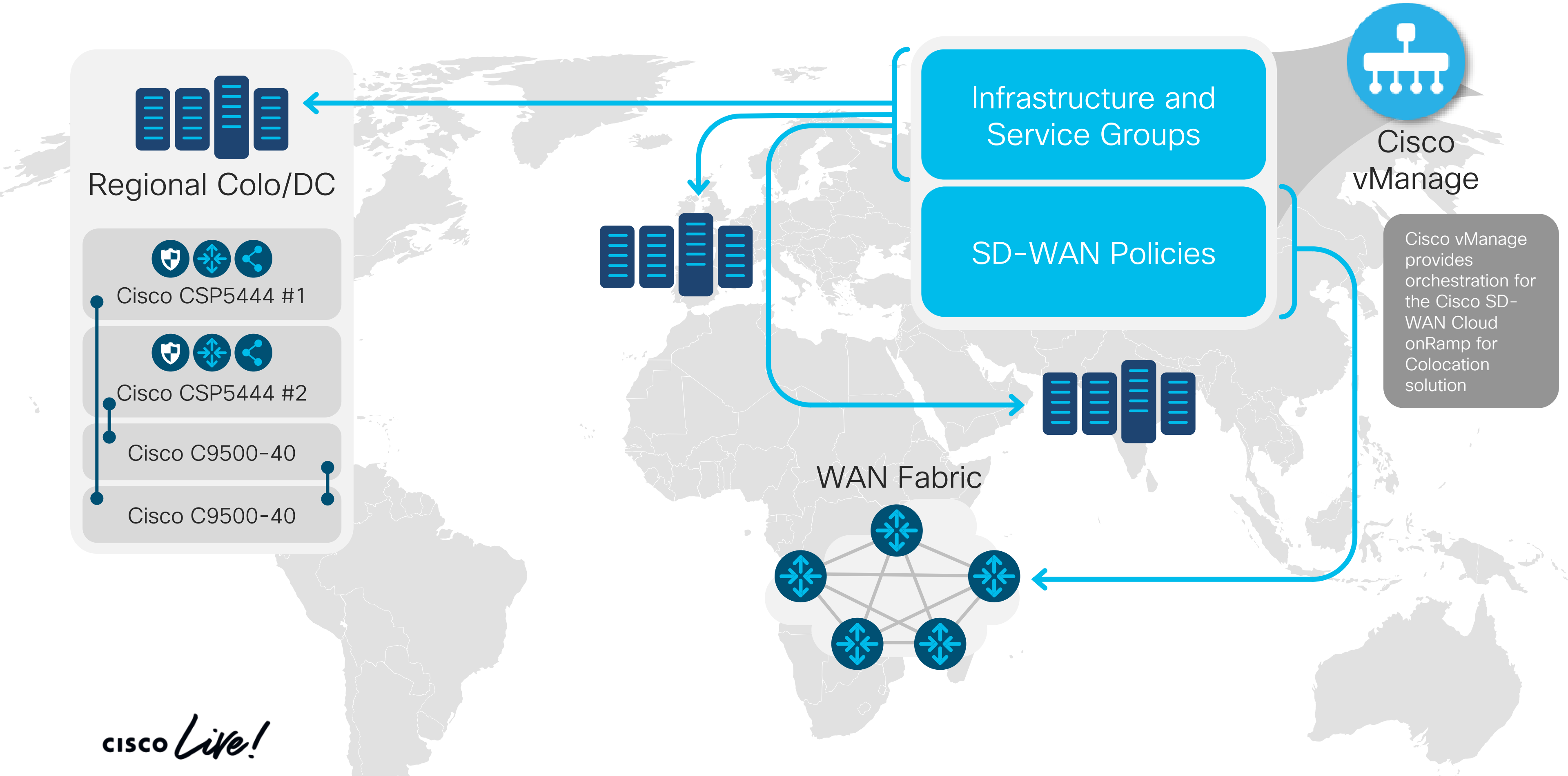
Application Experience:
Bring users closer to services

Address Risk & Compliance:
Data Sovereignty

Simplify Scale with Efficiency:
Consolidate network function deployment

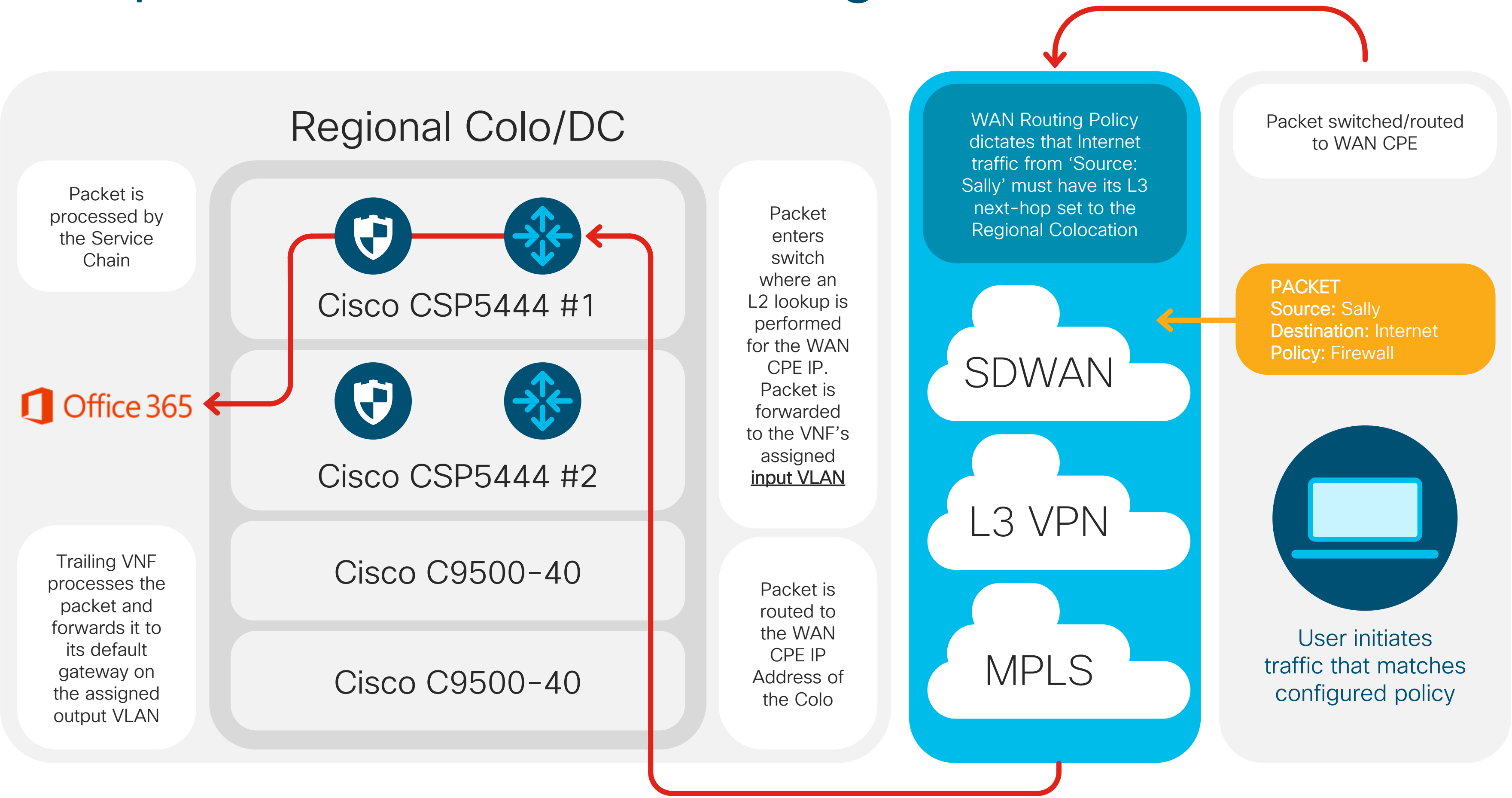


Architecture



Cisco vManage provides orchestration for the Cisco SD-WAN Cloud onRamp for Colocation solution

Simplified Packet Walkthrough



Regional Colo/DC

Packet is processed by the Service Chain

Office 365

Trailing VNF processes the packet and forwards it to its default gateway on the assigned output VLAN

Cisco CSP5444 #1

Cisco CSP5444 #2

Cisco C9500-40

Cisco C9500-40

Packet enters switch where an L2 lookup is performed for the WAN CPE IP. Packet is forwarded to the VNF's assigned <u>input VLAN</u>

Packet is routed to the WAN CPE IP Address of the Colo

WAN Routing Policy dictates that Internet traffic from 'Source: Sally' must have its L3 next-hop set to the Regional Colocation

SDWAN

L3 VPN

MPLS

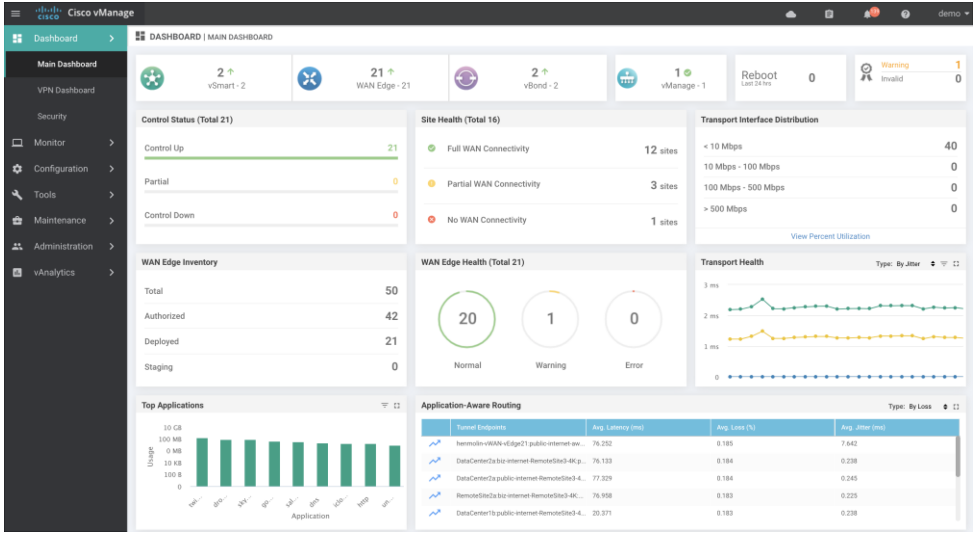
Packet switched/routed to WAN CPE

PACKET
Source: Sally
Destination: Internet
Policy: Firewall

User initiates traffic that matches configured policy

Management and Operations

Agile Operations



DASHBOARD | MAIN DASHBOARD

2 vSmart - 2

21 WAN Edge - 21

2 vBond - 2

1 vManage - 1

Reboot Last 24 hrs 0

Warning	1
Invalid	0

Control Status (Total 21)

Control Up	21
Partial	0
Control Down	0

Site Health (Total 16)

Full WAN Connectivity	12 sites
Partial WAN Connectivity	3 sites
No WAN Connectivity	1 sites

Transport Interface Distribution

< 10 Mbps	40
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Inventory

Total	50
Authorized	42
Deployed	21
Staging	0

WAN Edge Health (Total 21)

Normal	Warning	Error
20	1	0

Transport Health Type: By Jitter

Top Applications

Application-Aware Routing Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
henmolin-vWAN-vEdge21:public-internet-aw...	76.252	0.185	7.642
DataCenter2a:biz-internet-RemoteSite3-4K:p...	76.133	0.184	0.238
DataCenter2a:public-internet-RemoteSite3-4...	77.329	0.184	0.245
RemoteSite2a:biz-internet-RemoteSite3-4K:...	76.958	0.183	0.225
DataCenter1b:public-internet-RemoteSite3-4...	20.371	0.183	0.238

Power Tools

CLI

Linux Shell

REST

NETCONF

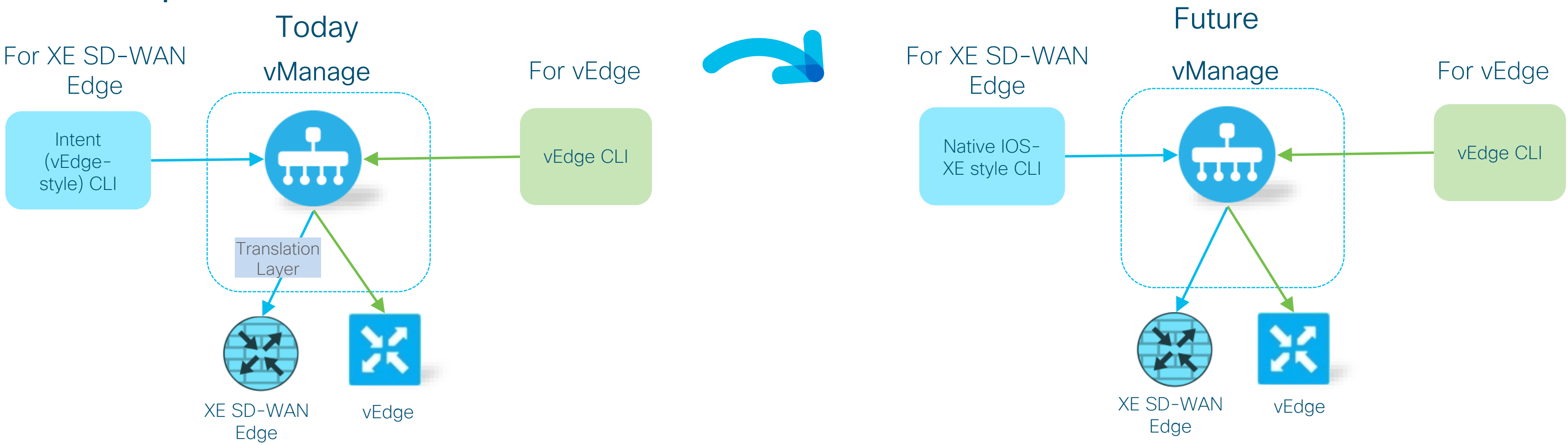
Syslog

SNMP

Flow Export

XE SD-WAN Device Templates

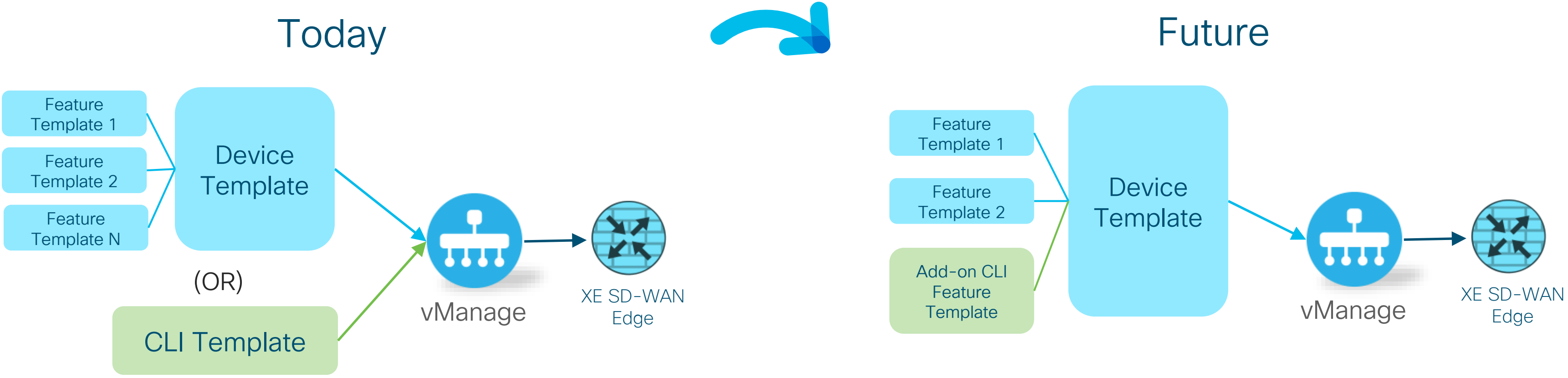
CLI Templates



- Operational Simplicity
- Easier to templatize with uniform CLI
- Use CLI template to configure specific ‘advanced’ knobs/features
- Expose specific IOS-XE capabilities quicker (ex. PPPoE, AA/TACACS)

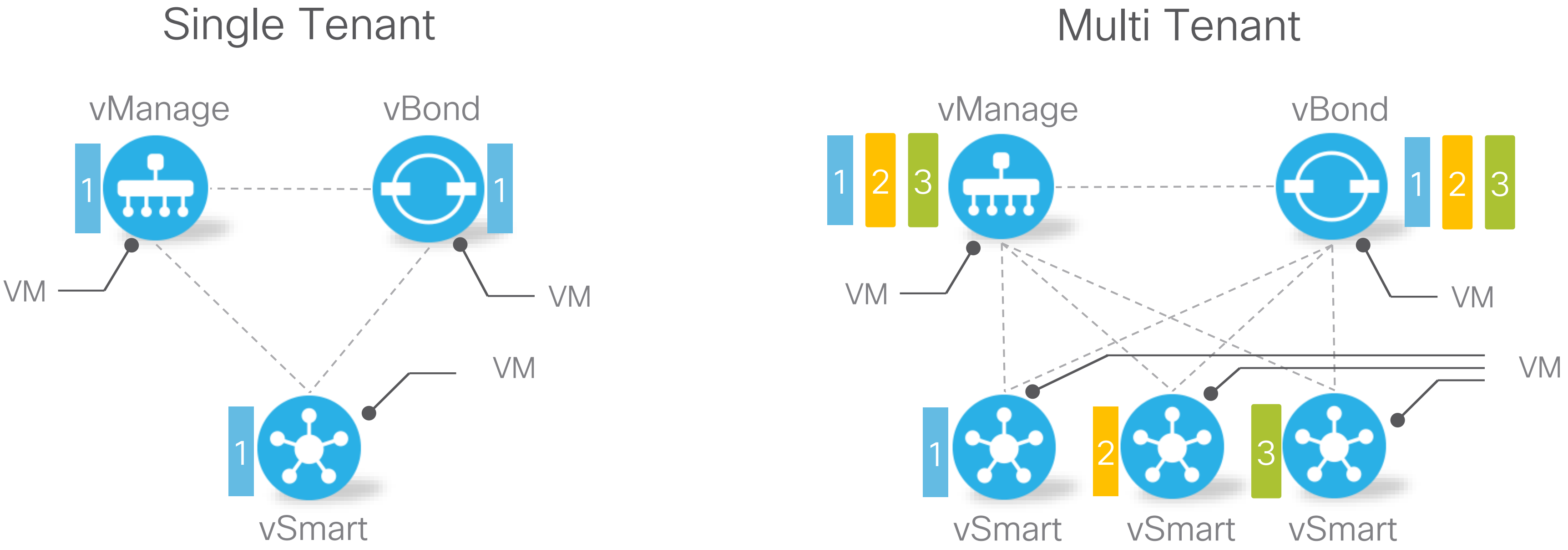
XE SD-WAN Device Templates

Add-on CLI Feature Template



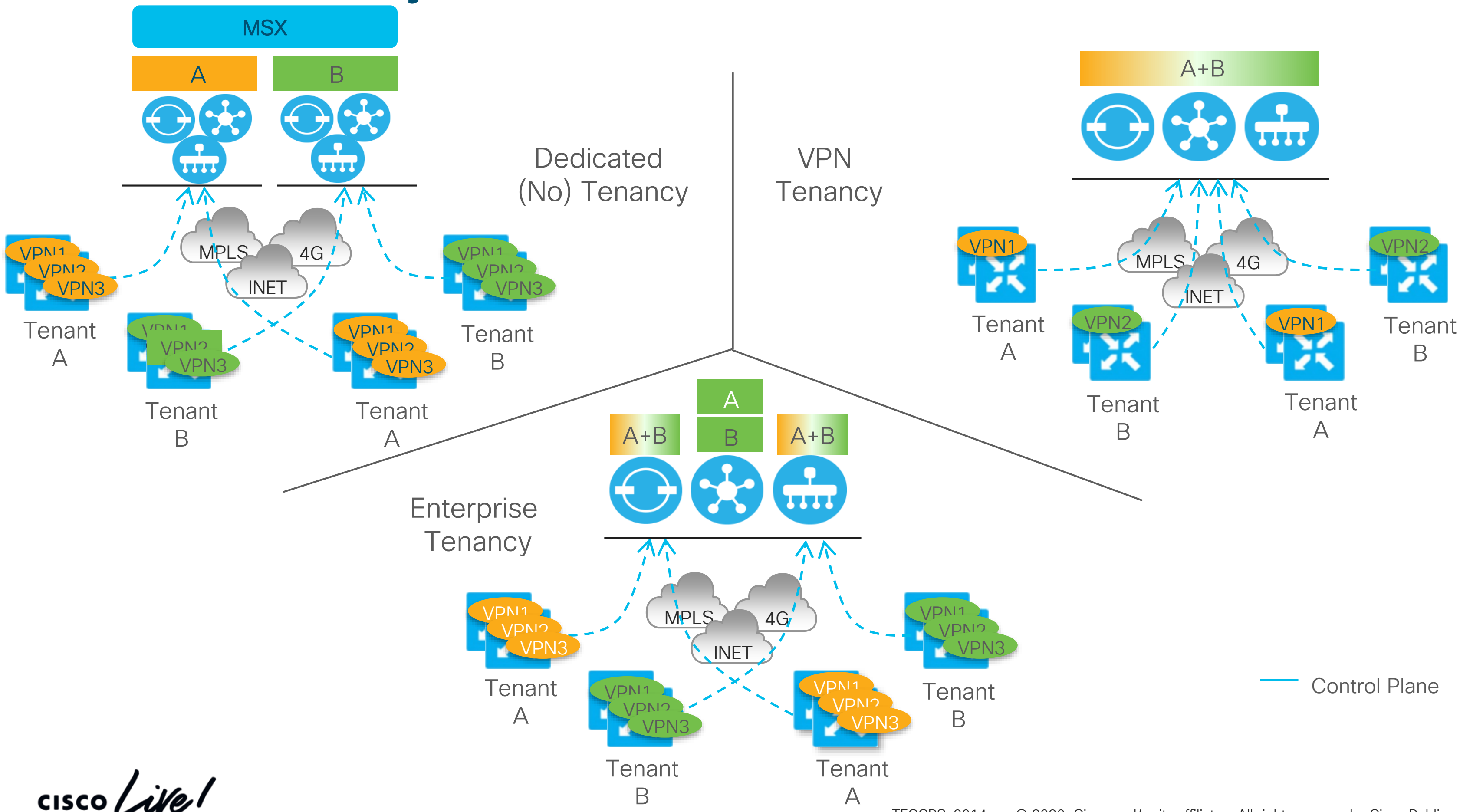
- Allows for Feature and CLI add-on templates to be attached to the same device
- Co-managed use case : Allows end-customer to use feature template and MSP to use CLI template
- Feature templates for majority of config; CLI add-on for additional flexibility and capabilities

Controller Tenancy



AWS, MS-Azure, KVM, ESXi

Multi-tenancy

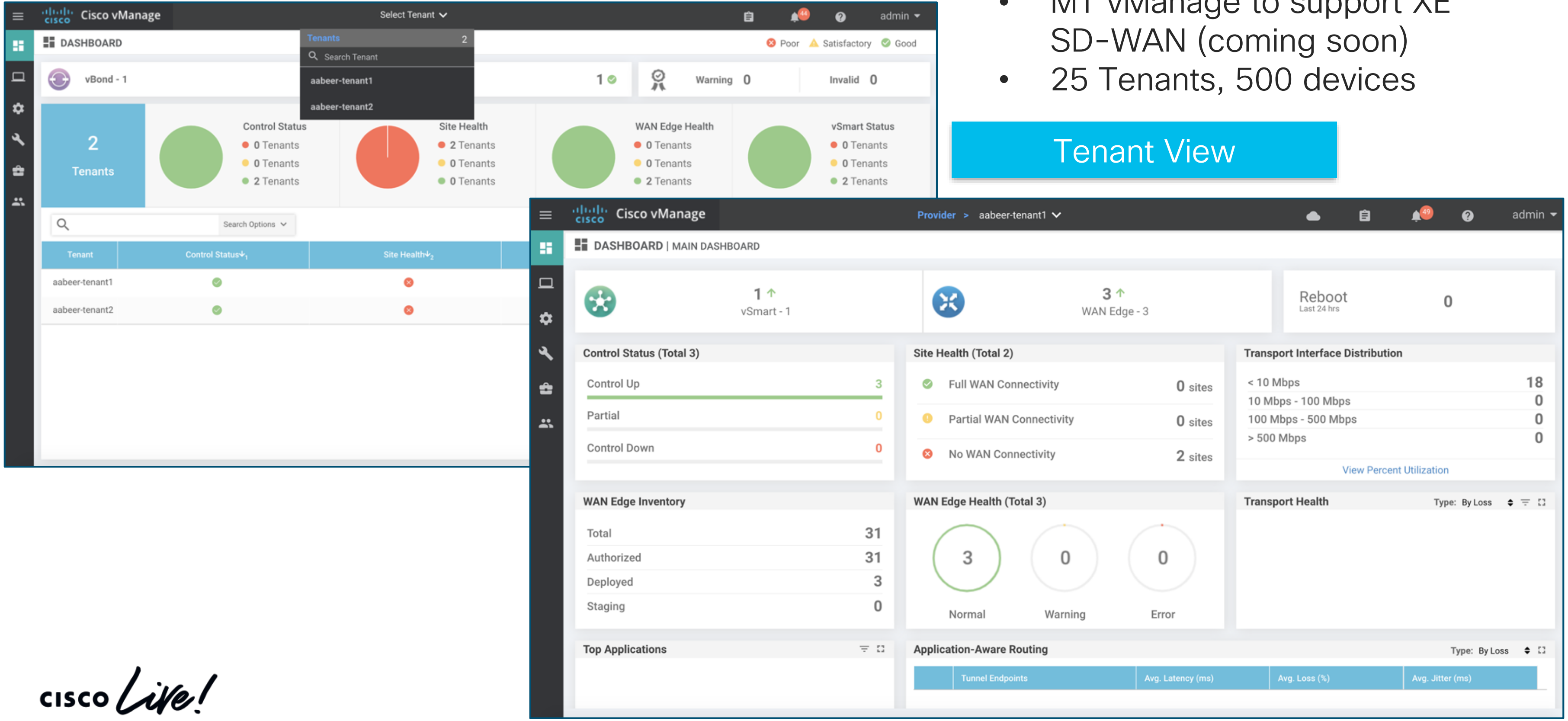


What is vManage Multi-Tenancy ?

- MT vManage to support XE SD-WAN (coming soon)
- 25 Tenants, 500 devices

Provider View

Tenant View



Cisco vManage | Select Tenant | admin

DASHBOARD | ● Poor ▲ Satisfactory ✓ Good

Tenants 2 | Search Tenant | aabeer-tenant1 | aabeer-tenant2

vBond - 1 | 1 ✓ | Warning 0 | Invalid 0

2 Tenants

Control Status	Site Health	WAN Edge Health	vSmart Status
0 Tenants	2 Tenants	0 Tenants	0 Tenants
0 Tenants	0 Tenants	0 Tenants	0 Tenants
2 Tenants	0 Tenants	2 Tenants	2 Tenants

Search Options

Tenant	Control Status	Site Health
aabeer-tenant1	✓	✗
aabeer-tenant2	✓	✗

Cisco vManage | Provider > aabeer-tenant1 | admin

DASHBOARD | MAIN DASHBOARD

1 ↑ vSmart - 1 | 3 ↑ WAN Edge - 3 | Reboot Last 24 hrs 0

Control Status (Total 3)

Control Up	3
Partial	0
Control Down	0

Site Health (Total 2)

Full WAN Connectivity	0 sites
Partial WAN Connectivity	0 sites
No WAN Connectivity	2 sites

Transport Interface Distribution

< 10 Mbps	18
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Inventory

Total	31
Authorized	31
Deployed	3
Staging	0

WAN Edge Health (Total 3)

Normal	Warning	Error
3	0	0

Transport Health | Type: By Loss

Top Applications

Application-Aware Routing | Type: By Loss

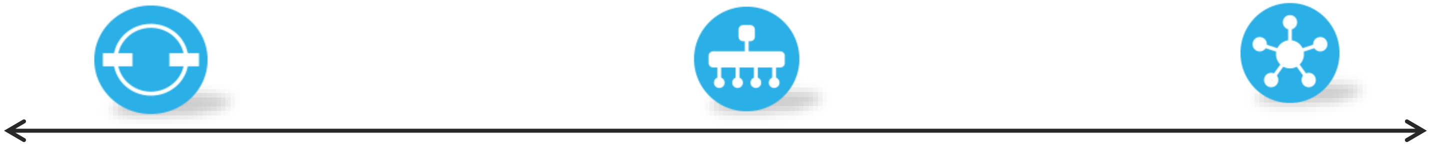
Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)

Horizontal Solution Scale

Orchestration Plane
(vBond)

Management Plane
(Multi-tenant or Dedicated)
(vManage)

Control Plane
(VMs)
(vSmart)

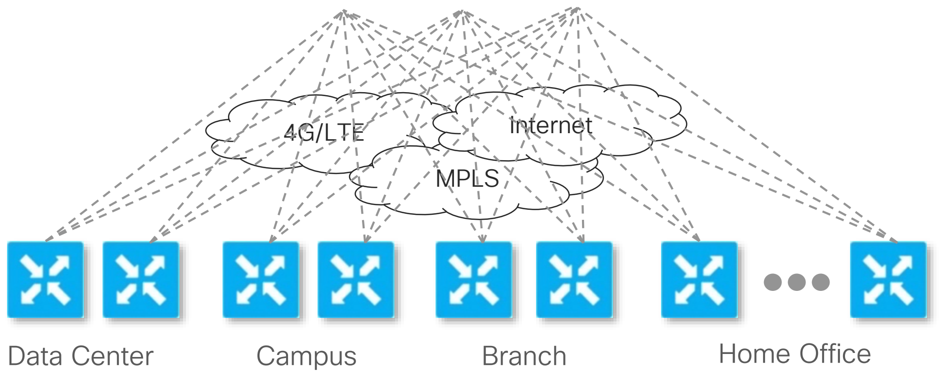


Horizontal Scale Out Model

Add vBond Orchestrators to increase WAN Edge bring-up capacity

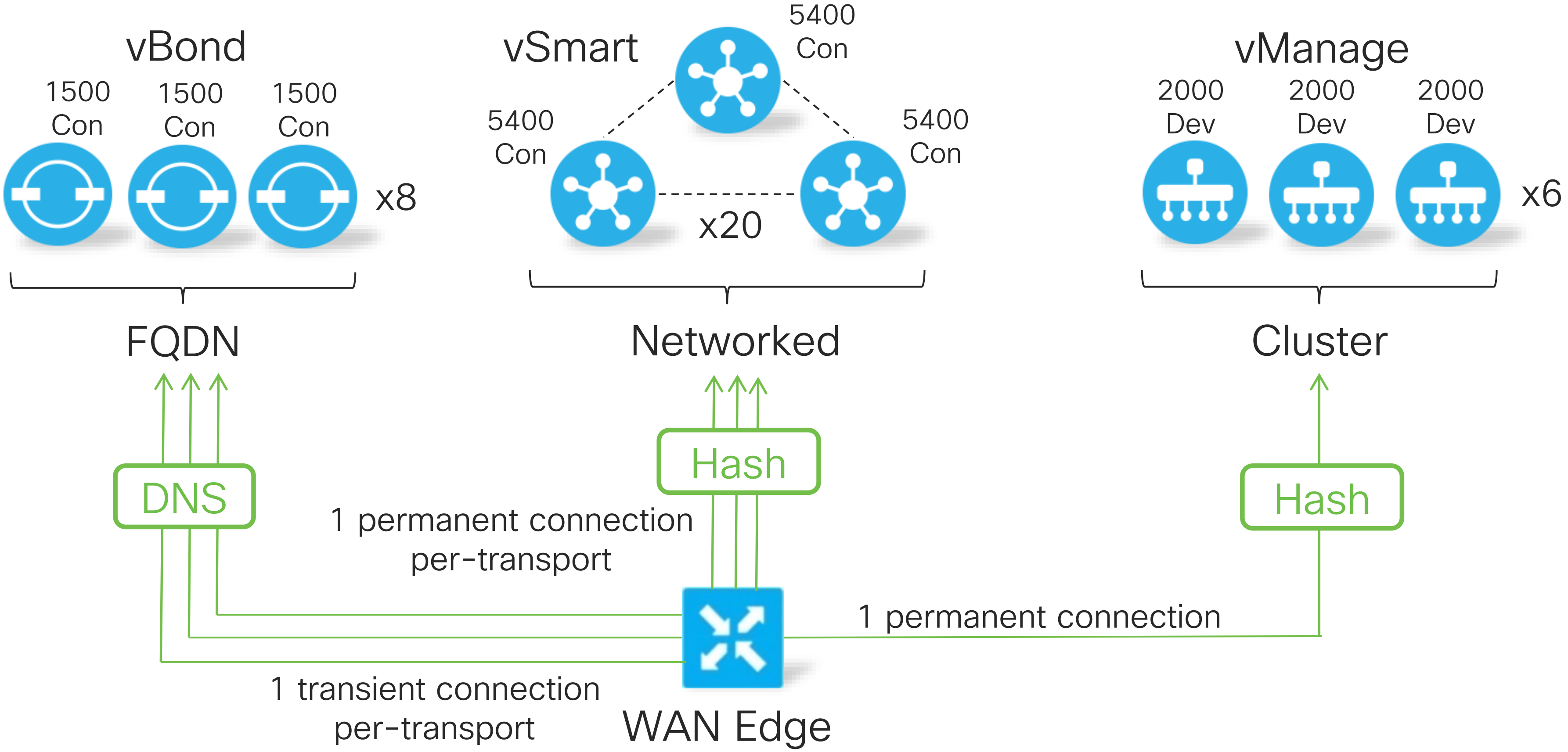
Create vManage cluster to accommodate more WAN Edge routers

Add vSmart Controllers for more control plane capacity

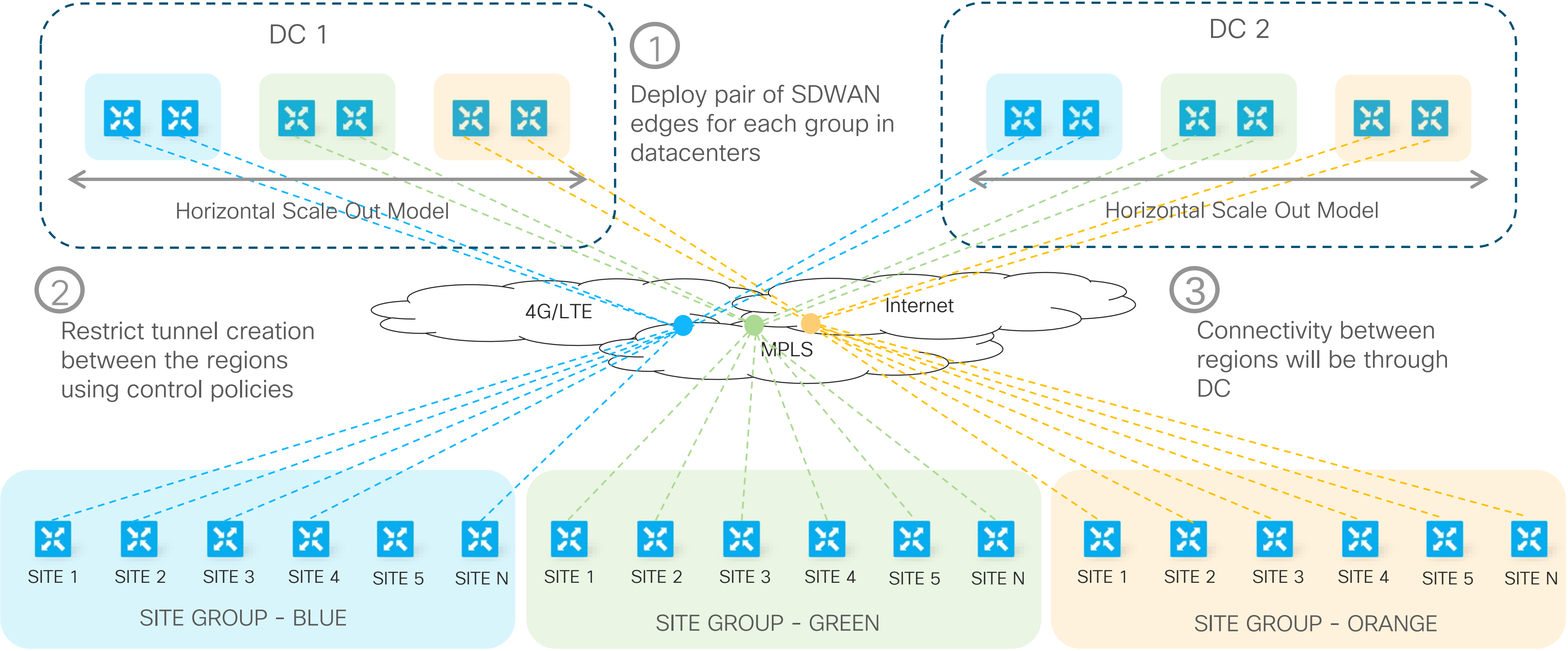


- Choose WAN Edge platform with appropriate IPSec tunnel scale
- Use control policies to define VPN topologies

Horizontal Solution Scale – Control Plane



Horizontal Solution Scale - Data Plane



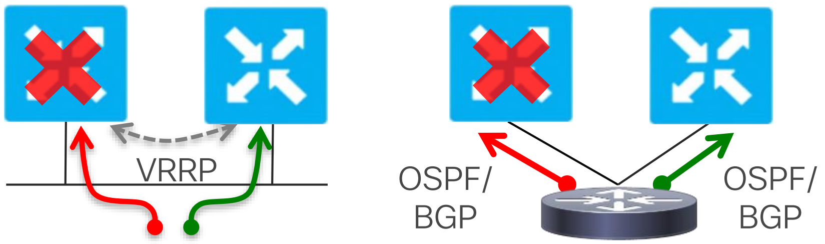
1 Deploy pair of SDWAN edges for each group in datacenters

2 Restrict tunnel creation between the regions using control policies

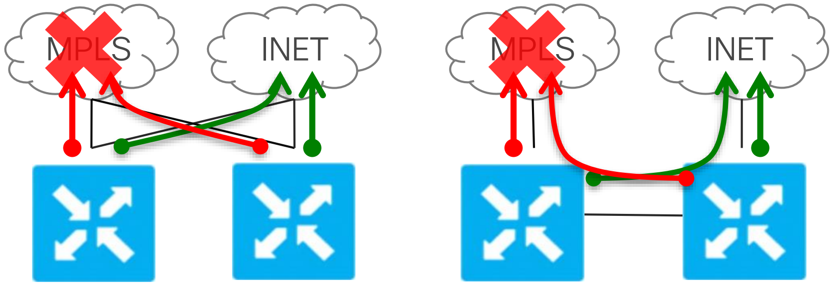
3 Connectivity between regions will be through DC

High Availability and Redundancy Overview

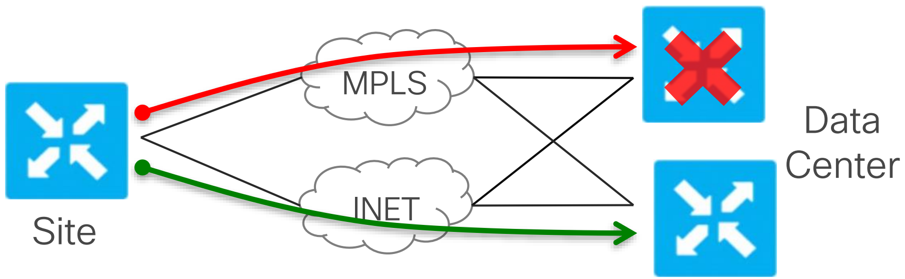
Site Redundancy



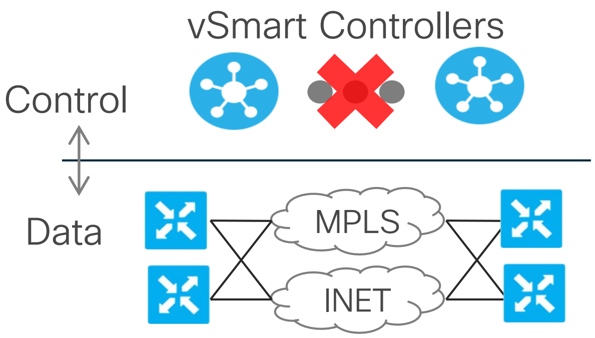
Transport Redundancy



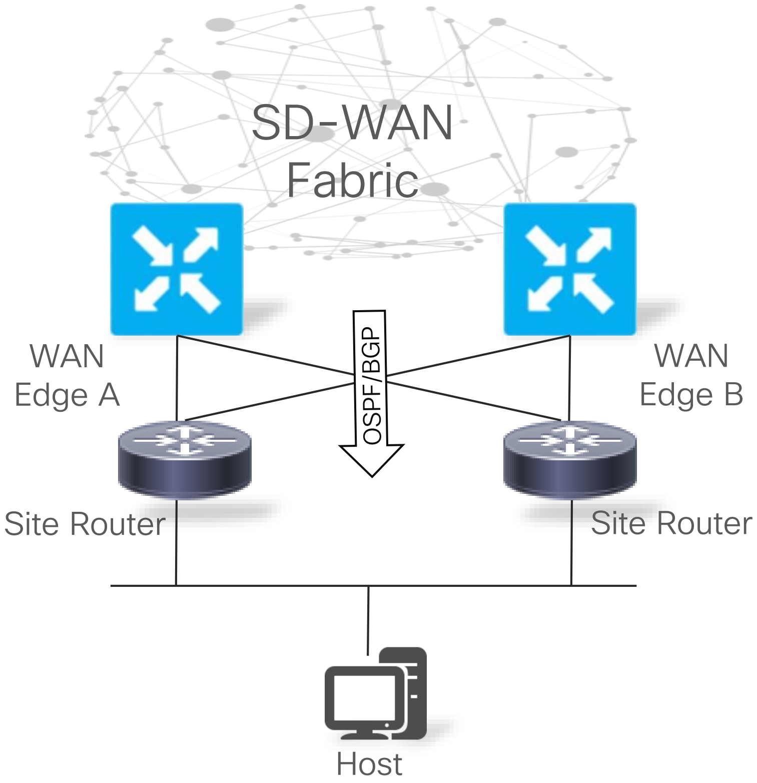
Network/Headend Redundancy



Control Redundancy

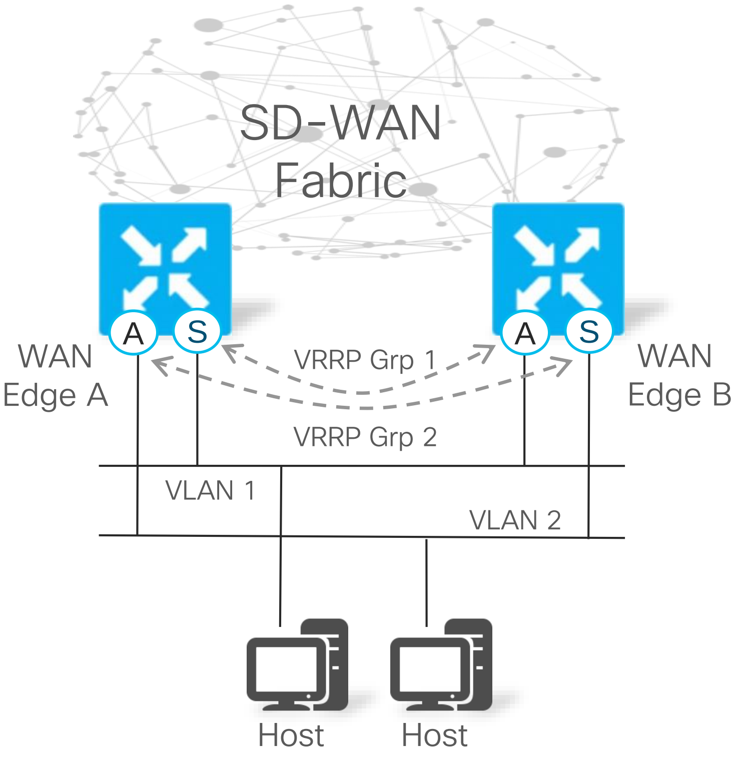


Redundancy - Site with LAN Routing



- Redundant WAN Edge routers
- OSPF/BGP between WAN Edge routers and site router(s)
- Bi-directional redistribution between OMP and OSPF/BGP
  - Loop prevention
- Multipathing for remote destinations across SD-WAN Fabric
  - Can manipulate OSPF/BGP to prefer one WAN Edge router over the other

Redundancy - Site with LAN Bridging



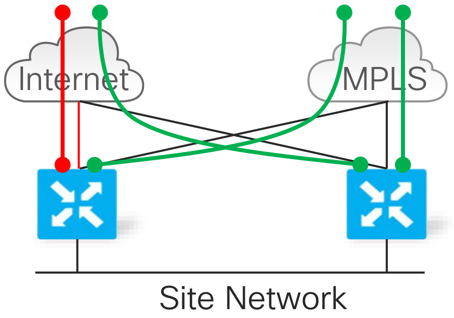
- Redundant WAN Edge routers
- VRRP between WAN Edge routers
  - Operates per-VLAN
- VRRP Active WAN Edge router responds to ARP requests for the virtual IP and virtual MAC*
- Prior to 18.3.0
  - New VRRP Active WAN Edge (vEdge) router sends out gratuitous ARP

* Virtual MAC requires minimum 18.3.0 code on vEdge

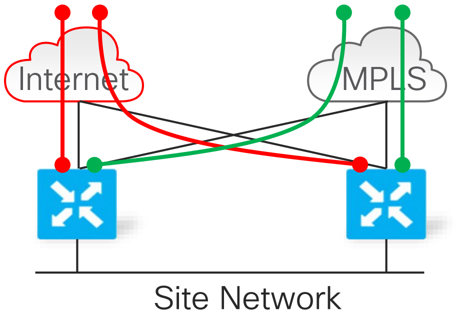
Redundancy - Meshed Transports

- WAN Edge routers are directly connected to all the transports
- SD-WAN tunnels are built through all directly connected transports

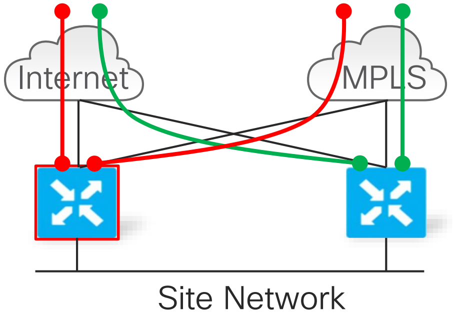
Circuit Failure



Transport Failure



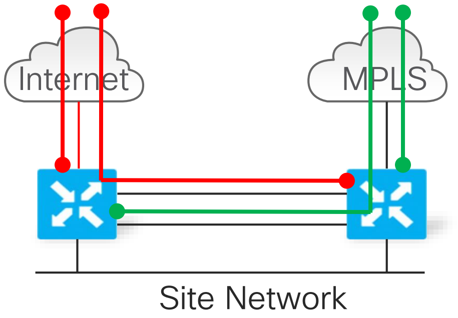
Router Failure



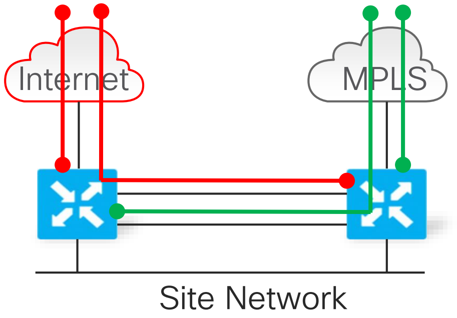
Redundancy – Extended Transports

- Each WAN Edge router is connected to a given transports
- SD-WAN tunnels are built through local and remote transports

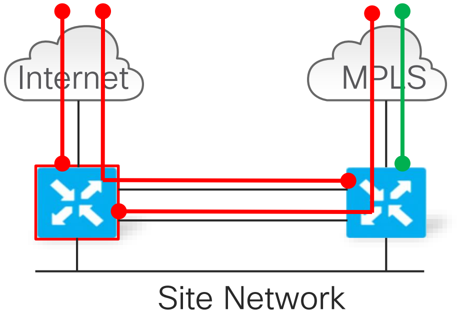
Circuit Failure



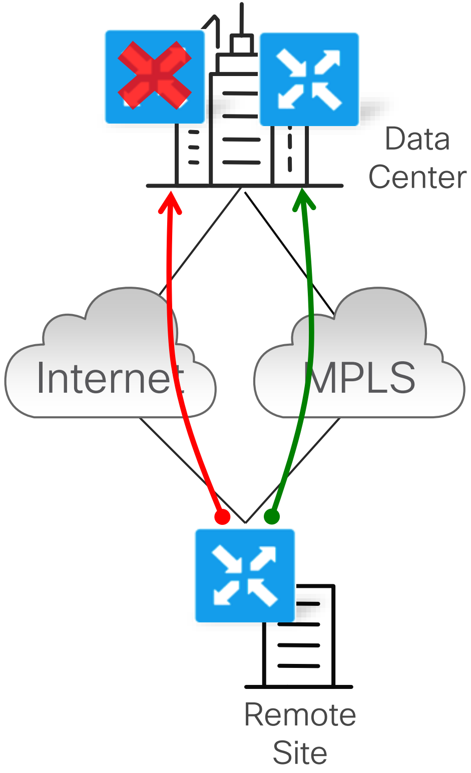
Transport Failure



Router Failure

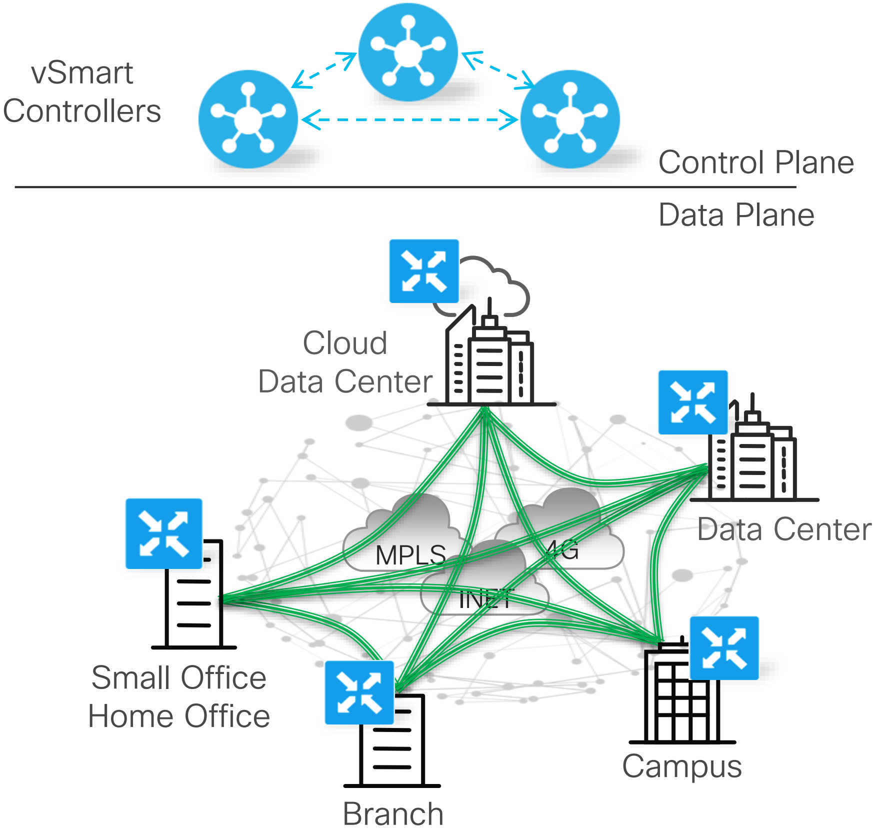


Redundancy – Path and Headend



- WAN Edge routers leverage BFD for detecting end-to-end tunnel liveliness
- Intermediate network path failures or remote-end WAN Edge failures can be detected
- Traffic will be rerouted after the failed condition had been detected
  - BFD timers can be tweaked for faster detection

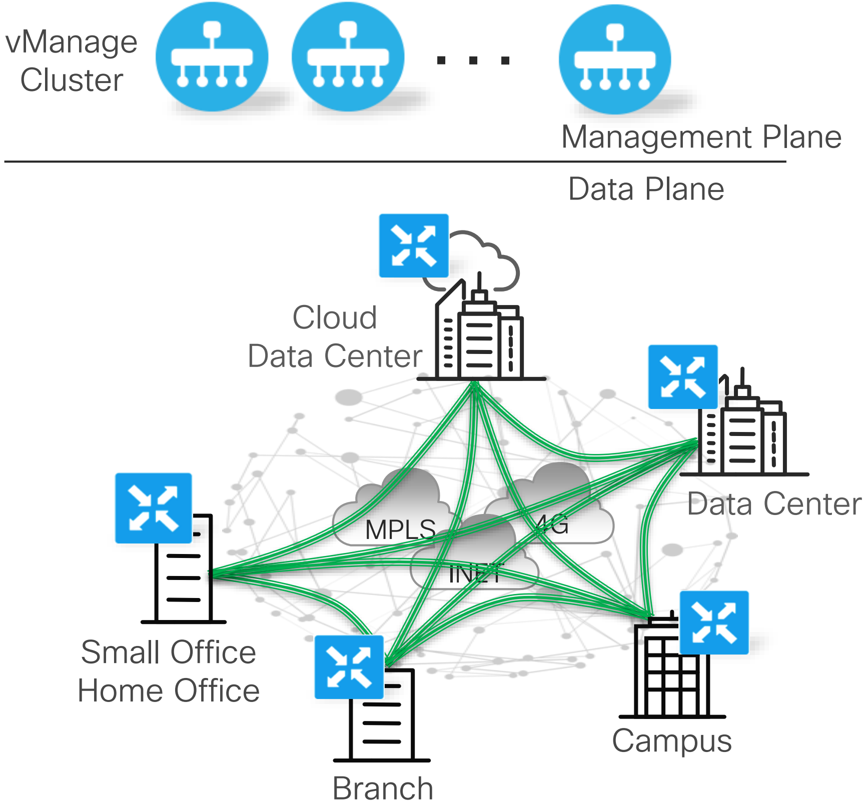
Redundancy – vSmart Control Controllers



- vSmart controllers exchange OMP messages and they have identical view of the SD-WAN fabric
- No impact as long as WAN Edge routers can connect to at least one vSmart Controller
- If all vSmart controllers fail or become unreachable, WAN Edge routers will continue operating on a last known good state for a configurable amount of time
  - No changes allowed

Redundancy – vManage

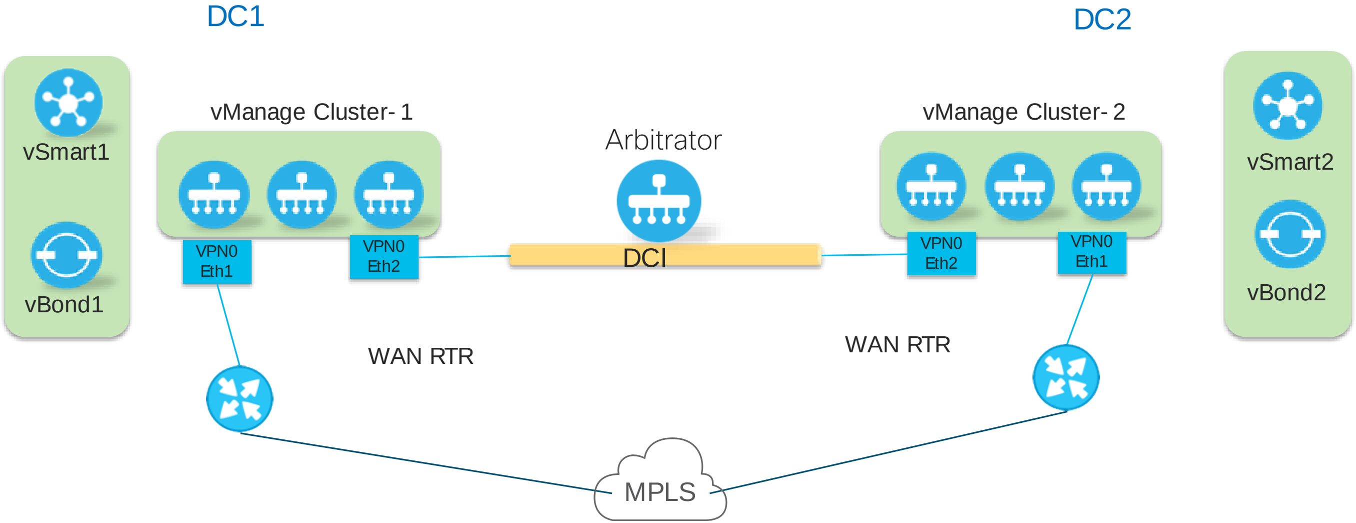
Clustering



- 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
- Loss of all vManage servers has no impact on fabric operation
  - No administrative changes
  - No statistics collection

Redundancy - vManage

Auto Disaster Recovery



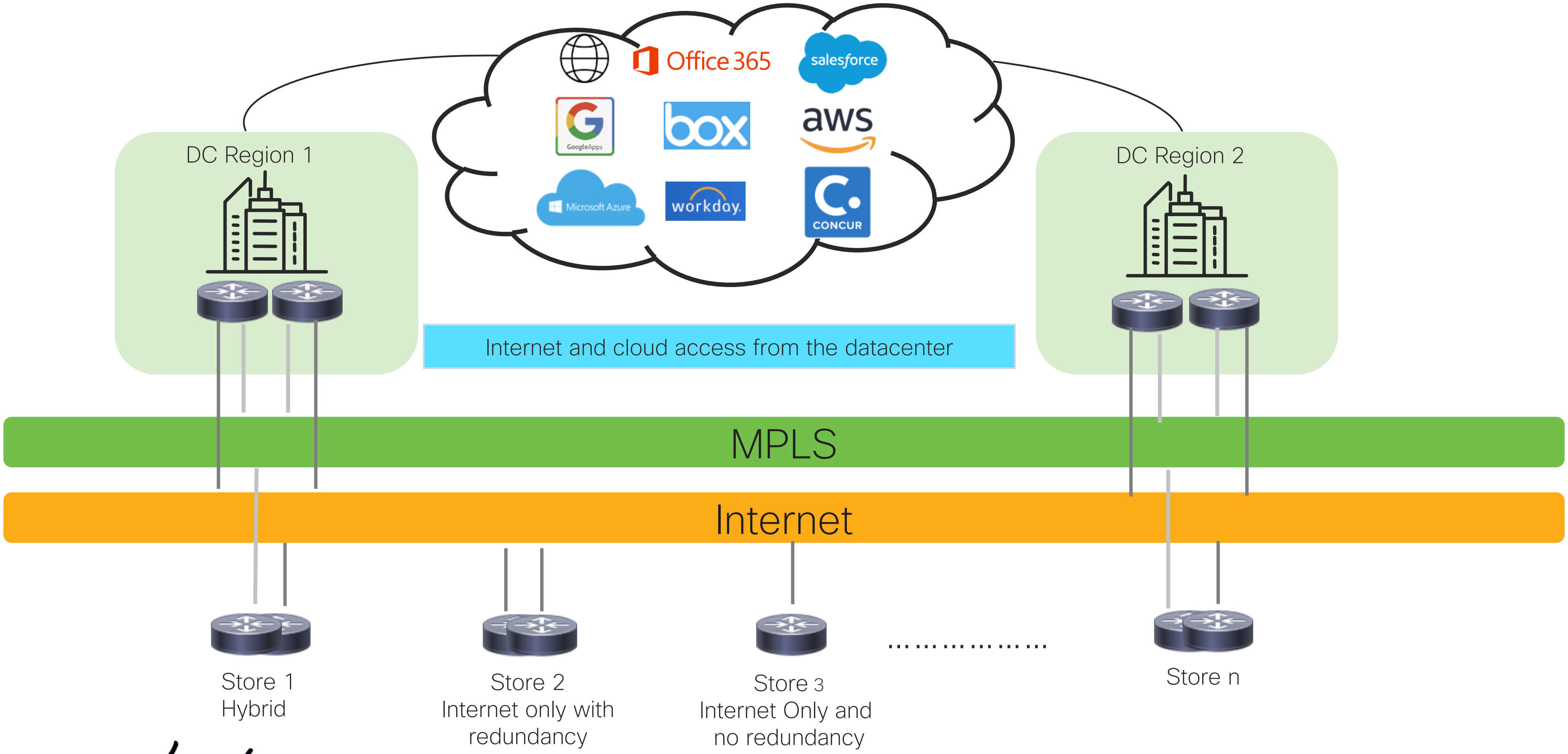
- Stateful replication of database from active to standby cluster
- Arbitrator cluster
  - Tracks health state of the cluster
  - Avoids split-brain scenarios
  - Triggers activation of secondary cluster in case of disaster
  - Edge devices to vManage reachability is not considered for vManage failover

- No configuration changes are needed on edge devices on failover
- Arbitrator and cluster members need IP connectivity between each other
- All communication between clusters will utilize DC backbone/interconnect

Customer Deployment

Use Case: Retail

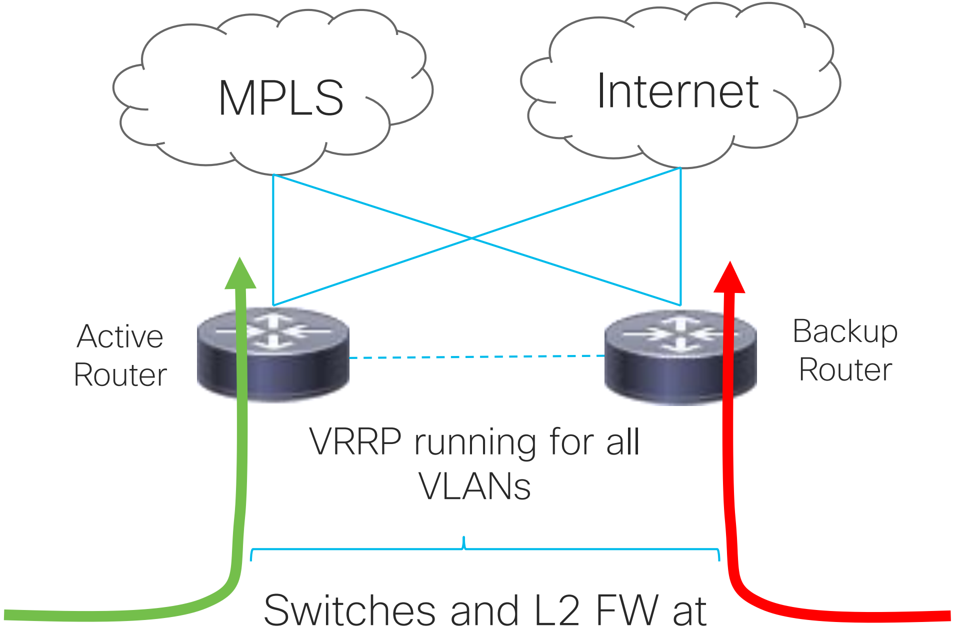
Legacy Design



Current Design For Remote Sites

VLANs

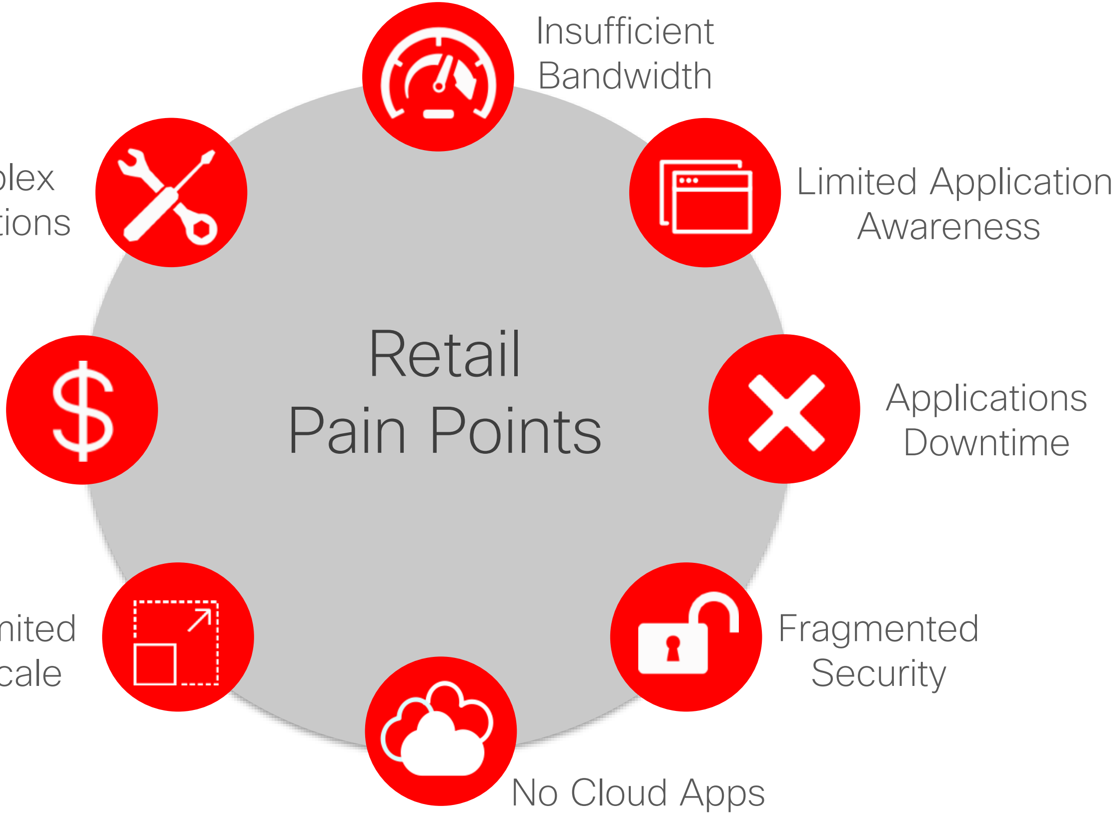
PCI
Voice
Guest Wireless
Corporate Wireless
Management
Internet Access – Guest
Internet Access – Employees
Vendor/Partner Connectivity



VRRP running for all VLANs

Switches and L2 FW at each remote location on the LAN side

Pain Points


Insufficient Bandwidth
Limited Application Awareness
Applications Downtime
Fragmented Security
No Cloud Apps Readiness
Limited Scale
High Cost
Complex Operations
Retail Pain Points

Retail Deployment – Use Cases

SCALE

Controller Deployment

aws

Microsoft Azure

Controllers are mostly in cloud

Seamless Migration

Multi Segment Overlay

Back Office

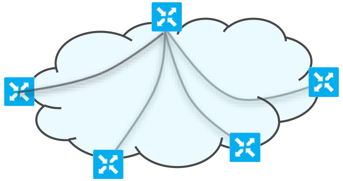
WiFi

Point of Sales

Voice

Management Network

Topology

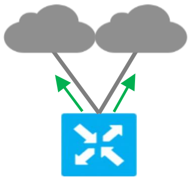


Hub and Spoke Topology

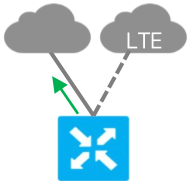
Secure Internet Access

Secure
Internet Gateway
Your secure onramp to the internet, anywhere users go

Redundancy



Dual Homed

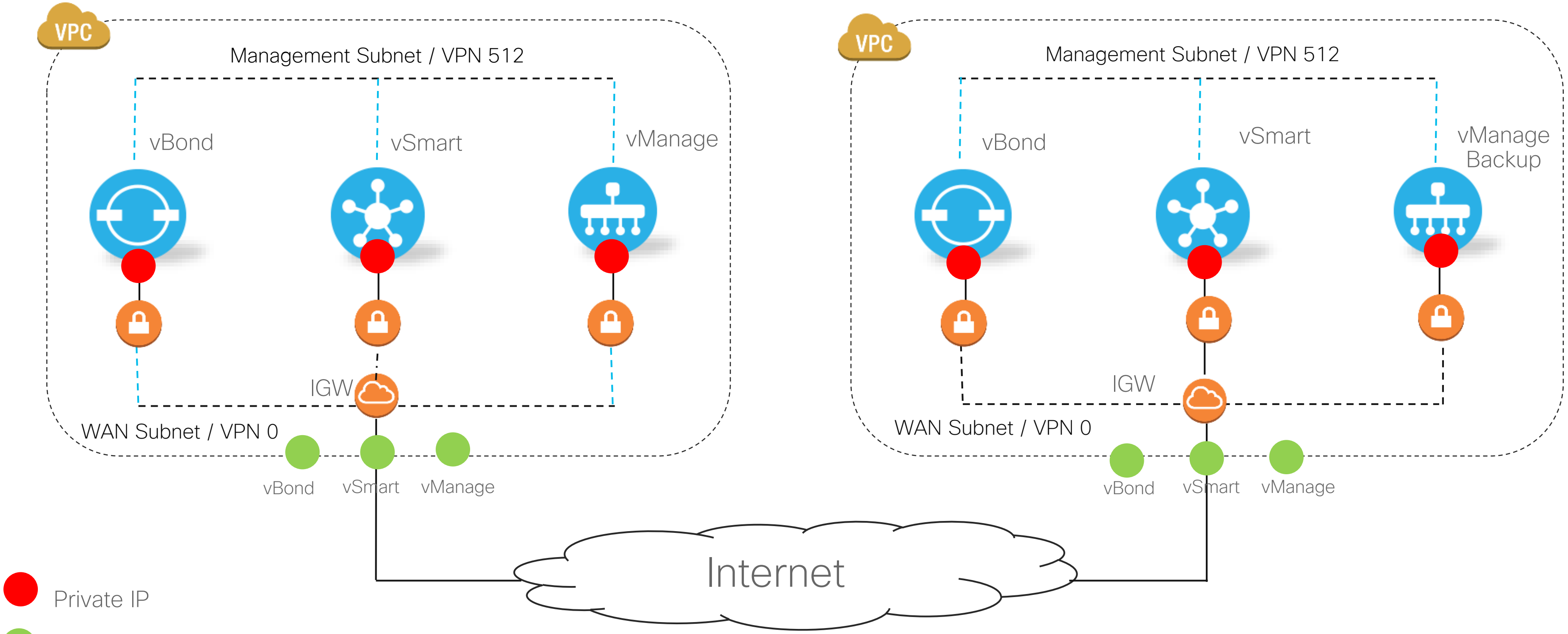


Single Home
with LTE backup

TIME TO MARKET

Controller Deployment

Controller Deployment in AWS

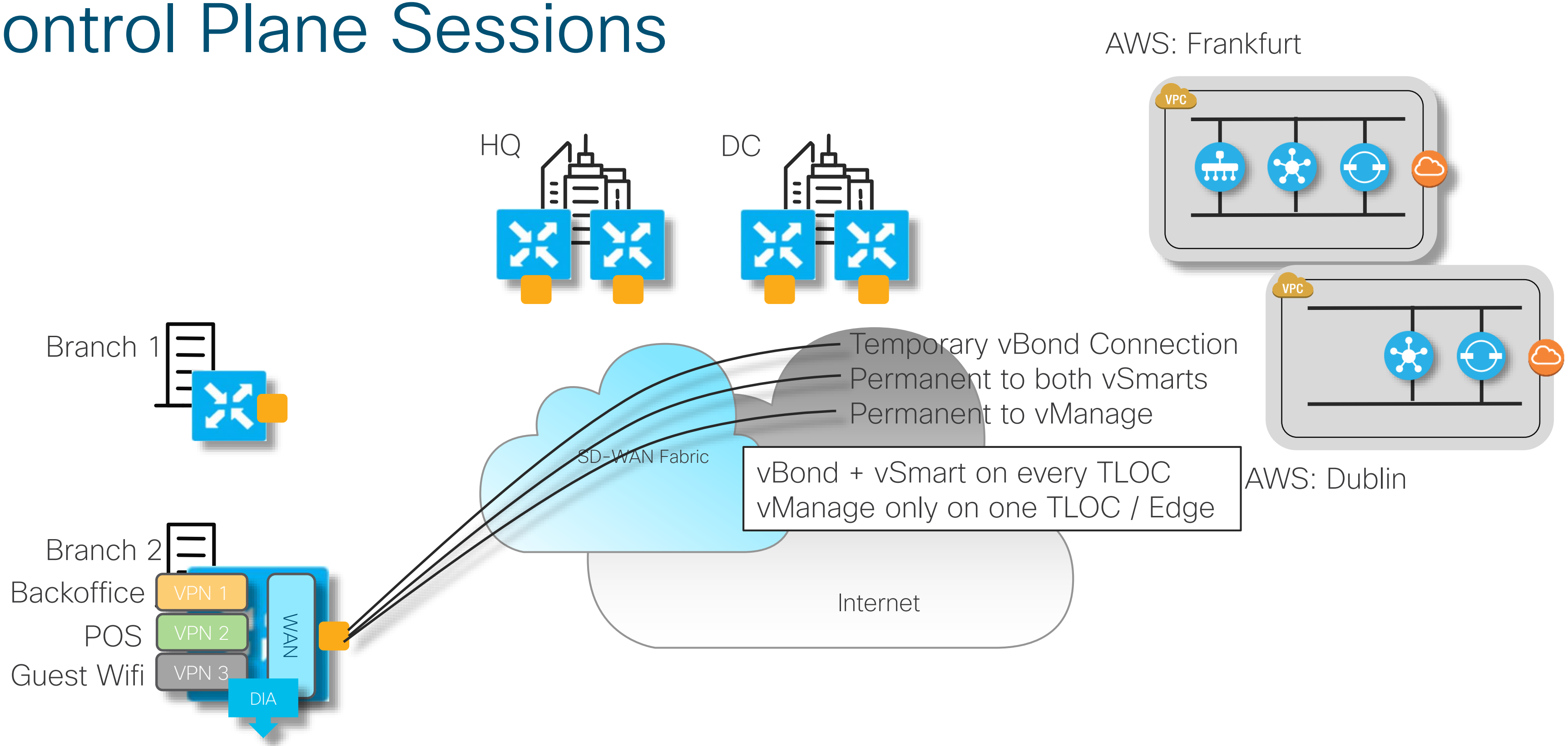


🔴 Private IP

🟢 Elastic IP

vManage/vSmart are configured with elastic IP of vBond to force communication to pass though IGW (recording Private/Public)

Control Plane Sessions



Temporary vBond Connection
Permanent to both vSmarts
Permanent to vManage

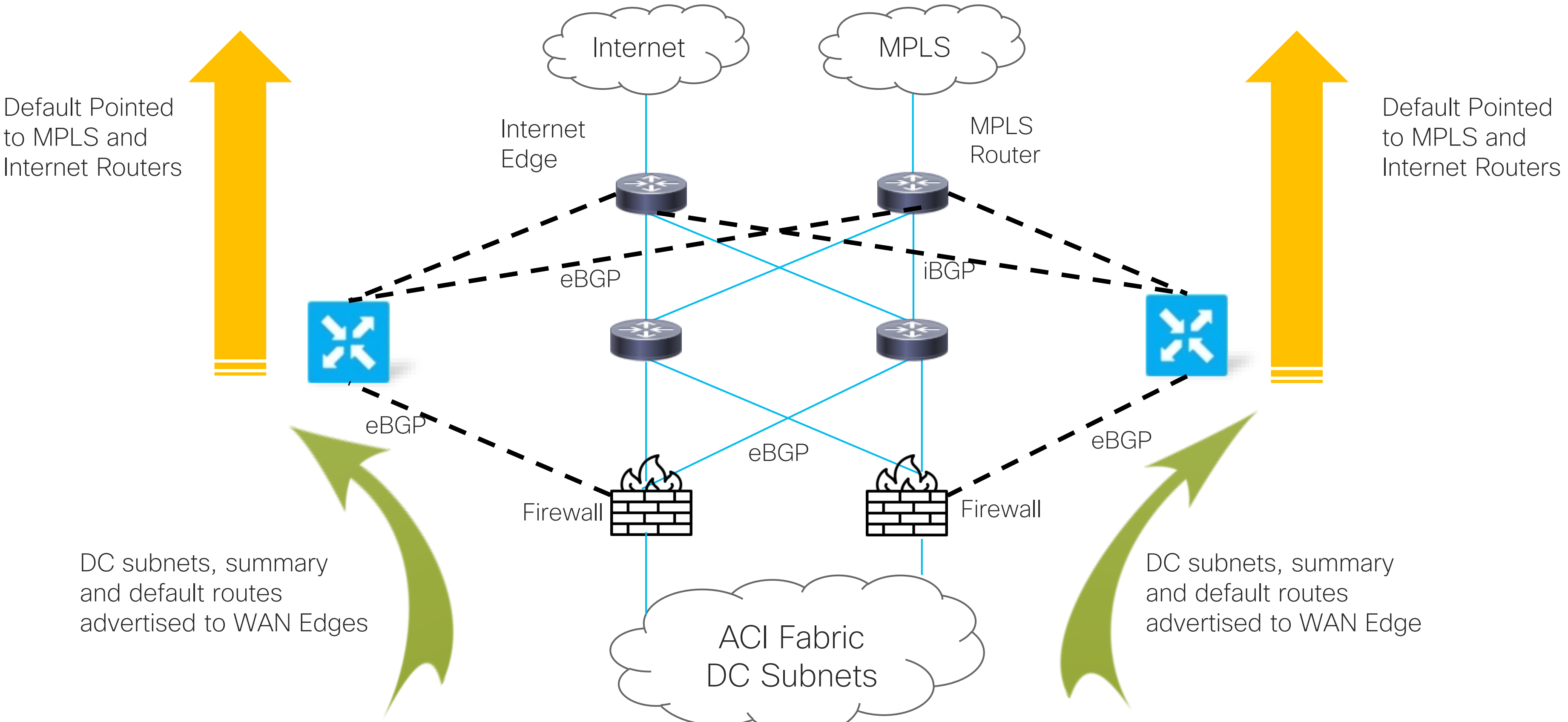
vBond + vSmart on every TLOC
vManage only on one TLOC / Edge

🟧 TLOC – Color public-internet

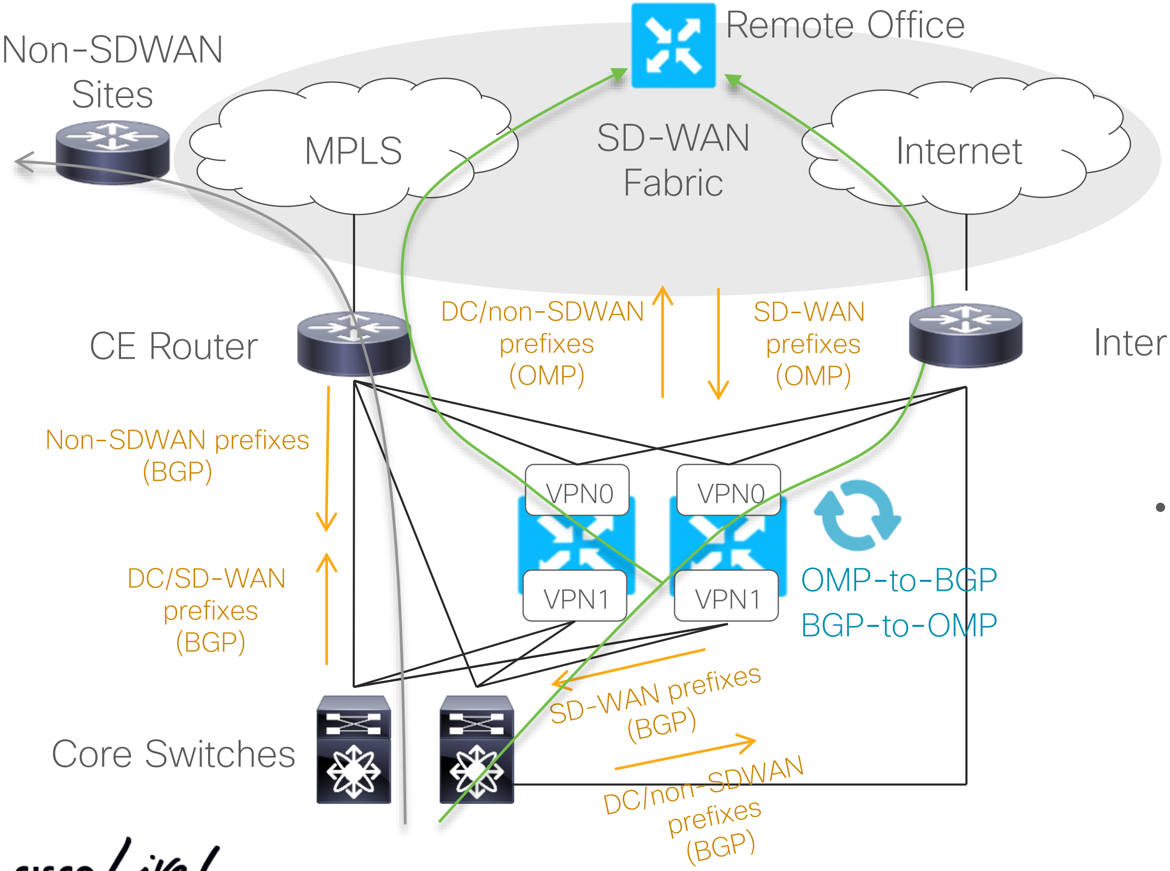
*HQ/DC/Main sites have default fully meshed data plane
All sites have control plane session with both AZ's

Seamless Migration

Datacenter Migration


Internet
MPLS
Internet Edge
MPLS Router
Default Pointed to MPLS and Internet Routers
Default Pointed to MPLS and Internet Routers
eBGP
iBGP
eBGP
eBGP
eBGP
Firewall
Firewall
DC subnets, summary and default routes advertised to WAN Edges
DC subnets, summary and default routes advertised to WAN Edge
ACI Fabric
DC Subnets

Data Center Overlay/Underlay Interoperability



- SD-WAN to non-SDWAN interoperability

Multi-Segment Overlay

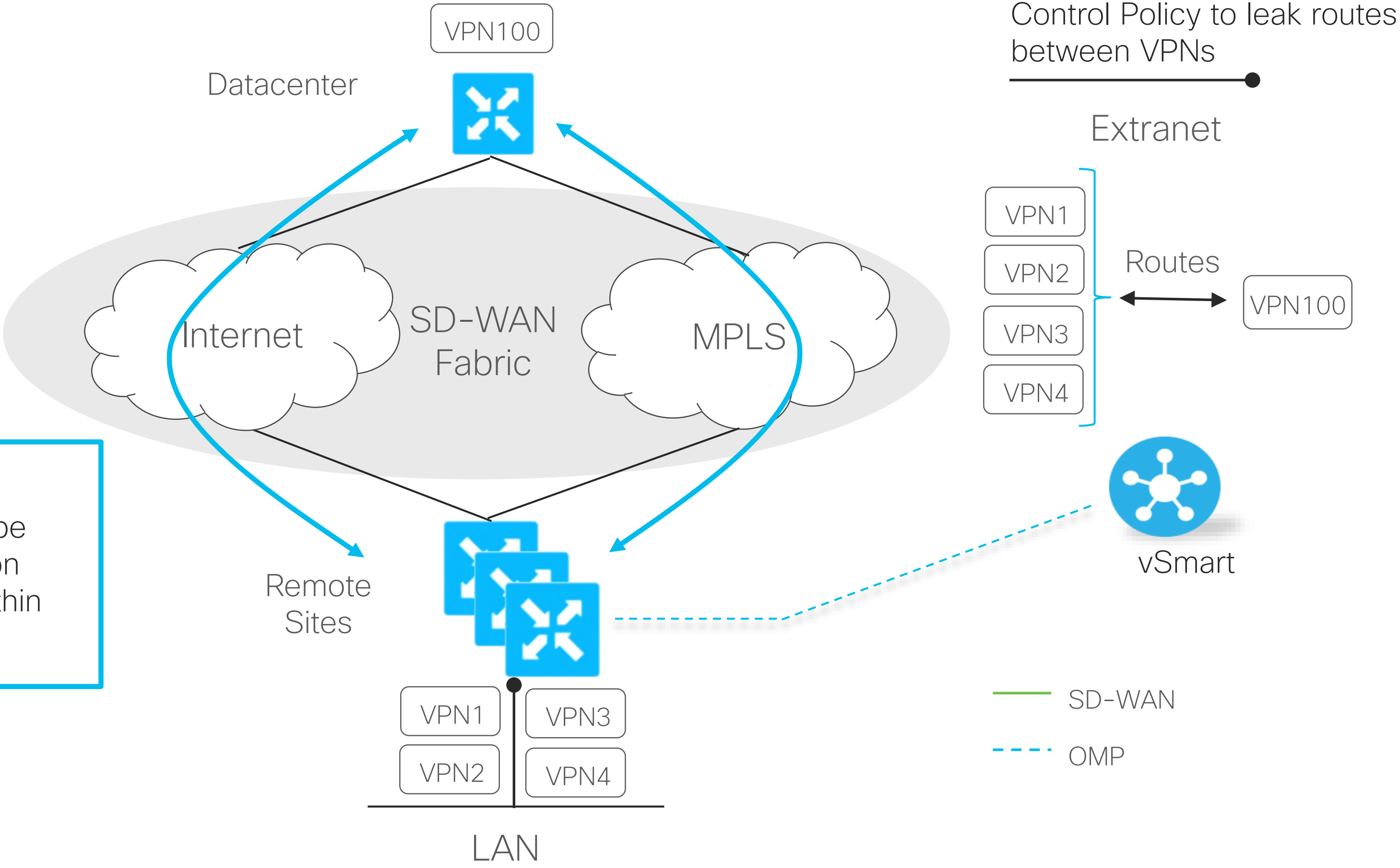
Segmentation vs Current Design

- Typically they have a single VRF in the MPLS
- Different VLANs for different users/applications
- Security enforced by using ACLs and firewall policies
- Datacenters subnets are typically shared amongst the VLANs

So its likely………

Legacy design does not have any segmentation while with SD-WAN, you are likely to introduce it

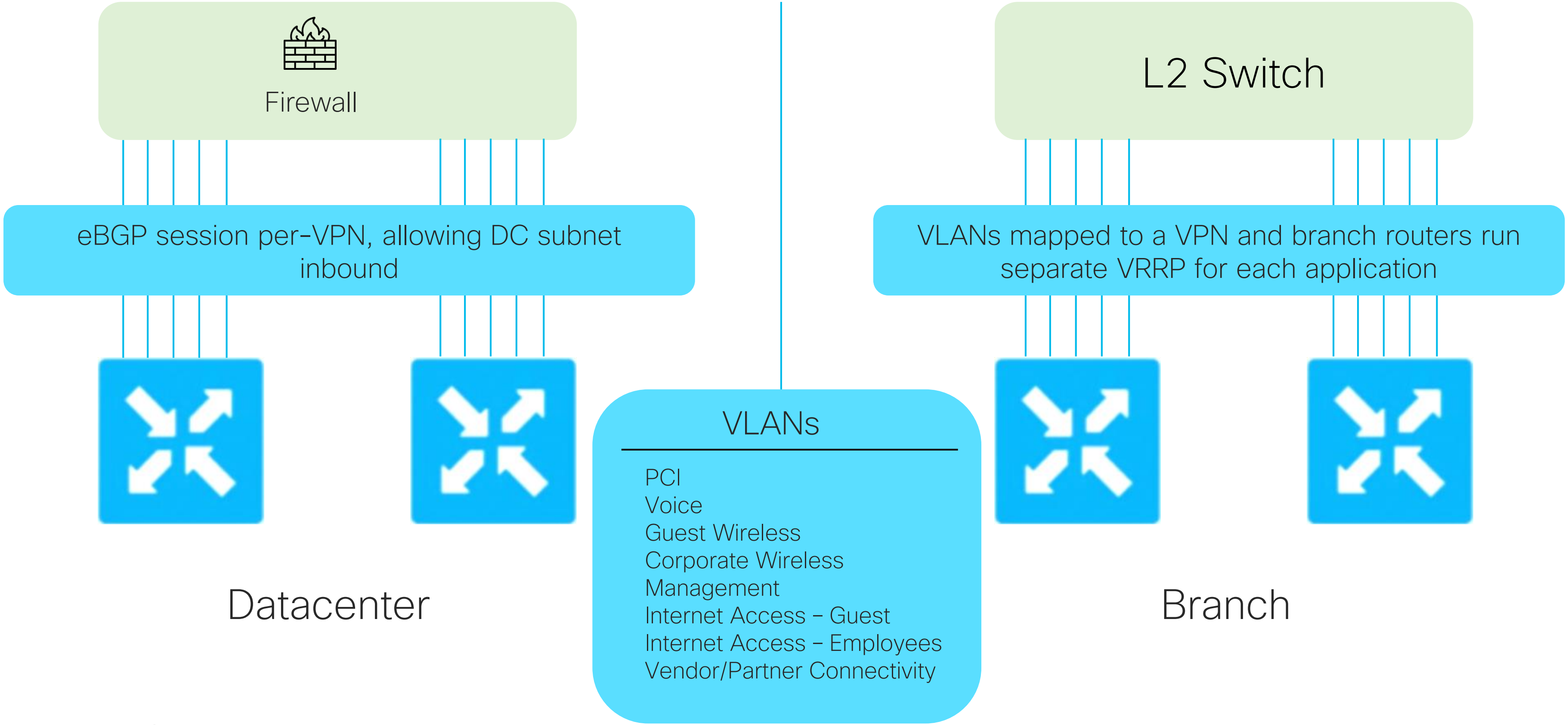
Option1: Extranet



Issue with Extranet

Design change would be required if segmentation must be introduced within the DC in the future

Option2: 1 to 1 VPN Mapping



Firewall

eBGP session per-VPN, allowing DC subnet inbound

Datacenter

L2 Switch

VLANs mapped to a VPN and branch routers run separate VRRP for each application

Branch

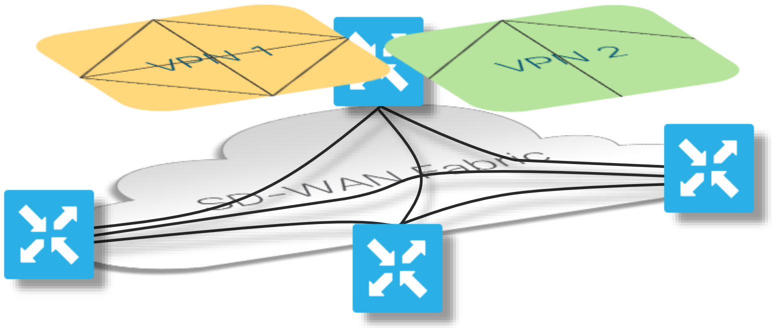
VLANs

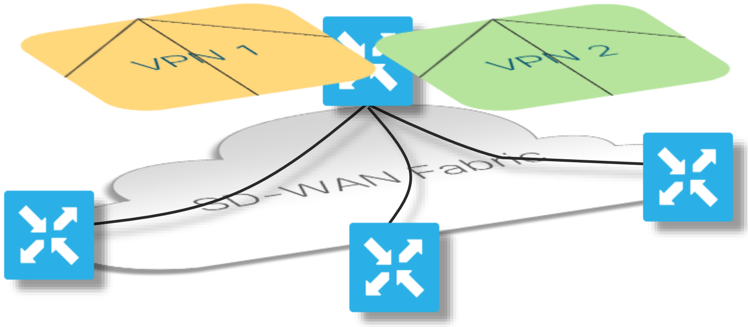
- PCI
- Voice
- Guest Wireless
- Corporate Wireless
- Management
- Internet Access – Guest
- Internet Access – Employees
- Vendor/Partner Connectivity

Hub and Spoke Topology

Hub and Spoke Topology

Data Plane or Individual VPNs subject to specific topologies / connectivity models



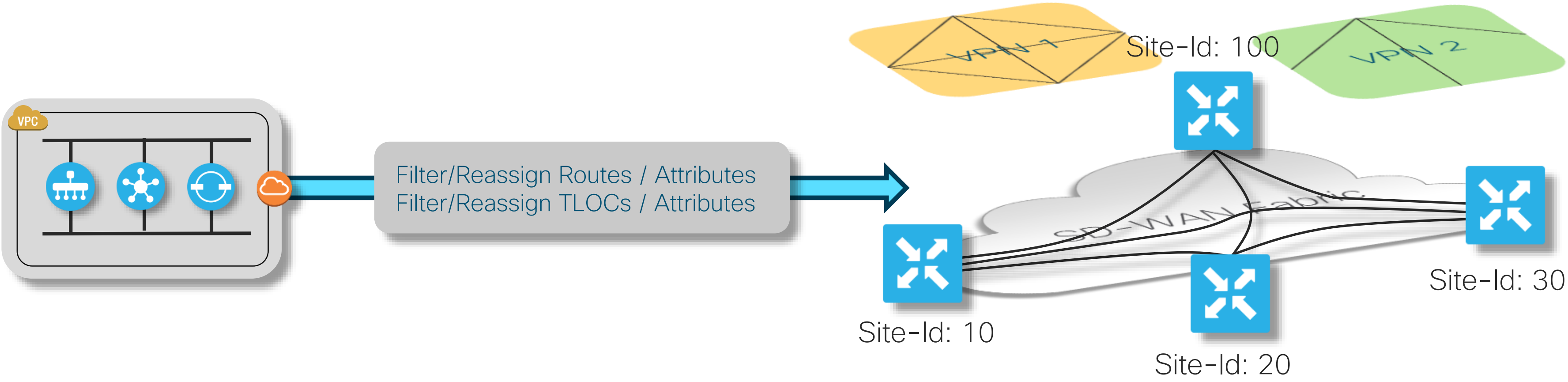


- Fully meshed fabric data plane is by default
- Can be overkill as the use case for spoke to spoke connectivity is limited

- Hub and spoke topology can be achieved using control policies
- Data plane is horizontally scalable by adding more SDWAN edges in the DC

Hub and Spoke Topology

Data Plane or Individual VPNs subject to specific topologies / connectivity models



Control Policy used for Topology Creation

Data Plane and VPN Hub-and-Spoke Topologies

```
Policy
 lists
  tloc-list hub-site_tlocs
   tloc 1.1.1.1 color red encap ipsec preference 100
   tloc 2.2.2.2 color red encap ipsec preference 100
   tloc 3.3.3.3 color red encap ipsec
  !
  site-list branch_sites
   site-id 1000-2000
  !
  site-list hub_sites
   site-id 1-100
  !
 !
```

```
apply-policy
 site-list branch_sites
  control-policy restricted_data_plane out
 !
!
```

```
Policy
 control-policy restricted_data_plane
  sequence 10
   match tloc
    site-list hub_sites
   !
   action accept
   !
  !
  sequence 20
   match route
    site-list branch_sites
   !
   action accept
    set
     tloc-list hub_site_tlocs
    !
   !
  !
  sequence 30
   match tloc
   !
   action reject
   !
  !
  default-action accept
```

Control Policy used for Topology Creation

VPN 1 Full Mesh and VPN 2 Hub-and-Spoke Topologies

Loose Hub-and-Spoke
Spokes communicate via hub(s)

```
Policy
 lists
  vpn-list VPN2
   vpn 2
  !
site-list branch_sites
  site-id 100-200
  !
 !
 control-policy vpn_multi-topology
  sequence 10
   match route
    site-list branch_sites
    vpn-list  VPN2
   !
   action accept
    set
     tloc 1.1.1.1 color red
    !
   !
  !
  default-action accept
```

Strict Hub-and-Spoke
No spoke to spoke communication

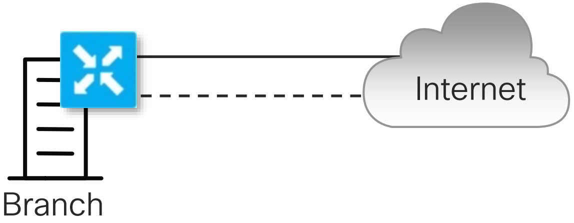
```
Policy
 lists
  vpn-list VPN2
   vpn 2
  !
site-list hub_sites
  site-id 1-2
  !
 !
 control-policy vpn_multi-topology
  sequence 10
   match route
    site-list hub_sites
    vpn-list  VPN2
   !
   action accept
  !
  sequence 20
   match route
   !
   action reject
  !
  default-action accept
```

cisco Live!

Secure Internet Access

SD-WAN Internet Breakout Options

Local Breakout using a Default Route

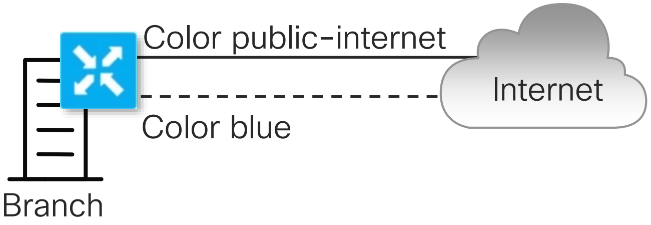


```
vpn 0
 interface ge0/0
  nat
 !
vpn 1
 ip route 0.0.0.0/0 vpn 0
```

- Static route in Service VPN
  - Can be default or more granular
- Redirects traffic to interfaces in VPN 0
  - Interfaces must have NAT enabled
  - Multiple interfaces enables per-flow load-sharing
  - Relies on VPN 0 routing table
- Can be complemented with a Tracker to monitor Internet availability beyond first hop gateway

SD-WAN Internet Breakout Options

Local Breakout using Data Policy



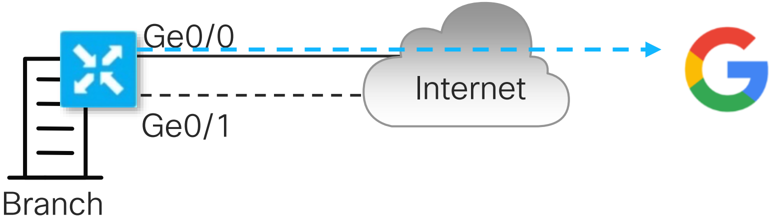
```
WAN Edge
vpn 0
 interface ge0/0
  nat
```

```
vSmart
policy
 data-policy internet-breakout
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.0/8
    !
    action accept
     nat use-vpn 0
     local–tloc public-internet
```

- Policy now redirects instead of static route
  - In case local exit fails, lookup can fall back to local service VPN routing table
- Redirects traffic to interfaces in VPN 0
  - Interfaces must have NAT enabled
  - Multiple interfaces enables per-flow load-sharing
  - Relies on VPN 0 routing table
- Can be complemented with a Tracker to monitor Internet availability beyond first hop gateway
- Local TLOC to be used can be specified

SD-WAN Internet Breakout Options

Using a Tracker to ensure functional Internet Access

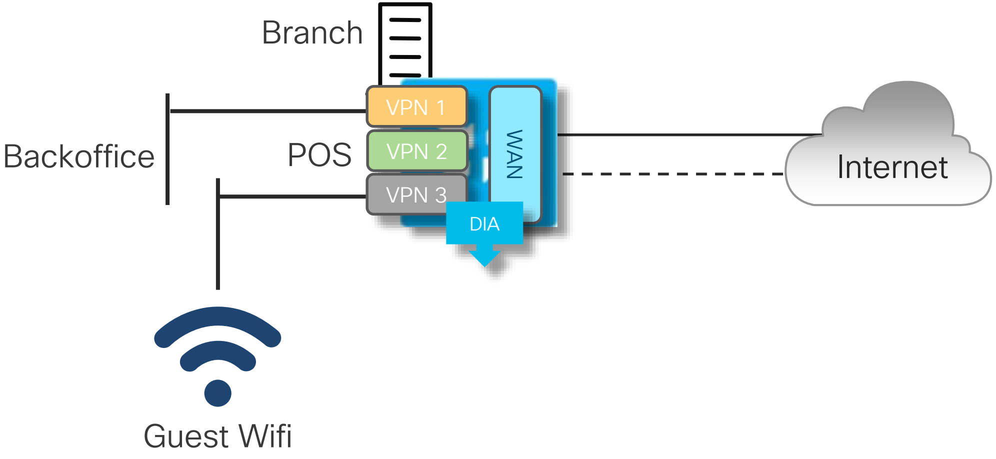


```
WAN Edge
System
 tracker google
  endpoint-dns-name www.google.com
  interval 60 (default, seconds)
  multiplier 3 (default)
  threshold 300 (default, ms)
 !
!
vpn 0
 interface ge0/0
  nat
  tracker google
```

- BFD only manages TLOC reachability
  - Different mechanism needed to qualify DIA connection as functioning
- Tracker uses native DIA path for probes
  - Configured on a per Interface basis
  - Uses HTTP Probes only
  - Relies on VPN 0 routing table
- With Tracker down, all routes resolving onto a tracked interface are invalidated

SD-WAN Internet Breakout Options

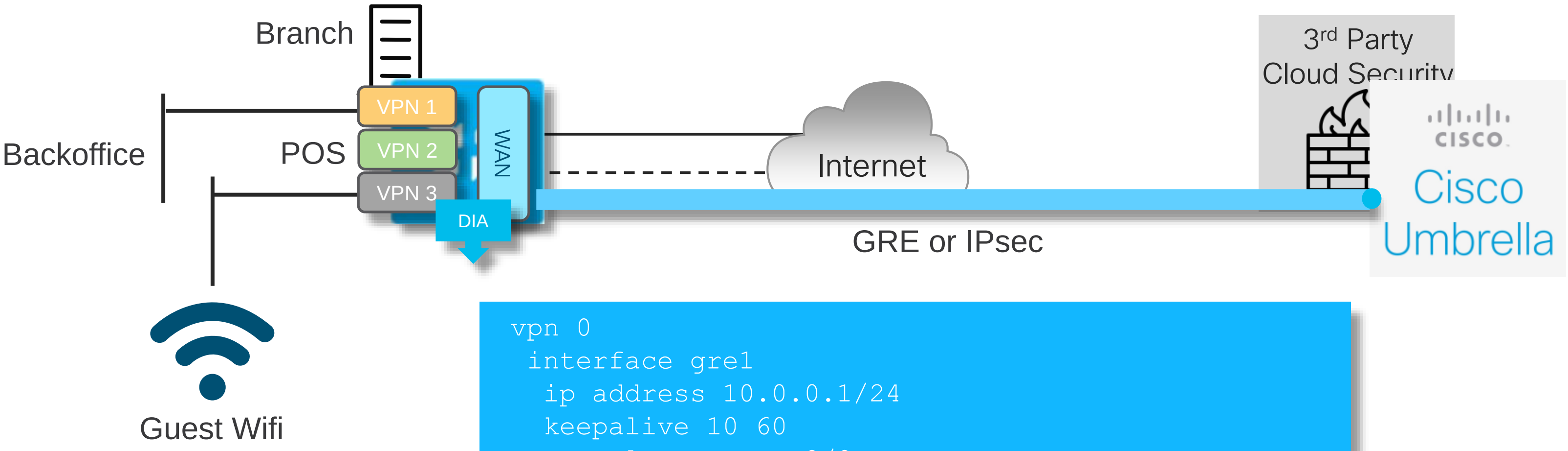
Localizing the WiFi Local Breakout / DIA



vSmart

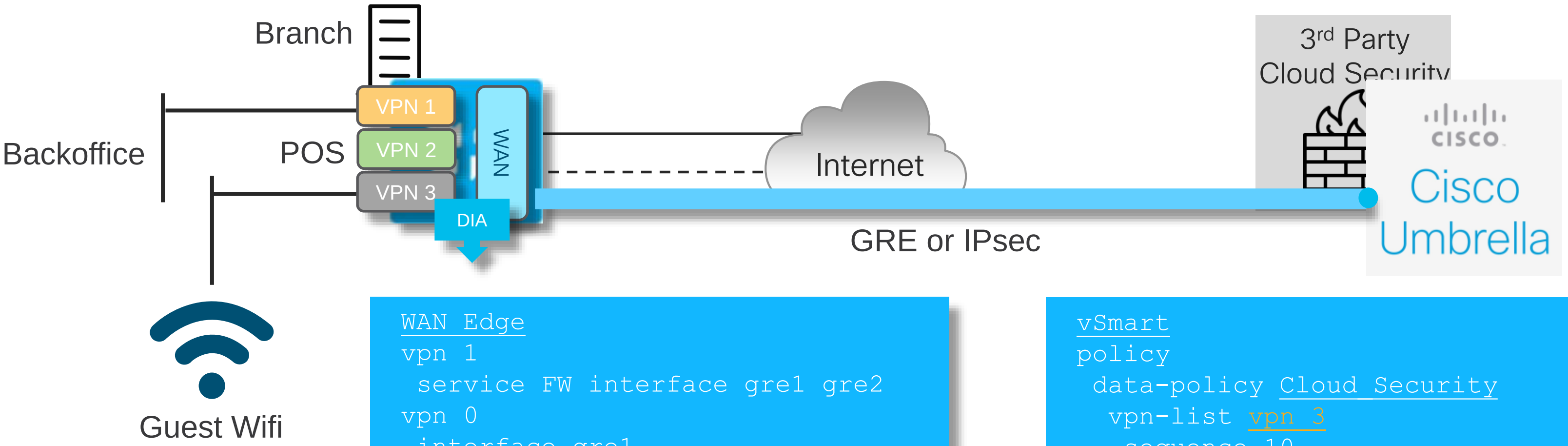
```
Policy
 lists
  vpn-list VPN3
   vpn 3
  !
site-list branch_sites
  site-id 100-200
  !
 !
 control-policy localize_wifi
  sequence 10
   match route
    vpn-list VPN3
   !
   action reject
   !
  !
  default-action accept
 !
!
apply-policy
  site-list branch-sites
   control-policy localize_wifi in
```

Cloud Security: Standard Routing with HA



```
vpn 0
 interface gre1
  ip address 10.0.0.1/24
  keepalive 10 60
  tunnel-source ge0/0
  tunnel-destination 2.1.1.1
  no shutdown
 !
 interface gre2
  …
 !
!
vpn 1
 ip gre-route 0.0.0.0/0 vpn 0 interface gre1 gre2
```

Cloud Security: Policy-Driven with HA



```
WAN Edge
vpn 1
 service FW interface gre1 gre2
vpn 0
 interface gre1
  ip address 10.0.0.1/24
  tunnel-source-interface ge0/0
  tunnel-destination 2.1.1.1
  no shutdown
 !
 interface gre2
  …
 !
!
```

```
vSmart
policy
 data-policy Cloud Security
  vpn-list vpn 3
   sequence 10
    match source-ip 10.0.0.0/8
   !
    action accept
     set
      service FW local
     !
    !
   !
   default-action accept
```

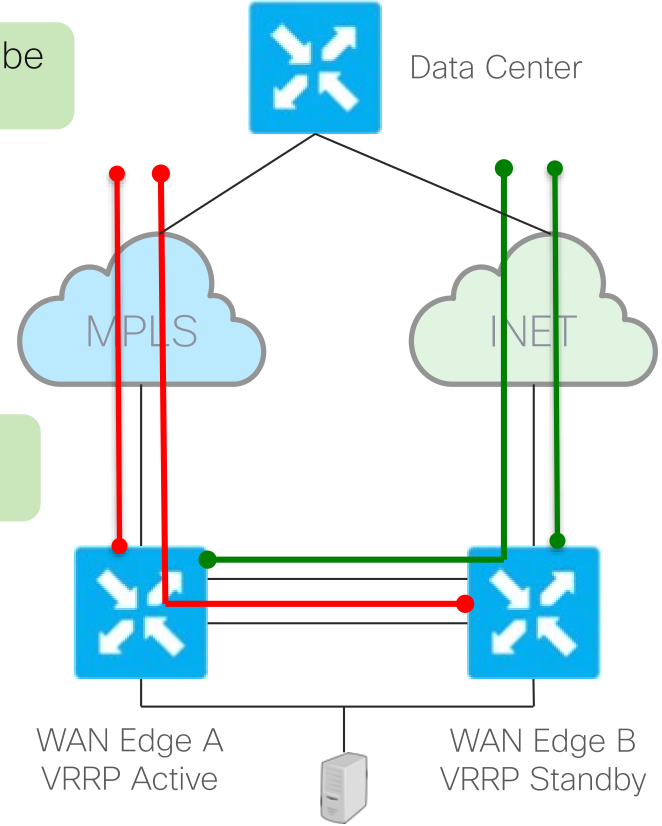
Redundancy

Fully Redundancy Architecture

- Cisco SDWAN has redundancy built into it in every aspect of the solution
- Controllers are deployed in a redundant fashion so that there is no single point of failure
- Even if all controllers are down, data plane continues to work without interruption
- Features and knobs available to achieve device and transport level redundancy

High Availability with DPI and Zone Based Firewall

For DPI and ZBF, traffic has to be symmetric



Outbound WAN Edge A is the VRRP Active Router

Inbound use higher preference on WAN Edge A to attract traffic

```
vpn 0
interface interface-name
tunnel-interface
          encapsulation (gre | ipsec)
                    preference number
                    weight number
```

Preference vs Weight

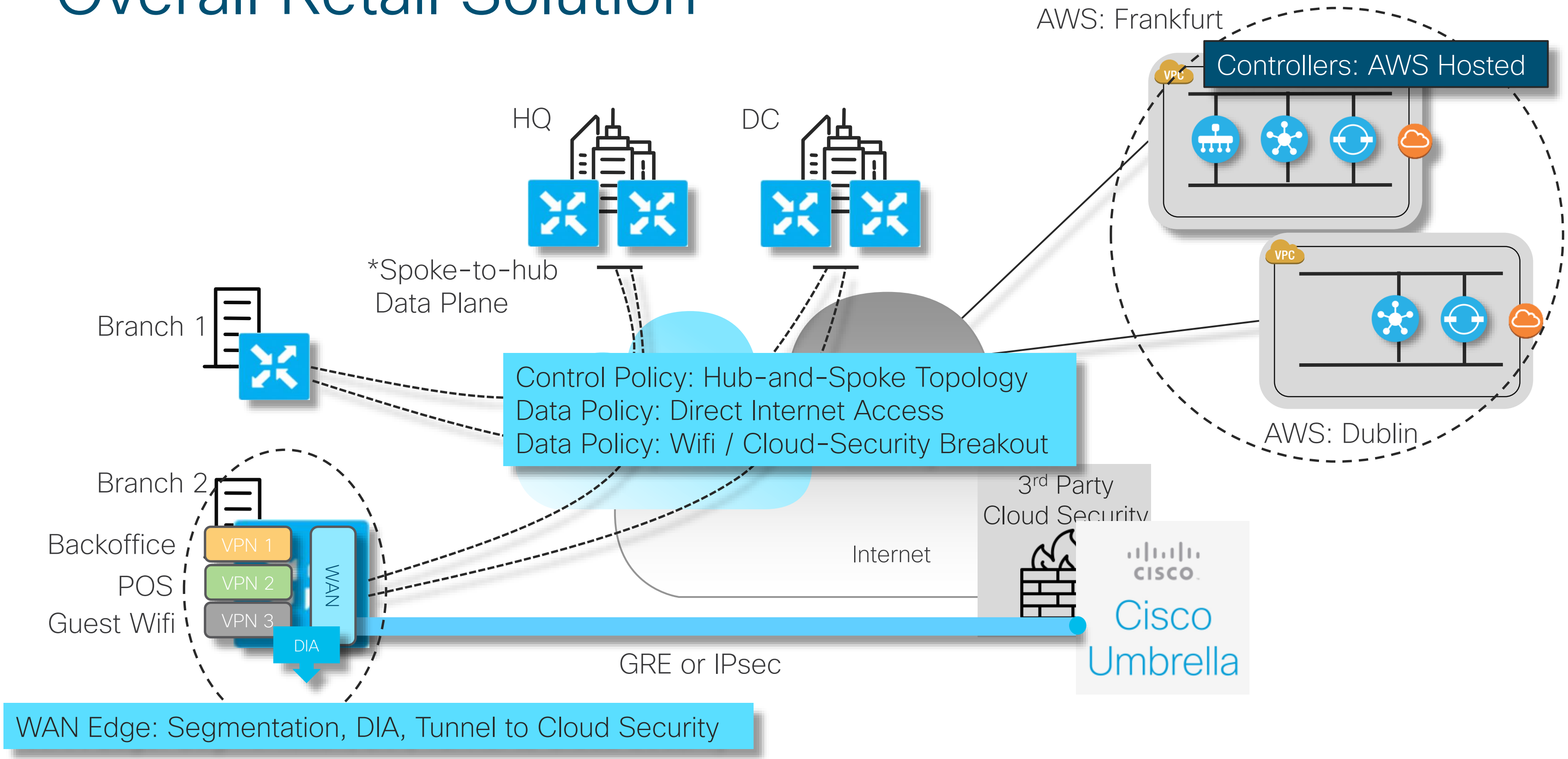
Preference

- TLOCs with the highest preference are chosen to forward outbound traffic
- If all TLOCs have the same preference traffic flows are evenly distributed among the tunnels, using ECMP.
- Configured under the tunnel interface

Weight

- Weight is used to achieve unequal cost multipath
- Flows are distributed across TLOCs based on the weight ratio
- For example, if TLOC A has weight 10, and TLOC B has weight 1, and both TLOCs have the same preference value, then roughly 10 flows are sent out TLOC A for every 1 flow sent out TLOC B.

Overall Retail Solution



vManage Network Design Builder

Cloud onRamp for IaaS
TGW Branch VPN Automation Demo

Cisco SD-WAN

Cisco vManage

Cloud onRamp for IaaS
TGW Sd-WAN GW Automation Demo

Cisco SD-WAN

Cisco vManage

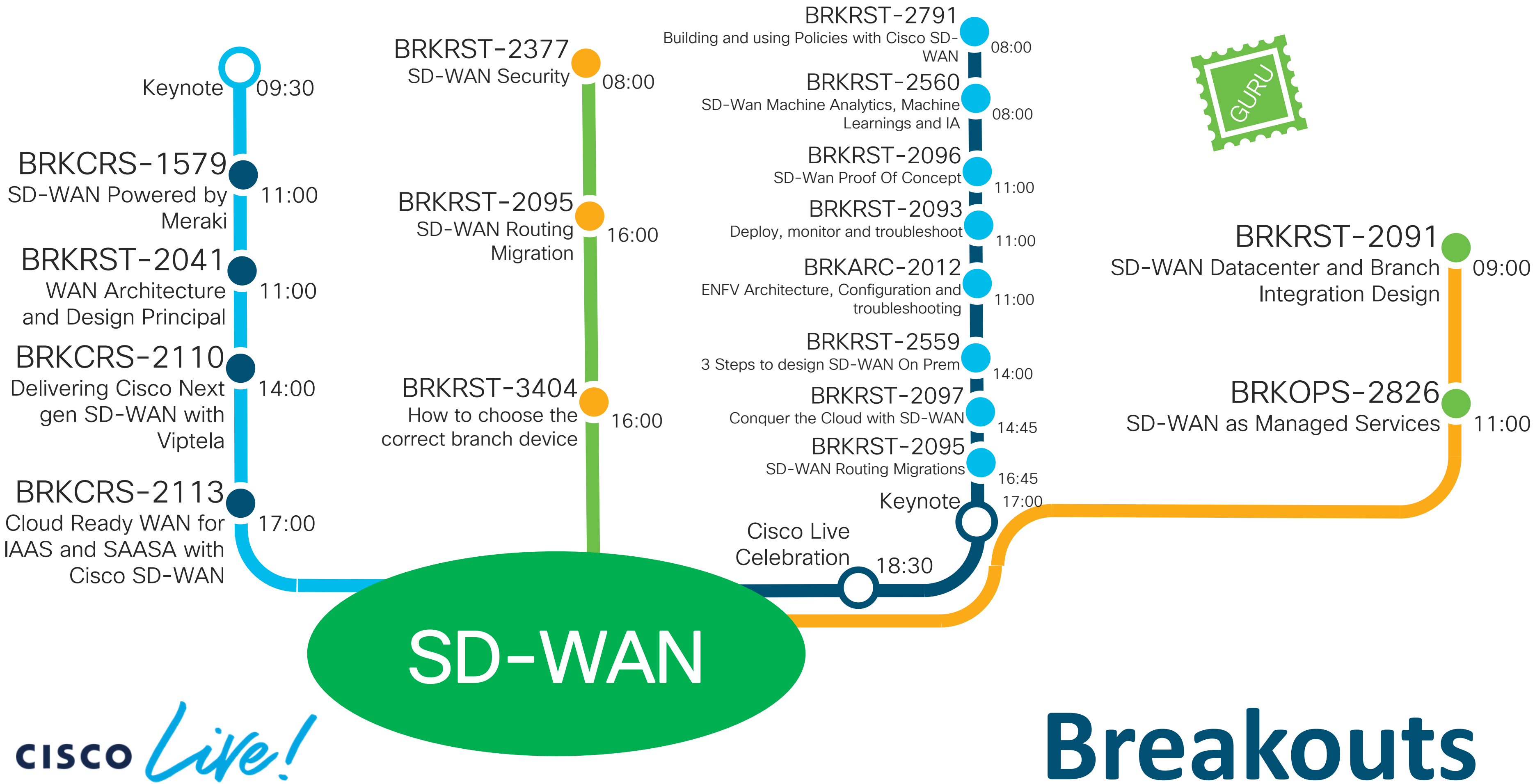
Wrap up

Key Messages

Cisco SD-WAN Solution helps you to:

- Reduce Cost
- Operate Faster with Security
- Integrate Latest Cloud and Network Technologies

Breakouts



Keynote 09:30

BRKCRS-1579
SD-WAN Powered by Meraki 11:00

BRKRST-2041
WAN Architecture and Design Principal 11:00

BRKCRS-2110
Delivering Cisco Next gen SD-WAN with Viptela 14:00

BRKCRS-2113
Cloud Ready WAN for IAAS and SAASA with Cisco SD-WAN 17:00

BRKRST-2377
SD-WAN Security 08:00

BRKRST-2095
SD-WAN Routing Migration 16:00

BRKRST-3404
How to choose the correct branch device 16:00

BRKRST-2791
Building and using Policies with Cisco SD-WAN 08:00

BRKRST-2560
SD-Wan Machine Analytics, Machine Learnings and IA 08:00

BRKRST-2096
SD-Wan Proof Of Concept 11:00

BRKRST-2093
Deploy, monitor and troubleshoot 11:00

BRKARC-2012
ENFV Architecture, Configuration and troubleshooting 11:00

BRKRST-2559
3 Steps to design SD-WAN On Prem 14:00

BRKRST-2097
Conquer the Cloud with SD-WAN 14:45

BRKRST-2095
SD-WAN Routing Migrations 16:45

Keynote 17:00

Cisco Live Celebration 18:30

BRKRST-2091
SD-WAN Datacenter and Branch Integration Design 09:00

BRKOPS-2826
SD-WAN as Managed Services 11:00

GURU

SD-WAN

cisco Live!

Complete your online session survey

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

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

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**

You make **possible**