
cisco
You make possible

SD-WAN Co-Management for MSPs

Concept, Architecture, and Example Implementation with Cisco SD-WAN

Iñigo Alonso, CX Delivery Architect
@_inigo_alonso

BRKOPS-2316

Barcelona | January 27-31, 2020

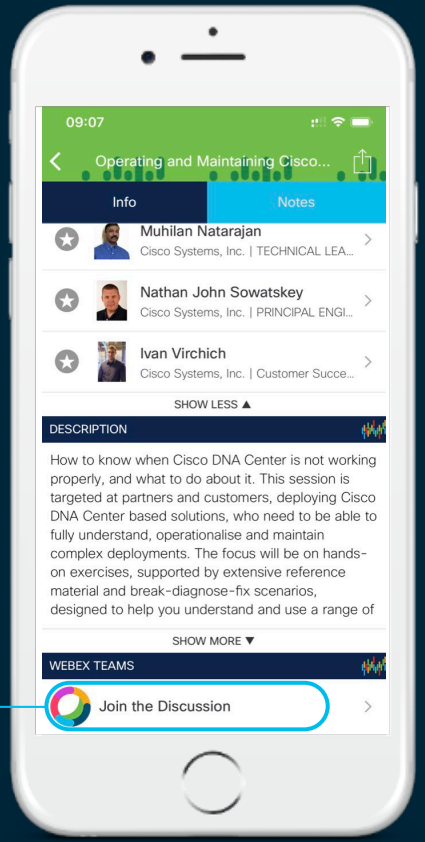
Cisco Webex Teams

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Co-Managed SD-WAN Concept
- Architecture Overview
- SD-WAN Deployment
- Provisioning
- Security
- Operations
- Key Takeaways

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Co-Managed SD-WAN Concept

The SD-WAN dichotomy: “a choice between DIY and a managed service”

Source: on-line IT publications

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN DIY vs Managed Service

Example Selection Criteria from Tenant's Perspective

DIY

- Flexibility, ease to evolve
- Application knowledge
- Control over network & data
- Integrations
- Cost

Managed Service

- Speed of deployment
- Procurement of HW and links
- Geographical coverage
- Skills & staffing
- Operations / incident management

Intermediate alternative: Co-Managed SD-WAN

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Co-Managed SD-WAN Concept

- A Co-Managed SD-WAN service provides the Tenant customer with the flexibility to self-manage their VPN services…
- … and enables the Managed Service Provider (MSP) to focus on the overall SD-WAN connectivity, the customer experience, and providing the network SLAs
- The co-managed approach offers to the Tenants the ability to customize the design of their WAN network, while remaining within a managed service SLA

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-WAN Architecture

Management Plane

- Single pane of glass
- Monitoring and Troubleshooting
- RBAC and APIs

Control Plane

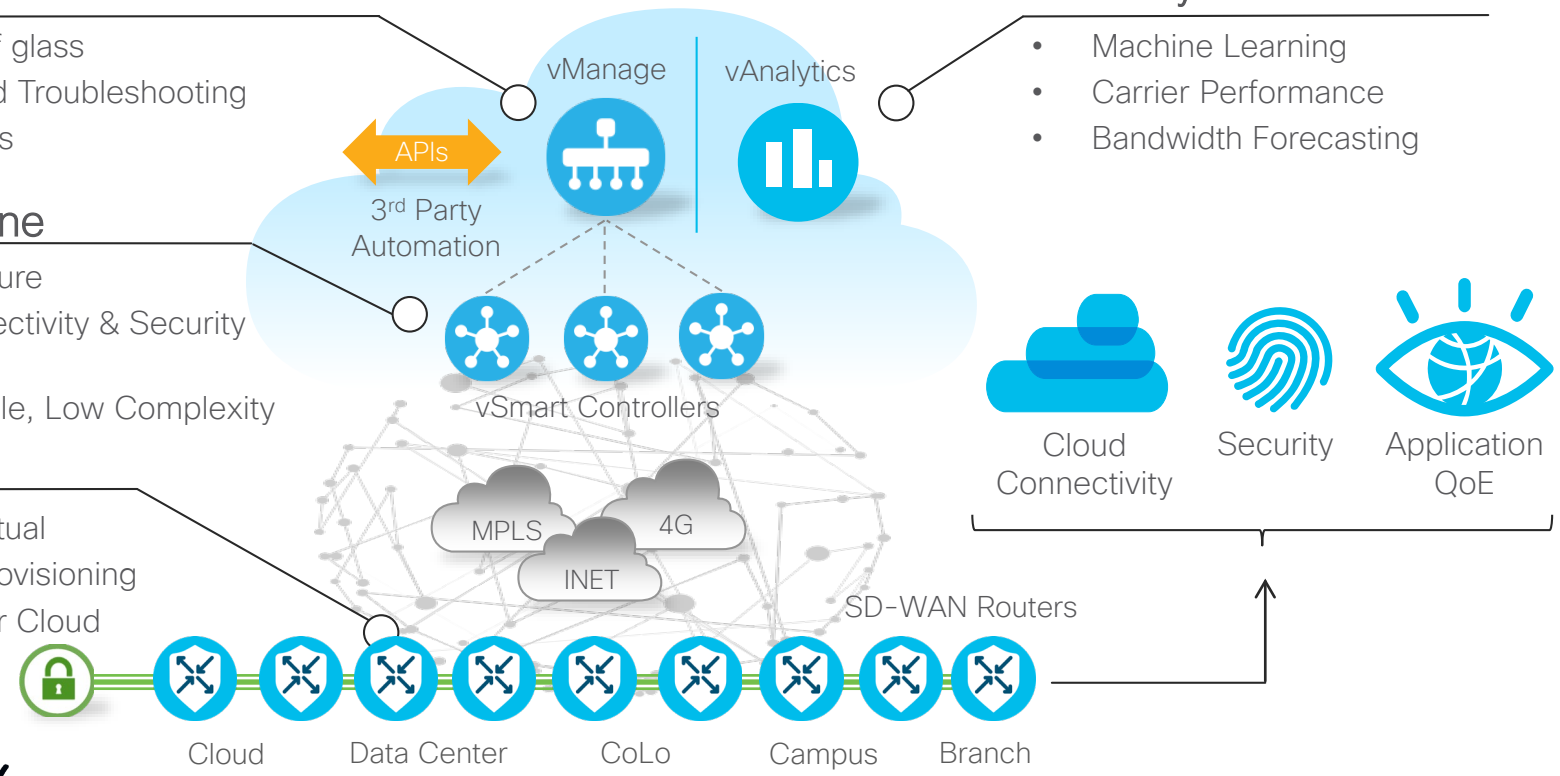
- SDN Architecture
- Flexible Connectivity & Security Distribution
- Horizontal Scale, Low Complexity

Data Plane

- Physical or Virtual
- Zero Touch Provisioning
- On-Premise or Cloud

Analytics

- Machine Learning
- Carrier Performance
- Bandwidth Forecasting

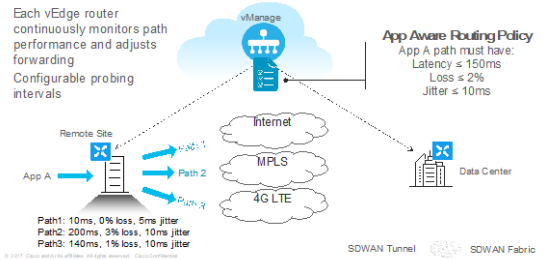


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Use-Case Examples

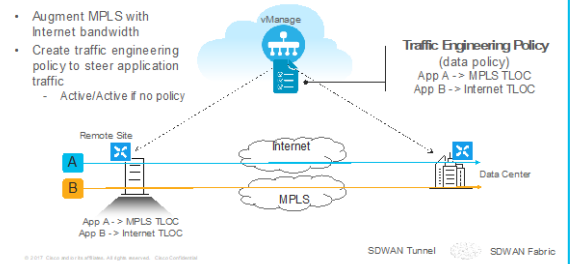
Critical Applications SLA

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



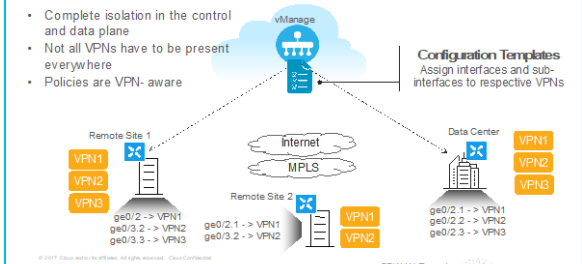
Bandwidth Augmentation

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



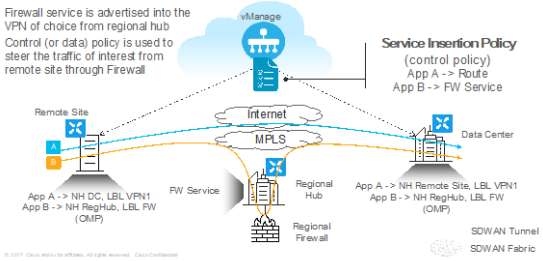
Secure Segmentation

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



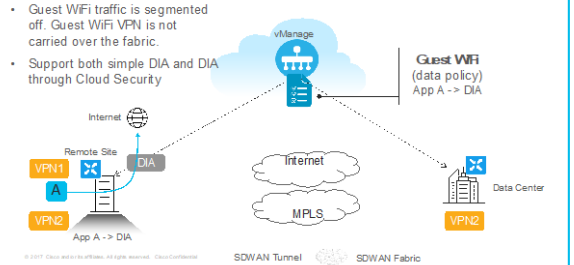
Regional Secure Perimeter

- 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



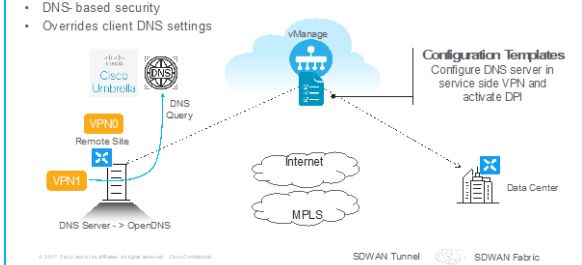
Guest WiFi

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



DIA & DCA

- DNS- based security
- Overrides client DNS settings



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Co-Managed SD-WAN Concept

MSP / Tenant Roles – Example High-Level Definition

MSP	Tenant
❑ SD-WAN Deployment	❑ Service VPNs & LAN configs
❑ Procure HW and WAN links	❑ Policies: Control, Data, Security
❑ Device onboarding	❑ Network Integrations
❑ Infra/Underlay Monitoring	❑ VPN Overlay Monitoring
❑ Design, Operations, Incident tracking	

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Co-Managed SD-WAN Concept

Drivers from MSP perspective

- Focus on the core functions & operation – common across all tenants
  - Procurement, initial build, underlay, geographical coverage, etc
- Leverage management controller capabilities / avoid duplicate development
- Augment the service catalog of supported designs and feature-set
- Flexibility to support end-user customizations
- Optionally invest in value-add features and common use-cases
- Re-use model for multiple SD-WANs

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Co-Managed SD-WAN Concept

Drivers from Tenant perspective

- Focus on the customization of the SD-WAN service
- Leverage knowledge of the application environment
- Support dynamic evolution and integrations: security, cloud, network domains, etc
- Reduce the investment in SD-WAN build and operations: skills, processes, tools, etc
- Single interface via MSP for WAN procurement
- Control over the usage of the SD-WAN

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Co-Managed SD-WAN Concept

Challenges

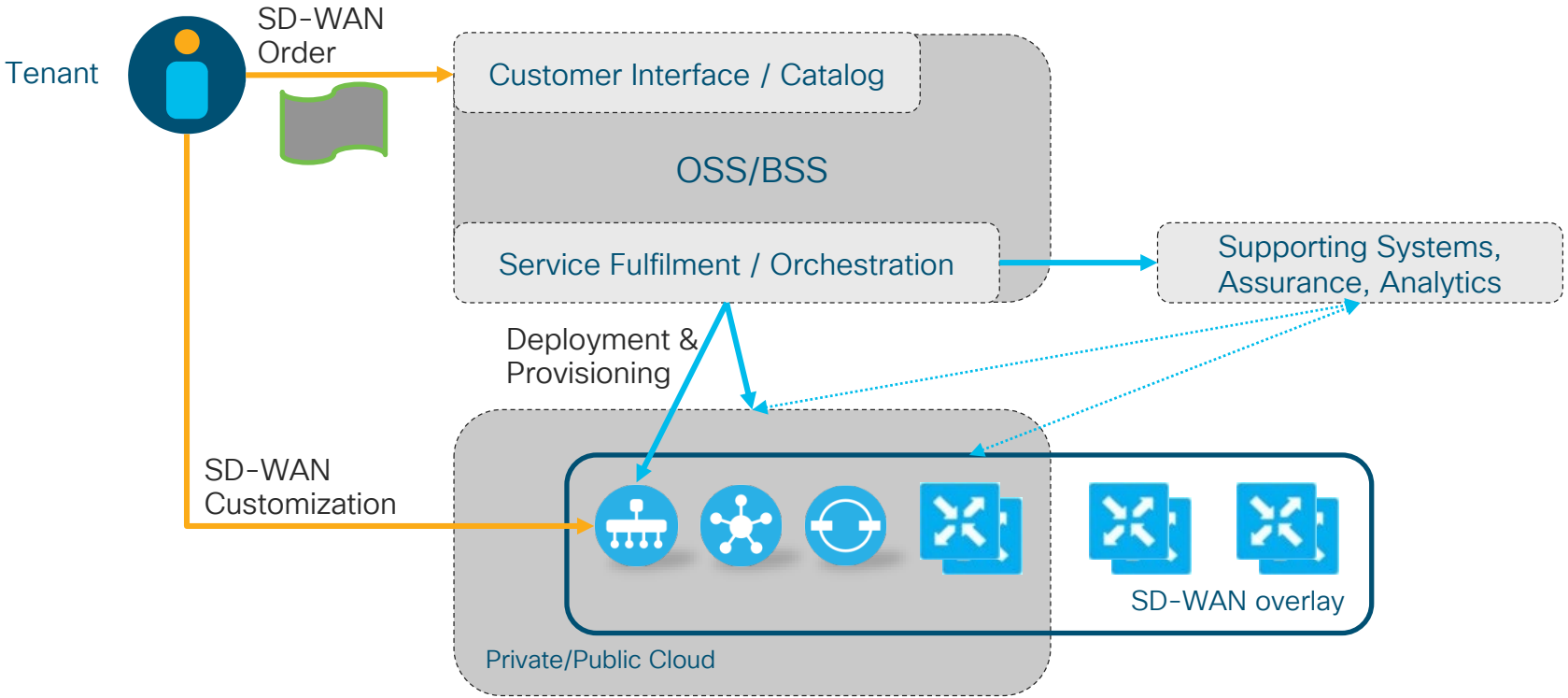
- MSP/Tenant roles overlap
  - Closer collaboration and coordination between parties required
  - Change control management
  - Incident tracking, troubleshooting
  - Distributed/complementary skills between both parties
- Limited RBAC capabilities in SD-WAN controllers
  - Limited support for MSP/Tenant role separation
  - Limited control by MSP of the features in use
- Contractual agreement
- Defining a Shared Responsibility Model

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Architecture Overview

MSP Architecture Overview

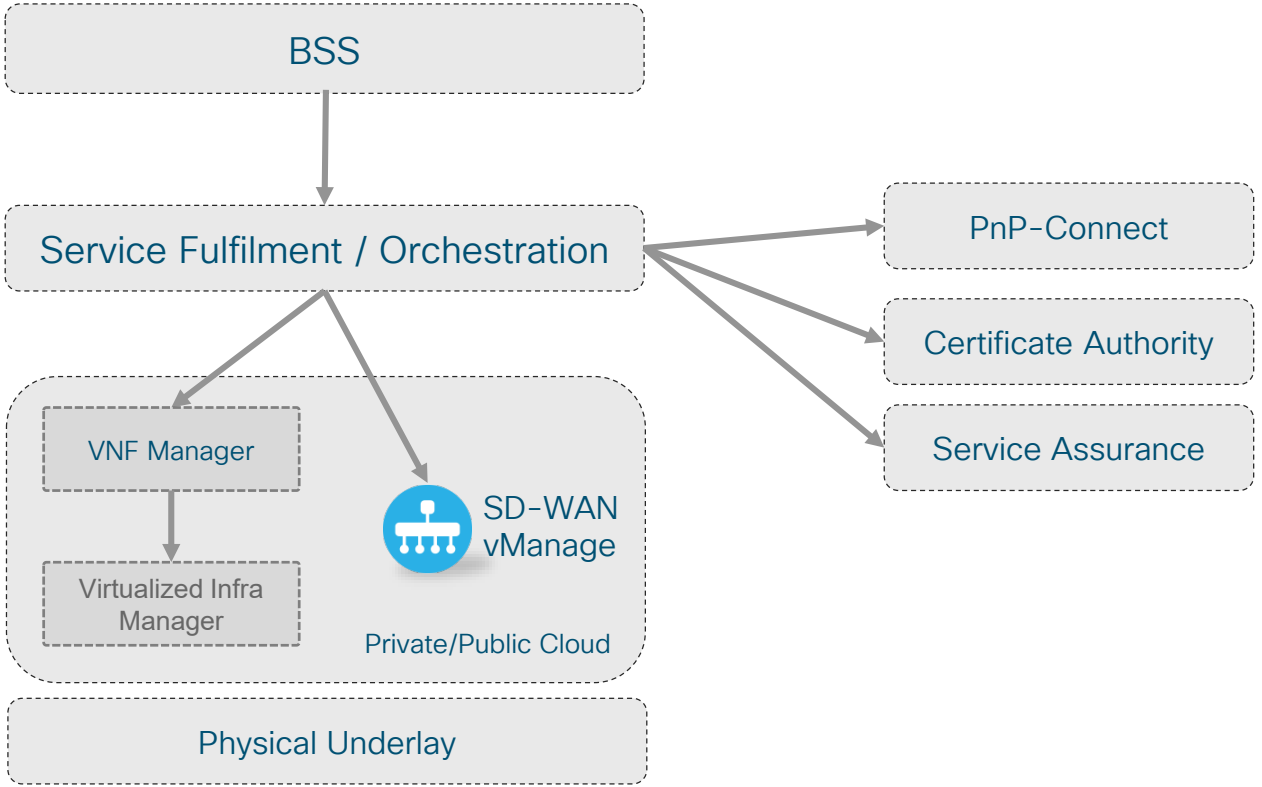
Building Blocks – Simplified High-Level View



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MSP Architecture Overview

Building Blocks – Simplified High-Level View



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

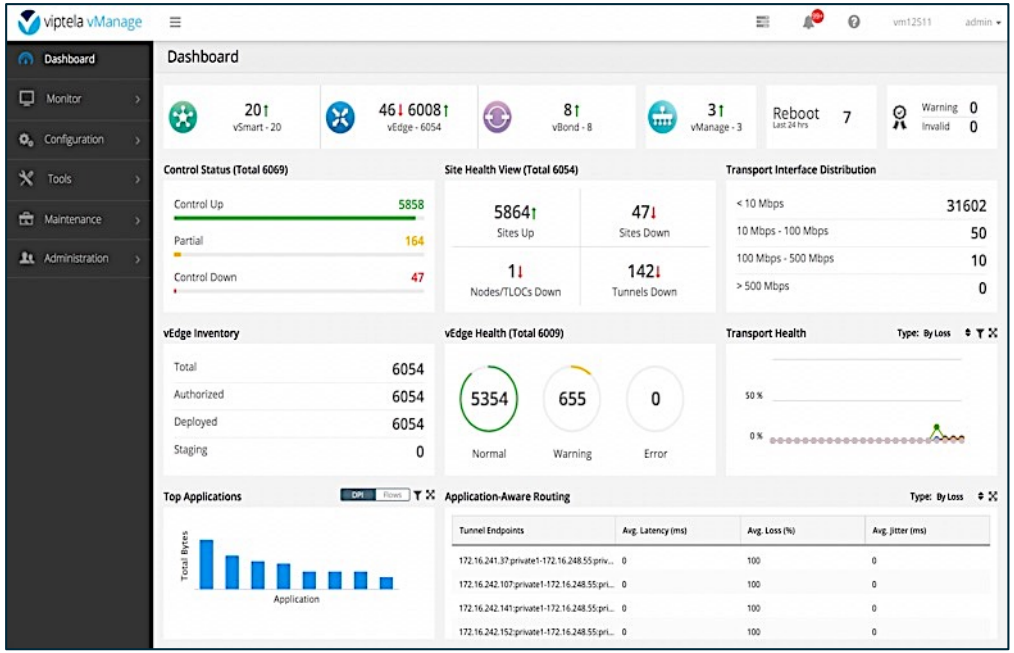
Cisco vManage Controller

Capabilities

- Single pane of glass for Day0, Day1 and Day2 operations
- Device whitelist: controller and WAN Edges
- Configuration management: provisioning of device configuration and policies
- Operations: SW management, upgrades, device inventory, etc
- Monitoring and Troubleshooting
- Manual/Automated workflows
- Programmatic interfaces (REST, NETCONF)
- Role-Based Access Control

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco vManage Controller



- Intuitive GUI driven operations
  - Management, monitoring and troubleshooting
- Cloud Delivered
  - Private, hosted or managed
- Single or Multi-tenant
- Role-based Access Control
- Clustered for scale and high availability
- REST APIs based

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deployment

SD-WAN Deployment
Example Co-Managed Roles

MSP

- Shared Infra: private/public cloud
- Integration of underlay(s)
- Supporting systems: ordering, PnP, CA, DNS …
- SD-WAN controller deployment
- Deployment and onboarding of WAN Edges

Tenant

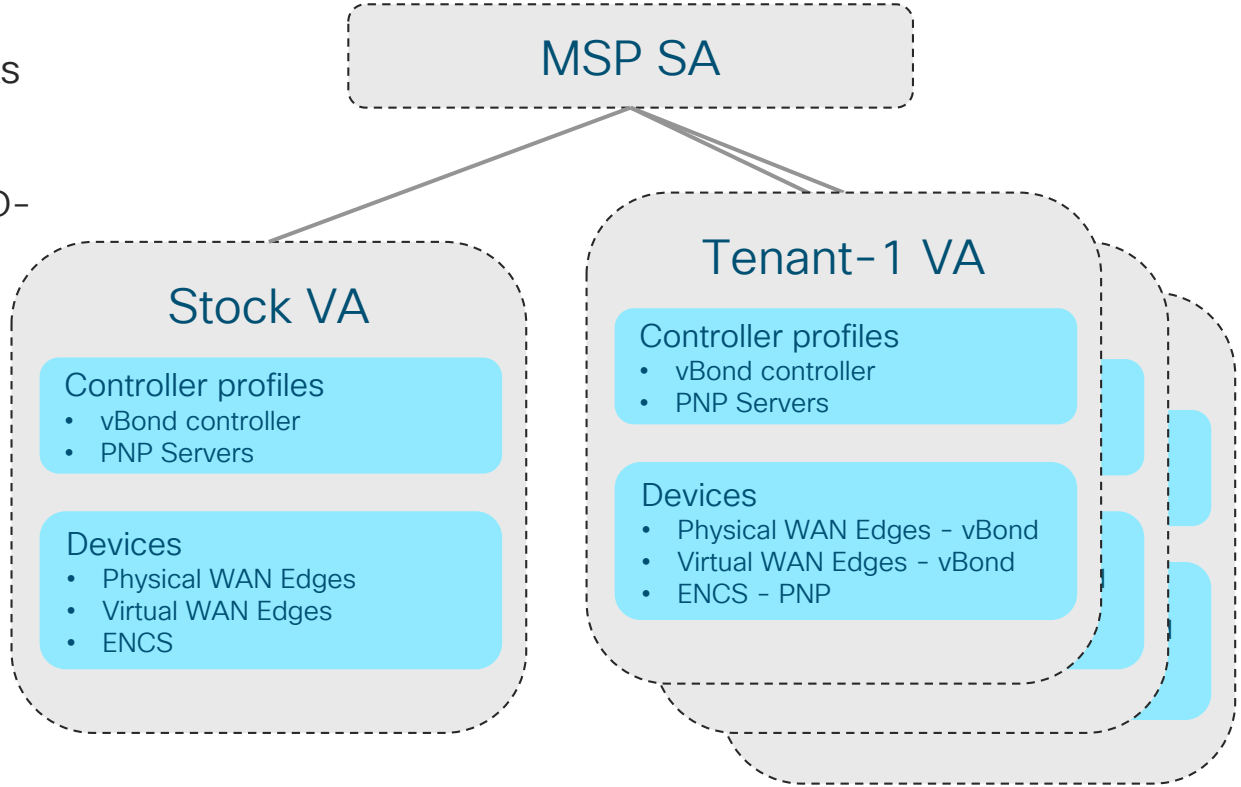
- Inputs for SD-WAN service order:
  - Deployment: size, regions, underlays
  - System parameters: control & data-plane operation
  - Network admin contacts and credentials (or IdP metadata for SSO)
  - Misc service parameters

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Smart Account / Virtual Account (SA/VA)

MSP PnP-Connect

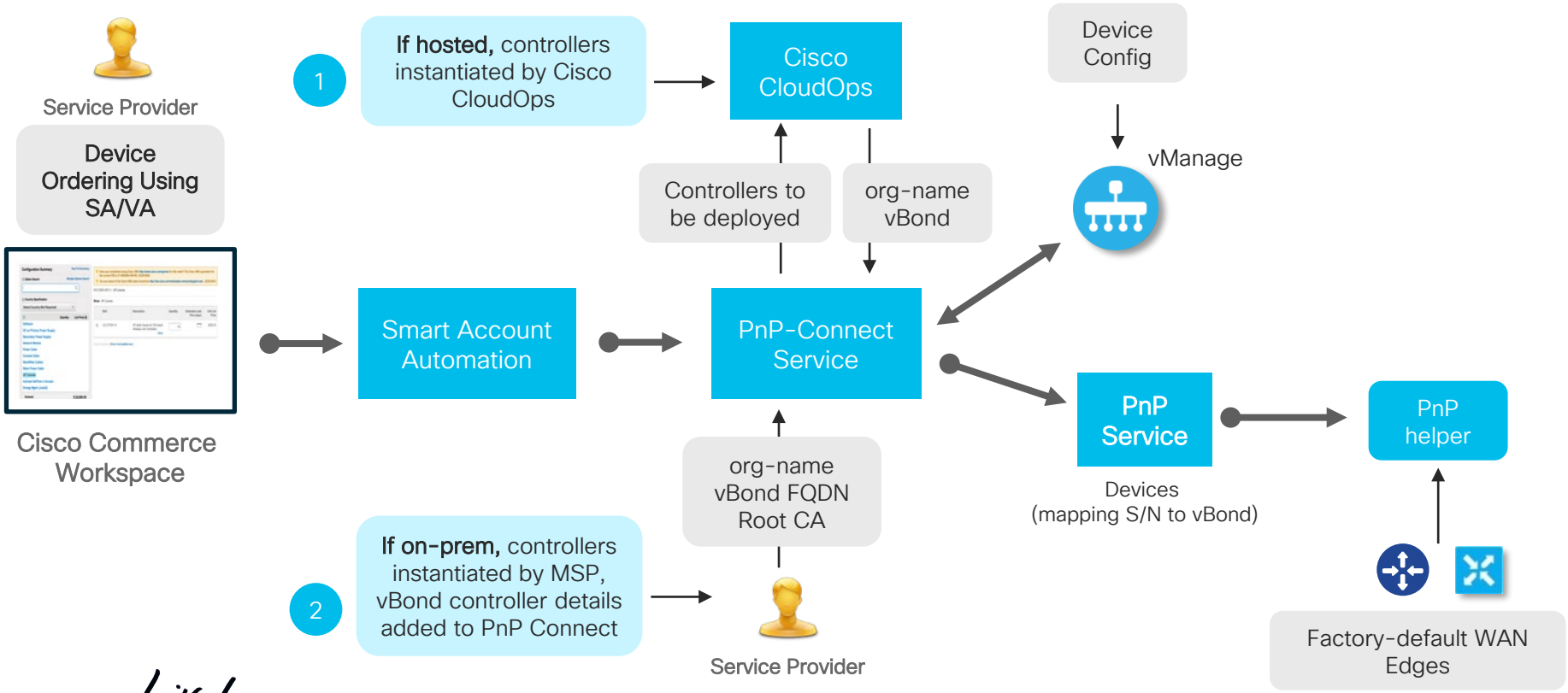
- An SA has multiple VAs
- 1x VA per Tenant
  - 1:1 mapping VA to SD-WAN name
- SD-WAN equipment order per SA/VA



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Smart Account / Virtual Account (SA/VA)

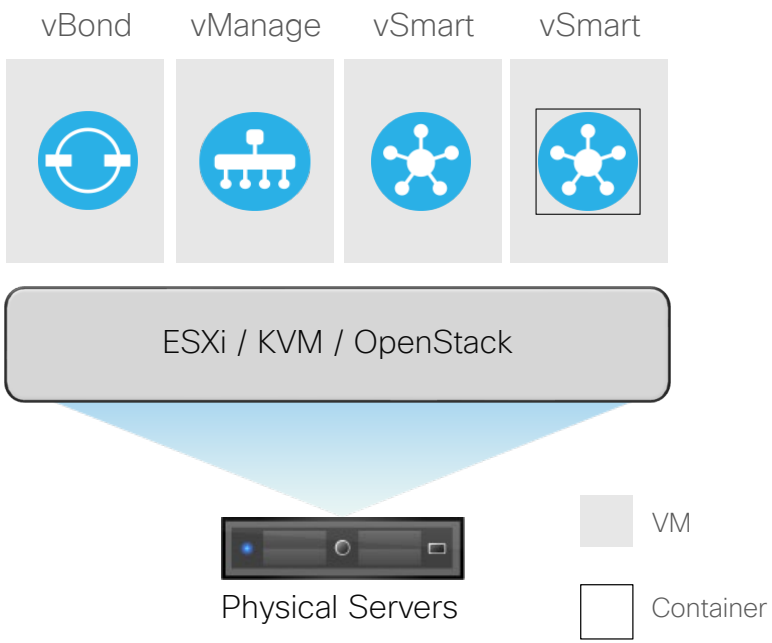
PnP-Connect Provisioning Flow



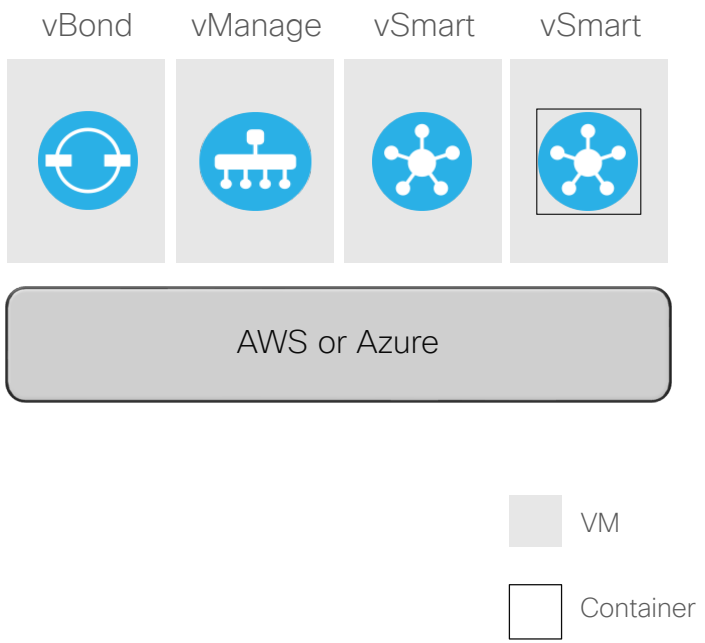
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Controller Deployment Options

On-Prem Deployment

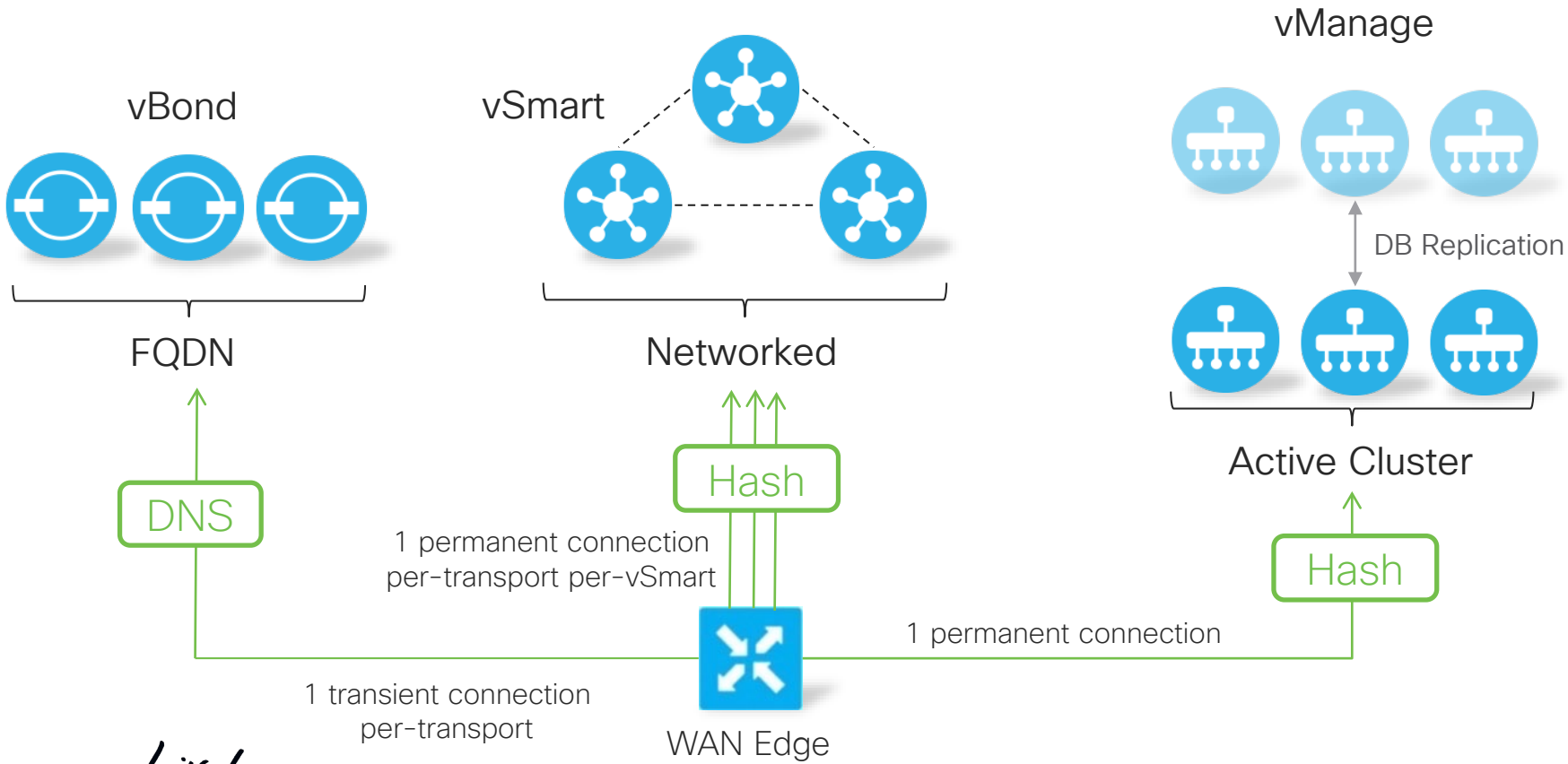


Cloud-Hosted



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

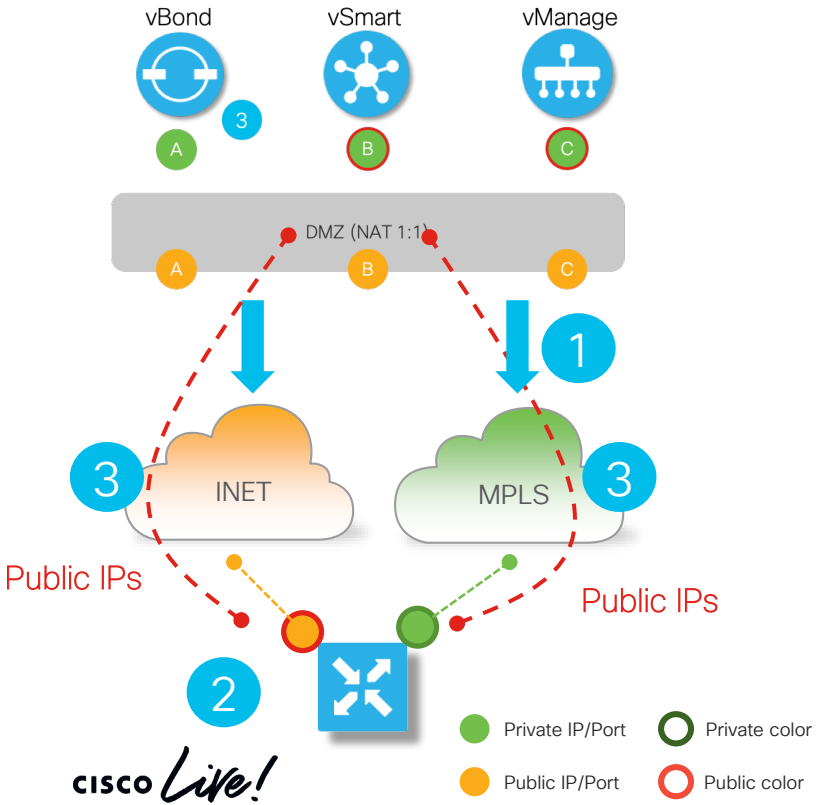
Controller HA and Horizontal Scale



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SP-Hosted Deployment Example

Control on MPLS/INET – Public IP Addresses

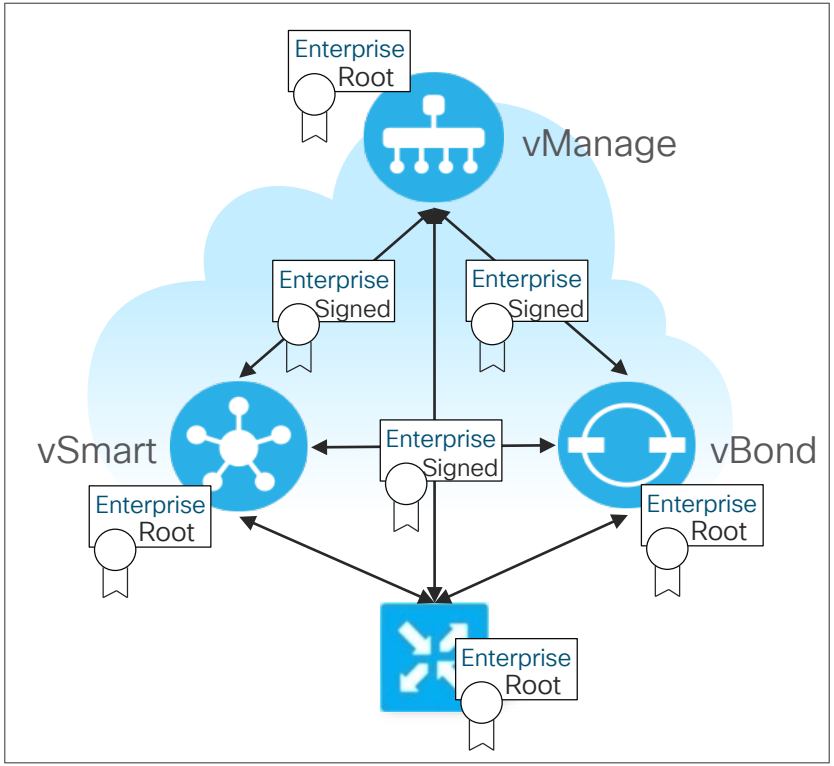


- (1) Controller (NATed) public IP addresses **are advertised into MPLS**
- (2) WAN Edge pointed to the (NATed) vBond public IP address
- (3) WAN Edge communicates with vSmart and vManage using (NATe)d public IP address
  - Private color to public color uses public IP address; public color to public color uses public IP address
  - vBond (NATed) public IP address is reachable through MPLS and Internet transports

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Certificate Authority Options

- Controller CA Options
  - Cisco Automated
  - Enterprise CA
  - Manual
- Virtual WAN Edge CA Options
  - vManage-signed
  - Enterprise CA



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

WAN Edge Deployment

Example Co-Managed Ownership

MSP

- Site Design Catalog:
  - Single/redundant WAN Edges, models
  - # and type of WAN interfaces
  - BW tiers
- HW and WAN link procurement
- Deploy and onboard WAN Edges
  - Prep: PnP, serial validation, initial config
  - Verification of successful onboarding

Tenant

- Ordering of SD-WAN sites:
  - Site Design
  - WAN Edge model
  - WAN link bandwidth
- Inputs for Edge configuration
  - System, ex: name, location, site-id (based on region, type, role, etc)
  - Network, ex: WAN static IP settings
  - Monitoring: snmp, syslog, etc

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

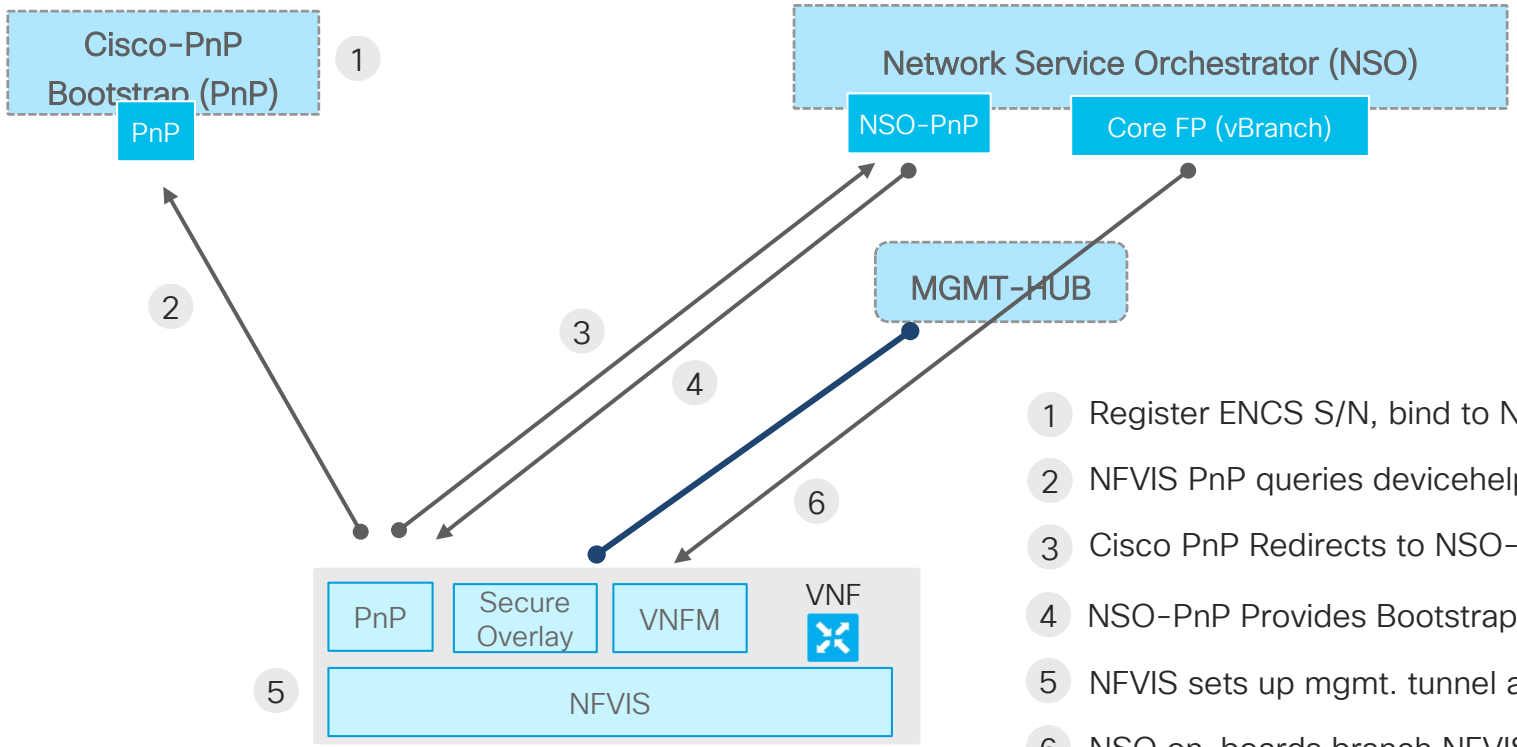
WAN Edge Onboarding
Options

- Onboarding using global PnP
- SD-WAN XE: bootstrap configuration
  - Bootstrap configuration ((“ciscosdwan.cfg”) includes required SD-WAN parameters
- Pre-staging using the “default WAN port” & global PnP
  - Non-default interface configuration (static-IP, sub-interface) applied during initial onboarding in pre-staging facility
  - “default WAN port” is platform-dependent

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Universal CPE (ENCS)

Deployment & Onboarding



1. Register ENCS S/N, bind to NSO-PnP controller
2. NFVIS PnP queries devicehelper.cisco.com
3. Cisco PnP Redirects to NSO-PnP
4. NSO-PnP Provides Bootstrap Config
5. NFVIS sets up mgmt. tunnel and NSO credentials
6. NSO on-boards branch NFVIS (NETCONF)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Provisioning

SD-WAN Configuration Elements

Example Co-Managed Ownership

Configuration Elements	Owner*
Controllers (devices)	MSP
WAN Edges (devices)	Shared
Centralized Policies (control, data, app-aware)	Tenant
Localized Policies	Shared
Security Policies	Tenant

*The “owner” integrates inputs from the other party

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

vManage GUI Role-Based Access Control

- RBAC: assign roles and responsibilities to different user groups
- vManage RBAC components
  - Users: user ids, either locally configured or authenticated via AAA
  - User Groups: user profiles, either locally configured or provided by AAA
  - Tasks: configuration and operational sections of the vManage GUI
  - Access Rights: Read and/or Write
- vManage RBAC “Tasks” apply to complete categories
  - Ex: “Template Configuration” applies to configuration for all device types
  - No current support for customization or more granular control

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

vManage RBAC – Example Tenant Profile

Feature	Read	Write
Alarms	✓	--
Audit Log	✓	--
Certificates	--	--
Cloud OnRamp	✓	✓
Cluster	--	--
Colocation	✓	✓
Device Inventory	✓	--
Device Monitoring	✓	--
Device Reboot	--	--
Events	✓	--
Interface	✓	✓
Manage Users	--	--
Policy	✓	✓
Policy Configuration	✓	✓
Policy Deploy	✓	✓
Routing	✓	✓
Security	✓	✓
Security Policy Configuration	✓	✓
Settings	--	--
Software Upgrade	✓	--
System	✓	--
Template Configuration	✓	✓
Template Deploy	✓	✓
Tools	✓	--
vAnalytics	--	--

- Cloud-on-Ramp for IaaS
- Cloud-on-Ramp for CoLo
- Centralized/Localized policies
- Security policies
- Device configuration

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Device Configurations

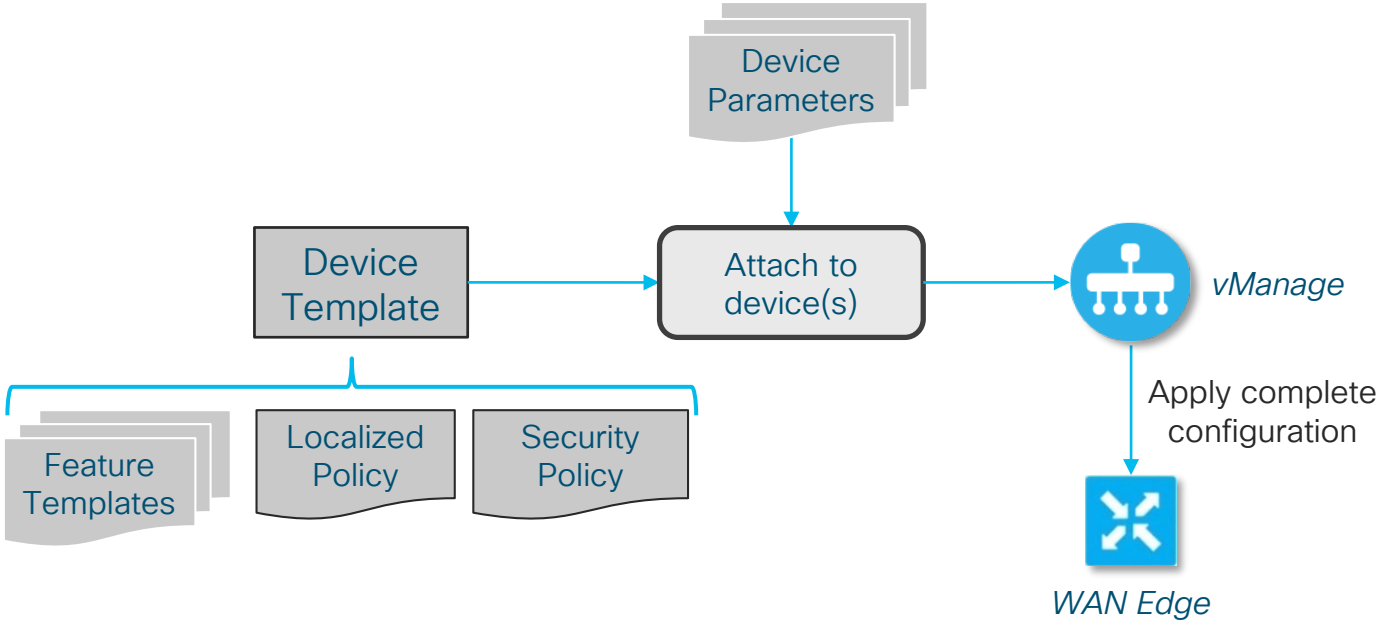
Example Co-Managed Ownership

- Controller Devices and MSP-owned Virtual WAN Edges
  - Full MSP ownership
  - Option between CLI and Feature Templates
- Customer WAN Edge Devices:
  - Shared ownership of configurations
  - “CLI Templates”: potentially complex split between MSP and Tenant
  - “Device and Feature Templates”: better fit for split ownership (next slides)

- MSP: preserve/protect owned configuration sections
- Tenant: flexibility to develop custom configurations

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

vManage Device Template

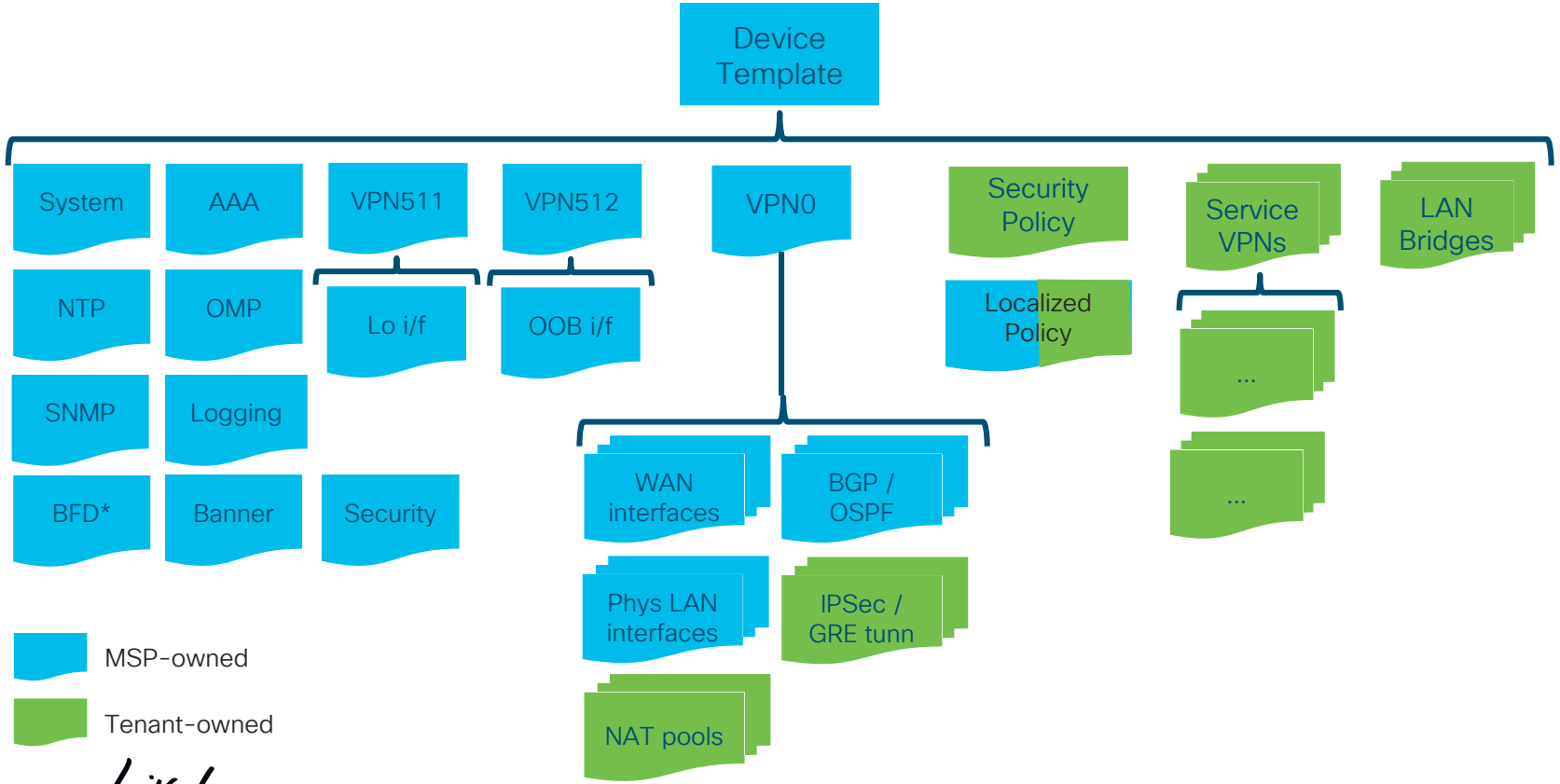


All template objects are defined in JSON format

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

vManage Feature Template Structure

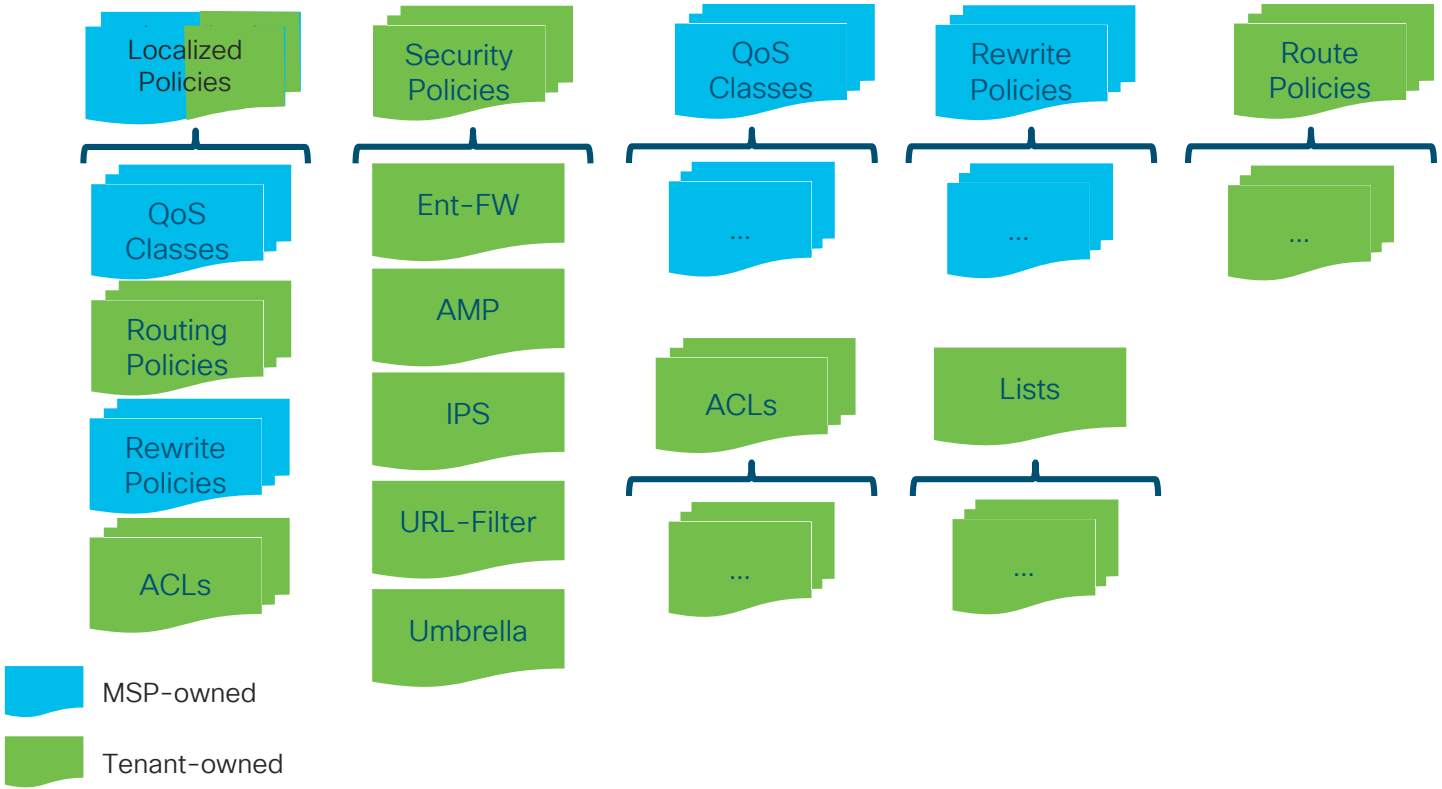
Example Co-Managed Ownership



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

vManage Feature Template Structure

Example Co-Managed Ownership

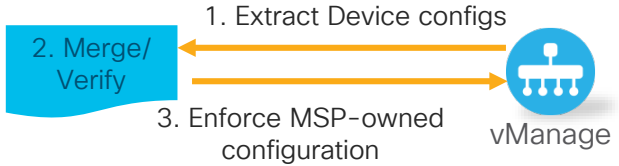


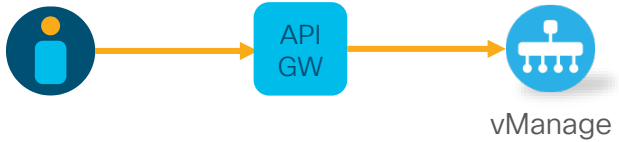
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Device Configurations

Preserving **MSP-owned** Configuration

- Configuration Verification / Overwrite
  - Verification of MSP-owned configurations: periodic / notification-triggered,
  - Templates defined in JSON format
- Reverse Proxy / API Gateway
  - Block Tenant's write access to controller configurations
- (Future) vManage RBAC extensions
  - Per-feature access control
  - Per-device access control





© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

WAN Edge QoS Configuration

Example Co-Managed Ownership

MSP

- WAN Egress Queuing policies
  - Aligned with underlay
- Underlay (outer) DSCP marking
- WAN Ingress/Egress Shaping
  - Enforce purchased bandwidth
- Inputs for QoS classification

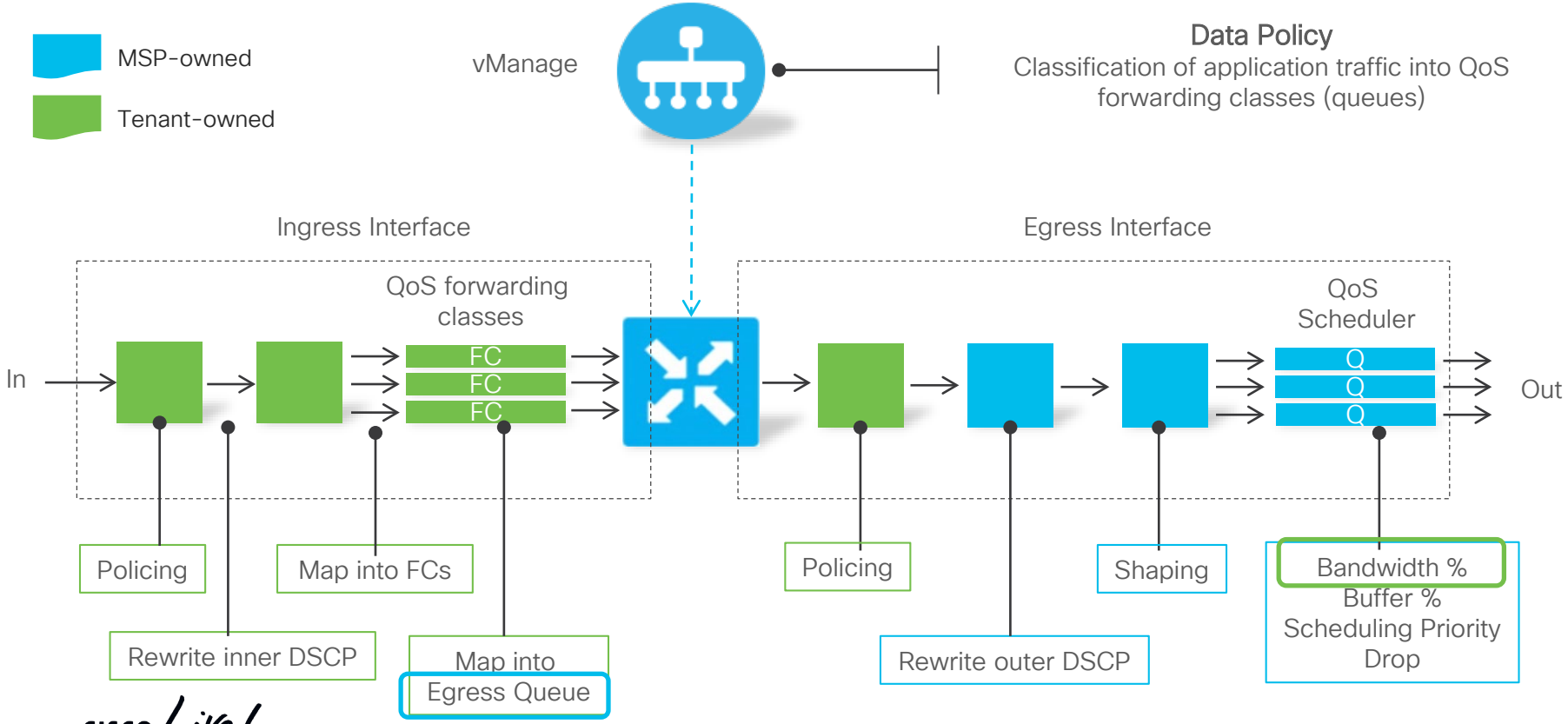
Tenant

- QoS Classification for VPN Traffic
  - DPI / ACL-based
- Overlay (inner) DSCP marking
- Mapping of overlay QoS classes to forwarding classes / queues
- Inputs for Egress Queuing

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

vEdge Router Device QoS Overview

Example Co-Managed Ownership



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Policies
Example Co-Managed Ownership

MSP

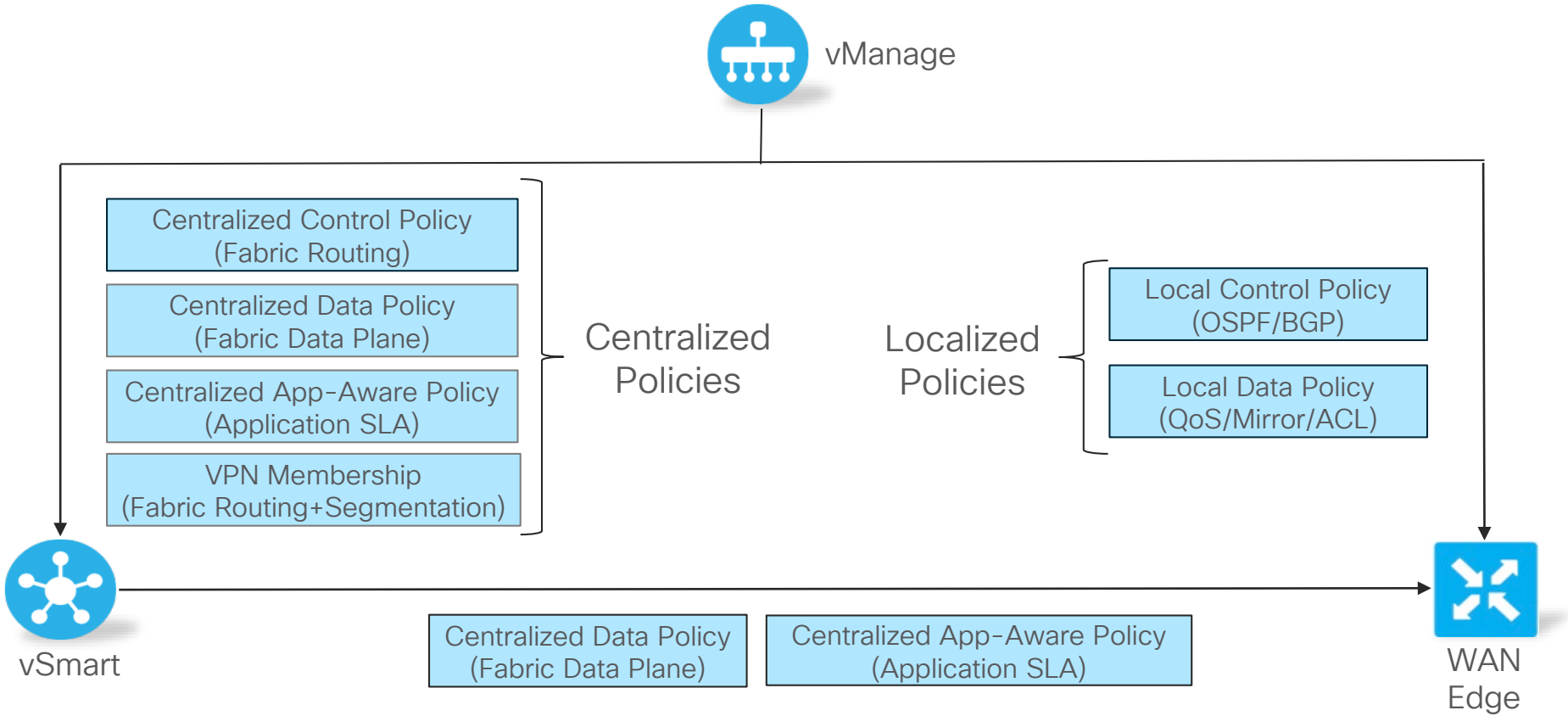
- Inputs for Centralized Policies
  - Forwarding classes for QoS policies
  - Site-ids for inband management VPN

Tenant

- Centralized Policy Configuration
  - Control, Data, App-aware, VPN membership policies
- Localized Policy Configuration
  - Local Routing, ACLs, policing, mirror
- Security Policy Configuration
  - Ent-FW, AMP, etc

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-WAN Policy Framework



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Policies

Co-Managed Considerations

- Control policies, use-cases:
  - Service Chaining, Traffic Engineering, Extranet VPNs, Service and Path affinity, VPN Topologies
- Data policies, use-cases:
  - Service Chaining, Cflowd, NAT, Traffic Policing and Stats, Transport Selection
- Application-Aware Routing policies, use-cases:
  - App-specific SLA compliant path through the SD-WAN fabric

- All policies are typically of interest for the Tenant SD-WAN customization
- May require coordination with MSP in some cases, ex:
  - Inband management VPN communication to MSP-owned WAN Edges

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud-on-ramp for IaaS

Example Co-Managed Ownership

MSP

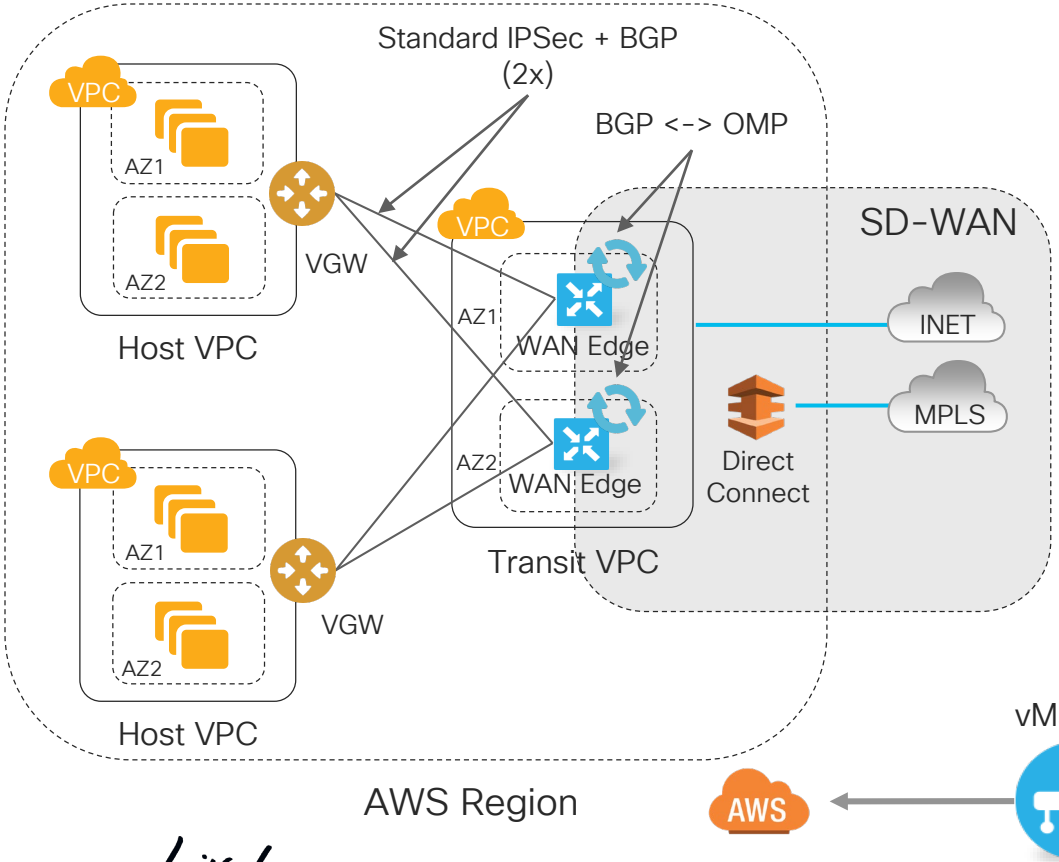
- Availability of virtual WAN Edges for deployment on IaaS
- Provide day0 configuration (MSP-owned sections)

Tenant

- Manage and Operate own IaaS account(s)
- Deploy SD-WAN on Cloud infra
  - Cloud-on-ramp for IaaS workflow
- Customize the virtual WAN Edge configuration (Tenant-owned sections)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud-on-ramp for IaaS - AWS



- Transit VPC per-region
  - Multiple for scale
- VGW for host VPCs
- Standard based IPSec
  - Connectivity redundancy
- BGP over IPSec tunnels for route advertisement
  - Active/active forwarding
  - BGP into OMP redistribution
  - Advertise default to host VPCs
- Optional AWS Direct Connect

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Universal CPE (ENCS)

Example Co-Managed Ownership

MSP

- Procure HW and WAN links
- Deploy and onboard uCPE
- Deploy Virtual WAN Edge with day0 configuration (MSP-owned sections)
- Deploy optional Service Chain VNF(s) with day0 configuration

Tenant

- Customization of virtual WAN Edge configuration (Tenant-owned sections)
- Customization of Service Chain VNFs

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud-on-Ramp for CoLocation

Example Co-Managed Ownership

MSP

- Procure HW and WAN links
- Deploy and onboard Co-Location cluster
- Deploy Virtual WAN Edge with day0 configuration (MSP-owned sections)
- Deploy optional Service Chain VNF(s) with day0 configuration

Tenant

- Customization of virtual WAN Edge configuration (Tenant-owned sections)
- Customization of Service Chain VNFs

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security

SDWaaS Security
Example Co-Managed Ownership

MSP

- Shared infra security
  - Access control, data protection, etc
- Tenant separation / isolation
- SD-WAN infra security
  - CA, device whitelist, pairwise keys, etc
  - Device system hardening
- Deployment of managed security services

Tenant

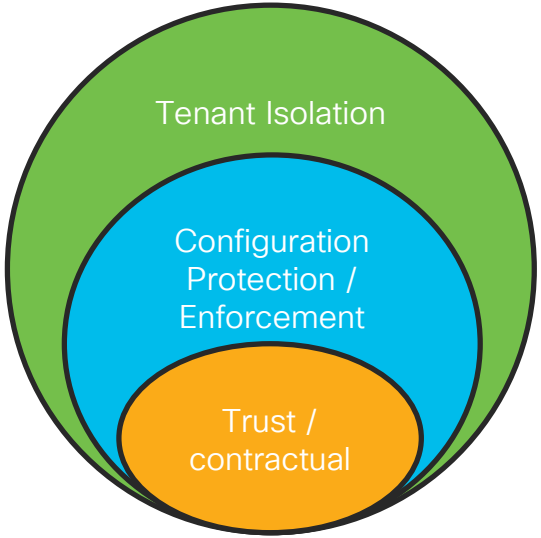
- SD-WAN overlay security:
  - Branch security services (Ent-FW, AMP,..)
  - Cloud-based security services (Umbrella, Zscaler, etc)
- Customization of managed security services

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Infrastructure Security

Tenant Protection / Separation

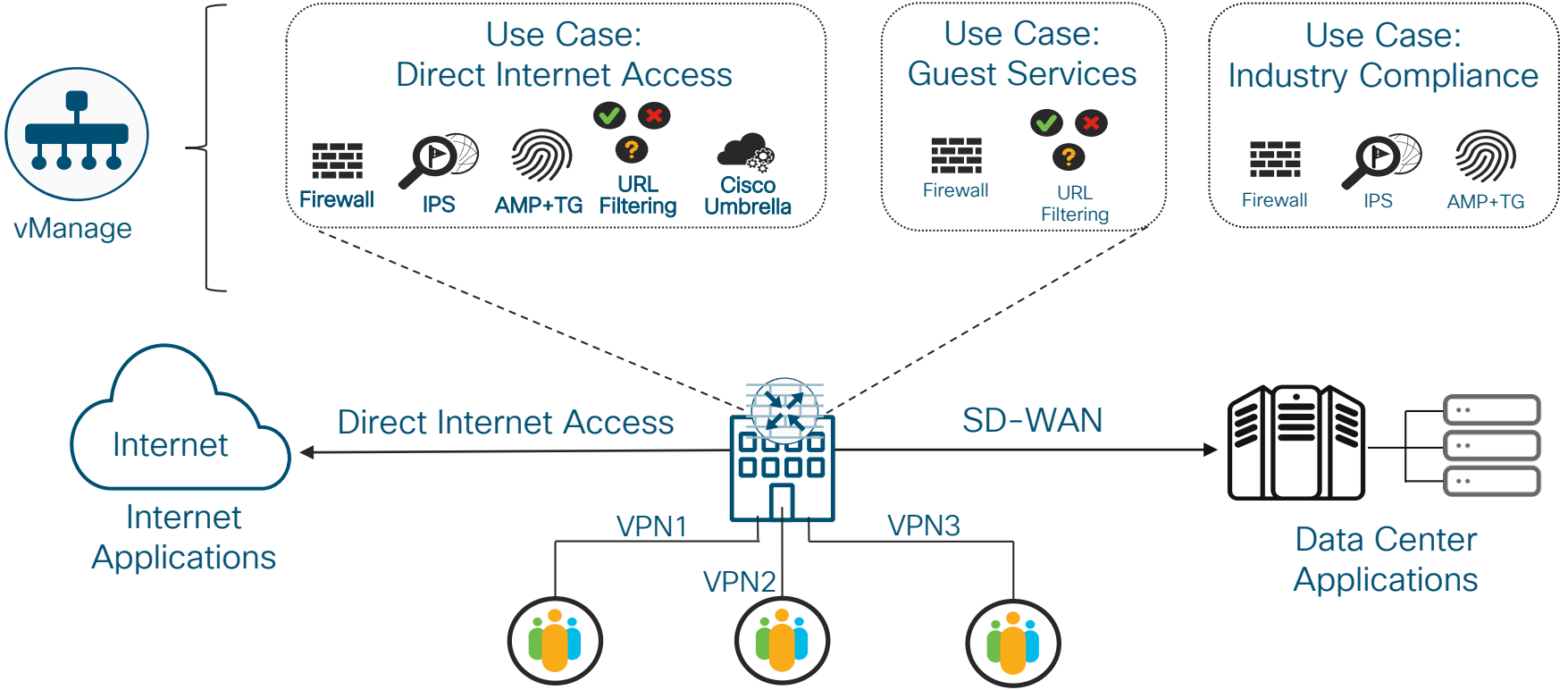
- Tenant isolation
  - Shared Infrastructure hardening to isolate tenants
- Configuration Enforcement
  - (future) Granular RBAC
  - Configuration verification check: periodic, or triggered by change notification from vManage
  - API gateway to enforce tenant access rights
- Trust / Contractual
  - MSP/Tenant role separation



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Edge Security Use-Cases

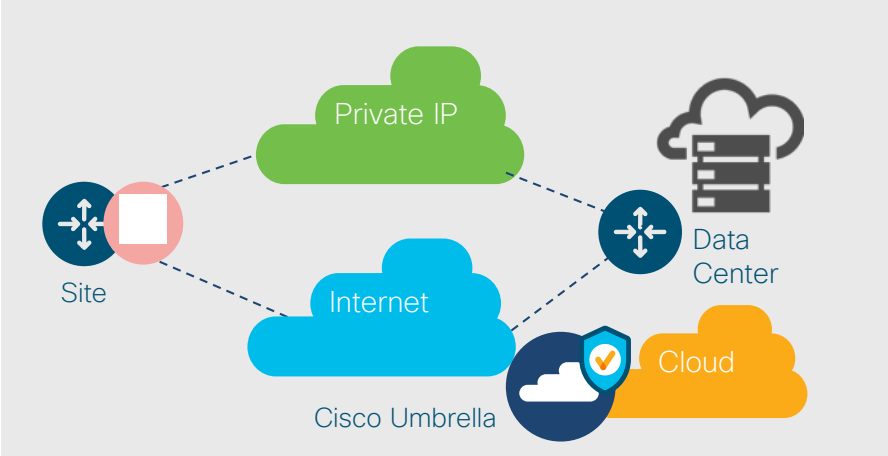
Under Tenant control in Co-Managed approach

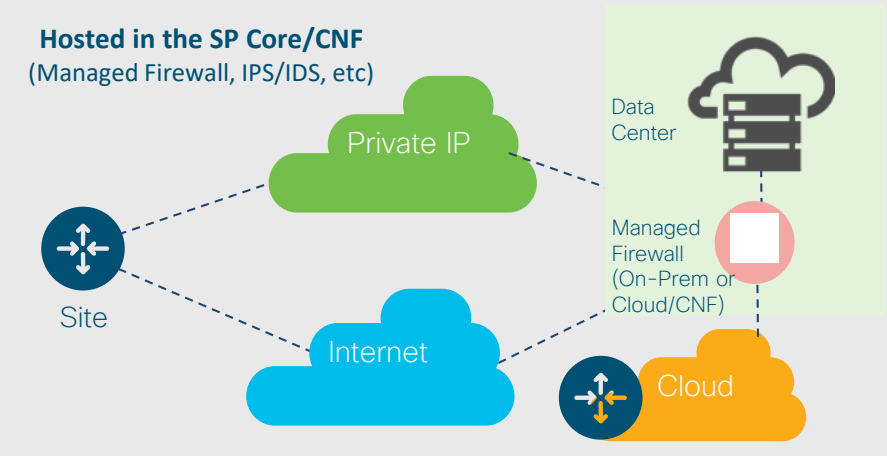


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Managed Network Security

Hosted On-Prem or Cloud Security Features





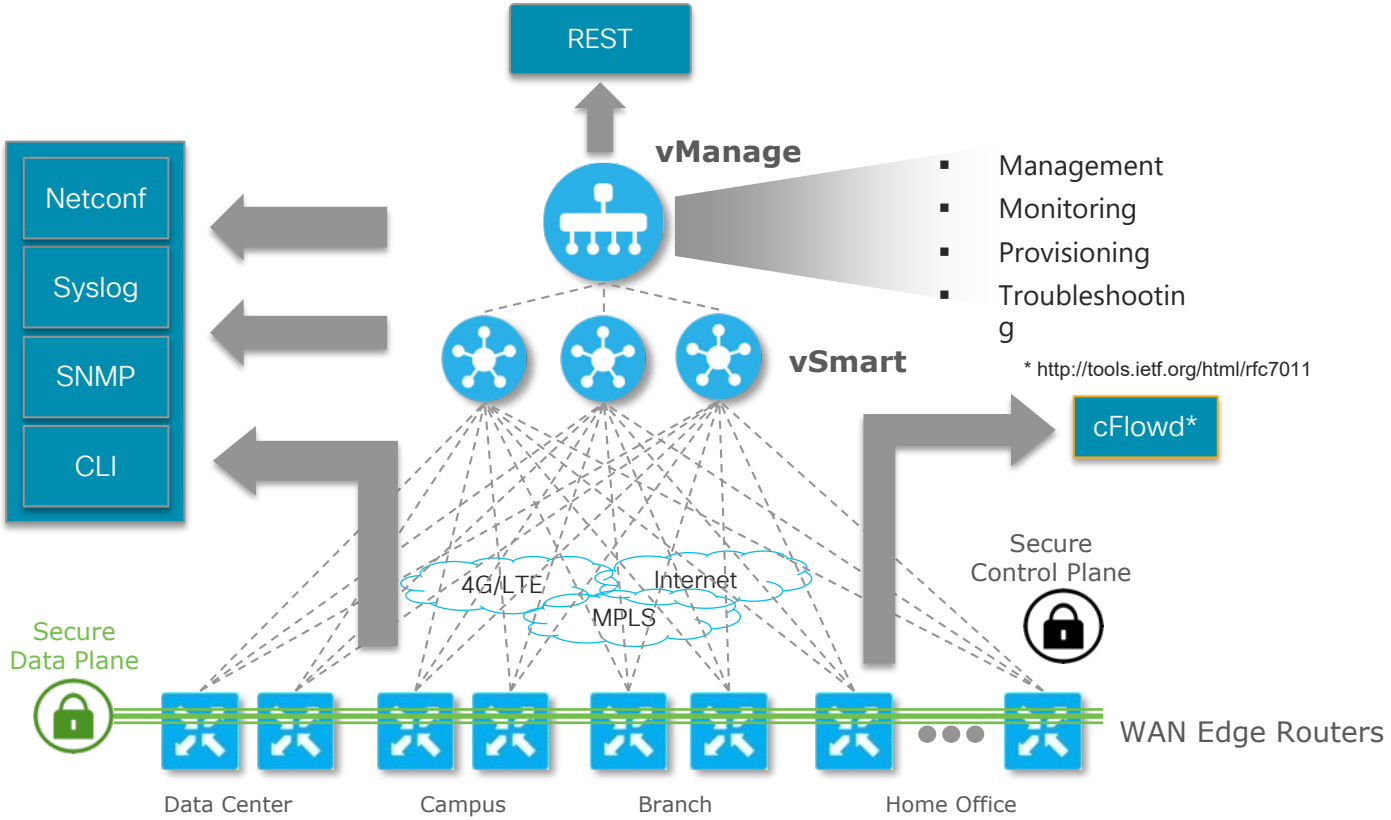
Hosted On-Premises
(Managed Firewall, IPS/IDS, etc)
Cloud-based Security with DIA

Hosted in the SP Core/CNF
(Managed Firewall, IPS/IDS, etc)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Operations

SD-WAN Management & Monitoring



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SDWaaS Operations
Example Co-Managed Ownership

MSP

- Management Connectivity
  - WAN Edges, uCPE, etc
- Infra/underlay/network monitoring
  - Events, stats, network SLA
  - Incident Management and Troubleshooting
- Change Management
  - Infra, upgrades, controller scaling
- VNF Lifecycle management
  - Backup & restore

Tenant

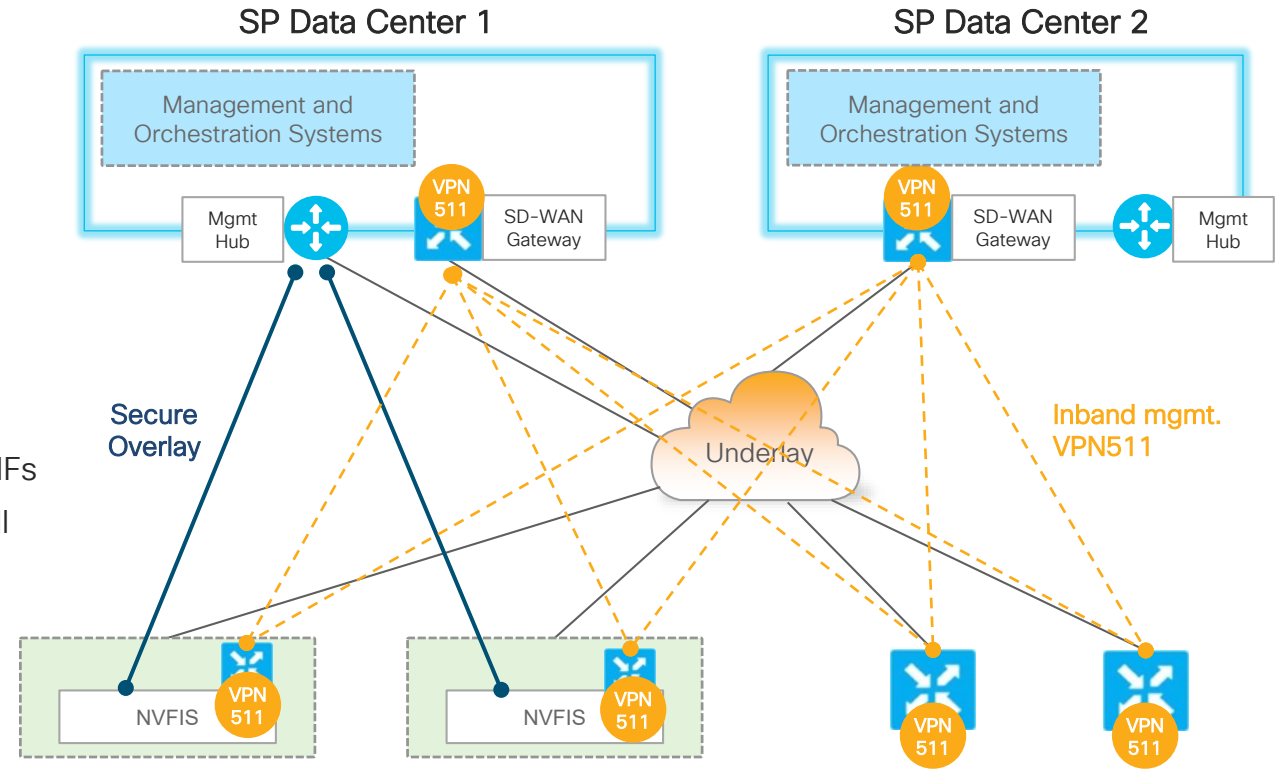
- VPN Service Monitoring
  - Apps SLA, QoS, events, stats
  - Incident Management and Troubleshooting
- Change Management
  - Configurations, policies
- Migration
  - Coordination with MSP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Management Connectivity

WAN Edges and uCPE

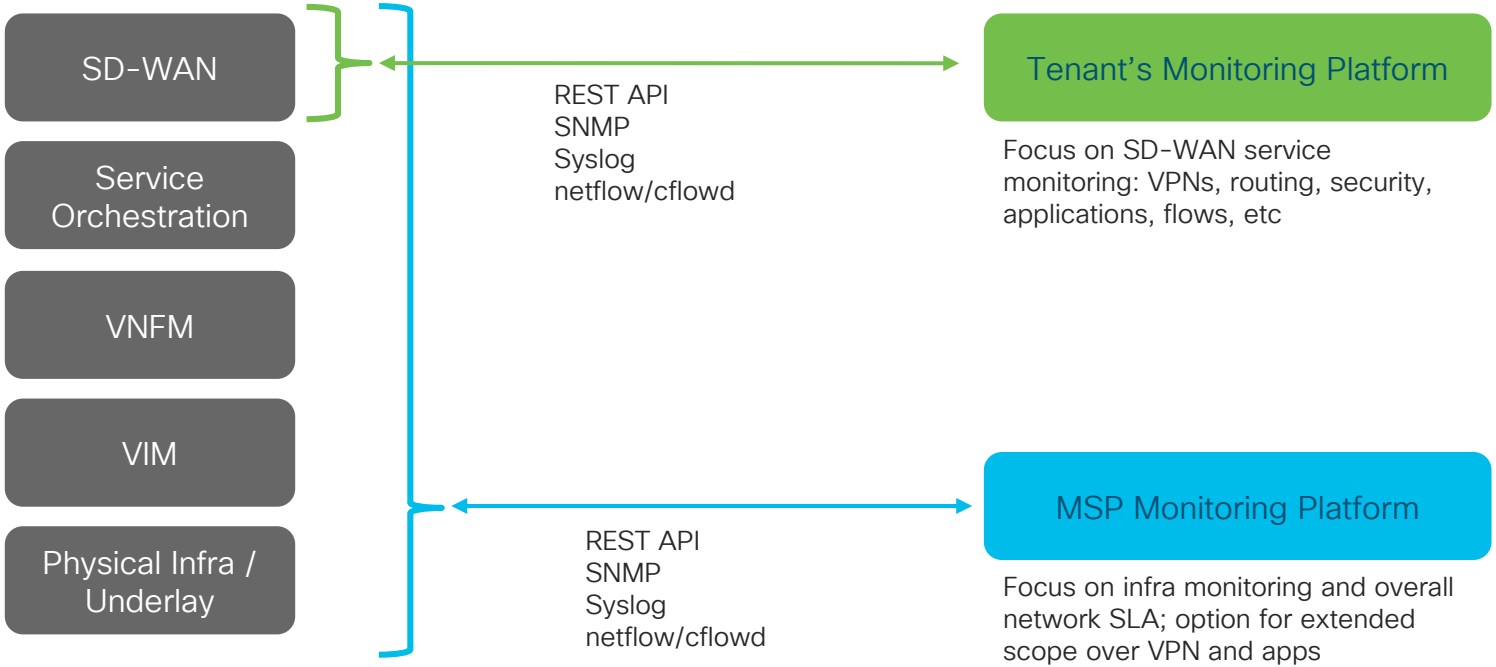
- Inband Management VPN
  - Dedicated for WAN Edge management traffic, including virtual WAN Edges on NFVIS
  - Requires SD-WAN control and data policies; MSP <-> Tenant coordination
- NFVIS Secure Overlay
  - IPSec tunnel
  - Mgmt access to NFVIS and VNFs
  - Outside of SD-WAN Fabric, full MSP control



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SDWaaS Monitoring

Co-Managed Roles



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco vAnalytics

Network Centric

- Site Availability
- Network Availability
- Site Usage Analysis
  - Top sites by bandwidth consumption
  - Historical bandwidth consumption
- Carrier Performance
  - Approute stats on a per-carrier basis
  - Carriers health ranking

Application/Flow Centric

- Based on DPI and cflowd
- Bandwidth Usage
  - Top sources, destinations, apps
  - Per-Site basis
- Application Performance
  - Application to tunnel binding and performance information
- Anomaly Detection
  - Baseline of application usage
  - Anomaly detection based on overall application usage (by application family, by site)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaways

Co-Managed SD-WAN – Takeaways

- Intermediate approach for managed service
- Tenant benefits: Increased flexibility and control
- MSP benefits: narrowed focus, easier to re-use and scale
- Closer collaboration required

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete your online session survey

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

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

cisco Live!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Applying the shared responsibility model to managed SD-WAN...

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

You make **possible**