



设计部署SD-WAN网络

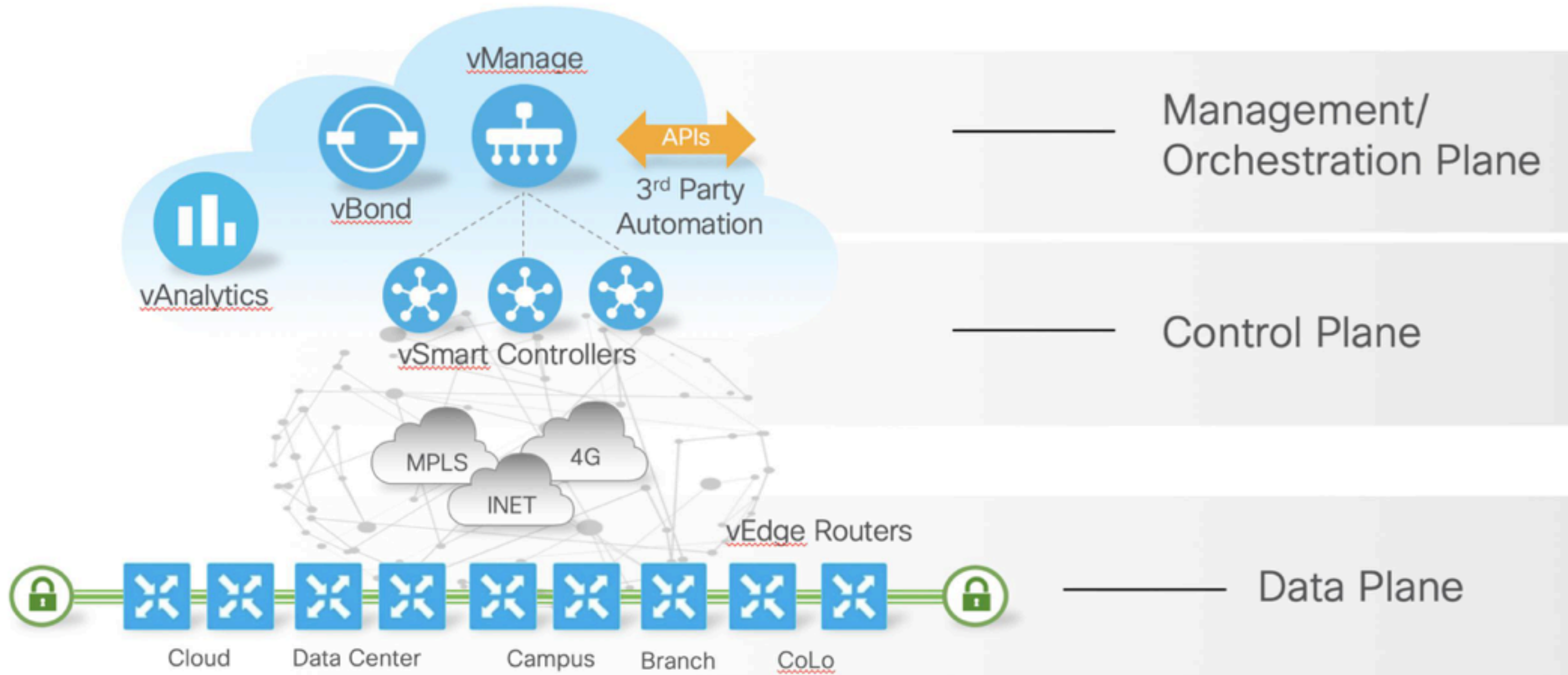
Qiuyong Wang

Technical Solutions Specialist

Enterprise Network

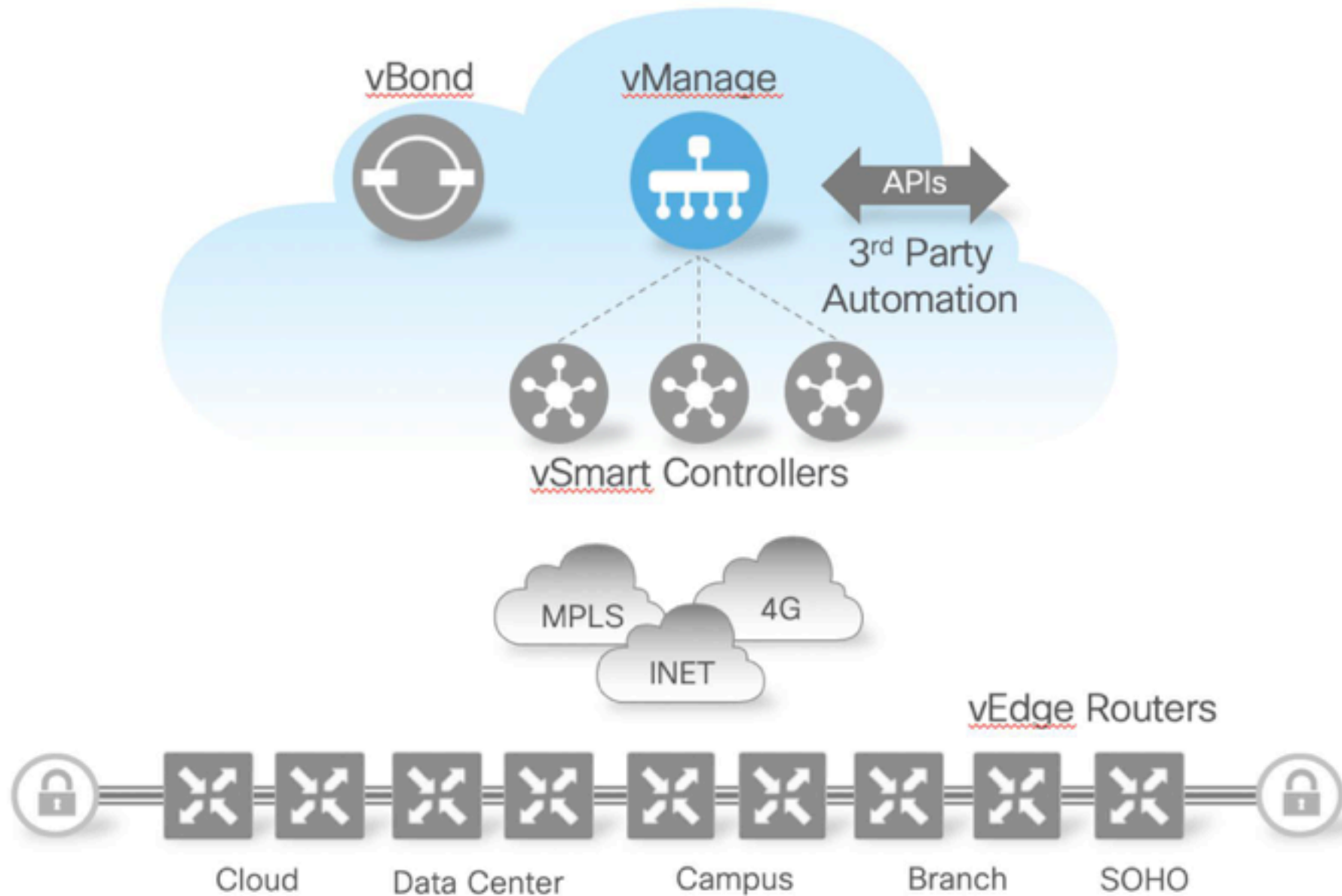
SD-WAN Component

Cisco SD-WAN Architecture Overview



Cisco SD-WAN Architecture Overview

Management Plane - vManage

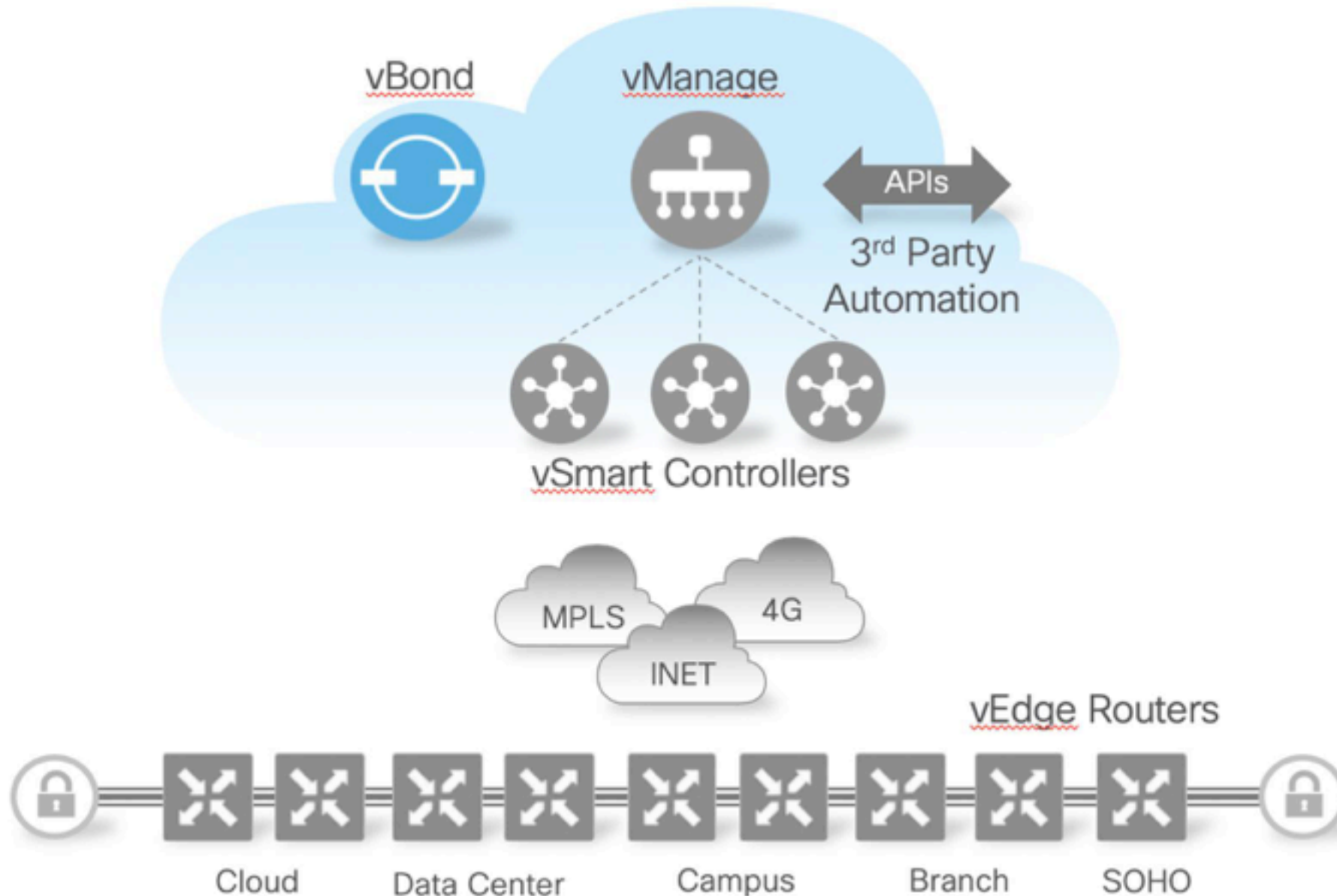


vManage

- Single pane of glass for Day0, Day1 and Day2 operations
- Centralized provisioning, monitoring and troubleshooting
- Multitenant or single tenant
- Policies and Templates
- RBAC
- Programmatic REST API

Cisco SD-WAN Architecture Overview

Orchestration Plane - vBond

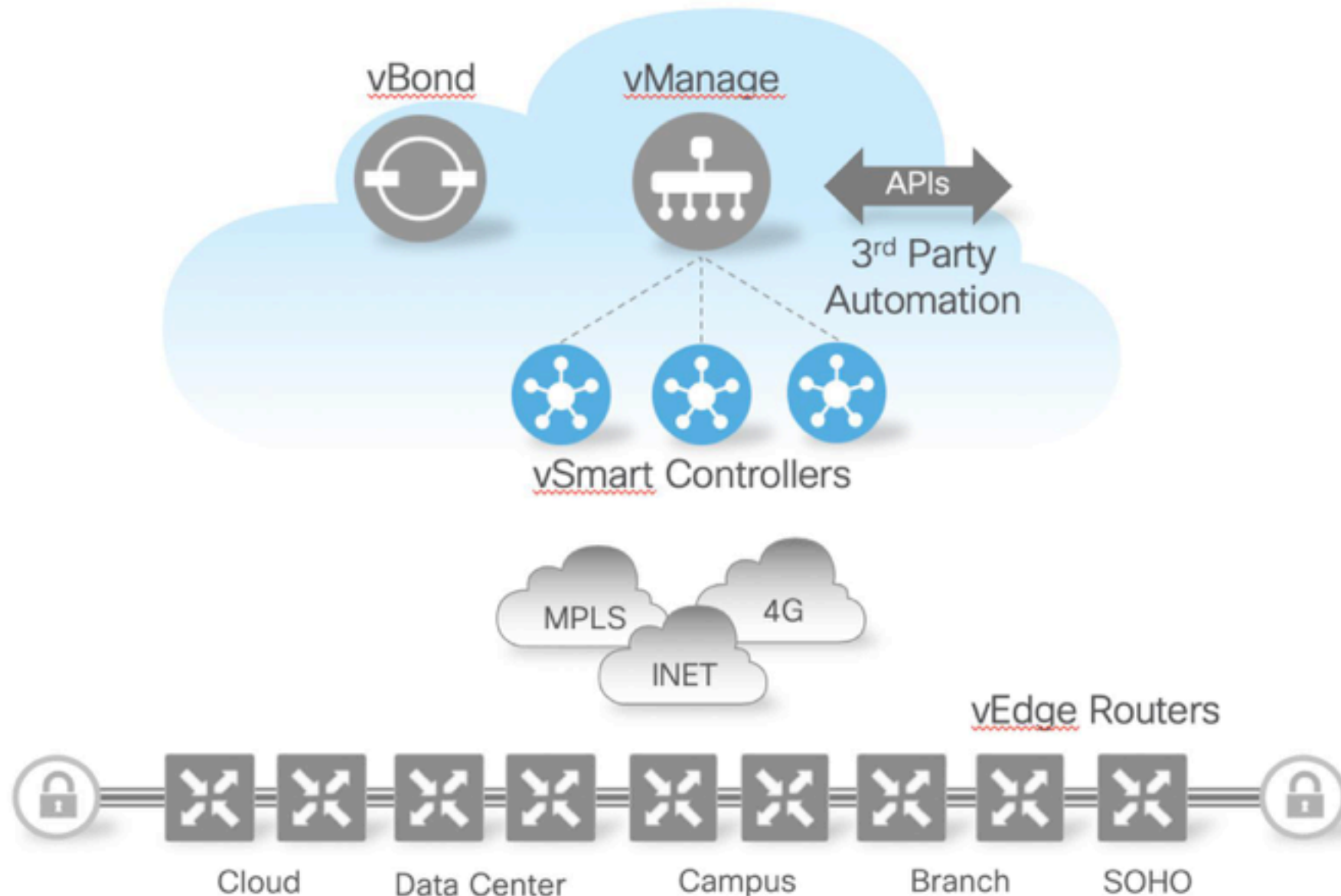


vBond

- Orchestrates control and management plane
- First point of authentication
- Distributes list of vSmarts/vManage to vEdge routers
- Facilitates NAT traversal
- Requires universally reachable IP-Address/Port [Can reside behind Port-Forwarding]
- Multitenant or single tenant

Cisco SD-WAN Architecture Overview

Control Plane - vSmart

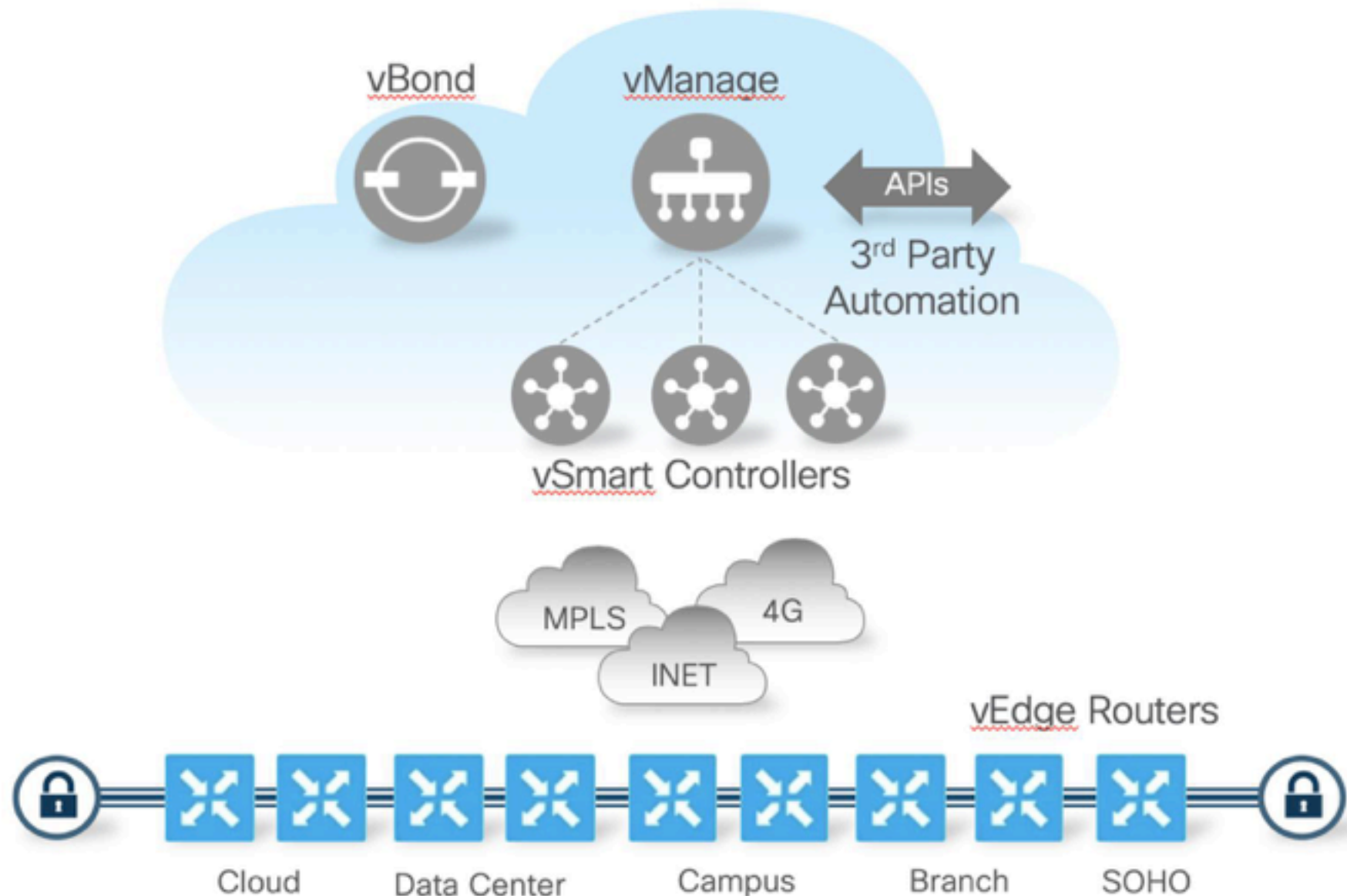


vSmart

- Facilitates fabric discovery
- Disseminates control plane information between vEdges
- Distributes Data Plane policies to vEdge routers
- Implements control plane policies

Cisco SD-WAN Architecture Overview

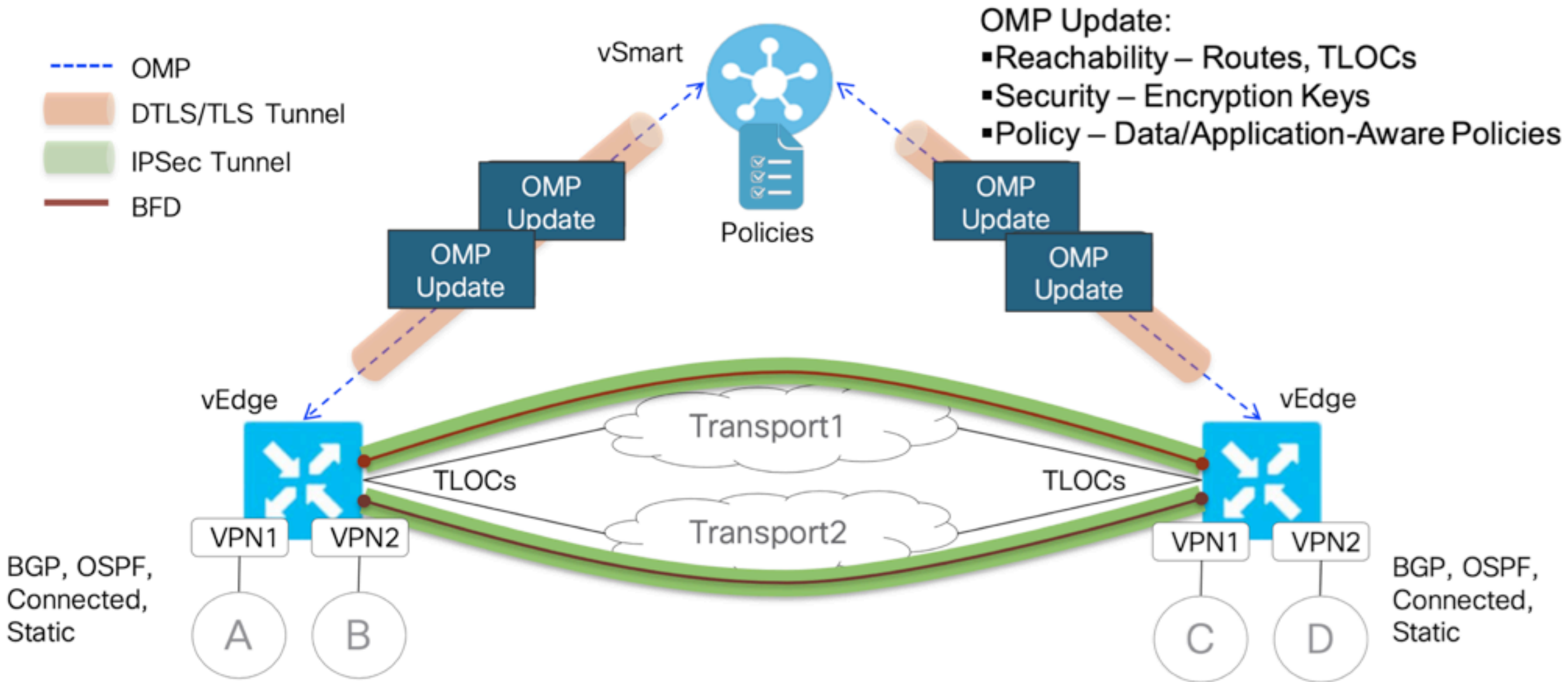
Data Plane - vEdge



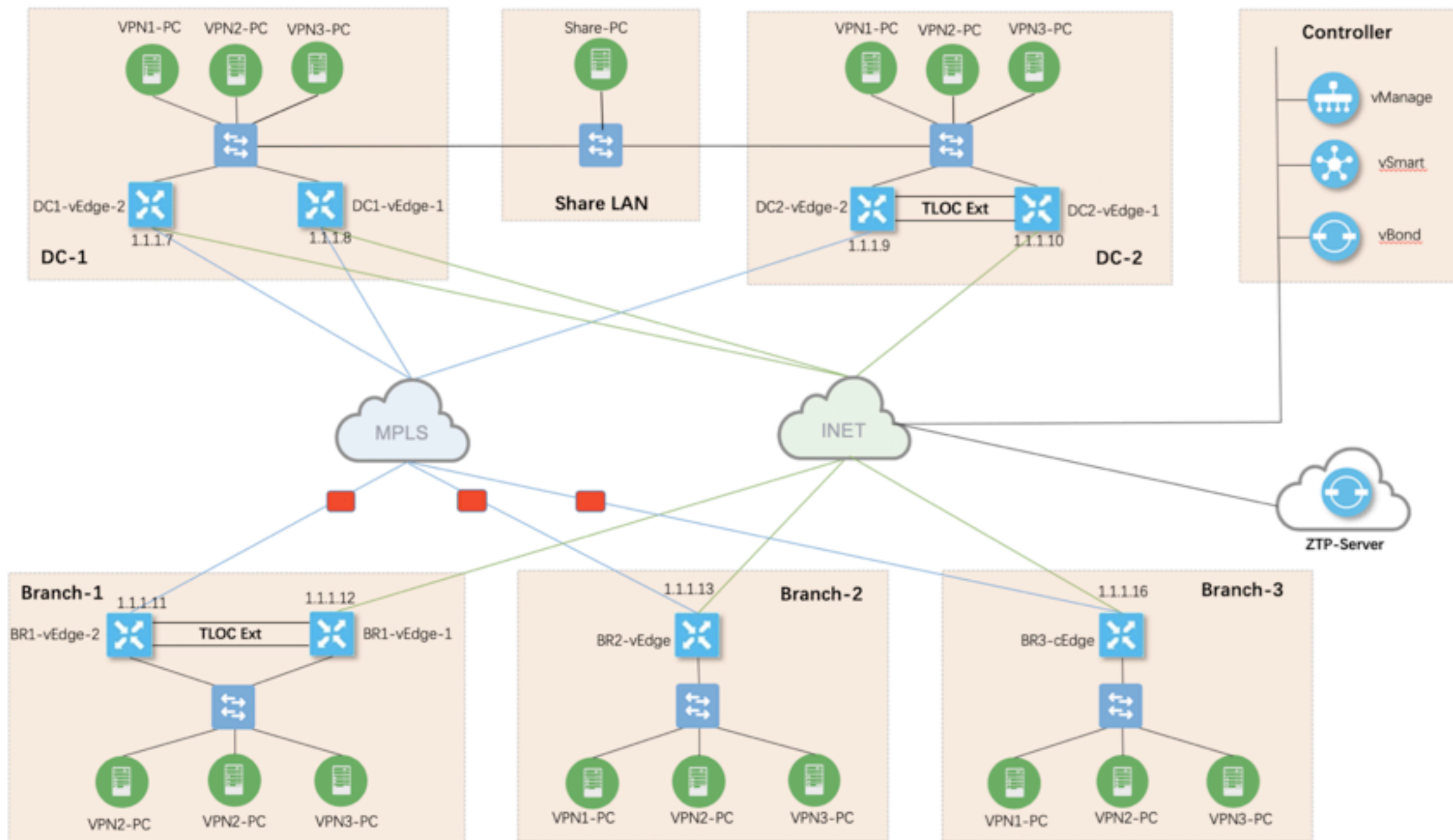
vEdge

- Secure data plane with remote vEdge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements Data Plane policies
- Supports Zero Touch Deployment
- Supports traditional routing protocols (OSPF, BGP) and First-hop Redundancy (VRRP)
- Physical or Virtual

Building the overlay fabric



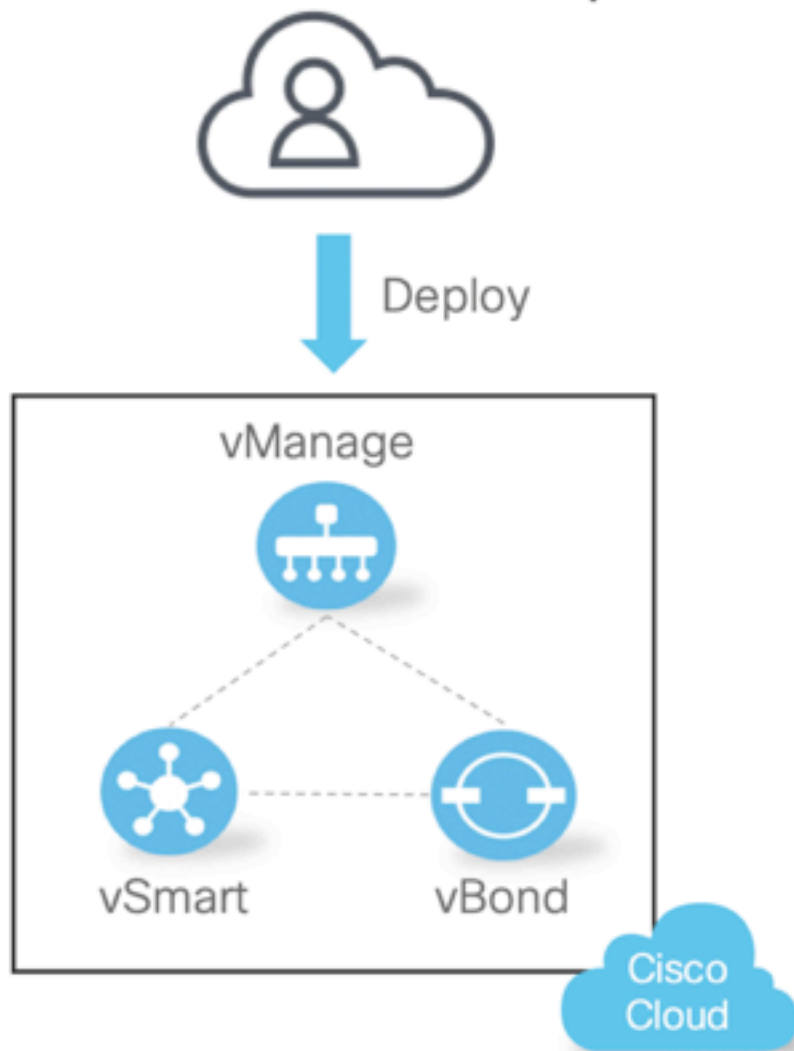
Building the overlay fabric



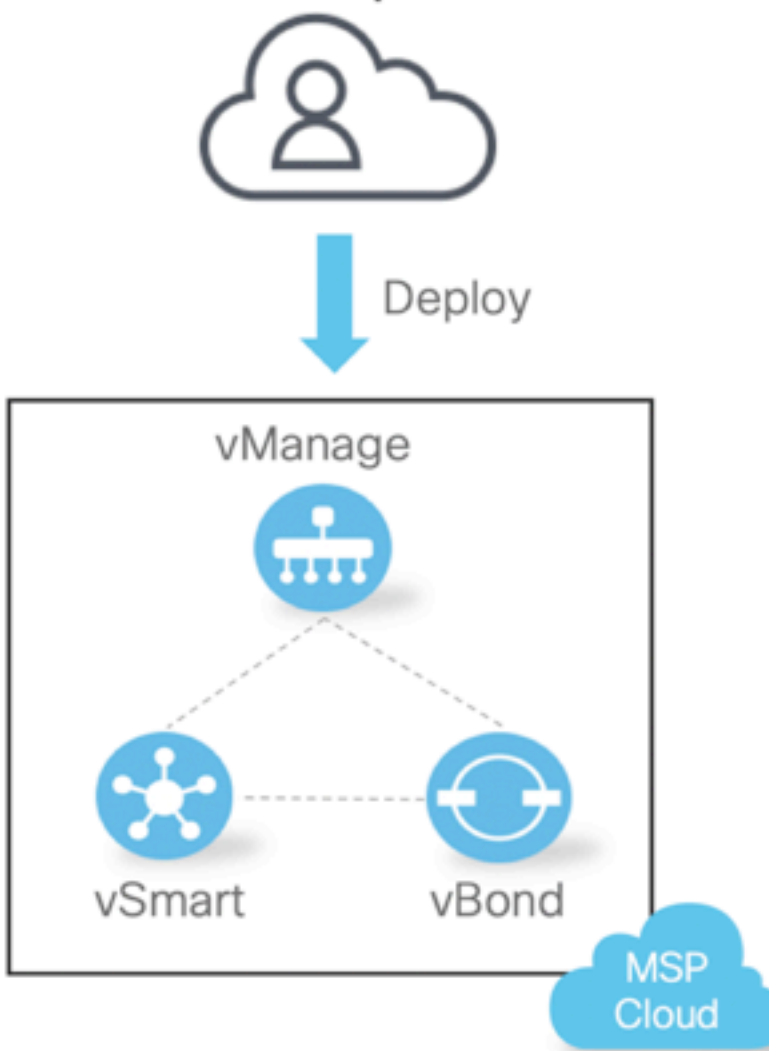
SD-WAN Deployment Model

Controller Deployment Models

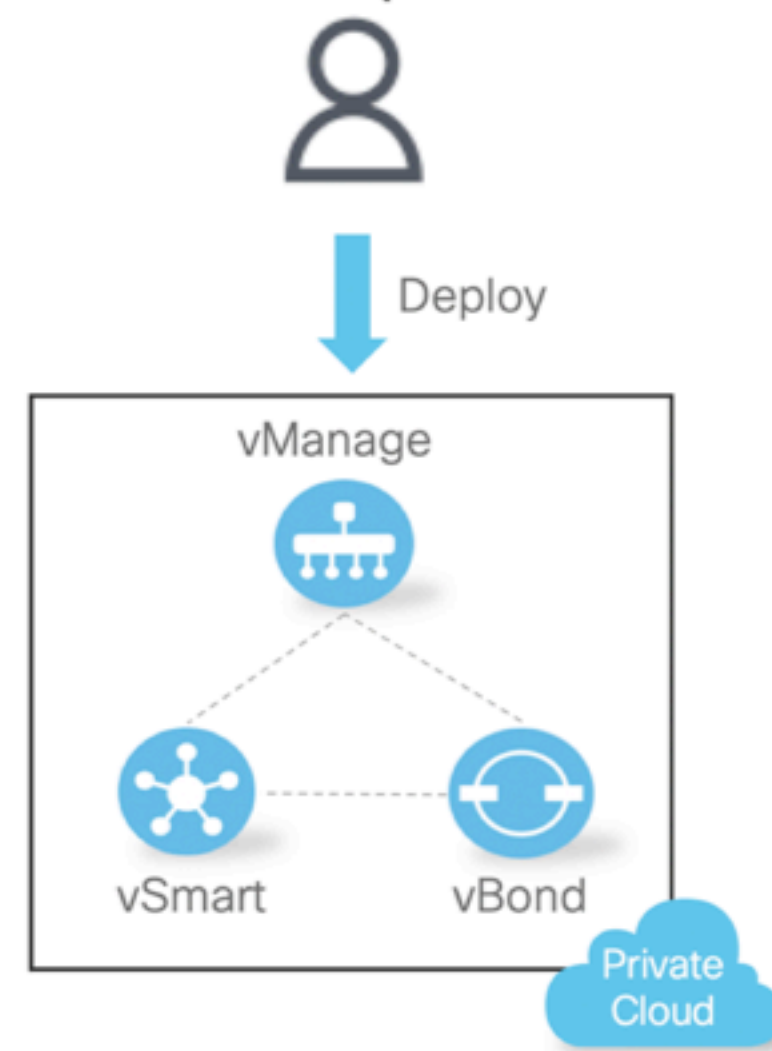
Cisco Cloud Ops



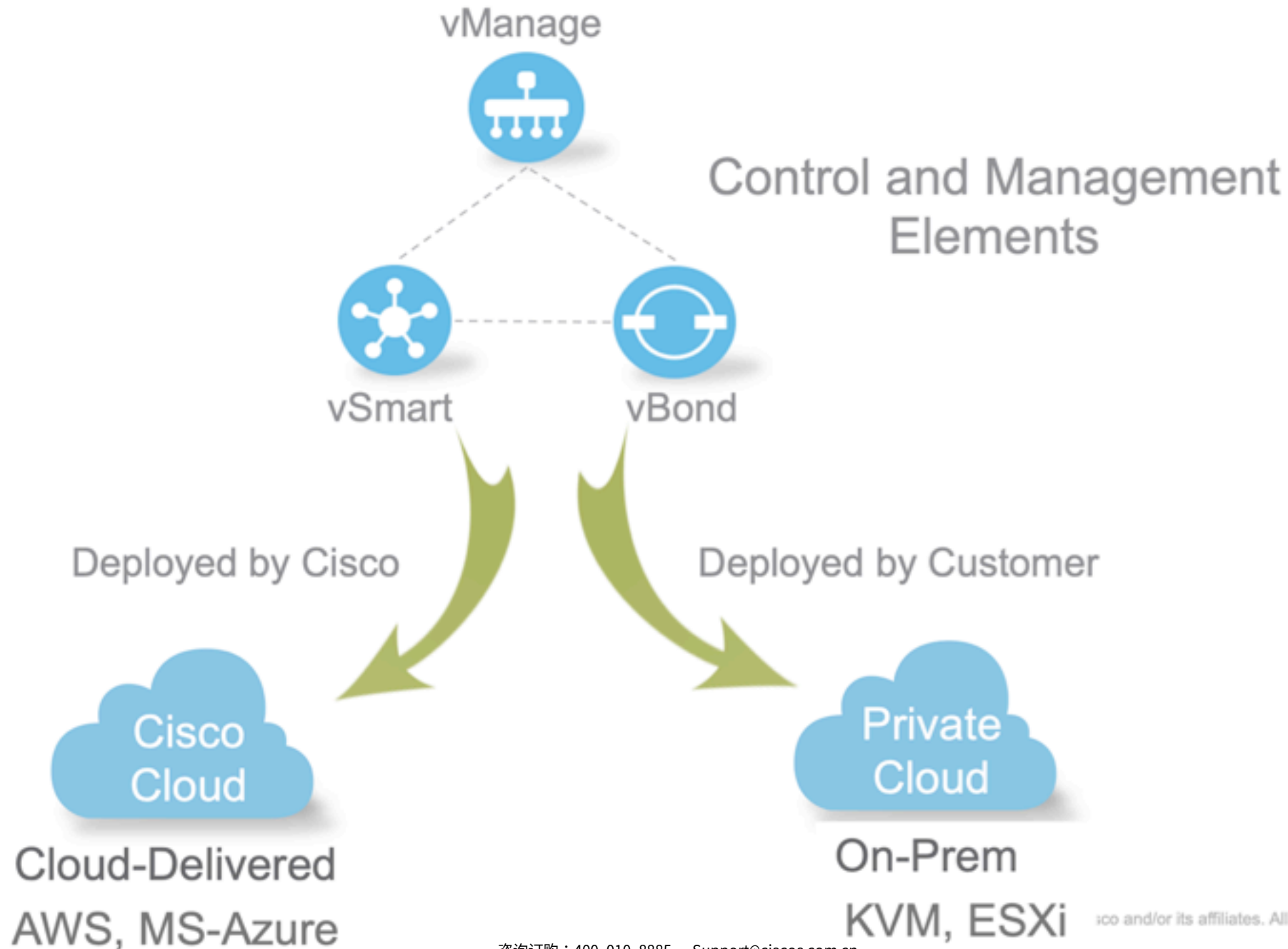
MSP Ops Team



Enterprise IT

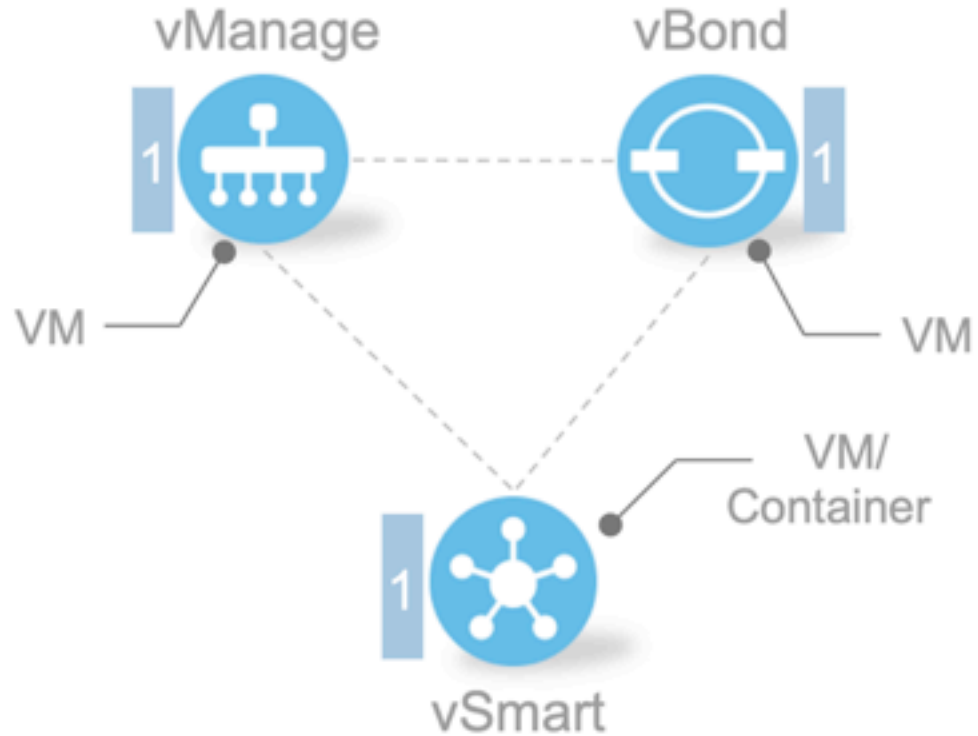


Controller Deployment Models

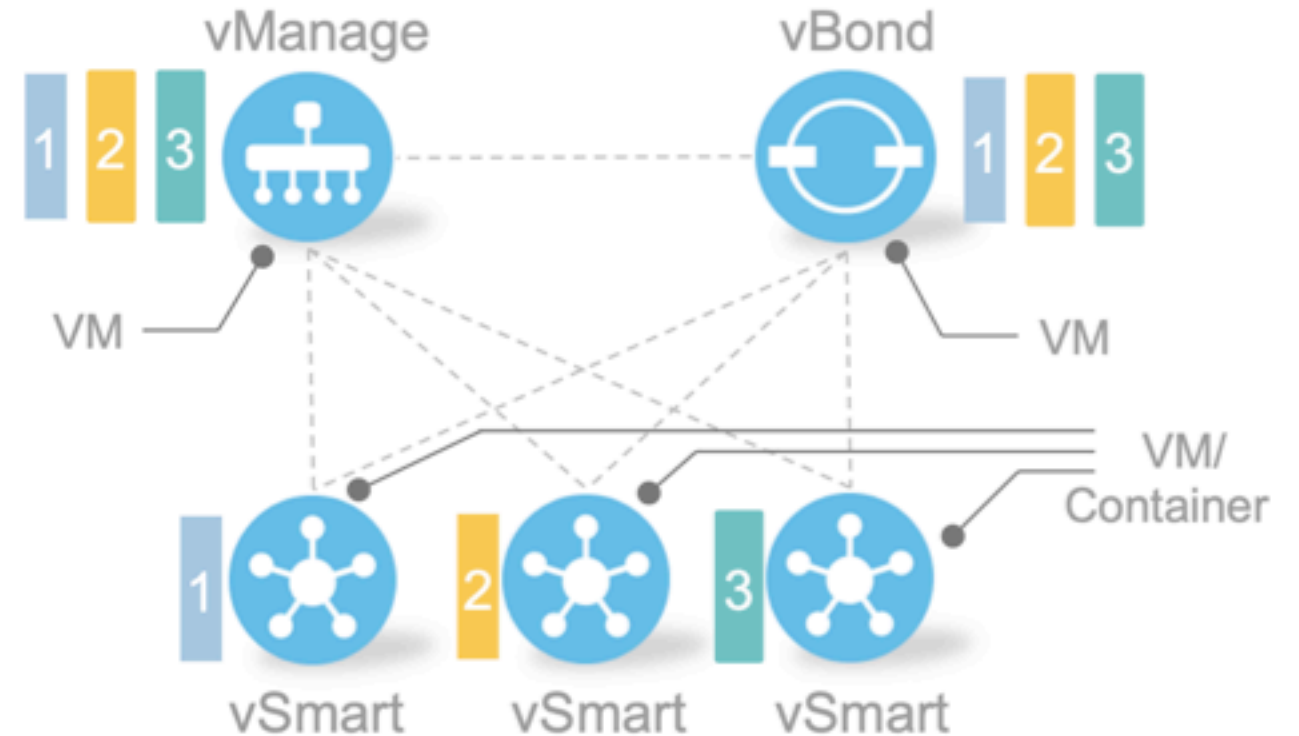


Controller Tenancy

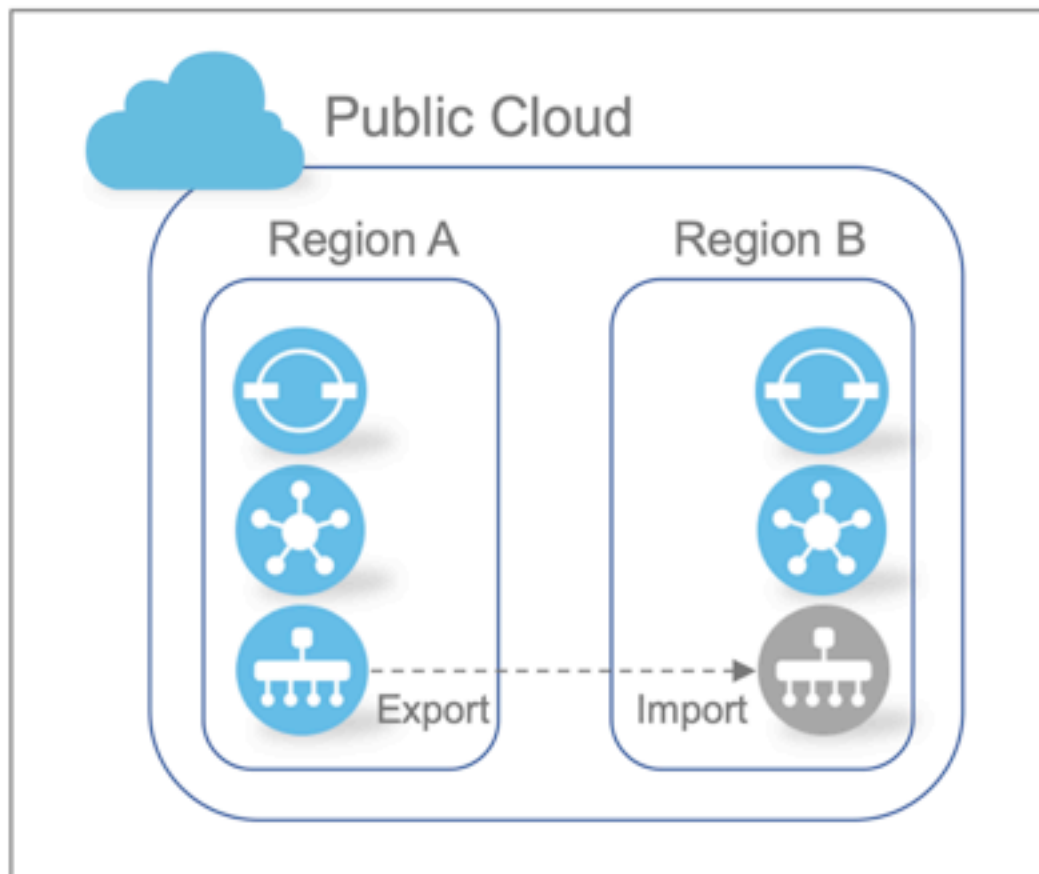
Single Tenant



Multi Tenant



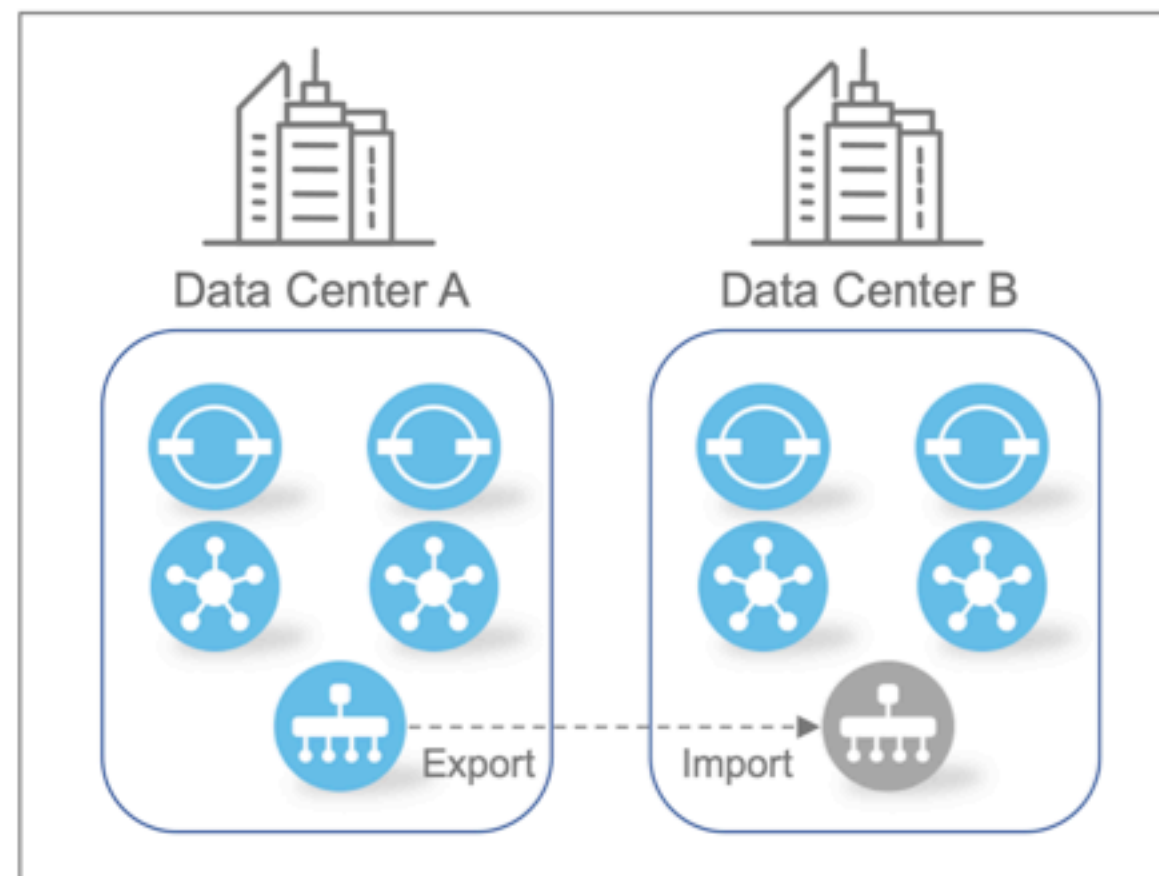
Controllers Redundant Deployment



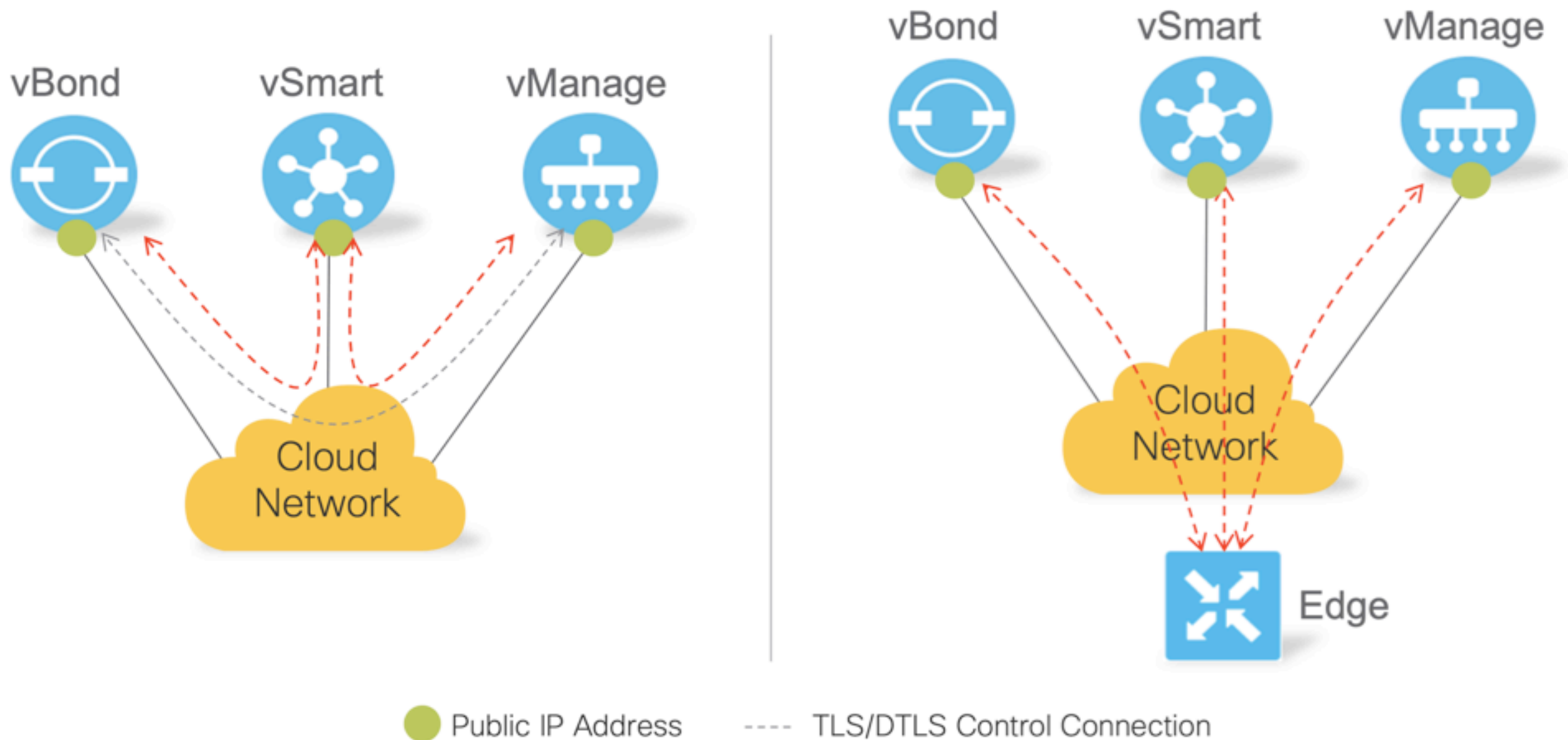
- Controllers are distributed across multiple public cloud regions
- Active-active, vManage is cold-standby



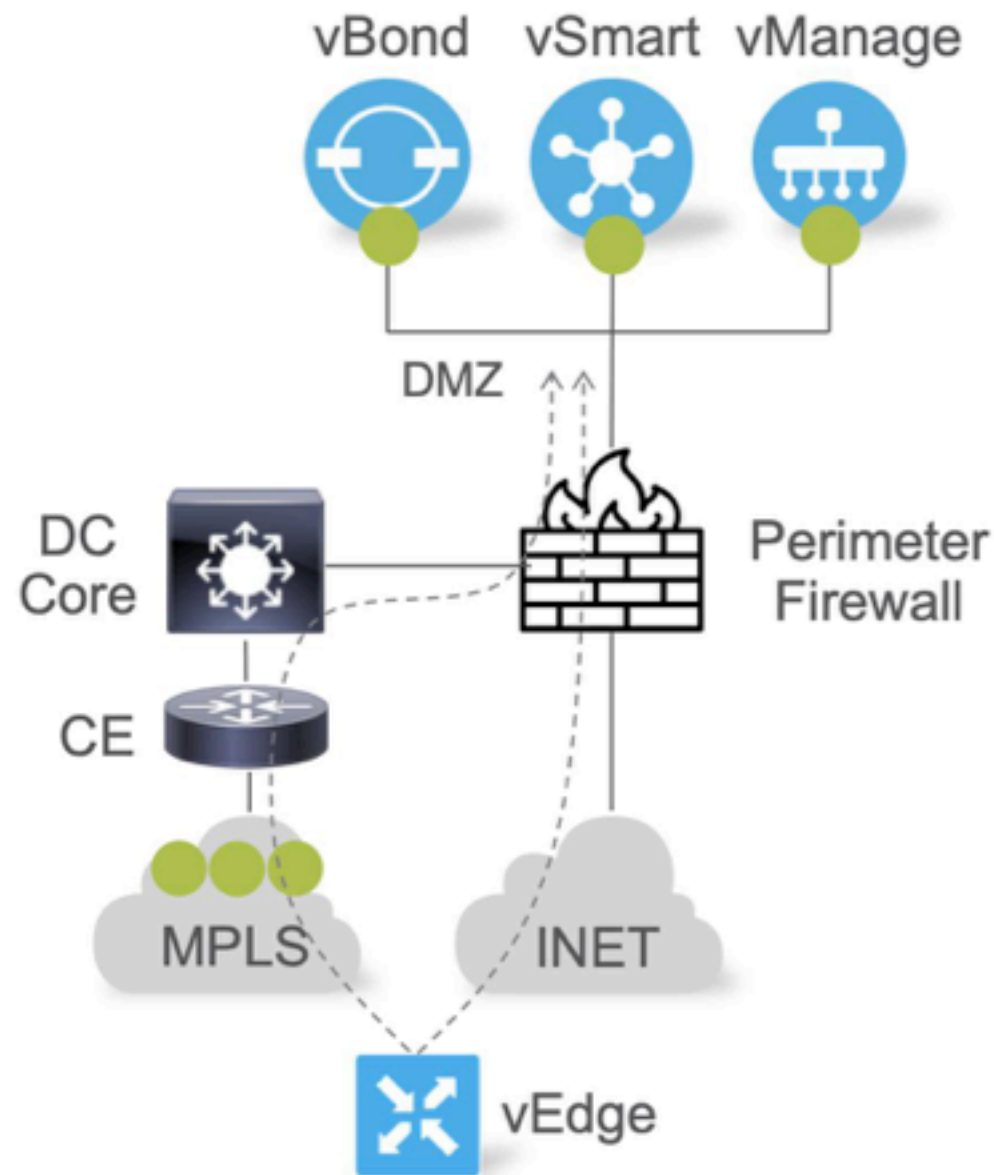
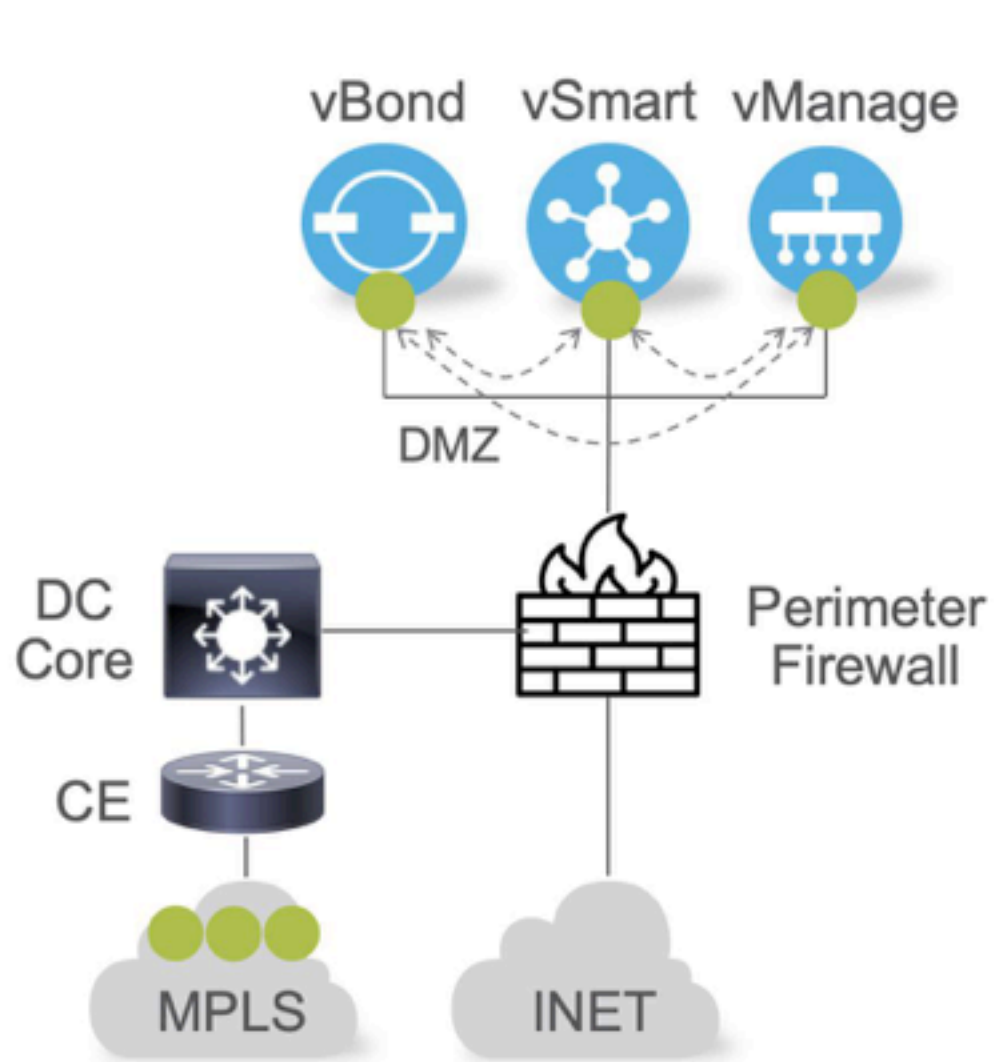
- Controllers are distributed across multiple private data centers
- Active-active, vManage is cold-standby



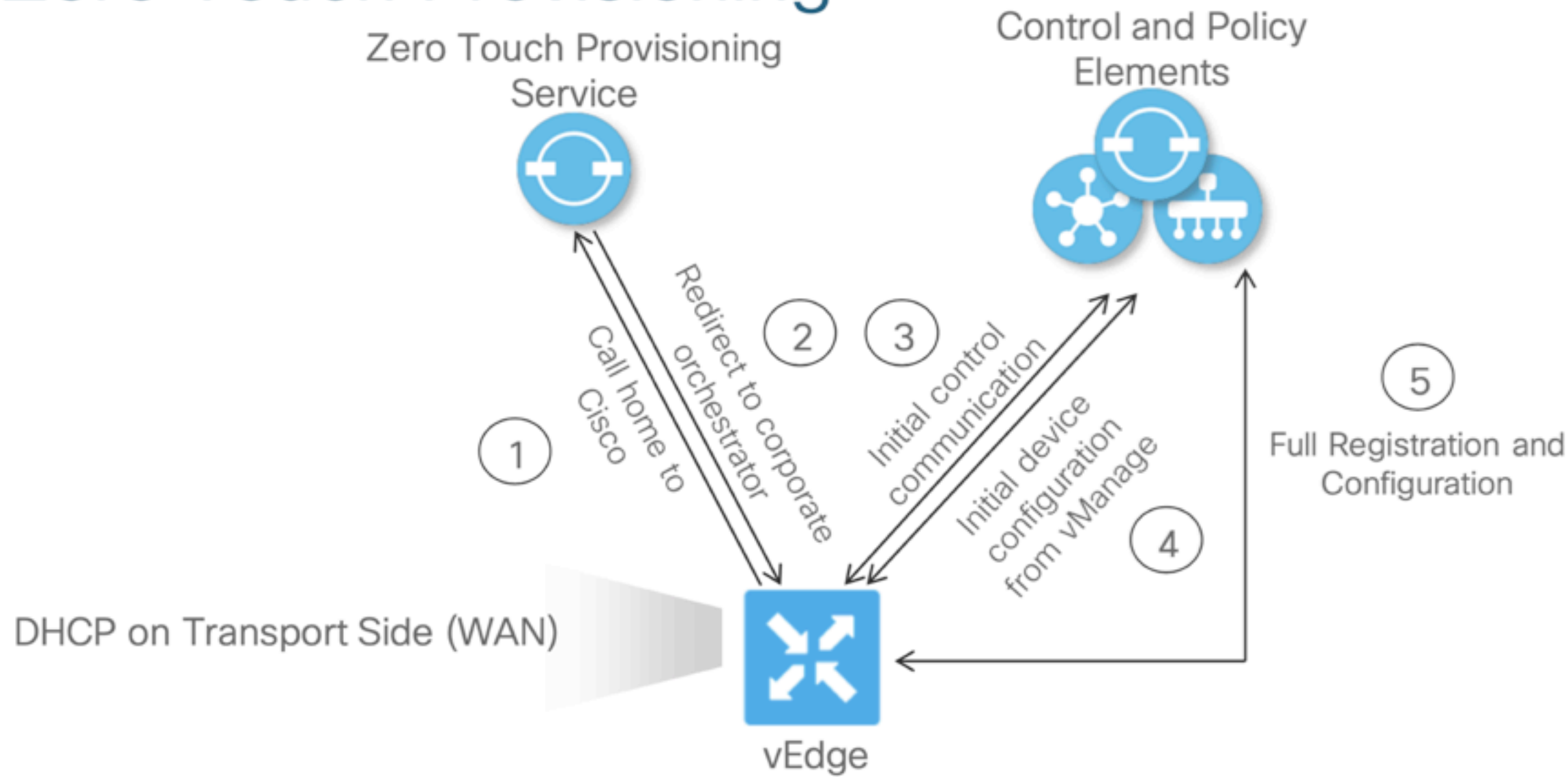
Cloud Controllers Connection



On-Prem Controllers Connections

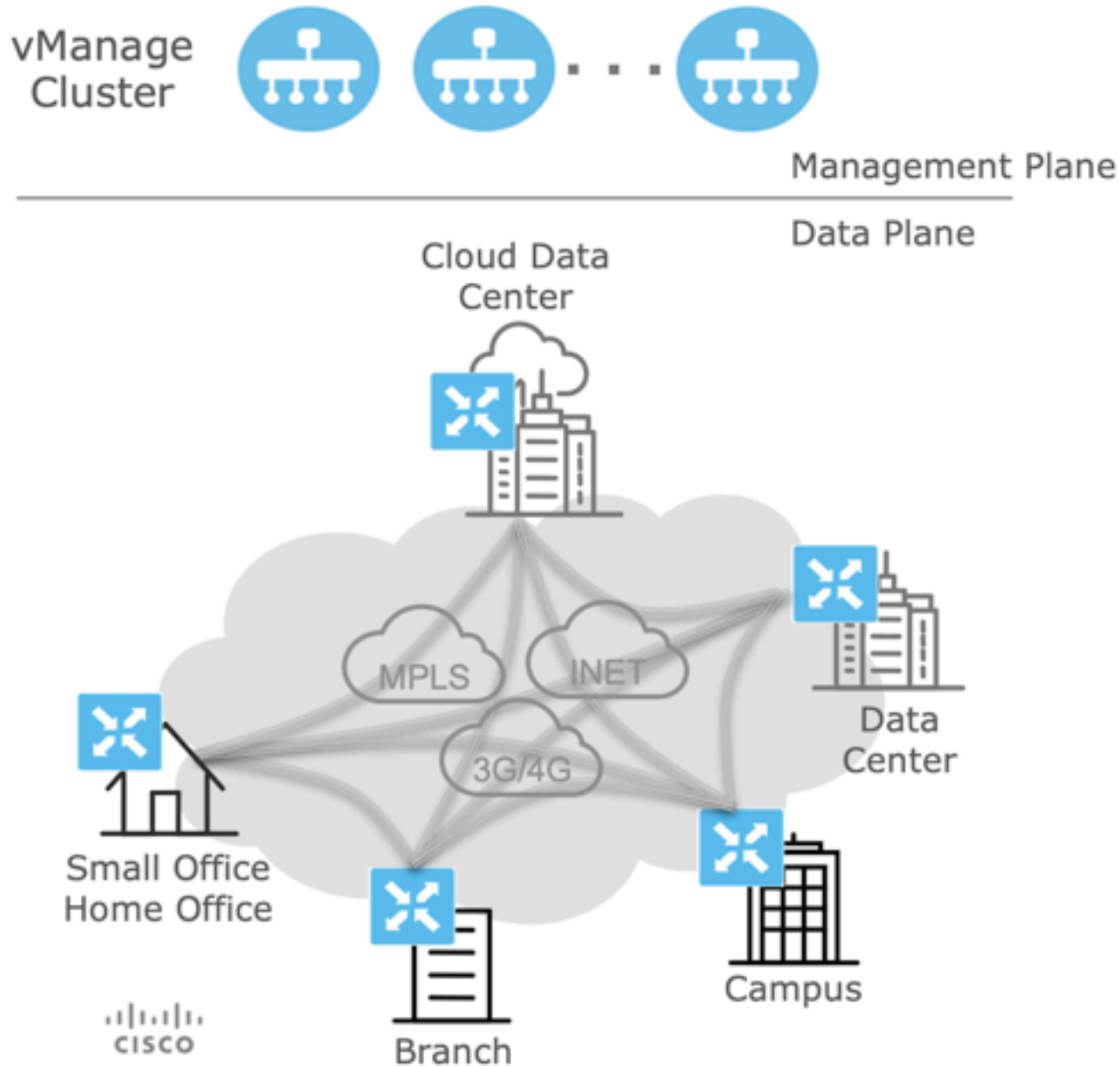


Zero Touch Provisioning



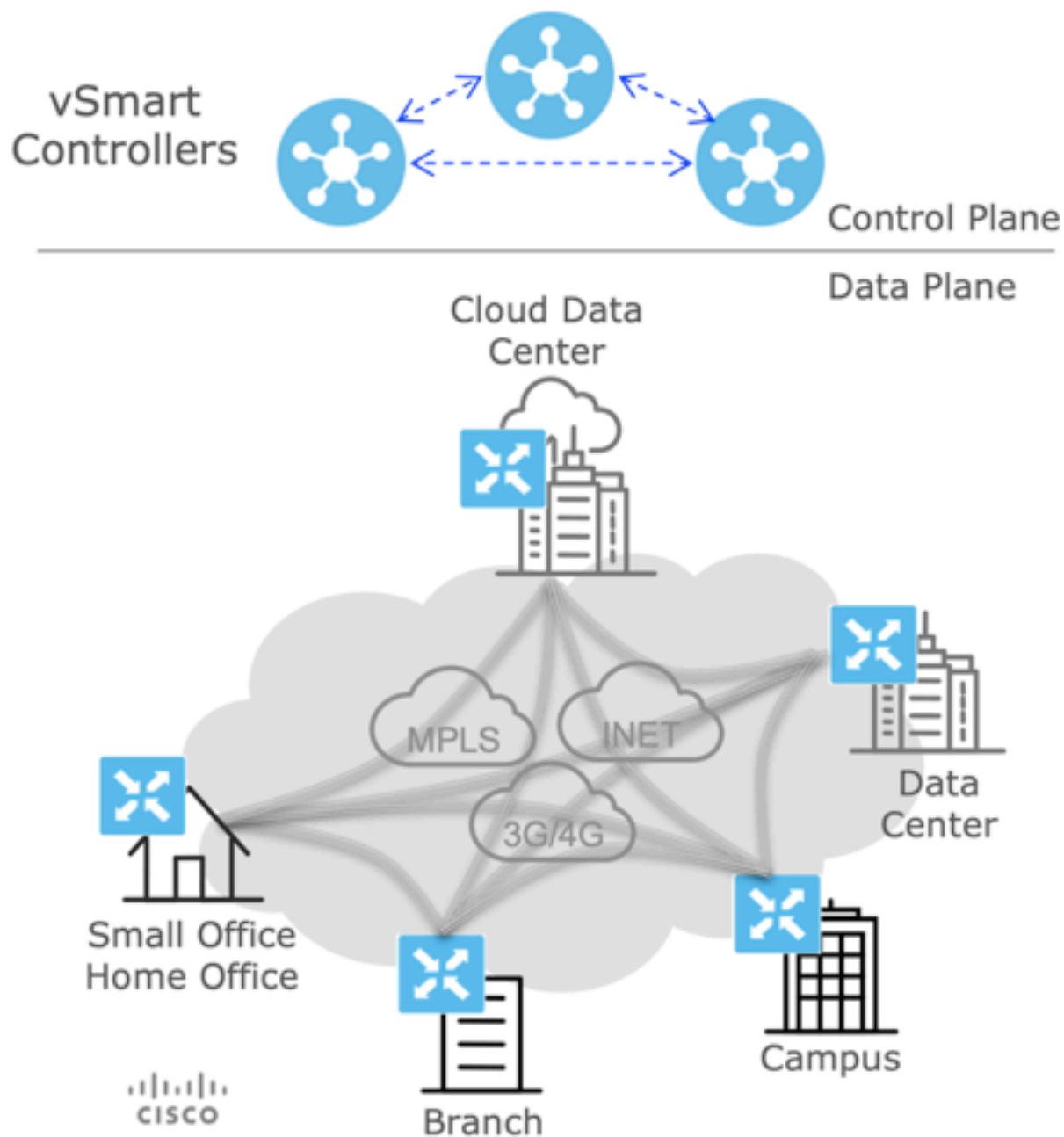
High Availability & Redundancy

Control Redundancy - vManage



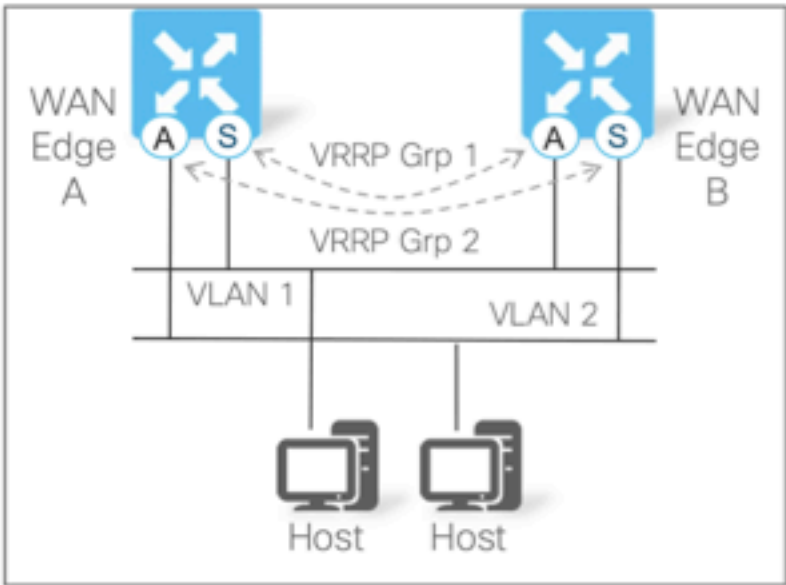
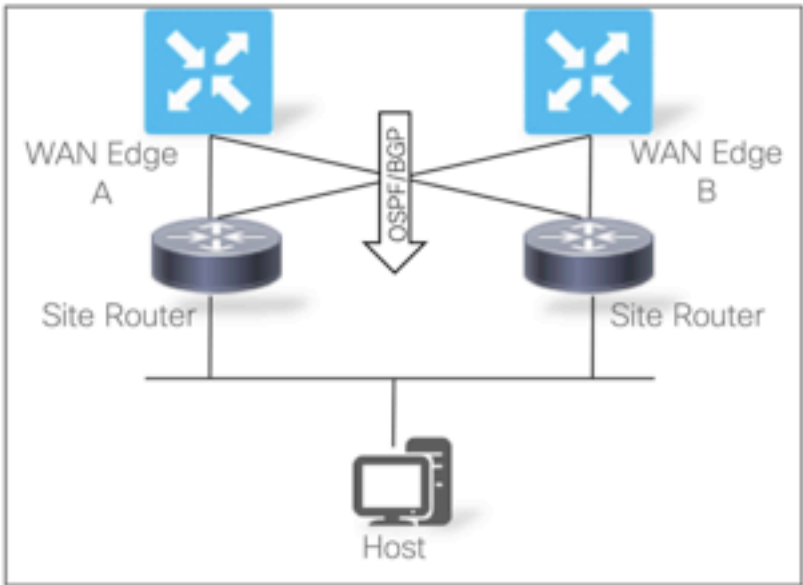
- vManage servers form a cluster for redundancy and high availability
- All servers in the cluster act as active/active nodes
 - All members of the cluster must be in the same DC / metro area
- For geo-redundancy, vManage servers operate in active/standby mode
 - Not clustered
 - Database replication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

Control Redundancy – vSmart & vBond

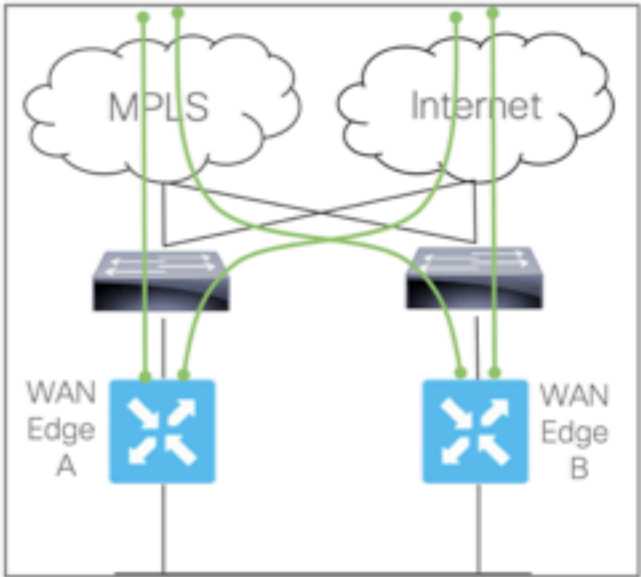
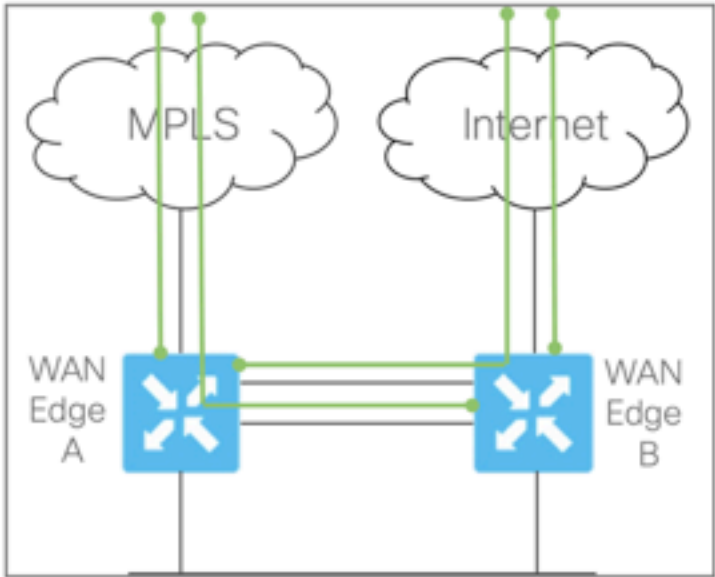
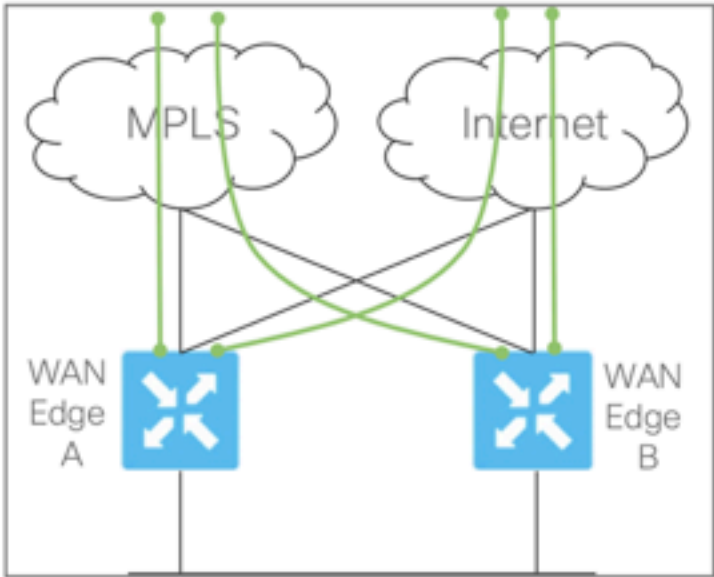


- vSmart controllers exchange OMP messages between themselves and they have identical view of the SD-WAN fabric
- vEdge routers connect to up to vSmart controllers for redundancy
- Single vSmart controller failure has no impact, as long as there is another vSmart controller vEdge routers are registered with
- If all vSmart controllers fail or become unreachable, vEdge routers will continue operating on a last known good state for a configurable amount of time (GR timer)
 - No updates to reachability
 - No IPSec rekey
 - No policy changes propagation

WAN Edge High Availability Scenarios

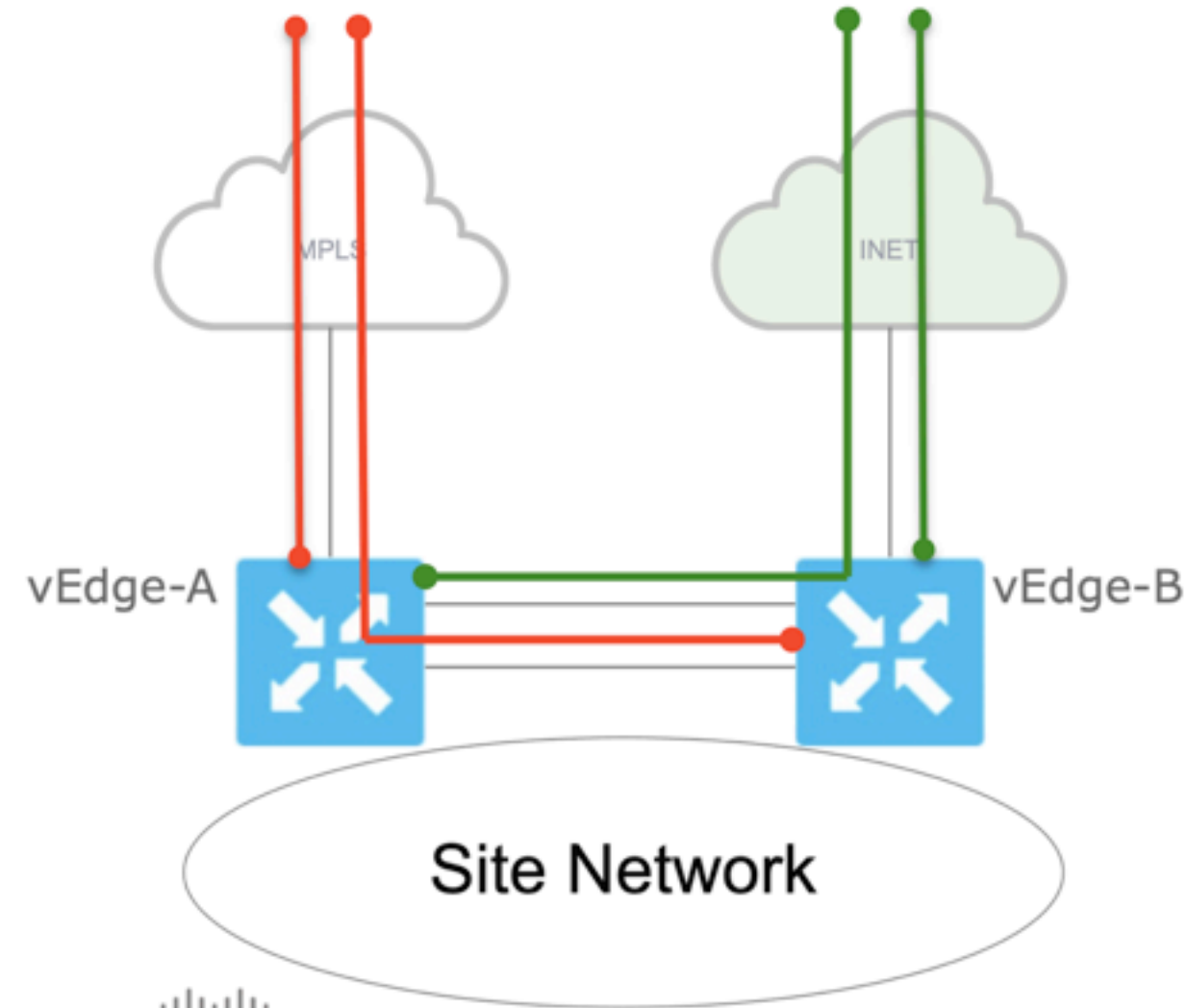


Service
Side



Transport
Side

Transport Redundancy – TLOC Extension



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

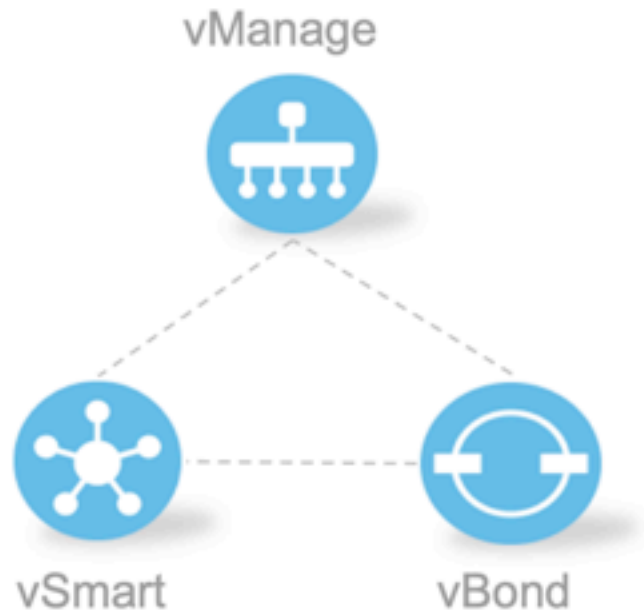
Migration

Migration Sequence

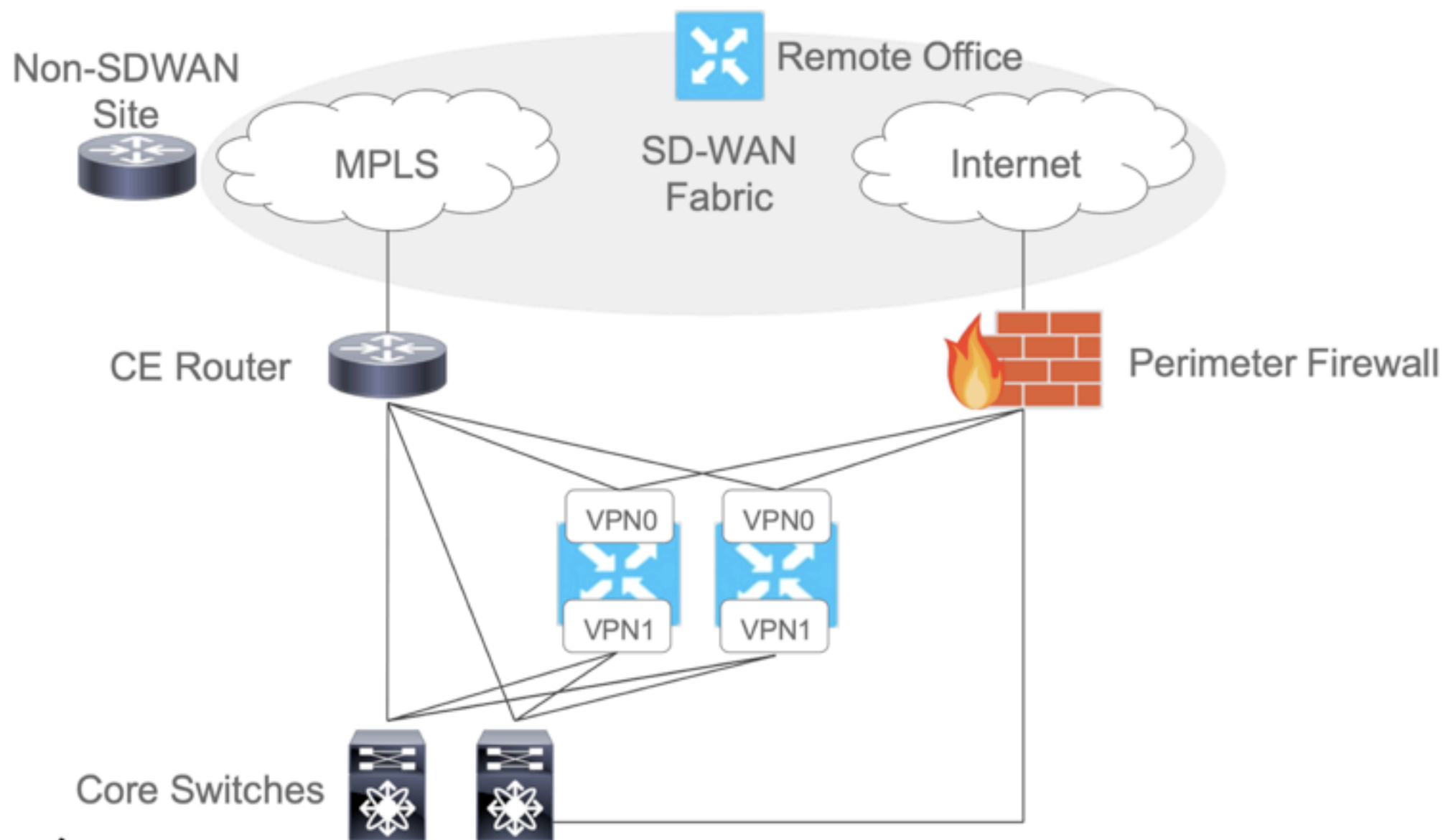
Controllers

Datacenter

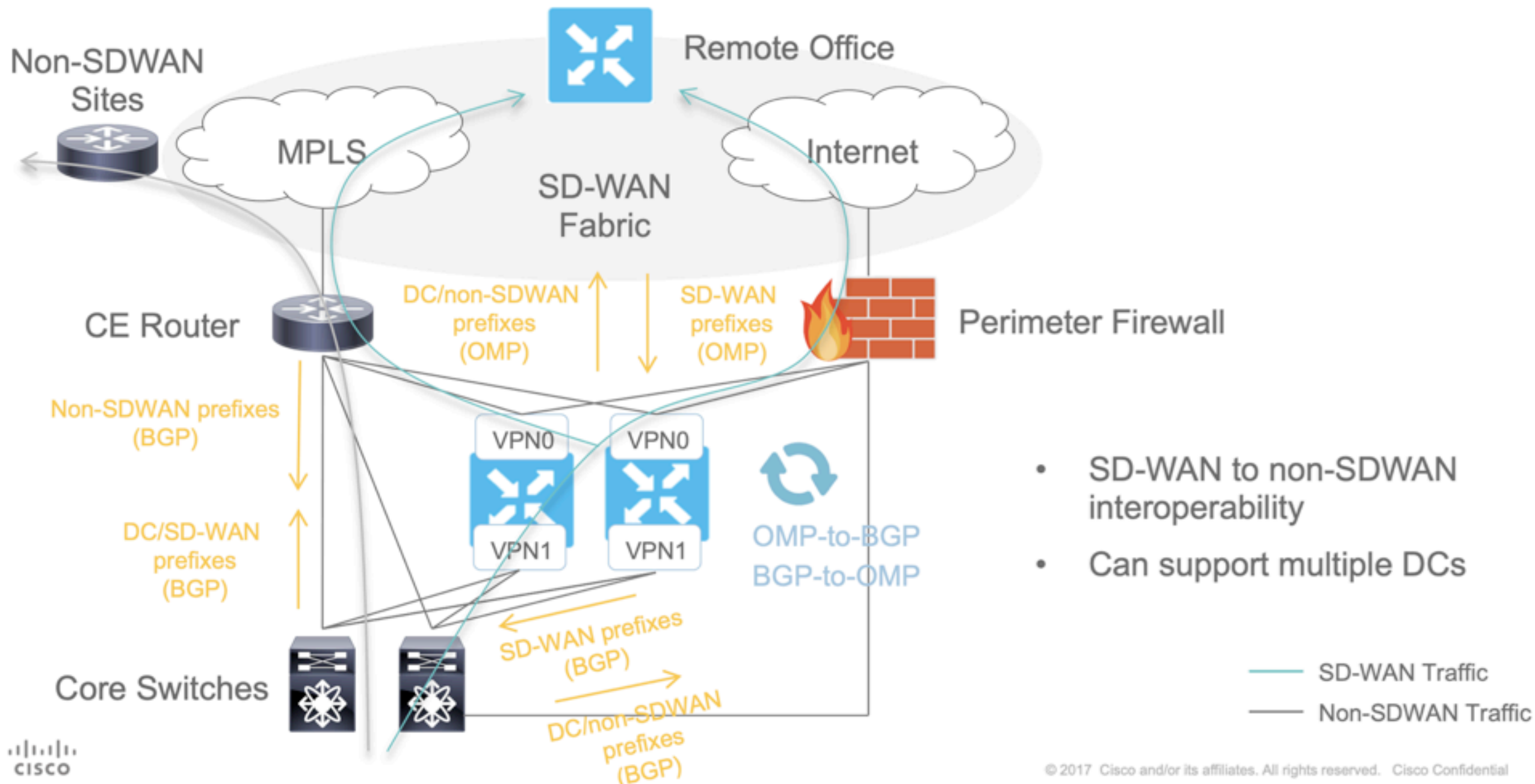
Branches



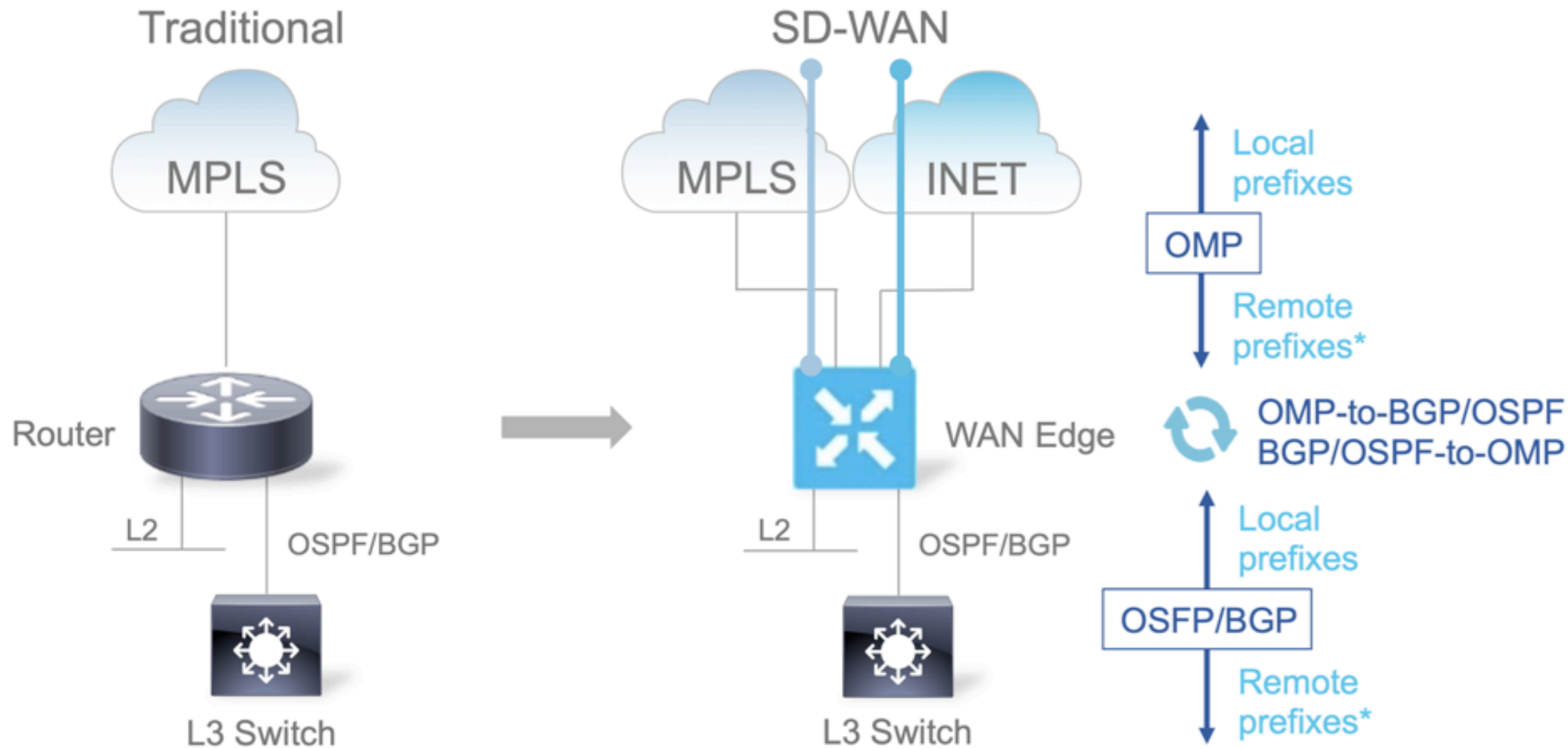
Data Center Migration



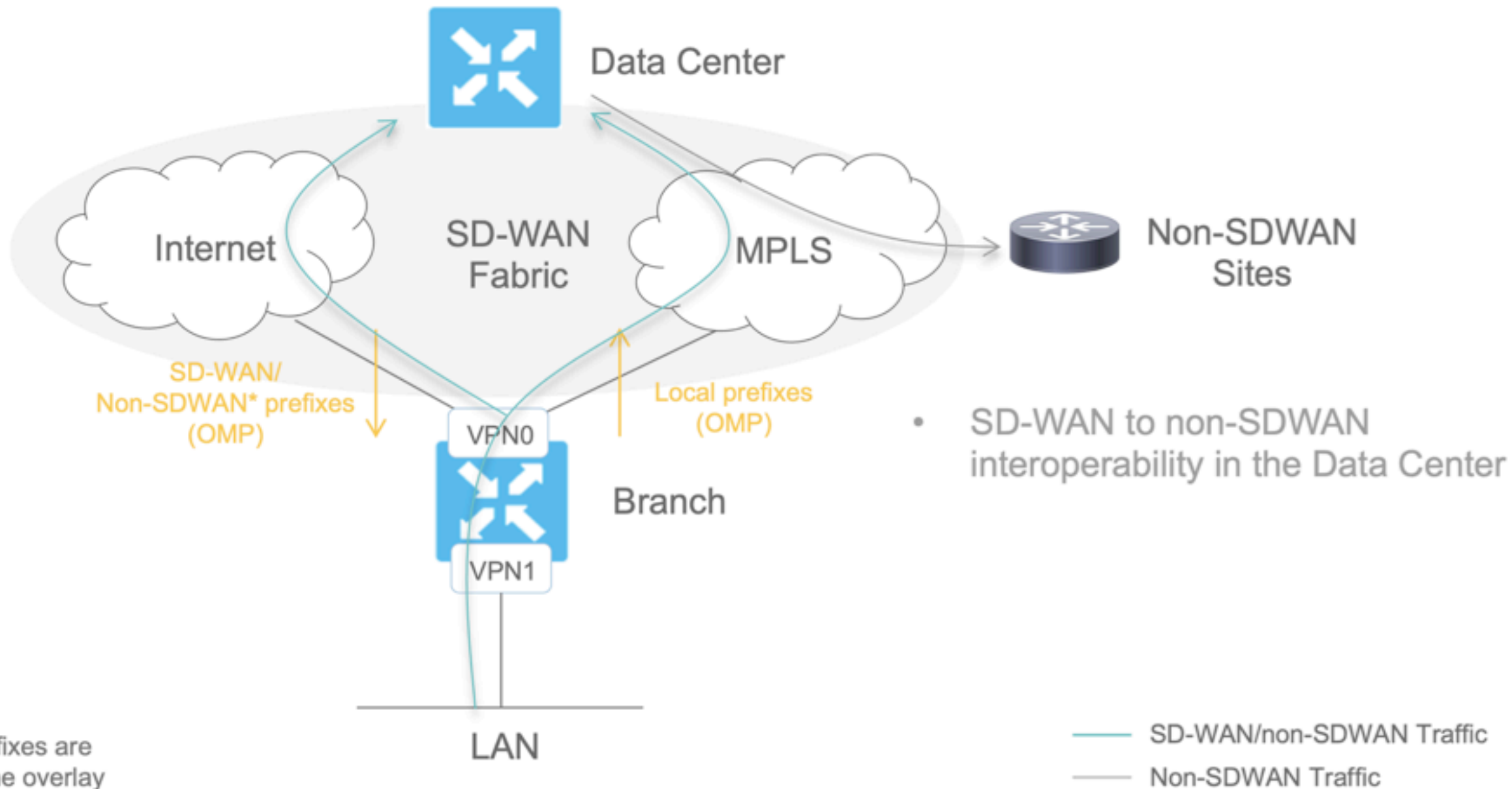
Data Center Migration



Branch Migration



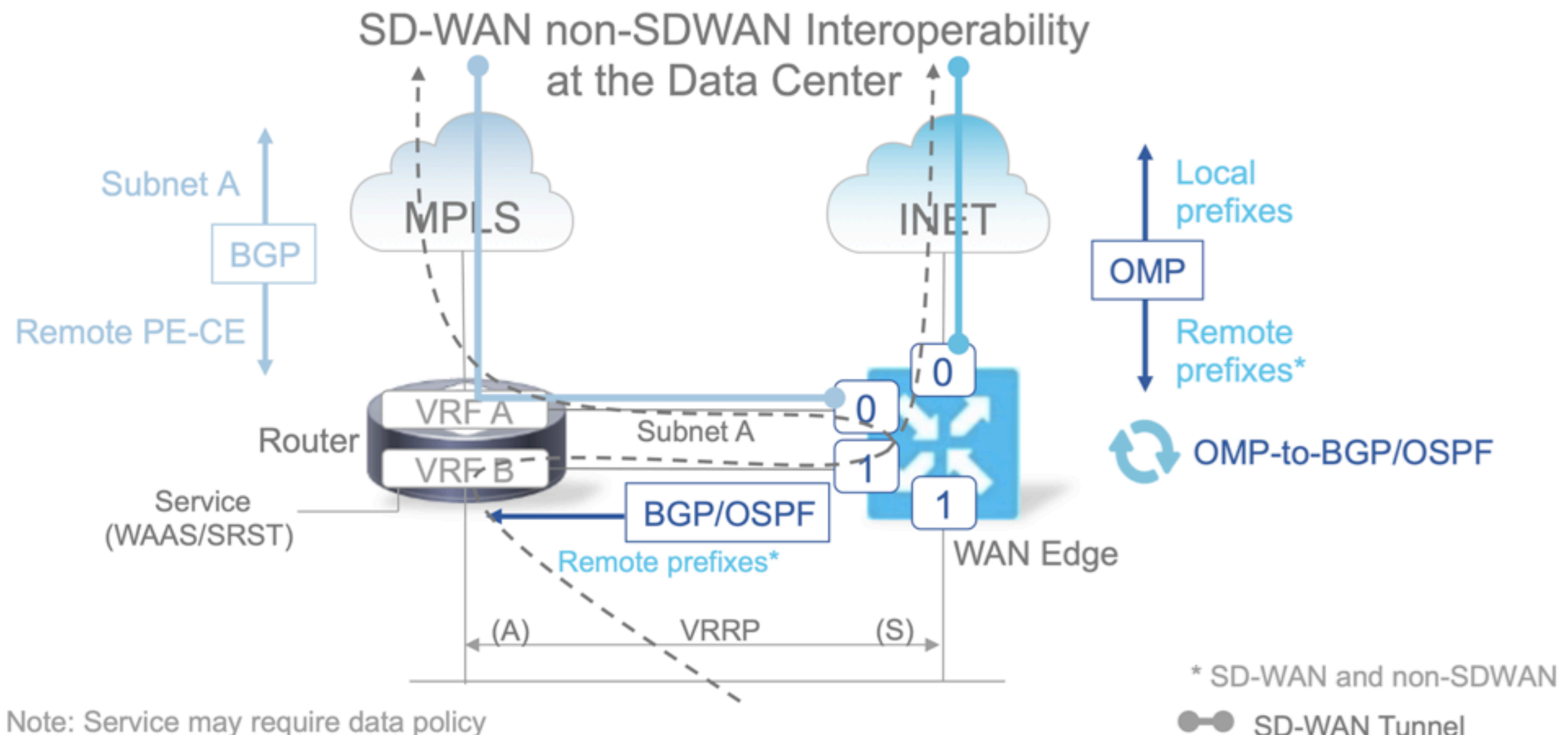
Branch Migration



* Non-SDWAN prefixes are received through the overlay

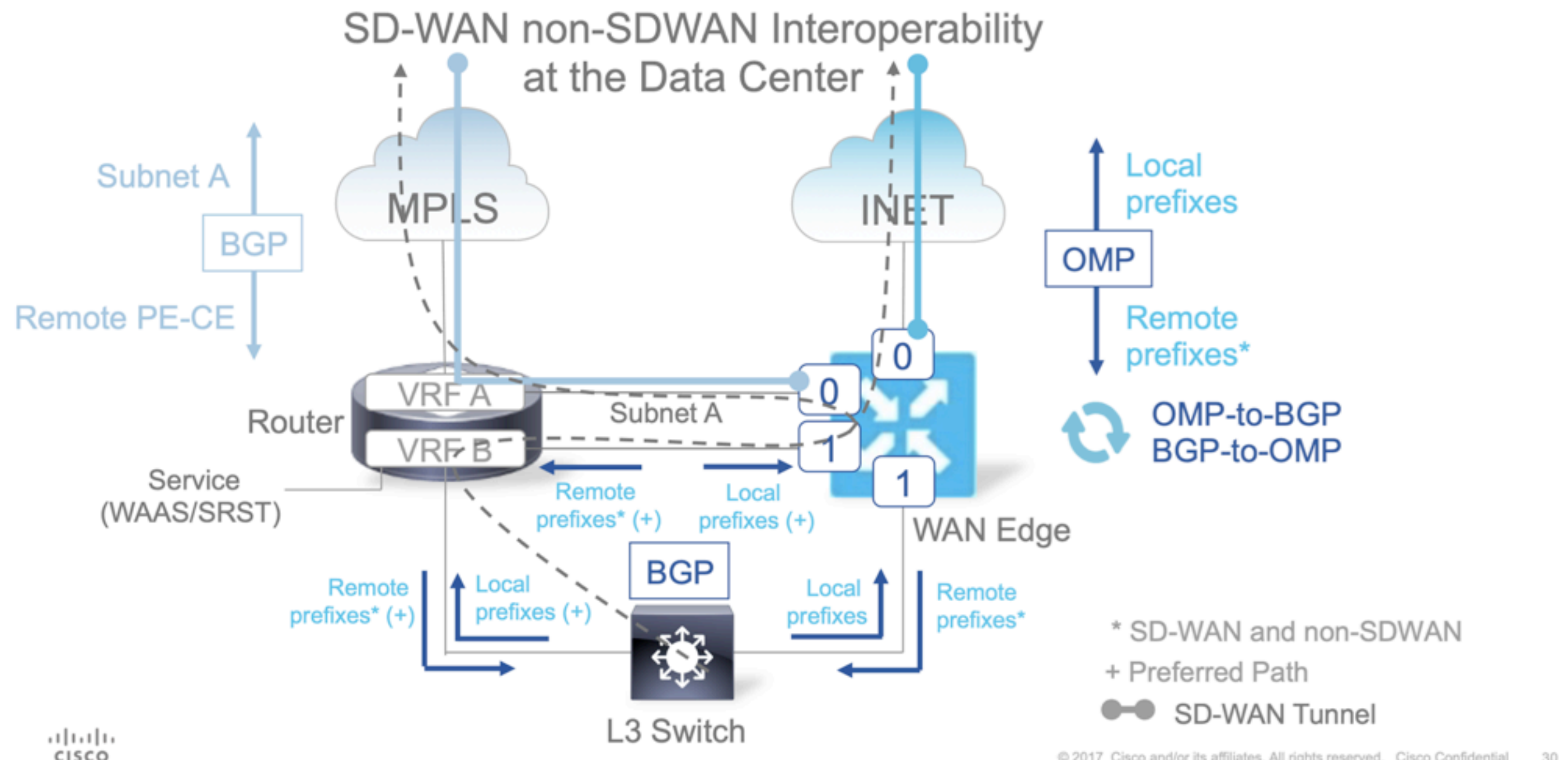


SD-WAN with Router Services and VRRP



Note: Service may require data policy on WAN Edge for return traffic

SD-WAN with Router Services and L3 Routing





TOMORROW starts here.