

Welcome

LA Networks
Jason Bomar, CCIE #9316
jbomar@la-networks.com

LAnet 

Cisco SD-WAN

INTRODUCTION & DEMO

Agenda

- The Evolving WAN
- Cisco SD-WAN Elements
- Cisco SD-WAN Templates
- Cisco SD-WAN Policies
- Cisco SD-WAN ZTP
- Demo
- Wrap Up

The Evolving WAN



More Users

We are seeing the work force expand, but in new and innovative ways: expanding branch offices, contractors, IoT devices, etc.



More Apps

Applications dominate the business landscape, and the ability to support them and allow for an optimal experience is now paramount.



More Threats

We are seeing more advanced attacks, and with the expansion of the branch, diversity of the applications, security now needs to be pervasive.



More Demands

Because of all of these shifts in the speed of business, the demands and expectations have skyrocketed

← Welcome to the digital revolution! Make yourself at home, it might be a while! →

The Evolving WAN

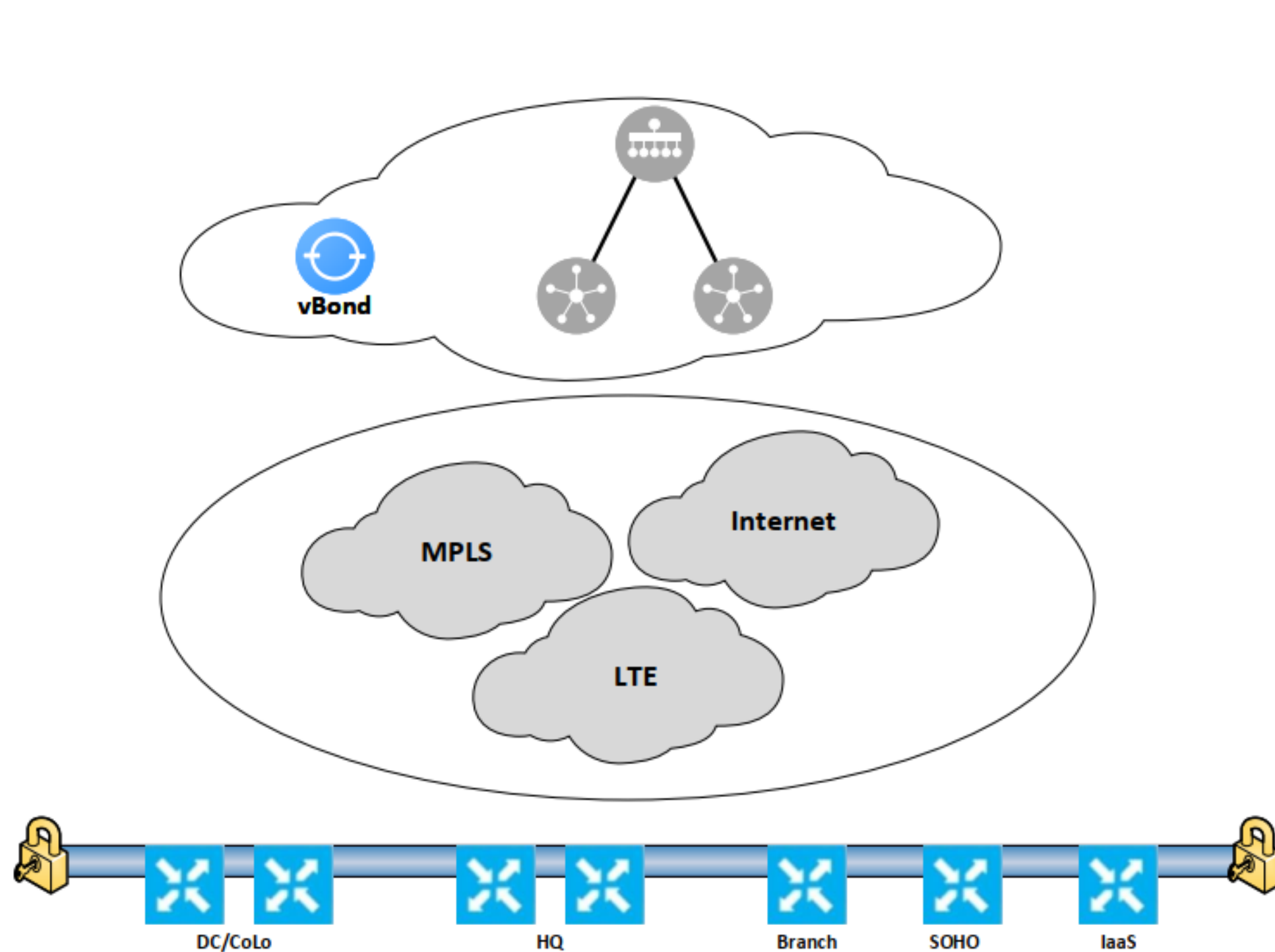


Regardless of the solution, SD-WAN should address these concerns. It should be ISP independent, have integrated security, work well with your cloud strategy and easy/simplify operations

SD-WAN Elements – Key Concepts

- Please be aware of the following constructs:
 - Site-ID: each 'location' gets a site-id, and all WAN Edges at the site share this Site-ID
 - System IP: Every WAN Edge will have a system IP, similar to a Loopback 0 interface
 - Color: This is a WAN Transport – there are two TYPES of colors: public and private
 - TLOC: This is a WAN Interface identifier and it combines a Color and IP Address
 - Transport Side: This is the WAN side of the Edge
 - Default here is VPN 0, all traffic in this VPN is tunneled and encrypted
 - Service Side: This is the LAN side of the Edge
 - Default here is VPN 1, but you can add additional Service Side VPN's
 - VPN: It is critical to be aware that in Cisco SD-WAN – VPN is equivalent to a VRF

SD-WAN Elements - vBond



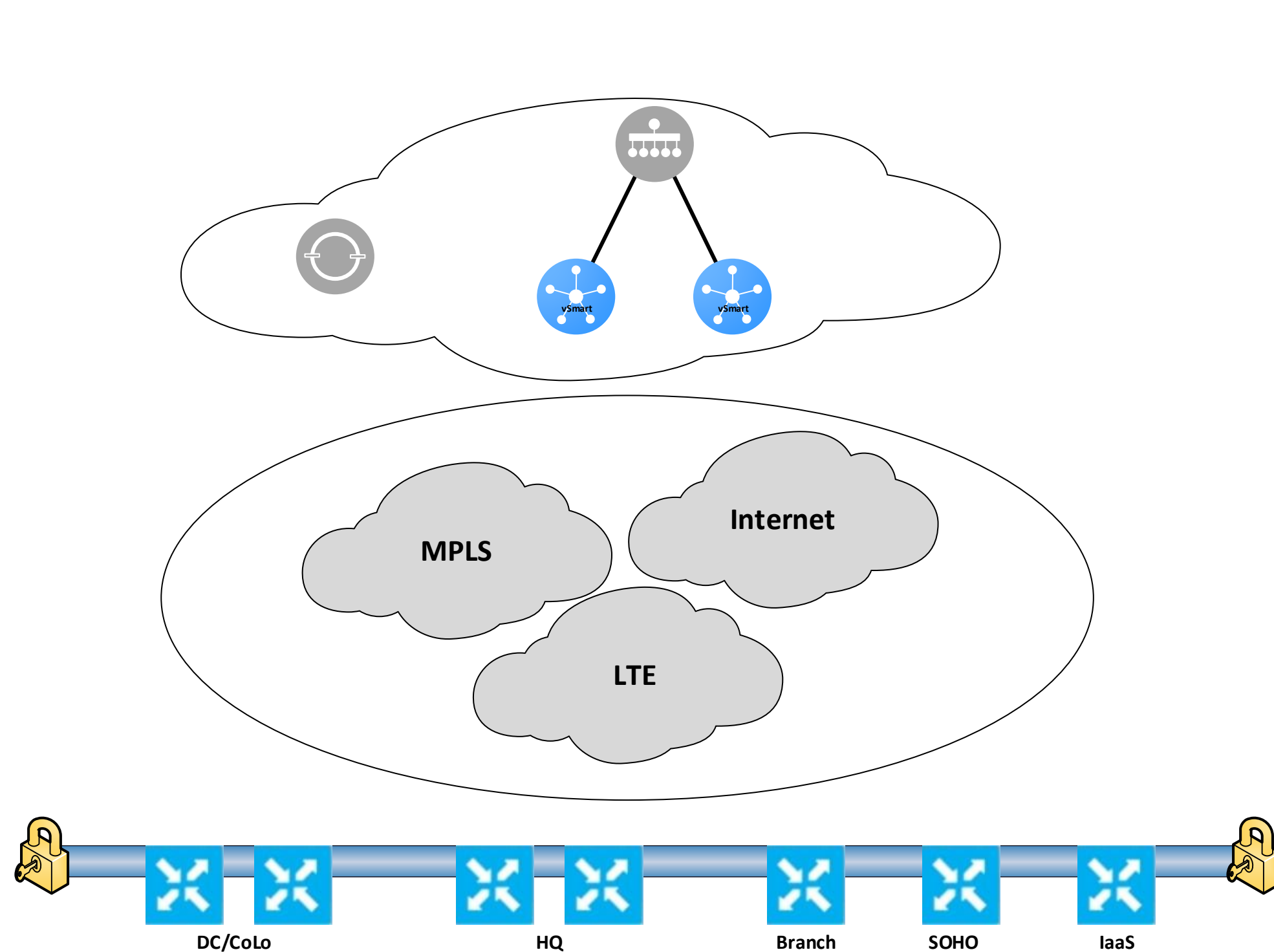
Orchestration Plane



Cisco vBond

- Orchestrates control and management plane
- First point of authentication (white-list model)
- Distributes list of vSmarts/vManage to all WAN Edge routers
- Facilitates NAT traversal
- Requires public IP Address [could sit behind 1:1 NAT]
- Highly resilient

SD-WAN Elements - vSmart

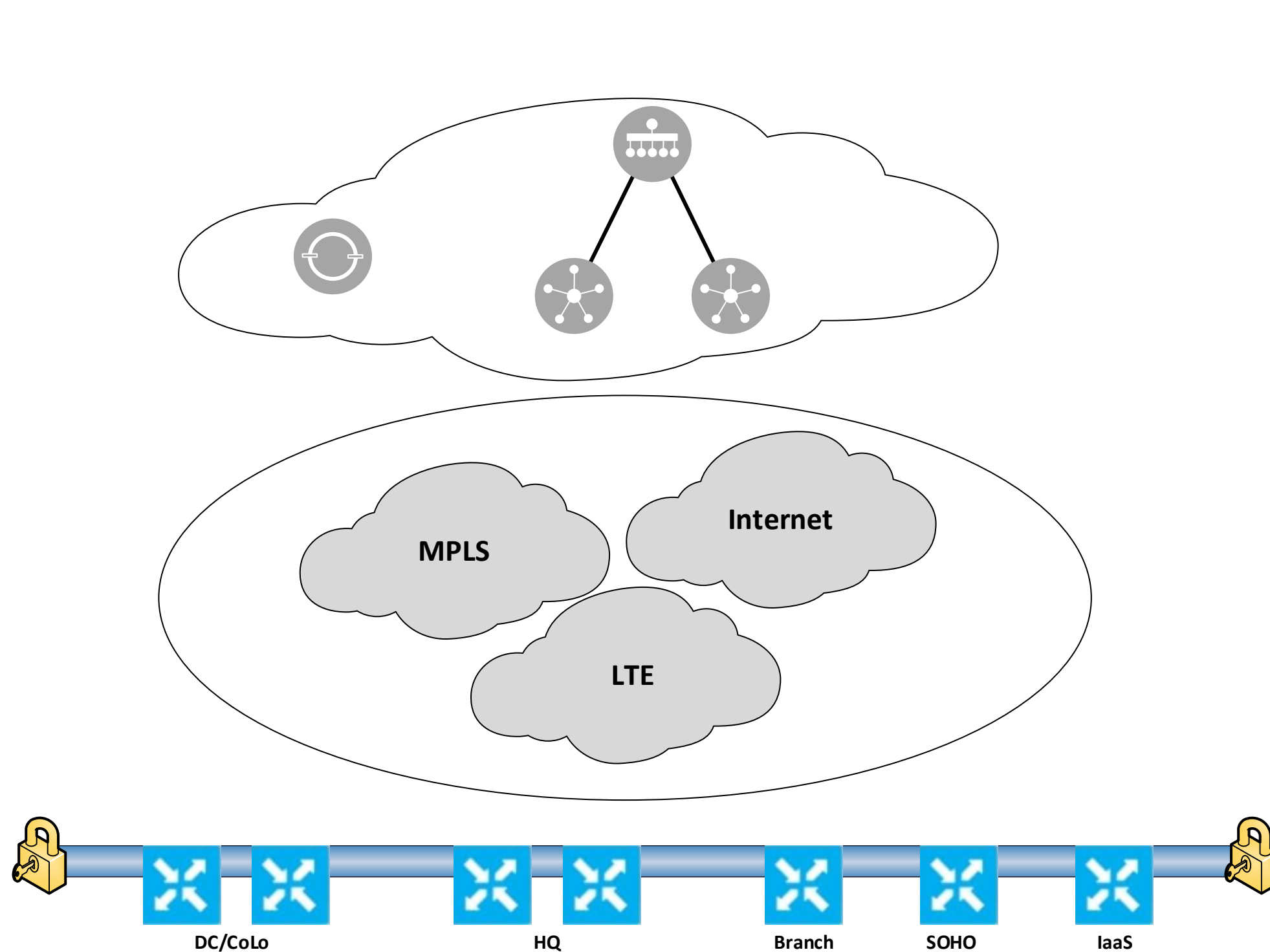


Control Plane



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

SD-WAN Elements – WAN Edge



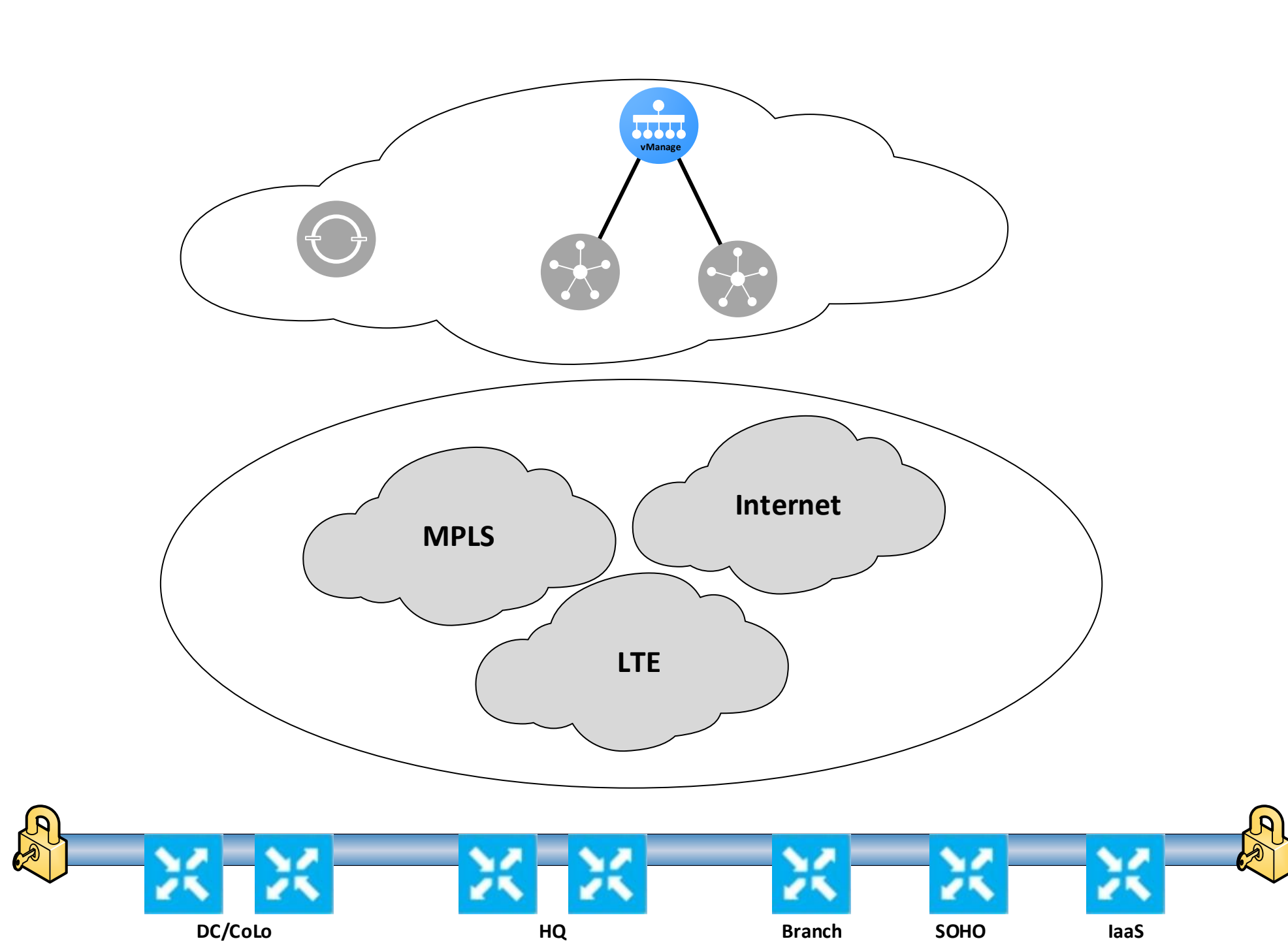
Data Plane



Cisco vEdge/cEdge

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

SD-WAN Elements - vManage



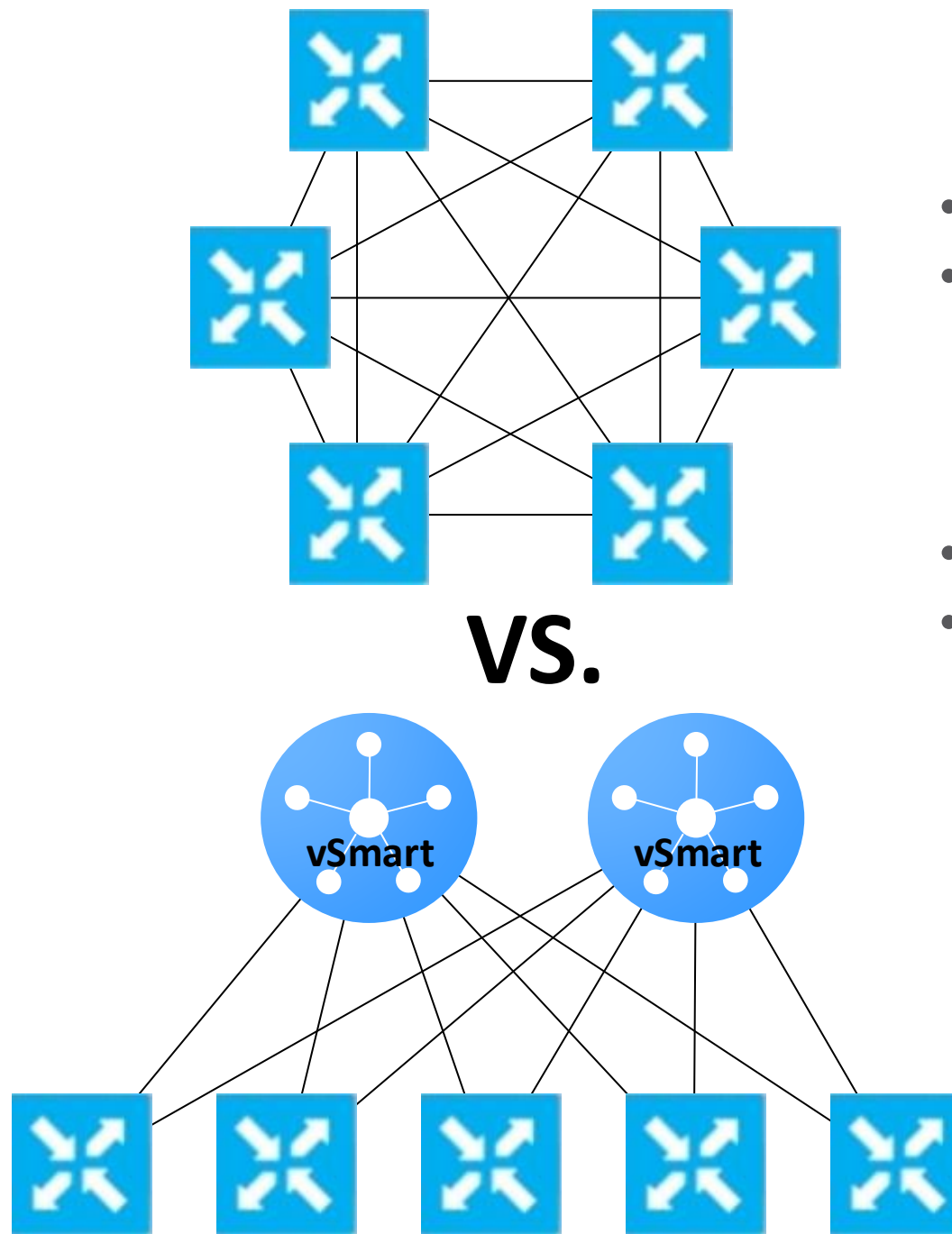
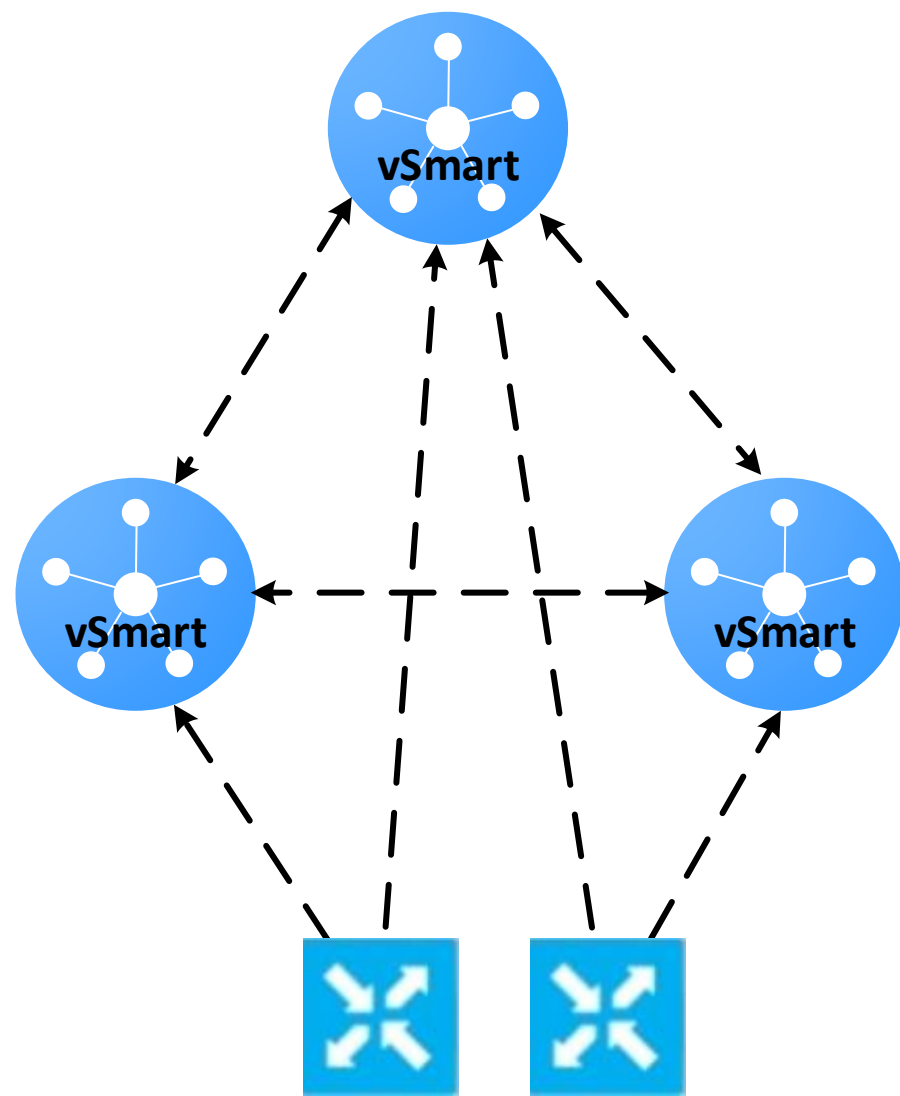
Management Plane



Cisco vManage

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- Programmatic interfaces (REST, NETCONF)
- Highly resilient*

SD-WAN Elements - OMP



OMP

- TCP based extensible control plane protocol
- Runs between vEdge routers and vSmart controllers and between the vSmart controllers
 - Inside TLS/DTLS connections
- Advertises control plane context
- Dramatically lowers control plane complexity and raises overall solution scale

SD-WAN Templates

Select Template

BASIC INFORMATION


AAA

NTP

System

- Templates are the primary method you will use for applying configuration to the WAN Edge devices
- Templates are broken into two types
 - Feature Templates
 - Device Templates
- Each type of template is tied to a hardware platform
 - You cannot mix vEdge/cEdge platforms, these need separate templates
 - If you add too many platforms, you might find that features get LCD in the template
- Generally speaking, you will have plenty of Feature templates

SD-WAN Templates

System *	<input type="text" value="ft_vedge_branch-system"/>
Logging*	<input type="text" value="Factory_Default_Logging_Template"/>
NTP	<input type="text" value="ft_vedge_branch-ntp"/> 

- Once you have your feature templates laid out, you create Device Templates
- Within the Device template form, you can call the different Feature templates you created earlier
- With the templates, you have to do a lot of upfront work – but on the backend the operations is simpler

SD-WAN Templates

- Some recommendations on Templates
 - Come up with a naming standard for your templates
 - Each Feature Template has three values you can set:
 - Default (the default value)
 - Global (this means you will use the same value for every device that utilizes the template)
 - Local (this means you will enter the data on a per device basis) – these also need a naming standard
 - Device templates usually revolve around common features based on the WAN design:
 - All DC's
 - All sites with IGP on the Service Side
 - All dual WAN branches
 - Etc.

SD-WAN Policies

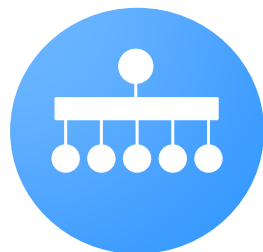
- What Templates do for basic configuration, Policies do for more advance configuration
- There are two types of Policies: Localized and Centralized
 - Localized policies are just that – local to a single site
 - If you redistributes OSPF into BGP and want to filter, that is a Localized policy
 - Centralized policies are for the SD-WAN fabric or multiple sites
 - If you want to configure AAR or set up a unique VPN topology for the Fabric, that is a Centralized policy

SD-WAN Policies

Localized Policies

Local Policy:

Local Control Policy –
Routing Policies (OSPF/BGP, etc.)
Local Data Policy (QoS, ACL, etc.)



Netconf



Centralized Policies

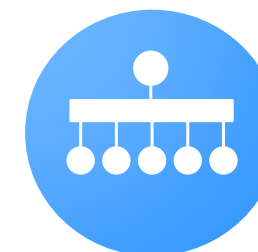
VPN Topology and Membership

Policy:

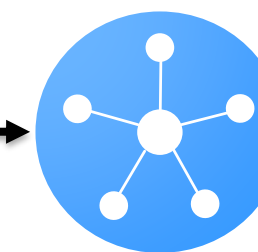
VPN Membership policy
Per VPN Topologies

Traffic Policy:

Application Aware Routing
Data Policy/PBR



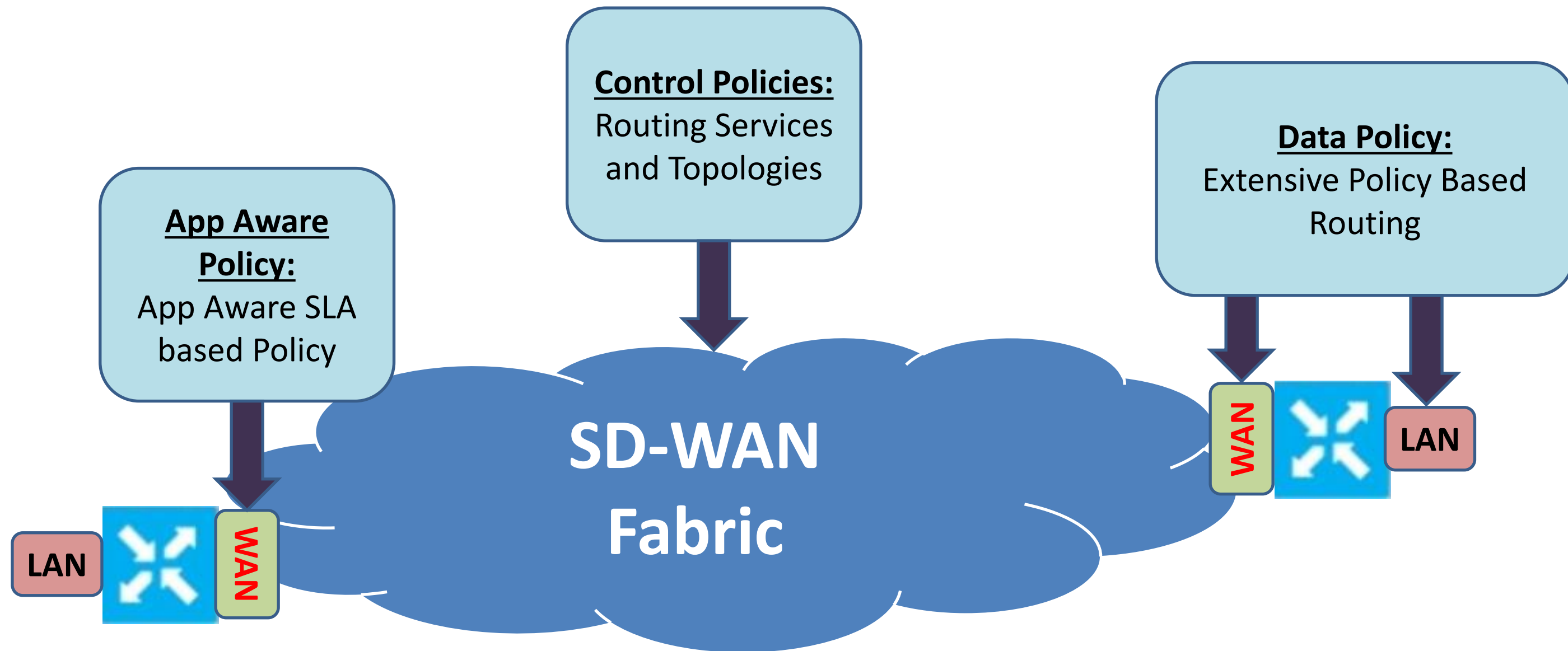
Netconf



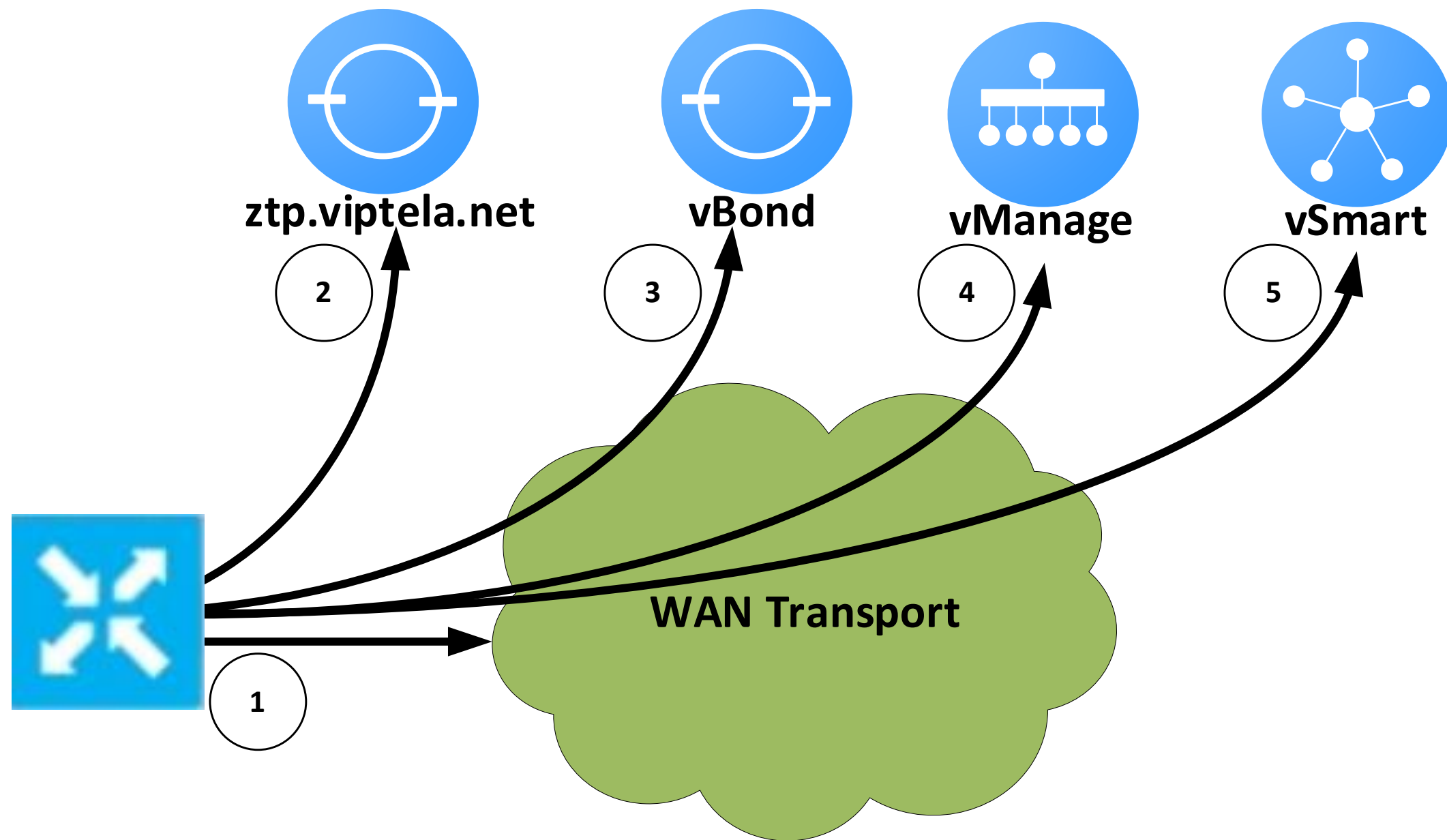
OMP



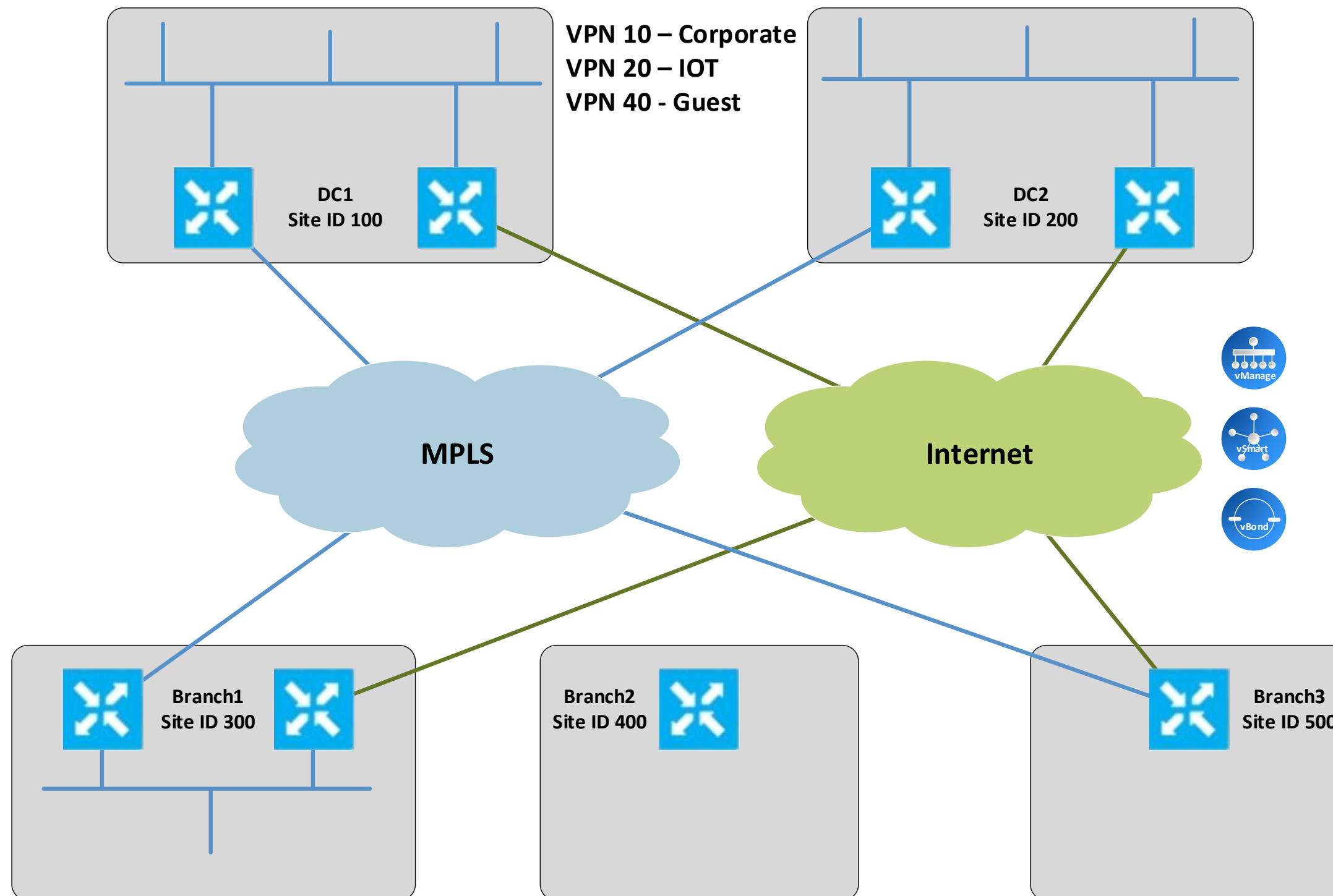
SD-WAN Policies



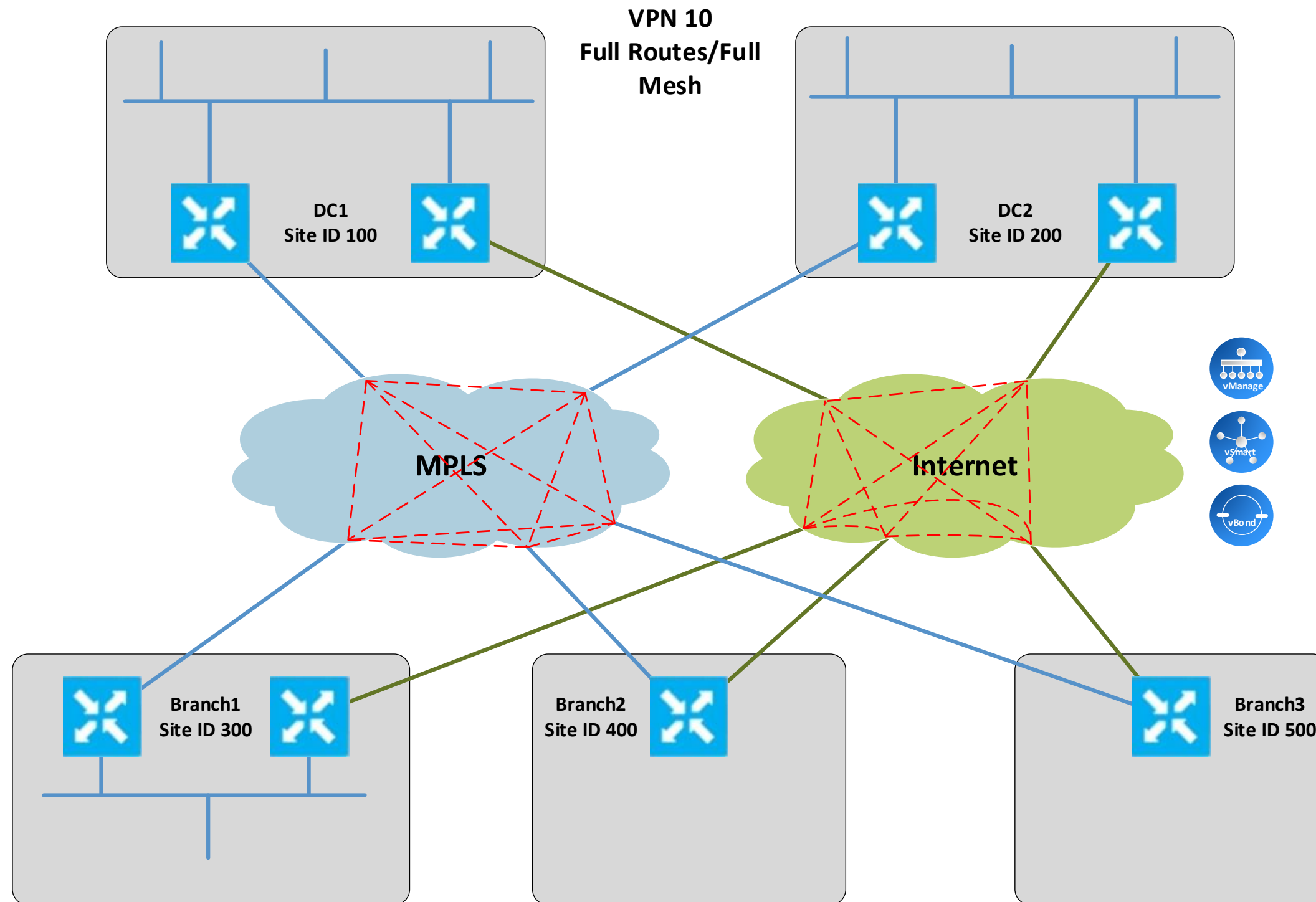
SD-WAN – Zero Touch Process



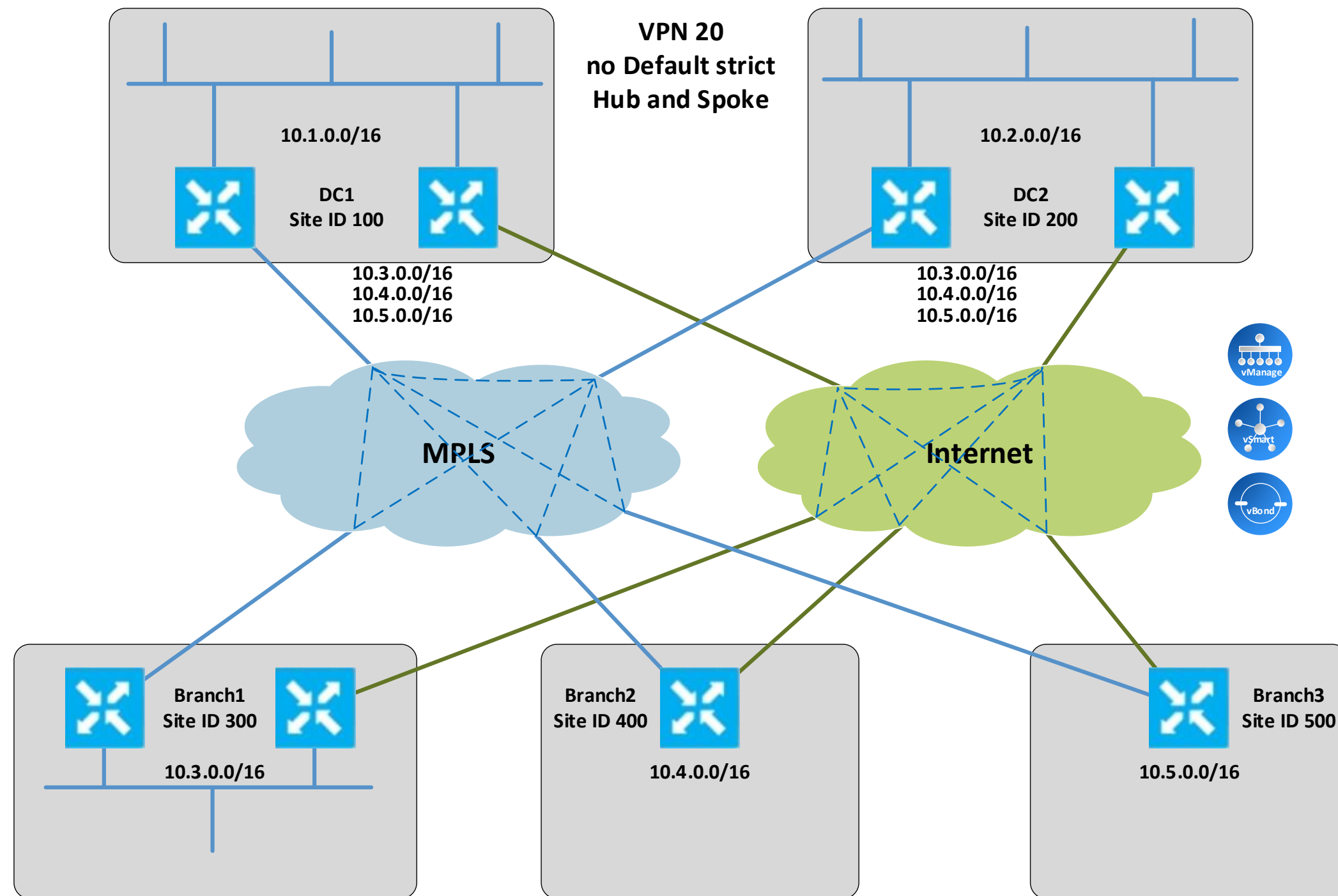
Demo Lab



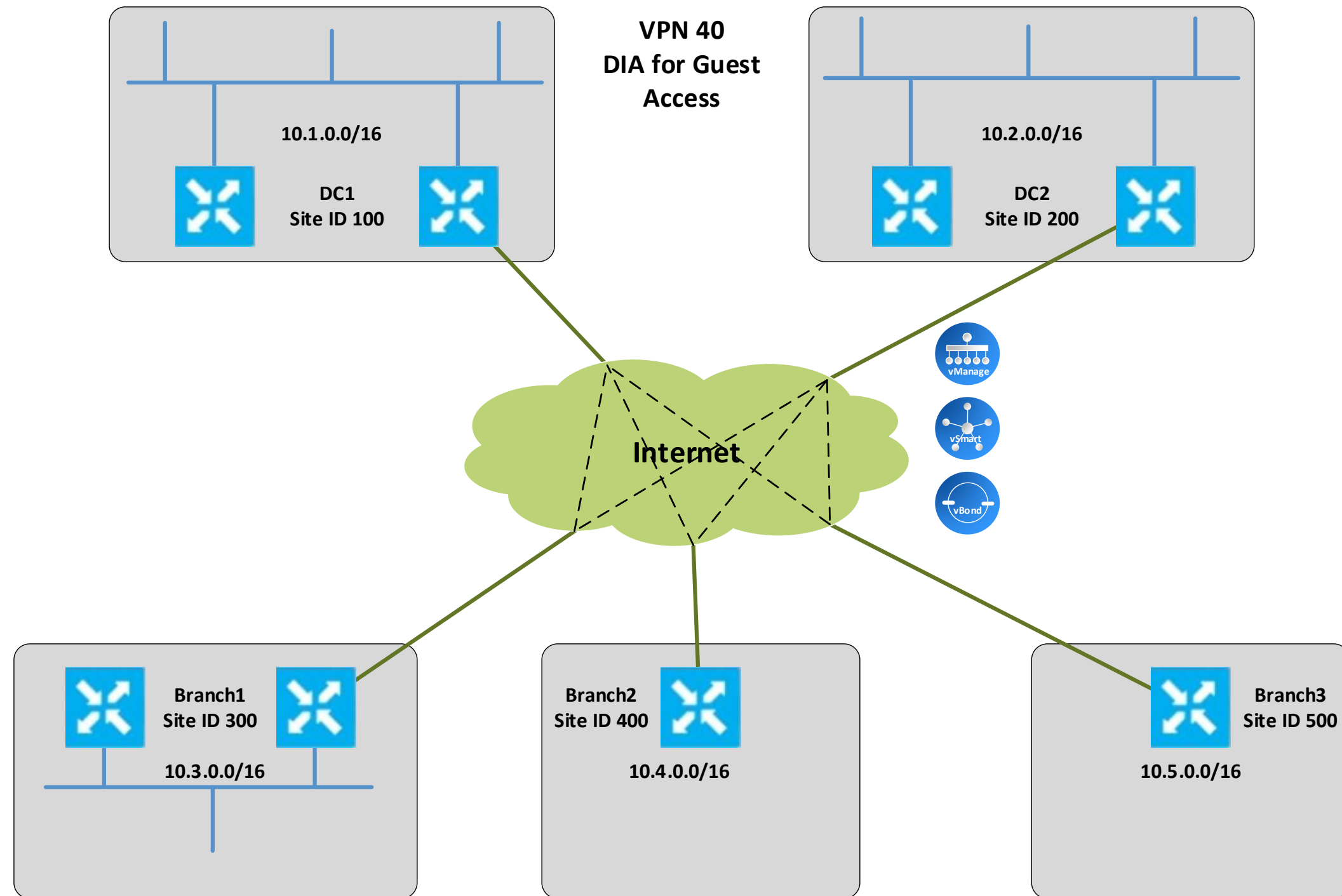
Demo Lab



Demo Lab



Demo Lab





Fin

Thank you for your time!

LAnet 