



Cisco SD-WAN

CVU – Cisco Virtual Update

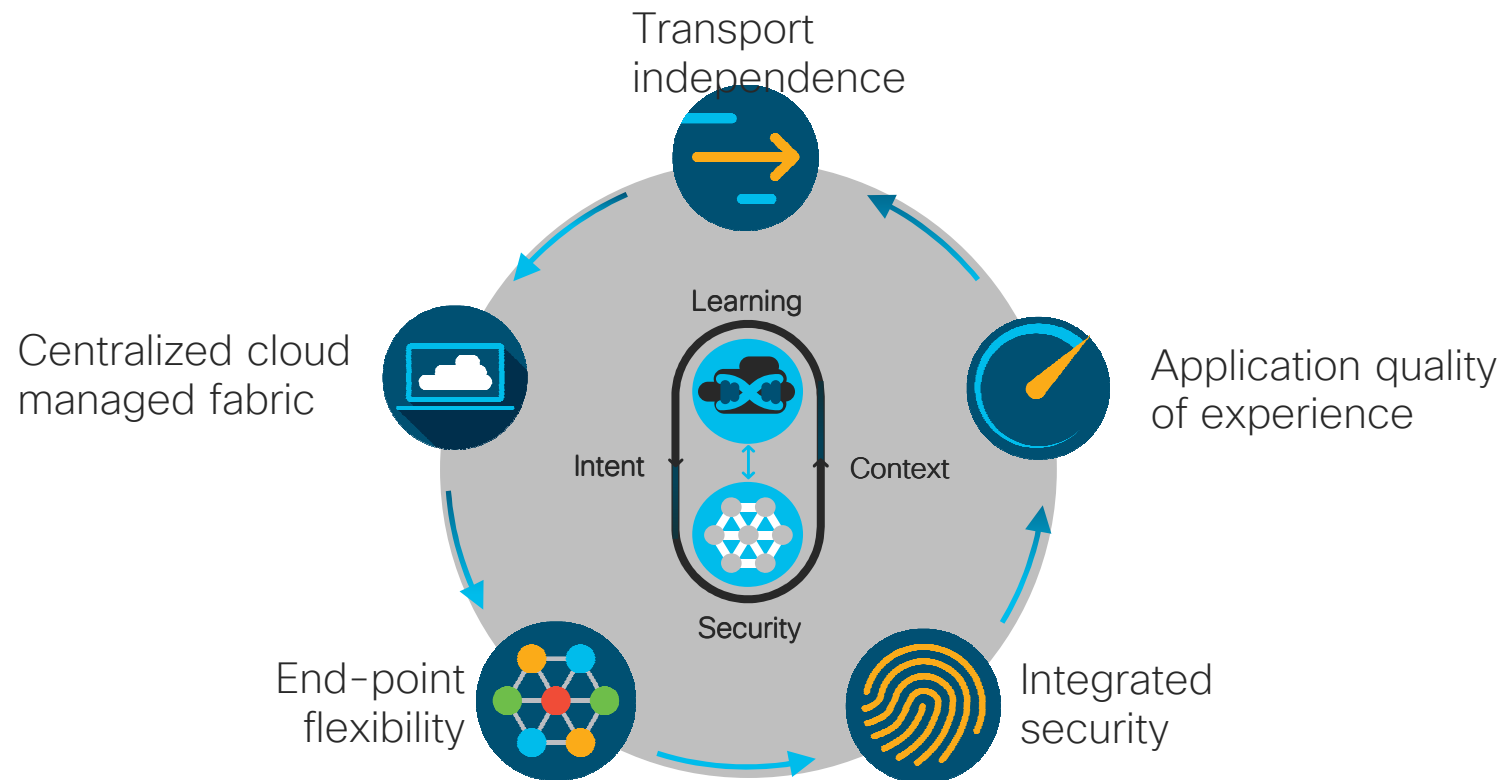
Per Jensen
per@cisco.com
June 27th 2018

Agenda

- ☐ Overview
- ☐ Solution Elements and Overview
- ☐ Selective “Deep-Dive”
- ☐ Bonus
- ☐ Licensing

Overview

Intent-based networking for the branch and WAN



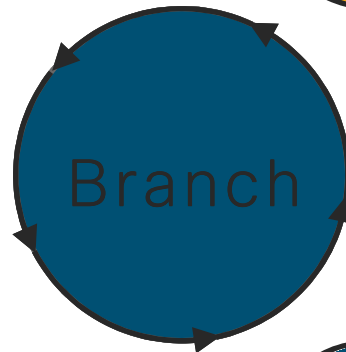
Cisco SD-WAN

Intent-based networking for the branch and WAN

4x Improved application experience

40% WAN opex savings

3.24h Time to threat detection



Better user experience

Deploy applications in minutes on any platform with consistent application performance



Greater agility

Simplify the deployment and operation of your WAN and get faster performance using less bandwidth



Advanced threat protection

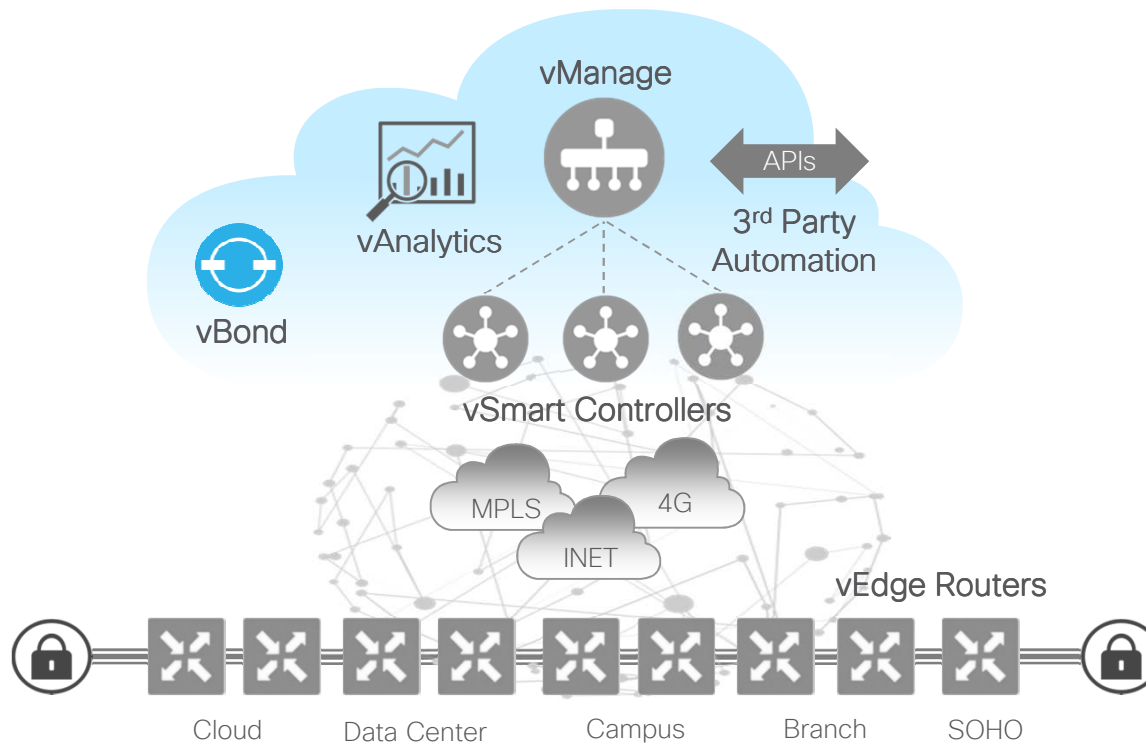
Securely connect your users to applications and protect your data from the WAN edge to the cloud

Agenda

- ☐ Overview
- ☐ Solution Elements and Overview
- ☐ Selective “Deep-Dive”
- ☐ Bonus
- ☐ Licensing

Cisco SD-WAN Solution Elements

Orchestration Plane



Orchestration Plane

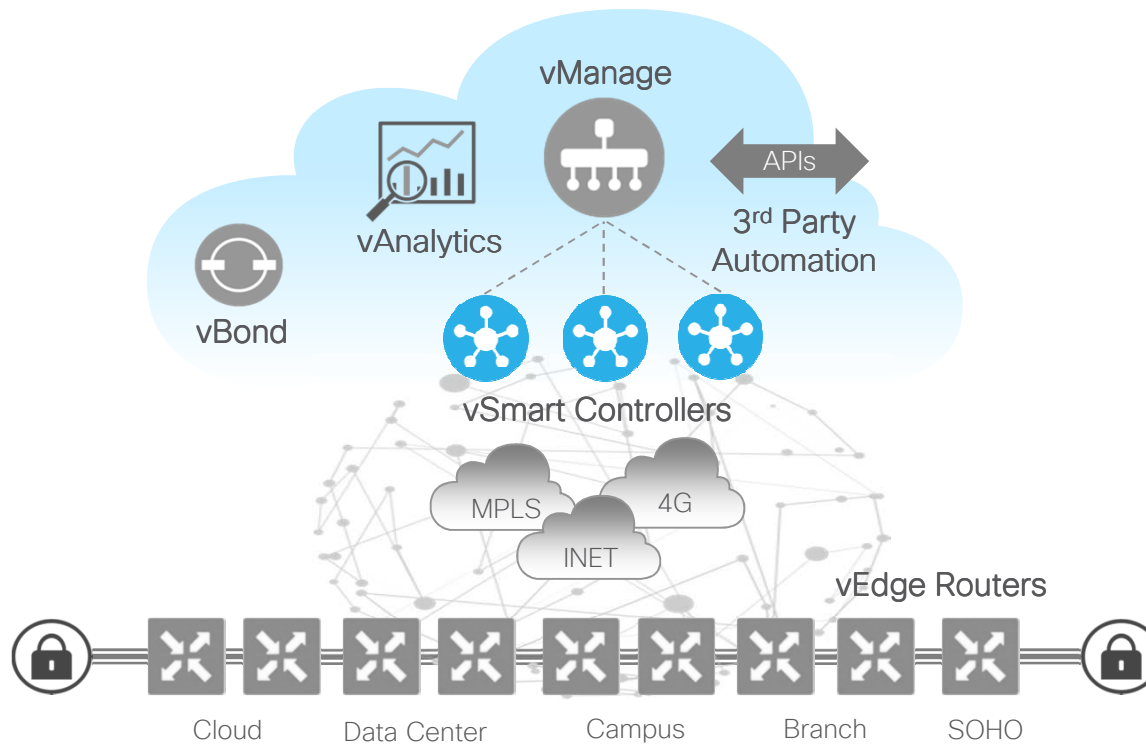


Cisco vBond

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

Cisco SD-WAN Solution Elements

Control Plane



Control Plane

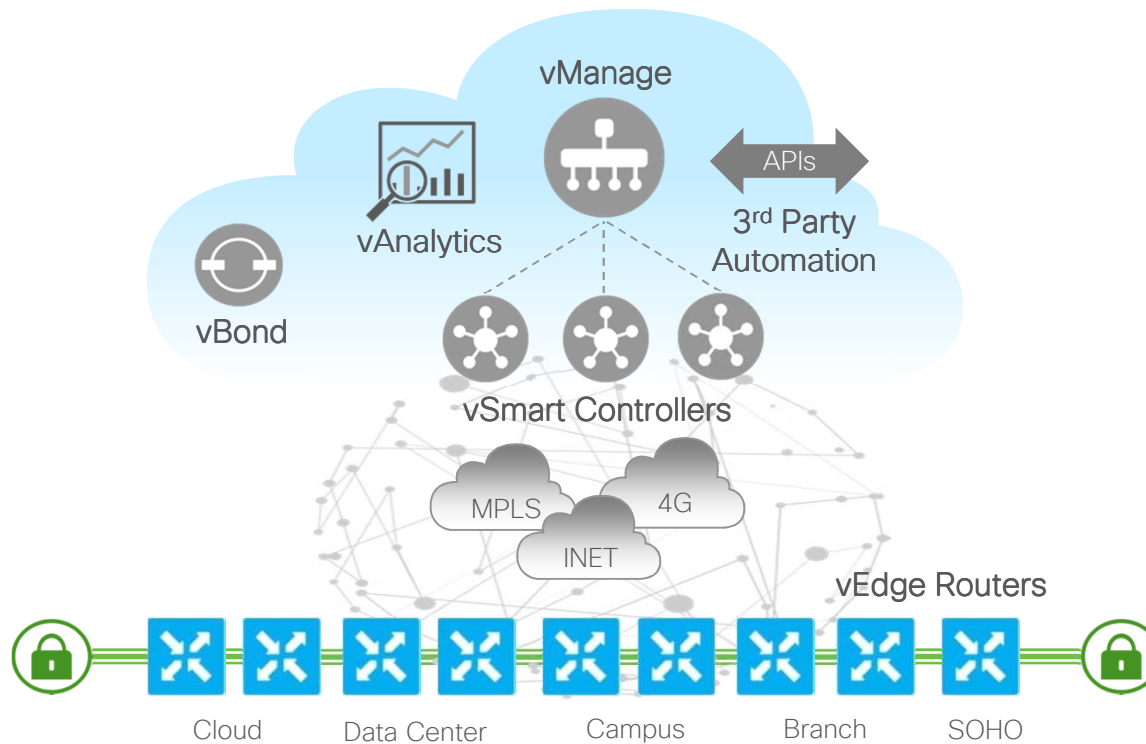


Cisco vSmart

- 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, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

Cisco SD-WAN Solution Elements

Data Plane



Data Plane

Physical/Virtual

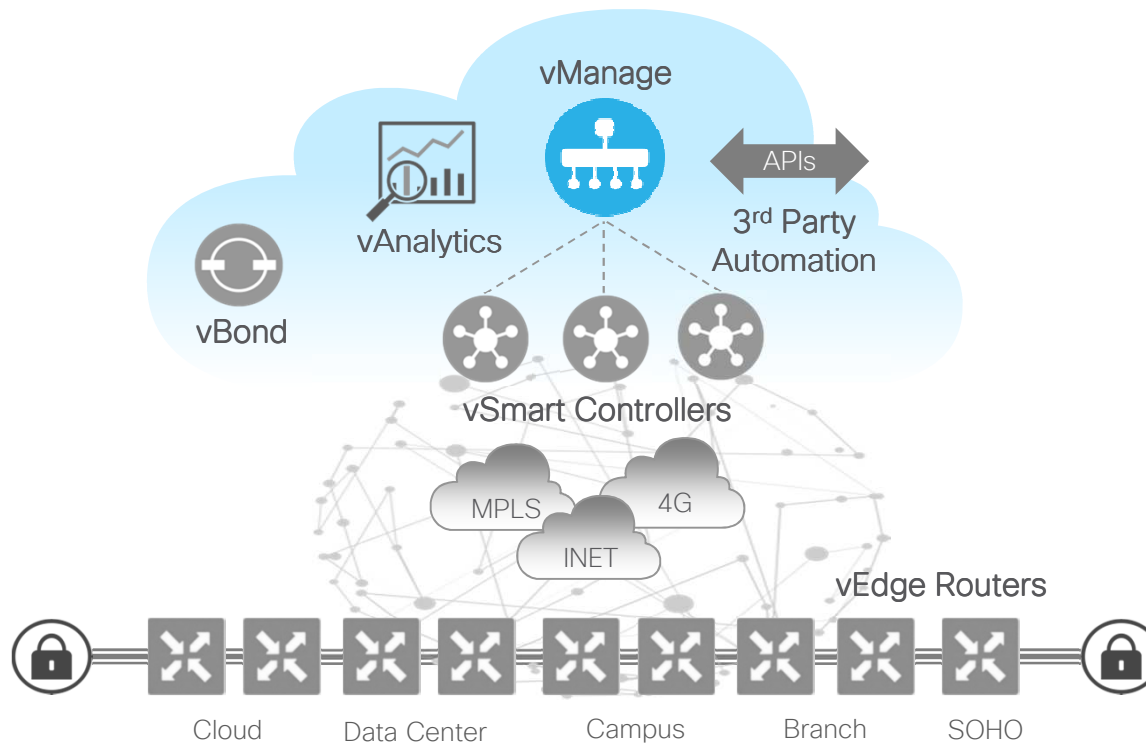


Cisco vEdge

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

Cisco SD-WAN Solution Elements

Management Plane



Management Plane

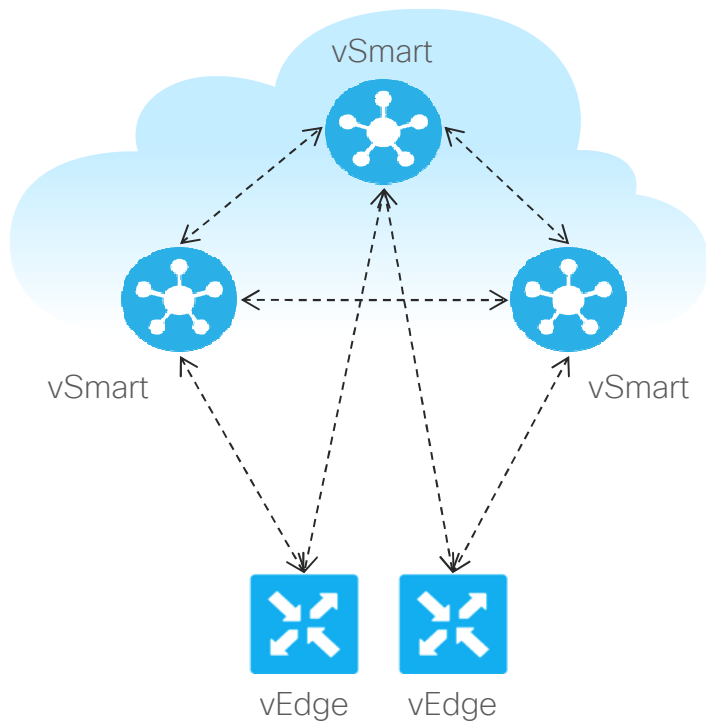


Cisco vManage

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

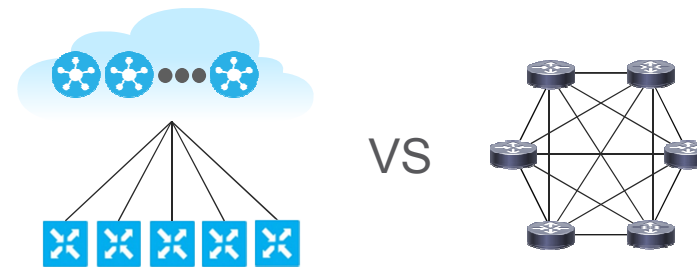
Overlay Management Protocol (OMP)

Unified Control Plane



Note: vEdge routers need not connect to all vSmart Controllers

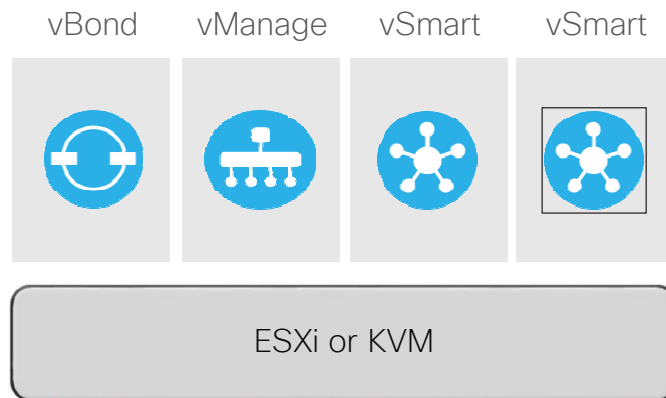
- TCP based extensible control plane protocol
- Runs between vEdge routers and vSmart controllers and between the vSmart controllers
 - Inside TLS/DTLS connections
- Advertises control plane context
- Dramatically lowers control plane complexity and raises overall solution scale



Controllers

Deployment Methodology

On-Premise



Physical Server

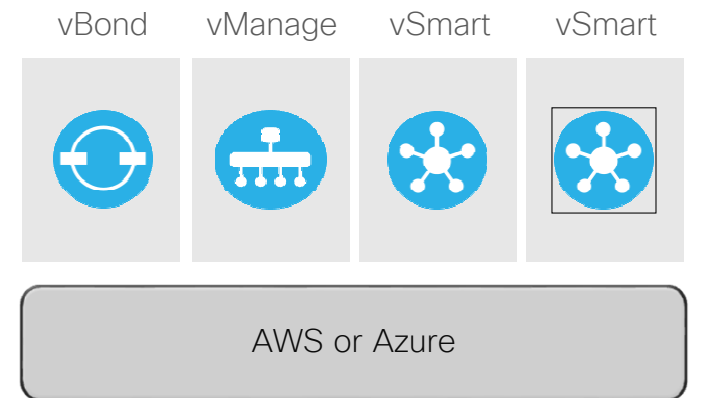


VM



Container

Hosted



VM



Container

SD-WAN Platforms

Branch virtualization

ENCS 5100



- Up to 250Mbps

ENCS 5400



- 250Mbps – 2GB

Public Cloud



SD-WAN

vEdge 100



- 100 Mbps
- 4G LTE & Wireless

vEdge 1000



- Up to 1 Gbps
- Fixed

vEdge 2000



- 10 Gbps
- Modular

Branch Services

ISR 1000



- 200 Mbps
- Next-gen connectivity
- Performance flexibility

ISR 4000



- Up to 2 Gbps
- Modular
- Integrated service containers
- Compute with UCS E

ASR 1000



- 2.5-200Gbps
- High-performance service w/hardware assist
- Hardware & software redundancy

vEdge-1000 and vEdge-2000 Routers

Hardware Specification

vEdge 1000



- 1 Gbps AES-256
- 1RU, standard rack mountable
- 8x GE SFP (10/100/1000)
- TPM chip
- 3G/4G via USB (or) Ethernet
- Security, QoS
- Dual Power supplies (external)
- Low power consumption

vEdge 2000



- 10 Gbps AES-256
- 1RU, standard rack mountable
- 4x Fixed GE SFP (10/100/1000)
- 2 Pluggable Interface Modules
- 8 x 1GE SFP (10/100/1000)
- 2 x 10GE SFP+
- TPM chip
- 3G/4G via USB (or) Ethernet
- Security, QoS
- Dual power supplies (internal)
- Redundant fans

vEdge 5000



- 20 Gbps AES-256
- 1RU, standard rack mountable
- 4 NIMs (Network Interface Modules)
- 8 x 1GE SFP (10/100/1000)
- 4 x 10GE SFP+
- TPM chip
- 3G/4G via USB (or) Ethernet
- Security, QoS
- Dual power supplies (internal)
- Redundant fans

vEdge-100 Routers

Hardware Specification

vEdge 100



- 100 Mbps AES-256
- 5x 1000Base-T
- TPM chip
- Security, QoS
- External AC PS
- Kensington lock
- Fan-less
- 9" x 1.75" x 5.5"
- GPS

vEdge 100m



- 100 Mbps AES-256
- 1RU
- 5x 1000Base-T
- 1x POE port
- 2G/3G/4G LTE
- Internal AC PS
- 1x USB-3.0
- TPM Board-ID
- Kensington lock
- Low power fan
- GPS

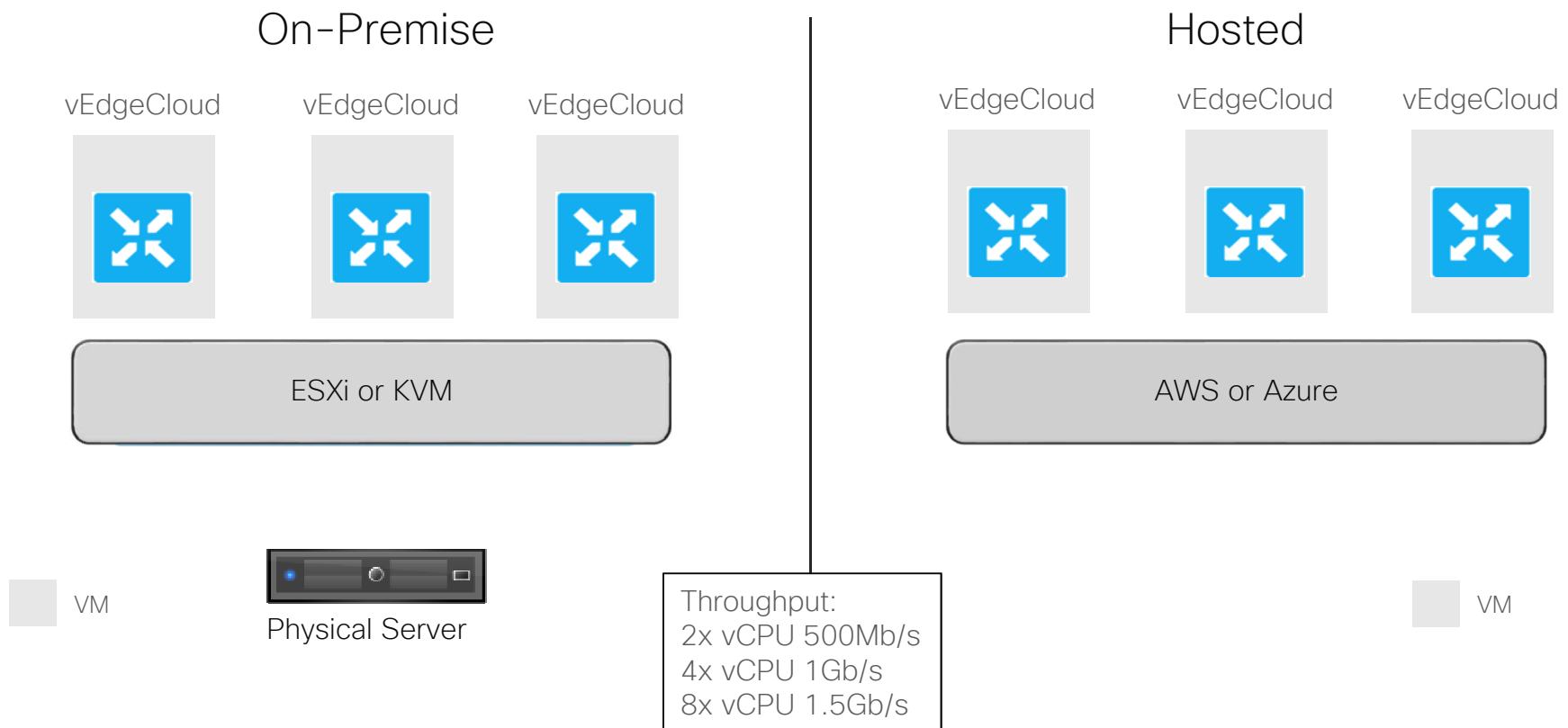
vEdge 100mw



- 100 Mbps AES-256
- 1RU
- 5x 1000Base-T
- 1x POE port
- 2G/3G/4G LTE
- 802.11a/b/g/n/ac
- Internal AC PS
- 1x USB-3.0
- TPM Board-ID
- Kensington lock
- Low power fan
- GPS

vEdge Cloud Virtual Routers

Deployment Methodology

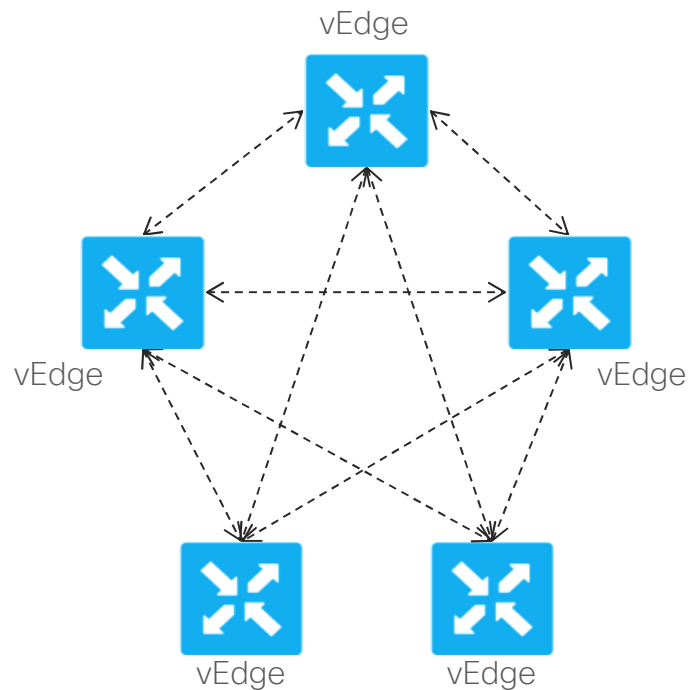


Agenda

- ☐ Overview
- ☐ Solution Elements and Overview
- ☐ Selective “Deep-Dive”
- ☐ Bonus
- ☐ Licensing

BFD

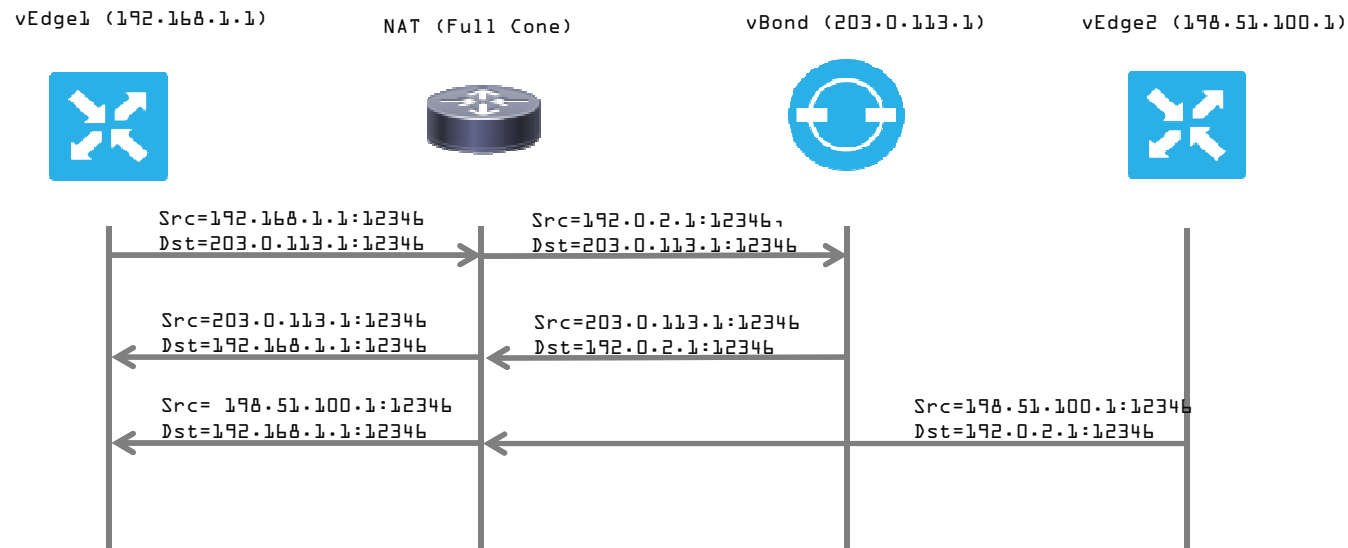
Bidirectional Forwarding Detection (BFD)



- Path liveliness and quality measurement detection protocol
 - Up/Down, loss/latency/jitter, IPSec tunnel MTU
- Runs between all vEdge and vEdge Cloud routers in the topology
 - Inside IPSec tunnels
 - Operates in echo mode
 - Automatically invoked at IPSec tunnel establishment
 - Cannot be disabled
- Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection
 - Fully customizable per-vEdge, per-color

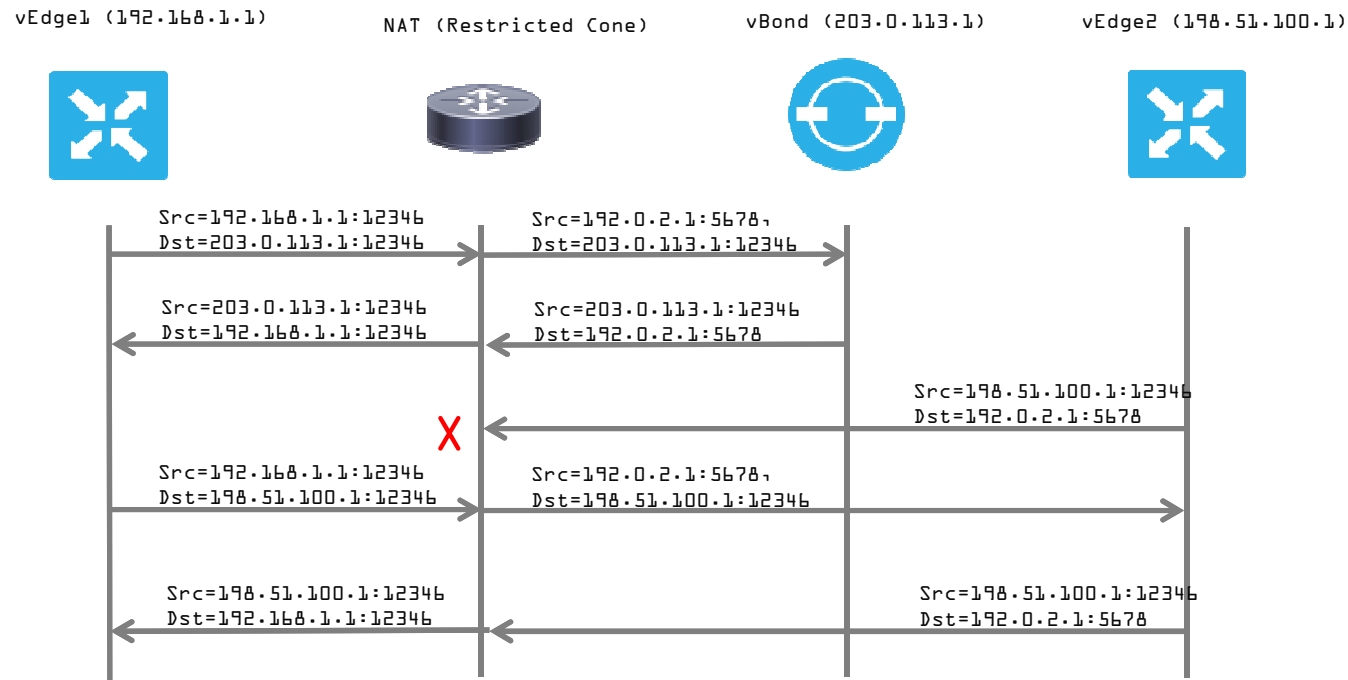
Understanding NAT Types

Full Cone NAT



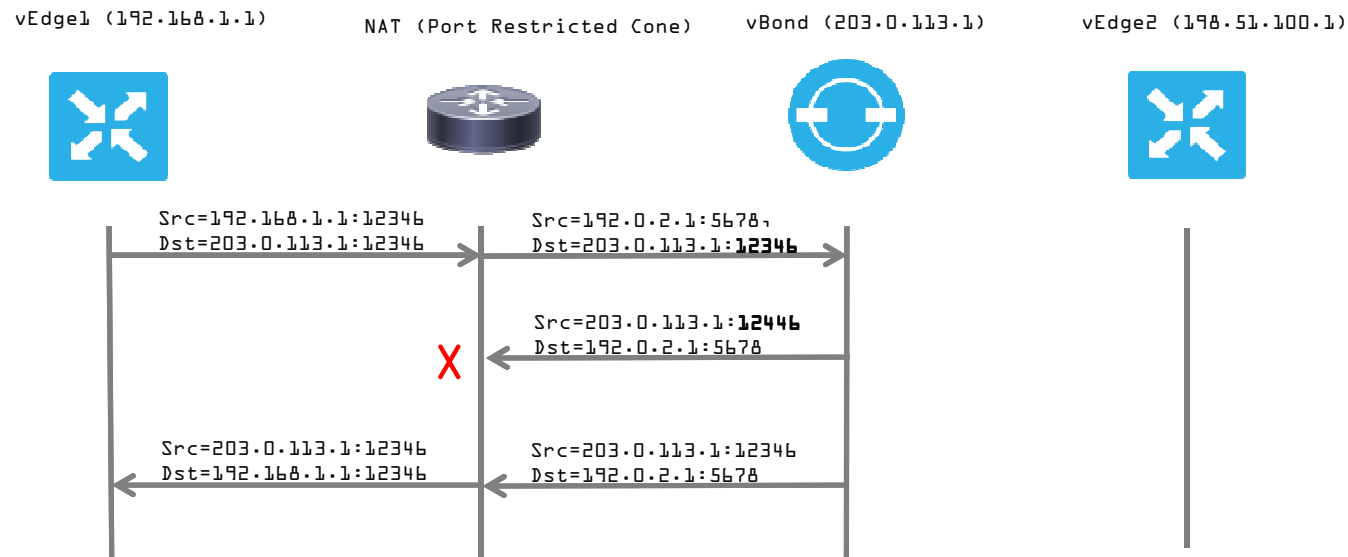
- Any external host can send packet to internal address:port by sending packet to external address:port once the mapping has been created

Restricted Cone NAT



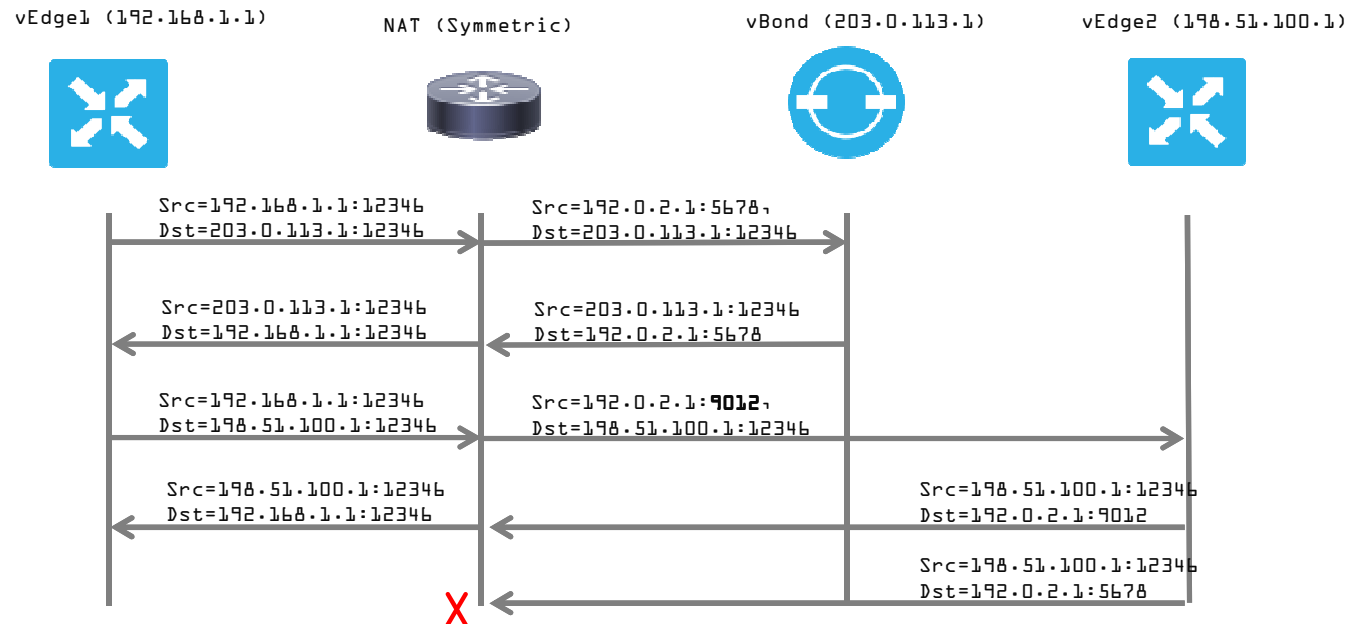
- Any external host can send packet to internal IP address if the internal device initiates a connection to the external host using previously created address mappings

Port Restricted Cone NAT















- Similar to Address restricted cone NAT with ports added to the mapping

Symmetric NAT



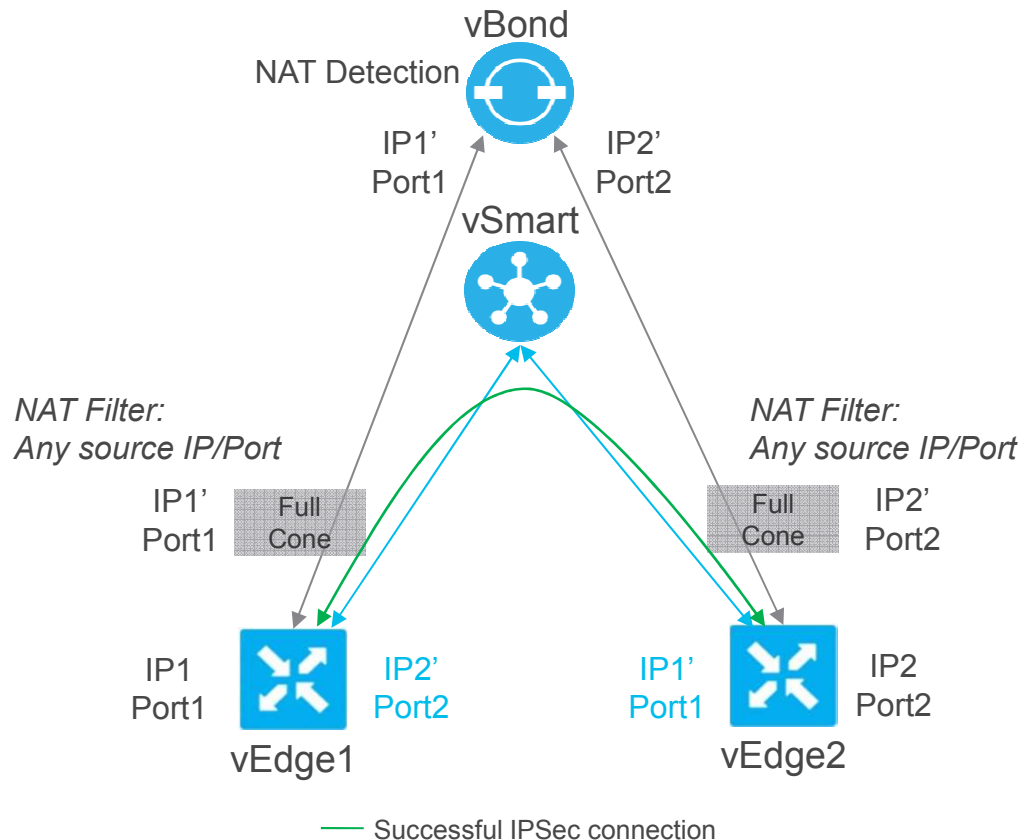
- Request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and **port**
- Only an external host that receives a packet from an internal host can send a packet back

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		

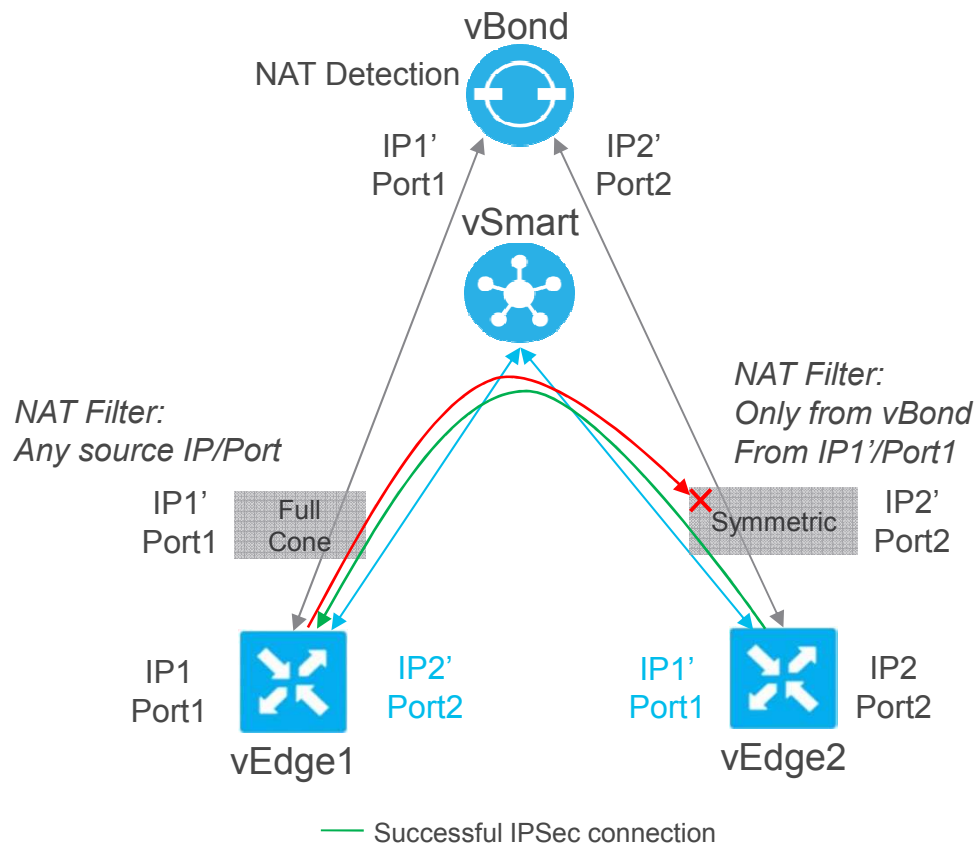
 Direct IPSec Tunnel
  No Direct IPSec Tunnel (traffic traverses hub)
  Mostly Encountered

NAT Traversal – Dual Sided Full Cone



- vBond discovers post-NAT public IP and communicates back to vEdges
 - STUN Server
- vEdges notify vSmart of their post-NAT public IP address
- NAT devices enforce no filter
 - Full-cone NAT
- Note: vEdge establishes initial connection with vBond at each bootup.

NAT Traversal – Full Cone and Symmetric

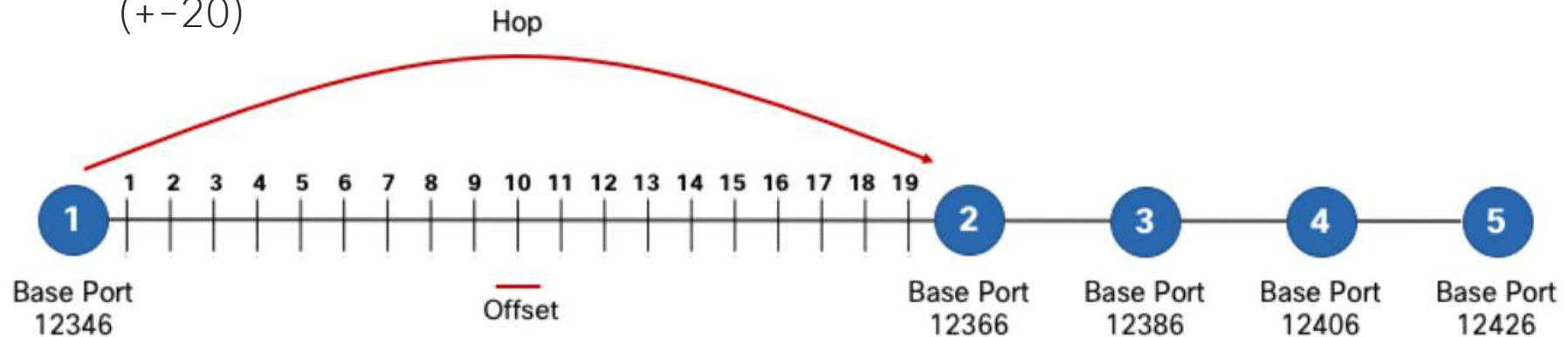


- vBond discovers post-NAT public IP and communicates back to vEdges
 - STUN Server
- vEdges notify vSmart of their post-NAT public IP address
- Symmetric NAT devices enforce filter
 - Only allows traffic from vBond
- vEdge behind symmetric NAT reaches out to remote vEdge
 - NAT entry created with filter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

Port Hopping

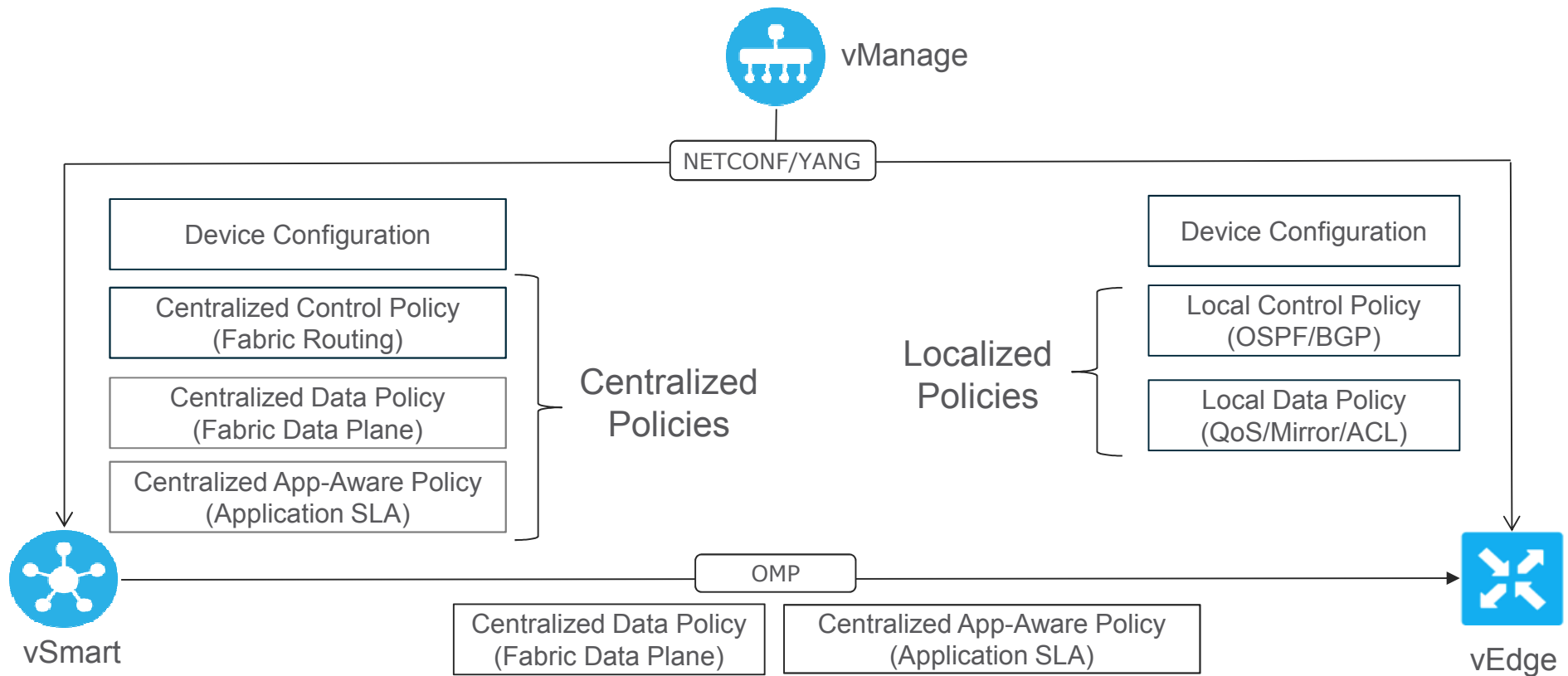
- Port Hopping
 - Adds increments from standard port to facilitate NAT-traversal
- Port Offset
 - Configure a static offset from the standard port (+-20)

- Defaults:
 - Base port 12346
 - Port offset: 0



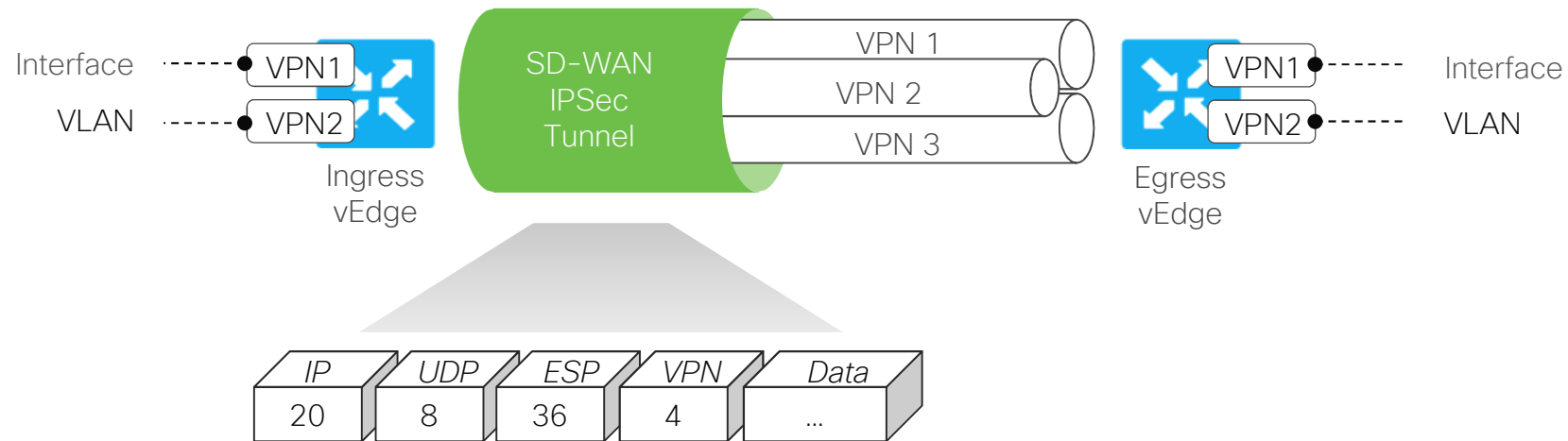
Policy framework

Policy Framework



End-to-End Segmentation

End-to-End Segmentation

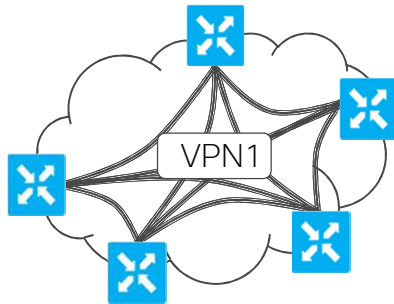


- Segment connectivity across fabric w/o reliance on underlay transport
- vEdge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs

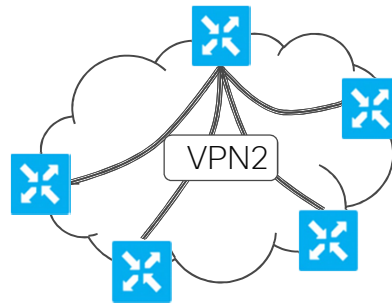
Topologies

Arbitrary VPN Topologies

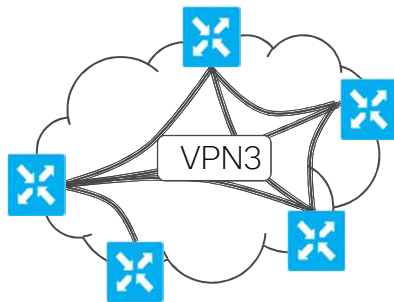
Full-Mesh



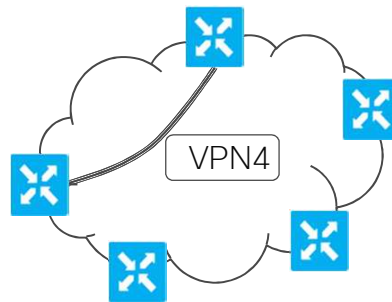
Hub-and-Spoke



Partial Mesh



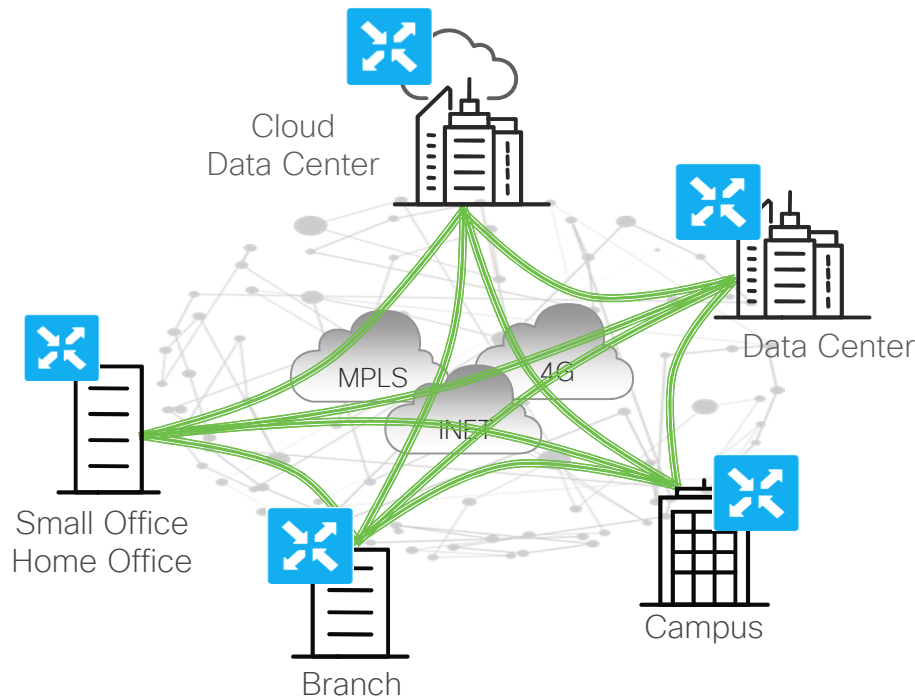
Point-to-Point



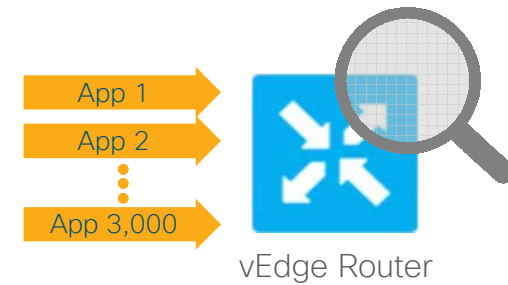
- Each VPN can have its own topology
 - Full-mesh, hub-and-spoke, partial-mesh, point-to-point, etc...
- VPN topology can be influenced by leveraging control policies
 - Filtering TLOCs or modifying next-hop TLOC attribute for OMP routes
- Applications can benefit from shortest path, e.g. voice takes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

Application Routing

Application Visibility and Recognition



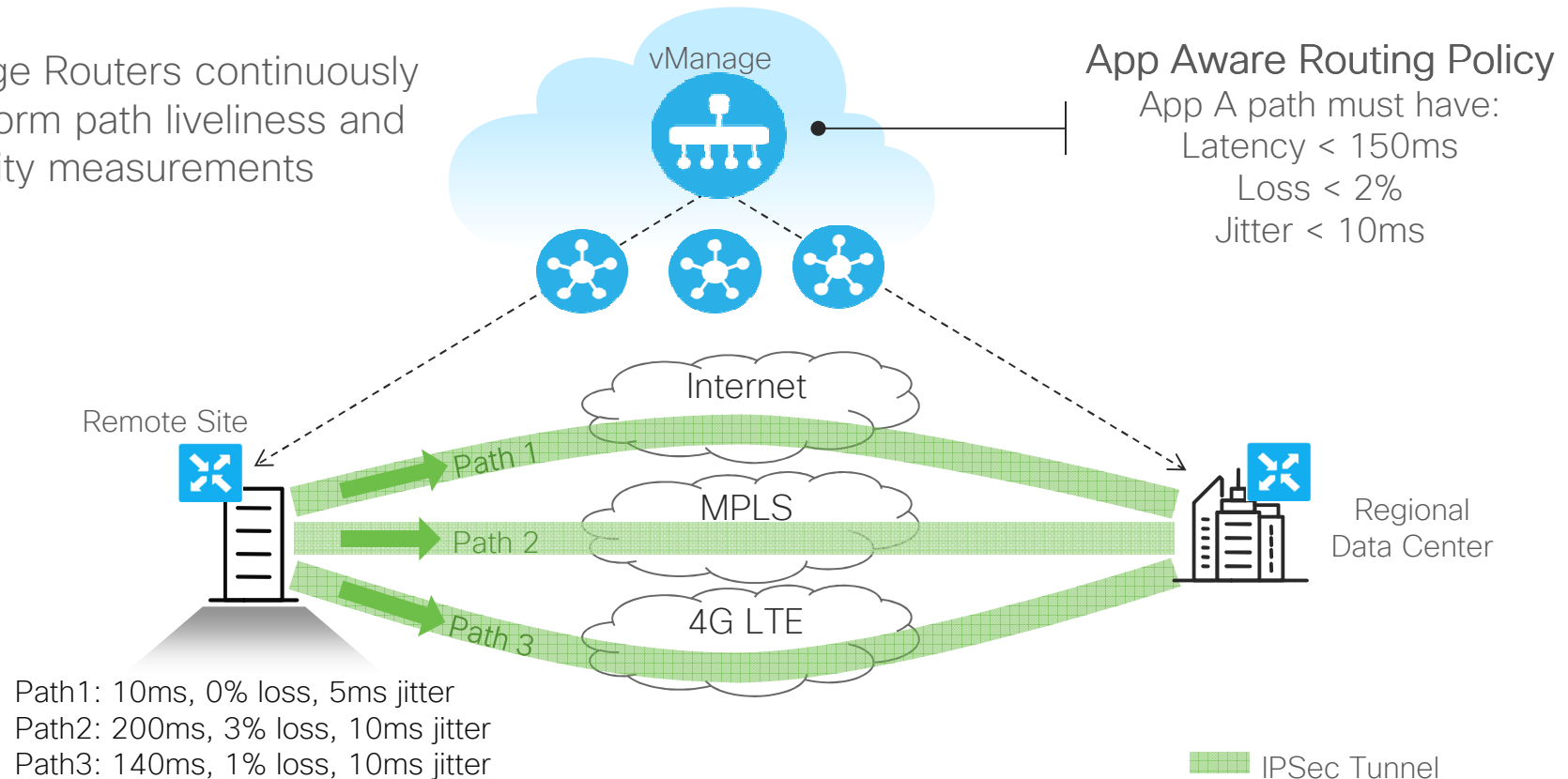
Deep Packet Inspection



- ✓ App Firewall
- ✓ Traffic prioritization
- ✓ Transport selection

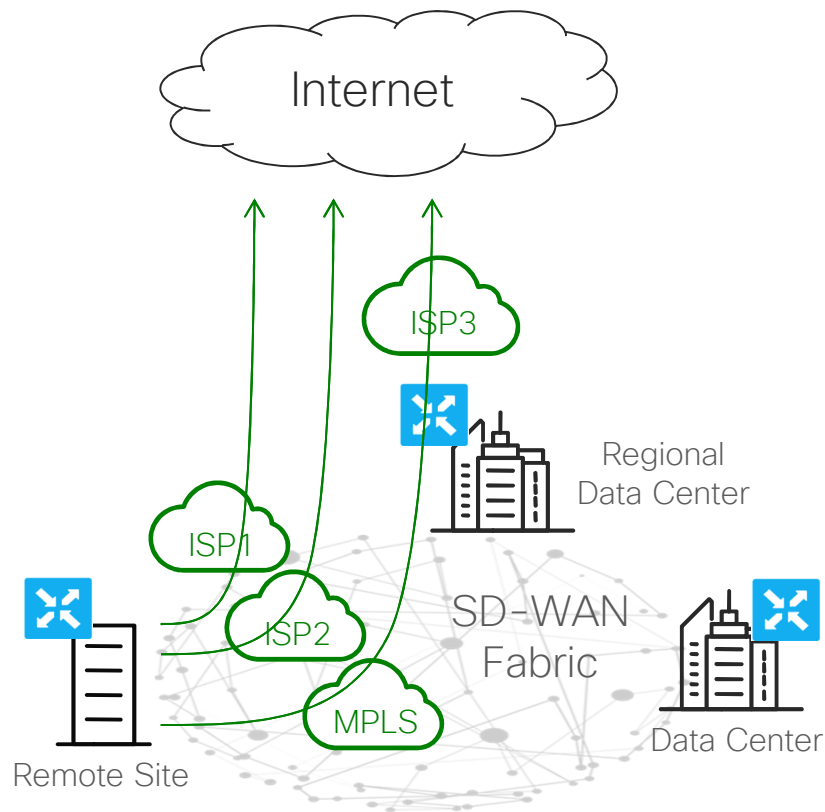
Critical Applications SLA

- vEdge Routers continuously perform path liveliness and quality measurements



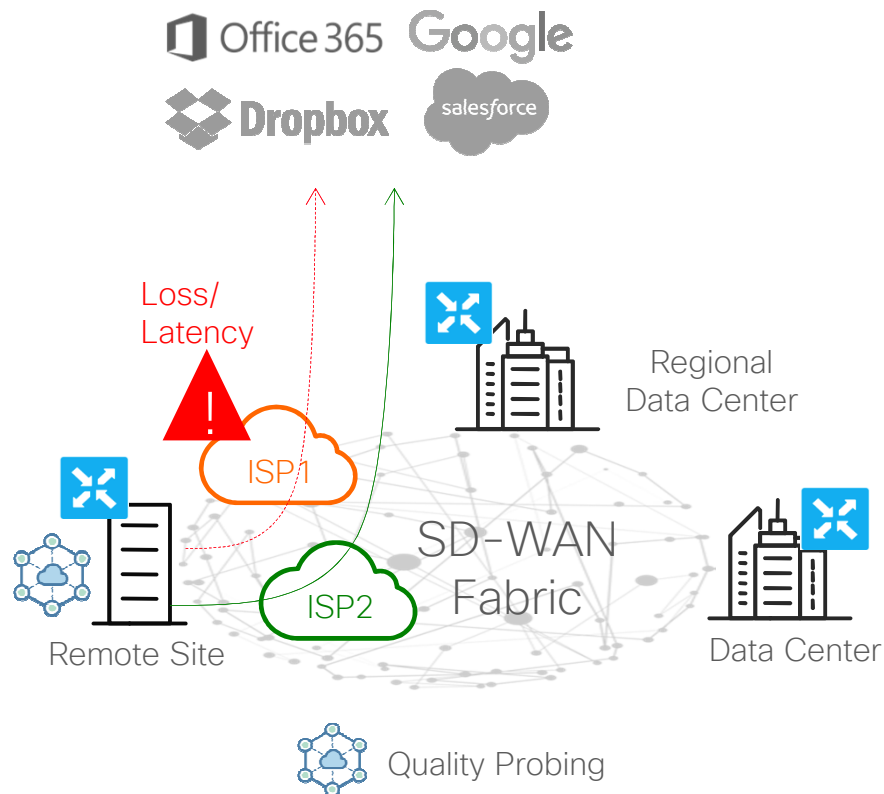
Cloud Adoption

Direct Internet Access



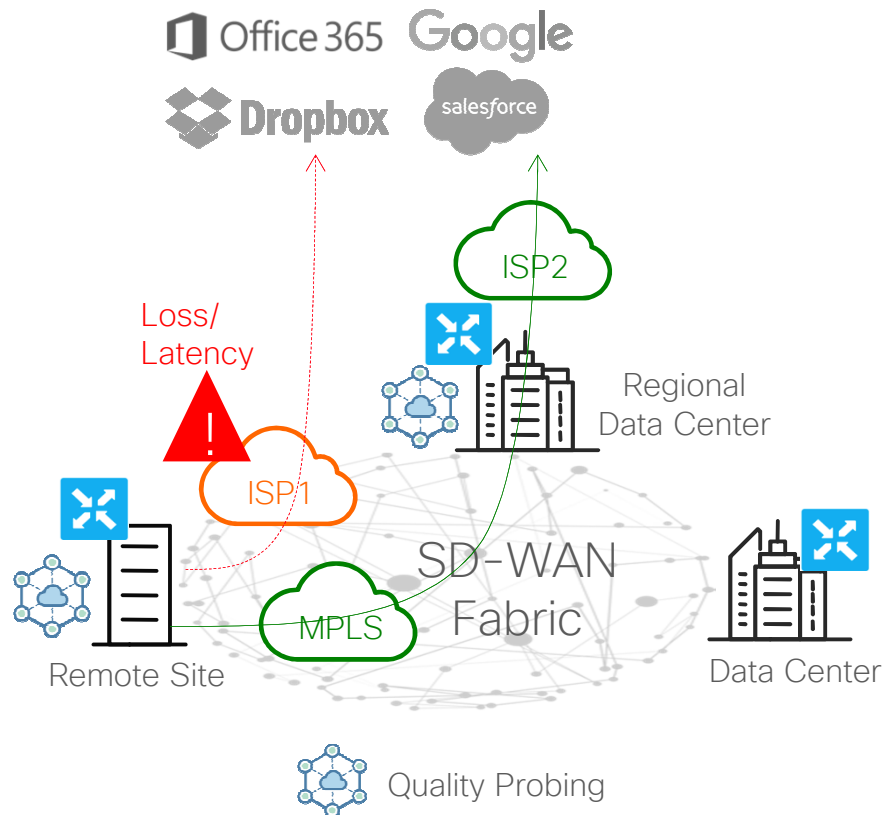
- Can use one or more local DIA exits or backhaul traffic to the regional hub through the SD-WAN fabric and exit to Internet from there
 - Per-VPN behavior enforcement
- VPN default route for all traffic DIA or data policy for selective traffic DIA
- Network Address Translation (NAT) on the vEdge router only allows response traffic back
 - Any unsolicited Internet traffic will be blocked by IP table filters
- For performance based routing toward SaaS applications use Cloud onRamp

Cloud onRamp for SaaS – Internet DIA



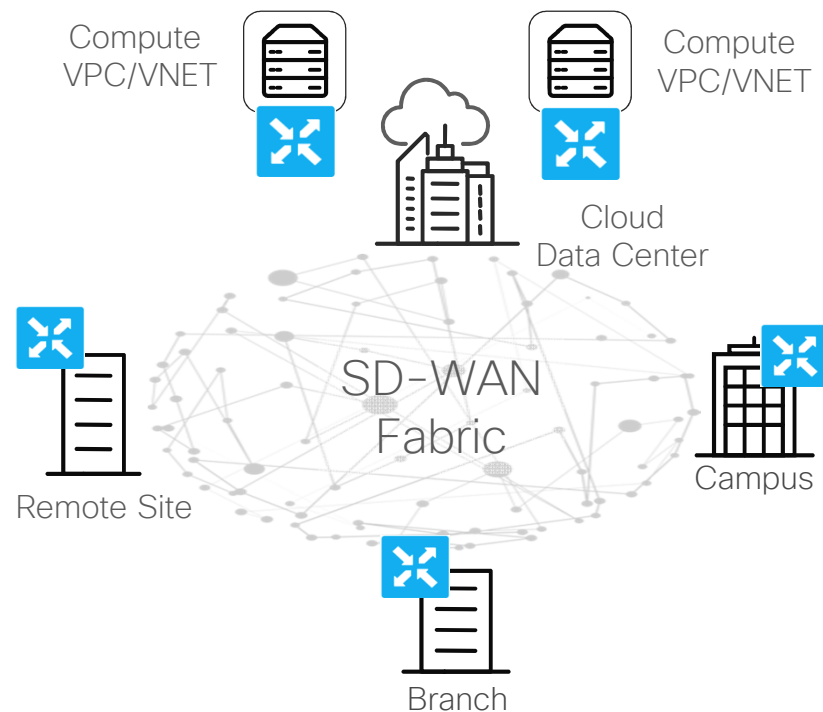
- vEdge router at the remote site performs quality probing for selected SaaS applications across each local DIA exit
 - Simulates client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
- Local DIA exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
 - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated

Cloud onRamp for SaaS – Regional Gateway



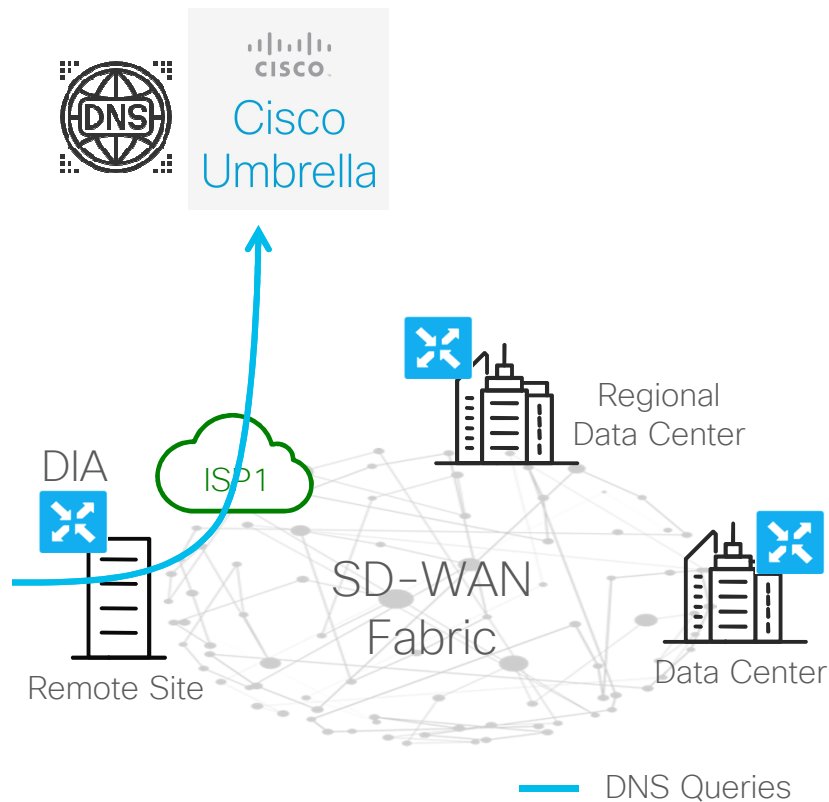
- vEdge routers at the remote site and regional hub perform quality probing for selected SaaS applications across their local Internet exits
 - Simulate client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
 - HTTP ping for local DIA and App-Route+HTTP ping for regional Internet exit
- Internet exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
 - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated

Cloud onRamp for IaaS – Attached Compute



- vEdge Cloud routers are instantiated in Amazon VPCs or Microsoft Azure VNets
 - Posted in marketplace
 - Use Cloud-Init for ZTP
- One vEdge Cloud router per VPC/VNET
 - No multicast support, can't form VRRP
 - No router redundancy
- vEdge Cloud routers join the fabric, all fabric services are extended to the IaaS instances, e.g. multipathing, segmentation and QoS
 - For multipathing, can combine AWS Direct Connect or Azure ExpressRoute with direct internet connectivity

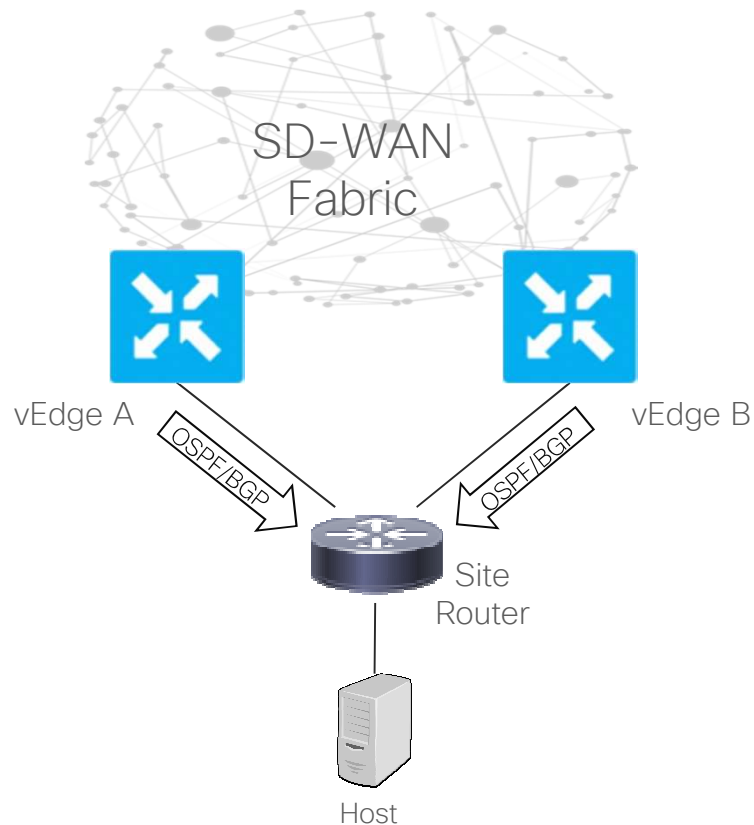
Cloud Security with Cisco Umbrella



- vEdge router intercepts client DNS queries
 - Deep Packet Inspection
- DNS queries are forwarded to Cisco Umbrella DNS servers based on the data or application aware routing policies centrally defined on vManage
 - Target DNS servers list is defined under the service side VPN
 - Policy can pin DNS query for specific application (DPI based) to specific DNS server from the list
- Cisco Umbrella enforces security policy compliance based on DNS resolution

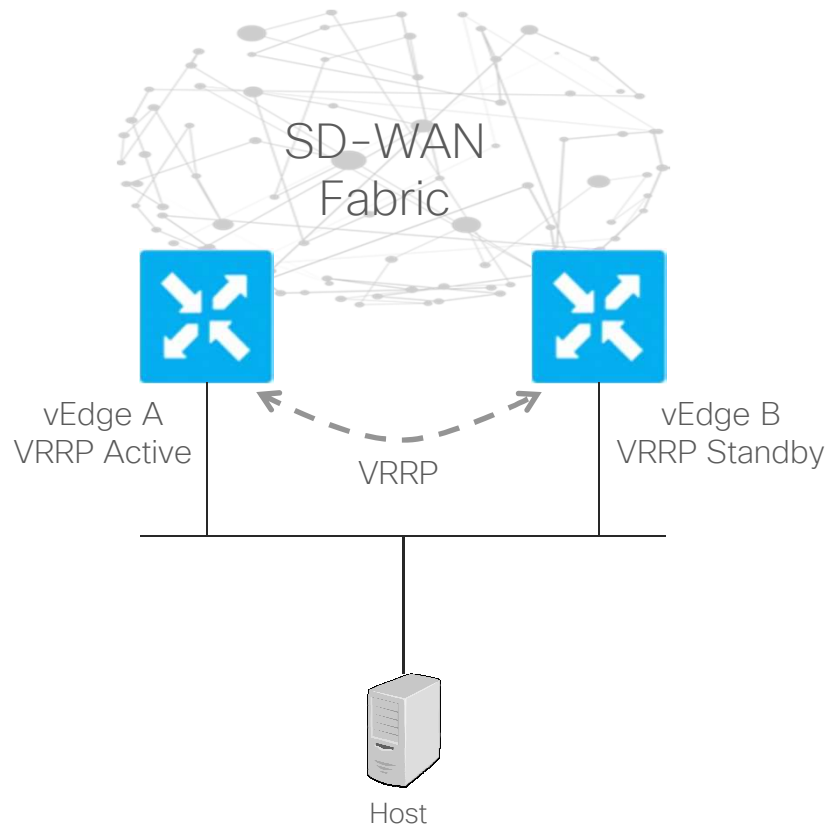
High Availability and Redundancy

Site Redundancy - Routed



- Redundant pair of vEdge routers operate in active/active mode
- vEdge routers are one or more Layer 3 hops away from the hosts
- Standard OSPF or BGP routing protocols are running between the redundant pair vEdge routers and the site router
- Bi-directional redistribution between OMP and OSPF/BGP and vice versa on the vEdge routers
 - OSPF DN bit, BGP SoO community
- Site router performs equal cost multipathing for remote destinations across SD-WA Fabric
 - Can manipulate OSPF/BGP to prefer one vEdge router over the other

Site Redundancy - Bridged

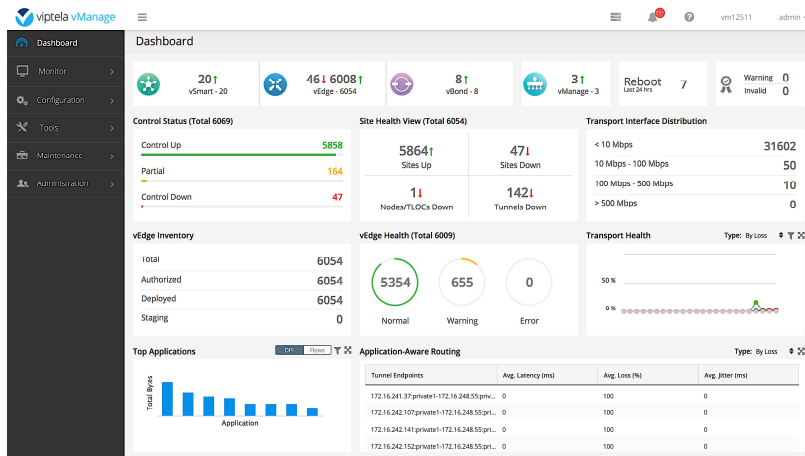


- vEdge routers are Layer 2 adjacent to the hosts
 - Default gateway for the hosts
- Virtual Router Redundancy Protocol (VRRP) runs between the two redundant vEdge routers
 - Active/active when using multi-group (per-VLAN)
- VRRP Active vEdge responds to ARP requests for the virtual IP with its physical interface MAC address
 - No virtual MAC
- In case of failover, new VRRP Active vEdge router sends out gratuitous ARP to update ARP table on the hosts and mac address table on the intermediate L2 switches

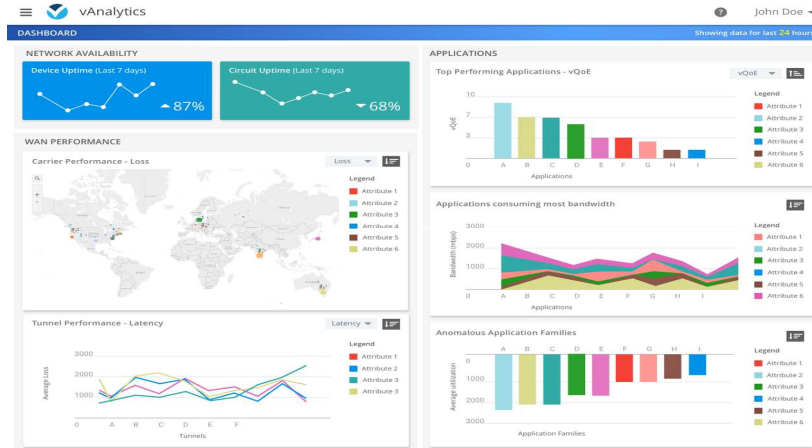
Operational Simplicity and Transparency

Simplified Management

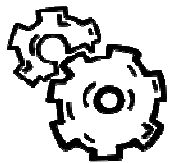
Single Pane Of Glass Operations



Rich Analytics



Power Tools



REST



NETCONF



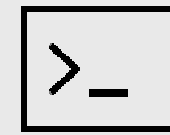
Syslog



SNMP



Flow Export

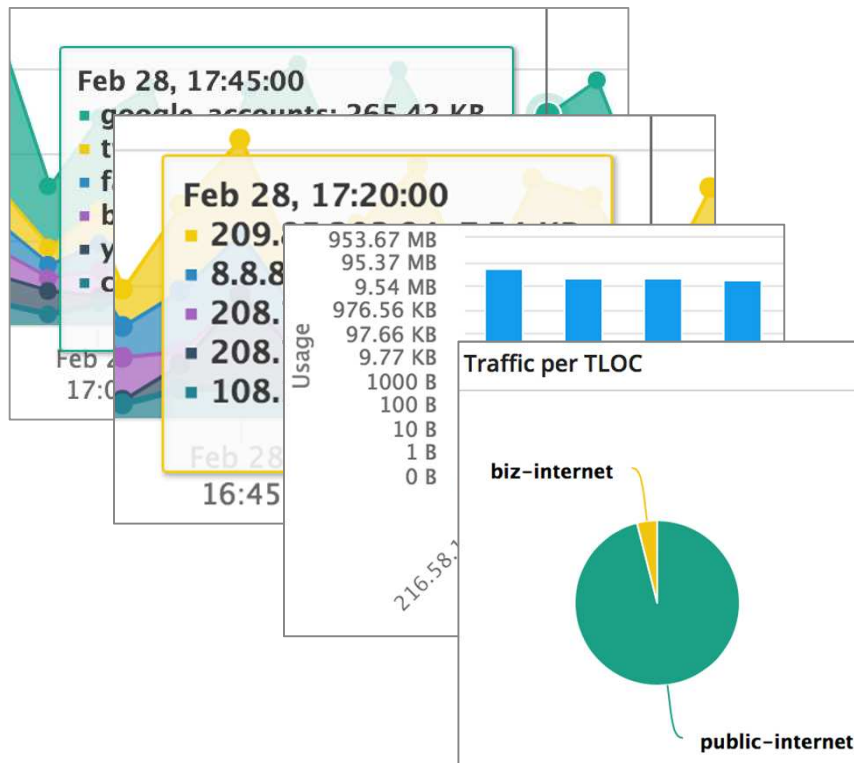


CLI



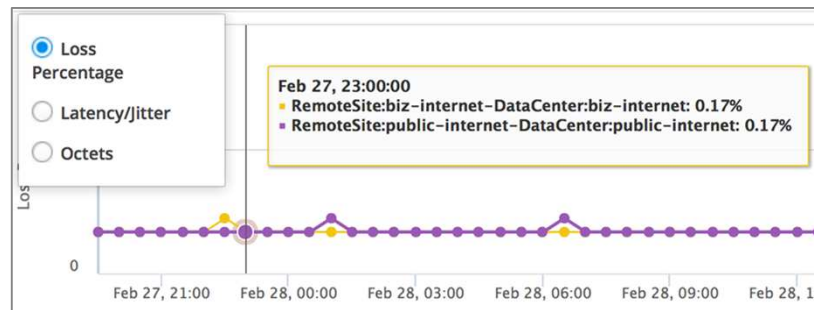
Linux Shell

Application and Flow Visibility



- Application and flow visibility for each vEdge router
 - DPI needs to be enabled for application visibility
 - Flow data can be exported from vEdge to external collector
- Realtime views or custom timeline views granularity
- Views can be zoomed into

Path Performance



- BFD is used to measure performance characteristics of each individual IPSec tunnel
- Loss, latency and jitter is represented in the tunnel performance graph on the vManage
- Realtime views or custom timeline views granularity
- Views can be zoomed into

Agenda

- ☐ Overview
- ☐ Solution Elements and Overview
- ☐ Selective “Deep-Dive”
- ☐ Bonus
- ☐ Licensing

Driving DNA subscriptions across EN

DNA subscriptions available across entire EN portfolio by end of Q3'18



Building DNA adoption momentum across EN

Benefits of software subscription for routing



Latest innovations
through simple
subscription tiers

Cisco ONE Advantage

DNA-Advantage

DNA-Essentials



Across the
routing portfolio

Across ISR 1000 & 4000,
ASR 1000, ENCS 5000,
Viptela vEdge routers



Management
flexibility

Cloud managed or
on-prem managed

Capabilities for Cloud Managed through vManage

DNA Essentials

Connectivity
VPN Overlay, Topology: Hub-n-spoke, NAT, Split tunnel,
2 VPNs: 1 transport, 1 service side
VPN with L2 or L3

Security
Encryption: AES-256,
Policy support: Local ACL only, Data policy

Application Experience
QoS (classification, policing, remarking, scheduling), App-aware routing (5 tuple only),
DPI for visibility, App visibility (name, throughput)

Management
Viptela vManage platform, Zero Touch
Provisioning, Day 0 , day 1, day N Changes

3,5 Year Terms

DNA Advantage (Include DNA Essentials)

Connectivity
Service-side routing, Mesh topology, Multicast
VPNs: 5 (1 transport, 4 service side)

Security
Control policy
Advanced policies: Service chaining, extranet

Application Experience:
DPI for app-aware routing and policies
SaaS on-ramp (was CloudExpress)
TCP Optimization

Management & Orchestration
End to end SD-WAN policy orchestration,
network and application trouble shooting

3,5 Year Terms

C1 Advantage (Include DNA Essentials & DNA Advantage)

Connectivity: VPNs: Up to system scale

Advanced Application Experience
WAN Full stack WAAS

Analytics:
VAnalytics platform

3,5 Year Terms

Platforms Supported Now: vedge
Platforms Support Post July: ISR, ASR, ENCS

