
cisco
You make possible

Delivering Cisco Next Generation SD-WAN with Viptela

Nikolai Pitaev
Engineer, Technical Marketing
Enterprise Networks BU
npitaev@cisco.com

BRKCRS-2110

cisco Live!
Barcelona | January 27-31, 2020

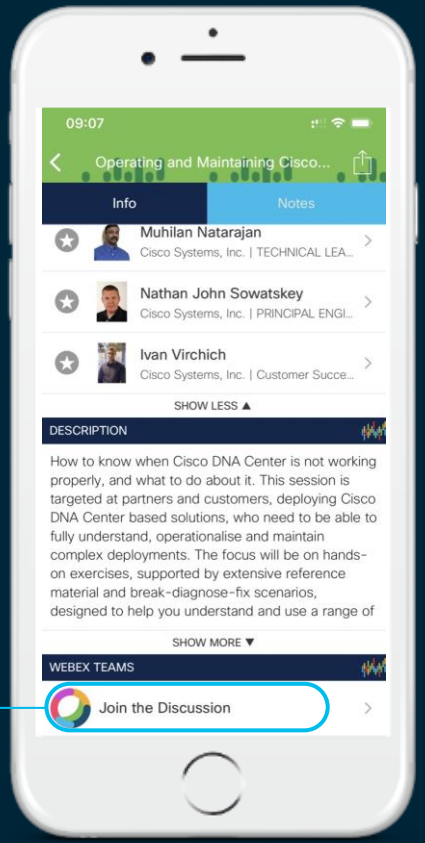
Cisco Webex Teams

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



“What’s in it for me?"

In this session:

- Introduction, design and building blocks
- Use cases and deployment options
- Live demonstrations

Out of scope:

- Detailed explanation how it technically works “under the hood”
- Troubleshooting and debugging
- Step-by-step migration

Target audience is technical attendees looking for **overview** and **basic understanding** of the Cisco SD-WAN solution powered by Viptela.

Why should I care?
Real life examples

- 80 percent reduction in cost/Mbps for a US insurance provider
- $20 million reduction in OpEx over three years for a retailer

- 5-fold improvement in Office 365 performance for an energy provider
- 4-fold improvement in application latency for a healthcare provider

- M&A integration in 2 weeks for a Fortune 50 healthcare provider
- Securely isolated 100+ business partners for a US manufacturer with more than 1,000 sites

Key Message of the presentation

Cisco SD-WAN Solution helps you to:

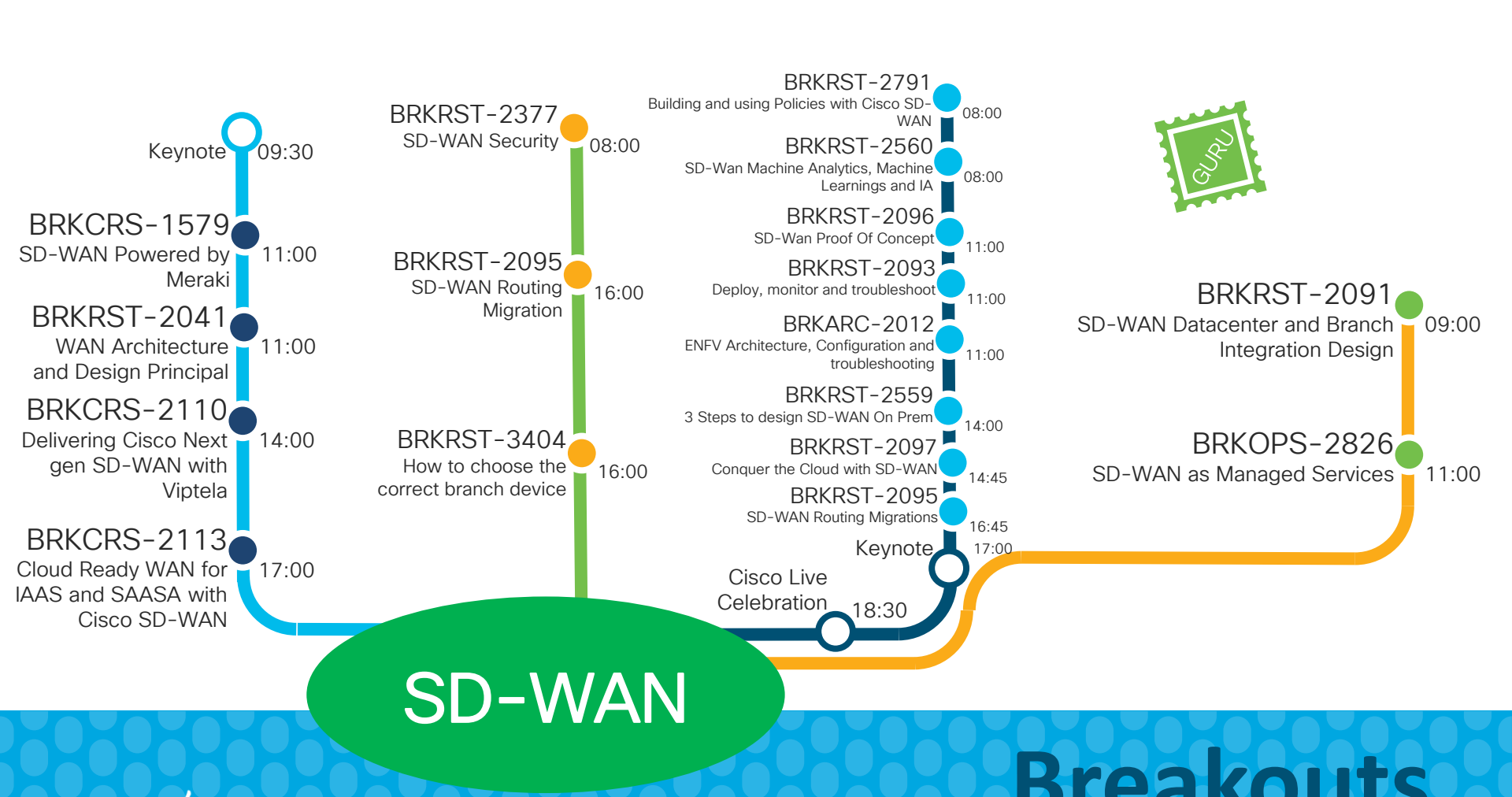
1. Reduce Cost

2. Operate Faster with better Performance and Security

3. Integrate Latest Cloud and Network Technologies

Agenda

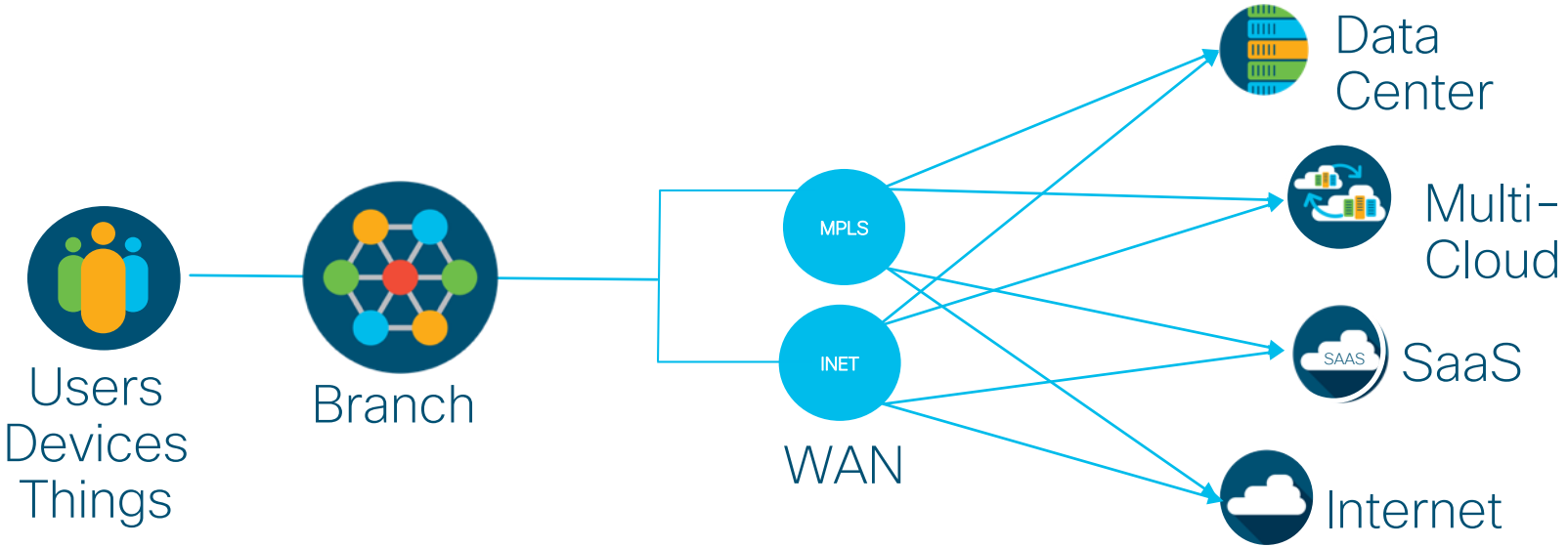
- Introduction: Why SD-WAN? Which SD-WAN?
- SD-WAN architecture and main components
- SD-WAN fabric
- Use cases and common enterprise deployments
- Conclusion: outlook and summary



Breakouts

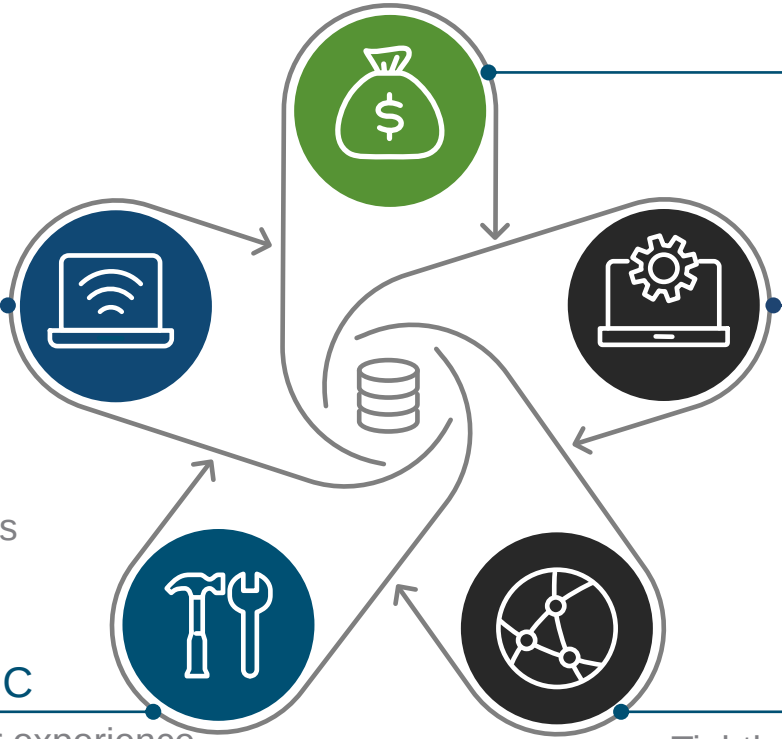
Introduction

The WAN Has Changed



Traditional and Legacy Architectures

Cannot Scale to Address Changing Needs



EXPENSIVE

Hardware-centric

Fixed capacity

POORLY INTEGRATED

Conflicting policies and configurations

Inflexible and static

Risk from accidental interactions and vulnerabilities

DIFFICULT TO SUPPORT

Discrete device-by-device configurations

Complex management silos

Require slow truck rolls for changes

CONNECTIVITY-CENTRIC

Fragmented, incomplete user experience

Not application-centric

INFLEXIBLE

Tightly controlled, client server model

Historical vs predictive management

Cisco SD-WAN Portfolio

cisco SD-WAN

Powered By

cisco Meraki

Full stack branch management for Lean IT

Powered By

Viptela

Flexible and sophisticated with secure segmentation and advanced routing

SD-WAN Architecture

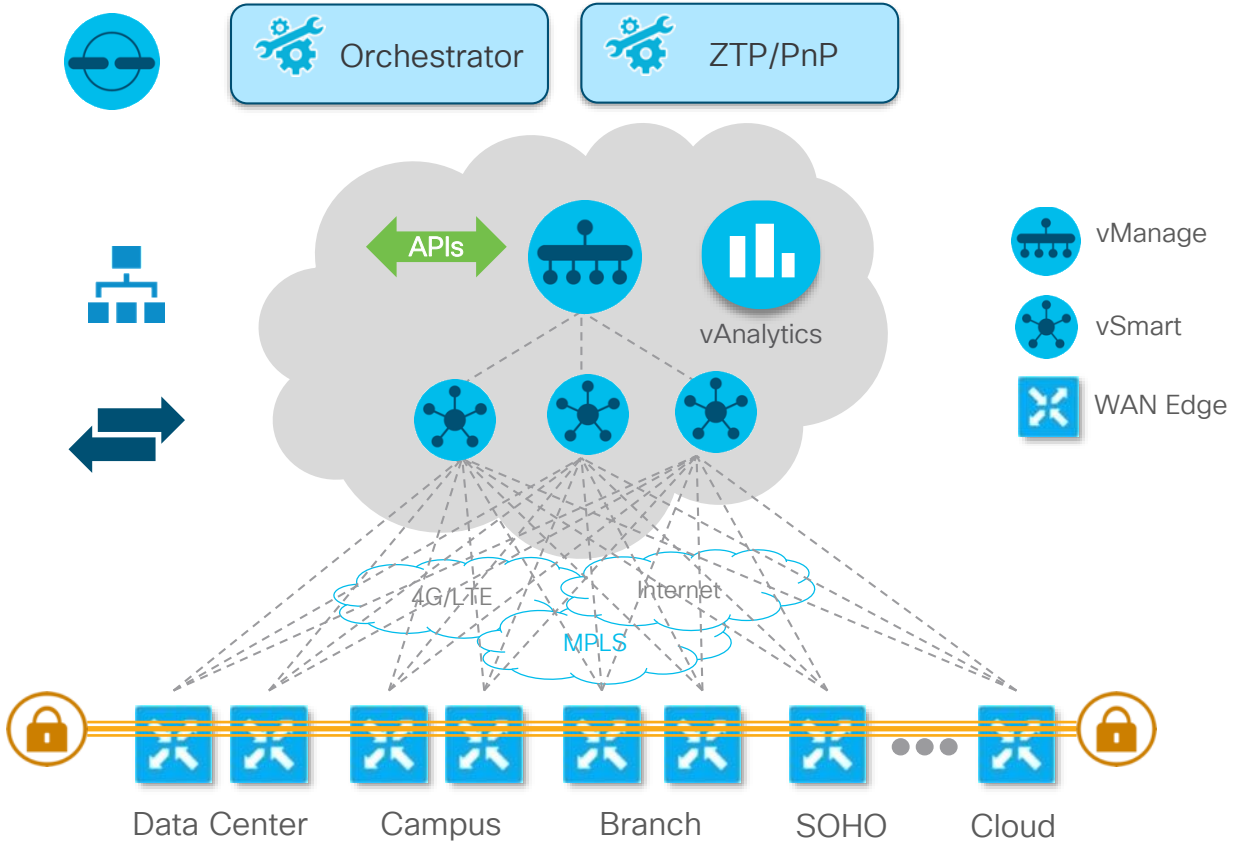
Cisco SD-WAN Architecture Overview

Orchestration = vBond

Management = vManage
(Multi-tenant or Dedicated)

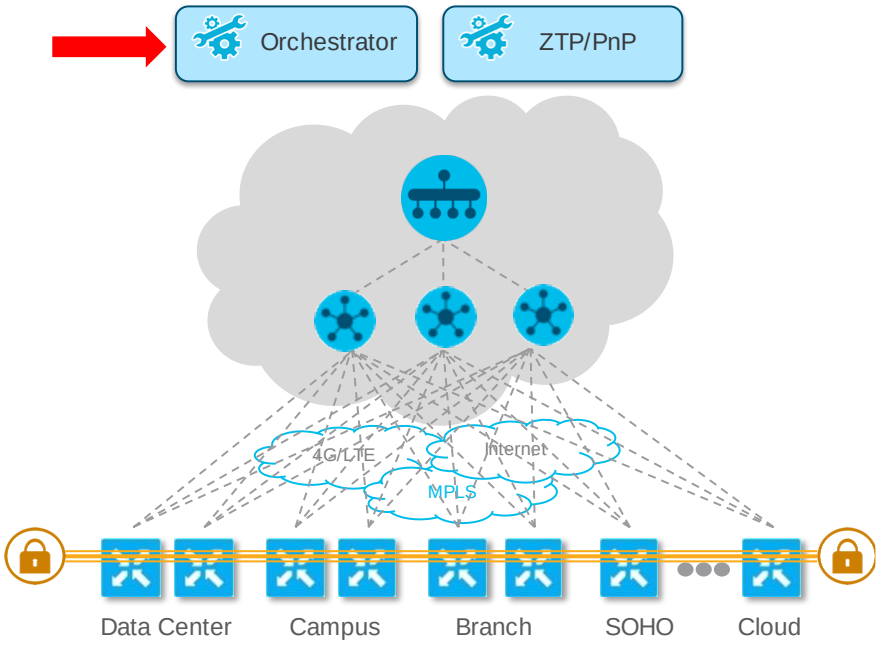
Control Plane = vSmart
(Containers or VMs)

Data Plane = WAN Edge
(vEdge, Cisco ISR/ASR/ENCS, Whitebox)



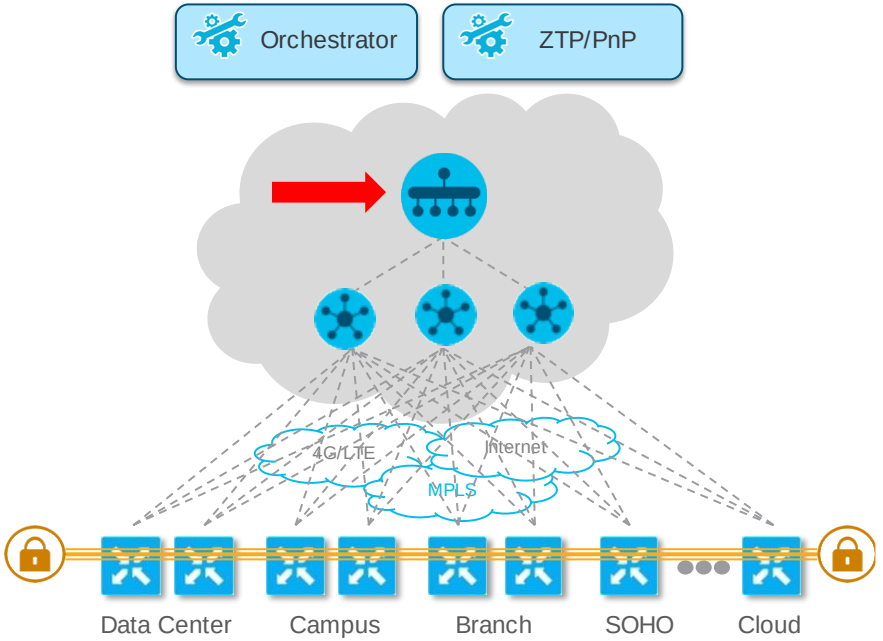
vBond is SD-WAN Orchestrator

- Orchestrates connectivity between management, control and data plane
- Serves as the first point of authentication
- Requires public IP address for non-private deployments
- All other components need to know the vBond IP or FQDN
- Authorizes all control connections based on white-list model



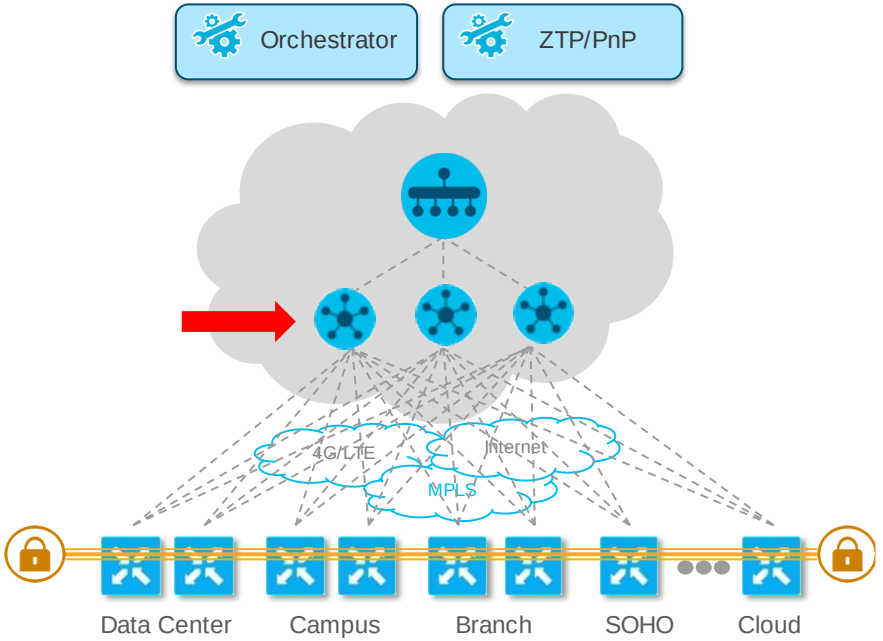
vManage is NMS for SD-WAN

- Single-tenant or Multitenant
- Single pane of glass for Day 0, Day 1 and Day 2 operations
- Enables centralized provisioning and simplifies changes
- Supports REST API, CLI, Syslog, SNMP, NETCONF
- Provides real time alerting
- Role Based Access Control

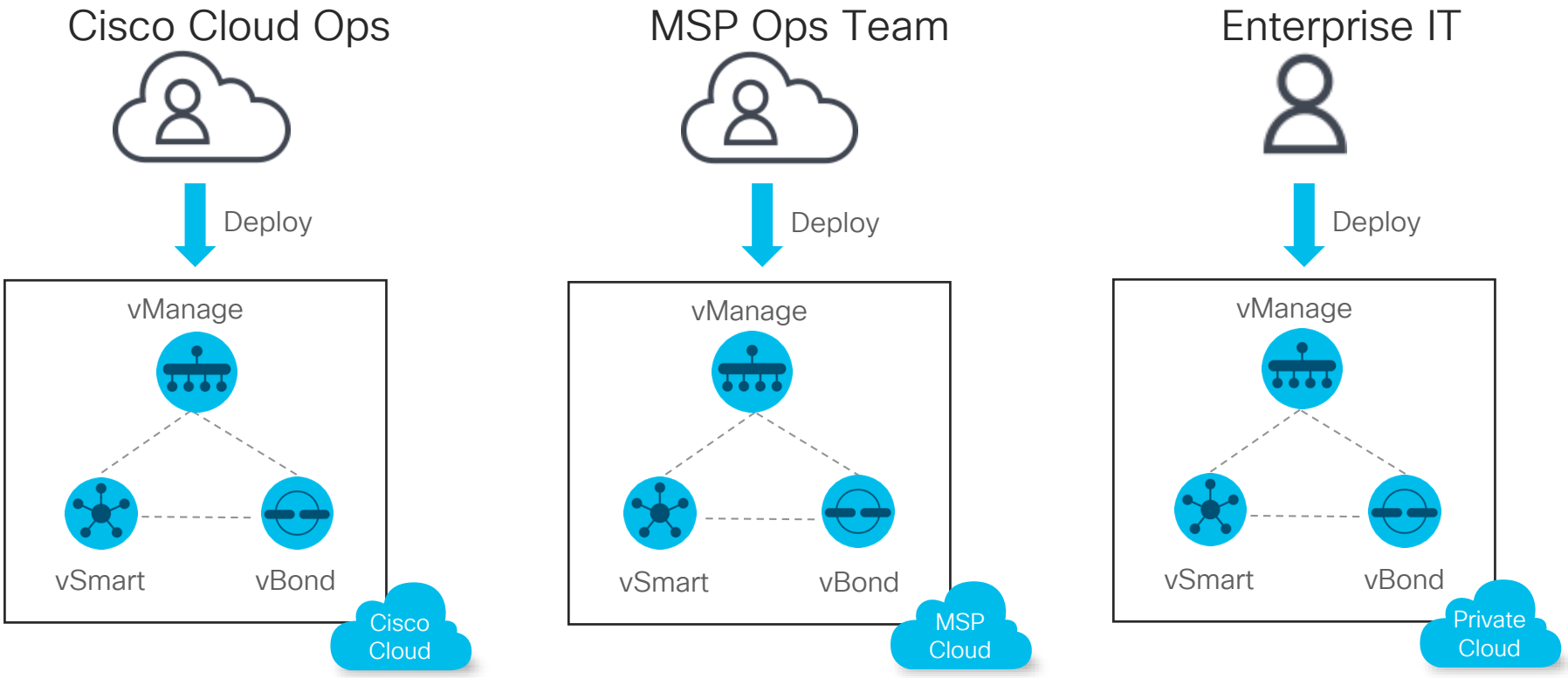


vSmart is Centralized Control Plane

- Implements control plane policies, such as service chaining, traffic engineering and per-VPN topology
- Reduces complexity of the entire network
- Establishes peering with all WAN Edges, distributes connectivity and security context



Controllers' Deployment Models



Validated Controller Scale

vManage:

2,000 Devices per-single instance
Max Production Deployment: 6 instances

vSmart:

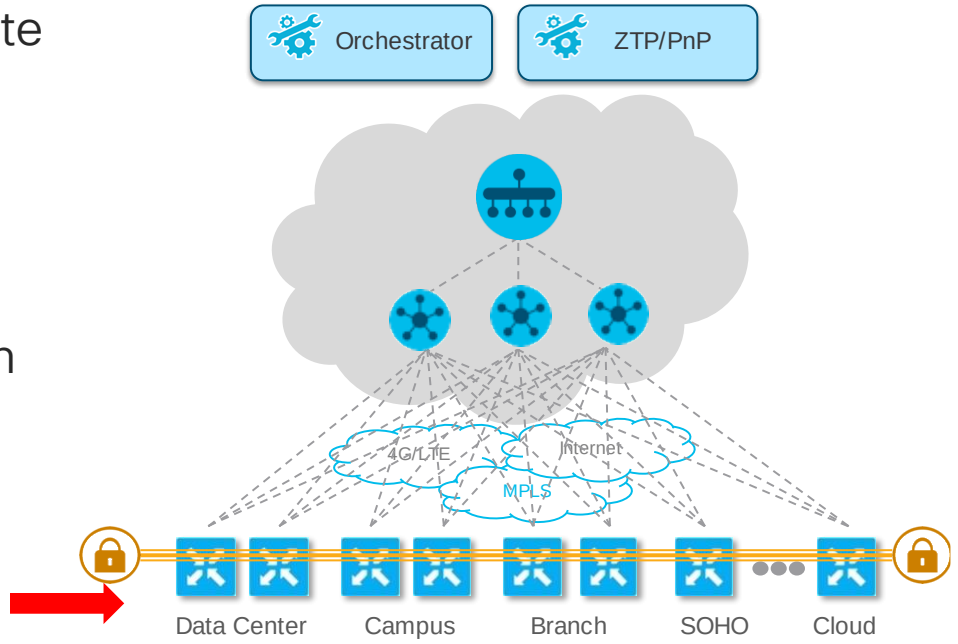
5,400 Connections per-single vSmart
Max Production Deployment: 20 vSmarts

vBond:

1,500 Connections per-single vBond
Max Production Deployment: 6 vBonds

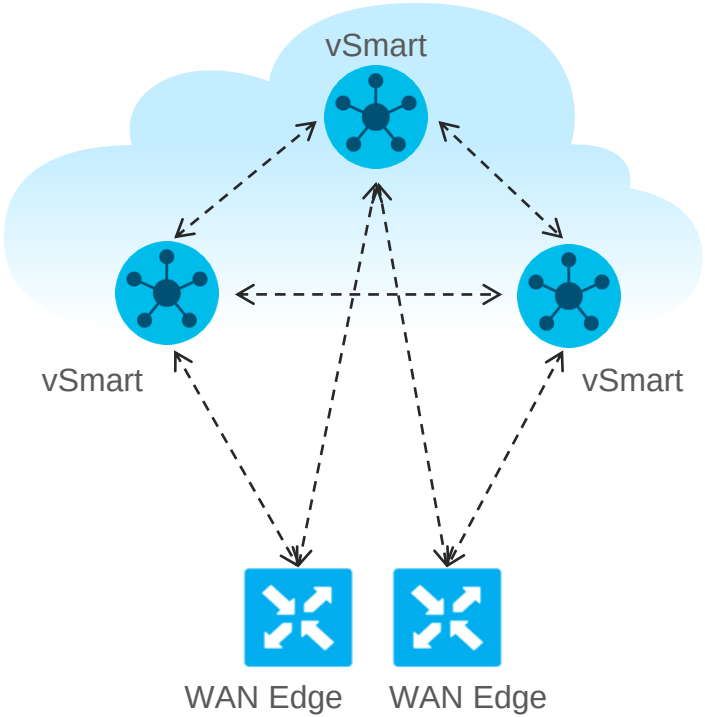
WAN Edge is your SD-WAN Data Plane

- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with vSmart controllers
- Implements data plane and application aware routing policies
- Exports performance statistics
- Physical or Virtual form factor



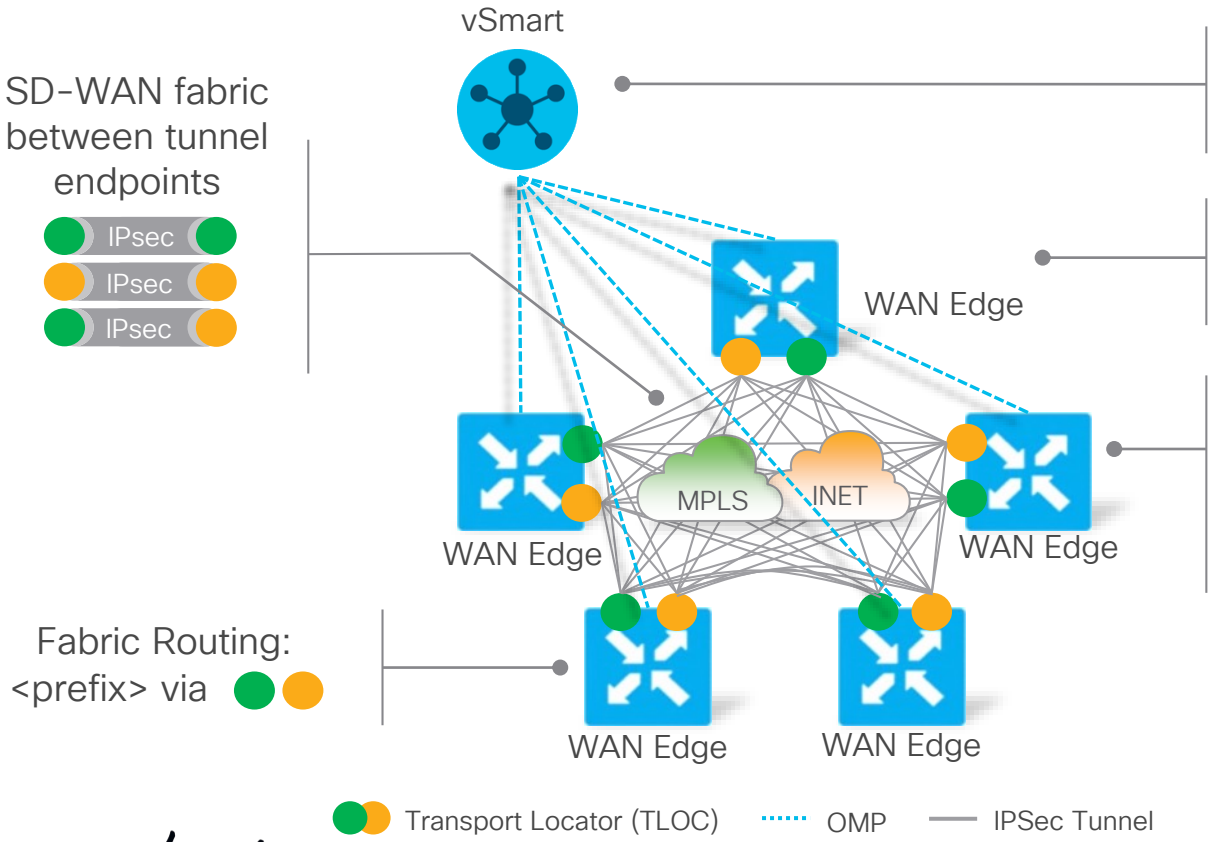
SD-WAN Fabric

Unified Control Plane



- Overlay Management Protocol (OMP)
- TCP based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane complexity and raises overall solution scale

Data Plane Establishment



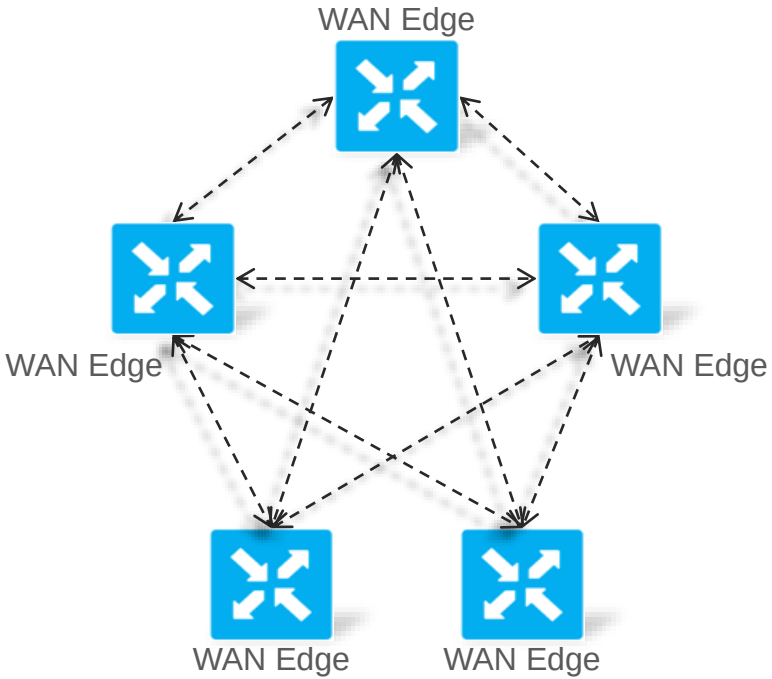
vSmarts advertise routes and encryption keys to WAN Edges in OMP updates

Routes and encryption keys are advertised to vSmarts in OMP updates

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

Security Context
- IPSec Encryption Keys

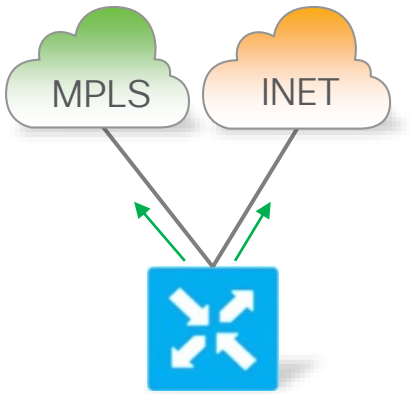
Data Plane Liveliness and Quality



- 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

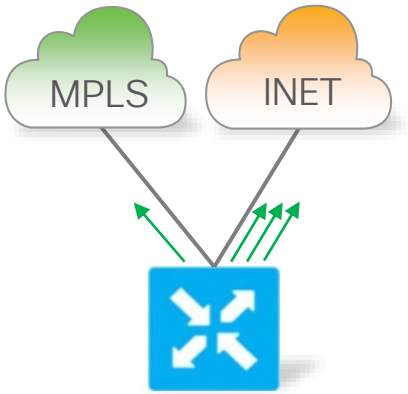
Common Data Plane Communication

Per-Session Load Sharing
Active/Active



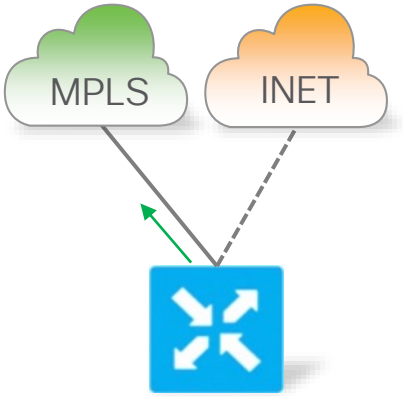
Default

Per-Session Weighted
Active/Active



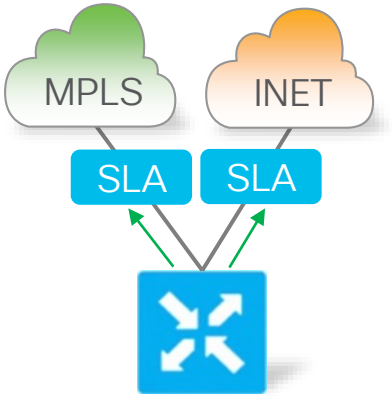
Device
Configurable

Application Pinning
Active/Standby



Policy
Enforced

Application Aware Routing
SLA Compliant



Policy
Enforced

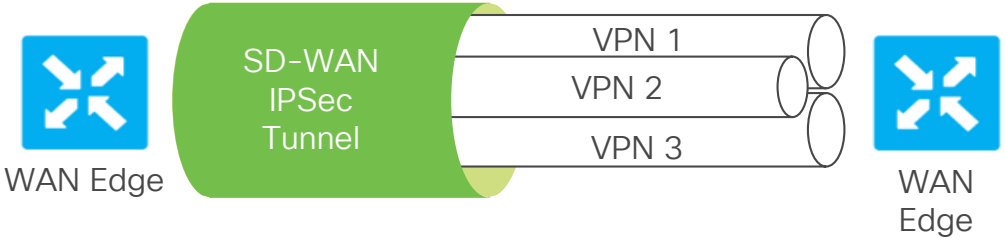
SD-WAN Use Cases

SD-WAN use cases

1. Segmentation, zero touch provisioning and automation
2. Improve application experience
3. Secure Direct Internet Access (DIA)
4. SaaS optimization
5. Extend SD-WAN to public clouds

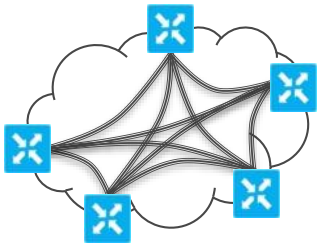
One user interface across branch, cloud and colocation

Segmentation

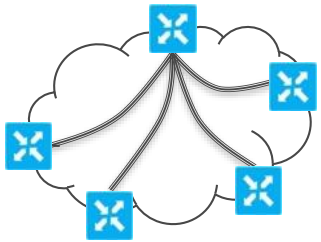


- Security Zoning
- Compliance
- Guest Wi-Fi
- Multi-Tenancy
- Extranet

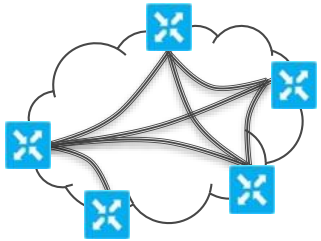
Per-VPN Topology



Full-Mesh

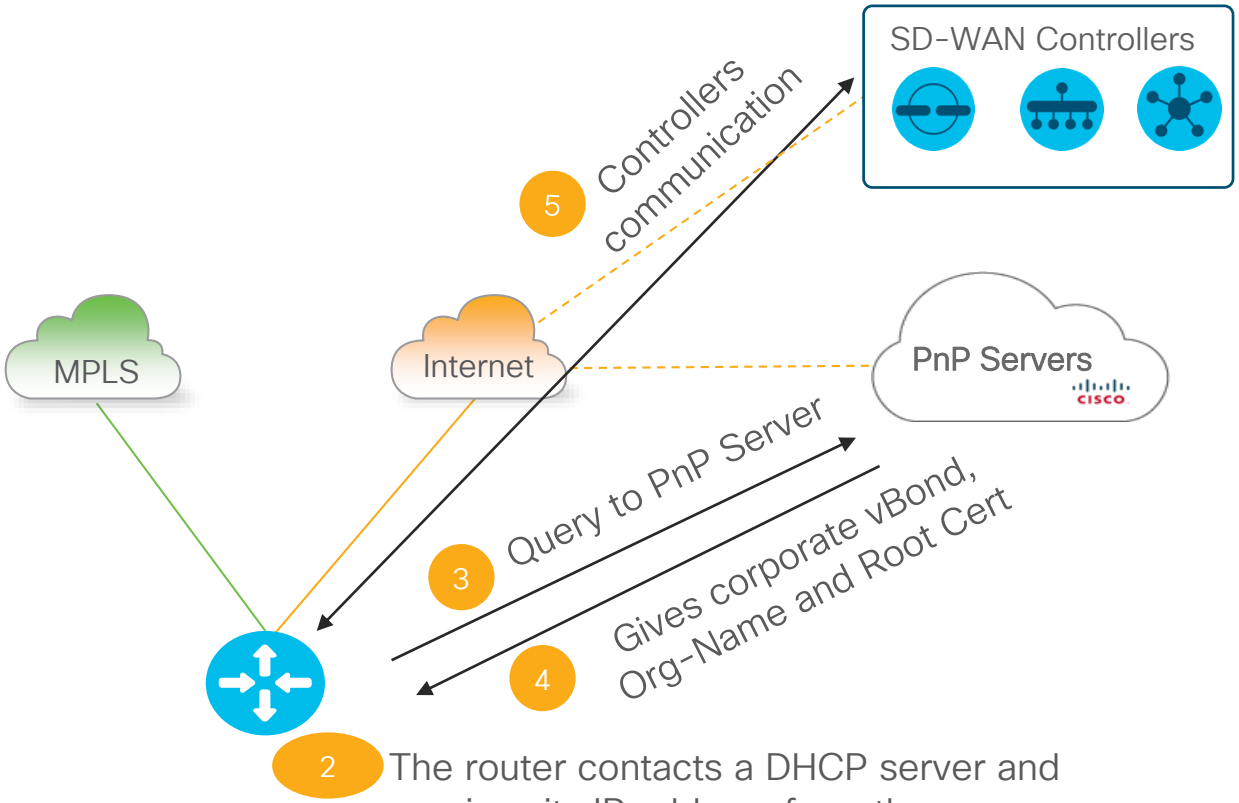


Hub-and-Spoke



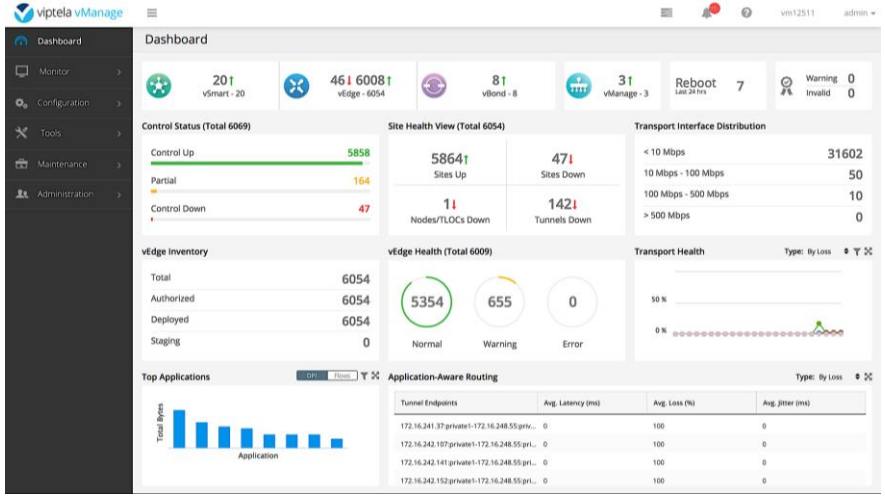
Any Topology

On-Boarding example for WAN Edge

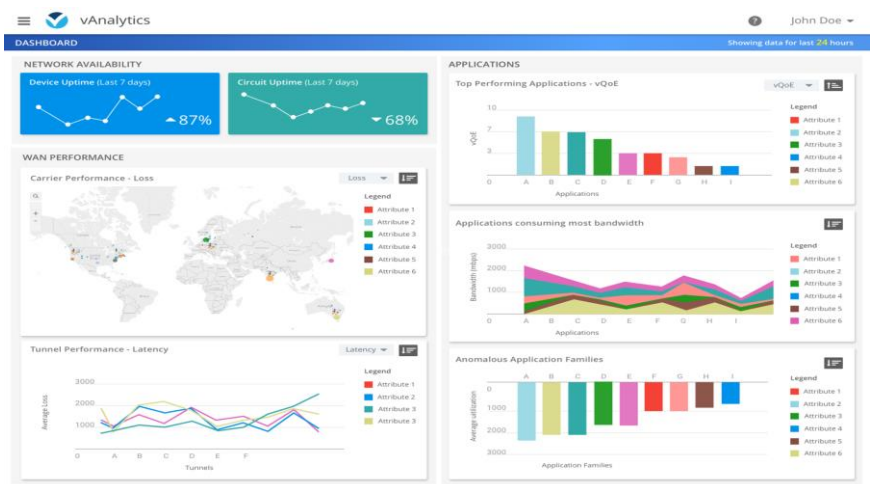


Automation and Simplified Management

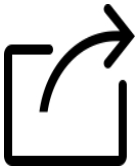
Single Pane Of Glass Operations



Rich Analytics

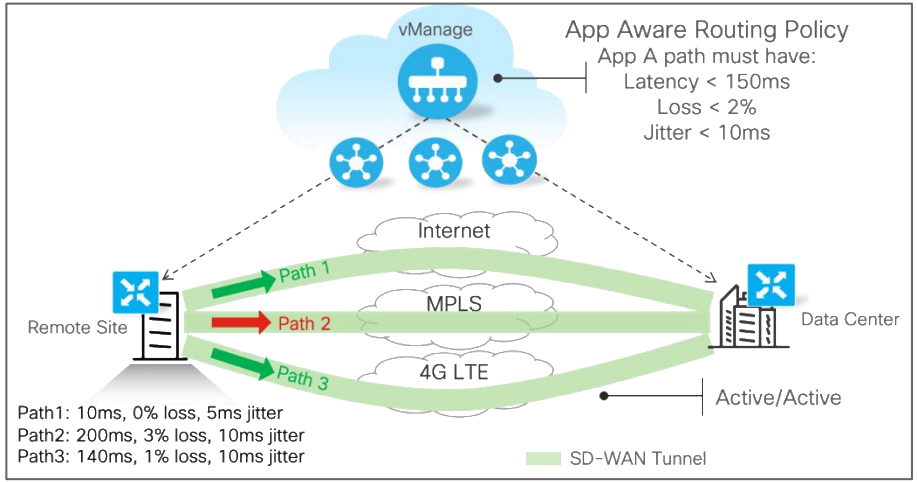


Power Tools

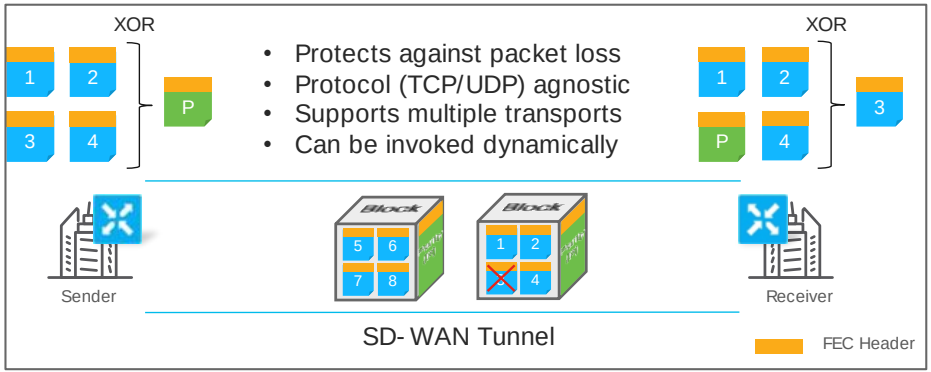


Critical Applications SLA

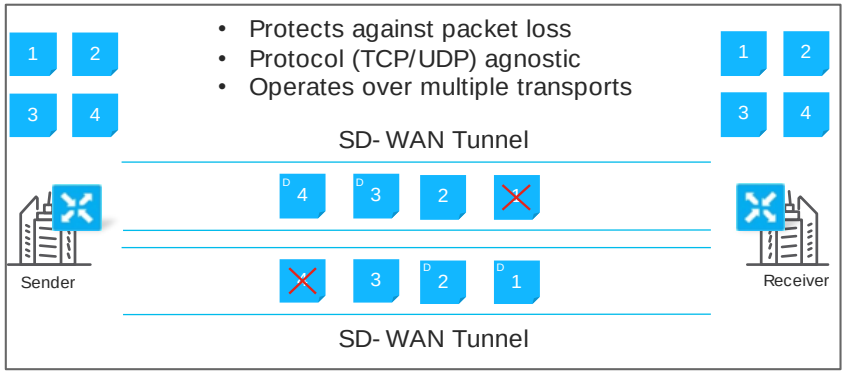
Application Aware Routing



Forward Error Correction (FEC)



Packet Duplication



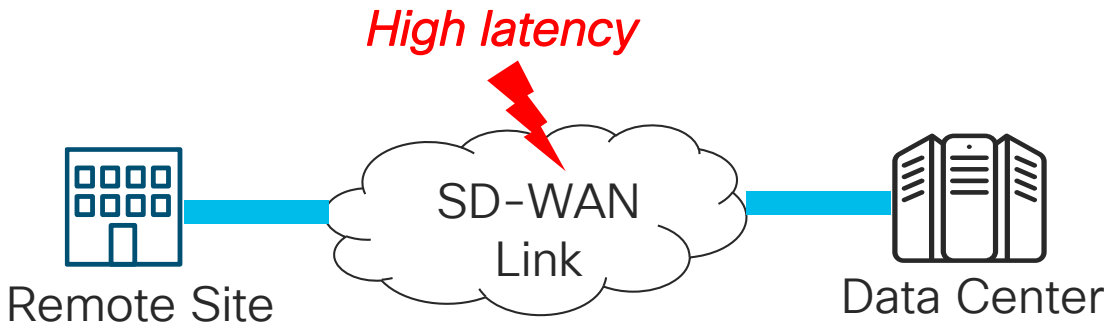
TCP Optimization

Problem:

- WAN Transport Link between two SD-WAN routers has high latency

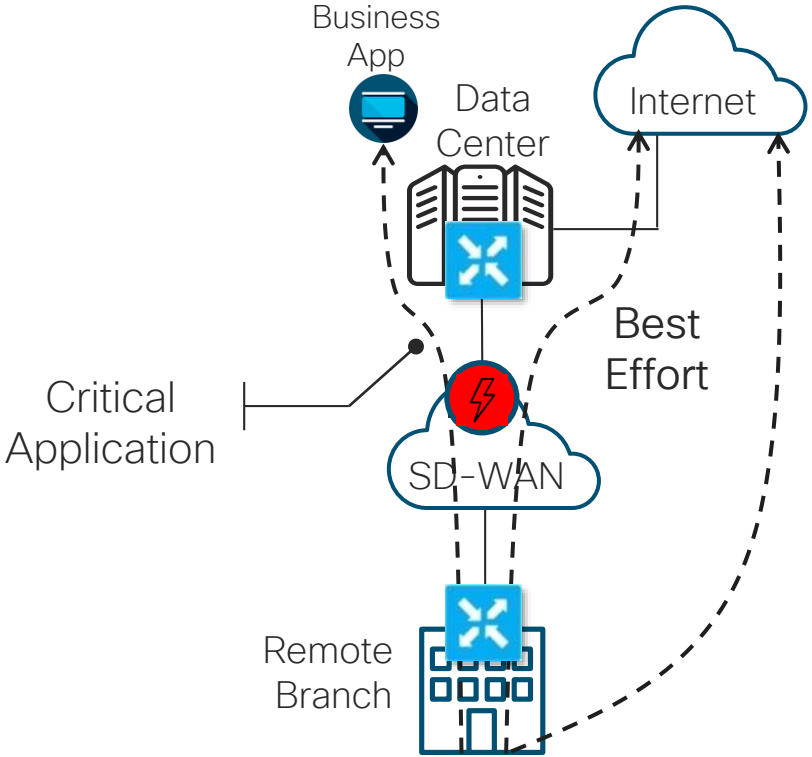
Solution:

- Enable TCP Optimization for critical traffic between two SD-WAN sites



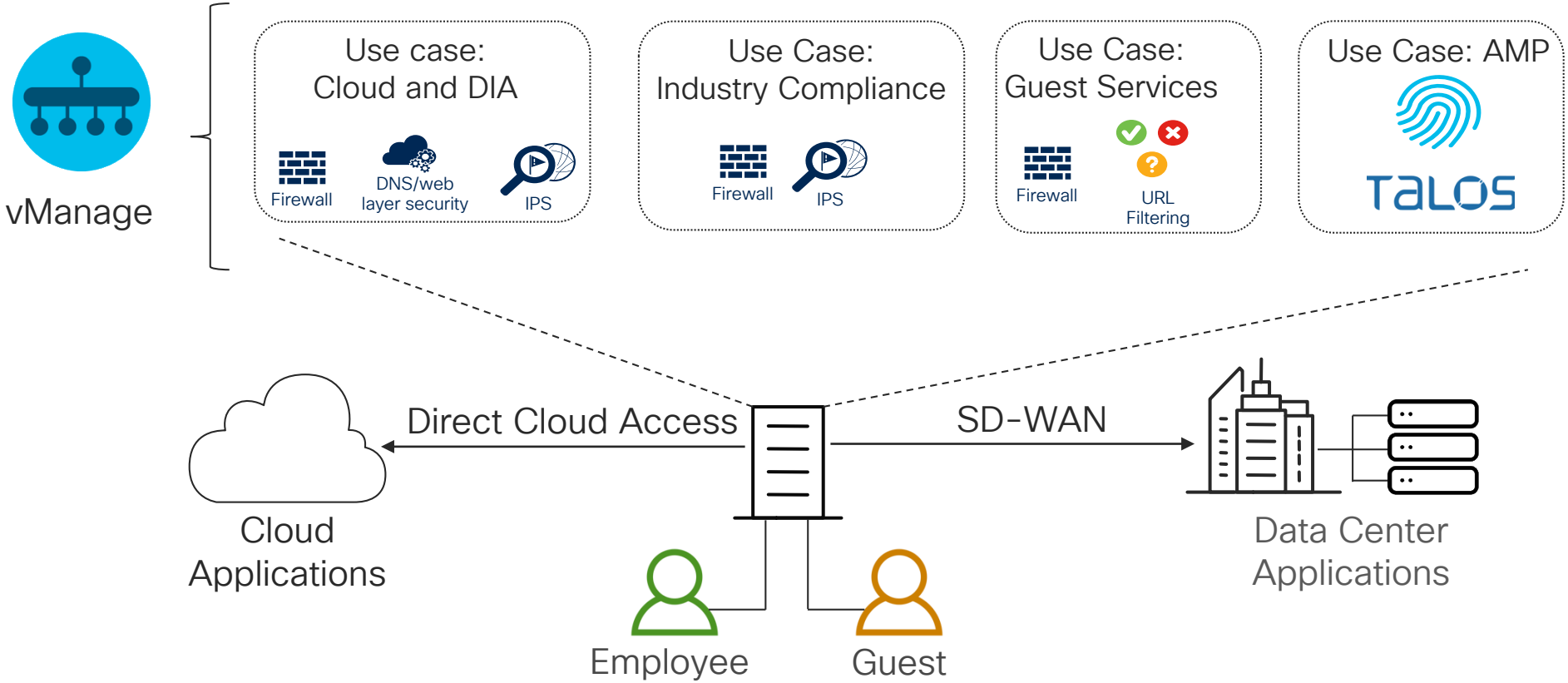
TCP Optimization demo

Direct Internet Access (DIA) offload



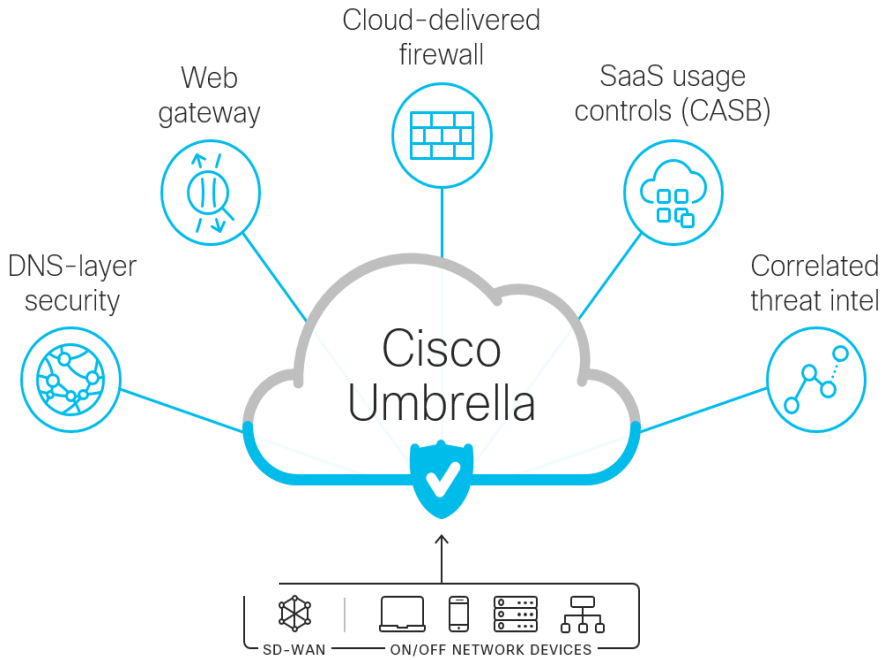
- Best Effort traffic congests WAN links and impacts critical app between DC and branch
- SD-WAN Policy reroutes Best Effort traffic over DIA
- Critical app performance is restored

Secure Direct Internet Access – on-prem



Secure Direct Internet Access – in the cloud

- Secure Internet Gateway (SIG) is a platform with many different security services.
- The current platform includes DNS-layer security, Web Gateway (SWG), Cloud Delivered Firewall, CASB
- Currently, Umbrella supports traffic redirection for SIG services via IPSec tunnel.
- WAN Edge routers will be supported with automated tunnel creation coming in 1HCY20.
  Today – simple manual provisioning.

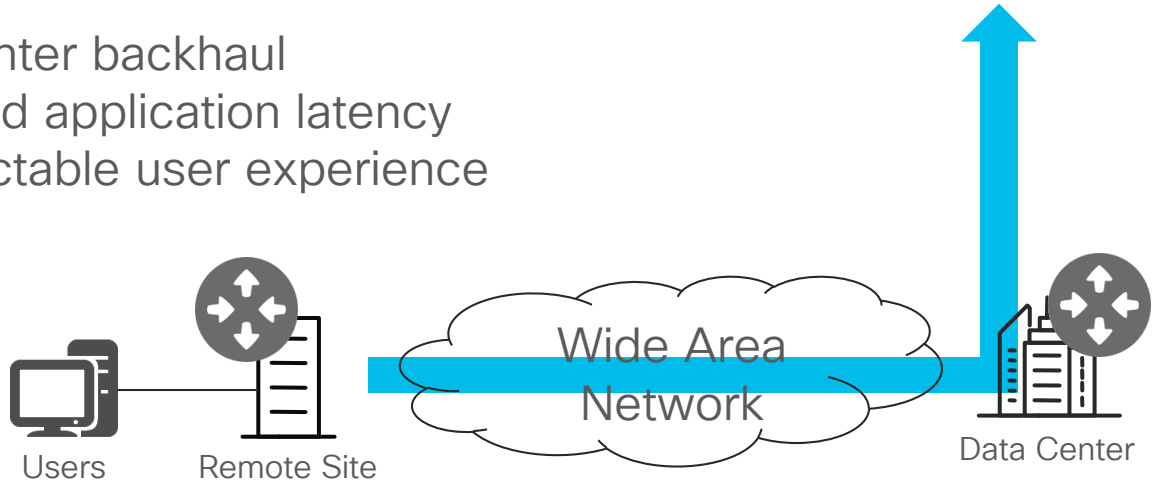


SaaS Optimization

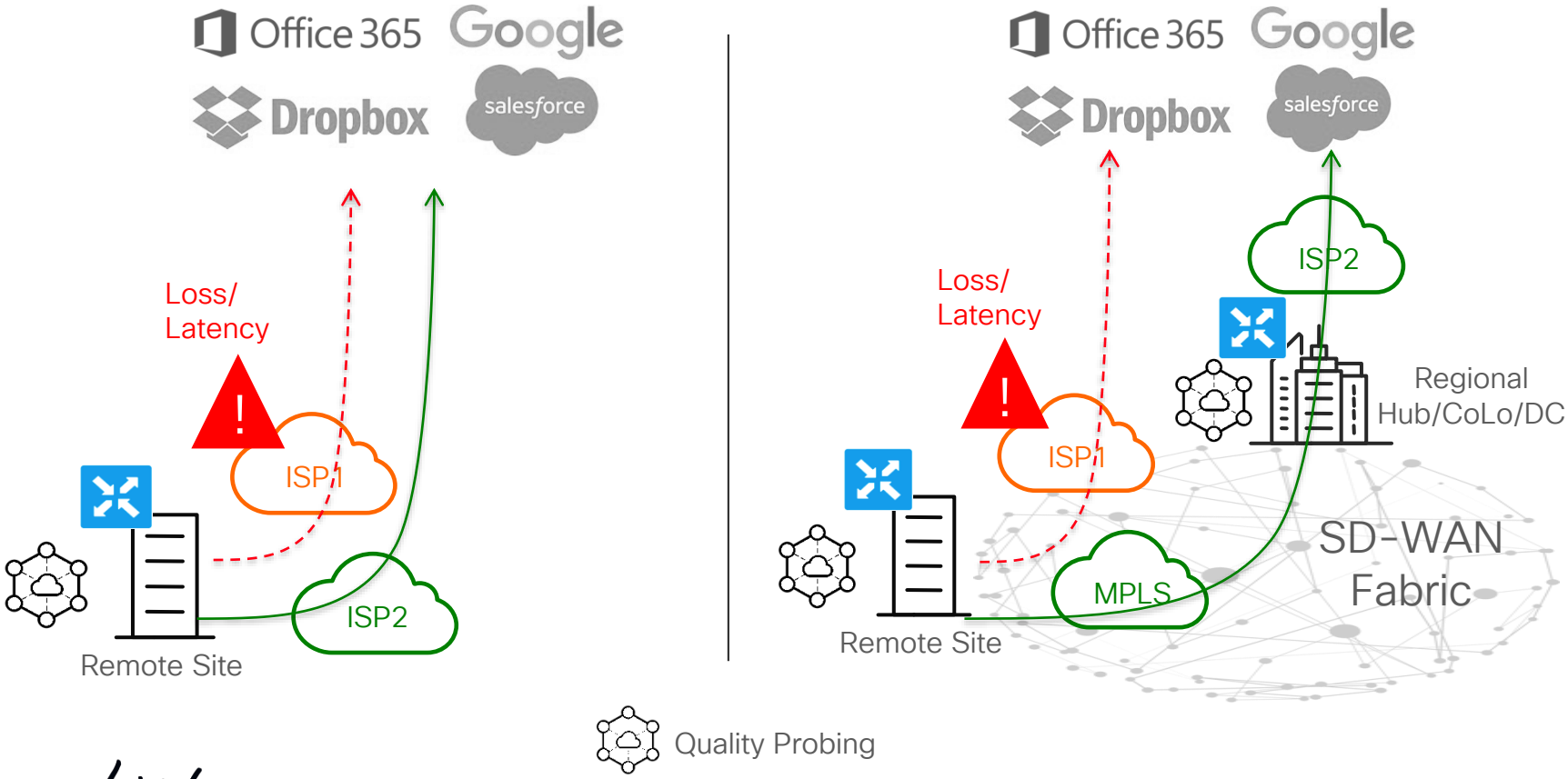
Traditional Cloud Applications Access

Office 365 Google Dropbox salesforce

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

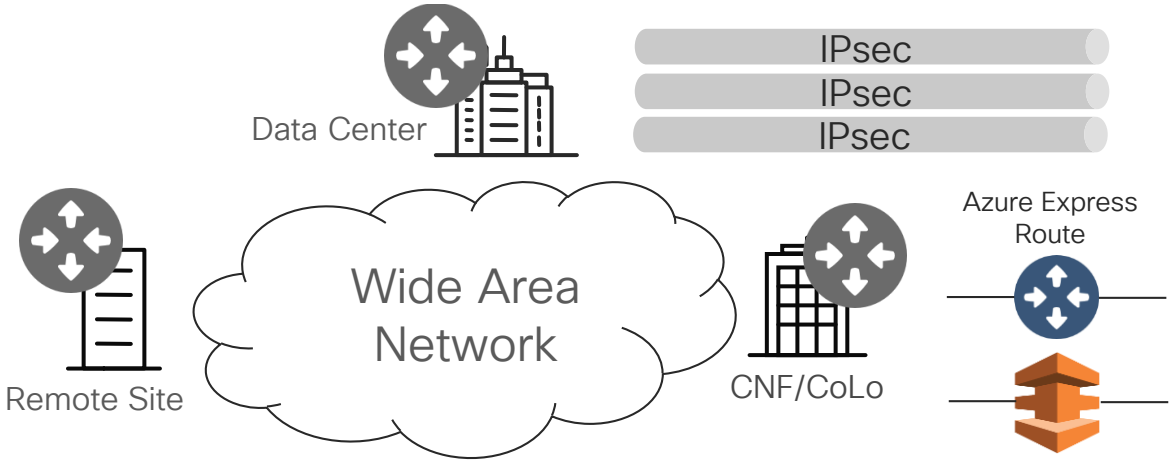


Cloud onRamp for SaaS



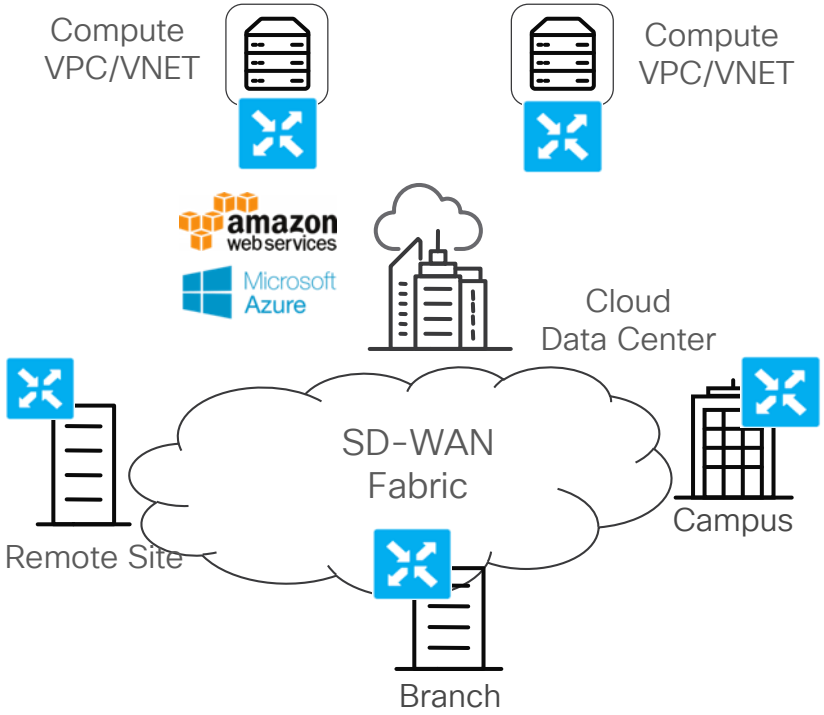
Traditional IaaS Access

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

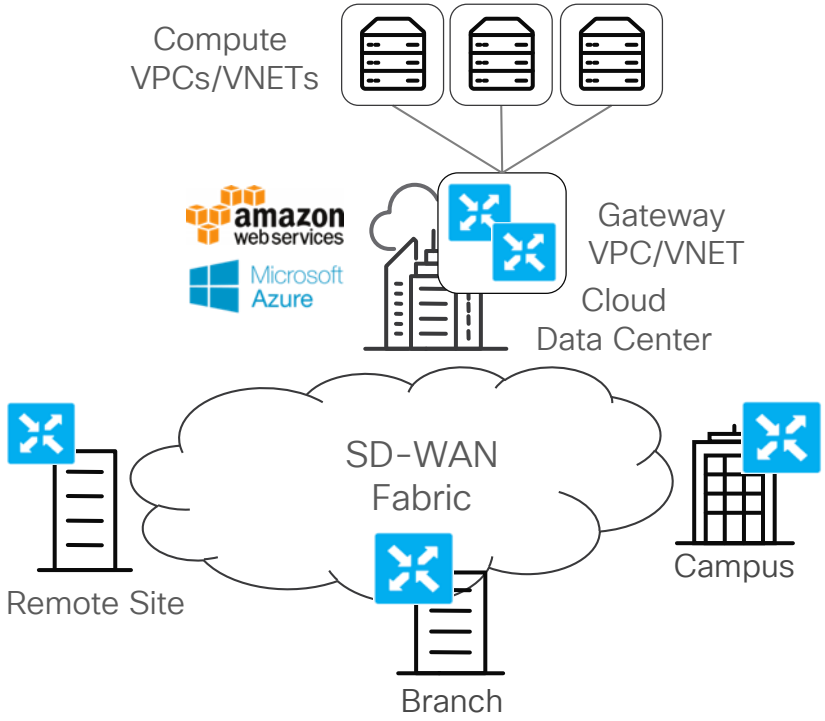


Cloud onRamp for IaaS

Using Marketplace (Do-it-yourself)

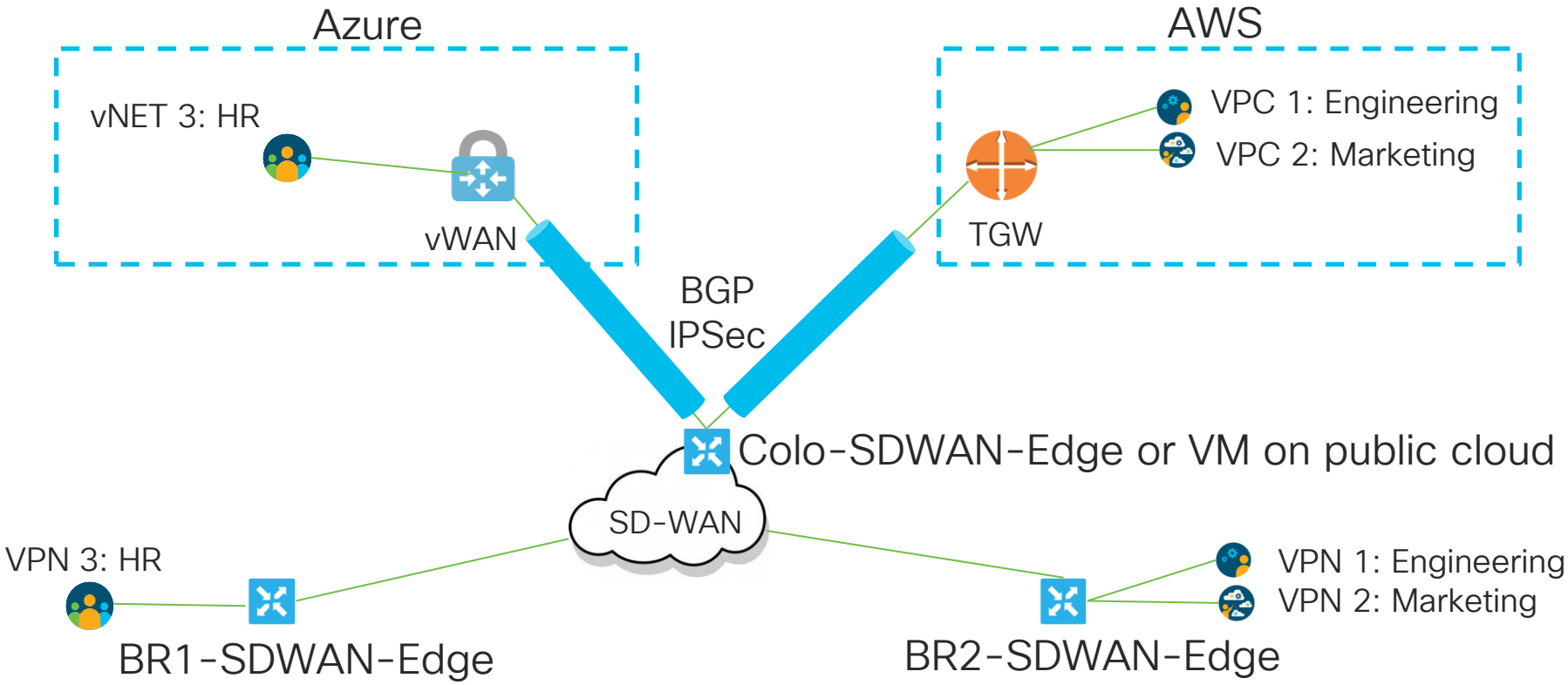


Fully Automated with Cloud onRamp

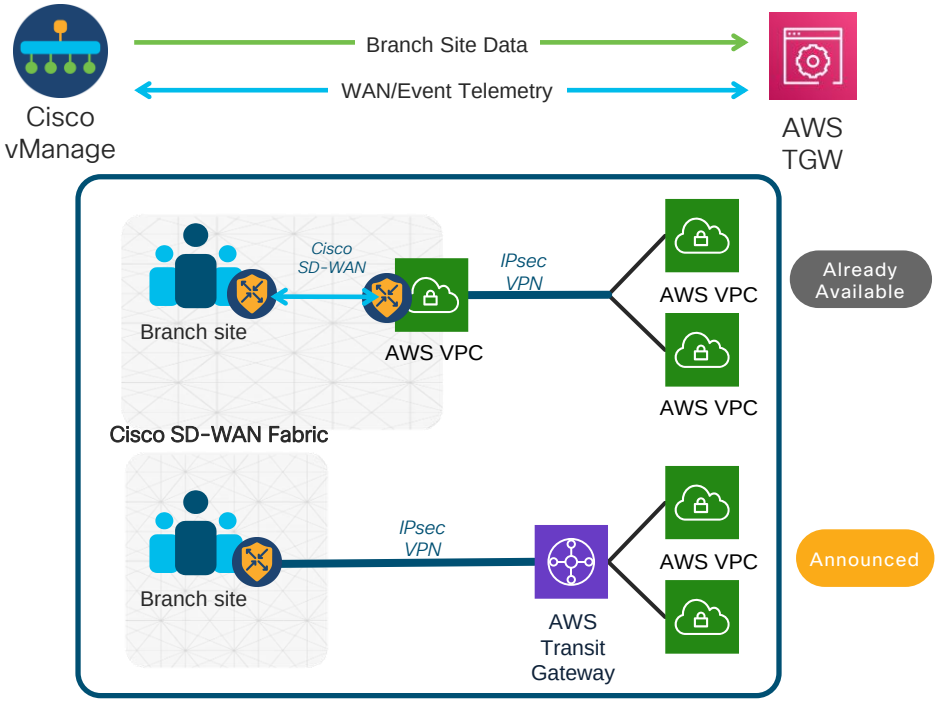


Cloud onRamp for IaaS Demo

Advanced multi-cloud IaaS with SD-WAN



Cisco SD-WAN Integration with AWS TGW



Cloud OnRamp for AWS

- Automated connectivity to AWS Cloud VPC workloads
- Visibility into inter-regional transit data and network telemetry
- Network segmentation across branch and cloud workloads

Clod onRamp for IaaS: TGW Demo

Cloud onRamp for Colocation

For SDWAN

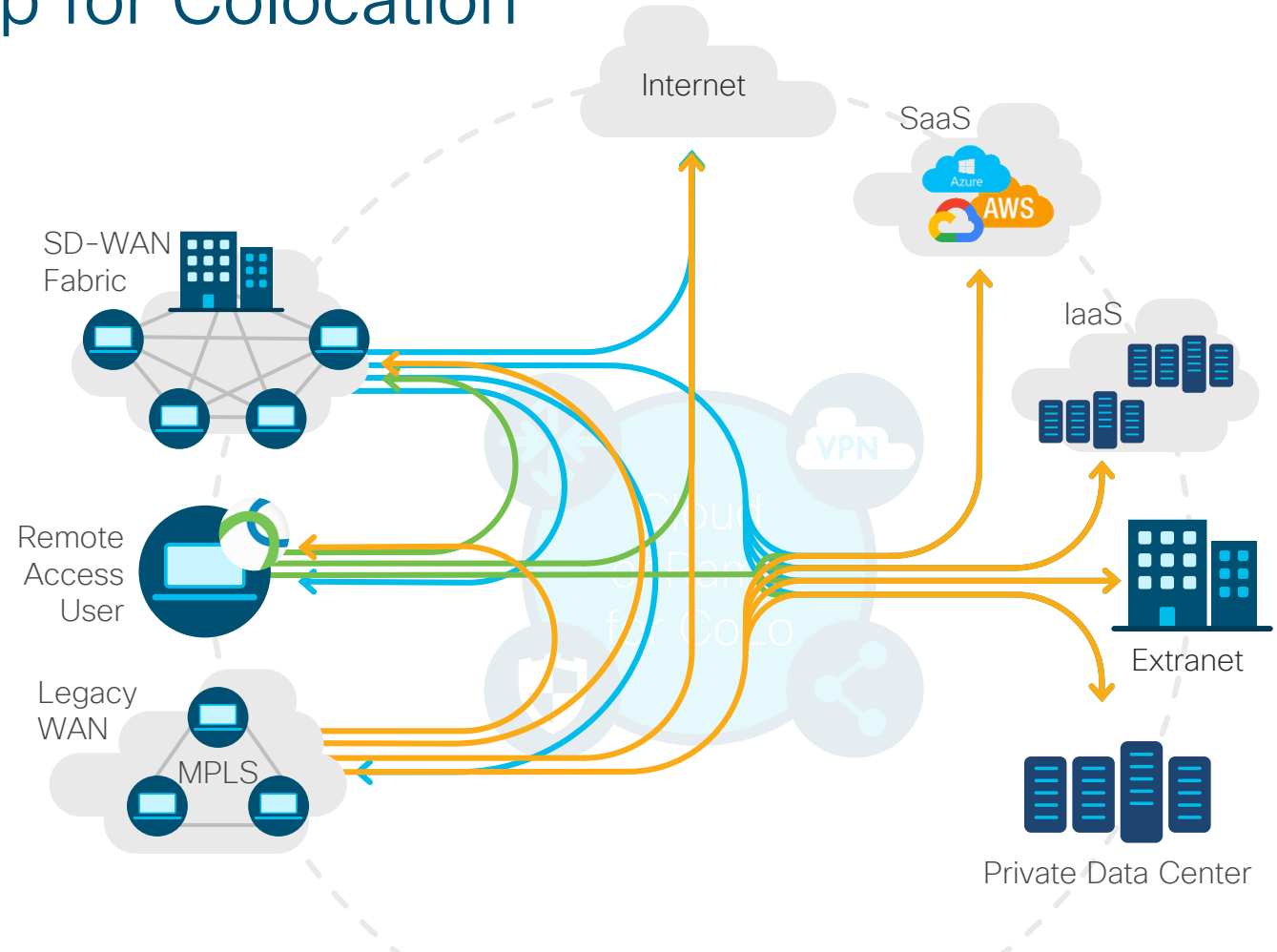
- Easier Migration(s)
- Remote Access VPN integration
- Optimized Cloud/DC Access
- Optimized Extranet Access

For Remote Access Users

- Optimized Cloud Access
- Anchor for IaaS, Extranet and optimized access to Private DC(s)
- Optimized Extranet Access

For Legacy WAN

- Remote Access VPN integration
- Optimized Cloud/DC Access
- Optimized Internet Access
- Optimized Extranet Access



SD-WAN deployment options

Cisco SD-WAN Platform Positioning

Pure Play SD-WAN

Transport Independence,
Cloud Management & Analytics

- ZBFW + Cloud Security
- Voice Optimization
- Cloud onRamp for IaaS and SaaS

Viptela OS: ISR 1100-4G, ISR 1100-6G, vEdge 2000

Integrated Services SD-WAN

Interface Flexibility,
Rich Services

- Adv. Cloud Security*
- Multi-Domain* (DC, Campus)
- Embedded Security
- Integrated Voice*
- Cloud onRamp for Colocation
- ZBFW+ Cloud Security
- Voice Optimization
- Cloud onRamp for IaaS and SaaS

IOS-XE SD-WAN OS: ISR[1], ASR, CSR

VRF and Tunnel Scale, Throughput

*Roadmap for FY21
[1] On select ISR Product family

One user interface across branch, cloud and colocation

SD-WAN Portfolio with New Platforms

Integrated Services IOS XE SD-WAN

Pure Play VIPTELA OS

Branch

ISR 1000

- Integrated wired and wireless access
- LTE Advanced
- VDSL2,ADSL2/2+

ISR1120 / 1160

(New 25 SKUs)

- 4G WWAN pluggable flexibility(CAT4/6/18)
- On-box Security

ISR 4000

ISR 4461
Highest performing ISR to-date

- WAN and voice module flexibility
- On-box Security
- Compute with UCS-E
- Slot Modularity, RPS(optional)
- 10GE option

ISR1100-4G

- 4 GE WAN ports

ISR1100-4GLTE

- 4G LTE (CAT4)

ISR1100-6G

- 6 WAN ports (4GE and 2 SFP)

Aggregation

ASR 1000 Fixed

- High-performance services with hardware assist

vEdge 2000

- RPS, PIM options

vEdge 5000

- Modularity, RPS

Virtualized

Cisco ENCS & CSP

- Service chaining virtual functions
- Options for WAN connectivity
- Open for 3rd party services & apps
- NFVIS Hypervisor

CSR 1000V vEdge Cloud

- Extend enterprise routing, security & management to cloud
- Cisco DNA virtualization

SD-WAN Help-Desk

- Ensure successful adoption of SD-WAN with TME/TSA assistance delivered through a help-desk for customers and partners
  - *High Level Design Review Consultation*
  - *Deployment consultation*
- Requests submitted through email
- Technical resources enabled on latest releases and implementation best practices

Email sdwanhelpdesk@cisco.com for design requests

Conclusion

Call To Action

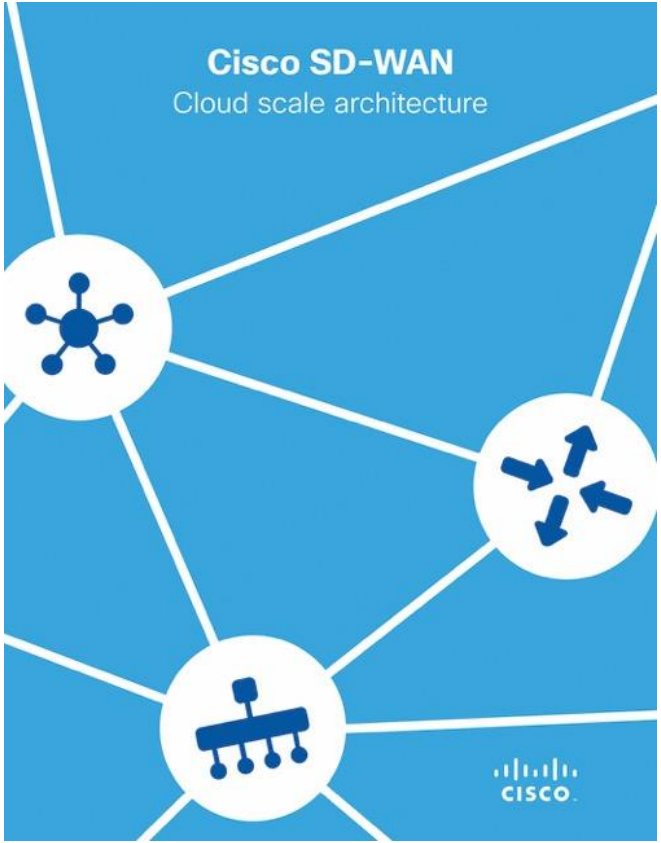
Learn more:

- eBook ”Cisco SD-WAN. Cloud scale architecture” (see next slide) cs.co/sdwanbook

Practice:

- Complete dCloud SD-WAN Lab “Cisco 4D SD-WAN (Viptela)”

eBook "Cisco SD-WAN. Cloud scale architecture"



Preface 7
Authors 8
Acknowledgements 9
Intended audience 10
Book structure 11

Introduction 13
Why SD-WAN? 14

What is Cisco SD-WAN? 17
Benefits 18
Components and architecture 20
Platforms 29
Cloud 31
Security 32
Application experience 33
Management and operations 34

Improving application experience 35
Business need 36
Application visibility 38
Quality of service 39
Circuit quality 43
Meeting SLAs 46
Cloud application performance 49
Case study 51
Key takeaways 52

Secure direct internet access 53
Business need 54
Direct Internet Access 55
Security policies 57
Security monitoring 63
Case study 65
Key takeaways 67

SaaS optimization 69
Business need 70
Cloud onRamp for SaaS 72
Design considerations 76
Case study 80
Key takeaways 81

Extend SD-WAN to public clouds 83
Business need 84
Cloud onRamp for IaaS 85
Case study 90
Key takeaways 91

Leveraging colocations 93
Business need 94
Cloud onRamp for Colocation 95
Case study 101
Key takeaways 102

Building a virtualized branch 105
Business need 106
Network Functions Virtualization 107
Service chaining 112
Case study 113
Key takeaways 115

...

Key Message of Our Presentation

Cisco SD-WAN Solution helps you to:

1. Reduce Cost

2. Operate Faster with better Performance and Security

3. Integrate Latest Cloud and Network Technologies

Proven Solution Across Multiple Verticals

For Your Reference

Customer	Industry	Challenge	Solution
GAP	Retail	High cost, slow change, limited flexibility	60-70% cheaper broadband at high bandwidth, centralized control, full visibility.
	Financial	Needed more bandwidth and guaranteed network uptime for a new teller application	Dollar cost averaged the bandwidth cost down using a mix of transport (MPLS, Broadband, LTE). Traffic now uses the optimal network path to avoid downtime and slowdowns.
Agilent Technologies	Tech	Slow performance and MPLS outages provided an expensive and poor user experience	Monthly savings reduced the cost per Mbps by more than 80%. Diverse circuits improve the reliability of the global network, with more than half of Agilent's sites doubling WAN redundancy.
Cigna	Healthcare	With an MPLS contract renewal approaching, Cigna wanted the flexibility to change carriers without a massive technology shift	Gained back control of its control plane and created the Cigna Service Provider Agnostic Network.
Kindred Healthcare	Healthcare	Security and high network cost	Satisfied strict security and audit requirements and provided greater flexibility for partnerships and secure clinical solutions. Cost reductions with the removal of remote site voice equipment and expensive PRIs, aging WAN acceleration equipment and maintenance.
SEVENTY SEVEN ENERGY	Energy	Scale to support evolving field operations, and support cloud migration and application SLAs	Provided 30-60% savings in overall bandwidth costs. Enabled faster response to acquisitions, divestitures and policy changes.

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!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

cisco Live!

You make **possible**