The bridge to possible

Cisco SD-WAN: Start here

Lars Granberg, Technical Solutions Architect, @larslilja

Prashant Tripathi, Principal/Chief Architect Cisco SD-WAN & Multi-Cloud
@prashant_tri

Cisco Webex App

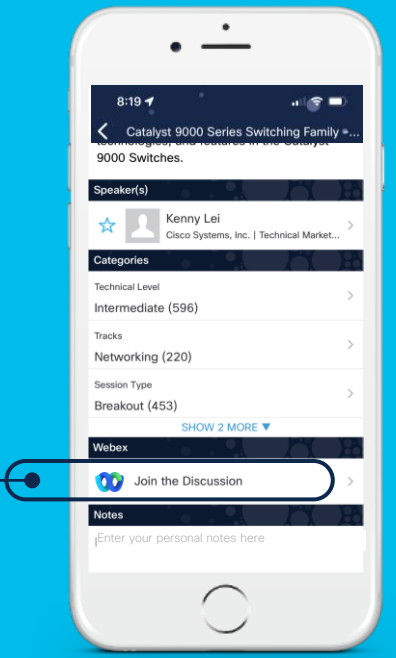
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



Agenda

- SD-WAN Recap
  - Where are we coming from
- Solution Architecture
  - What is it, how does it all come together?
- Software Features
  - Let’s scratch the surface
- Learn More
  - Where to go and when

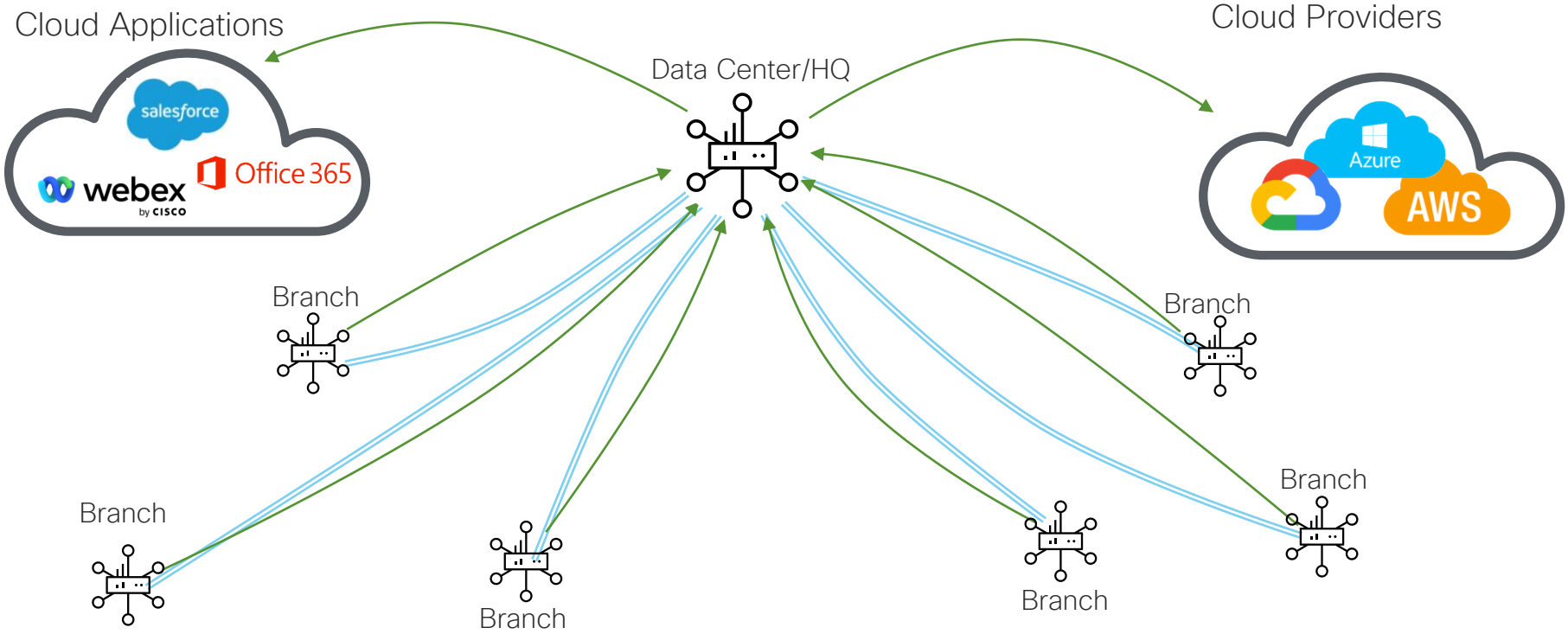
SD-WAN – This is it.

SD-WAN Recap

cisco Live!

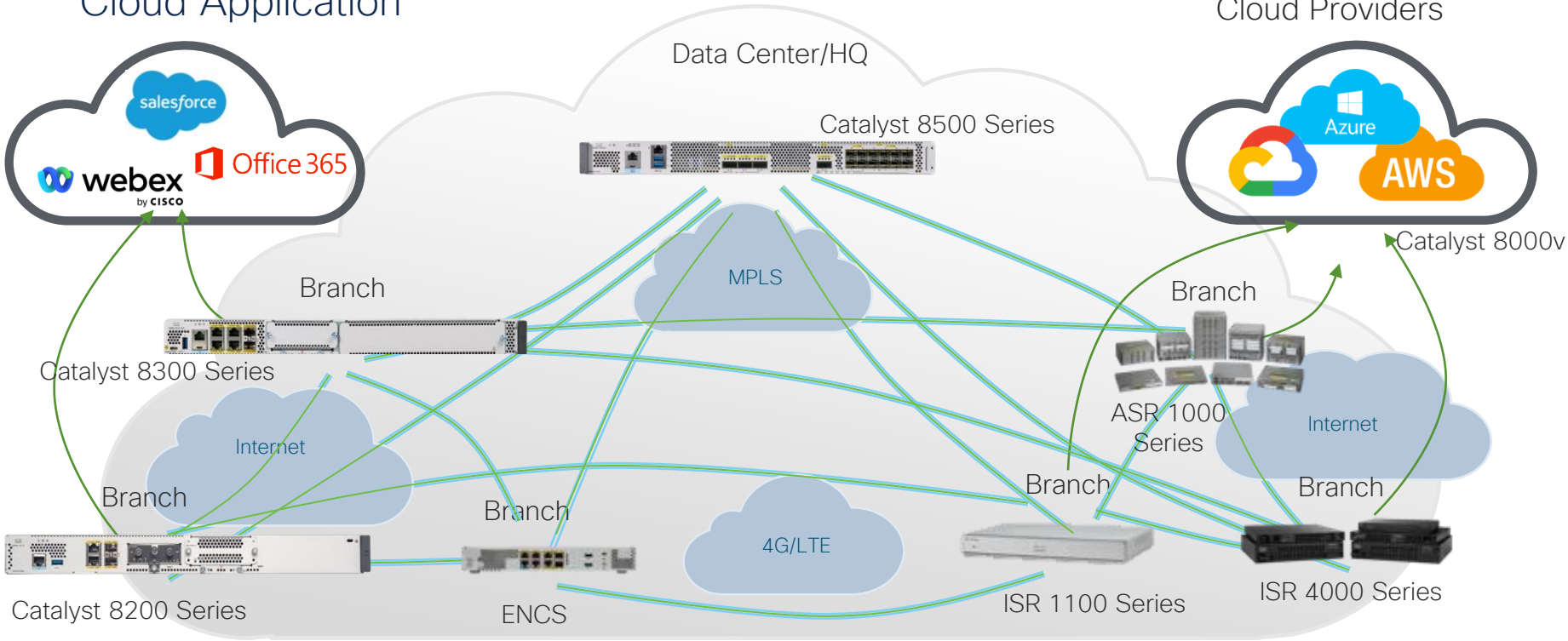
The Hardware Based WAN of Yesterday

Doesn't Keep up with the Needs of Today



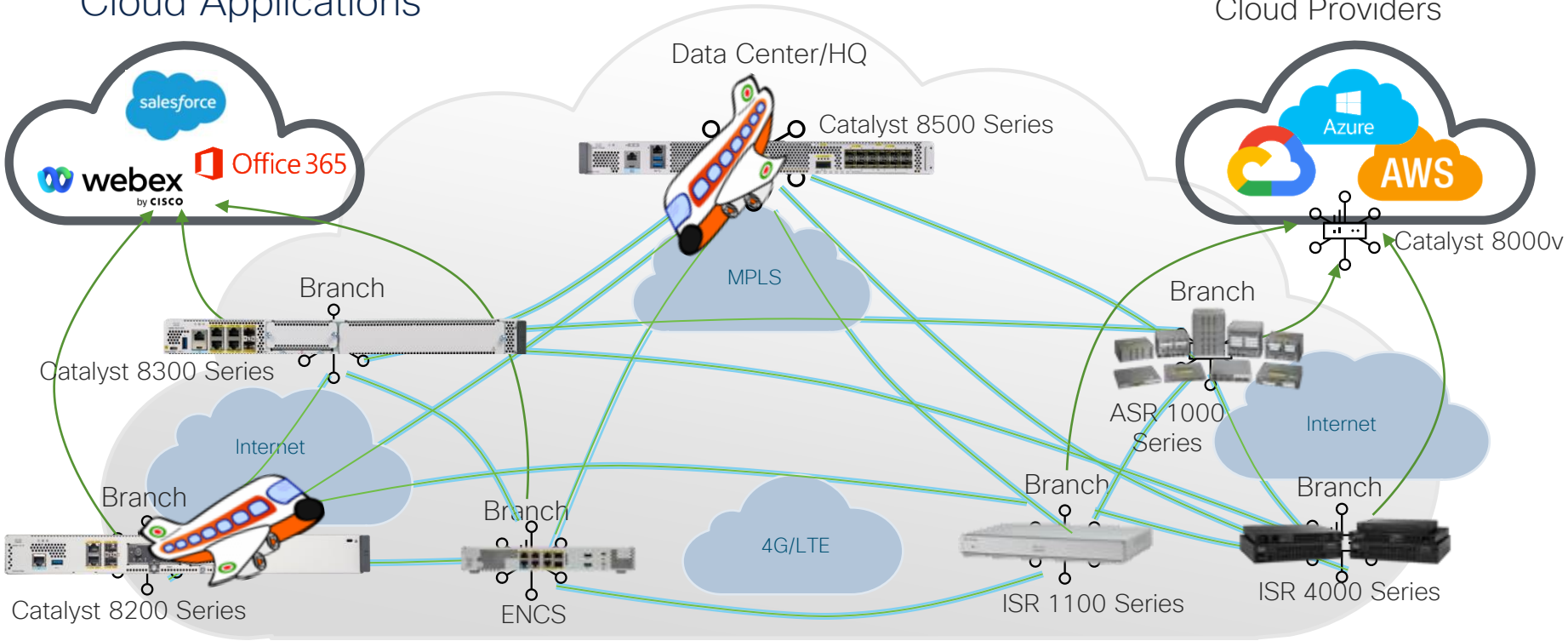
Cisco SD-WAN: Software Approach

Cloud Application



Cisco SD-WAN: Software Approach

Cloud Applications



Cisco SD-WAN: Software Approach

Cloud Applications

SD-WAN Recap

SD-WAN RECAP

Any Deployment

Management & Analytics

On-premise | Cloud | Multi-tenant
Automation | Network Insights | Machine Learning | AI
Open | Programmable | Scalable

Any Service

Multicloud Optimization

Multi-Layer Security

Analytics

Voice

Multi-Domain IBN Policy

Any Transport

Satellite

Internet

MPLS

5G/ LTE

SDCI*

Any Location

Branch

Colocation

Cloud

Remote Work

* Software Defined Cloud Interconnect

SD-WAN RECAP

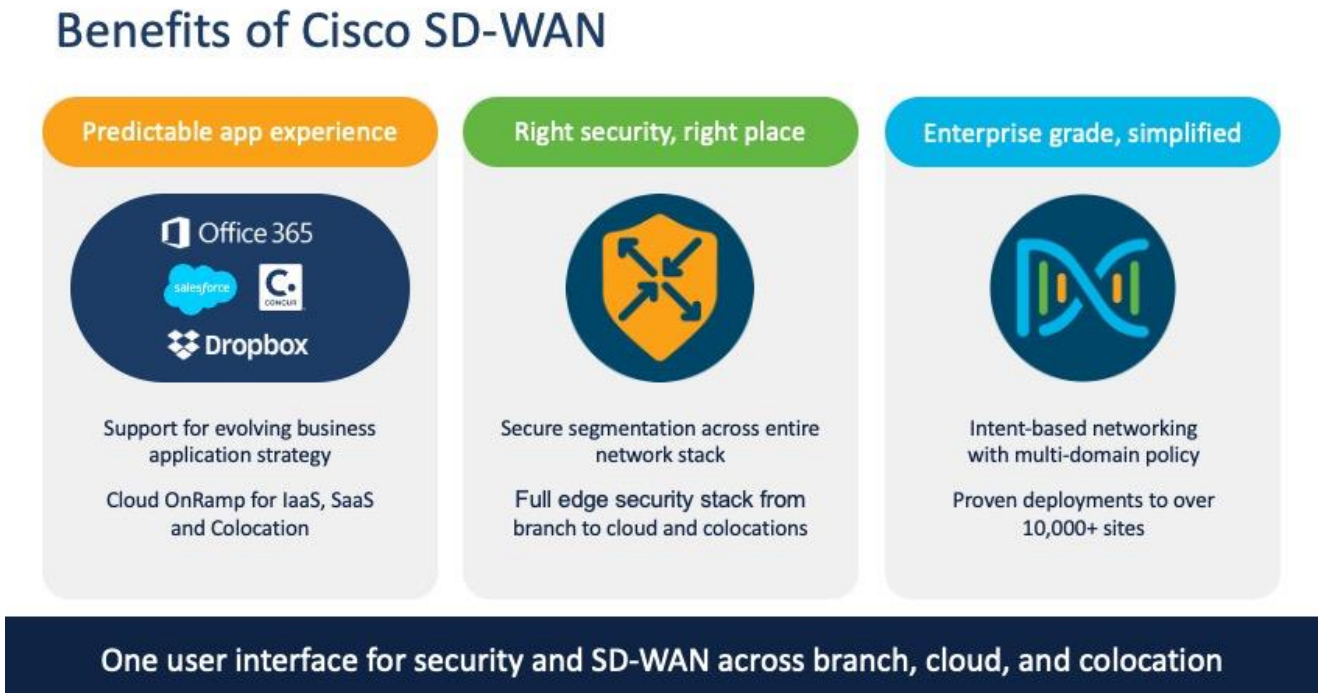
Lets Rewind 5 years 2018

SD-WAN Benefits

- $ Savings on WAN provision and TCO
- Expedited Provisioning
- Operations efficiency (centralized mgmt.)
- Inherent Hardening (Encryption)
- Improved Visibility
- Segregation
- Flexible physical and logical topologies
- Application Aware Routing (ARR)

..and back to today 2023

SD-WAN RECAP



“Application Analytics

Application visibility and analytics are becoming more important to get better feedback as to the applications running on the network and informing network decisions…….

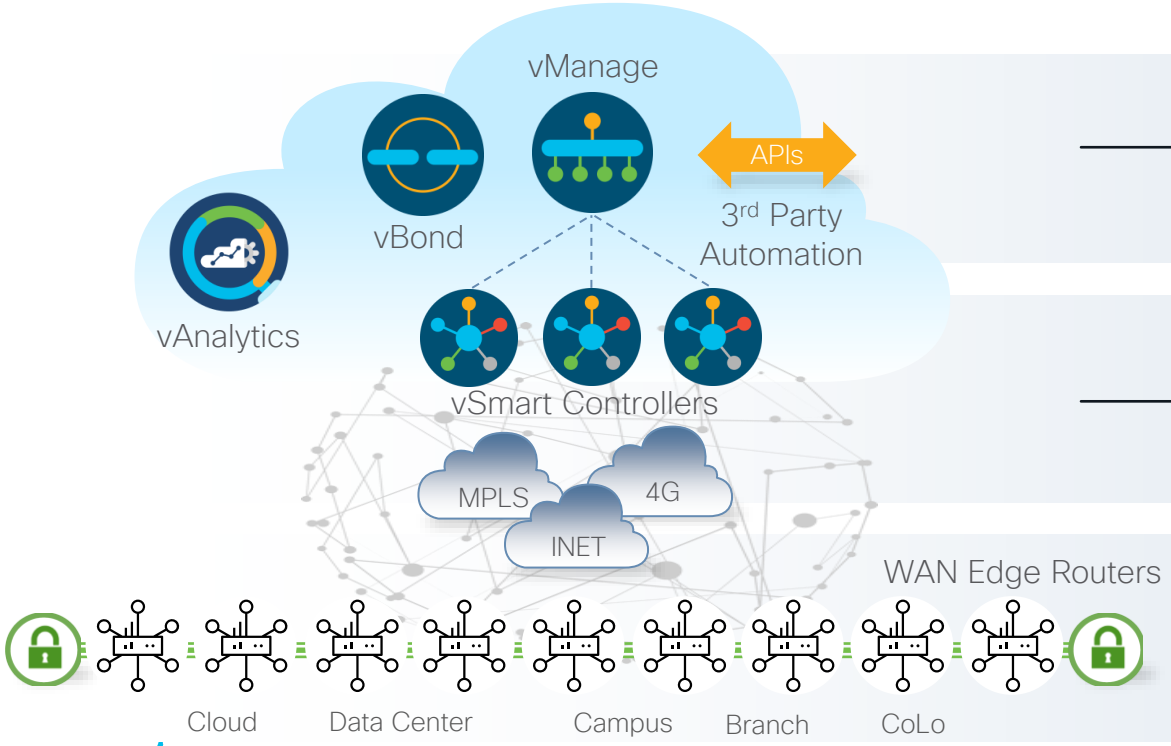
……specific application performance/quality of experience (QoE) is being delivered for end users. Increasingly, we see demand for end-user experience metrics from the end user to the actual application, which may be hosted in a CSP.

”

From Garrtner© Magic Quadrant for WAN Edge Infrastructure 2021

Solution Architecture

Cisco SD-WAN Solution Overview

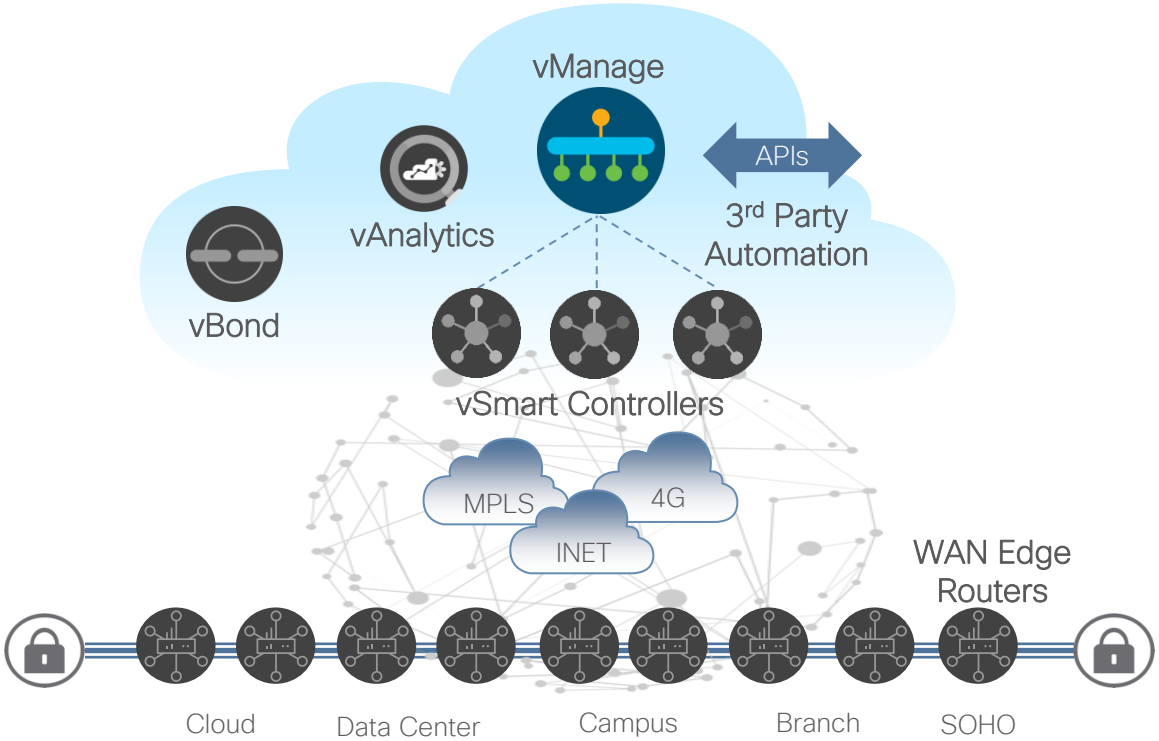


Management/
Orchestration Plane

Control Plane

Data Plane

Cisco SD-WAN Solution Elements

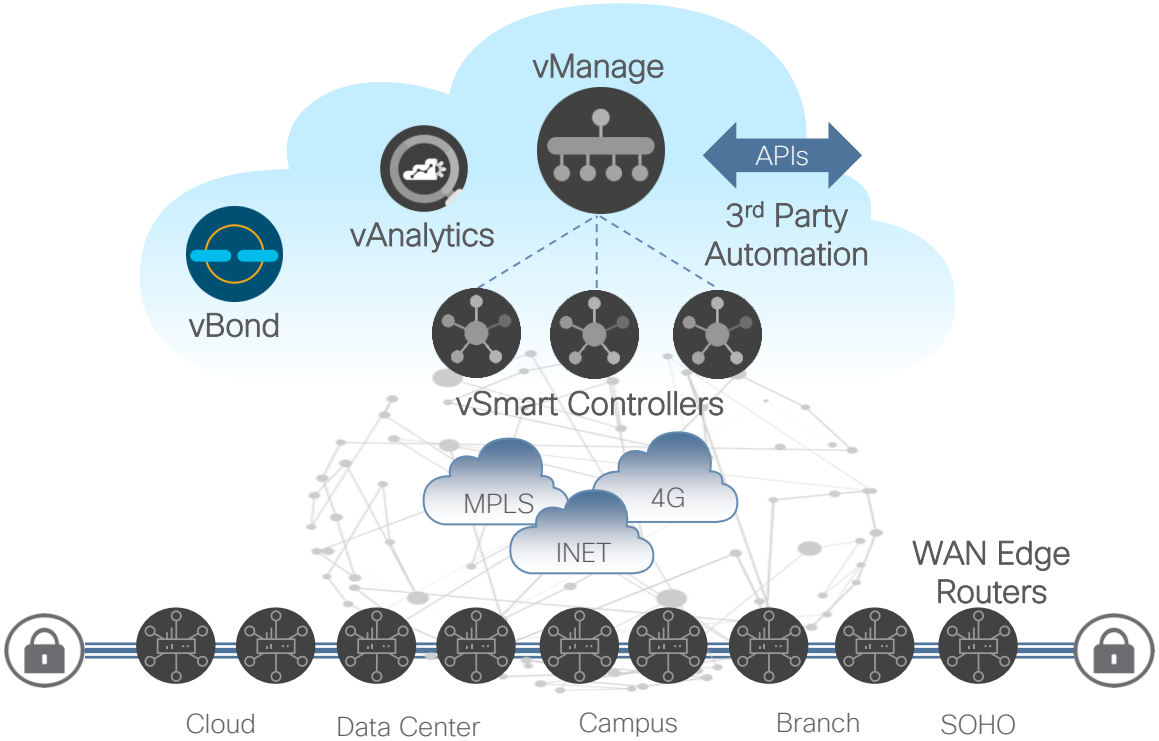


Management Plane

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

Cisco SD-WAN Solution Elements

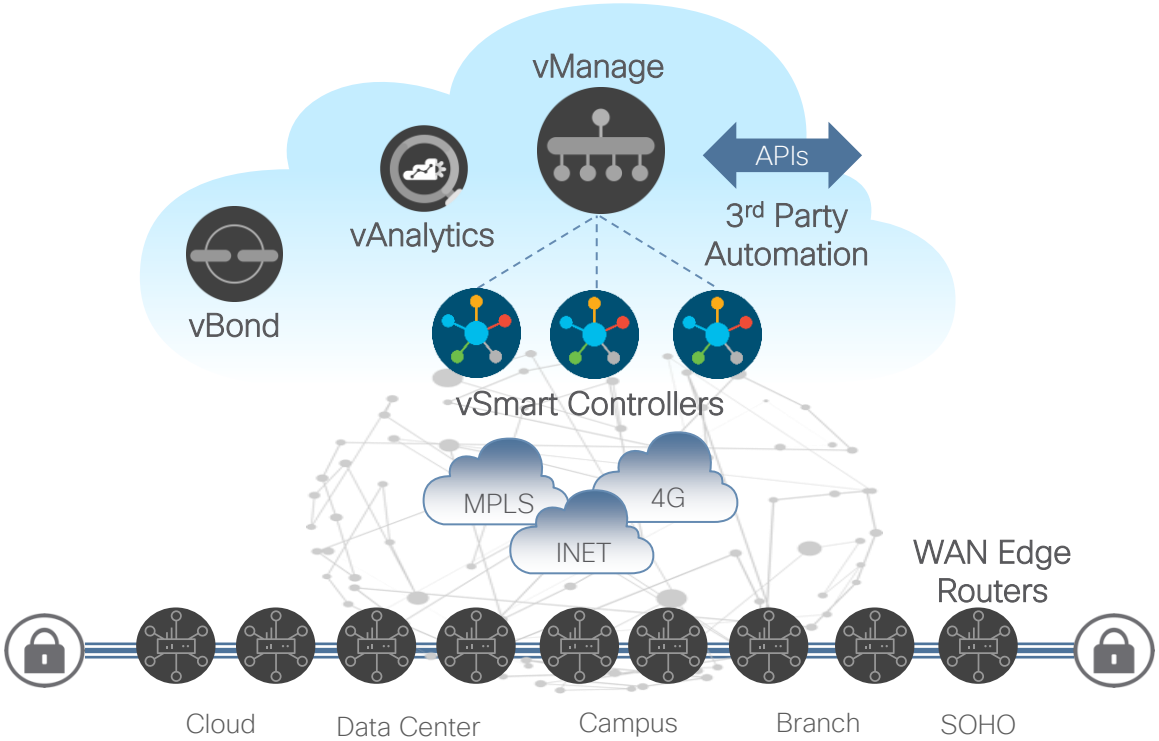


Orchestration Plane

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

Cisco SD-WAN Solution Elements

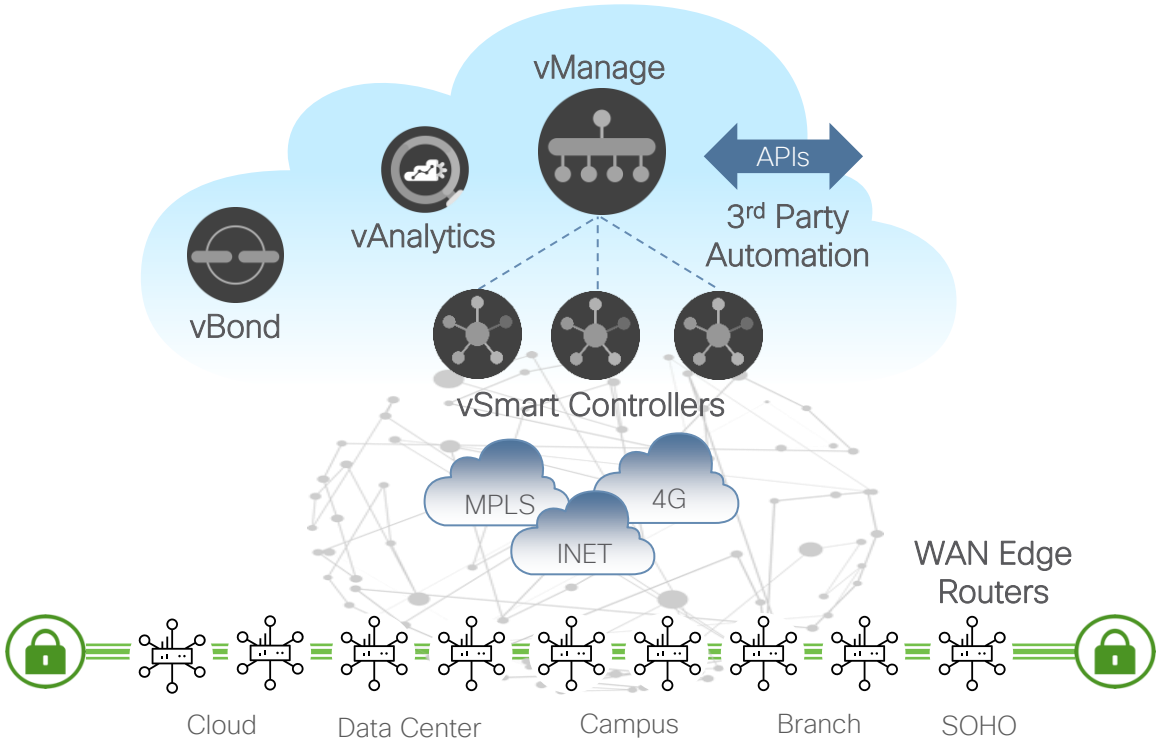


Control Plane

Cisco vSmart

- Facilitates fabric discovery
- Dissimilates control plane information between WAN Edge Routers
- Distributes data plane and app-aware routing policies to the WAN Edge 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

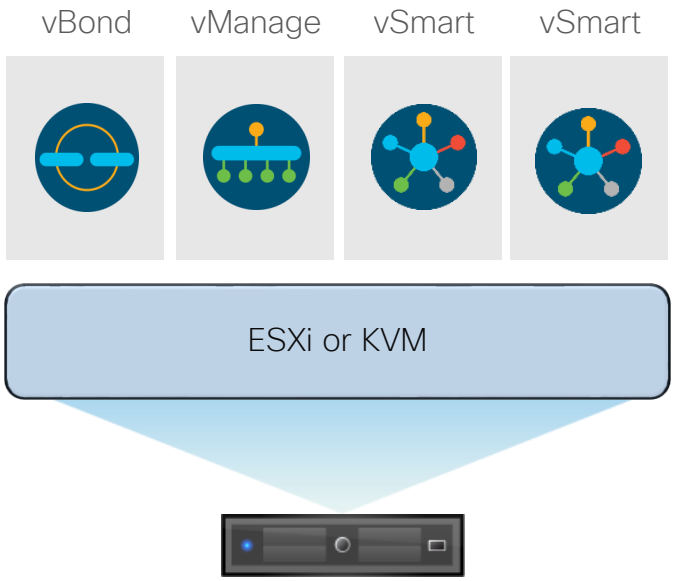
Physical/Virtual

Cisco WAN Edge

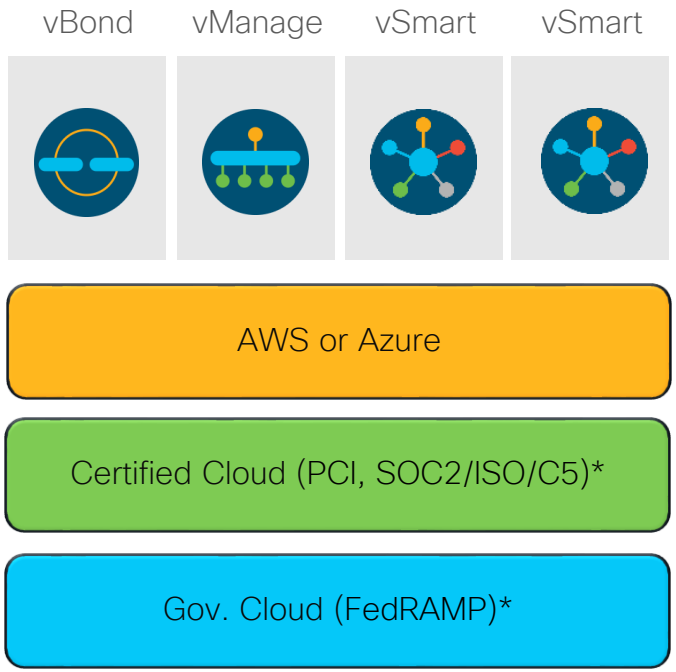
- WAN edge router
- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, and EIGRP
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mb, 1Gb, 10Gb,40Gb, 100Gb)

Controller Deployment Methodology

On-Premise



Cisco or MSP/Customer Hosted



VM

*Only Cisco hosted

vAnalytics: Translate Raw Data into Intelligent Insights

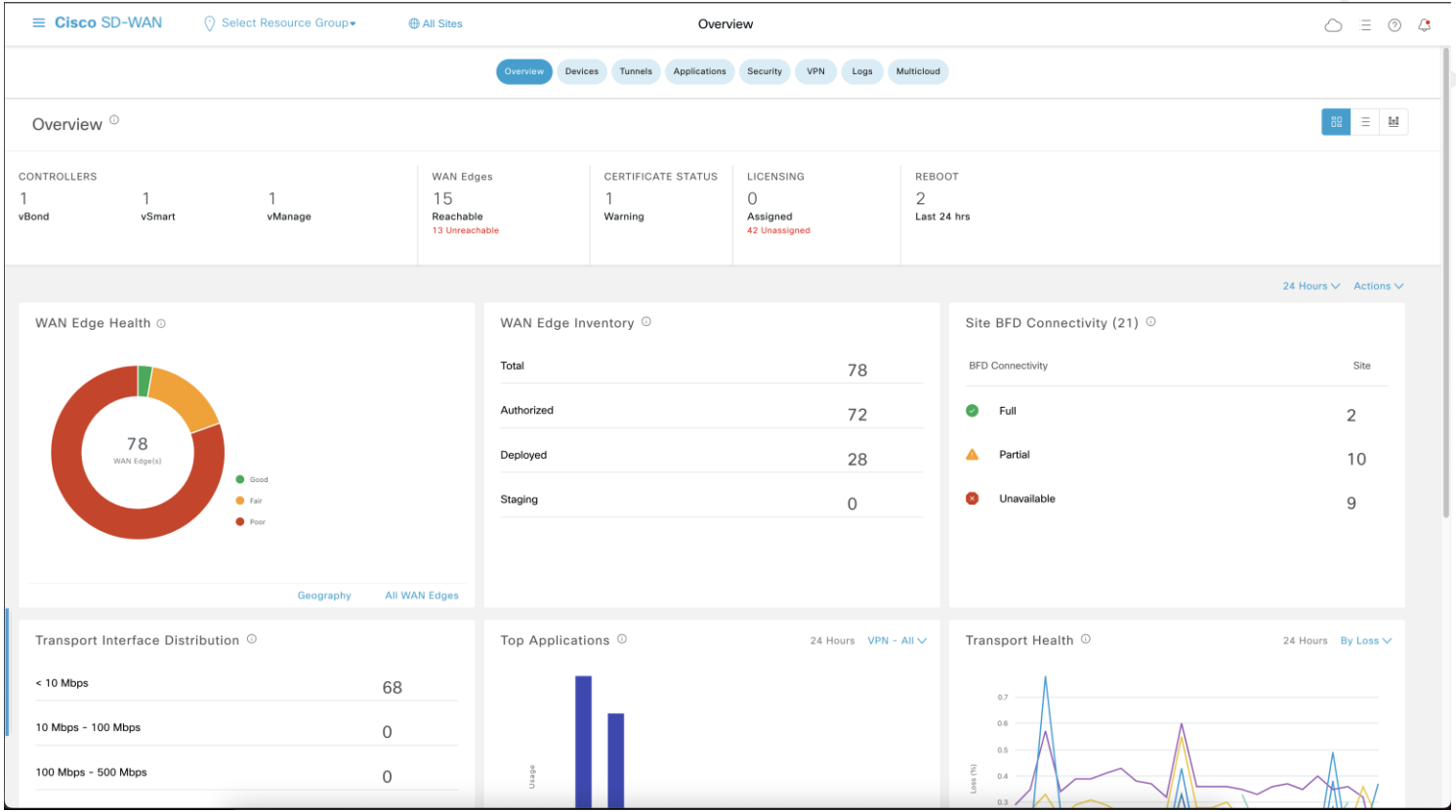
Intuitive Visualization of Network KPIs and historical trends

Correlate Application behavior (QoE) with the network conditions

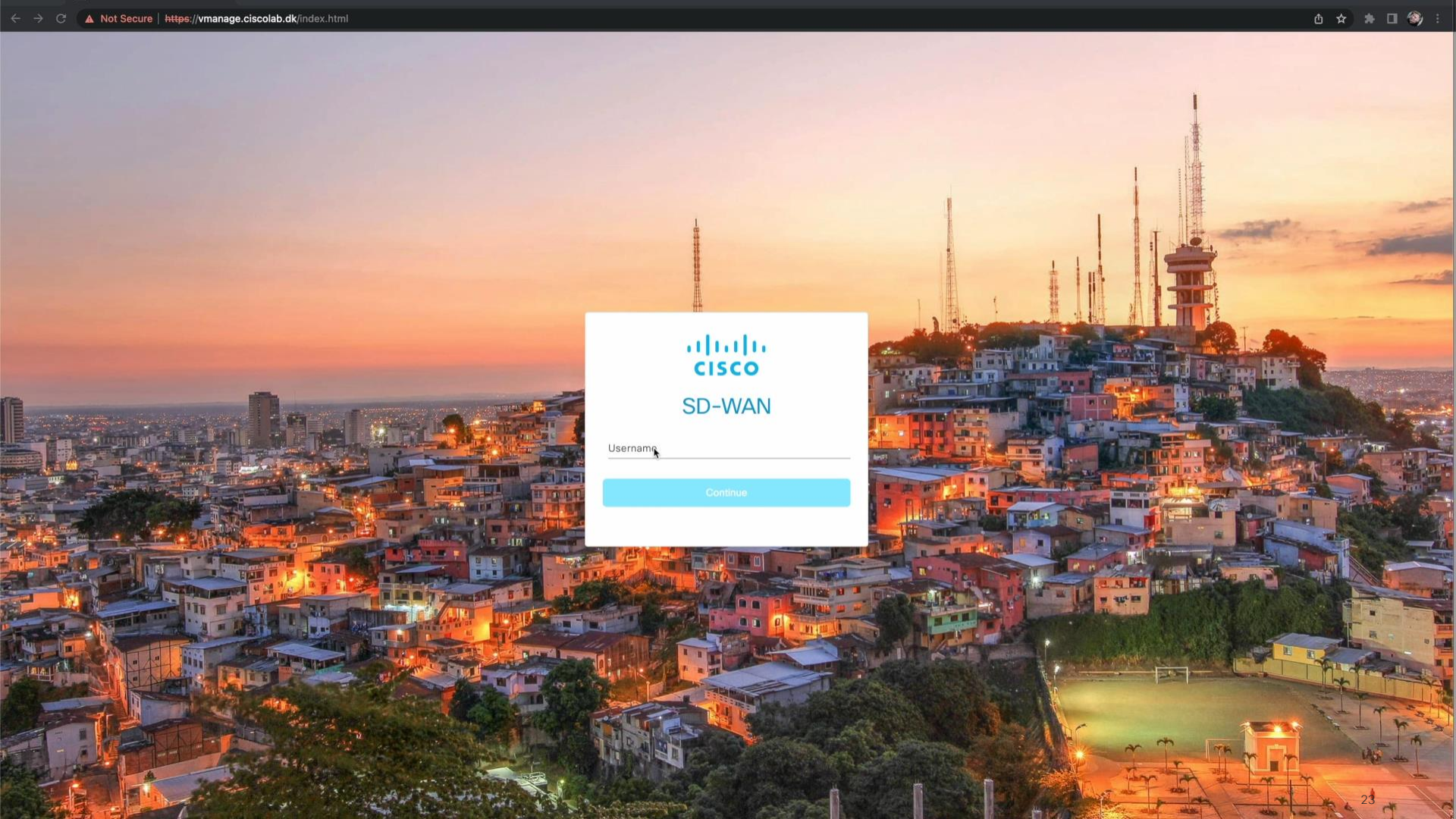
Leverage Insights for better planning

Robust, Scalable, Cloud-hosted SaaS Service

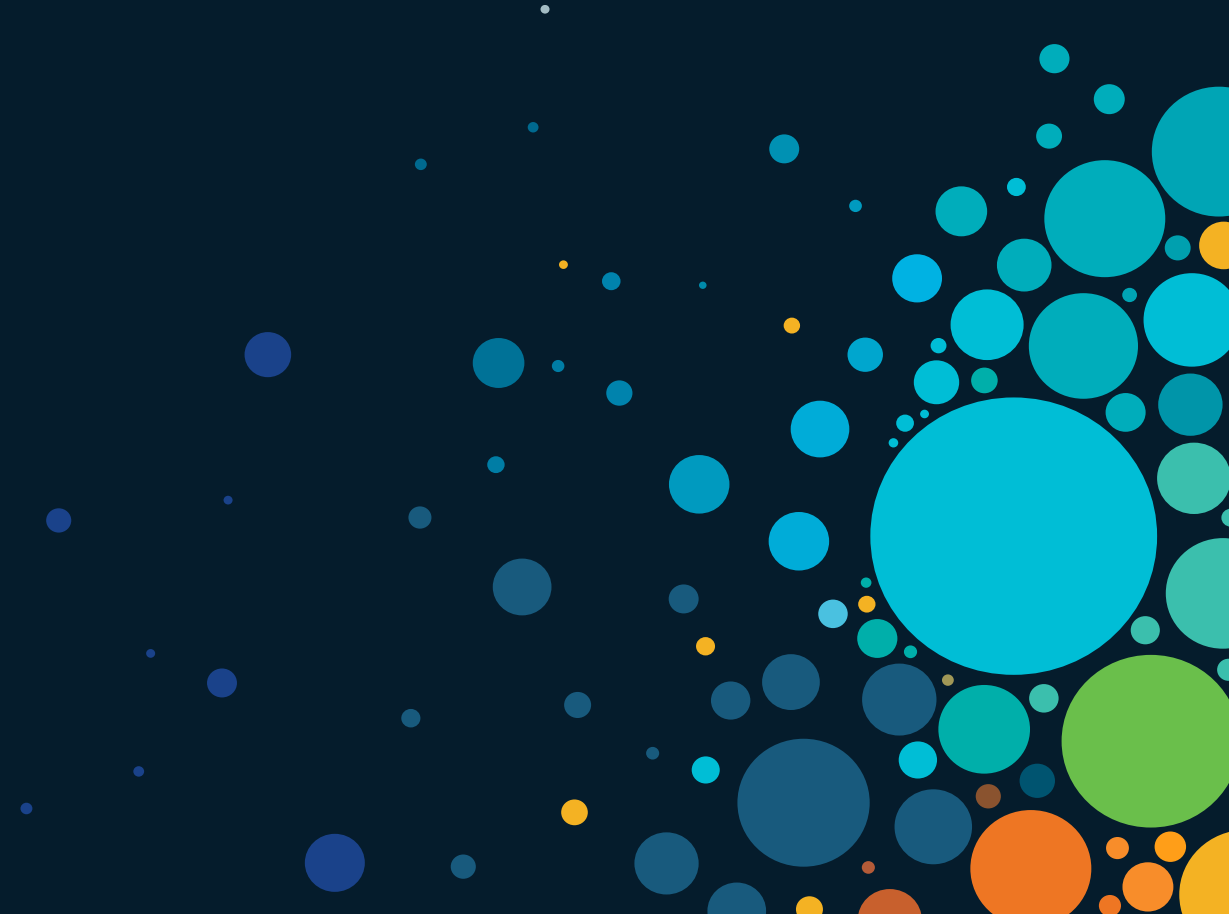
vMange UX



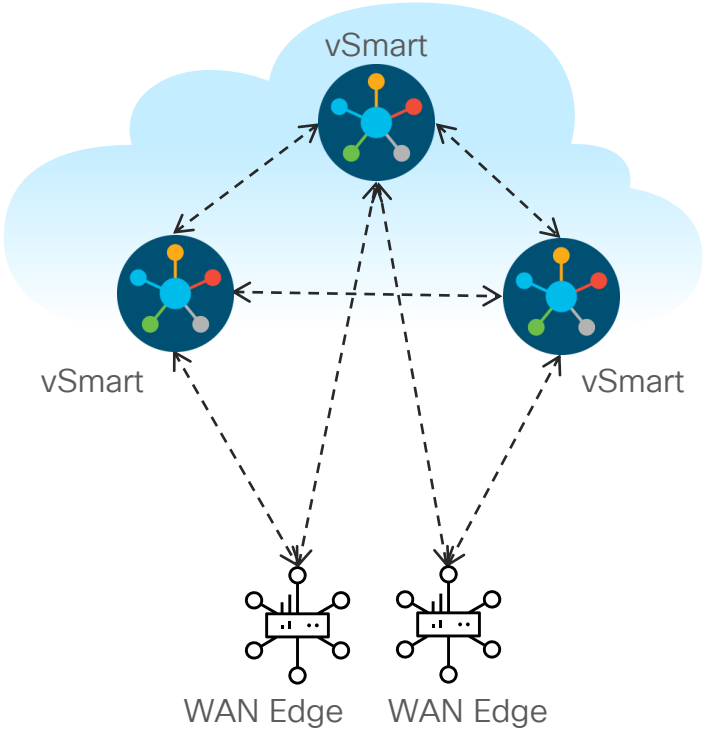
Demo


Not Secure | https://vmanage.ciscolab.dk/index.html
cisco
SD-WAN
Username
Continue

Software Features

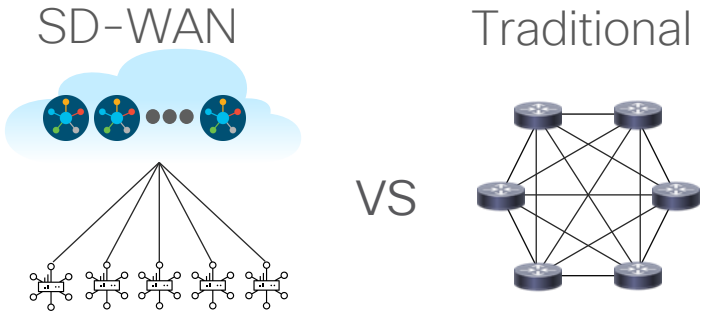


Overlay Management Protocol (OMP)

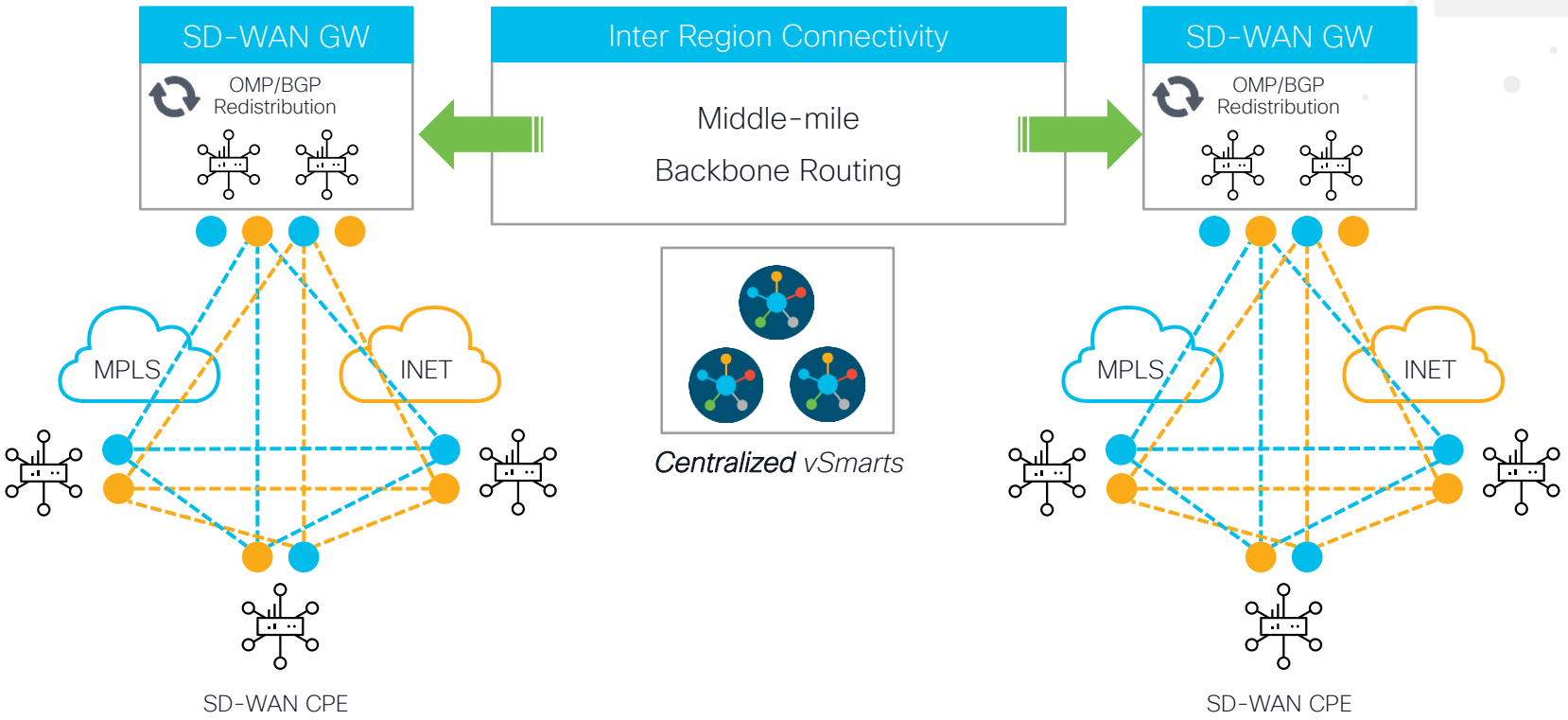


Note: WAN Edge routers need not connect to all vSmart Controllers

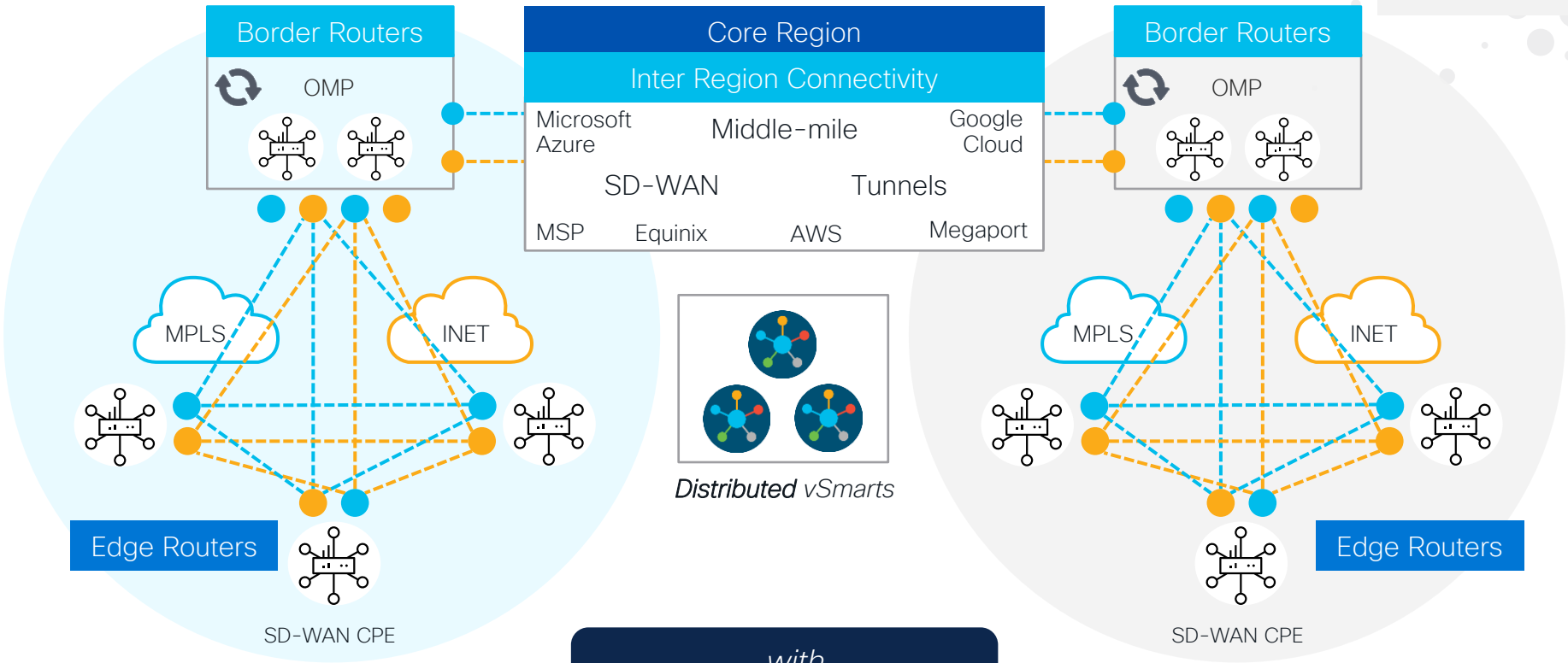
- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane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



The Network, *without* Multi-Region Fabric

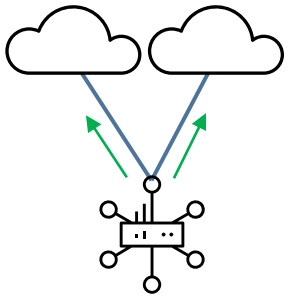


The Network, with Multi-Region Fabric

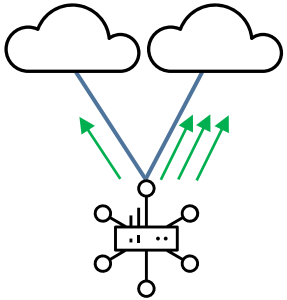


Fabric Communication

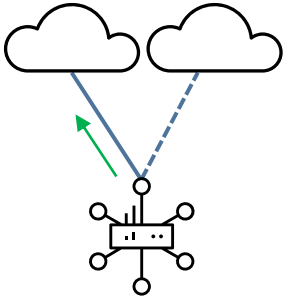
Per-Session Load-sharing
Active/Active



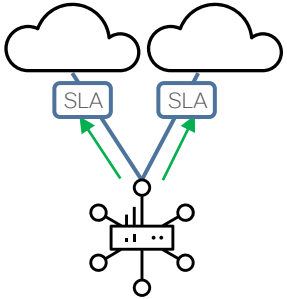
Per-Session Weighted
Active/Active



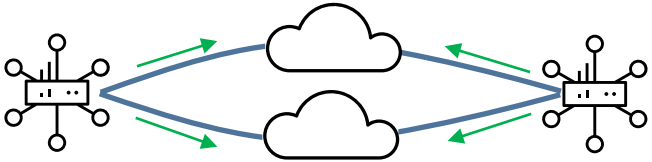
Application Pinning
Active/Standby



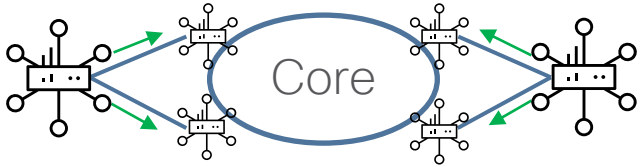
Application Aware Routing
SLA Compliant



Single-hop Fabric

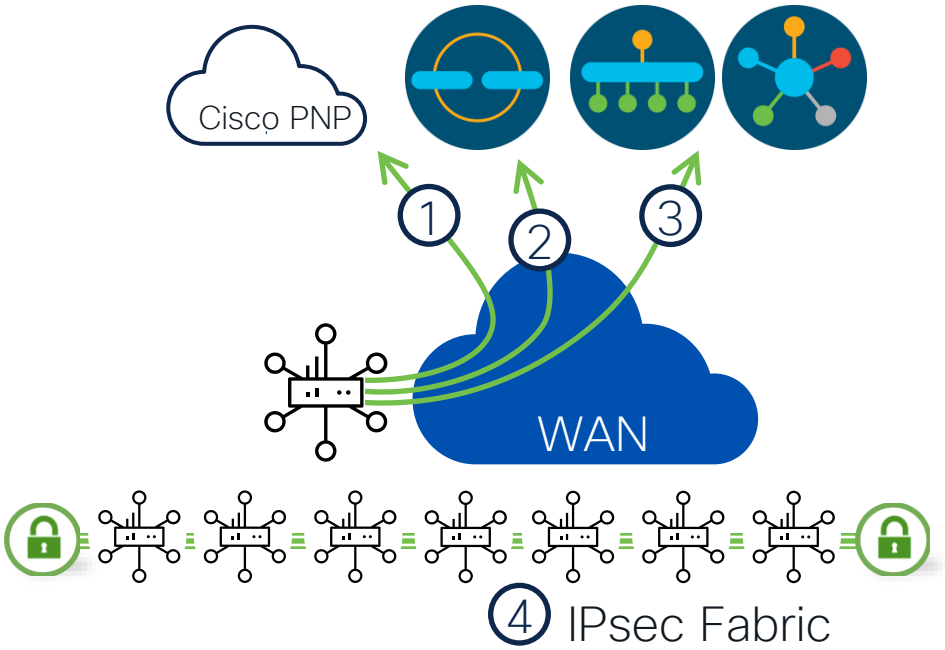


Multi-Region Fabric



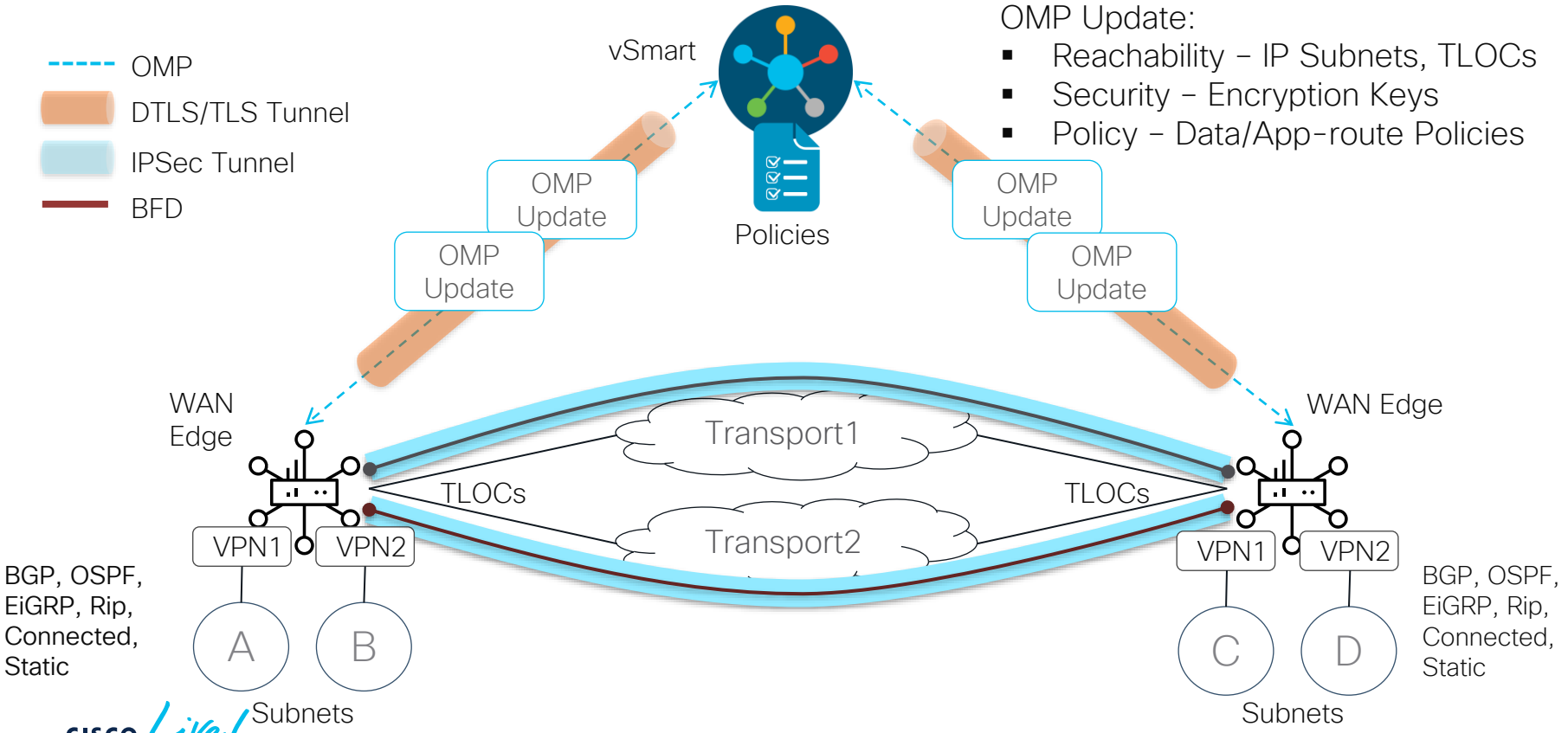
Lets bring it up

Automated, Zero-Touch Onboarding



- SD-WAN appliance will onboard itself into the SD-WAN fabric automatically with no administrative intervention.
- Connect the SD-WAN appliance to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.
- If no DHCP service is available then bootstrap file is an option either on USB or Bootflash

Fabric Operation Walk-Through



Demo

Not Secure | https://vmanage.ciscolab.dk/#/app/monitor2/overview

Cisco SD-WAN

Sites

Overview

Overview | Devices | Tunnels | Applications | Security | VPN | Logs | Multicloud

AN Edges
5
eachable
Unreachable

CERTIFICATE STATUS
1
Warning

LICENSING
0
Assigned
43 Unassigned

REBOOT
2
Last 24 hrs

24 Hours | Actions

24 Hours | Good Performing Sites

8.13

8.13

Usage (GB)

View Details

Tunnel Health

24 Hours | Latency (ms) | Good Tunnels

262
Tunnels

SDALAB-S4-R2:mpls-ICEman:mpls
SDALAB-S4-R2:mpls-GOOSE:mpls
SDALAB-S4-R2:mpls-DSV_ZTP:mpls
SDALAB-S4-R2:mpls-ASR1001_hub2:mpls
SDALAB-S4-R2:mpls-SDA-Prod-Hub_S1:mpls

Circuits

0

Latency (ms)

Good | Fair | Poor

View Details

24 Hours | CPU Load (%) | Good Devices

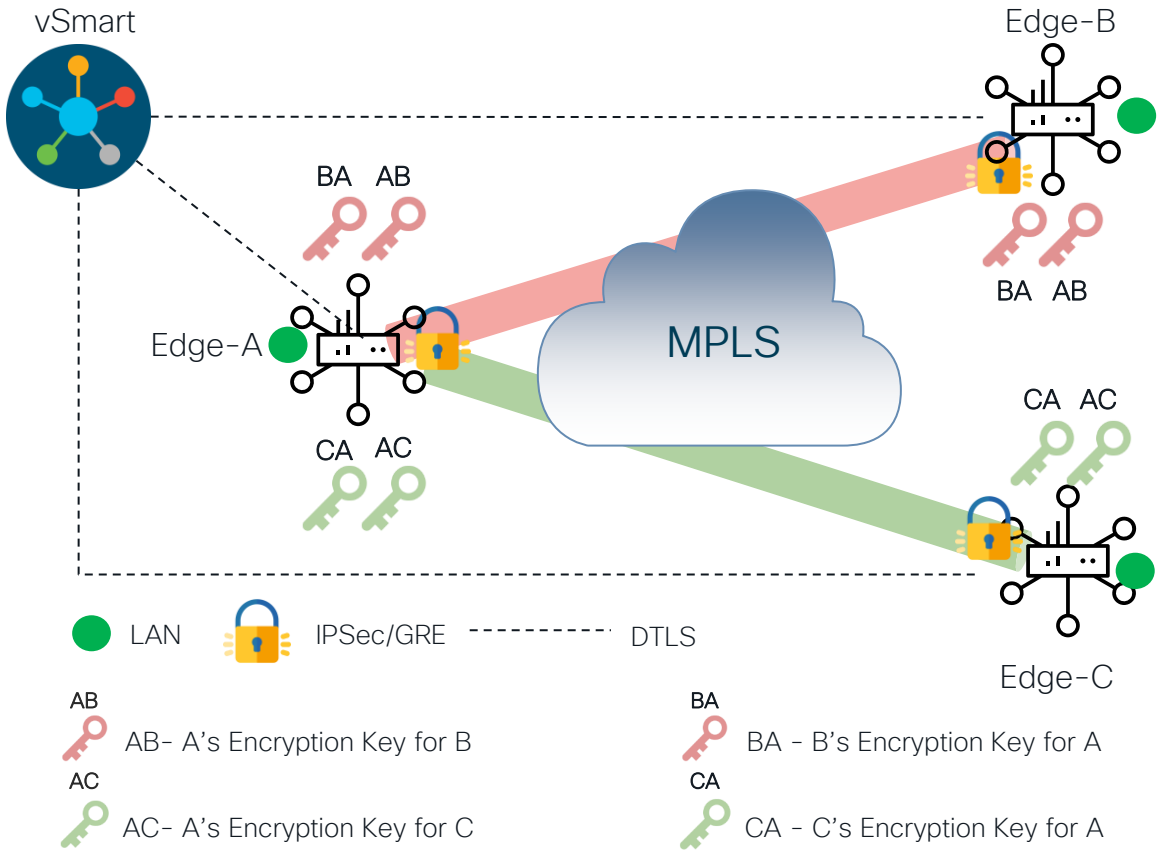
50450255
11.2
8.83
8.46

Transport Health

24 Hours | By Loss

33

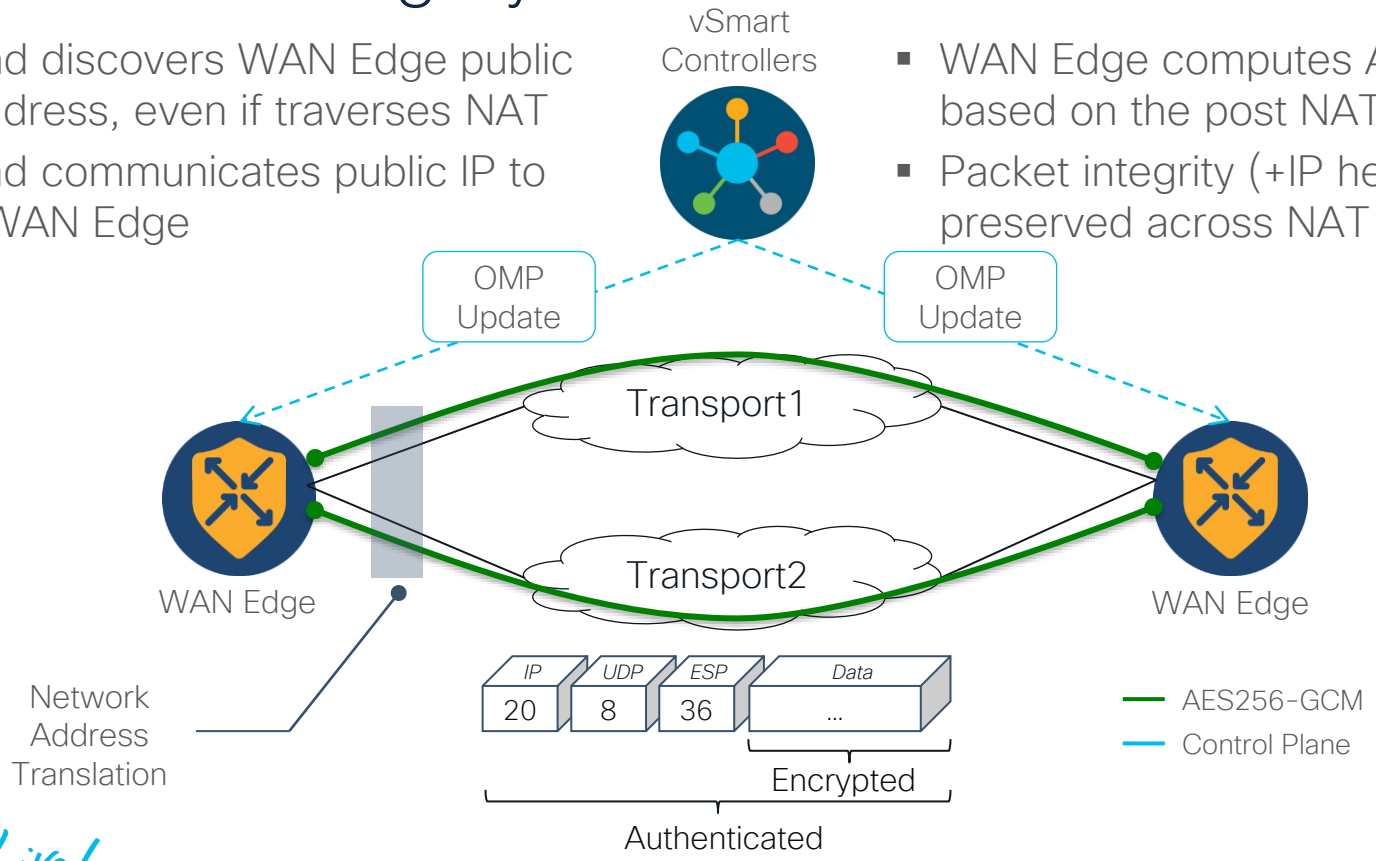
Data Plane Privacy (Pairwise)



- Each WAN edge will create separate session key for each transport and for each peer
- Session keys will be advertised through vSmart using OMP
- When Edge-A needs to send traffic to Edge-B, it will use session key "AB" (B will use key "BA")
- Backward compatible with non PWK devices
- PWK should be enabled

Data Plane Integrity

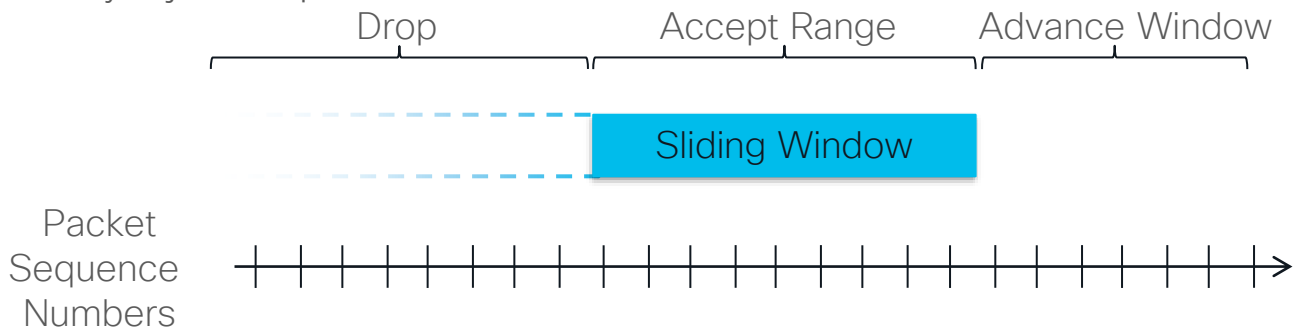
- vBond discovers WAN Edge public IP address, even if traverses NAT
- vBond communicates public IP to the WAN Edge



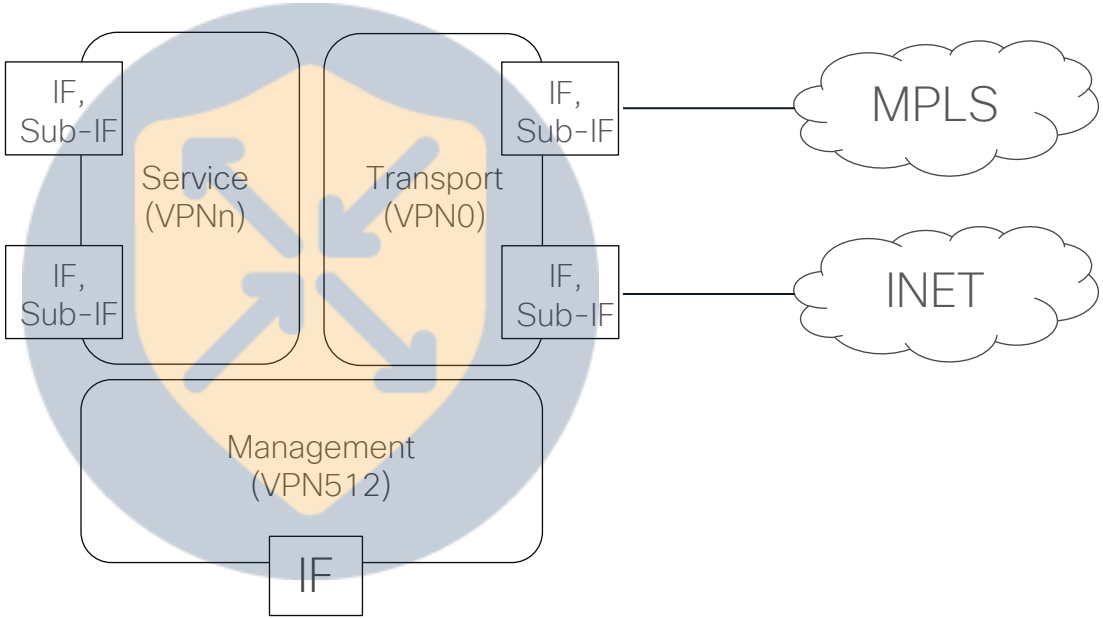
- WAN Edge computes AH value based on the post NAT public IP
- Packet integrity (+IP headers) is preserved across NAT

IPsec Anti-Replay Protection

- Encrypted packets are assigned sequence numbers. WAN Edge routers drop packets with duplicate sequence numbers
  - Replayed packet
- WAN Edge routers drop packets with sequence numbers lower than the minimal number of the sliding window
  - Maliciously injected packet
- Upon receipt of a packet with higher sequence number than received thus far, WAN Edge router will advance the sliding window
- Sliding window is CoS aware to prevent low priority traffic from “slowing down” high priority traffic



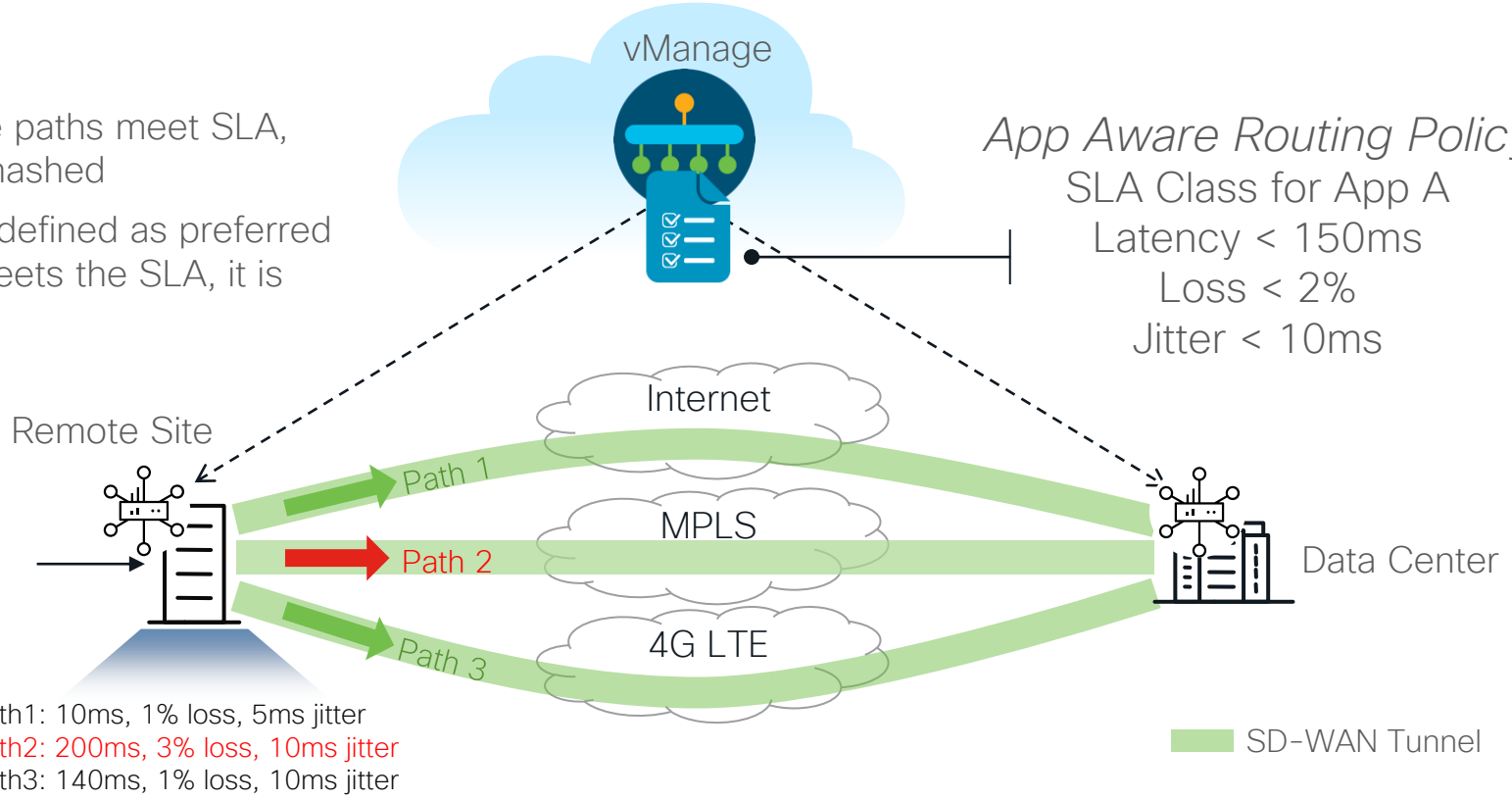
Cisco SD-WAN VPNs (VRFs)



- VPNs are isolated from each other, with each VPN has its own forwarding table
- Reachability within VPN is advertised by OMP
- VPN0 is reserved for WAN uplinks (Transport)
- VPN512 is reserved for Management interfaces
- VPNn represents user-defined LAN segments (Service)

Application Aware Routing

- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



Underlay Measurement and Tracing Service (UMTS)

New!

Benefits

Gain visibility into the exact underlay path* against SD-WAN tunnel

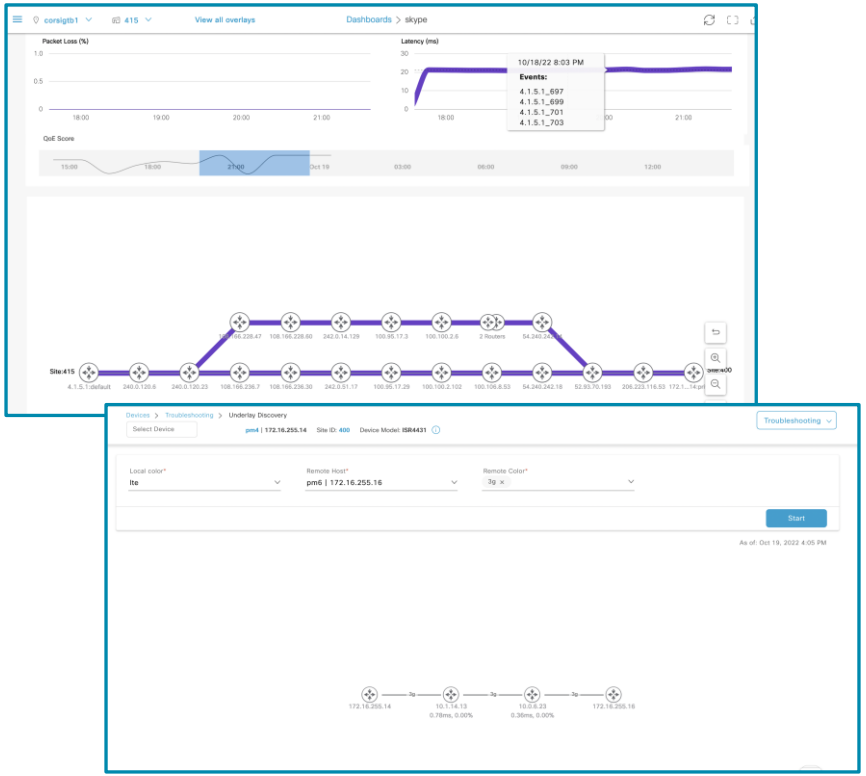
(including hop-by-hop metrics)

* Requires vManage 20.10+

Highlights

1. Zoom into the specific time period showcasing drop in application health (QoE) trend line
2. View the hop-by-hop underlay path along with loss and latency metrics at every hop
3. View associated loss, latency besides underlay path

- Underlay visibility available with vManage as well for on-demand troubleshooting
- Gain additional insights w/ ThousandEyes:
  - Underlay visualization for **DIA paths to SaaS Apps**
  - Discover multiple **candidate underlay paths**
  - Granular statistics - from 1-min thru 1-hour



Key Building Blocks of AppQoE

Configuration Management System

vManage – Virtualized | Scalable | Network Insights

DRE, LZ

Byte Level Caching & Compression

Protocol Agnostic

Forward Error Correction

Packet Duplication

110 110
1011 1011
010 010
110 110
1011 1011
010 010

TCP Optimization

BBR2 Congestion Algorithm

Window Scaling

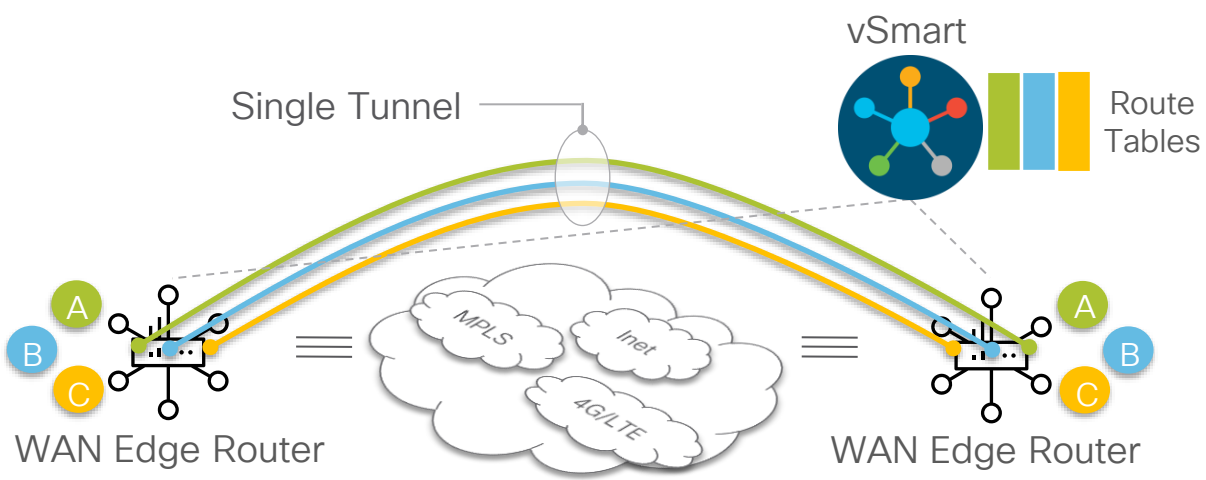
Large Initial Windows

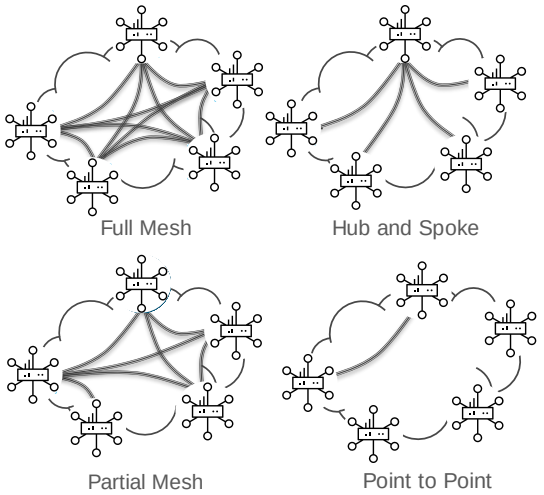
Selective Acknowledgement

BBR – Bottleneck Bandwidth and Round-trip propagation time

Security features

End-to-End Segmentation with Multi-Topology

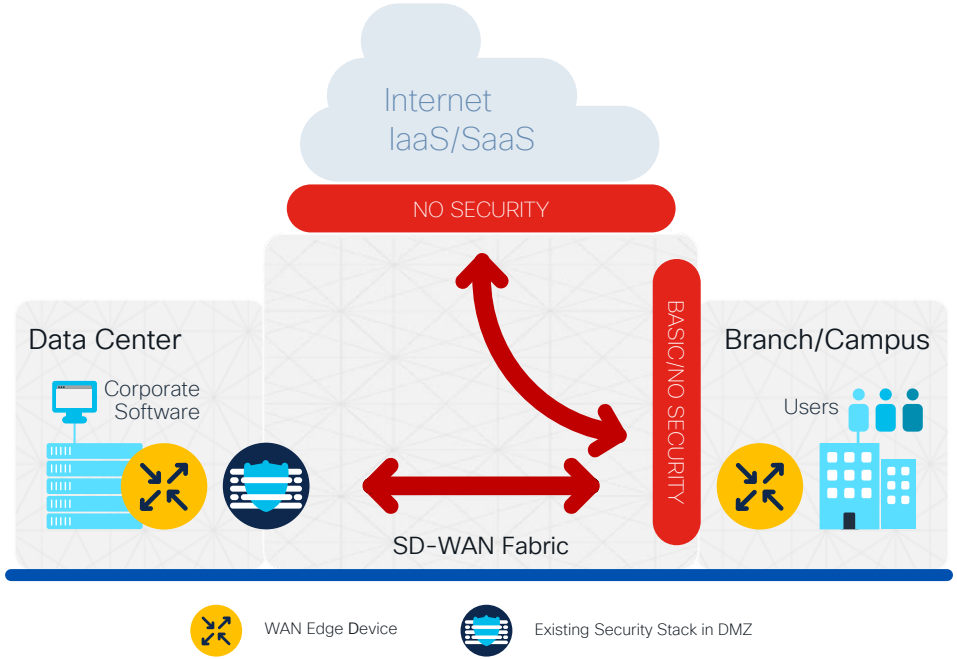




Segment connectivity across the SD-WAN fabric without reliance on underlay transport

WAN Edge routers maintain per-VPN routing table for complete control plane separation

How SD-WAN Exposes New Security Challenges



Internal & External Threats

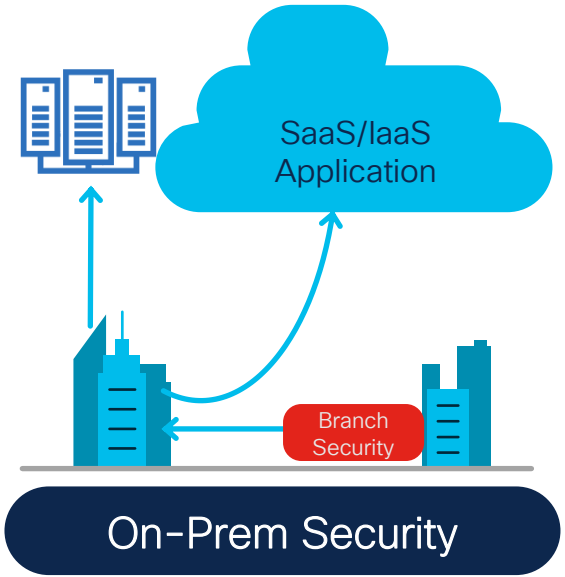
External

- Exposure to malware & phishing due to direct internet and cloud access
- Data breaches
- Guest access liability

Internal

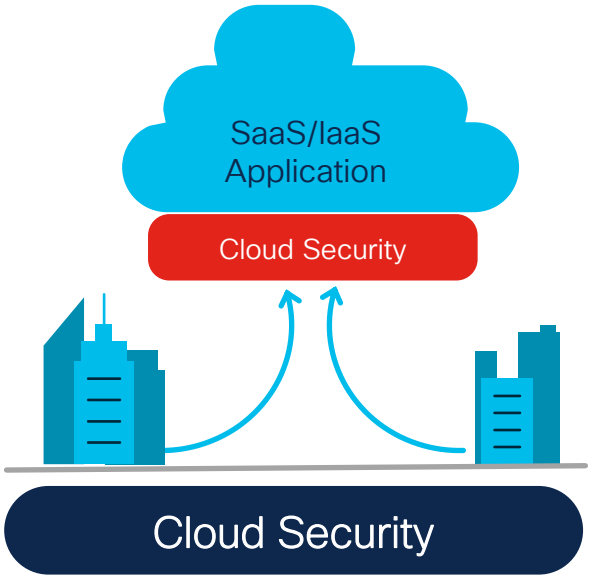
- Untrusted access (malicious insider)
- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)

Relevant Security Models. Driving towards SASE



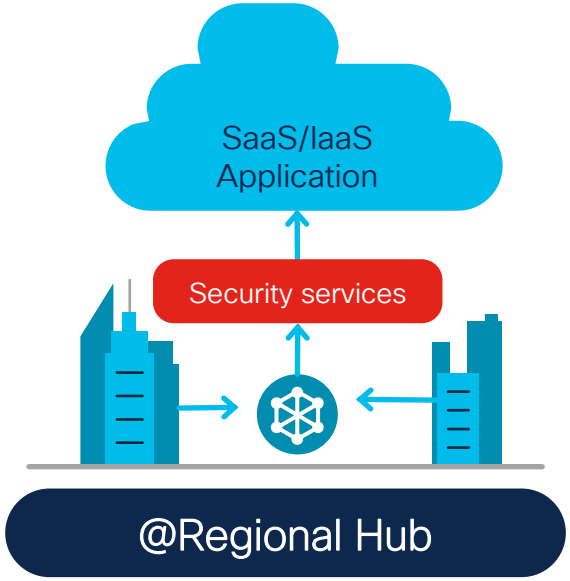
On-Prem Security

Thick branch with Routing and Security



Cloud Security

Thin branch with security in the cloud



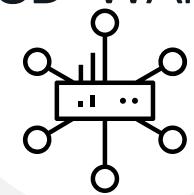
@Regional Hub

Security Services on a Regional Hub

Cisco SD-WAN Security & SASE Solution

Consistent across on-prem and cloud

Cisco SD-WAN



< 8G Ram

Cisco Security

Enterprise Firewall
Layer 3 to 7 apps classified with User Identity

Intrusion Protection System
Most widely deployed IPS engine in the world
Custom Applications

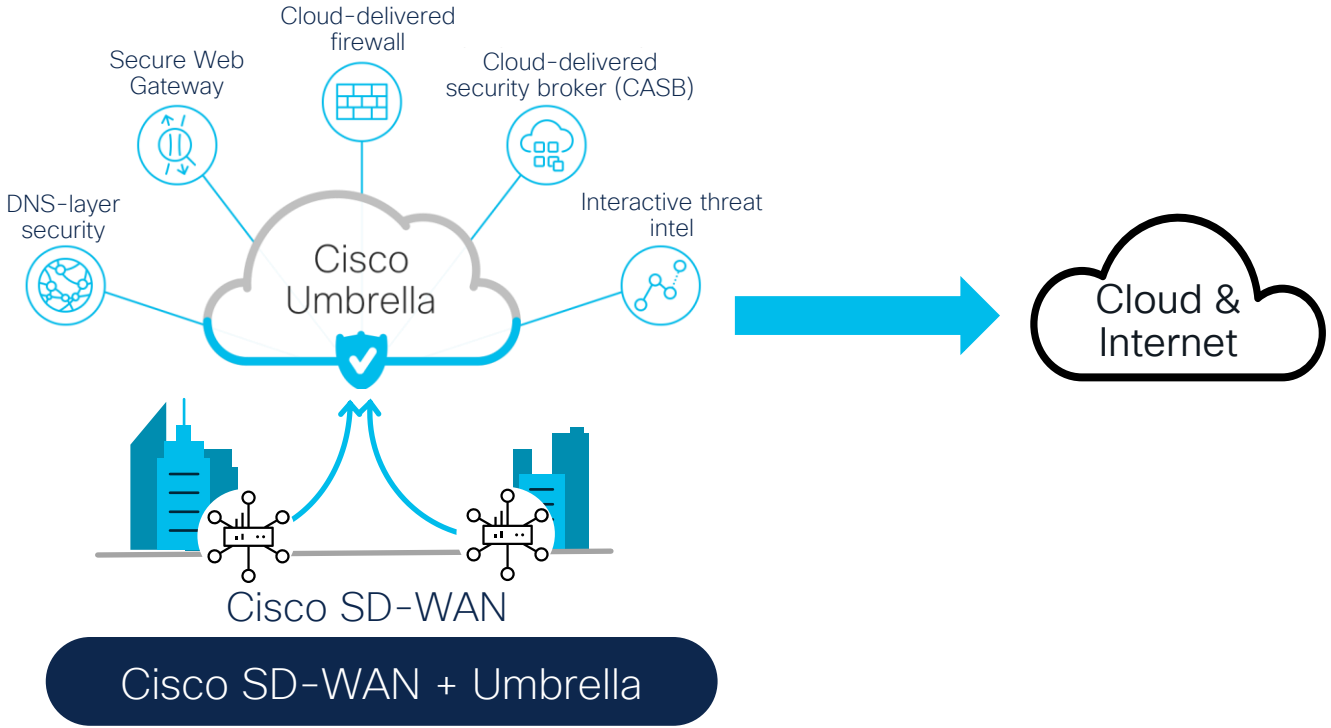
URL-Filtering
Web reputation score using 82+ web categories

Adv. Malware Protection
With File Reputation and Sandboxing (TG)

SSL Proxy
Detect Threats in Encrypted Traffic

Umbrella Cloud Security
DNS Security/Cloud FW with Cisco Umbrella

Transitioning towards a Cloud security model

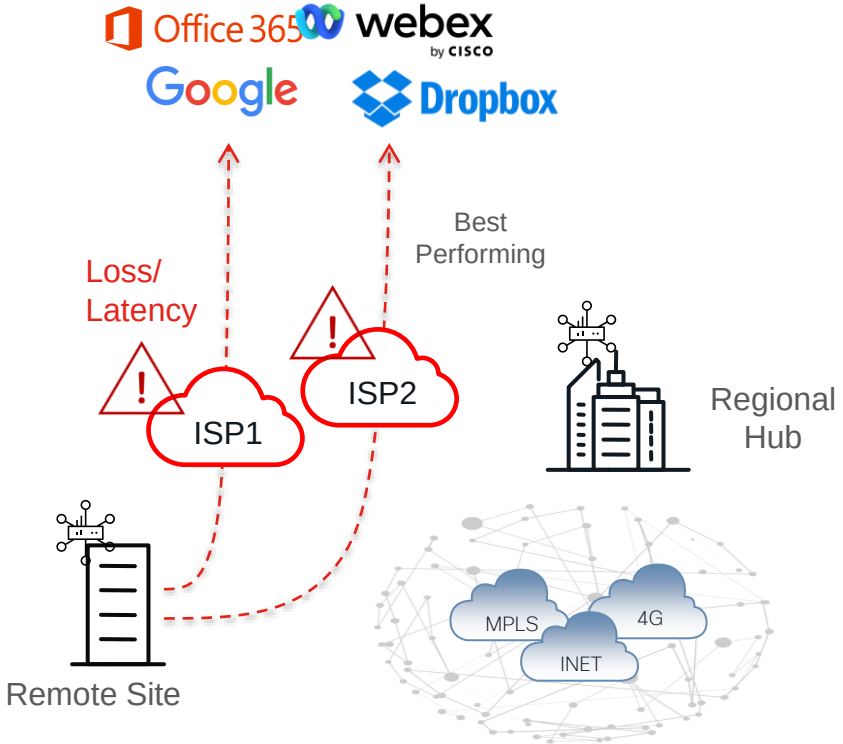


Cloud OnRamp for SaaS

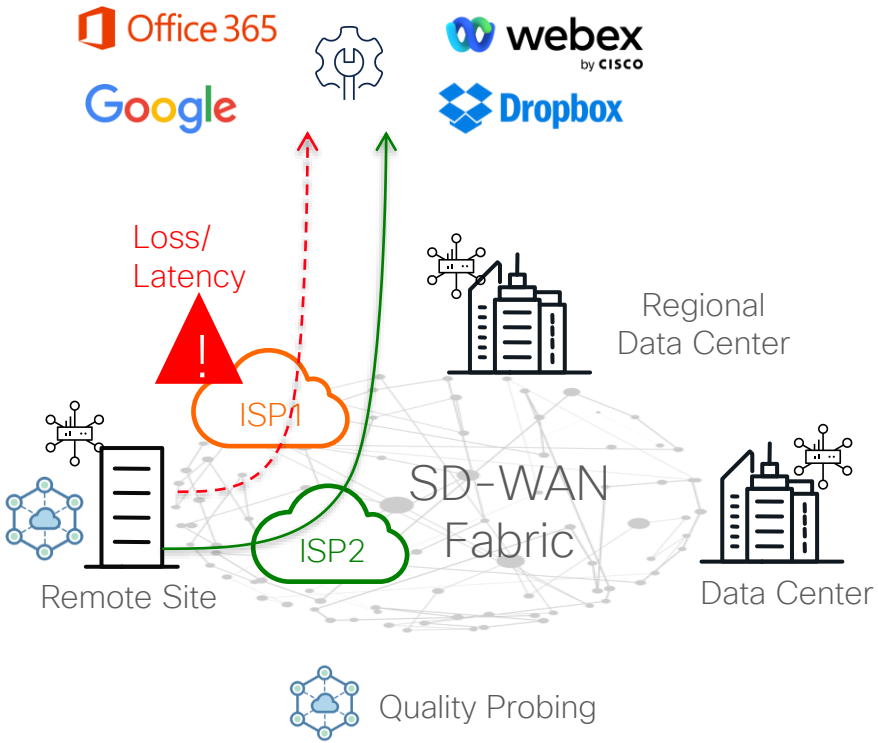
SaaS Optimization Challenges

Learn more watch BRKENT-3412

- Internet circuits performance is unreliable.
- How to get performance visibility for each available path?
- When specific path is having performance issues, How to automatically steer traffic ?

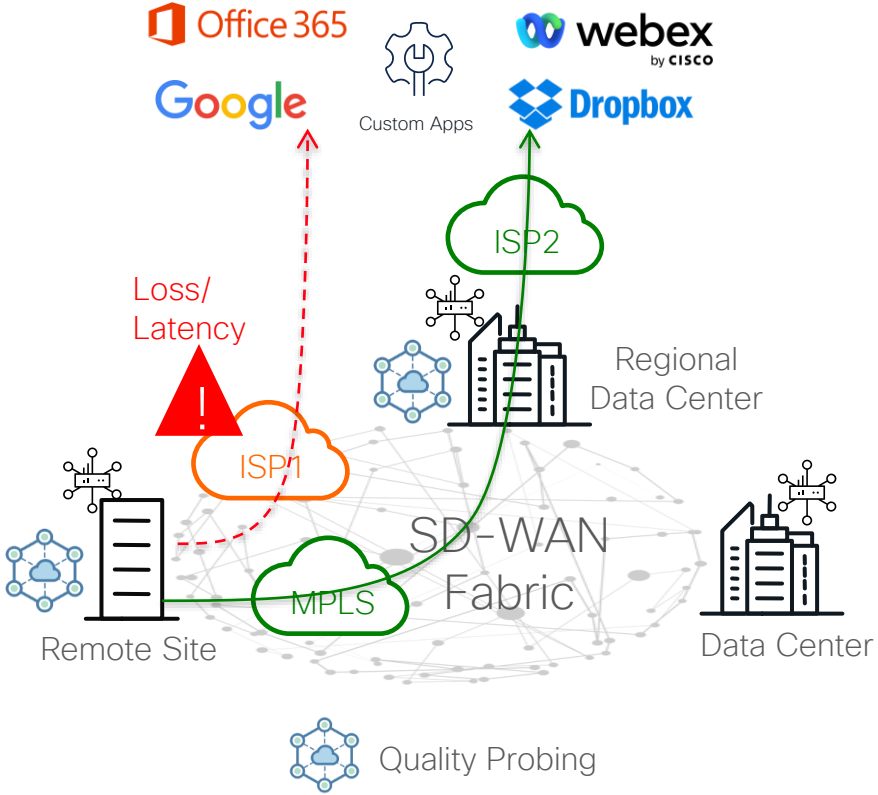


Cloud onRamp for SaaS – Internet DIA



- WAN Edge 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



- Wan Edge 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

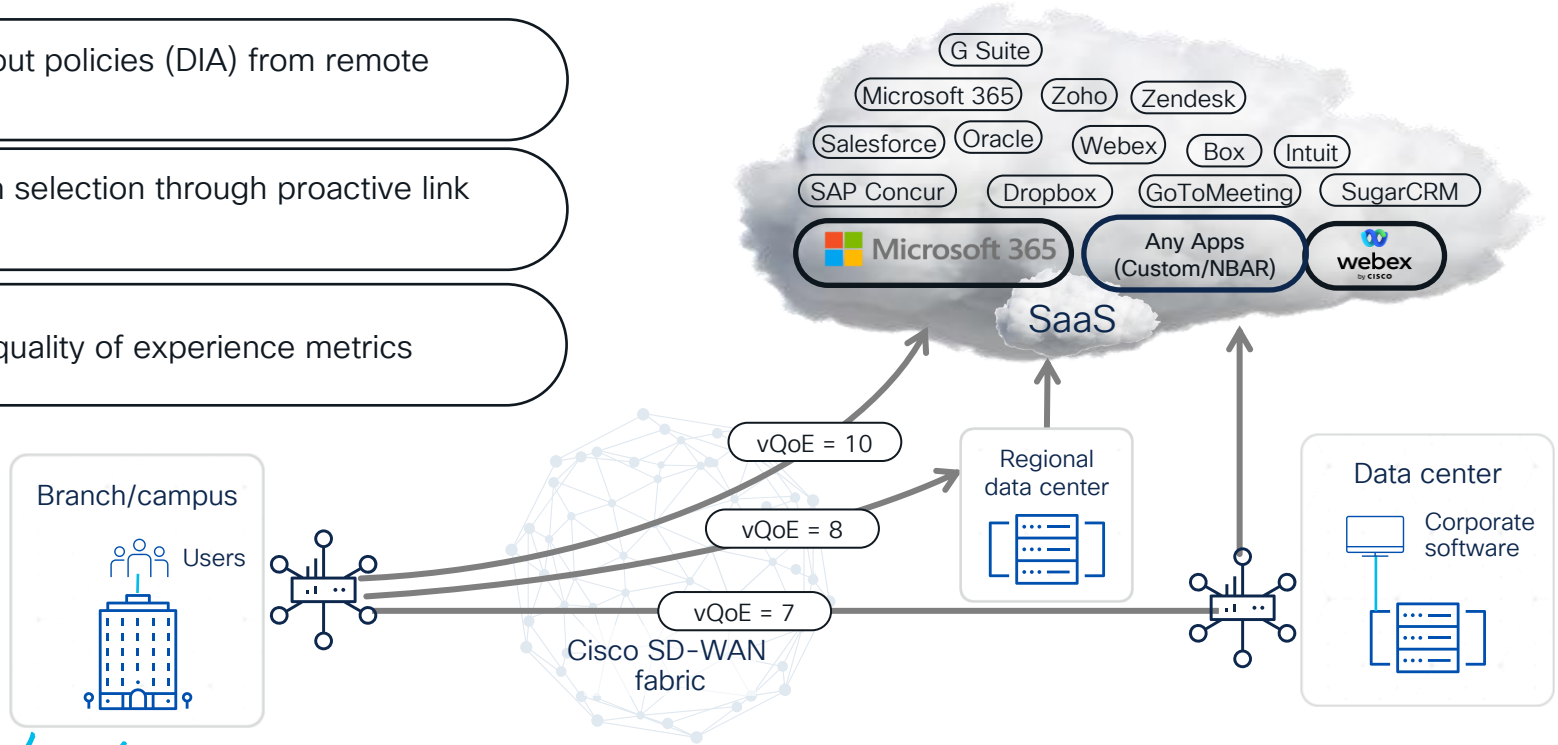
Cloud OnRamp for SaaS

Optimized Connectivity to Cloud Applications

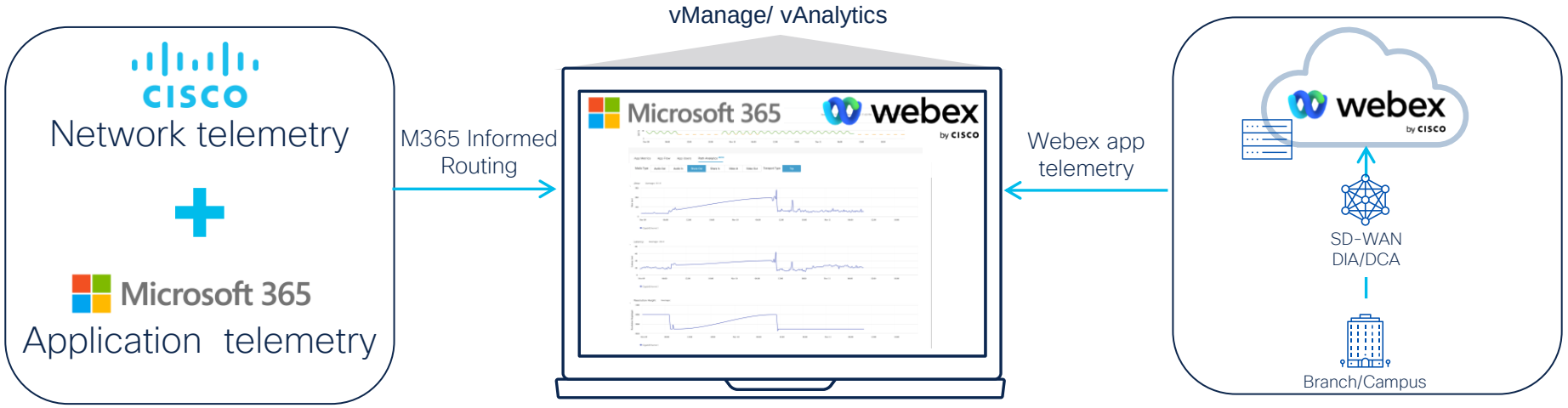
Local breakout policies (DIA) from remote site

Optimal path selection through proactive link probing

Visibility on quality of experience metrics



Application Optimization

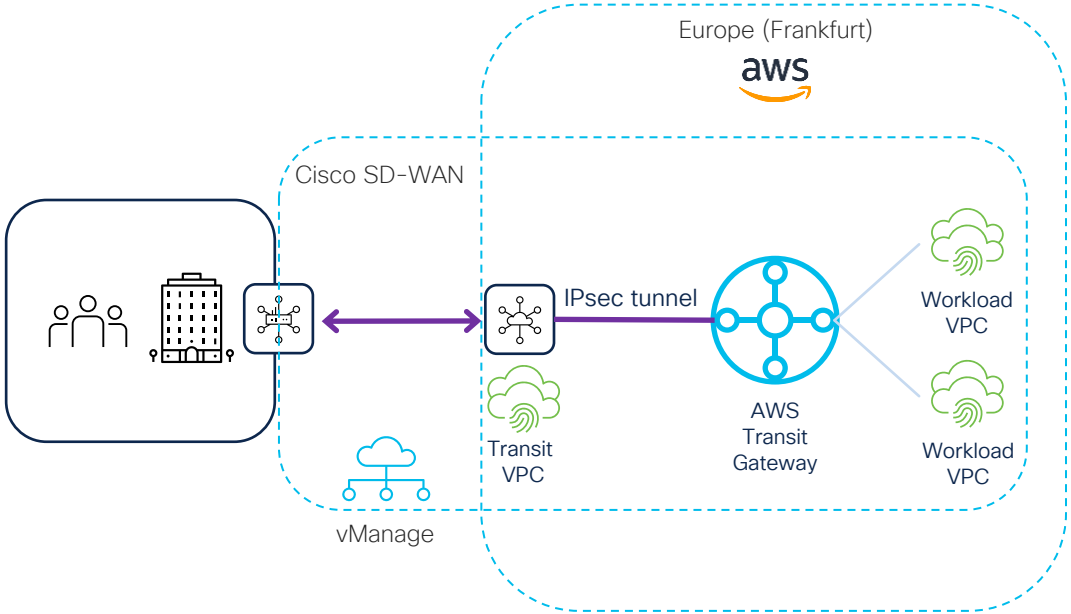


- Optimized Application Experience for Microsoft 365 using Informed Network Routing
- Real application experience feedback from Microsoft
- Application feedback received using telemetry
- Visibility into Application performance
- Webex traffic identification through Webex APIs
- Optimal path selection by link probing using Webex responders

Cloud OnRamp for MultiCloud–AWS

cisco Live!

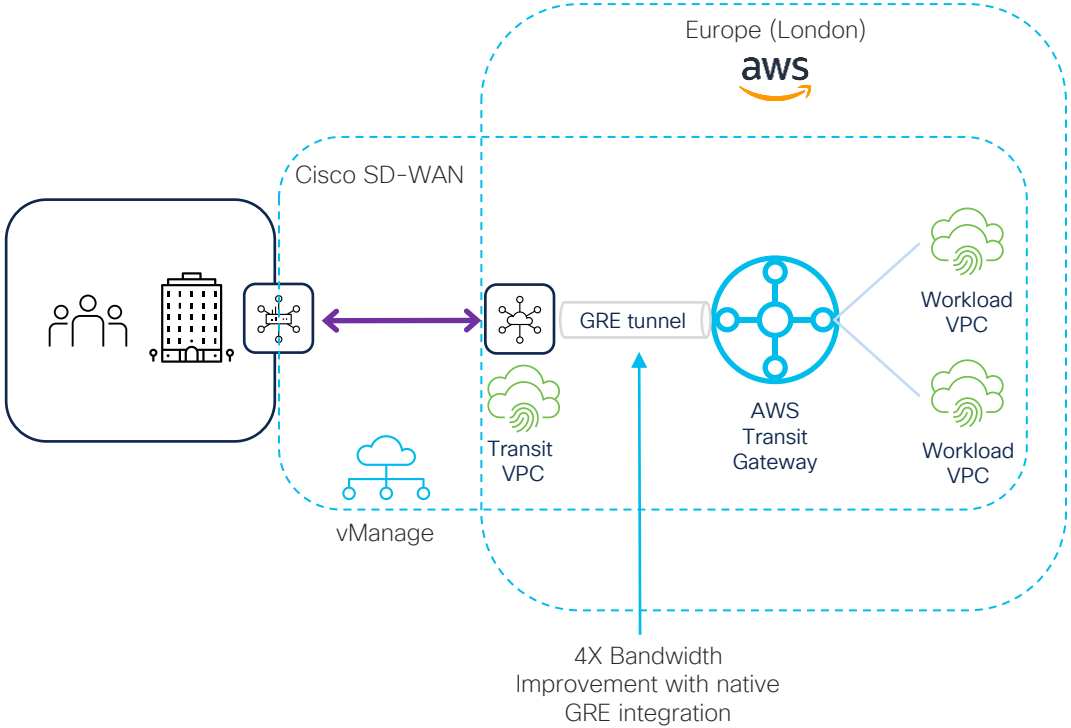
Cisco SD-WAN Cloud OnRamp for Multicloud with AWS Transit Gateway – Option 1



Cisco SD-WAN on-premises router

Cisco SD-WAN cloud router – Catalyst 8000V

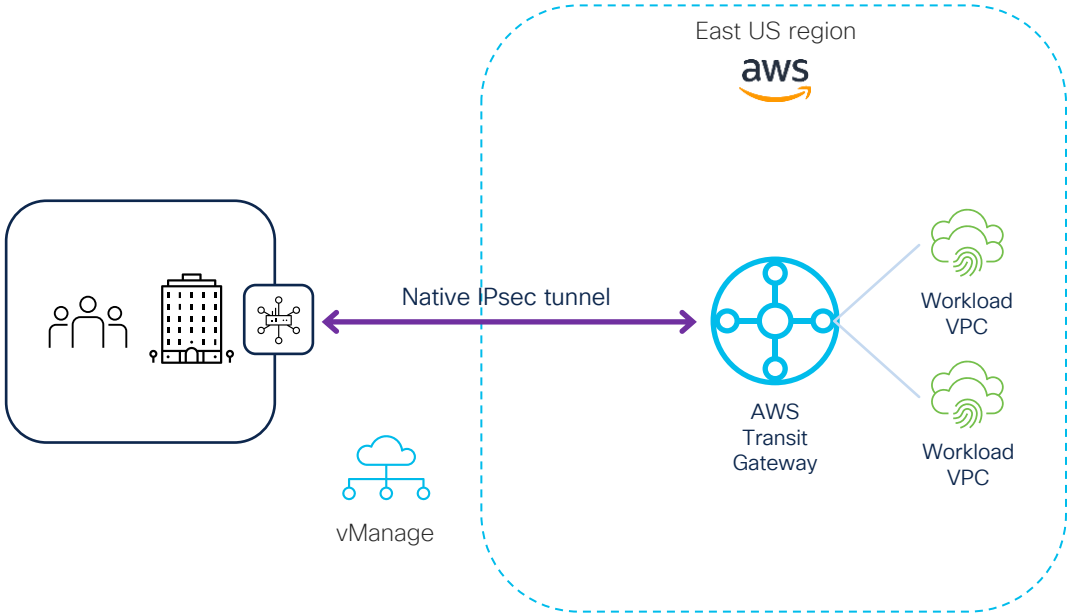
Cisco SD-WAN Cloud OnRamp for Multicloud with AWS Transit Gateway – Option 2



Cisco SD-WAN on-premises router

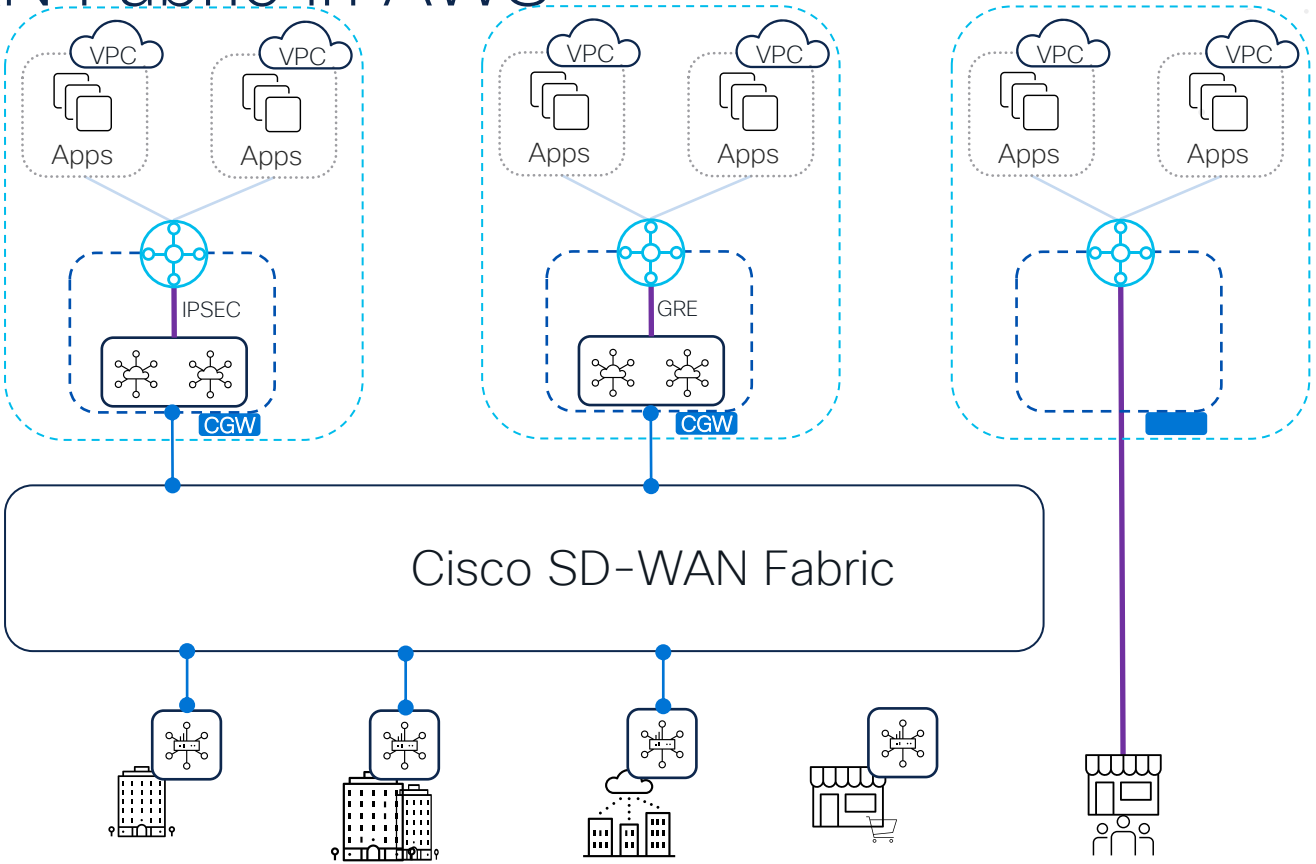
Cisco SD-WAN cloud router – Catalyst 8000V

Cisco SD-WAN Cloud OnRamp for Multicloud with AWS Transit Gateway – Option 3



Cisco SD-WAN on-premises router

SD-WAN Fabric in AWS

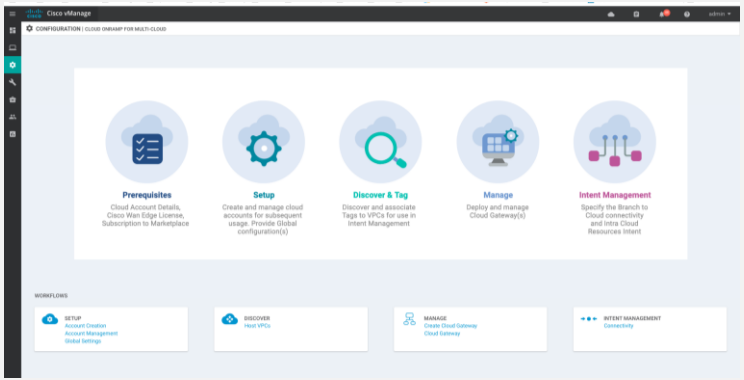


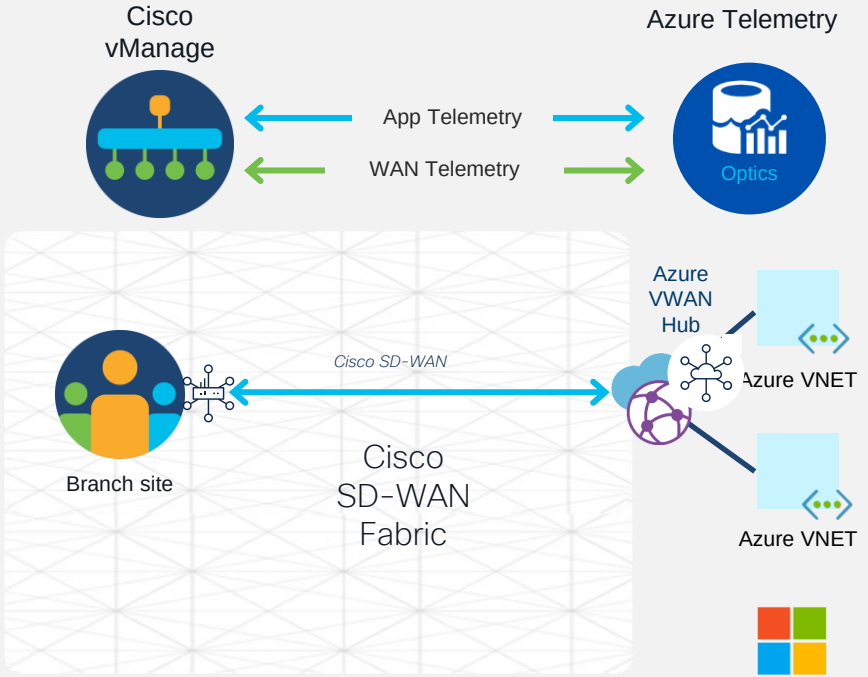
Cloud OnRamp for MultiCloud–Azure

cisco Live!

Cloud onRamp for Multicloud (Azure VWAN)

SD-WAN NVA (Network Virtual Appliances) in VWAN Hub





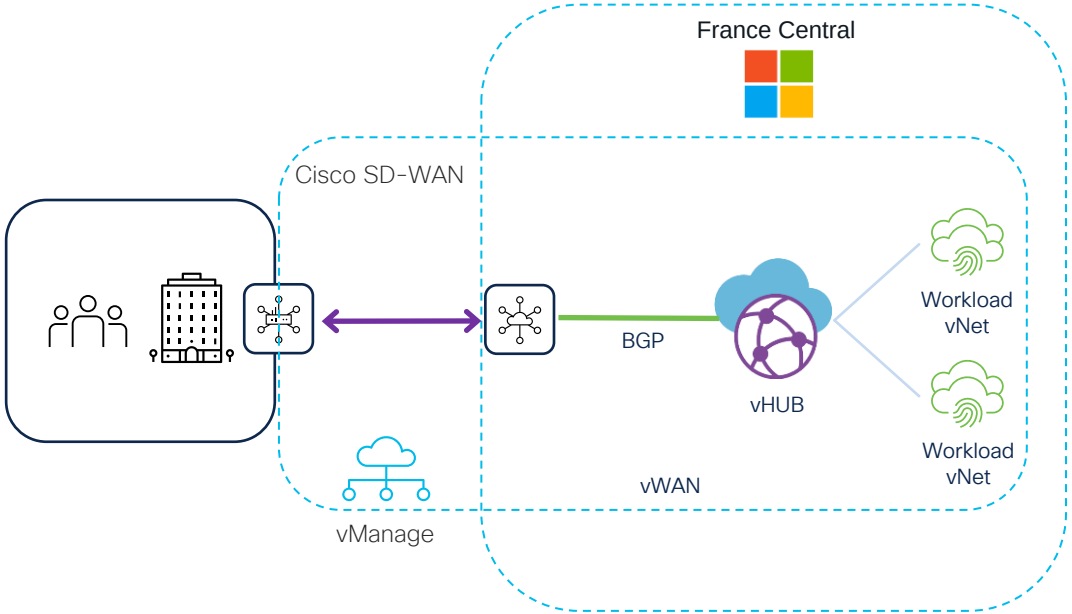
Seamless SD-WAN extension to Microsoft Azure using virtual instances of on-prem devices

Native integration of SD-WAN end points and policy extension into Microsoft vWAN

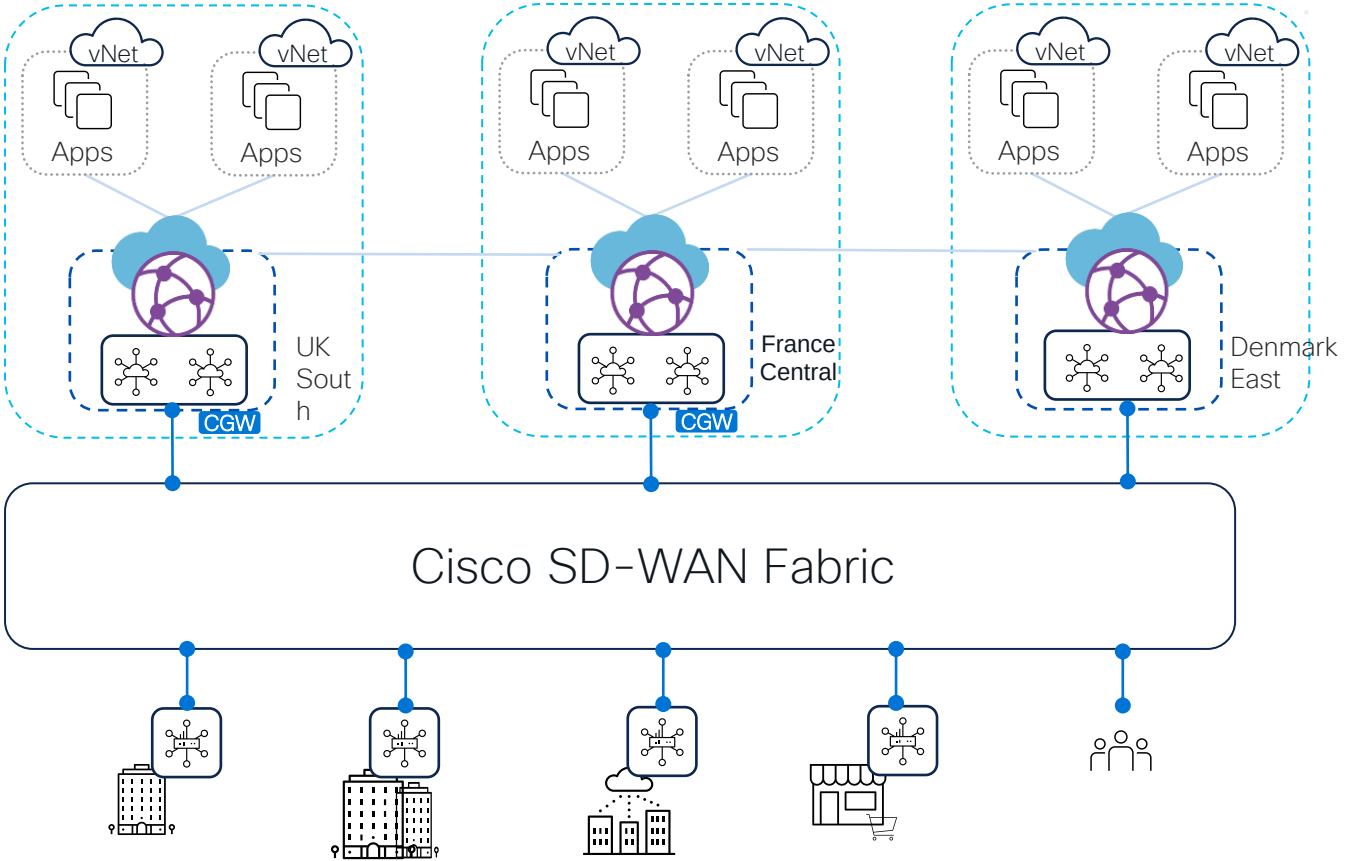
Azure Telemetry Sharing: Advanced APM, troubleshooting and remediation

SD-WAN NVA in VWAN Hub	Auto Peering with VWAN Hub Services	Policies synced with vWAN and vManage

Cisco SD-WAN Cloud OnRamp for Multicloud with Microsoft Azure



SD-WAN Fabric in Azure



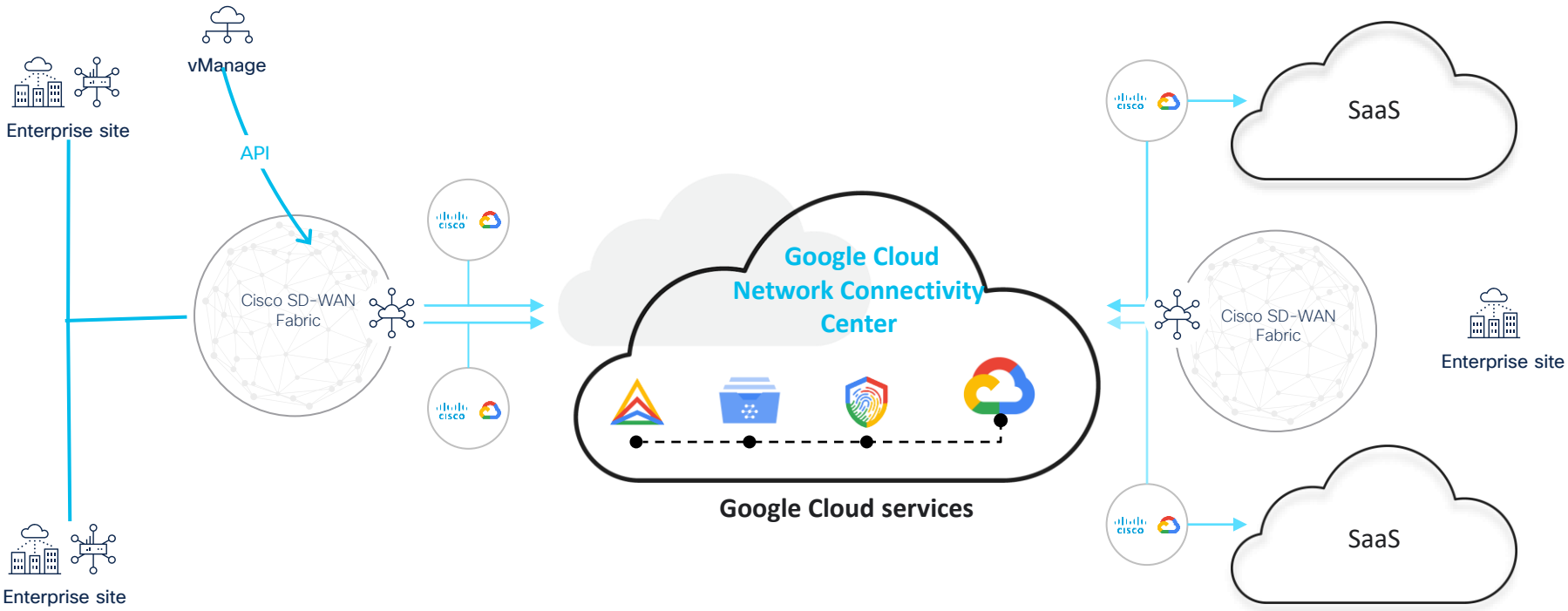
Cloud OnRamp for MultiCloud–Google Cloud

cisco Live!

Cisco SD-WAN Cloud Hub and Google Cloud Network Connectivity Center

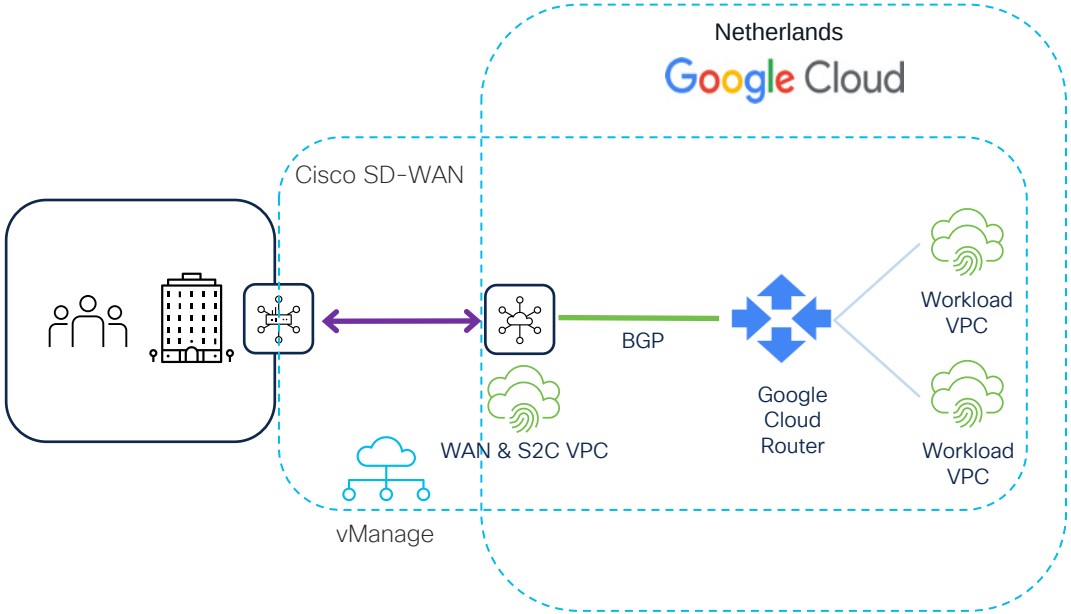
= Cisco SD-WAN router on-premises

= Cisco SD-WAN cloud router at Google Cloud PoP

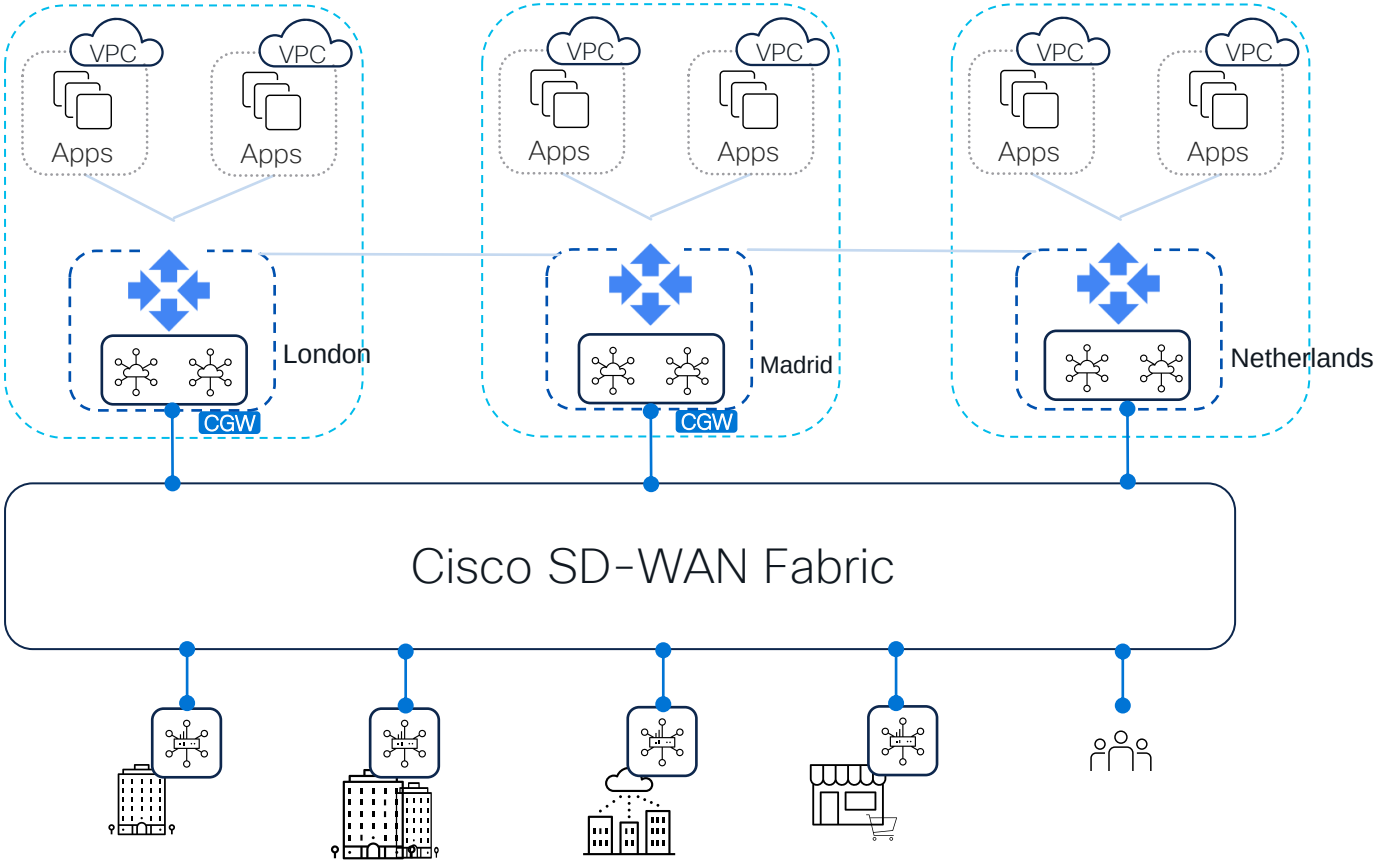


Cisco SD-WAN Cloud Hub with Google Cloud

Cisco SD-WAN Cloud OnRamp for Multicloud with Google Cloud



SD-WAN Fabric in Google Cloud



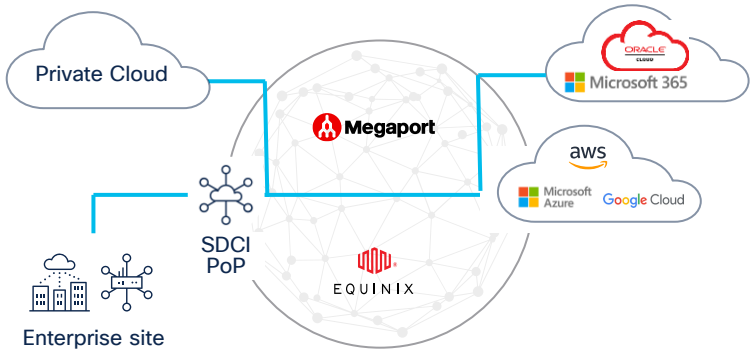
Cloud OnRamp With Interconnect–Megaport and Equinix

cisco Live!

Solution use cases with Cloud Interconnect Partners

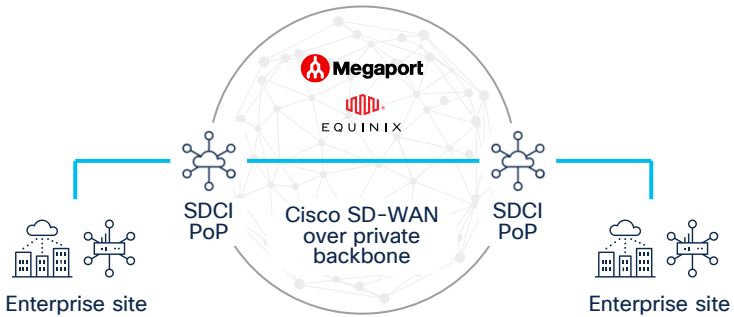
= Cisco SD-WAN router hosted at Megaport or Equinix

Site-to-multicloud



Simple | Automated | Secure

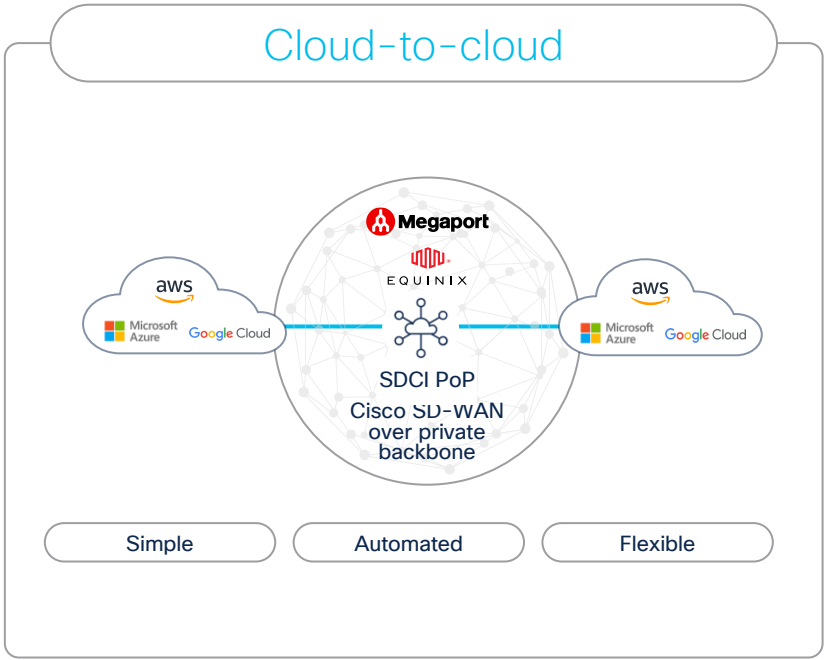
Site-to-site



On-demand | High performance | Global connectivity

Automated with Cisco vManage

Solution use cases with Cloud Interconnect Partners



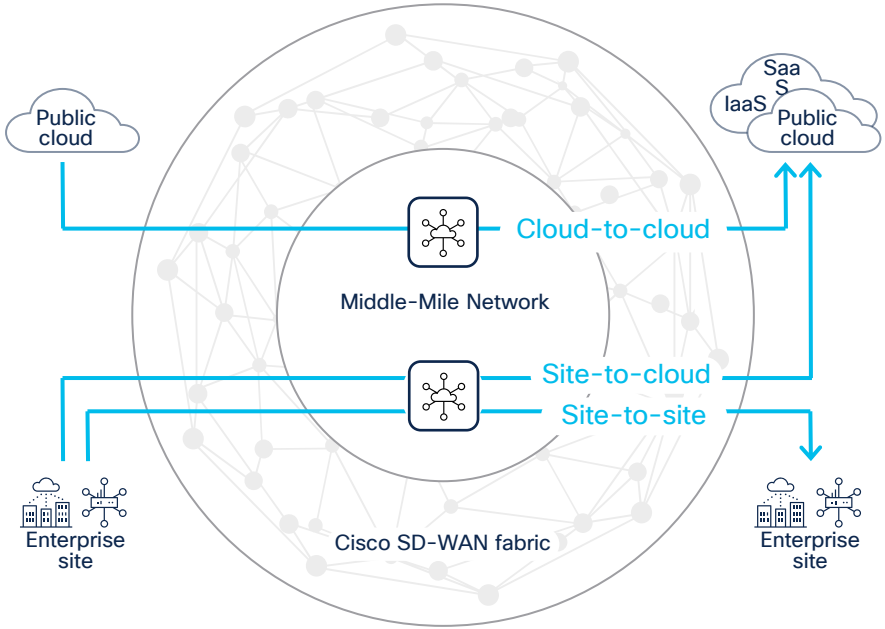
Automated with Cisco vManage

Cisco SD-WAN Middle-Mile Optimization

= Cisco SD-WAN virtual router

= Cisco SD-WAN router on-premises

Megaport EQUINIX aws Cloud WAN Google Cloud NCC Microsoft Azure



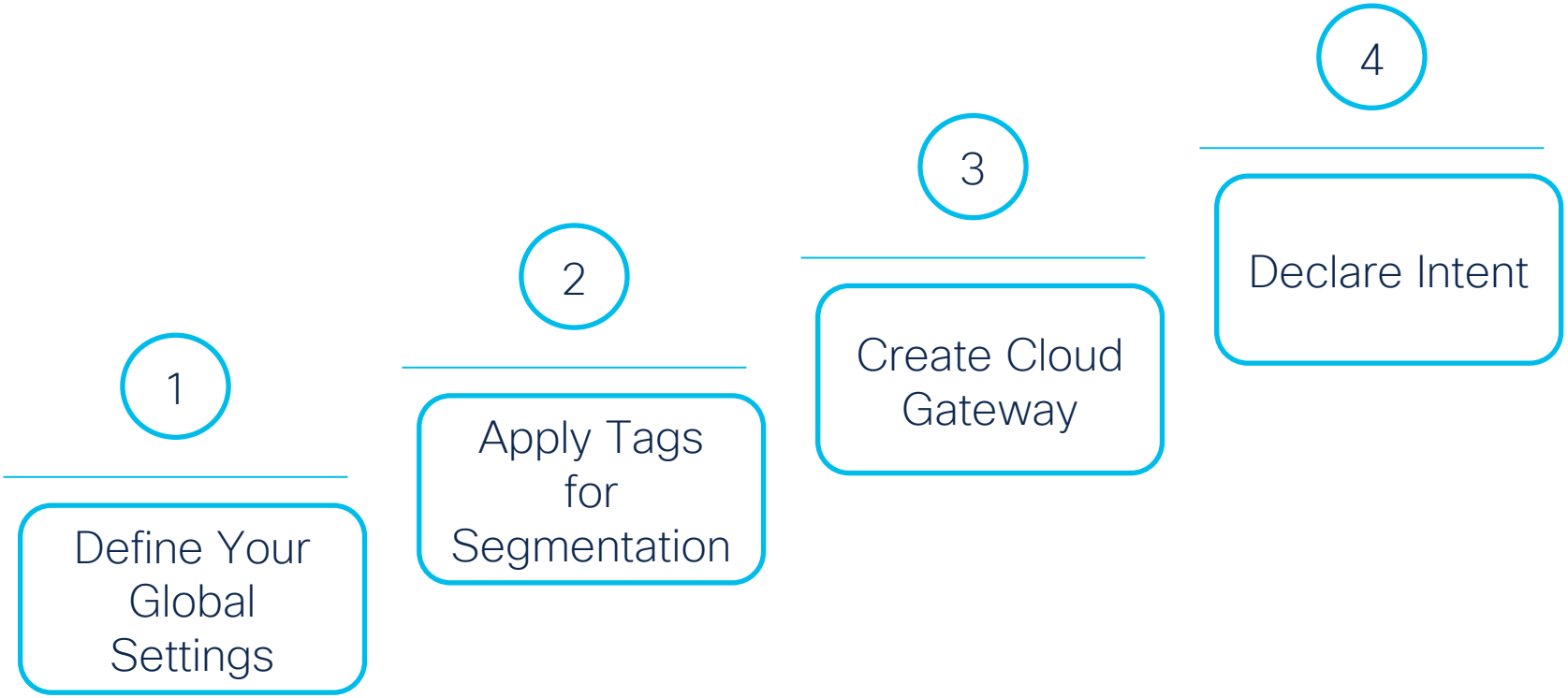
Flexibility
All or selective traffic sent based on type or app

Reliability
Reliable, high-speed connectivity between sites

Security
End-to-end encryption over middle mile global backbone

On-demand
Automated connectivity via vManage central dashboard

4 Easy Steps to Connect Your Sites to Cloud with Cisco SD-WAN

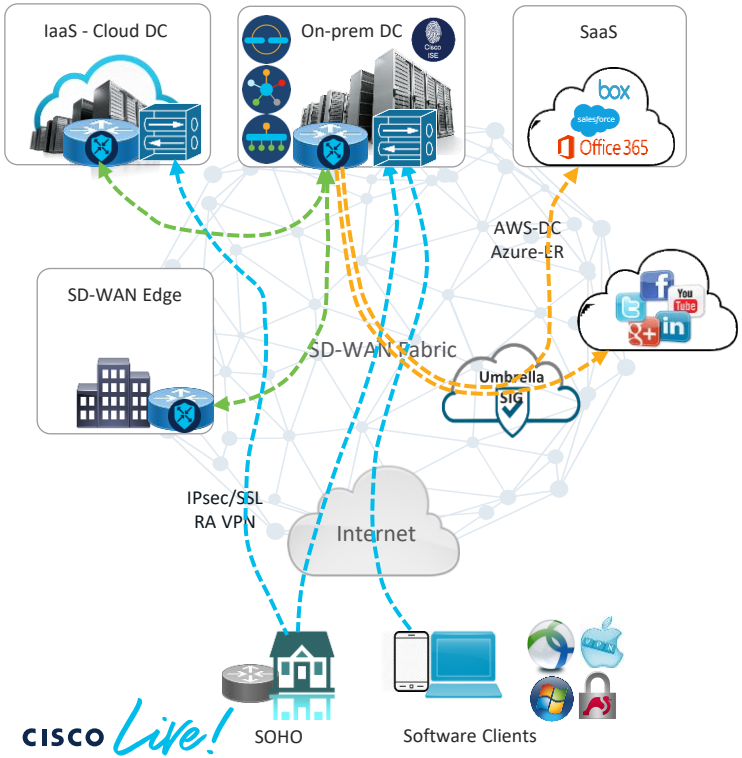


Cisco SD-WAN integrated Remote-Access (SD-WAN RA)

cisco Live!

Traditional Remote Access

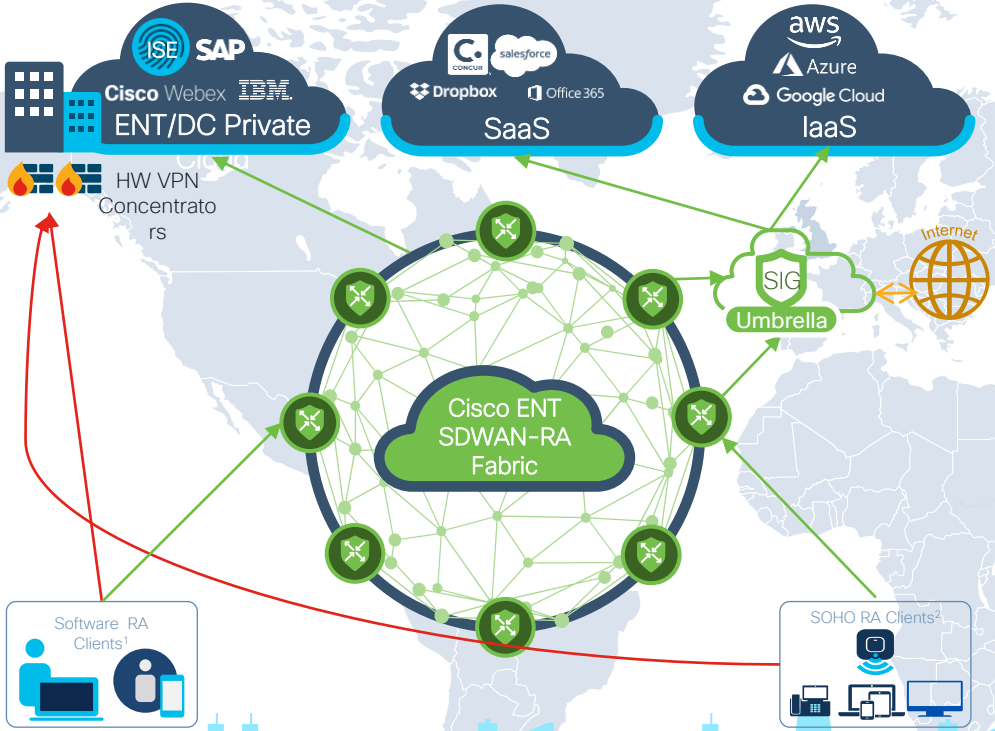
Traditional Remote-Access VPN design



Current Challenges

1. SD-WAN & RA networks treated as separate network
2. More VPN Hardware for higher scale of RA users
3. Separate Management station for Traditional RA network
4. Separate security policies for RA and ENT user traffic, no end-to-end segmentation
5. Backhaul of RA traffic through DC leading to poor application experience
6. RA traffic needs to be stitched to SD-WAN network at DC today

Cisco SD-WAN Remote-Access Architecture overview



Based on Cisco FlexVPN architecture

Cisco IOS-XE FlexVPN supports

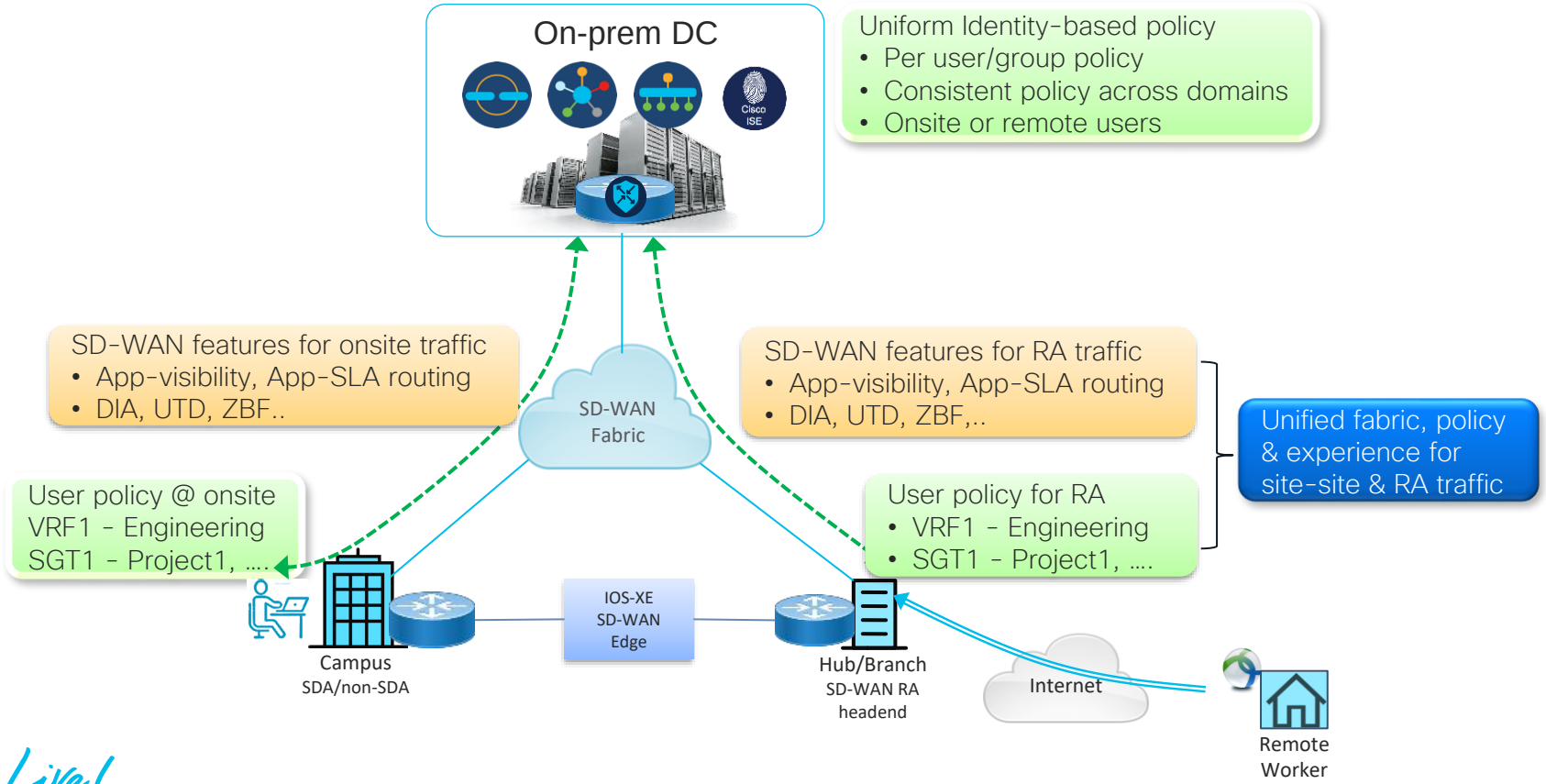
- IKEv2-IPSec based RA
- Dual-stack, micro/macro segmentation
- Integration with Advanced Security features

Cisco SDWAN Edge Router as RA Headend

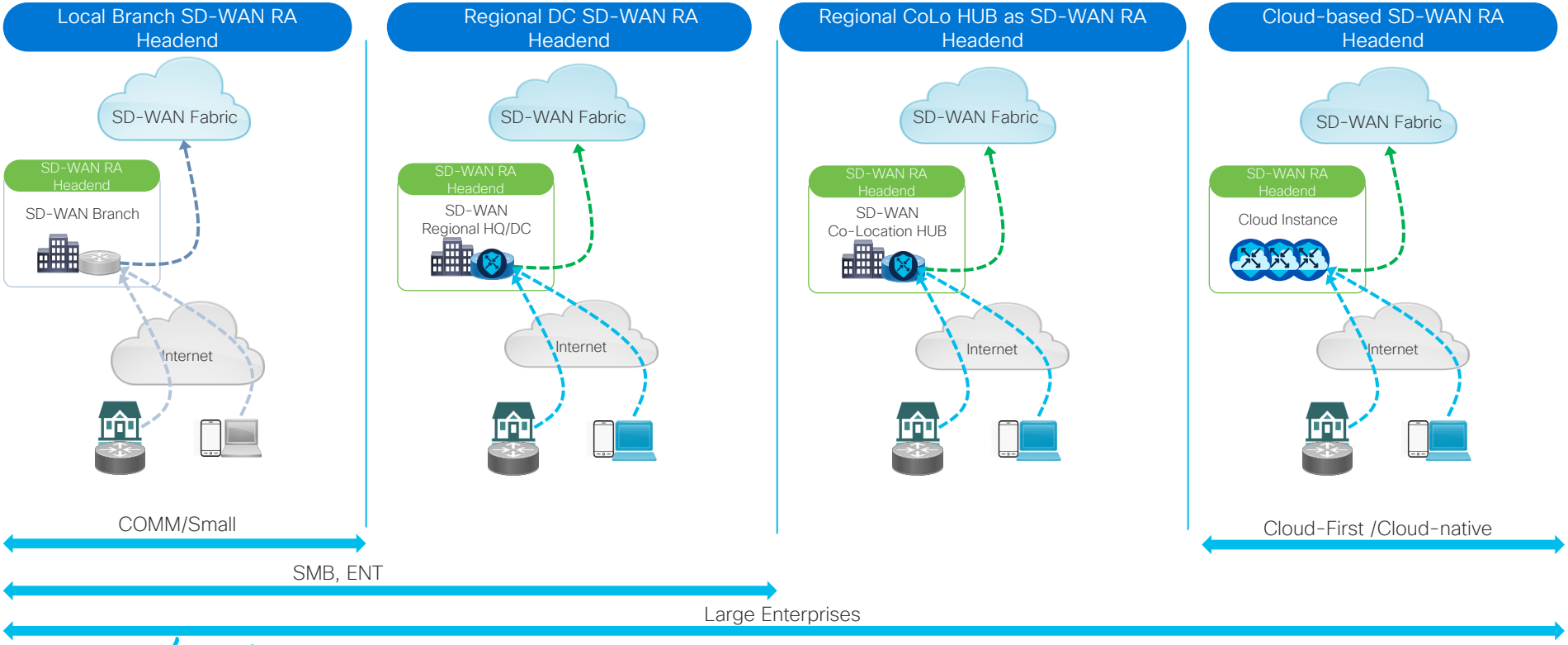
- No more VPN concentrators required
- vMANAGE based Config & Monitoring
- Day-0 integration with On-Prem/Cloud based advanced SDWAN security suite
- Supports both SW and HW based remote-access clients

Cisco SD-WAN RA for Hybrid Work

Enabled by IOS-XE SD-WAN & ISE

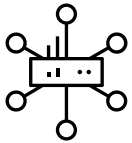


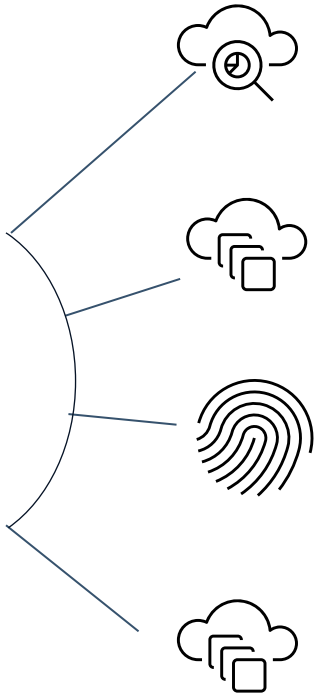
Cisco SD-WAN RA Deployment Models
Regional Hub, Colo, Cloud-based & Branch



Key Takeaways

Cisco SD-WAN





- Single pane of glass Automation
- Optimized for Cloud access
- Pervasive Security
- Predictable and actionable insights

SD-WAN – This is it.

Networking

SD-WAN

Learn how to confidently adopt Cisco's SD-WAN solution in a new or existing network. These sessions provide an advanced journey through the latest Cisco SD-WAN innovations including recent development and integration with Cloud, SASE and Assurance/Analytics.

START

Feb 5 | 16:00
LABENT-1350
Building Basic SD-WAN Overlay with IPv6 Network

Feb 6 | 08:30
TECARC-2407
Architecture, Deployments, and Troubleshooting Deep Dive for Catalyst 8000 Series Edge Platforms

Feb 6 | 14:00
TECTRS-3477
Advanced Troubleshooting SD-WAN

Feb 7 | 08:30
BRKENT-1656
Beginner's Guide to Enterprise Network Monitoring with ThousandEyes

Feb 7 | 11:30
BRKENT-2108
Cisco SD-WAN: Start Here

Feb 7 | 11:30
BRKNWT-2210
Predicting Networks are THERE !!

Feb 7 | 14:00
BRKENT-2628
ThousandEyes with Catalyst 8000 routers: Empowerment from Data in your Pocket

Feb 7 | 15:30
BRKENT-2139
How to Choose the Correct Branch Router

Feb 7 | 17:00
BRKENT-2423
SD-WAN From Design to Reality

Feb 8 | 08:30
BRKENT-2653
All You Need to Know about Forwarding on the Catalyst 8500 and 8500L Platforms

Feb 8 | 08:30
BRKOPS-2857
Deploy Visibility in Your SASE Architecture With ThousandEyes

Feb 8 | 08:30
LTRENT-2052
IPv6 Routing, SD-WAN and Services Lab

If you are unable to attend a live session, you can watch it On Demand after the event

Feb 8 | 08:30
LTRENT-3615
Cisco SD-WAN Multi-Region Fabric – from Zero to Hero

Feb 8 | 10:30
BRKXAR-2003
Extending Enterprise Network into Public Cloud with Cisco Catalyst 8000V Edge Software

Feb 8 | 12:00
BRKENT-2652
Simplify User Experience through Software defined Interconnect and Public cloud

Feb 8 | 14:30
BRKTRS-3475
Advanced Troubleshooting of cat8k, asr1k, ISR and SD-WAN Edge Made Easy

Feb 8 | 16:30
BRKENT-2060
Cisco SD-WAN Cloud OnRamp for Multicloud - from Connectivity to Application Integration

Feb 8 | 16:30
BRKENT-2651
Migration to Multi-Region Fabric - Transform and Simplify Middle-mile Based Network Designs for Large Scale, Cloud and Colo based SD-WAN Networks

Feb 8 | 16:45
BRKXAR-2001
Cisco Intent Based Cross and Multidomain Integrations for SDA and SD-WAN

Feb 9 | 08:30
BRKARC-2885
Cisco Catalyst 8500 Series Edge Platform Deep Dive

Feb 9 | 10:30
BRKENT-2837
GAME Time ! Will You Be the Networker of the Year ?

Feb 9 | 10:30
BRKENT-3297
Multi-Cloud SD-WAN Design

Feb 9 | 12:00
BRKENT-2312
Evolution of Cisco SD-WAN Security and Journey Towards SASE

Feb 9 | 14:15
BRKENT-3412
How to Optimize SaaS Applications using Cisco SD-WAN

Feb 9 | 15:45
BRKENT-2126
Three Steps to Gain Actionable Visibility in the Cisco SD-WAN Using ThousandEyes

Feb 9 | 15:45
BRKMER-1003
Cisco+ Secure Connect - Connect and Secure with Meraki

Feb 10 | 11:00
BRKTRS-3457
Cross-Domain Integration: Troubleshooting Cisco SD-Access - SD-WAN Integration

Feb 10 | 11:00
BRKTRS-3793
Advanced SD-WAN Routing Troubleshooting

Feb 10 | 11:15
FINISH
BRKOPS-3179
Wide Area Bonjour (mDNS) - Best practices, Design and Deployment

If you are unable to attend a live session, you can watch it On Demand after the event

cisco Live!

Complete your 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 (open from 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 Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Meet the speaker
Ask your question


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN