

The background is a vibrant, abstract graphic featuring a spectrum of colors (red, orange, yellow, green, blue) arranged in a radial, sunburst-like pattern. The colors transition from warm tones on the left to cooler tones on the right, with a bright white center. The overall effect is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco Catalyst SD-WAN: Start Here

Daniel Atalla, Technical Solutions Architect
BRKENT-2108

CISCO *Live!*

#CiscoLiveAPJC

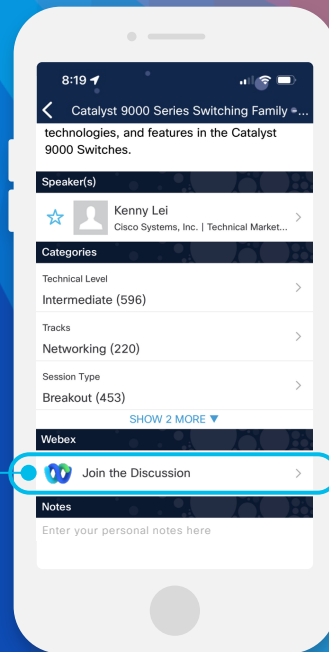
Cisco Webex App

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



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2108>

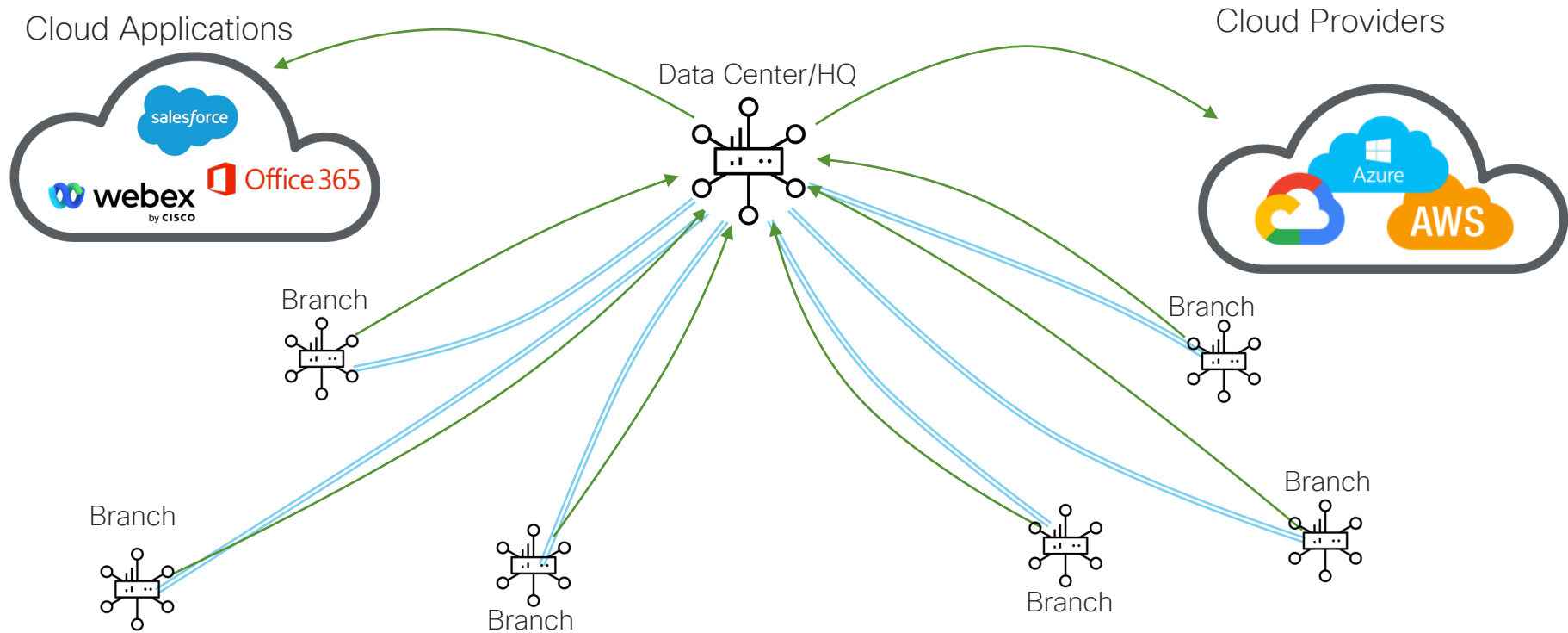
Agenda

- 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.

The Hardware Based WAN of Yesterday

Doesn't Keep up with the Needs of Today



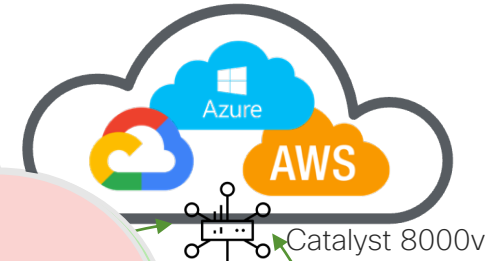


Learn more watch
BRKENT-2139

Cisco SD-WAN: Software Approach

Cloud Applications

Cloud Providers



Catalyst 8300 Series

Catalyst 8000v

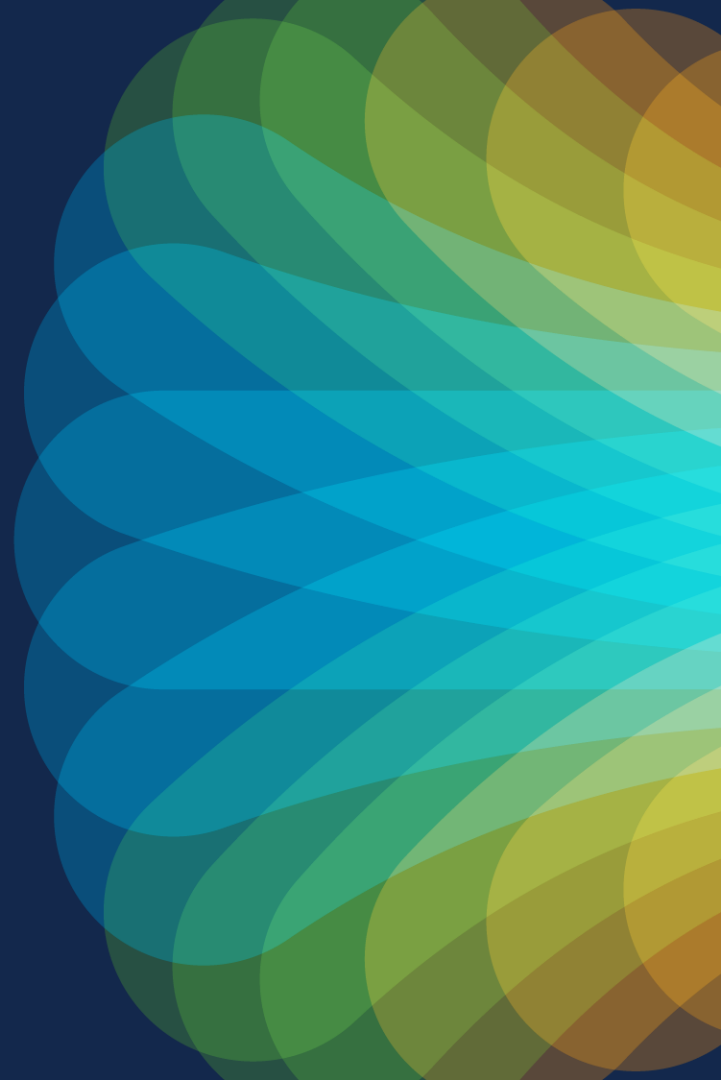
VPN 20 Corporate



Catalyst 8200 Series

Series

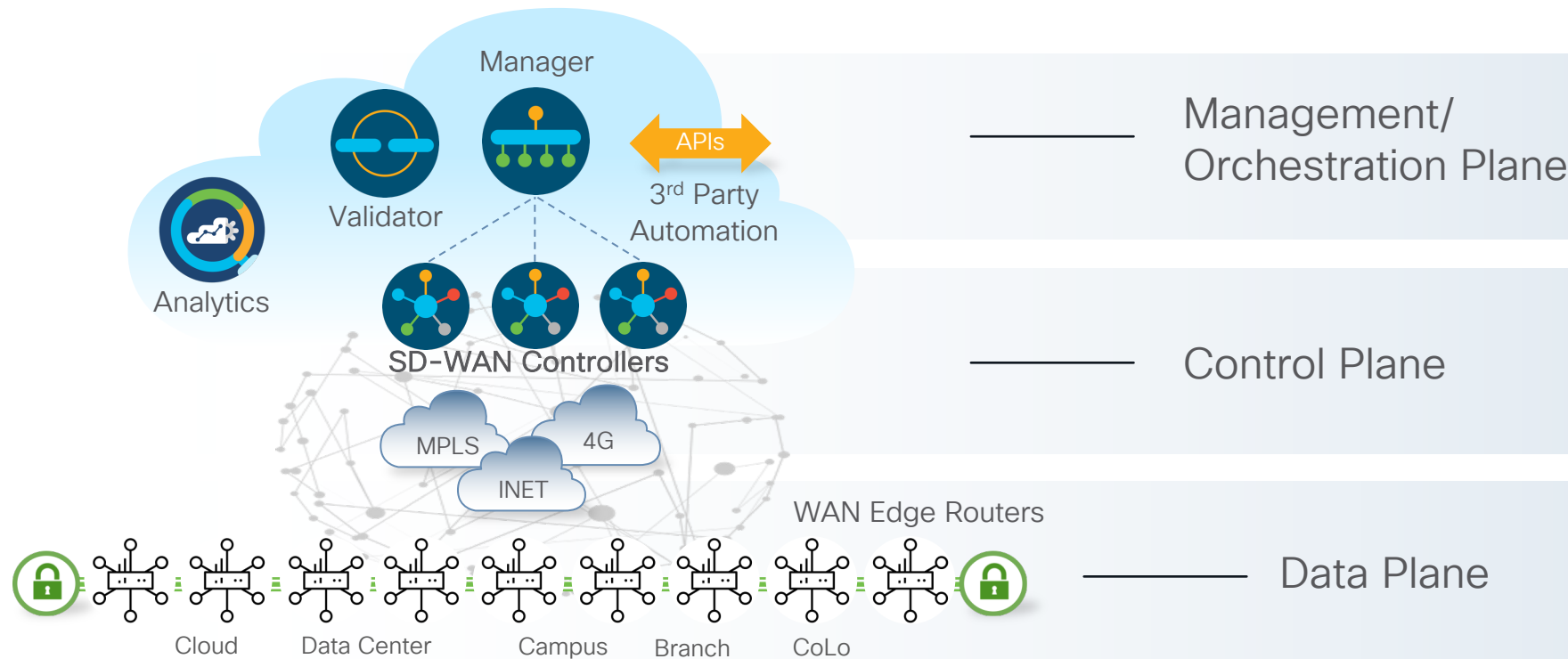
Solution Architecture



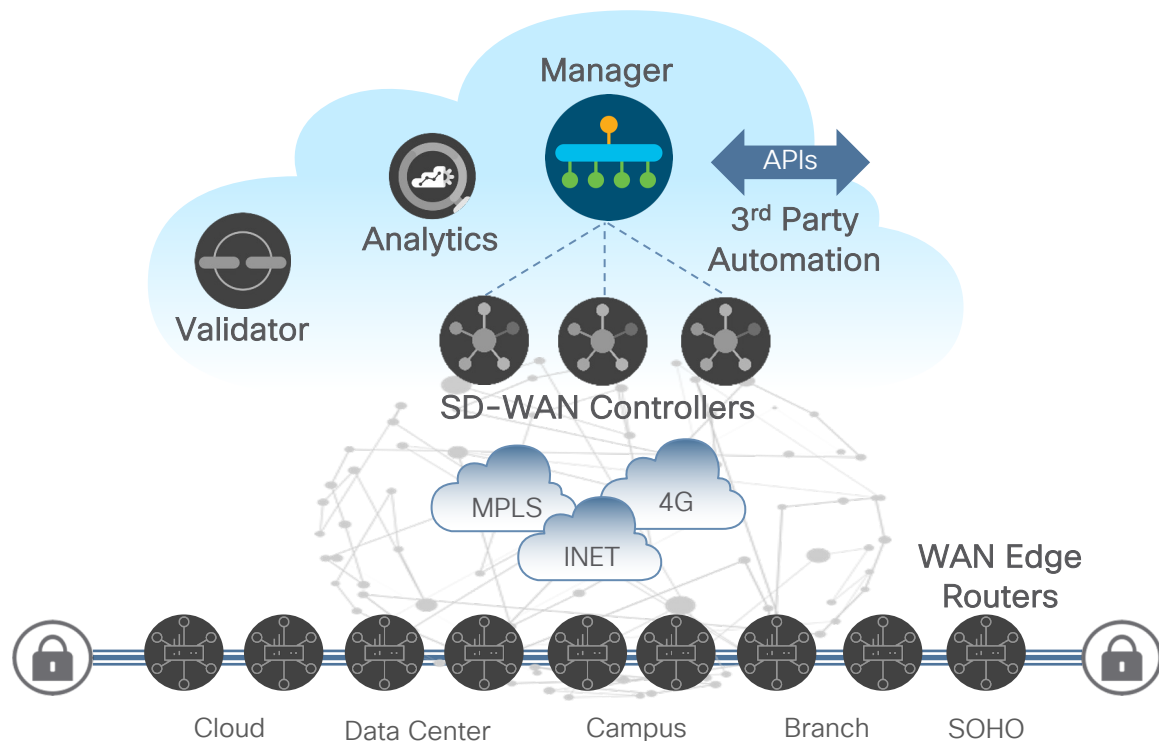
New Naming: Cisco Catalyst SD-WAN

Old Name	New Name (rebranding)	Documentation	Displayed on Screens	API/CLI - Documentation
Cisco SD-WAN	Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN	Cisco Catalyst SD-WAN
vManage	Cisco Catalyst SD-WAN Manager	SD-WAN Manager	Manager	vManage
vAnalytics	Cisco Catalyst SD-WAN Analytics	SD-WAN Analytics	Analytics	vAnalytics
vBond	Cisco Catalyst SD-WAN Validator	SD-WAN Validator	Validator	vBond
vSmart	Cisco Catalyst SD-WAN Controller	SD-WAN Controller	Controller	vSmart
Self Service Portal	Cisco Catalyst SD-WAN Portal	Cisco Catalyst SD-WAN Portal	Cisco Catalyst SD-WAN Portal	SD-WAN Portal
Cloud-Delivered Cisco SD-WAN	Cloud-Delivered Cisco Catalyst SD-WAN	Cloud-Delivered Cisco Catalyst SD-WAN	Cloud-Delivered Cisco Catalyst SD-WAN	NA

Cisco Catalyst SD-WAN Solution Overview



Cisco Catalyst SD-WAN Solution Elements



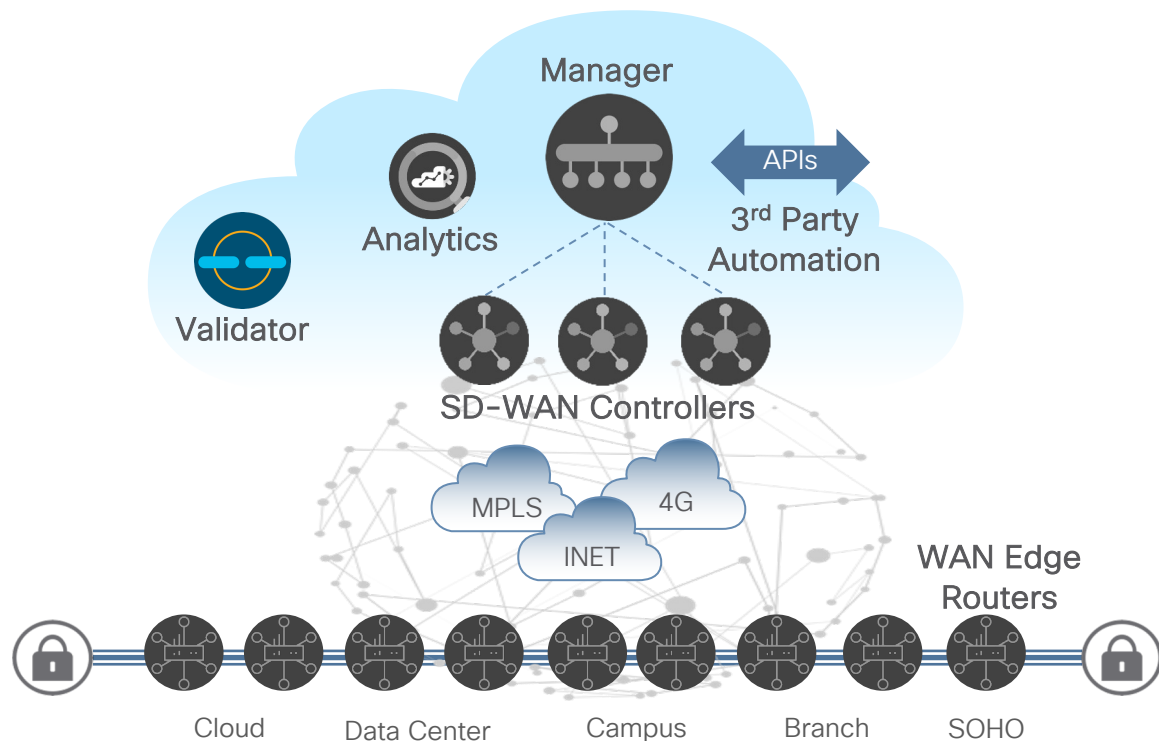
Management Plane



Cisco Catalyst
SD-WAN Manager

- 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 Catalyst SD-WAN Solution Elements



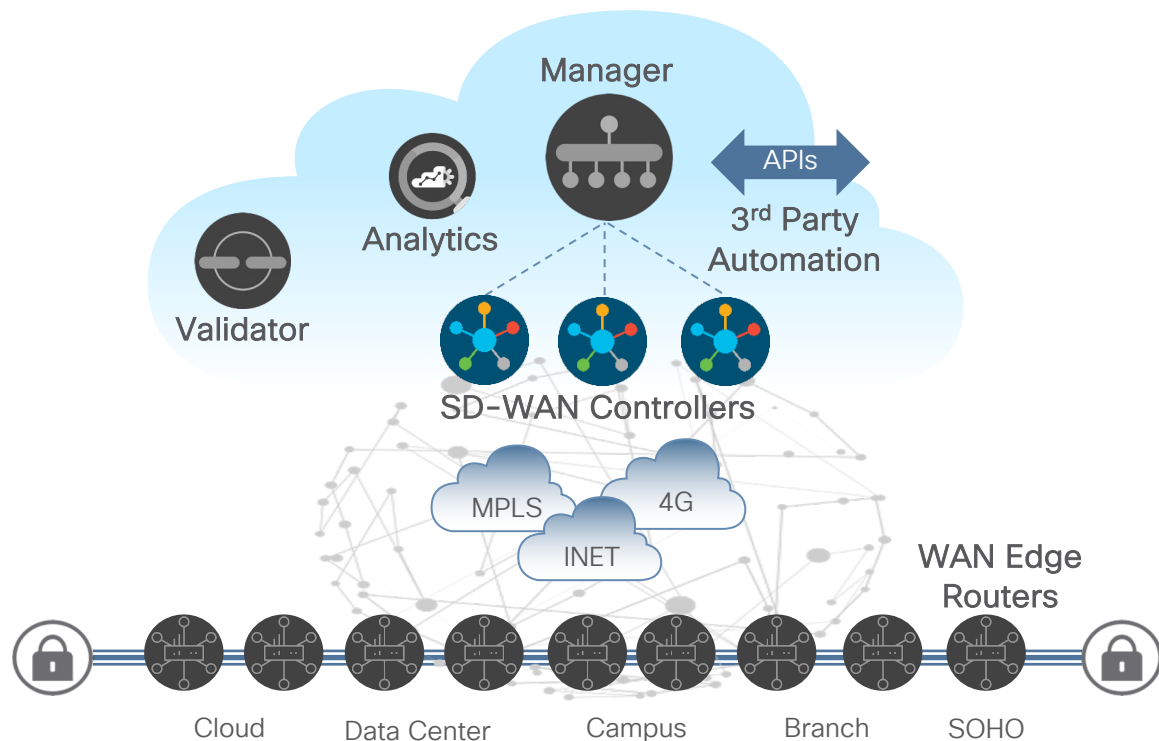
Orchestration Plane



Cisco Catalyst
SD-WAN Validator

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

Cisco Catalyst SD-WAN Solution Elements



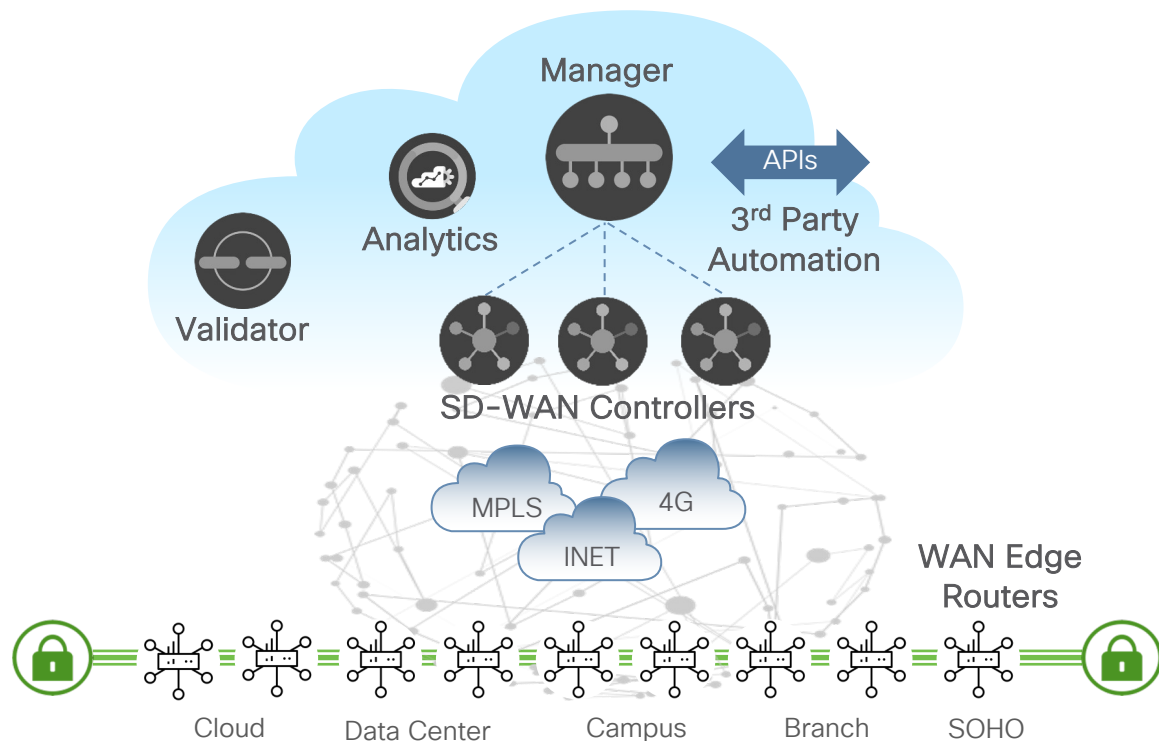
Control Plane



Cisco Catalyst
SD-WAN Controller

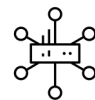
- Facilitates fabric discovery
- Dissimilates control plane information between WAN Edge Routers
- Distributes data plane and app-aware routing policies to the WAN Edge routers
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane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

Cisco Catalyst SD-WAN Solution Elements



Data Plane

Physical/Virtual

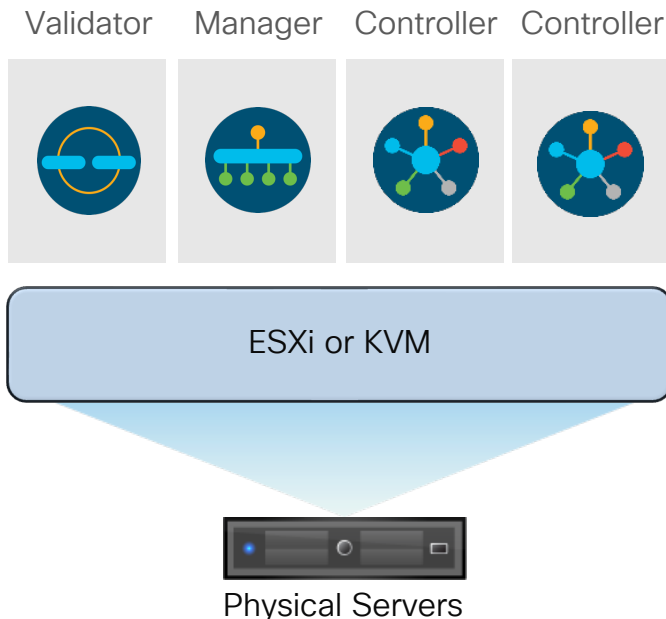


Cisco SD-WAN
WAN Edge

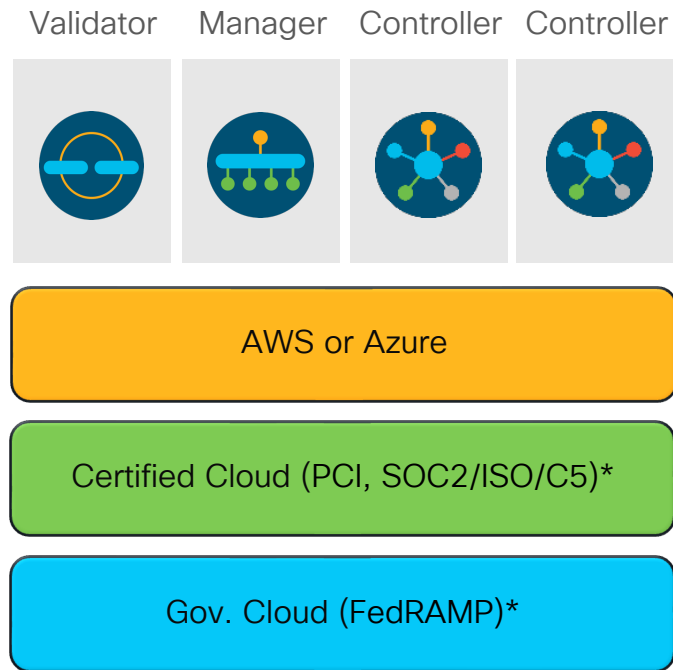
- WAN edge router
- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, and EIGRP
- Support 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



Demo

CISCO *Live!*

SD-WAN Features

Significance of TLOC Color

Color is an abstraction used to identify individual WAN transport

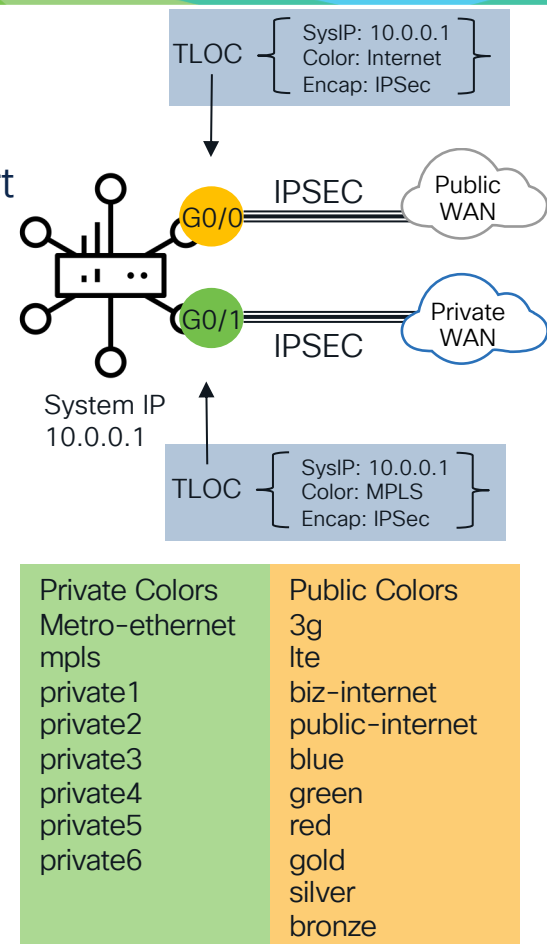
Colors are KEYWORDS not just LABELS

Policy is written based on these

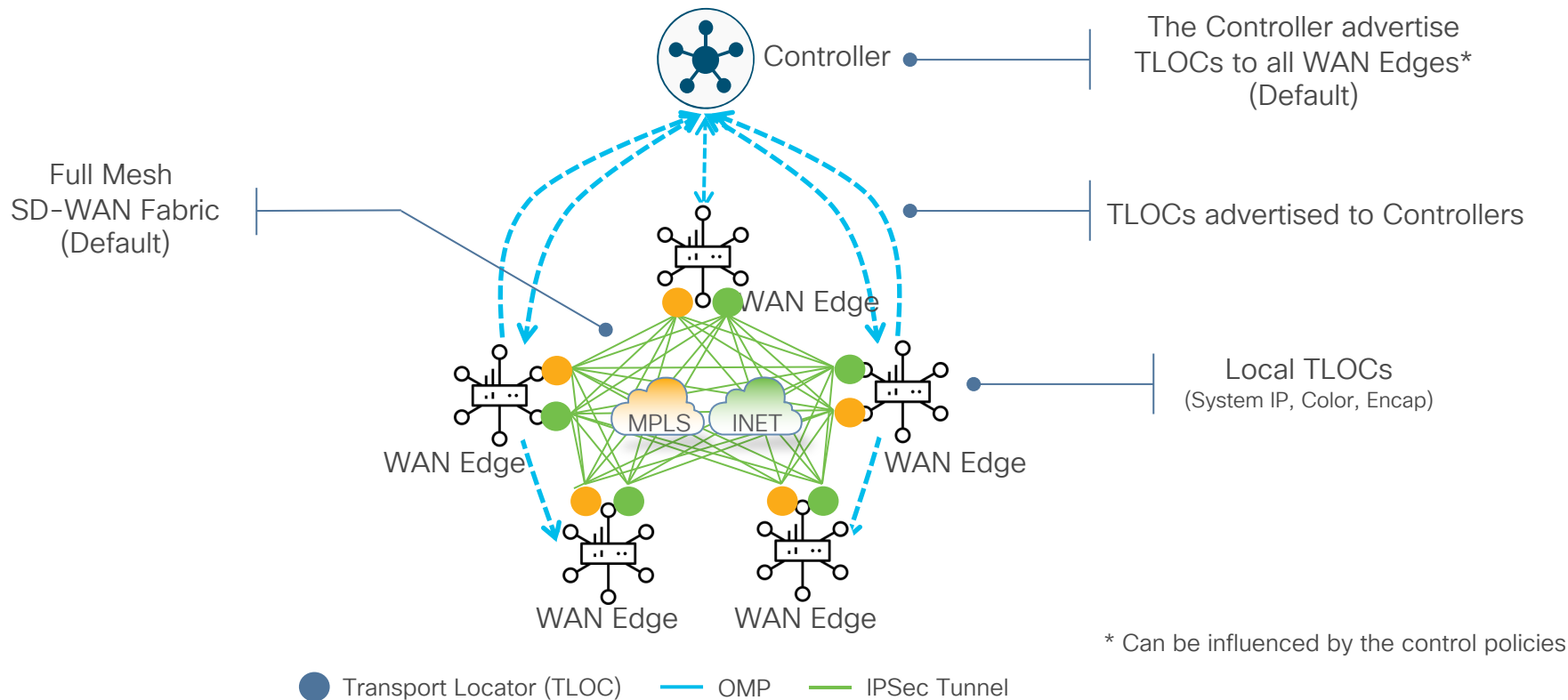
TLOC maps to a physical WAN interfaces

“Color” dictates the use of private-ip vs public-ip (dest)
for Tunnel Establishment when there is NAT present

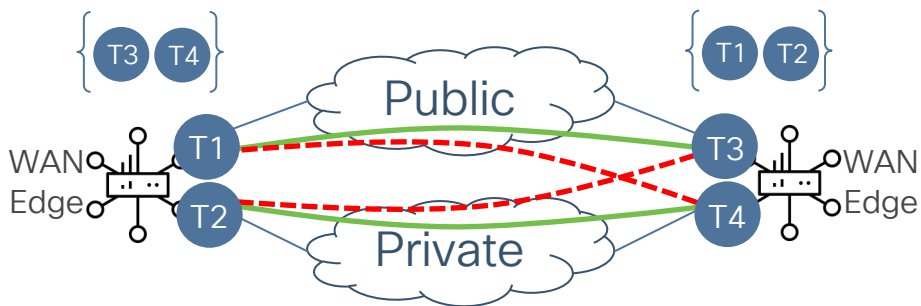
- Example:
 - If two ends have a **private** color: private IP address/port used for DTLS/TLS or IPSec
 - If endpoint has **public** color: Public IP is used for DTLS/TLS or IPSec



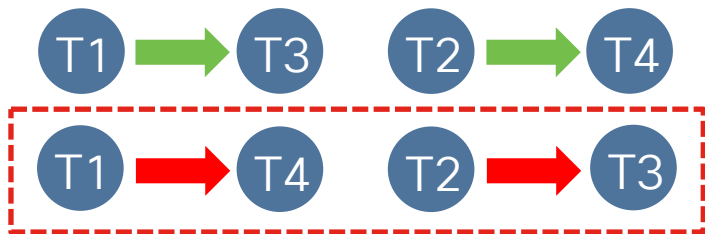
Transport Locators (TLOCs)



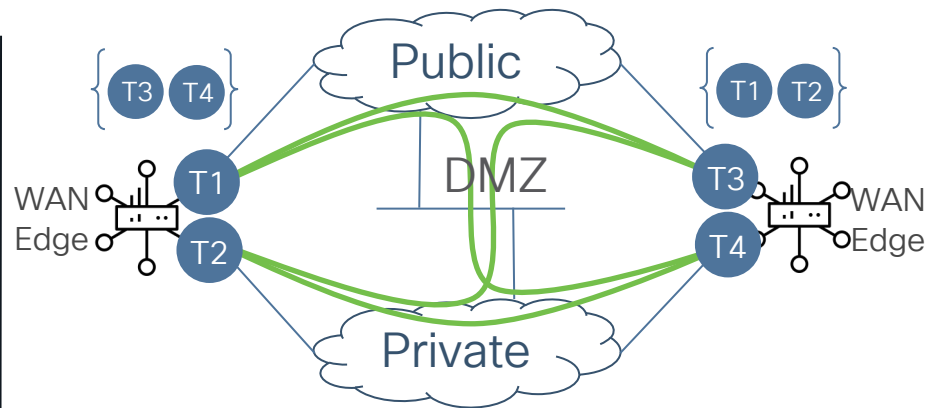
Transport Colors



T1, T3 – Public Color T2, T4 – Private Color



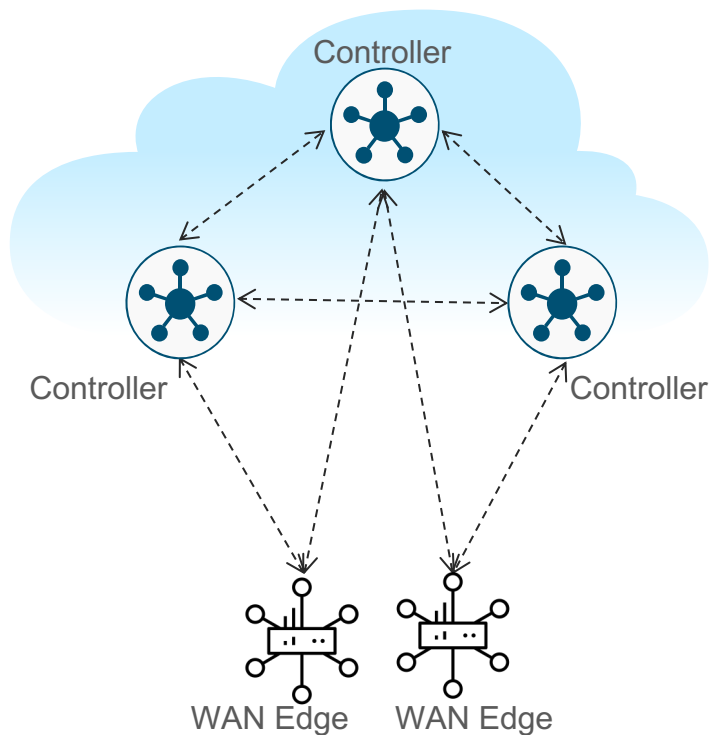
Color restrict will prevent attempt to establish IPsec tunnel to TLOCs with different color



T1, T3 – Public Color T2, T4 – Private Color

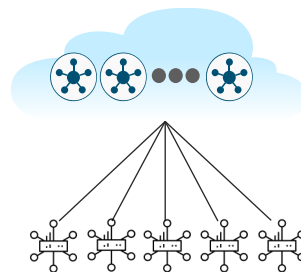


Overlay Management Protocol (OMP)



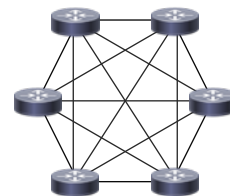
- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and controllers and between the controllers
 - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane complexity and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

SD-WAN



$O(n)$ Control Complexity

Traditional

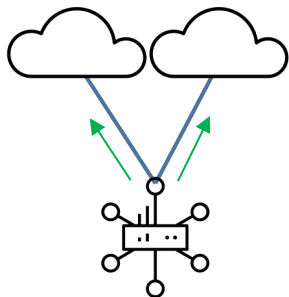


VS

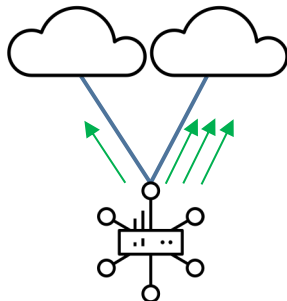
$O(n^2)$ Control Complexity

Fabric Communication

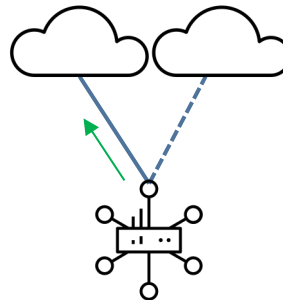
Per-Session Load-sharing
Active/Active



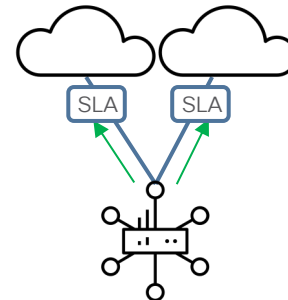
Per-Session Weighted
Active/Active



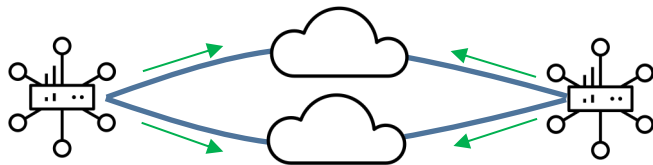
Application Pinning
Active/Standby



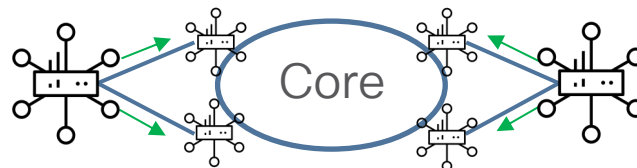
Application Aware Routing
SLA Compliant



Single-hop Fabric



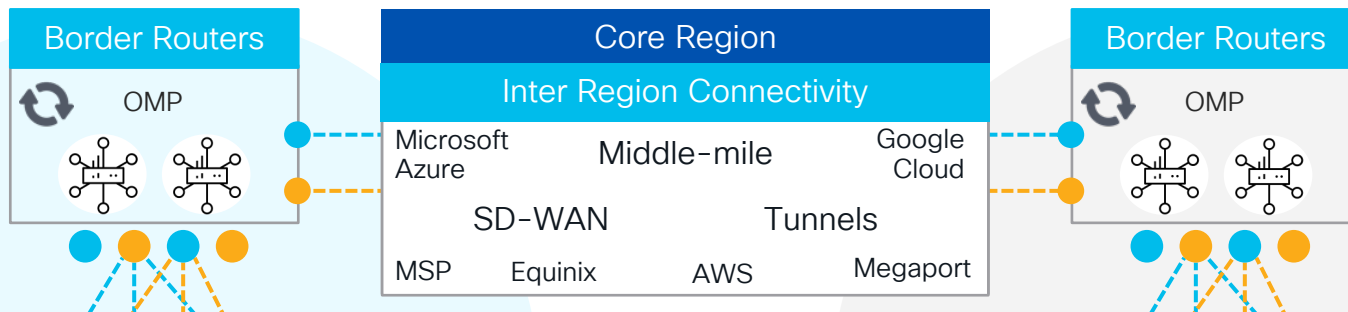
Multi-Region Fabric



The Network, with Multi-Region Fabric

Legend

SD-WAN Tunnels/TLOCs



Learn more OnDemand Sessions

Migration to Multi-Region Fabric - BRKENT-2651

Distributed vSmarts

Edge Routers

SD-WAN CPE

Access Region 1

Edge Routers

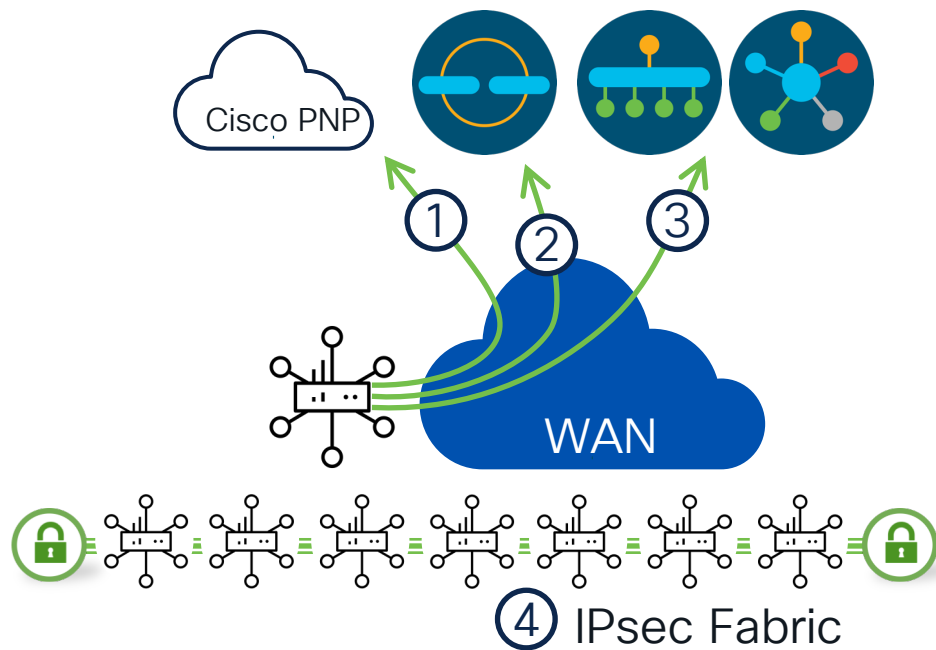
SD-WAN CPE

Access Region 2

...with
Multi-Region Fabric

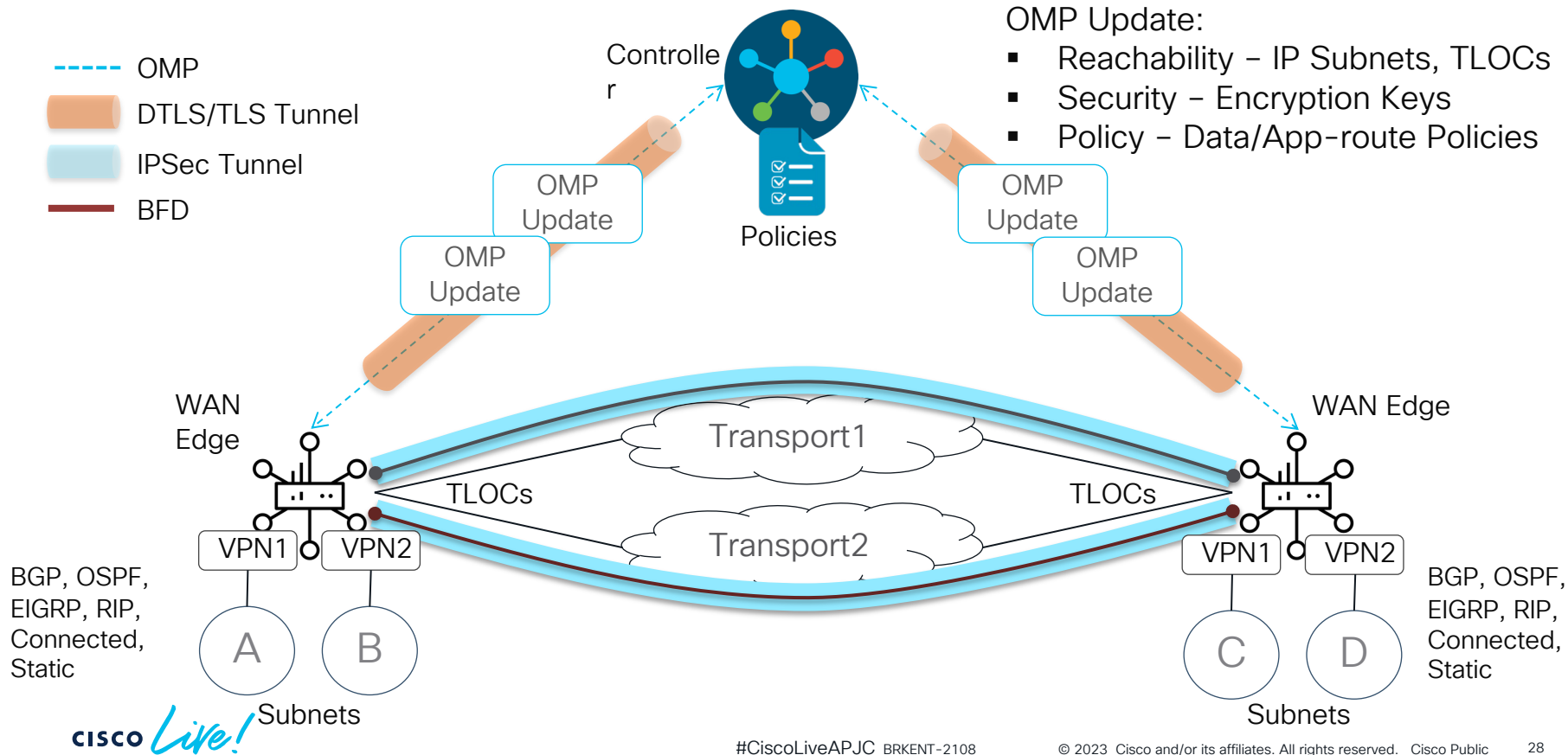
Let's bring it up

Automated, Zero-Touch Onboarding

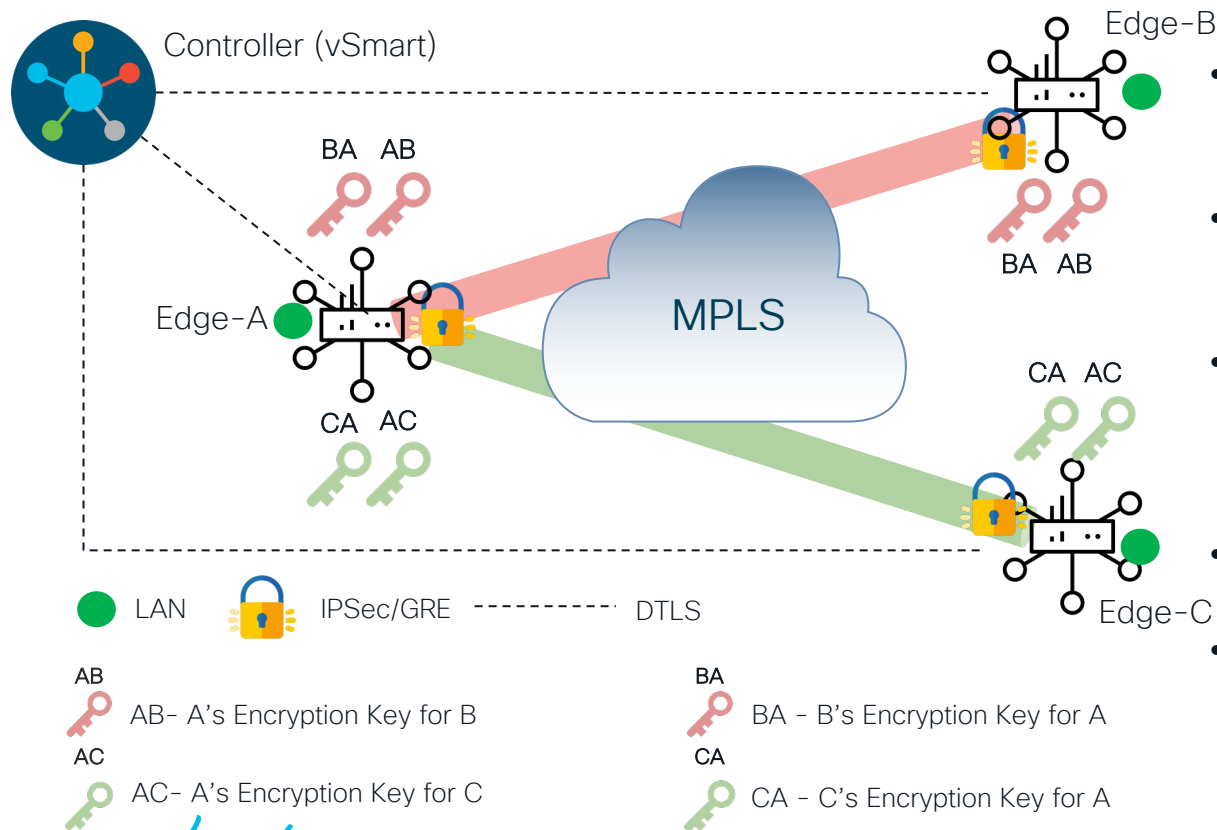


- SD-WAN appliance will onboard itself into the SD-WAN fabric automatically with no administrative intervention.
- Connect the SD-WAN appliance to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.
- If no DHCP service is available then bootstrap file is an option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

Fabric Operation Walk-Through

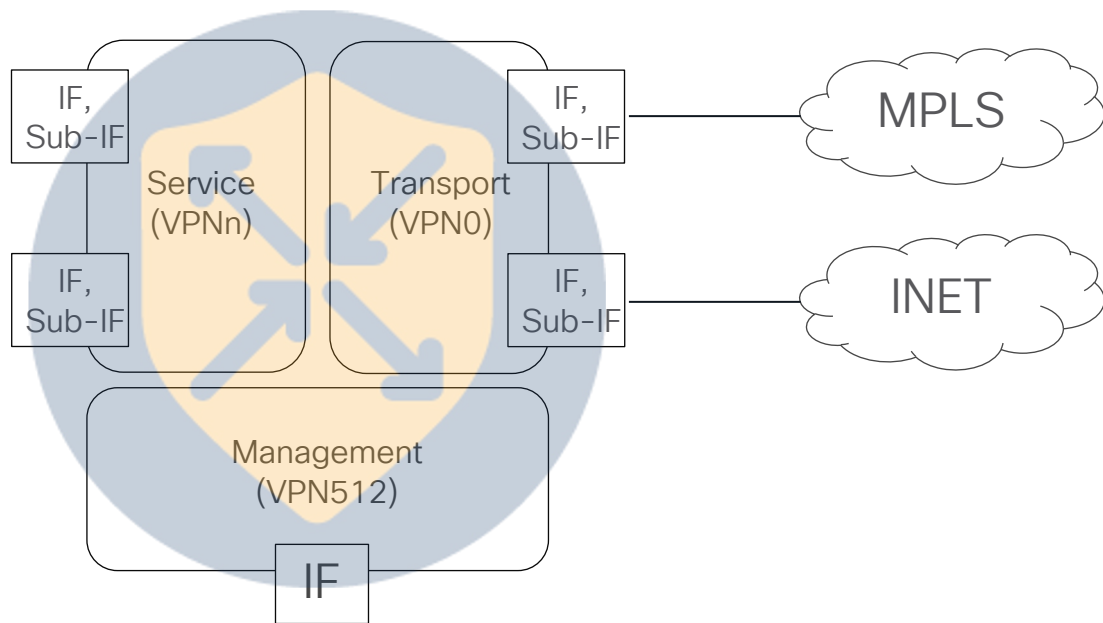


Data Plane Privacy (Pairwise)



- Each WAN edge will create separate session key for each transport and for each peer
- Session keys will be advertised through Controllers 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

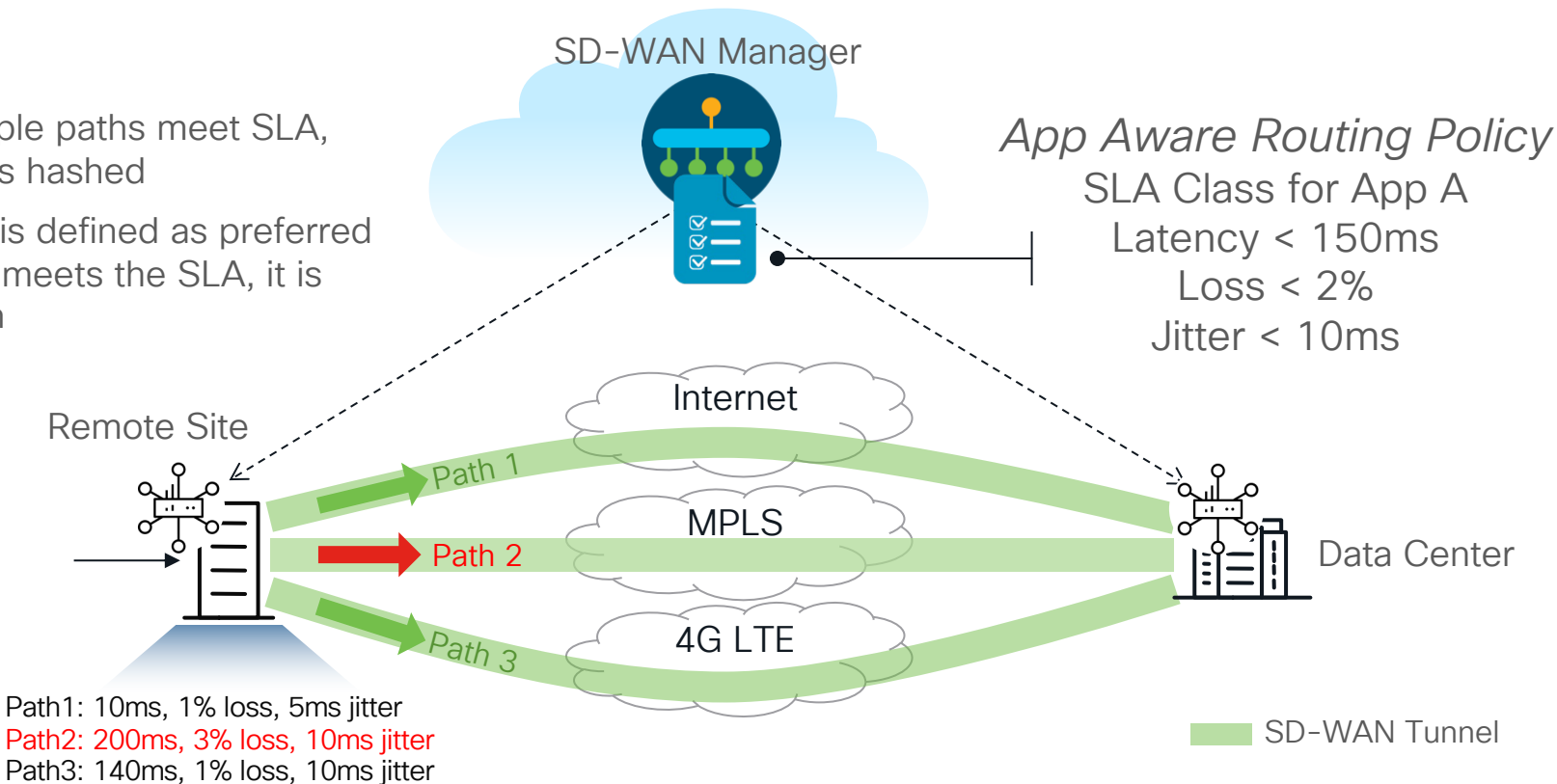
Cisco SD-WAN VPNs (VRFs)



- 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

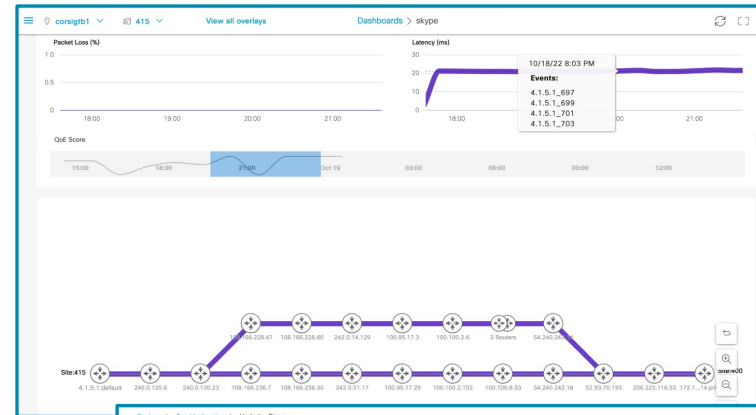
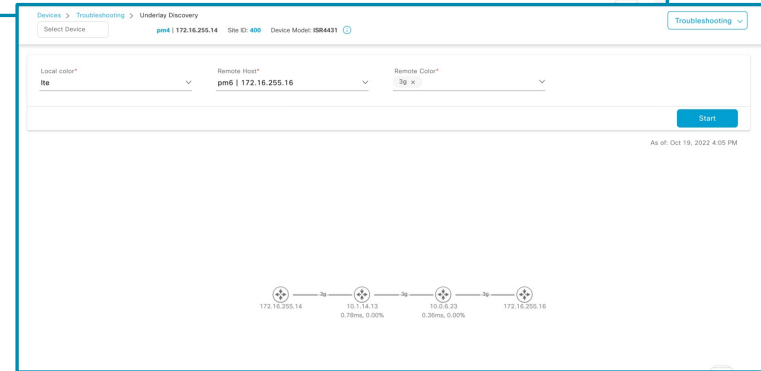
Gain visibility into the exact underlay path* against SD-WAN tunnel
(including hop-by-hop metrics)

* Requires Catalyst Manager 20.10+ and IOS-XE 17.10.1

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



Manager - Virtualised | 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

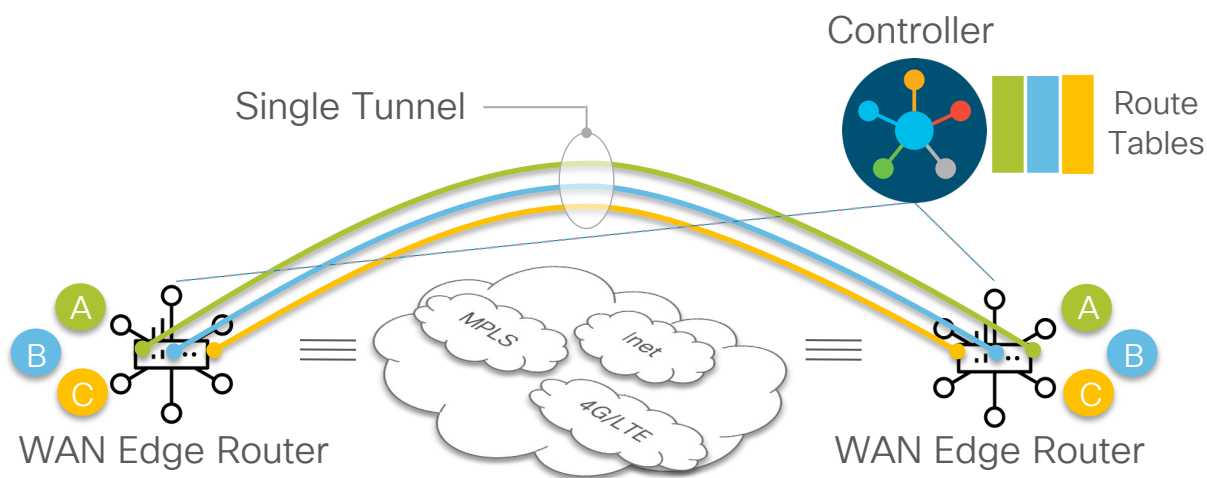
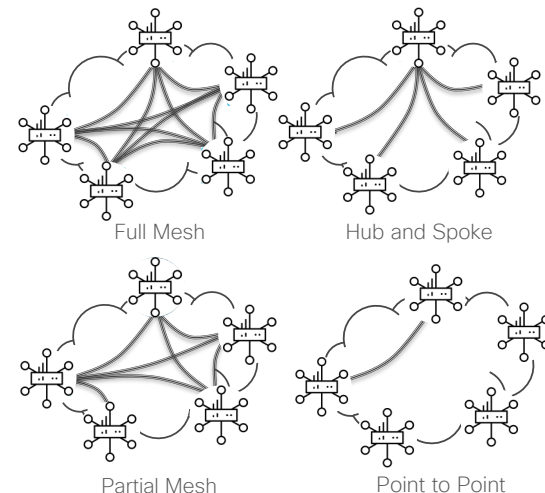


Selective
Acknowledgement

BBR - Bottleneck Bandwidth and Round-trip propagation time

Security features

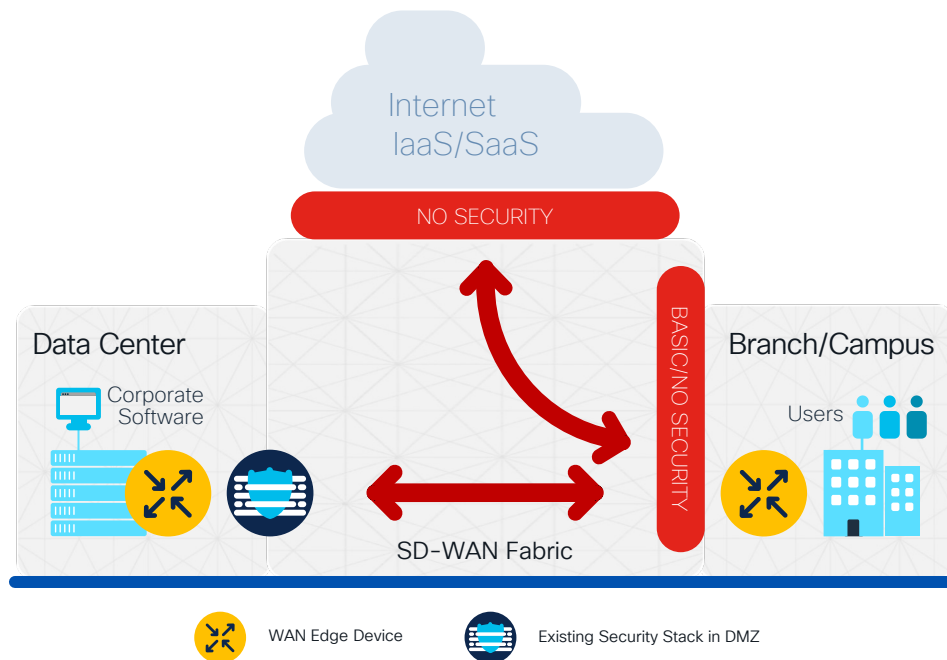
End-to-End Segmentation with Multi-Topology



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

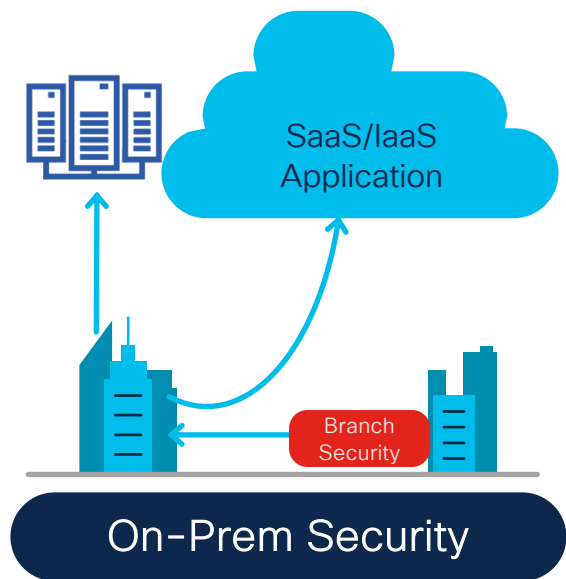
External

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

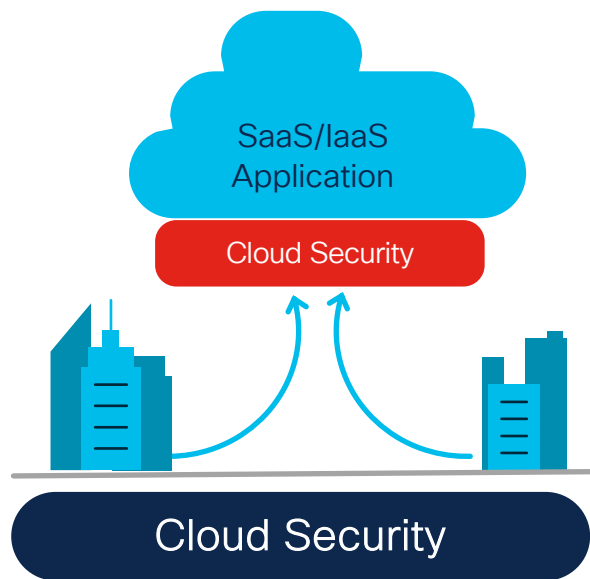
Internal

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

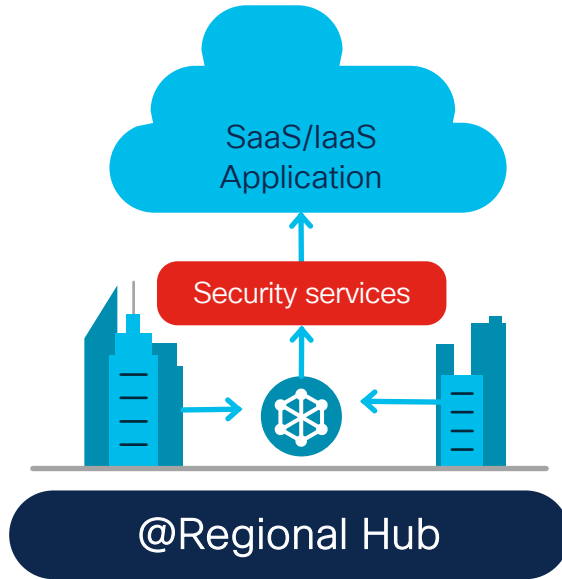
Relevant Security Models. Driving towards SASE



Thick branch with Routing
and Security



Thin branch with
security in the cloud

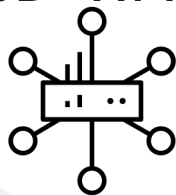


Security Services on a
Regional Hub

Cisco Catalyst SD-WAN – Security & SASE Solution

Consistent across on-prem and cloud

Cisco
SD-WAN



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)

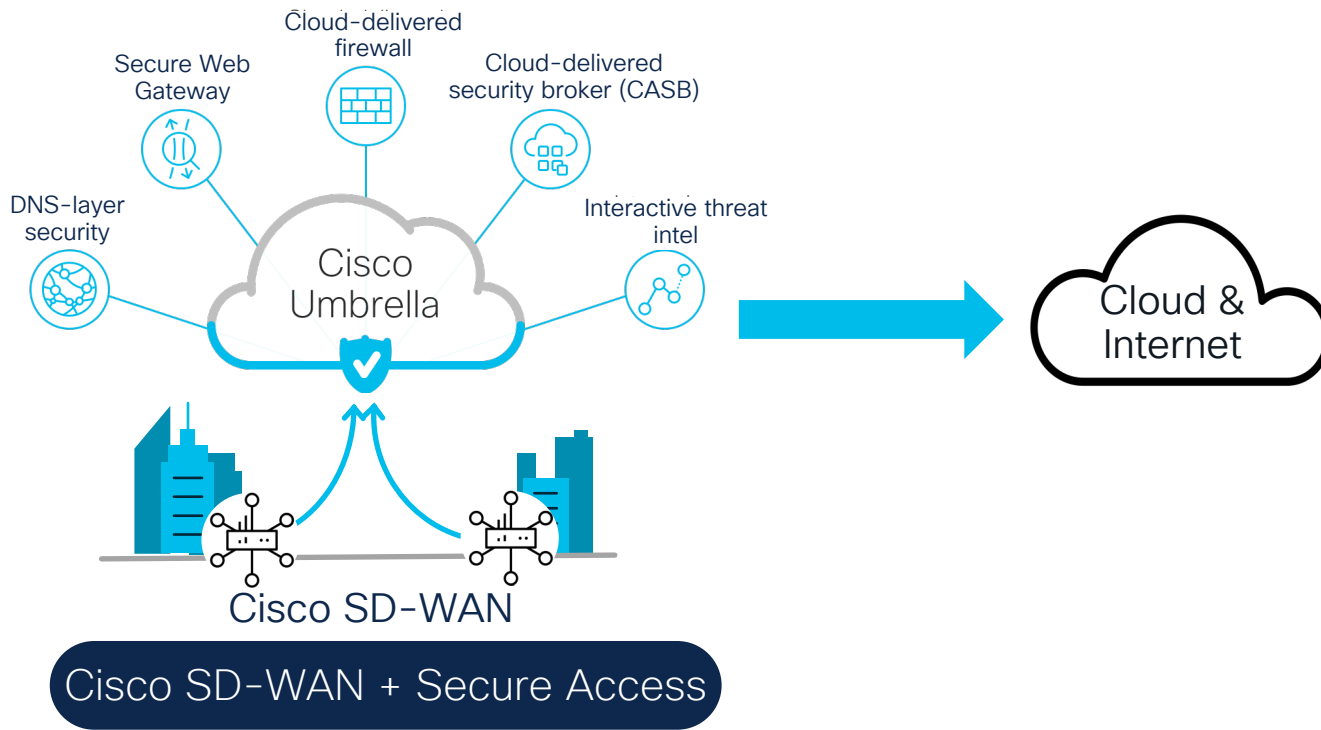
SSL Proxy

Detect Threats in Encrypted Traffic

Umbrella Cloud Security

DNS Security/Cloud FW with Cisco Umbrella

Transitioning towards a Cloud security model

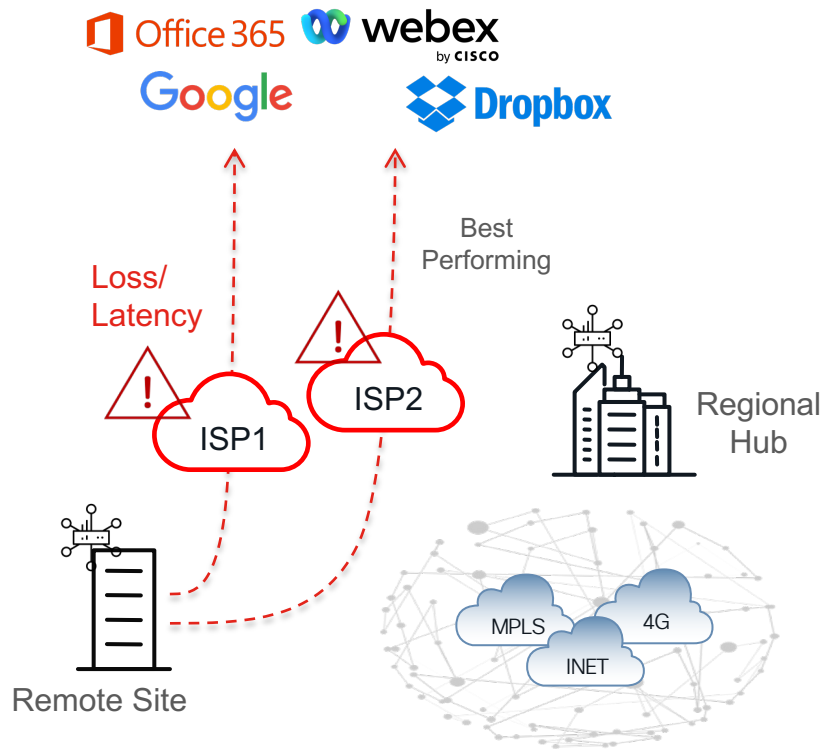


Cloud OnRamp for SaaS

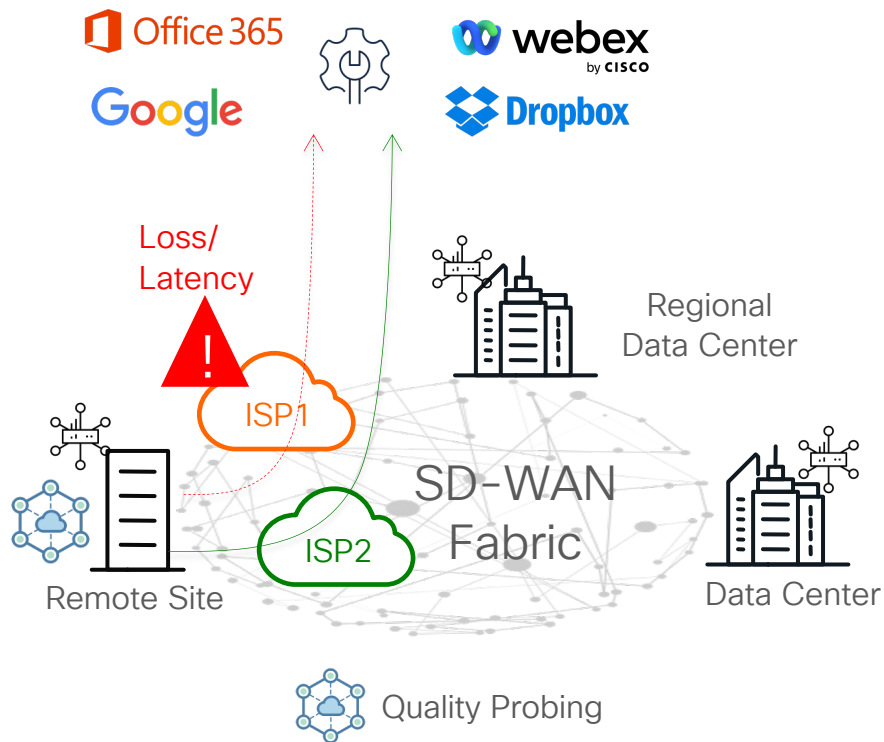


SaaS Optimization Challenges

- 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 ?

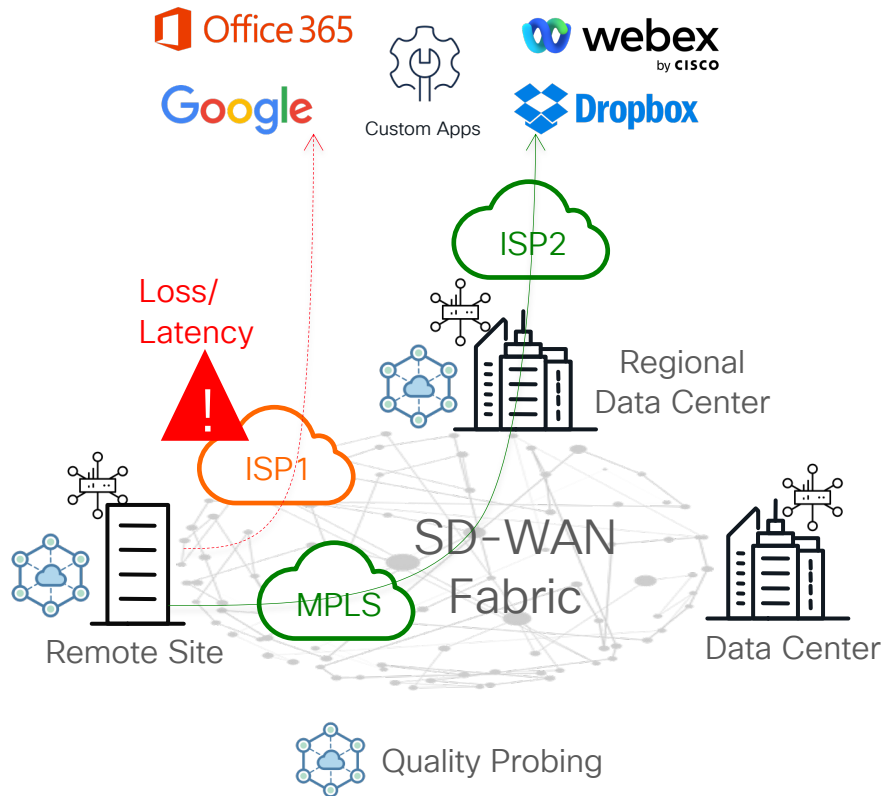


Cloud onRamp for SaaS – Internet DIA



- 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

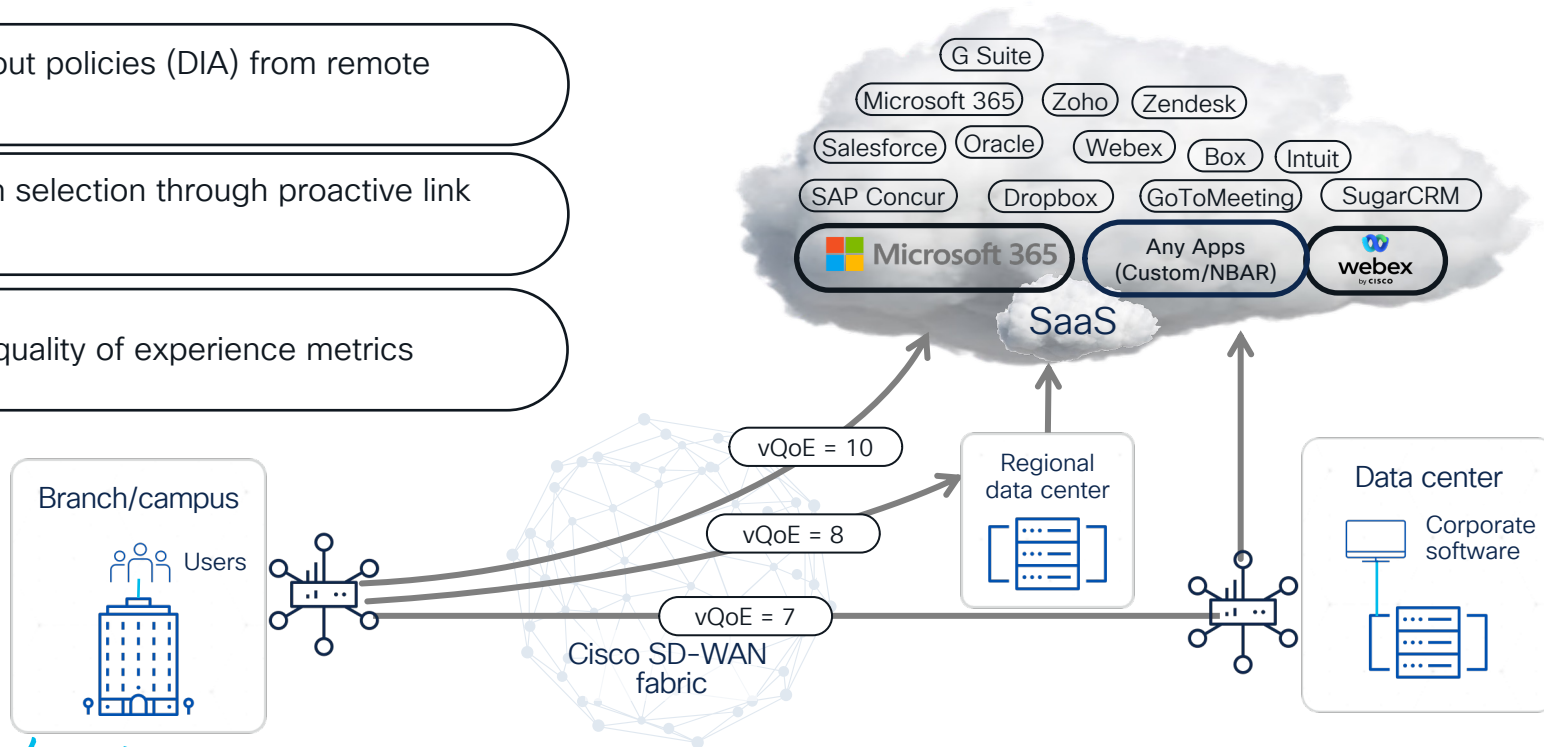
Cloud OnRamp for SaaS

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



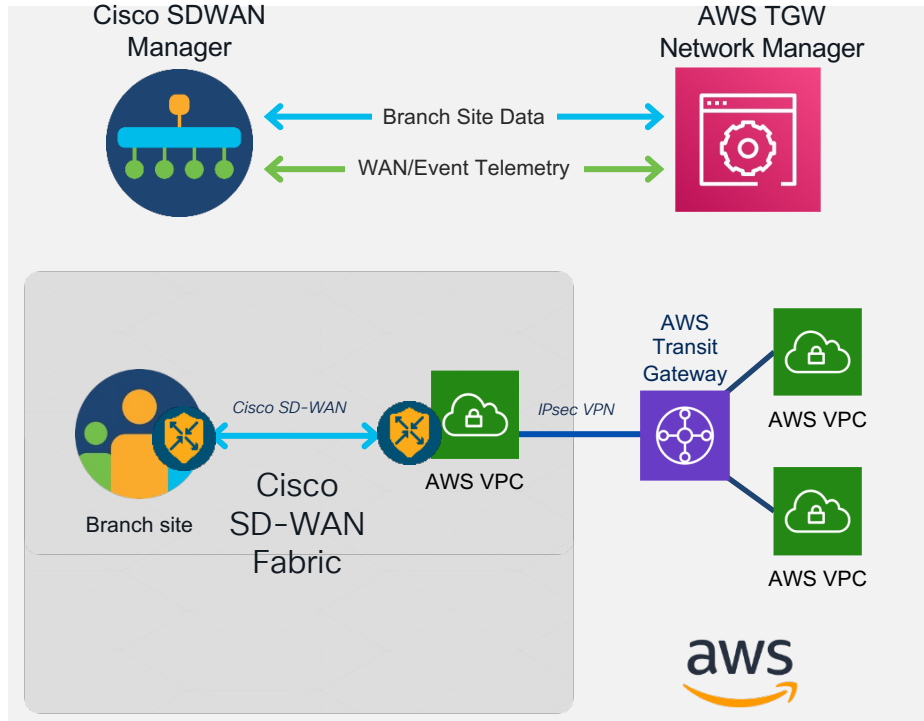
Cloud OnRamp for MultiCloud



Extending SD-WAN into Public Cloud (AWS as example)

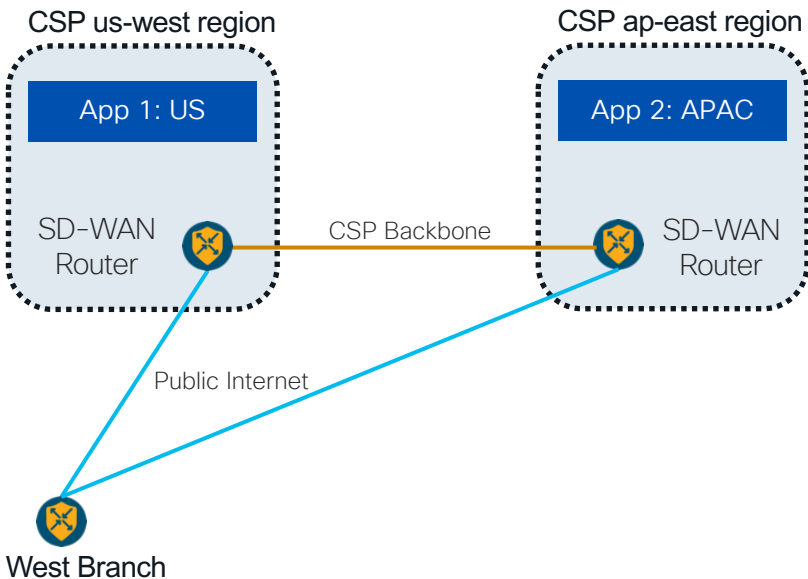
Benefits

- Automated provisioning of SD-WAN Transit VPC and TGW, route exchange for site to cloud and site to site traffic over AWS backbone
- Full Visibility into inter-regional transit traffic and telemetry with TGW Network Manager
- Consistent Policy and Segmentation across branch and cloud for enterprise class security

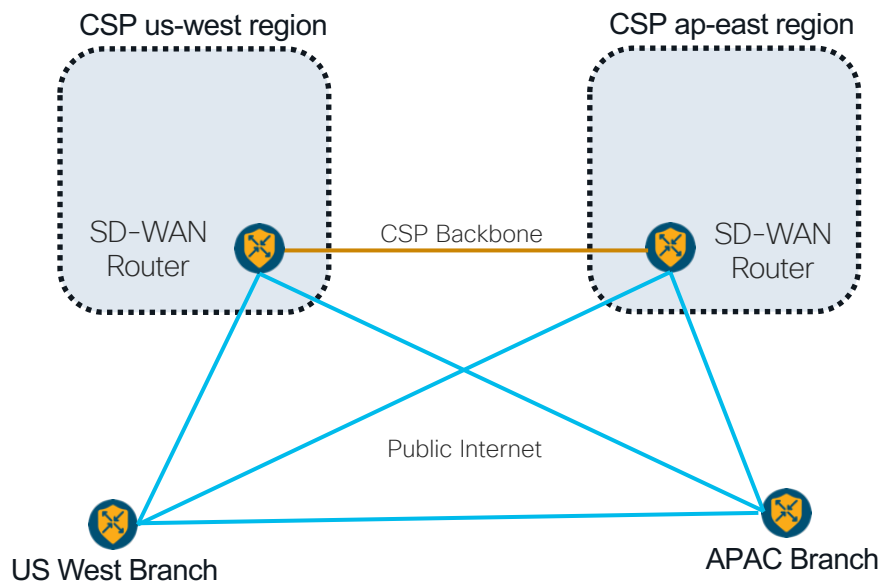


Two Major Use Cases: site-to-site and site-to-cloud

Site-to-cloud: branch to cloud-based App



Site-to-site: US branch to APAC branch



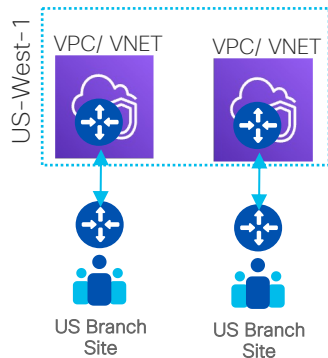
Common questions:

- Cloud design
- Performance and auto scale
- Security: Integration with virtual firewall and SIG
- Automation: Cloud OnRamp and custom (Terraform, Ansible)

High Level Design Options

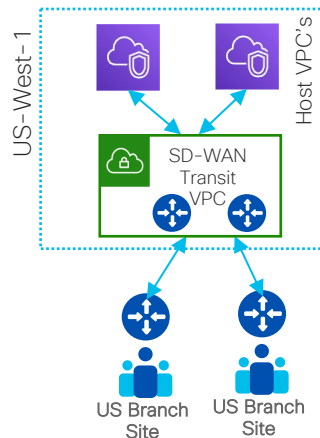
CSP-generic, AWS used as example

Cloud Gateway



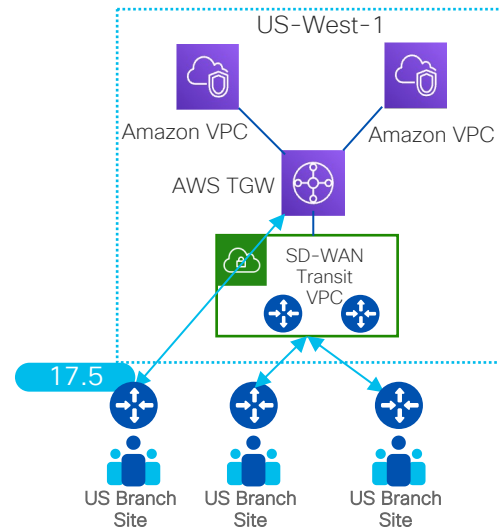
- SD-WAN Router in every VPC/VNET.
- Not scalable, but okay for one VPC.
- No built-in automation in Cloud onRamp, custom automation possible

Cloud OnRamp for IaaS



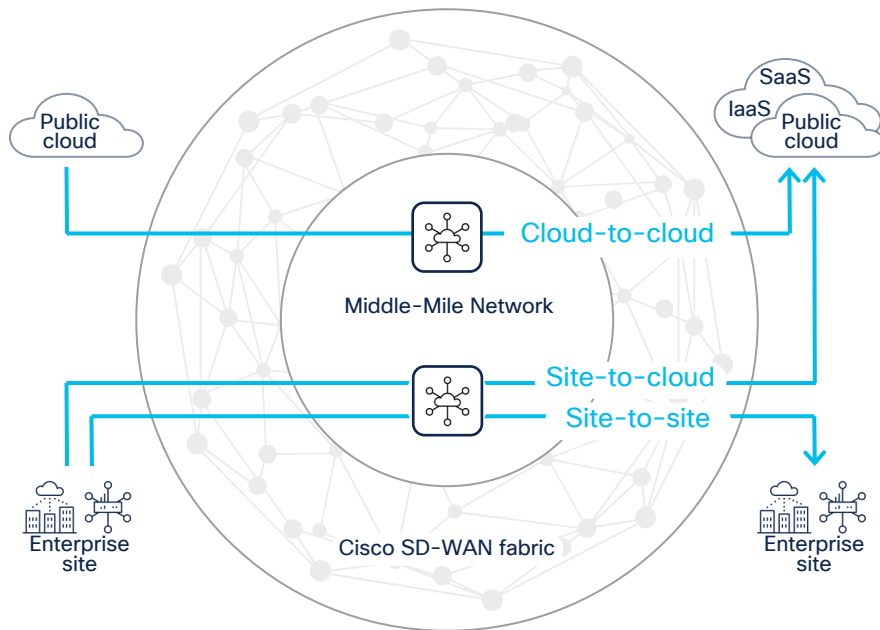
- Transit VPC with SD-WAN routers.
- IPSec to host VPCs / VNETS via VGW
- Cloud networks learnt via BGP, redistributed into OMP.
- AWS and Azure automation on vManage known as Cloud OnRamp for IaaS

Cloud OnRamp for Multicloud



- AWS TGW or Azure vWAN is used
- IPSec to AWS TGW, BGP on top of IPSec
- Cloud networks learnt via BGP, redistributed into OMP.
- AWS (17.3), Azure (17.4) and Google Cloud (17.5) automation on vManage known as Cloud onRamp for Multicloud
- Branch Connect - Traditional IPsec to AWS TGW (17.5)
- Cloud WAN coming in 2022

Cisco SD-WAN Middle-Mile Optimization



Flexibility

All or selective traffic sent based on type or app



Reliability

Reliable, high-speed connectivity between sites



Security

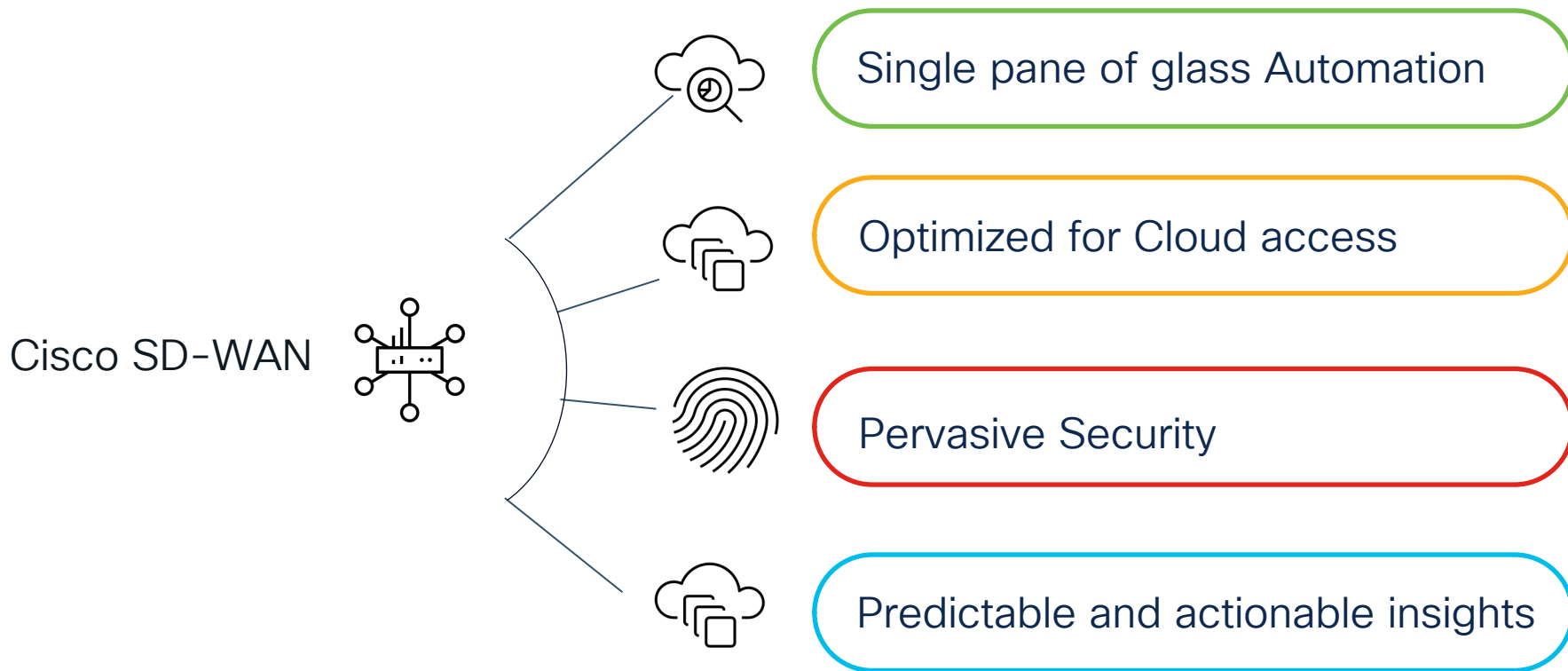
End-to-end encryption over middle mile global backbone



On-demand

Automated connectivity via vManage central dashboard

Key Takeaways



SD-WAN – This is it.



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a spectrum of colors (red, orange, yellow, green, blue, purple) arranged in a radial, sunburst-like pattern. The colors transition from warm tones on the left to cooler tones on the right, with a bright white center. The overall effect is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLiveAPJC