

CISCO *Live!*

Let's go



The bridge to possible

Cisco Catalyst SD-WAN: Start Here

Gizem Kirmizisac Gulsen
Systems Engineer, SD-WAN/SASE

CISCO *Live!*

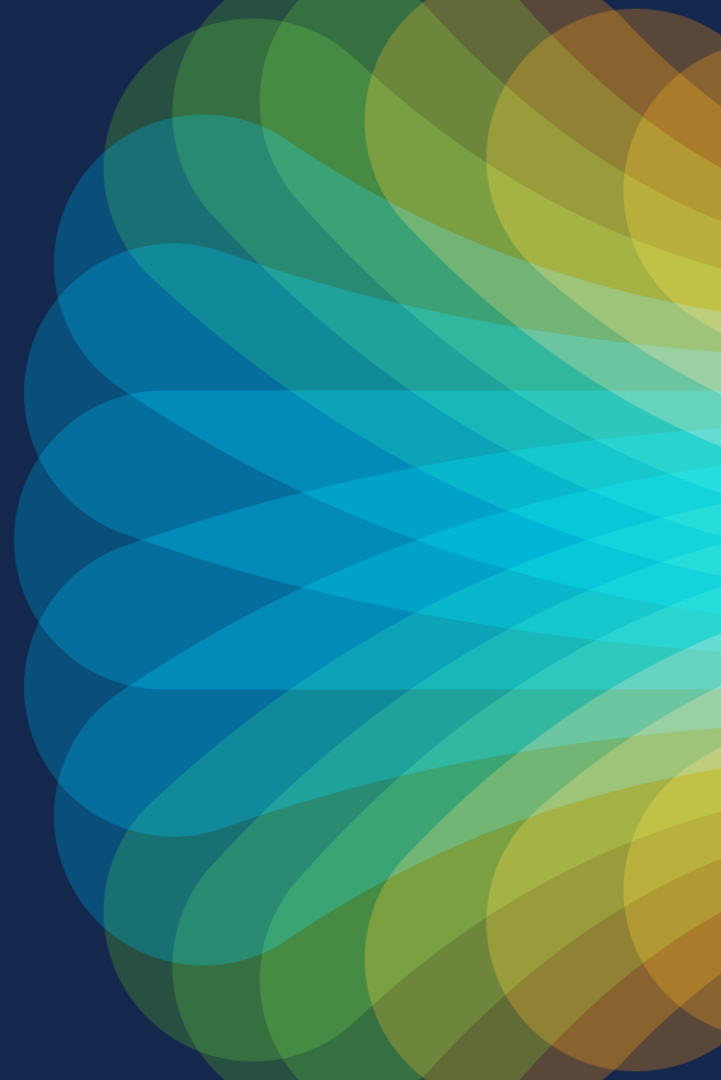
BRKENT-2108

Agenda

CISCO *Live!*

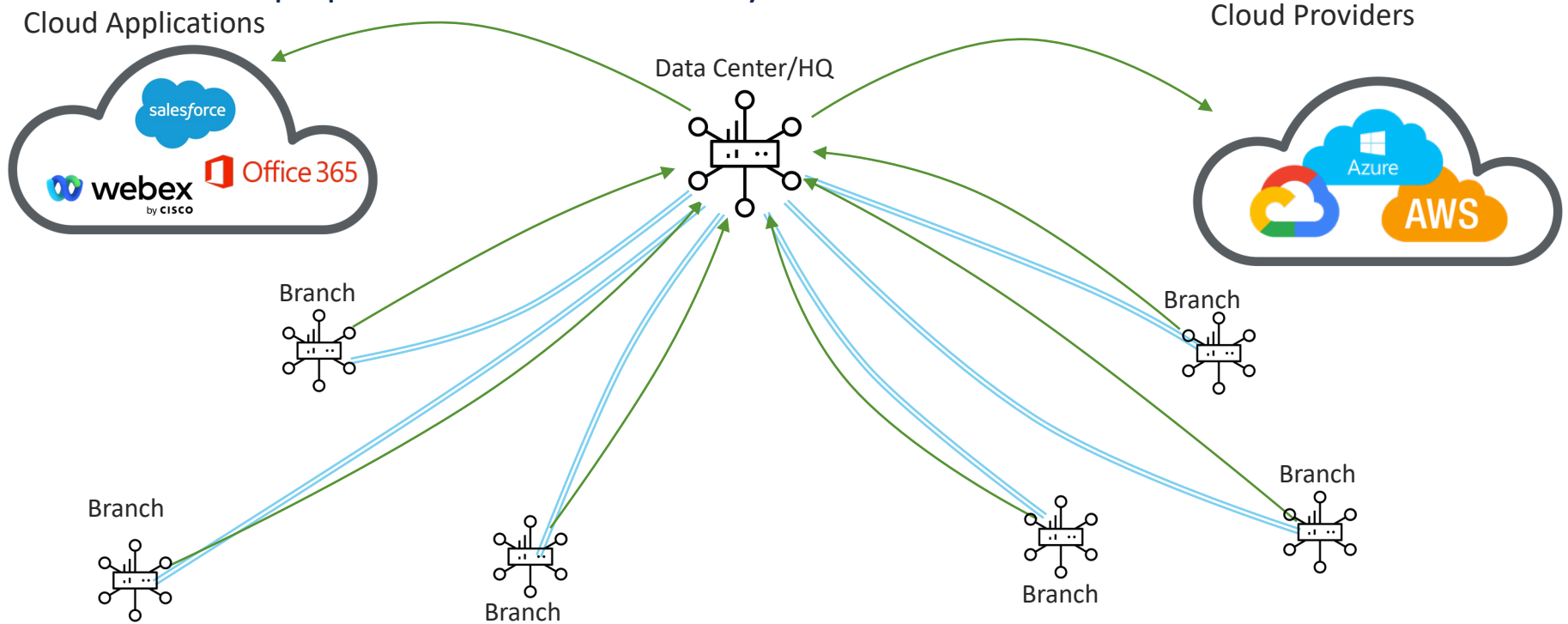
- Why SD-WAN
 - Where are we coming from
- Solution Architecture
 - What is it, how does it all come together?
- Software Features
 - Let's scratch the surface
- Learn More
 - Where to go and when

Why SD-WAN?



The Hardware Based WAN of Yesterday

Doesn't Keep up with the Needs of Today



Cisco SD-WAN: Software Approach

Cloud Applications

Cloud Providers



Cisco Catalyst SD-WAN

Flexible and scalable architecture for network transformation

Any Deployment



On-premise | Cloud | Multitenant | Multiregion
Automation | Network Insights | Machine Learning | AI
Open | Programmable | Scalable

Any Service



Multicloud optimization



Multilayer Security



Analytics



Voice



Multi-Domain IBN policy

Any Transport



Satellite



Internet



MPLS

5G

5G/LTE



SDCI

Any Location



Branch



Colocation

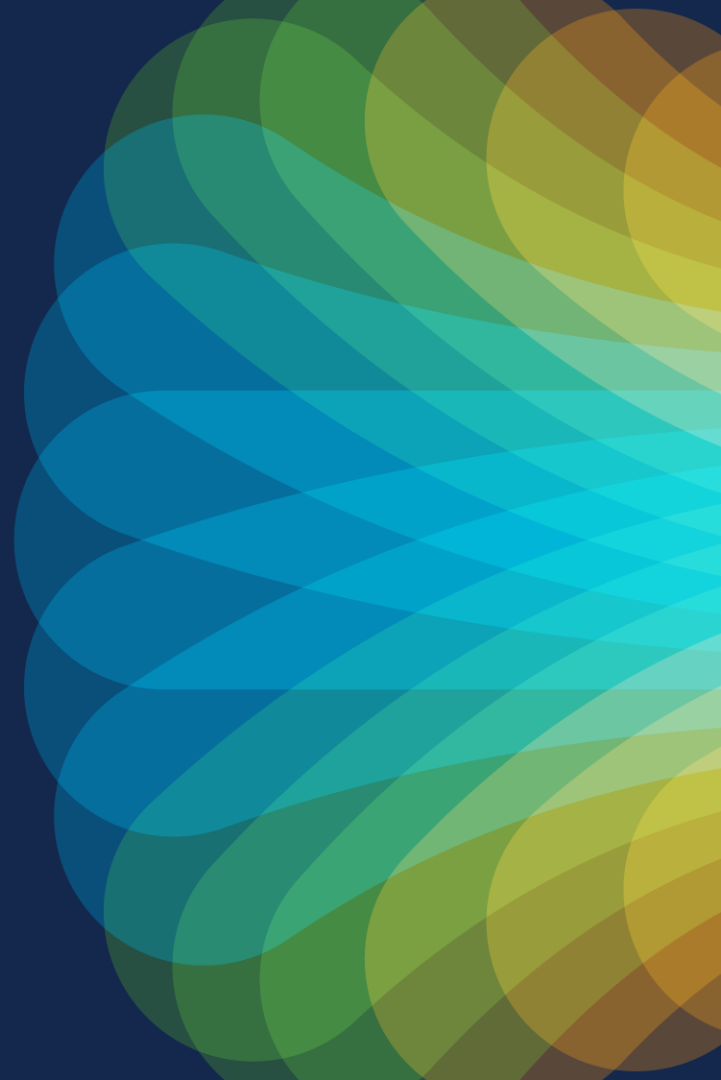


Cloud



Remote work

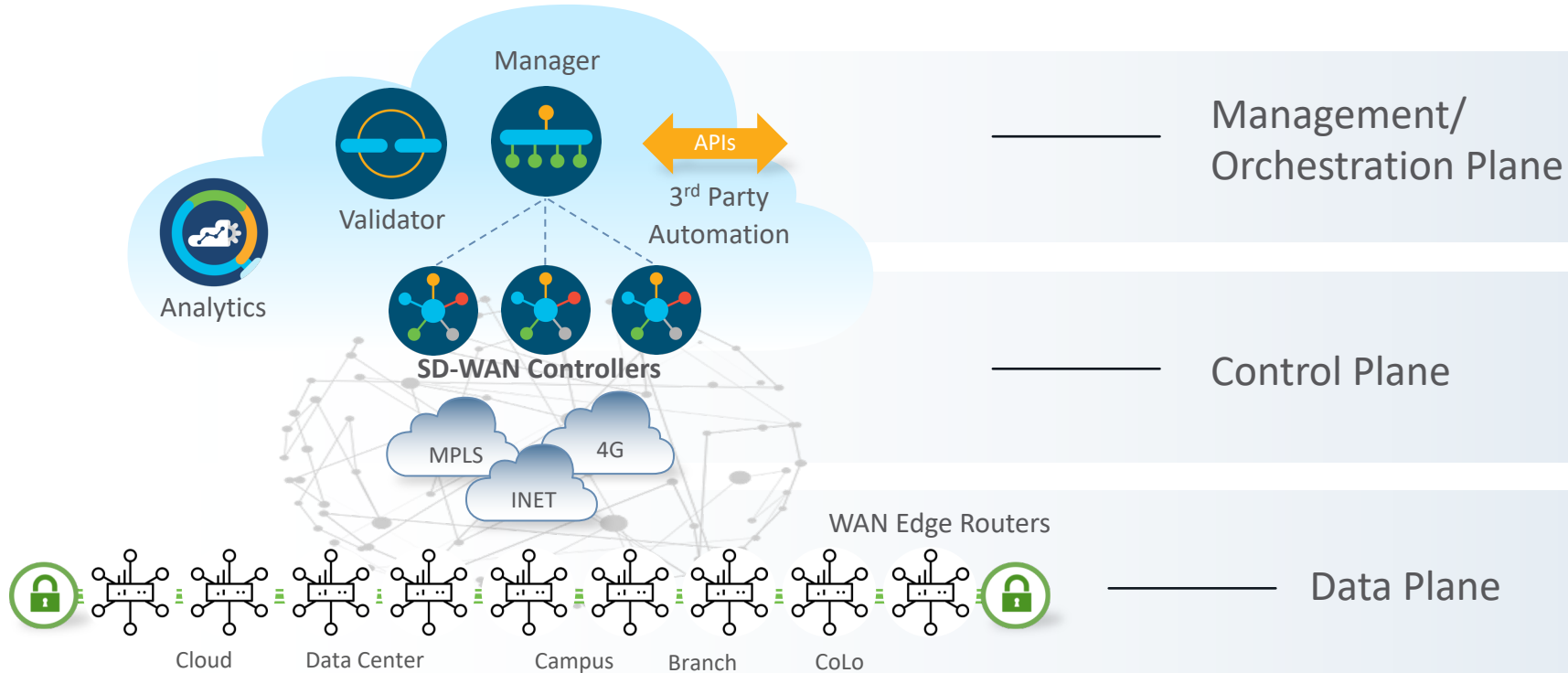
Solution Architecture



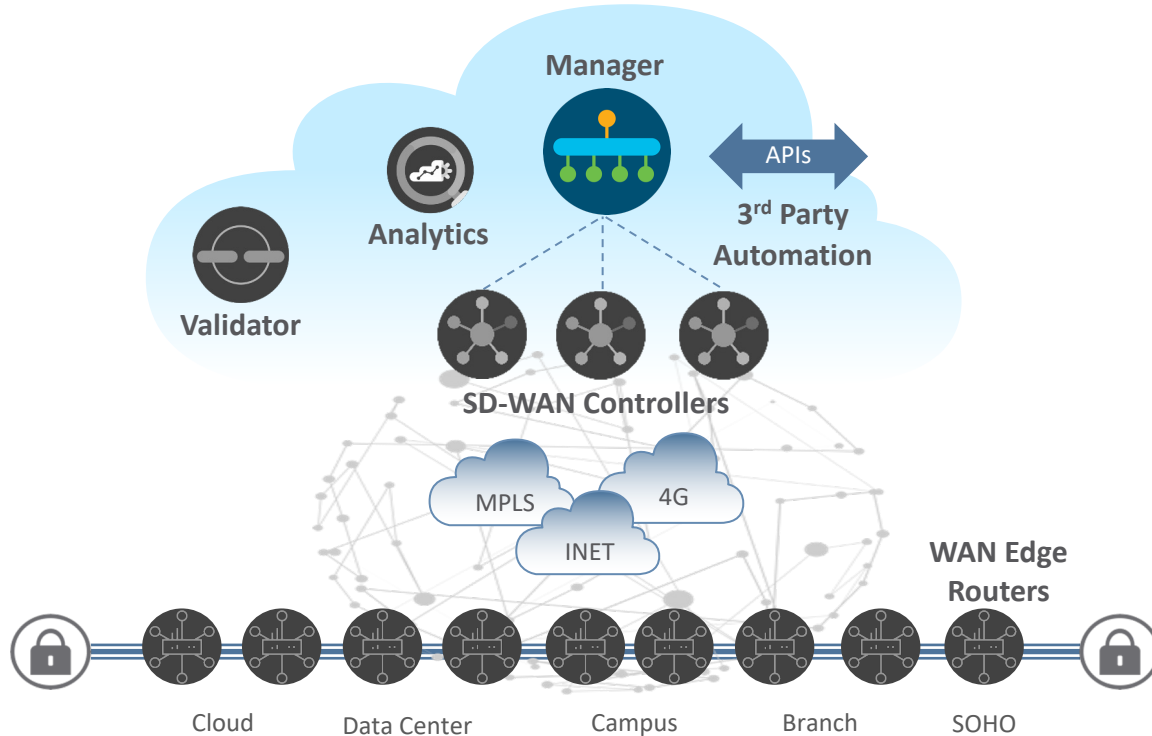
New Naming: Cisco Catalyst SD-WAN

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



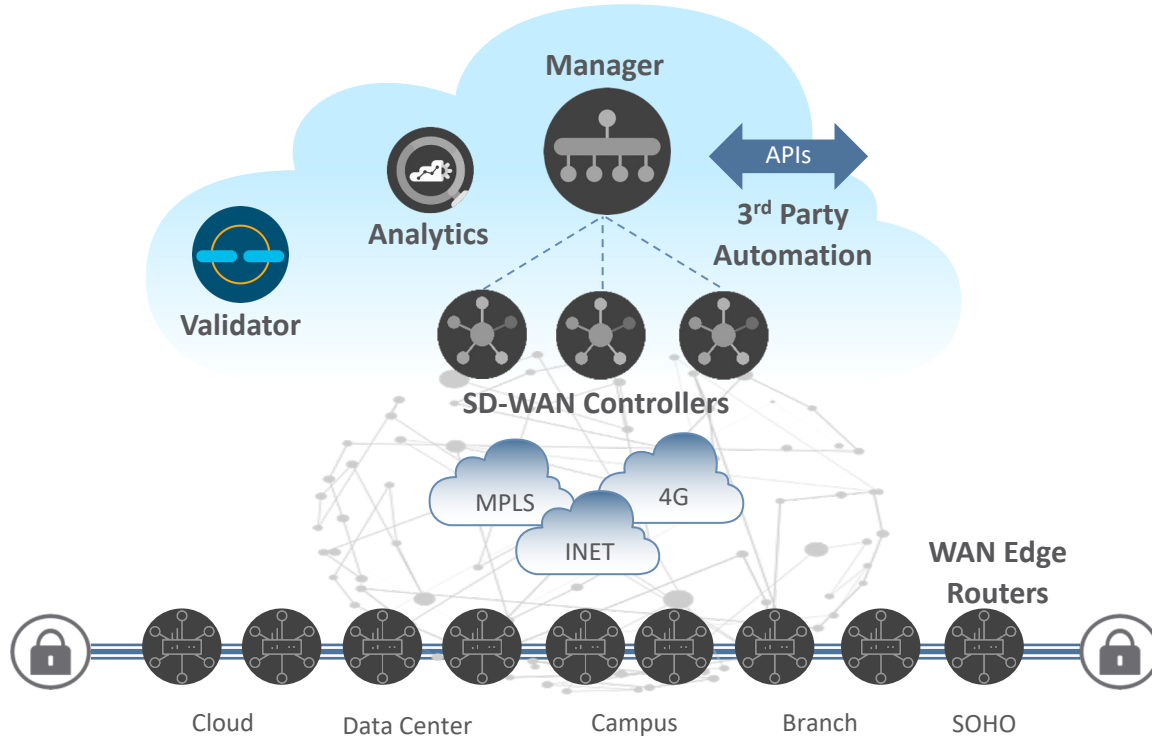
Management Plane



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



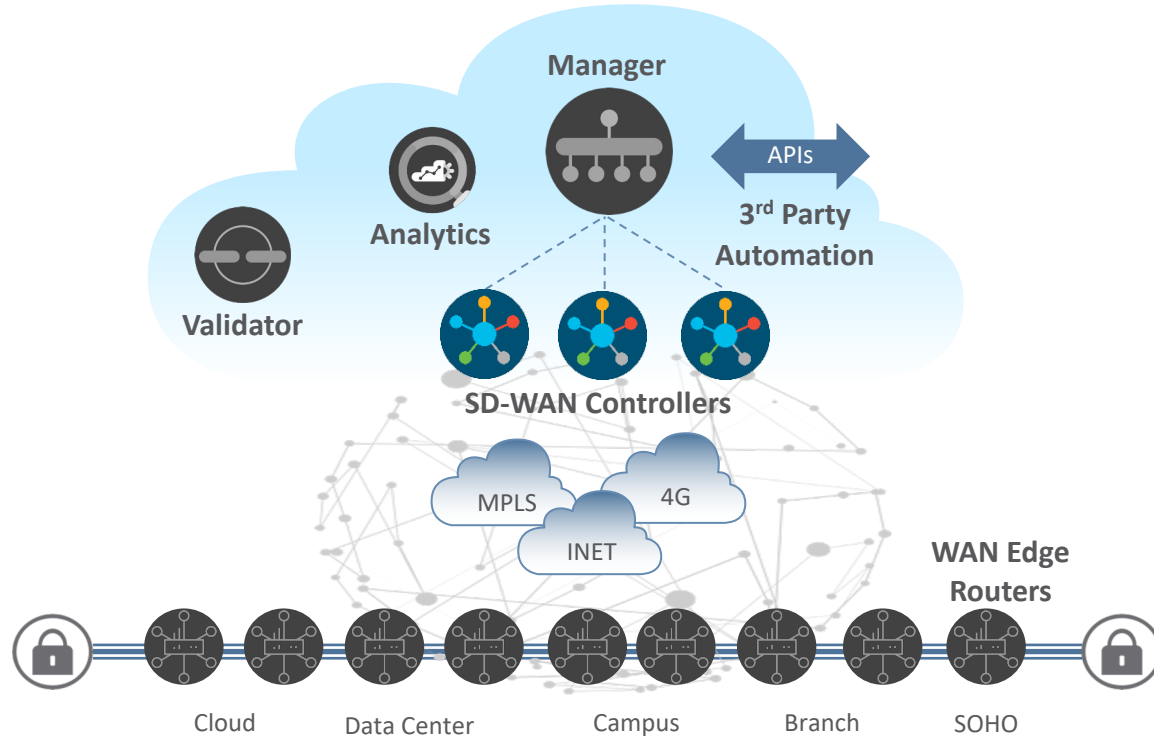
Orchestration Plane



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



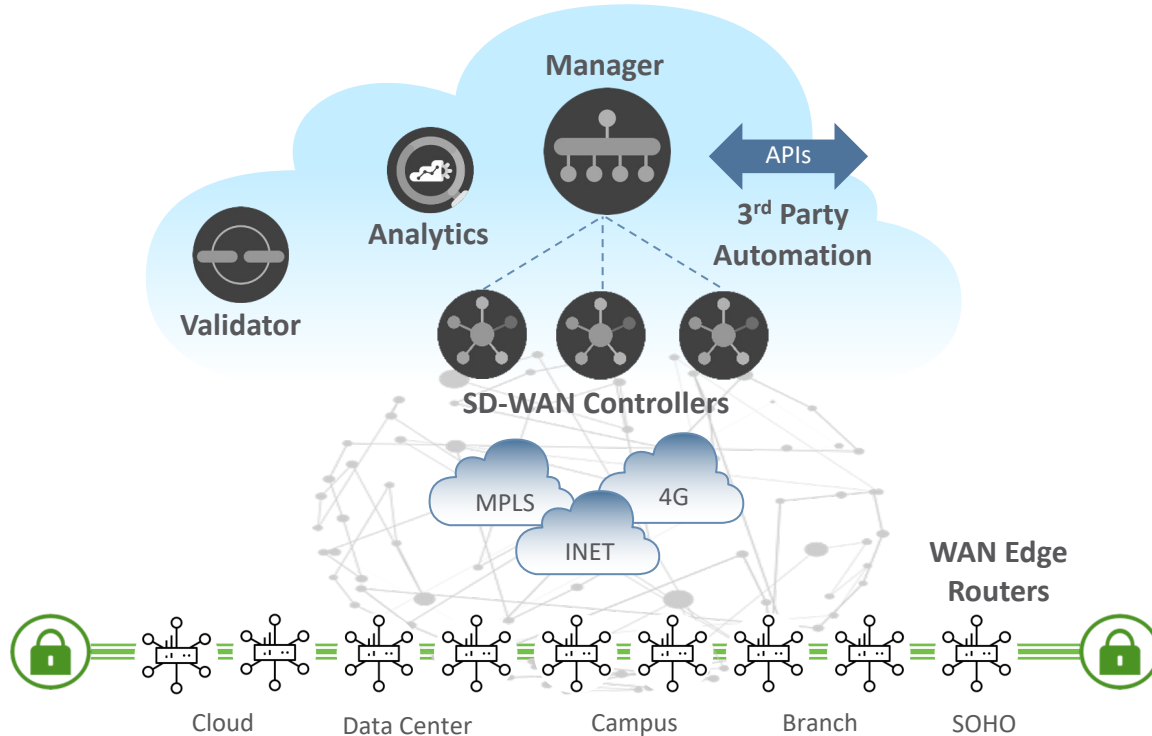
Control Plane



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

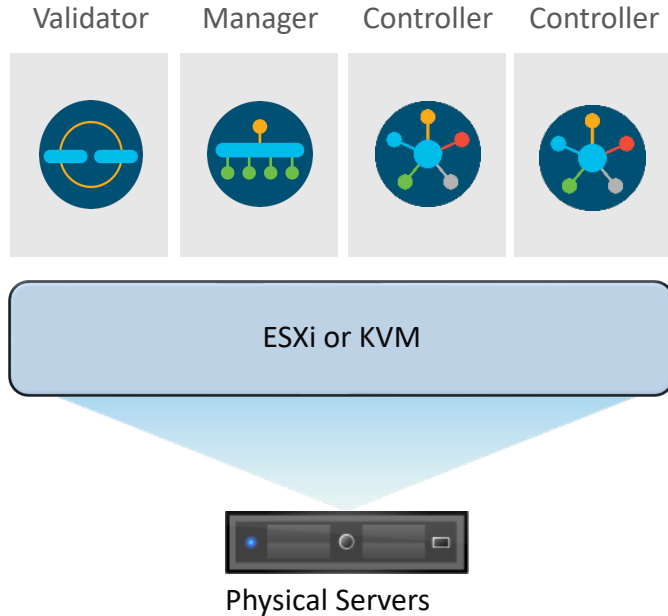


Cisco SD-WAN
WAN Edge

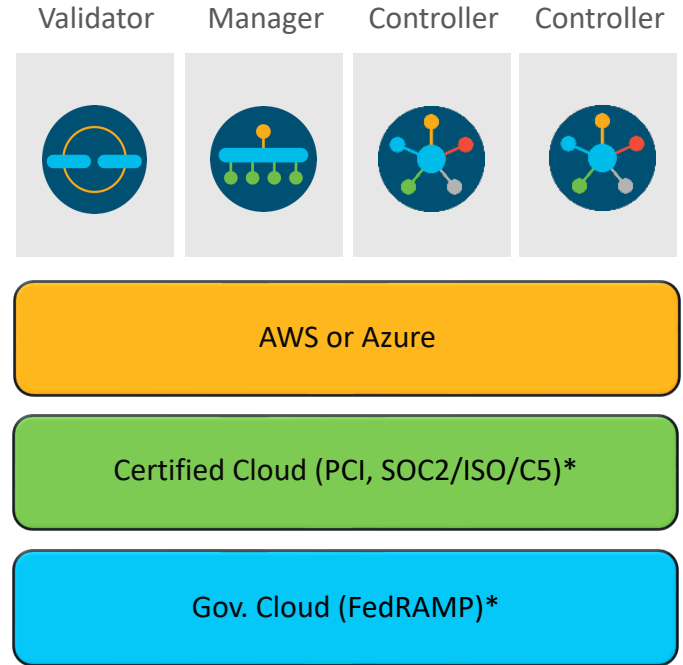
- WAN edge router
- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, and EIGRP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

Controller Deployment Methodology

On-Premise



Cisco or MSP/Customer Hosted



*Only Cisco hosted

SD-WAN platforms for any deployment

Virtual



CSP 5000



ENCS 5000

SD-WAN and routing devices

Catalyst 8000 Edge platforms family

Cloud



ASR 1000



Catalyst 8000V



Catalyst 8200 uCPE

Branch



ISR 1000



ISR 4000



Catalyst 8200, 8200L



Catalyst 8300

Core



Catalyst 8500, 8500L

Hybrid / Remote



Catalyst Wireless Gateway CG113



Catalyst Cellular Gateway CG418-E, 522-E

Industrial IoT Edge



Catalyst IR1100
Catalyst IR1101



Catalyst IR1800

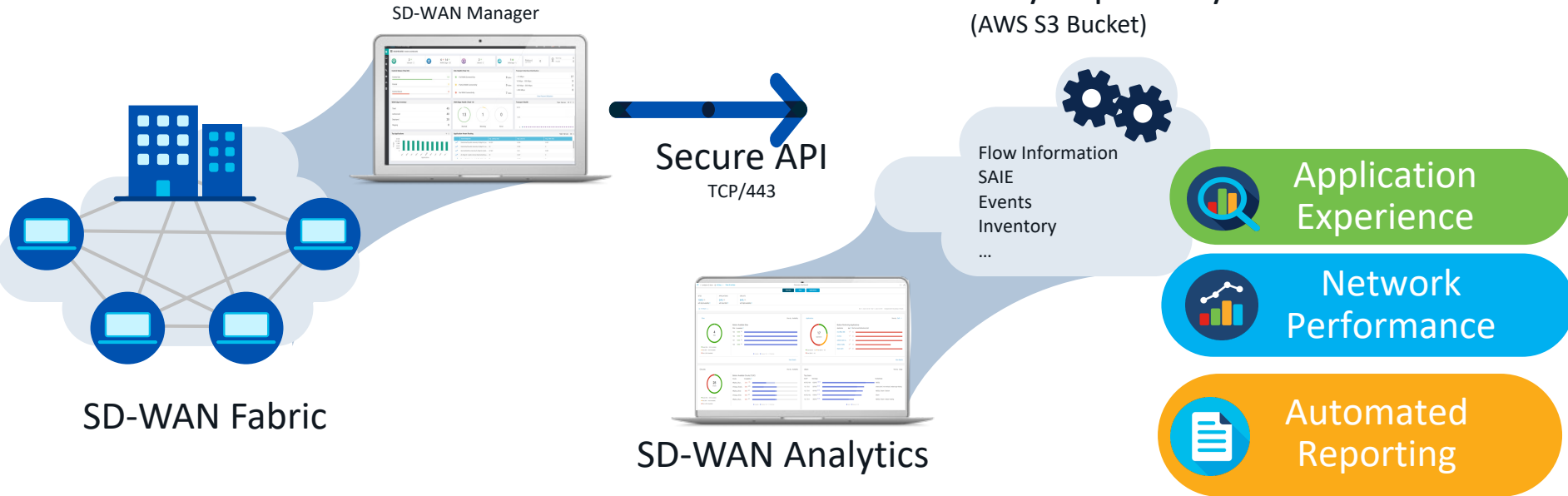


Catalyst IR8100



Catalyst IR8300

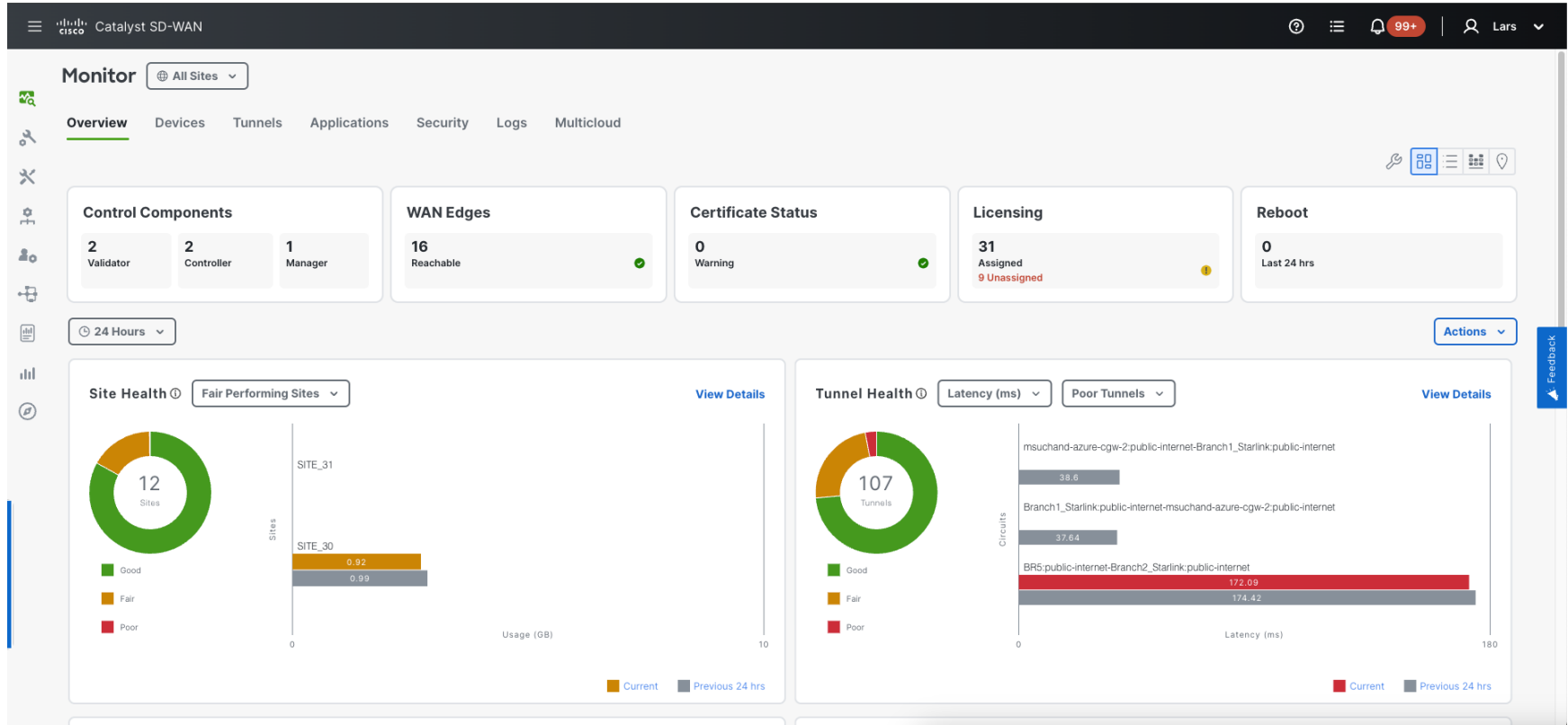
vAnalytics Architecture



On-Prem or Cloud-Hosted SD-WAN (vManage)

Cloud-Hosted vAnalytics

SD-WAN Manager UI



Demo

CISCO *Live!*



Catalyst SD-WAN

Username



Continue

SD-WAN Features

Significance of TLOC Color

Color is an abstraction used to identify individual WAN transport

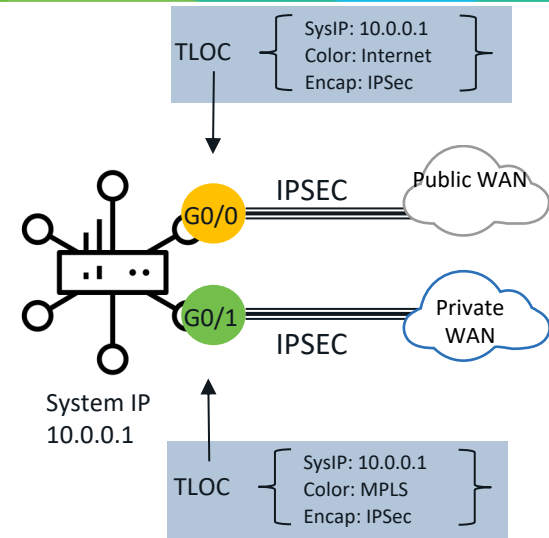
Colors are KEYWORDS not just LABELS

Policy is written based on these

TLOC maps to a physical WAN interfaces

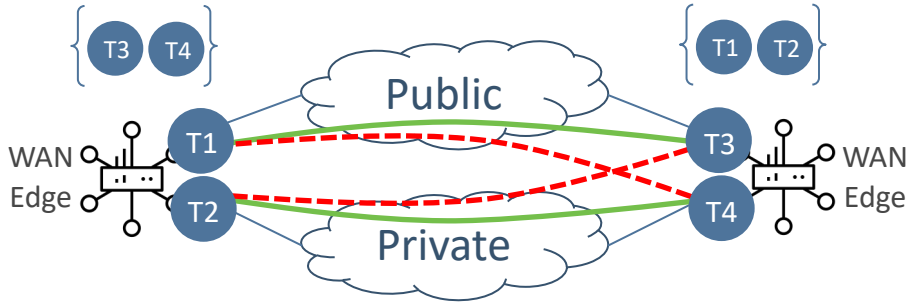
“Color” dictates the use of private-ip vs public-ip (dest) for Tunnel Establishment when there is NAT present

- 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



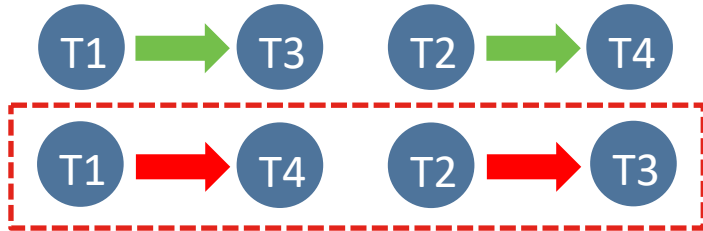
Private Colors	Public Colors
Metro-ethernet	3g
mpls	lte
private1	biz-internet
private2	public-internet
private3	blue
private4	green
private5	red
private6	gold
	silver
	bronze

Transport Colors

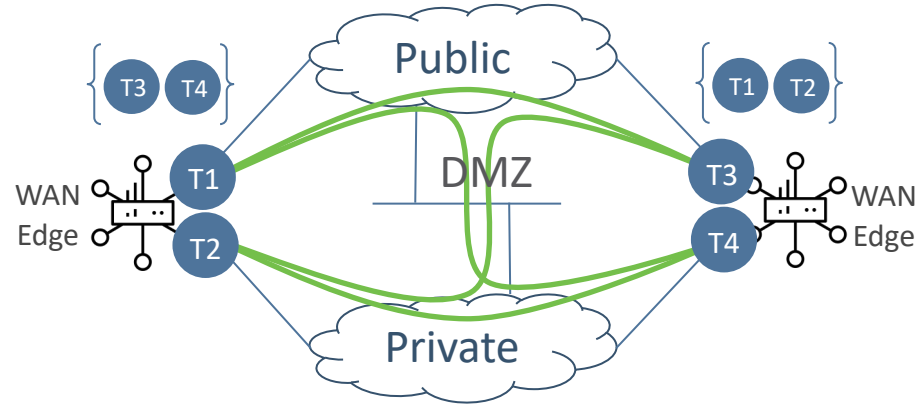


T1, T3 – Public Color

T2, T4 – Private Color



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



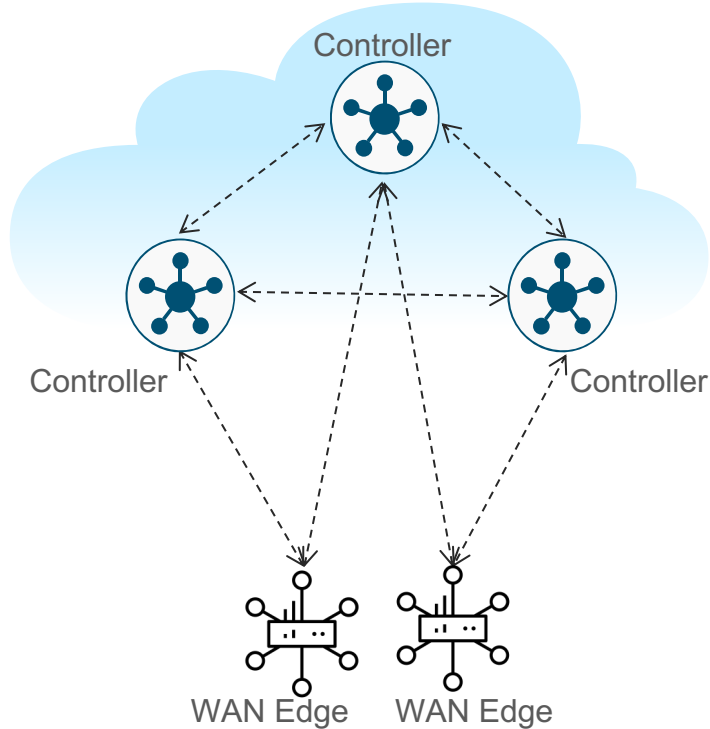
T1, T3 – Public Color

T2, T4 – Private Color

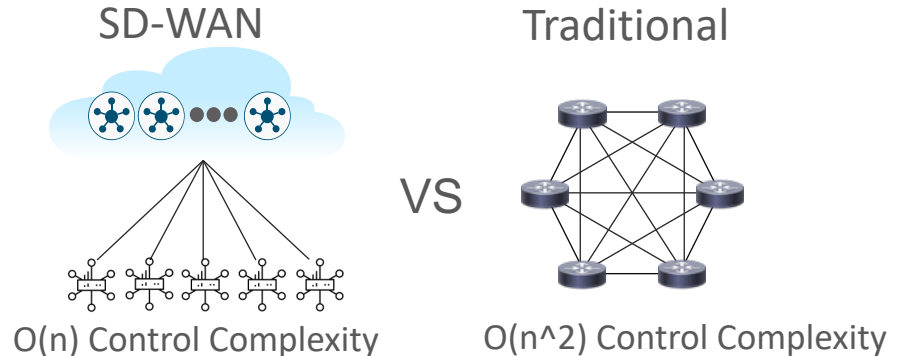




Overlay Management Protocol (OMP)

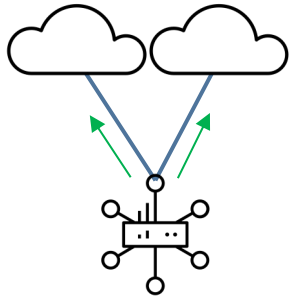


- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
 - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane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

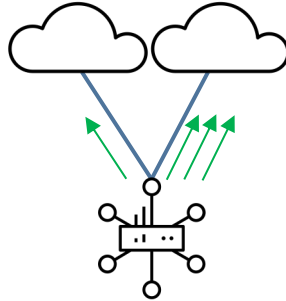


Fabric Communication

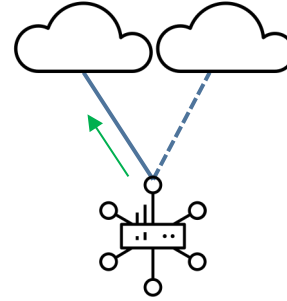
Per-Session Load-sharing
Active/Active



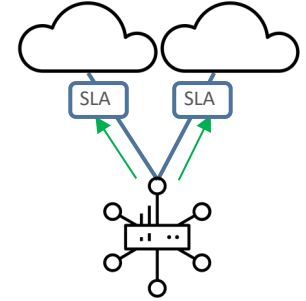
Per-Session Weighted
Active/Active



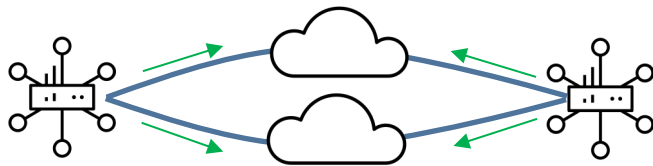
Application Pinning
Active/Standby



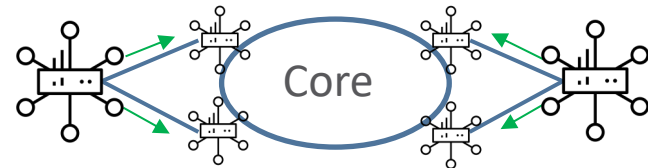
Application Aware Routing
SLA Compliant



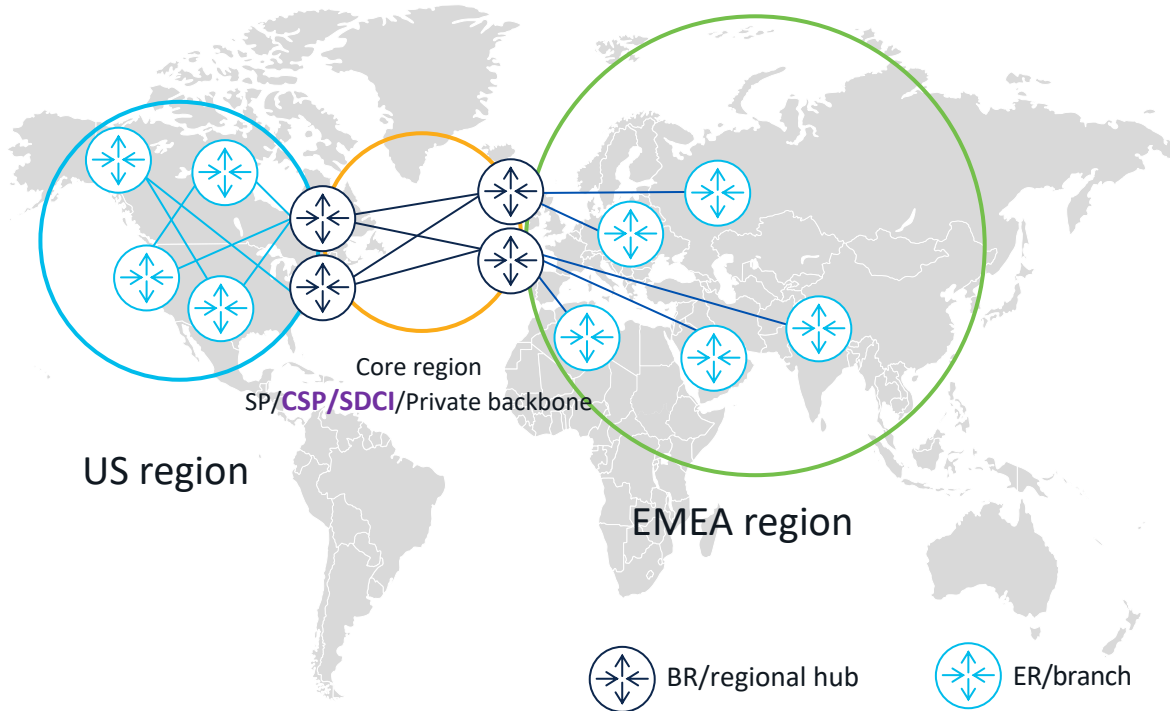
Single-hop Fabric



Multi-Region Fabric



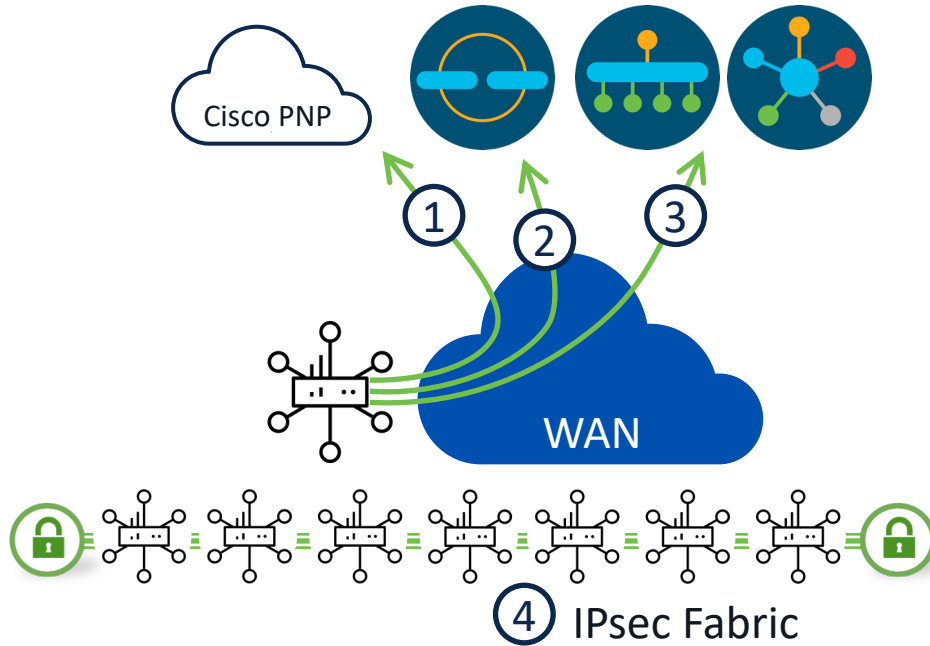
What is Multi Region Fabric (MRF)?



- Intuitive user-defined site grouping. E.g. based on geo
- Finer grouping using sub-regions
- Auto restrict overlay tunnels between regions
- Different topologies per region
- Mix access transports across regions
- Scale up control-plane per region(s)

Lets bring it up

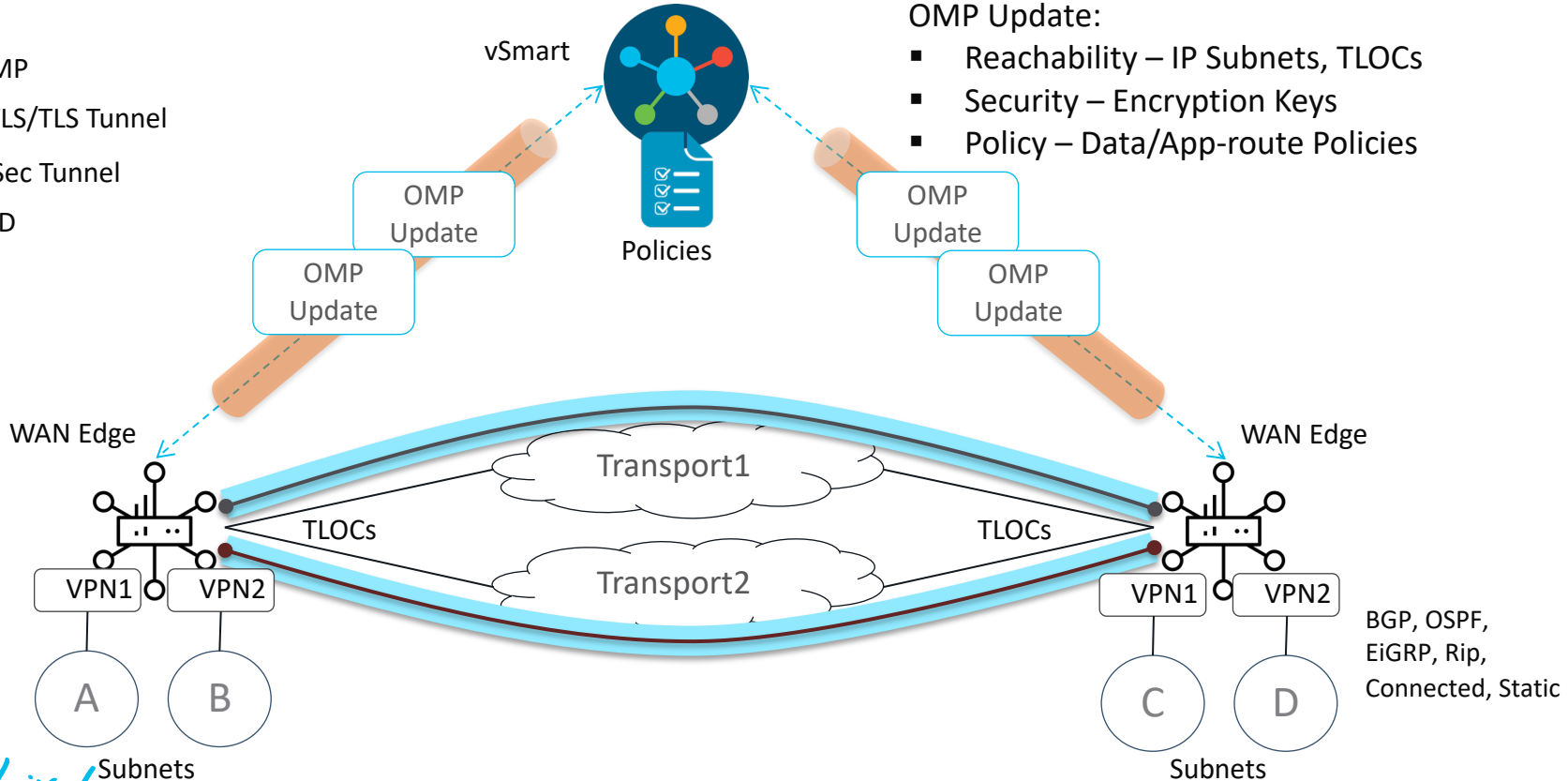
Automated, Zero-Touch Onboarding



- 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

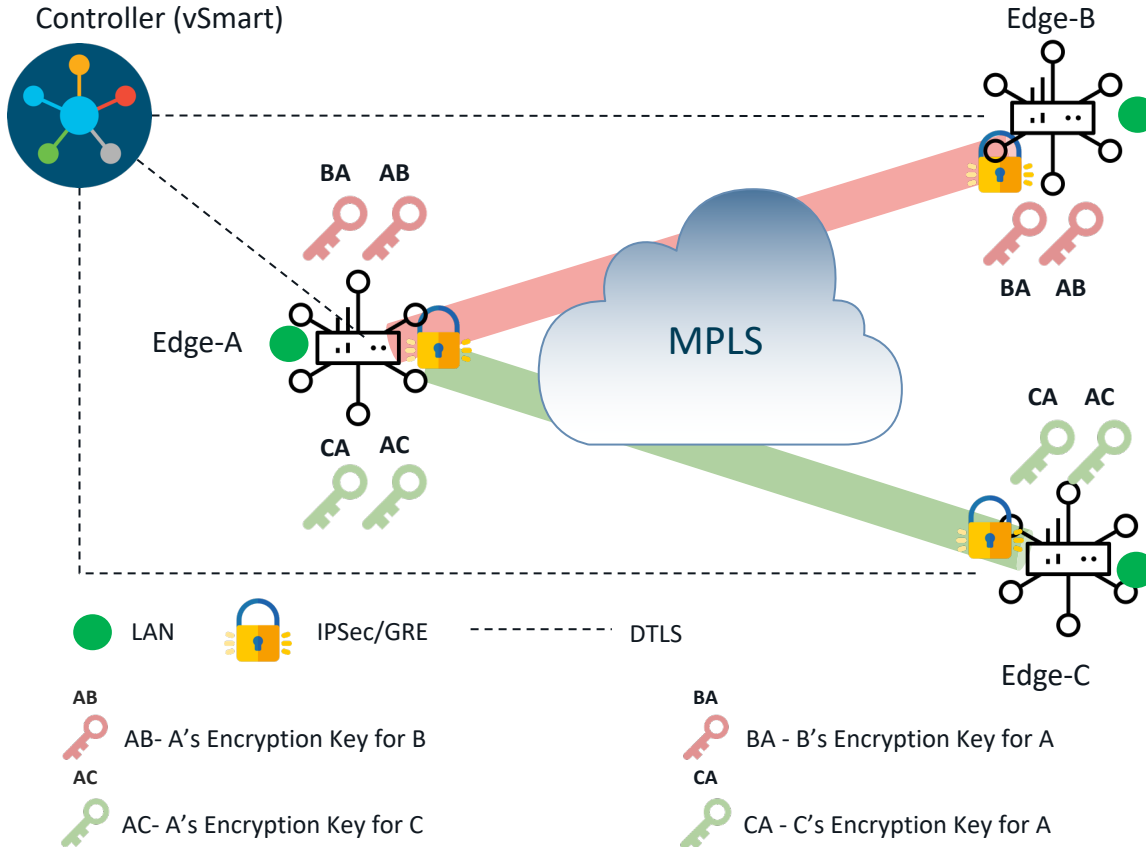
- OMP
- DTLS/TLS Tunnel
- IPsec Tunnel
- BFD



OMP Update:

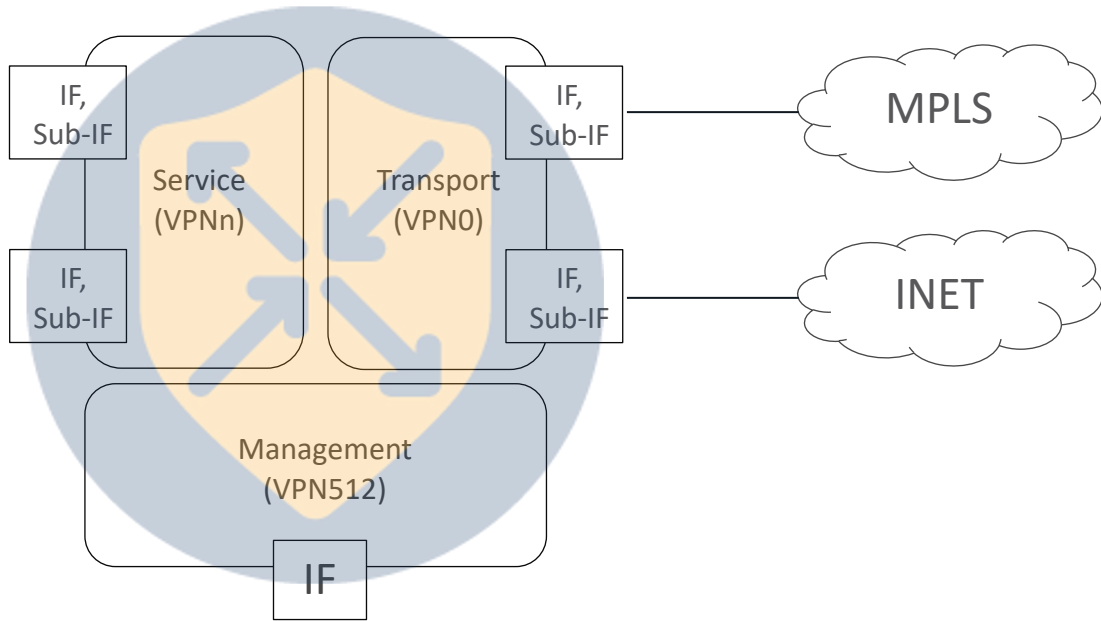
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies

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

Cisco SD-WAN VPNs (VRFs)

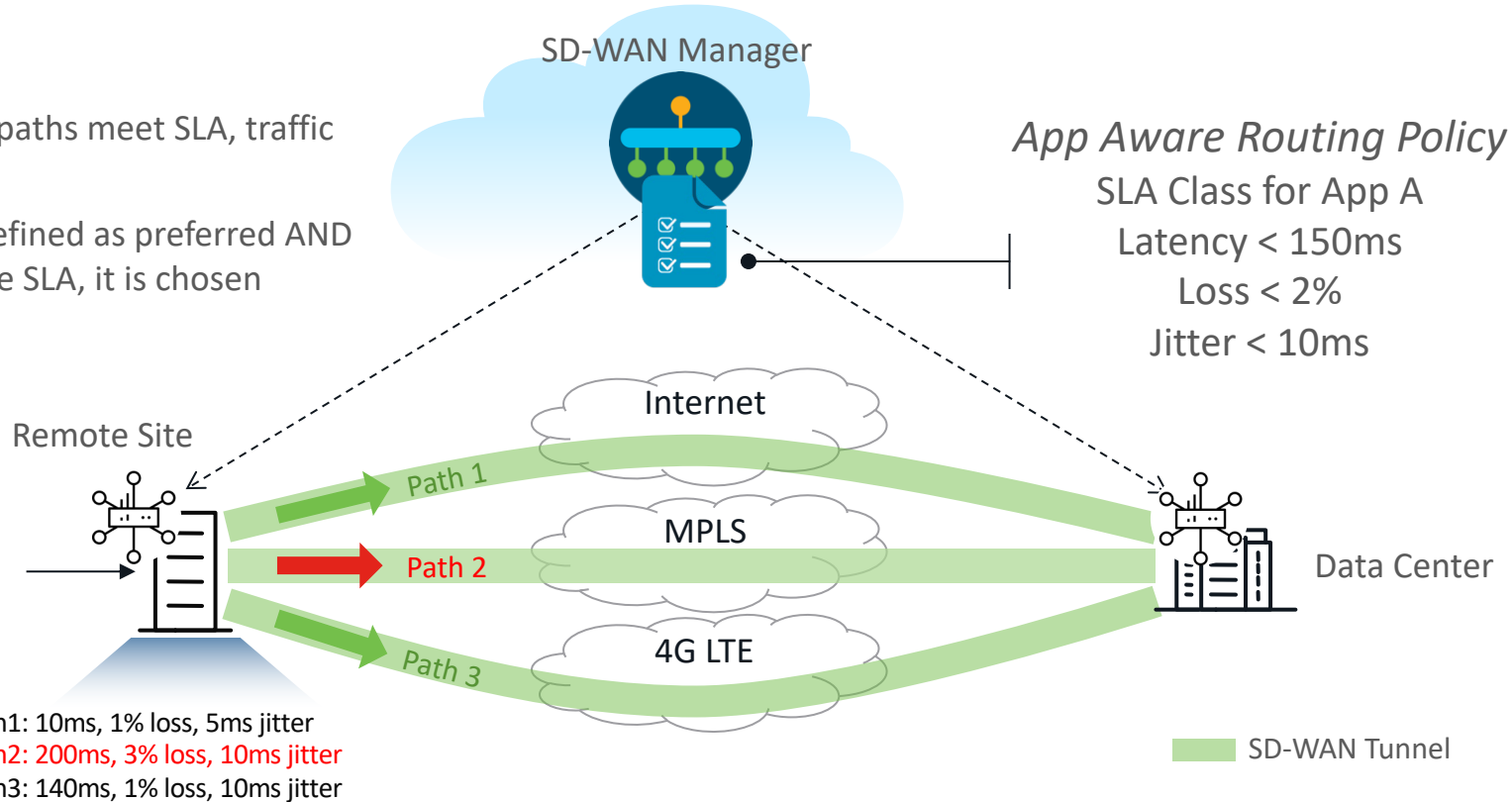


- VPNs are isolated from each other, with each VPN has its own forwarding table
- Reachability within VPN is advertised by OMP
- VPN0 is reserved for WAN uplinks (Transport)
- VPN512 is reserved for Management interfaces
- VPNn represents user-defined LAN segments (Service)



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)

Benefits

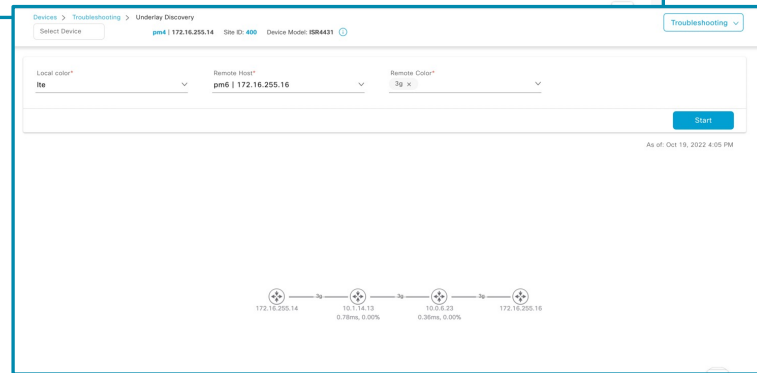
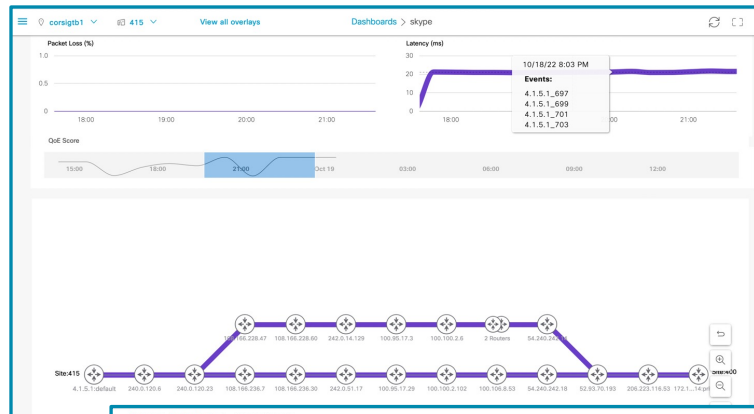
Gain visibility into the exact underlay path* against SD-WAN tunnel
(including hop-by-hop metrics)

* Requires vManage 20.10+ and IOS-XE 17.10.1

Highlights

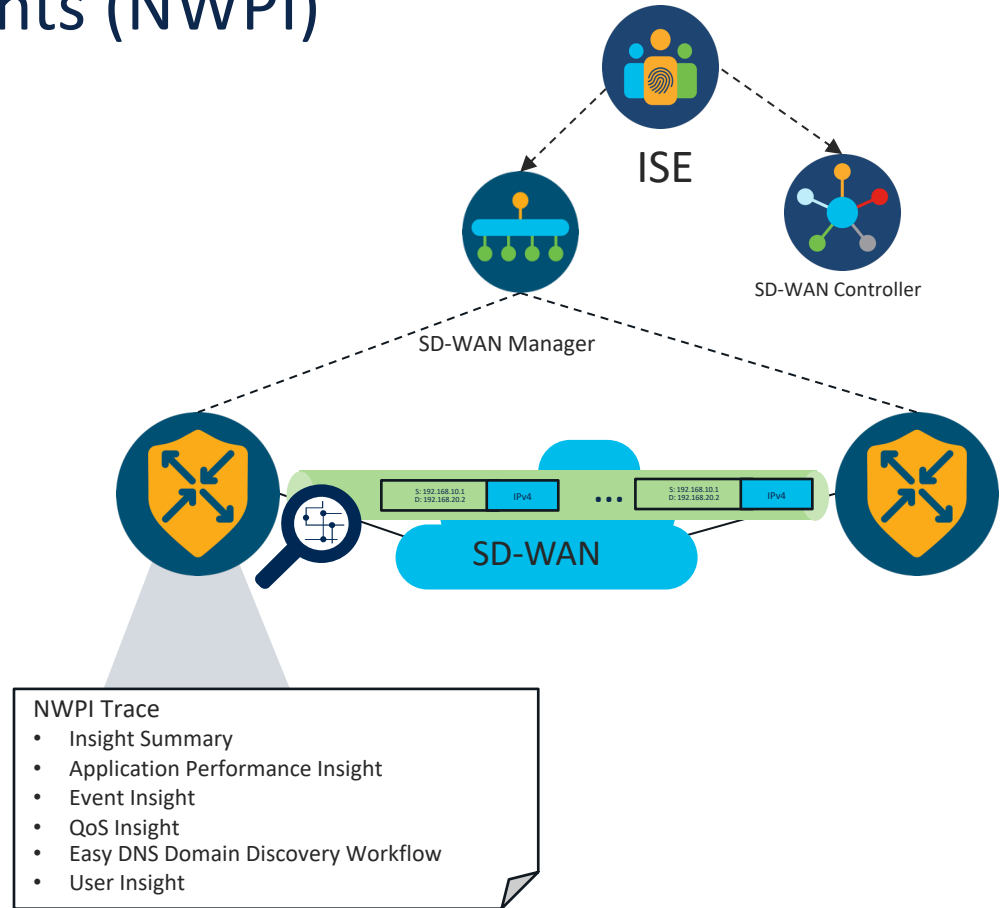
- 1 Zoom into the specific time period showcasing drop in application health (QoE) trend line
- 2 View the hop-by-hop underlay path along with loss and latency metrics at every hop
- 3 View associated loss, latency besides underlay path

- 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



Network Wide Path Insights (NWPI)

- NWPI provides network wide insights such as
 - Path insight overview,
 - Application Performance Insight,
 - Event Insight,
 - QoS Insight,
 - Flow Level Path Insights,
 - DNS domain discovery,
 - Path performance metrics.
- NWPI helps to validate policy design and insights for various application performance issues.
- In 20.13/17.13, in NWPI trace settings we can trigger trace for specific user and group Insight summary based on user filter.



Insight Summary - Overview

Overview

App Performance Insight

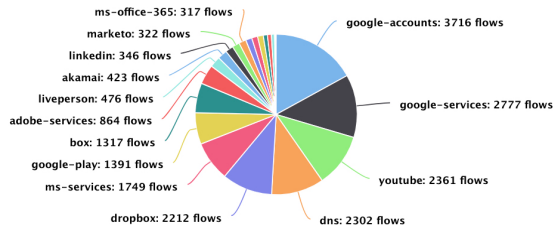
Event Insight

QoS Insight

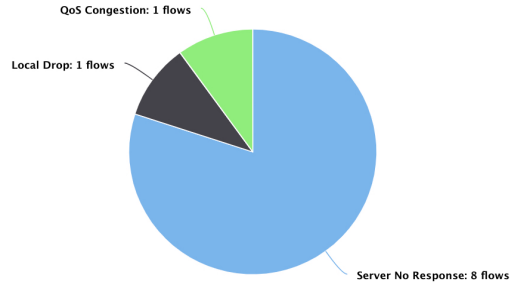
Trace: alanwan-0723-domain2 (ID: 8624) ⓘ

Critical Warning Informational

Applications



Events



Events: Server No Response x Local Drop x QoS Congestion x

What Server No Response
 impacted 7 unknown flows
 4 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:27:16 PM - 7/23/2022, 2:28:23 PM
 3 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:43:01 PM - 7/23/2022, 2:43:25 PM
 4 flows: RTP-Hub1:PUBLOC_INTERNET to SHN-Branch1:PUBLOC_INTERNET,7/23/2022, 2:27:16 PM - 7/23/2022, 2:28:15 PM
 3 flows: RTP-Hub1:PUBLOC_INTERNET to SHN-Branch1:PUBLOC_INTERNET,7/23/2022, 2:43:01 PM - 7/23/2022, 2:43:25 PM

Who impacted 1 adobe-services flows
 1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS)7/23/2022, 2:43:58 PM - 7/23/2022, 2:44:57 PM

Where 1 flows: RTP-Hub1:PUBLOC_INTERNET to SHN-Branch1:PUBLOC_INTERNET,7/23/2022, 2:43:58 PM - 7/23/2022, 2:44:57 PM

Why Local Drop
 impacted 1 box flows
 1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:18:19 PM - 7/23/2022, 2:18:40 PM
 drop cause: TailDrop

QoS Congestion
 impacted 1 box flows
 1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:18:19 PM - 7/23/2022, 2:18:40 PM
 policy: qos_template, type: qosMap, queue: 1

Hyperlink

Hyperlink will help user quickly spot impacted flows in one click and drill down to deeper understanding of "Why".

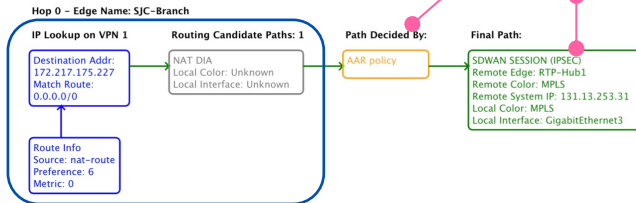
Path Insight at Flow Level

Flow Readout

Overview Path Insight

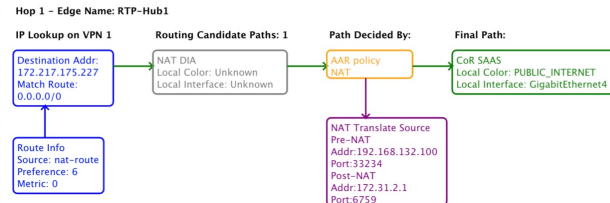
Trace: wzhou4-s32-asym (ID: 4704), Flow ID: 59996 (Application: google-services)

Upstream (From 192.168.132.100:33234 to 172.217.175.227:443)



Visibility to routing decision

Why this path? by what?



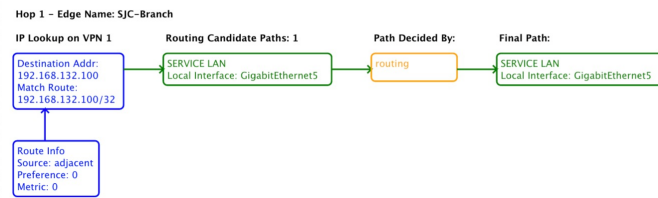
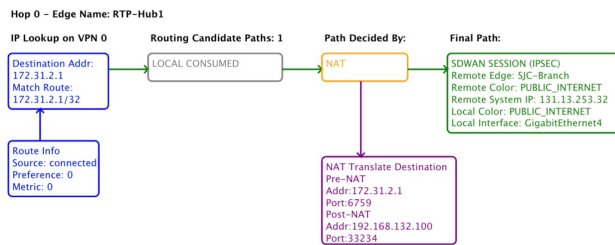
Insight Level 1- What

Office 365 takes Internet path



Insight Level 2- Why

Downstream (From 172.217.175.227:443 to 192.168.132.100:33234)



Data Policy

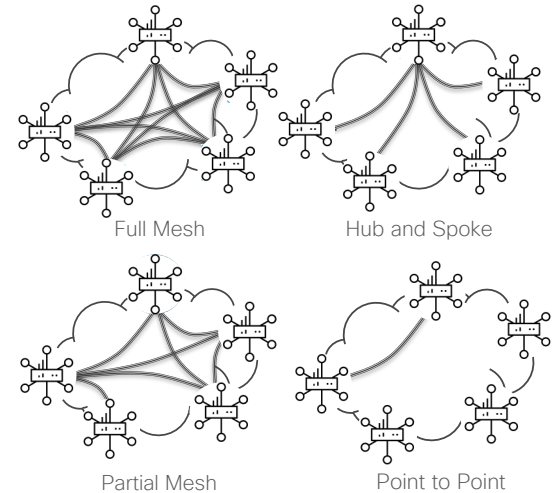
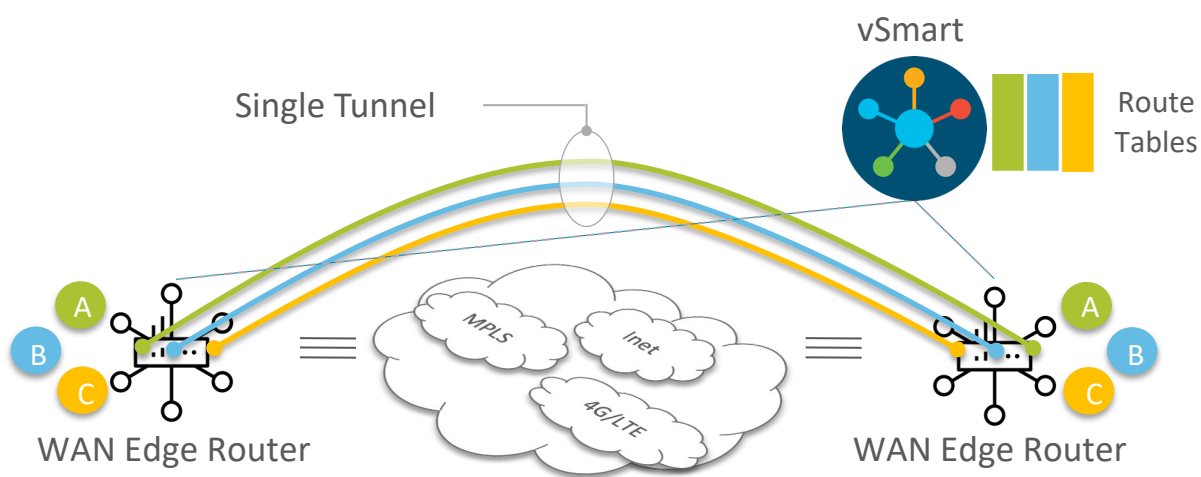


Insight Analysis

Google services application took the path decided by CoR-SaaS from SJC-Banch to RTP hub, then to Internet.

Security features

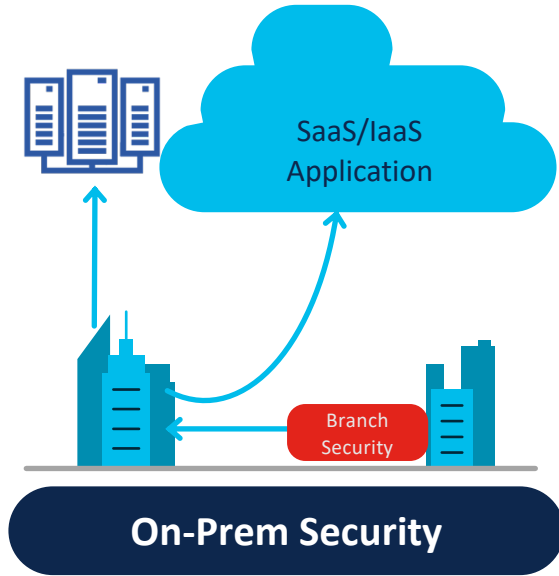
End-to-End Segmentation with Multi-Topology



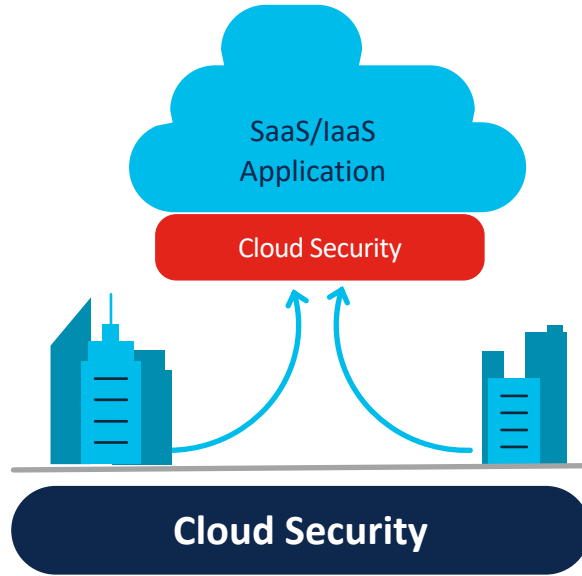
Segment connectivity across the SD-WAN fabric without reliance on underlay transport

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

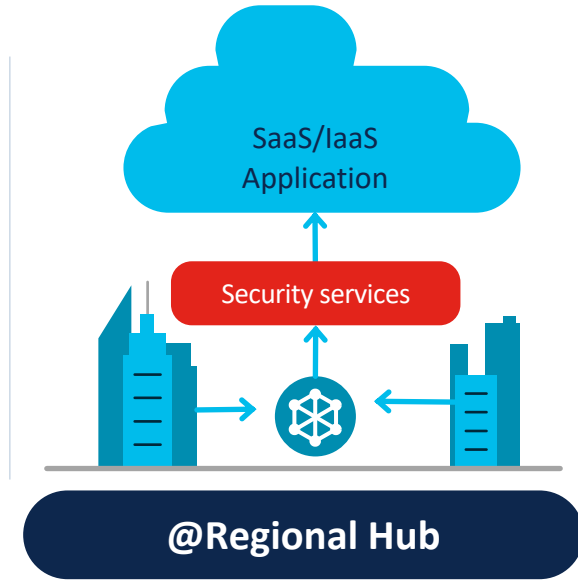
Relevant Security Models. Driving towards SASE



Thick branch with Routing and Security



Thin branch with security in the cloud

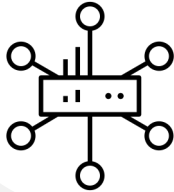


Security Services on a Regional Hub

Cisco Catalyst SD-WAN Security & SASE Solution

Consistent across on-prem and cloud

**Cisco
SD-WAN**



< 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

SSE Integration

DNS Security/Cloud FW with Cisco Secure Access

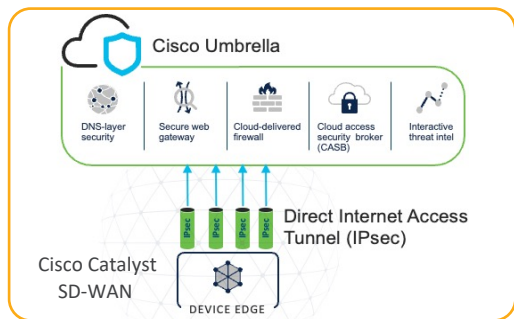
Catalyst SD-WAN + SSE: Redefining Security for Tomorrow...

Unified SASE



Cisco On Cisco

Cisco on Cisco - Tailored Security for Your Network's Unique Needs



Hands-off automation | Top notch protection | Simplified management



Integrated SASE



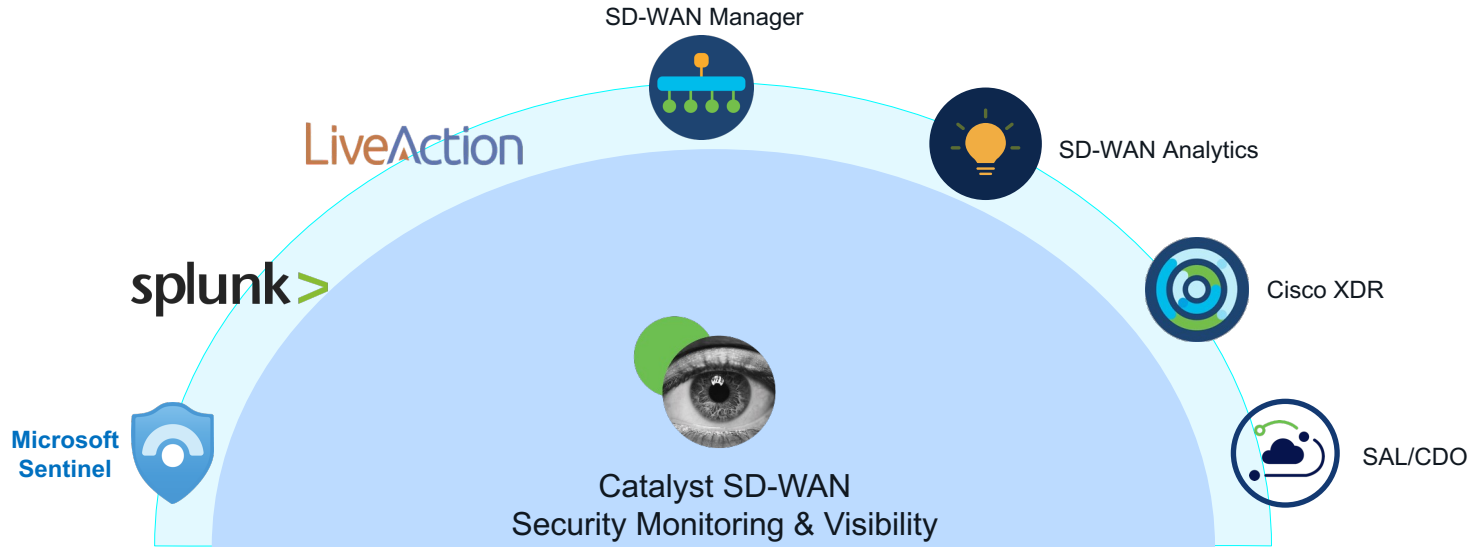
SASE a-la-carte

Build-your-own SASE approach



Security Threat Monitoring Ecosystem

- SD-WAN SecOps dashboard provides comprehensive Monitoring, Threat Visibility with user access control only for SecOps Team
- Ability to correlate user, threat, applications and associated Security function
- Logs can be exported and consumed through the 3rd party Security Logging & Monitoring tools like Splunk, Sentinel, etc
- Auditing & Compliance for long-term data retention

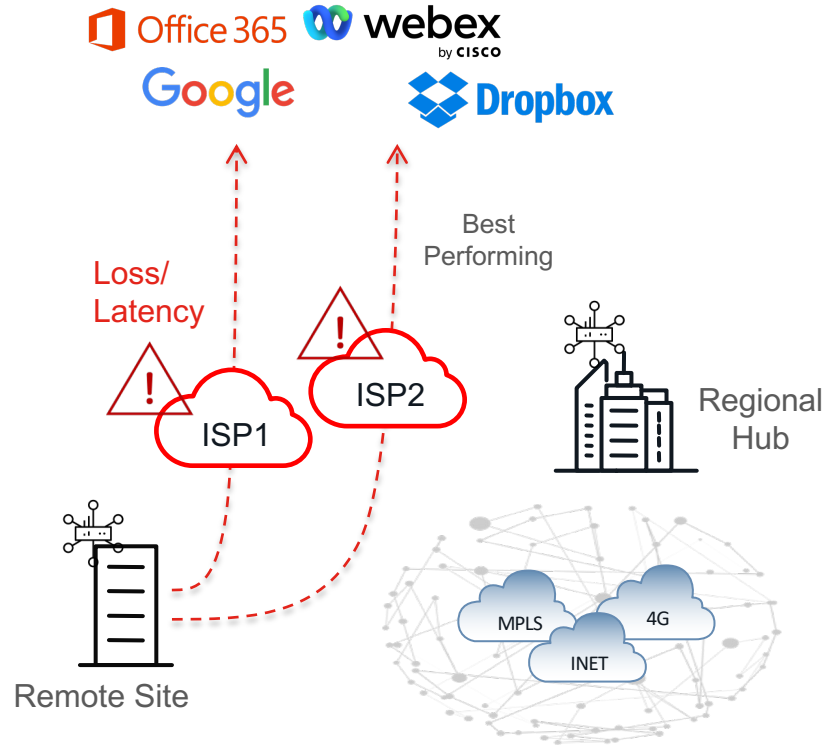


Cloud OnRamp for SaaS

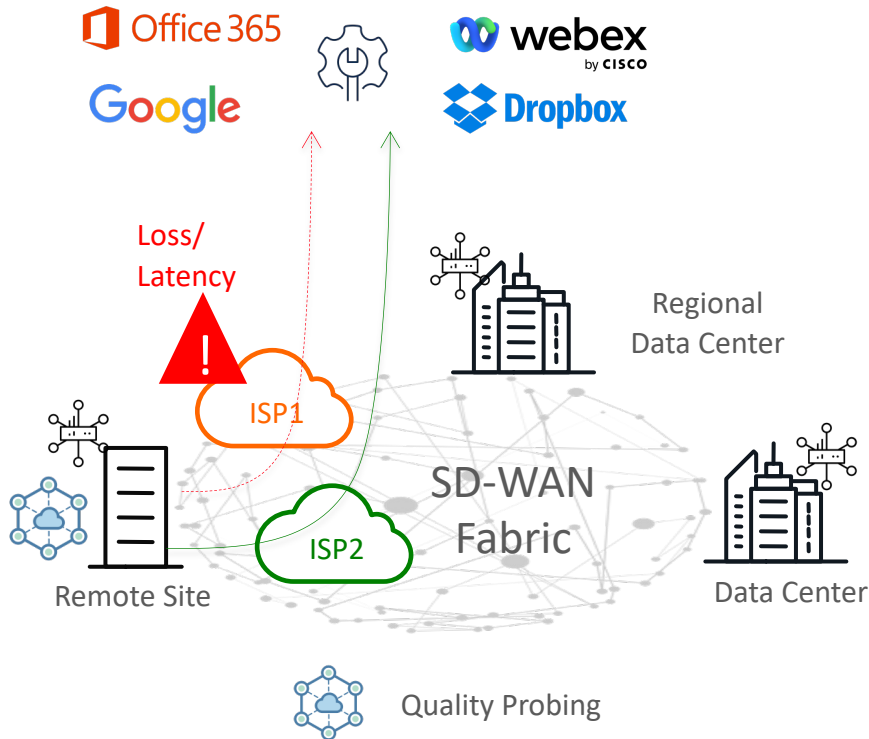


SaaS Optimization Challenges

- 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

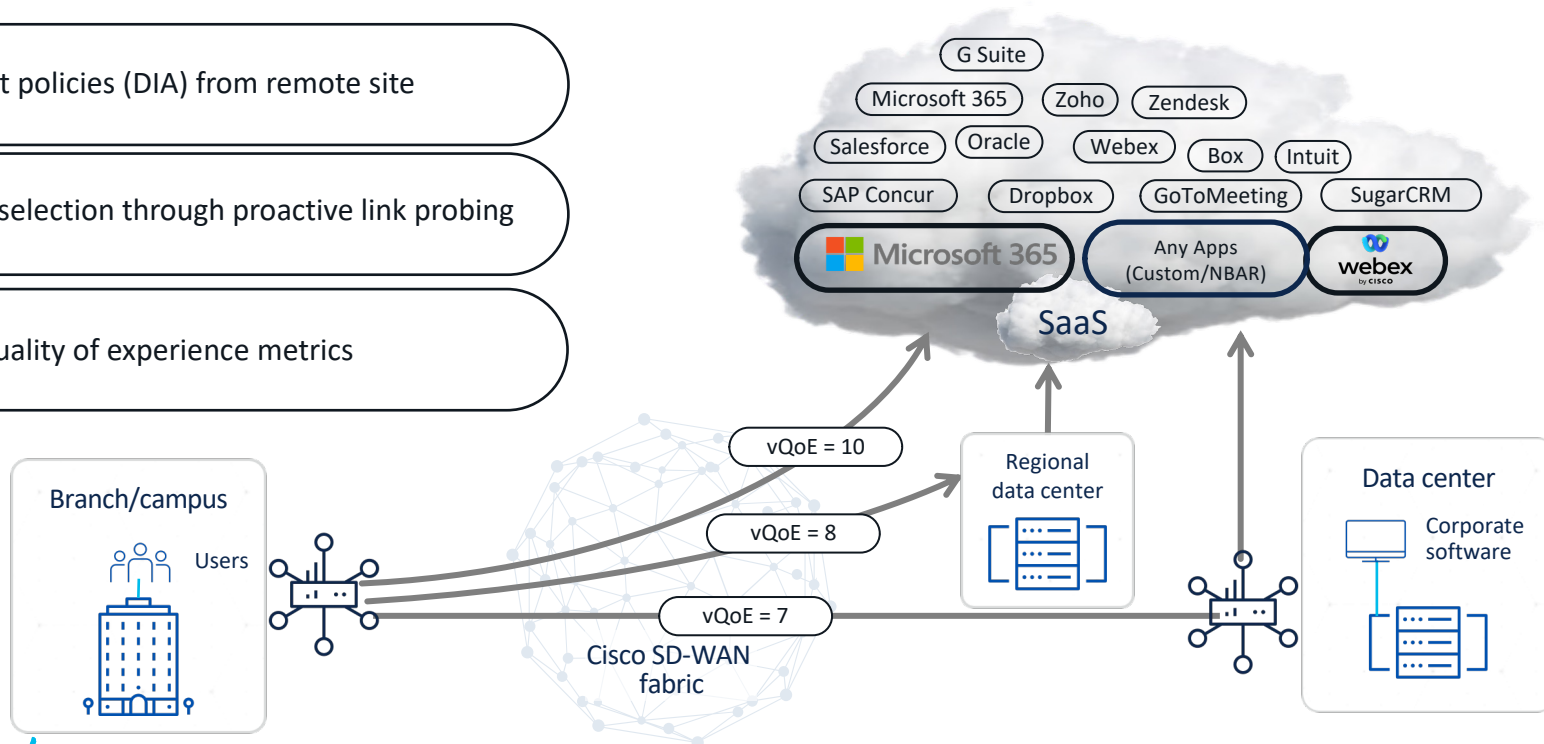
Cloud OnRamp for SaaS

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



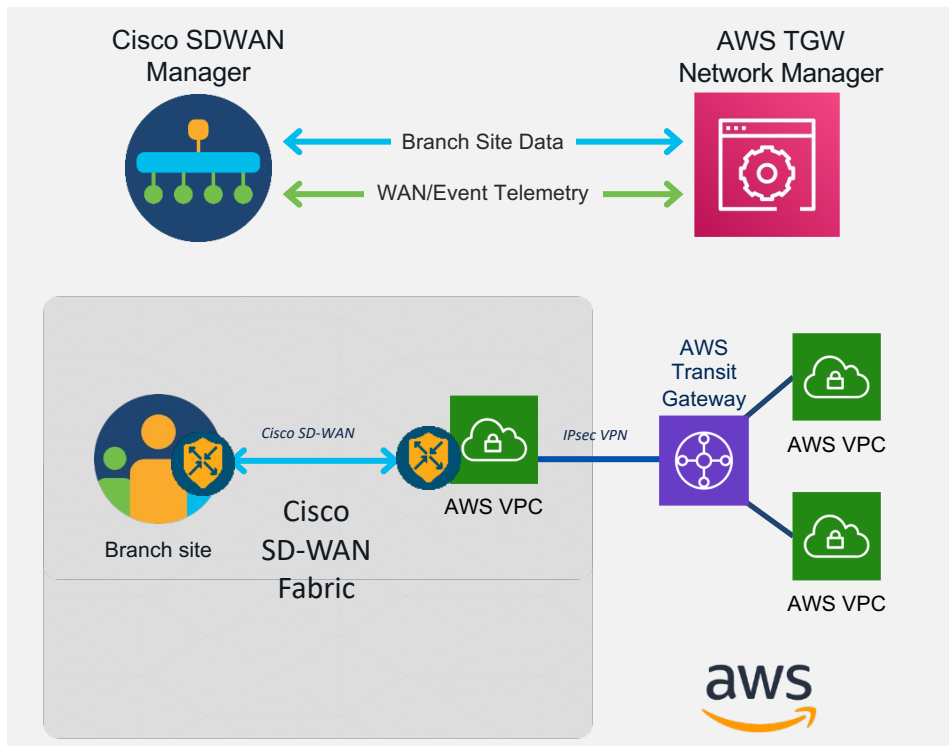
Cloud OnRamp for MultiCloud



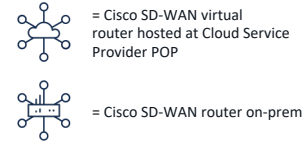
Extending SD-WAN into Public Cloud (AWS as example)

Benefits

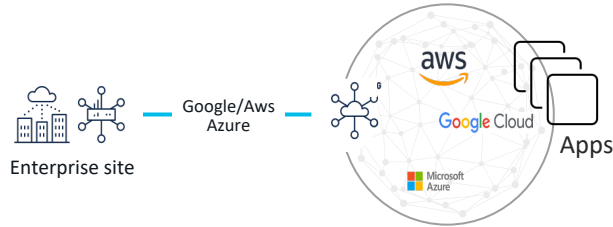
- Automated provisioning of SD-WAN Transit VPC and TGW, route exchange for site to cloud and site to site traffic over AWS backbone
- Full Visibility into inter-regional transit traffic and telemetry with TGW Network Manager
- Consistent Policy and Segmentation across branch and cloud for enterprise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



Cisco SD-WAN Cloud Hub- Use Cases



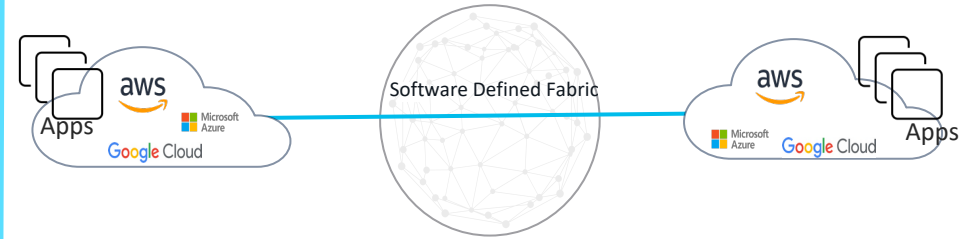
Enterprise Site to Cloud



Enterprise Site to Enterprise Site

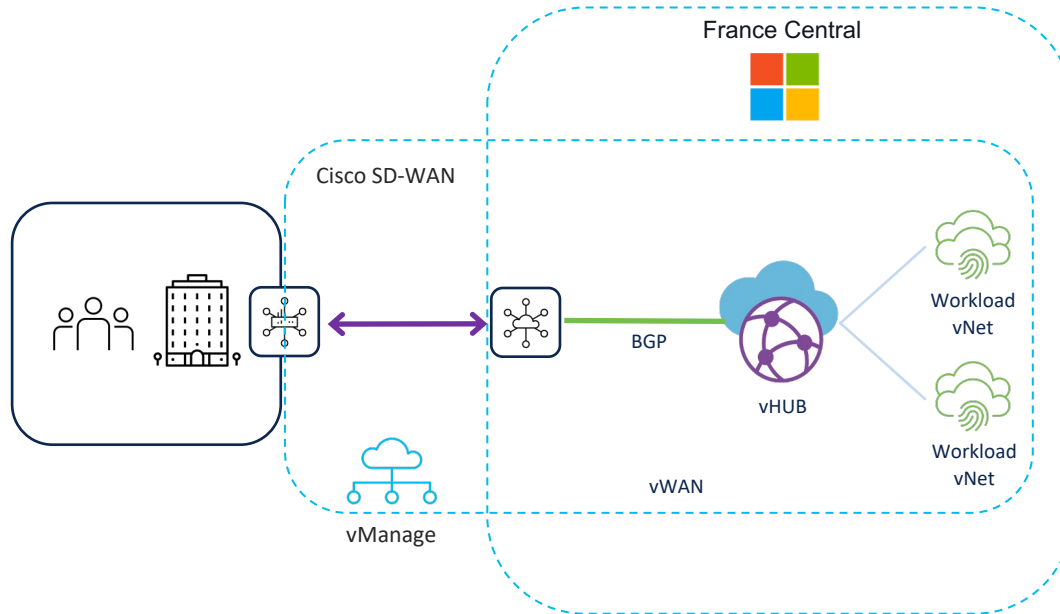


Cloud to Cloud/Inter-Cloud

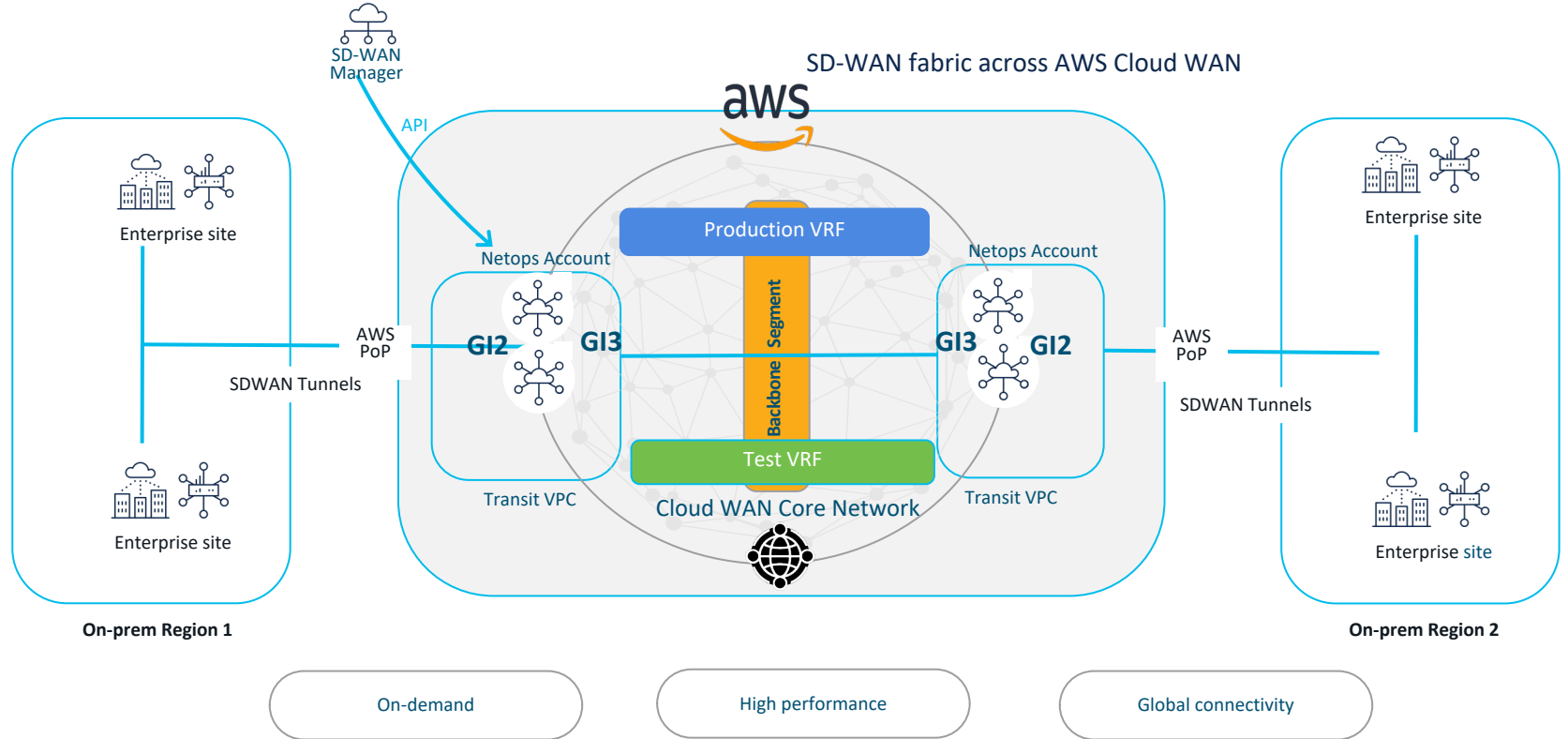


Cisco SD-WAN simplifying connectivity with fabric extension to cloud providers, it is building a programmable site-to-cloud, Region to Region, site-to-site and cloud to cloud connectivity using cloud providers Native contracts and backbone

Cisco SD-WAN Cloud OnRamp for Multicloud with Microsoft Azure



Site-to-Site with Cloud WAN



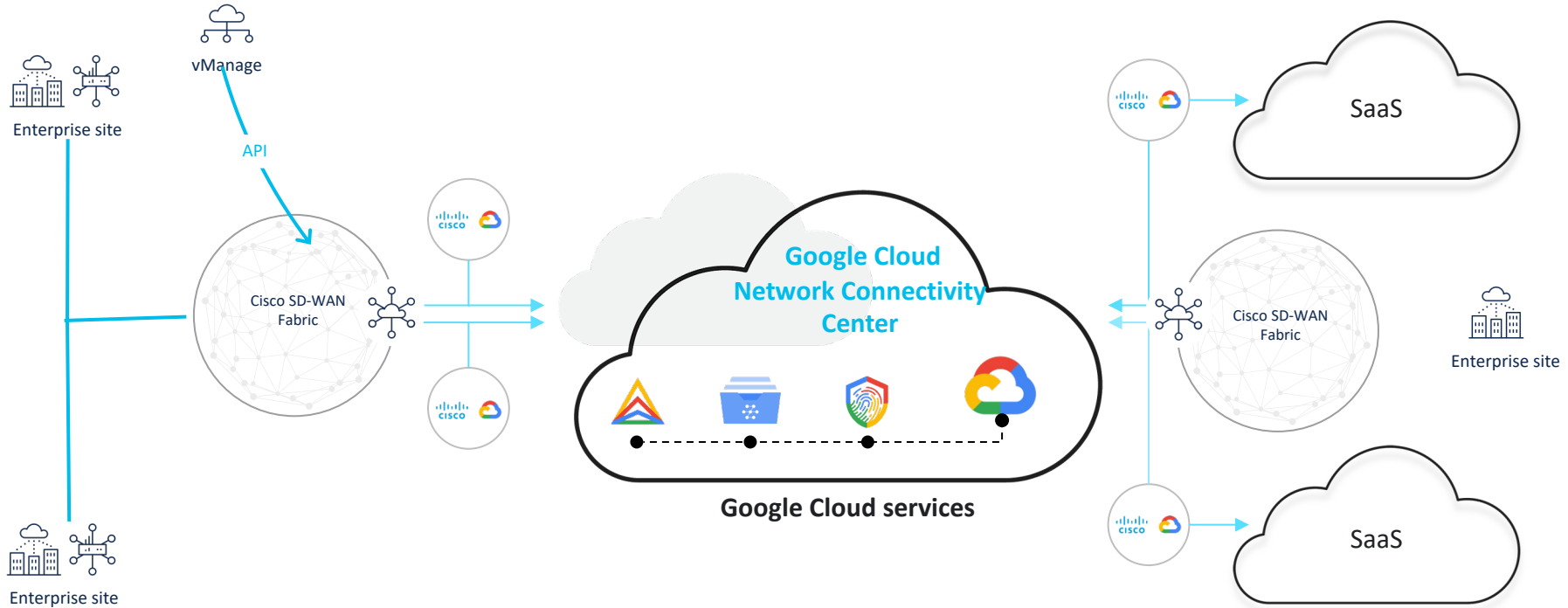
Cisco SD-WAN Cloud Hub and Google Cloud Network Connectivity Center



= Cisco SD-WAN router on-premises

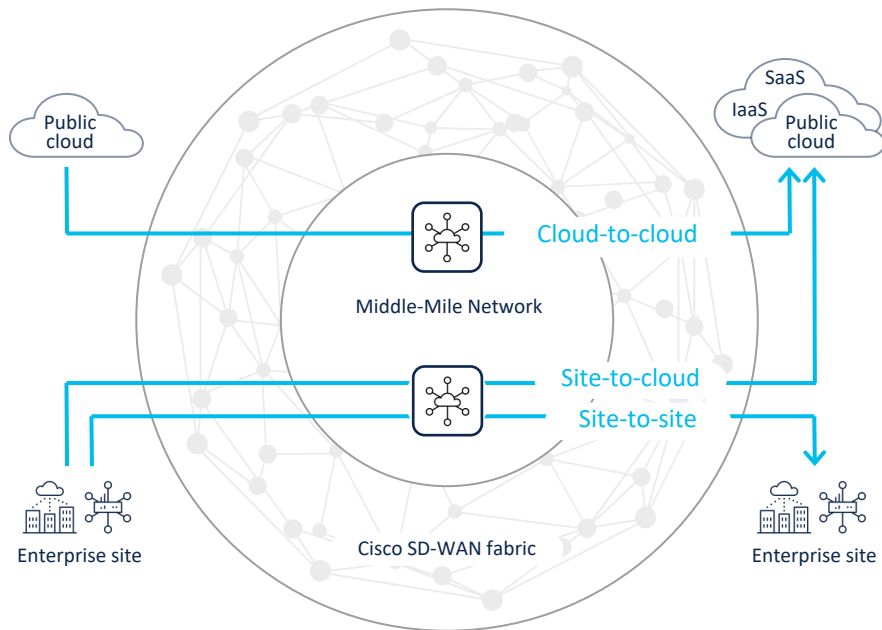
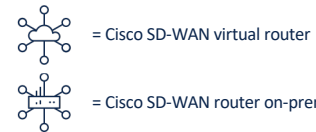


= Cisco SD-WAN cloud router at Google Cloud PoP




Cisco SD-WAN Cloud Hub with Google Cloud

Cisco SD-WAN 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

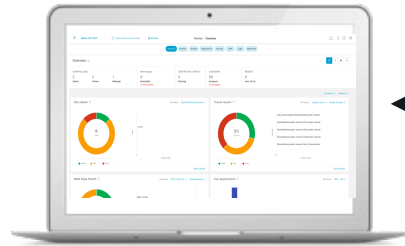
SD-Routing?

Introducing SD-Routing

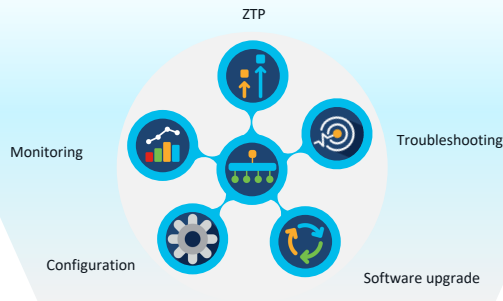
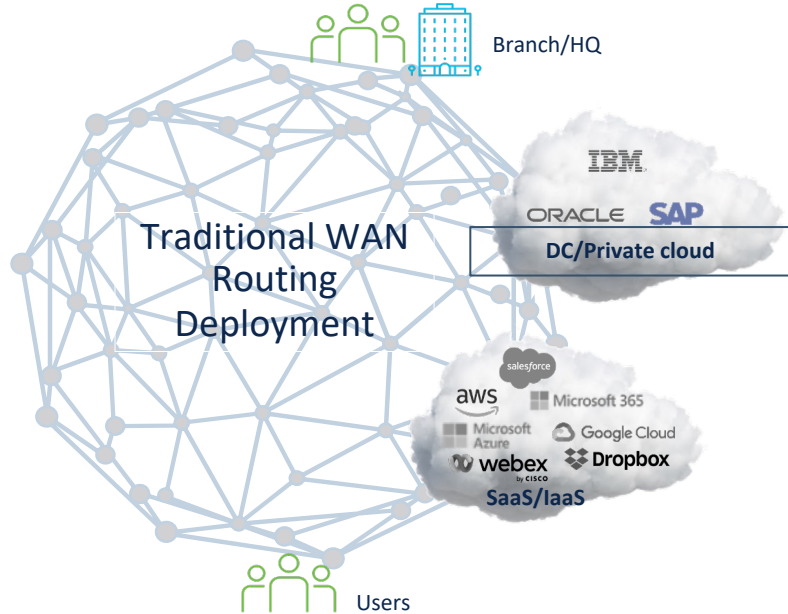
Transform the platform experience



Learn more watch
BRKENT-1039

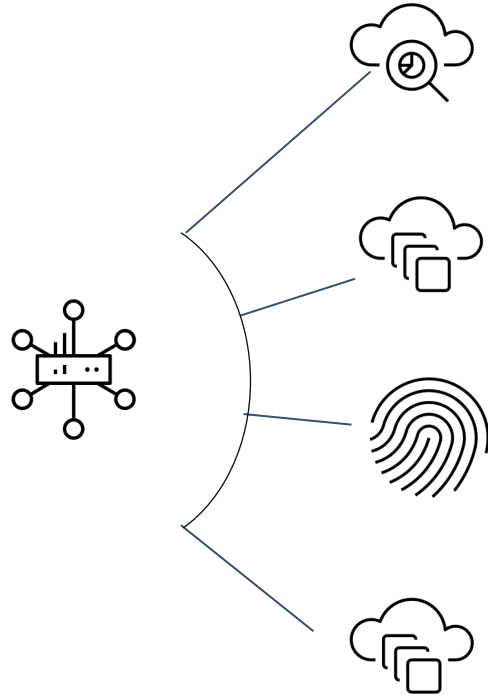


Catalyst SD-WAN Manager



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.



Continue
your education

CISCO *Live!*

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



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, creating a sense of motion and energy.

CISCO *Live!*

Let's go