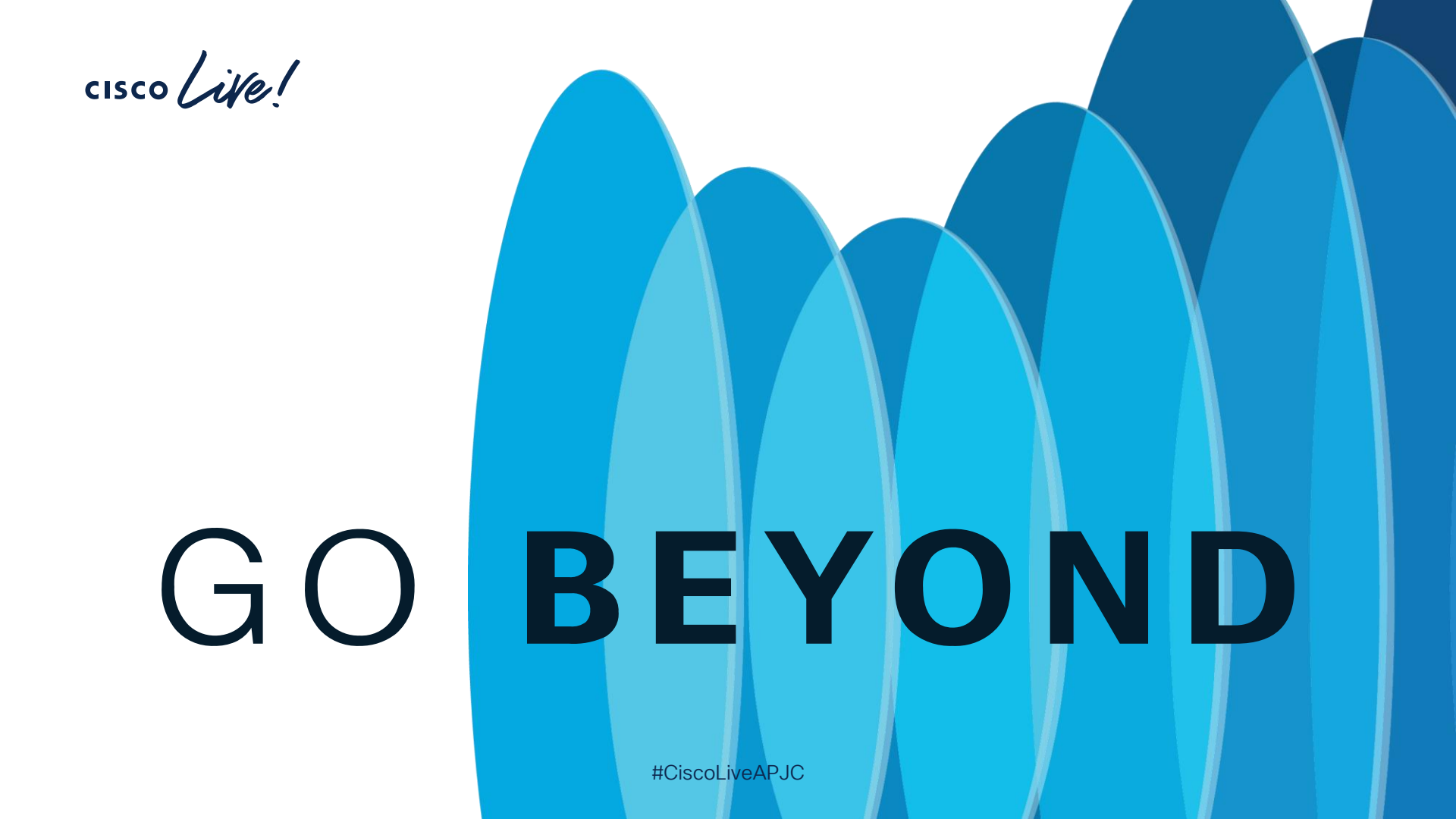

cisco Live!
GO BEYOND
#CiscoLiveAPJC

SD-WAN: Start here

Daniel Atalla, Solutions Engineer
@datalla

BRKENT-2108

Cisco Webex App

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

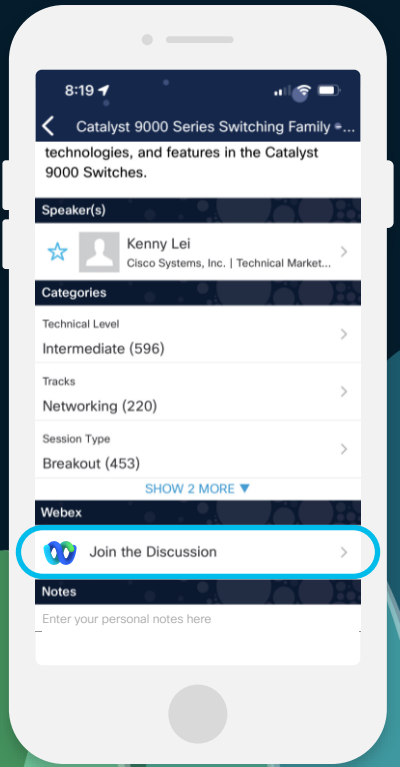
Questions?

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

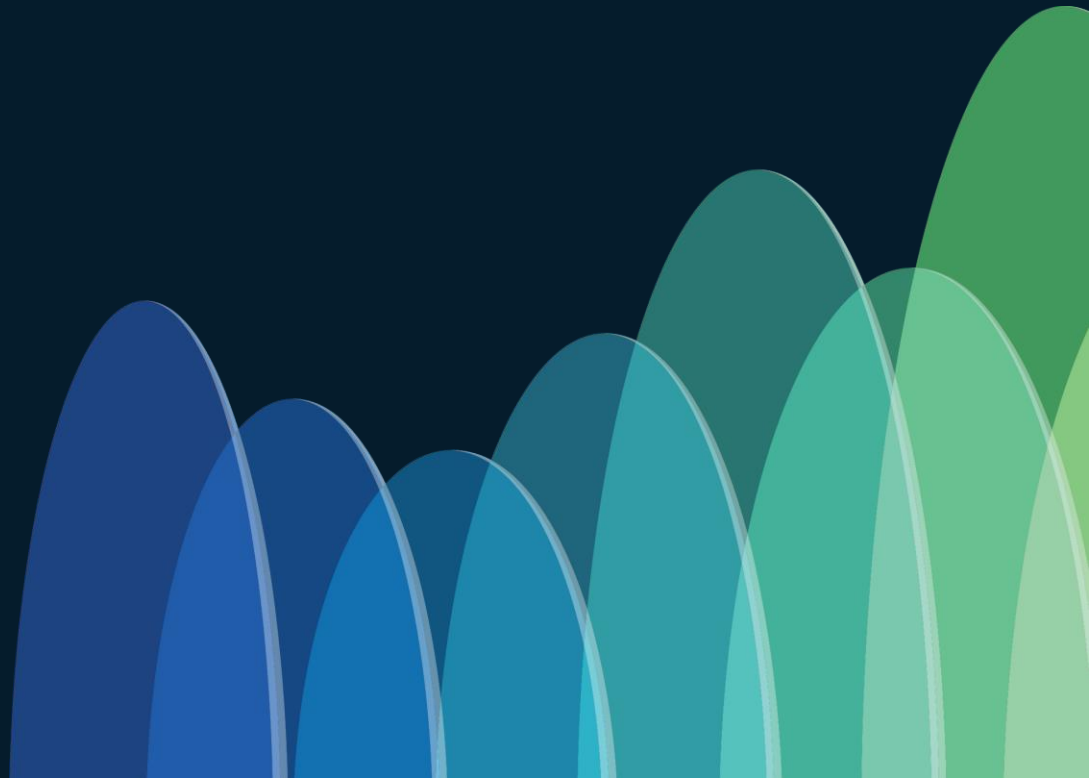
Webex spaces will be moderated by the speaker until June 7, 2024.



Agenda

- 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

Solution Architecture



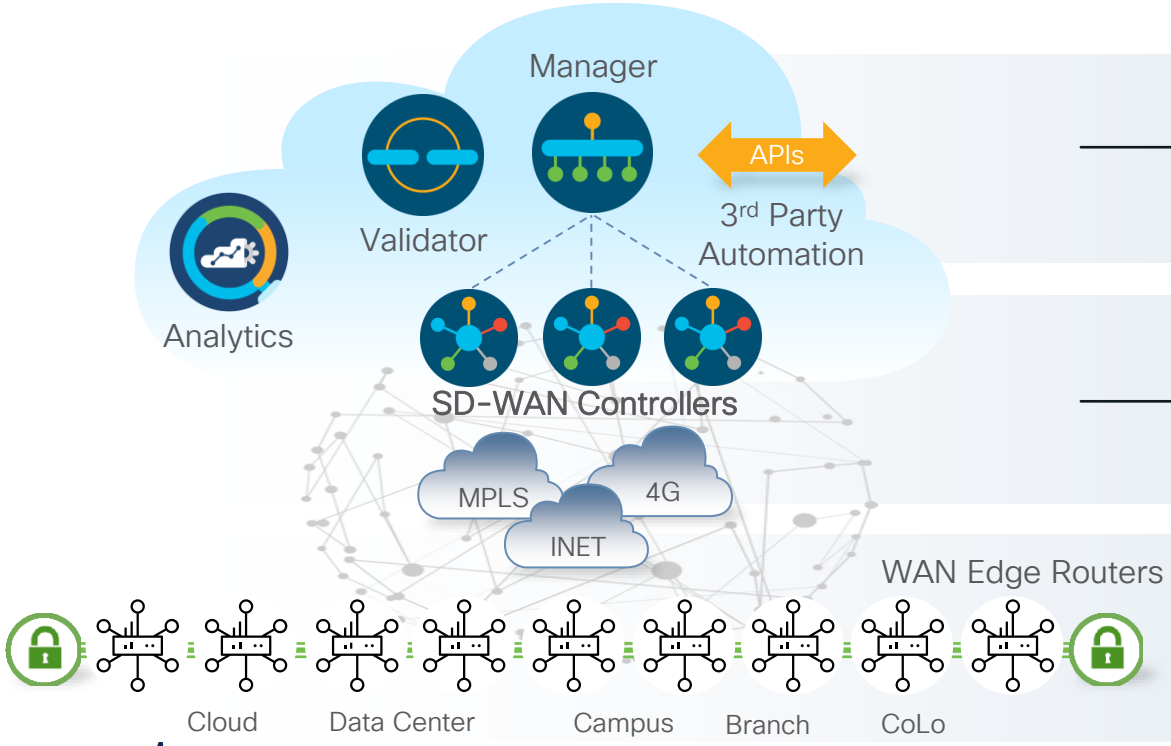
cisco Live!

FYI

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

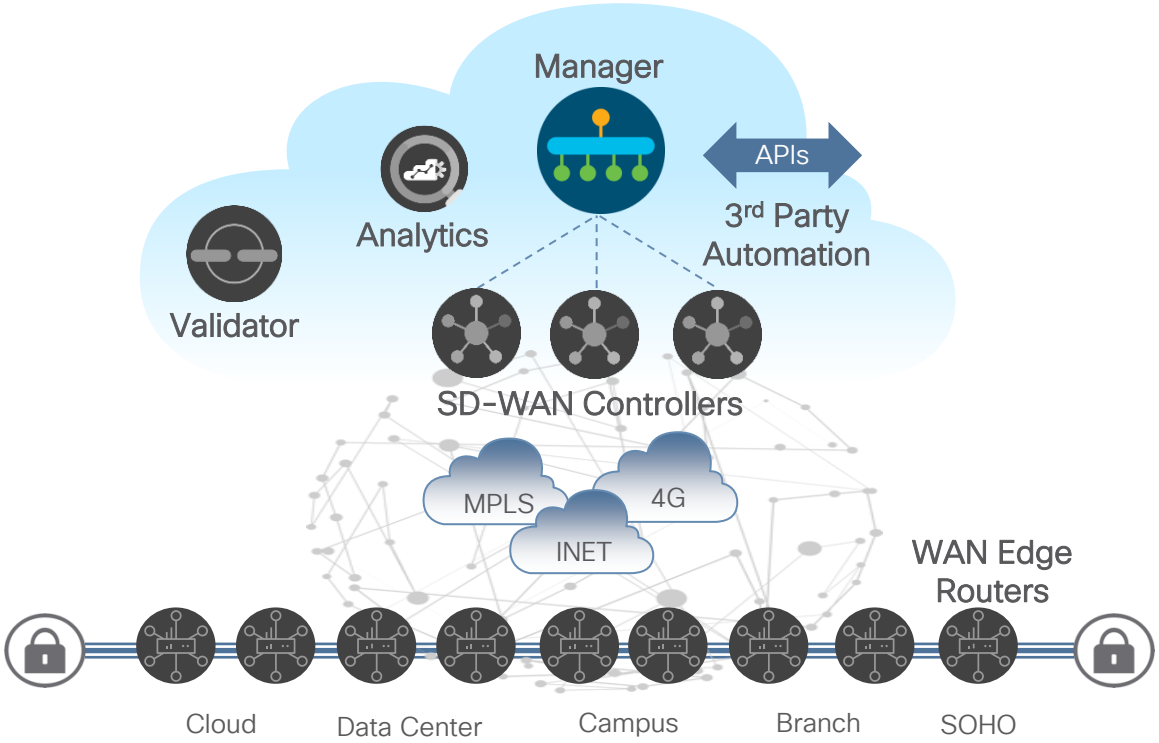


Management/
Orchestration Plane

Control Plane

Data Plane

Cisco Catalyst SD-WAN Solution Elements

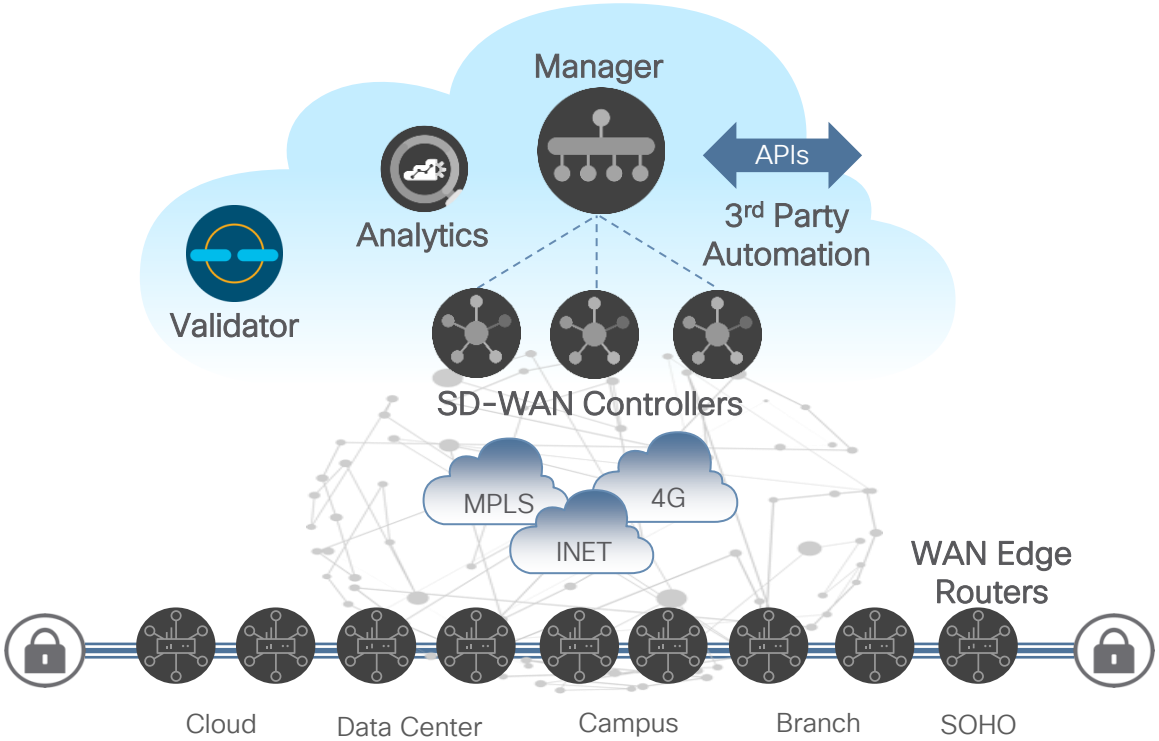


Management Plane

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

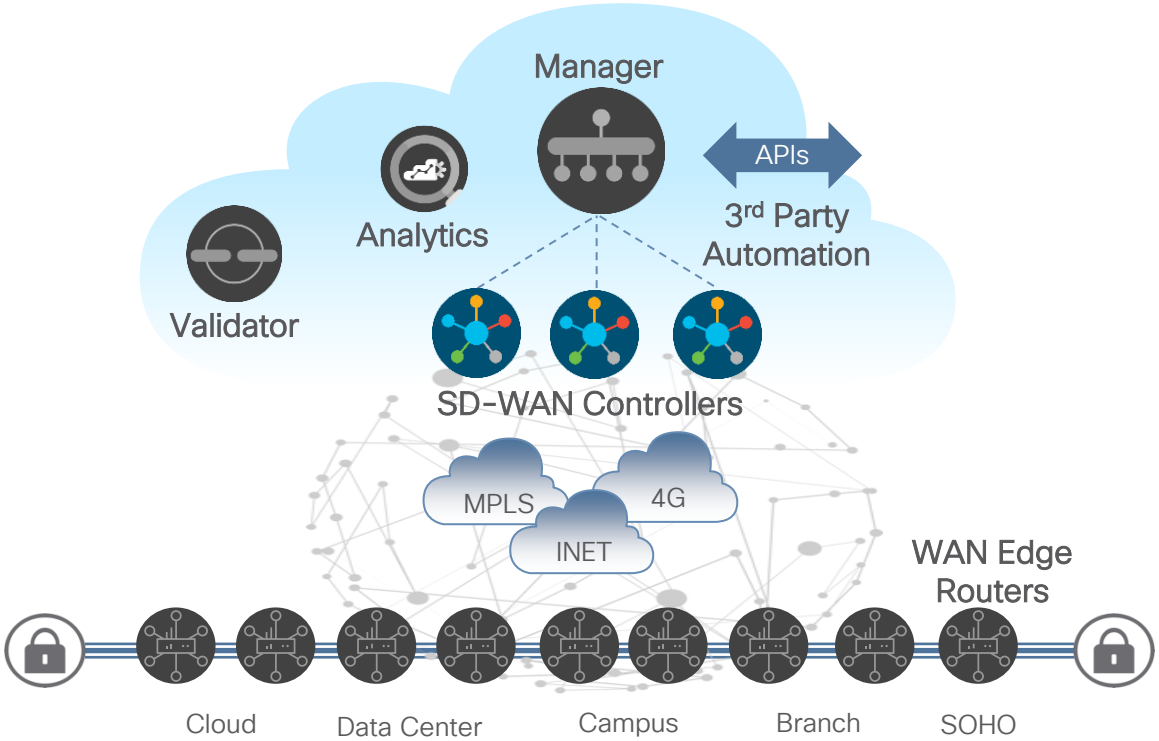


Orchestration Plane

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

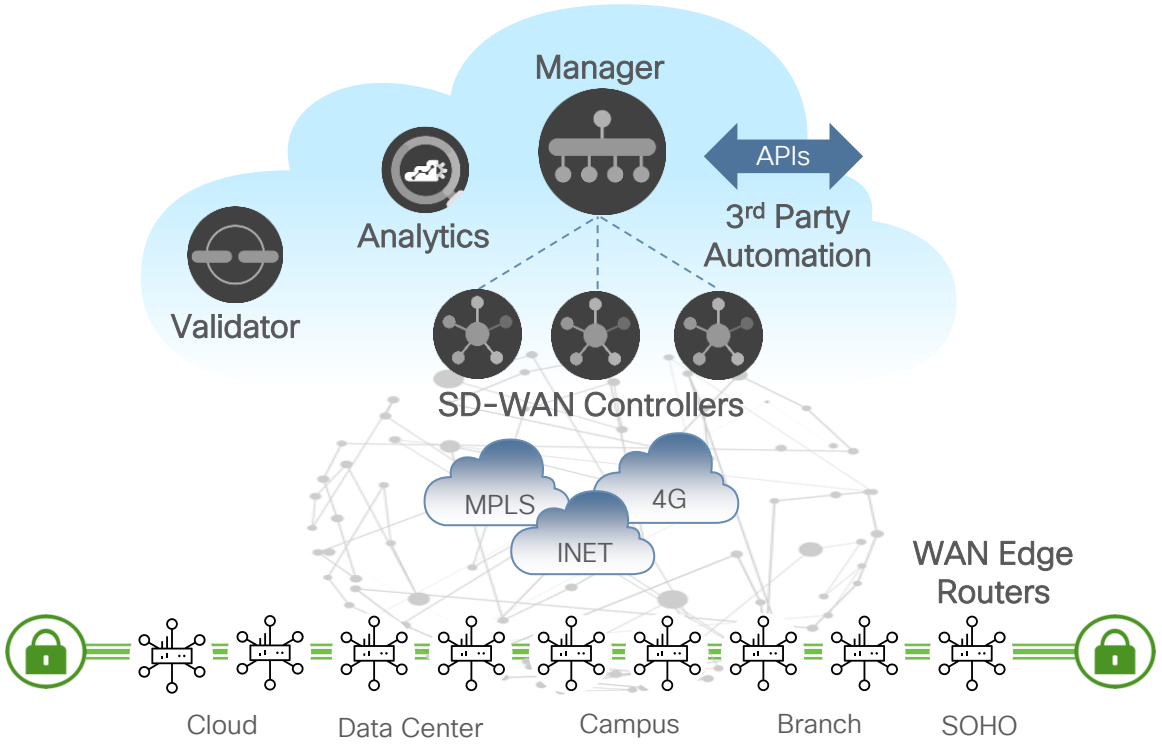


Control Plane

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

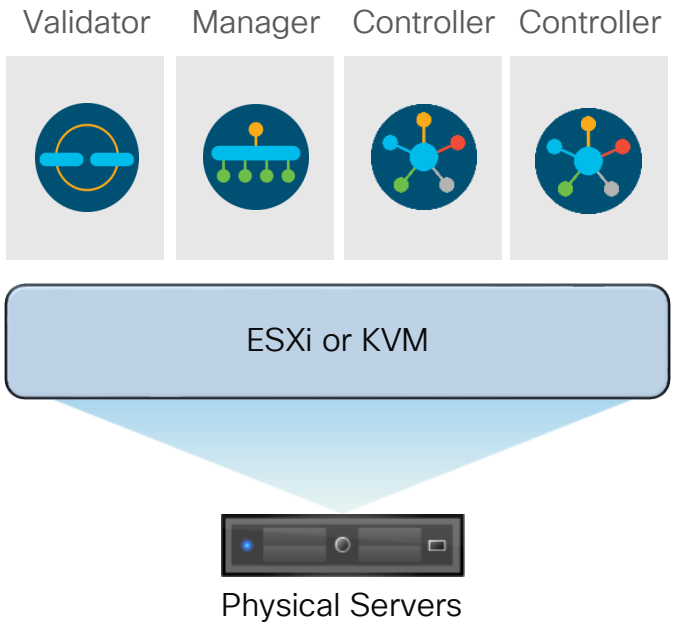
Physical/Virtual

Cisco SD-WAN
WAN Edge

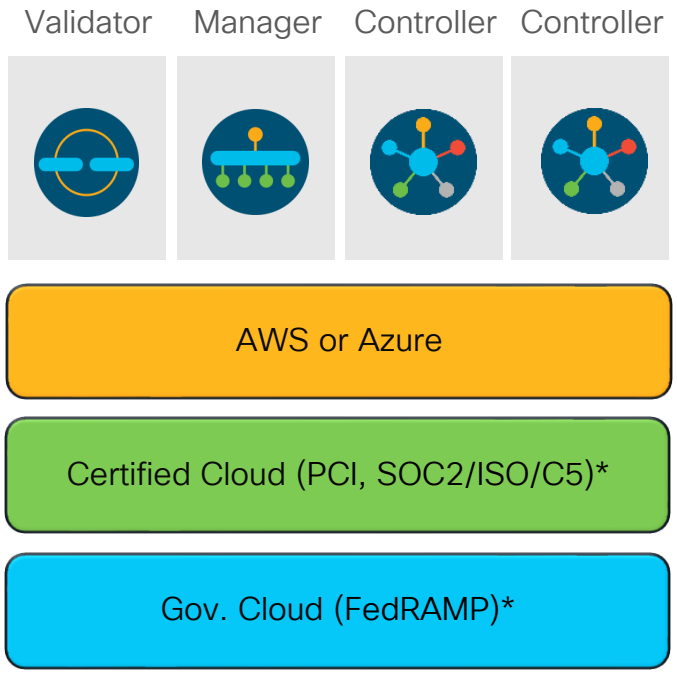
- WAN edge router
- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, and EIGRP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

Controller Deployment Methodology

On-Premise



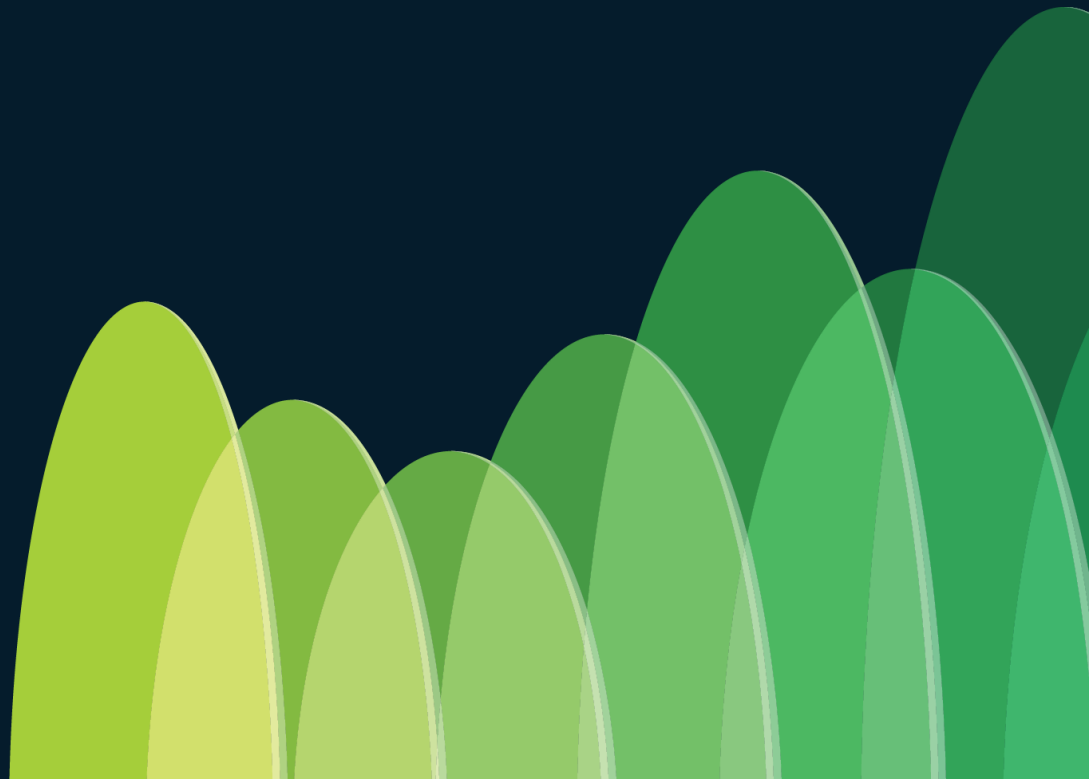
Cisco or MSP/Customer Hosted



VM

*Only Cisco hosted

SD-WAN Features



cisco Live!

Significance of TLOC Color

Color is an abstraction used to identify individual WAN transport

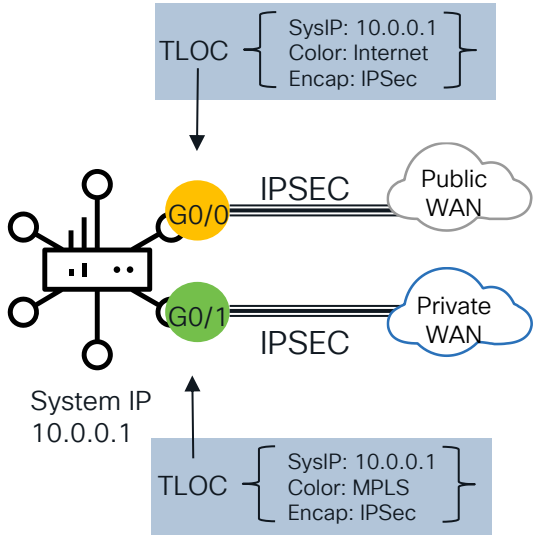
Colors are KEYWORDS not just LABELS

Policy is written based on these

TLOC maps to a physical WAN interfaces

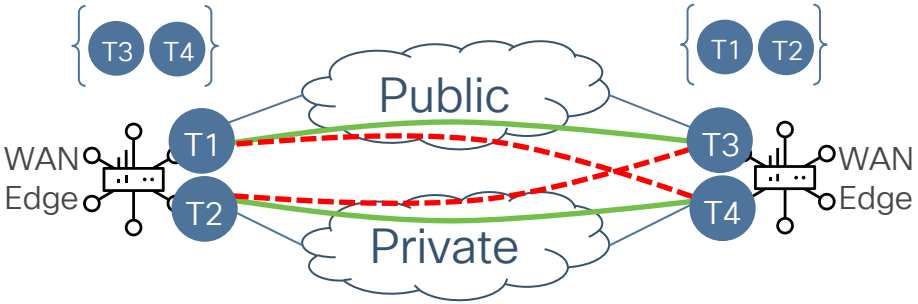
"Color" dictates the use of private-ip vs public-ip (dest) for Tunnel Establishment when there is NAT present

- 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

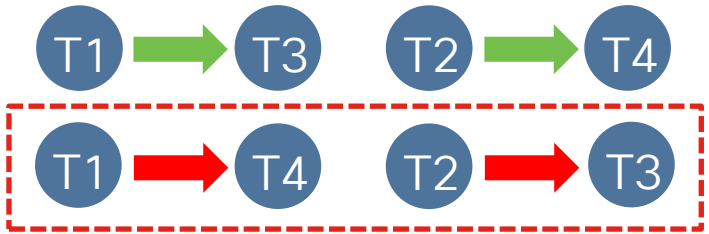


Private Colors	Public Colors
Metro-ethernet	3g
mpls	lte
private1	biz-internet
private2	public-internet
private3	blue
private4	green
private5	red
private6	gold
	silver
	bronze

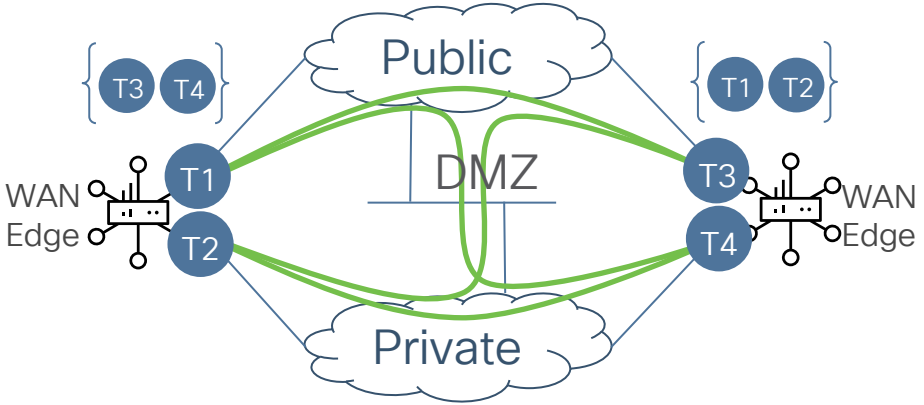
Transport Colors



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

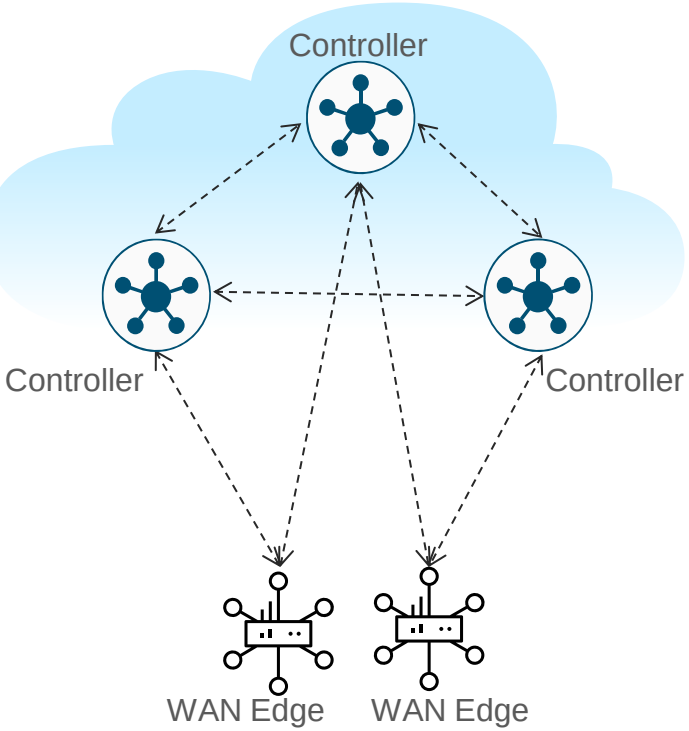


Color restrict will prevent attempt to establish IPSec tunnel to TLOCs with different color

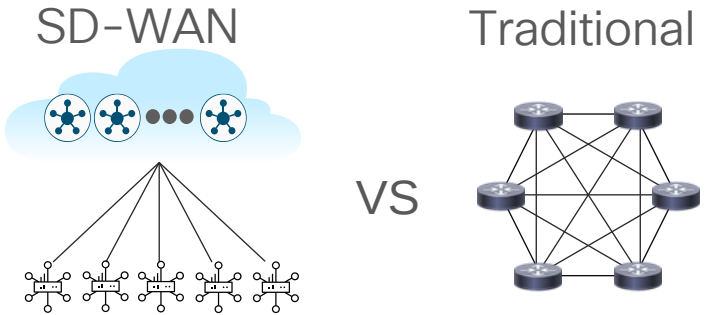


T1, T3 – Public Color T2, T4 – Private Color

Overlay Management Protocol (OMP)

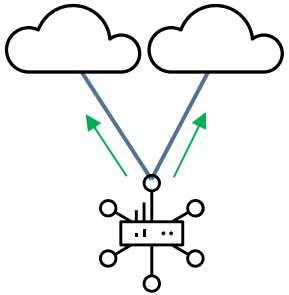


- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane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

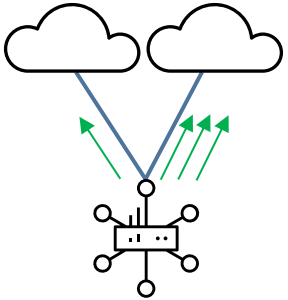


Fabric Communication

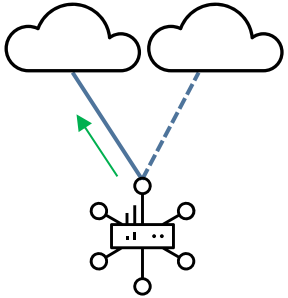
Per-Session Load-sharing
Active/Active



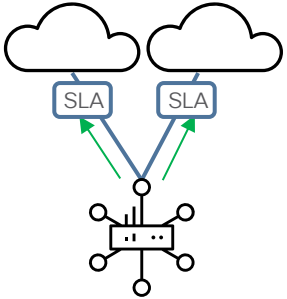
Per-Session Weighted
Active/Active



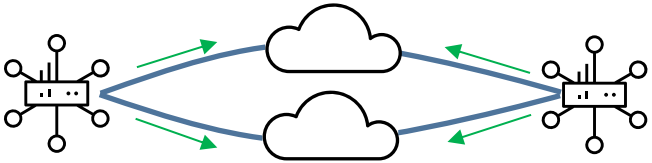
Application Pinning
Active/Standby



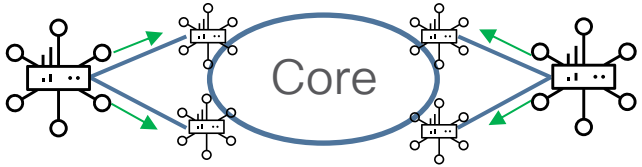
Application Aware Routing
SLA Compliant



Single-hop Fabric

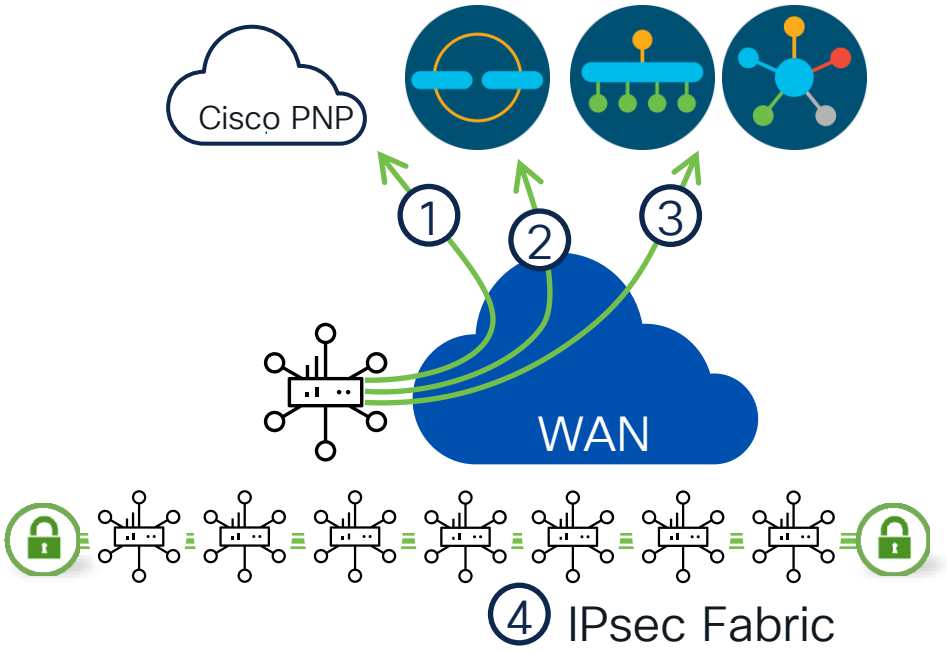


Multi-Region Fabric



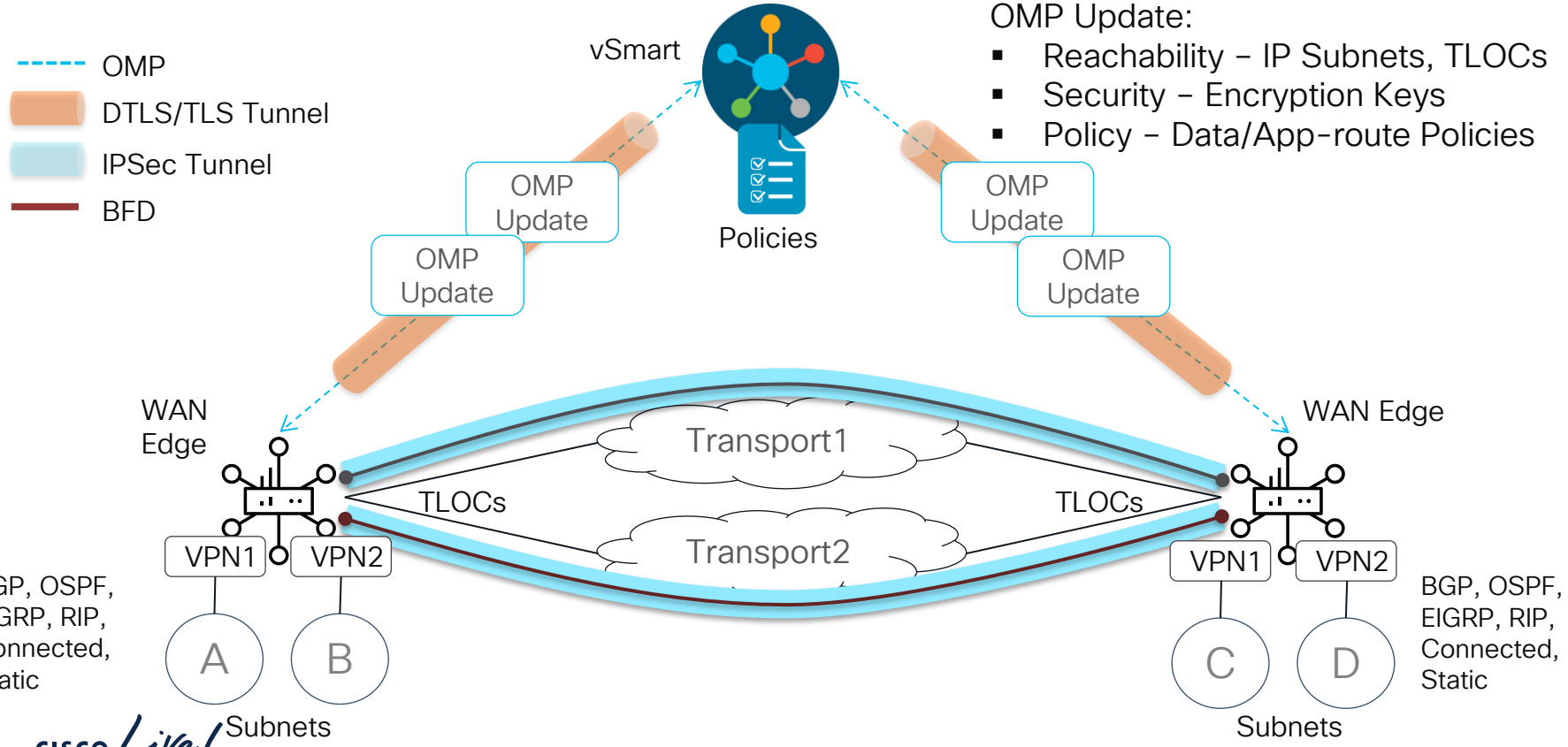
Lets bring it up

Automated, Zero-Touch Onboarding

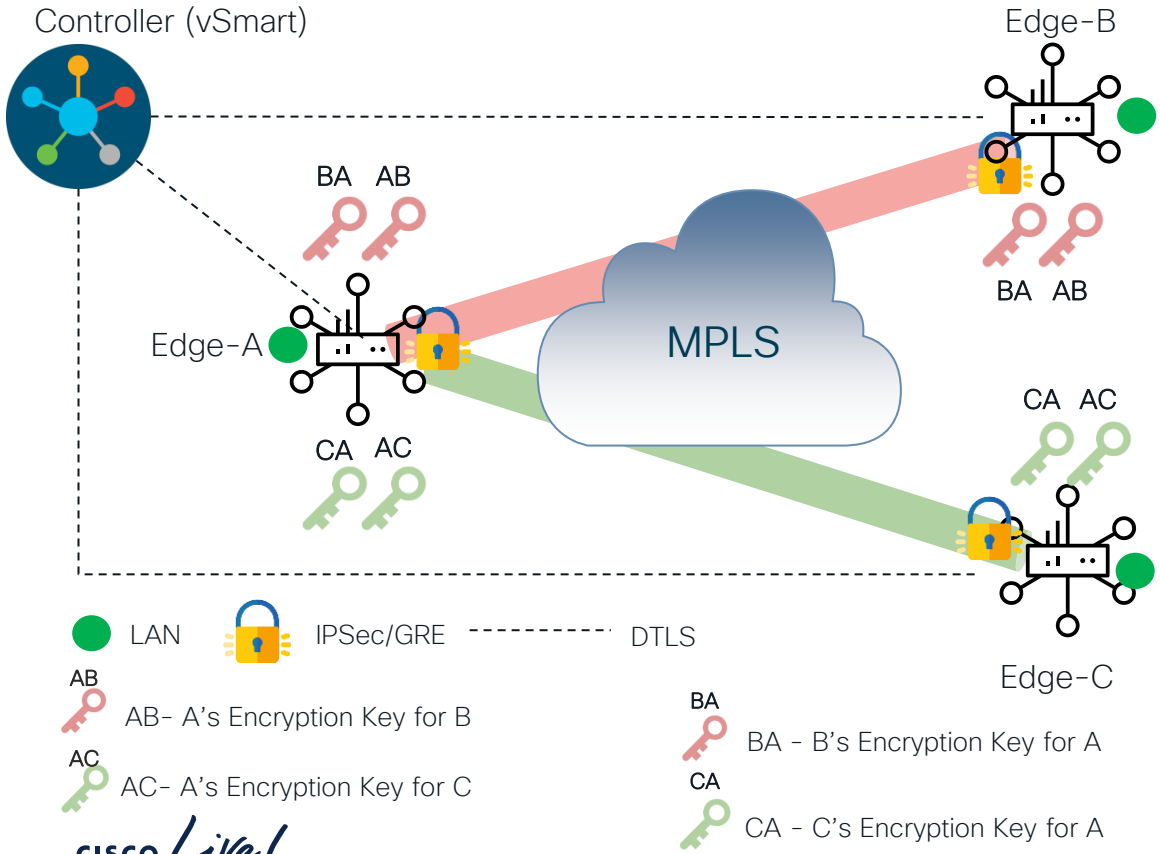


- SD-WAN appliance will onboard itself into the SD-WAN fabric automatically with no administrative intervention.
- Connect the SD-WAN appliance to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.
- If no DHCP service is available, then bootstrap file is an option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

Fabric Operation Walk-Through

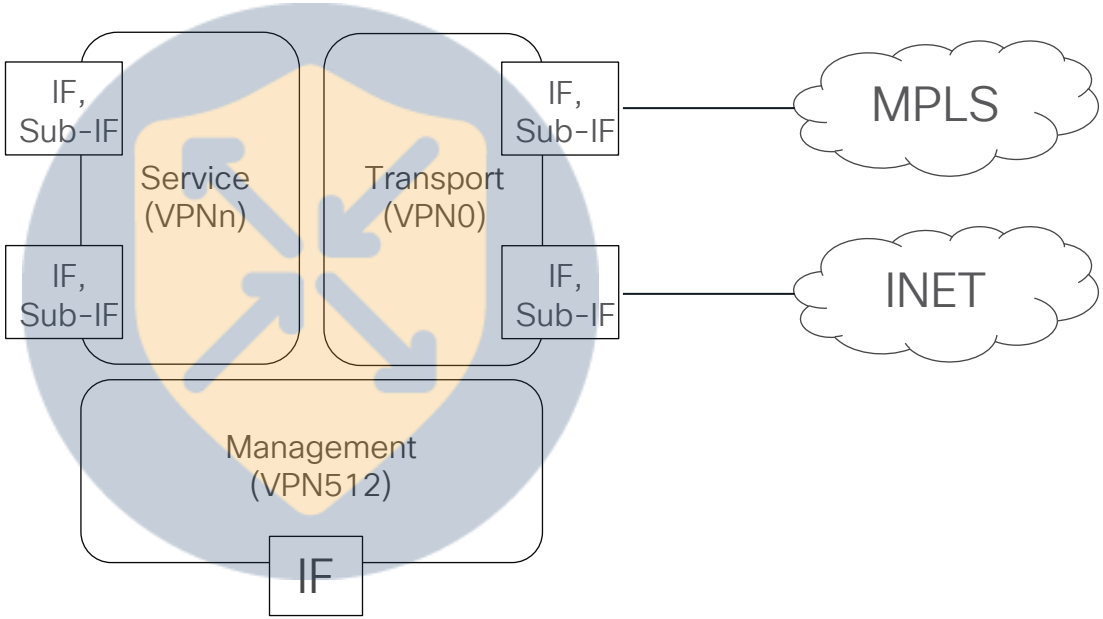


Data Plane Privacy (Pairwise)



- 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")

Cisco SD-WAN VPNs (VRFs)

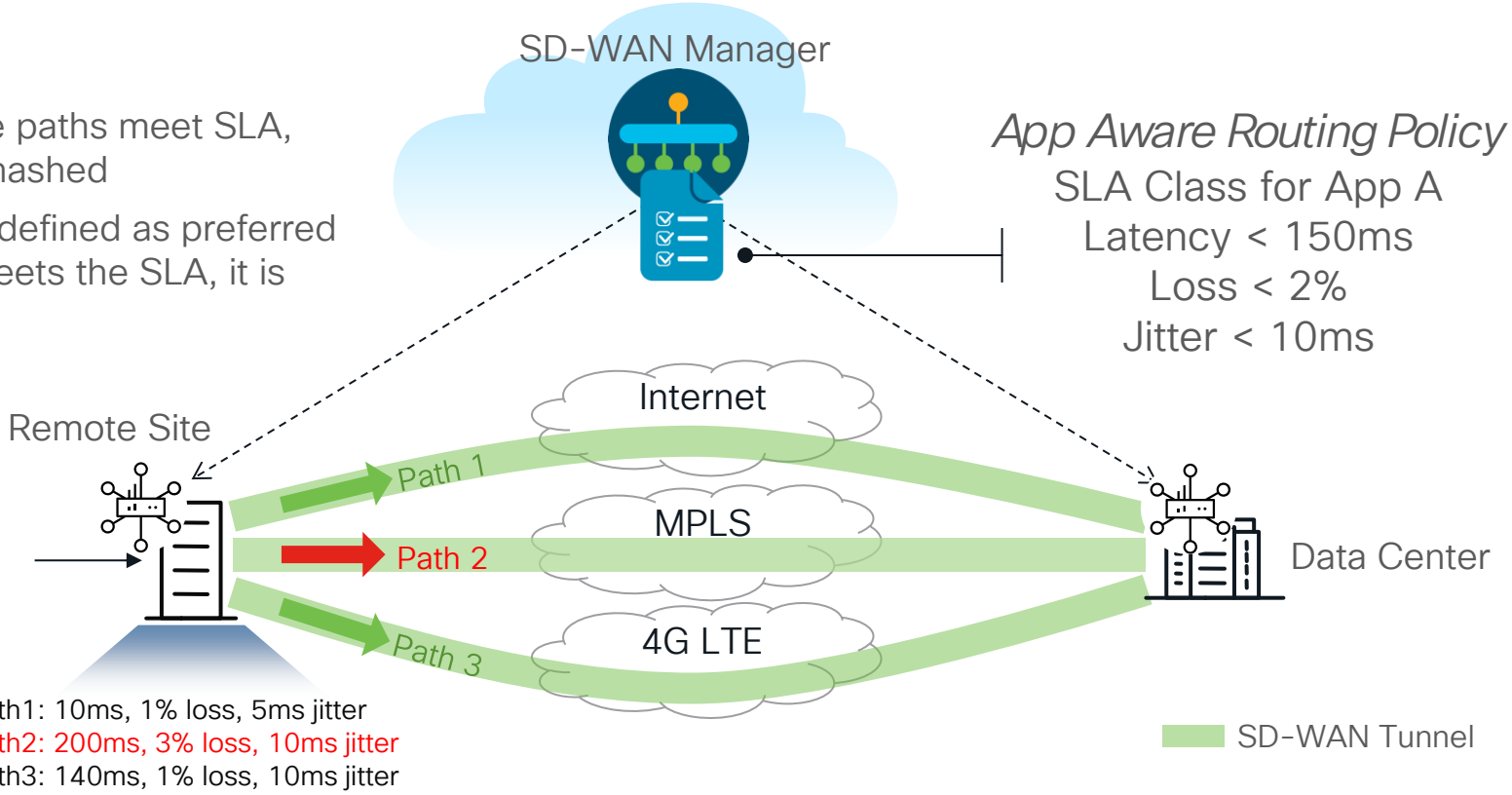


- VPNs are isolated from each other, with each VPN has its own forwarding table
- Reachability within VPN is advertised by OMP
- VPN0 is reserved for WAN uplinks (Transport)
- VPN512 is reserved for Management interfaces
- VPNn represents user-defined LAN segments (Service)

Application Aware Routing

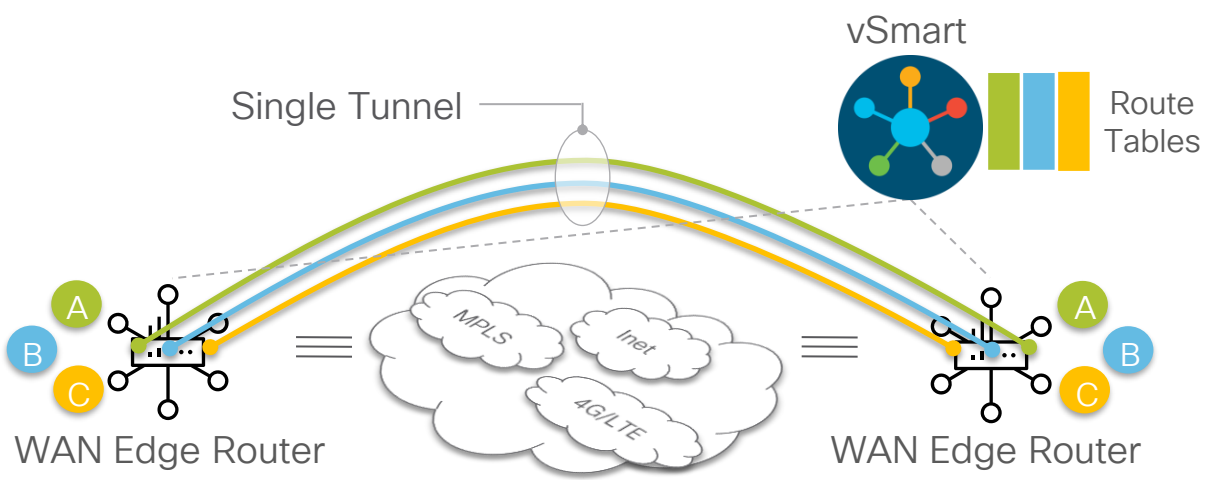
Learn more about policy watch BRKENT-2043

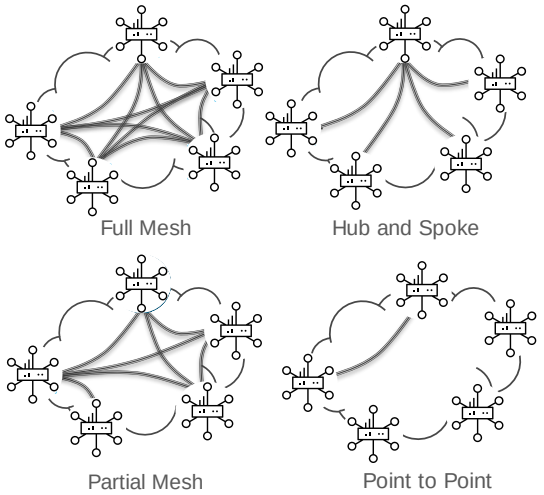
- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



Security features

End-to-End Segmentation with Multi-Topology

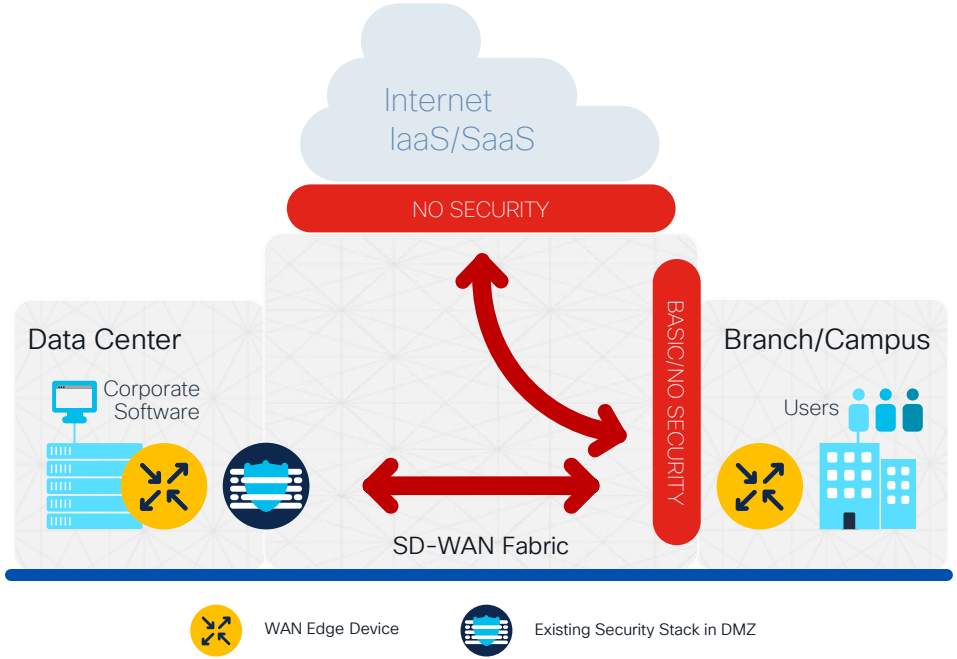




Segment connectivity across the SD-WAN fabric without reliance on underlay transport

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

How SD-WAN Exposes New Security Challenges



Internal & External Threats

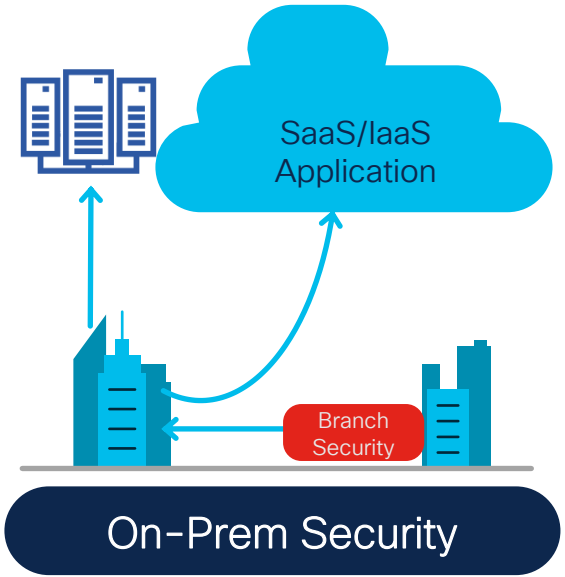
External

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

Internal

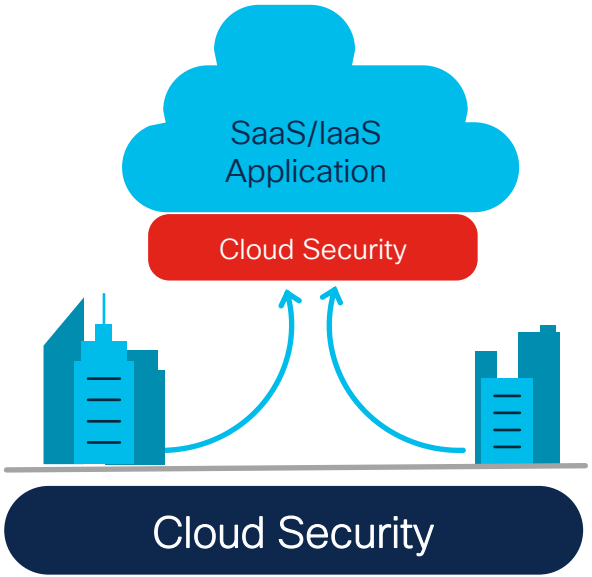
- Untrusted access (malicious insider)
- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)

Relevant Security Models. Driving towards SASE



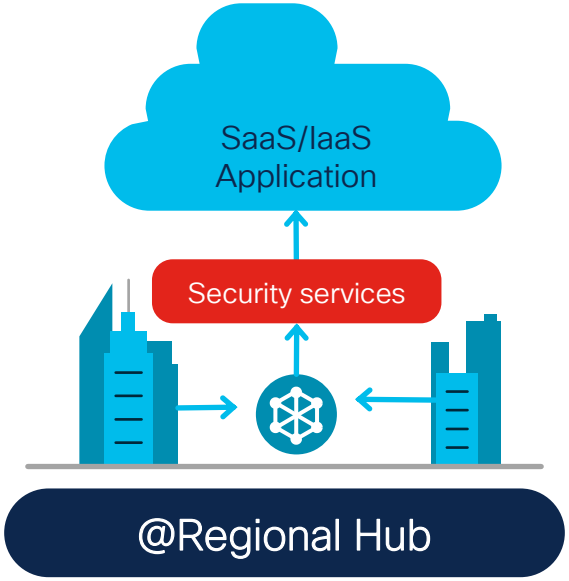
On-Prem Security

Thick branch with Routing and Security



Cloud Security

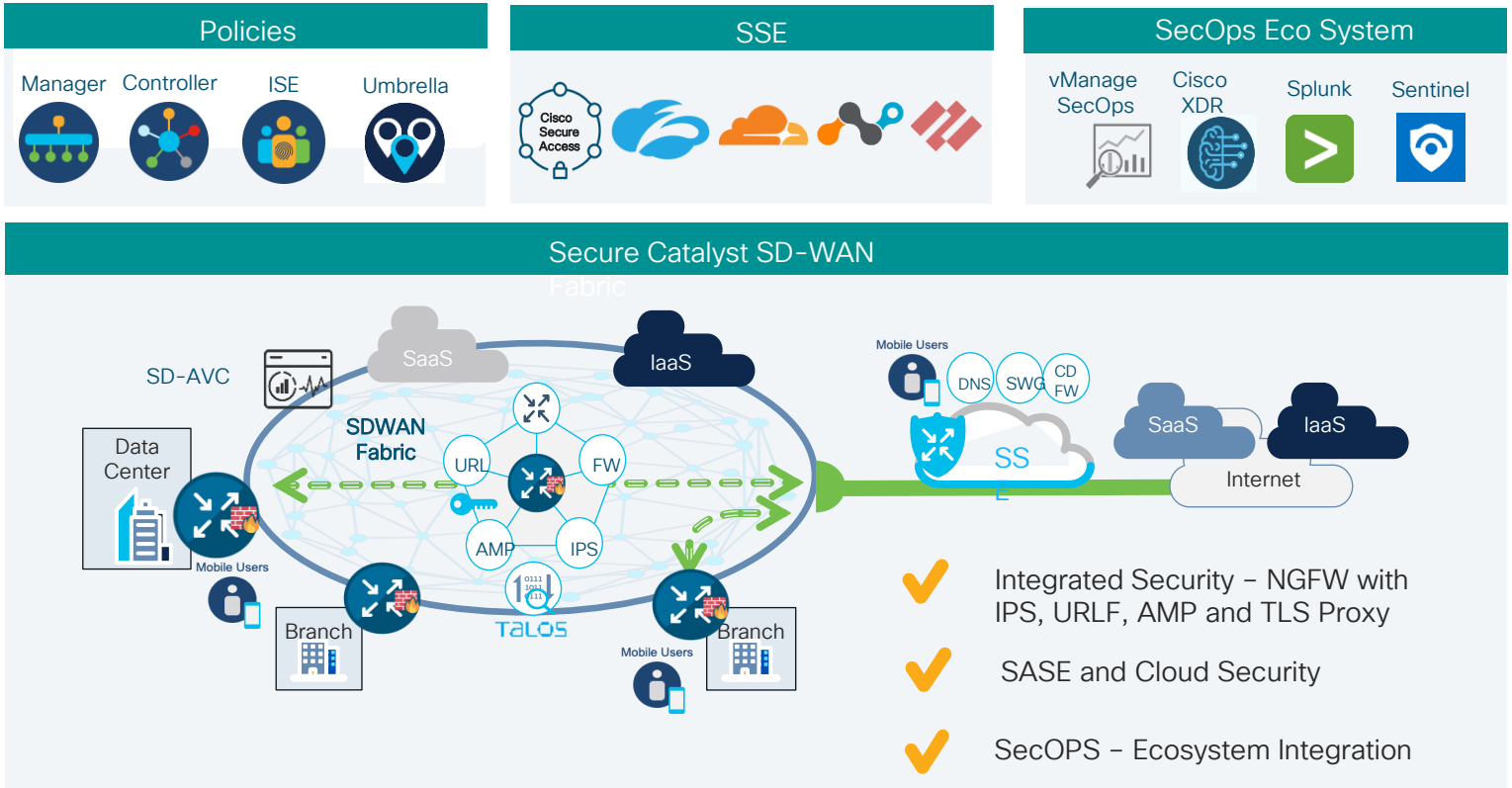
Thin branch with security in the cloud



@Regional Hub

Security Services on a Regional Hub

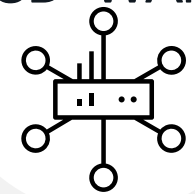
Catalyst SD-WAN Security



Cisco Catalyst SD-WAN Security & SASE Solution

Consistent across on-prem and cloud

Cisco SD-WAN



< 8G Ram

Cisco Security

NextGeneration 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

Catalyst SD-WAN / Splunk Integration - Capabilities

SoC Dashboard

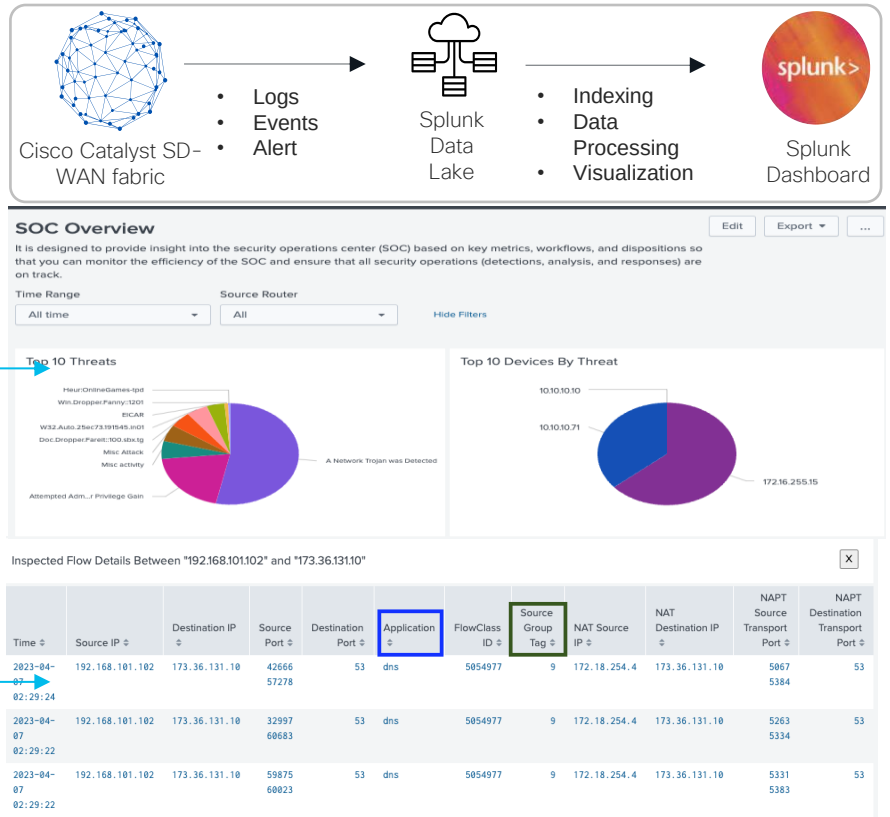
- Holistic view of all security events
- Real time updates
- Top Threats & Policy Hits
- Drill down to flow level

Threat Management

- Visualize user to threat mapping
- List all IPS and Malware events
- > 1 year Data Retention

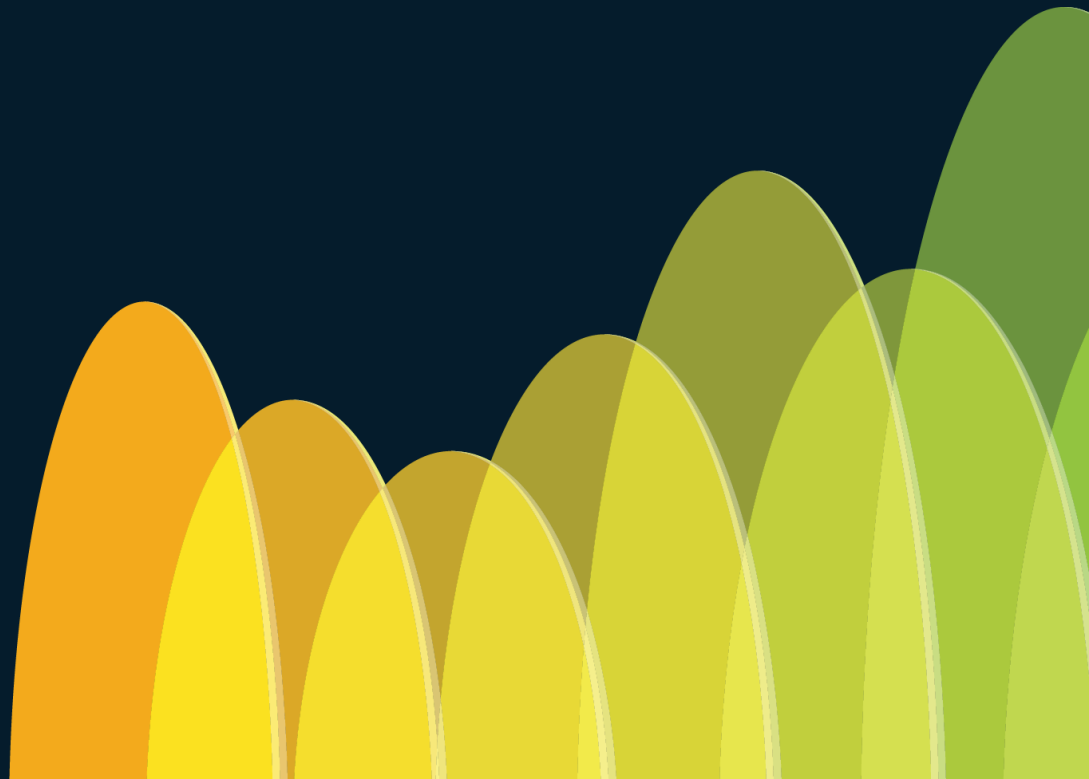
Flow Analysis

- Global map view
- Top applications accessed
- Top network talkers



App URL: https://splunkbase.splunk.com/app/6657
App Add-on: https://splunkbase.splunk.com/app/6656
HSL Add-on: https://splunkbase.splunk.com/app/6872

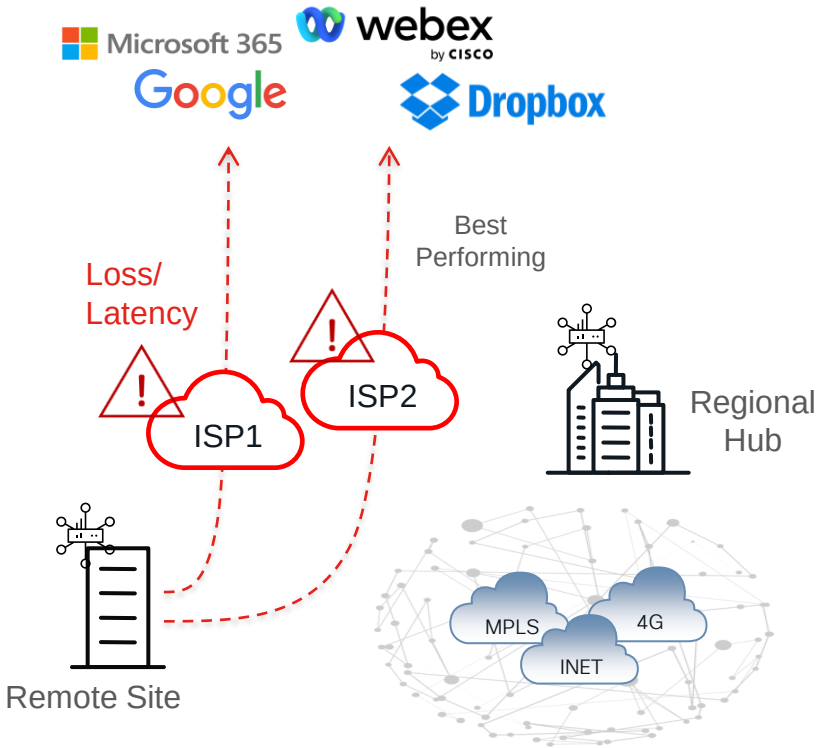
Cloud OnRamp for SaaS



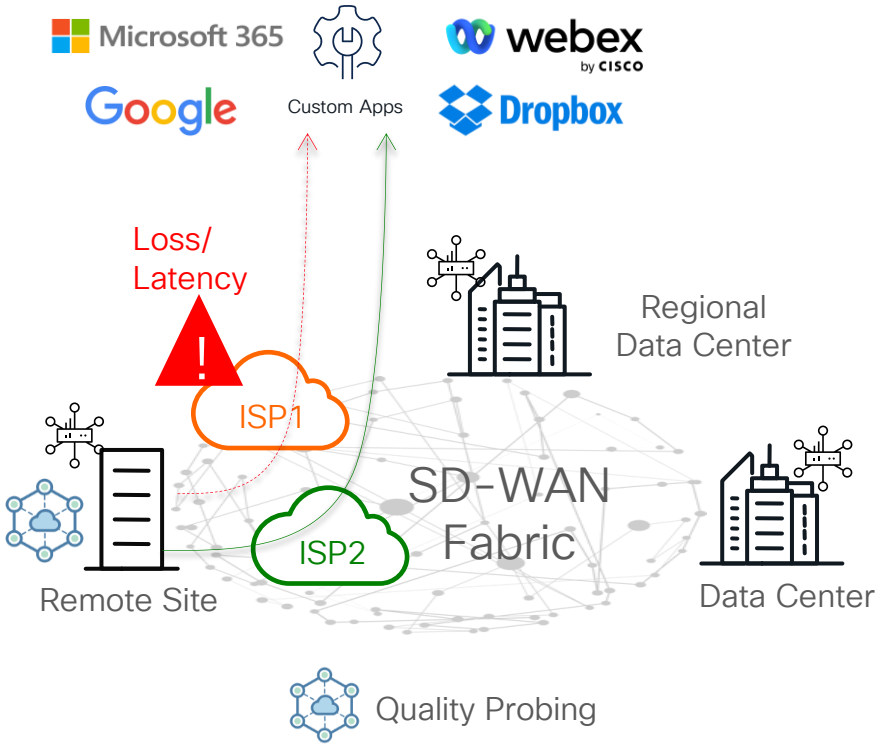
cisco Live!

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 ?

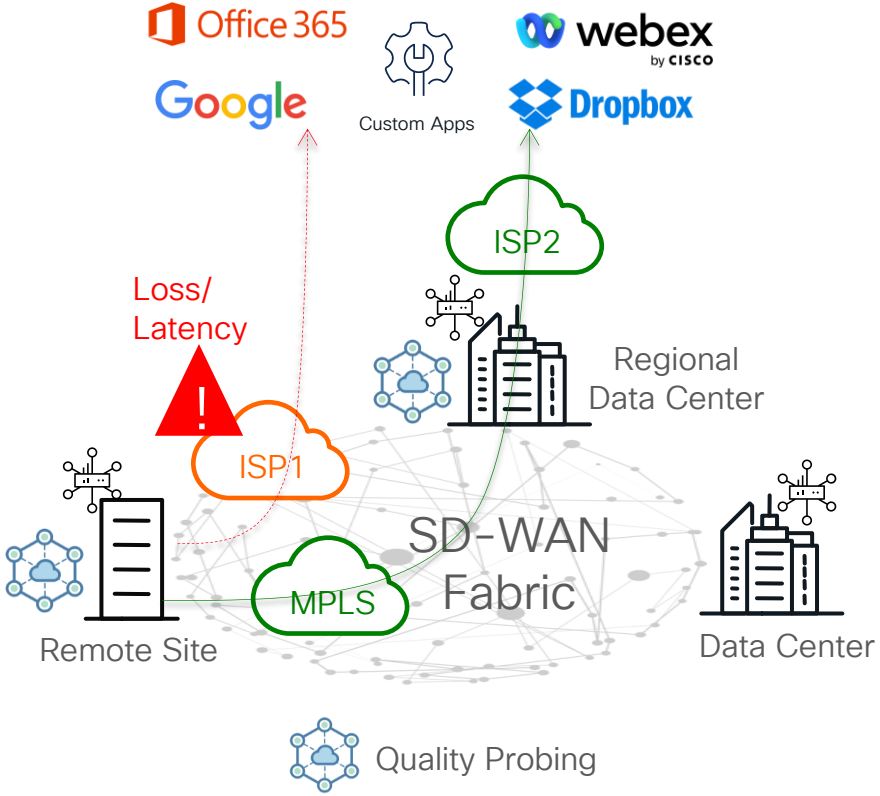


Cloud onRamp for SaaS – Internet DIA



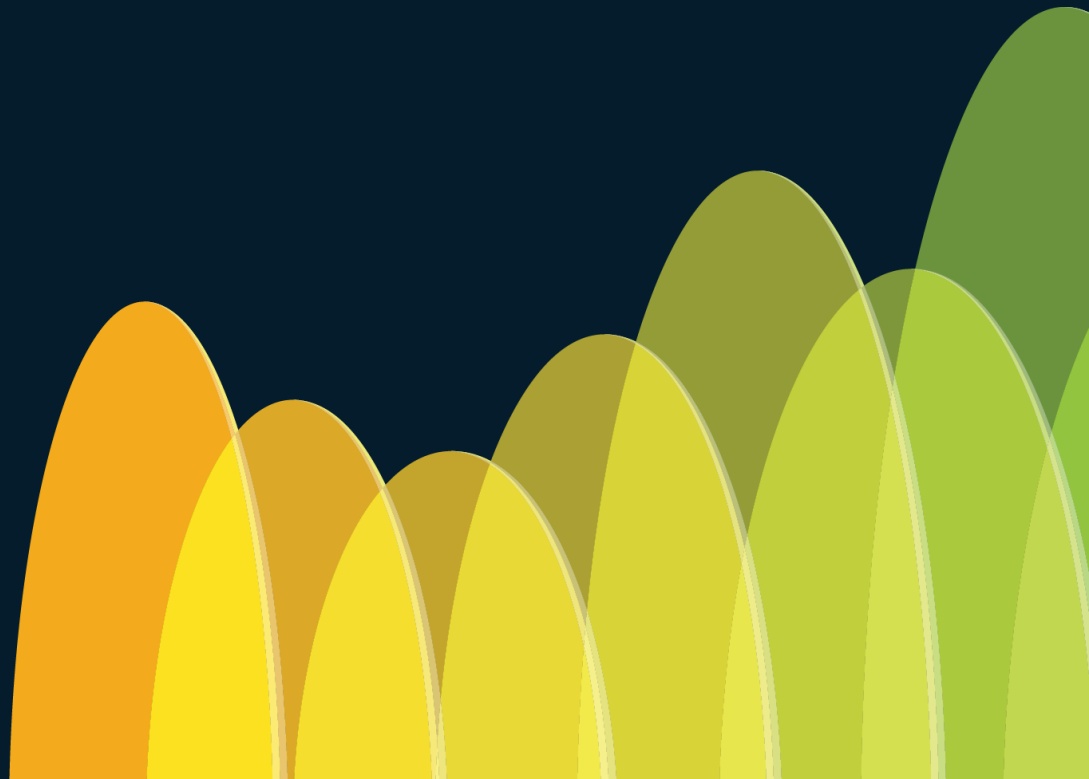
- WAN Edge router at the remote site performs quality probing for selected SaaS applications across each local DIA exit
  - Simulates client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
- Local DIA exit with better vQoE score is 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 MultiCloud



cisco Live!

Cisco SD-WAN Cloud Hub- Use Cases

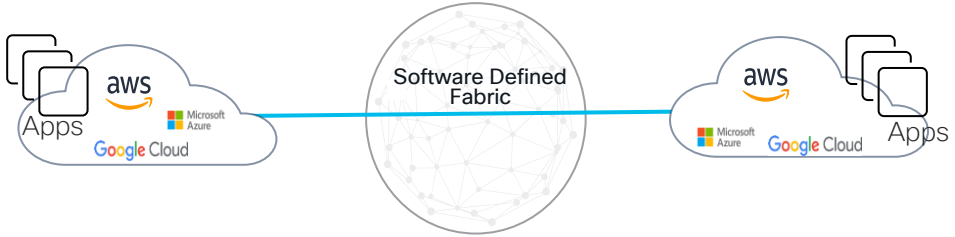
= Cisco SD-WAN virtual router hosted at Cloud Service Provider POP

= Cisco SD-WAN router on-premises

Enterprise Site to Cloud

Enterprise Site to Enterprise Site

Cloud to Cloud/Inter-Cloud



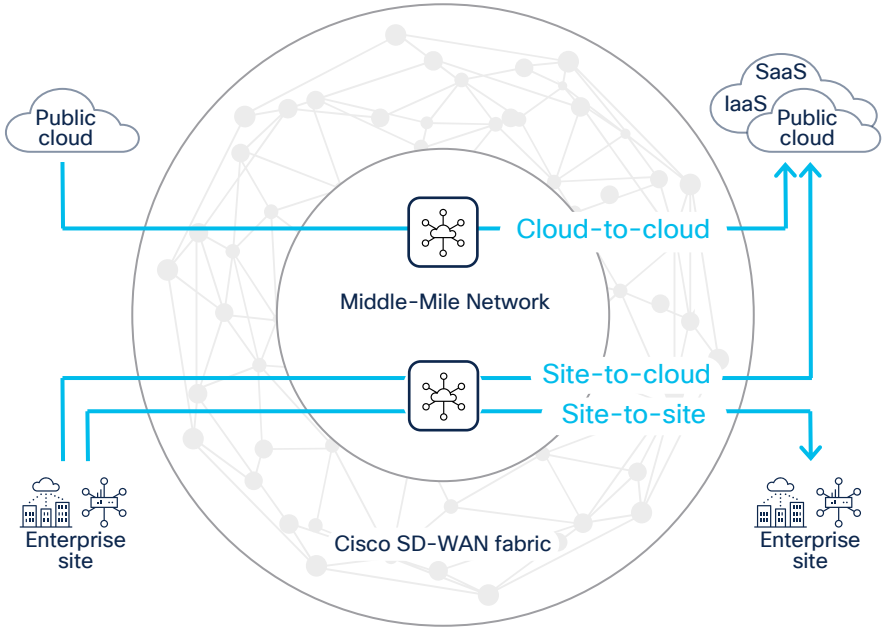
Cisco SD-WAN simplifying connectivity with fabric extension to cloud providers, it is building a programable site-to-cloud, Region to Region, site-to-site and cloud to cloud connectivity using cloud providers Native contracts and backbone

= Cisco SD-WAN virtual router

= Cisco SD-WAN router on-premises

Megaport EQUINIX aws Cloud WAN Google Cloud NCC Microsoft Azure

Cisco SD-WAN Middle-Mile Optimization



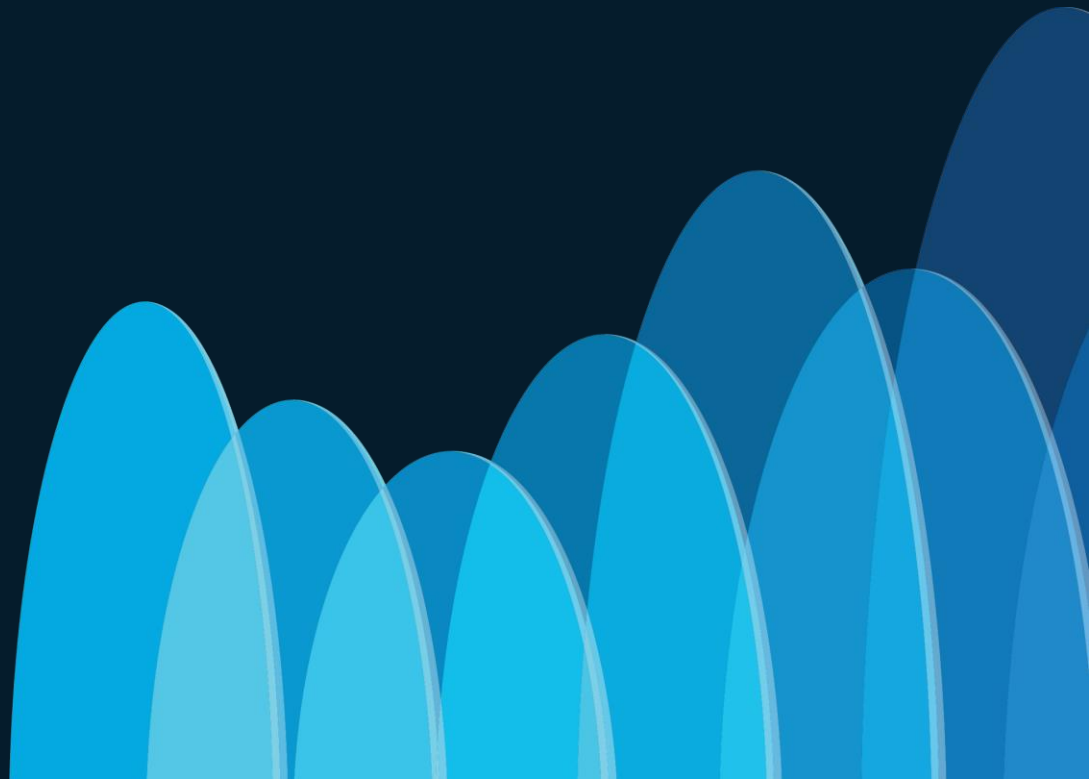
Flexibility
All or selective traffic sent based on type or app

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?

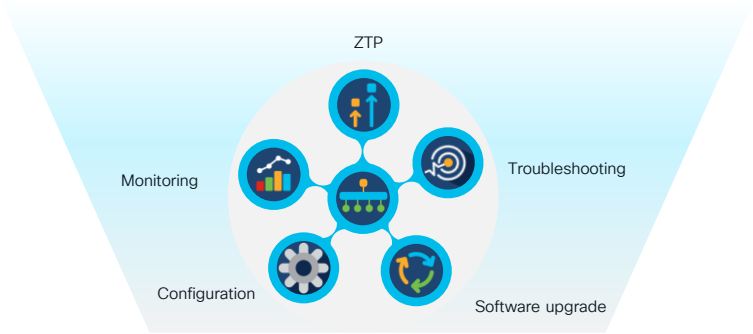


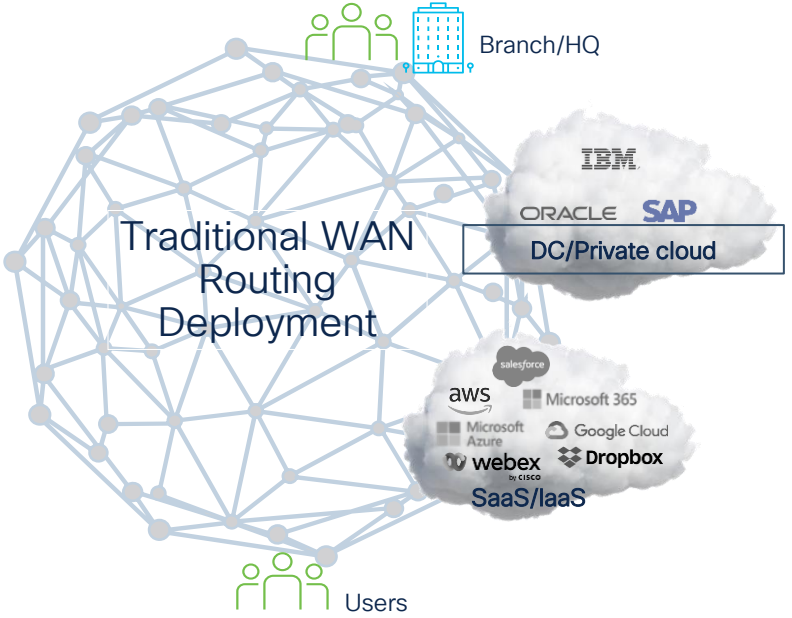
Learn more attend
BRKENT-1039

Introducing SD-Routing

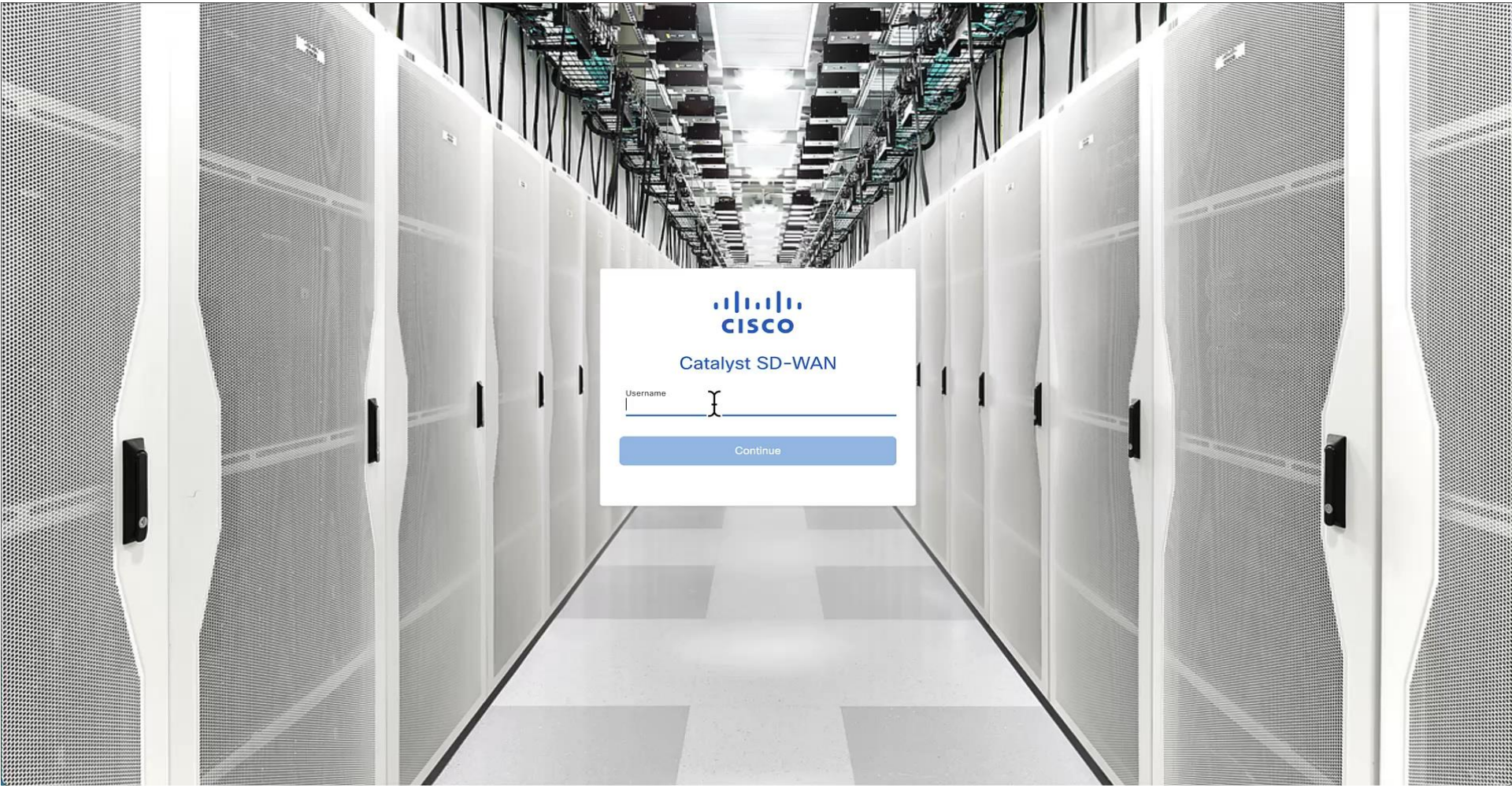
Transform the platform experience

Catalyst SD-WAN Manager



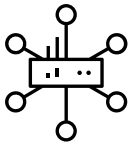


Demo



Key Takeaways

Cisco SD-WAN



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

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

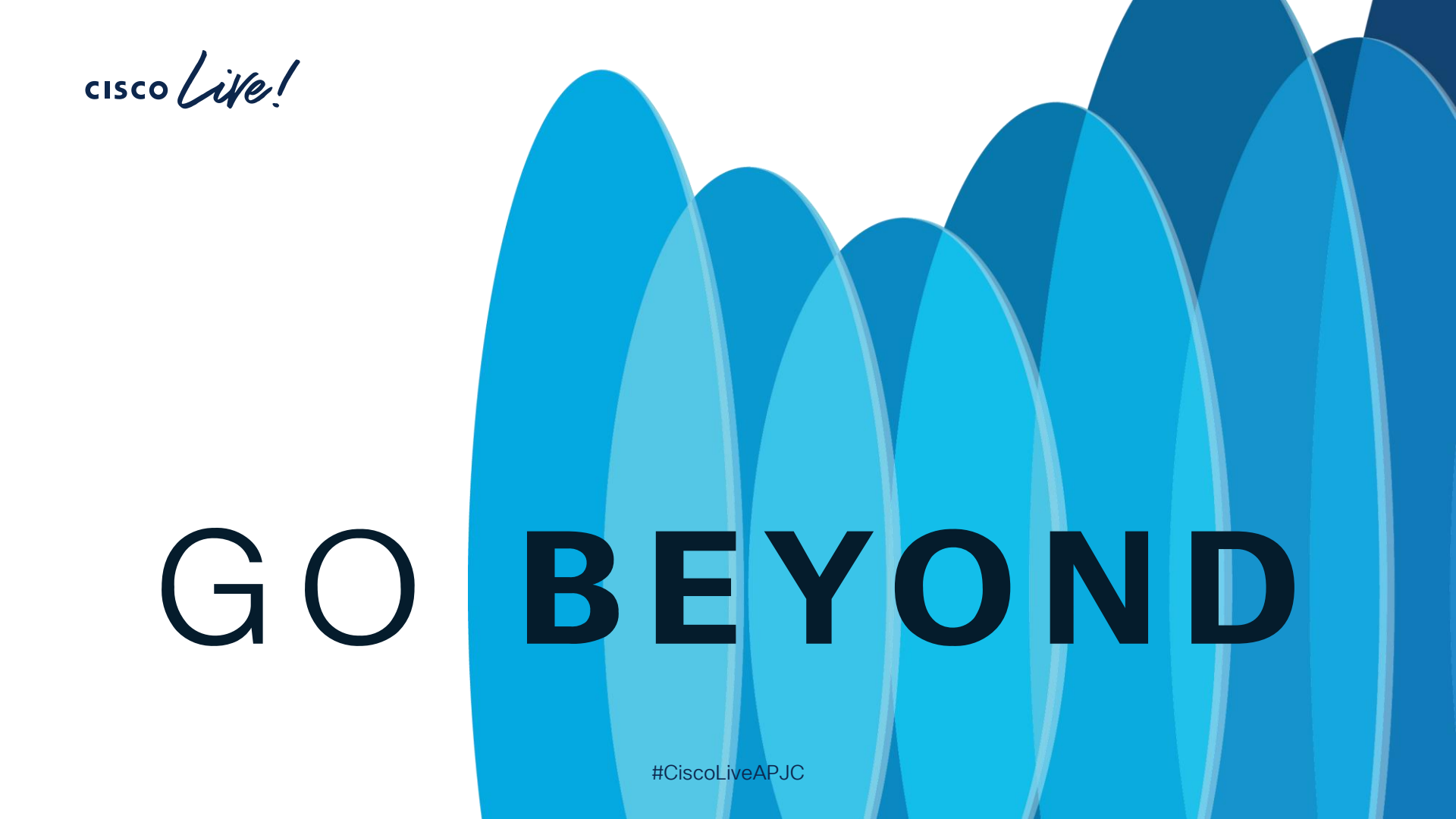
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

Continue your education

- Visit the Cisco Stand 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


cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC