The bridge to possible

SD-WAN: Start here

Subtitle goes here

Lars Granberg, Technical Marketing Engineer
@larslilja

BRKENT-2108

Cisco Webex App

Questions?

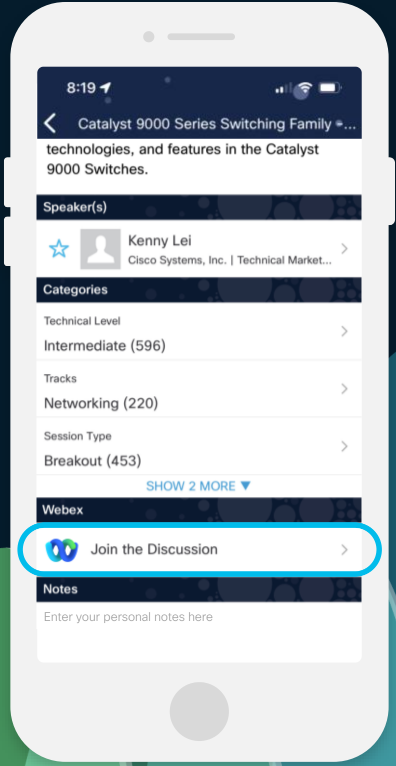
Use Cisco Webex App to chat
with the speaker after the session

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
by the speaker until June 7, 2024.

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



8:19

Catalyst 9000 Series Switching Family ▪...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Agenda

- 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

About me

Copenhagen, Denmark

Technical Marketing Engineer
SDWAN And Routing Business Unit

Before that:

- Systems Architect
- Technical Solutions Architect
- Systems Engineer

Cisco since 2014

Cisco Live Speaker

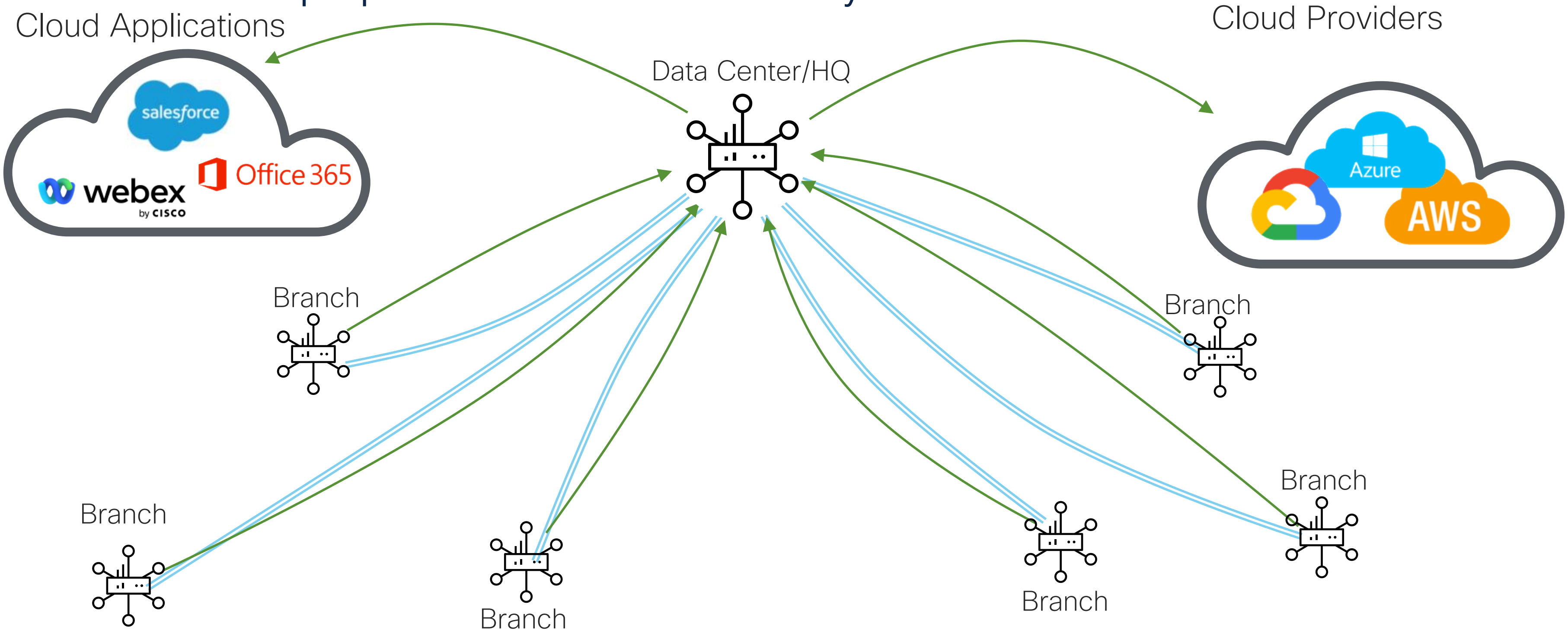
IT and networking since 2003

SD-WAN – This is it.

Why SD-WAN?

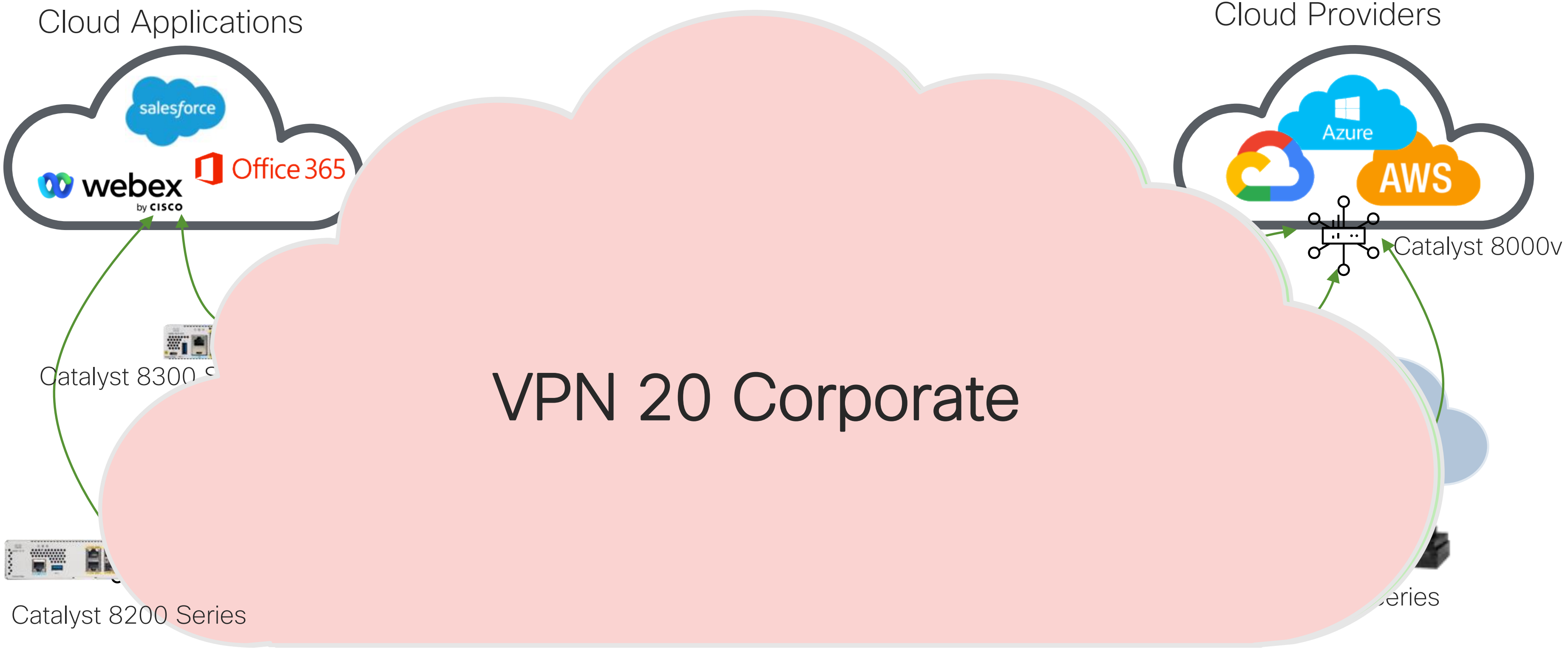
The Hardware Based WAN of Yesterday

Doesn't Keep up with the Needs of Today



Learn more attend BRKENT-2139

Cisco SD-WAN: Software Approach



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

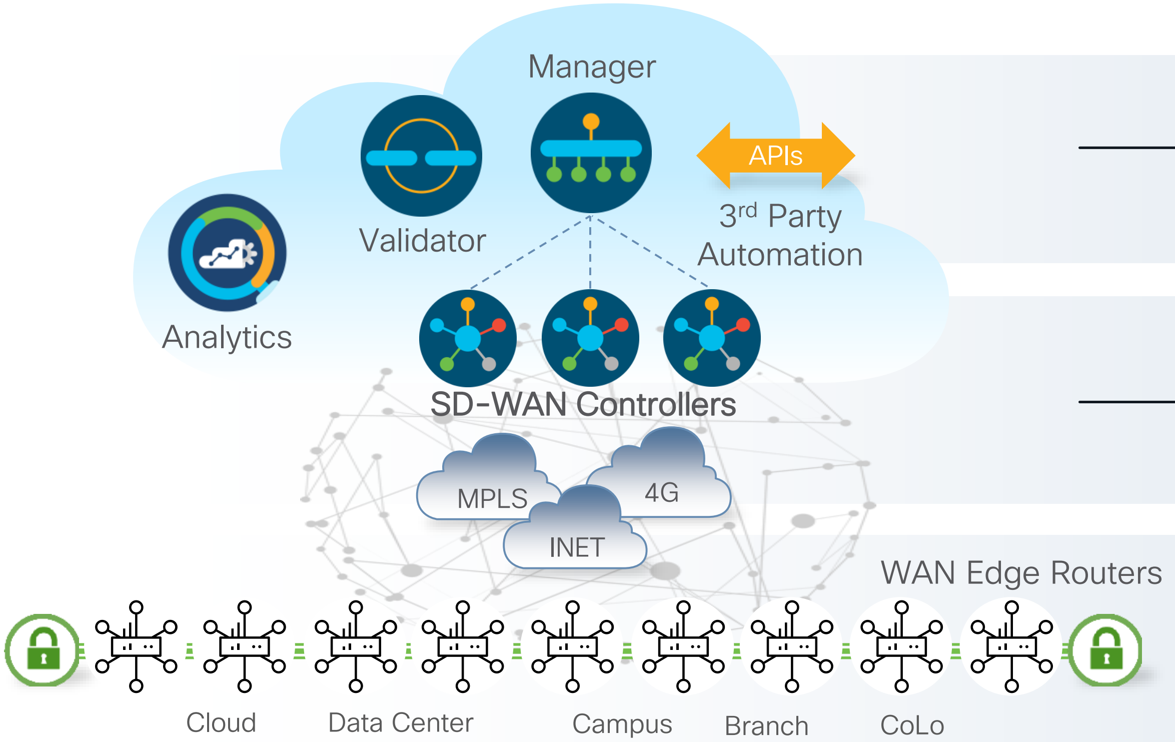
Solution Architecture

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

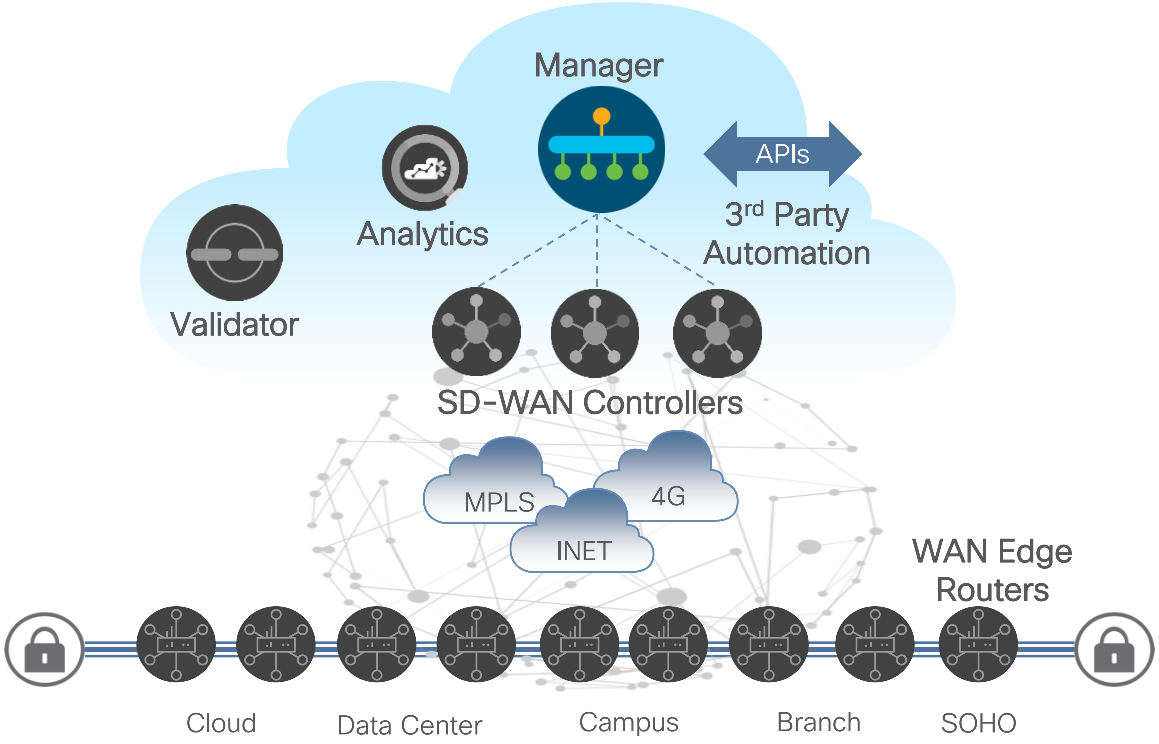


Management/
Orchestration Plane

Control Plane

Data Plane

Cisco Catalyst SD-WAN Solution Elements

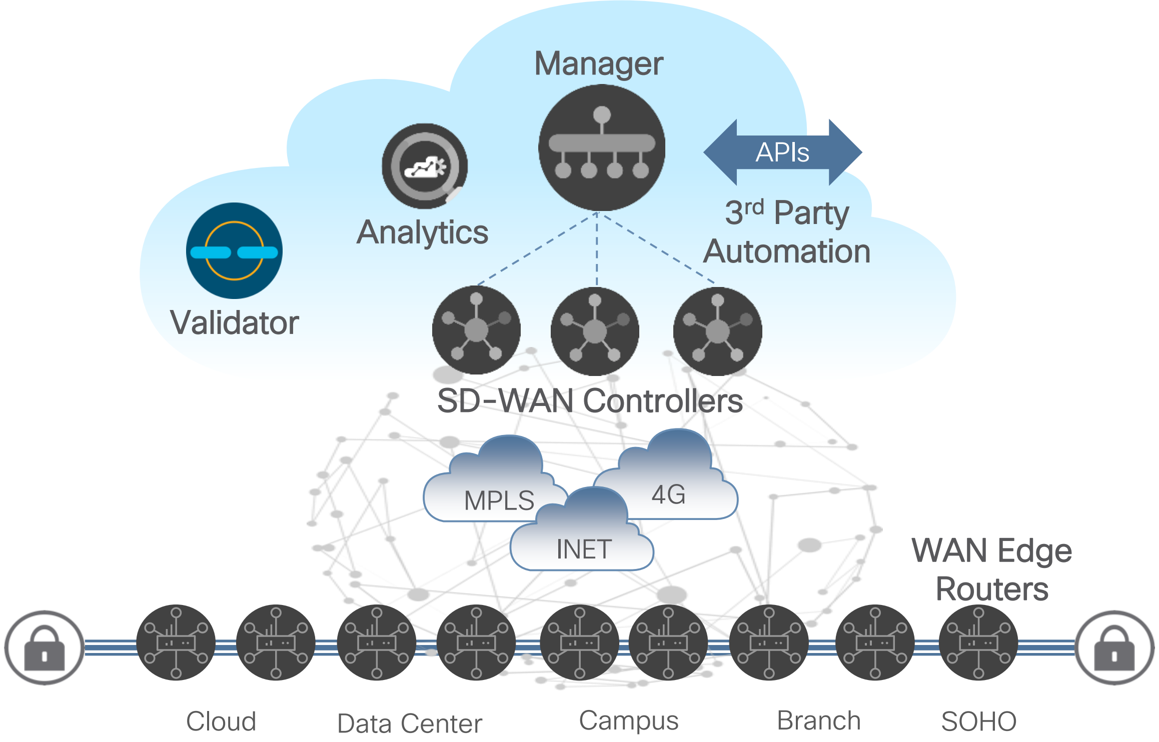


Management Plane

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

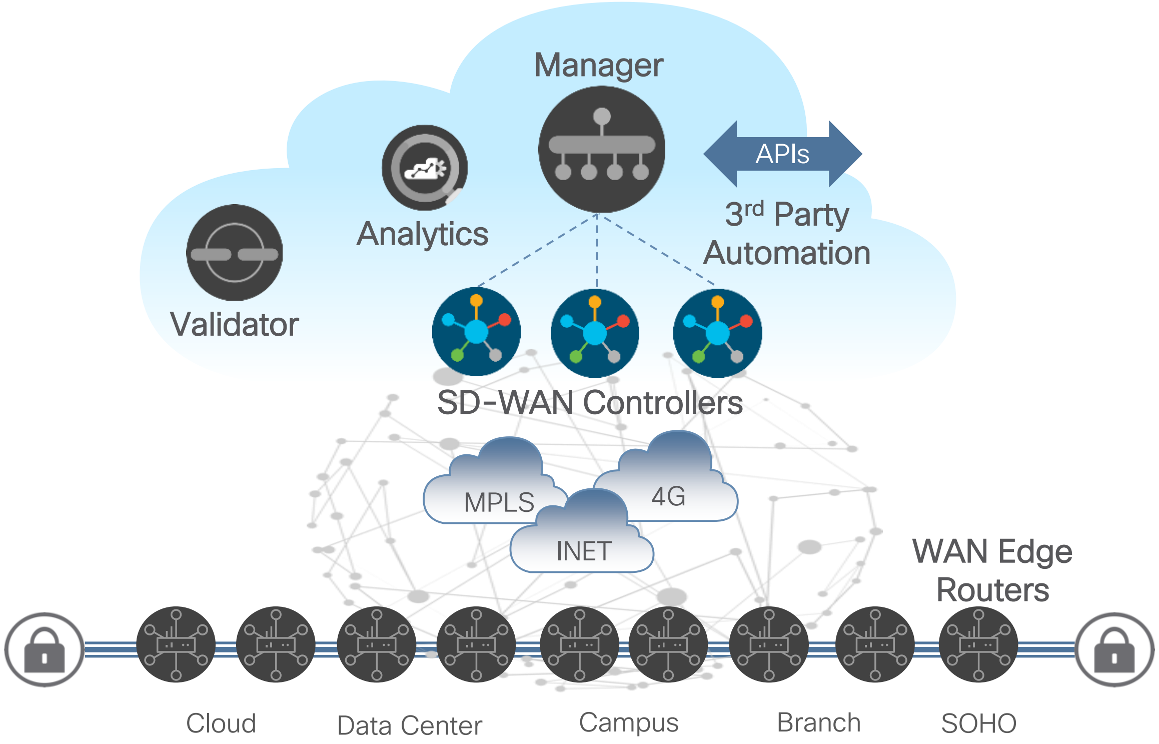


Orchestration Plane

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

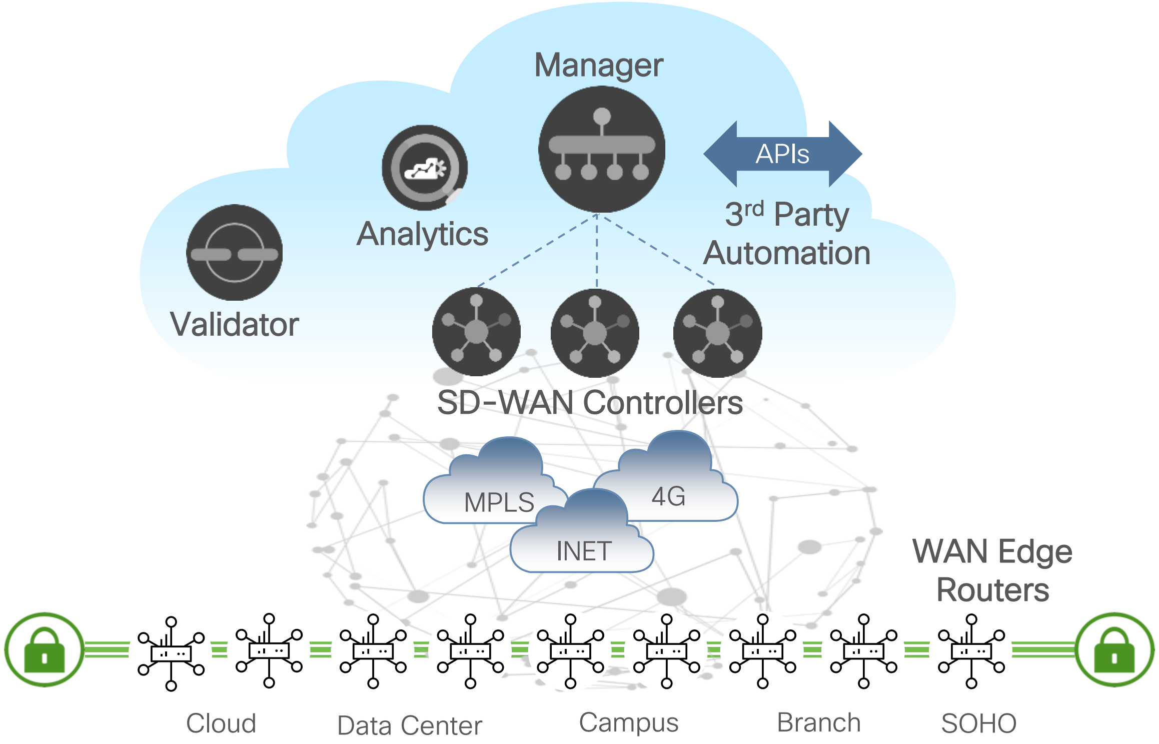


Control Plane

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



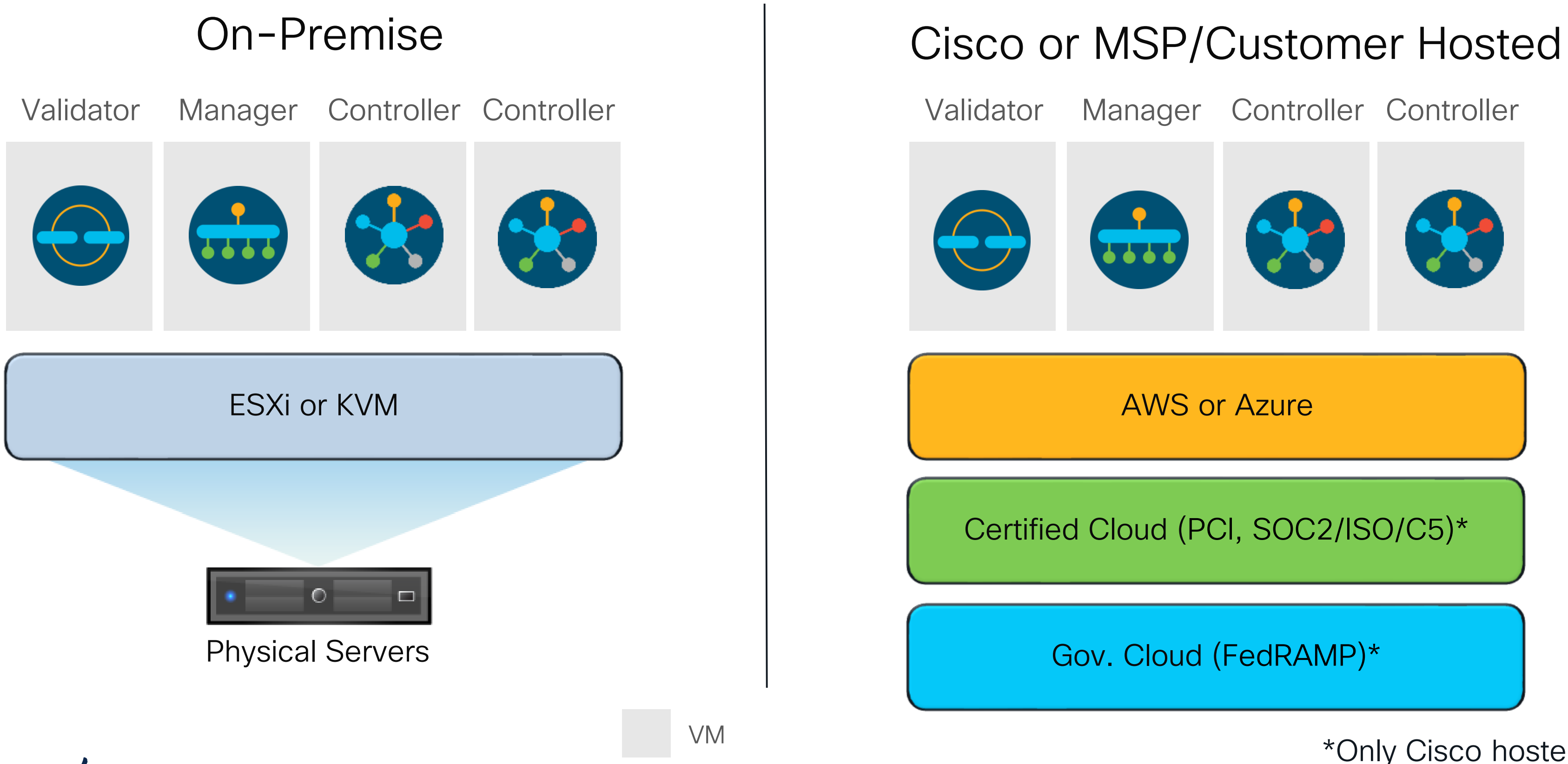
Data Plane

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

Validator Manager Controller Controller

ESXi or KVM

Physical Servers

Cisco or MSP/Customer Hosted

Validator Manager Controller Controller

AWS or Azure

Certified Cloud (PCI, SOC2/ISO/C5)*

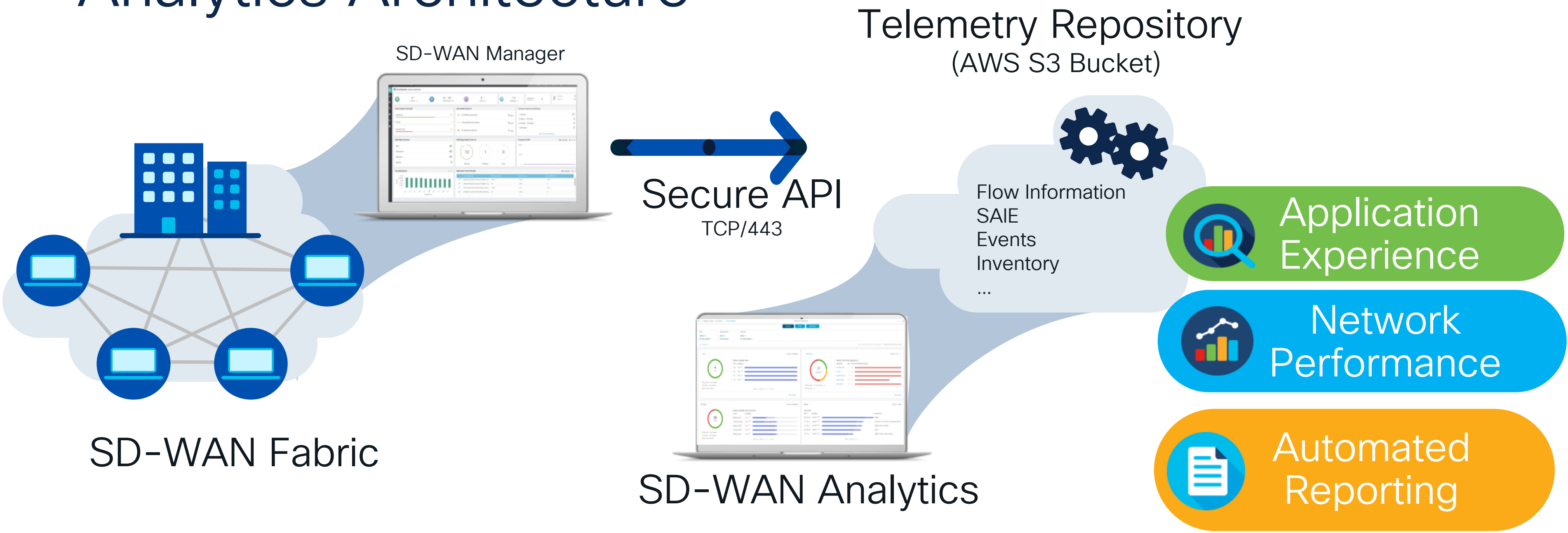
Gov. Cloud (FedRAMP)*

VM

*Only Cisco hosted

Learn more attend BRKENT-2469

Analytics Architecture



SD-WAN Manager

Secure API
TCP/443

Telemetry Repository
(AWS S3 Bucket)

Flow Information
SAIE
Events
Inventory
...

SD-WAN Fabric

SD-WAN Analytics

Application Experience

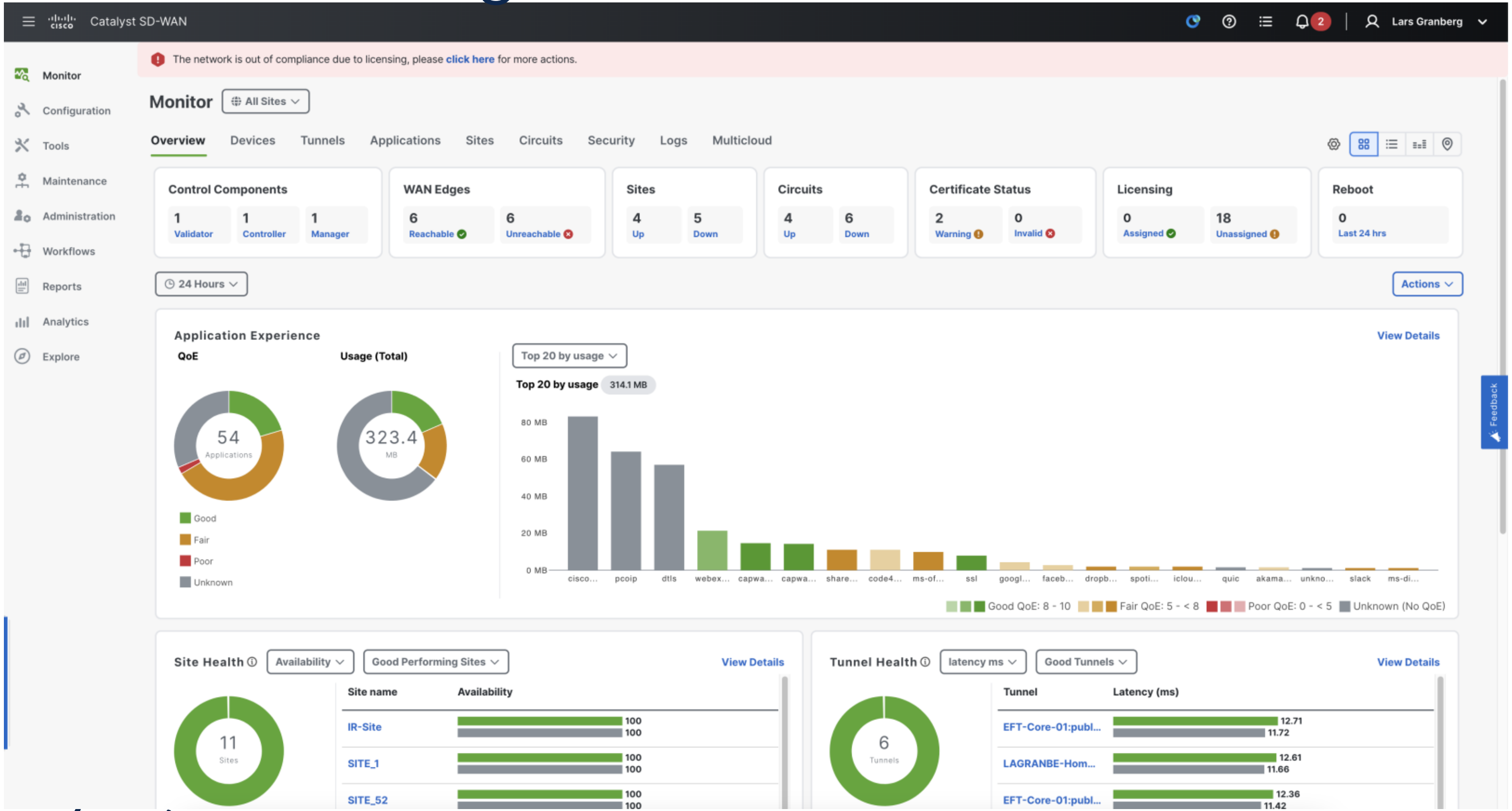
Network Performance

Automated Reporting

On-Prem or Cloud-Hosted SD-WAN Manager

Cloud-Hosted Analytics

SD-WAN Manager UI



The network is out of compliance due to licensing, please click here for more actions.

Control Components: 1 Validator, 1 Controller, 1 Manager

WAN Edges: 6 Reachable, 6 Unreachable

Sites: 4 Up, 5 Down

Circuits: 4 Up, 6 Down

Certificate Status: 2 Warning, 0 Invalid

Licensing: 0 Assigned, 18 Unassigned

Reboot: 0 Last 24 hrs

Application Experience

Site Health — Availability — Good Performing Sites — View Details

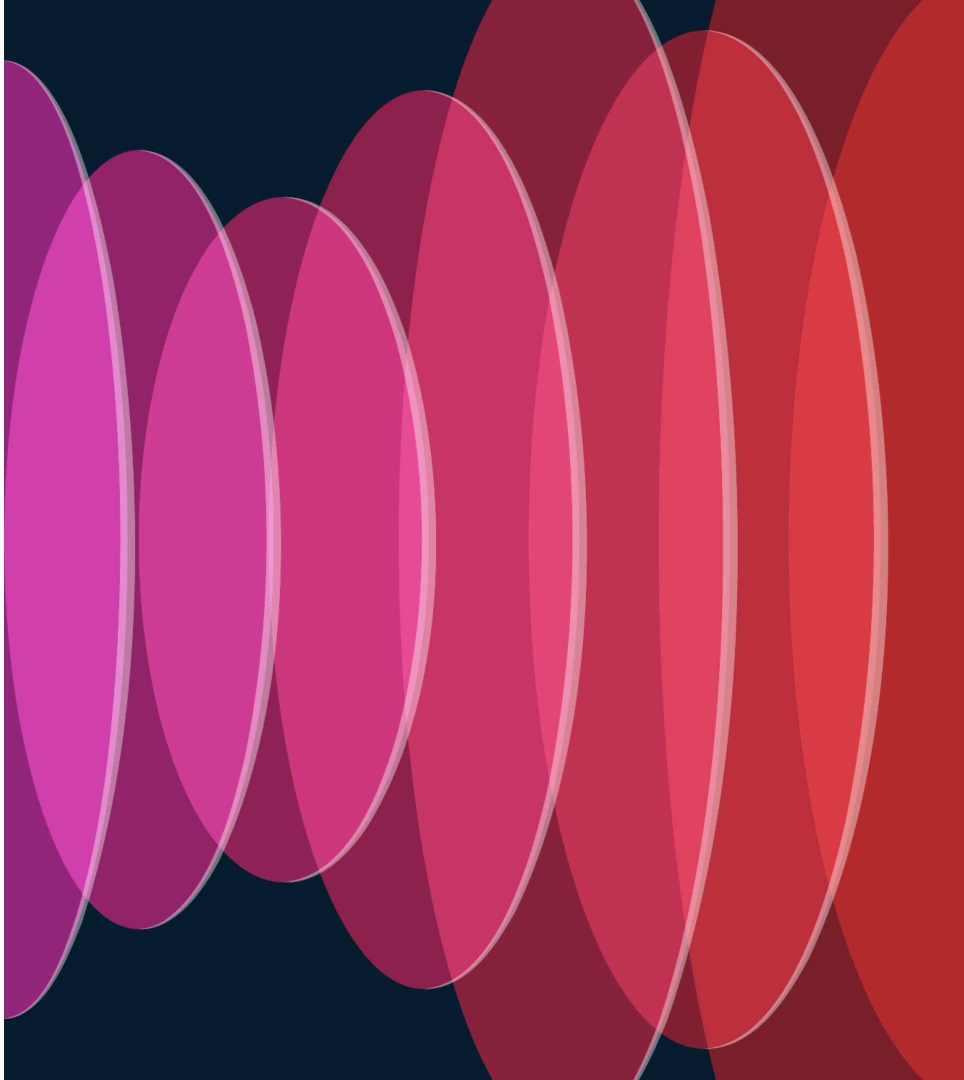
Site name	Availability
IR-Site	100 100
SITE_1	100 100
SITE_52	100 100

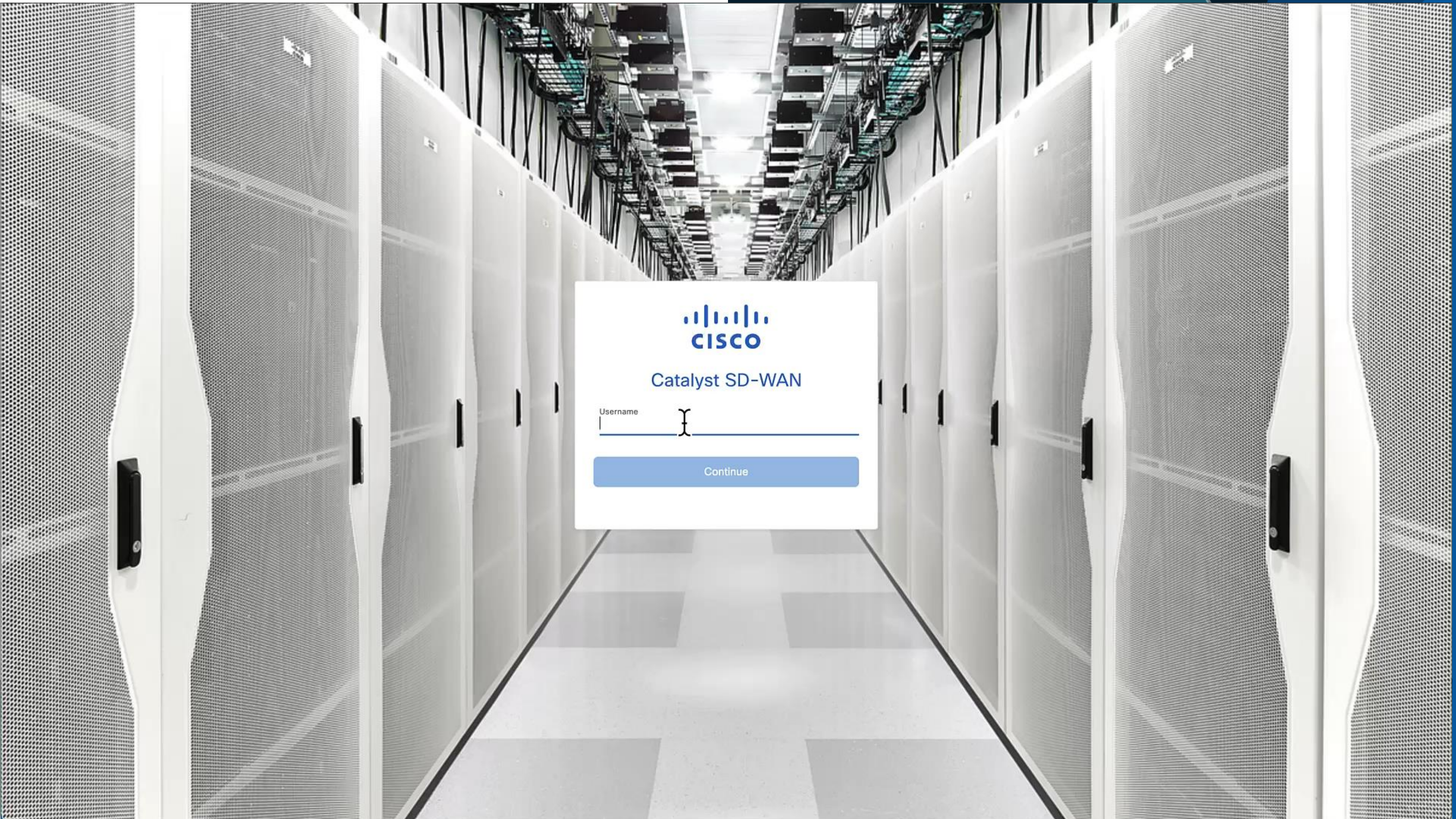
Tunnel Health — latency ms — Good Tunnels — View Details

Tunnel	Latency (ms)
EFT-Core-01:publ...	12.71 11.72
LAGRANBE-Hom...	12.61 11.66
EFT-Core-01:publ...	12.36 11.42

SD-WAN Manager 20.15.1

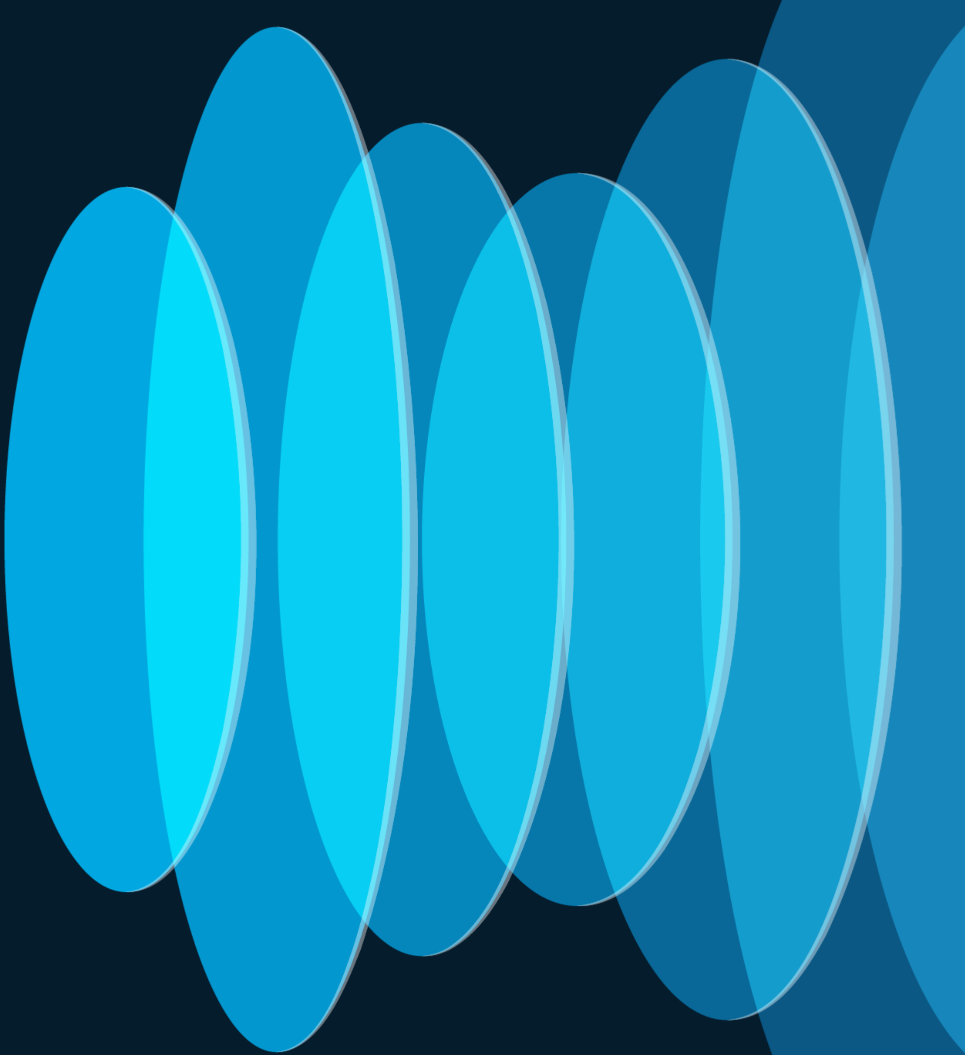
Demo





Catalyst SD-WAN

SD-WAN Features



cisco Live!

Significance of TLOC Color

Color is an abstraction used to identify individual WAN transport

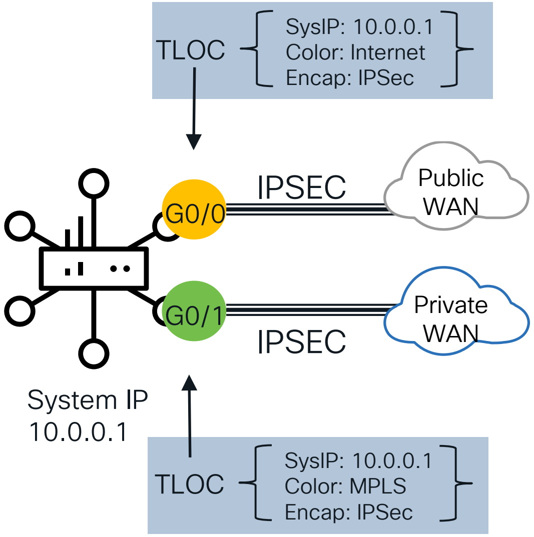
Colors are KEYWORDS not just LABELS

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



TLOC
SysIP: 10.0.0.1
Color: Internet
Encap: IPSec

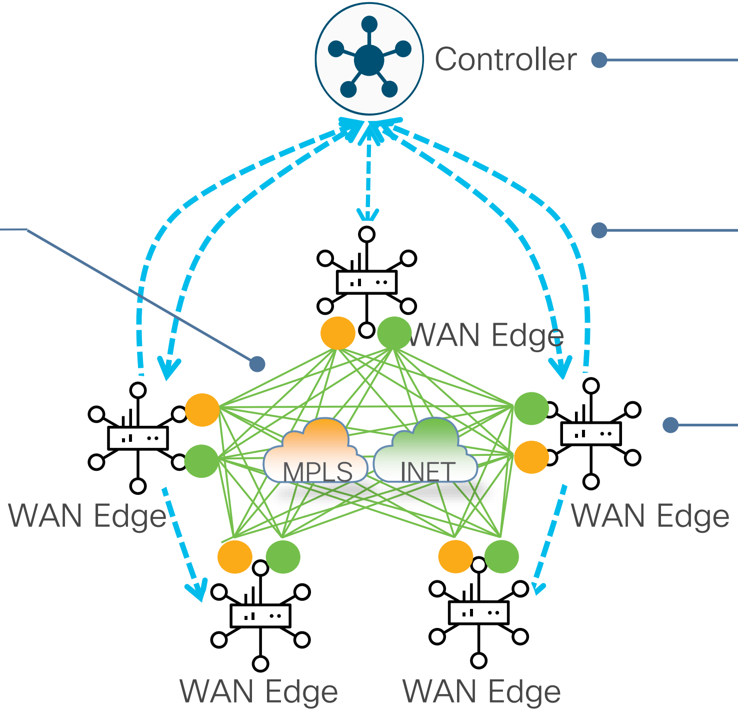
System IP
10.0.0.1

TLOC
SysIP: 10.0.0.1
Color: MPLS
Encap: IPSec

Private Colors
Metro-ethernet
mpls
private1
private2
private3
private4
private5
private6

Public Colors
3g
lte
biz-internet
public-internet
blue
green
red
gold
silver
bronze

Transport Locators (TLOCs)



The Controller advertise TLOCs to all WAN Edges* (Default)

Full Mesh SD-WAN Fabric (Default)

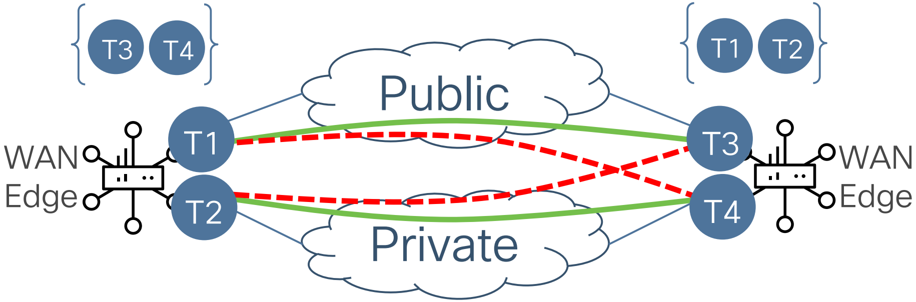
TLOCs advertised to Controllers

Local TLOCs
(System IP, Color, Encap)

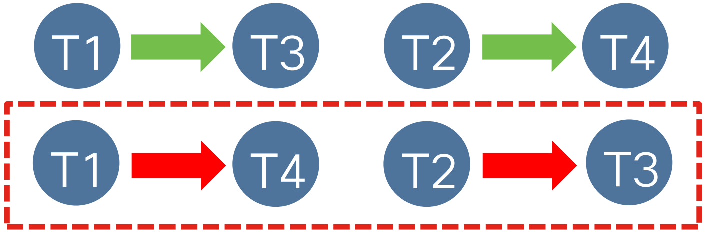
* Can be influenced by the control policies

● Transport Locator (TLOC) — OMP — IPSec Tunnel

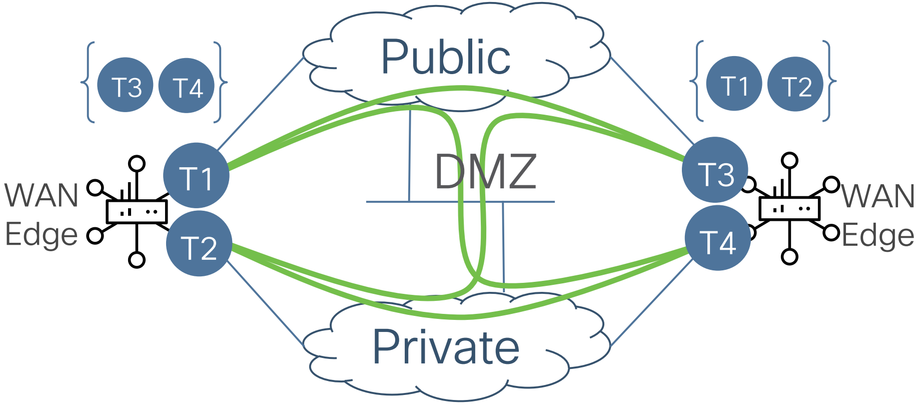
Transport Colors



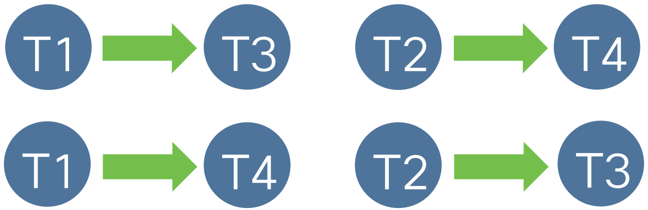
T1, T3 – Public Color   T2, T4 – Private Color



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

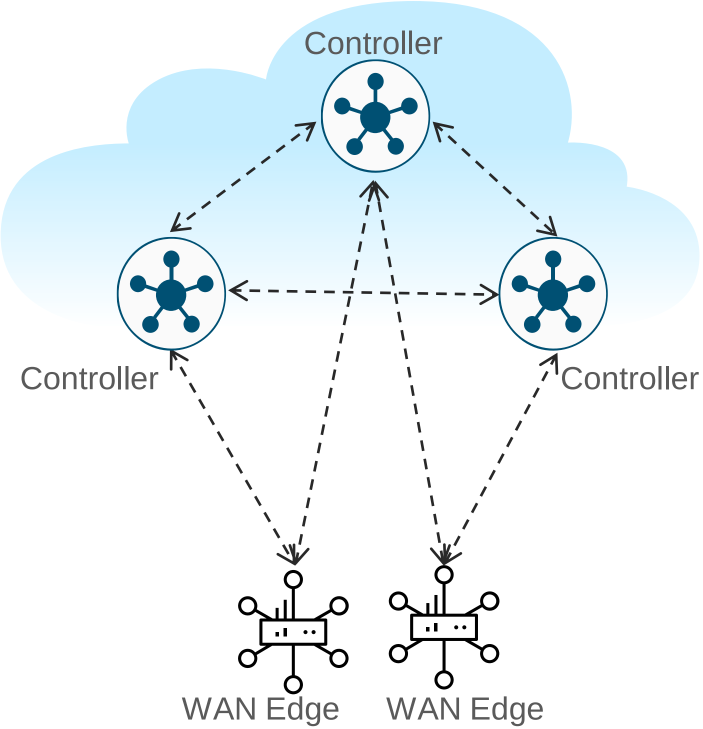


T1, T3 – Public Color   T2, T4 – Private Color

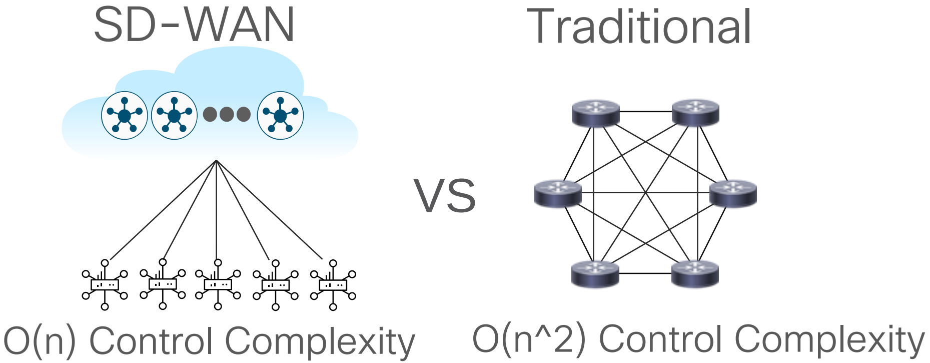


Learn more Watch
BRKENT-3115

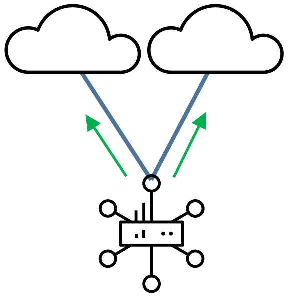
Overlay Management Protocol (OMP)

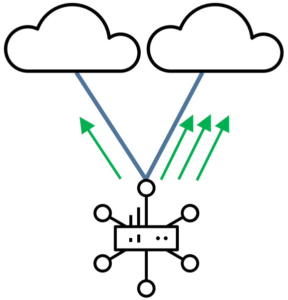


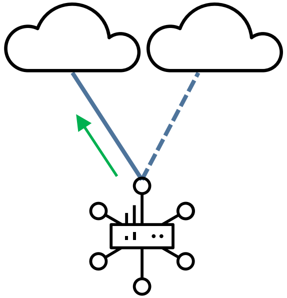
- Overlay Management Protocol (OMP)
- TCP-based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane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

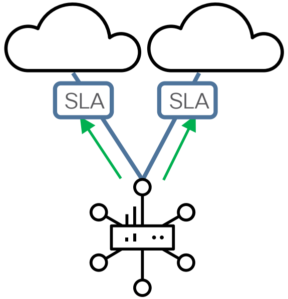


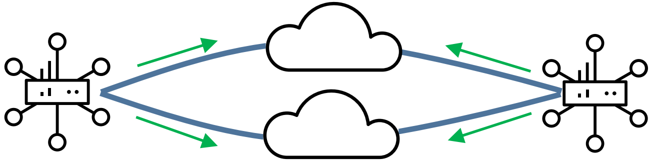
Fabric Communication

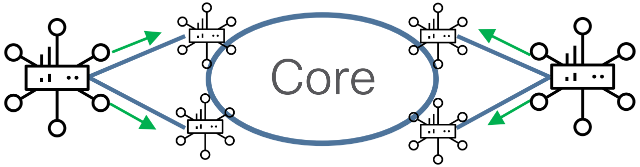

Per-Session Load-sharing
Active/Active


Per-Session Weighted
Active/Active

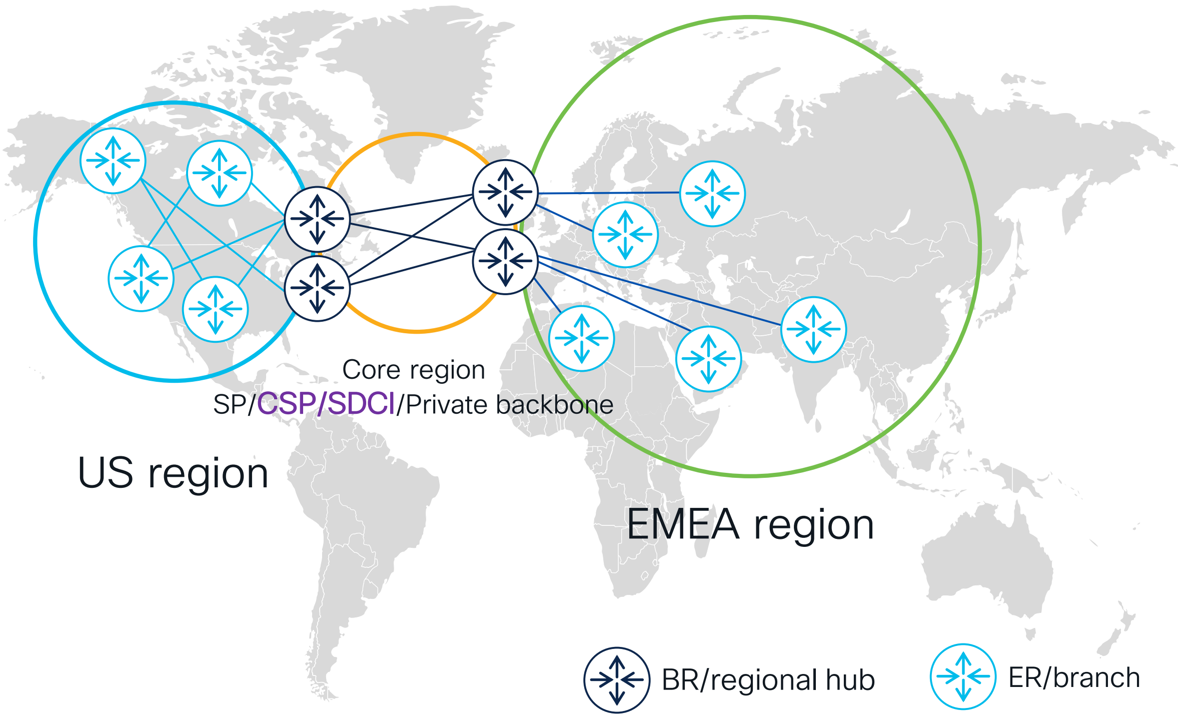

Application Pinning
Active/Standby


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)

CSP = Cloud Service Provider (AWS, Azure, GCP)
SDCI = Software Defined Cloud Interconnect

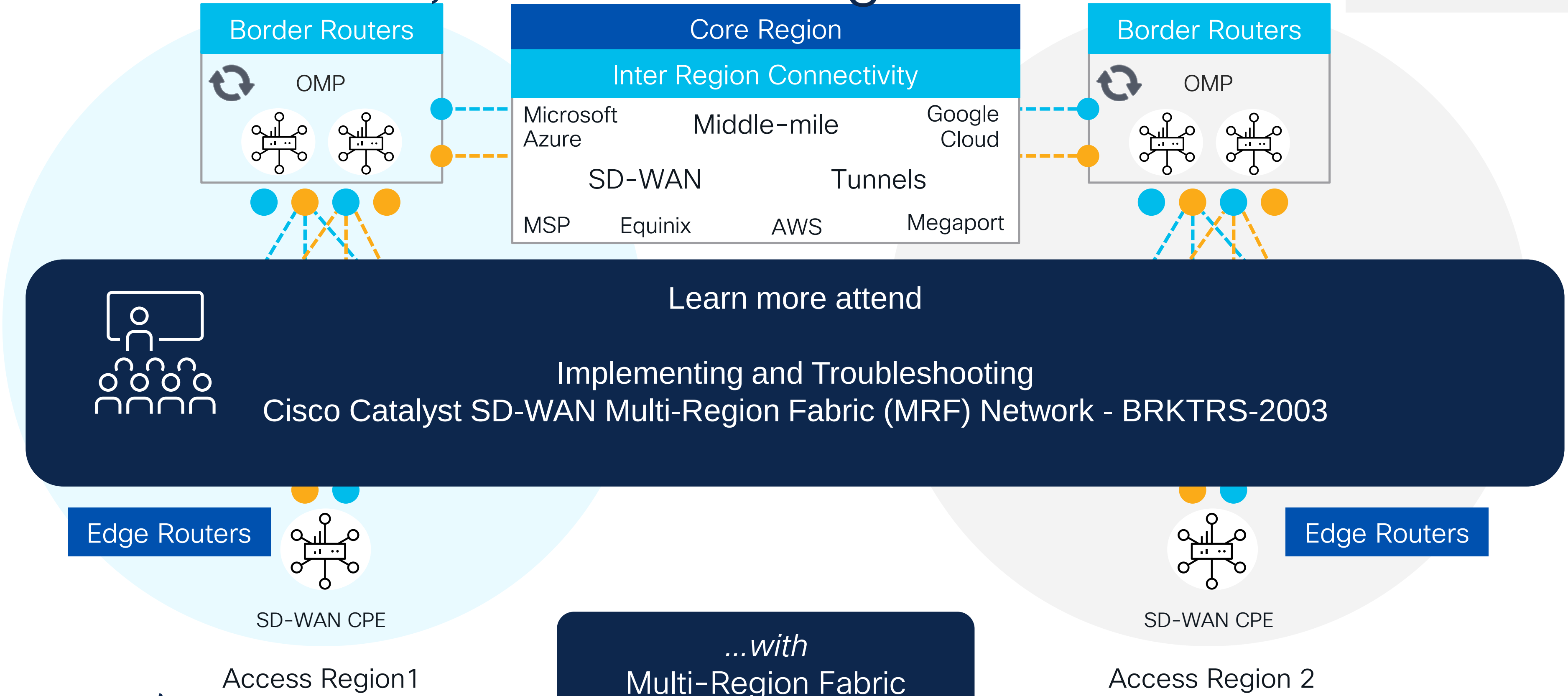
Legend

SD-WAN Tunnels/TLOCs

●- - - - -●

●- - - - -●

The Network, with Multi-Region Fabric



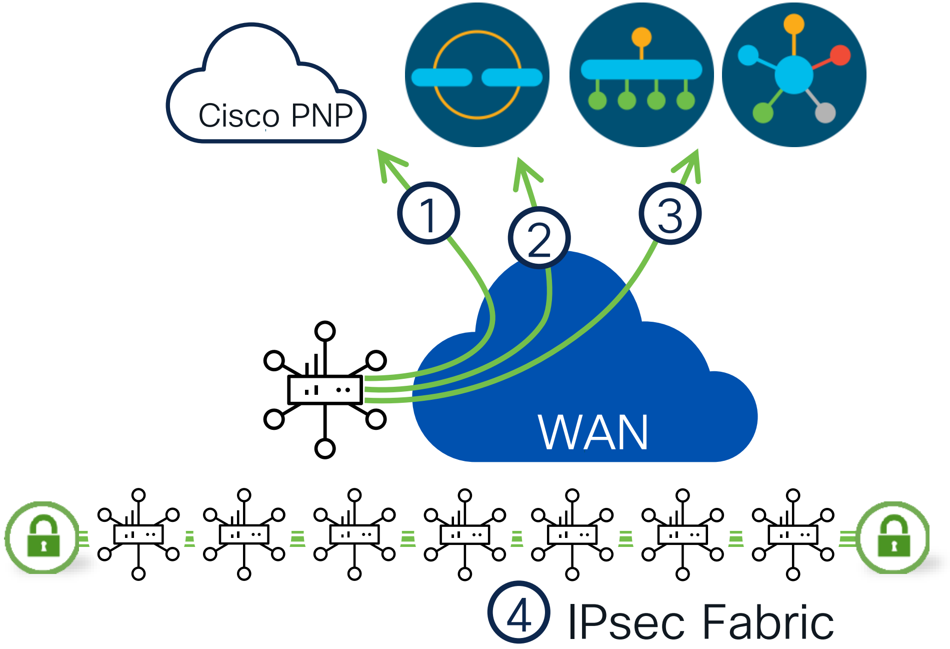
Learn more attend

Implementing and Troubleshooting
Cisco Catalyst SD-WAN Multi-Region Fabric (MRF) Network - BRKTRS-2003

...with
Multi-Region Fabric

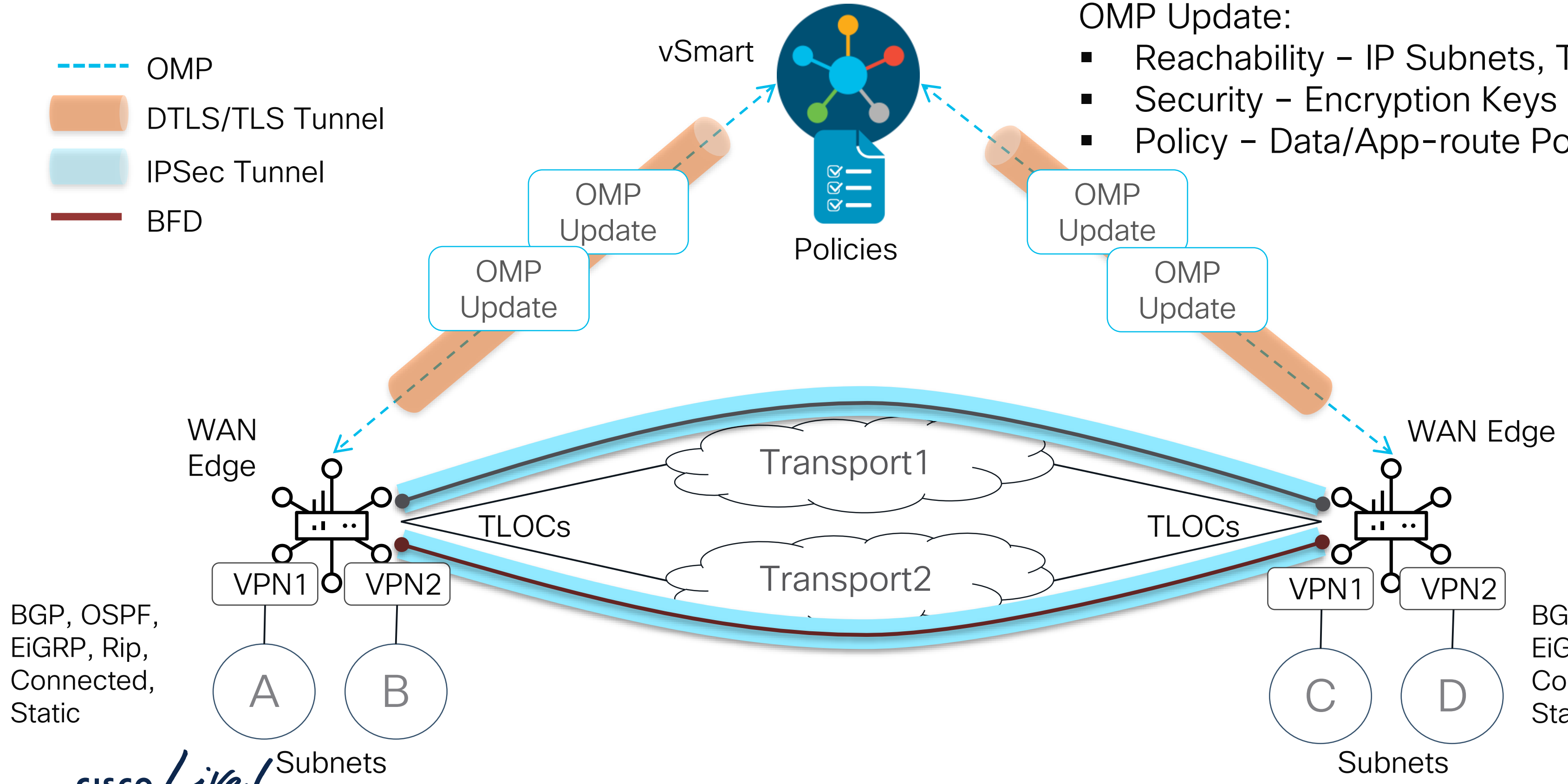
Lets bring it up

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

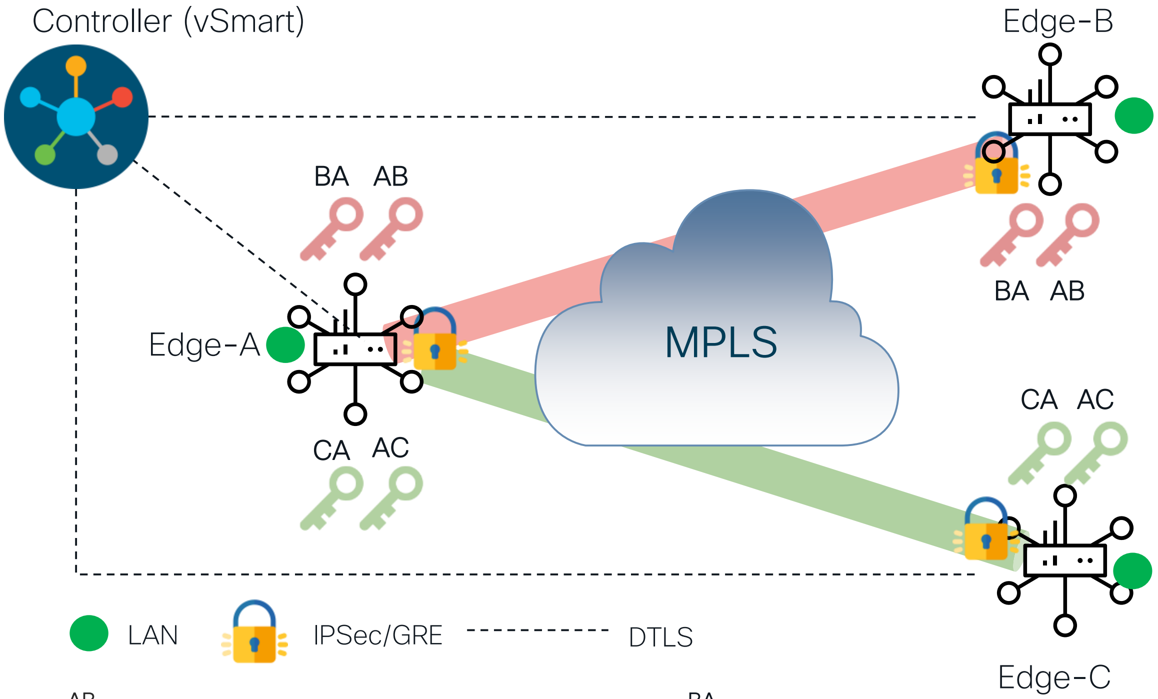


OMP Update:

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

FYI

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")

AB AB- A's Encryption Key for B

AC AC- A's Encryption Key for C

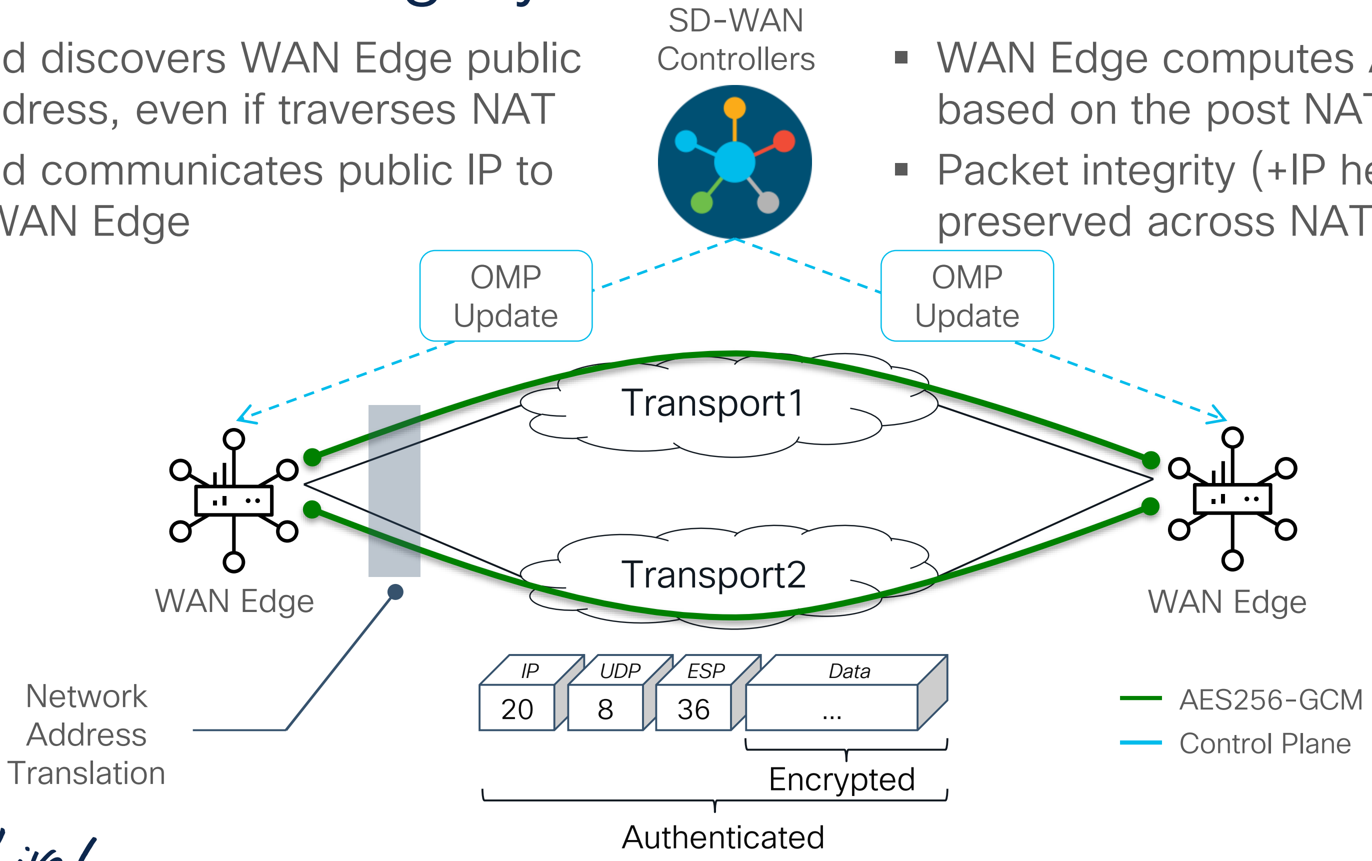
BA BA - B's Encryption Key for A

CA CA - C's Encryption Key for A

Data Plane Integrity

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

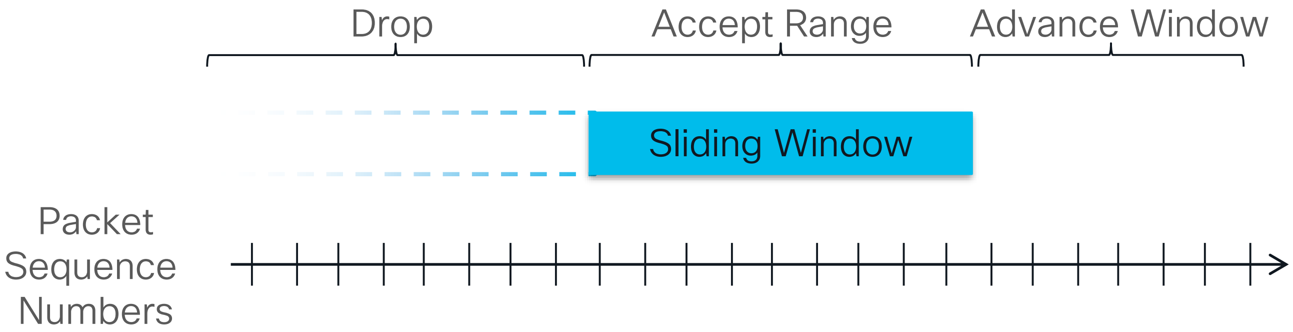
- WAN Edge computes AH value based on the post NAT public IP
- Packet integrity (+IP headers) is preserved across NAT



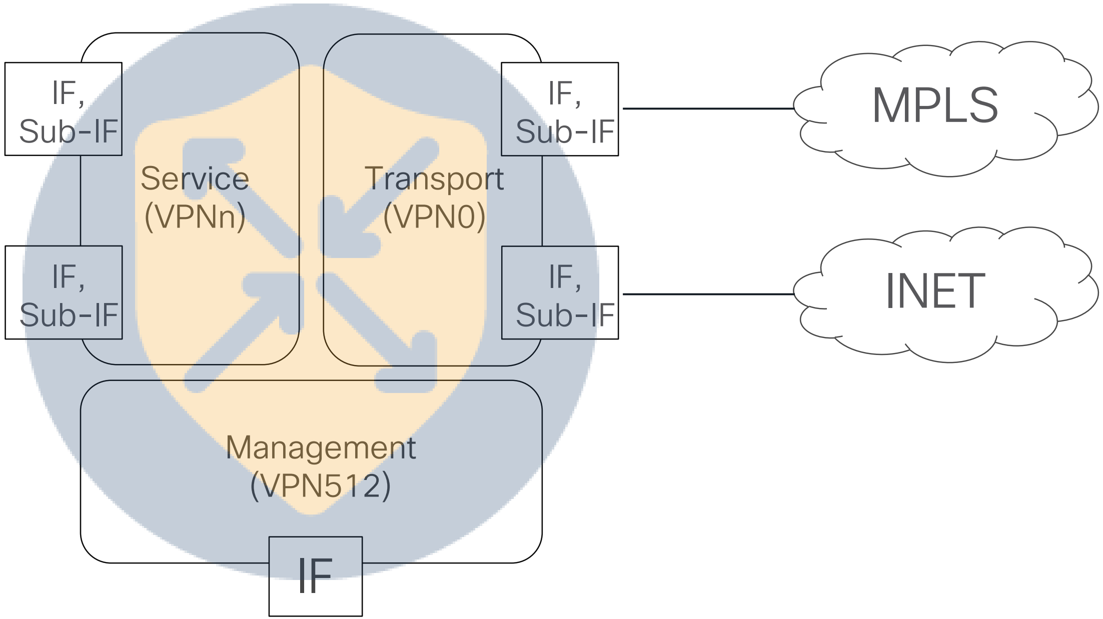
FYI

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)

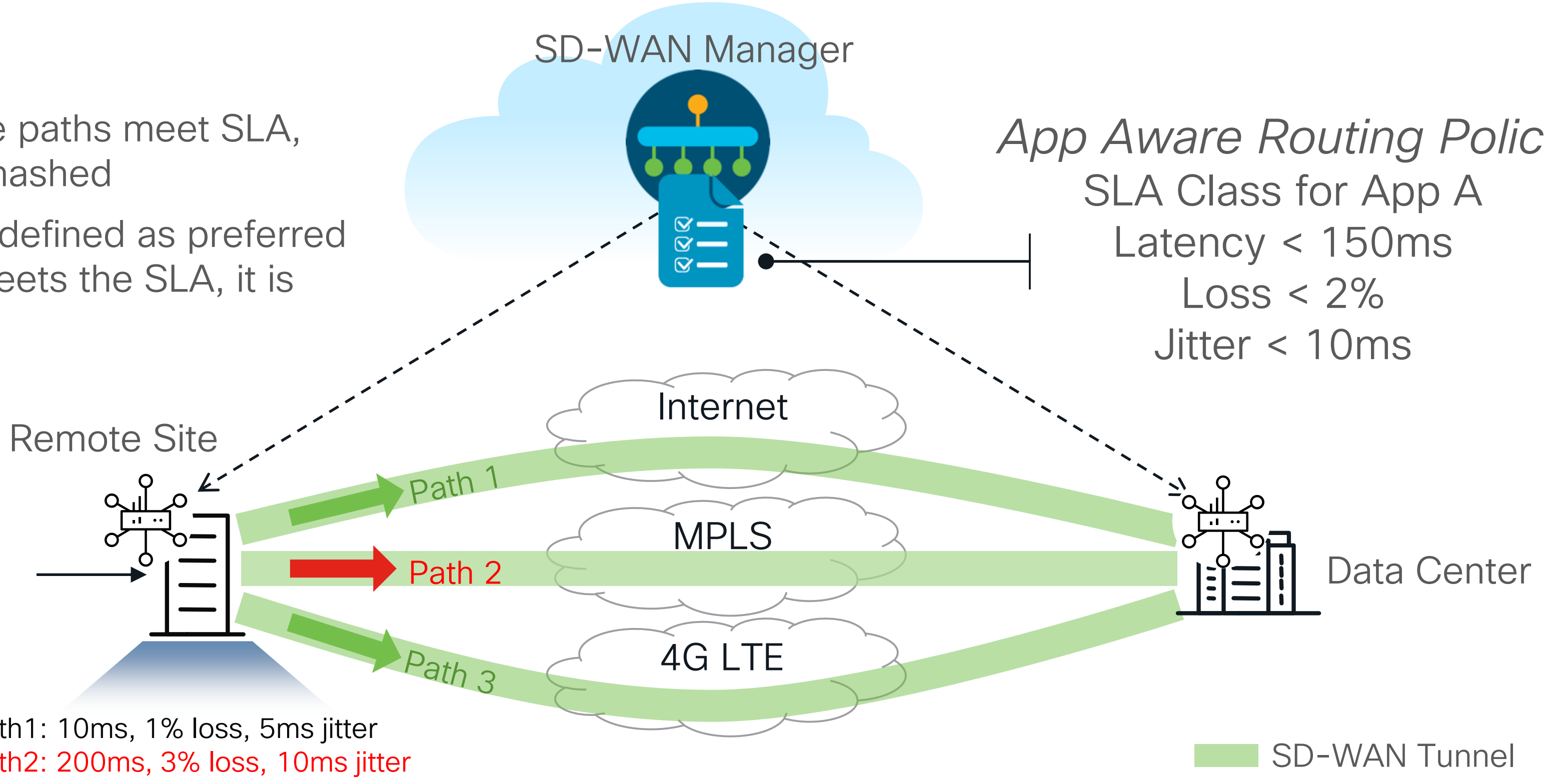


- VPNs are isolated from each other, with each VPN has its own forwarding table
- Reachability within VPN is advertised by OMP
- VPN0 is reserved for WAN uplinks (Transport)
- VPN512 is reserved for Management interfaces
- VPNn represents user-defined LAN segments (Service)

Application Aware Routing

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



App Aware Routing Policy
SLA Class for App A
Latency < 150ms
Loss < 2%
Jitter < 10ms

Path1: 10ms, 1% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

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

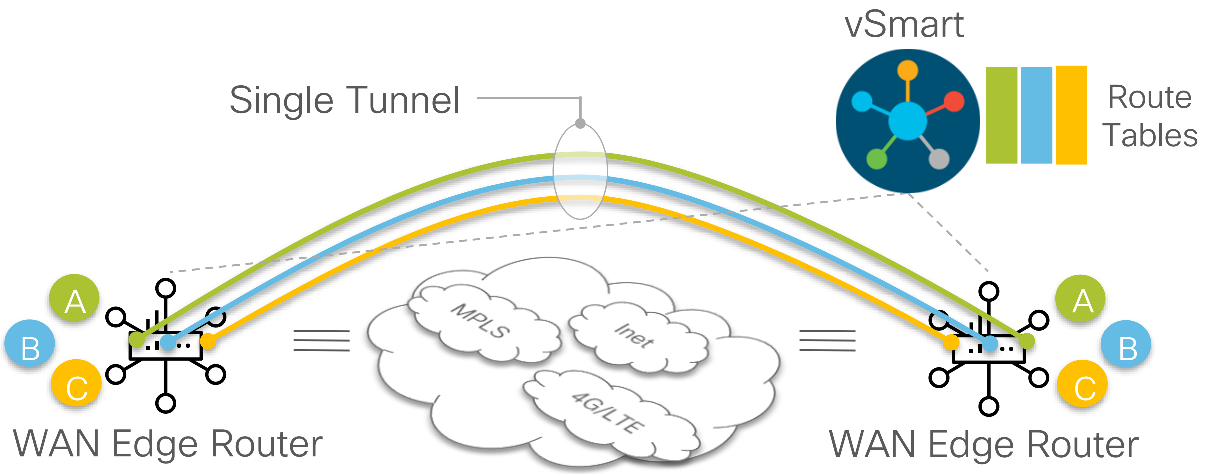
Large Initial Windows

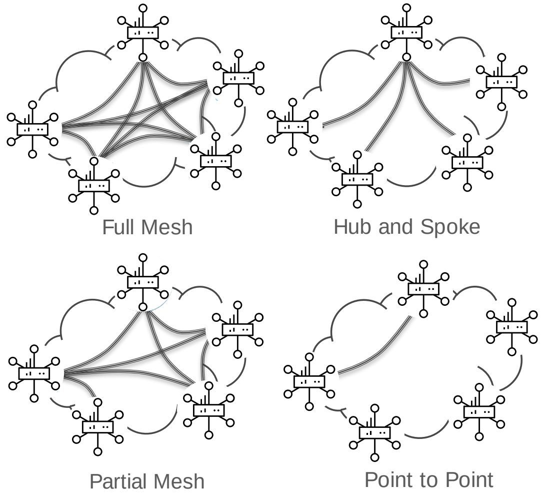
Selective Acknowledgement

BBR – Bottleneck Bandwidth and Round-trip propagation time

Security features

End-to-End Segmentation with Multi-Topology

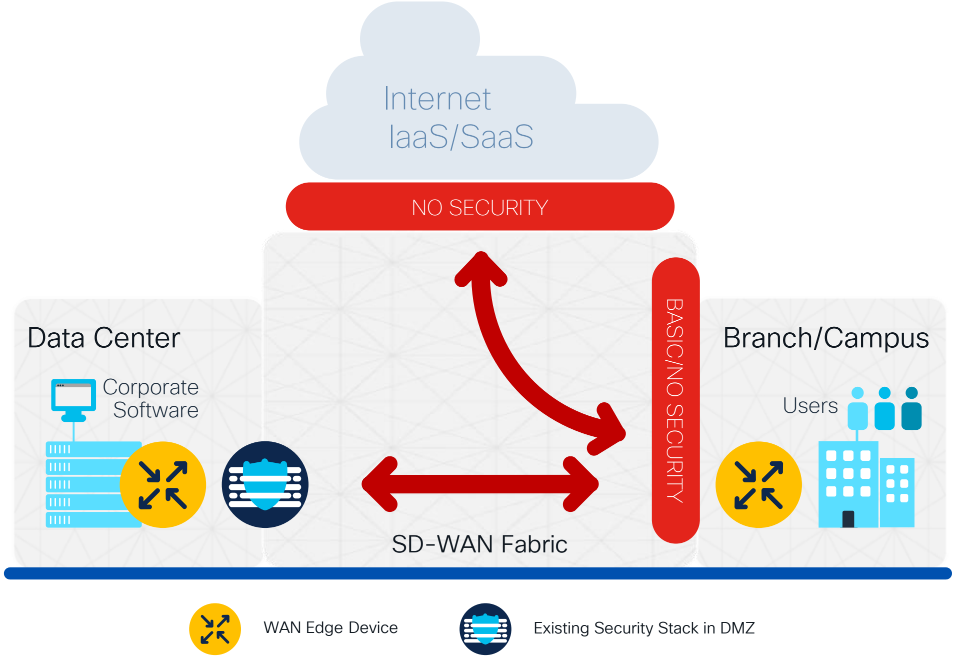




Segment connectivity across the SD-WAN fabric without reliance on underlay transport

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

How SD-WAN Exposes New Security Challenges



Internal & External Threats

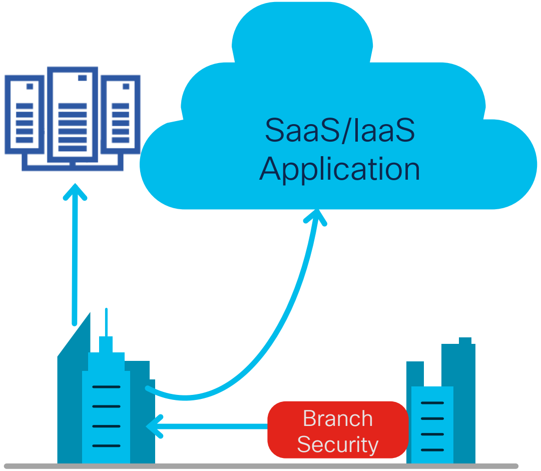
External

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

Internal

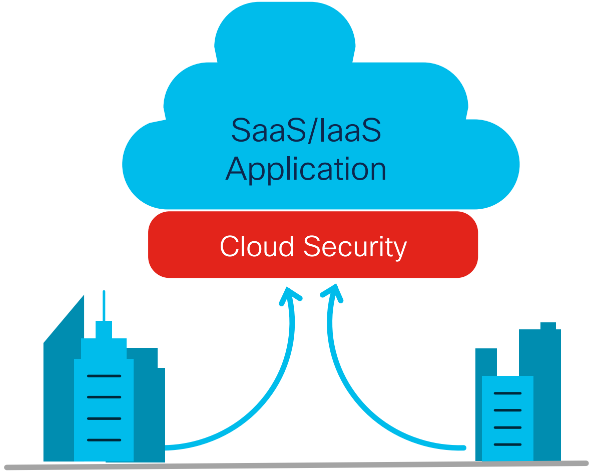
- Untrusted access (malicious insider)
- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)

Relevant Security Models. Driving towards SASE



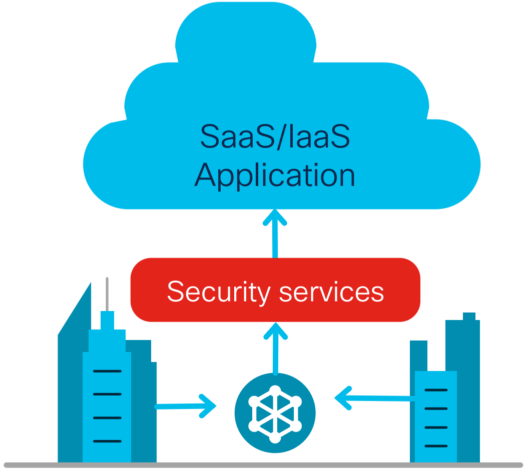
On-Prem Security

Thick branch with Routing and Security



Cloud Security

Thin branch with security in the cloud

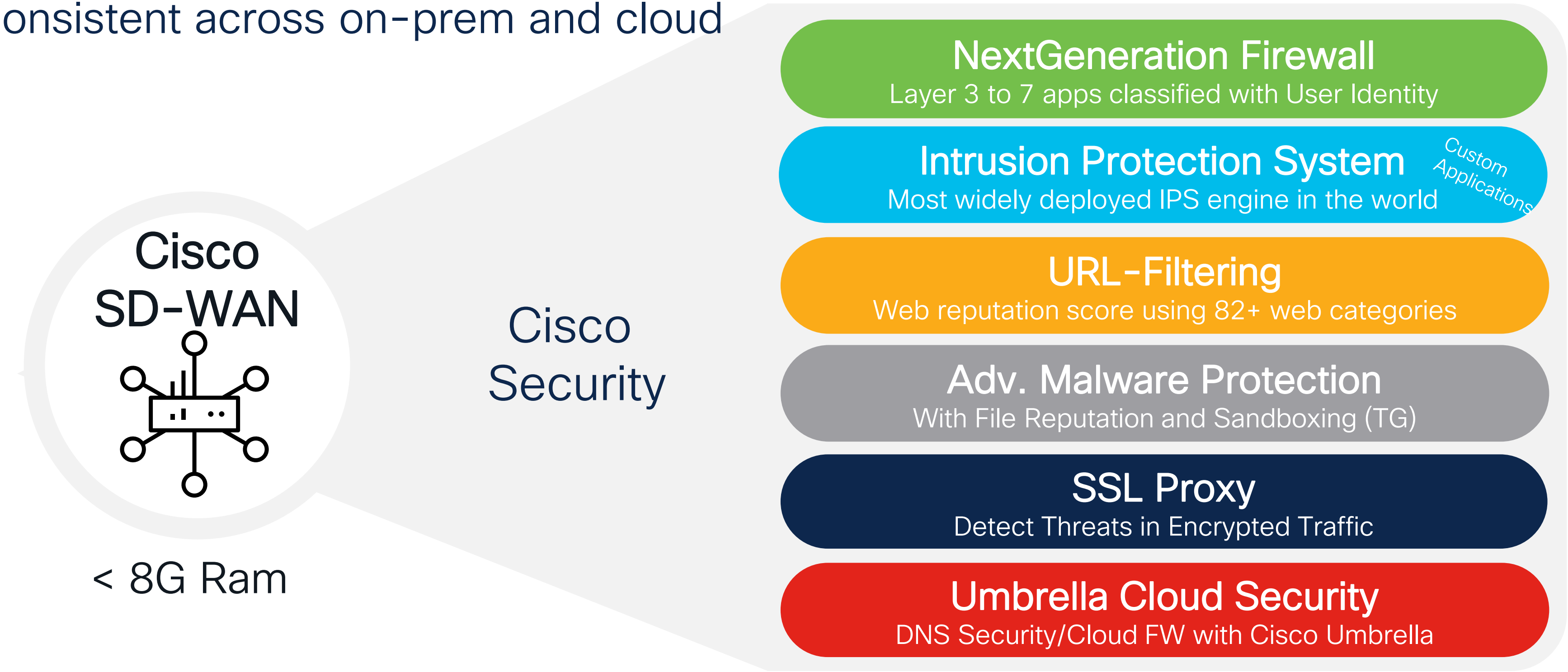


@Regional Hub

Security Services on a Regional Hub

Cisco 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

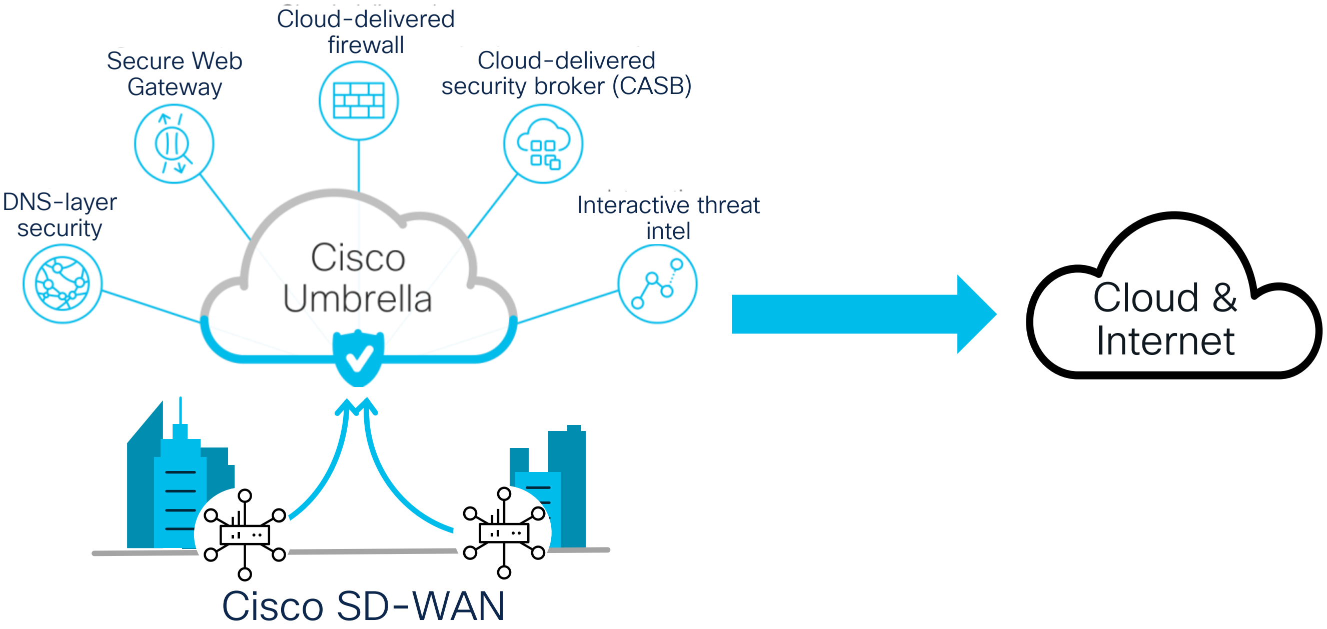
URL-Filtering
Web reputation score using 82+ web categories

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

SSL Proxy
Detect Threats in Encrypted Traffic

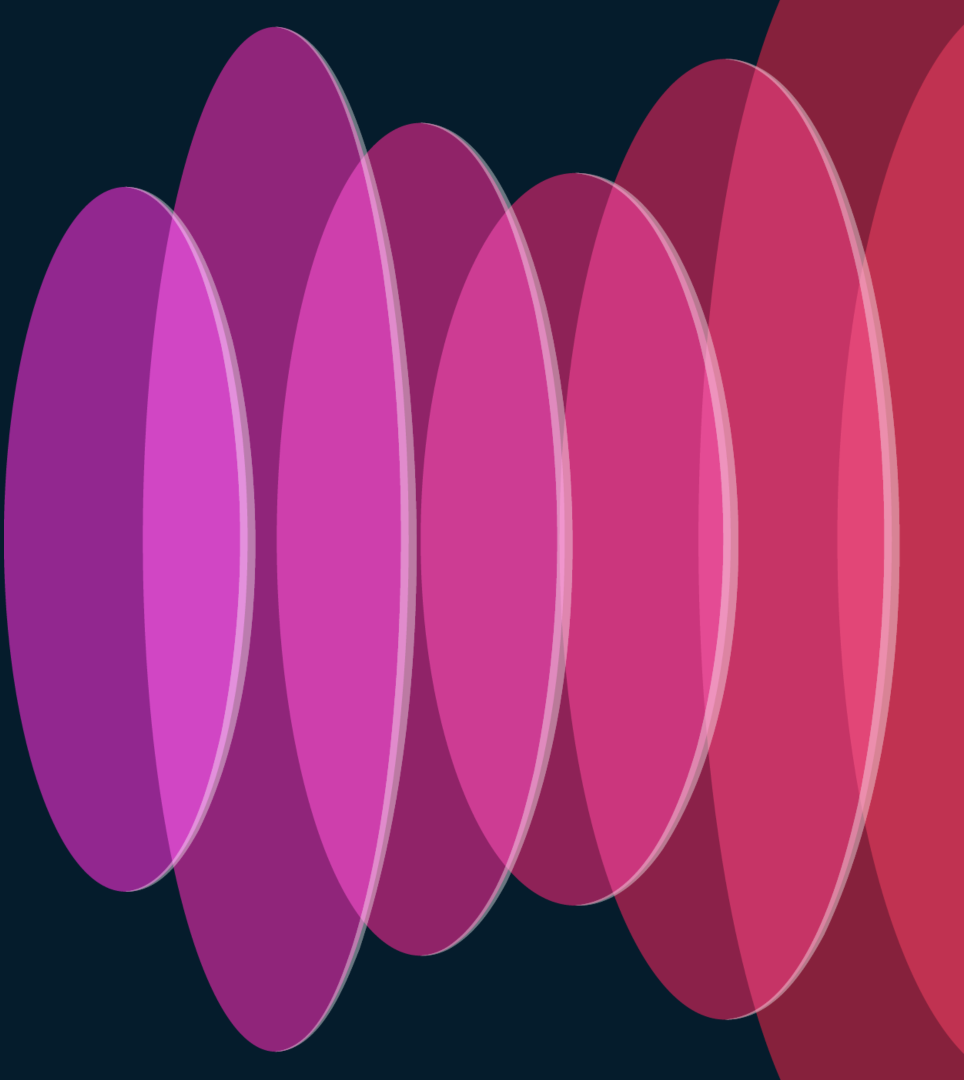
Umbrella Cloud Security
DNS Security/Cloud FW with Cisco Umbrella

Transitioning towards a Cloud security model



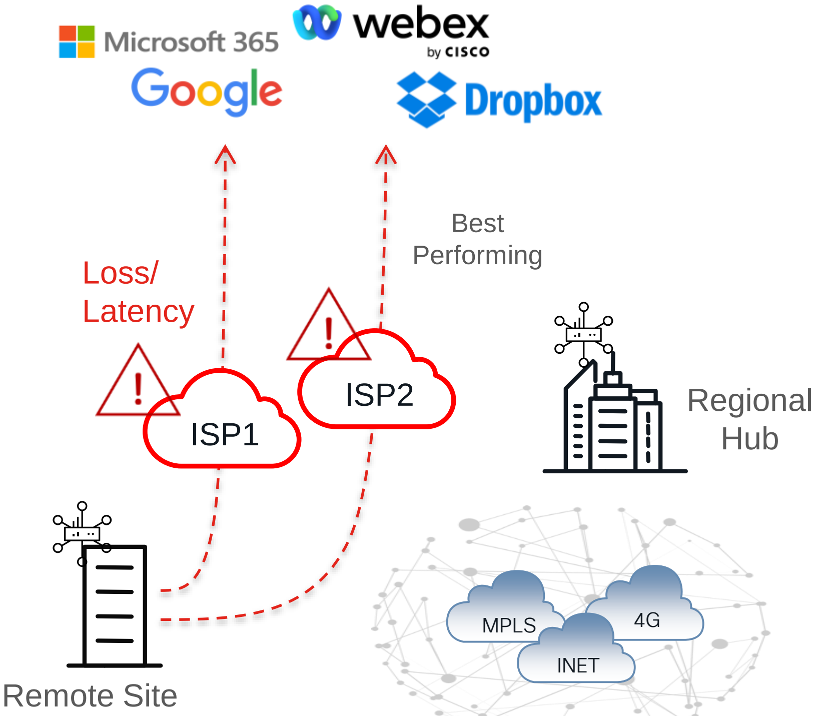
Cisco SD-WAN + Umbrella

Cloud OnRamp for SaaS

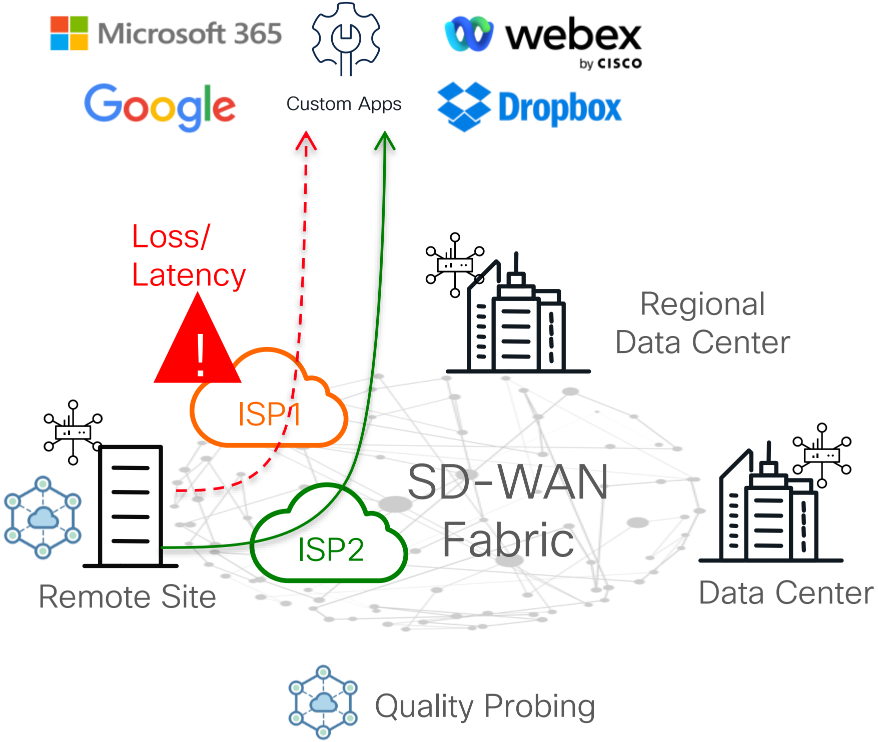


SaaS Optimization Challenges

- 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 ?

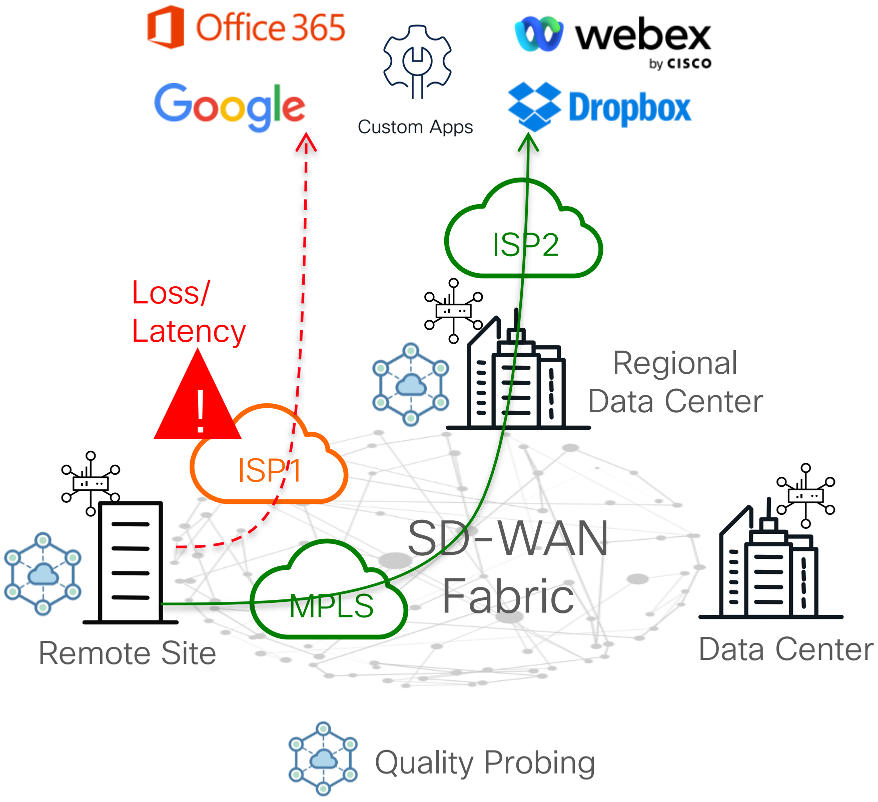


Cloud onRamp for SaaS – Internet DIA



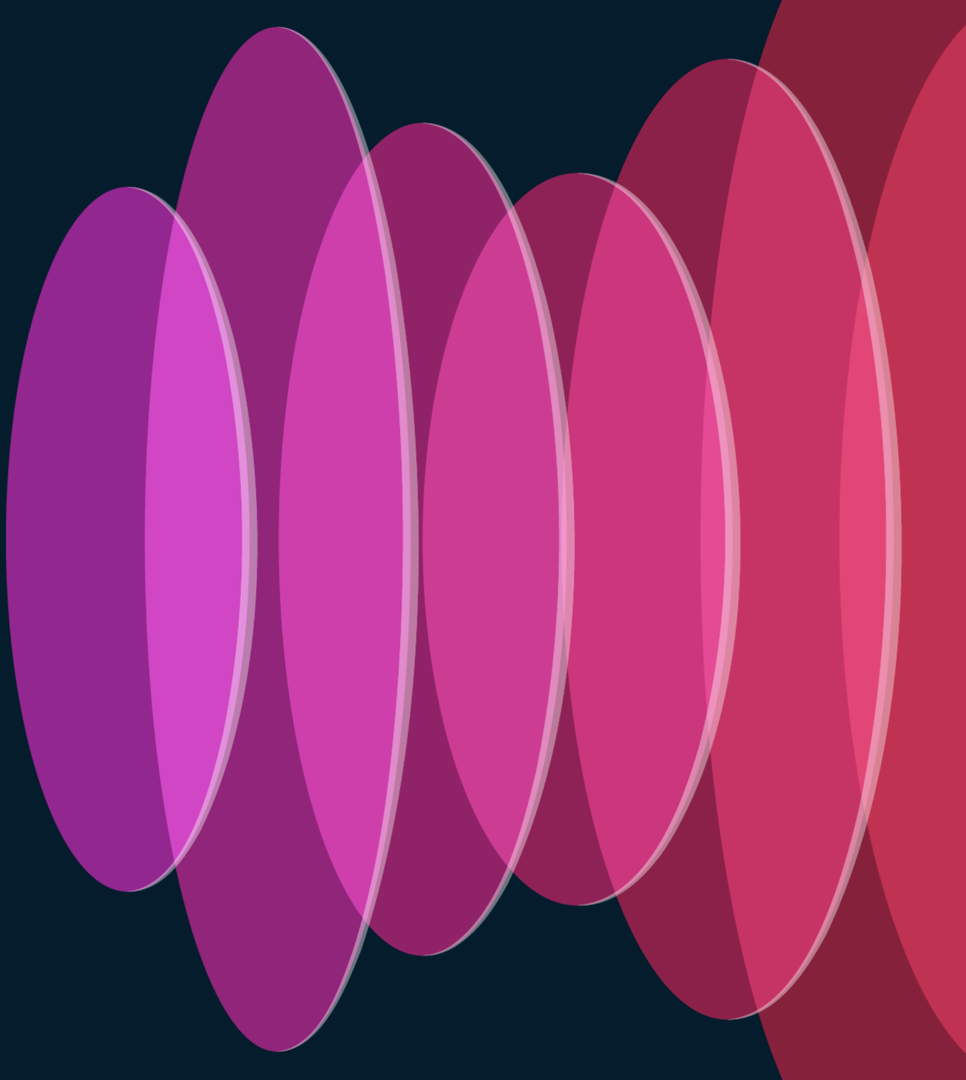
- WAN Edge router at the remote site performs quality probing for selected SaaS applications across each local DIA exit
  - Simulates client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
- Local DIA exit with better vQoE score is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

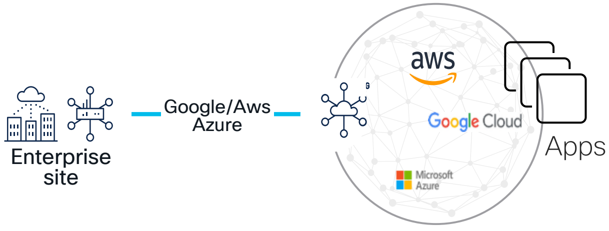


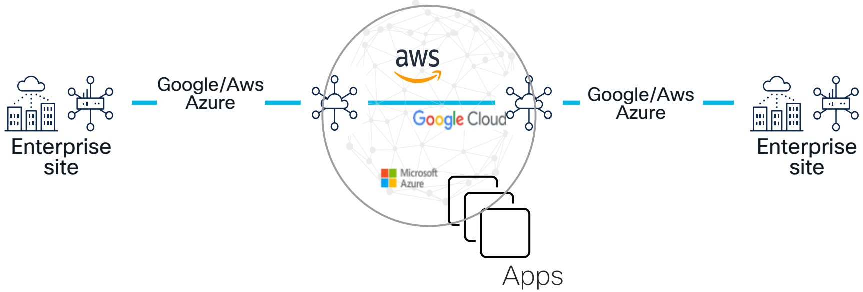
Cisco SD-WAN Cloud Hub- Use Cases

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

= Cisco SD-WAN router on-premises

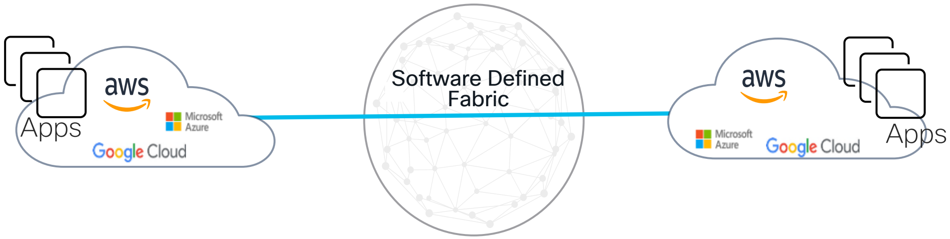
Enterprise Site to Cloud





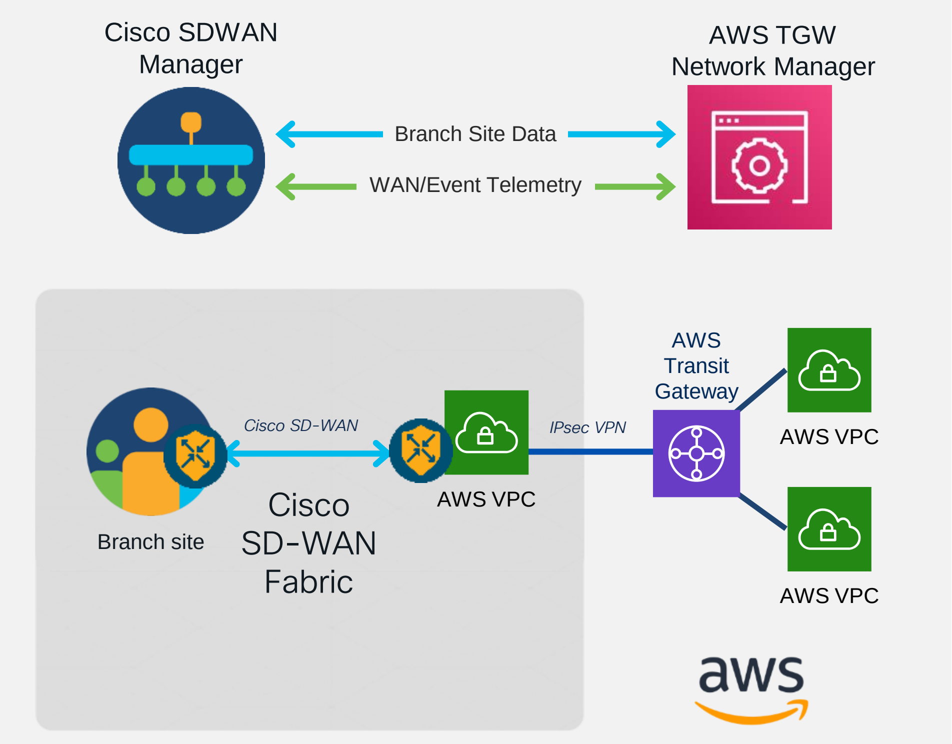
Enterprise Site to Enterprise Site

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

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



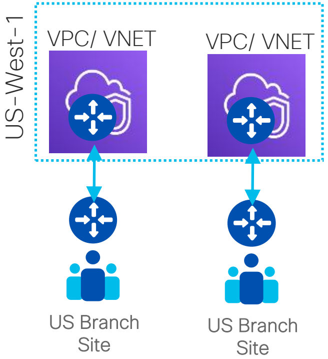
Benefits

- 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

High Level Design Options

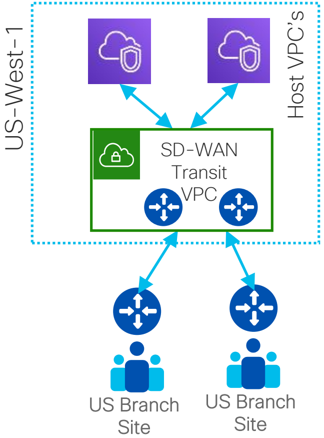
CSP-generic, AWS used as example

Cloud Gateway



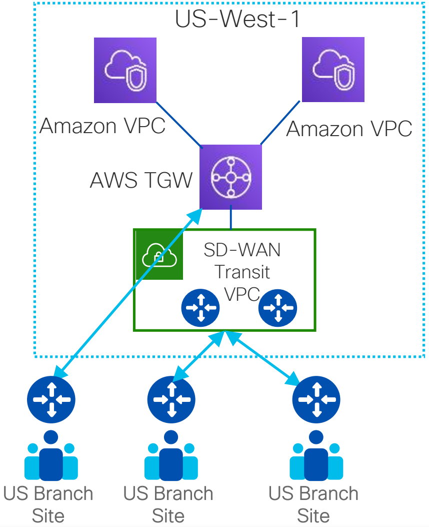
- SD-WAN Router in every VPC/VNET.
- Not scalable, but okay for one VPC.
- No built-in automation in Cloud onRamp, custom automation possible

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

FYI

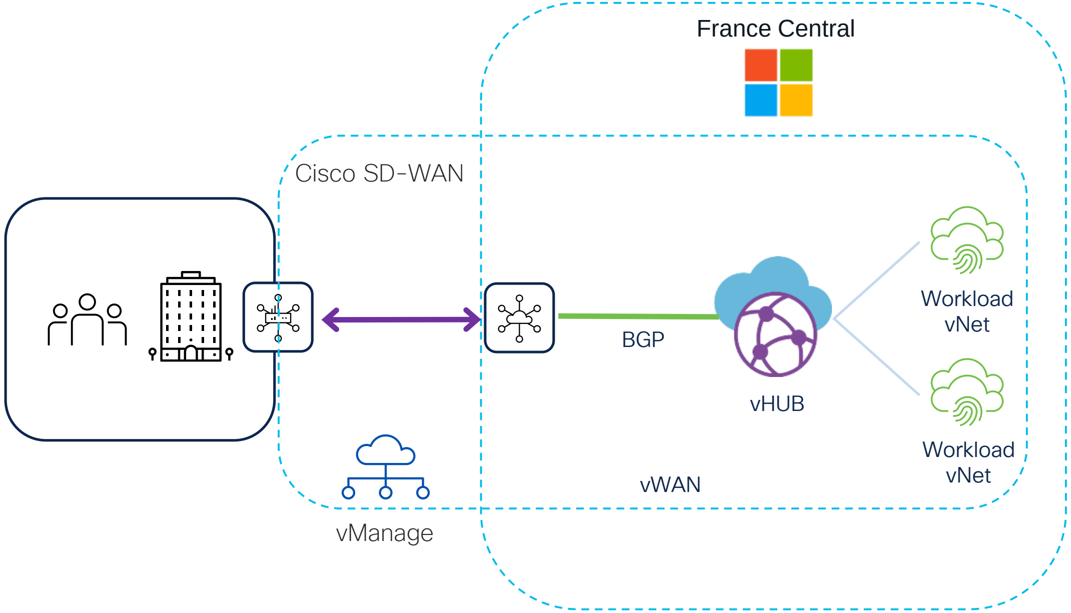
Automation (CSP-generic)

Different Automation options

- Cloud OnRamp (CoR) for Multicloud Automation built in vManage
- Custom Automation with 3rd party tools like Terraform and Ansible

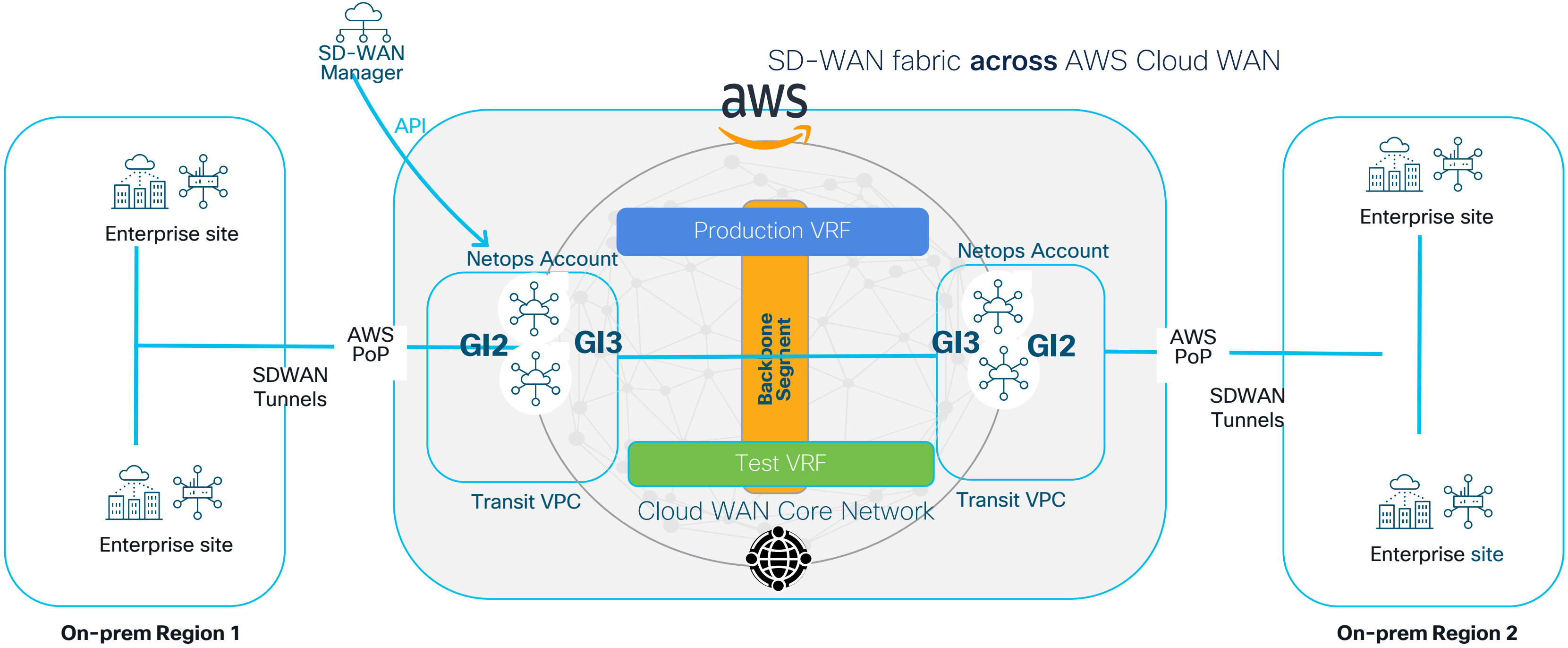
	Pros	Cons
Cloud OnRamp Automation	• Single UI in vManage for the whole workflow • Discovers host VPCs/VNETS and connects public-cloud with SD-WAN within minutes	• Not possible to add own customization for design changes i.e., virtual firewall • No built-in auto scale capabilities (yet)
Custom Automation	• Will do exactly what customer wants • Can be changed in case of any design changes	• Takes time and money to develop and test (customer, Cisco CX or Partner)

Cisco SD-WAN Cloud OnRamp for Multicloud with Microsoft Azure



Cisco SD-WAN on-premises router
Cisco SD-WAN cloud router - Catalyst 8000V

Site-to-Site with Cloud WAN



On-demand

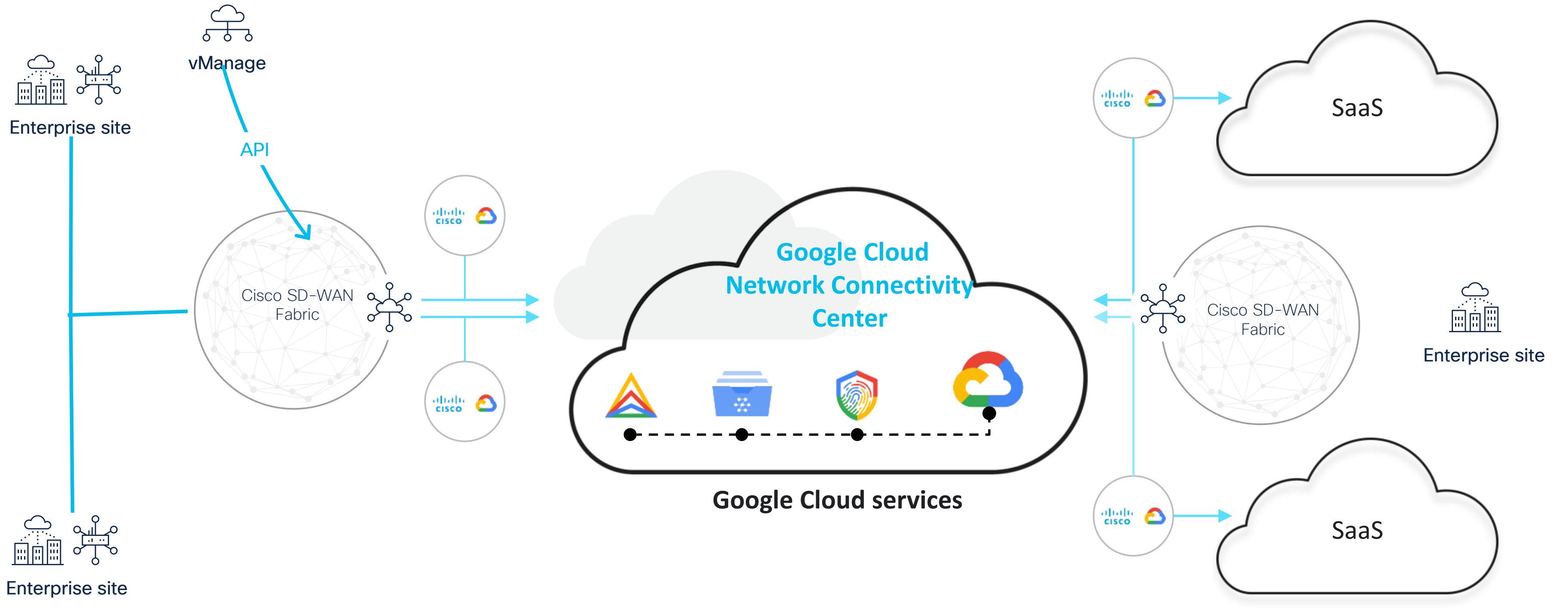
High performance

Global connectivity

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



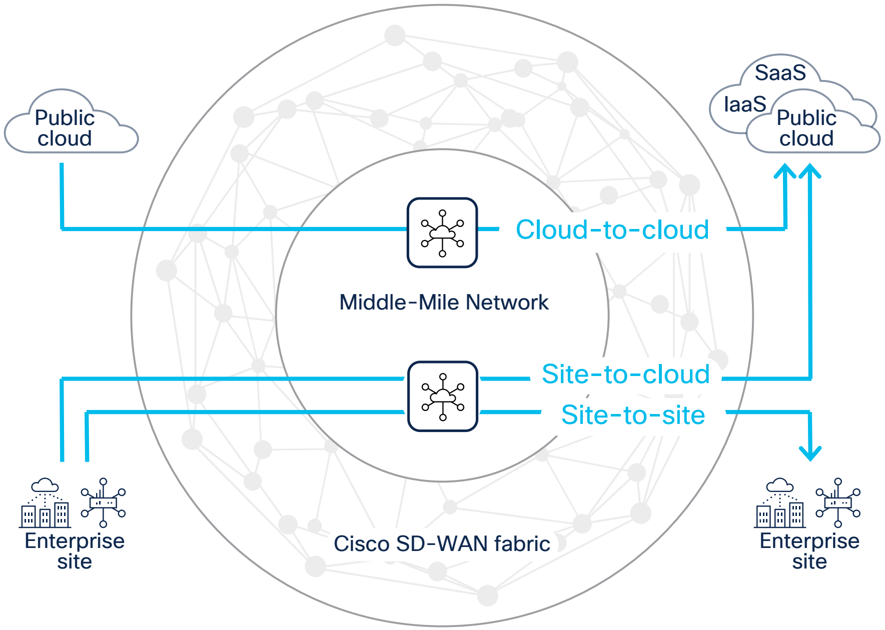
Cisco SD-WAN Cloud Hub with Google Cloud

Cisco SD-WAN Middle-Mile Optimization

Megaport EQUINIX aws Cloud WAN Google Cloud NCC Microsoft Azure

= Cisco SD-WAN virtual router

= Cisco SD-WAN router on-premises



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

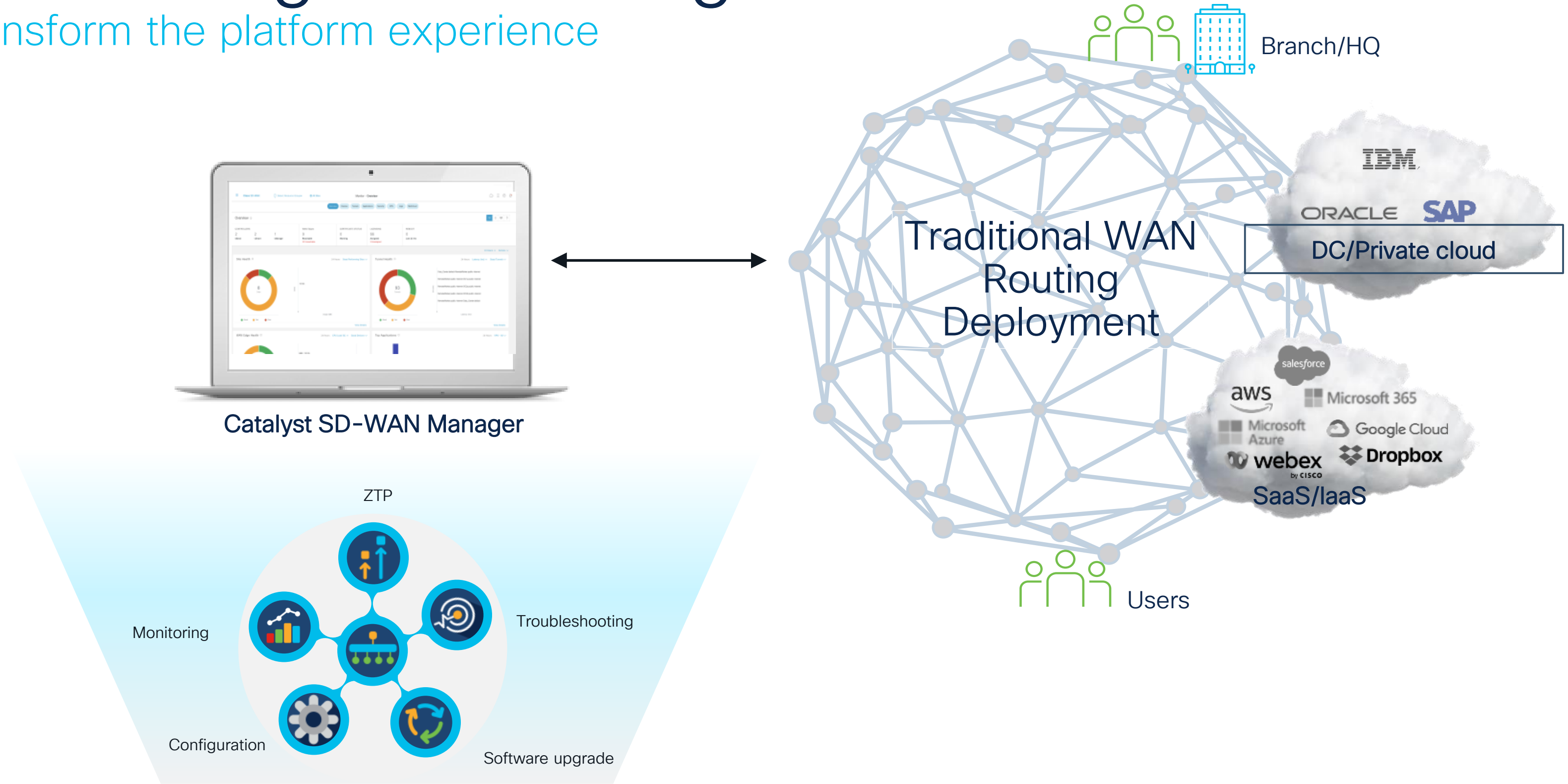
On-demand
Automated connectivity via vManage central dashboard

SD-Routing?

Learn more attend BRKENT-1039

Introducing SD-Routing

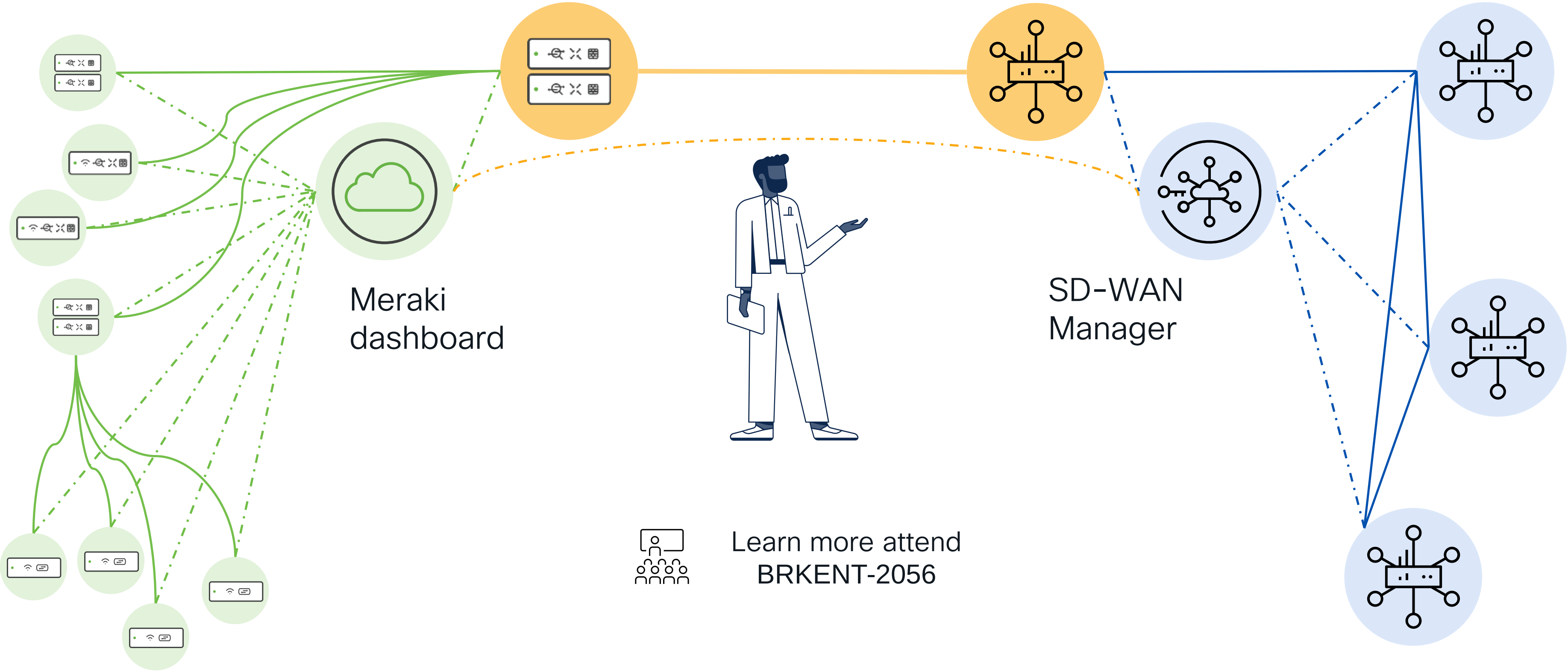
Transform the platform experience



What about Meraki SD-WAN?

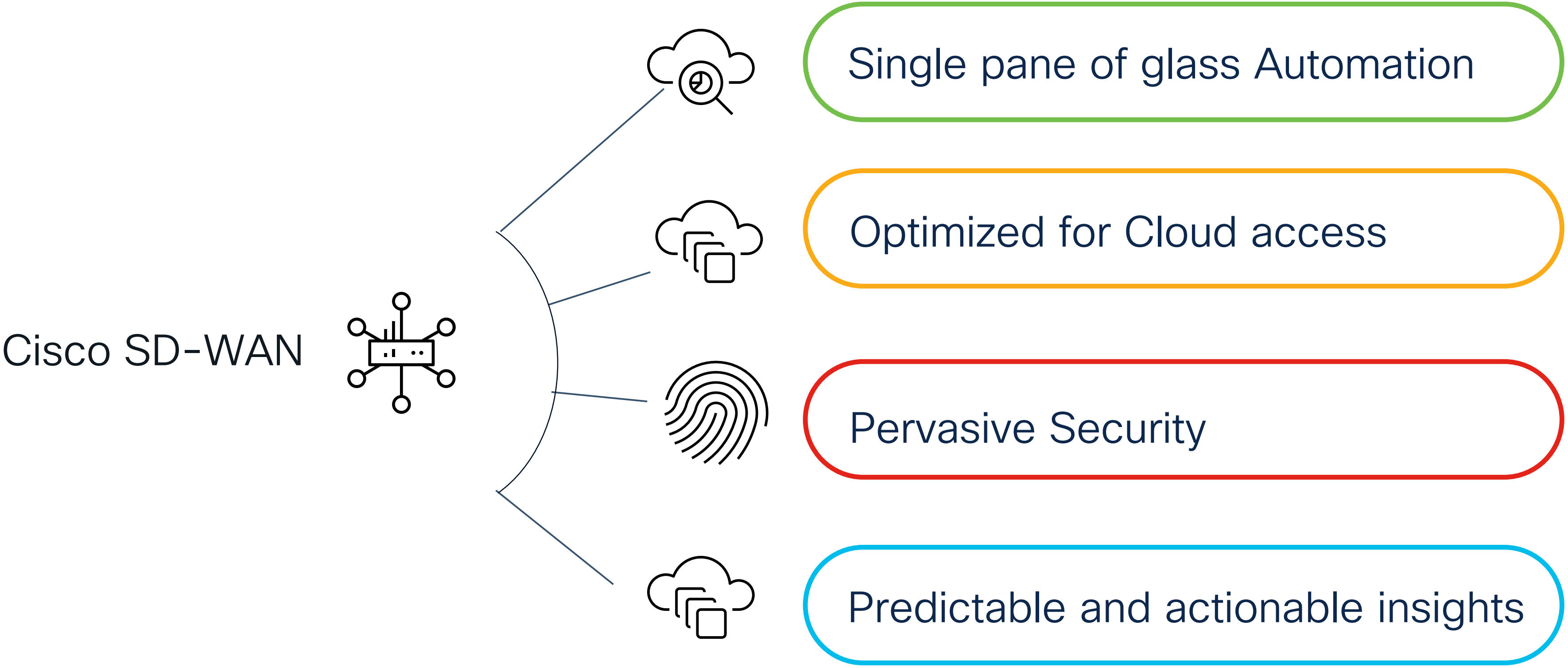
Cisco SD-WAN

Joining fabrics is now a simplified experience



Learn more attend BRKENT-2056

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 deploy and operate Cisco's SD-WAN solution in a new or existing network. These sessions provide a journey from the foundation to latest Cisco SD-WAN innovations focusing on design, innovations, and integrations with Cloud, SASE, and Assurance/Analytics.

START

Monday, June 3 | 8:00 a.m.
BRKENT-2108
Cisco SD-WAN: Start Here

Monday, June 3 | 8:30 a.m.
BRKENT-2469
How Cisco SD-WAN Analytics and Insight Powers Faster Time to Resolution

Tuesday, June 4 | 10:30 a.m.
BRKENT-2283
7 Steps: Master the art of unifying Multicloud secure Connectivity and Desig - Cisco SD-WAN + Multicloud Defense

Tuesday, June 4 | 4:00 p.m.
BRKENT-1313
Making SD-WAN Easy: Operational Simplification and User Experience

Wednesday, June 5 | 10:30 a.m.
BRKENT-2166
End to End Segmentation with Cisco Catalyst SD-WAN and ISE

Wednesday, June 5 | 10:30 a.m.
BRKENT-3797
Advanced SD-WAN Policies Troubleshooting

Wednesday, June 5 | 2:30 p.m.
BRKENT-2126
3 Steps to Gain Actionable Visibility in the Cisco Catalyst SD-WAN using ThousandEyes

Thursday, June 6 | 8:30 a.m.
BRKENT-2123
Empower Your Meraki SD-WAN: Unleashing Unified SASE with Cloud-Driven Secure Connect

Thursday, June 6 | 9:30 a.m.
BRKENT-2660
Customer Case Studies: Lessons Learned from the Cisco SD-WAN Design Council

FINISH

Thursday, June 6 | 10:30 a.m.
BRKENT-2353
Building a Secure SaaS Branch Network with Advanced Monitoring Capabilities

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

Contact me at: lagranbe@cisco.com

The bridge to possible

Thank you