CISCO *Live!*

ALL IN

#CiscoLive

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 17, 2022.

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
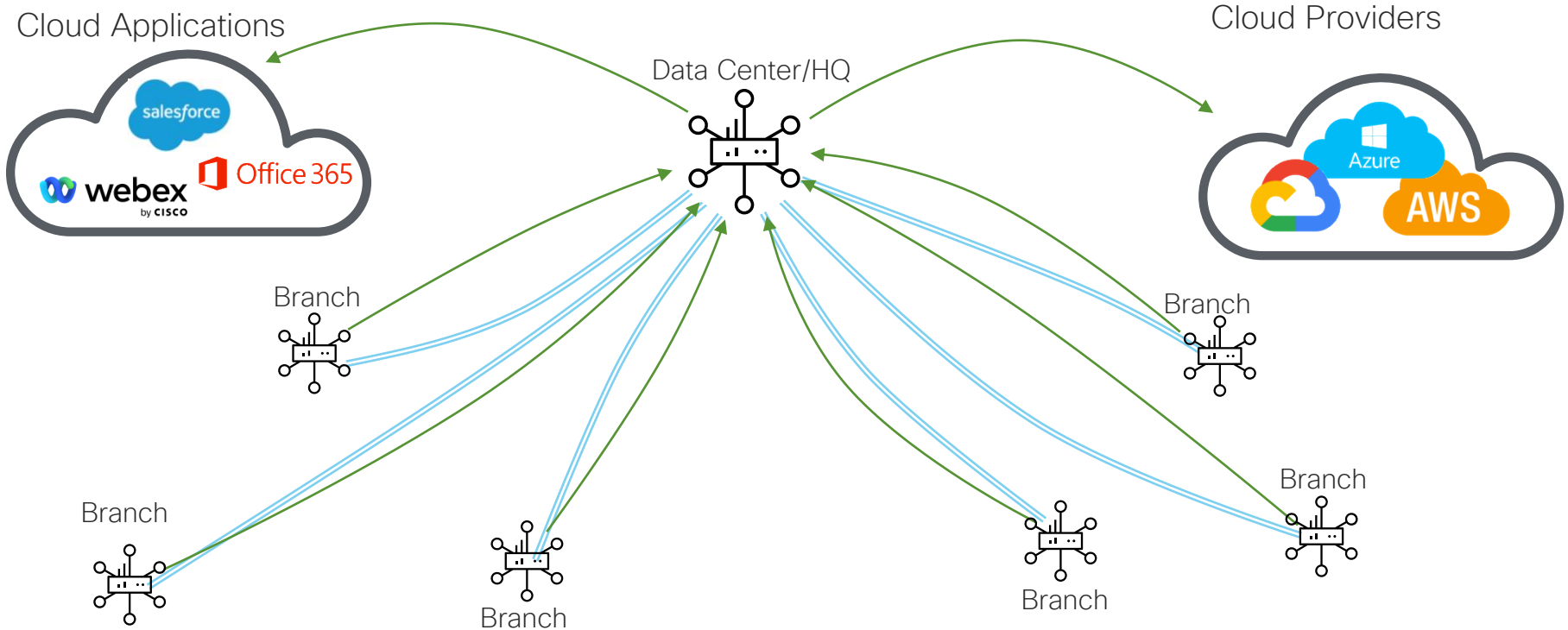 - Let's scratch the surface

- Learn More
  - Where to go and when

SD-WAN – This is it.

SD-WAN Recap

The Hardware Based WAN of Yesterday

Doesn't Keep up with the Needs of Today

Cloud Applications

Data Center/HQ

Cloud Providers

Branch

Branch

Branch

Branch

Branch

Branch

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

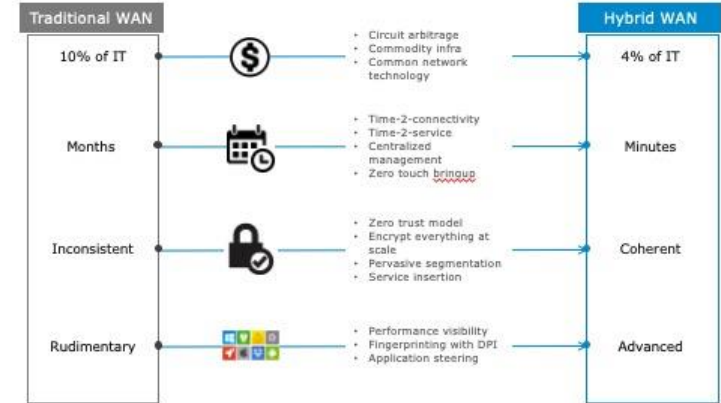Cloud

Remote Work

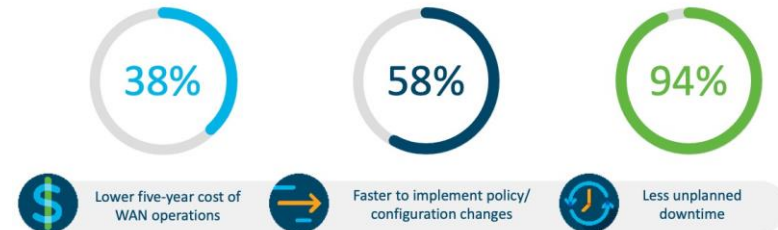* Software Defined Cloud Interconnect

Lets Rewind 3 years 2018
SD-WAN Benefits.

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

Need For SD-WAN – A CIO View

Traditional WAN			Hybrid WAN
10% of IT	$	• Circuit arbitrage • Commodity infra • Common network technology	4% of IT
Months	📅	• Time-2-connectivity • Time-2-service • Centralized management • Zero touch bringup	Minutes
Inconsistent	🔒	• Zero trust model • Encrypt everything at scale • Pervasive segmentation • Service insertion	Coherent
Rudimentary		• Performance visibility • Fingerprinting with DPI • Application steering	Advanced

IDC ANALYZE THE FUTURE

Business Value of Cisco SD-WAN

- 38% — Lower five-year cost of WAN operations
- 58% — Faster to implement policy/ configuration changes
- 94% — Less unplanned downtime

..and back to today 2022

Benefits of Cisco SD-WAN

Predictable app experience

Office 365
salesforce CONCUR
Dropbox

Support for evolving business application strategy

Cloud OnRamp for IaaS, SaaS and Colocation

Right security, right place

Secure segmentation across entire network stack

Full edge security stack from branch to cloud and colocations

Enterprise grade, simplified

Intent-based networking with multi-domain policy

Proven deployments to over 10,000+ sites

One user interface for security and SD-WAN across branch, cloud, and colocation

" **Application Analytics**

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

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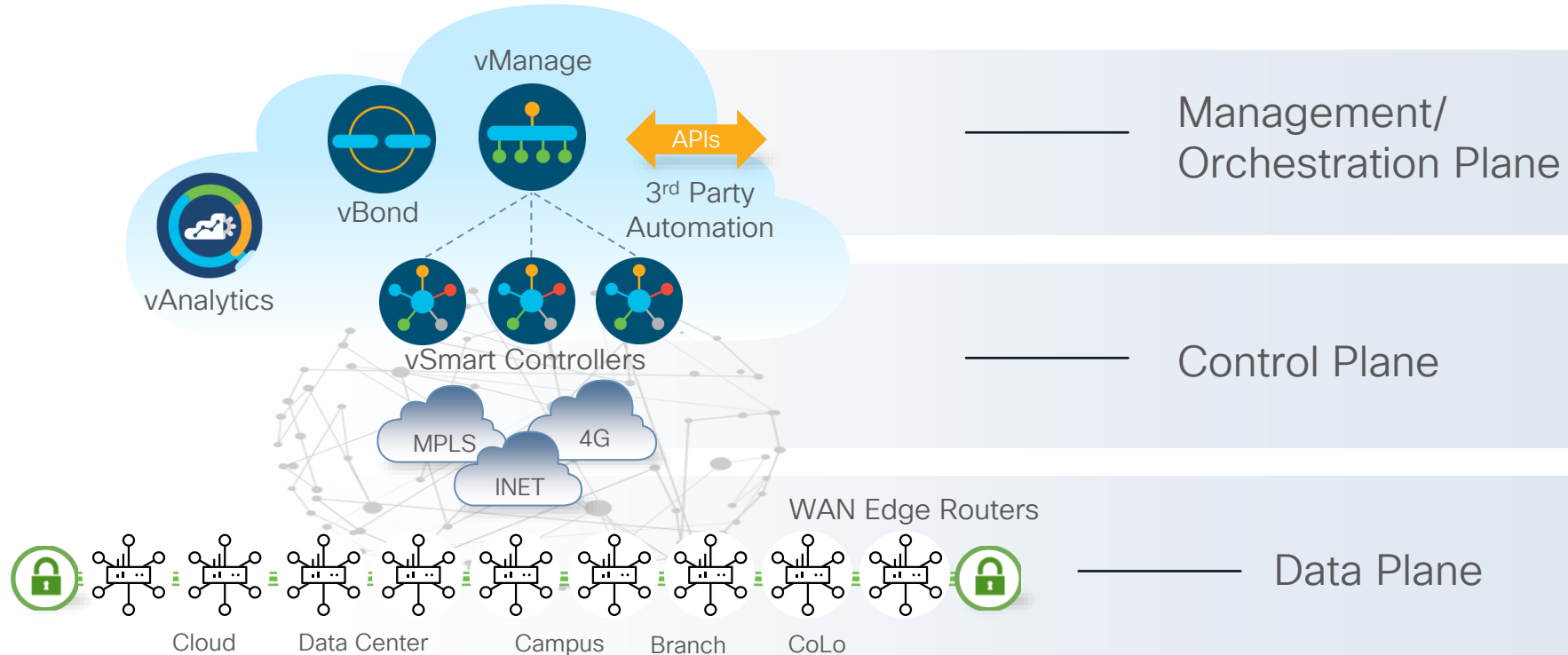
"

From Garrtner© Magic Quadrant for WAN Edge Infrastructure 2021
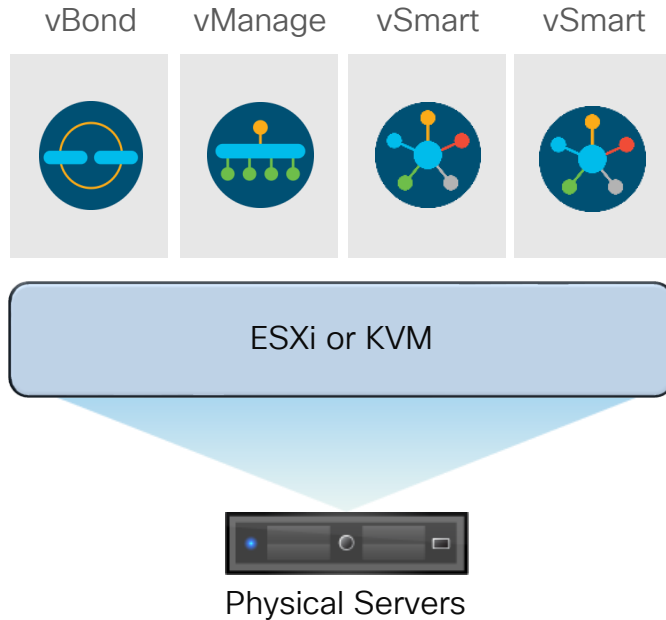
Solution Architecture

Cisco SD-WAN Solution Overview

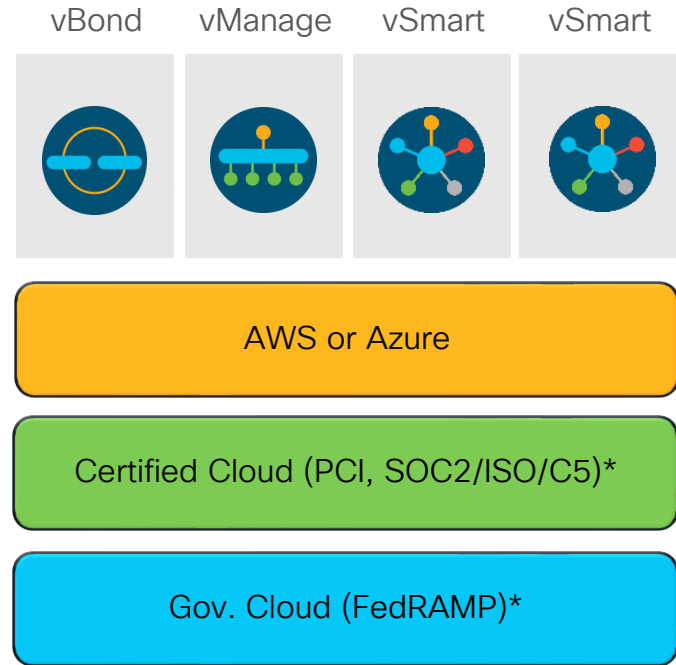Applying SDN Principles Onto The Wide Area Network

vManage

APIs

vBond

3rd Party Automation

vAnalytics

Management/ Orchestration Plane

vSmart Controllers

Control Plane

MPLS 4G INET

WAN Edge Routers

Data Plane

Cloud   Data Center   Campus   Branch   CoLo

Controller Deployment Methodology

On-Premise

vBond	vManage	vSmart	vSmart

ESXi or KVM

Physical Servers

Cisco or MSP/Customer Hosted

vBond	vManage	vSmart	vSmart

AWS or Azure

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

Gov. Cloud (FedRAMP)*

VM

*Only Cisco hosted

vAnalytics: Translate Raw Data into Intelligent Insights

Granular visibility

Multi-layer insights

Network KPIs

Application performance
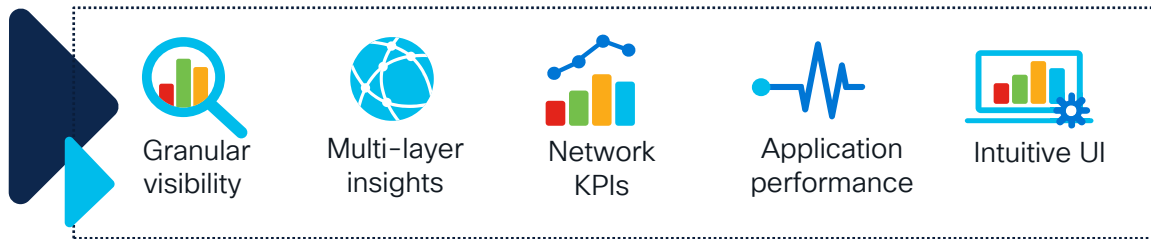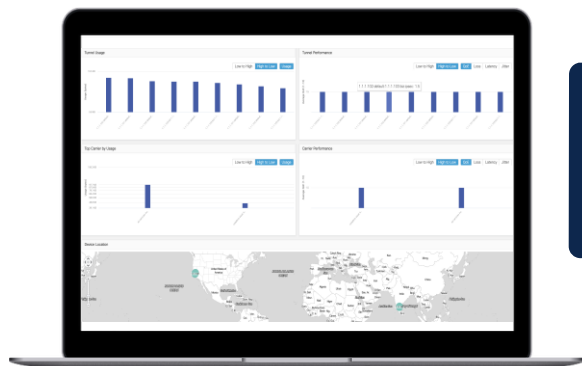
Intuitive UI

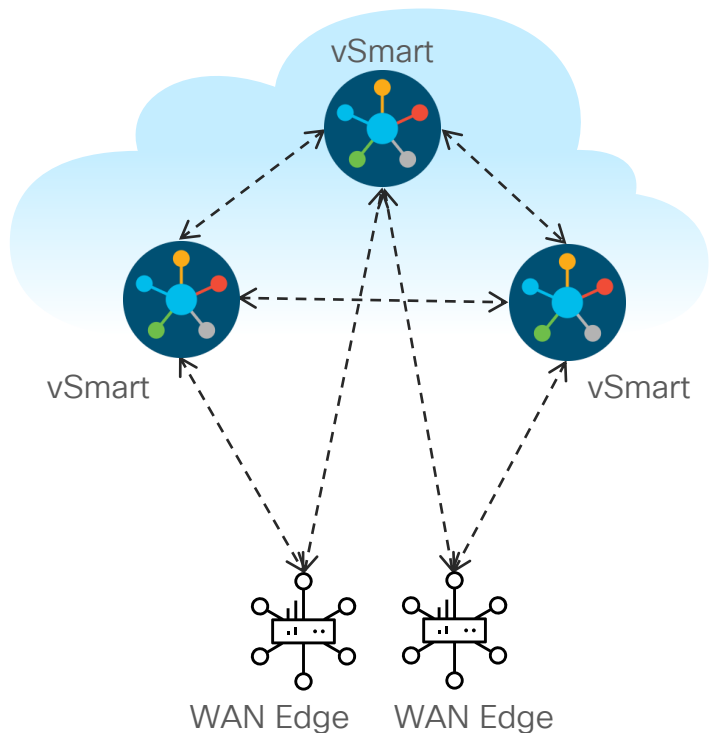Intuitive Visualization of Network KPIs and historical trends

Correlate Application behavior (QoE) with the network conditions

Leverage Insights for better planning

Robust, Scalable, Cloud-hosted SaaS Service

Software

Features

CISCO *Live!*

Overlay Management Protocol (OMP)

vSmart

vSmart
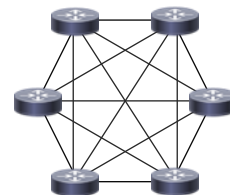
vSmart

WAN Edge   WAN Edge

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

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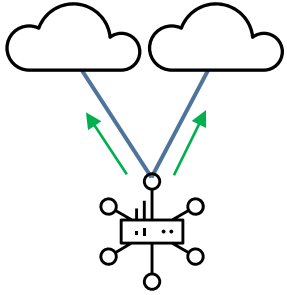
SD-WAN

Traditional

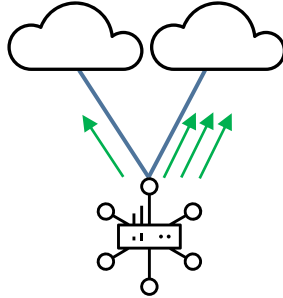VS
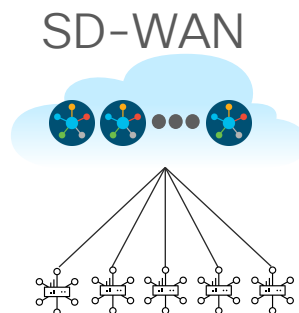
O(n) Control Complexity   O(n^2) Control Complexity
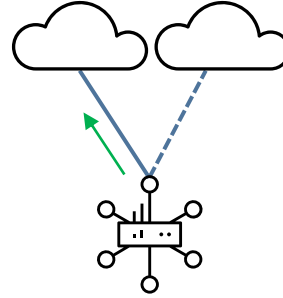
Fabric Communication

Per-Session Load-sharing
Active/Active

Per-Session Weighted
Active/Active

Application Pinning
Active/Standby

Application Aware Routing
SLA Compliant

SLA   SLA
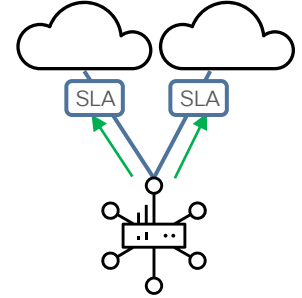
Single-hop Fabric
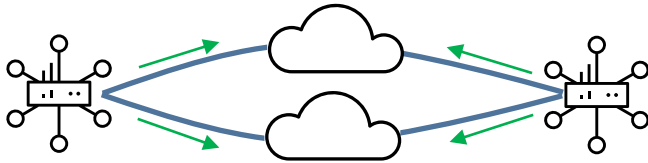
Multi-Region Fabric

Core
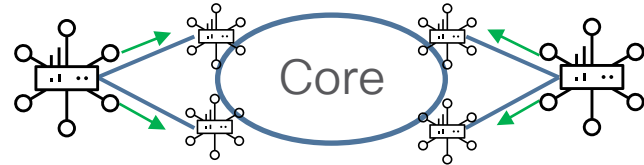
Lets bring it up

Automated, Zero-Touch Onboarding

Cisco PNP

① ② ③

WAN

④ IPsec Fabric
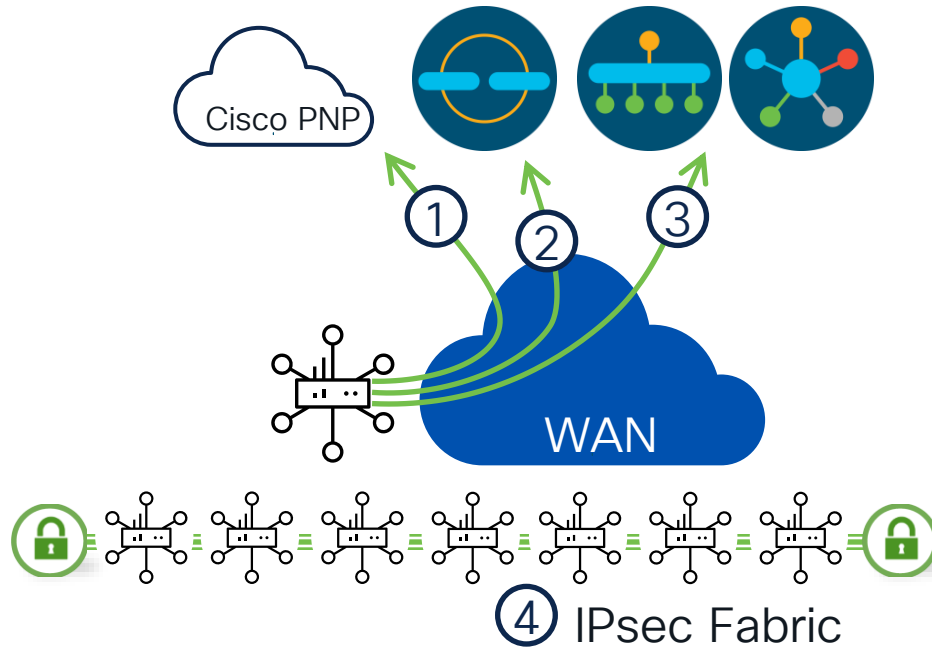
- SD-WAN appliance will onboard itself into the SD-WAN fabric automatically with no administrative intervention.

- 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

vSmart

Policies

---- OMP

DTLS/TLS Tunnel

IPSec Tunnel

BFD

OMP Update

OMP Update

OMP Update

OMP Update

WAN Edge

WAN Edge

Transport1

Transport2

TLOCs

TLOCs

VPN1 VPN2

VPN1 VPN2

BGP, OSPF, EiGRP, Rip, Connected, Static

BGP, OSPF, EiGRP, Rip, Connected, Static

A B

C D

Subnets

Subnets

Data Plane Privacy (Pairwise)

vSmart

Edge-B

BA AB

BA AB

Edge-A

MPLS

CA AC

CA AC

Edge-C

🟢 LAN   🔒 IPSec/GRE   - - - - -   DTLS

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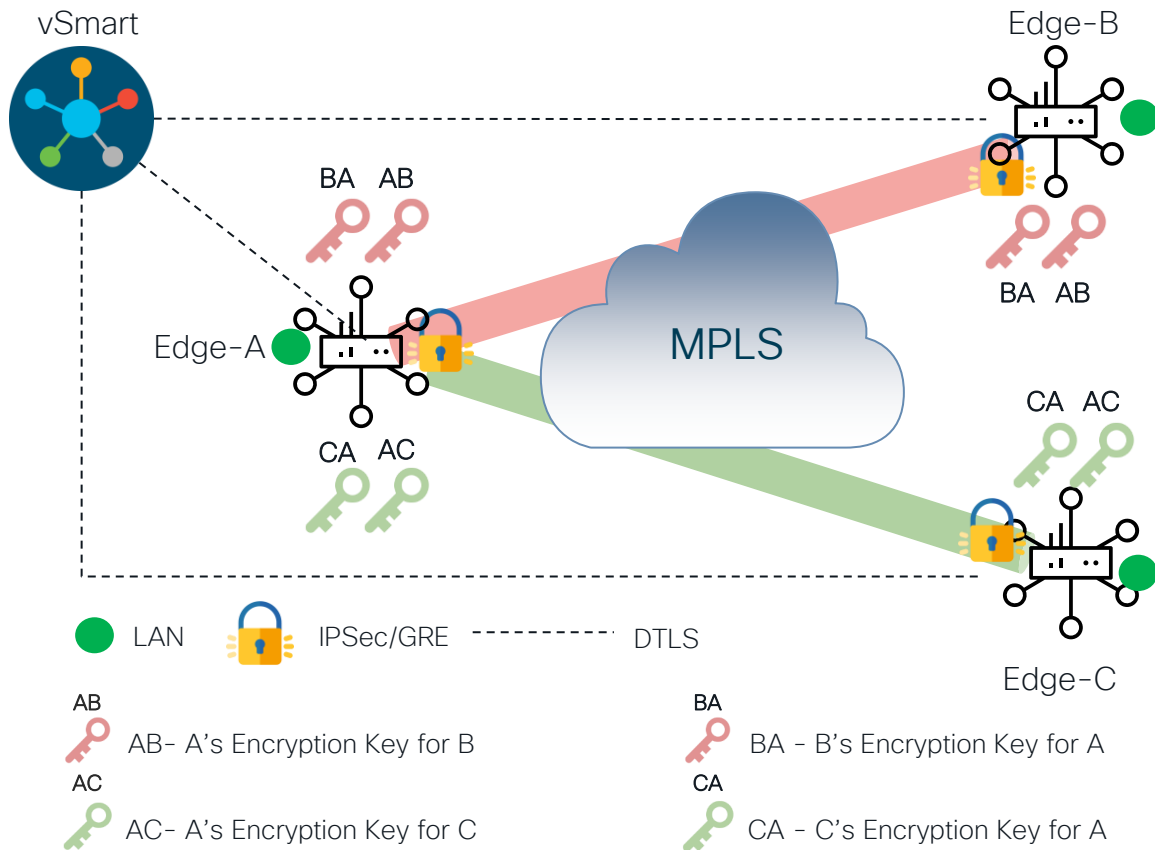
- Each WAN edge will create separate session key for each transport and for each peer
- Session keys will be advertised through vSmart using OMP
- When Edge-A needs to send traffic to Edge-B, it will use session key "AB" (B will use key "BA")
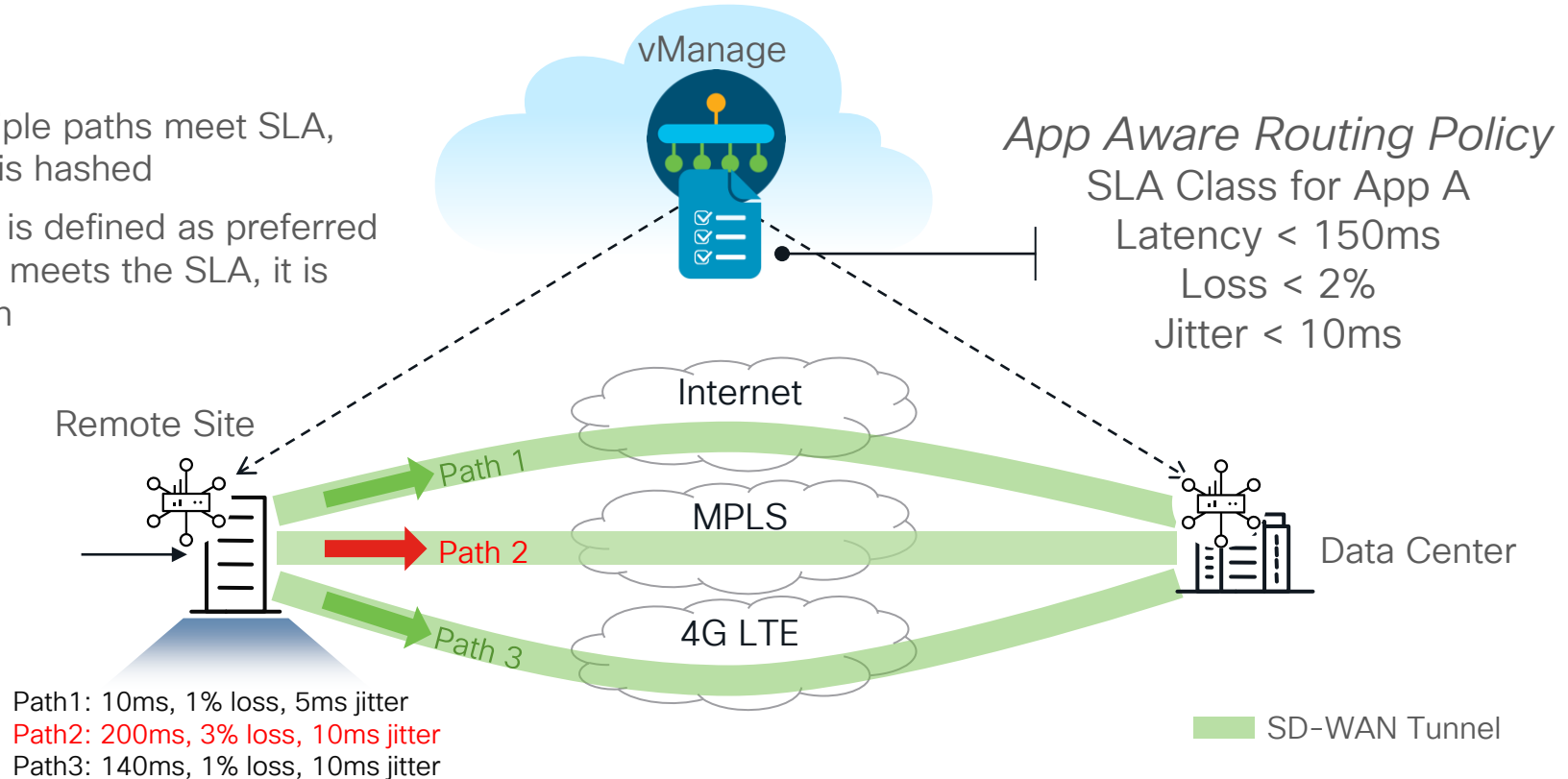- Backward compatible with non PWK devices
- PWK should be enabled

Application Aware Routing

vManage

- 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

Internet

Remote Site

Path 1

MPLS

Path 2

4G LTE

Path 3

Data Center

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

SD-WAN Tunnel

Key Building Blocks of AppQoE

Configuration Management System — vManage – Virtualized | Scalable | Network Insights

DRE, LZ — DRE Signature Database — 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

Single Tunnel

vSmart

Route Tables

A
B
C

WAN Edge Router

MPLS

Inet

4G/LTE

A
B
C

WAN Edge Router

Full Mesh

Hub and Spoke

Partial Mesh

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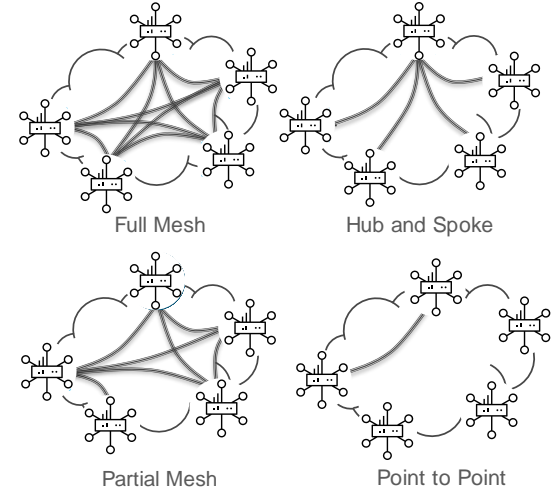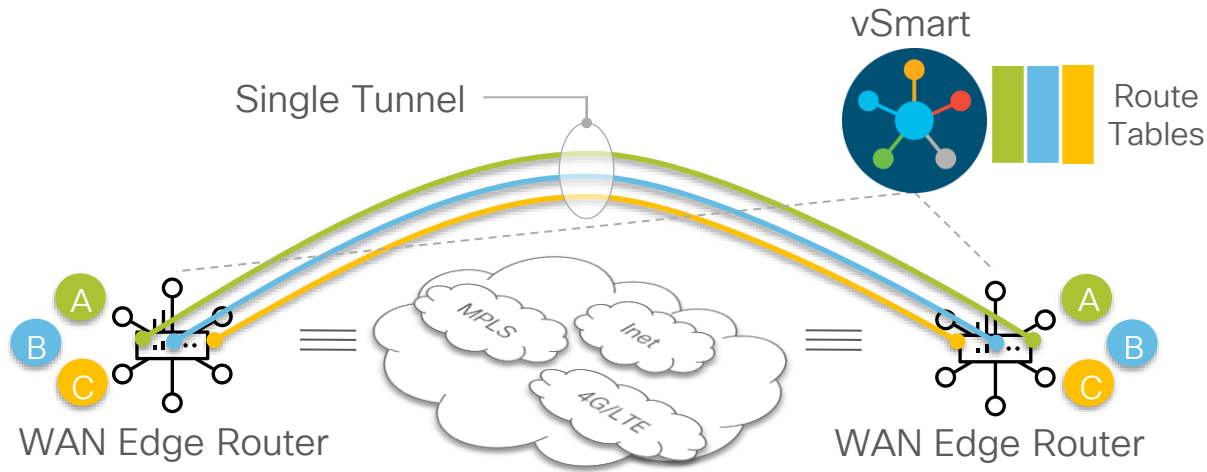
Segment connectivity across the SD-WAN fabric without reliance on underlay transport

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

How SD-WAN Exposes New Security Challenges

Internet IaaS/SaaS

NO SECURITY

Data Center

Corporate Software

BASIC/NO SECURITY

Branch/Campus

Users

SD-WAN Fabric

WAN Edge Device

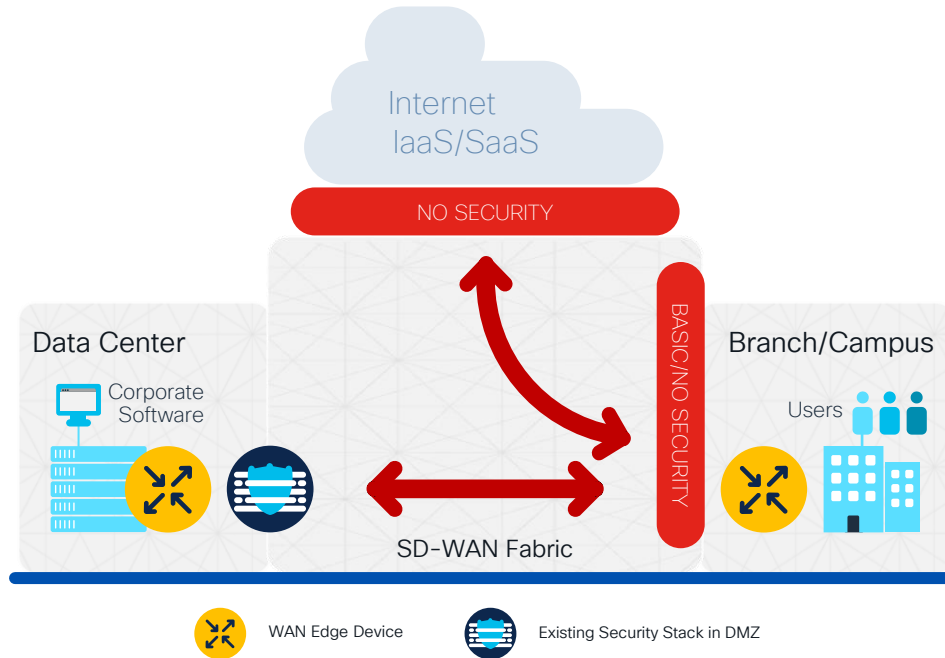Existing Security Stack in DMZ

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

SaaS/IaaS Application

Branch Security

Cloud Security

Thin branch with security in the cloud

SaaS/IaaS Application

Cloud Security

@Regional Hub

Security Services as VNF at Regional Colocation Hub

SaaS/IaaS Application

Colocation
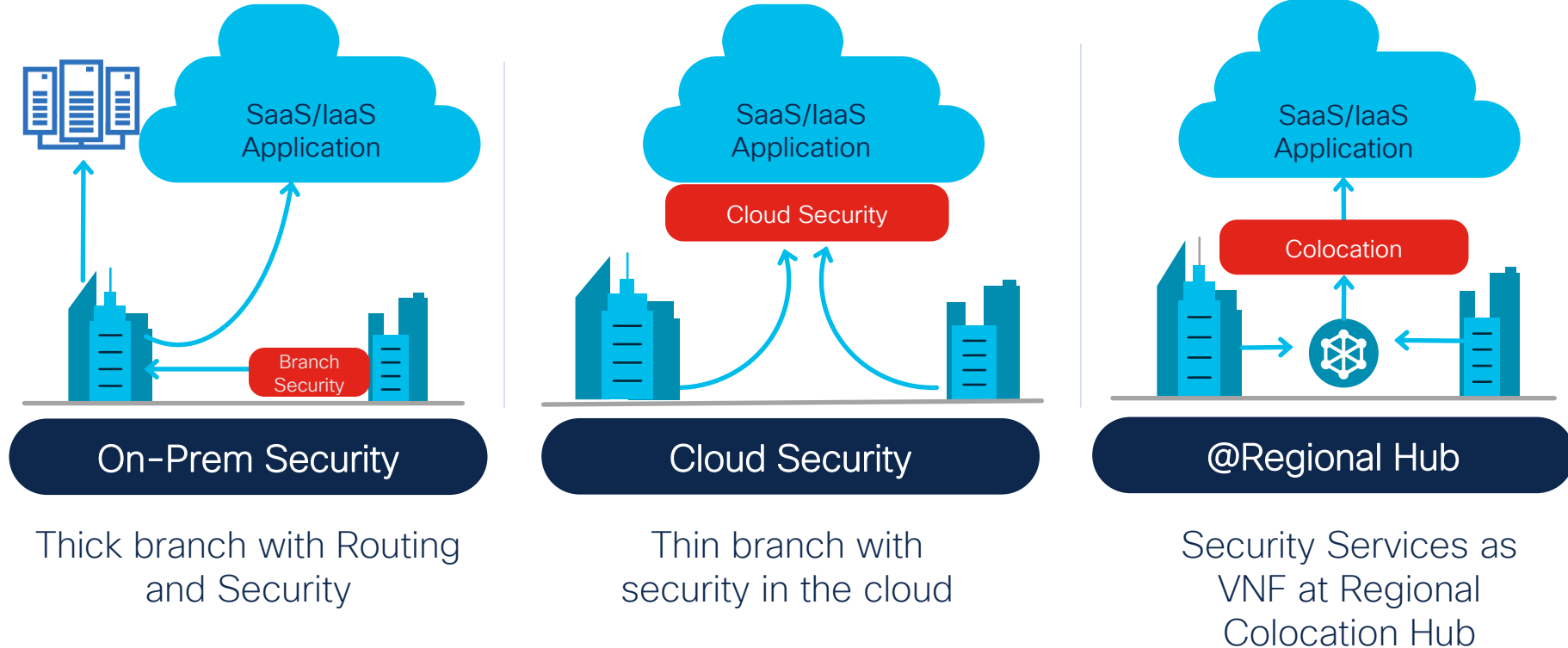
Cisco SD-WAN Security & SASE Solution
Consistent across on-prem and cloud

Cisco
SD-WAN
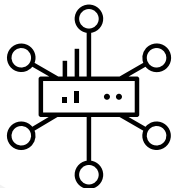
Cisco
Security

Enterprise Firewall
Layer 3 to 7 apps classified

Intrusion Protection System
Most widely deployed IPS engine in the world

URL-Filtering
Web reputation score using 82+ web categories

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

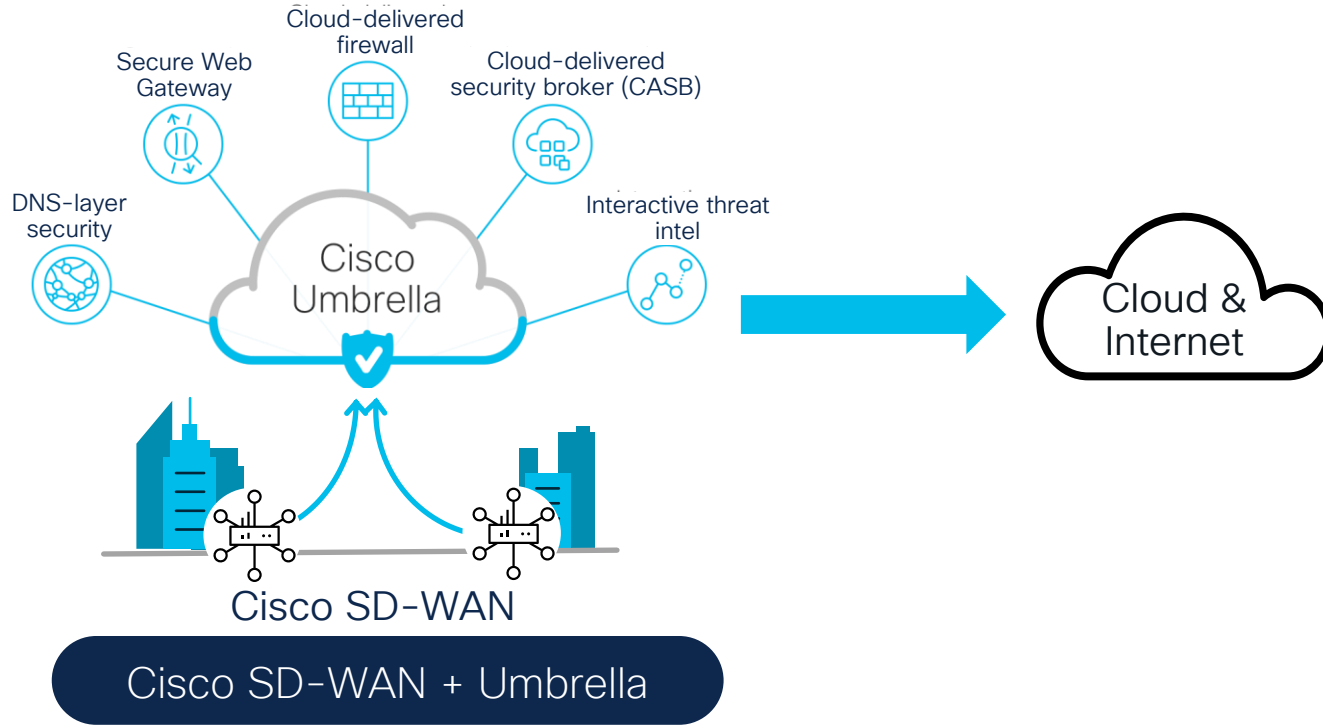**SSL Proxy**
Detect Threats in Encrypted Traffic

Umbrella Cloud Security
DNS Security/Cloud FW with Cisco Umbrella

Transitioning towards a Cloud security model

Cloud-delivered firewall

Secure Web Gateway

Cloud-delivered security broker (CASB)

DNS-layer security

Interactive threat intel

Cisco Umbrella

Cloud & Internet

Cisco SD-WAN

Cisco SD-WAN + Umbrella

Cloud OnRamp
for SaaS

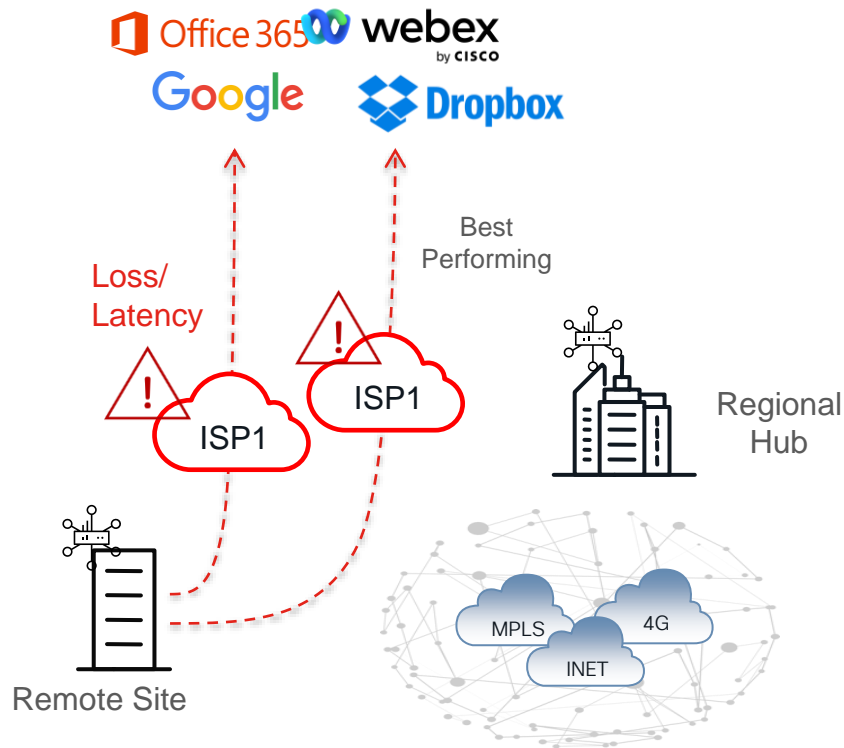# SaaS Optimization Challenges
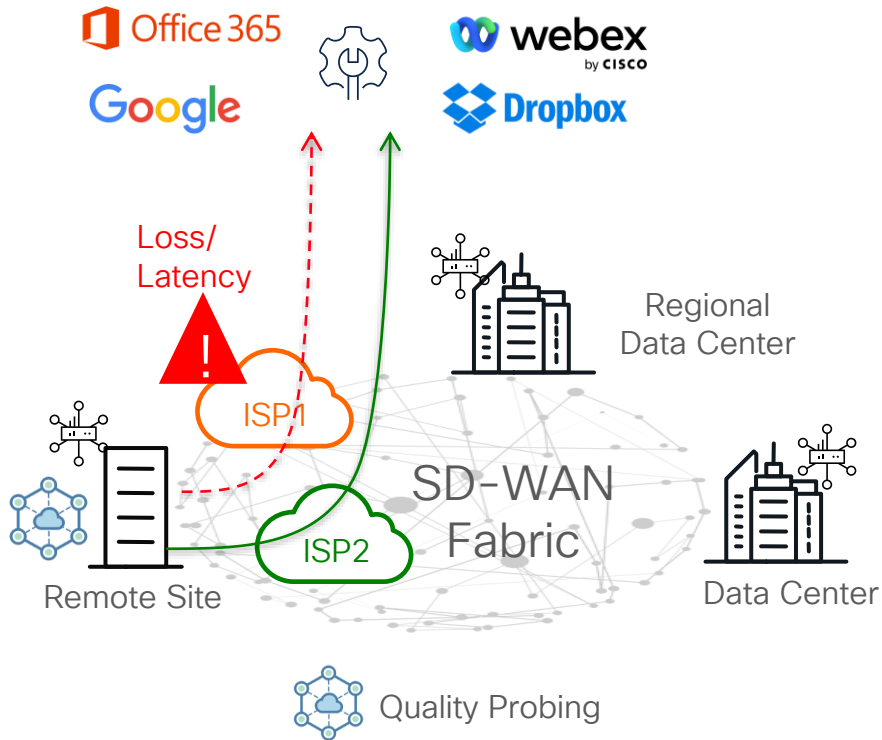
- Internet circuits performance is unreliable.

- How to get performance visibility for each available path?

- When specific path is having performance issues, How to automatically steer traffic ?

Office 365   webex by CISCO
Google   Dropbox

Best Performing

Loss/ Latency

! ISP1

! ISP1

Regional Hub

Remote Site

MPLS   4G
INET

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
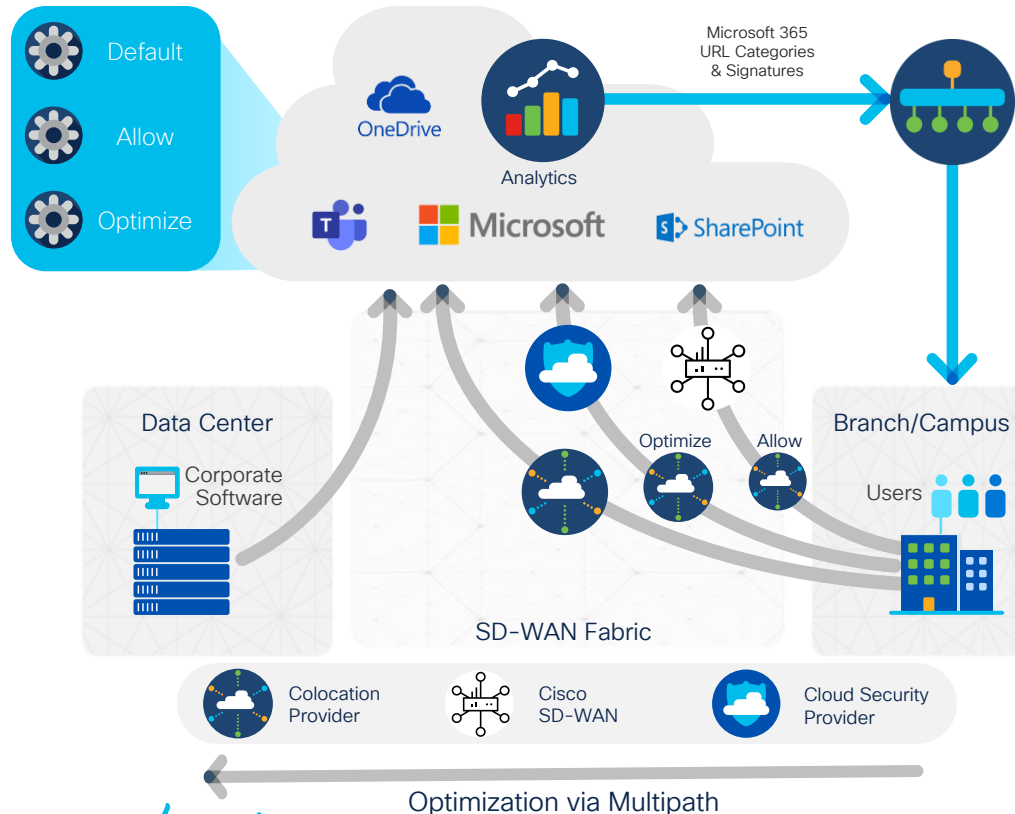
Microsoft 365 Optimization with Cisco SD-WAN
Improving the user experience

Default

Allow

Optimize

OneDrive

Analytics

Microsoft

SharePoint

Microsoft 365
URL Categories
& Signatures

Data Center

Corporate
Software

Optimize   Allow

Branch/Campus

Users

SD-WAN Fabric

Colocation
Provider

Cisco
SD-WAN

Cloud Security
Provider

Optimization via Multipath

Developed in Partnership with Microsoft
- SD-WAN Solution is **Microsoft Networking Partner Program** Certified
- First SD-WAN vendor to support **Microsoft 365 Informed Network Routing (Telemetry)**

Optimal SaaS experience
- Optimal path selection through proactive link probing
- Optimization at scale with lower TCO
- Visibility on QoE metrics
- App aware path selection through telemetry exchange
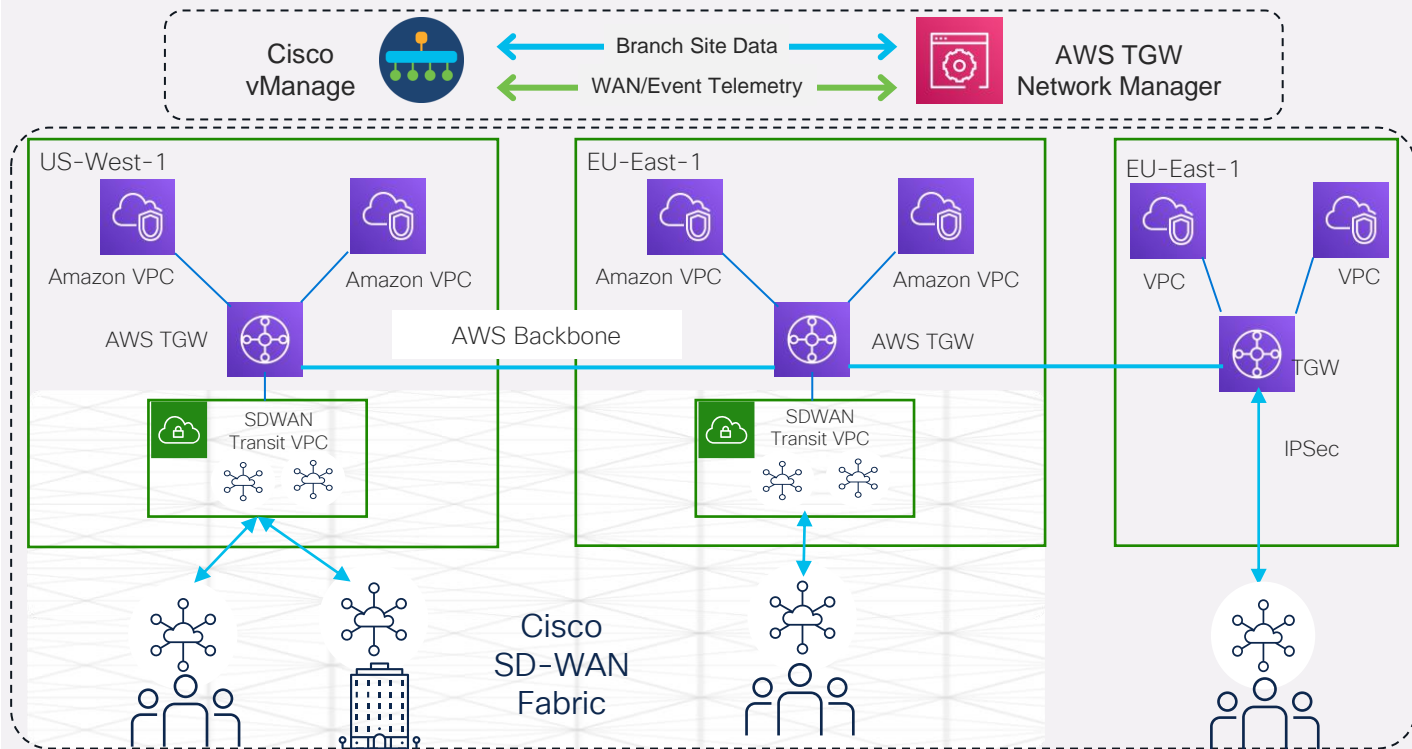- Granular policy per class of Microsoft 365 application

Microsoft Networking Partner Program
Microsoft 365 Informed Network Routing

Cloud OnRamp for MultiCloud

Cloud onRamp now supports AWS Transit Gateway

Cloud onRamp for Multicloud (Azure VWAN)
SD-WAN NVA (Network Virtual Appliances) in VWAN Hub
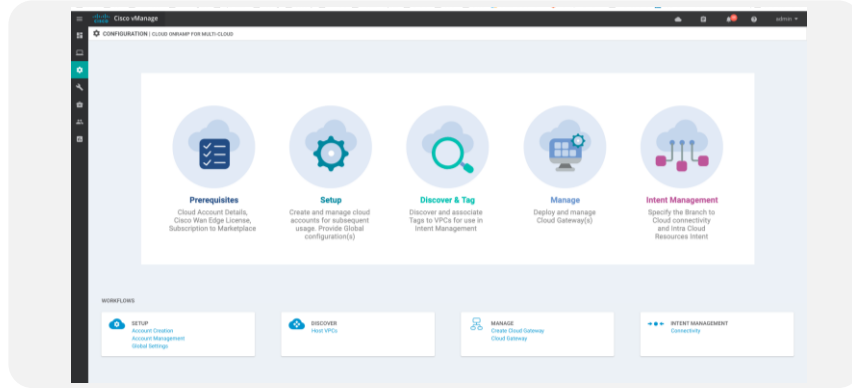
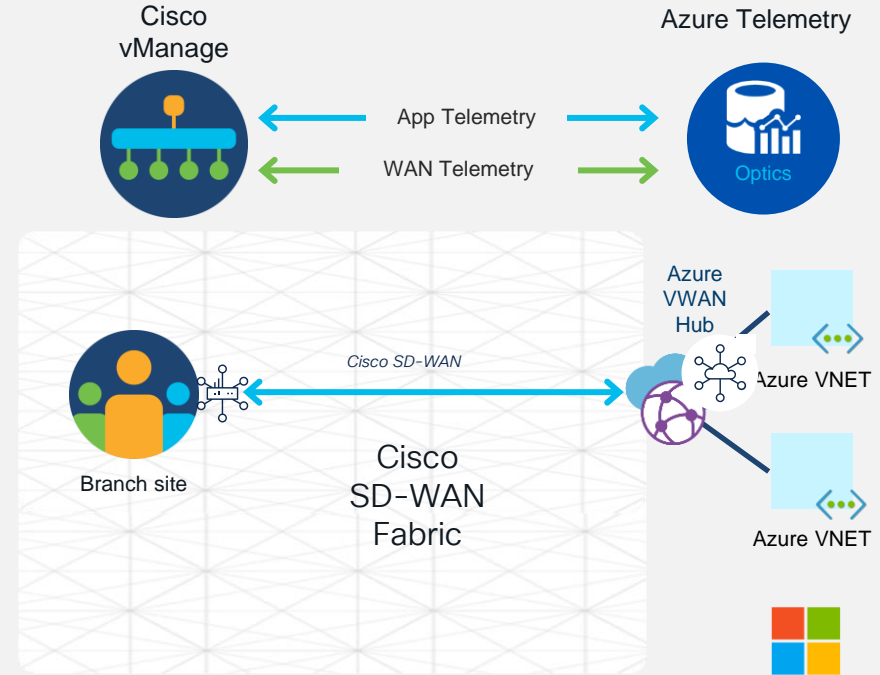Seamless SD-WAN extension to Microsoft Azure using virtual instances of on-prem devices

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

Azure Telemetry Sharing: Advanced APM, troubleshooting and remediation

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

Cisco SD-WAN Cloud Hub

Enterprise site — Google Cloud PoP — Google Cloud

- Simple
- Automated
- Secure

Enterprise site — Google Cloud PoP — Cisco SD-WAN / Google Cloud — Google Cloud PoP — Enterprise site
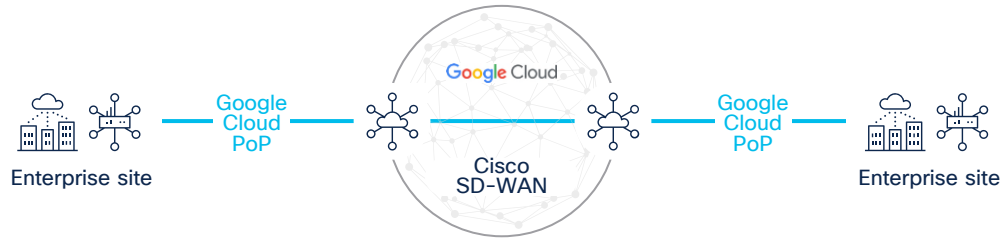
SD-WAN fabric across cloud service provider global network

- On-demand
- High performance
- Global connectivity

- Single pane of glass management
- On-demand connectivity
- Highly available backbone
- Secure SD-WAN

Cloud OnRamp With Interconnect

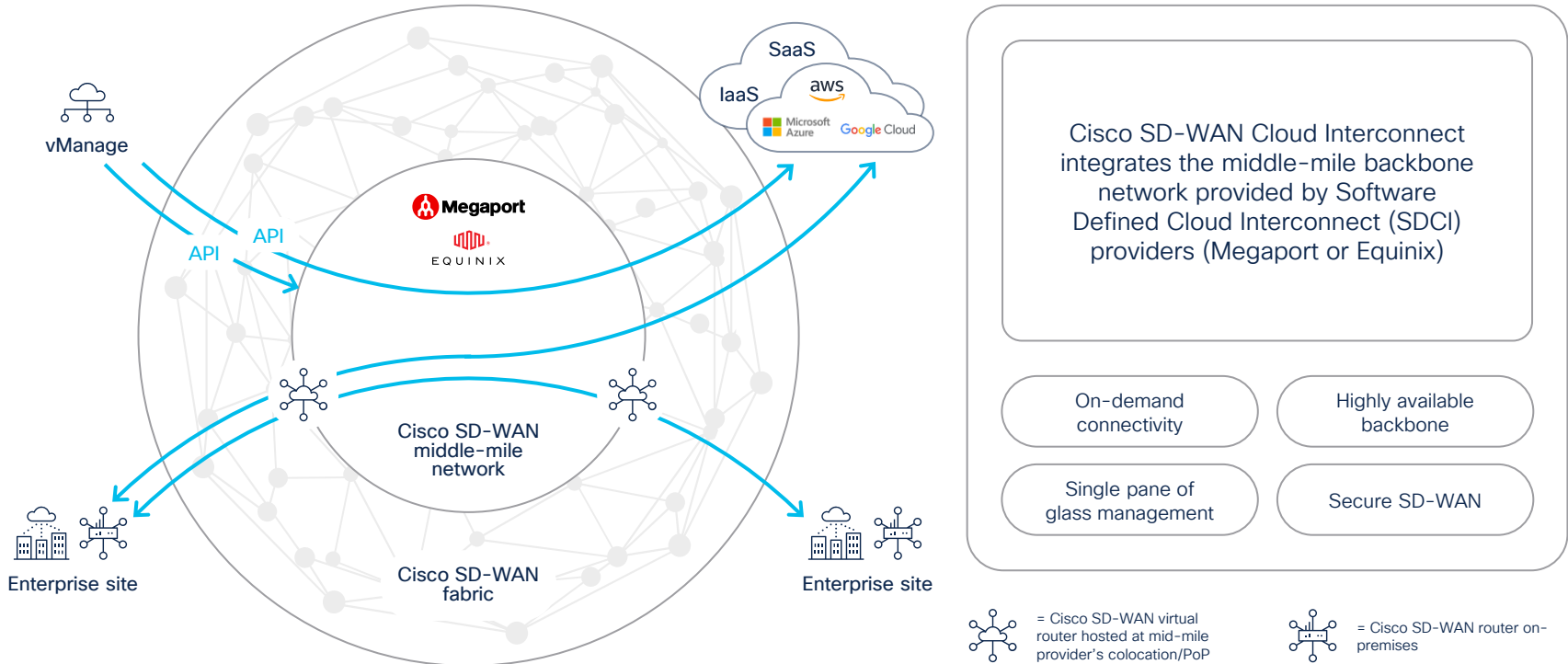# Cisco SD-WAN Cloud Interconnect

Cisco SD-WAN Cloud Interconnect integrates the middle-mile backbone network provided by Software Defined Cloud Interconnect (SDCI) providers (Megaport or Equinix)

On-demand connectivity

Highly available backbone

Single pane of glass management

Secure SD-WAN

vManage

API

API

SaaS

IaaS

aws

Microsoft Azure

Google Cloud

Megaport

EQUINIX

Cisco SD-WAN middle-mile network

Cisco SD-WAN fabric

Enterprise site

Enterprise site

= Cisco SD-WAN virtual router hosted at mid-mile provider's colocation/PoP

= Cisco SD-WAN router on-premises

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

START

June 13 | 8:00 a.m.
BRKENT-2108
Cisco SD-WAN: Start Here

June 13 | 9:30 a.m.
BRKENT-1005
SD-WAN Routing Innovations and Usecases

June 13 | 4:00 p.m.
BRKENT-2001
Secure SDWAN and Cloud Edge Transformation

June 14 | 10:30 a.m.
BRKENT-2135
Improving Application Quality of Experience through Cisco SD-WAN Middle-Mile Optimization

June 14 | 1:00 p.m.
BRKENT-2183
Cisco SD-WAN - The Usual Suspects

June 14 | 4:00 p.m.
BRKENT-2126
Three Steps to Gain Actionable Visibility in the Cisco SD-WAN Using ThousandEyes

June 14 | 4:00 p.m.
BRKENT-3793
Advanced SD-WAN Routing Troubleshooting

June 15 | 2:30 p.m.
BRKENT-2292
Hierarchical SD-WAN Overview and Principles

June 15 | 10:30 a.m.
BRKENT-2423a
SD-WAN From Design to Reality - Part 1

June 16 | 11:00 a.m.
BRKENT-2312
Cisco SD-WAN Security Evolution to SASE

FINISH

June 16 | 1:00 p.m.
BRKENT-3412
How to Optimize SaaS Applications using Cisco SD-WAN

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

CISCO Live!

BRKENT-2108

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers
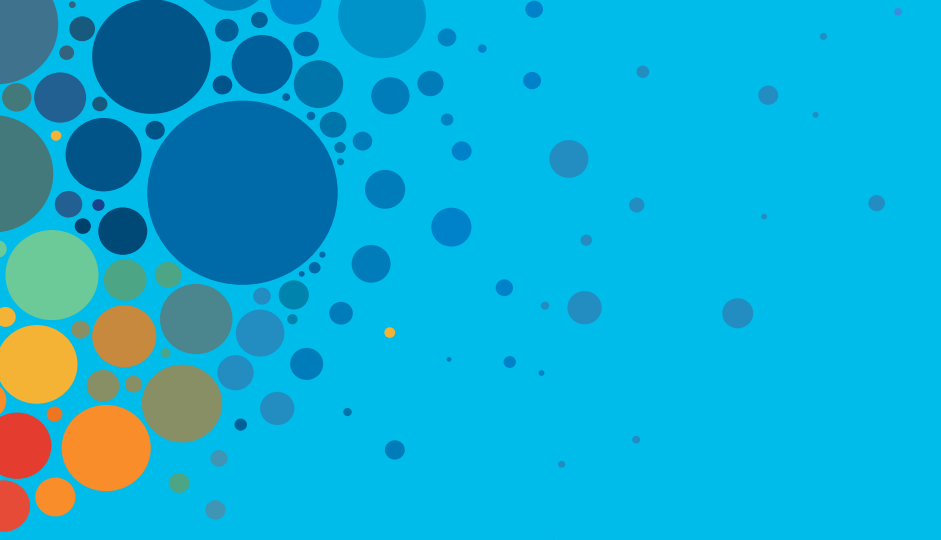
Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

Cisco SD-WAN @ CL WoS: Demo Highlights

- **ITO-01**: Cisco SD-WAN Management and Analytics (10 mins)
  - UX 2.0: Rapid Site Configuration Workflow (3-click Deployment)
  - Cloud onRamp Multi-Cloud
    - ✓ Support for various clouds: AWS, Azure, GCP, AWS Gov, Azure Gov
    - ✓ Cloud audit and 1-click self-healing
  - vAnalytics

- **SDW-03**: SD-WAN Remote Access and Remote Workers Solution (15-20 mins)
  - SD-WAN Remote Access
  - Identify-based ZBFW
  - SIG Integration

- **SDW-02**: Cisco SD-WAN Multicloud & Analytics (20-25 mins)
  - MSP Co-management (5-7 mins)
  - Cloud onRamp SDCI: Equinix (10 mins)
  - Cloud onRamp SaaS: Custom Apps (5-7 mins)

DEMSDW-02: SD-WAN Multicloud & Analytics
DEMSDW-03: SD-WAN for Remote Users

Platforms

SD-WAN Remote Access

Intuitive Experience

UX 2.0 Rapid Site Config

App Experience

SaaS Optimization M365, Webex, and Custom Apps

Multicloud

Multicloud Access (AWS/Azure/GCP)

SDCI / Cloud Backbone

Security

Unified Policy and Unified Logging

Identity-based ZBFW

SIG Integration

AIOps

vAnalytics v3

MSP

Multi-tenant Controllers (Control Plane)

Co-managed SD-WAN Service

Thank you

CISCO *Live!*

ALL IN

#CiscoLive