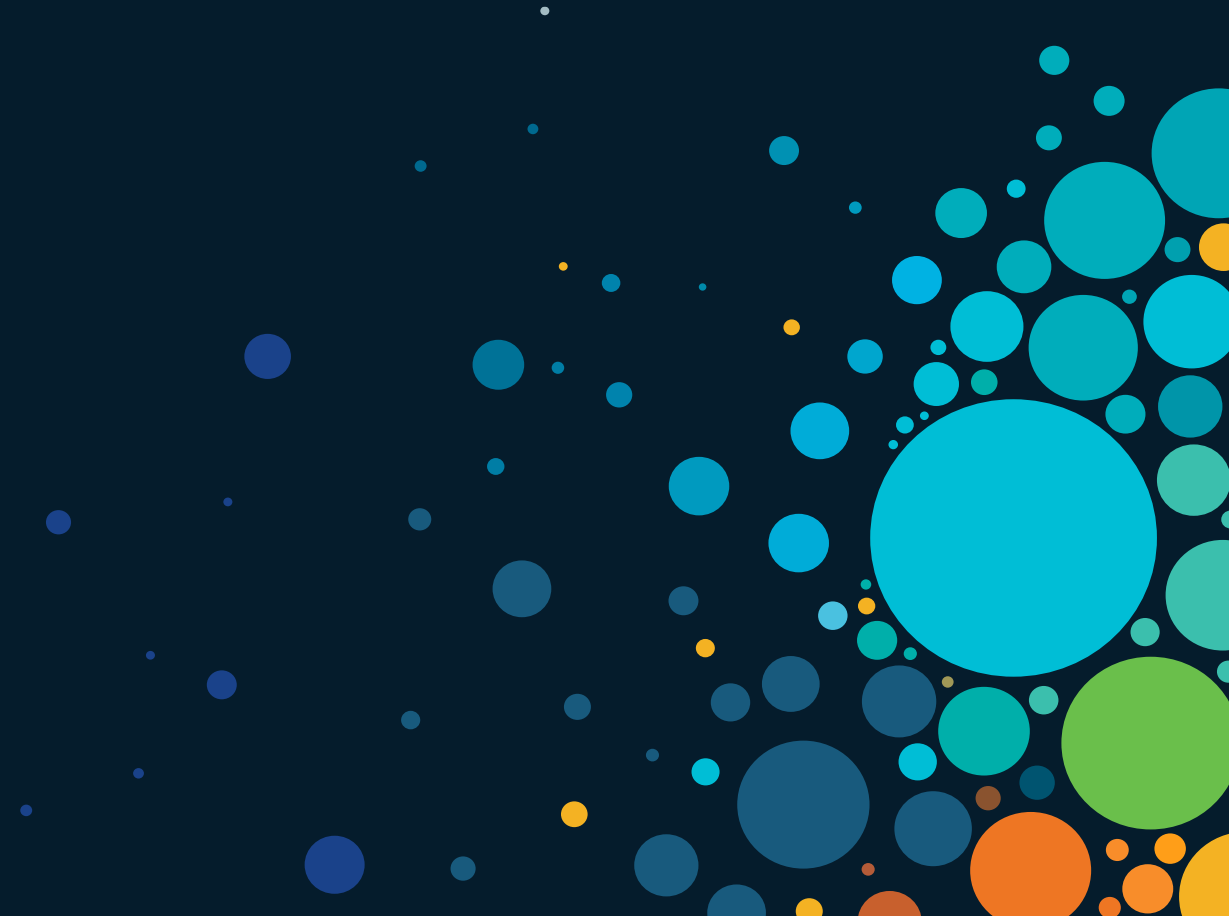
# Cisco SD-WAN

Miroslav Brzek

Technical Solutions Architect



# Agenda

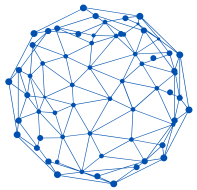
- WAN Network Transformation
- Cisco SD-WAN solution overview
- SD-WAN Use Cases
- Conclusion

# Enterprise Networks are Transforming

Devices and Things

Data Center/ Private Cloud

Campus and Branch Users



Cisco SD-WAN Fabric


SaaS

Mobile Users


IaaS

Apps are moving to the Cloud; **Application Experience is critical**

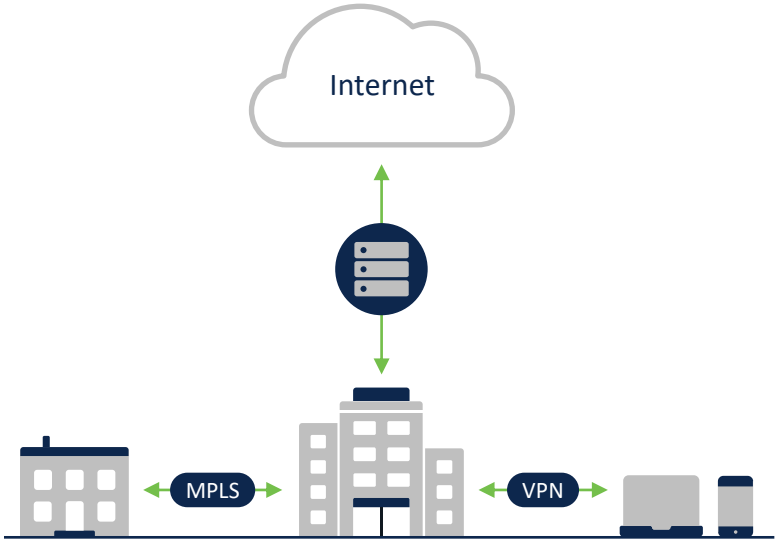
Traditional Security Perimeter is changing

Cyber Threats are increasing and sophisticated

Mobility is prevalent; IoT is growing explosively

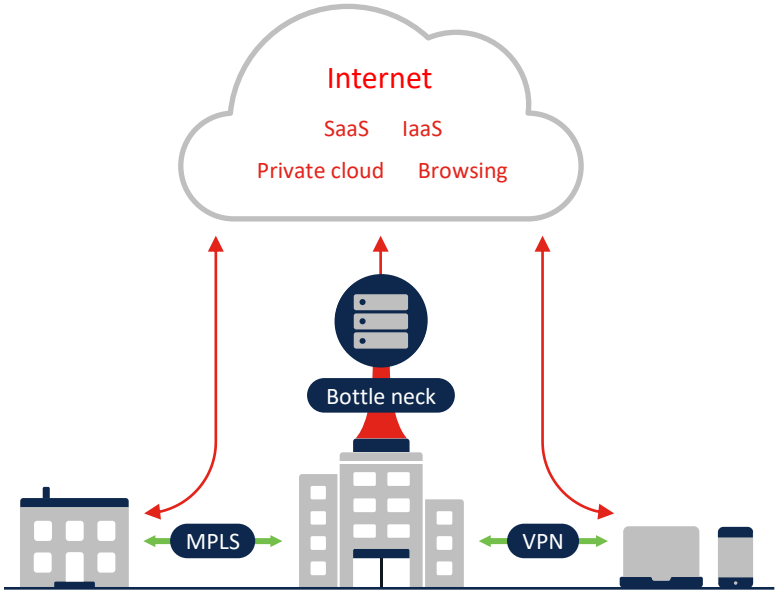
# WAN Network Transformation

## Before




Apps: Hosted in datacenter
Users: Connected to corporate network to work
Network: Centralized
Security: On-premises security stack

## What's changed




Apps: More hosted in the cloud
Users: More work done off-network
Network: De-centralized
Security: Gaps in protection

# The traditional networking model is inadequate

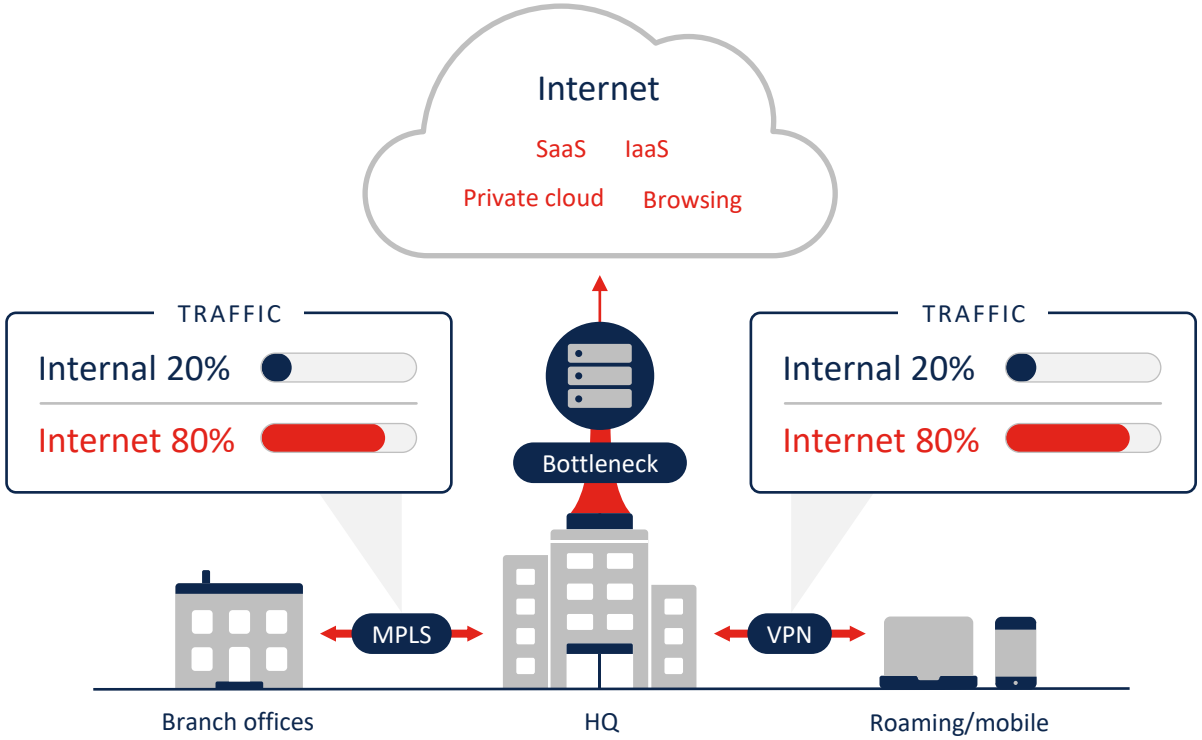
Changes in traffic patterns are creating bottlenecks and performance challenges

## Data Center Backhaul

- Increased App Latency
- Unpredictable User Experience

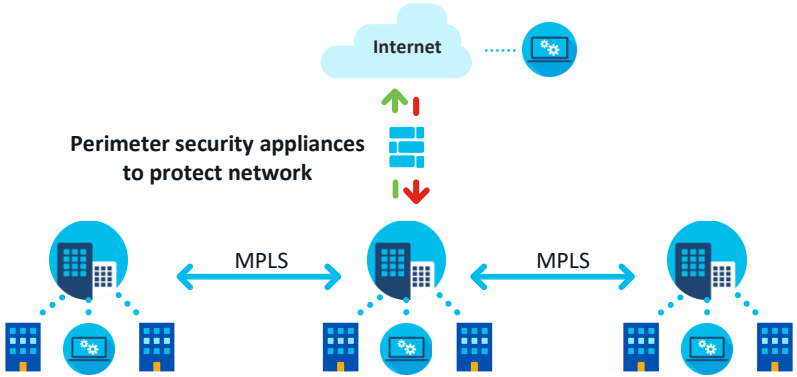
## Problems:

- Costs
- App performance
- User experience
- SaaS adoption issues



# The new role of WAN

## Site-to-site

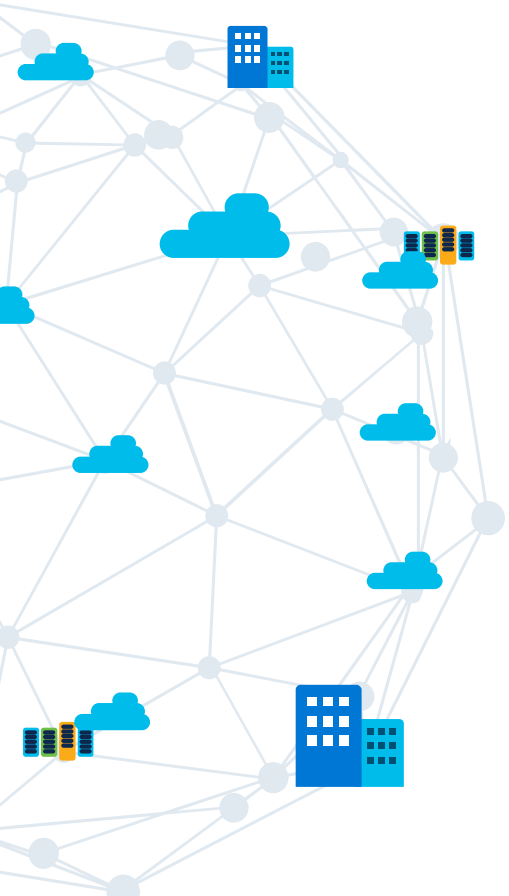



## User-to-application


**Site-to-site connectivity**
**MPLS transport**
**Core routing services**
**Perimeter security**
**Connectivity SLA**

**Site-to-Cloud Connectivity**
**SD-WAN/IP overlays over Internet**
**Routing, observability**
**Cloud-delivered security**
**Application SLA**

# Cloud Access is Shifting



## Situation

Cloud migration for IT agility in delivering best experience

**60%** of organizations expect majority of apps to be SaaS
**79%** of orgs shifting to some or all direct internet access

## Impact

Complexity in provisioning across multiple cloud providers in many ways

Expanded attack surface

Gaps in visibility beyond the campus network boundaries

# Cisco SD-WAN Solution Overview

# Cisco SD-WAN Architecture

## Orchestration Plane

- First point of authentication
- Distributes list of vSmarts/ vManage to all vEdge routers
- Facilitates NAT traversal

## Management Plane

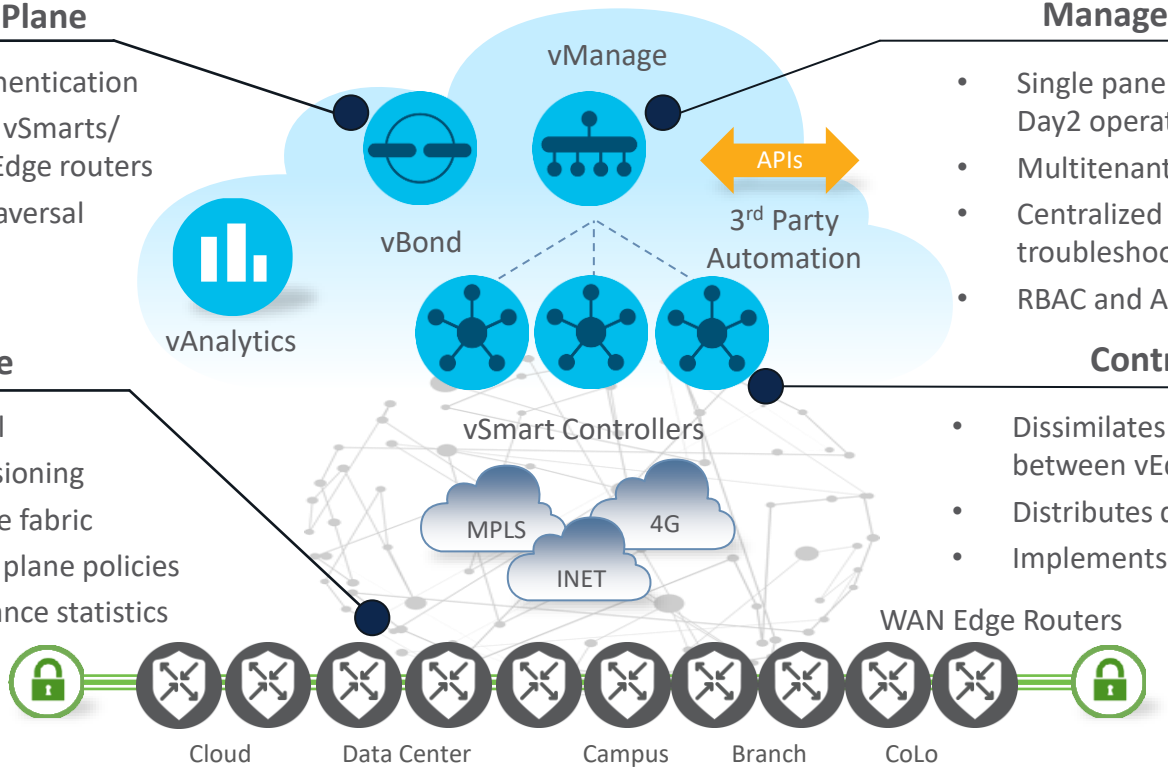
- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant or single-tenant
- Centralized provisioning, troubleshooting and monitoring
- RBAC and APIs

## Data Plane

- Physical or virtual
- Zero Touch Provisioning
- Establishes secure fabric
- Implements data plane policies
- Exports performance statistics

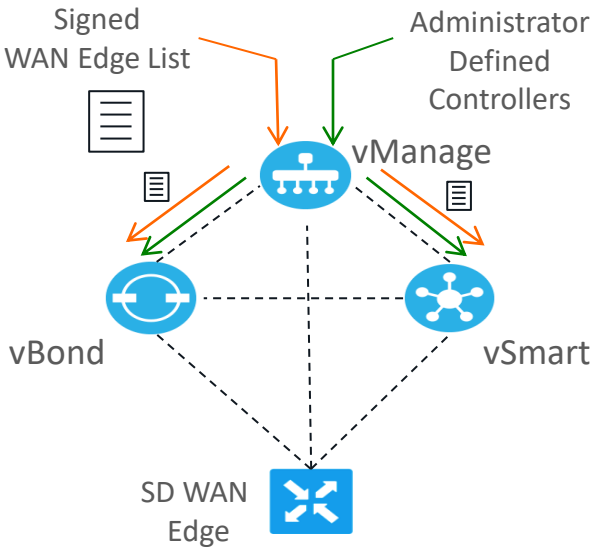
## Control Plane

- Dissimilates control plane information between vEdges
- Distributes data plane policies
- Implements control plane policies



# Cisco SD-WAN - Zero Trust Architecture

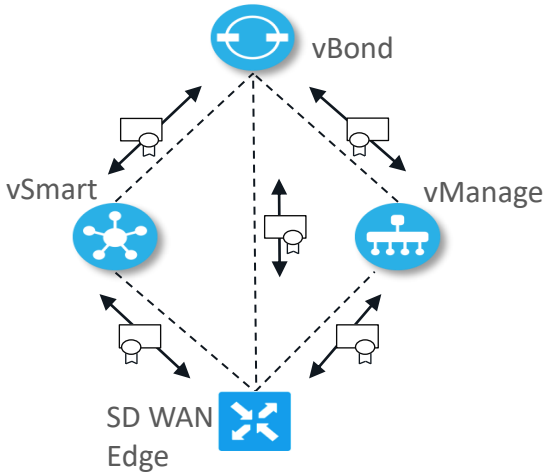
## WAN Edge and Controllers White-List




| Controller Type | Hostname | System IP | Certificate Serial |
|---|---|---|---|
| vBond | vBond1 | 1.1.1.2 | 46FD1AC2B1465B8E2EB5D7F7E10E1FEC |
| vBond | vBond2 | 1.1.1.11 | 64DAABDD54F3918EE30EA1CA13A97F06 |
| vManage | | | |
| vSmart | | | |
| vSmart | | | |

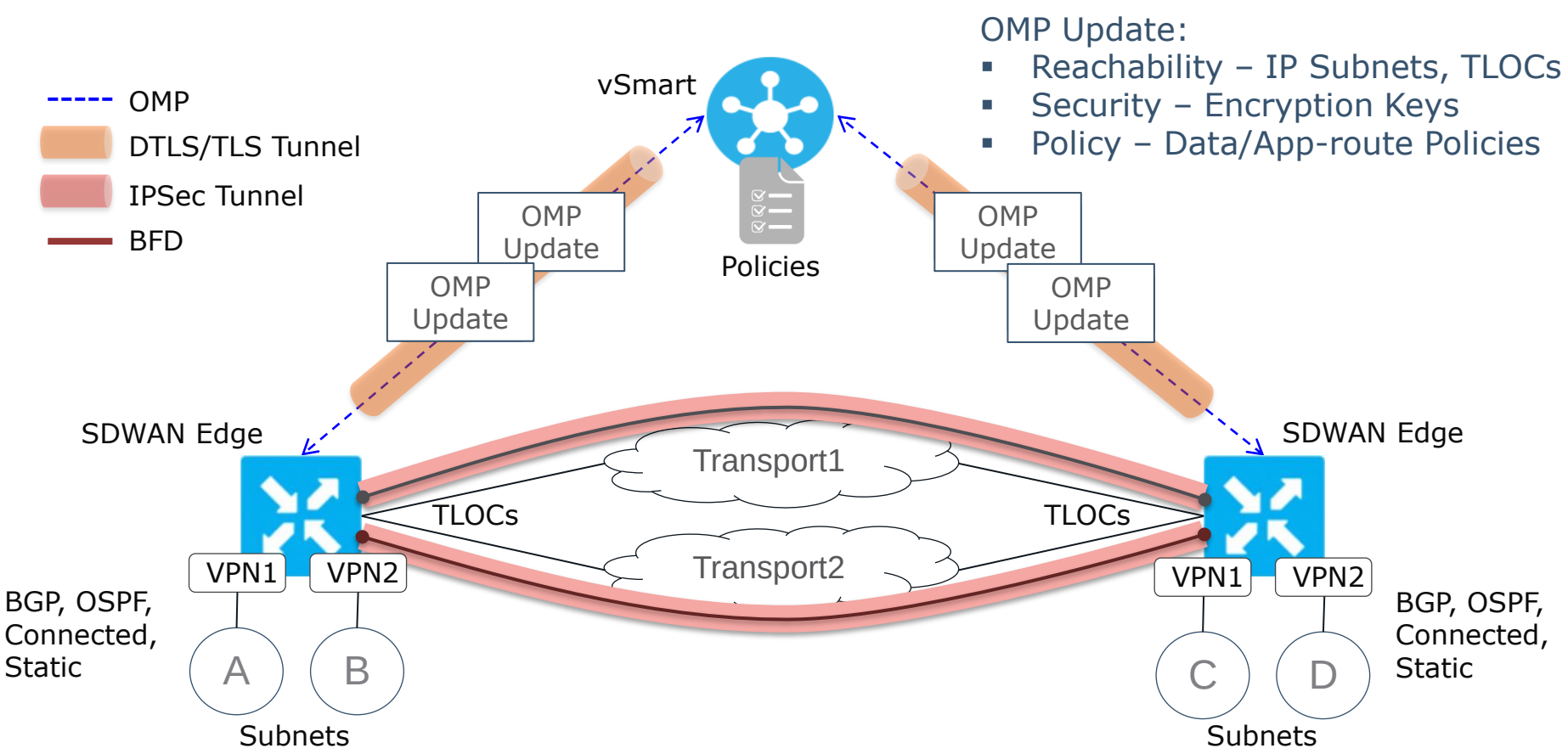
| Chassis Number | Serial No./Token | Hostname | System IP | Site ID |
|---|---|---|---|---|
| 4de0b85f-a2ae-42ec-8b45-3808285cd008 | 585A0084DEA8396DD... | RemoteSite1 | 1.1.1.1 | 101 |
| 5f05358a-bef7-4e15-9ade-8ffd8f27ec93 | 248792F938E6EA8BEE... | AWS | 1.1.1.5 | 105 |
| 9391da23-f0d1-4259-88d9-e10ae714708c | 0334D73E5EC036F87A... | DataCenter | 1.1.1.4 | 104 |
| 5db86b8b-8021-4afc-817c-eef48ae2e836 | 368EDA9249E64F2C5A... | RegionalHub | 1.1.1.3 | 103 |
| 6f8d368a-81c4-4b20-a420-404b827ca37e | 19EB7510F570D6BD23... | RemoteSite2 | 1.1.1.2 | 102 |

## Certificate Based Mutual Trust




- Bi-directional certificate-based trust between all elements
  - Public or Enterprise PKI
- White-list of valid WAN Edges and controllers
  - Certificate serial number as unique identification

# Cisco SD-WAN – Automated Data Plane Establishment



# SD-WAN use cases

# SD-WAN use cases

On demand & optimized cloud networking

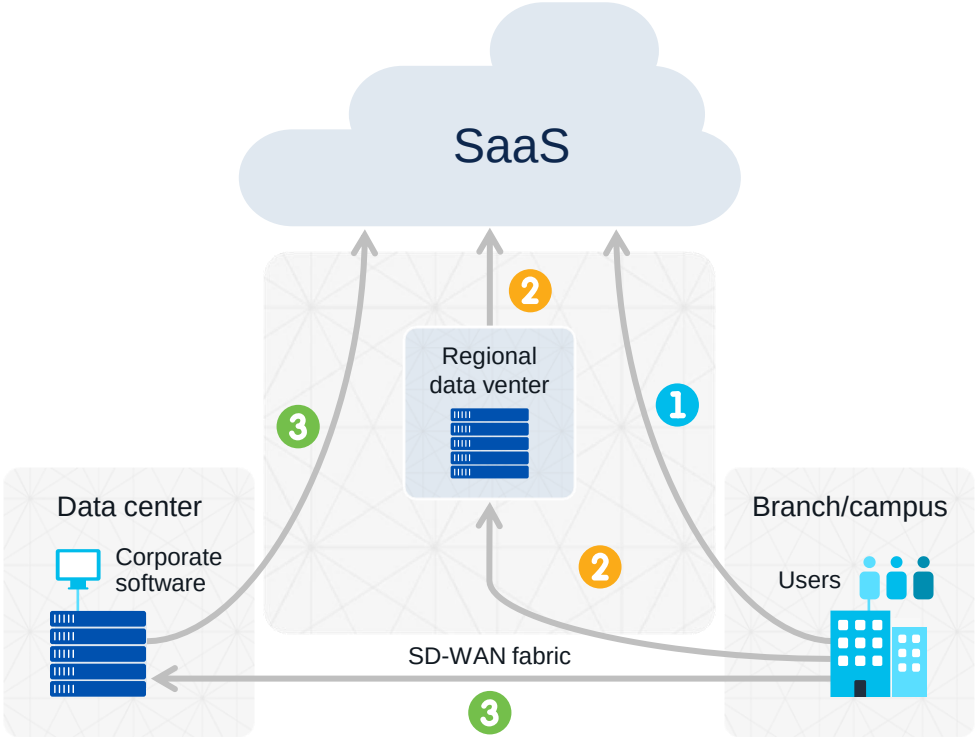
Optimized user application experience

Centralized configuration management and application visibility

Secure segmentation & Secure Branch

# SaaS optimization challenges

COR for SaaS




## Which path do I use for SaaS applications?

1 Direct internet access

2 Regional breakout

3 Data center backhaul

Best quality

Medium quality

Poor quality

Which path has better SLA for Microsoft 365?

How do I increase performance for each path?

Should all apps go to the DC first or can trusted apps like Microsoft 365 use DIA?

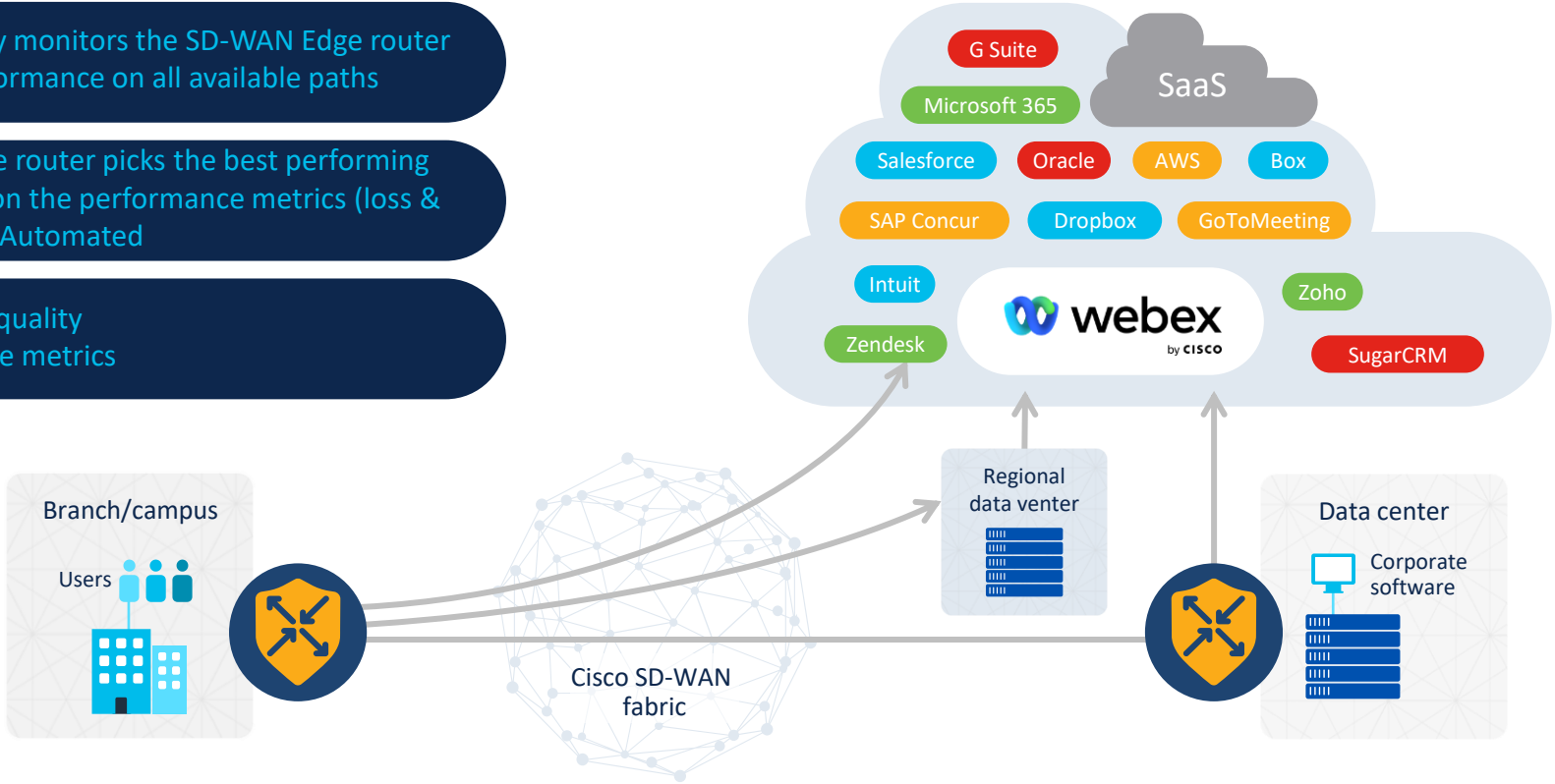
How do I automatically steer traffic to another path?

# Cisco SD-WAN Cloud OnRamp for SaaS

## Optimized connectivity to cloud applications

COR for SaaS

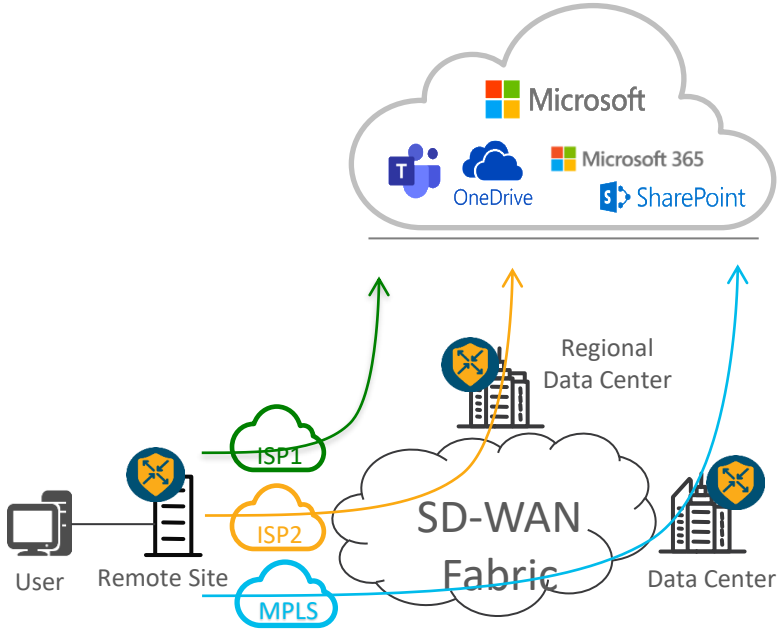
- Continuously monitors the SD-WAN Edge router to SaaS performance on all available paths
- SDWAN Edge router picks the best performing path based on the performance metrics (loss & delay), Fully Automated
- Visibility on quality of experience metrics



# Cloud OnRamp for Microsoft 365

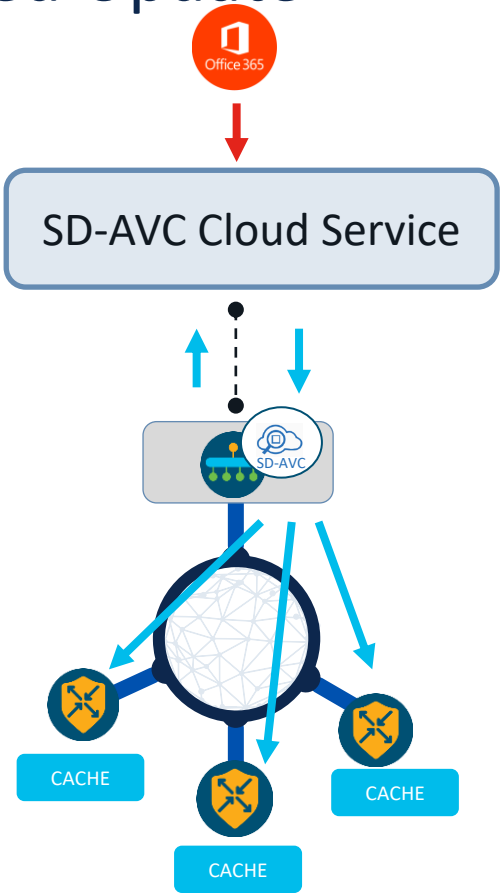
## Microsoft 365 Optimization Challenges

- How to optimize only certain Microsoft 365 Categories?
- How to gain Application telemetry view to gain insights into Application Performance?
- When specific path is having performance issues, How to automatically steer traffic?



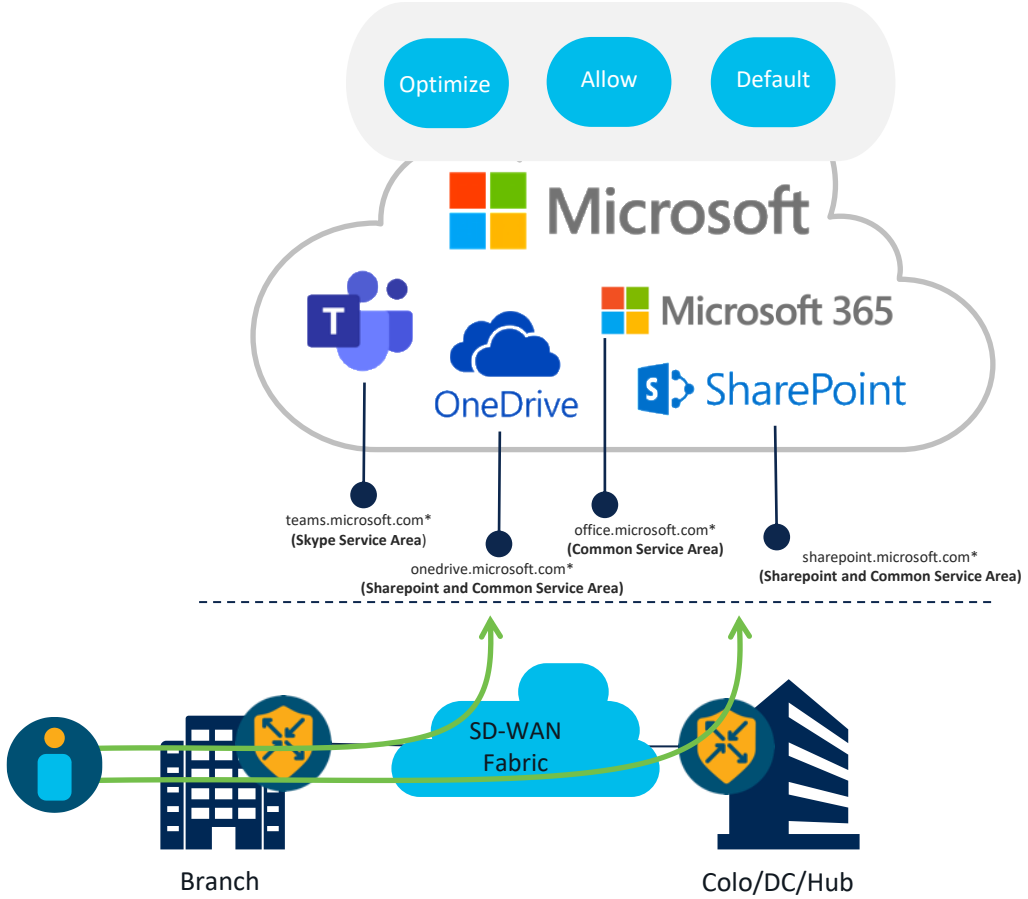
# Microsoft 365 Cloud Feed – Pre-Populated Update

- SD-AVC container runs on Cisco vManage
- SD-AVC Container pulls Microsoft 365 URL Categories using Microsoft 365 web service
- SD-AVC Container dynamically pre-populates Edge router's NBAR cache with Microsoft 365 IP addresses and URL Categories



# Microsoft 365 URL/IP Categories and Service Areas

- First Packet Classification using pre-populated NBAR cache
- Microsoft 365 divides applications into 3 categories based on sensitivity
- On SD-WAN routers, we classify Microsoft 365 traffic using URL categories i.e., Optimize, Allow and Default
- Enable Cloud OnRamp for specific Microsoft 365 categories like Optimize or Optimize and Allow or All Categories
- You can also enable CoR for SaaS for only specific Service Areas such as Exchange, SharePoint, Skype or Common

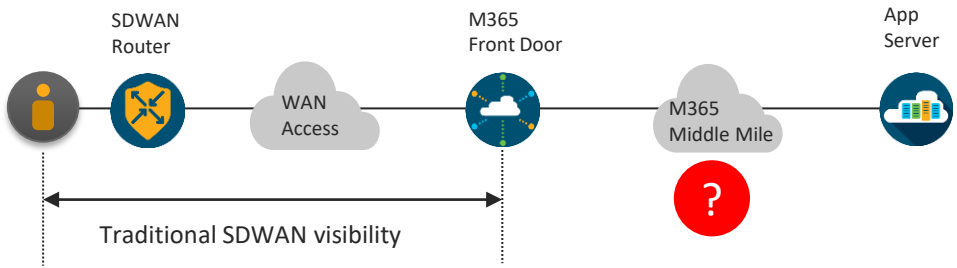


# Microsoft 365 Optimization

## Application Informed Network Routing

### Problem

- Traditional SD-WAN only probes the app front-end detect the best path for the appropriate SaaS app.
- Probe measurement only covers part of the network part.
- It does not take service performance into account



# Microsoft 365 Optimization

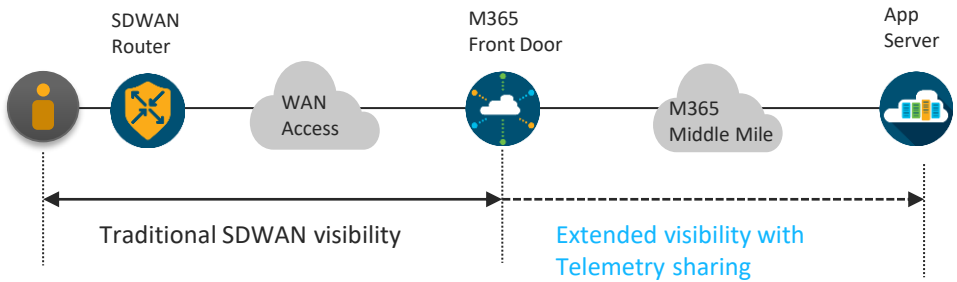
## Application Informed Network Routing

### Problem

- Traditional SD-WAN only probes the app front-end detect the best path for the appropriate SaaS app.
- Probe measurement only covers part of the network part.
- It does not take service performance into account

### Solution

- Cisco Cloud onRamp for SaaS probing is augmented by M365 SaaS telemetry.
- Microsoft monitors performance of App service and computes a score



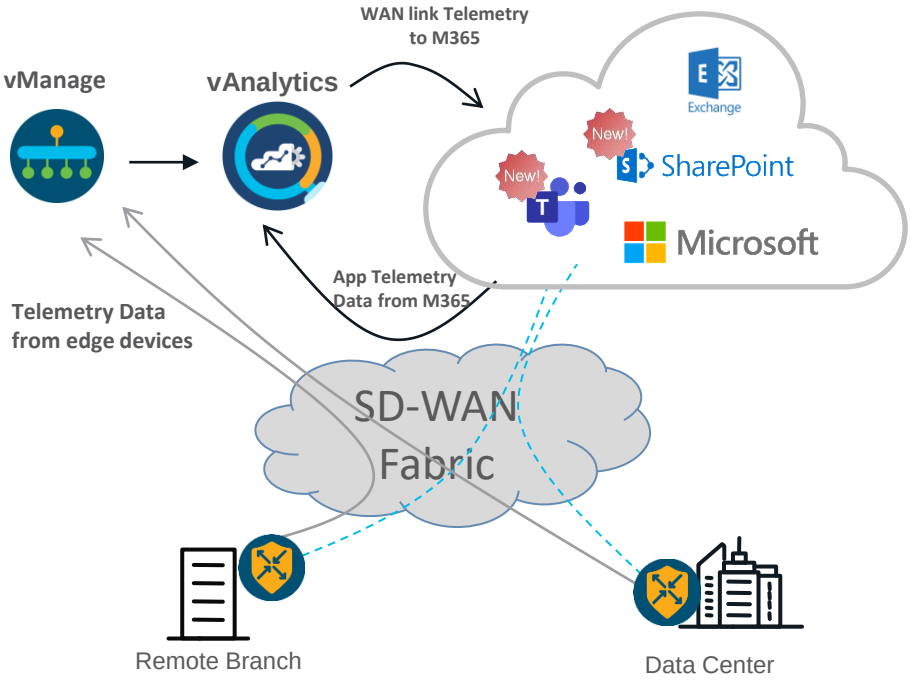
# Microsoft 365 Optimization with Cisco SD-WAN

## Application Informed Network Routing

- Developed in Partnership with Microsoft

  Cisco SD-WAN Solution is Microsoft Networking Partner Program Certified

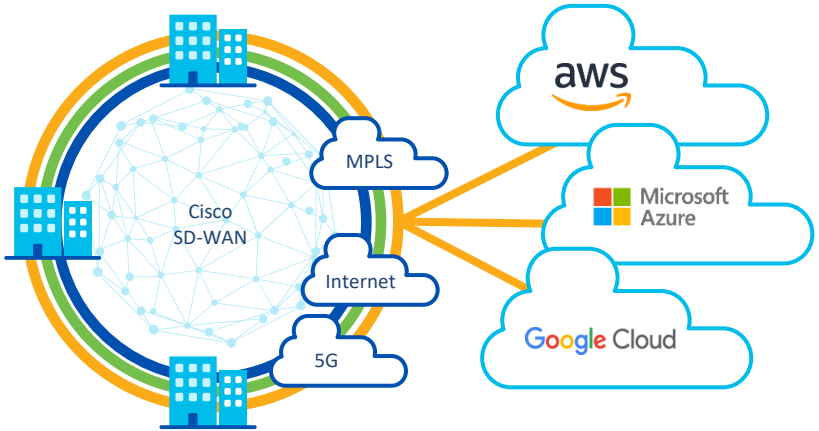
- vAnalytics receives Exchange, Teams and SharePoint telemetry data from Microsoft
- vAnalytics sends Network telemetry data to Microsoft 365
- Application and Network Telemetry provides application performance insights
- vAnalytics uses Network and App telemetry data to compute best path
- SD-WAN router selects best path based on results received from vAnalytics



# Cisco SD-WAN Cloud OnRamp for Multicloud

## Automate SD-WAN extension to IaaS via vManage

**Cisco is the only market player to partner with top 3 cloud providers for end-to-end solution**




**Greater automation**
Automate SD-WAN extension to the cloud with just a few clicks

**Normalized multicloud experience**
Consistent UI and workflow in vManage

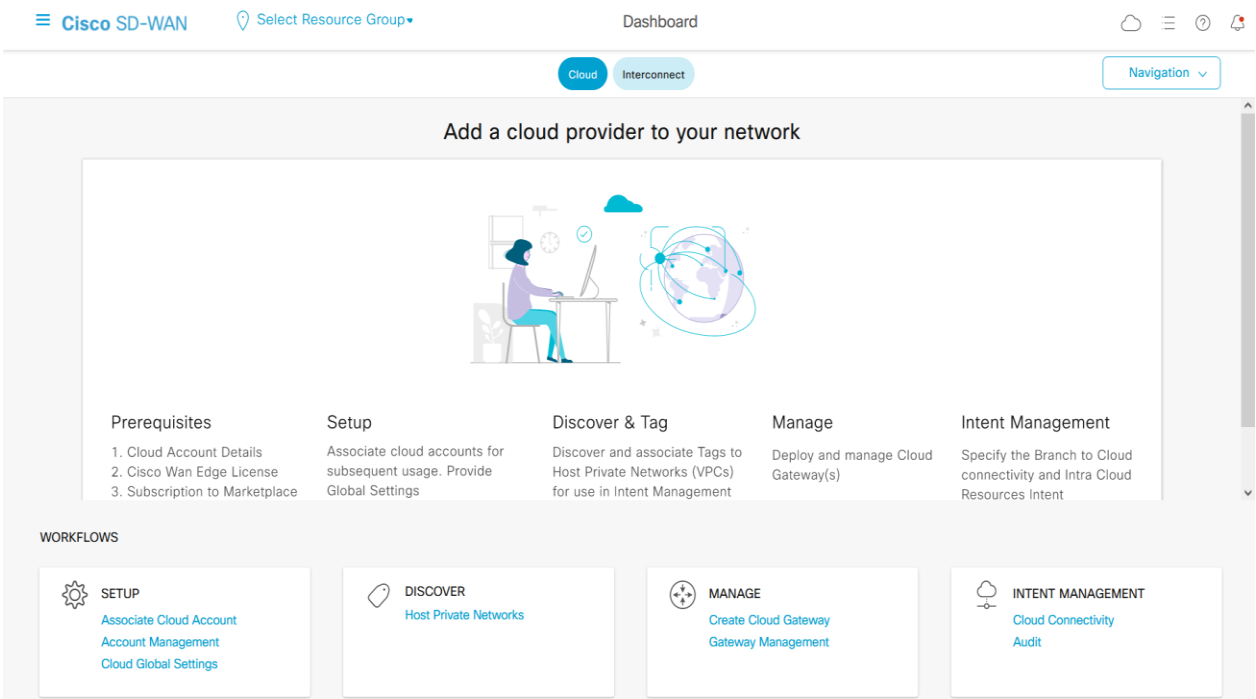
**Unified security policies**
Extend consistent enterprise segmentation policy into the cloud

**Ease of management**
Orchestrate Cisco and cloud provider networking resources via vManage

# Cloud OnRamp Automation on vManage

## Same configuration workflow for all 3 CSP (AWS, Azure, Google Cloud)

1. Enter Cloud Credentials
2. Create Cisco Cloud GW
3. Discover host VPCs/VNets
4. Map Branch nets to VPCs



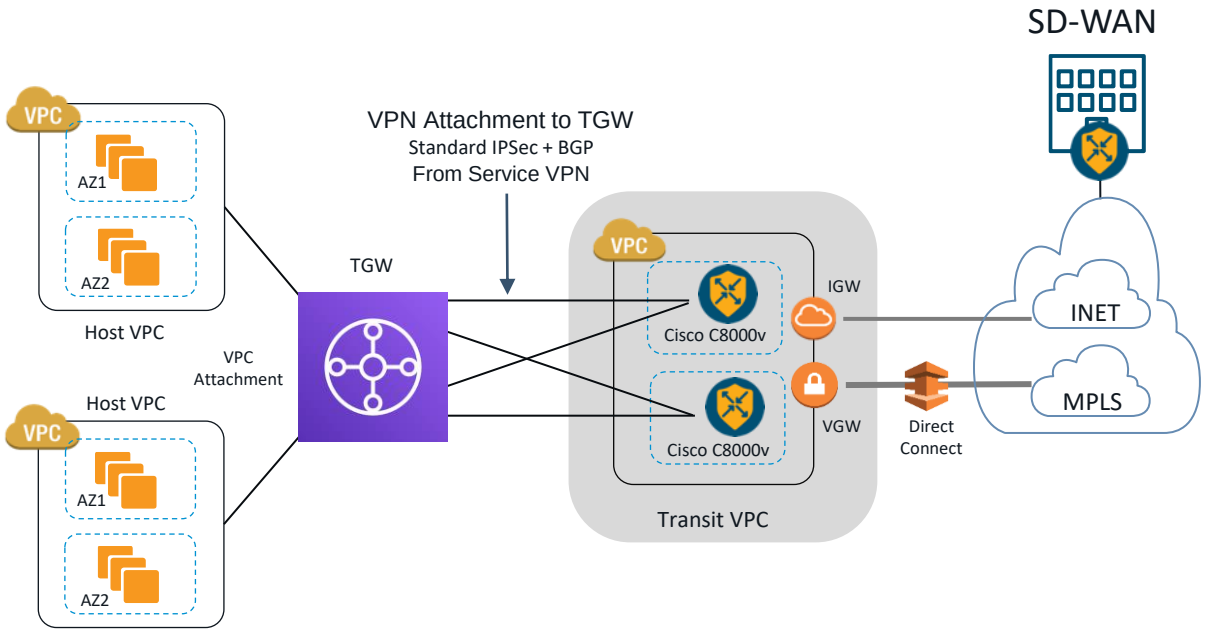
# Cloud OnRamp for Multicloud Automation: How it works

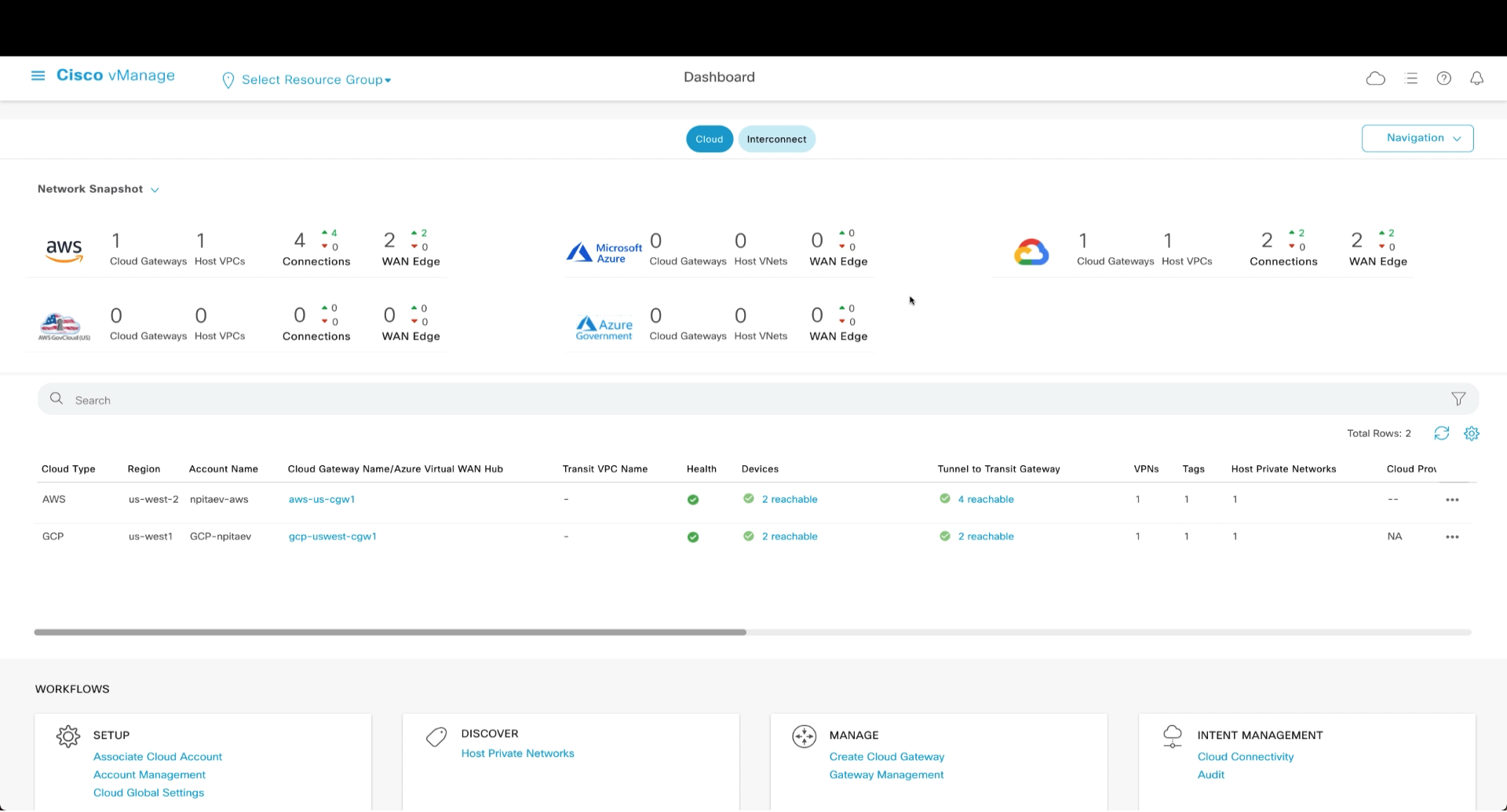
**vManage will do the following:**

1. Bring up Transit VPC with two CSR running SD-WAN image
2. Create TGW
3. Connect TGW and CSR
4. Connect host VPCs

**Single UI vManage Workflow:**

1. have two C8000v ready
2. define AWS Account
3. discover host VPCs
4. tag host VPCs as needed
5. enter TGW details
6. deploy and verify





# SD-WAN use cases

On demand & optimized cloud networking

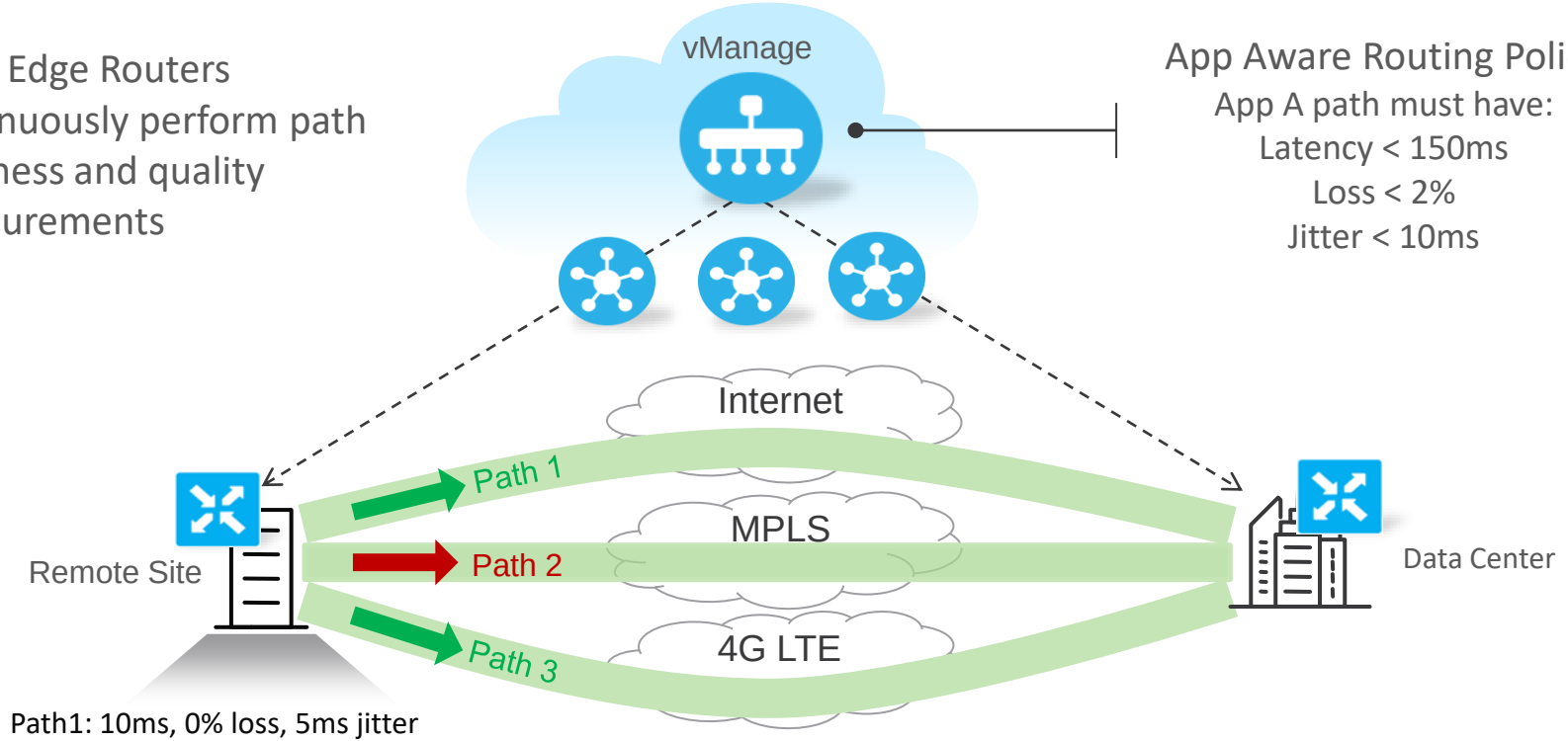
Optimized user application experience

Centralized configuration management and application visibility

Secure segmentation & Secure Branch

# Cisco SD-WAN: Improving Application Experience

- WAN Edge Routers continuously perform path liveliness and quality measurements



# SD-WAN use cases

On demand & optimized cloud networking

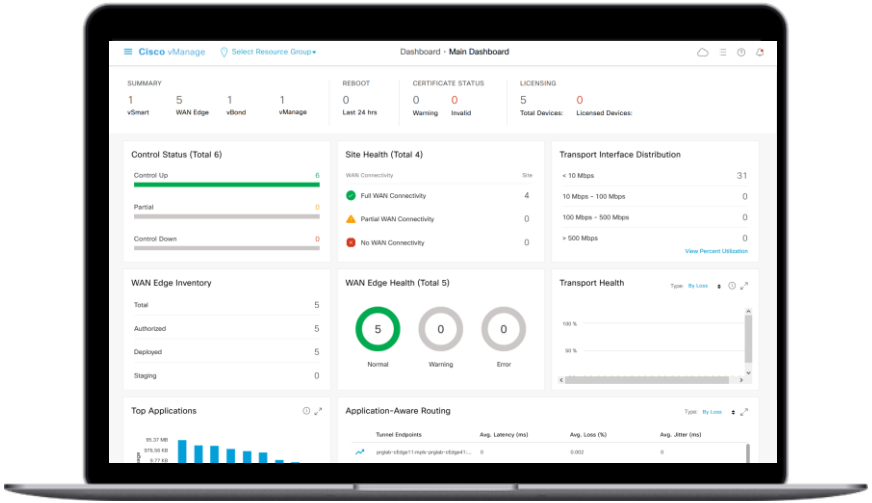
Optimized user application experience

Centralized configuration management and application visibility

Secure segmentation & Secure Branch

# Cisco SD-WAN Controller for simplified management

Cisco vManage

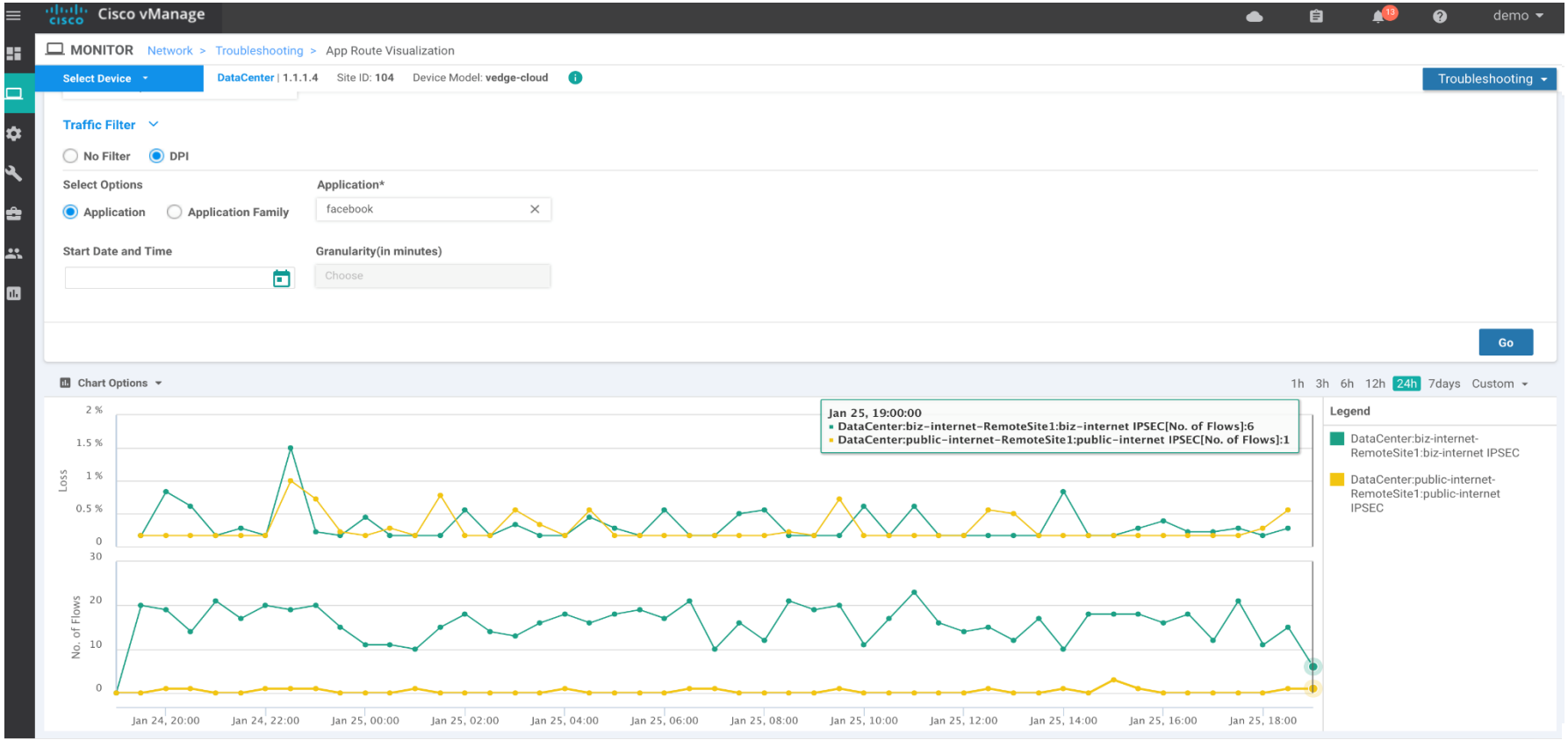



Single Monitoring Dashboard

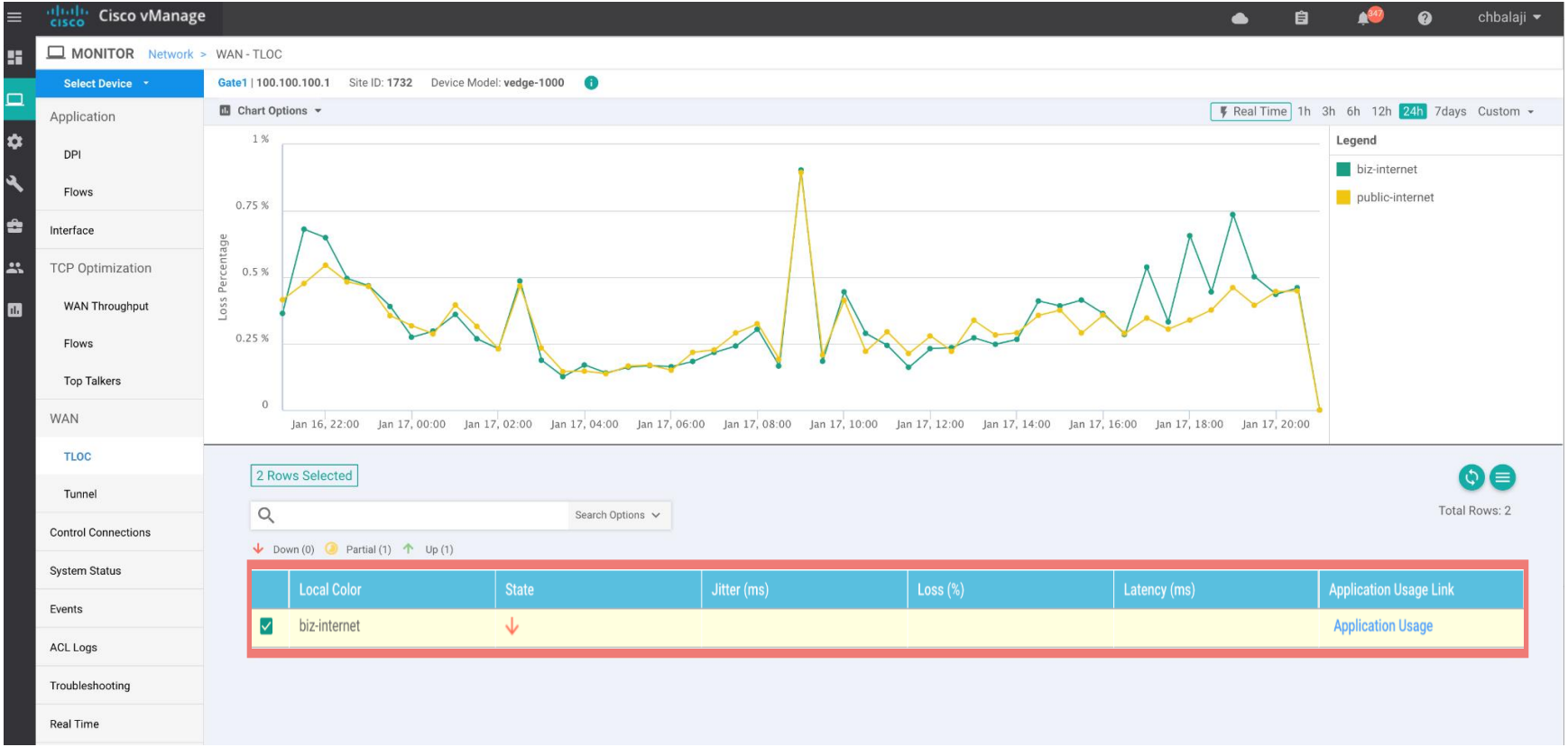
| Configuration: OnRamp, Security, Devices, Policies, Templates | Lifecycle Management | Role based access/ Multi-tenant |
|---|---|---|

One management dashboard for branch, co-location, cloud and Security

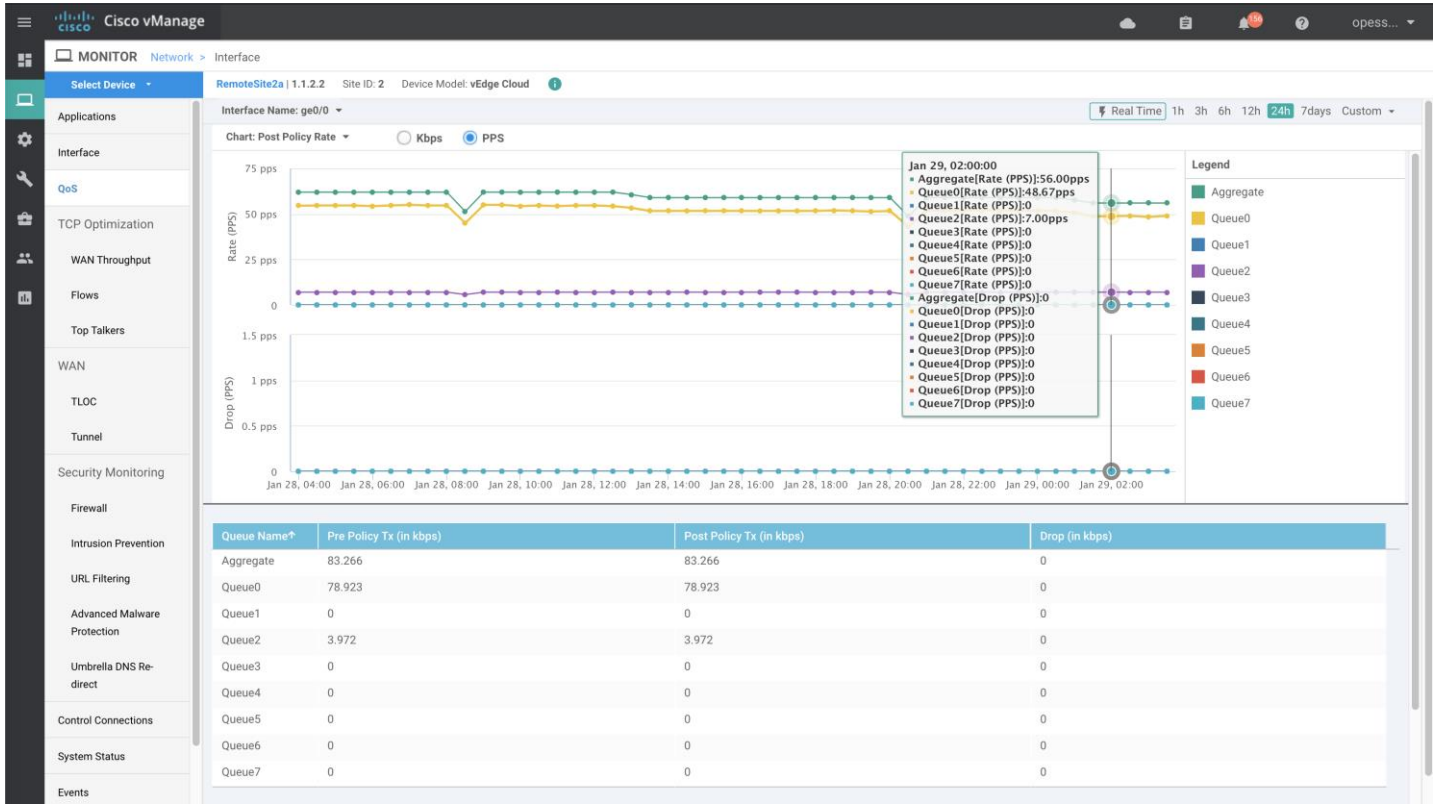
# Visualizing Application Paths



# Checking Transport Quality



# Checking QoS



# SD-WAN use cases

On demand & optimized cloud networking

Optimized user application experience

Centralized configuration management and application visibility

Secure segmentation & Secure Branch

# Cisco SD-WAN - Segmentation

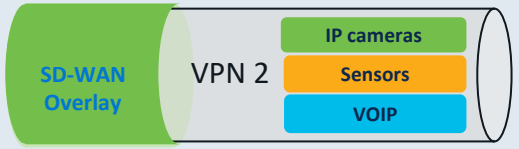
## Granular Segmentation Policy

### Macro Segmentation


VPN Level Segmentation

- Campus VPN
- IOT VPN
- Guest VPN

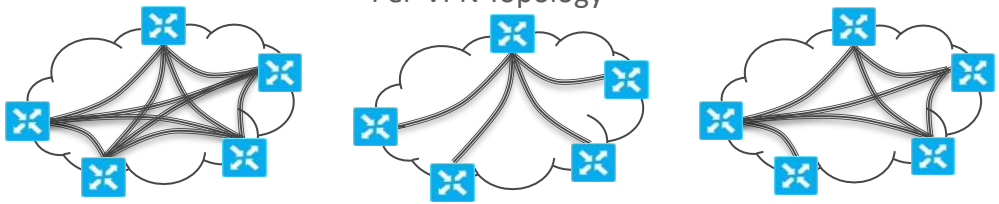
### Micro Segmentation




Identity based Group Level Segmentation - IOT VPN

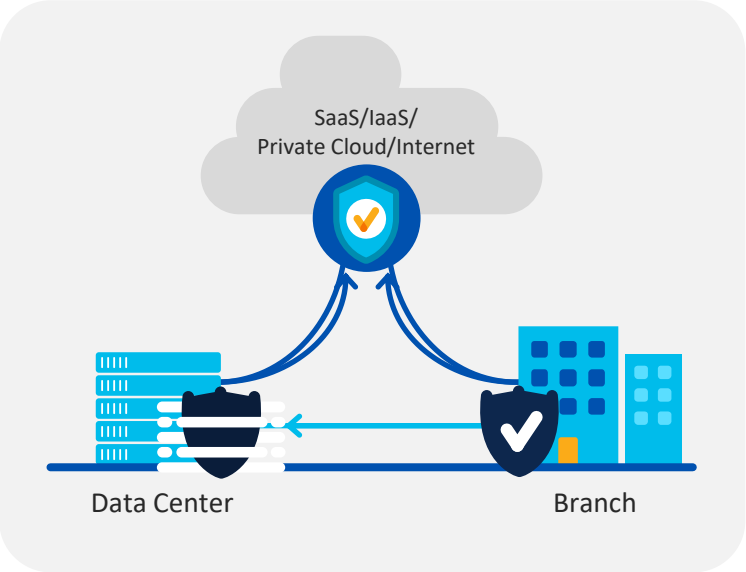
- IP cameras
- Sensors

Per-VPN Topology



Full-Mesh | Hub-and-Spoke | Partial Mesh

# Why Direct Internet Access (DIA)?




1. Avoid Backhauling

Benefit: Better use of WAN bandwidth

2. Benefit Regional SaaS PoP

Benefit: Improves application performance

3. Enable DIA

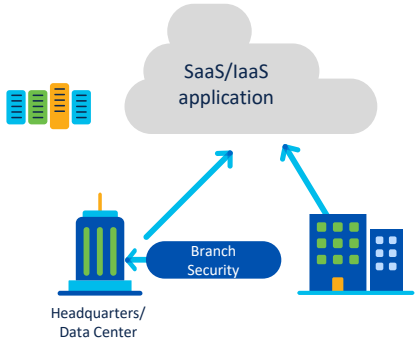
Benefit: Improves user experience

4. Centralized Policy/Monitoring

Benefit: Consistent Security Policy & monitoring

# Cisco SD-WAN Security Stack
## Flexible Deployment Model

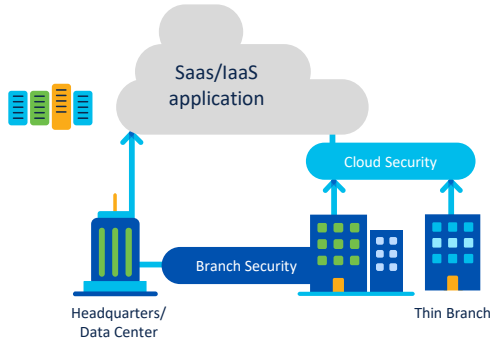
SD-WAN w/ On-Prem Security




Integrated Security

SD-branch model
Thick branch with routing and security

SD-WAN w/ SIG Integration
and Hybrid Security

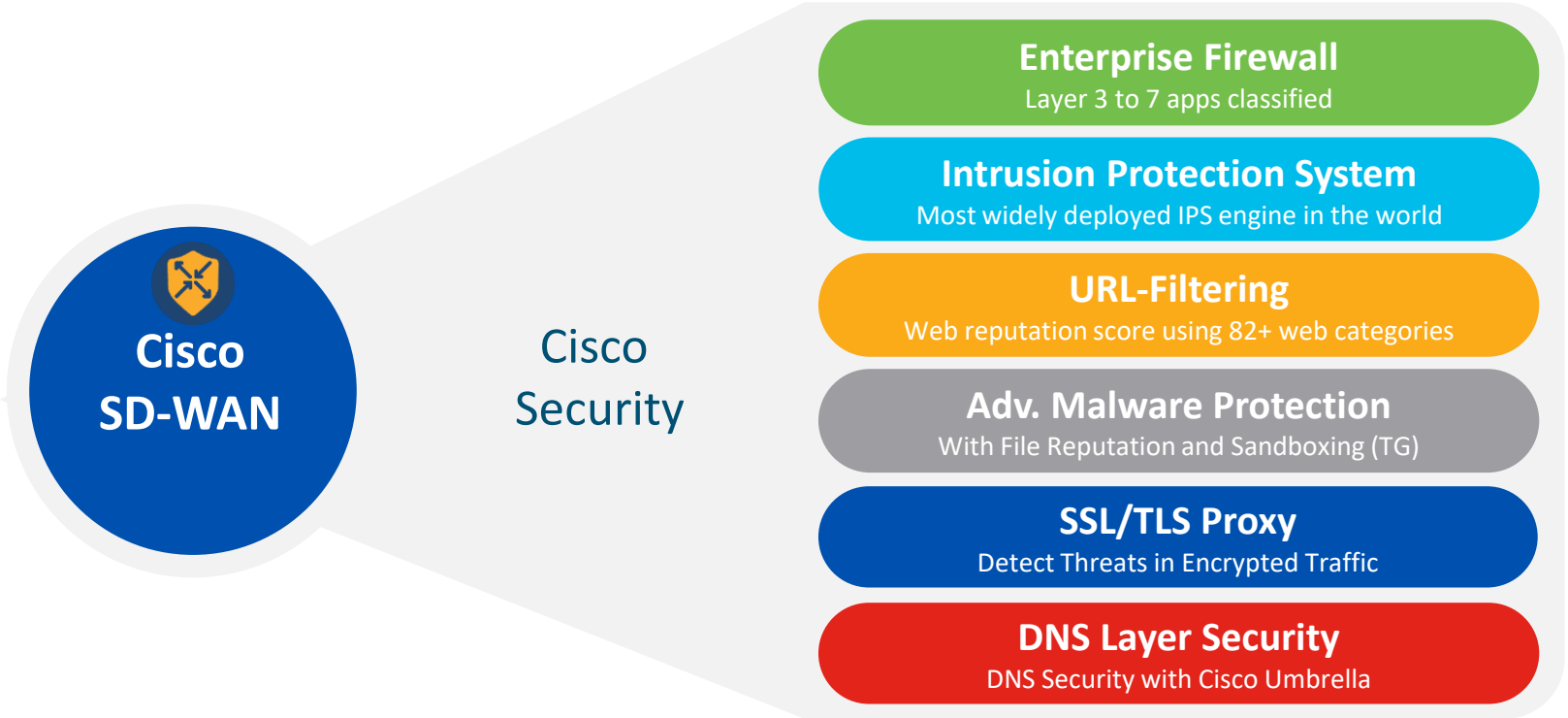



SD-WAN with SIG integration

Hybrid model
Thin branch with cloud security
Thick branch with routing and security

# Cisco SD-WAN Security Solution

## On-prem security capabilities



# Cisco Umbrella SIG security capabilities

Cisco Umbrella

| DNS-layer security | Secure web GW<br>Incl: RBI, File Control, App Control | Cloud-delivered Layer 7 firewall | Cloud access security broker<br>(CASB) | Interactive threat intel |
|---|---|---|---|---|
| Stop threats before traffic reaches my network | Full URL visibility/ control to enforce policy block advance threats | L7 security across all sites to stop non-web-based threats | Discover, report and control cloud application use. | Real-time threat context expediting incident investigation and response |

SecureX

Integrated security platform

Visibility across my entire security stack, with automated actions

# Cisco SD-WAN Innovations

# Cisco SD-WAN QOS features

## Per-Tunnel QOS

Allocates the Bandwidth on per tunnel basis

## Adaptive QOS

Allocates the Bandwidth as per availability

## Per-VPN QOS

Allocates the bandwidth on per VPN basis

# Cisco SD-WAN - Segmentation

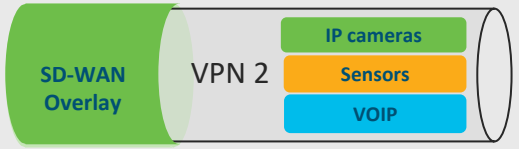
## Granular Segmentation Policy

### Macro Segmentation


VPN Level Segmentation

- Campus VPN
- IOT VPN
- Guest VPN

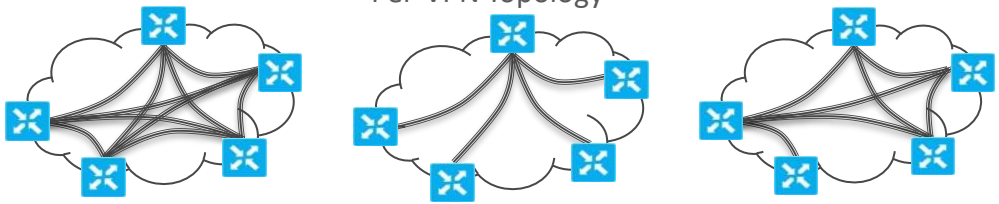
### Micro Segmentation




Identity based Group Level Segmentation - IOT VPN

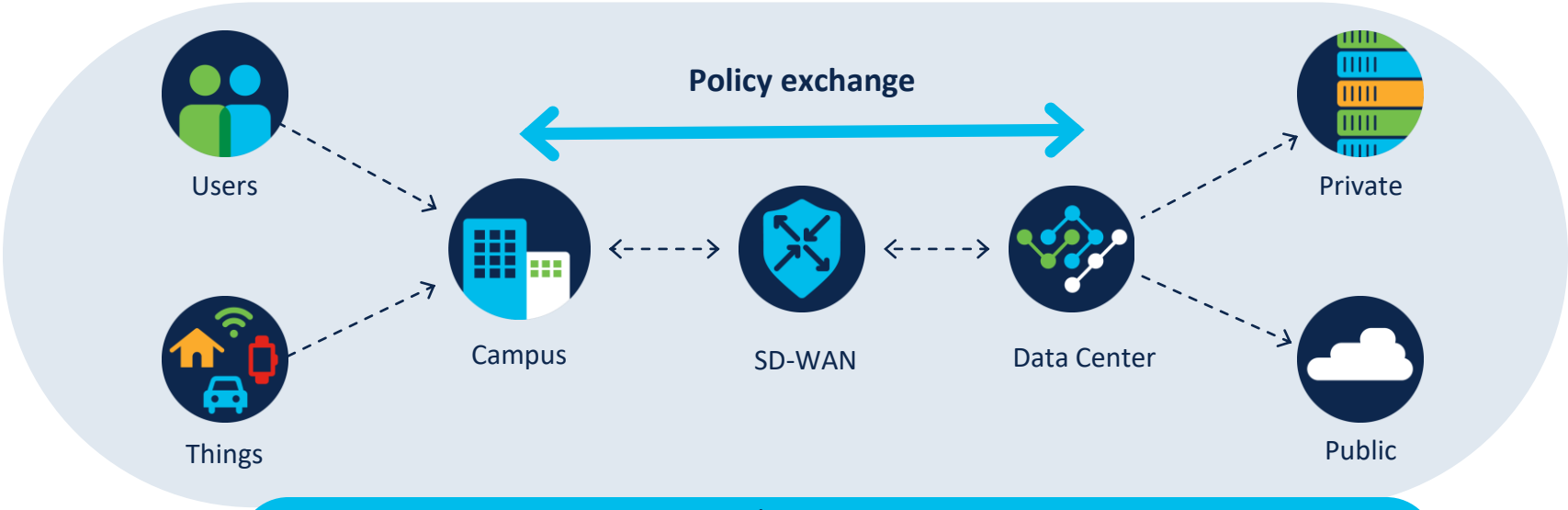
- IP cameras
- Sensors

Per-VPN Topology



Full-Mesh | Hub-and-Spoke | Partial Mesh

# Cisco SD-WAN extends segmentation and policies across the enterprise's networking domains



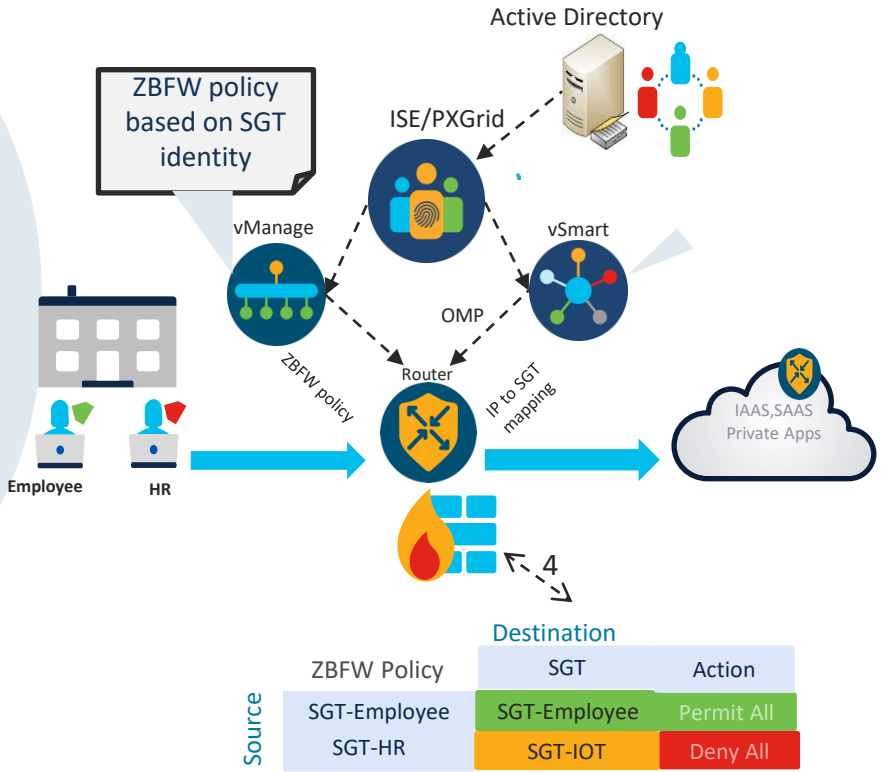

Cisco SD-WAN supports user/device identity SGT tags to be propagated via SD-WAN overlay, enabling end to end policy propagation.

# Cisco SD-WAN - Identity-based Firewall ISE-SGT integrations

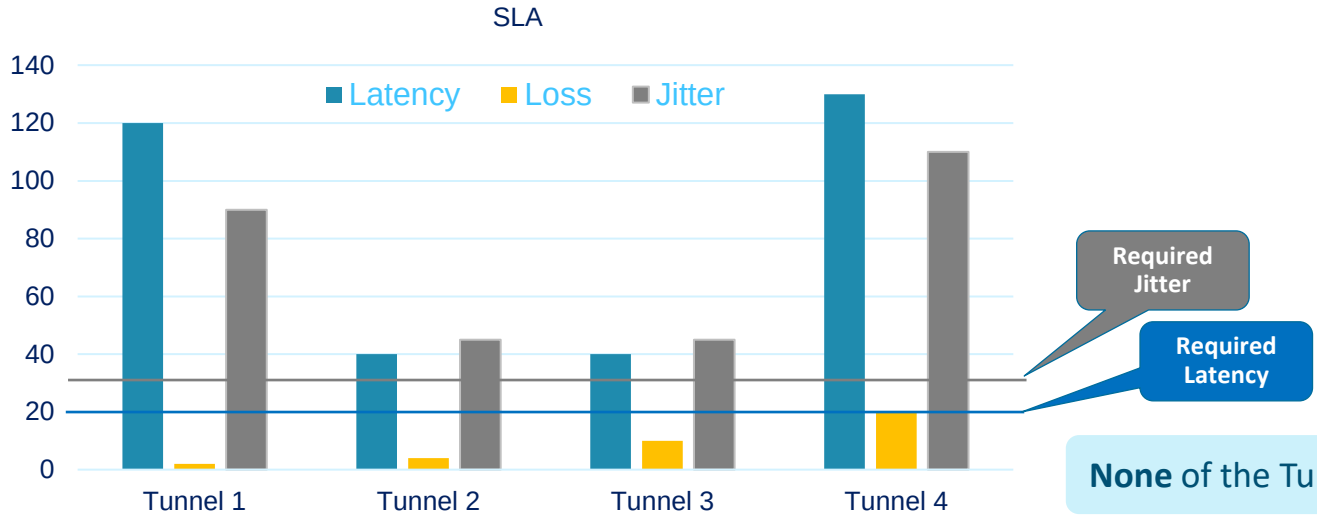
Security policies that align to identities rather than to IP addresses give organizations easier, more precise control over who can access the network/applications—and what they can access.

In a hybrid workforce environment, the users can access application from anywhere and from any IP, therefore applying security policy based on prefixes is not enough.

Cisco SD-WAN introduces capability for a WAN edge to match user/user-group identities and apply zone-based firewall policy based on it



# Application Aware Routing- Best of worst Tunnel Selection




```
policy
 sla-class Voice
   latency 20
   jitter  30
```

**None** of the Tunnel Meets SLA criteria

Traffic gets **routed as per ECMP**

This results in an **un-deterministic and inconsistent** user experience for same kind of application.

This would atleast provide a better user experience comparatively than the worst.


Therefore, best of worst tunnel is used

# Extended visibility with Cisco SD-WAN + ThousandEyes

## Cisco SD-WAN

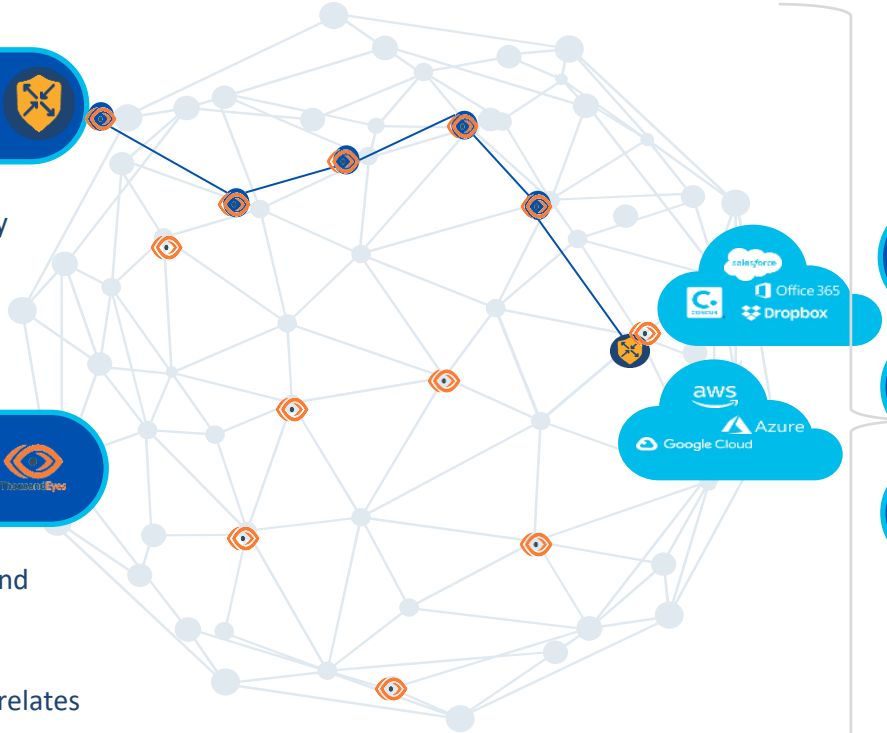
Measures point-to-point network telemetry

Enables automated routing based on network performance and availability

## Cisco ThousandEyes

Measures hop-by-hop network telemetry and path (SD-WAN underlay + end to end)

Measures application performance and correlates with network insight




**Cisco SD-WAN + ThousandEyes native integration**

- Turn-key agent deployment
- Rapid MTTI/MTTR
- Actionable insights

# Conclusion

# Cisco SD-WAN Benefits and Differentiation

## Cisco SD-WAN

**True SD-WAN Architecture flexibility:**

- Separate and dedicated components for the control plane, data plane, management and orchestration of the WAN designed for scalability and flexibility to implement overlay, underlay, physical, and virtual networks

**Hierarchical SD-WAN fabric capability**:

- These capabilities provides additional enhancement on scale and usability

**Proven deployments to over 10,000+ sites**


Cisco SD-WAN portfolio has achieved MEF SD-WAN 3.0 Certification.

## Multicloud

### Connect

**Extensive Cloud OnRamp integrations:**

- Enables seamless automated connectivity with any site-to-cloud and site-to-site configuration.

**Industry Firsts**

- Offer cloud onramp to the top three cloud service providers and first to deliver integrations for Microsoft Virtual Hub NVA, and Microsoft 365 informed network routing.

## Security

### Secure

**Micro-segmentation and identity-based policy management:**

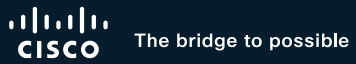
- Cisco TrustSec® provides micro-segmentation and identity-based policy management for SDA and non-SDA branches
- Drives consistent multidomain policy enforcement.

## Analytics

### Automate

**Enhance visibility into network behavior and user experience with applications deployed on-prem or in cloud**:

- Extends end-to-end visibility into network health and application performance
- Full hop-by-hop analysis across the internet and cloud.
- Expedite troubleshooting & reduce OpEx by offering actionable insights to help isolate problem areas




# Thank you