Cisco SD-WAN a typické příklady nasazení SD-WAN v prostředí podnikové sítě
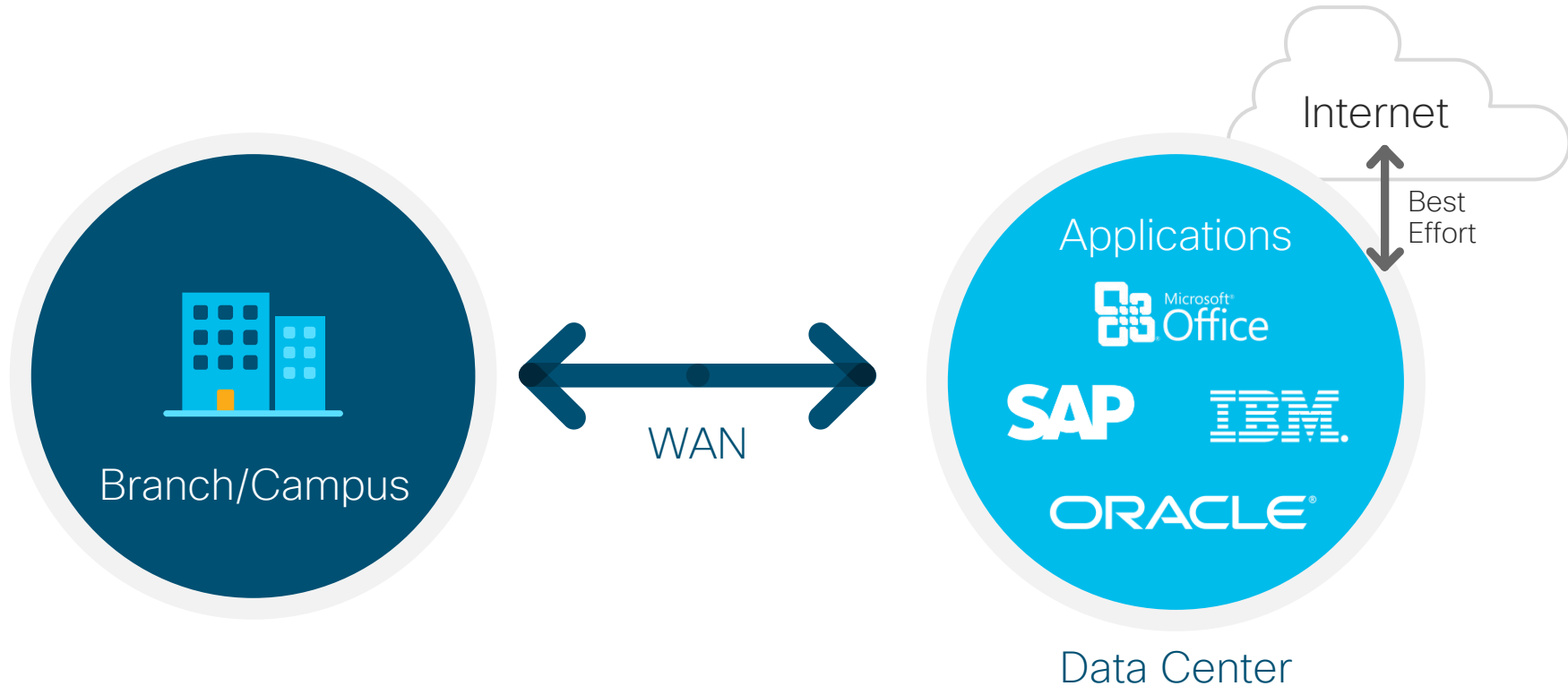
Miroslav Brzek
Technical Solutions Architect
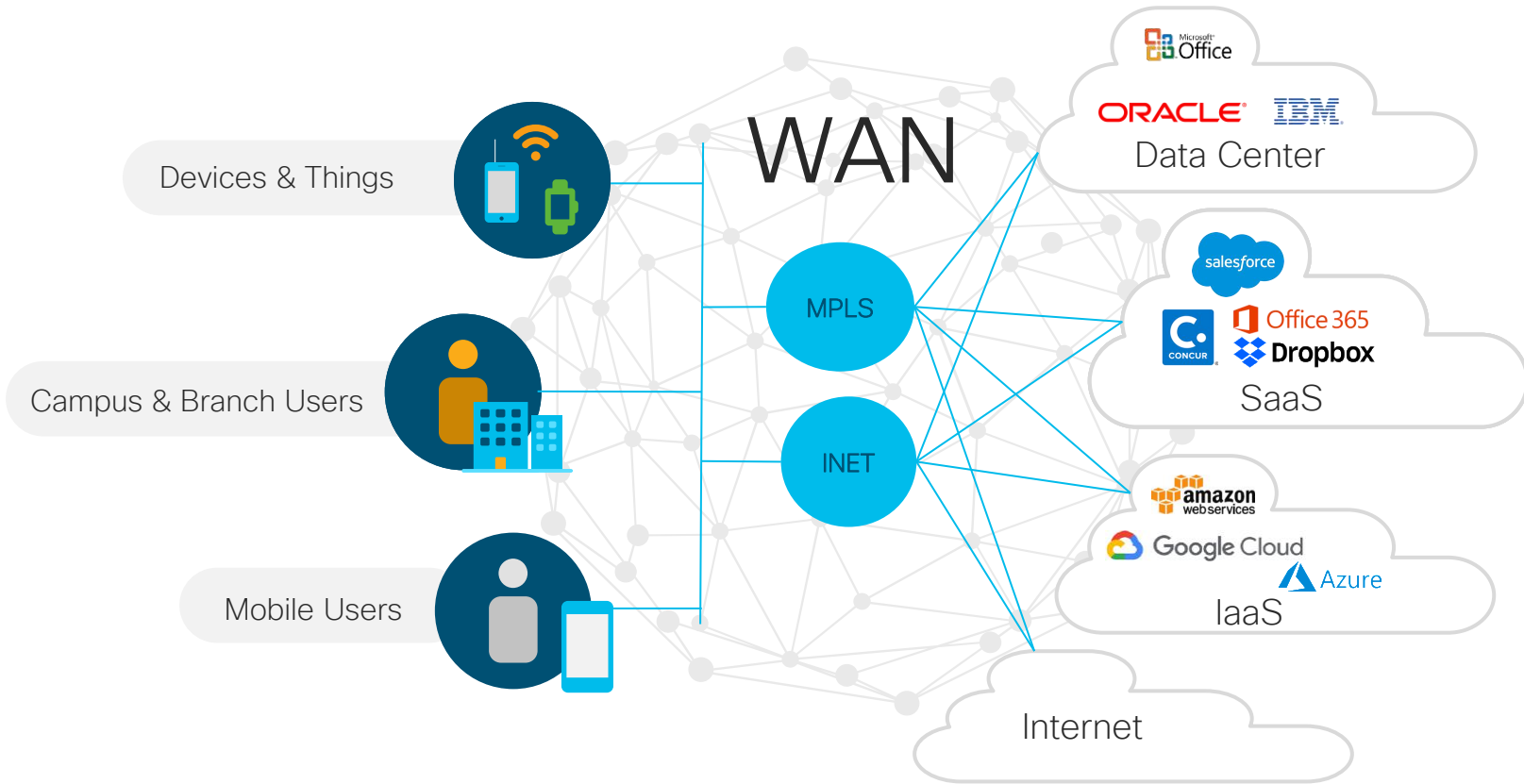
Agenda

1 Why SD-WAN

2 Cisco SD-WAN solution overview

3 Cisco SD-WAN and Application Experience

4 Cisco SD-WAN and Cloud Applications Optimization

5 Cisco SD-WAN and Secure Branch

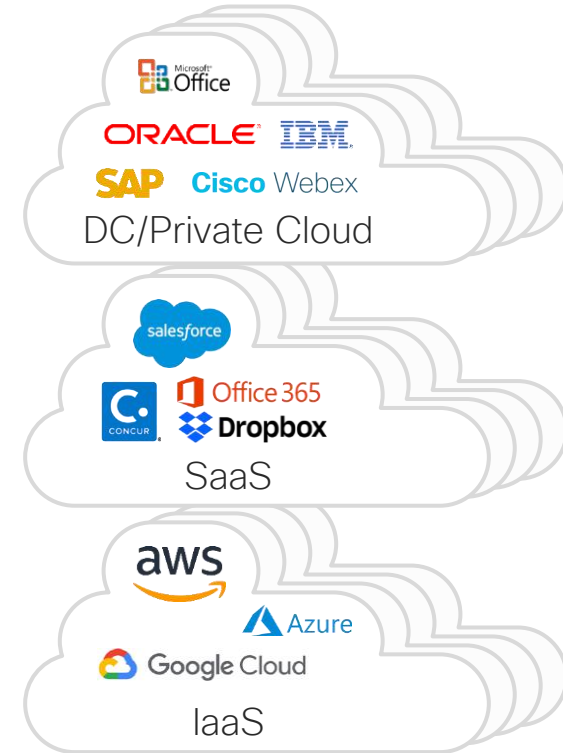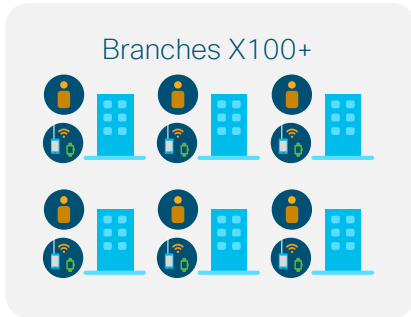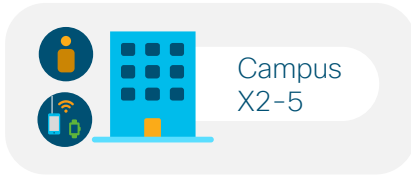**6** Cisco SD-WAN and Simplified Management

7 Conclusion

Connecting Users to Data Center was the Priority

Internet

Best Effort

Applications

Branch/Campus

WAN

Data Center

Today, things have changed completely

Internet Connectivity Becomes Business Critical

Campus X2-5

Branches X100+

Mobile Users X1000s

Exposure to cyber threats

Inconsistent user experience

Increasing complexity

Microsoft Office
ORACLE
IBM
SAP
Cisco Webex
DC/Private Cloud

salesforce
CONCUR
Office 365
Dropbox
SaaS

aws
Azure
Google Cloud
IaaS

More users, things and applications, everywhere

Cisco SD-WAN
Flexible yet simple at Cloud-scale

Management & Analytics

On-premise | Cloud | Multi-tenant

Automation | Network Insights | Machine Learning | AI

Open | Programmable | Scalable

Any Deployment

Any Service

Branch Security

Cloud Security

Application Quality of Experience

Voice and Collaboration

Optimization for SaaS/IaaS

Any Transport

Satellite

Internet

MPLS

5G/LTE

Any Location

Branch

Colocation

Cloud
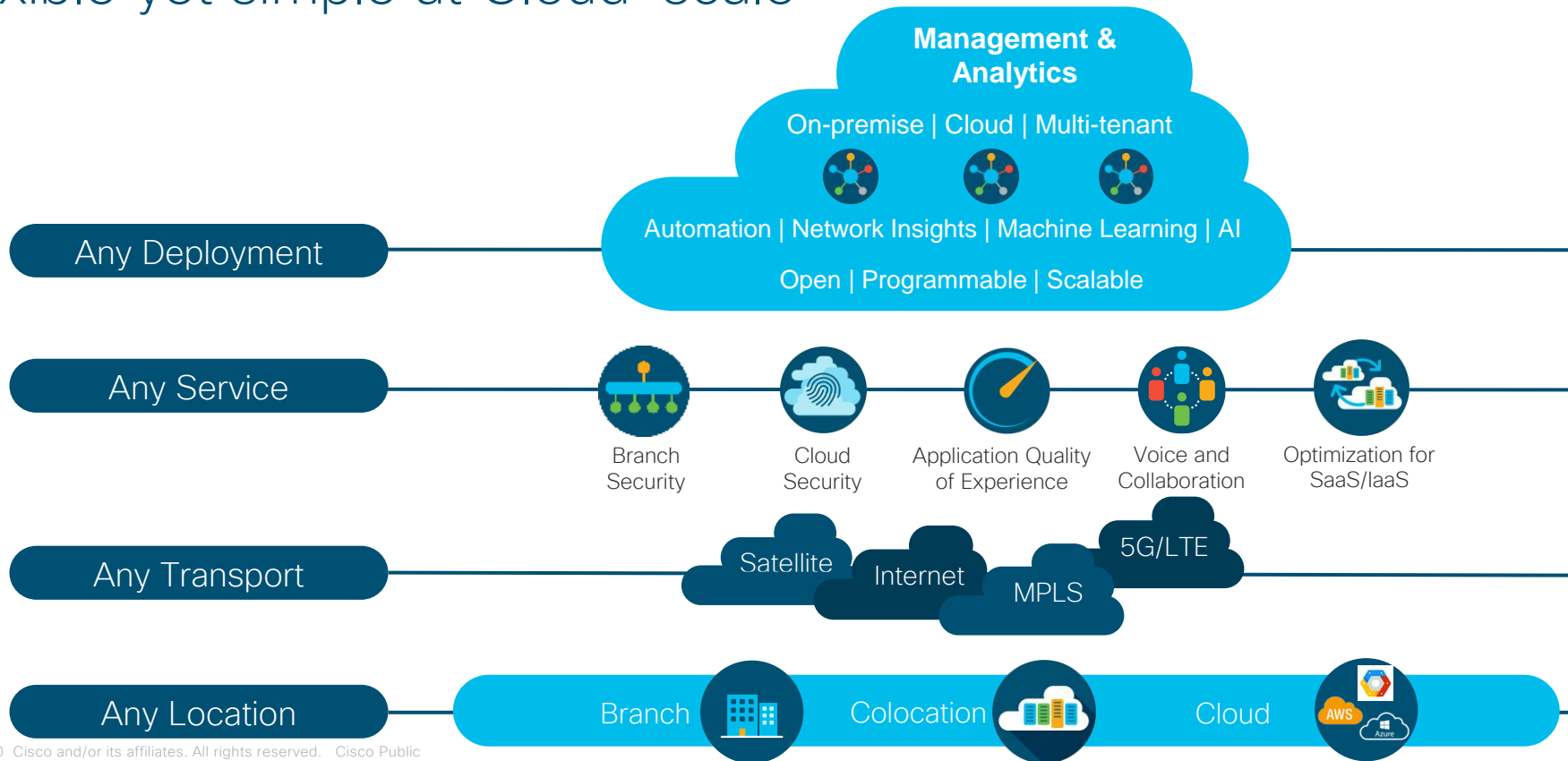
Cisco SD-WAN solution overview
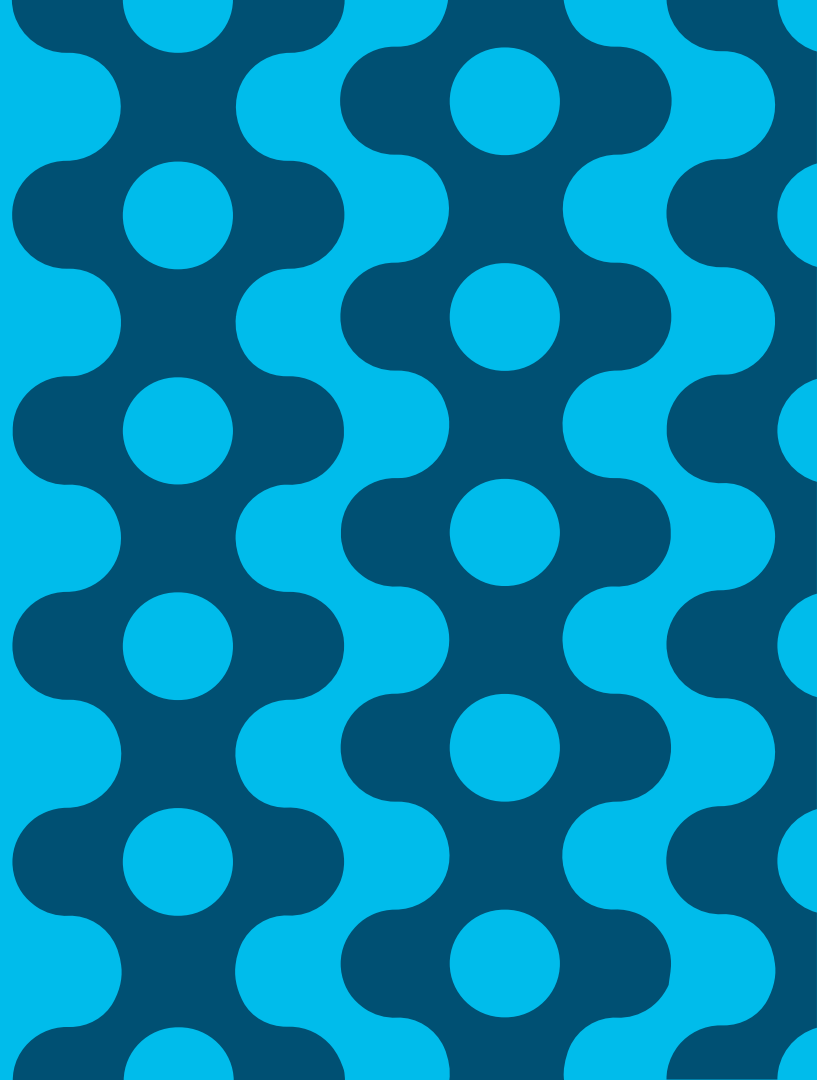
Cisco SD-WAN Architecture

Orchestration Plane

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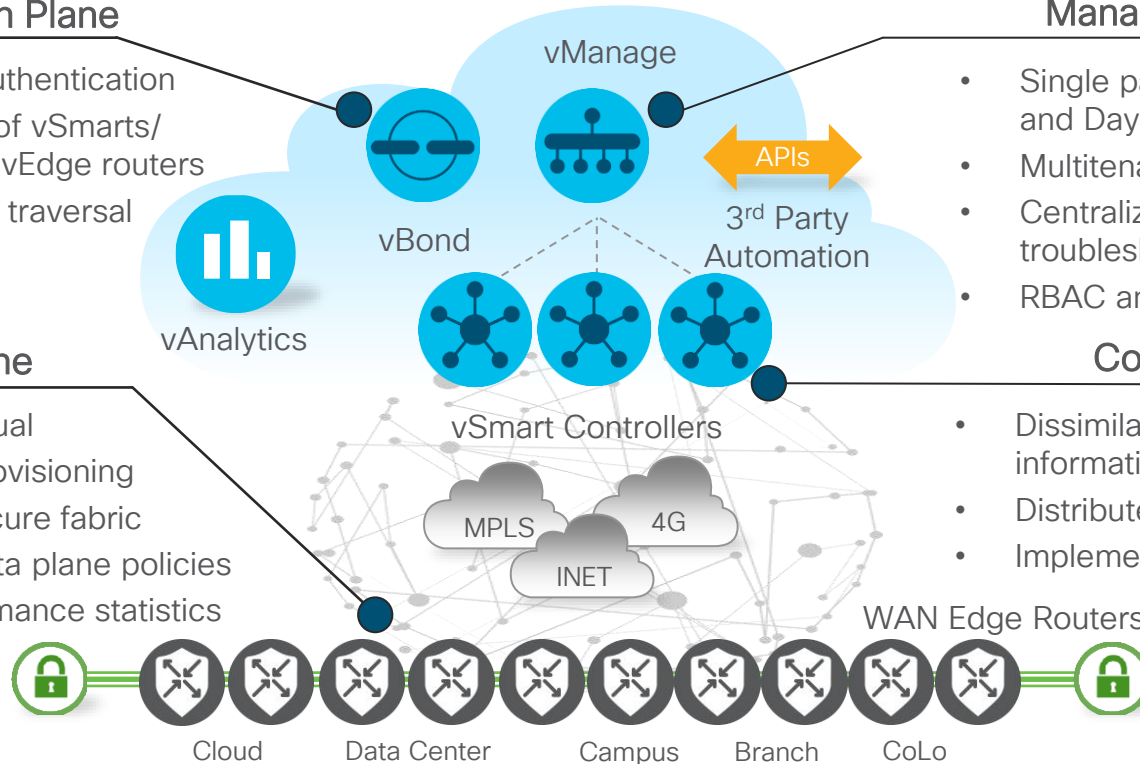- Facilitates NAT traversal

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
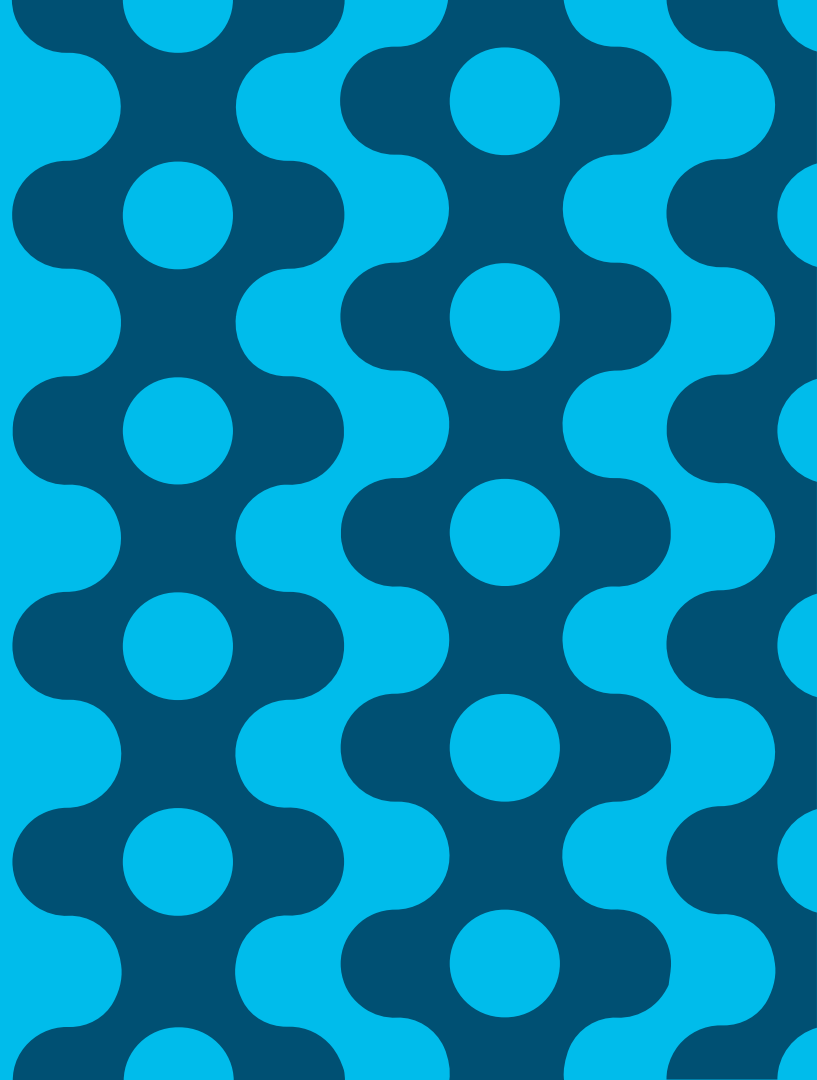- Exports performance statistics

Control Plane

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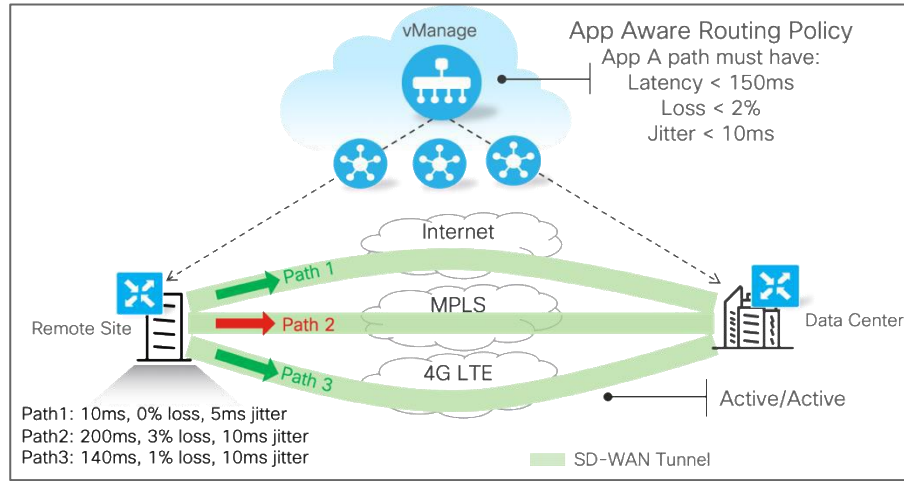- Implements control plane policies

vManage

vBond

vAnalytics

APIs

3rd Party Automation

vSmart Controllers

MPLS

4G

INET

WAN Edge Routers

Cloud   Data Center   Campus   Branch   CoLo

Cisco SD-WAN and Application Experience

Cisco SD-WAN – Improving Application Experience

Application Aware Routing

App Aware Routing Policy
App A path must have:
Latency < 150ms
Loss < 2%
Jitter < 10ms

Path1: 10ms, 0% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

SD-WAN Tunnel

Forward Error Correction (FEC)

- Protects against packet loss
- Protocol (TCP/UDP) agnostic
- Supports multiple transports
- Applied with data policy
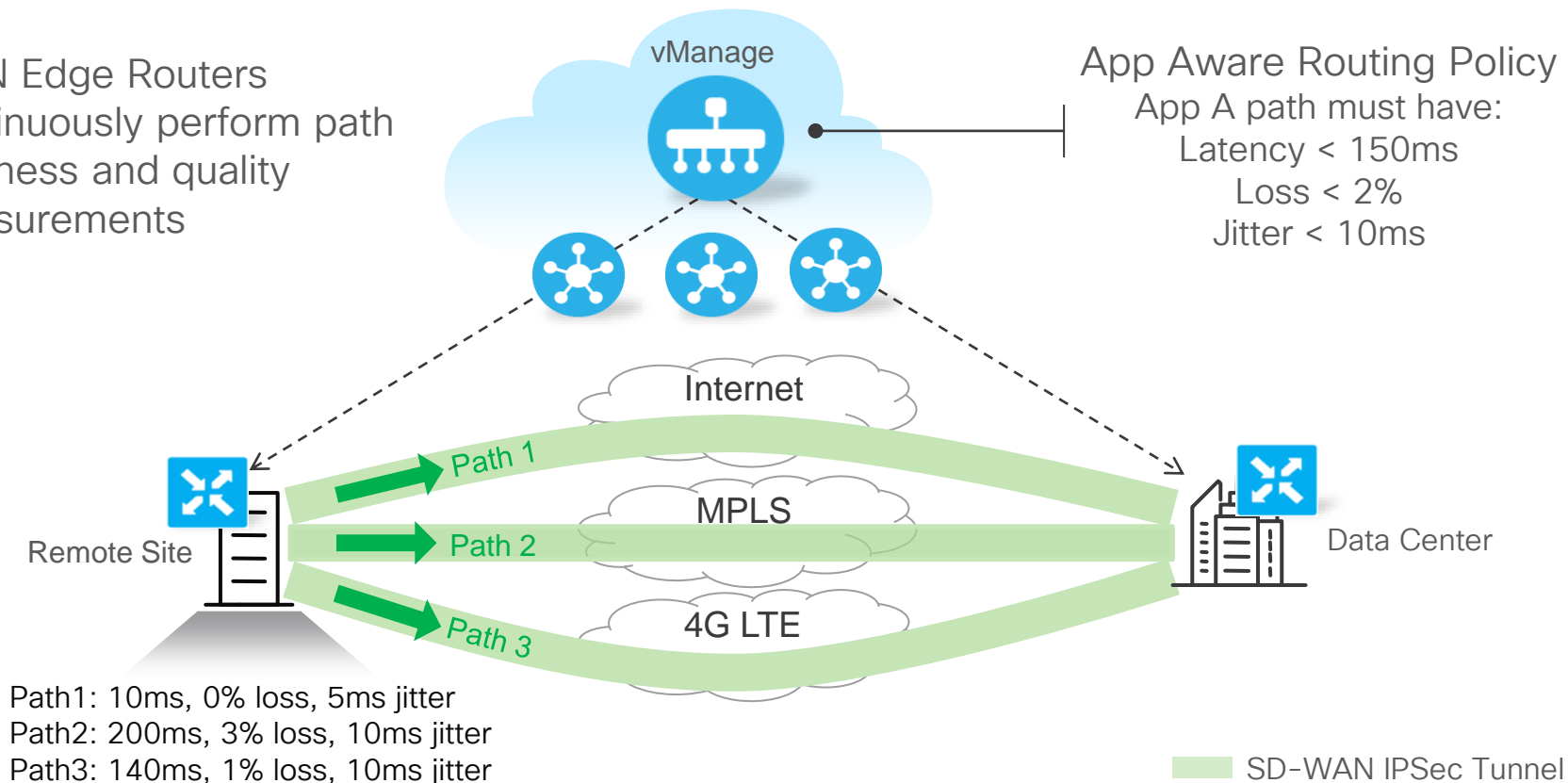

SD-WAN Tunnel

FEC Header
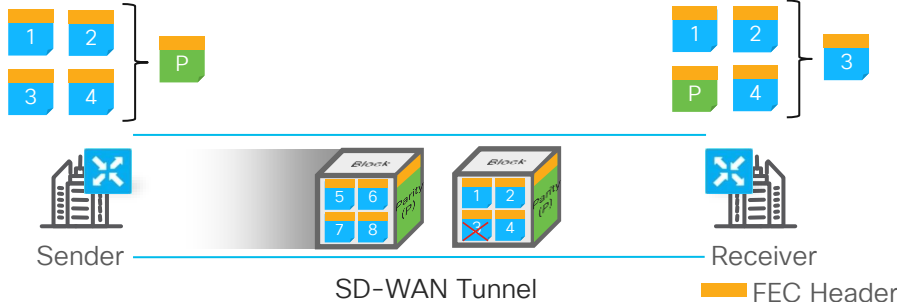
Packet Duplication

- Protects against packet loss
- Protocol (TCP/UDP) agnostic
- Operates over multiple tunnels
- Applied with data policy

Notes:
- Works only over multiple tunnels
- Duplicates are discarded on receiver
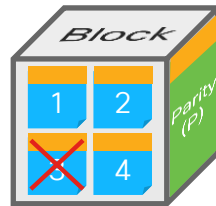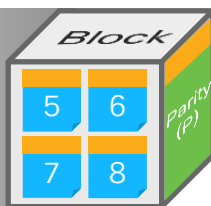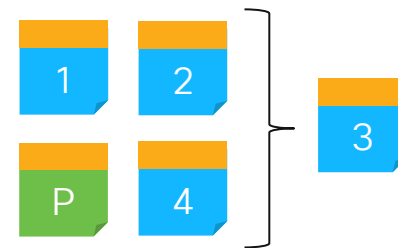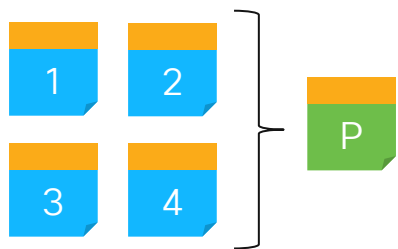

SD-WAN Tunnel

SD-WAN Tunnel
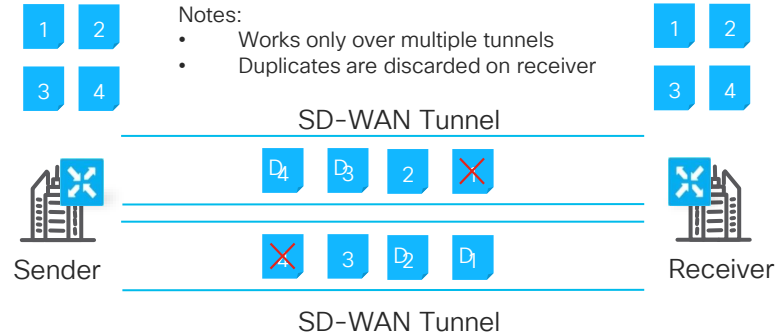
Application Aware Routing

- WAN Edge Routers continuously perform path liveliness and quality measurements

vManage

App Aware Routing Policy
App A path must have:
Latency < 150ms
Loss < 2%
Jitter < 10ms

Internet

Path 1

MPLS

Remote Site

Path 2

4G LTE

Path 3

Data Center

Path1: 10ms, 0% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

SD-WAN IPSec Tunnel

Application Aware Routing and FEC

- Works independently
- AppAware first, data policy next

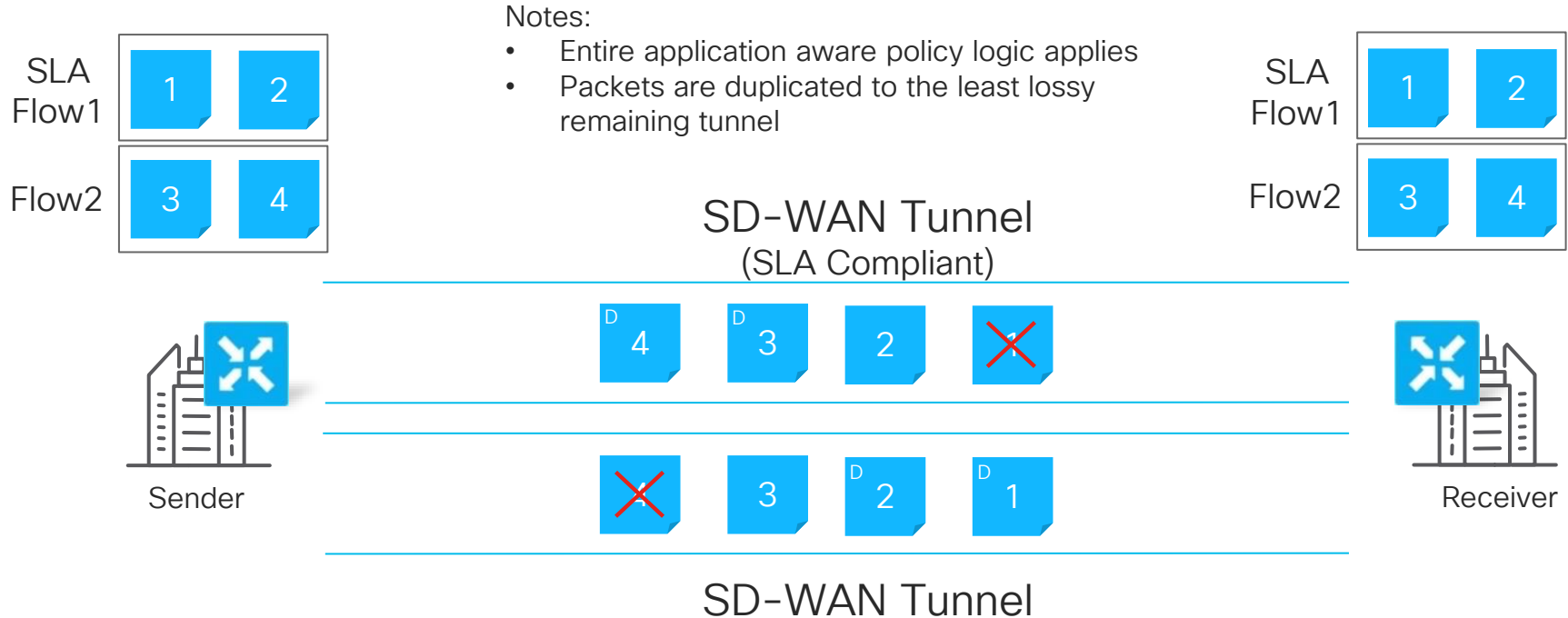- AppAware chooses SLA tunnel(s)
- Data policy applies FEC

Sender
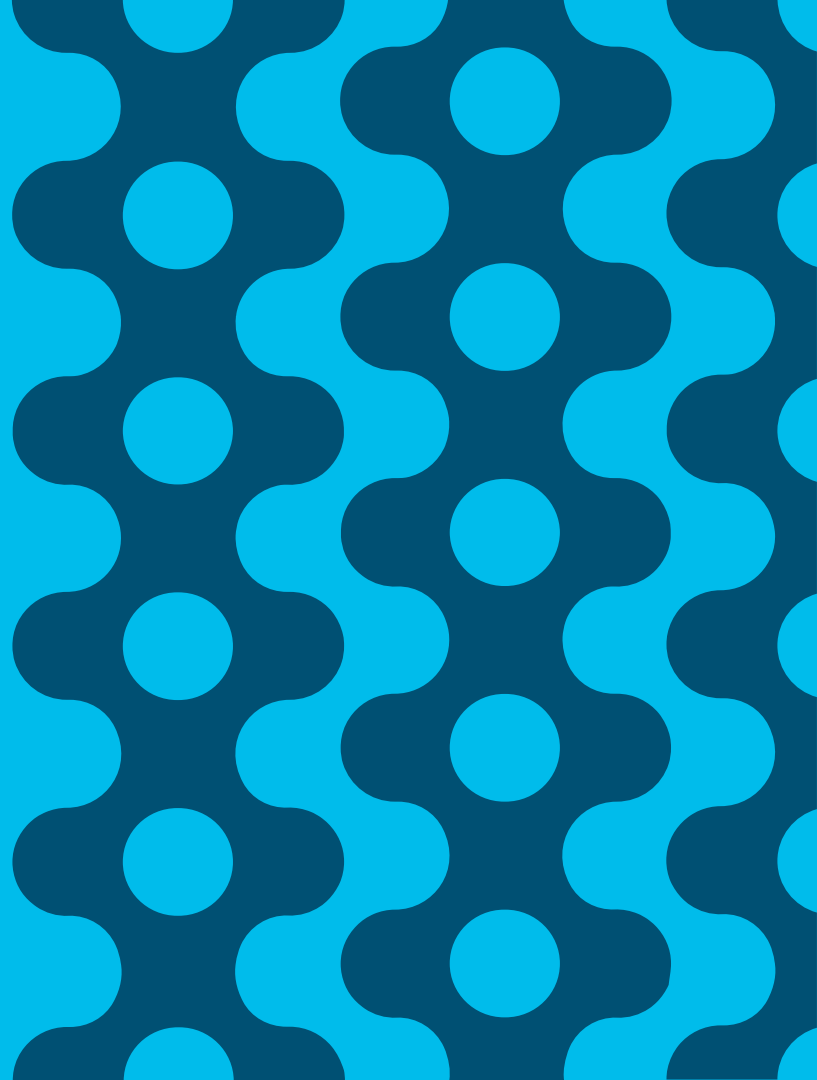
SD-WAN Tunnel

Receiver

FEC Header

Application Aware Routing and Packet Duplication

- Works independently
- AppAware first, data policy next

- AppAware chooses SLA tunnel(s)
- Data Policy applies duplication

Notes:
- Entire application aware policy logic applies
- Packets are duplicated to the least lossy remaining tunnel

SLA Flow1

1 2

Flow2

3 4

SD-WAN Tunnel
(SLA Compliant)

SLA Flow1

1 2

Flow2

3 4

Sender

D 4   D 3   2   ✗ 1
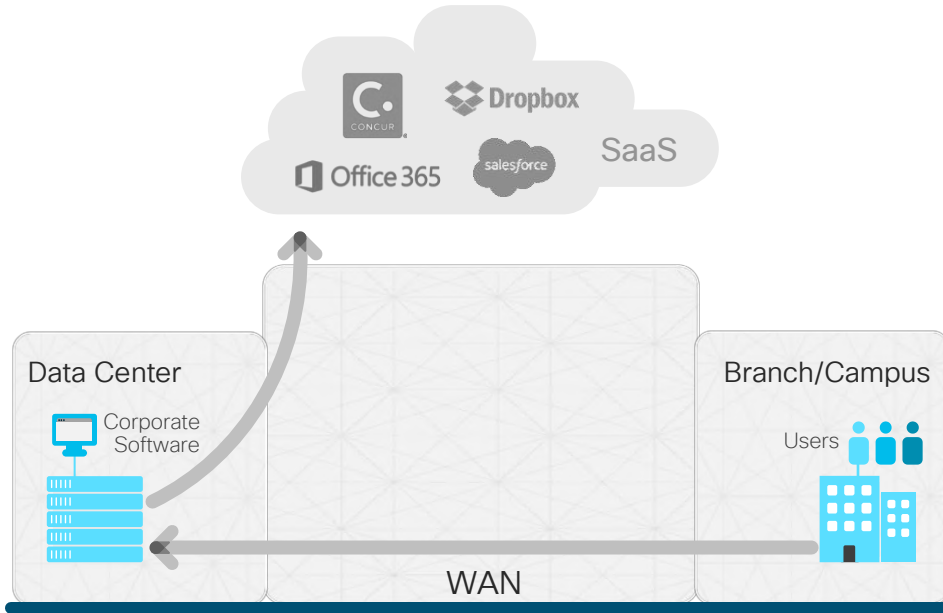
✗   3   D 2   D 1

Receiver

SD-WAN Tunnel

Cisco SD-WAN and Cloud Applications (SaaS) Optimization

Traditional Cloud Applications Access
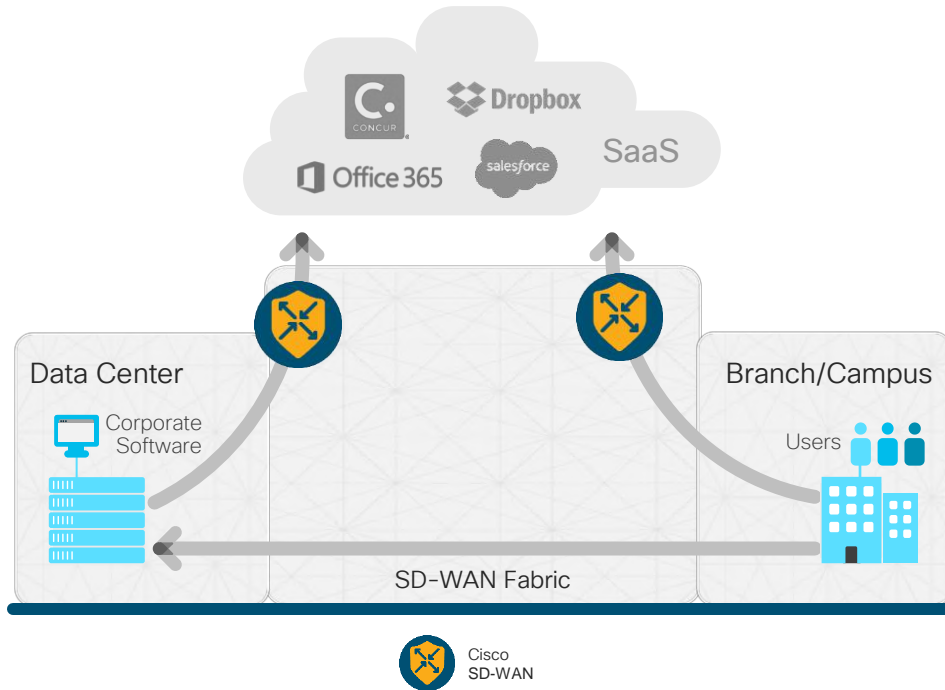## Why Backhauling Impacts Application Performance

- Data Center backhaul
- Costly MPLS transport
- Increased application latency
- Unpredictable user experience

All Internet and critical applications traffic competes for the same WAN bandwidth

Cisco SD-WAN – SaaS Optimization
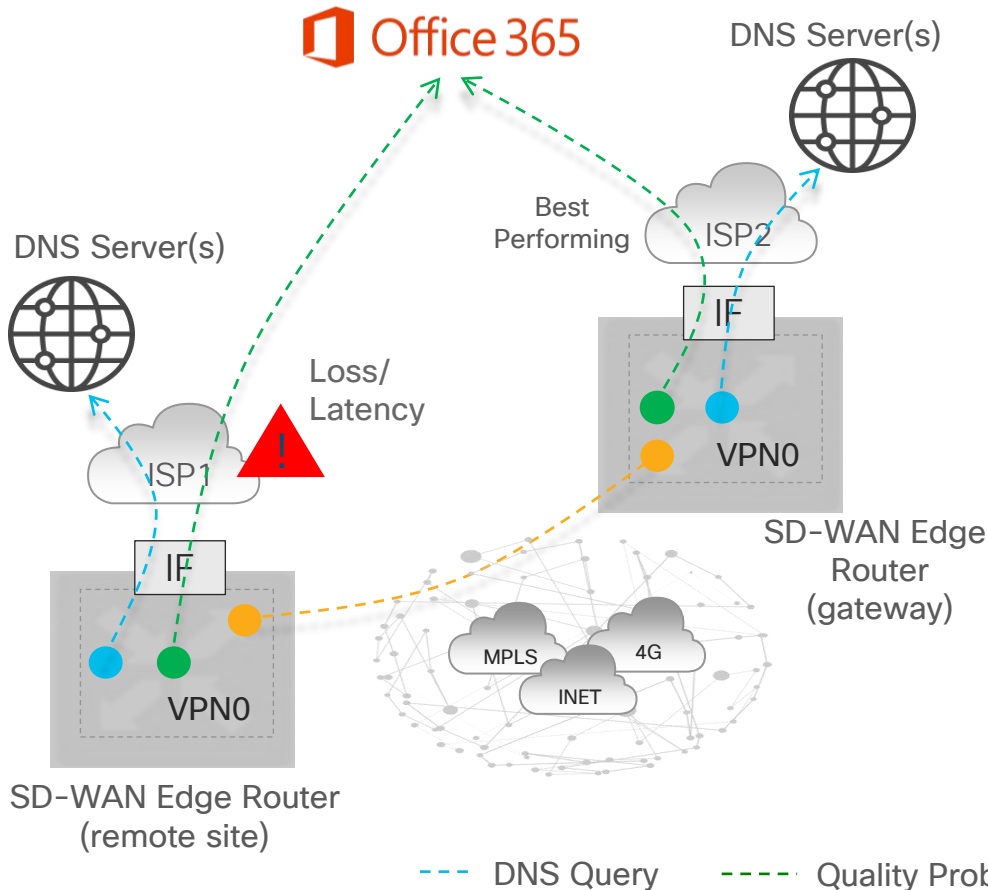## Cloud OnRamp for SaaS

- Continuously monitors the SD-WAN Edge router to SaaS performance on both DIA (Direct Internet Access) path and the back-haul path

- Picks the best performing path based on the performance metrics (loss & delay)

Increased reliability and utilization of best path for SaaS applications
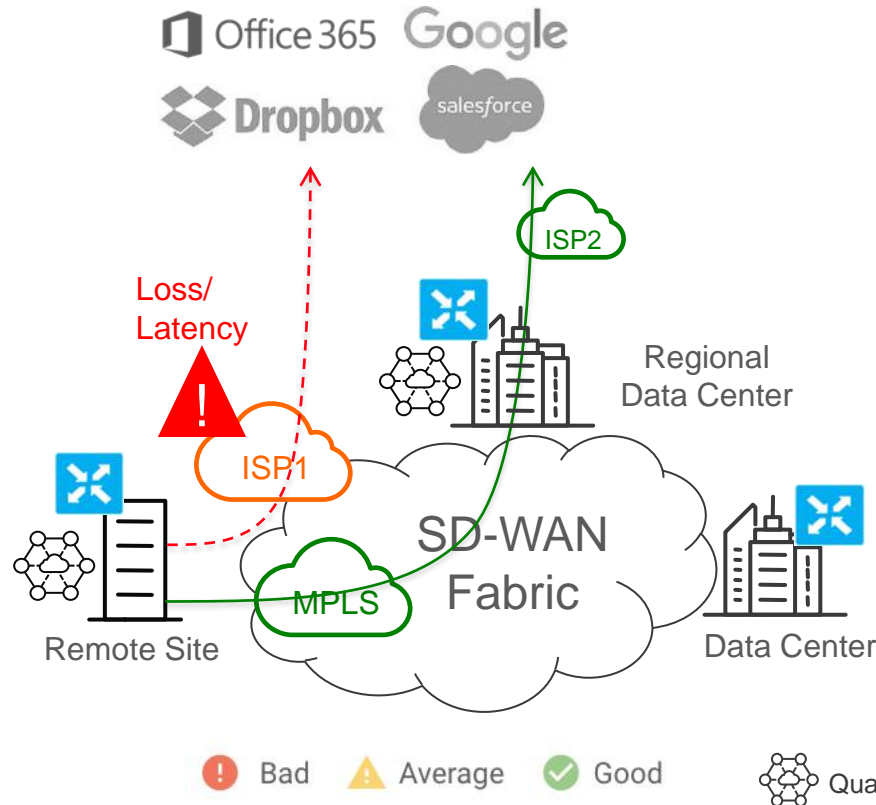
Cisco Cloud onRamp for SaaS
How does it work

- SD-WAN edge routers performs DNS resolution for the configured SaaS application on each path (DIA and gateway)

- SDWAN Edge routers initiates periodic HTTP pings toward the configured cloud onramp SaaS application

- A Quality of Experience (vQoE) score is then calculated for DIA and gateway
  - Remote Edge router compare SLA between local DIA and composite metric of HTTP ping + BFD through the Gateway Edge

- SDWAN Edge router determines best performing path toward Cloud onRamp SaaS applications based on vQoE scores

- - - DNS Query   - - - Quality Probe   - - - BFD

Cisco Cloud onRamp for SaaS
Direct Internet Access and Gateways

Office 365 Google

Dropbox salesforce

Loss/ Latency

!

ISP2

ISP1

Regional Data Center

SD-WAN Fabric

MPLS

Remote Site

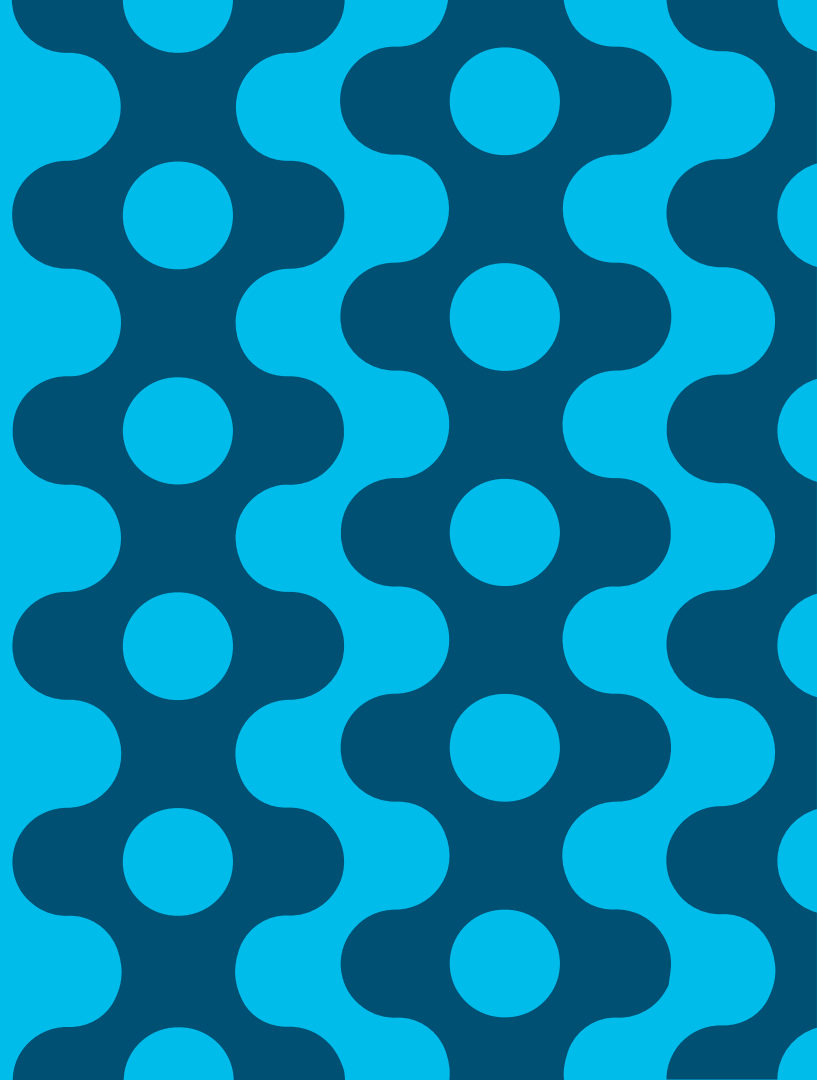Data Center

Bad Average Good Quality Probing

- One of the recommended designs, for SaaS deployments

- Cloud On-ramp continuously monitors the edge to SaaS performance on both DIA path and the back-haul path

- SDWAN Edge router picks the best performing path based on the performance metrics (loss & delay)
  - Per-Application, Per-VPN

- Automatic failover in case of performance degradation

- Fully automated

Cisco Cloud onramp for SaaS & vQoE scores

- The vQoE value ranges from 0 to 10, with 0 being the worst quality and 10 being the best.

- vQoE = desired metrics / actual metrics * 10

- vQoE score is computed for each remote site application and per path

| SaaS Application	Path 1 - vQoE on ISP1 DIA	Path 2 - vQoE on Gateway 1
O365	9	4
Sales force	8	4
Box	6	8
Dropbox	6	8
Google Apps	7	9
Goto Meeting	1	8
Intuit	3	9
Oracle	7	4
SugarCRM	8	8
ZenDesk	4	8
Zoho CRM	6	9

Cisco SD-WAN and Secure Branch

Traditional Branch Security

- Security enforcement at the branch is too costly, security enforcement at the data center is too inefficient (for cloud)

- Segmentation over MPLS is underlay specific, segmentation over-the-top is operationally cumbersome

- Per segment topology... forget about it!
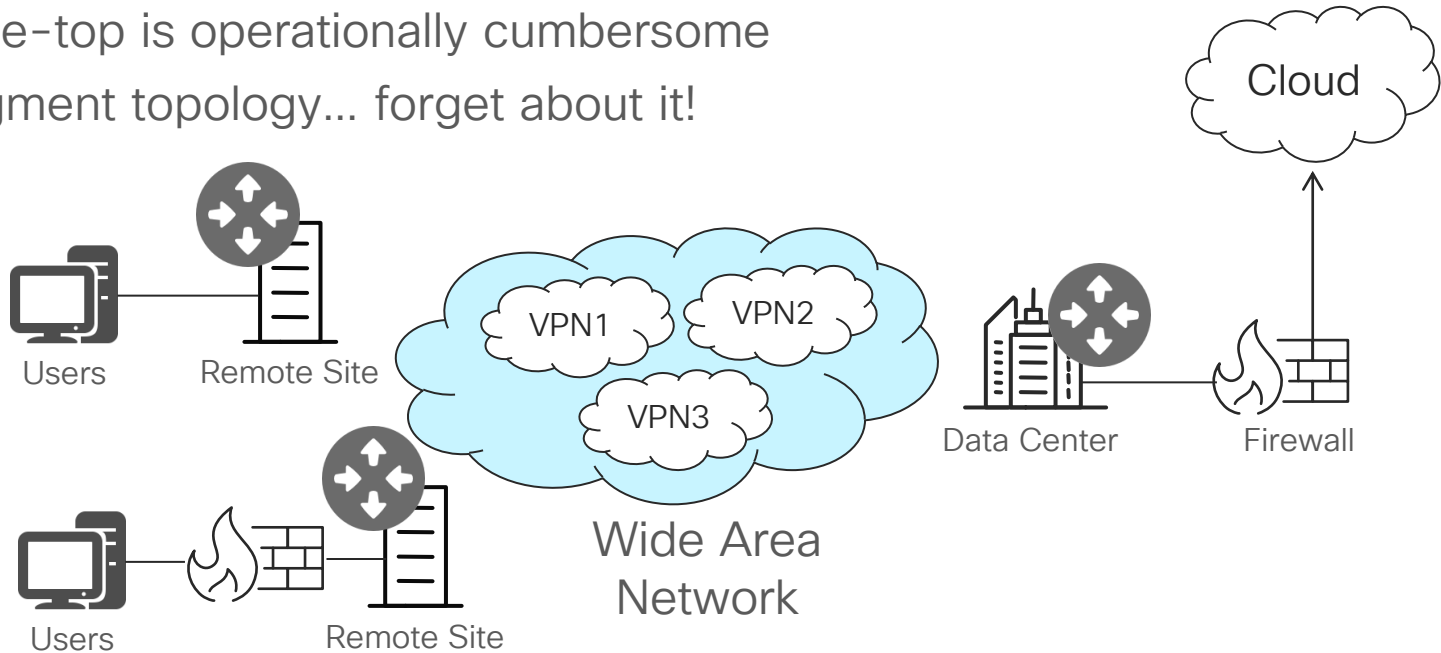
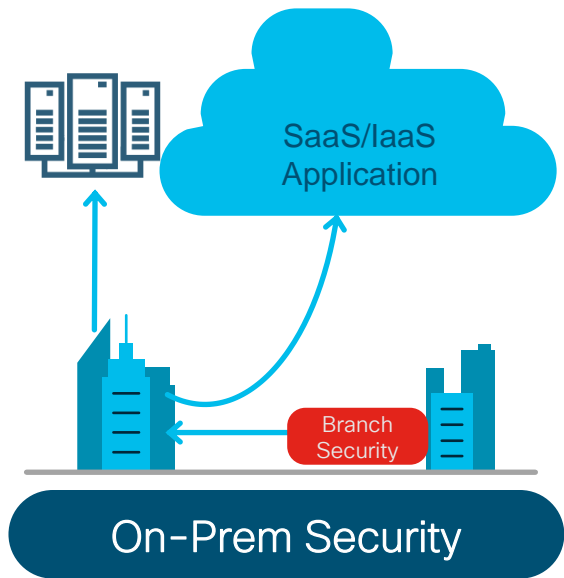# Why SD-WAN Branch Security?
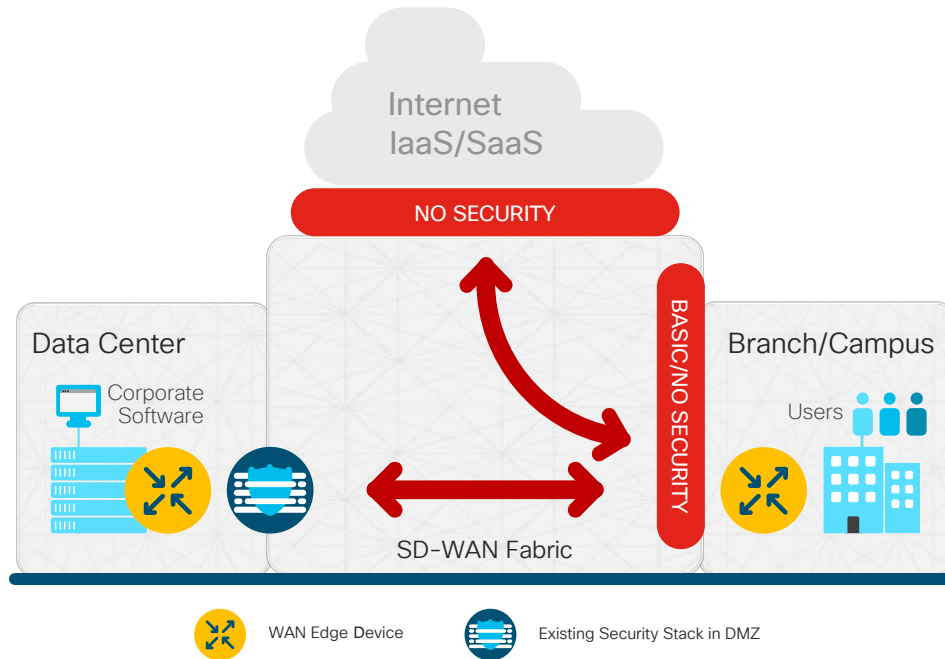
Internal & External Threats

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

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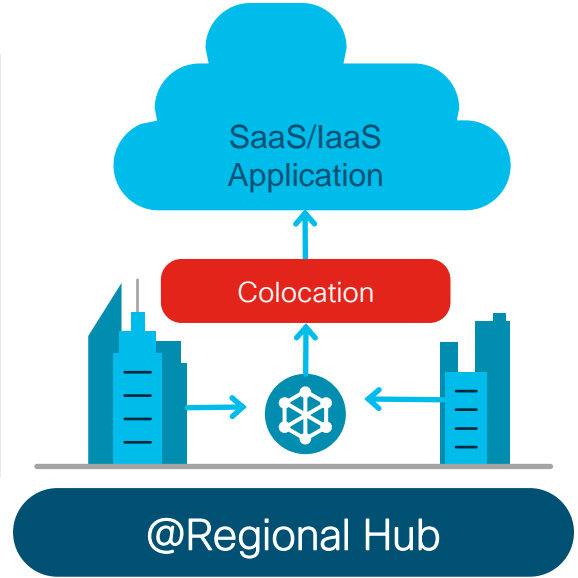- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)

SD-WAN Security Models. Driving towards SASE

SaaS/IaaS Application

Branch Security

On-Prem Security

Thick branch with Routing and Security (SD-Branch model)

SaaS/IaaS Application

Cloud Security

Cloud Security & SASE

Thin branch with security in the cloud

SaaS/IaaS Application

Colocation

@Regional Hub

Security Services as VNF at Regional Colocation Hub

Cisco Secure SD-WAN: Cisco SD-WAN + Branch Security

Internet IaaS/SaaS

Data Center

Corporate Software

Branch/Campus

Users

SD-WAN Fabric

Single Management Console
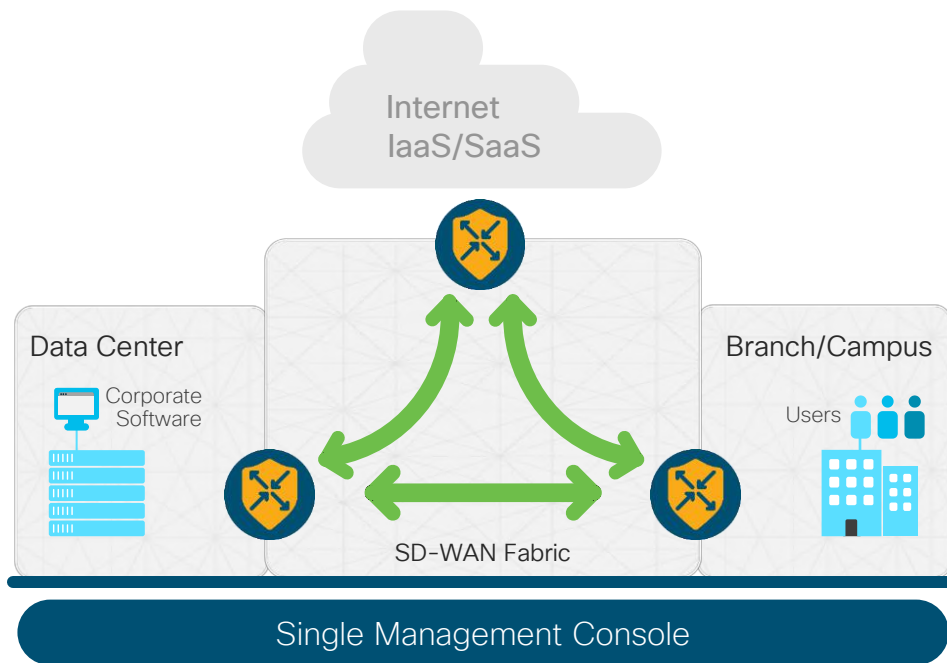
Full Edge Security Stack

On-Prem Security
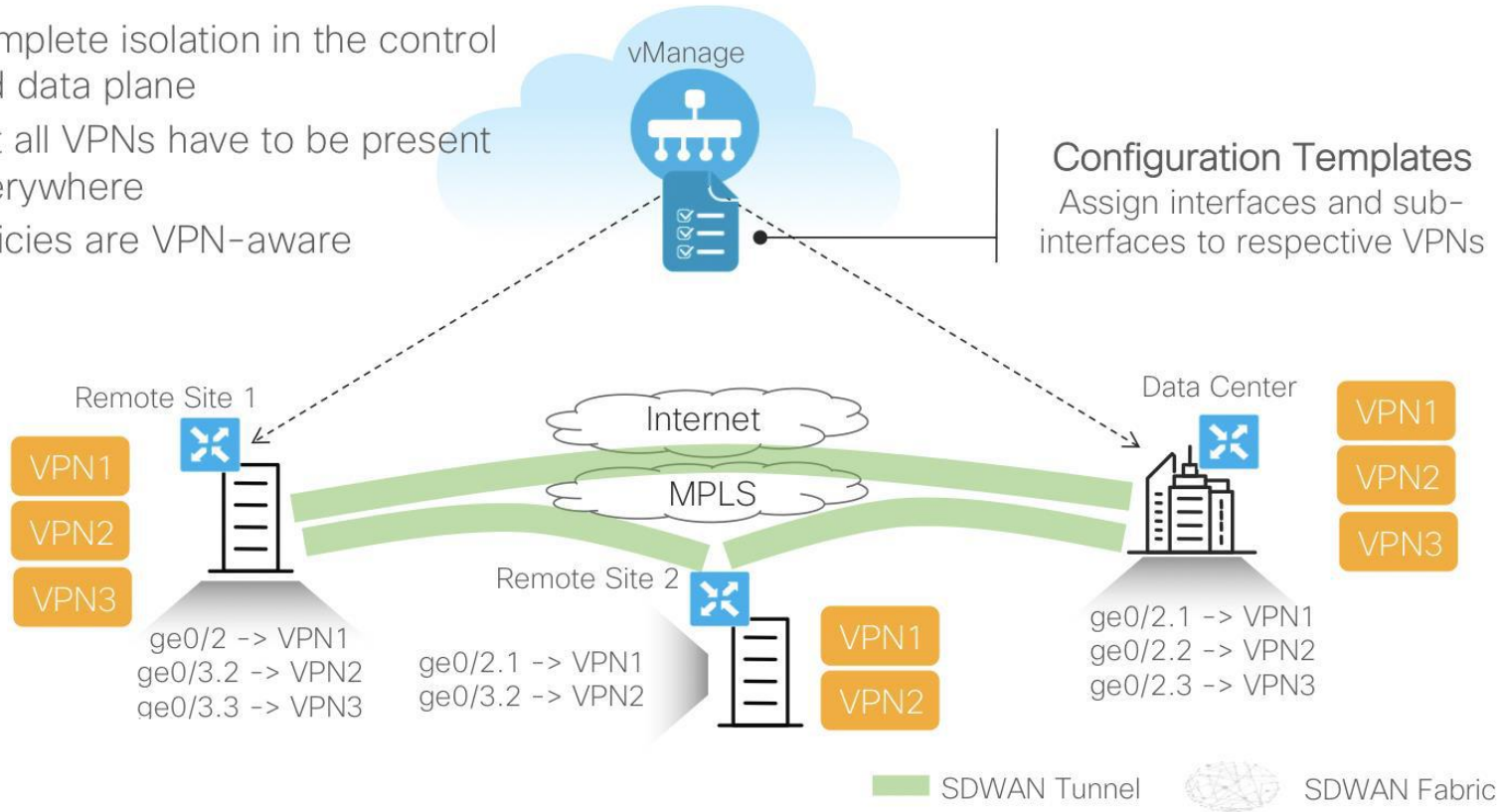Mitigate Internal & External Threats

Cloud Security
Mitigate External Threats at Scale

- SWG, DNS protection, CASB
- FW, URL filtering, IPS
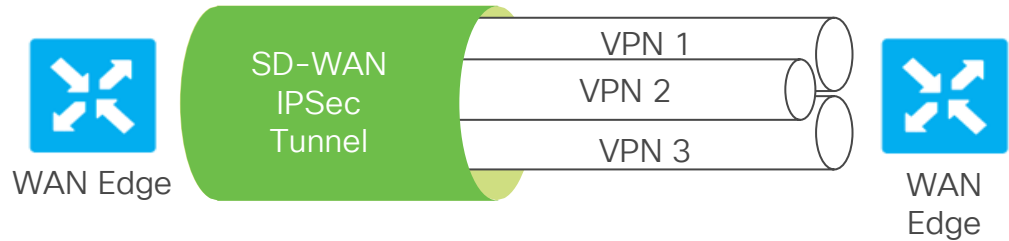- Segmentation & Policy
- Zero-trust authentication and Encryption

Cisco SD-WAN - Secure Branch Segmentation

- Complete isolation in the control and data plane
- Not all VPNs have to be present everywhere
- Policies are VPN-aware

vManage

Configuration Templates
Assign interfaces and sub-interfaces to respective VPNs

Remote Site 1

VPN1
VPN2
VPN3

Internet

MPLS

Data Center

VPN1
VPN2
VPN3

ge0/2 -> VPN1
ge0/3.2 -> VPN2
ge0/3.3 -> VPN3

Remote Site 2

ge0/2.1 -> VPN1
ge0/3.2 -> VPN2

VPN1
VPN2

ge0/2.1 -> VPN1
ge0/2.2 -> VPN2
ge0/2.3 -> VPN3

SDWAN Tunnel   SDWAN Fabric

Cisco SD-WAN - Secure Branch Segmentation

- Security Zoning
- Compliance
- Guest Wi-Fi
- Multi-Tenancy
- Extranet

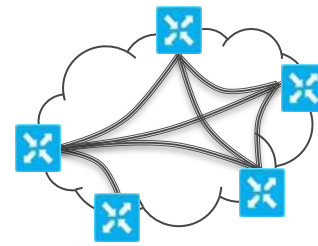SD-WAN IPSec Tunnel
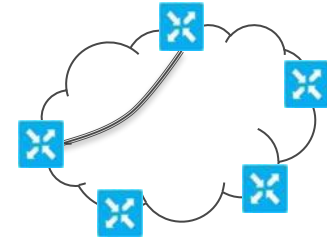
WAN Edge

VPN 1
VPN 2
VPN 3

WAN Edge

Per-VPN Topology
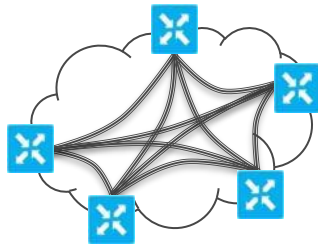
Full-Mesh
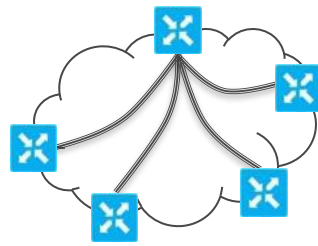
Hub-and-Spoke

Partial Mesh

Point-to-Point

Cisco 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

SD-WAN Security: vManage Provisioning Wizard

Add Security Policy

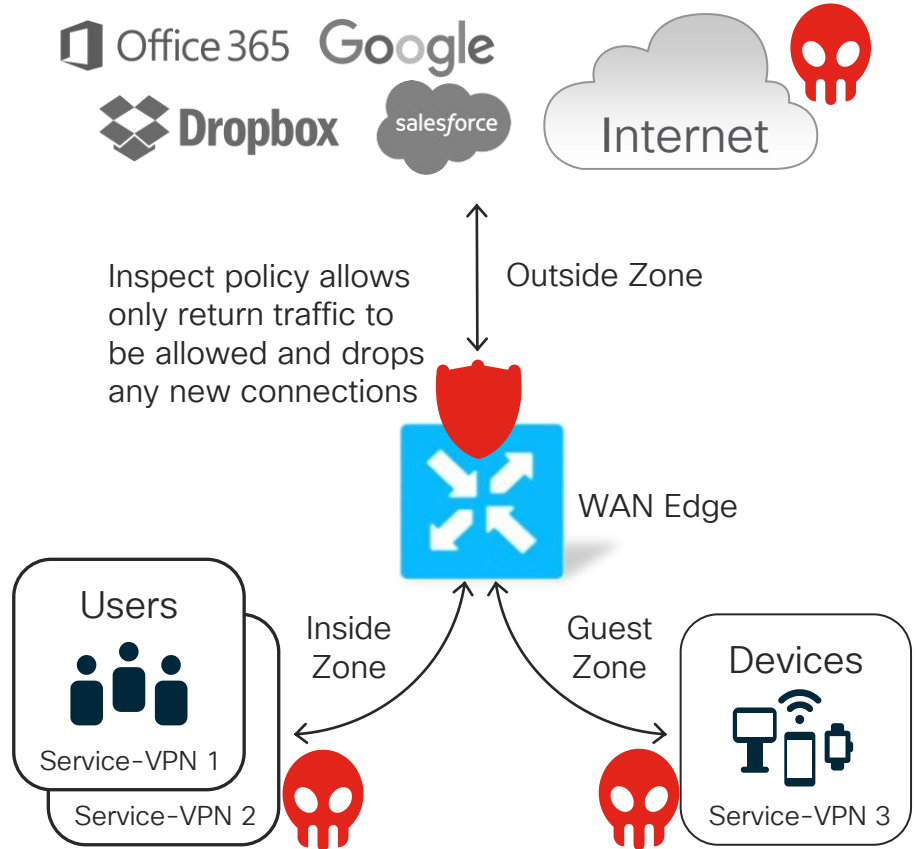Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention

Guest Access
Application Firewall | URL Filtering

Direct Cloud Access
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security

Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security

Custom
Build your ala carte policy by combining a variety of security policy blocks

Proceed   Cancel

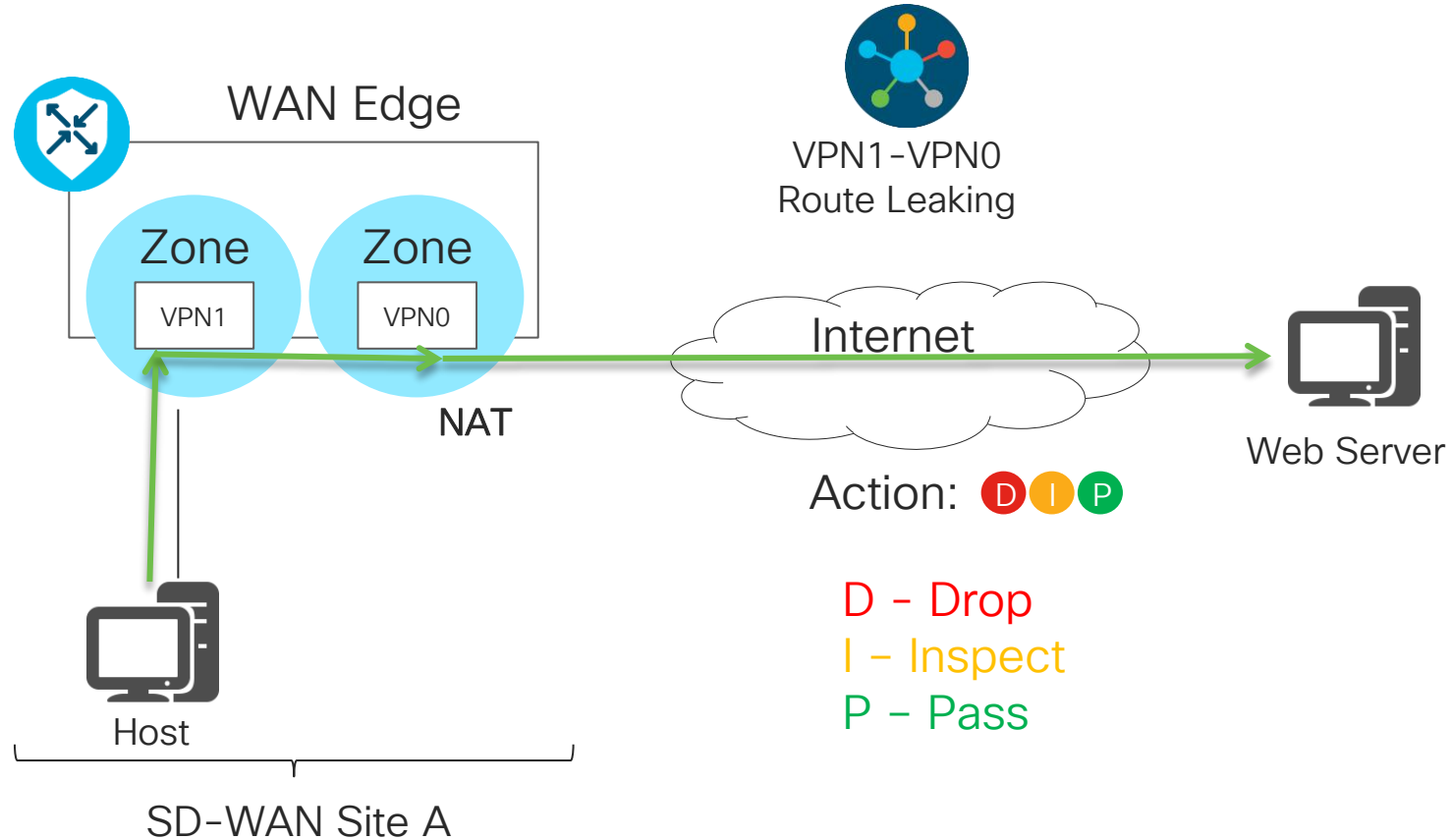Configuration > Security

⊕ Add Security Policy
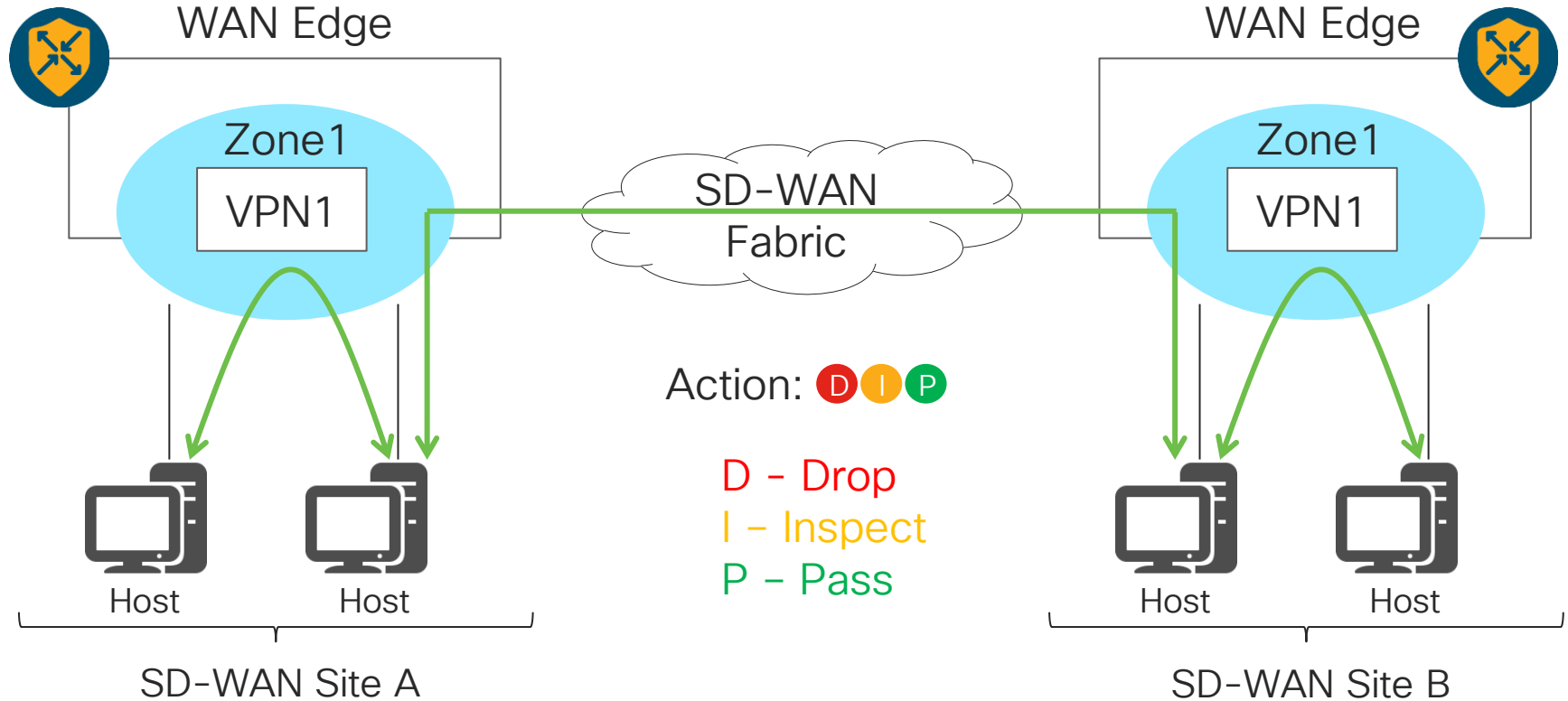
Application Aware Firewall

- ➤ Stateful Firewall, Zone Policies

- ➤ VPN(s) are mapped to a zone

- ➤ Intra-zone, inter-zone and zone to DIA traffic policies

- ➤ Block, pass or inspect traffic

- ➤ Block 1400+ Layer 7 Applications

- ➤ HSL Logging

- ➤ Self Zone Policy

Inspect policy allows only return traffic to be allowed and drops any new connections

Outside Zone

WAN Edge

Users
Service-VPN 1
Service-VPN 2

Inside Zone

Guest Zone

Devices
Service-VPN 3

Ent. Firewall App Aware: DIA / DCA

WAN Edge

Zone

VPN1

Zone

VPN0

NAT

VPN1–VPN0
Route Leaking

Internet

Web Server

Action: D I P

D - Drop
I – Inspect
P – Pass

Host

SD-WAN Site A

Ent. Firewall App Aware: Intra-Zone Security

WAN Edge

WAN Edge

Zone1

VPN1

SD-WAN Fabric

Zone1

VPN1

Host

Host

Action: D I P

D - Drop
I – Inspect
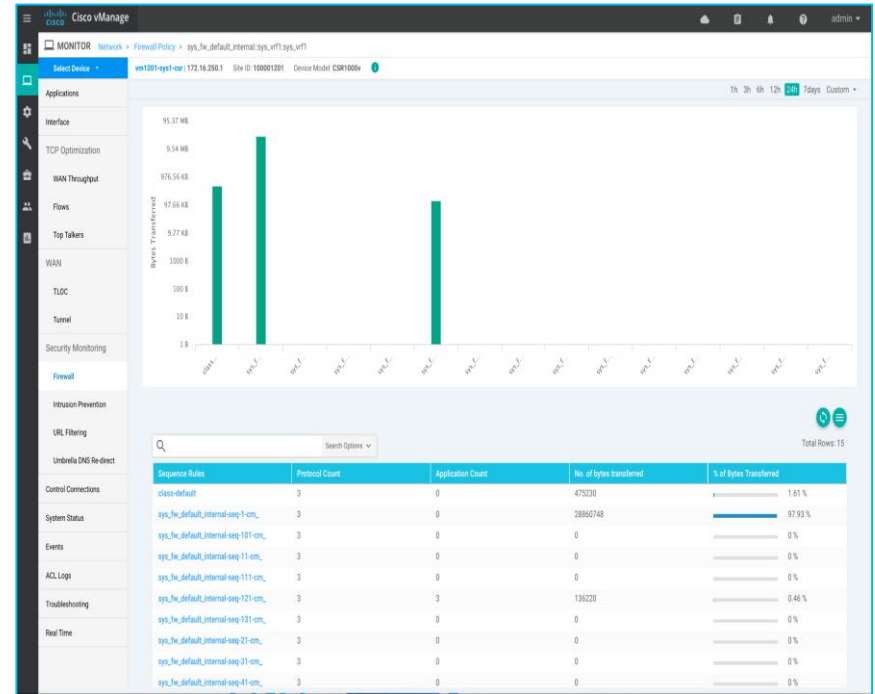P – Pass

Host

Host

SD-WAN Site A

SD-WAN Site B

Enterprise App Aware Firewall Monitoring

Overall Dashboard – Firewall Enforcement
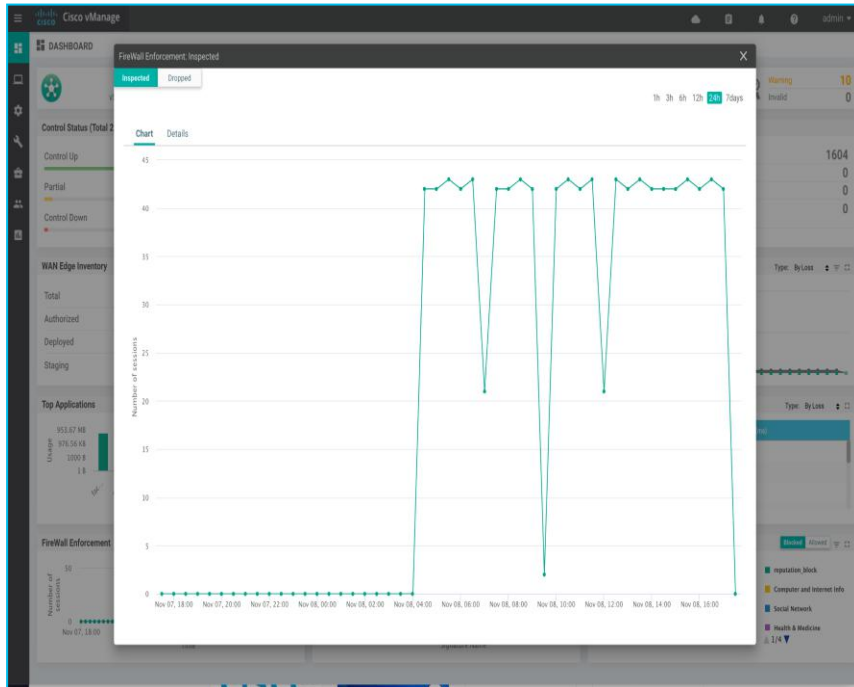
Device Dashboard – Firewall

Intrusion Prevention and Detection

➢ Snort IPS engine

➢ Runs in a service container on Cisco SD-WAN Edge routers (ISR1K/ISR4K/CSR1K)

➢ Backed by global Threat Intelligence (TALOS) signatures updated automatically

➢ Inspects traffic in VPNs of interest

➢ Supports three levels of signature sets

➢ Signature whitelist support

➢ Can run in detection mode

Internet

Signatures

TaLOS

WAN Edge

Users
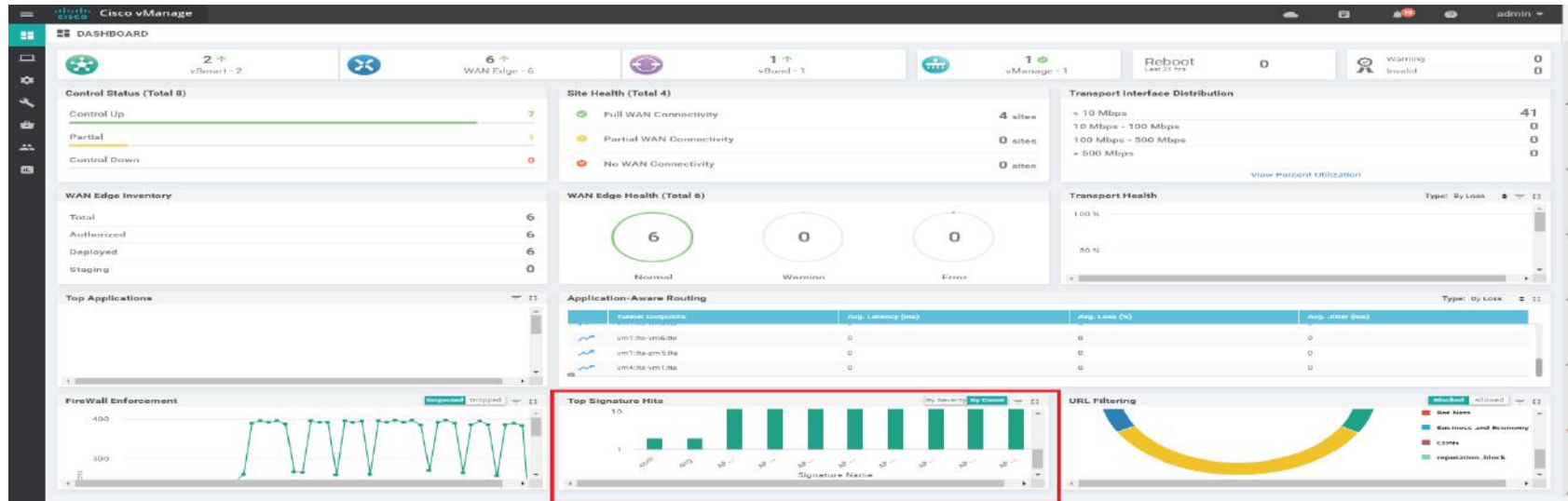Service-VPN 1

Users
Service-VPN 2
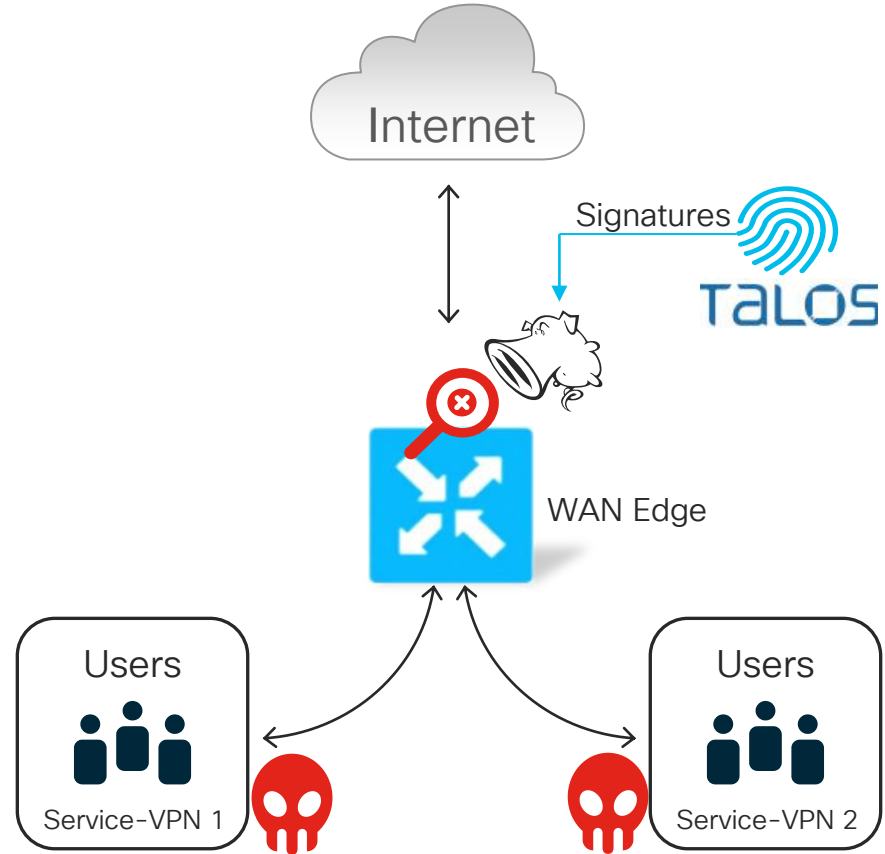
Intrusion Prevention – Monitoring

Top Signature Violations dashboard

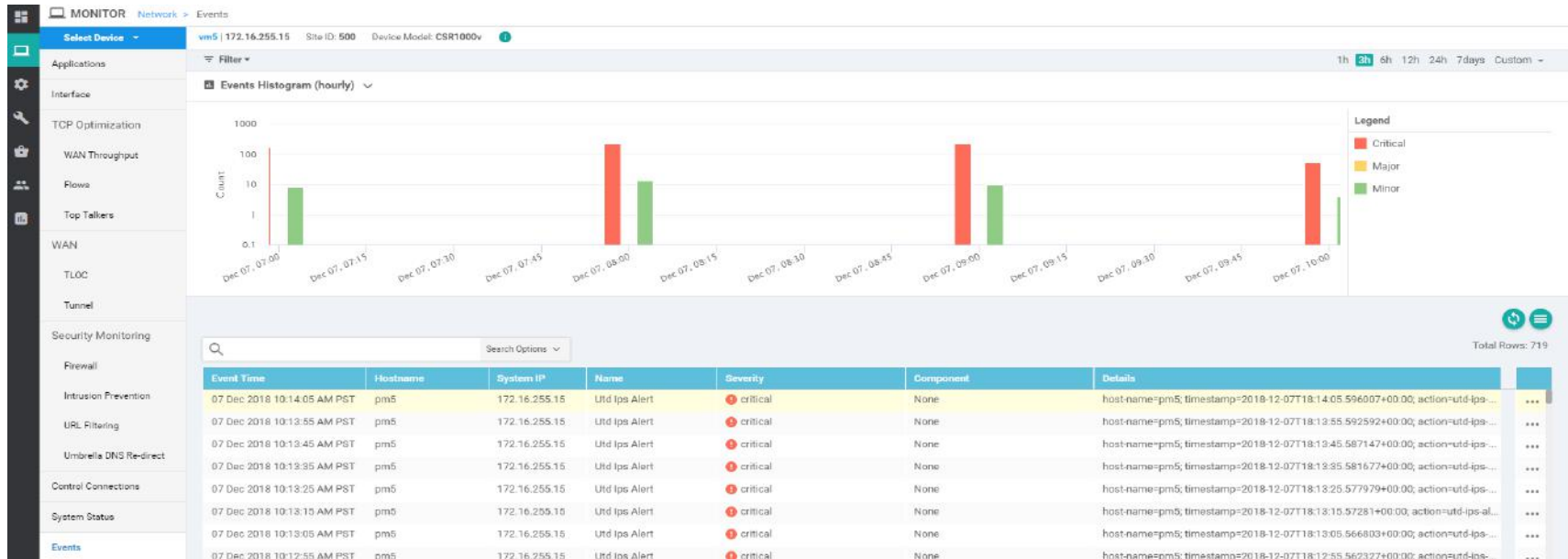Signatures seen by the devices running IPS in the network

Two Views:

- Threats by severity (over time)
- Total threat count (for the selected time period)

Intrusion Prevention – Monitoring

Check device level alerts in the Device events page

URL Filtering

➢ Runs in a service container on Cisco SD-WAN Edge Routers (ISR1K*/ISR4K/CSR1K)

➢ Cloud lookup with local caching or local lookup

    ➢ Local lookup downloads URL database to the router

➢ 82+ Web Categories with dynamic updates

➢ Inspects traffic in VPNs of interest

➢ Block based on Web Reputation score

➢ Create custom Black and White Lists

➢ Customizable end-user notifications

Internet

WAN Edge

Users
Service-VPN 1

Users
Service-VPN 2
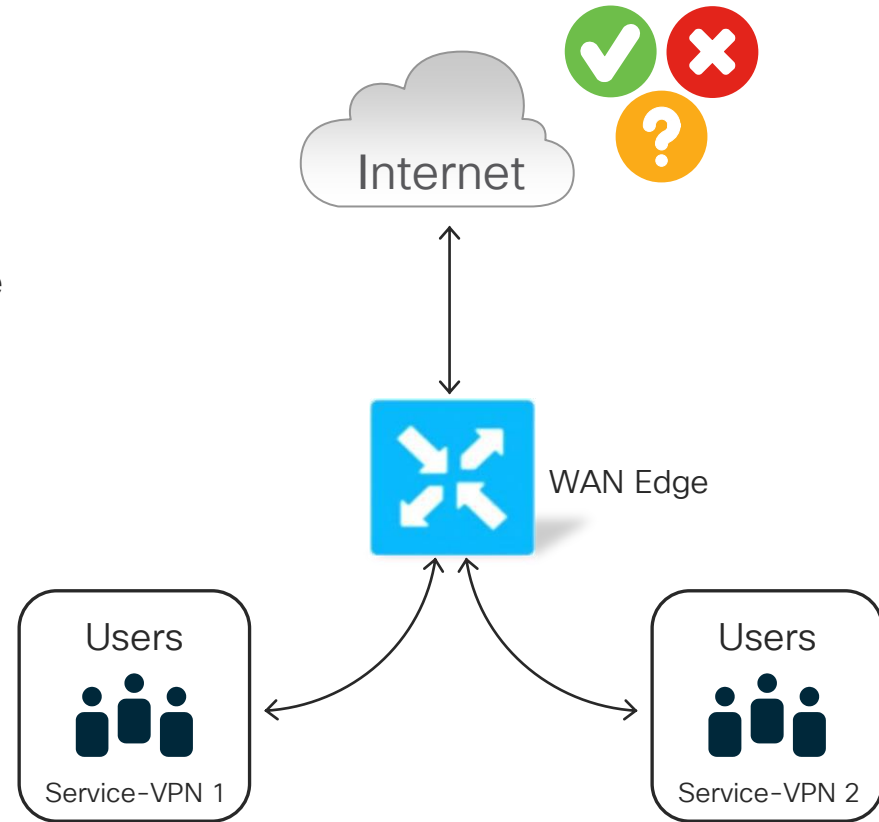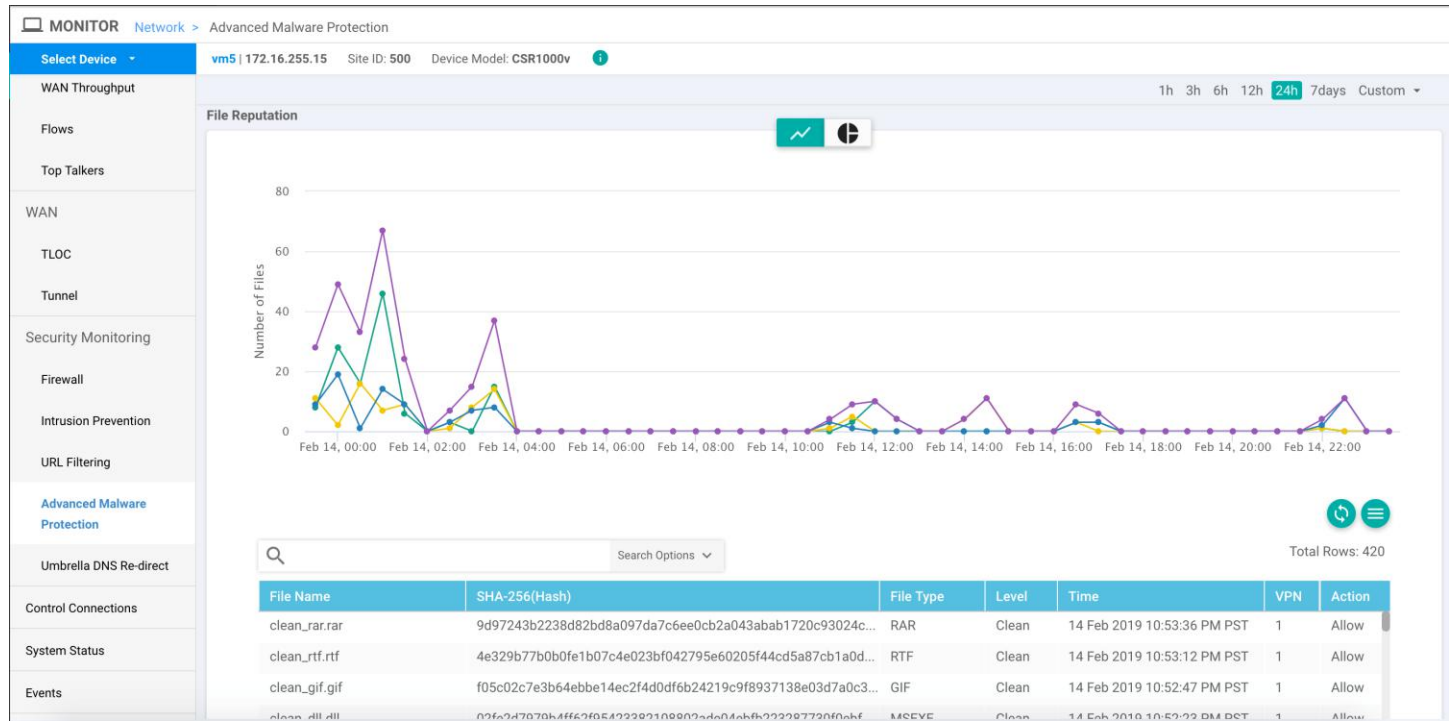
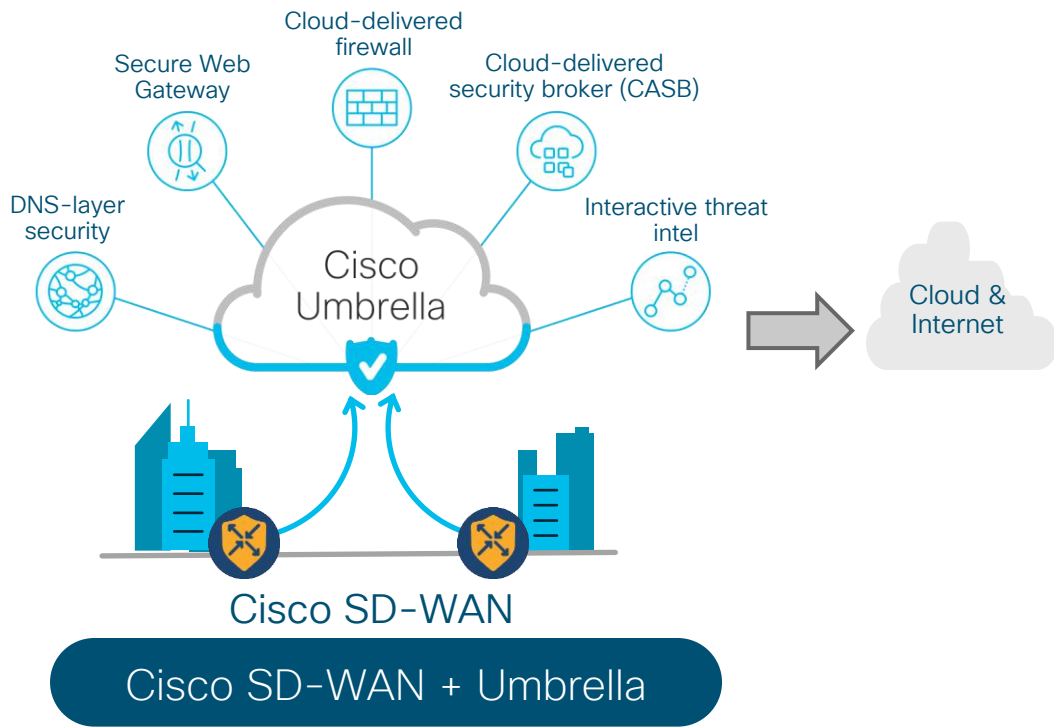# vManage – URL Filtering Monitoring
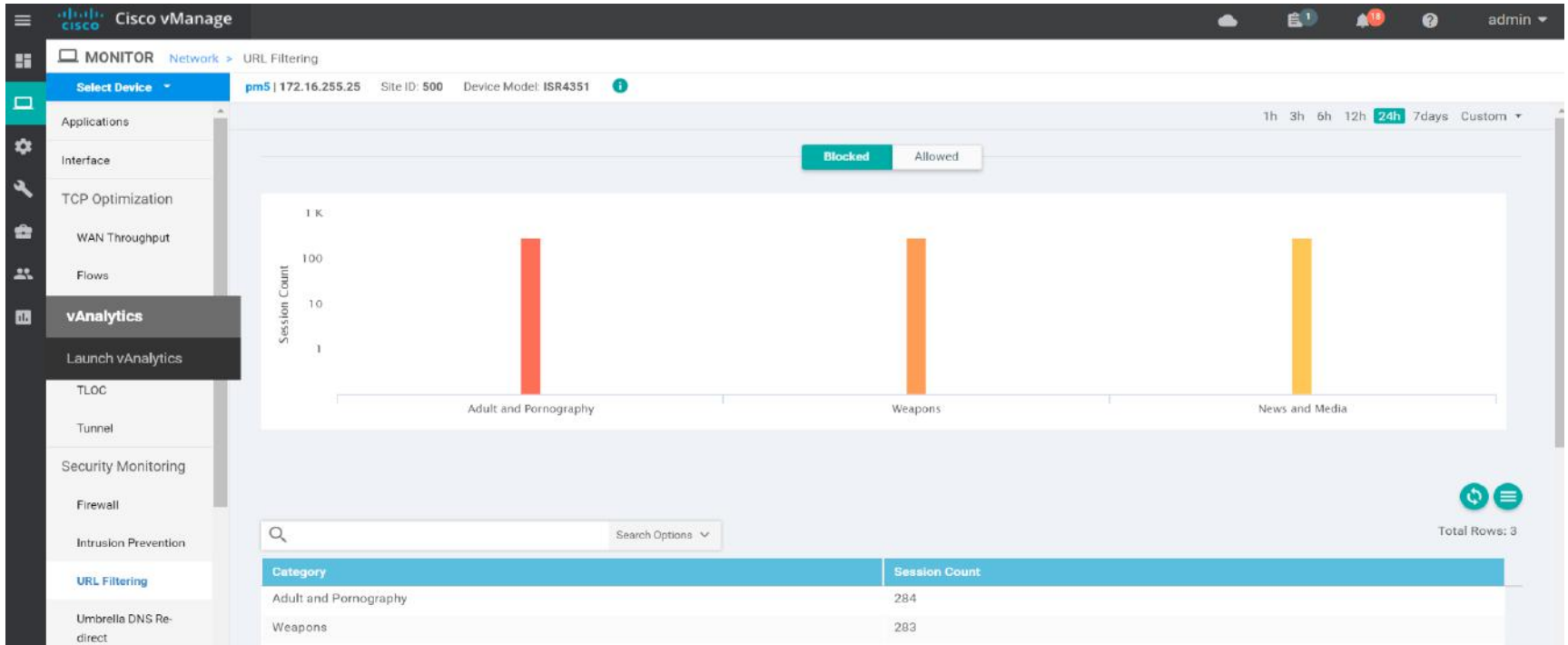
Advanced Malware Protection

➤ Runs in a service container on Cisco SD-WAN Edge routers (ISR1K/ISR4K/CSR1K)

➤ File reputation check powered by Talos

➤ Automated signature update from ThreatGrid to Talos

➤ Inspects traffic in VPNs of interest

➤ Leverages Snort engine to identify file transfers

➤ Sandboxing and file analysis for unknown signatures powered by ThreatGrid

TALOS

AMP

Check Signature

Internet

WAN Edge

Check file

ThreatGrid

Malware Sandbox
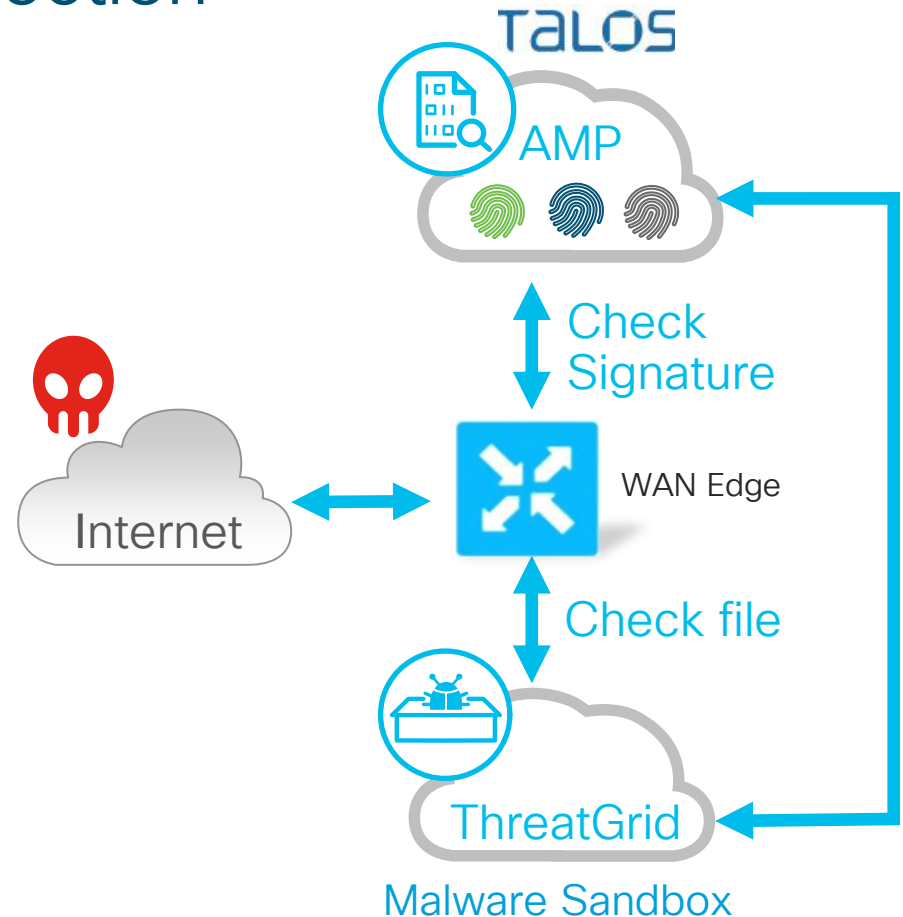
vManage – AMP Monitoring

Cisco SD-WAN and Cloud Security (SIG)

Secure Web Gateway

Cloud-delivered firewall

Cloud-delivered security broker (CASB)

DNS-layer security

Interactive threat intel

Cisco Umbrella

Cloud & Internet

Cisco SD-WAN

Cisco SD-WAN + Umbrella

- Cisco Umbrella - Secure Internet Gateway is a platform with many different security services

- The current platform includes DNS-layer security, Web Gateway (SWG), Cloud Delivered Firewall, CASB

- Traffic redirection for SIG services via IPSec tunnel
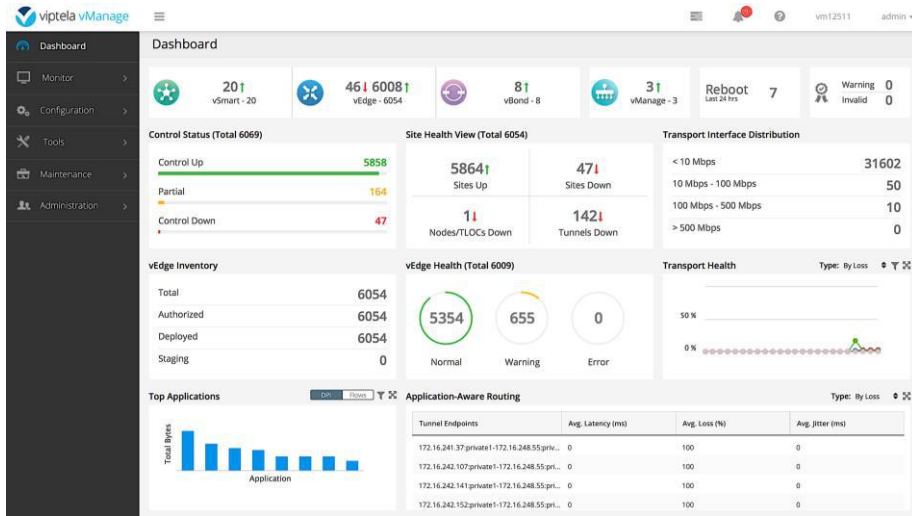
- Automated IPSec tunnel creation support

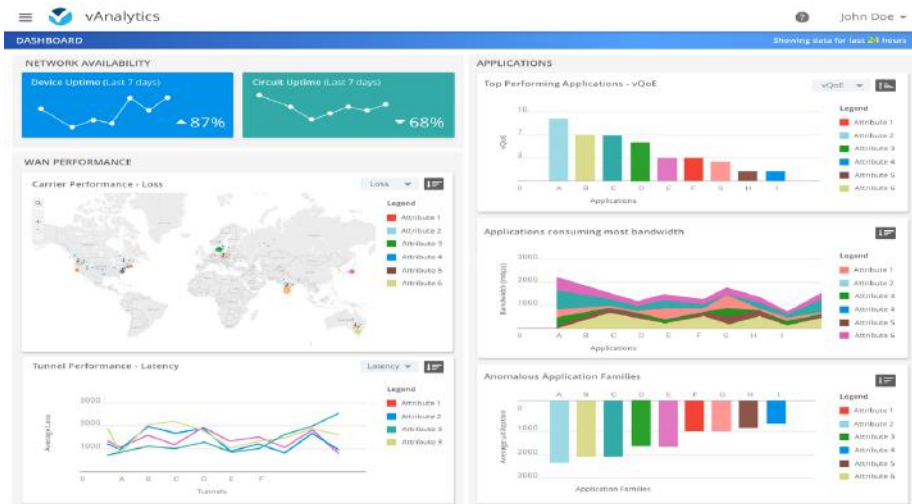# Cisco SD-WAN and Automation and Simplified Management
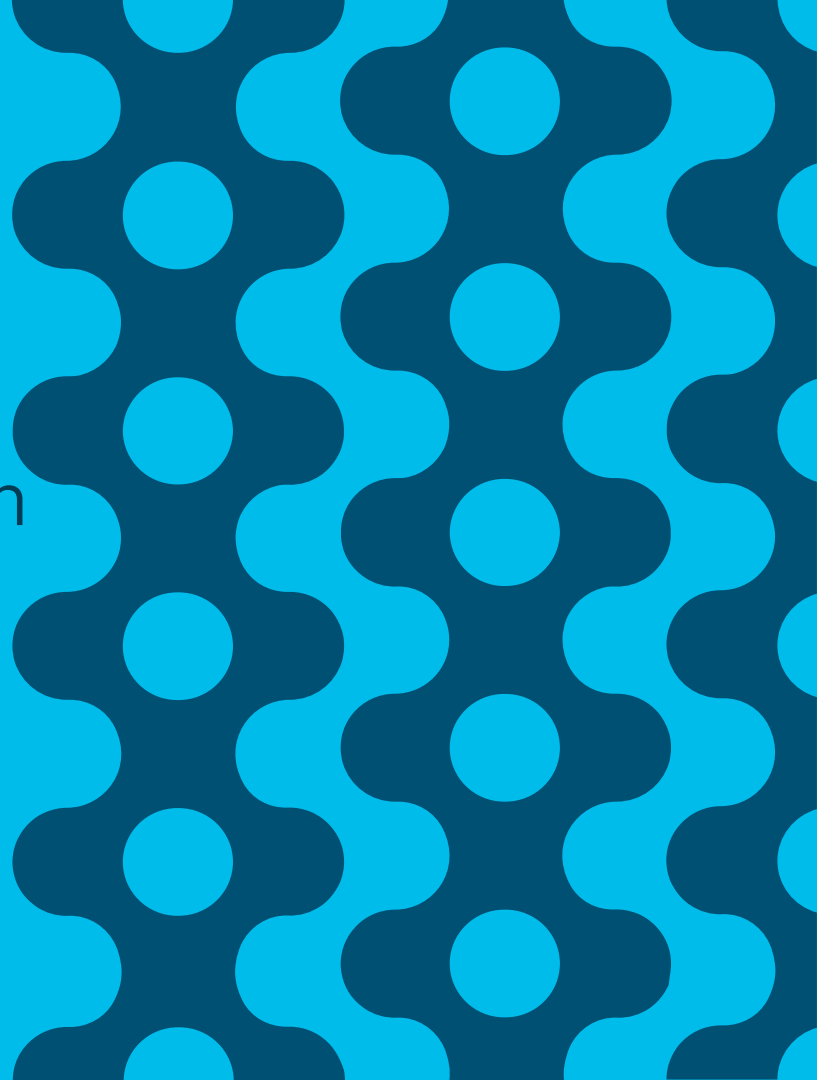
Cisco SD-WAN – Automation and Simplified Management

vManage – Single Pane Of Glass Operations

vAnalytics – Rich Analytics

Centralized Device Configuration Enforcement

- Centralized Feature Templates
- Enforces configuration compliance
- Self-recover on misconfiguration

- Feature Configuration with Variables

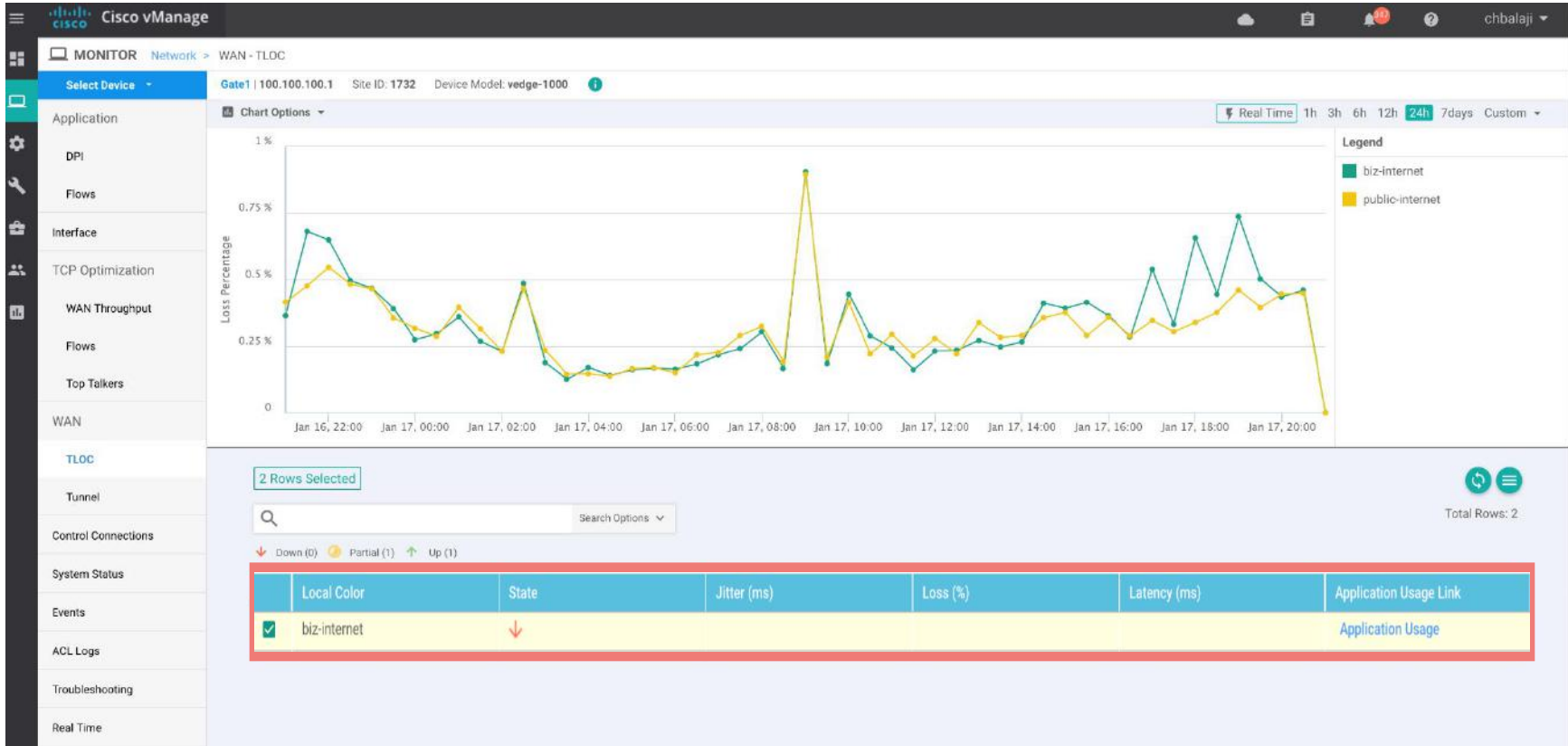| Status	Chassis Number	System IP	Hostname	Latitude	Longitude	System IP	Site ID	Bandwidth Upstream
✓	4de0b85f-a2ae-42ec-8b45-3808285cd008	1.1.1.4	RemoteSite	37.33	-121.88	1.1.1.4	104	100
✓	5f05358a-bef7-4e15-9ade-8ffd8f27ec93	1.1.1.6	AWS	45.52	-122.67	1.1.1.6	106	100
✓	9391da23-f0d1-4259-88d9-e10ae714708c	1.1.1.5	DataCenter	40.71	-74.0	1.1.1.5	105	250

Application and Flow Visibility
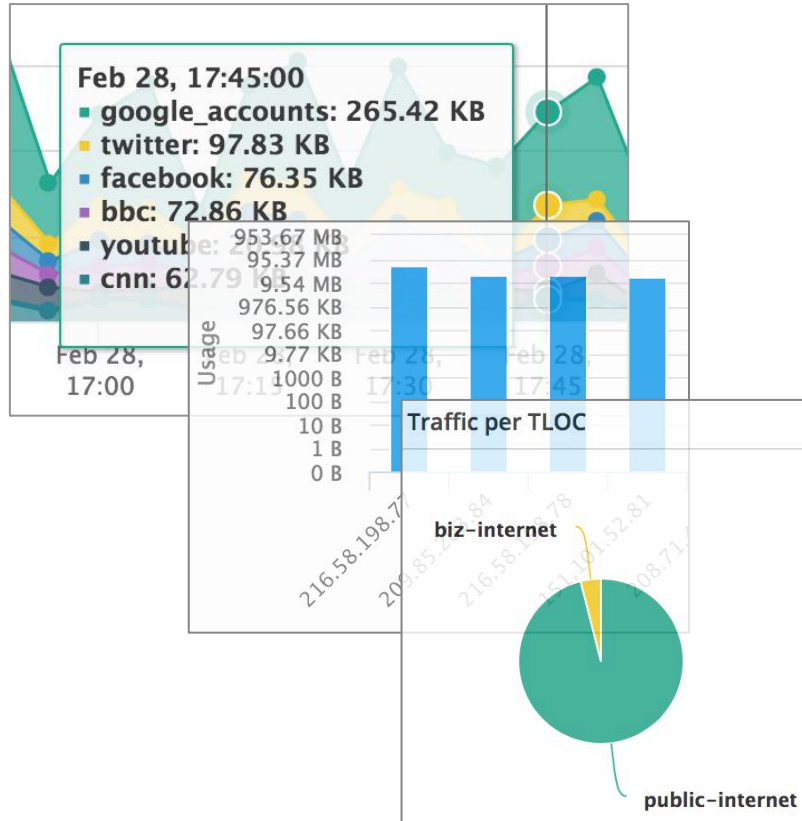
- Application and flow visibility for each WAN Edge router
  - DPI/NBAR2 need to be enabled for application visibility
  - Flow data can be exported from WAN Edge to external collector

- Realtime views or custom timeline views granularity
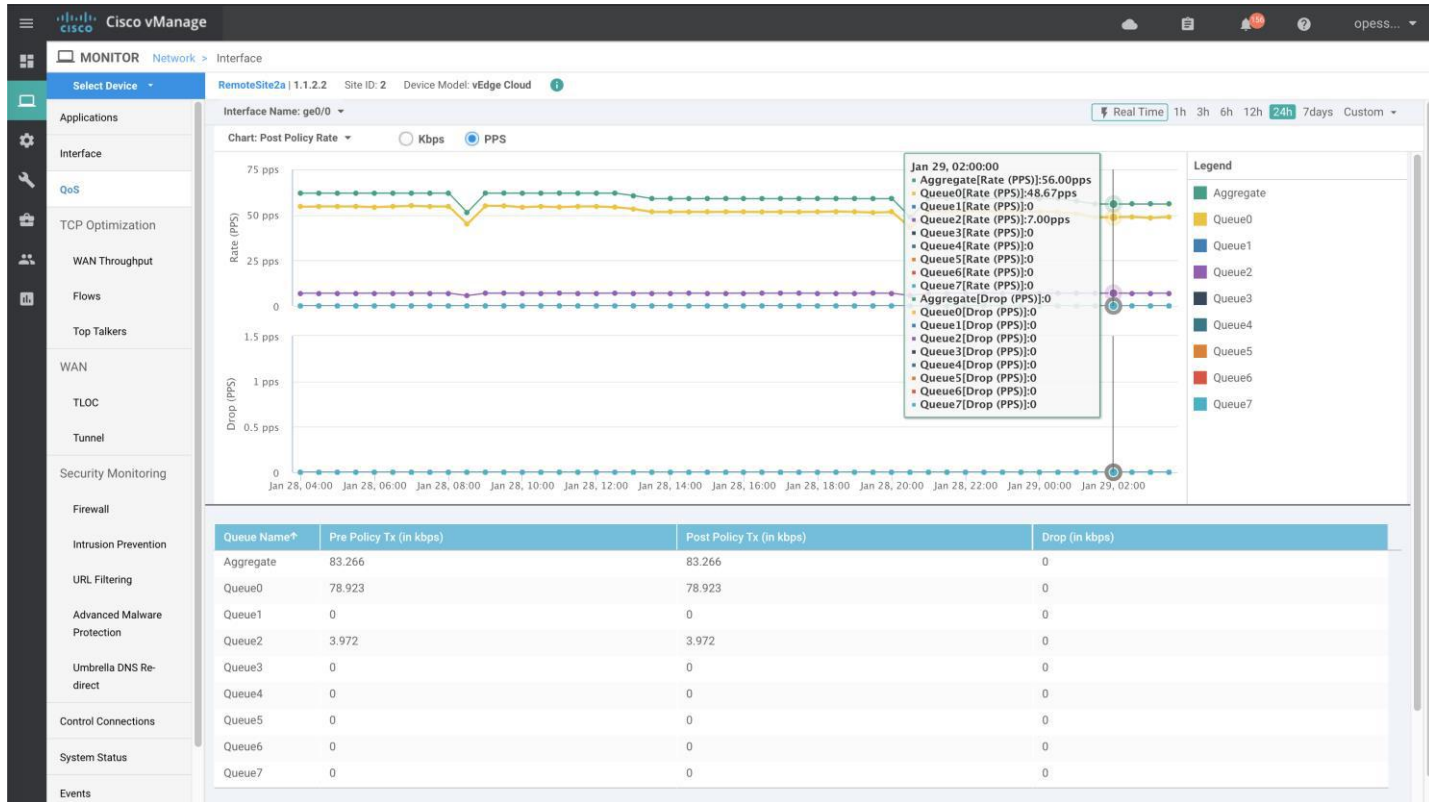
- Views can be zoomed into

Visualizing Application Paths
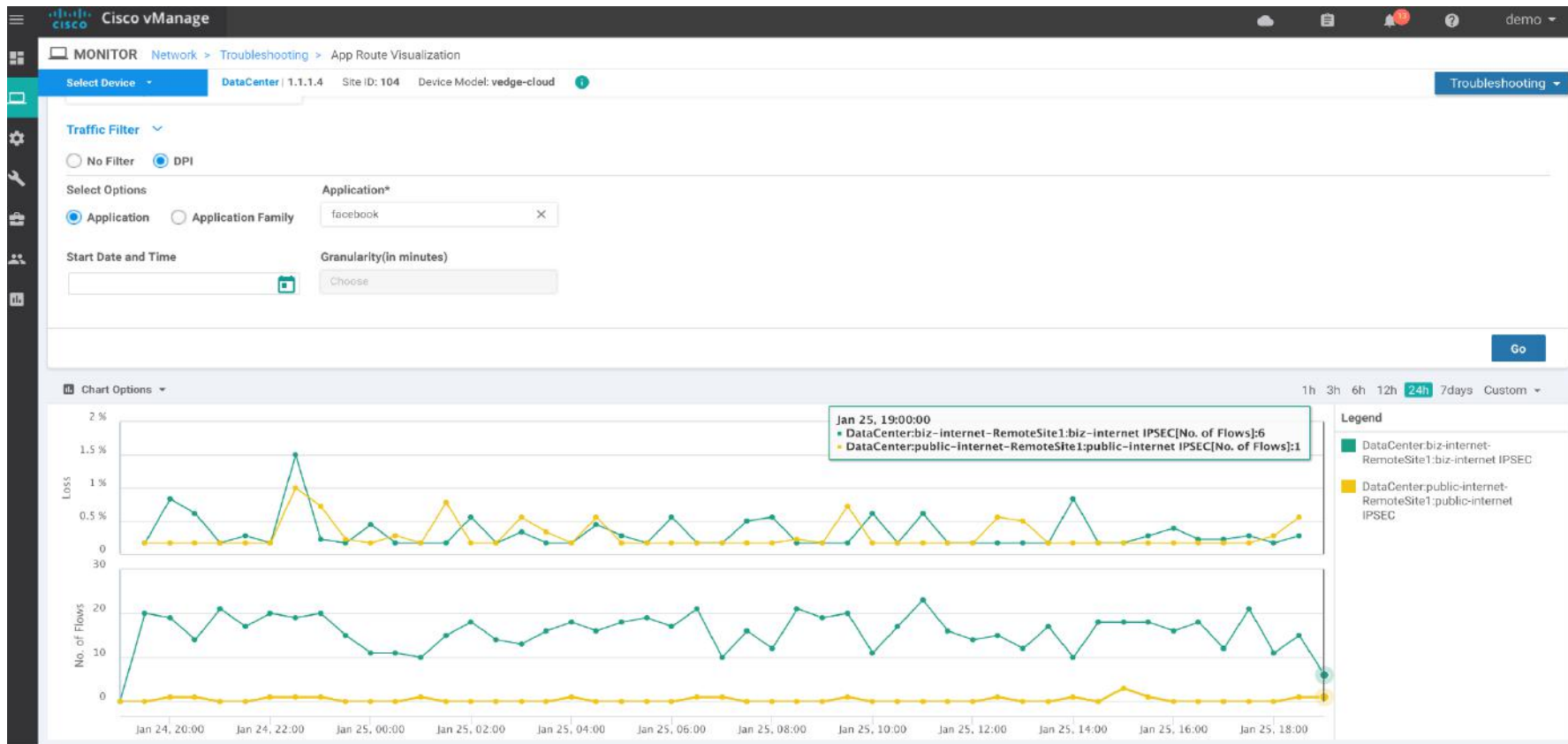
Checking Transport Quality

Checking QoS

Troubleshooting

- Basic connectivity troubleshooting with ping and traceroute from any vEdge in the topology to any destination

- Advance troubleshooting with real-time queries against vEdge routers

- Expert troubleshooting with full featured CLI and Linux bash shell

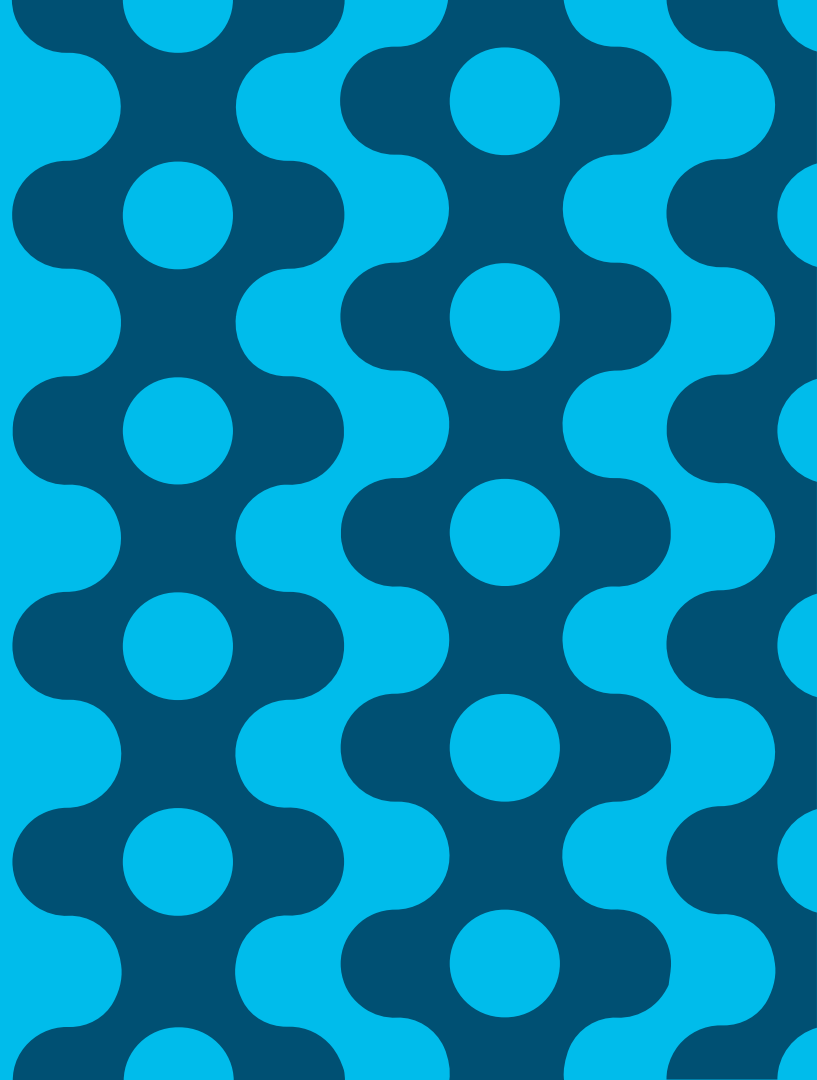- Traffic analysis with synthetic traffic generation to test policies

Conclusion

Benefits of Cisco SD-WAN

Predictable app experience

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 co-location