Quint@sQuinze: SD-WAN Innovations

André Oliveira – andreol@cisco.com

Arquiteto de Soluções SD-WAN LATAM

- May 2021

GSO Go-to-Market Strategy and Operations

The New Normal

Work is hardly about location
in a multi-cloud world

Agenda

1 WAN Disruption

2 Core Innovations

3 MultiCloud

4 SASE

5 User Experience and Analytics

Quiz - Sua empresa ou cliente possui solução WAN baseado em:

- Somente MPLS

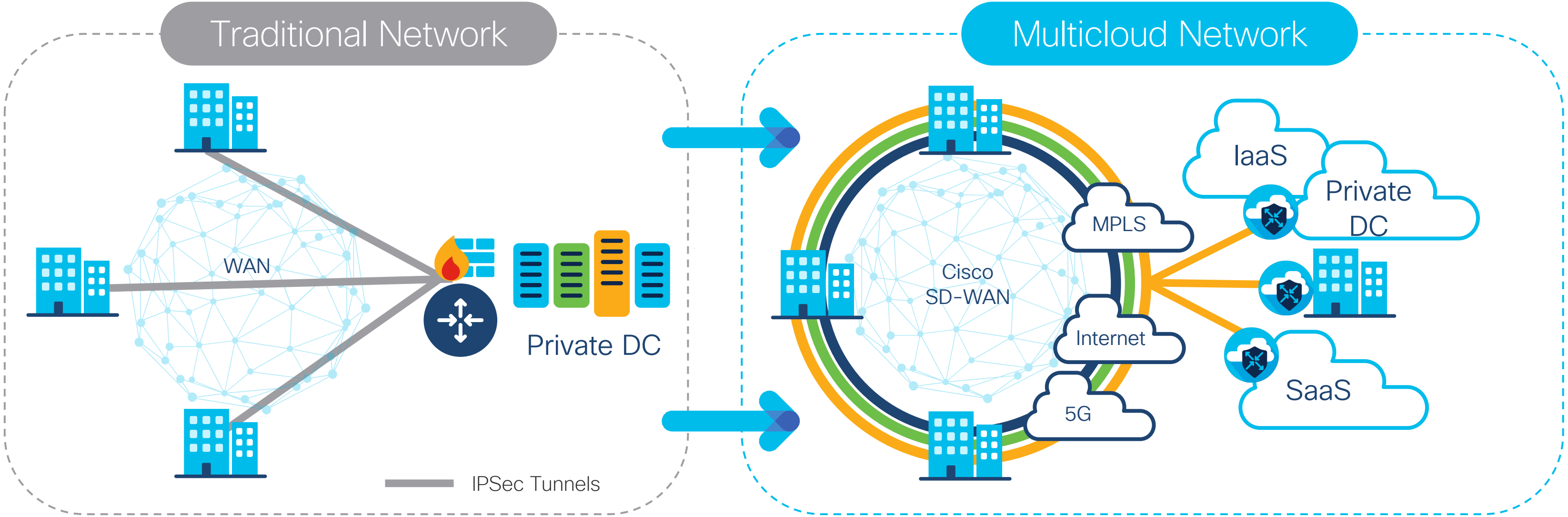
- Somente VPN sobre INTERNET

- MPLS e VPN com chaveamento baseado em status (up/down) do link

- SDWAN com funcionalidades básicas (balanceamento baseado em aplicação origem e destino)

- SDWAN com funcionalidades avançadas (balanceamento com segmentação, cloud on ramp, etc…

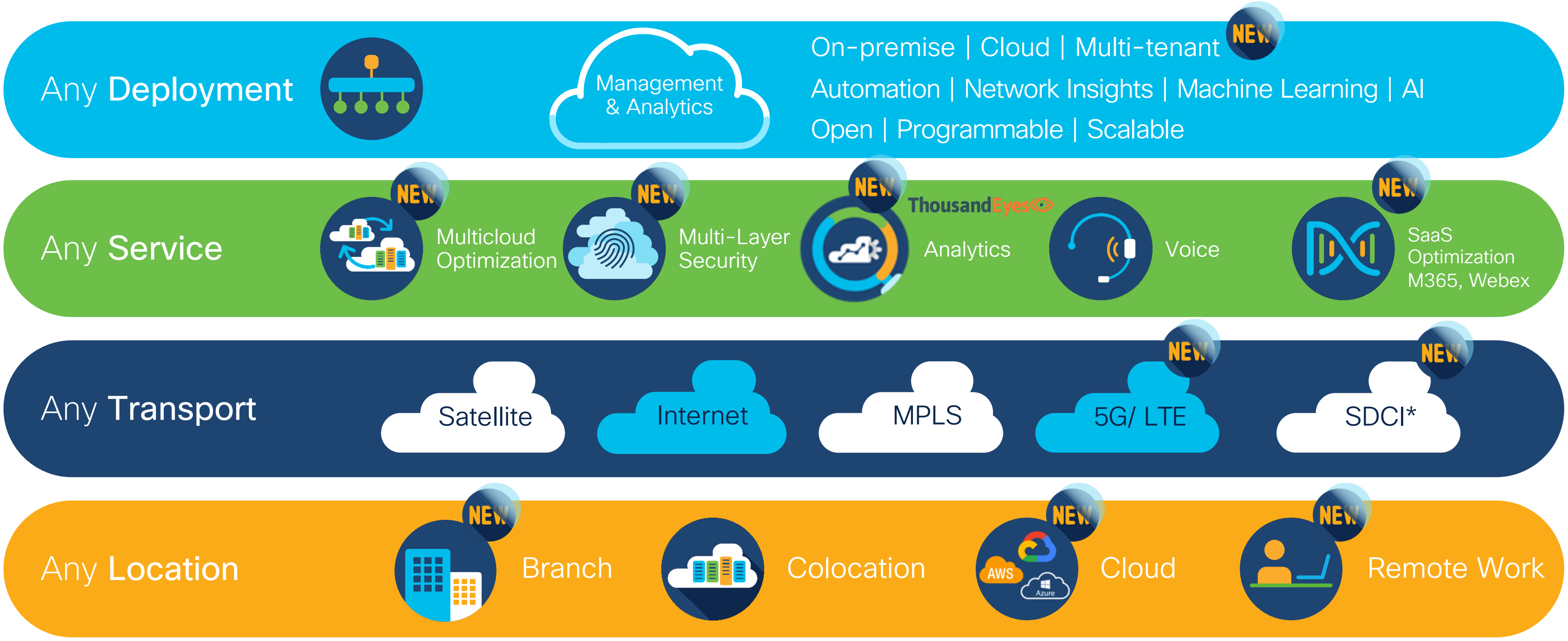
WAN - Disruptions



Multiple WANs to Secure SD-WAN

Secure Multi-Cloud SD-WAN

Cisco’s flexible architecture for Intent-based Networking



Any **Deployment**

Management & Analytics

On-premise | Cloud | Multi-tenant NEW

Automation | Network Insights | Machine Learning | AI

Open | Programmable | Scalable

Any **Service**

NEW Multicloud Optimization

NEW Multi-Layer Security

NEW ThousandEyes Analytics

Voice

NEW SaaS Optimization M365, Webex

Any **Transport**

Satellite

Internet

MPLS

NEW 5G/ LTE

NEW SDCI*

Any **Location**

NEW Branch

Colocation

NEW Cloud

NEW Remote Work

* Software Defined Cloud Interconnect

Recap: where we are taking Cisco SD-WAN next

Summary of Basic SD-WAN Capabilities

Circuit Load Balancing

Direct Internet Access

Centralized Management & Orchestration

Circuit Cost Savings

+

Security

- Holistic security solutions that evolve with customer's overtime
- Granular segmentation w/ Identity
- Cisco and 3rd party support

Multi Cloud

- Network & Security Services in partnership with Cloud/SaaS, Telco/SP
- End-to-End automation with policy control and observability
- Pluggable API Framework

Analytics & Assurance

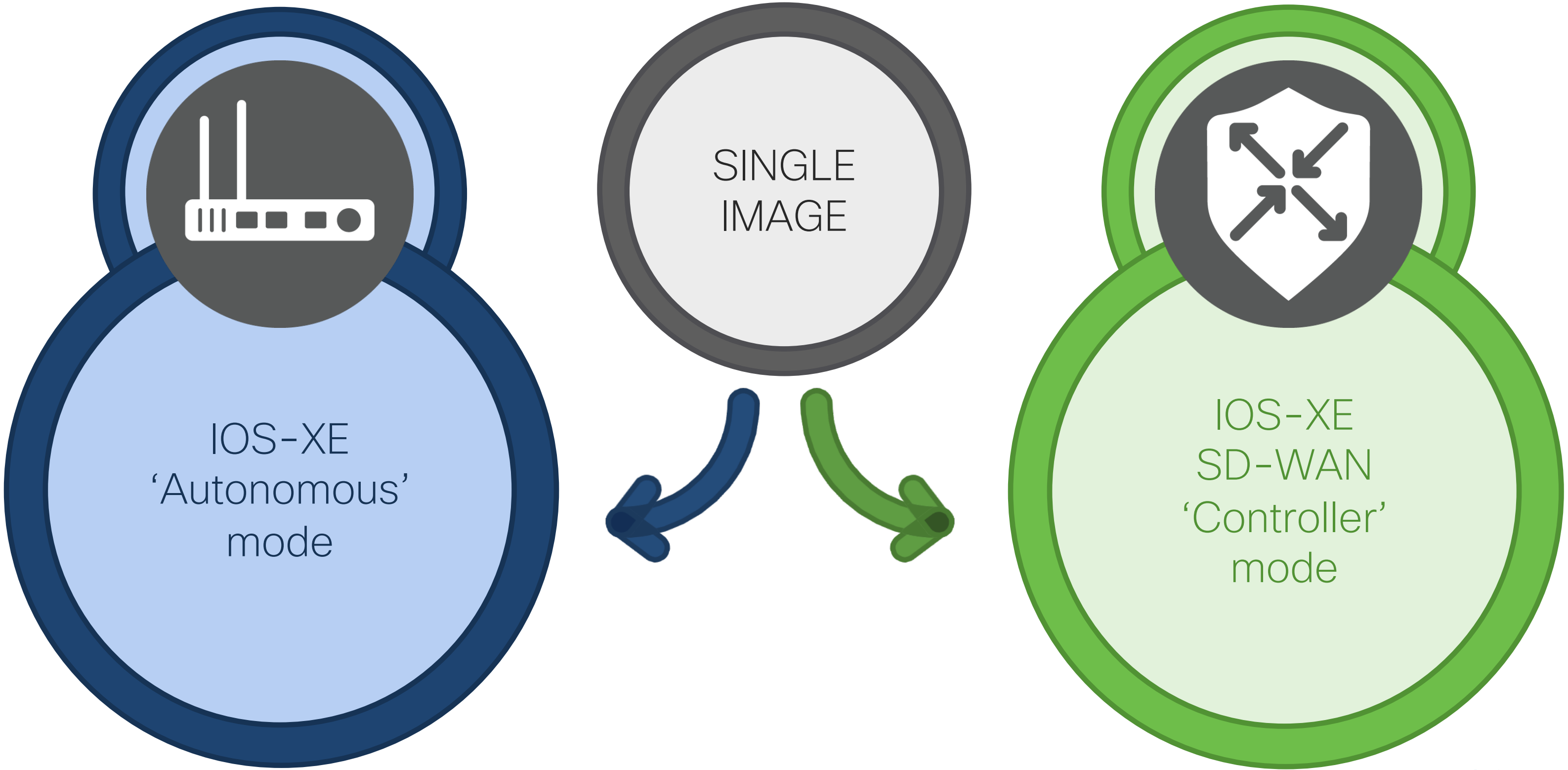
- End-to-end visibility from the user to cloud
- AI/ML to deliver service assurance and self-healing resiliency

Flexible consumption and deployment

Enhanced User Experience

Core Innovations

Single Image for IOS-XE and IOS-XE SD-WAN



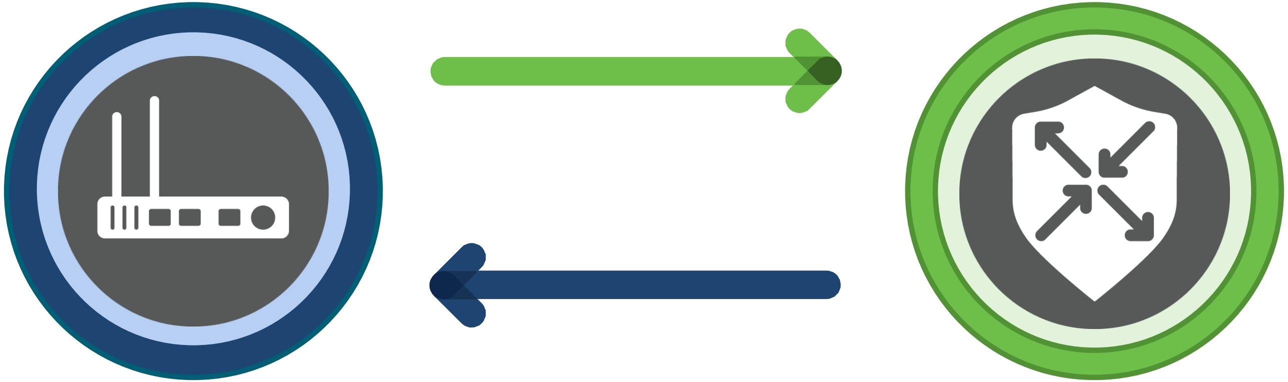
SINGLE IMAGE

IOS-XE ‘Autonomous’ mode

IOS-XE SD-WAN ‘Controller’ mode

Operational Mode Change

```
Router# controller-mode ?
  disable   controller-mode disable
  enable    controller-mode enable
  reset     controller-mode reset
```



Change to Autonomous Mode

- Config lost, device in day-0

Change to Controller Mode

- Config lost, device in day-0

Quick Look: Service Side NAT

vEdge ✓

cEdge ✓

Problem

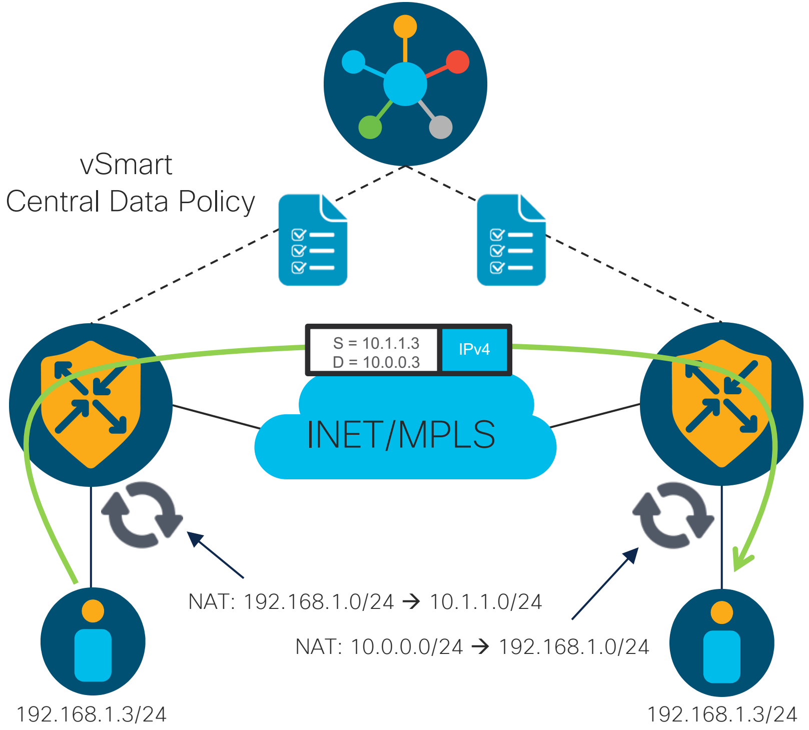
Address conservation, mergers/acquisitions and reducing operational overhead when resources shift around the network all bring in the potential for overlapping address ranges. How do you maintain connectivity to these resources?

Solution

SD-WAN v20.3 and IOS-XE v17.3 now support Service Side NAT wherein overlapping address spaces can be NAT'd to globally unique address pools or static assignments.

Caveats / Prerequisites

IPv4 only, no inter-VPN support, specific workflow must be followed (see TDM slides)



Quick Look: Dynamic On-Demand Tunnels

vEdge ✓

cEdge ✓

Problem

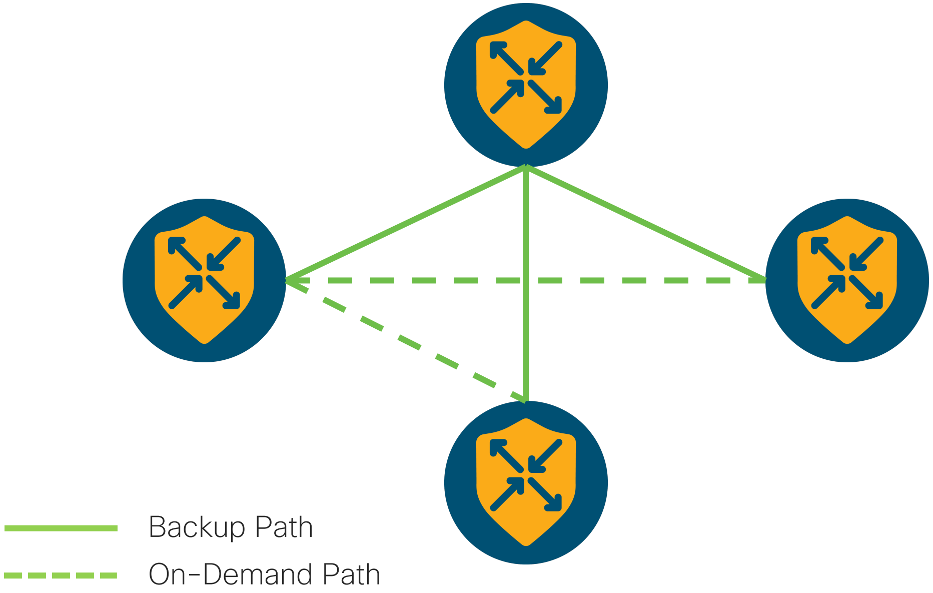
By default, Cisco SD-WAN operates in full-mesh. While topology modification is possible, full-mesh carries a huge computational burden on branch resources and, therefore, becomes difficult to scale. Enterprise customers need full-mesh connectivity, but also need a way to offset the resource burden that full-mesh generally entails.

Solution

SD-WAN v20.3 / 17.3 now support Dynamic On-Demand Tunneling. Branch routers will maintain an “always-on” tunnel to a hub location, then dynamically build site-to-site tunnels, where necessary.

Caveats / Prerequisites

Spoke locations must receive TLOC and vRoute of remote, must have backup path and Service TE set (see supporting slides)



Quick Look: DIA Tracker Support

vEdge ✓

cEdge ✓

Problem

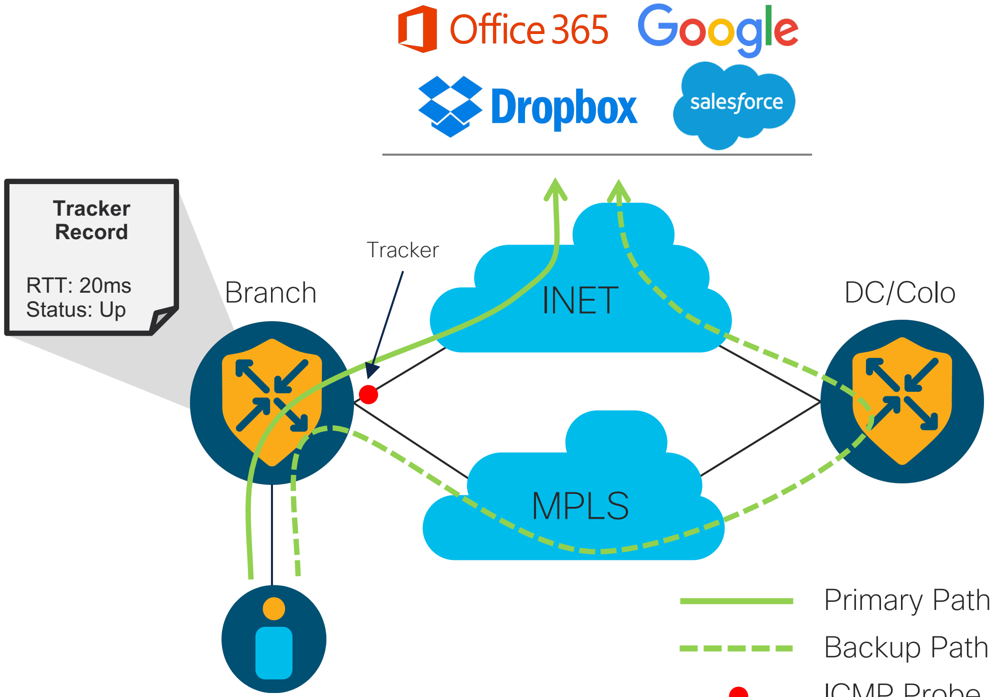
Enterprises that adopt a Direct Internet Access (DIA) model have limited visibility into the status of Internet-facing interface(s). Hence, in brownout conditions, Internet traffic forwarded to this interface would be silently dropped.

Solution

SD-WAN v20.3 and IOS-XE v17.3 now support SLA tracking on both vEdge and cEdge to probe the Internet (DIA) interface for reachability. Should the primary interface be degraded, the router can invoke a backup path.

Caveats / Prerequisites

No Dialer support, NAT-fallback is not supported (target 17.4), refer to TDM slides



Application Optimization

Per-Class BFD Probing for AAR

vEdge ✓

cEdge ✓

Problem

Currently, AAR reacts on probing done based on BFD probes marked with DSCP 48. Service Provider QoS treats DSCP 48 as high priority control traffic, which is different than actual data traffic tagged with different DSCP markings. This causes inaccurate BFD probing results and, hence, AAR cannot respond accordingly.

Solution

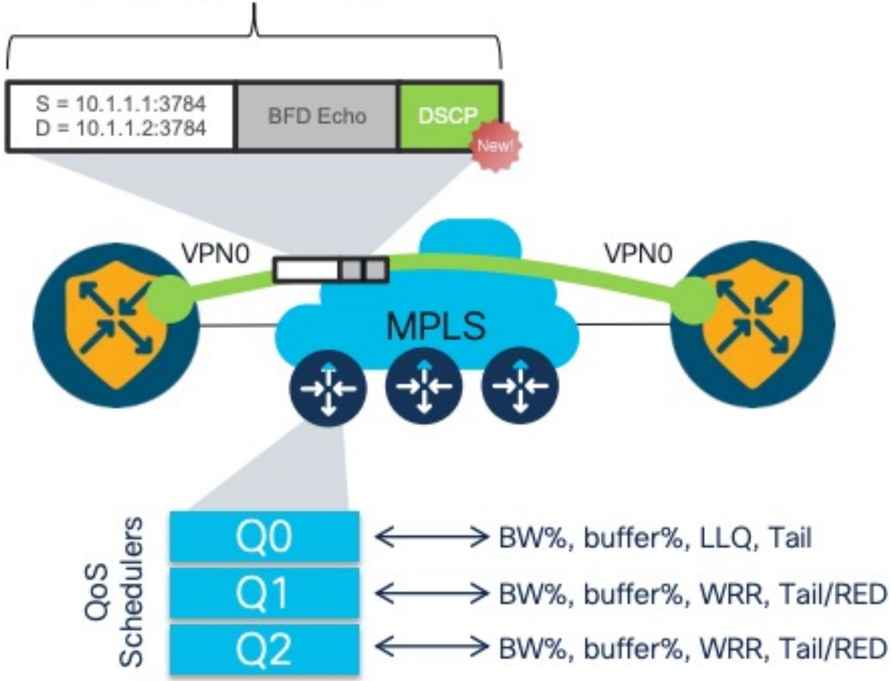
SD-WAN v20.4 / 17.4 introduces capability to customize BFD probes with different DSCP markings. This will help reflect the actual treatment of a user's packet and will allow a more accurate reading of loss/latency/jitter. Consequently, AAR can now route traffic based on more accurate measurements

Caveats / Prerequisites

None

Bi-directional Forwarding Detection (BFD)

- Utilizes UDP port 3784
- Measures Loss, Latency and Jitter
- Each BFD packet is ~100 bytes
- Configurable DSCP value



S = 10.1.1.1:3784
D = 10.1.1.2:3784

BFD Echo

DSCP

New!

VPN0

MPLS

VPN0

QoS Schedulers

Q0 ⟷ BW%, buffer%, LLQ, Tail

Q1 ⟷ BW%, buffer%, WRR, Tail/RED

Q2 ⟷ BW%, buffer%, WRR, Tail/RED

Application Aware Routing- Best of worst Tunnel Selection

vEdge ✓

cEdge ✓

Problem

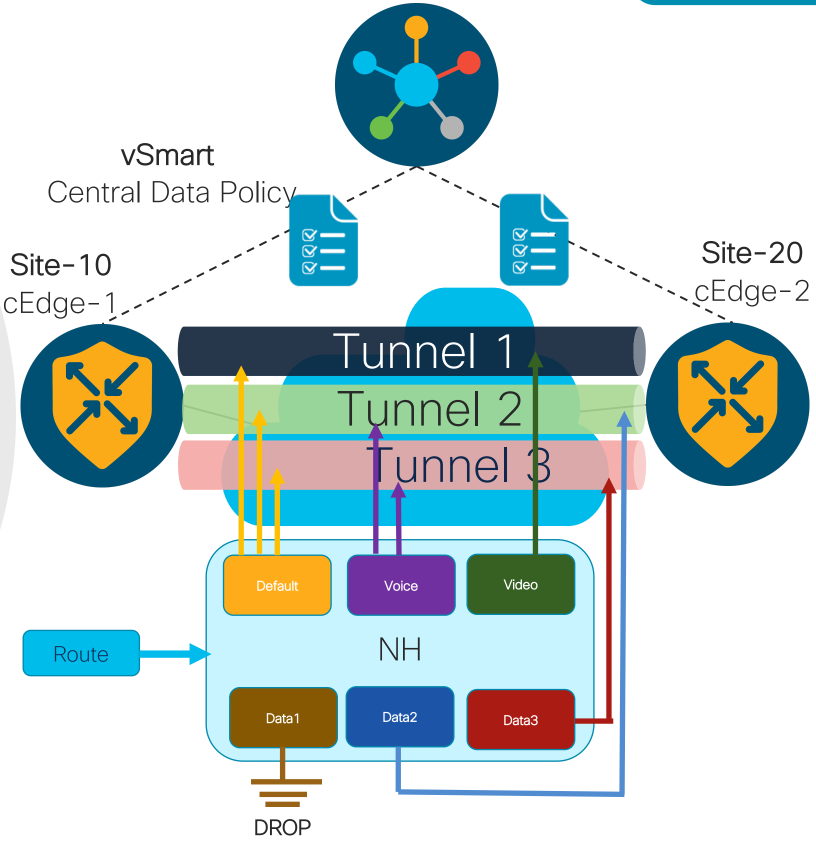
- Application Aware Routing Policy (AAR) matches the data traffic and selects the path based on configured action of the sequence.
- Currently, when configured SLA class for a given sequence doesn't match, data traffic is sent using configured **backup-preferred-color**.
- If backup-preferred-color is not configured, traffic is load balanced on all available tunnels present in the default SLA class.
- This results in undesired user experience especially for traffic like video and voice which are loss/latency sensitive.

Solution

- A new action "**fallback-to-best-path**" has been introduced from 17.5 IOS-XE version and 20.5 for vEdge platforms.
- This aids users by providing an option to define additional criteria's using "**fallback-best-tunnel criteria**" command under each SLA class so that the best path/color out of the available worst path/tunnel is selected **when SLA is not met**.
- This will ensure better user experience than natively forwarding the traffic through ECMP path where in traffic may end up flowing through a tunnel which is under-performing.

Caveats / Prerequisites

none



Quick Look: Multicast AAR

vEdge ✗

cEdge ✓

Problem

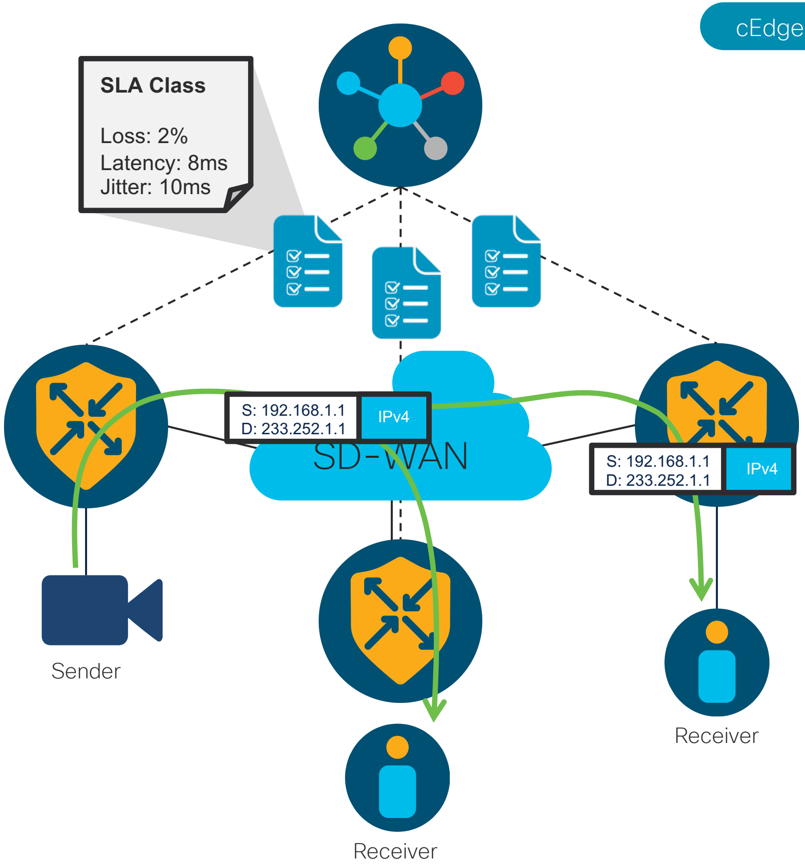
Currently, SD-WAN intelligent routing is bound to unicast flows. As multicast becomes more and more prevalent for content delivery, organizations are seeking to extend traffic routing intelligence to these flows as well.

Solution

SD-WAN v20.3 / 17.3 Application Aware Routing now supports multicast streams within policy.

Caveats / Prerequisites

cEdge only, IPv4 only, S/D IP + Protocol match only, no DPI/application match, no DSCP match



Quick Look: Custom Application Support

vEdge ✗

cEdge ✓

Problem

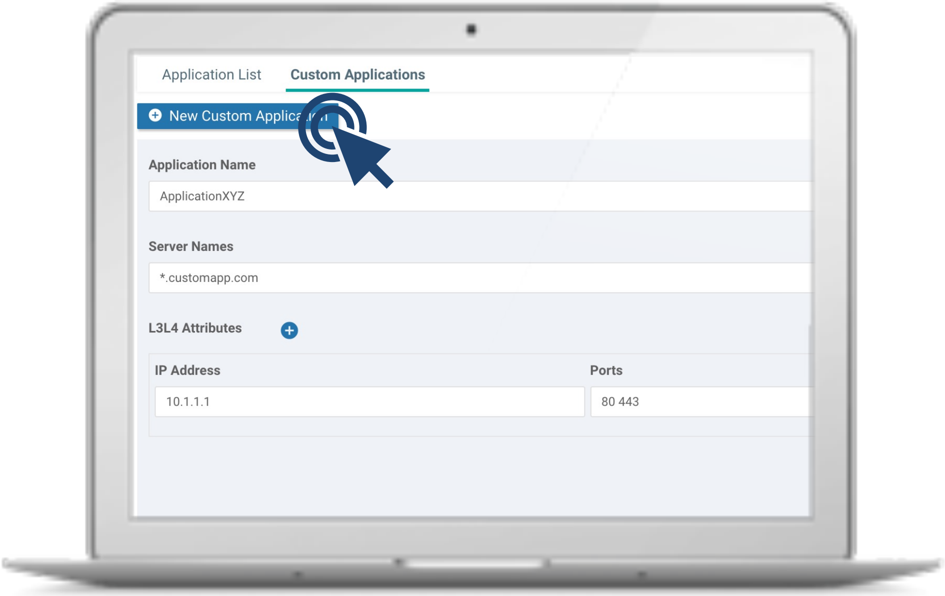
Application Recognition engines, such as NBAR2, often lack recognition for homegrown or less popular applications. As such, defining traffic policy can become challenging and cumbersome when customers need to take action against or monitor this traffic.

Solution

SD-WAN v20.3 and IOS-XE v17.3 now support Custom Application definition via NBAR2. By leveraging customer-defined signatures, traffic policy configuration and application monitoring becomes substantially easier.

Caveats / Prerequisites

cEdge only, IPv4 only, flow direction is unsupported, DSCP is unsupported, must have policy enabled



Application Name: ApplicationXYZ

Server Names: *.customapp.com

L3L4 Attributes

IP Address	Ports
10.1.1.1	80 443

Quick Look: Adaptive Quality of Service

vEdge ✓
cEdge ✓

Problem

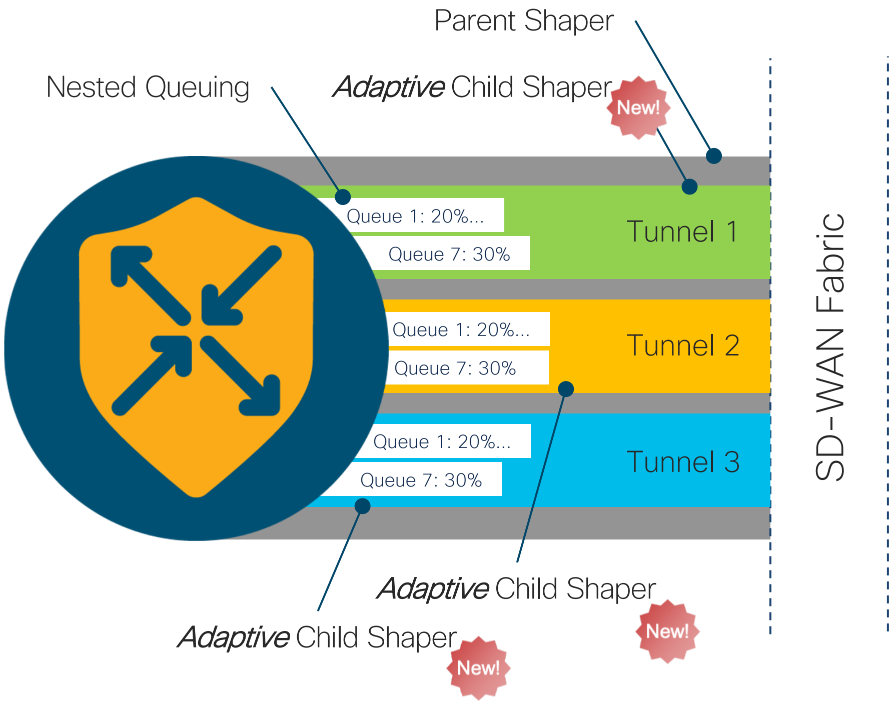
Per-Tunnel QoS, introduced in v20.1 / 17.2 of SD-WAN, allows for much more efficient use of bandwidth by allowing a Hub site to reduce the sending speed of data so as not to overwhelm the remote spoke. Unfortunately, this shaping mechanism is static and may not reflect the actual bandwidth available at the remote spoke.

Solution

SD-WAN v20.3 / 17.3 introduces support for Adaptive Quality of Service wherein the Spoke location will advertise its *current* bandwidth capability. The Hub sites can then dynamically adjust their shaping mechanisms to accommodate. In addition, the spoke can also adjust its upstream shaper.

Caveats / Prerequisites

See Per Tunnel QoS caveats



Multi-Cloud Optimizations

Predictable Application Experience

Quiz - Sua empresa ou cliente possui estratégia de adotar Arquitetura Multi-CLoud, quais provedores de Cloud?

- AWS
- Azure
- Google
- AWS, Azure
- AWS, Azure, Google

A Hybrid Multi-Cloud environment is the new norm

Enterprises are adopting cloud; forecasts show that investments will increase

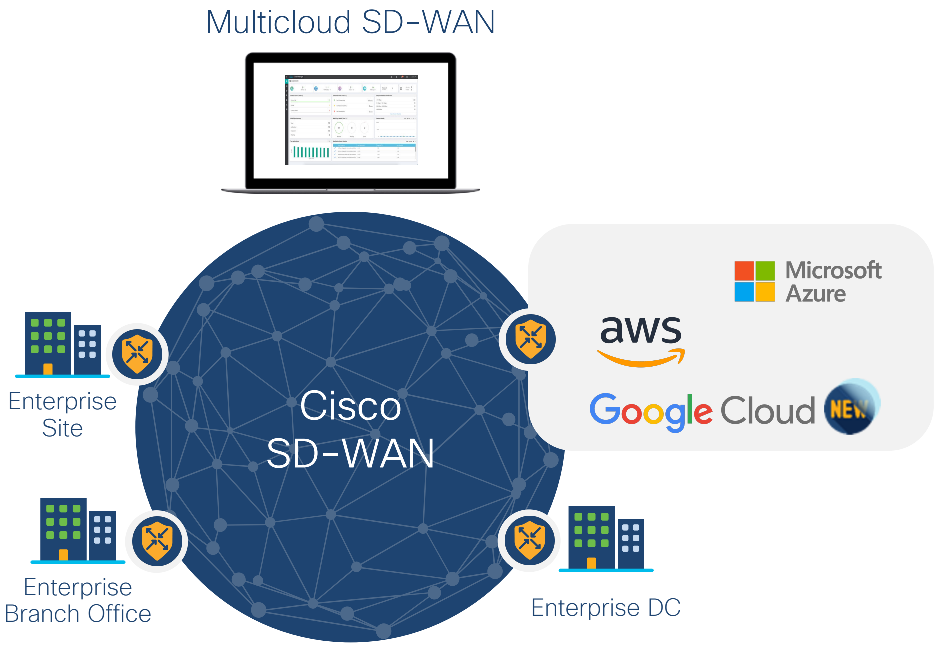
93% of enterprises embraced multi-cloud strategy

IaaS spend is projected to grow by 24% CAGR to reach $74B by 2022

57% of enterprise workloads will be deployed in public clouds in 12 months

Cisco SD-WAN Cloud OnRamp for Multicloud

Automate SD-WAN extension to IaaS via vManage



Greater Automation

Automate SD-WAN extension to the cloud

Normalized Multicloud Experience

Consistent UI and workflow in vManage

Ease of management

Orchestrate both Cisco and cloud provider networking resources via vManage

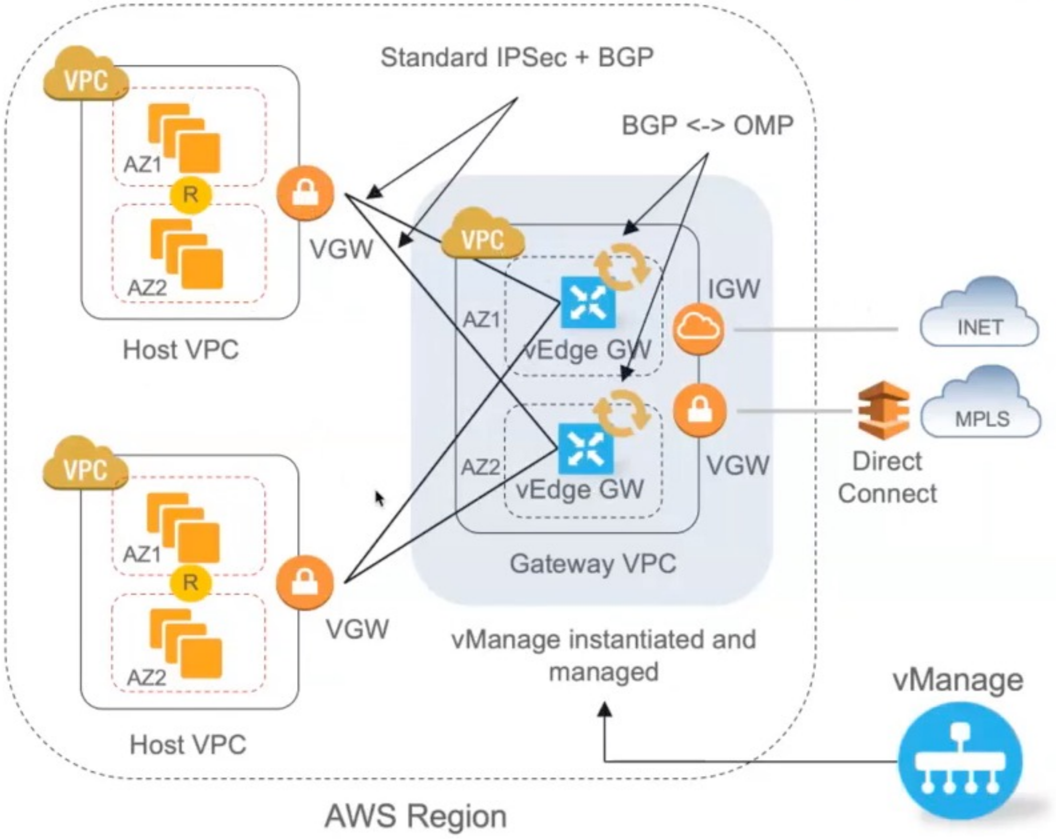
Unified Security Policies

Extend segmentation policy into cloud

Simplifies SD-WAN extension to Multicloud for an optimal cloud workloads experience

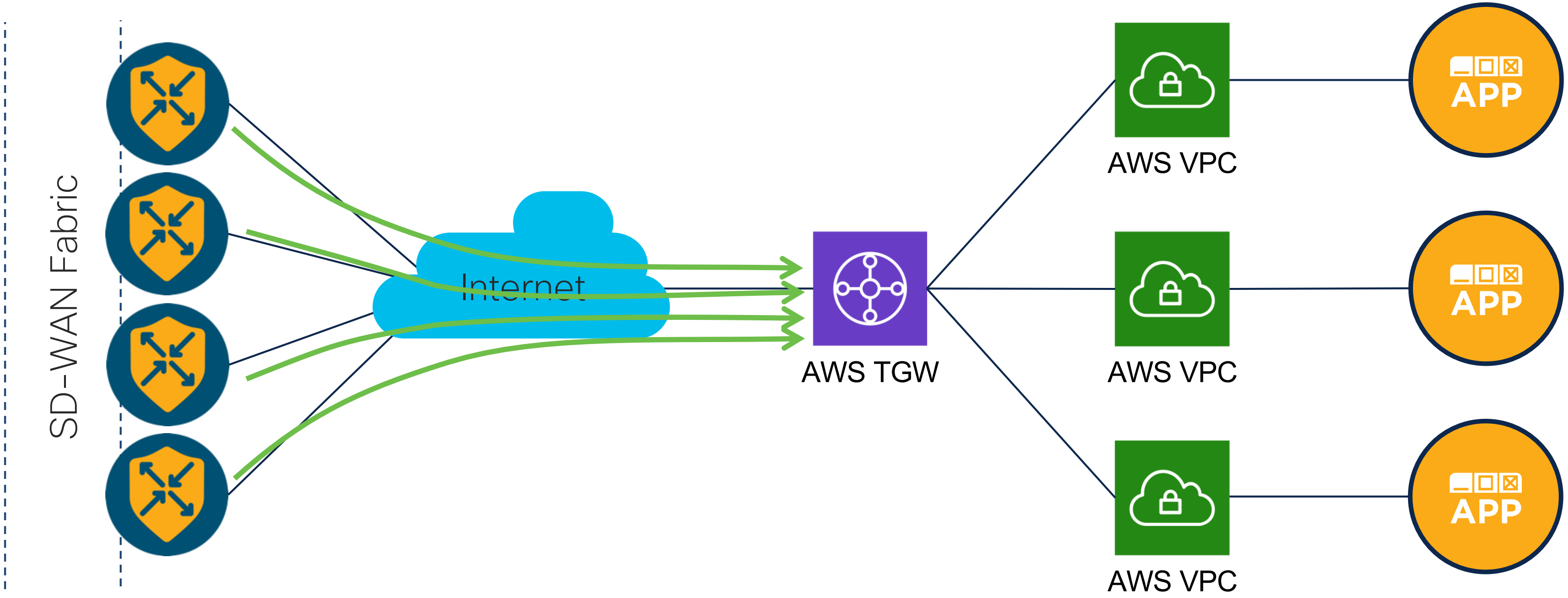
Cloud OnRamp for IaaS

Use Case 1 - Gateway VPC (VNET)



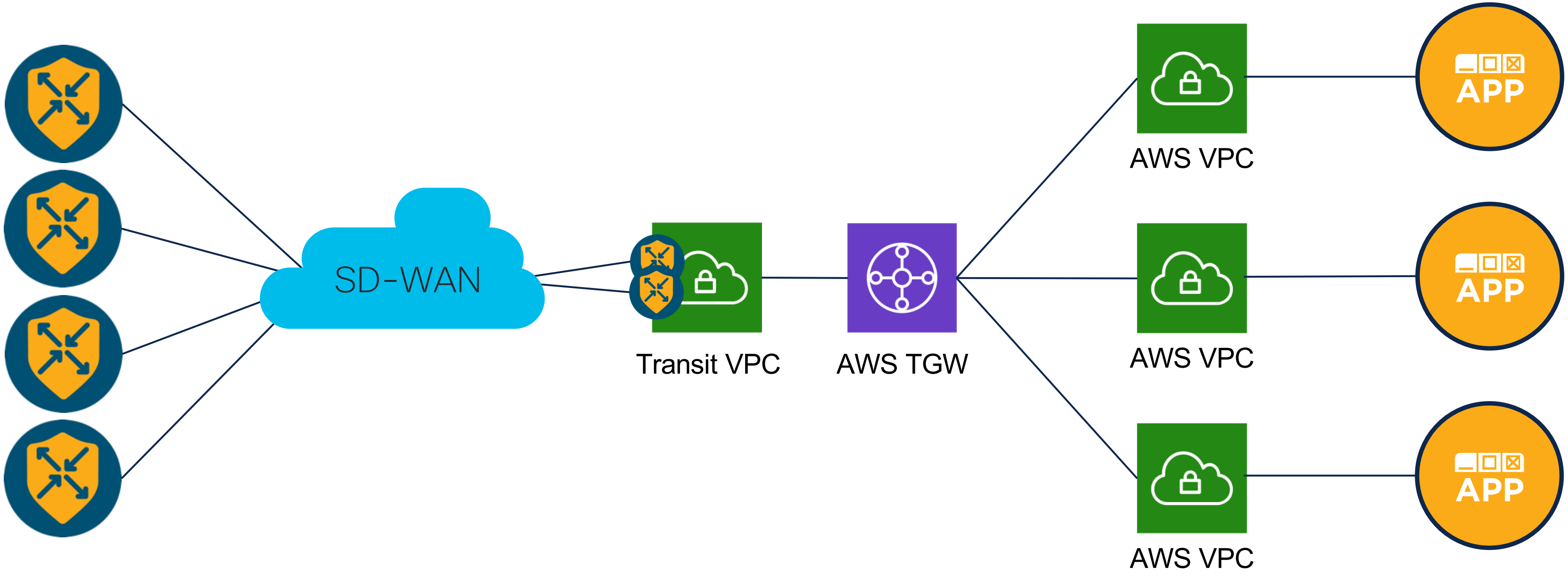
- Fully automated through vManage wizard
- Greatly simplifies brownfield integration
  - No changes are required on host VPCs
- Multipathing, segmentation, QoS
- Fast failover
  - Speed of BGP convergence

Use-Case 2: Traditional IPsec to TGW



Automated IPsec tunneling to TGW: Easily integrate existing TGW into SD-WAN fabric.

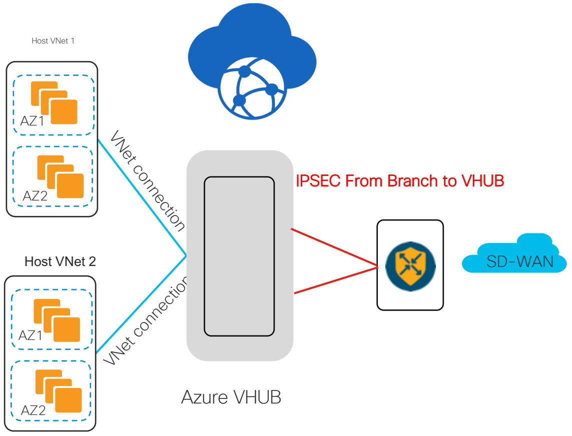
Use-Case 3: Transit VPC with TGW



- Automate and extend SD-WAN policy, structure, and (most importantly) visibility into the AWS cloud
- Operationally easier since SD-WAN can be leveraged for HA and dynamic routing
- Standard IPsec + BGP from Transit VPC to Transit Gateway (limited to 1.25Gb/ps)

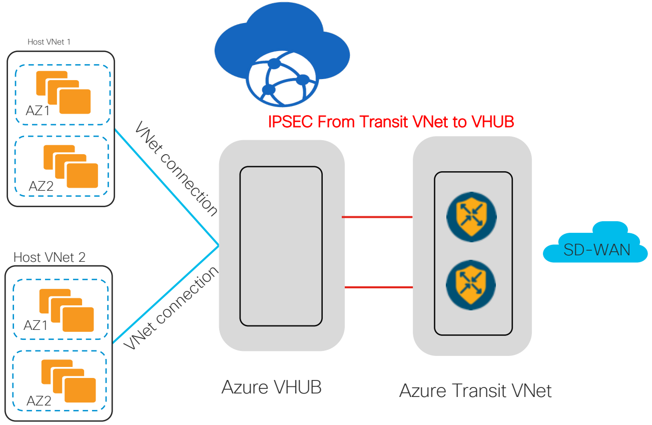
SD-WAN to VWAN connectivity models

Direct Interconnect



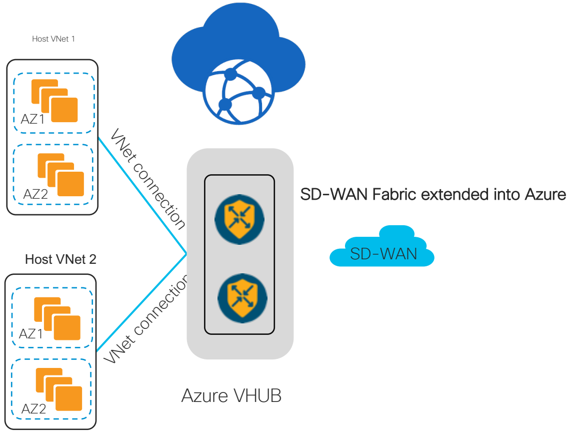
- One or more branches establish IPSEC tunnels to Azure VHUB
- Sub-optimal path and branches need to handle more traffic
- Does not extend SD-WAN fabric to Azure
- Manual configuration needed

Indirect Interconnect Model



- Need IPSEC Tunnel from Transit VNet to VHUB
- Extra hop
- Extra cost and operational complexity
- Manual configuration needed

Direct with NVA-in-vWAN-hub

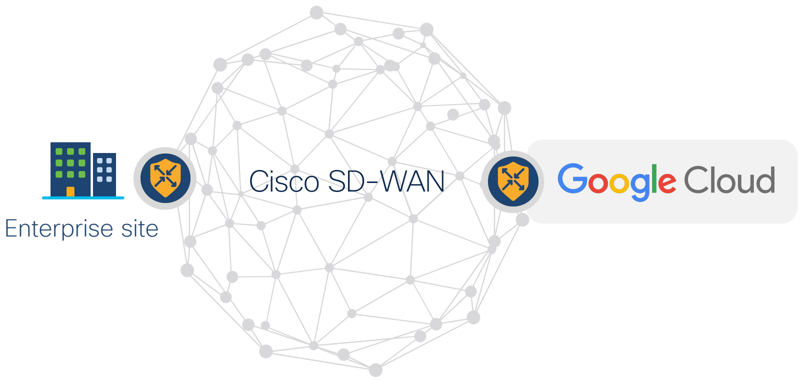


- Dynamic routing between SD-WAN routers and VHUB
- HA Pair of routers terminating SD-WAN IPSEC tunnels
- SD-WAN Fabric and policies extended into Azure
- Automated with vManage

Cisco SD-WAN Cloud Hub with Google Cloud

Site-to-Cloud

SD-WAN fabric **to** Google Cloud workloads



Enterprise site

Cisco SD-WAN

Google Cloud

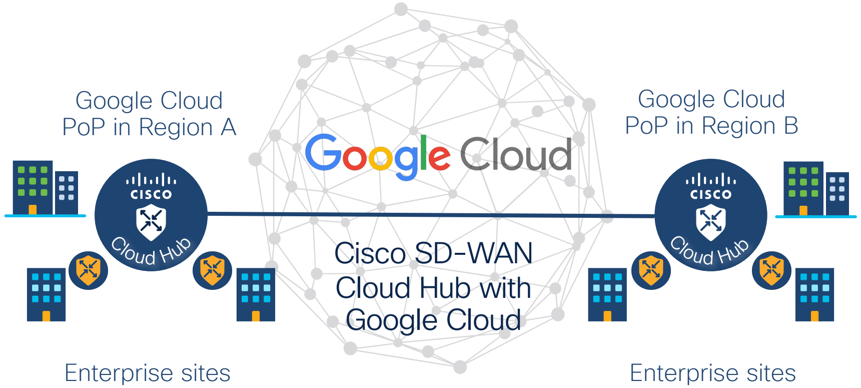
Simple

Automated

Secure

Site-to-Site

SD-WAN fabric **across** Google Cloud global network



Google Cloud PoP in Region A

Google Cloud PoP in Region B

Google Cloud

cisco Cloud Hub

cisco Cloud Hub

Cisco SD-WAN Cloud Hub with Google Cloud

Enterprise sites

Enterprise sites

On-Demand

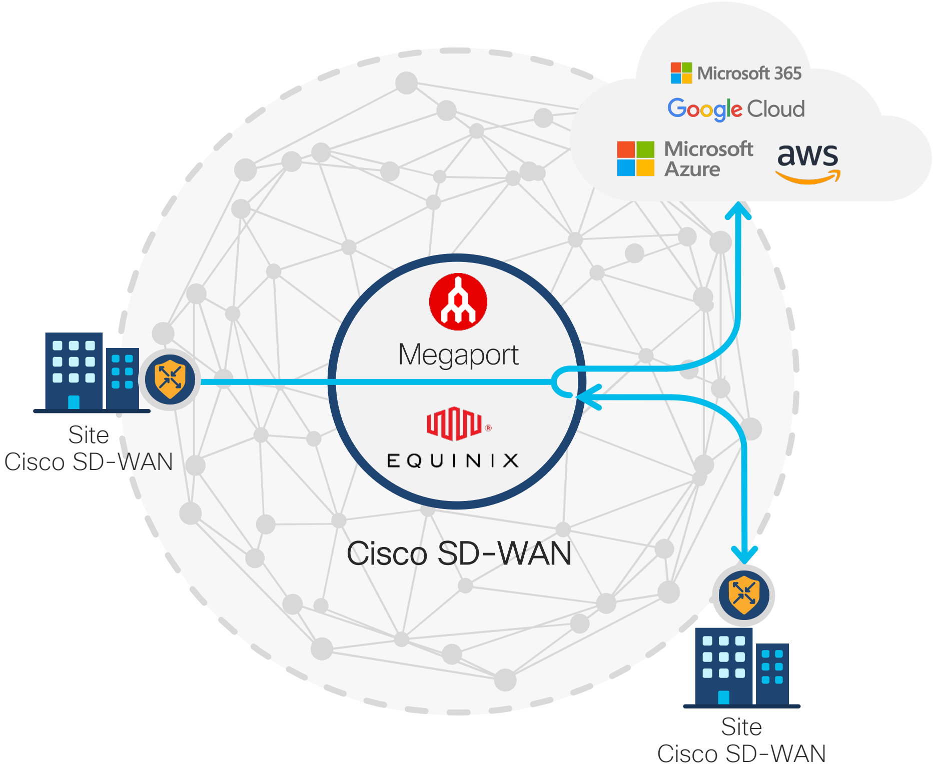
High Performance

Global Connectivity

First and only SD-WAN vendor integrating with Google Network Connectivity Center

Cisco SD-WAN Cloud Interconnect with Megaport & Equinix

BYO SDCI - Site to Cloud and Site to Site



Full stack Network Automation
Orchestrate SD-WAN overlay and SDCI underlay with point and click automation from vManage

Secure Private Backbone
End-to-end visibility, security, and policy over a private backbone with worldwide presence

On-demand Connectivity
Increase/decrease capacity to suit dynamic requirements of multicloud connectivity

Cloud-like Consumption Model
Pay for what you need with flexible, bandwidth-based consumption model

SD-WAN Fabric with Programmable Cloud Interconnects

Cloud OnRamp for SaaS

Enhanced Office365 Support

Problem

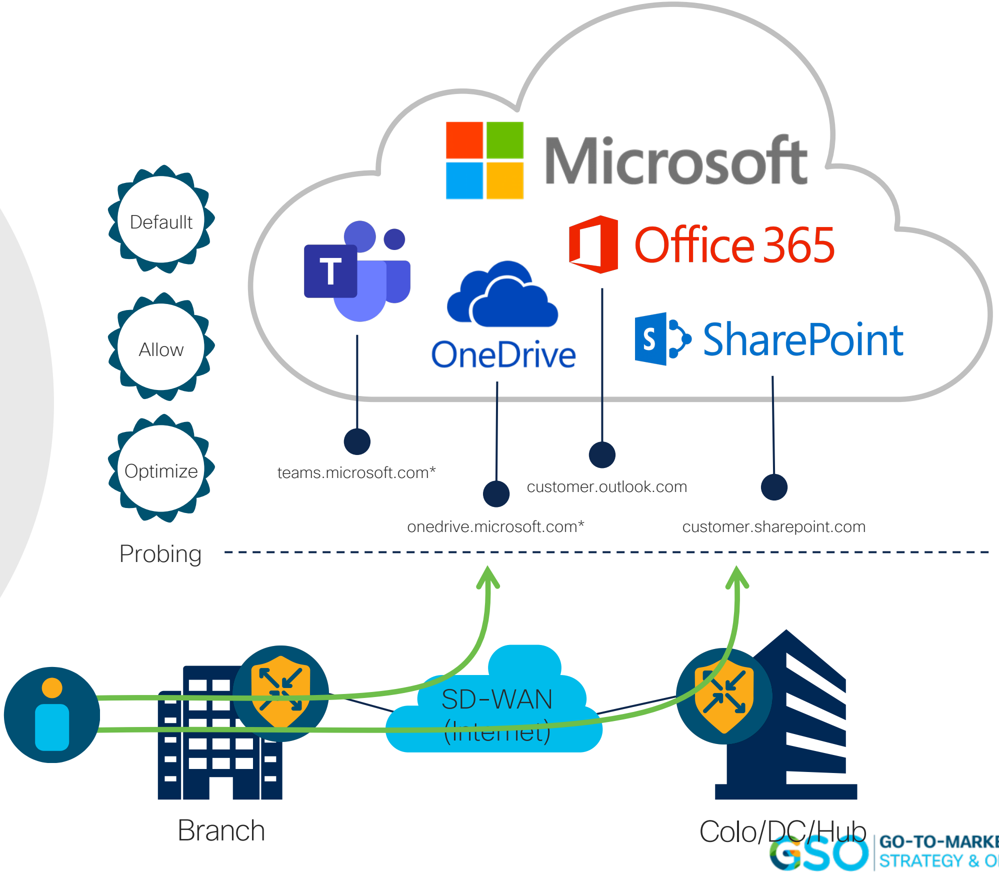
The current implementation of Cloud onRamp for SaaS (O365) does not differentiate between Office365 applications – such as Teams, Sharepoint, Mail, etc. Hence, Cisco SD-WAN cannot offer differentiated service levels for these applications.

Solution

Cisco has partnered with Microsoft to enhance the Office365 application experience for users. In short, Microsoft now publishes distinct URLs for various applications. Cloud onRamp for SaaS can then probe these URLs individually to optimize per application. More importantly, these URLs also help establish a precedence to the traffic (such as Teams Audio requiring priority treatment). Cisco is the first SD-WAN vendor to offer intelligent routing by utilizing metrics from the cloud provider.

Caveats / Prerequisites

None



SD-WAN Security

Control Your SASE Journey

Quiz -Sua empresa ou cliente possui a Estratégia de adotar SD-WAN com SASE – Secure Access Service Edge ?

Até 1 ano

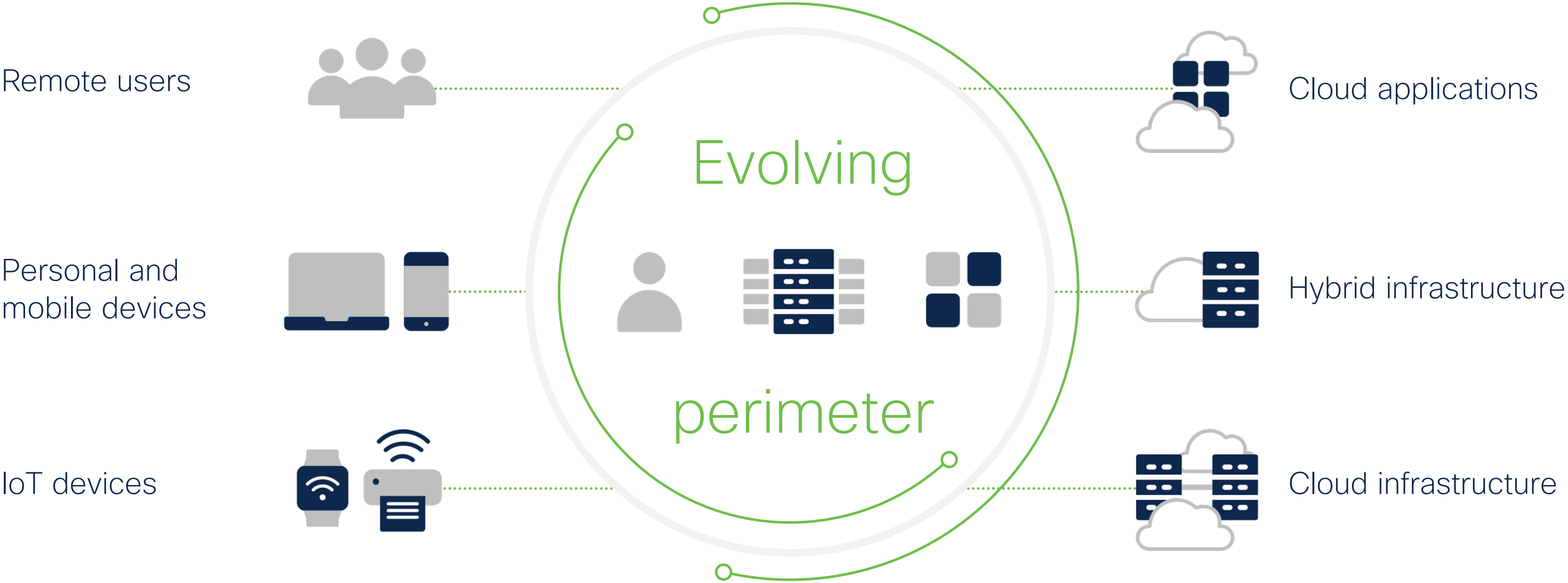
Até 2 anos

Até 3 anos

Sem previsão

Shift in IT landscape

Users, devices, and apps are everywhere



Remote users

Personal and mobile devices

IoT devices

Evolving perimeter

Cloud applications

Hybrid infrastructure

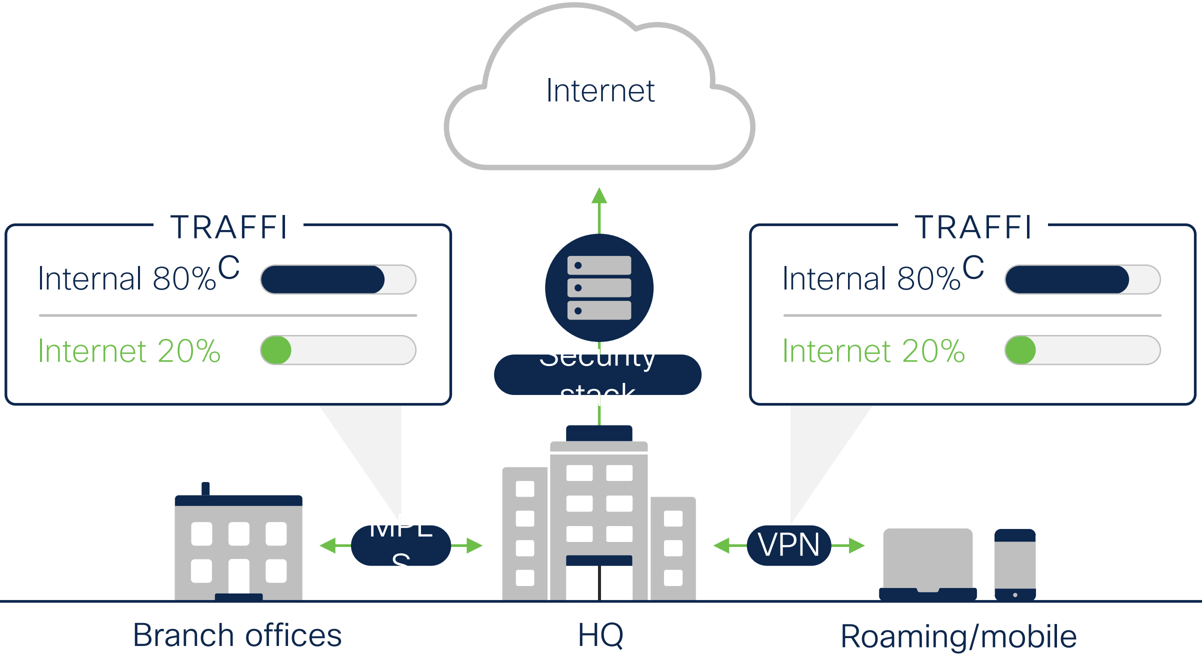
Cloud infrastructure

Historic traffic flows (change the icons color)

Led to the age of perimeter-based security and networking

Network
Centralized

Security
Single, on-premise security stack



Gartner

*"The legacy "data center as the center of universe" network and network security architecture is **obsolete** and has become a inhibitor to the needs of digital business".*

Changes in the types of traffic and destinations

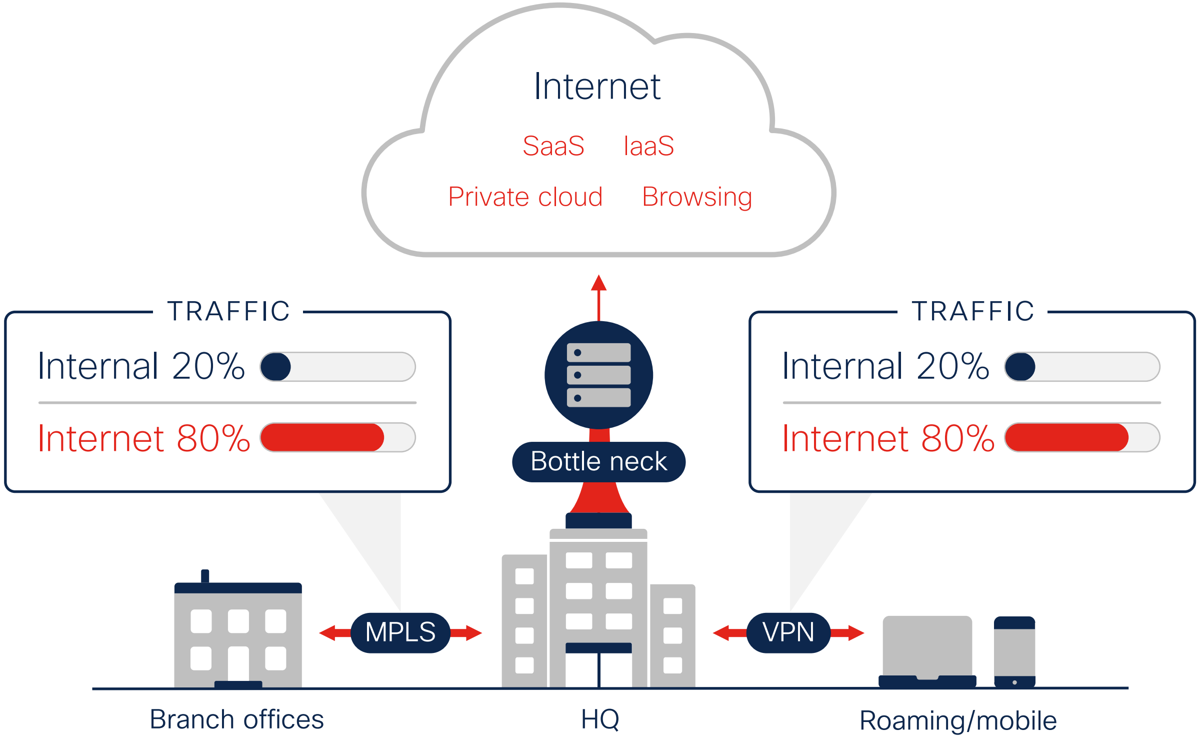
Have inverted the traffic model

Problems:

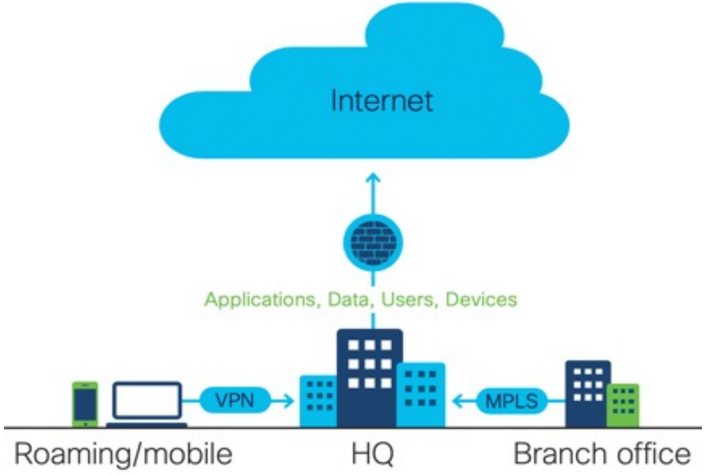
- Costs
- Performance
- # Tools/vendors
- Integrations
- Maintenance

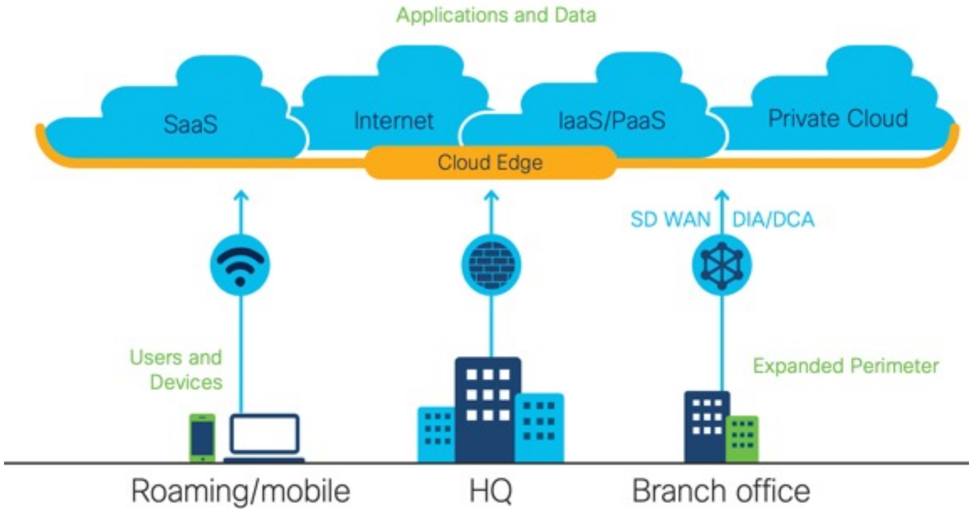
Data Center Backhaul

- Increased App Latency
- Unpredictable User Experience



Cloud Driving Major Network Architecture Shift





Legacy

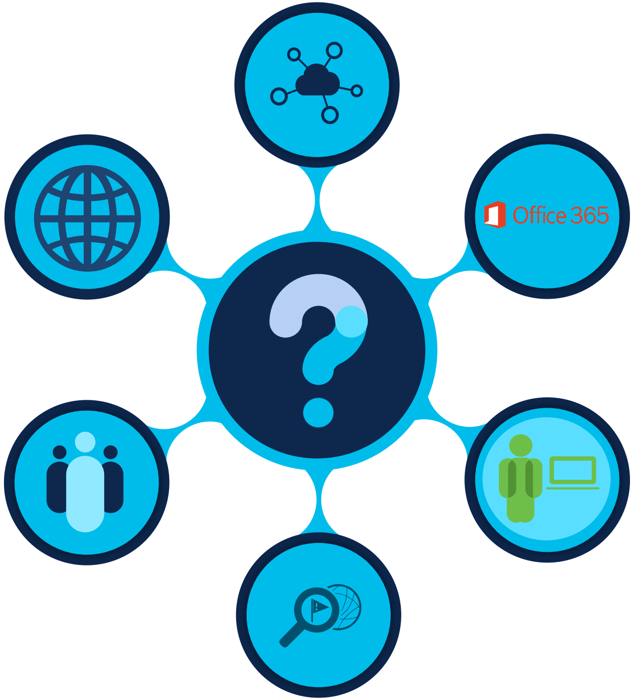
Hub & Spoke Architecture with on-prem appliances

Today & Future

Leading Cloud Edge essential to delivering Networking & Security capabilities in the cloud

Security Challenges

What's top of mind for our Customers ?



DIA

Secure & operate traffic

SASE

Single Pane of Glass
for Networking and Security

Office 365

0365 is demanding
DIA/ Express Route

Segmentation

Isolate my IoT, CCTV,
PoS and other traffic flows

User/Device Identity

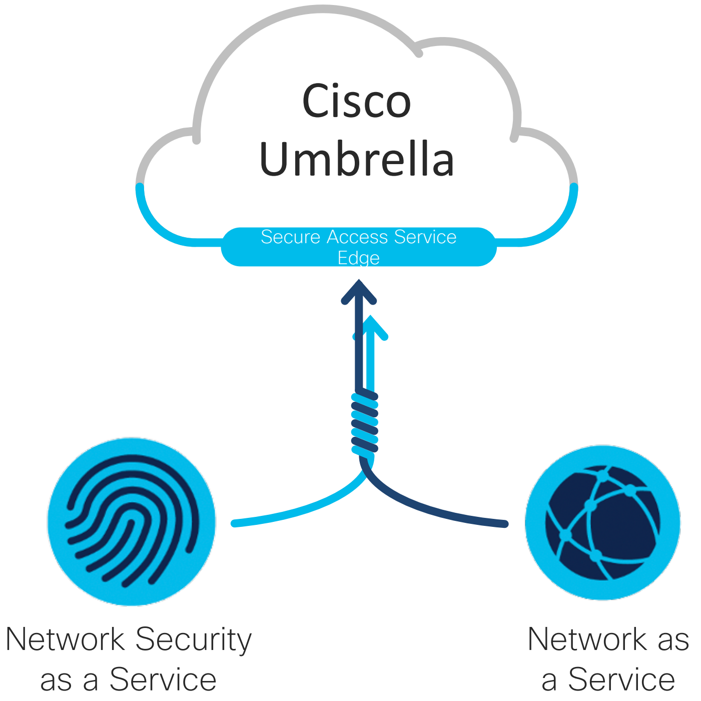
Drive consistent identity
driven policy

Visibility

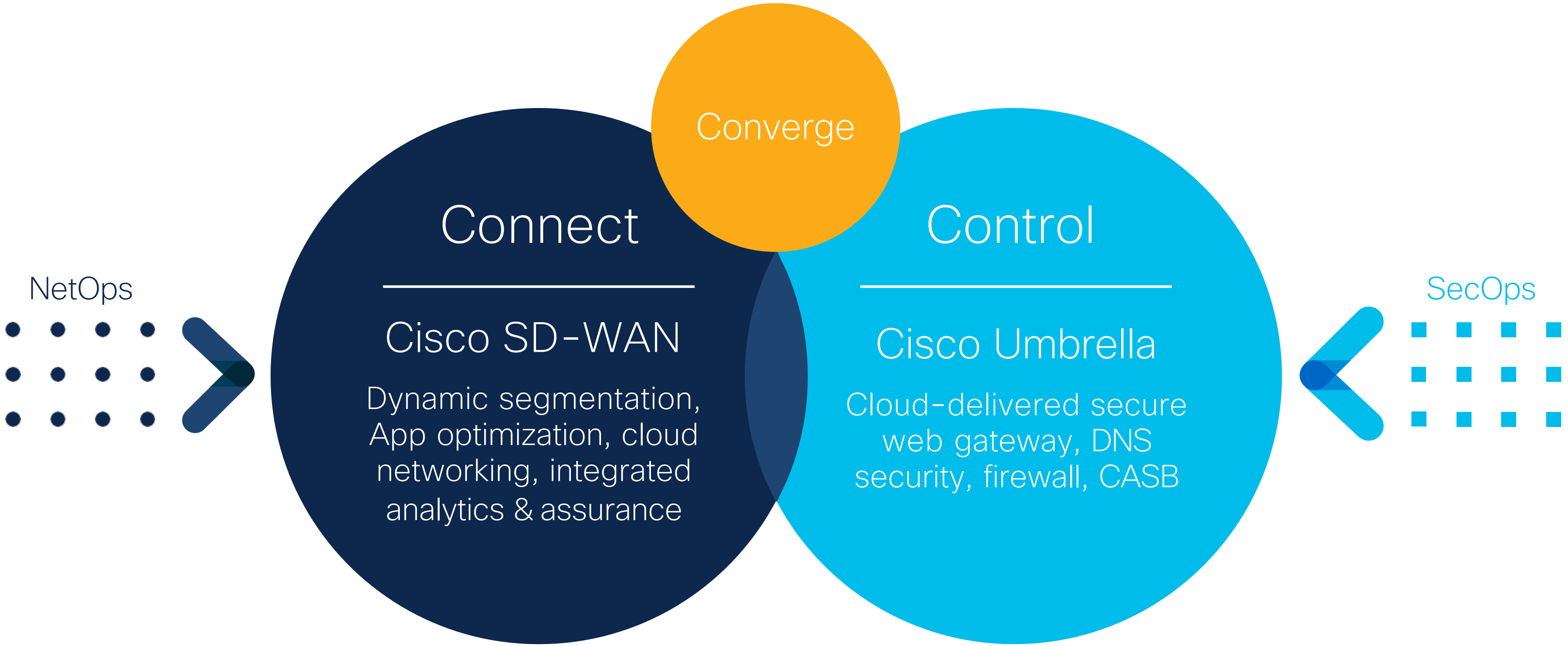
Visibility of my on-prem and Cloud Apps

What is SASE?

- ✓ SASE ("sassy") is Secure Access Service Edge
- ✓ Alternative to traditional, on-premise security
- ✓ Unifies networking and security services
- ✓ Delivers edge-to-edge security



Networking and Cloud Security convergence



Converge

NetOps

Connect

Cisco SD-WAN

Dynamic segmentation, App optimization, cloud networking, integrated analytics & assurance

SecOps

Control

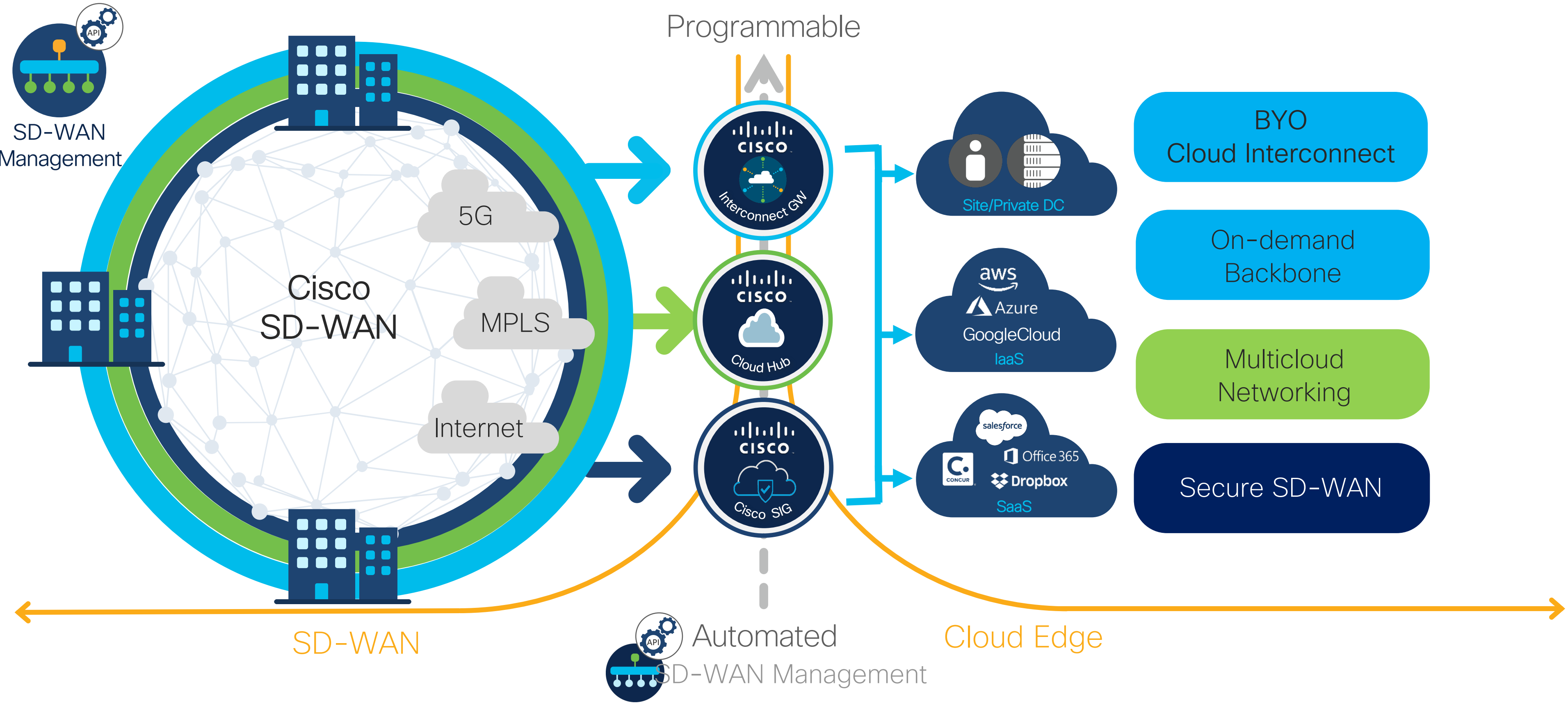
Cisco Umbrella

Cloud-delivered secure web gateway, DNS security, firewall, CASB

Highly available global cloud infrastructure | API-based, programmable architecture

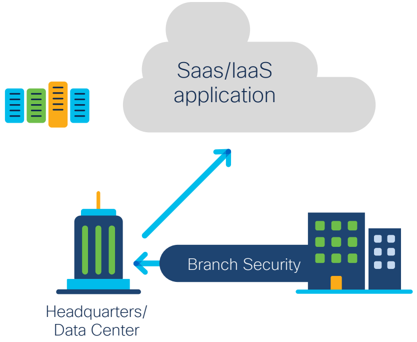
SecureX | Threat intelligence powered by Cisco Talos | 3rd party ecosystem

Secure SD-WAN For Multi-Cloud Networking



Control your journey to SASE

SD-WAN w/ On-Prem Security

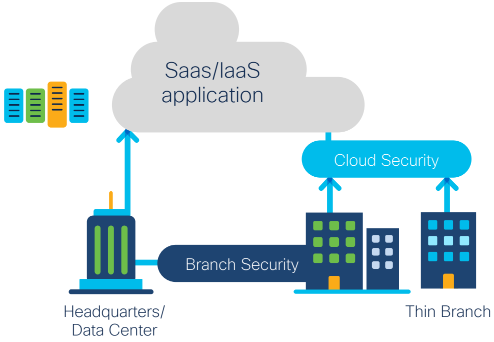


SD-WAN with on-prem security

SD-branch model

Thick branch with routing and security

SD-WAN w/ SIG Integration and Hybrid Security

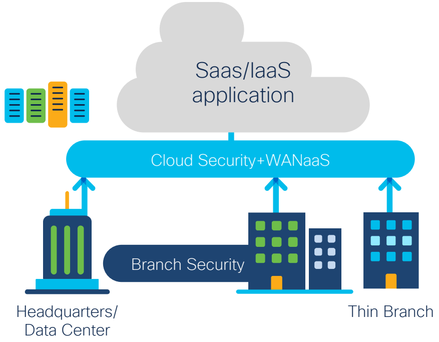


SD-WAN with SIG integration

Hybrid model

Thin branch with cloud security
Thick branch with routing and security

Future
As-a-service WAN and Cloud Security



SD-WANaaS/Sase

WAN aaS model

Thin and thick branches with unified on-prem and cloud security policies

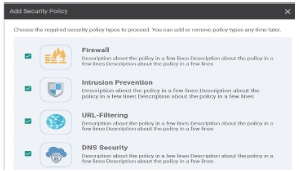
Feature Richness with Operational simplicity

SD-WAN Integrated Security

Starting point for SASE

Full Stack, Template Driven
Automated Security Offering

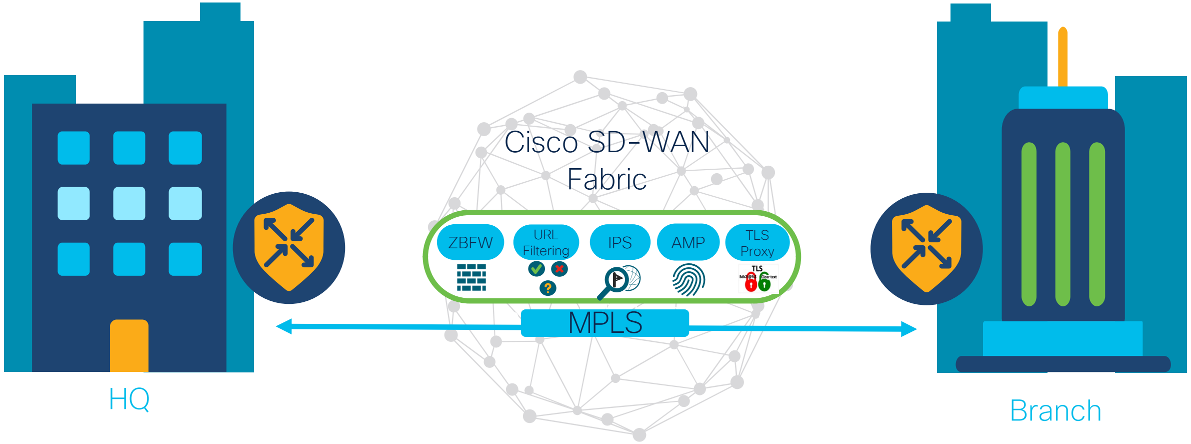
vManage
Automated
Templates



Add Security Policy

Choose the required security policy types to proceed. You can add or remove policy types any time later.

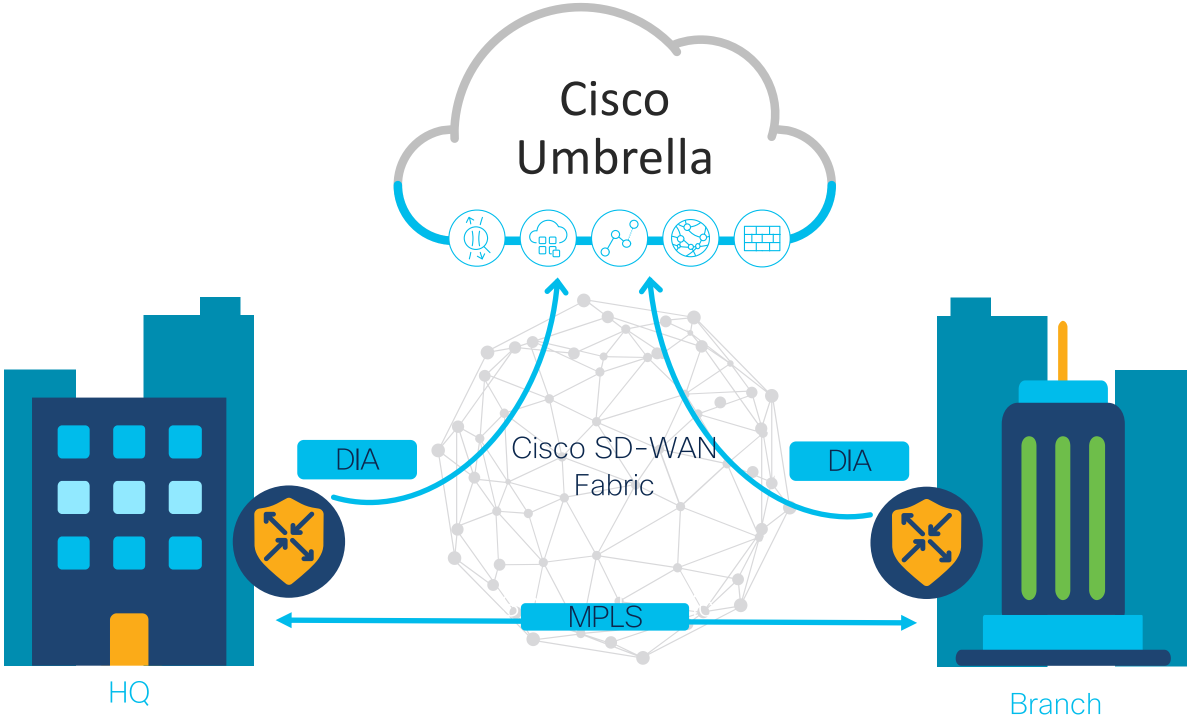
- ☑ **Firewall**
  Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines
- ☑ **Intrusion Prevention**
  Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines
- ☑ **URL-Filtering**
  Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines
- ☑ **DNS Security**
  Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines



- Enterprise Firewall
- Intrusion Prevention System
- URL-Filtering
- Advance Malware Protection
- DNS Security
- TLS/SSL Proxy

SD-WAN Cloud Security

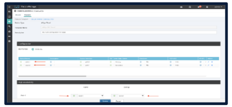
Auto Tunnel, Intelligent Traffic Steering



Use-Case

Unified policy for Mobile work force
Branch to Internet
Branch to Cloud(SaaS)

vManage
Auto-Templates



DNS-Layer Security

Secure Web Gateway

Cloud-Delivered Firewall

Cloud Access Security Broker

Interactive Threat Intel

SD-WAN Umbrella Integration

Integration Benefits

Superior Connectivity

Flexible traffic engineering, redirect traffic of interest “your” way

DNS-layer security

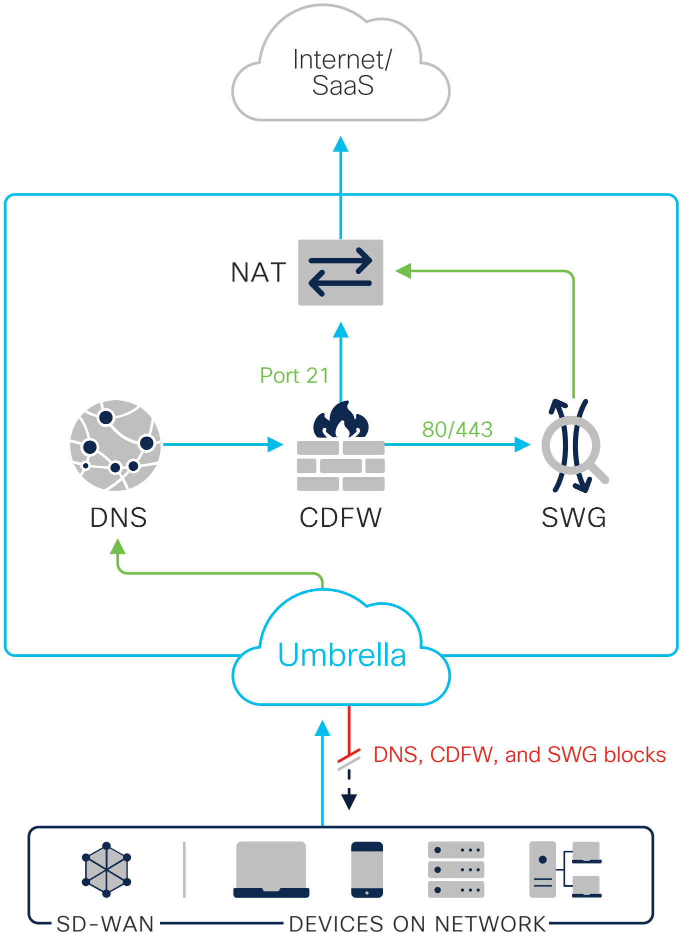
First check for domains associated with malware

Cloud-delivered firewall (CDFW)

Next check for IP, port, protocol and application rules

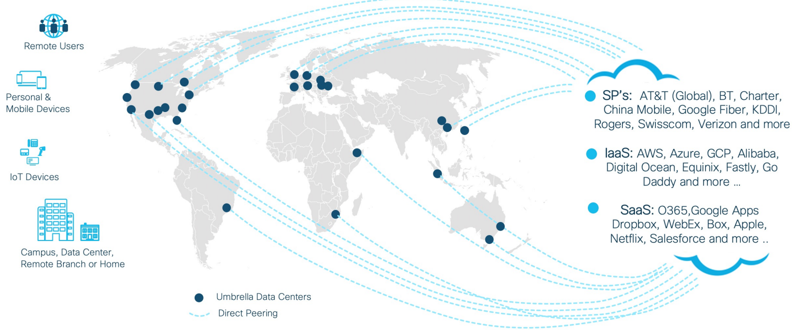
Secure web gateway (SWG)

Final check of all web traffic for malware and policy violations



Optimize the Middle-Mile

Improved Application Performance


Remote Users
Personal & Mobile Devices
IoT Devices
Campus, Data Center, Remote Branch or Home
● SP's: AT&T (Global), BT, Charter, China Mobile, Google Fiber, KDDI, Rogers, Swisscom, Verizon and more
● IaaS: AWS, Azure, GCP, Alibaba, Digital Ocean, Equinix, Fastly, Go Daddy and more ...
● SaaS: O365,Google Apps Dropbox, WebEx, Box, Apple, Netflix, Salesforce and more ..
● Umbrella Data Centers
Direct Peering

Use case

As a network admin, I want the best possible application performance across my network

Feature

- Direct peering lowers latency by providing more direct paths
- Global footprint with 20 Regional DCs, expanding to 32+
- Direct peering from Regional DCs to more than 1,000 organizations including leading SaaS and IaaS providers
- Up to 50% performance increase with key applications

SPs

- AT&T (Global)
- Bell
- Bharti Airtel Limited
- BT
- Charter
- China Mobile
- Google Fiber
- KDDI
- Rogers
- Swisscom
- Telkom
- Verzion
- Vodafone

IaaS

- Alibaba
- Amazon
- Dell Services
- Digital Ocean
- Equinix
- Fastly
- Go Daddy
- Google
- Huawei Cloud
- Microsoft
- Rackspace

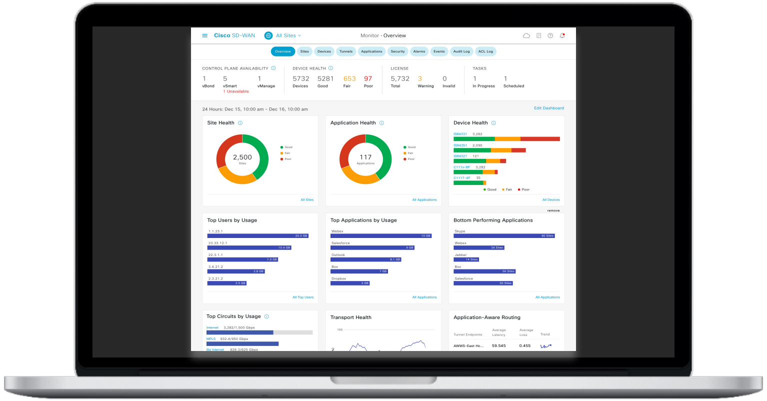
SaaS

- Apple
- Baidu
- Box
- Microsoft MSN
- Netflix
- Salesforce
- Yahoo!
- Webex
- Blizzard
- Dropbox
- Facebook

User Experience and Analytics

UX 2.0 & Thousand Eyes

UX 2.0



CONTROL PLANE AVAILABILITY: 1 vBond, 5 vSmart (1 Unavailable), 1 vManage

DEVICE HEALTH: 5732 Devices, 5281 Good, 653 Fair, 97 Poor

LICENSE: 5,732 Total, 3 Warning, 0 Invalid

TASKS: 1 In Progress, 1 Scheduled

24 Hours: Dec 15, 10:00 am - Dec 16, 10:00 am

Site Health: 2,500 Sites (● Good ● Fair ● Poor)

Application Health: 117 Applications (● Good ● Fair ● Poor)

Device Health:

ISR4331	3,282
ISR4351	2,090
ISR4321	121
C111x-8P	3,282
C1117-4P	35

● Good ● Fair ● Poor

Top Users by Usage:

1.1.23.1	20.3 GB
23.33.12.1	10.4 GB
22.3.1.1	7.9 GB
3.4.21.2	3.8 GB
2.3.21.2	3.5 GB

Top Applications by Usage:

Webex	10 GB
Salesforce	9 GB
Outlook	8.1 GB
Box	7 GB
Dropbox	3 GB

Bottom Performing Applications:

Skype	90 Sites
Webex	34 Sites
Jabber	14 Sites
Box	56 Sites
Salesforce	50 Sites

Top Circuits by Usage:

Internet	3,282/1,500 Gbps
MPLS	932.4/950 Gbps
Biz Internet	828.3/825 Gbps

Transport Health

Application-Aware Routing:

Tunnel Endpoints	Average Latency	Average Loss	Trend
AWWS-East-Hc...	59.545	0.455	

Enhanced GUI

Guided Experiences

Workflow Library

Configuration

Monitoring

Reporting

Cisco Vision: SD-WAN Analytics

Observability

- Application layer telemetry
- End-to-end path visualization from user to Hybrid Cloud applications
- Visibility into network behavior for underlay and overlay

Actionable Insights

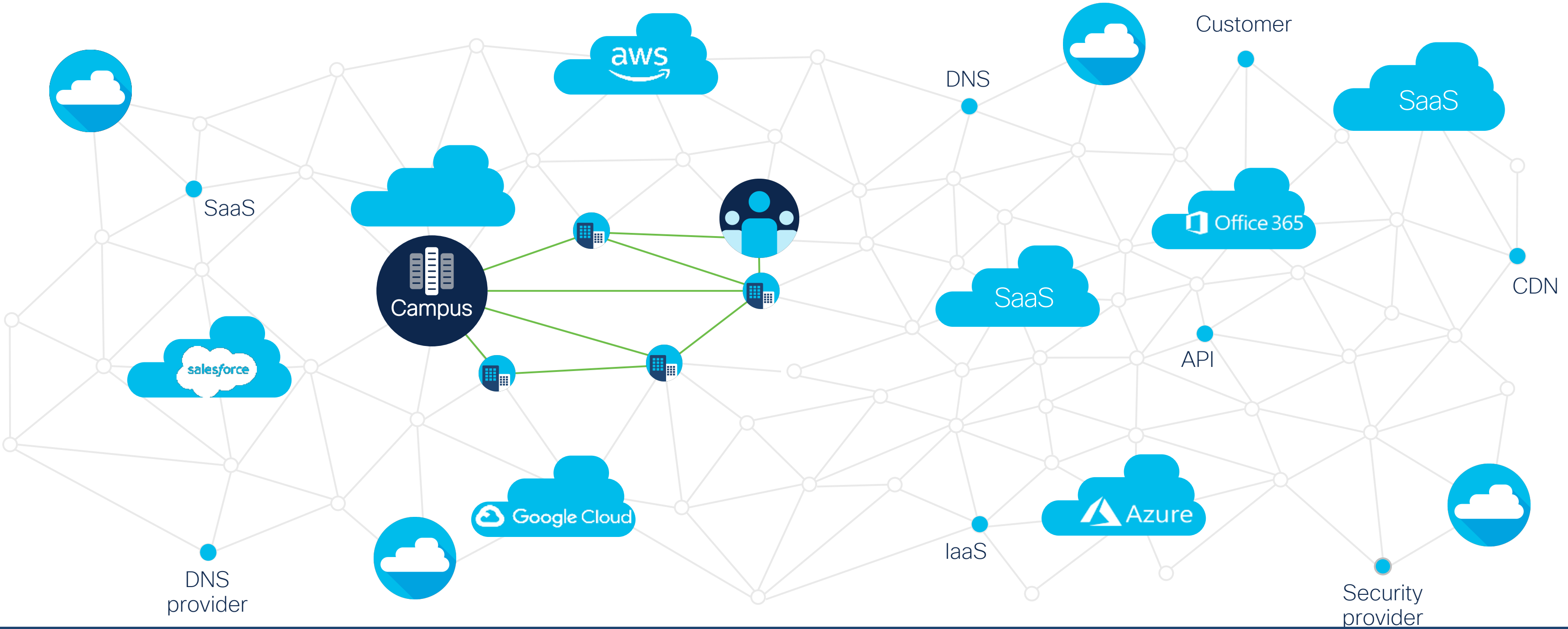
- Actionable, multi-layer insights to quickly resolve App experience issues
- Anomaly detection in routine network & application behavior
- Identify seasonal patterns

Predictive / Adaptive

- Predictive analysis of network and application behavior
- Adaptive network optimization for efficient application delivery
- Capacity management - Link quality assessments

Scalable, Cloud-first, Multi-domain Analytics Architecture

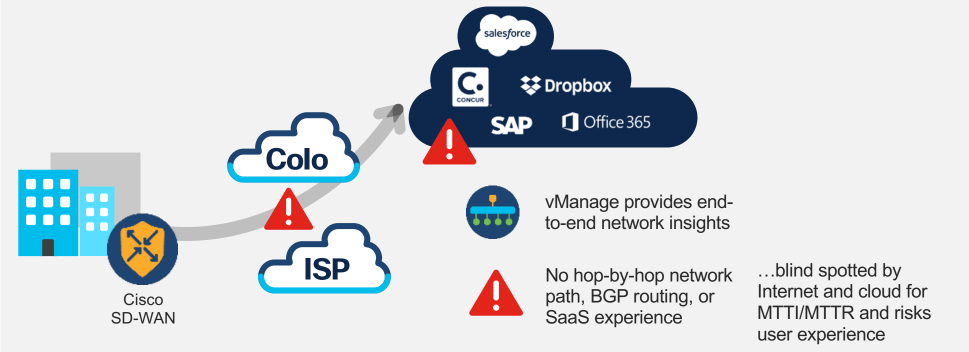
Thousand Eyes - Internet and Cloud introduce Blind Spots



Internet is the new WAN, cloud is the new data center, SaaS is new app stack.

SD-WAN solves Internet Blind Spots with Thousand Eyes

Scenario 1: Cisco SD-WAN optimizes connectivity to Multi-Cloud and SaaS

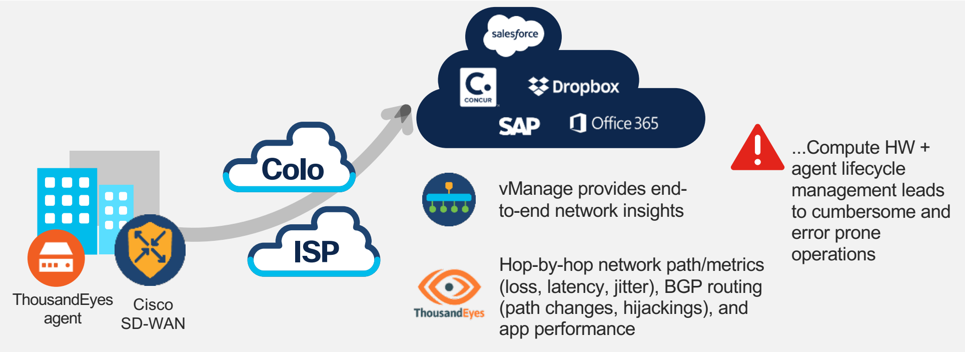


vManage provides end-to-end network insights

No hop-by-hop network path, BGP routing, or SaaS experience

…blind spotted by Internet and cloud for MTTI/MTTR and risks user experience

Scenario 2: Cisco SD-WAN + ThousandEyes Agent on external Compute



vManage provides end-to-end network insights

Hop-by-hop network path/metrics (loss, latency, jitter), BGP routing (path changes, hijackings), and app performance

...Compute HW + agent lifecycle management leads to cumbersome and error prone operations

Cisco SD-WAN + ThousandEyes native integration

salesforce
Office 365
Dropbox
ThousandEyes
aws
Azure
Google Cloud

Cisco SD-WAN with embedded ThousandEyes agent

Turn-key agent deployment

Rapid MTTI/MTTR

Actionable insights

SD-WAN Portifolio

Cisco SD-WAN Routing Portfolio

Branch | Aggregation | Cloud

SD-WAN + Services (IOS XE)

Branch

Catalyst 8300/8200

- ✓ Scalable Architecture for multi-cloud and muli-domain environment
- ✓ 10G Architecture with x86 SoC for Modular Access

ISR 1000

- ✓ Integrated wired and wireless access
- ✓ LTE Advanced
- ✓ VDSL2, ADSL2/2+

ISR 1120 / 1160
(New 25 SKUs)

- ✓ WWAN pluggable flexibility
- ✓ PIM: 4G LTE CAT4/6/18

ISR 4000

- ✓ WAN and voice module flexibility
- ✓ Compute with UCS-E
- ✓ Container Architecture

Aggregation

Catalyst 8500

- ✓ Scalable Architecture for multi-cloud and multi-domain environment
- ✓ 3rd Gen QFP + 40/100G for Aggregation

ASR 1000

- ✓ Hardware and software redundancy
- ✓ High-performance service with hardware assist

Cloud

Catalyst 8000V

CSR 1000V

Viptela OS

ISR 1100-4G

- ✓ 4 GE WAN ports

ISR 1100-4G LTE

- ✓ 4G LTE (CAT4)

ISR 1100-6G

- ✓ 6 WAN ports (4 GE and 2 SFP)

vEdge 2000

- ✓ RPS, PIM options

vEdge 5000

- ✓ Modularity, RPS

vEdge Cloud

NFV

Cisco ENCS & CSP

- ✓ Service chaining virtual functions
- ✓ Options for WAN connectivity
- ✓ Open for 3rd party services & apps
- ✓ NFVIS Hypervisor

Catalyst 8200 uCPE

CSR 1000V
vEdge Cloud

- ✓ Extend enterprise routing, security & management to cloud
- ✓ Cisco DNA virtualization

Questions ?