
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Building a Best of Breed Solution

Cisco SD-WAN Innovations

Aaron Rohyans, Senior Technical Marketing Engineer

BRKENT-2106

Aaron Rohyans

Senior Technical Marketing Engineer

cisco Live!

Agenda

- Introduction
- Core Functionality
- Application Quality of Experience
- Cloud
- Security
- Unified Communications
- vAnalytics
- Conclusion

Introduction

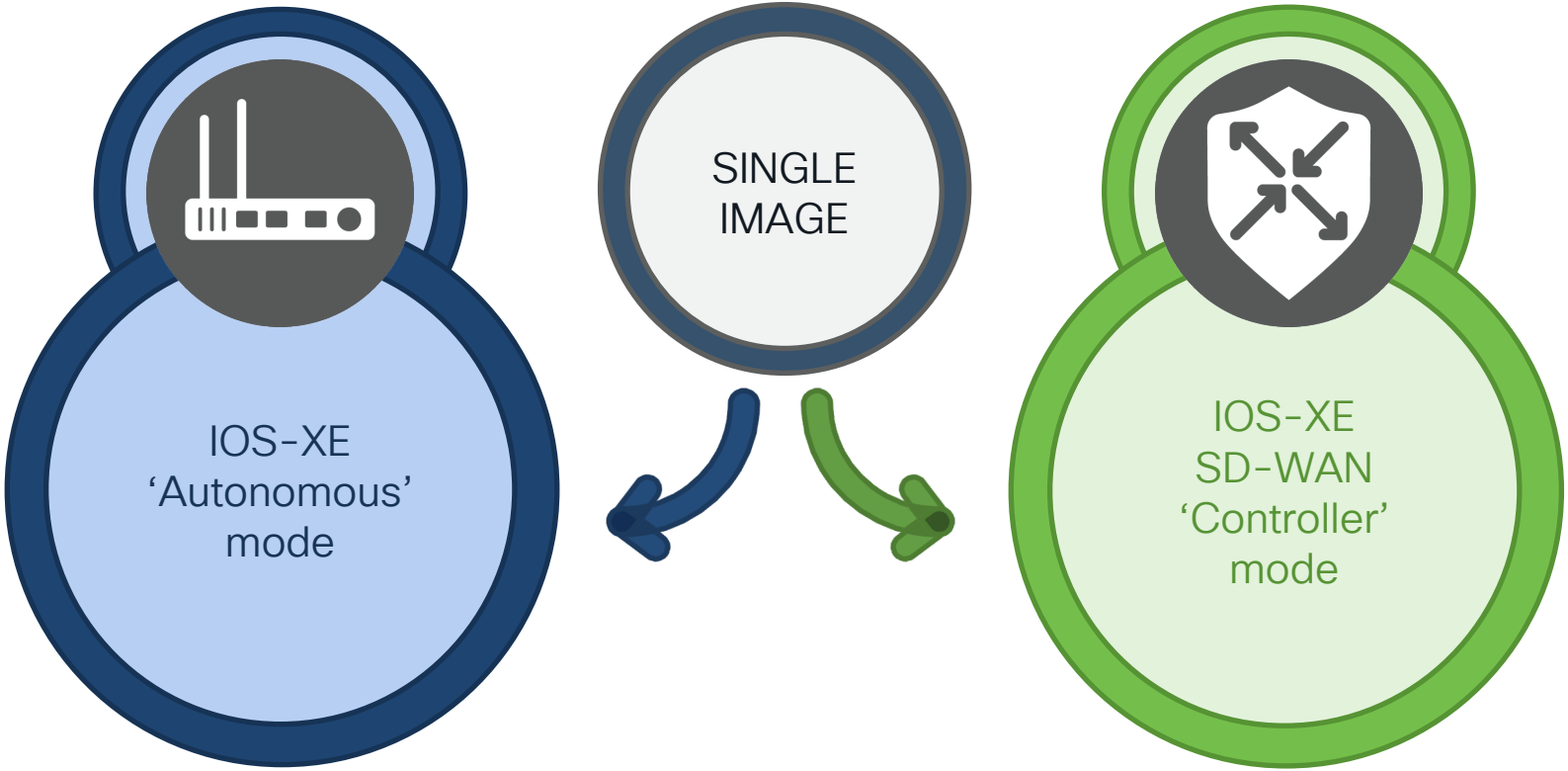
Cisco SD-WAN has come a long way in a short amount of time - providing new differentiators and closing gaps over the past year.

This session aims to provide an overview of several of these enhancements, allowing the attendee to become familiar with the feature's context, use-case and strategy.

Upon conclusion, attendees should have a good grasp on the tools in their toolbelt when deploying Cisco SD-WAN!

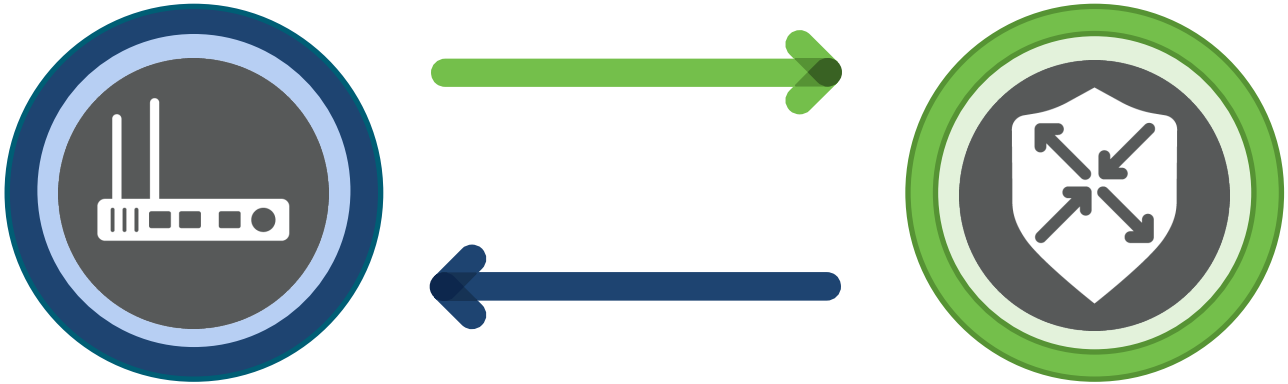
Core Functionality Enhancements

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



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

CLI Add-On Templates

Use Case:

- Needed feature or functionality does not yet exist in a vManage Feature Template
- Caveat or bug workaround

Solution:

- Configure Device Template as normal
- Attach CLI Add-On Template to append configuration

Service Side NAT

vEdge ✓

New! cEdge ✓

Problem

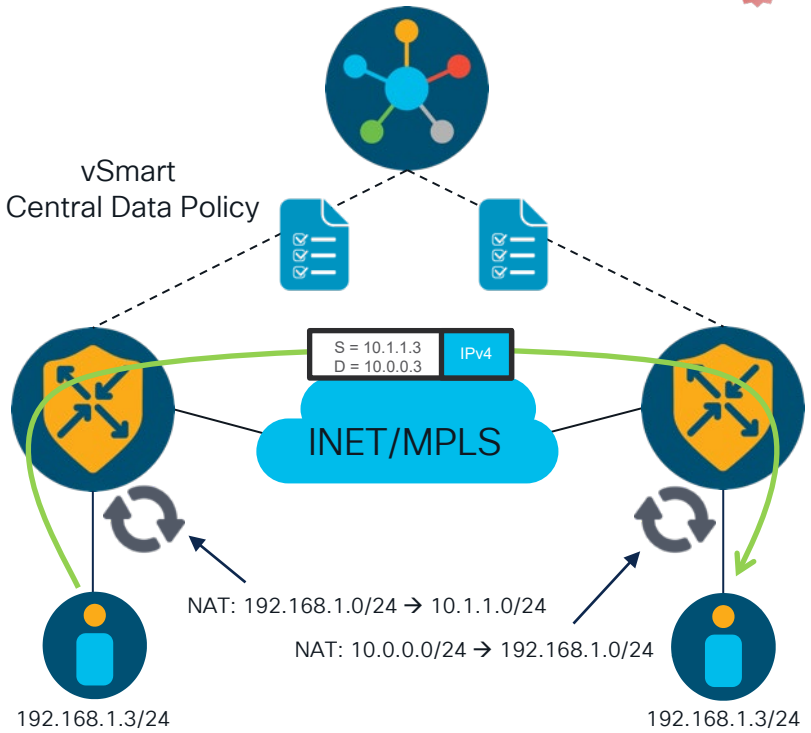
Address conservation, mergers/acquisitions and reducing operational overhead when resources shift around the network all bring in the potential for overlapping address ranges. How do you maintain connectivity to these resources?

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



DIA Tracker Support

vEdge ✓

New! cEdge ✓

Problem

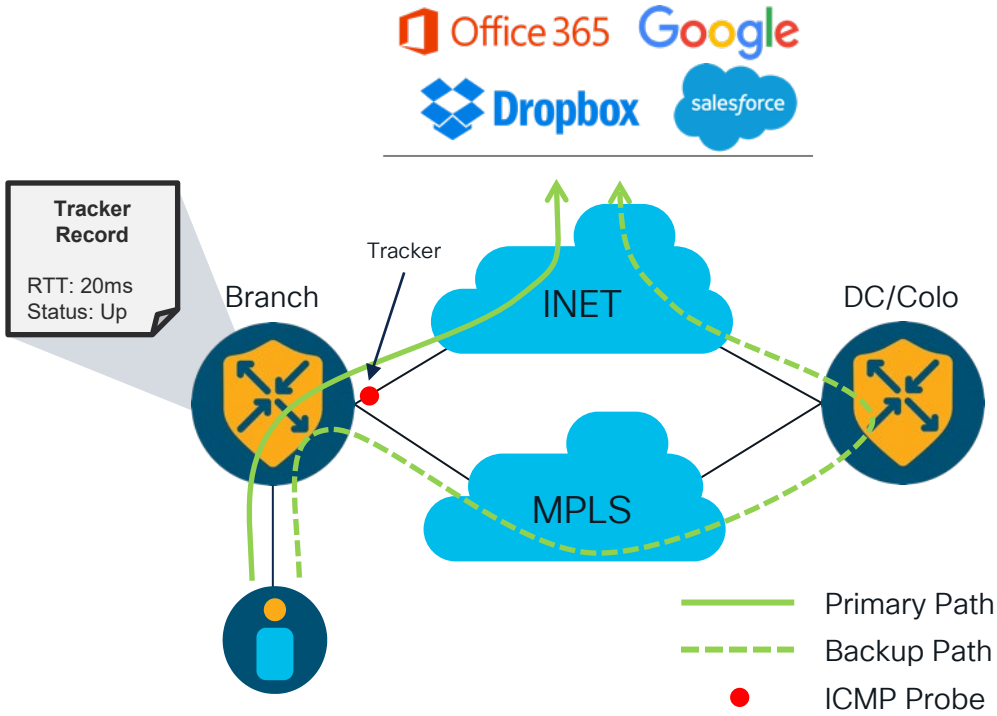
Enterprises that adopt a Direct Internet Access (DIA) model have limited visibility into the status of Internet-facing interface(s). Hence, in brownout conditions, Internet traffic forwarded to this interface would be silently dropped.

Solution

SD-WAN v20.3 and IOS-XE v17.3 now support SLA tracking on both vEdge and IOS-XE SD-WAN 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)



Static Route Tracker Support

vEdge ✓
cEdge ✓

Problem

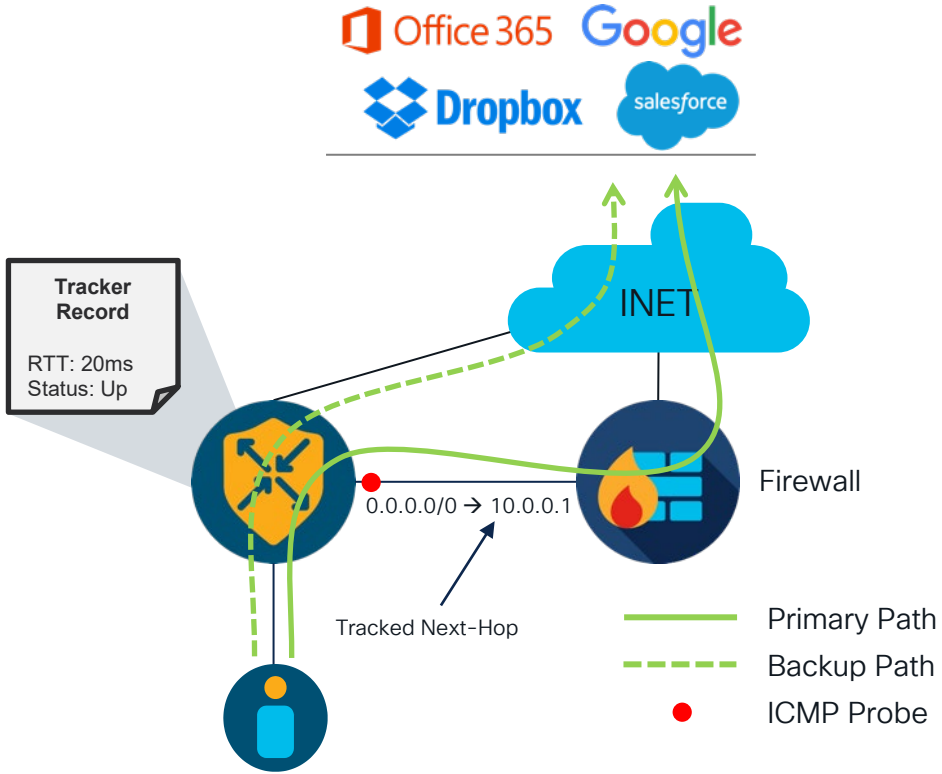
When configuring static routes, WAN routers often lack visibility into the reachability/status of the next-hop specified. Hence, traffic can be inadvertently dropped when/if the next-hop becomes unreachable.

Solution

SD-WAN v20.3 and IOS-XE v17.3 now support SLA tracking on IOS-XE SD-WAN to probe the next-hop address of static routes within Service VPNs. Should the next-hop become unreachable, the router can invoke a backup path.

Caveats / Prerequisites

IPv4 only, Service VPN only



Service Insertion Tracker Support

vEdge ✓

New! cEdge ✓

Problem

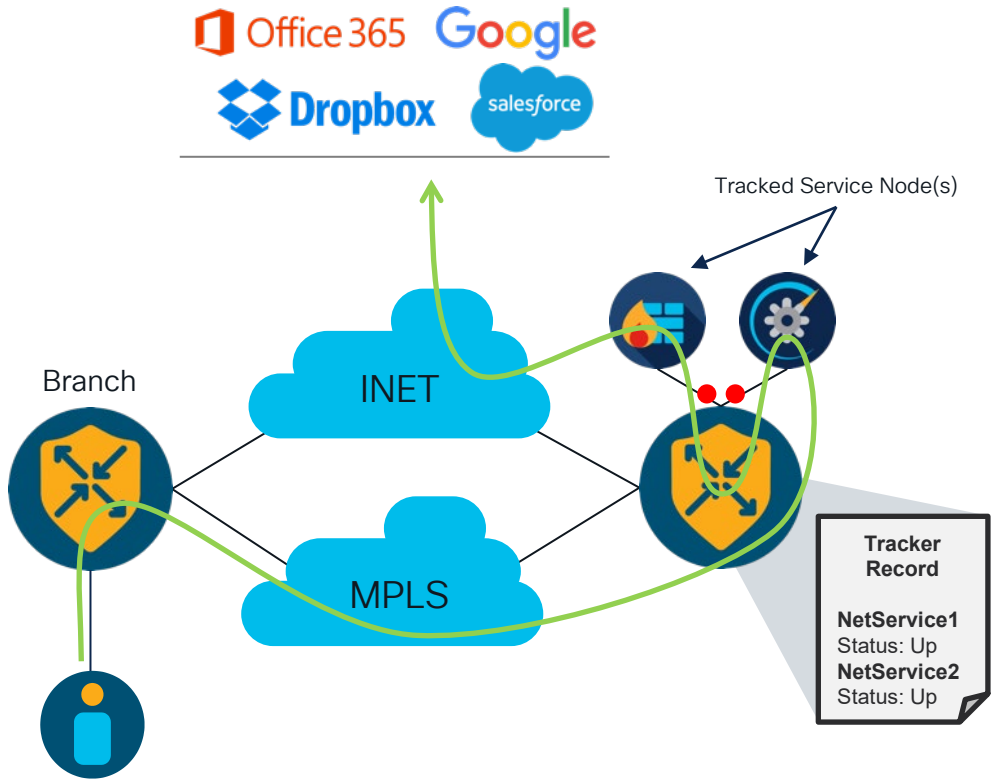
SD-WAN allows administrators to easily insert devices (Service Nodes) into the transit path of traffic traversing the WAN Edge - for inspection, monitoring, optimization, etc. Visibility into the reachability/status of the Service Node is limited, however. Hence, traffic can be inadvertently dropped if the Service Node becomes unavailable.

Solution

SD-WAN v20.3 and IOS-XE v17.3 now support SLA tracking on both vEdge and IOS-XE SD-WAN to probe the Service Node for reachability. Should the Service Node fail to respond, the router can invoke a backup path, or alternate Service Node.

Caveats / Prerequisites

Probe timeouts are fixed, interface tracking is not supported



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

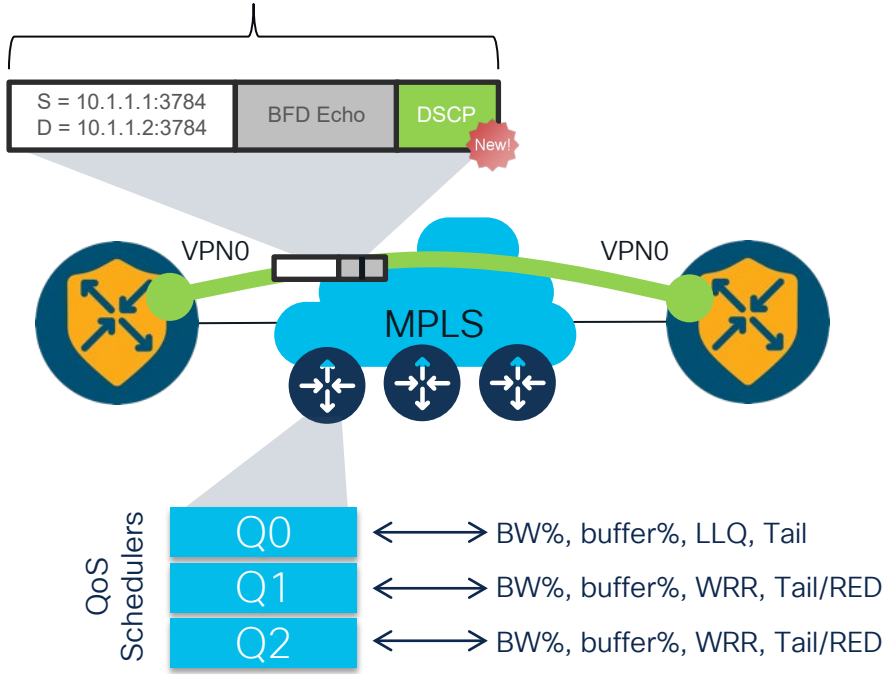
SD-WAN v20.4 / 17.4 introduces capability to customize BFD probes with different DSCP markings. This will help reflect the actual treatment of a user's packet and will allow a more accurate reading of loss/latency/jitter. Consequently, AAR can now route traffic based on more accurate measurements

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



Dynamic On-Demand Tunnels

vEdge ✓
cEdge ✓

Problem

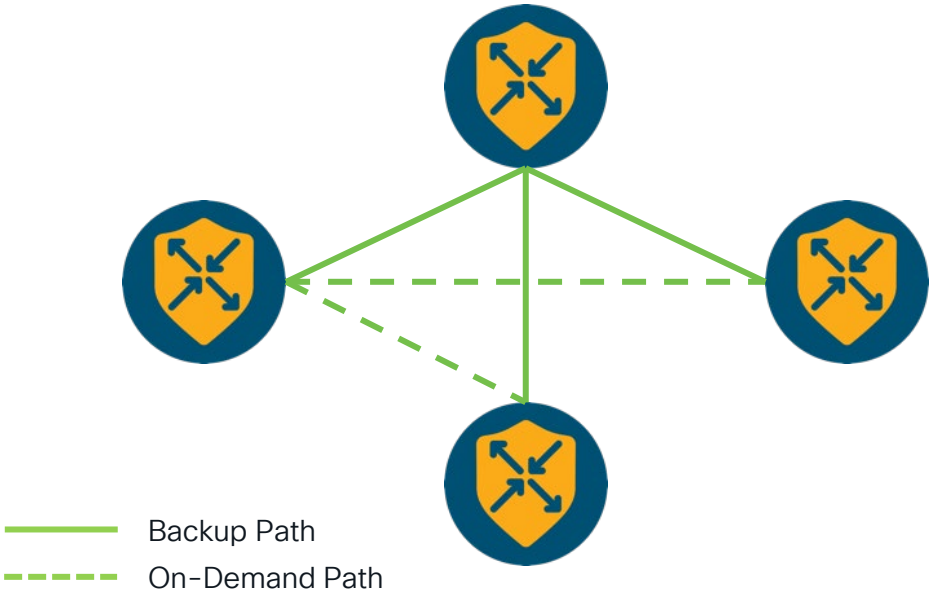
By default, Cisco SD-WAN operates in full-mesh. While topology modification is possible, full-mesh carries a huge computational burden on branch resources and, therefore, becomes difficult to scale. Enterprise customers need full-mesh connectivity, but also need a way to offset the resource burden that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



Demo:
On-Demand Tunnels

Enhanced Route Leaking

vEdge ✓
cEdge ✓

Problem

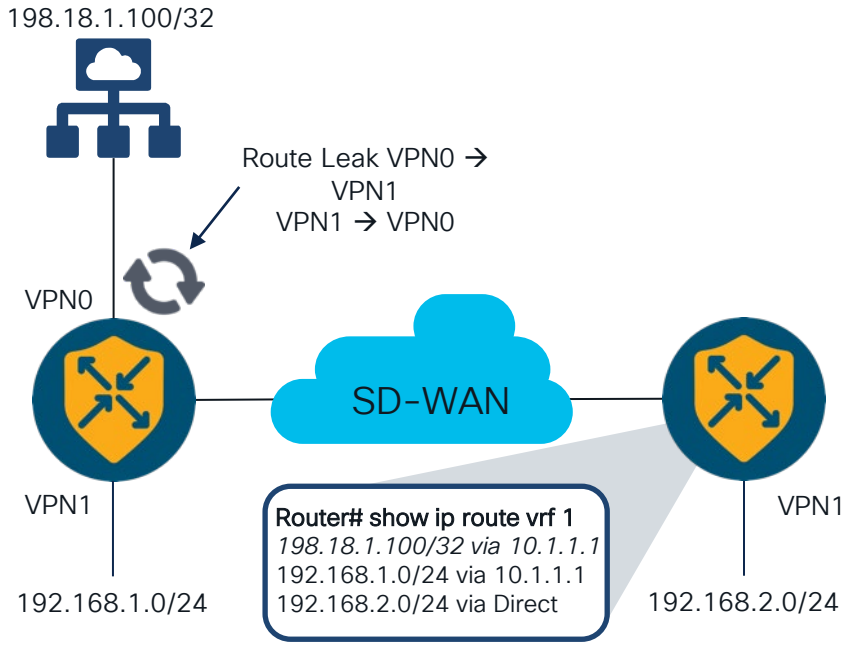
Many customers have expressed a need to expose underlay services within the SD-WAN overlay (such as hosted PBX/VoIP being made available to phones that exist in a Service VPN/VRF). At present (v17.2 / 20.1), SD-WAN only supports this type of route leaking between Service VPNs.

Solution

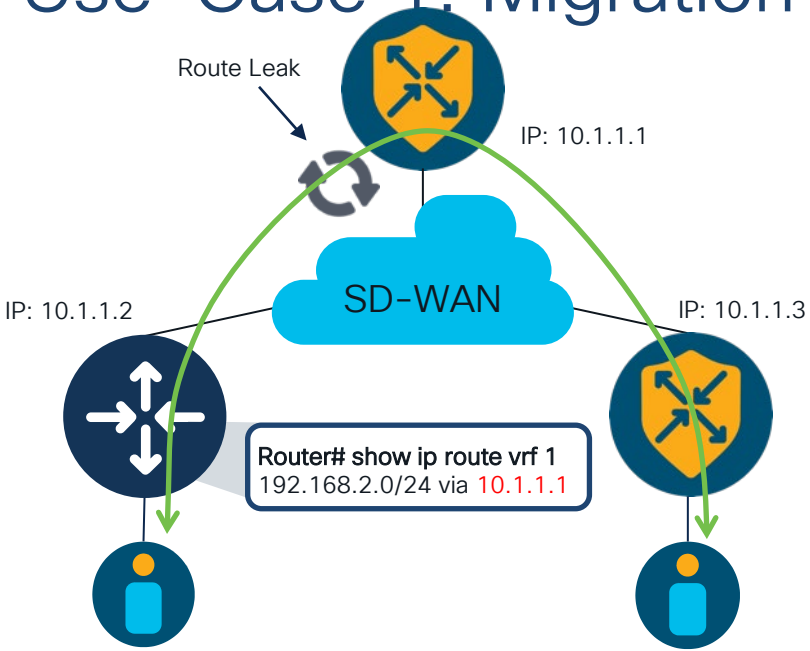
Cisco SD-WAN v20.3 / 17.3 now support route leaking between Service VPNs and the Transport VPN.

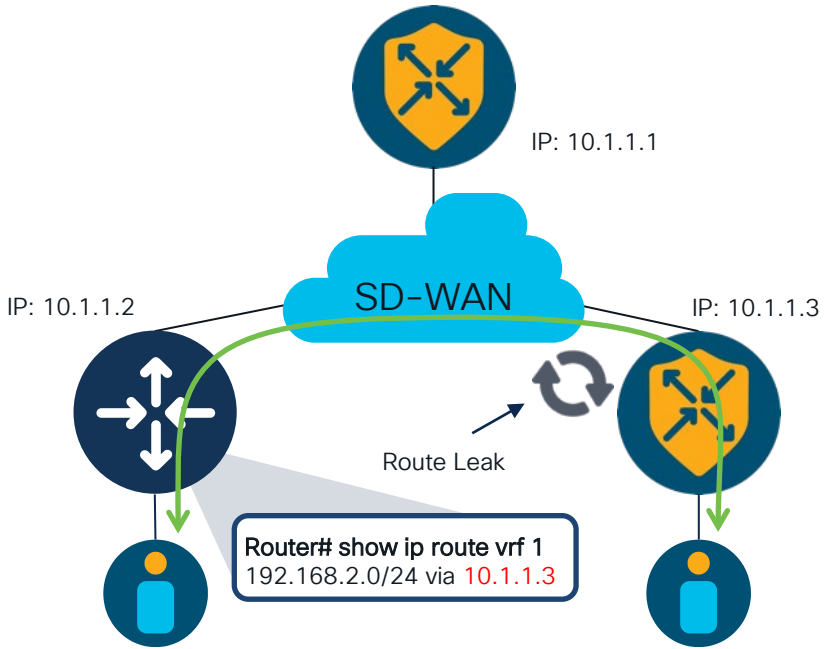
Caveats / Prerequisites

IPv4 only, no IOS-XE SD-WAN BGP route propagation support, SSNAT + Route Leak is not supported, VPN0 cannot be transit VPN, vEdge/IOS-XE SD-WAN workflow differs



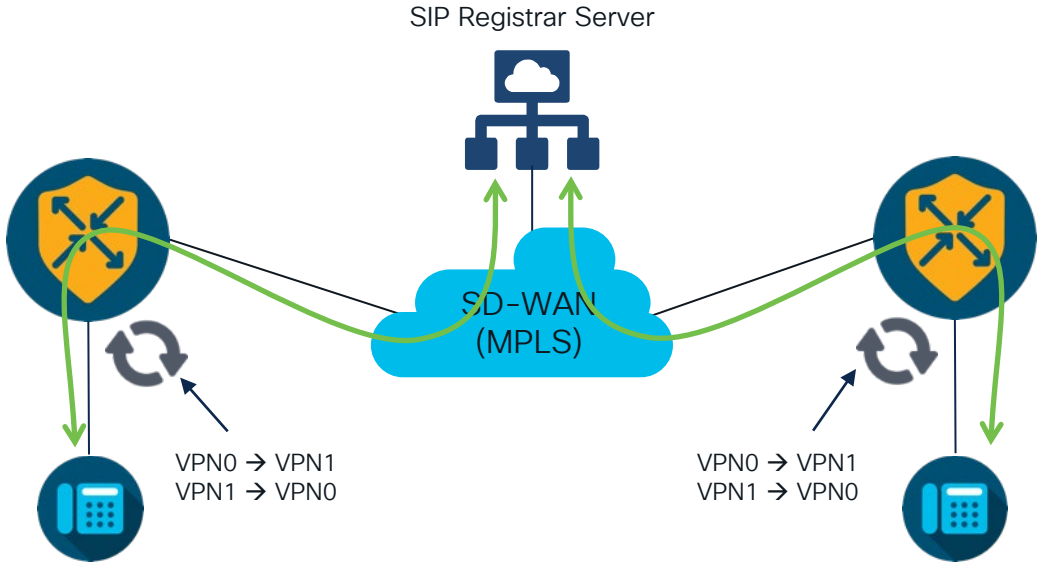
Use-Case 1: Migration





- Old way: Migrated to legacy site connectivity must traverse the hub (and vice versa)
- New way: Migrated to legacy site connectivity may go direct (and vice versa)

Use-Case 2: Underlay Service Access



- Old way: Access to services outside the SD-WAN fabric must traverse the hub, or utilize some form of direct breakout (which usually involves more equipment, or the use of NAT)
- New way: The SD-WAN router can directly access underlay services without the need to forward to an external appliance or invoke NAT

Multi-Tenancy

vEdge ✓

cEdge ✓

Problem

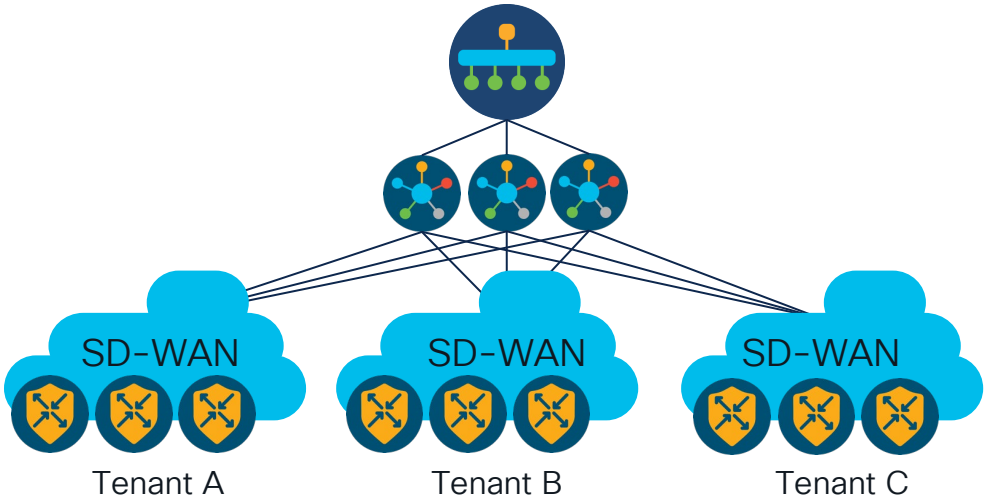
Deploying a single instance of controllers while managing multiple UIs, per customer, creates cost & operational challenges for Managed Service Providers.

Solution

Cisco's Multi-Tenant SD-WAN solution allows Service Providers to manage multiple customers from a single vManage, vBond, and vSmart. Having a shared vManage, vBond, and vSmart helps reduce the compute footprint.

Caveats/Supported platforms

17.4/20.4 is the first official GA release for vManage Multi-Tenancy, which means only Greenfield deployments are supported.

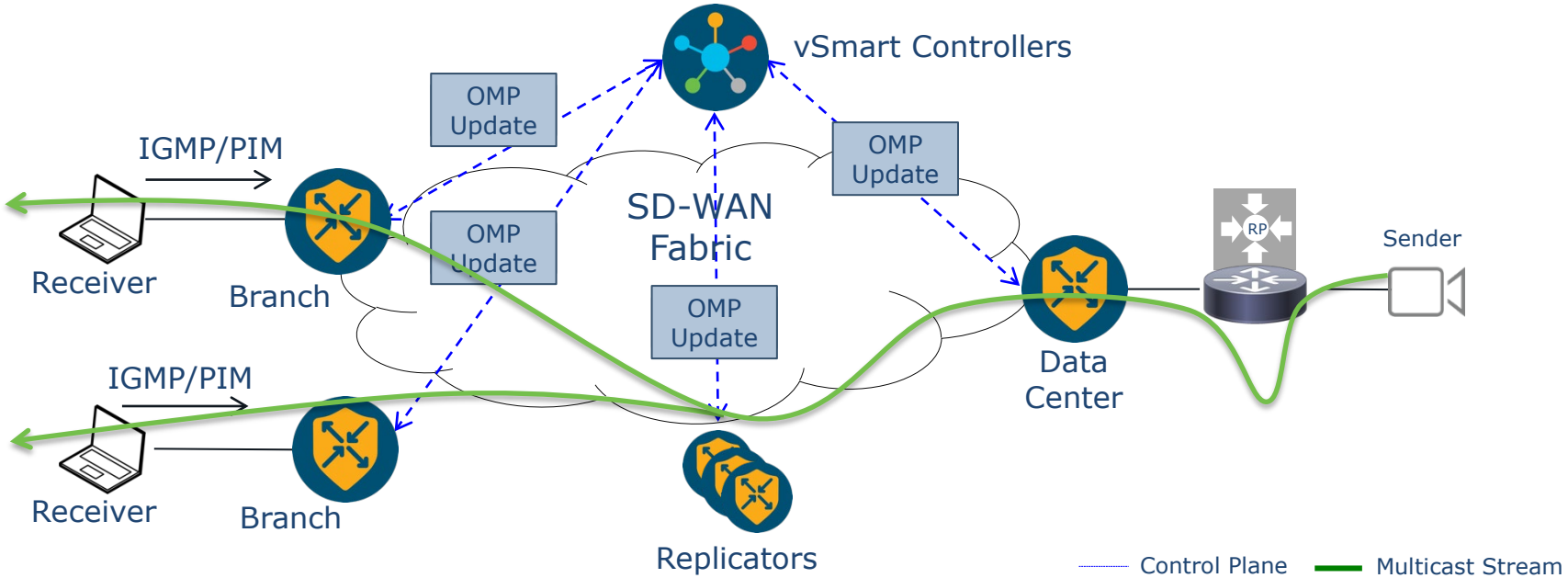


Multicast Support for SD-WAN

IOS XE SD-WAN's multicast supports sending data to multiple destinations

vEdge ✓

New! cEdge ✓



- IOS-XE SD-WAN devices interoperate with IGMP v2/v3 and PIM on the service side
- IOS-XE SD-WAN devices advertise receiver multicast groups using OMP
- cEdge Replicators replicate multicast stream to receivers
- Multicast is encapsulated in point-to-point tunnels

Application Quality of Experience Enhancements

cisco Live!

Multicast AAR

vEdge ✗

cEdge ✓

Problem

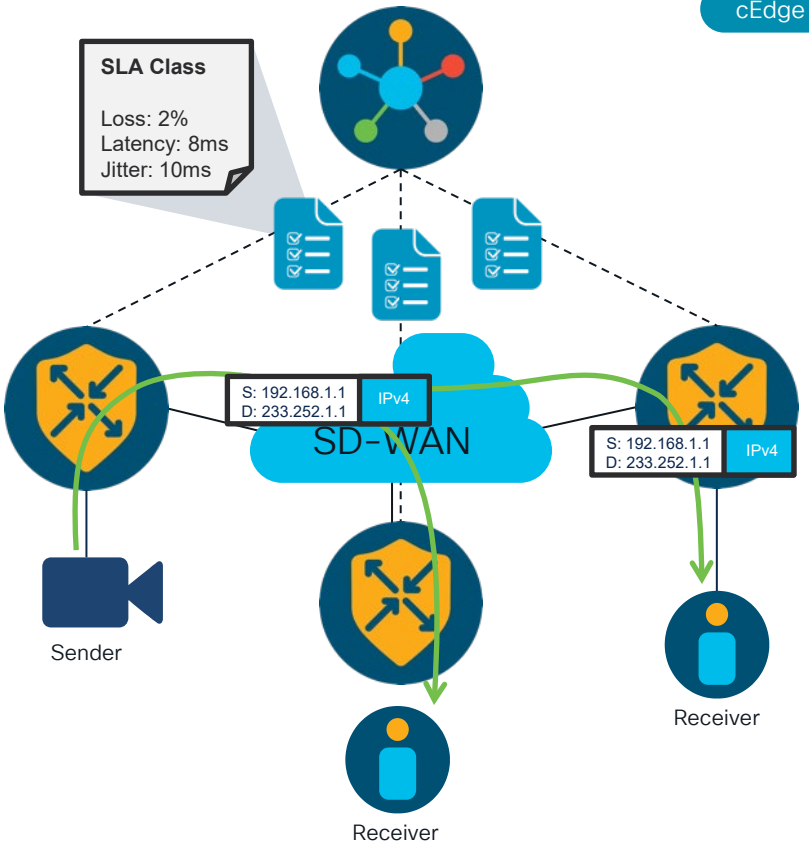
Currently, SD-WAN intelligent routing is bound to unicast flows. As multicast becomes more and more prevalent for content delivery, organizations are seeking to extend traffic routing intelligence to these flows as well.

Solution

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

Caveats / Prerequisites

IOS-XE SD-WAN only, IPv4 only, S/D IP + Protocol match only, no DPI/application match, no DSCP match



Custom Application Support

vEdge ✗
cEdge ✓

Problem

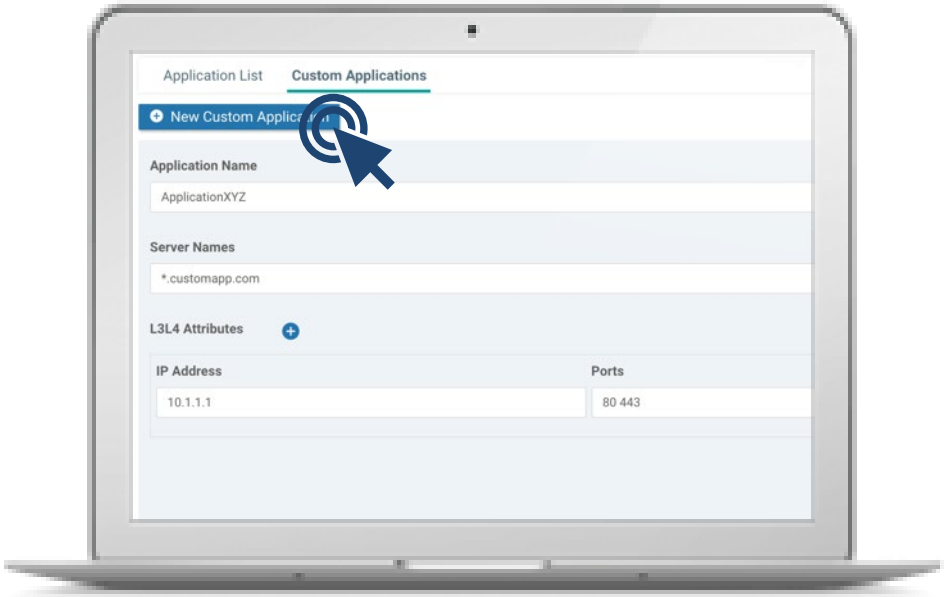
Application Recognition engines, such as NBAR2, often lack recognition for homegrown or less popular applications. As such, defining traffic policy can become challenging and cumbersome when customers need to take action against or monitor this traffic.

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.

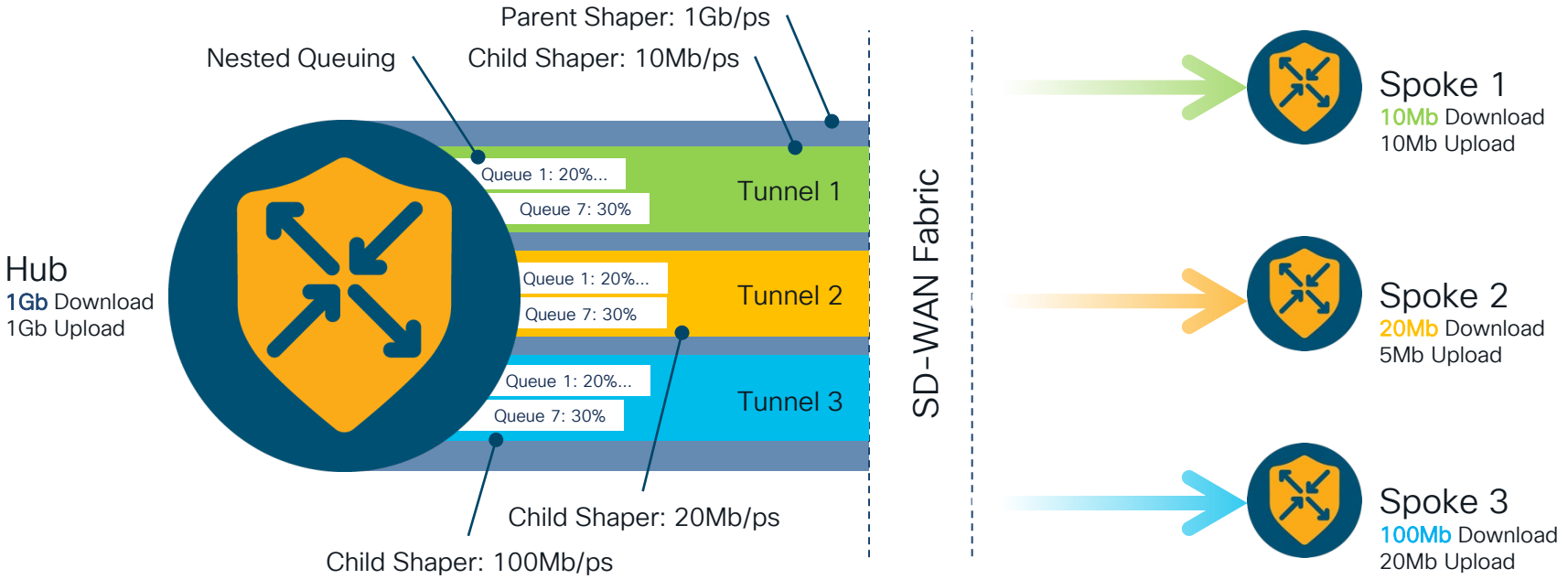
Caveats / Prerequisites

IOS-XE SD-WAN only, IPv4 only, flow direction is unsupported, DSCP is unsupported, must have policy enabled



Per-Tunnel QoS support on SD-WAN

vEdge ✓
cEdge ✓



Per-Tunnel QoS allows a site to dynamically adjust the sending rate of its traffic to accommodate lower bandwidth circuits at remote locations.

Adaptive Quality of Service

vEdge ✓

cEdge ✓

Problem

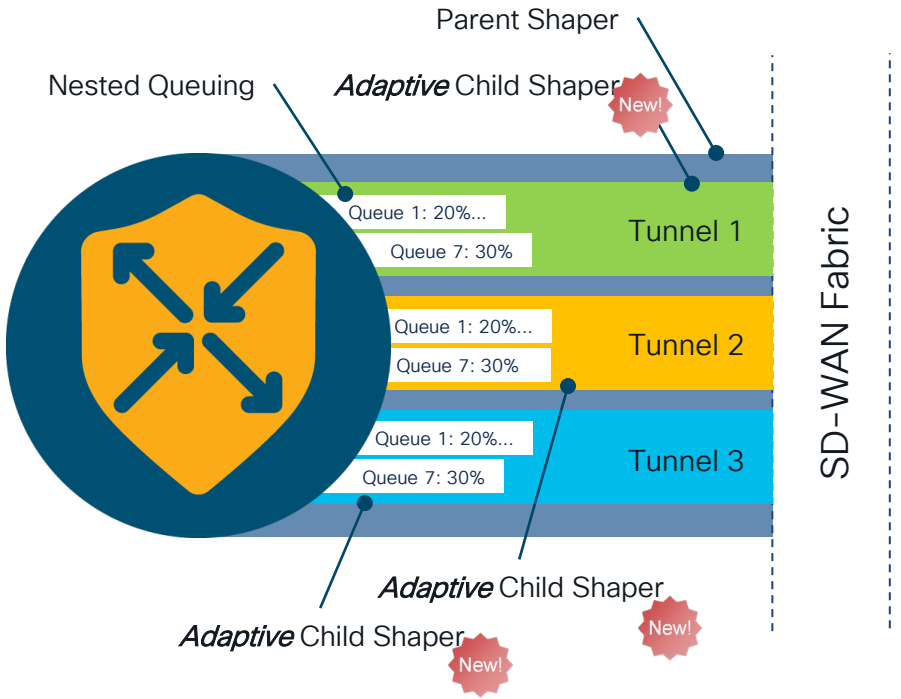
Per-Tunnel QoS, introduced in v20.1 / 17.2 of SD-WAN, allows for much more efficient use of bandwidth by allowing a Hub site to reduce the sending speed of data so as not to overwhelm the remote spoke. Unfortunately, this shaping mechanism is static and may not reflect the actual bandwidth available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

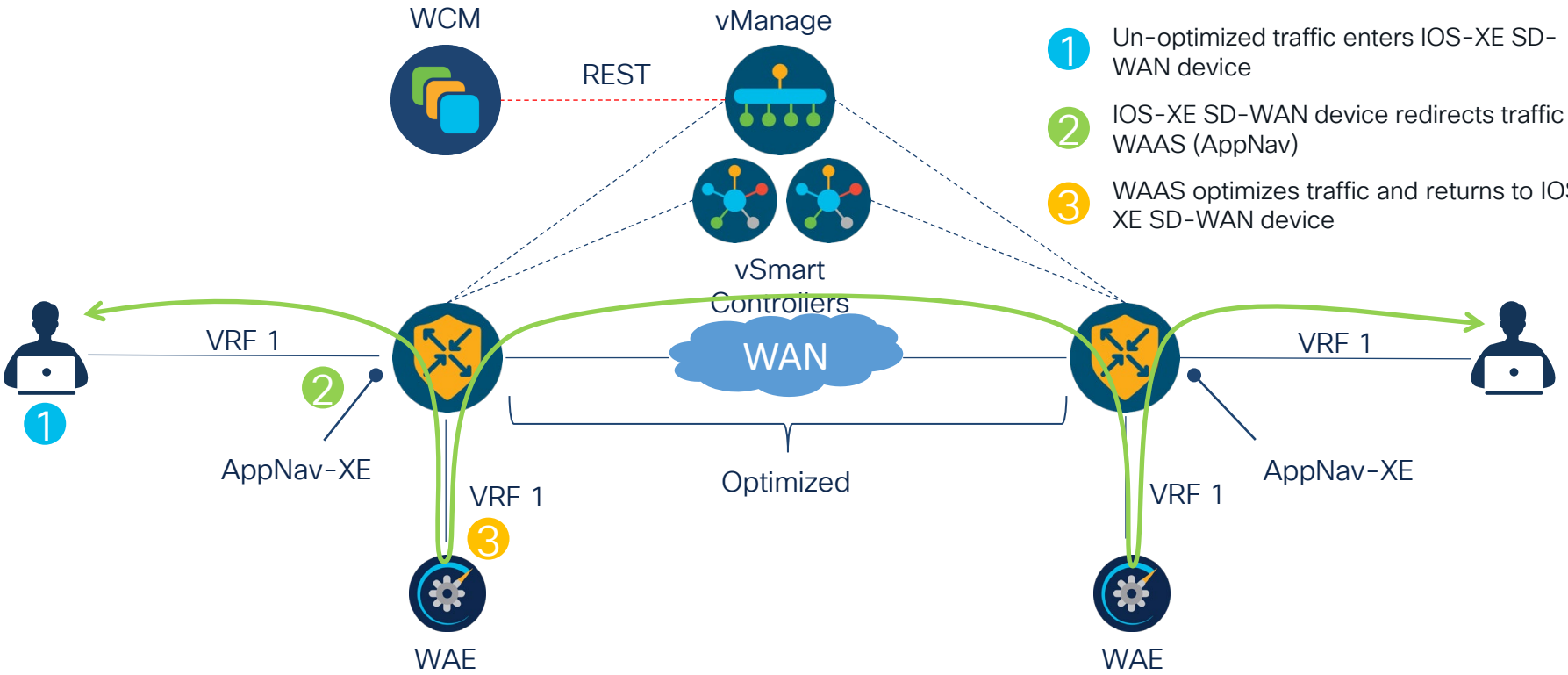
Caveats / Prerequisites

None



AppNav-XE with SD-WAN

vEdge ✗
cEdge ✓



1. Un-optimized traffic enters IOS-XE SD-WAN device
2. IOS-XE SD-WAN device redirects traffic to WAAS (AppNav)
3. WAAS optimizes traffic and returns to IOS-XE SD-WAN device

Quick Look: Multiple Service Nodes for AppQoE

vEdge ✗
cEdge ✓

Problem

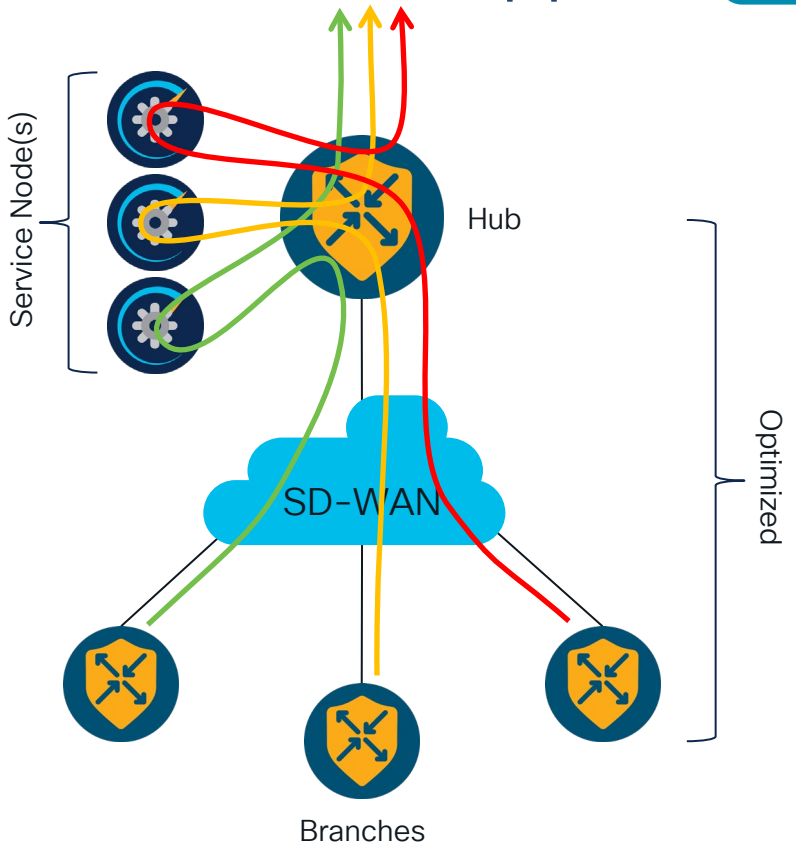
Implementing Application Quality of Experience, specifically features like TCP Optimization, can be burdensome to WAN Edge resources – reducing scalability and overall throughput of the platform. This is particularly evident in headend platforms that are optimizing/aggregating connections from all over the enterprise.

Solution

SD-WAN v17.4.1 / 20.4 provides support for AppQoE Service Nodes (C8KV) that can offload the optimization burden of headend devices.

Caveats / Prerequisites

SC only supports ASR/C8500 and C8KV, Service Node can only be C8KV



Cloud Enhancements

AWS Transit Gateway Support

vEdge ✓

cEdge ✓

Problem

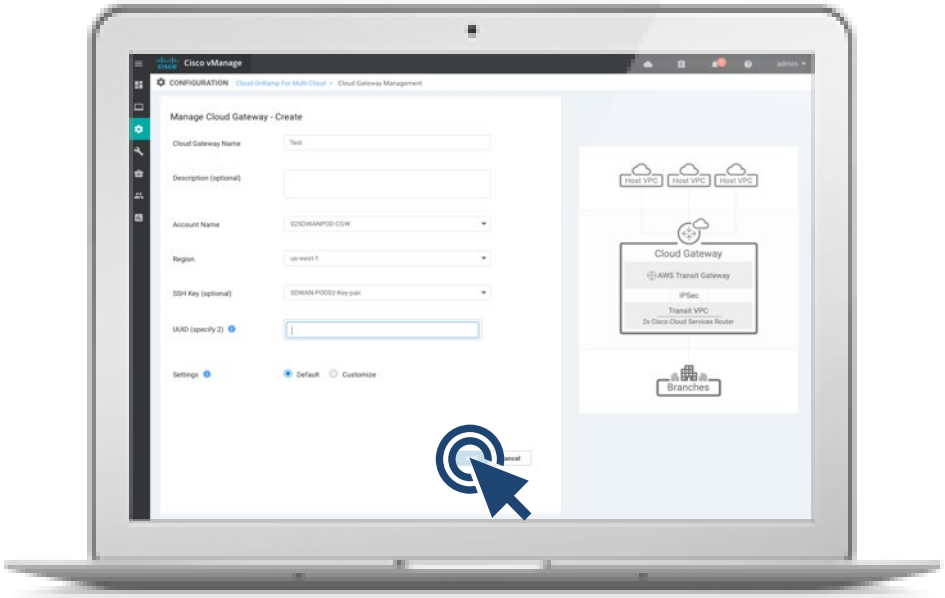
The current implementation of Cloud onRamp for IaaS (AWS) does not utilize the Transit Gateway model. Hence, customers have increased subscription costs and face a deprecated connectivity model when using Transit VPCs

Solution

SD-WAN v20.3 / 17.3 introduces Transit Gateway (TGW) support for Cloud onRamp for IaaS with AWS.

Caveats / Prerequisites

None



Azure Virtual Wan Integration

vEdge ✗

cEdge ✓

Problem

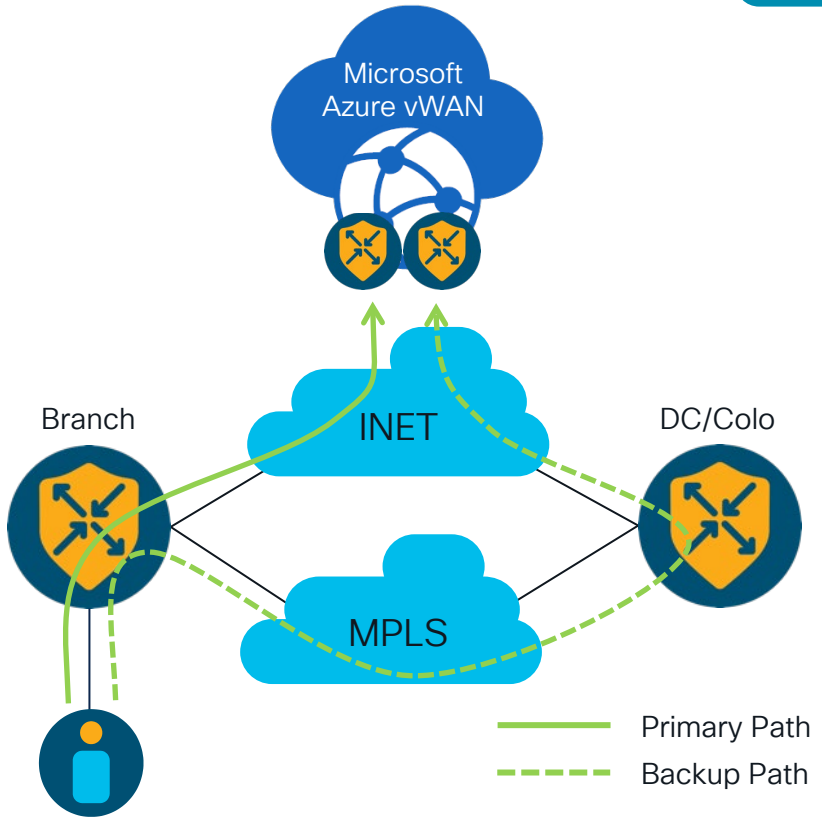
The current implementation of Cloud onRamp for IaaS (Azure) automates connectivity from SD-WAN branches and data centers to host VNETs on Azure. This architecture uses virtual Cisco SD-WAN routers deployed in transit VNETs but does not take advantage of Azure's Virtual WAN service optimizations.

Solution

Leveraging Cisco's partnership with Azure, SD-WAN v20.4 / 17.4 introduces tight native integration into Azure's Virtual Hub and VWAN. The CSR interfaces directly with the vHub and exchanges routes. The solution does not require an IPsec tunnel to achieve this. Configuration is automated through vManage.

Caveats / Prerequisites

None



Office365 Categorization

vEdge ✓

cEdge ✓

Problem

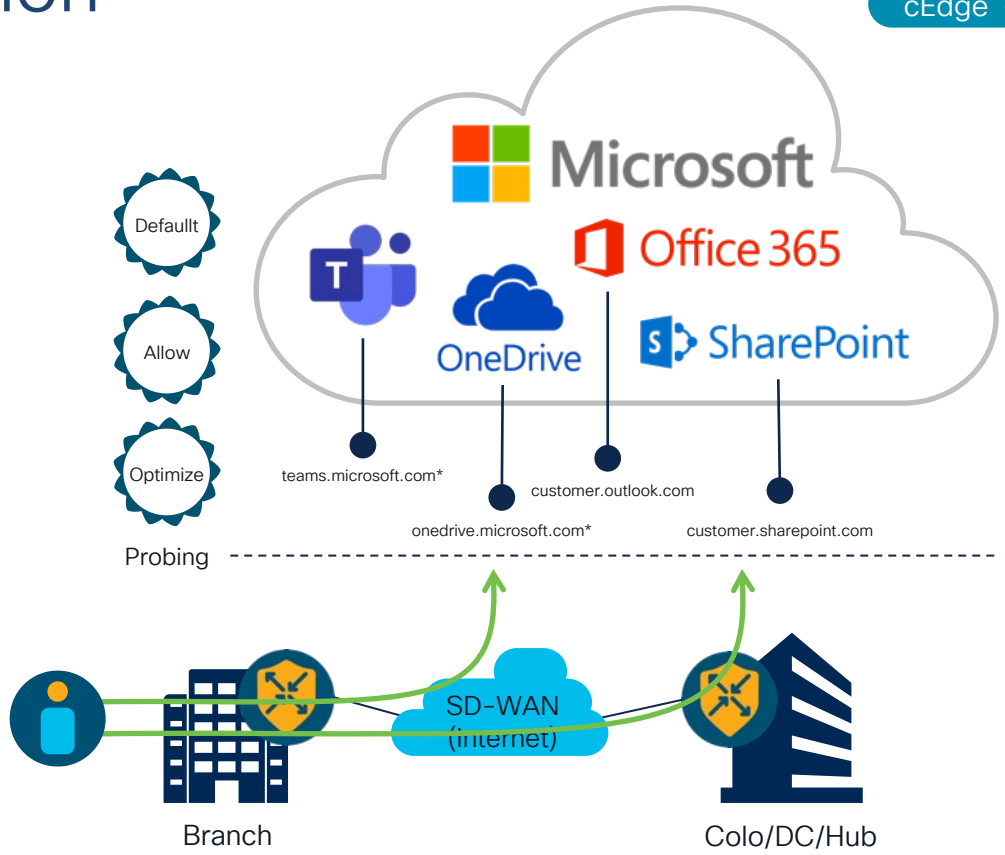
The current implementation of Cloud onRamp for SaaS (O365) does not differentiate between Office365 applications – such as Teams, Sharepoint, Mail, etc. Hence, Cisco SD-WAN cannot offer differentiated service levels for these applications.

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



Office365 Telemetry

vEdge ✗

cEdge ✓

Problem

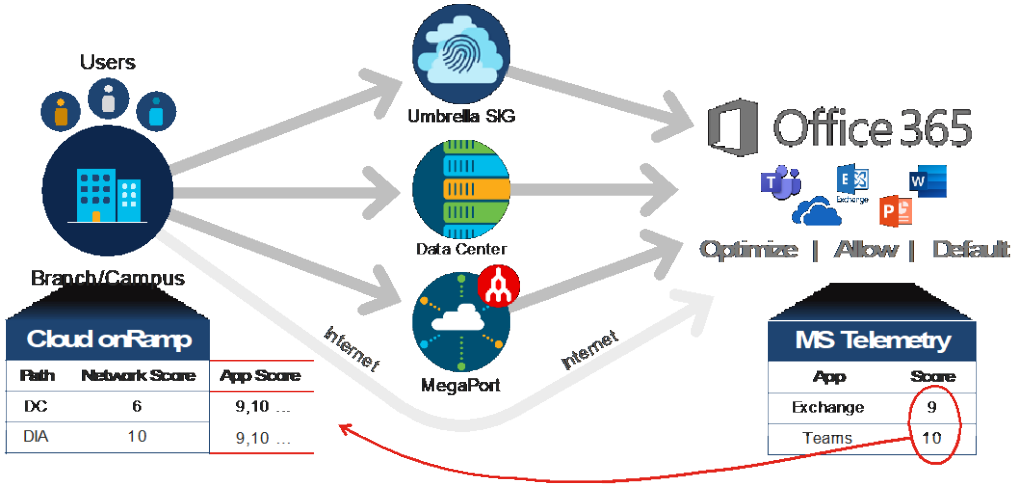
Based on App Sensitivity, Microsoft classifies O365 SaaS applications into 3 different categories (Optimize, Allow and Default). SD-WAN routers send probes and detect the best path for the appropriate SaaS app. However, this measurement is only one way. Cisco SD-WAN has no way to ingest telemetry from Microsoft

Solution

Cisco SD-WAN routers now have two data points for O365 routing decisions: Cloud onRamp for SaaS probing and Microsoft telemetry. By sending telemetry data from O365 to SD-WAN and taking this as an additional data point into application routing, Cisco SD-WAN improves O365 end user experience.

Caveats / Prerequisites

None



Demo:
Office365 Telemetry

Security Enhancements

TrustSec/SDA (SGT Transport)

vEdge ✗
cEdge ✓

Problem

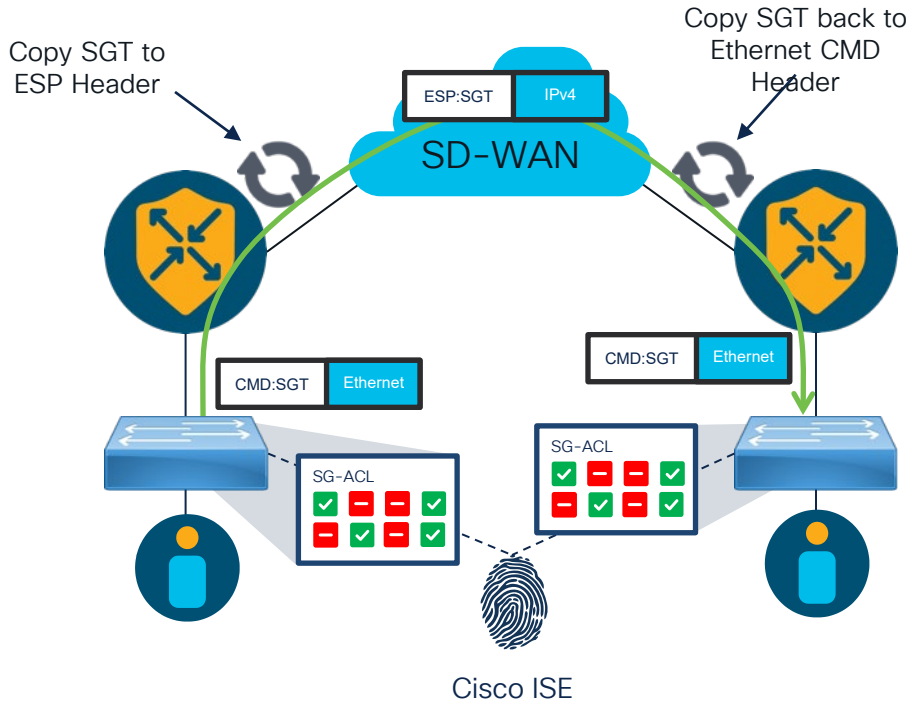
Customers choosing to adopt Secure Group Tagging technology (TrustSec/SDA) to facilitate user/group authorization throughout the network are forced to break inline propagation when traffic is transported across the SD-WAN fabric. This creates a burden (SXP) on the control-plane of SDA devices and ultimately proves to be unscalable.

Solution

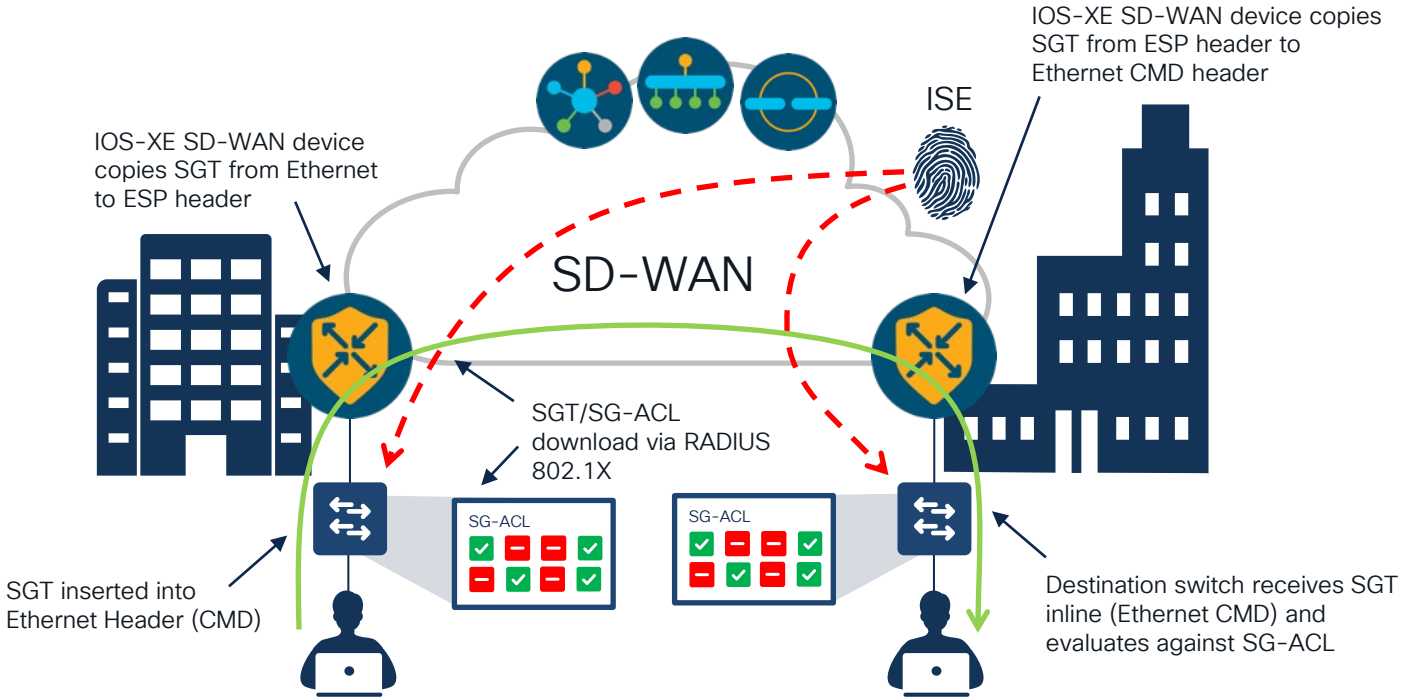
SD-WAN v20.3 and IOS-XE v17.3 now support inline SGT propagation. SGT tags from the LAN are copied to the ESP header within the SD-WAN fabric, where they can be delivered to the destination and acted on appropriately.

Caveats / Prerequisites

ISR4K, ASR1001/2X, ASR1001/2HX, CSR,
L3 interfaces only

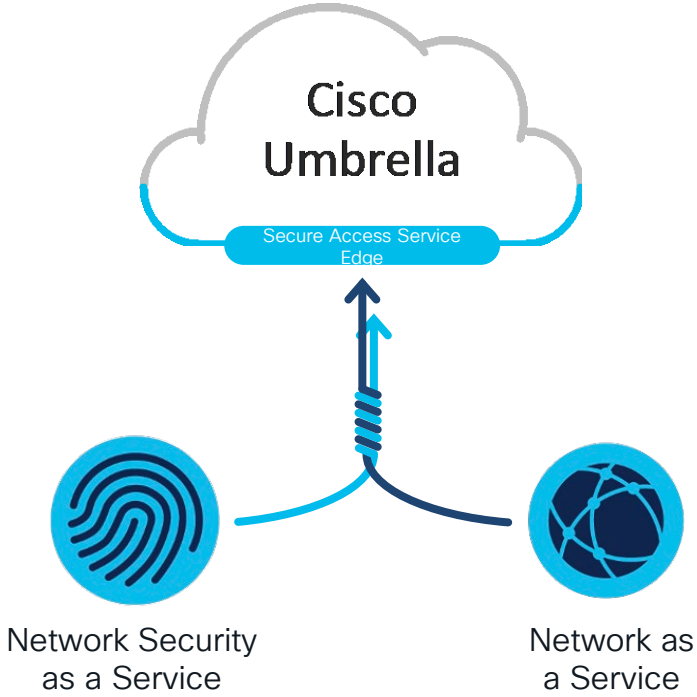


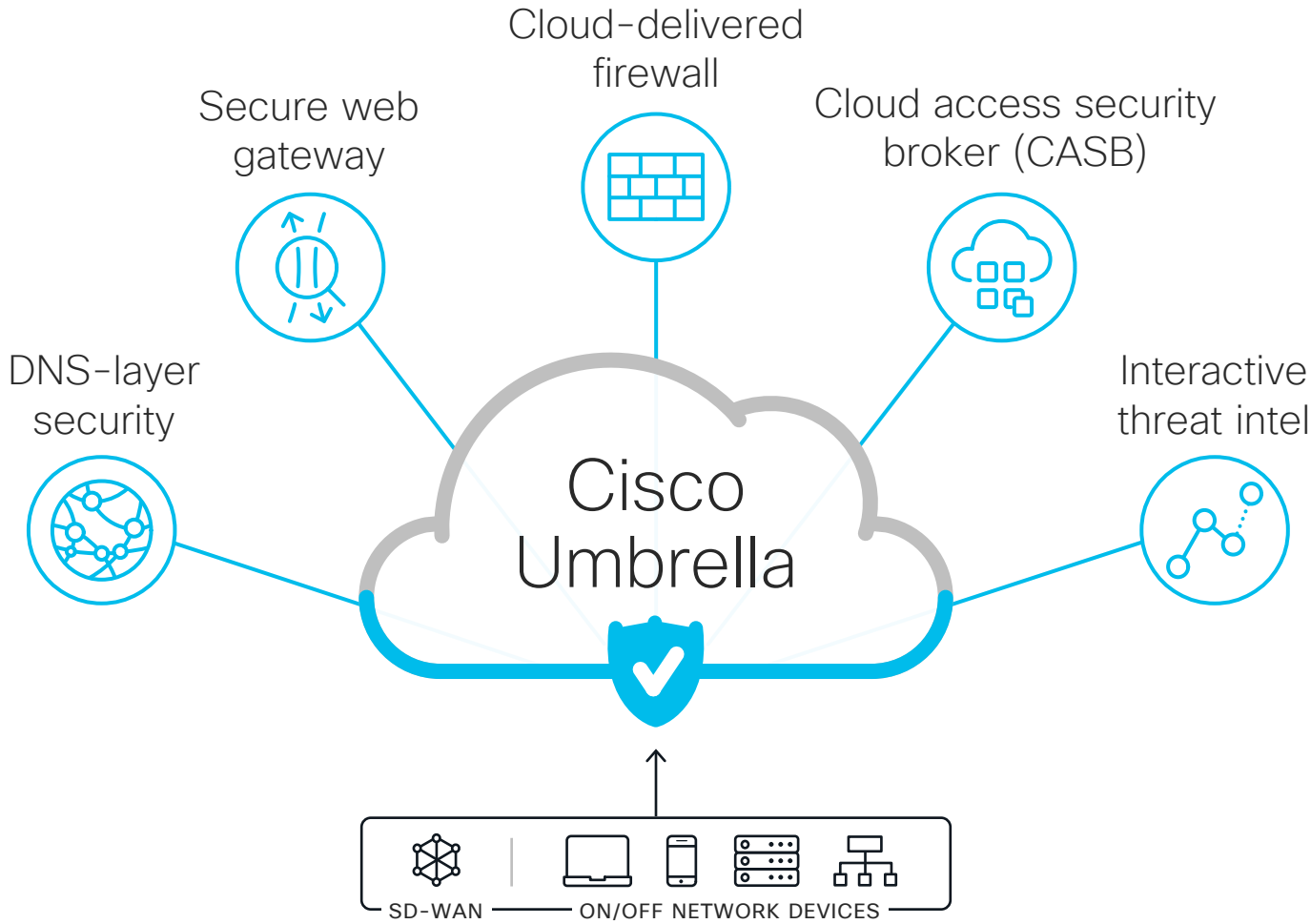
Use-Case 1: Inline Propagation



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




Cloud-delivered firewall
Secure web gateway
Cloud access security broker (CASB)
DNS-layer security
Interactive threat intel
Cisco Umbrella
SD-WAN
ON/OFF NETWORK DEVICES

New!

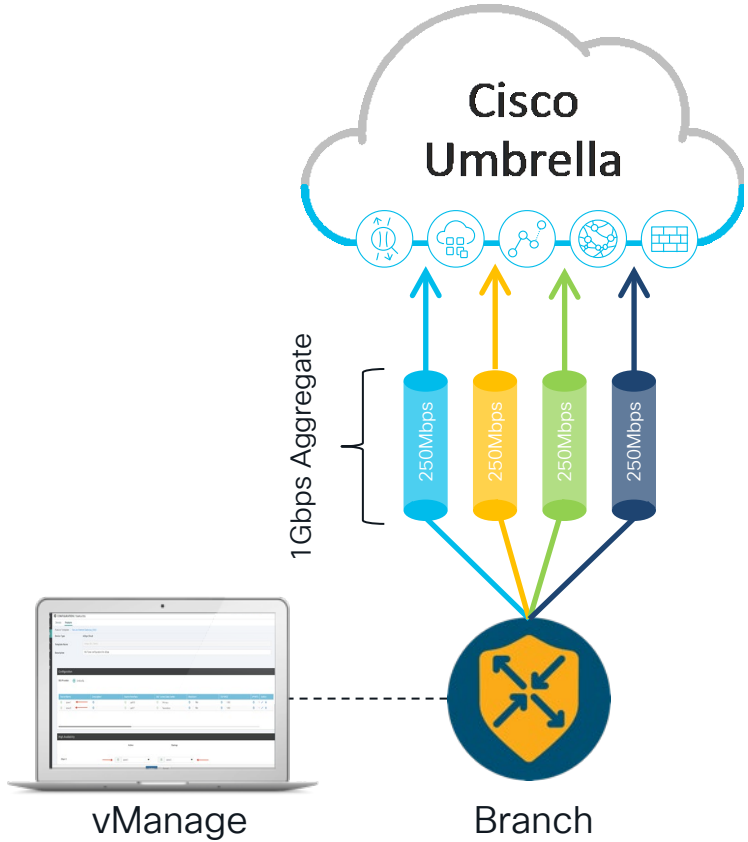
Highly Available and Highly Scalable Security

Use case

As a network admin, I need to pass 1Gbps of traffic to Umbrella SIG to maintain application performance

Feature

- Cisco SD-WAN vManage auto-templates allow up to 4 active IPsec tunnels (each operating at 250Mbps) from a single device
- Cisco SD-WAN ECMP load-balances traffic between IPsec tunnels
- Multiple tunnels can be established from a single public IP address



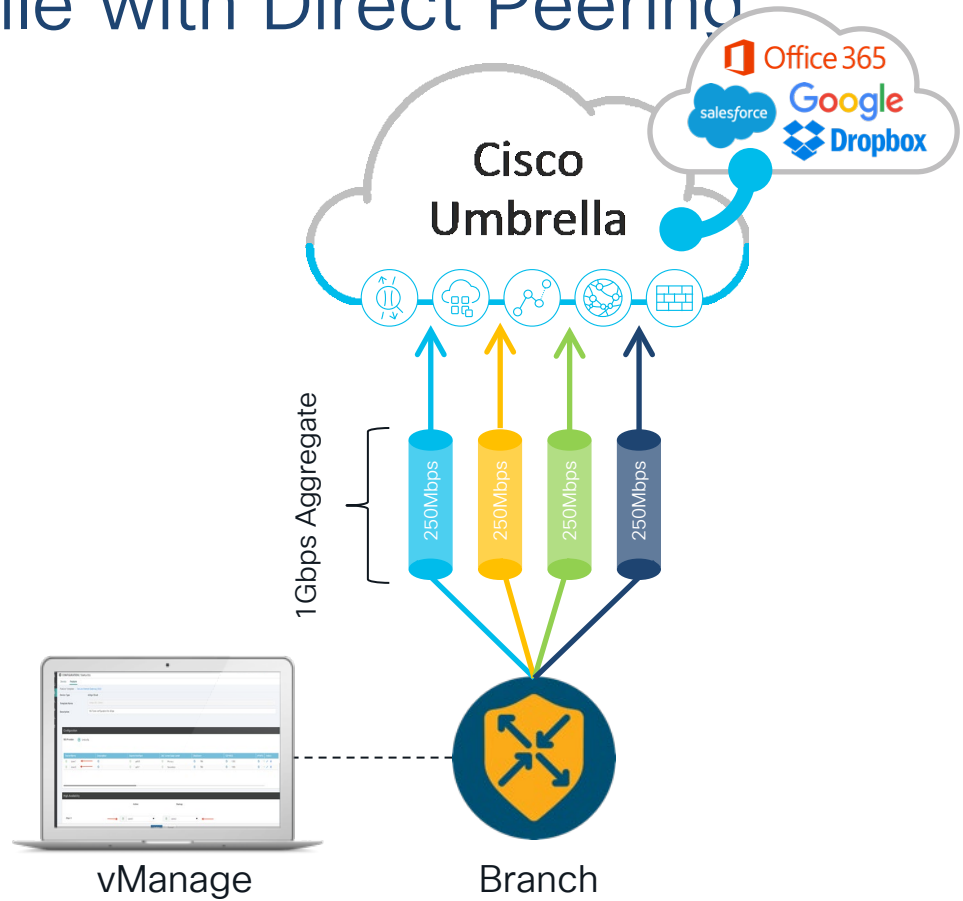
Optimize the Middle-Mile with Direct Peering

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



Selectively Route Traffic Based on Policy

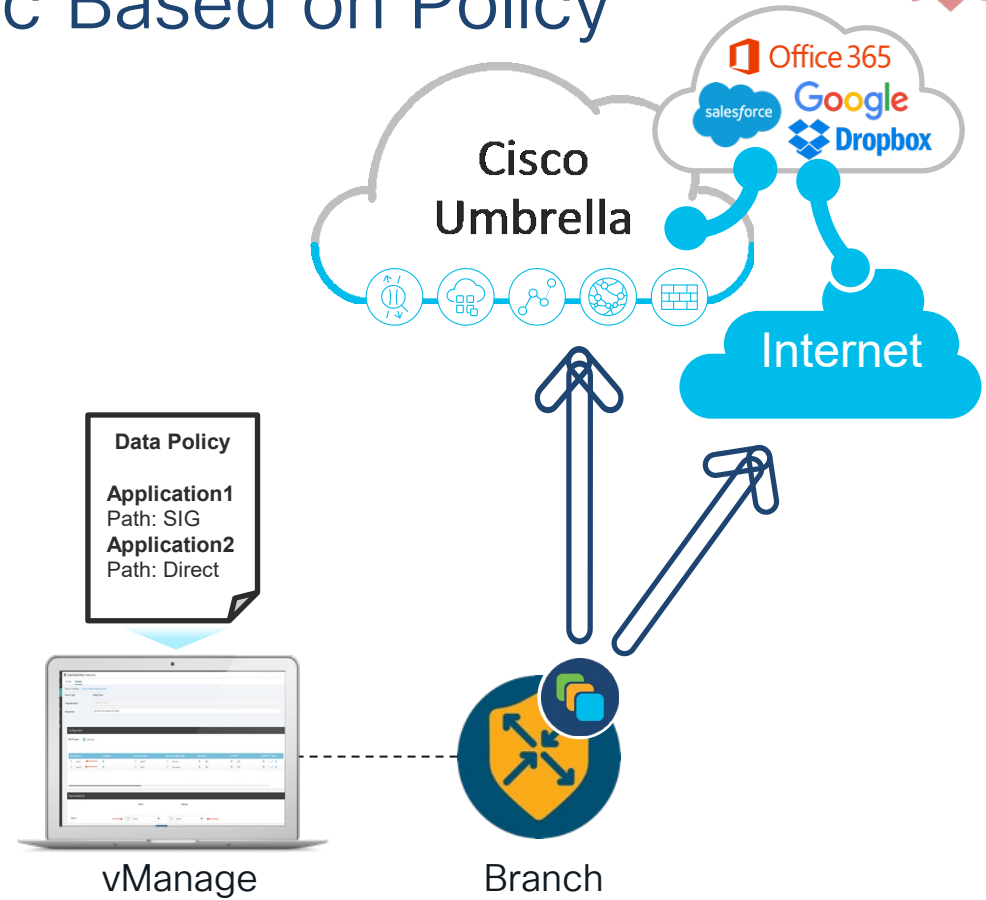
New!

Use case

As a network admin, I only want certain applications to be routed to Umbrella SIG. This allows me to optimize for my WAN capacity.

Feature

- Cisco SD-WAN v17.4/20.4 now allows customers to specifically identify traffic that should be routed Umbrella SIG
- Policy-based Routing can be enabled per branch, per VPN/VRF or organization-wide.



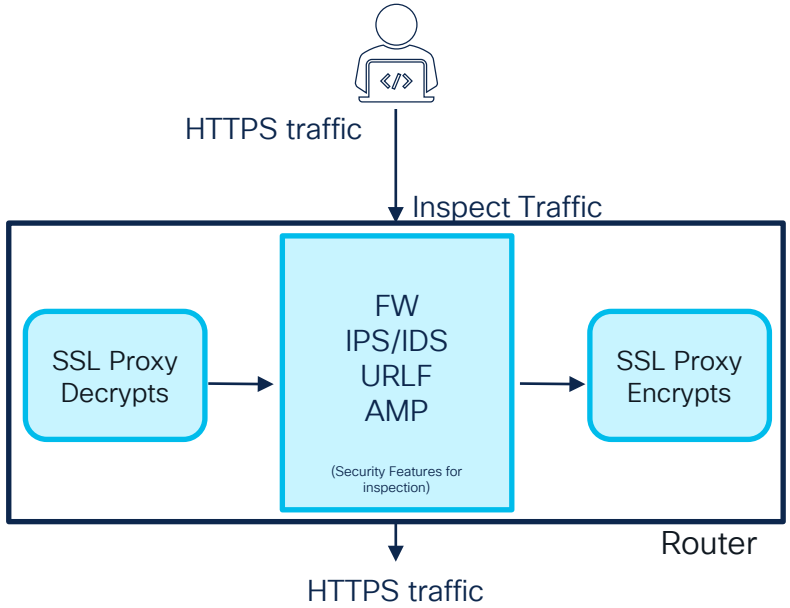
Demo:
Umbrella SIG

TLS/SSL Proxy Support with SD-WAN

SSL Proxy will help customers decrypt and inspect network traffic for malware

Cisco SD-WAN SSL Proxy…

- Intercepts/Redirects SSL traffic to ISR
- Decrypts packet and inspects
- Re-encrypts packet and sends
- Intercepts response
- Decrypts packet and inspects
- Re-encrypts packet and forwards to end user



"At the start of 2019, 87% of Web traffic was encrypted"

Mary Meeker, Internet Trends

Unified Communications

cisco Live!

Unified Communications

vEdge ✗

cEdge ✓

Problem

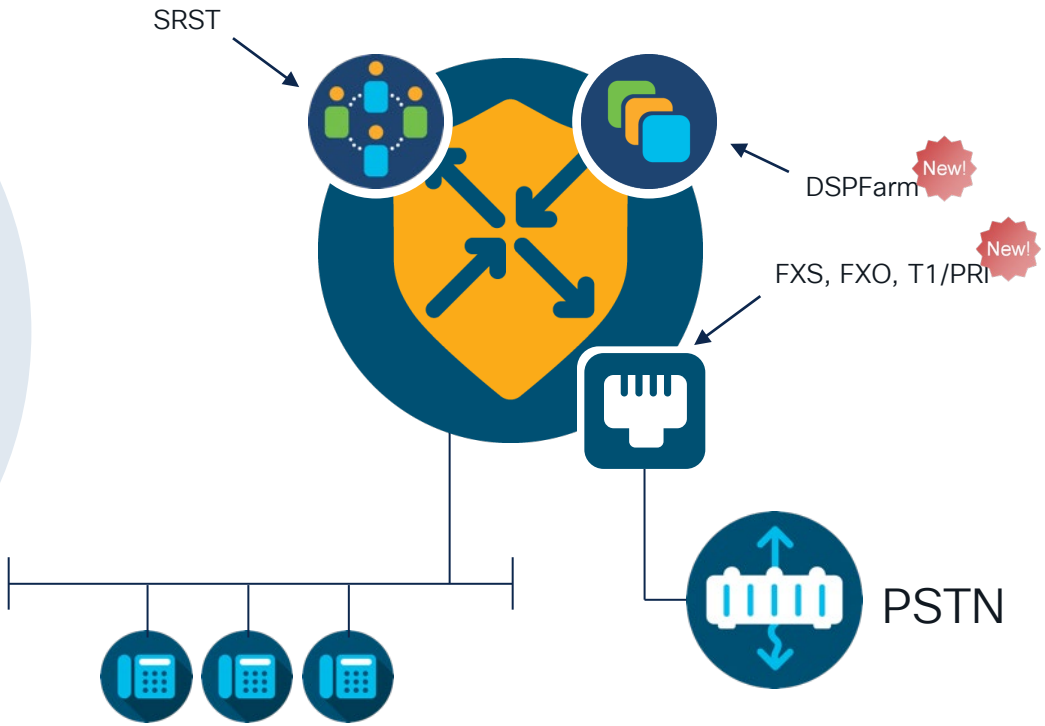
Customers seeking UC and SD-WAN integration were previously forced into a two-box solution at the branch. One box to terminate the SD-WAN fabric and another to handle UC termination. This increased cost, complexity and operational overhead.

Solution

As of v20.1 and 17.2.1 (Phase 1), Cisco SD-WAN now supports UC and SD-WAN within a single box (analog, basic SIP and SRST). Version 20.3 / 17.3 (Phase 2) adds additional capability for T1/PRI termination, DSPfarming and Fax Passthrough.

Caveats / Prerequisites

IOS-XE SD-WAN only, 4GB DRAM is supported, CUBE is not supported, H323/MGCP/SCCP are not supported, T1/PRI requires separate PVDM



FXO/FXS Support on SD-WAN

Connect to PBX or key systems, or provide off-premises connections to the public switched telephone network (PSTN)

Built-in DSP with high analog port-density support

NIM-2FXO	NIM-2FXS/4FXOP	SM-X-72FXS
NIM-4FXO	SM-X-8FXS/12FXO	
NIM-2FXSP	SM-X-16FXS/2FXO	
NIM-4FXSP	SM-X-24FXS/4FXO	

T1/E1 Voice PRI Support on SD-WAN

Packet Voice Solutions support (PBX & Central-Office Connectivity)

PSTN termination with multi calls per port: T1 PRI (23) and E1 (30)

NIM-1MFT-T1E1
NIM-2MFT-T1E1
NIM-4MFT-T1E1
NIM-8MFT-T1E1

NIM-1CE1T1-PRI
NIM-2CE1T1-PRI
NIM-8CE1T1-PRI

TIP

- T1/E1 Voice module contains onboard PVDM4 Slot
- PVDM4 Module required for T1/E1 packetization (purchased separately)
- Supported ISDN Switchtypes: QSIG, NET5, NTT, 4ESS, 5ESS, DMS100, and NI

DSPFarm Services for SD-WAN Voice

Multi party audio conferencing with (8,16, 32) participants

Save bandwidth with audio codec transcoding

Media Termination Point for IP Calls
(DTMF Conversion, SIP call bridging, Trusted Relay Point, etc.)

Form Factor:
SM-X-PVDM-500
SM-X-PVDM-1000
SM-X-PVDM-2000
SM-X-PVDM-3000

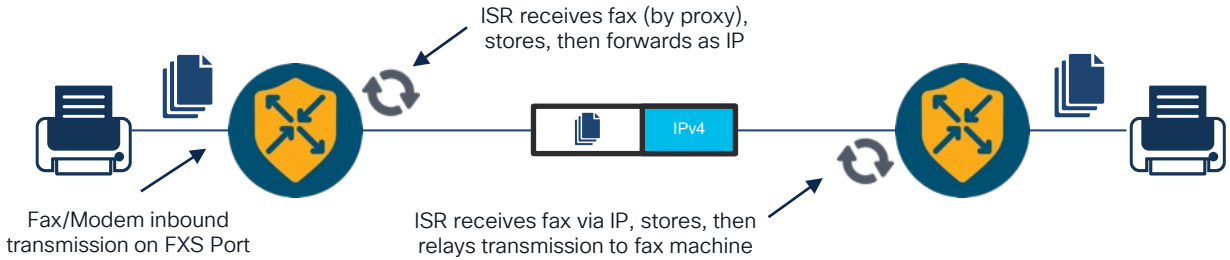
Form Factor:
PVDM4 – 32
PVDM4 – 64
PVDM4 – 128
PVDM4 – 256

Form Factor:
NIM-PVDM-32
NIM-PVDM-64
NIM-PVDM-128
NIM-PVDM-256

TIP

NIM-PVDM Modules for IP Voice Services
SM modules for high density DSP usage

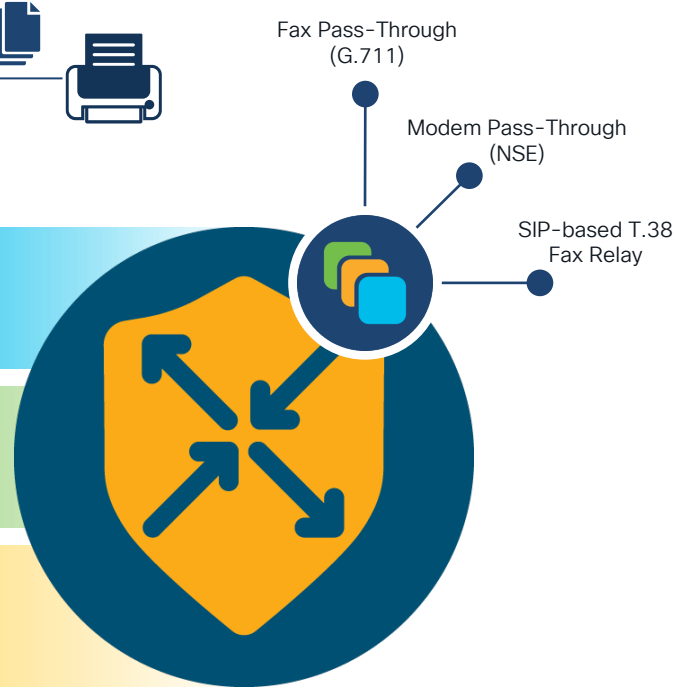
Fax/Modem Support on SD-WAN



Investment protection (use existing Fax/Modem with UC advantages)

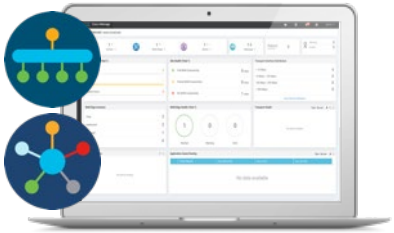
Industry standard T.38 Fax Relay support

High reliability & error-free transmission with T.38 Fax relay

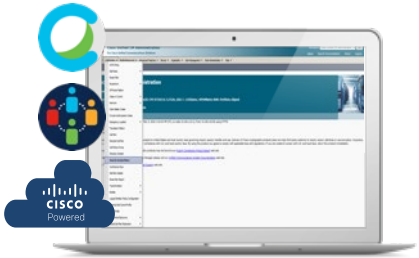


UC Configuration and Policy

vManage/vSmart



Does not participate in Call Routing
Provisions ISR for UC
- Distributed Dial Plan (SIP Dial Peer)
- Call Manipulation (Translation)
- Media/Codec Selection
- SRST



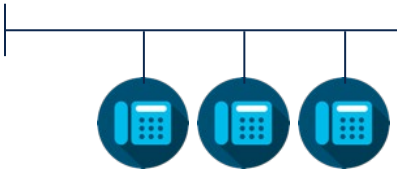
Call Control

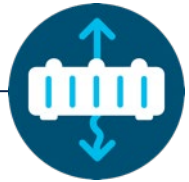
Participates in Data Plane
Provides extended Dial Plan support
- Enterprise call routing
- Media Termination
- SIP

Does not invoke configuration change

Management/Control Plane

Data Plane

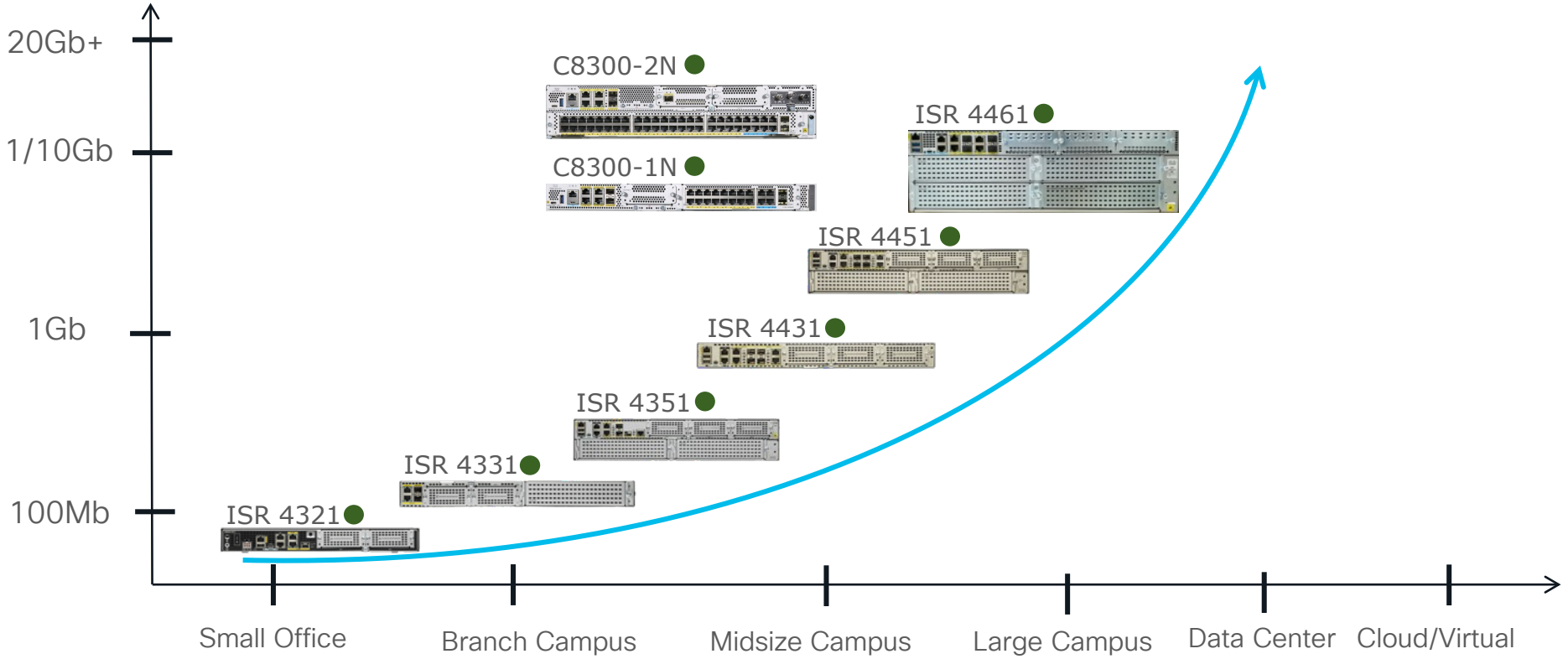




PSTN

ISR UCM Datasheet

UC Portfolio Summary



Demo:
Unified Communications

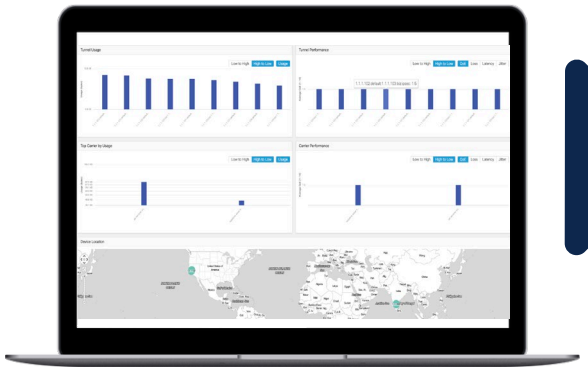
vAnalytics

vAnalytics Release 2.0

Network Performance	Visibility into network KPIs – loss, latency, jitters, and bandwidth consumption across WAN
Application Insights	Multi-layer insights correlating application behavior (QoE) with the underlying network conditions
Granular Statistics	Site-level, VPN-level, and Device-level statistics; Top Talkers, Top Flows
Improved experience	Refreshed GUI for easy navigation; Secure login with multi-factor authentication (MFA)

Improved overall network visibility and insights

vAnalytics: Translate Raw Data into Intelligent Insights

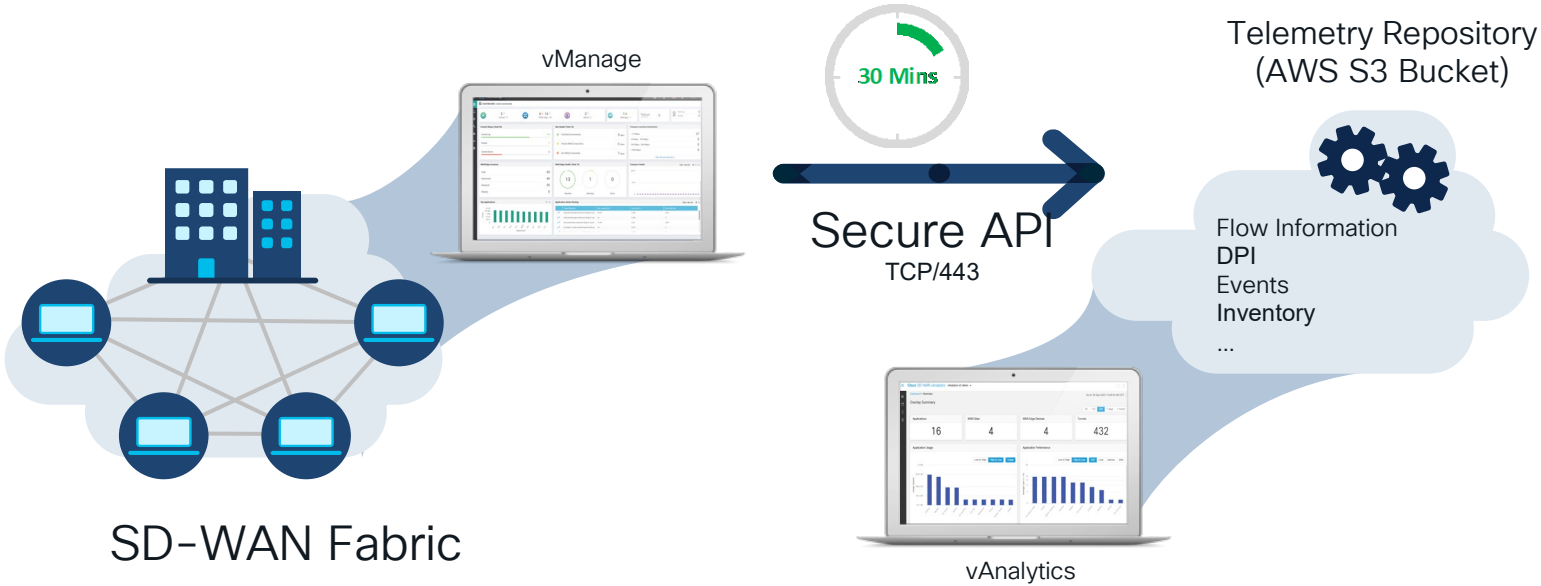


Intuitive Visualization of Network KPIs and historical trends

Correlate Application behavior (QoE) with the network conditions

Leverage Insights for better planning

vAnalytics Architecture



On-Prem or Cloud-Hosted SD-WAN

Cloud-Hosted Analytics

Demo:
vAnalytics 2.0

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive