Cisco SD-WAN and Secure Access Service Edge (SASE) Cloud Architecture Independent Assessment

DR201102B

November 2020

Miercom

Miercom.com

Contents

1.0 Executive Summary

Miercom was engaged by Cisco Systems to independently validate the functionality and performance of its SD-WAN solution with SASE architecture, designed to integrate applications in the cloud with branch site infrastructure for optimized, secure and scalable delivery for increased quality of experience. SD-WAN brings a centralized, software-defined approach to network management which intelligently automates, simplifies, and controls to yield high performance.

Testing assessed the impact of various configuration settings and deployment options of the throughput performance of the SD-WAN solution in public and private cloud environments. By comparing Cisco SD-WAN to traditional methods, we found this solution offered significant benefits for the modern branch network.

Key Findings and Observations:

- New capabilities are constantly being introduced in Cisco SD-WAN, making Cisco the thought leader in the SD-WAN market
- Cloud onRamp provides cost-effective, scalable SaaS capabilities for cloud applications with less latency and loss than traditional WAN link performance – using automated, real-time path routing for the highest efficiency, security and quality. Integration with Microsoft 365 is one of the key differentiators.
- onRamp for Multi-Cloud, a feature in vManage, balances workloads and provides controlled cloud access (e.g. AWS and Azure) – provisioning 200 branch sites in just 10 minutes. Native Integration into Microsoft Azure vWAN provides unique simplification and scale.
- Integrates with SDCI providers to offer customers a guaranteed underlay connection to connect worldwide branches to IaaS workloads and SaaS applications
- Integrates with Cisco Umbrella Secure Internet Gateway (SIG) for heightened application performance and security without exposing traffic to the vulnerabilities of the public Internet.
- Only SD-WAN vendor on the market to provide turnkey, single-box solution with native Unified Communications (UC) capabilities to reduce cost and operations.
- Leverages native UC in the cloud to extend SD-WAN fabric to nearby colocations – optimizing connections, such as Webex calling and video streaming, for reduced hop count, lower latency, and higher quality end user experience.
- SD-WAN Overlay Management aggregates routers to forward multicast streams, optimizing WAN bandwidth and enforcing centralized policies for up to 8,000 simultaneous multicast groups – four times the typical network scenario – with no loss for 128 and 1500-byte frames.
- vManage provides webhooks for optimized alarm management and monitoring with application-aware routing and data policies to avoid aggressive and wasteful alerts
- Automated integration of Cisco Meraki with Viptela SD-WAN allows for scalable API-based routing of LAN traffic over IPsec tunnels, using templates that reduce downtime, manual operations, human error and associated costs.

Based on the results of the testing, we proudly award the ***Miercom Performance Verified*** certification to Cisco's SD-WAN solution.

Robert Smithers

CEO, Miercom

2.0 Product Overview

2.1 SD-WAN Benefits

A typical Wide Area Network (WAN) connects branch users to applications hosted in data centers via MPLS, Metro Ethernet and Internet. As applications become more cloud-based, networks benefit from adopting Software as a Service (SaaS) and Infrastructure as a Service (IaaS). With traditional WAN, the data center introduced high latency, congestion and no resiliency during outages. Limited scalability was offered, as networks were forced to constantly upgrade WAN capacity. WAN not only reduces performance and degrades the user experience; it also makes security compliance more complicated.

Software-defined WAN (SD-WAN) solutions are part of a centralized software-defined network approach to management where the infrastructure is separate from the applications. This allows for increased automation, simplification, provisioning, monitoring and troubleshooting. SD-WAN intelligently avoids latency, congestion and outages using a bird’s eye view of the network.

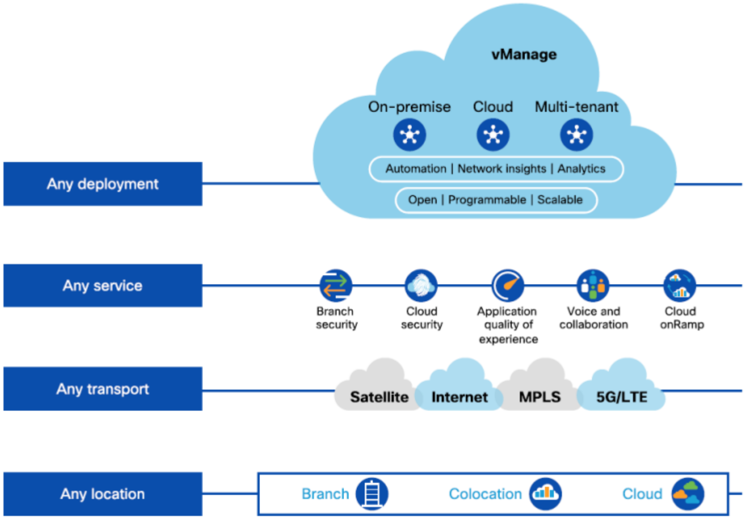
There are four main goals of SD-WAN:

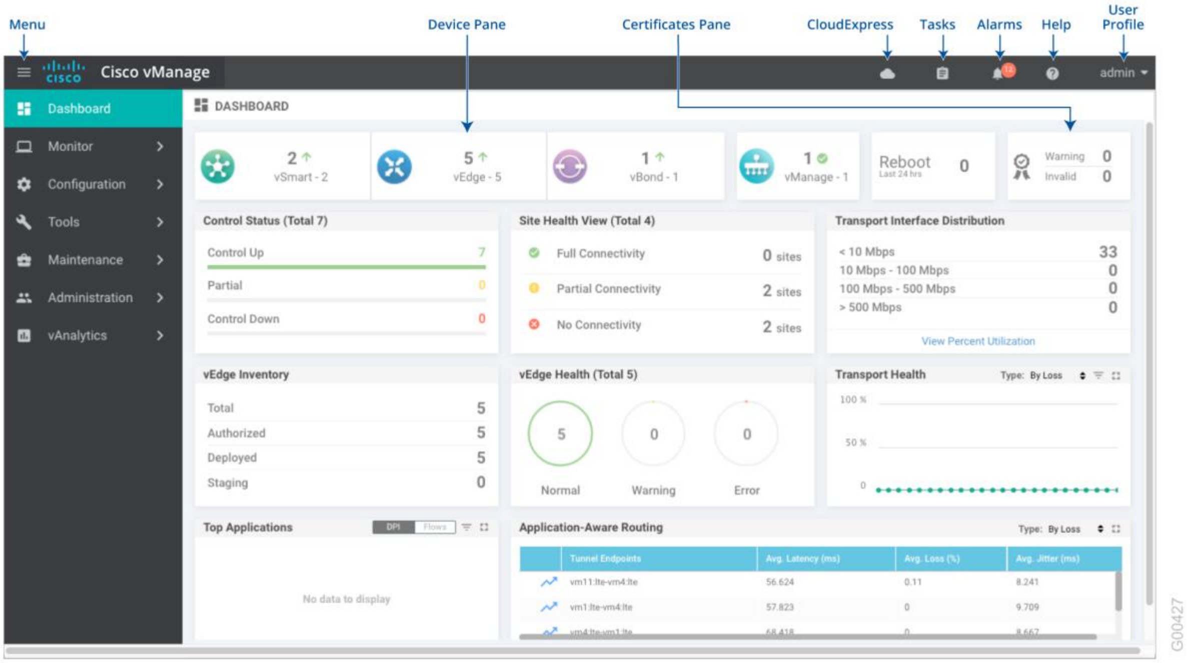
1. Increase bandwidth via backup links, dynamic load-balancing and horizontal scaling
2. Deliver faster cloud access using direct branch-to-Internet access as well as direct attachment to customer cloud infrastructure through the customer SD-WAN fabric.
3. Reduce operational and management costs through centralized management
4. Lower connectivity costs by switching MPLS to Internet or LTE, without compromising on security or reliability

2.2 Cisco SD-WAN Cloud

Cisco SD-WAN is a cloud-scale architecture that aims to optimize application user experience, provide flexible multi-layered security on-premise or in the cloud, and simplify scalability using end-to-end policies from the user to the application over thousands of sites.

Cisco vManage is a Graphical User Interface (GUI) where administrators and operators can configure, provision, troubleshoot and monitor activity centrally in the whole network including multiple clouds. vManage offers two dashboards: single-tenant and multi-tenant.





2	vSmart - 2
5	vEdge - 5
1	vBond - 1
1	vManage - 1
Reboot Last 24 hrs	0
Warning	0
Invalid	0

Control Status (Total 7)

Control Up	7
Partial	0
Control Down	0

Site Health View (Total 4)

Full Connectivity	0 sites
Partial Connectivity	2 sites
No Connectivity	2 sites

Transport Interface Distribution

< 10 Mbps	33
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

vEdge Inventory

Total	5
Authorized	5
Deployed	5
Staging	0

vEdge Health (Total 5)

Normal	Warning	Error
5	0	0

Transport Health Type: By Loss

100 %
50 %
0

Top Applications

No data to display

Application-Aware Routing Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
vm11:lte-vm4:lte	56.624	0.11	8.241
vm1:lte-vm4:lte	57.823	0	9.709
vm4:lte-vm1:lte	68.418	0	8.667

Cisco vManage is a snapshot of all hardware inventory, overlay network status, router information and more. All parts of the dashboard are interactable, meaning you can drill down for further details.

Cisco WAN Edge routers establish the network fabric and forward traffic. They can be physical and virtual, and they are selected based on the site's connectivity, throughput and functional needs. The Edge routers form Internet Protocol Security (IPsec) tunnels between them – forming the SD-WAN overlay. There is also a control channel between the routers to receive configuration, provisioning and routing information.

Together, these elements form part of the Cisco SD-WAN Fabric which offers the following benefits:

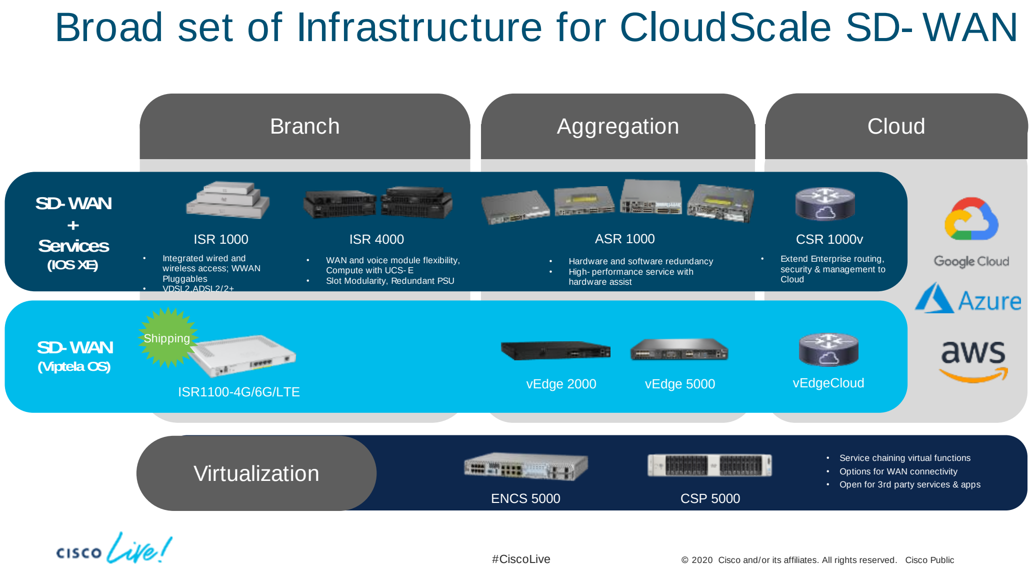
Cisco SD-WAN Advantages:

- **Secure Automated WAN**
  Enables enterprises to migrate away from traditional, operationally complex WANs that have many silos to a software-based, agile WAN with robust security features.
- **Application Performance Optimization**
  Designs a global network where the critical enterprise applications always maintain the highest service level agreements (SLAs) and guaranteed performance, even during problems in the network.
- **Secure, Direct Internet Access (DIA)**
  Enable branch offices to connect to Internet and cloud applications for fast application performance and comprehensive protection against attacks.

- **Branch Multi-cloud Access**
  Achieve rapid migration to the cloud with integrated Cloud onRamp capabilities for SaaS and public cloud like AWS and Azure, as well as private cloud using Cloud onRamp for Colocation.
- **Regional Hub Multi-cloud Access**
  Consolidate regional infrastructure closer to cloud applications within colocation hubs using architecture based on Cisco virtualized network functions (VNF).

2.3 SD-WAN Hardware Overview

View all Cisco routers, or compare SD-WAN platforms—a Gartner peer insights customers' choice—using the Cisco Router Selector: https://www.cisco.com/c/en/us/products/routers/router-selector.html?oid=caten020272&sd_wan=cisco_sd-wan



Broad set of Infrastructure for CloudScale SD- WAN

Branch | Aggregation | Cloud

SD- WAN + Services (IOS XE)

ISR 1000
- Integrated wired and wireless access; WWAN Pluggables
- VDSL2,ADSL2/2+

ISR 4000
- WAN and voice module flexibility, Compute with UCS- E
- Slot Modularity, Redundant PSU

ASR 1000
- Hardware and software redundancy
- High- performance service with hardware assist

CSR 1000v
- Extend Enterprise routing, security & management to Cloud

SD- WAN (Viptela OS)

Shipping

ISR1100-4G/6G/LTE

vEdge 2000

vEdge 5000

vEdgeCloud

Virtualization

ENCS 5000

CSP 5000

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

#CiscoLive

Please refer to the Cisco SD-WAN hardware compatibility matrix
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/compatibility-matrix.html

2.4 SD-WAN Licensing

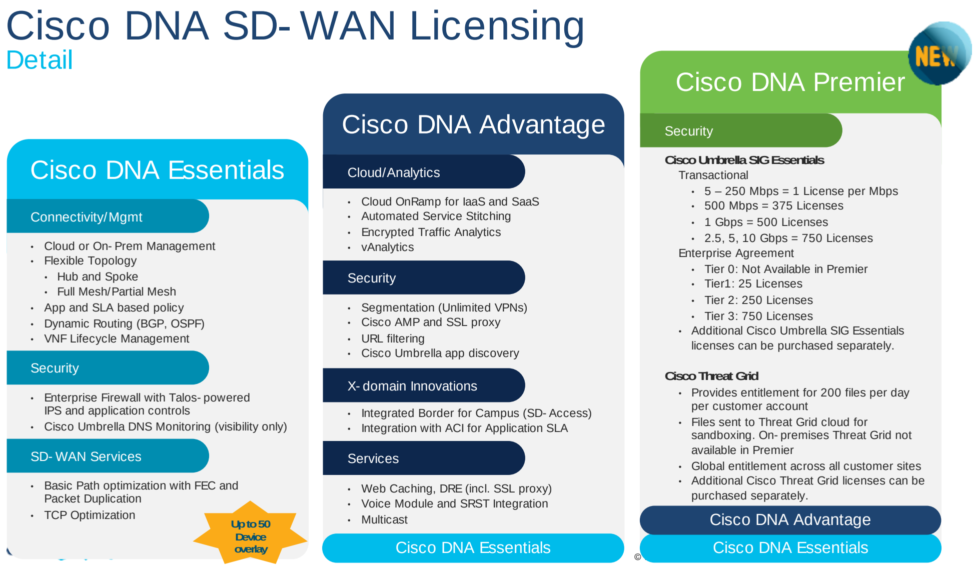
Find out about the software licensing subscriptions available for Cisco Digital Network Architecture (DNA) for SD-WAN and Routing: https://www.cisco.com/c/en/us/products/software/dna-subscription-wan/index.html

Cisco's intent-based WAN offers an entirely new approach to manage and operate your WAN infrastructure. It provides the following key benefits:

- Makes your network ready for SaaS applications
- Simplifies your WAN architecture and makes it easier to manage, operate, and consume
- Balances security and application experience with direct Internet access at the branch

Benefits of a software subscription for SD-WAN and Routing

- The latest innovations through simple subscription tiers
- Available across the portfolio
- Flexibility to choose on-premises or cloud management
- Easy license portability across premises and cloud
- Easy upgrade across tiers
- Software Support Service (SWSS) included



Cisco DNA SD- WAN Licensing

Detail

Cisco DNA Essentials

Connectivity/Mgmt

- Cloud or On- Prem Management
- Flexible Topology
  - Hub and Spoke
  - Full Mesh/Partial Mesh
- App and SLA based policy
- Dynamic Routing (BGP, OSPF)
- VNF Lifecycle Management

Security

- Enterprise Firewall with Talos- powered IPS and application controls
- Cisco Umbrella DNS Monitoring (visibility only)

SD- WAN Services

- Basic Path optimization with FEC and Packet Duplication
- TCP Optimization

Up to 50 Device overlay

Cisco DNA Advantage

Cloud/Analytics

- Cloud OnRamp for IaaS and SaaS
- Automated Service Stitching
- Encrypted Traffic Analytics
- vAnalytics

Security

- Segmentation (Unlimited VPNs)
- Cisco AMP and SSL proxy
- URL filtering
- Cisco Umbrella app discovery

X- domain Innovations

- Integrated Border for Campus (SD- Access)
- Integration with ACI for Application SLA

Services

- Web Caching, DRE (incl. SSL proxy)
- Voice Module and SRST Integration
- Multicast

Cisco DNA Essentials

Cisco DNA Premier

Security

Cisco Umbrella SIG Essentials

Transactional
- 5 – 250 Mbps = 1 License per Mbps
- 500 Mbps = 375 Licenses
- 1 Gbps = 500 Licenses
- 2.5, 5, 10 Gbps = 750 Licenses

Enterprise Agreement
- Tier 0: Not Available in Premier
- Tier1: 25 Licenses
- Tier 2: 250 Licenses
- Tier 3: 750 Licenses
- Additional Cisco Umbrella SIG Essentials licenses can be purchased separately.

Cisco Threat Grid

- Provides entitlement for 200 files per day per customer account
- Files sent to Threat Grid cloud for sandboxing. On- premises Threat Grid not available in Premier
- Global entitlement across all customer sites
- Additional Cisco Threat Grid licenses can be purchased separately.

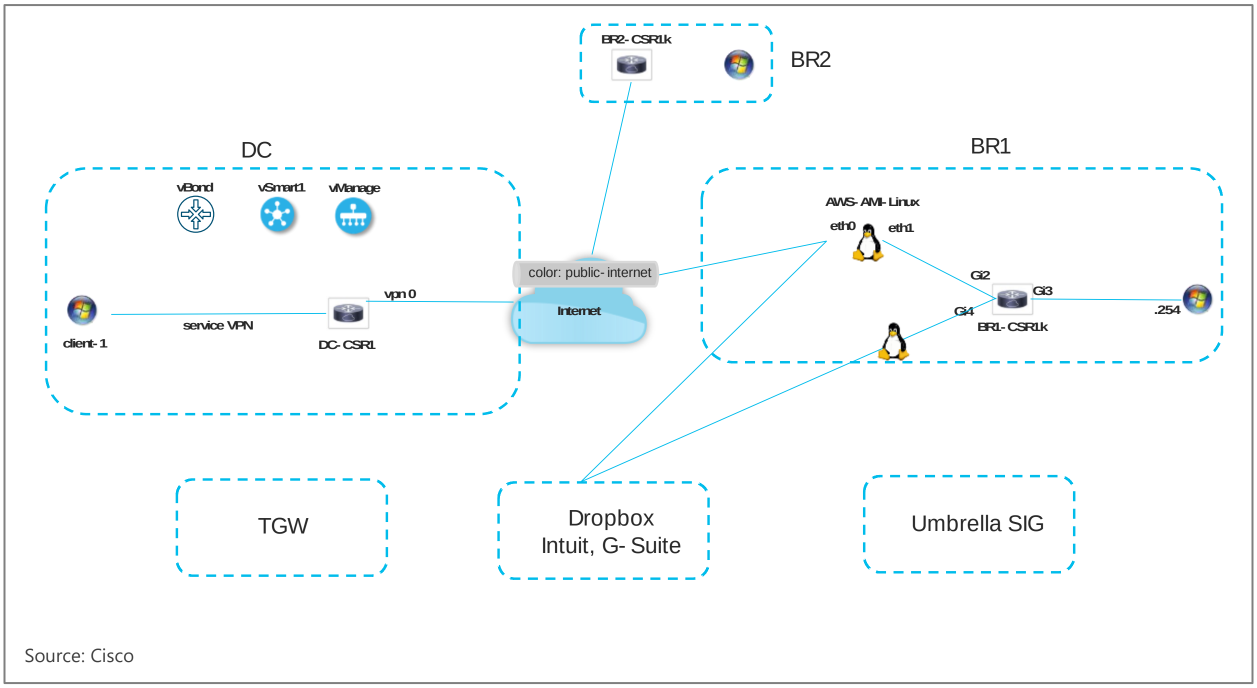
Cisco DNA Advantage

Cisco DNA Essentials

3.0 How We Did It

Our hands-on testing used a real-world network environment to challenge the SD-WAN solution with a realistic assessment of performance features and capabilities. The following topology was used for all performed tests.

Test Bed Diagram



Source: Cisco

Test Tools

Device under Test (DUT)	
Cisco SD-WAN Solution	vManage Software Version 20.3 IOS XE SD-WAN Software Version 17.3

Test Tool Descriptions	
Spirent Test Center Version 5.01.8216.0000	A high-speed test tool to generate products and services for testing high-density network scenarios. Traffic flow emulation allows for validation of scalability scenarios for small, medium and large network sizes.

Use cases for the following features were tested:

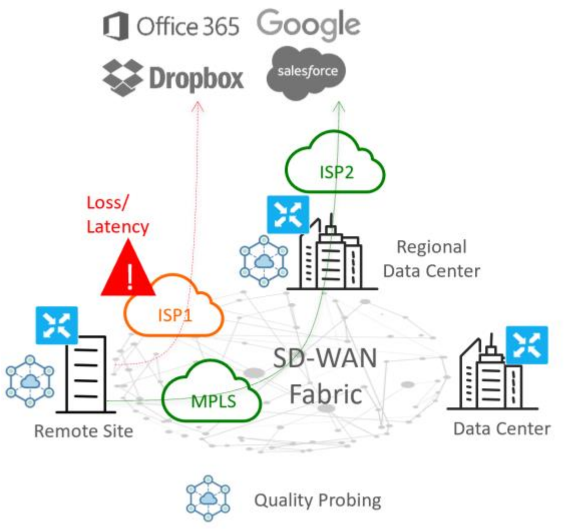
- Section 4.0: Cloud – SaaS and IaaS
- Section 5.0: Cloud – SASE (Service Access Service Edge)
- Section 6.0: SD-WAN and Unified Communication (UC)
- Section 7.0: SD-WAN and Multicast
- Section 8.0 SD-WAN Programmability

4.0 Cloud: SaaS and IaaS

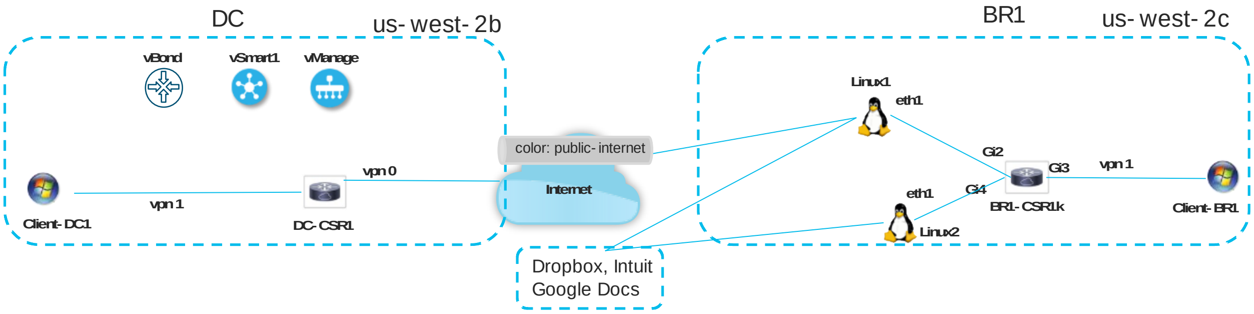
4.1 SaaS Optimization

Traditional WAN architecture is no longer relevant when cloud-based applications are used. The infrastructure is not designed to access the cloud – backhauling traffic becomes too expensive, and latency degrades the user experience. As more SaaS applications are adopted (e.g. Office 365, Salesforce), legacy networks become too complex to handle and administrators no longer have full visibility of performance metrics.

Cisco SD-WAN Cloud onRamp provides SaaS capabilities for cloud-based applications by continually measuring performance for multiple paths from branch to cloud. These paths are scored for their quality of experience, on a scale of 0 to 10 – 10 being best performance. The fabric uses automated, real-time path routing to dynamically find the best-performing way for users at the branch site to access the cloud SaaS application.



For this test, we ran a SaaS probe over two direct internet (DIA) links (Gi2 and Gi4). We then degraded one link with 40 percent degradation to demonstrate the intelligent path routing of the Cisco SD-WAN Cloud onRamp to switch to a better performing link.

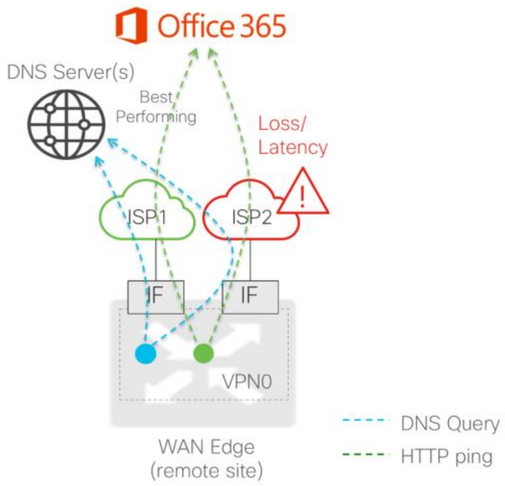


The remote branch site is attempting to access the Dropbox application. Traditionally the remote site would route through the data center to the Dropbox using one link (MPLS), and another link (Internet) to the Regional Data Center to the Dropbox application.

Using the traditional approach, performance can change throughout the day, varying in latency and loss. The user should not feel any change to their quality of experience. Cisco finds the best route available through SaaS optimization.

Using two links (ISP1 and ISP2) to the application, we began Quality Probing; we sent HTTP probes to the IP address and recorded loss and latency based on the response for each link. vQoE Scores (1-10) are recorded. The dynamic path selection was performed over a block of 12 minutes, in 6 iterations of 2 minutes each. This algorithm achieves a balance between ISPs to avoid flip-flopping between each DIA to maintain quality. vQoE Scores are color coded; red for under 5, yellow for 5-8 and green for 8-10.

We introduced delay and loss by impairing the links via Linux virtual machines to observe link switching for optimal SD-WAN experience with SaaS.



vManage was used to apply a template-based configuration for the routers to enable Cloud onRamp for SaaS. By clicking on the application, the administrator can view the vQoE score and see a timeline history for the difference in quality between ISP1 and ISP2 over the last 7 days. ISP2 was the better link as we have introduced impairment in ISP1. This was observed in the CLI via SD-WAN Cloud Express and, graphically, in vManage.

ISP	Packet Loss	Latency	vQoE
ISP1	0.44%	97.83 ms	5.02
ISP2	0.00%	22.12 ms	10

Then we removed ISP1 impairment and introduced delay on ISP2. Using the CLI via CSR1000v router, we sent a ping to the source of each link. There was no observed difference on the ISP1 link, but the ISP2 link increased in latency.

ISP	Initial Delay	Added Delay
ISP1 (Gi2)	25 ms	0 ms
ISP2 (Gi4)	13 ms	308 ms

Using the CLI via Cloud Express, we saw a Dropbox latency of 13ms for ISP2 (Gi4) before the switch. After 2 minutes, we saw a switch to ISP1 (Gi2), and it was successful.

The Cisco Advantage

Traditional Approach to SaaS Access:

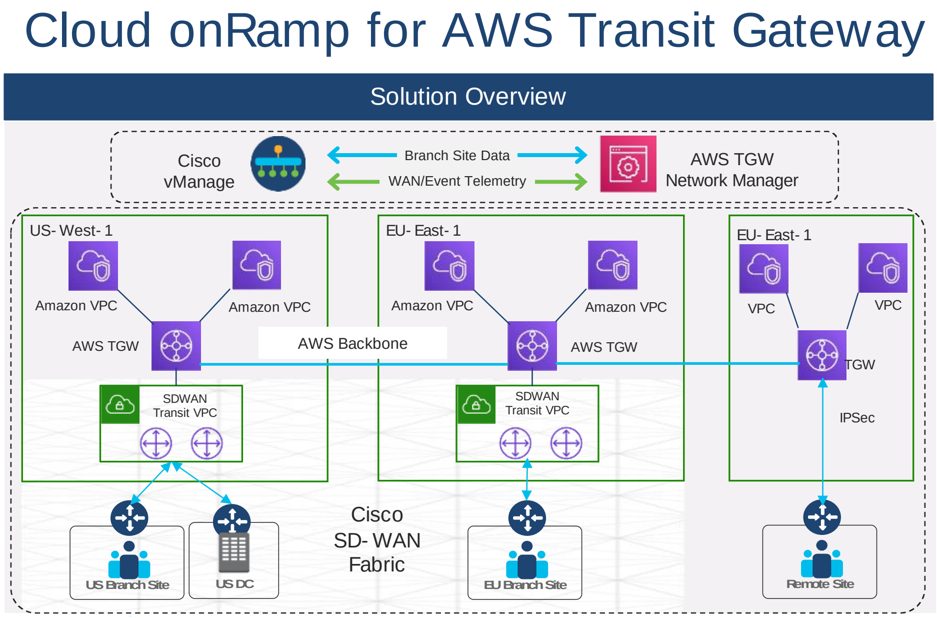
- Traffic backhauled through data center
- No optimal user experience
- Expensive MPLS transport

Benefits of Cloud Approach to SaaS Access:

- Automated, real-time path routing for best-performance path to cloud application
- Scalable optimization of the SaaS applications lowers total cost
- Full performance and quality visibility metrics
- Traffic security embedded at branch or cloud-delivered

4.2 IaaS Automation with AWS TGW

Branch deployments can be connected to each other and the data center using Cisco SD-WAN. It is common for on-premise applications to transition to cloud-based services for easier deployment and cost-savings. To accommodate this, the administrators must connect their infrastructure to the public cloud. The challenge is to automatically and securely connect these entities in a secure and automated way.

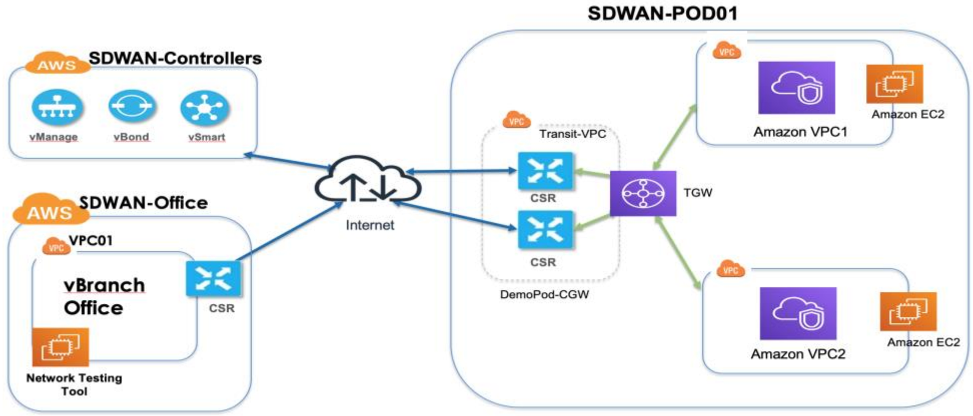


This test case looks at the integration between the Cisco SD-WAN solution and Amazon Web Services (AWS) Transit Gateway (TGW). We observed the use of Cisco Cloud onRamp for Multi-Cloud, a feature offered by vManage for connecting branch workloads in AWS.

The Cisco Advantage

Often, there are multiple departments (e.g. engineering, HR, marketing) sitting on the branch side within separate virtual networks accessing the same cloud-based application. Application access is segmented based on these department virtual networks. This process is normally done manually, but this requires costly and time-consuming training of staff for each application. Alternatively, customers will run multiple Virtual Private clouds to achieve this segmentation.

Cisco SD-WAN Cloud is a cloud agnostic solution that automatically interconnects branch networks to cloud-based applications, supporting multi-cloud use cases.

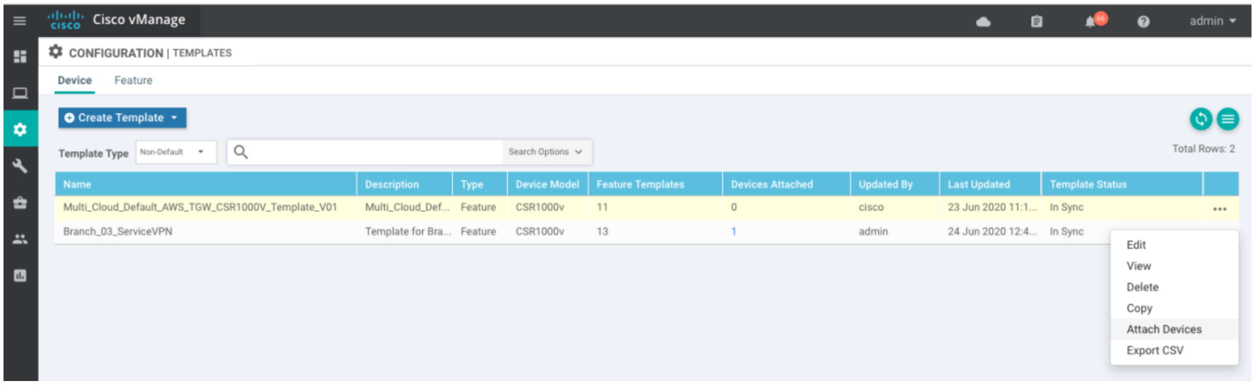


In the real-world scenario we tested, a customer has 200 branch locations across the globe with AWS infrastructure in different regions. Manually, this would be a complex, expensive process to implement. Cisco SD-WAN asks which VPC (application) to map to a specific branch network using a table-map selection tool in vManage. This then automatically connects branch networks to the cloud-based application Virtual Private Cloud (VPC) without the need to provision in AWS (or other cloud applications) to combine.

Key components of Integration:

1. Cisco Cloud onRamp for Multi-Cloud extends the fabric of the Cisco SD-WAN overlay network into public cloud instances, allowing branches with Cisco SD-WAN routers to connect directly to public-cloud application providers.
2. Cisco SD-WAN virtual-form-factor router (Cisco Cloud Services Router "CSR" 1000v) delivers comprehensive WAN gateway and network services functions into virtual and cloud environments and enables enterprises to transparently extend their WANs into provider-hosted clouds.
3. AWS TGW is a network transit hub for interconnecting VPCs and on-premise networks.
4. AWS TGW Network Manager enables customers to centrally manage their AWS networks that are built around Transit Gateways.

The AWS TGW connects the public cloud and on-premise networks via a CSR 1000v (and a secondary for failover). If a TGW does not exist, Cisco Cloud onRamp will create one, connect to it, perform a BGP route exchange to learn all the routes coming from the cloud via the TGW, and vice versa, advertising branch routes to customer VPCs through the TGW. Cloud VPC routes are then distributed into the routing domain of the SD-WAN via OMP. This workflow to accomplish all of this is performed in vManage.



Cisco vManage

CONFIGURATION | TEMPLATES

Device Feature

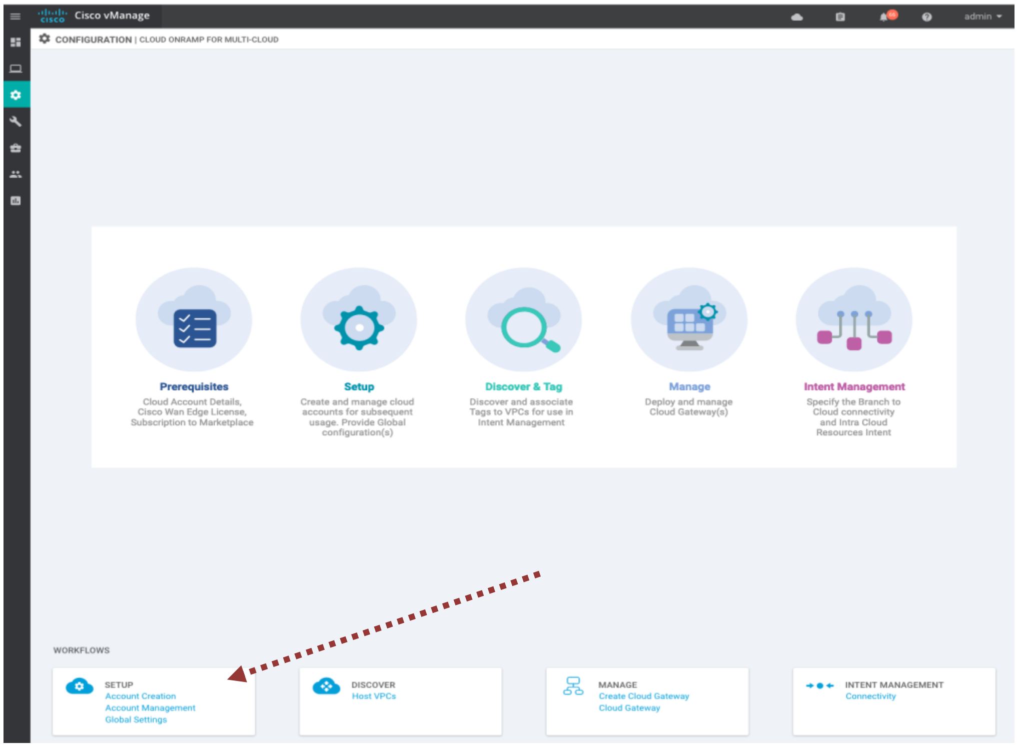
Create Template

Template Type: Non-Default

Total Rows: 2

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status
Multi_Cloud_Default_AWS_TGW_CSR1000V_Template_V01	Multi_Cloud_Def...	Feature	CSR1000v	11	0	cisco	23 Jun 2020 11:1...	In Sync
Branch_03_ServiceVPN	Template for Bra...	Feature	CSR1000v	13	1	admin	24 Jun 2020 12:4...	In Sync

Using vManage, we attached two selected CSR1000v routers to a pre-configured template, called "Multi_Cloud_Default_AWS_TGW_CSR1000V_Template_V01". For each router, we defined the hostname, system IP address and site ID; we configured each until we observed a "Done – Scheduled" status in vManage.



Cisco vManage

CONFIGURATION | CLOUD ONRAMP FOR MULTI-CLOUD

Prerequisites: Cloud Account Details, Cisco Wan Edge License, Subscription to Marketplace

Setup: Create and manage cloud accounts for subsequent usage. Provide Global configuration(s)

Discover & Tag: Discover and associate Tags to VPCs for use in Intent Management

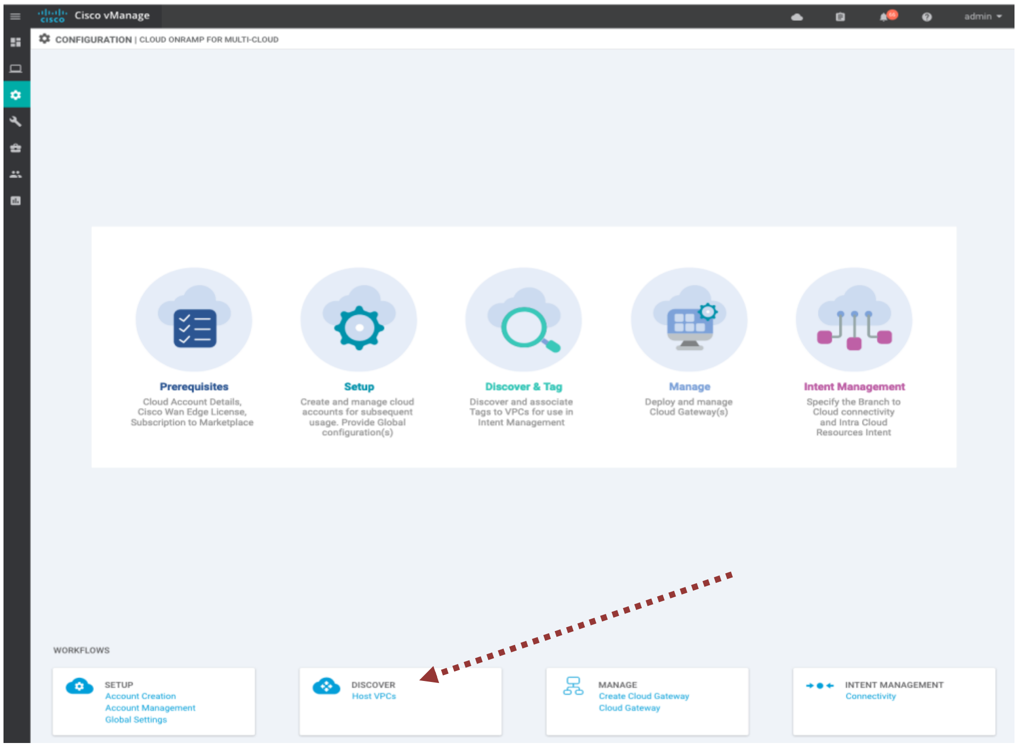
Manage: Deploy and manage Cloud Gateway(s)

Intent Management: Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent

WORKFLOWS

- SETUP: Account Creation, Account Management, Global Settings
- DISCOVER: Host VPCs
- MANAGE: Create Cloud Gateway, Cloud Gateway
- INTENT MANAGEMENT: Connectivity

We set up an AWS account to Cloud onRamp for Multi-Cloud, so vManage has access to create AWS resources. Next, we setup the CSR1000v routers in Cloud onRamp. During this, we had global settings for the virtual routers, including software image, instance size, cloud gateway solution, IP subnet pool, cloud gateway BGP ASN offset, intra tag communication, and program default route in VPCs towards TGW.



Prerequisites
Cloud Account Details, Cisco Wan Edge License, Subscription to Marketplace

Setup
Create and manage cloud accounts for subsequent usage. Provide Global configuration(s)

Discover & Tag
Discover and associate Tags to VPCs for use in Intent Management

Manage
Deploy and manage Cloud Gateway(s)

Intent Management
Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent

SETUP
Account Creation
Account Management
Global Settings

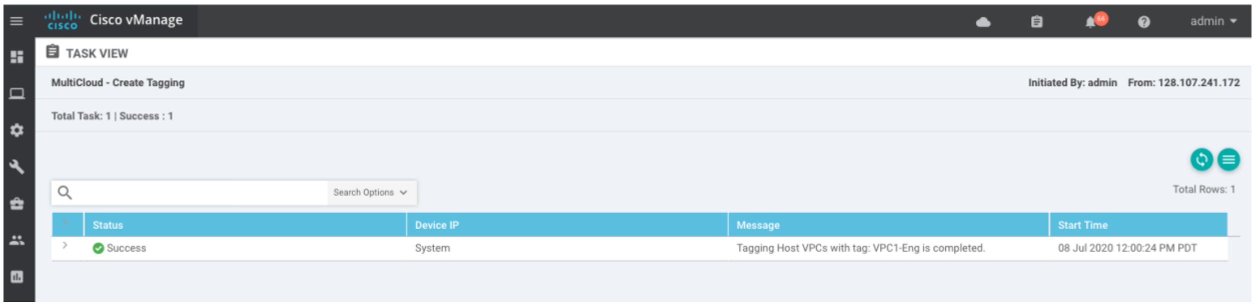
DISCOVER
Host VPCs

MANAGE
Create Cloud Gateway
Cloud Gateway

INTENT MANAGEMENT
Connectivity

We then began the discover process for Host VPCs across all AWS regions to add tags for better management.

During the mapping process, Cisco simplifies segmentation with VPC tagging and a few clicks for connecting service-side VPNs to different host VPCs for access control. Additionally, this process can be used for VPC-to-VPC communication control.



MultiCloud - Create Tagging

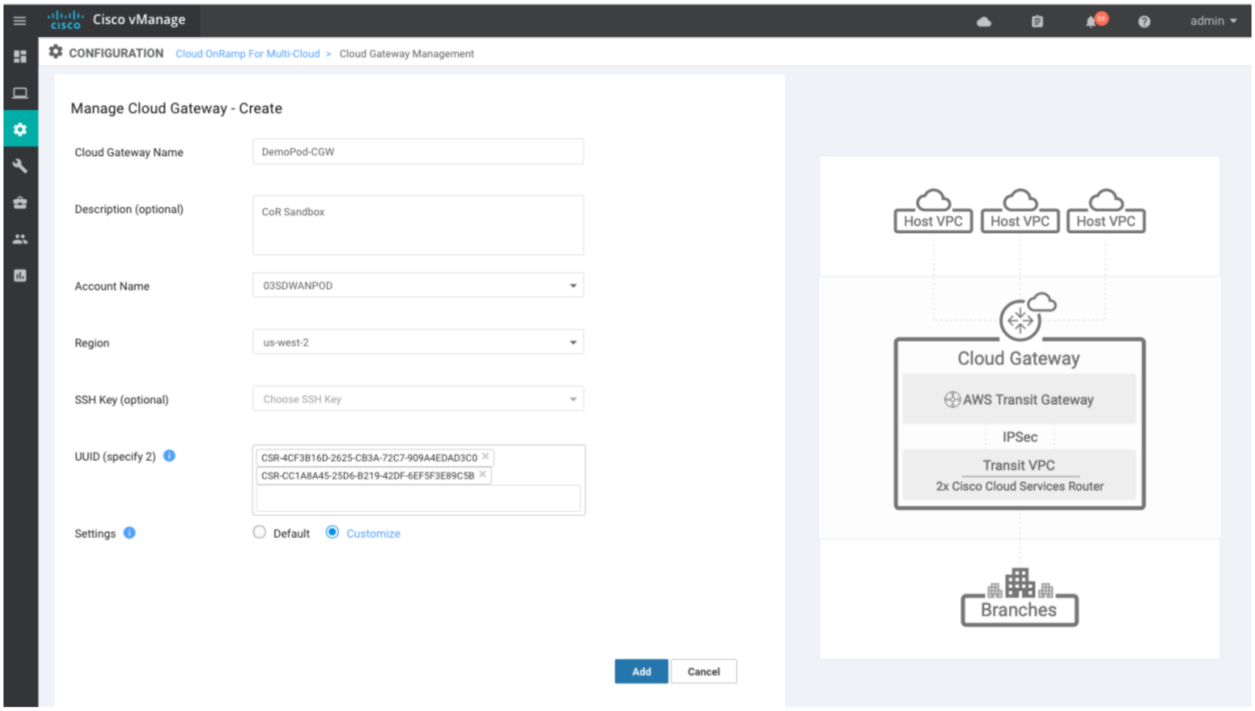
Initiated By: admin From: 128.107.241.172

Total Task: 1 | Success : 1

Total Rows: 1

Status	Device IP	Message	Start Time
Success	System	Tagging Host VPCs with tag: VPC1-Eng is completed.	08 Jul 2020 12:00:24 PM PDT

The VPC tagging status was shown as successful in vManage.



CONFIGURATION Cloud OnRamp For Multi-Cloud > Cloud Gateway Management

Manage Cloud Gateway - Create

Cloud Gateway Name: DemoPod-CGW

Description (optional): CoR Sandbox

Account Name: 03SDWANPOD

Region: us-west-2

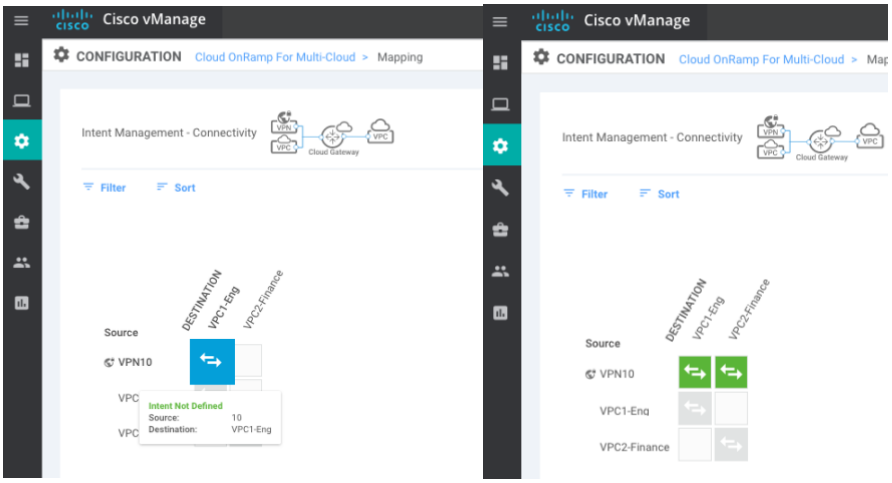
SSH Key (optional): Choose SSH Key

UUID (specify 2): CSR-4CF3B16D-2625-CB3A-72C7-909A4EDAD3C0, CSR-CC1A8A45-25D6-B219-42DF-6EF5F3E89C5B

Settings: ○ Default ● Customize

Add Cancel

Next, we created a Cloud Gateway under Cloud onRamp > Manage. We filled out the fields above and selected the two CSR devices we configured earlier. We then saw a success status message when the creation was complete.



CONFIGURATION Cloud OnRamp For Multi-Cloud > Mapping

Intent Not Defined
Source: 10
Destination: VPC1-Eng

Finally, we set up Intent Management for controlling service-side VPN to Host VPC and/or VPC-to-VPC communication. By clicking on the grey boxes, we enabled communication. Blue boxes with arrows indicate newly added rules which became effective once we saved this screen. and vManage configures the segmentation. Connectivity was successful, as indicated by green boxes.

We tested successful connections by pinging each VPN to its corresponding VPC. The total process took 8-10 minutes to be completed vs hours if one were to do this manually.

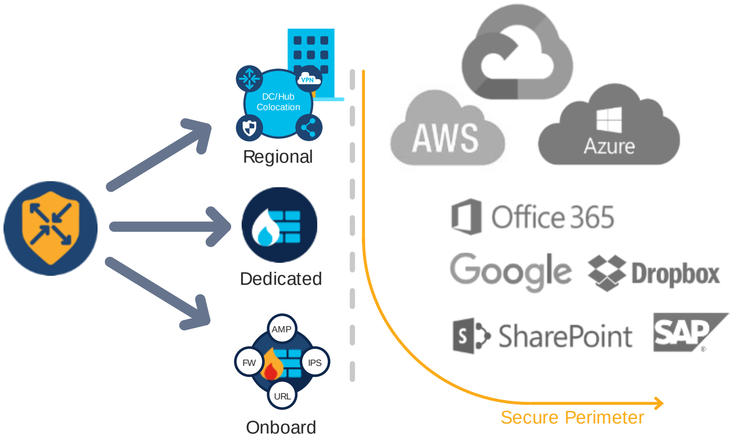
Benefits of Integration:

- **Simplified network management and improved visibility**: Cloud OnRamp for Multi-Cloud is a single pane-of-glass management console orchestrating both Cisco SD-WAN and AWS environment for site-to-cloud connectivity, including Transit VPC and TGW creation, peering and route exchange and host VPC auto-discovery and mapping.
- **Reduced deployment time and complexity:** End-to-end network automation through Cloud OnRamp for Multi-Cloud. The administrator must only define the cloud credentials – without the need to find the host VPC and manually provision each of the 200 sites. The integration process took about 10 minutes to automatically provision and connect 200 branch site networks to the AWS cloud application. This reduces human error, downtime and risk of outages that cost the business in productivity and profit.
- **Increased security:** Extends SD-WAN benefits to AWS, enabling inter-region VPC segmentation.

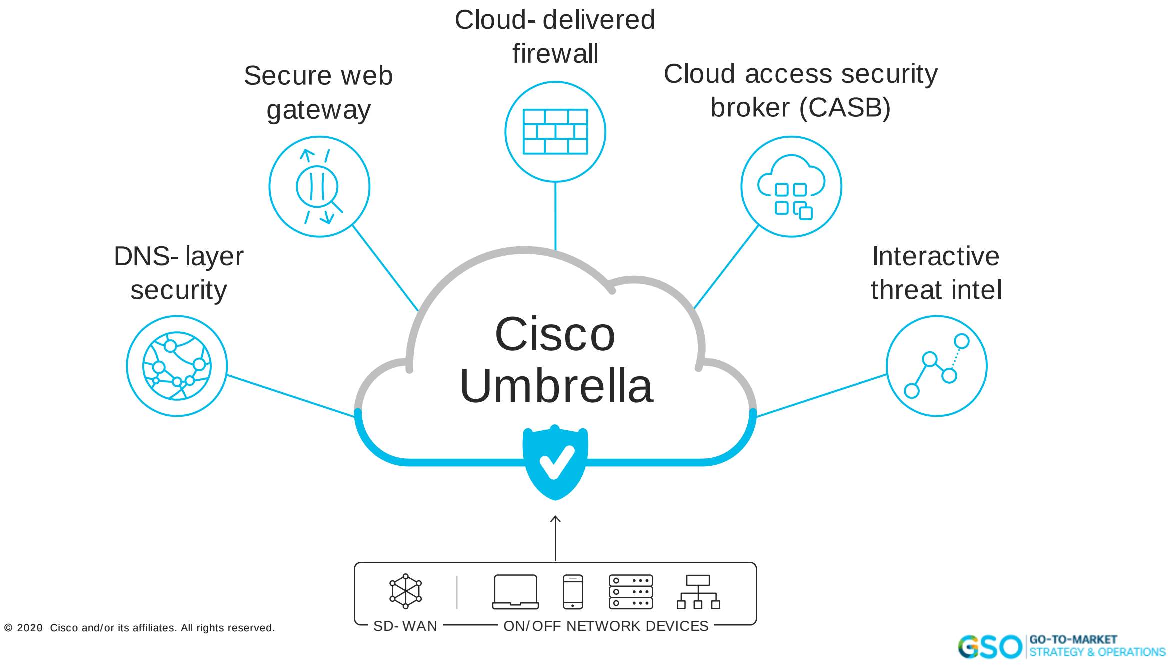
5.0 Cloud: SASE (Service Access Service Edge)

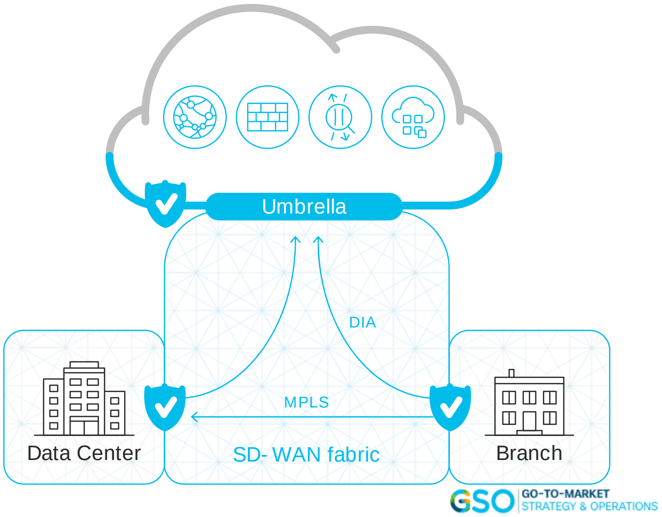
5.1 Auto-tunnel to Umbrella Secure Internet Gateway (SIG)

Cisco Umbrella Cloud Security Service peers with over 1,000 of the world's top internet service providers (ISPs), content delivery networks (CDNs) and SaaS platforms to deliver the fastest route for any request – resulting in superior speed, effective security and the best user satisfaction. With direct peering, customers gain a secure, high performance and low latency to their applications.



Cisco SD-WAN provides interconnectivity with Cisco Umbrella SIG to support full-stack security for cloud-based applications. Normally, a user cannot connect unprotected Direct Internet Access (DIA) from unsecure public Internet to the cloud application in the network. This leaves the branch network open to vulnerabilities. Cisco Umbrella SIG takes traffic from the branch side, using secure IPsec tunneling, then performs firewall protection and security checks before sending traffic to the cloud application (e.g. Dropbox, AWS).


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
© 2020 Cisco and/or its affiliates. All rights reserved.
GSO GO-TO-MARKET STRATEGY & OPERATIONS



This test case looks at how Umbrella SIG is available over the SD-WAN fabric, by auto-provisioning and deploying tunnels with just a few clicks. These secure tunnels provide reliability, low latency, deep inspection and control for firewall and secure web gateway functionality in the cloud.

The Cisco Advantage

In the use case of 200 branches, establishing tunnels is a daunting, manual process. This configuration would be time consuming, and training would be costly. To remedy, Cisco follows the IaaS mode of auto-tunnel establishment. Using vManage and Cisco Umbrella SIG credentials, we were able to establish IPsec tunneling between CSRs and Umbrella to provide robust security to cloud applications.

Traditionally, traffic flowed from the branch site to the data center, through a firewall to the public Internet. Today, most customers open DIA from the branch when using a cloud-based application, such as Dropbox. This violates security standards for the network.

With Cisco SD-WAN and Umbrella SIG integration, traffic is not routed directly to the Internet but to Umbrella SIG over secure IPsec tunnels. Umbrella SIG provides firewall and security checks before forwarding to the cloud application or the public Internet – or in some cases, block.

5.2 Umbrella Cloud-based Firewall Blocks Darknet

To demonstrate the effectiveness of integrating Umbrella SIG with Cisco SD-WAN, we used two policies: Block Torrent Download and Facebook Access. The Umbrella SIG was expected to have successful security for traffic tunneled from the branch sites of the SD-WAN fabric.

The Cisco Advantage

We enabled a firewall policy against Bit Torrent and connected an unprotected victim client behind one of the CSR1000v routers. From this client, we attempted to access Facebook and CNN.com, as well as download a Bit Torrent. All access was allowed.

Next, we used a configuration template for the router where the client was connected. We added a secure gateway with a template – all features were pre-configured. There was no need to manually define policies or create IPsec tunneling, which eliminated a lot of human error. We were able to successfully push the integration within 21 seconds, as opposed to an hour if done manually.

Pushing the integration does not require Umbrella SIG; this can be performed in vManage. The tunnel status was viewable based on geolocation (data center IP address) for the next available Umbrella SIG to perform security, then the traffic is routed to the Internet.

We attempted to access Facebook and CNN.com from the client; both websites were blocked over HTTP and HTTPS. We tried to download a Bit Torrent, and this was blocked.

Cisco provides easy and effective integration with a security service that customers would be willing to use to protect its branch sites from the public Internet or vulnerable cloud applications.

5.3 Umbrella SIG Scale

Currently, Cisco SD-WAN supports up to 250 Mbps per tunnel, and Umbrella SIG supports up to 500 Mbps per tunnel. In the next software release, version 17.4 in November 2020, Cisco will provide ECMP Load Balancing across 4 tunnels – supporting a total of 1 to 2-Gigabit Ethernet aggregated through to Umbrella SIG.

6.0 SD-WAN and Unified Communications

Traditionally, customers desiring both Unified Communications (UC) and SD-WAN had to use two boxes at the branch site. One box terminated the SD-WAN fabric, while the other terminated UC. This created more cost and complexity for network operations.

6.1 Single-box Solution

Cisco offers four calling solutions to choose from based on business size and strategy. Unified Communications Manager (UCM) for all business sizes on-premise, and the UCM Cloud is the same UCM services, but hosted in the cloud. UCM Cloud handles complex migrations for large enterprises and includes UCM/Jabber features. Two subset versions of UCM (either premise and cloud) are the Cisco UC-One for small and medium businesses with basic UC functionality, and Cisco Webex Calling for mid-market and large enterprises.

Customers want to extended Enterprise UC capabilities to branch locations, and Cisco UCM Cloud makes this possible via Viptela. Unfortunately, it was too memory-intensive to add Viptela capability in addition to IOS-XE software on Cisco Integrated Service Routers (ISRs). The result was routers without UC. To fix this, Cisco performed memory optimization to add UC to ISR 4000 models.

Cisco SD-WAN now supports a single-box solution for UC and SD-WAN integration – allowing analog, basic SIP, SRST (Survivable Remote Site Telephony), T1/PRI termination, DSP Farming and Fax Passthrough capabilities with less complexity and lower cost. If WAN service is lost between branch and data center, the router will account for this by acting as the temporary call control server.

While it is recommended to still upgrade router memory beyond 4 GB, UC capabilities are now available within this memory limitation. This is helpful for customers that previously wanted to upgrade to combined SD-WAN and UC functionality, but were not able to due to memory restrictions.

The Cisco Advantage

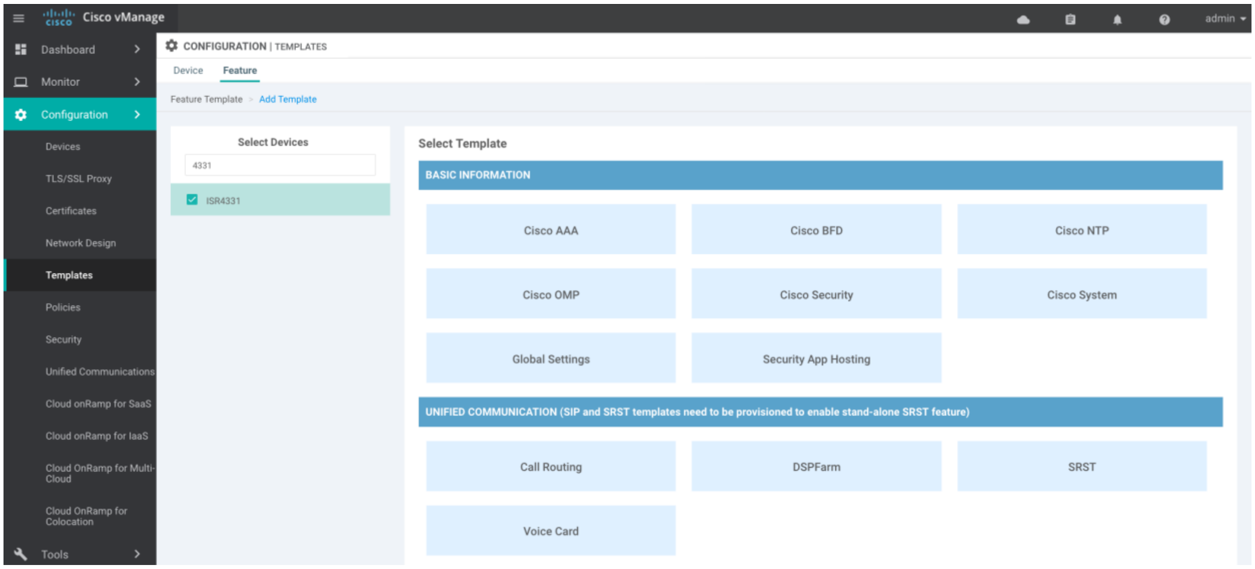
Instead of having a two-box solution, and consequently separate upgrades, to handle SD-WAN and UC, customers can use a single-box solution and one upgrade to accomplish these operations. This reduces the cost of a second box, as well as the associated operational overhead.

While other SD-WAN vendors can offer UC integration, they merely optimize UC or pass traffic through a third-party, cloud-based peering application (e.g. Zoom). Cisco is the only SD-WAN vendor to provide native integration for physical plug-in access to UC out of a single box.

UC can be installed using vManage in three simple steps:

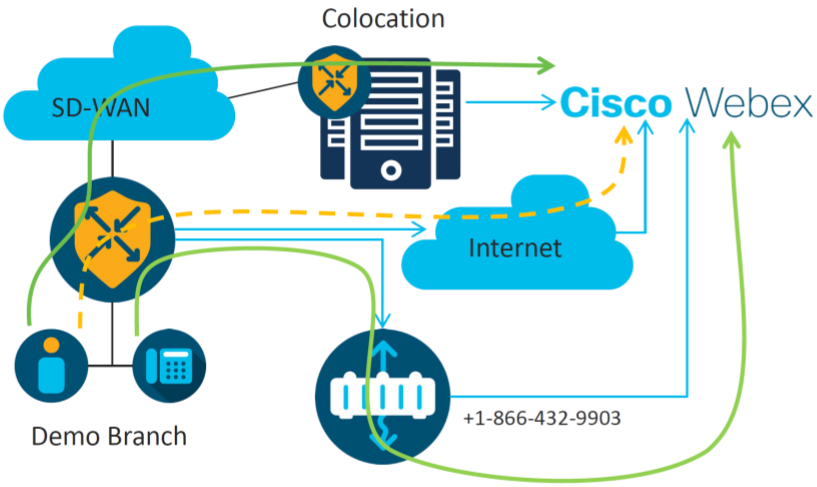
1. **In the Templates menu, define the cards and phones on the router.** Traditionally, engineers had to manually build dial tiers and configure voice cards for the routers using translation rules and profiles. This leads to consistency issues and challenging scalability. Cisco configures using templates. The engineer can define a single template and push it down to all the routers, automatically, at once. This gives reassurance of consistency across platforms, by reducing human

error, and minimizes scalability issues. Three templates are available for the popular Cisco ISR4331 router: Call Routing, SRST, and Voice Card.



By clicking the Voice Card, we name and add analog interface. For this test, we chose the NIM-4FXO interface to represent four ports installed on the router to terminate phone lines from the phone company. We chose a module slot, port type, port range – defining where the card is located on the router, what phone lines are connected to it, and where calls should go (e.g. reception). Traditionally, these items were defined using a text file pasted into the router. In the past this was very prone to errors. Further, for security, we selected a Trusted IPv4/IPv6 Prefix List – a fraud prevention tool for SIP communication from the Internet side of the router that acts as an attack vector.

2. **Define Voice Policy.** For customers who want to augment calls, they can use the natively integrated UC capabilities to optimize – a unique feature from Cisco in the SD-WAN market. Cisco can augment calls in many ways (e.g. raise volume, dynamic codec changes to enhance bandwidth utilization and quality, create failover profiles). The policy is then mapped to particular ports on the router using Cisco vManage. The SSH Terminal uses the traditional UC commands familiar to engineers within the vManage interface. There is no need to log into each individual router; it is performed centrally from vManage.



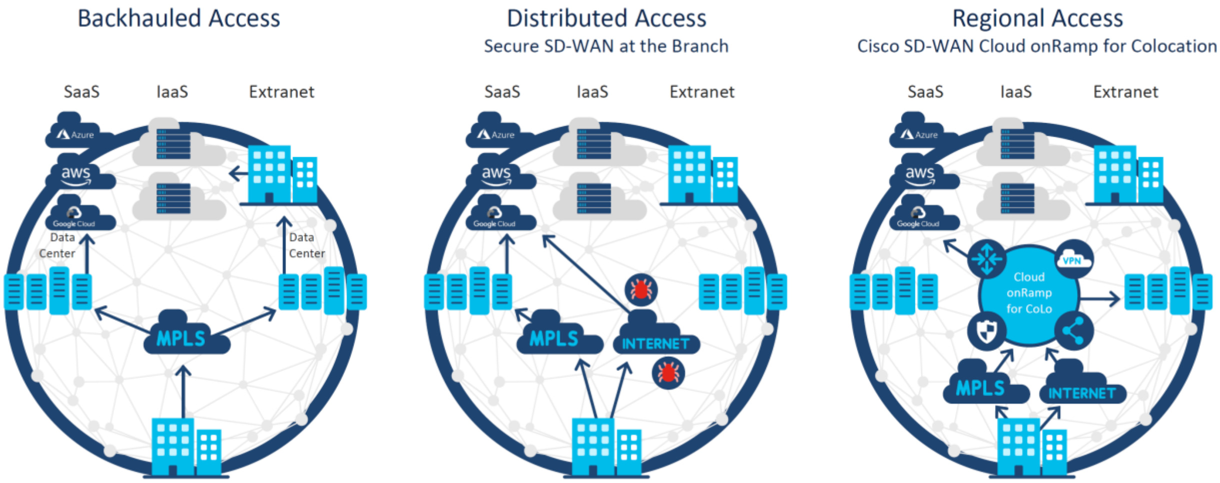
The phone call was successfully routed from a laptop through the local gateway to Cisco Webex.

6.2 Webex Connect Optimization with Colocation

After setting up the integrated UC for phone lines to Webex Calling with a single-box SD-WAN and UC solution, the next step is traffic optimization. This traffic includes audio, video and screen sharing.

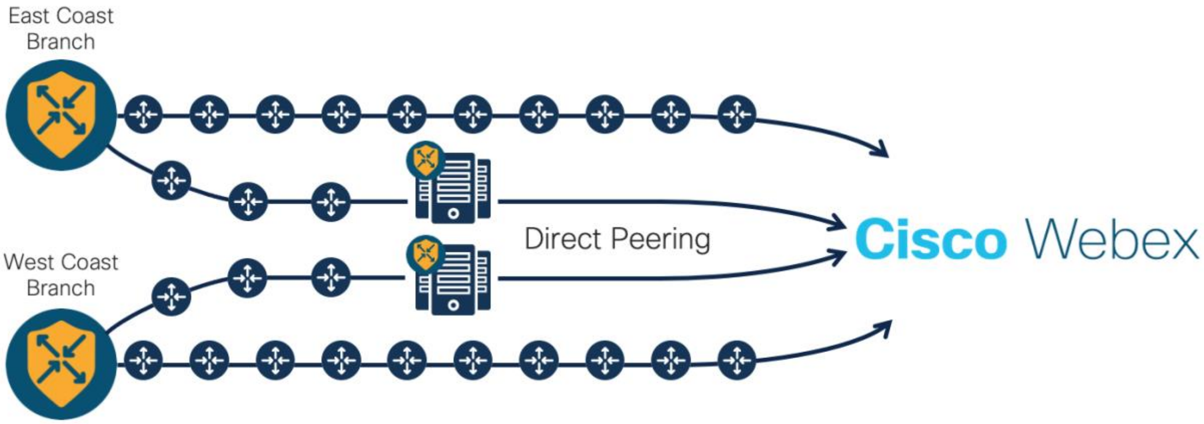
The Cisco Advantage

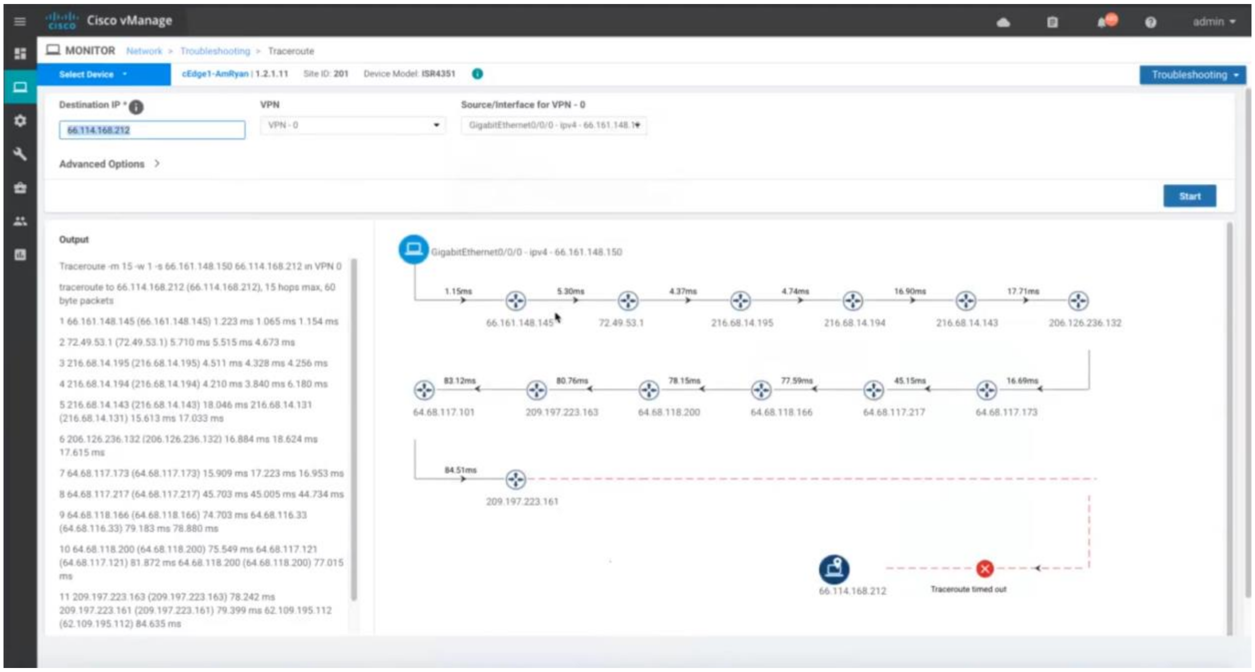
Cisco uses a new feature – cloud-based colocation. This middle mile approach expands on the current way to achieve branch access. Traditionally, backhauled access was used; everything was hosted in the data center hub and communicated to branches over MPLS. Next, came secure SD-WAN via distributed access which reduced loss and latency by balancing call or UC traffic using MPLS and Internet links. But there were advantages to the backhaul access – namely, all traffic was coming from a central location over few links that were easy to control, optimize and police.



To achieve efficient, secure and controllable traffic, a third model was created: Regional Access. Cisco uses this concept with the Cisco SD-WAN Cloud OnRamp for Colocation. Cloud OnRamp utilizes geographically proximal, rentable, colocations for flexible telecommunications, network service and cloud service. Colocation Centers are a multi-tenant approach to reduce physical space, increase security, reduce maintenance, and minimize costs of operation. According to Gartner, colocation, interconnectivity, and cloud partner ecosystems are a growing, critical need for future infrastructure.

This approach extends the SD-WAN fabric to the colocation facility to reduce hop count and latency, while providing end-to-end optimization for the end user. Before, Webex traffic was routed directly to the Internet which reduces efficiency. Instead, Cloud OnRamp finds the nearest colocation facility to send traffic for direct peering.





cEdge1-AmRyan | 1.2.1.11 Site ID: 201 Device Model: ISR4351

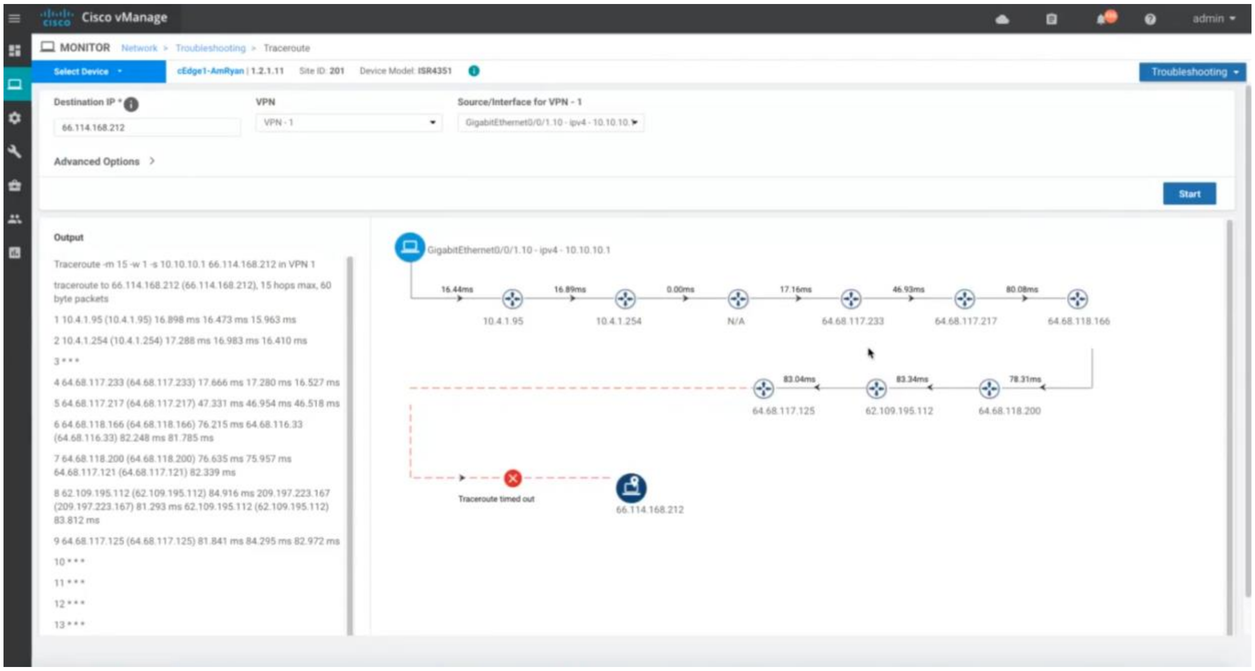
Destination IP *: 66.114.168.212

VPN: VPN - 0

Source/Interface for VPN - 0: GigabitEthernet0/0/0 - ipv4 - 66.161.148.1

```
Traceroute -m 15 -w 1 -s 66.161.148.150 66.114.168.212 in VPN 0
traceroute to 66.114.168.212 (66.114.168.212), 15 hops max, 60
byte packets
1 66.161.148.145 (66.161.148.145) 1.223 ms 1.065 ms 1.154 ms
2 72.49.53.1 (72.49.53.1) 5.710 ms 5.515 ms 4.673 ms
3 216.68.14.195 (216.68.14.195) 4.511 ms 4.328 ms 4.256 ms
4 216.68.14.194 (216.68.14.194) 4.210 ms 3.840 ms 6.180 ms
5 216.68.14.143 (216.68.14.143) 18.046 ms 216.68.14.131
(216.68.14.131) 15.613 ms 17.033 ms
6 206.126.236.132 (206.126.236.132) 16.884 ms 18.624 ms
17.615 ms
7 64.68.117.173 (64.68.117.173) 15.909 ms 17.223 ms 16.953 ms
8 64.68.117.217 (64.68.117.217) 45.703 ms 45.005 ms 44.734 ms
9 64.68.118.166 (64.68.118.166) 74.703 ms 64.68.116.33
(64.68.116.33) 79.183 ms 78.880 ms
10 64.68.118.200 (64.68.118.200) 75.549 ms 64.68.117.121
(64.68.117.121) 81.872 ms 64.68.118.200 (64.68.118.200) 77.015
ms
11 209.197.223.163 (209.197.223.163) 78.242 ms
209.197.223.161 (209.197.223.161) 79.399 ms 62.109.195.112
(62.109.195.112) 84.635 ms
```

In vManage, we were able to see the traced path route and reduced number of hops from employing Cloud OnRamp for colocation optimization.



Destination IP *: 66.114.168.212

VPN: VPN - 1

Source/Interface for VPN - 1: GigabitEthernet0/0/1.10 - ipv4 - 10.10.10.1

Advanced Options

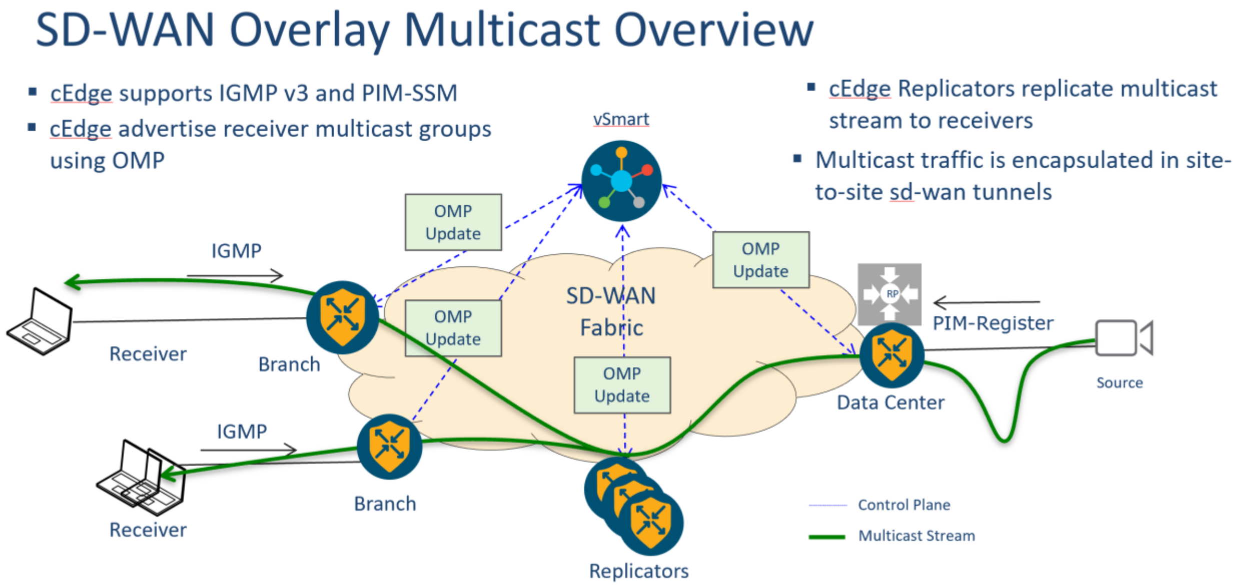
Output

```
Traceroute -m 15 -w 1 -s 10.10.10.1 66.114.168.212 in VPN 1
traceroute to 66.114.168.212 (66.114.168.212), 15 hops max, 60 byte packets
1 10.4.1.95 (10.4.1.95) 16.898 ms 16.473 ms 15.963 ms
2 10.4.1.254 (10.4.1.254) 17.288 ms 16.983 ms 16.410 ms
3 * * *
4 64.68.117.233 (64.68.117.233) 17.666 ms 17.280 ms 16.527 ms
5 64.68.117.217 (64.68.117.217) 47.331 ms 46.954 ms 46.518 ms
6 64.68.118.166 (64.68.118.166) 76.215 ms 64.68.116.33 (64.68.116.33) 82.248 ms 81.785 ms
7 64.68.118.200 (64.68.118.200) 76.635 ms 75.957 ms 64.68.117.121 (64.68.117.121) 82.339 ms
8 62.109.195.112 (62.109.195.112) 84.916 ms 209.197.223.167 (209.197.223.167) 81.293 ms 62.109.195.112 (62.109.195.112) 83.812 ms
9 64.68.117.125 (64.68.117.125) 81.841 ms 84.295 ms 82.972 ms
10 * * *
11 * * *
12 * * *
13 * * *
```

We observed a Webex call from a laptop first without Cloud OnRamp and recorded 13 hops. With Cloud OnRamp (peering with colocation using a virtual router service chain), the hop count reduces to 9. This test environment was a long-distance colocation deployment scenario, showing latency of about 10 milliseconds. In real-world customer deployments, colocations are very often much closer and will show even lower latency.

7.0 SD-WAN and Multicast

Traditional multicast routing on a WAN network utilizes Internet links, selectively and simultaneously sending and receiving control/data traffic across WAN/LAN networks. Routers communicate this information on the underlay. Cisco SD-WAN uses edge routers to join the multicast, as previously done, but instead uses the overlay. With the multicast streams now mapped to the overlay SD-WAN fabric, all control messages are managed by the controller, vSmart.



SD-WAN Overlay Multicast Overview

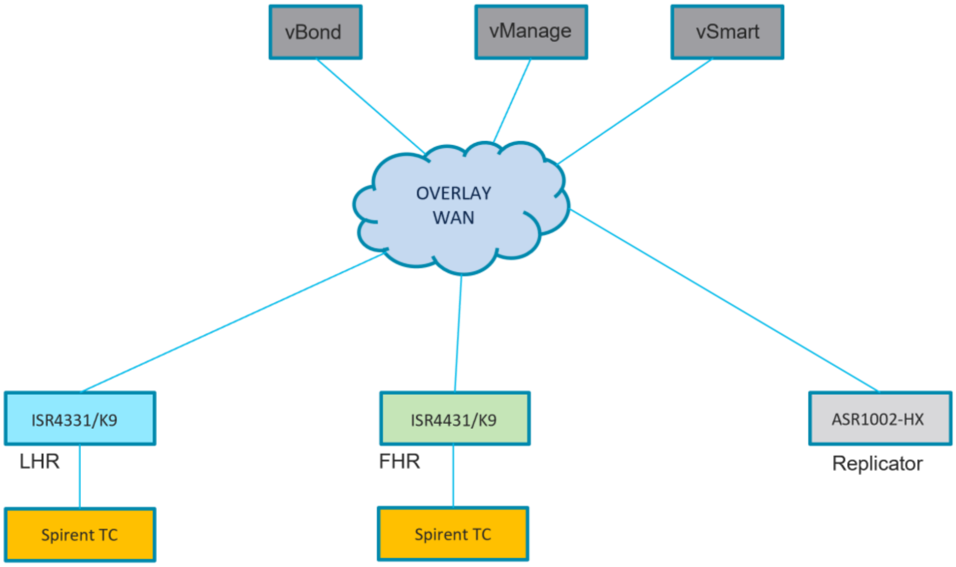
- cEdge supports IGMP v3 and PIM-SSM
- cEdge advertise receiver multicast groups using OMP

- cEdge Replicators replicate multicast stream to receivers
- Multicast traffic is encapsulated in site-to-site sd-wan tunnels

Cisco SD-WAN uses the Overlay Management Protocol (OMP) to exchange routing messages. OMP messages are forwarded to the vSmart hub, then vSmart sends to all other Edge routers using OMP. OMP on Edge devices then converts OMP to Protocol-Independent Multicast (PIM) messages for further multicast processing. The replicator on the overlay is a high-end aggregator IOS-XE router that forwards copies of multicast data streams to optimize WAN bandwidth and enforce centralized policies.

7.1 Join/Leave Delay Test

A host joining the multicast group uses traditional join messages that terminate on the SD-WAN router – in this case, the Cisco cEdge device with OMP enabled. This test looks at the number of join and leave messages sent using the Cisco SD-WAN overlay for multicast.

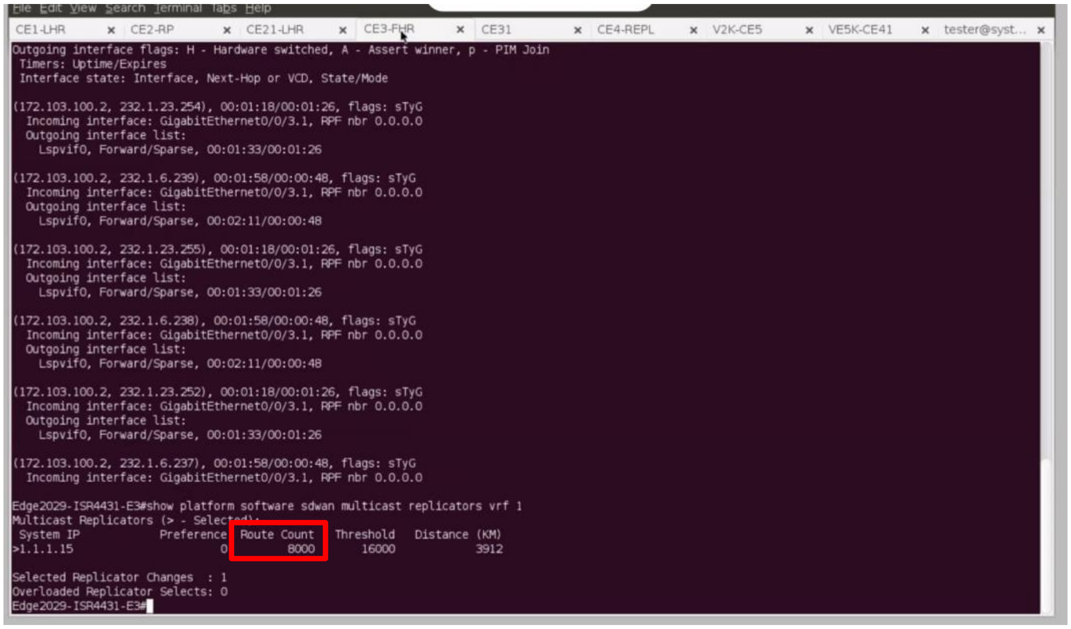


There are two Cisco ISR4331 branch routers connected to the Spirent Test Center, which simulates both end hosts (receivers) and the data center. The Cisco ASR1002 router acts as the replicator, distributing multicast streams to the receivers. We recorded the throughput performance and latency using the Spirent Test Center. Each link is 1-Gigabit Ethernet (GbE).

For this test, we scaled the network up to 8,000 multicast groups. This is a worst-case scenario; routes are usually not this high. The test was run using a large frame size of 1024-byte (B) packets for 10 seconds.

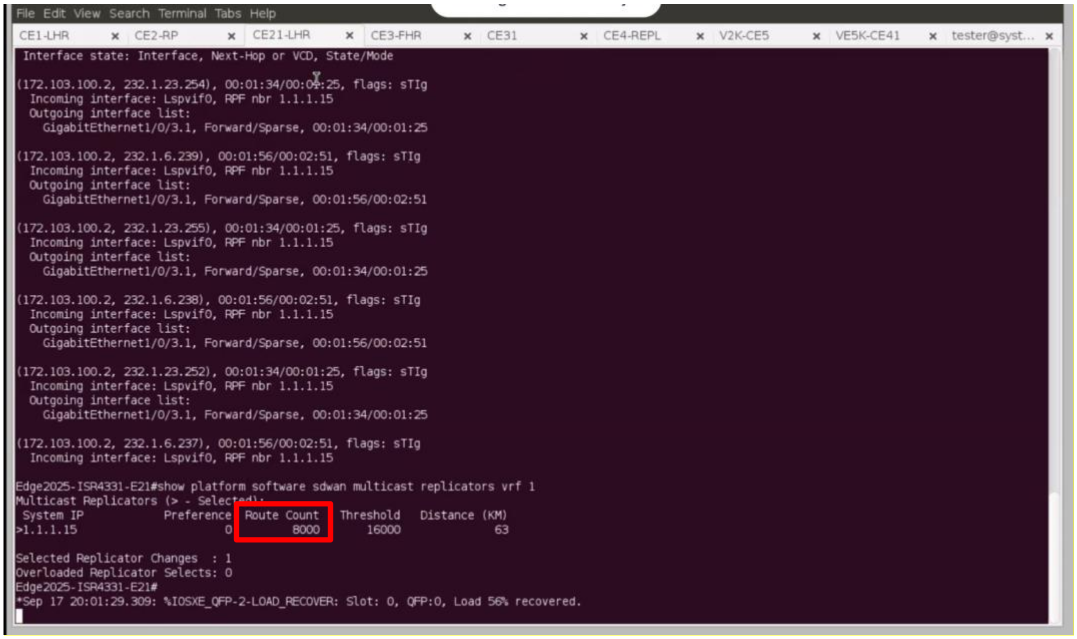
The Cisco Advantage

We observed successfully join messages for 8,000 routes – four times higher than the typical customer deployment, which is about only 2,000 groups. This observation is also not the maximum achievable for Cisco, as it has no hard limit on the number of groups it can support.



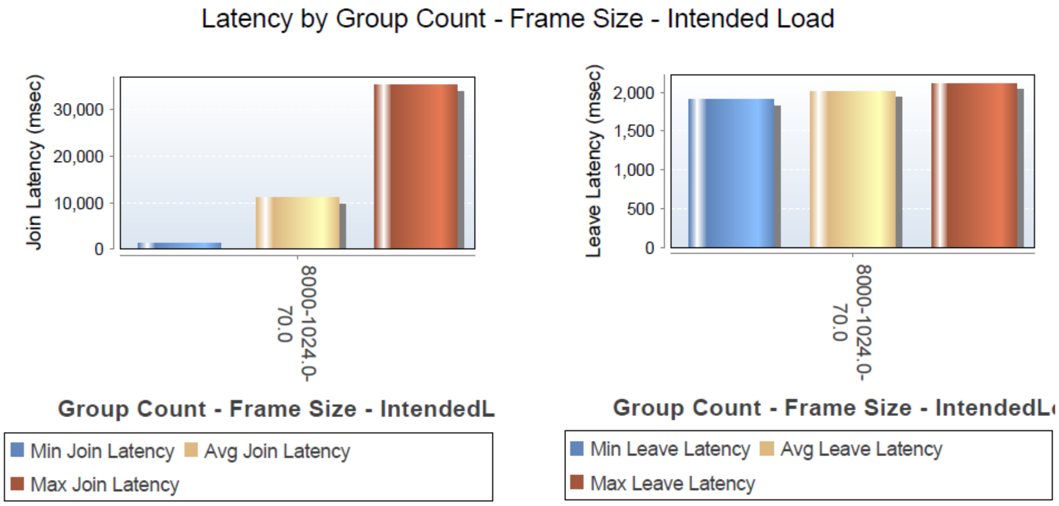
```
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(172.103.100.2, 232.1.23.254), 00:01:18/00:01:26, flags: sTyG
  Incoming interface: GigabitEthernet0/0/3.1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif0, Forward/Sparse, 00:01:33/00:01:26

(172.103.100.2, 232.1.6.239), 00:01:58/00:00:48, flags: sTyG
  Incoming interface: GigabitEthernet0/0/3.1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif0, Forward/Sparse, 00:02:11/00:00:48

(172.103.100.2, 232.1.23.255), 00:01:18/00:01:26, flags: sTyG
  Incoming interface: GigabitEthernet0/0/3.1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif0, Forward/Sparse, 00:01:33/00:01:26

(172.103.100.2, 232.1.6.238), 00:01:58/00:00:48, flags: sTyG
  Incoming interface: GigabitEthernet0/0/3.1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif0, Forward/Sparse, 00:02:11/00:00:48

(172.103.100.2, 232.1.23.252), 00:01:18/00:01:26, flags: sTyG
  Incoming interface: GigabitEthernet0/0/3.1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif0, Forward/Sparse, 00:01:33/00:01:26

(172.103.100.2, 232.1.6.237), 00:01:58/00:00:48, flags: sTyG
  Incoming interface: GigabitEthernet0/0/3.1, RPF nbr 0.0.0.0

Edge2029-ISR4431-E3#show platform software sdwan multicast replicators vrf 1
Multicast Replicators (> - Selected):
 System IP            Preference Route Count  Threshold   Distance (KM)
>1.1.1.15                     0        8000      16000            3912

Selected Replicator Changes  : 1
Overloaded Replicator Selects: 0
Edge2029-ISR4431-E3#
```

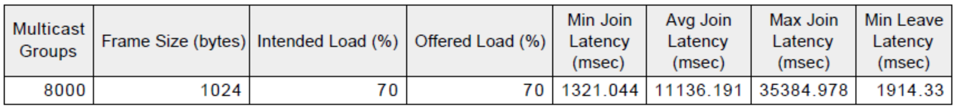
We observed 8,000 routes on the FHR (First Hop Router), which performs local replication.



```
 Interface state: Interface, Next-Hop or VCD, State/Mode

(172.103.100.2, 232.1.23.254), 00:01:34/00:01:25, flags: sTIg
  Incoming interface: Lspvif0, RPF nbr 1.1.1.15
  Outgoing interface list:
    GigabitEthernet1/0/3.1, Forward/Sparse, 00:01:34/00:01:25

(172.103.100.2, 232.1.6.239), 00:01:56/00:02:51, flags: sTIg
  Incoming interface: Lspvif0, RPF nbr 1.1.1.15
  Outgoing interface list:
    GigabitEthernet1/0/3.1, Forward/Sparse, 00:01:56/00:02:51

(172.103.100.2, 232.1.23.255), 00:01:34/00:01:25, flags: sTIg
  Incoming interface: Lspvif0, RPF nbr 1.1.1.15
  Outgoing interface list:
    GigabitEthernet1/0/3.1, Forward/Sparse, 00:01:34/00:01:25

(172.103.100.2, 232.1.6.238), 00:01:56/00:02:51, flags: sTIg
  Incoming interface: Lspvif0, RPF nbr 1.1.1.15
  Outgoing interface list:
    GigabitEthernet1/0/3.1, Forward/Sparse, 00:01:56/00:02:51

(172.103.100.2, 232.1.23.252), 00:01:34/00:01:25, flags: sTIg
  Incoming interface: Lspvif0, RPF nbr 1.1.1.15
  Outgoing interface list:
    GigabitEthernet1/0/3.1, Forward/Sparse, 00:01:34/00:01:25

(172.103.100.2, 232.1.6.237), 00:01:56/00:02:51, flags: sTIg
  Incoming interface: Lspvif0, RPF nbr 1.1.1.15

Edge2025-ISR4331-E21#show platform software sdwan multicast replicators vrf 1
Multicast Replicators (> - Selected):
 System IP            Preference Route Count  Threshold   Distance (KM)
>1.1.1.15                     0        8000      16000              63

Selected Replicator Changes  : 1
Overloaded Replicator Selects: 0
Edge2025-ISR4331-E21#
*Sep 17 20:01:29.309: %IOSXE_QFP-2-LOAD_RECOVER: Slot: 0, QFP:0, Load 56% recovered.
```

We observed 8,000 routes on the LHR (Last Hop Router).





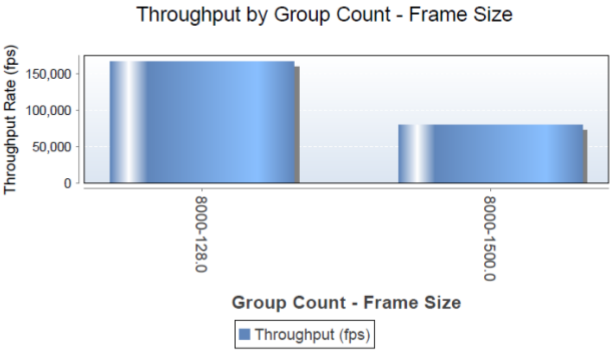
Multicast Groups	Frame Size (bytes)	Intended Load (%)	Offered Load (%)	Min Join Latency (msec)	Avg Join Latency (msec)	Max Join Latency (msec)	Min Leave Latency (msec)
8000	1024	70	70	1321.044	11136.191	35384.978	1914.33

7.2 Multicast Throughput Test

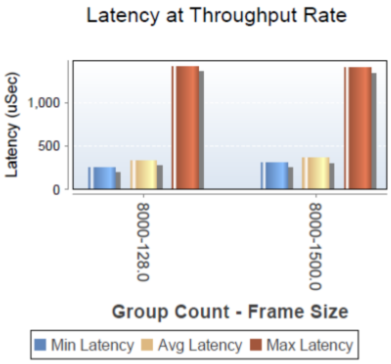
This test measures the RFC 3918 Aggregate Multicast Throughput for the Cisco SD-WAN overlay for one minute. The goal of this test is to see how much bandwidth the link can use without loss for 128 and 1500-byte frames.

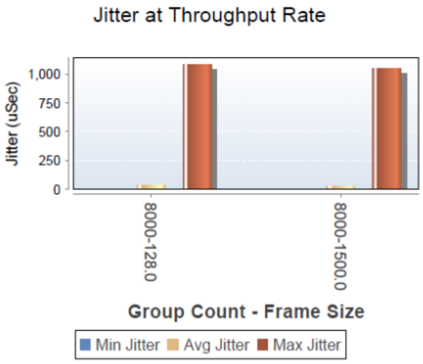
The Cisco Advantage

We observed Cisco having zero percent frame loss for throughput of 19.766 and 97.656 percent of the intended load for 128 and 1500-byte packets, respectively.



Multicast Group	Frame Size (bytes)	Intended Load (%)	Offered Load (%)	Throughput (%)	Throughput (fps)	Frame Loss (%)
8000	128	19.766	19.766	19.766	166939.43	0
8000	1500	97.656	97.656	97.656	80309.43	0





Multicast Group	Frame Size (bytes)	Intended Load (%)	Frame Loss (%)	Min Latency (uSec)	Avg Latency (uSec)	Max Latency (uSec)	Min Jitter (uSec)	Avg Jitter (uSec)	Max Jitter (uSec)
8000	128	19.766	0	253.11	330.456	1414.07	0	30.214	1086.39
8000	1500	97.656	0	307.37	359.769	1400.43	0	28.958	1052.72

8.0 SD-WAN Programmability

8.1 Webhooks

vManage is a centralized management system in the Cisco SD-WAN solution that operates using REST APIs and webhooks to integrate with third-party systems. Webhooks integration uses existing monitoring tools to get critical alerts sent via applications, like Webex Teams. Polling vManage for alarms can be expensive from an operational standpoint; it takes time to complete the life cycle of alarm management and monitoring tickets. Alarms set to random intervals may result in missed alerts, despite polling aggressively.

This test analyzes the benefits of webhook integration offered by Cisco.

The Cisco Advantage

vManage and Cisco SD-WAN can integrate with third-party tools for optimized alarm management and monitoring using application-aware routing and data policies based on specific application engineering requirements.

To avoid aggressive and wasteful alarms, webhooks enable a push-model mechanism to send notifications in real-time. These webhooks are "reversed APIs" that integrate with third-party solutions for more efficient, timely and relevant alarms.

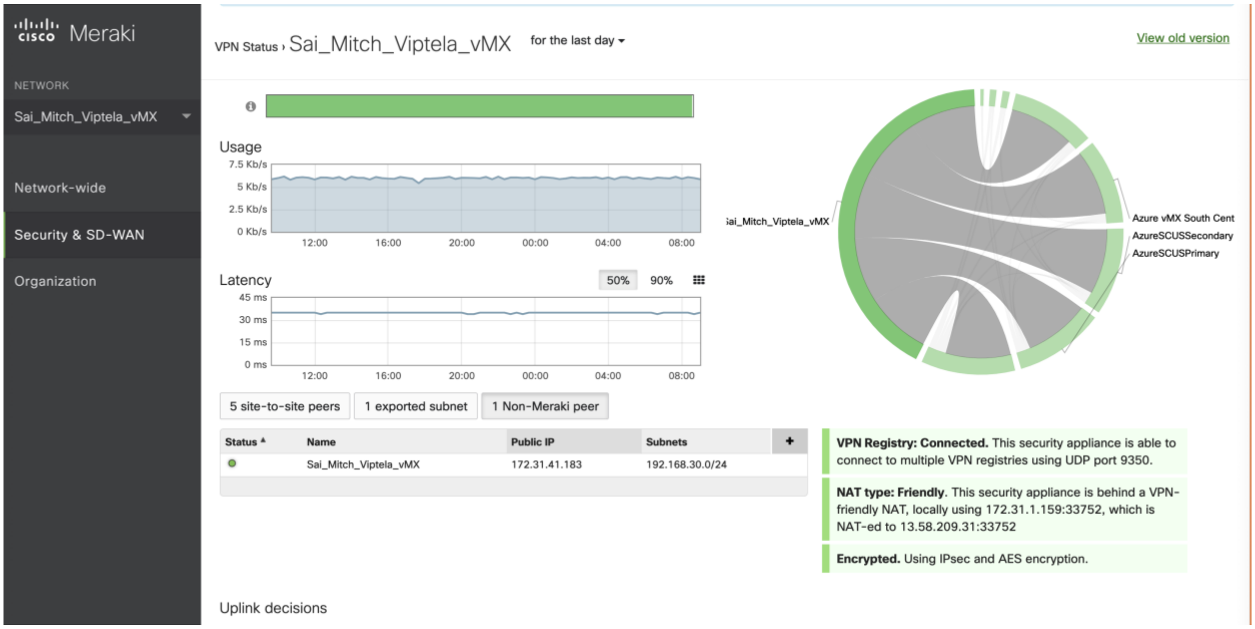
8.2 Cisco Meraki and Viptela SD-WAN Integration

In a typical acquisition (e.g. one company acquires another), it is possible to have integration of both the Viptela and Cisco Meraki SD-WAN solution. This type of deployment is difficult to scale because the networks must be joined manually through a UI.

This test shows the approach and benefits of automatically interconnecting two SD-WAN solutions using the Cisco Programmability functionality.

The Cisco Advantage

Using the vManage APIs, we created templates and configured IPsec tunnels from the vEdge routers to the Meraki MX SD-WAN appliances and using Meraki APIs, we created VPN endpoints on the Meraki MX devices. Required IPsec routes are automatically configured using APIs to route LAN traffic over IPsec tunnels between the vEdge router and Meraki SD-WAN devices.



Status ▲	Name	Public IP	Subnets	+
●	Sai_Mitch_Viptela_vMX	172.31.41.183	192.168.30.0/24	

VPN Registry: Connected. This security appliance is able to connect to multiple VPN registries using UDP port 9350.

NAT type: Friendly. This security appliance is behind a VPN-friendly NAT, locally using 172.31.1.159:33752, which is NAT-ed to 13.58.209.31:33752

Encrypted. Using IPsec and AES encryption.

This automated integration is faster than the manual approach, taking minutes to have traffic flowing from each side of the SD-WAN fabric. More importantly, the success of these templates helps integration not just for a single router but for scalable scenarios that would be costly in downtime and manual operations, prone to human error.

Independent Evaluation

This report was sponsored by Cisco Systems, Inc. The data was obtained completely and independently by Miercom engineers and lab staff as part of the Miercom Performance Verified assessment. Testing was based on a co-developed methodology with the sponsoring vendor. The test cases were designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in this independently published report by Miercom.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.