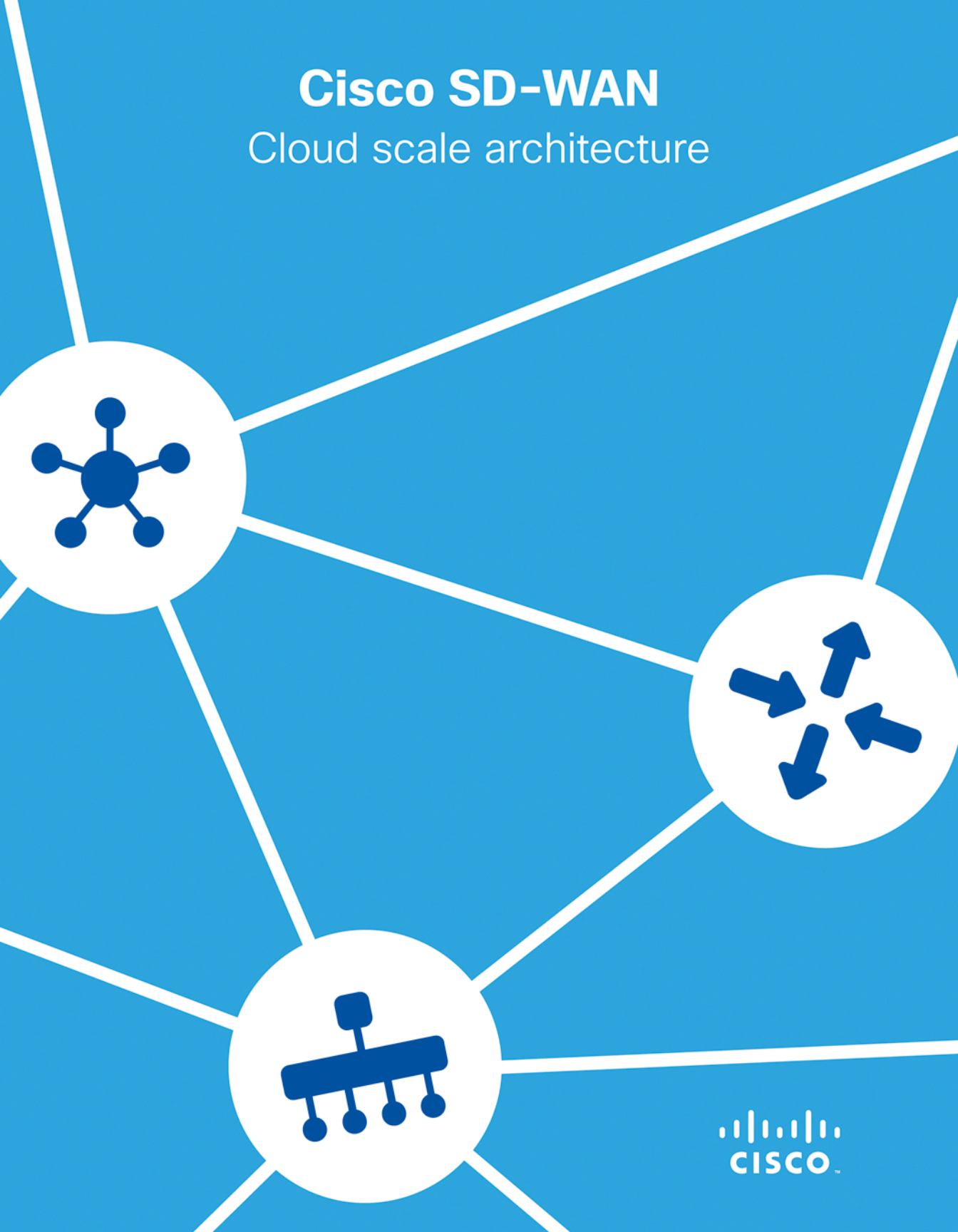
Cisco SD-WAN

Cloud scale architecture



Cisco SD-WAN

Cloud scale architecture

Preface

Authors

This book represents a collaborative effort between technical marketing, product management, sales, customer experience, engineering and marketing during a week-long session at Cisco® headquarters in San Jose, California.

- Aaron Rohyans - Technical Marketing Engineer
- Ali Shaikh - Technical Solutions Architect
- Chandra Balaji Rajaram - Technical Marketing Engineer
- David Klebanov - Technical Marketing Manager
- Deepesh Kumar - Technical Marketing Engineer
- Gina Cornett - Technical Marketing Engineer
- Hasham Malik - Technical Marketing Engineer
- Kiran Ghodgaonkar - Marketing Manager
- Madhavan Arunachalam - Product Manager
- Nikolai Pitaev - Technical Marketing Engineer
- Travis Carlson - Product Manager
- Zaheer Aziz - Senior Technical Leader

Acknowledgements

A special thanks to the Cisco Enterprise Networking Business Unit who supported the creation of this book.

Our gratitude also goes to the extended Cisco team for supporting this effort: Sehjung Hah, Rohan Grover, Sukruth Srikantha, and Misbah Rehman. Thanks to Christina Munoz for her exceptional resource organization and making sure we were all fed and watered. We also want to extend our appreciation to the Book Sprints (*www.booksprints.net*) team:

- Faith Bosworth (Facilitator)
- Henrik van Leeuwen and Lennart Wolfert (Illustrators)
- Agathe Baëz (Book producer)
- Raewyn Whyte and Susan Tearne (Proofreaders)

Intended audience

In 2017, Cisco acquired Viptela®, widely considered as a leader in SD-WAN. This book is intended for information technology professionals who are involved in the day-to-day running of wide area networks and have deployed or are evaluating Cisco SD-WAN powered by Viptela.

This book will give network engineers, managers, or architects involved in the design and architecture of wide area networks an overview of many of the features and capabilities of Cisco SD-WAN powered by Viptela, along with common use cases which may be encountered while deploying and managing a wide area network.

This book is not meant to be a design or deployment guide. Please visit the *Additional resources* section in the Appendix if you are looking for more detailed information on Cisco SD-WAN.

Book structure

This book takes a use case based approach to solving common business problems involving wide area networks. The book describes the Cisco SD-WAN architecture and then explores use cases that cover the business need and how Cisco SD-WAN solves them. It is supplemented by examples and case studies demonstrating the use case in real customer deployments. Each chapter has key takeaways and references for further reading.

Introduction

Why SD-WAN?

Businesses are embracing digital transformation and rapidly adopting technology to increase productivity, reduce costs, and transform the customer experience.

The traditional role of the wide area network (WAN) was to connect users at the branch or campus to applications hosted on servers in the data center. Dedicated MPLS circuits were used to help ensure security and reliable connectivity. This no longer works in a digital world where applications are moving out of the data center into the cloud, and the users consuming those applications are increasingly mobile, using a diverse set of devices.

As businesses increasingly adopt Software as a Service (SaaS) and Infrastructure as a Service (IaaS) across multiple clouds, IT departments are struggling with providing a satisfactory experience for business-critical applications. Traditional WAN networks heavily rely on data center infrastructure to provide cloud connectivity, however, this carries the inefficiencies of higher latency, heavy data center load, and a single point of failure. Explosion of bandwidth demands puts a significant stress on network capacity, forcing organizations to continuously upgrade their private WAN circuits. Some organizations turn their attention to internet circuits. Commodity internet circuits typically offer significantly higher capacity at much lower price points, however, organizations are struggling with operationalizing the internet as a viable means of business-critical connectivity - resorting to an inefficient active/standby approach.

Exposing an enterprise to the internet can introduce threat and compliance issues not previously experienced when internet access was secured at the data center. It is extremely challenging to protect the critical assets of an enterprise when applications are accessed by a diverse workforce whose level of access ranges from employee to partner, contractor, vendor, and guest. Enabling broadband in the WAN makes the security requirements even more acute, creating challenges for IT in balancing the user experience, security, and complexity.

Software-defined wide-area networking (SD-WAN) solutions have evolved to address these challenges. SD-WAN is part of the broader technology of software-defined networking (SDN). SDN is a centralized approach to network management which abstracts the underlying network infrastructure away from its applications. When compared to traditional networking solutions, which rely on integrated data, control and management planes in the same platform, SDN de-couples the forwarding plane from the control and management plane, allowing for centralization of network intelligence. This permits more network automation, simplification of operations, provisioning, monitoring, and troubleshooting. SD-WAN is the application of these SDN principles to the WAN.

So, the question remains: why SD-WAN? How do SDN principles solve challenges on the WAN? To answer this question, consider the analogy of traveling by car. Prior to the availability of GPS, if an individual wanted to travel from Indianapolis to Dallas by car, a road map might be used to identify the best route. If there was an accident or delay along the route, the driver would be forced to find an alternative route based on limited information. This is the way WAN routers used to operate. Each router would make its own autonomous decisions about how to forward traffic, based on a limited view of the world around them. Often times, these decisions were ignorant of disruptions downstream. Today, just as GPS has changed the game for car travel, SD-WAN changes the game for WAN architectures. With SD-WAN, edge routers can now rely on an "eye in the sky" for direction as to how and where to forward traffic. Whereas GPS can help a person avoid road construction, accidents, travel delays and inefficient routes, SD-WAN can help a branch router avoid loss, latency and jitter within the network.

What is Cisco SD-WAN?

Benefits

When SD-WAN first came to market over 5 years ago, the value proposition was based on four key requirements:

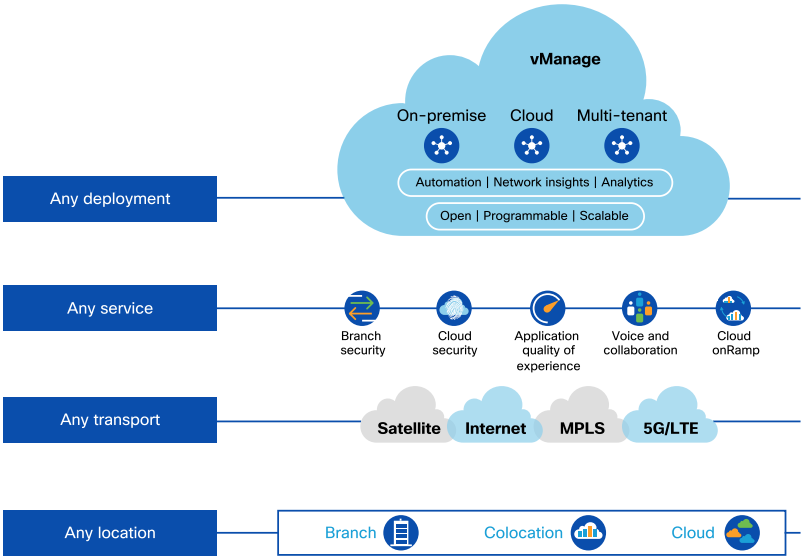
- Increasing bandwidth through the activation of idle backup links and dynamic load-balancing
- Delivering faster cloud access by enabling direct internet access at the branch
- Reducing operational and management costs through centralized management that was commonly cloud-based
- Lowering WAN costs through the use of cheaper internet or LTE connectivity as an alternative to MPLS

The digital business has evolved and the modern workforce is increasingly distributed and the applications they consume are becoming more decentralized, moving from the data center to a multi-cloud environment. When combined with the increasing number of users, devices and locations that need access to cloud applications, this creates an overwhelming complexity for IT. To address these challenges, IT has to consider more advanced WAN use cases that go beyond the basic capabilities offered by earlier SD-WAN solutions.

Cisco SD-WAN is a cloud-scale architecture designed to meet the complex needs of modern wide area networks through three key areas:

- Advanced application optimization that delivers a predictable application experience as the business application strategy evolves
- Multi-layered security which provides the flexibility to deploy the right security in the right place, either on-premise or cloud-delivered
- Simplicity at enterprise scale which enables end-to-end policy from the user to the application over thousands of sites

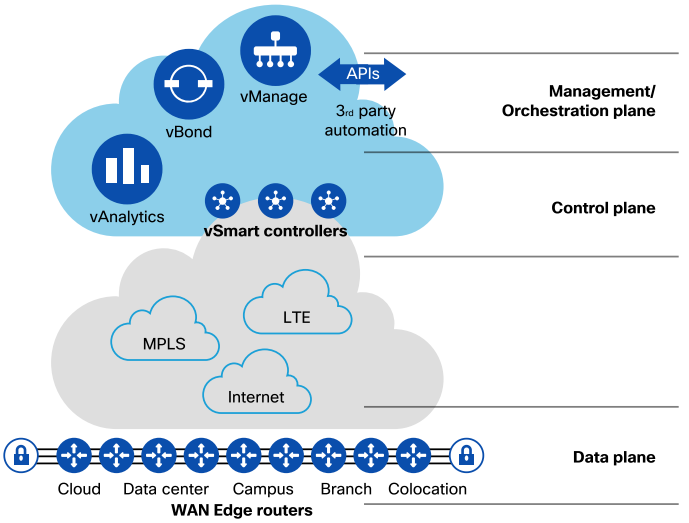
DIAGRAM Cisco SD-WAN Cloud-Scale Architecture



Components and architecture

The Cisco SD-WAN solution is a cloud-delivered Wide Area Network (WAN) overlay architecture that extends the principles of software-defined networking (SDN) into the WAN. The solution is broken up into four planes: data, control, management and orchestration.

DIAGRAM Applying SDN principles to the WAN



The Cisco SD-WAN solution contains four key components responsible for each plane of organization:

Cisco vManage

In the management plane, Cisco vManage represents the user interface of the solution. Network administrators and operators perform configuration, provisioning, troubleshooting, and monitoring activity here. vManage offers both a single-tenant dashboard and a multitenant dashboard for a variety of customer and service provider deployments.

Cisco vBond

Cisco vBond resides in the orchestration plane. The vBond controller is largely responsible for the Zero-Touch Provisioning process as well as first-line authentication, control/management information distribution, and facilitating Network Address Translation (NAT) traversal. When a router boots up for the first time in an unconfigured state, vBond is responsible for onboarding the device into the SD-WAN fabric. It is the job of vBond to understand how the network is constructed and then share that information amongst other components.

Cisco vSmart

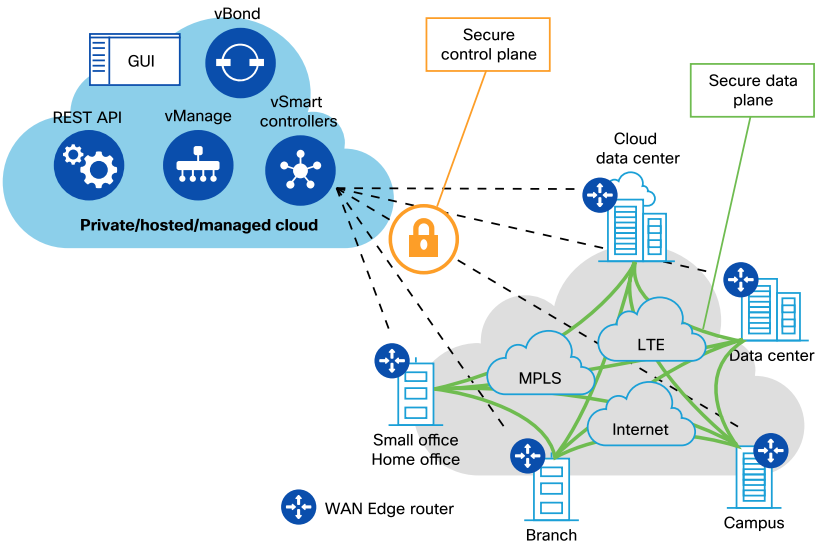
Cisco vSmart is the "brain" of the solution and exists within the control plane. As policies are created on vManage, vSmart is the component responsible for enforcing these policies centrally. When branches come online, their routing information is exchanged with the vSmart controller and not directly with other branches. By using policies, routing information is influenced and shared with other locations which determines how individual branches will communicate with each other. As routes are received via the Overlay Management Protocol (OMP) from branch locations, the vSmart controller can invoke policy created on vManage against these routes and control how traffic traverses the SD-WAN fabric.

Cisco WAN Edge routers

Cisco WAN Edge routers are responsible for establishing the network fabric and forwarding traffic. Cisco WAN Edge routers come in multiple forms, virtual and physical, and are selected based on the connectivity, throughput, and functional needs of the site.

All of these components combine to form the Cisco SD-WAN fabric. In the following diagram, notice the relationship between each of the components:

DIAGRAM Cisco SD-WAN fabric components



The WAN Edge routers form Internet Protocol Security (IPSec) tunnels with each other to form the SD-WAN overlay. In addition, a control channel is established between the WAN Edge routers and each of the control elements. Through this control channel, each component receives configuration, provisioning and routing information. Note that no data plane traffic is forwarded to the control infrastructure.

Overlay Management Protocol (OMP)

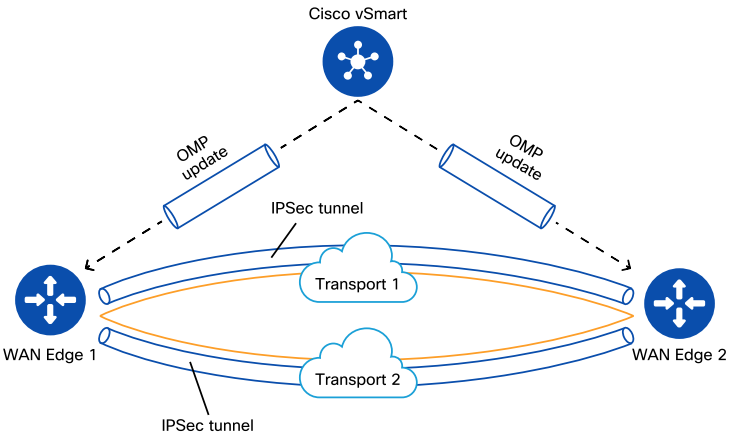
Cisco SD-WAN uses OMP which manages the overlay network. OMP runs between the vSmart controllers and WAN Edge routers where control plane information, such as route prefixes, next-hop routes, crypto keys, and policy information, is exchanged over a secure connection. If no policy is defined, the default behavior of OMP is to allow a full mesh topology, where each WAN Edge router can connect directly to other WAN Edge routers. OMP advertises three types of routes:

1. OMP routes are prefixes that are learned at the local site. The prefixes are redistributed into OMP so that they can be carried across the overlay. OMP routes advertise attributes including transport location (TLOC) information, which is similar to a BGP next-hop IP address for the route, and other attributes such as origin, originator, preference, site ID, tag, and VPN. An OMP route is only installed in the forwarding table if the TLOC to which it points is active.

2. TLOC routes are the logical tunnel termination points on the WAN Edge routers that connect into a transport network. A TLOC route is uniquely identified and represented by a three-tuple, consisting of system IP address, link color, and encapsulation.

3. Service routes represent services (such as firewall, IPS, application optimization, etc.) that are connected to the WAN Edge local-site network and are available for other sites for use with service chaining. In addition, these routes also include VPNs. VPN labels are sent in this update type to tell the vSmart controllers which VPNs are serviced at a remote site. For more information on service chaining, see the *Leveraging colocations* chapter later in this book.

DIAGRAM OMP



Bi-directional Forwarding Detection (BFD)

The BFD mechanism is used by the WAN Edge routers to probe and measure the performance of the transport links. It also determines the best performing path based on the result of the BFD probes, giving information about latency, jitter and loss on all the transport links.

High availability and redundancy

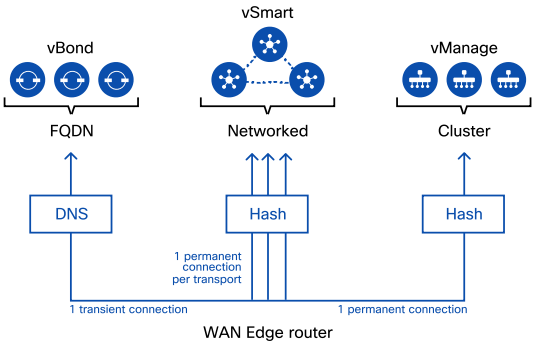
The Cisco SD-WAN solution is designed with application availability and performance as a cornerstone. The goal of any high-availability solution is to ensure that network services are resilient to failure. The core of the Cisco SD-WAN high-availability solution is achieved through a combination of three factors:

- **Device redundancy**: The strategy consists of installing and provisioning redundant devices and redundant components within hardware. These devices are connected by a secure control plane that operates in an active/active fashion.
- **Robust network design**: Support for multiple protocols (such as VRRP, BGP, and OSPF) and redundant physical connections to both LAN and WAN segments.
- **Software mechanisms**: Software mechanisms ensure rapid recovery from both direct and indirect failure. To provide a resilient control plane, the solution regularly monitors the status of all WAN Edge routers in the network and automatically adjusts to changes in the topology as routers join and leave the network. For data plane resilience, the Cisco SD-WAN software implements standard protocol mechanisms, specifically BFD, which runs on the secure IPsec tunnels between WAN Edge routers.

Control plane redundancy

Orchestration level redundancy is achieved by having one DNS name (FQDN) with multiple IP addresses representing different vBond controllers. Control plane redundancy is implemented with multiple vSmart controllers, one WAN Edge router will create a hash and contact two of the redundant vSmart controllers by default. Network management system redundancy can be achieved by building clusters with multiple vManage instances.

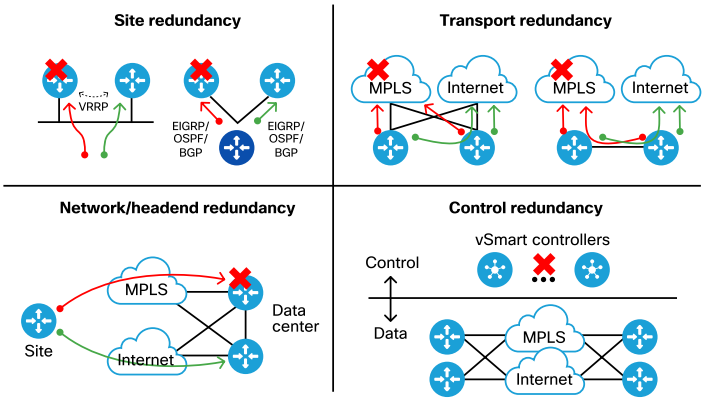
DIAGRAM Control plane redundancy



Data plane redundancy

Data plane redundancy is achieved on multiple levels. It starts with site redundancy, making sure that clients on the LAN side will use protocols like Virtual Router Redundancy Protocol (VRRP) or routing protocols, such as BGP, OSPF, or EIGRP. Features like TLOC extension help to build transport redundancy by using the cross link between two redundant WAN Edge routers. Network level redundancy is implemented by multiple geo-redundant data centers.

DIAGRAM Data plane redundancy



Putting it all together

As a result of its architecture, the simplified workflow to bring up a Cisco SD-WAN overlay is:

1. Build the configuration templates for the WAN Edge routers that will be joining the SD-WAN overlay.
2. As WAN Edge routers are located, powered on and cabled, they will begin the process of Zero-Touch Provisioning. These WAN Edge routers will utilize their connected circuits to contact the Cisco-hosted Plug-and-Play service. This hosted service will redirect the WAN Edge router to the vBond which will authenticate the device and allow it to receive its template configuration from the vManage.
3. Once the WAN Edge router is configured, it will build a channel to the vSmart.

4 As control plane connectivity is established, the WAN Edge router will set up OMP peerings with vSmart controllers. This peering allows the WAN Edge router to learn routing information about all other sites as well as information to facilitate its IPSec connection to remote branches.

5 As IPSec tunnels are established to form the SD-WAN overlay, WAN Edge routers will begin the process of forming BFD adjacencies with each other, based on the policies.

Platforms

The Cisco SD-WAN solution can be deployed on a number of different platforms, commonly called WAN Edge routers, which are available in different form factors. The WAN Edge routers can be used in either the branch, campus, data center, public cloud or a private cloud, such as a co-location facility. Regardless of which deployment is chosen, all WAN Edge routers will be part of the SD-WAN overlay fabric and are managed through vManage. There are two types of platforms that can be deployed as part of Cisco SD-WAN:

1. Hardware platforms

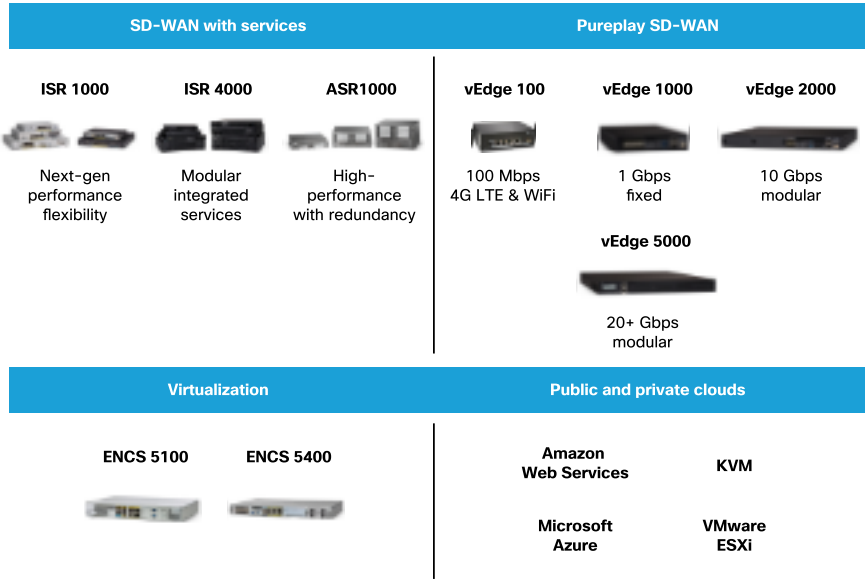
- Cisco vEdge (formerly Viptela vEdge) Routers running Viptela OS
- Integrated Services Router (ISR) 1000 and 4000 Series running IOS® XE SD-WAN Software
- Aggregation Services Router (ASR) 1000 Series running IOS XE SD-WAN Software

2. Virtual platforms

- Cloud Services Router (CSR) 1000v running IOS XE SD-WAN Software
- vEdge Cloud Router running Viptela OS

Virtual platforms can be deployed on Cisco x86 compute platforms, for example, the Enterprise Network Compute System (ENCS) 5000 Series, Unified Computing System® (UCS), and Cloud Services Platform (CSP) 5000 Series. Virtual platforms can also run on any x86 device using a hypervisor such as KVM or VMware ESXi.

DIAGRAM Hardware platforms and deployment cases



Cloud

Cisco SD-WAN offers a seamless way of connecting to applications in the cloud and extending the network to the cloud from any site including the data center (DC), hub or branch.

Using Cloud onRamp for Software as a Service (SaaS), connectivity to certain SaaS-based applications, such as Salesforce or Office 365, is optimized by choosing the best available path. Path selection is based on performance measurements obtained from all available paths. In the case of performance degradation on a path, the traffic will be moved dynamically to a more optimal path. Refer to the *SaaS optimization* section for more information.

The Cisco SD-WAN solution helps to automate connectivity between workloads in the public cloud from the branch or the DC. Using Cloud onRamp for Infrastructure as a Service (IaaS) from vManage, the virtual WAN Edge router instances are automatically spun up in the cloud to bring hosted services as part of the SD-WAN overlay. Refer to the *Extend SD-WAN to public clouds* section for more information.

By utilizing the Cloud onRamp for Colocation solution, application traffic can be steered towards the colocation facility and then sent to the destination in order to regionalize services and cloud access. Cloud onRamp for IaaS and Cloud onRamp for SaaS can be utilized to optimize IaaS and SaaS traffic from the colocation facility as well. Refer to the *Leveraging colocations* section for more information.

This book covers cloud-based SD-WAN scenarios and use cases comprehensively in individual chapters.

Security

Cisco SD-WAN architecture provides strong security for control plane, data plane, and management plane operations. This is explained in more detail in the *Meeting compliance requirements* chapter.

To enable the SD-WAN branches to have Direct Internet Access (DIA) without dependency on another device or solution for security, strong threat defense mechanisms are built into the WAN Edge router. This ensures the protection of user traffic at branch networks from internet threats, and it also improves the application performance, allowing traffic to securely use DIA when that is the optimal path.

Following are the threat defense features which are available on the WAN Edge router:

- Stateful application firewall
- Intrusion Protection & Detection (IPS/IDS)
- URL filtering
- Cisco Advanced Malware Protection (AMP) and ThreatGRID®
- Cisco Umbrella® DNS
- Tunneling to secure internet gateways in the cloud (third parties)

For more details on the threat defense features and how these can be used, please refer to the *Secure direct internet access* chapter.

Application experience

The Cisco SD-WAN solution provides multiple techniques to improve the application experience of end users. These include:

- Quality of Service (QoS) - provides application traffic prioritization.
- Forward Error Correction (FEC) and packet duplication features - remediates loss over poor quality circuits.
- Application-Aware Routing - provides SLAs and dynamic routing for critical business applications.
- TCP optimization - fine-tunes the processing of TCP data traffic to decrease round-trip latency and improves throughput
- Cloud onRamp for SaaS - optimizes performance for SaaS applications by dynamically measuring application performance and choosing the best path

See the *Improving application experience* chapter for more information on optimizing the application experience and see the *SaaS optimization* chapter for more detailed information on that solution.

Management and operations

The key benefits of the Cisco SD-WAN solution are automated management and simplified operations. Cisco vManage offers a single pane of glass for all management, monitoring, and troubleshooting aspects of the Cisco SD-WAN solution. Cisco vManage allows administrators to provision new sites, deploy policies, provide deep insights into application visibility and performance, check device health, perform software upgrades, and much more. Cisco vManage employs role-based access control (RBAC) to segregate duties by assigning different access privileges.

Cisco vManage exposes a rich set of REST APIs that can operate the entire Cisco SD-WAN solution. These APIs can also be used for user-defined automation and for integration into other orchestration systems or tools.

Cisco vAnalytics offers an additional SaaS-based service to provide more information about network health and availability, application performance and anomalies, and forecasting of network and application utilization for better capacity planning.

Cisco SD-WAN supports multitenancy, offering enterprises the flexibility of segregated operation. Multitenancy can also be used by partners and service providers to provide Cisco SD-WAN service offerings to their customers.

See the *Simplifying operations*, *Cisco SD-WAN APIs*, and *SD-WAN managed services* sections for more information on management and operations of the SD-WAN solution.

Improving application experience

Business need

Although networks are built to carry application traffic, delivering an optimal application experience is one of the most critical aspects of achieving higher user productivity. What does it take to deliver optimal application experience? The answer depends on a set of conditions and behaviors present in the network. It is a multidimensional problem to solve and much thought needs to be given to do so.

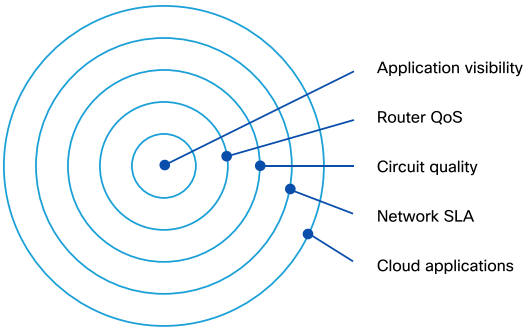
SD-WAN solutions need to be employed in a way that can make application quality issues less likely to appear, but should they appear, the network should respond with an automated remediation to minimize or eliminate any adverse impact.

Delivering optimal experience for business-critical applications requires an understanding of the applications in the network and appropriate controls to be applied to achieve the desired outcomes. Some issues impacting an application's quality of experience include:

- Data loss over poor quality circuits.
- Excess delay or jitter on a circuit impacting voice or other business-critical applications.
- Latency due to backhauling cloud traffic to a central data center.
- Inappropriate prioritization of business critical traffic on lower bandwidth links.

The Cisco SD-WAN solution can address these issues by offering a diverse set of capabilities to optimize Application Quality of Experience.

DIAGRAM Tools for optimizing Application Quality of Experience

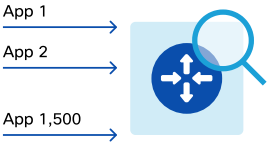


Application visibility

With applications moving to the cloud and increasing use of social media and streaming services, enterprise networks are carrying a growing volume of both business and recreational web traffic. Often, business applications, including cloud applications such as Office 365 and Cisco Webex®, use the same HTTP and HTTPS protocols used by recreational web traffic.

To optimize application performance and define policy for the applications utilizing the network, administrators need detailed visibility into the different types of applications running on the network.

DIAGRAM Deep Packet Inspection visibility



The Deep Packet Inspection (DPI) engine integrated into Cisco WAN Edge routers leverages multiple technologies to recognize more than 1,500 applications including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. Once applications are classified, policy can be set to prioritize business-critical applications and choose the WAN path with better SLA metrics.

Quality of service

WAN Edge routers play a pivotal role in delivering optimal application experience by enforcing behavior on application traffic as it gets routed between users and applications across the wide area network. Three key solution behaviors enforced on WAN Edge routers include:

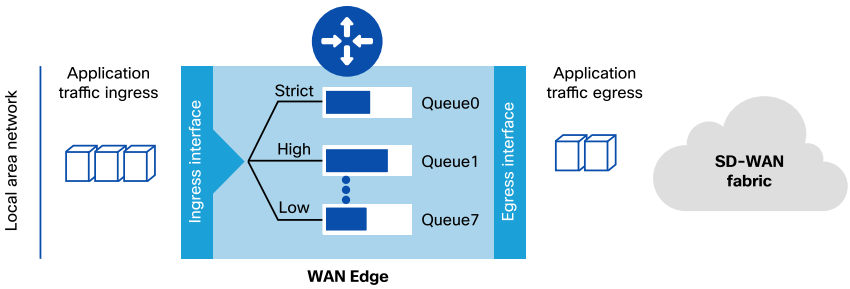
- Application traffic prioritization
- Mapping application traffic into service provider classes of service
- Avoiding excessive application traffic fragmentation

Application traffic prioritization

The application landscape is diverse and not all applications are created equal. Some applications need lots of bandwidth, some only care about the lowest possible delay (latency), some are sensitive to loss, and some perform poorly when delivered at variable delay intervals (jitter). As application traffic traverses WAN Edge routers, it typically traverses from a high bandwidth local area network, where network resource contention is uncommon, to a lower bandwidth wide area network, where at times "every bit counts." Even though the use of high-capacity broadband circuits as part of the Cisco SD-WAN solution has dramatically improved the situation, wide area network resource contention is still a problem.

In times of wide area network congestion, WAN Edge routers can employ QoS which helps prioritize business-critical traffic over lower classes of traffic. Queueing is used to help achieve this. Weighted round robin scheduling can allow different applications to get a fair share of the bandwidth while strict priority queuing can minimize jitter and latency for time-sensitive applications. WAN Edge routers can also employ mechanisms such as traffic shaping and traffic policing in order to comply with circuit capacity delivered by the carrier. Cisco vManage provides an interface for configuring QoS policies, as well as monitoring their behavior.

DIAGRAM Quality of Service



Mapping application traffic into service provider classes of service

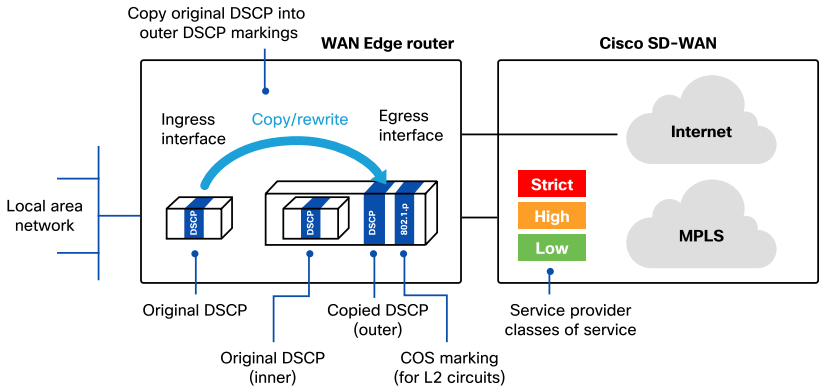
Cisco SD-WAN operates in a transport-independent fashion, leveraging any and all circuits provisioned on the WAN Edge router. Those circuits are responsible for delivering the actual application traffic between SD-WAN sites. When leveraging private circuits, a service provider may provision specific classes of service to prioritize application traffic as it traverses the core of their network. The mapping of application traffic into service provider classes of service is typically done by matching on DSCP markings, in the case of Layer 3 circuits, or by matching on a COS marking, in the case of Layer 2 circuits. Both DSCP and COS markings exist within the header of a datagram.

The Cisco SD-WAN solution leverages tunneling technologies such as IPsec or GRE to encapsulate application traffic before it is sent over wide area network circuits. This encapsulation places additional IP headers around the packet which "hide" the original IP headers and prevent a service provider from enforcing traffic prioritization. The Cisco SD-WAN solution, however, works alongside the service provider's class of

service prioritization by copying the original DSCP markings from the inner encapsulated IP header into the newly added outer IP header. In the case of Layer 2 circuits, the solution can also enforce COS marking on egressing frames.

Some service providers offer a fewer number of classes as compared to the number of classes used in the enterprise. With the Cisco SD-WAN solution, there is the ability to rewrite the original DSCP value into a different DSCP value in the outer header to match the classes supported by the service provider.

DIAGRAM Mapping application traffic into service provider classes of service



Allowing the service provider to honor their classes of service will go a long way to ensure adequate application experience over private transports. Internet circuits do not typically offer any type of QoS guarantees and other methods of ensuring optimal application experience are needed for traffic routed over these circuits.

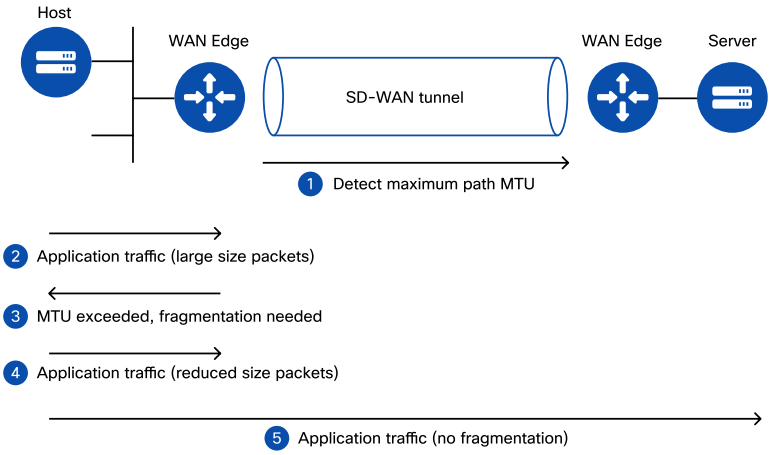
Avoiding application traffic fragmentation

Network circuits and router interfaces define the maximum transmission unit (MTU) size for any datagram transmitted through them (measured in bytes). IP packets exceeding the MTU size must be broken into segments before being transmitted. Application hosts communicating over the network may prohibit fragmentation by

setting a "do-not-fragment" (DF) flag within the IP header. DF markings can also be used in the process of path MTU discovery (PMTUD) to allow hosts to discover the MTU over the transit network before fragmentation must occur. This is a very important element of efficiency, since fragmentation and, more critically, re-assembly of fragments, can consume a considerable amount of processing power - which otherwise would have been utilized to process application traffic.

Since Cisco SD-WAN leverages IP encapsulation to send traffic between SD-WAN sites, additional headers are introduced that decrease the overall MTU available throughout the fabric. The increasing use of internet circuits raises the likelihood of an adverse effect of MTU reduction at inter-connect points between different service providers. To maintain optimal application experience, the Cisco SD-WAN fabric proactively discovers path MTU over all SD-WAN tunnels. It also interoperates with the host path MTU discovery process by notifying them of the MTU available through the fabric.

DIAGRAM Path MTU discovery process



Circuit quality

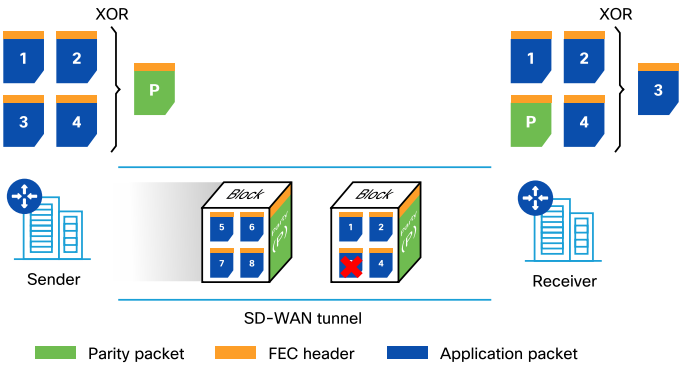
Using SD-WAN, internet circuits can be utilized for critical application traffic. Today's internet provides high bandwidth, however, the quality of experience is still not as reliable when compared to premium WAN circuits such as MPLS. As such, some applications may see occasional packet loss. Cisco SD-WAN provides circuit remediation features that allow applications to recover from packet loss without compromising performance.

Critical application traffic over an internet circuit

The Cisco SD-WAN Forward Error Correction (FEC) feature can be used to guarantee critical traffic works well across unreliable WAN links. FEC is a mechanism to recover lost packets on a link by sending extra “parity” packets for every pre-defined group of four packets. The receiving WAN Edge router can recover any lost packet from the group, using the received parity packet and performing an XOR calculation. This allows application performance to be preserved without the retransmission of application data.

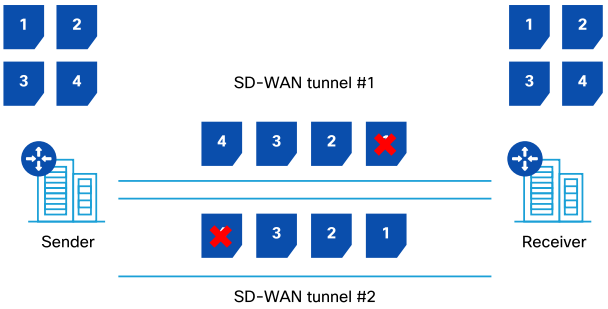
The figure below demonstrates FEC and shows application packet number three lost on the WAN link:

DIAGRAM Forward Error Correction feature



In addition to FEC, the Cisco SD-WAN Packet Duplication feature can be used to send the same application flows across multiple links to increase application reliability. If some packets of the flow are lost on a specific circuit, the receiving WAN Edge router uses the duplicate packets from the other circuit to recover the lost packets for that traffic flow.

DIAGRAM Packet Duplication feature



Be aware that Packet Duplication, although it increases application availability significantly, does so at the cost of increased bandwidth consumption. As a result, it should be enabled with caution.

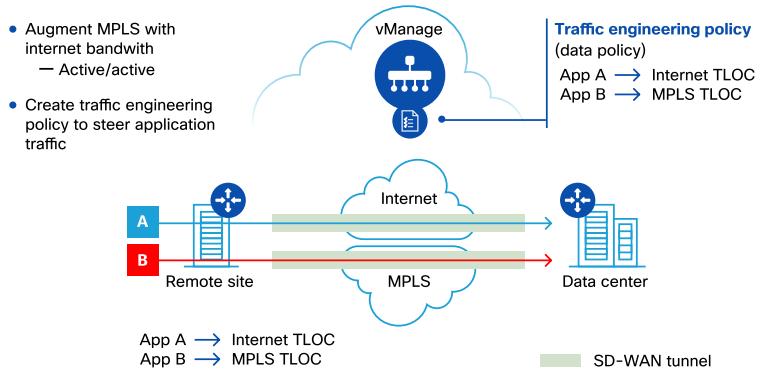
Meeting SLAs

Every customer has an urgent need to meet SLA requirements for critical applications across their network. SLA requirements consist of latency, loss, and jitter thresholds. Customers can meet these requirements using optimization techniques such as TCP-Optimization, Wide Area Application Services (WAAS), bandwidth augmentation, or by using Application-Aware Routing policies.

Bandwidth augmentation

Using bandwidth augmentation, customers can offload traffic from higher quality circuits such as MPLS to commodity internet circuits to achieve the same SLA for their applications. In theory, multiple internet circuits can achieve the same (or better) availability and performance as a single premium circuit at a fraction of the cost. Cisco SD-WAN provides the flexibility to choose all available transport bandwidth and extends this same level of availability and performance to the application. Cisco SD-WAN policies can be used to ensure identified traffic is mapped to the appropriate circuit. For example, voice is sent on MPLS and web browsing to the internet.

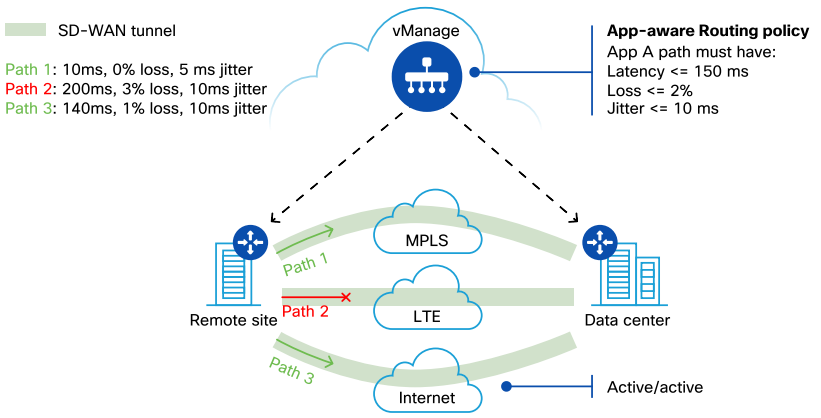
DIAGRAM Bandwidth augmentation



Application-based routing using Cisco SD-WAN

SLA-based policies can be used for choosing the optimal path for critical applications and dynamically switching the path in the event those SLAs are not met. Within the Cisco SD-WAN solution, these policies are part of a feature known as Application-Aware Routing. Application-Aware Routing policies can be defined in such a way, for critical applications, that strict SLAs are defined and a specific path is configured to be taken if the path meets the SLA. For example, the MPLS transport for voice traffic is chosen if MPLS is meeting the configured SLA. Another option would be to define the SLA such that traffic could be sent over any path that is compliant. In the figure below, only path 1 and 3 are meeting the SLA for Application A, therefore Application A flow will choose path 1 or 3 to reach the data center from the remote site.

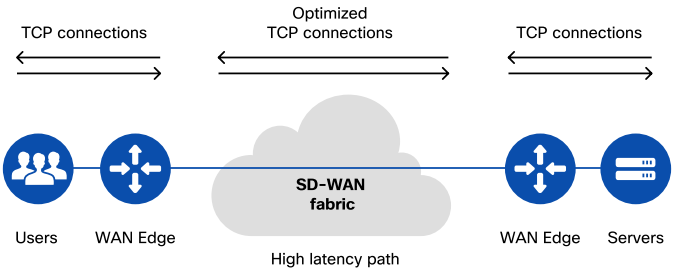
DIAGRAM Application-Aware Routing



TCP Optimization

The Cisco SD-WAN TCP Optimization feature uses TCP Selective Acknowledgement (SACK) to prevent unnecessary retransmissions and large initial TCP window sizes in order to maximize throughput and achieve a better quality of experience.

DIAGRAM TCP Optimization feature



Cloud application performance

Cisco SD-WAN provides the Cloud onRamp feature which allows visibility into SaaS applications and makes real-time forwarding decisions. In addition, Cloud onRamp also provides seamless integration with IaaS cloud service providers to improve cloud-based application experience.

Improving SaaS application experience

Enterprise software providers, such as Microsoft and Salesforce, deliver many applications over the internet via Software as a Service (SaaS). Latency and packet loss impact the performance of these applications, but in legacy networks, network administrators have little visibility into network characteristics between end users and SaaS applications. When a path is impaired in a legacy network, the manual process of shifting application traffic to an alternate path is complex, time-consuming, and error-prone.

Cloud onRamp for SaaS addresses these issues by optimizing performance for SaaS applications in the Cisco SD-WAN overlay network. From a central dashboard, Cloud onRamp for SaaS provides clear visibility into the performance of individual cloud applications and automatically chooses the best path for each one. It responds to changes in network performance in real-time, intelligently re-routing cloud application traffic onto the best available path. For more details, refer to the *SaaS optimization* chapter of this book.

Leveraging colocations

The Cloud onRamp for Colocation feature can be used as a gateway for SaaS applications in order to provide a redundant path. Ideally, Cisco Cloud onRamp for Colocation clusters will be placed in colocations that have direct connectivity to the SaaS provider's resources. It is important to get user traffic to the nearest colocation quickly and efficiently in order to capitalize on the colocation's high-speed tranport into the SaaS provider's cloud. When coupled with the Cloud onRamp for SaaS feature, application probes will also be sent through each colocation facility to measure loss and latency. In theory, the colocation will have the best loss and latency into the provider's

cloud and, hence, could be chosen as the primary path for reaching the application. In the event of loss or latency within the colocation, one of two outcomes are possible: the traffic will divert to the "next best" performing colocation, or alternatively, will utilize the locally attached internet circuit.

For more information on the Cloud onRamp for Colocation feature, please refer to the *Leveraging colocations* chapter in this book.

Improving IaaS application experience

Cloud onRamp for IaaS extends the fabric of the Cisco SD-WAN overlay network into public cloud instances, allowing branch routers to connect directly to public cloud application providers. By eliminating the need for a physical data center to provide this connectivity, Cloud onRamp for IaaS improves the performance of IaaS applications. The Cloud onRamp for IaaS feature works in conjunction with AWS Virtual Private Clouds (VPCs) and Azure Virtual Networks (VNETs).

For more details on this feature, please refer to the *Extend SD-WAN to public clouds* chapter in this book.

Case study

One of the largest banks in the United States, with more than 1,100 locations and almost 2,500 automated teller machines (ATMs), was looking for an SD-WAN solution for their 1,400 locations in order to achieve the following major goals:

- Improve customer experience for applications such as self-service kiosks, video conferencing with live experts, and new retail bank applications.
- Reduce overhead related to compliance and security.
- Share real-time data with financial technology partners.
- Simplify operations for branches and ATMs.
- Become more API-driven.

The chosen solution was a managed service built with Cisco SD-WAN which dramatically improved service delivery and quality of experience. It significantly shrunk the time needed to deliver higher bandwidth capacity to remote locations from 60 days to just a few days by leveraging the internet as transport alongside MPLS. Application performance improved due to dynamic SLA-based traffic routing over MPLS, internet, and LTE circuits. The higher performing network helped with data loss prevention and backup as well. In addition to enabling video and Wi-Fi in the branches, this network foundation helped the bank to move to agile development, use a nimbler web services architecture, and securely connect with financial technology partners. Centralized software updates driven by Cisco vManage were used to quickly update the network.

Key takeaways

Application performance is critical for business continuity and user experience. Network degradation and improper design can have an adverse impact on application performance. Cisco SD-WAN has many capabilities that can tremendously improve application experience. Each of the previously discussed features can be enabled individually, or in combination, to ensure that critical application traffic maintains a high level of quality.

The Cisco SD-WAN solution is able to provide:

- Quality of Service, including application prioritization and choosing the optimized path based on required SLAs for critical applications.
- Circuit remediation for critical traffic, so as to improve the end-user experience for traffic traversing poor quality circuits.
- Integration into cloud SaaS and IaaS providers to offer the best possible application experience.

Further reading

- Cisco SD-WAN Cloud onRamp for SaaS: *http://cs.co/onramp*
- Cisco Validated Design: Cloud onRamp for SaaS Deployment Guide: *http://cs.co/onramp-saas-cvd*

Secure direct internet access

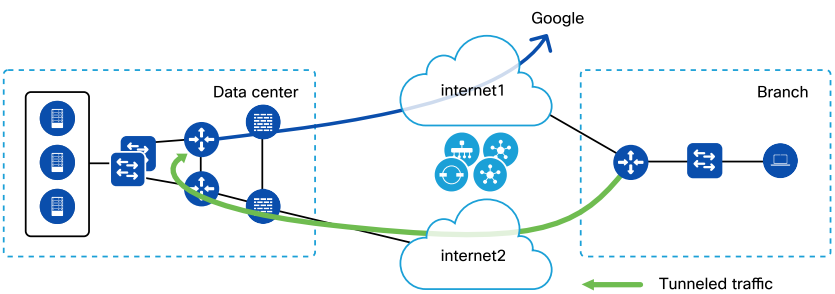
Business need

In traditional wide-area networking, internet traffic from a branch site is sent to a central location such as a data center or regional hub site. This allows traffic returning from the internet to be scrubbed by a security stack before being sent back to the branch. This is traditionally done due to the prohibitive cost of deploying a security stack in every location.

As the demand for internet traffic is increasing, more companies are utilizing cloud services such as SaaS (e.g Office 365, Box) and IaaS. In addition, more applications are internet-based, more business employees are teleworking, and Internet of Things (IoT) devices are demanding bandwidth as well.

Backhauling traffic to a central site for internet access causes increased bandwidth utilization at the central site. This is because traffic has to be tunneled to the central site before accessing the internet, which may also consume the premium bandwidth from branch to the central site. The security stack and network devices at the central site need to accommodate the incoming bandwidth from the branches. Applications also incur increased latency, resulting in a degradation of application performance.

DIAGRAM Backhauling internet traffic through a central site

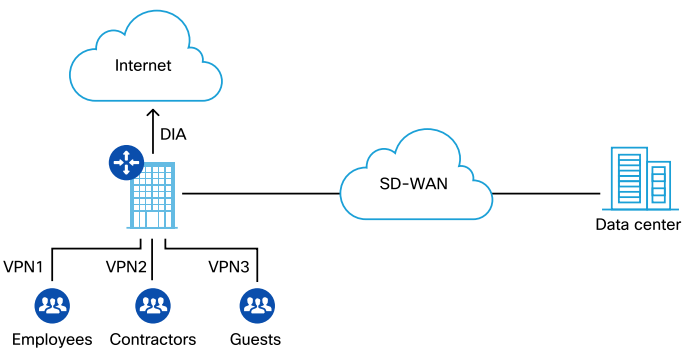


Direct Internet Access

Direct Internet Access improves internet experience for branch users by eliminating latency in backhauling traffic to a central site. It reduces bandwidth consumption at the central site, which thereby also reduces WAN costs.

The Cisco SD-WAN DIA solution is secure and easy to implement. DIA is configured for specific applications and keeps business-critical applications on premium WAN links. For example, DIA can be enabled for internet browsing and SaaS applications, whereas business-critical or latency-sensitive applications such as voice can remain on private WAN circuits. Inherent to the Cisco SD-WAN solution is the ability to segment users. Segmentation is useful in keeping employees and guests separate. Cisco SD-WAN allows DIA to be configured for a VPN segment, allowing control of internet access on a per VPN segment basis.

DIAGRAM DIA for different VPN segments from the branch



The users and branch network can be secured from the internet by implementing Cisco SD-WAN security features. Security features include application-aware firewall, intrusion protection, URL filtering, Advanced Malware Protection, and DNS security. These security features can be deployed either on the WAN Edge router itself, or as an integrated third-party security service.

Security policies

With Cisco SD-WAN, a branch can allow guest users or employees to access the internet directly which helps in:

- Improving application experience
- Offloading internet traffic from premium WAN connections
- Reducing the need for security appliances at every location, by providing in-built security features which include application-aware firewall, URL filtering, IPS/IDS, Advanced Malware Protection (AMP), and DNS security.

Guest access

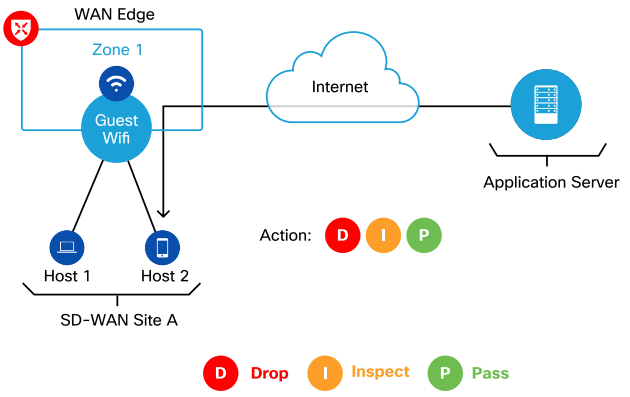
For guest access, security can be enabled either directly on the WAN Edge router, or by routing DIA traffic through a cloud security provider.

The key priorities for guest DIA traffic are:

- Restricting access to certain internet destinations
- Protecting the network from malware and/or malicious content
- Restricting bandwidth usage for guests.

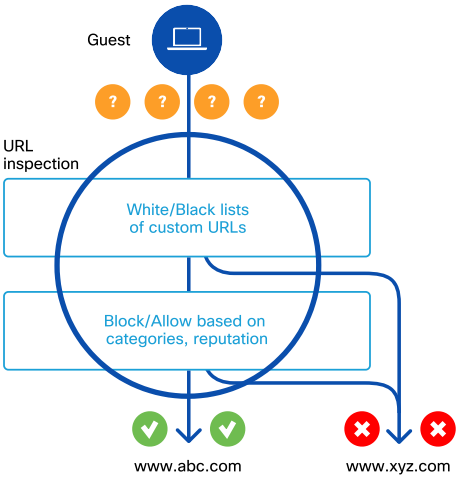
Application-aware firewall can be enabled on the WAN Edge router to inspect the traffic from guest devices to the internet. In the following diagram, the traffic between hosts and the application server over the internet gets inspected by the WAN Edge router.

DIAGRAM Application-aware firewall for DIA traffic from guest zone



URL-filtering works on the WAN Edge router to restrict the guest traffic from accessing certain destinations on the internet. In the diagram below, the guest user is allowed access to "www.abc.com" but is denied access to "www.xyz.com".

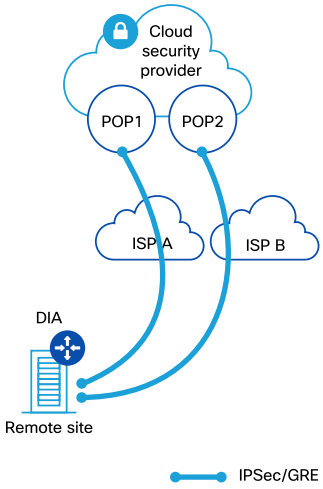
DIAGRAM URL filtering for DIA traffic from guest zone



Guest access through cloud security provider

Instead of enabling SD-WAN security on the branch router, the customer can also opt to route the internet-bound traffic to a cloud security provider. Traffic originating from the guest segment is redirected to the cloud security provider via point-to-point (IPSec or GRE) tunnels. In this case, the cloud security provider provides the required security filtering for DIA traffic.

DIAGRAM Guest DIA traffic through a cloud security provider



Employee access

As with guest access, employees can have access to internet destinations restricted by enabling SD-WAN security.

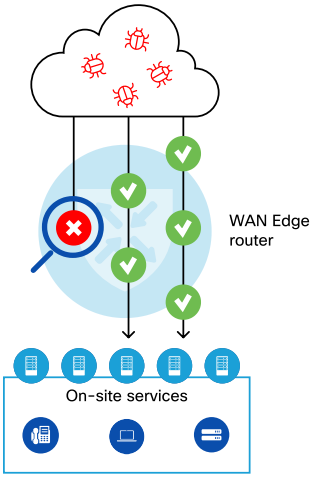
The key priorities for employee traffic are:

- Restricting access to certain internet destinations
- Detecting/preventing employees from downloading malware and/or malicious content

Along with application-aware firewalling and URL filtering, the WAN Edge router can be enabled with advanced security features such as IPS/IDS and AMP to prevent

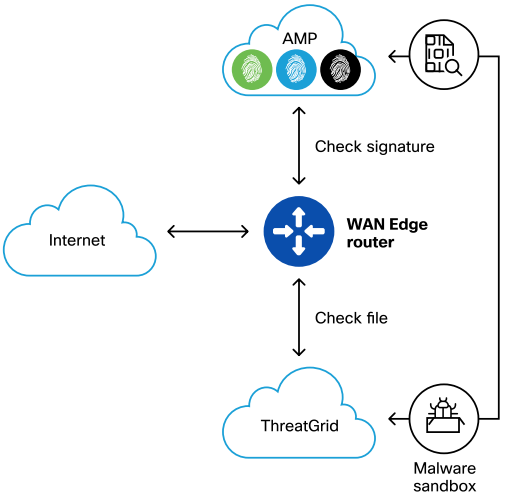
employees from downloading malicious content from the internet. In the following diagram, the WAN Edge router is enabled with IPS and prevents malicious packets from the internet entering the employee segment.

DIAGRAM IPS/IDS enabled to protect from internet threats



Leveraging the AMP feature, the WAN Edge router can prevent the employee from downloading a malicious file from the internet by checking the file reputation. The WAN Edge router talks to Cisco Threat Intelligence (CTI) in the background if file reputation is unknown and sandboxing is needed. Note that IPS/IDS and AMP features can also be used in the guest access use case if needed.

DIAGRAM File reputation and analysis

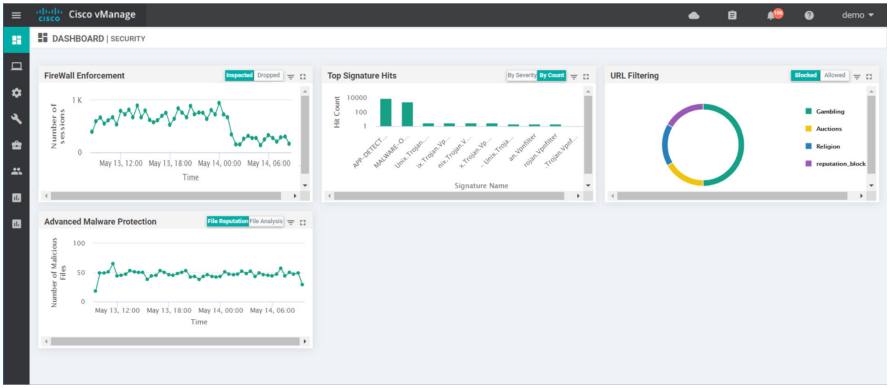


Security monitoring

The Cisco vManage dashboard can be used to monitor various factors for DIA traffic. For individual devices, factors such as interface bandwidth, application usage, real time flow information, and NAT translations can be monitored. The security dashboard can display the various aspects of security enabled for DIA traffic.

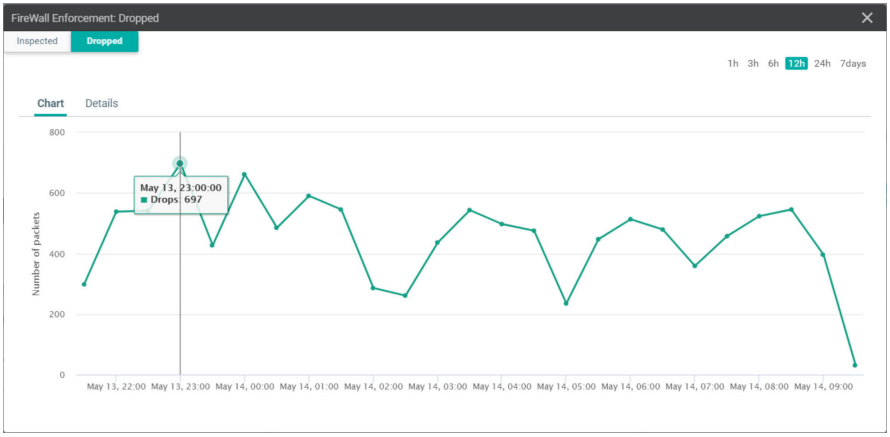
The following screenshot of the security dashboard shows firewall enforcement activity, IPS/IDS data, URL filtering results, and Advanced Malware Protection counts. Drilling down into each graph provides more information.

DIAGRAM SD-WAN security dashboard



Opening up the Firewall Enforcement graph details reveals how many inspections and drops occurred over time.

DIAGRAM Firewall Enforcement drops over time



In addition, specific session information can be obtained through vManage, by viewing Monitor > Network > Device > Real Time for any WAN Edge router. Similar information can be obtained for the other security features.

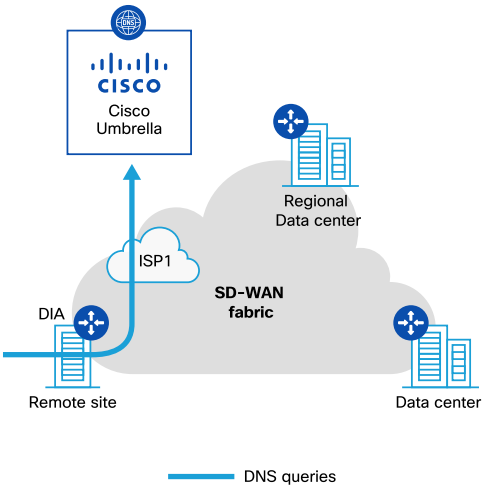
Case study

A large fashion retailer with over 1000+ locations was looking to increase the bandwidth at every location, to reduce the dependency on expensive private MPLS circuits, and provide better guest internet access.

As part of the Cisco SD-WAN deployment, the customer adopted a model of using WAN Edge router devices with dual internet circuits. These sites were also tied into Cisco Umbrella for DNS-based web filtering. This deployment model provided very desirable business outcomes - monitoring, integrated security, more bandwidth, and better performance with significant cost benefits.

The company now relies exclusively on internet connectivity for smaller sites and uses a combination of MPLS and internet circuits for larger and more critical sites. Having multiple internet circuits makes the network more reliable; if one fails, it can easily roll over to another one, and with DIA enabled, all the guest traffic goes to the internet directly. This vastly improves the end-user experience without exposing the environment to more risk, and ensures security policies are implemented in the environment.

DIAGRAM DNS-based web filtering through Cisco Umbrella for DIA traffic



Key takeaways

In traditional wide area networking, internet traffic from a branch site is sent to a central location such as a data center or regional hub site. This allows traffic returning from the internet to be scrubbed by a security stack before being sent back to the branch. This is traditionally done due to the cost-prohibitive nature of deploying a security stack in every location.

- Cisco SD-WAN allows Direct Internet Access at the branch with integrated security.
- This approach provides centralized control of the flow of internet-bound traffic using built-in security features.
- This helps to secure the network from internet threats and achieve better application experience.

Further reading

Configuring Direct Internet Access: *http://cs.co/config_local_internet_exit*

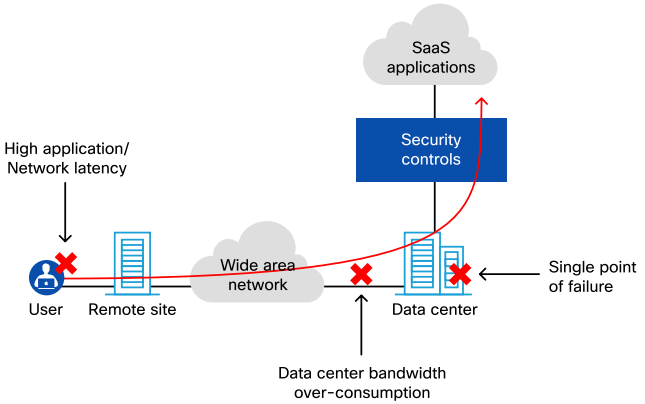
SaaS optimization

Business need

Traditional business applications hosted in enterprise data centers are evolving to become cloud-based and delivered as Software as a Service (SaaS). Access to SaaS applications is dependent on internet access. Properly engineered internet exit points play a pivotal role in ensuring optimal user experience when using SaaS applications. Unfortunately, the majority of existing wide area networks were not built with the cloud in mind. Internet-bound traffic is often sent through enterprise data centers, otherwise known as backhauling or hairpinning. This centralized internet access methodology was driven by the need to provide security controls for internet-bound traffic, traditionally offered only from the data centers. The use of data centers for cloud access holds several key inefficiencies:

- High application and network latency
- Data center bandwidth over-consumption
- Single point of failure

DIAGRAM Traditional centralized internet access through the data center



A different cloud strategy needs to be adopted in which access to SaaS applications, as well as security controls, is not dependent on data centers for cloud access.

Cloud onRamp for SaaS

The consumption of Software as a Service (SaaS) applications has increased over the last decade. The Cisco SD-WAN solution offers network intelligence to provide optimal user experience when consuming those applications. In the Cisco SD-WAN solution, this is called Cloud onRamp for SaaS.

In order to provide optimal SaaS application experience, it becomes essential to address the challenge of identifying and designing the path to the best-performing internet exit point. Cisco SD-WAN Cloud onRamp for SaaS achieves this by doing the following for every site:

- Identifies the sites
- Discovers SaaS applications
- Determines SaaS application performance
- Routes SaaS application traffic along the best peforming path
- Reports on Quality of Experience (vQoE) scores

Cloud onRamp for SaaS can also incorporate regional colocation facilities to diversify SaaS application access. This is done by choosing between one or more direct cloud access points at the remote site, and the regional cloud access point at the colocation facilities.

Identify the sites

The sites chosen to participate in the Cloud onRamp for SaaS solution are designated as having one of the following functions:

- DIA sites- sites with direct cloud access for local users.
- Gateway sites - sites with cloud access acting as gateways. DIA sites can use the gateway sites for routing SaaS application traffic in case of degraded performance across direct cloud access.
- Client sites - sites that do not have direct cloud access. They solely rely on the gateway sites for optimal SaaS applications routing.

Colocation centers can be used as gateway sites to provide SaaS access, providing flexibility to directly connect with a variety of telecommunications, network, and cloud service providers, while saving costs. The Cloud onRamp for Colocation solution allows creation of different VNF service chains, orchestrated in Cisco vManage and deployed on a cluster in a colocation facility. For more information on Cloud onRamp for Colocation, please refer to the *Leveraging colocations* chapter of this book.

Discover SaaS applications

Cloud onRamp for SaaS provides optimal experience for several popular SaaS applications. A number of popular SaaS applications are hosted at distributed cloud service provider data centers in different geographic locations for higher availability and better proximity to end clients. Microsoft Office 365 is one such application. The Cisco SD-WAN solution leverages DNS resolution from the WAN Edge routers participating in the setup in order to proactively discover the location (IP addresses) of the Office 365 service. DNS resolution is repeated periodically to accommodate any IP address changes of the Office 365 service. Office 365 is used as an example throughout the chapter, but the same solution logic applies to other supported SaaS applications.

Determine SaaS application performance

WAN Edge routers participating in Cloud onRamp for SaaS continuously perform quality probing using Hyper Text Transfer Protocol Secure (HTTPS) requests of the discovered IP addresses of the Office 365 service. These quality probes closely simulate end client application requests. This allows WAN Edge routers to discover the application quality experienced by end users.

The process of determining SaaS applications performance is carried out at the DIA sites across all direct cloud access paths, and also at the regional SaaS gateway sites. WAN Edge routers determine the best-performing path toward the SaaS applications based on the loss and latency characteristics detected by the HTTPS quality probes. For remote sites using a gateway site to access SaaS applications, the best performing path is calculated by measuring the performance of the entire path from the the remote site through the gateway to the SaaS application.

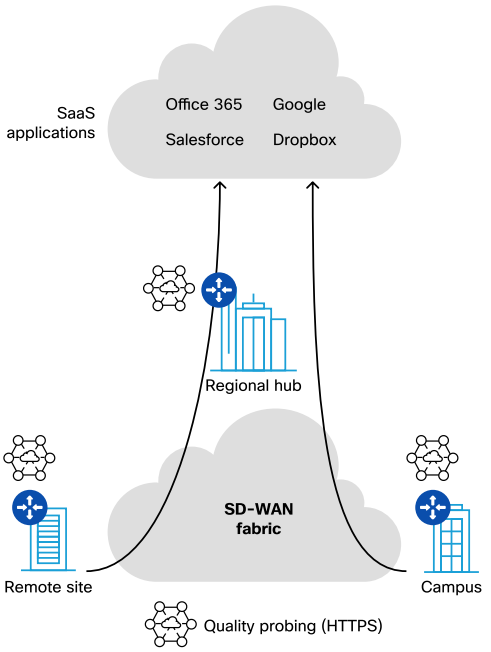
Route SaaS application traffic along the best performing path

WAN Edge routers detect applications by leveraging embedded application recognition capabilities, also known as deep packet inspection (DPI). The DPI engine is able to identify and classify more than 1000 applications and sub-categories of applications. For example, the Microsoft set of applications contains Exchange, Sharepoint, OneDrive, Skype, etc.

Once recognized, WAN Edge routers steer SaaS application traffic along the path with the best application quality of experience. This path may be through one of the direct internet access circuits at the local site or through the regional SaaS gateway across the SD-WAN fabric.

The process of quality probing is continuous and if a change in performance characteristics occurs, the WAN Edge router at the remote site can take an appropriate routing decision to maintain high quality of experience for the selected SaaS applications.

DIAGRAM Cloud onRamp for SaaS applications



Report on quality of experience (vQoE) scores

The user quality of experience when consuming SaaS applications is quantified as a vQoE score on a scale of 1 to 10, with 10 being the best, and 1 being the worst. The vQoE score takes into account the loss and latency characteristics discovered by the HTTPS quality probes. The quality score is calculated for all SaaS application exit points enabled with Cloud onRamp for SaaS solution.

Design considerations

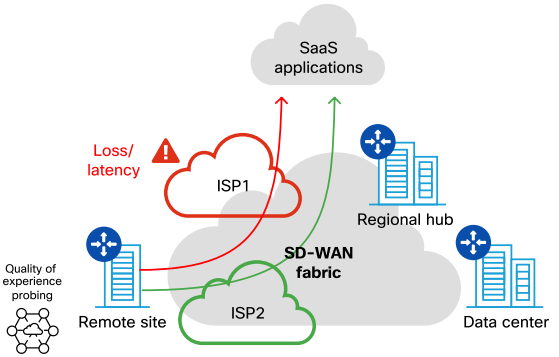
There are three possible design choices that can be utilized with Cloud onRamp for SaaS:

- Direct cloud access
- Gateway cloud access
- Direct cloud access with cloud security

Direct cloud access

In this case, Cloud onRamp for SaaS uses one or more direct internet access circuits at the remote site. Cloud onRamp for SaaS dynamically chooses the circuits which provide the best quality of experience for select SaaS applications.

DIAGRAM Cloud onRamp for SaaS with Direct Internet Access

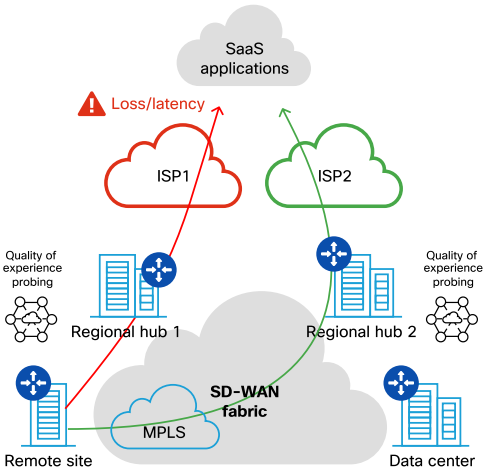


WAN Edge routers detect application quality of experience changes by continuously sending quality probes through all direct internet access circuits configured for Cloud onRamp for SaaS. In the case of multiple direct internet access circuits, WAN Edge routers will route SaaS application traffic across the circuit with the best application quality of experience score. Direct internet access at remote sites can be secured by the integrated SD-WAN security features. Both Cloud onRamp for SaaS and the SD-WAN security controls at the remote location are managed by Cisco vManage.

Gateway cloud access

In the gateway cloud access case, a site which has internet access can be designated as a gateway to reach SaaS applications for other sites. Gateway sites can include regional hubs, data centers, large branches, colocations, and can be in the public cloud as well. Gateways can be selected based on bandwidth, performance, and security features at those locations. Remote sites are configured as Cloud onRamp for SaaS client sites to the SaaS gateway sites. Cloud onRamp will measure performance from the client sites through the gateway to the SaaS application and ensure traffic takes the best-performing path.

DIAGRAM Cloud onRamp for SaaS through regional gateways

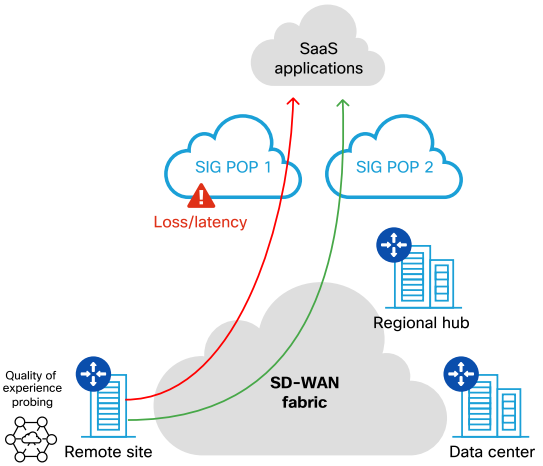


Direct cloud access through cloud security providers

Secure Internet Gateways (SIG) or Cloud Access Security Brokers (CASB) are approaches to enforcing security policies for SaaS application traffic. This model leverages security controls in the cloud rather than at the branch or colocation facilities.

Cloud onRamp for SaaS provides the path with the most optimal application experience from the remote site through one or more cloud security enforcement points.

DIAGRAM Cloud onRamp for SaaS through cloud security providers



Case study

This case study describes the SD-WAN efforts around SaaS adoption by Cisco IT. Cisco IT is responsible for all IT services within the Cisco worldwide network, spanning 92 countries. The network connects more than 400 offices over multiple topologies and transports to the regional hubs which deliver business-critical services to an agile and mobile workforce of connected employees and partners.

As the case with many of its customers, the Cisco application landscape is transitioning from data center applications to applications delivered in the SaaS model. Offloading internet traffic through direct internet access (DIA) circuits provisioned at the remote sites provided significant advantages, making effective use of wide area network bandwidth for applications hosted in Cisco data centers. Cisco IT evaluated and deployed Cloud onRamp for SaaS to optimize the experience for the most critical SaaS applications, Salesforce, Box, and Office 365 consumed by over 70,000 users at hundreds of remote locations.

The use of Cloud onRamp for SaaS allowed Cisco IT to customize area network capacity by moving SaaS applications to the direct internet access circuits based on the optimal application performance characteristics. Quality of Experience scores provided insight into the user application experience. Cloud onRamp for SaaS allowed Cisco IT to simultaneously use multiple direct internet access circuits to intelligently service multiple SaaS applications in an active fashion. Multiple DIA circuits also provided a degree of high availability to the SaaS applications.

Lastly, Cisco IT was able to leverage security controls across the DIA circuits, striking a delicate balance between optimal application experience and strong security posture.

For more information, please refer to the Cisco Live breakout session, BRKCOC-1236 at *http://cs.co/on-demand-library*

Key takeaways

The application landscape is changing and traditional application consumption is making way for SaaS applications delivered from the cloud. This transition is challenging existing wide area network designs which were not put in place with the cloud in mind. Cisco SD-WAN equips organizations with a cloud-friendly, easy-to-consume architecture that optimizes SaaS applications. Cloud onRamp for SaaS is a key element for organizations adopting SaaS applications.

Cloud onRamp for SaaS:

- Provides optimum path utilization for SaaS applications by leveraging a probing mechanism across all available transports
- Improves end-user experience due to loss and latency
- Helps achieve better application performance

Further reading

- Cisco SD-WAN Cloud onRamp for SaaS: *https://cs.co/onramp*
- Cisco Validated Design: Cloud onRamp for SaaS Deployment Guide: *http://cs.co/onramp-saas-cvd*
- Cisco SD-WAN Cloud onRamp for Microsoft Office 365: *http://cs.co/onramp-o365*

Extend SD-WAN to public clouds

Business need

Infrastructure as a Service (IaaS) is a set of basic computing resources that can be used to host and deliver enterprise applications over the internet. This includes storage, compute and networking components. With IaaS, the on-premise physical data center infrastructure is moved off-premise to a virtualized environment where computing resources are hosted by a public cloud provider such as Amazon Web Services (AWS) or Microsoft Azure. IaaS allows enterprise IT to choose when, how, and what computing resources to consume, and to quickly scale up or down as demands change, thereby drastically reducing the time to market.

Connecting an enterprise network to a cloud provider infrastructure can be challenging for IT since each cloud provider has different consumption models for connectivity. IT managers are looking for a seamless and automated way to extend their enterprise network into the public cloud. Enterprise IT also looks for a single overlay connectivity between multicloud and physical data centers and branches.

The following are the key reasons for integrating enterprise IaaS with Cisco SD-WAN:

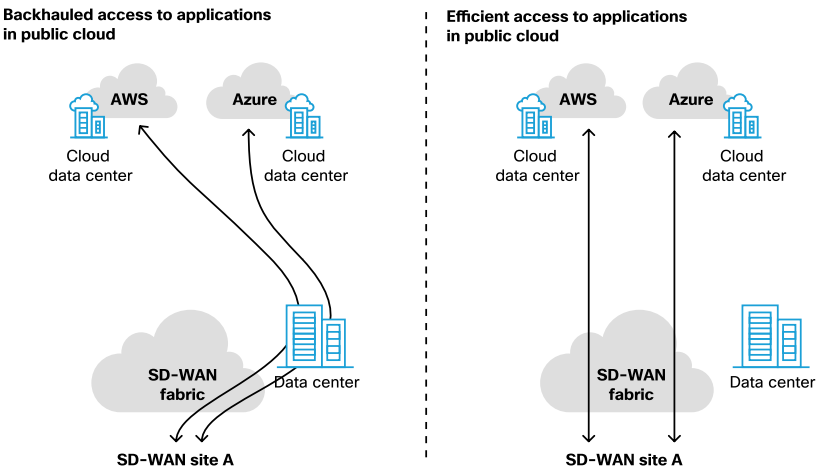
- Uses full SD-WAN capabilities in the cloud.
- Applies a common policy framework across SD-WAN and multiple clouds.
- Manages the cloud and physical routers via Cisco vManage.
- Ensures best infrastructure security.

Cloud onRamp for IaaS

The Cisco SD-WAN solution helps to automate connectivity to workloads in the public cloud from the branch or the data center (DC). Using this feature, the virtual WAN Edge router instances are automatically spun up via Cisco vManage in a specific region of the public cloud. These virtual instances become part of the SD-WAN overlay and establish data plane connectivity to the WAN Edge routers located in the branch or the data center. As a result, end-to-end connectivity is established between the workloads in the cloud, physical branches and data centers.

Cloud onRamp for IaaS provides a seamless extension of SD-WAN fabric into the public clouds. It improves the application performance hosted in the public cloud by eliminating the traffic from SD-WAN sites traversing through the data center. In addition, the Cloud onRamp for IaaS deploys a redundant pair of virtual routers providing path resiliency and high-availability to applications hosted in the public cloud.

DIAGRAM Efficient application access in public cloud using Cloud onRamp for IaaS



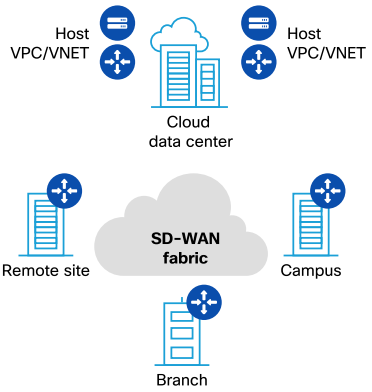
Design considerations

Amazon Web Services (AWS) and Microsoft Azure are two of the most common IaaS services used by customers worldwide. The Cisco SD-WAN solution allows extension of SD-WAN fabric intelligence into AWS and Microsoft Azure IaaS environments. There are two approaches to accomplish this.

- Cloud Gateway - a virtual WAN Edge router is manually deployed in each virtual network.
- Cloud onRamp for IaaS - a pair of virtual WAN Edge routers are deployed in a transit hub, acting as virtual aggregation routers.

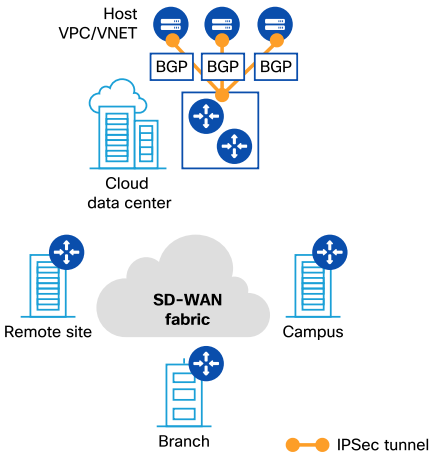
The first approach is to instantiate a virtual WAN Edge router in each AWS Virtual Private Cloud (VPC) or Microsoft Azure VNET. In this case the compute resources are directly attached to the WAN Edge router instance. This method is quite simple but requires deployment of a WAN Edge router instance into each existing (or new) VPC or VNET. This virtual router is seamlessly managed via vManage in the same way as any other physical router. It is available on both AWS and Azure Marketplace as a Bring-Your-Own-License (BYOL) instance.

DIAGRAM Cloud gateway



The second approach is called Cloud onRamp for IaaS. With Cloud onRamp for IaaS, a transit VPC/VNET (also known as gateway) can be leveraged to front-end all host VPCs/VNETs. A gateway VPC/VNET hosts a pair of redundant WAN Edge routers. Standard IKE-based IPSec connections are established between the gateway VPC/VNET and all the participating host VPCs/VNETs. The BGP routing protocol runs over these IPSec tunnels for mutual advertisement of SD-WAN fabric routes to the host VPCs/VNETs, and vice versa. In this approach, the gateway VPC/VNET becomes the entry point to the SD-WAN fabric and provides multipathing, security, segmentation and QoS. Multipathing can also be enabled by leveraging AWS Direct Connect or Azure Express Route and internet connectivity.

DIAGRAM Cloud onRamp for IaaS

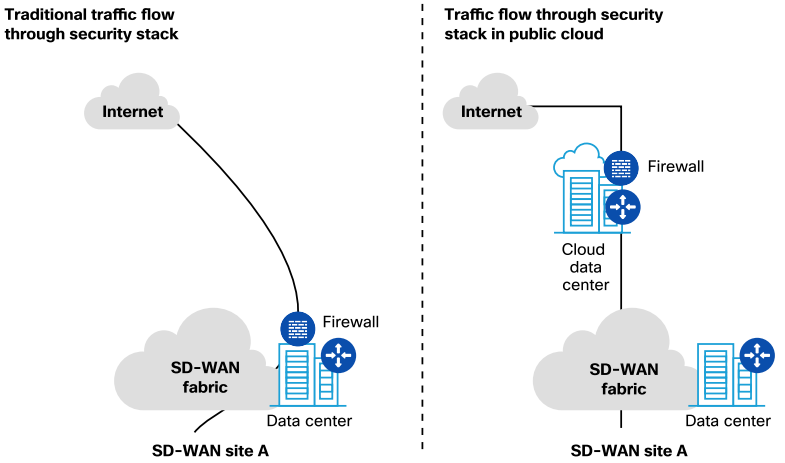


Cloud onRamp for IaaS can be used for extending SD-WAN into the public cloud. It can also be used to build a custom security stack in the public cloud.

Building a custom security stack in the public cloud

Cisco SD-WAN customers can build and use their own security stack (e.g firewall from vendor A, IPS from vendor B) in the public cloud as Virtual Network Functions (VNFs) hosted in their VPCs or VNETs. Any internet-bound traffic which requires further security analysis can be directed to the security stack running in the cloud through the SD-WAN fabric. Once the traffic reaches the cloud WAN Edge, it is filtered through the security stack and exits to the internet.

DIAGRAM Cloud security stack with Cloud onRamp for IaaS



Case study

Distributors play a key role in the food and beverage industry, serving as the intermediary between the manufacturer and their respective retail, restaurant, and food service customers. A Fortune 500 national food distributor was looking to connect all of its remote locations to the cloud without being vulnerable to a single point of failure. Driving this requirement was the need to add more bandwidth to deal with growth in cloud-based applications, and as the pace of business continued to increase, they were looking to move away from on-premise data centers into AWS to give them more flexiblity and agility.

Using Cisco SD-WAN and Cloud onRamp for IaaS, the customer was able to adopt a multicloud approach for their WAN. The customer was able to seamlessly extend their network (branch to cloud) into AWS by spinning up virtual instances of vEdge Cloud through the AWS marketplace and to manage all of their endpoints through Cisco vManage. By extending the SD-WAN fabric into the AWS cloud, the customer could connect their applications in the cloud with the rest of their network.

The key benefits include centralized management of security policy, greater agility through ease of deployment, and the ability to deliver applications faster to their customers. Most importantly, having the capability to quickly expand into the cloud means that the business can be more agile in terms of capital planning.

Key takeaways

Connecting an enterprise network to a cloud provider infrastructure can be challenging for IT since each cloud provider has different consumption models for connectivity. IT managers are looking for a seamless and automated way to extend their enterprise network into the cloud using single overlay connectivity between multicloud and physical data centers and branches.

Cisco Cloud onRamp for IaaS:

- Simplifies deployment in the public cloud.
- Provides seamless extension of the WAN into multiple public clouds.
- Shortens time required to onboard new or existing public clouds through automation.
- Reduces the on-premises security footprint by moving it to the public cloud, providing an optimal path to a secure gateway.
- Provides encrypted and direct access from branch sites giving IT maximum choice and control over their SD-WAN deployment.

Further reading

- Overview of Cisco SD-WAN Cloud onRamp configuration for IaaS
  http://cs.co/configure_onRamp_iaas
- Cisco Validated Design: Enabling Cisco Cloud onRamp for IaaS with AWS
  http://cs.co/onramp-iaas-cvd

- Configuring Cisco SD-WAN Cloud onRamp for IaaS with AWS
  http://cs.co/configure_onRamp_AWS
- Configuring Cisco SD-WAN Cloud onRamp for IaaS with Azure
  http://cs.co/configure_onRamp_Azure

Leveraging colocations

Business need

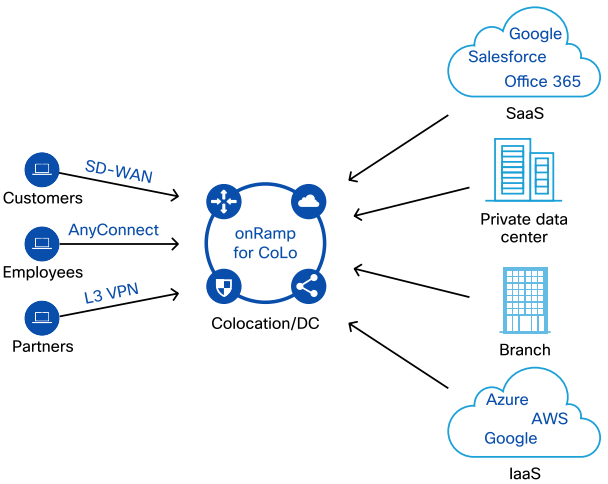
The traditional method of delivering traffic optimization (i.e. load balancing, security policy, WAN optimization, etc.) relied on centralized provisioning of elements, such as firewalls, intrusion detection/prevention sensors, URL filtering, proxies and other such devices at aggregation points within the network (most commonly data centers). For SaaS applications and internet access, this approach resulted in backhauling user traffic from remote sites into the main data centers, increasing application latency and negatively impacting overall user experience. For applications hosted in the data center, this approach resulted in the potential waste of data center bandwidth resources. In addition, this architectural method also challenged effective mitigation of security incidents, such as virus outbreaks, malware exploits and internally sourced denial of service attacks.

Today, as we move into the era of SD-WAN, this problem is exacerbated by the architectural shift into a distributed access model by using direct internet access as discussed earlier in this book. Branches and users are now free to access SaaS applications and internet resources directly - bypassing the aggregation points highlighted above. While this provides a much more efficient method of moving data from point A to point B, it can pose a challenge to IT teams whose organizations may be prohibited by regulatory agencies from accessing the internet directly from the branch. How then, do we get the benefits of a centralized architecture, with the efficiency of a distributed architecture? Cloud onRamp for Colocation allows an organization to adopt a hybrid approach to this problem by utilizing strategic aggregation points (colocations) - thus minimizing latency and consolidating network stacks.

Cloud onRamp for Colocation

Colocation centers allow you to rent equipment, bandwidth, or space in a secure public data center. These facilities provide flexibility to directly connect with a variety of telecommunications, network, and cloud service providers at a fraction of what it would cost to run direct connections to a private data center. One of the greatest benefits in utilizing a colocation center is geographical coverage. A colocation facility not only provides high-speed access into public and private cloud resources, but the center's geographical presence ensures that you can strategically select a facility (or multiple facilities) in close proximity to end users. Hence, when coupled with Cisco SD-WAN, end user traffic is directed to the nearest colocation - where that traffic gets optimized, further secured and transmitted to its intended destination over a high-speed backbone.

DIAGRAM Cloud onRamp for Colocation



How it works

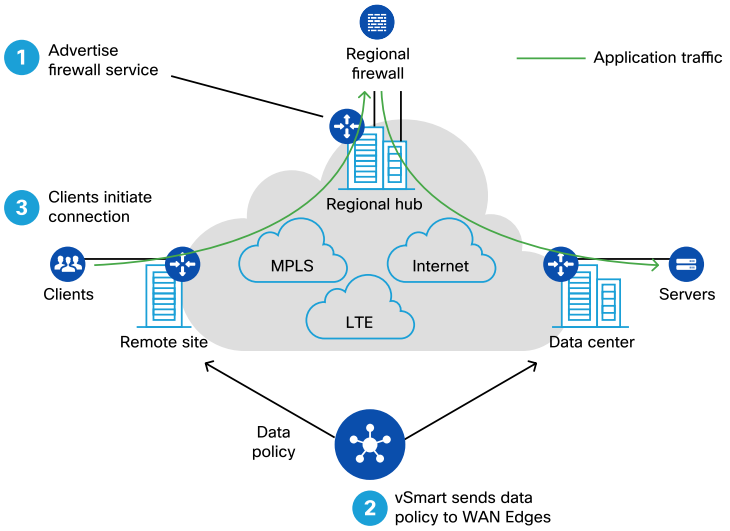
By leveraging service insertion policies and intelligent routing, Cisco SD-WAN can steer traffic of interest wherever necessary. It is this core function that gave birth to the concept of regionalized service-chaining. By positioning optimization/security network elements in strategic points across the network (i.e colocations), regional service-chaining strikes the right balance between operation, cost, application quality of experience and the ability to effectively mitigate security incidents.

SD-WAN service chaining is performed by the WAN Edge routers. This should not be confused with VNF Service Chaining, which is described in the *Building a virtualized branch* chapter. The branch router will identify traffic, analyze its payload and steer the traffic through the appropriate network function at the colocation facility, based on SD-WAN policy created within Cisco vManage. It is important to note that this functionality is not limited to internet destinations, nor to virtual appliances. In fact, organizations seeking to provide inter-site security and optimization can also utilize service chaining.

Network functions (such as WAN Edge routers, load-balancers, IDS/IPS, firewalls, proxies, etc.) are typically virtualized/hosted within a compute platform, such as Cisco ENCS or the Cloud Services Platform. These virtual (and sometimes physical) network functions can be directly connected to the WAN Edge router through VLAN stitching or physical cabling. Once connected, these appliances are announced to the rest of the SD-WAN fabric via OMP. Control and data policies are then used to influence traffic through a connected resource based on these announcements.

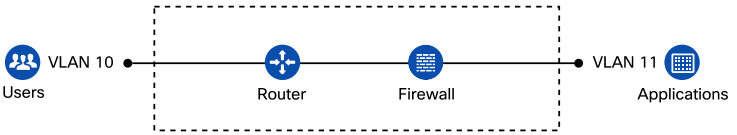
The following figure depicts how a firewall might be inserted into the user's transit path by leveraging data policy. Here, the Cloud onRamp for Colocation solution exists at the regional hub site, and is announcing a firewall service:

DIAGRAM Cloud onRamp for Colocation service chaining



The following example illustrates a simple router-firewall service chain.

DIAGRAM Service chain example



Service chaining for SaaS

SaaS traffic poses a unique challenge to the network architecture since these applications can only be accessed via the internet. Distributed internet access has solved this problem by allowing direct access from the branch location. However, organizations may have a need for additional layers of security for SaaS. Cisco SD-WAN, coupled with Cloud onRamp for Colocation, addresses this requirement.

With Cloud onRamp for Colocation, the administrator has the option of inserting a network service into the SaaS-bound traffic path. As an example, an administrator may choose to insert a Data Loss Prevention sensor into the transit path of traffic destined for a file sharing service - such as Dropbox. Here, by leveraging service chaining policy, the administrator could influence this traffic through any number of network services to satisfy the organization's security policy - whether those services are physical appliances, or virtualized services.

Service chaining for IaaS

It may be desirable to provision network functions within the transit path of traffic destined to IaaS. Traffic of interest will be directed to network functions where it will be processed and forwarded to the IaaS provider. There may be additional layers of security required by an organization. Service chaining can be leveraged to secure this traffic through Cloud onRamp for Colocation.

Service chaining design best practices

If interested in pursuing a strategy around Cloud onRamp for Colocation, consider the following stages while designing service chains:

- Identify Virtual Network Functions (VNFs)
- Identify traffic patterns
- Design service chains

As an example, the following connection patterns might emerge from an analysis of a typical customer network:

DIAGRAM Service chain design

Based on this information, SD-WAN service chaining policies can be derived, as can the VNFs (or physical appliances) necessary to satisfy the requirement. The table above shows which groups cannot interact with each other (red), which groups can interact but with certain controls (grey), and which groups can interact directly (green). For example, when creating a service chain for traffic coming from an organization's employees, fewer firewalls may be required as the source of such traffic is considered to be trusted.

Also, the following should be considered when selecting VNFs and their placement

- Compute needs
- High Availability (HA)
- Port channeling

Lastly, evaluate required compute needs. By default, a Cloud onRamp for Colocation cluster provides high throughput and ample compute capability for most applications. Each individual cluster is capable of expanding to meet the requirements.

Case study

Many organizations are seeking to consolidate and, in some cases, eliminate private data centers to save money. In one such case, a European customer sought to move all private data center workloads to the cloud. In doing so, they needed an effective way to maintain security and optimization policy on their traffic. While this would have previously been provided by a regional data center, the new model necessitated the use of regional colocation facilities. Utilizing the Cisco Cloud onRamp for Colocation, this customer was able to virtualize their security and optimization infrastructure by leveraging SD-WAN service chaining to influence traffic through these network elements. Branch users now enjoy minimal latency as their traffic is redirected to the nearest colocation facility, gets inspected/optimized and placed on a high-speed backbone towards the intended destination.

Utilizing the Cloud onRamp for Colocation feature, this customer was able to realize the following benefits:

- Increased WAN agility - WAN service chains could be deployed and withdrawn on demand to satisfy the dynamic needs of the business.
- Reduced latency - utilizing the colocation facilities' backbone, this customer was able to reduce latency to and from cloud applications.
- Consistent security - prior to Cloud onRamp for Colocation, this customer had to implement security policy at several points within the network: the data center, the branch and the cloud service provider. By leveraging this solution, however, this customer was able to deploy their security policy consistently across all branches, colocation facilities and cloud service providers - all through the vManage GUI.

Key takeaways

As enterprises adopt a multicloud strategy, they must look at optimizing traffic patterns for user experience, security, reducing circuit costs and providing flexibility. The success of multicloud solutions depends on a new cloud-edge capability, where all consumer networks terminate in a carrier-neutral facility and optimization policies can be enforced centrally.

This is where Cisco Cloud onRamp for Colocation comes in. Cloud onRamp for Colocation offers the capability of virtualizing your network edge and extending it to colocation centers – bringing the cloud to the customer, versus the customer extending to the cloud. The solution provides virtualization, automation, and orchestration for enterprise – negating the need to design infrastructure for future requirements or scale by providing an agile way of scaling up and down as required.

Cisco Cloud onRamp for Colocation:

- Extends the cloud to the branch, acting as a demarcation point between users/devices/things and application resources – regardless of their location.
- Is a prescriptive, turnkey, flexible architecture, ideally suited for customers looking at simplicity over customization.
- Provides a centralized managment GUI for both SD-WAN and WAN service-chain orchestration through vManage.
- Offers a Zero-Touch Deployment model.
- Supports service-chaining models that include both Cisco and third-party devices (with the option to customize your own VNFs).

Further reading

To learn more ways Cisco SD-WAN Cloud onRamp for Colocation can help to develop cloud strategy, please visit the following resources:

- Solution Guide: *http://cs.co/cor-for-colo*
- FAQ: *http://cs.co/cor-faq*

Building a virtualized branch

Business need

Enterprises and service providers alike are looking to streamline their operations and eliminate equipment failures by moving away from the proliferation of physical appliances at the branches into a virtualized infrastructure.

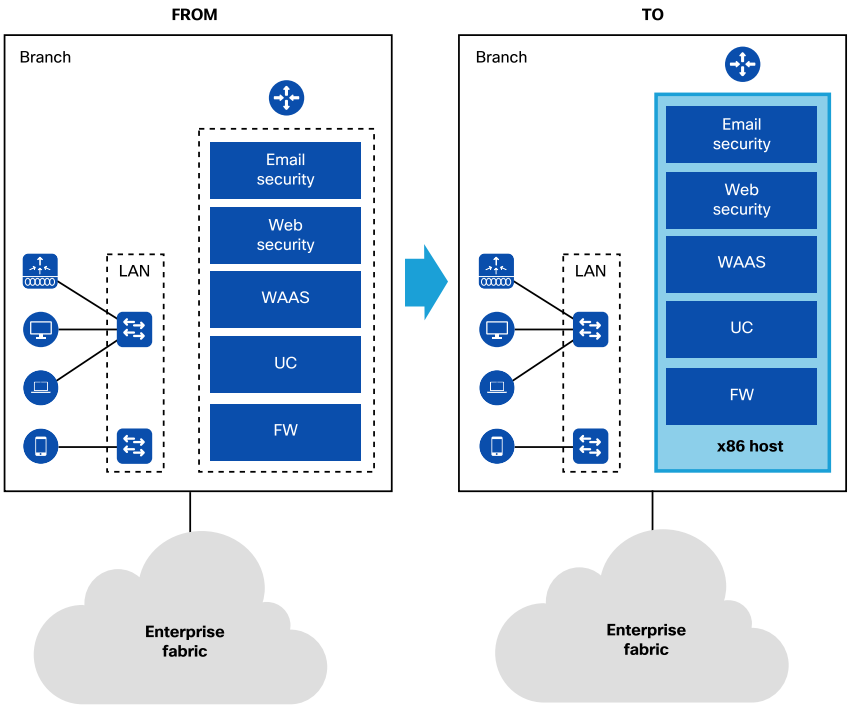
A typical multi-services branch deployment consists of multiple physical point products, each having a specific function, engineered into operating in a specific network topology. Often these products include routers, firewalls and WAN optimization appliances. Modifying something in that solution stack, such as adding a new function or changing connectivity for an existing function, requires significant effort to accommodate the change. This change can extend from running additional cabling to reconfiguring routing protocols and introduces risk, additional testing, and extended roll-out time - all of which can affect productivity.

Operational inefficiencies can cause not only significant delays and disrupt the business, but they can also result in significant costs. These costs can manifest themselves in dispatched IT personnel, or investing in higher cost physical appliances.

Network Functions Virtualization

Network Functions Virtualization (NFV) is the basic element for building multi-service environments. NFV provides the means to deliver network services by offering them as virtualized software running on an x86 compute platform rather than on dedicated/specialized hardware. NFV is often confused with Software-Defined Networking (SDN).

DIAGRAM Multiservice branch evolution



NFV solutions help with business goals by simplifying network operations to deliver new services faster. As a result, NFV allows users to reduce the cost of running services, and provides a means to generate new revenue. With NFV it is possible to run functions on general-purpose hardware, automate service delivery with orchestration, and scale easily.

The following tables summarize the perceived benefits for Capital Expenditure (CAPEX):

DIAGRAM Perceived benefits of virtualization - CAPEX

Motivation	Description
Deployment of standard x86-based servers	▪ Servers considered cheaper than routers/ appliances ▪ Servers already deployed in branch, DC, PoP
Deployment of best-of-breed	▪ Separation of network functions allows best-of-breed services ▪ Eliminates vendor lock-in ▪ Encourages openness and competition among software vendors ▪ CAPEX reduction through competition
Cost reduction through economies of scale	▪ Deployment of huge server farms in DCs can lead to better resource utilization
Simplified performance upgrades	▪ Increase performance through software upgrades without hardware upgrades

The following table shows a similar summary for Operational expenditure (OPEX):

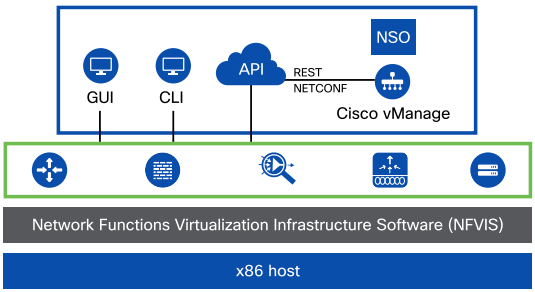
DIAGRAM Perceived benefits of virtualization - OPEX

Motivation	
Fewer branch visits	▪ Changes/upgrades in the service can be made in software ▪ No longer need to swap appliances on-site for service
Automated network operations	▪ Virtualization places focus on automation and elasticity, thus reducing management
Flexible VNF-based operation	▪ Software upgrades can be done independently ▪ VNFs can be placed flexibly in the branch, DC, or PoP
Elimination / reduction of organizational boundaries	▪ IT and network operations align

NFV building blocks

Cisco NFV Infrastructure Software (NFVIS) provides flexibility and freedom of choice in deployment options. By virtualizing and abstracting the network services from the underlying hardware, NFVIS allows Virtual Network Functions (VNFs) to be managed independently and to be provisioned dynamically. NFVIS supports Cisco VNFs such as vEdge Cloud, Integrated Services Virtual Router (ISRv), virtual WAN optimization (vWAAS), virtual ASA (ASAv), virtual wireless LAN controller (vWLAN), and Next-Generation Virtual Firewall (FTDv). NFVIS also supports running a multitude of third party network services.

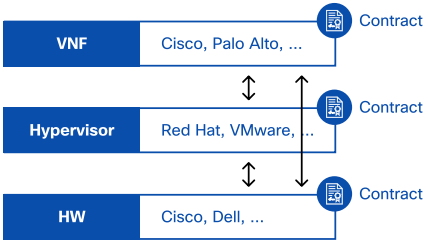
DIAGRAM NFVIS architecture



Support in a multi-service virtualized environment

In a multi-service virtualized branch, there may be a different vendor for the hardware appliance, hypervisor, and individual VNFs. This introduces the challenge of managing and supporting the deployment. When utilizing ENCS with NFVIS and the virtual Cisco WAN Edge router, Cisco will provide support for the overall solution. Cisco's NFVIS certification process also allows compatible third-party VNFs to be deployed and supported by Cisco.

DIAGRAM Simplified support through one solution



One Solution: VNFs + NFVIS + ENCS + Cisco SD-WAN

Service chaining

At this point it may be helpful to define some terms associated with service chaining.

Traffic steering is a method of optimizing the performance of a network by dynamically analyzing and regulating the behavior of data transmitted over that network.

Service insertion is the concept of steering application traffic of interest through specific devices using network service labels. This allows the network path to be altered without the need to re-engineer the network at either remote sites or data centers.

VNF service chaining is the order of traffic flow on an x86 compute platform. This is particularly important when deploying multiple VNFs on a universal CPE or on Cisco virtualization platforms (such as Enterprise Network Compute System [ENCS] or Cloud Services Platform [CSP]).

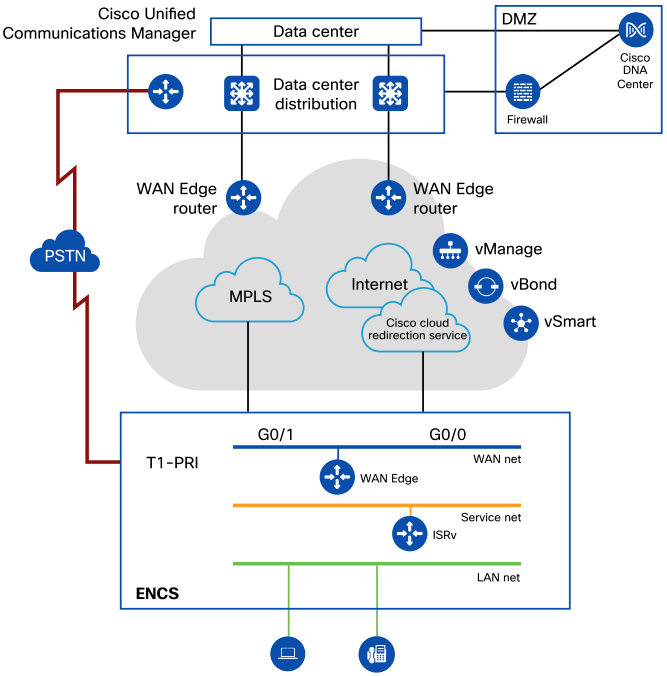
SD-WAN service chaining allows the administrator to insert network services into the transit path of a user, based on policy. It can range from manipulating the transit path of a single application to modification of an entire remote site's traffic flow. As traffic ingresses the branch WAN Edge router, it will be forwarded through the appropriate service chain as provisioned on Cisco vManage.

Case study

In this case study, the deployment of a simple software-defined branch with two virtual network functions involved deploying Cisco vEdge Cloud and Cisco ISRv. Cisco DNA Center is used as an orchestrator to deploy these VNFs onto the Cisco Enterprise Network Compute System (ENCS) 5412 platform. Cisco vManage is used as the SD-WAN orchestrator. The ENCS appliance is running the Cisco Network Function Virtualization Infrastructure Software (NFVIS). In this scenario, the ENCS is the x86 platform, and NFVIS is the hypervisor running the NFVs. Cisco DNA Center deploys the VNFs to the x86 platform, after which the WAN Edge routers register with vManage and join the SD-WAN fabric.

The aim is to combine the voice features of ISRv and SD-WAN features of vEdge Cloud by connecting these two virtual routers through a service network (VNF service chaining). This saves rack space and operational expenses (OPEX) by running only one physical device - ENCS - which has two virtual routers providing SD-WAN and multiple LAN services.

DIAGRAM ENCS deployment with ISRv and WAN Edge VNFs



For details, including router configuration and software version used, please refer to the following: *http://cs.co/nfvis-case-study*

Key takeaways

As enterprises evolve and seek to reduce costs, they must look at optimizing traffic patterns for user experience, security and flexibility. Cisco SD-WAN, coupled with ENCS, NFVIS and service chaining offers this capability by:

- Virtualizing the network edge
- Simplifying SD-WAN and WAN service chain orchestration through vManage
- Supporting both Cisco and third-party VNFs
- Lowering total cost of ownership
- Scaling up or down, as required, by negating the need to cable, rack and stack dedicated appliances.

Further reading

- For more information on the ENCS 5400 platform, please refer to the data sheet: *http://cs.co/5400_datasheet*
- See the Cisco ENFV home page: *http://cs.co/enfv*

Meeting compliance requirements

Business need

In a changing world with new business goals and greater information security threats, the digital technology industry is adopting stronger standards for compliance. Some standards comprise legal and regulatory frameworks, others provide harsh penalties for failure to comply. As technology continues to evolve, and business dependence on technology increases, the compliance requirements become more complex. For network owners, architects, administrators, and consumers, there is an ever-increasing pressure to meet greater compliance requirements and to provide businesses with a lower risk profile and protection against threats.

The Cisco SD-WAN solution offers appropriate measures for compliance, provides data protections, and gives users maximum trust and confidence.

Control plane security

The Cisco SD-WAN fabric incorporates a zero trust security model in its control plane, ensuring that all elements of the fabric are authenticated and authorized prior to admittance to the network. This model is built on the use of digital certificates to establish the identity of each fabric element. The certificates are used to establish secure Transport Layer Security or Datagram Transport Layer Security (TLS/DTLS) control channels between the WAN Edge routers and the controllers. Once the secure control channels are built, these channels are used to run the protocols OMP (Overlay Management Protocol) and NETCONF that allow the controllers to propagate configuration and networking information inside a secure encrypted channel. The OMP protocol ensures the propagation of the encryption keys used by the data plane.

Certificates

Cisco SD-WAN does not use any pre-shared keys in the system. Every element in the solution must have a unique device certificate issued by a trusted Certificate Authority (CA). To facilitate multiple avenues of certificates in the solution, each SD-WAN component is also preloaded with root certificates of multiple vendors:

- Avnet
- DigiCert/Symantec
- Cisco

If a customer chooses to use its own Enterprise CA instead of DigiCert and Cisco CA for signing certificates, they may do so.

The SD-WAN controllers require the generation of a Certificate Signing Request (CSR) based on which a certificate is issued to them by the Root CAs. The majority of certificates issued by Cisco use DigiCert and/or Cisco certificates for the controllers. These certificates are used by the controllers to communicate with other devices.

The physical WAN Edge routers are each preloaded with a unique individual device certificate. The WAN Edge routers are issued with a certificate at time of manufacturing. This certificate is presented to the controllers during the initial WAN Edge router authentication and authorization process and uniquely guarantees the identity of each software element in the solution.

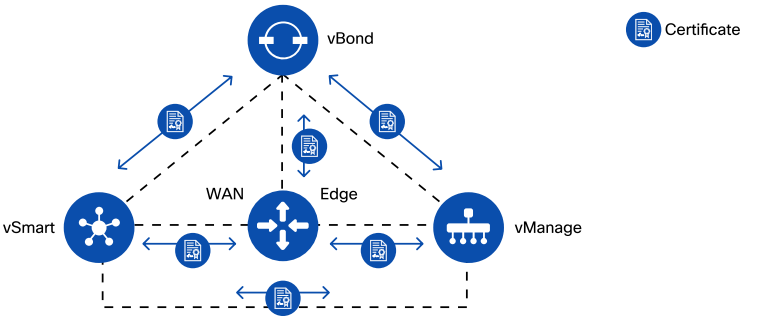
In case of virtual routers, each router must generate a CSR and obtain a certificate that will ensure the validity of that device. The virtual router is issued a one-time-use license token and presents that to the Cisco vManage. The vManage will validate the license token and generate a CSR for the device. Using the CSR, a certificate can be issued to the device from the trusted root CAs.

To provide administrative control over this environment, the SD-WAN solution leverages a white-listing model that allows administrators to revoke certificates from the environment, reject devices with valid certificates, and generate new certificates as determined by their security policy. In order to simplify the process of certificate activities, the solution provides APIs for such use. An audit trail of all activities is maintained.

TLS/DTLS

The certificates issued to each SD-WAN component are used in a mutual authentication process to establish bi-directional communication. Each controller will build a DTLS or TLS 1.2 connection to every other controller, allowing all the SD-WAN controllers to sync up. When the routers attempt to communicate with the controllers, they will also establish DTLS or TLS 1.2 connections. These secure tunnels are then used to establish the routing protocol, OMP, and adjacencies that will be used to establish the secure data plane. The hashing algorithm used in the SD-WAN control plane leverages SHA256 and the encryption algorithm used for this control tunnel is AES-256-GCM to meet the higher security requirements. The use of DTLS and TLS within the Cisco SD-WAN solution is based on standards published in RFC6347 and RFC5246.

DIAGRAM Certificate-based authentication



OMP and NETCONF

All routers communicate with the SD-WAN controllers using OMP for all routing, network policy and encryption information. SD-WAN devices use NETCONF to communicate with the management layer for configuration and telemetry inside the DTLS or TLS tunnel. This tunnel ensures that the routing updates and the encryption keys are distributed in a secure fashion.

The OMP protocol is of significant interest in the control plane. It is a scalable and highly available protocol, built on a secure DTLS/TLS tunnel. This protocol carries all the routing information between the devices and the SD-WAN controllers. This eliminates the need to use the Internet Key Exchange (IKE) protocol for site-to-site key exchange. By building a custom protocol to eliminate the need for N^2 adjacencies, and the ability to efficiently propagate unique encryption key information, OMP allows the Cisco SD-WAN environment to build very large-scale networks, from dozens to thousands of sites and beyond, in a single overlay.

Keys exchange

Each WAN Edge router generates symmetric encryption and hash keys per WAN link for its data plane. The WAN Edge routers use the secure off-path channel (OMP channel) to exchange their encryption and hash keys and bring-up IPSec Security Associations (SAs) between them. These encryption/hash keys are not stored/cached in the vSmart controller which just acts as a reflector in reflecting the encryption and hash keys to the remote devices which can build IPSec SAs between them. WAN Edge device-to-device communication is uniquely encrypted using IPSec SAs with AES-256-GCM.

Data plane security

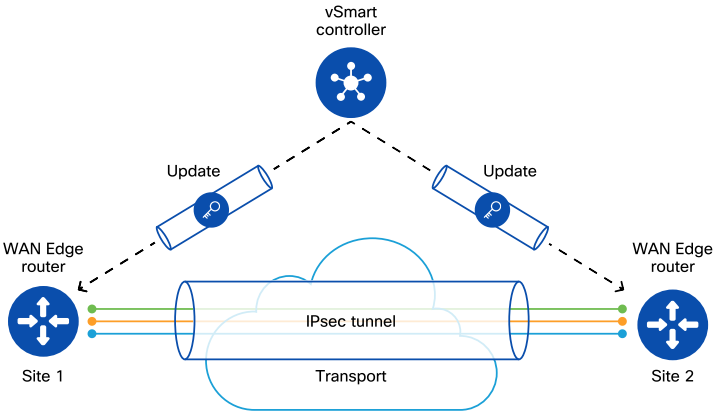
The data plane, sometimes referred to as the forwarding plane, is the part of an SD-WAN solution that carries user traffic across the WAN network. In most SD-WAN solutions, data plane security is most commonly recognized in the form of encryption between routers, though its responsibility does not end there. Many regulatory agencies require both traffic isolation and firewalling in addition to encryption in order to be compliant. As an example, Payment Card Industry (PCI) compliance mandates that, should a malicious user intercept traffic not intended for them, it should not be readable. Likewise, if a malicious user were to gain access to an unauthorized segment of a PCI-compliant network, they should be limited in the destinations they are allowed to access from that segment. Cisco WAN Edge routers are equipped with several features to assist the journey to becoming compliant.

Encryption

The Cisco SD-WAN solution employs the highest grade of encryption possible - Advanced Encryption Standard (AES) - using a 256-bit key length. AES has two modes of operation within Cisco SD-WAN: Galois/Counter Mode (GCM) and Cipher Block Chaining (CBC). GCM is the preferred mode, though CBC mode can also be instantiated when necessary (such as for multicast traffic).

Based on the previously explained key exchange method, the secure data plane communication channel between the WAN Edge routers is established as shown in the following diagram.

DIAGRAM Secure data plane communication



In a traditional IPSec framework, encryption keys would have been generated by the WAN Edge routers using the process known as Internet Key Exchange (IKE). One of the unique benefits of the Cisco SD-WAN architecture is how these keys are distributed via the control plane infrastructure instead. By forgoing the IKE process, Cisco WAN Edge routers can further save computational resources and scale higher.

In some cases, however, encryption may be required on data plane traffic outside of the SD-WAN fabric - such as when sending data to a third-party vendor or business partner outside of an organization. In these situations, the vendor or business partner does not share the same control infrastructure as the originating enterprise and, hence, cannot utilize the same key distribution methods. For this reason, Cisco WAN Edge routers are also capable of creating/terminating IPSec tunnels that utilize the traditional key distribution approach known as Internet Key Exchange (IKE). IKE has evolved in recent years to become more secure, with IKE version 1 (default, but widely used) being less preferred than IKE version 2. WAN Edge routers support both versions, however, to provide maximum compatibility. When enabling IKE-based IPSec tunnels on a WAN Edge router, the following properties are enabled by default for the IKE phase 1 exchange:

- Authentication: SHA1-HMAC
- Encryption: AES-256
- Diffie-Helman Group: 1, 14, 15 or 16 (default)
- Rekey Lifetime: 30 seconds up to 14 days (4-hour default)
- Mode: Main (default) or Aggressive

Once a secure channel is built in Phase 1, the WAN Edge router can begin the process of generating keys, encrypting and transmitting data to the remote endpoint - known as Phase 2. Much like with the SD-WAN fabric, traditional IPSec VPNs utilize AES as the encryption algorithm for sending data, though this parameter is configurable. It is important to note, however, that only the CBC variant is available as a mode of operation. WAN Edge routers can be configured with the following Phase 2 parameters (please refer to CCO documentation for device-specific IPSec support):

- Authentication: SHA1-HMAC or SHA2-HMAC
- Encryption: AES-128 or AES-256

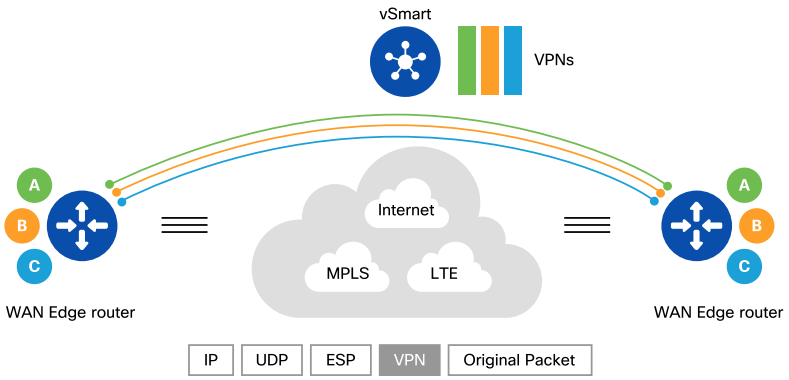
Segmentation

As with encryption, traffic isolation is a key element of any compliance strategy - both for its intrinsic benefits as well as the operational benefit it provides when constructing firewall policy based on segmentation. In the Cisco SD-WAN solution, segmentation is initiated in the control plane, but it is enforced within the data plane. As traffic enters the router, it is assigned to a VPN. Each VPN is assigned a numerical value (0-512, where 0 and 512 are reserved for system use). Each router then advertises these VPN values to the control plane via OMP. This VPN assignment not only isolates user traffic, but also provides routing table isolation. Hence, users in one VPN cannot (by default) transmit data to another VPN without explicit configuration allowing the traffic.

As a user transmits data across the WAN, the WAN Edge router will append the user's VPN (in the form of a label) to the traffic. This label, which is placed just behind the ESP header, identifies which VPN the user's traffic belongs to when it reaches the remote destination.

As the remote router decapsulates the encrypted data, the label is used to determine which VPN to deliver the traffic to.

DIAGRAM End-to-end segmentation



Firewall

One of the final pieces to compliance strategy on the data plane is a properly configured firewall. A firewall ensures that user traffic is restricted to authorized destinations as well as providing auditing in the event of a security incident. WAN Edge routers are equipped with a stateful firewall onboard that can aid in this endeavor.

Firewall policies are implemented via zones. Each zone is a VPN which consists of one or more interfaces/networks in the SD-WAN network. A source zone is defined and this identifies the VPNs from which data traffic originates, as is a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches a particular condition, the associated action or actions are taken and policy evaluation on that packet stops. The firewall policy can be defined using all or any combination of Source IP, Destination IP, Source Port, Destination Port, Protocol and Application to be dropped as match criteria, and the action can be any of Inspect, Pass or Drop.

Management plane security

The Cisco SD-WAN solution provides a management plane through the vManage Network Management System (NMS). vManage is the system that allows users to configure, monitor, and manage the SD-WAN network from a simple dashboard or using the Cisco SD-WAN APIs. Cisco SD-WAN provides management compliance by controlling who can access, read, and modify configurations and policies. This is achieved through Role-Based Access (RBAC) and white-listing of source IP addresses using Access Control Lists (ACL).

Role-Based Access Control

RBAC is used to control the permission for users based on their privileges and it falls under Authentication, Authorization, and Accounting (AAA) architecture. RBAC can be defined locally on vManage or integrated with existing customer AAA solutions via the SAML SSO, RADIUS and TACACS protocols to directory services.

Users are typically grouped into user groups which are assigned with different privileges to perform tasks in the environment.

- The "basic" group provides permission to view interface and system information.
- The "operator" group has permission only to view information.
- The "netadmin" can perform all operations. The user "admin" falls under this category.

Apart from the above pre-defined user groups, the customer can also create new custom user groups and choose the set of read/write privileges for the respective groups.

At initial setup, vManage will be setup with local authentication. Customers may choose to integrate via SAML SSO/RADIUS/TACACS and enable Multi Factor Authentication (MFA).

Controlling access to vManage

Network administrators can create white-list Access Control List (ACL) to restrict only allowed IP subnets to access vManage. This adds another layer of security, in addition to RBAC, to control which devices in the network can access vManage.

For example, if an administrator only wants to allow source IP subnet of 172.2.0.0/16 to reach vManage, then a simple ACL to permit 172.2.0.0/16 would achieve that goal. This prevents non-allowed users or compromised devices outside of 172.2.0.0/16 from reaching vManage.

Platform compliance

The Cisco SD-WAN solution is built on a secure platform. Platform compliance requires the following key aspects:

- Hardware compliance
- Software compliance
- Solution compliance

This section reviews these topics. The building of individual hardware components in a secure and trustworthy way is discussed, followed by discussion of the software development process and compliance of the SD-WAN solution.

Hardware compliance

The Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure cryptoprocessor; a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. WAN Edge routers use Certificate/RSA Keys in the TPM chip to authenticate themselves and participate in the SD-WAN network. Since each TPM chip has a unique and secret RSA key burned-in as it is produced, this guarantees that the key stored on the router is unalterable.

Cisco vEdge router

The manufacturing of Cisco vEdge router is a five-step process including burning a digital certificate to the device's TPM hardware.

1. Private and public keys are generated on the vEdge router.
2. Certificate Signing Request is generated.
3. The certificate is signed by Avnet and is valid for 25 years.
4. The certificate is loaded into the TPM-lite chip on the vEdge router.

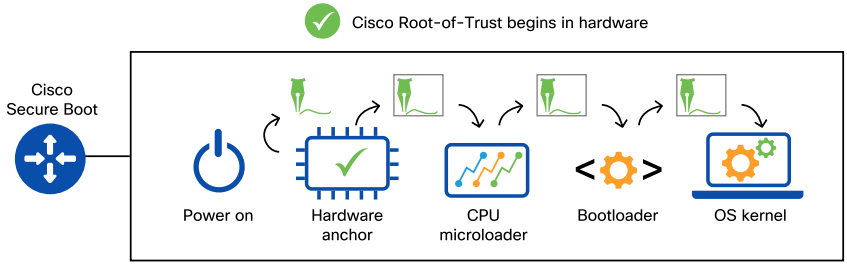
5 Cisco vEdge router ships with root CA trust chain for Digicert root cert, and Cisco CA root cert for authenticating the controllers and the remote WAN Edge routers.

Cisco IOS XE WAN Edge router

Cisco IOS XE-based WAN Edge routers use Secure Unique Device Identifier (SUDI) and are trustworthy systems.

- The SUDI is an X.509v3 certificate with an associated key-pair that is protected in hardware.
- Cisco IOS XE-based WAN Edge routers are "trustworthy systems", i.e. they do what it they are expected to do in a verifiable way.
- Key trustworthy technologies include image signing, secure boot, runtime defenses, and the Cisco Trust Anchor module (TAm). These protect against counterfeit hardware and software modification; help enable secure, encrypted communications; help enable Plug-and-Play (PnP) and Zero-Touch Provisioning (ZTP).
- Cisco Secure Boot helps ensure that the code that executes on Cisco hardware platforms is genuine and untampered.
- Using a hardware-anchored root of trust and digitally-signed software images, Cisco hardware-anchored Secure Boot establishes a chain of trust which boots the system securely and validates the integrity of the software at every step.

DIAGRAM Cisco Secure Boot process



Enforcing trust in virtualized network functions

Virtual Network Functions (VNF) for SD-WAN can be trusted as long as the appliance hardware has the proper built-in security features, such as a TAm, to enforce hardware-anchored Secure Boot. Whether the routing appliance is located in a secure data center, installed with zero-touch ops at a remote site, or is running in a cloud colocation facility, Cisco hardware supports VNFs with end-to-end security and trustworthiness.

When selecting the appropriate hardware to run critical virtualized functions such as routing and security, it's important that the entire hardware ecosystem is optimized to achieve the levels of performance required to support SLAs and the expected application Quality of Experience (QoE). When it comes to high-speed gigabit routing and real-time analysis of encrypted traffic, performance is more than processing power. By designing custom ASICs for complex routing functions, and including Field Programmable Devices (FPD) to support in-field updates, Cisco hardware is fine-tuned for network workloads, security analytics, and remote orchestration.

Software image signing

Image signing is a two-step process for creating a unique digital signature for a given block of code. First, a hashing algorithm, similar to a checksum, is used to compute the

hash value for the block of code. The hash is then encrypted with a Cisco private key, resulting in a digital signature that is attached to and delivered with the image. Signed images will be checked during boot-up to verify that the software has not been tampered.

Digitally-signed Cisco software increases the security posture of Cisco IOS devices by ensuring that the software running in the system has not been altered and originates from a trusted source. Administrators can verify the authenticity and integrity of the binary file by checking SHA512 and/or MD5 checksums.

Data retention

Records management and retention policies

Cisco maintains an Enterprise Records Retention Schedule (ERRS) which defines the retention timeframes based on country-specific business, legal, or global regulatory obligations. The ERRS standardizes records management across the enterprise and supports data retention throughout its lifecycle. At the end of the lifecycle, records are disposed of in a timely, efficient, and secure manner in accordance with information disposition policies based on retention requirements and the media in which the records are stored.

Personal information

Personal data processing users may sign into the user interface for the solution through the following methods:

- Non-Cisco Single Sign-on (i.e., RADIUS or TACACS), pursuant to which, any personal data is processed through the user's designated third party SSO operator.
- Cisco Single Sign-on (i.e., SmartAccount), pursuant to which, any personal data is processed through the Cisco Smart Account service.

All data stored within the Cisco hosted SD-WAN control infrastructure is protected via encrypted disks.

Username and password to use Cisco SD-WAN

Usernames and passwords are retained in the customer's SD-WAN account, hosted by Cisco. IP addresses and other unique identifiers are not captured by Cisco SD-WAN during the sign-on process.

Customers have the ability to delete their personal data through their account settings. Cisco does not have the ability to take this action on a customer's behalf while the customer has an active Cisco SD-WAN subscription. However, 60 days after expiration or termination of a customer's Cisco SD-WAN subscription, Cisco automatically deletes the customer's entire SD-WAN control infrastructure, including personal data stored within it.

Data classification policy

Cisco has a formal policy and associated standards and guidelines that establish the requirements for classifying, labeling, and protecting data. This includes general guidelines and a decision tree to help classify data and determine if an individual has a legitimate business purpose (need-to-know) to access and use the data.

Global presence

This book doesn't cover all region- and country-specific regulatory requirements or list all compliance statements. To do so would totally shift the goal of the book. At this place, we would like to mention that the Cisco SD-WAN solution is successfully deployed all across the globe, including the following regions/countries:

- North America
- Europe
- China
- Russia

Cisco SD-WAN leverages third-party cloud services. Customers can choose the region-specific data center appropriate for their environment (Australia, Brazil, Germany, India, Ireland, Japan, Singapore, USA).

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding corporate rules
- EU-US Privacy Shield framework
- Swiss-US Privacy Shield framework
- APEC cross-border privacy rules
- EU standard contractual clauses

Key takeaways

In a changing world with new business goals and greater information security threats, the digital industry is adopting stronger standards for compliance. For network owners, architects, administrators, and consumers, there is an ever-increasing pressure to meet greater compliance requirements and to provide businesses with a lower risk profile and protection against threats.

- The Cisco SD-WAN solution addresses compliance in an holistic way by addressing each and every component of the solution.
- Each SD-WAN technology component such as control, data, and management planes are hardened by using a combination of innovative techniques, industry standards, and the highest encryption algorithms.
- The solution has been deployed globally and satisfies multiple governments and regulatory compliance requirements.

Further reading

Privacy Data Sheet: *http://cs.co/SD-WAN-privacy-datasheet*

Migrating to Cisco SD-WAN

Business need

Businesses are challenged to transition seamlessly to new solutions and revenue-generating services. Faster time to market, risk mitigation, and minimal disruption to existing services and applications are all factors in a customer migration strategy. Even though each WAN migration is unique to a particular environment, migration to Cisco SD-WAN can be completed seamlessly without compromising on the above requirements.

It is important to understand what the organizational business goals might be, so they can be considered during the migration to Cisco SD-WAN. Here are some examples:

- Traffic prioritization and transport selection
- WAN cost reduction and bandwidth augmentation
- Segmentation
- Secure direct internet access
- Guest access

Migration planning

Migration planning is critical because moving to SD-WAN involves changes to the network architecture.

It is important to understand the current architecture of a network before a migration. Identify the current hardware and software, transports, applications, and traffic flows. To design the SD-WAN network properly, it is important to baseline the current bandwidth requirements and account for future growth.

Some areas to consider in order to plan a successful migration and deployment of the Cisco SD-WAN solution are given below.

Controller considerations

The deployment model needs to be selected, for example, cloud-hosted or on-premise. Sizing, scale and redundancy play very important roles during the preparation phase. Typical questions to address:

- How many Cisco vManage, Cisco vBond, and Cisco vSmart controllers will be needed?
- Where will the controllers be located?
- Will Cisco vManage be clustered?

SD-WAN controllers are deployed in geographically redundant data centers or cloud regions. This distributed deployment contributes to high availability and resiliency of the control and management plane infrastructure. Proper controller design allows deploying networks that scale from tens to thousands of locations.

Data center design considerations

When deploying WAN Edge routers, planning should account for how internet and private circuits will be connected into the headend routers at the data center locations.

The integration into the data centers' routing protocols is important to ensure path symmetry and loop avoidance. Cisco SD-WAN provides intelligent controls to integrate into BGP, OSPF and EIGRP-based data center environments. An important part of migration in the data center is to determine routing policy between SD-WAN overlay and any underlay networks, as this accounts for how traffic between SD-WAN and non-SD-WAN sites will be handled.

Region/branch design considerations

Branch network design, while simple, is the area that is most open to implementing different options available through SD-WAN. It provides opportunities to include additional circuits, private or internet-based. It is an excellent opportunity to integrate LTE as a backup circuit. LTE integration leads to design considerations around effective use of available bandwidth, while protecting against unnecessary usage on metered circuits. In addition to WAN changes, building highly available sites and introducing new services to the branch are also major design considerations.

Policy considerations

SD-WAN technology can create arbitrary topologies between various sites. The network topology needs to define the behavior for the applications. This is also where having a clear understanding of existing business-critical applications and their associated QoS configurations allows for an SLA definition to provide optimal application paths through the SD-WAN fabric.

Security capabilities can be added, such as segmentation, to separate different lines of business and create custom policies on a per-segment basis. A common usage is to implement direct internet access and enable the necessary security policies, so the customer experience is improved without increased security risk exposure.

Cloud considerations

SD-WAN technology provides the ability to extend the network into the cloud. It is important to know the routing considerations when accessing IaaS, the regions involved and whether there is a need to incorporate private cloud connectivity models, such as Microsoft ExpressRoute or AWS Direct Connect within the SD-WAN fabric. With SaaS endpoints, particularly Office 365 and the suite of applications that make it

up, it is important to identify which SaaS applications need to be optimized and the amount of bandwidth expected for the applications. In this way the SD-WAN environment can be set up with the policies that provide an ideal application experience.

Management and operation considerations

RADIUS, TACACS, and/or SSO requirements may significantly influence the migration. Existing monitoring tools and workflows must be described, so that they can be part of the design. The Cisco SD-WAN solution supports APIs, SNMP v2c/v3, Syslog, NETCONF and Netflow for monitoring. This means that the solution can integrate into existing infrastructure as part of the migration.

Miscellaneous considerations

The Cisco SD-WAN solution provides many additional features, which, if being implemented, require their own planning. IPv6 and multicast traffic are unique scenarios that are utilized in some environments. Using SD-WAN as a means to introduce IPv6 capabilities is often an important consideration. Maintaining or expanding multicast capabilities on the SD-WAN network requires an understanding of the environment where the protocols run, the senders and receivers of the multicast streams and the bandwidth requirements to support them.

Additional prerequisites

Before beginning the migration steps, ensure the following factors have also been considered:

- Firewall ports - Cisco WAN Edge routers require DTLS and, optionally, TLS connections to the controllers. Ensure the correct firewall ports are opened so that connections can be formed.
- Check requirements for hardware support. Convert to IOS XE SD-WAN software on existing IOS XE ASR/ISR routers, if required.
- Leverage the PnP Connect portal at http://software.cisco.com to ensure that WAN Edge routers are associated with a Smart Account and Virtual Account. The device authorization file from the PnP Connect portal can be manually

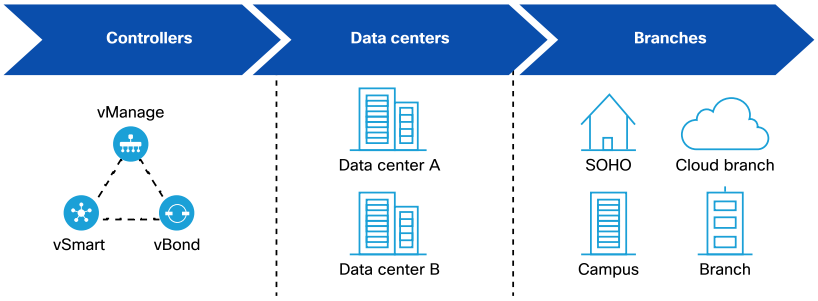
imported into Cisco vManage, or alternatively, Cisco vManage can automatically sync with the PnP Connect service.

See the *Further reading* section for additional details.

Migration strategy

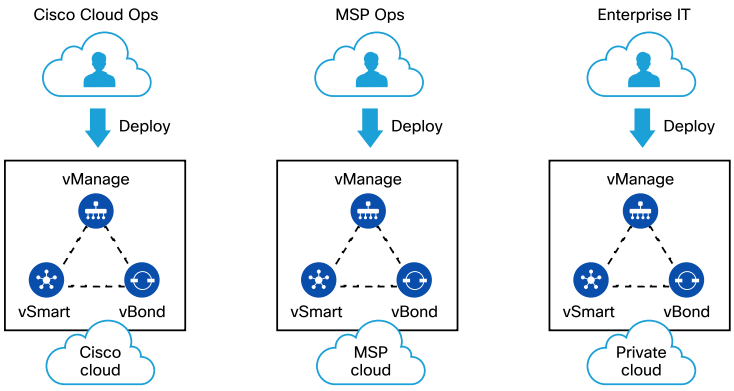
SD-WAN migration begins with deploying the SD-WAN controllers, then proceeds to deploying SD-WAN in the data center, and finally deploying SD-WAN at the branches, as shown in the diagram below.

DIAGRAM SD-WAN migration sequence



Cisco SD-WAN controllers can be deployed either in the Cisco-hosted cloud, MSP/partner-hosted cloud, or on-premise inside an organizational data center. The deployment model depends on the organization's choice or managed service contracts.

DIAGRAM Cisco SD-WAN controllers deployment models



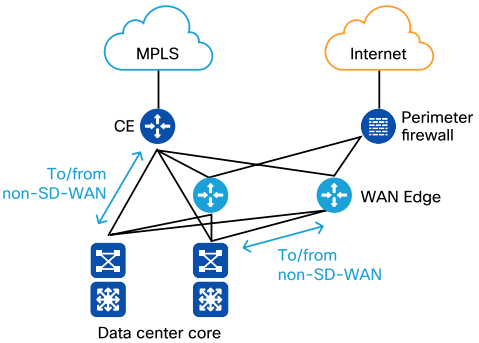
All controller deployment models provide equal SD-WAN capabilities.

Data center migration

The data centers are typically the first sites to migrate to SD-WAN in order to establish the initial SD-WAN fabric footprint. In the most common migration scenarios, data centers serve as transition hubs, routing the traffic between SD-WAN and non-SD-WAN sites, as well as continuing to provide access to applications and services hosted in the data center.

WAN Edge routers serve as SD-WAN fabric headends. They are typically deployed "behind" the MPLS Customer Edge (CE) routers and are also given internet access through the data center perimeter firewall through the DMZ. This allows WAN Edge routers to establish SD-WAN fabric to remote sites across all the transports. WAN Edge routers connect to the data center core/distribution layer.

DIAGRAM Cisco SD-WAN data center topology

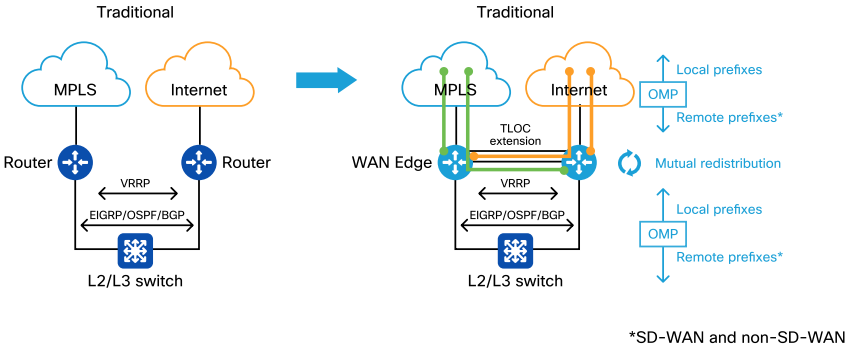


Branch migration

The branch sites can have different topologies depending on the type and number of WAN circuits and their high availability design requirements.

In the case of a site with a single router, the router can be upgraded to IOS XE SD-WAN software, converting the site into SD-WAN. In the case of a site with dual routers, both can be upgraded to IOS XE SD-WAN software, converting the site into SD-WAN. Alternatively, it is possible to take a phased approach and upgrade one router at a time. In this case, user traffic should be shifted to the non-migrated router during the time of software upgrade. Once both routers have been upgraded, high-availability can be configured to have them operate in an active/active fashion.

DIAGRAM SD-WAN branch migration with dual routers

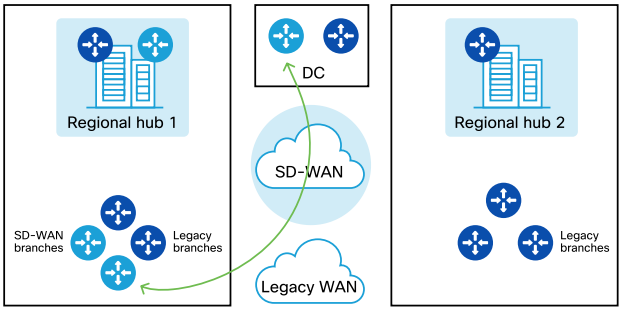


For additional details, please refer to the links provided in the *Further reading* section of this chapter.

Traffic flows

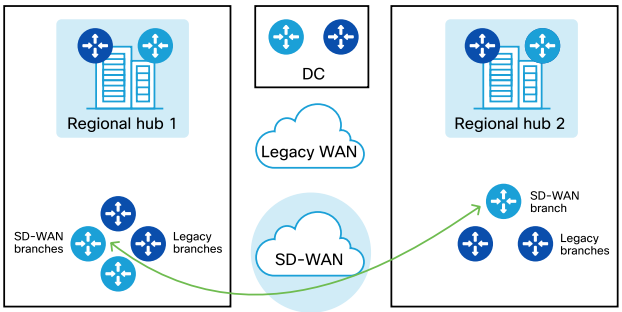
This section illustrates various traffic flow scenarios between regions during an SD-WAN migration. Communication remains intact between SD-WAN and non-SD-WAN branches during the entire period of migration. Communication between migrated and non-migrated branches occurs through the regional hubs or data centers.

DIAGRAM Branch and data center traffic flow over SD-WAN



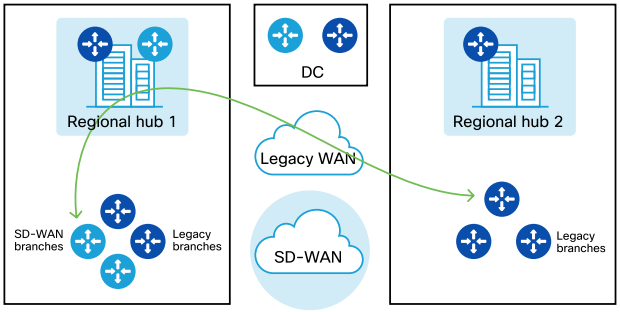
SD-WAN migrated branches communicate between themselves natively over the SD-WAN fabric. This occurs within and also across the regions.

DIAGRAM Migrated branch traffic flow over SD-WAN



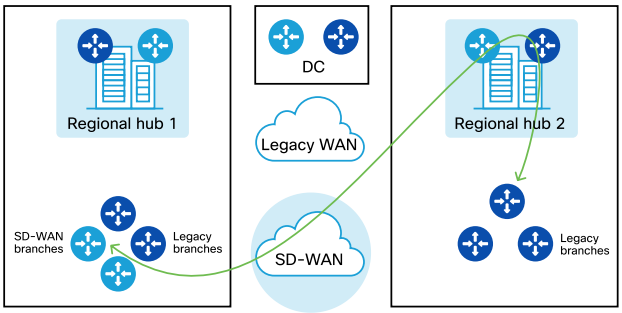
SD-WAN migrated branches communicate with the non-migrated legacy branches in a different region by sending the traffic through their local regional hub and the legacy WAN.

DIAGRAM Migrated and legacy branch traffic flow through legacy WAN



SD-WAN migrated branches communicate with the non-migrated legacy branches in a different region by sending the traffic through a remote regional hub over the SD-WAN fabric.

DIAGRAM Migrated and legacy branch traffic flow in different regions over SD-WAN



Case study

Recreation Equipment, Inc (REI) is an American retail outlet specializing in outdoor recreation. REI operates 154 stores across 36 states, retailing sporting goods, camping gear, travel equipment and clothing. REI moved to the Cisco SD-WAN solution in order to gain stability, ease-of-use, protocol standardization, and gain visibility and reporting for their retail stores. In around 6 months, REI was able to successfully migrate their network infrastructure to Cisco SD-WAN.

The migration experience installing the Cisco SD-WAN solution proved that the solution is flexible and provided REI with the means to deploy new stores easily. It also became clear that the design planning was paramount. As with all technologies, issues were encountered, but the team was able to resolve them quickly and mitigate any risk to their business operations.

To ensure that they benefited from Cisco's knowledge and experience deploying SD-WAN for thousands of customers, REI engaged Cisco to provide extensive training in all the migration areas.

For more information, visit *http://cs.co/rei-sdwan-migration*.

Key takeaways

Minimal disruption to existing services and applications is paramount when transitioning to a new architecture. Migrating to SD-WAN can be a seamless process if the migration is well planned. There are many factors in migration planning, such as controller, management, data center, branch, policy, and cloud. In the migration strategy, regardless of the starting point, controllers should be deployed first, followed by data center and branch sites. The data center is typically configured to promote seamless communication between SD-WAN sites and non-SD-WAN sites until migration is complete.

Further reading

- SD-WAN Migration Guide *http://cs.co/sdwan-migration*
- Software Installation and Upgrade for Cisco IOS XE Routers *http://cs.co/ios-xe-sdwan-install-upgrade*
- Cisco Live Session: Migration to Next-Gen SD-WAN BRKCRS-2111 *http://cs.co/on-demand-library*
- Cisco Validated Design: SD-WAN End-to-End Deployment Guide *http://cs.co/cvd-sdwan-deploy*

Simplifying operations

Business need

As part of network operations, organizations need to manage, monitor, and troubleshoot in a simple and effective manner. Many of today's organizations rely on numerous tools to operate the network infrastructure. Often times, tools address only certain operational needs, such as configuring routers, monitoring router health, monitoring WAN circuit utilization, and collecting alerts and events. Proliferation of individual tools creates significant operational challenges to correlate the collected data.

Cisco SD-WAN provides the means to manage, monitor, and troubleshoot the environment through Cisco vManage. vManage is a graphical user interface for all management, monitoring, and troubleshooting tasks. It can easily interface with existing tools by leveraging north-bound REST APIs or SNMP/Syslog/Netflow exports.

Monitoring and alerting

Cisco vManage comes with monitoring, alerting, and auditing capabilities.

Monitoring Dashboard

Cisco vManage offers three dashboards:

1. Main Dashboard - provides information about the status and health of the network
2. Security Dashboard - provides the status of the security features enabled in the network
3. VPN Dashboard - provides information about the VPN segments in the network

DIAGRAM Cisco vManage main dashboard

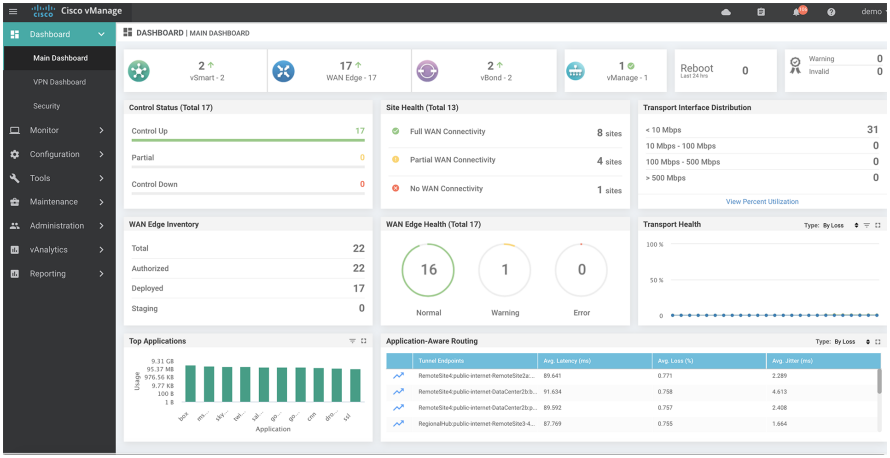


DIAGRAM Cisco vManage security dashboard

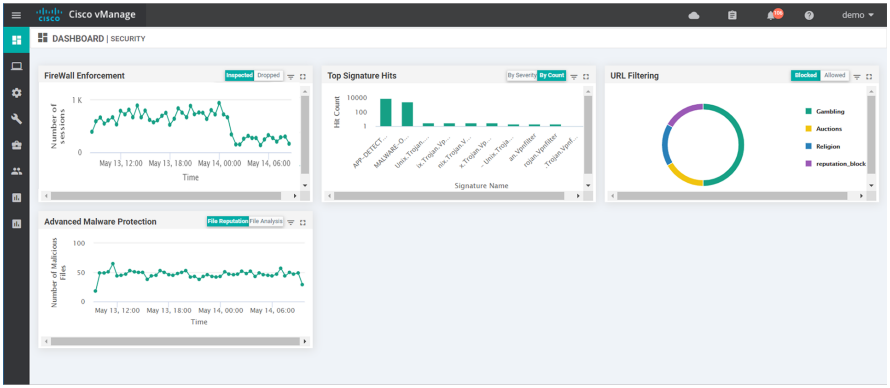
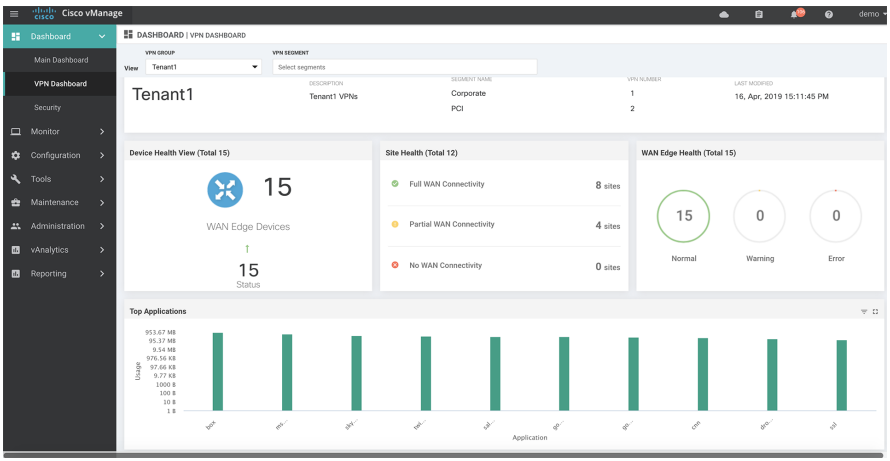


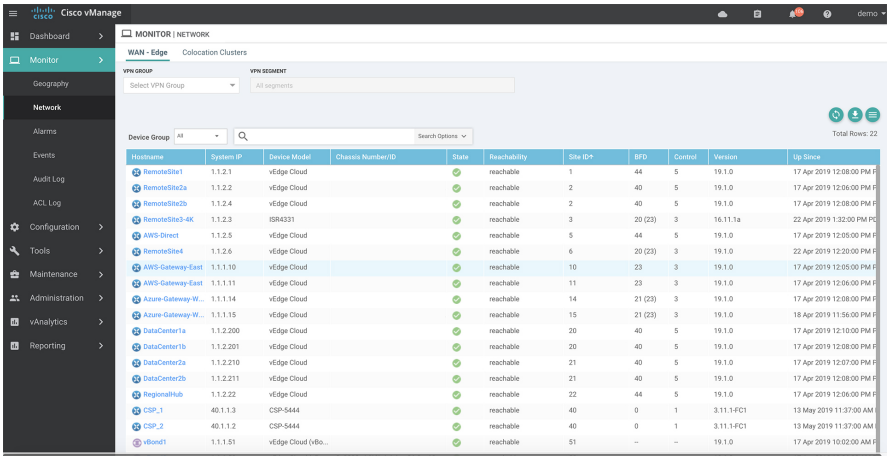
DIAGRAM Cisco vManage VPN dashboard



Device-level monitoring

Customers can see all the WAN Edge routers that make up the network through the Monitor tab options.

DIAGRAM WAN Edge device list

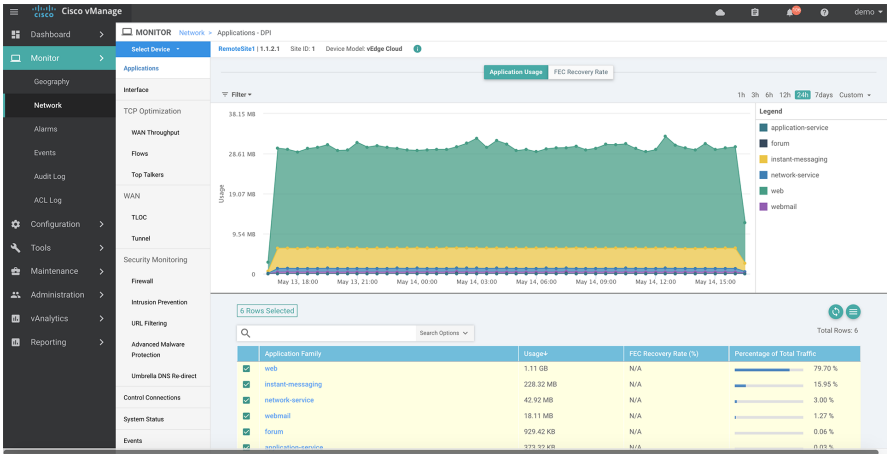


The administrator can then choose the individual WAN Edge router for more detailed information.

Application

Application visibility allows a view of all applications flowing through the selected WAN Edge routers. These applications are detected by the application recognition engine resident in software on the WAN Edge router itself. Applications are arranged in application families for easier identification. A percentage of consumed bandwidth per application family is also shown. The network operator can drill down to see individual applications and associated host information as well.

DIAGRAM Application recognition view

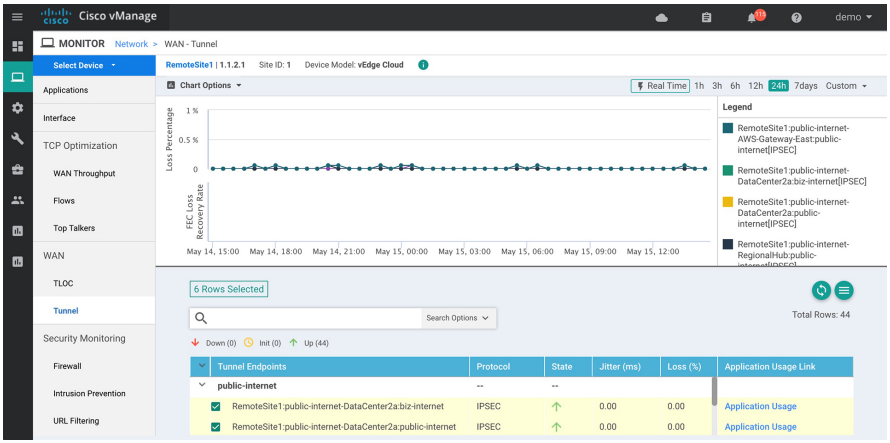


The Application view can be selected for a timeframe between 1 hour and 7 days. Longer views are possible in the custom timeframe selection. Entire historical application visibility data is also collected and maintained in the vAnalytics platform.

Tunnel performance monitoring

The SD-WAN tunnel performance view shows the loss, latency, and jitter performance characteristics of every SD-WAN tunnel. It would also show link remediation, such as the Forward Error Correction feature, if configured.

DIAGRAM Tunnel performance in vManage

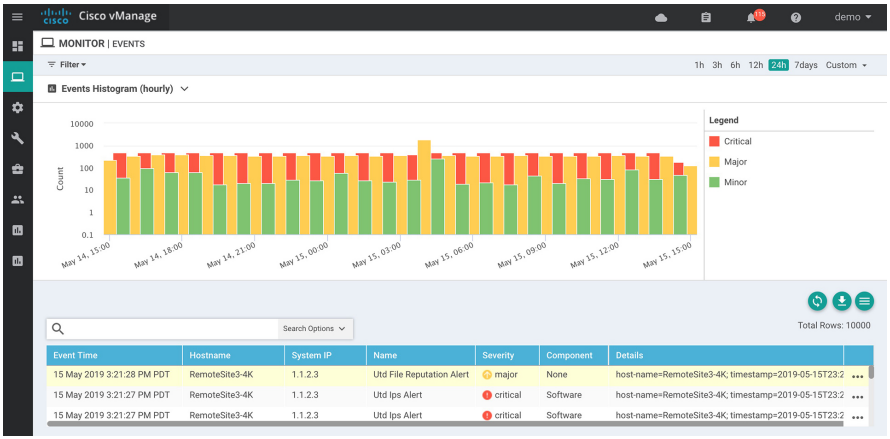


SD-WAN tunnel performance can be viewed in real time to allow the administrator to identify and troubleshoot application quality issues.

Events and alerts

Cisco vManage serves as a central repository for all events coming from the SD-WAN fabric. Events are categorized as Critical, Major, or Minor based on their severity. vManage performs event correlation and triggers alarms based on those events. Administrators can also be notified by email based on alarm severity.

DIAGRAM Events in vManage



Monitoring tools

The SD-WAN Edge routers support SNMP and can export flow data to external flow collectors. Routers also support sending Syslog messages to external logging servers to allow for integration into external monitoring tools, including security incident and event management (SIEM) tools.

APIs

Cisco vManage provides REST APIs; a programmatic interface for managing, monitoring, and troubleshooting all aspects of the SD-WAN solution. You can access the REST APIs through the Cisco vManage web server using a secure and authenticated HTTPS connection. For more information on this topic, please see the *Cisco SD-WAN APIs* chapter, found in this book.

Templates and policies

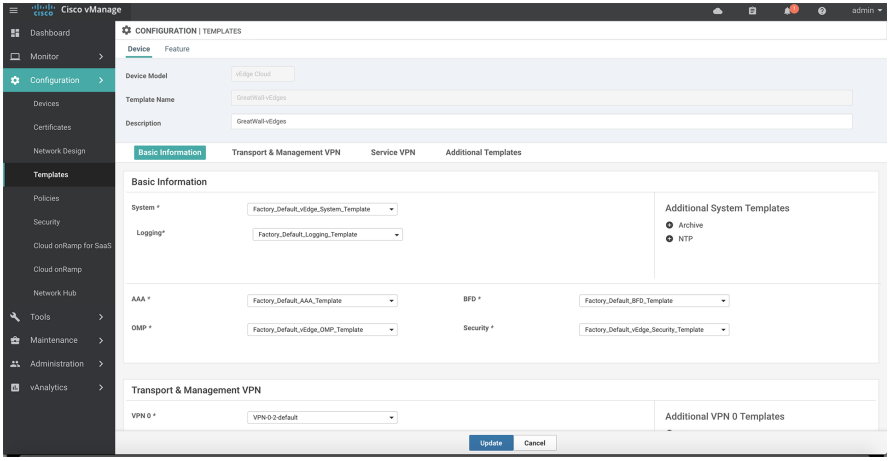
The configuration of WAN Edge routers and SD-WAN controllers is done using templates from vManage. A vManage template can be attached to multiple WAN Edge routers simultaneously. When changes are made to the configuration templates, these changes are automatically propagated to all attached WAN Edge routers.

There are two types of configuration templates: feature templates and device templates.

Feature templates help to build individual components of the router configuration such as segmentation, interfaces, system, routing, logging, and device access using RADIUS or TACACS.

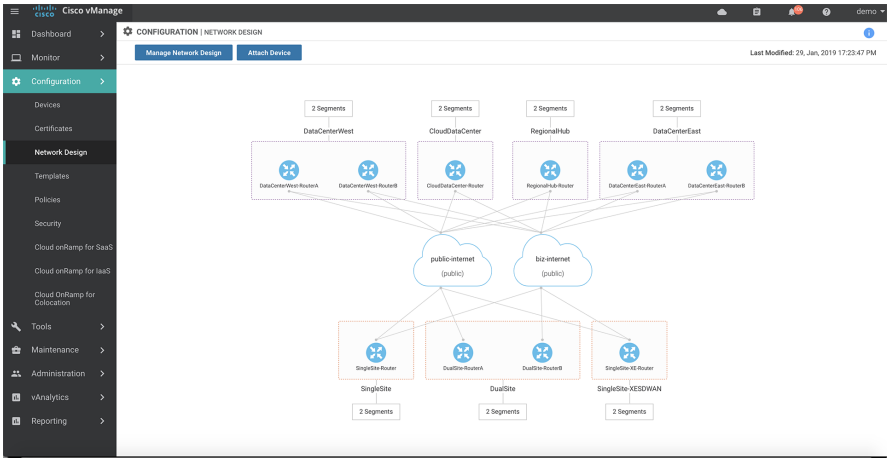
Device templates provide the framework for the entire router configuration and are made up of feature templates. Templates are flexible and allow for highly customizable router configurations. Efficient design of device templates allows customers to configure thousands of devices with minimal touch. When making an update to a template, the changes are propagated immediately to the WAN Edge routers. In case of configuration errors, the template configuration rolls back to its previous state. This rollback behavior protects the system against human errors.

DIAGRAM Sample Device Template



Another way to configure the WAN Edge routers is through the use of the Network Design feature, located under the configuration menu of Cisco vManage. With the help of Network Design, it is easy to design the network configuration by leveraging simple-to-follow wizards. vManage visually represents the configuration topology for the sites. The Network Design wizard automatically creates the templates and allows the user to start deploying WAN Edge routers.

DIAGRAM Network Design



Policies

SD-WAN policies are used to influence the flow of data traffic among WAN Edge routers in the SD-WAN fabric. Policies are of multiple types:

- Policies that affect the topology
- Policies that affect the flow of traffic
- Policies that are locally significant to a site

Topology policies

Centralized control policies operate on the routing and Transport Locator (TLOC) information within OMP and allow the customization of routing decisions. These policies can be used in configuring traffic engineering, path affinity, service insertion, and different types of VPN topologies (full-mesh, hub-and-spoke, regional mesh, etc.).

Traffic flow policies

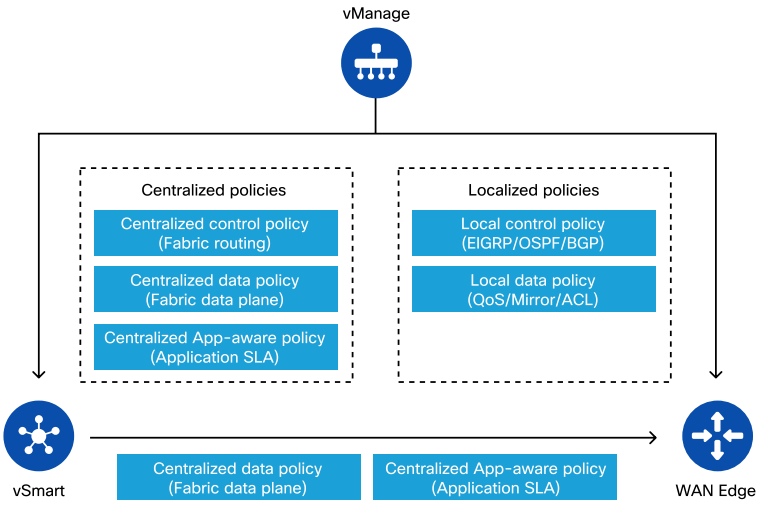
Data traffic policies influence the flow of traffic through the network, based on application signatures, fields in the IP headers, or the VPN segment the traffic is in. Centralized data policies are used in configuring application firewalls, service chaining, traffic engineering, and quality of service (QoS). These policies include Application-Aware Routing to apply SLAs for applications and traffic steering as well as activating AppQoE features such as packet duplication.

Locally significant policies

Localized policies are used to handle traffic at a specific site. These include Access Control Lists (ACLs), Quality of Service (QoS), and route maps for OSPF, BGP or EIGRP.

Policies are defined by the administrator using the policy wizard under the configuration menu of vManage. Centralized policies are applied by vManage to the vSmart controllers and localized policies are applied from vManage directly to the WAN Edge router.

DIAGRAM Cisco SD-WAN policy framework



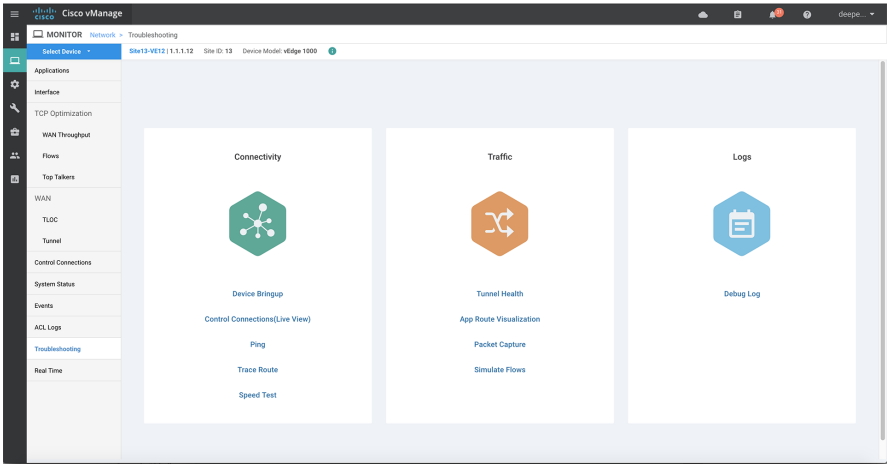
Troubleshooting

Cisco vManage allows an administrator to perform troubleshooting of all aspects of the SD-WAN solution right from the graphical user interface.

- Basic troubleshooting - such as Ping and Traceroute
- Intermediate troubleshooting - such as App Route Visualization and Simulate Flows
- Advanced troubleshooting - such as Packet Capture and Debug Logging

The troubleshooting section is available in vManage under Monitor > Network > Troubleshooting.

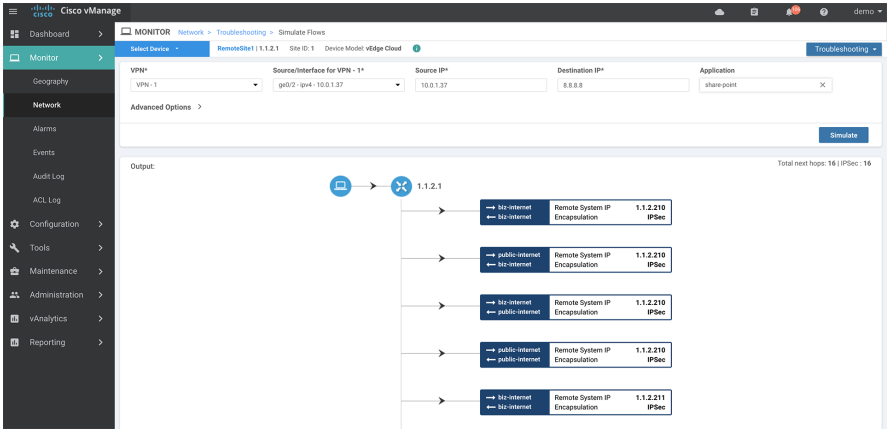
DIAGRAM Cisco vManage Troubleshooting



Cisco vManage allows many troubleshooting capabilities from its graphical user interface (GUI) and navigation to the individual WAN Edge router Troubleshooting sub-

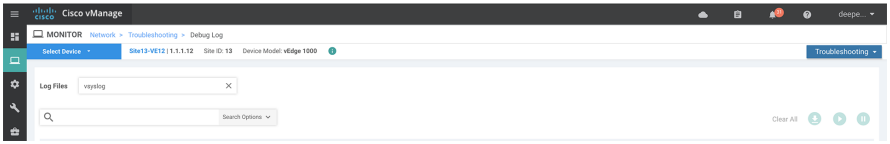
menus. Troubleshooting tools take the commands from the vManage GUI and instruct the WAN Edge routers to perform the tasks and report back their result. This eliminates the need to login to routers and perform these tasks manually. A simple Simulate Flow example for traffic destined to the Sharepoint application is shown below. This tool simulates how the WAN Edge router will treat this flow in real time by matching on the Sharepoint application using DPI, and visually depicting how the forwarding engine of the router chooses the outgoing transports after passing through all of the policies configured.

DIAGRAM Cisco vManage Troubleshooting Simulate Flows



Debugs can be enabled on the router and viewed on vManage under the Troubleshooting menu as well. Log files will be streamed directly to the vManage dashboard when performing detailed troubleshooting on these devices.

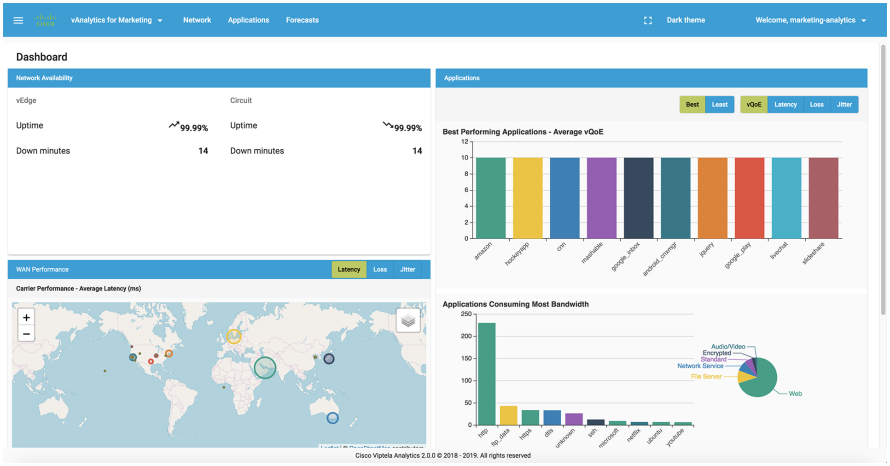
DIAGRAM vManage debug logs



Analytics

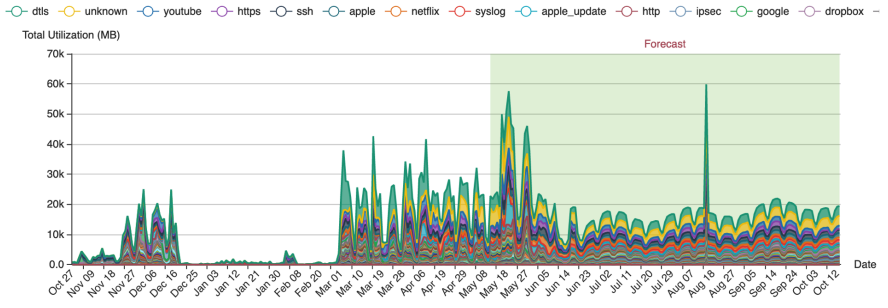
The Cisco vAnalytics platform is delivered as a Software as a Service (SaaS) offering from Cisco, providing graphical representations of the performance and availability of the entire Cisco SD-WAN fabric over time. It also provides visibility into the performance of applications passing over the fabric. In addition, vAnalytics can provide granular characteristics of individual carriers, tunnels, and applications at a particular time. Using vAnalytics, an enterprise can easily identify bandwidth usage, application performance, and detect anomalies based on historical trending.

DIAGRAM Cisco vAnalytics dashboard



Leveraging machine learning and artificial intelligence techniques, Cisco vAnalytics offers insights into future circuit and application utilization, assisting organizations in performing intelligent capacity planning.

DIAGRAM Cisco vAnalytics forecasting



Case study

With the Cisco SD-WAN solution, customers can use vManage to solve a number of their pressing issues. Below are 3 unique customers who have used vManage capabilities for 3 unique problem scenarios.

- A retailer looking to streamline a simplified network design
- A financial services institution using an API gateway for large-scale monitoring
- A healthcare organization leveraging the Operational Toolkit to troubleshoot applications

Retailer example

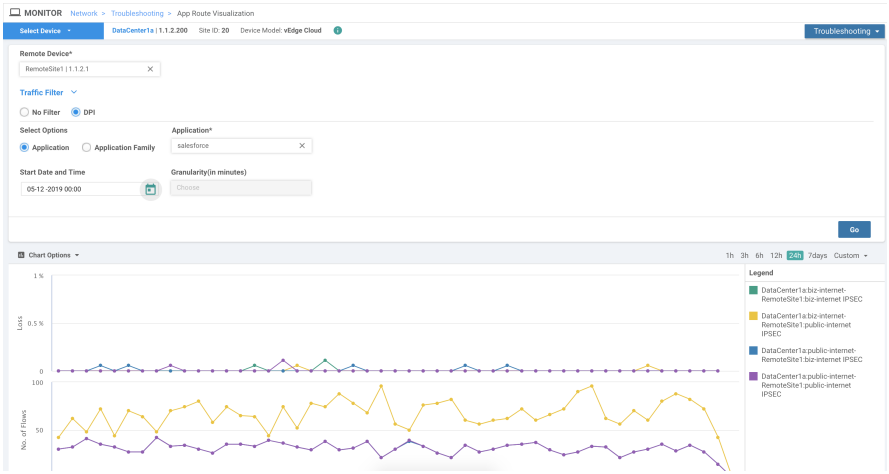
Though the Cisco SD-WAN solution is rich in features, some customers prefer to take advantage of its simplicity. In this case, a large retail outlet was able to utilize the vManage template construct to simplify remote branch deployment. By configuring a single template using variables, this organization was able to populate unique device-specific attributes by leveraging API calls to vManage. In addition, the customer was able to build a design framework with multiple data centers and remote sites that were homed to their respective hubs.

Financial example

A large financial services entity was in the process of deploying their SD-WAN environment. They realized that the telemetry data in the vManage system was valuable. This telemetry data included the loss, latency, and jitter experienced by each application at a site based on the the path that was taken. This was not just data that they used to troubleshoot problems when their clients reported application slowness, but also to observe circuit behavior over time. The network operators determined that they wanted to extract this data and process it in conjunction with other data they were collecting from other tools in their environment.

Using the vManage Bulk APIs, they were able to extract all data sets regarding all attributes at the site that they wanted to correlate to other network data. Instead of the laborious effort of extracting data on a site-by-site basis, they were able to request vManage to provide large data sets to obtain loss, latency, jitter, application usage over time and SLA violation data.

DIAGRAM App-route visualization



The customer now uses these reports to profile their circuits, report on applications affected, and engage with their internet service providers in a proactive manner to investigate issues in the underlying transport.

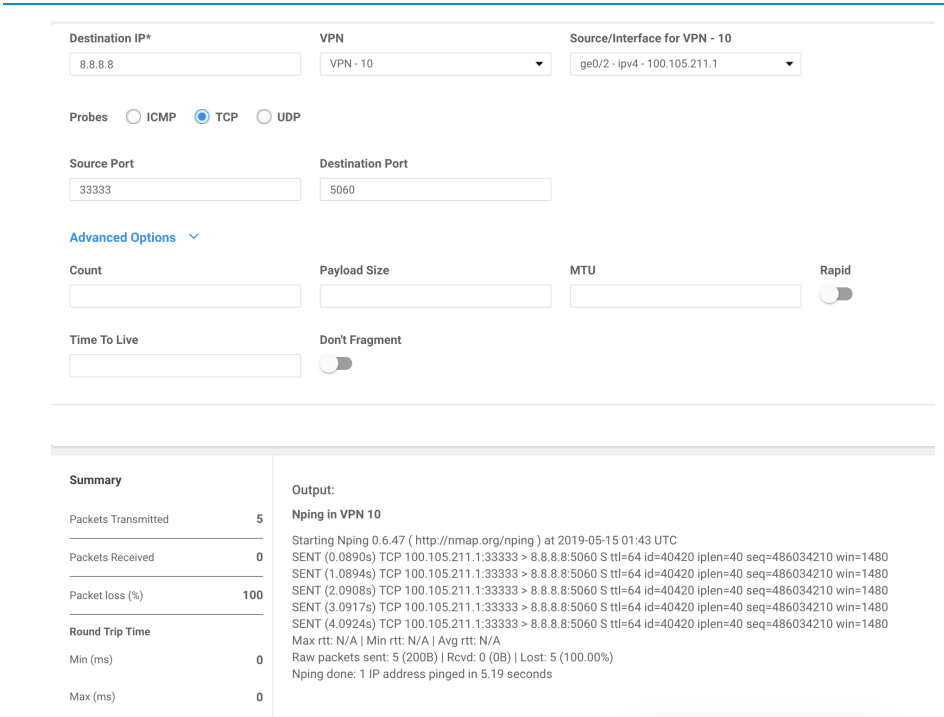
Healthcare example

The most significant need that the SD-WAN solution provides is very extensive tooling to respond to network situations as they arise. In this regard, when problems emerged, a particular healthcare customer used a combination of the Cisco SD-WAN tools to engage their own internal escalation resources, service providers, and the Cisco TAC. When an issue arose, they were able to:

- Extract path information for a particular traffic flow.
- Observe, in real-time, the loss, latency and jitter on the path in question.
- Take necessary packet captures for the traffic.

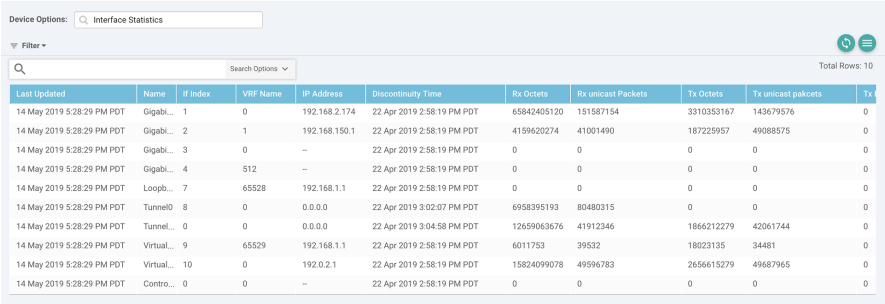
Specifically, the customer was able to validate the result of probes to observe expected behavior with specific applications from their users. In the diagrams below, note how the App Route Visualization tool is used along with the Ping tool to review the path the application took.

DIAGRAM vManage troubleshooting tools



In addition, this customer utilized the built-in device monitoring capabilities to review interface statistics, ensuring that traffic was properly delivered, processed and forwarded by the WAN Edge router.

DIAGRAM Interface statistics



Last Updated	Name	If Index	VRF Name	IP Address	Discontinuity Time	Rx Octets	Rx unicast Packets	Tx Octets	Tx unicast pakcets	Tx
14 May 2019 5:28:29 PM PDT	Gigabi...	1	0	192.168.2.174	22 Apr 2019 2:58:19 PM PDT	65842405120	151587154	3310353167	143679576	0
14 May 2019 5:28:29 PM PDT	Gigabi...	2	1	192.168.150.1	22 Apr 2019 2:58:19 PM PDT	4159620274	41001490	187225957	49088575	0
14 May 2019 5:28:29 PM PDT	Gigabi...	3	0	--	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0
14 May 2019 5:28:29 PM PDT	Gigabi...	4	512	--	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0
14 May 2019 5:28:29 PM PDT	Loopb...	7	65528	192.168.1.1	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0
14 May 2019 5:28:29 PM PDT	Tunnel0	8	0	0.0.0.0	22 Apr 2019 3:02:07 PM PDT	6958395193	80480315	0	0	0
14 May 2019 5:28:29 PM PDT	Tunnel...	0	0	0.0.0.0	22 Apr 2019 3:04:58 PM PDT	12659063676	41912346	1866212279	42061744	0
14 May 2019 5:28:29 PM PDT	Virtual...	9	65529	192.168.1.1	22 Apr 2019 2:58:19 PM PDT	6011753	39532	18023135	34481	0
14 May 2019 5:28:29 PM PDT	Virtual...	10	0	192.0.2.1	22 Apr 2019 2:58:19 PM PDT	15824099078	49596783	2656615279	49687965	0
14 May 2019 5:28:29 PM PDT	Contro...	0	0	--	22 Apr 2019 2:58:19 PM PDT	0	0	0	0	0

Key takeaways

As part of their network operations, organizations need to manage, monitor, and troubleshoot the environment in a simple and effective manner. This ensures that the network infrastructure is able to deliver on current and future business needs. The network infrastructure should provide the capabilities to quickly restore impacted services when issues arise.

- Cisco SD-WAN simplifies management and operations, and allows the network to deliver maximum network agility.
- Cisco vManage addresses Day 0, 1 and 2 tasks and challenges with a simple GUI-driven menu.
- Integration with other enterprise tools for log collection and flow collection is done through API's.

Further reading

Cisco Learning option Cisco SD-WAN Operation and Deployment (ENSDW) v1.0:
http://cs.co/SD-WAN-Operation-Training

Cisco SD-WAN APIs

Business need

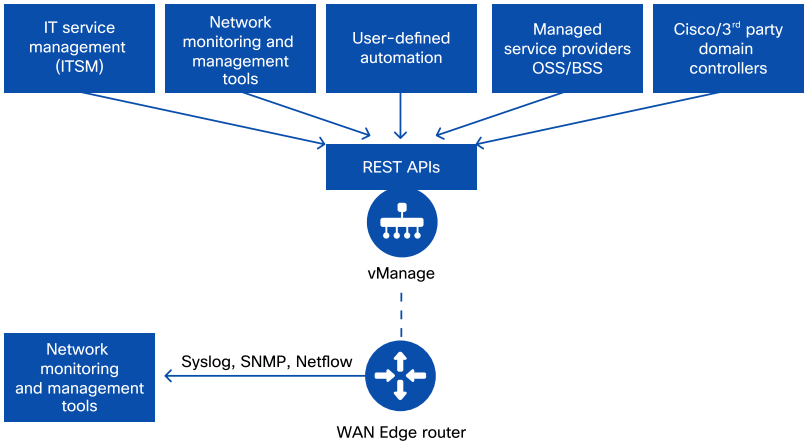
APIs enable IT to seamlessly integrate their existing operations environment with Cisco SD-WAN while also allowing a high level of flexibility to deliver new capabilities. For example, enterprise IT Service Management (ITSM) tools can be used to automate trouble tickets if there are issues with the WAN, while network monitoring tools can be used to aggregate data from the WAN with data from the rest of the network. This provides a more holistic view of the system, making it easier to pinpoint and troubleshoot problems faster. Service providers can also use APIs to integrate with their operations and billing systems to monitor customer networks and usage, while orchestrating changes across large numbers of nodes.

Tools integration

There are five different categories of tools that can be integrated with Cisco SD-WAN using the REST APIs in Cisco vManage. By integrating these tools with Cisco SD-WAN, additional levels of visibility, flexibility, control, and customization are achieved in order to meet unique business needs. The five categories of tools that can be integrated with Cisco SD-WAN are:

- IT Service Management (ITSM)
- Operational Support System and Billing Support System (OSS and BSS) tools for managed service providers
- Network monitoring and management tools
- User-defined automation
- Cisco or third-party domain controllers

DIAGRAM The Cisco vManage REST API interface



ITSM

Integrating Cisco SD-WAN with an ITSM system of choice can allow quicker identification of issues, reduce the time required to gather key information, simplify operations for support teams, and enable faster remediation to reduce downtime. ITSMs can:

- Automatically raise tickets in the ITSM system based on network conditions, allowing for quicker identification and remediation of critical network issues. For example, a workflow can be created that will automatically generate a ticket whenever a WAN Edge router or WAN circuit goes down.

- Retrieve key information from the network data and attach it directly to a ticket in the ITSM system to provide the operations team with the information they need to quickly identify or troubleshoot an issue.
- Enable automated remediation, allowing actions to be applied directly to the network without explicit involvement of IT personnel.

OSS/BSS tools for managed service providers

By leveraging the REST APIs exposed by Cisco vManage, MSPs can fully integrate their Cisco SD-WAN deployment with their operations and billing support systems (OSS/BSS). Key examples of these integrations include the following:

- Service orchestration, automating the deployment of MSP-hosted SD-WAN controllers for onboarding new customers or onboarding new customers as tenants onto existing MSP-hosted SD-WAN controllers.
- Self-service portal, allowing customers to subscribe to new services or change conditions of existing services. For example, procuring and configuring new circuits, increasing bandwidth of existing circuits, deploying SD-WAN security features on top of existing routing platforms, deploying network segmentation, etc.
- Leveraging service usage data collected by Cisco vManage to feed into the MSP billing system via REST APIs.

Network/security monitoring and management tools

Many modern network/security monitoring and management tools enable the use of vManage REST APIs. This allows a user to extract a greater level of detail on the operational state of the entire network and diminishes the need to collect and analyze individual device-level data. Traditional monitoring and management tools can still be leveraged, which primarily rely on Syslog, SNMP, and Netflow facilities made available

directly on the network devices. This is not an either-or choice and a user may opt for taking advantage of both approaches, especially during the time of transition from traditional networking to SD-WAN. Some examples of integrations for network/security monitoring and management tools are the following:

- Security Information and Event Management (SIEM), which provides insights into security exposure and on-going incidents and allows automated or manual remediative actions to mitigate them. The use of Cisco vManage APIs allows network-wide security policy enforcement and incident management.
- Application/network performance, which provides insights specific to application and network performance, often analyzing data across multiple elements, such as switches, routers, access-points, etc. The use of vManage APIs offers a consolidated view into network and application performance telemetry which can be easily consumed and integrated into end-to-end performance visibility.
- Network monitoring, which provides baseline monitoring for network availablity and utilization. Consuming network-wide data made available by the vManage APIs eliminates the need for individual device-level interrogation.
- Collecting and reacting to event notifications being generated by network devices (often generated using Syslog messages or SNMP traps).
- Allowing an efficient change management life cycle by planning and scheduling maintenance activities, but also allowing easier rollback, if necessary. This promotes operational consistency and transparency where executive management can be kept aware of the change activities taken on the infrastructure. vManage APIs provide a single interface for all operational activities, greatly simplifying the tasks required for executing infrastructure changes.

User-defined automation

While the vManage graphical user interface (GUI) provides a centralized management system and offers everything needed to operate the Cisco SD-WAN solution, vManage

REST APIs open a world of possibilities for extending automation to any user-defined task. Many users are leveraging these APIs to create custom automated sequences for managing, monitoring, configuring and troubleshooting the SD-WAN environment based on their specific needs. The use of APIs to automate specific vManage tasks is often times carried out by writing python scripts. For more advanced use cases, Ansible playbooks, or Chef and Puppet cookbooks can be leveraged. Here are some examples using vManage APIs:

- Time-based policy automation, based on the time of day in accordance with business requirements around application SLAs.
- Customized topology maps, network topology drawings based on customized vManage policy configuration.
- Location-based policies influencing fabric routing behavior based on the location of a mobile WAN Edge router.

Cisco/third-party domain controllers

Cisco vManage REST APIs can be leveraged for management plane integration across multiple domain controllers, in order to deliver a single end-to-end operational experience for management, monitoring, configuration, and troubleshooting. For example, vManage APIs can be leveraged by Cisco DNA Center and Cisco APIC controllers for campus and data center integration with the Cisco SD-WAN solution. Such integration can drive a common end-to-end policy for enforcing desired behavior across the entire infrastructure from user to application, from branch to cloud, and from cloud to cloud.

The open nature of vManage REST APIs allows easy integration of the Cisco SD-WAN fabric with third party domain controllers. These are control and management plane elements for operating a non-Cisco infrastructure, which may be present in the environment. Often, these are third-party services nodes which are managed by their own management tools.

For more information on multi-domain integration, see the *Multi-domain* chapter.

vManage API Library

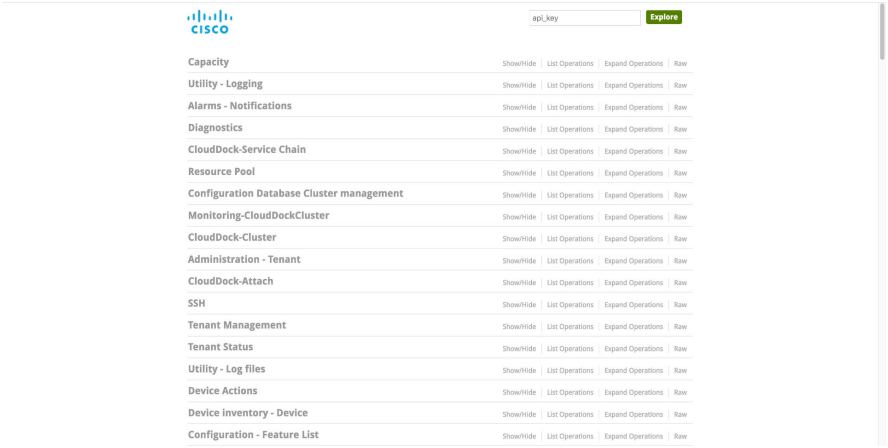
Cisco vManage has REST APIs which can be used for controlling, configuring, and monitoring SD-WAN Edge routers in the network. These APIs can be accessed through the vManage web server and are grouped into the following major categories:

Administration	Managing users and user groups, viewing audit logs, and managing the local vManage server.
Certificate management	Managing certificates and security keys.
Configuration	Creating feature and device configuration templates, retrieving the configurations in existing templates, and creating and configuring vManage clusters.
Device inventory	Collecting device inventory information, including serial numbers and system status.
Monitoring	Viewing status, statistics, and other information about operational devices in the overlay network.
Real-Time Monitoring	Retrieving, viewing, and managing real-time statistics and traffic information.
Troubleshooting tools	Troubleshooting devices for determining the effect of policy, updating software, and retrieving software version information.

In addition, a separate dashboard, where the user can look at the API library and test out the specific APIs which they want to use, can be accessed from a web browser using the following URL:

https://<vManage ip-address>:<port>/apidocs

DIAGRAM Cisco vManage API library dashboard



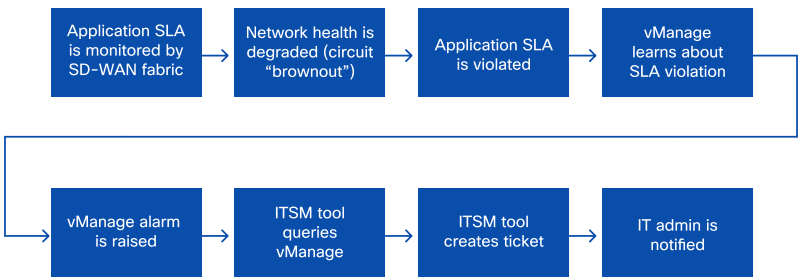
From the API dashboard, the user can test an API call to verify its usage and see the results.

Case study

Cisco SD-WAN programmatic APIs offer simple integration between Cisco vManage and IT Service Management (ITSM) tools. This case study example describes a financial organization which decided to use their ITSM tool to generate and track service requests.

Cisco vManage continuously monitors the health and availability of the entire SD-WAN fabric. Should any faults or sub-optimal conditions appear, vManage marks those as events and alarms, and they are periodically queried by the ITSM tool leveraging REST APIs. The ITSM tool creates a service request and populates the data extracted from vManage, which is then used by IT administrators to investigate and troubleshoot the issue further.

DIAGRAM Service request generation and tracking via REST API



The financial organization also decided to leverage Cisco vManage programmatic APIs to allow IT administrators to take remedial actions based on certain detected conditions. For example, the IT administrator could perform a router interface reset in order to restore connectivity across a failed WAN circuit by leveraging REST API calls invoked by a script executed directly from the ITSM administrative interface. The organization also chose to allow the ITSM tool to perform automated remedial actions

without explicit IT administrator involvement. These actions greatly expedited the time required to resolve service issues.

The integration of ITSM tools with vManage APIs allowed the organization to dramatically improve the service levels offered by the IT department to the rest of the organization and to lower the time required for full service restoration.

Key takeaways

Cisco SD-WAN offers a rich set of APIs available on the vManage. These APIs make it easy to integrate IT tools and processes into the day-to-day operations and management of the Wide Area Network. APIs provide the flexibility to further automate the Cisco SD-WAN solution without reliance on operating the Cisco vManage graphical user interface (GUI). Managed service providers and partners can use APIs to integrate Cisco SD-WAN with their billing and operations tools, as well as delivering customized services to their customers.

Further reading

To learn more about how APIs can be leveraged to automate and orchestrate SD-WAN, please visit the following resources:

- Cisco DevNet: *https://cs.co/sdwan-devnet*
- vManage REST API library: *https://cs.co/sdwan-apis*

Multi-domain

Business need

The way we work has transformed - users are mobile and always connected to the network. At the same time, there are more devices and things connecting to the network driven by the growth of IoT. These devices are managed from the cloud, where their data is stored. Applications themselves are becoming mobile and moving from data centers to the cloud, and in many cases, not moving to one cloud, but to a multicloud world. The challenge for IT is how to securely connect any user, on any device, in any network, to any application, regardless of where the user is located or where the application is hosted. Network domains include the data center, campus, branch, and external cloud providers. As part of the changing network landscape, security must be present and enforced end-to-end. The benefits of integrating these different domains gives IT the flexibility to distribute their workloads across the environment while maintaining reliable and secure access to users and devices.

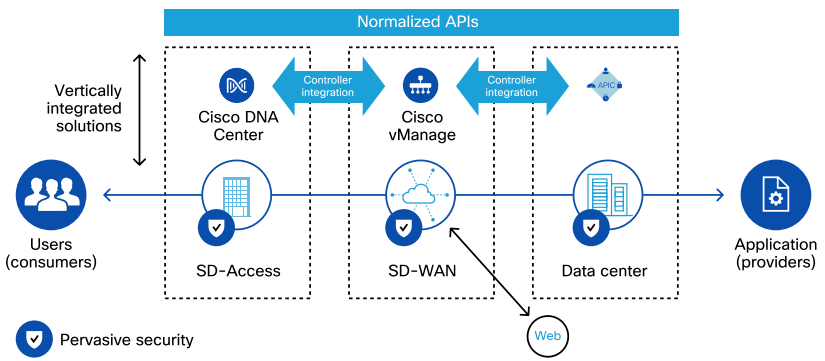
Multi-domain architecture

Cisco is building an architecture to help customers unify diverse networking domains. Using Cisco SD-WAN, the following use cases are possible with multi-domain integration:

- End-to-end segmentation
- Unified cross-domain policy
- Connecting access networks to multiple clouds

With the integration of Cisco SD-Access, Cisco SD-WAN and Cisco ACI, multi-domain integration delivers an end-to-end experience. Each of the domains is governed by its own domain manager and APIs are used to distibute the cross-domain intent. This approach offers a best-of-breed solution for the campus, WAN and data centers, while maintaining unique advantantages for each individual domain.

DIAGRAM Multi-domain architecture

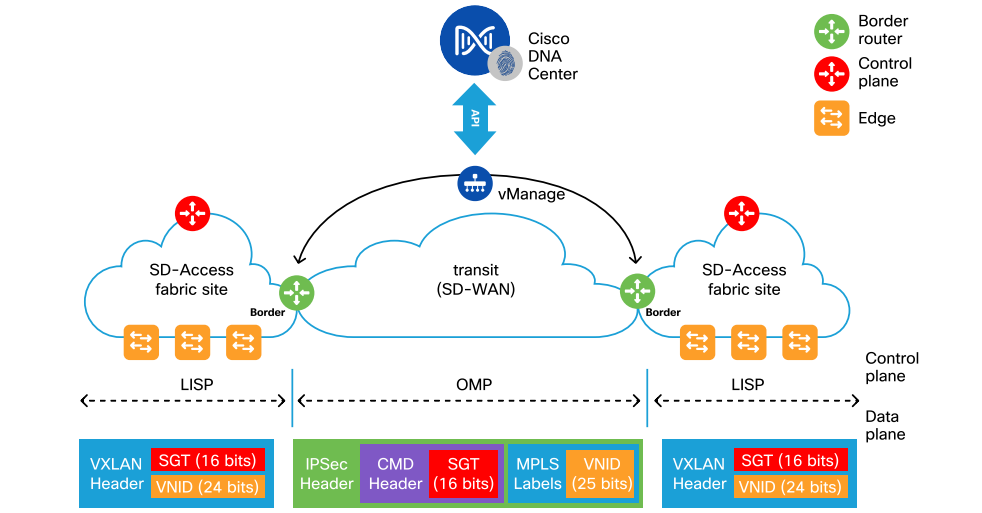


SD-WAN and SD-Access

Cisco Software-Defined Access (SD-Access) defines a single network fabric from the access layer to the cloud. Policy-based automation can be set for users, devices, and things to any application, without compromising on security and visibility within the network.

The SD-WAN integration with SD-Access involves carrying the Access metadata information in Scalable Group Tags (SGT) encapsulated in IPSec packets and sent over the WAN. The border router on the receiving SD-Access site de-encapsulates the traffic so it can be consumed on the receiving side. The following picture illustrates multi-site SD-Access with an integrated SD-WAN transit.

DIAGRAM Integrated SD-WAN and SD-Access



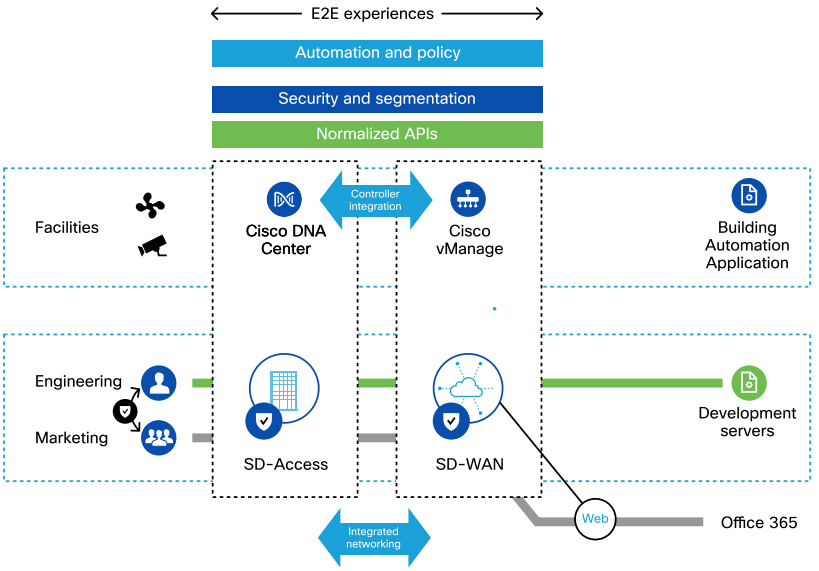
This integration achieves end-to-end secure connectivity. SD-Access identity services are critical in identifying users/things to deliver a trust-centric security layer. SD-

Access segmentation (macro/micro) prevents lateral movement of malware to deliver the first layer of a threat-centric security model. With the integration of SD-WAN, SD-Access segmentation is seamlessly extended between sites. The unification of segmentation policies between Cisco DNA Center and Cisco vManage is performed automatically.

SD-Access border routers perform two functions: WAN Edge and SD-Access termination. The WAN Edge functions are controlled through vManage and the SD-Access functions are controlled by Cisco DNA Center.

The management plane is integrated through the use of APIs. The solution integrates the visibility and assurance information across the domains for a comprehensive experience. All telemetry for border routers is transmitted back to Cisco DNA Center via the API connection between the SD-Access and SD-WAN controllers. The following figure shows this end-to-end architecture.

DIAGRAM SD-WAN and SD-Access unified management

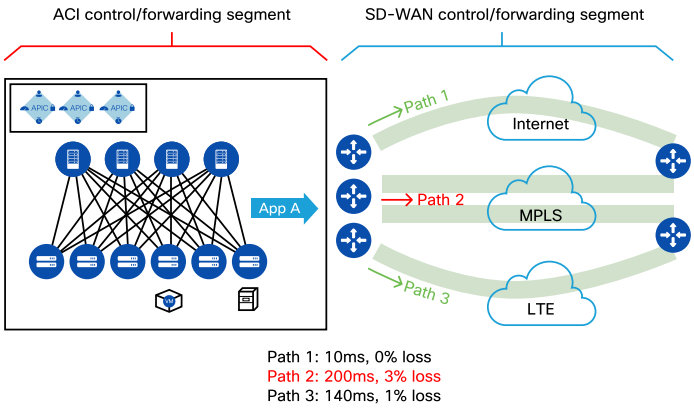


SD-WAN and Cisco ACI

The Cisco Application Centric Infrastructure (ACI) allows application requirements to define the network within the data center environment.

Remote site connectivity over the WAN towards applications residing in the data center is not SLA-aware and delay-sensitive. Applications will have poor user experience if connectivity is not reliable. Integrating SD-WAN with ACI helps to solve this problem by automatically propagating ACI policies into the SD-WAN fabric. This is done by automating workflows using REST APIs between Cisco vManage and the Cisco Application Policy Infrastructure Controller (APIC).

DIAGRAM SD-WAN ACI integration



Data center to branch connectivity can be enhanced with a user-defined policy that sets the SLA for certain application traffic. Using APIs, the Cisco vManage applies the SLA policy for specific applications from APIC, and pushes it to the WAN Edge router. Once the policy is enforced, the traffic will traverse the optimal path.

Future enhancements to this integration include:

- Having connectivity from the public cloud into the ACI fabric in the data center
- Multi-ACI data center connectivity over SD-WAN
- ACI remote-leaf connectivity within the branch.

Key takeaways

Network domains include the data center, campus, branch, and external cloud providers. As part of a changing network landscape, security must be present and enforced end-to-end. The benefits of these different domains give IT the flexibility to distribute their workload across their environment while maintaining reliable and secure access to users and devices.

- The integration of Cisco SD-Access, Cisco SD-WAN, and Cisco ACI delivers an end-to-end consistent experience.
- Each domain is governed by its own domain manager and APIs are used to distibute the cross-domain intent.
- Multi-domain offers the best-of-breed solution for campus, WAN and the data center, while maintaining unique advantages for each individual domain.

Further reading

- For more details on SD-Access please refer to the "Cisco Software-Defined Access" book, which can be found here: *http://cs.co/9001Ec6nD*
- For more details on the Cisco SD-WAN integration with Cisco ACI: *http://cs.co/ aci-sdwan*

SD-WAN managed services

Business need

As businesses look to evolve their WAN from traditional MPLS, Cisco SD-WAN can offer new revenue streams for both service providers and partners. Beyond SD-WAN as a managed service, security and application optimization are some examples of value-added services. Customers are looking to service providers to help them migrate to this new architecture. Likewise, for Cisco partners, SD-WAN presents the opportunity to enter the managed services market or expand existing managed services offerings beyond their core business.

Service orchestration

Partners and service providers looking to launch Cisco SD-WAN as a managed service require tools and capabilties to meet their needs around customer onboarding, automated provisoning, management, and monitoring. The following need to be considered for building a successful SD-WAN practice to operationalize end-customers:

- Pre-deployment device staging and certificate management
- New circuit turn up and circuit move/add/change assistance
- Day 0 and Day 1 configuration development and deployment
- End-to-end SD-WAN solution testing
- Day 2 operations, such as logging events and alerts collection (i.e. service ticket generation)
- Issue remediation using troubleshooting tools provided by Cisco vManage and/or by WAN Edge router CLI
- Software updates
- Customized reporting

Cisco SD-WAN provides partners and service providers with several choices in terms of how to orchestrate their Cisco SD-WAN service offering. The choices range from using Cisco vManage only, Cisco vManage with Cisco Network Services Orchestrator (NSO), or Cisco vManage with Cisco Managed Services Accelerator (MSX). Partners and service providers should evaluate these options to understand which one best meets their needs as well as the needs of their customers. Each of these options offer the ability to integrate with existing OSS/BSS tools to varying degrees.

Cisco vManage only

This model leverages Cisco vManage for a single or multitenant operation. It leverages the full set of Cisco vManage graphical user interface (GUI) capabilities and allows leveraging Cisco vManage APIs for programmatic provisioning and operation. Partners and service providers leveraging this model can consume the rich set of REST APIs exposed by Cisco vManage to integrate managed SD-WAN services into their own orchestration tools of choice and OSS/BSS systems (please refer to the *Cisco SD-WAN APIs* chapter for details on the REST APIs).

Cisco vManage and Cisco NSO

This model leverages Cisco NSO, a product that provides a highly customizable platform to build automation and workflows. Building on top of all functionality natively offered by Cisco vManage, Cisco NSO with its SD-WAN function pack adds and greatly simplifies a number of aspects of provisioning an SD-WAN infrastructure. Cisco NSO allows partners and service providers to unlock agility and flexibility at the Resource Facing Services layer (RFS).

Cisco vManage and Cisco MSX

This model leverages Cisco MSX, which is a complete orchestration and management platform that helps reduce the operational cost of building, deploying, and maintaining a managed services stack. The solution shifts the deployment of managed services away from the manual configuration of the latest network devices to the creation of a software abstraction to represent the service definition. This approach allows the service intent of the providers to be realized by using the service models to automate the creation and customization of cloud-based services, resulting in a significantly shorter time to making Cisco SD-WAN services live for all customers.

Multitenancy

Managed Service Providers (MSPs) and Cisco partners offer Cisco SD-WAN as a service for their end customers. MSPs running SD-WAN deployments for multiple customers have specific requirements regarding SD-WAN controllers. In order to run large and small scale deployments of Cisco SD-WAN, the solution provides options with the goal of simplifying provisioning, management, and monitoring for MSPs while keeping costs minimal.

When creating the SD-WAN service for their customers, MSPs may deploy a unique set of controllers for each customer or leverage the multitenant controller capabilities to support a larger number of customers. There are four possible deployment models for the SD-WAN controllers that MSPs can choose for their SD-WAN service.

Name	Single or Multitenant	Responsible party	Location
Cloud-hosted	Single tenant	Cisco	Cisco Cloud
Cloud-hosted	Multitenant	Cisco	Cisco Cloud
MSP-hosted	Single tenant	MSP	MSP Cloud
MSP-hosted	Multitenant	MSP	MSP Cloud

Cisco SD-WAN supports a wide range of physical and virtual WAN Edge routers that can be leveraged for their SD-WAN capability. MSPs choose the WAN Edge router from these options based on the needs of their customers. In many cases, this means leveraging a combination of both physical and virtual WAN Edge routers.

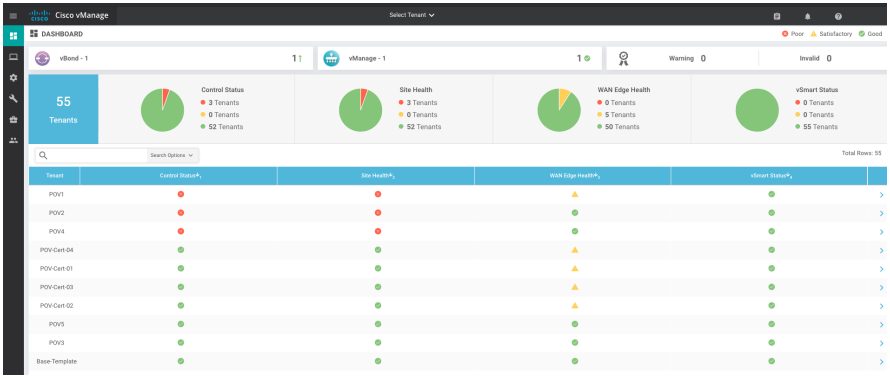
Tenancy models

When creating the service for their customers, the MSPs have the option to define tenancy in a number of ways and have granular control:

- Per Overlay Tenancy, where the controller infrastructure is shared, but the WAN Edge routers are dedicated per customer
- Per VPN Tenancy, where the controller and WAN Edge routers are shared, and the VPN segments are dedicated per customer

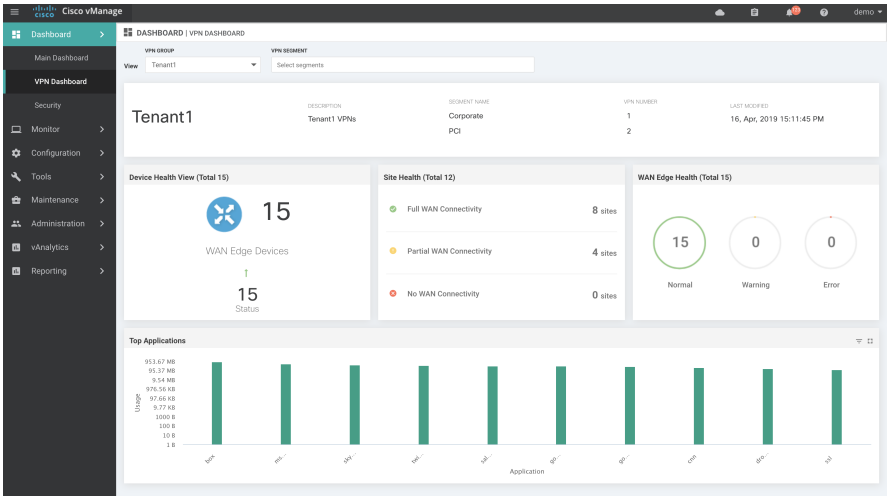
Using common SD-WAN vManage infrastructure, the MSP may choose to create fully isolated tenants in the environment. This deployment model results in WAN Edge routers that are isolated from any other tenant in the environment, and dedicated to a particular customer.

DIAGRAM vManage multitenant Dashboard



When MSPs use common WAN Edge routers to support multiple customers by leveraging VPN segmentation technology, they are able to create per-VPN tenants. In this case, a particular VPN or a set of VPNs is assigned to a specific customer, with their own configurations and monitoring dashboard environment.

DIAGRAM Cisco vManage VPN Tenancy



Role-based access allows MSPs to create service offerings which enable their customers to monitor and interact with the parts of the multitenant environment that service only that customer.

Case study

Cisco SD-WAN provides network automation and simplified configuration - a key benefit for any MSP. This case study shows how an MSP reduced SD-WAN deployment time for a global transportation and logistics company.

A customer planned a phased roll-out of new facilities by leveraging SD-WAN across its international locations. To achieve their business and technical goals, the customer reached out to their MSP requesting assistance to accelerate their remote site deployment. In the past, bringing up a new remote location took a long time; the average time to deliver an MPLS WAN connection to a remote site was 96 days. With Cisco SD-WAN, the MSP was able to have the remote site deployed in 10 hours, leveraging business-grade internet links and LTE. In addition to the speed of deployment, the MSP simplified the customer's day-to-day SD-WAN operations so they could focus on deploying new applications successfully. Application visibility, centralized network administration, and dashboard-based real-time analytics provided the customer with a new level of confidence.

Cisco Managed Services Accelerator (MSX) was leveraged by the MSP to enable Cisco SD-WAN for this multinational enterprise. This allowed the MSP to provision network services centrally and orchestrate a virtualized WAN Edge router on Cisco Enterprise Network Compute Systems (ENCS) platform to deliver a fully managed and multi-services branch.

Key takeaways

As businesses continue to develop their WAN strategy, many of them are looking to managed service providers and partners for help and answers. Capitalizing on this movement, service organizations can look to expand existing offerings, or create additional revenue streams while contributing this value. Cisco SD-WAN is equipped with the tools necessary to make MSPs and their partners successful in their endeavors.

- SD-WAN can offer new revenue streams for both service providers and partners.
- Managed service providers can deploy SD-WAN for their customers in single tenant or multitenant mode.
- Cisco SD-WAN provides MSPs with several choices in how they orchestrate their SD-WAN service (vManage, Network Services Orchestrator, Cisco Managed Services Accelerator).

Further reading

To learn more about how Cisco SD-WAN can help deliver SD-WAN as a managed service to customers, please visit the following resources:

- Cisco MSX: *http://cs.co/msx*
- Cisco vManage: *http://cs.co/9000EcMhw*
- Cisco NSO: *http://cs.co/9006Ec3Ba*

Appendix

Customer references

This is a sample of customer references at the time of publishing.
Please visit *http://cs.co/sdwan* to view the latest customers references.

"With the help of Cisco, we are more confident in making use of such technologies as mobile payments, biological recognition, intelligence applications, and big data, building retail big data ..."
Wang Mengzhe, IT Director of Xingbianli

"With Cisco SD-WAN, we've reduced our MPLS spending by 25 percent while increasing bandwidth by 3,075 percent."
Luis Castillo, Global Network Team Manager, National Instruments

Agilent's global rollout of Viptela SD-WAN enables our IT teams to respond rapidly to changing business requirements. We now achieve more than 80 percent improvement in turnaround times for new capability and a significant increase in application reliability and user experience.
Pascal Heger, Global Network Architect, Agilent Technologies

"SD-WAN on Cisco's ISR 4000 routers creates a robust, trusted platform on which to quickly realize security and performance benefits with a simple software upgrade."
Rui Pereira, Altice Portugal

"Verizon's Virtual Network Services offerings, leveraging Cisco's SD-WAN products, are deployed in tens of thousands of customer locations, enabling digital transformation and helping businesses accelerate their move to the cloud while reducing IT complexity and controlling cost."
Shawn Hakl, Senior Vice President, Verizon

"Optimal Office 365 performance is achieved by enabling local internet breakouts for key Office 365 scenarios, from users in the branch directly into Microsoft's global network. Modern SD-WAN solutions, such as Cisco's SD-WAN, make it easier for customers to implement this setup, support multiple DIA links, and dynamically choose the best one, improving the Office 365 user experience."
Konstantin Ryvkin, Partner Architect, Microsoft

"Cisco SD-WAN on ISR routers drives a reliable foundation to quickly integrate SD-WAN, simplify management, and improve real-time access to critical cloud-based business applications."
US Banking Institution

"With Cisco's SD-WAN advanced security, we can instantly turn any customer's entire network into a fortified wall across any cloud environment. This is a significant step toward adopting an enterprise architecture with integrated security, software-defined WAN, and cloud services, all managed via a single policy controller."
Bill Thompson, Practice Manager, World Wide Technology

"Bringing the WAN edge securely to the Internet is now possible with the new security features of Cisco SD-WAN delivered as a single consolidated solution."
Hussein Omar, Network Solutions Architect, Datacom

"Customers want more secure connections, usually with multiple cloud environments, so CDW sees Cisco's new integrated security features for SD-WAN as an important differentiator."
Will Kerr, Technical Architect, CDW

"With Cisco SD-WAN, my life as a network administrator is significantly easier. To deploy new configurations and policy changes across the entire network, which would have taken a very long time previously, touching many devices individually, now takes a matter of minutes."
Peter Castle, Network Administrator, Reece Group

Additional resources

Please visit the following sites for more detailed information about Cisco SD-WAN:

- Cisco SD-WAN main product page *http://www.cisco.com/go/sdwan*
- Cisco Communities - SD-WAN *https://cs.co/sdwan-community*
- Cisco Design Zone for Branch, WAN, and Internet Edge *http://cs.co/dz-sdwan*
- Cisco SD-WAN Product Documentation *http://cs.co/sdwan-docs*
- Cisco Validated Design SD-WAN Design Guide: *http://cs.co/sdwan-design*
- Software Licensing for SD-WAN and Routing: *http://cs.co/one-wan-subscription*

Acronyms

AAA - Authentication, Authorization, and Accounting

ACI - Application Centric Infrastructure

ACL - Access Control List

AES - Advanced Encryption Standard

AMP - Advanced Malware Protection

API - Application Programming Interface

APIC - Application Policy Infrastructre Controller

ASA - Adaptive Secuirty Appliance

ASIC - Application-Specific Integrated Circuit

ASR - Aggregation Services Routers

AWS - Amazon Web Services

BFD - Bidirectional Forwarding Detection

BGP - Border Gateway Protocol

BSS - Business Support System

BYOL - Bring Your Own License

CA - Certificate Authority

CBC - Cipher Blocker Chaining

CE – Customer Edge

COS - Class of Service

CSP - Cloud Services Platform

Cisco CSR - Cloud Services Router

CSR - Certificate Signing Request

CSV – Comma Separated Values

DIA - Direct Internet Access

DMZ - Demilitarized Zone

DNA - Digital Network Architecture

DNS - Domain Name Services

DPI - Deep Packet Inspection

DSCP - Differentiated Services Code Point

DTLS - Datagram Transport Layer Security

EIGRP - Enhanced Interior Gateway Routing Protocol

ENCS - Enterprise Network Compute System

ERRS - Enterprise Records Retention Schedule

ESP - Encapsulating Security Payload

FEC- Forward Error Correction

FPD - Field Programmable Devices

FQDN - Fully Qualified Domain Name

FTD - Firepower Threat Defense

GCM - Galois/Counter Mode

GRE - Generic Routing Encapsulation

GUI - Graphical User Interface

HTTP - Hyper Text Transfer Protocol

HTTPS - Hyper Text Transfer Protocol Secure

IaaS - Infrastructure as a Service

IDS - Intrusion Detection System

IKE - Internet Key Exchange

IoT - Internet of Things

IPFIX - Internet Protocol Flow Information Export

IPS - Intrusion Prevention System

IPSEC - Internet Protocol Security

ISR – Integrated Service Routers

IT - Infrastructure Technology

ITSM - Infrastructre Technology Service Management

KVM - Kernel-based Virtual Machine

LTE - Long Term Evolution

MFA - Multi-Factor Authentication

MPLS - Multi-Protocol Label Switching

MSP - Managed Service Provider

MSX - Managed Services Accelerator

MTU - Maximum Transmission Unit

NAT - Network Address Translation

NETCONF - Network Configuration Protocol

NSO - Network Services Orchestrator

OMP - Overlay Management Protocol

OPEX - Operating Expenses

OSPF - Open Shortest Path First

OSS - Operational Support Systems

PCI - Payment Card Industry

PnP - Plug and Play

QoS - Quality of Service

QoE – Quality of Experience

RADIUS - Remote Authentication Dial-In User Servic

RBAC - Role Based Access Control

REST - Representational State Transfer

RSA - Rivest–Shamir–Adleman

SA – Security Assocation

SaaS - Software as a Service

SAML - Security Assertion Markup Language

SDA - Software-Defined Access

SDN - Software-Defined Network

SGT - Scalable Group Tags

SHA - Secure Hash Algorithm

SIEM - Security Information and Event Management

SLA - Service-Level Agreement

SD-WAN - Software-Defined Wide Area Network

SNMP - Simple Network Management Protocol

SSO - Single Sign On

SUDI - Secure Unique Device Identifier

TAC – Technical Assistance Center

TACACS - Terminal Access Controller Access Control System

TAM - Trust Anchor Module

TCP - Transmission Control Protocol

TLOC - Transport Location

TLS - Transport Layer Security

TPM - Trusted Platform Module

UCS - Unified Computing System

URL - Uniform Resource Locator

VPN- Virtual Private Network

VPC - Virtual Private Cloud

VNF - Virtual Network Functions

VNET - Virtual Network

vQoE - Viptela Quality of Experience

VRRP - Virtual Router Redundancy Protocol

ZTP - Zero-Touch Provisioning

Aaron Rohyans
Ali Shaikh
Chandra Balaji Rajaram
David Klebanov
Deepesh Kumar
Gina Cornett
Hasham Malik
Kiran Ghodgaonkar
Madhavan Arunachalam
Nikolai Pitaev
Travis Carlson
Zaheer Aziz