

# Intro to SASE: SD-WAN Networking Foundation

Adapted and updated from *Journey into the World of SASE*  
Rohan Naggi and Ferdinand Sales, VMware Press, April 2021

[Download the full book](#)

## Table of contents

Key takeaways .....	3
Introduction .....	3
The networking journey .....	3
Router .....	3
Private link, MPLS and VPN .....	4
WAN optimization .....	4
SD-WAN .....	4
Traditional WAN challenges .....	5
SD-WAN advantages .....	6
WAN evolution .....	8
First generation WAN transformation: Private networks .....	8
Second generation WAN transformation: SD-WAN and cloud-ready .....	9
Third generation WAN transformation: Modern multi-cloud .....	10
SD-WAN transformation.....	11
VMware SD-WAN cloud-delivered model .....	12
Deployment simplification.....	12
Multiple deployment options .....	13
Zero-touch provisioning .....	13
Assured application performance .....	14
Business policy and smart defaults .....	14
Dynamic Multipath Optimization .....	15
Network visibility and agile troubleshooting .....	16
Architecture for the cloud .....	16
Network security .....	17
Distributed services insertion via service chaining .....	17
Network segmentation .....	17

**CHECKLIST: SD-WAN PRINCIPLES**

- The **software-defined networking model** unifies management of hardware, routing, and security components to reduce WAN complexity while improving user experience.
- Broadband connectivity can **coexist with or replace** expensive MPLS and leased line circuits, dramatically lowering bandwidth costs and hardware expenses.
- **Integrated architecture** provides granular, end-to-end visibility and control for both underlay and overlay networks.
- The **cloud-ready architecture** eliminates backhaul traffic and supports local Internet traffic breakout.
- **Centralized management** enables network segmentation, streamlines operations, reduces errors, and drives consistent security policy.
- **Automation and AI** intelligently steer traffic to deliver predictable application performance.
- Full support for **segmentation** includes the isolation of management, control, and data plane traffic.

**Key takeaways**

As applications move to the cloud, enterprises need a network that can keep up. To address the application performance issues of traditional wide area networks, a software-defined wide area network (SD-WAN) provides simplified and flexible deployment options, improved application performance, security, and complete visibility at the network edge.

SD-WAN solutions streamline management and deliver cost savings to the enterprise. They provide the foundation for cloud connectivity and modern operational models, allowing IT to deliver a new level of enterprise-wide service and user experience.

**Introduction**

Today's applications and network architectures require a novel approach. The emergence of cloud, virtualization, and as-a-service models have upended traditional enterprise networking. In this multi-cloud world, organizations have been forced to reconsider how they design their wide area networks to connect and unify their dispersed sites.

Management trends and practices are changing. Networking teams are under increased pressure to simplify the network, make it more flexible, and centralize controls while simultaneously optimizing application performance. Companies want to reduce costs through network simplification, cloud adoption, improving IT support and troubleshooting, and increasing software licensing efficiency. Improving security remains an overarching goal to ensure critical data is protected. Changing government and industry regulations mandate a continued focus on compliance.

The modern WAN must support connectivity for traditional applications and latency-sensitive real-time services such as voice-over-IP (VoIP) and videoconferencing. Bandwidth-intensive applications are not limited to the office/campus environment; connectivity is needed not just for communication and collaboration but also for digital signage, physical security, and surveillance.

The importance of agility has increased with the pace of business. The IT infrastructure is a crucial enabler of innovation and business growth. Stakeholders expect rapid access to technology resources and the ability to quickly scale up or down as business requirements change. In this fast-paced world of digital transformation, it is unacceptable for the network to be a bottleneck in delivering on-demand infrastructure. The network is expected to always be available and ready to deliver on any requirement; even a brief outage can cause significant disruption to the business.

This chapter explores challenges and opportunities in wide-area networking—where it started, how it has evolved, and why SD-WAN presents an opportunity for the future.

**The networking journey**

Wide area networks are composed of both networking and security stacks, with each moving through several phases of significant evolution. Historically, networking and security trends have often been thought of in terms of silos.

Networking began with the router, introduced new technologies such as WAN optimization, and then saw the evolution of the Edge and introduction of SD-WAN. In the security space, firewall offerings have evolved, and increasing consumption of cloud offerings has made new security-as-a-service models more relevant. Today's digital transformation journey brings together networking and security in the cloud, aligning them to address the needs of modern applications and users.

**Router**

Traditionally routers have been used at the enterprise edge to provide WAN connectivity. These routers lack policy-based control and automation as well as the intelligence for

cloud connectivity. Routers generally do not consider the details of underlying transport infrastructures; this lack of abstraction capability limits their flexibility when connecting to the cloud.

To support a redundant WAN design, complex BGP tuning is required to support load balancing. In this model, path attributes may not allow for the selection of the best-performing path, and path length is not necessarily correlated to performance. Additionally, WAN routers do not have insight into enterprise application SLAs and policies, leading to unpredictable performance.

### Private link, MPLS and VPN

MPLS and private line services are dedicated connections delivered by service providers. These services offer predictable performance and come with SLAs providing guaranteed traffic performance and delivery. Unfortunately, they tend to be significantly more expensive than broadband Internet services, which offer the benefit of being easier to procure and deploy than MPLS and private line services. While MPLS delivers key benefits, including scalability, performance, improved bandwidth utilization, and reduced network congestion, it is not designed for the cloud and SaaS. This is primarily because all traffic must be backhauled, adding latency that ultimately impacts user experience.

VPN links offer a cost-effective and secure remote connectivity alternative. These connections establish an encrypted tunnel across the public Internet for security, connecting remote users to the corporate network through a VPN client. While VPNs continue to be widely used, this technology still has the bandwidth, scaling, and security challenges. New approaches are being put in place to provide alternatives to VPN.

### WAN optimization

MPLS costs and application-specific requirements (e.g., latency sensitivity) were early factors driving WAN optimization over international links. With the rise of real-time voice and video traffic, services highly sensitive to latency and jitter, this capability was a welcome feature.

WAN optimization includes basic inline compression and a range of TCP optimizations, data deduplication, application proxies, and protocol-specific optimizations. These capabilities proved effective at managing latency-sensitive applications and transfers of large amounts of data across the limited bandwidth WAN links, especially for global transmissions.

Deploying WAN optimization solutions is complex and requires physical appliances at each end of the connection. These systems are limited to application proxy support and encryption applications such as TLS and SSL-based solutions. WAN optimization devices do not improve users' experience outside of the traditional office environment.

### SD-WAN

Over time, applications became smarter and less chatty on WAN links. Services began moving to the cloud (e.g., SaaS) while the public Internet became faster, more economical and available. Additionally, SD-WAN made broadband Internet connections more reliable, higher-performing, and secure for business communications and services; they were no longer viewed as only best-effort connections. Being transport-independent, SD-WAN could focus on application performance. It used application recognition, bandwidth aggregation, dynamic path selection while providing security and minimizing routing complexity. SD-WAN allowed enterprises to adopt software-defined networking (SDN) practices that separated the data, control, and management planes.

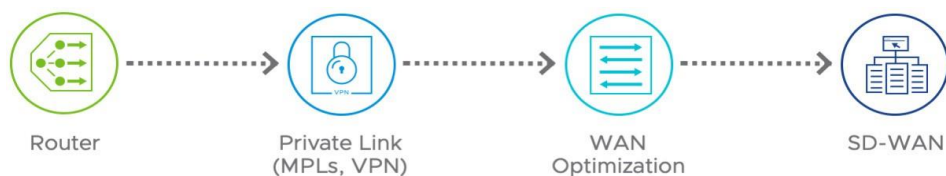


Figure 1: Transformation for WAN router to SD-WAN Edge device

## Traditional WAN challenges

Corporate WAN infrastructures have built up over time. They were designed to support applications and models that have since evolved. Problems with legacy applications are often evident, while issues with the underlying infrastructure—such as the WAN—are rarely obvious or prominent.

The traditional WAN faces challenges in many areas: complexity, scalability, quality of experience, architecture, and security. This section examines these issues in detail before exploring how SD-WAN capabilities address problems facing the modern wide-area network.

- Complexity:** Traditional management tools lack the visibility and control to unify the operational experience. Configuration is performed device by device, often through a command line interface, requiring customization for each site while being prone to human-induced errors. Important QoS policies are inconsistently defined and challenging to implement appropriately. Troubleshooting is a manual, time-consuming process that impacts availability and reliability. Network teams must deliver solutions that drive faster time-to-market, aid in quick adoption of new technologies, and move beyond manual operational processes to provide a more automated and agile infrastructure. A single solution is needed that configures, manages, monitors, and analyzes across the entire infrastructure.

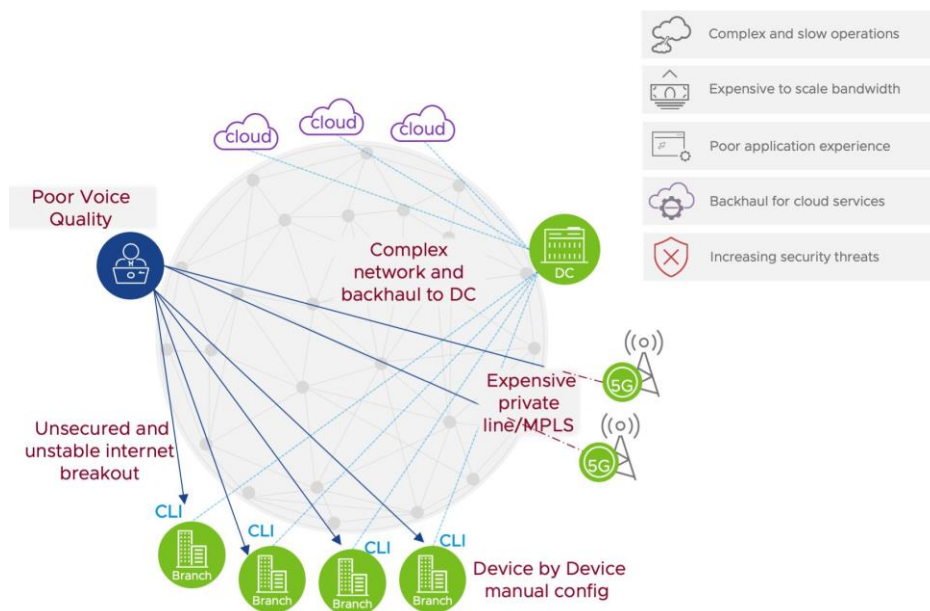


Figure 2: The WAN can be expensive, complex and inefficient

- **Increasing cost:** Businesses are forcing IT to reduce expenses. As budget reductions impact both CAPEX and OPEX, there are insufficient funds for additional traditional MPLS and private line circuits. Broadband connections do not provide the reliability and security that enterprises have come to rely on. Service level agreements (SLAs) are insufficient to address latency, packet loss, and jitter concerns that degrade modern application performance. Traditional WAN offerings do not provide high-quality, cost-effective solutions reaching from the branch edge through to the data center.
- **Quality of experience:** Traditional networks are not designed to address the needs of applications at the edge or in the cloud. As more users connect to the cloud to access their applications from anywhere, they must have an infrastructure that can deliver delay-sensitive traffic and reliable connectivity that provides the best user experience. Today's existing WAN infrastructure cannot support this type of user experience. Simply upgrading existing infrastructure with additional bandwidth is merely a bandage solution that is disruptive, costly, and ultimately delays application modernization in other areas.
- **Architecture:** Cloud solutions are everywhere—deployed as infrastructure as-a-service (IaaS) in cloud providers (e.g., AWS, Microsoft Azure, Google Cloud), at peering points (e.g., Equinix, Rackspace), with application providers (e.g., Microsoft 365, Salesforce), and as storage solutions (e.g., Box, Dropbox). The wide-area network must bring together corporate data center, campus, branch sites, cloud connectivity, and remote workers efficiently, cost-effectively, and securely. Legacy architectures and complexities hold organizations back. Backhauling of traffic from the branch to the data center and then to the cloud impacts performance by adding latency. Visibility is limited outside the corporate perimeter, where traffic routing is left to the Internet's whims. A solution is needed that can help with the challenges of managing WAN circuits, addressing last-mile quality issues, and steering traffic based on application policy and performance.
- **Security:** The cloud's global reach opens a new wave of security threats and breaches. The traditional corporate security perimeter is no longer sufficient. Enterprises need to be bold and think about an integrated approach beyond just on-premises security. Security organizations must look for solutions that encompass the corporate environment, including mobile access and the cloud.

## SD-WAN advantages

As networks have become more complex, organizations have turned to software-defined networking to improve infrastructure efficiency, manageability, and scalability. SDN abstracts the network to a set of functional capabilities independent of the physical implementation. Interaction with the network does not need to address specific networking equipment or other physical aspects that may regularly change.

One of the first practical SDN applications, SD-WAN applies these software-defined principles to the wide-area network to deliver similar advantages. SD-WAN segregates control and data planes to independently use the scaling and redundancy mechanisms best suited for each. Virtualized resources provide accelerated service delivery, better performance, and improved availability by automating network deployment and management while reducing the total cost of ownership.

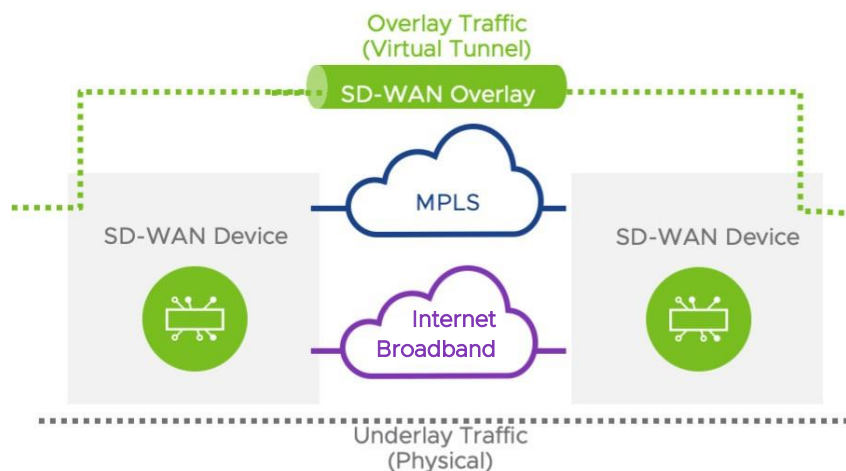


Figure 3: SD-WAN overlay tunnel on multiple links

SD-WAN provides a software abstraction layer to create a network overlay layer and decouple network software services from underlying hardware WAN circuits, as shown in Figure 3. This new abstraction layer lets network administrators control and manage networks more efficiently than possible using traditional approaches to address the underlying WAN hardware.

SD-WAN empowers organizations to address business-critical priorities at the edge by enabling rich deployment, management, and scaling capabilities. It allows network teams to cost-effectively provide the connectivity and performance that dispersed organizations need while maintaining deep controls and visibility across the infrastructure.

These capabilities unleash several benefits:

- **Optimized cloud architecture:** SD-WAN addresses the performance problems associated with the need to backhaul network traffic required with MPLS and other traditional models. It lets organizations utilize broadband Internet links to provide secure, high-performance connections from the branch to the cloud. This architecture also supports local Internet connectivity breakout with firewalling.
- **Business agility and flexibility:** SD-WAN makes it fast, easy, and cost-effective for organizations to deploy the WAN services needed to support branch offices. It minimizes the need for onsite IT services, eliminates unnecessary truck rolls, and offers the ability to leverage broadband Internet services, which are cheaper and easier to procure and deploy.
- **Broadband internet economics:** SD-WAN delivers the power of choice, freeing organizations to select from a variety of Internet connectivity options. These options are quick and easy to set up, allowing an organization to augment network connectivity with secure, dependable WAN services at a much lower price point than equivalent MPLS links.
- **Rapid adoption, simplified manageability:** Speed and business agility are essential. SD-WAN solutions are easy to deploy, powered by automation and centralized provisioning that accelerate deployment and minimize requirements for dedicated personnel at remote sites.
- **Hybrid WAN:** Most distributed organizations already have MPLS connecting their branch offices. SD-WAN complements existing technologies, allowing the deployment of additional broadband links without modifying the existing WAN infrastructure. As business requirements change, an organization can migrate traffic toward cost-effective



Internet bandwidth, freeing up MPLS links for applications that have distinct performance or compliance requirements.

- **Automation and traffic steering:** SD-WAN supports application-based traffic prioritization, providing tuning tools and the ability to dynamically modify flows to align with changing network conditions. The automation capabilities also enable faster provisioning and onboarding of new sites and users, eliminating redundant, time-consuming, error-prone manual processes. With SD-WAN, enterprises have complete visibility of their network, including detailed real-time analytics that provides actionable insights.

## WAN evolution

Wide-area network architecture and design have undergone a continuous transformation over the past few decades. In recent iterations, optimized access to cloud resources and application-tailored performance has become critical to enterprise productivity. Internet WAN evolution can be grouped into three distinct generations: private connectivity, cloud-ready, and modern multi-cloud architectures. The following sections examine the transition from foundational WAN models to current solutions and best practices.

### First generation WAN transformation: Private networks

The first generation wide-area networks were private links and MPLS services connecting branch offices to central campus and data center sites. Most, if not all, applications were located on-premises with predictable traffic patterns. Architectures commonly followed a hub/spoke model with branch-to-data center traffic flows. The enterprise managed several remote networking and security devices, including routers, switches, firewalls, load balancers, and intrusion detection system (IDS)/intrusion prevention system (IPS) appliances. Distinct tools were required for remote management, further adding to operational expenses.

Private line and MPLS circuits were the primary forms of connectivity for the branch to data center connectivity; public Internet connections were only considered as emergency backup links. Despite their inherent reliability and security, MPLS links proved to be costly as traffic demands grew. Traffic could not be effectively load-shared across public Internet links due to their lack of enterprise-grade performance; these links were an ongoing expense for rarely used backup capacity.

Traditional WAN design was static by nature; traffic flowed from branch offices to the data center and was secured by on-premises solutions. With the rise and rapid transition to cloud provider solutions, this architecture was not ready to address new challenges posed by the public Internet. Routing complexity further complicated the situation. Specialized technical skill sets were required to manage, configure, and support WAN devices properly. Lack of visibility created troubleshooting challenges. While larger corporations may have managed connections to multiple service providers, Internet connectivity was often a single pipe in and out of the network. There was rarely planning for proximity or performance related to providing services.

In summary, characteristics of first-generation enterprise WAN included:

- Expensive, point-to-point links connecting sites
- Inactive broadband Internet solely as a backup
- Static network topology, not focus on Internet and cloud-ready connectivity
- All traffic backhauled to the corporate data center for security/processing, creating delay and bandwidth contention
- Discrete systems with multiple points of management. Multiple User Interface (UI) for management
- Traditional routing (e.g., OSPF, BGP) was key to traffic management



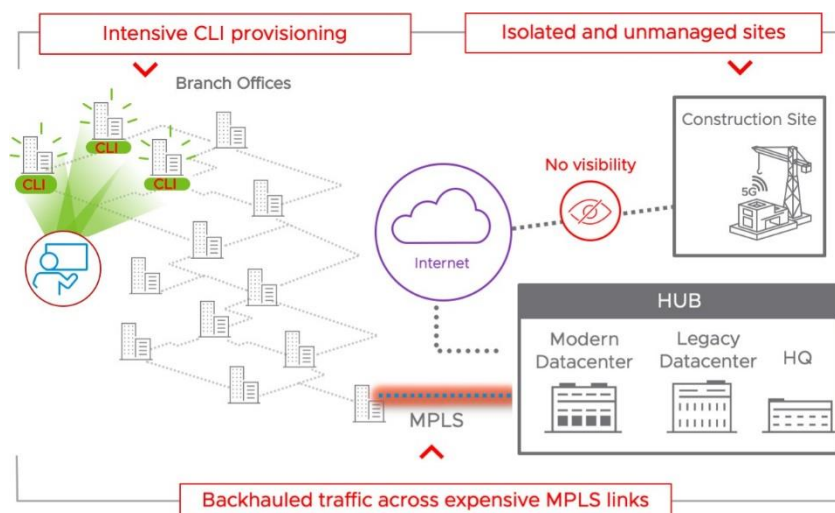


Figure 4: First-generation WAN transformation: Private networks

## Second generation WAN transformation: SD-WAN and cloud-ready

SD-WAN entered enterprise networks and marked the second generation of transformation. It was based on SDN principles that segregated the control, management, and data planes. SD-WAN provides a richer application experience combined with centralized management. Key to adoption was the deterministic application performance, end-to-end visibility, and integrated security. Individual solutions offered automated templates to speed cloud onboarding and delivering on promises of rapid time to deployment (e.g., zero-touch provisioning).

SD-WAN provided predictable and reliable performance across public broadband connections at a much lower price point. This allowed the Internet to become the de facto transport standard across which SD-WAN controls provide application awareness and routing, quality of experience (QoE), intelligent link remediation, and consistent security. At the same time, SD-WAN helped enterprises augment both public (e.g., broadband) and private (e.g., MPLS circuits) links for SaaS applications and cloud-based services.

As applications and platforms move to the cloud, SD-WAN removes requirements to backhaul traffic to the corporate data center. It enables direct branch-to-cloud connectivity with policy-based controls to ensure a fast and responsive SaaS experience.

Highlights of second-generation WAN capabilities include:

- Simplified operations through centralized management and zero-touch deployment, applicable to both green and brownfield environments.
- Fully functional APIs enable integration of third-party components (e.g., security services) and streamline connectivity to enterprise management tools.
- Assures application performance over any WAN link by providing link monitoring, dynamic traffic steering, policy-based prioritization, and real-time remediation.
- Direct access to SaaS, hybrid, and multi-cloud solutions reduces latency and improves user experience.
- Provides customization for implementing security, supporting security service insertion for third-party firewall services as virtual network functions (VNF), redirecting branch site traffic to cloud security services, and enabling end-to-end segmentation.

- Support for universal customer premises equipment (UCPE) for various network and security functions.
- Cost-effective connectivity with enterprise-grade performance.

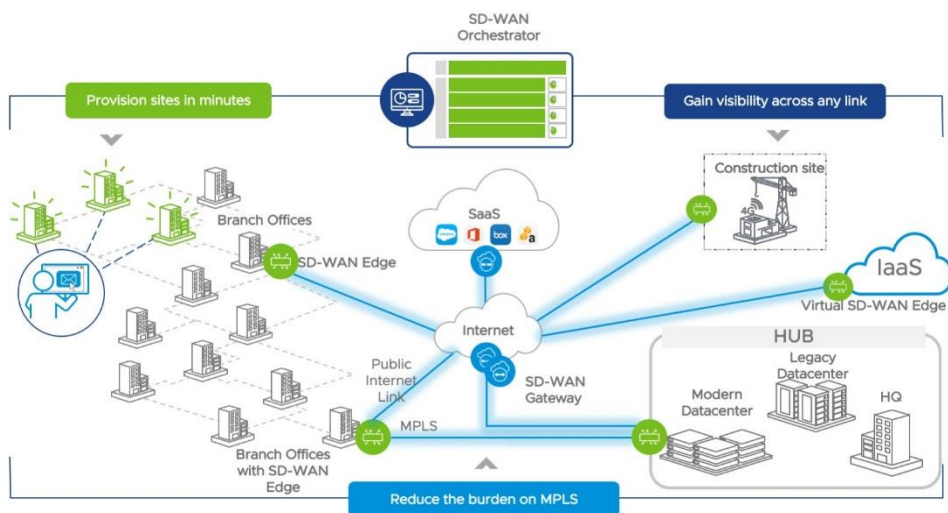


Figure 5: Second-generation WAN transformation toward SD-WAN

### Third generation WAN transformation: Modern multi-cloud

As enterprises move into the third generation, embracing and leveraging multiple cloud providers, they must invest in a network that provides seamless cloud infrastructure connectivity. Business drivers, including a dramatic increase in remote workforce demands, have accelerated the urgency and adoption of new technologies. The corporate perimeter continues to dissolve as applications are moving to the cloud and can be accessed from anywhere. As the complexities of connectivity and security continue to grow, it is essential to bring technologies and solutions together to deliver seamless access to end users.

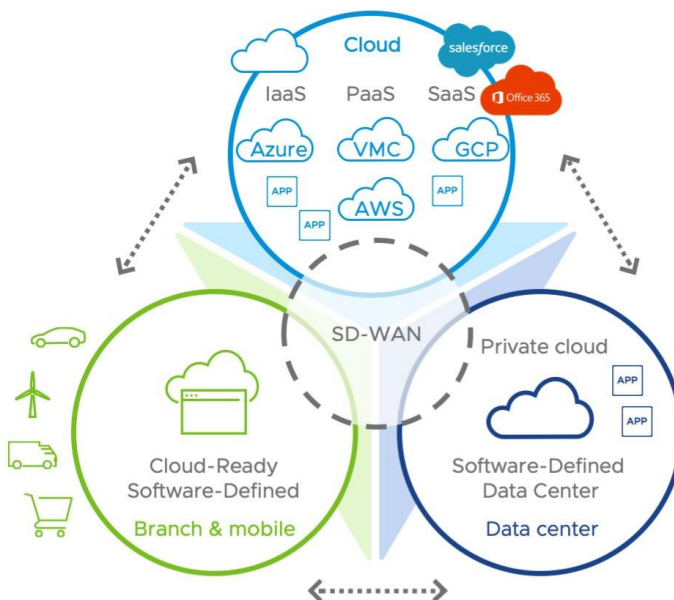


Figure 6: Third-generation WAN transformation toward multi-cloud

SD-WAN solutions are expanding to address multi-cloud connectivity demands. 5G is proving viable for WAN connectivity. Automation and AI are delivering self-healing networks. Vendors are unifying and simplifying end-to-end management with intrinsic security and Zero Trust network architectures.

With applications operating in a multi-cloud world, businesses must establish tight integration with the public cloud infrastructure. APIs are the preferred model to deliver an enhanced cloud experience and ensure cross-cloud compatibility. Cloud offerings such as infrastructure-as-a-service and software-as-a-service can be effectively implemented through specific API integrations with cloud provider platforms (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform).

**Infrastructure-as-a-service:** Through API integration, enterprises establish automated connectivity to the cloud to reach workloads directly from the data center or branch locations (e.g., AWS Transit Gateway, Microsoft Azure Virtual WAN). WAN edge instances are automatically deployed in the public cloud and become part of the SD-WAN overlay, establishing data plane connectivity to the existing data center and branch infrastructure.

This, in turn, pushes full SD-WAN capabilities into the cloud and establishes a common policy framework across the enterprise environment. This architecture eliminates the need for traffic from SD-WAN sites to traverse the data center, improving the performance of the public cloud applications. It uses path redundancy across commodity connectivity to deliver high availability in a cost-effective model.

**Software-as-a-service:** Branches have traditionally accessed SaaS applications through centralized data centers. This led to increased application latency and unpredictable user experience. As SD-WAN has evolved, enterprises have established direct branch-to-cloud connectivity and access through regional gateways or colocation sites. This approach creates a lack of visibility and performance of SaaS applications from remote sites. In turn, it is challenging to identify the best path for SaaS applications and deliver an optimal end-user experience.

Additionally, when network changes or link impairments occur, there is no easy way to move affected applications to an alternate path. An integrated API infrastructure allows enterprise customers to quickly and easily configure access to SaaS applications. This can be done directly from the branch or through gateway locations. By continuously measuring and monitoring each path's performance to SaaS application and choosing the best-performing path based on loss and delay, traffic can be dynamically and intelligently moved to an alternate, higher-quality path.

## SD-WAN transformation

SD-WAN was developed to simplify and transform networks by making them more responsive, scalable, and cost-effective.

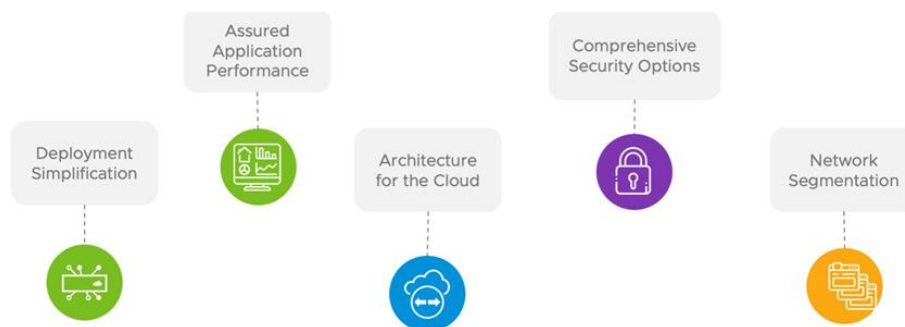


Figure 7: Five ways your networks need to evolve using VMware SD-WAN

## VMware SD-WAN cloud-delivered model

VMware SD-WAN™ simplifies WAN deployment with a cloud-delivered model. The solution is built on three components:

- The **VMware SD-WAN Edge** is deployed in branch or work-from-home locations. It provides WAN connectivity and replaces the branch office router. SD-WAN Edges are also installed at data center sites and configured as hubs. An SD-WAN Edge can be deployed as physical hardware, a virtual appliance, or instantiated from a cloud provider marketplace. The Edge provides SD-WAN data plane functionality.
- **VMware SD-WAN Gateways** are hosted in points of presence (PoPs) around the globe. Traffic is sent to the Gateways and then routed to the destination, which may be a corporate data center hub, cloud provider, or a SaaS application.
- The **VMware SD-WAN Orchestrator** is a cloud-hosted centralized management system. The Orchestrator is not customer-installed; it is a VMware-managed system that is available for direct customer connection. The Orchestrator operates across the SD-WAN management plane.

The components are delivered as a subscription service with the management and cloud interconnect gateways hosted in the cloud. The service is also available with all three components on the customer premises.

The VMware SD-WAN solution is strategically designed as a transport-independent overlay that can work across any circuits to connect branch locations to applications. It enables connectivity to enterprise data centers, SaaS applications, and IaaS in the cloud, dynamically optimizing traffic over multiple links.

## Deployment simplification

A VMware SD-WAN deployment starts with the deployment of a VMware SD-WAN Edge device at a location (e.g., branch office) and a larger Edge device, called the hub, in the data center. The SD-WAN Edge simplifies site deployment, enabling quick and efficient network expansion to new sites.

Edge devices are available as a hardware appliance, as a virtual appliance that can run on common hardware, or as a virtual instance on universal customer premises equipment (UCPE)—i.e., third-party off-the-shelf hardware—from various vendors. They are also available for cloud deployments and can be procured from providers for deployment in their respective clouds.

The Edge device connects a site to the service provider's WAN, routing through to the Internet to connect to an application's location—enterprise data center, service provider, or cloud. A smaller device at the remote location communicates with the larger hub device in the data center. The hub devices aggregate connections from all the Edge devices.

Edge devices communicate with each other to optimize the traffic flow. These devices are automatically configured via profiles from the VMware Orchestrator, so they are quick and easy to install. Their deployment cost is much lower than typical routers that must be configured manually, device-by-device.

Figure 8 depicts high-level deployment for VMware SD-WAN Edge devices in branches, data centers, and multiple verticals like construction sites, kiosks, and retail stores.

Deployment across this wide variety of environments remains rapid and efficient due to the zero-touch provisioning capabilities of the SD-WAN Edge.



Figure 8: VMware SD-WAN Edge simplifies site deployment

### Multiple deployment options

Edge devices offer flexible deployment options. There are three deployment choices for an Edge in branch offices:

- Coexist with the existing deployed switch or router to support existing network connections.
- Become the default device and provide failover capabilities to the branch using Virtual Router Redundancy Protocol (VRRP). The Edge can coexist at Layer 3 and use routing protocols such as border gateway protocol (BGP) or open shortest path first (OSPF) to support failover.
- Replace the existing router and firewall. Elimination of devices can lead to greater cost savings. VMware SD-WAN Edges are provided on a subscription basis rather than requiring the purchase of new hardware.

Enterprises can deploy SD-WAN on their choice of vendor appliances. Alternately they can choose to deploy the VMware SD-WAN Edge as a virtual network function (VNF) and choose from a list of tested and approved vendor appliances. APIs and SDKs support integration with a list of partner virtual customer premises equipment (CPE) management systems.

### Zero-touch provisioning

In a traditional WAN router deployment, each router needs to be individually configured by a network engineer through a command-line interface (CLI). This task is time-consuming and error prone. To make the deployment simple and scalable, VMware SD-WAN offers zero-touch provisioning to facilitate the deployment of the SD-WAN Edge. The goal of the activation is to allow an SD-WAN Edge to be registered to the SD-WAN Orchestrator so that any further device operations are centrally managed by the Orchestrator. The SD-WAN Orchestrator does not require the engineer to log in to the SD-WAN Edge individually for configuration and monitoring.

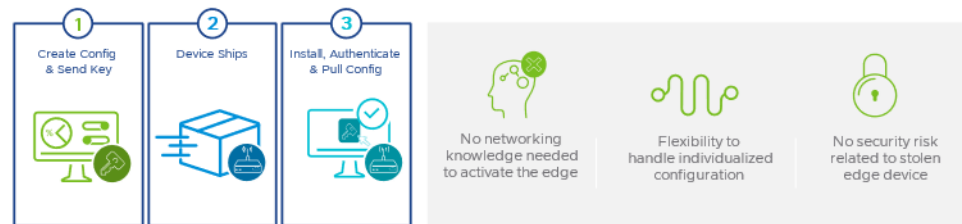


Figure 9: Simplified day 0-1 operations with VMware SD-WAN

## Assured application performance

VMware SD-WAN increases the performance of applications over the WAN with real-time remediation and traffic steering. The VMware SD-WAN Edge bonds multiple links and virtualizes them to act as one. If an existing link does not have enough throughput, a second link can be added to increase bandwidth without changing anything in the network.

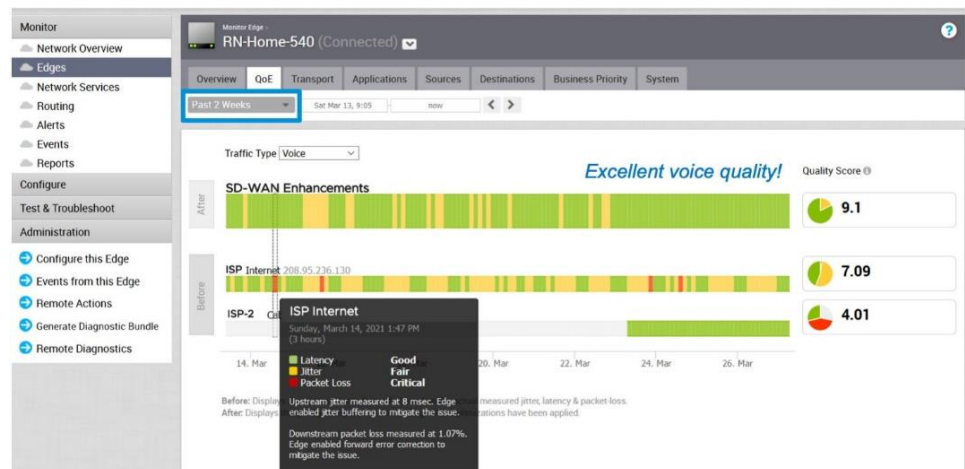


Figure 10: VMware SD-WAN Quality of Experience (QoE) score

VMware SD-WAN supports combining links of different types (e.g., broadband Internet with MPLS), enhancing options for connecting a branch site to the corporate data center. If there is a quality issue on one of the links, the Edge device immediately steers traffic to the other link. This ensures that the performance is never compromised, even if the links are of varying quality. With this arrangement, enterprises can increase throughput while reducing the cost per unit of throughput and still maintain the reliability of connections.

## Business policy and smart defaults

VMware SD-WAN performs application-aware, per-packet steering based on business policy configurations and real-time link conditions. The business policy contains out-of-the-box smart defaults that specify the default steering behavior and priority of more than 3,000 applications.

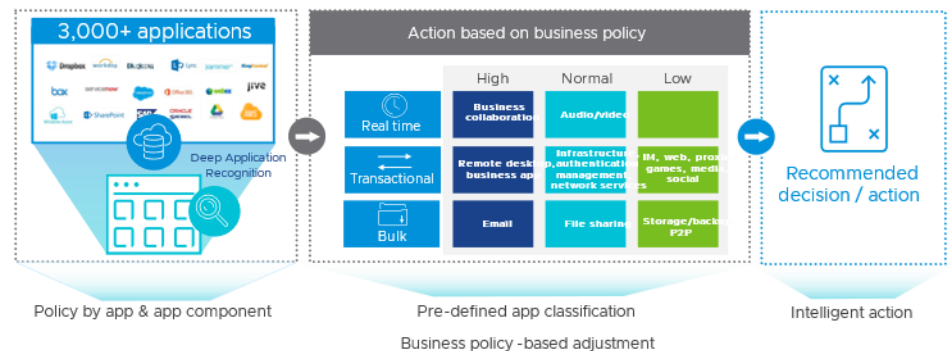


Figure 11: Smart application policies enable flexible and easy policy-based customization of app priorities

Dynamic packet steering and application-aware prioritization can be used immediately without having to define policies. Figure 12 shows an example of a business policy.

The screenshot shows the "Configure Rule" window with the following settings:

- Rule Name:** Rule Name
- Match:**
  - Source: Any
  - Destination: Any
  - Application: Any
- Action:**
  - Priority: Normal (selected)
  - Rate Limit: ☐
  - Network Service: Multi-Path (selected)
  - Link Steering: Auto (selected)
  - Inner Packet DSCP Tag: Leave as is
  - Outer Packet DSCP Tag: 0 - CS0/DF
  - NAT: Disabled
  - Service Class: Transactional (selected)

Buttons for "OK" and "Cancel" are at the bottom right.

Figure 12: VMware SD-WAN business policy example

Each application is assigned a category. Each category has a default action, which is a combination of traffic class (priority and service class), network service, and link steering. In addition to the default application list, customer applications can be defined manually.

### Dynamic Multipath Optimization

Dynamic Multipath Optimization™ (DMPO) provides continuous real-time link monitoring on a per-packet basis. If a link experiences packet loss, latency, or jitter, DMPO moves traffic to the best available link.





Figure 13: VMware SD-WAN Dynamic Multipath Optimization

DMPO enables sub-second failover response to any connectivity degradation (e.g., packet loss, jitter, latency) or connectivity failure (e.g., link failure) condition. In the event customers have a single link or all the links experience brownout conditions, DMPO initiates forward error correction (FEC) and remediates the degraded condition.

### Network visibility and agile troubleshooting

The VMware SD-WAN Orchestrator makes it easy to monitor Edge devices and the performance of applications on the network, providing visibility across the entire WAN. The Orchestrator can save hours of time normally spent on device management because it can configure all devices from the central console using defined policies.

VMware SD-WAN comes with smart default for business application traffic. The VMware SD-WAN Orchestrator is used to set policies for the prioritization of applications on the network to make sure that the most important applications get the top priority. The Orchestrator provides a dashboard to monitor the performance of network connections and applications, gaining firsthand benefits of VMware SD-WAN.

The application monitoring features in the VMware SD-WAN Orchestrator allow IT organizations to quickly troubleshoot and resolve issues and, in turn, prevent poor application performance and downtime.

### Architecture for the cloud

A significant benefit of the VMware SD-WAN solution is high-performance access to applications in the cloud and IaaS services. This is accomplished by connecting branch locations directly to the cloud through a VMware SD-WAN Gateway. These Gateways are hosted by VMware in points of presence (PoPs) close to the target application/IaaS. The VMware SD-WAN Gateway optimizes connectivity to the Edge device in the branch office location; no matter where the application resides, it provides a high-quality network connection with consistent policy across the enterprise.

Customers do not need to own or manage these Gateways. They are hosted by VMware and provided as a service as part of a subscription. There are two options available for connecting into the SD-WAN environment:

- Connect over the Internet using IPsec tunnels for a secure connection without any SD-WAN. The connection between the branch Edge device and the VMware SD-WAN Gateway is always optimized.
- Connect using SD-WAN and connect with a virtual Edge instance in the cloud. The virtual Edge is available from cloud marketplaces such as AWS and Azure.

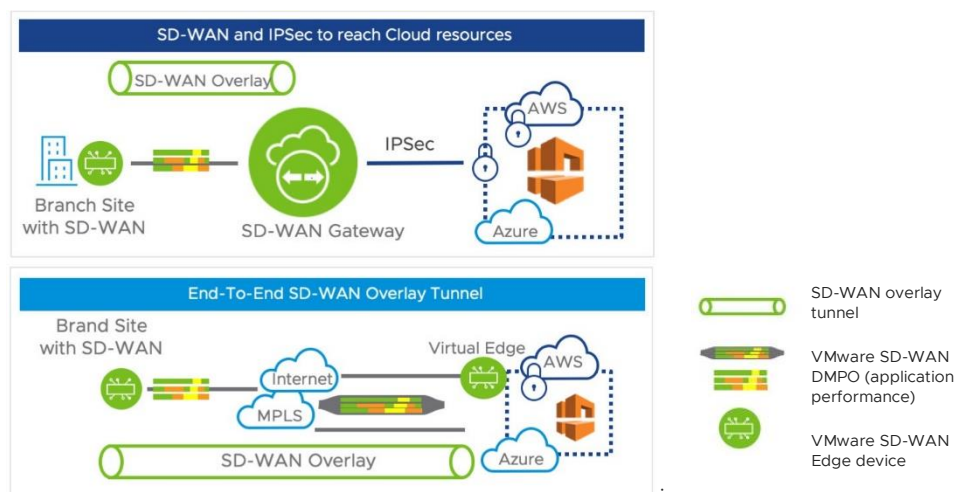


Figure 14: VMware SD-WAN connectivity to cloud

## Network security

Security is a critical component of enterprise networks. The SD-WAN Edge has several built-in security functions, including a firewall, network segmentation, and the ability to run third-party security functions as VNFs. This functionality provides options to reduce the attack surface and minimize breaches. It also reduces costs and allows the flexibility to choose solutions from alternate security vendors. Customers can combine all these functions with existing on-premises security devices (e.g., firewall, IPS/IDS, secure web gateway) and cloud web security solutions to build a comprehensive, network-wide—and cloud-inclusive—security solution.

## Distributed services insertion via service chaining

Security services can also be built by automating and service chaining capabilities. Service chaining can be implemented to direct traffic to cloud-hosted security services. Service chaining can provide any type of protection, including website URL filtering or firewalling. It automates tunneling, eliminating the need for site-by-site configurations. It also offers single-click, application-aware policies for service insertion. Using this method helps secure traffic going over the Internet.

## Network segmentation

Network security is not complete without the ability to isolate critical data traffic. Segmentation is the process of dividing the network into logical sub-networks using isolation techniques on a forwarding device such as a switch, router, or firewall. Network segmentation is essential when traffic from different organizations and/or data types must be isolated.

Segment-aware policies allow for rules to be set so specific traffic can be isolated, such as isolating guest Wi-Fi traffic or point-of-sale system data for better data integrity. Enterprises can configure a single physical network with multiple segments to address the need where a specific department in a company requires secure application access. Segmentation can be used to aid onboarding during mergers where IT wants to avoid overlapping IP addresses. Network services such as QoS and firewall policies can also be set per segment.

There are many use cases for segmentation:

- Line of business separation by departments for security/audit

- User data separation: guest, payment card information (PCI) data, employee traffic
- Enterprise uses overlapping IP addresses for different groups
- Carrying segmentation to VPNs for connecting off-network sites

Network segmentation is essential when traffic from different customers and/or business entities must be isolated from each other. Full support for segmentation includes the isolation of management, control, and data plane traffic. For instance, VMware SD-WAN provides a simple configuration for segmentation across the WAN. Segmentation can be enforced by an organization by data type and location. Organizations can isolate guest and employee-facing applications. Payment card data can be isolated for PCI audit compliance. Overlapping IP addresses can be provisioned to support acquired organizations.



**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [vmware.com](http://vmware.com) Copyright © 2021 VMware, Inc.  
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at [vmware.com/go/patents](http://vmware.com/go/patents). VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: SD-WAN-989-SD-WAN-Networking-Foundation-wp-0921