Enterprise WAN Simplicity, Performance and Security with VMware SD-WAN

vmware®

SD-WAN™

VMware SD-WAN increases agility and cost effectiveness, while assuring application performance and network security of corporate sites across the WAN.

The WAN is transitioning as enterprises seek to improve agility and economics and adapt to the shift of applications to the cloud. VMware SD-WAN™ offers enterprise-grade performance, security, visibility, and control over both the public Internet and private networks. VMware SD-WAN significantly simplifies the WAN with zero-touch deployment, one-click business policy, enhanced firewall service, easy service insertion, and cloud-based network-as-a-service. The result is a better-performing WAN with increased reliability and lower cost of ownership, with enhanced security for branch and remote users.

Today's branch office users are consuming more Wide Area Network (WAN) bandwidth as they collaborate online (for example, Zoom, WebEx, and Microsoft 365), consume Software-as-a-Service (SaaS) and cloud services, access large rich-media files, and use other bandwidth-intensive applications. Corporate IT faces significant challenges due to the architectural complexity, lack of security, and cost concerns of their existing WAN.

Most branch office WAN traffic is carried over expensive leased lines (such as private MPLS circuits) or unpredictable, unsafe Internet connections (such as DSL, cable, and LTE)—neither is ideal on its own. Deploying leased lines to satisfy bandwidth needs is cost-prohibitive and time-consuming. Using the public Internet might result in a poor user experience due to its lack of stability and protection against cyber-attacks. Moreover, legacy WAN has many inherent security concerns.

VMware SD-WAN enables enterprises to support application growth, simplified branch implementations, network and workforce agility, and enhanced network security. While delivering optimized access to cloud services, private data centers, and enterprise applications simultaneously over various types of transport, VMware SD-WAN also reduces cyber-attack risks with an enhanced firewall service, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), hosted firewall logging, and more—all under a single, unified management portal.

Challenges with branch office WAN

WAN technologies used in most branch offices today have changed little, if at all, in the last couple of decades. They were originally designed for applications in private, on-premises data centers. Today, the traditional branch office WAN architecture faces many networking and security challenges. Some common ones include:

- MPLS typically provides high-quality service but with the tradeoff of limited capacity, higher cost, and long deployment lead times. Branch offices with only private-circuit connections rely on backhauling all cloud applications, SaaS, and Internet traffic through the enterprise data center, adding latency, degrading application performance, and driving up network bandwidth costs. Traditional hub-and-spoke WAN architecture might not support cloud migration.
- Broadband provides fast deployments and greater capacity but can lack reliability, security, and assured performance, causing poor user experience.
- Traditional branch office networks lack centralized management, control, visibility, and protection from cyber-attacks. Too much management tool variety can make it difficult to troubleshoot or respond to threats quickly.
- Compliance requirements (such as PCI, HIPAA, GDPR, and more) can be difficult to maintain across multiple branch offices due to different security solutions from different vendors.

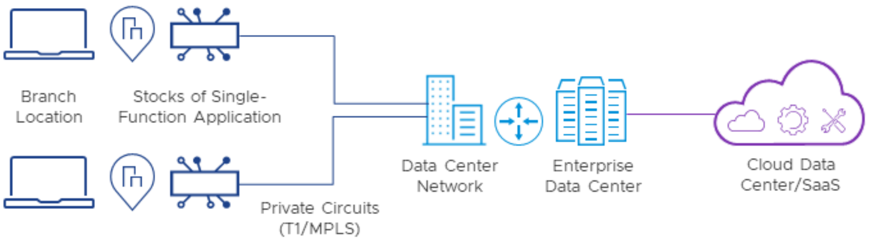

Figure 1: Traditional branch office WAN

VMware SD-WAN overview

VMware SD-WAN improves upon the economics and flexibility of a hybrid WAN with the deployment speed and low maintenance of a cloud-based service. It includes policy-based, network-wide application performance, visibility and control while dramatically simplifying the WAN by delivering virtualized services from the cloud to branch offices.

The VMware SD-WAN Edge appliance is a compact, thin edge device that is zero-touch provisioned from the cloud for secure, optimized connectivity to applications and data. The VMware SD-WAN Edge is also available as a virtual network function (VNF) for instantiation on a customer premises equipment (CPE) platform for great deployment flexibility.

The VMware SD-WAN Edge uses Dynamic Multipath Optimization™ (DMPO) and deep application recognition to improve delivery reliability. It aggregates multiple links (such as private line, cable, DSL, 4G-LTE or 5G, satellite) and steers traffic over the optimal links to other on-premises VMware SD-WAN Edges in branch offices, private data centers, campuses, and headquarters. The VMware SD-WAN Edge can also optionally connect to the system of global VMware SD-WAN Gateways to provide performance, security and visibility for cloud services (SaaS, IaaS, B2B Internet).

The Edge's built-in Enhanced Firewall Service—based on VMware's NSX Security technology—further strengthens SD-WAN branch security. By combining the power of NSX security with VMware SD-WAN Edge platforms, customers can eliminate legacy firewalls at the branch without sacrificing security and benefiting from the simplified network and security operations, all while taking advantage of VMware's investment in threat intelligence.

The system of VMware SD-WAN Gateways is deployed globally at top-tier cloud data centers to provide scalable and on-demand cloud network services. VMware SD-WAN Gateways implement VMware DMPO, cloud VPN and VMware Multisource Inbound Quality of Service (QoS) between global cloud services (SaaS, IaaS, network services) and each VMware SD-WAN Edge, enabling multiple broadband and private leased lines to appear as a single, high-performance WAN. The cloud-based VMware Edge Cloud Orchestrator is used to provision network-wide business policy, enable services insertion, perform real-time monitoring, and analyze application performance.

Deploy in minutes

Using VMware's zero touch deployment capability, VMware SD-WAN Edge installs quickly. The Edge is shipped to the branch office where a non-technical person simply plugs in power and a network cable. Activation, configuration, and ongoing management are all handled from the cloud.

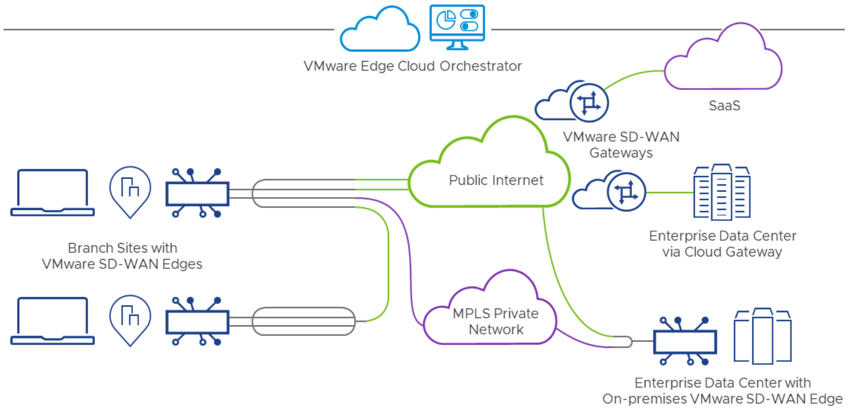
VMware Edge Cloud Orchestrator
SaaS
VMware SD-WAN Gateways
Public Internet
Branch Sites with VMware SD-WAN Edges
Enterprise Data Center via Cloud Gateway
MPLS Private Network
Enterprise Data Center with On-premises VMware SD-WAN Edge

Figure 2: VMware SD-WAN service

Enterprise-wide business policies

VMware SD-WAN makes setting policy as simple as a single click. Enterprises or their managed service providers can define business level policies that apply enterprise-wide across many Edges, all through a centralized, cloud-based Orchestrator. Link steering, link remediation, and QoS are all applied automatically based on set business policies; however, specific configuration overrides may also be applied. The centralized VMware Edge Cloud Orchestrator also provides an enterprise-wide view and configurability of routing in an overlay flow control table, eliminating complex node-by-node route configurations.

Assured application performance

VMware SD-WAN boosts the service level and capacity of hybrid networks or of standard broadband Internet links by implementing its unique DMPO. This includes several technologies.

Continuous monitoring

WAN circuits are automatically profiled, enabling zero touch deployments without manual, site-by-site adjustments of configuration parameters. Continuous monitoring of link and path quality and available capacity provide real-time feedback for dynamic optimization.

Dynamic application steering

Applications are automatically recognized and steered to the optimal link(s) based on business priority, built-in knowledge of application network requirements, and real-time link performance and capacity metrics. Dynamic per-packet steering can move a session, for example a voice call, mid-stream to avoid link degradation without any call drop or voice quality glitch. Single, high bandwidth flows can utilize aggregated bandwidth for faster response times.

On-demand remediation

Remediation, including error correction, jitter buffering, and local re-transmits are applied on-demand when only a single link is available or concurrent link degradations cannot be steered around. Remediation is only applied for priority applications that are network-sensitive and only when dim-out link degradations occur.

Quality of experience

The SD-WAN overlay with DMPO enables an application-specific quality of experience. Application performance is assured, delivering a high quality and capacity WAN through a virtual overlay across multiple links, including private and Internet broadband.

Unified and robust security

VMware SD-WAN provides unified, secure communications, regardless of the underlying transport type. Standard IPsec encryption is provided end-to-end between branches and data centers and for inter-branch communications. The unique, cloud-delivered architecture also provides automatic VPN from branches to cloud gateway aggregation points for interoperable access to IaaS, eliminating manual, two-sided tunnel setup from 1XN branches to 1XN cloud data centers. The solution provides the scalability and robust security of public key infrastructure (PKI) with the consolidated management of an integrated certificate server, secure onboarding of devices, and revocation management. Risk is minimized by pinning certificates to specific devices and using unique pair-wise encryption keys.

VMware’s SD-WAN solution has important security features built into the Edge's data plane. In addition to the stateful firewall, it offers other features such as traffic segmentation, intrusion detection and prevention (IDS/IPS), hosted firewall logging, and more. The Enhanced Firewall Service running on the Edge device improves overall branch network security by detecting unauthorized access to corporate network assets, mitigating threats, and defending against cyber-attacks. Today's distributed enterprises greatly benefit from Enhanced Firewall Service for user traffic protection, consolidated hardware, simple and unified management, reduced operational overhead, and overall cost saving. The Enhanced Firewall Service built into VMware SD-WAN is crucial to an enterprise's digital transformation initiatives.

One-click service delivery

The VMware SD-WAN solution simplifies the deployment of services at the branch, at more consolidated enterprise service hubs, and to the cloud, eliminating the need for many single-function devices in the branch. One-click service provisioning activates multiple VMware native services and third-party VNFs from technology partners on the branch edge. One-click business policies can service chain traffic from branches to both enterprise service hubs and cloud services easily and with application-level granularity.

SIEM integration for better security at the Edge

VMware SD-WAN integrates with major SIEM (Security Information and Event Management) providers, such as IBM QRadar, to better protect customers with improved security posture, timely detection of threats, proactive protection, and compliance with industry regulations. SIEM collects, analyzes, and correlates security data from various sources, such as logs, network traffic, and security alerts. Organizations gain visibility into user traffic, detect threats or malicious activity timely, and take responsive actions accordingly.

VMware SD-WAN components

VMware SD-WAN Edges provide zero-touch SD-WAN deployments in branches, and scalable on-premises hub deployments for headquarters and data center locations.

Additionally, all the benefits of SD-WAN, namely assured performance, security, and policy control are available directly at the doorstep of cloud SaaS and IaaS locations through VMware Gateways. The cloud-based VMware Edge Cloud Orchestrator provides enterprise-wide business policy, configuration, troubleshooting and at-a-glance monitoring.

VMware SD-WAN Edge

VMware SD-WAN Edges are available as easy to install appliances for remote branches with a range of throughput, ports for WAN and LAN connectivity, integrated wireless LAN, and security firewall services. Dynamic routing enables policy-based overlay insertion for both in-line and out-of-path deployments. High Availability (HA) setup provides redundancy and failover. In addition to appliance options, the VMware SD-WAN Edge is available as VNF software for deployment on standard x86 servers, including virtual CPE devices. The Enhanced Firewall Service protects corporate SD-WAN branch sites against unauthorized access to internal network assets. With the built-in advanced security features (such as application-aware and session-aware firewall, IDS/IPS, hosted firewall logging, and more), the Enhanced Firewall Service proactively defends against various cyber-attacks and mitigates threats that could potentially cause serious breaches.

VMware SD-WAN Gateway

Multitenant VMware SD-WAN Gateways are deployed by VMware and its partners at top-tier network points of presence (PoPs) and cloud data centers around the world for the full range of SD-WAN benefits. VMware SD-WAN Gateways provide a scalable and distributed infrastructure with the advantages of hosted, network-as-a-service flexibility. VMware SD-WAN Gateways provide the ideal architecture for optimized access to cloud applications and data centers, as well as access to private network backbones and legacy enterprise sites.

VMware Edge Cloud Orchestrator

The VMware Edge Cloud Orchestrator is a cloud-hosted (or on-premises) central management tool for all VMware SASE components: VMware SD-WAN, VMware Secure Access, VMware Cloud Web Security, and VMware Edge Network Intelligence. Its web-based user interface (UI) provides simplified configuration, provisioning, monitoring, fault management, logging, and reporting functions. VMware Edge Cloud Orchestrator enables flexible implementation of business-based policies for application delivery and traffic management.

Secure SDN for the WAN

VMware SD-WAN brings the software-defined network (SDN) concept to the enterprise branch WAN. VMware's software-based approach enables the flexibility and portability of deploying virtual SD-WAN Edges on off-the-shelf x86-based hardware or as VNFs on virtual CPEs.

Business policies implemented across the logical overlay deliver abstraction of application flows from the underlying physical transport. Agility is achieved based on adjusting forwarding to meet policy and real-time link conditions. SD-WAN has a distributed control plane for forwarding decisions to be made locally with context, so there are no latency issues or points of failure across the WAN. Each SD-WAN node receives centralized control policies for easy programmability and enterprise-wide visibility. Security policies are centrally configured from VMware Edge Cloud Orchestrator UI and enforced at Edge devices at branches. Management can be performed using GUI or REST API.

VMware SD-WAN and VMware Secure Access Service Edge (SASE)

VMware SD-WAN is a component of the overall VMware SASE solution, which converges cloud-hosted SD-WAN networking and advanced security services. VMware SASE, architected to leverage the power of the cloud while minimizing complexity at the edge, is an easy-to-consume platform that enables a unified edge and cloud service model with a single unified portal to manage business policy, security, configuration, and monitoring.

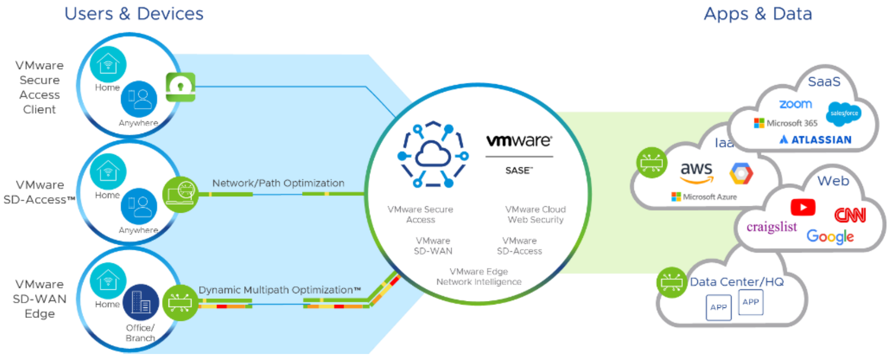

Figure 3: VMware SASE

Learn more

- VMware SD-WAN, *sase.vmware.com/sd-wan*
- VMware SASE, *sase.vmware.com*

VMware SD-Access™ is a cloud-managed, secure, and high-performance remote access solution for today's distributed enterprise workforce. Based on zero trust network access (ZTNA) and optimized for speed, VMware SD-Access ensures application quality and keeps remote workers protected and highly productive. This cloud-managed, scalable client service is set up in minutes. It replaces inflexible VPN infrastructure and delivers a high-performance, private network fabric between servers, clouds, and remote workers' desktops or mobile devices without requiring an SD-WAN Edge appliance. User traffic paths are optimized, avoiding "hairpinning." VMware SD-WAN Client significantly reduces IT's capital and operational expenses while extending the SD-WAN experience to users traveling or working at remote locations.

Remote and mobile workers who require optimal and secure cloud application access can utilize **VMware Secure Access™**. Bringing off-premises users into the VMware fabric enables remote users to access cloud-based applications that are optimized for delivery and performance, leveraging zero trust network access (ZTNA) and the benefits of a cloud-hosted solution. VMware Secure Access eases IT deployment and maintenance of costly virtual private network (VPN) services.

VMware Cloud Web Security™ offers IT teams visibility and control when users access SaaS applications and ensures compliance. It also includes URL filtering which helps IT control the web sites employees can or cannot access. IT can also reduce the attack surface with content filtering by determining what type of content users can or cannot access or upload. Content is inspected for malware attacks from known viruses using up to date threat intelligence. The solution protects against zero-day malware with sandbox support where the content is inspected in a contained environment.

VMware Edge Network Intelligence™ is an AIOps solution that gives IT true visibility and analytics for the IoT and end user devices on their network. IT can gain visibility into networks they don't control, such as home networks of remote users. This proven, vendor-agnostic solution provides a rich client experience for employees working from anywhere, and helps IT shift their time away from chasing root causes to proactive remediation.

Item No: sdwan-564-Enterprise-WAN-Agility-so-0321