Cloud Delivered Simplifies SD-WAN

VMware SD-WAN™ by VeloCloud®
brings users closer to the cloud

Cloud delivered VMware SD-WAN simplifies WAN deployment

As the growth of software-defined wide area network (SD-WAN) continues, organizations look for solutions that are easy to deploy and manage. VMware SD-WAN simplifies wide area network (WAN) deployment with a cloud delivered model. The major components of VMware SD-WAN are delivered as a service for a subscription with the main components hosted in the cloud. The VMware SD-WAN solution is built on three components.

The **VMware SD-WAN Edge** device is placed in the branch office. It can terminate multiple WAN connections and steer traffic over them for the best performance and reliability. The VMware SD-WAN Edge device provides support for routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP), along with static routing, with an IP service-level agreement (SLA). It can replace the legacy router and reduce the number of networking devices in the branch office.

The **VMware SD-WAN Gateways** are hosted in points of presence (PoPs) around the world. Traffic is sent to the VMware SD-WAN Gateways and they route traffic to the destination, which could be a cloud data center or the corporate data center. The VMware SD-WAN Gateways perform optimizations between them and the VMware SD-WAN Edge devices. The VMware SD-WAN Gateways bring the users' connections closer to the cloud for better performance.

The **VMware SD-WAN Orchestrator** is a cloud hosted centralized management system. The VMware SD-WAN Edge devices connect to the VMware SD-WAN Orchestrator and download their configurations from it. The VMware SD-WAN Orchestrator is used to manage the VMware SD-WAN Edge devices, provide visibility into application performance, and aid in troubleshooting. It's not necessary to install it or manage—it is hosted and managed by VMware and by select service providers.

VMware SD-WAN Edge simplifies site deployment

Expand your network to new sites and branches quickly and efficiently

A VMware SD-WAN deployment starts with placing a VMware SD-WAN Edge device at each location, such as a branch office, and a larger device in the data center to act as a hub. The hub devices aggregate connections from the VMware SD-WAN Edge devices. The VMware SD-WAN Edge device connects remote sites to the service provider's WAN and to the Internet.

Traffic connects through VMware SD-WAN Gateways to the applications, in data centers, or hosted at service providers or in the cloud. The VMware SD-WAN Edge and the VMware SD-WAN Gateway communicate with each other to deliver optimization between them. This model delivers optimization close to the cloud and connects to cloud hosted applications without having to backhaul over private links to the corporate data center.

vmware®

The VMware SD-WAN Edge devices are auto configured, so it's quick and easy to install them. The cost to deploy the VMware SD-WAN Edge devices will be much lower than with a typical router that must be configured manually device-by-device. The VMware SD-WAN Edge devices provide functions to make access to applications perform better. VMware SD-WAN Edges are gatekeepers of policy.

VMware SD-WAN Edge devices:

• Determine best route

• Communicates Dynamic Host Configuration Protocol (DHCP) Server

• Support OSPF-BGP

• Apply business policies

• Are high availability capable

• Replace traditional routers

VMware SD-WAN Edges are available as easy to install appliances for remote branches with a range of throughput, ports for WAN and local-area network (LAN) connectivity and integrated wireless LAN. Dynamic routing enables policy-based overlay insertion for both in-line and out-of-path deployments. High availability deployments are also supported.

VMware SD-WAN Edge devices are available as physical appliances, and as virtual network function (VNF) software for deployment on standard x86 servers, including virtual customer premises equipment (CPE) devices. VMware SD-WAN Edges are currently available as a virtual appliance on the popular cloud platforms, including Amazon Web Services (AWS) and Azure Cloud, Google Cloud, and Alibaba Cloud marketplaces with bring your own license (BYOL).

VMware SD-WAN delivers optimized access to the cloud

Assured application performance over any type of link

VMware SD-WAN is a transport independent overlay that can work across any combination of circuits. It can dynamically optimize traffic over multiple links. It enables connectivity to both enterprise data centers, software as a service (SaaS) applications, and the cloud. VMware SD-WAN can be used to connect to the Internet for direct access to applications in the cloud without backhaul to the data center.

Often organizations are paying for dual links, but the second link is just used for backup. Organizations can't take advantage of dual links in an active/active mode because they don't have a way to manage traffic over both links. Managing dual links is possible with SD-WAN. SD-WAN can aggregate bandwidth over both links to get more throughput and reliability for remote locations.

Dynamic link remediation ensures WAN performance

VMware SD-WAN provides continuous link monitoring. As it detects congestion, it moves traffic to the best link. It performs traffic steering packet by packet over both links at the same time, so there isn't a wait for a total failure for the switch over to happen or a wait for routes to reconverge, which is what happens with a legacy router.

If both links are experiencing congestion, the system will send duplicate packets in real time over both links to ensure that they get through. This means that VMware SD-WAN can deliver a quality user experience over sub-optimal link conditions, such as when directly connecting to the Internet for access to the cloud.

Routing is based on link conditions and performance by application

Routing is based on a combination of link conditions and application performance. The VMware SD-WAN solution has a built-in deep application recognition (DAR) engine, which identifies and classifies application traffic traversing all the WAN links and provides the ability, through the business policy framework, to set policies for each application or category of application.

The VMware SD-WAN solution was designed to reduce the complexity and time needed to configure and maintain the WAN network configurations. It does this by leveraging a single management system called the VMware SD-WAN Orchestrator, as well as RESTful application programming interfaces (APIs).

Reacting to change is critical and the goal is to act on change without intervention. This is achieved with the VMware SD-WAN Dynamic Multipath Optimization™ (DMPO) feature which is a per-packet technology. With DMPO, the steering capabilities take place while an application flow is being established. DMPO can move application flows, by configured policy, to better performing links while maintaining session persistence.

The policies operate at Layer 7 (application layer) and utilize the built-in DAR engine to recognize and classify over 3000 applications to which simple policies can be applied. While steering decisions are made based on variations in link conditions, each application is treated individually and has pre-configured performance objectives for which it seeks a combination of links to transport the flows.

Enforce traffic steering based on application reachability

VMware SD-WAN always provides multiple paths to a given destination and can detect failures and quality degradations within these paths. All application forwarding decisions (leveraging the business policy rules from a profile) are performed at the VMware SD-WAN Edge based on the link conditions in real time, when any WAN anomaly is detected.

Since the solution is per-packet, traffic can be steered dynamically within sub-seconds, causing minimal application impact. The steering is also carried out based on application groupings. Where the policies would change depends upon the application categorization being high priority/real time compared to low priority/transactional.

Traffic is intelligently forwarded based on type and destination

The VMware SD-WAN solution provides a varied set of redundant forwarding paths, which can be based on the application type plus the real time changes in link conditions. Traffic from VMware SD-WAN Edges can be steered to another VMware SD-WAN Edge within a data center (hub site) or to another branch VMware SD-WAN Edge using dynamic branch-to-branch tunnels.

If the customer is accessing SaaS applications, VMware SD-WAN Gateways are the best paths since these VMware SD-WAN Gateways are located at major geographic PoP locations around the world. They provide low latency access to the SaaS destination. These VMware SD-WAN Gateway PoPs are available through service providers but also directly from VMware.

A customer can always access all global PoPs and will be automatically assigned VMware SD-WAN Gateways based on geographic location, capacity and traffic destination. A VMware SD-WAN Edge will only connect to PoPs as needed to deliver traffic to its destination. VMware SD-WAN Gateways are not required, and traffic can flow from a VMware SD-WAN Edge to a hub in the data center.

Simplified WAN management for all your devices

Multitenant management platform eases deployment

The VMware SD-WAN Orchestrator provides centralized enterprise-wide configuration, management and real time monitoring, in addition to orchestrating the data flow through the cloud network. The VMware SD-WAN Orchestrator enables one click provisioning of virtual services in the branch, the cloud, or the enterprise data center.

The VMware SD-WAN Orchestrator manages the provisioning of the VMware SD-WAN Edge devices, saving time in setting up new sites and in keeping devices configured correctly. The VMware SD-WAN Orchestrator makes it easy to push out a predefined configuration and avoids the need to access each device and type in commands, like with older systems. It does health checks on the VMware SD-WAN Edge devices and can restore configurations that are out of spec. The VMware SD-WAN Orchestrator can handle your application traffic effectively, enabling your devices to operate at their best and if something happens, it can quickly be put right.

The VMware SD-WAN Orchestrator is a multitenant, hosted solution. It is designed to support multiple access tiers including a service provider operator, its agents and partners, and self-service portals for enterprise customers. Privileges are set separately for each tier.

The VMware SD-WAN data plane controller is available as a hosted service, with multitenant virtual VMware SD-WAN Gateways deployed both by VMware, and its service provider and cloud service provider partners. The controller is a part of the VMware SD-WAN Orchestrator software distribution.

The VMware SD-WAN Gateways provide all the SD-WAN functionality at major cloud data centers, as well as on the provider's private backbone. These are made available on a flexible, subscription basis to enterprises. Hosted VMware SD-WAN Gateways on a subscription provide SD-WAN to the doorstep of AWS, Azure, Google Cloud, VMware Cloud on AWS and others.

Gain line-of-sight to your entire WAN to verify application performance

The VMware SD-WAN Orchestrator makes it very easy to monitor your devices from one screen. You can see the performance of network connections and the improvements provided by VMware SD-WAN. The VMware SD-WAN Orchestrator provides analytics on the network and application performance to help with troubleshooting. Having a view of your connections and applications from one screen greatly speeds time to resolution of any network issues.

VMware reports on metrics for the application network, VMware SD-WAN Edge, VMware SD-WAN Gateway and VMware SD-WAN Orchestrator. These metrics are available with centralized, consolidated visualization and include:

• **Network metrics –** throughput, packet loss, latency and jitter

• **Application metrics –** DAR, application usage (bandwidth consumed) by app/category/sub-app, app categorization and identification, per app link utilization

• **Host metrics –** operating system (OS) and bandwidth usage by host

• **Quality of experience (QoE) score –** VeloCloud Quality Score (VQS) and continuous monitoring of QoE

From a diagnostic standpoint, the focus is on fast root cause detection and analysis done from the VMware SD-WAN Orchestrator. The Diagnostic Application reports on packet captures (PCAPS), Remote Traceroute and pings, VPN tests, remote access, cloud-based configuration management, device logs and controller logs, proactive troubleshooting with alerting and monitoring, and remote reboot. In addition, live view monitoring is available for selected VMware SD-WAN Edges and devices. Enterprise-wide and operator-wide visualization is also available.

Formats supported include, Simple Network Management Protocol (SNMP) v3, syslog, HTTPS, and Netflow Internet Protocol Flow Information Export (IPFIX). Through the RESTful API, all metrics from the VMware SD-WAN Orchestrator can be accessed and populated into third party security information and events management (SIEM) and reporting tools starting with IBM/Qradar.

VMware SD-WAN Gateways connect customers to the cloud

Improve application performance by bringing users closer to the cloud

A benefit of the VMware SD-WAN solution is high performance access to hosted applications. This is done by connecting remote office locations through a VMware SD-WAN Gateway, hosted by VMware or a service provider, to the cloud.

Instead of the connection going back to a company location and then going to the hosted application, traffic goes directly to the application in the cloud.

The VMware SD-WAN Gateway provides optimization between it and the VMware SD-WAN Edge devices in remote office locations.

The decision to have a gateway architecture—with gateways being hosted & managed by VMware—is unique in the SD-WAN space. The VMware SD-WAN Gateways are also stateless in nature, providing easy scalability if needed or to seamlessly failover if a VMware SD-WAN Gateway fails.

The VMware SD-WAN architecture is built for the cloud

There are multiple routes to the cloud. The VMware SD-WAN Gateway can act as a managed on-ramp to the cloud and SaaS. Users can connect to a hub or use a hub-less model with a VMware SD-WAN Gateway.

Aggregation of VMware SD-WAN provider networks simplifies the connection to Multiprotocol Label Switching (MPLS) networks and makes cross-network deployments possible.

The VMware SD-WAN Gateway is a route reflector and acts as a hub, taking policy details from the VMware SD-WAN Edge and acting upon them.

Cloud PoPs are multitenant and isolate customer traffic

Cloud PoPs are multitenant and isolate each customer's traffic from all other customer traffic. Shared gateways are the foundation for multitenancy within the VMware SD-WAN architecture. Having a gateway architecture provides VMware SD-WAN with a unique advantage. From a data plane traffic perspective, a strict isolation is maintained between the multiple tenants.

From a security standpoint, external third party vulnerability scans are executed on a routine basis against the VMware SD-WAN Orchestrator, VMware SD-WAN Gateway, VMware SD-WAN Edge and detected vulnerabilities are escalated to the security review board. Should customers require additional logical isolation, a dedicated set of VMware SD-WAN Gateways can also be provided. On-premises installations are also offered for strict isolation.

vmware®

VMware, now part of VeloCloud always understood that to cater to cloud-based applications, the network has to be cloud native as well, which led to the VMware SD-WAN Gateway architecture. Vulnerabilities identified for any component (VMware SD-WAN Edge, VMware SD-WAN Gateway or VMware SD-WAN Orchestrator) are assessed and patched based on the criticality of the scan result. Service impacting vulnerabilities are fixed and patched within 24 hours of identifying the issue.

Gateway federation for access to hosting data centers

Service VMware SD-WAN Gateways connect to provide access to hosted applications

A big part of access to hosted applications is the use of shared gateways. In addition to the VMware SD-WAN Gateways that are hosted by VMware, other Gateways are hosted by telco partners. With gateway federation, a managed VMware SD-WAN Edge hosted by one provider can share a Gateway from another provider to access applications hosted by that provider. A telco provider partner can deploy and manage their own partner VMware SD-WAN Gateways and VMware SD-WAN Edges via a partner portal in a hosted VMware SD-WAN Orchestrator. VMware also federates the hosted VMware SD-WAN Gateways. The telco partners can offer their enterprise customers the use of partner Gateways and the federated VMware SD-WAN Gateways. With this architecture, you can get access to many types of services from the different telco providers and from the cloud providers.

VMware SD-WAN Gateways are deployed in many cloud data centers. These include AWS, Microsoft Azure, Equinix, Bitrefinery, Cloud Sigma, Dimension Data, Limelight and offered as a service. VMware SD-WAN Gateways are multitenant, virtual versions of its SD-WAN nodes that are deployed by VMware in about 30 different regions, providing SD-WAN benefits to co-located SaaS, infrastructure as a service (IaaS) and network as a service (NaaS). A service subscription provides economical access to all these hosted locations, rather than procuring and installing software images on a data center by data center basis. VMware also offers VMware SD-WAN Edge software subscriptions that can be installed directly by enterprises.

Gateway federation greatly enhances the extensibility of the service architecture, allowing the VMware SD-WAN Cloud service to federate with, for example, a telco service based on VMware SD-WAN. In this model, a service provider in Australia need not deploy VMware SD-WAN Gateways off region; instead they can make use of VMware SD-WAN Gateways as a part of our VMware SD-WAN Gateway federation.

Offnet expansion using gateway federation

A global network overlay can be created using gateways from VMware partners. An aspect of gateway federation is to extend the network from one telco provider to another. Gateway federation allows a provider to federate VMware SD-WAN Gateways with their telco partners, who can offer a managed network service with VMware SD-WAN Gateways integrated into their backbone to extend the network across other telco backbones. This can be used to support a global enterprise that needs a global network. For geographies where the primary provider does not have coverage, a regional partner can be enlisted, and their Gateways can be used to extend the network. This regional partner can deploy and manage VMware SD-WAN Edges in their region, and Gateways from the partner telco provider via their partner portal in the VMware SD-WAN Orchestrator. With this model, the enterprise gets global connectivity, along with a global view of all their sites.

Service chain to security services in the cloud

One click SD-WAN service chaining for hybrid services

VMware SD-WAN provides a service chaining function to connect to services in the cloud. VMware SD-WAN performs service insertion with several cloud web security gateways such as Zscaler, Forcepoint, Palo Alto Networks and Check Point. A key benefit of this feature is that instead of configuring tunnels between every branch to the cloud web security gateways, VMware SD-WAN Edges automatically build tunnels to a VMware SD-WAN Gateway that service chains the cloud web security solution. If 1000 branches need to talk to two Zscaler instances each, typically 2000 tunnels would need to be configured. But with VMware SD-WAN, only two tunnels need to be configured from the VMware SD-WAN Gateway. This significantly reduces operational complexity and cost associated with managing N*N tunnels. This capability is key to large-scale deployments.

VMware SD-WAN integrated with cloud backbone network

Accelerated access to cloud & SaaS

VMware SD-WAN integrates with several of the cloud-based networks. If an organization is accessing SaaS applications or IaaS, they can use VMware SD-WAN to connect to the cloud network for preferred access to these resources. The VMware SD-WAN Gateway connects to the cloud node on the cloud network and shares information with it to dynamically determine the best long-haul path.

Reliability and security are built into VMware SD-WAN

Availability and uptime

• The VMware SD-WAN cloud hosted infrastructure has a 99.99 percent uptime SLA, with 24x7 automated failure detection.

• There is a global set of data centers for optimal selection and redundancy of the infrastructure.

• The VMware SD-WAN Orchestrator is not in the data path nor required for ongoing flow control.

• Management continuity is provided with failover of VMware SD-WAN Orchestrators and regular backups.

• Active/active VMware SD-WAN Gateways provide sub-second resiliency for VPN traffic.

• SaaS traffic can also failover to bypass VMware SD-WAN Gateways.

• Scheduled maintenance windows are advertised 72 hours in advance, and VMware SD-WAN Edge upgrade windows are deferrable with times requested by the account holder.

• Cloud connectivity does not impact customer network operations.

Cloud data centers

• Co-located in Tier IV SSAE 16 Type II certified data centers.

• ISAE 3402 (SAS 70/SSAE 16 replacement) certified facilities and providers deliver reliable failover design to ensure uninterrupted service in the event of a catastrophe.

• Multiple providers and multiple locations service each data center.

• Each data center meets the requirements of international privacy controls and is compliant with European safe harbor type policies.

Network infrastructure and security

• Secure account separation for multitenant VMware SD-WAN Controllers and VMware SD-WAN Gateways.

• Strong firewall policies to deny access for malicious traffic from public networks.

• Proactive monitoring, regular vulnerability scans, and penetration tests performed by a reputable service provider, and automated notifications.

• Management network communications protected by industry-standard encryption algorithms and security protocols.

• Multifactor authentication for administrative remote access.

• Configuration change monitoring and access audits for production network.

Account protection and privacy

• Accounts are password protected and accessed via secure sockets layer (SSL).

• Granular user, role-based access controls and policy framework help to manage third party access.

• Monitoring and incident response procedures are provided in all locations with 24x7 standby teams.

• No data traffic is captured or stored unless enabled by the customer with the packet capture feature.

• User and host machine information is only available to administrators selected by the account holder.

For more information

The WAN is in transition as enterprises seek to improve agility and economics, as well as adapt to the shift of applications to the cloud. VMware SD-WAN offers a cloud delivered solution for enterprise-grade performance, security, visibility, and control over both public Internet and private networks. VMware SD-WAN dramatically simplifies the WAN with zero touch deployment, one click business policy and services insertion, and cloud-based network as a service. The result is a better performing WAN with increased reliability and lower cost of ownership.

For more information about VMware SD-WAN, visit *www.velocloud.com*.