vmware® | netskope

VMware SD-WAN with Netskope

vmware®

SD-WAN™

VMware with Netskope enables optimized, scalable, reliable connectivity with data and threat protection for users at work or home.

Enterprise organizations are going through a digital transformation and the modern workplace is evolving. Organizations are using new applications to manage business processes. These applications are hosted in more locations, not just in the corporate data center, but in multiple clouds. Additionally, the concept of a workplace perimeter is changing, as employees require more flexibility in where they work and on which devices they work. Businesses are empowering employees to work from anywhere, anytime and a seamless user experience throughout the workday is a must.

The question is, how do you deliver the best possible digital workspace to your employees without compromising on performance and security? The answer is VMware SD-WAN™ with Netskope.

To support a cloud transition and deliver a quality user experience, enterprise network architects are re-evaluating their WAN architecture designs to find ways to route Internet traffic locally and take advantage of inexpensive broadband Internet services by adopting SD-WAN. SD-WAN architectures address availability, performance and cost challenges by dynamically utilizing multiple available connections (e.g., MPLS, broadband, cellular, satellite) to find the optimal delivery path for traffic across the entire network, shaping the bandwidth as needed to eliminate jitter and packet loss for all locations.

Using a lightweight IT footprint at branch offices, SD-WAN simplifies business connectivity because IT operations staff does not have to configure and maintain complicated appliances at the branch. Instead they can achieve results with remote monitoring and management.

Cloud-delivered VMware SD-WAN with Dynamic Multipath Optimization™ (DMPO) decides how traffic is steered on a per-packet basis and performs real-time monitoring and remediation without the complexity and effort required for legacy infrastructure. VMware SD-WAN can identify and prioritize traffic among over 3000 applications, offering the closest on-ramp access to leading cloud service providers via VMware edge points of presence (VMware Edge PoP™).

Benefits of VMware SD-WAN with Netskope

Performance without compromising security

Real time identification and prioritization of mission-critical applications along with inline security defenses at scale, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and more.

Reliable connectivity to cloud applications

Real time packet steering, link monitoring and remediation deliver enhanced quality of experience.

Centralized management

One console enables security operations (Netskope Console), while a second console simplifies network operations for branch connectivity (VMware Edge Cloud Orchestrator™).

Simplicity and scale

Minimal touch deployment and scale with centralized monitoring and management.

In addition to the need for reliable and high-performance connectivity, enterprises are equally concerned with how to safely enable cloud and web applications when employees work at home or outside organizations' premises. SaaS applications such as Google G Suite, Microsoft 365, Salesforce, Workday, Slack, and Zoom, combined with IaaS / public cloud services in AWS, Azure, and Google Cloud, now make up the bulk of network traffic. As more users, applications, devices, and data are now in the cloud and outside of a traditional network perimeter, it's essential to protect these users and data.

Netskope Security Cloud for comprehensive security

VMware SD-WAN integrates with Netskope Security to provide comprehensive cloud-enabled security in addition to optimized connectivity. VMware SD-WAN provides networking services by delivering high-performance, reliable branch access to services on cloud and off cloud, while Netskope provides complementary security services such as a next-gen secure web gateway (SWG) and a CASB with both API-enabled and inline protections.

VMware SD-WAN Edges can be deployed as a physical appliance or a virtual machine at the customer site. These devices communicate via secure IPSec or encapsulated GRE traffic to the Netskope Security Cloud. When accessing public clouds such as AWS or Azure, or SaaS applications such as Office 365 and Workday, VMware Edge PoPs hand off traffic to the Netskope Security Cloud, where granular security controls plus advanced data and threat protection are applied. More specifically, this extends users' virtual access to the Netskope NewEdge global network infrastructure. Netskope NewEdge is the network foundation for the Netskope Security Cloud, providing high-capacity, low-latency access to cloud apps and web sites for optimized user experience.

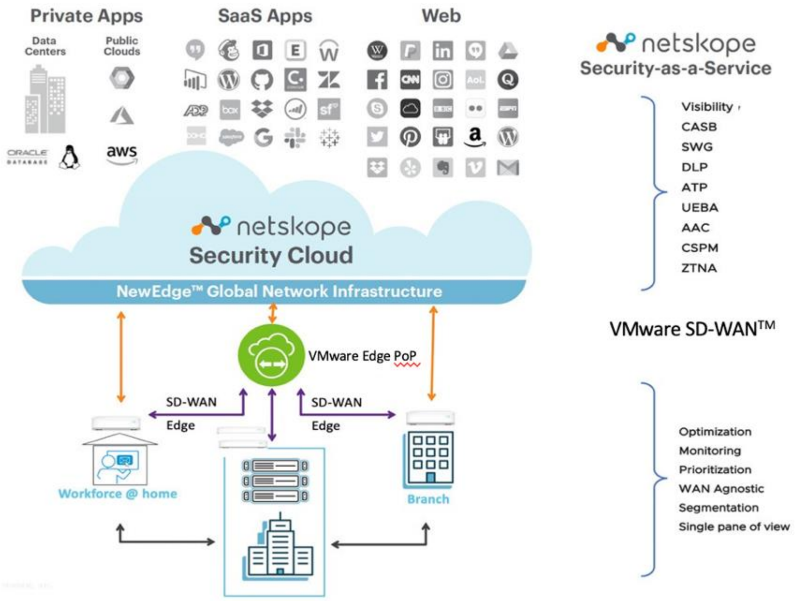

Figure 1: VMware SD-WAN with Netskope integration

Learn more

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

Based on application requirements, admins can choose to direct traffic from VMware SD-WAN Edges directly to the Netskope Security Cloud or via VMware Edge PoPs before handing off the traffic to the application tenant location. The highly available and distributed VMware Edge PoPs offer the added benefit of real time monitoring, packet steering and remediation on the link between users' sites and these PoPs, which then hand off the traffic to either a Netskope tenant location or to the cloud service locations. Remote users outside of the VMware SD-WAN environment can connect directly to the Netskope Security Cloud via encrypted SSL/TLS communications where security controls are applied.

Remote workforce on corporate or managed devices can use the lightweight Netskope client, which provides several key functions: it steers all traffic to the Netskope Cloud, delivers consistent notifications to end users for coaching and guidance purposes when they violate a policy, and it can provide the identity of the user with no additional setup needed by the customer. Remote workforce in branch offices or using their own personal or unmanaged devices, such as in organizations supporting Bring Your Own Device (BYOD), would be directed to the Netskope Security Cloud via its reverse proxy functionality and the security controls would subsequently be applied. Also, Netskope can work with identity providers to forward traffic to Netskope for application access when the remote worker will not or cannot install the Netskope Client.

Netskope and VMware tightly integrate security and SD-WAN features. The combination delivers network optimization services such as optimized connectivity, performance, link monitoring, remediation, and packet steering along with cloud-native, converged single-pass security controls including CASB, SWG, DLP, and Zero Trust Network Access (ZTNA). Together, Netskope and VMware offer organizations a highly scalable, fast and secure environment that protects users and data inside and outside the traditional corporate perimeter.

vmware®

Item No: sdwan-908-netskope-so-0720