WHAT IS SECURE SD-WAN AND HOW CAN IT SAVE ME MONEY?

By Scott Grebe

No matter your type of organization — large or small, public or private — cutting expenses is always a key initiative. After all, reducing your OpEx looks good on the books and enables the company to invest in other meaningful initiatives.

One cost every organization faces is internet connectivity. Access to the internet is essential for communications, website hosting, sharing files, serving up apps and a host of other activities. But it can be expensive, especially if your organization has multiple offices, branches or stores.

Today's broadband users, whether employees or customers, define their experience by performance rather than availability. We don't just expect to have access to apps and videos, we demand that they perform in real time. Any delay is met with complaints and a call for more bandwidth, which increases expenses.

How to Securely Connect, Network Remote Locations

When you have a distributed network with branch or remote locations, they need to be securely connected with each other and the corporate headquarters. This can be done using several techniques. One common method is multiprotocol label switching (MPLS). Using MPLS, organizations can create a private wide-area network (WAN) to securely send data between locations via the shortest path available without going through the public internet.
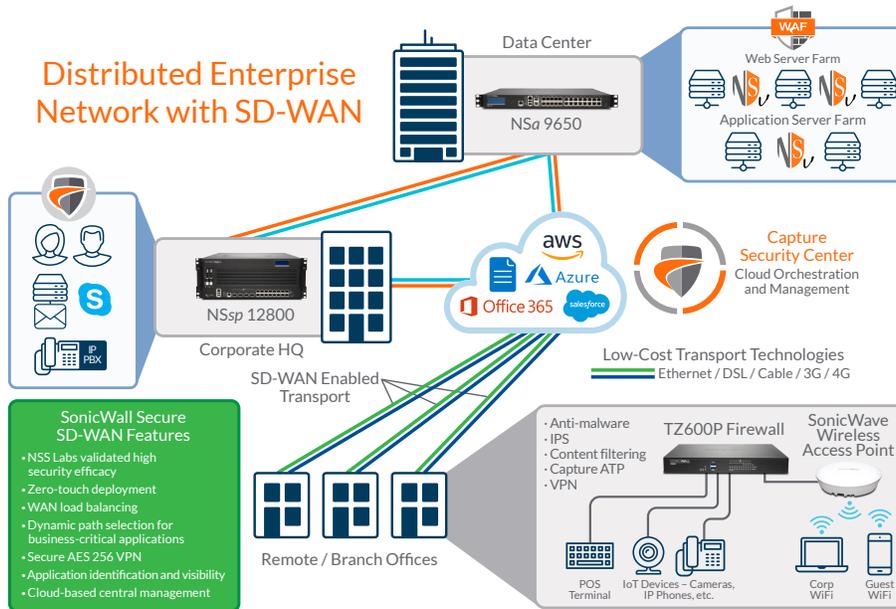
MPLS supports multiple connection types, including T1 and frame relay. The problem? These connections have to support an increasing number of connected devices and bandwidth-intensive applications that demand higher speeds, which means they're expensive. That's why many distributed organizations are moving to SD-WAN (software-defined wide-area network).

"For SD-WAN to be a viable alternative to private WANs, enterprises need to ensure they have the same level of inspection and enforcement at the branch and remote sites as they have at the data center," said Mike Fratto, analyst at 451, in SonicWall's official launch announcement. "Integrated security features with SD-WAN are table stakes for most enterprises adopting the technology."

Reduce Costs with Secure SD-WAN

To help organizations reduce their costs while still receiving secure and consistent performance for business-critical applications, SonicWall offers Secure SD-WAN. A feature of SonicOS 6.5.3, the operating system for SonicWall TZ and NSa firewalls, Secure SD-WAN technology enables distributed organizations to build, operate and manage secure, high-performance networks using readily-available, low-cost public internet services, such as DSL, cable and 3G/4G.

An alternative to more expensive WAN connection technologies, including MPLS, Secure SD-WAN enables virtually any organization — retailers, banks, manufacturers and others — to connect sites spread over great distances for the purpose of sharing data, applications and services. Features such as intelligent failover and load balancing help ensure consistent performance and availability of critical business and SaaS applications.

Distributed Enterprise Network with SD-WAN

Data Center

NSa 9650

Web Server Farm

WAF

Application Server Farm

Corporate HQ

NSsp 12800

aws
Azure
Office 365
salesforce

Capture Security Center
Cloud Orchestration and Management

SD-WAN Enabled Transport

Low-Cost Transport Technologies
Ethernet / DSL / Cable / 3G / 4G

SonicWall Secure SD-WAN Features
- NSS Labs validated high security efficacy
- Zero-touch deployment
- WAN load balancing
- Dynamic path selection for business-critical applications
- Secure AES 256 VPN
- Application identification and visibility
- Cloud-based central management

Remote / Branch Offices

- Anti-malware
- IPS
- Content filtering
- Capture ATP
- VPN

TZ600P Firewall

SonicWave Wireless Access Point

POS Terminal

IoT Devices – Cameras, IP Phones, etc.

Corp WiFi

Guest WiFi

And, unlike solutions from pure-play SD-WAN providers, Secure SD-WAN doesn't require you to purchase additional hardware or licenses.

Secure SD-WAN: Safe, Fast & Reliable

Reducing expenses is always a priority for every organization. What else is? Here are some other key issues Secure SD-WAN helps distributed enterprises solve:

1. **Protect your network from cyber criminals.** Both encrypted and unencrypted traffic run through a SonicWall next-generation firewall to be scanned for threats, such as malware and ransomware, ensuring maximum threat detection and prevention. If you have a separate SD-WAN-only solution, you'll need to make sure you also have a way to protect data from modern cyberattacks, such as encrypted threats and ransomware.

2. **Achieve consistent, optimized application performance.** Realize faster, more consistent performance for SaaS and business-critical applications, such as VoIP, video and unified communications, through capabilities such as deterministic application performance, which steers the apps over less-congested links to overcome jitter, latency, packet loss and other unfavorable network conditions.

3. **Enhance agility.** Using SonicWall Zero-Touch Deployment, bringing up new sites is greatly simplified. Provisioning hardware remotely removes the need to have onsite IT personnel perform the task. In addition, IT administrators can manage the entire network, including devices at SD-WAN-enabled branch/remote locations, through a single pane of glass using Capture Security Center, SonicWall's cloud-based management and analytics platform.

Learn more about how SonicWall can help your distributed enterprise reduce costs and complexity while enhancing security by switching from expensive MPLS to Secure SD-WAN.

"Integrated security features with SD-WAN are table stakes for most enterprises adopting the technology."

— Mike Fratto, Analyst 451

SONICWALL®