CONNECT | MANAGE | PROTECT

WHITE PAPER:

The Best SD-WAN Approach for 2021

How to establish secure connectivity for remote locations

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

SDWanWP012121

SageNet
CONNECT | MANAGE | PROTECT

EXECUTIVE SUMMARY

Organizations with multiple sites must ensure secure, reliable network connectivity for each location. Traditionally, that meant “backhauling” traffic from remote sites to headquarters over the corporate LAN. That worked well enough when most WAN traffic was destined for a central data center. Today, however, remote sites primarily connect to the Internet, making the traditional model costly and inefficient.

Connecting directly to the Internet makes sense but creates security risks. The public Internet is inherently insecure, so organizations must take steps to protect applications and data. A virtual private network (VPN) is one approach. VPNs use encryption and authentication to create secure connections between remote users and the corporate data center. However, site-to-site VPNs are complex and don’t provide all the security controls needed to combat today’s threats.

A software-defined WAN (SD-WAN) incorporates VPN capabilities while providing greater flexibility, agility, availability and performance. Best-in-class SD-WAN solutions also include additional security controls along with improved visibility and centralized management previously only available using expensive multiprotocol label switching (MPLS) services from the telcos. In a nutshell, SD-WAN puts unprecedented network control and flexibility, affordably in reach for even mid-sized organizations.

This whitepaper will explain why SD-WAN is the modern choice for secure connectivity in the multisite enterprise.

CHANGING CONNECTIVITY REQUIREMENTS

Traditional security architectures focus primarily on protecting the network perimeter. Firewalls and other devices are used to create a defensive barrier between an organization’s secure internal network and the open Internet. While perimeter security is still critical, the perimeter has undergone a metamorphosis beyond the scope of a simple outward-facing firewall. The cloud, mobile and an increasingly distributed IT environment have created a perimeter that is porous and ill-defined. Today’s network requires a risk adaptive “perimeter” with multiple layers of defense, identity, access control, and isolation techniques like VPNs.

Security risks have also increased due to shifts in WAN connectivity. In the past, organizations would connect branch offices to headquarters using dedicated private lines or MPLS services. Branch locations typically did not connect directly to the Internet. Instead, Internet traffic was backhauled over the WAN through headquarters, which had more robust defenses.

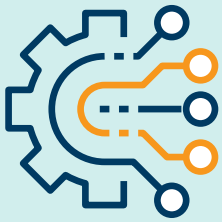
MPLS is reliable and secure but also expensive. While broadband Internet services typically cost $0.75 to $2.00 per megabit per month, MPLS ranges from $75 to $200 per megabit per month depending on location. Plus, MPLS lacks the agility that today's multisite operations need. Provisioning new services or adding bandwidth can take weeks or months, and changes require careful coordination with the telecom carrier. The carrier is in control of the network and can't change at the rate modern business requires.

In addition, MPLS is not well-suited to today's network traffic patterns, which emphasize cloud-based services and communication tools such as voice over IP (VoIP) and video conferencing. Backhauling Internet traffic results in bottlenecks that create latency and impact the user experience. SD-WAN acknowledges that not all network traffic is equal, and shape traffic at the application level.

As a result, organizations increasingly rely upon direct Internet connections for their remote locations and users. However, the Internet is not secure. Organizations need to take steps to ensure that sensitive information isn't compromised as it travels across the WAN.

The Role of MPLS in Today's WAN

Some industry analysts have speculated that direct Internet connections will ultimately replace MPLS in the corporate WAN. In a recent Frost & Sullivan survey, however, respondents indicated that they plan to maintain MPLS connectivity for critical applications. While a majority of sites use a combination of Ethernet and Internet links, many are using MPLS along with Internet and cellular connections.



USING VPNs FOR SECURE CONNECTIVITY

One way to secure Internet connections is to set up a VPN. VPNs use encryption to establish secure "tunnels" for private communications over the public Internet, providing users with highly secure access to enterprise network resources as if they were physically connected to the corporate LAN.

There are two broad categories of VPNs: remote-access and site-to-site. Remote-access VPNs provide secure connectivity for individual users, while site-to-site VPNs establish a connection between LANs in different locations.

With remote-access VPNs, users are authenticated by a VPN gateway that sits outside the corporate LAN, and a secure tunnel is established between the user's device and the gateway. Once connected, any data traveling to and from the user's device is encrypted, with the gateway serving as a relay to the corporate network.

With site-to-site VPNs, the secure tunnel is set up between VPN gateways at each site, eliminating the need for client software. Users connect to and are authenticated by the local VPN gateway, which handles encryption and decryption of the data.

Sites with more than a handful of users who regularly need to access the company network would be best served by a site-to-site VPN. This eliminates the need to manage VPN client software on each user's device, and generally provides better performance and greater scalability. VPN appliances with basic functionality are fairly inexpensive and easy to deploy.

However, more robust site-to-site VPNs are costly and require the management of highly complex routing tables that make moves, adds and changes difficult. Performance can be problematic, particularly with latency-sensitive applications such as voice and video. While applications can be prioritized before they enter the tunnel, all traffic is treated equally on a "best effort" basis once inside.

MPLS Requires a VPN

MPLS is generally more secure than the public Internet but it does not incorporate security controls. Thus, most organizations secure MPLS traffic with a VPN. MPLS VPNs use proprietary infrastructure rather than the public Internet and can prioritize traffic. However, the solution comes with a hefty price tag.

HOW SD-WAN IMPROVES SECURITY

The need to connect branch locations directly to the Internet is one of many factors driving the adoption of SD-WAN. SD-WAN makes it possible to mix multiple data transport services — including fiber/carrier Ethernet, broadband Internet, 4G/LTE wireless, satellite and / or MPLS — in an "active / active" configuration. A communication overlay uses policy-based automation to select the best path for WAN traffic based upon network conditions and application requirements.

This helps to overcome the inherent unreliability of the Internet while enabling organizations to reduce WAN expenses significantly by taking advantage of more cost-efficient bandwidth. In the event of a network outage or slowdown, the SD-WAN will automatically reroute traffic to an available circuit. Most SD-WAN solutions also make it possible to prioritize applications and control bandwidth based upon traffic type and user profile. While SD-WAN does not provide the end-to-end Quality of Service of MPLS, granular prioritization and intelligent path selection can improve the performance of latency-sensitive apps.

SD-WANs generally include standards-based authentication and encryption, automatically establishing a VPN tunnel to protect data traveling over the Internet. Best-in-class solutions also incorporate multiple security controls such as a next-generation firewall and unified threat management.

Because SD-WANs virtualize routing, load balancing, security and other WAN functions, they can be deployed quickly and easily across a large, distributed multisite environment. Organizations may even be able to consolidate the "branch stack," collapsing all WAN functionality onto the SD-WAN for greater simplicity. Everything is managed through a centralized controller, eliminating the need for IT to travel to each site to perform administrative tasks. The controller also ensures the consistent application of routing and security policies throughout the environment.

WHY CHOOSE SD-WAN

When comparing connectivity options, multisite organizations must consider their user and application requirements, business processes and in-house expertise. Some questions to ask include:

1. Are WAN availability and application performance critical?
2. Do connectivity requirements change frequently?
3. Does the organization utilize VoIP, video conferencing and other latency-sensitive applications?
4. Is there a need for greater WAN visibility and centralized management?
5. Do individual sites need perimeter protection as well as data encryption?
6. Could the organization benefit from consolidating WAN appliances?

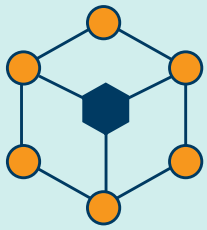
If the answer to any of these questions is yes, SD-WAN is likely the better choice for secure remote site connectivity. But which SD-WAN solution do you choose? Given the popularity of SD-WAN technology there are a number of products on the market with varying capabilities.

SageNet's advanced SD-WAN platform is designed especially for widely distributed multisite organizations. It delivers the availability, security, efficiency and flexibility that multisite operations need in a fully managed solution with around-the-clock monitoring and support.

Its active / active or active / standby architecture with optional session-based survival ensures that connectivity is available when needed. Multi-path technology can automatically select the best available link when the primary WAN path degrades. Application awareness enables prioritized application routing across network bandwidth based upon the specific application and user. Per-packet load balancing and tunnel bandwidth aggregation maximize network capacity.

Robust security is built into *Sage*CONNECT.SD. The solution features a best-of-breed next-generation firewall (NGFW) with threat protection, antivirus, intrusion prevention and application control. NGFW appliances automatically connect to the cloud for authentication and configuration, and IT gains centralized visibility of all *Sage*CONNECT.SD NGFWs across the distributed organization.

Benefits of a Fully Managed SD-WAN



Organizations looking to implement SD-WAN must navigate an unfamiliar technology and determine the best way to migrate their existing WAN infrastructure. They must also determine what kind of connectivity they'll need, find the right carrier and manage the provisioning process. Best-in-class solutions offer a choice of connectivity options and ensure that every site is turned up on time. Consolidated billing eliminates the need to navigate multiple, confusing invoices. A fully managed SD-WAN solution is also monitored around-the-clock by experienced professionals and proactively managed to prevent issues.

CONCLUSION

As organizations move away from traditional WAN architectures to direct Internet connectivity, they need to address security risks. At minimum, organizations must encrypt traffic traveling between remote sites and the corporate data center to protect sensitive data.

In the past, a MPLS + VPN was the go-to choice for secure site-to-site connectivity. Today, however, SD-WAN has emerged as a far more comprehensive solution that better aligns with connectivity trends. SD-WAN creates a more flexible, agile and scalable WAN, with built-in security controls.

Best-in-class SD-WAN solutions also provide greater visibility, centralized management and performance to ensure a high-quality user experience. When every site has ready access to a highly available and secure WAN connection, organizations can operate more efficiently and better serve their customers.

About SageNet

SageNet is passionate about trusted connections. The company believes that by creating, discovering and nurturing trusted connections with its customers, associates and community, SageNet enhances the world that connects us all.

As a leader in managed network and cybersecurity services, SageNet connects, manages and protects technologies and devices across the enterprise. SageNet's collaborative approach provides peace of mind and systems-confidence that empowers an organization to focus on its core mission.

The company offers world-class service and support via its three US-based 24/7 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically-diverse teleports, a central National Logistics Center, multiple data centers, and a nationwide field service organization.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation's largest retail, healthcare, financial, utilities and energy organizations. SageNet manages communications at more than 220,000 endpoints. Headquartered in Tulsa, SageNet has regional offices in Washington, D.C., Atlanta, Chicago and Philadelphia.