POINT OF VIEW

Effective WAN Transformation Depends on Security

Executive Summary

Traditional wide area networks (WANs) were not designed to support the volume and velocity of traffic that is being pushed to branch offices and distributed locations as a result of greater digitalization and distributed applications. These outdated WAN architectures rely on expensive multiprotocol label switching (MPLS) connectivity and centralized security performed by backhauling traffic through the corporate data center. This hub-and-spoke architecture can lead to bottlenecks at the network edge, which results in sluggish performance for end-users—especially under the ever-increasing bandwidth demands that come with digital transformation. Many organizations are choosing software-defined WAN (SD-WAN) solutions to gain better distributed network performance. But all SD-WAN solutions are not created equally—especially when it comes to security considerations.

Regarding SD-WAN, "IDC projects compound annual growth of 18.9% through 2025, when total revenues will top $7 billion."[1]

Include Security for Successful WAN Transformation

As distributed organizations embrace the cloud to improve business agility, modernizing WAN infrastructure has become unavoidable. MPLS connectivity cannot meet the radical change in network demands caused by digital transformation and an increasingly distributed workforce.[2] SD-WAN has quickly become a popular option for replacing traditional WAN infrastructure. SD-WAN uses a variety of commodity internet connections to replace MPLS links at significant cost savings. However, direct access to cloud and internet resources via LTE, DSL, or cable connections carries open exposure to threats—and most SD-WAN solutions on the market today do not have sufficient security capabilities built in or bolted on.

Security cannot be an afterthought with any WAN transformation project due to increasing threat volumes. For example, in the last year, ransomware attacks have increased 150% and the amount paid by victims has risen 300%.[3] In order to design proper security and apply correct policies, IT ideally needs to understand where applications reside, traffic patterns, and performance needs. They also need to anticipate the types of advanced security that will be needed for their specific environments (e.g., secure sockets layer [SSL]/transport layer security [TLS] inspection, URL filtering, intrusion prevention system [IPS], anti-malware, and video filtering). If security is not part of the original architecture design, cyberattacks will slip past incomplete defenses.

Avoid Architectural Complexity

Most SD-WAN solutions on the market today fall short when it comes to built-in security. They do not address the entirety of Layer 3 through Layer 7 advanced security, lack built-in IPS technology, web filtering, SSL/TLS inspection, and other types of essential protection. To address security requirements, some organizations choose to pair dedicated security appliances alongside their SD-WAN. But this adds infrastructure complexity.

SD-WAN installations are also highly dynamic. They are constantly monitoring, remediating, replacing, and restoring connections to maintain optimal application performance. Security solutions that are added on top of a networking-only SD-WAN solution struggle to keep up with these kinds of changes. Further, if these add-on security tools are not part of a fully integrated security architecture, it becomes virtually impossible to track applications and workflows from end to end across the organization. This kind of siloed visibility leaves gaps in protection that can be targeted and exploited.

Lessen Maintenance and Management Needs

Complex SD-WAN architectures can also be difficult to manage and harder to troubleshoot across all branches and locations. This becomes even more challenging when organizations extend SD-WAN to additional use cases—such as cloud to cloud, cloud to data center, or to remote workers who need a more robust connectivity solution. This complexity also increases total cost of ownership (TCO). This is true not only in terms of capital expenditures (CapEx), but also operational expenditures (OpEx) needed to manage and maintain additional firewalls in each location. Plus, other appliances may be needed to cover specific security capabilities or advanced protection needs.

An SD-WAN approach that depends on separate security appliances adds to maintenance and support demand because IT teams have to install, configure, and manage multiple appliances via separate management consoles. They have to stitch connectivity and policies between network and security appliances to protect users and business-critical applications.

The use of encryption on the internet has increased from about 50% in 2014 to about 85% today.[4] Unfortunately, most SD-WAN solutions cannot inspect SSL/TLS encrypted traffic[5] and detect the hidden malware placed there by cyber criminals.

"Centralized SD-WAN management needs to span all distributed branch environments, enabling administrators to deliver and orchestrate configurations and policies, and quickly identify and correct errors that may lead to cyber-risk exposure and network outages."[6]

When performing something as simple as a security OS update, IT has to worry if the upgrade might impact current configurations or possibly impact operations with the SD-WAN networking solution—and even potentially cause network downtime. And when troubleshooting issues, IT may have to deal with two different companies (one for security and another for SD-WAN). This increases the time for getting resolution and support.

Employ Consistent Security Policies

Configuring and managing individual security appliances at each branch office or remote location can be both a time-consuming and error-prone ordeal for IT. Without an integrated security architecture approach that centralizes and simplifies policy management processes across the entire organization, efforts to ensure consistent security policies and enforcement across all use cases and maintain centralized control of the SD-WAN infrastructure add to the burden on limited IT staff. At the same time, gaps are created for threat actors to exploit.

The Path Toward a Secure SD-WAN Solution

WAN transformation through SD-WAN adoption can help organizations unify their distributed operations while providing ample and affordable connectivity for accessing cloud applications and using the latest digital tools. But security must be a strategic consideration for SD-WAN adoption to succeed. To avoid the pitfalls of complexity, cost, management burdens, and inconsistent policies, organizations make sure an SD-WAN solution seamlessly integrates networking and security functions.

[1] Jeff Vance, "Top SD-WAN vendors and how they got there," Network World, August 18, 2021.

[2] Kiran Desai, "The Rapid Rise Of SD-WAN As Digital Acceleration Takes Root," Forbes, September 3, 2021.

[3] Brenda R. Sharton, "Ransomware Attacks Are Spiking. Is Your Company Prepared?," Harvard Business Review, May 20, 2021.

[4] "HTTPS encryption on the web," Google Transparency Report, accessed October 7, 2021.

[5] Nirav Shah, "The Challenges of Inspecting Encrypted Network Traffic," Fortinet, August 4, 2020.

[6] Nirav Shah, "Simplifying SD-WAN Operations with Centralized Management and Orchestration," Network World, June 24, 2020.

FORTINET

www.fortinet.com

October 12, 2021 11:42 PM
1226605-0-0-EN