FORTINET

WHITE PAPER

Understanding the Obstacles to WAN Transformation

Security, Performance, and TCO

Executive Summary

Network engineering and operations leaders are looking to replace their traditional wide-area network (WAN) architectures with software-defined wide-area networks (SD-WAN) in order to support the ever-increasing traffic demands (and associated connectivity costs) that come with digital innovation (DI). These DI-driven initiatives improve staff productivity and create new business opportunities. Yet, they also impact networking performance and ratchet up security concerns.

SD-WAN adoption is accelerating and many organizations have embarked on SD-WAN implementations. But many SD-WAN solutions present serious challenges—from inadequate security to high total cost of ownership (TCO). Understanding these issues is key to navigating the increasingly complex market for WAN edge technologies.

How DI Is Impacting Corporate Networks

Distributed organizations are embracing a wide range of DI technologies. This includes adoption of Software-as-a-Service (SaaS) applications, cloud on-ramping connectivity, Voice over IP (VoIP) and video communications tools, use of DevOps to speed time deployment for new web applications, and Internet-of-Things (IoT) devices for data collection and telemetry.

However, these DI initiatives present new challenges for network engineering and operations leaders who must sustain both performance and security from the data-center campus to branch offices on the network edge. Outdated traditional WANs at remote sites are not designed to support the volume and velocity of traffic that is being pushed to branches and distributed offices. Specifically, these WAN solutions employ a multiprotocol label switching (MPLS)-based network that backhauls all traffic through the corporate data center for filtering and security checks. 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 DI adoption.

But that is not the only problem with the traditional WAN solutions. MPLS connections are also expensive, and the costs can quickly compile as branch traffic volumes continue to climb with no end in sight.

IDC projects that the market for SD-WAN will experience a compound annual growth rate (CAGR) of more than 40% through 2022.[1]

"The emergence of SD-WAN technology has been one of the fastest industry transformations we have seen in years. Organizations of all sizes are modernizing their wide-area networks to provide improved user experience for a range of cloud-enabled applications."[2]

– Rohit Mehra
VP, Network Infrastructure
IDC

Encountering the Challenges of the Traditional WAN

In response, many organizations are embracing SD-WAN solutions on the basis that they deliver better network performance. Yet, there are a number of different SD-WAN solutions on the market with varying capabilities, and it can quickly become a challenge determining which one meets core business requirements. Before a network engineering and operations leader can evaluate available options, they need to consider the reasons this is the case with many SD-WANs.

Inadequate Security: Lack of Comprehensive Threat Protection

Although throughput suffers when a WAN routes all traffic through the data center, MPLS-based WANs are generally perceived as adequately secure. In contrast, for many SD-WAN solutions, advanced security is not built in or, if included, is insufficient. Specifically, the security capabilities in most SD-WAN solutions do not address the entirety of Layer 3 through Layer 7 advanced security, lacking built-in intrusion prevention system (IPS) technology, web filtering, secure sockets layer (SSL)/transport layer security (TLS) inspection, and other protection types.

To solve these security requirements in branch and remote office networks, network engineering and operations leaders must pair dedicated security appliances alongside their SD-WAN. At bare minimum, this involves the addition of a firewall in each location—though sometimes more (e.g., secure sockets layer [SSL]/transport layer security [TLS] inspection is not available in every firewall on the market). But this creates complexity, which increases TCO—from capital expenditures (CapEx) for the additional appliance to staff time (operational expenditures [OpEx]) spent managing the additional firewall and other appliances.

Even among SD-WAN solutions that do include more advanced technologies, gaps still exist. For example, not every SD-WAN solution has security options that have been thoroughly vetted by third-party experts such as NSS Labs. This objective comparison and analysis of SD-WAN solutions enables network engineering and operations leaders to determine which SD-WAN solutions meet real-world business requirements best.

Performance: A Trade-off With Security

The direct connectivity and load balancing of SD-WAN solutions improve performance over traditional WAN. But, just as is the case with security, this is another area where all SD-WAN solutions are not created equal. In particular, not every SD-WAN solution is able to identify and classify application traffic and apply routing policies at a very granular level. The result is that certain applications cannot be prioritized over others. With this one-size-fits-all application traffic model, critical applications, VoIP calls, and video can slow. This impedes end-user productivity.

Furthermore, among the subset of SD-WAN solutions with built-in security, some of the security settings have the potential to degrade network performance. For example, turning on deep inspection of encrypted SSL/TLS can have a huge impact on throughput performance. But for those organizations electing to leave it turned off, they put themselves at heightened risk with 72% of network traffic being encrypted and 60% of attacks using encryption to hide malware with SSL and TLS encryption.[4] In addition, if the solution cannot perform encrypted packet inspection, this obstructs correct traffic routing which degrades the quality of experience (QoE) for network users.

Cost and Resources: TCO Remains High

The increasing volume and velocity of network traffic from VoIP, video, and SaaS-based applications are alarming, which dramatically increases network bandwidth costs for many organizations. Considering that MPLS costs are growing by as much as fourfold or fivefold, the cost savings of SD-WAN that uses the public internet is significant.

Still, network engineering and operations leaders who deploy SD-WAN solutions are often surprised to find a much higher TCO than expected. Specifically, adding multiple appliances for different capabilities increases CapEx as well as the amount of time staff need to spend managing them (OpEx). Network staff must manually monitor and compile log information for threat management. This is time-consuming and highly inefficient.

Further, needing to deploy multiple point products for each remote office and branch location—everything from routers, to firewalls, to security web gateways, to WAN optimization—incurs substantial staff time to manage. Each of these has its own protocols and user interfaces. To achieve visibility and centralized control and demonstrate compliance with various industry and governmental regulations and security standards, network engineering and operations staff must expend manual time

"72% of the respondents [based on a Gartner survey] found that security was their topmost concern when it comes to their WAN."[3]

Many companies that transition to SD-WAN reap substantial savings on bandwidth connectivity—upwards of 40% in some cases.[5]

72% of network traffic is encrypted, with 60% of attacks using encryption today.

TCO for SD-WAN solutions ranges from $5 to $496 per megabit per second (Mbps). Organizations should carefully evaluate the short- and long-term TCO of the SD-WAN solution they are evaluating to determine which one offers the most capabilities at the lowest TCO.[6]

aggregating and reconciling data from each technology-specific silo. In the face of a skills shortage, this time expenditure can become quite costly, as network engineering and operations teams struggle to scale to meet these requirements.

Inefficiencies mount in distributed networks where management of networking and security solutions requires staff to travel to remote locations. Specifically, when SD-WAN solutions do not offer either a virtual alternative or zero-touch deployment capabilities, significant time expenditure for initial deployment and ongoing maintenance can add up quickly.

Conclusion: What to Look for in SD-WAN

When evaluating the many available SD-WAN solutions, network engineering and operations leaders should ask the following questions about each of the solutions on their shortlist:

- What is included in the SD-WAN solution? How many separate products are needed to obtain effective routing, SD-WAN networking, and security capabilities?
- What real-world results have been documented in independent third-party tests such as those conducted by NSS Labs?
- How has the solution been assessed in third-party analyst reports such as Gartner's Magic Quadrants?
- Assuming the solution has built-in security, does it include advanced capabilities—Layer 3 through Layer 7 security controls: 1) IPS, 2) web filtering, and 3) deep inspection of SSL/TLS encrypted traffic?
- Assuming the solution has SSL/TLS inspection capability, what performance impact occurs when it is turned on?
- Is the solution application-aware and does it employ automated path intelligence for optimized routing and prioritization of business-critical SaaS applications, VoIP calls, and video? Does the solution integrate with security elements across the enterprise and across different security areas (e.g., mail, cloud, endpoints, among others) for integrated and automated threat-intelligence sharing?

[1] "SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022," IDC, August 7, 2018.

[2] Ibid.

[3] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[4] John Maddison, "More Encrypted Traffic Than Ever," Fortinet Blog, December 10, 2018; Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[5] Paul Ruelas, "Catching the SD-WAN wave: the cost savings hype and MPLS misconceptions need more explanation," Network World, April 18, 2018.

[6] Thomas Skybakmoen, "SD-WAN Comparative Report," NSS Labs, August 8, 2018.

FURTINET®

www.fortinet.com

FORTINET

SOLUTION BRIEF

Fortinet Secure SD-WAN Transforms WAN Operations

Leave Behind Branch Routers, Realize Lower TCO, and Maximize User Experience

Overview

Software-defined wide-area networking (SD-WAN) has quickly become the solution of choice for legacy WAN infrastructure replacement in distributed organizations. But not all SD-WAN approaches are equally effective. While some implementations simply add basic SD-WAN capabilities to existing legacy routers (featuring a stateful firewall for security), doing so adds infrastructure complexity while exposing branches to undue security risks.

A true secure SD-WAN solution—such as Fortinet Secure SD-WAN—consolidates advanced routing, integrated next-generation firewall (NGFW), self-healing SD-WAN capabilities, and intuitive orchestration into a single, organically developed solution. It provides network engineering and operations leaders with robust branch WAN networking capabilities that support the latest high-performance digital applications while significantly simplifying and automating WAN operations.

Customers are able to improve user experience 5x while reducing costs by more than 40% on average, using Fortinet Secure SD-WAN.

Replacing Legacy Branch Routers with SD-WAN

Network engineering and operations leaders have struggled to incorporate digital innovation initiatives at branch and remote locations due to the limits of traditional WAN infrastructures featuring legacy routers. Specific problem areas include:

- Business application performance issues due to traffic bottlenecks
- Increasing costs due to expensive multiprotocol label switching (MPLS) connectivity
- Limited infrastructure visibility and associated security issues

SD-WAN is increasingly seen as the solution for addressing these problems. But while a basic SD-WAN solution can be swapped out for traditional WAN networking, other legacy parts of the branch infrastructure are not necessarily SD-WAN ready.

For example, many organizations currently rely on legacy routers featuring a simple stateful firewall for branch network security. These outdated devices typically lack key features such as:

- **Application visibility** into cloud traffic and business applications. This limitation increases vulnerability of branch network intrusions via the cloud. Critical applications in this area often include Microsoft Office 365 and Salesforce as well as unified communications tools for voice and/or videoconferencing.
- **Bandwidth utilization** capabilities that manage bandwidth/performance based on the application. It is important that bandwidth becomes smart in order to reduce WAN cost (via over-reliance on expensive MPLS connectivity). Effective bandwidth utilization capabilities require intelligent application awareness that selects and manages a range of connection options based on specific application and user priorities.
- **Advanced security** that applies real-time threat intelligence against the latest malware, botnets, and zero-day attacks. For example, inspection of encrypted network traffic is now essential, but at the same time, these security checks should not inhibit network or application performance.

Stitching SD-WAN functions onto a legacy router is an inefficient approach to upgrading WAN infrastructure. This method increases infrastructure complexity and overall costs while still lacking advanced features for visibility, security, and application awareness as well as unified management functionality. Networking teams typically struggle to maintain and protect branch networks that require a proliferation of point products to address new, advanced threat exposures as well as a growing set of compliance standards and requirements.

Fortinet Solutions for Secure SD-WAN

Fortinet Secure SD-WAN consolidates advanced routing, integrated NGFW, self-healing SD-WAN capabilities, and intuitive orchestration into a single, organically developed solution. Fortinet's approach to SD-WAN supports:

- Simplified operations with built-in features such as Intuitive Orchestrator to enable overlay automation and offer business-centric policies and sophisticated analytics
- Reduced cost through application-centric, self-healing SD-WAN that optimizes dynamic broadband connectivity while lowering WAN operating expenses (via MPLS connectivity)
- Cloud-ready branches by enabling secure network bandwidth and user quality of experience (QoE) for adoption of cloud on-ramping for things like Software-as-a-Service (SaaS) applications and Infrastructure-as-a Service (IaaS)

Fortinet Secure SD-WAN is available in diverse form factors with many different models to choose from to meet your needs ranging from hardware, VM appliances to six different cloud marketplaces for WAN edge transformation. Fortinet is the only vendor with a **purpose-built SD-WAN ASIC**.

SD-WAN Orchestrator in Fabric Management Center can be used to monitor and manage the FortiGate appliances, and is also available in different form factors including hardware, virtual, and SaaS, and from cloud marketplaces such as AWS and Azure.

FortiGuard Services for Fortinet Secure SD-WAN are part of a full range of services and subscriptions to help you simplify and make the most of your SD-WAN deployment with the lowest total cost of ownership (TCO) possible.

Fortinet Self-Healing SD-WAN enables better user experience for business-critical applications on any WAN transport while reducing cost. Intuitive SD-WAN Orchestrator significantly simplifies WAN operations with automation and sophisticated analytics. As the only vendor, with a **purpose-built Secure SD-WAN ASIC**, Fortinet achieves the industry's best security compute rating.

The Path Toward WAN Edge Consolidation

Using Fortinet Secure SD-WAN, network engineering and operations leaders can validate their application performance, cloud connectivity optimization, security posture, and operational costs of the WAN edge. They can also use it to plot a path toward:

1. **WAN edge simplification:** Fortinet Secure SD-WAN consolidates point products to simplify branch infrastructure. This enables bandwidth-constrained network teams to facilitate the transition to SD-WAN.
2. **WAN TCO reduction:** Fortinet Secure SD-WAN reduces WAN costs while providing better security at the edge (e.g., use of direct internet connections, application awareness for bandwidth management, automation, etc.). Indeed, Fortinet Secure SD-WAN delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.[1]
3. **Overall business agility:** A Fortinet Secure SD-WAN Assessment Report can help network engineering and operations leaders to target specific problem areas with existing branch infrastructure to facilitate the transition to SD-WAN implementation.

[1] Fortinet Secure SD-WAN delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.

CHECKLIST

The 5 Keys to Self-Healing, Secure SD-WAN

SD-WAN solutions have become increasingly popular as organizations request fast, scalable, and flexible connectivity among different network environments, and seek to lower overall total cost of ownership (TCO) while preserving user experience. But the wrong SD-WAN solution can significantly inhibit an organization's ability to quickly adapt to changing business demands, not least because it creates new security headaches.

Here are five requirements for a Secure SD-WAN solution that's flexible, scalable, and fit for the needs of today's distributed enterprises.

☑ It goes beyond the branch.

SD-WAN is perhaps best understood for supporting complex branch deployments and helping organizations reduce their reliance on branch routers and other legacy technologies. Effective SD-WAN solutions go well beyond branch office needs, however. Their functionality can extend to home office and teleworker use—especially appliances with built-in LTE for consistent connectivity—and among distributed clouds. SD-WAN solutions also need to come in virtual versions that are available in multi-cloud environments and have deeper integration to enable cloud on-ramp, enabling efficient SaaS adoption.

☑ It offers intuitive orchestration and zero-touch deployments.

Both of these features enable faster configuration rollouts at scale, often within minutes, to enable the best possible performance of collaboration applications such as VoIP, videoconferencing, and various SaaS applications, even for remote users based far away from the corporate data center. Orchestration enables overlay (VPN) automation for the most complex network with intuitive workflows.

☑ It prioritizes critical applications and enables self-healing WAN.

Connectivity alone isn't enough, especially in a remote work-heavy environment. A solution needs to identify a broad set of applications to meet all use cases, while advanced self-healing WAN automation will provide consistent user experience on any transport for any user. Many SD-WAN solutions only support limited use cases, limited numbers of users, and/or specific environments. Caveat emptor.

☑ It includes integrated security.

The difference between SD-WAN and Secure SD-WAN is that the latter is a solution, while the former is a connectivity offering providing another conduit for the bad guys to attack your network. An overlay security solution can't adapt to dynamic connectivity environments; security needs to be embedded into each SD-WAN device, enabling home users, branch office users, and the data center to use a common set of security policies and enforcement criteria. In true Secure SD-WAN, networking, connectivity, and security functions are so tightly integrated they're the one solution meeting three needs, instead of three discrete solutions.

☑ It offers comprehensive analytics and reporting.

A Secure SD-WAN solution needs to help organizations gain visibility into network and application performance (both real-time and historical statistics). That includes enhanced analytics as well as enhanced compliance. A single console and rich SD-WAN analytics can help customers fine-tune their business and security policies to improve quality of experience for all users.