WHITE PAPER

WAN Evolution Presents Opportunities to Service Providers

From Managed SD-WAN to Managed SD-Branch Services

Executive Overview

Many businesses are in a phase of changing expectations, preferences, and usage patterns in regard to the digital technologies they choose for business enablement. This shift expands the network attack surface—impacting everything from the data center to the furthest edges of the network. As applications, data, and compute resources are no longer contained solely within the data center, the evolving network edge of a modern distributed business requires a rethink—from how traffic is managed to how it is secured. This creates an opportunity for managed service providers (MSPs) and managed security service providers (MSSPs) to grow their annual revenue per user (ARPU) over time. Software-defined wide-area networks (SD-WAN) and SD-Branch deployments offer great potential in this regard, but they can also add infrastructure complexity and increase the burden on limited operations staff while exposing customers to new cyber risks.

Increasing Service Provider Revenues

MSPs and MSSPs operate within an extremely competitive space. Their constant challenge is to grow ARPU, profitability, and market share. Beyond adding new customers, they typically achieve this in two ways:

- Increasing margins on services via reduced capital (CapEx) and operational (OpEx) costs
- Launching new value-added services (VAS)

Managed service offerings based on SD-WAN offer a traditional WAN replacement for distributed office locations. But SD-WAN should be thought of as more than just a new connectivity service. It can provide a platform for additional value-added services such as SD-WAN security and SD-Branch (WAN/LAN) consolidation. But currently, the full potential of the SD-WAN platform is being underutilized by service providers.

Therefore, when service providers choose an SD-WAN solution as a foundation for their service offerings, they need to look for more than just pure SD-WAN. They need to consider other full capabilities and additional services that the SD-WAN platform can enable today and in the future. This is important, as a limited SD-WAN solution can negatively impact the associated costs, complexity, and time to market (TTM) of new service offerings for service providers as well as ongoing management expenses post-deployment.

The SD-WAN market is predicted to grow at a rate of 58% to reach $17 billion by 2025.[1] A major reason for this is that SD-WAN is becoming the de facto on-ramp to cloud applications—which greatly impacts user experience and productivity. But the complexity of deploying, managing, and securing these environments across a distributed organization is increasingly driving customers to service providers for their SD-WAN projects.

Almost 80% of IT infrastructure leaders in a recent survey indicate their SD-WAN solution consists of multiple pieces that are time-consuming and difficult to manage. At the same time, over half of them (53%) indicate they partner with service providers for implementation and management support.[2]

Choosing the Right SD-WAN Solution Brings Challenges

As businesses adopt digital initiatives, they often find that traditional WANs are too limited to support availability and performance of the latest digital services—such as Software-as-a-Service (SaaS), Voice over IP (VoIP), and videoconferencing.[3] Typically, the first step is to replace aging WAN connections with an SD-WAN solution. SD-WAN enables efficient, cost-effective, application-centric connectivity that supports the use of digital innovations by the enterprise and its ecosystem.

To facilitate this transition, many businesses are turning to SD-WAN service providers to fill gaps and skills shortages within their existing teams. A clear majority of business leaders do significant business with a service provider—especially for implementation and management roles for specific security products.[4] But despite the many advantages that SD-WAN affords, not every SD-WAN solution is the same. Choosing the wrong SD-WAN solution as the foundation for a managed service can have far-reaching repercussions.

Higher costs. Managed services based on an SD-WAN solution without integrated security capabilities place customers at a higher risk exposure, which in turn increases management overhead costs for service providers (e.g., staff hours spent cleaning up infected systems at branches). Pure SD-WAN solutions (which lack robust, built-in security features) also require the purchase of complementary security devices and appliances (or virtual appliances), plus more time spent assembling and managing the different pieces, and (ultimately) lower ARPU.

Poor visibility and manageability. Managed SD-WAN services cobbled together from multiple security and networking solutions result in a disaggregated view and disconnected policy controls. The added investment in siloed products and operations personnel drives down ARPU while, at the same time, it ratchets up risk due to potential gaps in an overly complex infrastructure. An SD-WAN solution without these embedded capabilities also complicates service onboarding and post-launch operations for service providers.

Application awareness. Application-aware routing can be especially problematic. Many SD-WAN solutions are not able to prioritize traffic based on user, devices, and applications. This not only degrades end-user performance but also can impact service-level agreements (SLAs) for service providers. For some, this may result in the need to purchase WAN optimizers (which increases CapEx costs and OpEx management).

Underequipped security features. Even when security is built into an SD-WAN service, it may be deficient. Point security products and/or services, when used in tandem with a stand-alone SD-WAN networking solution, can yield fragmented and reactive defenses. This increases risk to customers and creates further problems with SLAs, not to mention the added onboarding and operational complexity for the MSP.

Encryption inspection. Most SD-WAN solutions do not scale when secure sockets layer (SSL)/transport layer security (TLS) inspection is turned on. Instead, encryption inspection causes wide-ranging performance degradation for many network firewalls. And if SSL/TLS inspection is not turned on, organizations are at a much higher risk; as much as 60% of encrypted traffic contains hidden malware.[9] This means that service providers must acquire more SD-WAN firewalls or purchase separate encryption inspection equipment—whichever scenario adds CapEx and OpEx costs that drive down ARPU.

Getting in Early on SD-Branch

SD-WAN serves as both a precursor and an essential conduit to SD-Branch. SD-Branch solutions provide a "branch-in-a-box" with the operational agility to rapidly deploy and provision networking and security services for new locations.[10] SD-Branch consolidates both WAN and LAN infrastructure to simplify branch infrastructure while extending SD-WAN capabilities to the access layer in the branches.

Converting customers into an "as-a-service" model for branch office expansion simplifies deployment and orchestration for understaffed businesses, while simultaneously enabling service providers to expand their footprint in each account while potentially driving up ARPU. But again, pure SD-WAN solutions lack several critical capabilities for delivery of an SD-Branch managed service that effectively increases profitability.

Security. SD-WAN solutions that lack robust and integrated security capabilities cannot deliver critical SD-Branch requirements such as:

- Maintaining access control
- Identifying, tracking, and monitoring networked devices
- Analyzing branch traffic
- Detecting advanced malware from attackers looking to initiate an attack through the traditionally less secure branch office

As with SD-WAN, a solution with little to no security means added CapEx investment and OpEx management costs plus greater risk exposure for customers (and more time spent cleaning up infections at branch sites)—all of which drives down ARPU.

The cybersecurity skills shortage exacerbates security challenges at many organizations, and a majority of business leaders favor partnering with service providers to fill gaps in their existing teams.

- 58% of CIOs[5]
- 59% of CISOs[6]
- 66% of security architects[7]
- 74% of network engineering and operations leaders[8]

In a recent survey, security (50%) ranked as the top WAN challenge and the leading factor (81%) guiding companies in the SD-WAN selection process.[11]

A reported 41% of enterprises want their WAN management environment to cover branch LAN infrastructure (e.g., Wi-Fi, switching).[12]

Complexity and cost. Historically, complex branch infrastructures included multiple network and security toolsets—each of which must be purchased and managed separately. This kind of overhead drives down ARPU for service providers charged with managing them. As more branches (and point solutions) are added to the business, cost and complexity problems only intensify for service providers.

SLAs. Service providers may also struggle to meet SLAs without transparent visibility and integration at all access layers. For example, under traditional branch network configurations, service providers are unable to extend security enforcement and mitigation to all endpoint devices—including Internet-of-Things (IoT) devices.

The SD-Branch market is currently in the nascent stage and is expected to be worth $3 billion by 2022.[13]

The Challenge Going Forward for Service Providers

While not all SD-WAN technologies offer robust service capabilities, choosing the right solution gives service providers the ability to deliver more than just agile connectivity at the edge. It also enables them to add services for LAN access (wired and wireless), IoT visibility and control, on-ramp for public cloud, and (most importantly) security. SD-WAN can provide the foundation for an all-in-one VAS platform that allows service providers to expand their footprints and increase revenues while also reducing their onboarding efforts.

Controlling both CapEx and OpEx costs is a critical factor that must be considered in regard to TCO and maximizing profits. Effective service offerings should be based on technologies that consolidate and integrate network infrastructure. For service providers, this limits upfront investment while establishing a technology platform that delivers core benefits like deep visibility, seamless manageability, ease of deployment at scale, intelligence sharing, and automated cybersecurity responses.

[1] "SD-WAN Market to grow at over 58% CAGR from 2019 to 2025: Global Market Insights, Inc.," Globe Newswire, May 10, 2019.

[2] Survey of IT infrastructure leaders conducted by Fortinet. Broader findings of the survey found in "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, August 18, 2019.

[3] "The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, June 29, 2019.

[4] "Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges," Fortinet, September 4, 2019.

[5] Jason Pappalexis, "Security Controls in the US Enterprise: Software-Defined Wide Area Network (SD-WAN)," NSS Labs, accessed September 2, 2019.

[6] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[7] Ibid.

[8] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[9] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[10] Lee Doyle, "SD-Branch: What it is and why you'll need it," Network World, January 23, 2018.

[11] "Skills gap remains a top barrier to SD-WAN adoption," Help Net Security, July 18, 2019.

[12] Shamus McGillicuddy, "Survey: Enterprises want end-to-end management of SD-WAN," Network World, January 9, 2019.

[13] Cynthia Harvey, "SD-Branch: 4 Things to Know," Network Computing, July 11, 2018.

www.fortinet.com

October 2, 2019 10:42 PM

D:\Fortinet\Work\2019\October\wp-wan-evolution-presents-opportunities