FORTINET

How Service Providers Can Optimize Managed SD-WAN and SD-Branch Delivery and Management

Table of Contents

Executive Overview

As distributed enterprises and small and midsize businesses (SMBs) embrace digital innovation (DI), legacy networking and security infrastructures often fail to deliver sufficient performance and protection. Software-defined wide-area networking (SD-WAN) and SD-Branch solutions can help organizations consolidate traditional infrastructure and facilitate adoption of the latest business-enabling technologies.

This creates an opportunity for service providers and managed security service providers (MSSPs) to deliver managed SD-WAN and SD-Branch value-added service (VAS) offerings that elevate their annual revenue per user (ARPU). A platform for delivering SD-WAN and SD-Branch services must overcome the challenges presented by a patchwork of multiple point solutions. This includes increased capital and operational costs as well as new security risk exposures. Instead, service providers should look for solutions that integrate WAN-edge infrastructure into a single, consolidated solution that supports both secure SD-WAN and SD-Branch managed services via a common service platform.

Distributed Organizations Turn to Managed Services

As many organizations adopt digital initiatives throughout their distributed environment, they simultaneously face a historic shortage of skilled cybersecurity staff—nearly 3 million unfilled positions worldwide today.[1] This confluence presents an opening for service providers to create value. Indeed, according to recent survey findings, best-in-class cybersecurity leaders (i.e., those with the fewest intrusions) are four times more likely to outsource a majority of functions—security and nonsecurity related—to a services provider.[2]

In the case of the WAN edge, managed services solutions that replace traditional approaches to network-edge infrastructure at the branch have great potential for addressing the problems of distributed digital organizations. SD-WAN is a critical starting point, where organizations enhance or replace existing expensive multiprotocol label switching (MPLS) solutions with application-aware connectivity. This offsets performance degradation that is becoming an increasing problem due to the amount of Software-as-a-Service (SaaS), Voice-over-IP (VoIP), and video traffic being used in the distributed enterprise.

Providing a managed SD-WAN service allows network service providers to balance potential MPLS-related revenue losses by increasing overall ARPU as well as their depth of penetration and stickiness in each account. For service providers, SD-WAN offers a new service opportunity even if they do not own the underlying network—wherein they can operate an overlay network over any existing underlay or physical network from a different service provider. SD-Branch is a logical evolution from SD-WAN, enabling organizations to further consolidate and simplify network-edge infrastructure in remote deployments.

But the solutions that drive these services vary widely in terms of capabilities. Service providers must carefully consider all associated costs and effort—both capital expenses (CapEx) and operating expenses (OpEx)—as well as performance and security requirements in order to deliver services that increase ARPU over time without expanding complexity and risk. The following examines each of the above scenarios:

The managed security services market is growing at a 12% compound annual growth rate (CAGR) and is expected to reach $34 billion by 2022.[3]

Managed SD-WAN: Key Considerations

Choosing the underlying technology for a managed SD-WAN service is crucial—namely, it is a critical factor determining the service's scope, addressable markets, potential revenue, and size of margins. Beyond pure managed SD-WAN services, service providers should also consider the solution's comprehensive and consolidated functionality. The best options will provide the broadest range of extended value-added services (VAS) options for customers—including built-in security.

Consolidation lowers CapEx. Most SD-WAN solutions require multiple components that are disaggregated—separate devices for network firewalls, intrusion prevention (IPS), anti-malware, WAN optimizers, and other components. Acquiring multiple devices and appliances to deliver a fully featured and secure SD-WAN service greatly increases CapEx, which negatively impacts the service provider's ARPU. Instead, service providers should look for a secure, fully featured SD-WAN solution that is delivered via one physical or virtual appliance.

More than half (53%) of organizations report that they partner with managed security service providers for implementation and management support.[4]

Simplified orchestration and operations lower OpEx. Complex, nonintegrated SD-WAN solutions may require significant staff hours for training, deployment, configuration, and management. A consolidated SD-WAN solution helps improve efficiency for solution deployment and implementation. This reduces the time, resources, and costs required for onboarding new customers. An integrated solution with automation capabilities also helps to simplify ongoing management workflows for service provider staff. Even more, the capability to provide historical data and comprehensive analytics helps to troubleshoot and quickly address performance issues. This reduces the time, labor, and costs for managing customer deployments, all of which boosts ARPU.

Improved security. Disaggregated infrastructures have inherent gaps in security operations that can be exploited by cyberattacks. A solution that integrates advanced SD-WAN networking capabilities within a next-generation firewall (NGFW) provides a foundational element for a managed SD-WAN service. This consolidation reduces risk along with CapEx and OpEx costs.

Application awareness. With applications, users, and devices varying in their level of priority, bandwidth constraints and performance remain a concern for service providers tasked with service-level agreements (SLAs) in addition to reliable connectivity. Increasing WAN bandwidth demands can carry high costs while also failing to meet the designated SLA. Intelligent application awareness capabilities with link resiliency can address this issue.

In response, the SD-WAN solution should reference a broad database of known applications, which then allows it to prioritize traffic and automatically manage connections in real time—based on the critical needs of the organization. This helps service providers deliver high application availability to customers, while also optimizing network costs for lower total cost of ownership (TCO).

Encryption inspection scalability. Many SD-WAN solutions do not scale when secure sockets layer (SSL)/transport layer security (TLS) inspection is turned on. This can cause significant performance degradation for network firewalls. To address this challenge, service providers must purchase additional SD-WAN firewalls or separate encryption inspection equipment, which increases complexity and TCO. However, an integrated SD-WAN solution featuring high-performance, purpose-built SD-WAN processors can enable encrypted traffic inspection without performance impact. When service providers need to acquire more network firewalls or encryption inspection appliances to offset the performance degradation, this ratchets up CapEx costs, while adding more OpEx costs associated with the time required to manage the additional devices.

Almost 80% of organizations indicate their SD-WAN solution consists of multiple pieces that are time-consuming and difficult to manage.[5]

Beyond SD-WAN to the Network Edge with SD-Branch

Businesses are increasingly looking to replace both their WAN and LAN infrastructures in favor of a consolidated networking solution that delivers deeper integration and simplified operations at branch office locations. An effective SD-Branch managed service should consolidate WAN and LAN capabilities to simplify remote office infrastructure and optimize operations without introducing new risks.

A fundamental starting point for SD-Branch is the delivery of SD-WAN as a service. When it comes to selecting the right SD-Branch solution, service providers have multiple options and need to weigh them carefully. Factors such as orchestration, management, TCO, and security all impact ARPU potential over time.

41%

of enterprises want their WAN management environment to cover branch LAN infrastructure, such as Wi-Fi and switching.[6]

Following are the foremost elements service providers need to employ when choosing the right SD-Branch solution:

Extended security to the access edge. By design, an SD-Branch solution should protect connectivity across wired switches and wireless access points (APs). Beyond that fundamental capability, SD-Branch solutions should also secure the expanded access edge by combining NGFW, IPS, network access controls (NAC), security of switches and APs, and other critical capabilities in a single device. The ability to deliver this functionality as part of the existing managed SD-WAN service is a powerful benefit for the service provider, resulting in higher ARPU through greater simplicity and lower CapEx and OpEx.

Simplified management and scalability. A consolidated SD-Branch solution for service providers should also enable centralized orchestration and management capabilities via the following features. First, service providers should look for SD-Branch with zero-touch deployment to expedite setup and configuration of new customer branch locations. An SD-Branch solution must also offer multi-tenancy (among other things) to enable elastic branch scalability. And as the branch scales with the customers' business growth, it should do so without adding complexity or cost. To do so, the SD-Branch solution should offer a common management interface (via open APIs) in order to provide complete branch infrastructure visibility and control.

Visibility. Tracking devices, applications, and users can be difficult across distributed infrastructures. An SD-Branch solution should give the service provider end-to-end, actionable visibility across all locations of the business for advanced prevention and detection capabilities. Unsecured endpoints such as Internet-of-Things (IoT) devices present particular risks at branch locations, which may not have a regular on-site IT presence to oversee their deployment and management. As employees increasingly introduce unauthorized, high-risk connected devices to branch networks, security systems must be able to spot potential vulnerabilities that offer threats a gateway to the broader organization. Here, the ability to provide IoT visibility and control at the branch level as part of the SD-Branch service is an important capability, as the biggest concentration of IoT devices often resides there.

Control and compliance. A managed SD-Branch solution should include centralized, dynamic, and automated management of NAC based on the type of connection, endpoint device, user, and application. This delivers better edge protection while reducing the management burden for service providers. As an extension of NAC capabilities, an SD-Branch solution should also support automated logging, auditing, and reporting to simplify workflows and help prove compliance with privacy laws and industry regulations.

Lower TCO. A consolidated SD-Branch solution drastically reduces the number of tools and devices needed to provide a secure and functional branch infrastructure service to customers—which yields a lower CapEx investment for service providers. At the same time, a solution that offers centralized management and automated workflows helps to reduce ongoing OpEx costs. Having fewer technology vendors to manage, support, and train also helps service providers increase their margins, improve customer satisfaction, and boost seller confidence.

An effective SD-Branch solution should include intelligent, centralized management of SD-WAN, routing, integrated security, network switching (wired), and AP (wireless) functions.[7]

Integration and Automation Drive Simplicity and Revenue

Managed SD-WAN services that are powered by a fully featured, integrated solution lay the groundwork for adding SD-Branch capabilities. This gives service providers the ability to grow revenue with customers while significantly reducing additional infrastructure complexity, cost, and overall onboarding churn.

When evaluating a solution as the basis for delivering SD-WAN managed services, providers should ask the following questions to help them identify a solution that delivers optimal value:

- Does the solution provide **centralized management** across all branch locations for simplified operations and lower OpEX?
- Does it offer **zero-touch deployment** and **multi-tenancy** capabilities to support the rapid launch and configuration of new offices?
- Can the solution support robust **application awareness** that orchestrates traffic based on the application's business criticality and needs?
- Does it include effective **SSL/TLS encryption inspection** capabilities that do not degrade firewall or network performance?

To extend their customer footprint via an SD-Branch offering, solution providers should also ask these additional questions:

- Does the solution combine WAN/LAN infrastructure while **integrating critical security features like NGFW and management of switching/AP** functions?
- Is it capable of centralized **dynamic management of network access** based on the type of connection, endpoint device, user, and application?
- Are critical analytics features such as **logging, auditing, and compliance reporting** automated?
- Is **zero-touch deployment and provisioning for the branch** supported?
- Can the solution significantly reduce the service provider's CapEx and OpEx to **measurably lower TCO?**

[1] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

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

[3] "Managed Security Services (MSS) Market 2019 Global Trends, Size, Competitors Strategy, Regional Study and Industry Growth by Forecast to 2022," MarketWatch, February 1, 2019.

[4] 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.

[5] Ibid.

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

[7] Kelly Ahuja, "SD-Branch: The Next Destination On The Digital Transformation Journey," Forbes, November 9, 2018.

FORTINET

www.fortinet.com

394217-0-0-EN

November 15, 2019 1:32 PM

eb-service-providers-sd-wan