SOLUTION BRIEF

Fortinet Simplifies and Optimizes SD-Branch Managed Services

Executive Overview

Distributed branch networks and the point solution security products used to protect branch infrastructure have become difficult and costly to manage due to the rapid adoption of Internet-of-Things (IoT) devices, Software-as-a-Service (SaaS) applications, and digital voice/video tools. Managed service providers (MSPs) and managed security service providers (MSSPs) can extend their offerings and boost annual revenue per user (ARPU) by expanding current software-defined wide-area network (SD-WAN) customers to managed SD-Branch services. As an extension of services based on FortiGate Secure SD-WAN, Fortinet helps consolidate the network access layer within a secure platform that provides visibility and security to the network and all devices that connect to it. Its industry-best total cost of ownership (TCO) helps service providers to deliver extended value-added services (VAS) while boosting revenue.

Branch Infrastructure-as-a-Service Requires Consolidation, Cost Control, and Security

As distributed organizations look to consolidate branch infrastructure across the WAN edge, access layer, and endpoints, service providers are well-positioned to play a pivotal role. More than half (53%) of organizations report that they partner with MSPs or MSSPs for implementation and management support.[1] Here, SD-Branch technologies can consolidate WAN and LAN capabilities to simplify remote office infrastructure and optimize operations.

While a managed SD-Branch offering starts with delivery of SD-WAN as a service, service providers must consider critical factors such as integration (firewall, switches, access points), ease of deployment, centralized management, TCO, and security—which all impact ARPU potential over time.

Fortinet's Solution for SD-Branch Deployments

As an extension of FortiGate Secure SD-WAN, Fortinet's purpose-built SD-Branch capabilities allow service providers to deliver an SD-Branch VAS with unparalleled network performance and reliability, while providing centralized control and visibility across the entire network-edge attack surface. It covers all critical branch exposures—from the WAN edge, to the branch access layer, to a full spectrum of endpoint devices. It allows service providers to extend FortiGate Secure SD-WAN capabilities across wired and wireless networks while simplifying branch infrastructure management—increasing service capabilities and revenue streams without any additional capital expense (CapEx).

Extending security to the access edge

By unifying WAN and LAN environments, Fortinet's SD-Branch solution secures the expanded access edge by combining NGFW, intrusion prevention (IPS), network access controls (NAC), security of switches and APs, and other critical capabilities in a single device. The fact that it offers these advanced security and networking capabilities as part of an existing FortiGate Secure SD-WAN solution allows service providers to boost ARPU on existing managed services even further through greater simplicity and lower CapEx and operating expense (OpEx).

Simplified management and scalability

Fortinet's SD-Branch solution helps service providers centralize orchestration and management capabilities. It provides single-pane-of-glass management of security, network access, and SD-WAN. This combined interface for security and networking eases management burdens on service provider staff while enabling proactive risk management. Fortinet also enables elastic branch scalability through advanced features like multi-tenancy and zero-touch deployment. Zero-touch deployment also reduces the OpEx associated with initial setup and branch office expansion over time.

An effective SD-Branch solution should include intelligent, centralized management of SD-WAN, routing, integrated security, network switching (wired), and AP (wireless) functions.[2]

Visibility, control, and compliance

As part of the integrated Security Fabric architecture, Fortinet offers service providers a common management interface via open application programming interfaces (APIs) in order to provide comprehensive branch infrastructure visibility and control. Fortinet's SD-Branch solution automates discovery, classification, and security of all endpoints when they seek network access—including unsecured IoT devices.

In the latest NSS Labs NGFW group test, FortiGate delivered 99.3% security effectiveness and 100% evasions blocking.[3]

To further minimize managed service OpEx, Fortinet's SD-Branch solution also automates anomaly detection and remediation processes based on defined business logic. It supports dynamic and automated 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.

Without the right tools, compliance reporting processes can be time-consuming and costly (in terms of human resources) for service providers. Fortinet's solution provides automated tracking and reporting capabilities that help ensure adherence to privacy laws, security standards, and industry regulations while reducing collateral risks of fines and legal costs in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. They also monitor firewall policies and facilitate compliance audits—reducing staff time spent on these tasks while eliminating potential human errors and associated operational costs.

Lower TCO

Fortinet dramatically lowers the service provider's CapEx investment and boosts TCO by greatly reducing the number of tools and devices needed to provide secure and functional branch infrastructure to customers. Fortinet's solution integrates switches, firewalls, extenders, and wireless APs into a single, consolidated solution. At the same time, Fortinet's centralized management and automated workflows help reduce OpEx costs. With fewer technology vendors to manage, support, and train, service providers increase their margins, improve customer satisfaction, and boost seller confidence. As corroboration, Fortinet delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.[4]

Expand VAS Offerings with Security-driven Branch Networking

Remote branch locations need their own defenses that conform to the unique risks they present. Fortinet's solution for SD-Branch consolidates the network access layer within a secure platform that provides visibility and security to the network and all devices that connect to it.

Managed services based on FortiGate Secure SD-WAN provide a seamless migration for extending customers to the benefits of an SD-Branch VAS offering. This gives service providers the ability to cultivate new revenue streams with existing customers without additional infrastructure complexity, cost, or deployment churn.

[1] 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.

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

[3] "Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report," Fortinet, June 19, 2019.

[4] Ibid.

December 25, 2019 12:45 PM

395782-0-0-EN

D:\Fortinet\Work\2019\December\122519\sb-sd-branch-managed-services