FORTINET

Consolidating Networking and Security Functions Can Reduce Branch Vulnerability

Executive Overview

As enterprises embrace digital transformation (DX) initiatives (cloud, Internet of Things [IoT], and mobile), their attack surface rapidly expands and the risk of a breach increases. For example, distributed organizations with one or more remote locations are looking to software-defined wide-area networks (SD-WANs). But SD-WAN alone does not address three associated security problem areas: 1) protection of multiple WAN edges, 2) lack of endpoint visibility, and 3) branch infrastructure complexity. However, a solution that consolidates networking and security capabilities can help network engineering and operations leaders simplify infrastructure while providing better security and productivity at branch locations. An integrated SD-Branch approach can boost visibility, control, and manageability while lowering total cost of ownership (TCO) for distributed organizations.

Table of Contents

FORTINET

01 The Expanding Attack Surface of Distributed Enterprises

Adoption of new technologies as part of DX creates some unique complications for distributed organizations with branch networks.

Multiple WAN edges to secure. The edge of the WAN in the branch network is becoming more difficult to protect. It starts with rapidly growing traffic volumes—the result of an influx of Software-as-a-Service (SaaS) applications, cloud-based tools, Voice over IP (VoIP), and video services. It also includes a propagation in wireless access points and the number and types of devices accessing them. This evolution of the WAN edge exposes vulnerabilities that must be secured.

Visibility. Branch networks also must support many more endpoint devices (both wired and wireless). These include the various personal mobile devices of employees, suppliers, and visitors, as well as a growing number and diversity of IoT devices.

Some may not have fully patched and/or updated system software, and a large number (in the case of IoT) may not have any built-in security capabilities at all. And not all of these devices are even visible to network or security operations teams.

Complexity. The de facto approach to infrastructure at most companies has been addressing new network functions and security gaps one at a time by adding a new device. Over time, this creates extremely complex environments. And specifically, the large number of isolated point security products that have accumulated have become difficult to manage—in terms of both cost and time—while still leaving gaps in protection. Similarly, provisioning technologies into branches can also consume valuable time and resources.

Here, network engineering and operations leaders need a solution that can ensure security, performance, reliability, and availability at the branch. An effective network security approach must deliver powerful, scalable performance while integrating multiple network and security features within one offering. It also requires a network security architecture that provides centralized policy controls and transparent visibility across the attack surface.

02 Securing the WAN Edge

Traditional WAN has become too expensive due to costly MPLS connectivity in combination with expanding bandwidth and traffic requirements (as a result of things like dominant use of SaaS applications).

SD-WAN can enable DX of branch offices with cost savings and performance improvements. But for SD-WAN to do this, it must provide both networking and security—and performance is not a foregone conclusion. An effective SD-WAN solution should:

- Consolidate disparate network and security functions into one solution
- Offer zero-touch deployment of branch networks for low TCO
- Employ robust security that is built into the SD-WAN firewalls (without buying and managing separate security appliances)
- Optimize network bandwidth (application awareness and multi-broadband support)
- Inspect encrypted secure sockets layer (SSL)/transport layer security (TLS) traffic without bottlenecking network performance for optimal user productivity

The global SD-WAN market is projected to grow at over 40% compound annual growth rate (CAGR) to reach $4.5 billion by 2022.[1]

03 Securing Endpoints

Security also now requires the ability to see, categorize, and secure all connected endpoints—especially unseen IoT devices that may be deployed without official sanctioning of network operations or IT. Establishing a unified platform across the organization can further provide a transparent view of all connected devices on the branch network.

Once all devices on the network are discovered and visible, the centralized management capabilities of the SD-Branch should dynamically manage network access and enforce policy-based controls for consistent security across all users, applications, and endpoints—including vulnerable IoT devices. The solution should include automated access controls (e.g., to quarantine vulnerable or suspicious devices), as well as anomaly detection and incident response capabilities for fast remediation that reduces the burden on IT staff.

Cyber criminals have IoT devices on the vulnerable branch network edge squarely in their sights. An estimated 25% of all attacks will target IoT devices by 2020.[2]

04 Securing the Branch Access Layer

Integration of WAN and LAN platforms can further improve network performance and security. To simplify branch infrastructure, network leaders can consolidate multiple purpose-built appliances for network functions (e.g., routers, load balancers) and also specific security capabilities (e.g., intrusion prevention, detection) at the same time.

Convergence of both wired and wireless networking within a next-generation firewall (NGFW) device extends the capabilities of a secure SD-WAN solution to the branch access layer—combining NGFW security, switches, extenders, and APs in one interoperable solution. This integration reduces infrastructure complexity by simplifying branch management of security, network access, and SD-WAN. It eliminates multiple vendors, interfaces, and operating systems, which can burden limited staffing resources, while erasing defensive gaps along the seams between different solutions.

An effective solution should help increase agility through a single-pane-of-glass interface, which improves branch visibility and control. It should also support zero-touch solution deployment for improved TCO.

The average enterprise uses upwards of 75 different security solutions, many of which only address a single function or compliance requirement.[3]

05 Comprehensive Branch Security

With enterprise branches directly accessing internet connections (via SD-WAN), networking leaders need to implement next-generation security while enabling multi-path WAN to improve application performance. An effective branch deployment should seamlessly integrate networking and security capabilities across the aforementioned areas—WAN edge, access layer, and endpoints.

When evaluating a solution to optimize overall branch network functionality and improve security, the following questions may be useful:

- Does the solution effectively consolidate security and networking across the branch?
- Does the solution provide transparent visibility and granular control of devices and users?
- Does it offer a centralized management console (single pane of glass) with the ability to enforce global policies?
- Are there any third-party certifications or testing to validate the solution's performance, reliability, or value (TCO)?
- Does testing include performance evaluation for specific needs such as SaaS applications or VoIP/video performance?

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

[2] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed March 21, 2019.

[3] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

www.fortinet.com

419872-0-0-EN

June 12, 2019 11:54 AM

eb-branch-solution-research