FORTINET

WHITE PAPER

To Support Digital Innovation, Branch Networks Need Greater Simplicity and Visibility

Executive Summary

Distributed organizations are rapidly adopting the latest digital innovations (DI). These innovations include high-performance tools such as Software-as-a-Service (SaaS) applications, unified communications such as Voice-over-IP (VoIP) and videoconferencing, and a wide assortment of Internet-of-Things (IoT) devices. But these new technologies—and their associated traffic demands—are causing problems for network engineering and operations leaders in terms of performance, reliability, availability, and perhaps most of all, security. The explosion of new applications, devices, and users at the network edge has greatly expanded the attack surface of many businesses. The addition of point security products to address individual gaps or compliance requirements adds even more infrastructural complexity, which can compound security problems rather than alleviate them. As a result, network engineering and operations leaders lack visibility and centralized policy management over their increasingly complicated and risk-prone branch infrastructures.

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.[1]

The Expanding Attack Surface of Distributed Enterprise

With branch office users requiring access to the latest innovations, the demand on their networking infrastructures has exceeded the capacity of outdated wide-area network (WAN) technologies. The traditional WAN relies on expensive multiprotocol label switching (MPLS) connectivity and a hub-and-spoke architecture that backhauls all traffic through the corporate data center for centralized security and filtering checks. This approach creates performance bottlenecks that interfere with network performance and reliable availability of digital voice/video communications and critical SaaS applications.

While new technologies like software-defined WAN (SD-WAN) offer faster connectivity options to support DI applications, many solutions inherently lack security and advanced networking capabilities for application routing. To compensate, organizations typically add a proliferation of point security products and tools. This complexity creates new problems in terms of visibility and control at the branch. At the same time, widespread adoption of IoT devices (which mostly lack built-in security) open up their own unique blind spot when it comes to protecting distributed organizations.

The Need for a Secure Alternative to Traditional WAN

SD-WAN technologies that incorporate direct internet connections can alleviate network performance and cost limiters associated with MPLS—but at a cost of centralized security. As more innovative applications and devices are added to a branch network, the more opportunities there are for threats to penetrate the organization.

To compensate for this ever-expanding threat vulnerability at the network edge, many distributed organizations have opted to continuously add on more point security and networking products one at a time to support new capabilities, cover new cyber-risk exposures, and address evolving compliance requirements. 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.[2]

Deploying and managing all of the disparate pieces of this kind of fractured branch infrastructure creates a time-sink for staff. Each of the branch's disparate toolsets for networking and security must also be purchased and managed separately. This adds complexity and overhead in terms of staff management. As more branches (and point solutions) are added to the business, problems multiply for the organization. Total cost of ownership (TCO) is negatively impacted due to inefficiencies in capital (CapEx) and operating (OpEx) expenses.

Complexity Yields Poor Visibility at the Network Edge

Complex architectures additionally lack centralized administration, cohesive control of security policies, and transparent visibility across all parts of the branch network—especially at the access layer's wired switching and wireless access points (APs). As a result, organizations often struggle to support critical functions like:

- Access controls
- Traffic analysis
- Identification, tracking, and monitoring of networked devices
- Detection of advanced malware

Following are some of the repercussions of these challenges:

Slow response times. Lack of transparent visibility and centralized management ratchets up risk and increases inefficiencies for network engineering and operations leaders. The disaggregated networking and security products deployed across the branch infrastructure typically do not share threat intelligence or coordinate responses to cyber events that slow down response times to security events. This, in turn, increases the chances that critical operations across the organization will be disrupted and/or that valuable data will be exfiltrated.

Manual workflows. Proliferation of point security solutions also creates a need for more manual workflows. Beyond the aforementioned operational cost, manual processes inhibit security scalability and agility. They also lead to inconsistent application of security policies across the different parts of a distributed hybrid environment. More than half (52%) of all breaches are caused by human errors or system glitches (as opposed to malicious or criminal attacks).[4]

Manual workflows for compliance tracking, auditing, and reporting compound this problem further. As industry standards and privacy law requirements evolve year over year, lack of security automation in these areas places an undue burden on limited staff resources while increasing the risk of regulatory penalties due to human errors.

Encryption inspection. With nearly three-fourths (72%) of all network traffic being encrypted[6] and 60% of malware using encryption to infiltrate networks and exfiltrate data,[7] secure sockets layer (SSL)/transport layer security (TLS) inspection capabilities are now a must-have for branch offices in order to minimize risk exposure. Last year, more than one-fourth (28%) of breaches involved malware of some kind.[8]

Most branch firewalls significantly degrade network performance when inspection is turned on. To compensate, network engineering and operations leaders must either buy more firewalls or separate inspection appliances to help enforce inspection. As with any add-on point product approach to infrastructure, this increases branch TCO with ongoing CapEx investment and OpEx management costs. The difficult choice for many businesses becomes to either accept the higher costs and quality of experience (QoE) penalties of SSL/TLS encryption or increase risks by not inspecting encrypted traffic at all.

A reported 41% of enterprises want their WAN management environment to cover branch LAN infrastructure (e.g., Wi-Fi, switching).[3]

The vast majority (89%) of security leaders at large enterprises still struggle with visibility and insight into trusted data.[5]

90% of organizations have experienced or expect to experience a network attack using SSL or TLS encryption.[9]

IoT Devices Bring Unique Risk Exposure

IoT devices continue to multiply across enterprises, with an estimated 30 billion devices in use within the next year.[10] IoT devices include everything from light switches, to printers, to medical devices, to ATMs. But in terms of branch security, these connected devices present significant challenges. Cyber criminals frequently target IoT devices because they represent some of the weakest points on the network. Many IoT products are "headless"—unable to perform even simple patches and offering little to no built-in security. In addition, traditional endpoint security protections are too large or resource-intensive to run on most IoT devices. To make matters worse, many of these devices are added to the branch network without the knowledge of IT or security teams.

Unfortunately, branch security typically lacks key capabilities for addressing the particular issues that IoT devices present:

Lack of visibility. Network engineering and operations leaders need to be able to detect, classify, and secure every connected endpoint device on the branch network. The lack of comprehensive and centralized IoT device visibility leaves branches (and by extension, the broader organization) vulnerable to attack.

Lack of situational awareness. In the event of a coordinated attack across multiple devices and/or parts of the distributed organization (as is often the case with IoT-targeting botnets), nonintegrated security architectures lack the ability to share threat information in real time and adapt defenses to multiple points of attack in unison.

An estimated 25% of all cyberattacks will target IoT device vulnerabilities by 2020.[11]

Lack of automated threat responses. Outdated network access control solutions also often lack advanced capabilities for managing IoT devices—such as automated threat responses for policy-based responses to a potentially compromised device (such as device quarantine and detailed analyst alert reports). Unaddressed IoT device vulnerabilities at the branch also expose organizations to potential compliance violations in the event of a breach, compounding the financial damage to an organization.

The Evolution of Branch Infrastructure

As branches demand greater performance for the latest business applications, network engineering and operations leaders have a delicate balance to address in terms of connectivity options, reliability, availability, cost, and perhaps most of all, security. The current lack of visibility and centralized management of branch infrastructure puts their entire distributed organization at greater risk of attack. Therefore, network engineering and operations leaders must evaluate the state of their current branch infrastructure. The following questions can help lead that exploration:

- ☐ Are there ways to consolidate and simplify my branch network and security infrastructure for greater efficiency and cost savings?
- ☐ Do I have robust automation and orchestration functions to help reduce management costs—such as rapid deployment of new branches?
- ☐ Are there ways to improve optimization of network performance?
- ☐ Do I have intelligent routing of traffic based on the user and/or application?
- ☐ Do I have visibility across all security elements?
- ☐ Can I inspect all network traffic—encrypted and unencrypted—without network disruption?
- ☐ Can I see all IoT devices across all distributed locations and enforce policy-based controls to prevent a device-based breach from spreading?

[1] "Skills gap remains a top barrier to SD-WAN adoption," Help Net Security, July 18, 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] Shamus McGillicuddy, "Survey: Enterprises want end-to-end management of SD-WAN," Network World, January 9, 2019.

[4] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[5] "Why poor visibility is hampering cybersecurity," Help Net Security, June 24, 2019.

[6] "Quarterly Threat Landscape Report Q3 2018," Fortinet, November 2018.

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

[8] "2019 Data Breach Investigations Report," Verizon, April 2019.

[9] Ibid.

[10] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," Statista, accessed October 15, 2019.

[11] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed October 15, 2019.

www.fortinet.com