Doyle Research

Securing the SD-Branch

By: Lee Doyle, Principal Analyst at Doyle Research

Sponsored by Fortinet

Executive Summary

Organizations of all sizes are currently undergoing a digital transformation to improve customer satisfaction and enhance employee productivity. For many organizations, the branch edge is essential in how they deliver their products and services - and those locations are typically on the front line of digital innovation. The increased use of cloud-based platforms and SaaS applications, the popularity of BYOD, and the wide variety of IoT devices are placing significant stress on the branch network.

SD-WAN technologies are being deployed at these branch locations to reduce costs and improve cloud-based application performance. Expanding on the concept of software-controlled WAN connections, many vendors are extending that remote control into branch offices' wired and wireless networks – a solution called SD-Branch.

Secure SD-Branch builds upon SD-Branch and provides comprehensive networking and security at remote locations including SD-WAN, routing, Ethernet, Wi-Fi, network access control, and next-generation firewall. Secure SD-Branch solutions enable rapid provisioning of new branch locations, simplify operations, reduce overall costs of operations while delivering integrated and comprehensive security.

Fortinet provides a Secure SD-Branch solution which includes FortiGate firewall and SD-WAN appliance, switching and wireless infrastructure products, and a network access control server.

Digital Transformation Drives New WAN, Branch and IoT Requirements

Widespread digital transformation is rapidly changing requirements and architectures at the data center and the branch. IT organizations need to enable multi-cloud architectures, speed access to SaaS applications and securely network BYOD and IoT devices. Distributed organizations need to extend the same applications and functions to their branch office users as they provide to their corporate offices, such as unified communications, Office365, conferencing, and SalesForce.

IoT is a business reality for many organizations (including banks, retailers, insurance firms, and restaurants) with the need to securely connect a wide range of devices and sensors. For example, retail shops must connect cash registers and scanners, refrigeration units, thermostats, security cameras, and inventory control devices. Many of these IoT devices, while critical to the operation of the branch location, have poor security. Whether due to their design, the cost points, the CPU power, or the memory available, IoT devices are notorious for being susceptible to attack.

In addition, IT organizations face the difficult task of managing distributed locations remotely. Remote management includes provisioning new branch offices and adjusting networking policies to respond to changing organizational or employee requirements. Access to cloud-based applications and data via the Internet creates security challenges at the edge of the network. Experienced IT executives have shared that maintaining and securing remote locations are the most difficult aspects of owning a distributed network. The complexity of branch operations increases when the network/security devices in the branch are from different suppliers. Each vendor brings a requirement for their own, unique management consoles and siloed products, increasing the burden of the IT team to effectively monitor, manage, and respond.

SD-Branch

Branch operations are strategic for many organizations due to the number of remote employees, demanding customer requirements, critical local applications, and an increased number of connected IoT devices. Productivity and user/customer satisfaction at branch locations is highly dependent on network connectivity. Widespread mobility has further challenged branch network reliability and created new security challenges. To simplify the management of these remote locations, vendors have enhanced their products with software defined-Branch (SD-Branch).

SD-Branch leverages advances in software to converge previously separate functions of LAN (ethernet and Wi-Fi), SD-WAN and routing into a unified platform. In the same way that SD-WAN simplified the management of the WAN connection via software, SD-Branch simplifies the management of the Branch via software. SD-Branch takes the benefits of SD-WAN's ease-of-use and automation capabilities and applies it to the local area network.

SD-Branch eliminates the appliance sprawl at the branch enabling centralized IT staff to control and manage a large number of remote sites. It improves the quality of user experience by enabling better remote management of the network, which leads to appropriate bandwidth and prioritization for high-value applications. Doyle Research expects SD-Branch implementations to grow rapidly over the next five years and to become the standard platform for remote branch networking.

Defining SD-Branch – Doyle Research

> Advances in software networking virtualization enable the packaging of a wide range of network functions onto a unified platform. The SD-Branch simplifies network operations by consolidating WAN connectivity (SD-WAN and routing), and LAN/WLAN in a unified, easy to deploy and manageable platform

Requirements for the "Secure SD-Branch"

Security and risk management in remote locations are key concerns for IT executives. Sensitive applications and data reside throughout the organization and branch locations are especially vulnerable to attack via unsecured IoT devices or Internet connections. Advanced security needs to be systematically extended to the LAN and WAN traffic at the branch. A sound security strategy must detect and track network-attached devices, analyze traffic, and defend against advanced malware.

The Secure SD-Branch combines network security with LAN and WAN functions. Security tools need to be integrated into the ethernet switch, Wi-Fi, and SD-WAN so that security policies and network access controls can work as an unified system. The Secure SD-Branch should be able to discover and identify all devices on the network. Secure SD-Branch applies policies across LAN and WAN as well as wired or wireless networks. Secure SD-Branch needs to dynamically assign traffic to its appropriate network segment based on any given user's function and role.

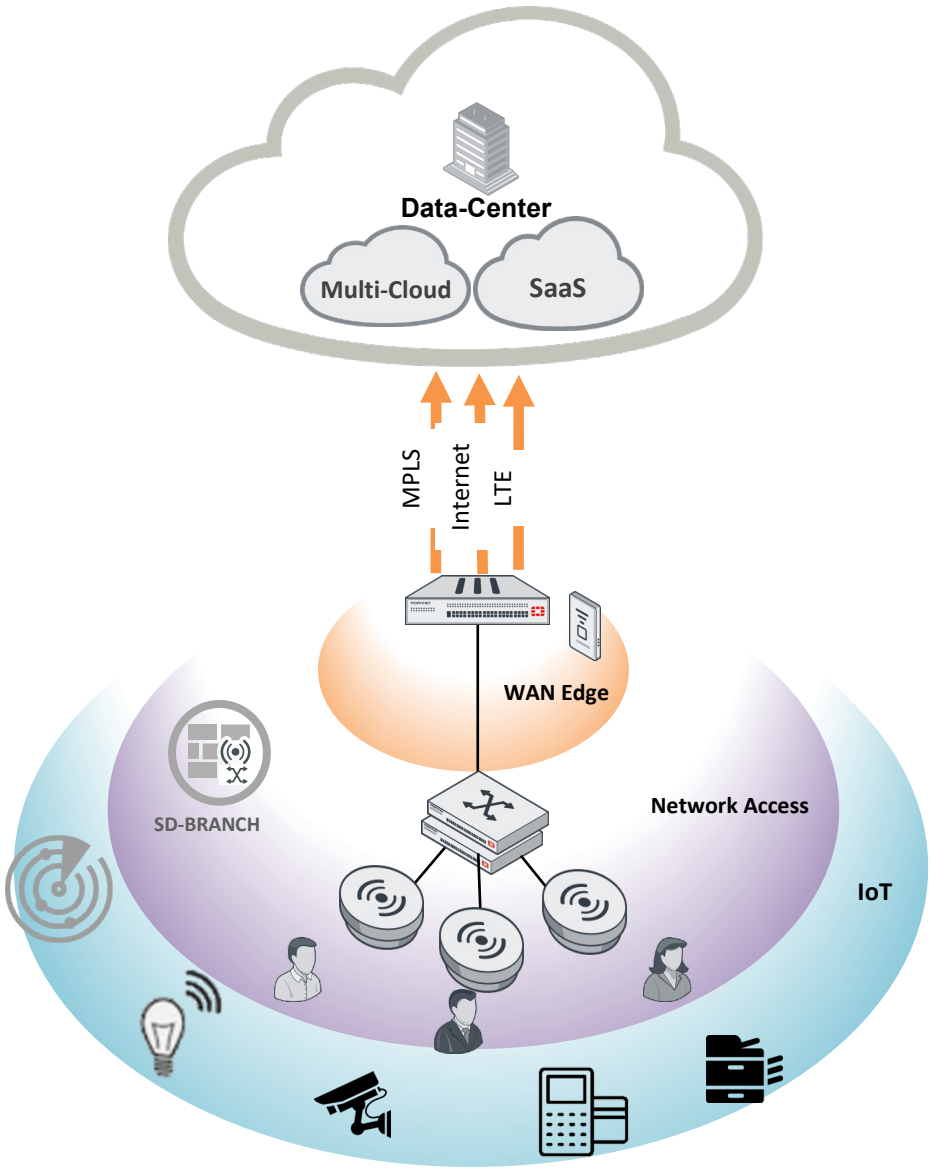
Secure SD-Branch architectures include a next-generation firewall (NGFW) for the necessary traffic and application control. Within the Secure SD-Branch, the NGFW extends the WAN edge security from the SD-WAN connection to ensure that all inbound and outbound traffic, including direct internet and cloud traffic, is inspected and secured at line rate. The integration between the NGFW and the LAN infrastructure both enhances the security of the branch office and simplifies the management of security policies.

For the protection of the unsecured IoT devices, a network access control (NAC) solution provides per-device security. It provides automatic discovery, identification, classification, and application of the appropriate security policies.

These policies should be able to restrict the network access of these devices so that they have the necessary access to perform their function and no more. For example, the refrigerator temperature sensor in the quick-serve gas station store should not have access to the PCI network. These policies need to be applied

automatically every time a device connects to the network or is moved onto the network. See Figure 1.

Figure 1: Secure SD-Branch



In addition to SD-WAN capabilities, the Secure SD-Branch should deliver the following:

- Zero-touch provisioning for rapid deployment
- Consolidated security and network access controls
- Delivery network security at scale and performance for a high-quality user experience

Fortinet Secure SD-Branch Solutions

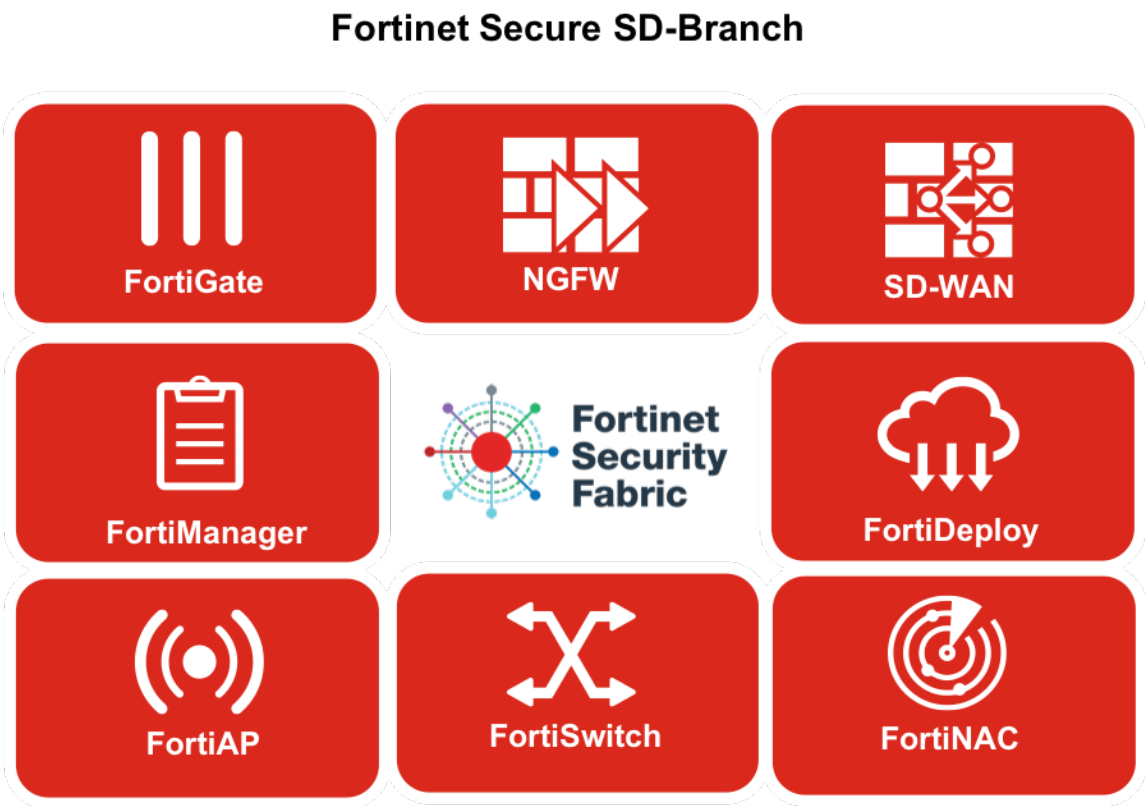
The Fortinet solution enables customers to converge their security and network access, extending the benefits of the Fortinet Security Fabric to their distributed branches. Secure SD-Branch is comprised of FortiGate next-generation firewall (NGFW), FortiNAC network access control, FortiSwitch, and FortiAP to deliver consolidation of branch services for network edge and device edge protection.

The Fortinet Secure SD-Branch solution builds upon the strong security provided by the NGFW combined with the tight integration of switches and access points to that NGFW. Fortinet is able to extend the security of the firewall out to the edge of the network where devices and users are connecting while also simplifying the management of the network, including security policies.

In coordination with the NGFW, FortiNAC solutions continuously monitor the network to discover new IoT devices and appropriately profile them. Once identified, IoT devices are then allowed onto the network in a least-access approach. This means that those devices can get appropriate access for their role or function only. For example, IP cameras do need access to the NVR server but do not need access to financial or customer data servers. FortiNAC applies such policies automatically. Additionally, FortiNAC can automatically respond to events and can quarantine suspicious or out-of-policy devices for remediation.

See Figure 2.

Figure 2
Fortinet Secure SD-Branch



SD-Branch Customer Example: Warrior Invictus

Warrior Invictus Holding Company, Inc. owns a half-dozen insurance companies in the U.S. mid-west. The company manages $100 million in annual premiums for nonstandard auto, property and casualty, and life and health insurance policies. As a financial services company that manages a broad array of insurance products, Warrior Invictus and its independent distributor network face enterprise-level security risks.

Due to security and compliance requirements, Warrior Invictus initiated a review of its network infrastructure. It decided to replace its existing routers, switches and firewalls with a comprehensive Fortinet solution at its headquarters and 16 branch locations. The company gained a number of benefits from its SD-Branch solution, including improved visibility, comprehensive security, and reduced downtime.

Conclusions and Recommendations for IT Leaders

The branch network is a key aspect of many organizations' digital transformation. The rise of popular cloud-based applications, BYOD, and new IoT devices continues to stress branch WAN networks. Security threats are ever-present, and attackers can leverage unsecured edge devices to gain access to the corporate network. The multitude of branch network elements (SD-WAN, routers, Wi-Fi, firewalls, etc.) makes it challenging to deploy and manage branch operations.

The network edge needs to be seen as part of an overall integrated network and security architecture. The virtualization of network software has enabled the convergence of wired and wireless networking, LAN and WAN with next-generation firewall functionality. The Secure SD-Branch solution combines all of the required branch network/security capabilities in one interoperable solution.

Secure SD-Branch provides advanced security, access control, and network management services in a zero-touch model so they can be deployed across multiple locations and then be remotely managed through a common interface. As well, Secure SD-Branch architecture can boost visibility, control, and manageability while lowering the total cost of ownership (TCO) for distributed organizations.

Secure SD-Branch solutions are now ready for implementation at the edge of the network. SD-Branch solutions eliminate many of the challenges of integrating

multiple LAN, wireless, WAN and security solutions at branch locations. SD-Branch can provide benefits for new (or branch refresh) builds including rapid deployment, unified management, and lower cost.

Fortinet provides an integrated Secure SD-Branch solution with ease of deployment, unifed security policies and consolidated management. Organizations evaluating SD-WAN and SD-Branch solutions should consider the Fortinet Secure SD-Branch solution.

Meet the Author

Lee Doyle is the Principal Analyst at Doyle Research, *providing client-focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Fierce, and Tech Target. Lee holds a B.A. in Economics from Williams College.*