SOLUTION BRIEF

Secure the Network Edge at the Branch with Fortinet SD-Branch

Executive Summary

Digital transformation (DX) has made branch networks much more complex and therefore, vulnerable to attack. In response, many organizations have deployed multiple point products to address new threat exposures as they appear. But, this approach further complicates branch infrastructures, adding greater cost, complexity, and vulnerability. To address these issues, branches should integrate networking and security capabilities across the WAN edge, access layer, and endpoints. The Fortinet SD-Branch solution consolidates the network access layer within a secure platform that provides visibility and security to the network and all devices that connect to it.

Addressing an Expanding Attack Surface

Rapid adoption of DX technologies, including Internet-of-Things (IoT) devices, Software-as-a-Service (SaaS) applications, digital voice and video tools, and bring-your-own-device endpoints, has caused an increase in the number of network edges that need to be secured at a given branch. The networks and point solution security products used to protect branch infrastructure have become complicated and costly to manage.

The rise of IoT, particularly connected office appliances, efficient lighting and climate controls, and employee-owned personal fitness products, represents many more devices coming onto the network, often with questionable security and unreliable visibility.

Fortinet SD-Branch Solution

Fortinet delivers a broad, integrated, and automated approach to network security at an unmatched price-performance ratio. Fortinet SD-Branch seamlessly expands to the new edges of the network and delivers unparalleled performance and reliability while providing centralized control and visibility across the entire branch attack surface.

SD-Branch consolidates networking and security capabilities into a single solution that provides seamless protection of distributed environments. It covers all critical branch exposures, from the WAN edge to the branch access layer to a full spectrum of endpoint devices. It extends Fortinet Secure SD-WAN capabilities across wired and wireless networks while simplifying branch infrastructure management.

Fortinet SD-Branch offers several key differentiators over competitive options. First, it enables secure networking using the FortiGate Next-Generation Firewall (NGFW) and broader Fortinet Security Fabric architecture to extend security throughout the network access layer.

The rapid pace at which new applications are being adopted, combined with a shortage of IT and security resources, means that security teams are often overwhelmed, potentially leaving gaps in the organization's defenses.[1]

The Internet of Things, with its devices' interconnected nature and vulnerabilities, has become an attractive target for cybercriminals operating out of the dark web.[2]

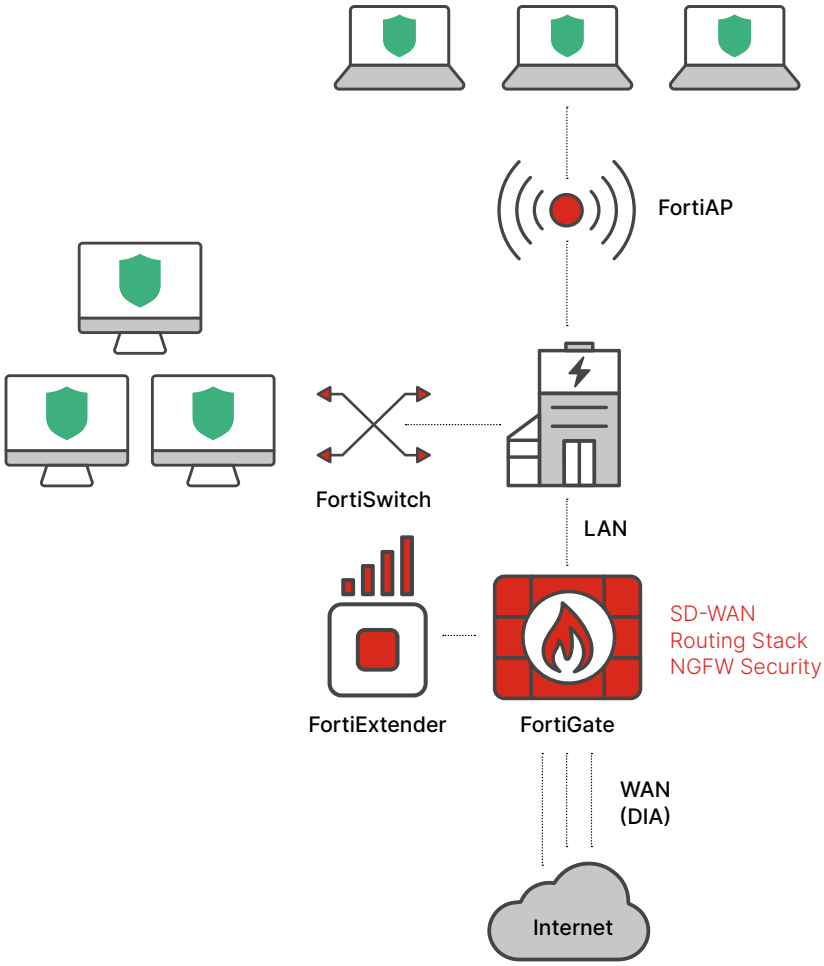


Figure 1: Fortinet SD-Branch consolidates WAN and LAN infrastructures.

This includes Fortinet solutions like FortiAPs (secure wireless access points) and FortiSwitches with FortiLink (secure Ethernet). The combination of networking equipment tied to the FortiGate via FortiLink allows for capabilities such as built-in onboard network access control (NAC) services. FortiLink NAC can automatically onboard devices into the correct security posture.

Additionally, this security overlay can be expanded to enable capabilities such as virtual patching, where vulnerable devices (such as IoT) can have compensating controls until a full firmware update can be applied. FortiNAC adds enhanced visibility, detection, real-time posture assessment, and control of IoT devices, with the ability to track anomalies via traffic analysis. FortiExtender 5G/LTE gateway devices can be added to increase WAN resiliency. The FortiGate seamlessly manages these and can improve SD-WAN performance for the site without adding management complexity.

Fortinet SD-Branch also includes single-pane-of-glass security management, network access, and SD-WAN. FortiManager enables extensible management at scale with zero-touch deployment. Its combined interface for security and networking helps ease the burden on IT staff while minimizing TCO.

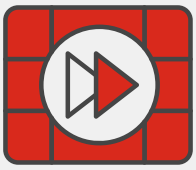
Key Benefits for Network Engineering and Operations Leaders

The lead benefits of the Fortinet SD-Branch solution come from improving security at the branch. Global policies are enforced at all WAN edges, at the branch access layer, and across all endpoint devices. It unifies WAN and LAN environments and extends security and network performance to the access layer. It automates the discovery, classification, and protection of IoT devices when they seek network access. It also automatically provides anomaly detection and remediation processes based on defined business logic. Finally, distributed organizations can rapidly scale operations across new offices and geographic locations.

Fortinet SD-Branch also helps to reduce the need for on-site resources, which lowers TCO. SD-Branch integrates firewalls, switches, and APs into a single, consolidated solution. Its single-pane-of-glass management capabilities combine security and network layer visibility to optimize staff efficiency while enabling proactive risk management. Zero-touch deployment features reduce the burdens associated with initial setup and business growth over time.

Secure Branch Networking

The continuing evolution of branch networks makes them a security challenge. Remote locations need their own defenses that conform to the unique risks they present. Fortinet SD-Branch provides secure networking as a natural extension of the Fortinet Security Fabric. In doing so, 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.



FortiGate NGFW featuring Secure SD-WAN scores 99.88% Security Effectiveness in 2023 CyberRatings.[3]

[1] Sarah W. Frazier, "4 Reasons Why SaaS Security Must Change," Grip, May 26, 2024.

[2] "How the Internet of Things (IoT) became a dark web target – and what to do about it," World Economic Forum, May 17, 2024.

[3] "Enterprise Firewall," CyberRatings.org, Q2 2023.

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 18, 2024 8:22 PM / 431530-B-0-EN