

SOLUTION BRIEF

Fortinet Secure SD-WAN Transforms WAN Operations

Leave Behind Branch Routers, Realize Lower TCO, and Maximize User Experience

Overview

Software-defined wide-area networking (SD-WAN) has quickly become the solution of choice for legacy WAN infrastructure replacement in distributed organizations. But not all SD-WAN approaches are equally effective. While some implementations simply add basic SD-WAN capabilities to existing legacy routers (featuring a stateful firewall for security), doing so adds infrastructure complexity while exposing branches to undue security risks.

A true secure SD-WAN solution—such as Fortinet Secure SD-WAN—consolidates advanced routing, integrated next-generation firewall (NGFW), self-healing SDWAN capabilities, and intuitive orchestration into a single, organically developed solution. It provides network engineering and operations leaders with robust branch WAN networking capabilities that support the latest high-performance digital applications while significantly simplifying and automating WAN operations.

Replacing Legacy Branch Routers with SD-WAN

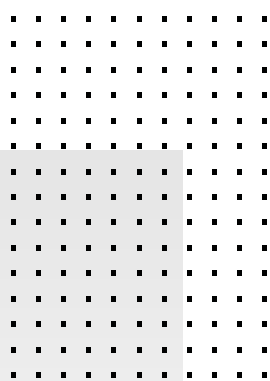
Network engineering and operations leaders have struggled to incorporate digital innovation initiatives at branch and remote locations due to the limits of traditional WAN infrastructures featuring legacy routers. Specific problem areas include:

- Business application performance issues due to traffic bottlenecks
- Increasing costs due to expensive multiprotocol label switching (MPLS) connectivity
- Limited infrastructure visibility and associated security issues

SD-WAN is increasingly seen as the solution for addressing these problems. But while a basic SD-WAN solution can be swapped out for traditional WAN networking, other legacy parts of the branch infrastructure are not necessarily SD-WAN ready.

For example, many organizations currently rely on legacy routers featuring a simple stateful firewall for branch network security. These outdated devices typically lack key features such as:

- **Application visibility** into cloud traffic and business applications. This limitation increases vulnerability of branch network intrusions via the cloud. Critical applications in this area often include Microsoft Office 365 and Salesforce as well as unified communications tools for voice and/or videoconferencing.
- **Bandwidth utilization** capabilities that manage bandwidth/performance based on the application. It is important that bandwidth becomes smart in order to reduce WAN cost (via over-reliance on expensive MPLS connectivity). Effective bandwidth utilization capabilities require intelligent application awareness that selects and manages a range of connection options based on specific application and user priorities.
- **Advanced security** that applies real-time threat intelligence against the latest malware, botnets, and zero-day attacks. For example, inspection of encrypted network traffic is now essential, but at the same time, these security checks should not inhibit network or application performance.



Customers are able to improve user experience 5x while reducing costs by more than 40% on average, using Fortinet Secure SD-WAN.



Stitching SD-WAN functions onto a legacy router is an inefficient approach to upgrading WAN infrastructure. This method increases infrastructure complexity and overall costs while still lacking advanced features for visibility, security, and application awareness as well as unified management functionality. Networking teams typically struggle to maintain and protect branch networks that require a proliferation of point products to address new, advanced threat exposures as well as a growing set of compliance standards and requirements.

Fortinet Solutions for Secure SD-WAN

Fortinet Secure SD-WAN consolidates advanced routing, integrated NGFW, self-healing SD-WAN capabilities, and intuitive orchestration into a single, organically developed solution. Fortinet's approach to SD-WAN supports:

- Simplified operations with built-in features such as Intuitive Orchestrator to enable overlay automation and offer business-centric policies and sophisticated analytics
- Reduced cost through application-centric, self-healing SD-WAN that optimizes dynamic broadband connectivity while lowering WAN operating expenses (via MPLS connectivity)
- Cloud-ready branches by enabling secure network bandwidth and user quality of experience (QoE) for adoption of cloud on-ramping for things like Software-as-a-Service (SaaS) applications and Infrastructure-as-a Service (IaaS)

Fortinet Secure SD-WAN is available in diverse form factors with many different models to choose from to meet your needs ranging from hardware, VM appliances to six different cloud marketplaces for WAN edge transformation. Fortinet is the only vendor with a **purpose-built SD-WAN ASIC**.

SD-WAN Orchestrator in Fabric Management Center can be used to monitor and manage the FortiGate appliances, and is also available in different form factors including hardware, virtual, and SaaS, and from cloud marketplaces such as AWS and Azure.

FortiGuard Services for Fortinet Secure SD-WAN are part of a full range of services and subscriptions to help you simplify and make the most of your SD-WAN deployment with the lowest total cost of ownership (TCO) possible.

The Path Toward WAN Edge Consolidation

Using Fortinet Secure SD-WAN, network engineering and operations leaders can validate their application performance, cloud connectivity optimization, security posture, and operational costs of the WAN edge. They can also use it to plot a path toward:

- 1. WAN edge simplification:** Fortinet Secure SD-WAN consolidates point products to simplify branch infrastructure. This enables bandwidth-constrained network teams to facilitate the transition to SD-WAN.
- 2. WAN TCO reduction:** Fortinet Secure SD-WAN reduces WAN costs while providing better security at the edge (e.g., use of direct internet connections, application awareness for bandwidth management, automation, etc.). Indeed, Fortinet Secure SD-WAN delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.¹
- 3. Overall business agility:** A Fortinet Secure SD-WAN Assessment Report can help network engineering and operations leaders to target specific problem areas with existing branch infrastructure to facilitate the transition to SD-WAN implementation.

Fortinet Self-Healing SD-WAN enables better user experience for business-critical applications on any WAN transport while reducing cost. Intuitive SD-WAN Orchestrator significantly simplifies WAN operations with automation and sophisticated analytics. As the only vendor, with a purpose-built Secure SD-WAN ASIC, Fortinet achieves the industry's best security compute rating.



www.fortinet.com

Copyright © 2021 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 General Counsel, 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. 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.