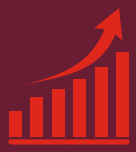
FORTINET

WHITE PAPER

Three Use Cases For Transforming Branches With Fortinet Secure SD-WAN

Executive Summary

Digital transformation (DX) of traditional branch networks offers several advantages for distributed enterprises. Many organizations are switching from performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures that offer faster connectivity, cost savings, and other benefits. But SD-WAN has its own challenges. Fortinet Secure SD-WAN offered as a feature integrated into industry's leading Next Generation Firewall, powered by industry's only SD-WAN ASIC improves application performance, higher performance, and better cost efficiency. Accurate application identification ensures complete visibility and control with SD-WAN business policies to provide best user experience for critical real-time and collaboration applications. Integrated security provides advanced protection against all threat landscapes. Three common uses cases show how Fortinet enables the full benefits of an SD-WAN architecture without sacrificing security.



With more than 21,550 SD-WAN customers, Fortinet leads the market with Secure SD-WAN innovations and fastest growing vendor with over 300% YoY growth.

Businesses strive to achieve security sensitive WAN edge to protect application data with faster cloud-on-ramp for SaaS applications.[2]

Introduction

Traditionally connectivity to external world for businesses meant a single dedicated service provider-based access for all application needs. Though expensive, control and securing this connection has been manageable while providing access to critical resources. This technology/infrastructure has severe implications on reliable access to external resources due to single point of connectivity often subject to outages. In addition, higher bandwidth demands by growing number of users and traffic intense applications cause more disruptions and experience high latency.

While this process (known as "backhauling") is secure, it also greatly slows network performance. With rapid increase in cloud applications, including SaaS such as google and voice /video conferencing, it makes more sense to access them on public internet instead of sending to an already burdened centralized office. This has translated to businesses aiming to augment their connectivity with multiple providers or more affordable broadband and other means of internet connectivity.

Software-defined WAN solution has evolved to make application intelligent business decisions on hybrid WAN links, including service provider, broadband, and LTE. Accurate application identification, visibility into network performance, and reliable switchover of application traffic between best performing WAN links have pivoted SD-WAN as the most sought-after WAN technologies by businesses across all verticals. Even after SD-WAN adoption, businesses kept sending all their sensitive and critical applications traffic to datacenters for security purposes or were forced to install a sophisticated firewall solution to inspect their direct internet access. This added another point product for security, making the network more complex, challenging to manage and delayed cloud adoptions.[1]

SD-WAN Challenges

But while SD-WAN offers inherently faster and cheaper connectivity than traditional WANs, it is not a panacea on its own. Despite its transformative capabilities for branch networks, several challenges must be addressed to fully articulate and actualize SD-WAN's potential:

Poor User Experience. Digital innovations has increased the demand for SaaS and UCaaS applications which require multi-cloud access. Traditional WAN network has limited access or a backhauled connectivity through datacenters to such critical applications. This creates a high latency WAN links which adversely affects user experience.

Lack of visibility. SD-WAN solutions typically lack visibility into applications at the branch level. This can lead to Shadow IT problems, including SaaS applications (unauthorized applications that may introduce security and/or compliance risks), as well as bandwidth limitations from branch users wasting bandwidth on nonessential applications (e.g., Pandora, YouTube).

Complexity. In addition to the other types of complexity that DX technologies introduce, SD-WAN architectures can be difficult to troubleshoot and hard to manage across all the branches. Most solutions do not offer a single management interface for consolidated network oversight and control across all of the enterprise's remote locations. This adds to the burden on limited IT staff and often creates defensive gaps for threats to exploit.

Security. Without the centralized protection provided by backhauling traffic through the data center, moving from MPLS to direct internet broadband connections exposes organizations to new risks—especially considering that cyberattacks are growing in both number and sophistication. Effective SD-WAN implementation requires additional security within the enterprise infrastructure to secure those connections and inspect high volumes of traffic—all without inhibiting network performance.

To address these challenges, one approach to effective SD-WAN implementation combines both networking and security functions in a unified solution. The Fortinet **Secure SD-WAN** solution can be enabled on **Fortinet NGFWs.** FortiGate combines NGFW and SD-WAN features into a single solution that improves both WAN efficiency and security. It provides efficient protection across all branch outposts by providing consistent policy enforcement with single-pane-of-glass management. It also allows enterprises to mitigate risks associated with DX. Three common use cases demonstrate how Secure SD-WAN can solve key enterprise challenges while enabling greater business value for organizations.

Use Case: Improve Application Experience

Businesses kept sending all their sensitive and critical applications traffic to datacenters for security purposes or were forced to install a sophisticated firewall solution to inspect their direct internet access.[4] This added another point product for security, making the network more complex, challenging to manage and delayed cloud adoptions.

The need to integrate SD-WAN, security and networking functionalities on a single appliance made absolute sense to reduce network complexity, associated costs, and ease of management.[5]

This allowed businesses to displace their multiple point products with a powerful appliance at a reduced cost and ease of management using a centralized console. A strong security posture offered businesses to send their cloud applications on more affordable, low latency direct internet reliably with optimal application performance and best user experience. Continued network performance health checks ensured the best available WAN link was chosen based on user-defined application service level agreements and remediate network degradation with fail-over of traffic to a better performing WAN link. Intuitive business policy work flows make it easy to configure and manage the application needs with the flexibility of prioritizing business critical applications.

As part of the Fortinet Security Fabric, a Fortinet NGFW with Secure SD-WAN provides advanced security features for protecting direct internet access. This includes comprehensive threat prevention, such as web filtering, anti-malware, and intrusion prevention (IPS). It also encompasses threat detection, such as SSL-encrypted traffic inspection, and sandboxing via FortiSandbox integration.

Visibility and control are also important considerations for SaaS adoption across an extended branch workforce. Individual employees can easily install cloud-based applications without the involvement or approval of IT management. This form of Shadow IT can directly introduce malicious threats to branch networks, create gaps in security, and even violate compliance with privacy laws and industry regulations if left unchecked. Secure SD-WAN supports full application visibility and control through several key features:

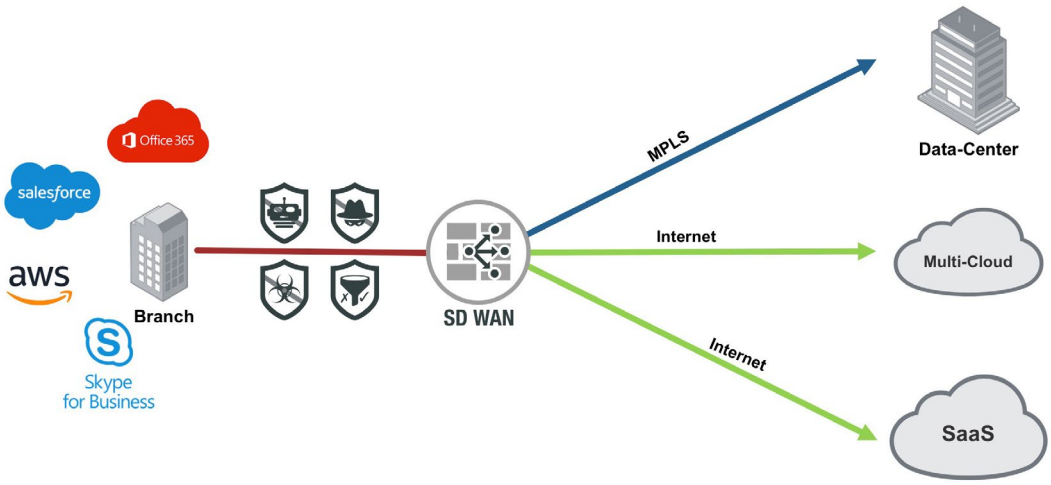


Figure 1: A FortiGate featuring secure SD-WAN can transform enterprise branch architectures.

Broad application awareness. FortiGate's application database supports more than 5,000+ application signatures, it provides accurate detection of such critical real-time applications. This level of application visibility enables systems administrators to define business policies with precise service level agreements for network parameters (latency, packet loss and jitter) because the SD-WAN solution automatically ensures that the best possible WAN link is chosen for traffic forwarding. New applications—including encrypted and cloud application traffic—can be identified and classified via an optional **FortiGuard Security Subscription Service.** Fortinet NGFWs can receive ongoing threat-intelligence updates from FortiGuard Labs researchers for more efficient application routing as well as real-time threat protection.

"…the areas of primary differentiation for SD-WAN products are quality of experience (QoE) for VoIP and video performance."

Automated multi-path intelligence. Fortinet Secure SD-WAN continuously monitors those connections, so should bandwidth conditions degrade for a given application, Fortinet Secure SD-WAN can seamlessly switch to a better performing WAN link – without any impact on application delivery. And in a worst-case scenario, where all WAN links are degraded, it can remediate these network conditions with advanced techniques such as forward error correction.

Maintaining high-quality performance for communications applications is especially important for regional branches and remote offices that rely on collaborative interaction for productive operations. In their 2019 SD-WAN Group Test Results, NSS Labs measured the quality of experience (QoE) of VoIP and video application performance offered by different SD-WAN solutions. Fortinet Secure SD-WAN received top marks for both VoIP (was the highest score) and video QoE and an overall "Recommended" rating.

Compliance tracking and reporting. Secure SD-WAN-enabled tracking and reporting helps ensure adherence to privacy laws, security standards, and industry regulations while reducing collateral risks of fines and legal costs in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. They also monitor firewall policies and help automate compliance audits. The **Fortinet Security Rating Service** provides best practices for compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and other regulations. As part of the service, organizations receive their own security posture score and are then able to compare that to the scores of their peers.

Use Case: Accelerated Cloud Access

Digital innovation is the key initiative for many distributed enterprises across all major sectors. Organizations are adopting a cloud-first strategy with 83% of the enterprise workloads estimated to run in the cloud by end of 2020. Yet, as more applications such as Office365 and Salesforce move to the cloud, the traditional approach of backhauling traffic over legacy WANs to the data center has become an obstacle, resulting in a poor cloud application experience.

Leveraging Fortinet Secure SD-WAN for cloud on-ramp to SaaS and multi-cloud improves the user experience for business applications. With integrated advance security, the enterprise branch security posture remains strong even with direct internet access to the cloud. Managing edges, cloud and SaaS applications through single-pane-of-glass management reduces the cost and complexity of the branch.

Multi-cloud access for business continuity. Fortinet Secure SD-WAN is available as a hardware appliance, as a network function virtualization (NFV) for on-premises deployments, and as a virtual appliance in Amazon Web Services (AWS), VMware Cloud, Azure, Google Cloud, Oracle, and Alibaba Marketplaces. The Secure SD-WAN solution assures accelerated connectivity to Software-as-a-Service (SaaS) applications as well as applications located in major public cloud providers globally. Deeply integrated with Azure Virtual WAN, Secure SD-WAN can be automatically set up, is ease of use, and provides visibility across the entire distributed infrastructure.

Remote VPN overlay connectivity. Virtual private networks (VPNs) are used to ensure a secure remote network connection by creating a protected "tunnel" over a less secure network transport (e.g., the public internet). One of the reasons for SD-WAN's popularity is connected to the cost-performance benefits of internet-based VPNs with the performance and agility of MPLS VPNs.

Fortinet Secure SD-WAN provides native management of remote VPN connectivity to allow organizations to maintain appropriate levels of security protection and inspection, while ensuring high levels of visibility and control. This applies not only to data and applications passing through the SD-WAN environment but also across the entire distributed network.

For an organization with many remote locations, high-performance scale for virtual VPN overlay is another critical feature of secure and effective SD-WAN. VPN overlays typically feature multiple layers of these network tunnels per branch. When multiplied across an

organization with a large number of branches or remote locations, network performance can degrade. Fortinet NGFWs feature powerful, purpose-built security processors (SPUs) that accelerate performance and scalability for high-volume virtual VPN overlay.

Use Case: Simplify with Centralized Management and Control

Many enterprise branches may want to simultaneously replace both their WAN and LAN devices in favor of a solution with deeper integration and simplified branch operations management. Using separate WAN and LAN infrastructures not only increases branch complexity (more devices to deploy and update with multiple management consoles). It also reduces visibility and control of operations while increasing the opportunities for security gaps that hackers can exploit.

Single-pane-of-glass management. Fortinet enables customers to focus on digital innovations and make network more agile. Fortinet offers intuitive Secure SD-WAN orchestrator as part of its Fabric Management Center. This allows customers to significantly simplify centralized deployment, enable automation to save time and offer business centric policies.

Fortinet Secure SD-WAN offers enhanced analytics and new SD-WAN reports with Fabric Management Center. Single console and rich SD-WAN analytics helps customers to fine-tune their business and security policies to improve quality of experience for all their users.

Users also see a need for WAN solutions that effectively integrate with local wireless LANs in the branch and IoT applications being deployed. This means an opportunity of convergence and deeper integration between the WAN and LAN platforms used in the branches."

A **software-defined branch (SD-Branch)** model eliminates these challenges by unifying WAN and LAN operations within a single solution. As an extension of the Fortinet Security Fabric, a Fortinet NGFW featuring Secure SD-WAN integrates with FortiAP and FortiSwitch solutions using a special FortiLink protocol. This enables customers to manage local endpoints (such as IoT devices) connected to LAN and automatically quarantine devices showing indicators of compromise. Fortinet-enabled SD-Branch deployments (Figure 2) provide deep WAN/LAN integration, simplicity, security, and the lowest TCO in the industry.

Zero-touch deployment. Deploying SD-WAN should also be as easy as turning on a feature—and this is exactly what Fortinet Secure SD-WAN zero-touch deployment offers. New branches can be quickly connected and secured with little expertise and no additional overhead. Fortinet simplifies infrastructure and delivers SD-Branch operations with consolidated WAN/LAN functions and advanced security features. No other vendor is able to provide this combination of capabilities.

Enhanced analytics for WAN link availability, performance SLA and application traffic in run-time and historical stats allow Infrastructure team to troubleshoot and quickly resolve network issues. Fabric Management Center offers advanced telemetry for application visibility and network performance to achieve faster resolution and reduce the number of IT support tickets. On-demand SD-WAN reports provides further insight into threat landscape, trust level and asset access which are mandated for compliance purposes.

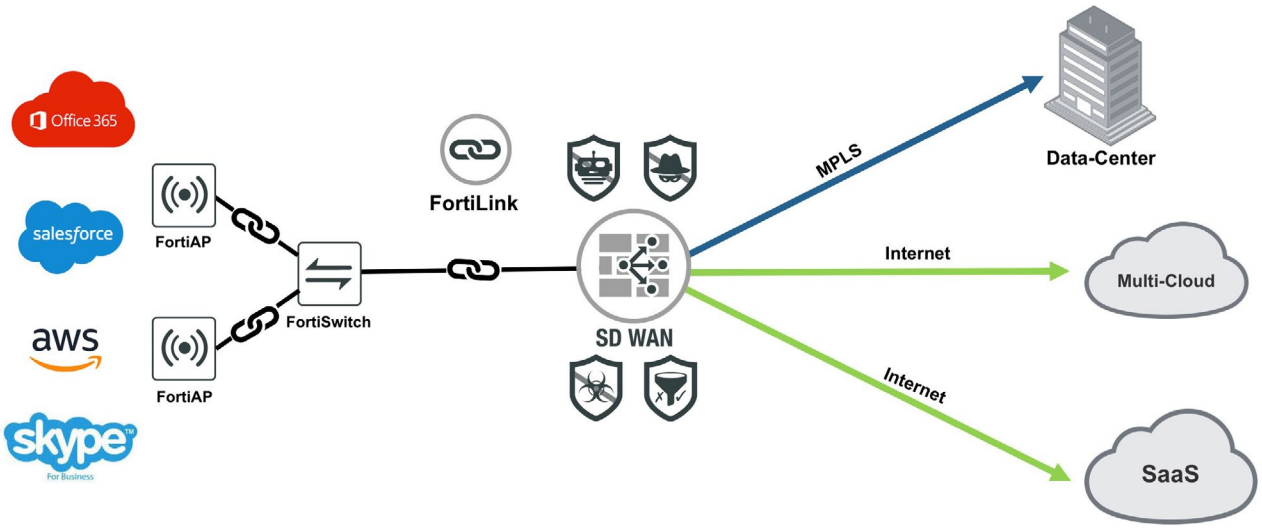


Figure 2: The Fortinet High-level SD-Branch model consolidates WAN and LAN infrastructures.

Realizing the Benefits of SD-WAN

With continuing growth in SaaS, VoIP, and video applications, SD-WAN can help distributed enterprises embrace the benefits of DX without bottlenecking network performance or impacting the productivity of end users.

The performance and security challenges that often come with SD-WAN are solved by Fortinet Secure SD-WAN—a native component of the Fortinet Security Fabric and the Fortinet NGFW. Secure SD-WAN allows organizations to rapidly adopt cloud applications while keeping security a top priority. It helps reduce OpEx costs while maintaining high-quality performance for VoIP, video, and VPN. It also simplifies the branch network infrastructure by combining networking and advanced security in a single, unified solution.

[1] "SD-WAN Infrastructure Market Poised to Reach $5.25 Billion in 2023", IDC, July 2019.

[2] "SD-WAN Should be a Feature, Not a Stand-Alone Solution," NetworkWorld, May 2020.

[3] "Fortinet Leads the Market with Secure SD-WAN Innovation," May 2020.

[4] "Learn more about a Fortune 500 customer that achieved a 65% cost reduction," Fortinet, Apr 2020.

[5] "Fortinet Secure SD-WAN receives a second consecutive "Recommended" rating in NSS Labs report," Fortinet July 2019.

May 26, 2020 10:00 PM

344544-A-0-EN

D:\Fortinet\White Paper\red white paper\RED - Refresh - 3 use cases for transforming breaches\wp-FA-three-use-cases-for-transforming-branches-5262020\wp-FA-three-use-cases-for-transforming-branches-5262020