CASE STUDY

SD-WAN Improves Global Corporation's WAN Performance, Management, and Visibility

Fortinet, a Fortune 500 company, is expanding rapidly. Since its initial public offering (IPO) in 2009, Fortinet's share price has increased 1,244%, nearly three times as much as its closest competitor.[1] Fortinet has grown physically as well, with a 172,000-square-foot building currently under construction near its headquarters in Sunnyvale, California, a new office in Valbonne, France, and expanding operations at its state-of-the-art data center in Burnaby, Canada.

Fortinet is a global leader in security-driven networking, with 21,000 of its customers implementing its Fortinet Secure SD-WAN (software-defined wide-area networking).[2] It behooved the company to serve as a center of excellence for secure SD-WAN as it adapted its own SD-WAN technology to support its business expansion.

> *"The new Fortinet WAN edge architecture makes management much easier since IT teams at remote sites do not need to work across time zones."*
>
> – *Nathan Ladd, SD-WAN Solutions Architect, Fortinet*

Details

Customer: Fortinet

Industry: Technology

Location: Sunnyvale, CA

The New Fortinet Global Network Architecture

Like its enterprise customers, Fortinet needs a wide-area network (WAN) that provides world-class security while maintaining network performance that meets application service-level agreements (SLAs) and delivers excellent user experience. As Fortinet stands up new sites and increases its use of Software-as-a-Service (SaaS) applications for core business needs, making the transition to SD-WAN throughout its network was a logical step.

As a result, the Fortinet global WAN is currently undergoing a significant redesign. In the past, the Fortinet network used an array of point-to-point IPsec virtual private network (VPN) solutions to ensure secure communication between its sites. The redesigned Fortinet WAN uses a new, hub-and-spoke VPN design and leverages the capabilities of Fortinet Secure SD-WAN at all hub and remote locations.

Simplifying Fortinet IPsec VPN Infrastructure

A crucial first step in building the new Fortinet global WAN was redesigning the VPN model. The current array of point-to-point IPsec VPNs was difficult to maintain and did not scale well to new locations.

Instead of point-to-point VPNs, each Fortinet branch office connects to two of five VPN hubs located at Fortinet's major sites (Figure 1). Smaller sites route their traffic through local hubs, dramatically decreasing the complexity and number of IPsec VPN links in the Fortinet corporate WAN.

Use of the Secure SD-WAN functionality, which is included in the FortiGate next-generation firewalls (NGFWs) that were already deployed at each of the hub and remote sites, is critical to the success of Fortinet new VPN architecture. Each of the five hubs maintains four IPsec VPN tunnels over two internet service providers (ISPs) to each of the other hubs for business resiliency. Traffic over these four channels is load balanced using SD-WAN to ensure high-performance, reliable, and secure connectivity throughout the Fortinet WAN.

Hub-and-spoke VPN Improves Operational Efficiency

The array of point-to-point IPsec VPNs that Fortinet used previously allowed it to implement a secure, global WAN over broadband internet. However, by redesigning its VPN architecture to a hub-and-spoke model, Fortinet reaps several benefits.

These point-to-point VPN tunnels limited visibility into the organization's network infrastructure. Many of these connections could be between remote sites with limited or no on-site network support. By transitioning to a hub-and-spoke model, Fortinet dramatically improved visibility into its network infrastructure by ensuring that every IPsec VPN link has a major site at one end, and that the majority of traffic flows over a finite number of hub-to-hub links.

Additionally, the use of point-to-point VPN connections between Fortinet sites made connecting new branch locations complex. Each new site required a new VPN link to be created to every other location. With the new hub-and-spoke model, connecting a new site only requires configuring links to two hubs, dramatically increasing the scalability of the Fortinet WAN. The reduced complexity of the VPN architecture decreases new site configuration time from 15 hours to 3 hours per new site. With one to two new sites being added each month, Fortinet saves about 216 staff hours per year, an 80% reduction.

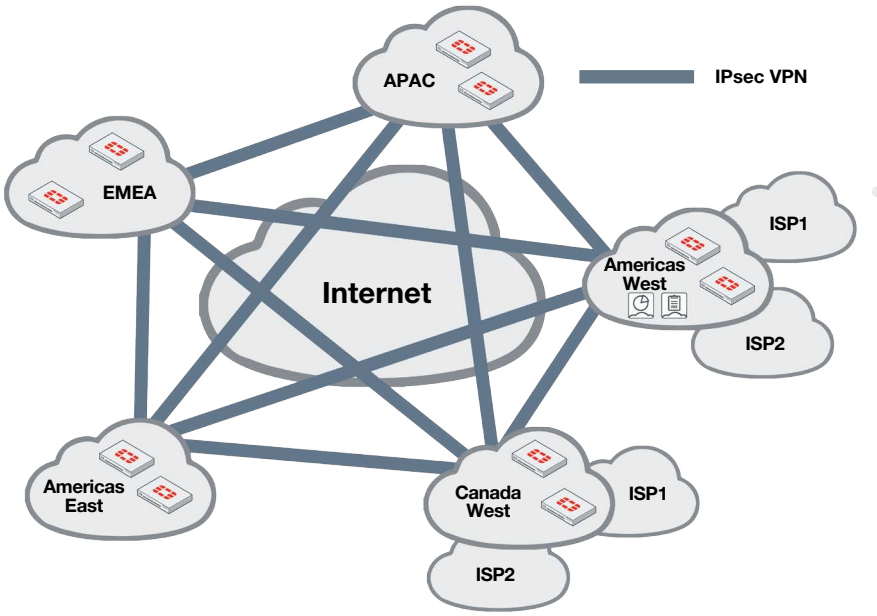
Solutions

- FortiGate
- Fortinet Secure SD-WAN
- FortiAnalyzer
- FortiManager

"Deploying SD-WAN throughout our corporate WAN also enables Fortinet to centralize visibility and management of our networking and security architecture across all of our sites. It is really exciting to see the Fortinet technologies in action."

– *Rick Huang, Senior Director Information Technology, Fortinet*

With point-to-point VPN connections, troubleshooting issues with the link are performed by the networking teams at each endpoint, which can be in very different time zones. According to Nathan Ladd, an SD-WAN solutions architect at Fortinet, "The new Fortinet WAN Edge architecture makes management much easier since IT teams at remote sites do not need to work across time zones." An access request to add or modify a route or firewall setting now takes half an hour. This is down from two hours in the previous configuration, resulting in an additional annual savings of 81 staff hours when dealing with the four to five requests that are made each month—a 75% reduction.



Core VPN Mesh

Fortinet's 5 primary sites in interconnected VPN mesh. Each site has 2x ISPs. Blue lines represent 4x load-balanced VPN tunnels.

Figure 1: Redesigned Fortinet VPN network uses a hub-and-spoke model to decrease complexity.

Leveraging SD-WAN Throughout the Fortinet WAN

Beyond leveraging Fortinet Secure SD-WAN to optimize links between global hubs, Fortinet also began to take advantage of the full capabilities of Secure SD-WAN at its smaller sites. Most of these sites use two or more ISPs for their internet connections and have been using intelligent routing, WAN link load balancing, and direct-to-internet steering of recreational traffic for some time. SD-WAN is also used to intelligently load balance internal traffic from remote sites to one of two VPN hubs to increase network resiliency and reduce congestion at the hubs.

Benefits of SD-WAN for the Fortinet Global WAN

The VPN redesign significantly simplified the architecture of the Fortinet IPsec VPN deployment and enabled more centralized visibility and management as a result. However, the majority of the benefits of Fortinet's redesign of its corporate WAN stem from the activation of SD-WAN functionality on FortiGate NGFWs across the organization.

Fortinet did not previously use multiprotocol label switching (MPLS) links for its WAN; however, if it had, the impact of switching to broadband internet optimized by SD-WAN would have been significant. Based off a price of $15 per Mbps for broadband internet and $300 per Mbps for an MPLS link,[3] Fortinet would save $399,000 per year in networking costs due to its transition to SD-WAN in 28 sites with an average of 50 Mbps per branch.[4 5]

Since the majority of Fortinet locations are served by at least two ISPs, each site's network connectivity is extremely resilient, as the IT team can switch between different ISPs as needed. "Secure SD-WAN allows us to automate load balance and failover between different ISPs, improving performance and decreasing latency during outages," says Ladd. With as many as 1,500 employees at one location, an ISP outage that required 30 minutes to detect and remediate would cause a productivity loss of 750 staff hours. In the case of just a few outages per year, the operational impact would be dramatic. However, with automated failover between two ISPs, the impact of such an outage is nonexistent.

Business Impact

- 80% reduction in time required to configure each new WAN deployment
- 75% reduction in ongoing WAN edge maintenance time
- Estimated 95% operational savings compared to use of MPLS bandwidth
- Potentially thousands of staff hours saved due to automated load balancing
- Centralized visibility and policy management for distributed branch-office networks for the first time

"SD-WAN allows us to automate load balancing and failover between different ISPs, improving performance and decreasing latency during outages."

– George Zeng, Senior IT Manager, Fortinet

Next-level Performance with Fortinet Solutions

As part of the transition to SD-WAN, Fortinet's branch locations have activated SD-WAN interfaces within their FortiGate NGFWs. Now, FortiAnalyzer solutions deployed at Fortinet's major sites have visibility into the network infrastructure of these remote sites. According to Rick Huang, senior director of information technology at Fortinet, "By activating SD-WAN interfaces across our global locations, we were able to achieve centralized visibility into those locations for the first time." Working in concert with FortiAnalyzer, FortiManager enables single-pane-of-glass policy management of the SD-WAN infrastructure throughout the Fortinet global WAN.

The FortiGate NGFWs deployed throughout the Fortinet WAN integrate both networking and security functionality, including an NGFW, SD-WAN appliance, router, and WAN optimization. By using a FortiGate instead of layering standalone appliances, Fortinet saved an estimated $7,880 in hardware and setup costs if these appliances had not already been in place.[6] Additionally, with 28 Fortinet sites currently under SD-WAN management, Fortinet saves an estimated $99,218 per year in support and management costs by using a FortiGate NGFW instead of multiple standalone appliances for each location.[7]

Finally, by deploying Secure SD-WAN across its global WAN, Fortinet creates an enterprise-scale, real-world testing environment for its products. By activating more of the features of Fortinet products on its own network, Fortinet gains additional real-world data about how they operate at scale and can more efficiently identify and correct bugs. This also allows Fortinet to build reference architectures and use-case examples for its customers, backed with real-world data and insights from its own network.

Enhanced Performance with Fortinet Secure SD-WAN

As Fortinet transitioned to a new hub-and-spoke architecture for its IPsec VPNs, leveraging Secure SD-WAN within its deployed FortiGate NGFWs made perfect sense. SD-WAN enables Fortinet to load balance traffic across multiple IPsec tunnels between VPN hubs and

provide integrated security and intelligent application traffic routing at the network edge. "Deploying SD-WAN throughout our corporate WAN also enables Fortinet to centralize visibility and management of our networking and security architecture across all of our sites," Huang sums up. "It is really exciting to see the Fortinet technologies in action."

[1] Stock performance as of March 31, 2019, posted on the Fortinet website.

[2] Tobias Mann, "Fortinet Leapfrogs Cisco With 21,000 SD-WAN Customers," SDxCentral, December 17, 2019.

[3] These numbers are averages based upon internal Fortinet research.

[4] 23 branch locations plus 5 VPN hub locations.

[5] ($300 – $15)*(50 Mbps)*(28 sites) = $399,000

[6] This saving is based on the comparative pricing of Cisco standalone solutions and FortiGate NGFWs with integrated SD-WAN and WAN optimization: $2,500 (Firewall) + $3,000 (SD-WAN) + $2,500 (Router + WAN Optimization) – $650 (Fortinet Secure SD-WAN) = $7,350. It additionally assumes staff-hour savings of $530 per branch location (28 in total) due to reduced effort in Secure SD-WAN setup for a total of $7,880 per branch location.

[7] These savings are calculated based off of the assumption that support costs are 40% of purchase price for Cisco appliances: $2,500 (Firewall) + $3,000 (SD-WAN) + $2,500 (Router + WAN Optimization) = $8,000 and 45% of purchase price for Fortinet Secure SD-WAN ($650). Additionally, each branch is assumed to save $636 in annual SD-WAN maintenance costs for a total savings of (28 sites): 40% of $8,000 for Cisco – 45% of Fortinet Secure SD-WAN ($650 + $636) = $99,218.

January 17, 2020 8:10 AM

545113-0-0-EN

D:\Fortinet\Case Study\Fortinet on FortiGate Secure SD-WAN\cs-sdwan-improves-global-corporations-wan-performance-mgmt-and-visibility-V2-1172020-810AM