FORTINET

# How Federal Agencies Can Maximize Benefits From a Move to SD-WAN

## Choosing the Right Solution Makes SD-WAN More Secure

# Table of Contents

# Executive Overview

Federal agency leaders looking to replace multiprotocol label switching (MPLS) with software-defined wide-area networking (SD-WAN) technologies typically evaluate products along three key dimensions: performance, cost, and manageability. These are certainly important considerations, but they cannot be evaluated in isolation.

Security considerations impact each of these areas. One possible response to security concerns is to deploy a next-generation firewall (NGFW) along with each SD-WAN solution, but this approach can lead to additional challenges. Instead, agency leaders are better off looking for secure SD-WAN solutions that combine networking and security functionality. The challenge is to find a solution that minimizes costs and required staff resources, while maximizing performance of network traffic. The solution research process helps agency leaders find the right fit.

# Introduction: Security Is Central in SD-WAN

Encouraged by the Enterprise Infrastructure Solutions (EIS) contract from the U.S. General Services Administration (GSA), IT leaders in many federal government agencies are determining whether the time is right to upgrade their MPLS network infrastructure. They are considering the advantages SD-WAN offers in terms of network performance. They are also running cost comparisons, which are generally favorable for SD-WAN, even if transitioning to SD-WAN means running the new technology side by side with the legacy MPLS network for some period of time. Finally, they are looking at the manageability of SD-WAN compared with MPLS.

In their due diligence on networking options, agency leaders must not lose sight of the security ramifications of each solution. Many agency end-users communicate highly sensitive and highly valuable data via the WAN. Moreover, uninterrupted access to key applications may be critical to the agency's ability to fulfill its mission. The security functionality built into the typical SD-WAN solution may not provide adequate protection. For example, many SD-WAN solutions lack intrusion prevention system (IPS), web filtering, and secure sockets layer (SSL) inspection, among other security features.

The virtual private network (VPN) connections utilized in an MPLS approach are inherently more secure than the public internet on which SD-WAN networking relies. A well-constructed SD-WAN infrastructure can overcome agency leaders' security concerns, but getting there requires careful solution research. The good news: The performance, cost, and manageability benefits make pursuit of a secure SD-WAN solution well worth the effort.

Here are three use cases for deploying secure SD-WAN networking under the EIS contract. The key to success is finding the right combination of cost, speed, manageability, and security.

# A well-constructed SD-WAN infrastructure can overcome agency leaders' security concerns. Getting there requires careful solution research.

# Section 1: Integrated NGFW Security at the Network Edge

To ensure their data and applications are effectively protected, many federal agencies moving to SD-WAN deploy new NGFWs along the network edge. The NGFWs will detect and respond to known threats and will include advanced security features that protect against unknown, emerging threats. They generally include sophisticated functionality that is missing from some standalone SD-WAN solutions, including IPS and SSL deep packet inspection. For this reason, agencies often pair each SD-WAN appliance with an NGFW.

Unfortunately, this approach can be expensive; every network entry point requires both the SD-WAN appliance and a firewall. Another downside to this approach is that it may substantially increase the staff time required to manage network security.

In some cases, the agency's networking team manages the SD-WAN solution, while a separate security team manages the NGFW. Even when the same team handles both solutions, the products typically come from different vendors, and they cannot be managed through a single console. Staff must collect and consolidate threat information across the solutions. This may consume a significant amount of time that would be better spent on more strategic activities. Worse, relying on humans to coordinate threat response across disparate networking and security products might also slow the organization's reaction time when a threat is detected.

That is why agencies considering moving to SD-WAN should look for a secure SD-WAN solution that incorporates industry-leading security functionality into the networking device itself. This approach reduces costs because the agency has fewer pieces of hardware to buy. Better yet, it can provide a single-pane-of-glass management view, reducing time spent on network management and accelerating threat response. Security for SD-WAN is most robust when a secure SD-WAN solution integrates tightly with the network's advanced threat protection solutions, such as sandboxing, to uncover encrypted threats hiding within SSL traffic.

**Security for SD-WAN is most robust when a secure SD-WAN solution integrates tightly with the network's advanced threat protection solutions to uncover encrypted threats hiding within SSL traffic.**

# Section 2: Support for Digital Innovation

Many agencies are undergoing digital innovation (DI). Staff require access to an array of Software-as-a-Service (SaaS) solutions and other cloud-based applications hosted on public and private cloud platforms. In many cases, these DI solutions incorporate bandwidth-intensive video or voice functionality. While this trend enables agency employees to access technologies they would not otherwise have, it also greatly increases traffic volume at the network edge, across campuses, and between branches throughout the agency. Thus, DI often leads to unacceptable levels of latency on the legacy MPLS network, which drives interest in shifting to higher-performing SD-WAN.

Secure SD-WAN solutions offer federal agencies a safe way to provide high-performance cloud access that supports DI. In fact, the right secure SD-WAN solution will enable an agency to adopt an increasing number of SaaS and other cloud applications without incurring a noticeable reduction in application performance.

A key criterion to consider in researching secure SD-WAN solutions is the effect of advanced threat protection on the performance of cloud applications that users access via the network. In some SD-WAN solutions, turning on deep inspection of SSL-encrypted traffic slows network throughput, inhibiting the performance of DI applications. When this happens, users may look for ways around the security settings that are slowing down their application performance, such as IPS functionality. In the end, the agency's IT staff may turn off critical security settings in order to keep users happy.

This is a compromise the IT team should never have to make. A secure SD-WAN solution with purpose-built high-performance security processors will be able to support typical network traffic demands with only minimal (if any) latency, even when all the security team's desired options and settings are turned on.

**In some SD-WAN solutions, turning on deep inspection of SSL-encrypted traffic slows network throughput, inhibiting the performance of DI applications.**

# Section 3: Streamlined Network Management for Distributed Branches

Federal agencies with numerous remote branches often struggle to find staff to deploy and manage the network edge in each location. Security staff are especially scarce, due to a large and growing global gap in cybersecurity skills.

The number of unfilled cybersecurity positions worldwide is expected to reach 3.5 million by 2021.[1] "There's not enough capability to go around," says the director of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.[2] The problem, of course, is that some of the same agencies grappling with a cybersecurity skills shortage are also considering adding an SD-WAN solution and a separate NGFW in each branch location.

Finding a solution that combines SD-WAN functionality and NGFW protections in a single device is especially critical for agencies with multiple locations that are facing a skills shortage. Such a consolidated solution minimizes staff time required for deployment, configuration, and management of both networking and security capabilities.

Agencies with many different locations should also look for consolidated SD-WAN and NGFW solutions that offer zero-touch deployment and centralized configuration management. Regarding SD-WAN specifically, device-level application steering is critical to avoid the risk created by centralized network orchestration as a single point of failure. At the same time, for distributed device management to be efficient, staff must be able to perform key deployment and update tasks remotely. Such capabilities enable security-focused staff to roll out and configure new solutions without having to travel to each branch to do so. Staff efficiency considerations like this one are key to minimizing the total cost of ownership (TCO) of the SD-WAN deployment.

# Staff efficiency considerations are key to minimizing the TCO of the SD-WAN deployment.

# Conclusion: Undertaking Thorough Due Diligence

As federal agency IT leaders reevaluate their network infrastructure in the transition to the EIS contract, they need to dedicate time and energy to the solution research process. Agency leaders need to find SD-WAN solutions that will keep crucial data and applications secure while providing high network performance to support DI applications. A secure SD-WAN platform must also provide all of the support needed for the agency to continue running its legacy applications. In particular, it should offer adequate throughput to support any Voice-over-IP (VOIP) and unified communications technologies the agency is running.

At the same time, agency leaders need secure SD-WAN solutions that will minimize TCO and the drag on precious security staff resources from deployment and management of networking and security solutions.

Federal agencies have many networking options to choose from. The benefits are large enough to demand a thorough and careful due-diligence process.

**Agency leaders need secure SD-WAN solutions that will minimize TCO and the drag on precious security staff resources from deployment and management of networking and security solutions.**

[1] Michelle Moore, Ph.D., "Inside the Government Cybersecurity Landscape: Federal vs. State Level Challenges," Tripwire, May 1, 2019.

[2] Jack Corrigan, "DHS Cyber Chief is Ready to Update Federal Tech Hiring," Nextgov, April 4, 2019.

FORTINET

www.fortinet.com



424425-0-0-EN

November 14, 2019 3:29 PM

eb-federal-agencies-sd-wan