CHECKLIST

Why Fortinet Performance and Security Are the Right Choice for Federal Agencies Transitioning to SD-WAN

Security needs to be front and center for any federal agency that decides to upgrade its network infrastructure for the General Services Administration's (GSA's) new Enterprise Infrastructure Solutions (EIS) contract. To improve throughput on the network edge, many agencies are considering transitioning from a legacy multiprotocol label switching (MPLS) environment to software-defined wide-area networking (SD-WAN).

As they think through their options, agency leaders need to make sure to balance their performance needs with security, cost, and manageability concerns.

5 Reasons to Select Fortinet Secure SD-WAN to Protect Federal Agency Networks

The FortiGate Secure SD-WAN solution is a natural choice for agency leaders. Fortinet security solutions are certified by ICSA Labs, Virus Bulletin, and AV-Comparatives, and they receive top ratings from leading third-party reviewers. For example, NSS Labs has "recommended" all nine Fortinet solutions it has tested, and Fortinet is the only vendor that NSS Labs recommends for SD-WAN that also has a security rating.[1]

Here are five key reasons why agency leaders transitioning away from MPLS are choosing FortiGate Secure SD-WAN:

☑ Protection against known and unknown threats

FortiGate next-generation firewalls (NGFWs) are best in class, providing Layer 7 security that integrates advanced threat protection, intrusion prevention system (IPS) functionality, web filtering, and application control. These capabilities are built into FortiGate Secure SD-WAN solutions, so an agency leader deploying FortiGate Secure SD-WAN automatically has access to advanced protection at the network edge.

Agencies might achieve the same level of security by deploying both an NGFW and a stand-alone SD-WAN solution at each network entry point. However, implementing a solution that integrates both types of functionality saves money, reduces staff time on rollout and ongoing management, and facilitates a coordinated response of the security infrastructure to any detected known threats.

For emerging threats, a secure SD-WAN solution needs to tie in with threat intelligence. At FortiGuard Labs, one of the industry's largest teams of security experts continuously studies the threat landscape to identify previously unknown malware. FortiGate Secure SD-WAN solutions leverage this market-leading intelligence, and integration of FortiGate and FortiSandbox technologies enables the isolation and testing of any network traffic that raises concerns.

☑ 100% coverage of TIC security requirements for distributed branches

FortiGate NGFWs have been at the heart of multi-agency and single-service Trusted Internet Connection Access Provider (TICAP) solutions for more than a decade. Thus, the security requirements defined in Trusted Internet Connections (TIC) memorandum M-19-26 are native functionality for the FortiGate Secure SD-WAN solution. Agencies looking to deploy FortiGate Secure SD-WAN per the approved TIC 3.0 use case can be assured that they will be implementing tried-and-true technology, drastically improving time to value for their new architecture enhancements, and speeding up the approval process.

☑ Coordinated threat response

Because FortiGate Secure SD-WAN solutions are an integral part of the Fortinet Security Fabric, they can share data in real time. Anytime a threat is detected, the other solutions in the agency's heterogeneous Security Fabric are immediately aware of the threat. Not only that, but they can respond in a coordinated manner, reducing the chance that a threat thwarted at one network entry point will successfully breach the network somewhere else.

☑ Optimized performance

With some firewalls, turning on advanced security features creates latency for network traffic. In contrast, FortiGate Secure SD-WAN appliances feature purpose-built security processing units (SPUs) that minimize performance degradation, even when IPS and other advanced features are enabled. For virtual or white-box deployments of FortiGate Secure SD-WAN, the new Fortinet virtual SPU (vSPU) architecture accelerates security performance in public and private clouds, or on hardware from a third-party provider.

This performance optimization is crucial for agencies that rely on video Software-as-a-Service (SaaS), Voice-over-IP (VoIP), or other cloud applications that require high throughput. By minimizing latency, FortiGate Secure SD-WAN provides an effective channel for agency communications.

☑ Better manageability

The tight integration of Security Fabric technologies—both from Fortinet and from third-party partner organizations—streamlines security activities for agency IT teams. Single-pane-of-glass management across FortiGate Secure SD-WAN solutions, NGFWs, endpoint protection, and other security technologies enhances visibility into threats and the resulting organizational response. It also minimizes security management demands on IT staff.

For agencies with many geographically dispersed offices, the virtual networking and zero-touch deployment available in FortiGate Secure SD-WAN solutions provide even greater benefits. Staff do not have to travel to remote offices to deploy or update their networking or security technologies. This reduces total cost of ownership (TCO) networkwide.

Conclusion: Why FortiGate Secure SD-WAN Is the Prudent Choice

The EIS contract is a perfect opportunity for federal agency IT leaders to make the move to SD-WAN. Performance, cost, manageability, and leading-edge security make FortiGate Secure SD-WAN solutions the perfect choice for this transition.

Integrating FortiGate Secure SD-WAN solutions with advanced threat protection from FortiSandbox and other elements of the Fortinet Security Fabric gives federal agencies data center-quality protection at every entry point along the network perimeter. Moreover, the Security Fabric approach lets agencies move first to SD-WAN networking, then incrementally add security capabilities over time.

[1] "Certifications," Fortinet, accessed September 9, 2019.

FORTINET

www.fortinet.com

November 22, 2019 7:57 AM

323490-0-0-EN

D:\Fortinet\Checklist\SD WAN_Checklist EIS Transition\cl-why-fortinet-performance-and-security-are-the-right-choice-for-federal-agencies-v1