FORTINET

WHITE PAPER

More Efficient Federal Agency Networks, Without Security Holes

Why Agencies Adopting SD-WAN in EIS Transition Must Keep Security Front and Center

Executive Overview

The Enterprise Infrastructure Solutions (EIS) contract from the U.S. General Services Administration (GSA), valued at $50 billion over 15 years, presents an excellent opportunity for federal agencies to improve their telecommunications infrastructure. Many agencies' IT leaders are taking advantage of this opportunity to augment traditional networks built on multiprotocol label switching (MPLS) connections.

Replacing MPLS-based network connections with software-defined wide-area networking (SD-WAN) technologies—now an approved Trusted Internet Connections (TIC) use case, per Memorandum M-19-26—can lead to faster performance for network traffic and applications, as well as lower costs. However, SD-WAN solutions can open an agency to new security concerns. It is imperative for federal agency IT leaders to ensure that traffic over direct internet connections, tied into the network via SD-WAN solutions, is just as secure as the traffic that is currently routed through a telecommunications provider's MPLS backbone.

60% of federal IT executives see cloud computing as a pathway to improving their agency's mission-critical services.[1]

Benefits of Modernizing a Federal Government Agency

Federal IT leaders are under pressure to support the same types of digital innovation (DI) initiatives as their private-sector peers. Some agencies are harnessing self-serve and automation technologies to dramatically reduce the paperwork and busywork that employees deal with day to day.[2] Others are undertaking DI to facilitate collaboration with other agencies to better serve their citizens.[3]

Moreover, like nearly every other entity, many federal agencies are taking advantage of cloud technologies to reduce costs and boost organizational agility. Increasingly, federal employees are utilizing bandwidth-intensive video and Voice-over-IP (VoIP) technologies in the course of their jobs. A recent survey of federal IT executives revealed that 60% see cloud computing as a pathway to improving mission-critical services.[4]

Internet-of-Things (IoT) technologies are also gaining a foothold in federal agencies.[5] These technologies offer a wide array of options for improving the efficiency and effectiveness of government entities. For example, for several years, the Department of Defense has been using radio frequency identification (RFID) chips to more accurately monitor movement of goods through its supply chain.[6] The U.S. Geological Survey uses IoT-enabled sensors to track bacteria in the nation's rivers and lakes.[7] Even the GSA has long utilized IoT technologies to confirm the energy efficiency of buildings that are labeled as "green."[8]

These innovations offer opportunities to simultaneously improve the information that supports agency decision-making and reduce staff time spent collecting and collating that data. Refusing to move forward is no longer an option. The challenge for many agencies is that cloud and IoT solutions may significantly increase an agency's need for bandwidth—and secure connectivity—beyond the walls of the data center.

Barriers to Innovation

Many agencies face three key impediments to modernization:

1. Obtaining funds for strategic IT investments is often challenging for federal agencies.[9]
2. Risk aversion can reduce IT leaders' willingness to experiment with new technologies.
3. When federal policy changes, oversight entities may be slow to provide guidance that agencies need in order to understand how to proceed.

United States government agencies spent $90 billion on IT in fiscal year 2019.[10] However, only a small proportion of this spending went to major improvement initiatives. In the typical agency, between 75% and 80% of the IT budget was spent on operations and maintenance of legacy systems that are rapidly becoming obsolete.[11]

Reportedly, some agencies are still using IT systems with components that are 50 years old.[12] Worse, in a 2018 study of a dozen different industries, government was revealed to be the sector with the highest level of "technical debt"—in other words, the amount of money it would take to upgrade legacy systems.[13] Such patterns of technology investment impede modernization and limit agencies' ability to meet current and future organizational needs.

75–80% of the IT budget in the typical federal agency was spent on operations and maintenance of legacy systems that are rapidly becoming obsolete.[14]

The transition to the EIS contract is a "tremendous opportunity to modernize the IT infrastructure."[17] It is an opportunity that federal agency leaders cannot afford to ignore.

EIS Transition Reduces Frictions That Inhibit Innovation

Fortunately for agency IT leaders struggling under a great deal of technical debt, the GSA's new EIS contract opens the door to change. The contract leverages the bulk purchasing power of the U.S. government to help agencies improve their telecommunications and networking infrastructure, and to adopt modern networking technologies. By offering substantially lower costs on communications solutions, the EIS contract reduces the friction that may prevent federal agency leaders from attempting to undertake transformative technology initiatives. Moreover, the need to transition and recompete communications and related technologies, which are covered by the EIS contract, may motivate some agencies to step back and recompete their entire IT infrastructure.

Modernization of the IT networking infrastructure is an explicit goal of the program. In late 2018, the GSA extended the deadline for agencies to transition to the EIS contract, from May 2020 to May 2023. However, to qualify for the extension, an agency must incorporate plans to modernize its network.[15]

Agencies facing perpetually tight IT budgets may find they finally have the funds to innovate by deploying technologies available through EIS or by moving to a managed-services model in which IT upgrades can be paid for as operational expenditures (OpEx) rather than out of the capital expenditure (CapEx) budget. Government officials see the EIS contract as a way to help large numbers of small agencies modernize. Many federal IT leaders are responding by considering options such as replacing T1 lines with satellite, cable, or wireless communications technologies. Others are evaluating the benefits of a more incremental approach, making modest changes that the agency can build on over time.

Either way, the transition to the EIS contract is a "tremendous opportunity to modernize the IT infrastructure," according to the GSA Blog.[16] It is an opportunity that federal agency leaders cannot afford to ignore.

Performance and Cost Considerations Point to SD-WAN

As opportunities to modernize federal agency networks dovetail with agency leaders' need to support cloud and IoT technologies, many are evaluating the benefits of replacing some MPLS connections with SD-WAN technologies.

Traditionally, federal agency WANs have utilized MPLS links to connect remote offices to headquarters. An MPLS backbone supports virtual circuits between network endpoints, creating a secure channel for communications between agency locations, to cloud-based applications, or with remote IoT devices. The MPLS connections route all agency network traffic through the agency data center, where it is inspected by the core security infrastructure.

MPLS networking raises two primary issues for federal IT leaders. First, the hub-and-spoke architecture of a WAN utilizing only MPLS connections reduces the perceived performance of cloud applications at remote sites, compared with direct internet access (DIA). The problem worsens when growth in traffic creates bottlenecks in network security devices. It is not uncommon, or particularly surprising, to hear federal workers complain that their internet connection is slower at work than at home.

The other key concern for federal IT leaders is that MPLS links are expensive. Agencies on tight budgets that are looking to modernize need to consider the cost differential between MPLS connections and DIA. Direct connections can significantly reduce the cost of the network overall, while increasing the performance of cloud and related applications.

SD-WAN May Be the Solution

Many agencies that are frustrated with the performance problems and cost of MPLS connections are drawn to the idea of using direct internet connections for dispersed branches, then tying these remote locations into the agency network via SD-WAN technologies. In this, agency IT leaders reflect the attitudes of many of their counterparts in the private sector, where SD-WAN adoption is brisk. Because SD-WAN links use DIA connections, they provide better performance for the agency's applications and data than a hub-and-spoke architecture that relies on MPLS connections.

SD-WAN uses much more reasonably priced public broadband connections such as 4G/LTE, reducing its cost. Furthermore, because SD-WAN solutions improve the speed that users experience in cloud-based software, they support growth in an agency's implementation of Software-as-a-Service (SaaS) solutions, which improves the predictability of spending on all sorts of functionality by moving IT expenses from the CapEx to the OpEx budget.

Standalone SD-WAN Requires Strengthened Security

For agencies transitioning to the EIS contract and leveraging SD-WAN, security is typically the biggest drawback. An MPLS connection is a virtual private network (VPN), which is inherently more secure than the public internet channels through which SD-WAN traffic travels. Although MPLS traffic is not encrypted, MPLS is considered a secure transport mode. Moreover, because MPLS traffic runs through data-center firewalls and other data-center security solutions, it is subjected to a higher level of scrutiny than traffic passing through a basic SD-WAN solution and thus bypassing the data center.

Standalone SD-WAN solutions generally provide some level of security, but many lack data-center-quality protections, including intrusion prevention system (IPS) technologies and the ability to inspect SSL-encrypted traffic. Such security gaps may inhibit an SD-WAN solution's ability to detect known threats. Attackers are increasingly encrypting their malware to slip past entry-level security. Deploying an SD-WAN solution with weaker security than that in the data center may inadvertently allow encrypted malware onto the agency network.

Some SD-WAN solutions also lack capabilities necessary to detect and respond to advanced, unknown threats. They may fail to connect to a well-regarded threat-intelligence service, which would give them up-to-the-minute information as emerging threats are identified. They may lack sandboxing capabilities, which would isolate prospective threats and determine the risk they pose before introducing them to the network.

If an agency deploys an SD-WAN solution that does not have security built in, it may find itself in a situation where disparate networking and security tools at different points of the network perimeter fail to communicate or to coordinate on threat response. Such information silos can inhibit visibility and security controls, potentially hindering the agency's ability to roll out cloud solutions for its stakeholders.

Agencies on tight budgets that are looking to modernize need to consider the cost differential between MPLS connections and DIA.

"According to our latest forecast, end-user spending on SD-WAN is expected to grow from $475 million in 2017 to $2.32 billion by 2022, at a five-year compound annual growth rate of 37.4%."[18]

"As the world becomes more interconnected and complex, and as cloud and IoT devices become part of the federal landscape, federal agencies need to be thoughtful and smart about how they combat the threats that are actively targeting them."[19]

TIC Opens Up to SD-WAN

Through late 2018, the TIC initiative from the federal Office of Management and Budget (OMB) prevented use of SD-WAN because it required all agencies' internet traffic to be routed through custom TICs, a Trusted Internet Connection Access Provider (TICAP), or a Managed Trusted Internet Protocol Services (MTIPS) connection.

That began to change in December 2018, when the OMB announced that it would begin adding TIC Use Cases that allow for new means of connectivity.[20] One of the use cases for the recently released TIC 3.0 guidance now allows SD-WAN to support connectivity between an agency's headquarters and remote offices. This use case enables agencies to directly connect approved traffic to the internet via SD-WAN networking, and to push security out to the edge or branch office.

This option may be a boon to the performance of agency networks, but inclusion of this use case in TIC 3.0 does not guarantee that an SD-WAN infrastructure will keep data secure. As a federal agency's attack surface expands, through migration to the cloud, IoT deployment, and other changes, the risks multiply. In 2017, 57% of government IT leaders reported a data breach; that number is up dramatically, from 34% in 2016.[21] SD-WAN solutions that are not adequately secured open the agency to a very real risk. Without IPS, sandboxing, and other advanced security technologies, SD-WAN solutions are less likely to detect threats designed to infiltrate agency networks and steal data or cause other harm.

57% of government IT leaders reported a data breach in 2017.[22]

"Agencies need to keep their foot on the gas to ensure they have time to transition their telecom services from their existing contracts and providers to EIS."[23]

Incremental Modernization

Time is of the essence for agencies taking advantage of the EIS contract to upgrade their network infrastructure. Even those that receive the extension until 2023 may be feeling pressure to move their IT procurement to the new contract in time. Nevertheless, it is important to keep in mind that changes to a network do not need to take place all at once.

Solutions implemented now, in the EIS transition period, can be expanded over time. An agency may roll out an SD-WAN network immediately, then add new layers of security as the budget and drive to modernize allow. For example, sandboxing technologies may be out of scope for the initial network modernization initiative, but the agency may be able to add them in another year or two.

The only factor limiting such an expansion of network security is the type of SD-WAN solution that the agency initially installs. To give themselves the flexibility to continue their incremental progress toward modernization, federal IT leaders need to make sure the SD-WAN solution they select fits snugly into a larger security architecture that they may eventually be able to fully implement.

Conclusion

The transition to the EIS contract is a forced moment in time, but it is also a great opportunity for federal agency IT leaders to consider shifting their network infrastructure from traditional MPLS links to less-costly and lower-latency SD-WAN solutions. Due to the continuous growth in threats, security must be at the forefront of agencies' IT planning processes.

Likewise, it is crucial to evaluate networking solutions in the context of both those solutions' current security offerings and their ability to integrate into a broader security fabric. Doing so ensures that the agency is getting the best possible network security in the short term, while maintaining an opportunity to expand protections into the future.

Moving a federal agency to a new networking technology is a massive undertaking. To ensure that such a shift is worth the time and effort, federal IT leaders must perform thorough due diligence with an eye toward the potential for incremental improvements. Doing so will increase the potential for innovating securely and cost-efficiently.

[1] "Federal Cloud Readiness Report," FedScoop.

[2] "How Digital Transformation Is Revolutionizing Government," Forbes, March 29, 2019.

[3] Ibid.

[4] "Federal Cloud Readiness Report," FedScoop.

[5] Tom McAndrew, "Breaking down the barriers to an IoT-enabled government," GCN, November 26, 2018.

[6] Max Meyers, et al., "Anticipate, sense, and respond: Connected government and the Internet of Things," Deloitte Insights, August 28, 2015.

[7] Ibid.

[8] Ibid.

[9] Dr. Gregory S. Dawson, "A Roadmap for IT Modernization in Government," IBM Center for The Business of Government, 2018.

[10] "IT Acquisitions and Operations—High Risk Issue," Government Accountability Office.

[11] Dr. Gregory S. Dawson, "A Roadmap for IT Modernization in Government," IBM Center for The Business of Government, 2018.

[12] "IT Acquisitions and Operations—High Risk Issue," Government Accountability Office.

[13] David McClure, Ph.D., "Decouple to Innovate: How federal agencies can unlock IT value & agility by remediating technical debt," Accenture, 2018.

[14] Dr. Gregory S. Dawson, "A Roadmap for IT Modernization in Government," IBM Center for The Business of Government, 2018.

[15] Mark Rockwell, "GSA extends EIS deadline to 2023," FCW, December 6, 2018.

[16] Bill Zielinski, "Agencies Have Four Years to Transition to Our Enterprise Infrastructure Solutions (EIS) Program," GSA, Office of Information Technology Category, March 14, 2019.

[17] Ibid.

[18] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[19] Jim Hansen, "The Role of SIEM Tools in Your IT Security Operations," Government Technology Insider, February 14, 2019.

[20] "Update to the Trusted Internet Connections (TIC) Initiative," Office of the Federal Chief Information Officer.

[21] "Modernizing Federal Agency IT and Security with GSA's Enterprise Infrastructure Solutions (EIS) Contract," Fortinet, September 11, 2018.

[22] Ibid.

[23] Bill Zielinski, "Agencies Have Four Years to Transition to Our Enterprise Infrastructure Solutions (EIS) Program," GSA, Office of Information Technology Category, March 14, 2019.

FORTINET

www.fortinet.com

Copyright © 2019 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.

October 29, 2019 7:54 PM

415436-0-0-EN

D:\Fortinet\Work\2019\October\102919\wp-efficent-agency-security