How Your Agency Can Modernize Using Secure SD-WAN

MARKET TRENDS REPORT

govloop FORTINET

Introduction

Federal IT departments have long been the gatekeepers of technology — deciding which applications employees could download and what devices they could connect to the network. But that all changed in recent years as tech-savvy employees, armed with mobile devices and the ability to easily download cloud-based apps from the internet to do their jobs, began charting their own paths to acquire IT resources.

Although this move seemingly empowered individuals, the shift also put a greater strain on the security of agencies' networks and created a hodgepodge of old and new applications that were too complex to properly manage. This scenario has played out at scale across multiple remote offices, in various locations throughout different agencies.

To overhaul this collection of homegrown systems, agencies are seeking to modernize and consolidate legacy IT networks. Governmentwide, secure network modernization is a significant component of the current administration's overarching efforts to move agencies away from costly and insecure technologies to more modern solutions.

But efforts like these don't come without challenges, including increased security complexity and lack of visibility as the attack surface expands. To meet these and other issues associated with modernization, agencies are eyeing a software-defined approach to managing wide area networks (SD-WAN) — one that gives them greater flexibility to centrally manage network connections among remote offices in a secure, cost-effective and transparent manner.

To better understand the network modernization challenges agencies face today and why software-defined wide area networks are critical to addressing them, GovLoop partnered with Fortinet, a leader in providing secure SD-WAN, on this report. In the following pages, you'll learn how SD-WAN supports federal initiatives such as Trusted Internet Connections (TIC) and migration to the new General Services Administration's (GSA) Enterprise Infrastructure Solutions (EIS) contract. You will also hear about the benefits of SD-WAN from Felipe Fernandez, Director of Systems Engineering for Fortinet Federal, and Nirav Shah, Senior Director, Product Marketing at Fortinet

BY THE NUMBERS

Network Modernization & SD-WAN Adoption

50

secure, external internet connections is the target set by the Office of Management and Budget (OMB) for agencies to reduce access points under the Trusted Internet Connections initiative.

Source: Report to the President on Federal IT Modernization

40%

of enterprises are expected to adopt SD-WAN by the end of 2019.

Source: Gartner

"Agencies will gain greater visibility and resilience against more sophisticated attacks, including insider threats that may have access to agency-owned networks by enhancing protections closer to the data."

Source: Report to the President on Federal IT Modernization

"Many organizations are eager to adopt new SD-WAN capabilities. However, technology managers must find SD-WAN solutions that meet the needs of both digital applications and secure cloud connectivity."

Source: Fortinet

$50 billion

is the valued amount of GSA's Enterprise Infrastructure Solutions contract.

Source: GSA

$1.79 billion

is what agencies spent on network and telecommunications services in fiscal 2016 under the General Services Administration's (GSA) legacy Networx contract.

Source: Report to the President on Federal IT Modernization

THE CHALLENGE
Managing Complex and Costly Federal Networks

Agencies are under mounting pressure to adopt digital and cloud-based tools that enhance workforce productivity and improve citizen services. These rising expectations come at a time when the roughly $88 billion federal IT budget is poised to remain relatively flat, if the president's 2020 budget proposal is any indication of what's to come.

The resource-intensive applications that today's mobile and remote workers need — such as video, voice and collaboration tools — put a strain on bandwidth and the already overburdened agency networks that face a barrage of cyberthreats daily. While acquiring IT resources, individual branches and departments have operated in a manner that has only exacerbated the issue.

"As governments built their IT networks and acquired IT assets, there was a lack of accountability or even software capability to keep track of a rapid deployment of IT on networks," Fernandez said. "That also lent itself to the shadow IT problem, where individuals who had a procurement capability were acquiring assets without even telling their leadership."

Oversight of these activities fell by the wayside to keep pace with IT demands. And the current environment of disparate hardware and software makes troubleshooting network issues all the more challenging, Shah said. Simple fixes now may take days or weeks, hindering mission-critical and time-sensitive work.

"Meanwhile, agency officials are overseeing the migration of traditional networks to direct internet services, and they face growing concerns about securing data and devices on the public network," he said.

IT officials need to ensure that new networking solutions and internet access are compliant with strict government and agency regulations, such as those set by the National Institute of Standards and Technology (NIST) and the Homeland Security Department (DHS). Agencies need to implement solutions that have built-in security — without hindering critical business operations — all while limiting downtime and reducing costs.

But not all agencies are located near prime internet hubs. Some are in very remote locations that have few options in terms of what's available for WAN or an internet service provider.

Ultimately, modernizing the telecommunications environment is limited by what's available in that area and the technical expertise of staff to deploy modern networks in the cloud.

THE SOLUTION
A Software-Defined Approach to Networking

With the escalating adoption of bandwidth-hungry SaaS applications, agencies must rethink their WAN strategies and how they can deliver secure, modern and cost-effective networking capabilities. Agencies need a software-defined approach to delivering and managing WANs.

Traditional WAN allows agencies to ensure distributed remote locations maintain seamless network access as digital demands increase. But agencies need WAN solutions that improve efficiency and enhance security to keep pace with greater demands on the network and increased cyberthreats.

That's where SD-WAN comes in. For example, Fortinet's Secure SD-WAN uses a software-based service that runs on a single platform and includes routing, critical network functions and applications (such as voice, video, Wi-Fi and internet) and comprehensive network security. Those functions also need to be seamlessly integrated into today's complex distributed networks, including multi-cloud. SD-WAN enables users to securely connect to cloud resources.

With SD-WAN, agencies have greater visibility and management across their network environments, access to an integrated security infrastructure, reduced WAN operating expenses and applications that are more reliable, robust and secure. One of the reasons is that SD-WAN separates networking hardware from its control mechanism — giving agencies greater flexibility to adapt to network changes.

The technology also frees agencies up from focusing on routing and how packets of data traverse the network to business outcomes and accessibility to mission applications.

BEST PRACTICES

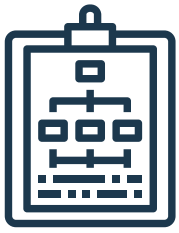
Implementing SD-WAN

I. Take a holistic approach

Holistically identify and classify the types of branch locations across your agency, such as main headquarters or remote locations. From there, determine what unique networking needs those branches have and what form factor would be best to address those issues.

"Maybe they require what we call universal customer premises equipment, or uCPE for short, which is a white box solution that can leverage or host virtual solutions from other vendors or even open source software to provide secure SD-WAN capability," Fernandez said.

As you determine the needs of each branch, keep in mind that SD-WAN provides the application automation and agility required to simplify network operations but lacks integration with other branch devices. Solutions such as those offered by Fortinet do, however, enable customers to extend SD-WAN to SD-Branch by using secure access point and switches.



2. Review options for managing solutions simultaneously

Does the solution you're considering allow you to deploy, configure and monitor all of your networking solutions at the same time on an enterprise scale? When you need to make rapid changes, quickly mitigate threats or when upgrades need to occur, a mature SD-WAN solution will support these activities. You must also consider the underlying software used to support your SD-WAN and whether it can do so at an enterprise scale.

3. Make security a priority upfront

There are dozens of SD-WAN providers on the market, and agencies must do their due diligence to ensure that security is not an afterthought when adopting the technology. Organizations are increasingly adopting direct internet access in their SD-WAN deployments, raising security concerns and new challenges for chief information security officers.

"Most SD-WAN vendors support basic capabilities, such as stateful firewalling and VPN; however, they depend on security partners for advanced functionalities such as intrusion prevention system, malware analysis and sandboxing," according to Gartner. Work closely with your SD-WAN provider to ensure that security capabilities are fully integrated in the solution.

4. Collaborate with a trusted partner

As agencies work to enhance network operations, having a trusted partner that understands the importance of secure, well-managed networks is key.

Fortinet's solution equips leaders with single-pane-of-glass visibility and management across modern environments, in addition to integration, automation and proactive threat intelligence-sharing in real time. It also reduces complexity with simplified management and enhanced visibility.

SD-WAN Use Cases

TIC 3.0

One example is the TIC initiative, which is intended to enhance network security across the federal government by consolidating and reducing the number of external network connections. But for many agencies, TIC became an impediment as they sought to access cloud services via the internet. OMB draft guidance to update TIC assumes that each remote office is separate from its agency's headquarters but utilizes HQ for most of its services, including generic web traffic. SD-WAN supports this initiative by providing agencies and their remote offices reliable, and in Fortinet's case, secure capabilities to access cloud services.

Integration with other security solutions

As agencies adopt SD-WAN, they should incorporate solutions that are able to integrate with third-party products and intelligence themes. Using Fortinet's Secure SD-WAN solution, agencies can reap the benefits of consolidated security features like client management and protection software. These capabilities position agencies to comply with NIST standards, the Comply to Connect (C2C) framework and more. The Defense Department (DoD) created C2C to serve as a formal framework for validating new devices, evaluating their compliance with DoD security policies and continuously monitoring these assets to ensure they remain in security compliance.

EIS adoption

SD-WAN is also expected to play a key role in agencies' transition from GSA's legacy contracts to its EIS contract by 2023. EIS transition leaders are under pressure to modernize their networks to support departmental goals, but the migration process exposes new security issues. They're up against an expanding attack surface, increased security complexity and rapidly changing threats as devices and networks move outside the four walls of the agency.

HOW FORTINET HELPS

Fortinet's Secure SD-WAN solution is the first to combine world-class, fully integrated security into an SD-WAN solution to meet the growing demands and requirements of today's connected federal agencies.

It is the only solution that provides a fully integrated SD-Branch solution where WAN, LAN and security functionalities can all be managed using a single management controller. FortiGate SD-WAN replaces separate WAN routers, WAN optimization and security devices with a single solution that is application-aware.

"Fortinet's Secure SD-WAN intelligently prioritizes the routing of applications across network bandwidth based on the specific application and user," Shah said.

It also offers multi-broadband support, improves application performance, reduces WAN operating expenses and minimizes management complexity.

For more information, visit www.FortinetFederal.com.

Conclusion

The adoption of cloud services and increasingly mobile workforces are accelerating advancements in WAN technologies. With enterprises directly accessing the internet, it's now vital to deploy next-generation security strategies and improve the performance of mission-critical applications.

Increasingly, organizations also realize that their SD-WAN solutions need to provide consistent security and management to meet compliance and business requirements.

As agencies continue down the path of digital transformation, SD-WAN will play a central role in delivering secure and reliant cloud-based services.

FORTINET®

ABOUT FORTINET

Fortinet secures the largest enterprise, service provider, and government organizations around the world. We empower our customers with intelligent, seamless protection across the expanding attack surface, and with the ability to take on ever-increasing performance requirements of the borderless network - today and into the future. Our federal solutions protect the classified and unclassified systems used by all 15 of the cabinet-level agencies, and those of numerous independent agencies, utilizing Fortinet's specially configured USG product line. These platforms comply with federal certification requirements including NIST FIPS 140-2, NIAP Common Criteria certification, and are on the Commercial Solutions for Classified Programs (CSfC) approved Components List.

Learn more at www.FortinetFederal.com.

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop