THE CRITICAL ROLE OF SD-WAN FOR DIGITAL TRANSFORMATION

Scoop News Group Report

How modern software-defined wide area networking gives agencies added agility and stronger security to manage the risks inherent in hybrid IT environments.

The demand for faster, more customer-focused and secure government service is driving greater adoption of digital tools to add more value to agency services. However, these tools require networks with higher bandwidth, scalability and flexibility than existing legacy network infrastructure may provide, and some organizations are struggling to keep pace.

In order to effectively and securely develop multi-cloud and hybrid IT environments, agency leaders will need to consider critical network upgrades — moving away from traditional wide area networks (WAN) and adopting newer software-defined networking (SD-WAN) solutions.

There have been significant changes to network technology over the past few years, and according to Gartner, SD-WAN is proving to be one of the fastest-growing segments of the network infrastructure.

While many network providers now offer SD-WAN solutions, not all SD-WAN is created equal, cautions Jim Richberg, Field CISO at Fortinet and former National Intelligence Manager for Cyber in the Office of the Director of National Intelligence. A best-of-breed SD-WAN solution, he says, "will tightly integrate networking, connectivity and security, meeting three needs at once."

"As agencies integrate more digital services, they are looking to tap into the dynamic connectivity of hybrid IT environments. Overlay security tools are no longer capable of adapting to these environments. When security is embedded into SD-WAN however, an organization's remote users, branch office users and their data centers will all use a common set of security policies and enforcement criteria."

Fortinet's SD-WAN solution is application aware: It can validate the user, inspect network traffic and ensure that a user is only connected to applications they are authorized to use. The ability to have that kind of insight and control is key to a zero-trust security approach."

- Jim Richberg, Fortinet

Quickening pace of change opens agencies to greater risk

2021 is proving to be a year when both public and private sector organizations are looking to reap the benefits of modern hybrid cloud networking, including lower costs, greater agility and stronger security.

In the midst of the COVID-19 pandemic, federal and state government leaders pushed to quickly approve investments that would support the remote workforce, acquiring online solutions like as-a-service platforms, voice and video applications and robotic process automation.

"The way secure connections are being created is as if employees were logging on from the office. But the reality is that with poor visibility across the network and inconsistent controls and security policies, a government issued device could get compromised within the home environment through vulnerable IoT devices such as baby cams and doorbells — or family members using personal applications, social media and gaming consoles," says Richberg.

Threat actors took advantage of these weakness, and in the second half of 2020 Fortinet saw ransomware instances coming in through the endpoint rise by 700%, swimming back upstream to the organization.

"Even with multifactor or endpoint security solutions, the reality is that organizations still don't know what is going on in the environment," he says.

Security risk management is a top priority

Digital transformation is enhancing the delivery of government services, but it is also bringing added cybersecurity risks and vulnerabilities for which federal and state government leaders need more modern detection and response strategies.

In May 2021, the White House signaled its support of stronger security controls embedded into IT enterprise networks by requiring federal agencies to implement a plan for a zero-trust security architecture within the year. And the National Association of State Chief Information Officers (NASCIO) continues to find its members placing cybersecurity and risk management at the top of their IT priorities list for 2021.

"With cyberthreats today, organizations can't afford to function as if the network and security are separate. These two functions are increasingly converged, and government agencies need an SD-WAN solution that is able to treat it as such," says Richberg.

5 KEYS TO SELF-HEALING, SECURE SD-WAN

1. **It goes beyond the branch.** Effective SD-WAN solutions can extend to home office and teleworker use and among distributed clouds.

2. **It offers intuitive orchestration and zero-touch deployments.** These features enable faster configuration rollouts at scale, often within minutes, of collaboration applications like VoIP, videoconferencing and SaaS apps.

3. **It prioritizes critical applications and enables self-healing WAN.** Able to identify a broad set of apps to meet all use cases, while advanced self-healing WAN automation provides a consistent user experience.

4. **It includes integrated security.** In true secure SD-WAN, networking, connectivity and security functions are tightly integrated into one solution meeting three needs.

5. **It offers comprehensive analytics and reporting.** It Uses enhanced analytics and compliance to help organizations gain visibility into network and application performance (both real-time and historical statistics).

The General Services Agency (GSA) shares this view, stating that WANs are increasingly unsuited to keep up with today's highly dynamic demands for bandwidth and connectivity. They issued a report in August 2020 providing an overview of SD-WAN in order to assist federal agencies in purchasing SD-WAN technologies under the Enterprise Infrastructure Solutions (EIS) contract task orders.

A key benefit of SD-WAN networking is that it supports zero trust strategies, including the ability to validate devices and users on the network, close visibility gaps in a hybrid environment and automate security policy updates across the network.

"For example, Fortinet's SD-WAN solution is application aware: It can validate the user, inspect network traffic to make sure its behaving as expected, and it can ensure that a user is only connected to applications they are authorized to use," explains Richberg. "The ability to have that kind of insight and control is key to a zero-trust security approach."

Choosing the wrong SD-WAN solution can inhibit an organization's ability to quickly adapt to changing demands and security concerns, Richberg maintains. Early versions of SD WAN technology focused solely on networking or offered ad hoc solutions to security. Implementing more modern and robust solutions — embedded with artificial intelligence and machine learning technology — gives agencies the ability to achieve a common operating picture of their networks and respond to threats more quickly, he explains.

"Data is the engine that fuels our 'fabric approach' to security and Fortinet is six generations into refining our algorithms and learning, based on the 100 billion security events we see daily," he shares.

Adding AI to policy-driven automation allows the system to validate users and deal with low level security anomalies automatically which frees agency employees to focus on those more complex tasks where they need to exercise their skill and judgement.

Forming trust partnerships to greater security

Since agencies live in a resource constrained world, Richberg advises that leaders look at the lessons learned in the private sector, where organizations have already taken on the work and risk of modernizing their networks.

"The Executive Order on security lays out a multitude of necessary tasks with aggressive timelines for completion. But if agencies try to do everything at once, they risk accomplishing nothing," cautions Richberg.

So, what are the early adopters in the private sector doing to try to solve networking and security challenges? They are investing in cloud and multi-cloud, software-defined networking, zero trust and secure remote access and leaning on partnerships to help them get there.

"The adversaries are, in some cases, certainly partnering to refine their attacks. So why should we be parochial and live in our stovepipes?" asks Richberg.

In his conversations with executives across the public sector, Richberg says he has seen the value agencies gain by working with trusted partners that can help with complicated tasks, such as security orchestration, and responses like advanced threat analytics and even Security Operations Center (SOC) as-a-service.

"Three main recommendations I would leave with any organization's leader are these: You can't protect what you don't understand; find a strategic advisor that can help you find creative ways to solve your problems; and don't try to reinvent the wheel when there are tried and tested solutions available to you," says Richberg

He adds that if your agency in interested in a product, ask for a proof-of-concept first to test it in your environment. In past cases, during this testing phase, Fortinet actually caught incoming ransomware attacks and quickly informed the organizations on changes that needed to be made immediately.

These testing periods can also prove to leadership the high return-on-investment possible in network upgrades, and help the organization build out a more holistic and secure network, he argues.

Learn more about why transitioning to secure SD-WAN is the right choice for government agencies.

This report was produced by Scoop News Group and underwritten by Fortinet and immixGroup.

FEDSCOOP

FORTINET

immixGroup