CASE STUDY

How Fortinet Improved Performance, Reliability, and Efficiency of the Pennsylvania Legislature's Core Network

The Pennsylvania Legislative Data Processing Center (LDPC) is the IT support structure on which the commonwealth's legislative business is built. The LDPC's services fall into three buckets, explains Jon Spinney, information security officer. "First, we manage the digital documents for all Pennsylvania bills as they move through the legislative process," Spinney says. "Then, once they pass as laws, we maintain that data as historical records. Second, we manage all the payroll data for the legislative body. And third, we are an MSP [managed service provider] for legislative state agencies."

Kye Kwon, supervisor of distributed systems for the Pennsylvania LDPC, adds, "We provide some services to all legislative state agencies, and for the agencies that are too small to have their own IT department, we serve as their IT team. Our services differ from agency to agency, but we typically run the network, provide desktop support, and support applications and email. We offer virtually all the same services that MSPs provide."

This means the Pennsylvania LDPC is crucial to ensuring that the business of the commonwealth gets done. "If we were to lose our network on a day that the Pennsylvania Senate or House of Representatives is in session, fire and brimstone would rain down," Spinney says. "Legislators' desks have buttons they push to indicate yea or nay, and those buttons are wired to the voting system, which we manage. If an attack brought that system down or resulted in network downtime, legislators could not vote on bills. So, the consequences would be dramatic."

UI, Support, and Price Make Fortinet the Clear Choice

Two years ago, the LDPC was grappling with network problems, and its firewall vendor was not particularly helpful in finding a solution. "Multiple showstopping issues were affecting the entire network at once, and the vendor could not figure out what was going on," Kwon says. "We had to frequently reboot the entire environment, and that went on for months and months while we waited for a response from the vendor. The reboots affected end-users' ability to get their jobs done. We clearly needed a new networking and security provider."

The LDPC team considered a plethora of options, approaching them with a broad range of decision criteria. "Cost was obviously a consideration," Kwon says. "But our primary concern was finding a vendor that is very strong in next-generation firewalls [NGFWs] and the technologies that come with that."

Ease of use was another key criterion, since the LDPC has only two network administrators. "We wanted a solution with a simple user interface [UI]," Spinney

"The increased visibility we have achieved through the combination of FortiAuthenticator and FortiClient gives us a better chance of catching malicious activity and reduces the time we spend troubleshooting. That accelerates our ability to respond."

Jon Spinney
Information Security Officer, Pennsylvania Legislative Data Processing Center

Details

Customer: Pennsylvania Legislative Data Processing Center

Industry: Government

Location: Harrisburg, Pennsylvania

Business Impact

- Increased chance of catching malicious activity due to streamlined processes and less troubleshooting
- Much lower downtime and higher performance across both LAN and VPN

explains. Excellent customer service rounded out LDPC's primary criteria. "Getting our legacy vendor to escalate major issues, particularly those that were bug-related, was incredibly challenging," Kwon reports. "Things that needed investigation never moved forward. We felt like a minnow in a sea of much larger fish that were getting more attention than we were, and that did not change no matter what level of support we purchased. We wanted a vendor whose customer service team would help us resolve issues quickly."

This combination of needs led the LDPC to hold proofs of concept with Fortinet and another company. The team found the NGFWs offered very similar features. "But the UI was a big factor tilting us toward Fortinet," Kwon says. "Both vendors' UIs were better than what we had, but we were more comfortable with Fortinet's UI. We found it easier to navigate and to enable certain features in the Fortinet interface."

Another decision factor was that Fortinet publishes online "cookbooks," videos with details on how to perform management and maintenance tasks within Fortinet solutions. "I do not think we have referenced any cookbooks thus far, but it is comforting to know that resource is available if we need it," Kwon says. "Also, some workflows made more sense to us in the FortiGate NGFWs. And all things equal, the FortiGates came in at a lower price point. That made the decision easy."

Streamlined Network, "Huge" Protections

The Pennsylvania LDPC engaged Trustlink to help design and implement a new network that revolves around FortiGate NGFWs and FortiSwitch secure Ethernet switches. "Trustlink was founded with a vision of being all-in on Fortinet as a value-added reseller, consultant, and integrator for Fortinet products and solutions," says Jon Kraft, the firm's founder and managing director. "Day in and day out, we are helping Fortinet customers get the most out of their investments and integrate Fortinet products."

Two months ago, the LDPC finished rolling out a high-availability (HA) pair of FortiGates in each of its two data centers. "We have two fault domains, each with an HA pair," Kwon explains. "We have secondary BGP [Border Gateway Protocol] peering set up across the two domains, so if one of our ISPs goes down, we can immediately start filtering traffic to the other ISP."

Within this architecture, the LDPC separated every Pennsylvania legislative agency into its own virtual LAN (VLAN) to prevent network traffic from moving laterally between agencies. "Everything is completely separated," Kwon says. "Each agency has its own unique set of firewall policies, and then we have an overarching external policy for everyone, depending on the traffic."

The FortiGates connect the data centers using Fortinet Secure SD-WAN, and they are protected by the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle. Spinney says the UTP bundle's distributed denial-of-service (DDoS) protection has been a game changer. "With our previous vendor, we did not have DDoS protection," he says. "Our ISPs offered to provide it, but that approach would not have given us a consolidated view. Having denial-of-service protection at the firewall level is huge."

More Reliable VPN, Better Visibility of Security Events

The LDPC team manages the FortiGates and FortiSwitches using the FortiManager enterprise management platform and FortiAnalyzer analytics solution. "The bulk

Business Impact (cont.)

- Performance issues with Microsoft Teams eliminated
- More availability of network team time for other projects, such as load-balancing initiative
- More reliable VPN provides better experience for remote users

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiClient

Services

- FortiGuard AI-Powered Security Services Unified Threat Protection Bundle

"We have seen an improvement in throughput with the FortiGates and FortiSwitches, and our network now has a lot less downtime than our legacy infrastructure did."

Kye Kwon
Supervisor, Distributed Systems, Pennsylvania Legislative Data Processing Center

of our configuration and policy adjustments happen in FortiManager," Kwon says. "FortiManager provides a central point from which we can push out policy and have it filter through the rest of the system."

A third-party security information and event management (SIEM) system pulls data from FortiAnalyzer in a way that was not possible on the LDPC's legacy network. "Our old firewalls exported to our SIEM, but they could not send all the information we needed," Spinney says. "The process would drop the most important data point because our SIEM was from a different vendor. So, we would have to research issues in the firewall logs rather than having it handy in a single pane of glass."

FortiAnalyzer has also improved the team's access to information about security events. "In our old system, reporting and logging were not intuitive and were very difficult to use," Kwon says. "Today, FortiAnalyzer consolidates logs across all our Fortinet devices, giving us immediate access to that information."

In fact, the team sees this consolidated management view as a key benefit of the transition to Fortinet. "With our legacy vendor, the UI had capabilities all over the place—so much so that adjusting some settings required the use of multiple applications," Kwon says. "That got tiresome, and it was even worse because the management applications were not reliable. By contrast, the Fortinet solution's single pane of glass makes our job much easier. We do not have to install three or four different applications just to manage the functions of one device."

> *"With our old solution, end-users had a lot of issues using Teams—I heard complaints all the time. But now, because Fortinet Secure SD-WAN helps Teams choose which ISP to send traffic through, I have not heard so much as a peep about performance issues with Teams."*
>
> **Kye Kwon**
> Supervisor, Distributed Systems, Pennsylvania Legislative Data Processing Center

To further streamline network and security management, the LDPC deployed the FortiAuthenticator user authentication solution and FortiClient endpoint management application. The agency is using FortiClient for multi-factor authentication (MFA) and VPN access, while FortiAuthenticator ensures that users are who they say they are. "Previously, we had a web-based VPN solution that was just not good," Kwon says. "FortiClient VPN has been much more reliable for our end-users." The tools gather identity context for all LDPC systems that connect to the network, so they enrich the Fortinet devices' logs with user information.

"If there is an issue, FortiAuthenticator and FortiClient enable us to see not just the IP address, but the user and device behind that issue," Spinney reports. "FortiClient also gives us visibility around whether specific clients are compliant with security policies, while FortiAuthenticator helps us restrict where users go within the network. The increased visibility we have achieved through the combination of FortiAuthenticator and FortiClient gives us a better chance of catching malicious activity and reduces the time we spend troubleshooting. We are no longer sending people on wild goose chases to find information. That accelerates our ability to respond."

Ease of Use Translates to Better Security

Although the Fortinet environment is still very new, it is already proving its worth. Security has improved significantly compared with the LDPC's legacy infrastructure. "Before, managing our firewalls was a challenge. We were constantly applying patches and hot fixes, struggling to keep things up to date," Spinney says. "We knock on wood every week, but we have not had a single issue since deploying the FortiGates."

Because the Fortinet environment is considerably easier to manage, the networking team can do their jobs better. "The UI's ease of use means the team that manages the firewalls is less likely to make mistakes," Spinney says. "And now, when someone wants to take malicious action on our network, we have more time to act because we get information so quickly with the Fortinet solutions. For example, when we were standing up FortiAnalyzer, we noticed that a couple of devices within LDPC were communicating with a C&C [command and control] server. That is something our previous solutions would not have been able to tell us."

Kwon says that over the past two months, the Fortinet solutions have started to improve staff productivity. "As we grow in familiarity with Fortinet, and get used to workflows through FortiManager and FortiAnalyzer, we will become considerably more efficient."

The LDPC will probably never reduce staffing on the team because it currently has just two network administrators, "and they need to be able to take vacations," Spinney points out. "But the Fortinet solutions' efficiency enables our team to get more done each day. They can take on more projects, such as a load-balancing project that is currently underway. In that case, our developers will have load-balancing capabilities sooner, which means they can develop more applications for the end users we support."

Reliability and performance are also up for both the LAN and the VPN. "We have seen an improvement in throughput with the FortiGates and FortiSwitches, and our network now has a lot less downtime than our legacy infrastructure did," Kwon says.

The company's experience with Microsoft Teams exemplifies the difference. "With our old solution, end-users had a lot of issues using Teams," Kwon says. "In bigger meetings, people joining from outside our domain would frequently drop off or experience slowness—I heard complaints all the time. But now, because Fortinet Secure SD-WAN helps Teams choose which ISP to send traffic through, we have had a lot of big meetings, and I have not heard so much as a peep about performance issues with Teams."

"The Pennsylvania LDPC team is now working with Business Communications Inc. (BCI), who acquired Trustlink, to determine how additional Fortinet solutions could further improve their network. They are considering the FortiNAC network access control solution and FortiAP secure wireless access points. "By leveraging more of the Fortinet infrastructure, we could lower total cost of ownership," Spinney says. "We are already reducing staff time spent moving between interfaces when managing the switches and firewalls, and we would like to expand those benefits with our access points, eliminating the need to log into another interface to manage the APs."

Eventually, he adds, the LDPC wants to move to zero-trust network access (ZTNA) "so that when users access the internet, FortiClient will automatically and securely link them. End users will love that, and we are working with Trustlink (BCI) to get it built."

May 20, 2025 2:23 AM / CS-69-0-0-EN