CASE STUDY

Propelling Research, Improving Efficiency, and Cutting Costs at University of South Carolina

Founded in 1801, the University of South Carolina system has eight campuses across the state, more than 50,000 students, and an annual budget in the billions of dollars today. The main campus in Columbia is recognized as one of the nation's top universities, with several of its undergraduate and graduate programs cited as number one in the country in various rankings. The university received $258 million in research grants in FY 2018 and has an endowment of $771 million.

Throughout 2017 and much of 2018, increased computing demand from campus researchers tested the capacity of the existing network and firewall infrastructure. The system suffered latency issues on a regular basis, frustrating students, faculty, and staff and impacting research projects. Worse yet, the network would occasionally become so overloaded that users were unable to access the network—once every three months or so during the worst stretch. "Each incident was different, but they all affected a large number of users," recalls Jason Boryk, the lead architect and manager of the university's network architecture team.

After they devoted significant effort tweaking the existing system to prevent these problems, it became clear to the network architecture team that the existing infrastructure would need to be replaced. "What we had was not acceptable for a research university," Boryk asserts. After meetings with internal stakeholders and university officials, the team began making plans to upgrade the university's Internet2 research network from 10 gigabits per second to 100 gigabits per second.

"The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams."

– *Jessie Hawkins, Systems Architect, University of South Carolina*

Details

Customer: University of South Carolina

Industry: Education

Location: Columbia, South Carolina, USA

Building a New Network

The team underwent a thorough planning process to build a state-of-the-art network backbone with robust security features built into the base architecture. "We did not want to just build the same network only 10 times bigger," explains Jessie Hawkins, a systems architect for the university. "Rather, we strove to follow current best practices and build a robust, secure network that will serve us many years into the future."

The infrastructure upgrade was concurrent with other technology changes that were in progress at the university. One pressing issue was that the on-premises data backup system was overloaded. "Our storage area network [SAN] was constantly at 97% of capacity, which is far more than recommended," Hawkins says. "Rather than spend millions of dollars on more SAN capacity, we decided that we would move our backups to a cloud repository in Amazon Web Services."

This change in the backup infrastructure was consistent with a university strategy that called for a gradual move to the cloud for most services. "In designing solutions for new applications and services, we are leveraging public and private cloud infrastructures to create a level of redundancy and stability that benefits an institution of our size," notes Boryk. "Our goal is to gradually move legacy services to the cloud as well. Long term, we hope to use the cloud for high-availability and disaster-recovery purposes."

Incorporating a Robust Security

As they searched for a security solution to protect the new infrastructure, the university's team knew that it must support both on-premises and cloud-based resources, including backups to AWS. They also hoped to find a way to integrate all of the elements of the security infrastructure for centralized visibility and control.

"We have services with Azure, Amazon Web Services, and Google Cloud Platform," Hawkins explains. "We were previously using the built-in security tools from each provider. The problem was that each tool worked a little differently. This meant that our small team had to specialize in three platforms, and the security team had to correlate security data from the three platforms manually."

In the last half of 2018, the team underwent proofs of concept from three next-generation firewall (NGFW) vendors that included Fortinet. "We tested the ease of configuration, the general user-friendliness of the interface, the accuracy of the vendors' claims about throughput, processing power, and different firewall features," Boryk says. "In short, we wanted a firewall solution that would scale to our current and future needs."

Selecting a Security Solution

FortiGate NGFWs quickly moved to the top of the list among the three major providers included in the proof of concept for several reasons. "Fortinet had, by far, the most scalable solution," Boryk begins. "Its native 100-gigabit interface was a perfect fit for our new infrastructure, whereas no other vendor had comparable levels of throughput. Additionally, configuration was a much easier process than with the other firewalls, and in general, the FortiGate NGFWs were much easier to work with."

Another major benefit of FortiGate NGFWs was the ability to integrate the entire security architecture—from the new data center infrastructure to the three cloud platforms—using the Fortinet Security Fabric. "The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams," Hawkins relates. The Fortinet Security Fabric provides an integrated security architecture to ensure that incident detection and response and remediation efforts are fully coordinated and optimally effective.

Business Impact

- Reallocated 40 to 80 staff hours monthly for architecture team due to stability of new network infrastructure
- $5 million cost avoidance for SSL/TLS inspection appliances required for competing solutions
- 27 staff hours in potential savings for each VPN setup
- 180 staff hours per year saved on a single, semiweekly report produced by the network team
- 15% reduction in storage cost
- Better coordination among the architecture, network, and security teams via centralized management and visibility

Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiSandbox Cloud
- Fortinet Professional Services
- Fortinet Network Security Academy
- FortiCare First program (Advanced Services technical support contract)

Deploying the NGFWs

The university began by deploying six FortiGate 7060E NGFWs in the data center at its main campus, pushing them live in January 2019. "We opted for the top-of-the-line boxes because of our speed requirements and the relative ease of configuration at the scale where we are operating," Hawkins explains. The team deployed FortiManager and FortiAnalyzer at the same time to provide centralized management, security automation, and robust reporting capabilities.

While the team currently routes all cloud traffic through the physical boxes using virtual domains (VDOMs), they are conducting a trial of FortiGate VM virtual NGFWs to eventually protect virtual and cloud resources. "We expect the ease of configuration to be even greater with the virtual firewalls, which will be integrated seamlessly with the physical ones," Boryk states.

The network team has activated, or is planning to activate, the secure sockets layer (SSL)/transport layer security (TLS) encryption, application control, intrusion prevention system (IPS), antivirus, and web filtering functionalities in the NGFW. "Having the SSL/TLS encryption built into the firewall was a requirement from our security team," Boryk explains. "Other vendors we considered did not have the same level of capability and integration we needed without having to invest in separate SSL/TLS inspection appliances, integrate them into the network, and spend valuable time managing them."

Getting a Jump-start with Fortinet Services

The university received assistance with the initial deployment from a resident engineer from Fortinet Professional Services. "During our first engagement, our engineer got the firewalls up and functioning, explained configuration and troubleshooting to us, and deployed FortiManager and FortiAnalyzer," Boryk remembers. "We also purchased an additional three-month engagement, during which we hope to create a more comprehensive firewall strategy and start working to thin our legacy rule set." Streamlining the rule set is the second step of a process that began with migrating more than 10,000 rules—many of them obsolete—from their old infrastructure using tools from Fortinet.

The university also purchased a FortiCare First program (Advanced Services technical support contract), which assigns a dedicated technical account manager (TAM) who works alongside the university's team to prioritize and coordinate support services. The team also invested heavily in training from the Fortinet Network Security Academy. "Everyone on the architecture, network, and security teams will receive full, classroom-based training on managing the solution," Boryk comments.

Achieving Impressive Results

In the short time since the initial deployment, the university is already seeing tangible results and can project further future gains based on preliminary results. The larger network upgrade project has stabilized the network and helped Boryk's team reclaim a lot of time. "Just keeping the network stable required 10 to 20 hours per month for each of our four team members—or a total of 40 to 80 hours monthly," he says. "On top of that, the events when our network required all hands on deck to return it to a stable state could sometimes require a full day of work for each of us. Getting that time back means that we can move on to strategic projects."

Enabling cloud backup also promises significant savings for the university, with a significant number of backups slated to move to Azure by December 2019. "Backup administration time has already been sharply reduced, and the cost of backing up to the cloud is much lower than with our SAN," Hawkins reports. "We expect a 15% annual saving in storage costs once we're fully up and running with cloud backups."

Leveraging built-in features such as the intrusion prevention system (IPS) in the FortiGate NGFW will also result in reduced licensing costs. "We currently have a separate point solution for IPS," Boryk explains. "Once we turn on the FortiGate IPS, we will save significantly in licensing and management overhead per year in costs for that solution."

Centralizing security operations on the FortiGate NGFWs is resulting in operational efficiencies as well. "We recently had to set up VPNs for private addressing from the university to one of our cloud providers," Hawkins states. "That project required 28 staff hours but would have taken just a few minutes if our FortiGate NGFWs had been set up." Another example of efficiency savings: one twice-a-week report produced by the network team now takes just a few minutes with FortiManager, compared with two hours previously. This saves 180 staff hours per year.

Better coordination among the architecture, network, and security teams is another benefit of the FortiGate NGFW and the Fortinet Security Fabric. “All our teams now use FortiManager and FortiAnalyzer to view status and run reports,” Hawkins relates. “It really contributes to a more coordinated and less siloed way of doing our jobs. And this benefit will grow as new elements are added to the Fortinet Security Fabric.”

Completing the Transformation

The University of South Carolina team expects to have the new network backbone and the entire Fortinet Security Fabric fully deployed by summer of 2020. “It was a massive undertaking, but the benefits we are already seeing make the effort well worth it,” Boryk contends. “Our relationship with Fortinet has been more than positive. Everyone has been really supportive and has gone out of their way to ensure our success.”

July 24, 2019 4:43 PM

352527-0-0-EN

cs-university-of-south-carolina