CASE STUDY

Large College Expands Network Access While Thwarting Security Threats

Tampa, Florida-based Hillsborough Community College (HCC) serves more than 47,000 students annually with more than 180 academic programs. HCC's students, as well as its 2,900 faculty and staff members, depend heavily on the college network, which spans seven campuses over 850 acres—with the most separated facilities being 27 miles apart.

BYOD Traffic Surges Across the College Network

As it aimed to better support the mobile resource-sharing and communication capabilities expected in 21st-century education environments, HCC instated a campuswide "bring-your-own-device" (BYOD) policy. Starting with the 2014-2015 school year, students, faculty, and staff were permitted to use their personal smartphones, tablets, and laptops to access the internet and college resources over Wi-Fi connections. As a result, HCC experienced a massive increase in network traffic and a surging demand for wireless access points. "We have grown quite a bit with our wireless footprint," notes Kenneth Compres, HCC's information security officer (ISO). Among his other duties, Compres oversees the college's network infrastructure, which comprises multiple server farms with several thousand access points.

Closing Endpoint Gaps Through Integration, Intent-based Segmentation

All those personal devices connecting over Wi-Fi added thousands of new attack vectors for cyber criminals to exploit. HCC had been defending its network edge with its legacy firewalls, but those devices could not protect the endpoints or provide visibility to security events occurring on compromised endpoints. As a remedy, Compres and his team decided to replace the edge devices with FortiGate next-generation firewalls (NGFWs). They also added FortiGate NGFWs in the data center.

To provide the needed protection and visibility, the FortiGate NGFWs integrate with all of the college's access points and with the endpoint security software on each user device. HCC also leveraged FortiAuthenticator to authenticate users accessing the network over 802.1X Wi-Fi connections and through its virtual private network (VPN). "We started using our system's native policy and access services for authentication, and they really didn't meet our requirements," Compres recalls. "FortiAuthenticator allows us to do multiple domain authentications. That is important for an educational institution like ours, which has two separate domains: one for students and one for employees."

"Previously, intrusions were a daily occurrence. Now, we have been able to reduce them by 90%. And in the rare case we need to handle an intrusion, we have taken advantage of the automation in FortiGate to make the process work much better."

– *Kenneth Compres, Information Security Officer, Hillsborough Community College*

Details

Customer: Hillsborough Community College

Industry: Education

Location: Hillsborough County, Florida

When they access the network—whether through HCC computers or their personal devices—authorized users are automatically identified as belonging to one of the two domains, and FortiAuthenticator permits access accordingly. "With FortiAuthenticator, we were able to integrate that seamlessly and have a single SSID [service set identifier] that can identify both devices," Compres says. "We can also take that information and pass it on to the FortiGate firewall, so we can identify where users are logged in at any given point."

Leveraging the intent-based segmentation capabilities of the FortiGate NGFWs, both at the network edge and at the wireless access points, HCC can apply business rules to ensure appropriate levels of access for each user. For example, faculty may have access to a student's academic but not personal information. Teaching assistants may be permitted to access students' work but not their grades. Access to some sensitive applications may not be permitted via personal mobile devices. "We have been very successful in implementing zero-trust methodologies with FortiGate, whereby we require systems requesting access to demonstrate that they are compliant before we permit access," Compres says.

HCC relies on the integrations available in the Fortinet Security Fabric to enable the FortiGate firewalls to coordinate with HCC's network access control (NAC) technologies and access points from other vendors. "We have found that when we combine all these other technologies with the Fortinet Security Fabric, they work very well," Compres says.

Peace of Mind in the Cloud

Like many educational institutions, HCC has adopted Office 365, running in the Azure cloud, to provide email services for faculty and staff. HCC also runs some of its DNS servers, Active Directory Federation Services (ADFS) and Canvas single sign-on (SSO) applications, and academic applications in Azure.

HCC recognized that it was responsible for all the data it stored in the Software-as-a-Service (SaaS)-based Office 365 environment. For the Azure-based services, which run in an Infrastructure-as-a-Service (IaaS) environment, the college is responsible for everything that resides on the Azure hardware. To protect its cloud environment, HCC elected to deploy FortiGate VM, a virtual NGFW specially designed to integrate with Azure. Compres says the FortiGate protection for ADFS was crucial. "When the cloud portion of ADFS first came out, we had numerous distributed denial-of-service [DDoS] attacks," he recalls. "We put the FortiGate NGFW out there and saw immediate results. At one point, we had more than 1,000 different attacks coming in the space of less than two minutes. With the FortiGate firewall in place, that completely died down."

As the number of cloud users grew, Compres appreciated the FortiGate VM Service Manager, which helped his team handle the mobility and varying device use of its faculty and staff. "Our IP addresses are changing every day," he says. "Our IT staff were having to manually reconfigure the IP addresses in the firewall, causing a lot of overhead. FortiGate VM Service Manager allows us to do much better QoS [quality-of-service] management."

Business Impact

- $750,000 reduction in the total cost of firewall, IDS, and IPS capabilities
- Nearly $700,000 annual FTE operational savings
- 90% reduction in intrusions, improving security and reducing staff time on remediation
- Effective threat protection and easier IP address management in Azure cloud
- WAN cost savings, resiliency, and quality-of-service capabilities with SD-WAN
- Closure of security gaps between wireless endpoints and internal network
- Faster audit response with prebuilt and customized reports
- Ability to give CIO clear picture of security posture

"ADFS in the cloud presented its own set of challenges; we had numerous distributed denial-of-service attacks. We put the FortiGate NGFW out there and saw immediate results."

– *Kenneth Compres, Information Security Officer, Hillsborough Community College*

Looking to SD-WAN for Resiliency and QoS Management

As HCC ramps up its use of cloud services, and with personal devices comprising an increasing proportion of network traffic, Compres must think about the cost and performance implications for the college's wide-area network (WAN). HCC has dedicated multiprotocol label switching (MPLS) links in place between its campuses, and it continues to use those for core academic and administrative applications. At the same time, it is also starting to take advantage of the software-defined WAN (SD-WAN) features of FortiGate NGFWs to provide resiliency. "That way, if one campus goes down, we have a different path out," Compres explains.

HCC is also planning to leverage the application awareness in FortiGate Secure SD-WAN to manage QoS for different applications running over the network. "If we have students watching Netflix in 4K [video resolution], we're not going to bring that traffic all the way over to our data center," Compres says. "We'll just route it over our lowest-cost internet line."

More Effective Intrusion Detection and Prevention Lead to Big Savings

In addition to its legacy firewalls, HCC had separate web application firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS) for its previous security configuration. "All those things had to be purchased separately with different licensing," Compres says. "It was just overly cumbersome and expensive, and we needed to have different experts for each of those systems. Once we started implementing IPS and IDS in FortiGate, it became a lot easier for us to manage. Our original budget for firewall, IPS, and IDS capabilities was close to a million dollars, and we were able to reduce that by 75%."

A major component of this cost was operational. Compres had eight staff members, each with a different product specialization; now he needs just three. "A person trained on FortiGate NGFWs can simply implement whatever rules and tweak whatever security features we need—IPS, IDS, firewall, and so on," he says. This efficiency improvement has been highly valuable. Like many managers in cash-strapped college departments, Compres was able to avoid submitting staff requisitions as some of his team members retired. This has saved his department close to $700,000 annually in staff costs.[1]

From a security standpoint, Compres also appreciated the drastic improvement in intrusion detection and prevention. "Previously, intrusions were a daily occurrence," he recalls. "Now, we have been able to reduce them by 90%. And in the rare case we need to handle an intrusion, we have taken advantage of the automation in FortiGate to make the process work much better. As an example, one FortiGate device recently detected ransomware sending command-and-control communication. It automatically signaled our endpoint software to quarantine the offending device and messaged our on-site tech to go and pick it up."

Security and Compliance Expertise Built In

With only three staff members, Compres must ensure that they can all competently configure firewall rules, even though they may not have as much experience as he does. Because Compres cannot be standing over their shoulders, he has deployed FortiManager to help staffers analyze the impact of their rules prior to implementation. It provides a risk score that Compres later uses to allow or reject the rule. "I tell them, 'If your score is lower than x, implement it; if it is higher, bring the rule to me for review,'" Compres explains. "It allows me to take a more hands-off approach."

Solutions

- FortiGate
- FortiGate VM (for Office 365 and Azure)
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiGate Secure SD-WAN
- Enterprise Subscription Bundle
- Security Rating Service
- FortiCare 365 Support
- Network Security Expert Training and Certification

"FortiAuthenticator allows us to do multiple domain authentications. That is important for an educational institution like ours, which has separate domains for students and employees."

– *Kenneth Compres, Information Security Officer, Hillsborough Community College*

Compres and his team also leverage FortiManager to replicate accepted rules, reducing the need to re-create them from scratch as needs arise across the network. "For example, we can replicate a rule across our edge firewalls, data center firewalls, and disaster recovery firewalls," Compres says. By knowing the risk of the rules across all these areas, HCC is less likely to be blindsided by a threat designed to exploit a firewall misconfiguration.

When selecting a licensing scheme for its Fortinet technologies, HCC opted for the Enterprise Subscription Bundle, which includes the Fortinet Security Rating Service. Compres uses the service to identify network security vulnerabilities and to compare HCC's security rating with those of similar higher-education institutions. "We always want to know where we stack up," he says. "Plus, it gives us the ability to proactively manage our security posture, identifying vulnerabilities and remediating them before they become a problem."

Financial industry and government regulators also want to know how HCC's security measures stack up. Due to its heavy compliance burden, HCC has been an early adopter of FortiAnalyzer. Compres's team uses a combination of prebuilt and custom reports for compliance and for internal oversight. In a recent audit, the team was asked to report on employee logs to particular websites. "Within a couple of minutes, we were able to provide the report," he says.

In planning its compliance efforts, HCC follows the National Institute of Standards and Technology (NIST) Cybersecurity Framework. For the most part, this ensures that HCC also complies with the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Security Standards Council (PCI SSC) framework. Compres uses FortiAnalyzer to generate monthly reports, which he submits to the CIO. "The reports we generate through FortiAnalyzer help us educate the CIO and the administration as to what our security posture looks like," he says. Because the information contained in these reports is also reflected in the Security Rating Service that HCC uses, Compres can use the Security Rating Service dashboard to present the data to the CIO and to other board members in a real-time context.

> *"Once we started implementing IPS and IDS in FortiGate, it became a lot easier for us to manage. Our original budget for firewall, IPS, and IDS capabilities was close to a million dollars, and we were able to reduce that by 75%."*
>
> – *Kenneth Compres, Information Security Officer, Hillsborough Community College*

Training Keeps Cybersecurity Skills up to Date

Most of the HCC IT staff have completed Fortinet Network Security Expert (NSE) training and certification. NSE is an eight-level program that exposes technical professionals to the full range of Fortinet security products and provides independent validation of network security skills and experience. "This helps in two ways," Compres explains. "The certification helps us retain our talent, and the training ensures that we have people who can competently implement solutions in the Fortinet Security Fabric, which is very helpful to us."

To further ensure the uninterrupted availability of its different Fortinet solutions, HCC leverages FortiCare 365 support. Although the NSE training has obviated much of the need for outside help, Compres notes, "The folks at Fortinet are very accessible. We have really had a great experience with FortiCare support."

Compres relates that HCC administration is highly appreciative of the IT team's ability to keep such a distributed and changing network environment running smoothly and securely. "They are extremely happy with us," he says. "They think we work magic here—and with Fortinet, we kind of do."

[1] Based on median annual salary of $98,350 x 5 FTEs x 1.4 multiplier for employer costs = $688,450. Salary data drawn from the Bureau of Labor Statistics website, accessed October 11, 2019.

FORTINET

www.fortinet.com

December 11, 2019 6:39 AM

511300-0-0-EN

D:\Fortinet\Case Study\Hillsborough Community College\cs-FA-large-college-expands-network-access-while-thwarting-security-threats\cs-FA-large-college-expands-network-access-while-thwarting-security-threats