FORTINET

CASE STUDY

Fortinet Secure SD-WAN Offers Laundry Service Provider Improved Reliability and Better ROI

Hospital Central Services (HCSC) is a healthcare support services organization that provides laundry and linen services to healthcare organizations in the mid-Atlantic region, as well as offering group-purchasing programs and operating a regional, nonprofit community blood center. Economies of scale reduce the organization's prices for these services, compared with what healthcare facilities would pay to handle the tasks themselves.

To provide high-quality service at the lowest cost possible, HCSC operates out of 13 locations across Pennsylvania, New Jersey, and Maryland. Staff use handheld scanners to manage their inventories of scrubs and other goods. Scanner data from each location is automatically transmitted to a central database. "This solution is crucial to our operations, so uptime needs to be 100%," says Adam Reifsnyder, systems engineer at HCSC. The same is true for the company's Voice-over-IP (VoIP) phone system.

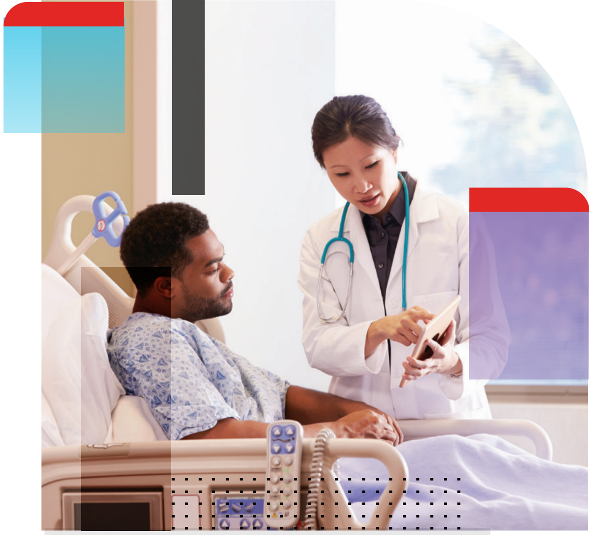
"Losing communications would be absolutely nightmarish because these systems are a linchpin of our business," Reifsnyder adds. "We have manual processes that we can use in disaster scenarios, but we do not want people processing stacks of paper to get information into our database."

Two years ago, HCSC was living that nightmare. Its multiprotocol label switching (MPLS) network was experiencing a significant amount of downtime. The company maintained two internet service providers (ISPs), but moving from one to the other was time-consuming and required travel to the site of the outage. Plus, HCSC outsourced network and security management to its MPLS provider, an arrangement that reduced productivity for the IT team.

"We would call when there was a problem," explains Chris Dieterick, senior systems engineer at HCSC, "and we would spend hours on the phone trying to find the right person and then convince them to look at the issue. Adam and I are the entire HCSC infrastructure team. The more tasks we can automate or streamline, the better—and we do not have time to waste waiting on hold."

SD-WAN: Reliability at Lower Cost

HCSC decided to bring network and security management in-house. Improving uptime, optimizing efficiency, and adequately protecting corporate data were three key goals in the transition. The company engaged Advanced Computer Solutions Group (ACSG), a managed service provider, to help design and roll out a new security-driven network infrastructure across HCSC's 13 locations.



HCSC

"Fortinet security-driven networking enables us to take a proactive, rather than reactive, approach to managing our network. We can identify an issue quickly and get ahead of it, ensuring a more efficient and effective response to every security threat."

– Adam Reifsnyder,
Systems Engineer,
Hospital Central Services

Details

Customer: Hospital Central Services

Industry: Healthcare

Location: Allentown, Pennsylvania

Business Impact

- Saving approximately $5,000 per month through transition from MPLS to SD-WAN
- Improved internet availability; failover to secondary ISP completes in seconds, vs. hours or days in legacy environment

ACSG recommended Fortinet Secure SD-WAN, which combines software-defined wide-area networking (SD-WAN) connectivity with next-generation firewall (NGFW) security. ACSG asserts that Fortinet has “a great feature set built around SD-WAN,” so it was a no-brainer for the provider to recommend Fortinet solutions to HCSC.

HCSC was already using FortiGate NGFWs through its hosting provider, and found them both effective and reliable. “In the five years we have used FortiGate NGFWs, we have had no breaches,” Reifsnyder says. “Knowing the firewalls at our network edge will stop any malicious activity that approaches the network boosts our peace of mind. In addition, the FortiGate firewall is one of the most reliable solutions I’ve ever seen. Over five years, we have not had to replace a single one.”

HCSC liked the cost savings Fortinet Secure SD-WAN offered over MPLS, as well as its straightforward, centralized network management. “I was making site visits on a weekly basis all over the tri-state area, often just to physically disconnect an uplink and plug it back in, to get our legacy MPLS product to work as it was supposed to,” says Reifsnyder. “Being able to perform most management tasks through a single pane of glass from headquarters was very appealing.” He estimates that HCSC is saving about $5,000 per month by utilizing SD-WAN rather than MPLS for all its locations.

Automated and Streamlined Implementation

ACSG helped HCSC plan the new infrastructure. They designed a network of Internet Protocol security (IPsec) virtual private network (VPN) tunnels, over Fortinet Secure SD-WAN, which connect every branch location with HCSC headquarters. The company’s primary and secondary data center edges are protected by high-availability pairs of FortiGate appliances, which automatically load balance network traffic between two ISPs. At each branch’s WAN edge, a FortiGate NGFW provides high-performance threat protection and SD-WAN routing. Additionally, a FortiExtender LTE wireless WAN extender in each branch provides connectivity through a 3G or 4G LTE connection in the event that both ISPs fail simultaneously.

Business Impact (contd.)

- Improved user experience, due to ISP load balancing and SD-WAN functionality
- Faster response to security threats, due to better visibility of all LAN and WAN edges
- Simplified operations, minimizing time demands on two-person IT infrastructure team
- Reduced time to add a website to whitelist/blacklist, from 1-2 hours previously to 5-10 minutes now
- Consistent application of security policies companywide

Solutions

- Fortinet Secure SD-WAN
- FortiExtender
- FortiManager
- FortiAnalyzer
- FortiAP

After designing the network, ACSG tested the configuration in their own lab environment to be sure everything performed as expected. Then they began rolling the solution out to HCSC locations.

ACSG leveraged the FortiManager management tool to its fullest potential. Once they got all the Secure SD-WAN configurations right, they built a template, then used FortiManager to roll out that template to the rest of HCSC’s locations. The centralized management capability will also make the network a lot easier to manage moving forward.

Huge Time Savings on VPN Management

Security profiles that restrict which traffic can pass into and out of the network tie into Active Directory (AD) groups via Lightweight Directory Access Protocol (LDAP). Now, to give a new user VPN access, HCSC just adds the person to the right AD group, and security settings are applied automatically.

This functionality has enabled HCSC's infrastructure team to hand end-user management over to operations staff. "Previously, VPN changes required direct, local admin access to the firewall, and the process was highly manual," Reifsnyder says. "With the LDAP integration in FortiManager, giving new users VPN access is a complete breeze. We have been able to shift end-user responsibilities back to the operations side, where they should be."

FortiManager also simplifies the process of managing security settings for the various AD groups. If a security profile needs to change, HCSC can just make the change in FortiManager and push it out to all the locations simultaneously. For its part, ACSG calls FortiManager "a great tool for managing networks at scale."

Reifsnyder concurs. "FortiManager is saving our two-man team a huge amount of time," he says. At ACSG, adding a website to a whitelist or a blacklist currently takes approximately 5 to 10 minutes; they just add the rule to FortiManager and push the policy down to all the firewalls. Without FortiManager, completing the same task across all firewalls at all 12 sites would take an hour or two.

> *"With the automated failover in Fortinet Secure SD-WAN, what was previously a drawn-out process now completes in seconds. Users typically do not even notice that there was a problem."*
>
> – Chris Dieterick, Senior Systems Engineer, Hospital Central Services

In addition to the time savings, this approach to firewall management helps the HCSC team standardize policies and ensure compliance. "Being able to set a policy once, then apply it to all the remote systems, helps ensure that our policies are consistent companywide," says Reifsnyder.

Optimizing the IT Investment

The solution is meeting HCSC's needs for network availability. In the legacy environment, failover to the secondary ISP would take hours, or even days. "With the automated failover in Fortinet Secure SD-WAN, what was previously a drawn-out process now completes in seconds," Dieterick says. "Failover is very predictable and easy to manage, and users typically do not even notice that there was a problem." In the 10 months that HCSC has been using its new network configuration, it has had one instance of a site requiring failover to FortiExtender.

"We had a situation where both ISPs for one of our branches became unavailable at the same time," Reifsnyder says. One preselected workstation running business-critical applications used FortiExtender to connect to the HCSC WAN. "That allowed us to maintain a base level of operations, and we were impressed by the FortiExtender's performance."

Load balancing within Fortinet Secure SD-WAN has improved network performance and eliminated the waste of having a secondary ISP sitting idle until failover is necessary. "Our previous environment did not fully utilize the investment in having dual ISPs at every location," Dieterick says. "Today, we are using both ISPs to expand our bandwidth and improve WAN performance for our network traffic, day in and day out."

HCSC is now expanding its SD-WAN deployment, transforming to a Fortinet Secure SD-Branch by deploying FortiAP access points in every location. Dieterick sees this as another optimization of the company's investment, since the FortiAP solution connects local-area network (LAN) traffic with the corporate WAN via the Fortinet Secure SD-WAN solution that is already in place. Other vendor access point solutions, by contrast, would require HCSC to manage the APs separately.

Most Important: Effective Security

HCSC uses the FortiAnalyzer security fabric analytics and automation solution to monitor security events across the network. "We can quickly figure out what is happening in our environment," Reifsnyder says. "Previously, even if we thought we knew what was going on, we would spend hours and hours on the phone with our service provider before we would get real visibility into the problem.

“Fortinet security-driven networking enables us to take a proactive, rather than reactive, approach to managing our network,” he continues. “I cannot overstate how important that is. We can identify an issue quickly and get ahead of it, ensuring a more efficient and effective response to every security threat.”

Dieterick adds: “Prior to FortiAnalyzer, our responses to threats were more reactive. Our view into the security of the network was limited to our antivirus management software alerting us to an issue. Utilizing FortiAnalyzer, we can now take a more proactive approach by setting up daily, weekly, or monthly reports; daily reviews of the firewall logs; and alerts through the NOC-SOC [network operations center–security operations center] dashboard.” Both Dieterick and Reifsnyder are confident that whenever threats approach the HCSC network, Fortinet Secure SD-WAN will prevent them from spreading companywide.

“In previous positions with other organizations, I have seen virus outbreaks on an MPLS network spread quickly to hundreds or thousands of company sites around the world,” Dieterick says. “Fortinet Secure SD-WAN does a much better job of containing threats to one site.” A couple of months ago, a command-and-control attack attempted to take over one of the company’s VPN tunnels. “The Fortinet solutions identified the malicious traffic and immediately alerted us that we needed to take that equipment offline. Seeing that functionality in action enables us to breathe easier.”

www.fortinet.com

May 18, 2021 9:49 AM
D:\Fortinet\Work\2021\0518\cs-hospital-central-services
931330-0-0-EN