



I D C C U S T O M E R S P O T L I G H T

Threat Protection: Halifax Health Safeguards Its Network with a Firewall Upgrade

September 2016

Sponsored by Fortinet

Introduction

As a public hospital created as a special taxing district of the state of Florida, Halifax Health is a safety net hospital. With that designation, "we care for everyone in our community who comes through our doors," says Tom Stafford, vice president and CIO of the Daytona Beach, Florida-based hospital. While providing quality healthcare is certainly a priority for Halifax Health, so too is ensuring that all patient medical records and data remain secure. Whether via targeted attacks perpetrated by sophisticated cybercriminals or inadvertent breaches that result from employee lapses, healthcare organizations are besieged by threats. Yet establishing security measures to protect networks and data cannot be restrictive to the point where it becomes inconvenient for staff to access the IT systems needed to do their jobs. It is a balance between protection and productivity that healthcare organizations such as Halifax Health must continuously strike. "We always work to make sure that we put the right level of security in and allow our users to still perform their duties," Stafford explains. "To do that, we focus on HIPAA's physical security, technical security, and administrative standards."

On the security technology front, firewalls have long been implemented to secure patient data and organizational networks. However, Halifax Health's legacy firewalls were aging to the point where performance was becoming an issue. "We couldn't really put any more traffic through it," Stafford says. "We didn't look to purchase new firewalls because of vulnerability; it was really just due to our existing equipment reaching its performance levels."

To accommodate increased traffic while still imparting strong security technology, Halifax Health opted to purchase external and internal firewalls from Fortinet, a major provider of network and other security appliances.

Solution Snapshot

Organization: Halifax Health is the largest healthcare provider in East Central Florida with a tertiary and community hospital with 678 licensed beds and more than 500 physicians on its medical staff

Operational challenge: Provide protection against network threats affordably and without hindering end users

Solution: Fortinet's Next Generation Firewall for the edge and Internal Segmentation Firewall for the core

Project duration: Approximately 3–4 months

Benefit: Improve performance at a cost that fits the budget; enable Halifax Health's small IT staff to monitor and manage distributed networks and systems from a single console

Implementation

The primary business drivers for seeking new firewall technology were to improve Halifax Health's security posture and increase performance while reducing costs. Stafford wanted to explore other firewall vendors because of what he had learned at an IT industry conference. In a panel discussion featuring Fortinet customers, the presenters described the products as "CFO friendly," which piqued Stafford's interest. As Stafford explains it, "We're all driven to reduce our costs." So in addition to replacing aging firewalls, his goal "was to find a product that met our security and performance needs but also met our financial requirements, too."

Along with the external firewall, Stafford intended to replace internal firewalls to streamline the management of the firewalls. As a result, he was looking to purchase external and internal firewalls from a single vendor, easing administration and allowing Halifax Health to manage and monitor network traffic from a single pane of glass. After attending the conference and liking what he heard, Stafford added Fortinet to a short list of three firewall vendors to evaluate and set about finding the best successor to the organization's existing firewalls.

To determine the best fit for Halifax Health, its IT department conducted a "test before you buy" study. "We installed the firewalls and ran the same traffic through them," Stafford explains. In addition to observing how the firewalls safeguarded against vulnerabilities, the IT staff also looked at overall performance and integration capabilities. In testing, Fortinet's performance represented a significant improvement over the performance of the existing firewall because, says Stafford, the product working at the firmware level and not the software level. Finally, Stafford considered the cost. Fortinet emerged as the most appropriate option for Halifax Health. The vendor, Stafford says, "charges a fair price for its products."

Given that the Fortinet firewall replaced an existing system, the implementation process was fairly straightforward. Stafford says that two IT staff members spent approximately 3–4 months deploying the external firewall. To eliminate downtime when the firewall went live, Halifax Health did extensive testing in several departments before rollout to the entire organization. The IT department went live first, followed by other departments that have high volumes of traffic. "Once we felt pretty confident that we had seen most of the potential issues, we went live with the entire house," Stafford recalls. Throughout the course of the implementation, Fortinet was on hand to provide consulting services and address any issues as they arose, Stafford says.

Challenges

Working with Fortinet to set up the external firewall initially was relatively straightforward. "The only challenge that my security team had with the Fortinet external firewall was the hierarchy required for access," Stafford says. "Web restrictions for users were different than in our incumbent firewall, so we had to think about how to do that and come up with a best practice." The hospital's security team worked with Fortinet consultants and was able to do everything needed for access prior to going live.

Halifax Health faced significant challenges when dealing with outside partners. As a healthcare provider, Halifax Health works with third-party vendors to transmit data back and forth. "Our real challenges were with vendors that needed to change things on their end to allow traffic to pass through the external firewall," Stafford explains.

As for lessons learned, Stafford says that it is important to consider the effect that a new firewall may have on external organizations. "If you're either installing an external firewall for the first time or switching to a different partner, you have to worry about all those downstream data feeds from other vendors," he says.

Benefits

From Stafford's perspective, one of the biggest benefits of the Fortinet firewall is financial. With a majority of payers from Medicare or Medicaid, "Fortinet really understood the Halifax Health mission," he says. In addition to performance and protection, "we needed to have a product that met our financial needs, too, and Fortinet did that."

Fortinet's Security Fabric will further accommodate Halifax Health's future needs. "We knew that we also needed to continue to secure our organization and protect electronic protected health information," Stafford explains. "So we wanted to also purchase an internal firewall with enhanced threat protection from the same vendor so we could manage them together on a single management console." This is why Halifax Health purchased an internal firewall from Fortinet at the same time as the external firewall. Replacing the existing internal firewall is an upcoming project that Stafford says will allow Halifax Health to streamline monitoring and management, an important benefit given the limited size of the security staff.

Stafford is exploring using other Fortinet security products and services because of the level of trust established while deploying the external and internal firewalls and the sense of a true partnership between Fortinet and Halifax Health. "You have vendors, and you have partners," explains Stafford. "A vendor simply supplies a product, and that might be okay. But a partner has a future vision of where the technology is going and a road map to get there. A partner understands your mission and is focused on meeting all of your needs."

Methodology

The project and organizational information contained in this document was obtained from multiple sources, including information supplied by Fortinet, questions posed by IDC directly to Halifax Health employees, and Halifax Health corporate documents.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the IDC Custom Solutions information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document require an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com