Hospital Trust Improves IT Security and Compliance

Customer Case Study

Cisco Next-Generation Firewalls enable Oxford University Hospitals NHS Trust to securely enhance patient experience

EXECUTIVE SUMMARY

Customer Name: Oxford University Hospitals NHS Trust

Industry: Healthcare

Location: United Kingdom

Number of Employees: 11,500

Challenge

- Maintain data security while fostering open collaboration
- Improve network traffic handling to reduce congestion
- Reduce costs by consolidating IT appliances

Solution

- Cisco security based on Cisco ASA 5500-X Series Next-Generation Firewalls

Results

- Faster access to healthcare information and tools with 16-fold increase in network speeds
- Boosted general practitioner Internet performance by 75 percent
- Reduced maintenance costs by US$56,000 a year

Challenge

Modern healthcare is going digital. While nothing can replace the human touch, the processes found in modern hospitals and clinics are increasingly carried out using electronic entries on electronic devices. This connected approach yields significant benefits in terms of patient care, and caregiver effectiveness, yet also creates a different set of data security challenges to those associated with traditional healthcare.

One organization that has faced and overcome these challenges is Oxford University Hospitals NHS Trust (OUH), a world-renowned center of clinical excellence and one of the largest National Health Service (NHS) teaching trusts in the United Kingdom. The center comprises four hospitals, and to a growing extent, the trust also coordinates research and treatment in other hospitals as well as doctors' surgeries across Oxfordshire. Given that much of this collaboration involves digital media, OUH has had to modernize its IT security systems to help ensure patient confidentiality is not compromised.

The trigger came in 2012, when existing firewalls reached end-of-support. At the time, OUH was using five perimeter firewalls: two for Internet access, one for Oxford University and JANET (the U.K. national research and education network), and two for N3 (the NHS broadband network).

Unusually for an NHS trust, OUH is able to publish its internal routes onto N3 using the Cisco® Enhanced Interior Gateway Routing Protocol (EIGRP). However, its firewalls were not able to take advantage of this functionality because they could only handle Open Shortest Path First routing protocols.

The result was that most Internet traffic ended up going over N3 links, throttling the NHS network and slowing the delivery of critical medical applications. At the same time, OUH was using a different vendor platform for URL filtering and proxy traffic, and wanted to combine this functionality with firewalling in a single solution for greater efficiency.

"Cisco Security Manager helped tremendously. We found it a lot quicker than expected, migrating our biggest firewall with no downtime in five days, whereas we'd thought it would take 15."

Craig McVeigh
Senior Network Consultant
Oxford University Hospitals NHS Trust

Solution

OUH started reviewing the offers from a range of IT security vendors. The selection process saw Cisco rapidly emerge as a frontrunner. "Cisco was the most competitive, owing to its ability to combine web filtering and firewall functions on one cost-effective platform," says Craig McVeigh, senior network consultant at OUH.

In addition, Cisco security products were able to handle EIGRP, enabling the hospital to split different types of traffic and optimize routing to keep its N3 connections free. Finally, the Cisco products were a familiar technology since OUH was already using Cisco ASA 5520 and 5505 Adaptive Security Appliances for its VPNs and inter-departmental firewalling.

OUH began replacing its external firewalls and URL filtering devices with five Cisco ASA 5555-X Series Next-Generation Firewalls. Configured as Layer 3 devices rather than inline firewalls, these were equipped with ASA CX modules for web filtering and administered via a Cisco Security Manager system.

"In implementing the new firewalls, we started with the N3 links," says McVeigh. "Cisco Security Manager helped tremendously. We found it a lot quicker than expected, migrating our biggest firewall with no downtime in five days, whereas we'd thought it would take 15."

In addition to these security technologies, OUH employees use Cisco AnyConnect® VPN Clients for secure networking. The hospital also maintains two Cisco ASA 5555-X Series Next-Generation Firewalls, without CX modules, for site-to-site connections with other trusts, and a number of Cisco ASA 5520 and 5510 Adaptive Security Appliances for other VPNs.

Results

"In the last five years there's been a massive increase in our need to liaise with other NHS trusts without compromising security," McVeigh says. OUH is now able to advance this goal and improve patient outcomes and lower costs.

For example, having better secure connectivity with other clinics and hospitals means patients do not need to always travel to an OUH center for diagnosis or treatment. This capability saves travel time and money, besides speeding recovery and helping reduce patient stress levels and carbon footprint.

Being able to separate Internet access from the N3 links has helped OUH improve the speed of the latter 16-fold, from around 50Mbps to 800Mbps. The delivery of N3-based medical applications has improved accordingly. Furthermore, OUH handles traffic for the other NHS trusts in Oxfordshire, representing around 30,000 endpoints in total. General practitioners using the service have reported a 75 percent improvement in Internet performance.

The Cisco Next-Generation Firewalls allow OUH to grant access to different applications based on Active Directory profiles, something it had not been able to do before. Thus, for example, people using OUH laptops can be granted full access to hospital networks, whereas those using personal or mobile devices have seen their usage capped.

This feature has been welcomed by the trust. When the firewalls were swapped out, OUH also upgraded its Internet link from 100Mbps to 1Gbps, raising concerns that extra bandwidth could lead to increased use of social media and other non-core applications. "In the event," says McVeigh, "we used the CX modules to rate-limit social media down to about 30Mbps, therefore protecting our core infrastructure for NHS use."

"We used the CX modules to rate-limit social media down to about 30Mbps, therefore protecting our core infrastructure for NHS use."

Craig McVeigh
Senior Network Consultant
Oxford University Hospitals NHS Trust

More widely, this capability has allowed OUH to support a growing bring-your-own-device trend, thus increasing patient and employee satisfaction, without compromising systems required for clinical excellence. OUH now offers free guest Wi-Fi, for example, with a per-user limit of 50Mbps. "The CX modules really opened that door for us," McVeigh says. "We held off offering free guest Wi-Fi until we had the modules in." The CX module also filters the content that users can reach on the hospital network, to safeguard against patients or visitors accessing adult or gambling sites, for example.

Finally, having just one vendor for security means maintenance and training costs have dropped, because most OUH technicians already have a good knowledge of the technology, and an ample public knowledge base of information exists on Cisco products. Compared to its previous vendor, OUH is saving around GB£10,000 (US$17,000) a year on maintenance. Adding URL filtering into the equation, the savings rise to about £33,000 ($56,000) a year.

Next Steps

Use of Active Directory-based authentication by OUH has so far been on a trial basis across two sites. However, plans are under way to extend this capability across the hospital group following work on the Active Directory system. This will help with compliance by allowing the trust to eventually eliminate generic user accounts, which can pose a security risk. OUH is also planning to use Cisco Security Manager to administer all its firewalls, further reducing administration.

For More Information

To learn more about the Cisco architectures and solutions featured in this case study, go to: www.cisco.com/go/cloud

Product List

Security

- Cisco ASA 5555-X Series Next-Generation Firewalls
- Cisco ASA 5520 Adaptive Security Appliances
- Cisco ASA 5510 Adaptive Security Appliances
- Cisco ASA 5505 Adaptive Security Appliances
- Cisco ASA CX Modules
- Cisco Security Manager
- Cisco AnyConnect VPN Client

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**