

LEADING MIDWEST HEALTHCARE SYSTEM ENHANCES COMPETITIVENESS WITH SECURE ACCESS TO KEY MEDICAL APPLICATIONS

Summary

Industry: Healthcare

Challenges:

- Provide physicians with secure remote access to a physician portal, Emageon, and other image-intensive medical applications, enabling the clinical staff to provide high quality, cost-effective healthcare
- Ensure easy access to a variety of applications, including those delivered over Citrix, Web-based, and traditional client/server

Selection Criteria: Alverno Information Systems, the IT organization for SSFHS, set out to find a remote access solution that gave physicians an easy, fast way to remotely access the hospital's image-intensive medical applications, while ensuring the highest levels of security and privacy.

Network Solution: Juniper Networks SA6000 SSL VPN Appliance

Results:

- Provides 7,000 clinicians at twelve major locations with easy-to-use, secure remote access to the physician portal, EMR, PACS, and other applications
- Makes it fast and easy for physicians with simplified sign-on to the network and core applications
- Uses technology as a competitive advantage to attract the best and brightest physicians in the area
- Mitigates risks of security breaches and regulatory non-compliance with strong access controls and encryption

A commitment to quality patient care, community health, and operational efficiency are the touchstones for Sisters of St. Francis Health Services (SSFHS), a leading Midwestern healthcare system. The health system attributes its success to partnering closely with physicians, collaborating with the community, and taking full advantage of advances in technology. SSFHS, which provides a broad range of acute care services, encompasses twelve major health services in Indiana and Illinois.

Challenges

SSFHS was an early adopter of McKesson electronic medical records (EMR) and also deployed Heartlab, a state-of-the-art cardiac image management system that allows its different hospitals to manage cardiac data with a single centralized system. It is this deep commitment to advanced technology that put SSFHS on the cutting edge of remote access five years ago. When it deployed its physician portal, it quickly discovered that its incumbent application delivery solution couldn't stand up to the heavy strain of medical imaging.

"We found that we were deploying more and more applications that weren't suitable for a remote access solution based on a remote desktop protocol," said Dr. Dick Roskam, chief clinical informatist at SSFHS. "Citrix couldn't render images fast enough to actually allow viewing of those images."

Deploying an IPsec VPN met with limited success, as the physicians found the client software difficult to use and IT found deploying and maintaining client software to be resource-intensive.

Selection Criteria

"We had high demand from physicians to remotely access our digital imaging applications so they could view both radiology and cardiology images from home," said Dr. Roskam. "We needed a remote access solution that was easy to learn and easy to use. It had to be reliable and have good response time."

Alverno Information Systems, the IT organization for SSFHS, set out to find a remote access solution that could stand up to the bandwidth demands of cardiology and radiology imaging and other performance-intensive medical applications. It needed a remote access solution that could support a mix of applications, including those delivered over Citrix, Web-based applications, and traditional client/server applications. Clinicians had to be able to quickly and easily access the physician portal, no matter where they were, as the portal was the gateway to their patient care. And given the sensitive nature of medical information, meeting stringent security and compliance requirements was essential.

Solution

SSFHS relies on the Juniper Networks® SA6000 SSL VPN Appliance to provide more than 7,000 medical staff with secure remote access to their essential application and information resources. SSFHS has been using Juniper's SSL VPN since 2004, and it has since become woven into the fabric of physician productivity. For IT, the SA6000 SSL VPN Appliance has been set and forget.

The SA6000 features best-in-class performance, scalability, and redundancy and is designed for enterprises that require high volume secure access and authorization. Juniper Networks SA Series SSL VPN Appliances use SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. With the SA Series appliances, SSFHS can enable controlled access to differentiated users and groups with no infrastructure changes, no DMZ deployments, and no software agents.

“Most of our hospitals have multiple competitors in their areas, so providing an easy-to-use, highly reliable remote access solution is an important competitive advantage for us to attract the best and brightest medical staff to our hospitals.”

Dr. Dick Roskam,
Chief Clinical Informatist, Sisters of St. Francis Health Services

“An advantage of the Juniper solution is having a user-specific list of applications that they need, even if those applications aren't available through their Citrix profile,” noted Dr. Roskam.

The SA6000 has three different role-based access methods, which take into account the account user, device, network attributes, and enterprise security policy. For instance, SSFHS uses Core Access to provide access to Web-based applications, email, and Citrix. SSFHS uses Network Connect to provide access to the Emageon and the McKesson physician portal. Network Connect provides network-layer connectivity via an automatically provisioned cross-platform download, so that users need only a Web browser for access while enjoying the highest performance possible for every network environment. Core Access provides the most easily accessible form of application and resource access from a variety of end user machines, with granular security and control options.

SSFHS has deployed the SA6000 as a high availability (HA) pair to provide seamless user failover in the event of a failure. The SA6000 hardware platform is designed to scale, with redundant hot swappable hard drives, power supplies, and fans. It also features built-in compression for Web and files, and a state-of-the-art SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes.

Results

In the fiercely competitive healthcare industry, every advantage counts, especially when it comes to providing physicians with the tools they need to care for their patients with the highest levels of quality and efficiency.

“Most of our hospitals have multiple competitors in their areas, so providing an easy-to-use, highly reliable remote access solution is an important competitive advantage for us to attract the best and brightest medical staff to our hospitals,” said Dr. Roskam.

SSFHS made physician access even smoother with the addition of single sign-on to key applications. SSFHS configured single sign-on between the SA Series appliance and Microsoft Active Directory, so users only need to log on once to access their most important resources. “Most of our core applications use a simplified sign-on,” said Roskam. “The advantage of the Juniper SSL VPN is that it simplified sign-on for our core applications, including PACS and the physician portal.”

Organizations have several options for providing remote employees and contractors with secure access to centralized applications, and for SSFHS, the SSL VPN approach was the smoothest. “Ease of use for the doctors is critical,” said Daniel Accinelli, CISSP and information security technologist at SSFHS. “An IPsec VPN client solution requires documentation on setting up users, which can be cumbersome. With an SSL VPN solution, establishing a VPN connection doesn't require any user input other than a user name and password.”

Dr. Roskam concurred: “The feature that tipped us toward Juniper was a zero-client setup.”

SSFHS noted another advantage of Juniper's SSL VPN. “One of Juniper's great features is that users can do password changes right from the login page. It's a huge help for physicians who are logging in but their accounts have expired. They don't have to call the help desk to get their password changed,” said Dr. Roskam.

With the SA6000, SSFHS can set up dynamic access privileges for clinical and other staff. When a user logs into the SA Series appliance, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Granular resource authorization policies further ensure exact compliance to security strictures, which are essential in any healthcare organization.

The IT team uses the Secure Meeting option on the SA Series appliance to provide end user support. “If IT needs to get into a doctor's computer remotely, the doctor is already familiar with the Juniper SSL VPN, so we can establish a connection easily,” said Accinelli.

Next Steps and Lessons Learned

“Five years ago, our decision was a bit of a gamble, because only a handful of companies had SSL VPN clients,” said Dr. Roskam. “The Juniper SSL VPN has proven itself to work, and we have continued to rely on it for secure access.”

For More Information

To find out more about Juniper Networks products and solutions, visit www.juniper.net.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.