

Preparing for H1N1: Virtual Appliance Enables Secure Remote Access to Business Critical Applications for Physicians and Staff

Solution Reduces Risk of Network Virus Outbreaks and Provides Reliable, Available and Scalable Access

Healthcare facilities around the country are preparing for a spike in H1N1 (Swine Flu) cases. At South Jersey Healthcare, network administrators need to provide secure remote access to business applications for physicians and staff so they can work remotely, reduce personal risk of infection and continue to deliver high levels of service to patients.

The South Jersey Healthcare Story

South Jersey Healthcare (SJH) is a nonprofit, integrated health care system, providing access to a continuum of health services. SJH provides hospital services, numerous community health clinics, home health services, and specialty services, which serve the medical and health care needs of Southern New Jersey residents.

Like other healthcare providers, SJH is committed to maintaining patient confidentiality and adhering to HIPAA standards. For physicians and staff that require outside access to patient data, SJH needs a secure way to authenticate, encrypt and control access to sensitive data. By migrating from AEP Netilla SSL VPN, a hardware-based platform, to the virtual edition of Netilla (Netilla VE), SJH is able to provide a scalable solution that protects the network, offers reliable performance, and delivers secure communication and application access that physicians and staff require when they are away from the office.

Reliable Remote Access

Whether it's the threat of an H1N1 pandemic or inclement winter weather, network administrators at SJH recognize the need to provide high levels of secure access to physicians and employees that will enable them to work from home when they are unable to be physically present at work. Although they had the Netilla SSL VPN appliance in place, it was an older hardware platform and becoming obsolete. Plus, the organization wasn't taking full advantage of its features and was restrictive in which employees could use it.

"One of our key challenges is providing physician and employee access into our system," said Andrew Gahm, systems and security engineer, South Jersey Healthcare. "Netilla is a secure appliance that gives us everything from SSL VPN to thin client access to terminal servers and reverse proxy access in a single device. It makes for much simpler access that doesn't need to be configured on individual PCs. With the threat of H1N1, we wanted to expand access so that anybody with a laptop or tablet can take it home and securely access our network. To support that goal, we are converting our physical platform into a virtual one using the Virtual Edition of the Netilla SSL VPN (Netilla VE)."

"The Netilla VE provides terminal server performance at home and enables our users to access their applications remotely as if they were in the office."

Andrew Gahm, Systems and Security Engineer, South Jersey Healthcare

Migrating to a Virtualized Environment

Netilla VE is a virtual application access gateway that enables secure Web browser access to a broad range of business applications. Remote users can quickly and securely reach the varied resources found in today's IT environment, including Microsoft Outlook, Windows Remote Desktop Services and server-based applications, as well as client/server applications over an SSL tunnel. SJH has two Netilla virtual appliances – linked via a Netilla Load Balancer – for the entire health system, sharing hardware with 135 other virtual servers.

"We have approximately 200 different applications running, and the performance through Netilla VE is excellent," said Gahm. "The Netilla VE provides terminal server performance at home and enables our users to access their applications remotely as if they were in the office."

Adds Tom Wurm, Jr., senior engineer with Adagio Consulting Group, "In healthcare, applications vary greatly in architecture from terminal emulation to Web to client server. AEP Netilla VE provides secure remote access that is hardware independent due to virtualization and offers flexibility in how organizations like SJHS deliver a diverse set of applications to their end users, ultimately providing the best possible experience."

The virtual implementation process is much easier than a physical implementation process. Instead of needing to get the physical device, hook it up to a

PC and boot with a CD, administrators can simply download a file, import it to VMware, assign an IP address and rapidly configure it. This reduces the process from hours to minutes.

“With the virtual edition, I’m able to spin up Netilla boxes on hardware I already have and I’m planning on setting up a virtual environment and disaster recovery in a second location,” explained Gahm. “I can easily move Netilla boxes from one location to another just by moving the virtual server to another physical server. I can also have Netilla use multiple network connections from different ISPs or different connection points on the same ISP.”

In addition to having a failsafe that improves uptime and access reliability, Netilla VE enables SJH to provide secure access both to physicians and staff using a company-issued tablet or laptop as well as to those accessing the network from their home PC. Users coming into the network from a home PC access it through Netilla, which is beneficial because servers aren’t exposed to the Internet. This reduces the risk of virus outbreaks or compromises to the network. Anybody with a company-owned laptop or tablet can take it home, connect to the network and it will authenticate that it is a SJH machine and ensure it is running up-to-date antivirus software. If it passes all the requirements, it will be allowed to VPN in and have full connectivity as if the computer was in the office.

“Application availability and security are always hot topics in healthcare,” said Jennifer Grillo, partner, Adagio Consulting Group. “And the need for remote access technology is growing fast. What makes Netilla VE an ideal solution is its ability to provide secure remote access to thousands of applications and the flexibility and functionality users require.”

“AEP Networks is ahead of the game when it comes to what they’re doing with the Netilla VE,” added Gahm. “They’ve recently added a solution that allows me to give users access to their desktops if they are left turned on – again without compromising the network. If there is a pandemic and 500 people cannot make it into work but their desktops are on I can give them full access from their home PCs. Netilla also has a feature where if users transfer files while they’re connected it can check and remove them from the home PC and clean up after itself. It’s one of the highest level security devices I’ve ever seen.”

Why AEP Netilla VE?

“AEP Networks’ Netilla VE gives us the connectivity that our physicians and staff need and requires very little support on our end. When we do need support, the customer service I have received from AEP Networks is top of the line. There are certain products you would stake your career on when you choose them and this is certainly one of them.”

About AEP Networks

AEP Networks offers secure communications, networking and application access for government, enterprise and carriers. We work with systems integrators, managed service providers and the distribution channel to deliver integrated solutions incorporating our leading edge products:

- Enhanced-grade secure voice and multi-service data platforms (based on the vadOS operating system) that support a wide range of communications protocols and network topologies
- High assurance networking via IPsec-based VPN encryptors for site-to-site security and remote access
- Hardware Security Modules (HSMs) for cryptographic key management and storage
- Secure remote access to networks and applications – including virtual environments – via application-layer security gateways and SSL VPNs.

Headquartered in Somerset, New Jersey, AEP Networks has key offices in the United Kingdom (Hemel Hempstead & Ascot), Malaysia and Australia.

Contact AEP Networks

info@aepnetworks.com, www.aepnetworks.com

U.S: 877-638-4552 x5219 • EMEA: +44 (0) 1442 458 600 • Asia/Pac: +60 (0) 3 2166 2260 • Aus/NZ: +61 (0) 2 9413 2282