



SECURE ACCESS FOR HEALTHCARE: SSL VPN ADVANTAGES

An AEP Networks White Paper

Introduction

Providing physicians and other caregivers with secure yet simple remote access to medical applications has emerged as a “must-have” for healthcare organizations. It’s not hard to see why momentum is building behind the new generation of remote access solutions. Healthcare organizations can leverage their investment in Picture Archiving and Communications System (PACS), electronic patient order entry (POE) systems, and other clinical applications and provide real-time access to patient health information, while maximizing physician time and productivity. Implementing the right remote access solution can lower costs, raise productivity and even bring about improved patient care.

The path to the best strategy, however, is not always clear. Hospitals deploying remote access solutions have been faced with something of a balancing act: How to make healthcare data available to authorized users outside the hospital’s walls in the most cost-effective manner, while ensuring the privacy and security of that critical patient data to meet the Health Insurance Portability and Accountability Act (HIPAA)?

Traditional remote access approaches—leased lines, dial-up remote access servers (RAS), and Internet Protocol Security (IPSec)-based VPNs—have proven inadequate to the task. Toll charges, deployment complexity, maintenance costs, lack of scalability and security concerns have led healthcare facilities to consider alternatives.

As a result, Secure Sockets Layer (SSL) VPNs have emerged as the logical choice for extending hospital network resources securely and cost effectively. AEP Networks has provided such remote application access solutions for over 150 healthcare organizations. Their ease of use, fast Return on Investment (ROI), and elegant reliance on the ubiquitous web browser validate SSL VPN technology as the best way to make clinical information easily yet securely available to remote physicians and other healthcare workers.

SSL VPNs: Simplified Use, Streamlined Security and Access Management

Since originally developed by Netscape to secure electronic commerce transactions, SSL, which is also referred to as IETF standard Transport Layer Security (TLS), has evolved into one of the leading security protocols throughout the Web. SSL provides server authentication, data encryption, and message integrity over TCP/IP connections. SSL today supports millions of online transactions daily and is the de facto standard for secure online credit card purchases, stock trading and banking.

SSL VPNs provide a number of advantages that are attractive to the healthcare industry, including their use of widely deployed, ready-made access clients: the Web browsers built into every modern computer. By taking advantage of this "client-less" deployment, SSL VPNs minimize the need to configure and maintain remote computers.

Taking the "client-less" deployment one step further, SSL VPNs such as the AEP Netilla Security Platform (NSP) provide an additional key benefit: easy access to legacy (Windows, Citrix and mainframe) applications quickly and securely over the Internet. This crucial functionality differentiates the various SSL VPN approaches, some of which are limited to Web applications or network file access only. The fact that remote users can leverage the NSP to access centralized applications securely from any Web browser frees IT staff from having to install, update and maintain application clients on hundreds of remote PCs.

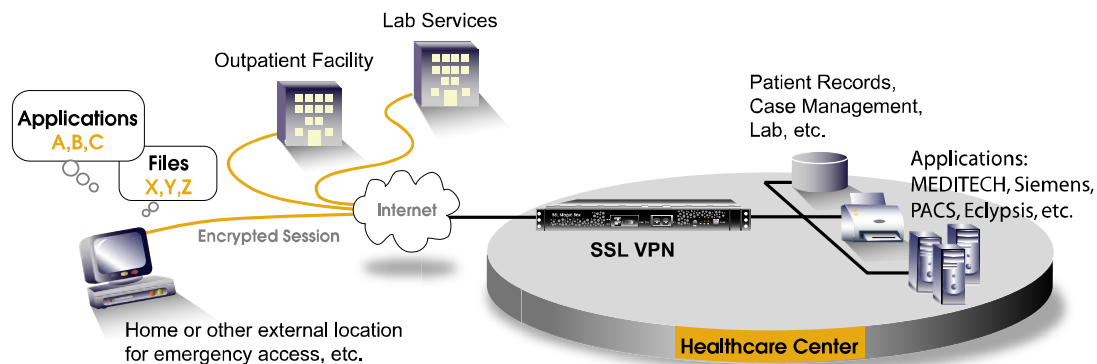


Figure 1: Remote Access Healthcare Network

Application Layer Proxy-based Security: Supporting Web, Microsoft Windows Terminal Services, and Citrix MetaFrame Environments

Beyond the deployment and access advantages brought by web-based approaches, SSL VPNs like the NSP deliver significant security advantages that are crucial to healthcare organizations concerned with meeting HIPAA regulations. In general, these advantages accrue from the application layer proxy access model that SSL VPNs employ; in particular, the NSP takes this approach one step further by incorporating Web-enabling technology directly within the platform.

In this “thin-client” computing model, shown in Figure 2, application processing is performed on datacenter-based servers (both Web and Terminal Servers), while the end user’s computer handles only the input and output data (keystrokes, mouse clicks, and graphical display). One advantage of this secure, “application layer proxy” arrangement is that the NSP generates a proxy or a representation of the application, rather than requiring application itself to be resident on the user’s PC. This means that the remote user gain access to any number of applications through native protocols - including Remote Desktop Protocol (RDP) data for Windows-based applications, Independent Computing Architecture (ICA) for Citrix MetaFrame applications, or HTML for web servers — via a single protocol, secure http (HTTPS). In this way, the NSP “proxies” the user’s traffic - network resources are kept safe on the private LAN. End users never directly access the applications and servers themselves.

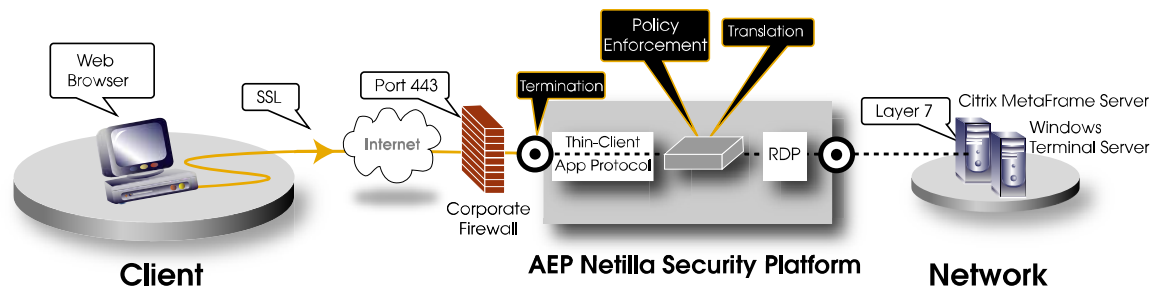


Figure 2: Thin Client Access to Server-based Applications

This powerful story means that an organization can extend applications to remote clinicians over the Internet without having to place application servers in a publicly accessible area, or having to install local versions of the applications themselves. Placing application servers in such a “Demilitarized Zone” (DMZ) would require much hardening to lock down and protect. Instead, with the NSP, application servers can remain safe on the private network behind the firewall, and are never exposed to the public network, while users gain access to the full, native versions of server-based applications, rather than just the stripped down, “webified” translations.

In this model, the NSP initiates a session to the application server – typically a Windows Terminal Server - on behalf of the user, and presents a rendering of the session to the remote user’s web browser. This allows the user to interact with the application as if it were installed locally no matter where they are located. The NSP “intermediates” the connection between remote-client requests and the network server, terminating incoming connections at the

application layer. Once the incoming request is terminated, the NSP processes and translates the data to the appropriate backend application protocol – such as RDP for a Windows Terminal Server. The NSP then resends the application data back to the user's browser, in the form of HTTPS traffic via “screen scraping” technology. A key point in this arrangement is the network protection advantages that such a scenario provide: At no time is the enduser directly connected to a “private side” network resource. The NSP SSL VPN appliance thus functions as a proxy on behalf of the remote user, protecting the application servers from direct exposure, and controlling access on a session-by-session basis.

A similar proxy approach is also well suited for Web-based applications. In this case – shown in Figure 3 - the NSP terminates, examines, and rewrites HTTP requests. Remote users are then presented with Web application resources as allowed by corporate-defined security policy. With this approach, a single point of entry over the Internet – the NSP itself – remote users gain access back-end, intranet Web servers that are otherwise inaccessible over the Internet, and do so securely and simply through a Web browser.

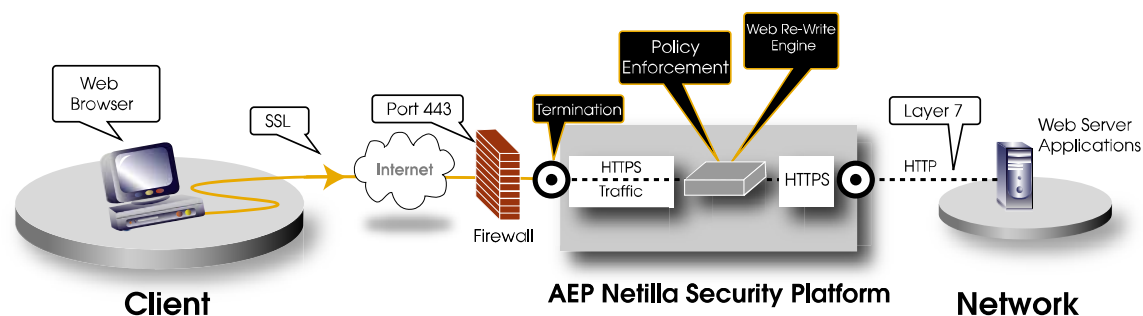


Figure 3: HTTP Reverse Proxy for Web Applications

Web Portal Security: Defining Policy and Access Rights

SSL VPNs like the NSP allow network administrations to create custom access portals to specific application as defined by policy. This means that different users gain access to key application depending on their role, or requirement. Network resources are not exposed to the entire user base: Administrators can set user permissions and policies to limit access to specific applications for specified users as needed. For example, some physicians who work directly with billing applications will be presented with just those applications upon sign-in. Others, who may be affiliated only with the radiology department of a facility, will be limited to “seeing” only the PACS application, for example.

Achieving HIPAA Compliance

As part of any access implementation criteria, the healthcare industry must consider rigorous federal standards regarding the privacy of Protected Health Information (PHI) dictated by HIPAA. SSL VPN appliances in general – and the NSP in particular - combine a number of security elements into a unified, hardened appliance that help healthcare organizations meet their HIPAA concerns with confidence.

These include multi-factor authentication — such as RADIUS, VASCO, RSA SecurID®, Active Directory, LDAP — policy, encryption, and third-party trusted digital certificates for site authentication. The confidentiality of PHI is further ensured through a deeply integrated, robust endpoint security solution that provides host integrity checking, a secure desktop environment, cache cleaning and adaptive policies, as well as securing the identification of an approved computer before it is allowed access to the network. Configurable session timeouts and optional forced re-authentication further help prevent “digital leakage” of private information, while event logging capabilities assist in achieving HIPAA compliance by documenting security incidents and attempted security breaches. Further, the NSP has earned key industry security approvals, including ICSA Labs' prestigious SSL VPN Gateway Certification and Virtual Private Network Consortium (VPNC) certification, and boasts a roster of hundreds of healthcare organizations who rely on the NSP for secure access to medical applications every day.

SSL VPNs in Action: Healthcare Case Study

When the largest healthcare provider in southern New Jersey needed a solution to provide secure access to over 900 remotely located physicians, they faced a difficult choice. As a non-profit organization, concerns over security and HIPAA were just as important as their need to keep costs low. They needed an intuitive access solution that would not overtax the hospital's IT support team. For all of these reasons, maintaining software clients on PCs outside the hospital's control would not be acceptable.

The hospital had already enjoyed a successful rollout of Siemens Physician Dashboard, a web-based, clinical system for results reporting, billing info, and medical reference. Yet when remote physicians began upgrading their PCs, they were unable to access the Siemens application, which did not support newer web browser versions. At the same time, the hospital wanted to provide their large deployment of server-based medical applications for remote access, yet found their attempts to roll out these Citrix-based applications challenging, since it required installing and configuring Citrix ICA clients on remote PCs. Furthermore, vulnerability scans performed by internal security consultants concluded that there were too many ports open on the hospital firewall for incoming Internet traffic, compounded by the Citrix application servers. The hospital needed to find a way to close down these multiple ports, which were a requirement for remote access into their Citrix server farm, and reduce their network exposure.

The hospital rejected an IPSec VPN approach, which would have required proprietary VPN clients on each remote PC – as well as an application client itself. Installing and maintaining clients and applications on remote computers presents real challenges in the remote physician model. In addition, IPSec VPNs establish a true network-level connection that makes it difficult to control which applications and network resources a remote user can use.

For these reasons, the hospital sought a web-based approach that would solve these concerns, concluding that an SSL VPN would best meet their needs. SSL-based VPNs operate at the application-level, providing fine-grained access control over which specific applications an authorized user is granted access to. Because a standard Web browser functions in effect as the VPN endpoint, no special software client needs to be installed and maintained; and

the 128-bit SSL encryption embedded into the browser encrypts communications as effectively as it safeguards credit card transactions. Another advantage of an SSL VPN is that by operating as an application-layer proxy between the remote user and the enterprise application server, there is no direct network-level connection – an important security plus. Because of their clientless nature, SSL VPNs are increasingly being used to provide remote access to the “nomadic fringe” of users who need to access applications anywhere, anytime and from any PC.

The hospital ultimately selected the NSP from AEP Networks. The NSP, with its ability to provide access to both Web-based and server-based applications, distinguished itself from competitors, allowing the hospital to greatly expand the number and type of applications they could deliver through their Physician Portal. Further, IT and help desk support requirements for the NSP promised to be minimal compared to IPSec and server-based remote access alternatives, since the NSP leverages the web browser as an access client.

Since deploying the NSP SSL VPN for remote access, the results have been positive -- with the system fulfilling its mandate of delivering browser-based remote access to multiple Health Information System (HIS) applications, with a high degree of security, and at a significantly lower cost than alternatives. With all encrypted traffic entering the network via one incoming firewall port – port 443, already open to secure SSL traffic – the hospital was able to satisfy their internal security requirements and close down their large number of open ports. Remote physicians now gain access to the Web portal from any location, from any standard Web browser. Once within the portal, physicians can access the Siemens dashboard application as well as numerous other programs, including medical reference libraries and drug interaction databases. Thanks to the NSP's ability to access client/server applications via thin-client technology, the hospital has been able to provide access to more than 50 applications to their user community, including much simpler and secure browser-based access to Citrix-based applications. The NSP's highly granular access controls provision each authorized user with only those applications he or she is allowed to use, providing a clear benefit over the full-network access typified by IPSec-based VPNs. And the NSP's ability to enforce enterprise security policies for all users – regardless of whether they are remote or onsite – have proven to be a powerful security advantage. The NSP has in fact become a secure gateway to the hospital's enterprise applications rather than simply as a remote access tool.

Finally, the NSP enabled the hospital to deliver remote access while conforming to HIPAA security and privacy mandates. The HIPAA security standards define a broad set of administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic PHI. The privacy rule governs authorized usage and disclosures of PHI, as well as patients' rights to view their PHI and to know who has seen it. With the use of an SSL VPN solution, the hospital has been able to comply with these HIPAA requirements by restricting access to PHI to specified users only via fine-grained access controls.

Conclusion: The Best Solution for the Healthcare Industry

SSL-based VPNs are particularly well-suited to meet the anytime, anywhere remote-access needs of the healthcare industry in general, while complying with the broad security demands of the industry in particular. Certainly, healthcare institutions need to choose the remote access solution that best meets their needs for a particular implementation. But taking into account its "total cost of ownership" benefits, its simplicity from a user's standpoint, the ease with which it can be deployed, and its ability to help meet HIPAA mandates, the NSP from AEP Networks is poised to bring the benefits of secure remote access to thousands of health care organizations around the world.

Contact AEP Networks

info@aepnetworks.com

www.aepnetworks.com

Corporate Headquarters	Government Solutions Group	
AEP Networks 347 Elizabeth Ave., Suite 100 Somerset NJ 08873 Toll-Free: 1-877-638-4552 Tel: +1 732-652-5200	AEP Networks 40 West Gude Drive, Suite 200 Rockville, MD 20850 Toll-Free: 1-800-495-8663 Tel: +1 240-399-1200	
European Headquarters	Asia-Pacific	Japan
AEP Networks Focus 31, West Wing, Cleveland Road Hemel Hempstead Herts HP2 7BW U.K. Tel: +44 1442 458 600	AEP Networks 2107 Tower 2 Lippo Centre 89 Queensway Hong Kong Tel: +852 2845 1118	JOYO Bldg 6-22-6 Shimbashi Minato-ku Tokyo 105-0004 Japan Tel: 81-3-3432-3336