Aventail SSL VPNs: The Right Prescription for Healthcare

Executive Summary

The healthcare environment is changing, and this evolution is impacting healthcare providers, physicians, and the technology that must support them. Doctors are more mobile than ever, frequently working from multiple locations, such as hospitals, private clinics, and universities. There is a dearth of some specialists, such as radiologists, who must provide their expertise and counsel from geographically remote locations.

At the same time, healthcare providers must meet strict privacy and security regulations, complying with the Health Insurance Portability and Accountability Act (HIPAA) and other government and industry policies. Even with U.S. government powers touting “a new age of healthcare IT” with the National Health Information Infrastructure (NHII) initiative, the reality is that healthcare IT faces many challenges in handling existing mobility and security issues. All of this with strapped IT budgets and manpower and increasingly complex computer networks.

So, it is with limited IT resources that healthcare organizations must find cost-effective ways to support the mobility of today’s doctors and meet regulatory demands.

While no single solution can handle all of these issues, many healthcare providers are turning to SSL VPNs (secure sockets layer virtual private networks), which offer clientless secure remote access of vital information and healthcare applications from virtually anywhere on any device. SSL VPN remote access solutions from companies like Aventail have some obvious benefits in providing cost-effective, secure remote access that is easy for the end user and for the network administrator.

Specifically, SSL VPNs can provide:

- Secure, encrypted transfer of confidential patient information and other resources from one system to another
- Strong support for security and privacy regulations such as HIPAA
- Secure access to billing and administrative records
- Ability to manage risk at unknown end points
- Ability for employees, physicians and vendors to gain intranet access to e-mail and other applications anywhere, anytime from any device

For healthcare providers who have implemented an SSL VPN, the ROI is clear and immediate, including increased productivity and time savings for IT staff, administrative personnel and physicians, lower support costs, ease of billing

Mount Sinai NYU Health

Business Challenge

To optimize patient care, some 1,000 mobile doctors, in-home nurses, and administrators needed immediate secure access to a variety of critical applications. Patient records, medical lab results, and administrative applications needed to be available to remote users over the Internet with the same level of access and security as to their internal users.

Solution

Mount Sinai quickly and successfully deployed Aventail’s SSL VPN. “The physicians and nurses found the transition to the new service seamless,” explained Fred Eisenberg, Director of Information Security, “Their ability to access their clinical desktop was uninterrupted. And, by migrating our users onto Aventail we saw significant cost savings. In addition, Aventail provides such easy access that we’ve been able to more than double the number of doctors and nurses using the system to access their clinical desktops.”

Benefits

- Higher application access availability for doctors, nurses, and administrators—contributing to improved patient care.
- A more secure infrastructure, helping Mount Sinai to comply with HIPAA regulations.
- A single infrastructure for access, making it easier to give more doctors and other healthcare workers clientless anywhere access.

> "As a former healthcare IT executive, I believe SSL VPN is a 'no brainer' for any healthcare provider that wants to provide secure remote access the right way."
>
> —Joe Brisson
> Healthcare Practice Leader,
> PSC Group

and reimbursement, and peace of mind regarding security and privacy. What's more, many hospitals are finding their SSL VPN technology provides them a competitive edge in attracting doctors and specialists to their hospital.

Remote access for today's mobile healthcare system

In the past, remote access was handled on a case-by-case basis for most healthcare providers. Perhaps the hospital CEO wanted remote access or a physician offsite needed access in the middle of the night to a patient file, so the IT department would put together a solution to meet these immediate needs. However, increasing physician demand for remote access—and the need for absolute security of that access—has brought this issue to the forefront.

Gnaden Huetten Memorial Hospital, a 111-bed hospital in Pennsylvania, was a typical example. The hospital wanted to give physicians more access to information they needed to make healthcare decisions and for streamlined billing processes. What's more, after a partnership with another institution near by, hospital executives wanted access to files and e-mail from both hospitals. George Sanchez, director of information services, looked at a lot of vendors and solutions before coming across SSL VPN. Today, physicians, employees and support personnel all go to an easy-to-use portal, where they click on a link and access vital information, all within the secure SSL VPN environment.

"The Aventail SSL VPN has made us heroes," says Sanchez. "Everyone that needs access has it wherever and whenever they want it, and we know it is secure and meeting regulations. And because it's clientless, there are no more calls to IT or to the records department, which has saved time and money for the hospital."

Supporting access from more places, more devices

Today, many physicians, particularly specialists, treat patients in multiple geographically-distributed locations, including hospitals, private clinics, and universities. They need access to a broad range of information—electronic patient records, lab results, drug efficacy information, and other systems—so they are able to offer the most appropriate, sometimes life-saving treatments. And when on-call, these physicians need access to the same confidential information from their home offices any time of day or night. In addition, doctors' offices need access to billing information and patient records from hospital systems.

Geographically remote doctors may provide best care

By providing secure anywhere access to specialists, healthcare organizations can provide patients with expert medical care. Centers of excellence are no long guaranteed in major cities. And for rural hospitals, the need for securely connecting doctors to patients and their information is crucial. For example, a West Coast healthcare provider uses Aventail SSL VPN technology to securely supply MRI, x-ray, and ultrasound images from multiple clinics to an Arizona-based radiologist for viewing and diagnosis. Local technicians from a variety of locations perform the necessary diagnostic tests, entering test results into a centralized hospital system. Digital images are

Support for any healthcare technology

Aventail supports applications from vendors such as:

- **Cerner**
- **Epic**
- **McKesson**
- **SMS**
- **IDX**
- **Misys**
- **Meditech**
- **GE Medical**
- **Siemens**

Healthcare providers can use Aventail to provide users with secure access to applications that streamline:

- Enterprise care management
- Laboratory radiology (LAB/RAD)
- Financial or billing information
- Practice management
- Case management
- Utilization management
- Electronic medical records (EMR)
- Cardiac monitoring

In addition, Aventail has helped customers to leverage their **Citrix** investments.

then available to a specialist for diagnosis. Whenever a local radiologist is unavailable, patient information, radiological images and laboratory results are easily and securely accessible by a remote specialist for diagnosis and treatment recommendations.

SSL VPNs: Broad access with low support costs

Hospital IT staff are often asked to do more with less. Not only do they need to provide remote access to a growing number of users and devices, they need to provide access to a broad range of resources—including Web, client/server and file sharing. Ideally they need a remote access solution that minimizes IT costs. While some hospitals try to make an existing IPSec VPN or other traditional solution work for remote access, most find that it doesn't adequately fit their needs for broad application access, and that the administrative complexities are too time-consuming and support costs are too high.

SSL VPNs deliver lower costs

SSL is easier to install and manage than a traditional IPSec-based VPN. Ongoing administration is also simpler with an SSL VPN. You'll spend less time on maintenance, which typically results in long-term savings. Plus, affiliated healthcare organizations won't need to increase their networking costs with equipment purchases and meet end-to-end integration requirements just so the VPN will work.

In addition, because SSL is included in standard Web browsers, SSL VPNs offer a clientless solution. This eliminates the administrative headaches of distributing and managing VPN clients to an entire provider/payer network, and can be easier to support in the long run.

SSL VPNs enforce security policy and help meet HIPAA compliance

In addition to the security and privacy regulations of HIPAA, U.S government powers are promoting a new age of healthcare IT with the National Health Information Infrastructure (NHII) initiative. This new government framework for transforming health care using IT includes:

- Promoting the use of electronic health-records and decision-support systems in physicians' offices
- Connecting clinicians so medical records follow patients from one point of care to another

With these initiatives, plus the broadening of remote access to end-points your IT department doesn't control, security issues become both increasingly critical and more difficult to manage.

Strong data encryption and authentication

With the electronic transfer of confidential patient information that takes advantage of the Internet, encryption and authentication are crucial. Most SSL VPNs offer strong data encryption. Strong authentication is also absolutely necessary in ensuring that the radiologist reviewing a patient's x-ray is exactly who he says he is. Aventail offers two-factor authentication that works with virtually any authentication system.

Aventail for security and HIPAA compliance

Designed with security in mind, Aventail's hardened SSL VPN appliances offer additional security options to protect your information assets:

- **Strong data encryption** for remote VPN access to applications or network resources.
- **Strong authentication**, including support for two-factor authentication such as RSA SecurID tokens and digital certificates.
- **Unified policy management and granular access control** across all back-end applications or resources, down to the specific user, resource, or URL.
- **Aventail Cache Control and Aventail Secure Desktop** provide data protection for access from end points your IT department doesn't control.

Easy, granular access control

SSL is a higher-layer security protocol that sits closer to the application in the OSI model and provides more granular access control than IPSec. That enables SSL VPNs to deliver very granular access control to help you maintain privacy of confidential information by easily controlling who can access the corporate network.

Aventail SSL VPN solutions combine these security features with ease-of-administration. You can easily manage and control access down to the user and resource level—even down to the specific URL—so physicians, case managers, and other authorized health partners are granted appropriate levels of access to applications and medical information. For example, only physicians with an established "need to know" can gain access to predetermined information. Authorized users and health partners (other providers or hospitals, government agencies, brokers, insurance companies, billing companies, etc.) can be added or deleted within seconds.

Customers frequently use Aventail's SSL VPNs with applications from companies including:

- BEA (Tuxedo, WebLogic)
- Cisco
- Check Point
- HP (HP-UX, OpenView, VMS)
- IBM (AIX, AS/400, DB2, Lotus Notes, Tivoli, WebSphere)
- ISS
- Lucent
- Microsoft (Exchange, Office, Outlook, SharePoint, Windows)
- Network Associates
- Nortel
- Oracle (databases, applications and tools)
- Peoplesoft
- Red Hat
- RSA Security
- SAP R/3
- Siebel
- Sun (Solaris, iPlanet)
- Symantec

Controlling the end point

Strong authentication, encryption, and even granular access control alone are not enough if patient records and other confidential information may be opened on devices your IT department doesn't control.

Aventail® Cache Control™ and Aventail® Secure Desktop™ can help you better protect sensitive information and network resources accessed from airport kiosks, wireless hot spots, home PCs, and PDAs.

Since Web browsers cache all data on computers, users may unknowingly leave sensitive information such as passwords, cookies, and documents stored on the computer—especially if they do not log off. This is a serious issue for public computers where the next, unauthorized, user can easily view sensitive information unintentionally left behind. With Aventail Cache Control and Aventail Secure Desktop, organizations can feel confident about extending secure remote access from non-corporate-owned equipment. Aventail Cache Control removes Web pages, temporary files, viewed e-mail attachments, browser history, cookies, auto-complete or stored passwords, and temporary or download files from any Windows, Macintosh, and Linux-supported device even if the user walks away. Aventail Secure Desktop creates a temporary virtual desktop and then erases the data completely from the system upon termination of the session.

Conclusion

Healthcare IT managers and industry experts expect the demand for secure remote access to continue to expand. Driving this growth is the mobility of physicians and healthcare workers, regulatory pressures on security and privacy, the government push for digitalization of healthcare, and the continued need to control IT costs. Healthcare providers need a solution that offers the flexibility of anywhere access, with the ensured security to handle the risks that access introduces. Leading healthcare providers depend on Aventail's proven SSL VPN appliances and managed services to stay ahead of government mandates and to deliver better patient care, attract quality physicians, comply with government regulations, and reduce administrative costs.

Aventail: the leading SSL VPN product company

Aventail is the leading SSL VPN product company and the authority on clientless anywhere secure access. Aventail's appliances and managed services deliver secure, seamless access from anywhere, to any application, on any device. With the most widely deployed SSL VPN on the market, Aventail is positioned in the Leader quadrant in Gartner's 2004 SSL VPN Magic Quadrant and was recently awarded "Best VPN" by *SC Magazine*. Major service providers such as AT&T, IBM Global Services, MCI, Sprint, SITA SC, and Bell Canada have built their SSL VPN managed service businesses on Aventail's technology. To find out what Aventail customers like Aetna, DuPont, Office Depot, Sanyo, and TNT already know about Aventail's SSL VPN, go to www.aventail.com.

Aventail™

Corporate Headquarters
808 Howell Street
Seattle, WA 98101
Tel 206.215.1111
Fax 206.215.1120
americas@aventail.com
www.aventail.com

Aventail Europe Ltd
Tel +44 (0) 870.240.4499
emea@aventail.com

Aventail Asia-Pacific
Tel +65 6832.5947
asiapac@aventail.com