

Making a healthy move away from IPsec VPN



Marcia Savage shows how one healthcare organization dealt with the problem of remote access security

With physician offices and hospitals spread out across 325 miles, having a safe system for doctors and other staffers to remotely access email and medical images was critical for Marquette General Health System (MGHS). Unfortunately its remote-access solution, a traditional IPsec VPN, had become a headache.

The system required client-side software, so MGHS engineers had to go to doctors' houses to install the software, which was cumbersome, explains Greg Gagnon, supervisor of enterprise systems and services at MGHS. Then, physicians sometimes installed other programs on their computers that were incompatible with the VPN client, preventing them from accessing the information they needed.

"They would try to use it and, when it didn't work, they'd call our helpdesk at two in the morning," recalls Gagnon. "By that time, the doctor is fed up. He's driving in here anyhow to read the case. He's mad. Our staff are waking up in the middle of the night and driving in to figure it out."

With business growing and remote-access needs growing too, MGHS began the search for an alternative. MGHS includes a regional medical center, several primary and specialty-care physician offices, home health services and an assisted-living facility. The organization partners with 14 community hospitals in Michigan's Upper Peninsula.

"Our primary goal in the beginning was to look for a product that worked with our email system and also with our teleradiology [system]," says Gagnon.

For email, MGHS uses Lotus Notes, both the web-based and fat-client versions. Its teleradiology system electron-



Marquette General Health System is using the FirePass SSL VPN from F5 Networks to improve its remote access

ically transmits images such as CTs, MRIs and X-rays so that physicians and radiologists can access them remotely.

MGHS looked at remote-access solutions with client software as well as products in the growing market of SSL VPNs, which do not require clients. "We looked at quite a few other vendors' applications, but they either didn't work or were very slow," says Gagnon.

In particular, some of the products MGHS tested could not handle its teleradiology system. "The throughput of the images was real slow. It was slow on a LAN, let alone trying to access them through the internet. We just couldn't have that," explains Gagnon.

But MGHS found its solution in one particular SSL VPN—the FirePass controller from F5 Networks, which handled the images and Lotus Notes without a hitch, he says. F5 acquired the SSL VPN technology last summer when it bought uRoam.

Now, the healthcare organization's

physicians can securely access images, email and information from other applications from any location and any web-enabled device. A radiologist on call, for example, can access an image from home via a standard web browser.

"A physician could be at his mother-in-law's house, say, when he gets the call, and as long as she's got an internet-connected computer, it wouldn't matter," says Gagnon.

In addition to images and email, physicians can access the organization's knowledge-based systems, so they do not need to be at the office or hospital to look up a medical journal.

The SSL VPN also helps streamline the work of MGHS's IT engineers. Not only does it eliminate the time they used to spend implementing and maintaining VPN clients, but it allows them to deal remotely with any issues that crop up during off hours. Instead of getting in the car at night and driving through freezing weather and several inches of

snow to get to the hospital, engineers can use FirePass to fix the problem remotely, saving time and frayed nerves.

Altogether, MGHS has 221 users accessing about a dozen applications via the FirePass box. The system is much more scalable than the old remote-access solution, which only had 12 to 24 users, says Gagnon.

As well as physicians and system administrators, vendors and outside contractors use the MGHS SSL VPN. To help it troubleshoot problems or deploy updates, MGHS enables vendors to access various systems via FirePass. One of the organization's partner hospitals requires contractors to provide dictation services remotely, which reduces the cost of having a regular transcriber on-site.

Gagnon says pinpointing the actual savings MGHS achieves with FirePass versus its old IPsec VPN is difficult. But the product clearly saves doctors and other users a lot of time. He adds: "It's the soft costs that are the saving grace."

According to Breakaway Marketing Group, a market-research firm focused on network security, the need to install and maintain IPsec clients is the primary cost difference between an IPsec VPN and an SSL VPN. The firm estimates an SSL VPN can save a company with a 500-user community that supports around 100 concurrent users more than \$100,000 over the first three years of ownership, compared to an IPsec VPN.

Aside from efficiency, FirePass provides MGHS administrators with better control over who is accessing the network remotely, points out Gagnon. The appliance's audit services provide reports from session and activation logs.

"It allows us to monitor and control it a lot better because we have a log of who was in and when they were in," he says. Under the old system of using modems, engineers had no way of knowing who was dialing into the network and when, creating a security risk. "If you have some 50 modems scattered everywhere and you don't even know about half of them, there's a problem," notes Gagnon.

FirePass helped MGHS lock down its network. "We're streamlining it [remote access] down to one central point, where we can manage the security of it and

have people accountable, and one place to change passwords," explains Gagnon.

The appliance offers granular access control by allowing administrators to authorize various levels of application access based on the user and what type of device they are using. FirePass also checks client PCs for security policies such as anti-virus protection or personal firewalls before allowing the machine full network access.

Gagnon also likes the device's cache and temporary file cleanup feature,



No news is good news. Usually you hear about things that aren't working in IT

Greg Gagnon, supervisor of enterprise systems and services, MGHS

which helps safeguard patient data as required by *HIPAA*. When a user logs off or times out, the ActiveX control that was downloaded after login will overwrite and delete the cached and temporary files. That ensures that a user does not inadvertently leave behind patient or other sensitive information on a café kiosk or other public system.

"The healthcare market with *HIPAA* requirements is a natural for an SSL VPN solution like FirePass," says Dore Rosenblum, director of product marketing at F5. "We allow a user to implement the strong security they need for remote users accessing information on their network and it's very simple, so it enables them to do so without a lot of client footprint."

Deployment of the appliance at Marquette General Hospital was easy and did not require any special training, recalls Gagnon. MGHS used the appliance's internal database to authenticate users, but generally, notes Rosenblum, customers use their existing Radius, Windows Domain Servers, or other authentication systems.

FirePass also supports RSA Security's SecurID two-factor, token-based authentication. "The way FirePass was designed was to drop in and integrate with literally any authentication system in place," he adds.

MGHS also bought a redundant box

for failover purposes, something that many FirePass enterprise customers with high-availability requirements do, says Rosenblum.

"We test it every time we do an upgrade, but we don't usually have to use it," says Gagnon. "Because of the physicians and the need, I wanted to make sure we had a redundant box just in case."

For example, in the event that a power plug is pulled out and a server fails, the failover server will take over and user sessions are not disrupted, says Rosenblum. "In certain environments, where you're doing a large image transfer, the last thing you want is to have your session disconnected where you have to start all over again."

The only challenge with the SSL VPN was educating the doctors how to use a different type of remote-access system. "In a month, most all of the key radiologists were fine. It just took a little time getting people used to a different way," recalls Gagnon.

He does not get much feedback on the system which he says is a good indicator that people are happy with it. "No news is good news. Usually you hear about things that aren't working in IT more than you hear about things that are."

In the future, MGHS might contemplate rolling out the desktop feature in FirePass to more users. The Desktop Adapter available for FirePass allows for secure remote control of Windows desktops from a web browser supporting Java or ActiveX downloads.

For example, an IT administrator might have a bunch of tools on their desktop at work that they cannot access remotely on the network, explains Rosenblum. The Desktop Adapter enables the administrator to use FirePass to run those tools from a home PC. "It is a nice feature and works well for being able to take over your desktop at work. I use it and love it," says Gagnon. "Everyone wants it, but do they need it?"

Down the road the main challenge will not have anything to do with the FirePass appliance. Rather, it will be "making sure we have enough bandwidth on our internet service to keep up with demand. That's our next, bigger challenge," concludes Gagnon. ■