# IPSec VPN alternatives gain ground

■ BY TIM GREENE

Vendors say Secure Sockets Layer gear now can connect remote users to corporate networks as if they were on the LAN, just like IP Security gear does, but without having to install permanent VPN clients on remote machines.

With Neoteris' introduction of Network Connect software last week and the earlier availability of VPN Connector from uRoam (since bought by F5 Networks; see www.nwfusion.com, Doc Finder: 7047) and Aventail Connect from Aventail, customers can avoid the hassles of distributing and managing dedicated clients.

Instead, software agents are downloaded to remote PCs after they are authenticated to an SSL appliance located between the Internet and the corporate network.

The clientless aspect of SSL remote access has been considered a big advantage by many customers that lack the resources to maintain large IPSec deployments. (For more on the SSL-IPSec debate, see the Face-Off on page 48.)

The downside had been that SSL gear supported only proxy access to Web-based applications and certain client/server applications. Server-initiated applications, such as Net Meeting, and some custom-written applications were inaccessible. Because IPSec creates a network-layer connection, any application available on the LAN is also available via an IPSec tunnel.

Previously, SSL vendors acknowledged that when users needed network-layer access, IPSec was the way to go. Now that argument is decreasing.

Maxim Management Services, a medical administration service provider in Buffalo, N.Y., is weaning its remote users off IPSec-based Cisco remote-access gear in favor of Neoteris' Network Connect because it dramatically reduces time spent solving client-software problems, says Randy Coleman, Maxim's CIO.

The company has used Cisco VPN gear for two-and-a-half years to give doctors and affiliated medical groups access to Maxim applications. The company tried to switch to SSL but one of its applications, called Medent, would not connect through the previous version of the Neoteris gear because it used unpredictable and uncommon firewall ports. With Network Connect, that limitation is gone. "We will use the Cisco [VPN gear] as a backup," Coleman says.

"There is no reason for IPSec to be preferable" over SSL, says David Thompson, an analyst with Meta Group, but customers should be aware of what peripheral security is on the remote machine. Without a personal firewall and without anti-virus protection, the machine could become an access point for hackers and viruses, he says. Aventail and Neoteris have partnered with firewall and anti-virus vendors to provide these features.

Support issues have driven businesses from IPSec to SSL for years, with many organizations maintaining both for different sets of users.

While some SSL vendors offer network-layer support that gives access to applications as if the remote machine were on the LAN, they all also offer Layer 7 access to Web applications and many client/server applications as well. So it is not necessary to give everyone network-layer access. With IPSec, network-layer access is the only option.

Loews, a conglomerate in New York, uses both Cisco IPSec VPN gear and Whale Communications SSL remote-access equipment for this reason, among others. The IT staff needs network-layer access to perform its job, and uses the IPSec VPN. But most users — about 500 of them — need access to just a few resources such as e-mails, faxes and access to the company's intranet, and they use the SSL gear, says Al Alexander, manager of Loews' information center.

Cisco's IPSec is more difficult to manage and maintain, he says. A recent upgrade required users to download custom batch files and reboot their machines three times before it was installed. This leaves a lot of room for error and calls for help. "It's a support issue. It's a time issue for downloading, and it's an administrative issue to keep after people that haven't done it yet," Alexander says.

IPSec gear can cost less initially, but support for it can quickly eat up that savings, Coleman says. Cisco gear for his network cost about $6,000, and the Neoteris equipment was about $20,000, he says. ■

## SSL vs. IPSec

**Two popular Internet remote-access technologies, IPSec and SSL, offer increasingly similar features, but differences remain.**

| Pro | Con |
|---|---|
| **SSL** | **SSL** |
| • Offers finer control of access and more-detailed records of remote users' activity. | • For remote access only, not site-to-site. |
| • Requires no pre-distributed client software. | • Some gear lacks network-layer access. |
| • Can avoid firewall configuration and network address translation problems. | • Some gear lacks checks on the security of the remote machine. |
| **IPSec** | **IPSec** |
| • Supports site-to-site and remote-access connections. | • Requires distribution, configuration and maintenance of remote software. |
| • Products are more mature. | • Requires cooperation of business partners to set up extranets. |
| • Initial costs can be much lower. | • Access limits are not as tight as they can be with SSL. |

# Nortel debuts advanced net services wares

SSL VPNs and acceleration for Web services traffic are among features aimed at smaller firms.

■ BY PHIL HOCHMUTH

Nortel last week announced hardware and software for smaller companies interested in deploying advanced network services such as intelligent firewalls, Secure-Sockets-Layer-based VPNs and traffic acceleration.

Nortel's Alteon Switched Firewall 5114 could be deployed to provide packet inspection at the edge of a midsize business. Two new Alteon Application Switch products for midsize firms also are being released for adding services based on Layer 4 to Layer 7 packet inspection and switching.

In its software offering last week Nortel also focused on SSL VPNs and application switching.

Version 21.0 of the Alteon Operating System — which runs on the Application Switch products — includes hooks that let a switch identify XML and Simple Object Application Protocol (SOAP) in packets. This could be used to load balance servers running Web services applications, which use these protocols. The new Alteon Operating System also includes updated denial-of-service attack pattern-matching technology, which could be used to stop hackers from bringing down Web sites.

Also new is Nortel's SSL VPN 4.1 software, which runs on platforms such as Nortel's SSL 310 and 410 VPN boxes. The software adds Web-based management features and an auto-logoff feature for closing inactive SSL VPN sessions.

SSL VPNs are in use at Care New England, a healthcare management firm that operates three hospitals in Rhode Island. Nortel's SSL VPN gear eases the deploying of remote-access applications, says Howard Rubin, director of IS for Care New England.

"We were looking for a clientless [technology] for providing remote access," Rubin says. SSL lets hospitals and affiliated doctors in remote offices access e-mail and other Web-enabled applications securely with a standard SSL-capable Web browser.

"We're interested in SSL VPNs because there are thousands of PCs out there that we don't have control over," that are used by employees and affiliates to access Care New England's applications, Rubin says. "We like this solution because we don't have to do anything on the client side," in terms of VPN client configuration, he adds.

Nortel's Alteon Switched Firewall 5114 can be deployed to provide stateful firewall packet inspection for a midsize business. The box can apply different firewall polices to various segments of a business. The firewall costs $16,000.

The Alteon Application Switch 2208 and 2216 offer eight and 16 100M bit/sec Layer 4 to Layer 7 switch ports, respectively. Both boxes come with two Gigabit Ethernet uplink ports. The 2208 model costs $16,000 and the 2216 is priced at $20,500.

The Alteon firewall and application switch gear competes with products such as Cisco's CSS content switch and PIX firewall, firewalls by NetScreen Technologies and Nokia, and application switches from F5 Networks, Foundry Networks and Radware.

The Alteon Operating System 21.0 with XML and SOAP switching capabilities is a license-enabled software feature and costs about $8,000.

The SSL VPN software ranges from $10,000 for a 100-user system to $40,000 for a 1,000-user system. The SSL VPN 310 and 410 hardware ranges from $20,000 to $25,000, depending on configuration. ■