Small- and medium-sized businesses (SMBs), like their enterprise big siblings, have a growing number of reasons to want to support secure remote access to the company network. Employees want access, at minimum, to their e-mail and calendars when out of the office, working from home or traveling. Increasingly, remote/mobile employees also want access to files, databases and applications, perhaps even to their office computer, as well as the ability to use IM (instant messaging) and VoIP (Voice over Internet Protocol).

Broadband and Wi-Fi Internet access provide paths for employees to connect to the company. But until recently, the Virtual Private Network (VPN) tunnels needed to establish secure connections from individual computers to the company network required enterprise-grade budgets and IT expertise. But that’s changing rapidly and dramatically with the availability of affordable and easy-to-use SSL (Secure Sockets Layer) VPN appliances from network vendors such as Linksys, NETGEAR, SonicWALL and WatchGuard.

History Lesson

Historically, VPNs used IPsec (Internet Protocol Security) to provide an encrypted “tunnel” between points.

An IPsec VPN is a full network-level connection, extending the headquarter’s LAN (local area network) to a branch office. While this gives the remote users access to all central resources, it also means that any spyware, viruses or other security breaches on remote systems can access the main LAN and vice versa.

Also, IPsec requires a preconfigured software client, or VPN appliance, at the user’s end. Providing these clients adds to IT’s budget and task list and means that employees, contractors, customers or others using noncompany computers can’t access the network via VPN.

The SSL protocol was developed by Netscape in the mid-1990s to transmit credit card numbers and other private information and documents to and from a Web browser securely across the Internet. Today, SSL is also being used to provide secure VPN connections — and unlike IPsec — basic SSL VPNs can be set up from nearly every modern Web browser from almost any desktop, notebook, handheld, kiosk or smartphone.

“The general trend for supporting remote access is SSL-based VPNs,” says Jeff Wilson, principal analyst, VPNs and Security at Infonetics Research. “Any company that is doing remote business has to have an SSL solution.”

Companies such as Cisco Systems and Juniper Networks have offered enterprise-oriented SSL VPN products for several years. However, they may be considered pricey and support many more concurrent users than any SMB is likely to need to support.
Recently, however, “These prices have come down, thanks to changes in technology and the availability of specialized silicon allowing smaller devices to be made,” says Brad Sakai, product marketing manager at Linksys, a division of Cisco Systems.

“For a small business, SSL VPNs are easier to use and support than IPsec,” says Infonetics’ Wilson. “Typically, a small business is looking to provide remote access to e-mail and calendars, maybe also secure file sharing, a Web portal and user desktops. This probably represents the remote access needs of 90 percent of SMBs. SSL VPNs are perfect for this; they’re not running complex business applications like SAP, PeopleSoft or CRM (Customer Relationship Management), which are harder to integrate into SSL VPNs.”

Some companies using IPsec VPNs want the benefits of SSL VPNs, says Brad Sakai of Linksys. “They decide they need to support remote access, and that SSL is easier. SSL isn’t a new paradigm of working; it’s making VPNs easier to deploy and more accessible to companies.”

Best Practices

For example, many hospitals only allow browser- or Web-based outside network access, notes Jan Sijp, product line manager for SonicWALL.

“Here an IPsec VPN won’t work, but an SSL VPN will,” says Sijp. Likewise, he notes, lawyers are often onsite with one client for weeks or months, and then they go to another client. “SSL VPNs avoid the need to go to IT to get a new IPsec VPN set up.”

SSL VPNs are best for providing access to contractors who need access to your company network, adds Linksys’s Sakai. “Also, they’re perfect for employees”
who didn’t bring their notebook computer home; they can use a home PC and access the company network securely.”

A growing number of network vendors, including D-Link, NETGEAR, SonicWALL and WatchGuard, now offer SSL VPN appliances at prices that fit the needs of small- to medium-sized businesses and for remote/branch offices. “SSL VPN products, like ones from Linksys and NETGEAR, are a good match for 10- to 20-person companies and offices,” comments Infonetics’ Wilson. “Products like ones from SonicWALL and WatchGuard are a good match for companies with 20 to 500 employees needing remote access.”

The RVL200 SSL/IPsec VPN router from Linksys, for example, “costs less than $200 and is a complete router/VPN, supporting five SSL VPN tunnels,” according to Sakai. “The RVL200 includes a four-port, full-duplex 10/100 Ethernet switch, so you can connect four PCs directly or connect additional switches. Since we also support IPsec, you can make a full LAN connection from a remote site to your main office, as well as support SSL VPN connections to the remote site.”

The RVL200 also includes an SPI (Stateful Packet Inspection) firewall and QoS (Quality of Service) features for VoIP and video traffic. “We can support IP VLANs (Virtual LANs) for customers who want separate VLANs for voice and data,” says Linksys’s Sakai.

NETGEAR’s ProSafe SSL VPN Concentrator 25 SSL312, in the sub-$400 range, supports 25 concurrent SSL VPN tunnels. Other features include support for automatic cache cleaning after sessions terminate to ensure privacy of users and their data. NETGEAR’s ProSafe SSL312 also integrates with popular user authentication directory systems for granular policy control, including Microsoft Active Directory, RADIUS (Remote Authentication Dial-In User Service), NTDomains and LDAP (Lightweight Directory Access Protocol).

SonicWALL’s products include SSL-VPN 200, for up to 10 concurrent users, in the sub-$600 range; the SSL-VPN 2000, for mid-sized organizations up to 500 employees, and a recommended maximum of 50 concurrent users, in the sub-$2,000 range; and the SSL-VPN 4000, for up to 200 concurrent tunnels, priced around $6,000.

Although SonicWALL specifies a recommended maximum of concurrent users for performance considerations, “We don’t restrict user numbers or don’t charge per tunnel,” says SonicWALL’s Sijp.

WatchGuard’s Firebox SSL VPN gateway appliance, starting in the sub-$2,000 range with licenses for five tunnels, supports up to 205 concurrent sessions. “We typically see companies buying licenses for five to 50 tunnels,” according to Mike Leo, senior product manager at WatchGuard, whose Firebox includes enterprise-class features including endpoint security. When allowing network access, Firebox continuously verifies endpoint security status, firewall settings, operating system and patch level, and the status of antivirus software, to make sure the user’s system hasn’t been compromised.

Different Approaches
For browser-based activities, employees using remote computers don’t need any additional software or configuration, which helps to make SSL VPNs very appealing to IT departments.

SSL capabilities are now included in just about every modern Web browser — not just Microsoft’s Internet Explorer, Mozilla Firefox, Apple Safari and Opera, but also the Web browsers used on handheld computers, PDAs, smartphones and other mobile devices.

In addition to the pure clientless SSL VPNs using a browser, there are also two other approaches to SSL VPNs, notes Infonetics’ Wilson. “There’s the on-demand ‘light’ client, usually ActiveX or Java, pushed through the browser. There’s also the ‘full-install’ client, which might be delivered via the Internet, but not automatically installed. These usually have to be installed and configured by IT.”

These SSL adapters, also known as “network shims” or “encapsulators,” establish a network connection, similar to IPsec, between the user’s computer and the company network. This may be necessary, notes Wilson, for companies that save business applications that aren’t Web-enabled.

Common Applications
“E-mail is by far the main application that remote users want access to,” observes SonicWALL’s Sijp. “Microsoft’s Outlook Web Access (OWA) lets users access Exchange Server folders. Alternatively, users can start up our NetExtender thin client and start up an e-mail client like Outlook or Lotus Notes.”

“Most of our customers have been small- and mid-sized businesses like real-estate...
professionals, doctors, lawyers and branch offices of larger companies,” reports Vivek Chugh, product line manager, NETGEAR. Many are using their SSL VPNS for simple tasks like checking e-mail and looking at spreadsheets, says Chugh. More advanced users are employing their SSL VPNS to access client-server applications such as Oracle and workflow applications.

When away from their offices, many employees like to access their main computer and the programs and data on it. Popular remote-desktop solutions, which can be used to connect over the network, include Microsoft’s Remote Desktop feature (included in Windows XP Professional), Symantec’s pcAnywhere and Citrix’s GoToMyPC service.

“IT doesn’t like having to open ports on the firewall,” notes SonicWALL’s Sijp. “Our SSL VPN appliance can work with these remote-desktop solutions.”

Another popular use of SSL VPNS, Sijp says, is accessing applications which have been published to a server, such as Microsoft Office or a CRM app, using Microsoft Terminal Server, which avoids the need to install these applications on each PC.

SSL Advantages
SSL VPNS have a much lower TCO (total cost of ownership) compared with IPsec VPNS, according to WatchGuard’s Leo, since additional software adapters, application connectors or network reconfiguring are not needed.

“SSL means you no longer need to pay for a client license, and have less training and fewer support calls, since almost everybody already knows how to use a browser.”

SSL also has security benefits compared to using IPsec VPNS, points out Infonetics’ Wilson. “If you let someone in via IPsec, you need an access or network control scheme in place, for example, segmenting your network or Network Access Control (NAC). With SSL VPNS, you can just decide what applications to grant them access to at a much higher level.”

For greater login security, SonicWALL offers tokenless one-time passwords, in addition to the regular username and password, according to SonicWALL’s Sijp.

“When you log in, the appliance generates a password and sends it to you some other way than the browser, like as an e-mail or a text message to your cell phone. This prevents any keylogger spyware on the computer the user is working on from capturing the second authorization without the need for a token-based two-factor system like RSA SecurID, which an SMB’s IT department may not want to implement, especially for a small number of users.”

If you’re expecting to use thin-client SSL VPNS, make sure the SSL VPN appliance you’re looking at supports the browser(s) your employees use. For example, ActiveX-based clients are limited to Windows machines. All SSL VPNS support Internet Explorer, and a growing number support Firefox, and have — or are working on — clients for MacOS and Linux.

CDW offers technology service support from top manufacturers and service providers across all product categories.