Simplifying Secure Remote Access: SSL VPNs

David M. Piscitello and Lisa Phifer

IPSec has come on strong, but for securing VPN communications to remote locations, SSL is gaining ground. There's still no panacea, but things are getting better.

The development of virtual private networks (VPNs) was motivated by the need to reduce the cost of secure communications by leveraging ubiquitous Internet access. While many organizations have used IPSec VPNs to meet these objectives for site-to-site networking, they have not achieved the same degree of success when deploying remote access VPNs. Simply put, IPSec remote access often proves harder to manage and costlier to implement than the investment appears to return.

The requirements for secure access can't be set aside; enterprises must provide connectivity to a growing mobile workforce more cost-effectively, and this mandate is now complemented by additional requirements to comply with existing and pending financial and healthcare privacy legislation. But the drivers that necessitate rapid adoption of secure access have led organizations to consider alternatives based on the Secure Sockets Layer (SSL).

SSL is a component of every major Web browser, and the combination of ubiquity, user familiarity with the Web interface and simplicity of deployment gives SSL quite an advantage in many deployment scenarios. Couple this with the fact that most organizations already have accumulated years of experience running SSL on their ecommerce and extranet sites, and it's not hard to understand why SSL has re-emerged as a contender for secure remote access.

At least a dozen vendors, including Array Networks, Aspelle, Aventail, Check Point, Neoteris, Netilla, NetSilica, Nortel, Rainbow Technologies, SaveWeb, URoam and Whale Communications, hope to triumph in the high-stakes market for secure remote access. Many of these companies are new, but even traditional IPSec VPN vendors are getting into the SSL game. The message they send is clear and uniform: SSL VPNs are simpler to deploy and demonstrably less expensive to implement and operate. The trump card that SSL VPN vendors hope to play is perceived return on investment (see "Boosting ROI," p. 48).

According to Michael Suby, author of Stratecast Partners' report, *"SSL VPN Sector Assessment*," 2003 will be the year that SSL VPNs become a true contender and achieve mass-market awareness. "This is a crowded space, with many vendors and plenty of noise," said Suby. "If you're a small company, survivability becomes a big challenge. I predict that this competitive market is going to become more intense—demand will grow, but can each of these companies grow with that demand?"

Why All The Fuss?

IPSec has proven successful for site-to-site VPNs, but remote access deployments have run headlong into severe limitations. The first is IP addressing. IPSec VPN administrators, and sometimes users, must worry about the details of addressing IPSec-encapsulated packets; for example, whether the addresses are dynamically assigned and from what pool, and how routing and security policies are affected by such assignment.

Addressing in IPSec VPNs also is seriously encumbered by the commonplace use of network address translation (NAT). Standard IPSec often won't work in environments where NAT address sharing is beyond the administrator's control, such as public Internet access kiosks, home networks and customer or business partner sites. Vendors have tried to solve this problem, but without one broadly implemented standard, interoperability is not assured.

The second problem many companies face is how to support an installed authentication infrastructure. IPSec was designed to provide mutual authentication of client and server using digital certificates or shared secret passwords. Administration of shared secrets doesn't scale well, and it's a weak form of authentication. But the

David Piscitello (dave@corecom.com) and Lisa Phifer (lisa@corecom.com) are, respectively, president and vice president of Core Competence, Inc., an internationally recognized consulting firm specializing in network security. David also is the founder of the Internet Security Conference, and has chaired the N+I Conference Program since 1996.

You can control IPSec client deployments within your organization, but not to external partners and customers

Boosting ROI

Return on investment is the difference between the total cost of VPN ownership and savings resulting from VPN adoption. In other words, if the VPN costs too much to provision and maintain, positive ROI may never be realized.

Remote access costs are influenced by a wide variety of factors, including the number of users, average connect time per user, location, carrier toll rates, Internet access rates, investment in capital equipment and training and the staff required to support user activation, software installation and update, trouble administration and policy enforcement.

A Rainbow Technologies analysis compared the cost of direct dial IPSec-style hardware VPN vs. an SSL VPN using Rainbow's NetSwift iGate appliance. For 1,000 remote users, implementing a hardware VPN ($442/user) is actually *more expensive* than dial ($195/user) due to investment in VPN client hardware.

However, few companies spend $398/user supplying IPSec client hardware to their entire workforce. Substituting $40-per-seat client software drops IPSec VPN implementation to $84/user. Because an SSL VPN requires no added client hardware or software, an iGate implementation runs just $72/user.

These figures cover initial implementation, but not the recurring cost of new user provisioning, policy and software updates and user support. But SSL VPNs can also be considerably less expensive to operate than IPSec VPNs. For example, Whale Communications estimates that managing an IPSec VPN runs between $5 and $30 per user per month. On the other hand, managing a Whale e-Gap SSL VPN runs a flat $1,000/month. Clearly, a remote access VPN does not need to be very large before SSL becomes more cost-effective.

Clearly, these numbers are just examples; every organization must calculate its own potential ROI, and results will vary widely. Rainbow made certain assumptions regarding the cost of dial-up and on-line time—assumptions that any company must adjust up or down when performing an ROI calculation for their own workforce. Whale used Cisco's IPSec VPN ROI calculator to estimate the ongoing cost of IPSec VPN operation, supplying parameters that should be customized on a case-by-case basis.

When it comes to ROI, there is simply no substitute for doing your own homework. Vendor-supplied calculations like these, however, can help you identify the factors that must be considered when preparing estimates of the impact on your bottom line□

alternative, digital certificates, and the need for some public key infrastructure (PKI) to manage them, is taxing and expensive.

The broader problem, however, is that the IPSec standards don't support asymmetric client authentication based on tokens or any of the challenge-response methods that many companies, after considerable investment, have implemented. Numerous proprietary and interim solutions exist, but none are broadly supported across IPSec vendors. Authentication and "NAT pass-through" extensions often require VPN gateway and client pairing, which in turn limits deployment options.

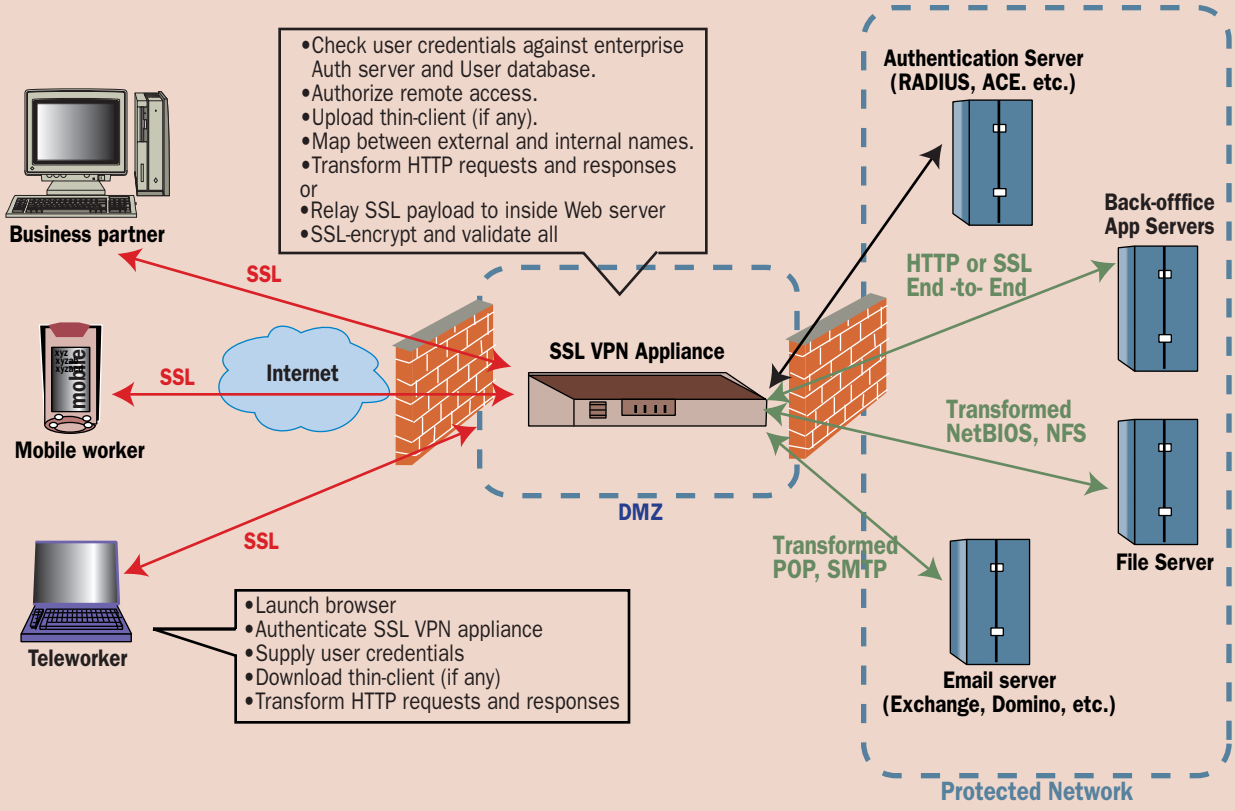
As the name suggests, IPSec creates an IP- or network-level tunnel (connection) between a client computer and VPN security gateway. This means that every remotely-connected user is directly connected to an organization's trusted network. When a client computer connects remotely using IPSec, every resource on this protected network is potentially available to the user, and therefore vulnerable to misuse and attack from that computer.

To counter this, organizations need to create security policies to limit user access. In large deployments, administrators can become overwhelmed by complicated, user-, group- or constituency-specific policies. Moreover, IPSec remote access may require policy coordination across many security systems, including Internet firewalls. Changes may be required to permit IPSec and its management protocol to move through the firewall, to reach IPSec VPN gateways and servers behind the firewalls.

Tethering remote workers to the protected network also increases the number of trusted systems that the IT staff must administer. This task is exacerbated when software and configurations must be administered on distant and intermittently connected computers owned by employees and business partners.

IPSec remote access requires VPN client software, requiring either purchase of third-party software or use of client software embedded in certain operating systems. In both cases, organizations are introducing unfamiliar software that must be installed/configured by the administrator or through a simplified processes whereby unsophisticated users download both software and policy from a trusted server. Some IPSec products include central policy configuration so that settings get packaged into the installer or pushed

FIGURE 1 Example of SSL VPN Application



over a bootstrap tunnel to the client. These methods work well in VPN deployments where companies have control over all systems requiring secure access. However, they become impractical when organizations try to extend secure remote access to business partner, supply-chain and customer computers.

These limitations are being addressed, albeit slowly, by IPSec VPN standards and product upgrades. Meantime, other vendors have capitalized on these problems to create a new market for SSL VPNs. After years of struggling with these limitations, many organizations are reconsidering whether their requirements for remote and extranet access are really best served by IPSec VPNs.

Many organizations just want to provide users with easy, intuitive access to specific applications. To accomplish this objective, they do not need the full network connection exposure that IPSec VPNs create. They don't want to be bothered with addressing and routing issues that result from network-layer tunneling. They would rather avoid additional or unfamiliar client software to manage and configure. They want a solution that meets their security needs, including flexible selection of authentication methods and integration with existing databases. By using SSL, organizations hope to combine these attributes—client software ubiquity, ease of administration and use and network transparency—with economic benefits that result from leveraging the familiar.

According to Stratecast's Michael Suby, SSL VPNs address the average worker's needs in a simple manner, reusing software that already resides on nearly every remote system. "SSL vendors are aware that to become successful, you do not want to remake the desktop—just make [VPN] a transparent extension to what workers already use," he said. [Browsers] have become a *de facto* standard to how users interact, and if you can play in that standard, then you've solved one of the hurdles."

How SSL VPNs Work

Nearly everyone has used SSL at one time or another. Browsers shipped with virtually every networked device support SSL. Merchant websites use SSL to secure ecommerce transactions. Enterprises use SSL to prevent unauthorized employees from accessing intranet services and data. But most of us assume SSL is "safe" without really understanding what it does.

Netscape defined SSL to enable ecommerce by letting the buyer (browser) verify that the seller (Web server) is legitimate, preventing disclosure of credit card numbers and giving both parties confidence that messages are not replayed or altered. These objectives are accomplished by establishing a TCP session, and then authenticat-

ing the server's certificate, encrypting encapsulated HTTP with a cipher like RC4 and applying a hashed message authentication code like MD5 to each packet.

In practice, users pay little attention to server certificates—browsers often automatically accept certificates issued by trusted authorities. Many applications add client *subauthentication*—for example, by presenting a login page, where cleartext username and password are protected by the SSL connection. Some applications use SSL to protect subauthentication, reverting to unprotected HTTP thereafter. Other applications protect the entire client/server dialog with SSL.

SSL VPNs usually do the latter. They use SSLv3 or TLSv1 (Transport Layer Security, the Internet standard version of SSL) to create a secure tunnel from the remote user to a Web server located near the edge of the protected network. To permit access only by authorized users, SSL VPNs always apply subauthentication. Supported methods vary by product, ranging from HTTP Basic Authentication to SecurID (two-factor) authentication to client-side certificates.

SSL VPN appliances relay requests between end users and applications inside the protected network

What happens next is what really differentiates an SSL VPN appliance from an ordinary Web server. Instead of processing data from the client, a VPN appliance relays requests between the user and a destination application inside the protected network. Precisely how this relay occurs depends upon the product (see Figure 1).

- The appliance may operate as a transparent relay, forwarding SSL payload directly to the destination server without interpretation. This lets the appliance focus on security—enforcing access controls, accelerating encryption—without becoming application-dependent. But each destination server and application must then provide a Web interface.
- The appliance may transform HTTP requests into another protocol. For example, the appliance may generate NetBIOS messages to browse a Windows fileshare on behalf of the remote user, in response to a user's Web request. In this case, content transformers are needed to "webify" each application. Appliances ship with transformers for common applications like email, contacts and file sharing, but custom development is required to webify other applications.
- The appliance may dynamically upload helper software—for example, a Java applet or ActiveX control—to extend the target application's native interface to the client. These thin-client GUIs can be more user-friendly, but also require more from the client system—for example, permission to run Java or download executables otherwise denied for security reasons. The appliance may ship with a GUI that supports common applications, extensible by custom webifier plug-ins.

Although SSL VPNs are based on *de facto* and IETF standards for secure tunneling, standards do not dictate proxy architecture, content transformation or the protocol to be carried inside the SSL tunnel. To illustrate product diversity, one need only consider three of the many SSL VPN appliance vendors.

- **Neoteris:** The Neoteris Instant Virtual Extranet (IVE) appliance serves as an application-layer gateway between the Internet and an organization's trusted networks. It processes client-authenticated and SSL-encrypted requests according to customer defined access control and authorization policies. Request handlers accommodate native Web (Java applets, Javascript), webified file shares, telnet/SSH, client/server and messaging applications. Content from incoming requests is parsed and transformed into the native resource protocol and forwarded onto the internal server that supports that protocol (e.g., Microsoft Terminal and Exchange Server, Lotus Notes, Internet email and IBM "green screen" applications). Responses pass through the same handlers, transforming the native protocol into a webified response to the user.

"The IVE is designed to make many applications look as similar to Web and as familiar as possible," comments Neoteris CTO Andrew Harding. "Since IVE's content transformation supports the widely used native protocols, organizations don't have to webify every application, which eliminates considerable duplication on their part."

- **Whale Communications:** Whale Communications' e-Gap Remote Access appliance handles Lotus Suite, Microsoft Outlook and network file-sharing applications. Special, optimized subsystems are available for Exchange and Domino, and "customizers" are provided to assist in webifying additional applications.

Whale appliances are based on an "air gap" technology. The appliance processes requests between authenticated users and back-office servers using a split reverse proxy technique that ensures that untrusted users never have direct access to the protected network. A switched, non-programmable memory bank is interposed between two single-board computers: a public-facing "virtual Web" server and a protected internal server. To protect back office servers from network-level attacks, the public server strips arriving message TCP/IP headers. Only the SSL-encrypted payload is forwarded across the air gap, so attackers have no exploitable network path to the

internal server or back office systems. The internal server hosts intelligent proxy and application inspection software, an SSL server, and optional SSL accelerator. Application request filtering protects resources on the internal network from malicious data injection.

According to Joseph Steinberg, Whale's director of technical services, SSL appliance deployment solves only part of the secure access problem. "SSL allows user access from any computer, including those at public kiosks, where user account and pasword information might be inadvertently left on browser and misused by a subsequent, unauthorized user," he said.

Whale mitigates this inherent HTTP vulnerability by using a secure logoff mechanism that prevents credential caching at browsers. To avoid leaving other sensitive data in the browser cache, Whale provides methods to prevent temporary file creation and clear downloaded files before logoff.

■ **Aventail Corporation:** Aventail's ASAP (Anywhere Secure Access Policy) Platform evolved from Aventail's Extranet Center, one of the first software-based SSL VPN solutions on the market. ASAP is sold in a stand-alone appliance (EX-1500), a managed appliance (SA-1000) and a managed system (SA-9000). It supports three proxied secure access methods: browser-based access for Web applications and file shares, a Java agent for thin client/server applications (e.g., Citrix) and a Win32 SSL/SOCKS client for secure access to any application.

Aventail's CTO Chris Hopen describes the re-emergence of SSL as "a solution we've known—and proven—addresses both secure remote and extranet access in a highly scalable and non-disruptive manner, whether deployed by an organization or outsourced to a competent service provider." Having competed for years with secure proxy vendors, Aventail has developed an extensive set of authentication methods, including client certificates, tokens and single sign-on adapters like Citrix ICA, Netegrity SiteMinder and Trusted User Identity Forwarding.

The experience Aventail accumulated while offering managed extranet, user and directory services is reflected in its scalable, central policy-management interfaces and granular authorization policies. Like Whale, Aventail includes secure logoff, cache content blocking and blocking of "auto completion" in sensitive forms to offset "kiosk" vulnerabilities.

What's The Catch?

Stratecast's Suby believes that IPSec and SSL will both succeed. "What we're hearing from AT&T, Sprint, Nortel, NetScreen, etc., is that a lot of customers look at SSL as complementary to IPSec," he said.

Why? Because, like every solution, SSL VPNs have certain limitations.

For starters, a network-layer protocol like IPSec is better suited for site-to-site VPNs. IP-level gateways can easily enforce policy at a single point for an entire network of users, multiplexing traffic onto a single site-to-site tunnel. A transport-layer proxy can be made to do this (e.g., using SOCKS), but that architecture does not exploit the browser-as-client benefits that are driving SSL VPN adoption.

Network gateways also are better positioned to support bandwidth-intensive, low-latency applications. IPSec appliances often use hardware acceleration to minimize latency. SSL appliances may follow suit, but proxies still incur content transformation overhead. "When dealing with voice or video, you need to ensure those applications have priority over everything else," noted Suby. "This is not so much an issue of differentiating traffic as it is the processing tax of a proxy environment." One possible deployment: SSL remote access for transactional applications, plus IPSec for teleworkers who re-quire streaming applications.

SSL VPNs are more vulnerable to denial-of-service attacks than IPSec

VPNs that rely upon content transformation or thin-client GUIs will forever play catch-up to support new applications. SSL VPNs may satisfy the majority who need only selective access to common business applications, but IPSec can fill in the gaps to reach unusual applications where custom development is not justified. Administrators and others who really do require broad network access can also use IPSec clients. True, this means two VPN implementations. But companies can leverage IPSec gateways deployed for site-to-site traffic to offer IPSec remote access as-needed to these smaller expert and power-user populations.

IPSec and SSL both use cryptography and authentication, but one must compare products, not protocols, to evaluate strength and ability to support your company's security policy. Most IPSec clients default to 3DES block encryption, but also support weaker alternatives like 56-bit DES. Browsers often default to 40- or 128-bit RC4 stream encryption, but SSL is perfectly capable of supporting 3DES CBC. The Advanced Encryption Standard (AES) is now being implemented for both protocols. Given comparable key lengths, block encryption is less vulnerable than stream encryption. Otherwise, both IPSec and SSL negotiate per-session keys, and both use cryptography to prevent eavesdropping and

For many companies, the question isn't whether to add SSL VPNs, but when

forgery. IPSec with mutual certificate authentication is more secure than SSL with one-way server certificate authentication, but this is a red herring. Remote access VPNs of both flavors commonly use authentication methods that are more or less secure than these two extremes.

A more significant security difference is the degree to which each solution is vulnerable to denial-of-service attacks. Network-layer VPNs deflect data forgery or packet-drop attacks more efficiently than higher-layer VPNs. SSL VPNs have more trouble deflecting these attacks because the TCP layer will discard corrupted packets before they can be delivered to the SSL process. The TCP layer will wait for valid packets to arrive, so sustained corruption or loss will eventually break the SSL tunnel.

SSL servers also are more vulnerable to TCP-based denial of service attacks like SYN floods. IPSec operation is based on IP and UDP datagrams, and flood attacks at these layers tend to be less disruptive because datagram protocols are stateless and designed to withstand loss.

Another near-term consideration is maturity. Most (but not all) IPSec VPN products have been field-tested for at least five years, while most (but not all) SSL VPN products are comparatively new and lack big-company backing for support and longevity. Enterprises may trial SSL VPNs for user communities experiencing the biggest IT pain, but very large company-wide rollouts may wait for the market to shake out.

More than a dozen vendors offer SSL VPN appliances or firewall extensions, and we've yet to hear announcements from the largest equipment vendors who shape the network and security markets. All of these players cannot survive, even in the healthiest times of venture capital investment. We expect to see some market attrition and consolidation as large players acquire smaller ones. Just as IPSec evolved from a standalone appliance to a firewall bolt-on, SSL VPNs may undergo similar integration over time.

Looking To The Future

For many companies, the question is not *whether* to add SSL remote access, but *when*. Is now a good time to get into SSL VPN? As always, the answer depends upon each company's circumstances and remote access requirements.

Because SSL VPNs leverage already-deployed browsers, experimenting with them requires modest investment in IT resources and trial hardware. Custom development can be deferred until built-in applications have been proven to meet expectations. Even if a first trial does not meet management, application, scalability or performance requirements, the experience can be used to select another product that does. Although not completely painless, migrating from one SSL VPN product to another is arguably much easier than migrating from one IPSec VPN product to another.

When considering any hardware investment, one must look beyond technical requirements and costs. With any new technology, the more research performed up front, the better the match. Because SSL VPN products are so diverse, it can be difficult to compare apples to apples. RFPs should clearly specify your organization's security policy, access control granularity, user management, authentication and application support requirements. Evaluate the feasibility and cost of webifying unsupported applications. Weigh vendor responses carefully, considering the extent to which each proposed solution can achieve ubiquity, transparency, ease of use and low-overhead objectives. Before making long-term commitments, check customer references, investigate the vendor's financial health and maturity and consider partnerships that may lead to acquisition. Such steps are particularly prudent in a dynamic market like this one.

Finally, while SSL VPNs are very promising, don't expect a silver bullet. When organizations become frustrated with one technology, it is natural to look at new technology as a panacea. No technology solves every problem, and no deployment comes without cost or growing pain. Any company that needs secure remote access for travelers, teleworkers and business partners should evaluate all available alternatives—including SSL VPNs. To that end, we hope this article has provided a foundation for understanding what SSL VPNs are, their benefits and their limitations□

Companies Mentioned In This Article

- Array Networks (www.arraynetworks.net)
- Aspelle (www.aspelle.com)
- AT&T (www.att.com)
- Aventail (www.aventail.com)
- Citrix (www.citrix.com)
- CheckPoint (www.checkpoint.com)
- IBM (www.ibm.com)
- Microsoft (www.microsoft.com)
- Neoteris (www.neoteris.com)
- Netegrity (www.netegrity.com)
- Netilla (www.netilla.com)
- NetScreen (www.netscreen.com)
- NetSilica (www.netsilica.com)
- Nortel (www.nortelnetworks.com)
- Rainbow Technologies (www.rainbow.com)
- SafeWeb (www.safewebinc.com)
- Sprint (www.sprint.com)
- URoam (www.uroam.com)
- Whale Communications (www.whalecommunications.com)