Web-Based Remote Access: Part 1
Global Networking Strategies
David Thompson

Secure Sockets Layer-based alternatives are quickly emerging in response to the manageability problems of IP Security virtual private network (VPN) clients. SSL VPNs have a place in the remote access portfolio, but they will require a user-profiling exercise to accurately determine for whom such solutions are suited.

Traditional IPSec remote access — using the IP Security protocol to connect via an authenticated and encrypted tunnel, termed a virtual private network — is suffering from its own success. The cost savings associated with Internet access as well as the efficiencies gained from enabling work at home and flexible access encourage organizations to broaden the user base for remote access. Unfortunately, IPSec-based remote access requires installation and management of complicated client software, which is frequently difficult and expensive to manage if machines are not under the IT organization’s control. In response to these challenges, remote access VPN products based on Secure Sockets Layer are emerging. Most solutions are based on an application proxy model, where at a single point (most often an appliance) SSL traffic is terminated and user sessions are proxied to various internal resources. An initial benefit of SSL VPN products is reduction of the complexity of the VPN client, but the proxy technology is also an important strategic development in the nature of security technology at the network perimeter, and part of the trend toward application-level security (see GNS Delta 1027).

During the next two years, SSL-based remote access will grow significantly, used in conjunction with IPSec VPNs, with 33% of organizations supporting SSL as the only access mechanism for a portion of the workforce. By 2005/06, SSL-based solutions will be the dominant remote access method, with 80% of users using SSL, though IPSec will still be used for specialized applications and user requirements. By 2006/07, the value proposition of SSL VPN appliance-only vendors will diminish, due to the more pervasive use of such proxying technology in other infrastructural components, primarily in the emerging application security gateway, rather than traditional network firewalls.

Various different technologies are grouped under the label of SSL VPN. Although almost all of these technologies include use of some sort of proxy technology, there are significant variations in the requirements for client code as well as in the nature of the server technology, and therefore in the applications supported. Solutions include numerous different configurations of client and server, as noted below, and many vendors support more than one of the listed modes — often with enhanced functionality enabled with the addition of client-side code such as applets.

The SSL Virtual Private Network Taxonomy

Client Side

- **Browser-only client:** Most solutions support basic functionality without requiring any client software installs or applet downloads. This client limitation typically is associated with Web proxy-only technology (see below), and some translational proxies.
- **Applet client:** Many vendors support downloadable Java applets and similar mobile code technology. For some, this code enables limited client/server application support through the SSL session, thereby allowing, for example, replication of Outlook or Notes

**META Trend:** Through 2002/03, investments in perimeter security will focus on implementing intrusion detection systems and improving robustness (high availability, performance, and capacity) of the demilitarized zone. By 2003, as threats proceed up the computing stack and encryption increasingly blinds network-based components, attention will shift to special-purpose firewalls/proxies and multifunction, node-centric solutions. Maturing by 2005/06, such solutions will lead to the dissolution of traditional perimeters.
e-mail clients with the mail server to be performed via SSL. Representative vendors include Aventail and Neoteris. For others, the code enhances the user experience or is required for translational proxies to work (e.g., connections to screen-scraping technology).

- **Full Windows client**: Some vendors support full client technology. Still using SSL, and often not suffering from the compatibility problems associated with IPSec clients, these full clients allow complete client/server application communication, often using SOCKS or other protocols (within SSL sessions). Aventail is the primary provider of this type of solution.

**Server Side**

- **Web proxies**: Similar to reverse proxies, Web proxy systems grant access to Web-only content, often including dynamic re-writing of URLs to safely externalize internal Web applications. Vendors should address the support for not only static Web pages but also dynamically assembled content and links, including scripted applications. Current solutions from Check Point and Nortel fit into this category, requiring only Web browsers but supporting the fewest applications (Web-enabled applications only). For most other vendors, this is just an aspect of their capabilities.

- **Translational proxies**: These proxies function similarly to Web proxies described above, but they also include the capability to represent and translate protocols into HTTP, making it possible to expose file-sharing servers, FTP, SMTP, and other applications. Some versions require no client software other than a browser (if the application is presented fully via the browser), while others require a Java applet or similar to connect any client software (such as Outlook or Notes e-mail clients) to the SSL tunnel at the remote node. Aventail, Neoteris, SafeWeb, and uRoam support this model.

- **Proxy-based VPN**: Much closer to a traditional IPSec virtual private network, proxy-based VPNs require client software and use a protocol such as SOCKS (within an SSL session) to provide access. Application support is usually quite good, more complete than any of the other SSL options, but the tradeoff is a full client install.

- **Screen scraper/terminal server**: Citrix and windows terminal server can also be used to present either the non-IPSec client (via the Citrix ICA client) or the Web-only client (via the Citrix NFuse technology) with application interfaces. These technologies do not rely on strict proxying, but instead push the presentation layer out to the client, while the execution remains on the server. In some cases, the terminal service is presented via a translational proxy (as noted above); the primary example is from Netilla.

The main goal of this analysis, aside from determining client software requirements (and thus endpoint flexibility), is to identify the remote applications that can be supported. SSL VPN application support is limited, often allowing access only to Web applications, e-mail, file sharing, and a few other miscellaneous applications. Because these are the applications required by most users, SSL access will be sufficient for much, if not all, of the user population. We recommend that a user profiling exercise be performed to match user types to remote access technology (see GNS Delta 1009), because SSL access can be supported at some level from any computer with an Internet connection and a Web browser. This access potentially extends to any device with a browser, and we expect vendors to support connections to personal digital assistants (PDAs) and other devices during the next three years. Even if client software is used, there is still benefit gained from eliminating the IPSec client from the mix, especially for any computer images over which the IT department does not have complete control. META Group research has uncovered significant deployment and support complexity and expense associated with supporting IPSec VPN clients, and we have a long history of recommending against doing so with non-corporate machines (see GNS Deltas 944 and 952).

Use of a proxy introduces numerous additional benefits — and some associated drawbacks — to the remote access environment, and these will be explored in future research Deltas on this topic. Factors to be discussed include enhanced security features and the possibilities of full integration with external portals, as well as a more complete examination of the security implications of SSL access.

**Bottom Line**

Organizations should examine the tactical benefits to be derived from Secure Sockets Layer VPN products, as well as the strategic benefits of SSL application proxy technology.

**Business Impact**: Safely granting remote access to critical applications without requiring complex client software installations can both reduce remote access support costs and enable extension of remote access to a wider population, including partners and customers as well as employees.