Web-Based Remote Access: Part 2
Global Networking Strategies
David Thompson

Although Secure Sockets Layer virtual private networks (SSL VPNs) can alleviate the client software and support problems of traditional IP Security-based VPN technology, customers should also examine the enhanced security features made possible through SSL VPNs. For the long term, it will be critical to examine the path of maturation that such products will follow — including integration with traditional portal and user life-cycle management tools.

Organizations must now explore the new security features possible with an SSL VPN, as well as the lingering unknowns associated with this emerging technology. It is not sufficient to evaluate only the characteristics of SSL VPN that reduce remote access complexity (i.e., reduced client complexity, support for larger and more flexible user populations, etc.). Of critical importance for the long term are the issues of integration with portal and user life-cycle management tools (see GNS Delta 1037).

During 2003/04, SSL-based remote access will grow significantly and be 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 method for remote access, with 80% of users using SSL, though IPSec will still be used for specialized applications and user requirements. To be successful, SSL VPN products must integrate not only with external user stores (directories), but also with tools for managing user privileges (i.e., user life-cycle management products). Such integration, along with the enhanced security provided, will make the SSL proxy technology an appealing addition to externalized portals. As a result, by 2006/07, the value proposition of SSL VPN appliance-only vendors will diminish, due to more pervasive use of this type of proxying technology in other infrastructural components (especially firewalls and portal security tools).

Our focus in previous research was on the increased simplicity and efficiency of, as well as a taxonomy for, Web-based remote access products (see GNS Delta 1087), and we will now focus on the possible enhanced security features associated with the SSL VPN. Because most of these solutions operate as a proxy at the application layer, the opportunity exists to implement more granular security services. Possible functions include:

- **Filtering:** At the application layer, the proxy can drop the HTTP or related commands that it deems unacceptable, and then scan for application/HTTP-based attacks on Web servers (i.e., buffer overflows, CGI attacks, malicious executables, etc.). This potentially includes offloading or integrating inspection of content for hygiene, viruses, etc. With a traditional network (IPSec) VPN, it is only possible to control source and destination address, as well as the port/protocol used.

- **Authorization:** Similarly, the proxy can control users’ access to back-end resources at a very granular level. Whereas an IPSec VPN can control access by IP address and port, a proxied VPN can control access in relation to URL, command, and similar more specific criteria. These rules currently are managed by the SSL VPN device, but during the next two years, we expect integration with portal security and user life-cycle management tools to centralize user role information. We have already seen the first tentative steps toward integration between some SSL VPN and Web access control vendors (e.g., Netegrity SiteMinder, IBM AccessManager, Entrust GetAccess). During 2003/04, we expect an SSL proxy to become a

**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.
tightly integrated portion of the Web access control product set.

- **Logging:** In the process of providing these connections, the proxy can log user activity at the URL and command level, rather than simply logging the amount of traffic to various IP addresses as a traditional IPSec VPN does.

These benefits do not come without a price, however. Organizations have deployed numerous security tools to protect their remote users, such as firewalls and antivirus tools. The enforcement of local security policy typically is implemented via integration between these tools and the IPSec VPN client. Removing this client removes the point of integration, and allowing access from any Web browser means that users will connect from untrusted computers (e.g., Internet kiosks, customer or partner machines. We believe SSL VPN vendors will integrate their solutions with personal firewalls and other tools during 2003/04, but such integration will require some form of client software. Therefore, we have recommended that SSL remote access not be used unless strong authentication tools are present (see GNS Delta 1008) to help mitigate the risks introduced by uncontrolled clients, and to ensure that no downloading of data to uncontrolled endpoints occurs (i.e., to endpoints without managed personal firewalls, antivirus software, etc.). Meeting this requirement is only possible if the proxy is able to differentiate between different client types as well as present different resources, depending on the security access of the client. We expect these capabilities to emerge during 2003-05.

Finally, scalability is a critical issue that has not yet been thoroughly addressed by many SSL VPN vendors. Simple rack-mounted appliances offer excellent out-of-the-box functionality, but both scalability and enterprise-readiness of such solutions are still questionable. By 2004/05, we believe that many of the components of these solutions will be decoupled and integrated with other infrastructure pieces, including the firewalls, load balancers, and portals. Similarly, as with any technology based on a proxy, the vendor must continuously update the proxy to ensure compatibility with various Web platforms (new IIS or Apache versions, etc.). This is an increasingly complex task due to non-Web applications being enabled with connectors, and will likely necessitate frequent upgrades, which can negatively impact availability and reliability.

**Portals, Portals, Everywhere**

Although the existence of an SSL proxy introduces numerous benefits, much of the functionality of remote access (to Web applications, at least) can be achieved with the use of tools that many organizations already use in their customer-facing applications:

- A portal
- A portal security tool (or Web access control tool)
- SSL-enabled Web applications

Although it is certainly possible for organizations to use this approach as a method for presenting internal Web applications to remote employees and partners, coordination of multiple products is clearly a more complex and expensive undertaking than deploying an SSL VPN appliance. For the long term, we believe the technology used in the SSL VPNs (the SSL proxy) will also be applied to external-facing portals, because it can provide three additional critical services to the portal infrastructure:

- Application proxying to enhance security (as detailed above)
- Application connectors to allow non-Web application interfaces
- A centralized point of enforcement for all security functions

Many portal vendors now recommend that a reverse proxy be used as a front end for the portal itself, and the SSL proxy/application proxy can be viewed as simply an evolution of the reverse HTTP proxy currently in use in many organizations.

**Bottom Line**

Use of SSL virtual private networks should be examined not only for the simplicity of client software and support, but also as a mechanism to enable tighter control of remote access, and longer term, as a technology to enhance the security of traditional portals and Web-based extranets.

**Business Impact:** The Secure Sockets Layer VPN has the potential to provide more cost-efficient remote access, as well as to enable access for user populations (e.g., partners, customers) that were previously unreachable with traditional virtual private network technologies.