

NeoAccel SSL VPN-Plus™

The Future of Virtual Private Networks

Overcoming the Performance Limitations of Conventional SSL VPN

Introduction: The Evolution of Virtual Private Networks

VPN (Virtual Private Network) technology was created to enable secure communications over public networks. Current VPN technology permits using the public Internet or any IP (Internet Protocol) network as if it were a private leased line between end-points, providing secure access to all private resources.

Earlier generations of VPN technology were “narrow” solutions that supported limited networking protocols, utilizing transport mechanisms including PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and today’s pre-dominant IPSec (Internet Protocol Security).

IPSec VPN technology was designed exclusively for IP networks. IPSec based VPN offers reasonable performance, standards-based security, and application transparency. However, IPSec suffers from technical complexity for both users of the VPN and administrators of the network infrastructure, resulting in a very high total cost of ownership (TCO).

The newest generation of VPN technology is based on the ubiquitous Secure Socket Layer (SSL), which is embedded in all contemporary web browsers and web servers. This newest generation emerged a few years ago to take advantage of the widespread adoption of SSL for secure web page delivery between a web server and a user’s web browser. The motivation behind the rapid adoption of SSL VPN technology was the desire to eliminate the high complexity and support costs of IPSec VPN for secure delivery of applications and information. SSL security protocols for web page delivery are universally supported by all web servers and web browsers. It is well understood and easy to implement and use. Importantly, network infrastructure, such as firewalls, are

typically configured to pass SSL traffic without administrator intervention of specialized configurations.

The Limitations of Conventional SSL VPN

The first generation of SSL VPN requires a gateway between remote clients and the private network. The remote user accesses the web site hosting the portal and supplies information for authentication purposes (such as a user ID and password). After being authenticated, the gateway serves as a proxy between the “web enabled” application and the end user. The link from the SSL VPN gateway to the end user is HTTPS (i.e., SSL-encrypted Web pages). The SSL VPN gateway proxies connections between the gateway and the end user, converting internal addresses to externally viewable pages that the remote user can access to appropriate applications and data. This is referred to as “no client, web enabled application access” or in many cases “kiosk” mode.

Today’s second generation of SSL VPN technology adds full application transparency without the need for applications to be web enabled. The problem with second-generation implementations is the high overhead and resulting slow performance of the communication between client and gateway. This performance impact is due to three architectural issues.

- 1) SSL is implemented in the “user space” of an operating system environment – as opposed to the kernel space. Since SSL works as a TCP application, the SSL-encrypted link between client and server contains the TCP data stream between the client and the target application server (Figure 1). This overhead results in the TCP-over-TCP meltdown problem that is well known in satellite networks. This TCP-over-TCP meltdown problem dramatically reduces data throughput by a factor of up to 30x and decreases the maximum number of concurrent connections. These performance and scalability limitations are due to the high overhead associated with context-switching operations between user space and kernel space.

- 2) The high latency conditions associated with “lossy networks” often results in significant packet loss especially in WLAN (wireless) environments.
- 3) The latency injection introduced by SSL processing in user space many times contributes to performance degradation compared to IPSec VPN.

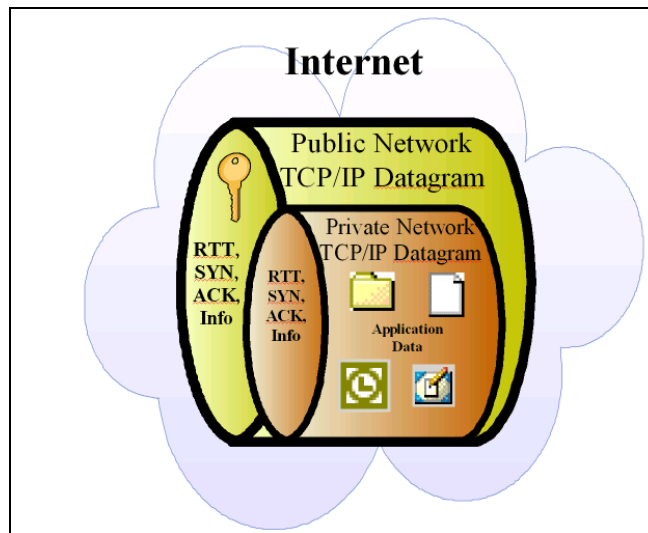


Figure 1 - TCP-over-TCP

Overcoming the TCP-over-TCP Meltdown Problem

The TCP-over-TCP meltdown problem can be overcome by processing SSL connections in the kernel space of the operating system which decreases the number of context-switching operations and eliminates the TCP resizing and slow start problems associated with wireless network jitter. Additionally, by adding hardware encryption, essentially all overhead of SSL processing can be eliminated to provide performance for SSL VPN equivalent to or greater than conventional IPSec VPN. However, if SSL processing is not performed in the kernel, then hardware-assisted encryption loses its acceleration benefits due to the overhead associated with moving data and session

information between the SSL processing routines in user space and the SSL encryption hardware driver in kernel space.

NeoAccel's SSL VPN-Plus™ is the first solution to implement the third generation of SSL VPN technology to overcome the performance-sapping overhead of SSL processing and eliminate the TCP-over-TCP meltdown that plagues conventional SSL VPN in “lossy” environments such as wireless LANs, which can typically consume as much as 20 percent of the SSL VPN throughput capacity. NeoAccel SSL VPN-Plus™ moves all SSL processing into the operating system's kernel space, thus reducing SSL protocol overhead by typically 80 percent compared to second-generation SSL VPN implementations as well as providing complete application transparency. Additionally, NeoAccel has implemented a unique solution based on its patent-pending **Intelligent Connection Acceleration Architecture™ (ICAA™)** that eliminates the need for the user's application session information to be encapsulated over an SSL session -- instead creating a single connection between the client and the VPN gateway.

It is not unusual for network traffic to suffer 1 to 10 percent packet loss, which produces TCP-over-TCP meltdown resulting in 1.5x to 30x longer response time for conventional SSL VPN. Most organizations that have adopted second-generation SSL VPN have experienced the frustration of gaining application transparency at the cost of unacceptable application performance. NeoAccel's SSL VPN-Plus™ uniquely offers the low overhead, high performance, and application transparency of IPSec VPN, but without the complexity experienced by end users or the heavy support costs required by IT organizations.

The following references are some market research analyst observations about the pros and cons of SSL VPN vs. IPSec VPN. Their observations and conclusion now need to be rewritten as a result of NeoAccel's new third generation of SSL VPN solutions.

NeoAccel SSL VPN-Plus™ now offers **ALL** of the performance and full-access advantages of IPsec VPN combined with the simplicity of SSL VPN. NeoAccel's SSL VPN-Plus™ overcomes the “conventional wisdom” that only IPsec VPN can provide site-to-site support while conventional SSL VPN providing only remote access support. Because of the unique architecture of SSL VPN-Plus™ and the resulting dramatic performance and scalability advantages, a third-generation SSL VPN can now offer both the site-to-site support of IPsec VPN and the remote access capabilities of SSL VPN.

SSL VPN and the Future of Virtual Private Networks

Gartner notes that the simplicity and portability of SSL VPN can lower the cost to implement remote-user VPN for corporate workstations, as well as access from non-corporate systems such as PCs. Where traditional VPN are not required, expect immediate value from investments in SSL VPN in the form of easier deployment and support.

However, META Group's METAspectrum SSL Virtual Private Networks Market Summary points to the future broad market adoption of SSL VPN as a replacement for IPsec VPN. “With the onset of widespread adoption and large-scale deployments (i.e., >1,000 concurrent users) during the next two years, the critical requirements will become scalable management functions (particularly configuration capabilities) and greater system performance/capacity. As with most other security solutions, vendors that best balance security, performance, and manageability – and in this case, accessibility to applications as well – will be positioned to dominate the market.”

Adds Michael Suby, senior research analyst at Stratecast Partners (a division of Frost & Sullivan), “Complete remote access solutions encompass three functional components – connectivity, security, and performance. Most SSL VPN are designed to address only connectivity and security. Where NeoAccel is positioned is in directly addressing the performance inhibitors in today's SSL VPN. Once overcome, we expect enterprise deployments of performance-enhanced SSL VPN in WAN and wireless LAN environments to accelerate.”



Contact NeoAccel

CORPORATE HEADQUARTERS

NeoAccel Inc,
2055 Gateway Place, Suite 240
San Jose, CA 95110

TEL: +1 408 274 8000

FAX: +1 408 274 8044

EMAIL: info@neoaccel.com

NeoAccel, SSL VPN Plus, Intelligent Connection Acceleration Architecture and Secure Everything are trademarks of NeoAccel. All other products are or may be trademarks of their respective owners.