

Overcoming the Performance Limitations of Conventional SSL VPN

April 26, 2006

**NeoAccel, Inc.
2055 Gateway Place, Suite 240
San Jose, CA 95110
Tel: +1 (408) 274 8000
Fax: +1 (408) 274 8044
Web: www.neoaccel.com**

VPN Overview

VPNs (Virtual Private Networks) allow communications and collaboration to move beyond the realms of a traditional single workplace LANs (Local Area Networks). Originally developed as a cost-effective way of expanding to a WAN (Wide Area Network) without the use of dedicated fixed-lines, VPNs enable secure communications across geographically dispersed low-cost IP networks like the Internet.

VPN History

Earlier generations of VPN technology were “narrow” solutions that supported limited networking protocols and required complicated network configurations. These utilized VPN tunnel technologies based on PPTP, L2TP and today’s pre-dominant IPSec. IPSec provides decent performance and full network access but has been hindered by difficult deployments and high-maintenance network configurations.

SSL VPN technology addresses the high human resource costs of IPSec by tunneling traffic over standard web-based SSL ports, allowing for simple, anywhere, anytime access to private network resources. Traffic bypasses most ISP filters, firewalls, and network address translation (NAT) issues and allows SSL VPNs to connect where IPSec cannot, for example in a hotel room or internet café. Maintenance costs are greatly reduced and new VPNs can be immediately deployed, anywhere in the world. The result is an 80% decrease in the number of IT helpdesk calls and invaluable productivity gains and accessibility by end-users.

SSL VPN History

First generation SSL VPNs allow network access only to webified application like Outlook Web Access (OWA) or Intranet websites. End-users are authenticated and connect through a proxy-like SSL-enabled web server. Only limited resources were available and access was slow but end-users could connect from anywhere.

The second generation of SSL VPNs adds full application support and features like granular access controls and endpoint security. Application support for all IP protocols is implemented through web-installed full access client software (FAT/PHAT). A granular access policy and endpoint security checks, not available on IPSec, ensure a system is virus-free before allowing it to connect and customized access groups once it does connect.

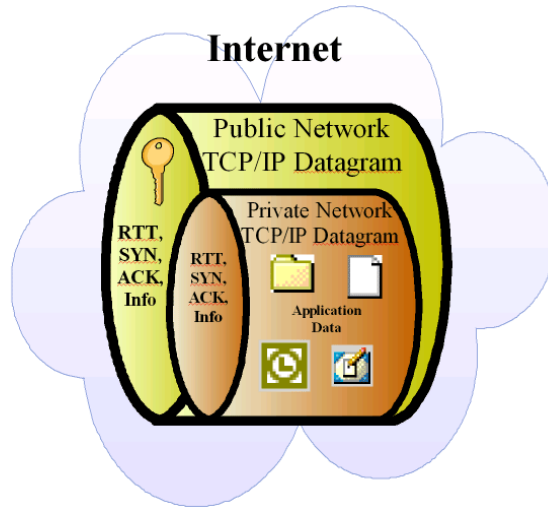
The major problem with current SSL VPN implementations is their lack of performance and scalability. Users experience and IT administrators know SSL VPNs are a tradeoff between performance and ease-of-use. The next-generation of SSL VPN technology developed by NeoAccel™ solves the performance barrier and allows for scalable LAN-like performance in an SSL VPN solution.

NeoAccel’s complete overhaul of the SSL VPN technology model solves two critical performance-draining barriers of existing SSL VPN solutions opening the door as a complete IPSec replacement.

TCP-over-TCP Tunneling

SSL VPN technologies tunnel private network traffic inside a second encrypted protocol for traversal over of the public Internet. This process has overhead but is compounded by the “TCP-over-TCP meltdown” which is inherent when encapsulating one protocol within another. Transmission control protocol (TCP) has various parameters (SYN, ACK, RTT) for setting retransmission times for the delivery of data from client to server in the event of packet loss.

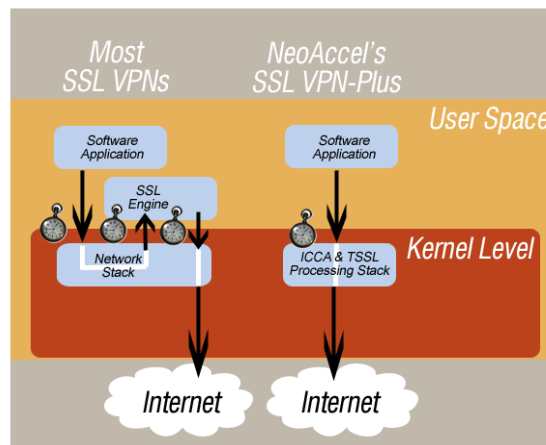
However this repair and recover mechanism fails when encapsulated in a second TCP stream. If the encapsulating or Internet layer drops a packet (which is common even under ideal networking conditions) both TCP streams will attempt to correct the error and retransmit duplicate data. This exponentially queues up data transmissions and prevents the real private network data from promptly reaching its destination.



NeoAccel solves the TCP-over-TCP meltdown with a unique patent-pending technology called Intelligent Connection Acceleration Architecture™ (ICAA™).

User-mode Encryption

Operating Systems have two levels of operation—the user space and kernel space. Most SSL VPNs implement SSL/TLS processing and encryption in the user-space because it's easier and less costly to program. Kernel level crypto, however increase performance by creating a direct data path and bypassing resource intensive copies between kernel and user space. The effect is a highly scalable gateway solution whose performance will not degrade with more users.

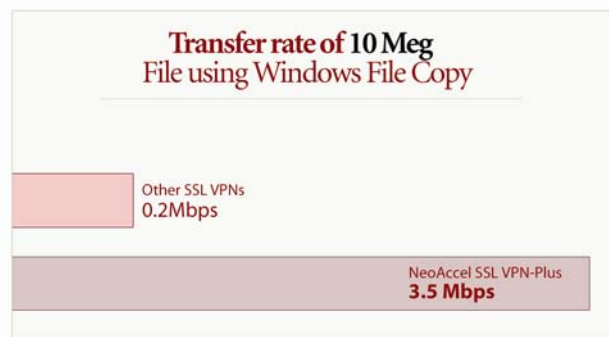


NeoAccel's Transparent SSL™ (TSSL™) bypasses slow user-mode SSL processing

ICAA and TSSL coupled with intelligent compression and an always-on persistent connection dramatically improves end-user experience creating an in-the-office, LAN-like high-performance remote access solution. End-to-end latency as a result of encryption is under 10ms regardless of server load and connections to corporate mail servers and file shares are established instantaneously without the need to tear down, and recreate a new TCP stream.

	Latency	Throughput	Concurrent Users	Time to transfer 5 MB PPT	Time to Download 50 Mail Messages	Initial Connection
NeoAccel	<10ms	950 Mbps	20,000	2 Sec	10 Sec	0 sec
Other SSL VPNs	40ms+	50 Mbps	Maybe 40	17 Sec	30 Sec	1 sec

Under a **perfect network** environment with zero packet loss and a single user connection, NeoAccel’s SSL VPN-Plus beats its competitors. Using bare minimum hardware (Pentium III, 384 Meg RAM) and no external SSL accelerator the NeoAccel SSL VPN-Plus software was able to perform at three times the speed and throughput of competing SSL VPNs *with* built-in SSL accelerators.



However, under simulated “real world” networking conditions and various user-loads the benefits of NeoAccel patent-pending ICAA and TSSL technologies are clear. Under “normal” Internet IP connections terminated by a typical **broadband DSL/cable** user connection, a 2% packet loss and 60ms latency can be expected. Tests results show a significant benefit in using SSL VPN-Plus which translates into transferring a 10 megabyte PPT in under 30 seconds, 20 seconds quicker than our nearest competitor.

When users connect over lossy or high jitter network connections, like **international bandwidth links, cellular modem connections, or wireless networks**, NeoAccel’s SSL VPN-Plus blows away the competition as the effects of TCP-over-TCP grow exponentially. Up to 20% packet loss and 100ms+ of latency is not unusual in these situations. SSL VPN-Plus surpasses the competition both in ability to establish a connection, response time, and data transfer rates. A typical user connecting and downloading 50 email messages can do so thirty times faster than with alternate solutions.

The productivity benefits of implementing a high-performance SSL VPN for a single transaction are evident in these results. However in actual, real-world deployments the benefits compound as multiple network communications through the SSL VPN are common for a single user on a single session. Over the course of a year, these seemingly incremental speed increases from a high-performance SSL VPN provide a compelling reason to choose the *Fastest VPN on the Planet*.

NeoAccel’s breakthrough performance and technological innovations coupled with granular access policies and easy-to-manage, plug-in ‘n relax network appliance opens the possibility for SSL VPN-Plus as an internal network access control (NAC) device. A study on implementing

NAC devices by Infonetics research concludes SSL VPNs will become the preferred method for network access controls into the future.

Granular access controls allow for customized, access-limited VPNs for every user. So, a CEO might have access to all network resources while an accountant might only have access to department-specific resources. This gives IT administrators' unprecedented control of the network. SSL VPN-Plus can be used both for remote access and as an **internal** device providing NAC.

Performance *was* the key limitation preventing SSL VPNs from overcoming IPSec VPNs and NeoAccel solves this with our SSL VPN-Plus product.

Although NeoAccel has attempted to provide accurate information in these materials, NeoAccel assumes no legal responsibility for the accuracy or completeness of the information.

© 2004-2006 NeoAccel, Inc. All Rights Reserved. NeoAccel, SSL VPN-Plus, Intelligent Connection Acceleration Architecture, SGX-1200, SGX-2400, SGX-4800 and Secure Everything are trademarks of NeoAccel. The information herein is provided for informational purposes only and is subject to change without notice. All other trademarks are the property of their respective owners.

NeoAccel Inc.
Proprietary and Confidential