

SSL VPN-PLUS™ VERSION 2.2

THE THIRD-GENERATION VPN

NeoAccel delivers all the advantages of SSL VPNs—better security, better return on investment and lower total cost of operation and universal access—without the performance degradation found in all other SSL VPN solutions.

SSL VPN-Plus

NeoAccel's patent pending SSL VPN-Plus™ solution is architected to address the deficiencies found in today's remote access solutions: lack of performance, security, return on investment, and ease of use.

High Performance and Capacity

NeoAccel delivers all the advantages of SSL VPNs at speeds faster than IPsec VPNs.

Conventional SSL VPN solutions suffer performance issues due to redundant tunneling of data (resulting in performance-degrading TCP-over-TCP meltdown), excessive packet processing and unnecessary data compression. NeoAccel's patent pending technology addresses all these issues and more.

Unique single-tunneling of data eliminates TCP-over-TCP meltdown. Kernel level-only processing of data eliminates excessive packet processing overhead. And dynamic compression determines when compression is beneficial.

Capacity of up to 10,000 concurrent users per gateway, ultra-low latency, addresses the largest of deployments.

Endpoint Security

All endpoints are subjected to policy-based compliance checks before they are admitted to a network. Hundreds of pre-defined checks for updated operating system and security software, malware

presence, and more, are done before authentication. Additional checks are easily configured. An administrator has control over download and print screen rights for the remote users. Endpoint cache cleanup at the end of session eliminates traces or finger prints of data from the remote machine.

Data Leak Prevention

Highly advanced feature like **Secure Workspace Access Terminal** in combination with zonal policies totally eliminates the possibility of data leakage through any medium thus ensuring business confidentiality. It creates a virtual 'crypt' of the session data and also (if specified) destroys it at end of session.

Return on Investment

Elimination of large, configuration-dependent clients make SSL VPNs a clear choice for secure remote access.

No client-side installs or updates are required. Automatic re-connection between user and gateways and high availability clustering ensure network failures and timeouts do not block access to critical applications and data. The result is reduced technical support calls and zero client management costs.

Full Access to All Applications

All enterprise applications are supported: Web applications, thin-clients, PHAT-clients and legacy applications means only a single remote access solution is required.

Granular Network Access

Once endpoint security is assured, powerful and

Overcome the limitations of other VPN solutions with...

- No performance degradation
- Improved return on investment
- Clientless remote access
- Support for all applications

easy policy management governs all network access. Policy decisions to allow, or deny, access is based on user and group policies. Security zones, with access control enforcement, provide full flexibility and granularity of network access—for both employees and non-employees.

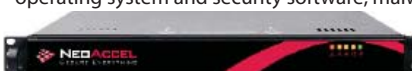
Advanced Log Reporting

Highly advanced Log reporting feature provides fabulous snapshots of remote accesses to your resources at a glance; provides 24 different parameters for log filtering; tracks and evaluates each remote user access. Thus, helps in your policy making decisions. Reports generated are dynamic; customized; available in multiple formats. Reports can be saved or taken as prints.

Ease of Use

Rather than granting conventional network-wide access to remote users, four modes of access provide as much, or as little, access as needed—all with minimal, central configuration. Complex client-side configurations are a thing of the past.

And the most popular enterprise platforms are supported—Windows®, Mac OS® and Linux®—ensuring no user is left behind. Deployment into existing networks is facilitated by support of existing authentication solutions.



NeoAccel SSL VPN-Plus Gateway

SSL VPN-PLUS GATEWAYS

THROUGHPUT AND CAPACITY

	Throughput	Capacity
SGX-4800	950Mbps	Up to 2,500 CCU
SGX-2400	500Mbps	Up to 2,000 CCU
SGX-1200	250Mbps	Up to 250 CCU
Logins/Second	1,800	
SSL Transactions/Sec	8,400	
Latency	<10ms	

APPLICATION SUPPORT

All IP-based applications (TCP, UDP)
 Web-enabled applications
 Dynamic IP- and port-based applications
 Legacy mainframe applications

ACCESS CONTROL AND AUTHORIZATION

Based on:
 Internal/external group membership
 Block cut/copy/paste/printscreens
 Per: protocol, IP address, time schedule, multiple port entries
 Security Policies
 Application execution and access control
 Group extraction from alternate authentication server, LDAP/AD

PROTOCOLS

SSL 3.0 and TLS 1.0
 Remote access VPNs
 Full, Split Tunneling, Local LAN Exception Encryption
 DES, 3DES, AES (256), AES (512) RC4
 Authentication
 MD-5, SHA-1, RSA 1024, RSA 2048

REMOTE ACCESS METHODS

Web Access Terminal (WAT) – Clientless
 For use with all browser-based applications
 Access through Web portal
 SSL VPN-Plus End Point Security enabled
 Access via any SSL-enabled browser
 Virtual Application Terminal (VAT) – Clientless
 For use with remote login and virtual desktop applications
 SSH, Telnet, Windows RDP, VNC
 Access via any SSL-enabled browser
 Session-only Java applets used
 Access through Web portal
 SSL VPN-Plus End Point Security enabled
 Quick Access Terminal (QAT) – Clientless
 For client-initiated TCP-based applications
 Access through Web portal
 SSL VPN-Plus End Point Security enabled
 Access via Microsoft Internet Explorer
 Full Access Terminal (PHAT) – Client-Based
 For use with all IP-based (TCP, UDP) applications
 Access via small-footprint client (2MB footprint)
 Windows 2000, Windows XP, Windows Vista 64 bit, Windows Mobile 5.0, 6.0
 MacOS X Leopard and Tiger, Linux (Fedora core 4-8; Ubuntu 6.06-8.04; and RHEL 3.5)
 Optional Access through Web Portal
 SSL VPN-Plus End Point Security enabled
 Layer 2-7 access controls
 Secure Workspace Access Terminal

ENDPOINT SECURITY ENFORCEMENT

Up to 40 Security Zones based on:
 Access control policy per group/user
 End point security policy compliance
 Pre-configured enforcement rules
 By: files/process/registry entry/ports/service/WMI/certificate based EPS rules
 Pre-configured enforcement policies
 Anti-spyware (updated and active), Anti-spam

(versions and updates), Anti-virus
 Desktop search engine presence
 Inbound port scanning
 IP forwarding
 Microsoft Windows
 Service Packs (presence and updated)
 Security patches (presence and updated)
 Firewall enabled
 Automatic Update activated
 Internet Explorer security settings
 Network Bridge enabled
 Personal firewalls (presence and updated)
 MAC and Linux support
 Cache cleaning
 URL history
 Temporary Internet files
 Downloaded program files
 Stored cookies
 Virtual keyboard to prevent keylogging
 Online EndPoint Upgrade Server

AUTHENTICATION

Local database
 RADIUS, LDAP
 Microsoft Active Directory
 RSA SecurID
 SSL Client via digital certificates
 Two-factor authentication via PKI, tokens
 NTLM and Kerberos based single sign-on (SSO)
 Dual Authentication
 Dynamic authentication based on EPS Trust Level

WEB PORTAL

Launch:
 Desktop applications, Web Applications
 Remote login and virtual desktop applications
 Tools
 Easy access URL, Multiple portal layouts
 Dynamic portal generation based on authorization

MANAGEMENT

OPERATING SYSTEM

NHOS (NeoAccel Hardened Operating System)

NETWORKING

Static routing; Dynamic routing: RIP v1/v2, OSPF
 DHCP
 Address Pools
 Network Address Translation (NAT, NAPT)
 NTP, 802.1q VLANs
 Firewall Rules

HIGH AVAILABILITY

Active/Passive

DEVICE MANAGEMENT

Single-user and role-based
 Command line interface
 Console, SSHv2
 Java-Based Web user interface
 HTTP, HTTPS
 SNMP version 2 and version 3

LOGGING AND MONITORING

Local and external Syslog server logging
 Statistics and Log reporting
 IP, port, user, resources accessed, login failures, bandwidth usage
 Per-user statistics, 3rd-party log analyzer-compatible

APPLIANCE (1U RACK MOUNT)

CHASSIS

Dimensions	(W/H/D)	Weight
SGX-1200	16.7"x1.7"x14"	17lbs
SGX-2400	16.7"x1.7"x 27"	18lbs
SGX-4800	17.2"x1.7"x 26.8"	20lbs

Interfaces

SGX-1200	2x1000BaseT
SGX-2400	4x1000BaseT
SGX-4800	8x1000BaseT

Hard Drives

SGX-1200	1x160G, Fixed
SGX-2400	2x160G, Hot-Swappable
SGX-4800	2x160G, Hot-Swappable

Hardware SSL Acceleration

On demand/requirement for SGX 2400 or above

Power

All	100-240 VAC, 50-60 Hz
SGX-1200	260W
SGX-2400	400W, Dual, Redundant
SGX-4800	560W, Dual, Redundant

Temperature

Operational	5° to 40°C
Storage	-40° to 70°C
Humidity	5% to 85%

Safety Compliance

cULus, CE

EMC Compliance

FCC Class A
 ROHS Compliant

Maintenance and support agreements available through an authorized reseller, or by contacting NeoAccel sales support at +1 408 436 1000 for more information.

Technical assistance available through an authorized reseller or through NeoAccel support online at <http://support.neoaccel.com>

NeoAccel, Inc.

4030 Moorpark Ave,
 Suite 114, San Jose,
 CA 95117 USA

Jaysynth Center,
 Plot No. 6, Sector 24,
 Turbhe, Vashi,
 Navi Mumbai,
 India - 400 705

Tel: +1 408 270 7500 (022)2783 0195/96

Fax: +1 408 274 8044 (022)2783 0197

E-Mail:

info@neoaccel.com

sales@neoaccel.com

Web: www.neoaccel.com