

# Virtualized SSL VPN-PLUS™

## The only 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 patented SSL VPN 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 issues with video/VoIP deployments.

### Superior Technology

SSL VPN-Plus's unique and superior technologies such as **ICAA** - Intelligent Connection Acceleration Architecture, **TSSL** - Transparent SSL, and **ATCE** - Accelerated Triggered Compression Engine performs single-tunneling of data that eliminates TCP-over-TCP meltdown, Processing of data at the Kernel level only, and eliminates excessive packet processing overhead respectively. The dynamic compression technology (ATCE) determines when compression is beneficial.

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



NeoAccel SSL VPN-Plus Gateway

### End Point 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

Overcome the limitations of other VPN solutions with...

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

applications means only a single remote access solution is required.

### Granular Network Access

Once endpoint security is assured, powerful and 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.

# Virtualized SSL VPN-PLUS™

## VIRTUAL GATEWAY (on VMWare ESX Server)

Run up to 128 independent virtual gateways  
 Central Management Interface specifically designed for MSPs  
 Appliance-wide or individual instance upgrades  
 Segregates traffic using layer 2 VLANs— independent VLANs for each SSL VPN-Plus instance  
 Easily integrated into existing network infrastructure  
 Utilizes VMWare ESX Server's superior virtualization platform  
 Adjustable minimum and maximum limits on hardware resource allocation  
 Allows for the maximum efficiency and simple hardware management by running multiple VPN instances on one appliance

## THROUGHPUT AND CAPACITY (SGX 5200)

VLANs per Appliance	Up to 128
Throughput	900Mbps per WAN/LAN pair
LAN/WAN ports	Expandable up to 8 pairs
Capacity	Up to 10000 Concurrent Users
Logins/Second	1,800SSL
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 (2U RACK MOUNT)

### CHASSIS

Form Factor	2U, rack mount
Dimensions (W/H/D)	17.2"x1.7"x 26.8"
Weight	46 lbs
Interfaces	4x1000 Fiber Optic
Hard Drives	2x46G, Hot Swappable expandable to 8x146G
Power Consumption	100-200 VAC, 50-60 Hz 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	

## Ordering Information

Product, maintenance, and support available through an authorized reseller, or by contacting NeoAccel sales at +1 408 274 8000 for more information.  
 Technical assistance available through an authorized reseller or through NeoAccel support online at [www.neoaccel.com/support](http://www.neoaccel.com/support).

## NeoAccel, Inc.

2025 Gateway Palace, Suite 467, 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: <a href="http://www.neoaccel.com">www.neoaccel.com</a>	