

General

- Mac OS X, Linux, Handheld & Windows Clients
- Multilingual User Interface
- Full & Split Tunneling Support
- VLAN Support
- Deployable behind a Firewall, Edge-facing, DMZ, Single Arm or Core

Application Support

- All IP based Applications (TCP & UDP)
- Dynamic IP and Port based Applications
- All Legacy Applications: Mainframe/midrange
- Web-enabled Applications: OWA, Lotus Notes, Oracle, Sharepoint Portals, Public Websites
- VoIP & Video Conferencing

Encryption Support

- SSL Protocol Support: SSLv3 and TLSv1.0
- Ciphers: AES up to 256 bits, DES, 3DES, RC4
- Hashes: MD5, SHA-1 RSA 1024, 2048 bits

Authentication By:

- Local Users & Groups Database
- Attached RADIUS, LDAP, or Active Directory
- Username/Password Authentication
- SSL Client Authentication via Certificates
- Two Factor Authentication

Access Control Based On:

- User & Group Authentication
- End Point Security Audit Results
- Destination Service (Exchange Server, SSH, FTP, Telnet, etc.)
- Source IP/IP Range/Network & Destination Server
- Day of week, date and time
- Current Number VPN Tunnels
- Max Session Lifetime

Monitoring & Reporting

- Per User Statistics
- Logs: IP, Port, User, Internal Resources Accessed, Login Failures & Bandwidth Usage
- Local and External Syslog Server Logging
- Support for 3rd Party Log Analyzers
- Web Accessible Logs via NMC
- Real-time User Termination

Configuration & Management

- Web/Java GUI NeoAccel Management Console (NMC)
- Sub-user Limited Access Management Accounts
- Remotely Manageable
- Serial COM Port CLI Support
- Network Troubleshooting Utilities
- XML RPC for Third Party Integration

Endpoint Security-General

- Real-time Checking for System Updates/Service Packs
- Check for 3rd Party EPS Software
- Detect Presence of Malware, Desktop Search Engines & Key-loggers
- Browser Cache Cleaning, URL History and Stored Password Cleanup
- Optional Prevention of Copy/Paste & Printing
- Custom EPS Checks based on Files, Registry, Process, Open Ports and Drivers.
- Virtual Keyboard

Built-in EPS Checks

- Installed Windows Service Packs
- Activated Windows Auto-Update
- Latest Windows Security Patches
- Appropriate Browser Security Level
- Windows Firewall Enabled
- IP Forwarding Disabled
- Network Bridging Disabled
- Active & Updated Anti-Virus (Norton, McAfee, TrendMicro, Symantec, AVG, NOD32)
- Active Firewalls (McAfee, AVG, TrendMicro)
- Inbound Port Scanning Check

Access Options

Web Access Terminal Client (Kiosk)

- Requires only a SSL enabled browser to access web based applications and services in corporate network
- Useful for access from Internet kiosks and low security systems
- Provides remote access from remote clients, which have limited access rights
- Terminal emulators for secure shell and virtual terminals (Telnet, SSH, VNC & RDP)
- File shares
- Endpoint Security Enabled Customized SSL VPN portal to provide user and group specific web pages; also helpful for customers to configure their own pages.

Quick Access Terminal Client (Port Forwarding Client)

- Access to all TCP and UDP based applications
- No Software installation required on endpoint machine
- No Administrative rights required
- Endpoint Security Enabled
- Supported OS: Windows 2000 family, Windows XP family, Mac OS X, Linux OS

Private Hyper Access Transport Client (Full Client)

- Full access to TCP, UDP and IP based applications
- Highest performance Optimized for VoIP & Video Conferencing
- Option for split tunneling/full tunneling
- Supported OS: Windows 2000 family, Windows XP family, Red Hat Linux Enterprise Server, CentOS, Knoppix, Debian
- Installation via Internet Explorer 4.0 or higher (Downloaded component is signed ActiveX Component 390KB), standalone installer for non-IE browsers (512KB)
- Total size of installed components on disk – 2 MB
- Endpoint Security Enabled
- SDK for VPN-izing Any Application
- Integration with GINA for domain controller access.