



## Secure Application Access Gateway for Your Business

The AEP Netilla Security Platform (NSP) SSL VPN enables secure, web browser access to a broad range of business applications. With any PC or laptop, telecommuters, day extenders, branch office employees, business partners and a mobile sales force can quickly and securely reach virtually any resource used in your business.

## Access All Your Applications

- Full icon-driven end user interface
- Server-based Windows® Terminal Server, Citrix®, UNIX®/Linux, Ericom Powerterm® WebConnect & Mainframes
- Any Web application or portal
- Any Client/Server application
- Web-based access to files and network shares
- Clustering, load balancing and failover for thousands of users
- Application auto-launch and logout support
- Portal customization (by V-Realm)

## Terminal Server Applications

The NSP provides browser-based, “thin client” proxy security for applications in a fully protected environment.

- Policy-driven, web-based access to Citrix, Microsoft® Windows Terminal Servers, UNIX/Linux & Mainframes
- Drive mapping for seamless interactivity with local and remote data
- Session persistence for workflow continuity
- Local and remote printing via Universal Print Driver
- High color for medical and graphic-intensive applications
- On-demand Microsoft Windows Terminal Server (RDP) and Citrix ICA (Native, ActiveX, Java) client delivery option

## Web Applications & Portals

HTTP reverse proxy technology protects your web applications and your network infrastructure.

- Secure access to any Web application, corporate intranet, or portal
- Application-layer proxy hides network topology
- Granular access controls to URLs, applications, and data
- Web application security: Protects against cookie snooping, denial of service & network access attacks, authentication hijacking, DMZ protocol attacks, and more

## Client/Server Applications

Emulates IPsec functionality with the performance and ease of use associated with SSL VPNs.



- Network adapter for Layer 3 tunnel connectivity
- Security (encryption) for VoIP applications
- Application adapter for Layer 4-7 connectivity
- On-demand, automatic adapter installation
- ToolTray and/or local client launchable (option)
- No end user configuration or installation – minimal Admin rights required
- Granular policy enforcement

## NSP Security Features

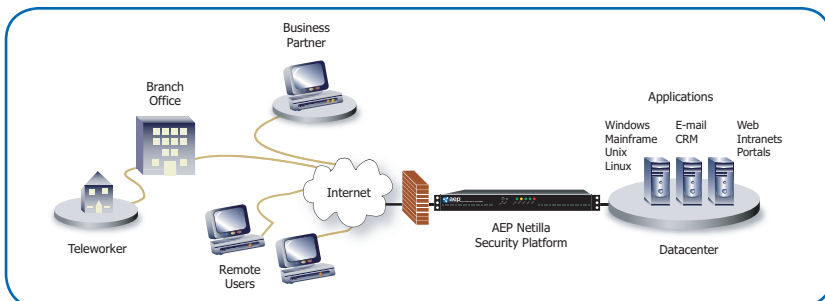
- Policy-enforced deployment of individual applications through an icon-driven webtop
- Application Layer Proxy protection: Shields your network resources from public exposure
- Complete Endpoint Security solution eliminates data leakage (Cache Cleaner, Host Integrity, Adaptive Policies)
- Client Machine Identification (CMID) authorizes specific PCs
- Configurable session timeouts and periodic re-authentication
- Certified solution: ICSA Labs, VPNC, CSIA
- Reporting and logging helps meet regulatory compliance
- FIPS 140-1, Level 3 Option

## NSP Management Features

- Seamless integration with directories: Microsoft Active Directory, LDAP
- Netilla V-Realm™-based granular access control and policy enforcement
- Simple, web-based administration
- Role-based administration
- SNMP and Syslog support
- Strong authentication for administrator login
- Connection management display and event reporting

## Benefits

- Broad application support – Access any application in the datacenter.
- Client integrity assures compliance with corporate policy, before allowing access
- Application servers stay deep in the datacenter minimizing security risks and patch management headaches.
  - Seamless connectivity with authentication and policy servers already in use
  - Easy to maintain appliance reduces IT admin and maintenance – Remote users only need a browser
  - Access, security, authentication and policy within a single platform – lowers costs of ownership.
  - Quick installation with no infrastructure changes required
  - Icon-driven user interface eliminates end-user retraining





## Security

### Netilla V-Realm Architecture

- Up to 1000 "virtual" realms per appliance
- Granular authentication and policy groupings (e.g., by department)
- Supports up to ten authentication, client integrity and policy stages per grouping
- Supports Microsoft Windows Global groups and Active Directory, LDAP groups, and local groups

### Authentication

- Microsoft Windows NT/2000/2003 - SMB/Active Directory
- RADIUS® and RADIUS Groups
- LDAP (Open LDAP, Novell eDirectory®, IPlanet)
- Kerberos
- Vasco® Digipass (Built-in server)
- RSA SecurID®
- ActivCard®
- Aladdin®
- Client-side certificates with revocation
- HTML forms-based

### Encryption

- 128-bit SSL 3.0 encryption
- AES cipher-suites (128, 256 bit key lengths)
- Encryption of all authentication and session data

### Firewall

- Stateful-inspection technology
- Single firewall traversal limits port openings
- Session-based for controlled tunneling access

### Additional

- Integrated Symantec Agent (SODA) Client Integrity suite
- Configurable session timeouts and Periodic Re-authentication
- Session disconnect on demand
- Single login enforcement
- FIPS-140 Level 3 compliance option
- CESG "Private" compliance

## Application Access

### Browser & O/S Recommendations

- Windows XP and Vista (32-bit): All Services
  - Microsoft Internet Explorer 6.x & 7.x
  - Mozilla Firefox 2.x
- Macintosh OS X: Thin Proxy, Web Reverse Proxy, Web Port Forwarding, and Files
  - Safari 2.x
- Linux Redhat: Thin Proxy, Web Reverse Proxy, Web Port Forwarding, and Files
  - Mozilla Firefox 2.x

### Email

- Outlook Web Access (OWA) or other Web-based e-mail
- Microsoft Exchange, Lotus iNotes, or other IMAP

### Applications

- Windows Terminal Services, Citrix MetaFrame Presentation Server, Ericom PowerTerm WebConnect, Linux/Unix/X-Window and mainframe character mode
- PACS, CRM, Sales Force Automation (SFA), Siebel, Oracle, PeopleSoft, portals, and any other web-based application
- Microsoft Exchange, Microsoft Great Plains, GoldMine, and any other client/server application
- Application auto-launch option
- Policy-driven, icon-based user interface

### File Access

- Java-based files browser
- Supports Microsoft ActiveDirectory, per-user bookmarks, drag and drop uploads/downloads
- Drive Mapping

### Continuity and Productivity

- Disaster Recovery Demand Licensing option
- High availability through AEP Netilla Security Platform Load Balancer (NSP-LB)
- Geographical Load Balancing and Clustering for up to 10 NSPs (with the NSP-LB)
- Session persistence (for Windows Terminal Servers)
- AEP GenIE™ security and system updates

### Management and Reporting

- Web-based Administration GUI
- Connection management and display tool
- SNMP and Syslog
- Minimal Admin rights required
- Firewall event monitoring
- Performance and system assurance monitoring

## Hardware

### Network Requirements

- Dedicated Internet access with static IP address
- Available 10/100/1000 BASE-T Ethernet connection/s

### Physical Specifications

- Appliances are available in A, B and G platforms, depending on your organization's capacity needs.
- Dimensions: 16.8 in. x 14 in. x 1.7 in. (427 mm x 356 mm x 43 mm)
- Fits in a standard single-unit 1U rack

### Power Requirements

- A-Class
  - AC Voltage: 100-240 V, 60-50/Hz
  - Power Consumption: 200 watts max
- B and G-Class
  - AC Voltage: 100-240 V, 60/50Hz
  - Power Consumption: 260 watts max

### Port Specifications

- Two RJ-45 10/100/1000 Ethernet
- One serial console port

## About AEP Networks

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network – from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, high assurance IPSec-based VPN encryptors, and hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company is headquartered in Somerset, New Jersey, with offices worldwide.

## Accreditation



## Contact Us

### CORPORATE HEADQUARTERS

347 ELIZABETH AVE., SUITE 100  
 SOMERSET NJ 08873  
 TOLL-FREE: 1 877 638 4552  
 TEL: (+1) 732 652 5200

### EUROPE

FOCUS 31, WEST WING  
 CLEVELAND ROAD  
 HEMEL HEMPSTEAD  
 HERTS HP2 7BW U.K.  
 TEL: (+44) 1442 458 600

### JAPAN

JOYO BLDG 6-22-6  
 SHIMBASHI MINATO-KU  
 TOKYO 105-0004  
 JAPAN  
 TEL: (+81) 3 3432 3336

### ASIA-PACIFIC

SUITE 315, JUJINGYUAN YONGJIN PLAZA  
 #266 - 268 WEST LAKE AVENUE,  
 SHANGCHENG DISTRICT  
 HANGZHOU CITY  
 ZHEJIANG PROVINCE 31002  
 CHINA  
 TEL: (+86) 571 8702 2892