



Secure Application Access Gateway for Your Business

The AEP Netilla 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 of Your Applications

- Any Web application or portal
- Any Client/Server application
- Server-based Windows® Terminal Server, Citrix®, UNIX®/Linux, Ericom Powerterm® WebConnect & Mainframe applications
- Web-based access to files and network shares
- Application auto-launch and logout support
- Full icon-driven end user portal interface
- Portal customization (by V-Realm™)
- Clustering, load balancing and failover for thousands of users (Netilla 4000/6000) Web Applications & Portals

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

Terminal Server Applications

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

- Identity-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 (via Thin proxy functionality)
- High color for medical and graphic-intensive applications
- On-demand Microsoft Windows Terminal Server (RDP) and Citrix ICA (Native, ActiveX, Java) client delivery option



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

Netilla Security Features

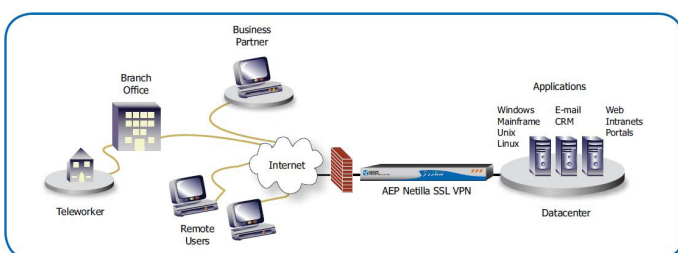
- Policy-enforced deployment of individual applications through an icon-driven webtop
- Application Layer Proxy protection: Shields your network resources from public exposure
- Endpoint Security solution eliminates threats of data leakage (Cache Cleaner and Host Integrity Checks)
- Client Machine Identification (CMD) authorizes specific PCs
- Configurable session timeouts and periodic re-authentication
- Certified solution: ICSC Labs, VPNC, CSIA
- Reporting and logging helps meet regulatory compliance
- FIPS 140-2 Level 4 Option

Netilla 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
- 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 cost 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™ Active Directory Global Security groups, LDAP groups, RADIUS Groups and local groups

Authentication

- Microsoft Windows Server 2000/2003/2008
- SMB/Active Directory
- RADIUS and RADIUS Groups
- LDAP (Open LDAP, Apple® Open Directory, Novell eDirectory®, IPlanet™)
- Kerberos
- Vasco® Digipass (Built-in server)
- RSA SecurID®
- ActivCard®
- Aladdin®
- Client-side certificates with CRL revocation support
- 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 Options

- Endpoint Security Suite (Cache Cleaner, Client Integrity)
- Configurable session timeouts and
- Periodic Re-authentication
- Session disconnect on demand
- Single login enforcement
- FIPS 140-2 Level 4 compliance option
- CERG “Private” compliance
- Power switch/hard drive redundancy

Continuity and Productivity

- High availability, Clustering and Geographical Load Balancing for up to 10 Netilla appliances through the AEP Netilla Load Balancer
- Session persistence (for Windows Terminal Servers)
- AEP Netilla GeNIE™ security and system updates

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/3.x
- Macintosh OS X (10.5): 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/3.x

Email

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

Applications

- Windows Terminal Services, Citrix® XenApp™, Ericom® PowerTerm WebConnect, VDI, 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, user home folders, drag and drop uploads/downloads
- Drive mapping

Management and Reporting

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

Network Requirements

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

Hardware

Physical Specifications

- 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

Licensing and Capacities

Appliances ship with unlimited user licensing and support access according to the following recommended capacities:

- **Netilla 2000:** 50 concurrent users
 - **Netilla 4000:** 250 concurrent users
 - **Netilla 6000:** 500 concurrent users
 - **Netilla 6100:** 1000 concurrent users
- * Thin proxy concurrent licensing option available

Power Requirements

- **Netilla 2000**
 - AC Voltage: 100-240 V, 60-50/Hz
 - Power Consumption: 200 watts max
- **Netilla 4000/6000**
 - AC Voltage: 100-240 V, 60/50Hz
 - Power Consumption: 260 watts max
- Redundant-powered systems available (**Netilla 6100**)

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, CAPS approved high assurance IPSec-based VPN encryptors, and FIPS certified hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company has design and development offices in its headquarters in Somerset, New Jersey, USA and Hemel Hempstead, UK.

Contact Us:

United States
Toll-Free: 1-877-638-4552
Tel: +1-732-652-5200
Europe
Tel: +44 1442 458 600

Email: sales@aepnetworks.com
Web: www.aepnetworks.com

Accreditation

