

Secure remote access is increasingly important for the enterprise. Making corporate resources and information securely accessible to any authorized user is a must for enterprise administrators, but racks full of equipment, puzzling licensing and maintenance schemes muddy remote access and disaster recovery response strategies. AEP Networks answers this by providing:

- ▶ An enterprise SSL VPN that plugs into your virtualization infrastructure
- ▶ A simple, affordable “pay as you grow” model that allows unlimited virtual appliances, providing a scalable and fault-tolerant architecture

Delivering seamless, secure, controlled access to employees, partners, and vendors who need managed access to corporate information can be a daunting task, AEP Netilla[®] SSL VPN Virtual Edition (Netilla VE) leverages existing infrastructure to ease the process.

Netilla VE Benefits

Scalable and Cost-Effective: Netilla VE provides a low entry cost. Get started with as few as 5 user licenses. Netilla VE allows IT security managers to take advantage of streamlined hardware maintenance processes, lower data-center power consumption and improved business continuity benefits inherent in server virtualization deployments.

Disaster Planning: Netilla VE is an excellent solution to ensure access to corporate data in the event of a disaster, harsh weather or other calamity. With the unrestricted licensing and the ability to turn up virtualized Netilla servers at will, you can scale your infrastructure instantly to accommodate these situations.

The Trusted Choice: AEP Networks is a pioneer in the development of secure remote access, application protection and user authentication solutions, with products used by numerous Global 1000 companies, governments and educational facilities around the world.

Easy Implementation and Use: Netilla VE drops into your existing virtualization infrastructure. Point port 443 on your firewall to Netilla, point Netilla to your authentication server, create your application policies and off you go. Integration with existing authentication and user directories means no separate user creation or maintenance.



Ideal for Enterprise Accounts

- Prepackaged virtual appliance streamlines installations for virtual servers such as VMware ESX/ESXi, giving you a custom fit for your environment
- Instant integration with existing authentication infrastructure.
- Deploy as many virtual machines as needed
- Web-Based clientless or installed client options
- Scalable and disaster proof: Install multiple instances as individually addressable appliances or cluster them together with an AEP Netilla Load Balancer solution for unrivalled scale and redundancy, even across geographies.

Netilla VE Key Features

- **Seamless Authentication:** Plugs into your existing authentication infrastructure, with support for Active Directory, Novell NDS, LDAP, Open Directory, RADIUS, SecurID, VASCO, PKI and HSPD-12.
- **Deep application support:** Terminal Services, VDI, Citrix, Web-based applications, SharePoint, Exchange, ANY TCP-based application, SSL Tunnel capability.
- **Client Machine Identification:** Ensure only PCs issued by the organization have access to specific resources. Access is restricted in the event of unauthorized machine modification.
- **Client Host Integrity:** Ensure client devices maintain corporate standard anti-virus, firewall and other requirements prior to access.
- **High Availability:** Scale your infrastructure and ensure access uptime in one or many geographically disbursed data centers.

Why Netilla VE?

- **Management:** Web based management, no complex CLI to learn.
- **Access:** Unparalleled access control options and ease of integration.
- **Certification:** ICSA v3 and CCTM certified, FIPS 140-2 Level 4 option available.
- **Security:** Unmatched security granularity, control applications and application policy by realm, group or user.



Netilla V-Realm Architecture

- Up to 1000+ "virtual" realms per appliance
- Granular authentication and policy groupings
- 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)
- RSA SecurID®
- ActivIdentity™
- 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
- CESA "Private" compliance
- Power switch/hard drive redundancy

Continuity and Productivity

- High availability, clustering and geographical load balancing for up to ten Netilla appliances through the AEP Netilla Load Balancer
- Session persistence (for Windows Terminal Servers)
- AEP Netilla GeNIE™ security and system updates

Browser & O/S Recommendations

- Windows XP and Vista (32-bit): All Services; 64-bit (Tunnel Service)
 - Microsoft Internet Explorer 8.x, 7.x, 6.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 Red Hat: 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
- MyDesktop direct client desktop access
- 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)

MyDesktop Client PC Access

- Secure, remote access to a single user's PC via auto-created access control lists (ACLs)
- Ease of setup: Publish one application that serves all users

Configuration

- Integrates with VMware® ESX/ESXi Infrastructure utilizing existing VMware administrative tools
- Integrates easily within enterprise-wide security framework
- Deploy as many virtual machines as needed
- Single virtual machine supports from 5 to 1000 users
- Netilla VE LB virtual load balancer available

Licensing Flexibility

- Low cost "pay as you grow" model
- User license packs range from 10-1000 users

About AEP Networks

AEP Networks offers secure communications, networking and application access for government, enterprise and carriers. We work with systems integrators, managed service providers, and the distribution channel to deliver integrated solutions incorporating our leading edge products: Enhanced-grade secure voice and multi-service data platforms (based on the vados operating system) that support a wide range of communications protocols and network topologies; High assurance networking via IPsec-based VPN encryptors for site-to-site security and remote access; Hardware Security Modules (HSMs) for cryptographic key management and storage; Secure remote access to networks and applications - including virtual environments - via application-layer security gateways and SSL VPNs.

Contact Us:

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

VMware Technology Alliance Partner



Accreditation

