

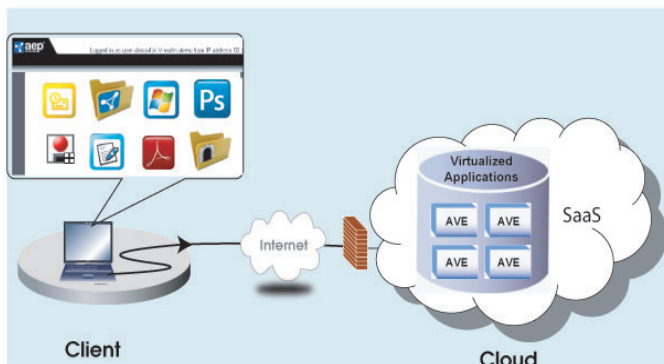
When virtualizing your data center, simply run the Series A virtual appliance within your existing assets, maximizing utilization. Easily deliver secure, virtual, remote access to your customers over any network from any device. Deploy as many Series A virtual machines as needed for user access Scalability and for Disaster Recovery. Go green and grow securely with Series A.

- ▶ **Instant Savings.** No need to purchase more hardware and you save on power and cooling costs as well as rack space. A virtual gateway solution from AEP is the new, green way for providing your customers with secure and fully featured enterprise and government remote access.
- ▶ **Scale Quickly.** Spin up as many Series A virtual machines as needed and immediately meet your growth demands without costly and time-consuming hardware deployments.
- ▶ **Highly Secure.** Two-factor authentication, comprehensive endpoint security, role-based application delivery, and much more are available with each user license.

## Securing Client Access to the Cloud

An often neglected part of the cloud is the client side. Encrypted communications, strong authentication and client health checks are just a few of the many measures Series A takes to safeguard the network.

And, traditionally, cloud clients are desktop computers or "thick clients". Why invest money in optimising the data center yet continue to run fat clients? With Series A, companies can continue to use their thick clients and plan a phased migration to thin clients such as Wyse terminals.



## 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.
- Deploy as many virtual machines as needed.
- Scalable and disaster proof: Install multiple instances as individually addressable appliances or cluster them together with a Series A Load Balancer virtual solution for unrivalled scale and redundancy, even across geographically distant areas.
- Detailed user activity reporting (username, IP address, applications accesses, successful/failed logins and more).

## Key Features

- **Seamless Authentication:** Plugs into your existing authentication infrastructure, with support for Active Directory, Novell NDS, LDAP, Open Directory, RADIUS, RSA SecurID, VASCO and PKI.
- **Deep application support:** Terminal Services, VDI, Citrix, Web-based applications, SharePoint, Exchange, ANY TCP-based application, SSL Tunnel capability.
- **Client Machine "Fingerprinting":** 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/Load Balancing:** Scale your infrastructure and ensure access uptime in one or many geographically disbursed data centers.

## Why Series A?

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

## Security

### Security Zone/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 security 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, just add tokens)
- RSA SecurID®
- ActivIdentity™
- Aladdin®
- Client-side certificates with CRL revocation support
- HTML forms-based
- Endpoint Security Suite (Cache Cleaner; Anti-virus, anti-spyware, client source location & OS level checks)
- Configurable session timeouts and
- Periodic Re-authentication
- Session disconnect on demand
- Single login enforcement

### Encryption

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

### Firewall

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

### High Security Options

- FIPS 140-2 Level 4 compliance option
- CESG "Private" compliance

### Continuity and Productivity

- High availability (active/passive)
- Clustering and Geographical Load Balancing for up to 10 AEP appliances through the AEP Load Balancer
- Session persistence (for Windows

## Application Access

### MyDesktop Client PC Access

- Secure, seamless 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

### Browser & O/S Recommendations

- Windows 7/XP/Vista; 64- & 32-bit
  - Microsoft IE 8.x, 7.x, 9.X
  - Mozilla Firefox 3.x
- Macintosh OS X (10.6, 10.5, 10.7)
  - Safari 4.0/3.x, 5.0.x
- Linux Redhat
  - Mozilla Firefox 5, 4

### Thin Clients

- Wyse C50LE (SLED 11)
- HP t5545 (HP Thin Pro OS)

### Tablets

- iPad (SRDS, MyDesktop, RDP)

### Email

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

### Applications

- Windows RDS, Citrix® XenApp™, VDI, Linux/UNIX/X-Windows, Mainframe character mode
- MyDesktop 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

### Activity Reporting

- Detailed user activity reporting

### Management and Reporting

- Push button Configuration Sync of all nodes in a cluster
- Web-based Administration GUI
- Connection management & 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)

## Virtualization

### Configuration

- Integrates with VMware® ESX/ESXi Infrastructure utilizing existing VMware administrative tools
- Integrates easily within enterprise-wide security framework
- Integrates with Citrix XenServer
- Integrates with MS Hyper-V
- Integrates with Red Hat KVM
- Deploy as many virtual machines as needed
- Single virtual machine supports up to 1000 users
- Series A LB virtual load balancer available

### Load Balancing

- Series A LB virtual load balancer available for robust load balancing and traffic distribution among Series A virtual appliances

## Contact us

### United States

Toll-Free: +1-877-638-4552  
Tel: +1-732-652-5200

### Europe

Tel: +44 1344 637 300

### Greater China

Tel: +8621 5116 7120

### SE Asia, Singapore

Tel: +852 2961 4566

### Japan

Tel: +81 3 5979 2149

### Australia/New Zealand

Tel: +61 2 9413 2282

### Malaysia:

Tel: +60 32166 2280

Email: [sales@aepnetworks.com](mailto:sales@aepnetworks.com)

Web: [www.aepnetworks.com](http://www.aepnetworks.com)

## VMware Technology Alliance Partner



## Accreditation

