

AEP's Series A Secure Application Access delivers outstanding performance to thousands of users enabling secure access to any business application in a fully protected environment. Identity-based application access and extensive endpoint security ensures thoroughly validated users only see what they are authorized to see.

### Benefits

- Access, security, authentication and policy all provided within a single platform lowering cost of ownership.
- Extensive endpoint security 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
- Quick installation with no infrastructure changes required
- Icon-driven user interface eliminates end-user retraining

### Security Features

- Identity-based deployment of authorized applications through an icon-driven webtop
- Set access limits and quarantine users based on endpoint security scan
- Application Layer Proxy protection: Shields your network resources from public exposure
- Endpoint Security solution eliminates threats of data leakage
- Device "fingerprinting" with Client Machine Identification (CMID) authorizes only pre-approved PCs
- Configurable session timeouts and periodic re-authentication
- Certified solution: CCTM; FIPS 140-2 Level 4 option
- Reporting and logging helps meet regulatory compliance



### Web Applications and Portals

- Secure access to any Web application, 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-Based Applications

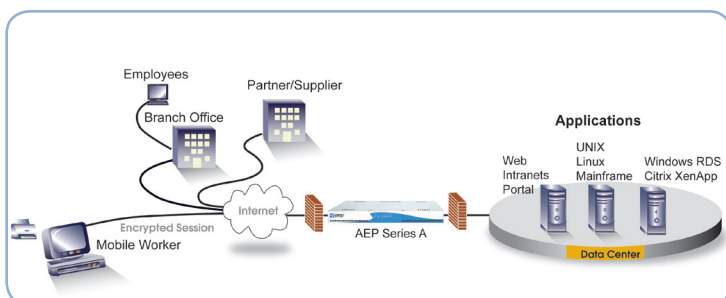
- Identity-driven, web-based access to Citrix, Microsoft® Windows Terminal Servers, UNIX/Linux & Mainframes.
- Drive mapping for seamless interactivity with local & remote data.
- Universal printing option (Windows RDS). No client requirements.
- Session persistence for workflow continuity
- High color for medical and graphic-intensive applications.
- On-demand Microsoft Windows Terminal Server (RDP) and Citrix ICA (Native, ActiveX, Java) client delivery.
- Application server load balancing (Windows RDS).

### MyDesktop Client Desktop Access

- Secure, seamless remote access to individual users' PCs via auto-created access control lists (ACLs)
- Easy to set up: Create one application type that serves all users

### Client/Server Applications

- Network adapter for Layer 3 tunnel connectivity
- Security (encryption) for VoIP applications
- Application adapter for Layer 4-7 connectivity
- On-demand, automatic adapter installation
- Tool Tray and/or local client launchable
- No end user configuration or installation
- Granular policy enforcement



## 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

### 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 (A6500/A8500 only)
- CESSG “Protect” compliance

### Continuity and Productivity

- High availability (active/passive) (not available on A2500)
- Clustering and Geographical Load Balancing for up to 10 AEP appliances through the AEP Load Balancer (not available on A2500)
- Session persistence (for Windows Terminal Servers)

## Application Access

### Browser & O/S Recommendations

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

### Email

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

### Applications

- Windows RDS (Terminal Services), Citrix® XenApp™, 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

## Reporting and Management

### Activity Reporting

- Detailed user activity reporting
- View reports online; have reports emailed at regular intervals
- Export report data (csv, pdf)

### Management and Logging

- Seamless integration: Microsoft Active Directory, LDAP Push button Configuration Sync of all Nodes in a Cluster
- Web-based Administration GUI
- Connection management and display tool
- SNMP and Syslog
- Firewall event monitoring
- Performance and system assurance monitoring
- Role-based administration

## 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

### Capacities

- A2500: 100 concurrent users
- A4500: 500 concurrent users
- A6500: 2,000 concurrent users
- A8500: 10,000 concurrent users

### Power

- A8500
  - Redundant-powered systems available

### OS

64-bit

### Port Specifications

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

### RAID

- A8500/A6500 Only
  - Redundant Dual mirrored SATA hard drive

### Network Requirements

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

## 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: +8180 5645 4503**Australia/New Zealand:** Tel: +61 2 9413 2282**Malaysia:** Tel: +60 32166 2280Email: [sales@aepnetworks.com](mailto:sales@aepnetworks.com)Web: [www.aepnetworks.com](http://www.aepnetworks.com)

## Accreditation

