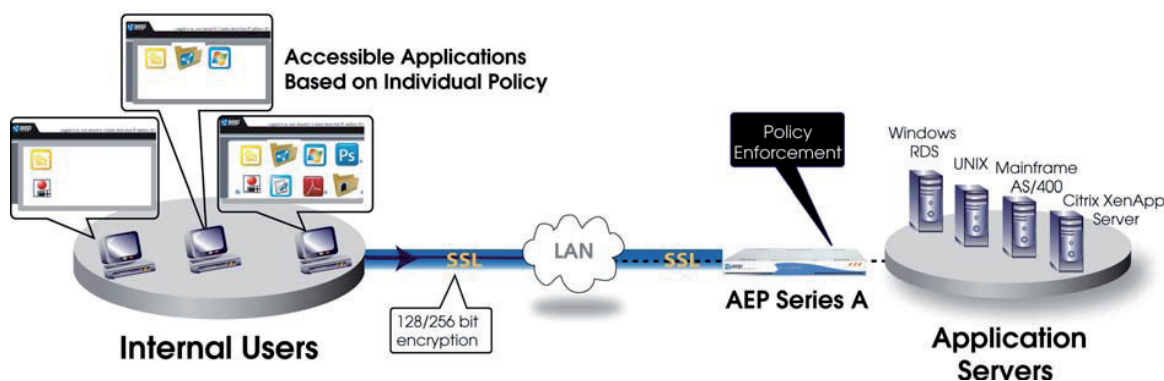


Secure, Controlled Internal Access

AEP Series A Central Access Gateway with Reporting

Concerned about internal network access? Have full control over the applications and services internal users can access, see or even know about. Protect all core assets from un-authorized access. Using AEP Series A's granular access controls, managers can ensure users only access authorised resources via an encrypted session. Each user is presented with an individual icon-driven web portal of only authorised resources such as desktops (whether physical, VDI or RDS-driven) or, to eliminate the risk of users roaming the network, individual applications/file shares.

Track User Activity with Series A Reporting. Produce standard and custom user activity reports (login/logout date and time; applications accessed; source address, and more) for auditing, compliance, and usage measurement reporting. Have reports emailed to you at regular intervals. As a built in feature, there's no need for expensive add ons or third party tools.



Key Capabilities

Fine-Grained Access Controls: Control access to URLs, applications, and data.

Unified Application Access: Central access to all authorized applications regardless of server environment (Windows RDS, Citrix XenApp, Mainframe, and UNIX).

Universal Printing: Users can print documents located on Terminal servers to their local printers. No client requirements.

Central Access Solution: External users can use this same internal solution.

Ease of Use: Familiar, icon-driven webtop delivers a single page for access to various application types.

Easy to Set Up: Web-based administration. Seamless connectivity with authentication and policy servers.

Virtual Appliance available. Choose from a hardware or virtual solution.

Security Features

SSL encryption for secure connections.

Strong, two-factor authentication support (RSA, VASCO—built in server).

Application Layer Proxy— Applications remain safe on the server and are never directly exposed to the public network.

Device Fingerprinting — Limits access to pre-approved client devices.

Layered Authentication — Flexible, V-realm framework combines numerous protocols: RSA SecurID®, LDAP, Windows® NT®, RADIUS, Windows Active Directory, Kerberos, ActivCard (Smart Cards), and more.

FIPS 140-2 Level 4 option — Security at the highest FIPS level.

United States

Toll-Free: +1-877-638-4552

Tel: +1-732-652-5200

Email: sales@aepnetworks.com

Europe

Tel: +44 1344 637 300

Web: www.aepnetworks.com

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 2260