



## Security Centered on Identity

Using the identity of a user or machine to enforce acceptable use policies according to a user's role is known as identity-based access control (IBAC).

If your servers and systems contain confidential personal information, credit card data, health records, account numbers, intellectual property, financial reports, digital identities, or other critical business assets, IBAC can help ensure that users are restricted to specific assets on a "need to know" basis.



## Enforce Policy and Control Access

Protecting the network perimeter or implementing NAC is not enough. Designed for the enterprise, IDpoint is placed in-line in front of sensitive networked application resources/servers as a hardened policy enforcement point. IDpoint enables you to:

- Enforce network layer and application layer access policies and privileges to reduce business risk and prove compliance for the resources that need it most
- Determine user access to protected resources or zones while stopping unauthorized network traffic from getting through
- Leverage existing directory systems for simple network configuration and change management
- Satisfy access control and usage auditing requirements of hypersensitive application (or database) resources

## AEP PacketTag™: Identity in the Data Stream

The IDpoint token inserts a secure, unique cryptographic representation of user identity, called AEP PacketTag™, into every IP packet destined for a protected resource for end-to-end real-time protection.

## Network Segmentation

IDpoint enforces granular identity-based access while eliminating inappropriate viewing of network topology. Protected resources are completely undetectable and invisible to unauthorized users.

- Manage outsourced contractors, partners and guests
- Segment your network and isolate critical resources from exposure - even unauthorized pings are dropped
- Easily build identity-driven security zones to "fence" valuable networked resources

## Auditing & Regulatory Compliance

IDpoint provides proof of all access attempts. With traceable, verifiable user identity in every packet, IDpoint aids reporting and compliance challenges in a manner well beyond less effective network authentication or IP/MAC addressing which may be dynamic or easily spoofed.

- Eliminates manual IP addresses log correlation or costly report consolidation tools
- Identity-correlated management reports show who accessed what critical information resources from where, when and for how long
- Aids compliance to virtually all regulatory guidelines with built-in logging and reporting

## AEP IDpoint Benefits:

### Identity-Driven Resource Access Control

User and group identity are harvested from existing authentication methods and directory data stores without extensions.

### Comprehensive Logging, Reporting and Management

**Central Reporting Server (CRS)** captures policy violations and PacketTag anomalies (user identity, source IP, time of day, policy violation, enforcement steps taken) which are logged as on-screen and exportable reports. Supports SNMP and Syslog.

### Stealth-Mode Policy Enforcement

Undetectable, "transparent" device silently inspects packets at wire-speed across two independent Gb/s enforcement paths (10Gb/s available soon), denying unauthorized traffic and isolating systems from inappropriate access. Enforceable at the network layer by host address, subnet, port, protocol and user identity.

### Zero Network Reconfiguration

Designed without an IP address in the protected path means seamless installation anywhere on the network. Operates independent of routing and switched infrastructure, authentication, firewall, IDS/IPS, IP address topology or other applications.

### AEP PacketTag Identity Injection

Non-refutable digital fingerprint embedded in each IP packet destined for protected resources without impact to other traffic. Works with web reverse proxy, port-forwarder, SSL tunnel and web-files services.

### Remote Access Identity Enforcement

IDpoint provides PacketTag interoperability with AEP Networks' Netilla® SSL VPNs to further extend identity-based access control through the network edge.

### WAN Compatibility

Supports branch-office, off-shoring, or extranet applications through Enhanced grade public sector AEP Net encryptors or any IPsec site-site, MPLS or metro-Ethernet WAN infrastructure.



### Physical Specifications

- 2U rack mount chassis; Height 3.45" (87.6mm), Width 17.4" (435.3mm), Depth 20" (508mm)
- AC Voltage: 100-240 V, 60/50Hz
- Fault-tolerant architecture:
  - Dual 600W redundant power units
- Multiple redundant fan system
  - Hot-swappable dual SAS drives with RAID capability
  - Optional active-passive redundant via VRRP/Ethernet interfact (Active/passive units do not require co-location)

### Authentication / Login support:

- Transparent Microsoft® Windows logon, Kerberos, SMB/Active Directory, RADIUS®/Groups, LDAP (Open LDAP, Novell eDirectory®, IPPlanet)
- Vasco® Digipass (Built-in), RSA SecurID®, ActivCard®, Aladdin®
- Client-side PKI certificates with CRL revocation
- Local, Microsoft Windows Global, and Active Directory / LDAP groups
- Web-based portal login for guests
- Up to 1000 "virtual" realms per appliance
  - Granular authentication and policy groupings (e.g., by department)
- Configurable session timeouts and period re-authentication

### Management and Reporting:

- Integrated web-based graphical interface for policy creation and administration and reporting via Central Reporting Server (CRS)
- Connection management and display tool
- SNMP and syslog output
- Firewall event monitoring
- Automatically generates email alert to administrator in event of failover occurrence
- Performance and system assurance monitoring
- Compliance reporting of user-level access to critical system resources

### Networking

- Two (2) independent wire-speed 1Gb/s Ethernet identity-protected stealth firewall paths
  - » 4 x 1 GbE copper or fiber-optic interface ports (2 input, 2 output)
- Low-latency bump-in-the-wire configuration
- Seamless transparent support for MetroE and WAN connections and site-site VPN configurations
- Dedicated Ethernet management interface port
- Wire-speed, PacketTag™ encrypted identification support for up to 2,500 concurrent authenticated users
- Remote access PacketTag™ integration with AEP Netilla SSL VPN for true end-to-end identity-based protection

### Minimum Client Configuration:

- Microsoft® Windows XP SP2 or Vista
- Administrative rights required for installation; compatible with software distribution tools
- Browser-based download capability

### High Availability

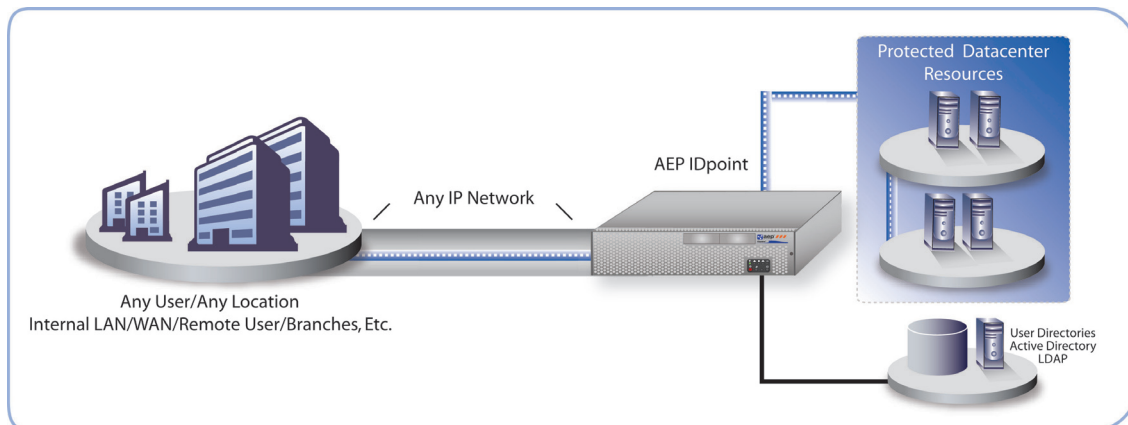
- Two-unit active/passive high availability via VRRP/Ethernet interface

### Compliance

- Payment Card Industry (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Homeland Security Presidential Directive (HSPD-12)
- Gramm-Leach-Bliley Act (GLBA)
- Basel II

### Central Reporting Server - Hardware Requirements

- Memory: 4GB
- CPUs: 2+
  - » Minimum: 2 core Intel CPU at 2Ghz
  - » Recommended: 4 Intel Xeon CPU at 2Ghz
- Network Adapters: 1 (minimum)
- Disks: RAID (recommended)
- VMware® version available



### 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, 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](mailto:sales@aepnetworks.com)

#### Web:

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