AEP NACpoint

Identity-based Network Admission Control Point

AEP NACpoint is a policy-centric Network Admission Control (NAC) appliance designed to secure LAN and wireless-based networks. NACpoint provides endpoint vulnerability assessment, user authentication, device quarantine and remediation for your entire network including:

- Managed end users
- Guest access
- Partner access
- Conference rooms
- Mobile users
- Shared workspaces

NACpoint allows you to:

- Provide isolated guest access while keeping the corporate network safe
- Protect network resources against unmanaged devices infected by other less-secure networks
- Guide end users through self-remediation **before** vulnerabilities spread
- Deploy highly granular access policies - with customizable templates - for quick and automatic enforcement
- Get up and running seamlessly - does not alter existing network configurations or equipment
- Integrate with all leading vendor infrastructure

AEP NACpoint provides a comprehensive data reporting system designed to give insight into:

- End user and device vulnerabilities: OS patches, security product version, malware
- Rogue devices connecting to the network
- Compliance auditing for policy infractions, authentication and user systems access

AEP Networks offers two platforms (AEP NACpoint and AEP NACpoint Small Office) that deliver a cost-effective NAC solution regardless of your organization's size. The AEP NACpoint Small Office platform is ideal as an entry level solution or for small businesses, branch/remote offices, or multiple retail locations.

NACpoint is part of a comprehensive AEP Policy Networking security product suite

Features	Benefits
Granular Policy Engine	• Powerful, highly customizable enforcement based on device health, authentication, location, time of day, Intrusion Prevention System (IPS) output, Operating System, agent presence, or registry configuration
Agentless or Optional Native Agent for vulnerability scans	• Fast pre- and post-connect assessment of AntiVirus, Firewall, OS, Anti-spyware, registry and OS patch levels without ANY additional host software
Multiple Automatic Quarantine Zones	• Isolates infected users for remediation, controlling potential outbreaks from spreading
Identity-based network segmentation	• Separates resources based on user authentication for policy conformance and control
Automatic Vulnerability Updates (via AEP NOCsets)	• Daily updates of vulnerability knowledge ensures administrators are always checking against the latest known threats
Out-of-band operation	• Simplified deployment with minimum network interruption. Operates out of the packet path to maximize security without throughput bottlenecks
Network Flexibility	• Integrates with virtually any Layer 2 or Layer 3 managed switch or WAP to isolate offending ports. 802.1x network configurations are supported but not required for full operation
Detailed, Integrated Reporting Engine with Learning Mode	• Demonstrates immediate value by discovering and auditing any device on the network. Comprehensive executive and detailed reports identify vulnerable users and remediation history. Customizable e-mail alerting on virtually any policy condition or event for integration into automated IT systems

Specifications

Authentication
- 802.1x
- Windows® ActiveDirectory Authentication
- LDAP
- RADIUS
- Web login

Supported Operating Systems (Client Agent)
- Microsoft Windows® XP, Vista
- Mac OS® X
- Others (without client agent)

Platforms
- AEP NACpoint Small Office: 50 managed ports (maximum)
- AEP NACpoint: 100 managed ports (initial configuration), with expansion capability to 2500+ managed ports
- High-Availability active-standby configuration

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

Power Requirements
- AC Voltage: 100-240 V, 50-60Hz
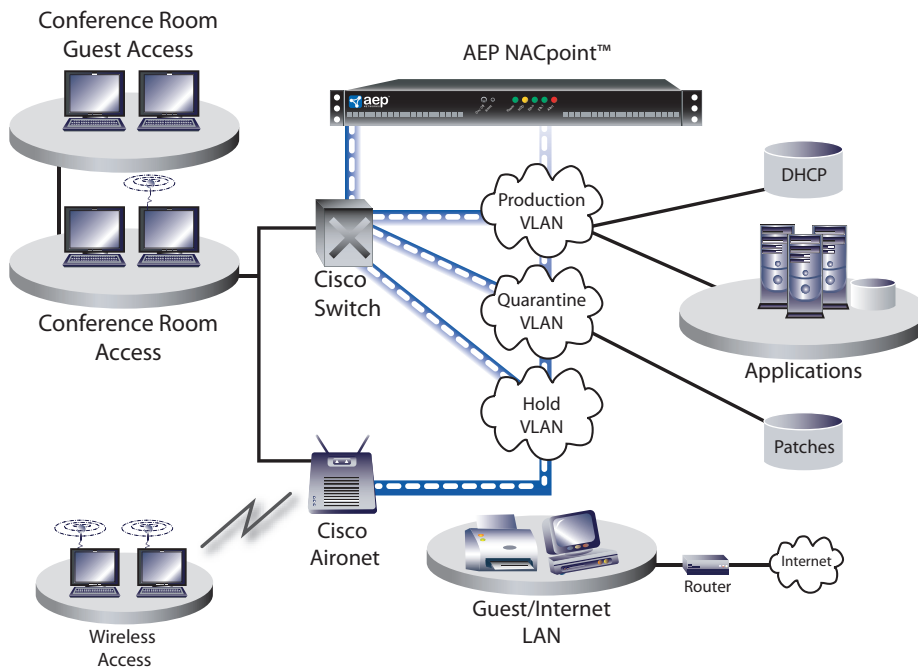- Power Consumption: 500 watts max

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

Sample Switch and WAP Support
- 3Com®
- Alcatel®
- Cisco®
- Enterasys®
- Extreme®
- Foundry®
- HP ProCurve®
- Nortel®
- Allied Telesis
- Hitachi®
- Trapeze®
- Aruba®
- Meru®
- And more!

Architecture

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 hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company is headquartered in Somerset, New Jersey, with offices worldwide.

Contact Us

www.aepnetworks.com

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com