

## LAN security is a major concern for any corporation or organization which posses an IP network



*Access Layer's flagship product, portnox, is a natural extension of existing security policies and methodologies, allowing network administrators to configure access parameters for physical network ports, and proceed to monitor, control, and manage LAN entities, including devices, switches, ports, access slots, and more.*

The traditional approach to LAN security has focused on perimeter security - preventing outside intrusion into the corporate LAN via such solutions as firewalls, authentication mechanisms, etc. These security measures all share a common vulnerability: they all protect the LAN from "outside" the network. Once access has been gained into the network, these measures are no longer effective, leaving the corporate network and its data wide open to breaches and intrusions.

*More recent LAN security developments have attempted to address this problem by providing*

*internal authentication, encryption and validation protocols - all of which rely on such mechanisms as digital certificates and handshakes between end-units, servers and LAN network switches. These solutions are still imperfect, as any number of devices connected to the LAN (for example non win32 systems, printers, time attendance, phones, legacy systems etc.) cannot use such protocols, rendering the LAN security coverage incomplete and vulnerable.*

*The end result of the traditional approach to LAN security is network coverage that is inherently vulnerable: concentrating its efforts on protecting from intrusion from outside the corporate network, while **leaving internal physical access unsecured**, as well as relying on cumbersome authentication mechanisms with implementation requirements that **create potential weaknesses**.*

## *The problems that exist in the world today can not be solved with the thinking methodology that created them...*

### What is portnox™?

portnox represents a new approach to LAN protection, providing complete online control of end-point access to the corporate network. A natural extension of existing security policies and methodologies, portnox allows network administrators to configure access parameters for physical network ports, determining which devices are allowed LAN access by:

- 1| Identifying if devices connected to the network are "part" of the network (a company known device and not a rogue device)
- 2| Insuring that each applicable device complies with the company network access security policy

Unique access rules can be configured for each physical port, allowing for customization based on business requirements mapped on physical locations.

*portnox enables you to monitor switch status, informs you of any violations or access problems, and provides direct switch management & audit capabilities.*

*portnox delivers full control of physical access ports, allowing you to determine which devices have access to your corporate LAN, when and where, and enables you to control port access on an ad-hoc or policy basis.*

*portnox supports a wide variety of regulatory and auditing requirements, including SOX & HIPPA.*

*With portnox, the most vulnerable point in your corporate network, the **physical network switch**, is monitored at all times, providing you with a centralized switch monitoring and management solution that fully protects the corporate network- from "the inside".*

## Key Features

- Multiple switch vendor support
- No Agent installation
- Software only based solution (Patent Pending)
- Directory integration
- Rapid deployment phase
- No network changes required
- No traffic shaping / mirroring / poisoning
- Interoperability - authentication schemes
- Score based authentication(Patent Pending)
- Real time visual NAS interaction
- No MAC address management or X509 computer enrollment (802.1x)
- 100% network port coverage
- Full switch & network auditing capabilities

## With portnox you can

- Receive real-time status information on LAN switches and ports
- Monitor port access attempts and identify the physical location of an attempted breach
- Maintain real-time control of individual ports via the portnox interface
- Know who's accessing the network, where, and when
- Configure access restrictions to different ports by physical location or role association (finance, management, lab, visitor's lounge, helpdesk, etc.)
- Maintain granular network access control at the point where your network begins!

## Portnox Manager / Enforcer Server - System Requirements:

### Software

- **Operating System:**
  - Windows® Server 2003 Standard SP1
- **Database:**
  - Microsoft® SQL 2005
  - Integrated Database
- **Web Server:** Internet Information Services

### Hardware

- Processor 1x2.8 Ghz Intel Pentium® 4 processor
- Memory 1 GB
- Storage 1 x 72 GB (SATA/SCSI)
- Network adaptors - 2 (IEEE 802.1Q support)

## About Access Layers

access layers was founded in 2005, with a vision to respond to the pressing need in the security market for systems that will complement traditional LAN security solutions, and provide the market with true network control and management capabilities.

## Contact Access Layers

33 Ben Gurion St.  
Herzlia, ISRAEL 46785  
Tel: +972-9-9579889  
Fax: +972-9-9579808  
<http://www.accesslayers.com>