NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION

NG INTRUSION DEFENSE NextGen Network Access Control

NACwalls: Protect Networks from the Inside-Out

Why small to medium-sized enterprises need internal security

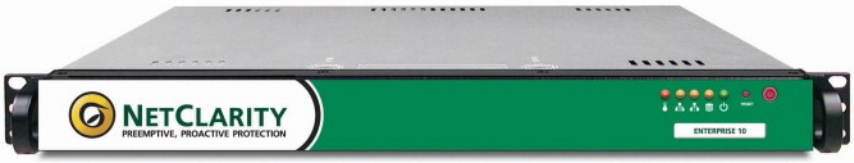
Hackers are targeting smaller businesses

In the early days of the Internet, a firewall and intrusion prevention system was enough to protect your network from hackers. Yet as the threat landscape evolved and the targets of these hackers changed from the large Fortune 1000 companies to small and mid-size businesses, it is no surprise that these external security solutions alone will no longer be enough to defend your network from attack.

Hackers can retrieve sensitive information from a business in many ways, largely stemming from holes in your internal network. Knowing the vulnerabilities that exist on your network as well as the devices, both trusted and not, are the first steps in securing your network from the inside-out. Yet internal security is expensive, and many businesses like yours are struggling to find the best fit to properly secure your networks at the right price and in a simple manner.

"The NACwall Next Generation (NG) Appliance family may very well be the most innovative NAC solution in the world, this year."

InfoSec Products Guide



The New Network Security Dilemma:

- 80% of New Attacks Occurring from the INSIDE (SANS.org)
- External Firewalls have made their way to SMB/SOHO, but not effective internal security
- AntiVirus is NOT enough; 60-90% effective (www.virusbtn.com)
  - And, what about the window before new malware identified?
- How do they know who is REALLY on their network?
- Bring Your Own Device (BYOD) introducing new demands/concerns for controlled access
- "The Smaller You Are, The Harder You Fall" - Breaches are a big deal to a large corporation, but can be devastating for SMB (brand, $$, etc.)

NetClarity NACwall – Protecting Networks from the Inside Out:

- Asset Identification/Classification in an **Agentless Architecture**
  - Trust/Untrusted List
  - Disable Rogue Devices
  - Bring Your Own Device (BYOD), Gas Pumps, to Barcode Scanners to VoiP Phones, Androids, Blackberries, iPads, iPhones to Desktops, Laptops, Netbooks and Critical Servers
- Zero-Day Malware Detection/Protection
- OS Fingerprinting
- Common Vulnerability and Exposure (CVE) Detection
- Compliance Reporting (PCI, HIPAA, GLBA, SOX, etc.)

Customer Benefits:

- Best Price Performance for a Multi-Faceted Internal Security Appliance
  - Smallest Model (Nano25) Can Protect 25 Assets for a low cost.
- Far beyond a simple Network Access Control (NAC) solution, NACwall is a suite of network security solutions included in a single SKU, priced for the SMB
- Ideal for Bring Your Own Device (BYOD) controlled access
- This type of security was previously only available to larger corporations
  - NACwall is "disruptive innovation" that now brings powerful internal security to the SMB space

Risk = Threats x Vulnerabilities x Assets

NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION

NACwalls: Manage Internal Risk

NG INTRUSION DEFENSE NextGen Network Access Control

ASSET DISCOVERY

Network Assets are discovered using Agentless NAC technology.

- Who's on the network?
- Baseline for building the trust list
- Activate easy-NAC blocking engine

ASSET ANALYSIS

Each asset, both wired and wireless, can be analyzed without the installation of agents or clients. Key information is obtained to make:

- Network access decisions
- Vulnerability assessments

ENDPOINT PROTECTION / MALWARE PROTECTION

Each asset is monitored for zero-day malware.

- Non-intrusive
- Looking for call-back URLs
- IT manager determines actions

ENDPOINT PROTECTION – Common Vulnerabilities and Exposures (CVE) AUDITING

Assets (or the entire network) can be audited to:

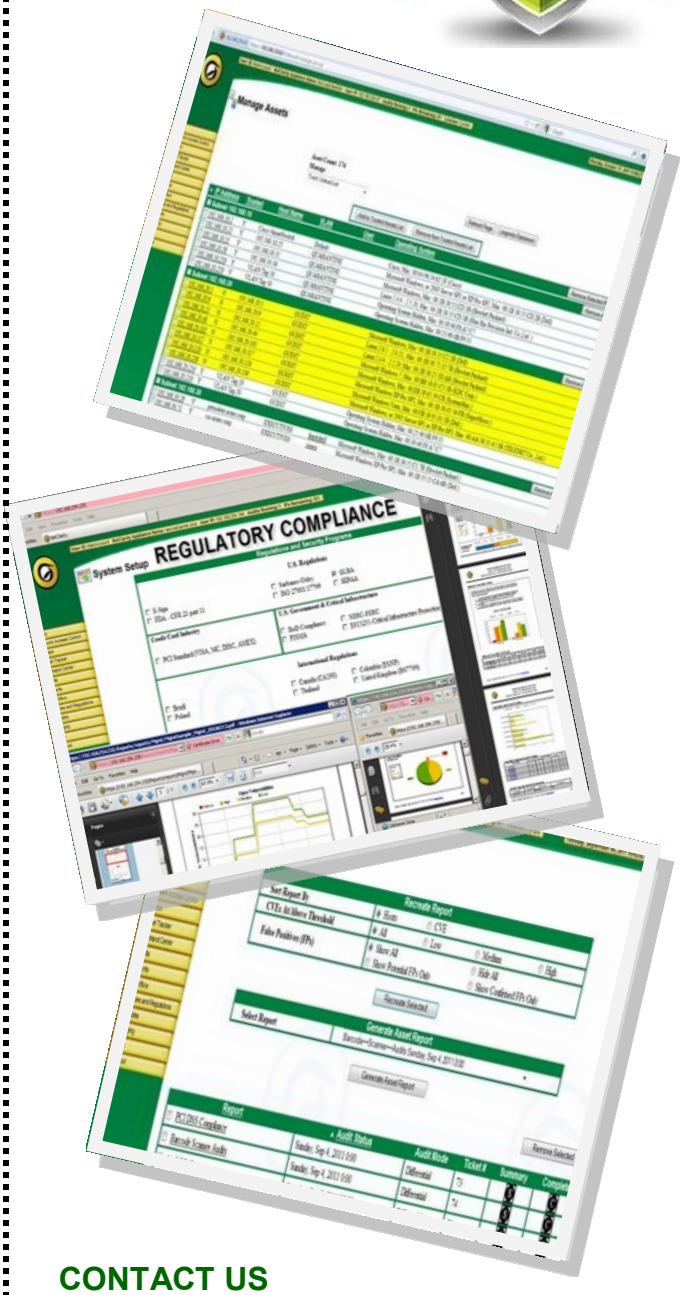
- Make access decisions and identify network trends
- Assess vulnerabilities

COMPLIANCE REPORTING

- **Audit** yourself with NACwall's built-in CVE® certified vulnerability scanning and management system.
- **Report** using over a dozen different reports including Differential and Trend Analysis reports.
- **Comply** with GLBA, HIPAA, Visa PCI, NERC/FERC and many other U.S. and international regulations.

SUBSCRIPTION SERVICES

- **Threat Service:** Zero-day malware heuristics updates are updated several times per day.
- **Vulnerability Service:** Common Vulnerabilities and Exposures (CVE) tests are updated daily.
- **Assets Fingerprint Service:** Network Asset signatures are updated as necessary to help control access and identify newly manufactured IP devices.
- **Firmware Update Service:** Provides firmware updates for new features and bug fixes.



CONTACT US

Visit: http://www.netclarity.net

Toll Free: 1-800-874-2133 (USA) or

International: +1-781-791-9491

Email: sales@netclarity.net

NetClarity, Inc.

Crosby Corporate Center

34 Crosby Drive

Bedford, MA, USA 01730

Or call your Partner Symtrex Inc - 866-431-8972/sales@symtrex.com