

## Complying with PCI Data Security Standard using NetClarity's NACwall NextGen Appliance

The Payment Card Industry (PCI) Data Security Standard (DSS) is designed to pressure retailers and merchant card service providers to maintain higher integrity in their IT security posture. With more consumers making purchases over the internet and telephone, security has become a key concern for the credit card processing industry.

The PCI DSS requires that retailers and related service providers:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement effective access control measures
- Regularly monitor and test networks
- Maintain an information security policy



Although building and maintaining a secure network seems as easy as deploying a firewall, tokens, single sign-on and anti-virus, it's actually become more complex than that. With the pervasive nature of PDAs, internet-enabled cell phones, netbooks and laptops, it's become extremely difficult to track and control internal network access. In addition, there are thousands of common vulnerabilities and exposures (CVEs) also known as exploitable "holes" in all networking equipment and devices from blackberry phones to droids, iphones, itouches, wireless routers, firewalls, desktops, laptops and servers.

To better comply with PCI DSS, you can use your NACwall appliance to:

- Build and maintain a secure network  
by protecting the internal network from rogue devices and malicious insiders.
- Protect cardholder data  
by using it to audit all payment gateway touchpoints, shopping cart software and database systems for their known CVEs and use the workflow engine to track your remediation and system hardening of these critical network assets.
- Maintain a vulnerability management program by using the built-in CVE differential auditing engine, reporting system and workflow engine.
- Implement effective access control measures by locking down your internal 'trust' list of users and trusted assets.
- Regularly monitor and test networks  
by running a SYSLOG server to obtain over 105 PCI compliant syslog traps from the appliance
- Maintain an information security policy By  
using the built-in ISO27001 policy tool

Ultimately, you can guard against data breaches and document PCI compliance using the NACwall NG appliance. For a real world example, read on to learn about the largest PCI breach in history and how it could have been prevented using the NACwall NG appliance.

The largest PCI breach in history was TJMAXX. It cost them \$200M+ to remediate the personally identifiable information (PII) data loss on over 100M consumers credit cards/profiles.

The breach was done by a hacker who sat in the parking lot, hacked the wireless router's (WIFI HACKING) common vulnerabilities and exposures (CVEs), spoofed a trusted asset (MAC SPOOFING), pretending to be a 'wiress barcode scanner' that was a trusted device, and then found the database server that connected to the Visa payment gateway and installed 'eavesdropping' software (PLANTING A BACKDOOR) to watch every credit card transaction that phoned home.

So the PCI compliance breach was:

1. WIFI HACKING
2. MAC SPOOFING
3. EXPLOITING CVEs
4. PLANTING BACKDOOR
5. PHONING HOME



The solution to this problem is:

1. NACwall EasyNAC blocking protection for WIFI against HACKING
  - a. No untrusted asset gains access to wifi
  - b. Even a WEPcrack, KISMET or BACKTRACK 4.0 (WPA) exploit attack is blocked.
2. NACwall MAC spoof protection should be enabled.
3. NACwall should be auditing all devices for their CVEs
4. Backdoors can't be planted if there is no access allowed and there are no CVEs to exploit
5. NACwall's Malware Quarantine engine should be enabled to block callbacks ie 'phoning home'.

This should take about 30-60 minutes to setup at a single location or using the command center to replicate these rules to all branch locations, automatically.

Problem Solved. PCI Breach Avoided.