# NG NAC WHITEPAPER

**Learn about Next Generation (NG) NAC....Available Now in NACwalls NG Appliances.**

It's more than another NAC solution, it's a NAC revolution.
At 1/4th the price of first generation (1G) NAC solutions
with deployment speeds up to 100x faster than 1G solutions.

January 2012




NetClarity, Inc. Crosby Corporate Center, 34 Crosby Drive, Bedford, MA USA 01730

USA/Toll Free: 1-800-874-2133 International: +1-781-791-9497 Email: sales@netclarity.net Web: www.netclarity.net

# Contents

# Today's IT Network Security Challenges

According to US-CERT (United States Computer Emergency Readiness Team), 95% of downtime and IT related compliance issues are a direct result of an exploit against a Common Vulnerability and Exposure. A firewall, IDS, IPS, anti-virus software and other countermeasures don't look for or show how to remove CVEs. ***So most companies are really only 5% secure.***

Most IT managers are not familiar with the term CVE, but the majority are aware of Blaster, Msblast, LovSAN and the Nachi and Welchia; worms which have caused massive downtime and financial losses. They all exploited one CVE – one minor hole. It was a software flaw running in most Microsoft Windows operating systems. This allowed hackers to send these exploits out and take advantage of the many Windows systems that had the fatal flaw.

On the U.S. National Vulnerability Database powered by CVE at http://nvd.nist.gov, it is possible to search for CVEs that may lurk in a network. If an organization has just purchased a new router or switch, or anything else that plugs into a network, it is a simple matter of typing the name of the system into the NVD and seeing how many CVEs (vulnerabilities) can be found.

The top 20 exploited vulnerabilities are available on http://www.sans.org/top20/ which lists ten vulnerabilities in Windows and ten in Unix/Linux systems. If any computer user has one of these holes, it needs to be closed as soon as possible to ensure the installation isn't attacked when least expected. ***In addition, more than 80% of these security breaches happen behind the firewall*** and on systems running the latest anti-virus software.

| Threat | Likelihood of occurrence | Trend | Business Impact $ | Historical IT Investment | Threat Aligned IT Investment |
|---|---|---|---|---|---|
| Traditional Viruses | HIGH | Flat | LOW | HIGH | LOW |
| Denial of Service and Traffic-based Attacks | MEDIUM | Growing slowly | MEDIUM | MEDIUM | LOW |
| Data Theft | MEDIUM | Growing Rapidly | MEDIUM | MEDIUM | MEDIUM |
| New Malware | LOW | Growing Exponentially | HIGH | LOW | HIGH |
| Vulnerability behind the firewall | LOW | Growing Exponentially | VERY HIGH | LOWER | HIGH |
| Malicious insiders or infected trusted users behind the corporate firewall | LOW | Growing Exponentially | SEVERE | VERY LOW | HIGH |

**Figure 1: Today's Threats, Trends and Business Impact**

There is a catastrophic impact upon business operations resulting from these attacks that occur behind firewalls. In addition, these types of attacks is growing exponentially – from guest and unmanageable devices stealing inside information and identities to internal propagation of zero-day malware, some of which, such as Stuxnet, are designed to cause physical damage, as well.

## *It's All About Risk*

Ultimately, you need to manage your risk posture. First, let's understand the risk formula:

# Risk = Threats x Vulnerabilities x Assets (R = T x V x A)

You will never be 100% secure but if you can manage risk, you'll be one step ahead of the problem.

Now, let's breakdown the formula:

**T**hreats - Zero-day malware, Untrusted and Rogue Access, Malicious Insiders.

**V**ulnerabilities - Known as Common Vulnerabilities and Exposures (CVEs) are all the exploitable "holes" in your network

**A**ssets - All dynamic, moving targets - people and their desktops, laptops, voip phones, PDAs found throughout your network

Hackers, viruses and worms cause Billions in damages by exploiting CVEs against business and the damages are growing annually (Source: CSO Magazine). How many CVEs are in a company's network? Is the risk of an internal breach, downtime and data theft taking you out of compliance?

Take a look at PrivacyRights.org and see for yourself – data breaches are accelerating at an incredible pace, yet billions of dollars have been spent on Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Anti-virus Software (AVS). It's been argued in CIO magazine that we've placed our largest investments and trust for network security in products that solve yesterday's problems. What about today and tomorrow?

## The Right Solution

Here is what customers around the globe are saying they want their NAC solution to do:

1. Know who is on my network;
2. Do they belong on my network;
3. When are they on my network;
4. If I don't trust them, I want an alert and I want them off my network instantly;
5. If I do trust them but they are exploitable or have running malware, I want to quarantine them immediately;


6. I want to remediate problems by hardening systems I trust and block those I don't;
7. I want to document and demonstrate regulatory compliance (for GLBA, HIPAA, SOX, FISMA, EO13231, PCI, NERC/FERC, etc.)

*These needs cannot be solved by 9 out of 10 NAC solutions.* Customers want a solution that manages risk on what most NAC vendors call "unmanageable devices" such as Blackberry devices, iPhones, iTouches, Androids, VoIP phones, Wireless barcode scanners, wireless routers and so much more. Most networks are 'alive' – they are very dynamic in nature. NAC needs to intelligently fingerprint every device that comes and goes on networks and helps IT staff manage these devices as well as user access and user behavior.

In addition, at the brick and mortar retail outlets, by spoofing the MAC address of a trusted device – one of the many wireless barcode scanners, one can continue to gain inside access into their network without ever stepping foot into the building.

## Why 1G NAC Didn't Work

The first generation of NAC was designed as an additional and complex layer of network management requiring forklift replacements of managed switches for new 802.1x switches. It was too cumbersome, too difficult to deploy and way too expensive – costing millions of dollars on single deployments.

Remember buying your first cellular telephone? Most likely it was not a first generation 1G cell phone. Very few could afford the first round of cell phones – usually only the wealthy had these installed in their cars with hefty boxes containing batteries and cabling connections to a fixed antenna mounted on their cars. These 1G cell phones were simply not practical for most of us. The same holds true for Network Access Control (NAC).

Market leaders of 1G NAC solutions admit that "deploying NAC is a complex, difficult, challenging, time consuming process requiring 'forklift' upgrades of smart switches, removal of wireless routers and unmanaged hubs and installation of software agents." They admit this and both Gartner and Forrester research analysts have confirmed it. They tell you that you need a 'trust' agent, that you need an 802.1x compatible switch infrastructure, that you need LDAP and Active Directory integration and RADIUS servers and complete network infrastructure reconfiguration to deploy Network Access Control (NAC), properly. [1] They tell you that the trust agent should do three seemingly important health checks:

[1] Source: IDC Enterprise NAC Survey: The Dynamic and Evolving Scope of NAC in the Enterprise - Gerry Pintal Charles J. Kolodgy Jon Crotty.

1. Windows Patch Level
2. Anti-virus Client Status Check
3. Windows Firewall Check

Any system (Desktop, Server, Laptop) that fails these posture checks goes into the 'quarantine' via a NAC proxy server and 802.1x protocol controls. Try this on one of your executives – run one of these solutions on their laptop and watch them sit there unproductive for an hour or two while these useless client software tools help you feel like you've done the right thing for Network Access Control (NAC). Over 30% of all computers in the world are infected with unknown malware, despite having passed these three checks.

How will you install a NAC agent on your VoiP phones, Wireless Routers, Hubs, iPhones and other devices? NAC agents are designed for only ½ of your network – your weak, already infected Windows® systems. If you truly want to control access, you need to solve all of these problems and ensure that rogue assets are not on your network today and are never allowed to gain access to your network in the future (see: www.netclarity.net).

Just take a look at the chart below and you'll see that conventional antivirus checks are absolutely NOT effective against threats that exploit common vulnerabilities and exposures (CVEs), known as Zero-day malware:

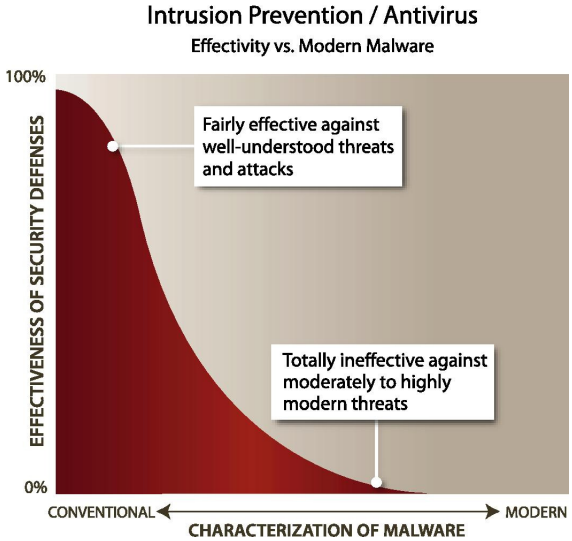


**Figure 2: Anti-virus is totally ineffective against moderately to high modern threats[2]**

[2] Source: ModernMalwareExposed.org.

Given the fact that First Generation (1G) NAC solutions were: inline, complex, required forklift managed switch upgrades to the extremely hackable 802.1x protocol, take months to deploy and were very expensive, no wonder so few deployments happened over the past few years. They could not solve the problems encountered at wireless routers as well as hot-ethernet ports, unmanaged switches, hubs and network-enabled devices such as Blackberry's, iPhones, Droids and other PDAs that do not support 'trust' agents, required by the 802.1x authentication methodologies in 1G NAC.

Just take a look at the following charts. Figure 3 depicts the percentage of your IT Security budget that a 1G NAC solution would require – way more than you have available. The second, Figure 4, shows you how easily a NG NAC solution fits into your budget. The timing couldn't be better to make a NAC investment – as long as it's in a NG NAC solution, not a clunky, costly, complex 1G NAC solution.

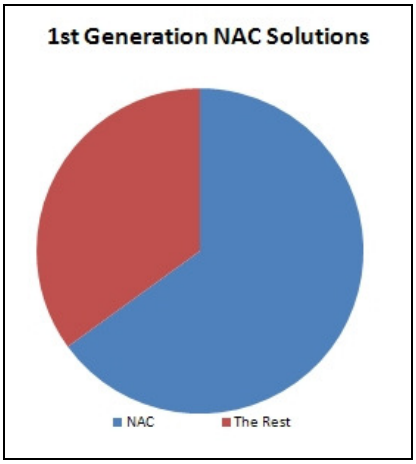


**Figure 3: No wonder why you didn't deploy 1G NAC – It would take 60% of Your IT Security Budget**

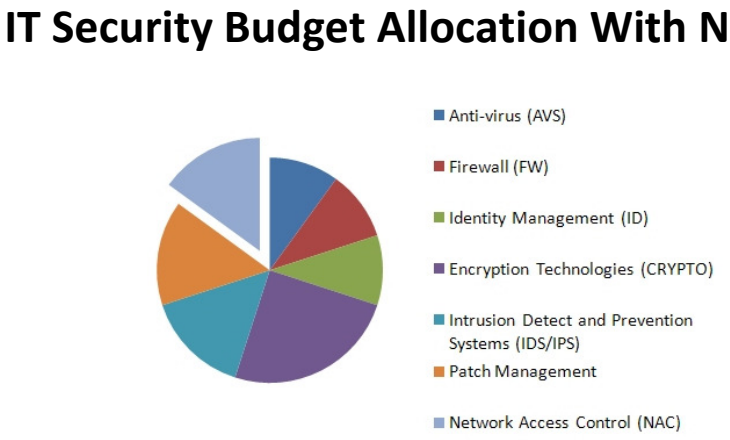


**Figure 4: IT Security Budget Allocation Considering Low Cost of NG NAC and High Performance**

**What is wrong with your current IT Security budget?**

You've probably already allocated most of your budget to deal with last year's threat. If you look at the chart above, you can see why you are missing out on the biggest risk facing your organization – trusted or un-trusted access behind the firewall bringing in New Malware or trusted systems behind the firewall that are extremely vulnerable with many critical holes that are easily exploitable.

However, not deploying NAC in 2011 is NOT an option (unless you want to be exploited). Given the fact that exploits and attacks inside the firewall are increasing at an exponential rate, now is the time to deploy a strong intrusion defense solution for the inside of your networks, behind your firewalls.

Based on the new threat profile, where exploits are new are coming in from behind the firewall on many devices, you'll need to take a new approach to IT Security Budget allocation.

So many devices now have TCP/IP 'internet' capabilities – some easily manageable and many 'unmanaged' such as VoIP phones, iPhones, Blackberry devices, wireless routers, rogue laptops, etc., you will need to reallocate some of your IT Security Budget towards dealing with these higher risk threats.

The good news is that NG NAC products are designed to handle these problems in a way that is cost-effective and easily managed, just in time to rethink your IT Security Budget for 2011.

# Key Compliance and Best Practices Issues

Each market has similar compliance issues – to ensure best practices are in place to protect confidential data – from Financial Services to Health Care, the compliance mandates are real, with serious negative financial consequences and lost brand or the cherished 'trust' image for those that are breached, as we've seen in PrivacyRights.org.

## *Financial Services*

These organizations deal with the flow of money. Whether it is a bank, mortgage lender, credit union or Wall Street market-maker, they all share a common need for strong internal controls, consistently managing and documenting their risk. With regulations from the SEC, FTC, OCC, FDIC and NCUA such as SOX or GLBA, a data breach can be very costly.

## *Utilities, Transportation and Government*

Critical infrastructure such as a Power Grid or a Railroad System or a Missle Defense Agency all share one thing in common – fear that as they move SCADA systems to TCP/IP protocols, the


next Stuxnet worm might target them, causing catastrophes that take human life. There are government mandates and regulation such as EO13231, FISMA and NERC/FERC which require stronger internal intrusion defense and IT compliance.

## *Retail*

Some of the biggest "paydays" for cyber criminals have been their successful breaches in the Retail market, gaining access to hundreds of millions of credit cards through cyber "identity theft" and hacking into merchant payment gateways and e-tailer shopping cart systems. In the brick and mortar side, branch offices are prone to localized attacks where hackers leverage wireless routers put in place for bar code scanner devices and wireless cash registers. This requires stronger centralized control and internal protection of payment gateway networks for PCI compliance.

## *Health Care*

With so many providers collecting and storing extremely confidential and sensitive patient data and medical records, this industry is 'ripe' for the pickings. Recently, hackers were able to exploit a vulnerability in a hospital network and changed the lab results on cancer tests, which would have in turn caused patients to take on chemotherapy treatments, when they actually tested negative for cancer. One simple flip of a bit in a database and a person's life is in jeopardy. Health care organizations need much stronger internal controls and data protection for HIPAA compliance.

## *Education*

It turns out that student and teacher productivity in the education sector is directly correlated to internal student hacker attacks. Some student hackers have changed their grades in the school databases while others used the school wireless router to initiate SKYPE chat sessions and cheat on tests by asking friends for the answers. In addition, Educational organizations are a major target for zero-day malware. With so many students using USB sticks, peer-to-peer file sharing services and installing illegal audio, video and other software, they become internally trusted but infected points of malware propagation. These organizations need to keep students and teachers safe, focused and productive while protecting confidential records, blocking these new approaches to cheating on exams and keeping the malware off their networks.


## Managing the Unmanageable Devices

The first generation (1G) NAC solutions were not aware of, nor could they manage and control access, to the dozens of new devices from VoiP phones to blackberry, iPod, iTouch, iPhone, Droid and other devices. As a result, with the dynamic nature of networks, more and more of these devices have been able to gain access as internally 'trusted' and 'unmanageable' devices, behind firewalls and wireless routers. There's a strong, growing need to detect, alert, block and control these devices without software clients or agents and it must be done in real-time. The only answer is NG NAC.

## What is NG NAC and Why is it Better

Next Generation (NG) NAC....It's more than another NAC solution, it's a ***NAC revolution***. Similar to the advances in Cellular Telephone technology, 1G Cell phones were bulky, expensive, rarely deployed until the advent of NG Cell phones. The same holds true for Network Access Control.

At 1/4th the price of first generation (1G) NAC solutions with deployment speeds up to 100x faster than 1G, you should be looking for a NG solution in 2011. The first NG solution in the NAC market is the NetClarity NACwall NG - providing real-time internal network access control (NAC) and intrusion defense without clients, without software agents. It is now available, worldwide, from trusted NetClarity channel partners. NetClarity intends to continue to push the innovation envelope on what a NAC solution should do to secure networks internally and help customers document their best practices for regulatory compliance.

### *Goals of NG NAC*

Because NAC represents an emerging category of security products, its definition is both evolving and controversial. The overarching goals of the concept can be distilled to:

#### Mitigation of Zero-day Attacks and Vulnerabilities

The key value proposition of NG NAC solutions is the ability to prevent weak or infected trusted devices from accessing the network and placing other computers at risk of cross-contamination of network worms. NG NAC enables automated, real-time quarantine of trusted assets that become weak and infected. You can find and fix your Common Vulnerabilities and Exposures (CVEs), hardening your network assets and preempting successful exploitation of holes.

## Policy enforcement using 802.1q VLANs

NG NAC solutions allow IT staff to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them automatically in all old and new unmanaged and managed switches that support the safer, more stable protocol of 802.1q as opposed to the easily hacked and circumvented 802.1x.

## Identity and access management

Where conventional IP networks enforce access policies in terms of IP addresses, NG NAC solutions support authenticated user identities, agentlessly communicating with Active Directory services, but don't place the trust and reliance upon client/agent-based services, like 1G NAC solutions. Criminals don't install trust agents and don't authenticate when they choose.

## *NG NAC is a Convergence*

Imagine three key areas: Identity Management, Device Security and Network Security. This is where NG NAC takes us. By focusing on the convergence of these three unique and distinct areas of corporate security, a NG NAC solution handles internal intrusion defense – where most IT Security and Regulatory Compliance issues arise, nearly automatically and in real-time. Take a look at the Venn diagram, below, for a visual understanding of where NG NAC fits:

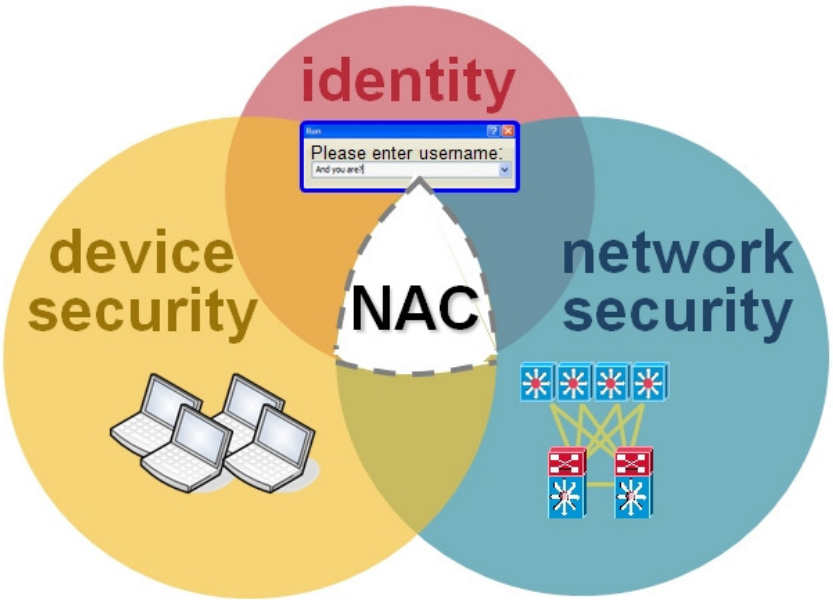


**Figure 5: NG NAC – the Convergence of Internal Intrusion Defense**


As network attackers have moved on to new threats constituting the majority of today's risk - and requiring new protection technologies (i.e. Network Asset "Cops") or NAC solutions that converge device security, network security and identity management. Firewalls can't do this and 1G NAC products cannot do this, either.

Critically telling of this evolution, Network Traffic "Cops" and 1G NAC solutions are unable to answer the new ABC's of Network Security:

A: Who is on my network?

B: Can I block those who don't belong on my network?

C: Can I find and correct hidden flaws and weaknesses in my most important network assets?

This is where 95% of the network threats now exist. So you'll need a NG NAC solution that provides intrusion defense for network security, improved availability, employee productivity and regulatory compliance.

Consider NACwall NG – the world's first NG NAC solution – hardware appliances that are customer controlled, non-inline, agent-less (or client-less), does not use the failed and flawed 802.1x protocol (over 60,000 links in google for hacking 802.1x) and work to protect all devices, network assets and users.

> *"We've been watching NetClarity for some time.*
>
> *In our view, this company is among the most innovative we've seen."*
>
> SC Magazine

NetClarity is the NG NAC market leader and innovator, launching the patented NACwall NG appliances into the marketplace beginning in the first quarter of 2011. With these appliances, you'll be able to automatically detect who is attempting to connect to your network. This is the solution of choice to handle both trusted and untrusted or unauthorized 'rogue' access across any device such as Blackberry, iPhone, Wireless Routers or using the switch port of a trusted VoIP device.

Unlike 1G NAC solutions, NACwall NG won't break when you put a low cost hub on the network, (an "unmanaged switch") and attack your peers. Many hackers have been able to circumvent most, if not all 1G NAC products by attacking peers on hubs, which are unknown to 1G NAC products because they are not manageable in the 802.1x protocol or through secure tunnels and command line interfaces.

## *NACwall NG Appliances are NG NAC Enabled*

NACwall NG appliances are typically 1/4th the price of first generation (1G) NAC solutions with deployment speeds up to 100x faster than 1G NAC. They provide real-time internal network access control (NAC) and intrusion defense without clients, without software agents. Available from NetClarity channel partners worldwide.

NetClarity, Inc. is a USA company, manufacturing in the USA and offers these appliances into the marketplace as the only NG NAC solution that is both non-inline and agent less and does not require 802.1x. With the right NG NAC solution, such as NACwalls from NetClarity, you'll be able to defend your organization from unexpected threats, untrusted network access, known vulnerabilities and their exploits. NACwall NG appliances function while you are at work and even while you are sleeping. It is completely automatic and easy to use; the same way a NG cell phone was adopted by everyone. No need for complex training to perform these key functions and defeat 'rogue' access, malicious insiders and new malware.


**Figure 6: The NACwall NG Enterprise 10**

## *Contacting NetClarity*

Send us an email to sales@netclarity.net or
Find us online at http://www.netclarity.net

***Corporate Headquarters***
Crosby Corporate Center
34 Crosby Drive
Bedford, MA 01730
United States of America
(781) 791-9497

SC MAGAZINE BEST BUY