

NAC Enforcement and the Role of the Client

February 2007





Copyright © 2007 by Infonetics Research, Inc.

Entire contents copyrighted by Infonetics Research, Inc. Unauthorized redistribution, electronic or otherwise, without prior written approval of Infonetics Research, Inc., is prohibited by law. Requests for permission to copy or distribute should be made to Infonetics Research, Inc.

Table of Contents

I.	The Promise of NAC	1
II.	NAC Architecture	4
III.	NAC Enforcement	6
	1. Client Enforcement	7
	2. Network Integrated NAC Enforcement	8
	3. NAC Enforcement Appliances.....	8
IV.	The Role of the Client	9
	1. Clientless NAC	9
	2. Informational Clients.....	10
	3. Enforcing Clients.....	10
V.	Where Clientless NAC Shines	11
	1. Ease of Deployment and Scalability.....	11
	2. Guest and Contractor Access	12
	3. Access from Non-Standard Devices.....	12
VI.	Conclusion	13

List of Exhibits

Exhibit 1	Security Deployment Drivers	2
Exhibit 2	NAC Deployment Plans	3
Exhibit 3	NAC Overview	4
Exhibit 4	NAC Enforcement Architecture	6
Exhibit 5	Network-Based NAC Enforcement Architecture	7

I. The Promise of NAC

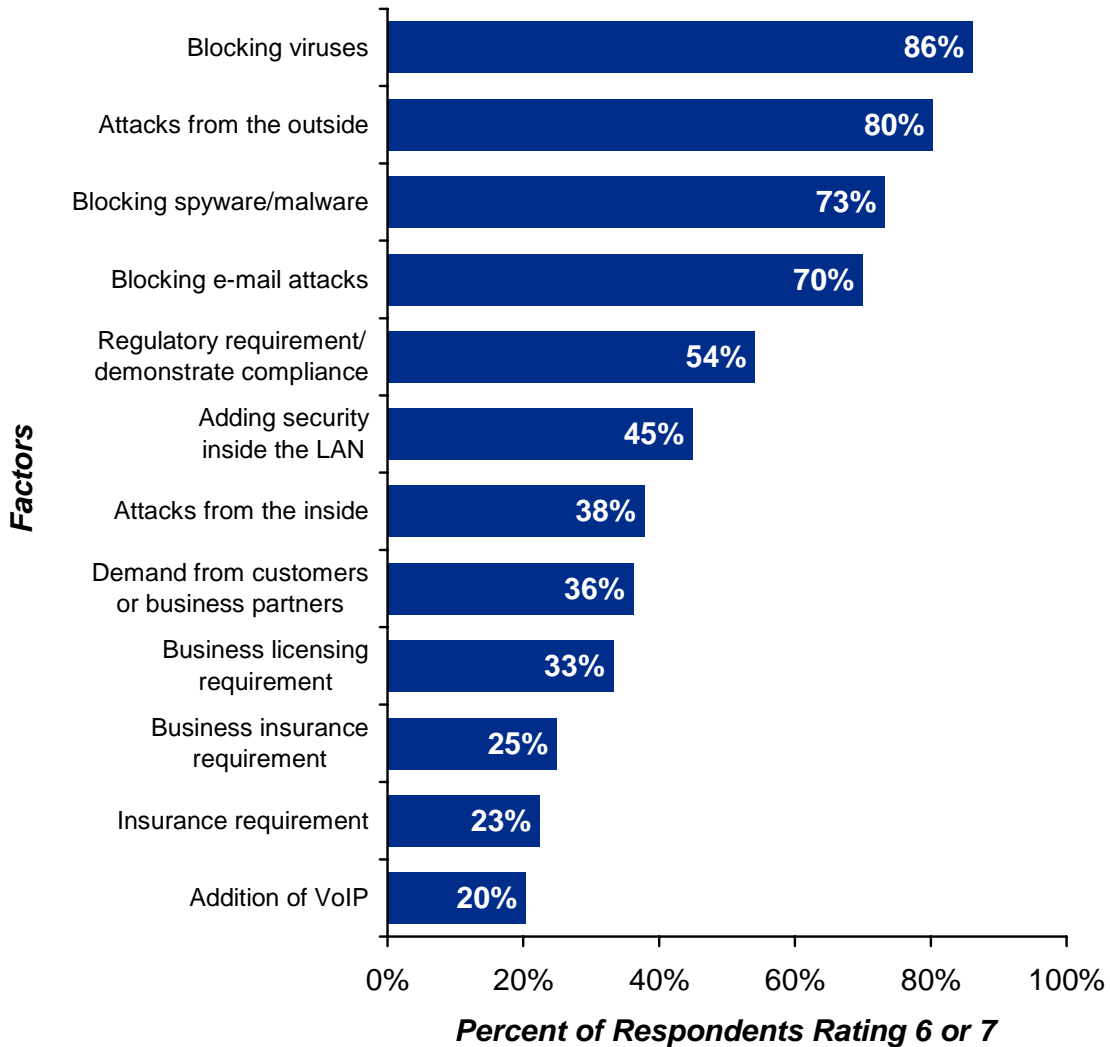
Protecting the average corporate network from attacks is incredibly complicated and expensive. By the mid 1990s, complex toolkits had been supplanted by pre-built firewall software packages and intrusion detection systems. As performance and usability requirements increased, software moved to hardware, and by 2000, the number of companies buying and deploying perimeter security skyrocketed. Features were integrated, costs came down, and technologies improved; today you can buy a top-of-the-line, stateful-inspection firewall at the local home electronics store. So has security technology innovation stopped? Are there no longer threats?

Year after year the CSI/FBI Computer Crime Survey shows that organizations experience roughly equal numbers of external and internal attacks. Yet the makers of early network security products largely ignored threats from the inside, because there were no easy, product-based solutions. Instead, they targeted the boundary between the corporate LAN and the Internet, because they could build products to do that, and because this was the most obvious point at which to defend against attacks from the outside. Now, thanks to distributed Internet connectivity, VPNs, wireless technology, network-connected PDAs, and extranets, most large enterprise networks no longer have borders. While this increase in connectivity is great for employee productivity, it is a security nightmare.

On top of real security threats, the current operating environment for the IT shop at many organizations is becoming hostile due to the requirement to demonstrate compliance (for regulatory purposes, business license acquisition and renewal, business insurance, and a host of other reasons). Companies no longer just need to be secure to protect their assets and business, they need to demonstrate that security on an ongoing basis to a third party or face stiff penalties.

In our recent survey of 240 organizations in North America (*User Plans for Network Security: North America 2006*), we asked about drivers for deploying new security products and technologies. Stopping a host of content-related attacks takes the top four slots, and the need to demonstrate compliance takes the fifth. These are real problems, and companies of all sizes are looking for real solutions.

Exhibit 1 Security Deployment Drivers



Source: User Plans for Security Products and Services: North America 2006 (*Infonetics Research*)

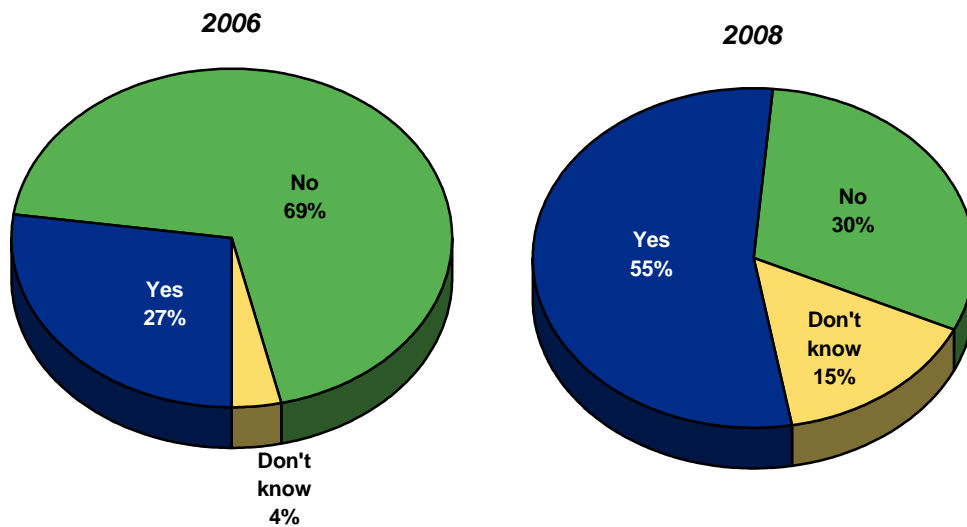
For the last three years there has been much talk about network access control (NAC), an intelligent network infrastructure that can identify users, identify and do integrity checks on the computers they are using, and grant them conditional access to specific locations or resources (and set policies). This is the holy grail of

access control, and is no simple feat, as it will impact all types of products, including client software, security appliances, network infrastructure, and the backend (authentication and policy databases, etc.). Increasingly the NAC definition is expanding to include not just posture checks, but scans of current system health, as well as post admission security, such as doing intrusion detection and prevention once clients pass the screening process.

From the perspective of the mass market security buyer, we are in the early stages of the NAC market; there are many vendors offering NAC solutions, but the solutions they're offering vary widely. So is it too early to say that NAC is a real market? In the same study referenced above, we asked respondents if they have deployed NAC, and if they plan to deploy by 2008. Twenty-seven percent of respondents have deployed, growing to 55% by 2008, with another 15% saying they don't know if they will in 2008. There is massive potential for NAC; the desire to clean up the network (and keep it clean), construct virtual secure borders where the old physical borders have broken down or are inefficient or cumbersome to impose, and document and demonstrate specific levels of security is driving organizations of all sizes to invest in NAC now and the future.

Exhibit 2

NAC Deployment Plans

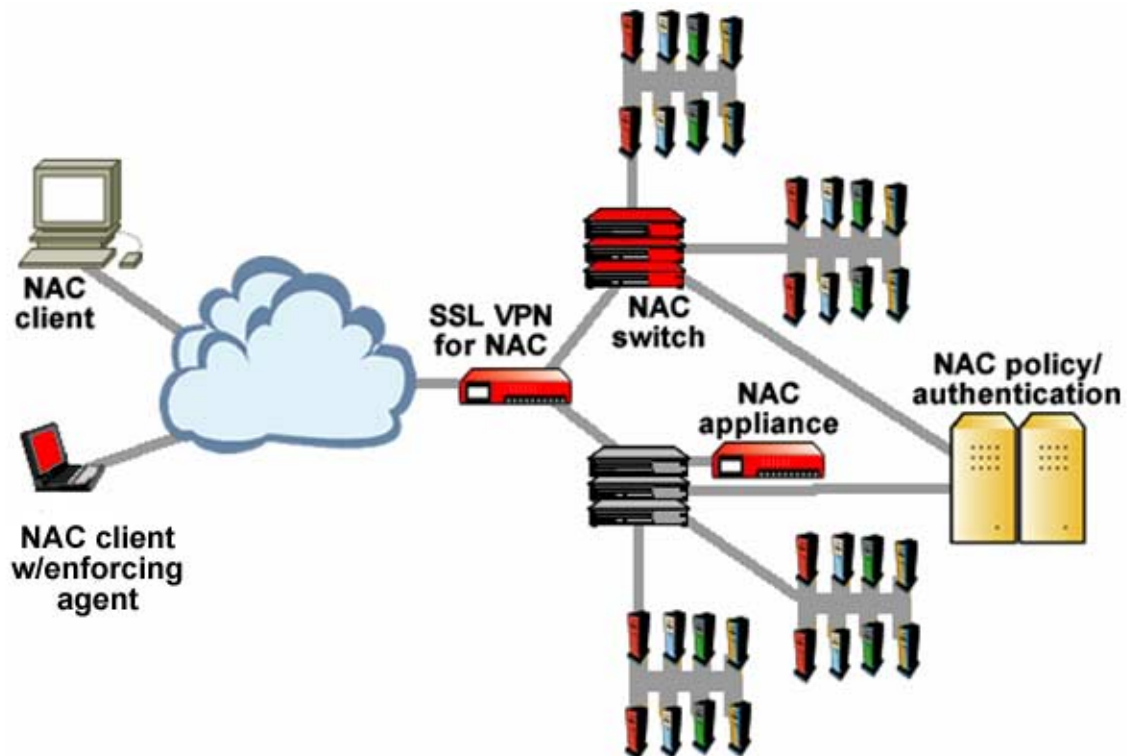


Source: User Plans for Security Products and Services: North America 2006 (Infonetics Research)

II. NAC Architecture

There are three main components of most NAC solutions: clients, enforcement, and the backend. This paper will focus on enforcement of NAC, meaning the location where access to the network and resources is unconditionally or conditionally allowed or denied (enforcement locations are marked in red on the diagram below). Enforcement can happen in the client itself (the left side of the diagram), or in the network (the center of the diagram), with policies typically served from the backend.

Exhibit 3**NAC Overview**



In a typical NAC solution, the following is done:

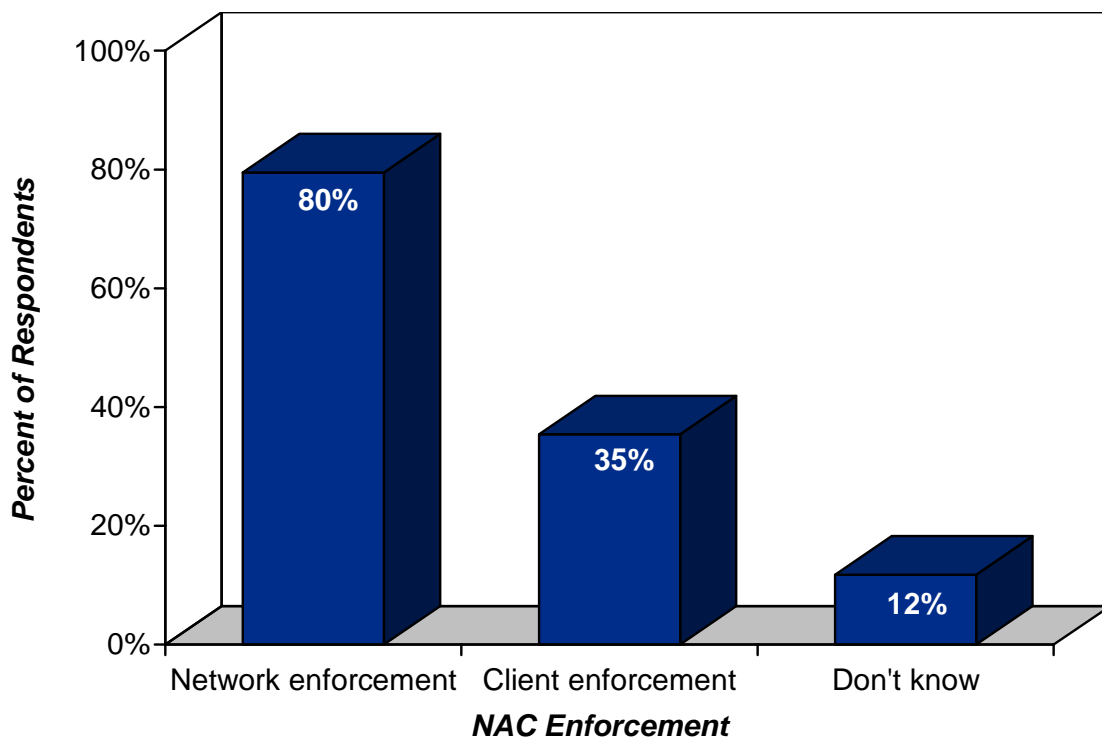
1. Authenticate the users (regardless of where they are coming from), typically using authentication credentials already supported by a company's infrastructure (anything from Windows login to two-factor tokens and biometrics)
2. Perform an integrity check on the user's computer (checking for OS patch and configuration information, presence of personal firewall and AV clients, etc.); in some cases, in addition to an integrity check, a NAC solution will also ascertain current system health (presence of malware typically)
3. Compare the authentication and integrity check results against set policies in a policy storehouse (generally located in the backend, but potentially located in the NAC enforcement device in cases where customers have simple environments that did not already include directories or policy servers)
4. Make a policy enforcement decision about what that user has access to, given the results of the authentication and integrity check; for the optimum balance between security and user productivity, this step enables a full spectrum of enforcement options, from allow all to deny all to moving users into specific VLANs for remediation of problems discovered during authentication and integrity checking
5. Pass authorization for network access to the enforcement device that can allow, deny, quarantine, or otherwise manipulate that user's traffic
6. Perform post-admission security functions, such as scanning all traffic from admitted clients and performing deep interrogation of the device itself in real time, looking for new policy violations or the presence of security risks (this post-admission function is not part of all NAC solutions)

III. NAC Enforcement

In simple terms there are two ways to enforce NAC. Once a client has been scanned and the user's credentials checked, access to the network can be granted or denied on the client itself or by some device on the network. In the same security study referenced above, 80% of the users we interviewed say they plan to enforce NAC in the network and only 35% plan to enforce at the client (some respondents do both).

Exhibit 4

NAC Enforcement Architecture

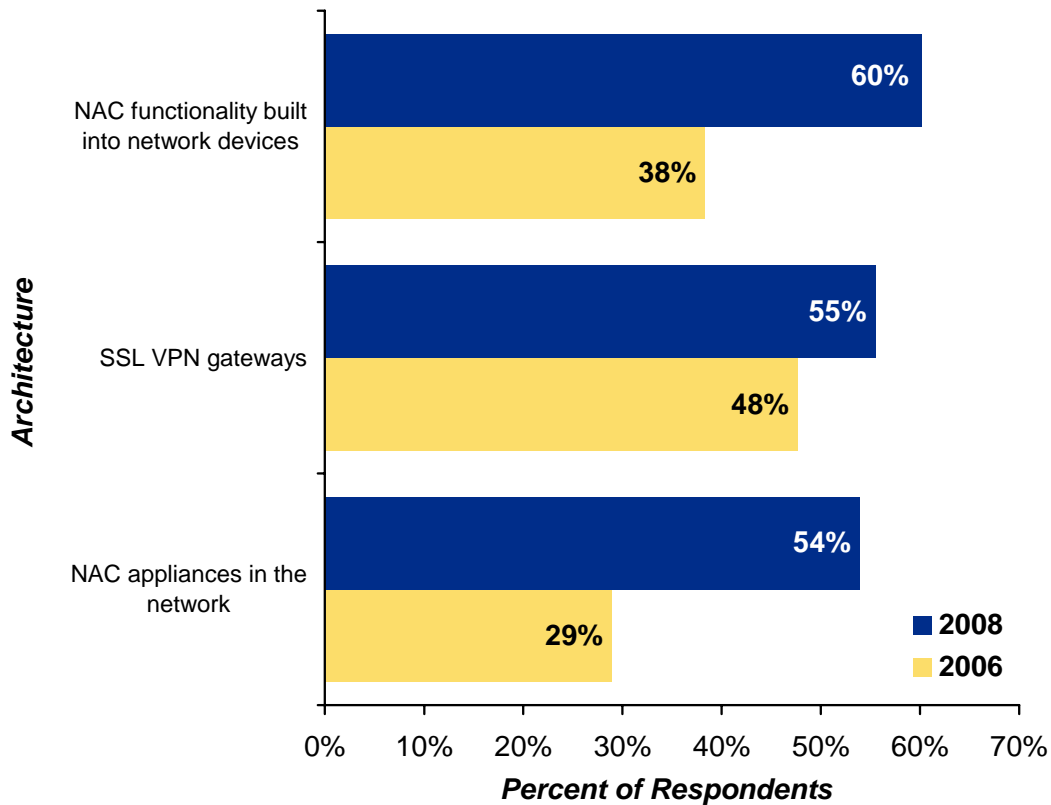


Source: User Plans for Security Products and Services: North America 2006 (Infonetics Research)

When enforcing NAC, users are faced with a variety of architectures and product choices. This is one of the fuzzy areas of the NAC market, and we expect preferences here to firm up as more companies pilot NAC. For now, the basic choices are to enforce NAC with functionality built into network devices (send a command to a switch using 802.1x to open or close a port and put a user into a specific VLAN), enforce using SSL VPN gateways, or to install a new layer of

NAC appliances behind the access network to deal with enforcing NAC. End-users are pretty evenly split on this issue, now and for the future.

Exhibit 5 Network-Based NAC Enforcement Architecture



Source: User Plans for Security Products and Services: North America 2006 (Infonetics Research)

Additionally, network-based enforcement solutions can be in-line with traffic flowing through them in real time, or out of band mirroring ports and watching traffic, but with no live traffic actually passing through them.

1. Client Enforcement

Some NAC solutions require a software client installed on the user’s computer, and then access is allowed or denied by the client itself (after it compares the results of the authentication and integrity check to the policy for that computer). This enforcing client can either prevent the computer from accessing the network entirely, or can direct the client to a quarantined portion of the network to assist in remediation. Some clients only handle pre-admission security, while others look at traffic on an ongoing basis once the user has been granted access to the

network, looking for security issues. Optimum protection requires a client on every network device for complete protection and that the client installed holds the enterprise's latest policy requirements.

2. Network Integrated NAC Enforcement

Cisco is the primary driver behind network-integrated NAC enforcement, but the general architecture could be executed in a multi-vendor environment, particularly as the work that the TCG is doing with TNC begins to mature. The basic idea is that switches, routers, firewalls, or any other existing network devices (in the case of Microsoft's NAP, a DHCP server running Microsoft software) communicate with both the clients looking for access (often running special client software), and with the backend authentication and policy servers, most often using 802.1x as the underlying transport protocol. Once the client is evaluated, the network device receives instructions from the policy server and executes those instructions, thus enforcing the NAC policy.

The most common type of network integrated NAC enforcement device will be an Ethernet switch that supports 802.1x and is able to talk to NAC clients and policy servers (either through proprietary or open means), but switches will not be alone. There will also be routers and firewalls and other security devices all handling NAC enforcement. Network integrated NAC enforcement is almost always in-line.

3. NAC Enforcement Appliances

Though integrating NAC enforcement into existing networking devices is a clean and simple idea, there are a variety of problems with it. Many companies interested in NAC will be forced to upgrade or replace large portions of network infrastructure (typically switches that are working just fine) with new products that have NAC supported functionality. In addition, many networks are multi-vendor, and as of yet multi-vendor network-integrated NAC solutions are scarce.

Luckily, a bunch of enterprising companies saw this gap between desire and available solutions, and came to the rescue, in most cases with standalone NAC appliances, some based on brand new technology, and others based on existing products (mainly in the wireless security and SSL VPN spaces).

Typically, these standalone appliances look like Ethernet switches, and for the most part they fit somewhere between the access network and the backbone. They come in as many flavors as there are vendors: some require that you deploy an informational agent (either their own or from a list of compatible vendors) and work with only a limited number of policy and authentication servers or directories on the backend; others require no agent at all, leveraging their own resources to sniff out new users on the network and force them to present authentication and device integrity data before allowing them access to the rest of the network.

Some of these devices do more than just handle NAC. They do network-based virus scanning and IPS as well (and other security functions), cleaning the traffic and looking for intrusions along the way. NAC enforcement appliances can be either in-line or out of band. The current generation of NAC enforcement appliances are the easiest, fastest, and most affordable way to deploy NAC.

IV. The Role of the Client

When investigating NAC solutions, the first thing many people notice is that some solutions require client software and others do not, and when digging deeper into the clients, it becomes clear that not all clients are the same. There are three different ways to set up end-users' computers for NAC: clientless, or with informational clients or enforcing clients.

1. *Clientless NAC*

Some NAC solutions require no client at all: no pre-installed client and no lightweight agent downloaded to the machine (agents typically use Java or Active-X and are downloaded to the user's computer dynamically to the session). So, what can you find out about a computer if you don't have a client or agent installed on it?

Typically in clientless NAC solutions the enforcement device inspects RPC-based functions, registry, and file sharing capabilities of the endpoint to assess compliance to network policies. This provides the system with information about OS type and version, presence and patch status of security client software, applications and services running, file sharing state, registry values, and more.

Many vendors offering clientless NAC solutions have proprietary methods (on top of RCP, registry, and file sharing status) for actively investigating device integrity. In addition, many clientless solutions can monitor traffic passing between the client and the network and analyze that traffic for security issues and policy violations.

Clientless solutions are typically the easiest to deploy, achieve broad protection and enforcement, and are the most scalable, but often don't have access to the depth of information client-based solutions have for integrity checking.

2. Informational Clients

Informational clients are agents that reside on the user's computer and feed the NAC enforcement/policy system information about the state of the device. These can be full install clients or temporary agents (again, Java or Active-X are the most likely) that are downloaded to the machine. Informational clients can provide all the information available in clientless NAC solutions and more, including configuration information about security client software and the operating system, data about signature files for security client software, existence of removable storage devices, and browser settings. Informational clients allow organizations to create policies based on a deeper set of information than clientless solutions provide. Informational clients do not enforce access policies: access is still allowed or denied by a device somewhere in the network.

Informational clients provide deep information about device state can work in conjunction with the clientless network solution, but can be costly and difficult to deploy and generally do not exist for every device on the network.

3. Enforcing Clients

Enforcing clients have the same inspection capabilities as informational clients, but also act as the actual enforcement point for NAC. Enforcing at the client has pros and cons; on the upside, enforcing clients can completely prohibit access to any part of the network. Enforcing clients can also control and/or reconfigure the connecting computer as needed to assist in remediation.

On the downside, many users are hesitant to install enforcing clients because they fear those clients can be circumvented, making it easy for a determined

hacker to skirt the NAC solution entirely. In addition, enforcing clients have the same drawbacks as informational clients; they can be expensive and difficult to deploy widely and are highly problematic for protection from visitors and contractors who need access to network resources.

V. Where Clientless NAC Shines

Now that we have a basic idea of the various roles of NAC clients, we'll drill down into the strengths of clientless NAC. If any of the following are key requirements for your NAC rollout, clientless NAC solutions should be at the top of your evaluation list.

1. Ease of Deployment and Scalability

Security solutions that require software to be installed and maintained on every device are a tough sell to most large IT departments. Though most have grudgingly invested in client security (usually host AV, personal firewalls, or VPN clients), they cringe at the idea of adding and maintaining yet another client, and almost always look at network-based solutions when they're available for two main reasons: cost and deployment complexity. Companies use client software for anti-virus, but are significantly increasing investments in gateway AV solutions as they become available. They use IPSec VPN clients in many cases, but the SSL VPN market developed initially because of the pain of deploying and maintaining IPSec clients. NAC is really part of the network infrastructure, and the people managing network infrastructure typically have a strong aversion to the vulnerability and currency of client solutions.

For a NAC solution to be truly useful, it has to be widely deployed, and suggesting to a large IT department that they will need to install and maintain thousands or tens of thousands of software clients usually elicits groans. In a clientless environment, once the infrastructure is in place it is relatively simple (even automatic) to add new users without adding "NAC client" to the list of applications the desktop support staff must install and configure when setting up new computers.

In some cases the additional functionality granted by a client-based solution justifies the pain, but for mass-market broad deployment there is more than

enough functionality in clientless solutions to create granular access policies that meet or exceed security and compliance requirements.

2. Guest and Contractor Access

Many companies deploy NAC to allow guests or contractors secure access to the network. Guest access can always be provided, but security and compliance cannot be assured; this is where clientless NAC proves very useful. In a clientless environment, you do not need to have any access to or administrative control over the connecting machine to make a basic assessment of security and grant restricted access. Guests can simply be identified and isolated into their own VLAN and granted extremely limited access (Internet only), or they can agree to be interrogated by the NAC system, which will then do the deeper inspection of their computer performed on non-guest devices, then possibly offer authenticated access to a wider range of resources on the network, all without having to install any kind of client.

Many companies report that secure guest and contractor access is one of the first applications they roll out once they have NAC in place, and it's ideal for highly regulated environments with pervasive guest requirements (patients at hospitals, consultants working at financial institutions), as well as chaotic environments that must admit guests but worry about the spread of security problems (guest access in municipal areas, hotels, convention centers, airports, and schools). If a client were required to secure guest access in these environments, the implementation effort would make drive most organizations to skip secure guest access rollouts.

3. Access from Non-Standard Devices

So far we have been talking about NAC and enforcing access control for devices where client software is readily available, but what about devices that cannot run client software at all (such as network-connected printers, copiers, IP telephones, and fax machines), or devices that don't have NAC client software available to them, but connect to the network anyway (such as PDAs or any other IP-connected client device running a non-standard OS)? Currently, for NAC solutions that require clients, there is no support for these devices.

At the 2006 BlackHat security conference, a security expert at a leading financial institution hacked a multi-function Xerox device, which was, in essence, a Linux server. Once the printer was under his control, he was able to use it to understand the layout of an organization's internal network; this is information that could help hackers set up later attacks. The breach also gave him access to any information printed, copied, or faxed from the device. He was able to change the internal job counter on the printer, a trick that could be used to reduce or increase a company's bill if the device was leased. NAC cannot leave out or ignore any of these devices. Where worry abounds at the connection of a new computer, little security effort accompanies the addition of a printer.

Network-connected printers and similar devices can pose a real threat; it seems reasonable that any organization deploying NAC must be able to include those devices in their rollout.

As for other types of devices with more obscure operating systems (such as PDAs and other handheld devices), many are already a critical part of the enterprise IT infrastructure, with a demonstrated need for coverage under a security policy in any situation where compliance is being monitored. These devices are also being exploited by hackers and used to propagate malware of all types, but many of them cannot be controlled in any way with current client-based NAC solutions, and many of the client solutions that support them are complex, expensive, and require the integration of products from multiple vendors.

VI. Conclusion

NAC is the most abused and misunderstood term in the enterprise security market, but underneath all the misinformation is actually the kernel of a great and needed idea: a comprehensive system to keep bad guys out of the network and ensure that the good guys are compliant, accessing only the things they specifically need to access. This is really the core of the idea, but there are many extensions to the technology (such as virus scanning and intrusion prevention on traffic from users that pass the NAC screening process) and a wealth of other problems for NAC to solve.

For mainstream adoption of NAC, and by mainstream we mean when there are as many people using NAC as, say, stateful-inspection firewalls, NAC will have to be affordably priced, easy to install and manage, massively scalable, and able to cover a broad range of platforms, applications, and user types. We believe that there is enough opportunity to support clientless, informational client, and enforcing client solutions, but we believe that the mainstream opportunity for NAC technology is greatest for clientless solutions. There are numerous NAC appliances on the market today that can help users quickly roll out clientless NAC, obviating the need for lengthy pilots or rollouts and going straight to protecting the network.

About Infonetics Research

Infonetics Research (www.infonetics.com) is the premier international market research and consulting firm specializing in data networking and telecom. We provide a complete view of the market through constant interaction with equipment manufacturers, service providers, end-users, chip and component manufacturers, sales channels, and the financial community. We offer quarterly market share and forecasting, end-user survey research, service provider survey research, and service provider capex analysis. We are respected in the industry for being objective and accurate and for delivering on time all the time.

Services

- Market Share, Market Size & Forecasts
- End-User & Service Provider Survey Research
- Service Provider Capex Analysis & Forecasts
- Consulting, Retainers & Quick Consults
- Webinar, Conference & Event Speaking
- Custom Demand-Side & Brand Market Research
- Custom Market Size & Forecasts
- Technology and White Papers
- Competitive Analysis & Due Diligence

Coverage Areas

- Broadband & IPTV
- Enterprise Voice & Data
- Network Security
- Service Provider Capex
- Service Provider Optical, Metro E, Routing & Switching
- Service Provider VoIP, IMS & FMC
- Total Telecom & Datacom
- Wireless & FMC

Contact Information

US Headquarters

900 East Hamilton Ave #230
Campbell, CA 95008
United States
t +1 408.583.0011
f +1 408.583.0031

Boston Metro Office

3 Baldwin Green Common #307
Woburn, MA 01801
United States
t +1 781.933.9649
f +1 781.933.9659

London Office

P.O. Box 629
Bromley, Kent BR1 4WB
United Kingdom
t + 44 168.985.1618
f + 44 168.985.1618

Sales

Larry Howard, Vice President

larry@infonetics.com

t +1 408.583.3335
f +1 408. 583.0031