

Getting Started with Network Access Control

If you'd like to implement Network Access Control, no matter what architecture you select, you definitely want to start by building a small interoperability lab. In this white paper, we'll give you some advice on what to think about before you get started, and outline what resources you'll need to have in place in order to begin testing.

Any NAC deployment must start by answering three critical questions:

- 1) What is my access control policy?
- 2) What are the access methods (such as LAN, wireless, or VPN) I want to protect?
- 3) How will this integrate with my existing infrastructure?

Once you answer these questions, you can begin to gather test lab resources, such as servers (for policy definition points), laptops or desktops (for network access requestors), and switches, access points, and VPN servers (for policy enforcement points).

What is my access control policy?

NAC is a generic concept that deals with defining access controls based on user authentication, end-point security assessment, and network environmental information. That's too big for most network managers to bite off in a single chunk, so many NAC deployments hone in on a subset of these goals and expand over time. You'd be wise to do the same---trying to do too much too early in the lifecycle of this emerging group of products will lead to undue frustration and unnecessary complexity.

To start, you should define a simple network access control policy. It is important to define your access control policy first, because that will frame the rest of your testing and deployment. You can put it in any format you want, but most network managers will be most comfortable with something that looks like a table. The following table might give you an idea of how to start:

User Identification	End-Point Security Status	Environment	Access Control
Auth, Group=STAFF	A/V is enabled and up-to-date	Inside the building	All access OK
Auth, Group=STAFF	A/V not up-to-date	Inside the building	Access to remediation network only
Auth, Group=GUEST	<don't care>	Inside the building	Access only to Internet
Unauthenticated	<don't care>	Inside the building	Redirect to portal server, no access
Auth, Group=STAFF	A/V is enabled and up-to-date	VPN Access	All access OK
Auth, Group=STAFF	A/V not up-to-date	VPN Access	Mail server only

NAC products, at this stage of their deployment, are not focused on fine-grained access control. Instead, they tend to use very coarse control, such as a "go/no-go" decision (all access or no access) or one based on VLANs. With VLAN-based access controls---the most common strategy we saw in the iLabs product testing---the NAC product is not really providing full control, but defers to your existing infrastructure, such as firewalls sitting between VLANs, to limit access between networks. The idea here is that if someone is placed on the "remediation VLAN," for example, there will be a firewall elsewhere on that VLAN which prohibits that user from wandering further into the network. While this very coarse control is not elegant, it is very common.

You will probably find that casting your access control policy in these kinds of coarse terms will give you the greatest flexibility in choosing available products and in integrating them with your current architecture. In other words, don't expect NAC products to provide full firewalling processes at the policy enforcement point (even if that's what you want) until this market niche has matured significantly. If you do need that level of access control, as defined by your policy, be sure to define it early so you don't go down a path of testing that won't meet your needs.

What access methods do I want to protect?

When thinking about NAC, you need to qualify what kinds of access methods you want to protect. Most networks have three main access methods: (1) wired and wireless LANs IPsec; (2) SSL VPN remote access connections (e.g., a single user running an IPsec or SSL VPN client), and (3) VPN-connected branch offices (a special case of the wired/wireless LAN connection, but important enough and different enough from local LAN connectivity that you may want to give it special consideration).

Your NAC strategy may cover one, two, or all three of these access methods, but you should decide early which ones you care about and focus your testing on those. You should also think about whether you want a unified strategy (i.e., the same components are used, no matter what the access method) or whether you want to create your own silos based on different user communities or varying access methods.

NAC became a very hot button several years ago as SSL VPN vendors realized the dangers of letting outside PCs have access to internal networks without knowing anything about the end-point security of those PCs. In the world of SSL VPN, this usually goes by the term “End Point Security,” or “Client Integrity,” but the concept is really just NAC, as applied to SSL VPNs.

With SSL VPN vendors firmly footed on the NAC bandwagon, IPsec vendors have also been adding NAC features to their products. Sometimes, this means simply recasting existing capabilities with a new name to make them fit the new buzzwords, and in other cases, this meant adding entirely new features.

The relative maturity (with emphasis on the “relative” aspect) of NAC in these VPN access methods means that you may not be able to easily merge new LAN-based NAC products with existing SSL or IPsec VPN products. If that’s a show stopper for you, get that on the table early. On the other hand, if you don’t care, this may simplify your NAC strategy enormously. IPsec and SSL VPN products have been shipping NAC for months, if not for years.

NAC both on the wired LAN and wireless LAN is much more difficult to implement, because it may entail large infrastructural changes, ranging from software and configuration changes to wholesale equipment upgrades or even replacement. The wired LAN is the largest barrier to full NAC deployment because most enterprises have mature and fully deployed Ethernet networks that they don’t really want to change. Most savvy network managers are looking at NAC as the “killer app” that finally justifies deploying 802.1X throughout the enterprise. While simple authentication with 802.1X hasn’t been important enough to justify widespread adoption on the wired LAN, the combination of posture assessment **and** authentication in NAC may give the business case for 802.1X deployment.

On the wireless LAN side, 802.1X (typically in the form of 802.11i, also called WPA2) has already become a standard in enterprises serious about wireless security. The question here is not whether you want to continue using 802.1X, but whether you want to add NAC capabilities to your existing (or planned) wireless deployment. Of course, if you haven’t already turned on 802.1X on your wireless LAN, NAC again may be the reason that finally makes better security a part of your wireless strategy.

As you decide which access methods you wish to protect, this will help you determine what equipment you need in your test lab. It will also help to narrow the range of products you can ultimately use and therefore need to test first. For example, if you want to use NAC in the wired LAN, but your switches cannot handle 802.1X authentication or VLAN switching, you may need to use a NAC technology that sits in the core of the network, upstream of your existing access layer switches. Figuring this out early will help you to narrow your options and save you time and effort.

How will I integrate this with my existing infrastructure?

NAC will be a disruptive factor because it affects not only the switches, routers, and firewalls, but also the software loaded on desktops and laptops, as well as the traffic load on authentication and policy servers. A very important part of testing and designing NAC in any network is making sure that the changes that it causes are compatible across the board. For example, installing the NAC client and posture collector tools on a ‘fresh from the factory’ laptop isn’t going to tell you whether this client will work on your existing laptops and desktops using your existing corporate standard software configuration. You need to test it on the exact configuration you have deployed.

If you are using software distribution tools and patch management servers, you need to be sure that the NAC client will complement your infrastructure and not disrupt it. This is a very good time to open what will be an on-going dialog with any end-point security or management tool vendors you have adopted, including patch managers, software update servers, and anti-virus, anti-spyware, and personal firewall tools. These vendors can help you understand what NAC protocols they are following and which architectures they are supporting.

While NAC is often thought of as a network security issue, the heavy disruption and integration actually occurs on the desktop and laptop. This is why bringing these other parts of the picture into focus early on in the process will help ensure the success of your NAC deployment.