

What is NAC?

Generic network access control at its core is a simple concept: Who you are should govern what you're allowed to do on the network. NAC, then, is simply the hardware and software that together let you enforce access control policies based on "who you are."

When all of the parts are in place, NAC will be a way to apply a policy for network access across LAN, wireless and VPN infrastructures. The access-control policy in NAC could range from simple, such as a go/no-go decision on network access or a choice of virtual LANs, or it could be as complex as a set of per-user firewall rules defining which parts of the network are accessible.

Since NAC is a huge step for people to consider adding to their network, we see all kinds of slants on the idea of NAC. For example, some products tightly focus on endpoint security as the key reason for implementing NAC, while others home in on authentication and policy as the prime pieces. In reality, a good NAC product is not simply a way to flop users between quarantine and production VLANs, but a generic access control system that authenticates and authorizes all traffic. NAC is different from control systems such as firewalls, because NAC is the first time that we really have the tools available to provide **user-focused access control**.

There are many products currently available that can do some or even all of NAC. In the iLabs, we focused on the three most significant NAC architectures and how products that implement these architectures interoperate with each other. This is not to say that you must pick an open or interoperable architecture. Depending on your network size and security philosophy, you may be perfectly happy with one of the many closed and proprietary NAC solutions on the market. Those, however, were not part of our testing in the iLabs.

How does NAC pick a policy?

If "who you are" is how a policy for access gets picked, then the definition of "who" is more complex than a simple username. Within a NAC deployment, the IT manager uses three main elements to pick an access-control policy: authentication, endpoint-security assessment and network environmental information. Effectively, these three things determine "who you are."

Authentication is the straightforward part of "Who are you." This is the basic identification (and authentication) transaction that users are accustomed to with other applications. As a concept, NAC doesn't have special requirements for authentication. A good NAC deployment would use the same authentication system as other applications. For example, if you're applying NAC to a remote access IPsec VPN tunnel, you should use the same authentication to bring up the IPsec tunnel as you do to authenticate a user. Some NAC products and architectures have skipped over the concept of user authentication in favor of the second part: evaluating the security posture of the end point.

Endpoint security assessment is the most complex part of selecting a policy in NAC, but it's also the driving factor for deploying NAC in the first place in many enterprises. The underlying idea is that the security posture of the connecting laptop, desktop or server should be a part of access control policies. For example, if a connecting system doesn't have the standard corporate anti-virus package, the user should get a different access control policy than if everything is installed and all the signatures are up-to-date.

The third part of "who you are" is environmental information. Only a few products really take this into consideration. Network environmental information is a small but important part of selecting access policies in a NAC scheme. Environmental information might be circumstantial data about whether you're connecting via a wireless network or through a VPN, or whether you're in the building or in another country. These circumstances play into the decision of what access control policy is assigned to the connecting system. For example, if you're coming in on a VPN, you might not be able to get to as many parts of the network as if you were in the building.

NAC is a hot buzzword; therefore, this component-level definition of what NAC is won't map directly to all NAC products and architectures. But most products being offered as part of an overall NAC strategy include at least some component, if not all, of this definition.

Where Does NAC Go In My Network?

There are three fundamental approaches to NAC based on where the access control is being enforced in the enterprise: edge control, core control and client control.

Edge control takes the principle of the firewall and pushes it to the edge of the network, where systems connect. If you are protecting a LAN, the individual switch port becomes the NAC control point, typically with 802.1X. This is the model we tested the most in the iLabs. If you are working with a VPN connection, the IPsec concentrator or the SSL VPN device is in charge of enforcing access controls. In a wireless environment, the access point or wireless switch plays the NAC role.

In the core control schema, controls can be enforced anywhere in the network providing it's in deeper than the edge device. You could insert a NAC device inline, or as a passive tap, between edge switches and the core, where it would collect authentication and endpoint-security information, and then enforce the appropriate access control policy. These devices inspect traffic or control-plane information passing by and reach into the network to change configuration to apply enforcement.

The client control approach focuses on the end system connecting to the network where greater attention is paid to the management and control of the end system. In a typical client control system, you'll install a fairly heavyweight application on each end system that enforces NAC policies and local access controls, such as disabling wireless access if the VPN client isn't in use. An endpoint protected by this kind of tool inherits a strong set of security protections, such as personal firewall, USB device locking and wireless controls that might be difficult (or impossible) to assemble and manage from a slew of other NAC vendors.

While the client control approaches are attractive from a lower budget and simplistic management point of view, they don't strongly overlap with NAC approaches that integrate with the network to help to defend itself, to force user authentication or to provide identity-based access controls.

Most of the NAC frameworks touted by the major network players overlap these categories, reflecting the reality of how people build and buy networks.

How does NAC work?

The easiest way to understand NAC is to follow a sample NAC transaction, as shown in the diagram to the right.

This diagram (from Network World magazine) follows a typical NAC transaction using terminology from the Trusted Computing Group's Trusted Network Connect architecture. You can map these terms to other generic and vendor-specific architectures using the Network Access Control Architecture Alphabet Soup handout available in the iLabs booth.

This diagram shows a one-time assessment as a system connects to the network. In reality, most NAC deployments are also focused on continual protection and provide the ability to change access control even after the user has been authenticated and connected to the network.

