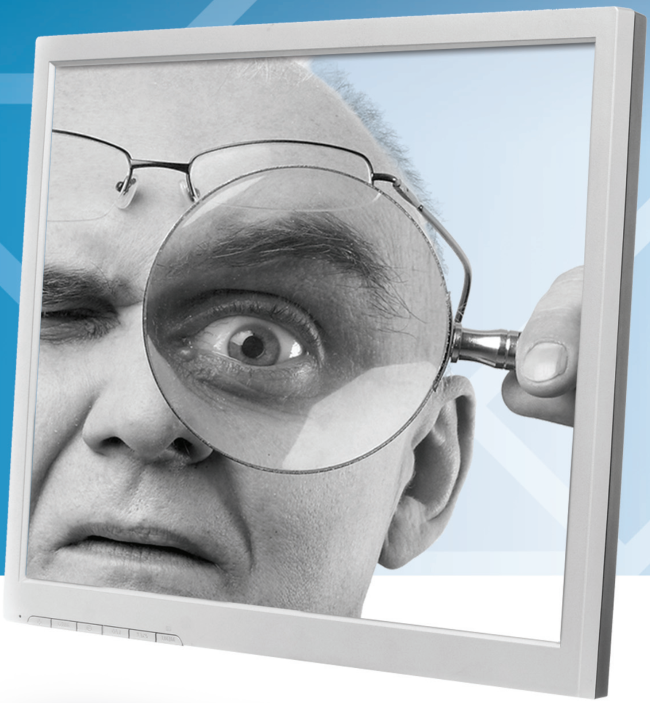
BLACK BOX®
NETWORK SERVICES

The Basics of NAC—Network Access Control

Network Access Control

What is it and why do you need it?

- Harden your network.
- Prevent network breaches.
- Eliminate unauthorized network connections.
- Identify non-compliant, vulnerable devices.



Veri-NAC™

724-746-5500 | blackbox.com

Table of Contents

We're here to help! If you have any questions about your application, our products, or this white paper, contact Black Box Tech Support at **724-746-5500** or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 20 seconds.

Introduction

Today's network environment is changing. Although desktop computers are still the primary means of network access, a network may also have to cope with an ever-increasing number of mobile devices such as laptop computers, netbooks, smartphones, and PDAs. Network managers are finding that portable devices joining their network are creating a real security threat. Controlling this access is what NAC is all about.

Network access control (NAC) is a method of ensuring that only known devices are allowed to connect to your network and that they meet your network's requirements before they are granted access. NAC keeps untrusted and unauthorized devices off the network, so it shields your network against everything from wireless Internet moochers to hackers stealing sensitive information through an unprotected network port.

Keeping untrusted devices off the network is pure NAC—NAC at its most basic level. But many vendors have expanded the functionality of their NAC products to include services that are not strictly network access control. Because NAC is a hot buzzword in networking at the moment, but isn't clearly defined, every vendor's version of NAC includes a different mix of NAC and NAC-related services. You may see NAC defined as anything from simple go/no-go network access to complex network-management schemes.

In addition to pure access control, NAC systems may also be able to dictate already trusted users' level of access and manage users' access once they're on the network by leveraging existing single sign-on systems such as Active Directory or LDAP (which already do this independently of NAC). NAC frequently includes extensive patch management systems that prompt users to update their systems before allowing them to join the network.

NAC system functionality may include:

- **Simple network access**— authenticating devices wishing to access the network and granting or denying them access.
- **Limiting network use**— controlling where users can go and what resources they can use once they get on the network, based on identity, time of day, location, and application.
- **Grouping users**—segmenting users into groups, for instance, trusted and untrusted or accounting and non-accounting.
- **Policy enforcement**—making sure network devices meet organizational standards—including software updates and virus control to make sure the network isn't compromised by problem devices.
- **Quarantine**—routing unknown devices or legitimate devices that are out of compliance onto a separate restricted IP network or VLAN.
- **Remediation and patch management**—providing tools that enable users to bring their devices into compliance.
- **Monitoring network activity and preventing suspicious activity**—potentially preventing zero-day attacks on vulnerabilities for which patches are not yet available.
- **Visibility**—providing a real-time overview of what devices are connected and what their status is.
- **Regulatory compliance**—keeping records to document compliance with standards such as Sarbanes-Oxley, HIPAA, PCI, and ISO.
- **Protecting against malware**—NAC can help to prevent infection by viruses and other malware both by limiting network access and by scanning the network for common vulnerabilities and exposures (CVEs).

Although a wide range of NAC functionality exists, the core function of NAC is always to control who can access your network. Some systems may also monitor network activity, enforce policies, control resources, and document security—even act as a stateful-inspection firewall—but pure NAC always comes back to network access.

Because of the wide range of available options, it's doubly important that you precisely define your requirements and know what you're buying before you invest in a NAC system.

An important part of your security plan

NAC has a special place in a network security plan because, unlike a firewall, which offers perimeter protection, NAC monitors the inside of your network. A firewall stops the hacker in Poland from getting to your network through the Internet. NAC stops the hacker inside your building from getting to your network through an Ethernet port or wireless access point.

NAC is especially useful for dealing with rogue access points—unauthorized access points that users have plugged into your Ethernet network for their own convenience. Unauthorized access points range from a mere nuisance to a real security threat in a large network. Because it's so easy for users to plug in an access point, you have to constantly guard against it. Just one unsecured access point can be a vulnerable entry point for an entire network.

It's important to keep in mind that NAC is only part of a security plan, not a complete security measure. It doesn't take the place of a firewall and won't protect against data leaving through e-mail, printouts, or USB flash drives. However, the majority of breaches and data theft occur behind firewalls, making NAC a critical component of a multilayered security policy.

NAC standards

Because NAC is still a very new technology, it's not been standardized, although there have been attempts in that direction. You may see references to these NAC standards:

IEEE 802.1x—This security and authentication protocol is often used for NAC and may be closest thing to a universal NAC standard. This standard is fully described in the NAC architecture section of this paper.

Trusted Network Connect (TNC)—This open-source standard was developed by the Trusted Computer Group to ensure that devices connecting to the network are free from malicious code and up to date.

Internet Engineering Task Force standards for NAC—These standards hold some promise for bringing NAC together under one umbrella, but, as of this writing, they're still in the work group phase.

Although these are some of the main contenders for a universal NAC standard, NAC is still very much a free-for-all with many vendors promoting a proprietary scheme of their own. Some of these are very, very good; and some are very, very…well, let's just say they're insufficient.

NAC architecture

NAC may use any one—or more—of a number of architectures. These are by no means the full range of NAC methods you may encounter.

Pre-admission and post-admission

NAC is generally divided into pre-admission and post admission NAC, based on whether policies are enforced before or after devices access the network.

Pre-admission NAC is the gatekeeper and inspects devices before allowing them on the network, checking credentials and ensuring that devices are in compliance with network policies.

Pre-admission NAC blocks devices that don't belong on the network and is often also used to identify which group users belong to—for instance, it can identify whether a user belongs to the organization or is a guest. It can even be used to sort users that "belong" into subgroups, for instance, different departments within an organization.

But gatekeeping is only half the battle. Post-admission NAC examines devices and controls what they're allowed to do once they're on the network. It can, for instance, place users into specific VLANs and control what applications they can use based on what group they belong to, their location, or even time of day. Post-admission NAC is often used to log network operations for help with auditing and compliance to meet specific requirements for compliance with standards such as HITECH or ISO.

Virtually all NAC systems offer pre-admission NAC—controlling who joins a network is, after all, the very basis of the idea of network access control. On the other hand, not all NAC systems offer post-admission NAC. Most organizations find they need both pre- and post-admission NAC to fully cover their security requirements.

In-line and out-of-band

The two major approaches to NAC architecture are in-line and out-of-band. They differ in how they relate to network data flow and require different considerations when you design your network.

In-line NAC calls for placing a NAC appliance in the flow of network traffic where it functions as a switch with network traffic flowing through it.

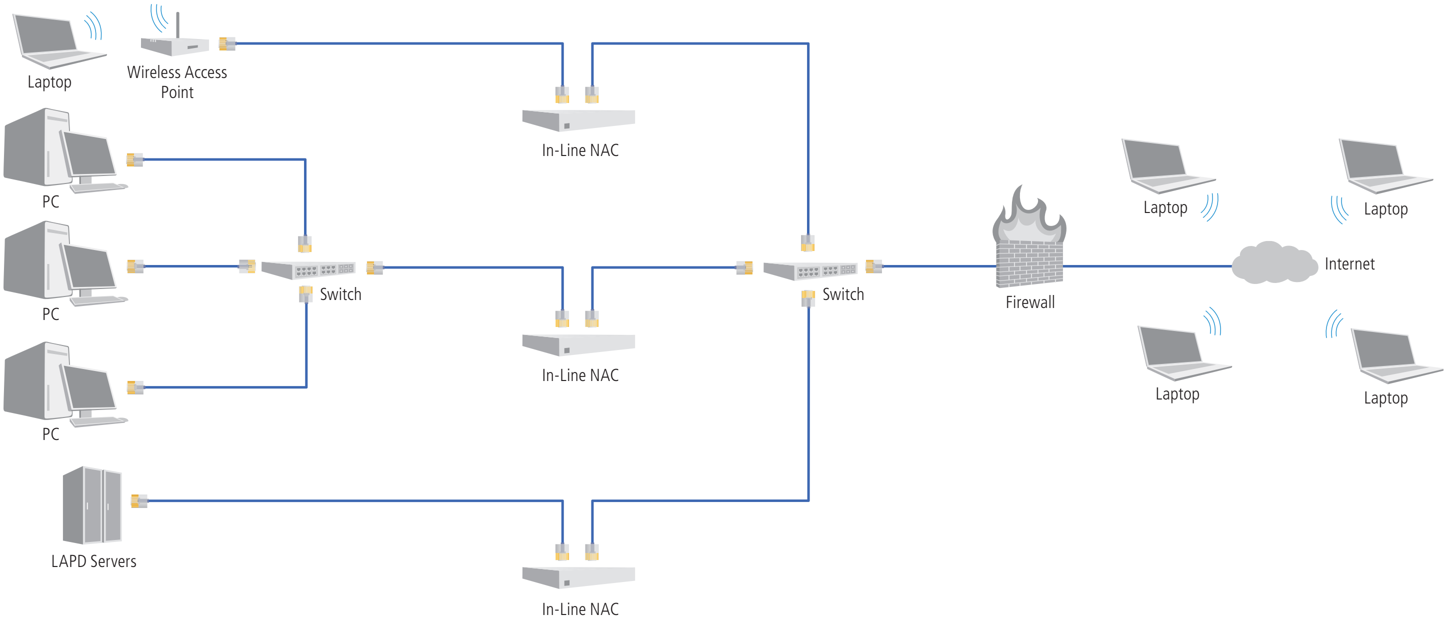
In-line NAC is very good at monitoring the network and detecting network anomalies. These systems are exceptionally adept in the post-admission arena by controlling access to specific network resources after a device has connected to the network. In-line NAC generally provides much tighter control over user behavior.

In-line NAC is often compared to an internal firewall that can enforce policy between network segments in a very precise way because it sees individual packets traveling across the network.

Network traffic travels through an in-line NAC, so it may slow the network. Many in-line NACs have special high-speed ASICs to keep data moving at wire speed.

An in-line NAC can only monitor the traffic that passes through it—it won't prevent unauthorized devices on another network segment—so it's important to place in-line NACs near the network core and pay attention to network architecture. Because in-line NAC often requires changes in network architecture, it's most often deployed in new networks. It's worth keeping in mind that installing inline NAC in an existing network requires that you take the network down for the installation. Also, keep in mind that if an in-line NAC goes down, it will take your network with it.

In-line NAC is most suitable for small networks because the larger the network is, the more NAC appliances you need. Because of problems of scale, you rarely see it being used for enterprise networks.



Out-of-band NAC accesses your network through one or more switches. Unlike another common definition of "out of band," which means to access a network device through a route other than the network, such as a serial port, an out-of-band NAC accesses network devices through the network. It's on the network but does not have network traffic flowing through it like an in-line NAC does.

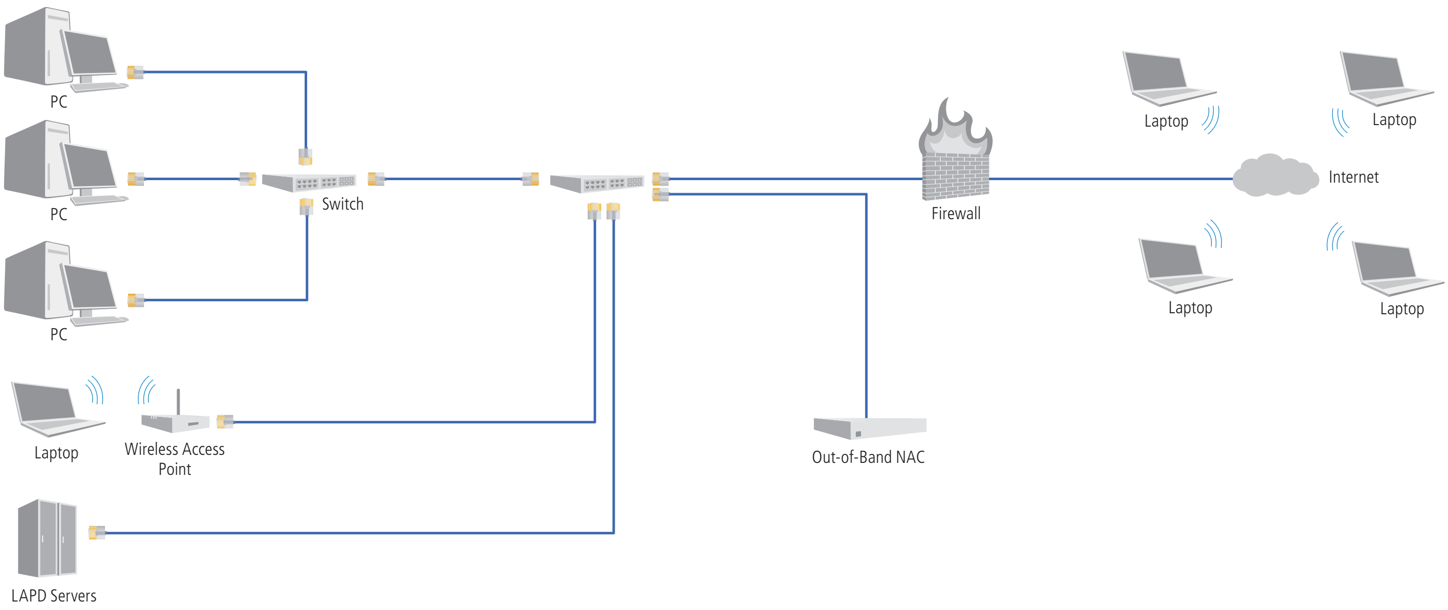
Out-of-band NAC systems use a wide range of enforcement tools. They may or may not use agents and may use 802.1X, VLAN steering, or IP subnet. This wide variability can make comparing two out-of-band NAC systems like comparing the proverbial apples and oranges.

Many out-of-band NAC products are limited to controlling network access and may also direct users to an IP subnet or VLAN. Because these systems are out of the flow of network traffic, out-of-band NAC solutions usually don't have the ability to monitor devices after they connect to the network, although this shortcoming is beginning to be overcome by some vendors.

There are management advantages to out-of-band NAC—many systems provide options that enable you to manage multiple networks from a central location.

Unlike in-line NAC, this method does not compromise network uptime or require that you shut down your network for installation —if an out-of-band NAC goes down, it doesn't take the network with it.

Because out-of-band NACs aren't as dependent on network architecture and install easily, they tend to be a good choice for existing networks.



Endpoint-based and network-based

Endpoint-based NAC, also called host-based NAC, requires the installation of software agents in connected devices such as PCs to gather information about these devices and report back to a NAC policy server. An agent may permanently reside on end devices or it may be dissolvable, which means it disappears after reporting information to the NAC.

NAC systems that use agents are inherently limited because agents frequently don't work with all devices and operating systems. For instance, NAC systems that use agents often don't provide agents for smartphones, networked printers, or PCs running Linux®. To some extent, this limitation can be worked around by using a browser-based dissolvable agent, but even this solution leaves out some devices.

The limit on devices that can accept an agent can be an advantage or a disadvantage, depending on whether your security goals are to limit the type of devices that may have network access or to include a wide range of devices.

Network-based NACs, which may be in-line or out-of-band, rely on network scans to discover attached devices and gather information about them. This method is really the only choice for networks that include devices that don't accept agents or that regularly host guest computers.

802.1x-based

IEEE 802.1x is a network security standard used as the basis of many NAC systems. Although the term 802.1x is often used interchangeably with NAC, not all NAC systems are based on 802.1x. 802.1x provides a way to accept or reject users who want network access. It works with both wired and wireless networks.

802.1x uses 802.1x compliant network devices such as switches and access points to act as middlemen between devices wishing to access the network and an authentication server—usually a RADIUS server—which decides whether or not to accept the request for network access. It also periodically re-authenticates devices to ensure they still deserve network access. This use of switches and access points as middlemen is also referred to as "port-based" NAC because access is granted at the port level.

802.1x is an extraordinarily versatile security protocol because it uses Extensible Authentication Protocol (EAP), which provides an authentication framework rather than a specific authentication method. Because EAP just provides the framework, it can support a variety of authentication methods such as certificates, one-time passwords, and public-key authentication.

802.1x also supports VLANs through the RADIUS server, which may also manage QoS assignments. This enables you to control exactly which services each user can access and how much bandwidth they can use.

The advantage of 802.1x is that it provides a highly standardized framework for authenticating and managing user traffic—all your 802.11x-compliant devices will work together. In addition, support for dynamically varying encryption keys makes this standard highly secure, and VLAN support provides versatility so you have high control of network traffic.

The major disadvantage of using 802.11x for NAC is that it requires that all the switches and access points in a network be upgraded to support 802.1x. Few organizations are willing to upgrade to 802.1x for NAC alone, although they may add 802.1x NAC as part of a general network upgrade.

It should also be noted that 802.1x NAC can be rendered fairly useless through the simple addition of a non-compliant hub. If a non-compliant hub is plugged into a port on an 802.1x switch and one user on that hub has network access, then anyone else can plug into the hub and also receive network access. This is frequently compared to "badge tailgating" in which a person with a badge enters a secure area and others follow through while the door is open.

802.1x NAC is secure, versatile, and highly standardized, but it requires a serious commitment to establishing and maintaining an 802.1x compliant network.

DHCP

Dynamic Host Configuration Protocol (DHCP) is sometimes used for pre-admission NAC. DHCP is a client-server protocol in which the DHCP server manages IP addresses and information about client computers. Because organizations usually already use DHCP to assign IP addresses, it seems natural to expand its range to include NAC, commonly through an in-line device between the DHCP server and the network, which assigns a client device an IP address that places it onto a quarantine network until the NAC device decides it meets network standards. A major drawback to this method is that a user can overcome it simply by assigning his or her device a static IP address.

Enforcement

After a NAC assesses the user’s status, it decides whether to accept or reject the user and what, if any, restrictions to place on that user. In some NAC systems, post-admission enforcement of standards can be very detailed and complex.

The most basic NAC just allows or disallows network access based on what it knows about a user. Most modern NAC systems, however, go beyond this simple go/no go method of enforcement to use a variety of post-admission methods to manage network access.

Quarantine Network

A NAC system may choose to quarantine users by allowing them access to only certain hosts and applications until they meet network standards and are approved. A quarantine network is usually set up using either a captive portal or VLAN.

Common uses of a quarantine network are:

- Restricting authorized users with out-of-date software or virus protection to a remediation network containing instructions and tools for bringing their computer into compliance.
- Routing visitors to a guest network that enables them to access the Internet but doesn’t allow them to view or access the corporate network.

A danger in implementing a quarantine network is that, eventually, you could wind up with a concentration of infected machines that infect and reinfect each other, creating a sort of zombie network.

VLAN

Virtual LANs (VLAN) aren’t NAC, but NAC systems commonly use VLANs to segregate users within a network. Based on who they are, or even which applications they’re running, NAC puts users into appropriate VLANs. For instance, there could be a separate VLAN for visitors, one for regular employees, and one for employees with access to sensitive financial information. These groups can see only the parts of the network the network administrator decides they need access to.

Choosing a NAC system

NAC is still very much the “Wild West” of the IT world—there are many different methods and approaches in a huge range of sizes, effectiveness, and price points. Choosing the right system for something that affects your entire network, like NAC does, is critical.

Some of the choices you’ll have to make include NAC method, policy enforcement, and form factor. You’ll have to evaluate NAC systems from many vendors. Plus, you probably have an organization with no experience in deploying NAC. Where to start?

With all the hype surrounding NAC, it’s important to do your research and sort through which NAC features are important to you—different systems lend themselves to solving different security problems.

By listing and defining your requirements, it will ultimately be possible to fit the right NAC architecture to the security needs of your network.

Before shopping for NAC, define exactly what it is you need from a NAC system. Put this in writing. Once you define your needs and go shopping, you’ll find that you can zero in on appropriate systems quickly.

Considerations when choosing a NAC system include:

- Cost — How much can you spend? Are you getting your money's worth?
- Network size—How many users share your network? How many subnets?
- Network use—Who uses your network and do you need to keep groups of users segregated?
- Effectiveness—How foolproof does your security have to be? How much is it worth to protect the data on your network? Does the NAC system scan for CVEs?
- Form factor—Are you willing to install, configure, and troubleshoot NAC software on a server or would a dedicated NAC appliance be best?
- Administrative burden—How well trained are your staff members? How much time can they spare to deal with NAC?
- Hardware fit—Will the NAC system work with the network you have or will you need to upgrade?
- Recordkeeping—Do you need the NAC device to keep extensive logs to comply with security standards such as PCI?

Cost

The cost of a NAC sytem ranges from free (that's right, free) to an amount that approximates the budget of a small country. It's unlikely that what you're looking for is at either extreme of the range.

It's worth noting that, although NAC cost varies with network size and capabilities, a good bit of the cost may also be for basic handholding—with the free NAC, you're on your own, whereas bloated NAC comes with an army of helpers and special classes.

Although cost shouldn't be your first consideration when choosing a NAC system, you should definitely shop around and make sure you're not paying for handholding and features you don't need.

Network Size

Most vendors rate their NAC systems according to how many users they support. This can be deceptive, because it's also important to look at how many subnets are in the network and how they relate to each other—ten users on the same subnet are entirely different than five users on a private subnet plus five users accessing the Internet over a public subnet.

The needs of a small organization and a large enterprise vary not only in the size of the NAC system they require, but also in the type they require. A very small network, for instance, can easily enforce NAC with a single in-line NAC appliance, whereas a large enterprise network would find in-line NAC practically impossible to implement.

A very small network of five or ten users can get by with a very basic in-line or out-of-band NAC appliance. In this range, ease of use trumps features, although a small network that's accessible for both public and private use will require VLAN capability.

Most small- to mid-sized networks can find an in-line or out-of-band NAC appliance to fit their network. Even some larger networks can find a NAC solution in multiple off-the-shelf NAC appliances that can be managed over the network. The larger the network is, the more practical out-of-band is as opposed to in-band. Also, as the network gets larger, NAC management features become more important.

NAC systems for very large enterprise networks are practically an entity unto themselves. When you start to get into these worldwide networks with many thousands of users, you're looking at specialized NAC integrated into the network structure. Enterprise NAC is very specialized and beyond the scope of this paper.

Network use

As important as the number of users on your network is the kinds of users on your network. If you have several groups of users that require access to different services and need to be kept secure from each other, you need a NAC system that supports virtual LAN (VLAN). The simplest example of this is a network that provides access to secure company servers for employees while simultaneously providing Internet access to visitors on the same network. Although employees and visitors are physically on the same network, the network they “see” is different.

Effectiveness

No NAC system is unbreakable, but some have more security holes than others and some have features that enhance the value of NAC.

802.1x is quite vulnerable in that a non-802.1x-compliant switch will let anyone into the network. A network using 802.1x-based NAC must be constantly monitored for non-compliant switches.

NAC systems that identify devices using MAC addresses are vulnerable to MAC address spoofing. Some NAC systems that use MAC addresses include algorithms to identify and prevent MAC address spoofing.

NAC based on agents trusts a client-based agent to report on the state of a device. Agents can be compromised or spoofed by malware, leading to the “lying endpoint” problem. Solutions to this problem are to be vigilant about virus and malware protection or to use an agentless NAC.

Many security products, including some NAC systems, check for Common Vulnerabilities and Exposures (CVEs) to keep their security coverage up to date. CVEs are cataloged in a dictionary of publicly known IT security flaws (http://nvd.nist.gov/).
A feature worth looking for in a NAC system is the ability to consult this database, scan the network, and send an alert if it finds a vulnerability. This ensures that known vulnerabilities are always addressed in a timely manner. Although scanning for CVEs isn’t, strictly speaking, a NAC function, a NAC appliance is ideal for this kind of job because it’s always keeping an eye on network assets. If a trusted asset has a CVE, it’s likely a target or already infected.

Form factor

NAC systems are available as software packages or dedicated NAC appliances.

Software-only NAC packages on the market tend to be very limited with far fewer features than appliance-based NAC.

They also tend to be very inexpensive—even free—although when considering a software-only NAC solution, consider not only the cost of the software, but also the cost of providing a server to run it on and the cost of labor to install and configure it. It’s best to look at NAC software as a sort of build-your-own NAC appliance kit.

Although it has limited capabilities and can require a great deal of time, software-only NAC does have its place. If you are, for instance, a non-profit organization with minimal security requirements, a donated server, and volunteer IT help, inexpensive or free NAC software could be a perfect fit for your needs. But a corporation with higher security requirements and extensive IT personnel would probably find one of these NAC solutions to be insufficient.

If you are going with a software-only NAC solution, don’t count out the free versions—just google “free NAC,” and you’ll find them. Free open-source NAC is still in its early stages but looks like it will do for the NAC marketplace what Linux did for operating systems. There are some serious drawbacks to open-source NAC—notably no tech support, no upgrades, and problems with interoperability—but with a bit of time and patience, it can be a good NAC solution.

Most NAC systems today come in the form of a dedicated appliance that combines hardware and software into one unit. Because the software is already installed, implementing NAC is easier with an appliance. Also, combining hardware and software into one appliance ensures that the NAC software is operating on suitable hardware.

But the primary reason to choose an appliance over software-only is that, as a group, these are far more capable NAC systems that usually include desirable features such as VLAN. A software-only system is often of the simple go/no go variety, whereas a dedicated NAC appliance can usually differentiate between different classes of users, decide which users can access which parts of the network, and direct out-of-compliance devices to a site that will help users bring them into compliance.

Administrative burden

The cost of IT personnel is a major consideration for most organizations. A NAC that eats up staff time is to be avoided, even if the up-front cost is minimal.

Long or complicated installation and configuration is a warning sign. Unless you have a worldwide enterprise network, if a NAC vendor tells you that setting up a NAC will take weeks or months or will require special classes for your IT staff, watch out. Although there are cases where a long installation time is justified, this can be a sign of a bloated, overcomplicated system that will eat up your staff's time.

If a NAC system requires software agents to be loaded on client devices, this will take staff time, although the chore can frequently be combined with other software updates.

Pay attention to what the NAC system can do for itself and how much the system relies on human intervention. Can the system automatically remediate connection problems and walk users through the steps they need to reconnect?

The NAC system you choose can have a huge impact on the productivity of your IT staff—you don't want a system that leads to increased help desk calls to have staff manually override access for users.

Hardware Fit

Some NAC systems are more adaptable to different network configurations. Look for a system that works with the network you have rather than one that makes you upgrade your network.

Because in-line NAC needs to be installed in the flow of network traffic, it can require a reconfiguration of your network. Out-of-band NAC is usually a better choice for established networks.

NAC systems based on 802.1x need 802.1x compliant switches. If you have older switches in your network, you will need to upgrade them to use 802.1x.

If your network contains a wide range of endpoints, including smartphones, VoIP phones, and network peripherals such as printers, you may not be able to use a NAC method that requires software agents to be installed on connected machines.

A brand-new network can more easily be configured to accommodate in-line NAC and 802.1x. Existing networks may need a considerable upgrade to work with some NAC systems. Some NAC systems don't work with devices such as smartphones or printers.

Recordkeeping

Look for a NAC system that keeps logs in an easy-to-access format. Good, searchable records enable you to see which users accessed which servers and which files, so if a security breach happens, you may be able to track down the culprit.

Another reason good recordkeeping is important is for compliance to various security standards. Depending on your industry, your organization may be required to comply with a security standard such as Sarbanes-Oxley, HIPAA, PCI, or ISO. One thing all major security standards have in common is that they require accurate recordkeeping.

Once you define your NAC requirements, it's time to wade through the vast number of offerings from many vendors to see which features match your needs.

Conclusion

NAC isn't a complete security solution, but it *is* an important part of your network-security arsenal, along with other measures such as physical security, user education, virus protection, and firewalls.

Many organizations perceive NAC as difficult and expensive. They worry about the lack of standards and about being locked into one vendor. They also worry about indirect costs in the form of downtime and burden on IT staff.

Although NAC is a new technology, it needn't be expensive or burdensome to implement. A bit of research and an understanding of what you're buying can give you the means to control network access in a time of proliferating mobile devices.

To learn more about the Veri-NAC network access appliance from Black Box, visit http://www.blackbox.com/go/Veri-NAC.

About Black Box

Black Box Network Services is a leading network solutions provider, serving 175,000 clients in 141 countries with 194 offices throughout the world. The Black Box catalog and Web site offer more than 118,000 products including network security products such as Veri-NAC network access control.

Veri-NAC is a network access control (NAC) system designed to provide maximum network security in a simple, agentless design. It requires no extensive training or dedicated personnel, no software agents, no network upgrades. Veri-NAC only lets computers and devices onto your network if they comply with criteria that you specify. It assembles a profile of each device and only lets known, trusted devices on the network. It can even detect and stop a machine trying to get in under a spoofed MAC address. Because of its agentless design and guaranteed compatibility with all existing LAN equipment, Veri-NAC has the lowest initial acquisition cost and lowest total cost of ownership.

Veri-NAC can also check to make sure each connected machine complies with your standards, including up-to-date operating system, patch management, and hardened configurations. If a machine isn't up to snuff, it can be locked out of the network except for the resources the user needs to bring the computer into compliance.

Unlike many other NAC systems, Veri-NAC doesn't require the installation of software agents on connected machines. This both simplifies installation and improves security because agents are vulnerable to hacking. It also allows you to secure devices such as smartphones, printers, and wireless access points, which won't accept an agent.

To learn more about Veri-NAC, visit www.blackbox.com/go/Veri-NAC or call us at 1-800-355-7996.

Black Box is also known as the world's largest technical services company dedicated to designing, building, and maintaining today's complicated data and voice infrastructure systems.