Chapter 1

Developing a Knack for NAC

In This Chapter

- Approaching network access control (NAC)
- Selecting the best approach
- Using your existing network infrastructure

Because you're looking at this book, you've probably heard or read all the hoopla about network access control (NAC). You've likely heard or read reports that NAC is the best thing since sliced bread, the be-all-and-end-all solution for network security or access control, and the best solution for network and device security since antivirus software and two-factor authentication.

Have you also heard that NAC isn't all it's cracked up to be? That it's costly, it takes a lot of time and labor to deploy, working with it can be trying, users don't like it, and it doesn't alleviate every network security and access control issue? Or perhaps that NAC doesn't provide you with a good return on your network security and access control investment?

You probably have at least one peer who told you that NAC isn't the only solution for all that ails networks and network security. And maybe you read or heard about the demise of the NAC market or product category — reports which have been greatly exaggerated.

Boy howdy, is this book for you!

In this chapter (and the whole book), you can discover

- What network access control (NAC) is — at least, according to many smart people and organizations
- The breadth of NAC
- How to home in on what makes the best NAC approach for your organization
- How some NAC solutions can enable you to leverage, repurpose, or reuse your organization's existing network infrastructure to deliver network access control, saving your organization time, costs, and labor — not to mention stress, sleepless nights, and gray hair!

NAC's Evolving Description

So, what's this network access control thing that you've been hearing and reading about?

First, NAC isn't the cure-all for whatever security or access control issues and challenges confront an organization and their network. But the right NAC solution, deployed appropriately, can deliver significant protection for

- Your network, its applications, and sensitive data
- Your users and their endpoint devices

The right NAC solution for your organization can protect against many (if not most) dangerous malware, nefarious hackers, and any malcontent users that the fast-paced, always connected, always on(line) networked world can throw at you.

So, NAC controls access to a network. Unfortunately, that simple definition and description is only partially right.

Many pundits, experts, and vendors find defining, or (more correctly) describing, NAC very difficult and elusive. You can find almost as many different descriptions of and meanings for NAC as organizations that have or want to deploy NAC, or vendors who produce or produced a NAC solution. But a definition exists that exactly fits your network needs — you just need to figure out which definition works for you.

To really understand how NAC works, consider this common — albeit painful, for some — metaphor to describe network access control: the airport!

The steps involved in operating network access control are, in many ways, similar to what happens when you go to an airport to board a plane for a trip:

1. You first stop at the ticket counter or self-service kiosk, where you need your confirmation number and a government-approved ID (such as your driver's license or your passport) so that the airline can authenticate your identity and confirm your reservation. You need to confirm who you are and that you're authorized to travel to your destination. A NAC solution does the same basic verification: It authenticates the user or device, and then checks the user's or device's authorization level to see whether that user or device has authorization to access the network. If your ID is valid, you have a confirmed reservation, and your name matches the name on the reservation, you receive a boarding pass, which means that you're authorized to travel on that flight. Similarly, NAC solutions match the user or device ID — such as a login user name

and password, two-factor authentication (which might include a token), or a smart card — to the authentication database or data store on the network to authenticate the user. If the NAC solution authenticates the user or device, that user or device receives the appropriate keys and credentials to access the network. If NAC doesn't authenticate, the user or device isn't allowed onto the network.

2. After the ticket counter, you have to go through a security checkpoint, including an x-ray machine and metal detector, before you're allowed into the secure area of the terminal gates. This is comparable to a NAC solution's endpoint integrity assessment or host check. In the same way that airport security checks you and your carry-ons for forbidden and dangerous items, NAC checks your endpoint device for any dangerous malware and potential vulnerabilities that hackers and other miscreants could exploit. If you or your baggage set off the metal detector at the airport, security may conduct a further search by hand or wand, if necessary. That extra search is like NAC's host checking of an endpoint device. If a NAC solution detects something amiss in the malware protection of your device, or detects an infection, it may instruct the network to quarantine your device until it can assess and address the anomaly or cure the infection. Then, the NAC solution's host checking can reassess your device before it allows or instructs an enforcement point to allow that device network access. Also, at the airport security checkpoint, security rechecks your ID and boarding pass, which is similar to a NAC solution rechecking authentication while it assesses (and, if needed, reassesses) your device's security state and integrity.

3. After you reach the secure zone at the airport, security can recheck you and your baggage for various reasons, including random security checks, if you're behaving strangely, or if you leave your suitcase unattended. Well, NAC solutions operate in the same way. Even after network admission — which is comparable to being allowed into the secure area — NAC can still conduct random assessment checks on you and your device to determine whether you still meet the organization's requirements to be on their network; or the NAC solution can recheck and reassess you or your device if it uncovers a state change in the security of your device while you're on the network. And, just like at the airport, if everything checks out okay, you and your device can remain in the secure area — or on the network. If the check finds something suspicious, then security (or NAC) may eject you from the secure zone (or deny you access to the network), subject to re-examination.

4. If an authority figure at the airport — a police officer, security agent or guard, or airline employee — feels that you're acting strangely or inappropriately, he or she may stop you and request your ID. He or she can even eject you from the secure zone or request a recheck on you and your carry-on luggage. On a NAC-equipped network, some NAC solutions can interoperate with existing network components, such as intrusion

prevention systems (IPSs), intrusion detection systems (IDSs), unified threat management (UTM)-enabled firewalls, or other network security components. And, if these devices deem that you or your device are exhibiting anomalous or bad behavior, they can signal the NAC solution. NAC can force you and your device into quarantine until you or your device stop the behavior, it addresses and solves the issue automatically (using automated remediation), or it is cured manually. NAC can also force you off the network in mid-session, not allowing you back onto the network until it clears you and your device.

5. The last step in your airport sojourn is the final check by an airline representative at the gate leading to the aircraft. The gate attendant checks your boarding pass and, in some cases, rechecks your ID to make sure that you're who you say you are (authentication), that you have a boarding pass (credentials), that your boarding pass matches the flight number and destination (authorization), and that your name on your ID matches the name on your boarding pass. This process is a lot like application access control on a network. Some NAC solutions can deliver applications access control, in which a NAC solution can recertify a user and device before that user and device can gain access to specific applications and servers, ensuring that only the properly authorized users can access certain specific, sensitive applications and data. For example, an air traveler named Adam may be authorized to take a particular flight to New York, but another flyer, Eve, has a boarding pass for a different flight number, so she can't board that particular flight to New York. A NAC solution delivers application access control in a similar way — only the correct users can access the applications and data.

What NAC is and what it does

Vendors, industry experts, and you may have difficulty in coming up with a common definition and description for NAC because a NAC solution has so many different components. Organizations have a tendency to focus on what problems NAC solves for them or why they want to deploy NAC. And the concept of network access control can include many different pieces of a network environment, or touch many different network entities or organizational departments.

When you factor in a network user's, vendor's, organization's, or individual's perspective when describing NAC — not to mention emotions, deployment, needs, and many other aspects — arriving at a commonly accepted definition or description for NAC becomes a jumble.

When you compare the components of NAC in the following sections, you might create a definition of what NAC is by what it does.

Endpoint integrity

One of the common core functions of a NAC solution involves running an *endpoint integrity* or *assessment check,* checking an endpoint device to ensure that endpoint meets a baseline of security and access control policies.

Policies

Policies are at the core of nearly every NAC solution. An organization can predefine their security and access control policies, or an organization can customize and define the policies they want to use. These policies usually focus on the actions and state of endpoint security products and software, such as antivirus, anti-spyware, anti-spam, or other anti-malware offerings; personal firewalls; host-based intrusion prevention systems (IPSs); specific operating-system and application patches and patch management; and other security-related offerings. Some NAC solutions can probe how vulnerable an endpoint device may be to attack or hack.

Assessment checks

The depth and breadth of integrity and assessment checks vary from NAC solution to NAC solution:

- Some NAC solutions simply check whether an endpoint device has loaded a specific product, or a certain set of security products or offerings. NAC may also check whether the device has turned on that product.
- Other NAC offerings probe much deeper, checking for the product and version name, the last scan time, when the device last updated the security product, whether the user has turned off real-time monitoring or protection, and so on.

Some NAC solutions check the security products of one or two vendors; other solutions check an assortment of vendor offerings and versions.

Extended assessment checks

A number of NAC solutions have extended endpoint device integrity and assessment checks that include operating system checks; checks for machine certificate values, specific applications, files, processes, port usage, registry, Media Access Control (MAC) addresses, Internet Protocol (IP) address; and other similar checks.

Other NAC solutions enable an organization to define and customize their own endpoint device checks that they want to include in their endpoint integrity and assessment check. Some solutions give you the ability to define an assessment check based on a specific industry or open standard. Others allow you to create your own specific endpoint assessment checks and write policies based on those checks.

Pre- and post-admission checks

The timing of an endpoint check can define a NAC solution, differentiating it from other solutions. Most NAC solutions check the integrity of an endpoint device and assess endpoint security before the endpoint device can connect to a network. This kind of check is usually called a pre-admission host or client check. However, some NAC solutions may perform these same checks periodically after an endpoint device gains admission to a network; these checks are called post-admission host or client checks. When using post-admission checks, some NAC solutions enable you to adjust or set the time for your endpoint-device integrity and assessment checks.

Some experts, vendors, organizations, and users define and describe NAC as the act of checking and assessing endpoint device integrity.

AAA

The acronym AAA, which stands for authentication, authorization, and accounting, is a common term in networking.

To authenticate a user or device, a AAA server ensures that the user or device is who he, she, or it says it is; in other words, the network asks, "Who are you?" The user or device has to prove identity.

Users and their devices can be authenticated in many ways, such as

- User name and password
- Two-factor authentication
- Smart cards
- Tokens
- Certificates
- Hardware-based authentication, such as the Trusted Platform Module (TPM), which the Trusted Computing Group (TCG) specified and standardized

The act of authentication is a must in today's networked world. Wherever you go, whatever network you attempt to access, that network needs to authenticate you. The network needs to know who you are *before* it grants you any level or form of network access. So, identity plays a vital role in yet another potential definition of NAC because NAC must keep track of differentiated access for different users.

In many NAC solutions, where and how a user accesses a network and its resources is dictated by that user's identity. In some solutions, NAC can also associate the user's identity with a specific role. That role determines what kind of access the user has to the network and its resources. For example, with some NAC solutions you can give guest users who attempt to connect to a network a different type of access than employees who access the same network. So, although an employee who accesses the network may have access to specific areas of and resources on that network, the guest user may receive access only to the Internet, not to any other region or resource on the network.

Some experts, vendors, and others define NAC by how NAC apportions access. But, access apportionment is only part of the definition of NAC because NAC encompasses so much more.

Control freak

Control is a vital part of network access control. Controlling admission to a network and controlling access while a user is on the network require similar but different capabilities. For instance, controlling admission to a network may be based on authentication, while controlling application access can be based on identity, authorization, and user roles. The ability to control the access of a user while he or she is on the network is a primary component of NAC — and, typically, a defining factor. Some NAC solutions can save you NAC deployment time and cost by allowing you to leverage existing access policies, working with appliances already deployed on the network (such as switches, wireless access points, firewalls, routers, and other equipment deployed as enforcement points within the network), or deploying new appliances to serve as enforcement points within the network environment. The enforcement points enforce the access control policies applied to users and devices, both pre- and post-admission to the network.

Evolving on the job

NAC needs to do more than just *control* network access. While threats evolve, NAC needs to adapt and evolve to protect against them.

For example, NAC solutions need to address application access control. *Application access control* is the ability of an organization to define policies that enable certain network users, and not others, to access specific, protected applications on their network. In effect, you can segment your network by using NAC.

You can base such access policies on user or device identity. Some NAC solutions can grant a specific user access to specific applications on a network based on that user's identity. Other NAC solutions determine where a user can go on a network, what applications that user may have access to, and how he or she can access protected resources based on a user's role. By identity-enabling application access, you can ensure that only the appropriate, approved users can access sensitive, critical applications and data on your network.

You can accomplish application access control by defining and enforcing access policies on the network that a NAC solution distributes, which routers and firewalls enforce to protect the vital network applications and resources. NAC solutions have made a huge evolution by addressing application access, and this evolution now enables organizations to best address regulatory compliance, for example.

NAC solutions also evolve by increasing visibility into, and monitoring of, user access. This extended user (and usage) monitoring and visibility can occur both when a user is attempting to gain network access and while he or she is on the network. Moreover, NAC solutions that include the ability to track users and their usage by user identity (such as user name) or a user's role on the network, are evolving faster than others. NAC solutions can address many situations (including regulatory compliance) if they can track users (particularly by user name or role, rather than simply by IP address), where those users go on the network, and what they use on the network. NAC that can track users by identity can also help address the growing scourge of insider threats by increasing the network visibility and monitoring into users already on the network, so organizations can more easily track users, and what those users are doing, throughout the network.

Your NAC solution needs to continue to evolve and expand its interoperation with other new or existing network security and infrastructure products, such as firewalls, intrusion prevention and detection systems (IPSs/IDSs), secure routers, security information and event management (SIEM) products, and so forth. Some NAC solutions can already interact with these devices, using the devices as access and security policy enforcement points to which the NAC solution pushes access control and security policies. But be sure your NAC definition includes that ability to evolve and expand.

NAC solutions can interact with IPS/IDS appliances, SIEM products, or other products that provide network behavior analysis (NBA) or deliver network behavior anomaly detection (NBAD). By using these products to locate, monitor, or address endpoint devices' irregular behavior on a network, you can mitigate threats based on signature and policy, as well as network behavior. But, when these systems and appliances can communicate with a NAC solution (and vice versa), NAC can then tie anomalous behavior to specific access

and security policies. Therefore, if a NAC solution that interacts with IPS/IDS, SIEM, or products that offer NBA or NBAD uncovers anomalous endpoint behavior, the NAC solution can propagate policies that address this situation to network enforcement points, and those enforcement points, acting on the policies created by and distributed to them by the NAC solution can shut down the user network session or disable user traffic through that port.

If the NAC solution leverages user name or role, rather than IP address, thus correlating the user name or role to the user's endpoint device and monitoring the user or device's path throughout the network, you can invoke access control and security policies specific to the user or device that's spewing the anomalous behavior through network enforcement points. You have many options open for how to handle a device that's acting anomalously. You can quarantine and remediate it; simply log its actions; or eject the device from the network (even in mid-session), forcing the user to manually remediate their device and reconnect to the network. By interacting and interoperating with additional network and security devices, and by using and referencing user and device identity and role (as opposed to an IP address), a NAC solution can better address insider threats, be more selective in how it handles certain behavior types, and be generally more effective to its organization.

The last word

Although you can find plenty of different types of NAC solutions available that may help define NAC, here's the reality: You may find defining and describing NAC difficult because NAC is a moving target.

How you define and describe NAC can depend on your perspective, the point of view of the user or organization deploying NAC, the issues that you want to address, and the features and functions that you or your organization want to implement. You can also define and describe NAC based on the vendor and the type of solution that the user or organization selects.

No one may ever come up with a single definitive definition or easy description for NAC. Think of NAC as what an organization wants or needs it to be. However, any NAC solution needs to be open and flexible, making it able to evolve so that it can meet ever-changing access control requirements and organizational infrastructure.

Throughout this book, we try to describe and define NAC, but you can draw only one conclusion — whatever your definition of NAC, you need to continue to extend it and allow it to evolve so that it can address the needs of a growing, shifting market and a constant, looming threat landscape.

A Diagram Is Worth a Thousand Descriptions

Although a picture is worth a thousand words, a diagram can help provide a visual definition or description of NAC — especially the different types of NAC solutions and deployment methods. In the following sections, you can find diagrams that illustrate different types of NAC solutions and deployment methods.

The different types of NAC solutions available include

- Appliance-based, divided by whether the appliance is inline or out-of-band
- Switch- or network equipment-based
- Client/host-based
- Agent-less or clientless

The various types of NAC deployment methods include

- Integrated with, or as an overlay to, network or security infrastructure
- Layer 2 or Layer 3 authentication

Appliance-based NAC solutions: Inline or out-of-band

Some NAC solutions are appliance-based, which means that a server, hardened appliance, or a network device of some type needs to reside in the network on which you want to implement the NAC solution. Appliance-based solutions are either inline or out-of-band.

An appliance may act as a policy server for the NAC solution, a receptacle in which an organization can define and manage network access and security policies, and then propagate those policies to NAC enforcement points on the network (out-of-band). Sometimes, instead of or in addition to the policies being propagated to enforcement points, these appliances may also enforce the policies. These network devices, whether inline or out-of-band, may also deliver authentication capabilities, such as serving double duty — working as both policy server and an authentication server; an authentication, authorization, and accounting (AAA) server; a RADIUS server; or even

a native authentication data store. These network devices can also include policy management, as well as device management, capabilities. What your NAC solution's policy server can do depends on whether the vendor's solution includes that functionality and capability within their appliance.

Get inline

If you use an inline NAC appliance that addresses policy development and management, and also enforces policies, all network traffic generally flows through the appliance or device, as shown in Figure 1-1. This placement enables you to make the access controls on an inline NAC appliance simple because all network traffic — and all associated individual data packets — flow through the appliance, thereby allowing the inline NAC appliance to apply granular access control.

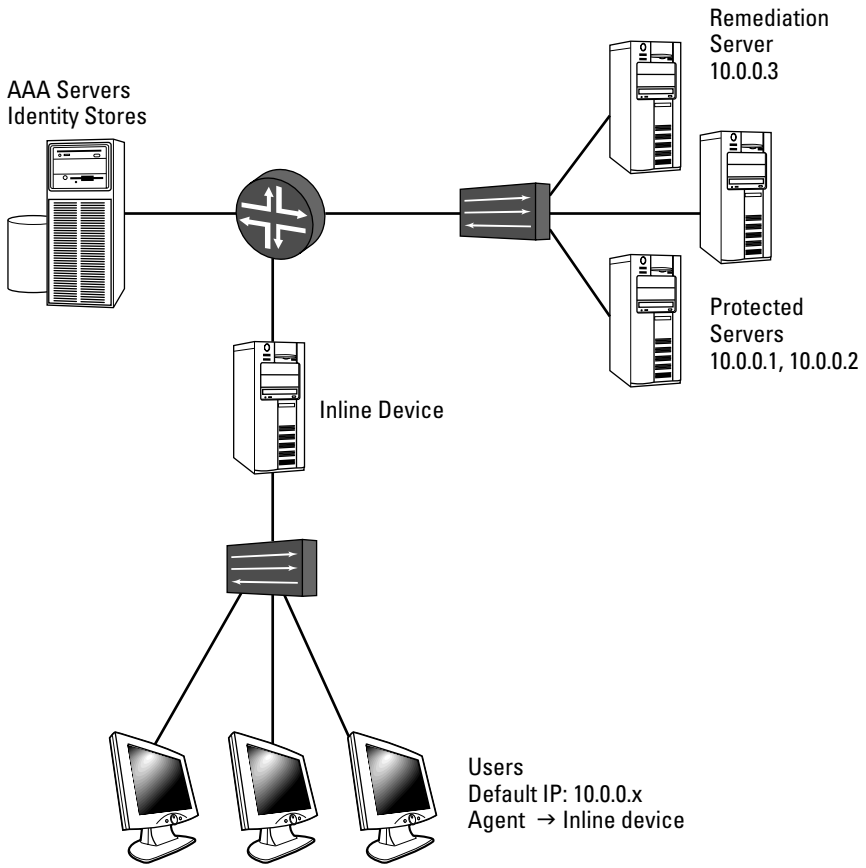

Figure 1-1: A sample diagram of an inline NAC solution.

You can easily deploy inline NAC appliances, particularly on a newly deployed or redesigned network. In many cases, these NAC solutions include a single network box that has policy creation and enforcement rolled into the one appliance.

While inline NAC appliances have their benefits (such as simplified deployment in new or renewed networks, a single-box approach, and policy enforcement and control in one place), be aware of a couple of potential challenges when you use an inline NAC appliance:

- **A single point of failure:** If the inline NAC appliance fails, so could network access control — because it's an inline appliance, it's applied to all network traffic. So, a failed inline NAC appliance could either create a roadblock that restricts access to your network or allow access to all who attempt to sign in to the network, without applying the appropriate policy and access control checks.
- **Performance:** Particularly in situations involving fast, substantial increases in network traffic, such as during disaster recovery, or mergers and acquisitions, the performance and rate of access control through an inline NAC appliance could suffer. Also, because all network traffic flows through an inline NAC device, that device can become a choke point in a network if too many users attempt network access simultaneously. To prevent your inline NAC appliance from becoming a choke point, you need to effectively load-balance the device and deploy it in a redundant fashion.
- **Scalability:** An inline, single-box solution can handle only a certain amount of network traffic; while network traffic increases, or the segments of the network on which you've deployed the NAC solution expand, you need to purchase more appliances and deploy them inline. You may not be able to easily maintain this kind of scaling solution or keep it cost effective.

Standing out-of-band

In an out-of-band NAC solution, you position the NAC appliance out of the line of fire of network traffic. Although some network traffic may flow to or through the out-of-band appliance, not all network traffic has to pass directly through it, as shown in Figure 1-2.

You can deploy both inline and out-of-band NAC appliances on an existing network infrastructure, but out-of-band NAC solutions typically are easier to deploy particularly because they are not in the direct line of traffic flow and many times do not require changes in traffic or network design. It can interact with the network components, leveraging them to provide authentication validation (by leveraging authentication data stores or databases), endpoint

security policies and updates (by leveraging antivirus or anti-malware policy servers), or policy enforcement (by leveraging switches, access points, firewalls, and so on). You can also deploy an out-of-band NAC solution as a separate appliance, away from an organization's network or security infrastructure, in an overlay deployment.

The NAC vendor can suggest where to place an out-of-band appliance, or your organization's deployment requirements can dictate this placement.

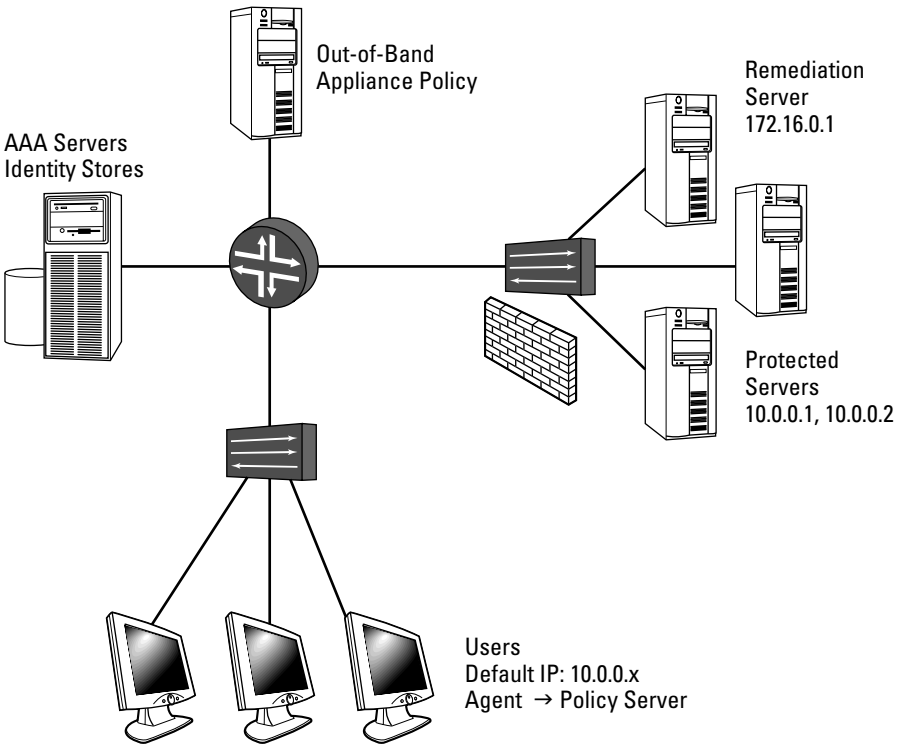

Figure 1-2: A sample diagram of an out-of-band NAC solution.

Out-of-band NAC appliances sometimes may also incorporate a client or agent, or a clientless or agent-less mode. The NAC appliance can deploy the client/agent to an endpoint device, either as a download or preload, to assess the device's security posture and health, returning the outcome of these checks to the appliance so that the appliance can dynamically incorporate that information into policy or consider it in setting policy. The out-of-band NAC appliance can also use some or all of these capabilities via a clientless or agent-less mode, if the vendor offers such a mode. A clientless or agent-less mode can be Web-based, use a captive-portal design (similar to what a user experiences

when he or she attempts to access the Internet from a hotel room or coffee shop), or be deployed by another method. A client/agent can also incorporate some security or access capabilities of its own as an added layer of protection for the user and organization against non-compliant or malware-infested endpoint devices. The client/agent may also serve a dual purpose, acting not only as a NAC host or agent, but also as an 802.lX client/supplicant that enables the user's device access to networks compliant with the IEEE 802.1X standard for port-based network access control, which we discuss in detail in Chapter 13.

Deploying an out-of-band NAC solution has several advantages over an inline solution:

- You can limit disruption on your organization's network and leverage existing network and security components as part of the NAC process.
- Out-of-band solutions usually scale more easily and quickly than inline NAC solutions.
- Out-of-band solutions allow for quicker, easier network changes because they aren't in the direct flow of network traffic, unlike inline solutions.
- In many cases, you can deploy them separate from existing network or security infrastructure.
- You can pair some out-of-band NAC solutions with inline, infrastructure, or other NAC solution types, as well as other NAC deployment scenarios, combining and emphasizing each other's capabilities while enabling and enforcing NAC from the edge of the network into the network's core.

Switch- or network equipment-based NAC solutions

A switch or network equipment-based NAC solution allows an organization to replace their existing switch or other network equipment deployment with a unit that has integrated NAC capabilities.

This type of solution can operate within an existing network environment, and if your organization is rebuilding an existing or creating a new network, you may find this kind of solution efficient. However, if your organization must rip-and-replace an existing switch environment to obtain NAC capabilities, this process could quickly become cost prohibitive.

Switch-based NAC solutions can deliver NAC capabilities to the network's edge, which enables an organization to implement NAC functionality (such as admission control, access control, and monitoring) from the edge of the network while maintaining performance. The devices can usually integrate within an existing network environment with little disruption; some devices

deliver and support multiple ways of enforcing NAC capabilities, such as 802.1X, DHCP, IPSec, or other standards.

Aside from the need to replace existing switches and equipment (which may be costly), this type of NAC solution may also have other hidden issues and costs. Keep these points in mind while exploring switch- or network equipment-based NAC solutions:

- Some switch-based NAC solutions require that you have an additional device — a controller, for example — on the network to provide policy control and management, which gives you another device that you need to manage.
- Like many products that combine multiple capabilities, you have to ensure that the device meets all your switching or network security requirements, not just your NAC needs.
- The device may meet your switching or network security goals but fall short of meeting your NAC requirements.

Client- or host-based NAC solutions

You can quickly and easily deploy client- or host-based NAC solutions. These software-based NAC solutions are usually independent of the network, its infrastructure, and (for the most part) any other equipment, as shown in Figure 1-3. (In many cases, a client- or host-based NAC solution requires a policy server to work with the client- or host-based NAC solution, delivering and managing the needed security and access policies.)

Your organization really needs only software to deploy a client- or host-based NAC solution. To implement NAC, you just have to preload, push, or automatically download the client or host software to an endpoint device. You can typically find this type of NAC solution available from vendors of endpoint security and protection software, and related suites.

Client- or host-based NAC, like all NAC solutions, has its pros and cons. On the pro side of the equation, client- or host-based NAC can

- Enhance interoperability.
- Be cost-effective while delivering solid investment protection and scalability.
- Address security challenges faced by a number of organizations today by combining admission control capabilities, such as endpoint assessment and policy compliance checks, with threat mitigation to protect the endpoint device and ultimately the network from attacks and hacks in economical fashion.

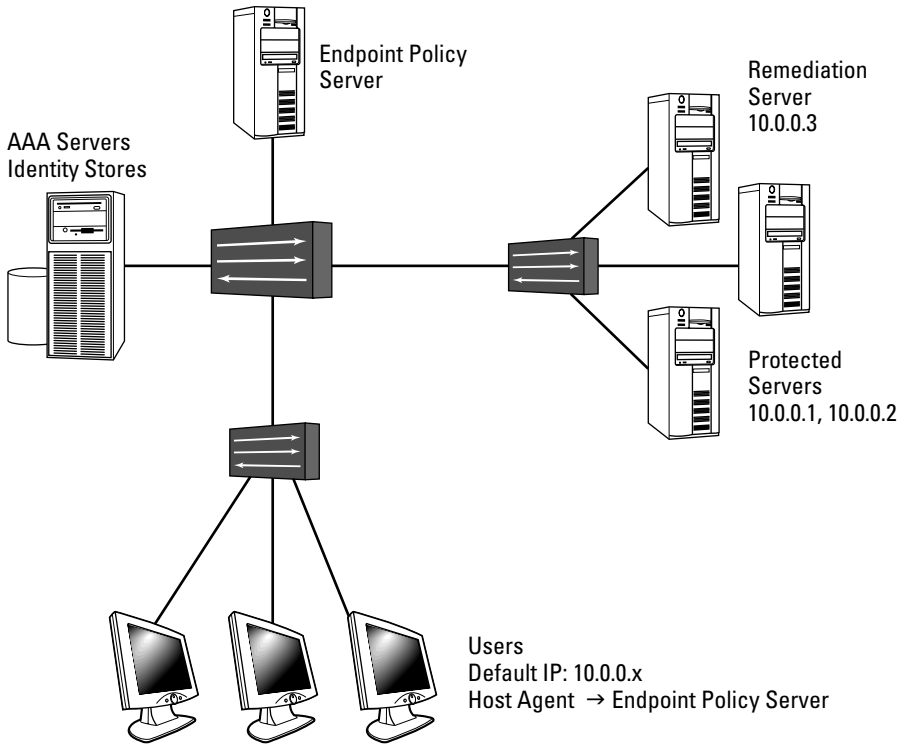

Figure 1-3: A sample diagram of a client- or host-based NAC solution.

On the downside of a client- or host-based NAC solution:

- **Quick spread of contamination:** If one user device is contaminated, compromised, or a *lying endpoint* (an endpoint device that's infected with malware which presents itself as being policy compliant and up-to-date with all its security inoculations), the organization's network is likely to become compromised, too.
- **How they handle unmanaged endpoint devices:** If a guest user — a contractor, partner, guest, or other non-employee user — attempts to access the organization's network by using an endpoint device that the organization hasn't provided or doesn't control (an *unmanaged* device), you may not be able to apply a client- or host-based NAC solution against that device. A guest user probably won't willingly agree to have an unknown client (particularly one that he or she may use only temporarily) downloaded to his or her endpoint device. So, how can a client- or host-based NAC solution check the unmanaged device and deem it compliant with the organization's access and security policies? Do you deny unmanaged endpoints network access? Do you funnel all

unmanaged endpoints attempting network access to quarantine? Or do you allow unmanaged endpoints to freely access your network? And which scenario is more painful? As you can see, guest users and unmanaged devices can be real issues for client- or host-based NAC solutions.

- **Relying only on software on an endpoint device to provide network access control across a network:** A client- or host-based NAC solution can sometimes limit network security. In many cases, by deploying a client- or host-based NAC solution, an organization is attempting to check out and secure the endpoint device at the same time it is also providing the base for the NAC solution.

Clientless NAC solutions

Clientless NAC solutions don't require an endpoint device to have a client loaded in order for the solution to assess the device pre-admission, or for the solution to provide user or device authentication.

Some of these NAC solutions use a Web-based, captive portal-like approach or a dissolvable client that's based on Java, Active X, or some other downloadable applet that can capture user and device credentials for authentication, assess endpoint security state and posture, and measure the device against access and security policies.

Some clientless NAC solutions must deploy a device on the network that monitors network traffic and determines whether a device attempting network access is managed or unmanaged, or whether it's *unmanageable* (a device that's incapable of accepting a client, dissolvable or not, such as a networked printer, cash register, HVAC system, even a vending machine) — essentially, any device connected to the network and that has an IP address. Using predefined policies, the clientless system that uses a network device decides how to handle the network disposition of the unmanageable device.

Types of deployment

There are differing methods of NAC deployment which you may have the option of choosing, or that may be required based on the type of NAC solution you select.

While there are key differences between the various NAC deployment methods, one thing they all have in common is the ability to control access to the network (and in some cases applications) based on a number of variables and settings.

Integrated or overlay

Whether you deploy a NAC solution as an integrated part of a network or as an overlay to network or security infrastructure, for the most part, depends on the NAC solution type that you select.

You usually have to deal with either integrated or overlay NAC deployment when you use any NAC solution type that incorporates or leverages an appliance or network box. If you don't need an appliance or a network component, then you usually don't have to worry about the integrated versus overlay deployment choice.

For example, although you may or may not have an out-of-band NAC appliance integrated within your network environment — it may also be deployed as an overlay to the network environment, ensuring that any changes to the NAC solution or to the network environment don't affect the other — you need to integrate an inline NAC appliance with the network infrastructure, particularly because the inline appliance must be in the network traffic flow to operate.

You first need to determine whether the NAC solution type with which you want to work can support integrated or overlay deployment. If the deployment can be either integrated or overlay (such as when you use an out-of-band NAC appliance solution), then you can decide how intrusive and integrated you want to make your NAC solution.

Sometimes, though, the choice of integrated or overlay comes down to the type of NAC enforcement that an organization selects and uses.

Layer 2 or Layer 3 enforcement deployment

Layer 2 and Layer 3 refer to the data link layer and network layer, respectively, on the Open Systems Interconnection (OSI) Basic Reference Model, which provides a graphic description of computer network communications and protocols.

The data link layer (Layer 2) facilitates the communications and transfer of information between network components. (The IEEE 802.1X industry standard for port-based network access control also operates at Layer 2. Many Ethernet switches and wireless access points deployed in networks around the world today support the 802.1X industry standard.)

Many NAC solutions use Layer 2 as a key enabling technology and the standard for policy enforcement on NAC enforcement points, such as switches, wireless access points, and similar devices. Layer 2 communicates with NAC components during authentication and policy enforcement processes, as shown in Figure 1-4.

Layer 3, the network layer in the OSI Basic Reference Model, provides the means of transferring data from a source to a destination over one or more networks. Also, network routing occurs in Layer 3. Some NAC solutions use a Layer 3 access and security policy enforcement model. This model typically leverages a firewall or a secure router as a NAC enforcement point, enforcing policy-based decisions about how to handle certain users, devices, and even network traffic, as shown in Figure 1-5. A Layer 3 NAC deployment is a strong overlay NAC deployment capability, as well.

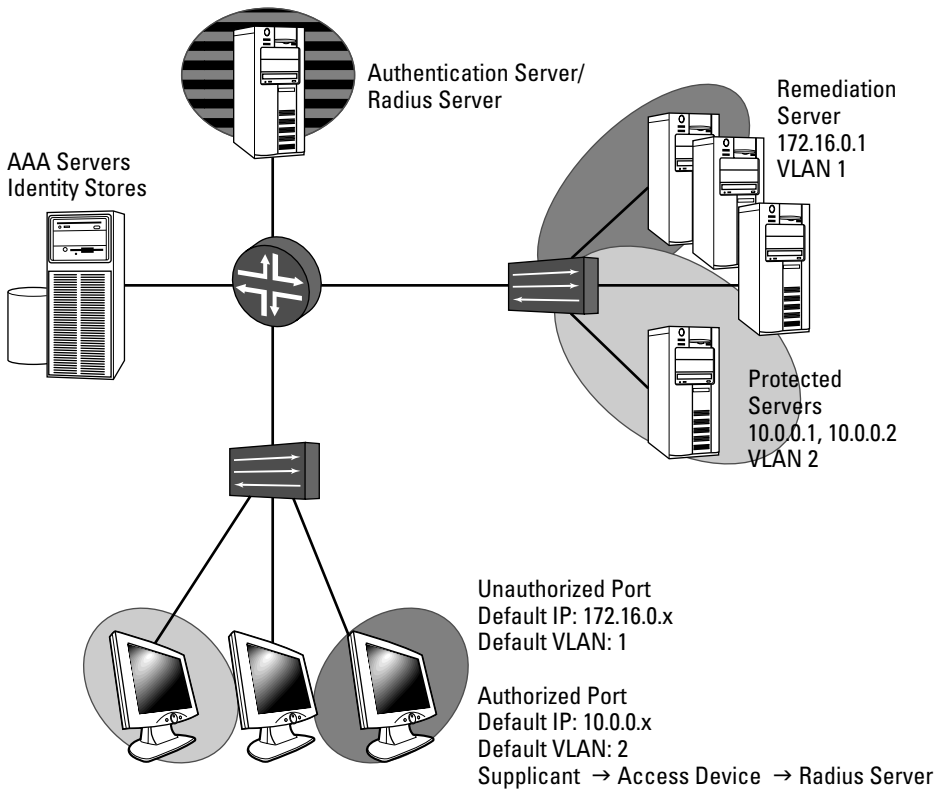

Figure 1-4: A sample diagram of a Layer 2 NAC deployment.

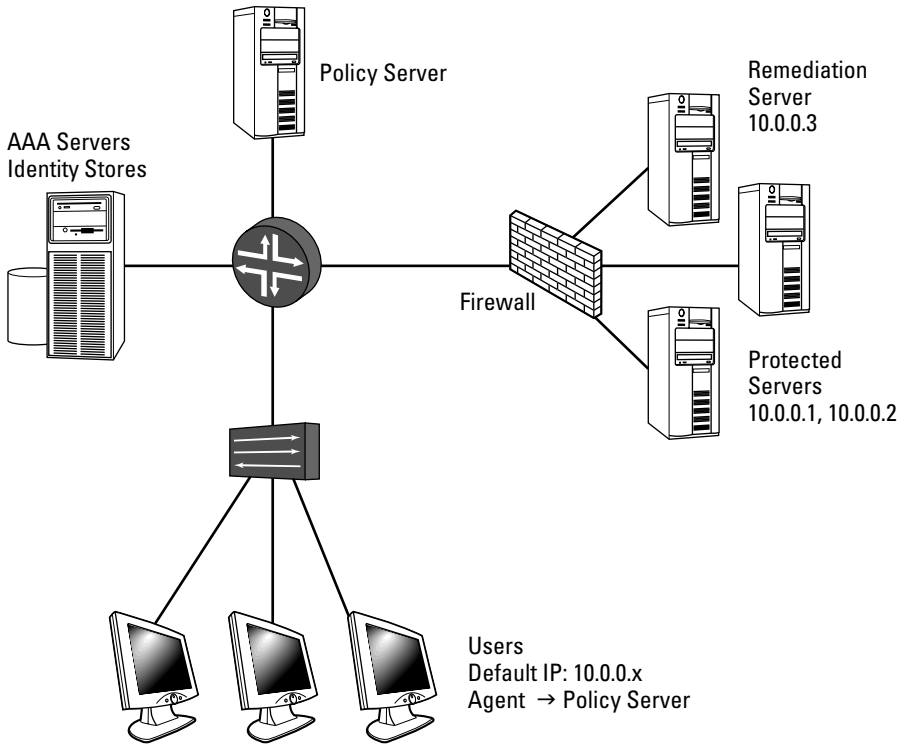

Figure 1-5: A sample diagram of a Layer 3 NAC deployment.

The Best NAC Approach

So, how do you decide the best NAC solution approach for you, your network, and your organization? How do you select a solution to best meet your access control needs, without forcing yourself to redesign or redefine your network?

No one offers a single, be-all-and-end-all NAC product. First, you and your organization must decide what area or areas of your network you need to secure, as well as what issue is the most dangerous to your organization, network, and resources. A NAC solution can address these kinds of needs:

- Giving guest users secure, appropriate access to your network, while protecting your key resources and IP
- Differentiating access for different user types, such as employees, contractors, partners, and guests

- Protecting sensitive data and intellectual property from unauthorized access
- Minimizing the fear of an insider threat
- Addressing regulatory compliance and preparing for compliance audits

Your organization first needs to consider whether a particular NAC solution can handle the different device types that will be trying to access the network. Any comprehensive NAC solution should seamlessly address employee or guest user authentication and endpoint compliance *before* it grants a user, and his or her endpoint device, access to a network.

Do your NAC homework

Regardless of the issue or issues that your organization prioritizes — what parts of the network your organization wants to control access to, from whom, and for whatever reason — you need to research and answer all these questions *before* you decide on the NAC solution type, vendor, and product that you want to review or purchase.

Walk through these simple steps:

1. **After you determine that you need NAC, figure out whether budget is, or could become, an issue.**

   Your organization may choose to leverage existing infrastructure, existing endpoint security software, and so on in an effort to maximize efficiencies, maintain costs, and protect existing network investments. If cost is an overriding issue, and scalability and performance aren't as vital, your organization may consider implementing certain NAC solution types, such as an inline NAC appliance that can deliver both a policy server and an enforcement point in a single networked box, a switch-based NAC solution, or client- or host-based NAC.

2. **Decide whether network and resource security is your organization's key concern.**

   If you want the ability to leverage existing network components, but also effectively segment your network so that you can allow only authorized users to access sensitive data and intellectual property, then your organization may need to investigate an out-of-band NAC appliance that has strong Layer 2 and Layer 3 enforcement capabilities.

3. **If your organization is concerned with guest user access, investigate NAC solutions that include a client-less or dissolvable client option.**

We describe these options in the section "Clientless NAC solutions," earlier in this chapter.

4. **Figure out whether your organization is most worried about keeping the wrong people off of the network and away from valuable resources and information.**

   In this situation, consider a NAC solution that supports strong two- or multi-factor authentication.

5. **If ensuring the security of critical networked resources keeps you up at night, then you need a NAC solution that focuses on the segregation of networked resources.**

   This kind of solution ensures that only the correct, authorized users who have the appropriate authority and access rights can access the critical resources.

6. **Determine what use cases are the most important for your organization.**

   If your organization needs to address regulatory compliance, outsourcing or even off-shoring, or business continuity during times of disaster, you can find a NAC solution that can address this for you.

Must-have traits of your NAC solution

Whatever your NAC needs, you can find a NAC solution, deployment type, and environment that can well address your security and access control needs. Just know about any limitations that your NAC solution has and take those limitations into consideration before purchasing the solution.

Absolutely, positively ensure that you find the following attributes and capabilities in any NAC solution that your organization reviews or selects.

Strong user/device authentication and integrity

NAC solutions usually combine two types of checks — user identity and endpoint integrity. A NAC solution, though, should be able to combine user identity, device integrity, and location information with policy to deliver dynamic, comprehensive NAC.

Dynamic identity- and role-based policies

A NAC solution should define policies based on user and/or device identity, as well as the user's role, which a NAC solution should predefine for the user. Also, a NAC solution should be able to create policies on the fly, dynamically, so that if endpoint device integrity, user or device identity, or other factors change, the solution can assign a new policy and take the appropriate actions to ensure network and resource security and integrity. You need the ability

to know who's on your network — as well as where they're going and what they're doing — particularly if you have to worry about regulatory compliance and audits. Tracking users and devices by IP address just isn't enough any longer.

Complete network protection

The NAC solution that you choose should be able to deliver a rich set of predefined endpoint integrity checks, as well as the ability to create custom endpoint checks right out of the box. It should also be capable of making dynamic network status changes if the endpoint device's security state, network information, or user information changes — even if the changes occur in the middle of a network session. Your NAC solution must enforce dynamic policy in real time across a distributed network. And any NAC solution that you select needs to effectively address the quarantine and remediation of an offending user, and his or her device, prior to granting network access. You also want a NAC solution that includes automatic or automated remediation, in addition to self-remediation capabilities.

Network and application-level control, visibility, and monitoring

If your organization must comply with industry or government regulations, then you really need to ask whether, and how, the NAC solution can accomplish this compliance. The best NAC solution simplifies adherence to regulatory compliance requirements, as well as providing the required security for and necessary data to prove compliance with industry and/or governmental regulatory requirements. A NAC solution also needs to address application access control, which enables an organization to apply user and/or device level policies for access to sensitive or protected applications, limiting access to critical data to only authorized users and devices. A NAC solution that addresses application access control can also provide a quick, effective way to virtually segment your network. Finally, any NAC solution today must have the ability to provide visibility into and monitoring of users and devices attempting to access a network and its applications. The ability to match user identity and role information with network and application usage enables the NAC solution to better track and audit network and application access. Plus, a NAC solution can leverage and use a user's role when determining access control policy.

Robust extended security

Consider whether the NAC solution leverages your investments in existing access and security devices. Your NAC solution needs to work with your existing firewalls, Ethernet switches and access points, and AAA infrastructure. Your network access control solution shouldn't require costly, time-consuming upgrades or a rip-and-replace scenario. Any NAC solution should integrate quickly and seamlessly with your existing AAA infrastructure to validate user identity. Your NAC solution should also deliver interoperability with existing network and security infrastructure components, effectively

extending NAC capabilities to include intrusion prevention systems (IPSs), security information and event management (SIEM) solutions, and other vital network infrastructure components to deliver investment protection and comprehensive NAC.

Flexible, phased deployment and ease of operation

When you look at NAC solutions, consider what you need to deploy the solution. Most organizations are best suited to a phased deployment approach to NAC. Flexibility in your NAC solution is vital because a network is fluid, not static; your NAC solution should be able to change with and adapt to your network while that network grows and changes. The NAC solution should be able to add an additional enforcement method without requiring you to rip and replace the network that you've already deployed. One of the best ways to ensure this level of interoperability is to seek solutions that are based on open specifications and standards.

Simple administration and management

Consider the ease of administration and management of a NAC solution when you select a solution for your organization. You can determine a NAC solution's ease of administration by considering whether you can use existing network management capabilities to manage that NAC solution. Can solutions or access control devices share or reuse security and access control policies? Does the NAC solution have a centralized management console that can aid in administering and provisioning various solution and/or infrastructure components? Also take into account how easily the NAC solution can create or edit policies, or deploy endpoint integrity checks, and whether the solution can predefine host checks or policies.

Value

The value that you can get from a NAC solution combines factors of deployment flexibility, ease of use, the time that you have to spend administering and managing the solution, the actual acquisition cost, and the time that you need to spend redesigning your network (if required). What security or access control components or policies can you leverage, reuse, or repurpose on your network to help enforce NAC? If a solution requires that you upgrade your switching infrastructure, you must also factor in the time you have to spend inventorying the devices on your network, determining what types of switches you already have deployed, and what version of code they're running; getting hardware and/or software upgrades, as required; and testing the network. You may find a phased approach to deployment easier to justify to your organization or management because it can save valuable time and expense. Be aware that you can easily deploy some NAC solutions in a phased manner, but you can't so easily deploy others in this way.

Leveraging What You Have Today

If you can leverage pieces and components of your existing network to deliver NAC, you can save time and expense when deploying a NAC solution.

Ensure that the NAC solution you review or select can leverage your existing network, policy, and reporting capabilities and resources as much as possible; work across standards and different platforms; and save yourself some headaches and a lot of wasted time and cost. The rest of this book shows you how.

You can use your existing network infrastructure, endpoint security software, security products, and other network hardware or software for NAC by considering any of the points in the following sections.

Standards

If you want to use the network that you have today to address NAC, you first need to determine whether the NAC solution that you're considering incorporates or uses industry standards; for example, the IEEE 802.1X standard for port-based network access control, which we cover in greater detail in Chapter 13. If the NAC solution that you're considering or reviewing utilizes the 802.1X standard and can work with an existing 802.lX network by leveraging 802.1X-compliant switches and wireless access points already in the network as NAC enforcement points, you've just leveraged a very vital — and expensive — portion of your existing network infrastructure. The more components that you can leverage on your existing network to deliver NAC, the more easily you can deploy NAC — and for less money. And, NAC doesn't just reuse or leverage existing network hardware, either.

Reuse policies

If you already have access control policies in place, repurposing or even copying those policies so that you can use them on your NAC solution can save you valuable time in policy definition, as well as in NAC deployment time and expense. For example, if you already have remote access or endpoint security policies defined and deployed, you can leverage them again in your NAC solution, which could save you a significant amount of time. Your staff, who might have needed to redefine, rewrite, or create new security policies if they couldn't be reused or repurposed, can instead address more pressing or strategic needs.

Interface with existing systems

The ability of a NAC solution to simply interface with your existing authentication systems or AAA infrastructure can save you a great deal of time and cost. Imagine that you have to duplicate your user database, which you've already spent time creating, redefining, and updating for your existing network access methods, for your NAC solution. You can save all that time, effort, and resources — and use those administrators to address other, vital projects — simply by ensuring that your existing authentication data stores can be leveraged as-is with your NAC solution.

Reporting

A hidden area of reusability — and one that some organizations seldom think about — is reporting. If you already have a series of reports defined and use an external reporting solution or an SIEM device, you can find your NAC solution's inability to interface or interoperate with those devices or to export information into existing report templates maddening — especially if you didn't even think about this sometime neglected, but very important, consideration before purchasing or deploying a NAC solution.