This chapter covers the following topics:

- Introduction to Network Admission Control
- Review of NAC Phase I and Phase II architecture
- Overview of the components that make up the NAC Framework solution, including:
  - Cisco Trust Agent
  - Cisco Security Agent
  - Network-access devices
  - Cisco Secure Access Control Server
  - Event monitoring, correlation, and reporting

CHAPTER 1

NAC Solution and Technology Overview

One of the biggest challenges corporations face today is securing the internal network. When the words *network security* are mentioned, most people immediately associate this phrase with protecting their network from external threats. Few people think of the internal threats that already exist. Unpatched end-host systems, out-of-date antivirus signatures, and disabled or nonexistent personal firewalls all weaken the internal security of corporate networks and make them vulnerable to data theft and attacks. Preventing or limiting these hosts' access to the corporate network has been difficult to do until now.

Cisco Systems has launched the Self-Defending Network Initiative (SDNI) to dramatically improve the network's capability to identify, prevent, and adapt to threats. A key part of this initiative is Network Admission Control (NAC). NAC is a multipart solution that validates the security posture of the endpoint before admitting it on the network. If admitted, NAC can also be used to define what resources the endpoint has access to, based on the endpoint's overall security posture.

This chapter is meant to provide you with an overall review of the NAC Framework solution. We start by covering what NAC is and why companies would want to deploy it. Then we cover an architectural overview of the initial NAC solution (NAC Phase I), followed by an architectural overview of the current NAC solution (NAC Phase II). In the remainder of the chapter, we provide an overview of the individual components that make up NAC. Each component has a dedicated chapter in this book where we cover the installation, configuration, and steps to troubleshoot that component in the NAC solution. After reading this chapter, you should be familiar with the concepts and components that make up the NAC Framework and should be ready to start installing and configuring NAC in your network.

If you are unfamiliar with NAC or are interested in learning more about the architecture of the NAC solution, we invite you to read *Cisco Network Admission Control, Volume I: NAC Architecture and Design* (ISBN 1587052415), published by Cisco Press.

Network Admission Control

Reports of data and identity theft have become hot topics in the news recently. Unfortunately, they have also become fairly common, often resulting in millions of dollars' worth of damage to the companies affected. Traditionally, network security professionals

have focused much of their time securing the front door to their networked companies—their Internet presence. Stateful firewalls often sit at the gateways, and, in most cases, these are supplemented with inline intrusion-prevention devices (IPS), antivirus scanners, and denial-of-service (DoS) mitigation devices. Behind this virtual fortress of protection sit hardened servers, which serve up the corporate web presence. Many companies are proud of their investment in this type of security and advertise this fact. Now, don't get me wrong—this type of security is important. However, sometimes in the zeal to make the web presence secure, we forget that a huge threat exists from within.

It is becoming mandatory these days for employees to have access to the Internet; often it is a critical component of their jobs. However, have you thought about devices that your employees are using to access the Internet? How secure are they? If they are corporate assets, they should have the corporate antivirus software installed and possibly a personal firewall. But how do you know the employee has not disabled one or more of these and thereby reduced the security of not only the device, but also your internal network, and opened it up to threats?

While you are pondering that thought, let me give you another. How many noncorporate assets connect to your network? How many employees bring in their personal laptop, their personal digital assistant (PDA), or even their cell phone and connect it to the corporate network? What about partners and outside vendors? How much control do you have over these devices? Imagine what could happen if a rootkit or some other Trojan back door was installed on one of these devices and now has access to your internal network. How many confidential documents or corporate secrets could be stolen by attackers within?

It is often easier to consider the mistakes or ignorance of others, but how many times have you been guilty of letting the security of your own PC lapse? How many times have you been notified of a new critical security patch for your laptop or desktop and clicked the Not Now button, choosing instead to install it later? I am sure all of us are guilty of this; I know I am.

Installing security patches, especially to the operating system, usually results in the mandatory reboot. This usually comes at the worst time of the day, when shutting down your applications and rebooting is not an option. So we make a mental note to install the patches when we leave for the day, but how many times do we actually follow through? More often than not, weeks or months could go by before we find the time to install the patches. During this time, the PC remains susceptible to the targeted attack.

Although I have highlighted only a few of the common threats to the internal security of your corporate network, I am sure you can think of many more. Home users connecting via a VPN tunnel, remote sales forces connecting from the local hotspot or hotel, partners with direct site-to-site tunnels to your company—the list goes on. These are the types of threats NAC was designed to protect you against and eliminate.

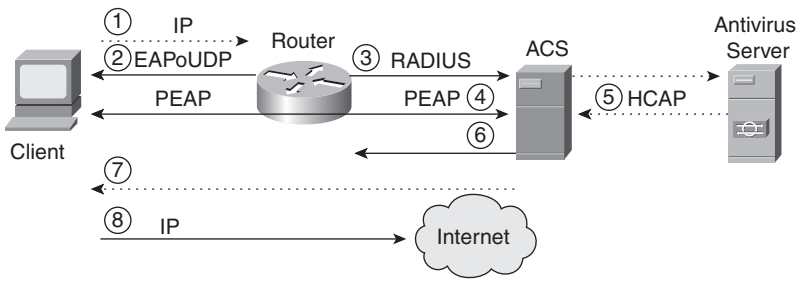
NAC is a Cisco-led, multivendor initiative focused on eliminating threats to the corporate network caused by insecure endpoints attaching to the network. In its simplest form, NAC

defines a set of policies that are used to evaluate the security posture of an endpoint that wants to join the network. The endpoint can be a PC, a PDA, a server, an IP phone, a printer, and so on. Based on the security posture of the endpoint, it can be given unrestricted access to the network—if it meets all the security requirements. Devices that fail to fully satisfy the security requirements can be quarantined where autoremediation ensues. (Remediation servers can automatically push out patches and updates to software running on the endpoints to improve their security posture.) Alternatively, devices can be denied access to the network altogether, or they can be placed in their own VLAN and given limited access to the network. All of these actions are fully configurable, along with the security policy to be enforced.

NAC: Phase I

Cisco rolled out NAC in a series of phases. Phase I was launched in the summer of 2004. It includes using Cisco routers as the enforcement point, running Cisco IOS Release 12.3(8)T or later. When NAC is deployed on Cisco IOS routers, it is called NAC-L3-IP because the router operates at Layer 3 (the IP layer) and contains noncompliant endpoints using Layer 3 Access Control Lists (ACLs). As endpoints attempt to access devices through the router, they are queried to determine their security posture. Based on the endpoint's security posture, a security policy for the endpoint is pushed down to the router that permits or restricts access. Figure 1-1 shows a NAC-L3-IP architecture overview.

Figure 1-1 *NAC-L3-IP Architecture Overview*



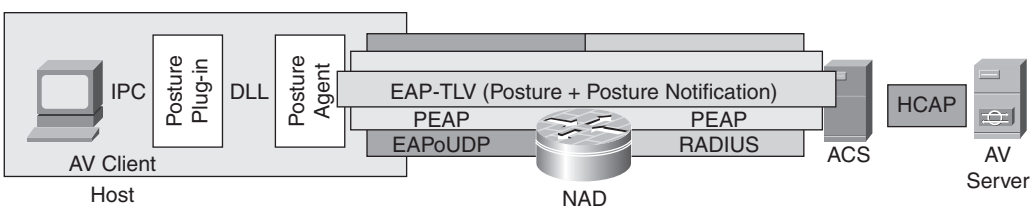
Follow along in Figure 1-1 as we walk through each step of this process:

1. The endpoint sends a packet, which passes through the router, on to its destination. The packet matches the *Intercept ACL* applied to the router's interface, which triggers the NAC-L3-IP posture-validation process.
2. The router initiates an EAP over UDP (EAPoUDP) tunnel to the Cisco Trust Agent (CTA) on the endpoint. This is the first part in setting up a secure tunnel between the endpoint and the Cisco Secure Access Control Server (ACS).

3. Next, the router initiates a RADIUS tunnel to the Cisco Secure ACS server. This is the second part in establishing a secure tunnel between the endpoint and Cisco Secure ACS.
4. With the EAPoUDP and RADIUS tunnels established, the Cisco Secure ACS server establishes a Protected Extensible Authentication Protocol (PEAP) tunnel with the endpoint and queries it for posture credentials. The posture credentials are sent to Cisco Secure ACS using EAP type-length-values (EAP-TLVs). The EAP-TLVs allow for any number of posture credentials to be returned from the end device.
5. (Optional) Cisco Secure ACS proxies some of the posture credentials to additional validation servers (in this case, an antivirus server) using the Host Credentials Authorization Protocol (HCAP).
6. Cisco Secure ACS analyzes the end host's security posture by passing the posture credentials through rules, defined by the administrator in Cisco Secure ACS, or by sending them to external posture-validation servers. The host is then assigned an overall security posture, based on those results. The overall security posture is then forwarded to the router, along with the associated access list, which restricts the host's access to the network, based on its security posture.
7. (Optional) Cisco Secure ACS can also send a message to the endpoint, which, in turn, is displayed to the user to provide notification about the security posture of the host. Cisco Secure ACS can also redirect the user's browser to a remediation server, where patches and updates can be applied.
8. If the host is deemed "healthy" (its security posture meets the requirements of the company), it is permitted to access the network unrestricted.

The protocols used in Figure 1-1 are discussed in more detail in later chapters. For now, it is important to know only that the posture credentials and security policy are carried over authenticated and encrypted tunnels for added security. Figure 1-2 illustrates the relationship among these protocols in a graphical way. The PEAP-encrypted tunnel is carried over both the RADIUS and EAPoUDP tunnels. It contains the EAP-TLVs used to determine the host's posture.

Figure 1-2 *Graphical Representation of Protocols Used in Phase I NAC*



NAC: Phase II

Cisco launched NAC Phase II in the summer of 2005. Phase II expands on Phase I by placing NAC capabilities into several more product lines, including the Catalyst line of switches, the VPN 3000 series concentrators, the ASA 5500 series and PIX 500 series security appliances, the Aironet wireless access points, and the Wireless LAN Service Module. With these new additions, the enforcement point has moved to the network edge, providing enforcement and containment at a port (or host) level instead of at the gateway. These additions also created some new terminology:

- **NAC-L2-IP**—The term *NAC-L2-IP* is used when NAC is applied to a Catalyst switch, on a per-port basis. You can think of NAC-L2-IP as being identical to NAC-L3-IP, but the enforcement policy is an IP-based ACL applied to a switch port instead of a routed port. Likewise, the protocol flow as defined in Figure 1-1 is the same for NAC-L2-IP.

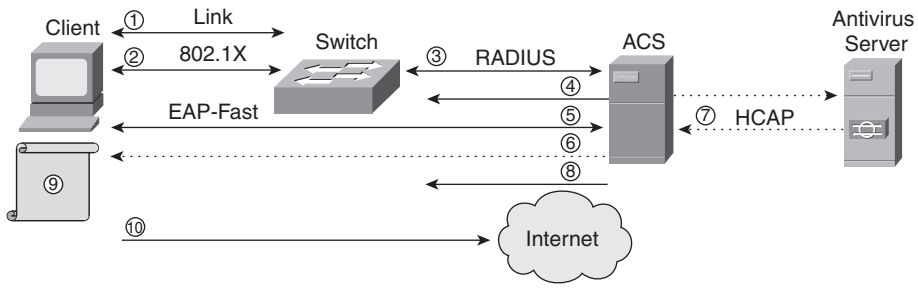
  One other difference between NAC-L2-IP and NAC-L3-IP is that, in NAC-L2-IP, the posture assessment is triggered when the switch port receives a Dynamic Host Configuration Protocol (DHCP) packet or an Address Resolution Protocol (ARP) packet from the endpoint attempting to connect to the network. Then the switch establishes the EAPoUDP tunnel to the endpoint to start the posture-validation process.

- **NAC-L2-802.1X**—The term *NAC-L2-802.1*X is used when NAC is applied to a switch port along with 802.1X authentication. 802.1X provides for both user- and machine-based authentication of the endpoint before the switchport forwards any traffic to the network. NAC-L2-802.1X adds security posturing to 802.1X by way of the Extensible Authentication Protocol–Flexible Authentication via Secure Tunneling (EAP-FAST) protocol. Thus, the posture credentials are carried through EAP-FAST over a Transport Layer Security (TLS) tunnel from the endpoint directly to Cisco Secure ACS. Consequently, an 802.1X supplicant that supports EAP-FAST is needed for NAC-L2-802.1X.

  When NAC-L2-802.1X is enabled and a PC is connected to a switch port, 802.1X authentication and posture validation occur within the same EAP transaction. The posture credentials are included within the EAP-FAST messages that are transmitted on top of the 802.1X protocol. However, unlike NAC-L3-IP and NAC-L2-IP, posture enforcement is done not through ACLs but instead solely through VLAN assignment.

Figure 1-3 illustrates NAC-L2-802.1X on a switch that uses 802.1X authentication as the Layer 2 protocol.

Figure 1-3 *NAC-L2-802.1X Architecture Overview*



Follow along in Figure 1-3 as we walk through the process of what happens when an endpoint connects to a switch with NAC-L2-802.1X enabled on the port:

1. The end device is attached to a switch port.
2. As the link comes up, the client's 802.1X supplicant initiates an authentication request with the switch via 802.1X.
3. The user's (or machine's) credentials are sent from the switch to the Cisco Secure ACS server via RADIUS.
4. The Cisco Secure ACS server authenticates the user (or machine).
5. CTA and Cisco Secure ACS now establish an EAP-FAST tunnel over the existing 802.1*x* and RADIUS sessions.
6. The Cisco Secure ACS server queries CTA for posture credentials using the EAP tunnel.
7. (Optional) Cisco Secure ACS optionally proxies some of the posture credentials to additional validation servers (in this case, an antivirus server) using HCAP. These validation servers can notify the agents on the endpoint and trigger their own updates.
8. Cisco Secure ACS applies the security policy to the retrieved posture credentials, and the host is assigned an overall posture. This security posture is forwarded to the switch along with the associated VLAN to be applied to the port the host is connected to.
9. (Optional) Based on the posture credentials, Cisco Secure ACS can send a message to the end host to be displayed to the user or can redirect the browser to a remediation server. The remediation server can automatically push out patches and updates to the endpoint to bring it in compliance with the corporate security policy.
10. The host is now permitted (or denied) access to the network, based on its posture and the VLAN it is assigned to.

Periodic Revalidation

Periodic revalidations are built into the NAC-L3-IP and NAC-L2-IP solution. The network-access device (NAD) initiates the process by periodically polling validated endpoints to determine whether a change has been made in their posture. CTA alerts the NAD of any changes on the end host, and the NAD then issues a full revalidation and posture assessment.

This security measure prevents users from validating their host and then lowering their security posture after they have been granted access to the network.

Additionally, a separate revalidation timer requires all active hosts to be fully revalidated every 30 minutes, by default. This enables the network administrator to change the security policy on the fly. All already-validated end hosts must meet this new policy when their revalidation timer expires. The following example further illustrates this point:

Bob, the network administrator of example.com, receives a new alert about a critical security vulnerability in Microsoft Windows. Realizing the security impact that this vulnerability might have on his network, Bob immediately modifies his NAC security policy to require the hotfix that addresses this vulnerability to be applied on all end hosts on his network. Because it is during the day, most users validated their machines on the network when they arrived in the morning. Without periodic revalidation, Bob would have to wait until each user disconnects and reconnects to the network before the endpoint is revalidated. However, the revalidation timer solves this by requiring all active, validated hosts to be fully revalidated every 30 minutes (by default).

NAC Agentless Hosts

A NAC agentless host (NAH) (or a clientless endpoint) is a device that does not have CTA installed. Therefore, it cannot respond to the EAPoUDP or EAP-FAST request from the NAD. A printer, a webcam, an IP phone, and a guest PC are all examples of NAHs.

Individual policies can be defined on the NAD for NAHs. The policy can be designed to exclude a specific MAC or IP address or a range of addresses. Alternatively, a global policy can be defined on Cisco Secure ACS for NAHs. After the EAPoUDP or EAP-FAST session times out, the NAD can notify Cisco Secure ACS of the NAH, and Cisco Secure ACS can apply the appropriate authorization rights. We look at NAHs in more detail in Chapters 4, “Configuring Layer 2 NAC on Network-Access Devices,” through 8, “Cisco Secure Access Control Server.”

Another option for NAHs (which is part of NAC Phase II) is to use an audit server to scan the host for the services running on it and potential vulnerabilities. Cisco Secure ACS instructs the audit server on which hosts to scan by using the Generic Authorization Message Exchange (GAME) protocol. When the scan is complete, the audit server returns the results to Cisco Secure ACS through the GAME protocol, and Cisco Secure ACS uses these results to apply a security posture and overall policy to the end host.

NAC Program Participants

Cisco Systems leads the NAC program, but is open to any vendor that wants to participate. To ensure interoperability, Cisco requires all vendors shipping NAC-enabled code to have it tested either by an independent third-party testing center or by Cisco Systems. At the time of publication, more than 75 vendors were enrolled in the NAC program. A current list of program participants is maintained by Cisco at http://www.cisco.com/web/partners/pr46/nac/partners.html.

Components That Make Up the NAC Framework Solution

The following sections examine the individual components that make up the NAC Framework solution. Although only an overview is provided here, each component is covered in detail in its associated chapter in this book.

Cisco Trust Agent

Cisco Trust Agent (CTA) is a small software application (approximately 3MB) that is installed locally on a PC and that allows Cisco Secure ACS to communicate directly with the PC to query it for posture credentials. Some common posture credentials are the OS name, the service pack installed, and specific hotfixes applied. Table 1-1 lists the posture credentials that CTA supports or for which CTA is a broker.

CTA is a core component of NAC and is the only communications interface between the NAD and the applications that reside on the PC. It receives posture credential queries from Cisco Secure ACS, brokers them to the correct application, and then forwards the application responses to Cisco Secure ACS. CTA has three key responsibilities (see Figure 1-4):

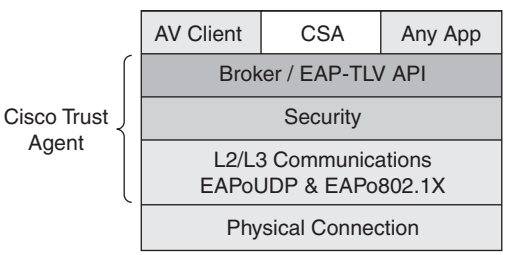
- **Communication**—Provides a communications link with the NAD using EAPoUDP or EAP-FAST.
- **Security**—Authenticates the device requesting posture credentials and ensures that all information is sent out encrypted on the wire.
- **Broker**—Provides an application programming interface (API) to query other applications running on the system and notifies them of the current system posture so they can react to posture changes.

Table 1-1 *Posture Credentials Supported by CTA*

Application	Posture Credentials
CTA (version 2)	CTA version Operating system name Operating system version Installed service packs Installed hotfixes Custom credentials returned through the optional scripting interface
Cisco Security Agent (CSA)*	CSA version CSA status (enabled/disabled) Fully qualified domain name (FQDN) of Cisco Security Agent Management Center (CSA-MC) Last poll of CSA
Antivirus*	Antivirus software name or identifier Software version Scan engine version DAT/pattern file version DAT/pattern file release date Antivirus enabled/disabled On-access scan enabled
Other software*	Varies by vendor

*CTA must be installed and acts as a broker agent to forward the posture credentials to Cisco Secure ACS.

Figure 1-4 *Responsibilities of CTA*



NOTE CTA is involved only in the posture query and response process; it does not take part in any enforcement action on its own. Thus, if a user disables (or removes) CTA, the host becomes clientless (a NAC agentless host). However, it still cannot bypass the NAC validation process and be granted unrestricted access to the network. Instead, the NAC agentless host policy takes effect, which can greatly restrict or even deny access to the network. This is unlike common personal firewall software or antivirus software, in which disabling the application lessens the protection provided.

Software Availability and Operating System Support

CTA is available free of charge to all registered Cisco.com users at http://cisco.com/cgi-bin/tablebuild.pl/cta. CTA supports the Windows NT, Windows 2000, Windows XP, Windows 2003, Red Hat Linux, and MAC OS 10.3 host operating systems. Internationalization support for CTA includes English, Japanese, Korean, French, Spanish, Arabic, Hebrew, and Russian.

CTA also includes an 802.1X supplicant bundled with it that supports EAP-FAST when running NAC. The 802.1X supplicant is needed to implement NAC-L2-802.1X. However, the 802.1X supplicant is limited to wired interfaces only—no wireless interfaces.

Chapter 2, "Cisco Trust Agent," fully covers the installation, configuration, operation, and troubleshooting of CTA.

Cisco Security Agent

Cisco Security Agent (CSA) is the Cisco award-winning host-based intrusion-prevention system (HIPS) installed on a desktop or server PC that protects it from known and unknown threats. CSA adds a shim into the network layer and into the kernel layer (to watch both network traffic and API calls to kernel). This allows CSA to not only be a personal firewall, but also to protect against buffer-overflow attacks and spyware/adware. In addition, it provides file protection, malicious application protection, and operating-system integrity protection. CSA is one of the few HIPS products that provide true protection against "Day Zero" attacks.

Starting with version 4.5, CSA integrates seamlessly with NAC through CTA. CTA queries CSA to establish the presence of the agent and determine whether it is in protect mode. This information is part of the posture credentials returned to Cisco Secure ACS and is used to determine the end host's overall security posture. Based on this posture, Cisco Secure ACS can apply a policy that alters the state of CSA. CSA's state change dynamically activates additional rules within CSA, thereby providing another level of protection to the host.

Cisco Security Agent Management Center (CSA MC) provides a powerful, scalable application used to manage all agents. When an agent is installed on a host, it first registers with CSA MC and downloads any updates to its rule set. Thereafter, the agent periodically polls CSA MC to check for any new software or rule updates. Besides the configuration and software update function, CSA MC receives real-time security events from the agents and immediately displays them in the Event Monitor for the network administrator to see. In addition, CSA MC correlates the events, received from all agents in the network, to detect suspicious activity across several hosts. If similar threats are detected across several agents, CSA MC creates and deploys dynamic rules to all the agents to provide an additional layer of protection against this newly spreading threat.

Chapter 9, "Cisco Security Agent," covers the installation, configuration, and operation of CSA.

Software Availability and Operating System Support

CSA MC versions 4.5 and 5.0 are a separately licensed product under the CiscoWorks VMS umbrella. They are supported on Windows 2000 Server and Windows 2000 Advanced Server. CSA MC Version 5.1 and higher are standalone products (no longer part of VMS) and are supported on Windows 2003 R2 Standard and Enterprise editions. CSA MC is capable of managing up to 100,000 agents in distributed mode.

CSA agents are supported on the following operating systems: Windows 2003, Windows XP, Windows 2000, Windows NT, Solaris, and Red Hat Linux. Internationalization is supported on Windows 2000 and later and includes all languages except Arabic and Hebrew. Localization is included for English, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish language desktops. The agent UI, events, and help system all appear in the language of the end user's desktop. Additional information can be found online at http://www.cisco.com/go/csa/.

Licensed users of CSA MC can obtain software updates at http://www.cisco.com/cgi-bin/tablebuild.pl/csa.

See Chapter 9 for installation and configuration information about CSA and CSA MC.

Network-Access Devices

NADs query the CTA installed on the endpoint. In NAC Phase I, the NAD could be only an IOS router. In Phase II, any of the following devices can be a NAD:

- Cisco IOS router
- Cisco Catalyst Switch running Cisco IOS or CAT OS
- Cisco VPN 3000 series concentrator

- Cisco ASA 5500 series adaptive security appliances and PIX 500 series security appliances
- Cisco wireless access device

NOTE Future phases of NAC will continue to expand the list of supported network devices.

Cisco IOS Router

Cisco IOS routers first supported NAC in Cisco IOS Release 12.3(8)T, in the Advanced Security, Advanced IP Services, or Advanced Enterprise Services feature sets. Table 1-2 lists Cisco IOS routers by platform and current NAC capability.

NOTE For the most up-to-date list of NAC-enabled routers, check online at http://www.cisco.com/go/nac/.

Table 1-2 *NAC Support in IOS Routers*

Cisco Router Platform	NAC Support
7500 series	Yes
7300 series	Yes
7200 series	Yes
7100 series	No
4500 series	No
3800 series	Yes
3700 series	Yes
3640, 3640A, 3660-ENT series	Yes
3620, 3660-CO series	No
2800 series	Yes
2600XM series, 2691	Yes
2600 series (non-XM Models)	No
1800 series	Yes
1701, 1711, 1712, 1721, 1751, 1751-V, 1760	Yes
1710, 1720, 1750	No
830 series	Yes
AS5850, AS5400, AS5400HPX, AS5350	No

When NAC is implemented on a router, this is called NAC-L3-IP. That is, the security enforcement point becomes the Layer 3 gateway instead of the physical port into which the end host is plugged.

Posture validation is triggered by defining an *intercept* ACL on the router's interface. Any traffic arriving on the interface from a nonpostured source that matches the *intercept* ACL triggers the posture-validation process, as illustrated in Figure 1-1. When the overall security posture of the host is determined, Cisco Secure ACS sends a host-based downloadable ACL to the router to restrict, prohibit, or permit that client's access to the network. Thus, policy enforcement takes place at Layer 3 with an ACL on the router's interface.

Online Resource: Cisco Routers

For more information about the line of IOS routers available from Cisco Systems, visit http://www.cisco.com/go/routers/.

See Chapter 5, "Configuring Layer 3 NAC on Network-Access Devices," for more information on configuring and troubleshooting NAC on a Cisco IOS router.

Cisco Catalyst Switch Running Cisco IOS or CAT OS

Catalyst switches first supported NAC in the summer of 2005 across various platforms and release trains. One benefit of adding NAC on the switch is enhanced posture-enforcement capabilities through containment. On Cisco IOS routers, policy enforcement was applied with a downloadable ACL on the router's interface. This enabled the administrator to restrict (or even deny) the endpoint's access through the router. However, the endpoint could not be restricted from sending packets to Layer 2–adjacent devices (because those packets did not traverse the router and, therefore, would not be subject to the downloadable ACL). However, on access switches, the endpoints are typically directly connected to a physical port on the switch. This allows for policy enforcement (through VLAN or ACL) as well as containment (because the endpoint is typically the only device connected to that port).

Catalyst switches can implement NAC on a per-port basis at Layer 2 or Layer 3. As mentioned previously in this chapter, when NAC is implemented at Layer 2, it is known as NAC-L2-802.1X because 802.1X is used as the underlying Layer 2 transport protocol. When NAC is implemented on a switch at Layer 3, it is known as NAC-L2-IP.

NAC-L2-802.1X and NAC-L2-IP have several administrative and operational differences that you should fully consider before selecting which one to deploy.

The following are attributes of NAC-L2-802.1X:

- 802.1X authentication must be implemented on the switch.
- The client's 802.1X supplicant triggers authentication and posture validation.
- The client's 802.1X supplicant must be CTA aware.
- Posture enforcement is provided by VLAN assignment only.
- EAP-FAST authenticates CTA to Cisco Secure ACS; therefore, no client-side certificate is needed.
- Endpoints must be directly connected, or be connected through an IP phone.

The following are attributes of NAC-L2-IP:

- Posture validation is triggered when the switch receives Address Resolution Protocol (ARP) packets from the endpoint. Optionally, Dynamic Host Configuration Protocol (DHCP) snooping can be enabled on the port to trigger posture validation when the switch receives the first DHCP packet.
- Posture enforcement is provided by downloadable ACLs.
- VLAN assignment is not supported.
- EAPoUDP is used to communicate between CTA and the NAD. PEAP is used between CTA and Cisco Secure ACS.
- URL redirection of the endpoint's web browser to a remediation server is supported.
- Endpoints can be directly connected, connected through an IP phone, or connected through a shared-media device (hub, non-NAC-capable switch, and so on.)

No "right" or "wrong" choice exists between the two. But there is a best choice for your network. If you don't know what that choice is, read *Cisco Network Admission Control, Volume I: NAC Architecture and Design,* which walks through several design scenarios, discusses the options available, and provides the rationale for the choices made.

An additional consideration (and probably the most important one) is which one will run on your existing switch hardware. Table 1-3 should come in handy in making that determination; it lists the various models of Catalyst switches and their NAC capabilities based on the OS.

NOTE For the most up-to-date list of NAC-enabled switches, check online at http://www.cisco.com/go/nac/.

Table 1-3 *NAC Support in Catalyst Switches*

Platform, Supervisor	OS	NAC-L2-802.1*x*	NAC-L2-IP	NAC-L3-IP	NAC Agentless Host
6500 - Sup32, Sup720	Native IOS	Planned	Yes, 12.2(18)SXF2	Planned	Yes, NAC-L2-IP
6500 – Sup2	Native IOS	No	No	No	No
6500 – Sup32, Sup720, Sup2	Hybrid	Yes, 8.5	Yes, 8.5	No	Yes, NAC-L2-IP
6500 – Sup32, Sup720, Sup2	Cat OS	Yes, 8.5	Yes, 8.5	No	Yes, NAC-L2-IP
6500 – Sup1A	All	No	No	No	No
5000 Series	All	No	No	No	No
4900 Series	IOS	Yes, 12.2(25)SG	Yes, 12.2(25)SG	Planned	Yes, NAC-L2-IP
4000/4500 Series – SupII+, II+TS, II+10GE, IV, V, V-10GE	Cisco IOS	Yes, 12.2(25)SG	Yes, 12.2(25)SG	Planned	Yes, NAC-L2-IP
4000 – SupI, II, and III	All	No	No	No	No
3750, 3560	Cisco IOS; advanced IP services, IP services, IP base	Yes, 12.2(25)SED	Yes, 12.2(25)SED	No	Yes, NAC-L2-IP
3550	Cisco IOS; IP services and IP base	Yes, 12.2(25)SED	Yes, 12.2(25)SED	No	Yes, NAC-L2-IP
3500XL, 2900XL	All	No	No	No	No
2970	Cisco IOS; LAN base	Yes, 12.2(25)SED	No	No	No
2960	Cisco IOS; LAN base	Yes, 12.2(25)SED	No	No	No
2950	Cisco IOS; EI, SI	Yes, 12.1(22)EA6	No	No	No
2955, 2940	Cisco IOS	Yes, 12.1(22)EA6	No	NO	No

continues

Table 1-3 *NAC Support in Catalyst Switches (Continued)*

Platform, Supervisor	OS	NAC-L2-802.1*x*	NAC-L2-IP	NAC-L3-IP	NAC Agentless Host
2948G-GE-TX	Cat OS	No	No	No	No
1900	All	No	No	No	No
Express 500	Cisco IOS	No	No	No	No

Catalyst switches are an integral part of the NAC solution, providing protection and containment of hosts that do not meet corporate security policies at the access layer. As such, Cisco is committed to providing NAC support on all new switch hardware.

Online Resource: Cisco Catalyst Switches

You can find more information about the Cisco Catalyst line of high-performance LAN switches at http://www.cisco.com/go/catalyst/.

See Chapter 4 for more information on configuring and troubleshooting NAC on a Catalyst switch.

Cisco VPN 3000 Series Concentrator

NAC support for the VPN 3000 series concentrators was first added in Release 4.7. The concentrator is a Layer 3 NAD and postures remote-access IPSec (or Layer 2 Tunneling Protocol [L2TP] over IPSec) clients. The posturing process is almost identical to that of NAC-L3-IP, described previously in the section "NAC: Phase I" (refer to Figure 1-1). The only difference is that the router is replaced with a VPN 3000 concentrator, and an IPSec tunnel is first established to the concentrator before the EAPoUDP session starts.

When the EAPoUDP session starts, a PEAP session is established between the client and the Cisco Secure ACS so posture validation can take place. Cisco Secure ACS then notifies the concentrator (through RADIUS) of the client's posture and passes down a filter list to be applied to the client. The filter list is the 3000's equivalent to a downloadable ACL.

One unique option that the concentrator provides is that clients can be excluded from posture validation based solely on OS type. This is because the Cisco VPN client sends its OS information during IPSec tunnel establishment, which occurs before NAC posture validation. Host exemption, along with all other NAC configuration, is specified under the group policy settings on the 3000. NAC configuration on the VPN 3000 concentrator is covered in detail in Chapter 6, "Configuring NAC on Cisco VPN 3000 Series Concentrators."

Online Resource: Cisco 3000 Series VPN Concentrators

For more information about the Cisco VPN 3000 series concentrators, see http://www.cisco.com/go/vpn3000/.

Cisco ASA 5500 Series Adaptive Security Appliance and PIX 500 Series Security Appliance

The NAC implementation on the Cisco 5500 series Adaptive Security Appliances (ASA) and PIX 500 series security appliances is identical to the implementation on the VPN 3000 concentrators. NAC-L3-IP is supported starting with Version 7.2(1) on all IPSec and L2TP over IPSec remote-access tunnels. Posture enforcement is provided by way of a downloadable ACL from Cisco Secure ACS. Additionally, just as with the VPN 3000, remote-access clients can be exempted from NAC posture validation based on OS type.

The ASA and PIX also support clientless authentication. Those hosts connecting through a remote-access tunnel that do not have CTA installed are marked as clientless. Cisco Secure ACS can then apply the clientless policy to those hosts, to limit (or remove entirely) their access to the network. Chapter 7, "Configuring NAC on Cisco ASA and PIX Security Appliances," contains the complete configuration of NAC on the ASA 5500 series appliances and PIX 500 series security appliances.

Online Resource: Cisco Adaptive Security Appliances

For more information about the Cisco ASA 5500 series adaptive security appliances, see http://www.cisco.com/go/asa/.

Cisco Wireless Devices

NAC Framework support for wireless devices is available on autonomous Access Points (AP), lightweight access points running the Lightweight Access Point Protocol (LWAPP), and the Wireless LAN Services Module (WLSM) for the Catalyst 6500. Table 1-4 lists the wireless devices and minimum supported software.

Table 1-4 *NAC Support in Wireless Devices*

Wireless Device	Minimum Supported Software
Autonomous APs running IOS: Aironet 1100, 1130AG, 1200, 1230AG, 1240AG, 1300 IOS-based access points	Cisco IOS Release 12.3(7)JA or later
Lightweight APs running LWAPP: Aironet 1000, 1130AG, 1200, 1230AG, 1240AG, 1500 + WLAN Controller 2000, 4100, or 4400	Cisco Unified Wireless Network Software Release 3.1 or later
Catalyst 6500 series WLSM	Cisco IOS Release 1.4.1 or later

Wireless devices are Layer 2 termination devices and, as such, support NAC-L2-802.1*x* as the posturing method. The process that a wireless client connecting to a wireless device goes through for posture validation is the same as for a wired client. Figure 1-3 depicts this posture. Note that wireless devices provide posture enforcement through VLAN only. This means that, to support NAC, the wireless devices must be configured for multiple VLANs per service set identifier (SSID).

Configuration and troubleshooting of NAC on Cisco wireless access points is covered along with other Layer 2 network-access devices in Chapter 4.

Online Resource: Cisco Wireless Access Points

For more information about the wireless line of products available from Cisco Systems, see http://www.cisco.com/go/wireless/.

Cisco Secure Access Control Server

The Cisco Secure Access Control Server (ACS) for Windows is another core required component of NAC. Cisco Secure ACS first supported NAC in Version 3.3, which was launched concurrently with Phase I in the summer of 2004. Cisco Secure ACS 4.0, released in the fall of 2005, added support for NAC Phase II, including all the NADs listed in the previous section.

Cisco Secure ACS is the central controller for all NAC policy decisions. It receives posture credentials from all agents and either processes them locally or forwards them on to partner validation servers for processing. If the posture credentials are forwarded on, Cisco Secure ACS waits to receive the application posture token (APT) back from the external validation server. It then combines this APT with the local APTs it created based on the defined policy; the result is an overall system posture token (SPT).

The SPT has one of the following values: Healthy, Checkup, Quarantine, Infected, or Unknown, which are mapped to a network access policy. The network-access policy and SPT are then transmitted to the NAD as part of policy enforcement. Optionally, Cisco Secure ACS can send a user-notification message that CTA displays on the end host. This message usually indicates the posture of the system along with some instructions (for the un-Healthy hosts). Cisco Secure ACS can also send a URL redirect to the end host via the NAD if either NAC-L3-IP or NAC-L2-IP is being used.

Chapter 8 covers installation, configuration, and troubleshooting of Cisco Secure ACS.

Online Resource: Cisco Access Control Server

For more information about the Cisco Secure Access Control Server, see http://www.cisco.com/go/acs/.

Event Monitoring, Analysis, and Reporting

Protecting the network from threats is the first step toward securing it. However, event monitoring, analysis, and reporting are also vital pieces in understanding the *network's* security posture:

- **Event monitoring**—The process of receiving events (or alerts) from the network and presenting them to the user in real time and in a meaningful way. This is usually provided with some sort of "dashboard" where new events are displayed as they come in.
- **Analysis**—The process of taking the events received and normalizing and correlating them to produce the most relevant set of data. The correlation process takes multiple streams of events from various device types and finds similarities in their data that can be linked to provide a detailed composite picture. The normalization process then removes the redundant data and improves data consistency.
- **Reporting**—The process of querying historical data for specific events and presenting those events in a useful way to the user.

Monitoring, analysis, and reporting are powerful tools that show the network administrator the state of the network at any given point in time. These tools are very important in networks where NAC is enabled because the volume of events that each network device generates for each postured host is huge. Monitoring the network devices individually for problems or anomalies is neither practical nor efficient. This is why Cisco has enhanced its Cisco Security Monitoring, Analysis, and Reporting System (CS-MARS) to support NAC.

The CS-MARS appliance is a topologically aware, high-performance event-correlation system. Syslogs, NetFlow data, Simple Network Management Protocol (SNMP) traps, and other network logging information can be sent to it from a variety of network sources. This includes routers, switches, firewalls, intrusion-prevention devices, Cisco Secure ACS, and even end hosts. All this information is then correlated within CS-MARS to detect network attacks and other types of security threats. When an attack is detected, an incident is fired and the attacker, victim, and path from attacker to victim are displayed in the CS-MARS interface. Additionally, based on the attack vector, CS-MARS can inform the user of the best way to mitigate the attack.

In support of NAC, CS-MARS parses, normalizes, correlates, and reports on posture-validation events for NAC-L3-IP, NAC-L2-IP, and NAC-L2-802.1X. Predefined reports enable network administrators to view the number of hosts in Healthy, Quarantined, Clientless, or other states throughout the entire network. Administrators can further drill down to determine the posture status on a per-device basis. They may also choose to receive daily reports (via e-mail) of the number and location of nonhealthy hosts in their network.

Help-desk support teams can use CS-MARS to identify problems reported from end users. CS-MARS can display IP addresses, machine/usernames, and the logical switch port number the user is connected to, along with the posture information or authentication

information of end hosts. This information can be displayed in real time and allows the help-desk teams to quickly and easily identify problems end users are having.

Chapter 17, "Monitoring the NAC Solution Using the Cisco Security Monitoring, Analysis, and Response System," covers the configuration and operation of CS-MARS in a NAC Framework solution.

Online Resource: Cisco Security Monitoring, Analysis, and Reporting System

For more information about the Cisco Security Monitoring, Analysis, and Reporting System, see http://www.cisco.com/go/mars/.

Summary

This chapter answered the question, "What is network access control?" by providing a solution overview as well as taking a look at the individual components that make up NAC. The different implementations of NAC were also explained, including NAC-L3-IP, NAC-L2-IP, and NAC-L2-802.1X. Network-access devices supporting NAC were presented, along with the version of software required.

Looking ahead, subsequent chapters focus on the installation, configuration, and operation of each individual NAC component. Once complete, the individual components are combined to illustrate real-world deployment scenarios in Part III, "Deployment Scenarios." Finally, Part IV, "Managing and Monitoring NAC," focuses on the overall management and monitoring of the NAC solution.

Review Questions

You can find the answers to the review questions in Appendix A, "Answers to Review Questions."

1. Which of the following is a required component of NAC?
   a. Remediation server
   b. Antivirus server
   c. Cisco Security Agent
   d. Cisco Secure Access Control Server
2. What is the posture-enforcement method for NAC-L3-IP?
3. What is the posture-enforcement method for NAC-L2-802.1X?

4. NAC-L3-IP and NAC-L2-IP use which of the following protocols to secure the communication between the endpoint and Cisco Secure ACS?

   a. EAP over UDP

   b. EAP-FAST

   c. 77RADIUS

   d. PEAP

5. The network-access device uses what protocol to send NAC-related messages to Cisco Secure ACS?

   a. EAP over UDP

   b. EAP-FAST

   c. RADIUS

   d. PEAP

6. The VPN 3000 concentrator and the ASA and PIX security appliances support NAC on which of the following:

   a. Remote-access IPSec and L2TP over IPSec connections

   b. Remote-access and LAN-to-LAN IPSec connections

   c. Remote-access PPTP and L2TP over IPSec connections

   d. Remote-access IPSec connections only