This chapter covers the following topics:

- Network admission control overview
- NAC Framework benefits
- NAC Framework components
- Operational overview
- Deployment models

Implementing Network Admission Control

Network Admission Control (NAC) is a technology initiative led by Cisco Systems working in collaboration with many leading security vendors, including antivirus and desktop management. Their focus is the creation of solutions that limit security threats, such as worms and viruses.

This technology provides a framework using existing Cisco infrastructure to enforce network admission policies on NAC-enabled endpoint devices, guaranteeing software compliance before network access is granted. If an endpoint device is determined noncompliant, a variety of admission actions are available to administrators, and how the actions are implemented is at the discretion of the network administrator. For example, a noncompliant endpoint may be placed in a quarantine area of the network and redirected to a remediation server to load the necessary software or patches. A notification is displayed to the user warning that their device is not compliant or, in the worse case, that they are denied network access entirely.

This chapter describes the Cisco NAC Framework, identifies benefits, describes the solution components and how they interoperate, and describes common deployment models.

Network Admission Control Overview

Worms and viruses continue to be disruptive, even though many businesses have significantly invested in antivirus and traditional security solutions. Not all users stay up to date with the many needed software security patches of antivirus files. Noncompliant endpoints are frequent and the reasons vary; for example:

- A user might choose to wait and install a new update later because they don't have the time

- A contractor, partner, or guest needs network access; however, the business may not control the endpoint

- The endpoints are not managed

- The business lacks the capability to monitor the endpoints and determine whether they are updated to conform to the business's security policy

When infected endpoints connect to the network, they unsuspectingly spread their infections to other improperly protected devices. This has caused businesses to examine how they should implement endpoint compliance enforcement besides user authentication before granting access to their networks.

Cisco Systems provides two network admission control solution choices:

- NAC Appliance
- NAC Framework

Chapter 7, "Cisco Clean Access," describes NAC Appliance, which was originally marketed as Cisco Clean Access (CCA). NAC Appliance is a turnkey self-sufficient package that does not rely on third-party products for determining and enforcing software compliance. This chapter focuses on NAC Framework.

NAC Framework is an integrated solution that enables businesses to leverage many of their existing Cisco network products, along with many third-party vendor products such as antivirus, security, and identity-based software. Vendor products must be NAC-enabled in order to communicate with the NAC-enabled network access devices. NAC Framework is extremely flexible because it can enforce more features available from other vendors' products. A comparison of customer preferences for choosing the NAC Appliance and NAC Framework is shown in Table 6-1.

Table 6-1 *NAC Customer Profile*

NAC Framework	NAC Appliance
Uses an integrated framework approach, leveraging existing security solutions from other vendors	Prefers bundled, out-of-the-box functionality with preinstalled support for antivirus and Microsoft updates
Complex network environment, leveraging many types of Cisco network access products	Heterogeneous network infrastructure
Longer, phased-in deployment model	Rapid deployment model
Can integrate with 802.1x	Independent of 802.1x

Source: Cisco Systems, Inc.[1]

NAC Framework Benefits

Following are some benefits that can be recognized by businesses that have implemented NAC Framework:

- **Protects corporate assets**—Enforces the corporate security software compliance policy for endpoints.

- **Provides comprehensive span of control**—All the access methods that endpoints use to connect to the network are covered, including campus switching, wireless, router WAN links, IP Security (IPSec), and remote access.

- **Controls endpoint admission**—Validates all endpoints regardless of their operating system, and it doesn't matter which agents are running. Also provides the ability to exempt certain endpoints from having to be authenticated or checked.

- **Offers a multivendor solution**—NAC is the result of a multivendor collaboration between leading security vendors, including antivirus, desktop management, and other market leaders. NAC supports multiple security and patch software vendors through APIs.

- **Leverages existing technologies and standards**—NAC extends the use of existing communications protocols and security technologies, such as Extensible Authentication Protocol (EAP), 802.1x, and RADIUS services.

- **Leverages existing network and antivirus investments**—NAC combines existing investments in network infrastructure and security technology to provide a secure admission control solution.

NAC Framework Components

The initial release of the Cisco NAC Framework became available in June 2004 and continues to evolve in phases. The functions of the solution architecture remain consistent; however, as each phase is introduced, more capabilities and deeper integration are added to the NAC Framework architecture. To stay up to date with NAC and partner products, refer to the URL www.cisco.com/go/nac.

NAC Framework includes the following main components, as shown in Figure 6-1:

- Endpoint security application
- Posture agent
- Network access devices
- Cisco Policy server
- Optional servers that operate as policy server decision points and audit servers
- Optional management and reporting tools are highly recommended (not shown)

Figure 6-1 *NAC Framework Components*
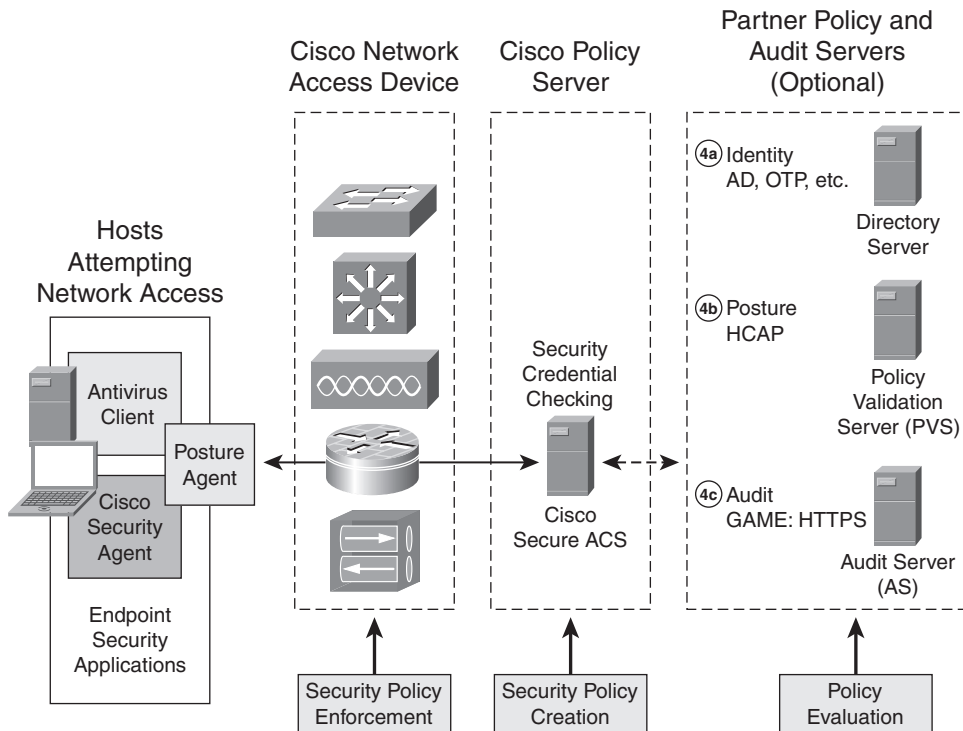
The next sections describe the main components in more detail.

Endpoint Security Application

An endpoint security application is security software that resides on a host computer. Depending on the application, it can provide host-based intrusion prevention system (HIPS), antivirus scanning, personal firewall, and other host security functions. Cisco Security Agent is a HIPS example.

NAC partners provide NAC-enabled security applications that use a posture plug-in that communicates their credentials and state with a posture agent, both residing on the same endpoint. Many endpoint security applications provide antivirus capabilities, and some provide additional identity-based services. For a list of NAC partners, refer to www.cisco.com and search for "Network Admission Control Current Participants."

Posture Agent

A posture agent is middleware or broker software that collects security state information from multiple NAC-enabled endpoint security applications, such as antivirus clients. It communicates the endpoint device's compliance condition. This condition is referred to as the *posture* of an endpoint. The posture information is sent to Cisco Secure Access Control Server (ACS) by way of the Cisco network access device.

The *Cisco Trust Agent* is Cisco's implementation of the posture agent. Cisco has licensed the trust-agent technology to its NAC partners so that it can be integrated with their security software client products. The trust agent is free and is also integrated with the Cisco Security Agent. Cisco Trust Agent can work with Layer 3 Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), and Cisco Trust Agent (CTA) version 2 can also work with Layer 2 with Extensible Authentication Protocol over 802.1x (EAPo802.1x) or Extensible Authentication Protocol over LAN (EAPoLAN).

Network Access Devices

Network access devices that enforce admission control policy include Cisco routers, switches, wireless access points, and security appliances. These devices demand endpoint security credentials and relay this information to policy servers, where network admission control decisions are made. Based on customer-defined policy, the network will enforce the appropriate admission control decision—permit, deny, quarantine, or restrict. Another term for this device is security policy enforcement point (PEP).

Policy Server

A policy server evaluates the endpoint security information relayed from network access devices (NADs) and determines the appropriate admission policy for enforcement. The Cisco Secure ACS, an authentication, authorization, and accounting (AAA) RADIUS server, is the foundation of the policy server system and is a requirement for NAC. Cisco Secure ACS is where the admission security policy is created and evaluated to determine the endpoint device's compliance condition or posture.

Optionally, Cisco Secure ACS may work in concert with other policy and audit servers to provide the following additional admission validations:

- **Identity**—User authentication can be validated with an external directory server and the result is communicated to Cisco Secure ACS. Examples include Microsoft Active Directory and one-time password (OTP) servers.

- **Posture**—Third-party, vendor-specific credentials such as antivirus and spyware can be forwarded using the Host Credential Authorization Protocol (HCAP) to NAC-enabled Policy Validation Servers (PVS) for further evaluation. This enables

businesses to leverage existing policies maintained in their PVS to validate and forward the software compliance result to Cisco Secure ACS, ensuring that a consistent policy is applied across the entire organization.

- **Audit**—Determines the posture for a NAC Agentless Host (NAH), which is a host without the presence of a posture agent such as Cisco Trust Agent. The Audit server works out of band and performs several functions:

  — Collects posture information from an endpoint.

  — Acts as a posture validation server to determine compliance of an endpoint and determine the appropriate compliance result in the form of a posture.

  — Communicates the result to Cisco Secure ACS using Generic Authorization Message Exchange (GAME) over an HTTPS session. GAME uses an extension of Security Assertion Markup Language (SAML), a vendor-neutral language enabling Web services to exchange authentication and authorization information.

The optional validation policy servers communicate the user authentication status or compliance status or both to Cisco Secure ACS, which makes the final determination as to the admission policy for the endpoint. *Policy decision point* is a term used to describe the function Cisco Secure ACS performs.

## Management and Reporting Tools

In addition to the required NAC components, a management system is recommended to manage and monitor the various devices. Reporting tools are available to operation personnel to identify which endpoints are compliant and, most importantly, which endpoints are not compliant. Examples include Cisco Security MARS and CiscoWorks Security Information Manager Solution (SIMS).

Operational Overview

This section describes how NAC determines admission compliance and how it then uses the network to enforce the policy to endpoints.

Network Admission for NAC-enabled Endpoints

This section describes the process in which a noncompliant endpoint device is discovered and is denied full access until it is compliant with the admission policy. This scenario is shown in Figure 6-2.

Figure 6-2 *Admission Process for Noncompliant Endpoint*
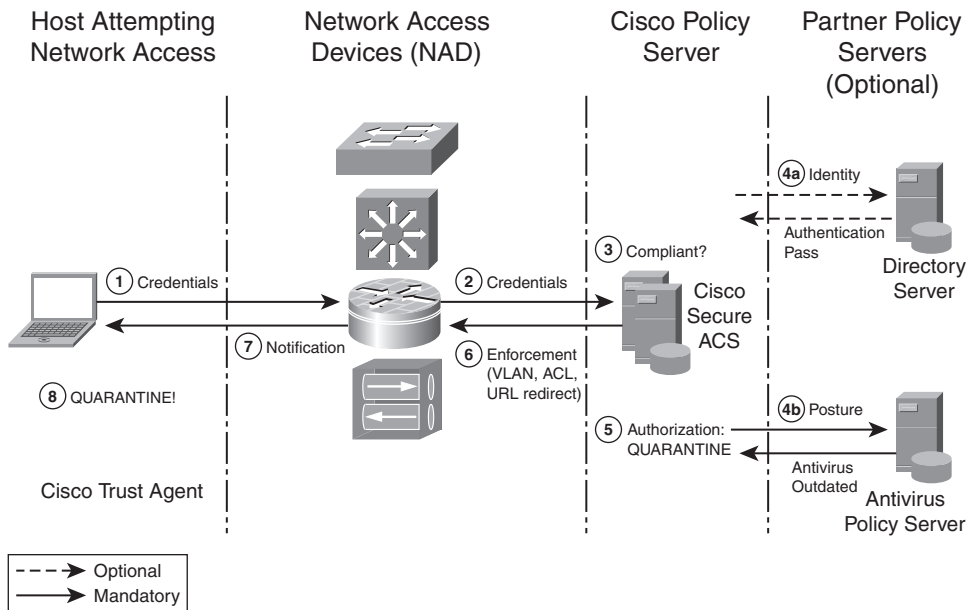
The following list is a summary of the admission process for a noncompliant endpoint shown in Figure 6-2:

1 An endpoint attempts to access the network.

2 The NAD notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access.

3 Cisco Secure ACS checks the NAC policy to determine whether the endpoint is compliant.

4 Cisco Secure ACS forwards specific information to other partner policy servers.

   a Identity information is sent to a directory server for authentication validation.

   b Host credentials are sent to an antivirus policy server for posture determination.

5 Cisco Secure Access uses information from the all-policy servers and decides the endpoints authorization. In this example, the endpoint is not compliant and is assigned a quarantine posture.

6 Quarantine enforcement actions are sent from Cisco Secure ACS to the NAD servicing the endpoint.

7 NAD enforces admission actions and communicates posture to Posture Agent.

8 Posture Agent notifies the user that the endpoint is quarantined.

The following sections explain each step in more detail.

Endpoint Attempts to Access the Network

In step 1, the admissions process begins when an endpoint attempts to access the network. What triggers the process is dependent upon the NAD's capabilities and configuration. The NAD initiates posture validation with Cisco Trust Agent using one of the following protocols:

- EAPoUDP
- EAPo802.1x

The protocol used is dependent upon the NAD to which the endpoint connects. Both of these protocols serve as a communication method between the endpoints using Cisco Trust Agent and the NAD. Cisco Trust Agent gathers credentials from NAC-enabled security applications such as antivirus.

NAD Notifies Policy Server

In step 2, the NAD notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access. A protected tunnel is set up between the policy server and the endpoints posture agent. Once communication is established, the credentials from each of the posture plug-ins are sent to Cisco Secure ACS.

Cisco Secure ACS Compares Endpoint to NAC Policy

In step 3, Cisco Secure ACS looks at the admission control policy and compares the endpoint credentials to the policy to determine whether it is compliant. It determines which of the following posture states to assign to the endpoint:

- **Healthy**—Endpoint is compliant; no network access restrictions.
- **Checkup**—Endpoint is within policy, but an update is available. This state is typically used to proactively remediate a host to the Healthy state or to notify a user that a more recent update is available and recommend remediation.
- **Transition**—This state became available in NAC phase 2. The endpoint posturing is in process; provide an interim access, pending full posture validation. This state is applicable during an endpoint boot in which all services may not be running or audit results are not yet available.
- **Quarantine**—Endpoint is out of compliance; restrict network access to a quarantine network for remediation. The endpoint is not an active threat but is vulnerable to a known attack or infection.

- **Infected**—Endpoint is an active threat to other endpoint devices; network access should be severely restricted or totally denied all network access.

- **Unknown**—Endpoint posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined.

Cisco Secure ACS Forwards Information to Partner Policy Servers

In step 4, Cisco Secure ACS can optionally send user login (4a) and credentials (4b) to other policy decision servers. When this is done, Cisco Secure ACS expects to receive authentication status and a posture state from each of the policy decision servers.

In step 4a when NAC L2-802.1x is used, Cisco Secure ACS can send identity information to an authentication server. It confirms that the username and password are valid and returns a passed authentication message to Cisco Secure ACS. If identity authentication fails, no posture is checked and the endpoint fails authentication, resulting in no network access.

In step 4b in this example, an antivirus policy server determines that the device is out of compliance and returns a quarantine posture token to Cisco Secure ACS.

Keep in mind that NAC partner policy servers vary and offer a variety of compliance checks besides antivirus. For example, some vendors offer checking for spyware and patch management.

Cisco Secure ACS Makes a Decision

In step 5, Cisco Secure ACS compares all the posture states and determines which posture is the worst; infected is the worst and healthy is the best. It always assigns the worst state and takes the action for that posture. In this example, the user has passed authentication but the endpoint has been assigned a quarantine posture.

Cisco Secure ACS Sends Enforcement Actions

Cisco Secure ACS takes the actions assigned to a quarantine state. In this quarantine example, they can include the following:

- Enforce quarantine access; this varies based on the NAD.
  - For NADs using NAC-L3-IP, the enforcement actions include a quarantine Access Control List (ACL) being applied to the endpoint.
  - For NADs using NAC-L2-IP, the enforcement actions include a quarantine ACL being applied to the endpoint.
  - For NADs using NAC-L2-802.1x, the enforcement action includes a quarantine virtual LAN (VLAN) being applied to the endpoint device.

- Optionally, the endpoint device may be assigned a URL redirect to the remediation server.

- Optionally, a notification message can be sent to the user, indicating that their device is not compliant and is being redirected for remediation.

NAD Enforces Actions

In step 7, the NAD receives the quarantine policy enforcement from Cisco Secure ACS and responds accordingly. In this example, such a response would be to quarantine the endpoint, enforce an endpoint URL redirect to the remediation server, and send a quarantine message to the posture agent.

Posture Agent Actions

In step 8, the posture agent displays the quarantine message, and the user is redirected to the remediation server.

Actions available vary by NAC partner products. Cisco Secure ACS is capable of sending different application actions from HCAP-compliant policy servers to their specific application plug-ins. This can trigger actions such as the following:

- Force an auto-remediation to a designated remediation server

- Force an auto-patch by instructing the host to download and apply a patch automatically

- Restart a stopped application service

In this example, the endpoint is now quarantined, and the user has been notified by a message. The user can elect to do nothing and remain quarantined, or comply and allow their computer to be updated.

The admission control process can take very little time, as little as milliseconds. The time varies and is based on many factors, including:

- Where the endpoint is located in relation to the policy server and optional partner policy servers

- Where the remediation server is located

- NADs performance capability

- Network bandwidth

- How busy the policy servers are

As shown in Figure 6-3, an endpoint is changing from quarantine to healthy posture state.

Figure 6-3   *Admission Process for Endpoint Changing from Quarantine to Healthy State*
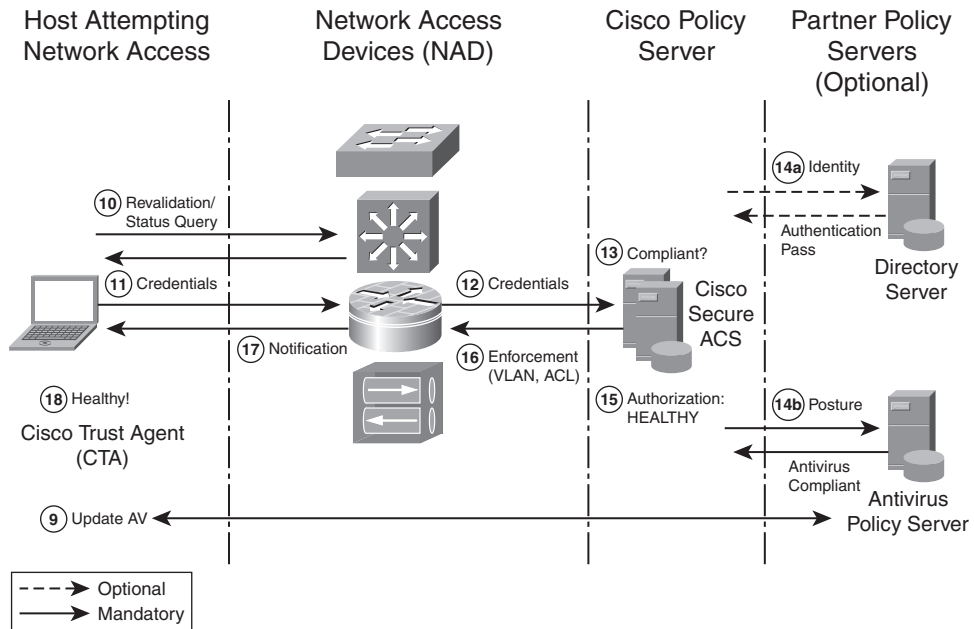
The following list explains the process shown in Figure 6-3:

9   Endpoint remediated.

10   Endpoint polled for change of compliance.

11   Host credentials gathered from endpoint.

12   Host credentials passed to Cisco Secure ACS.

13   Cisco Secure ACS rechecks the NAC policy to determine whether the endpoint is compliant.

14   Cisco Secure ACS forwards specific information to other partner policy servers.

    a   Identity information is sent to a directory server for authentication validation.

    b   Host credentials are sent to an antivirus policy server for posture determination.

15   Cisco Secure Access uses information from all policy servers and decides the endpoints authorization. In this example, the endpoint is compliant and is assigned a healthy posture.

16 Healthy enforcement actions are sent from Cisco Secure ACS to the NAD servicing the endpoint.

17 NAD enforces admission actions and communicates healthy posture to Posture Agent.

18 Posture Agent can notify the user that the endpoint is healthy. Many businesses prefer that a healthy posture be transparent to the user with no message notification displayed.

Endpoint Polled for Change of Compliance

Once an endpoint has been assigned a posture, it stays in effect and is not checked again until a NAC timer has expired or a posture agent trigger occurs.

The following are configurable timers for NAC:

- **Status Query**—Ensures that an endpoint remains compliant with the admission policy. The timer begins at policy enforcement for the endpoint; compliance is rechecked after the timer expires. Different Status Query timers can exist for different posture states. A shorter amount of time is beneficial for noncompliant states such as quarantine; the device can be rechecked sooner than a healthy device, in order to regain full network access.

- **Revalidation**—A time in which the posture remains valid. It can be set lower when an outbreak occurs, to force all endpoints to go through the admission policy process again. This enables endpoints to timeout at different intervals depending on where their timers are, versus forcing all endpoints to go through the validation process at the same time.

  In phase 2 with NAC-L2-802.1x, there is no capability to send a status query from the NAD by way of 802.1x. To overcome this, beginning with version 2 of Cisco Trust Agent, an asynchronous status query capability exists. Cisco Trust Agent can send an Extensible Authentication Protocol Over Lan (EAPOL)-Start to the NAD, or CTA can frequently poll all registered NAC application posture plug-ins looking for a change in credentials. If a change exists, it will trigger an EAPOL-Start signaling for a new posture validation.

  In step 10 of Figure 6-3, the quarantine status query timer has expired.

The NAD is aware that the timer has expired for the endpoint, so it begins rechecking for compliance. The posture agent gathers credentials from the posture plug-ins of NAC-enabled security applications such as antivirus.

Revalidation Process

From step 11 through step 18, the process is the same as the example described in Figure 6-2. The NAD notifies the policy server (Cisco Secure ACS) that an endpoint requests network access. This time, the Cisco Secure ACS determines that the posture is healthy for

all admission checks and that the user login is valid. Authentication is successful, and Cisco Secure ACS assigns the healthy policy.

The NAD receives the healthy policy enforcement from Cisco Secure ACS and responds accordingly by allowing full network access. The timers begin for the healthy state.

The NAD informs the posture agent of the healthy status, but no message is sent to the user this time. The user can now resume normal network activity.

Network Admission for NAC Agentless Hosts

The previous example described the admission process for a NAC-enabled endpoint running a posture agent, such as Cisco Trust Agent. This section describes the process for endpoints that do not have a posture agent.

NAC agentless hosts (NAH) can be accommodated by several methods, as shown in Table 6-2. A NAH exception list and whitelist can be created to identify known endpoints that do not have a posture agent installed and running. The option chosen is dependent upon the NAC Framework component and the NAD enforcement method used.

Table 6-2   *NAC Agentless Host Exceptions and Whitelisting*

Component	Administration Model	NAC-L2 IP	NAC-L3 IP	NAC-L2 802.1x
NAD	• Distributed, managed at the device level • Does not scale	Device Type, IP, or MAC Enforcement by intercept ACL (IP/MAC)	Device Type, IP, or MAC Enforcement by intercept ACL (IP)	MAC-Auth-Bypass (identity + posture)
Cisco Secure ACS whitelist	• Centralized • Scales	MAC (posture only)	MAC (posture only)	MAC-Auth-Bypass (identity + posture)
Audit	• Centralized • Scales	Active network scan, remote login, browser object, hardware/software inventory	Active network scan, remote login, browser object, hardware/software inventory	Not supported at the time of this writing

Source: Cisco Systems, Inc.[2]

The audit server can be used for NAH in all enforcement methods and is a single centrally managed server. As shown in Figure 6-4, an audit server can be included as a decision policy server for NAH. The audit server can determine the posture credentials of an endpoint without relying on the presence of a posture agent.

Figure 6-4 *Admission Control for NAC Agentless Host*
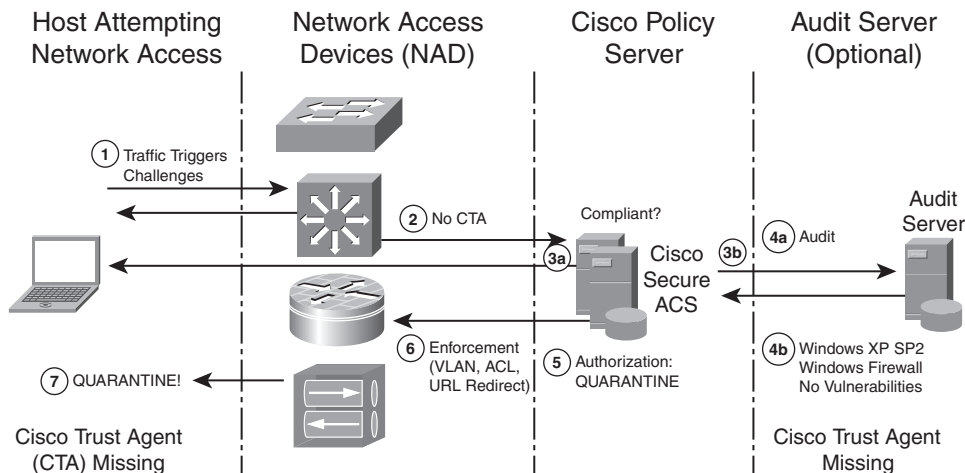
The following list explains the process shown in Figure 6-4:

  1 An endpoint attempts to access the network. The trigger mechanism is dependent upon the NAD's capabilities and configuration. The NAD attempts to initiate posture validation with the posture agent, but no posture agent (Cisco Trust Agent) exists.

  2 The NAD notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access with no Cisco Trust Agent (CTA) present.

  3 Cisco Secure ACS cannot determine whether the NAH is compliant because no posture agent exists. Cisco Secure ACS performs the following:

   a Assign a transition posture to grant a temporary, limited network access to the agentless host while the audit server is determining the full posture validation. The NAD enforces the transition admission policy.

   b Notify the external audit server that the NAH is requesting admission.

  4 Cisco Secure ACS cannot determine whether the NAH is compliant, so it notifies the audit server using GAME to conduct a scan on the endpoint.

   a The audit server scans the endpoint. It evaluates the endpoint's software information against the audit server's compliance policy. It determines that the operating system patch level is compliant or healthy, but the posture agent is missing, so it is considered noncompliant.

   b Quarantine is the application posture token (APT) assigned by the audit server for this NAH and is communicated to Cisco Secure ACS.

5　Cisco Secure ACS uses quarantine as the final posture, which is referred to as the system posture token (SPT), and takes the actions assigned to a quarantine state. The actions can include the following:

— **Enforce quarantine access**—This varies based on the NAD.

For NAC-L3-IP, the enforcement actions include a quarantine ACL being applied to the endpoint.

For NADs using NAC-L2-IP, the enforcement actions include a quarantine ACL being applied to the endpoint.

For NADs using NAC-L2-802.1x, the enforcement action includes a quarantine VLAN.

— **Enforce Redirection (optional)**—In this example, the endpoint device is assigned a URL redirect to the remediation server.

6　The NAD receives the quarantine policy enforcement from Cisco Secure ACS. It quarantines the endpoint and sends the endpoint a redirect URL to go to the remediation server.

7　The endpoint is now quarantined and redirected to a remediation server. With NAH, the URL redirect is the only way to provide feedback to the user because there is no posture agent present. At this point, the user can elect to do nothing and remain quarantined, or comply and allow their host to remediate by installing Cisco Trust Agent.

From this point, the NAC Framework process is the same as the example in which the endpoint state changed from quarantine to healthy as shown in Figure 6-3.

Deployment Models

Cisco NAC Framework is a flexible solution providing protection to connected endpoints regardless of network connectivity. As shown in Figure 6-5, it operates across all access methods including campus switching, wired and wireless, WAN and LAN links, IP Security (IPSec) connections, and remote access links.

Figure 6-5 *NAC Deployment Scenarios*
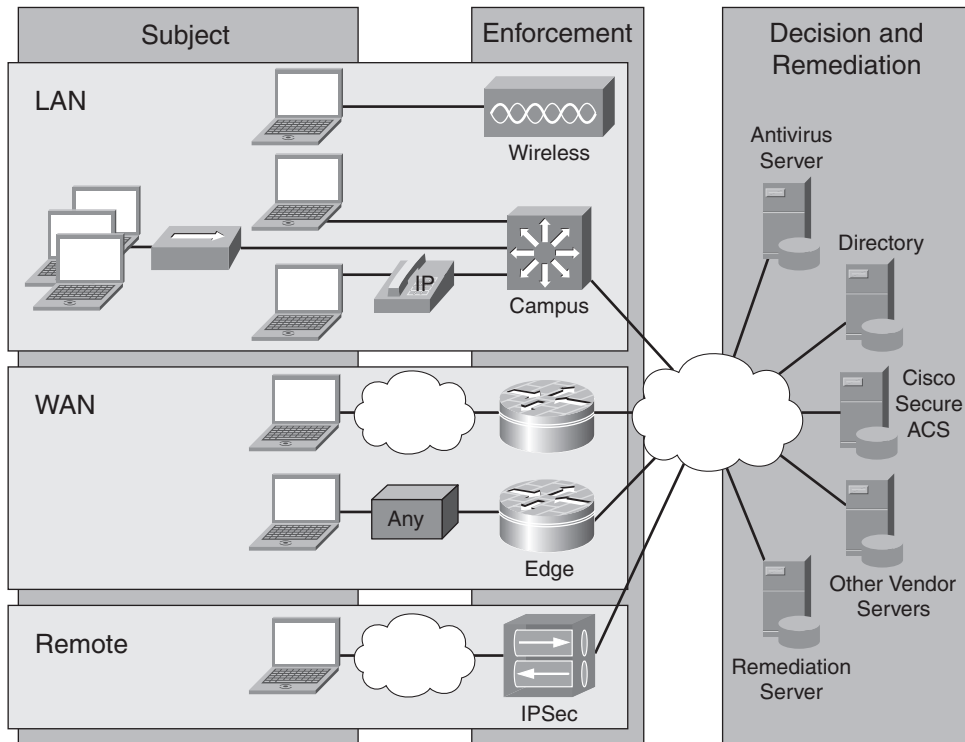
The first NAC Framework deployment rule of thumb is to use the NAC-enabled NAD closest to the endpoints for checking compliance, helping enforce a least-privilege principle. The second rule is that compliance checking for an endpoint should occur at one NAD (closest to the endpoint), not throughout the network. The NAD might not be capable of performing compliance checks or enforcing the admission policy. Examples include non-Cisco devices or an older NAD that does not support NAC. As a result, NAC deployments will vary.

The following sections describe common NAC deployment scenarios.

LAN Access Compliance

NAC monitors desktops and servers within the office, helping to ensure that these endpoints comply with corporate antivirus and operating system patch policies before granting them LAN access. This reduces the risk of worm and virus infections spreading within an organization by expanding admission control to Layer 2 switches.

NAC Framework can also check wireless hosts connecting to the network to ensure that they are properly patched. The 802.1x protocol can be used in combination with device and user authentication to perform this validation using the NAC-L2-802.1x method. Some businesses might not want to use the 802.1x supplicant, so instead they may choose to use the NAC-L2-IP method using either IP or MAC.

NAC can be used to check the compliance of every endpoint trying to obtain network access, not just those managed by IT. Managed and unmanaged endpoints, including contractor and partner systems, may be checked for compliance with antivirus and operating system policy. If the posture agent is not present on the interrogated endpoint, a default access policy can be enforced limiting the endpoint to a specific subnet, thus limiting its ability to infect other devices on the entire network.

WAN Access Compliance

NAC Framework can be deployed at branch or home offices to ensure that endpoints comply with the latest antivirus and operating system patches before allowing them access to WAN or Internet connections to the corporate network. Alternatively, compliance checks can be performed at the main office before access is granted to the main corporate network.

Remote Access Compliance

NAC Framework helps to ensure that remote and mobile worker endpoints have the latest antivirus and operating system patches before allowing them to access company resources through IP Security (IPsec) and other virtual private network (VPN) connections.

Summary

The Cisco Network Admission Control is a framework comprising Cisco networking infrastructure along with a variety of partner products to enforce network admission policies on NAC-enabled endpoint devices, guaranteeing software compliance before granting network access.

The Cisco NAC Framework consists of the following components:

- NAC-enabled security applications such as antivirus and host intrusion protection systems such as Cisco Security Agent
- Posture agents such as Cisco Trust Agent
- Network access devices such as routers, switches, and wireless access points
- Cisco Secure ACS, which is the Cisco Policy Server
- Optional third-party validation policy servers
- Optional management and reporting tools

NAC allows the appropriate level of network access only to compliant and trusted endpoint devices such as PCs, servers, and PDAs. NAC can also identify noncompliant endpoints, deny them access, and place them in a quarantined area or give them restricted access to computing resources.

NAC agentless hosts can be identified by exception lists, whitelisting, or audit servers and can be evaluated before granting network access.

NAC Framework operates across all network access methods including campus switching, wired and wireless, router WAN and LAN links, IPSec connections, remote access, and dial-up links.

References

[1] Cisco Systems, Inc. NAC Customer Profile Reference by Russell Rice. Network Admission Control (NAC) Cisco Security SEVT Update. April 6, 2005.

[2] Cisco Systems, Inc. NAC Agentless Host Exceptions and Whitelisting. 2005.

[3] Cisco Systems, Inc. Network Admission Control (NAC). 2005.