CHAPTER 3

The Building Blocks in a Cisco NAC Appliance Design

Knowledge of how to properly design security solutions is what separates the professional from the amateur. Without a proper design, the eventual implementation will most likely be a disaster. One of the keys to success when designing a security solution is to first understand all the pieces you have to work with. I like to call these building blocks. After you achieve understanding, you then need to become skilled at manipulating the pieces in ways that best fit your environment. This chapter focuses on the building blocks available with the Cisco NAC Appliance solution. The purpose and function of each piece is covered. The requirements, scalability, and performance of these building blocks are also discussed. The next chapter discusses your options for manipulating these building blocks.

Cisco NAC Appliance Solution Components

A NAC Appliance solution is made up of the following components:

- Mandatory components:
  - Cisco NAC Appliance Manager (Clean Access Manager)
  - Cisco NAC Appliance Server (Clean Access Server)
- Optional components:
  - Cisco Clean Access Agent
  - Cisco NAC Appliance Network Scanner

Each piece has a distinct role to play in the solution. In this section, you examine the roles of each in more detail.

NOTE Cisco NAC Appliance was formerly known as Cisco Clean Access. The legacy name Clean Access is still widely used in the industry, but this book will use the new name: Cisco NAC Appliance.

Cisco NAC Appliance Manager

The roles of NAC Appliance Manager are as follows:

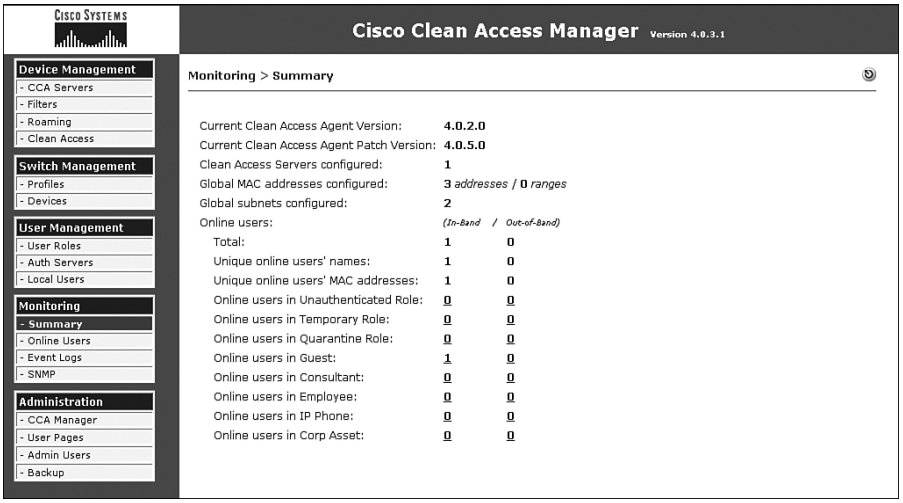
- Central administration and monitoring
- Management of up to 40 NAC Appliance Server pairs
- Central configuration of security policy and requirements
- Performing automatic download of the latest Clean Access policies and updates
- Centrally controlling network devices
- Central user authentication to back-end authentication sources such as Lightweight Directory Access Protocol (LDAP), RADIUS, and Kerberos

NAC Appliance Manager is the administration server. It allows you to centrally manage and monitor your deployment of NAC Appliance Servers and Agents. It is here that you configure your security policies that define the checks your hosts will have to pass to be considered clean or up to date. The NAC Appliance allows you to build your own customized checks, but it also comes with many preconfigured checks. It is a big job to manually maintain and track all the new updates that come out for antivirus, antispyware, Microsoft Windows, and so on. That is why the NAC Appliance Manager is also responsible for receiving regular version and policy updates from Cisco. These policy updates contain information on the latest operating system patches, antivirus versions, and antispyware versions. The prepackaged software checks and security policies are automatically updated with this new version information. Using the policy update feature makes it easier to ensure your hosts are always checked for the latest versions before they are allowed network access.

NAC Appliance Manager is configured using a web console after a minimal bootstrapping process. NAC Appliance Manager is capable of scaling to administer up to 40 NAC Appliance Server pairs. NAC Appliance Manager's web console allows you to configure both global security policies and per-server local policies. Global security policies save time and are much easier to manage. For example, you could create a global policy that says all hosts connecting to the network through any NAC Appliance Server must have an up-to-date antivirus program installed. NAC Appliance Manager then pushes this policy out to all the NAC Appliance Servers for local checking and enforcement. If you have some specific local security policies that pertain to only a single NAC Appliance Server, you can use NAC Appliance Manager's web console to configure those as well. Figure 3-1 shows NAC Appliance Manager's web console.

NAC Appliance Manager is responsible for authenticating all users in the NAC Appliance deployment with the exception of single sign-on (SSO) users. SSO users are authenticated by the local NAC Appliance Server. NAC Appliance Manager can use either its local user database or an external user database such as LDAP or RADIUS as an authentication source.

Figure 3-1 *NAC Appliance Manager Web Console*



Cisco NAC Appliance Server

The roles of the NAC Appliance Server are as follows:

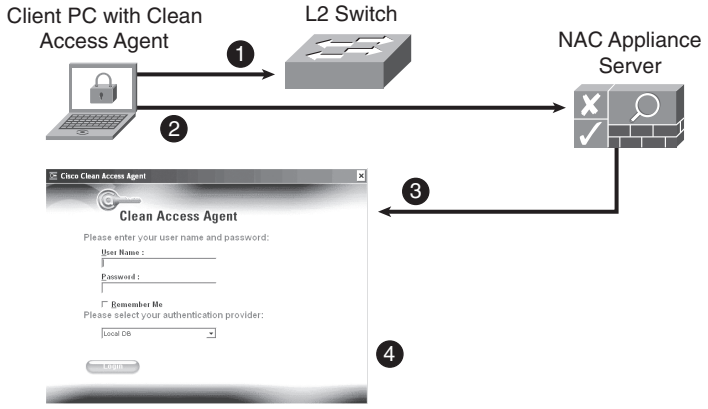
- Security policy assessment
- Security policy enforcement

NAC Appliance Server is the policy enforcer, or the policy firewall, between the untrusted networks and the trusted networks. NAC Appliance Server's job is to enforce the security policies created in NAC Appliance Manager. NAC Appliance Server, in conjunction with NAC Appliance Manager, actively checks the identity of users and the security posture of their host when they try to obtain access to the network. Based on the results of the check, NAC Appliance Server enforces the proper network access policy. It is important to note that NAC Appliance Server and NAC Appliance Manager act as a team in this process. NAC Appliance Server is mostly responsible for asking for authentication and posture information from the clients. This information is then forwarded to NAC Appliance Manager for checking. Based on the results, NAC Appliance Manager instructs the server to start enforcing a particular policy for that client.

For NAC Appliance Server to work, it must be physically or logically inline between the clients and their destinations during the initial posture assessment and remediation. After the clients pass the posture assessment, NAC Appliance Server can be removed from the dataflow (out of band) or remain in the dataflow (in band). The next chapter will discuss these different options in detail.

Clients can use either the Clean Access Agent or web login to trigger NAC Appliance posture assessment. Figure 3-2 illustrates the steps that trigger inspection of a client with a Clean Access Agent preinstalled.

Figure 3-2 *Steps to Trigger Assessment Using a Clean Access Agent*



The following is an explanation of the numbered process in Figure 3-2.

Step 1 The host plugs into a switch port and requests a DHCP address. Acting as the DHCP server, NAC Appliance Server replies to the host's DHCP request. Clean Access Agent detects the new network connection.

Step 2 To find NAC Appliance Server, Clean Access Agent sends out discovery packets to all the default gateways present in the host's routing table. In Figure 3-2, NAC Appliance Server is the host's default gateway and receives the discovery packets.

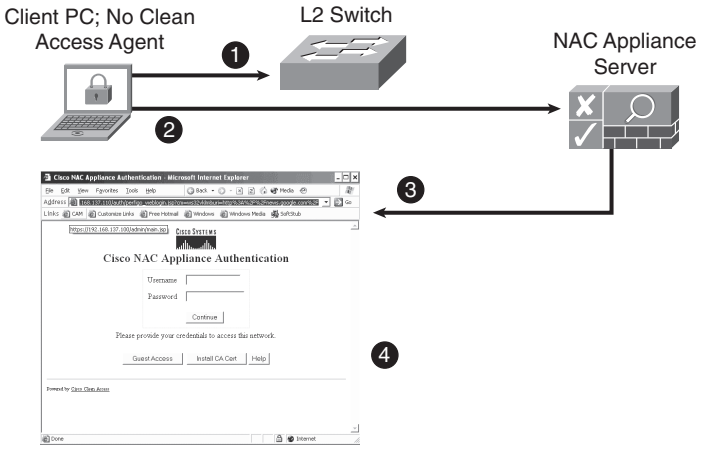
Step 3 The discovery packets trigger NAC Appliance Server to perform assessment of the new host. First it checks to see whether the host MAC address is already permitted. If so, the host is allowed to pass through NAC Appliance Server. If not, NAC Appliance Server sends back a login request to Clean Access Agent.

Step 4 Clean Access Agent pops up the agent log in a dialog box and waits for the user to enter a username and password.

NOTE Clean Access Agent uses a proprietary discovery protocol called SWISS. SWISS runs on UDP port 8905 for Layer 2 users and 8906 for Layer 3 users. Clean Access Agent performs discovery every 5 seconds. The NAC Appliance Server listens on UDP 8905/8906 for the SWISS packets being sent from the agents.

Figure 3-3 illustrates the steps that trigger inspection of a client using the web login.

Figure 3-3 *Steps to Trigger Assessment Using Web Login*



The following is an explanation of the numbered process in Figure 3-3.

Step 1 The host plugs into a switch port and requests a DHCP address. Acting as the DHCP server, NAC Appliance Server replies to the host's DHCP request.

Step 2 The user launches a web browser and requests a website. NAC Appliance Server sees this request. It checks the MAC address or IP address of the host to see whether it is already permitted. If so, the host is allowed on the network. If not, NAC Appliance Server intercepts the web request.

Step 3 The web page request triggers NAC Appliance Server to perform assessment of the host. The intercepted web page request is stopped, and a redirect to NAC Appliance Server's web login page is sent back to the user's web browser.

Step 4 The user is redirected and presented with the web login page. NAC Appliance Server waits for the client to log in or click on guest access.

CAUTION Before a successful login, all clients are in the Unauthenticated role. Client traffic in this role will by default be dropped by NAC Appliance Server. The exceptions are DHCP and DNS queries, which are allowed through. Therefore, if other traffic types and services are required, you will have to customize the traffic filters. A common example of this is allowing clients to log in to the Windows Active Directory (AD) domain when they first boot up.

NAC Appliance Manager's web console is used to centrally manage NAC Appliance Servers. However, each server does have a local web console and supports Secure Shell (SSH). These can be useful for troubleshooting purposes but are not generally used for local configuration after NAC Appliance Server's initial setup script is run.

Cisco Clean Access Agent

Technically, Clean Access Agent and Network Scanner are optional components. However, in most cases, you will use the Clean Access Agent and Network Scanner in your deployment.

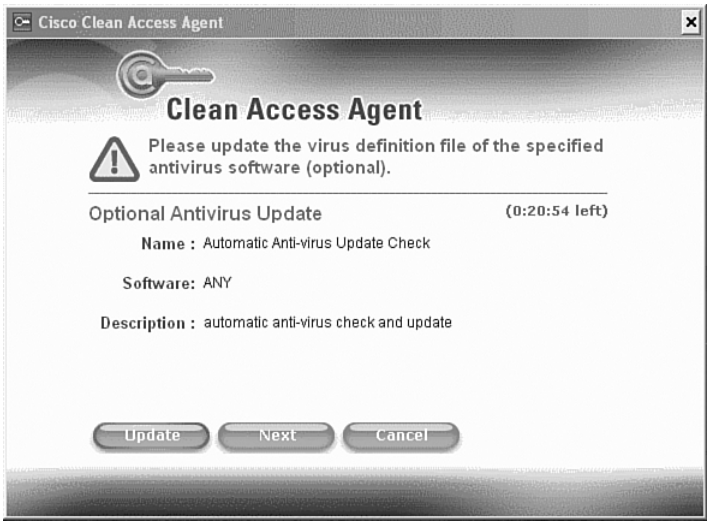
CAUTION If you choose not to use either the Clean Access Agent or the Network Scanner, then you cannot perform any host security assessment checks (for example, checking for up-to-date antivirus definitions). You will, however, be able to perform user authentication checking via web login.

Clean Access Agent is a free software program that resides on client PCs. It is a read-only agent whose job is to gather information about the user and the host it is installed on. It then matches that against the requirements received for that user, role, or OS from NAC Appliance Server and sends back a report to NAC Appliance Manager via NAC Appliance Server. If the requirements are met, the host is allowed on the network. If the host fails, Clean Access Agent presents the user, via a dialog box, with the remediation instructions received from NAC Appliance Manager. The information it checks for is configured by you at the NAC Appliance Manager level and then pushed out to each NAC Appliance Server. The information that can be checked by Clean Access Agent includes applications, files, registry keys, and services. For example, Clean Access Agent could check for the presence of a Windows hotfix or check to see whether an antivirus program is current.

Hosts that fail a system check are then put into a Clean Access Agent Temporary role. This role is configured to restrict network access to only those resources they will need to remediate their host. This may include access to websites, such as update.microsoft.com, or access to antivirus vendor update servers (local or on the Internet). These restrictions are enforced at the closest NAC Appliance Server in the traffic path of Clean Access Agent. No enforcement is done locally at the Clean Access Agent level. Clean Access Agent will then help the user fix up, or remediate, the host. It uses pop-up dialog boxes to notify the user of

security policy violations that have occurred. It also provides a remediation button to fix the violation. See Figure 3-4 for an example.

Figure 3-4 *Clean Access Agent Remediation Example*



Cisco NAC Appliance Network Scanner

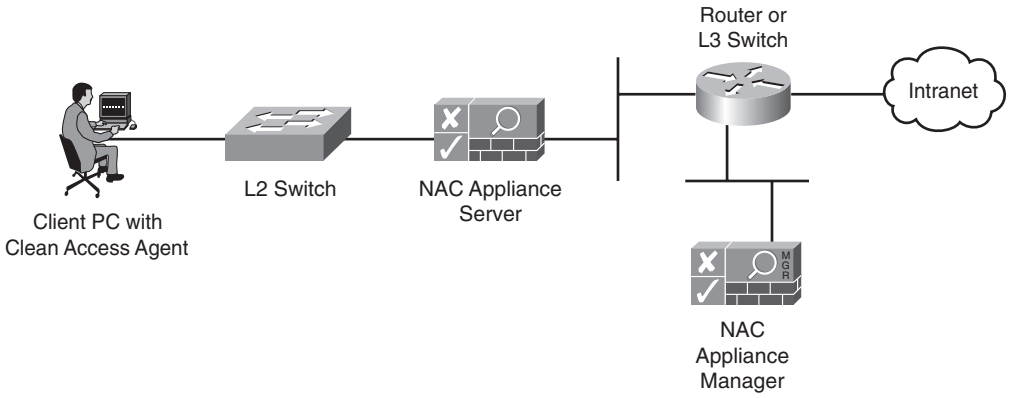
Network Scanner allows you to scan hosts to check for known vulnerabilities. Network Scanner is integrated into the NAC Appliance Manager and NAC Appliance Server software and is not a standalone piece. Network Scanner uses Nessus to scan hosts. You add in the Nessus plug-ins of your choice. For example, you can add the plug-ins that check to see whether music file-sharing applications are running on the host. If such programs are running, you could notify the end users that they must disable or uninstall the offending software before they are allowed on the network. Network Scanner can also be used to posture assess hosts that run operating systems not supported by Clean Access Agent, such as Linux.

TIP For more information about the Nessus tool and its plug-ins, visit http://www.nessus.org or http://www.nessus.org/plugins.

The following simple example illustrates where the pieces of a Cisco NAC Appliance design are placed in a network. Figure 3-5 shows a NAC Appliance deployment using

Layer 2 in-band. Layer 2 means that NAC Appliance Server is Layer 2 adjacent to the clients it will control. In-band means that data traffic always flows through NAC Appliance Server.

Figure 3-5 *Cisco NAC Appliance Deployment Example (Layer 2 In-Band)*



Cisco NAC Appliance Minimum Requirements

Cisco NAC Appliance Manager and NAC Appliance Server can be purchased two ways. You can buy only the software from Cisco and buy the hardware somewhere else, or you can buy the hardware and the software together in one of several appliance models available from Cisco. Typically, the term *appliance* means that the hardware and software come as a unit and you don't have the flexibility to buy your own hardware.

That is not the case with NAC Appliance. The NAC Appliance software-only option is packaged on a bootable CD or DVD in such a way that it completely self-installs everything you need on the hardware of your choice. There are no install scripts to run or questions to answer; just pop in the CD or DVD, boot up the system, wait a few minutes, and then you have NAC Appliance Manager or NAC Appliance Server ready to be configured.

However, the recommended path is to purchase the hardware and software NAC Appliance from Cisco. This is a true appliance and comes preinstalled and ready to go. It makes for a cleaner solution. There are three NAC Appliance hardware and software models. Table 3-1 shows the mapping of licenses to appliance models. A 3310 or 3350 appliance can be purchased as either NAC Appliance Manager or NAC Appliance Server—the hardware supports both. A 3390 supports only NAC Appliance Manager.

Table 3-1 *Cisco NAC Appliance 3300 Series*

	Cisco NAC Appliance 3310	Cisco NAC Appliance 3350	Cisco NAC Appliance 3390
Cisco NAC Appliance Server	Supported User Licenses: 100, 250, 500	Supported User Licenses: 1500, 2500, 3500	
Cisco NAC Appliance Manager	NAC Appliance Manager Lite—supports up to three NAC Appliance Server pairs	NAC Appliance Manager—supports up to 20 NAC Appliance Server pairs	NAC Appliance Super Manager—supports up to 40 NAC Appliance Server pairs

The 3350 and 3390 appliances both include an SSL accelerator card and a hard disk array. The sections that follow describe the requirements for each component of the solution.

Cisco NAC Appliance Manager and Server Requirements

Cisco NAC Appliance is sold as software only or as an appliance with hardware and software preinstalled. If you go the software-only route, you have to provide your own hardware. This hardware must be on the current supported server configurations list. Hardware not on the list will not be supported by Cisco Technical Assistance Center. To obtain the current supported server list, go to http://www.cisco.com and search for "supported server configurations nac." After you select a supported server vendor and model, make sure that it meets the NAC Appliance minimum requirements listed in Table 3-2. Of course, if you go with the Appliance-packaged version of NAC Appliance, you do not need to worry about any of this; it is already optimized.

Table 3-2 *NAC Appliance Manager and Server Minimum Requirements*

Component	Minimum Requirement
CPU	Single 2.4 GHz or greater.
RAM memory	1 GB or greater (see "Reasons to Exceed the Recommended minimum Requirements").
Hard disk space	10 GB or greater.
NICs[1]	Dual Fast or Gigabit Ethernet ports (see "Reasons to Exceed the Recommended minimum Requirements"). Intel or Broadcom recommended.
Web browser for web admin console	Internet Explorer 6.0 or above is required.

1. network interface cards

CAUTION Always check the latest NAC Appliance Release Notes at Cisco.com for the most up-to-date details about hardware and software requirements.

Reasons to Exceed the Recommended Minimum Requirements

It is generally a good idea to exceed the minimum requirement's but here are some specific reasons.

RAM Memory:

- Consider 2 GB of memory or greater if you plan to deploy NAC Appliance Manager with a large number of device filters, traffic policies, local users, or multiple NAC Appliance Servers fully loaded with more than 1000 users
- Consider 2 GB of memory or greater if you are deploying NAC Appliance Server as a DHCP server, configuring /30 subnets, or supporting close to 1500 users.

Network Interface Cards:

- If running NAC Appliance Servers in High Availability mode, it is recommended to configure a third NIC card. That NIC will be dedicated for high availability purposes.
- You should have 2 GB of memory if you have more than 500 users.

Cisco Clean Access Agent Requirements

The Cisco Clean Access Agent currently runs on Windows and Macintosh operating systems. Table 3-3 provides details as to the host requirements needed to run the Agent. Be sure to check Cisco.com to see whether additional operating systems or requirements have been added.

Table 3-3 *Clean Access Agent Requirements*

Host	Requirement
Supported operating systems	Microsoft Vista (all versions, including Japanese), Windows XP Professional, Windows XP Home, Windows XP MCE, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE, Windows Me, Japanese and simplified Chinese Windows XP SP2 Mac OS X[1]
Hard drive space	Minimum of 10 MB free
Hardware	No minimum requirements

1. Mac OS X agent currently supports only user authentication. No host posture assessment checks are supported. This is a roadmapped feature; check with Cisco for availability.

Scalability and Performance of Cisco NAC Appliance

To ensure a good design, understanding the scalability and performance limits of NAC Appliance is important. Table 3-4 depicts the scalability and performance numbers that are relevant to properly designing a NAC Appliance solution.

Table 3-4 *Scalability and Performance of NAC Appliance*

NAC Appliance Manager	Maximum Managed Server Pairs/Manager	20
NAC Appliance Super Manager	Maximum Managed Server Pairs/Manager	40
NAC Appliance Server	Data Throughput/Server	~950 Mbps
	Maximum Users/Server	3500
	Maximum MAC Addresses/Server	8000

Summary

This chapter examined the various building blocks that make up the Cisco NAC Appliance solution. Those building blocks are as follows:

- Cisco NAC Appliance Manager
- Cisco NAC Appliance Server
- Cisco Clean Access Agent
- Cisco NAC Appliance Network Scanner

The purpose and function of each piece was covered and can be summarized as follows:

- NAC Appliance Manager is the administration server. It allows you to centrally manage and monitor your deployment of NAC Appliance Servers and Clean Access Agents.
- NAC Appliance Server is the policy enforcer, or the policy firewall, between the untrusted networks and the trusted networks. NAC Appliance Server's job is to enforce the security policies created in NAC Appliance Manager.
- Clean Access Agent is a free software program that resides on client PCs. It is a read-only agent whose job is to gather information about the user and host it is installed on.
- NAC Appliance Network Scanner allows you to scan hosts to check for known vulnerabilities. It uses the embedded Nessus vulnerability scanning software for this function.

The chapter finished with an overview of the minimum hardware and software requirements and performance metrics of the different building blocks. It was recommended that the newer appliance form factors be used for the NAC Appliance Manager and NAC Appliance Server pieces.