Introducing Network Admission Control

This chapter provides background information required to implement Network Admission Control (NAC), an industry-wide collaboration sponsored by Cisco Systems. It includes the following sections:

Overview

This section describes the benefits of NAC and how it works, and includes the following topics:

The Benefits of Network Admission Control

Virus infection on data networks has become an increasingly serious problem. The resources consumed during just one disinfection process are much greater than the resources necessary to implement an anti-virus feature in the network such as Network Admission Control.

Cisco NAC helps ensure the health of client workstations before they are granted network access. NAC works with anti-virus software to assess the condition, called the posture, of a client before allowing access to the network.

NAC helps ensure that a network client has an up-to-date virus signature set and has not been infected before gaining access to a data network. If the client requires a signature update, the NAC solution directs it to complete the update. If the client has been compromised or if a virus outbreak is occurring on the network, NAC places the client into a quarantined network segment until disinfection is completed.

How Network Admission Control Works

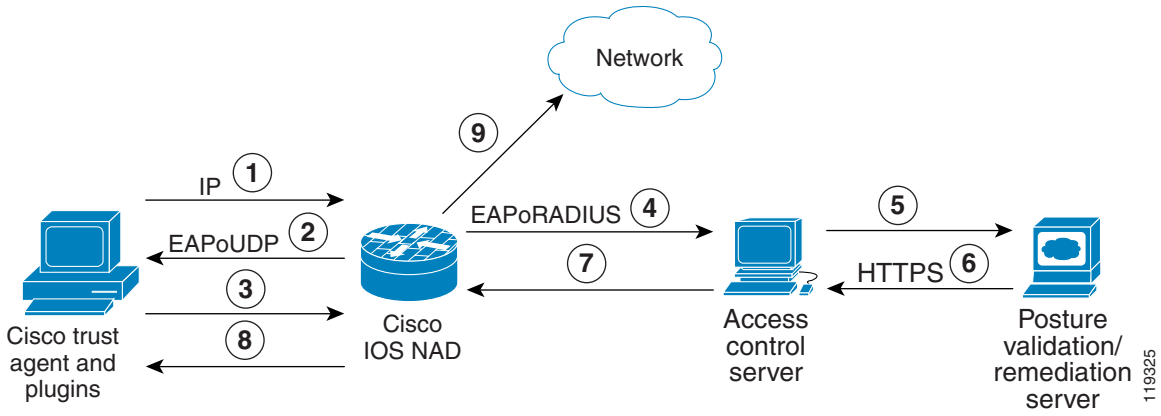
NAC implementation combines a number of existing protocols and Cisco products with some new products and features, including the following:

- Cisco Trust Agent (CTA) and plug-ins
- Cisco IOS Network Access Device (NAD)
- Extensible Authentication Protocol (EAP)
- Cisco Secure Access Control Server (ACS)/Remote Authentication Dial-In User Service (RADIUS)
- Posture validation/remediation server

CTA communicates with other software on the client computer over a published Application Program Interface (API) and answers posture queries from the NAD. CTA also implements the communication (EAP over UDP) necessary to implement NAC. The resident software includes a Posture Plug-In (PP) that interfaces with the CTA. The PP is an agent included with third-party software that reports on the policy and state of this software.

In the current implementation of NAC, the NAD is a Layer 3 Cisco IOS software device that queries client machines seeking network access using EAP over UDP (EOU). The way that the different components of the NAC solution interact is shown in Figure 1-1.

Figure 1-1 NAC Operation



NAC component interaction occurs as follows:

1. Client sends a packet through a NAC-enabled router.
2. NAD begins posture validation using EOU.
3. Client sends posture credentials using EOU to the NAD.
4. NAD sends posture to Cisco ACS using RADIUS.

5. Cisco Secure ACS requests posture validation using the Host Credential Authorization Protocol (HCAP) inside an HTTPS tunnel.
6. Posture validation/remediation server sends validation response of pass, fail, quarantine, and so on.
7. To permit or deny network access, Cisco Secure ACS sends an accept with ACLs/URL redirect.
8. NAD forwards posture response to client.
9. Client is granted or denied access, redirected, or contained.

When the client sends a request for network access (1), the NAD starts the posture validation process (2). The identity it receives from the CTA is passed on to Cisco Secure ACS, which then initiates a protected EAP (PEAP) session with the CTA (the PEAP session is not shown).

CTA then sends its credential with any credentials it gets from PPs on the client machine to the NAD (3), which forwards them using the RADIUS protocol to Cisco Secure ACS (4). These credentials contain attributes that hold information about the current state of the client software.

Cisco Secure ACS checks and validates the credentials by comparing the attributes contained in the credentials against its policy database. Cisco Secure ACS can also be configured to pass these credentials and attributes to an external server for validation (5). This is done using HCAP over an HTTPS tunnel. This may be the preferred option when client software comes with a PP and an external posture validation server for credential evaluation.

Where there is an external posture validation server, the external server checks the credentials and attributes against its internal database and returns an application posture token (APT) to Cisco Secure ACS. Cisco Secure ACS then collects all APTs from any local or external policies. The most restrictive of these APTs becomes the system posture token (SPT).

Cisco Secure ACS then places the client in a group corresponding to its SPT. These groups correspond to the access rights granted by the SPT and may be Healthy, Checkup, Quarantine, Infected, or Unknown. Cisco Secure ACS then sends the appropriate access control list (ACL) for the group to the NAD to be applied against the client (8).

Cisco Secure ACS can optionally include an HTTP redirect in the returned policy sent to the NAD to force a client to visit a particular server for a mandatory update and to determine if remediation has occurred.

A posture agent can be developed to return information contained in its credential by the CTA that can be used in many ways, including assessment for host intrusion detection system (HIDS), host intrusion prevention system (HIPS), personal firewalls, operating system patch levels, and application version control.

NAC Operational Detail

This section provides additional details about the NAC process for those who want to understand the process at a more technical level. This level of understanding is not required to implement NAC, but is helpful for troubleshooting and fine-tuning the process.

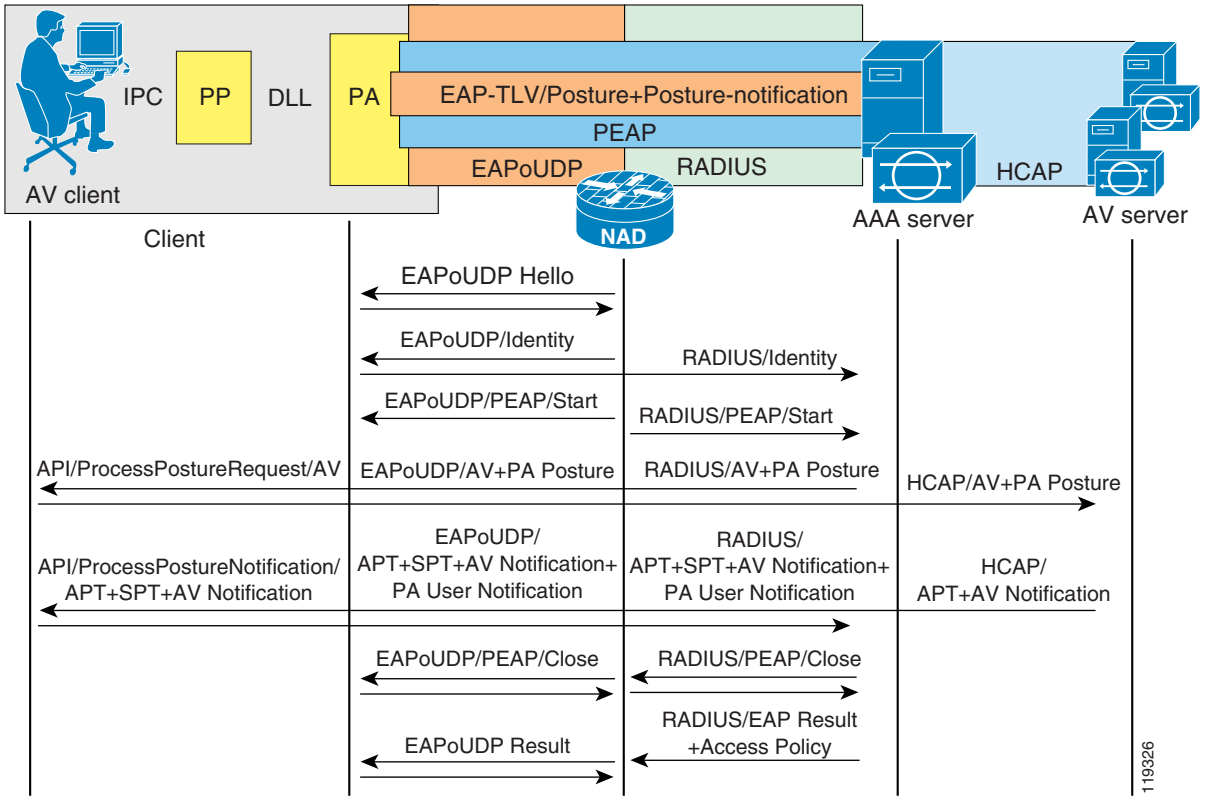
NAC is dependant on a Layer 3 Cisco IOS software device for policy enforcement. The installation of CTA and any compatible client software has no effect until the required commands are configured on the Cisco IOS software enforcement device, called the NAD.

The admission control process is triggered by a Layer 3 packet entering a router interface with admission control configured. After the NAC process is triggered, the router sends an EOU hello message to which the client host answers with an EOU hello. When the NAD and client recognize each other, the NAD asks for the identity of the client. When received, this identify is passed to Cisco Secure ACS in the form of an EAP over RADIUS packet. Cisco Secure ACS then initiates a PEAP session with the client host.

Note that the router acts as a pass-through device at this point; it does not proxy any part of the PEAP session but merely re-encapsulates the PEAP packets from UDP to RADIUS.

After the PEAP session has been established, Cisco Secure ACS queries the client for the credentials from registered software on the client. This causes the CTA on the client to query the PPs that have been registered with CTA for their credentials and attributes. These credentials and attributes are collected and sent to Cisco Secure ACS in the PEAP session. During this initialization phase, the packets received on the router interface are subject to any access list applied on that interface. Some packets may be dropped during this initialization. Figure 1-2 shows the details of this process.

Figure 1-2 Protocol Flows



When Cisco Secure ACS receives the credentials from the CTA, it looks for a NAC external user database configured in ACS with the best match of the same mandatory credentials as those it received from the CTA. The NAC external user databases have one or more policies configured in them. When the Cisco Secure ACS finds a match, it checks the credentials and attributes against any local or external policies in the matched database. These policies specify the values that the attributes in the received credentials must have to meet the admissions policy for the configured network.

Each policy returns an APT in a single credential back to the client, along with any supported actions, which are unique to each posture agent. The most restrictive of the application posture tokens are used as the SPT. The SPT determines the group into which Cisco Secure ACS places the client and the overall posture of that client. The actual enforcement rules are configured in the Cisco Secure ACS group policy. Enforcement rules take the form of downloadable ACLs, URL redirection, and timer adjustments. These enforcement rules are sent to the NAD by ACS at the termination of a successful validation session.

The NAD periodically queries the host to determine whether the posture of the client has changed or whether the host is the same host that has gone through the validation process. The NAD can also enforce a URL redirection to cause a client to automatically go to an attribute-value (AV) server for updates when the client attempts web access. This URL redirection is configurable from Cisco Secure ACS for each posture state.

You can also configure Cisco Secure ACS to shorten the status query value or the re-validation time on the NAD by sending a Cisco IOS AV pair with the specific timer values to be applied for a particular client to help ensure that the client successfully completes the remediation process. As each application is remediated, the application APT returns to a healthy condition, and eventually a healthy SPT is achieved.

If there has been a change, such as a new DHCP address being assigned or a changed DHCP client, (the client holding that address has dropped off line and a new client has been assigned the same address), the status query process fails and the validation process is restarted. If no response is received from the client, the system can download a default enforcement policy to the NAD to limit the network access of the client, depending on the overall network security policy.

Limitations and Guidelines

NAC is a Layer 3 technology, and NAC posture validation and enforcement is currently restricted to Layer 3.

Because communication between Cisco Secure ACS and the CTA uses PEAP, the CTA must trust Cisco Secure ACS. This trust is established using X.509 certificates. If you already have a certification authority (CA), you can generate a certificate signing request from Cisco Secure ACS and send it to your CA for enrollment. The CA (root) certificate must be installed on each client taking part in admission control. CA certificate installation occurs automatically at installation time if the certificate is placed in the \certs directory located below the directory from which the program ctasetup.exe is run. For details, see the section on CTA installation.

Cisco Secure ACS can also generate a self-signed certificate. In this case, the certificate from Cisco Secure ACS is installed on each client taking part in the admissions control process. This also occurs automatically if the certificate is placed in the \certs directory located below the directory from which ctasetup.exe is run.

If you generate an external private key and certificate for use on Cisco Secure ACS, you must install the certificate and private key files on Cisco Secure ACS.

Pre-Deployment Considerations

Successful deployment of NAC requires some planning ahead of the deployment. The primary consideration is the handling of clients as they go through the NAC process. This includes enforcement action for clients without CTA installed yet. Consider using a phased enforcement policy initially to limit the enforcement action taken when a large number of clients do not yet have CTA installed. This significantly limits network disruption.

This section describes other issues to consider and includes the following topics:

- Access Restrictions for Postured Clients
- Non-Responsive Hosts Handling

Access Restrictions for Postured Clients

This section provides an overview of the access restrictions for postured clients and describes the various conditions for which NAC tests. It includes the following topics:

Category and Token Assignment

During the admission control process, clients are placed into a particular category and are assigned a token. One token is assigned per policy configured in the Cisco Secure ACS NAC external user databases. The token assigned depends on the values of the attributes contained in the credential originated by the NAC-compliant software on the client. The assigned categories of these returned tokens give each client specific access rights.

Category assignment can also cause pop-up messages to appear on the client screen and redirect a web browser to a specific URL. Cisco Secure ACS can send configured actions to individual software applications taking part in NAC. The particular actions are not discussed in this document because they are specific to the different applications participating in NAC. These actions can include the triggering of a software update or some other type of software-specific action. See specific software documentation for more details about the configurable actions supported by your vendor software.

Healthy

The Healthy category is assigned when the information received from the client posture agent credentials are current with the policy defined in the NAC external user database on Cisco Secure ACS. In this case, the scanning engine and the signature files are considered current for an AV policy or the current policy for a personal firewall are current, and no further action needs to be taken by the user. Normally, no access restriction is placed on a client in this condition.

Checkup

The Checkup category is assigned when the client may have some files, either the AV signature file or the scanning engine or some other third party software that supports NAC, which is not completely current with the network admission policy. Users should upgrade their client software to maintain currency, but no access restrictions are normally placed on the client in this state. This state can trigger normal AV DAT file updates or other non-mandatory file upgrades. A pop-up message can be configured to alert the user of the available upgrade.

Quarantine

When a client is assigned to the Quarantine category, the user must take immediate action to update their anti-virus files. A client might be placed in this condition during a virus outbreak to prevent the spread of the virus or when a particular OS vulnerability has been discovered to force a personal firewall policy

upgrade. To enforce this policy, an ACL can be downloaded to the NAD that permits access only to the upgrade server, and a URL redirection can force the client to visit the upgrade server. This effectively blocks any other network access and forces the client to immediately come into compliance with the network access policy.

Infected

The Infected category can be assigned when the client has been actively infected with a virus. It is normally the job of the posture agent installed on the client to check for an infected condition.This condition triggers ACLs to be downloaded that prevent any network access by the infected client until a remediation process is completed. A pop-up message can notify the user of the state of the machine and indicate the required action that must be taken by that user. A URL re-direction is normally configured in this case.

Unknown

The Unknown category can be assigned when there is no CTA on the client or the host did not respond to the EOU queries by the NAD. This can occur with hosts that do not have the admission control software loaded, with hosts that have unsupported operating systems, or with IP devices that do not support NAC. A clientless exception policy can be configured that is applied to any clientless device present on an interface performing NAC by creating a “clientless user” in the IOS NAD configuration. The unknown group contains the access restrictions necessary for these devices. These exception policies can include the specific destination hosts with which the excepted devices are permitted to communicate.

Non-Responsive Hosts Handling

Generally speaking, a non-responsive host is a client without posture agent software loaded. These clients might be IP devices such as IP phones, network-attached printers, or other IP devices. Any PCs or workstations that do not have the CTA or posture agent software loaded are also considered non-responsive hosts. These workstations may be running MacOS, Solaris, or unsupported versions of Windows. This can also occur with a client that does not trust the Cisco Secure ACS that is performing the validation process. Non-responsive hosts may be handled in the following three ways:

- Static policy—This configuration is performed on the NAD device only. These devices can be statically excepted via IP address, MAC address, or by device type (such as a Cisco IP Phone).
- Clientless user—A clientless user name and password is configured on the NAD. The same username and password is configured on the Cisco Secure ACS, and the username is assigned to a particular group with the appropriate access restrictions configured. These access restrictions can include IP access lists and URL redirections. This method of handling non-responsive hosts is identical to the creation of a clientless user for the unknown category mentioned previously.
- Restricted access—This classification takes no action whatsoever. The interface ACL configured on the NAD provides the default access restrictions for all non-responsive hosts on that interface.

Static Policy

One way to handle a non-responsive host is to configure a static policy in Cisco IOS software, which includes the IP address of the host, the MAC address of the host, or the configured NAD host type; and building an ACL that identifies the IP addresses and networks with which an unknown host can communicate. To use a static policy for non-responsive host handling, certain information about the hosts must be known, and this information must remain static.

Clientless User

A second method of handling non-responsive hosts is to define a clientless user. A clientless user is simply a username and password that have been configured in the NAD to be used in a RADIUS authentication packet when no credentials have been received during the posture validation process. A corresponding user is created in Cisco Secure ACS with the appropriate access limitations. For example, the user is placed into the unknown group in Cisco Secure ACS or another group with specific access restrictions enforced by downloadable ACLs. This limits the access of non-responsive clients according to the security policy.

Default Access

A third way to handle non-responsive hosts is to allow them to fail the posture checking process without a static policy configured and without permitting a clientless user. This prevents any access other than what is expressly permitted by the interface ACL configured on the router interface on which the posture validation occurs.

System Components

NAC consists of components from Cisco and various third-party vendors. NAC requires a supported Cisco IOS software platform (a router) between the client undergoing the admissions process and the protected network. NAC also requires Cisco Secure ACS version 3.3 or later as an integral part of the admissions control process. The CTA is a client-side component provided by Cisco that resides on the client and provides an interface to supported third-party software.

This section provides some detailed information about the required system components and includes the following topics:

- Hardware Requirements
- Software Requirements

Hardware Requirements

This section describes the hardware requirements for NAC implementations and includes the following topics:

- Access Control Server Hardware Requirements
- Client Hardware Requirements
- Cisco IOS Software Platform Hardware Requirements

Access Control Server Hardware Requirements

Cisco Secure ACS requires an Intel workstation with the following minimum hardware requirements:

- Pentium III processor running at 550 Mhz or faster
- 256 MB of memory
- 250 MB of free disk space
- Minimum supported graphics resolution is 256 colors at 800 x 600 screen resolution

If a Cisco Secure ACS internal user database is running on the same computer running Cisco Secure ACS, more disk space is recommended.

Client Hardware Requirements

There are negligible additional requirements for the client machines other than the necessary memory and processor speed to run the anti-virus software and Cisco Security Agent. See the anti-virus vendor or CSA documentation for further details about client requirements.

Cisco IOS Software Platform Hardware Requirements

The Cisco hardware platforms that are supported as NADs in a NAC implementation are shown in Table 1-1. This table also summarizes the software images that support NAC, the amount of flash memory required, and the amount of dynamic RAM required for each platform.

Table 1-1 Cisco IOS Software Platform Hardware Requirements

Router Model	Image Name	DRAM Required	Flash Required
Cisco 83x Series Router	c831-k9o3sy6-mz c831-k9o3y6-mz	48 MB 48 MB	12 MB 8 MB
Cisco 1700 Series Router	c1700-adventerprisek9-mz c1700-advipservicesk9-mz c1700-advsecurityk9-mz	128 MB 96 MB 64 MB	32 MB 32 MB 16 MB
Cisco 1841 Integrated Services Router	c1841-advsecurityk9-mz.123-8.T5.bin	128 MB	32 MB
Cisco 2600XM IP Communications Voice/Fax NM	c2600-adventerprisek9-mz c2600-advipservicesk9-mz c2600-advsecurityk9-mz	128 MB 128 MB 96 MB	32 MB 32MB 32 MB
Cisco 2691 Multiservice Platform	c2691-adventerprisek9-mz c2691-advipservicesk9-mz c2691-advsecurityk9-mz	128 MB 128 MB 128 MB	64 MB 64 MB 32 MB
Cisco 2801 Integrated Services Router	c2801-advsecurityk9-mz.123-8.T5.bin c2801-advipservicesk9-mz.123-8.T5.bin c2801-adventerprisek9-mz.123-8.T5.bin	128 MB	64 MB
Cisco 2811, 2821, 2851 Integrated Services Router	c2800nm-advsecurityk9-mz.123-8.T5.bin c2800nm-advipservicesk9-mz.123-8.T5.binc 2800nm-adventerprisek9-mz.123-8.T5.bin	256 MB	64 MB

Table 1-1 Cisco IOS Software Platform Hardware Requirements (continued)

Router Model	Image Name	DRAM Required	Flash Required
Cisco 3640 Multiservice Platform	c3640-jk9o3s-mz	128 MB	32 MB
Cisco 3660-ENT Series Router	c3660-jk9s-mz	128MB	64 MB
Cisco 3725/3745 Multiservice Access Router	c37x5-adventerprisek9-mz c37x5-advipservicesk9-mz c37x5-advsecurityk9-mz	128 MB 128 MB 128 MB	64 MB 64 MB 32 MB
Cisco 3825 Integrated Services Router	c3825-advsecurityk9-mz.123-11.T2.bin	256 MB	64 MB
Cisco 3845 Integrated Services Router	c3845-advsecurityk9-mz.123-11.T2.bin	256 MB	64 MB
Cisco 7200 Series Router	c7200-jk9o3s-mz	128MB	48 MB

Each successfully validated client consumes a fixed amount of about 6 Kb. In addition, each downloadable ACL applied as a dynamic entry uses an additional .8 Kb of memory.

Software Requirements

NAC requires the following software:

- Cisco Secure ACS
- CTA on each client
- PP provided by a supported third-party anti-virus vendor

A posture validation server, which can be obtained from the anti-virus vendor with the appropriate PP, is optional. Table 1-2 summarizes the specific requirements for each of these components.

Table 1-2 Software Requirements

Component	Software Requirement
Access Control Server	• Any of the following: – Windows 2000 Server or Advanced Server with Microsoft Service Pack 3 or 4 – Windows 2003 Server Enterprise Edition • Either of the following: – Internet Explorer version 6.0 SP1 – Netscape 7.0.2 for browser access English language versions only are supported at this time. For further details, see the latest release notes available at the following URL: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/release/notes/RNwin332.html
Cisco Trust Agent	One of the following: • Microsoft Windows 2000 • Microsoft Windows XP • Microsoft Windows NT version 4.0 with Service Pack 4 or later • One or more posture plug-ins provided by a NAC-supported vendor
Cisco IOS software images	Advanced security images or greater, beginning with version 12.3(8)T. IOS version 12.3(8)T5 is recommended.

Third-Party Supported Software

A variety of third-party Cisco partners provide software that participates in the NAC solution. A list of the supported software and the third-party vendors can be found at the following URL: http://www.cisco.com/en/US/partners/pr46/nac/partners.html.