CHAPTER 7

Network Admission Control

This chapter includes the following sections:

Information about Network Admission Control

Network Admission Control protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy and vulnerability checks as a condition for production access to the network. We refer to these checks as *posture validation.* You can configure posture validation to ensure that the anti-virus files, personal firewall rules, or intrusion protection software on a host with an IPsec or WebVPN session are up-to-date before providing access to vulnerable hosts on the intranet. Posture validation can include the verification that the applications running on the remote hosts are updated with the latest patches. NAC occurs only after user authentication and the setup of the tunnel. NAC is especially useful for protecting the enterprise network from hosts that are not subject to automatic network policy enforcement, such as home PCs.

The establishment of a tunnel between the endpoint and the ASA triggers posture validation.

You can configure the ASA to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server, such as a Trend server, uses the host IP address to challenge the host directly to assess its health. For example, it may challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host.

Following successful posture validation or the reception of a token indicating the remote host is healthy, the posture validation server sends a network access policy to the ASA for application to the traffic on the tunnel.

In a *NAC Framework* configuration involving the ASA, only a Cisco Trust Agent running on the client can fulfill the role of posture agent, and only a Cisco Access Control Server (ACS) can fulfill the role of posture validation server. The ACS uses dynamic ACLs to determine the access policy for each client.

As a RADIUS server, the ACS can authenticate the login credentials required to establish a tunnel, in addition to fulfilling its role as posture validation server.

Note Only a NAC Framework policy configured on the ASA supports the use of an audit server.

In its role as posture validation server, the ACS uses access control lists. If posture validation succeeds and the ACS specifies a redirect URL as part of the access policy it sends to the ASA, the ASA redirects all HTTP and HTTPS requests from the remote host to the redirect URL. Once the posture validation server uploads an access policy to the ASA, all of the associated traffic must pass both the Security Appliance and the ACS (or vice versa) to reach its destination.

The establishment of a tunnel between an IPsec or WebVPN client and the ASA triggers posture validation if a NAC Framework policy is assigned to the group policy. The NAC Framework policy can, however, identify operating systems that are exempt from posture validation and specify an optional ACL to filter such traffic.

Prerequisites for NAC

When configured to support NAC, the ASA functions as a client of a Cisco Secure Access Control Server, requiring that you install a minimum of one Access Control Server on the network to provide NAC authentication services.

Guidelines and Limitations

Following the configuration of one or more Access Control Servers on the network, you must use the **aaa-server** command to name the Access Control Server group. Then follow the instructions in the "Configuring a NAC Policy" procedure on page 7-5.

ASA support for NAC Framework is limited to remote access IPsec and WebVPN client sessions. The NAC Framework configuration supports only single mode.

NAC on the ASA does not support Layer 3 (non-VPN) traffic and IPv6 traffic.

Viewing the NAC Policies on the Security Appliance

Before configuring the NAC policies to be assigned to group policies, we recommend that you view any that may already be set up on the ASA. Because the default configuration does not contain NAC policies, entering this command is a useful way to determine whether anyone has added any. If you, you may decide that policies already configured are suitable and disregard the section on configuring a NAC policy.

Detailed Steps.

	Command	Purpose

Step 1	**`show running-config nac-policy`**
	Example:
	`hostname# ` **`show running-config nac-policy`**
	`nac-policy nacframework1 nac-framework`
	` default-acl acl-1`
	` reval-period 36000`
	` sq-period 300`
	` exempt-list os "Windows XP" filter acl-2`
	`hostname#`
		Views any NAC policies that are already set up on the ASA.
		Shows the configuration of a NAC policy named nac-framework1

Step 2	• default-acl—NAC default ACL applied before posture validation. Following posture validation, the security appliance replaces the default ACL with the one obtained from the Access Control Server for the remote host. The ASA retains the default ACL if posture validation fails. • reval-period—Number of seconds between each successful posture validation in a NAC Framework session. • sq-period—Number of seconds between each successful posture validation in a NAC Framework session and the next query for changes in the host posture. • exempt-list—Operating system names that are exempt from posture validation. Also shows an optional ACL to filter the traffic if the remote computer’s operating system matches the name. • authentication-server-group—Name of the of authentication server group to be used for NAC posture validation.	Shows the nac-framework attributes.

	Command	Purpose

Step 3	`show nac-policy`
	Example:
	`asa2(config)#` **`show nac-policy`**
	`nac-policy framework1 nac-framework`
	`  applied session count = 0`
	`  applied group-policy count = 2`
	`  group-policy list:    GroupPolicy2    GroupPolicy1`
	`nac-policy framework2 nac-framework is not in use.`
	`asa2(config)#`
		Displays the assignment of NAC policies to group policies.
		Shows which NAC policies are unassigned and the usage count for each NAC policy.

Step 4	• applied session count—Cumulative number of VPN sessions to which this ASA applied the NAC policy. • applied group-policy count—Cumulative number of group polices to which this ASA applied the NAC policy. • group-policy list—List of group policies to which this NAC policy is assigned. In this case, the usage of a group policy does not determine whether it appears in this list; if the NAC policy is assigned to a group policy in the running configuration, then the group policy appears in this list.	Explains the fields in the show nac-policy command. **Note** When a policy is not assigned to any group policies, “is not in use” displays next to the policy type.

Refer to the following sections to create a NAC policy or modify one that is already present.

Adding, Accessing, or Removing a NAC Policy

Enter the following command to add or modify a NAC policy:

Detailed Steps

	Command	Purpose
Step 1	`global`	Switches to global configuration mode.

Step 2	**`nac-policy`** *nac-policy-name* **`nac-framework`**
	Example:
	`hostname(config)# `**`nac-policy nac-framework1 nac-framework`**
	`hostname(config-nac-policy-nac-framework)`
		Adds or modifies a NAC policy.
		nac-policy-name is the name of a new NAC policy or one that is already present. The name is a string of up to 64 characters.
		`nac-framework` specifies that a NAC Framework configuration will provide a network access policy for remote hosts. A Cisco Access Control Server must be present on the network to provide NAC Framework services for the ASA. When you specify this type, the prompt indicates you are in `nac-policy-nac-framework` configuration mode. This mode lets you configure the NAC Framework policy.
		Note You can create more than one NAC Framework policy, but you can assign no more than one to a group policy.
		Creates and accesses a NAC framework policy named nac-framework1.

Step 3	(Optional) [`no`] **`nac-policy`** *nac-policy-name* **`nac-framework`**	Removes a NAC policy from the configuration. You must specify both the name and type of the policy.
Step 4	(Optional) **`clear configure nac-policy`**	Removes all NAC policies fromthe configuration except for those that are assigned to group policies.
Step 5	**`show running-config nac-policy`**	Displays the name and configuration of each NAC policy already present on the security appliance.

Configuring a NAC Policy

After you use the **nac-policy** command to name a NAC Framework policy, use the following sections to assign values to its attributes before you assign it to a group policy.

Specifying the Access Control Server Group

You must configure at least one Cisco Access Control Server to support NAC.

Detailed Steps

	Command	Purpose
Step 1	**aaa-server host**	Names the Access Control Server group even if the group contains only one server.
Step 2	(Optional) **show running-config aaa-server** **Example:** hostname(config)# **show running-config aaa-server** aaa-server acs-group1 protocol radius aaa-server acs-group1 (outside) host 192.168.22.44 key secret radius-common-pw secret hostname(config)#	Displays the AAA server configuration.
Step 3	**nac-policy-nac-framework**	Switches to nac-policy-nac-framework configuration mode.
Step 4	**authentication-server-group** *server-group* **Example:** hostname(config-nac-policy-nac-framework)# **authentication-server-group acs-group1** hostname(config-nac-policy-nac-framework)	Specifies the group used for NAC posture validation. *server-group* must match the server-tag variable specified in the **aaa-server host** command. It is optional if you are using the **no** version of the command. Specifies acs-group1 as the authentication server group used for NAC posture validation.
Step 5	(Optional) [no] **authentication-server-group** *server-group*	Removes the command from the NAC policy.

Setting the Query-for-Posture-Changes Timer

After each successful posture validation, the ASA starts a status query timer. The expiration of this timer triggers a query to the remote host for changes in posture since the last posture validation. A response indicating no change resets the status query timer. A response indicating a change in posture triggers an unconditional posture revalidation. The ASA maintains the current access policy during revalidation.

By default, the interval between each successful posture validation and the status query, and each subsequent status query, is 300 seconds (5 minutes). Follow these steps to change the status query interval:

Detailed Steps

	Command	Purpose
Step 1	**`nac-policy-nac-framework`**	Switches to nac-policy-nac-framework configuration mode.

Step 2	**`sq-period seconds`**
	Example:
	`hostname(config-group-policy)#` **`sq-period 1800`**
	`hostname(config-group-policy)`
		Changes the status query interval.
		seconds must be in the range 30 to 1800 seconds (5 to 30 minutes).
		Changes the query timer to 1800 seconds.

Step 3	(Optional) `[`**`no`**`]` **`sq-period`** *`seconds`*	Turns off the status query timer.
Step 4	**`show running-config nac-policy`**	Displays a 0 next to the sq-period attribute, meaning the timer is turned off.

Setting the Revalidation Timer

After each successful posture validation, the ASA starts a revalidation timer. The expiration of this timer triggers the next unconditional posture validation. The ASA maintains the current access policy during revalidation.

By default, the interval between each successful posture validation is 36000 seconds (10 hours). To change it, enter the following command in nac-policy-nac-framework configuration mode:

Detailed Steps

	Command	Purpose
Step 1	**`nac-policy-nac-framework`**	Switches to nac-policy-nac-framework.

Step 2	**`reval-period`** ***`seconds`***
	Example:
	`hostname(config-nac-policy-nac-framework)#`
	`reval-period 86400`
	`hostname(config-nac-policy-nac-framework)`
		Changes the interval between each successful posture validation.
		seconds must be in the range is 300 to 86400 seconds (5 minutes to 24 hours).

Step 3	(Optional) `[`**`no`**`]` **`reval-period`** *`seconds`*	Turns off the status query timer.
Step 4	**`show running-config nac-policy`**	Displays a 0 next to the sq-period attribute, which means the timer is turned off.

Configuring the Default ACL for NAC

Each group policy points to a default ACL to be applied to hosts that match the policy and are eligible for NAC. The ASA applies the NAC default ACL before posture validation. Following posture validation, the ASA replaces the default ACL with the one obtained from the Access Control Server for the remote host. The ASA retains the default ACL if posture validation fails.

The ASA also applies the NAC default ACL if clientless authentication is enabled (which is the default setting).

Detailed Steps

	Command	Purpose
Step 1	**nac-policy-nac-framework**	Switches to nac-policy-nac-framework configuration mode.
Step 2	**default-acl** *acl-name* **Example:** hostname(config-nac-policy-nac-framework)# **default-acl acl-2** hostname(config-nac-policy-nac-framework)	Specifies which ACL to use as the default ACL for NAC sessions. *acl-name* is the name of the access control list to be applied to the session. Identifies ac1-2 as which ACL to apply before posture validation succeeds.
Step 3	(Optional) [**no**] **default-acl** *acl-name*	Removes the command from the NAC framework policy. Specifying the *acl-name* is optional.

Configuring Exemptions from NAC

The ASA configuration stores a list of exemptions from NAC posture validation. You can specify the operating systems that are exempt. If you specify an ACL, the client running the operating system specified is exempt from posture validation and the client traffic is subject to the ACL.

To add an entry to the list of remote computer types that are exempt from NAC posture validation, enter the following command in nac-policy-nac-framework configuration mode:

Detailed Steps

	Command	Purpose
Step 1	`nac-policy-nac-framework`	Switches to nac-policy-nac-framework configuration mode.

Step 2	**`exempt-list os`** `"`*`os-name`*`" [` **`disable`** `|` **`filter`** *`acl-name`* `[` **`disable`** `]`
	Example:
	`hostname(config-group-policy)#` **`exempt-list os "Windows XP"`**
	`hostname(config-group-policy)`
	`hostname(config-nac-policy-nac-framework)#` **`exempt-list os "Windows XP" filter acl-2`**
	`hostname(config-nac-policy-nac-framework)`
	`hostname(config-nac-policy-nac-framework)#` **`no exempt-list os "Windows XP" filter acl-2`**
	`hostname(config-nac-policy-nac-framework)`
		Adds an entry to the list of remote computer types that are exempt from NAC posture validation.
		• *os-name* is the operating system name. Use quotation marks if the name includes a space (for example, "Windows XP").
		• **filter** applies an ACL to filter the traffic if the computer's operating system matches the *os name*. The **filter**/*acl-name* pair is optional.
		• **disable** performs one of two functions, as follows:
		– If you enter it after the "os-name," the ASA ignores the exemption, and applies NAC posture validation to the remote hosts that are running that operating system.
		– If you enter it after the *acl-name*, ASA exempts the operating system, but does not apply the ACL to the associated traffic.
		• *acl-name* is the name of the ACL present in the ASA configuration. When specified, it must follow the **filter** keyword.
		Adds all hosts running Windows XP to the list of computers that are exempt from posture validation.
		Exempts all hosts running Windows XP and applies the ACL acl-2 to traffic from those hosts
		Removes the same entry from the exemption list.

Step 3	(Optional)
	`[`**`no`**`]` **`exempt-list os`** `"`*`os-name`*`" [` **`disable`** `|` **`filter`** *`acl-name`* `[` **`disable`** `] ]`
	Example:
	`hostname(config-nac-policy-nac-framework)#` **`no exempt-list`**
	`hostname(config-nac-policy-nac-framework)`
		Removes all exemptions from the NAC framework policy. Specifying an entry when issuing the no form of the command removes the entry from the exemption list.
		Removes all entries from the exemption list.

Note When the command specifies an operating system, it does not overwrite the previously added entry to the exception list; enter the command once for each operating system and ACL you want to exempt.

Assigning a NAC Policy to a Group Policy

Upon completion of each tunnel setup, the ASA applies the NAC policy, if it is assigned to the group policy, to the session. By default, the `nac-settings` command is not present in the configuration of each group policy. The ASA automatically enables NAC for a group policy when you assign a NAC policy to it.

Detailed Steps

	Command	Purpose
Step 1	`group-policy`	Switches to group-policy configuration mode.
Step 2	**nac-settings** { **value** *nac-policy-name* | **none** }	Assigns a NAC policy to a group policy. • **nac-settings none** removes the *nac-policy-name* from the group policy and disables the use of a NAC policy for this group policy. The group policy does not inherit the nac-settings value from the default group policy. • **nac-settings value** assigns the NAC policy you name to the group policy.
	Example: hostname(config-group-policy)# **nac-settings value framework1** hostname(config-group-policy)	Assigns the NAC policy named framework1 to the group policy.
Step 3	(Optional) [no] **nac-settings** { **value** *nac-policy-name* | **none** }	Removes the nac-policy-name from the group policy. The group policy inherits the nac-settings value from the default group policy.
Step 4	(Optional) **show running-config nac-policy**	Displays the name and configuration of each NAC policy

Changing Global NAC Framework Settings

The ASA provides default settings for a NAC Framework configuration. Use the instructions in this section to adjust these settings for adherence to the policies in force in your network.

Changing Clientless Authentication Settings

NAC Framework support for clientless authentication is configurable. It applies to hosts that do not have a Cisco Trust Agent to fulfill the role of posture agent. The ASA applies the default access policy, sends the EAP over UDP request for posture validation, and the request times out. If the ASA is not configured to request a policy for clientless hosts from the Access Control Server, it retains the default access policy already in use for the clientless host. If the ASA is configured to request a policy for clientless hosts from the Access Control Server, it does so and the Access Control Server downloads the access policy to be enforced by the ASA.

Enabling and Disabling Clientless Authentication

Clientless authentication is enabled by default. The default configuration contains the **eou allow clientless** configuration.

Restrictions

The **eou** commands apply *only* to NAC Framework sessions.

Detailed Steps

Follow these steps to enable clientless authentication for a NAC Framework configuration:

	Command	Purpose
Step 1	`global`	Switches to global configuration mode.
Step 2	`eou allow {audit | clientless | none}`	Enables clientless authentication for a NAC framework configuration. • **audit** uses an audit server to perform clientless authentication. • **clientless** uses a Cisco Access Control Server to perform clientless authentication. • **none** disables clientless authentication.

	Example:
	`hostname(config)# eou allow audit`
	`hostname(config)#`
		Shows how to configure the ASA to use an audit server to perform clientless authentication.

Step 3	`[no] eou allow {audit | clientless | none}`	Removes the command from the configuration.

	Example:
	`hostname(config)# no eou allow audit`
	`hostname(config)#`
		Disables the use of an audit server.

Changing the Login Credentials Used for Clientless Authentication

When clientless authentication is enabled, and the ASA fails to receive a response to a validation request from the remote host, it sends a clientless authentication request on behalf of the remote host to the Access Control Server. The request includes the login credentials that match those configured for clientless authentication on the Access Control Server. The default username and password for clientless authentication on the ASA matches the default username and password on the Access Control Server; the default username and password are both “clientless.”

Prerequisites

If you change these values on the Access Control Server, you must also do so on the ASA.

Detailed Steps

Enter the following to change the username used for clientless authentication:

	Command	Purpose
Step 1	**global**	Switches to global configuration mode.
Step 2	**eou clientless username** *username* **Example:** hostname(config)# **eou clientless username sherlock** hostname(config)# **eou clientless password 221B-baker** hostname(config)#	Changes the username used for clientless authentication. *username* must match the username configured on the Access Control Server to support clientless hosts. Enter 1 to 64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), quotation marks ("), asterisks (*), and angle brackets (< and >). Changes the username and password for clientless authentication to sherlock and 221B-baker respectively. You can specify only the username, only the password, or both.
Step 3	**eou clientless password** *password*	Changes the password used for clientless authentication. *password* must match the password configured on the Access Control Server to support clientless hosts. Enter 4 – 32 ASCII characters.
Step 4	(Optional) **no eou clientless username** **Example:** hostname(config)# **no eou clientless username** hostname(config)#	Changes the username to its default value.
Step 5	(Optional) **no eou clientless password** **Example:** hostname(config)# **no eou clientless password** hostname(config)#	Changes the password to its default value.

Changing NAC Framework Session Attributes

The ASA provides default settings for the attributes that specify communications between the ASA and the remote host. These attributes specify the port no. to communicate with posture agents on remote hosts and the expiration counters that impose limits on the communications with the posture agents. These attributes, the default settings, and the commands you can enter to change them are as follows:

Detailed Steps

	Command	Purpose
Step 1	`global`	Switches to global configuration mode.

Step 2	**`eou port`** *`port_number`*
	Example:
	`hostname(config)#` **`eou port 62445`**
	`hostname(config)#`
		The default port number is 21862. This command changes the port number (on the client endpoint) used for EAP over UDP communication with posture agents.
		port_number must match the port number configured on the CTA. Enter a value in the range 1024 to 65535.
		Changes the port number for EAP over UDP communication to 62445.

Step 3	(Optional)
	`no` `eou port`
	Example:
	`hostname(config)#` **`no eou port`**
	`hostname(config)#`
		Changes the port number to its default value.

Step 4	**`eou timeout retransmit`** *`seconds`*
	Example:
	`hostname(config)#` **`eou timeout retransmit 6`**
	`hostname(config)#`
		Changes the retransmission retry timer. When the ASA sends an EAP over UDP message to the remote host, it waits for a response. If it fails to receive a response within *n* seconds, it resends the EAP over UDP message. By default, the retransmission timer is 3 seconds.
		seconds is a value in the range 1 to 60.
		Changes the retransmission timer to 6 seconds.

Step 5	(Optional)
	`no eou timeout` **`retransmit`**
	Example:
	`hostname(config)#` **`no eou timeout retransmit`**
	`hostname(config)#`
		Changes the retransmission retry timer to its default value.

Step 6	**`eou max-retry`** *`retries`*
	Example:
	`hostname(config)#` **`eou max-retry 1`**
	`hostname(config)#`
		Changes retransmission retries. When the ASA sends an EAP over UDP message to the remote host, it waits for a response. If it fails to receive a response, it resends the EAP over UDP message. By default, it retries up to 3 times.
		retries is a value in the range 1 to 3.
		Limits the number of EAP over UDP retransmissions to 1.

	Command	Purpose

Step 7	(Optional)
	`no eou max-retry`
	Example:
	`hostname(config)# no eou max-retry`
	`hostname(config)#`
		Changes the maximum number of retransmission retries to its default value.

Step 8	`eou timeout hold-period seconds`
	Example:
	`hostname(config)# eou timeout hold-period 120`
	`hostname(config)#`
		Changes the session reinitialization timer. When the retransmission retry counter matches the max-retry value, the ASA terminates the EAP over UDP session with the remote host and starts the hold timer. When the hold timer equals *n* seconds, the ASA establishes a new EAP over UDP session with the remote host. By default, the maximum number of seconds to wait before establishing a new session is 180 seconds.
		seconds is a value in the range 60 to 86400.
		Changes the wait period before initiating a new EAP over UDP association to 120 seconds

Step 9	**(Optional)**
	`no eou timeout hold-period`
	Example:
	`hostname(config)# no eou timeout hold-period`
	`hostname(config)#`
		Changes the session reinitialization to its default value.