CHAPTER 33

Configuring Network Admission Control

This chapter includes the following sections.

Uses, Requirements, and Limitations

Network Admission Control (NAC) 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 establishing an IPSec session are up-to-date. Posture validation can include the verification that the applications running on the remote hosts are updated with the latest patches. NAC supplements the identity-based validation that IPSec and other access methods provide. It is especially useful for protecting the enterprise network from hosts that are not subject to automatic network policy enforcement, such as home PCs.

Note When configured to support NAC, the security appliance 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.

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 Configuring Basic Settings, page 33-1 to configure NAC.

ASA support for NAC is limited to remote access IPSec and L2TP over IPSec sessions. NAC on the ASA does not support WebVPN, non-VPN traffic, IPv6, and multimode.

Configuring Basic Settings

The instructions in the following sections describe how to enter the minimum set of commands to configure support for NAC on the security appliance:

Note See Uses, Requirements, and Limitations, page 33-1 before following these instructions.

Specifying the Access Control Server Group

You must configure at least one Cisco Access Control Server to support NAC. Then use the **aaa-server host** command to name the Access Control Server group even if the group contains only one server. Then enter the following command in tunnel-group general-attributes configuration mode to specify the same group as the group to be used for NAC posture validation:

nac-authentication-server-group *server-group*

server-group must match the server-tag variable specified in the **aaa-server host** command.

For example, enter the following command to specify acs-group1 as the authentication server group to be used for NAC posture validation:

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

To inherit the authentication server group from the default remote access group, access the alternative group policy from which to inherit it, then enter the following command:

no nac-authentication-server-group

For example:

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

Enabling NAC

To enable or disable NAC for a group policy, enter the following command in group-policy configuration mode:

nac {enable | disable}

The following example enables NAC for the group policy:

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)
```

To inherit the NAC setting from the default group policy, access the alternative group policy from which to inherit it, then issue the following command:

no nac

For example:

```
hostname(config-group-policy)# no nac
```

```
hostname(config-group-policy)#
```

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 security appliance applies the NAC default ACL 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. It retains the default ACL if posture validation fails.

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

Note Because NAC is disabled by default, VPN traffic traversing the security appliance is not subject to the NAC Default ACL until NAC is enabled.

Enter the following command in group-policy configuration mode to specify the ACL to be used as the default ACL for NAC sessions:

nac-default-acl value *acl-name*

acl-name is the name of the posture validation server group, as configured on the security appliance using the **aaa-server host** command. The name must match the server-tag variable specified in that command.

For example, enter the following command to specify acl-1 as the NAC default ACL:

```
hostname(config-group-policy)# nac-default-acl value acl-1
hostname(config-group-policy)
```

To inherit the ACL from the default group policy, access the alternative group policy from which to inherit it and enter the following command.

no nac-default-acl

For example:

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

You also have the option of disinheriting the ACL from the default group policy and specifying no NAC default ACL. To do so, enter the following command:

nac-default-acl none

For example:

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)
```

Configuring Exemptions from NAC

The security appliance 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 group-policy configuration mode:

vpn-nac-exempt os "*os name*" [**filter** *acl-name*] [**disable**]

Note This command 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.

os name is the operating system name. Use quotation marks if the name includes a space (for example, "Windows XP").

For example, enter the following command to add all hosts running Windows XP to the list of computers that are exempt from posture validation:

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

The remaining keywords and arguments are optional:

- **filter** to apply an ACL to filter the traffic if the computer matches the os name.
- *acl-name* is the name of the ACL present in the security appliance configuration.
- **disable** to disable the entry in the exemption list without removing it from the list. Not entering this keyword enables the entry.

For example, enter the following command to exempt all hosts running Windows 98 and apply the ACL acl-1 to traffic from those hosts:

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

The following example shows how to add the same entry to the exemption list, but disable it:

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

To disable inheritance and specify that all hosts are subject to posture validation, enter the following command:

vpn-nac-exempt none

For example:

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

To remove an entry from the exemption list, enter the following command, naming the operating system (and ACL) in the exemption to be removed.

no vpn-nac-exempt [os "*os name*"] [**filter** *acl-name*]

For example, enter the following command to remove the entry with Windows 98 and acl-1 from the exemption list, regardless of whether it is disabled:

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

To remove all entries from the exemption list associated with this group policy and inherit the list from the default group policy, enter the following command without specifying additional keywords:

no vpn-nac-exempt

For example:

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

Changing Advanced Settings

The security appliance provides default settings for NAC. 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 support for clientless authentication is configurable. It applies to hosts that do not have a posture agent, such as the Cisco Trust Agent. The security appliance applies the default access policy, sends the EAP over UDP request for posture validation, and the request times out. If the security appliance 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 security appliance 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 security appliance.

Enabling and Disabling Clientless Authentication

Enter the following command in global configuration mode to enable clientless authentication:

eou allow clientless

For example:

```
hostname(config)# eou allow clientless
hostname(config)#
```

The **eou clientless** command is meaningful only if NAC is enabled.

Note Clientless authentication is enabled by default.

Enter the following command in global configuration mode to disable clientless authentication:

no eou allow clientless

For example:

```
hostname(config)# no eou allow clientless
hostname(config)#
```

Changing the Login Credentials Used for Clientless Authentication

When clientless authentication is enabled, and the security appliance 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 security appliance matches the default username and password on the Access Control Server; the default username and password are both “clientless”. If you change these values on the Access Control Server, you must also do so on the security appliance.

Enter the following command in global configuration mode to change the username used for clientless authentication:

eou clientless username *username*

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 >).

Enter the following command in global configuration mode to change the password used for clientless authentication:

eou clientless password *password*

password must match the password configured on the Access Control Server to support clientless hosts. Enter 4 – 32 ASCII characters.

You can specify only the username, only the password, or both. For example, enter the following commands to change the username and password for clientless authentication to sherlock and 221B-baker, respectively:

```
hostname(config)# eou clientless username sherlock
hostname(config)# eou clientless password 221B-baker
hostname(config)#
```

To change the username to its default value, enter the following command:

no eou clientless username

For example:

```
hostname(config)# no eou clientless username
hostname(config)#
```

To change the password to its default value, enter the following command:

no eou clientless password

For example:

```
hostname(config)# no eou clientless password
hostname(config)#
```

Configuring NAC Session Attributes

The ASA provides default settings for the attributes that specify communications between the security appliance 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:

- Port no. on the client endpoint to be used for EAP over UDP communication with posture agents.

  The default port no. is 21862. Enter the following command in global communication mode to change it:

  eou port *port_number*

  port_number must match the port number configured on the CTA. Enter a value in the range 1024 to 65535.

  For example, enter the following command to change the port number for EAP over UDP communication to 62445:

  ```
  hostname(config)# eou port 62445
  hostname(config)#
  ```

  To change the port number to its default value, use the **no** form of this command, as follows:

  no eou port

  For example:

  ```
  hostname(config)# no eou port
  hostname(config)#
  ```

- Retransmission retry timer

  When the security appliance 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. To change this value, enter the following command in global configuration mode:

  eou timeout retransmit *seconds*

  seconds is a value in the range 1 to 60.

  The following example changes the retransmission timer to 6 seconds:

  ```
  hostname(config)# eou timeout retransmit 6
  hostname(config)#
  ```

  To change the retransmission retry timer to its default value, use the **no** form of this command, as follows:

  no eou timeout **retransmit**

  For example:

  ```
  hostname(config)# no eou timeout retransmit
  hostname(config)#
  ```

- Retransmission retries

When the security appliance 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. To change this value, enter the following command in global configuration mode:

eou max-retry *retries*

retries is a value in the range 1 to 3.

The following example limits the number of EAP over UDP retransmissions to 1:

```
hostname(config)# eou max-retry 1
hostname(config)#
```

To change the maximum number of retransmission retries to its default value, use the **no** form of this command, as follows:

no eou max-retry

For example:

```
hostname(config)# no eou max-retry
hostname(config)#
```

- Session reinitialization timer

  When the retransmission retry counter matches the max-retry value, the security appliance terminates the EAP over UDP session with the remote host and starts the hold timer. When the hold timer equals *n* seconds, the security appliance 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. To change this value, enter the following command in global configuration mode:

  eou timeout hold-period *seconds*

  seconds is a value in the range 60 to 86400.

  For example, enter the following command to change the wait period before initiating a new EAP over UDP association to 120 seconds:

```
hostname(config)# eou timeout hold-period 120
hostname(config)#
```

  To change the session reinitialization to its default value, use the **no** form of this command, as follows:

  no eou timeout hold-period

  For example:

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

Setting the Query-for-Posture-Changes Timer

After each successful posture validation, the security appliance 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 security appliance 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). The group policy inherits the value of the status query timer from the default group policy unless you change it. Enter the following command in group-policy configuration mode to change the status query interval:

nac-sq-period *seconds*

seconds must be in the range is 300 to 1800 seconds (5 to 30 minutes).

The following example changes the status query timer to 1800 seconds:

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

To inherit the value of the status query timer from the default group policy, access the alternative group policy from which to inherit it, then enter the following command.

no nac-sq-period [*seconds*]

For example:

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)
```

Setting the Revalidation Timer

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

By default, the interval between each successful posture validation is 36000 seconds (10 hours). The group policy inherits the value of the revalidation timer from the default group policy unless you change it. Enter the following command in group-policy configuration mode to change the revalidation interval:

nac-reval-period *seconds*

seconds must be in the range is 300 to 86400 seconds (5 minutes to 24 hours).

For example, enter the following command to change the revalidation timer to 86400 seconds:

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

To inherit the value of the revalidation timer from the default group policy, access the alternative group policy from which to inherit it, then enter the following command.

no nac-reval-period

For example:

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)
```