NAC-Auth Fail Open

Last Updated: October 24, 2011

In network admission control (NAC) deployments, authentication, authorization, and accounting (AAA) servers validate the antivirus status of clients before granting network access. This process is called posture validation. If the AAA server is unreachable, clients do not have access to the network. The NAC--Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable. The administrator can configure a global policy that applies to a device, or a rule-based policy that applies to a specific interface.

When the AAA server returns to a reachable status, the posture validation process resumes for clients that are using the NAC--Auth Fail Open policy.

Prerequisites for NAC-Auth Fail Open

You can configure this feature in networks using NAC and an AAA server for security. NAC is implemented on Cisco IOS routers running Cisco IOS Release 12.3(8)T or a later release.

Restrictions for NAC-Auth Fail Open

To apply local policies to a device or an interface when the AAA server is unreachable, you must configure the **aaa authorization network default local** command.

Information About Network Admission Control

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Controlling Admission to a Network

NAC protects networks from endpoint devices or clients (such as PCs or servers) that are infected with viruses by enforcing access control policies that prevent infected devices from adversely affecting the network. It checks the antivirus condition (called *posture*) of endpoint systems or clients before granting the devices network access. NAC keeps insecure nodes from infecting the network by denying access to noncompliant devices, placing them in a quarantined network segment or giving them restricted access to computing resources.

NAC enables network access devices (NADs) to permit or deny network hosts access to the network based on the state of the antivirus software on the host. This process is called posture validation.

Posture validation consists of the following actions:

- Checking the antivirus condition or credentials of the client.
- Evaluating the security posture credentials from the network client.
- Providing the appropriate network access policy to the NAD based on the system posture.

Network Admission Control When the AAA Server Is Unreachable

Typical deployments of NAC use a AAA server to validate the client posture and to pass policies to the NAD. If the AAA server is not reachable when the posture validation occurs, the typical response is to deny network access. Using NAC--Auth Fail Open, an administrator can configure a default policy that allows the host at least limited network access while the AAA server is unreachable.

This policy offers these two advantages:

- While AAA is unavailable, the host continues to have connectivity to the network, although it may be restricted.
- When the AAA server is once again reachable, users can be validated again, and their policies can be downloaded from the access control server (ACS).

Note When the AAA server is unreachable, the NAC--Auth Fail Open policy is applied only when there is no existing policy associated with the host. Typically, when the AAA server becomes unreachable during revalidation, the policies already in effect for the host are retained.

How to Configure NAC-Auth Fail Open

You can configure NAC--Auth Fail Open policies per interface, or globally for a device. Configuring NAC--Auth Fail Open is optional, and includes the following tasks:

Configuring a NAC Rule-Associated Policy Globally for a Device

This task creates a NAC rule and associates a policy to be applied while the AAA server is unreachable. You can apply a policy globally to all interfaces on a network access device, if you want to provide the same level of network access to all users who access that device.

An AAA server must be configured and NAC must be implemented on the NAD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name* }] [**list** {*acl* | *acl-name* }] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name* }]
4. **ip admission** *admission-name [* **event timeout aaa policy identity** *identity-policy-name]*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* [**eapoudp** [**bypass**]	**proxy** {**ftp**	**http**	**telnet**}	**service-policy type tag** {*service-policy-name* }] [**list** {*acl*	*acl-name* }] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name* }] **Example:** `Router (config)# ip admission name greentree event timeout aaa policy identity aaa-down`	(Optional) Configures a rule-specific policy globally for the device. If a rule is configured, then it is applied instead of any other global event timeout policy configured on the device. To remove a rule that was applied globally to the device, use the **no** form of thecommand.

	Command or Action	Purpose
Step 4	**ip admission** *admission-name [* **event timeout aaa policy identity** *identity-policy-name]* **Example:** `Router (config)# ip admission event timeout aaa policy identity AAA_DOWN`	(Optional) Configures the specified IP NAC policy globally for the device. To remove IP NAC policy that was applied to the device, use the **no** form of thecommand. **Note** This policy applies only if no rule-specific policy is configured.
Step 5	**end** **Example:** `Router (config)# end`	Exits the global configuration mode.

Applying a NAC Policy to a Specific Interface

An IP admission rule with NAC--Auth Fail Open policies can be attached to an interface. This task attaches a NAC--Auth Fail Open policy to a rule, and applies the rule to a specified interface on a device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip access-group** {*access-list-number* | *name*} **in**
5. **ip admission** *admission-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-id* **Example:** `Router (config)# interface fastEthernet 2/1`	Enters interface configuration mode.
Step 4	**ip access-group** {*access-list-number* | *name*} **in** **Example:** `Router (config-if)# ip access-group ACL15 in`	Controls access to the specified interface.
Step 5	**ip admission** *admission-name* **Example:** `Router (config-if)# ip admission AAA_DOWN`	Attaches the globally configured IP admission rule to the specified interface(s). To remove the rule on the interface, use the **no** form of the command.
Step 6	**exit** **Example:** `Router (config)# exit`	Returns to global configuration mode.

Configuring Authentication and Authorization Methods

This task configures the authentication and authorization methods for the device. The access granted using these methods remain in effect for users who attempt reauthorization while the AAA server is unavailable. These methods must be configured before you configure any policy to be applied to users who try to access the network when the AAA server is unreachable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default group radius**
5. **aaa authorization network default local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router (config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication eou default group radius** **Example:** `Router (config)# aaa authentication eou default group radius`	Sets authentication methods for Extensible Authorization Protocol over User Datagram Protocol (EAPoUDP). To remove the EAPoUDP authentication methods, use the use the **no** form of the command.
Step 5	**aaa authorization network default local** **Example:** `Router (config)# aaa authorization network default local`	Sets the authorization method to local. To remove the authorization method, use the **no** form of the command.

Configuring RADIUS Server Parameters

Identifying the RADIUS Server

A RADIUS server can be identified by:

- hostname
- IP address
- hostname and a specific UDP port number

- IP address and a specific UDP port number

The combination of the RADIUS server IP address and a specific UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, authentication--the second host entry configured acts as the backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Determining When the RADIUS Server Is Unavailable

Because the NAC--Auth Fail Open feature applies a local policy when the RADIUS server is unavailable, you should configure “dead criteria” that identify when the RADIUS server is unavailable. There are two configurable dead criteria:

- time--the interval (in seconds) without a response to a request for AAA service
- tries--the number of consecutive AAA service requests without a response

If you do not configure the dead criteria, they are calculated dynamically, based on the server configuration and the number of requests being sent to the server.

You can also configure the number of minutes to wait before attempting to resume communication with a RADIUS server after it has been defined as unavailable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server dead-criteria [time** *seconds]* **[tries** *number-of- tries]*
4. **radius-server deadtime** *minutes*
5. **radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port***udp-port*] [**key***string*] [**test username***name* [**idle-time***time*]
6. **radius-server attribute 8 include-in-access-req**
7. **radius-server vsa send authentication**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius-server dead-criteria [time** *seconds]* **[tries** *number-of- tries]* **Example:** `Router (config)# radius-server dead-criteria time 30 tries 20` **Example:**	(Optional) Sets the conditions that are used to decide when a RADIUS server is considered unavailable or *dead* . • The range for *seconds* is from 1 to 120 seconds. The default is that the NAD dynamically determines the *seconds* value within a range from 10 to 60 seconds. • The range for *number-of-tries* is from 1 to 100. The default is that the NAD dynamically determines the *number-of-tries* parameter within a range from 10 to 100.
Step 4	**radius-server deadtime** *minutes* **Example:** `Router (config)# radius-server deadtime 60`	(Optional) Sets the number of minutes that a RADIUS server is not sent requests after it is found to be dead. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.

Command or Action	Purpose
Step 5 **radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port***udp-port*] [**key***string*] [**test username***name* [**idle-time***time*] **Example:** `Router (config)# radius-server host 10.0.0.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234` **Example:**	(Optional) Configures the RADIUS server parameters by using these keywords: • **acct-port** *udp-port*-- Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. If the port number is set to 0, the host is not used for accounting. • **auth-port** *udp-port*-- Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. If the port number is set to 0, the host is not used for authentication. **Note** You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values. • **key** *string*-- Specifies the authentication and encryption key for all RADIUS communication between the NAD and the RADIUS daemon. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. • **test username** *name* -- Enables automated testing of the RADIUS server status, and specify the username to be used. • **idle-time** *time*-- Sets the interval of time in minutes after which the NAD sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). To configure multiple RADIUS servers, reenter this command.
Step 6 **radius-server attribute 8 include-in-access-req** **Example:** `Router (config)# radius-server attribute 8 include-in-access-req`	If the device is connected to nonresponsive hosts, configures the device to send the Framed-IP-Address RADIUS attribute (attribute[8]) in access-request or accounting-request packets. To configure the device to not send the Framed-IP-Address attribute, use the **no radius-server attribute 8 include-in-access-req** global configuration command.
Step 7 **radius-server vsa send authentication** **Example:** `Router (config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes (VSAs).

	Command or Action	Purpose
Step 8	**end** **Example:** `Router (config)# end`	Returns to privileged EXEC mode.

Displaying the Status of Configured AAA Servers

This task displays the status of the AAA servers you have configured for the device.

SUMMARY STEPS

1. **enable**
2. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show aaa servers** **Example:** `Router# show aaa servers`	Displays the status of the AAA servers configured for the device.

Displaying the NAC Configuration

This task displays the current NAC configuration for the device.

SUMMARY STEPS

1. **enable**
2. **show ip admission configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip admission configuration** **Example:** `Router#` **`show ip admission configuration`**	Displays all the IP admission control rules configured for the device.

Displaying the EAPoUDP Configuration

This task displays information about the current EAPoUDP configuration for the device, including any NAC--Auth Fail Open policies in effect.

SUMMARY STEPS

1. **enable**
2. **show eou ip 10.0.0.1**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show eou ip 10.0.0.1** **Example:** `Router#` **`show eou ip 10.0.0.1`**	Displays information about the EAPoUDP configuration for the specified interface.

Enabling EOU Logging

A set of new system logs is included in Cisco IOS Release 12.4(11)T. These new logs track the status of the servers defined by the methodlist, and the NAC Auth Fail policy configuration. You should enable EOU logging to generate syslog messages that notify you when the AAA servers defined by the methodlist are unavailable, and display the configuration of the NAC--Auth Fail Open policy. The display shows

whether a global or rule-specific policy is configured for the NAD or interface. If no policy is configured, the existing policy is retained.

This task enables EOU logging.

SUMMARY STEPS

1. **configure terminal**
2. **eou logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**eou logging** **Example:** `Router (config) #` **eou logging**	Enables EOU logging.

Configuration Examples for NAC-Auth Fail Open

Sample NAC-Auth Fail Open Configuration Example

The example below shows how to configure the NAC--Auth Fail Open feature:

```
Switch# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip admission name AAA_DOWN eapoudp event timeout aaa policy identity
global_policy
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# aaa authentication eou default group radius
Switch(config)# identity policy global_policy
Switch(config-identity-policy)# ac
Switch(config-identity-policy)# access-group global_acl
Switch(config)# ip access-list extended global_acl
```

```
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
```

Sample RADIUS Server Configuration Example

The example below shows that the RADIUS server is considered unreachable after 3 unsuccessful tries:

```
Switch(config)# radius-server host 10.0.0.4 test username administrator idle-time 1 key
sample
Switch(config)# radius-server dead-criteria tries 3
Switch(config)# radius-server deadtime 30
Switch(config)# radius-server vsa send authentication
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# int fastEthernet 2/1
3
Switch(config-if)# ip admission AAA_DOWN
Switch(config-if)# exit
```

show ip admission configuration Output Example

The following example shows that a policy called “global policy” has been configured for use when the AAA server is unreachable:

```
Switch# show ip admission configuration

Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-
list
is disabled
Authentication Proxy Rule Configuration
 Auth-proxy name AAA_DOWN
    eapoudp list not specified auth-cache-time 60 minutes
    Identity policy name global_policy for AAA fail policy
```

show eou Output Example

The example below shows the configuration of the AAA servers defined for a NAC--Auth Fail policy configuration:

```
Router# show eou ip 10.0.0.1


Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
! Authtype is show as AAA DOWN when in AAA is not reachable.
AuthType : AAA DOWN
! AAA Down policy name:
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

show aaa servers Output Example

The example below shows sample status information for a configured AAA server:

```
Switch# show aaa servers
RADIUS: id 1, priority 1, host 10.0.0.4, auth-port 1645, acct-port 1646
     State: current UP, duration 5122s, previous duration 9s
     Dead: total time 79s, count 3
     Authen: request 158, timeouts 14
             Response: unexpected 1, server error 0, incorrect 0, time 180ms
             Transaction: success 144, failure 1
     Author: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Account: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Elapsed time since counters last cleared: 2h13mS
```

EOU Logging Output Example

The example below shows the display when EOU logging is enabled:

```
Router (config)# eou
 logging
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=Existing policy retained.
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=aaa_unreachable_policy
```

Additional References

Related Documents

Related Topic	Document Title
Configuring NAC	Network Admission Control module.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
IEEE 802.1x	IEEE Standard 802.1X - 2004 Port-Based Network Access Control

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NAC-Auth Fail Open

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for NAC--Auth Fail Open

Feature Name	Releases	Feature Information
NAC--Auth Fail Open	12.3(8)T	In network admission control (NAC) deployments, authentication, authorization, and accounting (AAA) servers validate the antivirus status of clients before granting network access. This process is called posture validation. If the AAA server is unreachable, clients do not have access to the network. The NAC--Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable. The administrator can configure a global policy that applies to a device, or a rule-based policy that applies to a specific interface. When the AAA server returns to a reachable status, the posture validation process resumes for clients that are using the NAC--Auth Fail Open policy. This feature was introduced in Cisco IOS Release 12.3(8)T. The following commands were introduced or modified: **ip admission**, **ip admission name**, **show eou**, **show ip admission**