



CHAPTER 25

Applying AAA for Network Access

This chapter describes how to enable AAA (pronounced “triple A”) for network access.

For information about AAA for management access, see the “[Configuring AAA for System Administrators](#)” section on page 16-25.

This chapter includes the following sections:

- [AAA Performance, page 25-1](#)
- [Configuring Authentication for Network Access, page 25-1](#)
- [Configuring Authorization for Network Access, page 25-9](#)
- [Configuring Accounting for Network Access, page 25-15](#)
- [Using MAC Addresses to Exempt Traffic from Authentication and Authorization, page 25-16](#)

AAA Performance

The FWSM uses “cut-through proxy” to significantly improve performance compared to a traditional proxy server. The performance of a traditional proxy server suffers because it analyzes every packet at the application layer of the OSI model. The FWSM cut-through proxy challenges a user initially at the application layer and then authenticates against standard AAA servers or the local database. After the FWSM authenticates the user, it shifts the session flow, and all traffic flows directly and quickly between the source and destination while maintaining session state information.

Configuring Authentication for Network Access

This section includes the following topics:

- [Information About Authentication, page 25-2](#)
- [Configuring Network Access Authentication, page 25-3](#)
- [Authenticating Directly with the Security Appliance, page 25-4](#)
- [Configuring Advanced Authentication Options, page 25-6](#)

Information About Authentication

The FWSM lets you configure network access authentication using AAA servers. This section includes the following topics:

- [One-Time Authentication, page 25-2](#)
- [Applications Required to Receive an Authentication Challenge, page 25-2](#)
- [FWSM Authentication Prompts, page 25-2](#)
- [Static PAT and HTTP, page 25-3](#)

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the Configuration > Firewall > Advanced > Global Timeouts pane for timeout values.) For example, if you configure the FWSM to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the Global Timeout is set, because the browser caches the string “Basic=Uuhjksdkfhk==” in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the FWSM to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the FWSM allows other traffic requiring authentication.

The authentication ports that the FWSM supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

FWSM Authentication Prompts

For Telnet and FTP, the FWSM generates an authentication prompt. After you authenticate correctly, the FWSM redirects you to your original destination. If the destination server also has its own authentication, you enter another username and password.

For HTTP, you log in using basic HTTP authentication supplied by the browser. For HTTPS, the FWSM generates custom login windows.

**Note**

If you use HTTP authentication, by default the username and password are sent from the client to the FWSM in clear text; in addition, the username and password are sent on to the destination web server as well. See the [“Enabling Secure Authentication of Web Clients” section on page 25-7](#) for information to secure your credentials.

For FTP, a user has the option of entering the FWSM username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the FWSM password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> user1@user2
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

Static PAT and HTTP

For HTTP authentication, the FWSM checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the FWSM intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant access lists permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the FWSM intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the FWSM allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the FWSM sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Configuring Network Access Authentication

To enable network access authentication, perform the following steps. For more information about authentication, see the [“Information About Authentication” section on page 25-2](#).

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Authentication Rule**.
The Add Authentication Rule dialog box appears.
 - Step 2** From the Interface drop-down list, choose the interface for applying the rule.
 - Step 3** In the Action field, click one of the following, depending on the implementation:
 - **Authenticate**
 - **Do not Authenticate.**
 - Step 4** From the AAA Server Group drop-down list, choose a server group. To add a AAA server to the server group, click **Add Server**. See the [“Configuring AAA Server Groups” section on page 15-7](#) for more information.
If you chose LOCAL for the AAA server group, you can optionally add a new user by clicking **Add User**. See the [“Adding a User Account” section on page 15-14](#) for more information.
 - Step 5** In the Source field, add the source IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.

- Step 6** In the Destination field, enter the destination IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 7** In the Service field, enter an IP service name or number for the destination service, or click ellipsis (...) button to choose a service.
- Step 8** (Optional) In the Description field, add a description.
- Step 9** (Optional) Click **More Options** to do any of the following:
- To specify a source service for TCP or UDP, enter a TCP or UDP service in the Source Service field. The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
 - To make the rule inactive, uncheck **Enable Rule**.
You may not want to remove a rule, but instead turn it off.
 - To set a time range for the rule, from the Time Range drop-down list, choose an existing time range. To add a new time range, click the ellipsis (...). For more information, see [Configuring Time Ranges, page 20-13](#).
- Step 10** Click **OK**.
The dialog box closes and the rule appears in the AAA Rules table.
- Step 11** Click **Apply**.
The changes are saved to the running configuration.
-

Authenticating Directly with the Security Appliance

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the FWSM but want to authenticate other types of traffic, you can authenticate with the FWSM directly using HTTP, HTTPS, Telnet, or SSH.

- [Authenticating HTTP\(S\) Connections with a Virtual Server, page 25-5](#)

Authenticating Telnet or SSH Connections with a Virtual Server

Although you can configure network access authentication for any protocol or service (see the [“Configuring Authentication for Network Access” section on page 25-1](#)), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the FWSM, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the FWSM, and the FWSM provides a Telnet prompt.

You must configure authentication for Telnet or SSH access to the virtual Telnet or SSH address as well as the other services you want to authenticate according to the [“Configuring Authentication for Network Access” section on page 25-1](#).

When an unauthenticated user connects to the virtual Telnet or SSH IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message “Authentication Successful.” Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet or SSH address as a destination interface in the Access Rule applied to the source interface. Moreover, you must add a static NAT rule for the virtual Telnet or SSH IP address, even if NAT is not required. An identity NAT rule is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an Access Rule to an inside interface, be sure to allow access to the virtual Telnet or SSH address. A static NAT rule is not required.

To logout from the FWSM, reconnect to the virtual Telnet or SSH IP address; you are prompted to log out.

To enable direct authentication using Telnet or SSH, perform the following steps:

-
- Step 1** From the Configuration > Firewall > Advanced > Virtual Access pane, check the **Enable** check box for Virtual Telnet or Virtual SSH.
- Step 2** In the Virtual Telnet/SSH Server field, add the IP address of the virtual Telnet or SSH server.
Make sure this address is an unused address that is routed to the FWSM. For example, if you perform NAT for inside addresses accessing an outside server, and you want to provide outside access to the virtual Telnet server, you can use one of the global NAT addresses for the virtual Telnet server address.
- Step 3** Click **Apply**.
The virtual server is added and the changes are saved to the running configuration.
-

Authenticating HTTP(S) Connections with a Virtual Server

Virtual HTTP provides the following functions:

- Cascading HTTP authentications—When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This feature redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the FWSM. The FWSM prompts for the AAA server username and password. After the AAA server authenticates the user, the FWSM redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.



Note Do not set the uauth timeout duration to 0 seconds when using this feature, because this setting prevents HTTP connections to the real web server. See the Configuration > Firewall > Advanced > Global Timeouts pane.

- Direct authentication with the FWSM—You can authenticate directly with the FWSM using the virtual HTTP IP address. Although you can configure network access authentication for any protocol or service, you can authenticate directly with HTTP(S), Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is

allowed through. If you do not want to allow HTTP, Telnet, or FTP through the FWSM, but want to authenticate other types of traffic, you can configure virtual HTTP; the user connects using HTTP to a given IP address configured on the FWSM, and the FWSM provides an HTTP prompt.

You must configure authentication for HTTP access to the virtual HTTP address as well as the other services you want to authenticate according to the [“Configuring Authentication for Network Access” section on page 25-1](#).

When an unauthenticated user connects to the virtual HTTP IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user can successfully access other services that require authentication.

You must also include the virtual HTTP address as a destination interface in the Access Rule applied to the source interface. Moreover, you must add a static NAT rule for the virtual HTTP IP address, even if NAT is not required. An identity NAT rule is typically used (where you translate the address to itself).

To logout from the FWSM, reconnect to the virtual HTTP IP address; you are prompted to log out.

To allow users to authenticate with the FWSM virtual server separately from the HTTP server, perform the following steps:

-
- Step 1** From the Configuration > Firewall > Advanced > Virtual Access > Virtual HTTP Server area, check the **Enable** check box.
- Step 2** In the Virtual HTTP Server field, add the IP address of the virtual HTTP server.
Make sure this address is an unused address that is routed to the FWSM. For example, if you perform NAT for inside addresses accessing an outside server, and you want to provide outside access to the virtual HTTP server, you can use one of the global NAT addresses for the virtual HTTP server address.
- Step 3** (Optional) To assign a hostname to the virtual HTTP server, enter a name in the Host field.
When a user is forwarded to the virtual HTTP server to enter their AAA username and password, you see the hostname in the following authentication dialog box message:
`Username for `HTTP Authentication (sessionID) from host_name' at server virtual_http_ip`
This information helps differentiate the AAA prompt from the destination HTTP server prompt.
- Step 4** (Optional) If you are using text-based browsers, where redirection does not happen automatically, check the **Display redirection warning** check box. This enables an alert to notify users when the HTTP connection is being redirected.
- Step 5** Click **Apply**.
The virtual server is added and the changes are saved to the running configuration.

Configuring Advanced Authentication Options

You can configure advanced authentication options, described in the following topics:

- [Enabling Secure Authentication of Web Clients, page 25-7](#)
- [Configuring the Authentication Proxy Limit, page 25-8](#)
- [Disabling Authentication Challenges, page 25-8](#)
- [Expiring Authentication Connections After Timing Out, page 25-8](#)

Enabling Secure Authentication of Web Clients

If you use HTTP authentication, by default the username and password are sent from the client to the FWSM in clear text; in addition, the username and password are sent on to the destination web server as well. The FWSM provides several methods of securing HTTP authentication, including the following methods:

- Enabling Virtual HTTP—Virtual HTTP lets you authenticate separately with the FWSM and with the HTTP server. Even if the HTTP server does not need a second authentication, this feature achieves the effect of stripping the basic authentication credentials from the HTTP GET request. See the [“Authenticating HTTP\(S\) Connections with a Virtual Server”](#) section on page 25-5 for more information.
- Enabling the Exchange of Usernames and Passwords Using HTTPS—To enable the exchange of usernames and passwords between a web client and the FWSM with HTTPS, perform the following steps:
 - a. From the Configuration > Firewall > AAA Rules pane, click **Advanced**. The AAA Rules Advanced Options dialog box appears.
 - b. Under Secure HTTP, click **Enable Secure HTTP**.
 - c. Click **OK**, and then click **OK** to exit the AAA Rules Advanced Options dialog box. Click **Apply**.

This is the only method that protects credentials between the client and the FWSM, as well as between the FWSM and the destination server. You can use this method alone, or in conjunction with either of the other methods so you can maximize your security.

After enabling this feature, when a user requires authentication when using HTTP, the FWSM redirects the HTTP user to an HTTPS prompt. After you authenticate correctly, the FWSM redirects you to the original HTTP URL.

Secured web-client authentication has the following limitations:

- A maximum of 128 concurrent HTTPS authentication sessions are allowed. If all 128 HTTPS authentication processes are running, a new connection requiring authentication will not succeed.
- When the uauth timeout is set to unlimited, HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the uauth timeout to 1 second (see the Configuration > Firewall > Advanced > Global Timeouts pane). However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.
- Because HTTPS authentication occurs on the SSL port 443, users must not configure an Access Rule to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port.
- HTTP users see a pop-up window generated by the browser itself if Secure HTTP is not configured. If Secure HTTP is configured, a form loads in the browser to collect username and password. In either case, if a user enters an incorrect password, the user is prompted again. When the web server and the authentication server are on different hosts, use Virtual HTTP to get the correct authentication behavior.

Configuring the Authentication Proxy Limit

You can manually configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user.

To set the proxy limit, perform the following steps:

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, click **Advanced**.
The AAA Rules Advanced Options dialog box appears.
 - Step 2** In the Proxy Limit area, check **Enable Proxy Limit**.
 - Step 3** In the Proxy Limit field, enter the number of concurrent proxy connections allowed per user, from 1 to 128.
 - Step 4** Click **OK**, and then click **Apply**.
-

Disabling Authentication Challenges

You can configure whether the FWSM challenges users for a username and password. By default, the FWSM prompts the user when a AAA rule enforces authentication for traffic in a new session and the protocol of the traffic is FTP, Telnet, HTTP, or HTTPS. In some cases, you may want to disable the authentication challenge for one or more of these protocols.

If you disable challenge authentication for a particular protocol, traffic using that protocol is allowed only if the traffic belongs to a session previously authenticated. This authentication can be accomplished by traffic using a protocol whose authentication challenge remains enabled. For example, if you disable challenge authentication for FTP, the FWSM denies a new session using FTP if the traffic is included in an authentication rule. If the user establishes the session with a protocol whose authentication challenge is enabled (such as HTTP), FTP traffic is allowed.

To disable authentication challenges, perform the following steps:

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, click **Advanced**.
The AAA Rules Advanced Options dialog box appears.
 - Step 2** In the Authentication Challenge area, uncheck the protocols for which you do not want challenges.
 - Step 3** Click **OK**, and then click **Apply**.
-

Expiring Authentication Connections After Timing Out

You can force any active connections to close immediately after the user authentication times out or when you clear the authentication session with the **clear uauth** command. Without this option, active connections are not terminated even though the user authentication session expired.

To set the authentication timeout values, see the Configuration > Firewall > Advanced > Global Timeouts pane.

When a connection is ended because of this option, syslog message 109036 is generated.

To identify hosts for which you want to clear connections, perform the following steps:

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, click **Advanced**.
The AAA Rules Advanced Options dialog box appears.
- Step 2** In the Expired Connections area, click **Add**.
The Add Clear Connection dialog box appears.
- Step 3** From the Interface Name drop-down list, choose the interface name connected to the source IP address.
- Step 4** In the IP Address field, enter the source IP address of the users for which you want to terminate connections.
- Step 5** From the Mask drop-down list, choose the source IP subnet mask.
- Step 6** Click **OK**, and then click **Apply**.
-

Configuring Authorization for Network Access

After a user authenticates for a given connection, the FWSM can use authorization to further control traffic from the user.

This section includes the following topics:

- [Configuring TACACS+ Authorization, page 25-9](#)
- [Configuring RADIUS Authorization, page 25-11](#)

Configuring TACACS+ Authorization

You can configure the FWSM to perform network access authorization with TACACS+. After a user authenticates, the FWSM checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the FWSM sends the username to the TACACS+ server. The TACACS+ server responds to the FWSM with a dynamic access list for that traffic, based on the user profile.

Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the FWSM.



Note

We suggest that you identify the same traffic for authentication as for authorization. Due to the way the FWSM uses the dynamic access list, if you have a more restrictive authorization statement than authentication, then some connections are unexpectedly denied. When a user first authenticates, if the connection matches the authentication statement and not the authorization statement, then later connections for that user that match the authorization statement are denied (for as long as the uauth session exists). Conversely, if the first connection matches the authorization statement, then later connections that do not match the authorization statement but that match the authentication statement are denied. Therefore, you need to match the authentication and authorization configurations.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

To configure TACACS+ authorization, perform the following steps:

-
- Step 1** Enable authentication. For more information, see the [“Configuring Network Access Authentication” section on page 25-3](#). If you have already enabled authentication, continue to the next step.
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Authorization Rule**.
The Add Authorization Rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface for applying the rule.
- Step 4** In the Action field, click one of the following, depending on the implementation:
- **Authorize**
 - **Do not Authorize.**
- Step 5** From the AAA Server Group drop-down list, choose a server group. To add a AAA server to the server group, click **Add Server**. See the [“Configuring AAA Server Groups” section on page 15-7](#) for more information.
Only TACACS+ servers are supported.
- Step 6** In the Source field, add the source IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
Be sure to use the same criteria as an authentication rule.
- Step 7** In the Destination field, enter the destination IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 8** In the Service field, enter an IP service name or number for the destination service, or click ellipsis (...) button to choose a service.
- Step 9** (Optional) In the Description field, add a description.
- Step 10** (Optional) Click **More Options** to do any of the following:
- To specify a source service for TCP or UDP, enter a TCP or UDP service in the Source Service field.
The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
 - To make the rule inactive, uncheck **Enable Rule**.
You may not want to remove a rule, but instead turn it off.
 - To set a time range for the rule, from the Time Range drop-down list, choose an existing time range. To add a new time range, click the ellipsis (...). For more information, see [Configuring Time Ranges, page 20-13](#).
- Step 11** Click **OK**.
The dialog box closes and the rule appears in the AAA Rules table.
- Step 12** Click **Apply**.
The changes are saved to the running configuration.
-

Configuring RADIUS Authorization

When authentication succeeds, the RADIUS protocol returns user authorizations in the access-accept message sent by a RADIUS server. For more information about configuring authentication, see the [“Configuring Authentication for Network Access” section on page 25-1](#).

When you configure the FWSM to authenticate users for network access, you are also implicitly enabling RADIUS authorizations; therefore, this section contains no information about configuring RADIUS authorization on the FWSM. It does provide information about how the FWSM handles access list information received from RADIUS servers.

You can configure a RADIUS server to download an access list to the FWSM or an access list name at the time of authentication. The user is authorized to do only what is permitted in the user-specific access list.

**Note**

If you have enabled the Per User Override Setting (see the Configuration > Firewall > Access Rules > Advanced > Access Rules Advanced Options dialog box), be aware of the following effects of this feature on authorization by user-specific access lists:

- Without the per-user-override feature, traffic for a user session must be permitted by both the interface access list and the user-specific access list.
- With the per-user-override feature, the user-specific access list determines what is permitted.

This section includes the following topics:

- [Configuring a RADIUS Server to Send Downloadable Access Control Lists, page 25-11](#)
- [Configuring a RADIUS Server to Download Per-User Access Control List Names, page 25-15](#)

Configuring a RADIUS Server to Send Downloadable Access Control Lists

This section describes how to configure Cisco Secure ACS or a third-party RADIUS server, and includes the following topics:

- [About the Downloadable Access List Feature and Cisco Secure ACS, page 25-11](#)
- [Configuring Cisco Secure ACS for Downloadable Access Lists, page 25-13](#)
- [Configuring Any RADIUS Server for Downloadable Access Lists, page 25-14](#)
- [Converting Wildcard Netmask Expressions in Downloadable Access Lists, page 25-15](#)

About the Downloadable Access List Feature and Cisco Secure ACS

Downloadable access lists is the most scalable means of using Cisco Secure ACS to provide the appropriate access lists for each user. It provides the following capabilities:

- Unlimited access list size—Downloadable access lists are sent using as many RADIUS packets as required to transport the full access list from Cisco Secure ACS to the FWSM.
- Simplified and centralized management of access lists—Downloadable access lists enable you to write a set of access lists once and apply it to many user or group profiles and distribute it to many FWSMs.

This approach is most useful when you have very large access list sets that you want to apply to more than one Cisco Secure ACS user or group; however, its ability to simplify Cisco Secure ACS user and group management makes it useful for access lists of any size.

The FWSM receives downloadable access lists from Cisco Secure ACS using the following process:

1. The FWSM sends a RADIUS authentication request packet for the user session.
2. If Cisco Secure ACS successfully authenticates the user, Cisco Secure ACS returns a RADIUS access-accept message that contains the internal name of the applicable downloadable access list. The Cisco IOS `cisco-av-pair` RADIUS VSA (vendor 9, attribute 1) contains the following attribute-value pair to identify the downloadable access list set:

```
ACS: CiscoSecure-Defined-ACL=acl-set-name
```

where `acl-set-name` is the internal name of the downloadable access list, which is a combination of the name assigned to the access list by the Cisco Secure ACS administrator and the date and time that the access list was last modified.

3. The FWSM examines the name of the downloadable access list and determines if it has previously received the named downloadable access list.
 - If the FWSM has previously received the named downloadable access list, communication with Cisco Secure ACS is complete and the FWSM applies the access list to the user session. Because the name of the downloadable access list includes the date and time it was last modified, matching the name sent by Cisco Secure ACS to the name of an access list previously downloaded means that the FWSM has the most recent version of the downloadable access list.
 - If the FWSM has not previously received the named downloadable access list, it may have an out-of-date version of the access list or it may not have downloaded any version of the access list. In either case, the FWSM issues a RADIUS authentication request using the downloadable access list name as the username in the RADIUS request and a null password attribute. In a `cisco-av-pair` RADIUS VSA, the request also includes the following attribute-value pairs:

```
AAA:service=ip-admission
AAA:event=acl-download
```

In addition, the FWSM signs the request with the Message-Authenticator attribute (IETF RADIUS attribute 80).

4. Upon receipt of a RADIUS authentication request that has a username attribute containing the name of a downloadable access list, Cisco Secure ACS authenticates the request by checking the Message-Authenticator attribute. If the Message-Authenticator attribute is missing or incorrect, Cisco Secure ACS ignores the request. The presence of the Message-Authenticator attribute prevents malicious use of a downloadable access list name to gain unauthorized network access. The Message-Authenticator attribute and its use are defined in RFC 2869, RADIUS Extensions, available at <http://www.ietf.org>.
5. If the access list required is less than approximately 4 KB in length, Cisco Secure ACS responds with an access-accept message containing the access list. The largest access list that can fit in a single access-accept message is slightly less than 4 KB because some of the message must be other required attributes.

Cisco Secure ACS sends the downloadable access list in a `cisco-av-pair` RADIUS VSA. The access list is formatted as a series of attribute-value pairs that each contain an ACE and are numbered serially:

```
ip:inacl#1=ACE-1
ip:inacl#2=ACE-2
.
.
ip:inacl#n=ACE-n
```

An example of an attribute-value pair follows:

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

6. If the access list required is more than approximately 4 KB in length, Cisco Secure ACS responds with an access-challenge message that contains a portion of the access list, formatted as described above, and an State attribute (IETF RADIUS attribute 24), which contains control data used by Cisco Secure ACS to track the progress of the download. Cisco Secure ACS fits as many complete attribute-value pairs into the cisco-av-pair RADIUS VSA as it can without exceeding the maximum RADIUS message size.

The FWSM stores the portion of the access list received and responds with another access-request message containing the same attributes as the first request for the downloadable access list plus a copy of the State attribute received in the access-challenge message.

This repeats until Cisco Secure ACS sends the last of the access list in an access-accept message.

Configuring Cisco Secure ACS for Downloadable Access Lists

You can configure downloadable access lists on Cisco Secure ACS as a shared profile component and then assign the access list to a group or to an individual user.

The access list definition consists of one or more FWSM commands that are similar to the extended **access-list** command, except without the following prefix:

```
access-list acl_name extended
```

The following example is a downloadable access list definition on Cisco Secure ACS version 3.3:

```
+-----+
| Shared profile Components                               |
|                                                         |
|     Downloadable IP ACLs Content                       |
| Name:      acs_ten_acl                                 |
|                                                         |
|     ACL Definitions                                    |
| permit tcp any host 10.0.0.254                         |
| permit udp any host 10.0.0.254                         |
| permit icmp any host 10.0.0.254                       |
| permit tcp any host 10.0.0.253                       |
| permit udp any host 10.0.0.253                       |
| permit icmp any host 10.0.0.253                      |
| permit tcp any host 10.0.0.252                       |
| permit udp any host 10.0.0.252                       |
| permit icmp any host 10.0.0.252                      |
| permit ip any any                                     |
+-----+
```

For more information about creating downloadable access lists and associating them with users, see the user guide for your version of Cisco Secure ACS.

On the FWSM, the downloaded access list has the following name:

```
#ACSACL#-ip-acl_name-number
```

The *acl_name* argument is the name that is defined on Cisco Secure ACS (*acs_ten_acl* in the preceding example), and *number* is a unique version ID generated by Cisco Secure ACS.

The downloaded access list on the FWSM consists of the following lines:

```
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
```

```

access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit ip any any

```

Configuring Any RADIUS Server for Downloadable Access Lists

You can configure any RADIUS server that supports Cisco IOS RADIUS VSAs to send user-specific access lists to the FWSM in a Cisco IOS RADIUS cisco-av-pair VSA (vendor 9, attribute 1).

In the cisco-av-pair VSA, configure one or more ACEs that are similar to the **access-list extended** command, except that you replace the following command prefix:

```
access-list acl_name extended
```

with the following text:

```
ip:inacl#nnn=
```

The *nnn* argument is a number in the range from 0 to 999999999 that identifies the order of the command statement to be configured on the FWSM. If this parameter is omitted, the sequence value is 0, and the order of the ACEs inside the cisco-av-pair RADIUS VSA is used.

The following example is an access list definition as it should be configured for a cisco-av-pair VSA on a RADIUS server:

```

ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#99=deny tcp any any
ip:inacl#2=permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#100=deny udp any any
ip:inacl#3=permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0

```

For information about making unique per user the access lists that are sent in the cisco-av-pair attribute, see the documentation for your RADIUS server.

On the FWSM, the downloaded access list name has the following format:

```
AAA-user-username
```

The *username* argument is the name of the user that is being authenticated.

The downloaded access list on the FWSM consists of the following lines. Notice the order based on the numbers identified on the RADIUS server.

```

access-list AAA-user-bcham34-79AD4A08 permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list AAA-user-bcham34-79AD4A08 permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list AAA-user-bcham34-79AD4A08 permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list AAA-user-bcham34-79AD4A08 deny tcp any any
access-list AAA-user-bcham34-79AD4A08 deny udp any any

```

Downloaded access lists have two spaces between the word “access-list” and the name. These spaces serve to differentiate a downloaded access list from a local access list. In this example, “79AD4A08” is a hash value generated by the FWSM to help determine when access list definitions have changed on the RADIUS server.

Converting Wildcard Netmask Expressions in Downloadable Access Lists

If a RADIUS server provides downloadable access lists to Cisco VPN 3000 series concentrators as well as to the FWSM, you may need the FWSM to convert wildcard netmask expressions to standard netmask expressions. This is because Cisco VPN 3000 series concentrators support wildcard netmask expressions but the FWSM only supports standard netmask expressions. Configuring the FWSM to convert wildcard netmask expressions helps minimize the effects of these differences upon how you configure downloadable access lists on your RADIUS servers. Translation of wildcard netmask expressions means that downloadable access lists written for Cisco VPN 3000 series concentrators can be used by the FWSM without altering the configuration of the downloadable access lists on the RADIUS server.

You configure access list netmask conversion on a per-server basis when you add a server to a server group, on the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area. See the [“Adding a Server to a Group”](#) section on page 15-8.

Configuring a RADIUS Server to Download Per-User Access Control List Names

To download a name for an access list that you already created on the FWSM (at the CLI) from the RADIUS server when a user authenticates, configure the IETF RADIUS filter-id attribute (attribute number 11) as follows:

```
filter-id=acl_name
```

**Note**

In Cisco Secure ACS, the value for filter-id attributes are specified in boxes in the HTML interface, omitting **filter-id=** and entering only *acl_name*.

For information about making unique per user the filter-id attribute value, see the documentation for your RADIUS server.

See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using the CLI* to create an access list on the FWSM.

Configuring Accounting for Network Access

The FWSM can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the FWSM. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the FWSM for the session, the service used, and the duration of each session.

To configure accounting, perform the following steps:

- Step 1** If you want the FWSM to provide accounting data per user, you must enable authentication. For more information, see the [“Configuring Network Access Authentication”](#) section on page 25-3. If you want the FWSM to provide accounting data per IP address, enabling authentication is not necessary and you can continue to the next step.
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Accounting Rule**. The Add Accounting Rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface for applying the rule.

- Step 4** In the Action field, click one of the following, depending on the implementation:
- **Account**
 - **Do not Account.**
- Step 5** From the AAA Server Group drop-down list, choose a server group. To add a AAA server to the server group, click **Add Server**. See the “[Configuring AAA Server Groups](#)” section on page 15-7 for more information.
- Step 6** In the Source field, add the source IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 7** In the Destination field, enter the destination IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 8** In the Service field, enter an IP service name or number for the destination service, or click ellipsis (...) button to choose a service.
- Step 9** (Optional) In the Description field, add a description.
- Step 10** (Optional) Click **More Options** to do any of the following:
- To specify a source service for TCP or UDP, enter a TCP or UDP service in the Source Service field. The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
 - To make the rule inactive, uncheck **Enable Rule**.
You may not want to remove a rule, but instead turn it off.
 - To set a time range for the rule, from the Time Range drop-down list, choose an existing time range. To add a new time range, click the ellipsis (...). For more information, see [Configuring Time Ranges](#), page 20-13.
- Step 11** Click **OK**.
The dialog box closes and the rule appears in the AAA Rules table.
- Step 12** Click **Apply**.
The changes are saved to the running configuration.

Using MAC Addresses to Exempt Traffic from Authentication and Authorization

The FWSM can exempt from authentication and authorization any traffic from specific MAC addresses. For example, if the FWSM authenticates TCP traffic originating on a particular network but you want to allow unauthenticated TCP connections from a specific server, you would use a MAC exempt rule to exempt from authentication and authorization any traffic from the server specified by the rule. This feature is particularly useful to exempt devices such as IP phones that cannot respond to authentication prompts.

The order of entries matters, because the packet uses the first entry it matches, as opposed to a best match scenario. If you have a permit entry, and you want to deny an address that is allowed by the permit entry, be sure to enter the deny entry before the permit entry.

To use MAC addresses to exempt traffic from authentication and authorization, perform the following steps:

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add MAC Exempt Rule**.
The Add MAC Exempt Rule dialog box appears.
- Step 2** From the Action drop-down list, click one of the following, depending on the implementation:
- **MAC Exempt**
 - **No MAC Exempt**
- The MAC Exempt option allows traffic from the MAC address without having to authenticate or authorize. The No MAC Exempt option specifies a MAC address that is not exempt from authentication or authorization. You might need to add a deny entry if you permit a range of MAC addresses using a MAC address mask such as ffff.fff.0000, and you want to force a MAC address in that range to be authenticated and authorized.
- Step 3** In the MAC Address field, specify the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn.
- Step 4** In the MAC Mask field, specify the portion of the MAC address that should be used for matching. For example, ffff.ffff.ffff matches the MAC address exactly. ffff.ffff.0000 matches only the first 8 digits.
- Step 5** Click **OK**.
The dialog box closes and the rule appears in the AAA Rules table.
- Step 6** Click **Apply**.
The changes are saved to the running configuration.

