



CHAPTER 19

Configuring AAA Rules

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

For information about AAA for management access, see the [“AAA Access” section on page 11-1](#)

This chapter includes the following sections:

- [AAA Performance, page 19-1](#)
- [Configuring AAA Rules, page 19-1](#)
- [Configuring a RADIUS Server for Authorization, page 19-15](#)

AAA Performance

The security appliance 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 security appliance cut-through proxy challenges a user initially at the application layer and then authenticates against standard AAA servers or the local database. After the security appliance 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 AAA Rules

This section describes how to configure AAA rules, and includes the following topics:

- [AAA Rules, page 19-2](#)
- [Add/Edit Authentication Rule, page 19-4](#)
- [Add/Edit Authorization Rule, page 19-7](#)
- [Add/Edit Accounting Rule, page 19-10](#)
- [Add/Edit MAC Exempt Rule, page 19-12](#)
- [Configuring Advanced AAA Features, page 19-12](#)

AAA Rules

The Security Policy pane shows your network security policy expressed in rules. This window includes tabs for AAA Rules, as well as for other rules. This topic describes AAA Rules. For an overview of AAA services, see [Chapter 10, “Configuring AAA Servers.”](#)

When you choose the **AAA Rules** tab, you can define authentication, authorization, or accounting (AAA) rules, as well as MAC exempt rules. AAA tells the security appliance who the user is, what the user can do, and what the user did. You can use authentication alone, or with authorization. Authorization always requires authentication. For example, if you authenticate outside users who access any server on the inside network, then authentication alone is adequate. However, if you want to limit the inside servers that a particular user accesses, you can configure an authorization server to specify which servers and services that user is allowed to access.

AAA provides a greater level of protection and control for user access than using access lists alone. For example, you can create an access list allowing all outside users to access a server on the DMZ network. But if you want only registered users to Telnet to the server, you can configure AAA to allow only authenticated and/or authorized users to make it past the security appliance. If the server also has its own authentication and authorization, the user enters a second set of user name and password (in the case of FTP, the user must enter both usernames and passwords separated by an at sign (@)).

Each AAA rule identifies the following characteristics for matching traffic:

- The source and destination network
- The action (authentication, authorization, or accounting; a rule can also exempt a MAC address from AAA)
- The AAA server group
- The service type (for example, Telnet or FTP)

Restrictions

ASDM does not support a mixed configuration of AAA rules that:

- Specify the source and destination addresses
- Match access lists for the source and destination addresses

If your configuration already contains AAA rules, then you can add only AAA rules of the same kind. If you have not configured any AAA rules, then ASDM allows you to add only rules that match access lists. To convert your rules to match access lists, you must delete all of your AAA rules in ASDM, then re-add them (with no rules configured, ASDM defaults to access list mode). In ASDM, the configuration of AAA rules is the same in both modes.

- For FTP authentication, the user must enter the name and password in the following format:
security appliance_name@ftp_name
security appliance_password@ftp_password
- The security appliance forwards the FTP name and password to the FTP server after successful authentication on the security appliance. Other services such as Telnet and HTTP (if configured for authentication) require you to enter a second name and password at the destination server prompt.
- Some services are not reliably authenticated, such as mail or SMTP. If you specify that *all* services need to be authenticated, then the user must first authenticate with Telnet, FTP, HTTP, or HTTPS (or another service that reliably provides an authentication prompt), and then use the other services.
- AAA authorization rules support TACACS+ servers, but not other servers. However, you can use the local database to authorize users for security appliance commands.
- AAA accounting rules are not supported using the local database as the AAA Server Group.

Prerequisites

1. Define each host or server in the Configuration > Features > Properties > AAA Setup > [AAA Server Groups](#) pane.
2. Add users to the local database. (See **Configuration > Features > Properties > Administration > User Accounts**.)
3. Be sure that users can access the specified network (by an [Access Rules](#) if required).
4. Set up the AAA server correctly.

Fields

- **Add**—Adds a new AAA rule. Choose the type of rule you want to add from the drop-down list.
- **Edit**—Edits an AAA rule.
- **Delete**—Deletes a AAA rule.
- **Move Up**—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.
- **Move Down**—Moves a rule down.
- **Cut**—Cuts a rule.
- **Copy**—Copies a rule's parameters so you can start a new rule with the same parameters using the Paste button.
- **Paste**—Opens an Add/Edit Rule dialog box with the copied or cut rule's parameters prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.
- **Find**—Filters the display to show only matching rules. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
 - **Filter drop-down list**—Choose the criteria to filter on, either Interface, Source, Destination, Service, Action, or Rule Query. A rule query is a collection of multiple criteria that you can save and use repeatedly.
 - **Filter field**—For the Interface type, this field becomes a drop-down list so you can choose an interface name, or **All Interfaces**. For the Action type, the drop-down list includes Permit and Deny. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type one manually, or browse for one by clicking the ... button and launching the Browse Address dialog box. The Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can type one manually, or browse for one by clicking the ... button and launching the [Browse Service Groups](#) dialog box.
 - **Filter**—Runs the filter.
 - **Clear**—Clears the Filter field.
 - **Rule Query**—Opens the [Rule Queries](#) dialog box so you can manage named rule queries.
- **Show Rule Flow Diagram**—Shows the Rule Flow Diagram area under the rule table. This diagram shows the networks, type of traffic, interface name, direction of flow, and action (for example, Authenticate or Do Not Authenticate).
- **Packet Trace**—Opens the [Packet Tracer](#) tool with the parameters pre-filled with the characteristics of the selected rule.

The following description summarizes the columns in the AAA Rules table. You can edit the contents of these columns by double-clicking on a table cell. Double-clicking on a column header sorts the table in ascending alphanumeric order, using the selected column as the sort key. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- **No**—Indicates the order of evaluation for the rule.
- **Enabled**—Indicates whether the rule is enabled or disabled.
- **Action**—Specifies the type of AAA rule.
- **Source**—Lists the IP addresses that are subject to AAA when traffic is sent to the IP addresses listed in the Destination column.
- **Destination**—Lists the IP addresses that are subject to AAA when traffic is sent from the IP addresses listed in the Source column.
- **Service**—Shows the service or protocol specified by the rule.
- **Action**—Shows the action specified by the rule, including Authenticate, Do Not Authenticate, Authorize, Do Not Authorize, and so on.
- **Server Group**—Specifies the AAA Server Group tag. Configure AAA server groups in Properties > AAA Setup > [AAA Server Groups](#). To create new AAA rules, a server group must exist and have one or more servers in it.
- **Time**—Specifies the name of the time range in effect for this rule.
- **Description**—The description you entered when you added the rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Authentication Rule

The security appliance lets you configure network access authentication using AAA servers or the local database.

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See [Timeouts](#) for timeout values.) For example, if you configure the security appliance 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.

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

If you do not want to allow HTTP(S), Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can configure virtual Telnet. With virtual Telnet, the user Telnets to a given IP address configured on the security appliance and the security appliance provides a Telnet prompt.

For Telnet, HTTP(S), and FTP, the security appliance generates an authentication prompt. If the destination server also has its own authentication, the user enters another username and password.

For HTTP authentication, the security appliance checks local ports when static NAT is configured. If it detects traffic destined for local port 80, regardless of the global port, the security appliance 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.

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

If the local port is different than port 80, then users do not see the authentication page. Instead, the security appliance sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.



Note

If you use HTTP authentication without using secure HTTP client authentication (see [Configuring Advanced AAA Features](#)), the username and password are sent in clear text to the destination web server, and not just to the AAA server. For example, if you authenticate inside users when they access outside web servers, anyone on the outside can learn valid usernames and passwords. We recommend that you use secure HTTP client authentication whenever you enable HTTP authentication.

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

```
name> jamiiec@jchrichton
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 (@).

Fields

Interface and Action—Choose the interface, action, and AAA server group.

- Interface—Choose the interface on which to apply this rule.
- Action—Choose **Authenticate** or **Do not Authenticate**.
- AAA Server Group—Choose a AAA server group or the local database. You must add the server group in Properties > AAA Setup > [AAA Server Groups](#).
- **Add Server/User**—Click this button to add a server to the selected AAA server group, or a user to the local database.

Source—Specify the source address for traffic you want to authenticate.

- Type—Choose the type of address you want to use, including any, IP address, Network Object Group, or Interface IP.

If you choose **IP address**, the you see the following fields:

- IP Address—Enter it manually or click the ... button to choose from the Browse Address dialog box.
- Netmask—Choose a subnet mask from the drop-down list.

If you choose **Network Object Group**, you see the following field:

- Group Name—Choose a group name from the drop-down list, or click the ... button to bring up the Browse Address dialog box. From the Browse Address dialog box, you can add a network object group.

If you choose **Interface IP**, you see the following field:

- Interface—Choose an interface from the drop-down list.

Destination—Specify the destination address for traffic you want to authenticate.

- Type—Choose the type of address you want to use, including any, IP address, Network Object Group, or Interface IP.

If you choose **IP address**, the you see the following fields:

- IP Address—Enter it manually or click the ... button to choose from the Browse Address dialog box.
- Netmask—Choose a subnet mask from the drop-down list.

If you choose **Network Object Group**, you see the following field:

- Group Name—Choose a group name from the drop-down list, or click the ... button to bring up the Browse Address dialog box. From the Browse Address dialog box, you can add a network object group.

If you choose **Interface IP**, you see the following field:

- Interface—Choose an interface from the drop-down list.

Protocol and Service—Specify the port or protocol for traffic you want to authenticate.

- Protocol—Choose the protocol for the traffic, either tcp, udp, ip, icmp, or other.

If you choose **tcp** or **udp**, then you see the following fields:

- Source Port—Set the source port for the traffic you want to authenticate.

Service—Click this radio button to enter a port or range of ports. Choose an operator from the drop-down list, including = (equal), != (not equal), > (greater than), < (less than), and range. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.

Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

- Destination Port—Set the destination port for the traffic you want to authenticate.

Service—Click this radio button to enter a port or range of ports. Choose an operator from the drop-down list, including = (equal), != (not equal), > (greater than), < (less than), and range. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.

Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

If you choose **icmp**, then you see the following fields:

- ICMP Type—Click this radio button to enter an ICMP type. Either type a number, or choose a well-known type from the drop-down list.
- ICMP Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

If you choose **other**, then you see the following fields:

- Protocol—Click this radio button to enter an IP protocol type. Either type a number, or choose a well-known type from the drop-down list.
- Protocol Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

Rule Flow Diagram—Shows the Rule Flow Diagram for this rule. This diagram shows the networks, type of traffic, interface name, direction of flow, and action (for example, Authenticate or Do Not Authenticate).

Options—Set options for this rule.

- **Time Range**—Choose the name of an existing time range from the drop-down list. A time range enables a rule only during the specified times. Create a time range on [Configuring Time Ranges](#).
- **Description**—Enter a description for this rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Authorization Rule

You can configure the security appliance to perform network access authorization with TACACS+.



Note

When you configure the security appliance to authenticate users for network access using RADIUS, you are also implicitly enabling RADIUS authorizations. RADIUS authorization does not require a separate authorization rule, like TACACS+. See the “[Configuring a RADIUS Server for Authorization](#)” section on page 19-15 for more information about using RADIUS for authorization.

Authentication and authorization rules are independent; however, any unauthenticated traffic matched by an authorization rule will be denied. For authorization to succeed, a user must first authenticate with the security appliance. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the security appliance checks the authorization rules for matching traffic. If the traffic matches the authorization rule, the security appliance sends the username to the TACACS+ server. The TACACS+ server responds to the security appliance with a permit or a deny for that traffic, based on the user profile. The security appliance enforces the authorization rule in the response.

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

Fields

Interface and Action—Choose the interface, action, and AAA server group.

- Interface—Choose the interface on which to apply this rule.
- Action—Choose **Authorize** or **Do not Authorize**.
- AAA Server Group—Choose a AAA server group or the local database. You must add the server group in Properties > AAA Setup > [AAA Server Groups](#).
- **Add Server/User**—Click this button to add a server to the selected AAA server group, or a user to the local database.

Source—Specify the source address for traffic you want to authorize.

- Type—Choose the type of address you want to use, including any, IP address, Network Object Group, or Interface IP.

If you choose **IP address**, the you see the following fields:

- IP Address—Enter it manually or click the ... button to choose from the Browse Address dialog box.
- Netmask—Choose a subnet mask from the drop-down list.

If you choose **Network Object Group**, you see the following field:

- Group Name—Choose a group name from the drop-down list, or click the ... button to bring up the Browse Address dialog box. From the Browse Address dialog box, you can add a network object group.

If you choose **Interface IP**, you see the following field:

- Interface—Choose an interface from the drop-down list.

Destination—Specify the destination address for traffic you want to authorize.

- Type—Choose the type of address you want to use, including any, IP address, Network Object Group, or Interface IP.

If you choose **IP address**, the you see the following fields:

- IP Address—Enter it manually or click the ... button to choose from the Browse Address dialog box.
- Netmask—Choose a subnet mask from the drop-down list.

If you choose **Network Object Group**, you see the following field:

- Group Name—Choose a group name from the drop-down list, or click the ... button to bring up the Browse Address dialog box. From the Browse Address dialog box, you can add a network object group.

If you choose **Interface IP**, you see the following field:

- Interface—Choose an interface from the drop-down list.

Protocol and Service—Specify the port or protocol for traffic you want to authorize.

- **Protocol**—Choose the protocol for the traffic, either `tcp`, `udp`, `ip`, `icmp`, or `other`.

If you choose **tcp** or **udp**, then you see the following fields:

- **Source Port**—Set the source port for the traffic you want to authorize.

Service—Click this radio button to enter a port or range of ports. Choose an operator from the drop-down list, including = (equal), != (not equal), > (greater than), < (less than), and range. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.

Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

- **Destination Port**—Set the destination port for the traffic you want to authorize.

Service—Click this radio button to enter a port or range of ports. Choose an operator from the drop-down list, including = (equal), != (not equal), > (greater than), < (less than), and range. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.

Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

If you choose **icmp**, then you see the following fields:

- **ICMP Type**—Click this radio button to enter an ICMP type. Either type a number, or choose a well-known type from the drop-down list.
- **ICMP Group**—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

If you choose **other**, then you see the following fields:

- **Protocol**—Click this radio button to enter an IP protocol type. Either type a number, or choose a well-known type from the drop-down list.
- **Protocol Group**—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

Rule Flow Diagram—Shows the Rule Flow Diagram for this rule. This diagram shows the networks, type of traffic, interface name, direction of flow, and action (for example, authorize or Do Not Authorize).

Options—Set options for this rule.

- **Time Range**—Choose the name of an existing time range from the drop-down list. A time range enables a rule only during the specified times. Create a time range on [Configuring Time Ranges](#).
- **Description**—Enter a description for this rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Accounting Rule

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. 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 security appliance for the session, the service used, and the duration of each session.

Fields

Interface and Action—Choose the interface, action, and AAA server group.

- Interface—Choose the interface on which to apply this rule.
- Action—Choose **Account** or **Do not Account**.
- AAA Server Group—Choose a AAA server group or the local database. You must add the server group in Properties > AAA Setup > [AAA Server Groups](#).
- **Add Server/User**—Click this button to add a server to the selected AAA server group, or a user to the local database.

Source—Specify the source address for traffic you want to authenticate.

- Type—Choose the type of address you want to use, including any, IP address, Network Object Group, or Interface IP.

If you choose **IP address**, the you see the following fields:

- IP Address—Enter it manually or click the ... button to choose from the Browse Address dialog box.
- Netmask—Choose a subnet mask from the drop-down list.

If you choose **Network Object Group**, you see the following field:

- Group Name—Choose a group name from the drop-down list, or click the ... button to bring up the Browse Address dialog box. From the Browse Address dialog box, you can add a network object group.

If you choose **Interface IP**, you see the following field:

- Interface—Choose an interface from the drop-down list.

Destination—Specify the destination address for traffic you want to account.

- Type—Choose the type of address you want to use, including any, IP address, Network Object Group, or Interface IP.

If you choose **IP address**, the you see the following fields:

- IP Address—Enter it manually or click the ... button to choose from the Browse Address dialog box.

- Netmask—Choose a subnet mask from the drop-down list.

If you choose **Network Object Group**, you see the following field:

- Group Name—Choose a group name from the drop-down list, or click the ... button to bring up the Browse Address dialog box. From the Browse Address dialog box, you can add a network object group.

If you choose **Interface IP**, you see the following field:

- Interface—Choose an interface from the drop-down list.

Protocol and Service—Specify the port or protocol for traffic you want to account.

- Protocol—Choose the protocol for the traffic, either tcp or udp.
 - Source Port—Set the source port for the traffic you want to account.

Service—Click this radio button to enter a port or range of ports. Choose an operator from the drop-down list, including = (equal), != (not equal), > (greater than), < (less than), and range. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.

Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.
 - Destination Port—Set the destination port for the traffic you want to account.

Service—Click this radio button to enter a port or range of ports. Choose an operator from the drop-down list, including = (equal), != (not equal), > (greater than), < (less than), and range. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.

Group—Click this radio button to specify a service group, created on [Service Groups](#). Choose a group name from the drop-down list, or click the ... button to bring up the [Browse Service Groups](#) dialog box. From the [Browse Service Groups](#) dialog box, you can add a service group.

Rule Flow Diagram—Shows the Rule Flow Diagram for this rule. This diagram shows the networks, type of traffic, interface name, direction of flow, and action (for example, Account or Do Not Account).

Options—Set options for this rule.

- **Time Range**—Choose the name of an existing time range from the drop-down list. A time range enables a rule only during the specified times. Create a time range on [Configuring Time Ranges](#).
- **Description**—Enter a description for this rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit MAC Exempt Rule

The security appliance can exempt from authentication and authorization any traffic from specific MAC addresses.

For example, if the security appliance 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.

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.

Fields

- **Action**—Choose **MAC Exempt** or **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.ffff.0000, and you want to force a MAC address in that range to be authenticated and authorized.
- **MAC Address**—Specifies the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn.
- **MAC Mask**—Specifies 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Configuring Advanced AAA Features

The Advanced AAA Configuration dialog box enables secure HTTP, sets the Proxy Limit, and enables interactive authentication.

Fields

- **Secure HTTP**—Specifies whether to enable or disable Secure HTTP (HTTPS).
- **Enable Secure HTTP**—Enables secure HTTP authentication. Without securing HTTP authentication, usernames and passwords from the client to the security appliance are passed as clear text. By enabling this option, you enable the exchange of usernames and passwords between a web client and the security appliance with HTTPS. After enabling this feature, when a user requires authentication when using HTTP, the security appliance redirects the HTTP user to an HTTPS prompt. After you authenticate correctly, the security appliance redirects you to the original HTTP URL.
- **Proxy Limit**—Specifies Proxy Limit parameters.

- **Enable Proxy Limit**—Limits the number of concurrent proxy connections allowed per user. The maximum is 128. If you do not enable this feature, no limit is imposed.
- **Proxy Limit**— Specifies the number of concurrent proxy connections allowed. The range is 1 through 128. The default is 16.
- **Interactive Authentication**—Configures interactive authentication for HTTP and HTTPS traffic. The default is to use inline basic authentication. This area also configures direct authentication. See the [“Adding an Interactive Authentication Rule” section on page 19-13](#) for detailed information about interactive authentication.
 - **Interface**—Shows the interface on which you enabled interactive authentication.
 - **Protocol**—Shows the protocol, HTTP or HTTPS.
 - **Port**—Shows the listening port.
 - **Redirect**—Shows whether you enabled redirection for through traffic. Without redirection, this rule only enables direct authentication.
 - **Add**—Adds an interactive authentication rule.
 - **Edit**—Edits an interactive authentication rule.
 - **Delete**—Deletes an interactive authentication rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Adding an Interactive Authentication Rule

By default for HTTP, the security appliance uses basic HTTP authentication. For HTTPS, the security appliance generates a similar custom login screen. Using the Configuration > Security Policy > AAA Rules > Advanced AAA Configuration > Add Interactive Authentication dialog box, you can configure the security appliance to redirect users to an internal web page where they can enter their username and password.

If you enable the redirect method of HTTP and HTTPS authentication, then you also automatically enable direct authentication with the security appliance. Direct authentication is useful if you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic; a user can authenticate directly with the security appliance using HTTP or HTTPS before other traffic is allowed. You can configure direct authentication independently if you want to continue to use basic HTTP authentication for through traffic. To access the login page for direct authentication, enter one of the following URLs:

```
http://interface_ip[:port]/netaccess/connstatus.html
https://interface_ip[:port]/netaccess/connstatus.html
```

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

To configure an interactive authentication rule, perform the following steps:

-
- Step 1** From the Configuration > Security Policy > AAA Rules > Advanced AAA Configuration dialog box, click **Add**.
- Step 2** From the Protocol menu, choose **HTTP** or **HTTPS**.
To enable listeners for both HTTP and HTTPS, you need to create two separate rules.
- Step 3** From the Interface menu, choose the interface name on which you want to enable the listener.
- Step 4** From the Port menu, either choose a common port or type the port number on which you want to listen. The default is 80 for HTTP and 443 for HTTPS.
- Step 5** To redirect through traffic to the listening port for authentication, check the **Redirect network users for authentication requests** check box.
If you do not check this check box, then only direct authentication is enabled.
- Step 6** Click **OK**.
-

Fields

- Protocol—Sets the protocol for the interactive authentication rule, either HTTP or HTTPS.
- Interface—Sets the interface name on which you want to enable the listening port.
- Port—Sets the port number on which you want to listen. Choose a common port or type the port number. The default is 80 for HTTP and 443 for HTTPS.
- Redirect network users for authentication requests—Redirects through traffic to the listening port for authentication. If you do not check this check box, then only direct authentication is enabled.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Configuring a RADIUS Server for Authorization

When authentication succeeds, the RADIUS protocol returns user authorizations in the access-accept message sent by a RADIUS server.

When you configure the security appliance 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 security appliance. It does provide information about how the security appliance handles access list information received from RADIUS servers.

You can configure a RADIUS server to download an access list to the security appliance 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 used the **access-group** command to apply access lists to interfaces, be aware of the following effects of the **per-user-override** keyword on authorization by user-specific access lists:

- Without the **per-user-override** keyword, 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** keyword, the user-specific access list determines what is permitted.

For more information, see the **access-group** command entry in the *Cisco ASA 5500 Series Command Reference*.

This section includes the following topics:

- [Configuring a RADIUS Server to Send Downloadable Access Control Lists, page 19-15](#)
- [Configuring a RADIUS Server to Download Per-User Access Control List Names, page 19-19](#)

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 19-15](#)
- [Configuring Cisco Secure ACS for Downloadable Access Lists, page 19-17](#)
- [Configuring Any RADIUS Server for Downloadable Access Lists, page 19-18](#)
- [Converting Wildcard Netmask Expressions in Downloadable Access Lists, page 19-19](#)

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 security appliance.
- 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 security appliances.

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 security appliance receives downloadable access lists from Cisco Secure ACS using the following process:

1. The security appliance 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 security appliance examines the name of the downloadable access list and determines if it has previously received the named downloadable access list.
 - If the security appliance has previously received the named downloadable access list, communication with Cisco Secure ACS is complete and the security appliance 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 security appliance has the most recent version of the downloadable access list.
 - If the security appliance 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 security appliance 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 security appliance 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
```

- 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 security appliance 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 security appliance 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 security appliance, 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 security appliance consists of the following lines:

```
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-ac_s_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-ac_s_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 security appliance 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 security appliance. 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 security appliance, 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 security appliance 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 security appliance 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 security appliance, you may need the security appliance to convert wildcard netmask expressions to standard netmask expressions. This is because Cisco VPN 3000 Series Concentrators support wildcard netmask expressions but the security appliance only supports standard netmask expressions. Configuring the security appliance 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 security appliance without altering the configuration of the downloadable access lists on the RADIUS server.

You configure access list netmask conversion on a per server basis, using the **acl-netmask-convert** command, available in the `aaa-server` configuration mode. For more information about configuring a RADIUS server, see [AAA Setup](#). For more information about the **acl-netmask-convert** command, see the *Cisco ASA 5500 Series Command Reference*.

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 security appliance 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.

