Managing Firewall AAA Rules

You can use Authentication, Authorization, and Accounting (AAA) rules to control access to network resources based on user privileges rather than by IP addresses. If you configure authentication rules, users must enter a username and password whenever they attempt to access a network behind the protected device. Once authenticated, you can further require that the user account be checked to ensure the user is authorized for network access. Finally, you can use accounting rules to track access for billing, security, or resource allocation purposes.

AAA rule configuration is complex and requires that you configure more than just the AAA rules policy. The following topics explain AAA rules in greater detail and include procedures that explain not only the AAA rules policy configuration but also what you must configure in related policies:

The following topics can help you with general rule table usage:

Understanding AAA Rules

You can use Authentication, Authorization, and Accounting (AAA) rules to control access to network resources based on user privileges rather than by IP addresses. AAA rules provide a different type of control compared to traditional access rules; where access rules allow you to control which IP addresses and services are allowed, AAA rules allow you to configure ACLs for each user to define the authorization available on a user basis, regardless of the IP address from which the user connects. (These per-user ACLs are configured in the AAA server, not in the AAA rule defined on the device.)

AAA rules policies differ from other device platform AAA policies in that AAA rules apply to traffic that is passing through the device, not to traffic directed specifically at the device. By using AAA rules, you can control entry into, or out of, a network. This might be useful if you have a network segment that

is high security, where you want to carefully control access. AAA rules are also useful for circumstances where you need to maintain per-user accounting records for billing, security, or resource allocation purposes.

The AAA rules policy actually configures three separate types of rule, and the configuration of these rules differs significantly between IOS devices on the one hand and ASA, PIX, and FWSM devices on the other hand. For IOS devices, these policies define what is called authentication proxy admission control. When creating shared AAA rules, create separate rules for these types of devices. Following are the types of rules you can configure with AAA rules:

- Authentication rules—Authentication rules control basic user access. If you configure an authentication rule, users must log in if their connection request goes through the device on which the rule is defined. You can force users to log in for HTTP, HTTPS, FTP, or Telnet connections. For ASA, PIX, and FWSM devices, you can control other types of services, but users must first authenticate using one of the supported protocols before other types of traffic are allowed.

  The device recognizes these traffic types only on the default ports: FTP (21), Telnet (23), HTTP (80), HTTPS (443). If you map these types of traffic to other ports, the user will not be prompted, and access will fail.

- Authorization rules—You can define an additional level of control over and above authentication. Authentication simply requires that users identify themselves. After authentication is successful, an authorization rule can query the AAA server to determine if the user has sufficient privileges to complete the attempted connection. If authorization fails, the connection is dropped.
  - For ASA, PIX, and FWSM devices, you define authorization rules directly in the AAA rules policy; if you require authorization for traffic that does not also require authentication, the unauthenticated traffic is always dropped. If you use RADIUS servers for authentication, authorization is automatically performed and authorization rules are not necessary. If you configure authorization rules, you must use a TACACS+ server.
  - For IOS devices, to configure authorization, you must configure an authorization server group in the **Firewall > Settings > AAA** policy; authorization is done for any traffic that is subject to authentication. You can use TACACS+ or RADIUS servers.

- Accounting—You can define accounting rules even if you do not configure authentication or authorization. If you do configure authentication, accounting records are created for each user, so that you can identify the specific user who made the connection. Without user authentication, accounting records are based on IP address. You can use TACACS+ or RADIUS servers for accounting.
  - For ASA, PIX, and FWSM devices, you define accounting rules directly in the AAA rules policy. You can perform accounting for any TCP or UDP protocol.
  - For IOS devices, to configure accounting, you must configure an accounting server group in the **Firewall > Settings > AAA** policy; accounting is done for any traffic that is subject to authentication.

Understanding How Users Authenticate

When you create AAA rules to require that users authenticate when trying to make connections through a device, users will be prompted to supply credentials: a username and password. These credentials must be defined in a AAA server or in the local database configured on the device.

Users are prompted only for HTTP, HTTPS, FTP, and Telnet connections (if you configure those protocols to require authentication). For ASA, PIX, and FWSM devices, you can also require authentication for other protocols; however, users are not prompted for them, and so they must first attempt one of the four supported protocols and successfully authenticate before completing connections of any other protocol that requires authentication.

Tip For ASA, PIX, and FWSM devices, if you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can require that the user authenticate with the security appliance directly using HTTP or HTTPS by configuring the interface to use interactive authentication (using the **Firewall > Settings > AAA Firewall** policy). The user would then authenticate with the appliance before trying other connections, using one of the following URLs, where *interface_ip* is the IP address of the interface and *port* is optionally the port number, if you specify a non-default port for the protocol in the interactive authentication table:
http://*interface_ip*[**:***port*]**/netaccess/connstatus.html** or
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**.

When attempting a connection through the device, the user is prompted based on the protocol:

- HTTP—The device prompts the user with a web page to provide username and password. The user is prompted repeatedly until successfully authorized. After the user authenticates correctly, the device redirects the user to the original destination. If the destination server also has its own authentication, the user enters another username and password.

  For ASA, PIX, and FWSM devices, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can improve the user experience by configuring the interface for interactive authentication and specifying redirect for HTTP traffic. This redirects the user to a web page hosted on the appliance for authentication. To configure an interface to use interactive authentication, add the interface to the Interactive Authentication table on the **Firewall > Settings > AAA Firewall** policy (see AAA Firewall Settings Page, Advanced Setting Tab, page 15-20). Ensure that you select the HTTP and Redirect options when adding the interface.

  You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if 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.

  However, when using basic HTTP authentication, if the user is going to an HTTP server that requires authentication, the same username and password used to authenticate with the appliance is sent to the HTTP server. Thus, login to the HTTP server fails unless the same username and password are used by the ASA and HTTP server. To avoid this problem, you must configure a virtual HTTP server on the ASA. You can configure a virtual HTTP server using the **Firewall > Settings > AAA Firewall** policy (see AAA Firewall Settings Page, Advanced Setting Tab, page 15-20).

Tip In HTTP authentication, the username and password are transmitted in clear text. You can prevent this by selecting the **Use Secure HTTP Authentication** option on the **Firewall > Settings > AAA Firewall** policy. This option ensures that credentials are encrypted.

- HTTPS—The user experience for HTTPS is the same as for HTTP; the user is prompted until successfully authorized, and then redirected to the original destination.

For ASA, PIX, and FWSM devices, the security appliance uses a custom login screen. Like with HTTP, you can configure the interface to use interactive authentication, in which case HTTPS connections use the same authentication page as HTTP connections. You must configure the interface separately for HTTPS redirection; use the **Firewall > Settings > AAA Firewall** policy.

For IOS devices, HTTPS connections are authenticated only if you enable SSL on the device and your AAA rules require HTTP authentication proxy. This configuration is explained in Configuring AAA Rules for IOS Devices, page 15-7.

- FTP—The device prompts once for authentication. If authentication fails, the user must retry the connection.

  When prompted, the user can enter the username required for device authentication followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user would then enter the device authentication password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

  name> asa1@partreq
  password> letmein@he110

  For IOS devices, this method of entering both the device and FTP credentials is required. For ASA, PIX, and FWSM devices, this feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

- Telnet—The device prompts several times for authentication. After a number of failed attempts, the user must retry the connection. After authentication, the Telnet server prompts for its username/password. You can configure a virtual Telnet server using the **Firewall > Settings > AAA Firewall** policy (see AAA Firewall Settings Page, Advanced Setting Tab, page 15-20).

Configuring AAA Rules for ASA, PIX, and FWSM Devices

When you configure AAA rules for an ASA, PIX, or FWSM device, you are configuring policies that define who is allowed to make HTTP, HTTPS, FTP, and Telnet connections through (not to) the device. To fully configure network access authentication, you need to configure several policies, not just the AAA rules policy.

The following procedure covers all policies you would need to configure to supply full authentication, authorization, and accounting support for network access authentication. You do not need to configure options for features you do not need.

Related Topics

- Understanding AAA Rules, page 15-1
- Understanding How Users Authenticate, page 15-2
- Creating a New Shared Policy, page 5-54
- Modifying Policy Assignments in Policy View, page 5-54
- Understanding Networks/Hosts Objects, page 6-79
- Understanding Interface Role Objects, page 6-72
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Understanding AAA Server and Server Group Objects, page 6-27
- Understanding Interface Role Objects, page 6-72

Step 1 Do one of the following to open the AAA Rules Page, page 15-10:

- (Device view) Select **Firewall > AAA Rules** from the Policy selector.
- (Policy view) Select **Firewall > AAA Rules** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the row after which you want to create the rule and click the **Add Row** button or right-click and select **Add Row**. This opens the Add and Edit AAA Rule Dialog Boxes, page 15-13.

Tip If you do not select a row, the new rule is added at the end of the local scope. You can also select an existing row and edit either the entire row or specific cells. For more information, see Editing Rules, page 12-10.

Step 3 Configure the rule. Following are the highlights of what you typically need to decide. For specific information on configuring the fields, see Add and Edit AAA Rule Dialog Boxes, page 15-13.

- Authentication (with or without User-Identity), Authorization, or Accounting Action—Select the options applicable for this rule. Authentication prompts the user for a username and password when attempting HTTP, HTTPS, FTP, or Telnet access. Authorization is an additional level, where after the user authenticates, the AAA server is checked to ensure that the user is authorized for that type of access. Accounting generates usage records in the AAA server and can be used for billing, security, or resource allocation purposes. You can generate accounting information for any TCP or UDP traffic.

  When you select Authentication, you can also select User-Identity (ASA 8.4(2+) only). This option indicates that the ASA should use the Active Directory servers configured in the identity-firewall domain mappings to authenticate users (see Identifying Active Directory Servers and Agents, page 13-8). If the user enters a domain name, the AD server associated with the domain is queried. Otherwise, the AD server associated with the default domain is queried. When you select User-Identity, and you do not select Authorization or Accounting, do not specify a AAA server group.
- Permit or Deny—Whether you are subjecting the identified traffic to AAA control (permit) or you are exempting it from AAA control (deny). Any denied traffic is not prompted for authentication and is allowed to pass unauthenticated, although your access rules might drop the traffic.
- Source and Destination addresses—If the rule should apply no matter which addresses generated the traffic or their destinations, use “All-Addresses” as the source or destination. If the rule is specific to a host or network, enter the addresses or network/host objects. For information on the accepted address formats, see Specifying IP Addresses During Policy Definition, page 6-87.
- Source and Destination Security Groups (ASA 9.0+ only)—You can specify TrustSec security groups used to filter traffic in addition to the source and destination addresses. See Selecting Security Groups in Policies, page 14-16, Configuring TrustSec-Based Firewall Rules, page 14-17 and Creating Security Group Objects, page 14-14 for more information about security groups.
- Source Users (ASA 8.4.2+ only)—You can further define the traffic source by specifying Active Directory (AD) user names (in the format NetBIOS_DOMAIN\username), user groups (NetBIOS_DOMAIN\\user_group), or identity user group objects that define the names and groups. The user specification is conjoined to the source address to limit the match to user addresses within the source address range. For more information, see Configuring Identity-Based Firewall Rules, page 13-21 and Creating Identity User Group Objects, page 13-19.
- Services—You can specify any type of service for authentication and authorization rules; however, the user is prompted to authenticate only for HTTP, HTTPS, FTP, and Telnet connections. Thus, if you specify something other than these services, the user must first attempt one of these connections

and successfully authenticate (and be authorized, if you include that action) before any other types of connections are allowed. For accounting rules, you can specify any TCP or UDP service (or simply TCP and UDP themselves), if you want to account for all types of traffic.

- AAA Server Group—The AAA server group policy object to be used for authentication, authorization, or accounting. If the rule applies more than one of these actions, the server group must support all selected actions. For example, only TACACS+ servers can provide services for authorization rules (although using RADIUS for authentication rules automatically includes RADIUS authorization), and only TACACS+ and RADIUS servers can provide accounting services. If you want to use different server groups for particular actions, define separate rules for each type of action that requires different groups.
- Interfaces—The interface or interface role for which you are configuring the rule.

Click **OK** when you are finished defining your rule.

Step 4 If you did not select the right row before adding the rule, select the new rule and use the up and down arrow buttons to position the rule appropriately. For more information, see Moving Rules and the Importance of Rule Order, page 12-19.

Step 5 Select **Firewall > Settings > AAA Firewall** (in Device or Policy view) to open the AAA Firewall Settings Page, Advanced Setting Tab, page 15-20. Configure the AAA firewall settings:

- If you configured rules for HTTP authentication, you should select **Use Secure HTTP Authentication**. This ensures that the username and password entered for HTTP authentication are encrypted. If you do not select this option, the credentials are sent in clear text, which is insecure.

Tip If you select this option, ensure that you do not configure 0 for the user authentication timeout (**timeout uauth 0**, configured in the **Platform > Security > Timeouts** policy), or users might be repeatedly prompted for authentication, making the feature disruptive to your network.

- If you configured authentication for HTTP or HTTPS traffic on an interface, you should consider adding the interface to the Interactive Authentication table. When you enable an interface for interactive authentication, users get an improved authorization web page, one that is the same for both HTTP and HTTPS.

  Click **Add Row** to add the interface to the table. Select whether the interface should listen for HTTP or HTTPS traffic (add the interface twice to listen for both protocols), and the port to listen on if not the default port for the protocol (80 and 443, respectively). Select **Redirect network users for authentication request** so that network access traffic gets the improved authentication prompt; if you do not select the option, only users trying to log into the device get the prompt.

Note You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if 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.

- For FWSM devices, you can also disable the authentication challenge for protocols you have otherwise configured to require authentication. You can also add interfaces to the Clear Connections table to ensure that active connections for users whose authentication has timed out are cleared and do not hang.

- If you want to exempt some devices from your AAA rules based on their media access control (MAC) address, click the **MAC Exempt List** tab to open the AAA Firewall Page, MAC-Exempt List Tab, page 15-26. Enter a name for the exemption list, and then click the **Add Row** button and fill in the Firewall AAA MAC Exempt Setting Dialog Box, page 15-27 to add the MAC address to the table with a permit rule. You might want to do this for secure, trusted devices.

  The order of entries matters, so ensure that any specific entries that are covered by broader entries come before the broad entries in the table. The device processes the list in order and the first match is applied to the host. For more detailed information about how the entries on the MAC exempt list are processed, see AAA Firewall Page, MAC-Exempt List Tab, page 15-26.

Step 6 If you are configuring authentication rules using a RADIUS server, and you include per-user ACL configurations in the user profiles, enable per-user downloadable ACLs on the interface. (RADIUS authentication automatically includes authorization checking.) For information on configuring per-user ACLs, see the information on configuring RADIUS authorization in the *Cisco ASA 5500 Series Configuration Guide Using the CLI* at http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_fwaaa.html.

a. Select **Firewall > Settings > Access Control** (in Device or Policy view) to open the Access Control Settings Page, page 16-24.

b. Click the Add Row button beneath the interface table and fill in the Firewall ACL Setting Dialog Box, page 16-26 with at least these options:

   - Enter the interface or interface role on which you are performing authorization.
   - Select **Per User Downloadable ACLs**.

c. Click **OK** to save your changes.

Configuring AAA Rules for IOS Devices

When you configure AAA rules for an IOS device, you are configuring authentication proxy (AuthProxy) admission control policies. These policies define who is allowed to make HTTP, HTTPS, FTP, and Telnet connections through (not to) the device. To fully configure authentication proxy, you must configure several policies, not just the AAA rules policy.

The following procedure covers all policies you would need to configure to supply full authentication, authorization, and accounting support for authorization proxy. You do not need to configure options for features you do not need.

Related Topics

- Understanding AAA Rules, page 15-1
- Understanding How Users Authenticate, page 15-2
- Creating a New Shared Policy, page 5-54
- Modifying Policy Assignments in Policy View, page 5-54
- Understanding Networks/Hosts Objects, page 6-79
- Understanding Interface Role Objects, page 6-72
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Understanding AAA Server and Server Group Objects, page 6-27
- Understanding Interface Role Objects, page 6-72

Step 1 Do one of the following to open the AAA Rules Page, page 15-10:

- (Device view) Select **Firewall > AAA Rules** from the Policy selector.
- (Policy view) Select **Firewall > AAA Rules** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the row after which you want to create the rule and click the **Add Row** button or right-click and select **Add Row**. This opens the Add and Edit AAA Rule Dialog Boxes, page 15-13.

Tip If you do not select a row, the new rule is added at the end of the local scope. You can also select an existing row and edit either the entire row or specific cells. For more information, see Editing Rules, page 12-10.

Step 3 Configure the rule. Following are the highlights of what you typically need to decide. For specific information on configuring the fields, see Add and Edit AAA Rule Dialog Boxes, page 15-13.

- **Authentication Action**—Select this option. Authentication rules are the only type of rule you can configure in the AAA rules policy for IOS devices.
- Permit or Deny—Whether you are subjecting the identified traffic to AAA control (permit) or you are exempting it from AAA control (deny). Any denied traffic is not prompted for authentication and is allowed to pass unauthenticated, although your access rules might drop the traffic.
- Source and Destination addresses—If the rule should apply no matter which addresses generated the traffic or their destinations, use “All-Addresses” as the source or destination. If the rule is specific to a host or network, enter the addresses or network/host objects. For information on the accepted address formats, see Specifying IP Addresses During Policy Definition, page 6-87.
- Source and Destination Security Groups (ASA 9.0+ only)—You can specify TrustSec security groups used to filter traffic in addition to the source and destination addresses. See Selecting Security Groups in Policies, page 14-16, Configuring TrustSec-Based Firewall Rules, page 14-17 and Creating Security Group Objects, page 14-14 for more information about security groups.
- Source Users (ASA 8.4.2+ only)—You can further define the traffic source by specifying Active Directory (AD) user names (in the format NetBIOS_DOMAIN\username), user groups (NetBIOS_DOMAIN\\user_group), or identity user group objects that define the names and groups. The user specification is conjoined to the source address to limit the match to user addresses within the source address range. For more information, see Configuring Identity-Based Firewall Rules, page 13-21 and Creating Identity User Group Objects, page 13-19.
- Services—You can specify any type of service for authentication and authorization rules; however, the user is prompted to authenticate only for HTTP, HTTPS, FTP, and Telnet connections. Thus, if you specify something other than these services, the user must first attempt one of these connections and successfully authenticate (and be authorized, if you include that action) before any other types of connections are allowed. For accounting rules, you can specify any TCP or UDP service (or simply TCP and UDP themselves), if you want to account for all types of traffic.
- Interfaces—The interface or interface role for which you are configuring the rule.
- Service triggering the authentication proxy—Select the checkboxes for the type of traffic you want to trigger user authentication: HTTP, FTP, or Telnet. You can select any combination. If you want to trigger the proxy for HTTPS support, select HTTP and perform the HTTPS configuration that is explained in a subsequent step in this procedure.

Click **OK** when you are finished defining your rule.

Step 4 If you did not select the right row before adding the rule, select the new rule and use the up and down arrow buttons to position the rule appropriately. For more information, see Moving Rules and the Importance of Rule Order, page 12-19.

Step 5 Select **Firewall > Settings > AuthProxy** (in Device or Policy view) to open the AAA Page, page 15-28. Configure the authentication proxy settings:

- **Authorization server groups**—If you want all of your authentication rules to also perform user authorization, specify the list of AAA server group policy objects that identify the TACACS+ or RADIUS servers that control authorization. You can also specify LOCAL to use the user database defined on the device. If you do not specify a server group, authorization is not performed.

Tip You must configure per-user ACLs in your AAA server to define the privileges you want to apply to each user. When configuring authorization, specify **auth-proxy** as the service (e.g. service = auth-proxy), with a privilege level of 15. For more information on configuring the AAA server, including information on configuring authentication proxy in general, see the "Configuring the Authentication Proxy" section in the *Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T* at http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy_ps6441_TSD_Products_Configuration_Guide_Chapter.html.

- **Accounting server groups**—If you want to perform accounting for all of your authentication rules, specify the list of AAA server group policy objects that identify the TACACS+ or RADIUS servers that perform accounting. If you do not specify a server group, no accounting is performed. When performing accounting, also configure the following options as appropriate:
  - If you specify more than one server group, consider selecting **Use Broadcast for Accounting**. This option sends accounting records to the primary server in each server group.
  - The **Accounting Notice** option defines when the server is notified. The default is to notify the server at the start and stop of a connection, but you can select to only send stop notices (or none at all).
- You can also customize authentication banners for each service, and on the Timeout tab, you can change the default idle and absolute session timeouts globally or for each interface.

Step 6 Select **Platform > Device Admin > AAA** (in policy view, this is in the Router Platform folder) to open the AAA Policy Page, page 62-6. Configure these options on the Authentication tab:

- Select **Enable Device Login Authentication**.
- Enter the list of server groups that will control authentication in priority order. Typically, you will use at least some of the same LDAP, RADIUS, or TACACS+ server groups used in the AuthProxy policy. However, this policy also defines device login control, so you might want to include some other server groups. For more information, see AAA Page—Authentication Tab, page 62-6.

Step 7 If you are using the authentication proxy with HTTP connections, and you also want to use the proxy with HTTPS connections, select **Platform > Device Admin > Device Access > HTTP** (in policy view, this is in the Router Platform folder) to open the HTTP Policy Page, page 62-31. Configure these options:

- Select **Enable HTTP** and **Enable SSL** if they are not already selected.
- On the AAA tab, ensure that the configuration for login access to the device is appropriate. If you are using AAA to control access through the device, you might want to use it for access to the device.

AAA Rules Page

Use the AAA Rules page to configure AAA rules for device interfaces. AAA rules configure network access control (called authentication proxy on IOS devices), which forces the user to authenticate when attempting network connections that traverse the device. Authenticated traffic can also be required to undergo authorization (where after the user enters a valid user name and password, the AAA server is checked to verify that the user is authorized for network access). You can also configure accounting rules, even for unauthenticated traffic, to provide information you can use for billing, security, and resource allocation purposes.

Note With the release of Security Manager 4.4 and versions 9.0 and higher of the ASA, the separate policies and objects for configuring IPv4 and IPv6 AAA rules were "unified," meaning one set of AAA rules in which you can use either IPv4 or IPv6 addresses, or a mixture of both. (See Policy Object Changes in Security Manager 4.4, page 1-10 for additional information.) In Policy view, IPv4 and unified versions of the AAA policy type are provided. In addition, a utility that you can use to convert existing IPv4 policies is provided (see Converting IPv4 Rules to Unified Rules, page 12-28). The following descriptions apply to all versions of the AAA rule table, except where noted.

If you assign an IPv4 AAA-rule shared policy to a 9.0+ device, you will no longer be able to assign unified versions of those policies to that device. Likewise, if you assign a unified AAA-rule shared policy to a 9.0+ device, you will no longer be able to assign IPv4 versions of those shared policies to that device--the device will not be included in the list of available devices on the Assignments tab for the shared policy.

AAA rule configuration is complex and differs significantly based on the operating system. Carefully read the following topics before configuring AAA rules:

- Understanding AAA Rules, page 15-1
- Understanding How Users Authenticate, page 15-2
- Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4
- Configuring AAA Rules for IOS Devices, page 15-7

Tip Disabled rules are shown with hash marks covering the table row. When you deploy the configuration, disabled rules are removed from the device. For more information, see Enabling and Disabling Rules, page 12-20.

Navigation Path

To access the AAA Rules page, do one of the following:

- (Device view) Select a device, then select **Firewall > AAA Rules** from the Policy selector.
- (Policy view) Select **Firewall > AAA Rules** from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click a device and select **Edit Firewall Policies > AAA Rules**.

Related Topics.

- Adding and Removing Rules, page 12-9
- Editing Rules, page 12-10
- Moving Rules and the Importance of Rule Order, page 12-19

- Using Sections to Organize Rules Tables, page 12-20
- Using Rules Tables, page 12-7
- Filtering Tables, page 1-48

Field Reference

Table 15-1 AAA Rules Page

Element	Description
Expand all rows/Collapse all rows	Use these buttons to expand or collapse all sections in the rules table. **Note** The buttons are located in the upper-right corner of the Filter area above the access rules table.
Conflict Indicator icons	Identifies conflicts and provides a quick visual representation of the type of conflict. For more details, including types of conflicts and the actions you can take from this column, see Understanding the Automatic Conflict Detection User Interface, page 16-30.
No.	The ordered rule number.
Permit	Whether the defined traffic will be subject to the rule (Permit) or exempted from the rule (Deny): • Permit—Shown as a green check mark. • Deny—Shown as a red circle with slash.
Sources	The sources of traffic for this rule; can be networks, security groups (ASA 9.0+ only), and users. Multiple entries are displayed on separate lines within the table cell.
Destinations	The destinations for this rule; can be networks and security groups (ASA 9.0+ only). Multiple entries are displayed on separate lines within the table cell.
Service	The services or service objects that specify the protocol and port of the traffic to which the rule applies. Multiple entries are displayed on separate lines within the table cell. See Understanding and Specifying Services and Service and Port List Objects, page 6-100.
Interface	The interfaces or interface roles to which the rule is assigned. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. Multiple entries are displayed as separate subfields within the table cell. See Understanding Interface Role Objects, page 6-72.

Table 15-1 AAA Rules Page (Continued)

Element	Description
Action	The type of AAA control defined by this rule: • Authenticate—Users making connections through the device must authenticate with their username and password. Protocols requiring authentication are defined by the Service field (for ASA/PIX/FWSM devices) or the AuthProxy methods (for IOS devices). • Authorize—Authenticated users are also checked with the AAA server to ensure that they are authorized to make the connection (ASA/PIX/FWSM only). • Account—Accounting records for the identified traffic are sent to the AAA server (ASA/PIX/FWSM only). You can right-click the Action cell in an existing AAA rule and choose Edit Action to change your selections. See Edit AAA Option Dialog Box, page 15-19 for more information.
AAA Method (IOS) (not presented for ASA 9.0+ devices)	The authentication method for this rule: Web Authorization Proxy (Auth-Proxy), HTTP Basic, or Windows NT LAN Manager (NTLM)
AuthProxy	The protocols that require authentication using the authentication proxy method. This applies only to IOS devices. You can right-click the AuthProxy cell in an existing AAA rule and choose Edit AuthProxy to change your selections. See AuthProxy Dialog Box, page 15-19 for more information.
Server Group	The AAA server group that provides the authentication, authorization, or accounting support defined in the rule. This group is used for ASA/PIX/FWSM devices only. For information on configuring AAA servers for IOS devices for use with these rules, see Configuring AAA Rules for IOS Devices, page 15-7. You can right-click the Server Group cell in an existing AAA rule and choose Edit Server Group to change your selections. See Edit Server Group Dialog Box, page 15-19 for more information.
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Description	The description of the rule, if any.
Last Ticket(s)	Shows the ticket(s) associated with last modification to the rule. You can click the ticket ID in the Last Ticket(s) column to view details of the ticket and to navigate to the ticket. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page, page 11-71).
Page elements below the rules table	
Query	Click this button to run a policy query, which can help you evaluate your rules and identify ineffective rules. See Generating Policy Query Reports, page 12-28

Table 15-1 AAA Rules Page (Continued)

Element	Description
Find and Replace button (binoculars icon)	Click this button to search for various types of items within the table and to optionally replace them. See Finding and Replacing Items in Rules Tables, page 12-16.
Up Row and Down Row buttons (arrow icons)	Click these buttons to move the selected rules up or down within a scope or section. For more information, see Moving Rules and the Importance of Rule Order, page 12-19.
Add Row button	Click this button to add a rule to the table after the selected row using the Add and Edit AAA Rule Dialog Boxes, page 15-13. If you do not select a row, the rule is added at the end of the local scope. For more information about adding rules, see Adding and Removing Rules, page 12-9.
Edit Row button	Click this button to edit the selected rule. You can also edit individual cells. For more information, see Editing Rules, page 12-10.
Delete Row button	Click this button to delete the selected rule.

Right-click Menu

A right-click menu is also available. This menu provides access to many of the functions listed above; the options presented depend on the location right-clicked:

- If you right-click a rule in the table, the options may include editing functions relative to the specific table cell right-clicked. For example, the command “Edit Server Group” is included when you right-click a Server Group cell. See Editing Rules, page 12-10 for more information.
- The Combine Rules option is also included in the right-click menu. See Combining Rules, page 12-22 for more information.

Add and Edit AAA Rule Dialog Boxes

Use the Add and Edit AAA Rules dialog boxes to add and edit AAA rules. AAA rule configuration is more complex than just filling in this dialog box, and differs significantly based on the operating system. Carefully read the following topics before configuring AAA rules:

- Understanding AAA Rules, page 15-1
- Understanding How Users Authenticate, page 15-2
- Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4
- Configuring AAA Rules for IOS Devices, page 15-7

Navigation Path

From the AAA Rules Page, page 15-10, click the **Add Row** button or select a row and click the **Edit Row** button.

Related Topics

- Adding and Removing Rules, page 12-9
- Editing Rules, page 12-10

Field Reference

Table 15-2 Add and Edit AAA Rules Dialog Boxes

Element	Description
Enable Rule	Whether to enable the rule, which means the rule becomes active when you deploy the configuration to the device. Disabled rules are shown overlain with hash marks in the rule table. For more information, see Enabling and Disabling Rules, page 12-20.
Action (Permit/Deny)	Whether the defined traffic will be subject to the rule (Permit) or exempted from the rule (Deny). For example, if you create an authentication deny rule for the 10.100.10.0/24 network to any destination using the HTTP service, users on this network are not prompted to authenticate with the device when making HTTP requests.

Table 15-2 Add and Edit AAA Rules Dialog Boxes (Continued)

Element	Description
Sources	Provide traffic sources for this rule; can be networks, security groups, and users. You can enter values or object names, or Select objects, for one or more of the following types of sources: • Network – You can specify a various network, host and interface definitions, either individually or as objects. If you Select an interface object as a source, the dialog box displays tabs to differentiate between hosts/networks and interfaces. The "All-Address" objects do not restrict the rule to specific hosts, networks, or interfaces. These addresses are IPv4 or IPv6 addresses for hosts or networks, network/host objects, interfaces, or interface roles. **Note** You can only specify a fully qualified domain name (FQDN) by providing an FQDN network/host object, or a group object that includes an FQDN object. You cannot directly type in an FQDN. See Understanding Networks/Hosts Objects, page 6-79, Specifying IP Addresses During Policy Definition, page 6-87 and Understanding Interface Role Objects, page 6-72 for additional information about these definitions. • Security Groups (ASA 9.0+) – Enter or Select the name or tag number for one or more source security groups for the rule, if any. See Selecting Security Groups in Policies, page 14-16, Configuring TrustSec-Based Firewall Rules, page 14-17 and Creating Security Group Objects, page 14-14 for more information about security groups. • Users – Enter or Select the Active Directory (AD) user names, user groups, or identity user group objects for the rule, if any. You can enter any combination of the following: – Individual user names: NetBIOS_DOMAIN\username – User groups (note the double \): NetBIOS_DOMAIN\\user_group – Identity user group object names. For more information, see: – Selecting Identity Users in Policies, page 13-21 – Configuring Identity-Based Firewall Rules, page 13-21 – Creating Identity User Group Objects, page 13-19 **Note** Enter more than one value in any of these fields by separating the items with commas. Each specification is combined with any others to limit traffic matches to only those flows that include all definitions. For example, specified user traffic originating from within a specified source address range.

Table 15-2 Add and Edit AAA Rules Dialog Boxes (Continued)

Element	Description
Destinations	Provide traffic destinations for this rule; can be networks or security groups. As with Sources, you can enter values or object names, or Select objects, for one or more destinations of Network and Security Group (ASA 9.0+) type.
Services	The services that define the type of traffic upon which to act. You can enter or Select any combination of service objects and service types (which are typically a protocol and port combination). Enter more than one value by separating the items with commas. It is important that you select the service type carefully based on the device type: • For IOS devices, only the protocols you select with the authorization proxy check boxes at the bottom of the dialog box are used for AAA control, so you can use IP as the protocol. • For ASA, PIX, and FWSM devices, although you can force authentication for any type of traffic, the security appliance prompts only for HTTP/HTTPS, FTP, and Telnet traffic. If you specify a service other than one of these, users are prevented from making any connection through the appliance until they try one of these services and successfully authenticate. If the rule is only for accounting, you can specify any TCP or UDP protocols for which you want to create records. For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects, page 6-100. **Note** Due to an issue in PIX 6.3 and FWSM devices, if you specify a service with a source port, no traffic is authenticated. Therefore, source ports are ignored when the CLI is generated from your rule for these device types.
Interface	The interface or interface role object that identifies the interface from which to authenticate, authorize, or account users. Enter the name of the interface or interface role, or click **Select** to select it from a list or to create a new interface role object. For authentication rules on ASA and PIX devices, you can modify how this interface authenticates HTTP/HTTPS traffic by using the **Firewall > Settings > AAA Firewall** policy. Configuring the interface as an HTTP/HTTPS listening port can improve the authentication experience for users. For more information, see Understanding How Users Authenticate, page 15-2 and AAA Firewall Settings Page, Advanced Setting Tab, page 15-20.
Description	An optional description of the rule (up to 1024 characters).

Table 15-2 Add and Edit AAA Rules Dialog Boxes (Continued)

Element	Description
The Authentication Action, Authorization Action, and Accounting Action check boxes define the types of rules that will be generated on the device. Each type generates a separate set of commands, but if you select more than one option, your other selections in this dialog box are limited to those supported by all selected actions. You can right-click the Action cell in an existing AAA rule and choose Edit Action to change your selections. See Edit AAA Option Dialog Box, page 15-19 for more information.	
Authentication Action User-Identity	• Authentication—Users must supply a user name and password to make a connection through the device. For ASA, PIX, and FWSM devices, what you enter in the Services field determines which protocols require authentication, although the device will prompt only for HTTP, HTTPS, FTP, and Telnet connections. For IOS devices, the protocols that require authentication are based on the authorization proxy check boxes you select at the bottom of the dialog box. – User-Identity (ASA 8.4(2+) only.)—For ASA devices, when you select Authentication Action, you also have the option to select User-Identity. This option indicates that the device should use the identity-firewall domain mappings defined in the Identity Options policy to authenticate users instead of the AAA Server Group setting in the AAA rule. If the user enters a domain name, the AD server associated with the domain is queried. Otherwise, the AD server associated with the default domain is queried. See Identifying Active Directory Servers and Agents, page 13-8.
Authorization Action (PIX/ASA/FWSM)	Authorization—After successful authentication, the AAA server is also checked to determine if the user is authorized to make the requested connection. If you specify a RADIUS server for authentication rules, authorization happens without you having to configure authorization rules. If you are using a TACACS+ server, you must create separate authorization rules.
Accounting Action (PIX/ASA/FWSM)	Accounting—Accounting records will be sent to the TACACS+ or RADIUS server for the TCP and UDP protocols specified in the Services field. If you also configure authentication, these records are per-user; otherwise, they are based on IP address. For IOS devices, accounting is configured in the **Firewall > Settings >ScanSafe Web Security** policy, not in AAA rules, and applies only to the protocols you select for authentication proxy.

Table 15-2 Add and Edit AAA Rules Dialog Boxes (Continued)

Element	Description
AAA Server Group (PIX, ASA, FWSM)	The AAA server group policy object that defines the AAA server that should provide authentication, authorization, or accounting for the traffic defined in the rule. Enter the name of the policy object or click **Select** to select it from a list or to create a new object. You must select a type of server that can perform all actions defined in the rule. For example, the local database (defined on the device) cannot provide authorization services. If you use a RADIUS server for authentication, it automatically provides authorization services, but you cannot define an authorization rule that uses a RADIUS server. You can use a mix of server groups for different actions for the same source/destination pair by creating separate rules for the desired combination of authentication, authorization, and accounting actions. For more information on AAA server group objects, see Understanding AAA Server and Server Group Objects, page 6-27. **Tips** • If you select Authenticate Action and User-Identity, but not the Authorization or Accounting actions, any server you specify here is ignored. Do not select a server to avoid validation warnings. • AAA server groups for IOS devices are defined in other policies. For a complete explanation of the configuration, see Configuring AAA Rules for IOS Devices, page 15-7. • You can right-click the Server Group cell in an existing AAA rule and choose Edit Server Group to change your selections. See Edit Server Group Dialog Box, page 15-19 for more information.
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Method (IOS) (not presented for ASA 9.0+ devices)	Choose Auth-Proxy, HTTP-basic, or NTLM. If you choose Auth-Proxy, the following options are available: • HTTP • FTP • Telnet Specify the protocols for which you want to enforce authentication using the authentication proxy. If you select HTTP, you can also configure HTTPS authentication proxy by enabling SSL on the device. For specific information, see Configuring AAA Rules for IOS Devices, page 15-7. You can right-click the AuthProxy cell in an existing AAA rule and choose Edit AuthProxy to change your selections. See AuthProxy Dialog Box, page 15-19 for more information.

Edit AAA Option Dialog Box

Use the Edit AAA Option dialog box to select whether the rule performs authentication (with or without user identity), authorization, or accounting. Authorization and accounting rules work only on ASA, PIX, and FWSM devices. For a complete explanation of these options, see the related explanations in the following topics:

- Add and Edit AAA Rule Dialog Boxes, page 15-13
- Understanding AAA Rules, page 15-1

Navigation Path

Right-click the Action cell in a AAA rule (on the AAA Rules Page, page 15-10) and select **Edit AAA**.

AuthProxy Dialog Box

Use the AuthProxy dialog box to edit the authorization proxy settings in a AAA rule. For IOS devices, select the protocols (HTTP, FTP, or Telnet) for which you want to enforce authentication using the authentication proxy. If you select HTTP, you can also configure HTTPS authentication proxy by enabling SSL on the device. For specific information, see Configuring AAA Rules for IOS Devices, page 15-7.

Navigation Path

Right-click the AuthProxy cell in a AAA rule (on the AAA Rules Page, page 15-10) and select **Edit AuthProxy**.

Edit Server Group Dialog Box

Use the Edit Server Group dialog box to edit the AAA server group used in a AAA rule, which defines the AAA server that should provide authentication, authorization, or accounting for the traffic defined in the rule. Enter the name of the policy object or click **Select** to select it from a list or to create a new object. For more information on AAA server group objects, see Understanding AAA Server and Server Group Objects, page 6-27.

You must select a type of server that can perform all actions defined in the rule. For example, the local database (defined on the device) cannot provide authorization services. If you use a RADIUS server for authentication, it automatically provides authorization services, but you cannot define an authorization rule that uses a RADIUS server. Unlike the Add and Edit AAA Rule Dialog Boxes, page 15-13, this dialog box does not validate your selection.

Note This setting applies only to ASA, PIX, and FWSM devices. AAA server groups for IOS devices are defined in other policies. For a complete explanation of the configuration, see Configuring AAA Rules for IOS Devices, page 15-7.

Navigation Path

Right-click the Server Group cell in a AAA rule (on the AAA Rules Page, page 15-10) and select **Edit Server Group**.

AAA Firewall Settings Policies

The AAA firewall settings policy configurations influence the behavior of your AAA rules.

This section contains the following topics:

AAA Firewall Settings Page, Advanced Setting Tab

Use the AAA Firewall settings policy to configure optional settings to refine how your AAA rules policy behaves. This topic describes the settings available on the Advanced Setting tab; for information on the MAC Exempt List tab, see AAA Firewall Page, MAC-Exempt List Tab, page 15-26.

Navigation Path

To access the AAA Firewall settings page, do one of the following:

- (Device view) Select an ASA, PIX, or FWSM device, select **Firewall > Settings > AAA Firewall**; select the **Advanced Setting** tab if necessary.
- (Policy view) Select **Firewall > Settings > AAA Firewall** from the Policy Type selector. Create a new policy or select and existing one, then select the **Advanced Setting** tab if necessary.
- (Map view) Right-click an ASA, PIX, or FWSM device and select **Edit Firewall Settings > AAA Firewall**, then select the **Advanced Setting** tab if necessary.

Related Topics

- Understanding AAA Rules, page 15-1
- Understanding How Users Authenticate, page 15-2
- Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4

Field Reference

Table 15-3 Advanced Setting Tab, AAA Firewall Settings Page

Element	Description
Use Secure HTTP Authentication	Whether to require users making HTTP requests that traverse the security appliance to first authenticate with the security appliance using SSL (HTTPS). The user is prompted for username and password. Secure HTTP authentication offers a secure method for user authentication to the security appliance prior to allowing HTTP-based web requests to traverse the security appliance. This is also called HTTP cut-through proxy authentication. If you select this option, ensure that your access rules do not block HTTPS traffic (port 443), and that any PAT configuration also includes port 443. Also, be aware that a maximum of 16 concurrent authentications are allowed, and that if you configure 0 for the user authentication timeout (**timeout uauth 0**, configured in the **Platform > Security > Timeouts** policy) users might be repeatedly prompted for authentication, making the feature disruptive to your network. **Tip** If you do not select this option, HTTP authentication sends the username and password in clear text.
Enable Proxy Limit Maximum Concurrent Proxy Limit per User	Whether to allow proxy connections. If you enable proxies, you must set a limit on the number of proxy connections allowed for each user, from 1 to 128. The device default is 16, but you must specify a number.

Table 15-3 Advanced Setting Tab, AAA Firewall Settings Page (Continued)

Element	Description
Enable Virtual HTTP	Whether to configure a virtual HTTP server. This feature redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the ASA. The ASA prompts for the AAA server username and password. After the AAA server authenticates the user, the ASA 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. For more information, see Understanding How Users Authenticate, page 15-2. For inbound users (from lower security to higher security), 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). 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 HTTP address. A static NAT rule is not required. To configure a virtual HTTP server: 1. Select the Enable Virtual HTTP check box. 2. Enter the IP address or select a Networks/Hosts object representing the virtual HTTP server. Make sure this address is an unused address that is routed to the ASA. 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. 3. (Optional) If you are using text-based browsers, where redirection does not happen automatically, select the Warning check box. This enables an alert to notify users when the HTTP connection is being redirected.

Table 15-3 Advanced Setting Tab, AAA Firewall Settings Page (Continued)

Element	Description
Enable Virtual Telnet	Whether to configure a virtual Telnet server. When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. After the user is authenticated, the message "Authentication Successful" appears. 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 address as a destination interface in the access rule applied to the source interface. In addition, you must add a static NAT rule for the virtual Telnet 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 address. A static NAT rule is not required. To configure a virtual Telnet server: 1. Select the Enable Virtual Telnet check box. 2. Enter the IP address or select a Networks/Hosts object representing the virtual Telnet server. Make sure this address is an unused address that is routed to the ASA. 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.
Interactive Authentication table (ASA/PIX 7.2.2+)	Use this table to identify the interfaces that should listen for HTTP or HTTPS traffic for authentication. If your AAA rules require authentication for these protocols on interfaces designated in this table, the user is presented with an improved authentication web page as opposed to the default authentication pages used by the appliance. These pages are also used for authenticating direct connections to the device. • To add an interface to the table, click the **Add Row** button and fill in the Interactive Authentication Configuration Dialog Box, page 15-24. • To edit a setting, select it and click the **Edit Row** button. • To delete a setting, select it and click the **Delete Row** button.

Table 15-3 Advanced Setting Tab, AAA Firewall Settings Page (Continued)

Element	Description
Disable FTP Authentication Challenge Disable HTTP Authentication Challenge Disable HTTPS Authentication Challenge Disable Telnet Authentication Challenge (All options FWSM 3.x+ only.)	Whether to disable authentication challenges for the indicated protocols. By default, the FWSM prompts the user for a username and password 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 might 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 AAA rule. If the user establishes the session with a protocol whose authentication challenge is enabled (such as HTTP), FTP traffic is allowed.
Clear Connections When Uauth Timer Expires table (FWSM 3.2+ only.)	Use this table to identify the interfaces and source addresses where you want to 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. (User authentication timeouts are defined in the **Platform > Security > Timeouts** policy.) For any interface/source address pairs not listed in this table, active connections are not terminated even though the user authentication session expired. • To add any interface and source address pair, click the **Add Row** button and fill in the Clear Connection Configuration Dialog Box, page 15-25. • To edit a setting, select it and click the **Edit Row** button. • To delete a setting, select it and click the **Delete Row** button.

Interactive Authentication Configuration Dialog Box

Use the Interactive Authentication Configuration dialog box to configure an interface to listen for HTTP or HTTPS traffic to authenticate network users. The authentication web page used by a listening port provides an improved user experience compared to the default authentication pages used for these protocols. The authentication pages are used for connections directly to the device and if you select the redirection option, also for through traffic if your AAA rules policy requires HTTP/HTTPS network access authentication. For more information, see Understanding How Users Authenticate, page 15-2.

Navigation Path

Go to the AAA Firewall Settings Page, Advanced Setting Tab, page 15-20 and click the **Add Row** button beneath the Interactive Authentication table, or select an item in the table and click the **Edit Row** button.

Related Topics

- Understanding AAA Rules, page 15-1
- Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4

Field Reference

Table 15-4 Interactive Authentication Configuration Dialog Box

Element	Description
Protocol	The protocol that you want to listen for, either HTTP or HTTPS. If you want to listen for both protocols on an interface, add the interface to the table twice.
Interface	The interface or interface role on which to enable listeners. Enter the name of the interface or interface role, or click **Select** to select it from a list or to create a new interface role.
Port	The port number that the security appliance listens on for this protocol if other than the default, which is 80 (HTTP) and 443 (HTTPS).
Redirect network users for authentication request	Whether to redirect users who are making requests through the device to the authentication web page served by the security appliance. If you do not select this option, only traffic directed to the interface is prompted with the improved authentication web page.

Clear Connection Configuration Dialog Box

Use the Clear Connection Configuration dialog box to identify the source addresses whose active connections to close immediately after the user authentication times out or when you clear the authentication session with the **clear uauth** command. You must specify the interfaces on which those sessions should be cleared. These settings are used only for FWSM 3.2+ devices.

User authentication timeouts are defined in the **Platform > Security > Timeouts** policy.

Navigation Path

Go to the AAA Firewall Settings Page, Advanced Setting Tab, page 15-20 and click the **Add Row** button beneath the Clear Connections When Uauth Timer Expires table, or select an item in the table and click the **Edit Row** button.

Field Reference

Table 15-5 Clear Connection Configuration Dialog Box

Element	Description
Interface	The interfaces or interface roles for which you are configuring settings. Enter the name or click **Select** to select the interface or interface role or to create a new role. Separate multiple entries with commas.
Source IP Address/Netmask	The host or network addresses for which you want to clear connections immediately when the user authentication timer expires. The list can include host IP addresses, network addresses, address ranges, or network/host objects Separate multiple addresses with commas. For more information on entering addresses, see Specifying IP Addresses During Policy Definition, page 6-87.

AAA Firewall Page, MAC-Exempt List Tab

Use the MAC Exempt List tab of the AAA Firewall settings policy to identify hosts that should be exempt from authentication and authorization for ASA, PIX, and FWSM 3.x+ devices. 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, create a rule permitting traffic from the MAC address of the server.

You can use masks to create rules for groups of MAC addresses. For example, if you want to exempt all Cisco IP phones whose MAC addresses start with 0003.e3, create a permit rule for 0003.e300.0000 with the mask ffff.ff00.0000. (An f in a mask exactly matches the corresponding number in the address, whereas a 0 matches anything.)

Deny rules are necessary only if you are permitting a group of MAC addresses but there are some addresses within the permitted group that you want to require to use authentication and authorization. Deny rules do not prohibit traffic; they simply require the host to go through normal authentication and authorization. For example, if you want to allow all hosts with MAC addresses that start with 00a0.c95d, but you want to force 00a0.c95d.0282 to use authentication and authorization, enter these rules in order:

1. Deny 00a0.c95d.0282 ffff.ffff.ffff
2. Permit 00a0.c95d.0000 ffff.ffff.0000

When you deploy the policy to the device, these entries are configured using the **mac-list** and **aaa mac-exempt** commands.

Tip The MAC exempt list is processed on a first match basis. Thus, the order of entries matters. If you want to permit a group of MAC addresses, but deny a subset of them, the deny rule must come before the permit rule. However, Security Manager does not allow you to order MAC exempt rules: they are implemented in the order shown. If you sort the table, your policy changes. If your entries do not depend on each other, this does not matter. Otherwise, ensure that you enter rows in the proper order.

Navigation Path

To access the MAC Exempt List tab, do one of the following:

- (Device view) Select an ASA, PIX, or FWSM device, then select **Firewall > Settings > AAA Firewall**. Select the **MAC-Exempt List** tab.
- (Policy view) Select **Firewall > Settings > AAA Firewall** from the Policy Type selector. Create a new policy or select an existing one, then select the **MAC-Exempt List** tab.
- (Map view) Right-click an ASA, PIX, or FWSM device and select **Edit Firewall Settings > AAA Firewall**, then select the **MAC-Exempt List** tab.

Related Topics

- Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4
- Filtering Tables, page 1-48

Field Reference

Table 15-6 MAC-Exempt List Tab, AAA Firewall Settings Page

Element	Description
MAC-Exempt List Name	The name of the MAC exempt list.

Table 15-6 MAC-Exempt List Tab, AAA Firewall Settings Page (Continued)

Element	Description
MAC Exempt List table	The MAC exempt rules that you want to implement. The table shows the MAC addresses and masks (in hexadecimal) and whether you are permitting them (exempting them from authentication and authorization) or denying them (making them go through standard authentication and authorization). The device processes the entries in order and uses the first match (not the best match). • To add an exemption rule, click the **Add Row** button and fill in the Firewall AAA MAC Exempt Setting Dialog Box, page 15-27. • To edit an exemption rule, select it and click the **Edit Row** button. • To delete an exemption rule, select it and click the **Delete Row** button.

Firewall AAA MAC Exempt Setting Dialog Box

Use the Firewall AAA MAC Exempt Setting dialog box to add and edit exemption entries in the MAC Exempt List table. The security appliance skips authentication and authorization for hosts associated with permitted MAC addresses.

Navigation Path

Go to the AAA Firewall Page, MAC-Exempt List Tab, page 15-26 and click the **Add Row** button beneath the MAC Exempt List table, or select an item in the table and click the **Edit Row** button.

Field Reference

Table 15-7 Firewall AAA MAC Exempt Setting Dialog Box

Element	Description
Action	The action you want to take for the hosts that use the specified MAC addresses: • Permit—Exempts the host from authentication and authorization. • Deny—Forces the host to go through authentication and authorization.
MAC Address	The MAC address of the hosts in standard 12-digit hexadecimal format, such as 00a0.cp5d.0282. You can enter complete MAC addresses or partial addresses. For partial addresses, you can enter 0 for digits you are not matching.
MAC Mask	The mask to apply to the MAC address. Use f to match a digit exactly, 0 to match any digit at that place: • To specify an exact match of the address, enter ffff.ffff.ffff. • To match an address pattern, enter 0 for any digit for which you want to match any character. For example, ffff.ffff.0000 matches all addresses that have the same first 8 digits.

AAA Page

Use the AAA firewall settings policy to identify the servers and banners to use for the authentication proxy and to configure non-default timeout values. The authentication proxy for IOS devices is a service that forces users to log in and authenticate when trying to make HTTP, Telnet, or FTP connections through an IOS device. The settings you configure here work in conjunction with your AAA rules; only if a AAA rule requires user authentication for one of these services does your AuthProxy settings come into play.

Ensure that your configuration of this policy is consistent with your **Firewall > AAA Rules** policy. Additionally, you must use the **Platform > Device Admin > AAA** policy to define the AAA server groups to use for authenticating user access; this policy defines only the authorization and accounting server groups. If you also want to use authorization proxy for HTTPS access, you must enable SSL and configure AAA in the **Platform > Device Admin > Device Access > HTTP** policy in addition to enabling HTTP authorization proxy in your AAA rules policy.

Tip You must configure per-user ACLs in your AAA server to define the privileges you want to apply to each user. When configuring authorization, specify **AAA** as the service (e.g. service = AAA), with a privilege level of 15. For more information on configuring the AAA server, including information on configuring authentication proxy in general, see the "Configuring the Authentication Proxy" section in the *Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T* at http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy_ps6441_TSD_Products_Configuration_Guide_Chapter.html.

Navigation Path

To access the AAA page, do one of the following:

- (Device view) Select a device, then select **Firewall > Settings > AAA** from the Policy selector.
- (Policy view) Select **Firewall > Settings > AAA** from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click a device and select **Edit Firewall Settings > AAA**.

Related Topics

- Understanding AAA Rules, page 15-1
- Understanding How Users Authenticate, page 15-2
- Configuring AAA Rules for IOS Devices, page 15-7

Field Reference

Table 15-8 AAA Firewall Settings Policy

Element	Description
Virtual IP Address	You use the Virtual IP Address only in communications between the IOS HTTP authentication and clients. For the system to operate correctly, the virtual IP address must be set (it cannot be 0.0.0.0), and no other device on the network can have the same address. Configure with an unassigned and unused gateway IP address, such as 1.1.1.1.

Table 15-8 AAA Firewall Settings Policy (Continued)

Element	Description
General Tab	
Authorization Server Groups	The AAA server group policy objects that identify the LDAP, TACACS+, or RADIUS servers that will provide per-user authorization control. You can also use the LOCAL user database defined on the device. Enter the names of the server group objects, or click **Select** to select them from a list or to create new objects. Ensure that you put the groups in priority order; authorization is attempted with the first group and if that group is not available, with subsequent groups.
Accounting Server Groups Use Broadcast for Accounting	The AAA server group policy objects that identify the LDAP, TACACS+, or RADIUS servers that will provide accounting services. Accounting collects per-user usage information for billing, security, or resource allocation purposes. Enter the names of the server group objects, or click **Select** to select them from a list or to create new objects. Ensure that you put the groups in priority order; if you do not select the broadcast option, accounting is attempted with the first group and if that group is not available, with subsequent groups. If you select **Use Broadcast for Accounting**, accounting records are sent simultaneously to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
Accounting Notice	The types of accounting notices to be sent to the accounting server groups: • Start-stop—Sends a start accounting notice at the beginning of a user process and a stop accounting notice at the end of the process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server. • Stop-only—Sends a stop accounting notice at the end of the requested user process. • None—No accounting records are sent.
HTTP Banner FTP Banner Telnet Banner	The banner you want to present on the authentication proxy page to the user when the user is prompted to authenticate for the specified service: • Disable Banner Text—No banner is displayed. • Use Default Banner Text—Displays the default banner “Cisco Systems, *router hostname* Authentication.” • Use Custom Banner Text—Enter the text you want to present to the user.

Table 15-8 AAA Firewall Settings Policy (Continued)

Element	Description
Use HTTP banner from File URL	Whether you want to use your own web page to authenticate HTTP connections. Enter the URL for your HTTP banner. If you configure both HTTP banner text and a URL, the URL banner take precedence; however, the banner text is also configured on the device.
Advanced Tab	
Global Inactivity Time	The length of time, in minutes, that the authentication proxy for a user is maintained when there is no user activity in the session. If this timer expires, the user session is cleared along with its dynamic user access control list (ACL), and the user must re-authenticate. The range is 1 to 2,147,483,647. The default is 60 minutes. Ensure that this timeout value is greater than or equal to the idle timeout values configured in the **Firewall > Settings > Inspection** policy; otherwise, timed-out user sessions might continue to be monitored and eventually hang.
Global Absolute Time	The length of time, in minutes, that an authentication proxy user session can remain active. After this timer expires, the user session must go through the entire process of establishing its connection as if it were a new request. The range is 0 to 35,791. The default is 0, which means that there is no global absolute timeout; user sessions are maintained as long as they are active.
Interface Timeout Table	This table contains the interfaces for which you want to configure timeout values that differ from the global timeout values. If you want to use the global values for all interfaces, you do not need to configure anything in this table. • To add an interface with customized timeout values, click the **Add Row** button and fill in the Firewall AAA IOS Timeout Value Setting, page 15-30. • To edit a setting, select it and click the **Edit Row** button. • To delete a setting, select it and click the **Delete Row** button.

Firewall AAA IOS Timeout Value Setting

Use the Firewall AAA IOS Timeout Value Setting dialog box to configure idle and absolute timeout values for specific interfaces. These values override the global timeout values configured on the **Firewall > Settings > ScanSafe Web Security** policy Server Timeout tab.

Navigation Path

From the Advanced tab of the AAA Page, page 15-28, click the **Add Row** button beneath the table of interfaces, or select a row and click the **Edit Row** button.

Field Reference

Table 15-9 Firewall AAA IOS Timeout Value Setting Dialog Box

Element	Description
Interfaces	The interfaces or interface roles for which you are configuring timeout values. Enter the names of the interfaces or roles, or click **Select** to select them from a list or to create new interface roles. Separate multiple entries with commas.
Auth Proxy Tab	
Inactivity/Cache Time	The length of time, in minutes, that the authentication proxy for a user is maintained when there is no user activity in the session on the interface. If this timer expires, the user session is cleared along with its dynamic user access control list (ACL), and the user must re-authenticate. The range is 1 to 2,147,483,647. The default is the global inactivity timeout value (whose default is 60 minutes).
Absolute Time	The length of time, in minutes, that an authentication proxy user session can remain active on the interface. After this timer expires, the user session must go through the entire process of establishing its connection as if it were a new request. The range is 1 to 35,791. The default is 0, which means that there is no absolute timeout; user sessions are maintained as long as they are active.
Authentication Proxy Method (IOS)	The protocols to which these timeout values should apply. You can select any combination of HTTP, FTP, or Telnet.

Table 15-9 Firewall AAA IOS Timeout Value Setting Dialog Box (Continued)

Element	Description
HTTP/NTLM Tab	The HTTP and the NTLM areas contain the same following fields and selections: Set the **Inactivity/Cache Time** and the **Absolute Time** for HTTP/NTLM and then, if desired, select Enable Passive Authentication. Finally, select the **Identity Policy** that you want to apply.
Method Order Tab	Select the checkbox of each method you want to employ and then use the up and down arrows to arrange the methods in the order you desire.
AAA Settings Tab	Select the **AAA Settings** tab to specify the Authentication, Authorization, and Account settings as detailed below.
Authenticate Using	In the Authenticate Using section you can select the server group(s) to use for authentication. Choices are: • **None**—No authentication • **Default**—Use the default authentication server group(s). • **Custom**—Enable the selection of user specified authentication server group(s). Then click **Select** to specify or add a server group.
Authorize Exec Operation Using	In the Authorize Exec Operation Using section you can select the server group(s) to use for authorization of executive operations. Choices are: • **None**—No authorization • **Default**—Use the default authorization server group(s) • **Custom**—Enable the selection of user specified authorization server group(s). Then click **Select** to specify or add a server group.
Perform Exec Operation Using	In the Authorize Exec Operation Using section you can select the server group(s) to use for performing executive operations. Choices are: • **None**—No authorization • **Default**—Use the default server group(s) • **Custom**—Enable the selection of user specified server group(s). Then click **Select** to specify or add a server group.
Accounting Notice	Use Accounting Notice to specify accounting operations. • **None**—No accounting notices • **Start-stop**—Accounting notices at the beginning and end of operations • **Stop-only**—Accounting notices at the end of operations.
Accounting Server Groups	Specify what accounting server groups to use. Either enter or select the Accounting Server group. **Note** If you choose to select an accounting server group, you are also give the option to add an Accounting Server group.
Use Broadcast for Accounting	Select this checkbox to broadcast accounting notices.