



CHAPTER 21

Configuring AAA Rules

This chapter describes how to enable AAA (pronounced “triple A”) for network access. This chapter includes the following sections:

- [AAA Performance, page 21-1](#)
- [Configuring Authentication for Network Access, page 21-1](#)
- [Configuring Authorization for Network Access, page 21-5](#)
- [Configuring Accounting for Network Access, page 21-11](#)
- [Using MAC Addresses to Exempt Traffic from Authentication and Authorization, page 21-13](#)
- [Configuring Advanced AAA Features, page 21-13](#)
- [Configuring Virtual Access, page 21-15](#)



Note

For information about AAA for management access, see the “[Configuring AAA for System Administrators](#)” section on page 13-24.

For an overview of AAA services, see [Chapter 12, “Configuring AAA Servers and User Accounts.”](#)

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 Authentication for Network Access

This section includes the following topics:

- [Authentication Overview, page 21-2](#)
- [Enabling Network Access Authentication, page 21-4](#)

- [Secure Authentication of Web Clients](#), page 21-3
- [Configuring Authorization for Network Access](#), page 21-5

Authentication Overview

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

- [One-Time Authentication](#), page 21-2
- [Applications Required to Receive an Authentication Challenge](#), page 21-2
- [Security Appliance Authentication Prompts](#), page 21-2
- [Static PAT and HTTP](#), page 21-3
- [Secure Authentication of Web Clients](#), page 21-3

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the [“Configuring Global Timeouts”](#) section on page 27-22 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.

Applications Required to Receive an Authentication Challenge

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

The authentication ports that the security appliance supports for AAA are fixed:

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

Security Appliance Authentication Prompts

For Telnet and FTP, the security appliance generates an authentication prompt.

For HTTP, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (see the [“Configuring Advanced AAA Features”](#) section on page 21-13).

For HTTPS, the security appliance generates a custom login screen. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (see the [“Configuring Advanced AAA Features”](#) section on page 21-13).

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; 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.

After you authenticate correctly, the security appliance redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure virtual HTTP (see the [“Configuring Virtual Access” section on page 21-15](#)).

**Note**

If you use HTTP authentication, by default the username and password are sent from the client to the security appliance in clear text; in addition, the username and password are sent on to the destination web server as well. See the [“Secure Authentication of Web Clients” section on page 21-3](#) for information to secure your credentials.

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@patm
password> letmein@he110
```

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

Static PAT and HTTP

For HTTP authentication, the security appliance checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped 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 rules 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.

Secure Authentication of Web Clients

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

- Enable the redirection method of authentication for HTTP—See the [“Adding an Interactive Authentication Rule” section on page 21-14](#). This method prevents the authentication credentials from continuing to the destination server.
- Enable virtual HTTP—See the [“Configuring Virtual HTTP” section on page 21-16](#) to let you authenticate separately with the security appliance and with the HTTP server. Even if the HTTP server does not need a second authentication, this command achieves the effect of stripping the basic authentication credentials from the HTTP GET request.
- Enable the exchange of usernames and passwords between a web client and the security appliance with HTTPS—See the [“Using HTTPS to Exchange Credentials for HTTP Authentication” section on page 21-13](#) to enable the exchange of usernames and passwords between a web client and the security appliance with HTTPS. This is the only method that protects credentials between the client and the security appliance, as well as between the security appliance and the destination server. You can use this method alone, or in conjunction with either of the other methods so you can maximize your security.

Enabling Network Access Authentication

To enable network access authentication, perform the following steps:

-
- Step 1** Configure a AAA server group according to [Chapter 12, “Configuring AAA Servers and User Accounts.”](#)
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Authentication Rule**. The Add Authentication Rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface to which you want to apply the rule.
- Step 4** Click **Authenticate** or **Do not Authenticate**.
For example, if you want to authenticate 10.1.1.0/24, but want to exclude 10.1.1.50 from authentication, then create two rules, one using the Authenticate option and the other using the Do not Authenticate option. Be sure to order the rules appropriately. For example, put the above Do not Authenticate rule above the Authenticate rule so that traffic from 10.1.1.50 will match the Do not Authenticate rule first.
- Step 5** From the AAA Server Group drop-down list, choose a server group or the LOCAL user database.
- Step 6** (Optional) To add a AAA server to the server group, click **Add Server**. To add a user to the LOCAL database, click **Add User**.
See [Chapter 12, “Configuring AAA Servers and User Accounts,”](#) for more information about configuring server groups and the local user database.
- Step 7** In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
Enter **any** to specify any source address.
Separate multiple addresses by a comma.
- Step 8** In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any destination address.

Separate multiple addresses by a comma.

Step 9 In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.

If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocol/port*. For example, enter TCP/8080.

By default, the service is TCP.

Separate multiple services by a comma.

Be sure to include the destination ports for either HTTP, HTTPS, Telnet, or FTP because the user must authenticate with one of these services before other services are allowed through the security appliance.

Step 10 (Optional) Enter a description in the Description field.

Step 11 (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.

Step 12 (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.

This setting might be useful if you do not want to remove the rule, but want to turn it off.

Step 13 (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.

To add a new time range, click the ... button. See the [“Configuring Time Ranges”](#) section on page 8-14 for more information.

This setting might be useful if you only want the rule to be active at predefined times.

Step 14 Click **OK**.

Configuring Authorization for Network Access

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

This section includes the following topics:

- [Configuring TACACS+ Authorization, page 21-5](#)
- [Configuring RADIUS Authorization, page 21-7](#)

Configuring TACACS+ Authorization

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

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.

To configure TACACS+ authorization, perform the following steps:

-
- Step 1** Enable authentication for the traffic you want to authorize. For more information, see the [“Configuring Authentication for Network Access”](#) section on page 21-1. If you have already enabled authentication, continue to the next step.
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Authorization Rule**.
The Add Authorization Rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface to which you want to apply the rule.
- Step 4** Click **Authorize** or **Do not Authorize**.
For example, if you want to authorize 10.1.1.0/24, but want to exclude 10.1.1.50 from authorization, then create two rules, one using the Authorize option and the other using the Do not Authorize option. Be sure to order the rules appropriately. For example, put the above Do not Authorize rule above the Authorize rule so that traffic from 10.1.1.50 will match the Do not Authorize rule first.
- Step 5** From the AAA Server Group drop-down list, choose a server group or the LOCAL user database.
- Step 6** (Optional) To add a AAA server to the server group, click **Add Server**. To add a user to the LOCAL database, click **Add User**.
See [Chapter 12, “Configuring AAA Servers and User Accounts,”](#) for more information about configuring server groups and the local user database.
- Step 7** In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
Enter **any** to specify any source address.
Separate multiple addresses by a comma.
- Step 8** In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
Enter **any** to specify any destination address.
Separate multiple addresses by a comma.
- Step 9** In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.
If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocol/port*. For example, enter TCP/8080.
By default, the service is TCP.
Separate multiple services by a comma.
- Step 10** (Optional) Enter a description in the Description field.

- Step 11** (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.
- The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
- Step 12** (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.
- This setting might be useful if you do not want to remove the rule, but want to turn it off.
- Step 13** (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.
- To add a new time range, click the ... button. See the [“Configuring Time Ranges” section on page 8-14](#) for more information.
- This setting might be useful if you only want the rule to be active at predefined times.
- Step 14** Click **OK**.
-

Configuring RADIUS Authorization

When authentication succeeds, the RADIUS protocol returns user authorizations in the access-accept message sent by a RADIUS server. For more information about configuring authentication, see the [“Configuring Authentication for Network Access” section on page 21-1](#).

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. The user is authorized to do only what is permitted in the user-specific access list.



Note

If you have an access rule, be aware of the following effects of the Per User Override Setting (see the [“Advanced Access Rule Configuration” section on page 19-7](#)) on authorization by user-specific access lists:

- Without the Per User Override Setting, 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 Setting, the user-specific access list determines what is permitted.
-

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 21-8](#)
- [Configuring Cisco Secure ACS for Downloadable Access Lists, page 21-9](#)
- [Configuring Any RADIUS Server for Downloadable Access Lists, page 21-10](#)
- [Converting Wildcard Netmask Expressions in Downloadable Access Lists, page 21-11](#)

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
```

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

The 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-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_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 option, available in the Configuration > Device Management > Users/AAA > AAA Server Groups > Add/Edit AAA Server dialog box. For more information about configuring a RADIUS server, see [Chapter 12, “Configuring AAA Servers and User Accounts.”](#)

Configuring Accounting for Network Access

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.

To configure accounting, perform the following steps:

- Step 1** If you want the security appliance to provide accounting data per user, you must enable authentication. For more information, see the [“Configuring Authentication for Network Access”](#) section on page 21-1. If you want the security appliance to provide accounting data per IP address, enabling authentication is not necessary and you can continue to the next step.
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Accounting Rule**. The Add Accounting Rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface to which you want to apply the rule.

Step 4 Click **Account** or **Do not Account**.

For example, if you want to account 10.1.1.0/24, but want to exclude 10.1.1.50 from accounting, then create two rules, one using the Account option and the other using the Do not Account option. Be sure to order the rules appropriately. For example, put the above Do not Account rule above the Account rule so that traffic from 10.1.1.50 will match the Do not Account rule first.

Step 5 From the AAA Server Group drop-down list, choose a server group or the LOCAL user database.**Step 6** (Optional) To add a AAA server to the server group, click **Add Server**. To add a user to the LOCAL database, click **Add User**.

See [Chapter 12, “Configuring AAA Servers and User Accounts,”](#) for more information about configuring server groups and the local user database.

Step 7 In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any source address.

Separate multiple addresses by a comma.

Step 8 In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any destination address.

Separate multiple addresses by a comma.

Step 9 In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.

If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocol/port*. For example, enter TCP/8080.

By default, the service is TCP.

Separate multiple services by a comma.

Step 10 (Optional) Enter a description in the Description field.**Step 11** (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.

Step 12 (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.

This setting might be useful if you do not want to remove the rule, but want to turn it off.

Step 13 (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.

To add a new time range, click the ... button. See the [“Configuring Time Ranges”](#) section on page 8-14 for more information.

This setting might be useful if you only want the rule to be active at predefined times.

Step 14 Click **OK**.

Using MAC Addresses to Exempt Traffic from Authentication and Authorization

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.

This feature is particularly useful to exempt devices such as IP phones that cannot respond to authentication prompts.

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

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add MAC Exempt Rule**.
The Add MAC Exempt Rule dialog box appears.
 - Step 2** From the Action drop-down list, choose **MAC Exempt** or **No MAC Exempt**.
For example, if you want to exempt 00a0.c95d.0000 ffff.fff.0000, but do not want to exempt 00a0.c95d.0282 ffff.fff.fff, then create two rules, one using the MAC Exempt option and the other using the No MAC Exempt option. Be sure to order the rules appropriately. For example, put the above No MAC Exempt rule above the MAC Exempt rule so that traffic from 00a0.c95d.0282 ffff.fff.fff will match the No MAC Exempt rule first.
 - Step 3** In the MAC Address field, enter the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn.
 - Step 4** In the MAC Mask field, enter the portion of the MAC address that should be used for matching.
For example, ffff.fff.fff matches the MAC address exactly. ffff.fff.0000 matches only the first 8 digits.
 - Step 5** Click **OK**.
-

Configuring Advanced AAA Features

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

- [Using HTTPS to Exchange Credentials for HTTP Authentication, page 21-13](#)
- [Adding an Interactive Authentication Rule, page 21-14](#)

Using HTTPS to Exchange Credentials for HTTP Authentication

The security appliance provides a method of securing HTTP authentication. Without securing HTTP authentication, usernames and passwords from the client to the security appliance would be passed as clear text. By using the Secure HTTP feature, 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.

Secured web-client authentication has the following limitations:

- A maximum of 16 concurrent HTTPS authentication sessions are allowed. If all 16 HTTPS authentication processes are running, a new connection requiring authentication will not succeed.
- When the authentication absolute timeout is set to 0 (see the Authentication absolute option in the “[Configuring Global Timeouts](#)” section on page 27-22), HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the authentication absolute timeout to 1 second. However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.
- Because HTTPS authentication occurs on the SSL port 443, users must not configure an access rule to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port.

To enable secure authentication of web clients, perform the following steps:

-
- Step 1** From the Configuration > Firewall > AAA Rules pane, click the **Advanced** button at the bottom of the pane.
- The AAA Rules Advanced Options dialog box appears.
- Step 2** Check **Enable Secure HTTP**.
- Step 3** Click **OK**.
-

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 > Firewall > AAA Rules pane, click the **Advanced** button at the bottom of the pane.
- The AAA Rules Advanced Options dialog box appears.
- Step 2** In the Interactive Authentication area, click **Add**.
- Step 3** From the Protocol menu, choose **HTTP** or **HTTPS**.
- To enable listeners for both HTTP and HTTPS, you need to create two separate rules.
- Step 4** From the Interface menu, choose the interface name on which you want to enable the listener.
- Step 5** 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 6** 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 7** Click **OK**.
-

Configuring Virtual Access

This section describes how to configure direct authentication using Telnet, or how to configure a virtual HTTP server for use with basic HTTP authentication. This section includes the following topics:

- [Enabling Direct Authentication Using Telnet, page 21-15](#)
- [Configuring Virtual HTTP, page 21-16](#)

Enabling Direct Authentication Using Telnet

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the security appliance, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate using a AAA authentication rule (see the “[Configuring Authentication for Network Access](#)” section on page 21-1).

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. Once authenticated, the user sees the message “Authentication Successful.” Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet address as a destination interface in the access rule applied to the source interface. Moreover, you must add a static NAT rule for the virtual Telnet 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 logout from the security appliance, reconnect to the virtual Telnet IP address; you are prompted to log out.

To configure a virtual Telnet server, perform the following steps:

-
- Step 1** From the Configuration > Firewall > Advanced > Virtual Access pane, check **Enable Telnet Server**.
 - Step 2** In the Virtual Telnet Server field, enter the IP address to which you want to Telnet.
Make sure this address is an unused address that is routed to the security appliance. For example, if you perform NAT for inside addresses when they access the outside, and you want to provide outside access to the virtual Telnet server, you can use one of the global NAT addresses for the virtual Telnet server address.
 - Step 3** Click **OK**.
-

Configuring Virtual HTTP

When you use HTTP authentication on the security appliance (see the [“Configuring Authentication for Network Access” section on page 21-1](#)), the security appliance uses basic HTTP authentication by default. You can change the authentication method so that the security appliance redirects HTTP connections to web pages generated by the security appliance itself (see the [“Adding an Interactive Authentication Rule” section on page 21-14](#)).

However, if you continue to use basic HTTP authentication, then you might need a virtual HTTP server when you have cascading HTTP authentications.

If the destination HTTP server requires authentication in addition to the security appliance, then the virtual http command lets you authenticate separately with the security appliance (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This feature redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the security appliance. The security appliance prompts for the AAA server username and password. After the AAA server authenticates the user, the security appliance 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 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, perform the following steps:

-
- Step 1** From the Configuration > Firewall > Advanced > Virtual Access pane, check **Enable HTTP Server**.
- Step 2** In the Virtual HTTP Server field, enter the IP address of the virtual HTTP server.
Make sure this address is an unused address that is routed to the security appliance. For example, if you perform NAT for inside addresses when they access the outside, and you want to provide outside access to the virtual HTTP server, you can use one of the global NAT addresses for the virtual HTTP server address.
- Step 3** (Optional) To notify users that the HTTP connection needs to be redirected to the security appliance, check **Display redirection warning**.
This option applies only for text-based browsers, where the redirect cannot happen automatically.
- Step 4** Click **OK**.
-

