Firewall Authentication Proxy for FTP and Telnet Sessions

First Published: May 14, 2003
Last Updated: August 10, 2010

Before the introduction of the Firewall Authentication Proxy for FTP and Telnet Sessions feature, users could enable only HTTP when configuring authentication proxy. This feature introduces support for FTP and Telnet, providing users with three protocol options when configuring authentication proxy.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Firewall Authentication Proxy for FTP and Telnet Session" section on page 18.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Contents

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

Restrictions for Firewall Authentication Proxy for FTP and Telnet Sessions

- Authentication proxy is an IP-only feature; thus, it comes with only -o3 images.
- "proxyacl#<n>" is the only supported attribute in the authentication, authorization, and accounting (AAA) server's user configuration.
- Authentication proxy is subjected only to the traffic that passes through the router; traffic that is destined for the router continues to be authenticated by the existing authentication methods that are provided by Cisco IOS.

Information About Firewall Authentication Proxy for FTP and Telnet Sessions

To configure the Authentication Proxy for FTP and Telnet Sessions feature, you must understand the following concepts:

- Feature Design for FTP and Telnet Authentication Proxy, page 2
- Absolute Timeout, page 7

Feature Design for FTP and Telnet Authentication Proxy

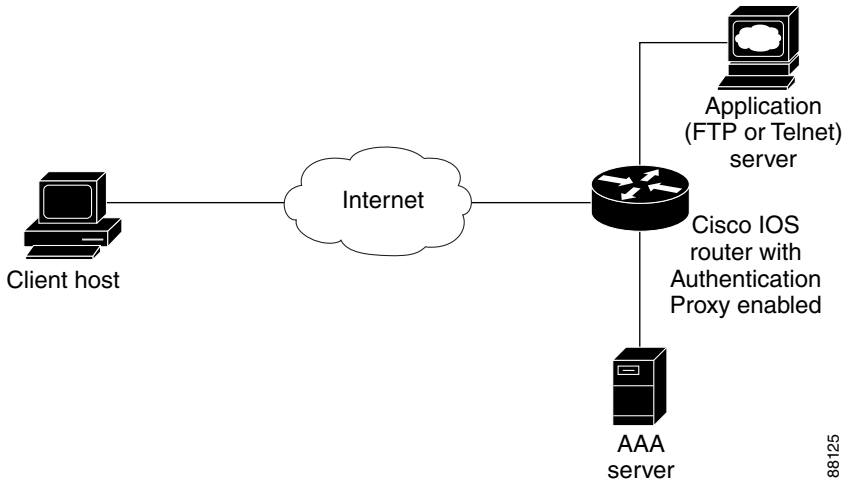
Authentication proxy for FTP and Telnet Sessions functions like authentication proxy for HTTP; that is, FTP and Telnet are independent components in the Cisco IOS software and can be enabled or disabled on the interface of an unauthenticated host.

Many of the authentication proxy for FTP or Telnet functions are similar to those used with HTTP, such as the interaction between the authentication proxy router and the AAA server during authentication. However, because of protocol differences, FTP and Telnet login methods are different from HTTP.

FTP and Telnet Login Methods

Figure 1 displays a typical authentication proxy topology.

Figure 1 Typical Authentication Proxy Topology



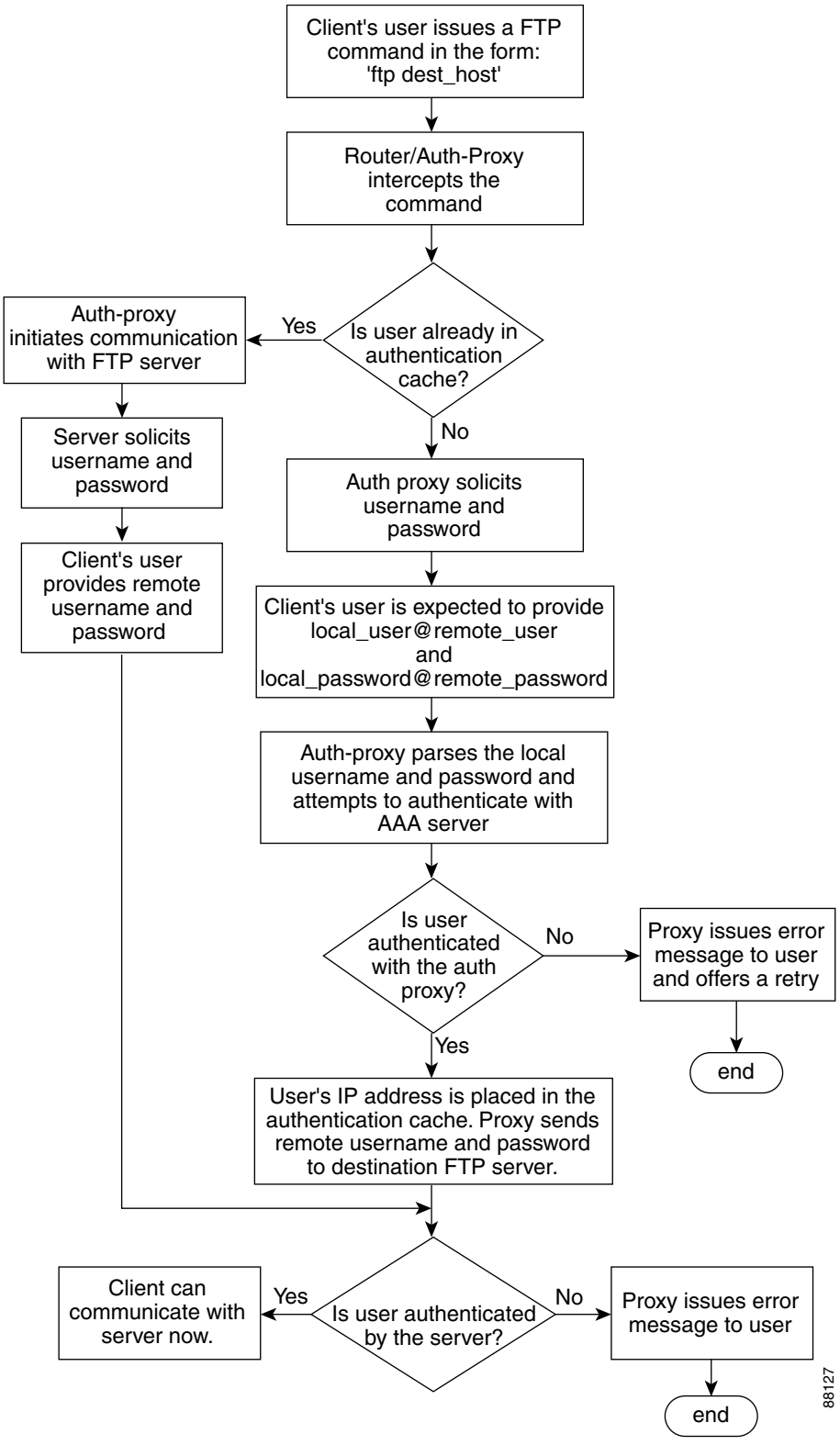
Just as with HTTP, the authentication proxy router intercepts traffic that is sent from the client host. Upon receiving a FTP or Telnet packet, the router will look into its authentication cache to check whether the client host has already been authenticated. If it has been authenticated, the router will forward the client host's traffic to the FTP or Telnet server for additional authentication. If the IP address of the client host is not in the cache of the router, the router will try to authenticate the client host with the AAA server using the username and password of the router.

FTP Login

For FTP login, the client host will be prompted (by the authentication proxy router) for the username and password of the router; the client must respond with the username and password in the following format: "login: proxy_username@ftp_username" and "password: proxy_passwd@ftp_passwd:". The authentication proxy will use the proxy username and password to verify the client's profile against the AAA server's user database. After the client is successfully authenticated with the AAA server, the authentication proxy will pass the FTP (remote) username and password to the FTP server (destination server) for the application server authentication.

A flow chart that depicts an overview of the FTP authentication proxy process is shown in Figure 2.

Figure 2 FTP Authentication Proxy Overview

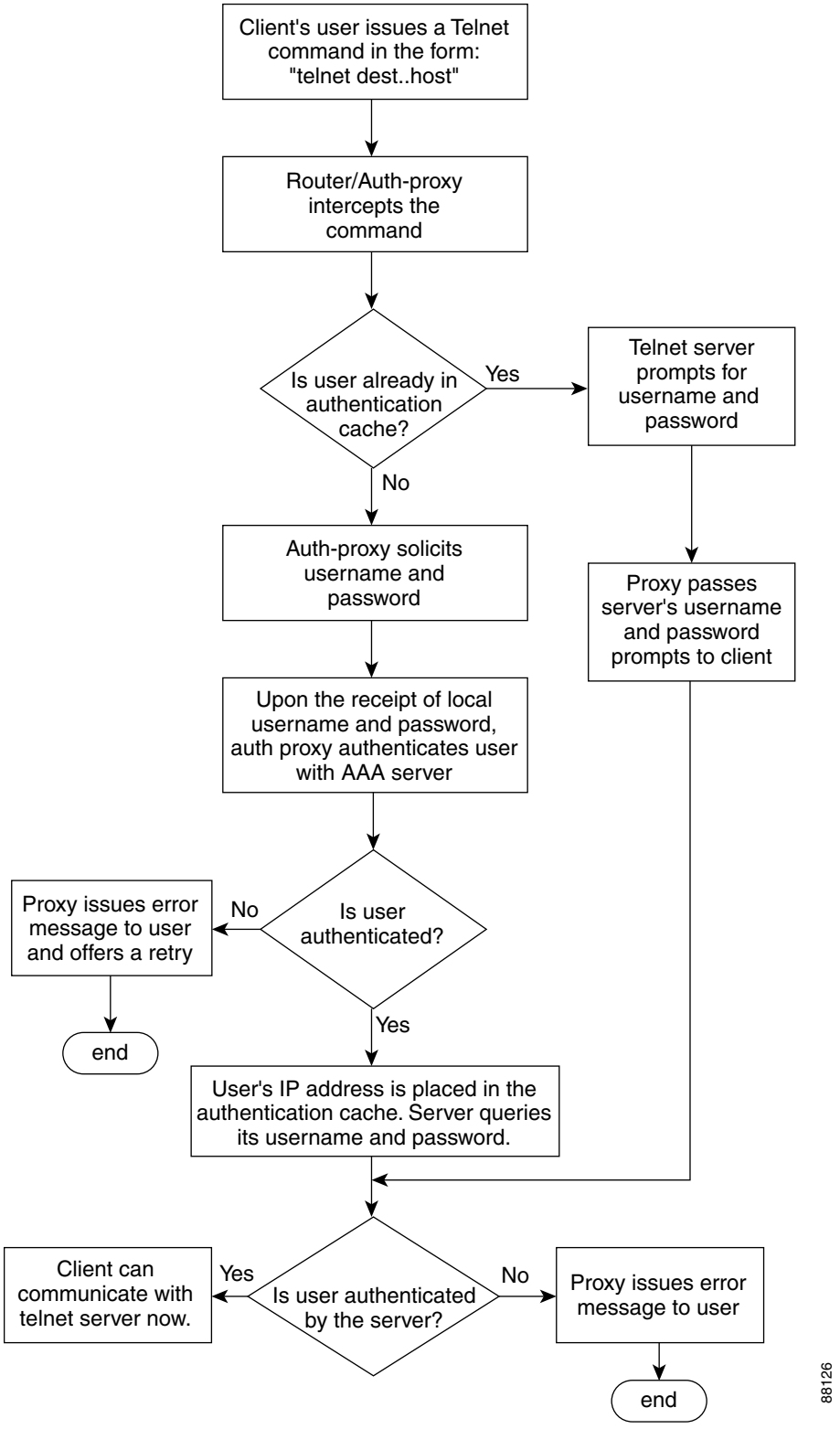


Telnet Login

For Telnet login, the client host will be prompted (by the authentication proxy router) for the username, followed by the password; the client must respond with the username and password in the following format: “login: proxy_username:” and “password: proxy_passwd):”. The username and password will be verified against the AAA server’s user database. After the client is successfully authenticated with the AAA server, the Telnet server (destination server) will prompt the client for the username and password of the Telnet server.

A flow chart that depicts an overview of the Telnet authentication proxy process is shown in Figure 3.

Figure 3 Telnet Authentication Proxy Overview



If authentication with the AAA server fails, the proxy will inform the client accordingly. With Telnet, the proxy does not have any interest in the Telnet server's username and password. If the client is authenticated with the AAA server but fails with the Telnet server, the client will not have to authenticate with the AAA server the next time he or she logs into the network; the client's IP address will be stored in the authentication cache. The client will have to authenticate only with the Telnet server.

Note With FTP, the client must always reenter the local and remote username and password combination every time he or she tries to log into the network—regardless of a successful AAA server authentication.

Absolute Timeout

An absolute timeout value has been added to allow users to configure a window during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy will be disabled regardless of any activity. The absolute timeout value can be configured per protocol (through the **ip auth-proxy name** command) or globally (through the **ip auth-proxy** command). The default value of the absolute timeout is zero; that is, the absolute timer is turned off by default, and the authentication proxy is enabled indefinitely and is subject only to the timeout specified by the **inactivity-timer** keyword.

Note The **inactivity-timer** keyword deprecates the **auth-cache-time** keyword in the **ip auth-proxy name** and the **ip auth-proxy** commands.

How to Configure FTP or Telnet Authentication Proxy

To enable FTP or Telnet authentication proxy, you must enable AAA services, configure the FTP or Telnet server, and enable authentication proxy. This section contains the following procedures:

- Configuring AAA, page 7
- Configuring the Authentication Proxy, page 9
- Verifying FTP or Telnet Authentication Proxy, page 11
- Monitoring and Maintaining FTP or Telnet Authentication Proxy Sessions, page 11

Configuring AAA

To use authentication proxy, you must configure a AAA server for authentication. The authentication proxy service of the AAA server must also be configured for authorization. To configure these tasks, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default group tacacs+ group radius**

5. **aaa authorization auth-proxy default** [[**group tacacs+**] [**group radius**]]
6. **aaa authorization exec default** [**group tacacs+**] [**group radius**]
7. **aaa accounting auth-proxy default stop-only** [**group tacacs+**] [**group radius**]
8. **access-list** *access-list-number* {**permit** | **deny**} {**tcp** | **ip** | **icmp**} **host** *source* **eq** *tacacs* **host** *destination*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router (config)# aaa new-model`	Enables the AAA functionality on the router.
Step 4	**aaa authentication login default group tacacs+ group radius** **Example:** `Router (config)# aaa authentication login default group tacacs+ group radius`	Defines the list of authentication methods at login.

Step 5	`aaa authorization auth-proxy default [[`**group tacacs+**`] [`**group radius**`]]`
	
	Example:
	`Router (config)# aaa authorization auth-proxy default group tacacs+ group radius`
		Uses the **auth-proxy** keyword to enable authorization proxy for AAA methods.

Step 6	`aaa authorization exec default [`**group tacacs+**`] [`**group radius**`]`
	
	Example:
	`Router (config)# aaa authorization exec default group tacacs+ group radius`
		Enables authorization for TACACS+ and RADIUS.

	Command or Action	Purpose

Step 7	`aaa accounting auth-proxy default stop-only [group tacacs+] [group radius]`
	
	Example:
	`Router (config)# aaa accounting auth-proxy default stop-only group tacacs+ group radius`
		Activates authentication proxy accounting and uses the **auth-proxy** keyword to set up the authorization policy as dynamic access control lists (ACLs) that can be downloaded.

Step 8	`access-list` *access-list-number* {**permit** | **deny**} {**tcp** | **ip** | **icmp**} **host** *source* **eq** *tacacs* **host** *destination*
	
	Example:
	`Router (config)# access-list 111 permit tcp host 209.165.200.225 eq tacacs host 209.165.200.254`
	
	or
	
	`Router (config)# access-list 111 deny ip any any`
	
	or
	
	`Router (config)#  access-list 111 permit icmp any any`
		Creates an ACL entry to allow the AAA server to return traffic to the firewall.
		
		The source address is the IP address of the AAA server, and the destination is the IP address of the router interface where the AAA server resides.

What to Do Next

Ensure that your FTP or Telnet server is enabled and that the user credentials of the client (the username and password) are stored in the server's database.

Configuring the Authentication Proxy

To configure the authentication proxy, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip auth-proxy** {**inactivity-timer** *min* | **absolute-timer** *min*}
4. **ip auth-proxy auth-proxy-banner** {**ftp** | **http** | **telnet**} [*banner-text*]
5. **ip auth-proxy name** *auth-proxy-name* {**ftp** | **http** | **telnet**} [**inactivity-timer** *min* | **absolute-timer** *min*] [**list** {*acl* | *acl-name*}]
6. **interface** *type*
7. **ip auth-proxy** *auth-proxy-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip auth-proxy** {**inactivity-timer** *min* | **absolute-timer** *min*} **Example:** `Router (config)# ip auth-proxy inactivity-timer 30`	Sets the global authentication proxy idle timeout values in minutes. • **inactivity-timer** *min*—Specifies the length of time in minutes that an authentication cache entry is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes. • **absolute-timer** *min*—Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.
Step 4	**ip auth-proxy auth-proxy-banner** {**ftp** | **http** | **telnet**}[*banner-text*] **Example:** `Router (config)# ip auth-proxy auth-proxy-banner ftp hello`	Optional) Displays the name of the firewall router in the authentication proxy login page. Disabled by default. • **ftp**—Specifies the FTP protocol. • **http**—Specifies the HTTP protocol. • **telnet**—Specifies the Telnet protocol. • *banner-text*—(Optional) A text string that replaces the default banner.
Step 5	**ip auth-proxy name** *auth-proxy-name* {**ftp** | **http** | **telnet**} [**inactivity-timer** *min*] [**absolute-timer** *min*] [**list** {*acl* | *acl-name*}] **Example:** `Router (config)# ip auth-proxy name ftp_list1 ftp absolute-timer 60 ftp list 102`	Configures authentication proxy on an interface. • **ftp**—Specifies FTP to trigger that authentication proxy. • **http**—Specifies HTTP to trigger that authentication proxy. • **telnet**—Specifies Telnet to trigger that authentication proxy. • **inactivity-timer** *min*—Overrides global authentication proxy cache timer for a specific authentication proxy name. • **absolute-timer** *min*— Overrides the global value specified through the **ip auth-proxy** command. • **list** {*acl* | *acl-name*}—Specifies a standard (1–99), extended (1–199), or named access list to use with the authentication proxy.

	Command or Action	Purpose
Step 6	**interface** *type* **Example:** `Router (config)# interface e0`	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 7	**ip auth-proxy** *auth-proxy-name* **Example:** `Router(config-if)# ip auth-proxy authproxyrule`	In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

Verifying FTP or Telnet Authentication Proxy

To verify your FTP or Telnet authentication proxy configuration, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip auth-proxy configuration**
3. **show ip auth-proxy cache**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**show ip auth-proxy configuration** **Example:** `Router# show ip auth-proxy configuration`	Displays the current authentication proxy configuration.

Step 3	`show ip auth-proxy cache`
	
	Example:
	`Router# show ip auth-proxy cache`
		Displays the list of user authentication entries.
		
		The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is ESTAB or INTERCEPT, the user authentication was successful.

Monitoring and Maintaining FTP or Telnet Authentication Proxy Sessions

To monitor FTP or Telnet authentication proxy sessions, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **debug ip auth-proxy {detailed | ftp | function-trace | object-creation | object-deletion | telnet | timers}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**debug ip auth-proxy** {**detailed** | **ftp** | **function-trace** | **object-creation** | **object-deletion** | **telnet** | **timers**} **Example:** `Router# debug ip auth-proxy ftp`	Displays the authentication proxy configuration information on the router.

Configuration Examples for FTP and Telnet Authentication Proxy

This section provides the following configuration examples:

- Authentication Proxy Configuration Example, page 12
- AAA Server User Profile Examples, page 13

Authentication Proxy Configuration Example

The following example shows how to configure your router for authentication proxy:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa authorization auth-proxy default group tacacs+
enable password lab
!
ip inspect name pxy_test ftp
ip auth-proxy name pxy auth-cache-time 1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.224
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect pxy_test in
 ip auth-proxy pxy
 no shut
!
interface Ethernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip access-group 102 in
 no ip directed-broadcast
```

```
no shut
!
ip http authentication aaa
!
access-list 102 permit any
access-list 102 permit tcp host 209.165.200.234 eq tacacs any
access-list 102 deny   tcp any any
access-list 102 deny   udp any any
access-list 102 permit ip any any
access-list 105 permit tcp any any eq www
access-list 105 permit ip any any
access-list 105 deny   tcp any any
access-list 105 deny   udp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 209.165.200.234
tacacs-server key cisco
!
line con 0
 transport input none
 login authentication special
line aux 0
line vty 0 4
 password lab
```

AAA Server User Profile Examples

This section includes examples of the authentication proxy user profile entries on the AAA servers. The "proxyacl" entries define the user access privileges. After the user has successfully used the authentication proxy to log in, these entries are transferred to the firewall router. Each entry in the profile must specify "permit" access for the service or application. The source address in each entry is set to "any", which is replaced with the IP address of the authenticating host when the profile is downloaded to the firewall. The privilege level must be set to 15 for all AAA users.

This section contains the following examples:

- TACACS+ User Profiles: Example, page 13
- Livingston RADIUS User Profiles: Example, page 14
- Ascend RADIUS User Profiles: Example, page 15

TACACS+ User Profiles: Example

The following example are sample TACACS+ user profiles:

```
default authorization = permit
key = cisco
user = http_1 {
  default service = permit
      login = cleartext test
         service = exec
        {
                priv-lvl = 15
                inacl#4="permit tcp any host 209.165.200.234 eq 23"
                inacl#5="permit tcp any host 209.165.200.234 eq 20"
                inacl#6="permit tcp any host 209.165.200.234 eq 21"
                inacl#3="deny -1"

        }
```

```
      service = auth-proxy
          {
              priv-lvl=15
              proxyacl#4=”permit tcp any host 209.165.201.1 eq 23”
              proxyacl#5=”permit tcp any host 209.165.201.1 eq 20”
              proxyacl#6=”permit tcp any host 209.165.201.1 eq 21”
              proxyacl#7=”permit tcp any host 209.165.201.1 eq 25”
          }

}
user = http {
          login = cleartext test
      service = auth-proxy
         {
              priv-lvl=15
              proxyacl#4=”permit tcp any host 209.165.201.1 eq 23”
              proxyacl#5=”permit tcp any host 209.165.201.1 eq 20”
              proxyacl#6=”permit tcp any host 209.165.201.1 eq 21”
          }
}
 user = proxy_1 {
          login = cleartext test
      service = auth-proxy
          {
              priv-lvl=14
        }
}

user = proxy_3 {
          login = cleartext test
      service = auth-proxy
          {
              priv-lvl=15
        }
}
```

Livingston RADIUS User Profiles: Example

The following examples are sample user profiles for the Livingston RADIUS server:

```
#--------------- Proxy user ---------------------------------

http                    Password = “test” User-Service-Type=Outbound-User
       cisco-avpair = “auth-proxy:priv-lvl=15”,
       cisco-avpair = “auth-proxy:proxyacl#3=permit tcp any any eq 23”

http_1                     Password = “test”
         User-Service-Type = Shell-User,
         User-Service-Type=Dialout-Framed-User,
         cisco-avpair = “shell:priv-lvl=15”,
         cisco-avpair = “shell:inacl#4=permit tcp any host 209.165.200.234
eq 23
         cisco-avpair = “auth-proxy:priv-lvl=15”,
         cisco-avpair = “auth-proxy:proxyacl#3=permit tcp any any eq 23”


http_fail               Password = “test” User-Service-Type=Outbound-User
       cisco-avpair = “auth-proxy:priv-lvl=14”,
       cisco-avpair = “auth-proxy:proxyacl#3=permit tcp any any eq 23”

proxy  Password = “cisco” User-Service-Type=Outbound-User       cisco-avpair =
“auth-proxy:proxyacl#4=permit tcp any any eq 20”
```

Ascend RADIUS User Profiles: Example

The following examples are sample user profiles for the Ascend RADIUS server:

```
#--------------- Proxy user ---------------------------------

http                    Password = "test" User-Service=Dialout-Framed-User
       cisco-avpair = "auth-proxy:priv-lvl=15",
       cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_2                   Password = "test"
User-Service=Dialout-Framed-User
       cisco-avpair = "auth-proxy:priv-lvl=15",
       cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23",
       cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234 eq 25"

http_1                    Password = "test"
         User-Service=Dialout-Framed-User,
         cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234 eq 23",
         cisco-avpair = "auth-proxy:priv-lvl=15",
         cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_fail               Password = "test" User-Service=Dialout-Framed-User
       cisco-avpair = "auth-proxy:priv-lvl=14",
       cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

        cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 23",
       cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
       cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq 20"


#-------------------------------------------------------------

proxy Password = "cisco" User-Service = Dialout-Framed-User

       cisco-avpair = "auth-proxy:priv-lvl=15",

       cisco-avpair = "auth-proxy:priv-lvl=15",
       cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
       cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
```

Additional References

The following sections provide references related to the Firewall Authentication Proxy for FTP and Telnet Sessions feature.

Related Documents

Related Topic	Document Title
Additional authentication proxy configuration tasks	"Configuring Authentication Proxy"
Additional authentication proxy commands	*Cisco IOS Security Command Reference*
RADIUS and TACACS+ configuration information	"Configuring RADIUS" and "Configuring TACACS+"
RADIUS and TACACS+ attribute information	"RADIUS Attributes Overview and RADIUS IETF Attributes" and "TACACS+ Attribute-Value Pairs"
Additional authentication proxy information	"Firewall Support of HTTPS Authentication Proxy"

Standards

Standards	Title
None	—

MIBs

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

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Firewall Authentication Proxy for FTP and Telnet Session

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Firewall Authentication Proxy for FTP and Telnet Sessions

Feature Name	Releases	Feature Information
Firewall Authentication Proxy for FTP and Telnet Sessions	12.3(1)	Before the introduction of the Firewall Authentication Proxy for FTP and Telnet Sessions feature, users could enable only HTTP when configuring authentication proxy. This feature introduces support for FTP and Telnet, providing users with three protocol options when configuring authentication proxy. This feature was introduced in Cisco IOS Release 12.3(1). The following commands were introduced or modified: **debug ip auth-proxy**, **ip auth-proxy**, **ip auth-proxy auth-proxy-banner**, **ip auth-proxy name**.