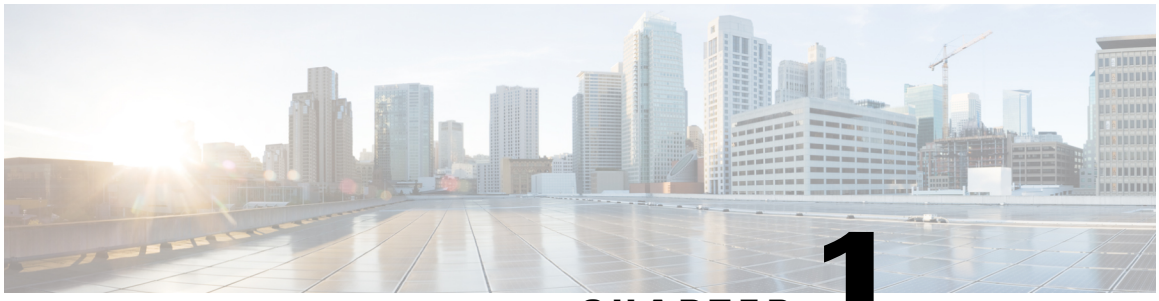
Authentication Proxy Configuration Guide, Cisco IOS Release 15M&T

First Published: November 28, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring Authentication Proxy

The Cisco IOS Firewall Authentication Proxy feature provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Authentication Proxy

Prior to configuring authentication proxy, review the following:

- For the authentication proxy to work properly, the client host must be running the following browser software:

  - Microsoft Internet Explorer 3.0 or later
  - Netscape Navigator 3.0 or later

- The authentication proxy has an option to use standard access lists. You must have a solid understanding of how access lists are used to filter traffic before you attempt to configure the authentication proxy. For an overview of how to use access lists with the Cisco IOS Firewall, see the "Access Control Lists: Overview and Guidelines" module of the *Security Configuration Guide: Access Control Lists* publication.
- The authentication proxy employs user authentication and authorization as implemented in the Cisco authentication, authorization, and accounting (AAA) paradigm. You must understand how to configure AAA before you configure the authentication proxy. For more information about user authentication, authorization, and accounting, see the *Authentication, Authorization, and Accounting (AAA) Configuration Guide*.
- To run the authentication proxy successfully with Cisco IOS Firewall, configure Context-Based Access Control (CBAC) on the firewall. For more information about CBAC, see the "Configuring Context-Based Access Control" module of the *Security Guide Publication: Context-Based Access Control Firewall*.
- HTTP services must be running on the standard (well-known) port, which is port 80 for HTTP.
- Client browsers must enable JavaScript for secure authentication.

Restrictions for Configuring Authentication Proxy

- The authentication proxy is triggered only on HTTP connections.
- The authentication proxy access lists apply to traffic passing through the device. Traffic destined to the device is authenticated by the existing authentication methods provided by Cisco software.
- The authentication proxy does not support concurrent usage; that is, if two users try to log in from the same host at the same time, authentication and authorization applies only to the user who first submits a valid username and password.
- Load balancing using multiple or different AAA servers is not supported.

Information About Configuring Authentication Proxy

The Cisco IOS Firewall Authentication Proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access were associated with a user IP address, or a single security policy had to be applied to an entire user group or subnetwork. Now, users can be identified and authorized on the basis of their per-user policy. Tailoring of access privileges on an individual basis is possible, as opposed to applying a general policy across multiple users.

With the Authentication Proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco security features such as Network Address Translation (NAT), Context-Based Access Control (CBAC), IP Security (IPsec) encryption, and Cisco Secure VPN Client (VPN client) software.

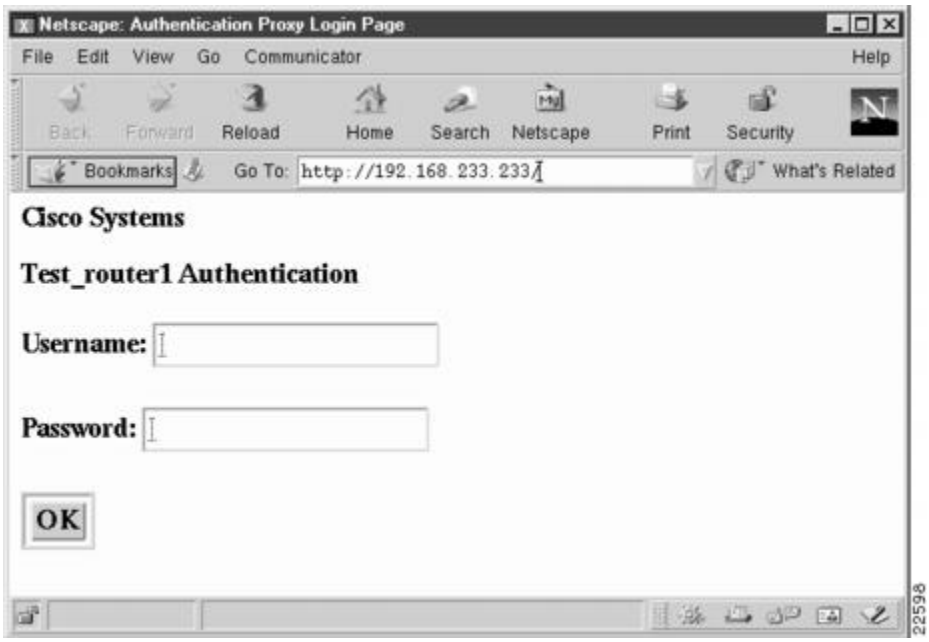
This section contains the following sections:

How Authentication Proxy Works

When a user initiates an HTTP session through the firewall, the authentication proxy is triggered. The authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by the authentication proxy. If no entry exists, the authentication proxy responds to the HTTP connection request by prompting the user for a username and password.

The figure below illustrates the authentication proxy HTML login page.

Figure 1: Authentication Proxy Login Page



Users must successfully authenticate themselves with the authentication server by entering a valid username and password.

If the authentication succeeds, the user's authorization profile is retrieved from the AAA server. The authentication proxy uses the information in this profile to create dynamic access control entries (ACEs) and add them to the inbound (input) access control list (ACL) of an input interface and to the outbound (output) ACL of an output interface, if an output ACL exists at the interface. This process enables the firewall to allow authenticated users access to the network as permitted by the authorization profile. For example, a user can initiate a Telnet connection through the firewall if Telnet is permitted in the user's profile.

If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple login retries. If the user fails to authenticate after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

Note The number of login retries is configurable. The default number of retries is five.

The login page is refreshed each time the user makes requests to access information from a web server.

The authentication proxy customizes each of the access list entries in the user profile by replacing the source IP addresses in the downloaded access list with the source IP address of the authenticated host.

At the same time that dynamic ACEs are added to the interface configuration, the authentication proxy sends a message to the user confirming that the login was successful. The figure below illustrates the login status in the HTML page.

Figure 2: Authentication Proxy Login Status Message

The authentication proxy sets up an inactivity (idle) timer for each user profile. As long as there is activity through the firewall, new traffic initiated from the user's host does not trigger the authentication proxy, and authorized user traffic is permitted access through the firewall.

If the idle timer expires, the authentication proxy removes the user's profile information and dynamic access lists entries. When this happens, traffic from the client host is blocked. The user must initiate another HTTP connection to trigger the authentication proxy.

Secure Authentication

The authentication proxy uses JavaScript to help achieve secure authentication using the client browser. Secure authentication prevents a client from mistakenly submitting a username and password to a network web server other than the authentication proxy router.

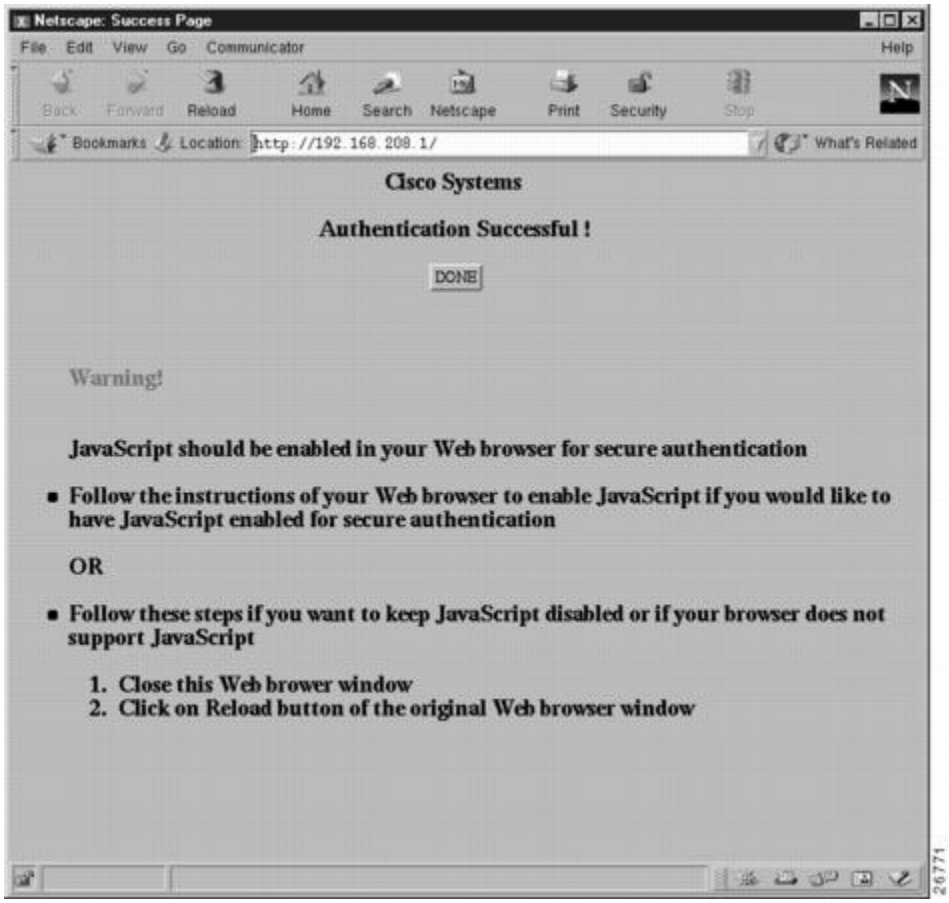
Operation with JavaScript

Users should enable JavaScript on the browser prior to initiating an HTTP connection. With JavaScript enabled on the browser, secure authentication is done automatically, and the user sees the authentication message shown in the Authentication Proxy Login Status Message figure, in the How the Authentication Proxy Works module. The HTTP connection is completed automatically for the user.

Operation Without JavaScript

If the client browser does not support JavaScript, or if site security policy prevents users from enabling JavaScript, any login attempt generates a popup window with instructions for manually completing the connection. The figure below illustrates the authentication proxy login status message with JavaScript disabled on the browser.

Figure 3: Authentication Proxy Login Status Message with JavaScript Disabled



To close this window, click Close on the browser File menu.

After closing the popup window, the user should click Reload (Refresh for Internet Explorer) in the browser window in which the authentication login page is displayed. If the user's last authentication attempt succeeds, clicking Reload brings up the web page the user is trying to retrieve. If the user's last attempt fails, clicking Reload causes the authentication proxy to intercept the client HTTP traffic again, prompting the user with another login page that solicits the username and password.

If JavaScript is not enabled, it is strongly recommended that site administrators advise users of the correct procedure for closing the popup window as described in the section Establishing User Connections Without JavaScript.

Using Authentication Proxy

Unlike some Cisco IOS Firewall features that operate transparently to the user, the authentication proxy feature requires some user interaction on the client host. The table below describes the interaction of the authentication proxy with the client host.

Table 1: Authentication Proxy Interaction with the Client Host

Authentication Proxy Action with Client	Description
Triggering on HTTP connections	If a user is not currently authenticated at the firewall router, any HTTP connection initiated by the user triggers the authentication proxy. If the user is already authenticated, the authentication proxy is transparent to the user.
Logging in using the login page	Triggering the authentication proxy generates an HTML-based login page.The user must enter a username and password to be authenticated with the AAA server. The Authentication Proxy Login Page figure, in the How the Authentication Proxy Works module, illustrates the authentication proxy login page.
Authenticating the user at the client	Following the login attempt, the authentication proxy action can vary depending on whether JavaScript is enabled in the browser. If JavaScript is enabled, and authentication is successful, the authentication proxy displays a message indicating the status of the authentication as shown in the Authentication Proxy Login Status Message figure, in the How the Authentication Proxy Works module. After the authentication status is displayed, the proxy automatically completes the HTTP connection. If JavaScript is disabled, and authentication is successful, the authentication proxy generates a popup window with additional instructions for completing the connection. See the Authentication Proxy Login Status Message with JavaScript Disabled figure, in the Secure Authentication module. If authentication is unsuccessful in any case, the user must log in again from the login page.

When to Use the Authentication Proxy

Here are examples of situations in which you might use the authentication proxy:

- You want to manage access privileges on an individual (per-user) basis using the services provided by the authentication servers instead of configuring access control based on host IP address or global access policies. Authenticating and authorizing users from any host IP address also allows network administrators to configure host IP addresses using DHCP.
- You want to authenticate and authorize local users before permitting access to intranet or Internet services or hosts through the firewall.
- You want to authenticate and authorize remote users before permitting access to local services or hosts through the firewall.
- You want to control access for specific extranet users. For example, you might want to authenticate and authorize the financial officer of a corporate partner with one set of access privileges while authorizing the technology officer for that same partner to use another set of access privileges.
- You want to use the authentication proxy in conjunction with VPN client software to validate users and to assign specific access privileges.
- You want to use the authentication proxy in conjunction with AAA accounting to generate “start” and “stop” accounting records that can be used for billing, security, or resource allocation purposes, thereby allowing users to track traffic from the authenticated hosts.

Applying Authentication Proxy

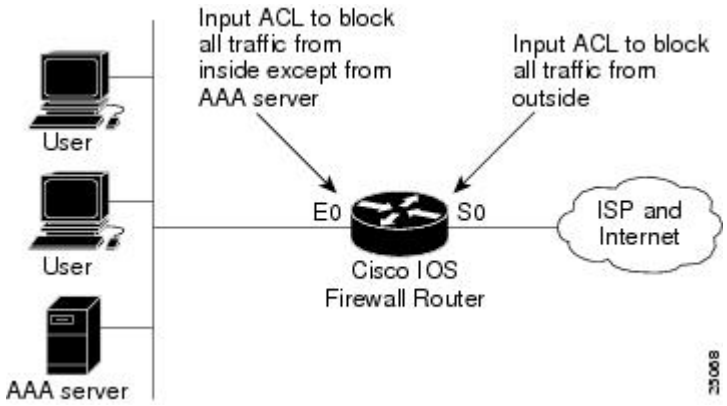
Apply the authentication proxy in the inbound direction at any interface on the router where you want per-user authentication and authorization. Applying the authentication proxy inbound at an interface causes it to intercept a user’s initial connection request before that request is subjected to any other processing by the firewall. If the user fails to gain authentication with the AAA server, the connection request is dropped.

How you apply the authentication proxy depends on your security policy. For example, you can block all traffic through an interface and enable the authentication proxy feature to require authentication and authorization for all user initiated HTTP connections. Users are authorized for services only after successful authentication with the AAA server.

The authentication proxy feature also allows you to use standard access lists to specify a host or group of hosts whose initial HTTP traffic triggers the proxy.

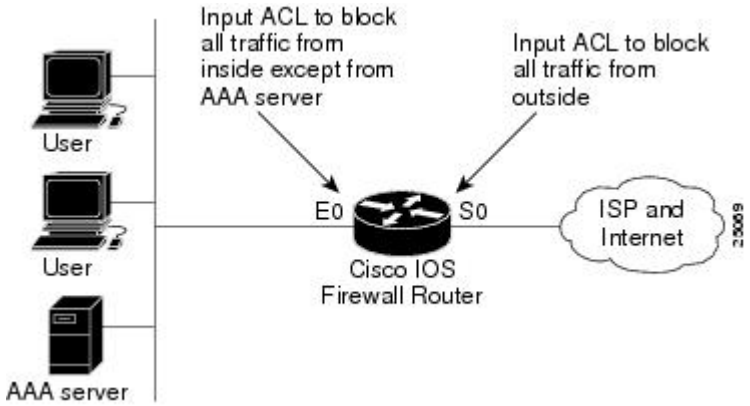
The figure below shows the authentication proxy applied at the LAN interface with all network users required to be authenticated upon the initial connection (all traffic is blocked at each interface).

Figure 4: Applying the Authentication Proxy at the Local Interface



The figure below shows the authentication proxy applied at the dial-in interface with all network traffic blocked at each interface.

Figure 5: Applying the Authentication Proxy at an Outside Interface



Operation with One-Time Passwords

Given a one-time password, the user enters the username and one-time password in the HTML login page as usual.

The user must enter the correct token password within the first three attempts. After three incorrect entries, the user must enter two valid token passwords in succession before authentication is granted by the AAA server.

Compatibility with Other Security Features

The authentication proxy is compatible with Cisco software and with Cisco security features:

- Cisco IOS Firewall Intrusion Detection System (IDS)
- NAT
- CBAC
- IPsec encryption
- VPN client software

The authentication proxy works transparently with the Cisco IOS Firewall IDS and IPsec encryption features.

NAT Compatibility

The authentication proxy feature is compatible with NAT only if the ACL and authentication are completed prior to the NAT translation. Although NAT is compatible with the authentication proxy feature, NAT is not a requirement of the feature.

CBAC Compatibility

Although authentication proxy is compatible with CBAC security functions, CBAC is not required to use the authentication proxy feature.

Authentication proxy's authorization returns access control entries (ACEs) that are dynamically prepended into a manually created ACL. Thereafter, apply the ACL to the "protected side" inbound interface, allowing or disallowing an authorized user's source IP address access to the remote networks.

VPN Client Compatibility

Using the authentication proxy, network administrators can apply an extra layer of security and access control for VPN client traffic. If a VPN client initiates an HTTP connection, the authentication proxy first checks for prior client authentication. If the client is authenticated, authorized traffic is permitted. If the client is not authenticated, the HTTP request triggers the authentication proxy, and the user is prompted for a username and password.

If the user authentication is successful, the authentication proxy retrieves the user profile from the AAA server. The source address in the user profile entries is replaced with the IP address of the authenticated VPN client from the decrypted packet.

Compatibility with AAA Accounting

Using the authentication proxy, you can generate "start" and "stop" accounting records with enough information to be used for billing and security auditing purposes. Thus, you can monitor the actions of authenticated hosts that use the authentication proxy service.

When an authentication proxy cache and associated dynamic access control lists are created, the authentication proxy will start to track the traffic from the authenticated host. Accounting saves data about this event in a data structure stored with the data of other users. If the accounting start option is enabled, you can generate an accounting record (a "start" record) at this time. Subsequent traffic from the authenticated host will be recorded when the dynamic ACL created by the authentication proxy receives the packets.

When an authentication proxy cache expires and is deleted, additional data, such as elapsed time, is added to the accounting information and a “stop” record is sent to the server. At this point, the information is deleted from the data structure.

The accounting records for the authentication proxy user session are related to the cache and the dynamic ACL usage.

Note The accounting records must include RADIUS attributes 42, 46, and 47 for both RADIUS and TACACS+.

For more information on RADIUS attributes, see the *RADIUS Attributes Configuration Guide*.

Protection Against Denial-of-Service Attacks

The authentication proxy monitors the level of incoming HTTP requests. For each request, the authentication proxy prompts the user’s for login credentials. A high number of open requests could indicate that the router is the subject of a denial-of-service (DoS) attack. The authentication proxy limits the level of open requests and drops additional requests until the number of open requests has fallen below 40.

If the firewall is experiencing a high level of connection requests requiring authentication, legitimate network users may experience delays when making connections, or the connection may be rejected and the user must try the connection again.

Risk of Spoofing with Authentication Proxy

When the authentication proxy is triggered, it creates a dynamic opening in the firewall by temporarily reconfiguring an interface with user access privileges. While this opening exists, another host might spoof the authenticated users address to gain access behind the firewall. The authentication proxy does not cause the address spoofing problem; the problem is only identified here as a matter of concern to the user. Spoofing is a problem inherent to all access lists, and the authentication proxy does not specifically address this problem.

Comparison with the Lock-and-Key Feature

Lock-and-key is another Cisco IOS Firewall feature that uses authentication and dynamic access lists to provide user access through the firewall. The table below compares the authentication proxy and lock-and-key features.

Table 2: Comparison of the Authentication Proxy and Lock-and-Key Features

Lock-and-Key	Authentication Proxy
Triggers on Telnet connection requests.	Triggers on HTTP connection requests.
TACACS+, RADIUS, or local authentication.	TACACS+ or RADIUS authentication and authorization.
Access lists are configured on the router only.	Access lists are retrieved from the AAA server only.

Lock-and-Key	Authentication Proxy
Access privileges are granted on the basis of the user's host IP address.	Access privileges are granted on a per-user and host IP address basis.
Access lists are limited to one entry for each host IP address.	Access lists can have multiple entries as defined by the user profiles on the AAA server.
Associates a fixed IP addresses with a specific user. Users must log in from the host with that IP address.	Allows DHCP-based host IP addresses, meaning that users can log in from any host location and obtain authentication and authorization.

Use the authentication proxy in any network environment that provides a per-user security policy. Use lock-and-key in network environments that might benefit from local authentication and a limited number of router-based access control policies based on host addresses. Use lock-and-key in environments not using the Cisco Secure Integrated Software.

AAA Fail Policy

The AAA fail policy is a method for allowing a user to connect or to remain connected to the network if the AAA server is not available. If the AAA server cannot be reached when web-based authentication of a client is needed, instead of rejecting the user (that is, not providing the access to the network), an administrator can configure a default AAA fail policy that can be applied to the user.

This policy is advantageous for the following reasons:

- While AAA is unavailable, the user will still have connectivity to the network, although access may be restricted.
- When the AAA server is again available, a user can be revalidated and the user's normal access policies can be downloaded from the AAA server.

Note When the AAA server is down, the AAA fail policy is applied only if there is no existing policy associated with the user. Typically, if the AAA server is unavailable when a user session requires reauthentication, the policies currently in effect for the user are retained.

While the AAA fail policy is in effect, the session state is maintained as AAA Down.

Customization of the Authentication Proxy Web Pages

The router's internal HTTP server hosts four HTML pages for delivery to an authenticating client during the web-based authentication process. The four pages allow the server to notify the user of the following four states of the authentication process:

- Login—The user's credentials are requested
- Success—The login was successful

- Fail—The login has failed
- Expire—The login session has expired due to excessive login failures

You can substitute your custom HTML pages for the four default internal HTML pages, or you can specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success page.

How to Configure Authentication Proxy

Configuring AAA

You must configure the authentication proxy for AAA services. To enable authorization and define the authorization methods, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default** *method1*[*method2*]
5. **aaa authorization auth-proxy default**
6. **aaa accounting auth-proxy default start-stop group tacacs+**
7. **tacacs-server host** *hostname*
8. **tacacs-server key** *key*
9. **access-list** *access-list-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA functionality on the device.

	Command or Action	Purpose
Step 4	**aaa authentication login default** *method1*[*method2*] **Example:** `Device(config)# aaa authentication login default TACACS+ RADIUS`	Defines the list of authentication methods at login.
Step 5	**aaa authorization auth-proxy default** **Example:** `Device(config)# aaa authorization auth-proxy default`	The **auth-proxy** keyword enables authentication proxy for AAA methods.
Step 6	**aaa accounting auth-proxy default start-stop group tacacs+** **Example:** `Device(config)# aaa accounting auth-proxy default start-stop group tacacs+`	Activates authentication proxy accounting. The **auth-proxy** keyword sets up the authorization policy as dynamic ACLs that can be downloaded.
Step 7	**tacacs-server host** *hostname* **Example:** `Device(config)# tacacs-server host host1`	Specifies an AAA server. For RADIUS servers, use the **radius server host** command.
Step 8	**tacacs-server key** *key* **Example:** `Device(config)# tacacs-server key key1`	Sets the authentication and encryption key for communications between the device and the AAA server. For RADIUS servers use the **radius server key** command.
Step 9	**access-list** *access-list-number* **Example:** `Device(config)# access-list accesslist1`	Creates an ACL entry to allow the AAA server to return traffic to the firewall.

What to Do Next

In addition to configuring AAA on the firewall device, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service **auth-proxy** on the AAA server as outlined here:

- Define a separate section of authorization for the **auth-proxy** keyword to specify the downloadable user profiles. This keyword does not interfere with other type of services, such as EXEC. The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
service = auth-proxy
{
```

```
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 10.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
}
}
```

- The only supported attribute in the AAA server user configuration is proxyacl#n.Use the proxyacl#n attribute when configuring the access lists in the profile. The attribute proxyacl#n is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.
- The access lists in the user profile on the AAA server must have access commands that contain only the **permit**keyword.
- Set the source address to the **any**keyword in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are:
  - CiscoSecure ACS 2.1.x for Windows NT
  - CiscoSecure ACS 2.3 for Windows NT
  - CiscoSecure ACS 2.2.4 for UNIX
  - CiscoSecure ACS 2.3 for UNIX
  - TACACS+ server (vF4.02.alpha)
  - Ascend RADIUS server radius-980618 (required attribute-value pair patch)
  - Livingston RADIUS server (v1.16)

What to Do Next

What to Do Next

In addition to configuring AAA on the firewall device, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service **auth-proxy** on the AAA server as outlined below.

Define a separate section of authorization for the **auth-proxy** keyword to specify the downloadable user profiles. This keyword does not interfere with other type of services, such as EXEC.

The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
service = auth-proxy
{
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 10.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
```

```
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
}
}
```

Note the following points:

- The only supported attribute in the AAA server user configuration is proxyacl#n.Use the proxyacl#n attribute when configuring the access lists in the profile. The attribute proxyacl#n is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.
- The access lists in the user profile on the AAA server must have access commands that contain only the **permit** keyword.
- Set the source address to the **any** keyword in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are:
  - CiscoSecure ACS 2.1.x for Windows NT
  - CiscoSecure ACS 2.3 for Windows NT
  - CiscoSecure ACS 2.2.4 for UNIX
  - CiscoSecure ACS 2.3 for UNIX
  - TACACS+ server (vF4.02.alpha)
  - Ascend RADIUS server radius-980618 (required attribute-value pair patch)
  - Livingston RADIUS server (v1.16)

Configuring the HTTP Server for Authentication Proxy

This task is used to enable the HTTP server on the firewall and configure the HTTP server's AAA authentication method for authentication proxy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http access-class** *access-list-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip http server** **Example:** `Device# ip http server`	Enables the HTTP server on the device.
Step 4	**ip http access-class** *access-list-number* **Example:** `Device(config)# ip http access-class 20`	Specifies the access list for the HTTP server.

Configuring the Authentication Proxy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip auth-proxy auth-cache-time** *min*
4. **ip auth-proxy auth-proxy-banner**
5. **ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl acl-name*}]
6. **interface** *type number*
7. **ip auth-proxy** *auth-proxy-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip auth-proxy auth-cache-time** *min* **Example:** `Device(config)# ip auth-proxy auth-cache-time 5`	(Optional) Sets the global authentication proxy idle timeout value in minutes.
Step 4	**ip auth-proxy auth-proxy-banner** **Example:** `Device(config)# ip auth-proxy auth-proxy-banner`	(Optional) Displays the name of the firewall router in the authentication proxy login page. The banner is disabled by default.
Step 5	**ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl acl-name*}] **Example:** `Device(config)# ip auth-proxy name HQ_users http`	Creates authentication proxy rules.
Step 6	**interface** *type number* **Example:** `Device(config)# interface Ethernet0/0`	Enters interface configuration mode by specifying the interface type and number on which to apply the authentication proxy.
Step 7	**ip auth-proxy** *auth-proxy-name* **Example:** `Device(config-if)# ip auth-proxy HQ_users http`	Applies the named authentication proxy rule at the interface.

Verifying Authentication Proxy

Checking the Authentication Proxy Configuration

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip auth-proxy configuration** **Example:** `Device# show ip auth-proxy configuration`	Displays the authentication proxy configuration.

Example: Checking the Authentication Proxy Configuration

In the following example, the global authentication proxy idle timeout value is set to 60 minutes, the named authentication proxy rule is “pxy”, and the idle timeout value for this named rule is one minute. The display shows that no host list is specified, meaning that all connections initiating HTTP traffic at the interface are subject to the authentication proxy rule.

```
Device# show ip auth-proxy configuration

Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 1 minutes
```

Displaying the User Authentication Entries

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip auth-proxy cache** **Example:** `Device# show ip auth-proxy cache`	Displays the list of user authentication entries.

Example: Displaying the 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 HTTP_ESTAB, the user authentication was successful.

```
Device# show ip auth-proxy cache

Authentication Proxy Cache
 Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

Wait for one minute, which is the timeout value for this named rule, and ask the user to try the connection again. After one minute, the user connection is denied because the authentication proxy has removed the user's authentication entry and any associated dynamic ACLs. The user is presented with a new authentication login page and must log in again to gain access through the firewall.

Establishing User Connections with JavaScript

To establish user connections using the authentication proxy with JavaScript enabled on the client browser, follow this procedure.

SUMMARY STEPS

1. From a client host, initiate an HTTP connection through the firewall. This generates the authentication proxy login page.
2. At the authentication proxy login page, enter a username and password.
3. Click **OK** to submit the username and password to the AAA server.

DETAILED STEPS

Step 1 From a client host, initiate an HTTP connection through the firewall. This generates the authentication proxy login page.

Step 2 At the authentication proxy login page, enter a username and password.

Step 3 Click **OK** to submit the username and password to the AAA server.

A popup window appears indicating whether the login attempt succeeded or failed. If the authentication is successful, the connection is completed automatically. If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries.

What to Do Next

Note If the authentication attempt is unsuccessful after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

Establishing User Connections Without JavaScript

To ensure secure authentication, the authentication proxy design requires JavaScript. You can use the authentication proxy without enabling JavaScript on the browser, but this poses a potential security risk if users do not properly establish network connections. The following procedure provides the steps to properly establish a connection with JavaScript disabled. Network administrators are strongly advised to instruct users on how to properly establish connections using the procedure in this section.

Note Failure to follow this procedure can cause user credentials to be passed to a network web server other than the authentication proxy or can cause the authentication proxy to reject the login attempt.

To verify client connections using the authentication proxy when JavaScript is not enabled on the client browser, follow this procedure:

SUMMARY STEPS

1. Initiate an HTTP connection through the firewall.
2. From the authentication proxy login page at the client, enter the username and password.
3. Click **OK** to submit the username and password to the AAA server.
4. If the popup window displays a failed authentication message, click **Close** on the browser **File** menu.
5. From the original authentication login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar. The user login credentials are cleared from the form.
6. Enter the username and password again.
7. Click **Close** on the browser **File** menu.
8. From the original authentication proxy login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar.

DETAILED STEPS

Step 1 Initiate an HTTP connection through the firewall.
This generates the authentication proxy login page.

Step 2 From the authentication proxy login page at the client, enter the username and password.

Step 3 Click **OK** to submit the username and password to the AAA server.
A popup window appears indicating whether the login attempt succeeded or failed. If the popup window indicates successful authentication, go to Step7.

Step 4 If the popup window displays a failed authentication message, click **Close** on the browser **File** menu.
Note Do not click **Reload** (**Refresh** for Internet Explorer) to close the popup window.

Step 5 From the original authentication login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar. The user login credentials are cleared from the form.

Note Do not click **OK**. You must click **Reload** or **Refresh** to clear the username and password and to reload the form before attempting to log in again.

Step 6 Enter the username and password again.
If the authentication is successful, a window appears displaying a successful authentication message. If the window displays a failed authentication message, go to Step 4.

Step 7 Click **Close** on the browser **File** menu.

Step 8 From the original authentication proxy login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar. The authentication proxy completes the authenticated connection with the web server.

Monitoring and Maintaining Authentication Proxy

Displaying Dynamic ACL Entries

You can display dynamic access list entries when they are in use. After an authentication proxy entry is cleared by you or by the idle timeout parameter, you can no longer display it. The number of matches displayed indicates the number of times the access list entry was hit.

To view dynamic access lists and any temporary access list entries that are currently established by the authentication proxy, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show ip access-lists**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip access-lists** **Example:** `Device# show ip access-lists`	Displays the standard and extended access lists configured on the firewall, including dynamic ACL entries.

Example: Displaying Dynamic ACL Entries

Consider the following example where ACL 105 is applied inbound at the input interface where you configure authentication proxy. The initial display shows the contents of the ACLs prior to authentication. The second display shows the same displays after user authentication with the AAA server.

Note If NAT is configured, the **show ip access-lists** command might display the translated host IP address for the dynamic ACL entry or the IP address of the host initiating the connection. If the ACL is applied on the NAT outside interface, the translated address is displayed. If the ACL is applied on the NAT inside interface, the IP address of the host initiating the connection is displayed. The **show ip auth-proxy cache** command always displays the IP address of the host initiating the connection.

For example, the following is a list of ACL entries prior to the authentication proxy:

```
Device# show ip access-lists
    .
    .
    .
Extended IP access list 105
 deny tcp any any eq telnet
 deny udp any any
 permit tcp any any (28 matches)
 permit ip any any
```

The following sample output shows a list of ACL entries following user authentication:

```
Device# show ip access-lists
    .
    .
    .
Extended IP access list 105
! The ACL entries following user authentication are shown below.
 permit tcp host 192.168.25.215 any eq 26
 permit icmp host 192.168.25.215 host 10.0.0.2
 permit tcp host 192.168.25.215 any eq telnet
 permit tcp host 192.168.25.215 any eq ftp
 permit tcp host 192.168.25.215 any eq ftp-data
 permit tcp host 192.168.25.215 any eq smtp
 deny tcp any any eq telnet
 deny udp any any
 permit tcp any any (76 matches)
 permit ip any any
```

Deleting Authentication Proxy Cache Entries

When the authentication proxy is in use, dynamic access lists dynamically grow and shrink as authentication proxy cache entries are added and deleted. To manually delete an authentication proxy cache entry, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **clear ip auth-proxy cache** {***** | *host-ip-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip auth-proxy cache** {* | *host-ip-address*} **Example:** `Device# clear ip auth-proxy cache *`	Deletes authentication proxy entries from the firewall before they time out. Enter an asterisk to delete all authentication cache entries. Enter a specific IP address to delete an entry for a single host.

Configuration Examples for Authentication Proxy

Example: Authentication Proxy Configuration

The following examples highlight the specific authentication proxy configuration entries. These examples do not represent a complete configuration. Complete configurations using the authentication proxy are included later in this module.

Example: AAA Configuration

```
aaa new-model
aaa authentication login default group tacacs group radius
! Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default group tacacs group radius
! Define the AAA servers used by the router.
aaa accounting auth-proxy default start-stop group tacacs+
! Set up authentication proxy with accounting.
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
```

Example: HTTP Server Configuration

```
! Enable the HTTP server on the router.
ip http server
! Set the HTTP server authentication method to AAA.
ip http authentication aaa
! Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
```

Example: Authentication Proxy Configuration

```
! Set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
! Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
```

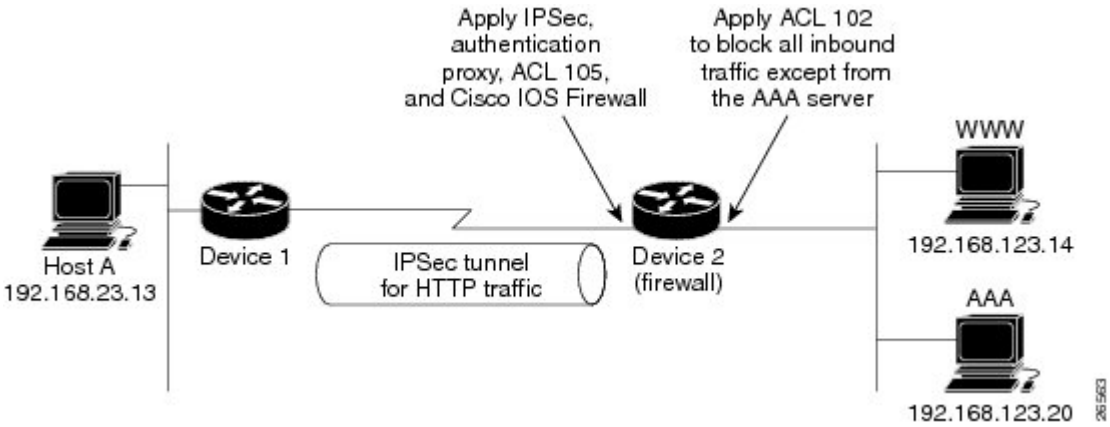
Example: Interface Configuration

```
! Apply the authentication proxy rule at an interface.
interface ethernet0
ip address 10.1.1.210 255.255.255.0
ip auth-proxy HQ_users
```

Example: Authentication Proxy, IPsec, and CBAC Configuration

The following example shows a configuration with the authentication proxy, IPsec, and CBAC features enabled. The figure below illustrates the configuration.

Figure 6: Authentication Proxy, IPsec, and CBAC Configuration Example



In this example, Host A initiates an HTTP connection with the web server (WWW). The HTTP traffic between Device 1 and Device 2 is encrypted using IPsec. The authentication proxy, IPsec, and CBAC are configured at Serial interface 0 on Device 2, which is acting as the firewall. ACL 105 blocks all traffic at interface Serial0. ACL 102 is applied at Ethernet interface 0 on Device 2 to block all traffic on that interface except traffic from the AAA server.

When Host A initiates an HTTP connection with the web server, the authentication proxy prompts the user at Host A for a username and password. These credentials are verified with the AAA server for authentication and authorization. If authentication is successful, the per-user ACLs are downloaded to the firewall to permit services.

Example: Device 1 Configuration

```
! Configure Device 1 for IPSec.
```

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Device1
!
logging buffered 4096 debugging
no logging console
enable secret 5 $1$E0OB$AQF1vFZM3fLr3LQAOsudL/
enable password junk
!
username Device2 password 0 welcome
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.2
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
!
 crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set rule_1
 match address 155
!
interface Ethernet0/0
 ip address 192.168.23.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Serial3/1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation PPP
 ip route-cache
 no ip mroute-cache
 no keepalive
 no fair-queue
 clockrate 56000
 crypto map testtag
!
!
ip classless
ip route 192.168.123.0 255.255.255.0 10.0.0.2
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.23.13 host 192.168.123.14 eq www
access-list 155 permit tcp host 192.168.23.13 eq www host 192.168.123.14
```

Example: Device 2 Configuration

```
! Configure Device 2 as the firewall, using the authentication proxy, IPSec, and CBAC.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Device2
!
logging buffered 4096 debugging
aaa new-model
aaa authentication login default group tacacs
aaa authentication login console_line none
aaa authentication login special none
aaa authentication ppp default group tacacs
aaa authorization exec default group tacacs
! Configure AAA for the authentication proxy.
aaa authorization auth-proxy default group tacacs+
enable password junk
!
```

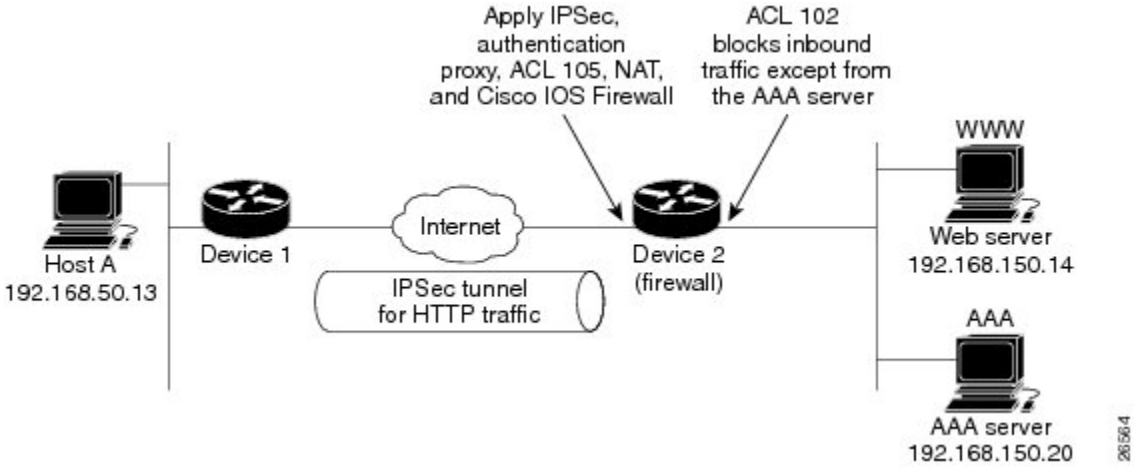
```
! Create the CBAC inspection rule HTTP_TEST.
ip inspect name rule22 http
ip inspect name rule22 tcp
ip inspect name rule22 ftp
ip inspect name rule22 smtp
!
! Create the authentication proxy rule PXY.
ip auth-proxy name pxy http
! Turn on display of the device name in the authentication proxy login page.
ip auth-proxy auth-proxy-banner
ip audit notify log
ip audit po max-events 100
!
! Configure IPSec.
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.1
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
 crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set rule_1
 match address 155
!
! Apply the CBAC inspection rule and the authentication proxy rule at serial interface 0/0
!
interface Serial0/0
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect rule22 in
 ip auth-proxy pxy
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 no keepalive
 no fair-queue
crypto map testtag
!
interface Ethernet0/1
 ip address 192.168.123.2 255.255.255.0
 ip access-group 102 in
 no ip directed-broadcast
 ip route-cache
 no ip mroute-cache
!
no ip classless
ip route 192.168.23.0 255.255.255.0 10.0.0.1
ip route 192.168.50.0 255.255.255.0 16.0.0.1
! Configure the HTTP server.
ip http server
ip http access-class 15
ip http authentication aaa
!
! Create ACL 15 to block all traffic for the http server.
access-list 15 deny any
! Create ACL 102 to block all traffic inbound on Ethernet interface 0/1 except for
! traffic from the AAA server.
access-list 102 permit tcp host 192.168.123.20 eq tacacs host 192.168.123.2
access-list 102 deny   tcp any any
access-list 102 deny   udp any any
access-list 102 permit ip any any
! Create ACL 105 to block all traffic inbound on Serial interface 0/0. Permit only IP
! protocol traffic.
access-list 105 deny   tcp any any
access-list 105 deny   udp any any
access-list 105 permit ip any any
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.123.14 host 192.168.23.13 eq www
access-list 155 permit tcp host 192.168.123.14 eq www host 192.168.23.13
!
! Define the AAA server host and encryption key.
```

```
tacacs-server host 192.168.123.14
tacacs-server key cisco
!
line con 0
 exec-timeout 0 0
 login authentication special
 transport input none
line aux 0
 transport input all
 speed 38400
 flowcontrol hardware
line vty 0 4
 password lab
```

Example: Authentication Proxy, IPsec, NA,T and CBAC Configuration

The following is a sample configuration with the authentication proxy, IPsec, NAT, and CBAC features enabled. The figure below illustrates the configuration.

Figure 7: Authentication Proxy, IPsec, NAT, and CBAC Configuration Example



In this example, Host A initiates an HTTP connection with the web server (WWW). The HTTP traffic between device 1 (BRI interface 0) and device 2 (Serial interface 2) is encrypted using IPsec. The authentication proxy is configured on device 2, which is acting as the firewall. The authentication proxy, NAT, and CBAC are configured at Serial interface 2, which is acting as the firewall. ACL 105 blocks all traffic at Serial interface 2. ACL 102 is applied at Ethernet interface 0 on device 2 to block all traffic on that interface except traffic from the AAA server. In this example, the authentication proxy uses standard ACL 10 to specify the hosts using the Authentication Proxy feature.

When any host in ACL 10 initiates an HTTP connection with the web server, the authentication proxy prompts the user at that host for a username and password. These credentials are verified with AAA server for authentication and authorization. If authentication is successful, the per-user ACLs are downloaded to the firewall to permit services.

Example: Device 1 Configuration

```
! Configure device 1 for IPSec.
version 12.0
```

```
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Device1
 !
 logging buffered 4096 debugging
 no logging console
 !
isdn switch-type basic-5ess
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco1234 address 10.0.0.2
 crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
 !
  !
  crypto map testtag 10 ipsec-isakmp
  set peer 10.0.0.2
  set transform-set rule_1
  match address 155
 !
 !
 process-max-time 200
 !
 interface BRI0
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  encapsulation ppp
  dialer idle-timeout 5000
  dialer map ip 10.0.0.2 name router2 broadcast 50006
  dialer-group 1
  isdn switch-type basic-5ess
  crypto map testtag
 !
 interface FastEthernet0
  ip address 192.168.50.2 255.255.255.0
  no ip directed-broadcast
 !
 ip classless
 ip route 192.168.150.0 255.255.255.0 10.0.0.2
 no ip http server
! Identify the IPSec specific traffic.
 access-list 155 permit tcp host 192.168.50.13 host 192.168.150.100 eq www
 access-list 155 permit tcp host 192.168.50.13 eq www host 192.168.150.100
 dialer-list 1 protocol ip permit
 !
 line con 0
  exec-timeout 0 0
  transport input none
 line aux 0
 line vty 0 4
  password lab
  login
```

Example: Device 2 Configuration

```
! Configure device 2 as the firewall, using the authentication proxy, IPSec, NAT, and
! CBAC.
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname device2
 !
 logging buffered 4096 debugging
 aaa new-model
 aaa authentication login default group tacacs+
 aaa authentication login console_line none
```

```
 aaa authorization exec default group tacacs+
 ! Configure AAA for the authentication proxy.
 aaa authorization auth-proxy default group tacacs+
!
 ! Create the CBAC inspection rule “rule44.”
 ip inspect name rule44 http java-list 5
 ip inspect name rule44 tcp
 ip inspect name rule44 ftp
 ip inspect name rule44 smtp
 !
 ! Create the authentication proxy rule “pxy.” Set the timeout value for rule
 ! pxy to three minutes. Standard ACL 10 is applied to the rule.
 ip auth-proxy name pxy http list 10 auth-cache-time 3
 isdn switch-type primary-5ess
 !
 ! Configure IPSec.
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco1234 address 10.0.0.1
 !
 !
 crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
 !
  !
  crypto map testtag 10 ipsec-isakmp
  set peer 10.0.0.1
  set transform-set rule_1
  match address 155
!
 controller T1 2/0
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
! Apply ACL 102 inbound at interface Ethernet0/1 and configure NAT.
interface Ethernet0/1
 ip address 192.168.150.2 255.255.255.0
 ip access-group 102 in
 no ip directed-broadcast
 ip nat inside
 no ip mroute-cache
!
! Apply the authentication proxy rule PXY, CBAC inspection rule HTTP_TEST, NAT, and
! and ACL 105 at interface Serial2/0:23.
interface Serial2/0:23
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
 ip nat outside
 ip inspect rule44 in
 ip auth-proxy pxy
 encapsulation ppp
 ip mroute-cache
 dialer idle-timeout 5000
 dialer map ip 10.0.0.1 name device1 broadcast 71011
 dialer-group 1
 isdn switch-type primary-5ess
 fair-queue 64 256 0
 crypto map testtag
!
! Use NAT to translate the Web server address.
ip nat inside source static 192.168.150.14 192.168.150.100
ip classless
ip route 192.168.50.0 255.255.255.0 10.0.0.1
! Configure the HTTP server.
ip http server
ip http access-class 15
ip http authentication aaa
!
! Create standard ACL 5 to specify the list of hosts from which to accept java applets.
! ACL 5 is used to block Java applets in the CBAC inspection rule named “rule44,” which
! is applied at interface Serial2/0:23.
```

```
access-list 5 permit any
! Create standard ACL 10 to specify the hosts using the authentication proxy. This ACL
! used in the authentication proxy rule named “PXY”, which is applied at interface
! Serial2/0:23.
access-list 10 permit any
! Create ACL 15 to block all traffic for the http server.
access-list 15 deny any
! Create extended ACL 102 to block all traffic inbound on interface Ethernet0/1
! except for traffic from the AAA server.
access-list 102 permit tcp host 192.168.150.20 eq tacacs 192.168.150.2
access-list 102 deny   tcp any any
access-list 102 deny   udp any any
access-list 102 permit ip any any
! Create extended ACL 105 to block all TCP and UDP traffic inbound on interface
! Serial2/0:23.
access-list 105 deny   tcp any any
access-list 105 deny   udp any any
access-list 105 permit ip any any
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.150.100 host 192.168.50.13 eq www
access-list 155 permit tcp host 192.168.150.100 eq www host 192.168.50.13
dialer-list 1 protocol ip permit
! Define the AAA server host and encryption key.
tacacs-server host 192.168.126.14
tacacs-server key cisco
!
line con 0
 exec-timeout 0 0
! Define the AAA server host and encryption key.
 login authentication console_line
 transport input none
 line aux 0
 line vty 0 4
 password lab
!
!
 end
```

Example: AAA Server User Profile

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.

Example: CiscoSecure ACS 2.3 for Windows NT

This section describes how to configure authentication proxy on CiscoSecure ACS 2.3 for Windows NT. For detailed information about CiscoSecure ACS, refer to the documentation for that product.

The following sample configuration is for the TACACS+ service of CiscoSecure ACS for Windows NT.

SUMMARY STEPS

1. Click the Interface Configuration icon and click **TACACS+** (Cisco).
2. Click the Network Configuration icon.
3. Click the Group Setup icon.
4. Click the User Setup icon.
5. Click Group Setup icon again.

DETAILED STEPS

Step 1 Click the Interface Configuration icon and click **TACACS+** (Cisco).

a) Scroll down to New Services.
b) Add a new service, “auth-proxy”, in the Service field. Leave the Protocol field empty.
c) Select both the User and Group check boxes for the new service.
d) Scoll down to Advance Configuration Options and check the Per-user Advance TACACS+ features.
e) Click **Submit**.

Step 2 Click the Network Configuration icon.

a) Click the Add Entry icon for Network Access Servers and fill in the Network Access Server Hostname, IP address, and key (the key configured on the router) fields.
b) Select TACACS+ (Cisco) for the Authenticate Using option.
c) Click the Submit + Restart icon.

Step 3 Click the Group Setup icon.

a) Select a user group from the drop-down menu.
b) Select the Users in Group check box.
c) Select a user from the user list.
d) In the User Setup list, scroll down to TACACS+ Settings and select the “auth-proxy” check box.
e) Select the Custom Attributes check box.
f) Add the profile entries (do not use single or double quotes around the entries) and set the privilege level to 15.

Example:

```
priv-lvl=15
proxyacl#1=permit tcp any any eq 26
proxyacl#2=permit icmp any host 10.0.0.2
proxyacl#3=permit tcp any any eq ftp
proxyacl#4=permit tcp any any eq ftp-data
proxyacl#5=permit tcp any any eq smtp
proxyacl#6=permit tcp any any eq telnet
```

g) Click **Submit**.

Step 4 Click the User Setup icon.

a) Click **List All Users**.
b) Add a username.
c) Scoll down to User Setup Password Authentication.
d) Select SDI SecurID Token Card from the Password Authentication drop-down menu.
e) Select the previous configured user group 1.

f) Click **Submit**.

Step 5 Click Group Setup icon again.

a) Select the user group 1.
b) Click **Users in Group**.
c) Click **Edit Settings**.
d) Click the Submit + Restart icon to make sure the latest configuration is updated and sent to the AAA server.

Example: CiscoSecure ACS 2.3 for UNIX

This section describes how to configure authentication proxy on CiscoSecure ACS 2.3 for UNIX. For detailed information regarding CiscoSecure ACS, refer to the documentation for that product.

To manage the CiscoSecure ACS using the Administrator program, you need a web browser that supports Java and JavaScript. You must enable Java in the browser application. You can start the Java-based CiscoSecure Administrator advanced configuration program from any of the CiscoSecure ACS Administrator web pages.

The following sample configuration procedure is for the TACACS+ service of CiscoSecure ACS 2.3 for UNIX.

SUMMARY STEPS

1. On the CiscoSecure ACS web menu bar of the CiscoSecure ACS web interface, click **Advanced** and then click **Advanced** again.
2. In the CiscoSecure Administrator advanced configuration program, locate and deselect Browse in the Navigator pane of the tabbed Members page.
3. In the Navigator pane, do one of the following:
4. Click **Create Profile** to display the New Profile dialog box.
5. Make sure the Group check box is cleared.
6. Enter the name of the user you want to create and click **OK**. The new user appears in the tree.
7. Click the icon for the group or user profile in the tree that is displayed in the Navigator pane of the tabbed Members page.
8. If necessary, in the Profile pane, click the Profile icon to expand it.
9. Click **Service-String**.
10. Click **string**, enter **auth-proxy** in the text field, and click **Apply**.
11. Select the Option menu.
12. On the Option menu, click **Default Attributes**.
13. Change the attribute from Deny to **Permit**.
14. Click **Apply**.
15. On the Option menu, click **Attribute** and enter the privilege level in the text field:
16. On the Option menu, click **Attribute** and enter the **proxyacl** entries in the text field:
17. When you have finished making all your changes, click **Submit**.

DETAILED STEPS

Step 1 On the CiscoSecure ACS web menu bar of the CiscoSecure ACS web interface, click **Advanced** and then click **Advanced** again.
The Java-based CiscoSecure Administrator advanced configuration program appears. It might require a few minutes to load.

Step 2 In the CiscoSecure Administrator advanced configuration program, locate and deselect Browse in the Navigator pane of the tabbed Members page.
This displays the Create New Profile icon.

Step 3 In the Navigator pane, do one of the following:

- Locate and click the group to which the user will belong.
- If you do not want the user to belong to a group, click the [Root] folder icon.

Step 4 Click **Create Profile** to display the New Profile dialog box.

Step 5 Make sure the Group check box is cleared.

Step 6 Enter the name of the user you want to create and click **OK**. The new user appears in the tree.

Step 7 Click the icon for the group or user profile in the tree that is displayed in the Navigator pane of the tabbed Members page.

Step 8 If necessary, in the Profile pane, click the Profile icon to expand it.
A list or dialog box that contains attributes applicable to the selected profile or service appears in the window at the bottom right of the screen. The information in this window changes depending on what you have selected in the Profile pane.

Step 9 Click **Service-String**.

Step 10 Click **string**, enter **auth-proxy** in the text field, and click **Apply**.

Step 11 Select the Option menu.

Step 12 On the Option menu, click **Default Attributes**.

Step 13 Change the attribute from Deny to **Permit**.

Step 14 Click **Apply**.

Step 15 On the Option menu, click **Attribute** and enter the privilege level in the text field:

Example:

```
priv-lvl=15
```

Step 16 On the Option menu, click **Attribute** and enter the **proxyacl** entries in the text field:

Example:

```
proxyacl#1="permit tcp any any eq 26"
```

Repeat this step for each additional service or protocol to add:

Example:

```
proxyacl#2=”permit icmp any host 10.0.0.2”
proxyacl#3=”permit tcp any any eq ftp”
proxyacl#4=”permit tcp any any eq ftp-data”
proxyacl#5=”permit tcp any any eq smtp”
proxyacl#6=”permit tcp any any eq telnet”
```

Step 17 When you have finished making all your changes, click **Submit**.

Example: TACACS+ Server

```
default authorization = permit
key = cisco
user = Brian {
login = cleartext cisco
service = auth-proxy
 {
  priv-lvl=15
  proxyacl#1="permit tcp any any eq 26"
  proxyacl#2="permit icmp any host 10.0.0.2
  proxyacl#3="permit tcp any any eq ftp"
  proxyacl#4="permit tcp any any eq ftp-data"
  proxyacl#5="permit tcp any any eq smtp"
  proxyacl#6="permit tcp any any eq telnet"
 }
}
```

Example: Livingston Radius Server

```
Bob Password = "cisco" User-Service-Type=Outbound-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#2=permit icmp any host 10.0.0.2",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq ftp-data",
cisco-avpair = "auth-proxy:proxyacl#5=permit tcp any any eq smtp",
cisco-avpair = "auth-proxy:proxyacl#6=permit tcp any any eq telnet"
```

Example: Ascend Radius Server

```
Alice Password = "cisco" User-Service = Dialout-Framed-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#2=permit icmp any host 10.0.0.2",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq ftp-data",
cisco-avpair = "auth-proxy:proxyacl#5=permit tcp any any eq smtp",
cisco-avpair = "auth-proxy:proxyacl#6=permit tcp any any eq telnet"
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication, authorization, and accounting	*Authentication, Authorization, and Accounting (AAA) Configuration Guide*
Access lists and the Cisco IOS Firewall	"Access Control Lists: Overview and Guidelines" module of the *Security Configuration Guide: Access Control Lists* publication.
Context-Based Access Control (CBAC)	"Configuring Context-Based Access Control" module of the *Security Guide Publication: Context-Based Access Control Firewall*
RADIUS	*RADIUS Configuration Guide* *RADIUS Attributes Configuration Guide* *General RADIUS Configurations Configuration Guide*
TACACS+	*TACACS+ Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

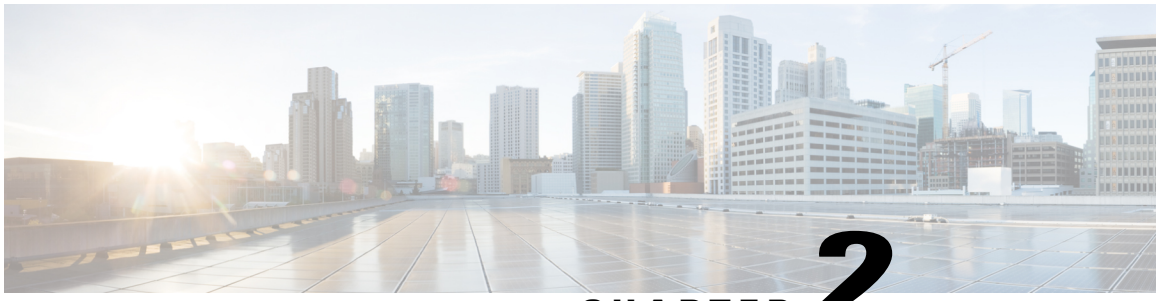
Feature Information for Authentication Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Authentication Proxy

Feature Name	Releases	Feature Information
Cisco IOS Firewall Authentication Proxy	12.1(5)T	The Cisco IOS Firewall Authentication Proxy feature provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks.
Web Authentication with Critical Authentication Support	15.2(2)T	The AAA fail policy is a method for allowing a user to connect or to remain connected to the network if the AAA server is not available. AAA Fail Policy
Web Authentication Enhancements	15.2(2)T	Substitute your custom HTML pages for the four default internal HTML pages or specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success page. Customization of the Authentication Proxy Web Pages



CHAPTER 2

Customizing Authentication Proxy Web Pages

The Customization of Authentication Proxy Web Pages feature allows you to provide four substitute HTML pages to be displayed to the user in place of the switch's internal default HTML pages during web-based authentication. The four pages are Login, Success, Fail, and Expire.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Customization of Authentication Proxy Web Pages

The switch's internal HTTP server hosts four HTML pages for delivery to an authenticating client during the web-based authentication process. The four pages allow the server to notify the user of the following four states of the authentication process:

- Login—The user's credentials are requested.
- Success—The login was successful.

- Fail—The login has failed.
- Expire—The login session has expired due to excessive login failures.

You can substitute your custom HTML pages for the four default internal HTML pages or you can specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success page.

How to Configure Custom Authentication Proxy Web Pages

Configuring the Custom Authentication Proxy Web Pages

To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch's internal disk or flash memory and then perform this task.

Before You Begin

Note To enable the custom web pages feature, you must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages will be used.

- The four custom HTML files must be present on the disk or flash of the switch.
- An image file has a size limit of 256 KB. All image files must have a filename that begins with “web_auth_” (such as “web_auth_logo.jpg” instead of “logo.jpg”).
- All image file names must be less than 33 characters.
- Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.
- Any external link from a custom page will require configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.
- If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http login page file** *device:login-filename*
4. **ip admission proxy http success page file** *device:success-filename*
5. **ip admission proxy http failure page file** *device:fail-filename*
6. **ip admission proxy http expired page file** *device:expired-filename*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip admission proxy http login page file** *device:login-filename* **Example:** `Device(config)# ip admission proxy http login page file disk1:login.htm`	Specifies the location in the switch memory file system of the custom HTML file to be used in place of the default login page. The device: is either disk or flash memory, such as disk0:.
Step 4	**ip admission proxy http success page file** *device:success-filename* **Example:** `Device(config)# ip admission proxy http success page file disk1:success.htm`	Specifies the location of the custom HTML file to be used in place of the default login success page.
Step 5	**ip admission proxy http failure page file** *device:fail-filename* **Example:** `Device(config)# ip admission proxy http failure page file disk1:fail.htm`	Specifies the location of the custom HTML file to be used in place of the default login failure page.

	Command or Action	Purpose
Step 6	**ip admission proxy http expired page file** *device:expired-filename* **Example:** `Device(config)# ip admission proxy http expired page file disk1:expired.htm`	Specifies the location of the custom HTML file to be used in place of the default login expired page.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Specifying a Redirection URL for Successful Login

To specify a redirection URL for successful login, perform this task.

Before You Begin

Note You can specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success HTML page.

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available. You can perform redirection in the custom login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http success redirect** *url-string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip admission proxy http success redirect** *url-string* **Example:** `Device(config)# ip admission proxy http success redirect www.company.com`	Specifies a URL for redirection of the user in place of the default login success page.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying the Configuration of Custom Authentication Proxy Web Pages

Perform this task to verify the configuration of custom authentication proxy web pages and the redirection URL for successful login:

SUMMARY STEPS

1. **enable**
2. **show ip admission configuration**
3. **show ip admission configuration**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show ip admission configuration**

Displays the configuration of custom authentication proxy web pages.

Example:

```
Device# show ip admission configuration

Authentication proxy webpage
 Login page           : disk1:login.htm
 Success page         : disk1:success.htm
 Fail Page            : disk1:fail.htm
 Login expired Page   : disk1:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Step 3 **show ip admission configuration**

Displays the configuration of custom authentication proxy web pages.

Example:

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.company.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Configuration Examples for Customization of Authentication Proxy Web Pages

Example: Configuring Custom Authentication Web Pages

```
Device> enable
Device# configure terminal
Device(config)# ip admission proxy http login page file disk1:login.htm
Device(config)# ip admission proxy http success page file disk1:success.htm
Device(config)# ip admission proxy http failure page file disk1:fail.htm
Device(config)# ip admission proxy http expired page file disk1:expired.htm
Device(config)# end
```

Example: Configuring a Redirection URL for Successful Login

```
Device> enable
Device# configure terminal
Device(config)# ip admission proxy http success redirect www.company.com
Device(config)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication, authorization, and accounting	*Authentication, Authorization, and Accounting (AAA) Configuration Guide*
Access lists and the Cisco IOS Firewall	"Access Control Lists: Overview and Guidelines" module of the *Security Configuration Guide: Access Control Lists* publication.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

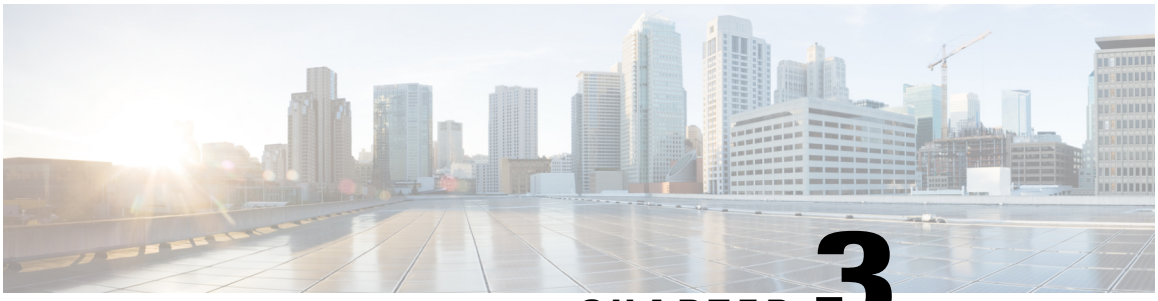
Feature Information for Customization of Authentication Proxy Web Pages

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Customization of Authentication Proxy Web Pages

Feature Name	Releases	Feature Information
Web Authentication Enhancements - Customization of Authentication Proxy Web Pages	15.2(2)T	The Customization of Authentication Proxy Web Pages feature allows you to provide four substitute HTML pages to be displayed to the user in place of the switch's internal default HTML pages during web-based authentication. The four pages are Login, Success, Fail, and Expire.



CHAPTER 3

Consent Feature for Cisco IOS Routers

The Consent Feature for Cisco IOS Routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent web page. This web page lists the terms and conditions according to which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent web page.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Consent Feature for Cisco IOS Routers

- To enable a consent web page, you must be running an Advanced Enterprise image.
- You must use one of the following options to enable the Consent feature if you configure the **ip http secure-server** command.

- Configure the **ip admission virtual-ip** command after you configure the **ip http secure-server** command.
- Either install a third-party Secure Socket Layer (SSL) certificate or install the Cisco IOS self-signed certificate as the root certificate in the client. Follow the browser-specific instructions as below:
  - Google Chrome—In the event of certificate errors or warnings, accept the warning and continue the session.
  - Opera—In the event of certificate errors or warnings, accept the warning and continue the session.
  - Windows Internet Explorer 8 (IE8)—Clear the certificate cache and configure the Consent feature.
  - Mozilla Firefox—Install the SSL certificate and configure the Consent feature.

Information About Consent Feature for Cisco IOS Routers

Authentication Proxy Overview

Authentication proxy is an ingress authentication feature that grants access to an end user (out an interface) only if the user submits valid username and password credentials for ingress traffic that is destined for HTTP, Telnet, or FTP. After the submitted authentication credentials have been checked against the credentials that are configured on an Authentication, Authorization, Accounting (AAA) server, access is granted to the requester (source IP address).

When an end user posts an HTTP(S), FTP, or Telnet request on a router's authentication-proxy-enabled ingress interface, the network authenticating device (NAD) verifies whether the same host has already been authenticated. If a session is already present, the ingress request is not authenticated again, and it is subjected to the dynamic (Auth-Proxy) application control engines (ACEs) and the ingress interface ACEs. If an entry is not present, the authentication proxy responds to the ingress connection request by prompting the user for a valid username and password. When authenticated, the network access profiles (NAPs) that are to be applied are either downloaded from the AAA server or taken from the locally configured profiles.

An Integrated Consent-Authentication Proxy Web Page

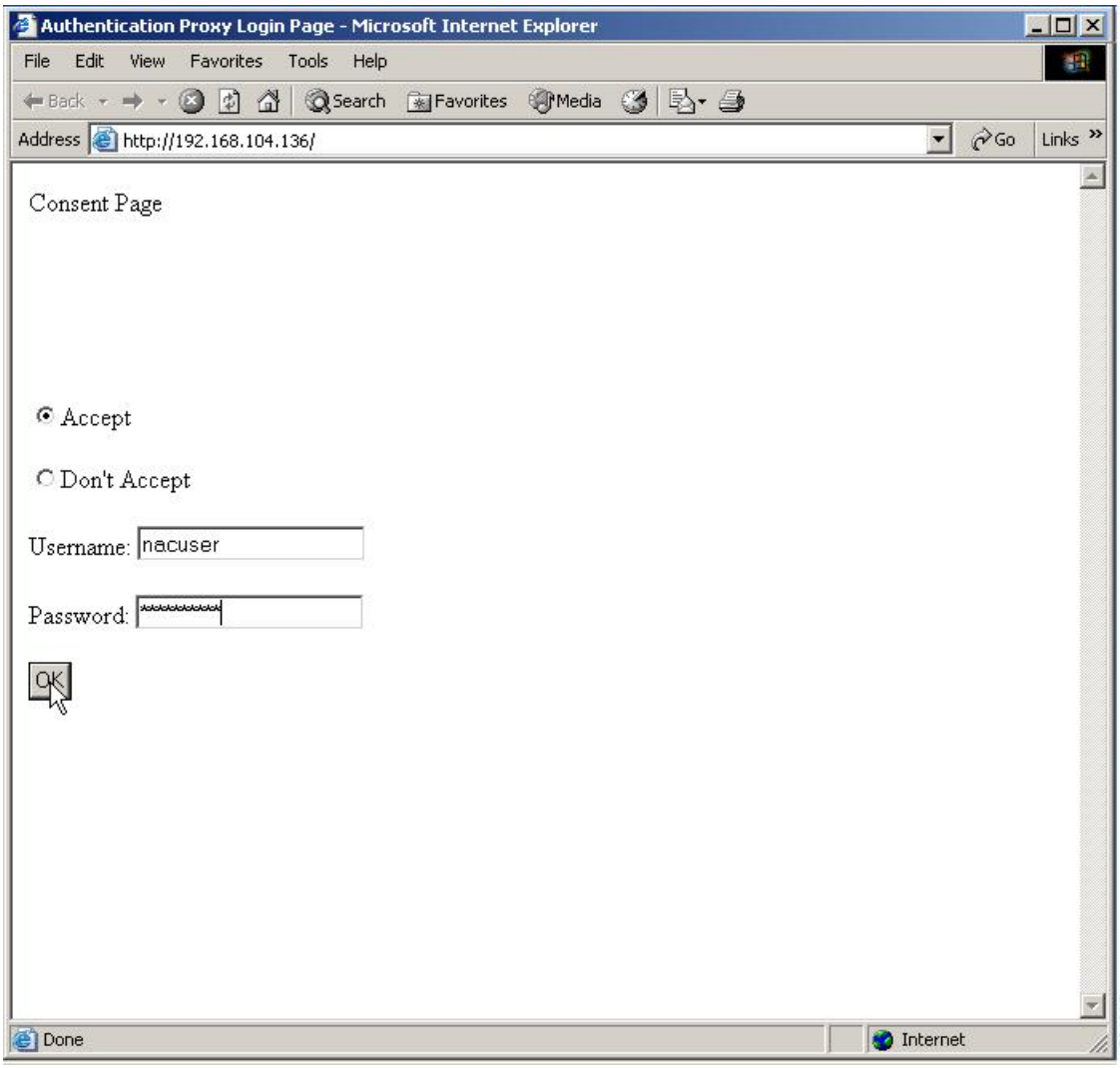
The HTTP authentication proxy web page has been extended to support radio buttons—"Accept" and "Don't Accept"—for the consent web-page feature. The consent web-page radio buttons are followed by the authentication proxy input fields for a username and a password. (See the figure below.)

The following consent scenarios are possible:

- If consent is declined (that is, the "Don't Accept" radio button is selected), the authentication proxy radio buttons are disabled. The ingress client session's access will be governed by the default ingress interface access control list (ACL).
- If consent is accepted (that is, the "Accept" radio button is selected), the authentication proxy radio buttons are enabled. If the wrong username and password credentials are entered, HTTP-Auth-Proxy

authentication will fail. The ingress client session's access will again be governed only by the default ingress interface ACL.

- If consent is accepted (that is, the "Accept" radio button is selected) and valid username and password credentials are entered, HTTP-Auth-Proxy authentication is successful. Thus, one of the following possibilities can occur:
  - If the ingress client session's access request is HTTP_GET, the destination web page will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.
  - If the ingress client session's access request is HTTPS_GET, a "Security Dialogue Box" will be displayed on the client's browser. If the user selects YES on the Security Dialogue Box window, the destination web page will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs. If the user selects NO on the Security Dialogue Box window, the destination page will not open and the user will see the message "Page cannot be displayed." However the ingress client session's access will still be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.



Note When HTTP authentication proxy is configured together with the Consent feature, any HTTP authentication proxy-related configurations or policies will override the Consent page-related configurations or policies. For example, if the **ip admission name** *admission-name* **consent** command is configured, the **ip admission consent banner** command is ignored, and only the banner that is configured by the **ip admission auth-proxy-banner** command is shown.

How to Configure Authentication Proxy Consent

Configuring an IP Admission Rule for Authentication Proxy Consent

Use this task to define the IP admission rule for authentication proxy consent and to associate the rule with an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **consent** [**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]
4. **ip admission consent banner** [**file** *file-name* | **text** *banner-text*]
5. **interface** *type number*
6. **ip admission** *admission-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* **consent** [**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*] **Example:** `Device(config)# ip admission name consent_rule consent absolute-timer 304 inactivity-time 204 list 103 parameter-map consent_parameter_map`	Defines the IP admission rule for authentication proxy consent.
Step 4	**ip admission consent banner** [**file** *file-name* | **text** *banner-text*] **Example:** `Device(config)# ip admission consent banner file flash:consent_page.html`	(Optional) Displays a banner in the authentication proxy consent web page.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 0/0`	Specifies the interface on which the consent IP admission rule will be applied and enters interface configuration mode.
Step 6	**ip admission** *admission-name* **Example:** `Device(config-if)# ip admission consent_rule`	Applies the IP admission rule created in Step 3 to the interface.

Troubleshooting Tips

To display authentication proxy consent page information on the router, use the **debug ip admission consent** command.

```
Device# debug ip admission consent errors

IP Admission Consent Errors debugging is on
Device# debug ip admission consent events

IP Admission Consent Events debugging is on
Device# debug ip admission consent messages

IP Admission Consent Messages debugging is on
Device#
Device# show debugging

IP Admission Consent:
IP Admission Consent Errors debugging is on
IP Admission Consent Events debugging is on
IP Admission Consent Messages debugging is on
```

Defining a Parameter Map for Authentication Proxy Consent

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type consent** *parameter-map-name*
4. **copy** *src-file-name dst-file-name*
5. **file** *file-name*
6. **authorize accept identity** *identity-policy-name*
7. **timeout file download** *minutes*
8. **logging enabled**
9. **end**
10. **show parameter-map type consent** [*parameter-map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type consent** *parameter-map-name* **Example:** `Device(config)# parameter-map type consent consent_parameter_map`	Defines an authentication proxy consent-specific parameter map and enters parameter-map type consent configuration mode. To use a default policy-map, enter **default** for the parameter-map-name.
Step 4	**copy** *src-file-name dst-file-name* **Example:** `Device(config-profile)# copy tftp://192.168.104.136/consent_page.html flash:consent_page.html`	Transfers a file (consent web page) from an external server to a local file system on your device.

	Command or Action	Purpose
Step 5	**file** *file-name* **Example:** `Device(config-profile)# file flash:consent_page.html`	(Optional) Specifies a local filename that is to be used as the consent web page.
Step 6	**authorize accept identity** *identity-policy-name* **Example:** `Device(config-profile)# authorize accept identity consent_identity_policy`	(Optional) Configures an accept policy. **Note** Currently, only an accept policy can be configured.
Step 7	**timeout file download** *minutes* **Example:** `Device(config-profile)# timeout file download 35791`	(Optional) Specifies how often the consent page file should be downloaded from the external TFTP server.
Step 8	**logging enabled** **Example:** `Device(config-profile)# logging enabled`	(Optional) Enables syslog messages.
Step 9	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.
Step 10	**show parameter-map type consent** [*parameter-map-name*] **Example:** `Device# show parameter-map type consent`	(Optional) Displays all configured consent profiles or a specified configured consent profile.

Configuration Examples for Authentication Proxy Consent

Example: Defining the Ingress Interface ACL and Intercept ACL

The following example shows how to define the ingress interface ACL (via the **ip access-list extended 102** command) to which the consent page policy ACEs will be dynamically appended. This example also shows

how to define an intercept ACL (via the **ip access-list extended 103** command) to intercept the interesting ingress traffic by the IP admission consent rule.

```
ip access-list extended 102
 permit ip any 192.168.100.0 0.0.0.255
 permit ip any host 192.168.104.136
 permit udp any any eq bootps
 permit udp any any eq domain
 permit tcp any any eq www
 permit tcp any any eq 443
 permit udp any any eq 443
 exit
!
ip access-list extended 103
 permit ip any host 192.168.104.136
 permit udp any host 192.168.104.132 eq domain
 permit tcp any host 192.168.104.136 eq www
 permit udp any host 192.168.104.136 eq 443
 permit tcp any host 192.168.104.136 eq 443
 exit
!
```

Example: Configuring a Consent Page Policy

The following example shows how to configure the consent page policy ACL and the consent page identity policy:

```
ip access-list extended consent-pg-ip-acc-group
 permit ip any host 192.168.104.128
 permit ip any host 192.168.104.136
 exit
!
identity policy consent_identity_policy
 description ### Consent Page Identity Policy ###
 access-group consent-pg-ip-acc-group
 exit
```

Example: Defining a Parameter Map for Authentication Proxy Consent

The following example shows how to define the consent-specific parameter map “consent_parameter_map” and a default consent parameter map:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

Example: Configuring an IP Admission Consent Rule

The following example shows how to configure an IP admission consent rule, which includes the consent page parameter map as defined in the "Example: Defining a Parameter Map for Authentication Proxy Consent" section:

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 param-map
consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
ip admission virtual-ip
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
 ip access-group 102 in
 ip admission consent-rule
 no shut
 exit
!
interface FastEthernet 0/1
 description ### AAA-DHCP-AUDIT-SERVER-N/W ###
 ip address 192.168.104.170 255.255.255.0
 no shut
 exit
!
line con 0
 exec-timeout 0 0
 login authentication noAAA
 exit
!
line vty 0 15
 exec-timeout 0 0
 login authentication noAAA
 exit
!
```

Additional References for Consent Feature for Cisco IOS Routers

Related Documents

Related Topic	Document Title
Additional authentication proxy configuration tasks	Configuring Authentication Proxy feature module

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/support

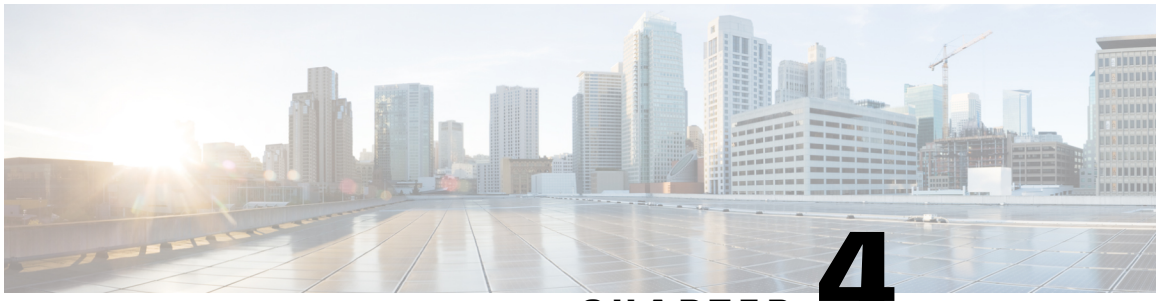
Feature Information for Consent Feature for Cisco IOS Routers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for Consent Feature for Cisco IOS Routers

Feature Name	Releases	Feature Information
Consent Feature for Cisco IOS Routers	12.4(15)T	The Consent Feature for Cisco IOS Routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent web page. This web page lists the terms and conditions according to which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent web page. In Cisco IOS Release 12.4(15)T, this feature was introduced. The following commands were introduced or modified: **authorize accept identity**, **copy (consent-parameter-map)**, **debug ip admission consent**, **file (consent-parameter-map)**, **ip admission consent banner**, **ip admission name**, **logging enabled**, **parameter-map type**, **show ip admission**, **timeout file download**.



CHAPTER 4

Firewall Support of HTTPS Authentication Proxy

The Firewall Support of HTTPS Authentication Proxy feature allows a user to encrypt the change of the username and password between the HTTP client and the Cisco IOS router via Secure Socket Layer (SSL) when authentication proxy is enabled on the Cisco IOS firewall, thereby ensuring confidentiality of the data passing between the HTTP client and the Cisco IOS router.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Firewall Support of HTTPS Authentication Proxy

Before enabling this feature, ensure that your router is running a crypto image with k8 and k9 designations and that your Cisco IOS image supports SSL.

Restrictions for Firewall Support of HTTPS Authentication Proxy

- Although Port to Application Mapping (PAM) configuration is allowed in Cisco IOS Firewall processing, authentication proxy is limited to the server ports that are configured by the HTTP subsystem of the router.
- To conform to a proper TCP connection handshake, the authentication proxy login page will be returned from the same port and address as the original request. Only the postrequest, which contains the username and password of the HTTP client, will be forced to use HTTP over SSL (HTTPS).

Information About Firewall Support of HTTPS Authentication Proxy

Authentication Proxy

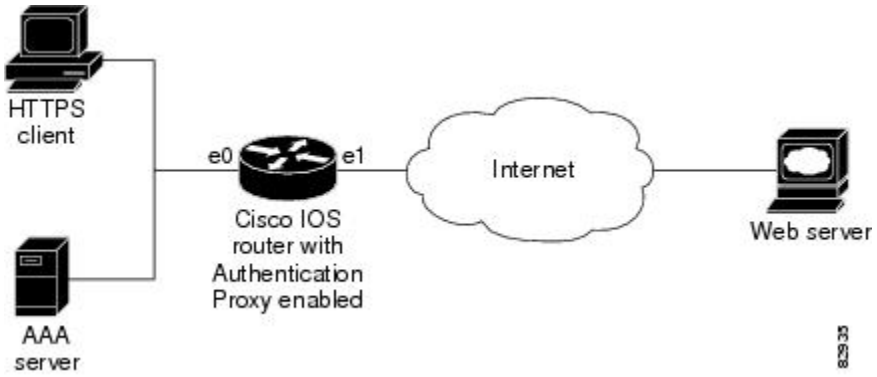
Authentication proxy grants Internet access to an authorized user through the Cisco Secure Integrated Software (also known as a Cisco IOS firewall). Access is granted on a per-user basis after the proper identification process is completed and the user policies are retrieved from a configured authentication, authorization, and accounting (AAA) server.

When authentication proxy is enabled on a Cisco router, users can log into the network or access the Internet via HTTP(S). When a user initiates an HTTP(S) session through the firewall, the authentication proxy is triggered. Authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by authentication proxy. If no entry exists, the authentication proxy responds to the HTTP(S) connection request by prompting the user for a username and password. When authenticated, the specific access profiles are automatically retrieved and applied from a CiscoSecure Access Control Server (ACS), or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

Feature Design for HTTPS Authentication Proxy

Authentication proxy support using HTTPS provides encryption between the HTTPS client and the Cisco IOS router during the username and password exchange, ensuring secure communication between trusted entities.

The figure below and the corresponding steps explain how the data flows from the time the client issues a HTTP request to the time the client receives a response from the Cisco IOS router.



1. The HTTP or HTTPS client requests a web page.
2. The HTTP or HTTPS request is intercepted by the Cisco IOS router with authentication proxy.
3. The router marks the TCP/IP connection and forwards the request (with the client address) to the web server, if authentication is required.
4. The web server builds the authentication request form and sends it to the HTTP or HTTPS client via the original request protocol--HTTP or HTTPS.
5. The HTTP or HTTPS client receives the authentication request form.
6. The user enters his or her username and password in the HTTPS POST form and returns the form to the router. At this point, the authentication username and password form is sent via HTTPS. The web server will negotiate a new SSL connection with the HTTPS client.

Note Your Cisco IOS image must support HTTPS, and HTTPS must be configured; otherwise, an HTTP request form will be generated.

1. The router receives the HTTPS POST form from the HTTPS client and retrieves the username and password.
2. The router sends the username and password to the AAA server for client authentication.
3. If the AAA server validates the username and password, it sends the configured user profile to the router. (If it cannot validate the username and password, an error is generated and sent to the router.)
4. If the router receives a user profile from the AAA server, it updates the access list with the user profile and returns a successful web page to the HTTPS client. (If the router receives an error from the AAA server, it returns an error web page to the HTTPS client.)
5. After the HTTPS client receives the successful web page, it retries the original request. Thereafter, HTTPS traffic will depend on HTTPS client requests; no router intervention will occur.

How to Use HTTPS Authentication Proxy

Configuring the HTTPS Server

To use HTTPS authentication proxy, you must enable the HTTPS server on the firewall and set the HTTPS server authentication method to use AAA.

Before You Begin

Before configuring the HTTPS server, the authentication proxy for AAA services must be configured by enabling AAA and configuring a RADIUS or TACACS+ server. The certification authority (CA) certificate must also be obtained. See Additional References module for informaton on document related to these tasks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http authentication aaa**
5. **ip http secure-server**
6. **ip http secure-trustpoint** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip http server** **Example:** `Router (config)# ip http server`	Enables the HTTP server on the router. • The authentication proxy uses the HTTP server to communicate with the client for user authentication.

	Command or Action	Purpose
Step 4	**ip http authentication aaa** **Example:** `Router (config)# ip http authentication aaa`	Sets the HTTP server authentication method to AAA.
Step 5	**ip http secure-server** **Example:** `Router (config)# ip http secure-server`	Enables HTTPS.
Step 6	**ip http secure-trustpoint** *name* **Example:** `Router (config)# ip http secure-trustpoint netCA`	Enables HTTP secure server certificate trustpoint.

What to Do Next

After you have finished configuring the HTTPS server, you must configure the authentication proxy (globally and per interface). See the Related Documents table in the Additional References section for a list of documents related to these tasks.

Verifying HTTPS Authentication Proxy

To verify your HTTPS authentication proxy configuration, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip auth-proxy configuration**
3. **show ip auth-proxy cache**
4. **show ip http server secure status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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 HTTP_ESTAB, the user authentication was successful.
Step 4	**show ip http server secure status** **Example:** `Router# show ip http server secure status`	Displays HTTPS status.

Monitoring Firewall Support of HTTPS Authentication Proxy

Perform the following task to troubleshoot your HTTPS authentication proxy configuration:

SUMMARY STEPS

1. **enable**
2. **debug ip auth-proxy detailed**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**debug ip auth-proxy detailed** **Example:** `Router# debug ip auth-proxy detailed`	Displays the authentication proxy configuration information on the router.

Configuration Examples for HTTPS Authentication Proxy

HTTPS Authentication Proxy Support Example

The following example is output from the **show running-config** command. This example shows how to enable HTTPS authentication proxy on a Cisco IOS router.

```
Router# show running-config
Building configuration...
Current configuration : 6128 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 7200a
!
boot system disk0:c7200-ik9o3s-mz.emweb
aaa new-model
!
!
aaa authentication login default group tacacs+ group radius
aaa authorization auth-proxy default group tacacs+ group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
!
ip domain name cisco.com
!
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 3
ip auth-proxy name authname http
ip audit notify log
ip audit po max-events 100
!
! Obtain a CA certificate.
crypto ca trustpoint netCA
 enrollment mode ra
 enrollment url http://10.3.10.228:80/certsrv/mscep/mscep.dll
 subject-name CN=7200a.cisco.com
 crl optional
crypto ca certificate chain netCA
 certificate ca 0702EFC30EC4B18D471CD4531FF77E29
  308202C5 3082026F A0030201 02021007 02EFC30E C4B18D47 1CD4531F F77E2930
  0D06092A 864886F7 0D010105 0500306D 310B3009 06035504 06130255 53310B30
  09060355 04081302 434F3110 300E0603 55040713 07426F75 6C646572 31163014
  06035504 0A130D43 6973636F 20537973 74656D73 310C300A 06035504 0B130349
```

```
  54443119 30170603 55040313 10495444 20426F75 6C646572 202D2043 41301E17
  0D303230 31323532 33343434 375A170D 31323031 32353233 35343333 5A306D31
  0B300906 03550406 13025553 310B3009 06035504 08130243 4F311030 0E060355
  04071307 426F756C 64657231 16301406 0355040A 130D4369 73636F20 53797374
  656D7331 0C300A06 0355040B 13034954 44311930 17060355 04031310 49544420
  426F756C 64657220 2D204341 305C300D 06092A86 4886F70D 01010105 00034B00
  30480241 00B896F0 7CE9DCBD 59812309 1793C610 CEC83704 D56C29CA 3E8FAC7A
  A113520C E15E3DEF 64909FB9 88CD43BD C7DFBAD6 6D523804 3D958A97 9733EE71
  114D8F3F 8B020301 0001A381 EA3081E7 300B0603 551D0F04 04030201 C6300F06
  03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 14479FE0 968DAD8A
  46774122 2276C19B 6800FA3C 79308195 0603551D 1F04818D 30818A30 42A040A0
  3E863C68 7474703A 2F2F6369 73636F2D 736A7477 77383779 792F4365 7274456E
  726F6C6C 2F495444 25323042 6F756C64 65722532 302D2532 3043412E 63726C30
  44A042A0 40863E66 696C653A 2F2F5C5C 63697363 6F2D736A 74777738 3779795C
  43657274 456E726F 6C6C5C49 54442532 30426F75 6C646572 2532302D 25323043
  412E6372 6C301006 092B0601 04018237 15010403 02010030 0D06092A 864886F7
  0D010105 05000341 0044DE07 3964E080 09050906 512D40C0 D4D86A0A 6B33E752
  6E602D96 3F68BB8E 463E3EF6 D29BE400 615E7226 87DE1DE3 96AE23EF E076EE60
  BF789728 5ED0D5FC 2C
  quit
 certificate 55A4795100000000000D
  308203FC 308203A6 A0030201 02020A55 A4795100 00000000 0D300D06 092A8648
  86F70D01 01050500 306D310B 30090603 55040613 02555331 0B300906 03550408
  1302434F 3110300E 06035504 07130742 6F756C64 65723116 30140603 55040A13
  0D436973 636F2053 79737465 6D73310C 300A0603 55040B13 03495444 31193017
  06035504 03131049 54442042 6F756C64 6572202D 20434130 1E170D30 32303631
  38323030 3035325A 170D3033 30363138 32303130 35325A30 3A311E30 1C06092A
  864886F7 0D010902 130F3732 3030612E 63697363 6F2E636F 6D311830 16060355
  0403130F 37323030 612E6369 73636F2E 636F6D30 5C300D06 092A8648 86F70D01
  01010500 034B0030 48024100 F61D6551 77F9CABD BC3ACAAC D564AE53 541A40AE
  B89B6215 6A6D8D88 831F672E 66678331 177AF07A F476CD59 E535DAD2 C145E41D
  BF33BEB5 83DF2A39 887A05BF 02030100 01A38202 59308202 55300B06 03551D0F
  04040302 05A0301D 0603551D 0E041604 147056C6 ECE3A7A4 E4F9AFF9 20F23970
  3F8A7BED 323081A6 0603551D 2304819E 30819B80 14479FE0 968DAD8A 46774122
  2276C19B 6800FA3C 79A171A4 6F306D31 0B300906 03550406 13025553 310B3009
  06035504 08130243 4F311030 0E060355 04071307 426F756C 64657231 16301406
  0355040A 130D4369 73636F20 53797374 656D7331 0C300A06 0355040B 13034954
  44311930 17060355 04031310 49544420 426F756C 64657220 2D204341 82100702
  EFC30EC4 B18D471C D4531FF7 7E29301D 0603551D 110101FF 04133011 820F3732
  3030612E 63697363 6F2E636F 6D308195 0603551D 1F04818D 30818A30 42A040A0
  3E863C68 7474703A 2F2F6369 73636F2D 736A7477 77383779 792F4365 7274456E
  726F6C6C 2F495444 25323042 6F756C64 65722532 302D2532 3043412E 63726C30
  44A042A0 40863E66 696C653A 2F2F5C5C 63697363 6F2D736A 74777738 3779795C
  43657274 456E726F 6C6C5C49 54442532 30426F75 6C646572 2532302D 25323043
  412E6372 6C3081C6 06082B06 01050507 01010481 B93081B6 30580608 2B060105
  05073002 864C6874 74703A2F 2F636973 636F2D73 6A747777 38377979 2F436572
  74456E72 6F6C6C2F 63697363 6F2D736A 74777738 3779795F 49544425 3230426F
  756C6465 72253230 2D253230 43412E63 7274305A 06082B06 01050507 3002864E
  66696C65 3A2F2F5C 5C636973 636F2D73 6A747777 38377979 5C436572 74456E72
  6F6C6C5C 63697363 6F2D736A 74777738 3779795F 49544425 3230426F 756C6465
  72253230 2D253230 43412E63 7274300D 06092A86 4886F70D 01010505 00034100
  9BAE173E 337CAD74 E95D5382 A5DF7D3C 91F69832 761E374C 0E1E4FD6 EBDE59F6
  5B8D0745 32C3233F 25CF45FE DEEEB73E 8E5AD908 BF7008F8 BB957163 D63D31AF
  quit
!!
!
voice call carrier capacity active
!
!
interface FastEthernet0/0
 ip address 192.168.126.33 255.255.255.0
 duplex half
 no cdp enable
!
interface ATM1/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
```

```
 no cdp enable
!
interface FastEthernet3/0
 ip address 192.168.26.33 255.255.255.0
! Configure auth-proxy interface.
 ip auth-proxy authname
 duplex half
 no cdp enable
!
interface FastEthernet4/0
 ip address 10.3.10.46 255.255.0.0
 duplex half
 no cdp enable
!
interface FastEthernet4/0.1
!
ip nat inside source static 192.168.26.2 192.168.26.25
ip classless
! Configure the HTTPS server.
ip http server
ip http authentication aaa
ip http secure-trustpoint netCA
ip http secure-server
ip pim bidir-enable
!
!
access-list 101 deny   tcp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
! Configure AAA and RADIUS server.
tacacs-server host 192.168.126.3
tacacs-server key letmein
!
radius-server host 192.168.126.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key letmein
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 password letmein
!
!
end
```

RADIUS User Profile Example

The following example is a sample RADIUS user profile for Livingston RADIUS:

```
#--------------- 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 192.168.134.216
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”
```

TACACS User Profile Example

The following examples 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 192.168.134.216 eq 23”
                inacl#5=”permit tcp any host 192.168.134.216 eq 20”
                inacl#6=”permit tcp any host 192.168.134.216 eq 21”
                inacl#3=”deny -1”

        }
      service = auth-proxy
          {
              priv-lvl=15
              proxyacl#4=”permit tcp any host 192.168.105.216 eq 23”
              proxyacl#5=”permit tcp any host 192.168.105.216 eq 20”
              proxyacl#6=”permit tcp any host 192.168.105.216 eq 21”
              proxyacl#7=”permit tcp any host 192.168.105.216 eq 25”
          }

}
user = http {
           login = cleartext test
      service = auth-proxy
          {
               priv-lvl=15
               proxyacl#4=”permit tcp any host 192.168.105.216 eq 23”
               proxyacl#5=”permit tcp any host 192.168.105.216 eq 20”
               proxyacl#6=”permit tcp any host 192.168.105.216 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
```

HTTPS Authentication Proxy Debug Example

The following is a sample of **debug ip auth-proxy detailed command output**:

```
*Mar  1 21:18:18.534: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.534:  SYN SEQ 462612879 LEN 0
*Mar  1 21:18:18.534: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.538: AUTH-PROXY:auth_proxy_half_open_count++ 1
*Mar  1 21:18:18.542: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.542:  ACK 3715697587 SEQ 462612880 LEN 0
*Mar  1 21:18:18.542: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.542: clientport 3061 state 0
*Mar  1 21:18:18.542: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.542:  PSH ACK 3715697587 SEQ 462612880 LEN 250
*Mar  1 21:18:18.542: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.542: clientport 3061 state 0
*Mar  1 21:18:18.554: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.554:  ACK 3715698659 SEQ 462613130 LEN 0
*Mar  1 21:18:18.554: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.554: clientport 3061 state 0
*Mar  1 21:18:18.610: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.610:  ACK 3715698746 SEQ 462613130 LEN 0
*Mar  1 21:18:18.610: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.610: clientport 3061 state 0
*Mar  1 21:18:18.766: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.766:  FIN ACK 3715698746 SEQ 462613130 LEN 0
*Mar  1 21:18:18.766: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.766: clientport 3061 state 0
*Mar  1 21:18:33.070: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:33.070:  SYN SEQ 466414843 LEN 0
*Mar  1 21:18:33.070: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar  1 21:18:33.070: clientport 3061 state 0
*Mar  1 21:18:33.074: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:33.074:  ACK 1606420512 SEQ 466414844 LEN 0
*Mar  1 21:18:33.074: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar  1 21:18:33.074: clientport 3064 state 0
*Mar  1 21:18:33.078: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:33.078:  PSH ACK 1606420512 SEQ 466414844 LEN 431
*Mar  1 21:18:33.078: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar  1 21:18:33.078: clientport 3064 state 0
*Mar  1 21:18:33.090: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.090: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.226: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.226: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.546: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.546: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.550: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.550: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.594: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.594: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.594: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.594: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.598: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.598: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.706: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.706: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.810: AUTH-PROXY:proto_flag=7, dstport_index=0
```

```
*Mar  1 21:18:33.810: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.810: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar  1 21:18:33.810: AUTH-PROXY:Protocol not configured on if_input
*Mar  1 21:18:33.810: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:33.810:  ACK 1606421496 SEQ 466415275 LEN 0
*Mar  1 21:18:33.810: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar  1 21:18:33.814: clientport 3064 state 6
*Mar  1 21:18:33.814: AUTH-PROXY:Packet in FIN_WAIT state
*Mar  1 21:18:33.838: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:33.838:  FIN ACK 1606421496 SEQ 466415275 LEN 0
*Mar  1 21:18:33.838: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar  1 21:18:33.838: clientport 3064 state 6
*Mar  1 21:18:33.838: AUTH-PROXY:Packet in FIN_WAIT state
```

Additional References

The following sections provide references related to the Firewall Support of HTTPS Authentication Proxy feature.

Related Documents

Related Topic	Document Title
Authentication proxy configuration tasks	Configuring Authentication Proxy
Authentication proxy commands	*Cisco IOS Security Command Reference*
Information on adding HTTPS support to the Cisco IOS web server	HTTPs - HTTP Server and Client with SSL 3.0
Information on configuring and obtaining a CA certificate.	Trustpoint CLI, C isco IOS Release 12.2(8)T feature module

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[1]	Title
RFC 1945	*Hyptertext Transfer Protocol -- HTTP/ 1.0*
RFC 2616	*Hyptertext Transfer Protocol -- HTTP/ 1.1*

1 Not all supported RFCs are listed.

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 Support of HTTPS Authentication Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6: Feature Information for Firewall Support of HTTPS Authentication Proxy

Feature Name	Releases	Feature Information
Firewall Support of HTTPS Authentication Proxy	12.2(11)YU 12.2(15)T	The Firewall Support of HTTPS Authentication Proxy feature allows a user to encrypt the change of the username and password between the HTTP client and the Cisco IOS router via Secure Socket Layer (SSL) when authentication proxy is enabled on the Cisco IOS firewall, thereby ensuring confidentiality of the data passing between the HTTP client and the Cisco IOS router. This feature was introduced in Cisco IOS Release 12.2(11)YU. This feature was integrated in Cisco IOS Release 12.2(15)T.

Glossary

ACL --access control list. An ACL is a list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

Cisco IOS Firewall --The Cisco IOS Firewall is a protocol that provides advanced traffic filtering functionality and can be used as an integral part of your network's firewall.

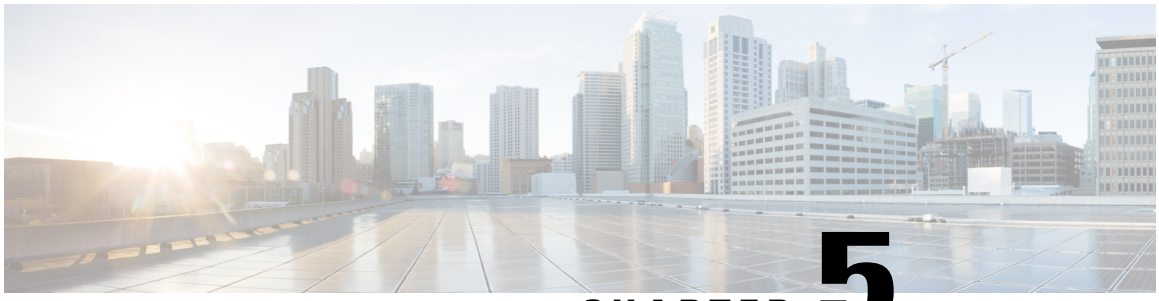
The Cisco IOS Firewall creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered the Cisco IOS Firewall when exiting through the firewall.

firewall --A firewall is a networking device that controls access to the network assets of your organization. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

HTTPS --HTTP over SSL. HTTPS is client communication with a server by first negotiating an SSL connection and then transmiting the HTTP protocol data over the SSL application data channel.

SSL --Secure Socket Layer. SSL is encryption technology for the web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.



CHAPTER 5

Firewall Authentication Proxy for FTP and Telnet Sessions

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 caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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

Feature Design for FTP and Telnet Authentication Proxy

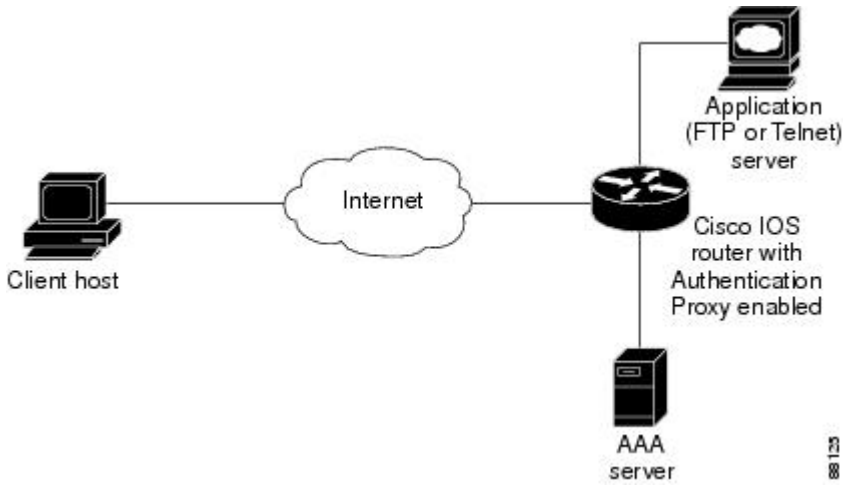
Authentication proxy for FTP and Telnet Sessions functions like authentication proxy for HTTP; that is, FTP and Telnet are independent components in the Cisco IOS software and can be enabled or disabled on the interface of an unauthenticated host.

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

The figure below displays a typical authentication proxy topology.

Figure 8: 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

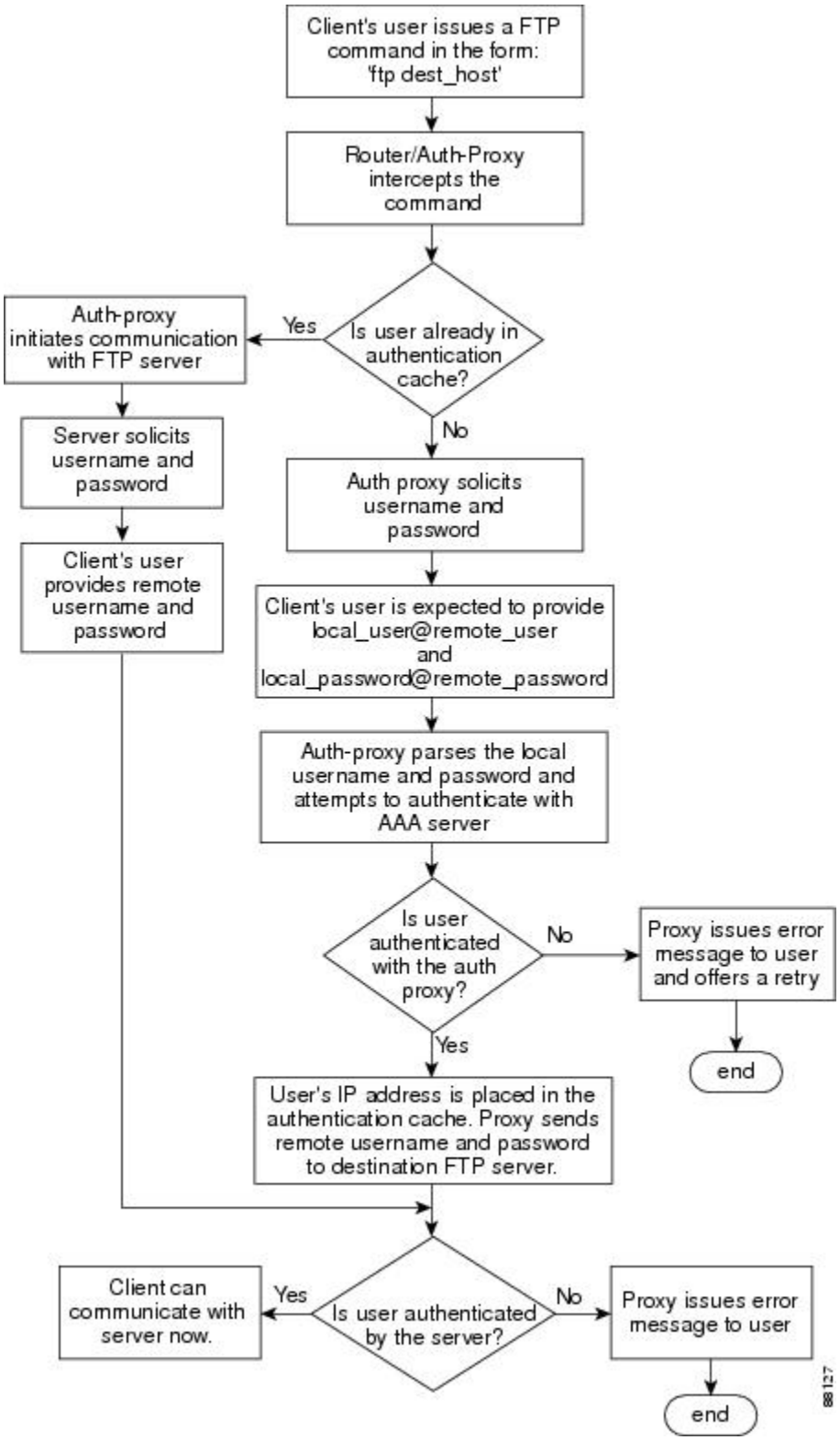
of the router, the router will try to authenticate the client host with the AAA server using the username and password of the router.

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 the figure below.

Figure 9: FTP Authentication Proxy Overview

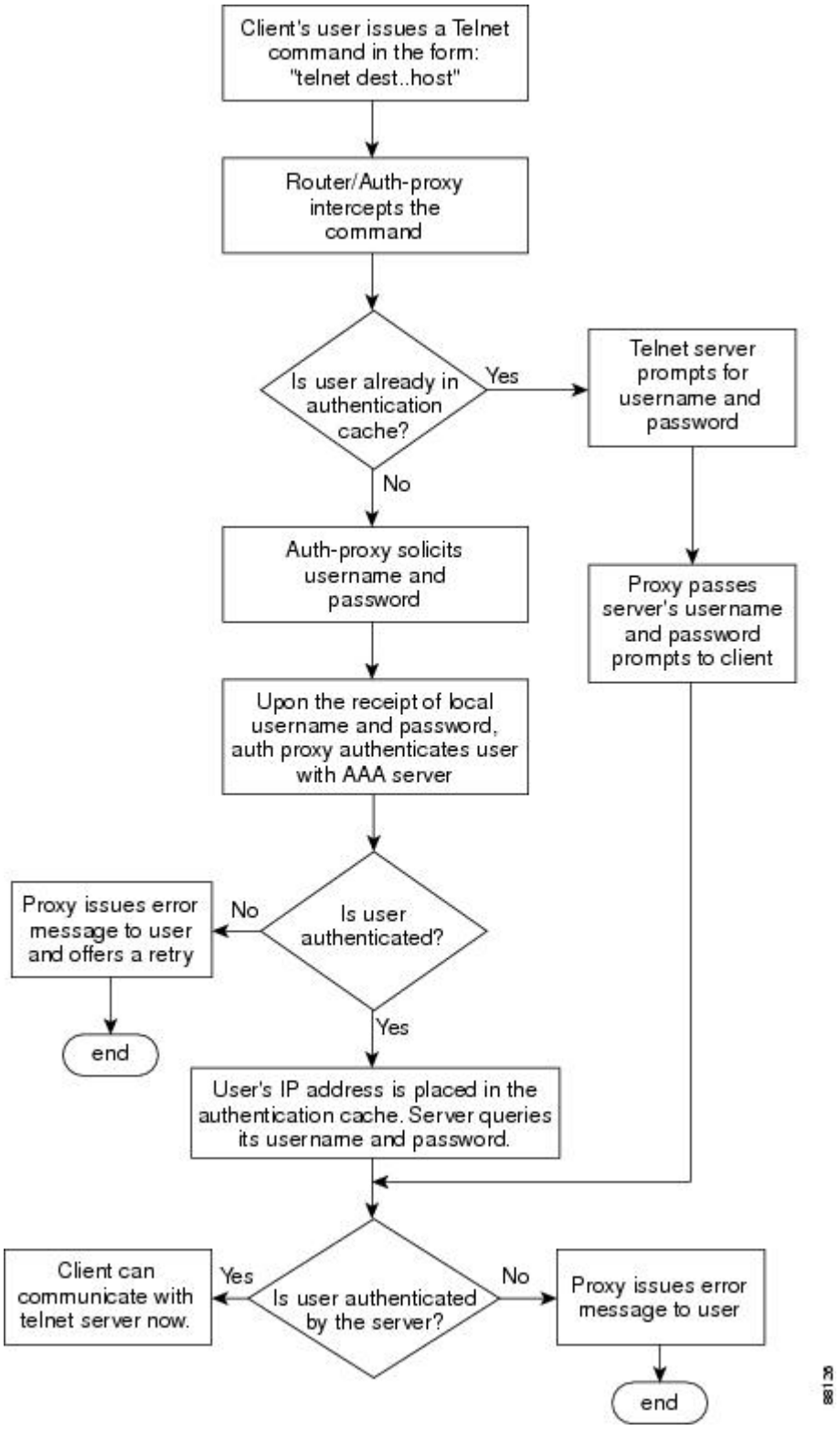

Client's user issues a FTP command in the form: 'ftp dest_host'
Router/Auth-Proxy intercepts the command
Is user already in authentication cache?
Yes
Auth-proxy initiates communication with FTP server
Server solicits username and password
Client's user provides remote username and password
No
Auth proxy solicits username and password
Client's user is expected to provide local_user@remote_user and local_password@remote_password
Auth-proxy parses the local username and password and attempts to authenticate with AAA server
Is user authenticated with the auth proxy?
No
Proxy issues error message to user and offers a retry
end
Yes
User's IP address is placed in the authentication cache. Proxy sends remote username and password to destination FTP server.
Is user authenticated by the server?
Yes
Client can communicate with server now.
No
Proxy issues error message to user
end
88127

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 the figure below.

Figure 10: 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

Configuring AAA

You must configure the authentication proxy for AAA services. To enable authorization and define the authorization methods, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default** *method1*[*method2*]
5. **aaa authorization auth-proxy default**
6. **aaa accounting auth-proxy default start-stop group tacacs+**
7. **tacacs-server host** *hostname*
8. **tacacs-server key** *key*
9. **access-list** *access-list-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA functionality on the device.
Step 4	**aaa authentication login default** *method1*[*method2*] **Example:** `Device(config)# aaa authentication login default TACACS+ RADIUS`	Defines the list of authentication methods at login.
Step 5	**aaa authorization auth-proxy default** **Example:** `Device(config)# aaa authorization auth-proxy default`	The **auth-proxy** keyword enables authentication proxy for AAA methods.
Step 6	**aaa accounting auth-proxy default start-stop group tacacs+** **Example:** `Device(config)# aaa accounting auth-proxy default start-stop group tacacs+`	Activates authentication proxy accounting. The **auth-proxy** keyword sets up the authorization policy as dynamic ACLs that can be downloaded.
Step 7	**tacacs-server host** *hostname* **Example:** `Device(config)# tacacs-server host host1`	Specifies an AAA server. For RADIUS servers, use the **radius server host** command.
Step 8	**tacacs-server key** *key* **Example:** `Device(config)# tacacs-server key key1`	Sets the authentication and encryption key for communications between the device and the AAA server. For RADIUS servers use the **radius server key** command.

	Command or Action	Purpose
Step 9	**access-list** *access-list-number* **Example:** `Device(config)# access-list accesslist1`	Creates an ACL entry to allow the AAA server to return traffic to the firewall.

What to Do Next

In addition to configuring AAA on the firewall device, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service **auth-proxy** on the AAA server as outlined here:

- Define a separate section of authorization for the **auth-proxy** keyword to specify the downloadable user profiles. This keyword does not interfere with other type of services, such as EXEC. The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
service = auth-proxy
{
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 10.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
}
}
```

- The only supported attribute in the AAA server user configuration is proxyacl#n.Use the proxyacl#n attribute when configuring the access lists in the profile. The attribute proxyacl#n is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.
- The access lists in the user profile on the AAA server must have access commands that contain only the **permit**keyword.
- Set the source address to the **any**keyword in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are:
  - CiscoSecure ACS 2.1.x for Windows NT
  - CiscoSecure ACS 2.3 for Windows NT
  - CiscoSecure ACS 2.2.4 for UNIX
  - CiscoSecure ACS 2.3 for UNIX
  - TACACS+ server (vF4.02.alpha)

- Ascend RADIUS server radius-980618 (required attribute-value pair patch)
- Livingston RADIUS server (v1.16)

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip auth-proxy auth-cache-time** *min*
4. **ip auth-proxy auth-proxy-banner**
5. **ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl acl-name*}]
6. **interface** *type number*
7. **ip auth-proxy** *auth-proxy-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip auth-proxy auth-cache-time** *min* **Example:** `Device(config)# ip auth-proxy auth-cache-time 5`	(Optional) Sets the global authentication proxy idle timeout value in minutes.
Step 4	**ip auth-proxy auth-proxy-banner** **Example:** `Device(config)# ip auth-proxy auth-proxy-banner`	(Optional) Displays the name of the firewall router in the authentication proxy login page. The banner is disabled by default.

	Command or Action	Purpose
Step 5	**ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl acl-name*}] **Example:** `Device(config)# ip auth-proxy name HQ_users http`	Creates authentication proxy rules.
Step 6	**interface** *type number* **Example:** `Device(config)# interface Ethernet0/0`	Enters interface configuration mode by specifying the interface type and number on which to apply the authentication proxy.
Step 7	**ip auth-proxy** *auth-proxy-name* **Example:** `Device(config-if)# ip auth-proxy HQ_users http`	Applies the named authentication proxy rule at the interface.

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.

	Command or Action	Purpose

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

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.

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

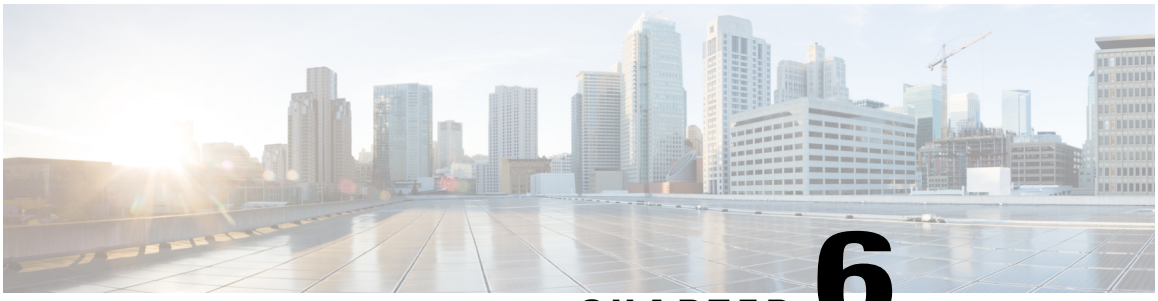
Feature Information for Firewall Authentication Proxy for FTP and Telnet Session

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: 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.**



CHAPTER 6

Transparent Bridging Support for Authentication Proxy

The Transparent Bridging Support for Authentication Proxy feature allows network administrators to configure transparent authentication proxy on existing networks without having to reconfigure the statically defined IP addresses of their network-connected devices. The result is that security policies are dynamically authenticated and authorized on a per user basis, which eliminates the tedious and costly overhead required to renumber devices on the trusted network.

Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable, which allows administrators to deploy different authentication proxy rules on bridged and routed domains.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Transparent Bridging Support for Authentication Proxy

Authentication Proxy is not supported on vLAN trunk interfaces that are configured in a bridge group.

Information About Transparent Bridging Support for Authentication Proxy

Authentication proxy provides dynamic, per-user authentication and authorization of network access connections to enforce security policies. Typically, authentication proxy is a Layer 3 functionality that is configured on routed interfaces with different networks and IP subnets on each interface.

Integrating authentication proxy with transparent bridging enables network administrators to deploy authentication proxy on an existing network without impacting the existing network configuration and IP address assignments of the hosts on the network.

Transparent Bridging Overview

If configured for bridging, a Cisco IOS device can bridge any number of interfaces. The device can complete basic bridging tasks such as learning MAC addresses on ports to restrict collision domains and running Spanning Tree Protocol (STP) to prevent looping in the topology.

Within bridging, a user can configure Integrated Routed Bridging (IRB), which allows a device to bridge on some interfaces while a Layer 3 Bridged Virtual Interface (BVI) is presented for routing. The bridge can determine whether the packet is to be bridged or routed on the basis of the destination of the Layer 2 or Layer 3 IP address in the packet. Configured with an IP address, the BVI can manage the device even if no interface is configured for routing.

How to Configure Transparent Authentication Proxy

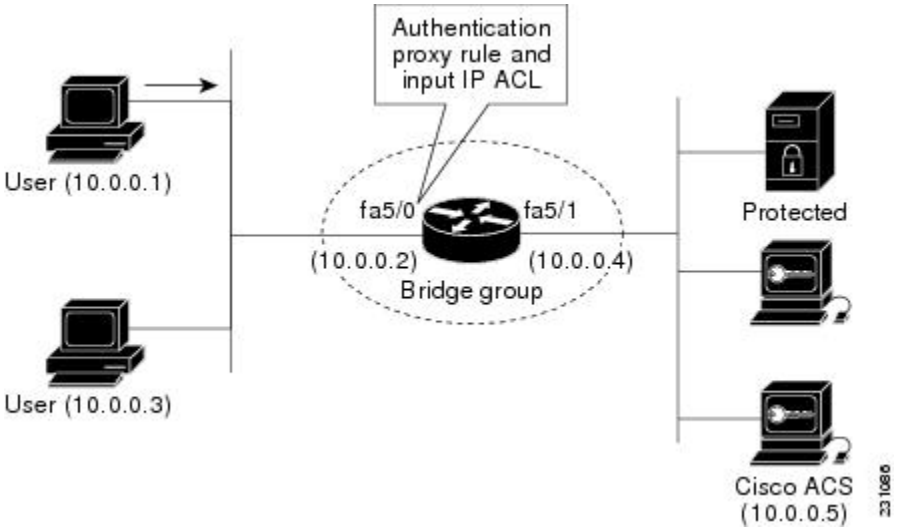
To configure authentication proxy on bridged interfaces, you must configure the interface in a bridge group and apply an authentication proxy rule on the interface. You must also set up and configure the authentication, authorization, and accounting (AAA) server (Cisco ACS) for authentication proxy. For examples on how to configure authentication proxy on a bridged interface, see the section, Configuration Examples for Transparent Authentication Proxy.

Configuration Examples for Transparent Authentication Proxy

Authentication Proxy in Transparent Bridge Mode Example

The following example (see the figure below) shows how to configure authentication proxy in a transparent bridged environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 11: Authentication Proxy in Transparent Bridging Mode: Sample Topology




```
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
no ip routing
!
!
no ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
```

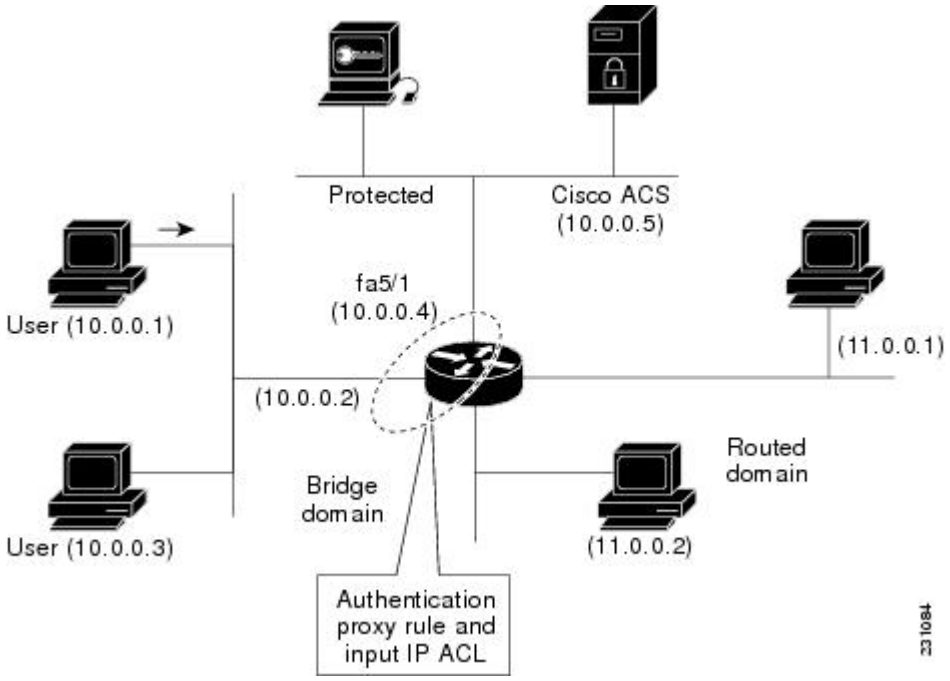
```
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
!
Router# show ip auth-proxy cache
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
                timeout 60, Time Remaining 60, state ESTAB
```

Authentication Proxy in Concurrent Route Bridge Mode Example

Concurrent routing and bridging configuration mode allows routing and bridging to occur in the same router; however, the given protocol is not switched between the two domains. Instead, routed traffic is confined to the routed interfaces and bridged traffic is confined to the bridged interfaces.

The following example (see the figure below) shows how to configure authentication proxy in a concurrent routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 12: Authentication Proxy in Concurrent Route Bridge Mode: Sample Topology




```
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radiusb
!
ip cef
!
```

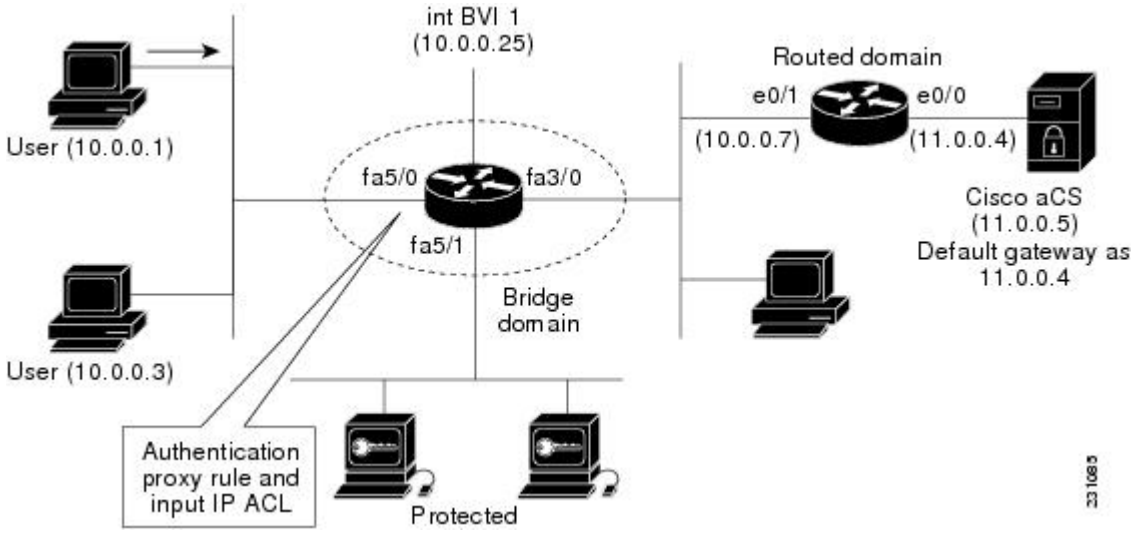
```
bridge crb
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
!
Router# show ip auth-proxy cache
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1145,
                timeout 60, Time Remaining 60, state ESTAB
```

Authentication Proxy in Integrated Route Bridge Mode Example

In an integrated routing and bridging environment, a bridged network is interconnected with a router network. Both routing and bridging can occur in the same router with connectivity between routed and bridged domains.

The following example (see the figure below) shows how to configure authentication proxy in an integrated routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 13: Authentication Proxy in Integrated Route Bridge Mode: Sample Topology




```
!
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
bridge irb
!
interface FastEthernet3/0
 no ip address
 duplex half
 bridge-group 1
!
interface FastEthernet5/0
 no ip address
 ip auth-proxy AuthRule
 ip access-group 100 in
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 duplex auto
 speed auto
 bridge-group 1
!
interface BVI1
 ip address 10.0.0.25 255.255.255.0
!
!
ip route 11.0.0.0 255.255.255.0 10.0.0.7
!
```

```
ip http server
ip http secure-server
!
radius-server host 11.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
bridge 1 route ip
!
Router# show ip auth-proxy cache
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
                timeout 60, Time Remaining 60, state ESTAB
```

Additional References

The following sections provide references related to the Transparent Bridging Support for Authentication Proxy feature.

Related Documents

Related Topic	Document Title
Authentication proxy commands	*Cisco IOS Security Command Reference*
Bridging commands	*Cisco IOS Bridging Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	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

RFC	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

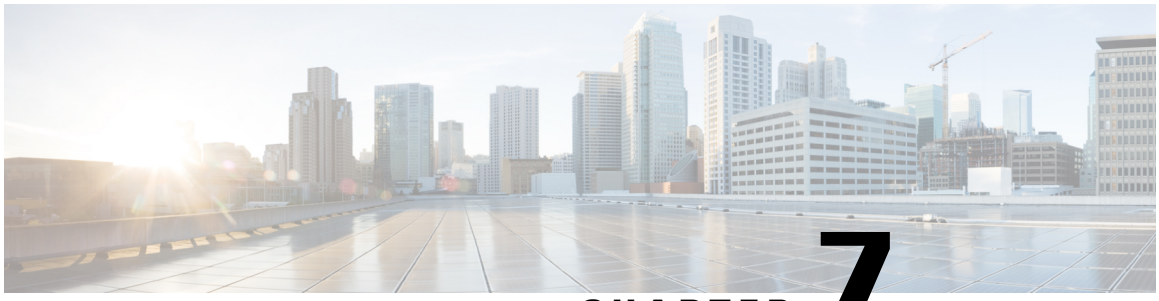
Feature Information for Transparent Authentication Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8: Feature Information for Transparent Authentication Proxy

Feature Name	Releases	Feature Information
Transparent Bridging Support for Authentication Proxy	12.4(15)T	The Transparent Bridging Support for Authentication Proxy feature allows network administrators to configure transparent authentication proxy on existing networks without having to reconfigure the statically defined IP addresses of their network-connected devices. The result is that security policies are dynamically authenticated and authorized on a per user basis, which eliminates the tedious and costly overhead required to renumber devices on the trusted network. Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable, which allows administrators to deploy different authentication proxy rules on bridged and routed domains. This feature was introduced in Cisco IOS Release 12.4(15)T.



CHAPTER 7

Browser-Based Authentication Bypass

The Browser-Based Authentication Bypass feature enables web browsers to bypass authentication methods such as HTTP Basic, Web Authorization Proxy, and Windows NT LAN Manager (NTLM) (passive or explicit). Specific web browsers can be configured for authentication, and other browsers can be configured to bypass authentication.

This module provides information about the feature and how to configure it.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Browser-Based Authentication Bypass

- You must configure at least one of these authentication methods—HTTP Basic, Web Authorization Proxy, or Windows NTLM—with browser-based authentication bypass.
- Use browser-based authentication bypass with the Default User-Group Policy feature.

Information About Browser-Based Authentication Bypass

Browser-Based Authentication Bypass Overview

While using web browsers, as part of the user authentication, a pop-up or dialog box appears in some web browsers. The Browser-Based Authentication Bypass feature helps to bypass this user authentication and thus avoid the authentication pop-ups.

With the Browser-Based Authentication Bypass feature, you can configure web browsers that must be authenticated and browsers that can bypass user authentication. Bypassing is supported for authentication methods such as HTTP Basic, Web Authorization Proxy, and Windows NT LAN Manager (NTLM) (passive or explicit).

The Browser-Based Authentication Bypass feature supports the following web browsers:

- Chrome
- Firefox
- Internet Explorer 8 (IE8)
- IE9
- Safari

A network administrator configures a list of regular expression (regex) patterns in the IP admission module. When the IP admission module receives the HTTP Get request, the module compares the user-agent string in the HTTP header to the regex pattern that the administrator has configured for the bypass method.

The following rules apply to the Browser-Based Authentication Bypass feature:

- If a configured regex pattern does not match the user-agent field, a web browser is authenticated on the basis of the configured web authentication method.
- If a configured regex pattern matches the user-agent field, authentication is bypassed for the web browser and the HTTP traffic goes through to the Cisco Web Security cloud.

How to Configure Browser-Based Authentication Bypass

Configuring Browser-Based Authentication Bypass

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *regex-map*
4. **pattern** *expression*
5. **exit**
6. **ip admission name** *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*]
7. Perform one of the following tasks:
   - **ip admission name** *admission-name* **ntlm**
   - **ip admission name** *admission-name* **http-basic**
   - **ip admission name** *admission-name* **proxy http**
8. **interface** *type number*
9. **ip admission** *admission-name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type regex** *regex-map* **Example:** `Device(config)# parameter-map type regex regex-map1`	Configures a parameter-map type with a regular expression (regex) to match a specific traffic pattern and enters parameter-map type inspect configuration mode.

	Command or Action	Purpose
Step 4	**pattern** *expression* **Example:** `Device(config-profile)# pattern Chrome`	Configures a matching pattern that compares the user-agent field in the HTTP Get request and the regex pattern.
Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 6	**ip admission name** *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*] **Example:** `Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10`	Creates an IP Network Admission Control (NAC) rule to enable browser-based authentication bypass.

Step 7	Perform one of the following tasks:
	• **ip admission name** *admission-name* **ntlm**
	• **ip admission name** *admission-name* **http-basic**
	• **ip admission name** *admission-name* **proxy http**
	
	Example:
	`Device(config)# ip admission name rule1 ntlm`
	
	`Device(config)# ip admission name rule1 http-basic`
	
	`Device(config)# ip admission name rule1 proxy http`
		Configures one of the following authentication methods:
		• Windows NT LAN Manager (NTLM)
		• HTTP Basic
		• Web Authorization Proxy

Step 8	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet0/1/0`	Configures an interface and enters interface configuration mode.
Step 9	**ip admission** *admission-name* **Example:** `Device(config-if)# ip admission rule1`	Creates a Layer 3 Network Admission Control (NAC) rule to be applied to the interface.

	Command or Action	Purpose
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

What to Do Next

For any parameter-map change to be reflected, remove and configure the **ip admission name** *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*] command in global configuration mode.

Verifying Browser-Based Authentication Bypass

SUMMARY STEPS

1. **enable**
2. **show ip admission cache**
3. **show ip admission configuration**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show ip admission cache**
Displays the current list of network admission entries and verifies the browser authentication bypass.

Example:

```
Device# show ip admission cache

Client Name N/A, Client IP 172.31.108.123, Port 63142, timeout 60, Time Remaining 60, state ESTAB
(Browser Auth Bypass)
```

Step 3 **show ip admission configuration**
Displays the Network Admission Control (NAC) configuration.

Example:

```
Device# show ip admission configuration

Auth-proxy name webauth-profile
!
browser bypass, regex parameter-map name: reg-map inactivity-time 12 minutes absolute-timer 10 minutes
```

Configuration Examples for Browser-Based Authentication Bypass

Example: Configuring Browser-Based Authentication Bypass

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex regex-map1
Device(config-profile)# pattern Chrome
Device(config-profile)# exit
Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10
Device(config)# ip admission name rule1 ntlm
Device(config)# interface gigabitethernet0/1/0
Device(config-if)# ip admission rule1
Device(config-if)# end
```

Additional References for Browser-Based Authentication Bypass

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cisco Web Security	"Cisco Web Security" module in the *Security Configuration Guide: Zone-Based Policy Firewall*
Authenticating and authorizing connections	"Configuring Authentication Proxy" module in the *Authentication Proxy Configuration Guide*

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/support

Feature Information for Browser-Based Authentication Bypass

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: Feature Information for Browser-Based Authentication Bypass

Feature Name	Releases	Feature Information
Browser-Based Authentication Bypass	15.3(3)M	The Browser-Based Authentication Bypass feature enables web browsers to bypass authentication methods such as HTTP Basic, Web Authorization Proxy, and Windows NTLM (passive or explicit). The following command was introduced: **ip admission name bypass regex**.