

## Lab 6.1.4 Configure Authentication Proxy

### Objective

In this lab exercise, the students will complete the following tasks:

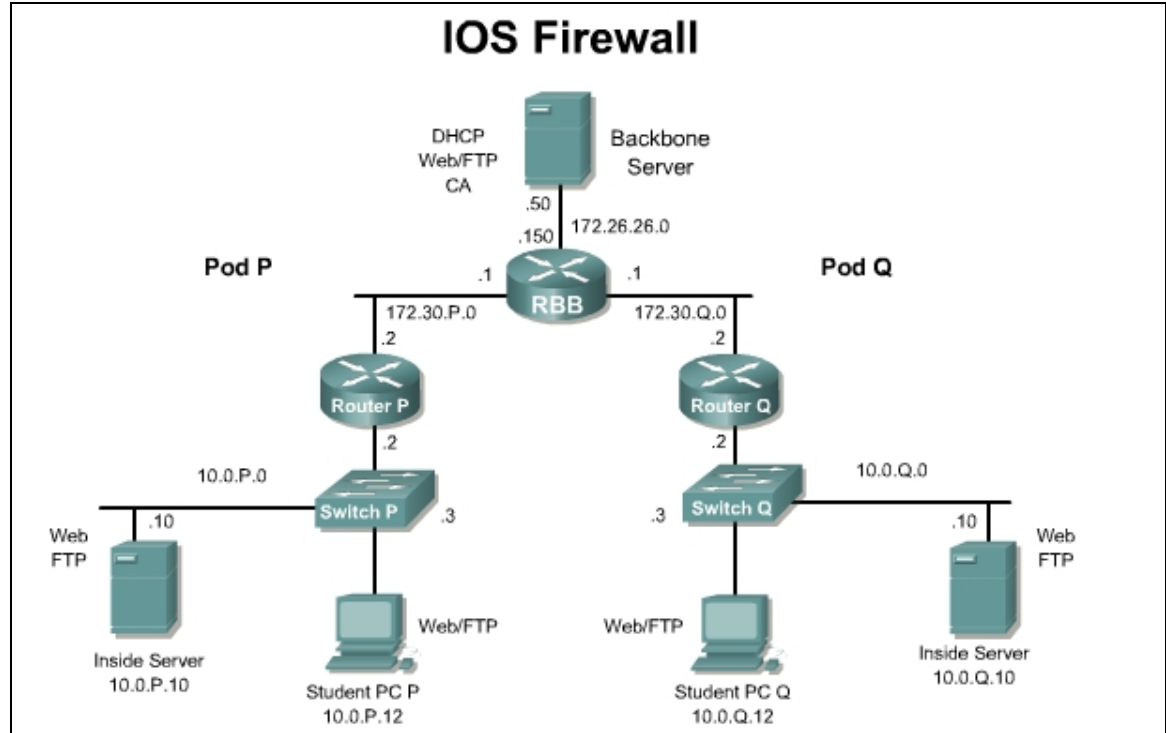
- Configure Cisco Secure Access Control Server (CSACS) for Windows 2000.
- Configure authentication, authorization, and accounting (AAA).
- Configure an authentication proxy.
- Test and verify an authentication proxy.

### Scenario

A company wants to require users to authenticate internally before accessing external web and ftp resources on the Internet. The security policy has been updated accordingly. As an IT administrator, configure the perimeter router to act as an authentication proxy in order to meet the security policy requirements.

### Topology

This figure illustrates the lab network environment.



## Preparation

Begin with the standard lab topology and verify the starting configuration on the pod routers. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

In preparation for this lab, CSACS should be configured with a user in the Default Group with a username of aaauser and aaapass as the password.

## Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Cisco Secure Access Control Server (CSACS) 3.3 or later for Windows 2000

## Additional materials

Further information about the objectives covered in this lab can be found at the following websites:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800d981d.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d981d.html)

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_command\\_reference\\_book09186a008017cf42.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017cf42.html)

## Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
<code>aaa authentication</code>	Defines AAA authentication parameters.
<code>aaa authorization</code>	Defines AAA authorization parameters.
<code>aaa new-model</code>	Enables AAA.
<code>debug aaa authentication</code>	Enables AAA authentication debugging.
<code>ip auth-proxy</code>	Defines authentication proxy rules.
<code>ip http</code>	Defines HTTP settings.
<code>tacacs-server</code>	Defines TACACS Server settings.

## Step 1 Configure CS ACS for Windows 2000

- a. On the workstation, open Cisco Secure ACS from the desktop.
  - b. Click **Interface Configuration** on the far left column of CSACS to go to the Interface Configuration window.
  - c. Click **TACACS+ (Cisco IOS)** to configure this option. Scroll down to the New Services frame.
  - d. Select the first line under New Services and enter **auth-proxy** under Services. Select the checkbox next to the field where **auth-proxy** has been entered. Make sure to check the checkbox directly to the left of the Service field.
  - e. Under **Advanced Configuration** Options, choose **Advanced TACACS+ Features** if it is not already selected.
  - f. Click **Submit** to submit the changes.
  - g. Click **Group Setup** to open the Group Setup window. Select **0: Default Group (1 user)** in the Group drop-down menu. Click the **Edit Settings** button to go to the Group Setup for this group.
  - h. Scroll down to the **auth-proxy** check box and the **Custom attributes** check box near the bottom of the Group Settings frame. Check both the **auth-proxy** check box and the **Custom attributes** check box.
  - i. Enter the following in the **Custom attributes** box.  

```
proxyacl#1=permit tcp any any
priv-lvl=15
```
  - j. Click the **Submit + Restart** button to submit the changes and restart CSACS. Wait for the interface to return to the Group Setup main window.
    1. Did CSACS restart successfully?
- 

## Step 2 Configure AAA

To configure AAA, complete the following steps:

- a. On the router, enter global configuration mode.

```
RouterP# configure terminal
```

- b. Enable AAA.

```
RouterP(config)# aaa new-model
```

1. The **aaa ?** command provides what options?

---

---

---

- c. Specify the authentication protocol.

```
RouterP(config)# aaa authentication login default group tacacs+
```

- d. Specify the authorization protocol.

```
RouterP(config)# aaa authorization auth-proxy default group tacacs+
```

- e. Define the TACACS+ server and its key.

```
RouterP(config)# tacacs-server host 10.0.P.12
```

---

**Note** If ACS is running on a computer other than the student PC, this IP address will be different.

---

(P=pod number.)

```
RouterP(config)# tacacs-server key secretkey
```

### Step 3 Define the ACLs to Allow TACACS+ Traffic

- a. Define the ACLs to allow TACACS+ traffic to the inside interface from the AAA server. Also allow outbound Internet Control Message Protocol (ICMP) traffic as well as FTP and WWW traffic. Block all other inside initiated traffic.

```
RouterP(config)# access-list 101 permit tcp host 10.0.P.12 eq tacacs  
host 10.0.P.2
```

```
RouterP(config)# access-list 101 permit icmp any any
```

```
RouterP(config)# access-list 101 permit tcp 10.0.P.0 0.0.0.255 any  
eq ftp
```

```
RouterP(config)# access-list 101 permit tcp 10.0.P.0 0.0.0.255 any  
eq www
```

```
RouterP(config)# access-list 101 deny ip any any
```

(where P = pod number)

- b. Define the ACLs to allow inbound ICMP traffic as well as FTP and WWW traffic to the inside web or FTP server. Block all other outside initiated traffic.

```
RouterP(config)# access-list 102 permit eigrp any any
```

```
RouterP(config)# access-list 102 permit icmp any any
```

```
RouterP(config)# access-list 102 permit tcp any host 10.0.P.10 eq  
ftp
```

```
RouterP(config)# access-list 102 permit tcp any host 10.0.P.10 eq  
www
```

```
RouterP(config)# access-list 102 deny ip any any
```

- c. Enable the router HTTP server for AAA.

```
RouterP(config)# ip http server
```

```
RouterP(config)# ip http authentication aaa
```

1. What options are available with the `ip http ? help` command?

---

---

---

---

## Step 4 Configure an Authentication Proxy

Complete the following steps to configure authentication proxy:

- a. Define an authentication proxy rule.

```
RouterP(config)# ip auth-proxy name APRULE http auth-cache-time 5
```

1. What other protocols can use AAA as an authentication proxy?
- 

- b. Apply the authentication proxy rule to the inside interface.

```
RouterP(config)# interface fastethernet 0/0
```

```
RouterP(config-if)# ip auth-proxy APRULE
```

```
RouterP(config-if)# ip access-group 101 in
```

```
RouterP(config-if)# exit
```

- c. Apply the ACL to the outside interface.

```
RouterP(config-if)# interface fastethernet 0/1
```

```
RouterP(config-if)# ip access-group 102 in
```

## Step 5 Test and Verify an Authentication Proxy

Complete the following steps to test and verify authentication proxy:

- a. On the router, use the **show access-list** command to check the access lists. Fill in the blanks below using the output from this command.

```
RouterP# show access-list
```

1. Extended IP access list 101

---

---

---

---

2. Extended IP access list 102

---

---

---

---

- b. Use the **show ip auth-proxy configuration** command to verify the authorization proxy configuration. Fill in the blanks below using the output from this command.

```
RouterP# show ip auth-proxy configuration
```

1. Authentication global cache time is \_\_\_\_\_ minutes
2. Auth-proxy name \_\_\_\_\_
3. http list not specified auth-cache-time \_\_\_\_\_ minutes

- c. Use the **show ip auth-proxy cache** command to verify the authorization proxy configuration.

```
RouterP# show ip auth-proxy cache
```

1. Why is the cache empty?
- 

- d. From the workstation command prompt, ping the backbone server.

```
C:\> ping 172.26.26.50
```

```
Pinging 172.26.26.50 with 32 bytes of data:
```

```
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
```

```
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
```

```
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
```

```
Reply from 172.26.26.50: bytes=32 time=36ms TTL=125
```

- e. Use the web browser to connect to the backbone web server.
- f. In the URL field enter **http://172.26.26.50**.
- g. Enter the following when the web browser prompts for a username and password.

```
Username: aaauser
```

```
Password: aaapass
```

- h. Use the **show access-list** command to check the ACLs. Fill in the blanks below using the output from this command.

```
RouterP# show access-list
```

1. Extended IP access list 101

---

---

---

---

2. Extended IP access list 102

---

---

---

---

---

- i. On the router, use the **show ip inspect all** command to see the CBAC parameters:

```
RouterP# show ip inspect all
```

---

---

---

---

- j. Use the **show ip auth-proxy cache** command to verify the authorization proxy configuration. Fill in the blank below using the output from this command.

RouterP#**show ip auth-proxy cache**

---

## Step 6 Test and Verify Authentication Proxy

Complete the following steps to test and verify authentication proxy a second time:

- a. Use the web browser to connect to the backbone web server.  
b. In the URL field enter **http://172.26.26.50**.

---

**Note** Use a "." at the end of the IP address to download a new copy of the web page. Otherwise, the browser may display a cached copy.

---

1. Was it necessary to authenticate again? Why?

---

---

---

- c. Use the **clear ip auth-proxy cache \*** command to clear the authorization proxy cache.

RouterP# **clear ip auth-proxy cache \***

1. Why is it necessary to clear the cache?

---

---

- d. Use the **show ip auth-proxy cache** command to verify the cache has been cleared.

RouterP# **show ip auth-proxy cache**

1. Has the cache been cleared?

---