



Lab 6.3.10 Configure AAA on the PIX Security Appliance Using Cisco Secure ACS for Windows 2000

Objective

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

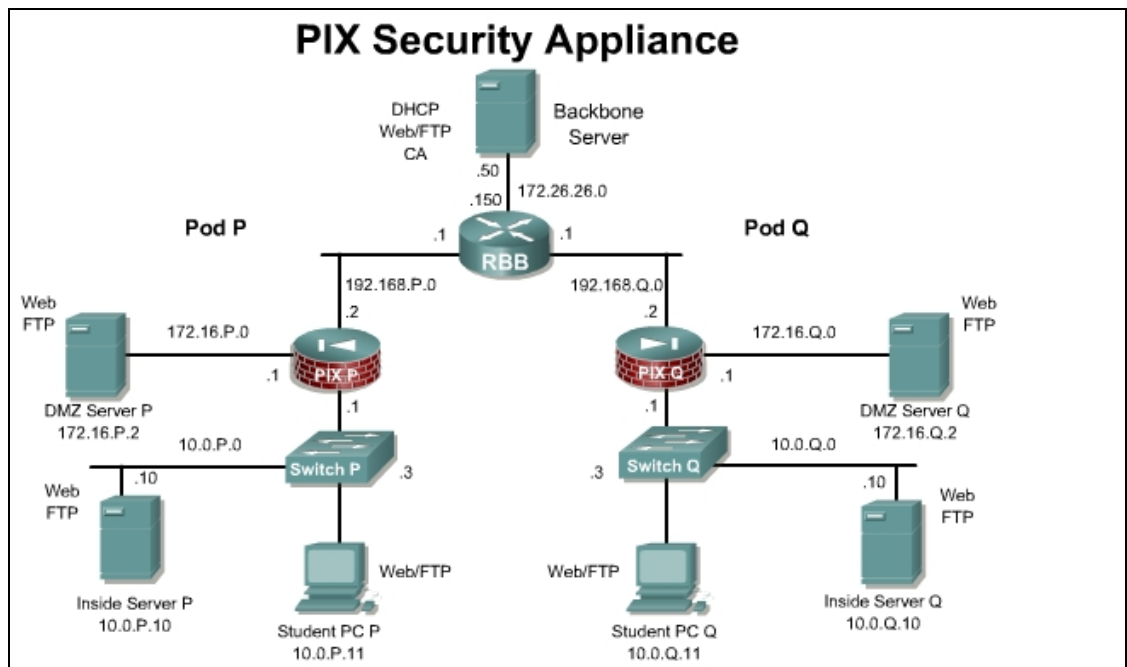
- Add a user to the Cisco Secure ACS database.
- Identify the AAA server and protocol.
- Configure and test inbound and outbound authentication.
- Configure and test console access and Virtual Telnet authentication.
- Change and test authentication timeouts and prompts.
- Configure and test authorization and accounting

Scenario

A small company has grown from 10 users to over 50. A Windows 2000 Server has just been installed and configured with Cisco Secure ACS software. All of the appropriate patches and updates have been completed. At this point, the PIX Security Appliance must be configured to use server based AAA.

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology and verify the starting configuration on pod PIX Security Appliances. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

On the Backbone Server, ensure that FTP is configured with the following account:

User: **ftpuser** Password: **ftppass**

To download a trial version of ACS for educational purposes only go to <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-eval> or contact the instructor for instructions. A CCO login is required to access this page.

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- Cisco Secure ACS version 3.3 or later.

Additional Materials

Student can use the following links for more information on the objectives covered in this lab:

<http://www.cisco.com/go/acs>

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 secure-http-client</code>	Enable encrypted authentication session.
<code>aaa authentication { include exclude } authentication-service interface-name local-ip local-mask [foreign-ip foreign-mask] server-tag</code>	Configure AAA authentication
<code>aaa authorization { include exclude } service interface-name local-ip local-mask foreign-ip foreign-mask server-tag</code>	Configure AAA authorization
<code>aaa accounting {include exclude} service interface-name local-ip local-mask foreign-ip foreign-mask server-tag</code>	Configure AAA accounting
<code>aaa authentication {serial enable telnet ssh http} console server-tag [LOCAL]</code>	Configure AAA to authenticate serial, telnet, http, or ssh remote administration sessions

Command	Description
<code>aaa-server server-tag [(interface-name)] host server-ip [key] [timeout seconds]</code>	Specify an AAA server. (Configuration mode.)
<code>auth-prompt [accept reject prompt] string</code>	Change the AAA challenge text. (Configuration mode.)
<code>clear configure aaa</code>	Removes aaa command statements from the configuration.
<code>clear configure aaa-server</code>	Removes aaa-server command statements from the configuration.
<code>clear uauth</code>	Removes an auth-prompt command statement from the configuration.
<code>show running-config aaa</code>	Displays the AAA authentication configuration.
<code>show running-config aaa-server</code>	Displays AAA server configuration.
<code>show running config auth-prompt</code>	Displays authentication challenge, reject or acceptance prompt.
<code>show uauth</code>	Displays one or all currently authenticated users, the host IP to which they are bound, and, if applicable, any cached IP and port authorization information.
<code>timeout [xlate conn udp icmp rpc h225 h323 mgcp mgcp-pat sip sip_media uauth hh:mm:ss]</code>	Set the maximum idle time duration. (Configuration mode.)

Step 2 Verify the Users in the Cisco Secure ACS Database

Complete the following steps to verify users in the Cisco Secure ACS database:

- a. Double click the ACS Admin icon on the desktop to launch the Cisco Secure ACS.
- b. The Cisco Secure ACS interface should now be displayed in the web browser. Click **User Setup** to open the User Setup interface.
- c. To view the list of current users, press **Find**. The User List will appear on the right hand side of the interface.
 1. Is there an entry for **aaauser**?
- d. If there is an entry for **aaauser**, proceed to Step 3. If there is no entry for **aaauser**, complete the remaining substeps to add a user in the Cisco Secure ACS database.
- e. Add a user by entering **aaauser** in the user field.
- f. Click **Add/Edit** to go into the user information edit window.
- g. Give the user a password by entering **aaapass** in both the Password and Confirm Password fields.

- h. Click **Submit** to add the new user to the Cisco Secure ACS database. Wait for the interface to return to the User Setup main window.

Step 3 Verify the Existing AAA Clients

Complete the following steps to verify the existing AAA clients:

- a. The Cisco Secure ACS interface should be displayed in the web browser. Click **Network Configuration** to open the Network Configuration Setup interface. The Network Configuration Setup interface provides the ability to search, add, and delete AAA Clients, AAA Servers, and Proxy Distribution Tables.
- b. Click the **(Not Assigned)** link to view the AAA Clients and Servers. The table at the top of the window displays all AAA Clients that have been configured.
 1. Is there an AAA client entry for PixP?

- c. If there is an entry for PixP in the AAA Client table, proceed to Step 4. If there is no entry for PixP, continue to Step3d below to configure PixP as an AAA client.
- d. To add PixP as an AAA client, click **Add Entry**. Enter the following information in the text boxes:
AAA Client Hostname: **PixP**
AAA Client IP Address: **10.0.P.1**
Key: **secretkey**
- e. Verify the authentication is **TACACS+ (Cisco IOS)**. If any of check boxes are selected, uncheck them and press **Submit + Restart**.
After a few moments, the Network Configuration Setup interface will refresh.
 1. Is the PixP AAA client displayed?

Step 4 Identify the AAA Server and the AAA Protocol on the PIX Security Appliance

Complete the following steps to identify the AAA server and the AAA protocol on the PIX Security Appliance:

- a. Create a group tag called MYTACACS and assign the TACACS+ protocol to it:
`PixP(config)# aaa-server MYTACACS protocol tacacs+`
- b. Return to configuration mode.
`PixP(config-aaa-server-group)# exit`
`PixP(config)#`
- c. Define the AAA server:
`PixP(config)# aaa-server MYTACACS (inside) host 10.0.P.11`

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

- d. Define the key used to authenticate to the AAA server:
`PixP(config-aaa-server-host)# key secretkey`
- e. Return to configuration mode.
`PixP(config-aaa-server-host)# exit`
`PixP(config)#`

- f. Verify the configuration:

```
PixP(config)# show running-config aaa-server  
aaa-server MYTACACS protocol tacacs+  
aaa-server MYTACACS host 10.0.P.11  
key secretkey
```

Step 5 Enable the Use of Inbound Authentication

Complete the following steps to enable the use of inbound authentication on the PIX Security Appliance:

- a. Configure the PIX Security Appliance to require authentication for all inbound traffic:

```
PixP(config)# aaa authentication include any outside 0 0 0 0  
MYTACACS
```

Warning: The keyword 'any' will be converted to 'tcp/0' in config.

- b. Verify the configuration:

```
PixP(config)# show running-config aaa  
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0  
0.0.0.0 MYTACACS
```

- c. Enable console logging of all messages:

```
PixP(config)# logging on  
PixP(config)# logging console debug
```

Note If the web browser is open, close it. Choose **File-Close** from the web browser menu.

- d. Now test a peer pod inbound web authentication. Open the web browser, and initiate an HTTP connection with the DMZ web server of the peer pod:

http://192.168.Q.11

(where Q = peer pod number)

Or, from an internet PC, test your configuration.

http://192.168.P.11

(where P = pod number)

- e. When the web browser prompts, enter **aaauser** for the username and **aaapass** for the password. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-302013: Built inbound TCP connection 277 for  
outside:192.168.Q.10/3408 (192.168.Q.10/3408) to dmz:bastionhost/80  
(192.168.1.11/80)  
  
%PIX-6-109001: Auth start for user '???' from 192.168.Q.10/3408 to  
bastionhost/80  
  
%PIX-6-302014: Teardown TCP connection 277 for  
outside:192.168.Q.10/3408 to dmz:bastionhost/80 duration 0:00:09  
bytes 111 TCP FINs  
  
%PIX-6-302013: Built inbound TCP connection 278 for  
outside:192.168.2.10/3409 (192.168.Q.10/3409) to dmz:bastionhost/80  
(192.168.P.11/80)
```

```
%PIX-6-109001: Auth start for user '???' from 192.168.Q.10/3409 to
bastionhost/80

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1

%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 279 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1042
(10.0.P.1/1042)

%PIX-2-109011: Authen Session Start: user 'aaauser', sid 1

%PIX-6-109005: Authentication succeeded for user 'aaauser' from
192.168.Q.10/3409 to bastionhost/80 on interface outside

(where P = pod number, and Q = peer pod number)
```

If the authentication does not occur, the PIX Security Appliance will display an error message similar to the following example:

```
aaa server host machine not responding
```

If this happens, there could be a configuration problem in the ACS software. Make sure the ACS server is reachable using the ping command. Verify that the secret keys match.

- f. After a peer successfully authenticates to the PIX Security Appliance, display the PIX Security Appliance authentication statistics:

```
PixP(config)# show uauth

                        Current Most Seen
Authenticated Users           1         1
Authen In Progress           0         1
user 'aaauser' at 192.168.Q.10, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00

(where Q = peer pod number)
```

1. What does the value in absolute timeout mean?

Step 6 Enable the Use of Outbound Authentication

Complete the following steps to enable the use of outbound authentication on the PIX Security Appliance:

- a. Configure the PIX Security Appliance to require authentication for all outbound traffic:

```
PixP(config)# aaa authentication include any inside 0 0 0 0 MYTACACS
Warning: The keyword 'any' will be converted to 'tcp/0' in config.
```

- b. Verify the configuration:

```
PixP(config)# show running-config aaa

aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS

aaa authentication include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
```

Test HTTP outbound authentication from the Student PC. Ping RBB first.

```
C:\> ping 172.26.26.150
```

Pinging 172.26.26.150 with 32 bytes of data:

```
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
```

```
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
```

```
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
```

```
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
```

Ping statistics for 172.26.26.150:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

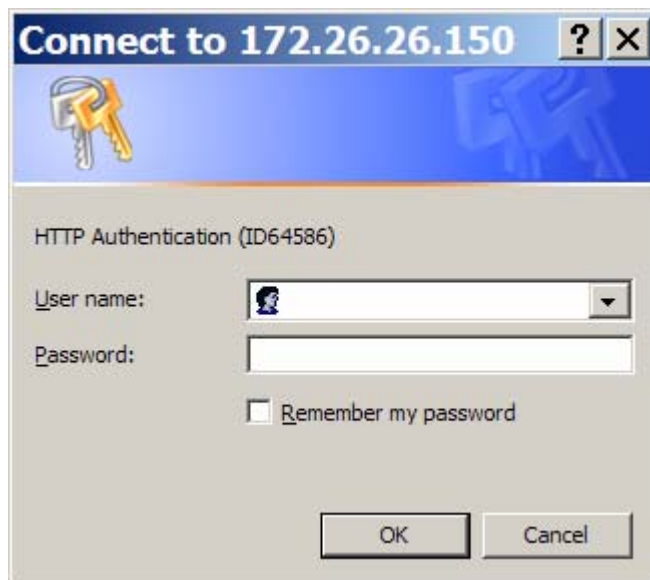
Approximate round trip times in milli-seconds:

```
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- c. Open a web browser on the Student PC and connect to RBB. When the web browser prompts, enter **aaauser** for the username and **aaapass** for the password.

http://172.26.26.150

After the HTTP session is authenticated, a password is still required to access RBB. When prompted, leave the username blank and use '**cisco**' for the password.



1. Why did the ping work without authentication?

-
- d. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user '???' from insidehost/3454 to 172.26.26.150/80
```

```
%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1
```

```
%PIX-6-609001: Built local-host inside:10.0.P.10
```

```
%PIX-6-302013: Built outbound TCP connection 315 for inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1043 (10.0.P.1/1043)
```

```
%PIX-2-109011: Authen Session Start: user 'aaauser', sid 2
```

```
%PIX-6-109005: Authentication succeeded for user 'aaauser' from
insidehost/3454to 172.26.26.150/80 on interface inside
```

(where P = pod number)

- e. Display authentication statistics on the PIX Security Appliance:

```
PixP(config)# show uauth

                        Current Most Seen
Authenticated Users           2         2
Authen In Progress           0         1
user 'aaauser' at insidehost, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
user 'aaauser' at 192.168.Q.10, authenticated
absolute timeout: 0:05:00
inactivit   y timeout: 0:00:00
```

Note If the web browser is open, close it. Choose **File-Exit** from the web browser menu

- f. By default the username and password are sent in clear text during HTTP authentication. To increase security it is best to use an SSL encrypted session. First, clear the authenticated sessions. Then configure the PIX Security Appliance to secure HTTP client authentication traffic using SSL.

```
PixP(config)# clear uauth
PixP(config)# aaa authentication secure-http-client
```

- g. Open a web browser on the Student PC and connect to RBB. When the web browser prompts, enter **aaauser** for the username and **aaapass** for the password

http://172.26.26.150

Please Authenticate

HTTPS Authentication

Username:

Password:

- h. Accept the certificate.

After the HTTP session is authenticated, a password is still required to access RBB. When prompted, leave the username blank and use 'cisco' for the password.

Step 7 Enable Console Telnet Authentication

Complete the following steps to enable console Telnet authentication at the PIX Security Appliance:

- a. Configure the PIX Security Appliance to require authentication for Telnet console connections:

```
PixP(config)# aaa authentication telnet console MYTACACS
```

- b. Verify the configuration:

```
PixP(config)# show running-config aaa  
  
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0  
0.0.0.0 MYTACACS  
  
aaa authentication include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0  
0.0.0.0 MYTACACS  
  
aaa authentication telnet console MYTACACS  
  
aaa authentication secure-http-client
```

- c. Configure the PIX Security Appliance to allow console Telnet logins from the inside host:

```
PixP(config)# telnet insidehost 255.255.255.255 inside
```

- d. Verify the configuration:

```
PixP(config)# show telnet  
  
insidehost 255.255.255.255 inside
```

- e. Clear the uauth sessions:

```
PixP(config)# clear uauth  
  
PixP(config)# show uauth  
  
Current Most Seen  
Authenticated Users 0 2  
Authen In Progress 0 1
```

- g. Telnet to the PIX Security Appliance console:

```
C:\> telnet 10.0.P.1  
  
Username: aaauser  
Password: aaapass  
Type help or '?' for a list of available commands.  
PixP>  
  
(where P = pod number)
```

- h. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-605005: Login permitted from insidehost/3507 to  
inside:10.0.1.1/telnet for user "aaauser"
```

- i. Close the Telnet session:

```
PixP>quit  
  
(where P = pod number)
```

Step 8 Enable the Use of Authentication with Virtual Telnet

Complete the following steps to enable the use of authentication with virtual Telnet on the PIX Security Appliance:

- a. Configure the PIX Security Appliance to accept authentication to a virtual Telnet service:

```
PixP(config)# virtual telnet 192.168.P.5
```

(where P = pod number)

- b. Verify the virtual Telnet configuration:

```
PixP(config)# show running-config virtual
```

```
virtual telnet 192.168.P.5
```

(where P = pod number)

- c. Clear the uauth sessions:

```
PixP(config)# clear uauth
```

```
PixP(config)# show uauth
```

	Current	Most	Seen
Authenticated Users	0	2	
Authen In Progress	0	1	

- d. Telnet to the virtual Telnet IP address to authenticate from the Student PC:

```
C:\> telnet 192.168.P.5
```

```
LOGIN Authentication
```

```
Username: aaauser
```

```
Password: aaapass
```

```
Authentication Successful
```

```
Connection to host lost.
```

```
C:\>
```

(where P = pod number)

1. Why would a virtual Telnet IP address be created on the PIX Security Appliance?

Note If the web browser is open, close it. Choose **File-Close** from the web browser menu.

- e. Test the authentication. Open the web browser and enter the following in the URL field:

http://172.26.26.150

There should be no authentication prompt.

- f. Clear the uauth timer:

```
PixP(config)# clear uauth
```

```
PixP(config)# show uauth
```

	Current	Most	Seen
Authenticated Users	0	2	
Authen In Progress	0	1	

Note: If the web browser is open, close it. Choose **File-Close** from the web browser menu.

- g. Test that there is no authentication and need to re-authenticate. On the Student PC, open the web browser and enter the following in the URL field:
- http://172.26.26.150**
- h. When prompted, enter **aaauser** for the username and **aaapass** for the password.
1. Why is authentication needed this time?
-

Step 9 Change the Authentication Timeouts and Prompts

Complete the following steps to change the authentication timeouts and prompts:

- a. View the current uauth timeout settings:
- ```
PixP(config)# show running-config timeout uauth
timeout uauth 0:05:00 absolute
```
- b. Set the uauth absolute timeout to 3 hours:
- ```
PixP(config)# timeout uauth 3:00:00 absolute
```
- c. Set the uauth inactivity timeout to 30 minutes:
- ```
PixP(config)# timeout uauth 0:30:00 inactivity
```
- d. Verify the new uauth timeout settings:
- ```
PixP(config)# show running-config timeout uauth
timeout uauth 3:00:00 absolute uauth 0:30:00 inactivity
```
- e. View the current authentication prompt settings:
- ```
PixP(config)# show running-config auth-prompt
```
- Nothing should be displayed.
- f. Set the prompt that users get when authenticating:
- ```
PixP(config)# auth-prompt prompt Please Authenticate
```
- g. Set the message that users get when successfully authenticating:
- ```
PixP(config)# auth-prompt accept You've been Authenticated
```
- h. Set the message that users get when their authentication is rejected:
- ```
PixP(config)# auth-prompt reject Authentication Failed, Try Again
```
- i. Verify the new prompt settings:
- ```
PixP(config)# show running-config auth-prompt
auth-prompt prompt Please Authenticate
auth-prompt accept You've been Authenticated
auth-prompt reject Authentication Failed, Try Again
```
- j. Clear the uauth timer:
- ```
PixP(config)# clear uauth
PixP(config)# show uauth
```
- | | Current | Most | Seen |
|---------------------|---------|------|------|
| Authenticated Users | 0 | | 2 |
| Authen In Progress | 0 | | 1 |

- k. Telnet to the Virtual Telnet IP address to test the new authentication prompts.
From the Student PC, enter the following:

```
C:\> telnet 192.168.P.5

LOGIN Authentication
Please Authenticate
Username: wronguser
Password: Authentication Failed, Try Again
LOGIN Authentication
Please Authenticate
Username: aaauser
Password: aaapass
You've been Authenticated
Authentication Successful
(where P = pod number)
```

Step 10 Enable the Use of Authorization

Complete the following steps to enable the use of authorization on the PIX Security Appliance:

- a. Configure the PIX Security Appliance to require authorization for all outbound FTP and HTTP traffic:

```
PixP(config)# aaa authorization include ftp inside 0 0 0 0 MYTACACS
PixP(config)# aaa authorization include http inside 0 0 0 0 MYTACACS
```

1. What are some of the benefits of implementing authorization? Drawbacks?

- c. Verify the configuration:

```
PixP(config)# show running-config aaa

aaa aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS

aaa authentication include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS

aaa authentication telnet console MYTACACS

aaa authorization include ftp inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
MYTACACS

aaa authorization include http inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS

aaa authentication secure-http-client
```

- d. Test FTP authorization failure from the Student PC:

```
C:\> ftp 172.26.26.50

Connected to 172.26.26.50

220-FTP Server : (user 'aaaserver')
```

```
220
User (172.26.26.50:(none)): aaauser@ftpuser
331-Password:
331
Password: aaapass@ftppass
530
Login failed
```

- e. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user 'aaauser' from insidehost/3707 to
172.26.26.50/21

%PIX-6-302015: Built outbound UDP connection 1086 for
outside:171.70.157.213/1029 (171.70.157.213/1029) to
inside:insidehost/3708 (192.168.P.10/3708) (aaauser)

%PIX-6-302015: Built outbound UDP connection 1087 for
outside:171.68.222.151/1029 (171.68.222.151/1029) to
inside:insidehost/3708 (192.168.P.10/3708) (aaauser)

%PIX-6-302015: Built outbound UDP connection 1088 for
outside:171.68.10.142/1029 (171.68.10.142/1029) to
inside:insidehost/3708 (192.168.P.10/3708) (aaauser)

%PIX-6-302016: Teardown UDP connection 1069 for
outside:171.70.157.213/1029 to inside:insidehost/3703 duration
0:02:02 bytes 0 (aaauser)

%PIX-6-302016: Teardown UDP connection 1070 for
outside:171.68.222.151/1029 to inside:insidehost/3703 duration
0:02:02 bytes 0 (aaauser)

%PIX-6-302016: Teardown UDP connection 1071 for
outside:171.68.10.142/1029 to inside:insidehost/3703 duration
0:02:02 bytes 0 (aaauser)

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1
%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 1090 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1049
(10.0.P.1/1049)

%PIX-6-109008: Authorization denied for user 'aaauser' from
insidehost/3707 to 1
```

(where P = pod number)

- f. Test web authorization failure. Open the web browser and go to the following URL:

<http://172.26.26.150>

- g. When prompted for a username and password, enter **aaauser** as the username and **aaapass** as the password:

```
User Name: aaauser
Password: aaapass
```

- h. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user 'aaauser' from insidehost/3748 to
172.26.26.150/80

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1

%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 1148 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1052
(10.0.P.1/1052)

%PIX-6-609001: Built local-host NP Identity Ifc:172.26.26.150

%PIX-6-106015: Deny TCP (no connection) from 172.26.26.150/80 to
insidehost/3748 flags RST ACK on interface NP Identity Ifc

%PIX-6-609002: Teardown local-host NP Identity Ifc:172.26.26.150
duration 0:00:00

%PIX-6-109008: Authorization denied for user 'aaauser' from
insidehost/3748 to 172.26.26.150/80 on interface inside
```

(where P = pod number)

- i. On Cisco ACS, click **Group Setup** to open the Group Setup interface.
- j. Choose **0: Default Group (1 user)** from the Group drop-down menu.
- k. Click **Users in Group** to display the users in the Default Group. The following information should be shown for the user:
- User: **aaauser**
 - Status: **Enabled**
 - Group: **Default Group (1 user)**
- l. Click **Edit Settings** to go to the Group Settings interface for the group.
- m. Scroll down in Group Settings until Shell Command Authorization Set is displayed, and select the **Per Group Command Authorization** button.
- n. Select the **Permit** radio button.
- n. Select the **Command** check box.
- o. Enter **ftp** in the Command field.
- p. Enter **permit 172.26.26.50** in the Arguments field.
- q. Click **Submit + Restart** to save the changes and restart Cisco Secure ACS. Wait for the interface to return to the Group Setup main window.
- r. Test FTP authorization success from the Windows 2000 server:

```
C:\> ftp 172.26.26.50
Connected to 172.26.26.50
220-FTP Server (user 'aaauser')
220
User (172.26.26.50:(none)): aaauser@ftppuser
331-Password:
331
Password: aaapass@ftppass
230-220 172.26.26.50 FTP server ready.
```

```

331-Password required for ftpuser
230-User ftpuser logged in.
230
ftp>

```

- s. On the PIX Security Appliance console, the following should be displayed:

```

%PIX-6-109001: Auth start for user 'aaauser' from insidehost/3869 to
172.26.26.50/21
%PIX-6-609001: Built local-host NP Identity Ifc:10.0.1.1
%PIX-6-609001: Built local-host inside:10.0.1.10
%PIX-6-302013: Built outbound TCP connection 1502 for
inside:10.0.1.10/49 (10.0.1.10/49) to NP Identity Ifc:10.0.1.1/1102
(10.0.1.1/1102)
%PIX-6-109007: Authorization permitted for user 'aaauser' from
insidehost/3869 to 172.26.26.50/21 on interface inside
(where P = pod number)

```

Step 11 Enable the Use of Accounting

Complete the following steps to enable the use of accounting on the PIX Security Appliance:

- a. Configure the PIX Security Appliance to perform accounting for all outbound traffic:

```
PixP(config)# aaa accounting include tcp/0 inside 0 0 0 0 MYTACACS
```

- b. Verify the configuration:

```

PixP(config)# show running-config aaa accounting

aaa accounting include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
MYTACACS

aaa authentication secure-http-client

```

- c. Clear the uauth sessions:

```

PixP(config)# clear uauth
PixP(config)# show uauth

Current Most Seen
Authenticated Users      0          2
Authen In Progress      0          1

```

- d. Test FTP outbound accounting from the Student PC:

```

C:\> ftp 172.26.26.50
Connected to 172.26.26.50
220-Please Authenticate :
220
User (172.26.26.50:(none)): aaauser@ftppuser
331-Password:
331
Password: aaapass@ftppass
230-220 172.26.26.50 FTP server ready.

```

```

331-Password required for ftpuser
230-User ftpuser logged in.
230
ftp>

```

- e. View the accounting records. On Cisco Secure ACS, click **Reports and Activity** to open the Reports and Activity interface.
- f. Click the **TACACS+ Accounting** link.
- g. Click the **TACACS+ Accounting active.csv** link to open the accounting records.

The following should be displayed:

Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	**	NAS Portname	NAS IP Address	cmd
5/24/2005	11:14:45	aaauser	Default Group	10.0.P.11	start	**	28	10.0.P.1	ftp

(where P = pod number)

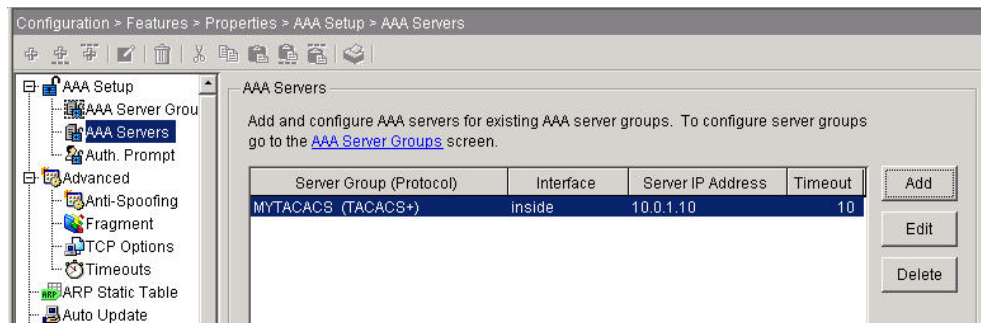
- h. Verify the PIX running configuration with the ending configuration.
- j. Turn off logging on the PIX Security Appliance:

```
PixP(config)# no logging on
```

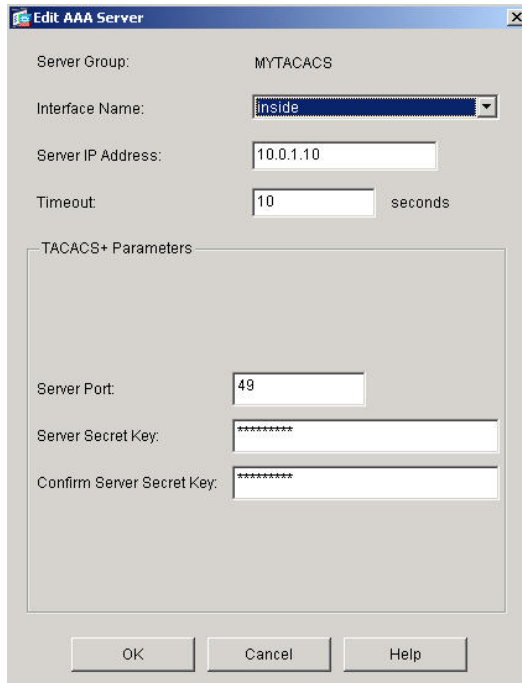
Step 7 Verify and Monitor Local AAA using ASDM

Complete the following steps to verify and monitor Local AAA using ASDM.

- a. Log into ASDM.
- b. Navigate to **Configuration>Features> Properties>AAA Setup>AAA Servers**



- c. Double click on the Server in the list to verify the AAA Server configuration. After reviewing the properties, click the **OK** button to close the window.

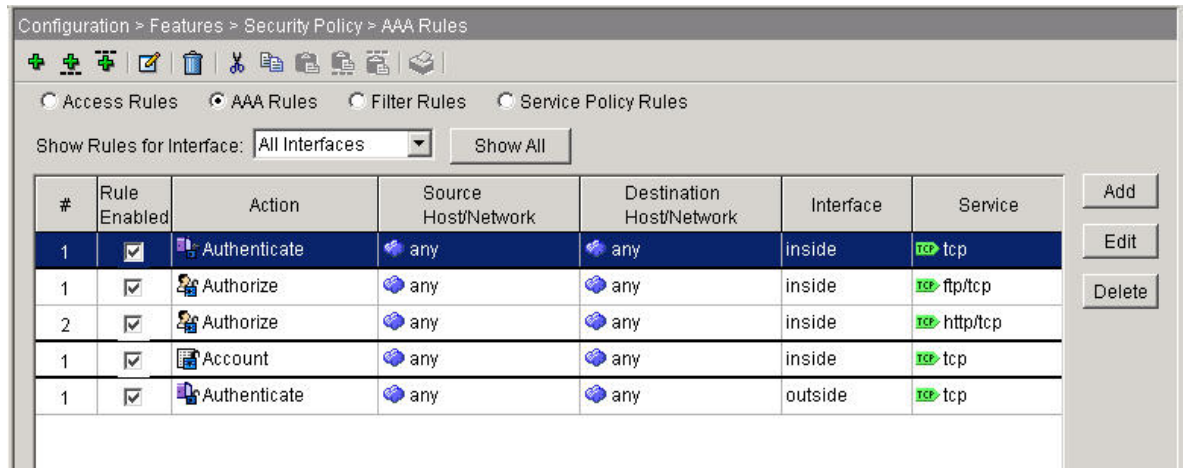


The 'Edit AAA Server' dialog box shows the following configuration:

- Server Group: MYTACACS
- Interface Name: inside
- Server IP Address: 10.0.1.10
- Timeout: 10 seconds
- TACACS+ Parameters section:
 - Server Port: 49
 - Server Secret Key: (masked with asterisks)
 - Confirm Server Secret Key: (masked with asterisks)

Buttons at the bottom: OK, Cancel, Help.

- d. Navigate to **Configuration>Features>Security Policy>AAA Rules**.



The 'Configuration > Features > Security Policy > AAA Rules' window shows the following configuration:

- Access Rules: ☐ AAA Rules: ☒ Filter Rules: ☐ Service Policy Rules: ☐
- Show Rules for Interface: All Interfaces
- Show All button
- Table of AAA Rules:

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Interface	Service
1	<input checked="" type="checkbox"/>	Authenticate	any	any	inside	tcp
1	<input checked="" type="checkbox"/>	Authorize	any	any	inside	ftp/tcp
2	<input checked="" type="checkbox"/>	Authorize	any	any	inside	http/tcp
1	<input checked="" type="checkbox"/>	Account	any	any	inside	tcp
1	<input checked="" type="checkbox"/>	Authenticate	any	any	outside	tcp

Buttons on the right: Add, Edit, Delete.

- e. Double click on any of the rules to edit.