

Lab 6.3.9 Configure Local AAA on the PIX Security Appliance

Objective

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

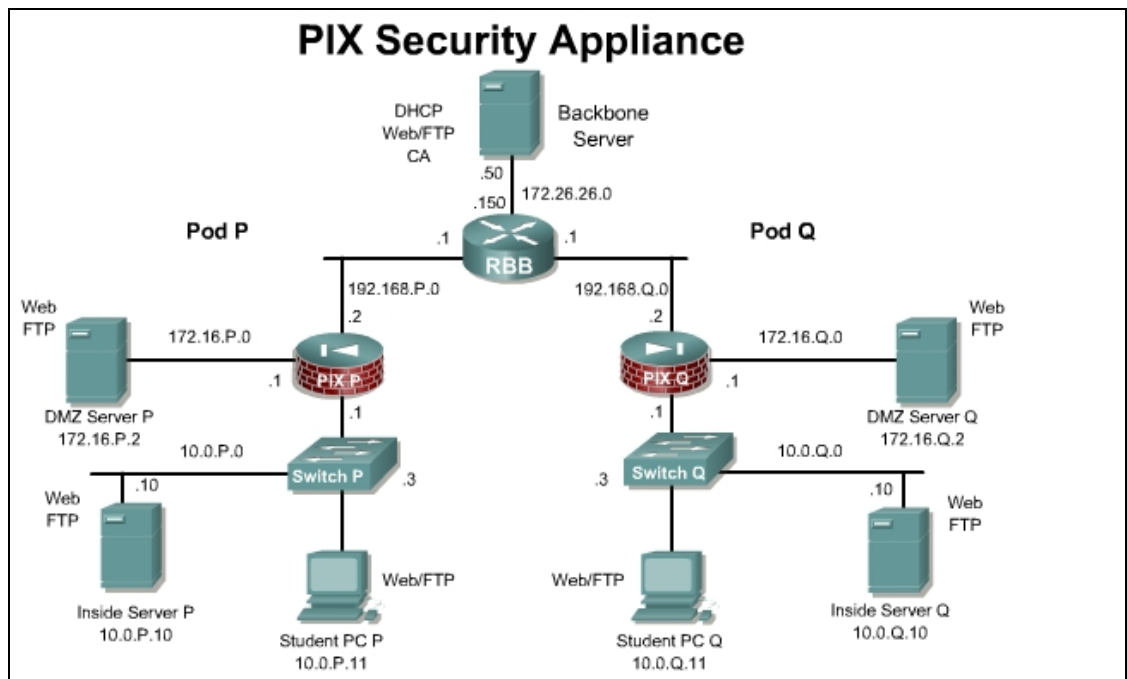
- Configure a local user.
- Configure and test inbound and outbound authentication.
- Configure and test telnet and http console access
- Configure and test Virtual Telnet authentication.
- Change and test authentication timeouts and prompts.

Scenario

A small company only has 10 users, but would like to implement stronger user authentication through the PIX Security Appliance. Currently, the budget cannot accommodate a AAA Server. Within the next year, the company plans to expand to 50 users and will need to implement server-based AAA with local AAA backup. Configure the Local AAA features on the PIX.

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology and verify the starting configuration on pod PIX Security Appliance. 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.

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

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

- <http://www.cisco.com/go/pix>

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 authentication {serial enable telnet ssh http} console server-tag [LOCAL]</code>	Configure AAA to authenticate serial, telnet, http, or ssh remote administration sessions
<code>aaa { authentication authorization accounting } match acl-name interface-name server-tag</code>	Bind an ACL to a AAA configuration.
<code>auth-prompt [accept reject prompt] string</code>	Change the AAA challenge text. (Configuration mode.)
<code>clear configure aaa</code>	Removes all AAA 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 auth-prompt</code>	Displays authentication challenge, reject or acceptance prompt.

Command	Description
<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>	Sets the maximum idle time duration. This command is used in global configuration mode.
<code>username {name} {nopassword password password [encrypted]} [privilege priv_level]</code>	Configure a local username and password

Step 1 Add a User in the Local Database

Complete the following steps to configure local users

- a. Configure a local user.

```
PixP(config)# username aaalocal password aaapass privilege 15
```

- b. Verify the user:

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

```
username aaalocal password VaA5TNJEpa8lcyOT encrypted privilege 15
```

Step 2 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 using the local user database for all inbound traffic:

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

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

(Where P = pod number)

- 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 LOCAL
```

- 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. Test the configuration by initiating an HTTP session with the peer bastion host at 192.168.Q.11 or from an Internet PC located on the 172.26.26.0 network, test the configuration by initiating an HTTP session with the pod bastion host.

http://192.168.P.11

(where P = pod number)

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

```
%PIX-6-609001: Built local-host outside:192.168.Q.10
%PIX-6-609001: Built local-host dmz:bastionhost
%PIX-6-302013: Built inbound TCP connection 1645 for
outside:192.168.2.10/4178 (
192.168.2.10/4178) to dmz:bastionhost/80 (192.168.P.11/80)
%PIX-6-109001: Auth start for user '???' from 192.168.Q.10/4178 to
bastionhost/80
%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 1
%PIX-6-109005: Authentication succeeded for user 'aaalocal' from
192.168.2.10/4178 to bastionhost/80 on interface outside.
```

- 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 'aaalocal' at 192.168.Q.10, authenticated
    absolute timeout: 0:05:00
    inactivity timeout: 0:00:00
```

1. What does the value in absolute timeout mean?
-
-

Step 3 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 10.0.P.0
255.255.255.0 0 0 LOCAL
```

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

Verify the configuration:

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

aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 LOCAL
aaa authentication include tcp/0 inside 10.0.1.0 255.255.255.0
0.0.0.0 0.0.0.0 LOCAL
```

- b. Test HTTP outbound authentication from the Student PC. Ping RBB first to test connectivity.

```
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 for HTTP Authentication, enter **aaalocal** 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-6-609001: Built local-host outside:172.26.26.150
```

```
%PIX-6-302013: Built outbound TCP connection 1699 for  
outside:172.26.26.150/80 (172.26.26.150/80) to  
inside:insidehost/4285 (192.168.1.10/4285)
```

```
%PIX-6-109001: Auth start for user '???' from insidehost/4285 to  
172.26.26.150/80
```

```
%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 3
```

```
%PIX-6-109005: Authentication succeeded for user 'aaalocal' from  
insidehost/4285 to 172.26.26.150/80 on interface inside
```

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

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

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

user 'aaalocal' at insidehost, authenticated (idle for 0:00:05)

absolute timeout: 0:05:00

inactivity timeout: 0:00:00

- f. Clear any existing uauth sessions.

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

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

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

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

- g. This form of authentication passes the username and password in clear text. To increase security it is best to use an SSL encrypted session.

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

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

http://172.26.26.150

Please Authenticate

HTTPS Authentication

Username:

Password:

- i. Accept the certificate.

- j. The following will be displayed on the PIX.

```
%PIX-6-109001: Auth start for user '???' from insidehost/4315 to 172.26.26.150/443
%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 5
%PIX-6-109005: Authentication succeeded for user 'aaalocal' from insidehost/4315 to 172.26.26.150/443 on interface inside
```

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 4 Enable Authentication for CLI Access

Complete the following steps to enable authentication of Telnet and ASDM access to the PIX Security Appliance:

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

```
PixP(config)# aaa authentication telnet console LOCAL
PixP(config)# aaa authentication http console LOCAL
```

- 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 LOCAL
aaa authentication include tcp/0 inside 10.0.P.0 255.255.255.0
0.0.0.0 0.0.0.0 LOCAL
aaa authentication telnet console LOCAL
aaa authentication http console LOCAL
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 running-config telnet
insidehost 255.255.255.255 inside
```

- e. Clear any existing 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: aaalocal
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-6-609001: Built local-host NP Identity Ifc:10.0.P.1
%PIX-6-302013: Built inbound TCP connection 1847 for
    inside:insidehost/4346 (insidehost/4346) to NP Identity
    Ifc:10.0.P.1/23 (10.0.1.1/23)
%PIX-7-710001: TCP access requested from insidehost/4346 to
    inside:10.0.P.1/telnet
%PIX-7-710002: TCP access permitted from insidehost/4346 to
    inside:10.0.P.1/telnet
%PIX-6-611101: User authentication succeeded: Uname: aaalocal
%PIX-6-605005: Login permitted from insidehost/4346 to
    inside:10.0.P.1/telnet for user "aaalocal"
```

- i. Close the Telnet session:

```
PixP>quit
```

(where P = pod number)

Step 5 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 any existing uauth sessions

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

	Current	Most	Seen
Authenticated Users	0	1	
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: aaalocal
Password: aaapass
Authentication Successful
Connection to host lost.
```

(where P = pod number)

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

```
%PIX-6-609001: Built local-host outside:192.168.P.5
%PIX-6-302013: Built outbound TCP connection 1909 for
outside:192.168.P.5/23 (192.168.P.5/23) to inside:insidehost/4364
(192.168.P.10/4364)
%PIX-6-109001: Auth start for user '???' from insidehost/4364 to
192.168.P.5/23
%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 7
%PIX-6-109005: Authentication succeeded for user 'aaalocal' from
insidehost/4364 to 192.168.P.5/23 on interface inside
```

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

Since the user has already been authenticated using virtual telnet, there should be no authentication prompt for the HTTP session. Although the HTTP session is already authenticated, a password is still required to access RBB. When prompted, leave the username blank and use **'cisco'** for the password.

- f. Clear the uauth timer:

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

	Current	Most	Seen
Authenticated Users	0		1
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 the user is no longer authenticated and that there is a 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 **aaalocal** for the username and **aaapass** for the password.

1. Why is authentication needed this time?

Step 6 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 runnig 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 runnig-config auth-prompt
```

```
auth-prompt prompt Please Authenticate
```

```
auth-prompt accept You've been Authenticated
```

```
auth-prompt reject Authentication Failed, Try Again
```
- j. Clear any existing uauth sessions:

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

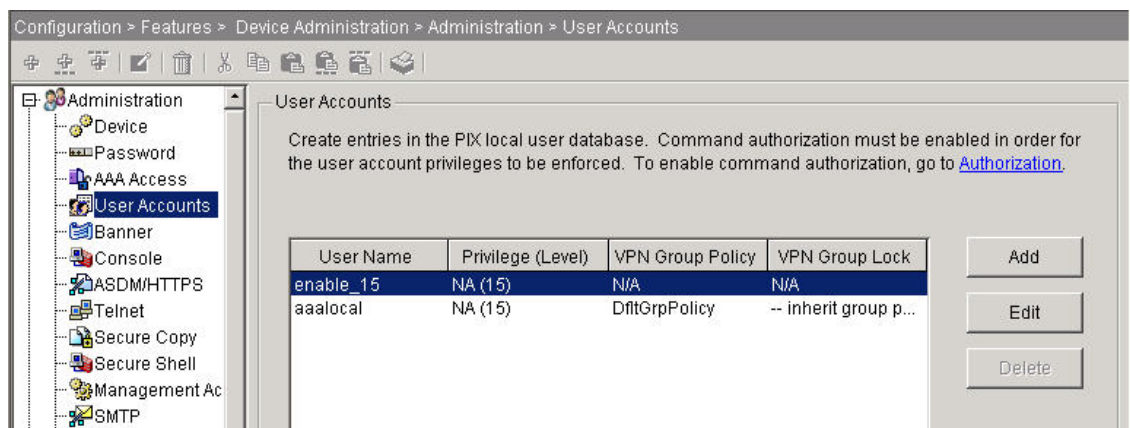
```
PixP(config)# show uauth
```

	Current	Most	Seen
Authenticated Users	0		1
Authen In Progress	0		1
- k. Initiate an HTTP connection to RBB to test the new authentication prompts.
 From the Student PC, enter the following URL in a web browser:
http://172.26.26.150
- l. Verify the running configuration of the PIX Security Appliance against the ending configuration provided for this lab activity.

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 using the **aaalocal** and **aaapass** credentials.
- b. Navigate to **Configuration>Features>Device Administration>Administration>User Accounts**

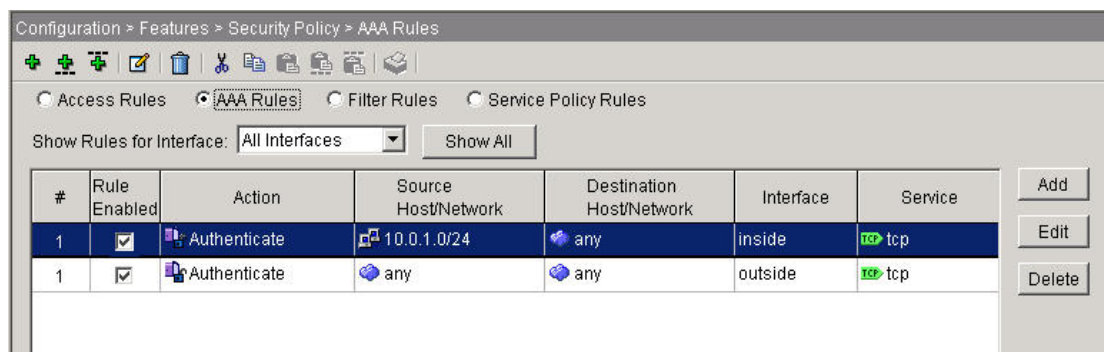


- c. Add a new user **aaalocal2/aaapass2** with a privilege level of **15**. Click **Apply**

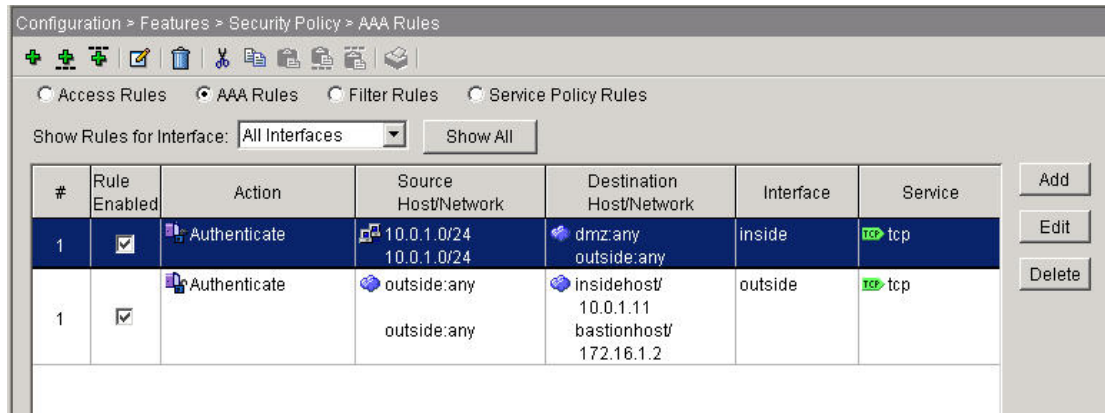
Navigate to **Configuration>>Features>Properties> AAA Setup>Auth. Promt.** Notice the 3 authentication prompts that were configured previously



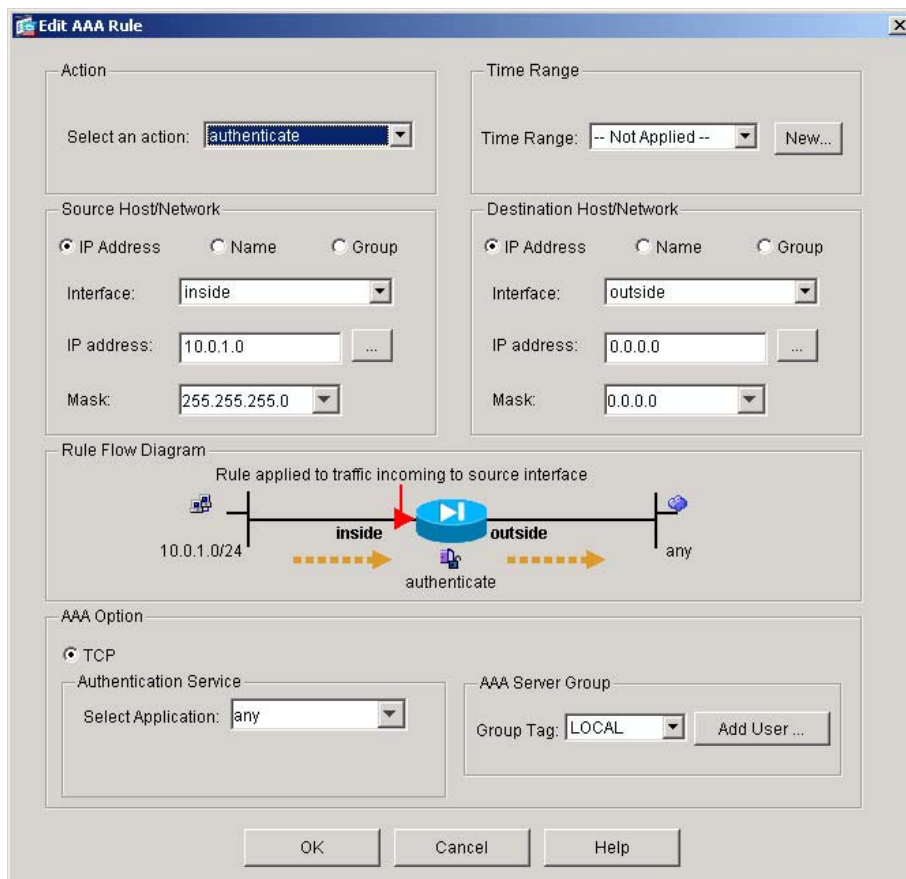
- d. Edit these as desired. Click **Apply** when done.
- e. Navigate to **Configuration>Features>Security Policy**
- f. Click on the **AAA Rules** radio button. Notice the 2 authentication rules that were configured previously.



- g. Click on the **Show Detail** radio button to view more details about the AAA rules.



- h. Double click on the top rule. The Edit Rule window will open.



- i. Review the actions that are available in the drop down menu.
Change the Destination to the DMZ network of 172.16.P.0/24. Click **OK**.
- j. Click **Apply** to change the rule. Click the **Send** button if prompted.
- k. If prompted with a warning that the keyword 'any' will be changed 'to tcp/0' in the configuration, click the **OK** button to continue.
- l. From the Menu, go to **Tools>Command Line Interface**
Clear any existing authentication by entering the `clear uauth` command. Click the **Send** Button. Click the **Close** button after the command is sent.

- m. From the Student PC web browser, initiate an HTTP connection to the DMZ web server. A PIX authentication window will appear.

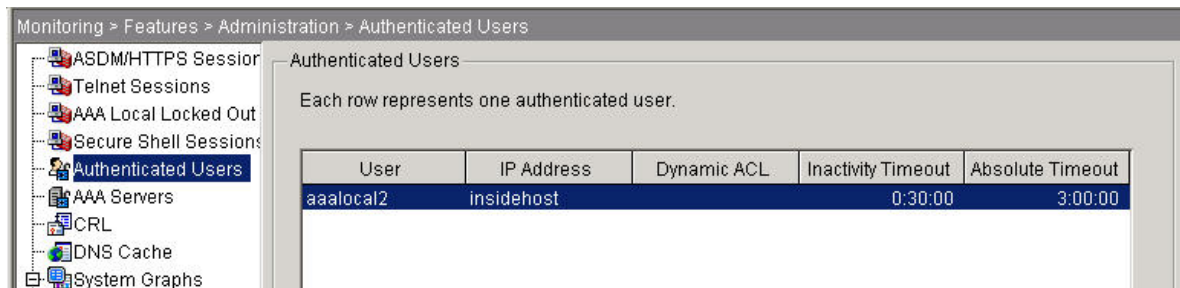
Please Authenticate

HTTPS Authentication

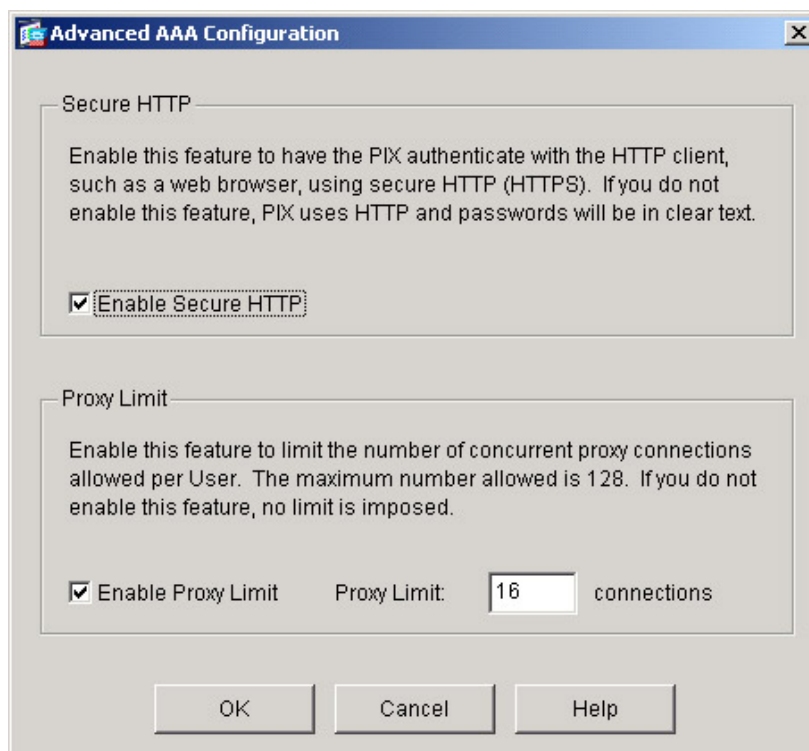
Username:

Password:

- n. Authenticate to the PIX with the username **aaalocal2** and the password **aaapass2..** The DMZ web page should appear.
- o. Return to PDM. Navigate to **Monitoring Features > Administration > Authenticated users** to verify that the user is logged in.



- p. Navigate to **Configuration > Features > Security Policy**. Click on the **AAA Rules** radio button. At the bottom of the Access Rule window, click on the **Advanced** button. This is where the Secure HTTP can be enabled or disabled.



- q. Click on the **Cancel** button in the Advanced AAA Configuration window.