



Lab 8.4.3a Configure User Authentication and Command Authorization using ASDM

Objective

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

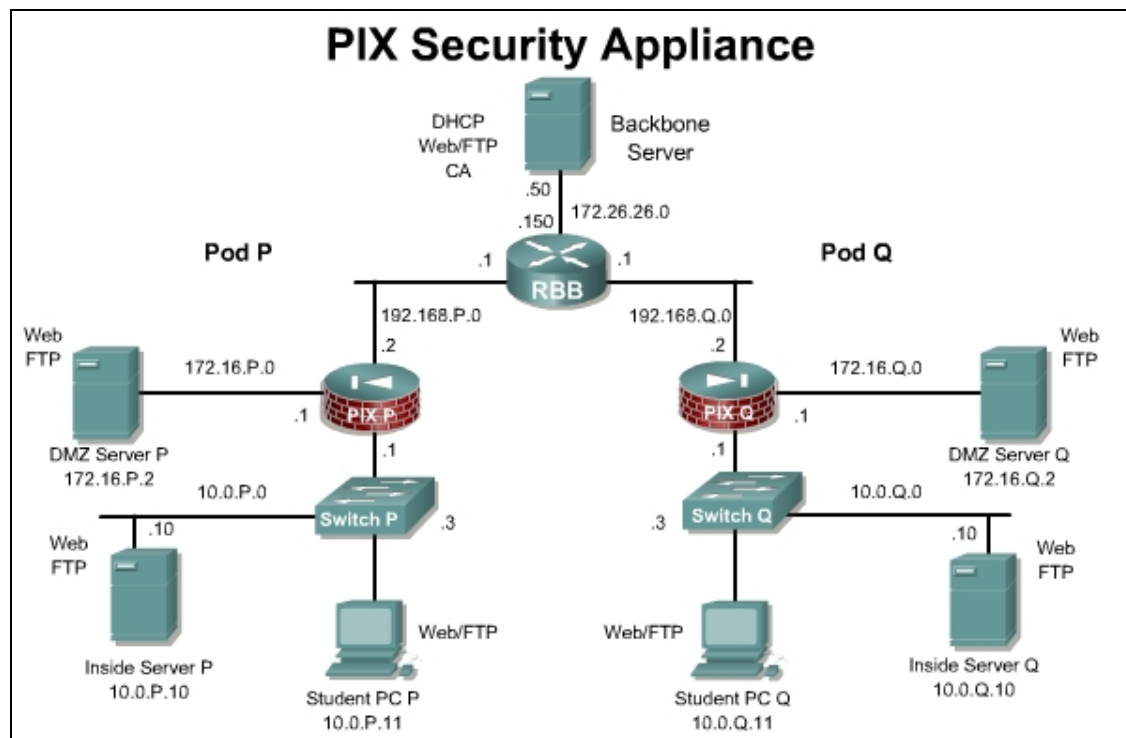
- Configure command authorization.
- Configure Local User Authentication.
- Configure SSH

Scenario

A company has just expanded and now has 5 remote offices with PIX Security Appliances. Currently there are no VPN tunnels between the remote offices and the main office. To increase security of the remote management session, it is necessary to use SSH to protect the administrator username and password. SSH should also be used when managing devices over the LAN. It is also necessary to setup limited access accounts on the PIX for junior administrators and various IT staff.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configurations on the 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.

A SSH client is required for this lab. <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Tools and resources

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

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

Additional materials

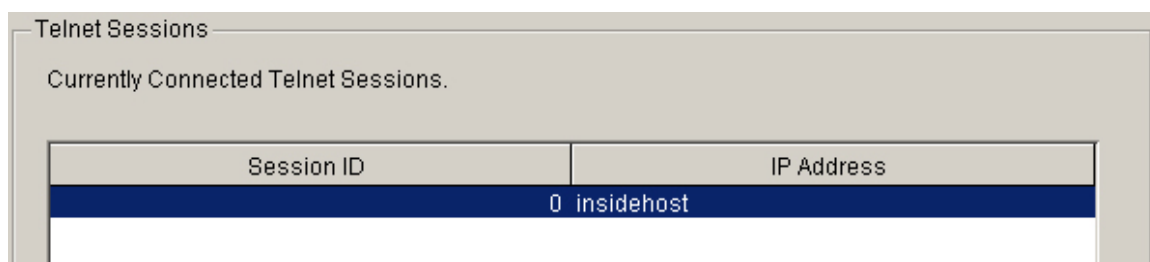
Students can use the following links for more information on the objectives covered in this lab:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450d39.html

Step 1 Configure Administrative Passwords and Monitor Sessions.

To configure these passwords, complete the following steps:

- Initiate an ASDM connection to the PIX Security Appliance.
- Navigate to **Configuration>Features>Device Administration>Administration>Password**.
- Check the **Change the privileged mode password** checkbox.
- Change the enable password to **cisco123**. Click the **Apply** button. Click **Send** if prompted.
- Change the telnet password from the default of **cisco** to **telnet123**. Click the **Apply** button.
- ASDM will prompt for authentication. Log in using **cisco123**.
- On the Student PC, open a command prompt and telnet to the PIX. Notice the failed attempt.
- Navigate to **Configuration>Features>Device Administration>Administration>Telnet**.
- Click the **Add** button. Allow the Student PC address to access the PIX Security Appliance inside interface using Telnet. Apply the changes.
- On the Student PC, open a command prompt and telnet to the PIX.
- Log in using the new **telnet123** password. Enter into privileged mode with the new password **cisco123**.
- Navigate to **Monitoring>Features>Administration>Telnet Sessions**. The following should be displayed:



Session ID	IP Address
0	insidehost

- Close the session, but leave the command prompt window open.

- n. Navigate to **Configuration>Features>Device Administration>Administration>Secure Shell**.
- o. Click the **Add** button. Permit the Student PC address to access the PIX Security Appliance inside interface using Secure Shell. Apply the changes.
- p. On the Student PC, open a PuTTY session and SSH to the PIX
- q. Log in using the default username **pix** the **telnet123** password. Enter into privileged mode with the new password **cisco123**.
- r. Navigate to **Monitoring>Features>Administration>Secure Shell Sessions**. The following should be displayed.

Secure Shell Sessions						
Currently Connected Secure Shell Sessions.						
Client	User	State	Version	Encryption (In)	Encryption (Out)	Host
insidehost	pix	SessionStarted	2.0	aes256-cbc	aes256-cbc	sh...

- s. Navigate to **Monitoring>ASDM/HTTPS Sessions**. The following should be displayed.

ASDM/HTTPS Sessions	
Currently Connected ASDM/HTTPS Sessions.	
Session ID	IP Address
0	insidehost

- t. Disconnect the SSH session.

Step 2 Enable Command Authorization with Privileged Mode Passwords

Perform the following tasks to enable command authorization with privileged mode passwords.

- a. Navigate to **Configuration>Features>Device Administration>Administration>User Accounts**.
- b. Add the following users and apply the changes.

User	Password	Privilege level
admin	admin	15
readonly	readonly	5
monitor	monitor	3
user	user	0

- c. The following users should now appear in the User Accounts window.

User Accounts

Create entries in the PIX local user database. Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

User Name	Privilege (Level)	VPN Group Policy	VPN Group Lock
enable_15	NA (15)	N/A	N/A
admin	NA (15)	DfltGrpPolicy	-- inherit group p...
readonly	NA (5)	DfltGrpPolicy	-- inherit group p...
monitor	NA (3)	DfltGrpPolicy	-- inherit group p...
user	NA (0)	DfltGrpPolicy	-- inherit group p...

Add

Edit

Delete

- d. Click the **Apply** button.
- e. Click the **Authorization** hyperlink to go to **Configuration>Features>Device Administration>Administration>AAA Access>Authorization**.
- f. Click the **Authentication** tab. Enable AAA Authentication for HTTP/ADSM, Serial, SSH, and Telnet using the LOCAL database. Do not apply the changes yet.
- g. Check the **Enable** checkbox to enable AAA authentication to use privileged mode commands. Do not apply the changes yet.

Authentication/Authorization/Accounting

Authentication | Authorization | Accounting

Enable authentication for administrator access to the PIX .

Require authentication to allow use of privileged mode commands

☒ **Enable** Server Group: **LOCAL** ☐ Use LOCAL when server group fails

Require authentication for the following types of connections

☒ HTTP/ASDM Server Group: **LOCAL** ☐ Use LOCAL when server group fails

☒ Serial Server Group: **LOCAL** ☐ Use LOCAL when server group fails

☒ SSH Server Group: **LOCAL** ☐ Use LOCAL when server group fails

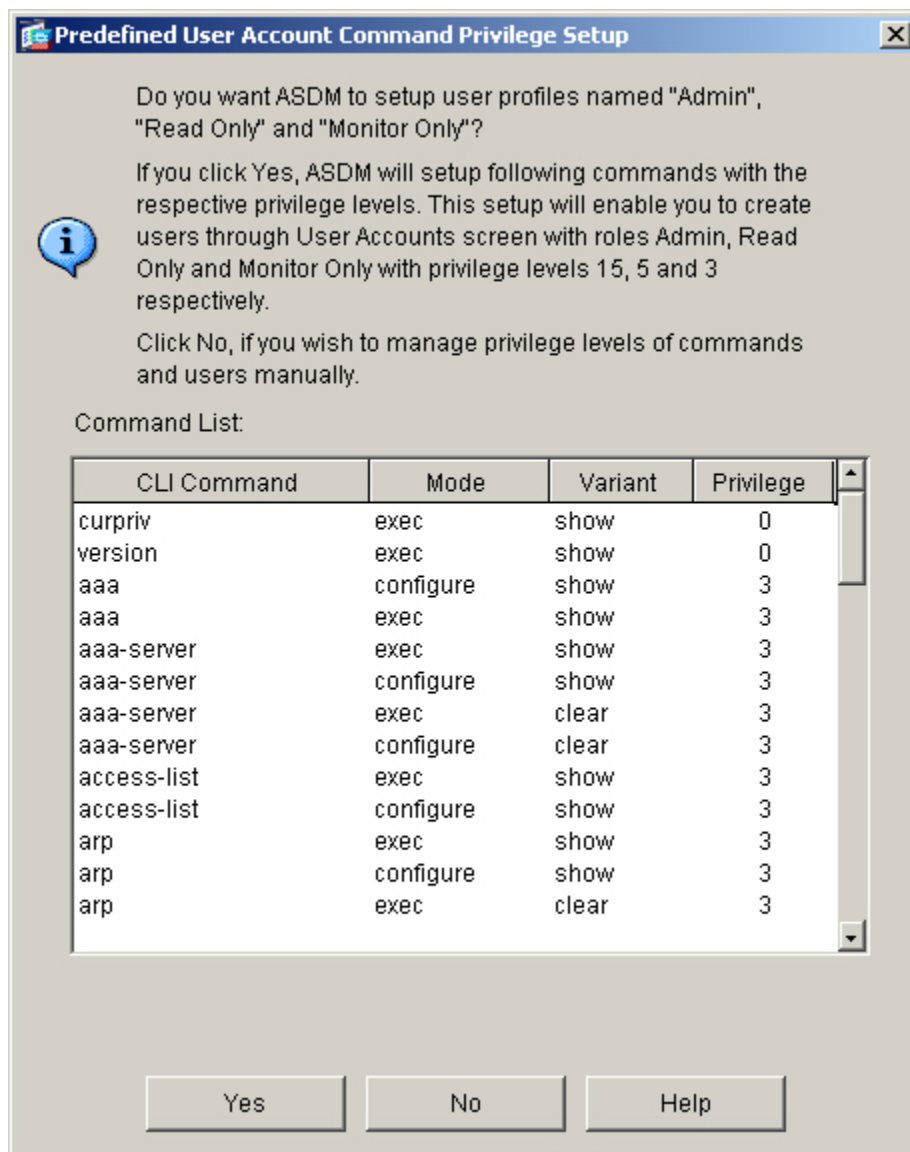
☒ Telnet Server Group: **LOCAL** ☐ Use LOCAL when server group fails

Apply **Reset**

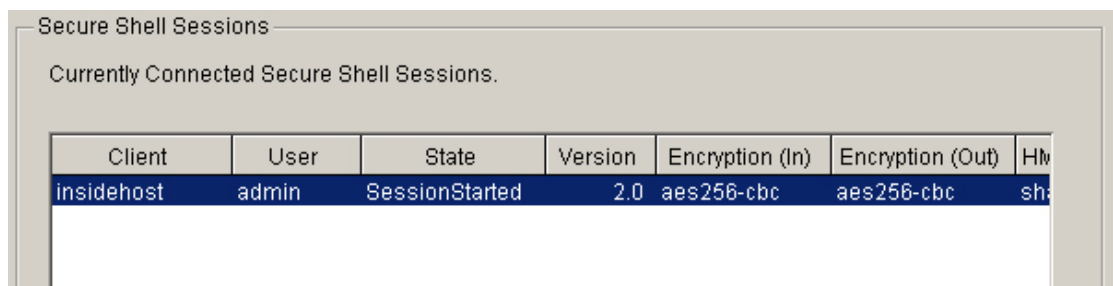
- h. Verify the configuration, using the sample above.
- i. Return to the Authorization tab. Click on the **Advanced** button to view the current privilege levels of all the commands.
- j. Select the checkbox next to **Enable Authorization for PIX command access** to enable command authorization using the LOCAL database.

Note Enabling AAA authentication and authorization for enable commands will cause the user to be required to use the `login` command in user mode to gain access to the enable mode.

- k. Click the **Apply** button to implement the changes.
- l. A message about Predefined User Account Privileges will appear. Note the CLI commands and privilege levels.



- m. Click the **Yes** button to continue.
- n. Click on the **Advanced** button again, noting the new command privilege levels. After reviewing the privilege levels, click the **OK** button to close the window.
- u. On the Student PC, open PuTTY and initiate an SSH connection to the PIX
- v. Log in using the **admin** password. Enter into privileged mode with the new password **admin**.
- w. Navigate to **Monitoring>Features>Administration>Secure Shell Sessions**. The following should be displayed.



- x. Navigate to **Monitoring>Features>Administration>ASDM/HTTPS Sessions**. The following should be displayed.

ASDM/HTTPS Sessions	
Currently Connected ASDM/HTTPS Sessions.	
Session ID	IP Address
0	insidehost

Step 3 Test Command Authorization

- Exit out of the console connection. Log back in using **user/user**. Type the **?** to see which commands are available. Try to enter into privileged mode. Access should be denied.
- Telnet and SSH to the PIX, using the various accounts. Type the **?** to see which commands are available. Try to enter into privileged mode. Exit the sessions when finished.
- Navigate to **Configuration>Features>Device Administration>Administration>AAA Access>Authorization**.
- Click on the **Advanced** button. Allow the readonly user to view the tech support.
- Click on the **tech-support** line, click **Edit** and change to **5**. Click the **OK** button to continue. Click **Apply**.
- Using the console, login with the readonly account. Verify the command is accessible. Logout using the **logout** command.

```
PixP# logout
Logoff
Username:
```

- Change the tech-support command back to level 15.
- Login with the readonly account.
- Verify the show tech-support command is not accessible.

```
PixP# show tech-support
Command authorization failed
```

- View the user account that is currently logged in:

```
PixP# show curpriv
Username : readonly
Current privilege level : 5
Current Mode/s : P_PRIV
```

- Why would different levels and passwords be assigned?
