



## Lab 8.4.3b Configure SSH, Command Authorization, and Local User Authentication using CLI

### Objective

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

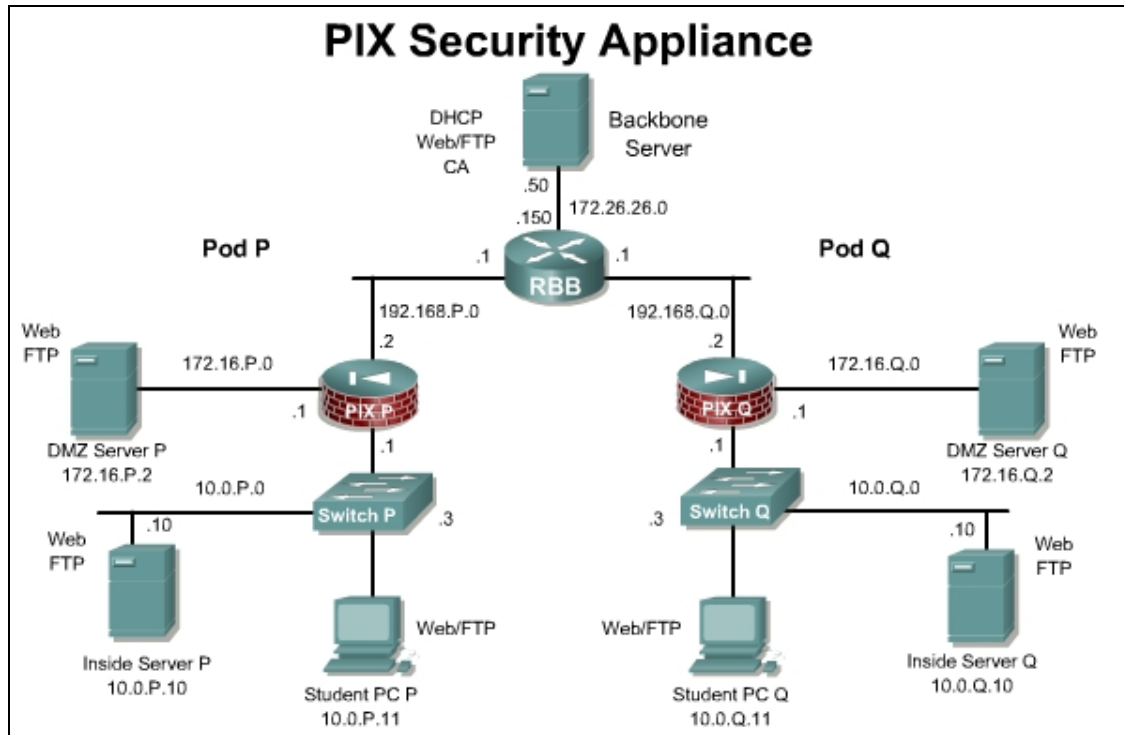
- Configure and verify SSH operation
- Configure command authorization.
- Configure Local User Authentication.

### 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 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 HyperTerminal on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

An 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](http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450d39.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
<b>aaa authorization command</b> <b>{LOCAL   tacacs_server_tag}</b>	Enable or disable LOCAL or TACACS+ user authorization services. Configuration mode.
<b>enable password</b> <i>password</i>	Configures the enable password
<b>ca generate rsa key</b> <i>modulus</i>	The <b>ca generate rsa</b> command generates Rivest, Shamir, and Adleman (RSA) key pairs for the PIX Security Appliance. RSA keys are generated in pairs of one public RSA key and one private RSA key. Configuration Mode.
<b>clear aaa</b>	Removes <b>aaa</b> command statements from the configuration.
<b>debug ssh</b>	Debug information and error messages associated with the <b>ssh</b> command.
<b>privilege [show   clear   configure] level</b> <i>level</i> [ <b>mode enable   configure</b> ] <b>command</b> <i>command</i>	Configures or displays command privilege levels. Configuration mode.
<b>show ca</b>	Displays information about CEP (Certificate Enrollment Protocol).

Command	Description
<b>show ssh [sessions [ip_address]]</b>	Displays active, all or host-specific SSH sessions on the PIX Security Appliance.
<b>ssh timeout mm</b>	Specify a host for PIX Security Appliance console access through Secure Shell (SSH). Configuration mode.
<b>static [(internal_if_name, external_if_name)] {tcp   udp}{global_ip   interface} global_port local_ip local_port [netmask mask][max_conns [emb_limit [norandomseq]]]</b>	Configure a persistent one-to-one address translation rule by mapping a local IP address to a global IP address. This is also known as Static Port Address Translation (Static PAT). Configuration mode.
<b>username username {[{nopassword   password password} [encrypted]] [privilege level]}</b>	Sets the username for the specified privilege level. Configuration mode.

### Step 1 Enable Command Authorization with Privileged Mode Passwords

To enable command authorization with privileged mode passwords, complete the following steps:

- Set privilege level 10 for the enable mode **configure** command:

```
PixP(config)# privilege configure level 10 mode enable command  
configure
```

- Set privilege level 10 for the **nameif** command:

```
PixP(config)# privilege level 10 command nameif
```

- Set privilege level 12 for the **interface** command:

```
PixP(config)# privilege level 12 command interface
```

- Assign an enable password for privileged level 15:

```
PixP(config)# enable password prmode15
```

- Assign an enable password for privileged level 5:

```
PixP(config)# enable password prmode5 level 5
```

- Assign an enable password to privileged level 10:

```
PixP(config)# enable password prmode10 level 10
```

- Assign an enable password to privileged level 12:

```
PixP(config)# enable password prmode12 level 12
```

- Why would different levels and passwords be assigned?

---



---

- h. Enable command authorization by entering the following command:

```
PixP(config)# aaa authorization command LOCAL
```

1. What other command authorization services can be used? Why can't RADIUS be used?
- 

- i. Exit configuration mode:

```
PixP(config)# exit
```

```
PixP#
```

- j. Exit privileged mode:

```
PixP# exit
```

```
Logoff
```

```
Type help or '?' for a list of available commands.
```

```
PixP>
```

## Step 2 Test the Command Authorization

To test the command authorization configured in Step 1, complete the following steps:

- a. Enter privileged mode level 12. When prompted for a password, enter **prmode12**.

```
PixP> enable 12
```

```
Password:
```

```
PixP#
```

- b. Enter configuration mode:

```
PixP# configure terminal
```

- c. Verify that the **interface** command is useable:

```
PixP(config)# interface ethernet2
```

- d. Verify that the **nameif** command is useable:

```
PixP(config-if)# nameif PRIVTEST
```

- e. View the configuration:

```
PixP(config-if)# show nameif
```

Interface	Name	Security
Ethernet0	outside	0
Ethernet1	inside	100
Ethernet2	PRIVTEST	50

- f. Exit configuration mode:

```
PixP(config)# end
```

```
PixP#
```

- g. Exit privileged mode:

```
PixP# exit
```

```
Logoff
```

```
Type help or '?' for a list of available commands.
```

PixP>

- h. Enter privileged mode level 10. When prompted for a password, enter **prmode10**:

PixP> **enable 10**

Password:

PixP#

- i. Enter configuration mode:

PixP# **configure terminal**

PixP(config)#

- j. Try to use the **interface** command:

PixP(config)# **interface ethernet2**

Command authorization failed.

- k. Exit configuration mode:

PixP(config)# **exit**

PixP#

- l. Exit privileged mode:

PixP# **exit**

Logoff

Type help or '?' for a list of available commands.

PixP>

- m. Enter privileged mode level 5. When prompted for a password, enter **prmode5**.

PixP> **enable 5**

Password:

PixP#

- n. Try to enter configuration mode:

PixP# **configure terminal**

Command authorization failed.

- o. Exit privileged mode:

PixP# **exit**

Logoff

Type help or '?' for a list of available commands.

PixP>

- p. Enter privileged mode. When prompted for a password, enter **prmode15**.

PixP> **enable**

Password:

PixP#

- q. Enter configuration mode:

PixP# **configure terminal**

PixP(config)#

### Step 3 Generate an RSA Key Pair

To generate an RSA key pair to encrypt the SSH terminal session, complete the following steps:

- a. Delete any previously created RSA keys:

```
PixP(config)# crypto key zeroize rsa
```

- b. Save the configuration to complete the erasure of the old RSA key pair:

```
PixP(config)# write memory
```

- c. Configure the domain name:

```
PixP(config)# domain-name cisco.com
```

- d. Generate an RSA key pair to use to encrypt SSH sessions:

```
PixP(config)# crypto key generate rsa modulus 1024
```

```
INFO: The name for the keys will be: <Default-RSA-Key>
```

```
Keypair generation process begin. Please wait...
```

```
PixP(config)#
```

1. What are the modulus sizes that can be used?
- 

- e. Save the keys to Flash memory:

```
PixP(config)# write memory
```

- f. View the public key:

```
PixP(config)# show crypto key mypubkey rsa
```

```
Key pair was generated at: 16:05:11 UTC Jun 4 2005
```

```
Key name: <Default-RSA-Key>
```

```
Usage: General Purpose Key
```

```
Modulus Size (bits): 1024
```

```
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181  
00bc43bf
```

```
33d9c65d e508b6df ecf71e37 5574a21d 56185faf cbb9fe14 5a345222  
42cd2927
```

```
604fd719 a58d4f82 dc382fc4 ae037d15 f4f11ca8 06020c8d 5cd350d1  
9bf19457
```

```
a6dc1a86 f1e101ae 842b0281 f42f38c5 c8e5c095 711ac751 f28d693f  
ffdc40f
```

```
2892169e 90be60dd 15c2fdc9 b8bda690 e55b29bf 670ed794 30e9c012  
5f020301 0001
```

(where P = pod number)

### Step 4 Connect to the PIX Security Appliance using SSH

To securely connect to the PIX Security Appliance using SSH, complete the following steps:

- a. Enable SSH debugging:

```
PixP(config)# debug ssh
```

```
SSH debugging on
```

- b. Grant SSH access to the inside subnet:

- For a local lab:

```
PixP(config)# ssh 10.0.P.0 255.255.255.0 inside
```

(where P = pod number)

- c. Set the SSH inactivity timeout to 30 minutes:

```
PixP(config)# ssh timeout 30
```

- d. Minimize, but do not close, the HyperTerminal session window. Double-click the **PuTTY** icon on the desktop. The shortcut will vary depending on the SSH client used.

- e. Enter the IP Address of the pod PIX.

```
10.0.P.1
```

- f. Select the **SSH** radio button.

- g. Click **Yes** to the Security Warning window. The SSH Authentication window opens.

- h. The following will be displayed in the PIX console:

```
SSH: Device opened successfully.
SSH0: SSH client: IP = 'insidehost' interface # = 2
SSH: host key initialised
SSH: license supports 3DES: 2
SSH: license supports DES: 2
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message:
      83 (83)
SSH0: client version is - SSH-2.0-PuTTY-Release-0.56
client version string:SSH-2.0-PuTTY-Release-0.56SSH0: begin server
      key generation
SSH0: complete server key generation, elapsed time = 1980 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes256-cbc hmac-shal none
SSH2: kex: server->client aes256-cbc hmac-shal none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
```

- i. Enter **pix** as the username and **cisco** as the pass phrase.

```
SH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication successful for pix
SSH2 0: channel open request
SSH2 0: pty-req request
SSH2 0: requested tty: xterm, height 24, width 80
SSH2 0: shell request
SSH2 0: shell message received
SSH2 0: channel window adjust message received 52
SSH2 0: channel window adjust message received 7
```

- j. In the SSH window, enter the privileged mode. When prompted for a password, enter **prmode15**.

```
PixP>enable
Password:
PixP#
```

- k. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```

- l. To view the status the SSH session, enter the following command:

```
PixP(config)# show ssh sessions
```

SID	Client IP	Version	Mode	Encryption	Hmac	State	Username
0	insidehost	2.0	IN	aes256-cbc	sha1	SessionStarted	pix
			OUT	aes256-cbc	sha1	SessionStarted	pix

- m. Disconnect the SSH session:

```
PixP(config)# ssh disconnect 0
```

- n. Return to the HyperTerminal session window, and change the PIX Security Appliance's Telnet password from **cisco** to **sshpass**:

```
PixP(config)# passwd sshpass
```

- o. Exit configuration mode:

```
PixP(config)# exit
PixP#
```

- p. Exit privileged mode:

```
PixP# exit
Logoff
Type help or '?' for a list of available commands.
PixP>
```

- q. Minimize the HyperTerminal window. Do not close it.

- r. Leave this HyperTerminal session open throughout the rest of this lab exercise.



- s. Establish another SSH session to the PIX Security Appliance. When prompted to authenticate, enter **pix** as the username and **sshpass** as the pass phrase.

## Step 5 Configure Local User Authentication using a Secure SSH Session

To configure local user authentication using a secure SSH session, complete the following steps:

- a. Enter privileged mode. When prompted for a password, enter **prmode15**.

```
PixP>enable
```

```
Password:
```

```
PixP#
```

- b. Enter configuration mode:

```
PixP# configure terminal
```

```
PixP(config)#
```

- c. Create three user accounts in the local database:

```
PixP(config)# username user10 password user10pass privilege 10
```

```
PixP(config)# username user12 password user12pass privilege 12
```

```
PixP(config)# username admin password adminpass privilege 15
```

1. Why is setting user's privilege level different recommended?

---

---

- d. Enable authentication using the LOCAL database:

```
PixP(config)# aaa authentication enable console LOCAL
```

- e. Disconnect the SSH session.

## Step 6 Test Command Authorization with Local User Authentication

To test command authorization with local user authentication, complete the following steps:

- a. Return to the HyperTerminal session.
- b. Enter privileged mode. When prompted for a username, enter **user12**. When prompted for a password, enter **user12pass**.

```
PixP> enable
```

```
Username:
```

```
Password:
```

```
PixP#
```

- c. Enter configuration mode:

```
PixP# configure terminal
```

```
PixP(config)#
```

- d. View the user account that is currently logged in:

```
PixP(config)# show curpriv
```

```
Username : user12
```

```
Current privilege level : 12
```

```
Current Mode/s : P_PRIV P_CONF
```

- e. Verify that the **interface** command is useable:

```
PixP(config)# interface ethernet2
```

Verify that the **nameif** command is useable by attempting to change the Ethernet 2 name back to **dmz**:

```
PixP(config-if)# nameif dmz
```

- f. View the configuration:

```
PixP(config)# show nameif
```

Interface	Name	Security
Ethernet0	outside	0
Ethernet1	inside	100
Ethernet2	dmz	50

- g. Try to create a static mapping for a demilitarized zone (DMZ) host 172.16.P.4:

```
PixP(config)# static (dmz,outside) 192.168.P.18 172.16.P.4 netmask 255.255.255.255
```

Command authorization failed

(where P = pod number)

- h. Log out of the user12 account:

```
PixP(config)# logout
```

Logoff

Type help or '?' for a list of available commands.

```
PixP>
```

- i. Log in to the user 10 account. When prompted for a username, enter **user10**. When prompted for a password, enter **user10pass**.

```
PixP>login
```

Username:

Password:

```
PixP#
```

- j. Enter configuration mode:

```
PixP# config t
```

```
PixP(config)#
```

- k. Try to use the **interface** command to configure the Ethernet 2 interface:

```
PixP(config)# interface ethernet2
```

Command authorization failed

- n. Log out of the user10 account:

```
PixP(config)# logout
```

Logoff

Type help or '?' for a list of available commands.

```
PixP>
```

- o. Log in to the user admin account. When prompted for a username, enter **admin**. When prompted for a password, enter **adminpass**.

```
PixP>login
```

Username:

Password:

PixP#

- p. Enter configuration mode:

PixP# **configure terminal**

PixP(config)#

- q. Clear the AAA configuration:

PixP(config)# **clear configure aaa**