



Lab 8.4.4 Perform Password Recovery on the PIX Security Appliance

Objective

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

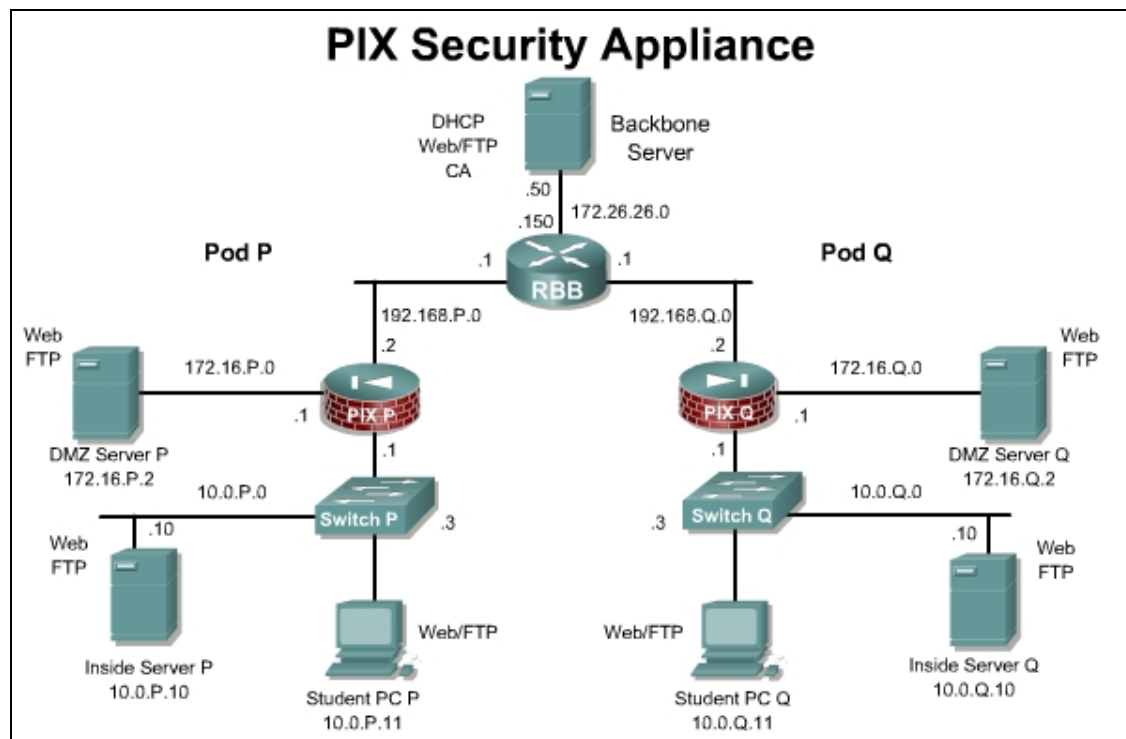
- Upgrade the PIX Security Appliance image.
- Perform password recovery procedures.

Scenario

One of the major job duties of a network administrator is planning. Network administrators plan for new network design projects, future performance requirements, image upgrades, and contingency plans. Upgrading and performing password recovery are core skills needed by all network administrators. There may be situations when network administrators are locked-out of their PIX Security Appliance. Password lockouts can occur from incorrectly configured enable passwords, incorrectly configured AAA parameters, and improperly documenting passwords. In this lab, students will perform the steps involved in performing password recovery and upgrading the image of a PIX Security Appliance.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the 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. Also, download the proper password recovery file and copy to the TFTP root folder. Some TFTP programs may not work properly with the PIX.

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- TFTP server
- PIX password recovery file (np70.bin)

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/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450b92.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>clear xlate</code>	Clears the contents of the translation slots.
<code>copy tftp[:[<i>location</i>] [<i>tftp_pathname</i>]] flash[:<i>path</i>]</code>	Downloads Flash memory software images via TFTP without using monitor mode.
<code>reload</code>	Reloads the PIX Security Appliance.

Step 1 Perform a Password Recovery for the PIX Security Appliance Model 515E

To perform a password recovery for the PIX Security Appliance model 515E, complete the following steps:

- Open and minimize the TFTP server on the desktop.
- Clear the translation table on the PIX Security Appliance:

```
PixP(config)# clear xlate
```
- Create an enable password for entering into privileged mode:

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

- d. Save the configuration:

```
PixP(config)# write memory  
Building configuration...  
Cryptochecksum: e18c684e d86c9171 9f63acf0 f64a8b43  
[OK]
```

- e. Log out of the admin account:

```
PixP(config)# logout  
Logoff  
Type help or '?' for a list of available commands.  
PixP>
```

- f. Attempt to enter privileged mode with the old password, **prmode15**:

```
PixP> enable  
Password:  
Invalid password:
```

- g. Enter privileged mode with the new password, **badpassword**:

```
Password:  
PixP#
```

- h. Reboot the PIX Security Appliance.

```
PixP# reload
```

Note If the enable password is lost and the **reload** command cannot be used, the PIX can be powered off and then powered back on using the power switch on the back of the appliance.

- i. When the PIX Security Appliance reboots, interrupt the boot process to enter monitor mode. To do this, press the Escape key or send a break character.

- j. Specify the PIX Security Appliance interface to use for TFTP:

```
monitor> interface 1
```

- k. Specify the PIX Security Appliance interface IP address:

```
monitor> address 10.0.P.1  
(where P = pod number)
```

- l. Verify connectivity to the TFTP server:

```
monitor> ping 10.0.P.11  
(where P = pod number)
```

- m. Name the server:

```
monitor> server 10.0.P.11  
(where P = pod number)
```

- m. Name the image filename:

```
monitor> file np70.bin
```

- o. Start the TFTP process:

```
monitor> tftp
```

```
tftp
np70.bin@10.0.0.11.....
.....
.....
```

Received 73728 bytes

Cisco Secure PIX Firewall password tool (3.0) #0: Wed Mar 27
11:02:16 PST 2002

Flash=i28F640J5 @ 0x300

BIOS Flash=AT29C257 @ 0xd8000

(where P = pod number)

- p. When prompted, press **Y** to erase the password:

Do you wish to erase the passwords? [yn] **y**

The following lines will be removed from the configuration:

enable password GlFe5rCOwv2JUi5H level 5 encrypted

enable password .7P6WvOREyZHKnus level 10 encrypted

enable password tgGMO76/Nf26X5Lv encrypted

passwd w.UT.4mPsVA4l8Ij encrypted

Do you want to remove the commands listed above from the
configuration? [yn]

Please enter a y or n.

- q. When prompted, press **Y** to erase the passwords:

Do you want to remove the commands listed above from the
configuration? [yn] **y**

Passwords and aaa commands have been erased.

The system automatically erases the passwords and starts rebooting.

Note If AAA is running, it will prompt for a username and password (user: pix, password:
<enter>).

- r. Verify that the password **badpassword** has been erased by entering privileged mode on the PIX Security Appliance:

Pix> **enable**

password: **<Enter>**

PixP#

Step 2 Load the PIX Security Appliance 515E Image Using TFTP

To load the PIX Security Appliance 515E image using TFTP, complete the following steps:

- a. Ask the instructor for the PIX security appliance image file name. Use the **copy tftp flash** command to load the image file:

PixP# **copy tftp: flash:**

Address or name of remote host[]? **10.0.1.10**

Source filename []? **pix-701.bin**

Destination filename [pix-701.bin]? **<Enter>**

(where P = pod number)

- b. Use the **show bootvar** command to ensure that the boot image file is correctly defined. If it is not, be sure to use the **boot system flash** command to set the boot image:

```
PixP# show bootvar
BOOT variable = flash:/pix701.bin
Current BOOT variable = flash:/pix701.bin
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

- c. After the PIX Security Appliance has received the image from the TFTP server and it has been verified that the boot variable is pointing to the correct image, reload the PIX Security Appliance. When prompted to confirm, press **Enter**.

```
PixP# reload
Proceed with reload? [confirm] <Enter>
```

(where P = pod number)

- d. After the PIX finishes reloading, enter the **show version** command to verify that the correct version PIX Security appliance has been loaded.

```
PixP> show version
Cisco PIX Security Appliance Software Version 7.0(1)
Device Manager Version 5.0(1)
Compiled on Thu 31-Mar-05 14:37 by builders
System image file is "flash:/pix701.bin"
Config file at boot was "startup-config"
Pixl up 7 mins 48 secs
Hardware:   PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xffff00000, 16MB
BIOS Flash AM29F400B @ 0xffffd8000, 32KB

 0: Ext: Ethernet0           : media index  0: irq 10
 1: Ext: Ethernet1           : media index  1: irq 11
 2: Ext: Ethernet2           : media index  2: irq 11

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering                : Enabled
Security Contexts           : 5
```

GTP/GPRS : Disabled
VPN Peers : Unlimited
This platform has an Unrestricted (UR) license.
Serial Number: 807043526
Running Activation Key: 0xc335d572 0xa882e04f 0x24f21c7c 0xbbe45090
0x420cf18a
Configuration has not been modified since last system restart.
(where P = pod number)