



Lab 3.4.6b Configure the PIX Security Appliance using CLI

Objective

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

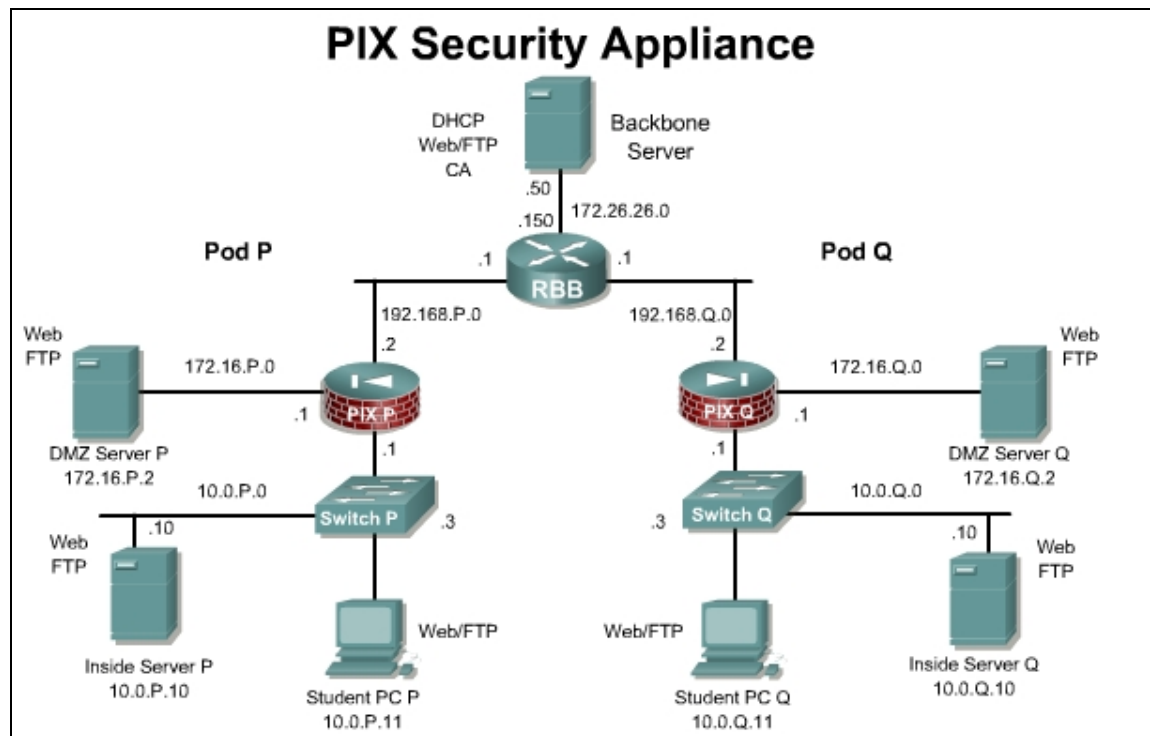
- Execute general maintenance commands.
- Configure the PIX Security Appliance inside and outside interfaces.
- Test and verify basic PIX Security Appliance operation.

Scenario

ASDM is very useful for the most common configurations; however advanced configuration and modification of existing PIX configuration are usually best completed through the CLI. Afterwards, the configuration can be pasted in PIX configuration mode. Students familiar with IOS should be able to quickly adapt to the PIX IOS-like command structure.

Topology:

This figure illustrates the lab network environment.



Preparation

Verify the devices are cabled according to the standard lab topology. Access the PIX console port using the terminal emulator on the Student PC. If desired, save the configuration to a text file for later analysis. Refer back to the “Student Lab Orientation” if more help is needed.

Tools and Resources

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

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

Additional Materials

Further information about the objectives covered in this lab can be found at, http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080423230.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
interface	To configure an interface and enter interface configuration mode, use the interface command in global configuration mode.
ip address <i>ip_address</i> <i>[netmask]</i>	The ip address command defines the IP address of each interface.
nameif <i>if_name</i>	The nameif command defines a name of an interface. This command is used to assign interface names on the PIX Security Appliance.
security-level	To set the security level of an interface, use the security-level command in interface configuration mode. The interface named as inside has a default security level of 100, and the interface named as outside has a default security level of 0.
reload	The reload command reboots the PIX Security Appliance and reloads the configuration from a bootable floppy disk or, if a diskette is not present, from Flash memory.
route <i>if_name ip_address</i> <i>netmask gateway_ip [metric]</i>	Use the route command to enter a default or static route for an interface.
show history	The show history command displays previously entered commands.

Command	Description
<code>show memory</code>	The <code>show memory</code> command displays a summary of the maximum physical memory and current free memory available to the PIX Security Appliance operating system. Memory in the PIX Security Appliance is allocated as needed.
<code>show running-config</code>	The <code>show run</code> command displays the current configuration on the terminal.
<code>show version</code>	The <code>show version</code> command displays the following details of the PIX Security Appliance unit such as software version, operating time since last reboot, processor type, flash memory type, interface boards, serial number (BIOS ID), activation key value , timestamp for when the configuration was last modified
<code>write erase</code>	The <code>write erase</code> command clears the Flash memory configuration.
<code>write memory</code>	The <code>write memory</code> command stores the current configuration in Flash memory, along with the activation key value and timestamp for when the configuration was last modified.
<code>write terminal</code>	The <code>write terminal</code> command displays the current configuration on the terminal.

Step 1 Practice General Commands

The instructor will provide the procedures for access to the PIX Security Appliance console port, as this will vary according to the lab connectivity. After connecting to the PIX Security Appliance console port, the PIX Security Appliance prompt appears. If the prompt that appears is not the configuration mode prompt, enter configuration mode. The password should be null. Ask the instructor for assistance if necessary.

```
PixP>enable
Password: <Enter>
PixP#configure terminal
PixP(config)#
```

- Erase the PIX Security Appliance default configuration. When prompted to confirm, press **Enter**.

```
PixP(config)# write erase
Erase PIX configuration in flash memory? [confirm] <Enter>
```

- Reboot the PIX Security Appliance. When prompted to confirm, press **Enter**.

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

- The PIX Security Appliance prompts to load through interactive prompts. Press **Ctrl + Z** to escape, or type **no** at the prompt and press **Enter**. The unprivileged mode prompt appears.

```
Pre-configure PIX Firewall through interactive prompts [yes]?
Ctrl + Z
pixfirewall>
```

- d. Display the list of help commands:

```
pixfirewall> ?
```

- e. Enter the privileged mode of the PIX Security Appliance. When prompted for a password, press **Enter**.

```
pixfirewall> enable
Password: <Enter>
pixfirewall#
```

- f. Display the list of help commands:

```
pixfirewall# ?
```

- g. Use the **write terminal** or **show run** command to display the PIX Security Appliance configuration on the terminal screen.

Note	Press the Q key to escape the PIX Security Appliance output. Press the Enter key to go line by line. Press the Spacebar to go page by page. Also, the write terminal and show run commands can be used in Privileged EXEC [pixfirewall#] and Global Configuration [pixfirewall(config)#] modes on a PIX Security Appliance. This is different from the operations of a Cisco IOS Router.
-------------	---

```
pixfirewall# write terminal
: Saved
:
PIX Version 7.0(1)
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
pager lines 24
no failover
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
```

```

inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
[OK]
pixfirewall#
h.      Enter the show memory command:
pixfirewall# show memory

```

1. How many total bytes does the PIX Security Appliance have? How many bytes are free?
-
-

- h. Enter the **show version** command:

```

pixfirewall# 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"
pixfirewall up 3 mins 37 secs
Hardware:   PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xffff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 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.
```

- i. Enter the **show history** command:

```
pixfirewall# show history
```

1. What commands are displayed with the show history command?
-
-

Note: The up and down cursor keys on the keyboard can be used to recall commands. The IOS shortcuts **Ctrl + P** and **Ctrl + N** can also be used in the same way.

- j. Enter the configuration mode and change the hostname to **PixP** using the **hostname** command:

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

(where P = pod number)

- k. Enable the use of names rather than IP addresses:

```
PixP(config)# names
```

- l. Assign the name 'bastionhost' to the server on the DMZ:

```
PixP(config)# name 172.16.P.2 bastionhost
```

(where P = pod number)

- m. Assign the name 'insidehost' to the student PC:

```
PixP(config)# name 10.0.P.11 insidehost
```

(where P = pod number)

- n. Save the configuration to Flash memory:

```
PixP(config)# write memory
Building configuration...
Cryptchecksum: e901c202 27a9db19 7e3c2878 0fc0966b
[OK]
```

Step 3 Configure PIX Security Appliance Interfaces

To configure PIX Security Appliance Ethernet interfaces, complete the following steps:

- a. Configure the PIX Security Appliance interfaces as follows:

```
PixP(config)# interface ethernet0
Pix1(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
Pix1(config-if)# ip address 192.168.P.2 255.255.255.0
Pix1(config-if)# speed auto
Pix1(config-if)# duplex full
Pix1(config-if)# no shutdown
```

```

Pixl(config-if)# interface ethernet2
Pixl(config-if)# nameif dmz
Pixl(config-if)# security-level 50
Pixl(config-if)# ip address 172.16.P.1 255.255.255.0
Pixl(config-if)# speed auto
Pixl(config-if)# duplex full
Pixl(config-if)# no shutdown
Pixl(config-if)# interface ethernet1
Pixl(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
Pixl(config-if)# ip address 10.0.P.1 255.255.255.0
Pixl(config-if)# speed auto
Pixl(config-if)# duplex full
Pixl(config-if)# no shutdown
PixP(config)# show nameif

```

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

Note By default the interfaces are disabled.

Note Make sure to check the switch or hub device, which connects to the PIX. A different hardware speed and duplex setting may be required.

- b. Verify the interface configuration with the **show interface** command:

```

PixP(config)# show interface
Interface Ethernet0 "outside", is up, line protocol is up
Hardware is i82559, BW 100 Mbps
    Full-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000b.fd81.e81d, MTU 1500
    IP address 192.168.1.2, subnet mask 255.255.255.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier

```



```

    input queue (curr/max blocks): hardware (128/128) software
    (0/0)

    output queue (curr/max blocks): hardware (0/0) software (0/0)
    Received 0 VLAN untagged packets, 0 bytes
    Transmitted 0 VLAN untagged packets, 0 bytes
    Dropped 0 VLAN untagged packets

Interface Ethernet1 "inside", is up, line protocol is up
Hardware is i82559, BW 100 Mbps
    Full-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000b.fd81.e81e, MTU 1500
    IP address 10.0.1.1, subnet mask 255.255.255.0
    57 packets input, 11088 bytes, 0 no buffer
    Received 57 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software
    (0/0)

    output queue (curr/max blocks): hardware (0/0) software (0/0)
    Received 0 VLAN untagged packets, 0 bytes
    Transmitted 0 VLAN untagged packets, 0 bytes
    Dropped 0 VLAN untagged packets

    Interface Ethernet2 "dmz", is up, line protocol is up
Hardware is i82559, BW 100 Mbps
    Full-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 0002.b3bb.d61f, MTU 1500
    IP address 172.16.1.1, subnet mask 255.255.255.0
    54 packets input, 10812 bytes, 0 no buffer
    Received 54 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software
    (0/1)

    output queue (curr/max blocks): hardware (0/1) software (0/1)
    Received 15 VLAN untagged packets, 3113 bytes

```

Transmitted 1 VLAN untagged packets, 28 bytes

Dropped 15 VLAN untagged packets

- c. Ensure that the IP addresses are correctly configured and are associated with the proper network interface:

```
PixP(config)# show ip address
```

System IP Addresses:

Interface	Name	IP address	Subnet mask
Ethernet0	outside	192.168.P.2	255.255.255.0
Ethernet1	inside	10.0.P.1	255.255.255.0
Ethernet2	dmz	172.16.P.1	255.255.255.0

Current IP Addresses:

Interface	Name	IP address	Subnet mask
Ethernet0	outside	192.168.P.2	255.255.255.0
Ethernet1	inside	10.0.P.1	255.255.255.0
Ethernet2	dmz	172.16.P.1	255.255.255.0

where P = pod number)

- d. Write the configuration to the Flash memory:

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

- e. Use the **show config** command to verify the saved configuration

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

Step 4 Configure global addresses, NAT, and routing for inside and outside interfaces

Complete the following steps to configure a global address pool, Network Address Translation (NAT), and routing:

- a. Enable nat configuration requirement

```
PixP(config)# nat-control
```

- b. Assign one pool of registered IP addresses for use by outbound connections:

```
PixP(config)# global (outside) 1 192.168.P.20-192.168.P.254 netmask 255.255.255.0
```

```
PixP(config)# show run global
```

```
global (outside) 1 192.168.P.20-192.168.P.254 netmask 255.255.255.0
```

(where P = pod number)

- c. Configure the PIX Security Appliance to allow inside hosts to use NAT for outbound access:

```
PixP(config)# nat (inside) 1 10.0.P.0 255.255.255.0
```

(where P = pod number)

- d. Display the currently configured NAT:

```
PixP(config)# show run nat
```

```
nat (inside) 1 10.0.P.0 255.255.255.0 0 0
```

(where P = pod number)

- e. Assign a default route:

```
PixP(config)# route outside 0 0 192.168.P.1
```

(where P = pod number)

- f. Display the currently configured routes:

```
PixP(config)# show route
```

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.P.1, outside
```

```
C    10.0.P.0 255.255.255.0 is directly connected, inside
```

```
C    172.16.P.0 255.255.255.0 is directly connected, dmz
```

```
C    192.168.P.0 255.255.255.0 is directly connected, outside
```

(where P = pod number)

1. Is newly created default route shown in the output? What is the difference between the newly created route and the other routes displayed?

- g. Copy the current configuration to Flash memory:

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

- h. Write the current configuration to the terminal and verify that the previous commands have been entered correctly:

```
PixP(config)# write terminal
```

```
: Saved
```

```
:
```

```
PIX Version 7.0(1)
```

```
names
```

```
name 172.16.1.2 bastionhost
```

```
name 10.0.1.11 insidehost
```

```
!
```

```
interface Ethernet0
```

```
duplex full
```

```
nameif outside
```

```
security-level 0
```

```
ip address 192.168.P.2 255.255.255.0
```

```

!
interface Ethernet1
    duplex full
    nameif inside
    security-level 100
    ip address 10.0.P.1 255.255.255.0
!
interface Ethernet2
    duplex full
    nameif dmz
    security-level 50
    ip address 172.16.P.1 255.255.255.0
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PixP
ftp mode passive
pager lines 24
mtu dmz 1500
mtu outside 1500
mtu inside 1500
no failover
monitor-interface dmz
monitor-interface outside
monitor-interface inside
asdm image flash:/asdm
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 192.168.P.20-192.168.P.254 netmask 255.255.255.0
nat (inside) 1 10.0.P.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.P.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact

```

```

snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
  !
service-policy global_policy global
Cryptochecksum:186cbc95531d29b184276f9e35b1579d
: end
[OK]
[OK]

```

(where P = pod number)

- i. Test the operation of the global and NAT statements configured by originating connections through the PIX Security Appliance by completing the following substeps:
- j. Open a web browser on the student PC.
- k. From the Student PC, use a web browser to access the Backbone server at IP address 172.26.26.50 by entering **http://172.26.26.50**.

- I. Observe the translation table:

```
PixP(config)# show xlate
```

The display should appear similar in the following:

```
1 in use, 1 most used
```

```
Global 192.168.P.20 Local insidehost
```

(where P = pod number)

A global address chosen from the low end of the global range has been mapped to the student PC.

Step 5 Test the Inside, Outside, and DMZ Interface Connectivity

To test and troubleshoot interface connectivity using the PIX Security Appliance **ping** command, complete the following steps:

- a. Ping the inside interface:

```
PixP(config)# ping 10.0.P.1
```

```
Sending 5, 100-byte ICMP Echos to 10.0.P.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- b. Ping the inside host:

```
PixP(config)# ping insidehost
```

```
Sending 5, 100-byte ICMP Echos to insidehost, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- c. Ping the outside interface:

```
PixP(config)# ping 192.168.P.2
```

```
Sending 5, 100-byte ICMP Echos to 192.168.P.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

- d. Ping the backbone router:

```
PixP(config)# ping 192.168.P.1
```

```
Sending 5, 100-byte ICMP Echos to 192.168.P.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

- e. Ping the DMZ interface:

```
PixP(config)# ping 172.16.P.1
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

f. Ping the bastion host:

```
PixP(config)# ping bastionhost
```

```
Sending 5, 100-byte ICMP Echos to bastionhost, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10  
ms
```