



Lab 8.3.3 Configure a PIX Security Appliance as a Transparent Firewall

Objective

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

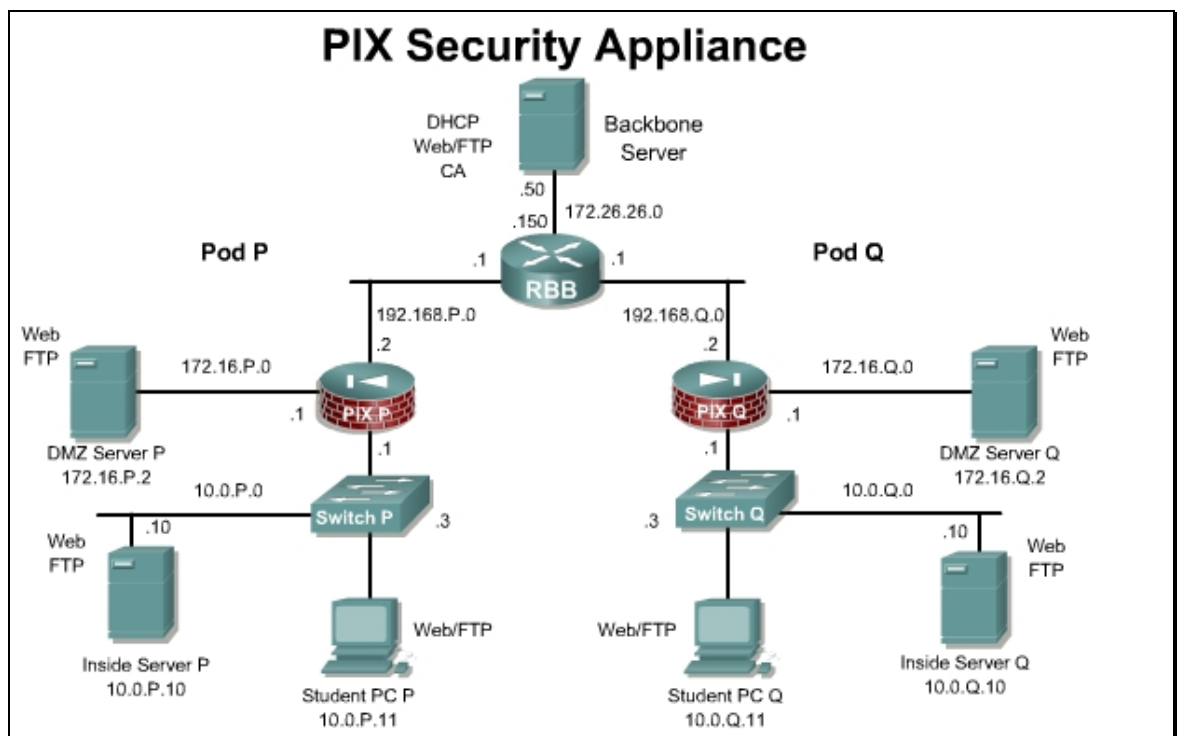
- Enable transparent firewall mode.
- Configure the PIX Security Appliance interfaces and a management IP address.
- Test the inside and outside connectivity.
- Allow ICMP traffic through the transparent firewall
- Disable transparent firewall mode.

Scenario

The XYZ Company has decided to change the operational mode of an existing PIX Firewall from router to transparent. The PIX must be reconfigured to operate in transparent mode. The PIX will also need to be configured to allow layer 3 traffic, such as ICMP, to pass through the transparent firewall as allowed by the company security policy.

Topology

This figure illustrates the lab network environment:



Preparation

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

When the PIX Security Appliance is in transparent firewall mode, both of the interfaces are on the same IP network. The student PC must be reassigned to the same IP network as the outside host for this lab activity. Use the IP address 172.16.P.11/24 and a default gateway of 172.16.P.1 for the student PC. (Where P = pod number)

Tools and Resources

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

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

Additional Materials

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

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450b68.html

Step 1 Enable Transparent Firewall Mode

To enable the PIX Security Appliance to operate in transparent firewall mode, complete the following steps:

- a. Save the configuration to flash:

```
PixP# copy running-config flash:saved.cfg
Source filename [running-config]? <Enter>
Destination filename [saved.cfg]? <Enter>
Cryptochecksum: bdeb536f 156358e5 a7d99020 7f1ed561
2420 bytes copied in 0.940 secs
```

- b. Change to configuration mode:

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

- c. Set the firewall mode to transparent:

```
PixP(config)# firewall transparent
Switched to transparent mode
Pixfirewall(config)#
```

- d. Confirm that the PIX Security Appliance is now operating in transparent firewall mode.

```
Pixfirewall(config)# show firewall
Examine the running configuration:
Pixfirewall(config)# write terminal
: Saved
:
PIX Version 7.0(1)
```

```

firewall transparent
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
pager lines 24
no ip address
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 rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
  !
service-policy global_policy global
Cryptochecksum:bdeb536f156358e5a7d990207f1ed561
: end

```

Step 2 Configure the PIX Security Appliance Interfaces and Management Address

Complete the following steps to configure PIX Security Appliance Ethernet interfaces and management address:

- a. Configure the Ethernet 1 interface.

Note By default the interfaces are disabled. Any interface that will be used must be enabled.

```

pixfirewall(config)# interface ethernet1
pixfirewall(config-if)# nameif inside
pixfirewall(config-if)# no shutdown

```

- b. Configure the Ethernet 2 interface.

```

pixfirewall(config-if)# interface ethernet2
pixfirewall(config-if)# nameif outside
pixfirewall(config-if)# no shutdown

```

- c. Exit interface configuration mode.

```

pixfirewall(config-if)# exit

```

- d. Configure the management IP address.

```
pixfirewall(config)# ip address 172.16.P.30 255.255.255.0
(where P = pod number)
```

- e. Verify the management IP address configuration.

```
pixfirewall(config)# show ip address
Management System IP Address:
    ip address 172.16.P.30 255.255.255.0
Management Current IP Address:
    ip address 172.16.P.30 255.255.255.0
(where P = pod number)
```

- f. Write the configuration to memory.

```
pixfirewall(config)# write memory
```

Step 3 Test Inside and Outside Connectivity

Complete the following steps to test and troubleshoot interface connectivity using the PIX Security Appliance **ping** command:

- a. Ping the inside host:

```
pixfirewall(config)# ping 172.16.P.11
Sending 5, 100-byte ICMP Echos to 172.16.P.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
(where P = pod number)
```

- b. Ping the outside host:

```
pixfirewall(config)# ping 172.16.P.2
Sending 5, 100-byte ICMP Echos to 172.16.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)
```

- c. Examine the MAC address table:

```
pixfirewall(config)# show mac-address-table
```

interface	mac address	type	Age(min)
outside	0002.fdlc.3c43	dynamic	4
inside	00d0.b7b9.62af	dynamic	4

- d. Test the inside host connectivity, by pinging the outside host from the student PC:

```
C:\>ping 172.16.P.2
Pinging 172.16.P.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Request timed out.

Step 4 Allow ICMP Through the Transparent Firewall

Complete the following steps to allow ICMP traffic through the PIX Security Appliance transparent firewall:

- a. Create an ACL that allows ICMP traffic from the inside to the outside network:

```
pixfirewall(config)# access-list ACLIN permit icmp 172.16.P.0  
255.255.255.0 172.16.P.0 255.255.255.0
```

(where P = pod number)

- b. Apply the ACL to the inside and outside interfaces:

```
pixfirewall(config)# access-group ACLIN in interface inside  
pixfirewall(config)# access-group ACLIN in interface outside
```

- c. Test the inside host connectivity, by pinging the outside host from the student PC:

```
C:\>ping 172.16.P.2  
  
Pinging 172.16.P.2 with 32 bytes of data:  
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126  
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126  
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126  
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126
```

- d. Verify the access list and note the hit counts:

```
pixfirewall(config)# show access-list  
  
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max  
4096)  
  
alert-interval 300  
  
access-list ACLIN: 1 elements  
  
access-list ACLIN line 1 extended permit icmp 172.16.P.0  
255.255.255.0 172.16.P.0 255.255.255.0 (hitcnt=2)
```

- e. If desired, compare the running configuration with the ending configuration provided for this lab.

Step 5 Disable Transparent Firewall Mode

Complete the following steps to disable Transparent Firewall mode:

- a. Set the firewall mode to router:

```
pixfirewall(config)# no firewall transparent  
  
Switched to router mode
```

- b. Restore the original configuration and reboot:

```
pixfirewall# copy flash:saved.cfg startup-config  
Source filename [saved.cfg]? <Enter>  
Copy in progress...C  
2420 bytes copied in 0.70 secs  
pixfirewall(config)# reload
```