



## Lab 9.4.10 Configure and Test Advanced Protocol Handling on the Cisco PIX Security Appliance

### Objective

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

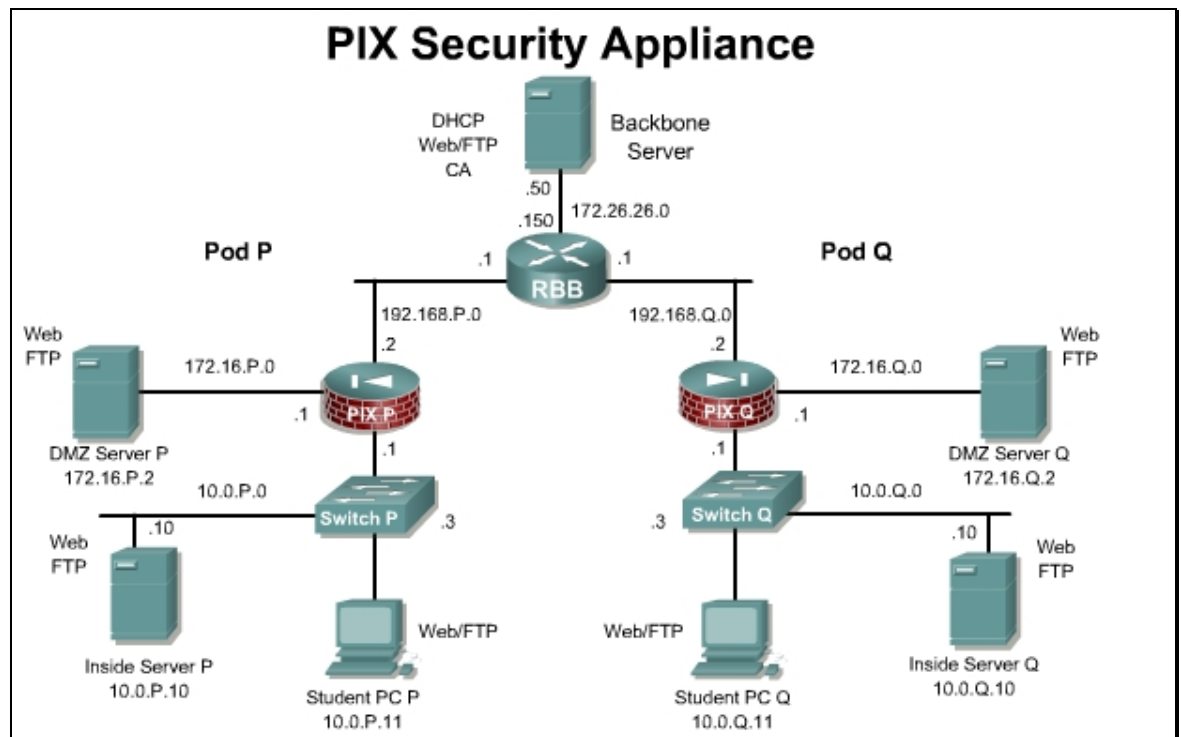
- Display the Inspection protocol configurations
- Change the Inspection protocol configurations
- Test the outbound FTP Inspection protocol
- Perform FTP deep packet inspection

### Scenario

Some applications embed addressing information into the application data stream and negotiate randomly picked Transport Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers or IP addresses. In these cases application aware inspection must be performed.

### 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.

## Tools and resources

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

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

## 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 configure fixup</code>	To clear the fixup configuration, use the <code>clear configure fixup</code> command in global configuration mode.
<code>ftp-map map_name</code>	To identify a specific map for defining the parameters for strict FTP inspection, use the <code>ftp-map</code> command in global configuration mode.
<code>policy-map name</code>	To configure a policy, use the <code>policy-map</code> command in global configuration mode.
<code>show running-config policy-map</code>	To display all the policy-map configurations or the default policy-map configuration, use the <code>show running-config policy-map</code> command in privileged EXEC mode.
<code>show running-config service-policy</code>	To display all currently running service policy configurations, use the <code>show running-config service-policy</code> command in global configuration mode.

## Step 1 List the Fixup Protocols

Complete the following steps and enter the commands as directed to view the current configurations of the PIX Security Appliance:

- a. Show the default modular policy class-map running on the PIX security appliance:

```
pixP# show run class-map
class-map inspection_default
match default-inspection-traffic
```

1. What is the default class-map name?

---

- b. Show the default modular policy-map running on the PIX security appliance:

```
pixP# show running-config policy-map
!
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
```

1. What is the default policy-map name?

---

2. What is the class for this policy?

---

3. By default, which protocols are inspected by the PIX Security Appliance? Check each protocol that applies:

<b>dns</b>	
<b>ftp</b>	
<b>h323 ras</b>	
<b>rsh</b>	
<b>sip</b>	
<b>skinny</b>	
<b>sunrpc</b>	
<b>xdmcp</b>	
<b>netbios</b>	

<b>mgcp</b>	
<b>tftp</b>	
<b>snmp</b>	
<b>rtsp</b>	
<b>icmp</b>	
<b>h323 h225</b>	
<b>esmtpt</b>	
<b>sqlnet</b>	
<b>http</b>	

- c. List the default modular policy service-policy running on the PIX Security Appliance:

```
PixP# show running-config service-policy
service-policy global_policy global
```

1. What is the default service-policy name?
- 

2. Where is the default service-policy applied?
- 

## Step 2 Change the Protocol Inspection Configuration

Complete the following steps and enter the commands as directed to change some of the current configurations of the PIX security appliance:

- a. Disable the following Inspection protocols in the default policy-map:

```
PixP# configure terminal
PixP(config)# policy-map global_policy
PixP(config-pmap)# class inspection_default
PixP(config-pmap-c)# no inspect sunrpc
PixP(config-pmap-c)# no inspect h323 ras
PixP(config-pmap-c)# no inspect sqlnet
PixP(config-pmap-c)# exit
PixP(config-pmap)# exit
PixP(config)#
```

(where P = pod number)

- b. Show the changes to the default modular policy-map running on the PIX Security Appliance:

```
PixP# show running-config policy-map
```

1. After the policy-map change, which protocols are inspected by the PIX Security Appliance?

<b>dns</b>	
<b>ftp</b>	
<b>h323 ras</b>	
<b>rsh</b>	
<b>sip</b>	
<b>skinny</b>	
<b>sunrpc</b>	
<b>xmcp</b>	
<b>netbios</b>	

<b>mgcp</b>	
<b>tftp</b>	
<b>snmp</b>	
<b>rtsp</b>	
<b>icmp</b>	
<b>h323 h225</b>	
<b>esmtpt</b>	
<b>sqlnet</b>	
<b>http</b>	

### Step 3 Test Outbound FTP Protocol Inspection

Complete the following steps and enter the commands as directed to test the outbound FTP Protocol Inspection:

- a. FTP to the backbone server from the student PC using the Windows FTP client:

```
C:\> ftp 172.26.26.50  
User (172.26.26.50:(none)): ftpuser  
331 Password required for ftpuser.  
Password: ftppass
```

1. Was it possible to log into the server? Why or why not?
- 

- b. Do a directory listing at the FTP prompt:

```
ftp> dir
```

1. Was it possible to see a file listing? Why or why not?
- 

- c. Quit the FTP session:

```
ftp> quit
```

- d. Turn off the FTP Inspection protocol on the PIX Security Appliance:

```
PixP(config)# policy-map global_policy  
PixP(config-pmap)# class inspection_default  
PixP(config-pmap-c)# no inspect ftp  
PixP(config-pmap-c)# exit  
PixP(config-pmap)# exit  
PixP(config)#
```

(where P = pod number)

- e. Again, ftp to the backbone server from the student PC using the Windows FTP client:

```
C:\> ftp 172.26.26.50  
User (172.26.26.50:(none)): ftpuser  
331 Password required for ftpuser.  
Password: ftppass
```

1. Was it possible to log into the server? Why or why not?
- 

2. Do a directory listing at the FTP prompt:

```
ftp> dir
```

3. Was it possible to see a file listing? Why or why not?
- 

- f. Quit the FTP session:

```
ftp> quit
```

---

**Note** If the FTP client is hung, press Ctrl+C until the C:\ prompt returns, or close the command prompt window.

---

- g. Open a browser. Set the browser for passive FTP. In Internet Explorer, this can be done through navigation to **Tools > Internet Options > Advanced** and select **Use Passive FTP**. It should be possible to make an FTP connection to the backbone server from the student PC.

- h. Enter the following in the URL field:

**ftp://172.26.26.50**

1. Was the connection successful? Why or why not?  

---
2. Was it possible to see a file listing? Why or why not?  

---

- i. Disable passive FTP on the browser. Close the web browser.

#### Step 4 Perform FTP Deep Packet Inspection

Complete the following steps to perform FTP deep packet inspection:

- a. Set all protocol inspection to the factory defaults:

```
PixP(config)# clear configure fixup
```

(where P = pod number)

- b. Define an FTP-map to disallow the FTP **get** command:

```
PixP(config)# ftp-map no_get
```

```
PixP(config-ftp-map)# deny-request-cmd retr
```

```
PixP(config-ftp-map)# exit
```

```
PixP(config)#
```

- c. FTP to the backbone server from the student PC using a web browser. It should be possible to open a file because the restrictions that were configured in the previous step have not been applied. To test default FTP inspection, enter the following in the URL field:

**ftp://172.26.26.50**

1. Was the connection successful? Why or why not?  

---
2. Was it possible to see a file listing? Why or why not?  

---
3. Was it possible to open one of the listed files? Why or why not?  

---

- d. Close the browser

- e. Apply the FTP-map restriction to the default policy-map:

```
PixP(config)# policy-map global_policy
```

```
PixP(config-pmap)# class inspection_default
```

```
PixP(config-pmap-c)# inspect ftp strict no_get
```

```
PixP(config-pmap-c)# exit
```

```
PixP(config-pmap)# exit
```

```
PixP(config)#
```

- f. FTP to the backbone server from the student PC using a web browser. It should not be possible to open, or retrieve, a file. To do this, enter the following in the URL field:

**ftp://172.26.26.50**

1. Was the connection successful? Why or why not?
- 

2. Was it possible to see a file listing? Why or why not?
- 

3. Was it possible to open one of the listed files? Why or why not?
- 

- g. Close the browser.

- h. Verify the change to the default policy-map settings:

```
PixP(config)# show run policy-map
```

```
policy-map global_policy
```

```
class inspection_default
```

```
inspect dns
```

```
inspect netbios
```

```
inspect rtsp
```

```
inspect tftp
```

```
inspect xdmcp
```

```
inspect sunrpc
```

```
inspect ftp strict no_get
```

```
inspect h323 h225
```

```
inspect h323 ras
```

```
inspect rsh
```

```
inspect sqlnet
```

```
inspect sip
```

```
inspect skinny
```

(where P = pod number)

- i. View the Service-Policy statistics. Examine the inspect ftp packet, drop, and reset-drop count.

```
pixl(config)# show service-policy
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: inspection_default
```

```
Inspect: dns, packet 0, drop 0, reset-drop 0
```

```
Inspect: netbios, packet 0, drop 0, reset-drop 0
```

```
Inspect: rtsp, packet 0, drop 0, reset-drop 0
```

```
Inspect: tftp, packet 0, drop 0, reset-drop 0
```

```
Inspect: xdmcp, packet 0, drop 0, reset-drop 0
```

```
Inspect: ftp strict no_get, packet 236, drop 0, reset-drop 8
Inspect: h323 ras, packet 0, drop 0, reset-drop 0
Inspect: rsh, packet 0, drop 0, reset-drop 0
Inspect: esmtp, packet 0, drop 0, reset-drop 0
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
Inspect: sip, packet 0, drop 0, reset-drop 0
Inspect: skinny, packet 0, drop 0, reset-drop 0
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
```

- j. Set all protocol inspection to the factory defaults:

```
pixP(config)# clear configure fixup
```

(where P = pod number)

- k. Verify the protocol inspection settings:

```
pixP(config)# show run policy-map
```

```
policy-map global_policy
```

```
class inspection_default
```

```
inspect dns
```

```
inspect netbios
```

```
inspect rtsp
```

```
inspect tftp
```

```
inspect xdmcp
```

```
inspect sunrpc
```

```
inspect ftp
```

```
inspect h323 h225
```

```
inspect h323 ras
```

```
inspect rsh
```

```
inspect sqlnet
```

```
inspect sip
```

```
inspect skinny
```

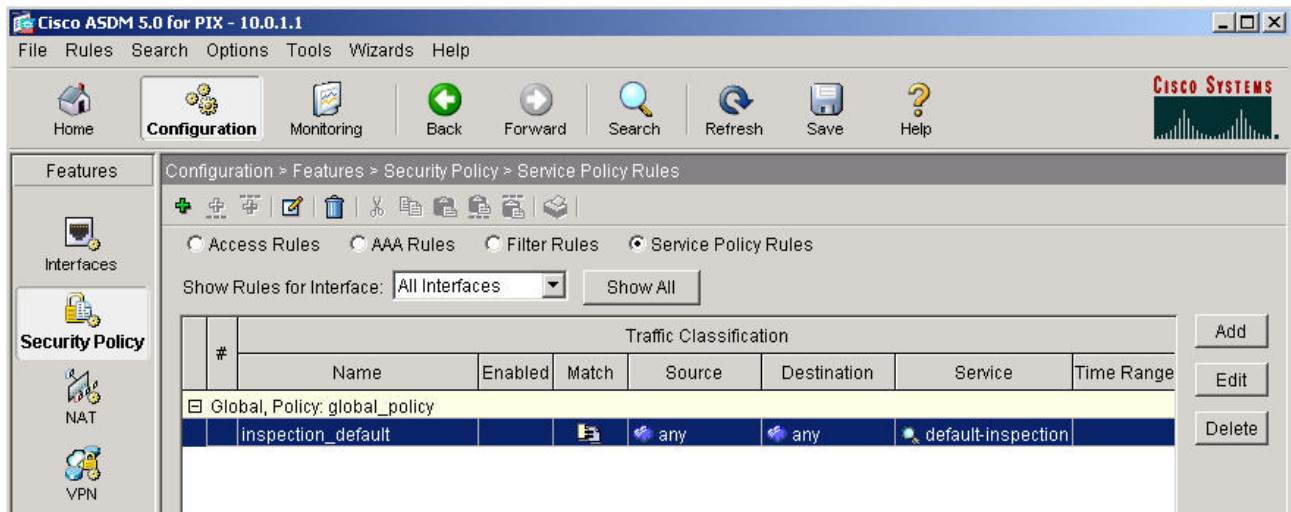
(where P = pod number)

## Step 5 View the Fixup Protocols using ASDM

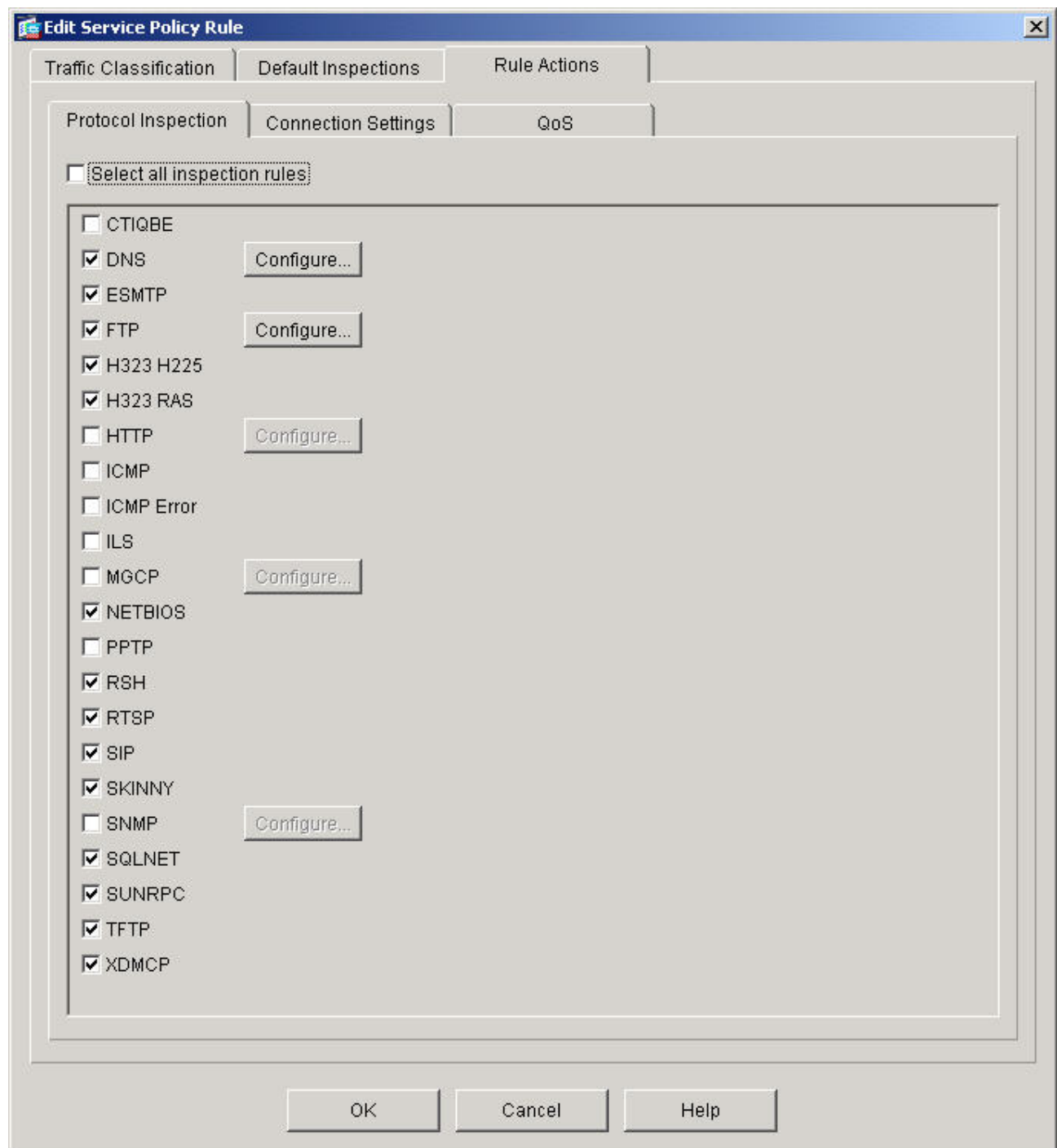
Complete the following steps:

- Log into ASDM
- Navigate to **Configuration>Features>Security Policy>Service Policy Rules**.





- c. Double click on the **inspection\_default** rule. The **Edit Service Policy** window appears.
- d. Click the **Rule Actions** tab, then click the **Protocol Inspection** tab. This tab allows the administrator to enable or disable the different types of application inspection that are available.



- e. After reviewing the protocol inspection information, exit ADSM.