



Lab 2.3.3 Configure Intrusion Prevention on the PIX Security Appliance

Objective

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

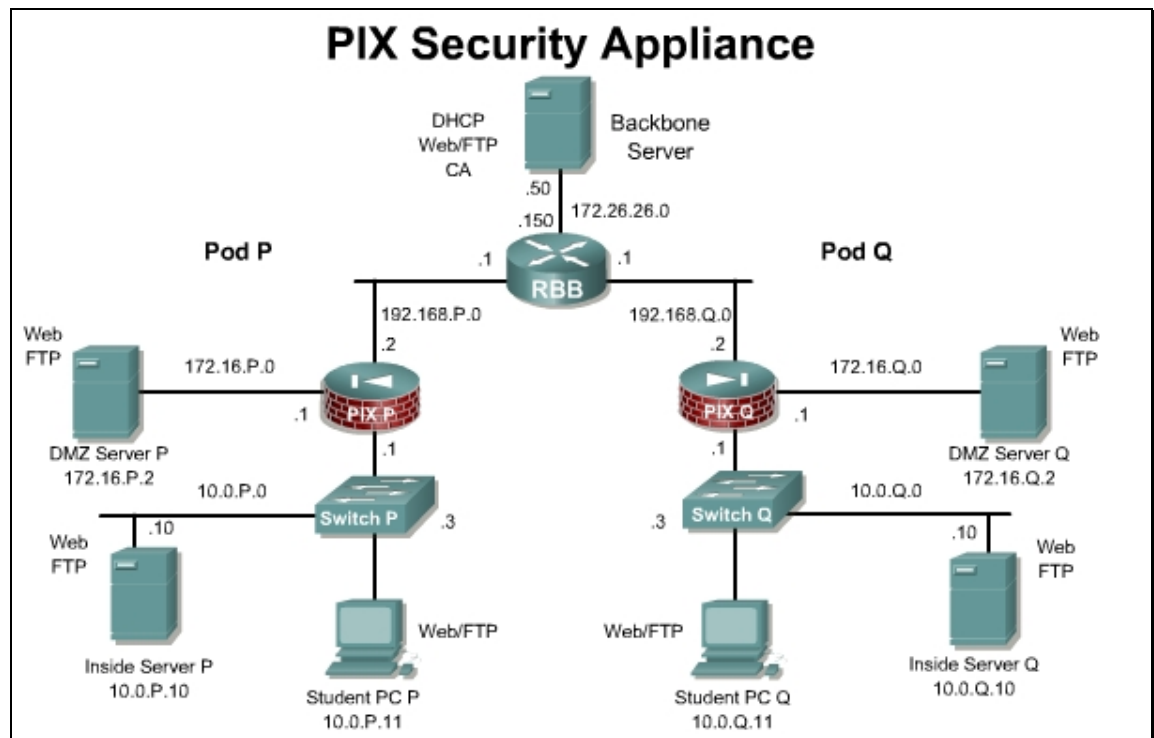
- Configure the use of Cisco Intrusion Prevention System (IPS) information signatures and send Cisco IPS Syslog output to a Syslog server.
- Configure the use of IPS attack signatures and send Cisco IPS Syslog output to a Syslog server.

Scenario

A small company is wants to increase security by adding intrusion prevention on the current PIX Security Appliance. Any output produced by the IPS will be logged to a Syslog server and monitored.

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 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.

Download NMapWin from <http://sourceforge.net/projects/nmapwin> and install on the Student PC.

Tools and Resources

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

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

Additional materials:

Refer to *Cisco PIX Security Appliance System Log Messages* for a list of the supported IPS signature messages. The documentation can be viewed online at the following website:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.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
ip audit interface <i>interface_name policy_name</i>	To assign an audit policy to an interface, use the ip audit interface command in global configuration mode.
ip audit name <i>name</i> { info attack } [action [alarm] [drop] [reset]]	To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use the ip audit name command in global configuration mode.
show ip audit count [global interface <i>interface_name</i>]	To show the number of signature matches when you apply an audit policy to an interface, use the show ip audit count command in privileged EXEC mode.
show running-config ip audit attack	To show the ip audit attack configuration in the running configuration, use the show running-config ip audit attack command in privileged EXEC mode.
show running-config ip audit interface	To show the ip audit interface configuration in the running configuration, use the show running-config ip audit interface command in privileged EXEC mode.
show running-config ip audit name [<i>name</i> [info attack]]	To show the ip audit name configuration in the running configuration, use the show running-config ip audit name command in privileged EXEC mode.

Step 1 Configure the Use of IPS Information Signatures and Send Cisco IPS Syslog Output to a Syslog Server

Reboot the PIX and load the starting configuration.

Complete the following steps to configure the use of Cisco IPS information signatures and to send Cisco IPS Syslog output to a Syslog server:

- a. Turn on logging and send messages to the syslog server:

```
PixP(config)# logging enable
PixP(config)# logging host inside insidehost
PixP(config)# logging trap debugging
```

- b. Verify connectivity by pinging RBB from the Windows command prompt:

```
C:\>ping 192.168.P.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

- c. Specify the information signature policy on the PIX Security Appliance:

```
PixP(config)# ip audit name INFOPOLICY info action alarm reset
```

- d. Apply the information signature policy to the inside interface:

```
PixP(config)# ip audit interface inside INFOPOLICY
```

- e. Disable the chargen signature, which is number 4052

```
PixP(config)# ip audit signature 4052 disable
```

- f. Verify the information signature policy on the PIX Security Appliance:

```
PixP(config)# show running-config ip audit interface
ip audit interface inside INFOPOLICY
PixP(config)# show running-config ip audit name
ip audit name INFOPOLICY info action alarm reset
PixP(config)# show running-config ip audit signature
ip audit signature 4052 disable
```

- g. Open and the Kiwi Syslog Daemon on the desktop. Clear any existing log entries.

- h. Return to the Windows command line and attempt to ping RBB. The ping should fail.

```
C:\>ping 192.168.P.1
```

- i. Observe the messages that appear on the Kiwi Syslog Daemon display. The log should be similar to the following:

Kiwi Syslog Daemon (Version 7.1.4)				
File View Help				
Display 00 (Default)				
Date	Time	Priority	Hostname	Message
06-01-2005	11:17:42	Local4.Warning	10.0.1.1	%PIX-4-400014: IDS:2004 ICMP echo request from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:17:40	Local4.Warning	10.0.1.1	%PIX-4-400014: IDS:2004 ICMP echo request from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:17:39	Local4.Warning	10.0.1.1	%PIX-4-400014: IDS:2004 ICMP echo request from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:17:37	Local4.Warning	10.0.1.1	%PIX-4-400014: IDS:2004 ICMP echo request from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:17:36	Local4.Warning	10.0.1.1	%PIX-4-400014: IDS:2004 ICMP echo request from insidehost to 192.168.1.1 on interface inside

- j. View the IP audit counts

```
PixP# show ip audit count
```

- Which info signatures were incremented?

- k. Remove the information signature policy from the inside interface:

```
PixP(config)# no ip audit interface inside INFOPOLICY
```

- l. Remove the audit policy audit_name:

```
PixP(config)# no ip audit name INFOPOLICY
```

- m. Verify that the information signature policy has been removed from the inside interface, the default informational actions have been restored, and the ip audit name has been removed:

```
PixP(config)# show running-config ip audit interface
```

```
PixP(config)# show running-config ip audit name
```

Step 2 Configure the Use of IDS Attack Signatures and Send IDS Syslog Output to a Syslog Server

Complete the following steps to configure the use of IDS attack signatures and send IDS Syslog output to a Syslog server:

- a. Ping the bastion host with an Internet Control Message Protocol (ICMP) packet size of 10000 from the command line of the student PC:

```
C:\>ping /l 10000 192.168.P.1
```

```
Pinging 192.168.P.1 with 10000 bytes of data:
```

```
Reply from 192.168.P.1: bytes=10000 time=23ms TTL=255
```

```
Reply from 192.168.P.1: bytes=10000 time=17ms TTL=255
```

```
Reply from 192.168.P.1: bytes=10000 time=18ms TTL=255
```

```
Reply from 192.168.P.1: bytes=10000 time=18ms TTL=255
```

- c. Specify an attack policy:

```
PixP(config)# ip audit name ATTACKPOLICY attack action alarm reset
```

- d. Apply the attack policy to the inside interface:

```
PixP(config)# ip audit interface inside ATTACKPOLICY
```

- e. Ping the bastion host with an ICMP packet size of 10000 from the Windows 2000 command line:

```
C:\>ping /l 10000 192.168.P.1
```

```
Pinging 192.168.P.1 with 10000 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
Request timed out.
Request timed out.
```

- f. Observe the messages that appear on the Kiwi Syslog Daemon display. The log should be similar to the following:

The screenshot shows the Kiwi Syslog Daemon window with a table of log entries. The table has columns for Date, Time, Priority, Hostname, and Message. The messages are all warnings from 10.0.1.1 regarding ICMP activity on interface inside.

Date	Time	Priority	Hostname	Message
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400025: IDS:2154 ICMP ping of death from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400023: IDS:2150 ICMP fragment from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400023: IDS:2150 ICMP fragment from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400023: IDS:2150 ICMP fragment from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400023: IDS:2150 ICMP fragment from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400023: IDS:2150 ICMP fragment from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:31:16	Local4.Warning	10.0.1.1	%PIX-4-400023: IDS:2150 ICMP fragment from insidehost to 192.168.1.1 on interface inside

At the bottom of the window, statistics are shown: 100%, 2743 MPH, 11:31, 06-01-2005.

- Why is the syslog server showing the ICMP fragment in the log?

- n. View the IP audit counts

```
PixP# show ip audit count
```

- Which info signatures were incremented?

- g. Ping the bastion host with an increased ICMP packet size from the command line of the student PC:

```
C:\>ping /l 65000 172.16.P.2
```

```
Pinging 172.16.P.2 with 65000 bytes of data:
```

```
Request timed out.
```

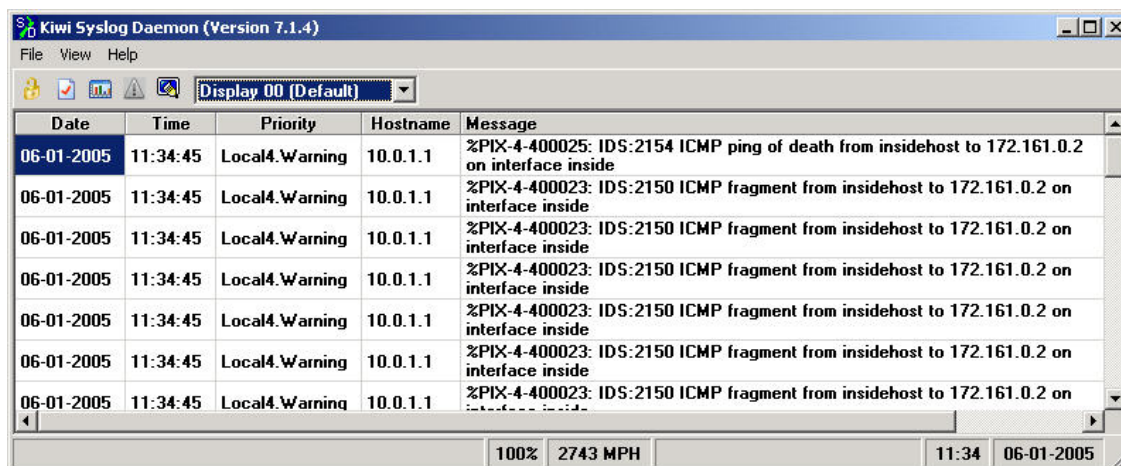
```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

(where P = pod number)

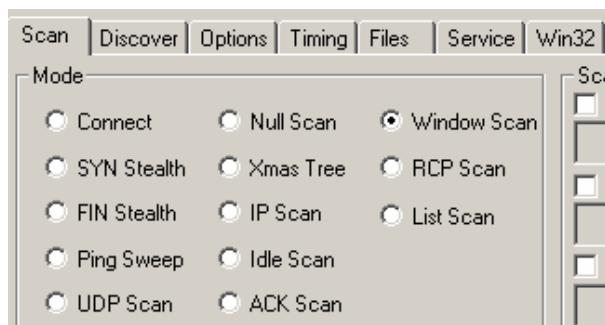
- g. Observe the messages that appear on the Kiwi Syslog Daemon display. The log should be similar to the following:



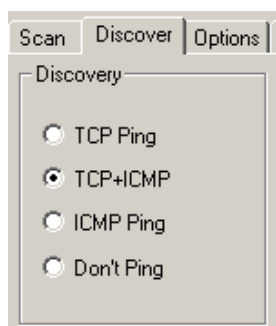
Step 3 Launch an NMapWin scan

Complete the following steps to launch a NMAP scan against RBB:

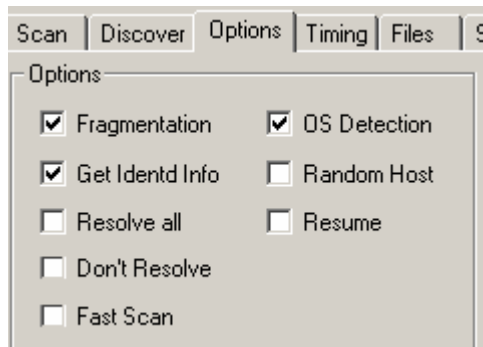
- Open NMapWin.
- In the Scan tab, choose Window Scan.



- In the Discover tab choose TCP+ICMP.



- In the Options tab, choose the following:



- e. In the Host field, enter 192.168.P.1 and click the Scan button.

Host:

192.168.1.1

- f. Return to the Kiwi Syslog Daemon display.

Kiwi Syslog Daemon (Version 7.1.4)

File View Help

Display 00 (Default)

Date	Time	Priority	Hostname	Message
06-01-2005	11:42:46	Local4.Warning	10.0.1.1	%PIX-4-400009: IDS:1103 IP teardrop attack from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:42:46	Local4.Critical	10.0.1.1	%PIX-2-106020: Deny IP teardrop fragment (size = 16, offset = 0) from insidehost to 192.168.1.1
06-01-2005	11:42:33	Local4.Warning	10.0.1.1	%PIX-4-400009: IDS:1103 IP teardrop attack from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:42:33	Local4.Critical	10.0.1.1	%PIX-2-106020: Deny IP teardrop fragment (size = 16, offset = 0) from insidehost to 192.168.1.1

- g. Stop the previous scan and perform a Null Scan. View the Kiwi output

Kiwi Syslog Daemon (Version 7.1.4)

File View Help

Display 00 (Default)

Date	Time	Priority	Hostname	Message
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside
06-01-2005	11:46:08	Local4.Warning	10.0.1.1	%PIX-4-400026: IDS:3040 TCP NULL flags from insidehost to 192.168.1.1 on interface inside

100% 1991 MPH 11:46 06-01-2005

- h. Stop the Nmap Scan.
- i. Compare the current configuration to the ending configuration for this lab if desired.
- j. Remove the attack policy.
- k. Verify that the attack policy has been removed from the inside interface, the default attack actions have been restored, and the ip audit name has been removed:

```
PixP(config)# no ip audit name ATTACKPOLICY
```

```
PixP(config)# show running-config ip audit interface
```

```
PixP(config)# show running-config ip audit attack
```

```
PixP(config)# show running-config ip audit name
```