



## Lab 7.4.6 Configure SNMP Monitoring of the PIX Security Appliance Using ASDM

### Objective

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

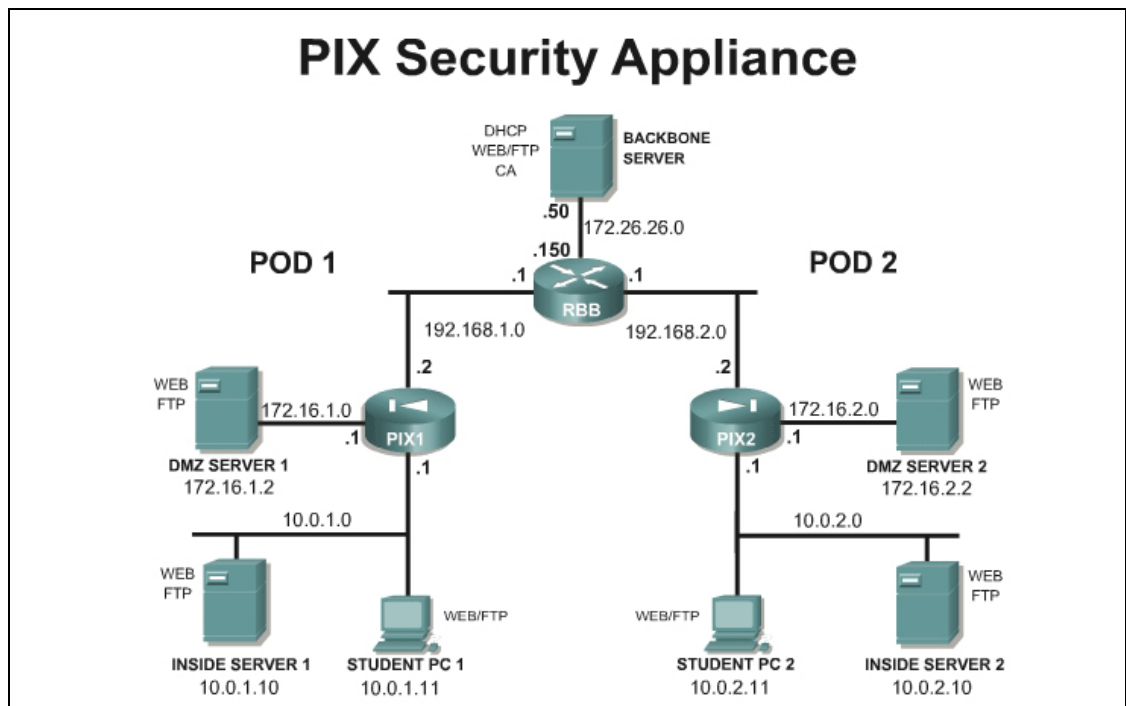
- Enable SNMP community string
- Establishing the Contact and location of the SNMP Agent
- Limit SNMP to inside server
- Testing the configuration

### Scenario

A small company wants to monitor the PIX Security Appliance using SNMP.

### 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 SNMPwalk for Windows from [http://www.bradford-sw.com/board/board.cgi?id=BSI\\_Tools&action=view&gul=13&page=1&go\\_cnt=0](http://www.bradford-sw.com/board/board.cgi?id=BSI_Tools&action=view&gul=13&page=1&go_cnt=0)

## Tools and Resources

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

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

## Additional Materials

For more information on PIX SNMP go to:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/products\\_configuration\\_guide\\_chapter09186a0080450bf7.html#wp1042028](http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450bf7.html#wp1042028)

## Step 1 Verify SNMP Operation

Complete the following steps to verify that SNMPWalk is operational

- a. Download and install SNMPWalk in a folder with the name **SNMP** on C:\
- b. On the Student PC, open a command prompt.
- c. Get to a root C:\> by entering `cd \`
- d. Go to the snmp directory and verify the files

```
C:\> cd snmp
```

```
C:\SNMP>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is A49B-A399
```

```
Directory of C:\SNMP
```

```
06/25/2004  03:05 PM    <DIR>          .
06/25/2004  03:05 PM    <DIR>          ..
04/03/1999  08:57 AM                99,840  libsnmp.dll
04/03/1999  08:58 AM                11,776  snmpget.exe
04/03/1999  08:59 AM                11,776  snmpwalk.exe
               3 File(s)                123,392 bytes
               2 Dir(s)  17,925,615,616 bytes free
```

```
C:\SNMP>
```

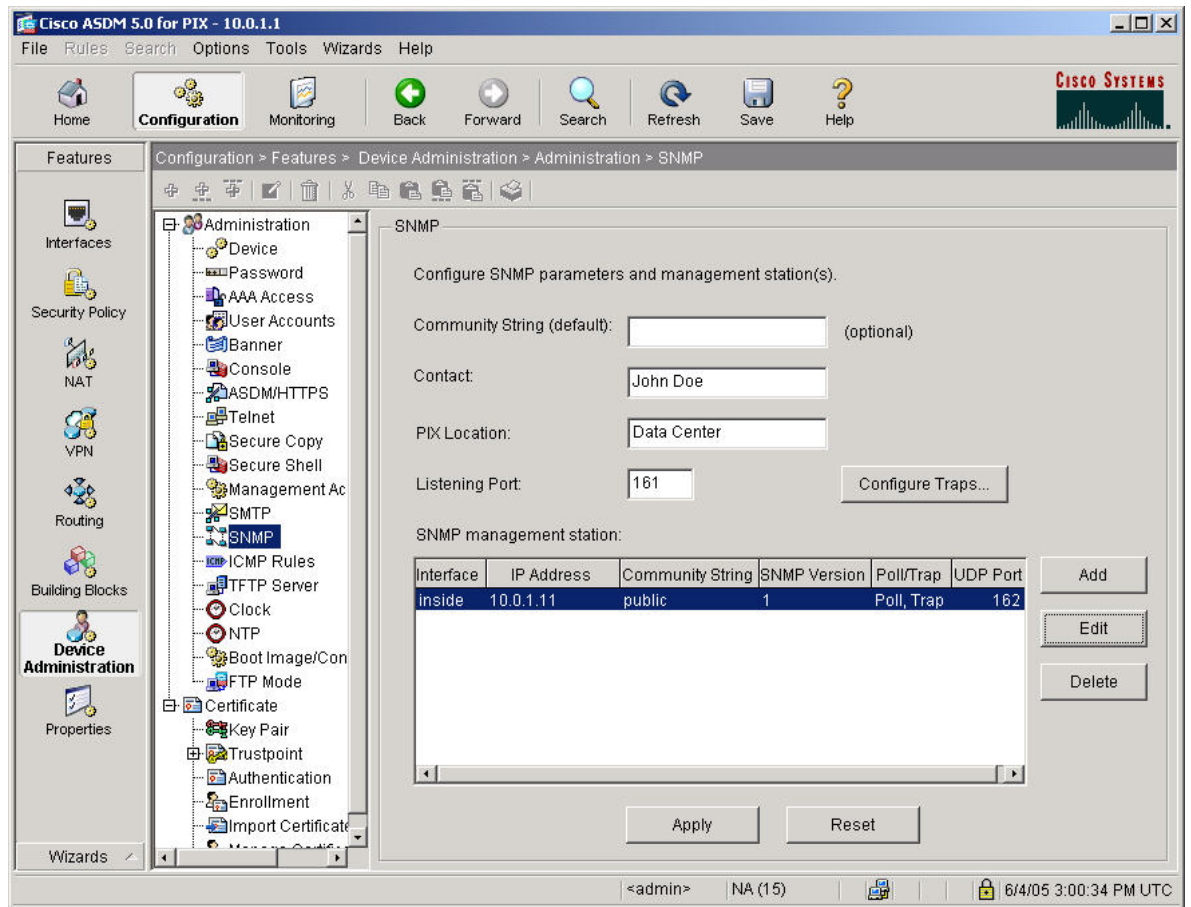
- e. Perform SNMP reconnaissance using SNMPWalk. Some output has been omitted.

```
C:\SNMP> snmpwalk -v 1 10.0.1.1 public  
Timeout: No Response from 10.0.1.1  
C:\SNMP>
```

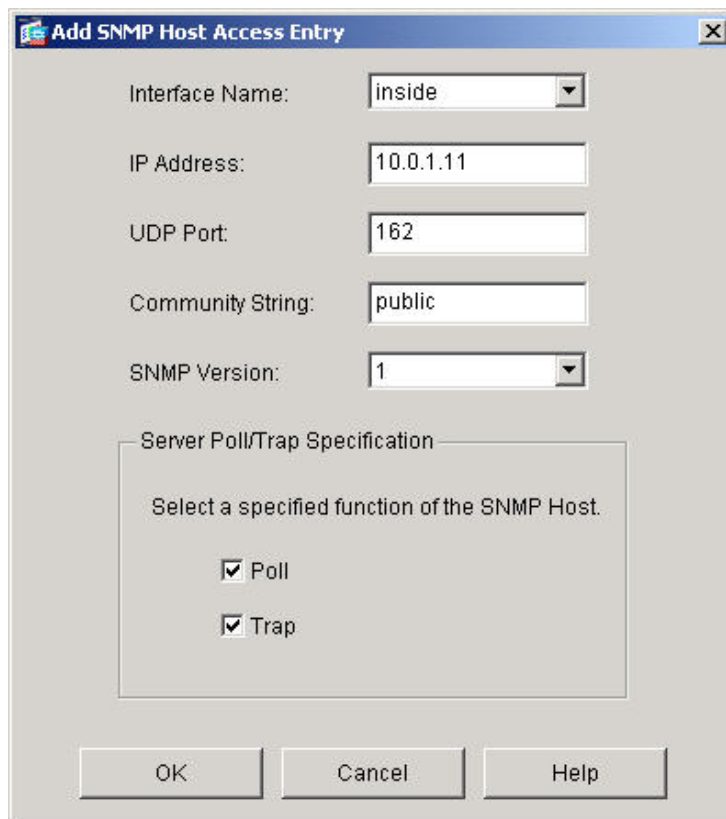
## Step 2 Configure the PIX Security Appliance to Send SNMP Messages

Complete the following steps to configure the PIX Security Appliance to send SNMP messages to a SNMP server:

- Initiate an ASDM session with the PIX Security Appliance.
- Navigate to **Configuration>Features>Device Administration>Administration>SNMP**.



- Configure a System administrator name and location.
- Click the **Add** button to configure the Student PC address as the SNMP management station. Select **inside** for the interface and verify that both **Poll** and **Trap** functions are checked.



**Add SNMP Host Access Entry**

Interface Name:

IP Address:

UDP Port:

Community String:

SNMP Version:

Server Poll/Trap Specification

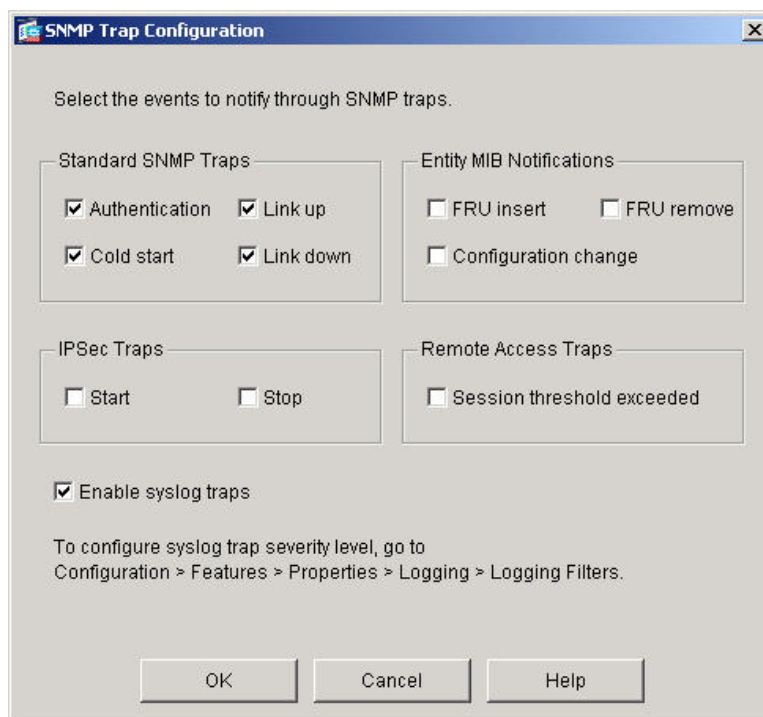
Select a specified function of the SNMP Host.

☒ Poll

☒ Trap

OK Cancel Help

- e. Click the **OK** button to return to the SNMP window.
- f. Click the **Configure Traps** button to configure the SNMP trap properties. Check the **Enable syslog traps** button. Click the **OK** button. A warning appears with a notification regarding the logging trap level.



**SNMP Trap Configuration**

Select the events to notify through SNMP traps.

Standard SNMP Traps

☒ Authentication ☒ Link up

☒ Cold start ☒ Link down

Entity MIB Notifications

☐ FRU insert ☐ FRU remove

☐ Configuration change

IPSec Traps

☐ Start ☐ Stop

Remote Access Traps

☐ Session threshold exceeded

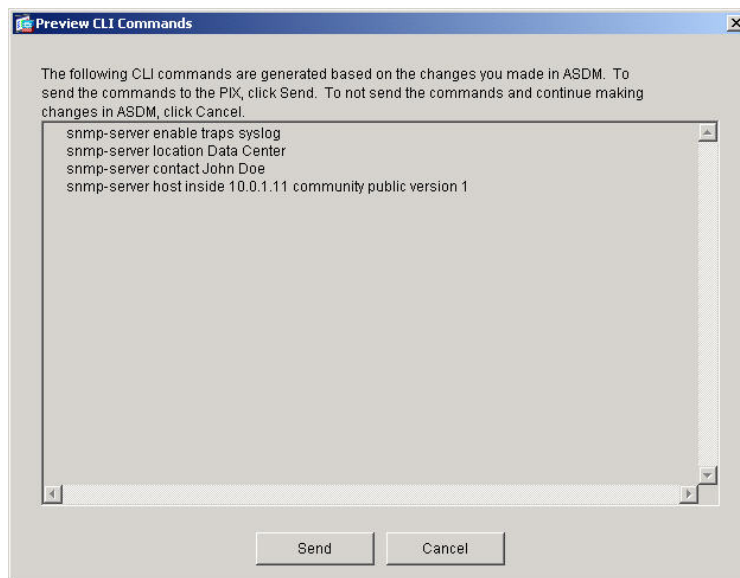
☒ Enable syslog traps

To configure syslog trap severity level, go to  
Configuration > Features > Properties > Logging > Logging Filters.

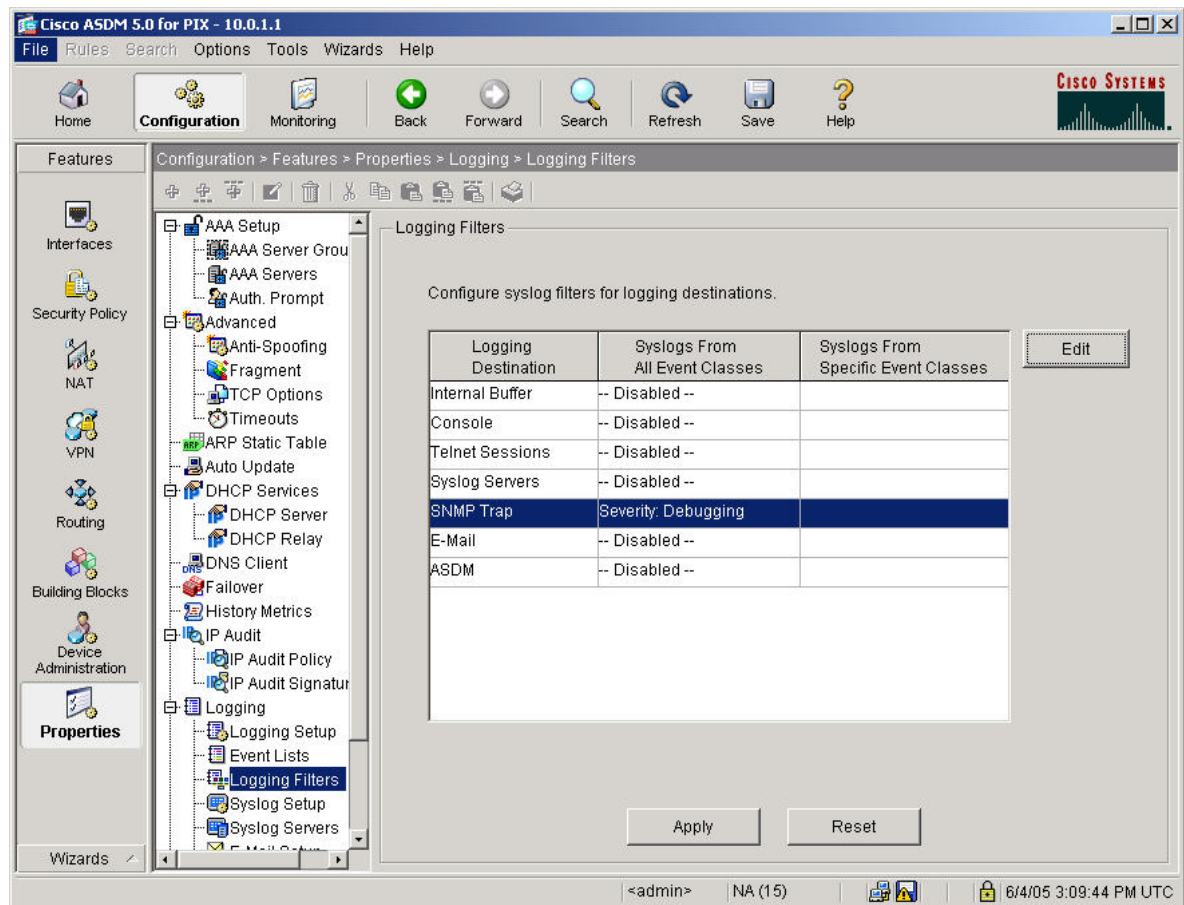
OK Cancel Help

- g. Click the **OK** button to return to the SNMP window.

- h. Click the **Apply** button.
- i. If the **Preview CLI Commands** window appears, click the **Send** button to continue.



- j. Navigate to **Configuration>Features>Properties>Logging>Logging Filters**.
- k. Select **SNMP Trap** from the **Logging Filters** group. Click the **Edit** button to bring up the **Edit Logging Filters** window.
- l. Select the **Filter on severity** radio button and then select **Debugging** from the drop down menu.
- m. Click the **OK** button to return to the **Logging Filters** window.



- n. Click the **Apply** button.
- o. If the **Preview CLI Commands** window appears, click the **Send** button to continue.

### Step 3 Verify SNMP Operation

Complete the following steps to verify SNMP is operational

- a. Download and install SNMPWalk in a SNMP folder on C:\
- b. On the Student PC, open a command prompt.
- c. Get to a root C:\> by entering `cd \`
- d. Go to the snmp directory.

```
C:\> cd snmp
```

```
C:\SNMP>
```

- e. Perform SNMP reconnaissance using snmpwalk.exe. Some output has been omitted.

```
C:\SNMP>snmpwalk -v 1 10.0.1.1 public
.iso.3.6.1.2.1.1.1.0 = "Cisco PIX Firewall Version 7.0(1)."
```

...

```
.iso.3.6.1.2.1.1.2.0 = OID: .iso.3.6.1.4.1.9.1.451
.iso.3.6.1.2.1.1.3.0 = Timeticks: (128200) 0:21:22.00
.iso.3.6.1.2.1.1.4.0 = "John Doe"
.iso.3.6.1.2.1.1.5.0 = "Pixl.cisco.com"
.iso.3.6.1.2.1.1.6.0 = "Data center"
.iso.3.6.1.2.1.2.2.1.2.1 = "Cisco PIX Security Appliance 'outside'
interface"
.iso.3.6.1.2.1.2.2.1.2.2 = " Cisco PIX Security Appliance 'inside'
interface"
.iso.3.6.1.2.1.2.2.1.2.3 = " Cisco PIX Security Appliance 'dmz'
interface"
.iso.3.6.1.2.1.2.2.1.4.1 = 1500
.iso.3.6.1.2.1.2.2.1.4.2 = 1500
.iso.3.6.1.2.1.2.2.1.4.3 = 1500
.iso.3.6.1.2.1.2.2.1.5.1 = Gauge: 100000000
.iso.3.6.1.2.1.2.2.1.5.2 = Gauge: 100000000
.iso.3.6.1.2.1.2.2.1.5.3 = Gauge: 100000000
.iso.3.6.1.2.1.2.2.1.6.1 = Hex: 00 0B FD 81 EB 83
.iso.3.6.1.2.1.2.2.1.6.2 = Hex: 00 0B FD 81 EB 84
.iso.3.6.1.2.1.2.2.1.6.3 = Hex: 00 02 B3 BB D0 D0
.iso.3.6.1.2.1.2.2.1.9.1 = Timeticks: (3531000000) 408 days,
16:20:00.00
.iso.3.6.1.2.1.2.2.1.9.2 = Timeticks: (3545000000) 410 days,
7:13:20.00
.iso.3.6.1.2.1.2.2.1.9.3 = Timeticks: (3557000000) 411 days,
16:33:20.00
.iso.3.6.1.2.1.4.20.1.1.10.0.1.1 = IPAddress: 10.0.1.1
.iso.3.6.1.2.1.4.20.1.1.172.16.1.1 = IPAddress: 172.16.1.1
```

```
.iso.3.6.1.2.1.4.20.1.1.192.168.1.2 = IPAddress: 192.168.1.2  
.iso.3.6.1.2.1.4.20.1.3.10.0.1.1 = IPAddress: 255.255.255.0  
.iso.3.6.1.2.1.4.20.1.3.172.16.1.1 = IPAddress: 255.255.255.0  
.iso.3.6.1.2.1.4.20.1.3.192.168.1.2 = IPAddress: 255.255.255.0
```