Graduate Program in Information Science, Telecommunications and Networking
School of Information Sciences
University of Pittsburgh

TEL2821/IS2150: INTRODUCTION TO SECURITY
Lab: Firewall Operation Basics

Version 1.1, Last Edited 11/6/2007

Students Name: _____

_____

_____

Date of Experiment: _____

GSA: Carlos Caicedo

Read the following guidelines before working in the lab

General Guidelines

Equipment requirements
For this lab assignment you will use the following devices.

PIX 501 Firewall
3 Windows Vista Ultimate PC (PC1, PC2, PC3)
1 Windows XP PC environment (Administration PC)
2 WS 3550 Workgroup switches
Cables and patch cords

The network setup you will be working on is shown in figure 1.

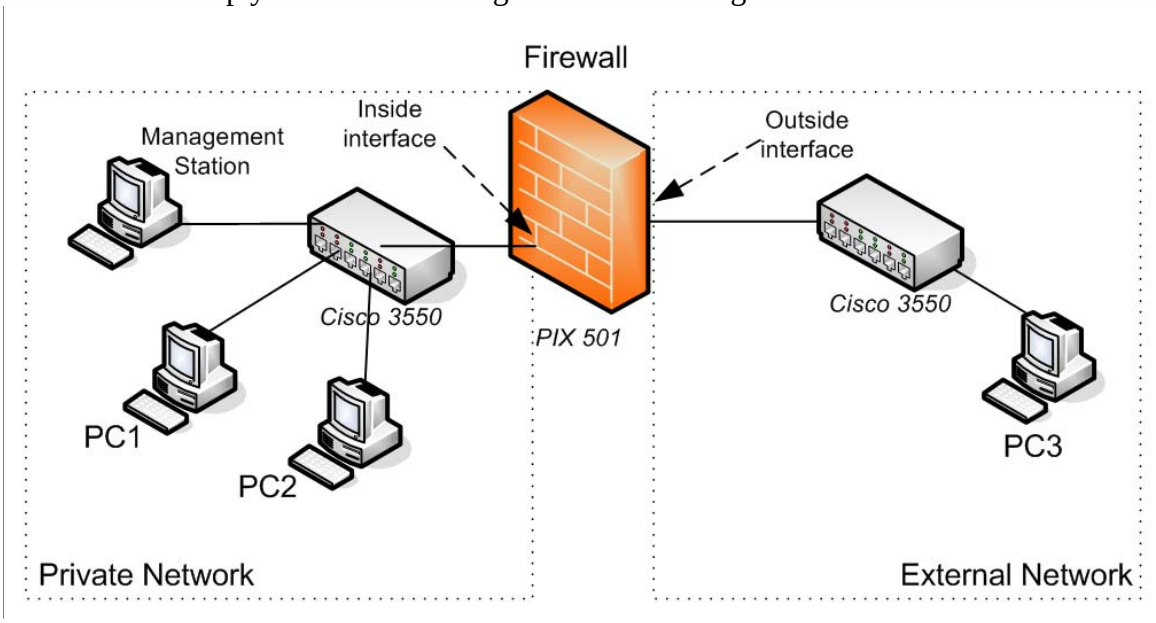

Figure 1. Network Setup

Equipment configuration
Up to two groups of students can be in the LERSAIS Lab working on this lab assignment. Each group will be working on a different set of devices configured as shown in figure 1. When you registered for this lab you should have registered as GROUP A or GROUP B. Each PC in the lab has a label with its name. Table 1 lists the IP addresses given to each machine. Please check the table to determine the devices you will be using in the lab and some of their configuration details.

Device/Interface	Group A	Group B
PC1	SECURITY05 IP: 192.168.20.5	SECURITY10 IP: 192.168.20.10
PC2	SECURITY06 IP: 192.168.20.6	SECURITY11 IP: 192.168.20.11
PC3	SECURITY07 IP: 10.1.1.7	SECURITY03 IP: 10.1.1.3
PIX Firewall Inside interface	PIX1 IP: 192.168.20.31	PIX2 IP: 192.168.20.42
PIX Firewall Outside interface	IP: 10.1.1.1	IP: 10.1.1.22
Management Station	SECURITY02	SECURITY04

Table 1. Device configuration data

Working with FTP and Telnet

For some of the steps in this lab you will be required to establish FTP or Telnet session between machines. The steps for establishing these sessions are explained in the Appendix of this document.

Working with the management station

In this lab you will not be changing the configuration of any PC, you will however, change the configuration of a Firewall device (Cisco PIX 501 Firewall) from a Management station in which software (PIX Device Manager) has been loaded for you to make changes to the behavior of the firewall via a graphical user interface (GUI).

Please keep the following in mind when working with the management station software:

- The management software as configured in the lab is running over a virtualized Windows XP environment which sometimes makes the handling of the screen pointer with a mouse somewhat tedious. When the cursor does not get to the place in the screen you want, try moving the mouse really fast to get it to a given position on the screen.
- **Do not** close the management software window and never exit the program or hit the *Save* option. If you do, contact the GSA to solve the problem.
- Every time you make a change to the configuration of the firewall, it might take up to three seconds for you to see a screen refresh that shows the changes you have made. Be patient and don't click around the screen when the refresh is being made.

Written report

A written report is required for this assignment. You should turn in this printout as part of your written report. Space has been provided to answer some of the questions of the exercises in this lab. However, you should attach extra sheets of paper with your answers for some of the questions. Please label your extra sheets with your name and indicate precisely which questions you are answering.

Objective

To familiarize the student with the functionality of firewalls and access control lists and their use in securing network environments.

Background on the PIX firewall

The PIX 501 firewall has two main interfaces. The *inside* interface to which the private network is connected and the *outside* interface to which the public and/or less secure network is attached. The basic function of the firewall is to block traffic from the outside world (public / *outside* interface) from getting into the private network. The firewall can also be used to control what traffic from the private network can get to the public network.

Lab Procedures

Part 1: Checking the system

Before you experiment on the firewall perform the following tasks. If your system does not comply to any of the following steps, contact the GSA.

1. Go to your Management Station. A window displaying the PIX Device Manager window should be present.
2. Click on the *Configuration* icon. Select the *Access Rules* tab and choose the *Access Rules* option. You should a list of the access rules configured on the firewall. The only access rule present should look like the one shown in Figure 2.

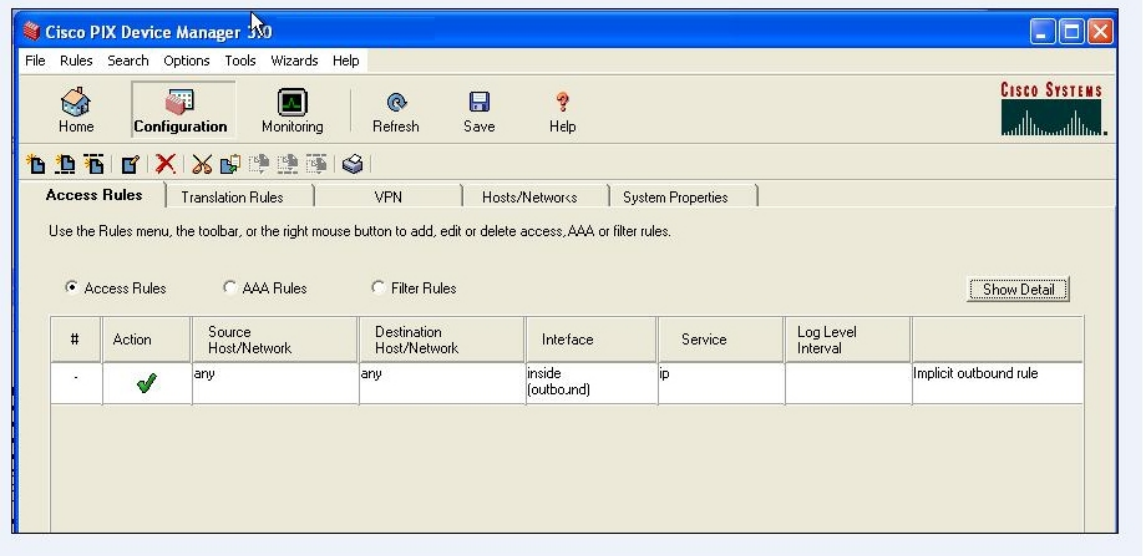

Figure 2. Initial access rule list

Question #1: What do you think this access rule means? You can refine your answer after doing the steps in this part of the lab.

_____
_____
_____
_____
_____

3. Select the *Translation Rules* tab and choose the *Translation Rules* option. The only translation rule present should look like the one displayed in Figure 3.

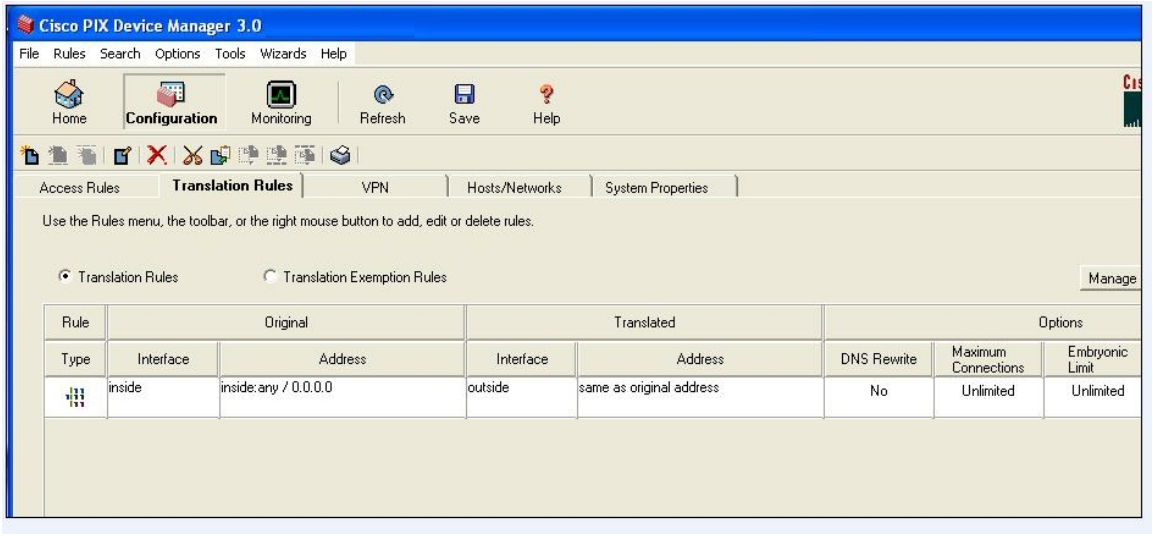

Figure 3. Translation rule

Translation rules refer to the way. IP addresses are translated between interfaces.

4. If Steps 2 and 3 were successful, the firewall is configured appropriately. Now, establish the following sessions between machines and mark your results in the following table. Go to the source machine, login with the *StudentAdmin* account (password: security) and establish the session to the destination machine.

Session type	**Source machine**	**Destination machine**	**Result Success / Failure**
FTP	PC1	PC2	
Telnet	PC1	PC2	
FTP	PC1	PC3	
Telnet	PC1	PC3	
FTP	PC3	PC1	
Telnet	PC3	PC1	

Question #2: Why do you think some of the sessions were successful and others unsuccessful.

_____
_____
_____
_____
_____
_____
_____

Part 2: Enabling *ping* (ICMP) traffic

Ping is a command that can be used for network diagnostics. It can be used to determine if a machine is reachable (alive) through the network. This is good when you are a network manager and want to know if the machine is accessible or not. However, for an attacker, the ping command tells him the list of machines that are available in a network which he might later decide to attack.

The *ping* command sends messages based on the ICMP protocol in order to determine the reachability of a system. A machine (source) that sends a ping to another one actually sends an ICMP request message that is answered by the destination machine with an ICMP reply message. If either message is lost or blocked, reachability of the system cannot be determined.

Usually firewalls **block** ICMP traffic in order to hide the machines of the internal network from users in the external network. However, for learning purposes only, we will enable ping traffic through the PIX firewall. Again, this is not good practice and is done only for learning purposes. Follow these steps:

1. On PC1, open a command window and try to *ping* PC3. That is, execute the following command

ping <PC3's IP address>

2. The command should not have worked. To allow ping (ICMP) traffic through the firewall first go to the PIX Device Manager in the management station and perform the following:

3. Click on the *Configuration* icon. Select the *Access Rules* tab and choose the *Access Rules* option. You should see a list of the access rules configured on the firewall. We will add a new rule to allow ICMP traffic through the firewall. To start the process, click on the *Rules* menu in the menu bar and click on *Add…*

4. We want to permit ICMP traffic from the *outside* network interface to go into the *inside* network. To do this, change the options on the *Add Rule* window to those shown in Figure 4. After making the changes, click the *OK* button.

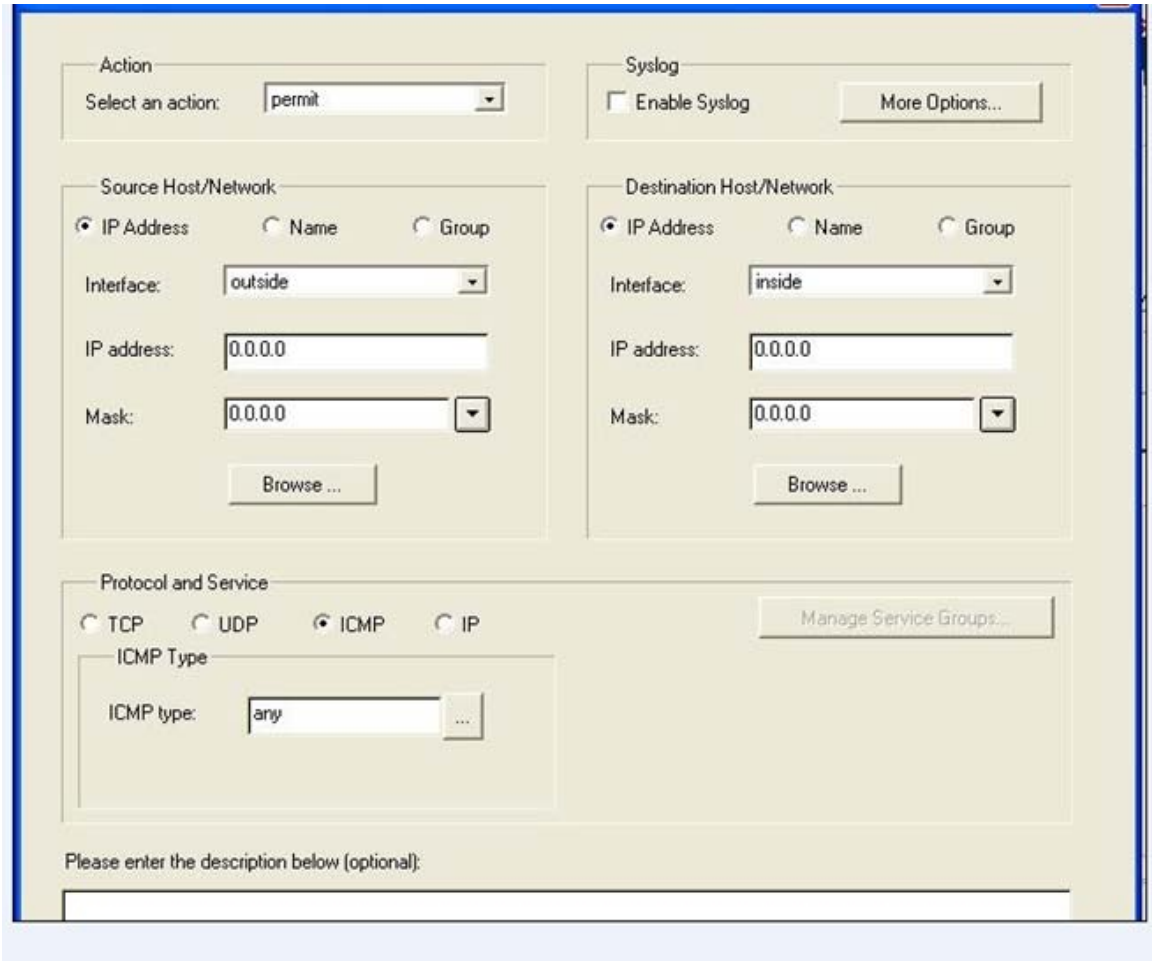

Figure 4. Allowing ICMP traffic (outside to inside)

5. Apply the rule by clicking the *Apply* button. Wait a couple of seconds for the new configuration to go to the firewall.

6. Repeat step 1. This time the ping should have been successful.

Question #3: How does the new rule you just added look like in the *Access Rules* table? Write the access rule display here.

_____
_____
_____
_____
_____

Question #4: Express in your own words what this rule is telling the firewall to do. Try to be as technical as possible.

_____
_____
_____
_____
_____

Question #5: What do you think the IP address 0.0.0.0 stands for? It was used when you defined the access rule.

_____
_____
_____

Part 3: Allowing FTP access for external network nodes

In this part of the lab, we will make the FTP service on PC2 accessible to nodes in the external network (PC3 in this case).

1. On PC3, open a command window and try to *ping* PC2. That is, execute the following command

ping <PC2's IP address>

2. The command should have worked. Now, try establishing a FTP session from PC3 to PC2.
You should have observed that the FTP session establishment was unsuccessful. At this point ICMP traffic can reach PC2 from the external network but FTP traffic cannot. To allow nodes in the external network (PC3) to access PC2 (internal network) we need to add another access rule.

3. Go to the *PIX Device Manager* in the Management station. Click on the *Configuration* icon. Select the *Access Rules* tab and choose the *Access Rules* option. You should see a list of the access rules configured on the firewall. We will add a new rule to allow FTP traffic from the outside network through the firewall to PC2. To start the process, click on the *Rules* menu in the menu bar and click on *Add…*

4. We want to permit FTP traffic from the *outside* network interface to go into the *inside* network but only to PC2. To do this, change the options on the *Add Rule* window to those shown in Figure 5. After making the changes, click the *OK* button.
Note: In the field marked with an oval in Figure 5 put the IP address for PC2 that belongs to your group list (Group A or Group B)

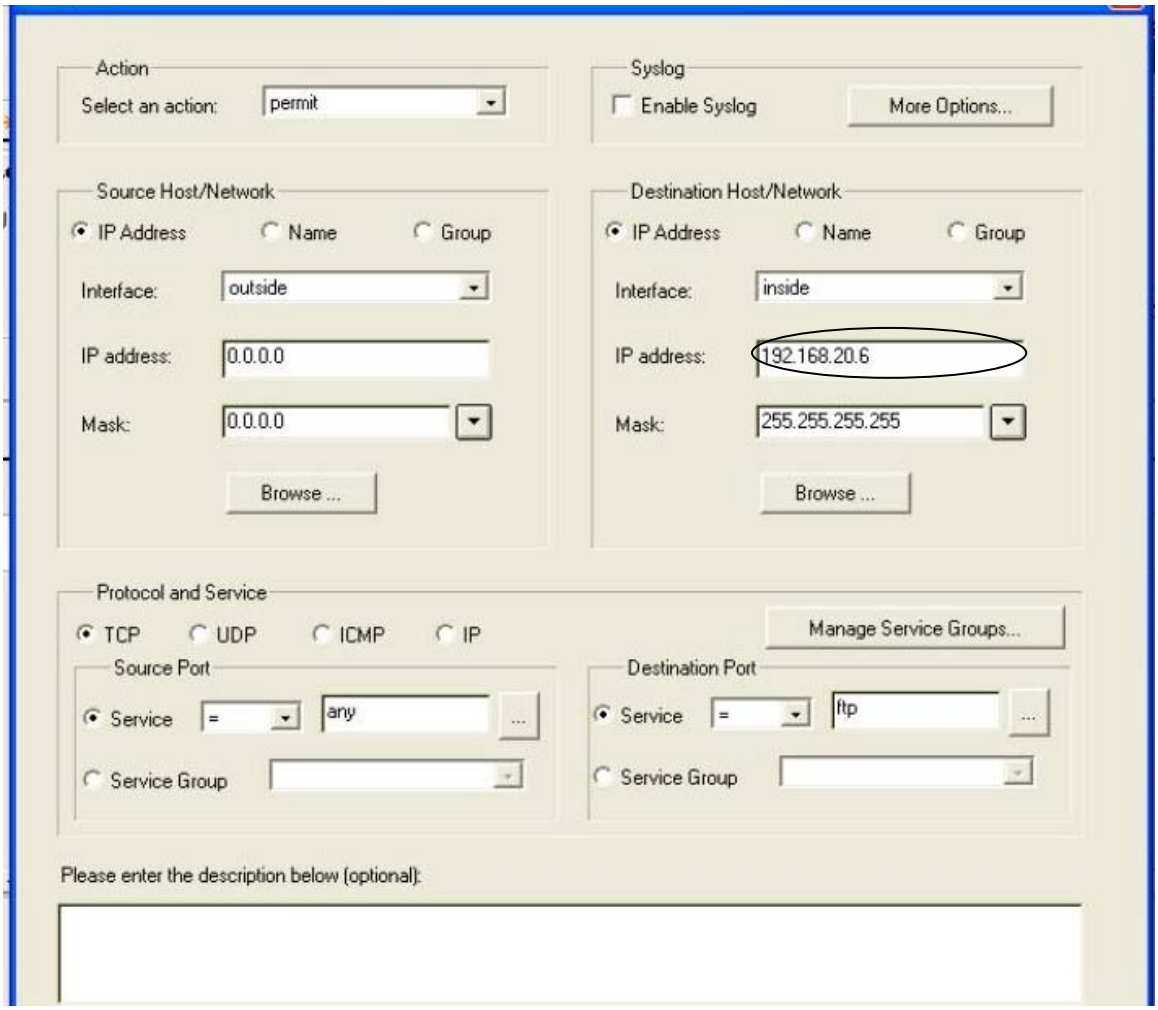

Figure 5. Allowing FTP access to PC2 from the outside network

5. If you get a message saying that the PDM cannot find the IP address of PC2 on the inside interface. Click the *OK* button to start the process to add PC2 to the interface hosts list. Then click on *Next* in the *Basic Information* request window and *Finish* in the *NAT (Network Address Translation)* window.

6. Apply the rule by clicking the *Apply* button. Wait a couple of seconds for the new configuration to go to the firewall.

7. Try establishing a FTP session from PC3 to PC2. It should have worked.

Question #6: How does the new rule you just added look like in the *Access Rules* table? Write the access rule display here.

_____

_____

_____

Question #7: Express in your own words what this rule is telling the firewall to do. Try to be as technical as possible.

_____
_____
_____
_____
_____

Part 4: Denying Telnet access for internal nodes

In this part of the lab we will block (deny) the *Telnet* service traffic from all hosts that are on the inside network to the external (outside) network.

1. Establish a telnet session from PC1 to PC3. This should have been successful.

2. To deny *telnet* service traffic from the inside network to the outside network, let's add an access rule to the firewall. Go to the *PIX Device Manager* in the Management station. Click on the *Configuration* icon. Select the *Access Rules* tab and choose the *Access Rules* option. You should see a list of the access rules configured on the firewall.
We will add a new rule. To start the process, click on the *Rules* menu in the menu bar and click on *Add…*

3. We want to deny Telnet traffic from the *inside* network interface from going to the *outside* network. To do this, change the options on the *Add Rule* window to those shown in Figure 6. After making the changes, click the *OK* button.

4. Try establishing a telnet session from PC1 to PC3. This should have been *un*successful this time.

Question #8: What is the error message you got in PC1 when you tried to establish the telnet session to PC3 ?

_____
_____
_____

Question #9: Looking back at Figure 6 can you think of another way you could have established the same result on the system (denying *Telnet* traffic from the inside to the outside)? Describe your reasoning.

_____
_____
_____
_____
_____

Question #10: Again, looking at Figure 6 what would you change to deny Web traffic (HTTP) to hosts from the inside network to the outside.

Note: Suppose you want to prevent your employees to surf the web while they are on your company's computers. ;-)

_____
_____
_____
_____
_____

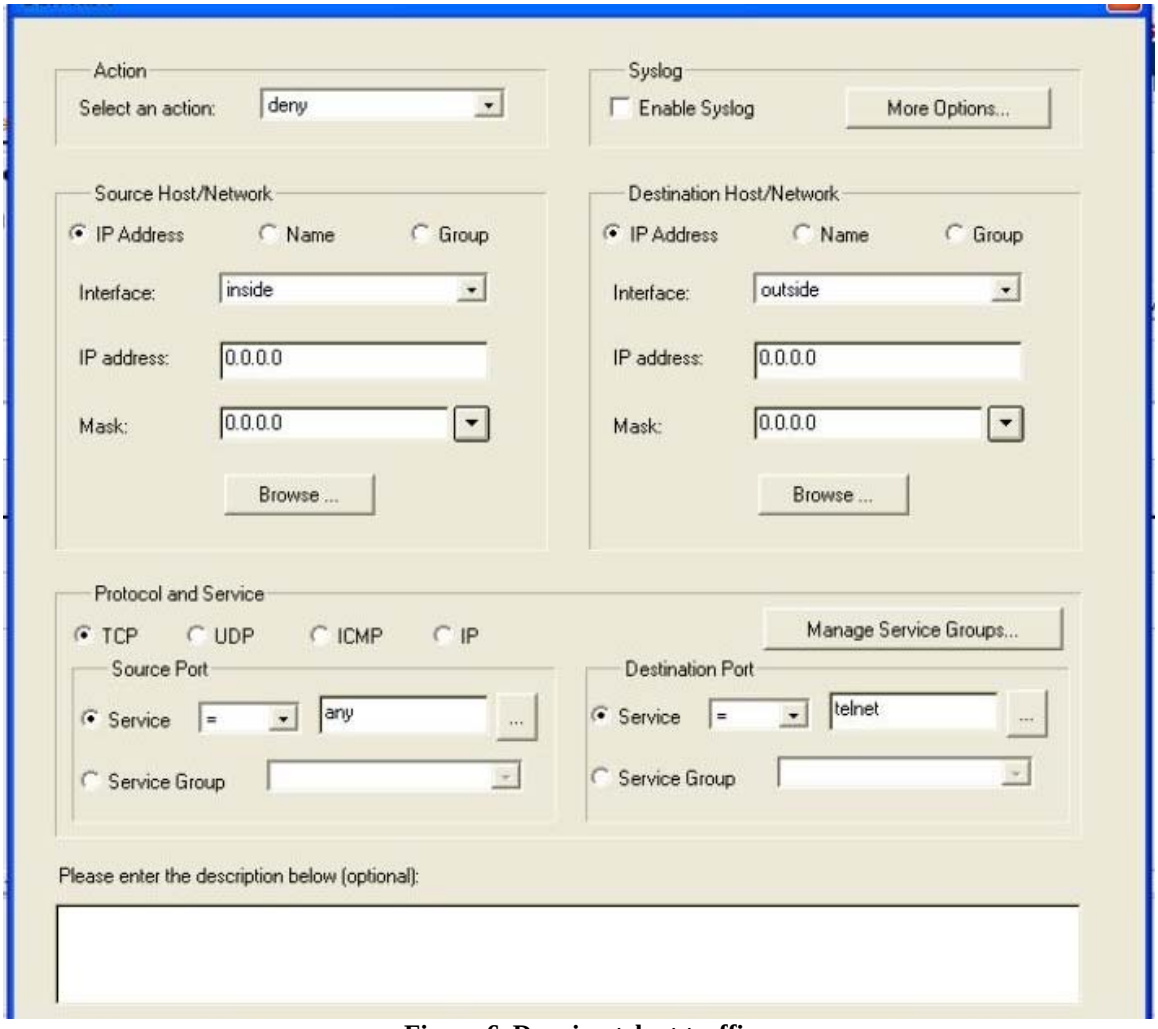

Figure 6. Denying telnet traffic

Part 5. Restoring the system

Please restore the firewall to its original configuration before leaving the lab. Follow these steps.

1. Select each *Access Rule* you have added and delete it. (Hold down the *Right* mouse buttion and click on *Delete*)

2. Click on *Apply* to send the new configuration to the firewall. You should see one access rule only in the access rule list. This list should look like the one in Figure 2.

3. **Do not** close the PIX Device Manager window in the Management station but do logout from the *StudentAdmin* account on PC1, PC2 and PC3.

The End

Appendix

Establishing a FTP session
To establish a FTP session from machine A to machine B do the following:

1. Open a command screen from machine A: Press and hold the *Windows* key while also pressing the key for the letter R. The *Run* command window should open. Write *cmd* in the Run command window. A black text based command screen window should open up.

2. On the command screen start a FTP session to machine B by executing:
   ftp <ip_address_of_Machine_B>

3. Login as user *anonymous* , there is no password so you can press the *Enter* key at the password prompt.

4. When you want to logout of the FTP server type *quit*

Establishing a Telnet Session
To establish a Telnet session from machine A to machine B do the following:

1. Open a command screen from machine A: Press and hold the *Windows* key while also pressing the key for the letter R. The *Run* command window should open. Write *cmd* in the Run command window. A black text based command screen window should open up.

2. On the command screen start an FTP session of machine B by executing:
   telnet <ip_address_of_Machine_B>

3. You don't need to write your account and password information. These have been pre-configured for you. In this session you will be logging in to Machine B you're your *StudentAdmin* account. The system will give you a message asking you if you want to send your password information, type *y* (for yes) to proceed.

4. Although the screen might not change substantially, you can verify that you are connected to Machine B because its IP address will be displayed in the upper right hand corner of the Telnet window.

5. When you want to exit the telnet session type *exit.*