University of Pittsburgh
School of Information Science

IS2820/TEL2813 - Security Management

Lab assignment #1
Firewall operation and Access Control Lists

Lab GSA: Carlos Caicedo
Document version: 1.0 / 2008

I. Lab resources for this assignment

PIX 501 Firewall (PIX 1)
4 Windows Vista PCs (SECURITY02, 05, 06, 07)
1 WS 2940 Workgroup switches (glswitch1)
1 Hub (HUB 01)
Cables and patch cords

II. Preliminary questions

Answer these questions and turn in your answers at the time and date specified by the instructor or GSA.

1. What is the difference between Network Address Translation (NAT) and Port Address Translation (PAT) ?

2. Read the assignment statement and figure out the necessary address translation scheme that you'll need to use as well as the commands required to implement it. Write the details of your address translation scheme and the sequence of commands you will issue. You might figure out that you need to change some of your commands when you actually get to configure the equipment but this will give you a good point to start with.

3. To test your configuration you might want to use the **ping** command, however this command relies on ICMP protocol based messages. Unless you allow these messages to go through the firewall you cannot use ping to test reachability.
    a. How does a PIX firewall handle ICMP messages by default?
    b. How do you allow ICMP messages to go through the firewall?

Note:
If you enable **ping** during the testing/debugging phase of your configuration process make sure that you take out any configuration changes that allowed ping (ICMP) traffic to go through the firewall before turning in your results.

III. Setup description:

The network structure for this lab is shown in figure 1. All computers shown have the IP addresses displayed in the figure and are configured as FTP and Telnet servers.

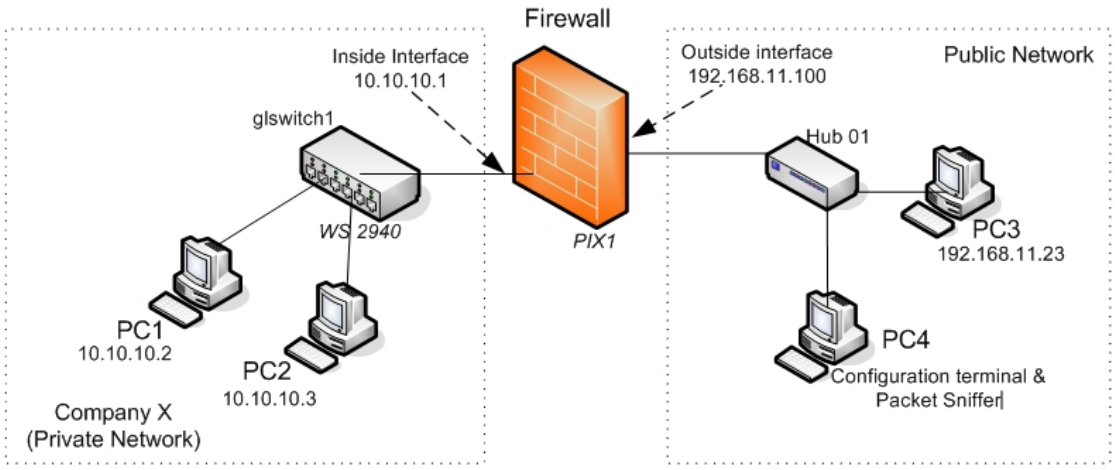

Figure 1

Node	Computer Label	IP address	Comments
PC1	SECURITY05	10.10.10.2	Node in the private network
PC2	SECURITY06	10.10.10.3	Node in the private network
PC3	SECURITY07	192.168.11.23	Node in the public network
PC4	SECURITY02	192.168.11.24	This computer will be used as the configuration terminal (with *putty*) and as a packet sniffer (with *WireShark*)

IV. Lab objective

You must restrict the traffic between the Company X's private (inside) network and the public (outside) network according to the following requirements:

Part A:

- Permit FTP access from the public network to PC1 in the private network, no private IP addresses should be exposed in the process.
- Telnet access from the public network to PC1 is not to be allowed
- FTP and Telnet from the public network to PC2 is not to be allowed
- FTP and Telnet access from the private network PCs to the public network PCs is allowed
- The true IP addresses of the computers on the private network should not be seen in the public network.
- Use the address pools that are mentioned in section IV

Part B:

- Modify the configuration of Part A to deny FTP and Telnet access from private network PCs to the public network

Satisfaction of these requirements can be approved by satisfying the following criteria:

Compliance criteria for Part A:

1. Users from the public network should be able to FTP to PC1 but not to PC2. Users FTP to PC1 without directly using one of Company X's private IP addresses.
2. Traffic from the private network that goes into the public network must not reveal the private network's IP addresses. The packet sniffer should be used to validate this.
3. Telnet access from the public network to PCs in the private network should not work
4. Telnet and FTP access from the private network PCs to the public network's PCs works.

Compliance criteria for Part B:

1. Satisfy compliance criteria 1, 2 and 3 of part A
2. Telnet and FTP access from the private network PCs to the public network's PCs does not work.

V. Technical details

Log in for the Windows Vista machines

For your work in this lab you will use the username *StudentAdmin* with password *security* on all Windows Vista based machines.

Address pools

Company's X private address pool for its network is 10.10.10.0 with a netmask of 255.255.255.0

Company's X public address pool is 192.168.11.0 – 192.168.11.7 although only addresses from 192.168.11.1 – 192.168.11.6 are usable.

Connecting to and configuring the PIX1 firewall

Configuration of the PIX1 firewall will be done through the *console* port of the PIX which is attached to a blue cable and a USB to Serial adapter on PC4. **Do not** remove the blue cable under any circumstance.

To activate a configuration terminal on PC4, double click on the icon of the application called *putty* which should be in the desktop of PC4's Windows Vista. Once activated double click on the *Security Lab* session configuration to connect to the PIX. You might have to press the *Enter* key several times to "wake up" the connection.

You will not be using the PIX Device Manager's graphical user interface to configure the firewall in this assignment.

Erasing previous configurations on the PIX firewall

Before starting to configure the PIX firewall you should erase any previous configuration already stored on it so that you can start your work from an unconfigured system. To do this enter privileged mode on the PIX firewall and use the following commands:

write erase
reload

These commands erase the current configuration from the flash memory of the PIX and reboot the firewall. To start configuring the PIX answer *yes* to any prompt that shows up except for the one that says *Pre-configure PIX Firewall now through iterative prompts?* to which you should answer *no.*

After all this you'll be left at the prompt of the unprivileged mode of the PIX. Since there is no configuration stored on it, the enable (privileged mode) password is blank. When asked for the enable password just press the *Enter* key.

When you have finished this lab assignment, erase the configuration that you have provided to the PIX firewall so the next student team will also start from an unconfigured system.

IP address for the Firewall's interfaces

To have a good behaving network setup and to avoid having to configure any IP address and routing details on the PC nodes you **must** assign IP address 10.10.10.1 to the inside interface of the firewall and IP address 192.168.11.1 to the outside interface. Note that this means that you'll be reserving and using one of addresses from your public address pool to identify your connection to the public network (outside interface).

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.*

VI. Lab report

The lab report for this assignment should include.

1. Answers to the questions posted in the *Preliminary Questions* section of this assignment if they have not been requested before by the instructor or GSA.

2. Evidence that you satisfy two of the compliance criteria for Part A and Part B by posting the screenshots or text of any kind of test that you conducted to verify such compliance.
   You can use the Windows Vista "snipping tool" located in the Accessories folder to capture screenshots. Just make sure to delete the files before you leave the lab.

3. Final configuration of the PIX firewall that satisfies all the compliance criteria. Include the configuration file that satisfies the requirements of Part A and the configuration file that satisfies the requirements of Part B (or a list of changes that you had to do to Part A's configuration).

Tip: To capture the configuration of the firewall, open a Terminal connection through the console port of the firewall (as explained in the introductory session) , enter privileged mode and execute the **show running configuration** command (The short version is **sh run**). Then select the configuration text and press *Ctrl-C.* Open a text editor (like Wordpad) and paste the configuration text with *Crl-V.* Save the file and include its contents in the report.

VII. Firewall Lab references

These are some references you can use to prepare for this lab. They are available online via PittCat.

Title: *Cisco security* specialist's guide to PIX Firewall [electronic resource] / Vitaly Osipov.
Author: Osipov, Vitaly.
Published: Rockland, Mass. : Syngress Pub., c2002.
Read: Chapters 2 and 3 (4 is optional) , (9 if you plan to use graphical GUI)

Title: CCSP *Cisco* Secure PIX firewall advanced exam certification guide [electronic resource] : CCSP self-study / [Greg Bastien and Christian Degu].
Author: Bastien, Greg.
Published: Indianapolis, IN : *Cisco* Press, c2003.
Read: Chapters 5 and 6

Title: Managing *Cisco* network *security* [electronic resource] / Eric Knipp ... [et al.] ; technical editor, Edgar Danielyan.
Edition: 2nd ed.
Published: Rockland, Mass. : Syngress Media, c2002.
Read: Chapters 3 – 5