**University of Pittsburgh**
**School of Information Science**

**IS2820/TEL2813 - Security Management**

# Lab assignment #2
# IPSec and VPN Tunnels
**(Document version 1.1)**

Lab GSA: Carlos Caicedo

**Page**



## I. Lab resources for this assignment

2 PIX 501 Firewalls (PIX1 , PIX2)
5 Windows Vista PCs (SECURITY02, 05, 06, 07, 10)
2 Cisco WS 2940 Workgroup switches (glswitch1, glswitch2)
1 Cisco WS 3550 switch/router
1 Hub
Cables and patch cords

## II. Preliminary questions

*You must have submitted the answers to these questions before you attempt to do the lab assignment. The GSA or course instructor will give you the dates for submission of the answers to these questions and of the lab report.*

1. What are the benefits or disadvantages of VPNs? Briefly mention the ways in which VPNs can be implemented.

2. What is IPSec? Briefly describe the operation modes of IPSec.

3. What are the setup phases of the ISAKMP/IKE protocol?
   a. Describe each of them.
   b. What information is required during each phase?
   c. What commands are useful to setup ISAMP/IKE on a PIX?

## III. Bibliographical 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
Author: Osipov, Vitaly.
Published: Rockland, Mass. : Syngress Pub., c2002.
Read: Chapter 7

Title: CCSP Cisco Secure PIX firewall advanced exam certification guide
Author: Bastien, Greg.
Published: Indianapolis, IN : Cisco Press, c2003.
Read: Chapters 11 and 12

## IV. 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.

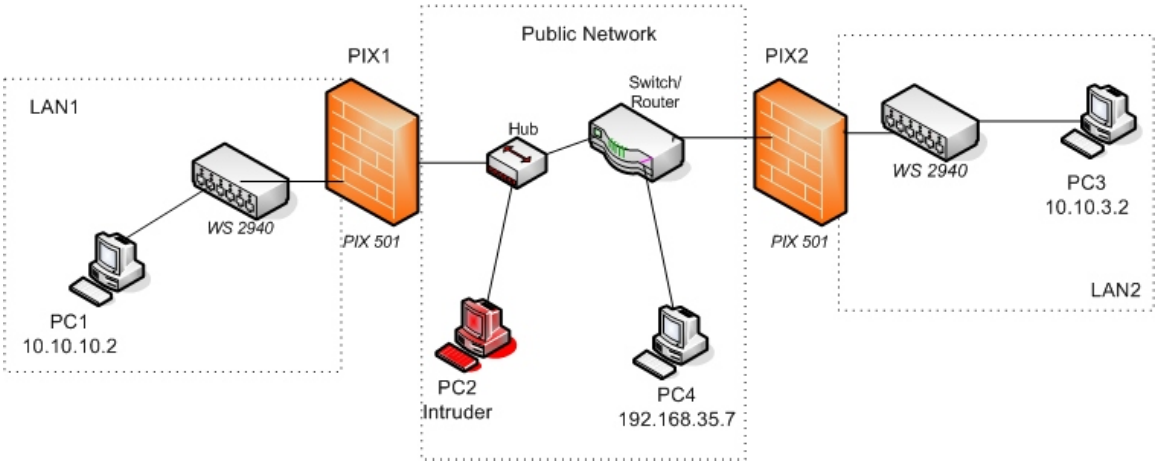


**Figure 1**

| Node | Computer Label | IP address | Comments |
|---|---|---|---|
| PC1 | SECURITY07 | 10.10.10.2 | Node in the private network LAN1 |
| PC2 | SECURITY06 | ---------- | Node in the public network |
| PC3 | SECURITY10 | 10.10.3.2 | Node in the private network LAN2 |
| PC4 | SECURITY05 | 192.168.35.7 | Node in the public network |
| PC5 | SECURITY02 | ---------- | This computer will be used as the configuration terminal (not shown in figure 1) |

# V. Lab Objective

You must establish an IPSec VPN tunnel between the two firewalls (PIX1 and PIX2) so that the traffic that flows through the tunnel from LAN1 to LAN2 is encrypted and cannot be interpreted by any intruder in the public network.
***Note**: No certificate authority is required for this lab.*

***Read all sections of this document so that you are informed of the details of the tasks that you'll have to perform and the methods you'll use to perform them.***

## *A. Part A:*

*Requirements*

1. Allow telnet access to PC1 from any PC outside LAN1.
    a. PC1s true IP address should not be revealed so it is recommended that you create a static NAT entry for PC1
2. Configure NAT in PIX 1 and PIX2
3. Establish a telnet session from PC3 to PC1 and capture the session's traffic with Wireshark on PC2 (The Intruder's PC). Login from PC3 to PC1 with your *StudentAdmin* account.

*Tasks*

1. Analyze the captured traffic and determine the packets in which the StudentAdmin's account password is being sent.

*Compliance criteria for Part A:*

1. Users from the networks outside LAN1 (PC3 and PC4) can telnet to PC1
2. Traffic from the private network that goes into the public network must not reveal the private network's IP addresses.
3. The traffic flow between LAN 1 and LAN 2 can be captured for your analysis.

## *B. Part B:*

*Requirements*

1. Reconfigure PIX1 and PIX2 to establish an IPSec VPN tunnel between them that will secure traffic flowing from LAN1 to LAN2. This means, securing traffic that will flow between networks 10.10.10.0 and 10.10.3.0
   **Note: For true VPN functionality, NO address translation must affect traffic flow between LAN1 and LAN2 ONLY. Additionally, services on LAN1 and LAN2 should work for any user of either LAN.**
2. Establish a telnet session from PC3 to PC1 and capture the session's traffic with Wireshark on PC2. Login from PC3 to PC1 with your *StudentAdmin* account.

*Tasks*

1. Analyze the captured traffic and determine the differences with the packets captured for a similar session in part A.
2. Can you access any service on the PCs of LAN1 or LAN2 from PC4 ? Can the PCs from either LAN access services on PC4 ? What does this tell you about the security of the VPN tunnel you have configured?

*Compliance criteria for Part B:*

1. Telnet and FTP access among the computers on LAN1 and LAN 2 works. (PC1 can Telnet to PC3 and vice versa, PC1 can FTP to PC3 and vice versa)
2. The captured traffic flow between LAN1 and LAN2 shows encrypted packets.

# VI. Technical details

## *A. Address pools*

LAN1's internal (private) address pool for its network is 10.10.10.0 with a netmask of 255.255.255.0
LAN1's external (public) address pool is 192.168.2.1 – 192.168.2.63 However, 192.168.2.1 has to be assigned to PIX1's outside interface

LAN2's internal (private) address pool for its network is 10.10.3.0 with a netmask of 255.255.255.0
LAN2's external (public) address pool is 192.168.10.1 – 192.168.10.63 However, 192.168.10.1 has to be assigned to PIX2's outside interface

## *B. IP addresses for the PIX firewalls*

PIX1
Inside interface : 10.10.10.1
Outside interface: 192.168.2.1
(Use the *hostname* command to provide a name to the firewall *hostname pix1* sets the name to *pix1*)

PIX2
Inside interface : 10.10.3.1
Outside interface: 192.168.10.1
(Use the *hostname* command to provide a name to the firewall)

## *C. Routing information and default route settings*

Traffic between LAN1 and LAN2 has to go through a public routed network in this assignment. The routing settings for this network have been set for you but you must take care of indicating the correct default gateways to the firewalls that will take care of the traffic of LAN1 and LAN2 as follows:

On PIX1 set the default gateway to be 192.168.2.65
On PIX2 set the default gateway to be 192.168.10.65

### *D. VPN Tunnel parameters*

- Use only ESP since traffic is going through a "public" network.
- Use pre-shared keys for device authentication. The key can be a string of characters and numbers selected by you. *Example: cisco123*.
- For encryption use DES only.

All other parameter values (DH group, HMAC standard, etc) should be chosen by each student group.

### *E. Connecting to and configuring the PIX firewalls*

You will be configuring two PIX firewalls with one configuration terminal (PC5). In order to connect the configuration terminal to the appropriate firewall you will have to move the selector knob in the *data switch* box that you'll find in the lab.

If you position the selector knob in the **A** position the configuration terminal will be connected to the PIX1 firewall. To connect to the PIX2 firewall, move the selector knob to the **C** position. Do not tamper with the cables connected to the data switch, just move the selector knob.

Once you have selected the firewall that you want to configure, you can activate a configuration terminal on PC5 by double clicking on the icon of the application called *putty* which should be in the desktop of PC5's Windows Vista environment. 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.

### *F. 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.

### *G. 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.

### *H. 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*

### *I. 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.*

### *J. Running Wireshark to capture packets*

The software application *Wireshark* is installed on all computers of the security lab. However for this lab you will only need to activate it in PC2 . To activate *Wireshark* and start a packet capture, do the following:

1. Login into each machine as *StudentAdmin*
2. Activate the ***Wireshark*** icon that is on the Desktop
3. Go to the *Capture* menu and click on the OK button to start the packet capture. A capture progress window should pop-up.
4. Once enough packets have been captured or enough time has elapsed, click on the Stop button. Capture only the packets you need in order to make your analysis easier.
5. Once you have stopped the packet capture, you should be able to recognize three different screen sections: The packet list section (upper section), the packet details section (middle section) and the packet bytes section (lower section). Each time you select a packet in the packet list section the other two sections will change accordingly. You can now analyze the captured packets as you wish.

Note: The **Filter:** text field on the main screen allows you to specify which packets should be displayed on the packet list section of the screen. Use this to get a view of only those packets that you are interested in. For example, if you write *telnet* in this field you will only see the packets related to a captured telnet session.

## VII. Lab report

The lab report for this assignment should include.

1. Printout or screen capture of one of the packets captured with Wireshark for part A and another for part B.
2. 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). Include a list of the VPN parameters that were chosen by you and their respective values.
3. Explain the information contained in at least one of the packets that relate to task 1 of part A
4. Write down the analysis you completed for task 1 of part B
5. Answer the questions mentioned in task 2 of part B

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.

PIX Firewall provides a graphical user interface to help simplify configuration tasks. Once you have specified the network interface speed and IP addresses (as described in the last section), you need to enter two additional commands and you can then use a network browser, such as Netscape, to complete the configuration. To access PIX Firewall from a network browser, enter these commands to specify an access password and your workstation's IP address and network mask: pixfirewall(config)# passwd access_password. pixfirewall(config)# http ip_address network_mask.