

# CS393/682 - Network Security - Lab Assignment 6

## IPSEC and VPN

### Summary:

In this Lab you will learn how to set up VPN tunnels using IPSEC. IPSEC could be used in several ways and one can set up multiple tunnels to achieve maximum security. In this Lab you will explore these properties and set up a tunnel between two hosts in different network. To do this you need to cooperate with another team of your choice.

### Pre-Lab:

Download and install IPSEC in your machines. To configure it read the documents:

- [http://www.freeswan.org/freeswan\\_trees/freeswan-1.3/doc/index.html](http://www.freeswan.org/freeswan_trees/freeswan-1.3/doc/index.html)
- <http://www.snort.org/docs/SnortUsersManual.pdf>
- [http://www.snort.org/docs/writing\\_rules/](http://www.snort.org/docs/writing_rules/)

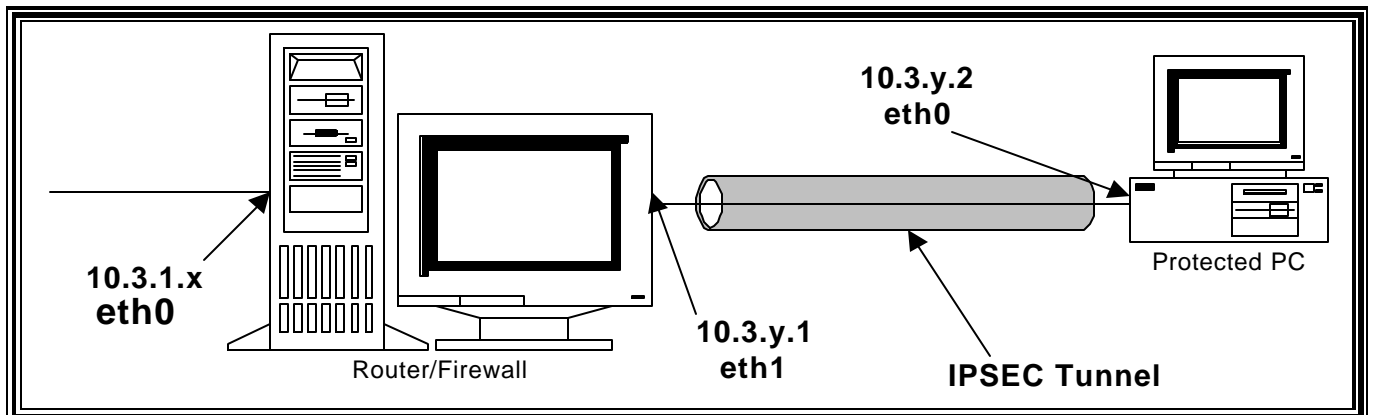
### Lab Work:

#### Part I:

Answer the following questions:

- 1) What layer or layers of the OSI model does IPSEC provide security? Explain why and how.
- 2) What is the overhead involved in using:
  - a. Just AH
  - b. Just ESP
  - c. ESP and AH
- 3) What are the different modes IPSEC can function?
- 4) Explain how IPSEC's authentication and confidentiality mechanisms work?
- 5) Explain a scenario where IPSEC is more effective than using an application level security protocol?
- 6) Explain a scenario where using IPSEC is inefficient?
- 7) Compare and contrast IPSEC to SSL?

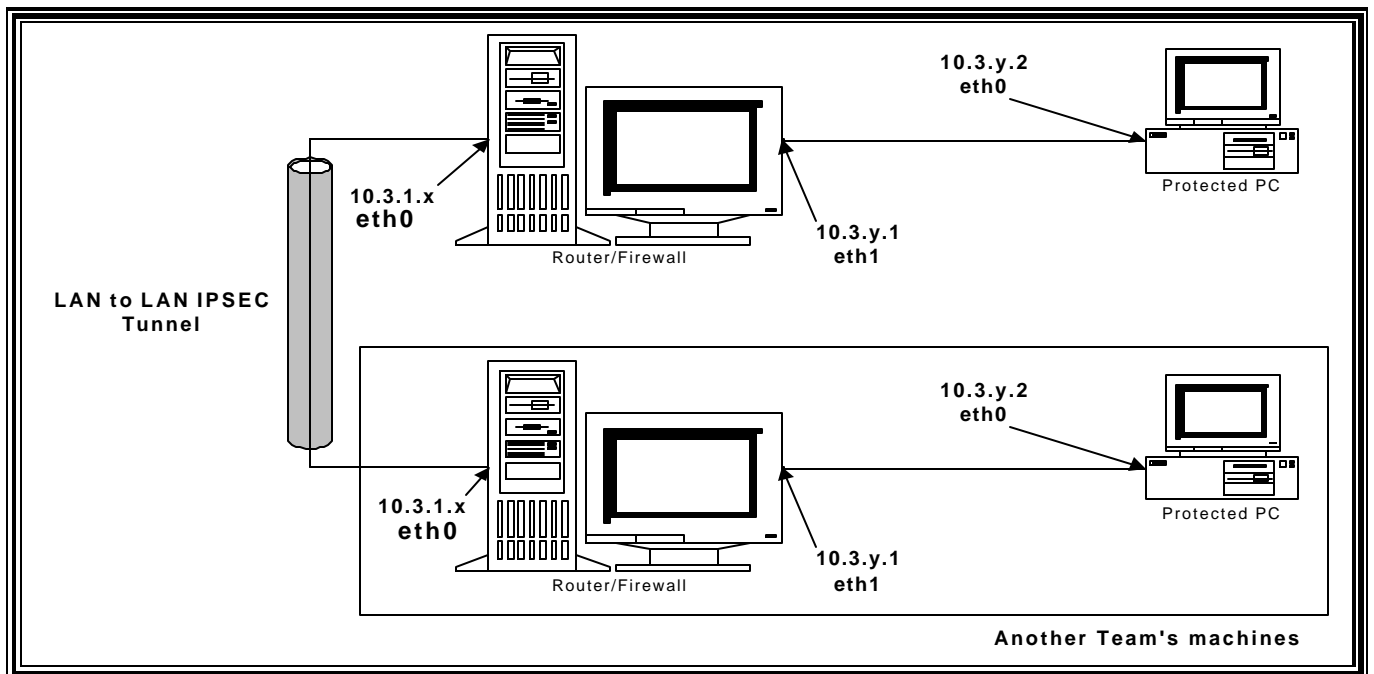
#### Part II:



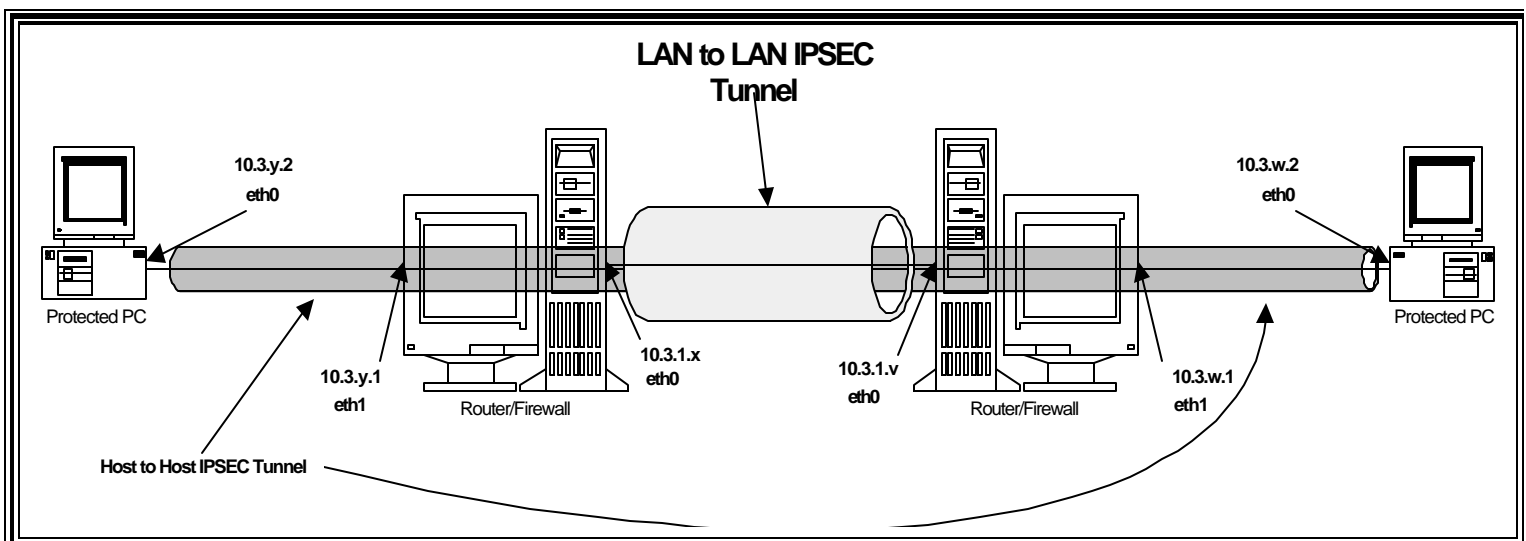
Setup a tunnel between the protected server and your firewall. You must test your tunnel using minisniff that you extended in lab-03 (by checking whether the traffic between the machines are encrypted or not) and include a screen shot or output (sniffed data) to prove that you did setup the tunnel properly. You must also include your configuration file in your report. You are allowed to use secret key authentication instead of RSA

### Part III:

Setup a tunnel between your firewall and another team's firewall. See the figure in the next page. You can use secret key authentication for this part too, which means you'll have to share the keys with the other team. Again you must test your tunnel using minisniff and include a screen shot or output (sniffed data) to prove that you did setup the tunnel properly.



### Part IV:



Finally, setup a tunnel between your protected server and the other teams protected server. You can use secret key authentication for this part too, which means you'll have to share the keys with the other team. Again, you must test your tunnel using minisniff and include a screen shot or output (sniffed data) to prove that you did setup the tunnel properly. In your report explain how you did this and please include your configuration file. (ipsec.conf- only the part where you modified)

### **What to Handin?**

- Answers for question in Part I.
- Explain the steps you took to set up Part II
- Explain, in general, how you configured and setup IPSEC tunnels in part III and IV. Also include your configuration file in your report. (ipsec.conf- only the part where you modified) you used in each part.