CS 646 – Spring 2018

Project 3 (due April 24 @ 6:00pm)

For any questions regarding the assignment, please email the instructor at rr8@njit.edu

This lab will help you learn basic configuration of a firewall and a VPN.

Deliverables:

1. A report in **PDF** format

   Your report should:

   - Document your configuration with screenshots
   - Provide justification for why you configured your devices in a particular way
   - Provide proof that your configuration meets the requirements with screenshots & packet traces

Each task will be worth 25 points. Collaboration via the forum is encouraged for this project. Students are welcome to discuss all aspects of this project with their classmates. There is a tremendous amount of information about pfSense on the Internet. Students are free to post relevant articles & videos that will be valuable in completing the project.

Task 1 – Basic Configuration:

Download and install two instances of pfSense in a virtual environment (https://www.pfsense.org/download/)

Download and install two instances of your favorite Linux distribution in a virtual environment

The server should have a web server and SSH server installed and operational

Configure the virtual networks and associated network interfaces as per the diagram

Task 2 – Basic Security Configuration:

Configure access rules on both firewalls so that the client can connect to the server on TCP/80 but cannot access SSH. (If you don't have a GUI installed on the Client, you can use Lynx)

Configure access rules on the Site B Firewall to that no unsolicited connections can be made from the Server network to the Client network.

***Note**: the client and server will be able to communicate because we are using a private address range for the outside network (e.g. the "Internet"). In the "real world" the ISP would refuse to carry the packets from either site because they are using RFC1918 private IP addresses. To make this work, we need to configure NAT.

Task 3 – Basic Network Address Translation (NAT) Configuration:

Configure NAT rules on the site A firewall so that packets from the inside interface have their source addresses translated to the IP address of the outside interface. Also configure NAT rules on the site B firewall so that the server is "published" to the IP address of the outside interface. That is, the client will now be connecting to port 80 of the IP address of the outside interface of the site B firewall, not the server's IP. Remember, in the real world, the client network and the server network use private IP addresses. The server won't be reachable and therefore will need to have its IP address mapped to an IP address that is routable on the Internet. Show a packet trace from the server that shows that arriving packets have the source address of the outside interface of the site A firewall and not the address of the client. Show a packet trace from the client that shows an established connection HTTP connection to the site B firewall's outside interface.

Task 4 – Basic Site-to-Site VPN Configuration:

Modify your configuration so that both the client network and the server network can communicate using IPsec. That is, establish a VPN tunnel between the site A and site B firewalls. Communication between the client and server should be carried through this tunnel. Use the strongest available security settings for both security associations. Provide screenshots and packet traces to prove that your VPN is operating properly.