INFOTC 3001 - Computer Network Security
Laboratory # 9 - Virtual Private Network (Linux)

I. Objectives

Set up a Virtual Private Network on Centos 7 using OpenVPN, RSA 3.0 and Firewalld.

II. Material Required

Desktop Virtualization Software (VMware Workstation/Fusion) and CentOS.

III. Activity

1. Go through the material in 'Module #6 VPNs' on Canvas.
2. Make sure CentOS has 2 network adapters, one connected to the Internet Through NAT, and the other one connected to VMnet2 (or private to my network).
3. Update your CentOS system and install OpenVPN packages, then create a clone of the system.
4. CentOS and CentOS CLONE interfaces connected to VMnet2 should have different IP addresses, make sure they can reach (ping) to each other to verify connectivity.
5. Configure OpenVPN in the server and client. **Use the range of 172.20.20.0/24** for the VPN IP addresses (tip: configure the server.conf file).

IV. Review Questions

Take screenshots for the following review questions.

1. After the OpenVPN is installed and configured in the SERVER succesfully execute the `$sudo systemctl start openvpn@server.service` command, type your pawprint in the command line and take a screenshot.
2. In the SERVER type `ifconfig` showing the new virtual network interface created by the VPN, type your pawprint and take a screenshot.
3. After the OpenVPN is installed and configured in the CLIENT succesfully, execute `$sudo openvpn --config client.ovpn` (take a screenshot).
4. From VPN SERVER ping the VPN CLIENT using the VPN IP addresses.