

IT357 Tools and Techniques in Defensive Security
Assignment 4 – OpenVPN Configuration
10 Questions – 40 Points

Objective: To implement a remote access VPN connection using OpenVPN to provide an encrypted channel to the organization's LAN.

Preparation:

For this assignment, you will use the Ubuntu-LAN VM, Win10-WAN VM, and the pfSense Web-UI Console.

Check that your power settings on the Win10 VM is set to "NEVER".

Scenario:

You are administering an organization who has a remote office/mobile office worker who needs access to the internal private network to carry out job related tasks. Since the remote connection goes through the untrusted public Internet, we will need to create a secure channel for this connection using VPN technology, in addition to providing appropriate access to internal resources.

Setup steps for the scenario

To install the required software for this assignment:

1. Install the **OpenVPN Client Export** package on the pfSense firewall.
 - a. From the Ubuntu-LAN VM, open the pfSense Web UI at <https://192.168.1.1> from a web browser. Then navigate to **System→Package Manager** and click on the **Available Packages** tab.
 - b. Scroll down the list and click the **Install** button for the *openvpn-client-export* package. Click the **Confirm** button on the following page to proceed with the installation.
2. Record required IP addresses:
Ubuntu-LAN IP address: 192.168.1.189
pfSense WAN interface IP address: 10.111.22.184
3. Install Telnet and test Telnet on Ubuntu-LAN VM:
 - a. Open the terminal in the Ubuntu-LAN VM and issue the following commands.
 - i. `sudo apt update -y`
 - ii. `sudo apt install telnetd -y`
 - iii. `sudo systemctl status inetd`
 - b. Then check to see that port 23 is active with the following command
 - i. `ss -tnlp`
 - ii. The local address:port column should show 0.0.0.0:23 as LISTEN
 - c. Now let's add a user, "vmtelnet" for the telnet terminal logon.
 - i. `sudo adduser vmtelnet`

- ii. Answer the questions for password and just hit “enter” for the remaining questions. May I suggest you use the password “ab12cd34”, then you won’t need to remember a different one.
- d. You can now test the telnet by
 - i. `telnet localhost`
 - ii. and you can logon with the vmtelnet user and password “ab12cd34”.
- e. Verify this works before moving on.

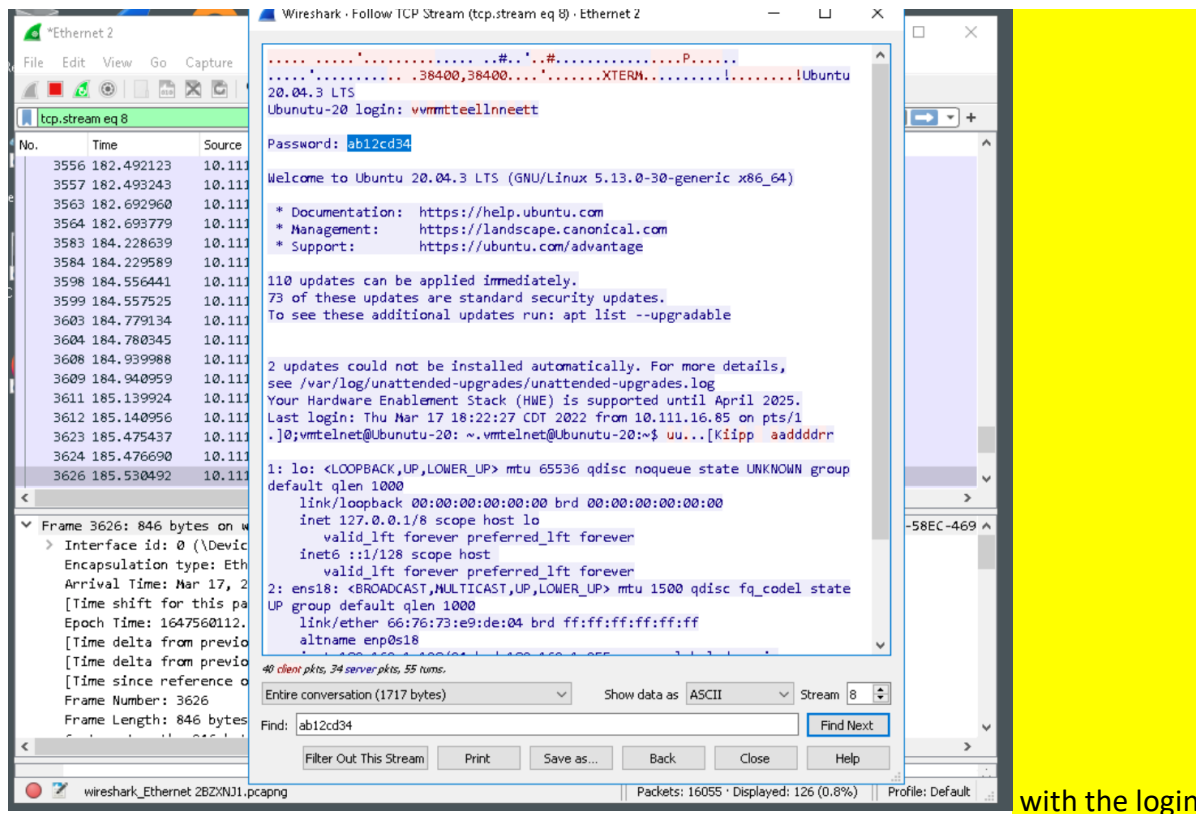
Telnet and unencrypted traffic

One of the benefits of using a VPN to connect two endpoints is the confidentiality aspect of VPNs and its ability to encrypt traffic. You will first emulate an eavesdropping attack and see how plaintext protocols such as Telnet are prone to eavesdropping attack.

- 1) Create a port forwarding rule to forward Telnet (TCP port 23) protocol to the Ubuntu-LAN VM on the pfSense firewall. Note: don’t forget to “Add Associated Filter Rule” then “apply” any changes.
- 2) Open Wireshark on the Win10-WAN VM and double click the Ethernet interface to start listening to the network traffic. Apply the filter “tcp.port == 23” in the display filter box, without the quotes.
- 3) Open Putty on the Win10-WAN VM and use it to Telnet to the pfSense WAN interface IP address. Use the Ubuntu-LAN “vmtelnet” credentials to login to the machine remotely. Note: if you don’t get the login prompt, go check your pfSense firewall rule. You can’t proceed until you get the login.
- 4) Stop the Wireshark capture on the Win10-WAN VM. Locate the first packet in the capture window. Right click and select Follow→TCP stream. A new window will open and allow you to see the contents of the packet payloads of the session.

Q1) Locate the Login and Password lines in the window to see the login credentials. (3 pts)

[Insert a screen shot showing Wireshark



credentials here.]

Now that you've seen how cleartext protocols are vulnerable to eavesdropping attacks, eliminate this threat by creating an encrypted SSL tunnel between the machines. You will first configure the OpenVPN server on pfSense, followed by the OpenVPN-GUI client on Win10-WAN VM.

OpenVPN Server configuration

OpenVPN is an SSL based VPN service that allows remote networks or wireless clients, such as laptops, to connect to pfSense. Connections will then be forward to the appropriate internal resources as permitted by the firewall rules.

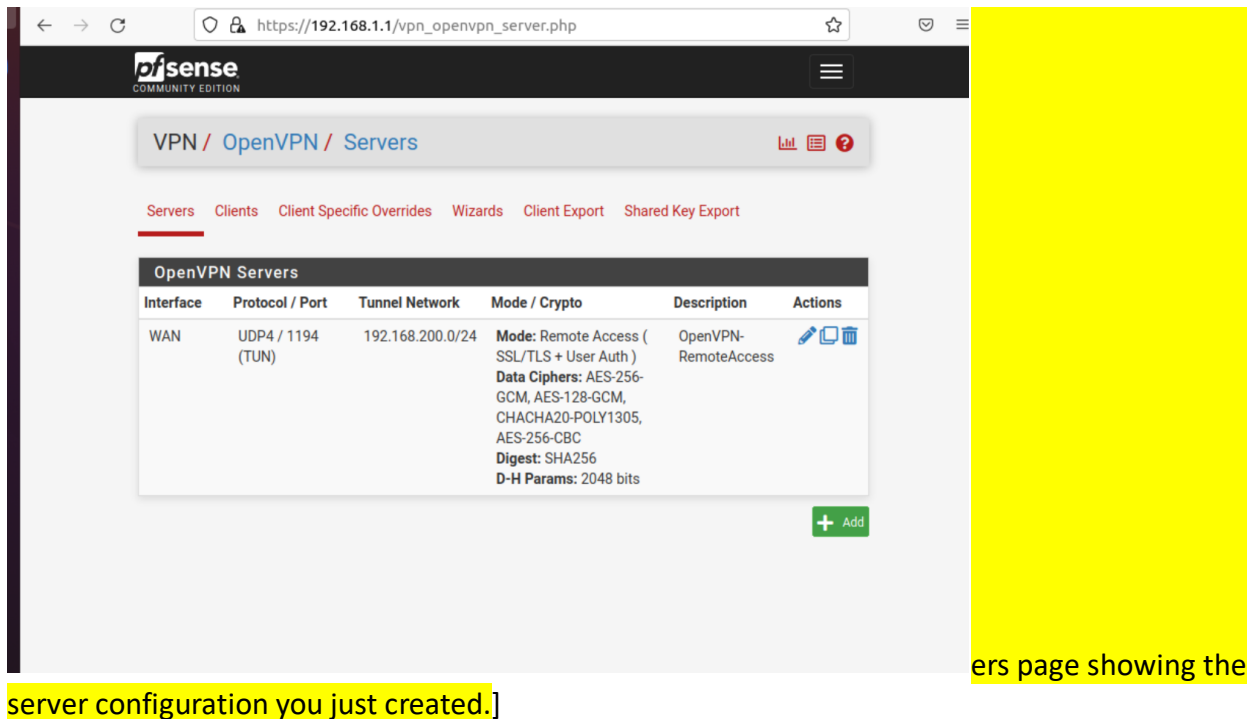
- 1) Go to the pfSense web console. Navigate to **VPN→OpenVPN** and click on the **Wizards** tab. Under the *Select an Authentication Backend Type* section, be sure that **Local User Access** is selected for Type of Server and click **Next**.
- 2) On the next page, we will essentially be creating a certificate that declares the pfSense firewall to be a valid Certificate Authority that has the ability to create and sign certificates. Under the *Create a New Certificate Authority (CA) Certificate* section, use "pfSense-CA" for the **Descriptive name**. For the **Organization**, enter "ISU" and click the **Add new CA** button on the bottom of the page.
- 3) The following page leverages the firewall's new authority as a CA to create a certificate

for the OpenVPN server. Here, for the **Descriptive name** use “pfSense-OpenVPN”. Leave the other fields at their defaults and click on the **Create new Certificate** button at the bottom of the page.

- 4) The first two pages of the OpenVPN wizard were first setting up the necessary certificates for the server. The page we find ourselves on now, begins the configuration of the actual OpenVPN server. In the *General OpenVPN Server Information* section enter “OpenVPN-RemoteAccess” for the **Description**.
- 5) The **Tunnel Network** under the *Tunnel Settings* refers to the subnet that will be used to allow communication between the clients and the OpenVPN server. Therefore, this will also represent the IP addresses that will be assigned to the TUN/TAP virtual network adapters created by the remote client once a VPN tunnel is established. In our case, for **Tunnel Network** use “192.168.200.0/24”. The Local Network is the network that we want to allow the remote user to access over the VPN. In our case we will want the remote user to access the LAN network. Enter the LAN’s subnet, “192.168.1.0/24”, for the **Local Network**. Leave the remaining settings at their default and click the **Next** button on the bottom of the page.
- 6) On the next page, be sure to **check the boxes** for **Firewall Rule** and for **OpenVPN rule**. These two settings will automatically create Firewall and OpenVPN rules respectively to allow the VPN traffic through the firewall. Click the **Next** button on the bottom of this page and the **Finish** button on the bottom of the next.

Q2) After clicking Finish, you should now be on the VPN/OpenVPN/Servers page on the pfSense firewall. (3 pts)

[Take a screen shot of the OpenVPN Serv



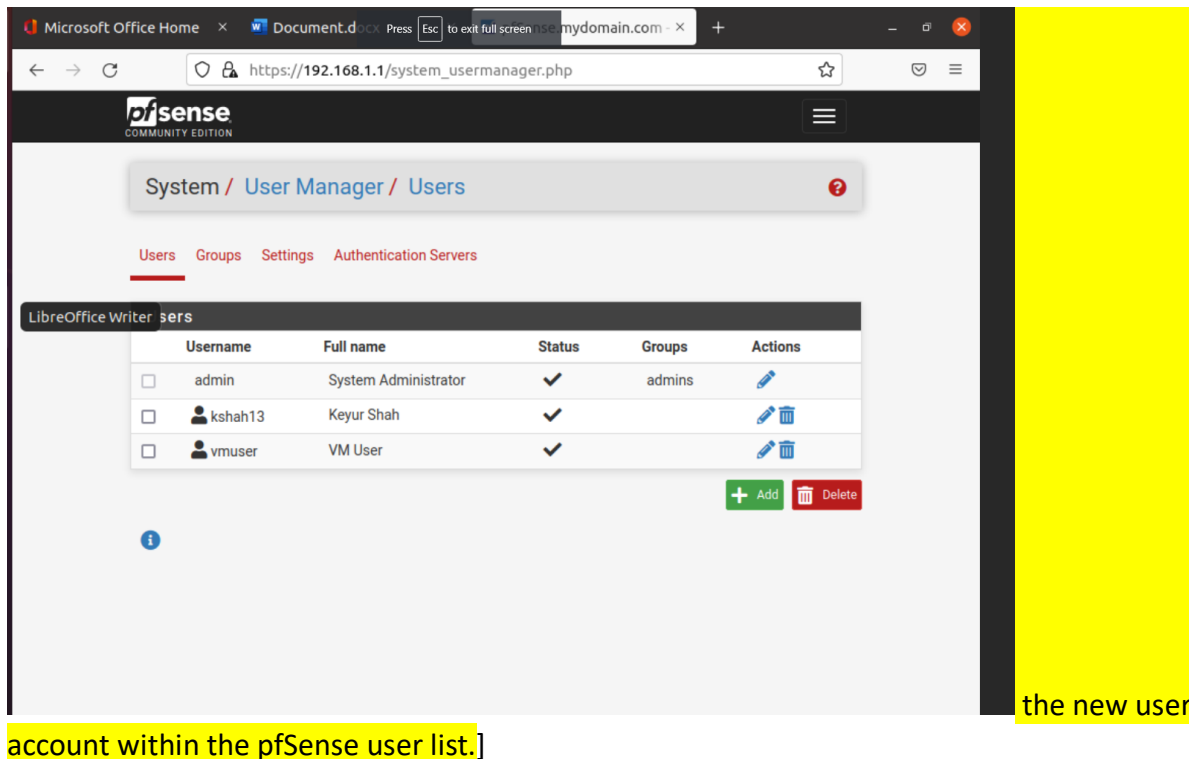
Creating a user

Now that the OpenVPN server is configured, we'll need to create a pfSense local user account that will utilize the newly created remote access VPN.

- 1) Navigate to **System→User Manager**. Be sure that you are on the **Users** tab and click on the green **Add** button. The Edit User page should now be open. Under the *User Properties* section enter your ULID for the **Username**, use "ab12cd34" for the **Password** field, and use your first and last name for the **Full name** field. Be sure to **check the box** for the **Certificate** to create a user certificate for your newly created user account. Under the Create Certificate for User section, use your "ulid-cert" for the **Descriptive name**. (i.e. username-cert or bbob1-cert) Finally, click on the blue **Save** button at the bottom of the page.

Q3) With your new user account created, you should now be back on the System/User Manager/Users page. (3pts)

[Take a screen shot showing



account within the pfSense user list.]

Download the client configuration

Our VPN server is ready to go, our user account has been created, now we just need to download the client configuration file which will contain the necessary settings for our remote user to connect to our server as well as the user certificate for authentication.

- 1) Navigate to **VPN→OpenVPN** and click on the **Client Export** tab. If you do not see the Client Export tab make sure you didn't skip the install of this package at the beginning of the assignment.
- 2) Scroll down to the *OpenVPN Clients* section and find the user name that you just created. To the far right of the screen under the Export column, look for *Inline Configurations*, click on the **Most Clients** button to download the necessary .ovpn file to the default Downloads directory.

Note: If you do not have anything listed in **OpenVPN Clients section**, it is likely that you missed the Certificate checkbox when adding the new user account. You will need to go back to the User Manager, edit the user account, and add a user certificate. Use *username-cert* for the Descriptive name and the *username* for the Common name.

You will now need to copy the file you downloaded onto the Win10-WAN VM, as it is needed for the OpenVPN client configuration. I would recommend using your OneDrive (accessible at <https://office365.ilstu.edu>)

- 1) Using a browser on Ubuntu-LAN, upload the file
- 2) Download the file to the Win10-WAN VM using the same web address to Office365

OneDrive

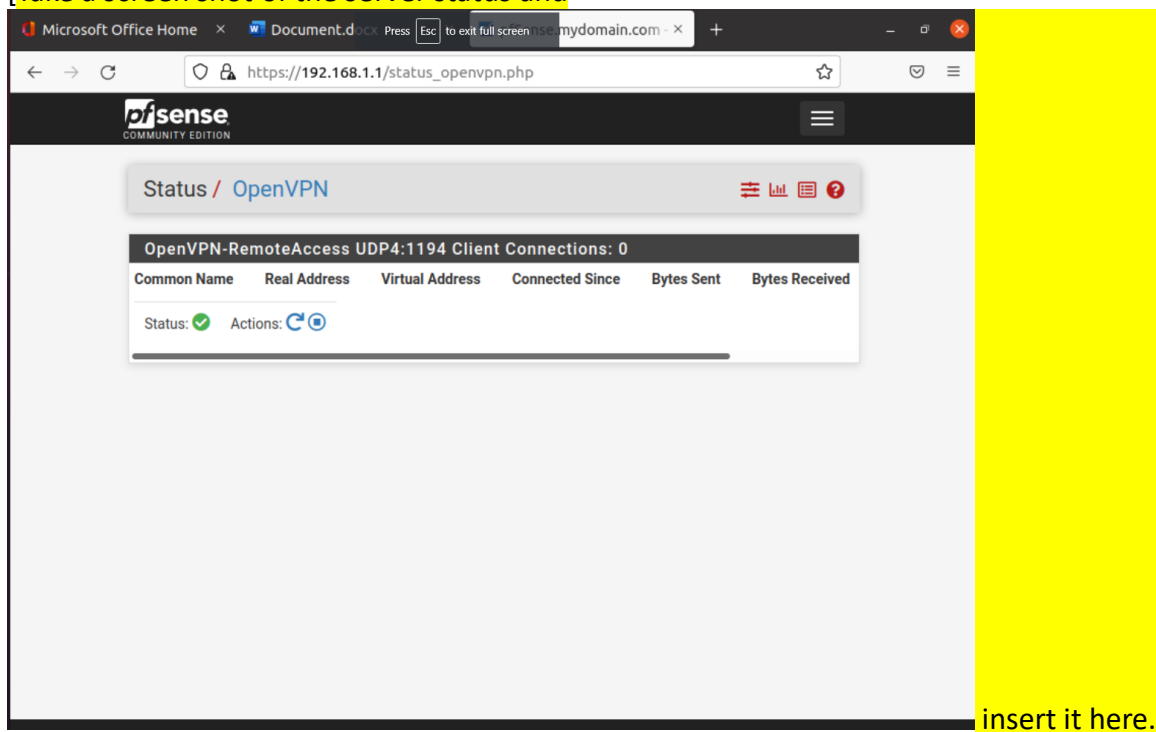
- 3) Once the .ovpn file is downloaded to Win10-WAN, right click on the OpenVPN GUI as shown below and select "Import file...". Navigate to the folder containing the .ovpn file and select it to import the user profile.



Connect the OpenVPN remote client

Q4) Return to the pfSense console on Ubuntu-LAN VM and navigate to **Status**→**OpenVPN** page. Verify that the OpenVPN service is running represented by a green check mark next to Status. (3 pts)

[Take a screen shot of the server status and



Now, back on the Win10-WAN VM:

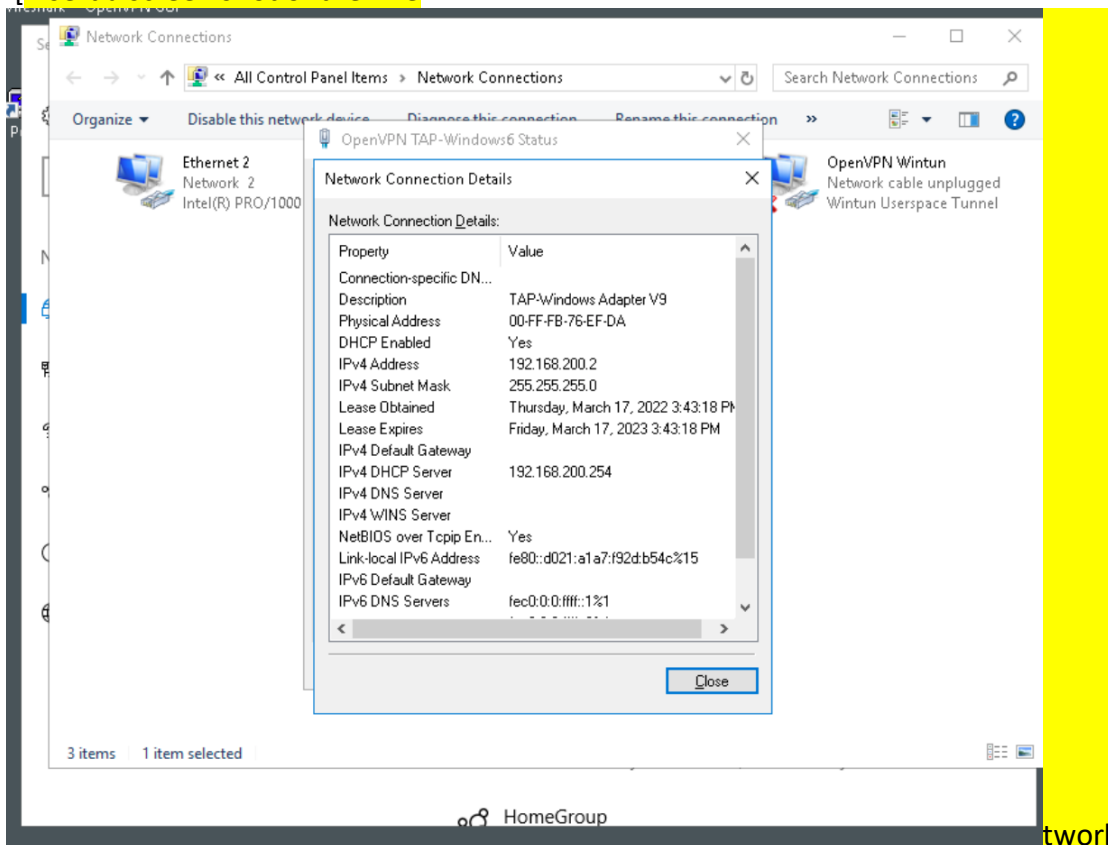
- 1) Did you get the .ovpn file downloaded?
- 2) Right click the OpenVPN GUI icon in the system tray and select "Connect" to start the connection. You will be prompted for the Client profile username and password

("ab12cd34") that was set during the user configuration. The connection process should complete and the OpenVPN GUI color should change to green.

- 3) Open **Network & Internet Settings** by clicking on the network icon on the bottom right corner.
- 4) Click on **Change adapter options** to bring up the Network Connections window containing all of the network interfaces. Double click on the OpenVPN TAP (or TUN depending on which is connected) interface and click on the **Details** button. The "Network connection details" window should open, showing the interface IP address and other details. Is it in the 192.168.200.x subnet?

Q5) The IP address should be from the *Tunnel Network* subnet that was configured earlier during the OpenVPN Server setup. (3 pts)

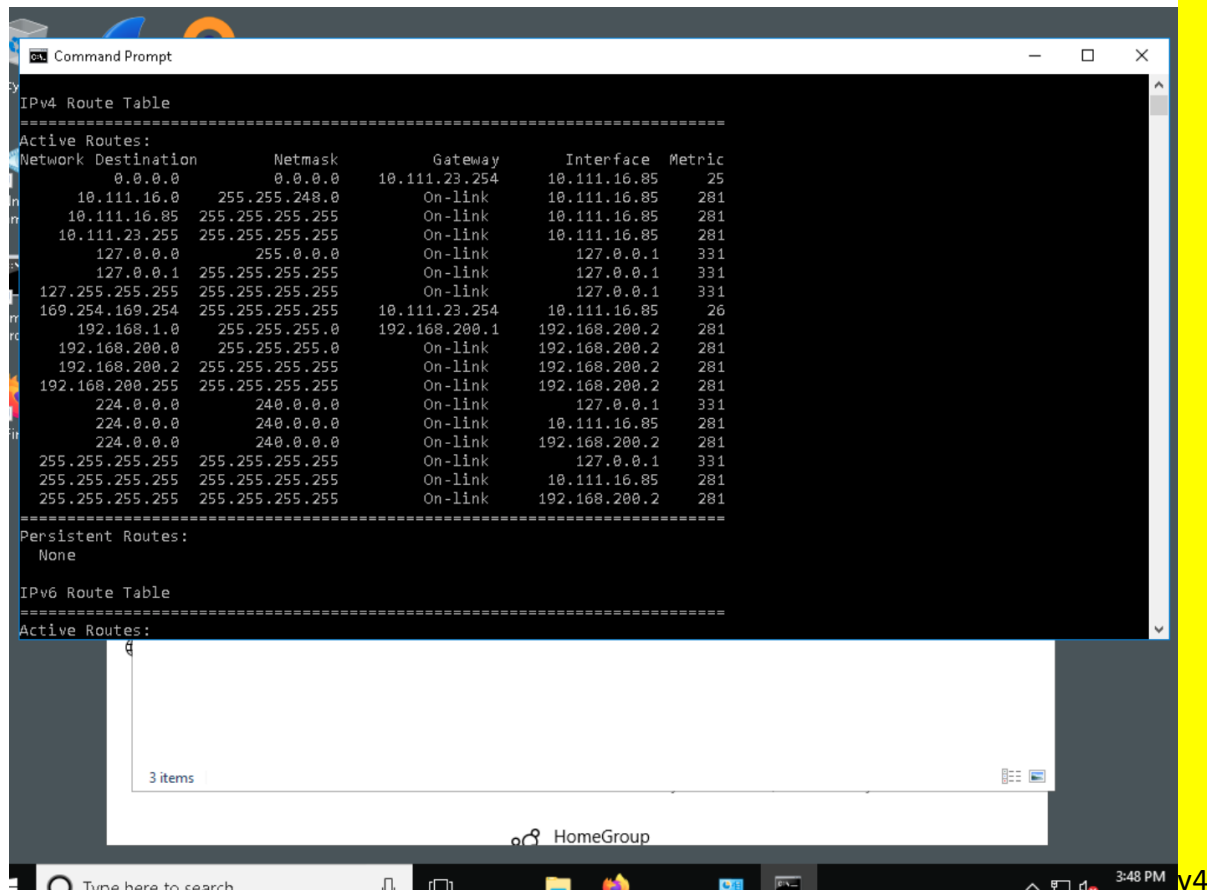
[Insert a screen shot of the "Ne



Connection Details" Window here.]

Q6) Open a command prompt window and type the command "route print" to print the host routing table. Locate the IPv4 Route Table entry for the remote LAN subnet IP address range (192.168.1.0). You may need to scroll up in the window to find it. The Interface column for this subnet should show the IP address of the OpenVPN adapter from the previous task. (3 pts)

[Insert a screen shot of the IP



```
Command Prompt

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.111.23.254    10.111.16.85      25
10.111.16.0                255.255.248.0    On-link          10.111.16.85      281
10.111.16.85               255.255.255.255  On-link          10.111.16.85      281
10.111.23.255              255.255.255.255  On-link          10.111.16.85      281
127.0.0.0                  255.0.0.0        On-link          127.0.0.1         331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1         331
127.255.255.255            255.255.255.255  On-link          127.0.0.1         331
169.254.169.254            255.255.255.255  10.111.23.254    10.111.16.85      26
192.168.1.0                255.255.255.0    192.168.200.1    192.168.200.2     281
192.168.200.0              255.255.255.0    On-link          192.168.200.2     281
192.168.200.2              255.255.255.255  On-link          192.168.200.2     281
192.168.200.255            255.255.255.255  On-link          192.168.200.2     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1         331
224.0.0.0                  240.0.0.0        On-link          10.111.16.85      281
224.0.0.0                  240.0.0.0        On-link          192.168.200.2     281
255.255.255.255            255.255.255.255  On-link          127.0.0.1         331
255.255.255.255            255.255.255.255  On-link          10.111.16.85      281
255.255.255.255            255.255.255.255  On-link          192.168.200.2     281

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:

```

Route Table output from the "route print" command.]

Q7) Return to the OpenVPN Status page on Ubuntu-LAN VM. If you are already on this page and there has been no change, you may need to refresh your browser. The connected user should now be listed under Common Name along with the remote user's IP Address and virtual adapter address. (3 pts)

[Take a screen shot showing the OpenVPN s

The screenshot shows the pfSense web interface at the URL `https://192.168.1.1/status_openvpn.php#`. The page title is "Status / OpenVPN". Below the title, there is a table titled "OpenVPN-RemoteAccess UDP4:1194 Client Connections: 1". The table has six columns: "Common Name", "Real Address", "Virtual Address", "Connected Since", "Bytes Sent", and "Bytes Received". The table contains one entry for a client named "kshah13" with a real address of "10.111.16.85:49231" and a virtual address of "192.168.200.2". The client has been connected since "2022-03-17 21:00:24", has sent "4 KiB" of data, and received "12 KiB". Below the table, the status is "Status: ✓" and there are "Actions: ↺ ⚙". At the bottom, there is a button "Show Routing Table" with a tooltip that says "Display OpenVPN's internal routing table for this server."

status and
connected user information.]

Q8) Disable the “Telnet” port forwarding rule on pfSense and click **Apply Settings** to apply the changes. Carry out the Telnet Wireshark packet capture again however, this time **use the actual Ubuntu-LAN IP address** (the 192.168.1.x address) to Telnet to, not the pfSense WAN interface that we used at the beginning of the assignment. The connection should complete, and you should be able to login to the Ubuntu-LAN VM using the “vmtelnet” credentials you created earlier. However, you should NOT see any Telnet packets in the Wireshark trace this time. (3 pts)

[Insert a screen shot showing **both** the active Putty telnet session and the blank Wireshark window showing no Telnet packets here.]

Thought Questions:

9. Where did the Telnet packets go in the last task and why are they no longer visible in the Wireshark packet capture? (3 pts)

because we disable NAT port forwarding and we using direct LAN address that's why packets no longer using port 23 and we can not see any package which is using port 23 in Wireshark.

10. Give two differences between SSL based VPNs and IPSEC based VPNs. (3 pts)

IPsec VPN works at layer 3 while SSL VPN works between layer 4-7.

IPsec VPN need host-based clients and SSL VPN based on browser with optional thin client.

SAVE THIS AS A PDF, SUBMIT ON REGGIENET