JW4158-INFO8580-22S-Portfolio-3

John White

6714158

INFO8580

Table of Contents

Lab 5 – Host to Network (Roadwarrior) IPSEC VPN

Description

The purpose of this lab is to teach us how to configure a “Roadwarrior” (host to network) VPN using the IPsec protocol on a pfSense router.

Preparation

To prepare for this lab, we need a pfSense router with a Windows desktop connected to it. We will also need the server to have a certificate authority and an endpoint certificate created by that authority. Refer to the previous portfolio for detailed instructions on this.

Observations

Go to VPN > IPsec and then go to the Mobile Clients tab. Modify the settings as shown in Figure 1.1 and 1.2. Next, create the Phase 1 definition for the VPN. Either click the button that appears at the top or go to the Tunnels tab and add one there. Configure the settings as shown in Figure 1.3, 1.4, and 1.5. Then save settings, add a phase 2 entry, and configure it according to Figure 1.6. Once both phases are configured, we need to add a Mobile Ipsec User profile that our remote host can use for authentication. Go to VPN > IPsec and go to the ‘Pre-Shared Keys’ tab. Add a new entry give it a username and password. Next, we need to add a firewall rule to allow traffic from our VPN tunnel though to our router. Go to Firewall > Rules and then go to the IPsec tab. From there, create a new rule as shown in Figure 1.6, be sure to allow traffic from the virtual address that we specified earlier in our mobile client settings. We must also disable the default Firewall rules that block private and bogon networks as shown in Figure 1.8 and 1.9 Our router should now be configured.

To test our router configuration, we will need to set up another machine as a Mobile Client. I will use a Windows 10 desktop for this. First export the certificate authority and import it to the mobile client. Open the .cert file with the Crypto Shell Extensions and install the certificate in the location shown in Figure 1.10. Next go to Network & Internet Settings and under VPN, create a new connection and configure it as shown in Figure 1.11.

Screenshots

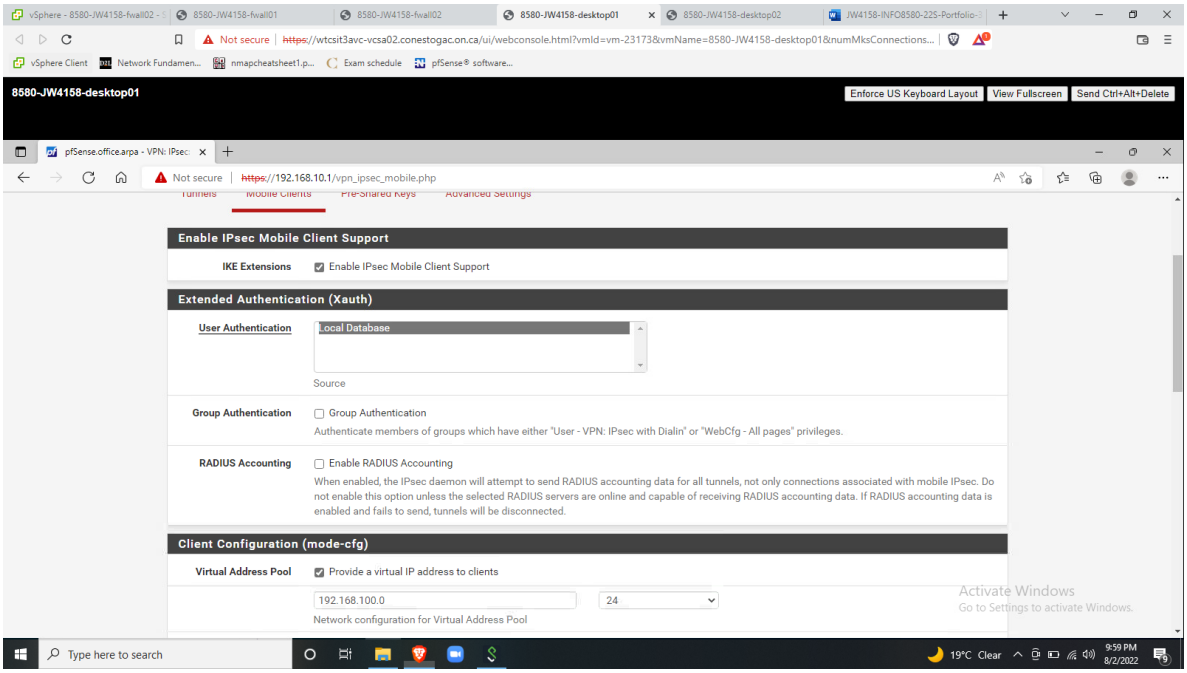

Figure 1.1 - Mobile client settings part 1

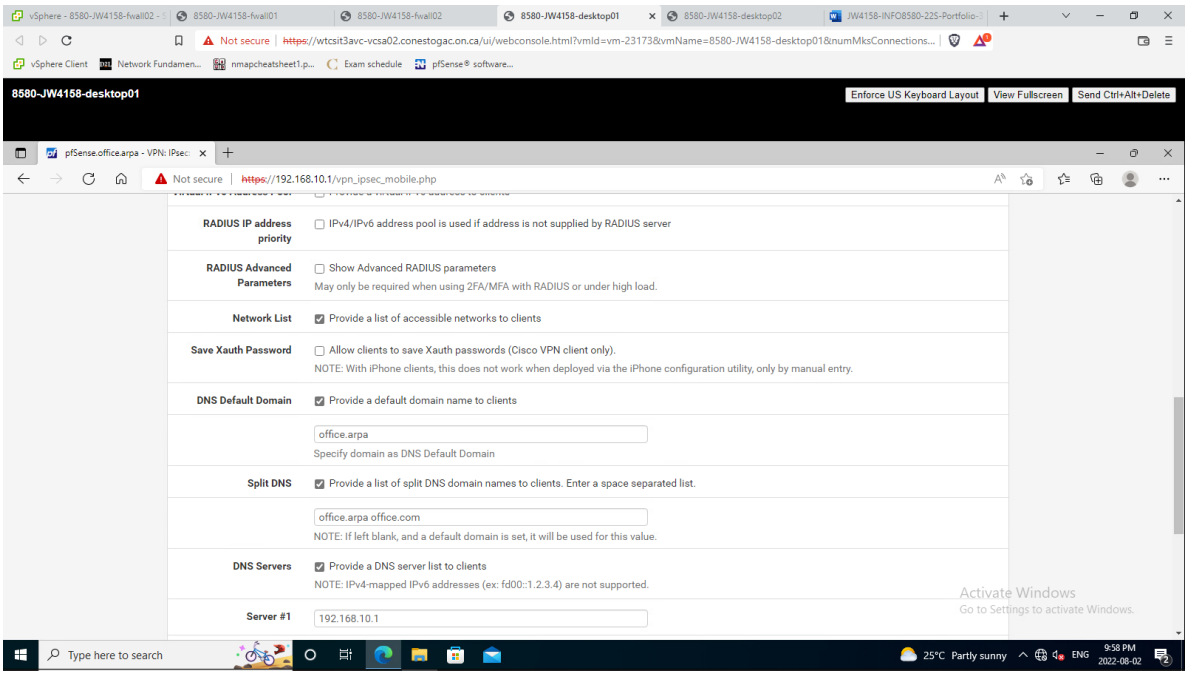

Figure 1.2 - Mobile client settings part 2

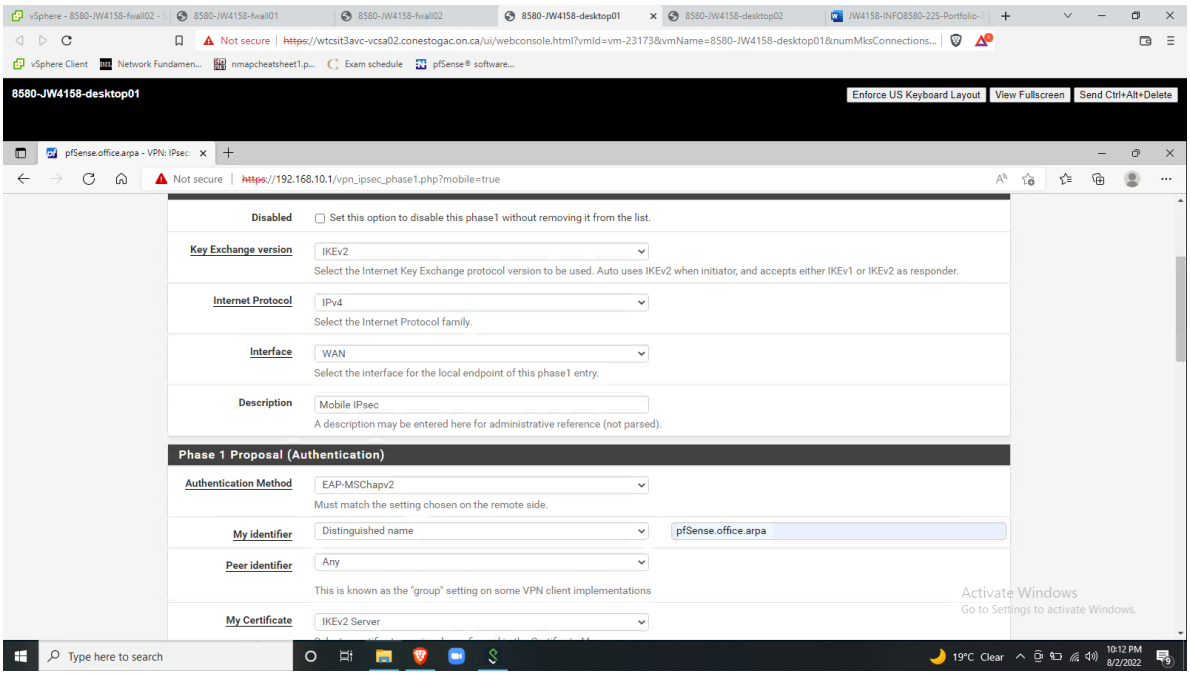

Figure 1.3 - Phase 1 settings part 1

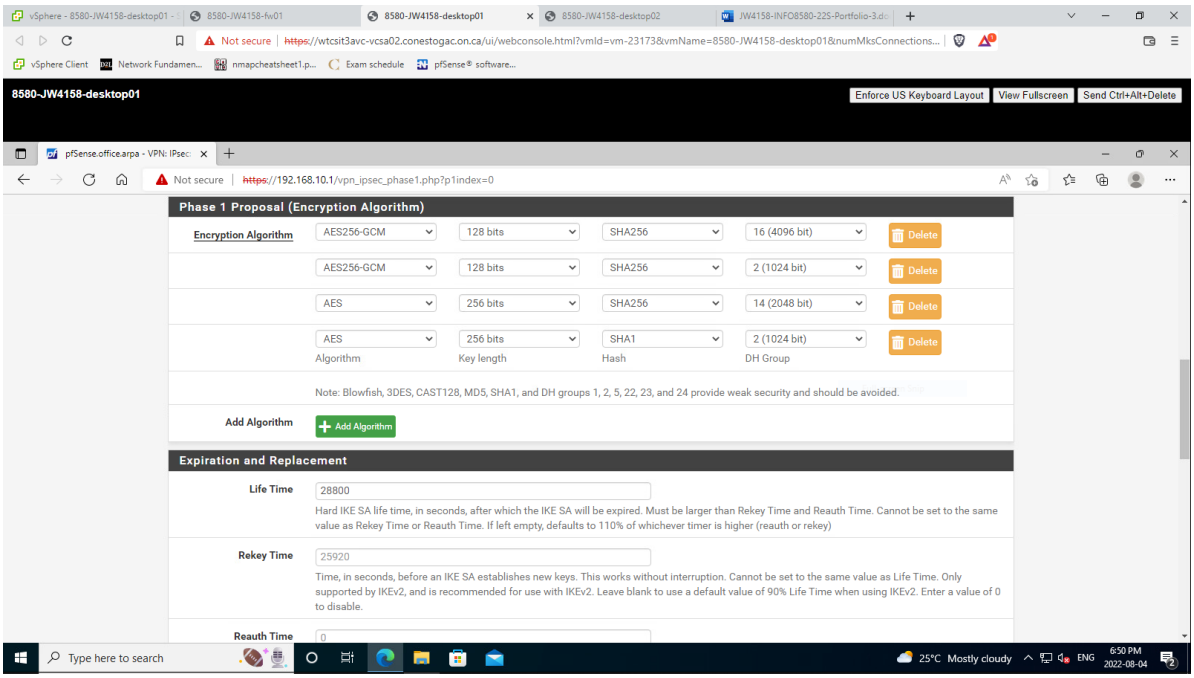

Figure 1.4 - Phase 1 settings part 2

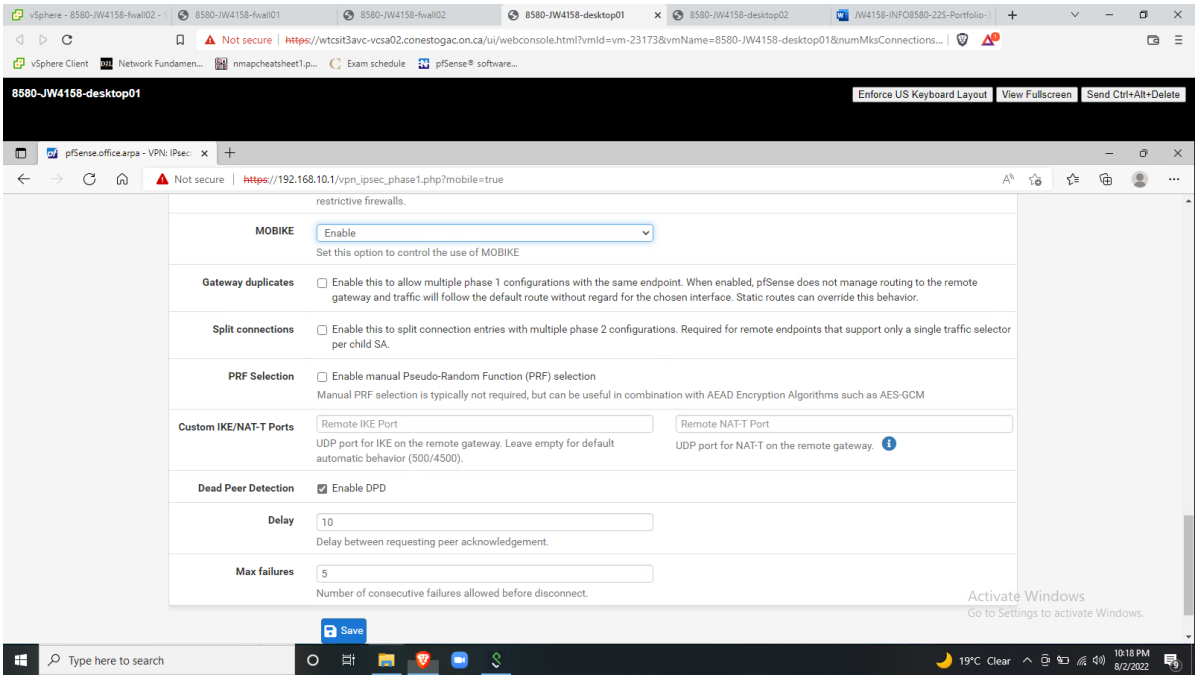

Figure 1.5 - Phase 1 settings part 3

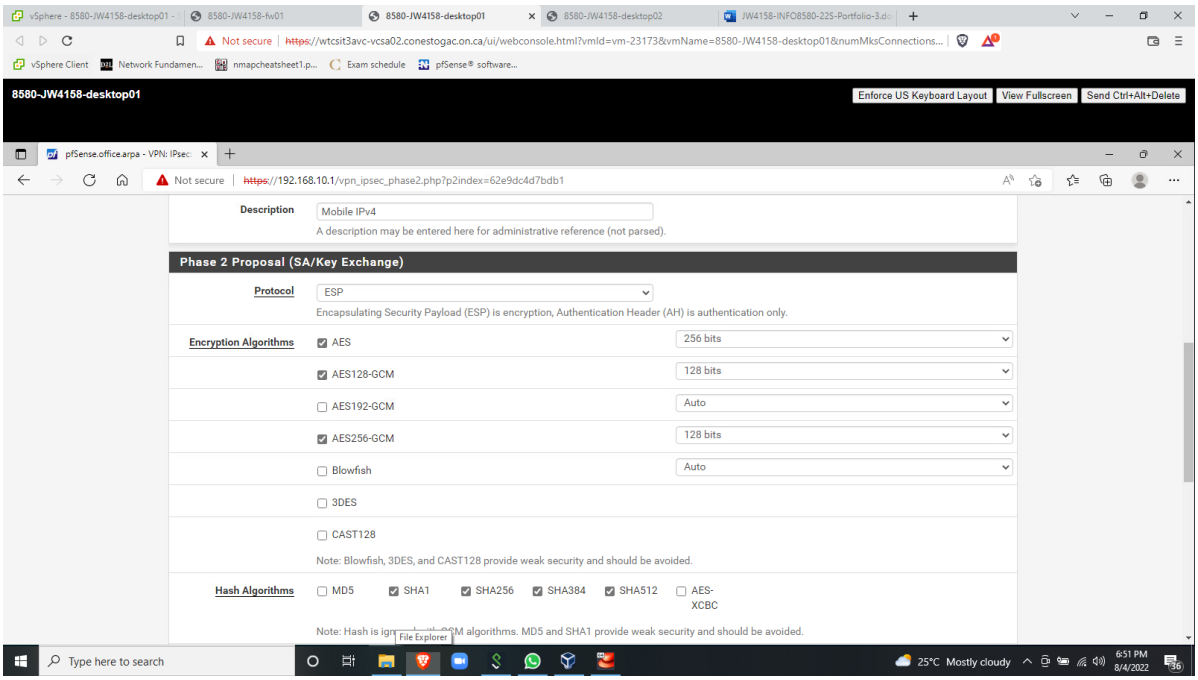

Figure 1.6 - Phase 2 settings

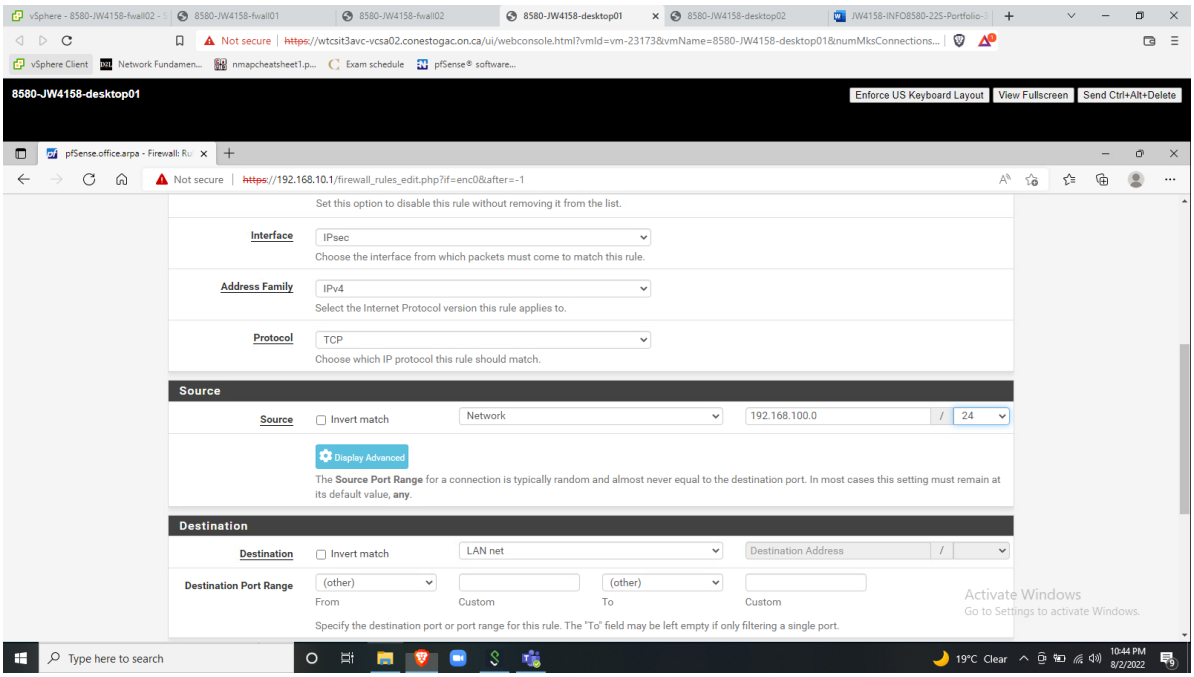

Figure 1.7 - Adding the firewall rule

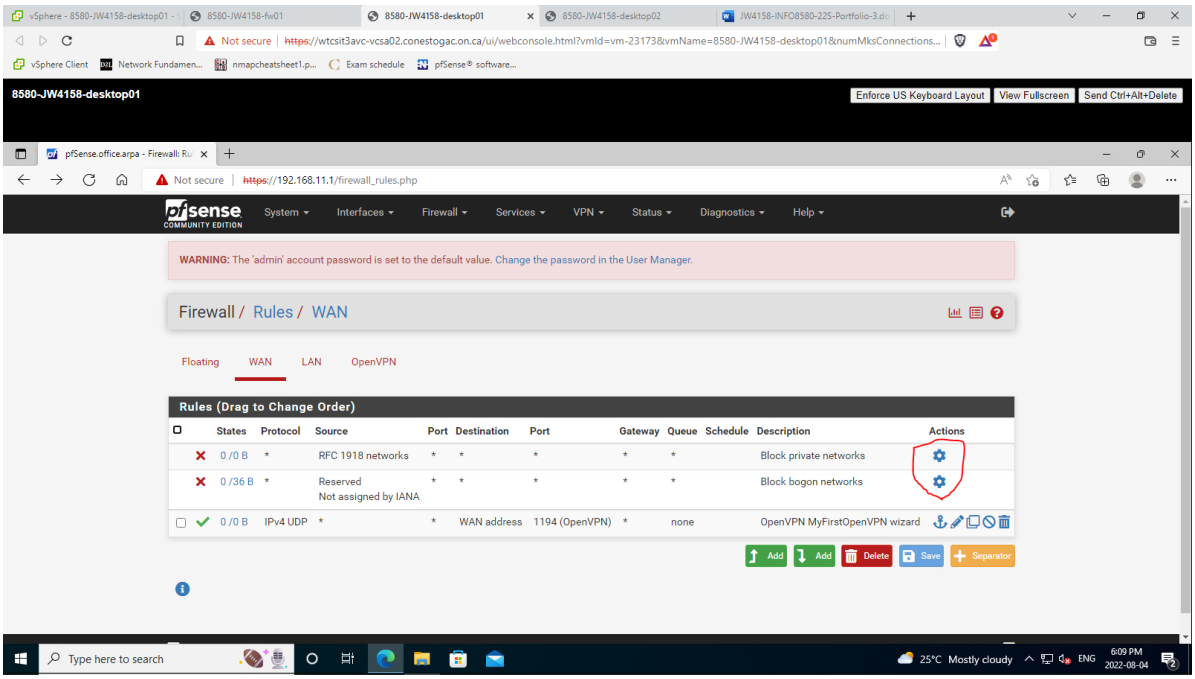

Figure 1.8 - Enabling private and bogon networks part 1

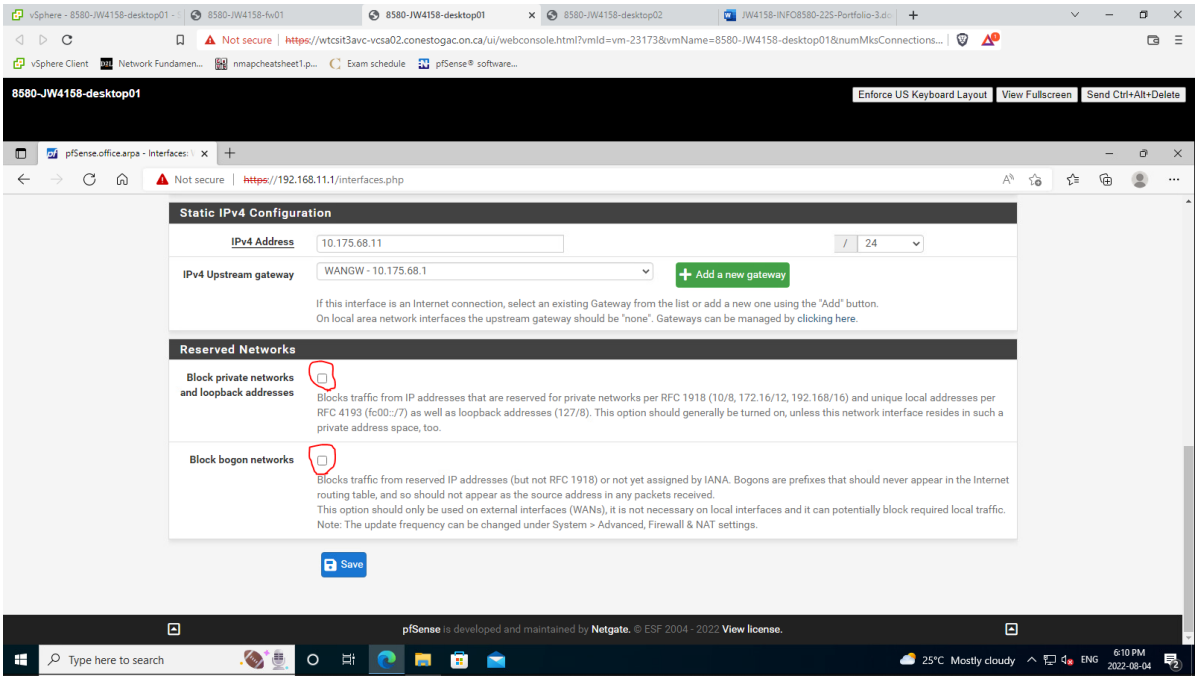

Figure 1.9 - Enabling private and bogon networks part 2

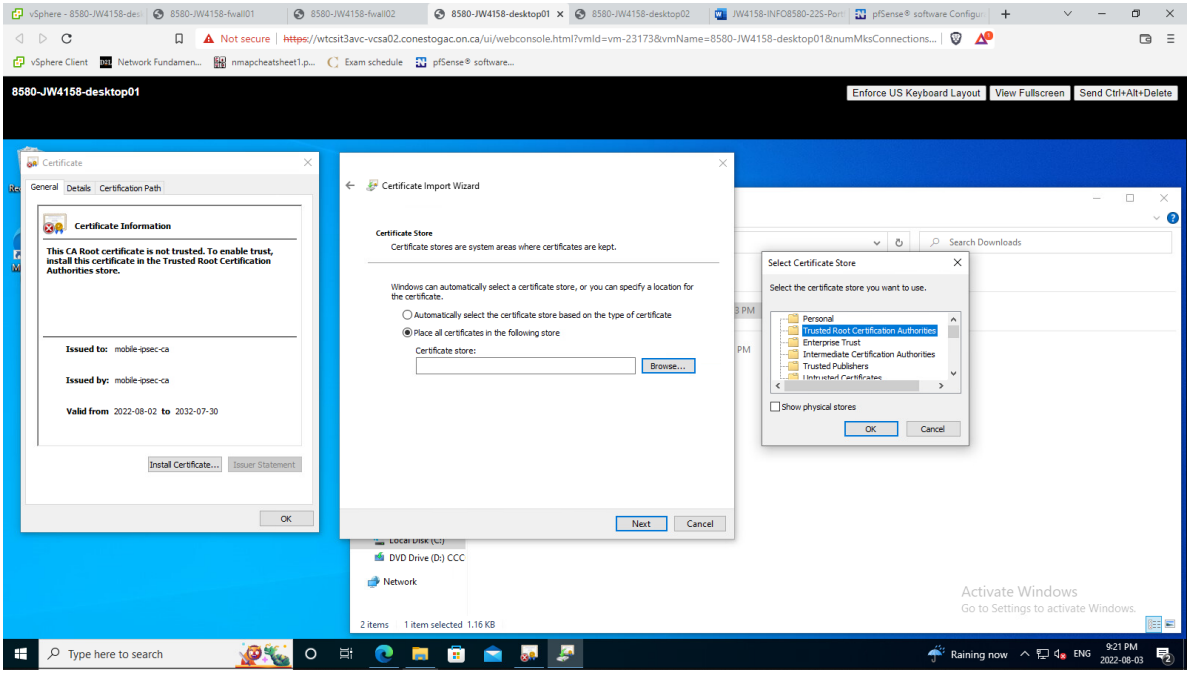

Figure 1.10 - Certificate Installation

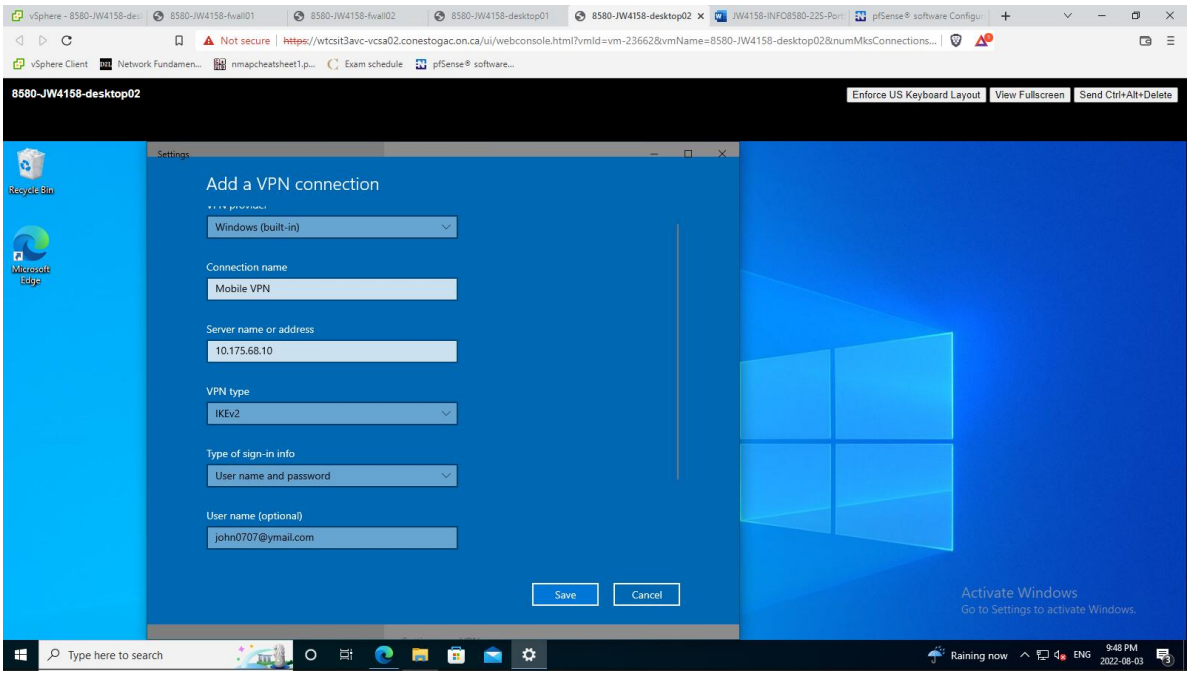

Figure 1.11 - VPN connection settings

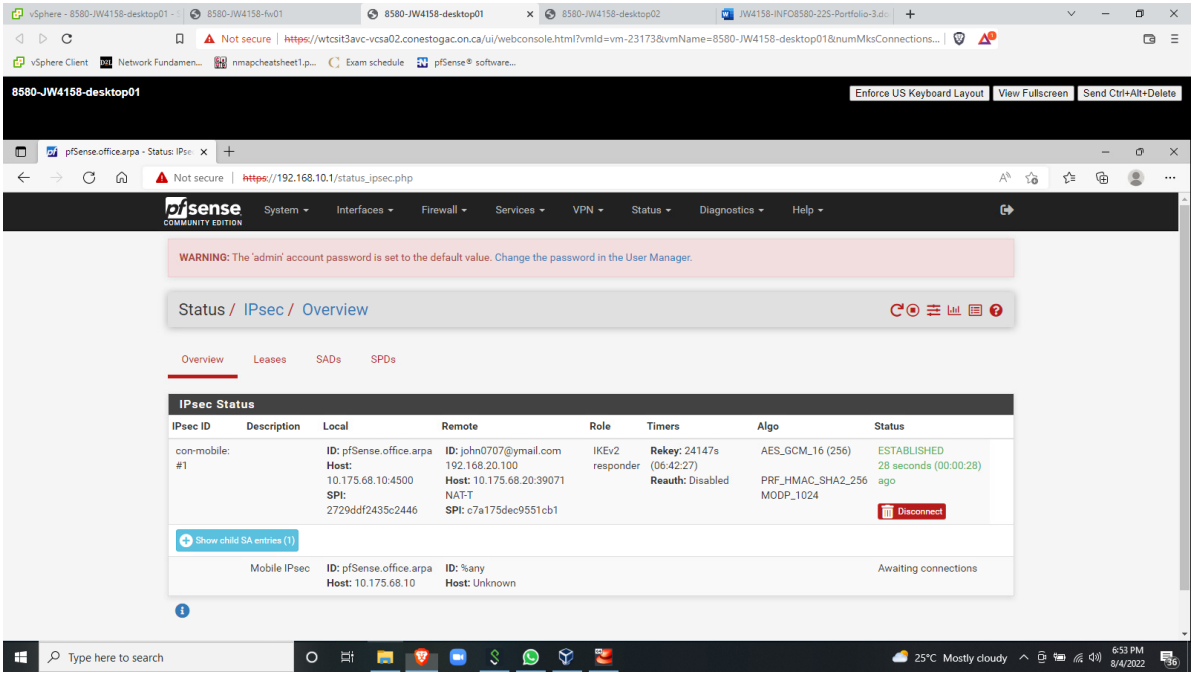

Figure 1.12 - Successful connection

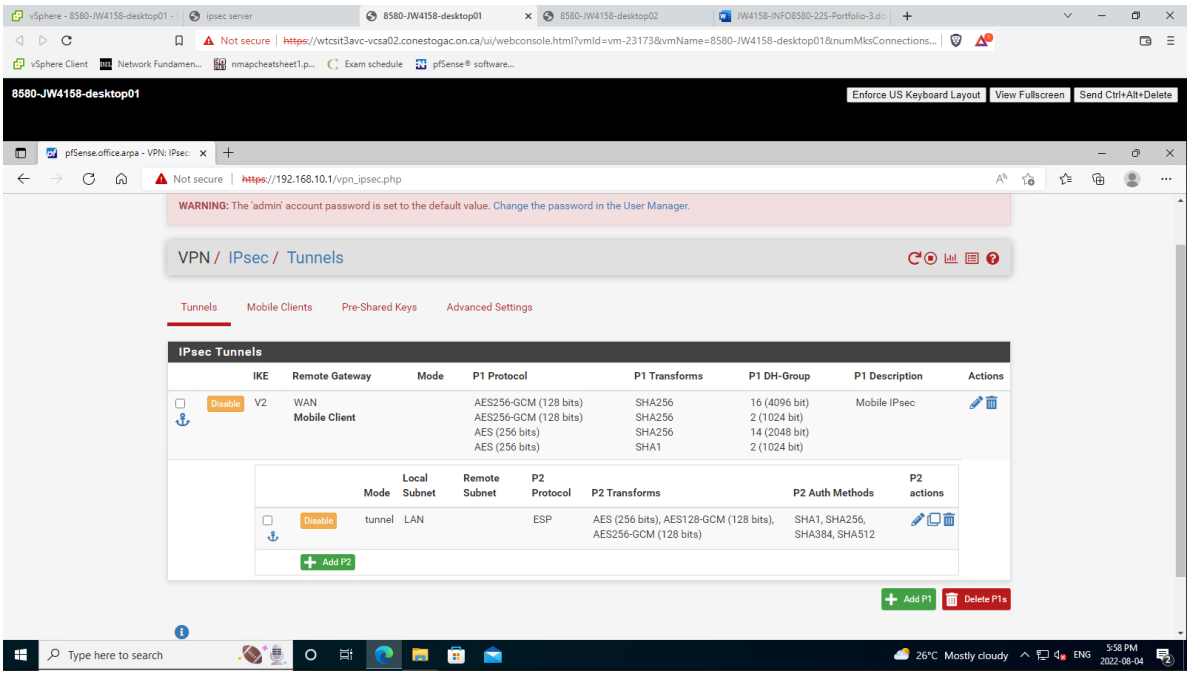

Figure 1.13 - Tunnel configuration (for reference)

Reflection

The biggest issue I had with this lab was that some of my default firewall rules were blocking the traffic. After disabling these rules, I was getting an “Invalid payload received" error but I fixed this by making sure my phase 1 and phase 2 encryption settings matched.

Using IPsec is advantageous because it operates on the network layer (layer 3) this means that it can monitor all activity on the network. IPsec also provides data confidentiality as all traffic is encrypted using keys. The downside to this is that any security breach can easily reach other computers on the network and it is difficult to prevent this without special security software.

References

1. Netgate Docs, 2022 (IPsec Remote Access VPN Example Using IKEv2 with EAP-MSCHAPv2 retrieved from https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-eap-mschapv2.html on August 2, 2022)
2. Netgate Docs, 2022 (Configuring IPsec IKEV2 Remote Access VPN Clients on Windows retrieved from https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-client-windows.html on August 2, 2022)

Lab 6 – Host to Network (Roadwarrior) OpenVPN

Description

The purpose of this lab is to teach us how to configure a host to network VPN using OpenVPN instead of IPsec on a pfSense router.

Preparation

To prepare for this lab, we need a pfSense router with a Windows desktop connected to it. We will also need the server to have a certificate authority and an endpoint certificate created by that authority. Refer to the previous portfolio for detailed instructions on this.

Observations

Begin by going to VPN > OpenVPN and then going to the 'Wizards' tab. Select the server type you want to configure, for this lab we will choose 'Local User Access'. Confirm that we want to use the CA and endpoint certificate that we created earlier. On the 'Server Settings' page, configure the settings as shown in Figure 1.1 and 1.2. On the Firewall Rule Configuration page, check both boxes. Finish the wizard and the OpenVPN server should now be running. As in the first lab, we must also remove the firewall rules that block private traffic. Afterwards, go to System > User Manager and add a new user. Set the username and password and check the option to create a certificate for them. Make sure it uses the correct CA. Then go to the packages manager and download the package called openvpn-client-export. Next, go back to VPN > OpenVPN and go to the new Client Export page. Scroll down to the bottom and click on the download button labeled 'Most Clients'.

Now we need to prepare our client. Import the .ovpn file that was generated in the previous step. Next, go to the community downloads page for OpenVPN download the Windows x64 MSI installer and install OpenVPN. Afterwards, right-click the new icon in the icon tray and import the .ovpn file. We should now be able to connect to our OpenVPN server.

Screenshots

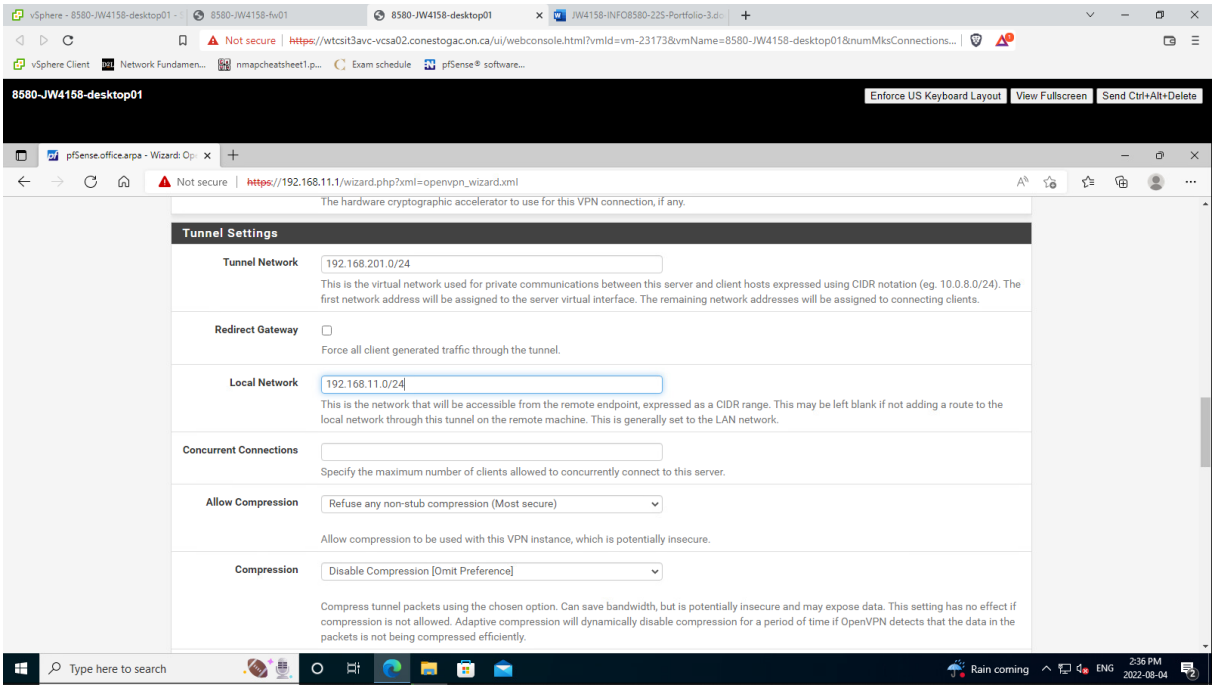

Figure 1.1 - Server Settings part 1

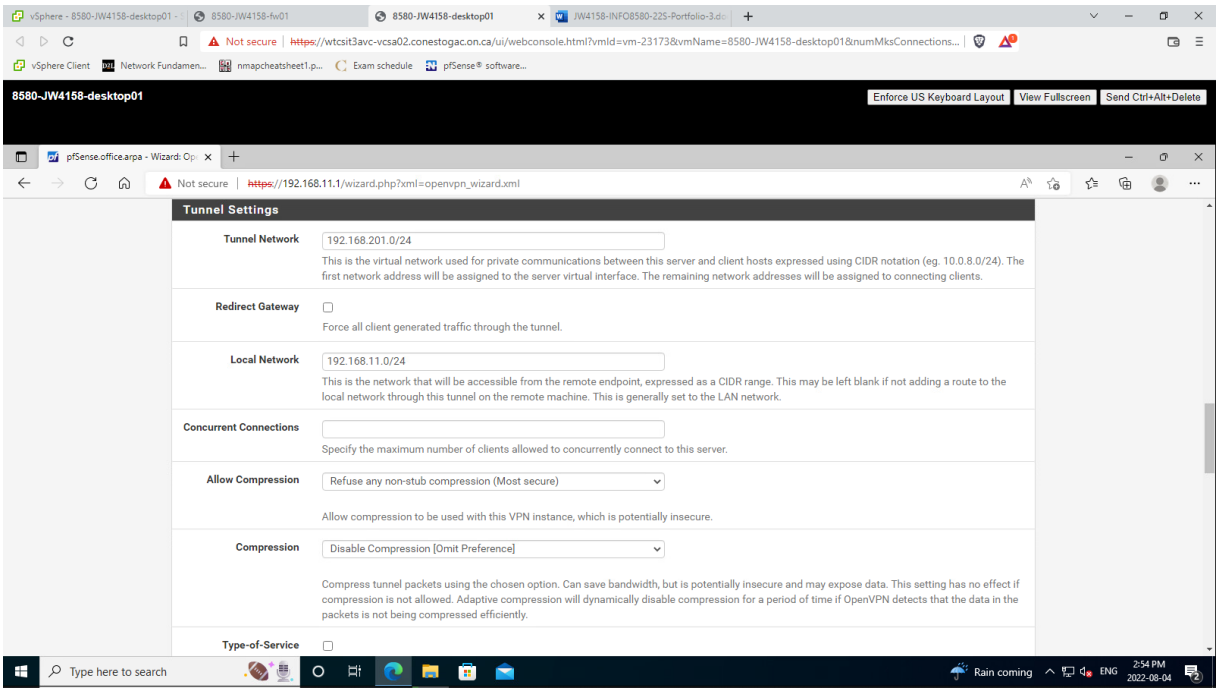

Figure 1.2 - Server Settings part 2

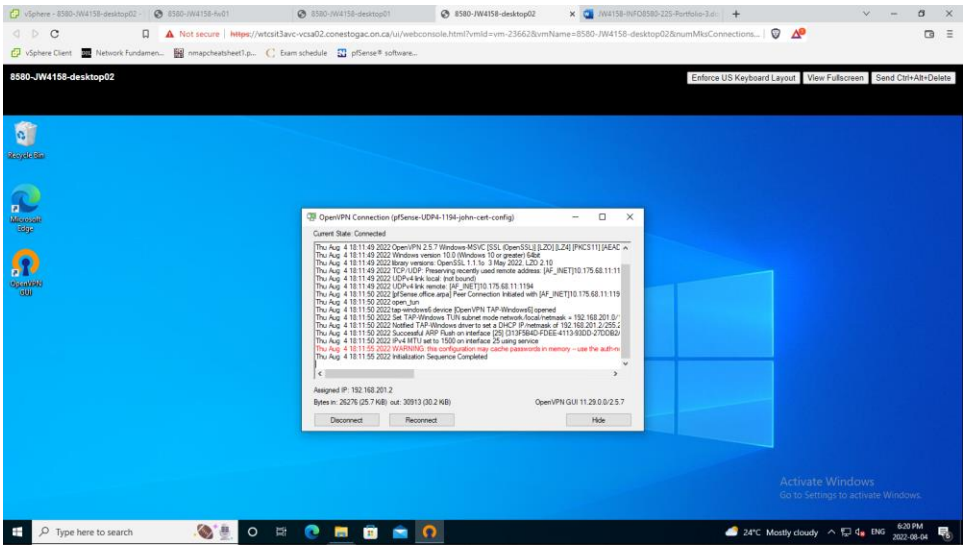

Figure 1.3 - Successful connection

Reflection

Other than the issue faced in the previous lab, I had no difficulties with this lab.

Using a split tunnel VPN means that some of your traffic is being routed over a VPN but some of it isn't. The advantage of this is that you can avoid a large amount of the overhead that comes with using a VPN while also protecting your most sensitive data. The drawback is that this leaves your computer vulnerable to attacks that come from your unprotected internet traffic. This applies to the privacy of your data as well. It is best to use a split tunnel VPN if you are willing to sacrifice some security in favour of usability. If security is your top priority, then they are best avoided.

References

1. Netgate Docs, 2022 (OpenVPN Remote Access Configuration Example retrieved from https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html on August 2, 2022)