Luke Alvarado gar407 Lab 01

IS-3424-003-202420

Student:	Email:
Luke Alvarado	lukealvarado71@gmail.com

Time on Task:	Progress:
1 hour, 38 minutes	100%

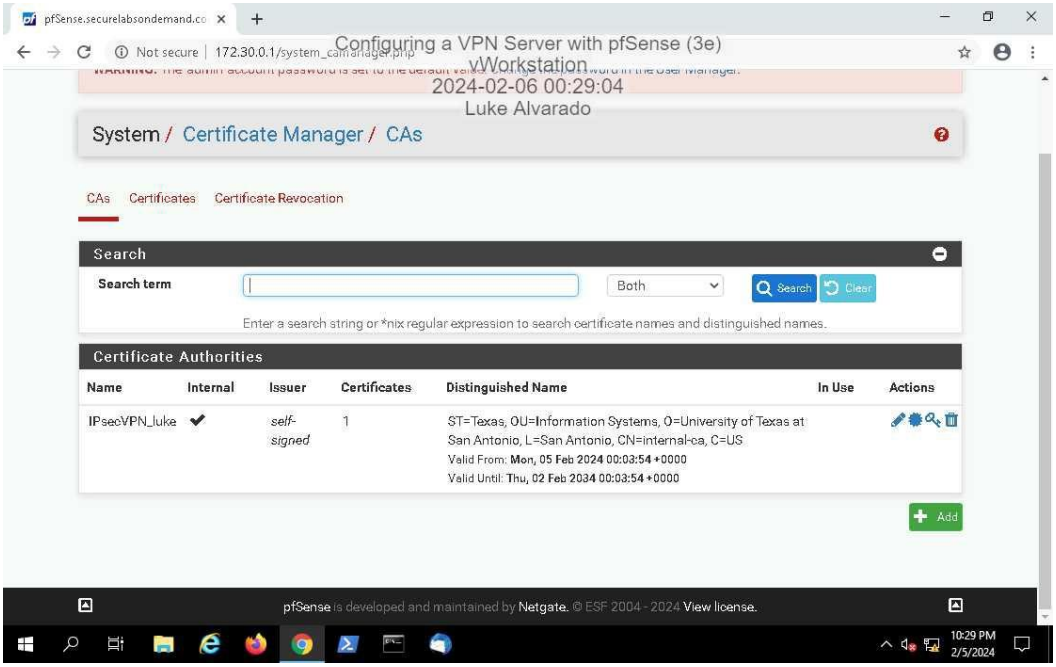
Report Generated: Tuesday, February 6, 2024 at 11:58 PM

Section 1: Hands-On Demonstration

Part 1: Configure an IPsec VPN Server

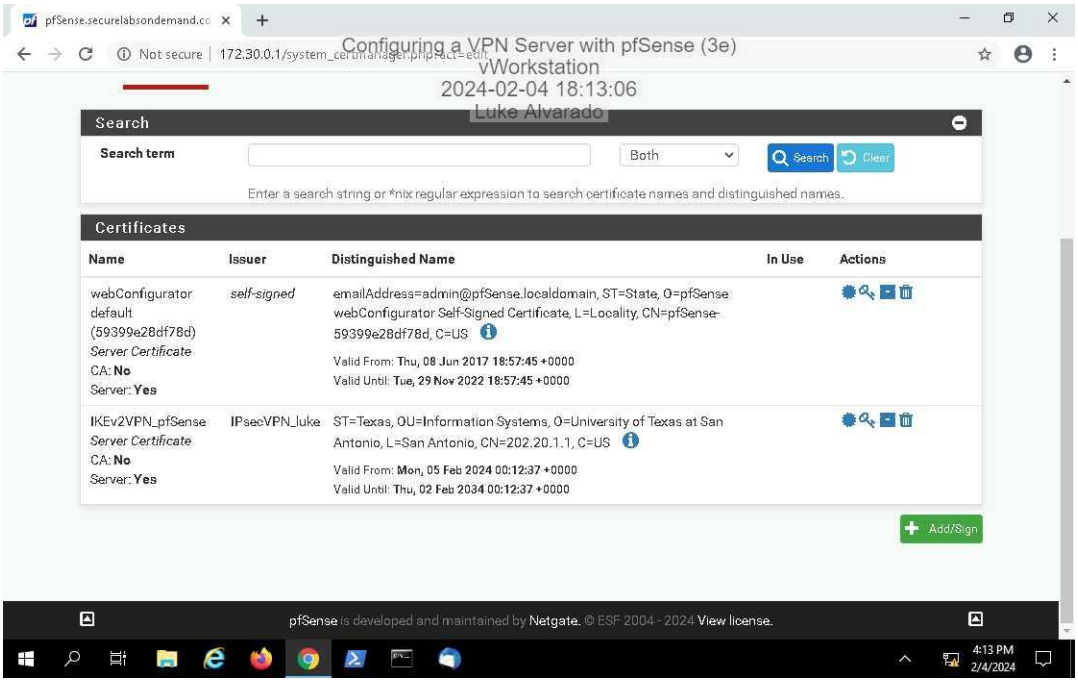
18. **Make a screen capture** showing the **updated Certificate Authorities table**.

Here I created an internal Certificate Authority through pfsense to verify the public key for the IPsec VPN for the digital signature and certificate. I added personal information to be a self-issued authority.



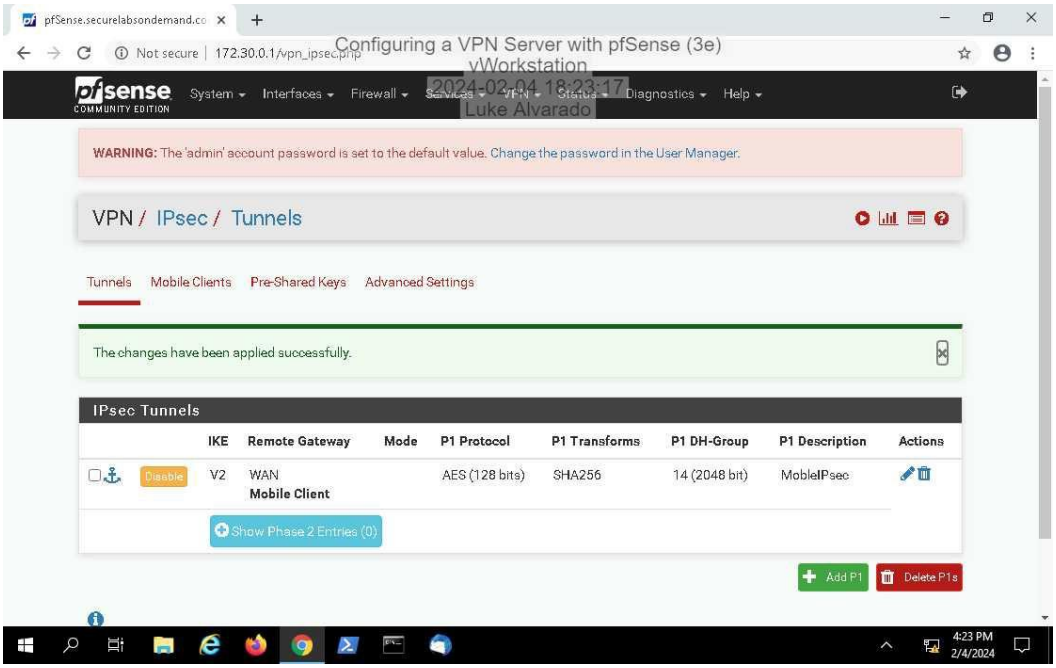
32. **Make a screen capture** showing the **updated Certificates table**.

Here I issued a certificate to the VPN server using the certificate authority made earlier. This CA and certificate confirm the public key for usage in a digital signature authentication for the IPsec VPN remote connections.



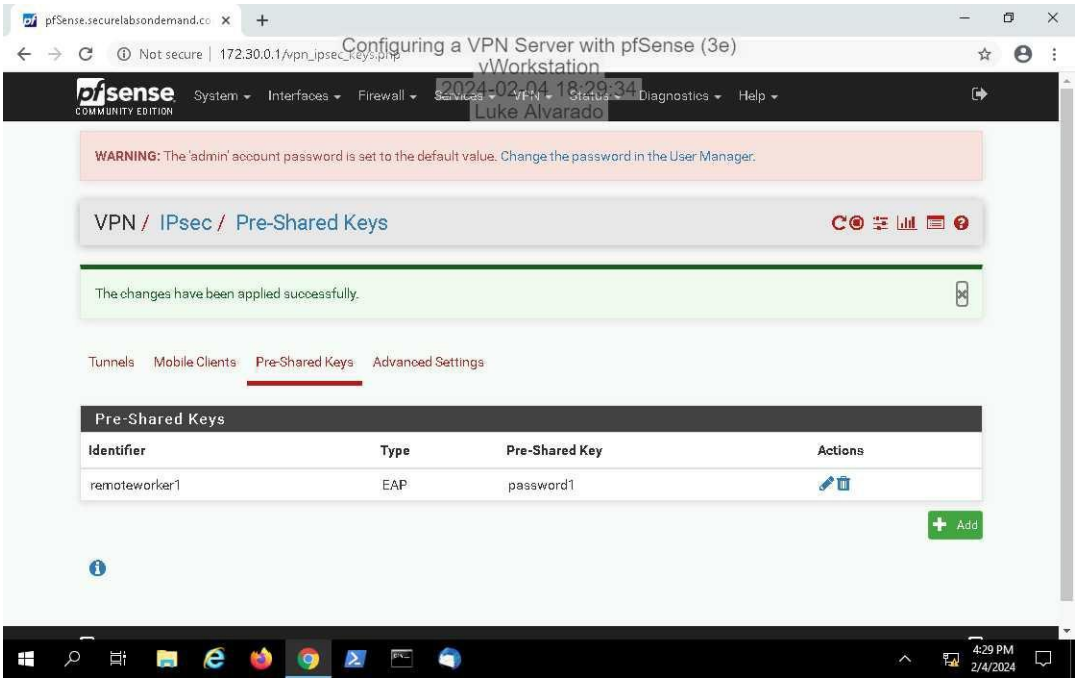
56. **Make a screen capture** showing the **updated IPsec Tunnels table.**

Here I created the phase one definition for the IPsec VPN in where I specified the key exchange method, the authentication method, and the encryption algorithm to be used.



74. **Make a screen capture** showing the **updated Pre-Shared Keys table**.

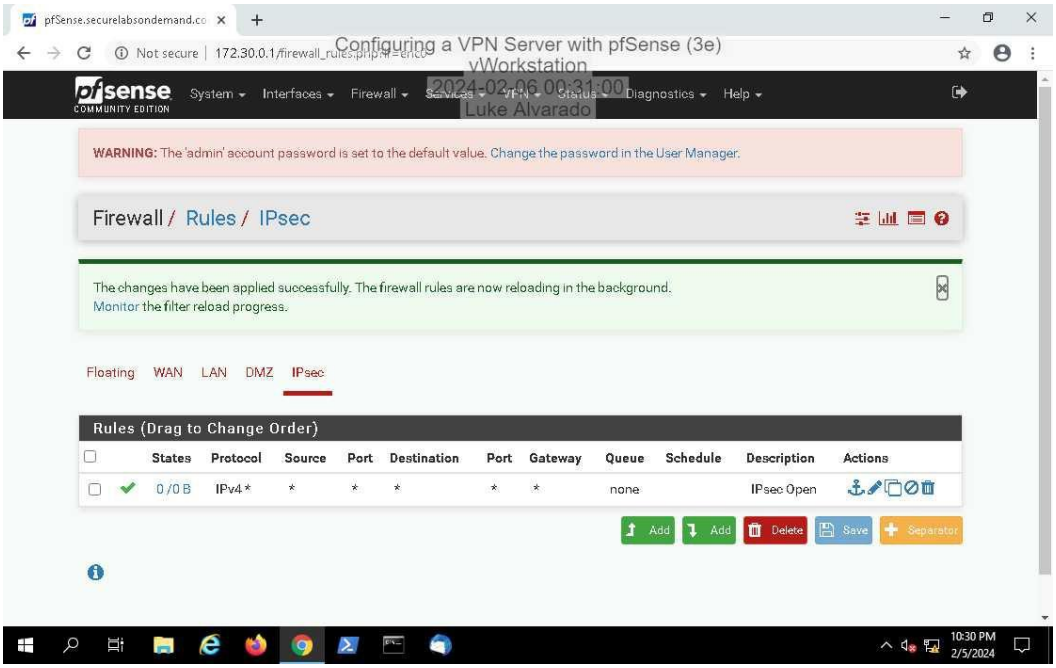
Here I defined a pre-shared key to be known before connection by server and client to perform the password-based authentication in phase 1 of the VPN negotiations.



Part 2: Configure a Firewall Rule for VPN Traffic

9. **Make a screen capture** showing the **updated IPsec Rules table**.

Here I defined a firewall rule to basically make it transparent, in that it allows all protocols to come through unimpeded.

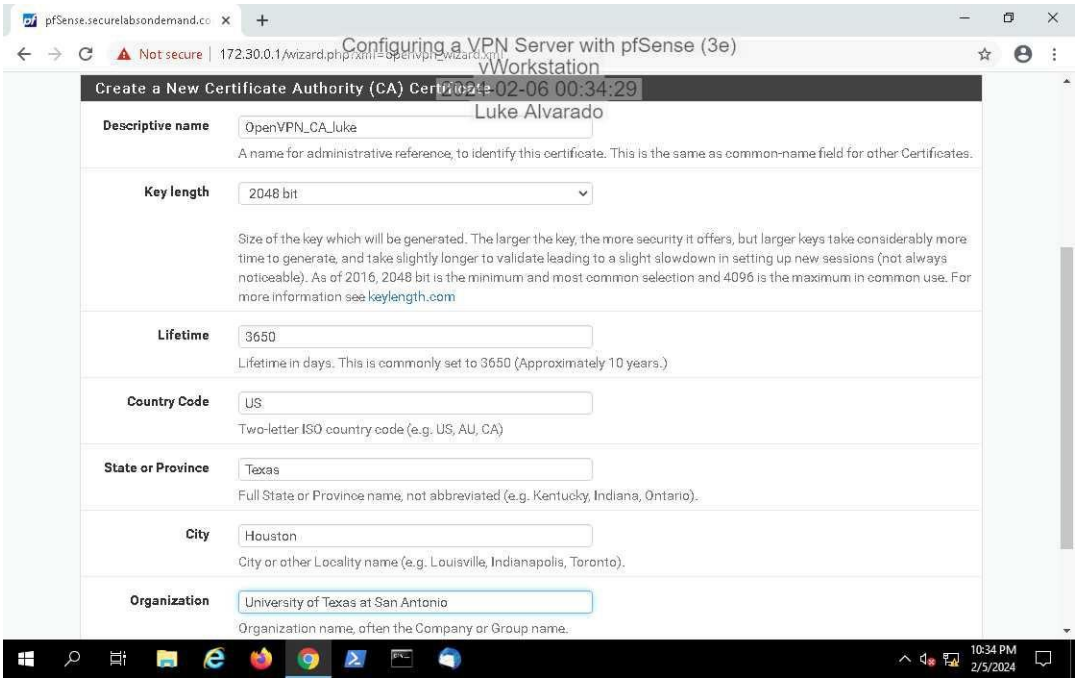


Section 2: Applied Learning

Part 1: Configure an OpenVPN VPN Server

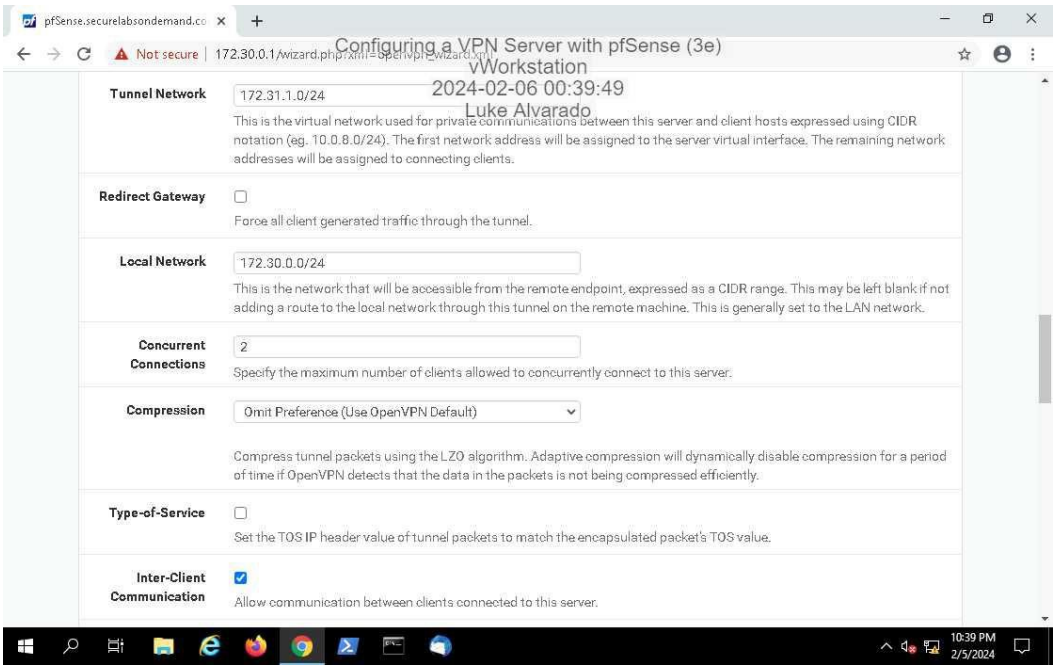
13. **Make a screen capture** showing the **CA configuration form.**

Here I made an internal CA for an OpenVPN VPN server in the same manner I did for an IPsec VPN server.



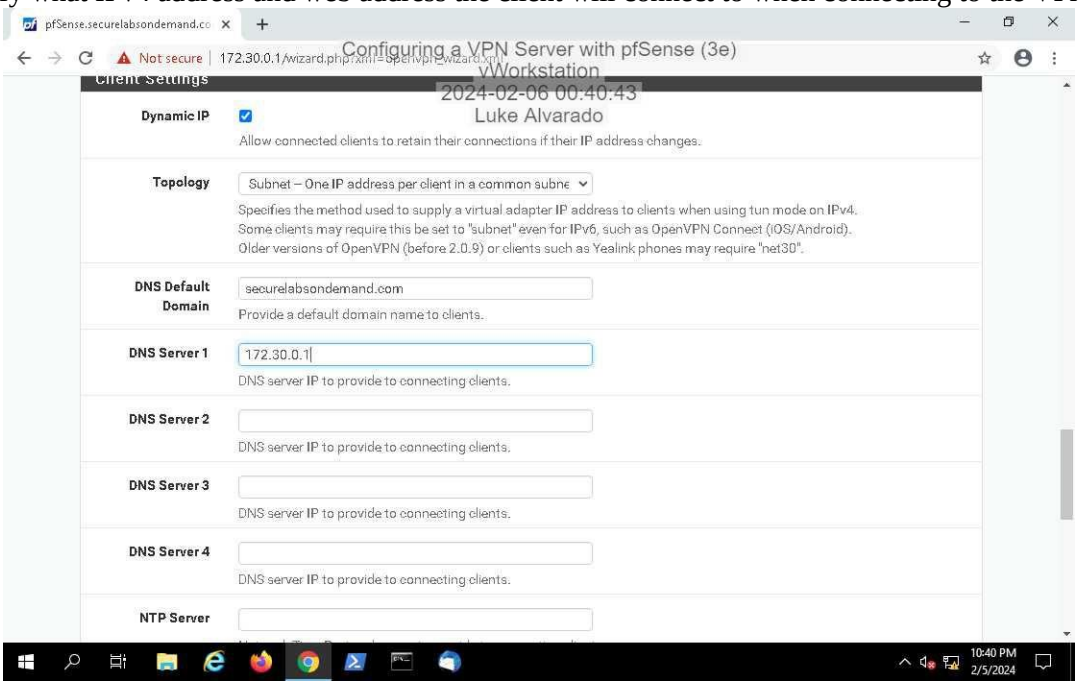
27. **Make a screen capture** showing the **Tunnel Settings section**.

Here I configure the OpenVPN VPN tunnel through the certificate configuration page to allow for communication between VPN clients connected to the server.



30. **Make a screen capture** showing the **Client Settings section.**

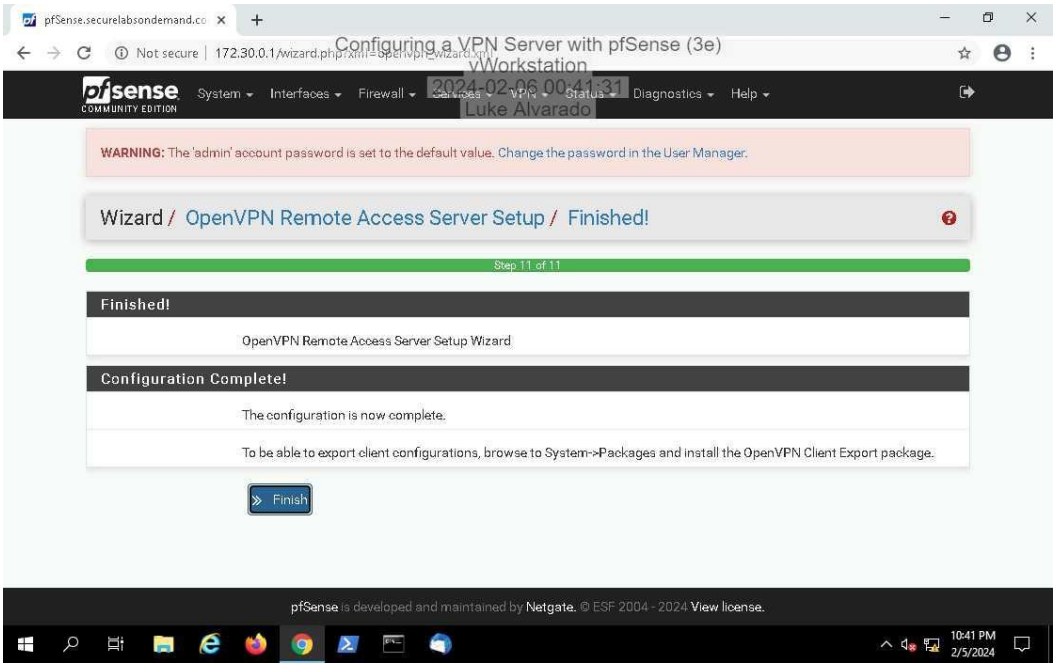
Here I specify what IPv4 address and web address the client will connect to when connecting to the VPN.



Part 2: Configure a Firewall Rule for VPN Traffic

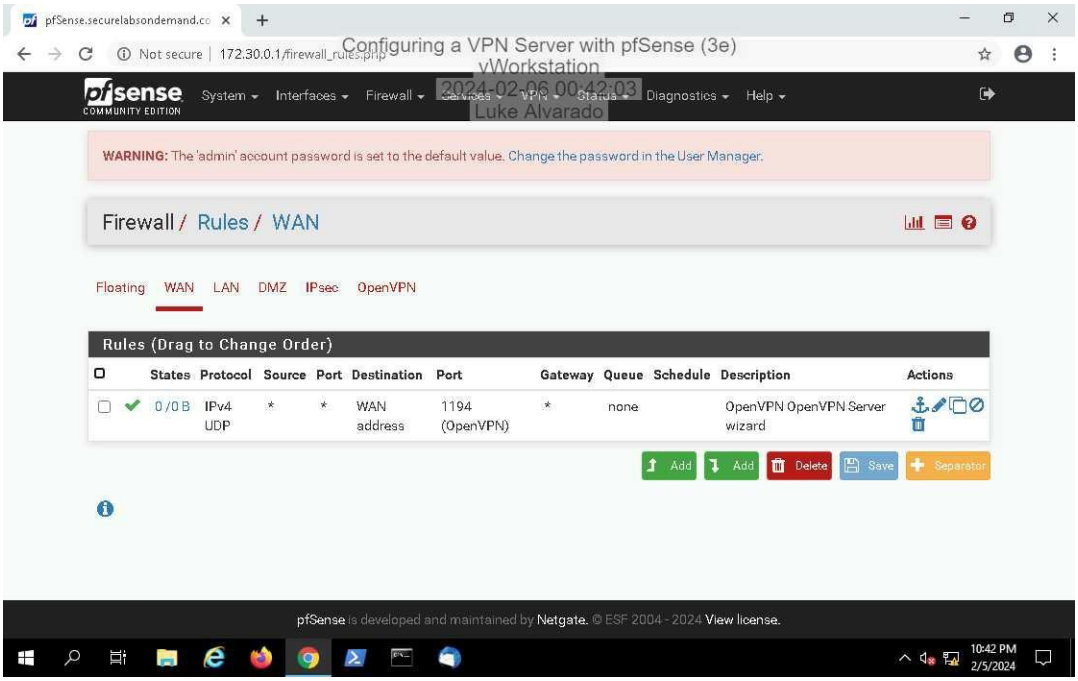
2. **Make a screen capture** showing the **completed OpenVPN configuration**.

He re it is shown I fully configured the OpenVPN VPN after I completed implementation and configuration of the CA, certificate, and the firewall, the latter for which I used the default values.



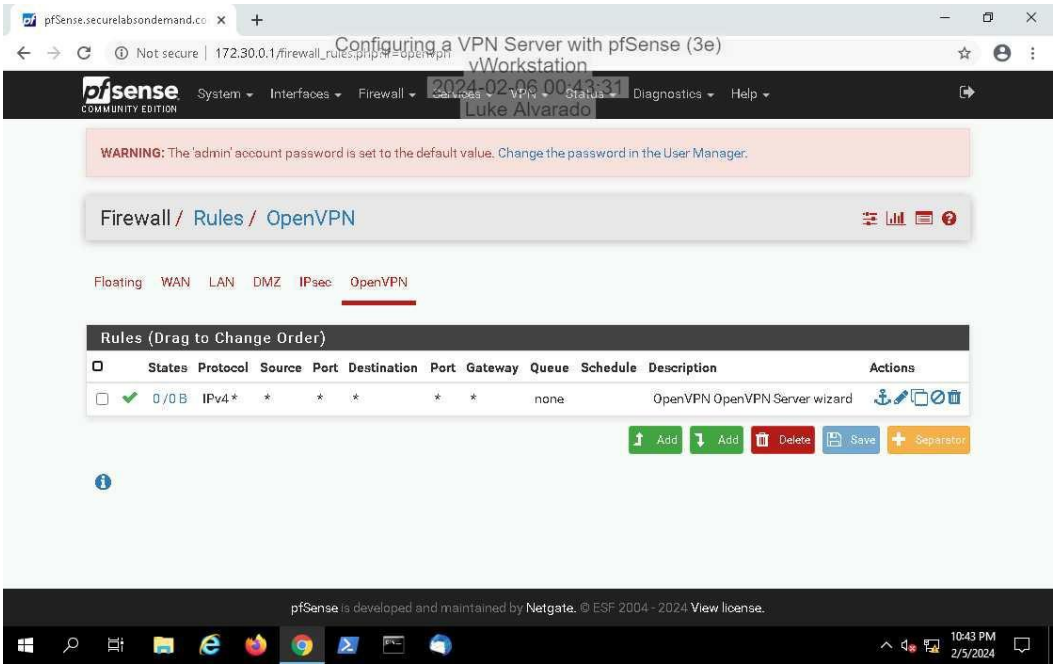
5. **Make a screen capture** showing the **OpenVPN rule on the WAN Rules table.**

Here is shown the default firewall rule accepted earlier for use on Wan connections.



7. **Make a screen capture** showing the **OpenVPN rule on the OpenVPN Rules table**.

Here are all the rules regarding OpenVPN, and because the default configuration was used, a simple rule that lets all traffic pass is present.

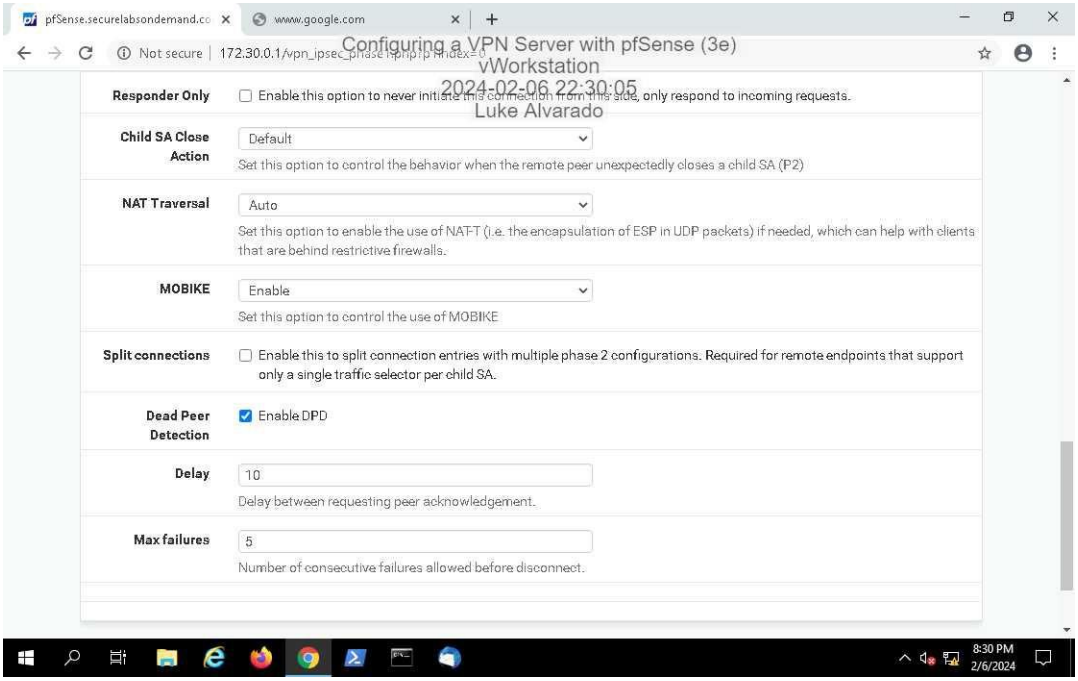


Section 3: Challenge and Analysis

Part 1: Enable IP Roaming for Remote VPN Clients

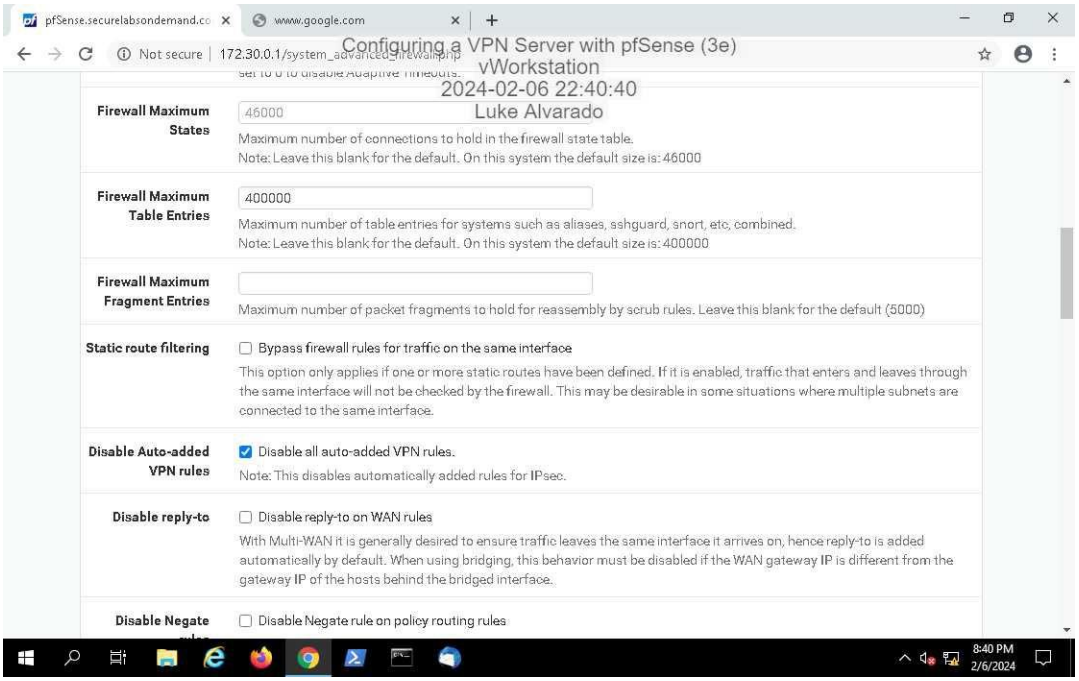
Make a screen capture showing the **enabled MOBIKE option in the IPsec tunnel configuration**.

Here I enabled MOBIKE in the system/advanced settings to allow for stable connection for users switching from wireless to wired.



Part 2: Create Explicit Firewall Rules for an IPsec VPN

Make a screen capture showing the **disabled automatic IPsec rule creation option**.
Here I clicked the setting to turn off all auto-created rules so that I may define stricter and more rigid ones.



Make a screen capture showing your **firewall rules that permit IPsec traffic**.

Here I defined the 3 rules to allow specific traffic from the two ports belonging to IPsec NAT-T and IKE in which I allowed UDP, and I also allowed any packet of ESP to be let through the firewall.