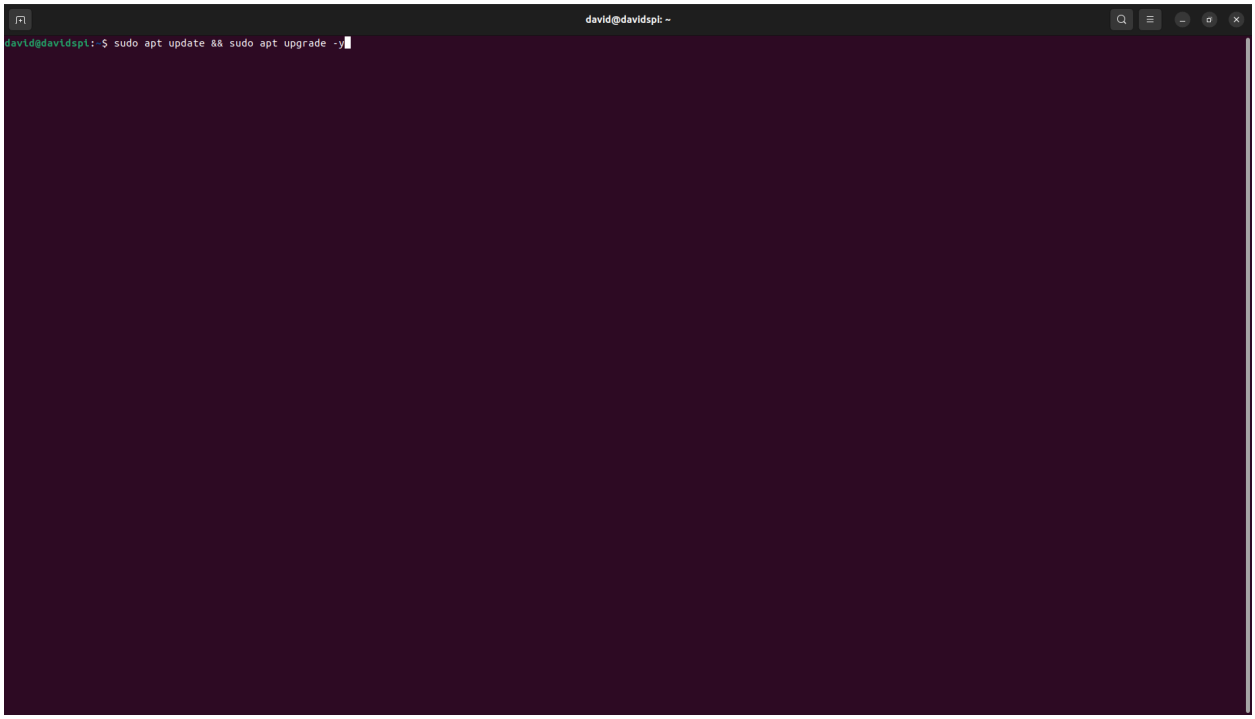
WireGuard

Objective: For this project, I set up a secure VPN using WireGuard. I installed WireGuard on both the server and client machines, generated key pairs, and configured the connection settings to define how the devices communicate. The server was set up to listen on a specific port and handle traffic for certain IP ranges, and the client was configured to connect using the server's public key and address. I also updated firewall rules and routing to make sure everything worked smoothly. In the end, I built a lightweight and fast VPN tunnel that securely connects the devices over the internet.

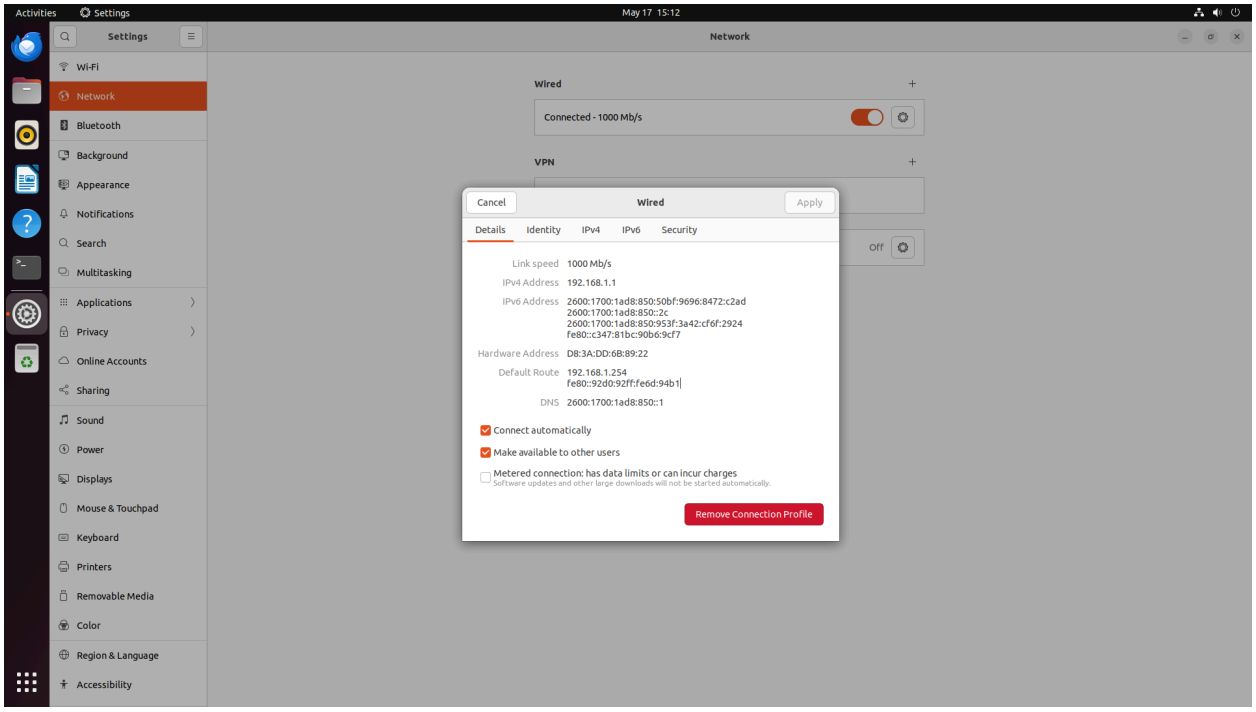
Equipment: Raspberry Pi 4, Wireguard, and AT&T Router

Steps:

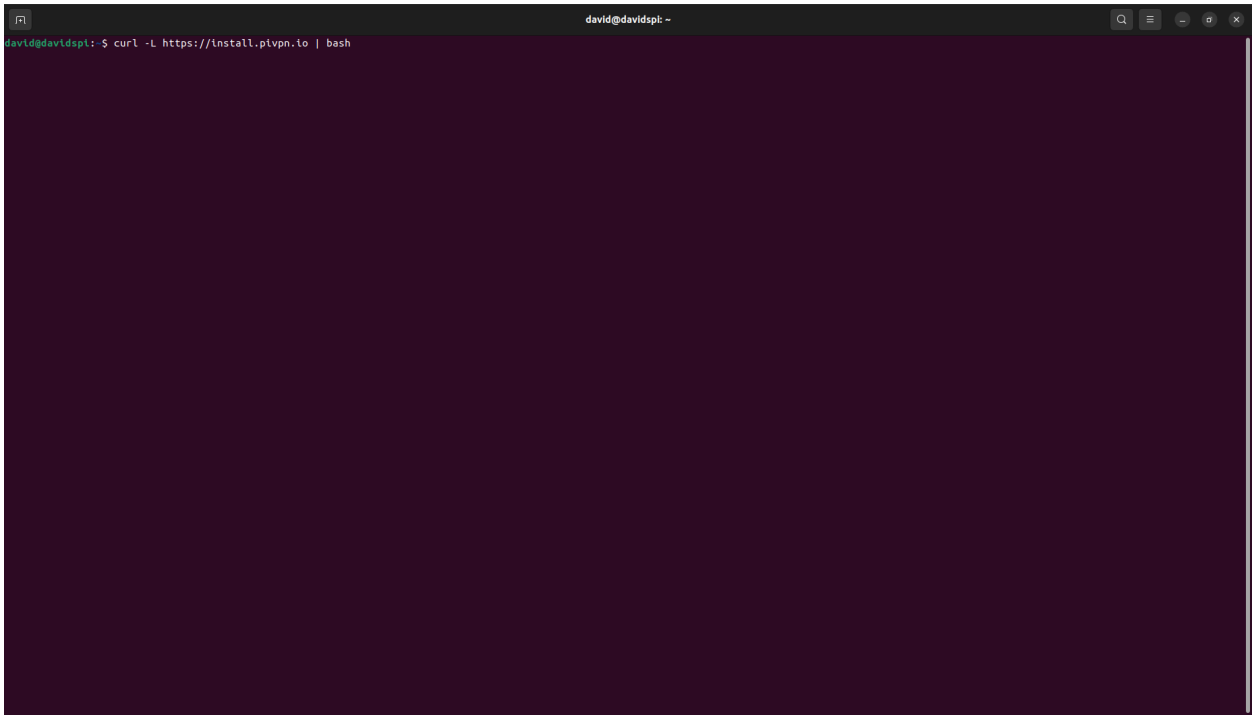
1. I ran the command **sudo apt update && sudo apt upgrade -y** to make sure my pi is up to date



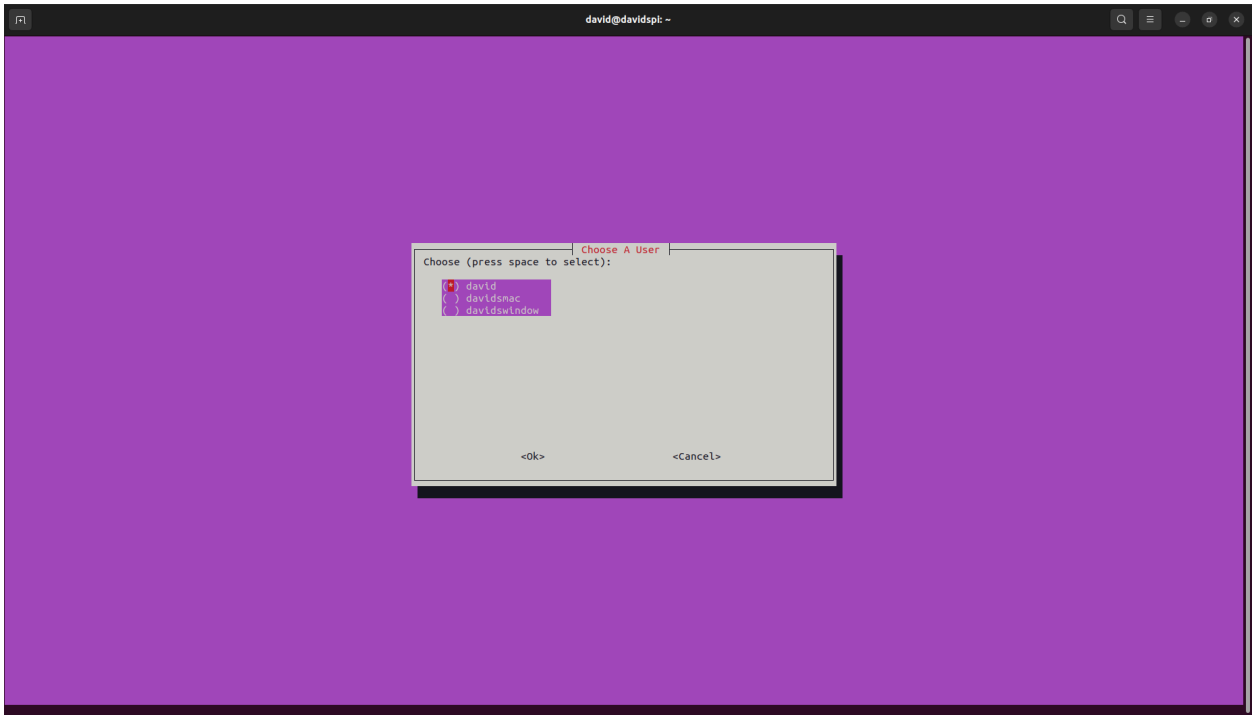
2. I **created a static IP profile**



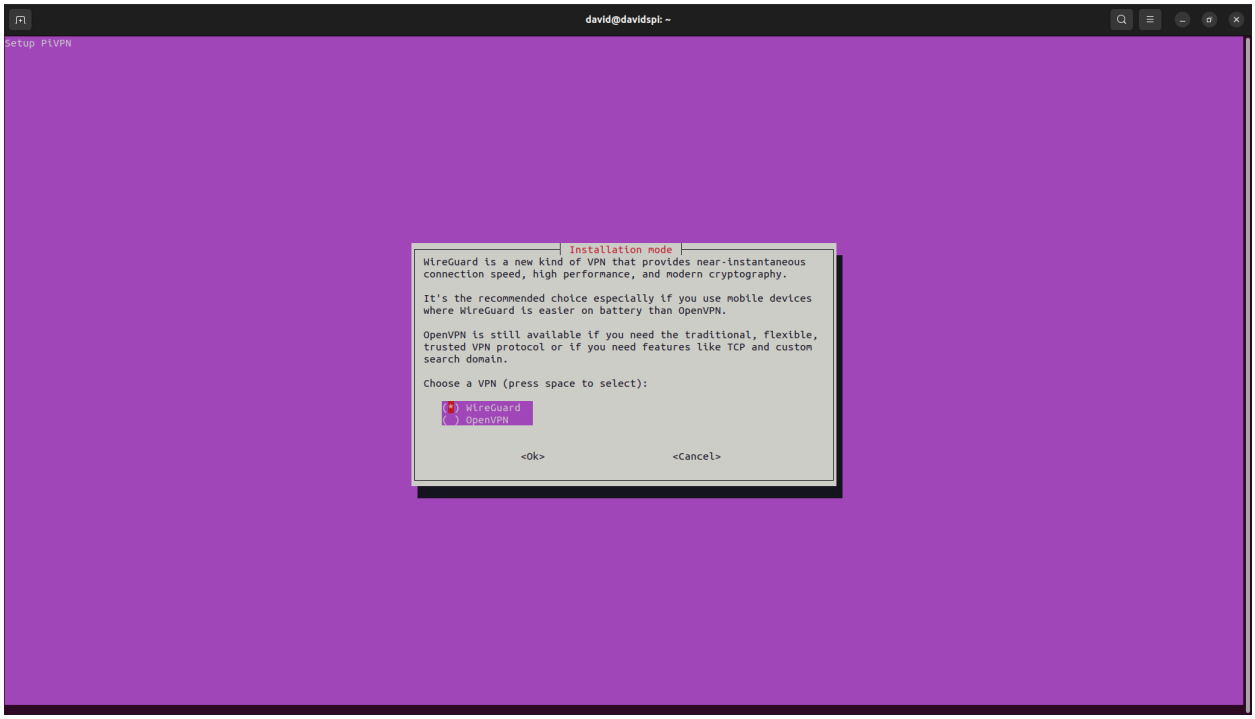
3. I ran the command **curl -L https://install.pivpn.io | bash** to install wireguard



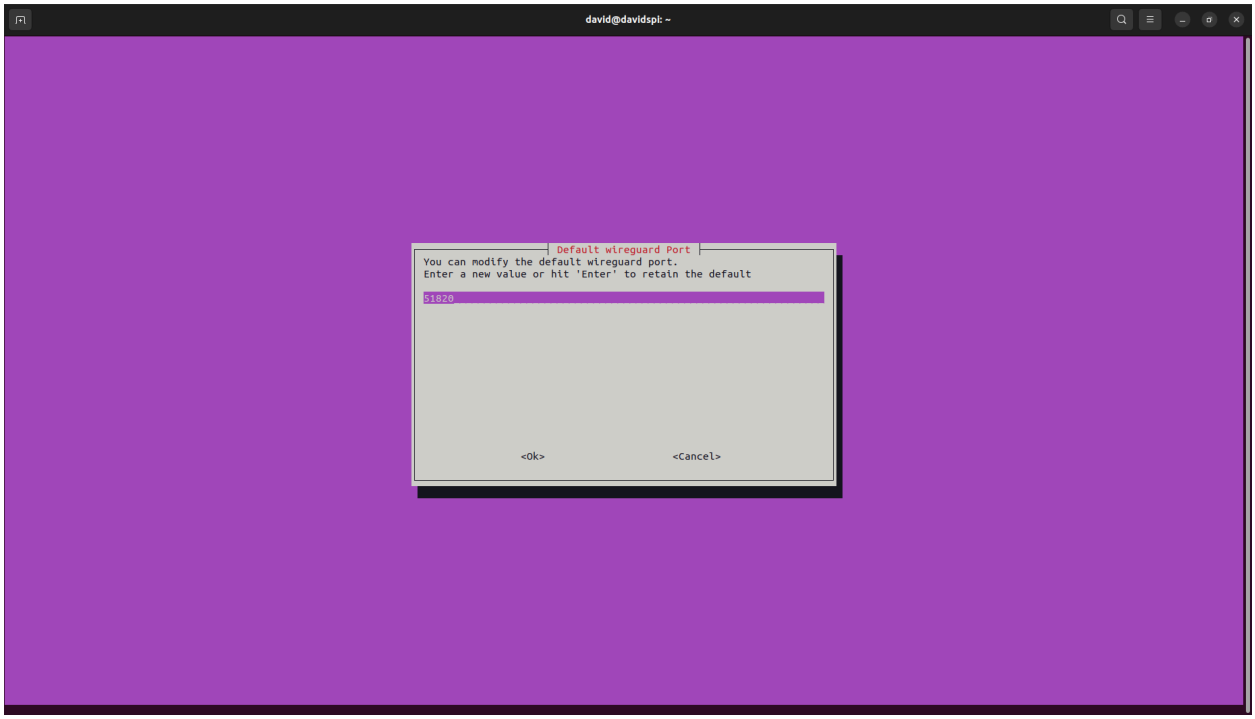
4. I make my **main user on the raspberry pi as the admin**



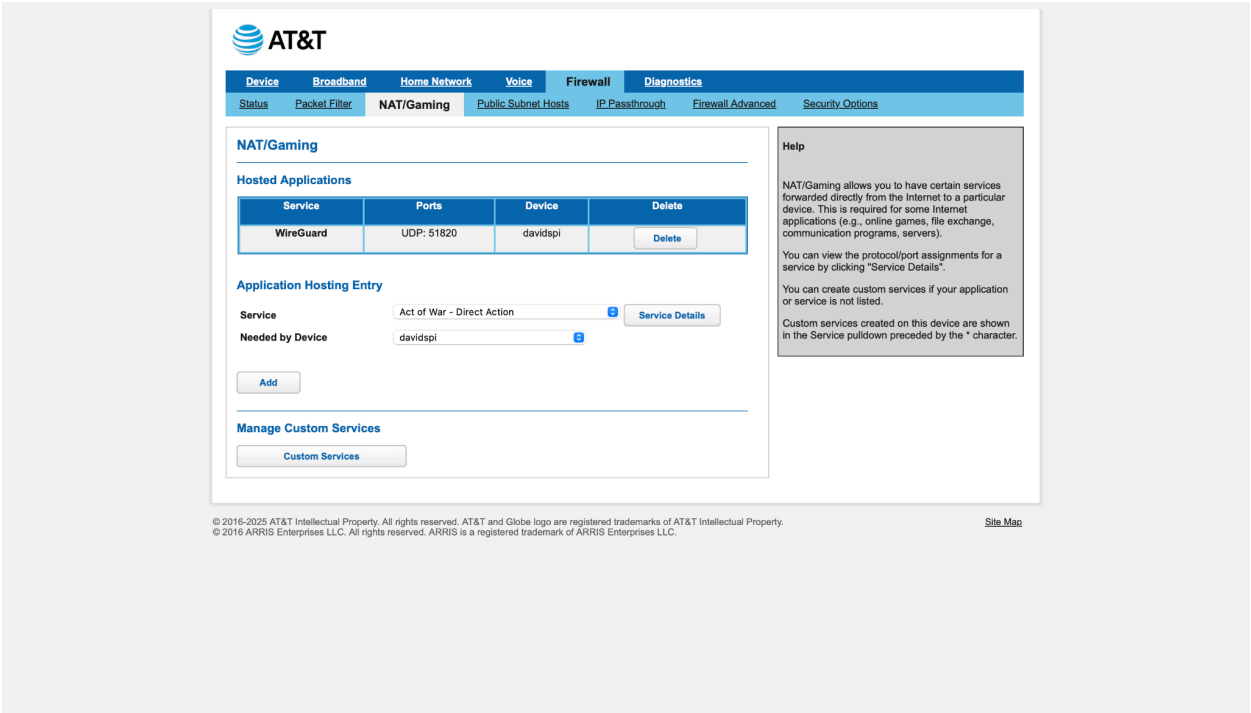
5. I installed WireGuard



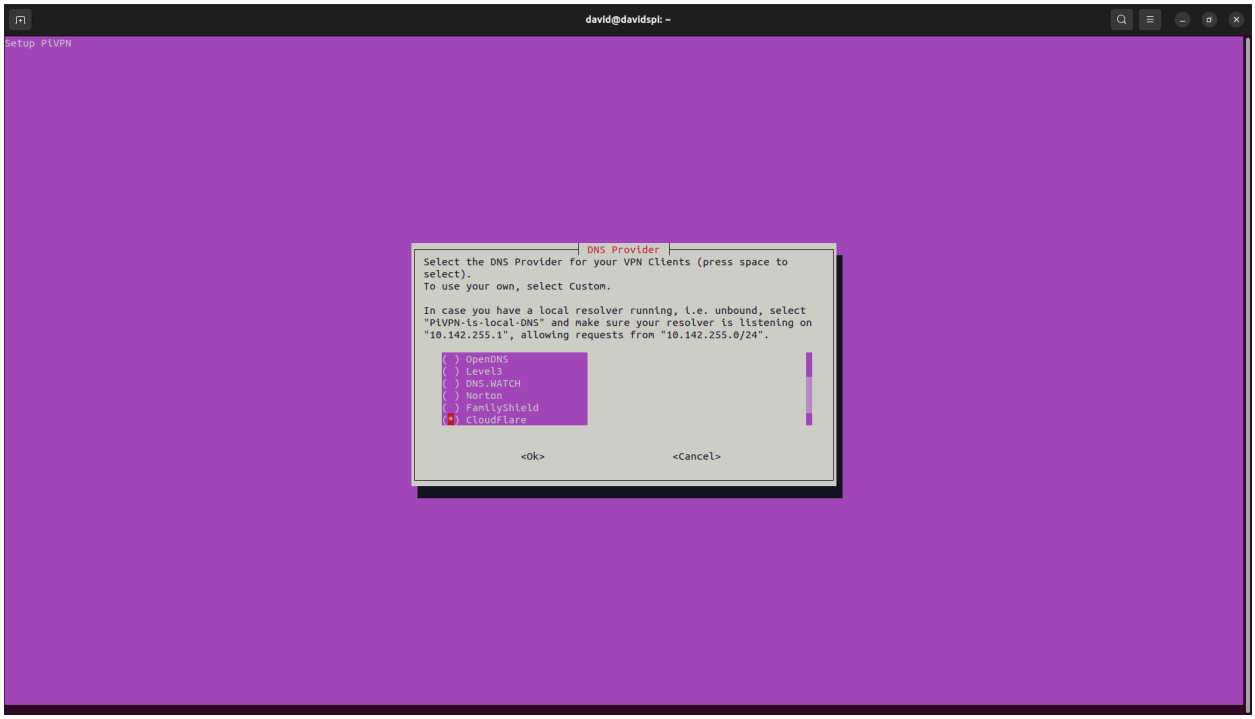
6. I selected the **port 51820**



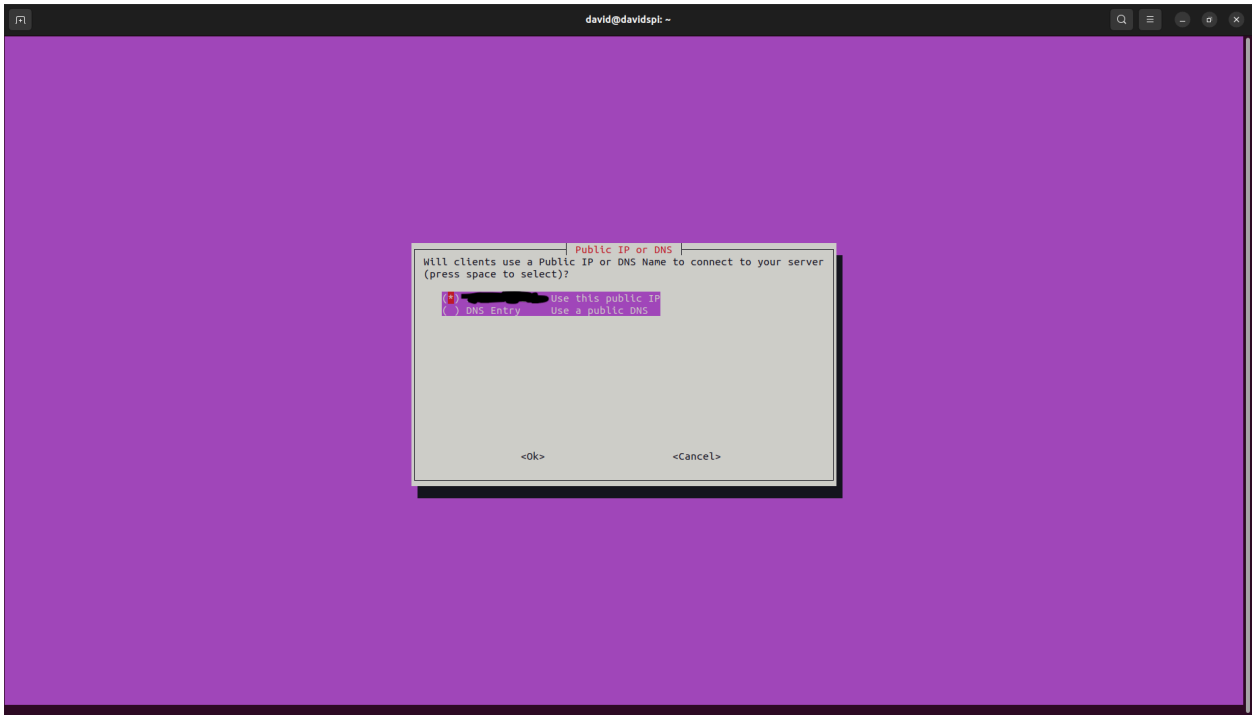
7. I **opened the port on my firewall** settings within my router



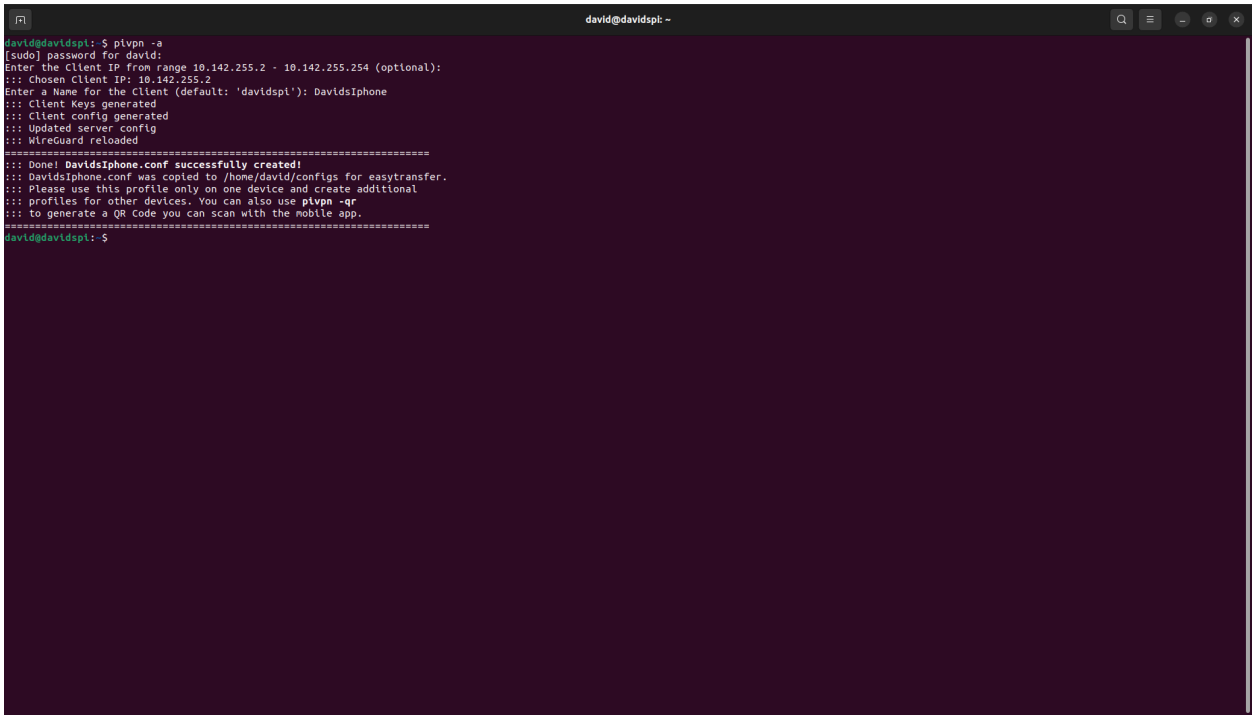
8. I **selected cloudflare as the DNS Server**



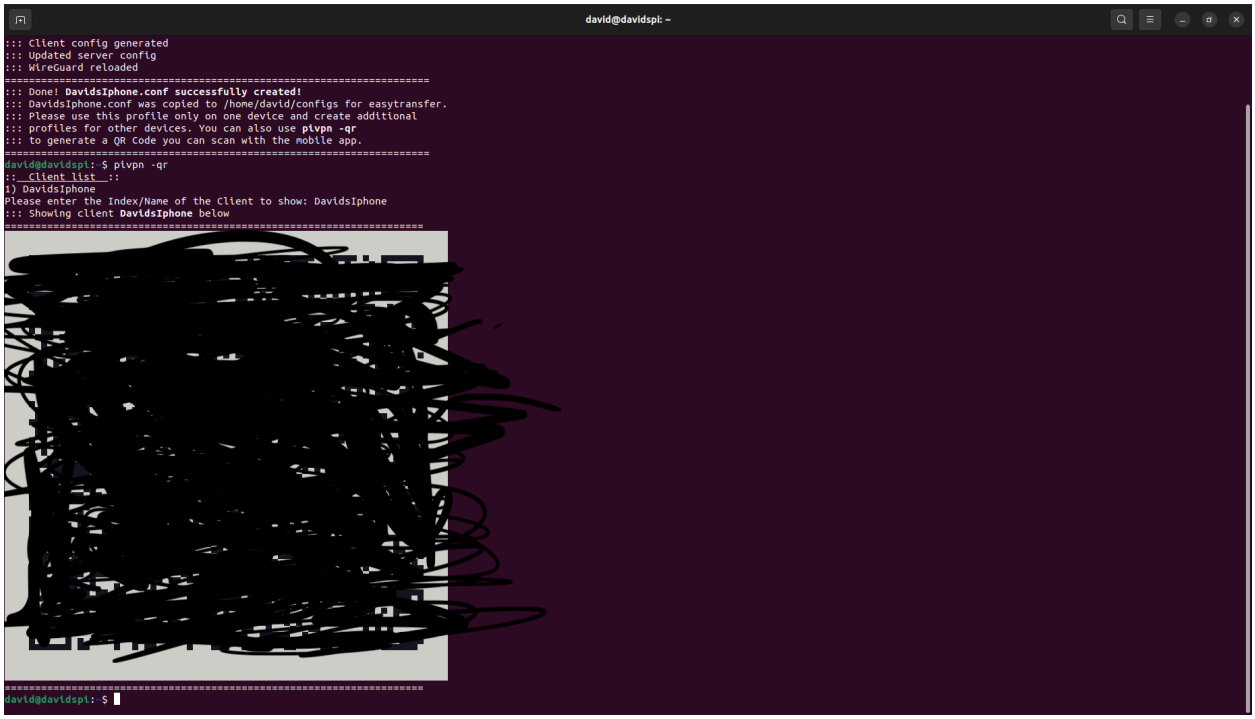
9. I selected my **public IP address** to connect the server



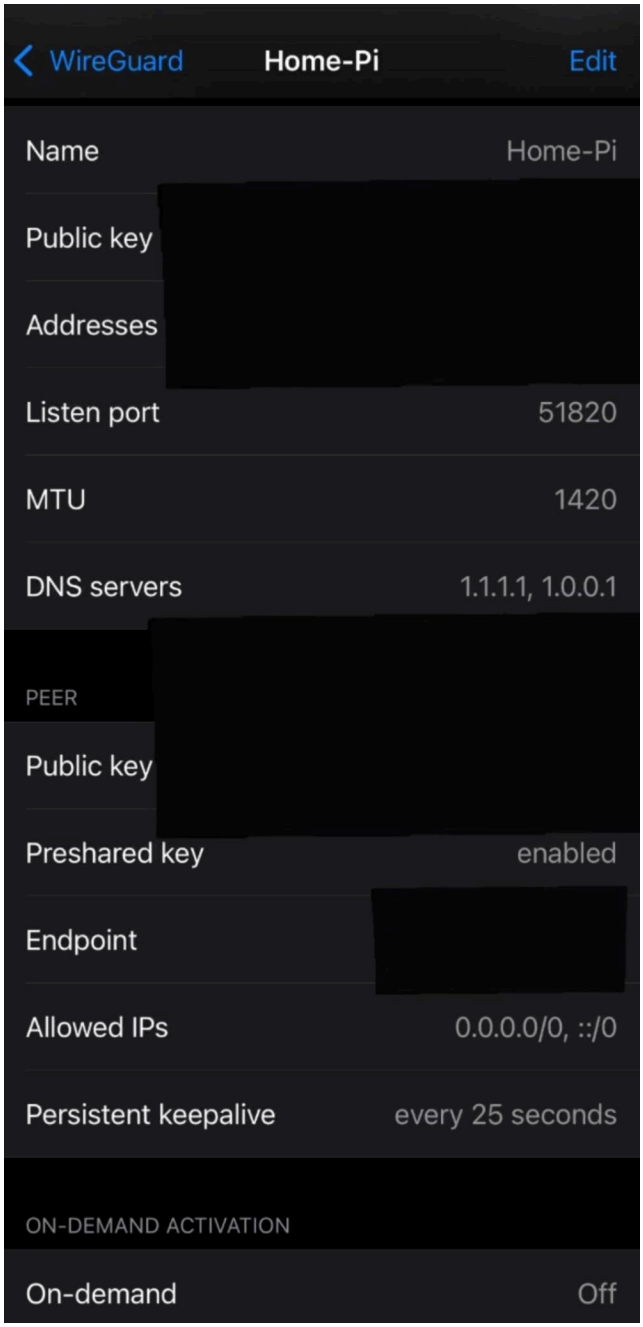
10. I **created a user my Iphone**



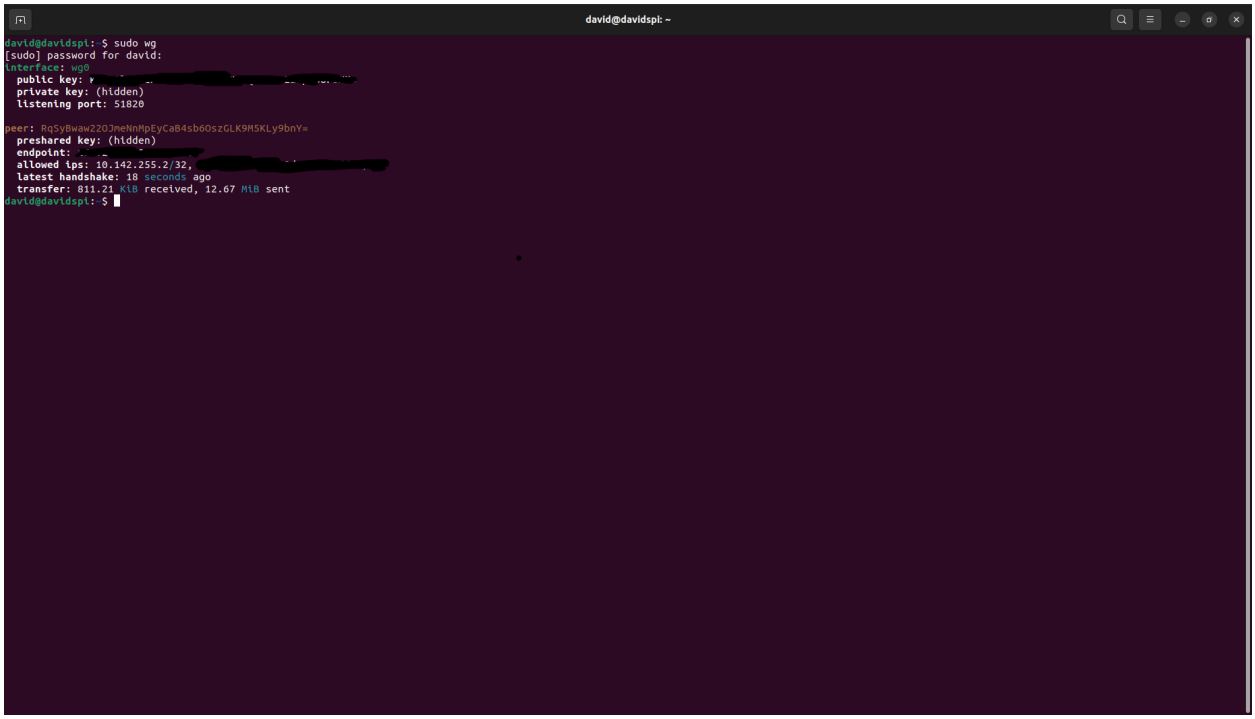
11. I **generated a QR code for easy setup**



12. I **configured the tunnel and made sure everything is correct**



13. I ran the command **sudo wg** to verify the connection



14. Lastly I tried accessing my home router while on the VPN (as you can see I'm on 5G)