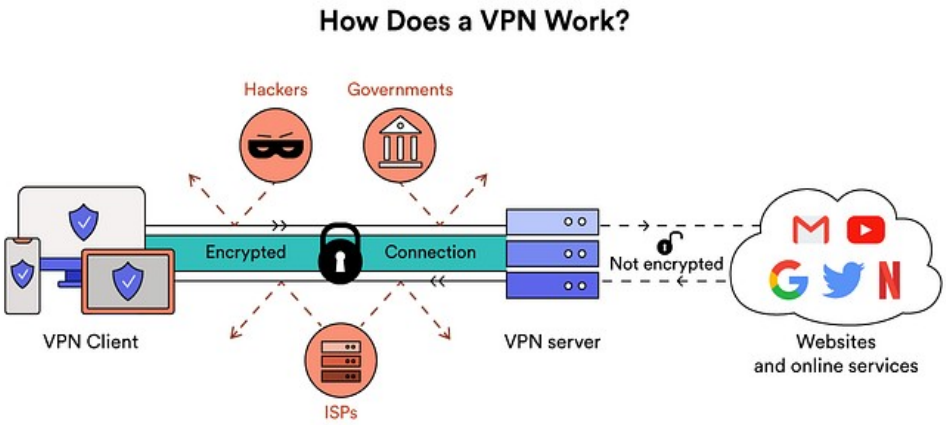
Mandar Tarmale
Roll No : 19
UID No: 2309027

Setting up a Free VPN Service on AWS

First, let's make a distinction between **Privacy** and **Anonymity**.

Private = Encrypted = Confidential
You can be known as a sender of a message but the message itself is secret and only you can read
Anonymous = Unknown Sender/Receiver
But it's not necessarily private and confidential.
A VPN can provide both or just one. Most web traffic is already encrypted with HTTPS. So at best without a VPN your ISP or anyone on your Local Area Network can see the domains. Not content. They know what sites you visit but can't see plain text content.
Adding a VPN creates an encrypted tunnel to the VPN server. The VPN server acts as a proxy and forwards traffic to its destination.



So if you connect to a VPN server hosted by a 3rd party then your ISP can see the IP of the VPN server but nothing else. However, the VPN server can keep logs and they basically get to snoop your traffic since you've given them the trust.
Self-hosted VPNs are those where you host your own VPN server. So you know for certain if you

keep logs or not. This is by far the best way to go but is also limiting in some ways.

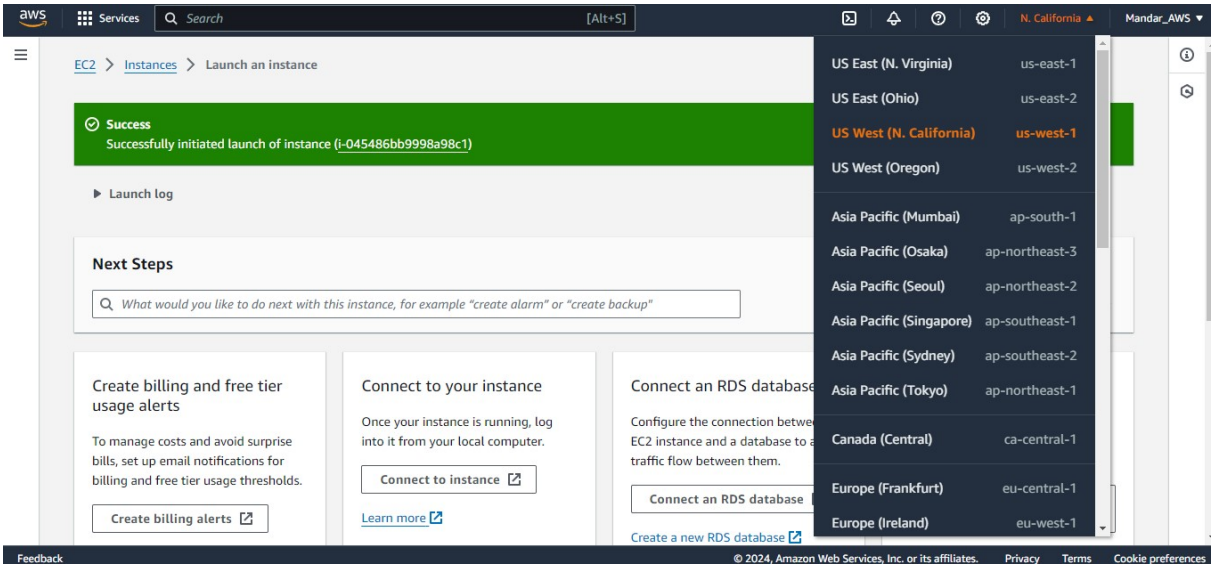
You can host OpenVPN in AWS.
That gives some level of anonymity because you can pick a server located in Hong Kong for example but if you want many server locations to choose from then you'd have to host a server for each geographic location which can get expensive.

Requirements for Setup :

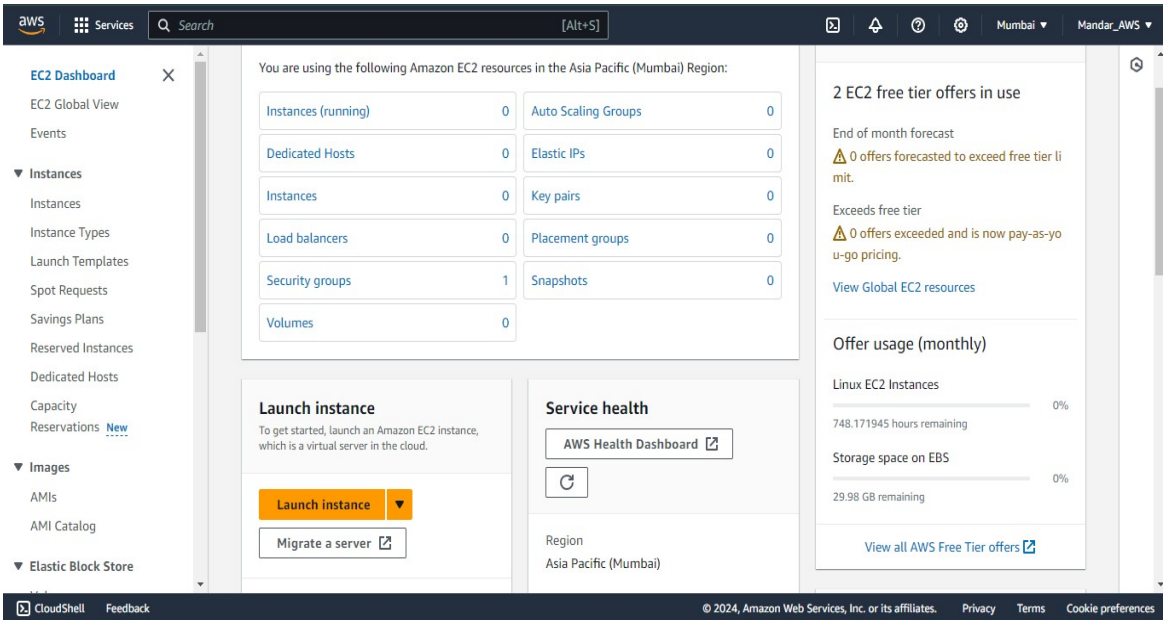
- An AWS account — a new account comes with a Free Tier Eligibility for 12 months which covers 750 hours of usage per month, so you won't be charged for running the VPN on AWS.

STEP 1 — Launch OpenVPN Access Server from AWS Marketplace

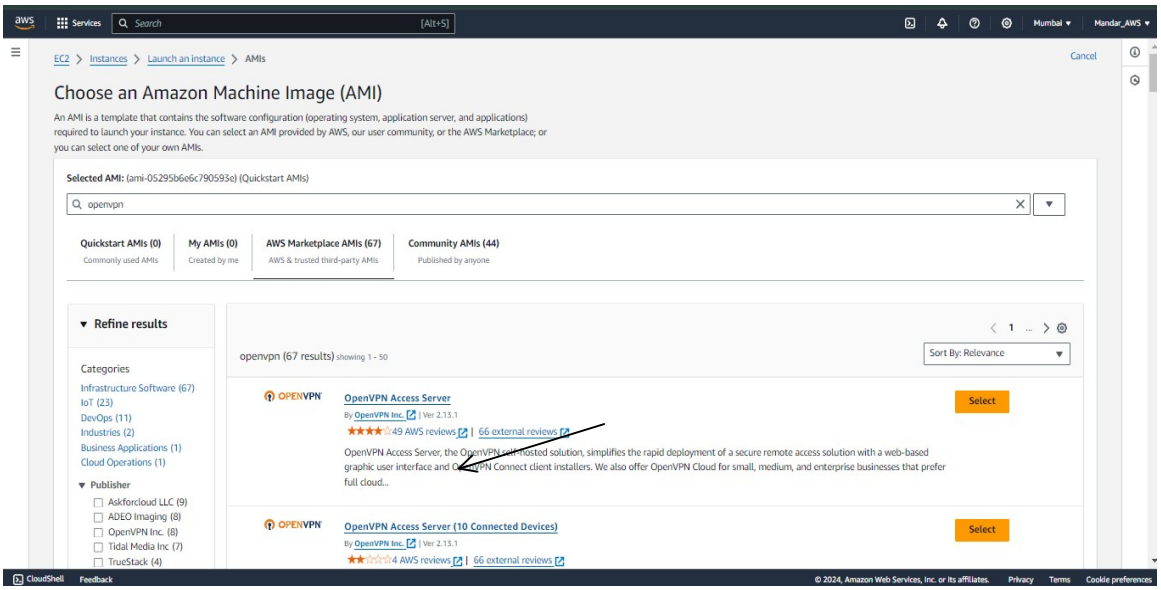
1. Sign in to the AWS Management Console and Select to the **EC2 service from Services**.
2. If you are located in India change your region to Asia Pacific (Mumbai) ap-south-1. Then click on Launch Instance. I have choose the region as ***US West (N. California) us-west-1.***



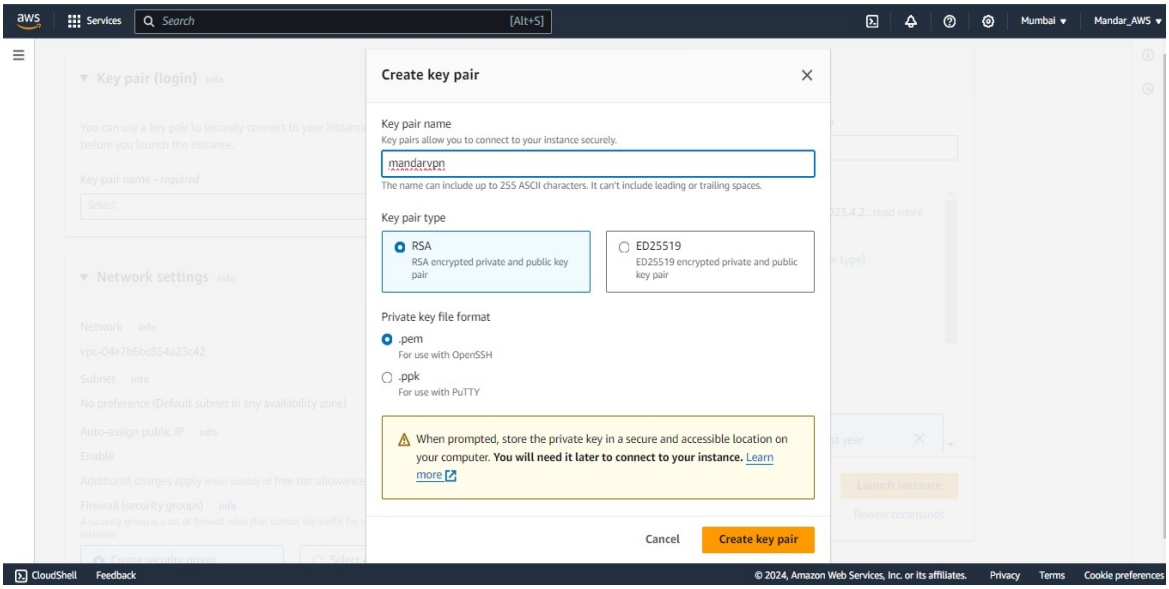
3. In the dashboard, click **Launch instance**.



4. On the launching Instance, Select OPENVPN from AWS Marketplace. Select the very first one as it is free tier eligible and it gives Free Tier Eligibility for 12 months which covers 750 hours of usage per month, so you won't be charged for running the VPN on AWS.



5. Create a new key pair (or use an existing one if you already have one), enter a name, and click create key pair. Then click Launch Instance and wait for the instance to go to running state.



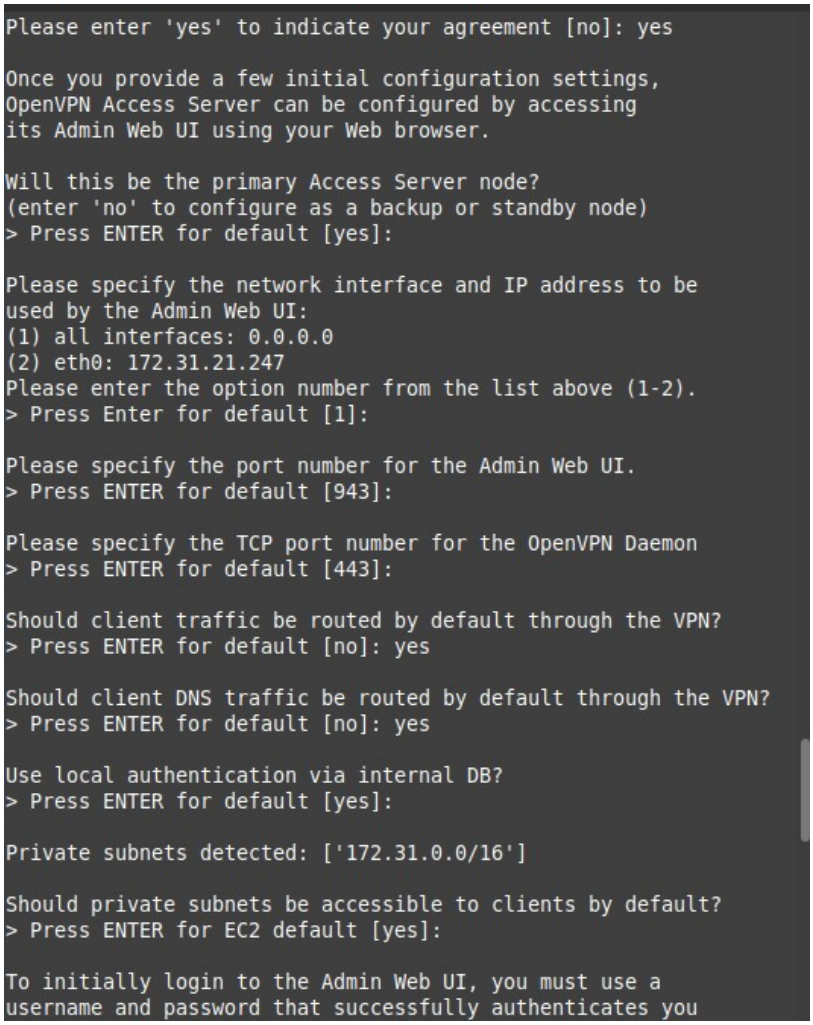
STEP 2 — Configure the Server

- Here I'm using Windows Power Shell, opening my terminal and SSH to my server as openvpnas:

  ssh -i "mandar_vpn.pem" openvpnas@ec2-54-177-121-147.us-west-1.compute.amazonaws.com

- Next, type **yes** for the agreement, then you'll be prompted with how you want to configure your VPN.

```
Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]:

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 172.31.21.247
Please enter the option number from the list above (1-2).
> Press Enter for default [1]:

Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]:

Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]:

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes

Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes

Use local authentication via internal DB?
> Press ENTER for default [yes]:

Private subnets detected: ['172.31.0.0/16']

Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]:

To initially login to the Admin Web UI, you must use a
```



- Type **yes** for the following prompt:

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes

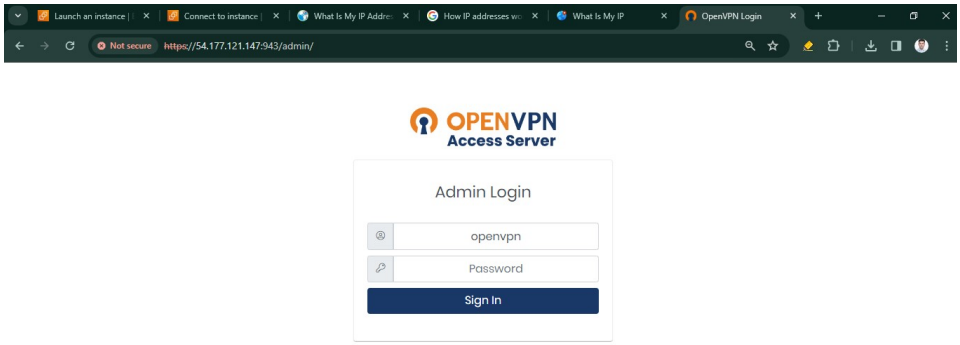
- Just hit enter for the rest to have all the defaults confirmed.
- Once you reached the end, change the password for the user. Enter a new password twice and you're all set.

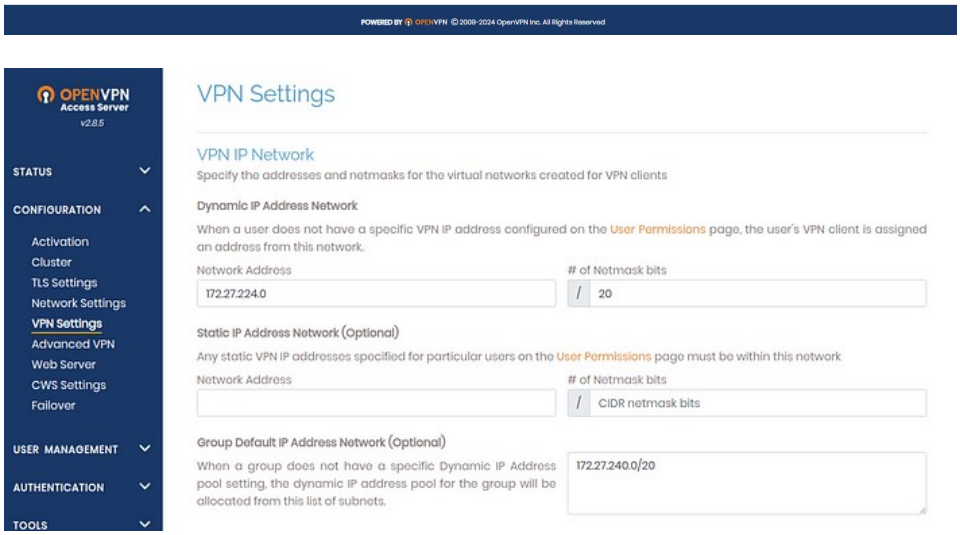
sudo passwd openvpn

- Next, opening a browser window and typing

https://54.177.121.147:943/admin

- Login with openvpn and the password you just set.





- □ Scroll down and then apply the following changes:

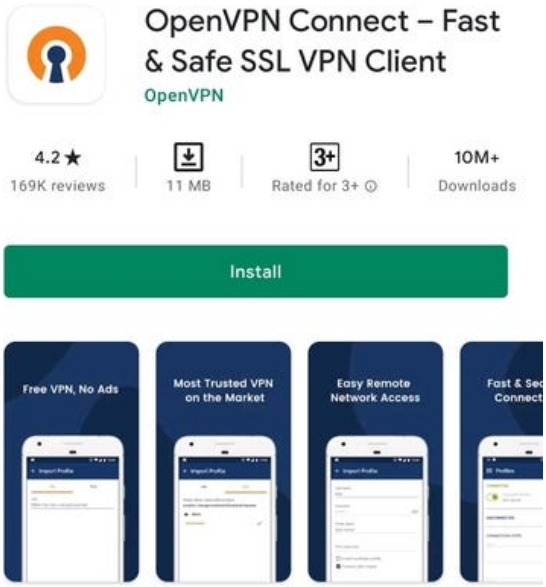
Make sure the toggle for *Should client Internet traffic be routed through the VPN?* is set to **Yes**

- Save the settings and then click on **Update Running Server.**

STEP 3 — Using the VPN

A VPN Client is required that can handle capturing the traffic you wish to send through the OpenVPN tunnel, and encrypting it, and passing it to the OpenVPN server.

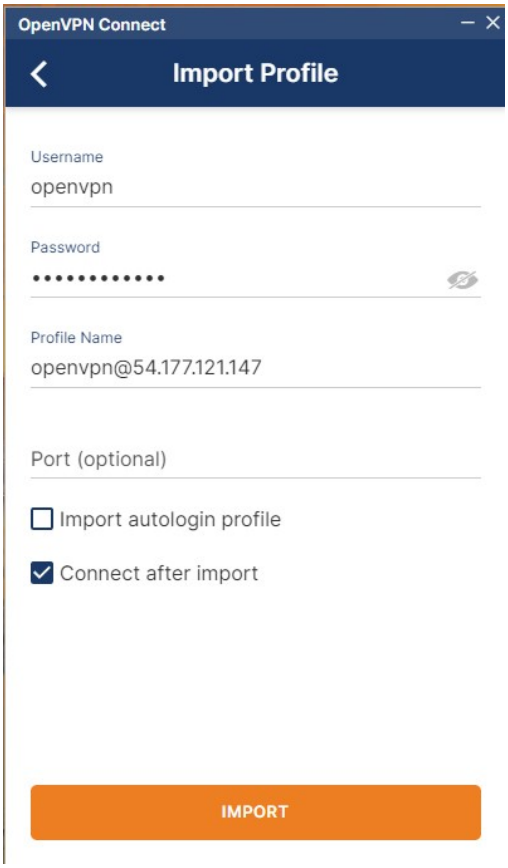
I. To obtain the Official OpenVPN Connect app, either go to the Google Play Store on your Android device or download it from your own pc by typing https:IPv4-Public-IP-address on chrome browser and install the Official OpenVPN Connect app.



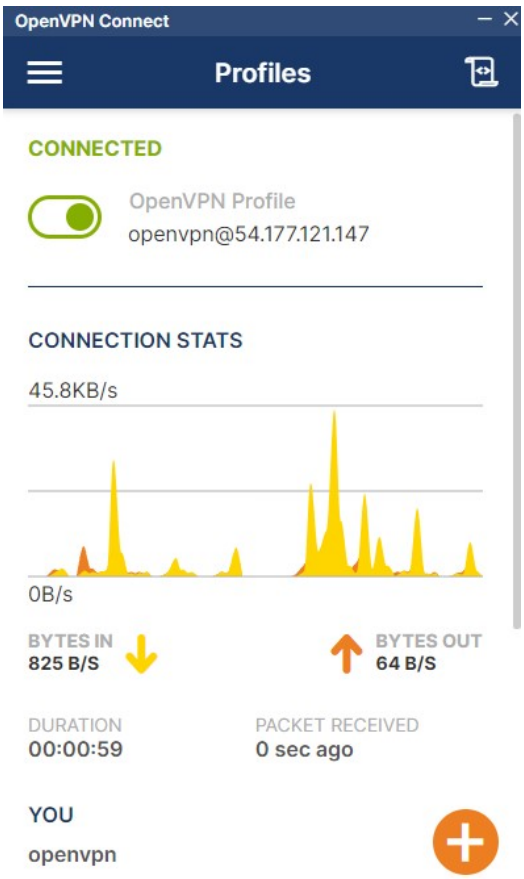
Download it as per your Operating System

II. Open the app & start the import process by entering the IPv4-Public-IP-address of **your running EC2.**

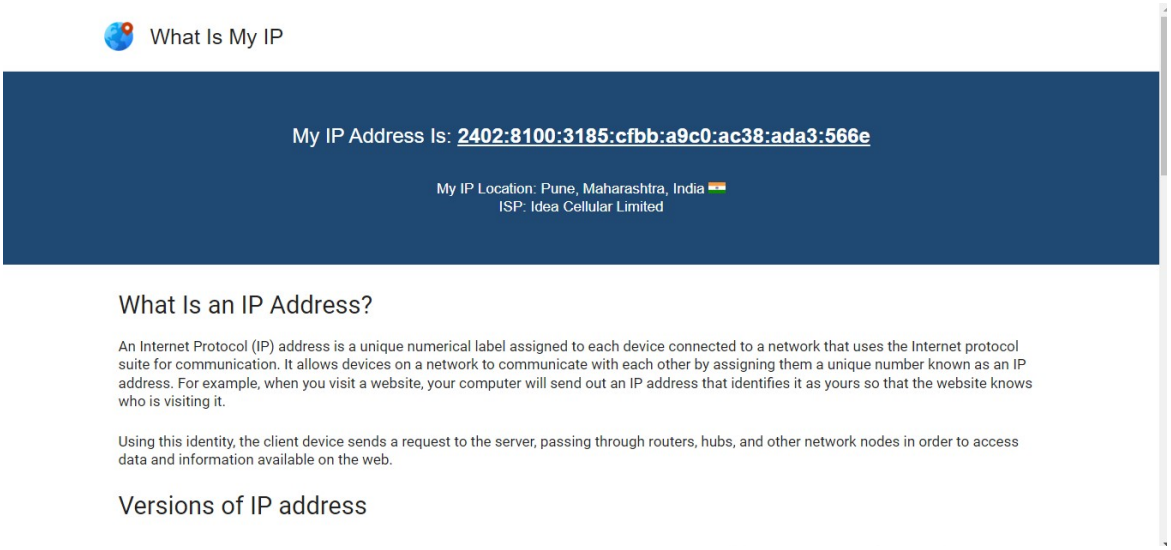
III. Input the username as **openvpn** and the password you had set.



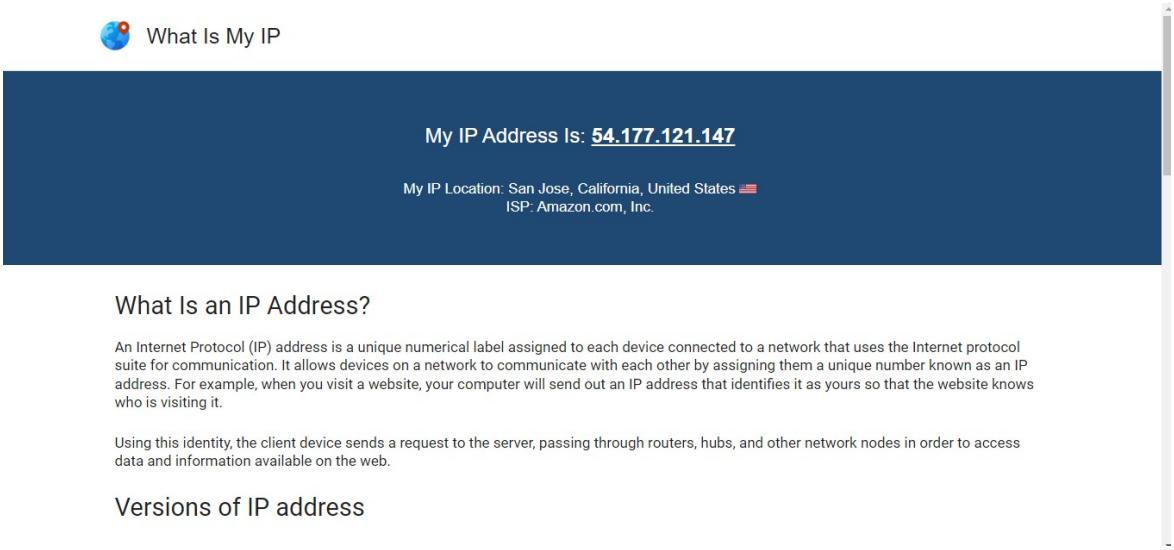
IV. Once the import has completed, we are ready to use the app!



Before connecting to VPN, my IPv4-Public-IP-address was;



Now, after connecting to VPN, my IPv4-Public-IP-address was set as;



So, That is how We can connect to our very own VPN server and enjoy a private surf of the net.