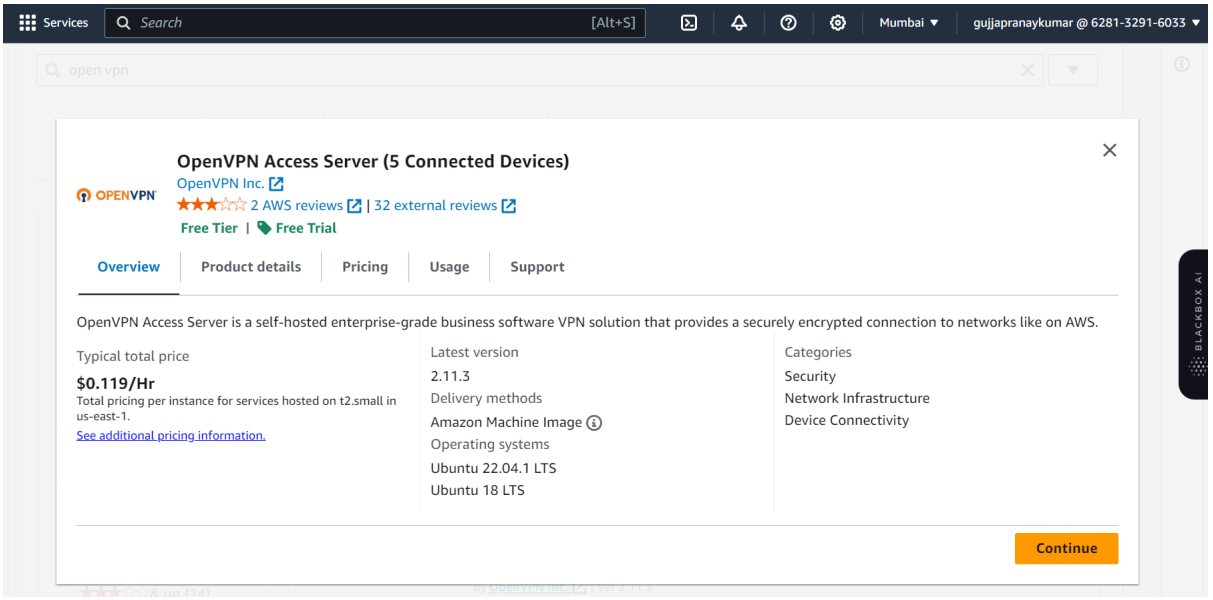
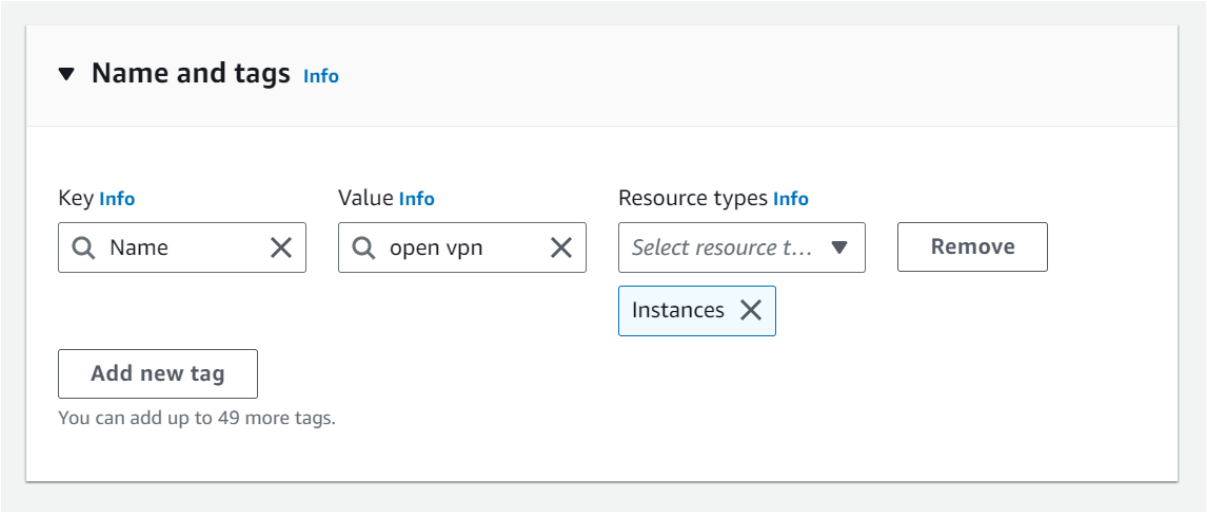
VPN server configuration in AWS

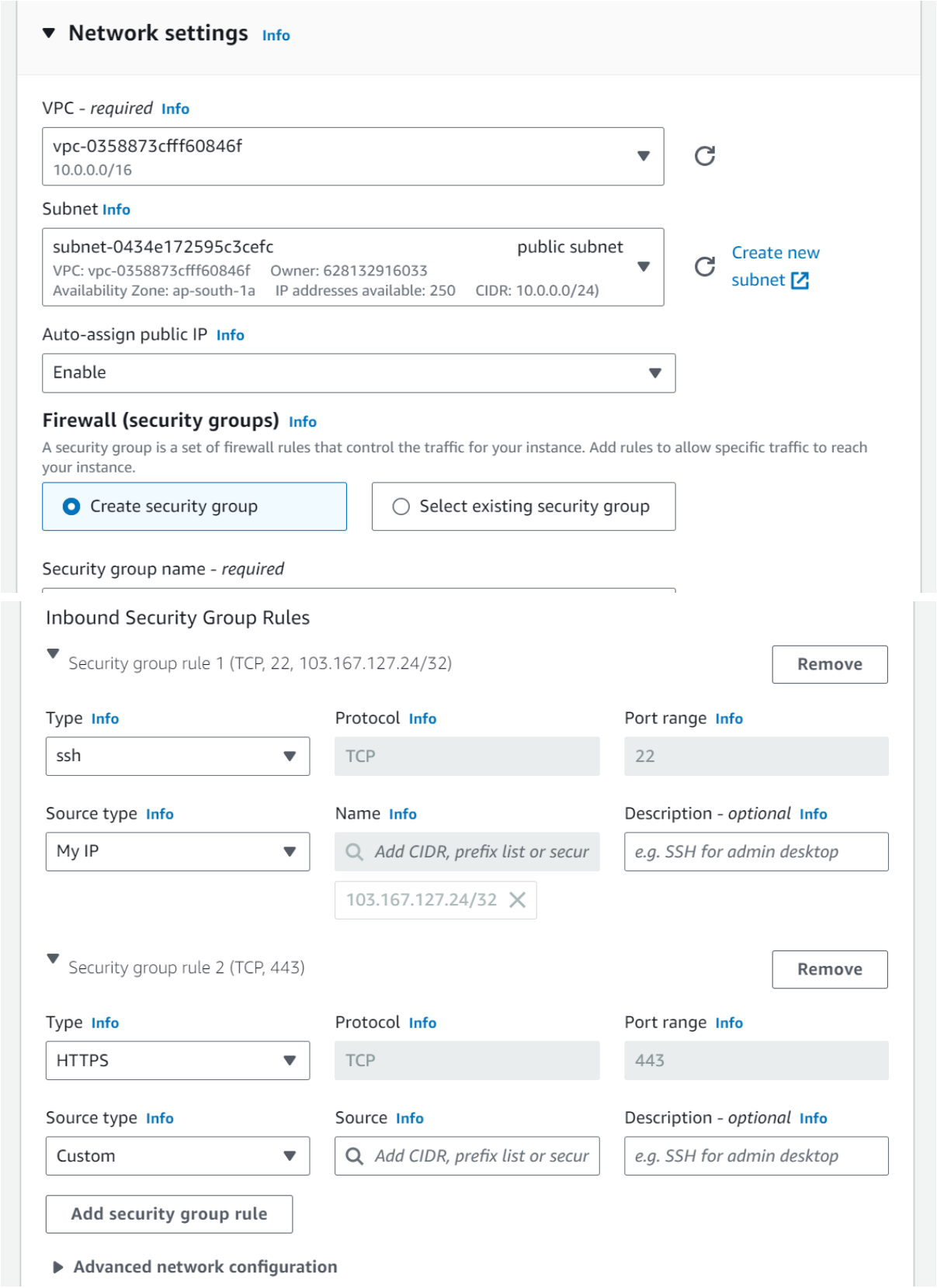
1.Navigate EC2 -> Launch instance

2.In the AWS marketplace search text ”openvpn” you will find the results. Select the first Image “OpenVPN Access Server”
A:



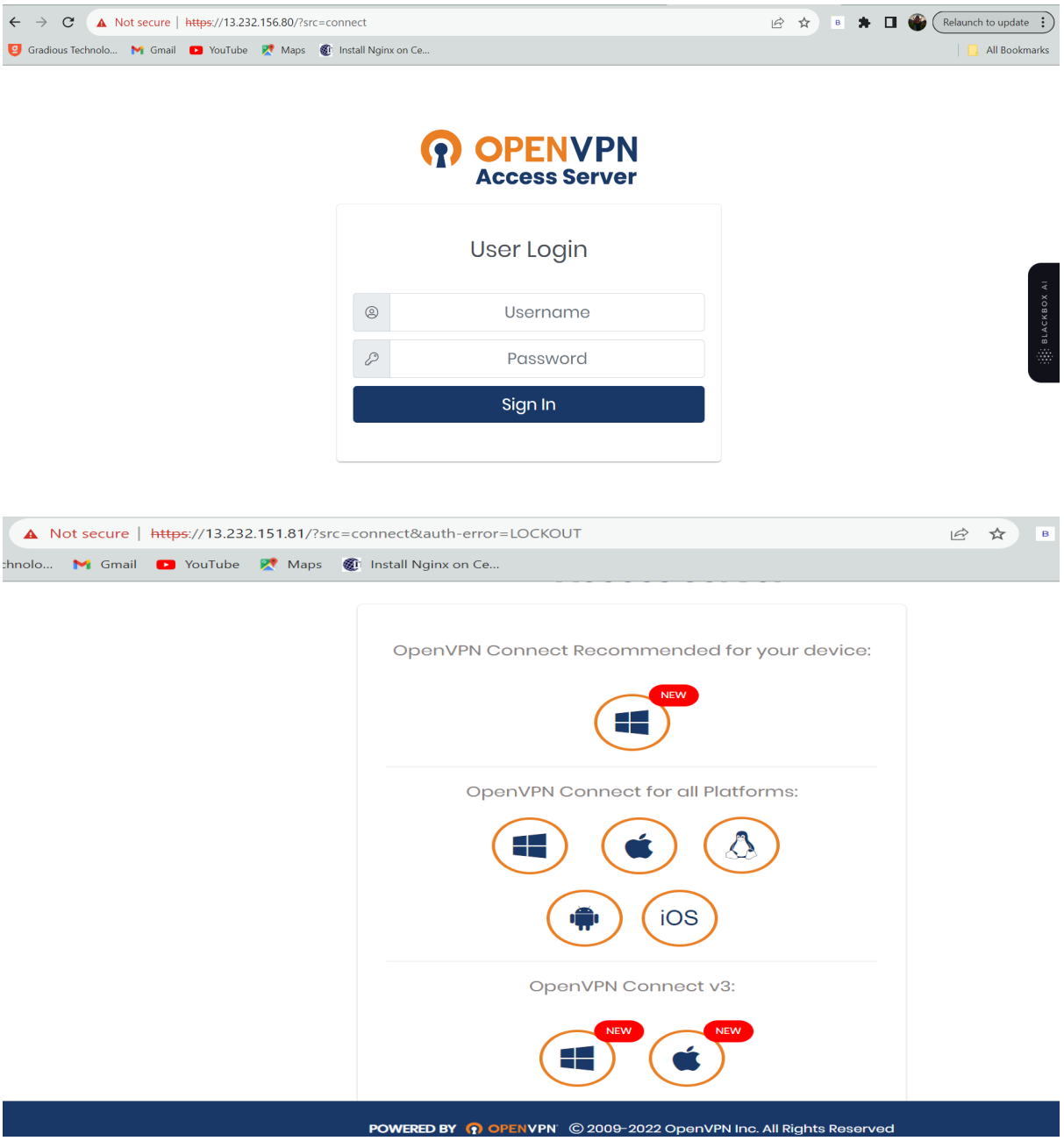

3.In the Instance type select “t2.micro” and click config instance details
4.Select your VPC, select the Public subnet that you have created previously, Auto Assign ip -> enable, host name -> Use subnet setting (Ip name) and click Add storage
5.Storage settings can be default, click Add tags
6.Add tag key as “Name” and provide the value and click configure security group (Note : The default settings allows all traffic for ssh, you can change to “my IP” to be more secure)
Click “Review & Launch” and then click “Launch option” . Choose the existing keypair from the list that you generated and then click “Launch Instance”
8.Verify your Instance is running
A: 3 5 6 7 8






9.Login to the VPN server (Note : you can either ssh from windows/linux machine where you have copied the private key, or you can use putty as well) You need to use username as openvpnas instead of root

A:



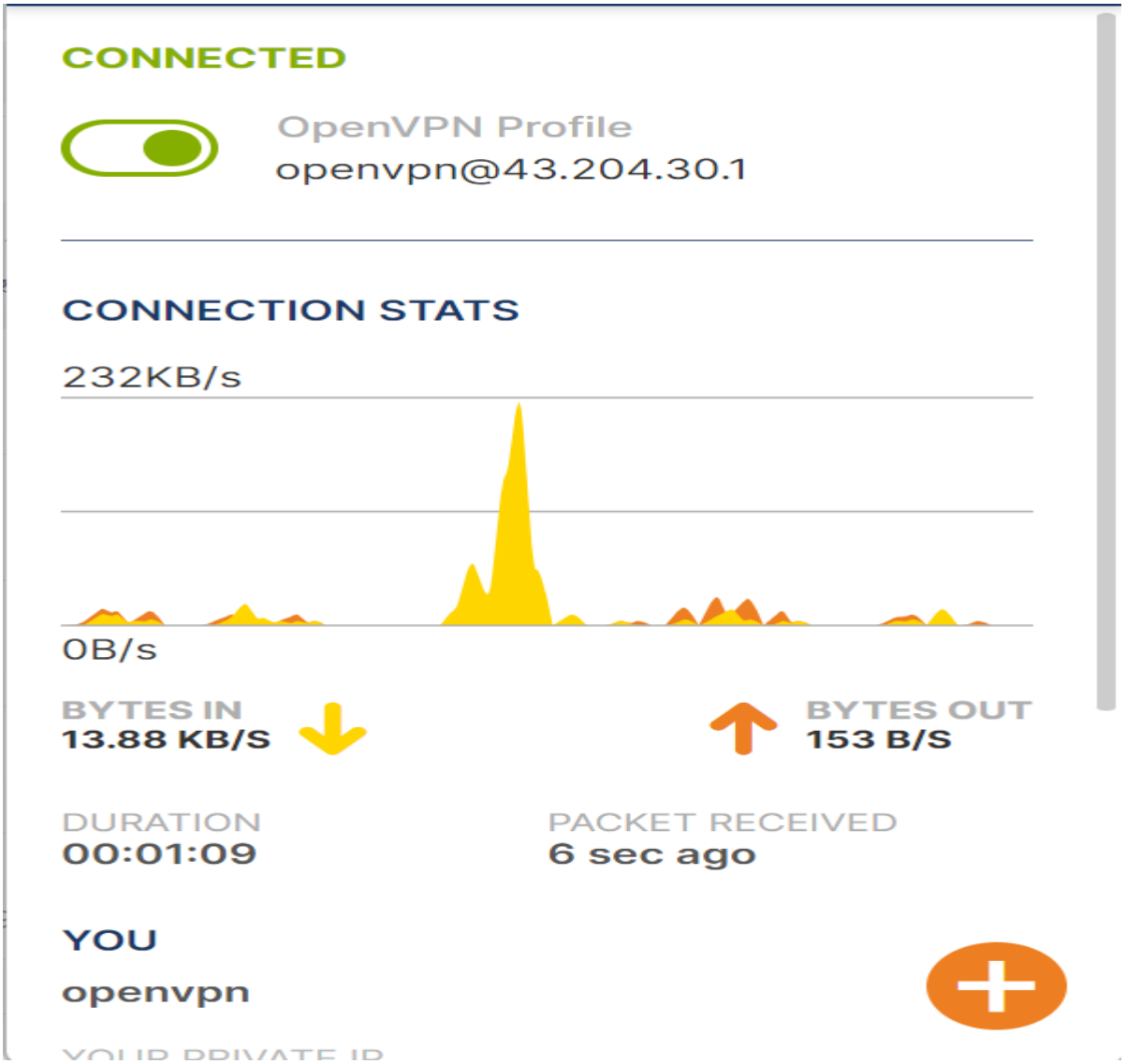

10. Once you try gave your username it prompts for configurations .Follow the screenshots and make changes Will this be the primary Access server node ? - Enter for default : yes
Please specify the network interface - Press Enter for default : 1
Press Enter for default [943] : “click enter”
Press ENTER for the default[443] : “click enter”
Should client traffic be routed by default through VPN? -
Press ENTER for default [no] : yes
Should client DNS traffic be routed by default through VPN? - “yes”
Use local authentication via internal DB? “Click enter”
Should private subnets be accessible to clients by default?
Press enter for EC2 default [yes]: “click enter”

11. Now you are logged in as “openvpnas” user

12. In order to login to the VPN server in GUI you need to login as user “openvpn”. Generate the new password for openvpn user
Run the command “sudo passwd openvpn” and change the password
(note : give a strong password as it needs to be secured)
13. Now login to the web GUI using your public Ip https://”yourvpnip”, login using your openvpn username and password
14. You can download openvpn connect for client if this prompt appears for you, if not You can download it separately(This is for windows) Please refer end of the document if you want to configure OpenVpn client in your Linux Machine
A:

```
openvpnas@ip-10-0-0-52:~$ sudo passwd openvpnas
New password:
Retype new password:
passwd: password updated successfully
openvpnas@ip-10-0-0-52:~$
```

```
[pranay@localhost ~]$ ssh -i "firstinstance.pem" openvpnas@13.232.156.80
Welcome to OpenVPN Access Server Appliance 2.11.3
```

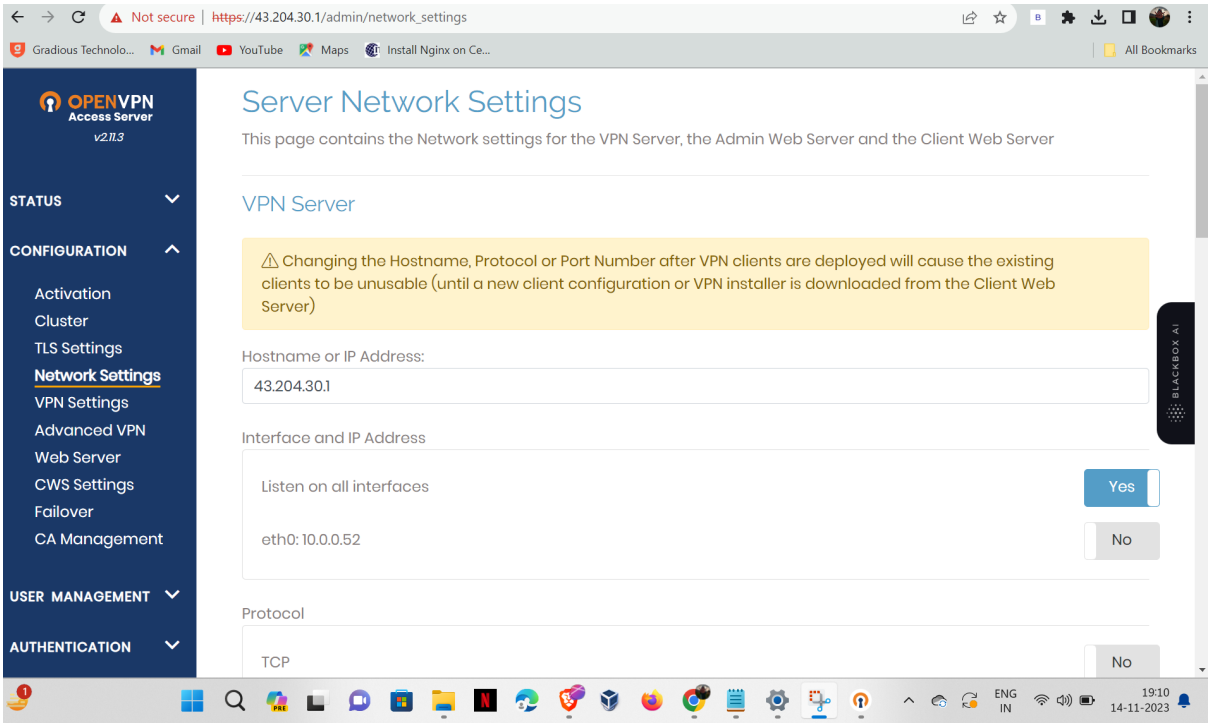



14. You can create customized users in this settings

15. Navigate to configuration -> VPN settings -> configure the routing Specify the private subnets -> you can give your private subnet range in the field
16. Click on save changes
Note : Everytime when your public ip got changed make sure you update here, save the changes and restart the running server
17. Now you need to connect to the VPN network using VPN connect , launch “open vpn connect from your windows” . You need to import the profile using the VPN url. Once you did you can connect using your username password
18. Add the following marked rules in the security group of your private Instance
19. You can now access your private instance from your windows. If you want to access from your linux machine then you need to configure openvpn in it
A: **need to give openvpn private ip in the security groups of the private instance ssh security rule then we can access the private instance**

| Security group rule ID | Port range | Protocol | Source | Securit |
|---|---|---|---|---|
| sgr-075918bf9eb4b4dfc | All | ICMP | 0.0.0.0/0 | launch- |
| sgr-0af74b2a14e3cd4b3 | 80 | TCP | 0.0.0.0/0 | launch- |
| sgr-02e54cb41a709f7a2 | 22 | TCP | 10.0.0.52/32 | launch- |

Here it is the openvpn public ip



```
C:\Users\model>ssh -i C:\Users\model\Downloads\firstinstance.pem ec2-user@10.0.2.106
The authenticity of host '10.0.2.106 (10.0.2.106)' can't be established.
ED25519 key fingerprint is SHA256:l51QTxMO78aOy/oGxdS81Lo+rqsUBBuWR3Z/ZZ5cUV4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.106' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Nov 14 15:05:52 2023 from 10.0.0.52
[ec2-user@ip-10-0-2-106 ~]$ exit
logout
Connection to 10.0.2.106 closed.
```