OPENVPN INSTALLATION ON AWS IN VPC

Create an Ubuntu 14 Linux instance with the following security group rules.

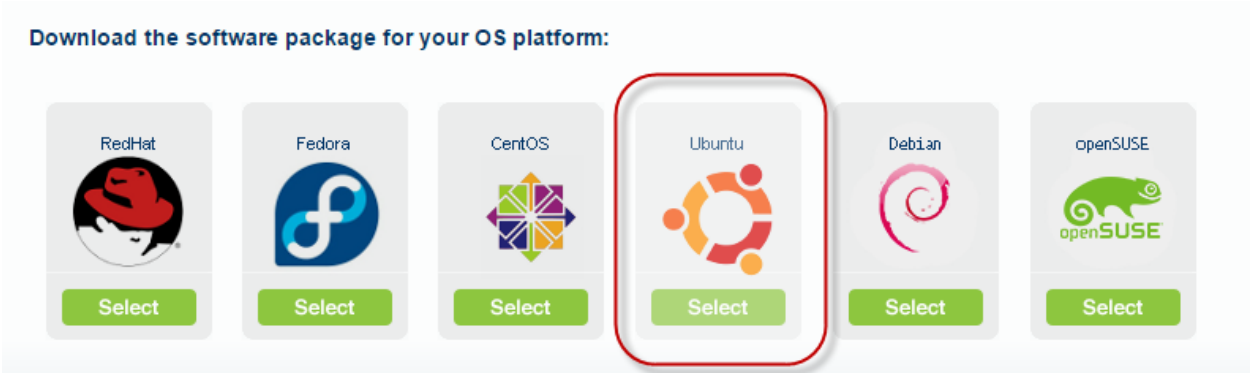
Description | **Inbound** | Outbound | Tags

Edit

Type	Protocol	Port Range	Source
Custom UDP Rule	UDP	1194	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
Custom TCP Rule	TCP	943	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

Then go to the openvpn access server downloads page and download the package for respective Linux server.

Download URL: https://openvpn.net/index.php/access-server/download-openvpn-as-sw.html




```
root@ip-10-100-2-121:~# wget http://swupdate.openvpn.org/as/openvpn-as-2.1.2-Ubuntu14.amd_64.deb
--2016-09-18 19:54:55--  http://swupdate.openvpn.org/as/openvpn-as-2.1.2-Ubuntu14.amd_64.deb
Resolving swupdate.openvpn.org (swupdate.openvpn.org)... 104.24.0.59, 104.24.1.59
Connecting to swupdate.openvpn.org (swupdate.openvpn.org)|104.24.0.59|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31902098 (30M) [application/octet-stream]
Saving to: 'openvpn-as-2.1.2-Ubuntu14.amd_64.deb'

100%[=========================================================================================

2016-09-18 19:54:57 (16.8 MB/s) - 'openvpn-as-2.1.2-Ubuntu14.amd_64.deb' saved [31902098/3190209
```

Once downloaded use dpkg command to install the openvpn access server.

```
root@ip-10-100-2-121:~# dpkg -i openvpn-as-2.1.2-Ubuntu14.amd_64.deb
Selecting previously unselected package openvpn-as.
(Reading database ... 51172 files and directories currently installed.)
Preparing to unpack openvpn-as-2.1.2-Ubuntu14.amd_64.deb ...
Unpacking openvpn-as (2.1.2-Ubuntu14) ...
Setting up openvpn-as (2.1.2-Ubuntu14) ...
The Access Server has been successfully installed in /usr/local/openvpn_as
Configuration log file has been written to /usr/local/openvpn_as/init.log
Please enter "passwd openvpn" to set the initial
administrative password, then login as "openvpn" to continue
configuration here: https://10.100.2.121:943/admin
To reconfigure manually, use the /usr/local/openvpn_as/bin/ovpn-init tool.

Access Server web UIs are available here:
Admin  UI: https://10.100.2.121:943/admin
Client UI: https://10.100.2.121:943/
```

Once installed, change the password for openvpn user.

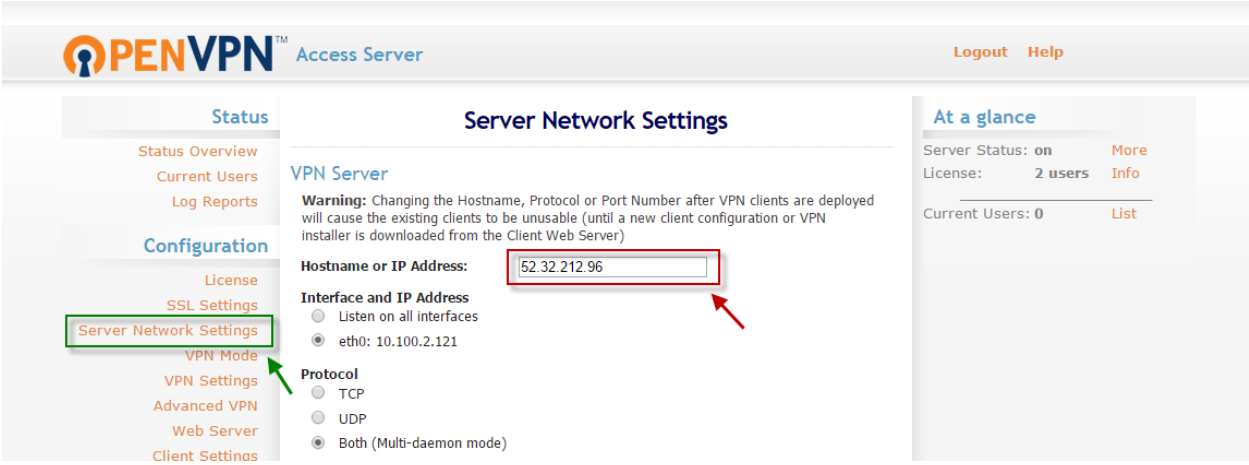
```
root@ip-10-100-2-121:~# passwd openvpn
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Then open vpn admin console by opening like below.

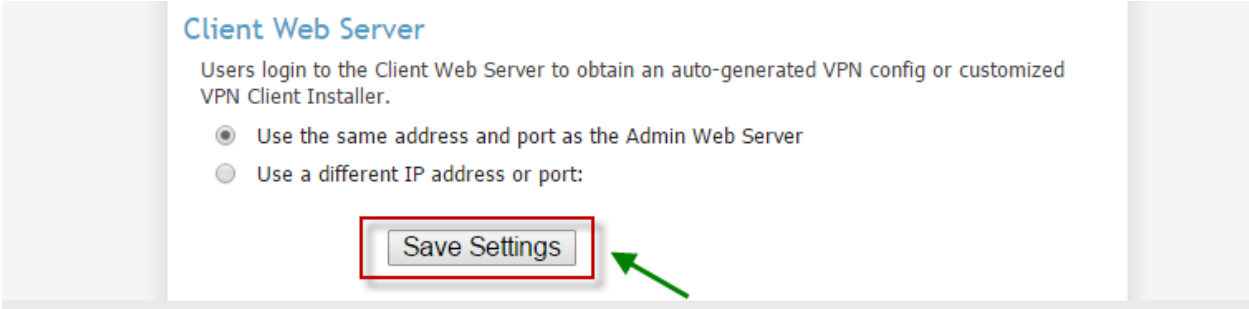
https://server-ip-address/admin

specify username as openvpn and password as which you have just changed above and click login.

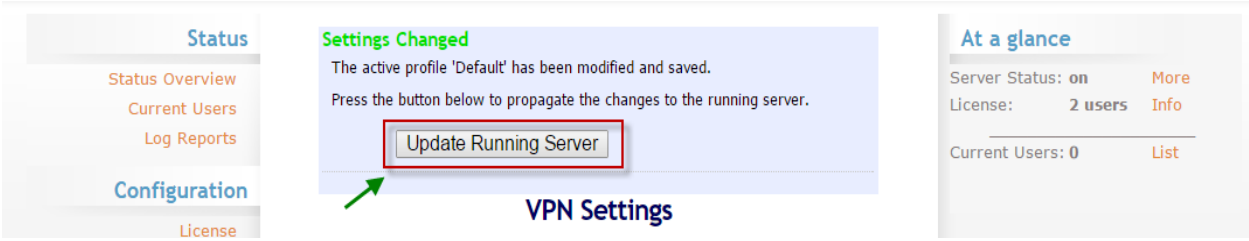
Once logged in, go to the Server Network Settings from the left pane, change the Hostname or IP Address to the Public IP address which you got from AWS.



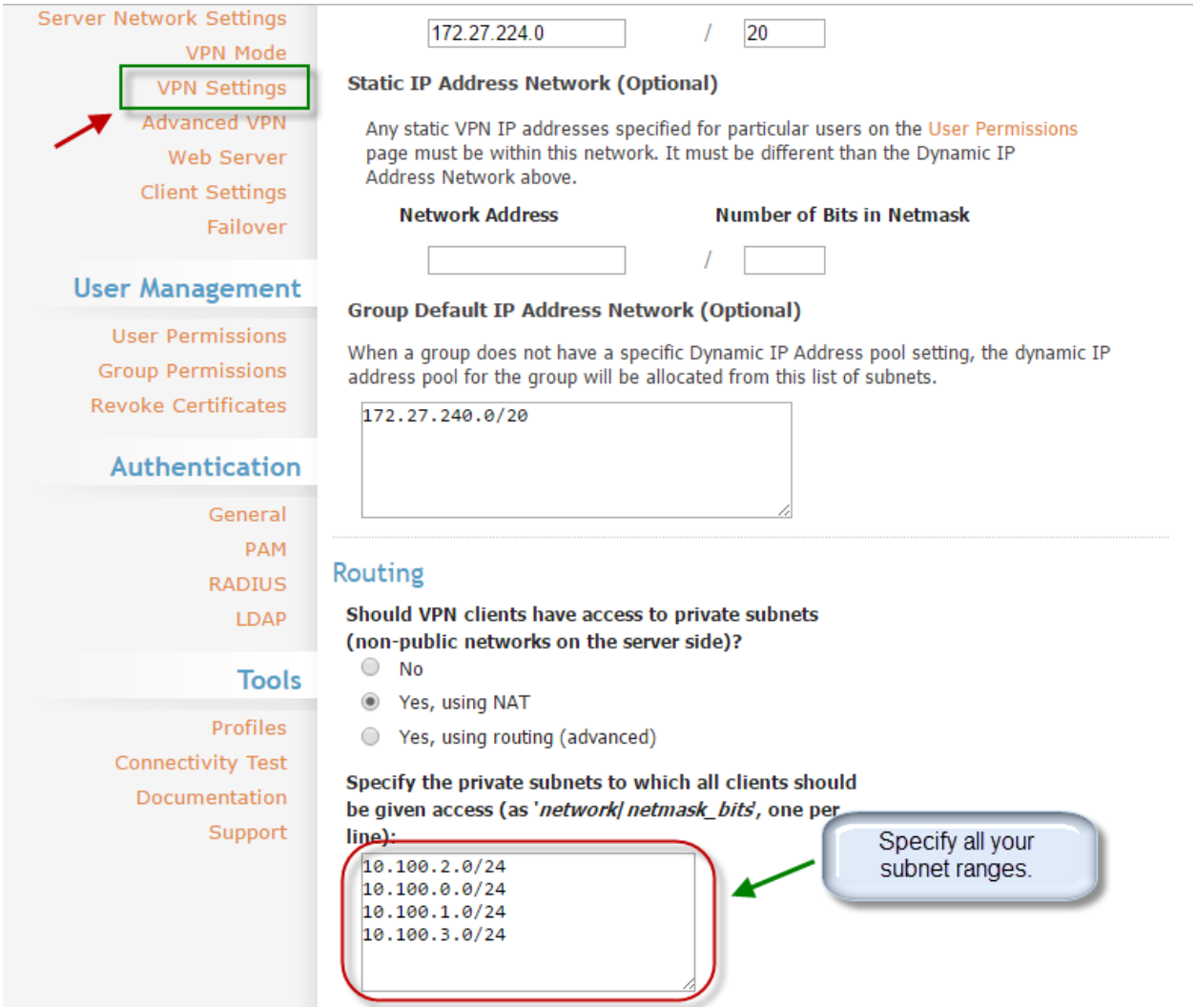
Next, go to below the page, and choose save settings to save the settings.

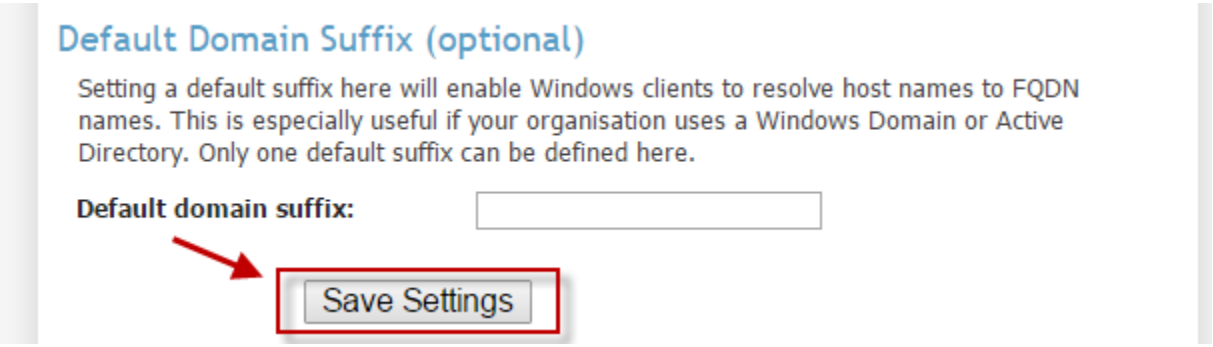


Next, click on Update Running Server to take in to effect the changes which you saved.

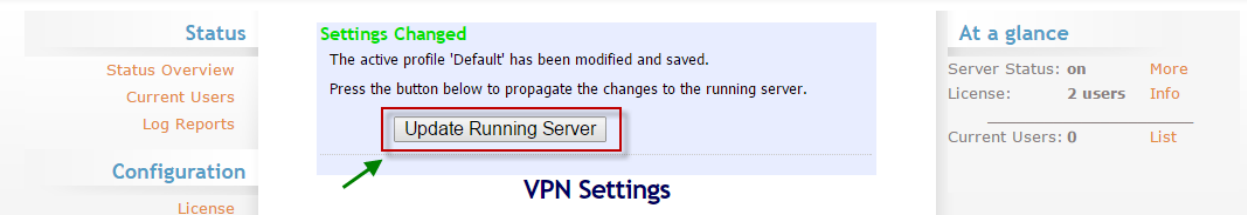


Next go to VPN settings page from the left pane. Go to Routing settings and specify all your Public and Private subnet IP Address ranges in the text box. Next go to end of the page choose save seetings.



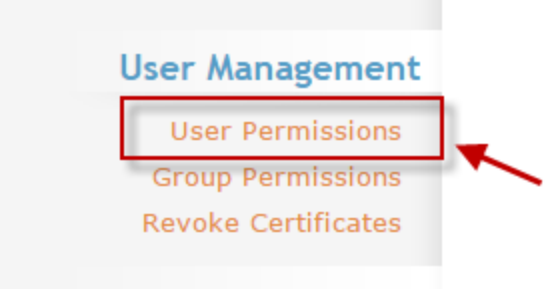


Next, click on Update Running Server to make changes to take in to effect.



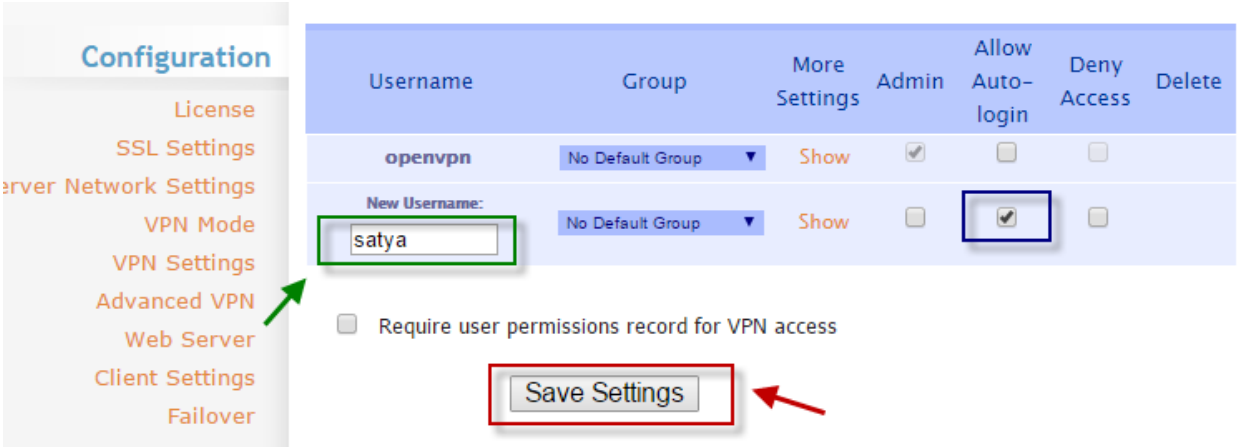
Next, we will go with user creation and giving users VPN access.

Go to User Permissions from the left pane.

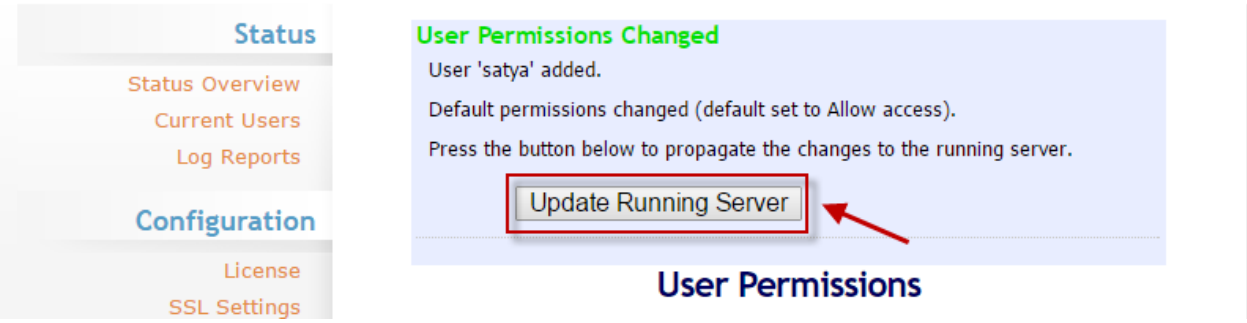


Create a user in Linux and add a password to the user.

Specify a username, click Allow Auto login, and click on save settings.

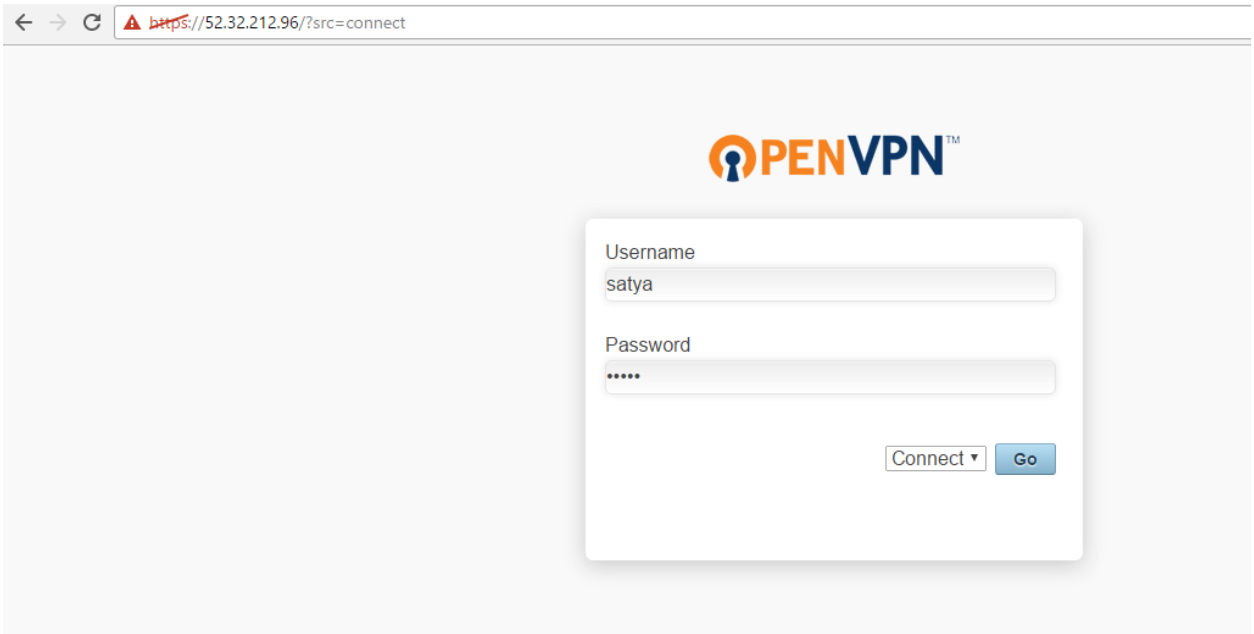


Run Update Running Server to effect changes which you saved.

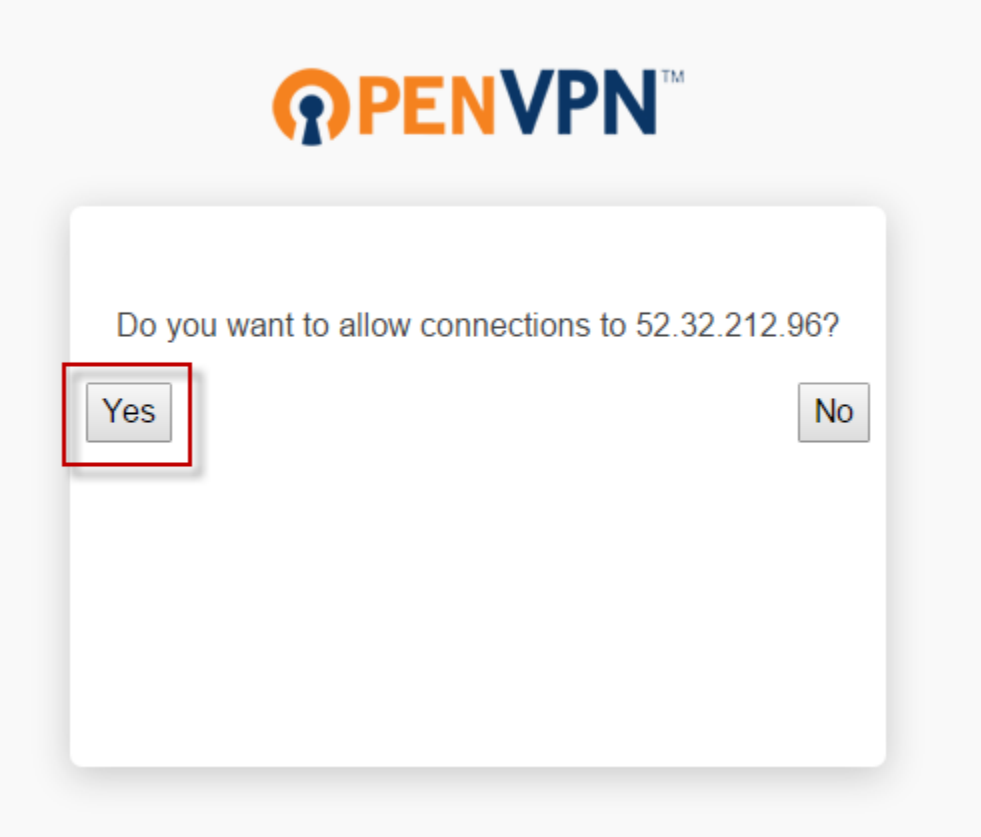


Next, Open below URL and specify user and password credentials then choose Go to connect.

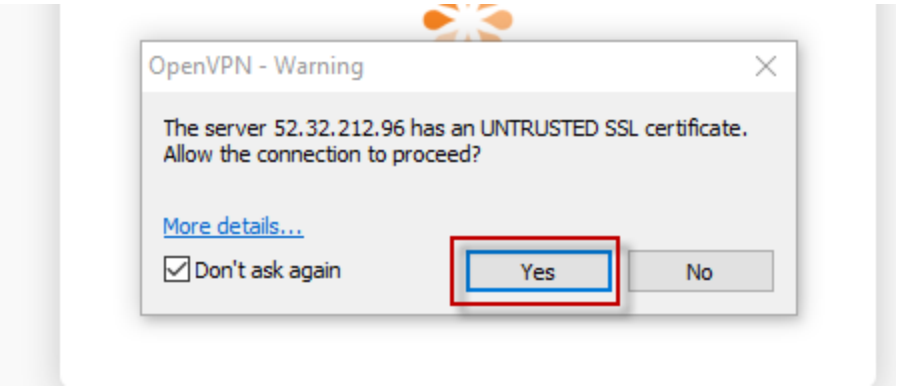
Web URL: https://your-server-ip-here/



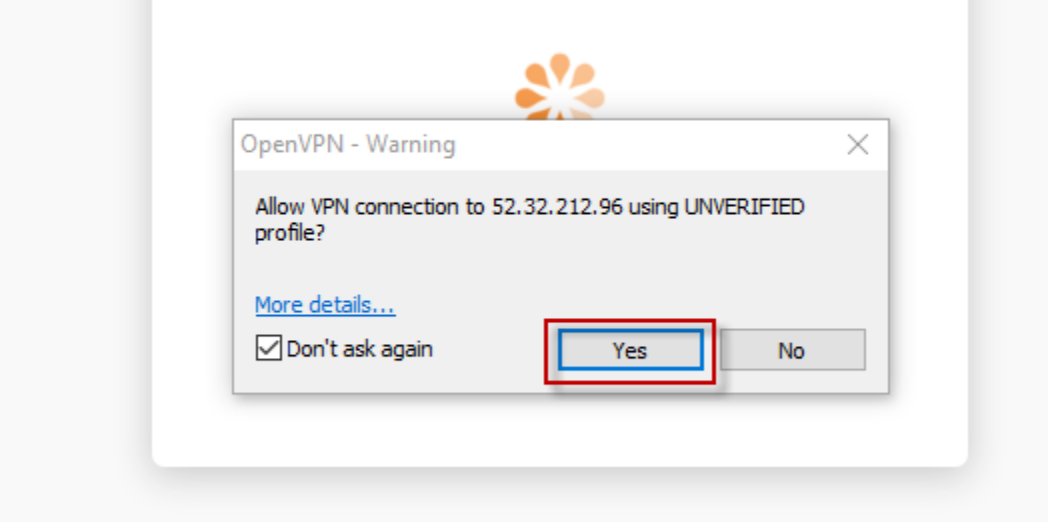
Next choose Yes to allow connection.



Next, choose yes to use untrusted SSL cert.



Next, choose yes to Allow VPN connection.



Once done, you will be presenting with page like below.

Now you can connect to the Private subnet instances over VPN secure connection.