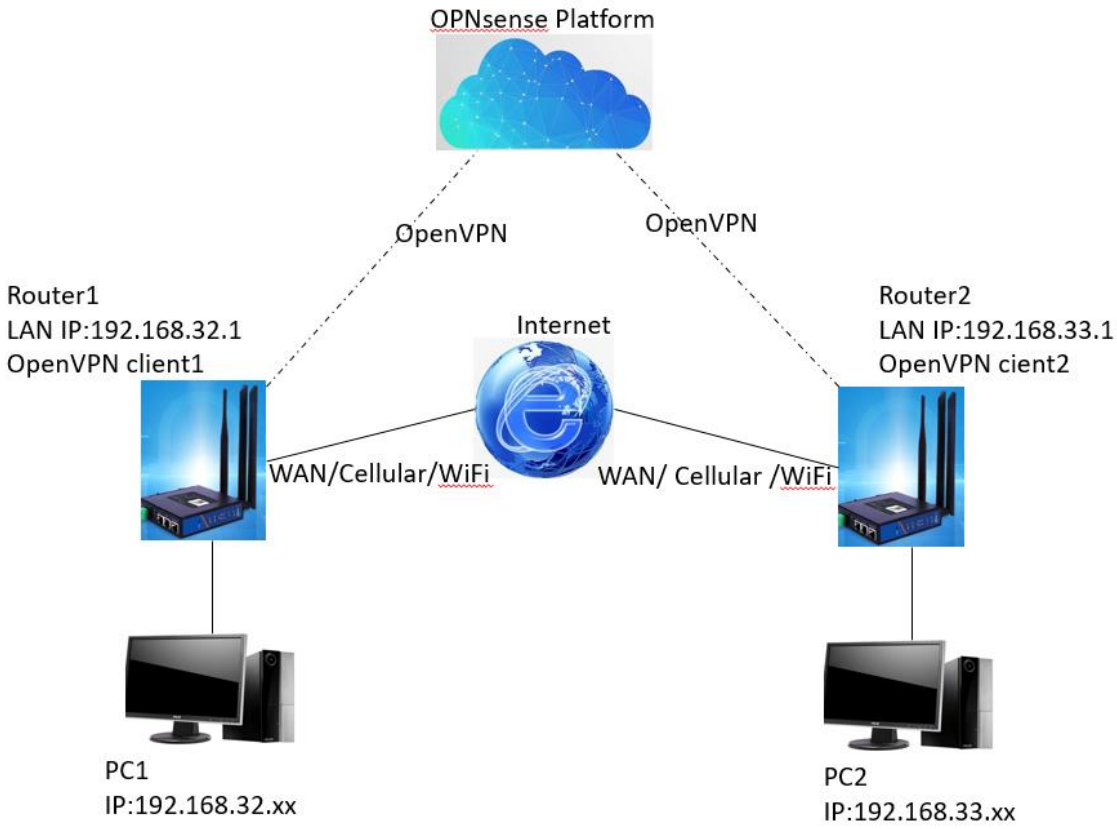
PUSR Routers Connect to OPNsense Server

1. Login the OPNsense server

In this case, the OPNsense server IP is 60.208.44.205. If you have your own OpenVPN server, you can login your server with correct username and password.

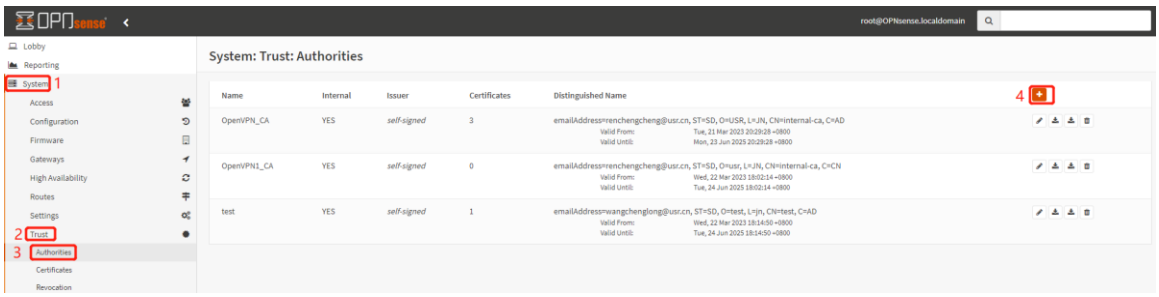
In this case, we configure the OpenVPN server and the OpenVPN clients to achieve the function as the following picture:



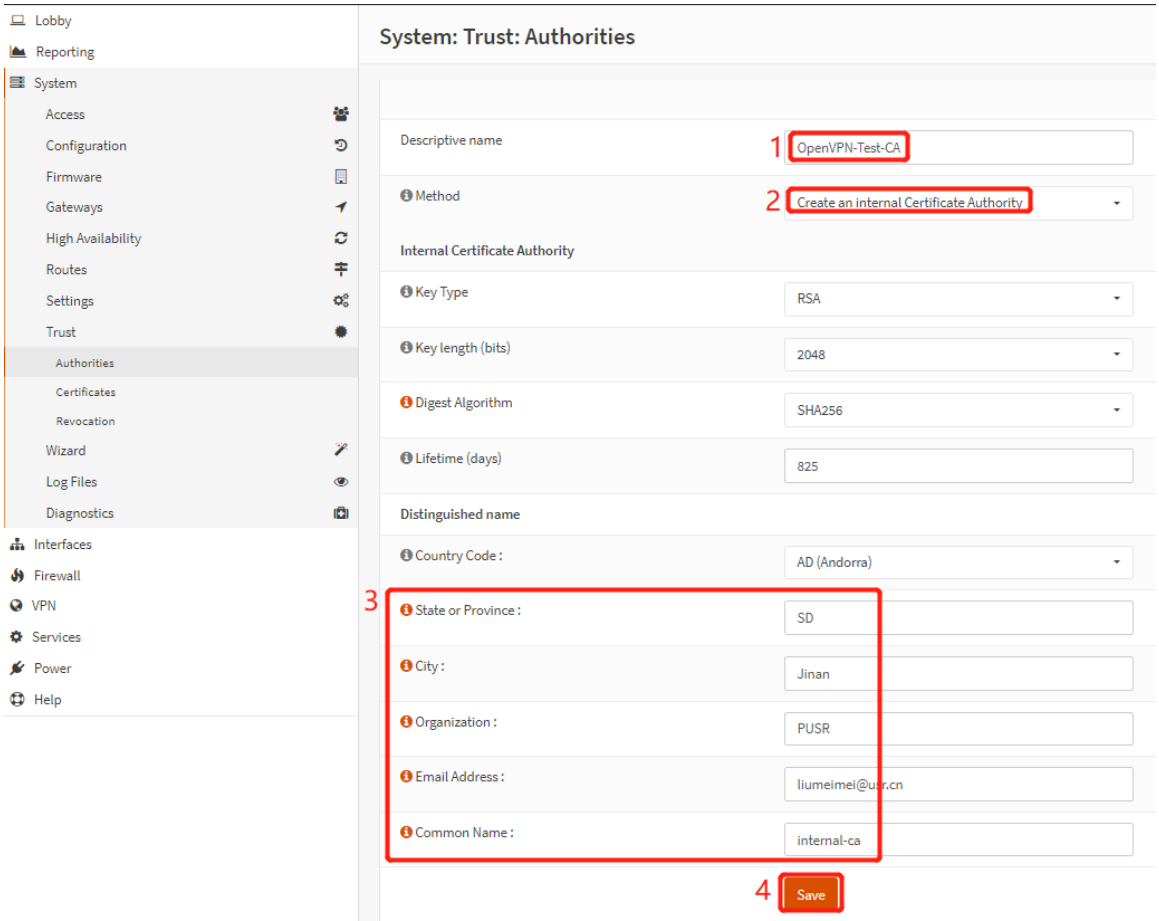
2. Create authorities and certificates

2.1 Create a CA certificate.

System->Trust->Authorities



Edit authorities:



2.2 Create Server Certificate

System->Trust->Certificates

1>Method: Select “Create an internal Certificate”,

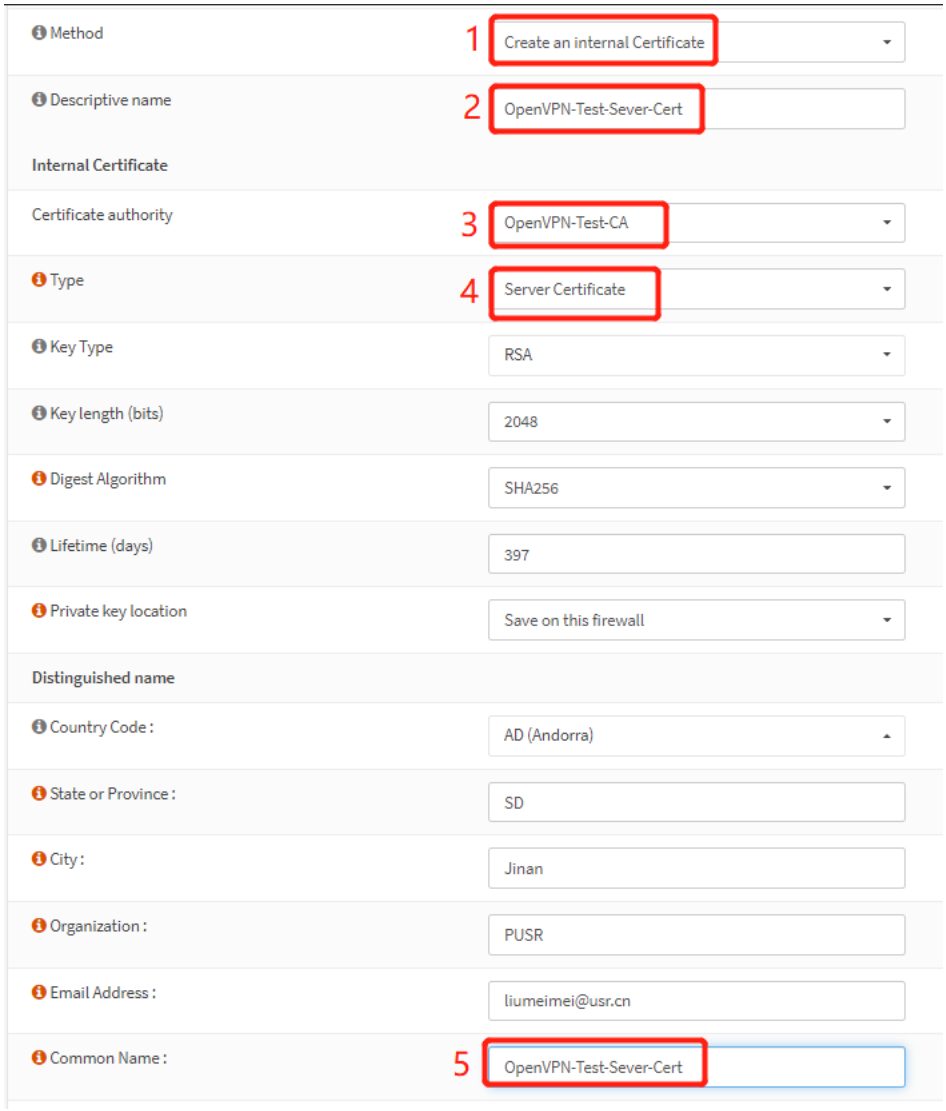
2>Enter the descriptive name of the certificate,

3>Certificates authority: Select the “OpenVPN-Test-CA” which is created in the Step 2.1,

4>Type: Server Certificate,

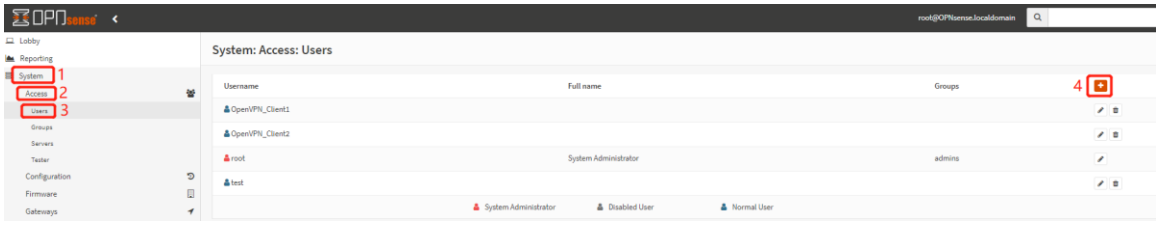
5>Enter the common name,

6>Click “Save”.



2.3 Add users and create user certificates

System->Access->Users



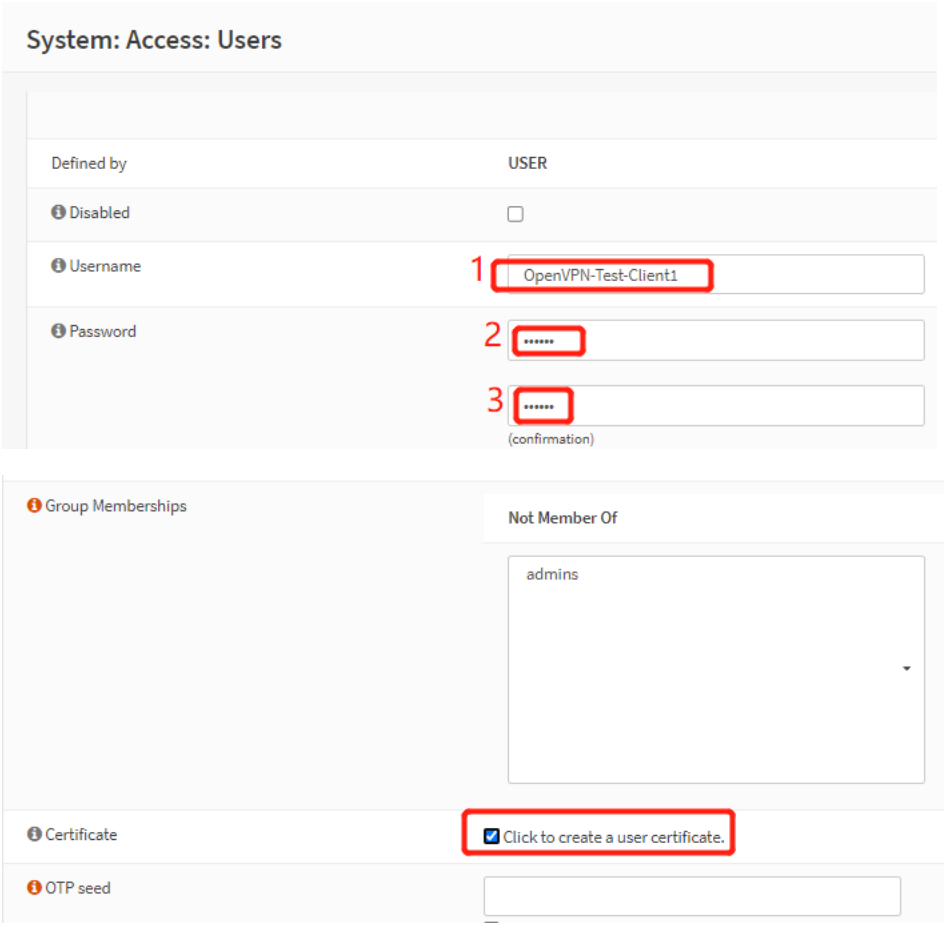
1>Enter custom username,

2>Enter the password,

3>Confirm the password,

4>Check the “Click to create a user certificate”,

5>Click “Save” button.



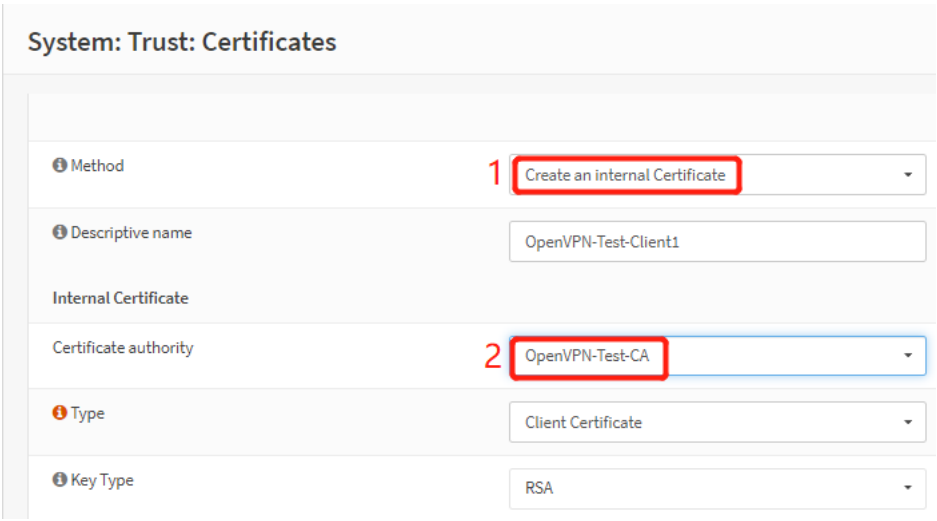
After clicking the “Save” button, it will automatically redirect to a new page as following, in this page:

1> Method: Create an internal Certificate,

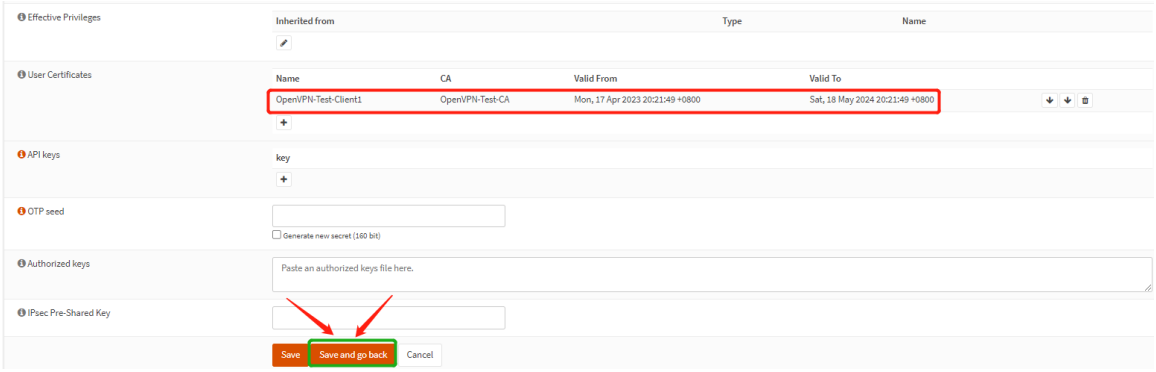
2> Certificates authority: Select the “OpenVPN-Test-CA” which is created in the Step 2.1,

3> The other parameters stay the default,

4> Click “Save” button.



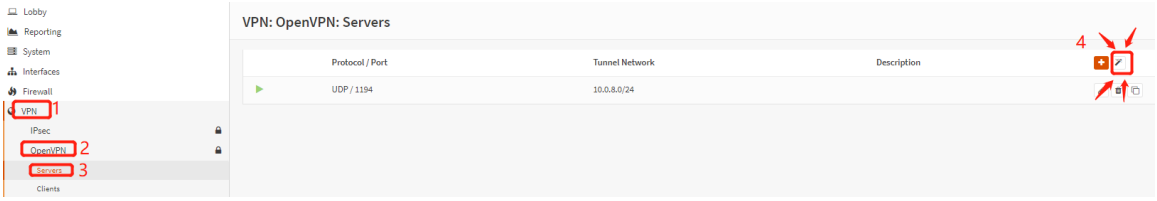
After saving the parameters, it will return to the user accessing page, and we can see the user certificate listed. Then we need to click “Save and go back”.



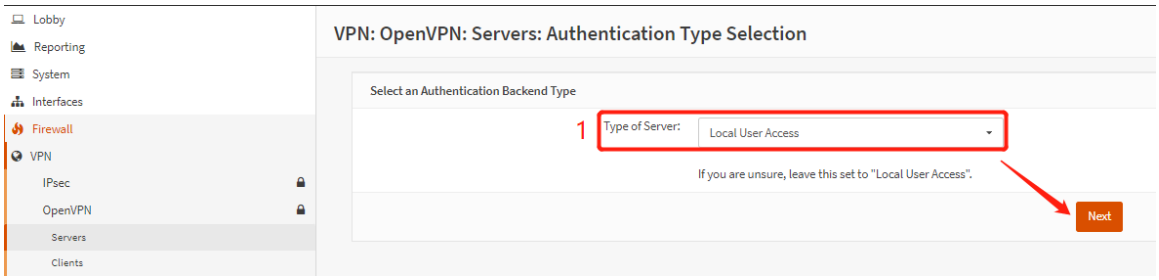
In this case, we need 2 users and certificates, and the second one can be added using the same steps.

2.4 Configure OpenVPN Server

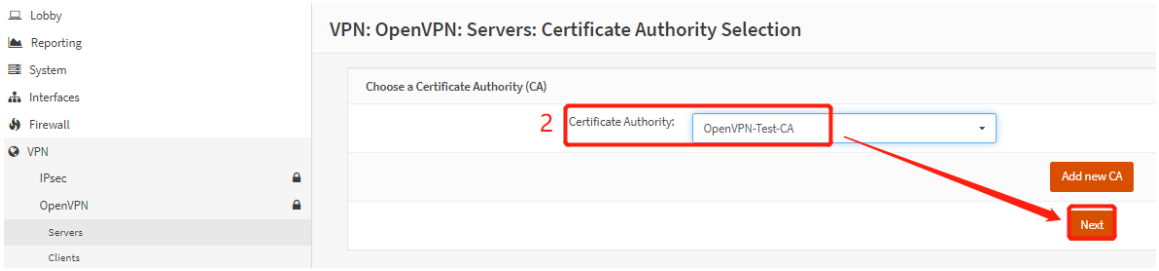
VPN->OpenVPN->Servers->Use a wizard to setup a new server



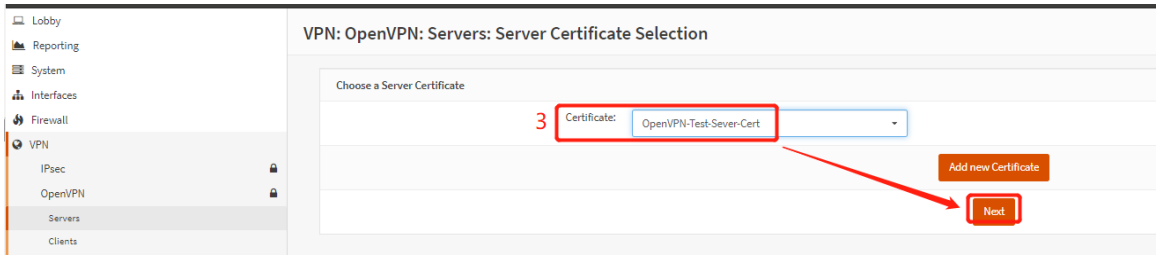
1>Type of Server: Local User Access



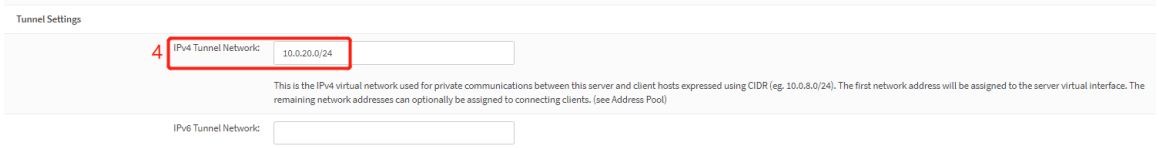
2>Certificate Authority: “OpenVPN-Test-CA” created in Step 2.1



3>Certificate: “OpenVPN-Server-Test-Cert” created in Step 2.2

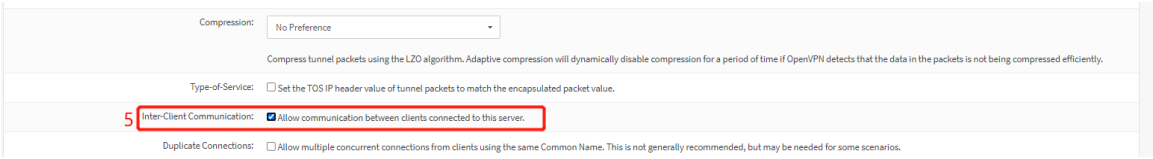


4>Tunnel Settings->IPv4 Tunnel Network: 10.0.20.0/24

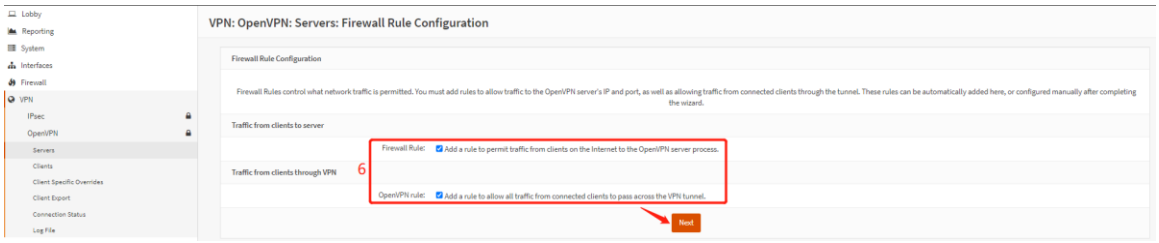


5>Tunnel Settings->Inter-Client Communication

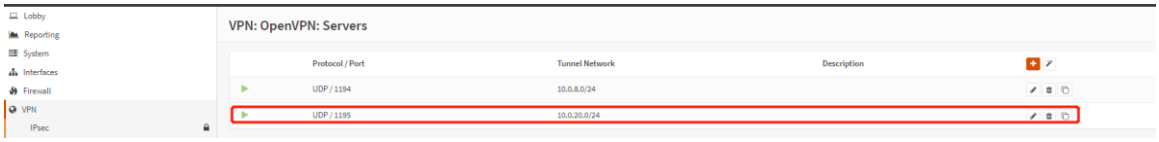
Tips: The other parameters in “Server Setup” page can stay default.



6>Firewall and OpenVPN rules need be enabled in this case.

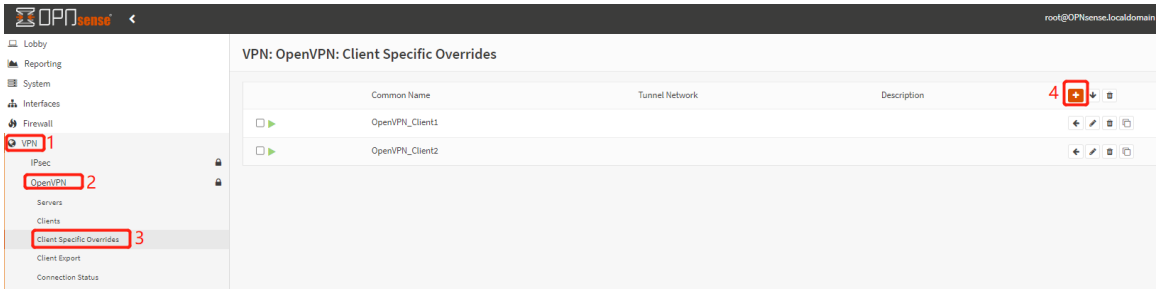


7>Click “Finished” button, the servers are listed. “UDP / 1195” is the server we added.



2.6 Configure the OpenVPN client and subnet

VPN->OpenVPN->Client Specific Overrides



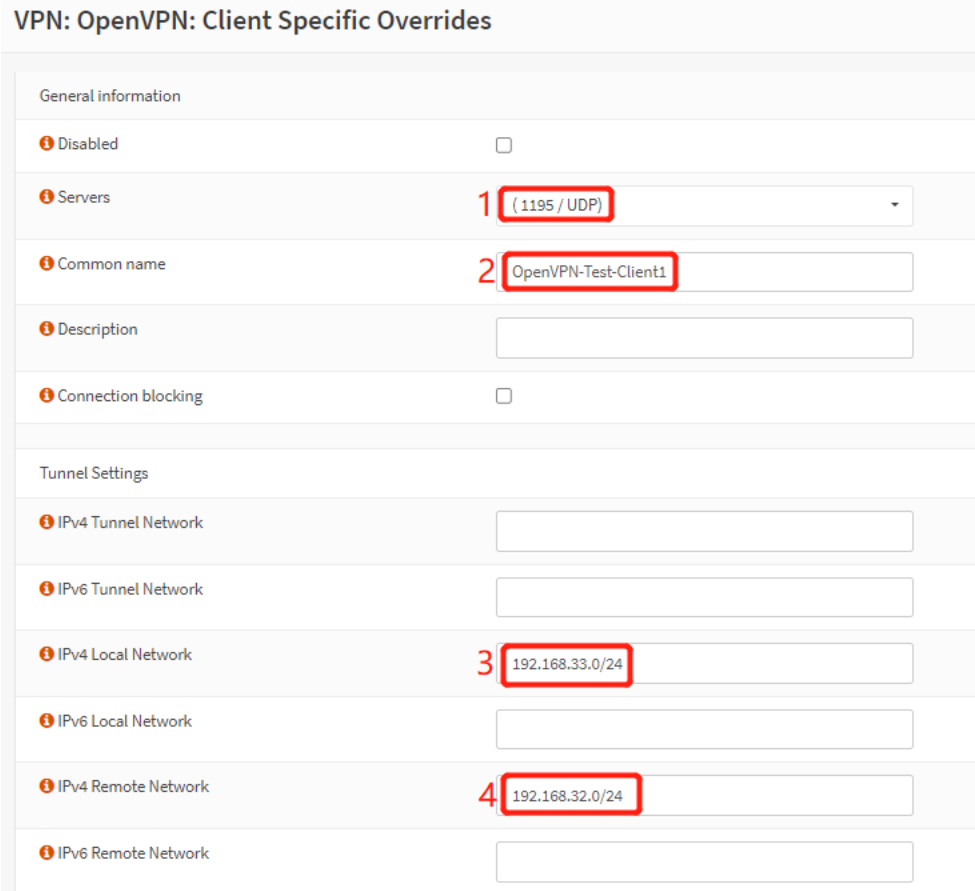
1>Servers: Select “1195 / UDP” added in chapter 2.4,

2>Common name: This name should be kept consistent with the first username in chapter 2.3,

3>IPv4 Local Network: 192.168.33.0/24, the second router’s LAN IP,

4> IPv4 Remote Network: 192.168.32.0/24, the first router’s LAN IP,

5>Click “Save”.



In this case, we need 2 clients, and the second one can be added using the same steps.

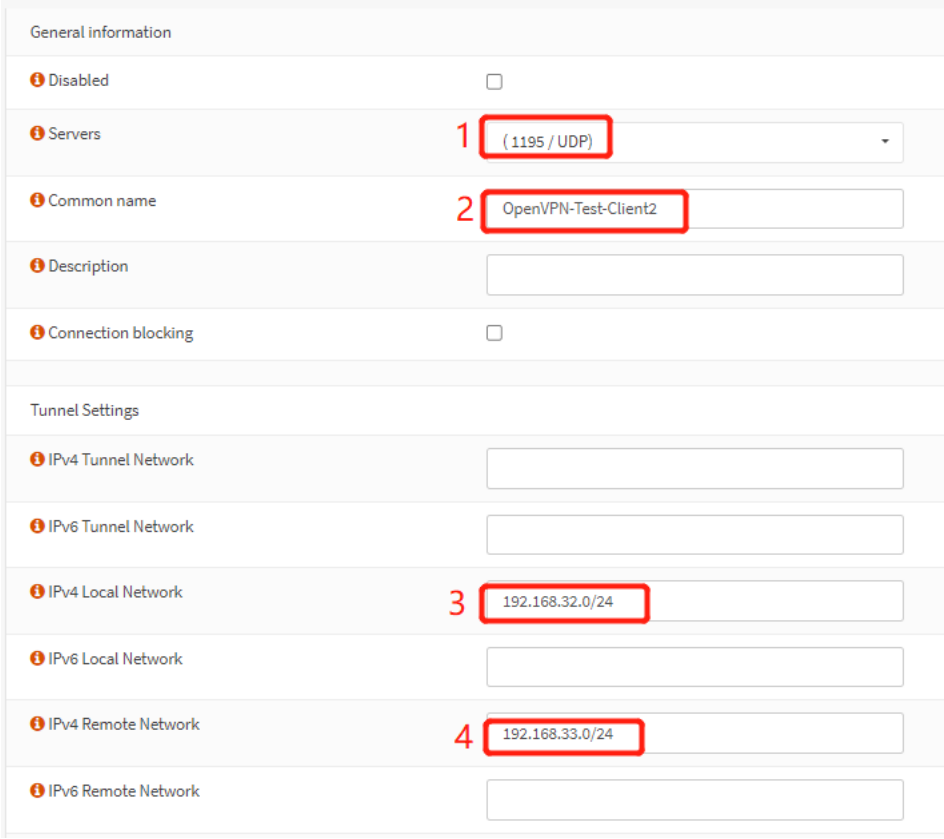
1>Servers: Select “1195 / UDP” added in chapter 2.4,

2>Common name: This name should be kept consistent with the second username in chapter 2.3,

3>IPv4 Local Network: 192.168.32.0/24, the first router’s LAN IP,

4> IPv4 Remote Network: 192.168.33.0/24, the second router’s LAN IP,

5>Click “Save”.



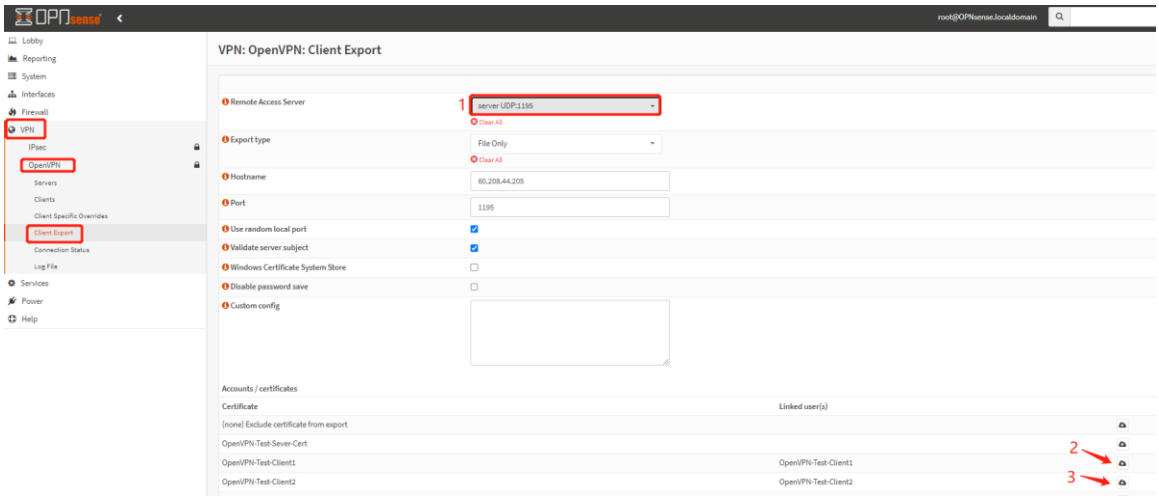
2.7 Export the OpenVPN client package

VPN->OpenVPN->Client Export

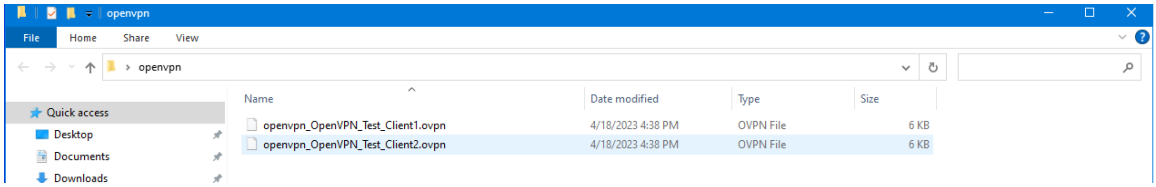
1> Remote Access Server: Server UDP:1195,

2>Download the package of Client1,

3> Download the package of Client2.



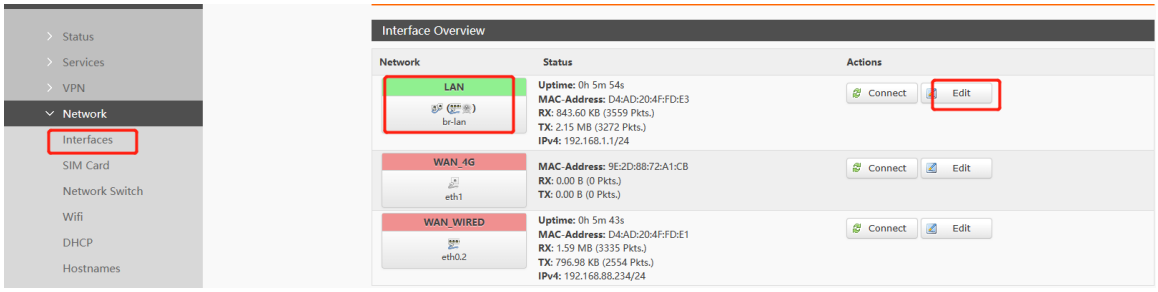
The downloaded file.

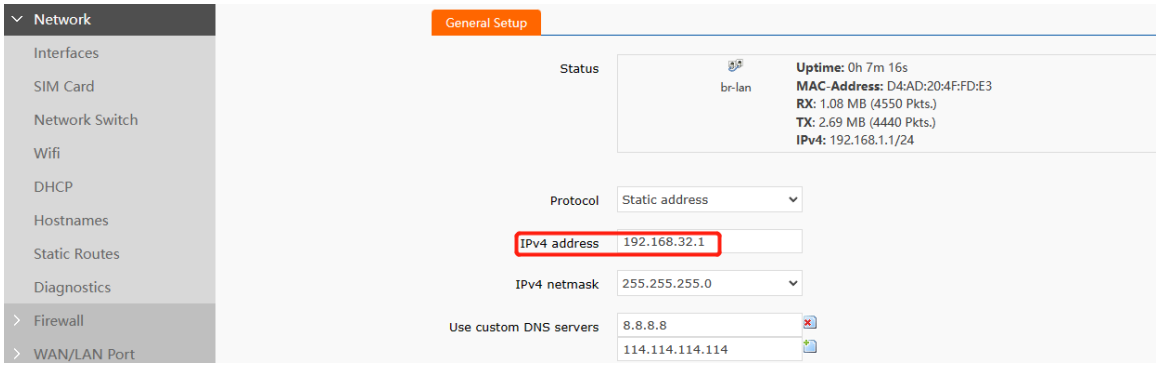


3. Configure router's parameters

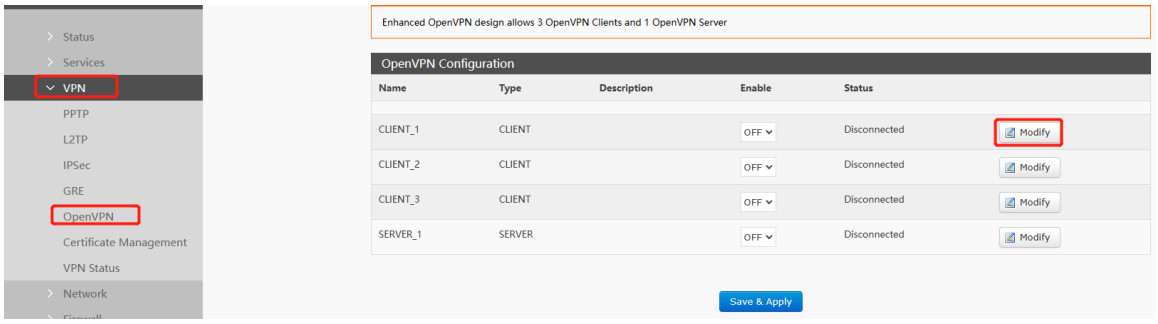
3.1 Configure the first router as OpenVPN Client1

1>Change LAN IP to 192.168.32.1





2>Modify the OpenVPN parameter,

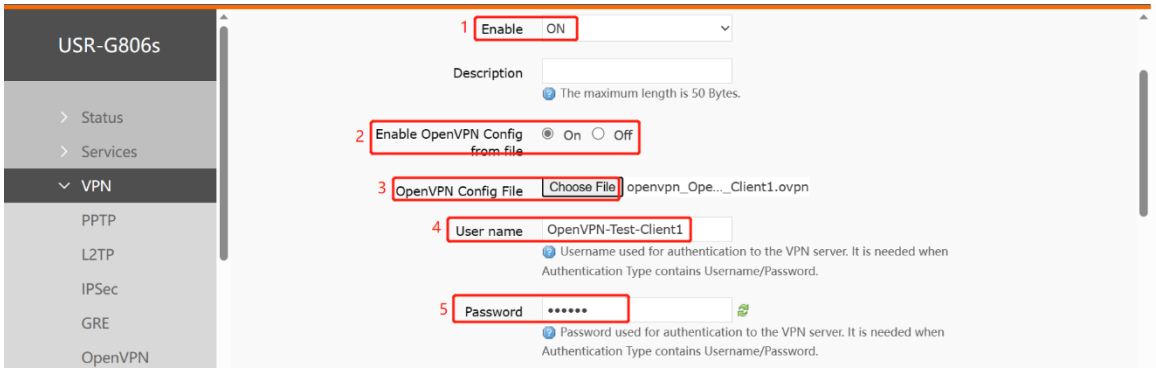


3>OpenVPN Config File: choose the "client1.ovpn" file downloaded in Chapter 2.7,

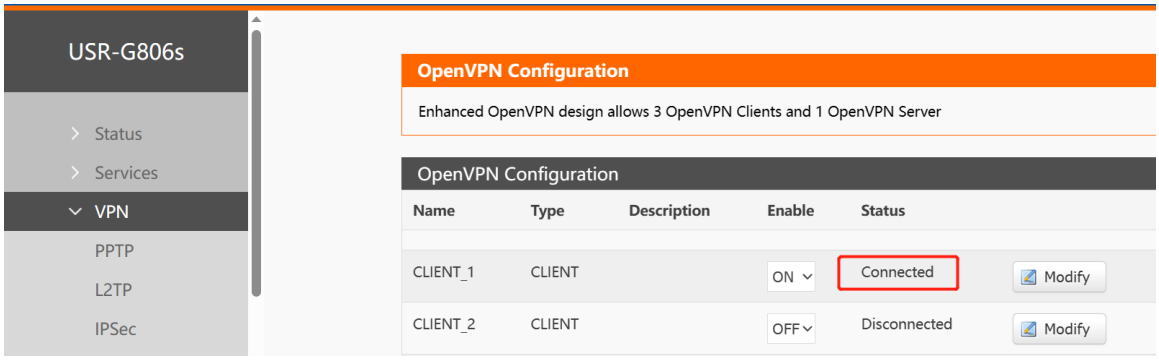
4>User name: The entered name of the OpenVPN-Test-Client1 in Chapter2.3,

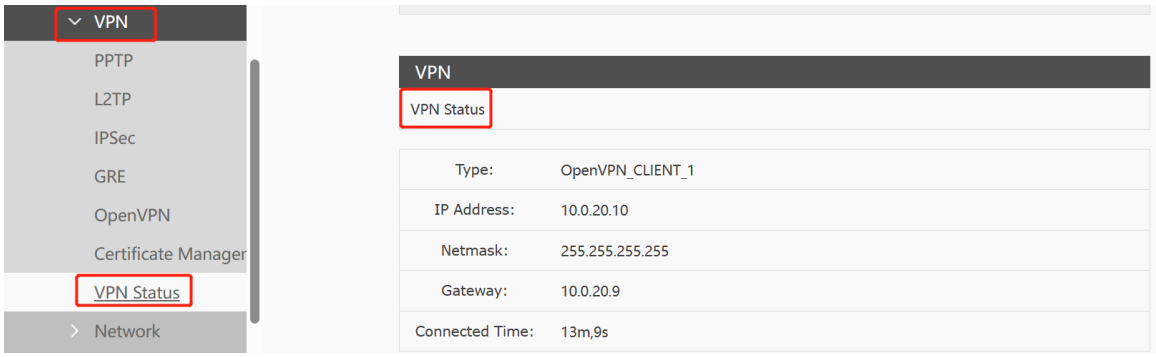
5>Password: The password of the OpenVPN-Test-Client1 in Chapter 2.3,

6>Click “Save & Apply” button.

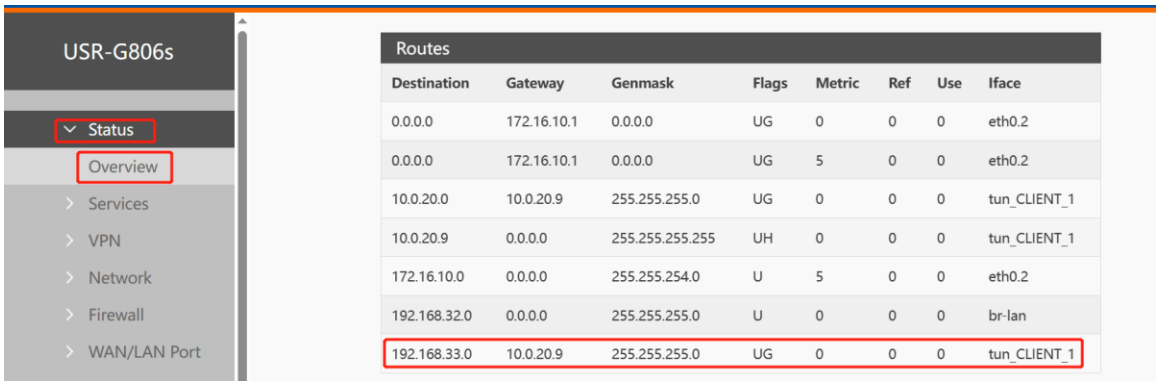


7>The OpenVPN connection is connected, and more details of the connection can be check in VPN status page.



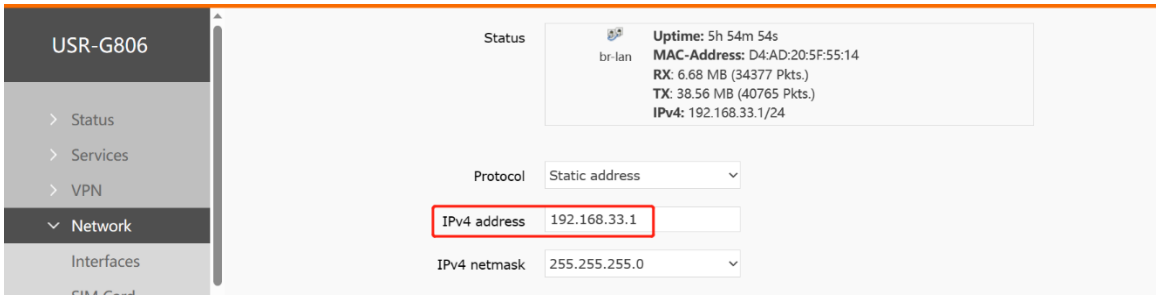


8>Check the routes of router1.



3.2 Configure the second router as OpenVPN Client2

1>The LAN IP of the second router is 192.168.33.1

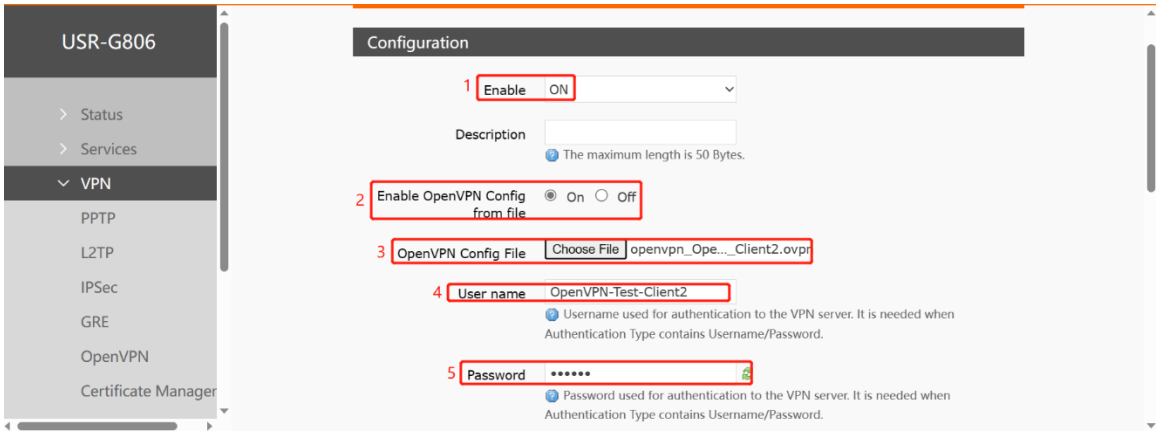


2>OpenVPN Config File: choose the “client2.ovpn” file downloaded in Chapter 2.7,

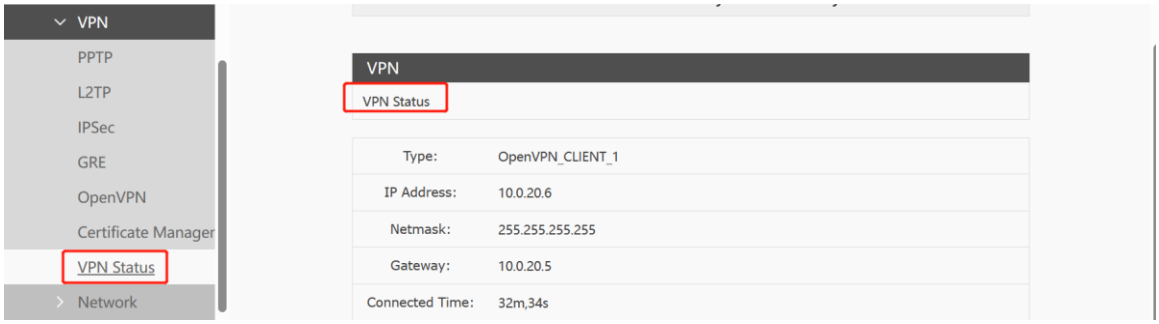
3>User name: The entered name of the OpenVPN-Test-Client2 in Chapter2.3,

4>Password: The password of the OpenVPN-Test-Client2 in Chapter 2.3,

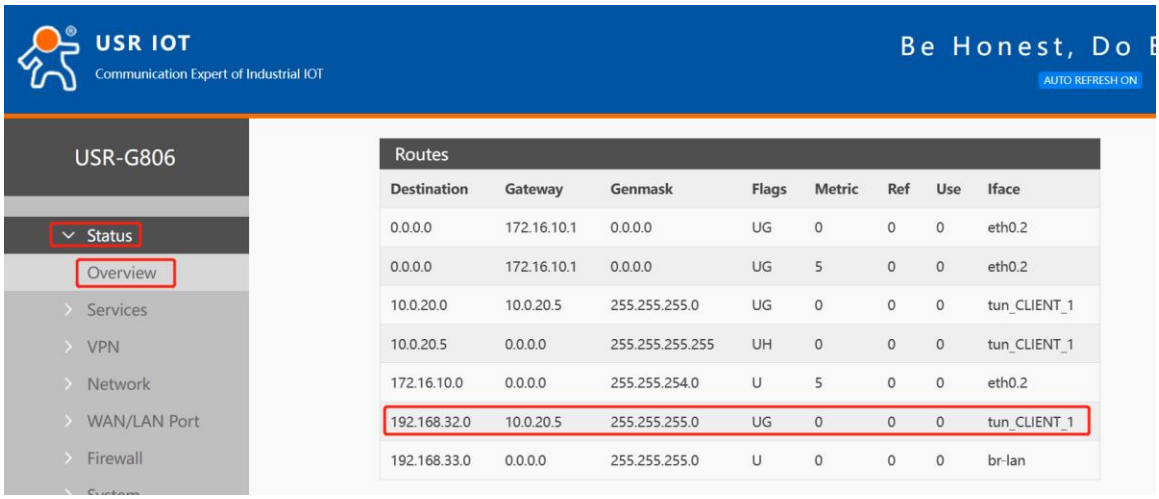
5>Click “Save & Apply” button,



6>The OpenVPN connection is connected, and more details of the connection can be check in VPN status page.

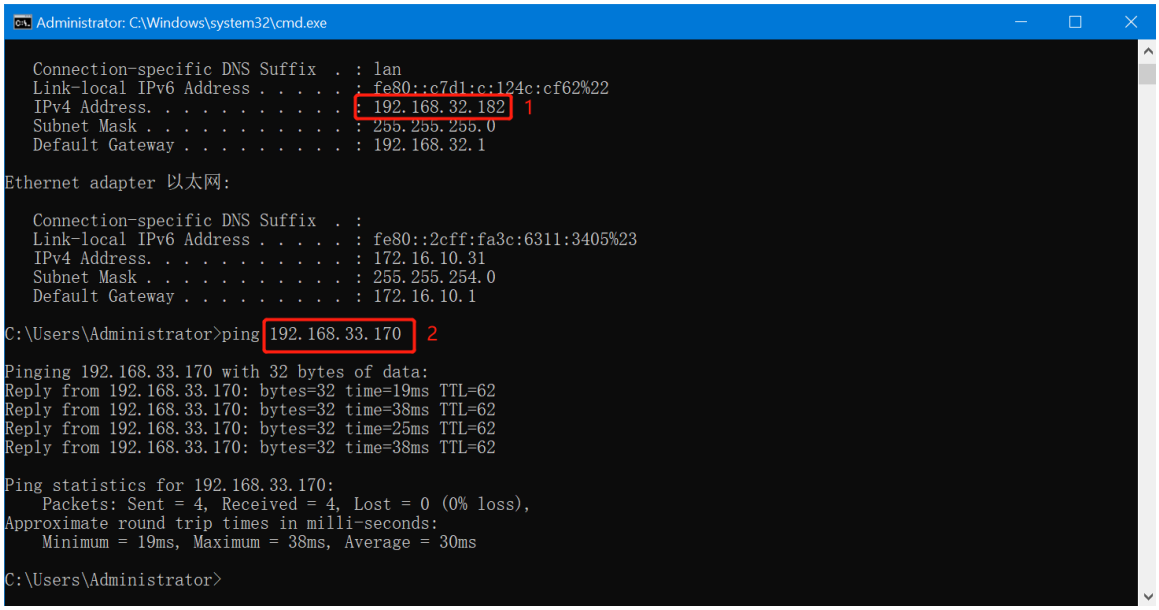


7> Check the routes of router2.



4. Inter-subnet connectivity testing

In this case，the IP of PC1 is192.168.32.182, and the IP of PC2(phone) is192.168.33.170.




App Store
下午 5:29
97%
返回
Ping
启动
服务器
192.168.32.182
添加到服务器列表
输出信息:
PING 192.168.32.182 (192.168.32.182): 56 data bytes
64 bytes from 192.168.32.182: icmp_seq=0 ttl=32 time=76.731 ms
64 bytes from 192.168.32.182: icmp_seq=1 ttl=32 time=45.212 ms
64 bytes from 192.168.32.182: icmp_seq=2 ttl=32 time=223.148 ms
64 bytes from 192.168.32.182: icmp_seq=3 ttl=32 time=80.995 ms
--- 192.168.32.182 ping statistics ---
4 packets transmitted, 4 received, 0.00% packet loss
round-trip min / avg / max = 45.212 / 106.522 / 223.148 ms