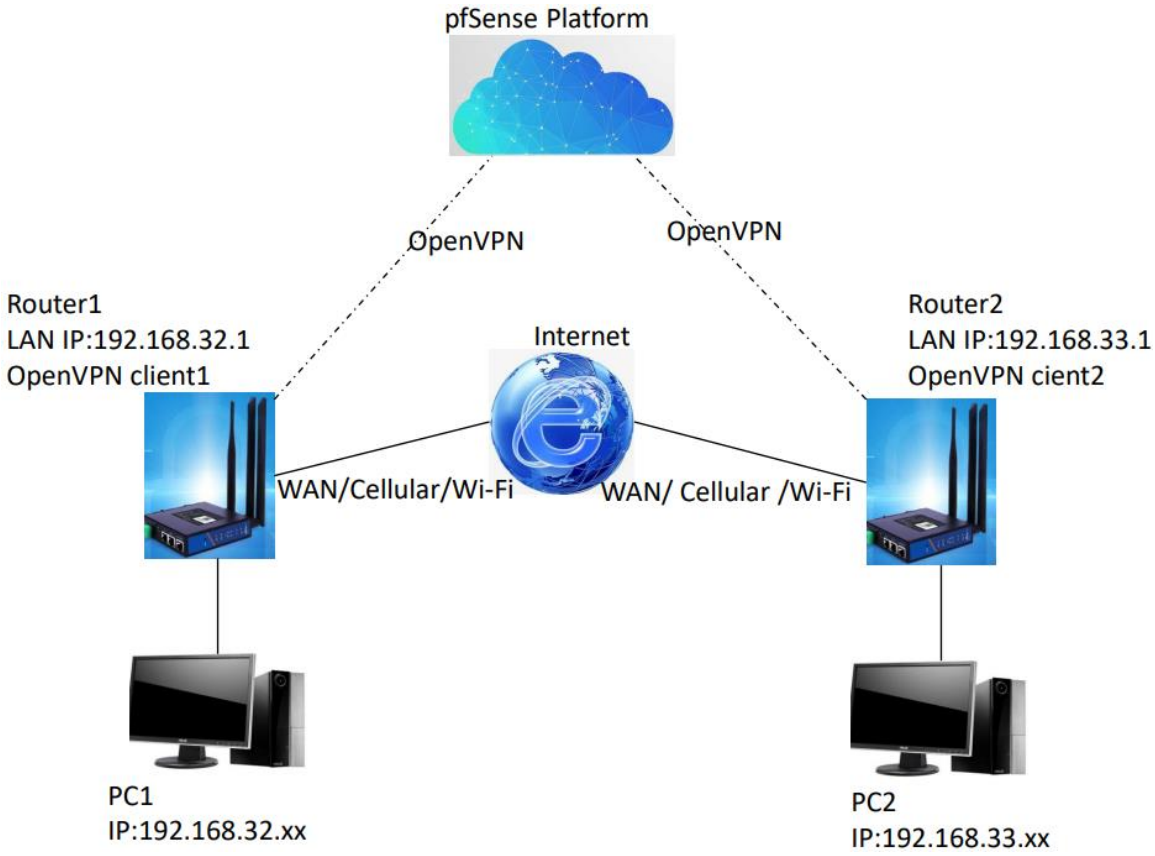
PUSR Routers Connect to pfSense Server

1. Login the pfSense server

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

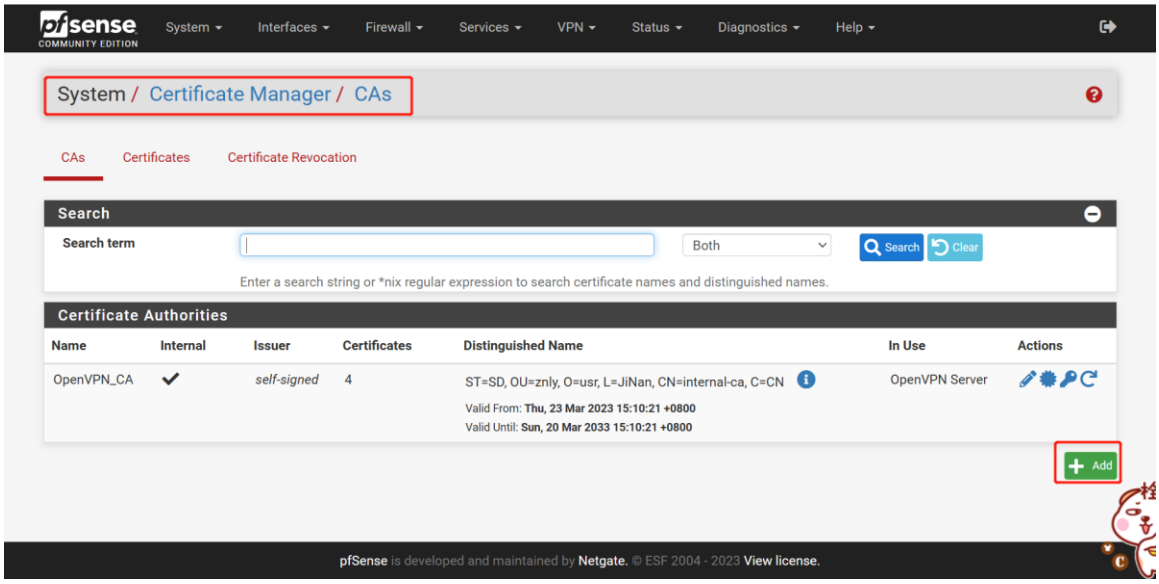
In this case, we configure the OpenVPN server and the OpenVPN clients to achieve the function as the following picture:



2. Create authorities and certificates

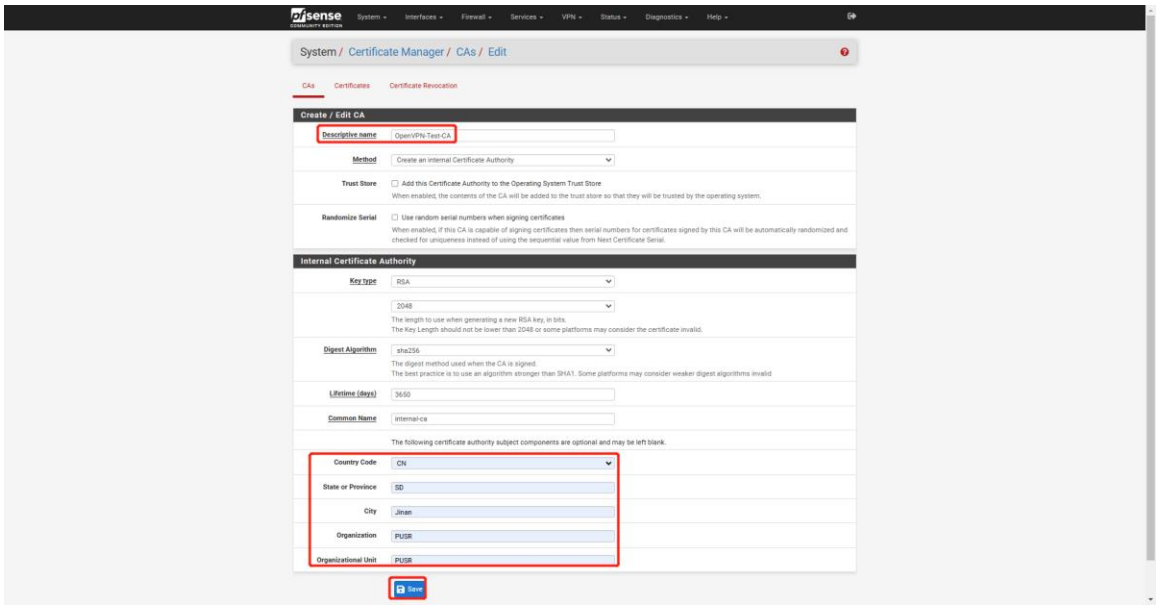
2.1 Create a CA certificate.

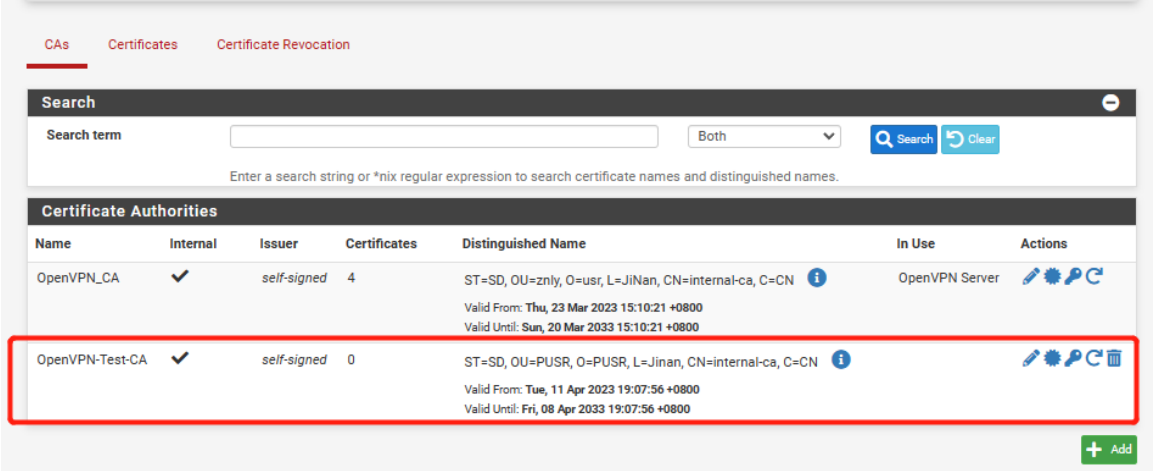
1>System->Cert. Manager->Cas



2>Enter descriptive name: In this case, it's "OpenVPN-Test-CA",

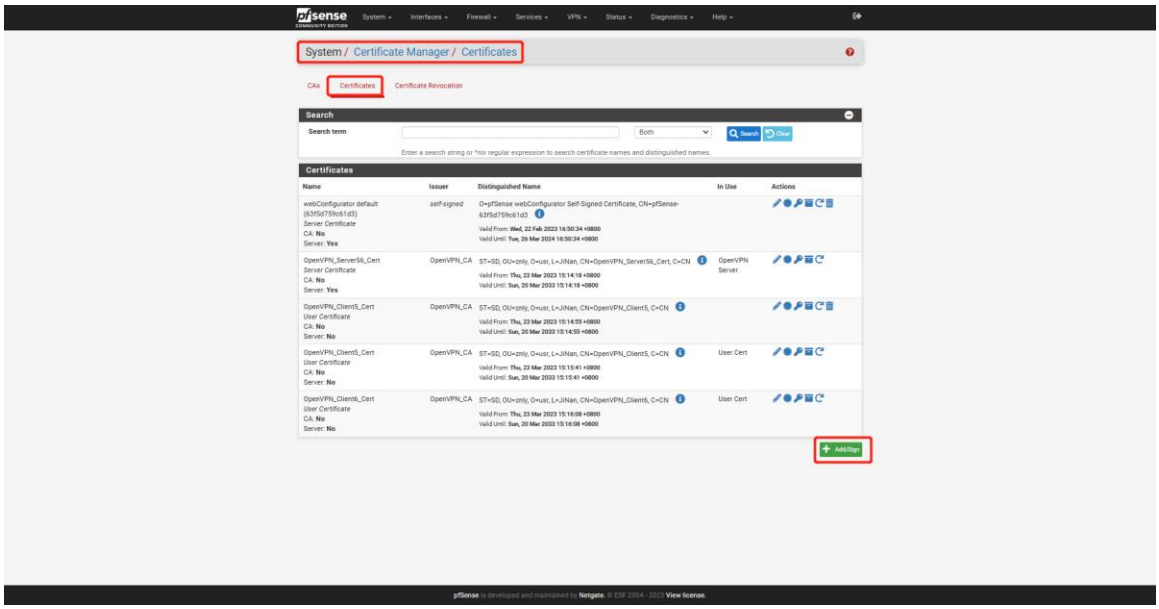
3>Click "Save" button.





2.2 Create Server Certificate

1>System->Cert. Manager->Certificates

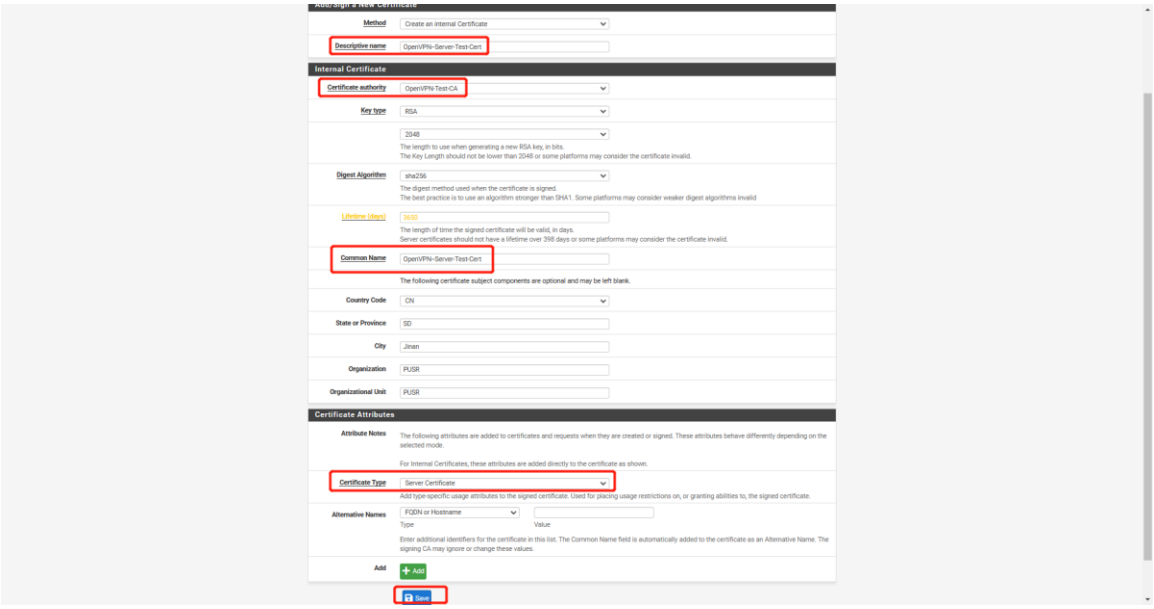


2>Descriptive name: OpenVPN-Server-Test-CA,

Certificates authority: Select “OpenVPN-Test-CA” which created in the Chapter 2.1,

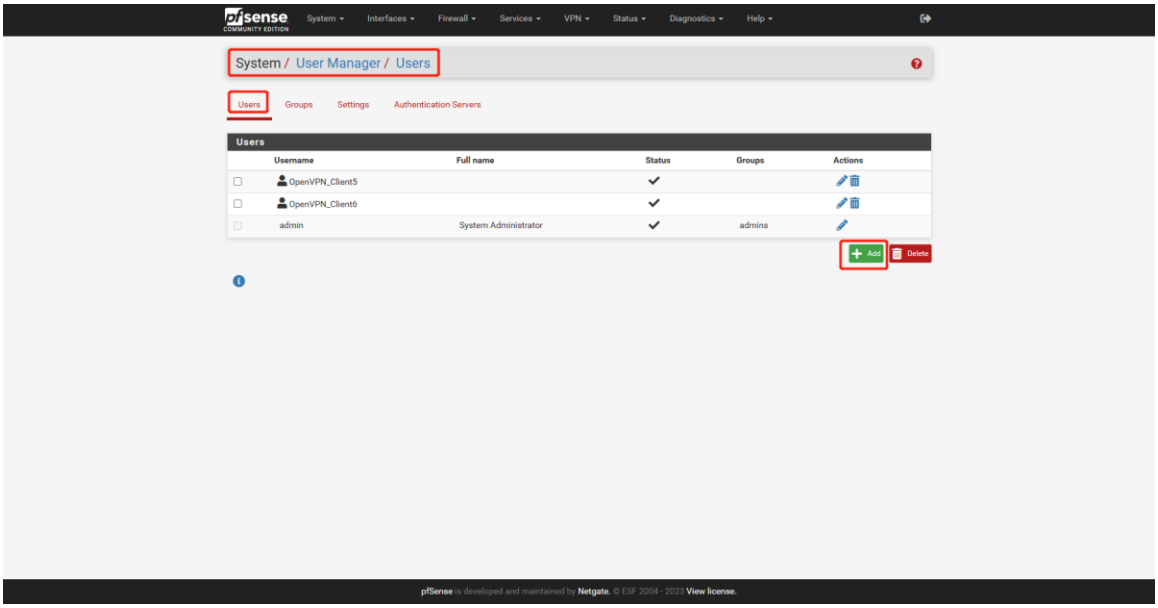
Common name: Keep consistent with the “Descriptive name”,

Certificate Type: Select the “Server Certificate”



2.3 Add users and create user certificates

1>System->User Manager->Users

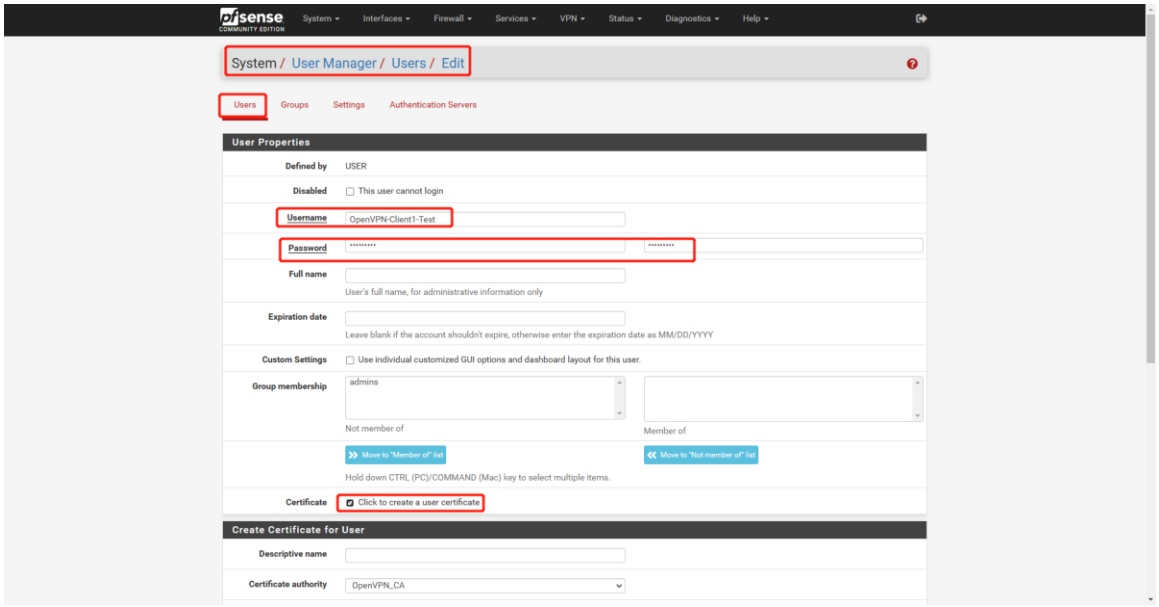


2>Username: OpenVPN-Client1-Test,

Password: Enter password and confirm the password,

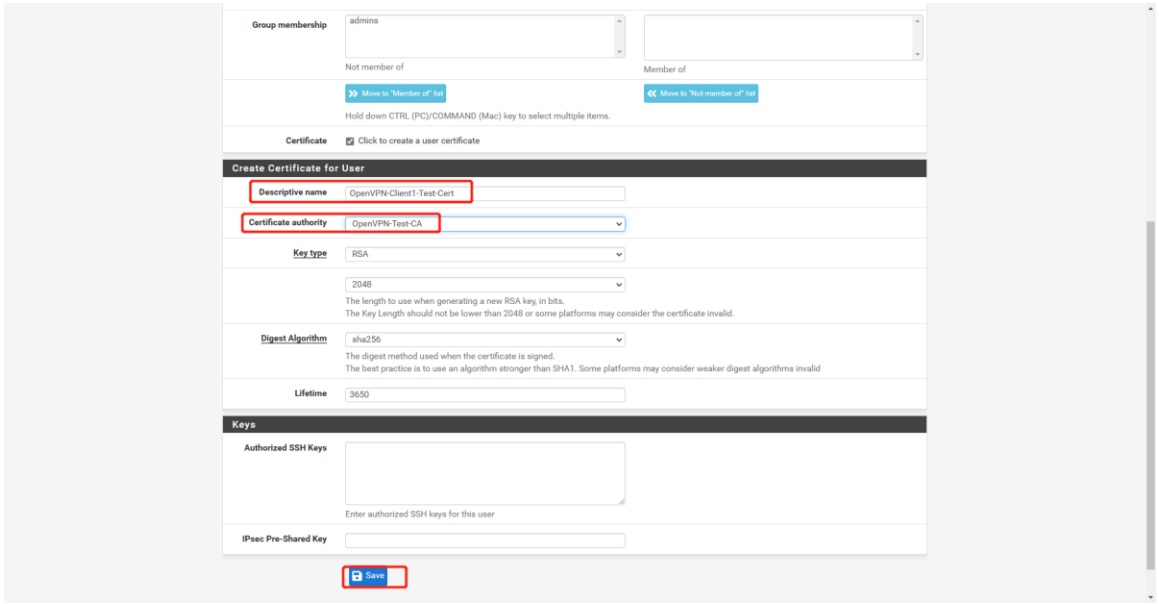
Certificate: Enable “Click to create a user certificate”

Certificate: Enable “Click to create a user certificate”,

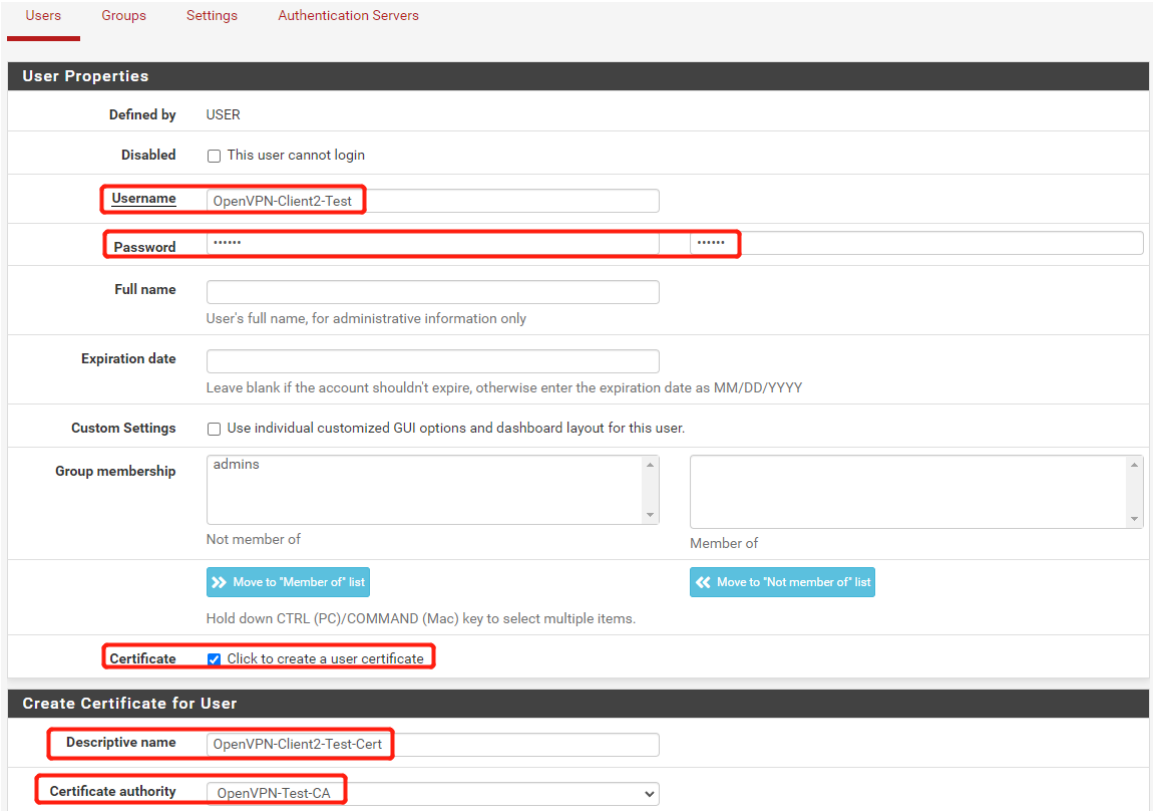


3> Descriptive name: OpenVPN-Client1-Test-Cert,

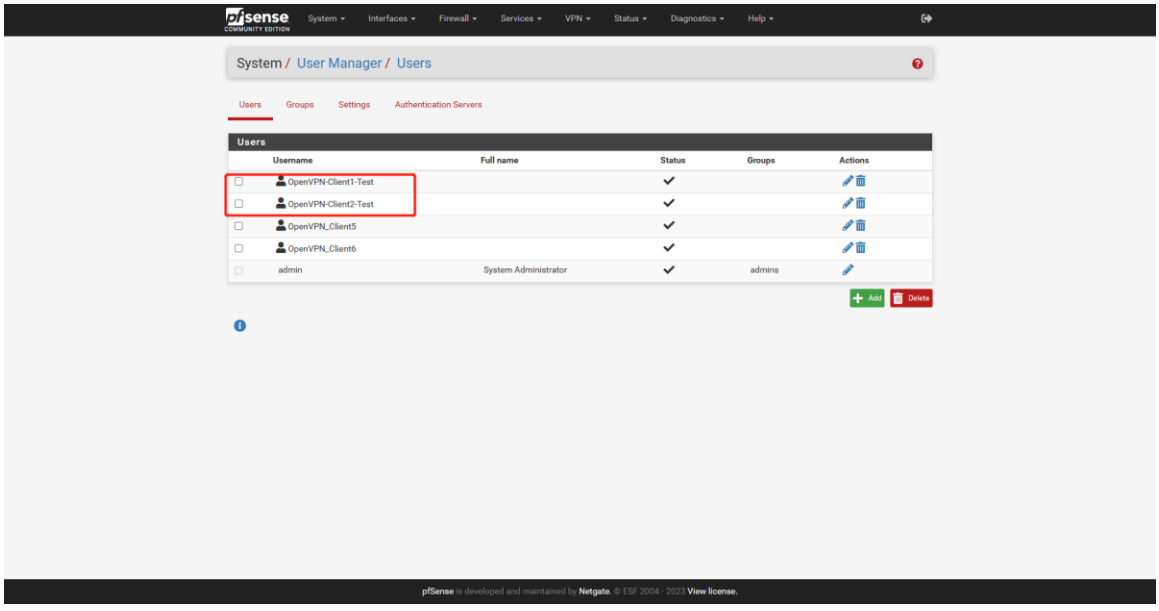
Certificate authority: Select “OpenVPN-Test-CA” which created in the Chapter 2.1,



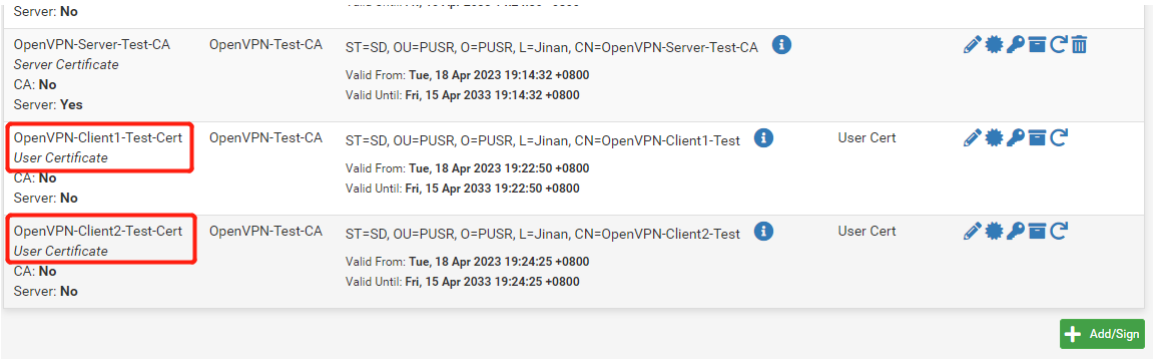
4>Add the second user using the same steps



5>Users are added successfully.



6>The certificates of users is also added successfully. They can be checked in "System->Cert. Manager->Certificates".



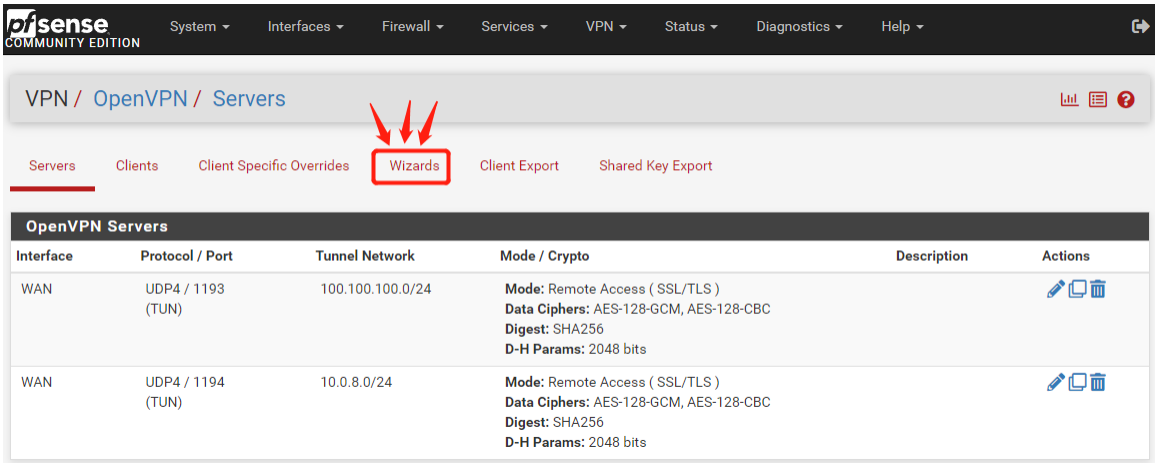
2.4 Install the client configuration file export package.

[If the package has already been installed, you can skip this step]

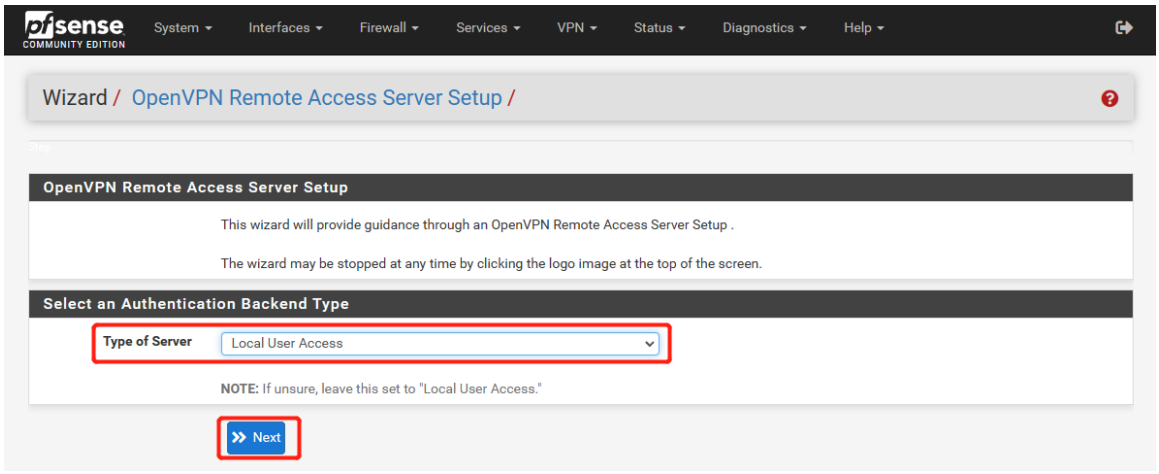
System->Package Manager->Available Packages

2.5 Configure OpenVPN Server

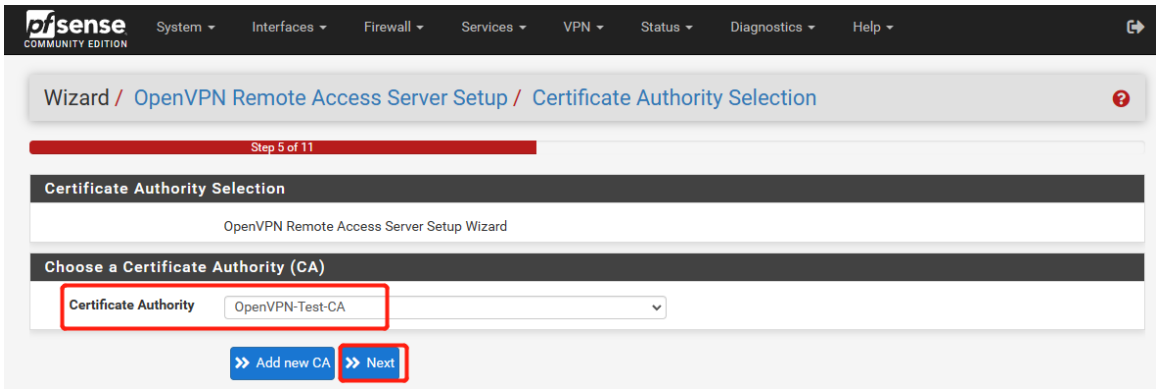
1>VPN->OpenVPN->Wizards



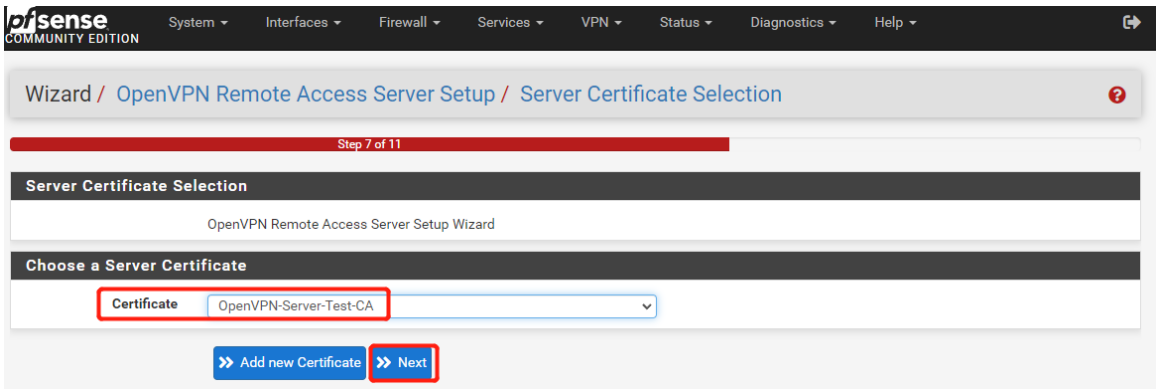
2>Type of Server: Local User Access



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



4>Certificate: Select “OpenVPN-Server-Test-CA” created in Step 2.2

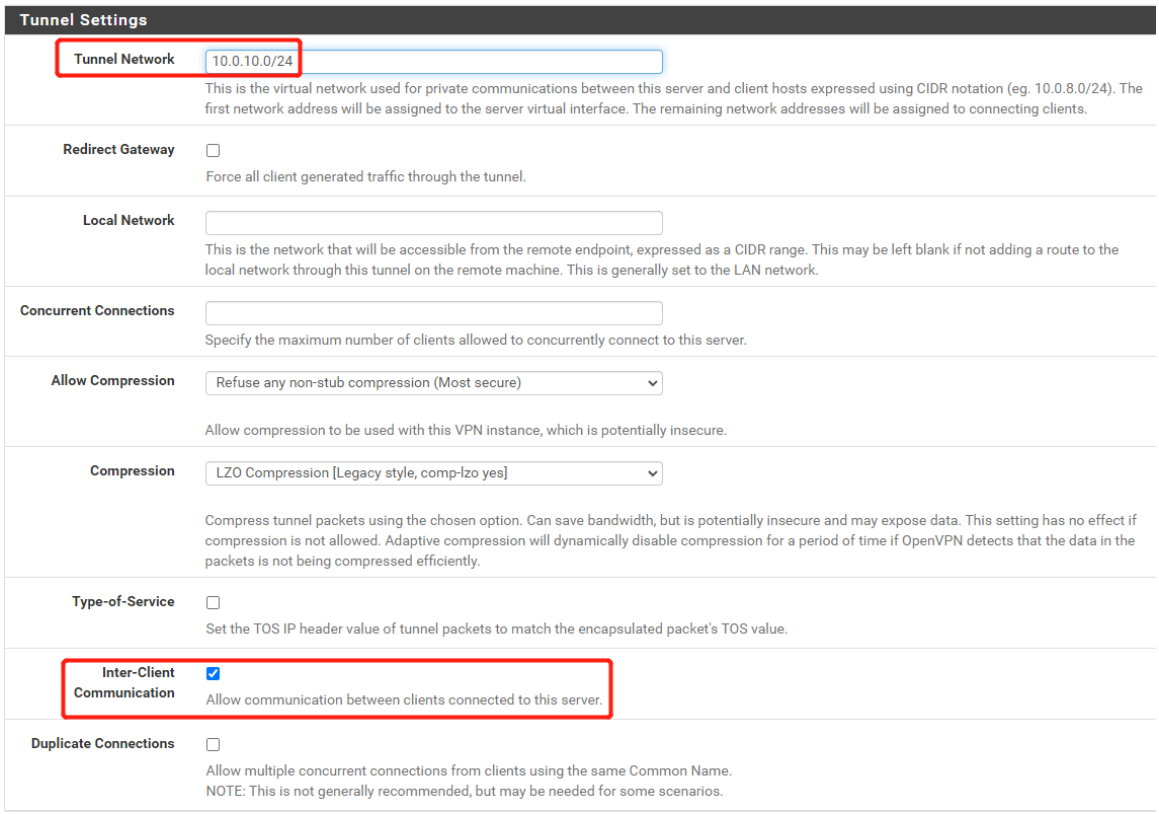


5>Tunnel Settings

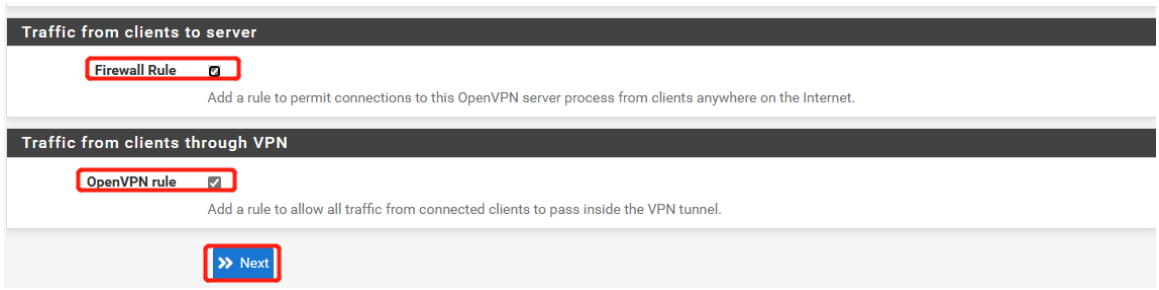
Tunnel Network: 10.0.10.0/24

Inter-Client Communication: This function should be enabled.

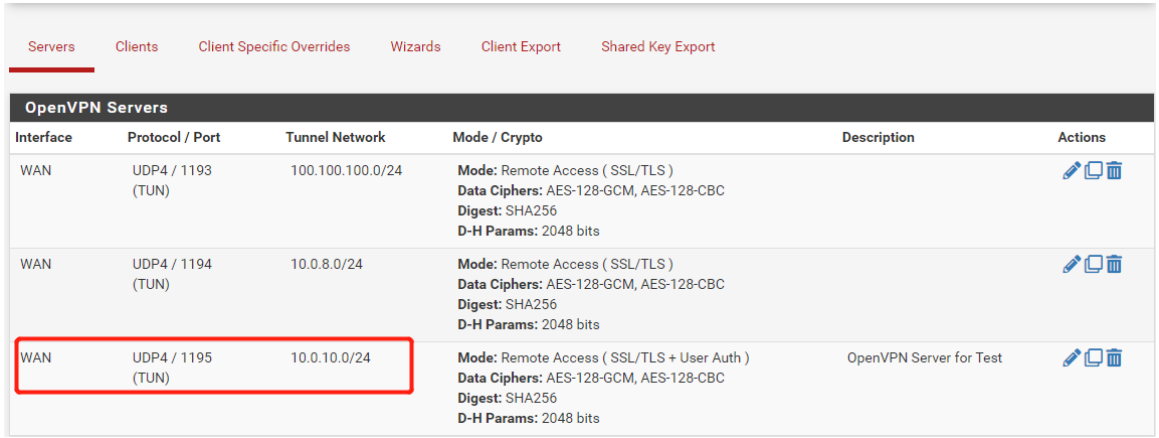
The other parameters in this page can stay default.



6>Firewall and OpenVPN rules are enabled by default.

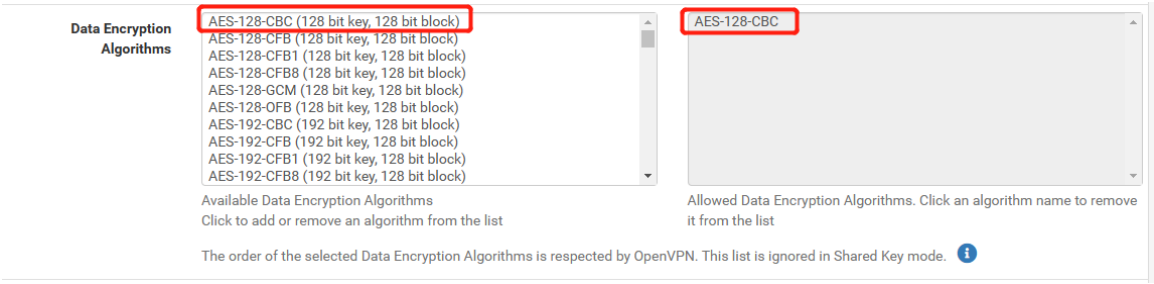


7> OpenVPN server is added successfully.



Server mode: Select “Remote Access(SSL/TLS)”

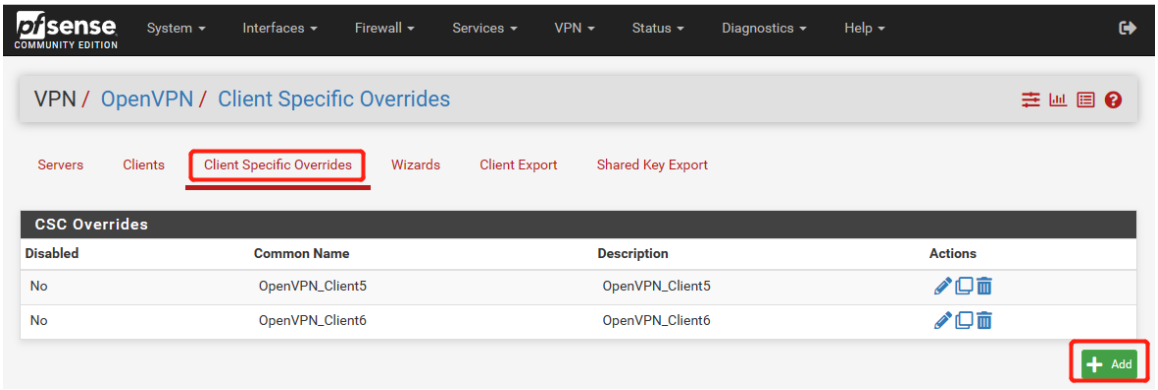
Select “AES-128-CBC”



2.6 Configure the OpenVPN client and subnet

- Add the first OpenVPN client

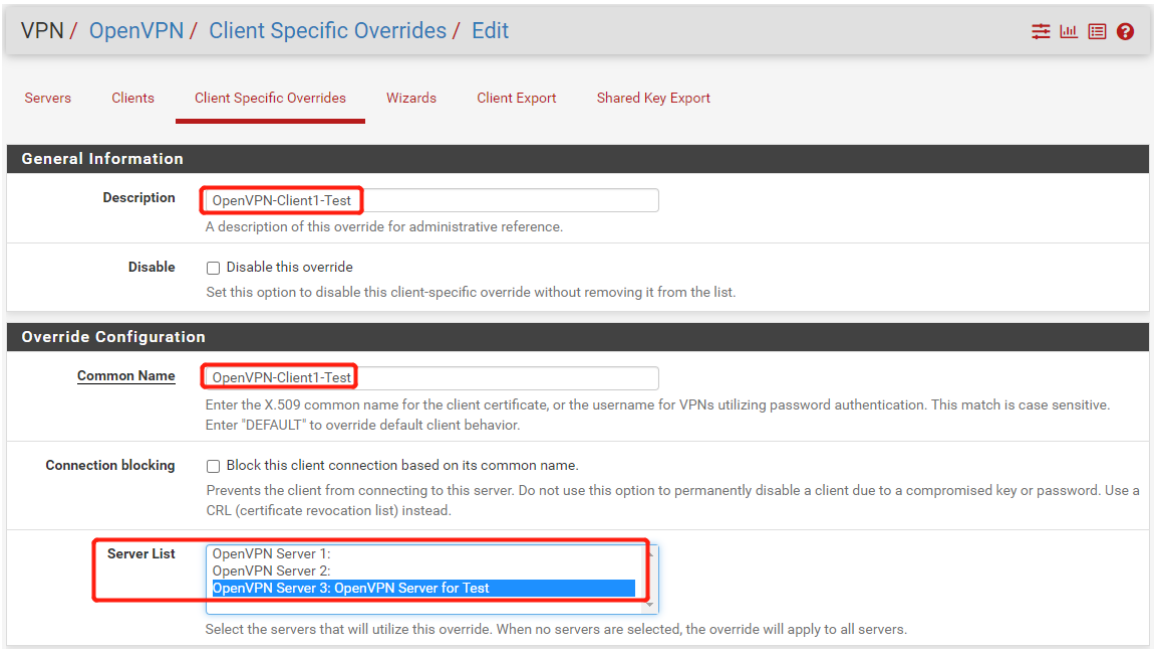
1>VPN->OpenVPN->Client Specific Overrides->Add



2> Description： OpenVPN-Client1-Test

Common name：OpenVPN-Client1-Test

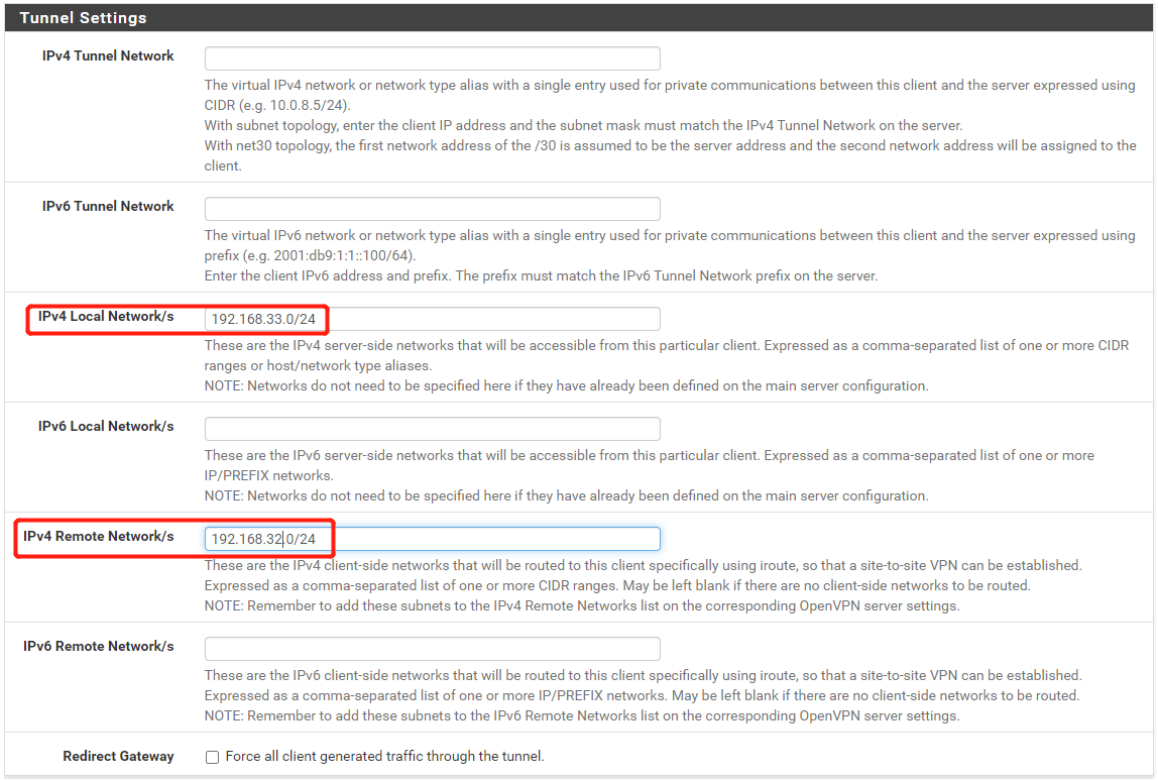
Server List： Select “OpenVPN Server 3” added in Chapter 2.5



3>Tunnel Settings:

IPv4 Local Network/s:192.168.33.0/24, the LAN IP of router2,

IPv4 Remote Network/s:192.168.32.0/24, the LAN IP of router1,

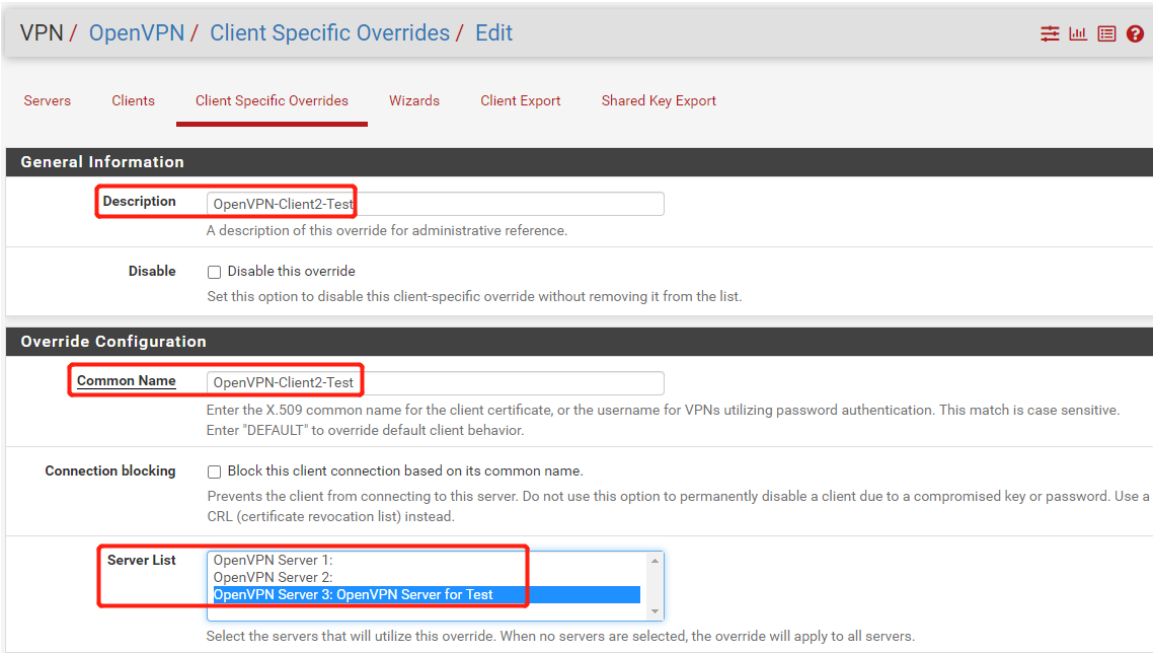


- Add the second OpenVPN client using the same steps.

1> Description： OpenVPN-Client2-Test

Common name：OpenVPN-Client2-Test

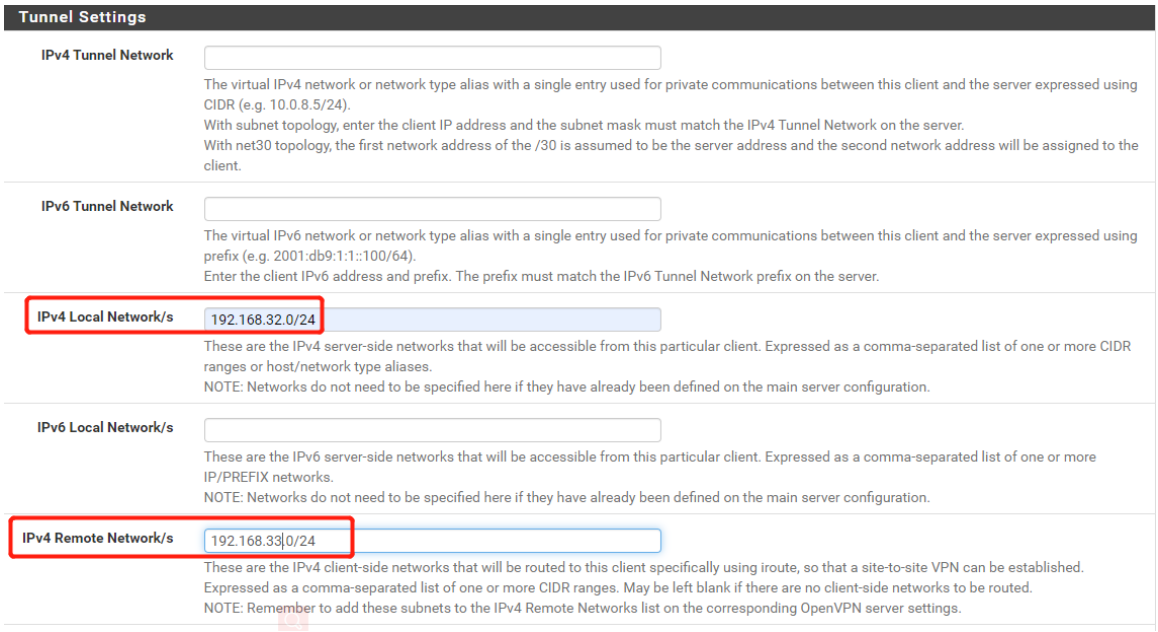
Server List： Select “OpenVPN Server 3” added in Chapter 2.5



2> Tunnel Settings:

IPv4 Local Network/s:192.168.33.0/24, the LAN IP of router1,

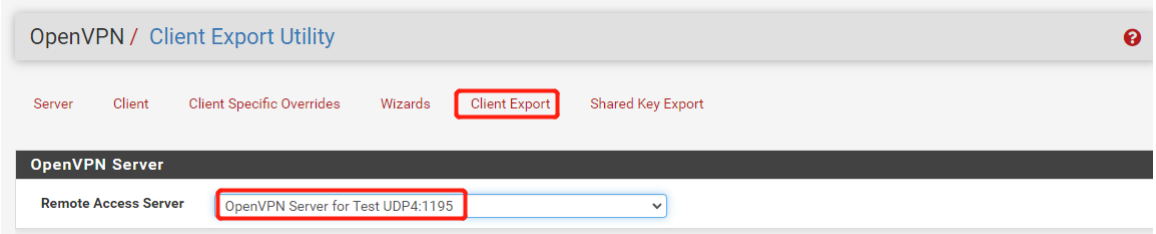
IPv4 Remote Network/s:192.168.32.0/24, the LAN IP of router2,



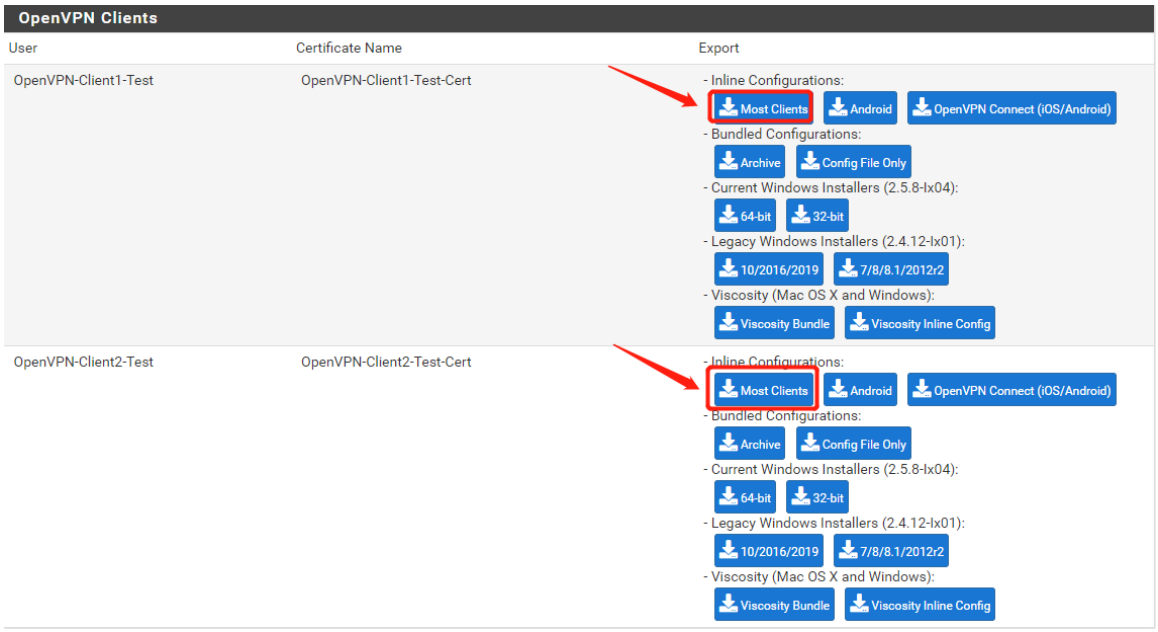
2.7 Export the OpenVPN client package

VPN->OpenVPN->Client Export

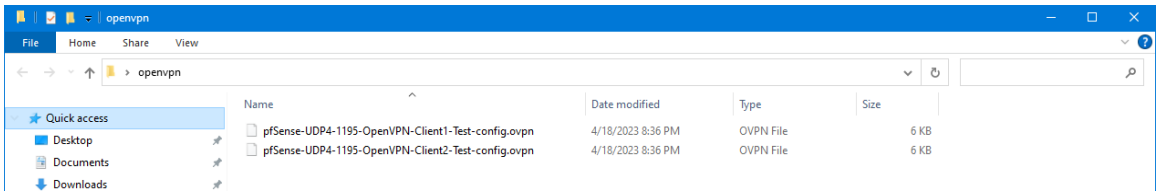
1>Remote Access Server: Select the OpenVPN Server added in chapter 2.5,



2>Download the package of OpenVPN client



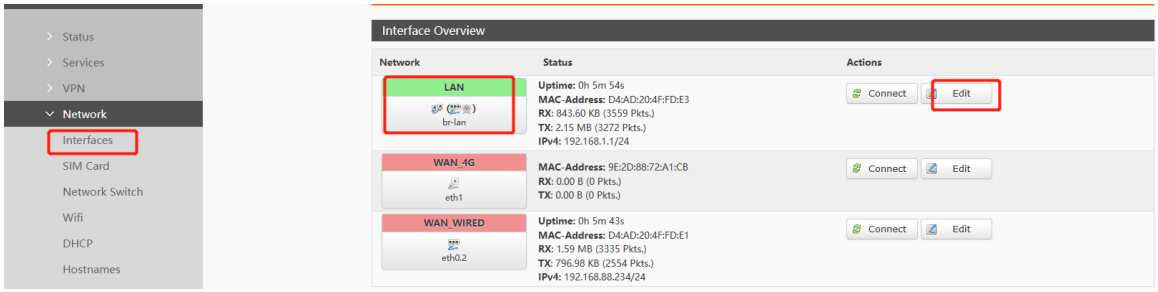
3>The downloaded files.

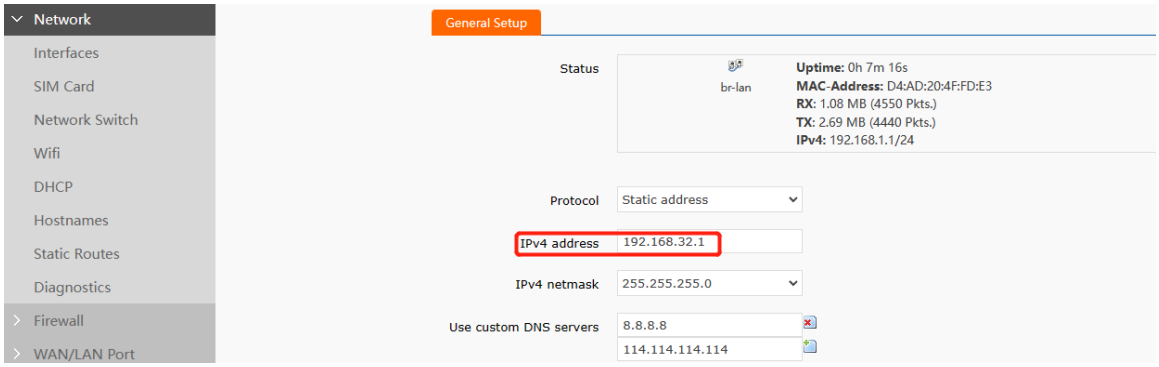


3. Configure routers' parameters

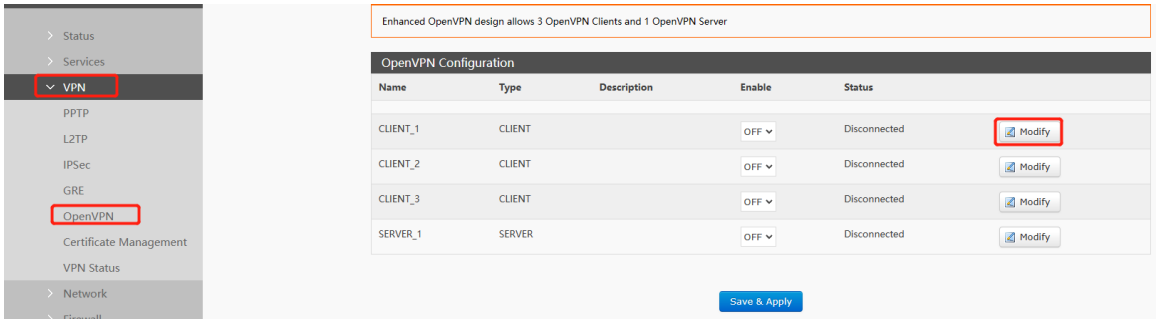
3.1 Configure the router1 as OpenVPN Client1

1>Change LAN IP to 192.168.32.1





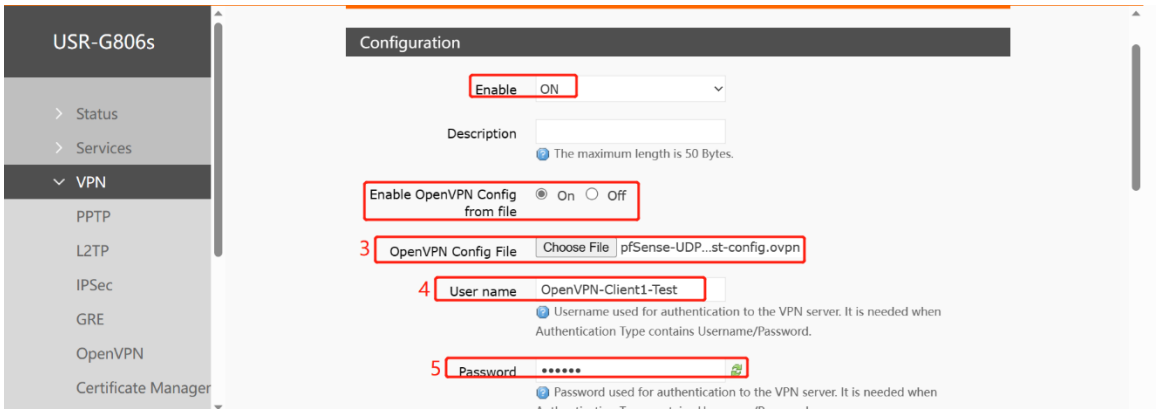
2>Modify the OpenVPN parameters



3>OpenVPN Config File: choose the "Client1-Test-config.ovpn" file downloaded in Chapter 2.7,

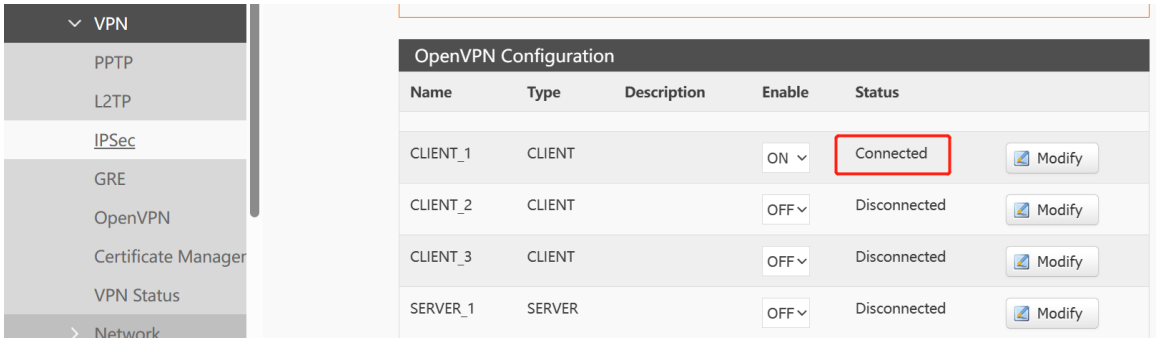
4>User name: The entered name of the OpenVPN-Test-Client1 in Chapter2.3

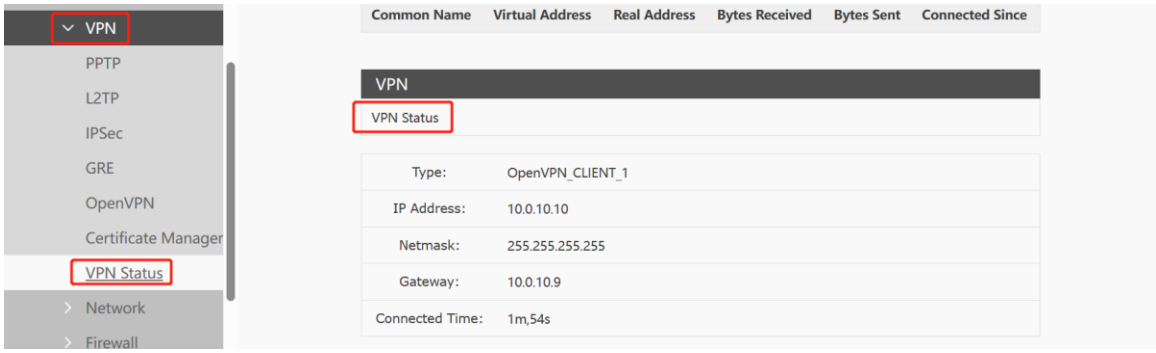
5>Password: The password of the OpenVPN-Test-Client1 in Chapter 2.3



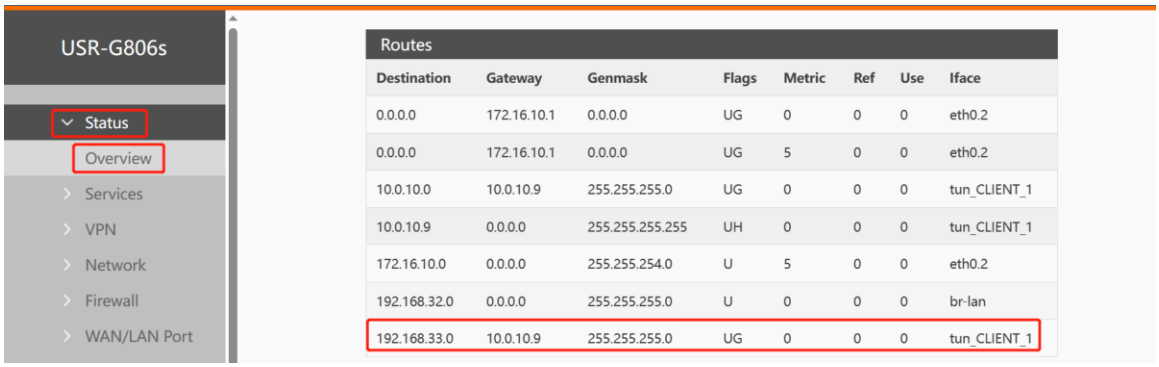
6>Click “Save & Apply” button.

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



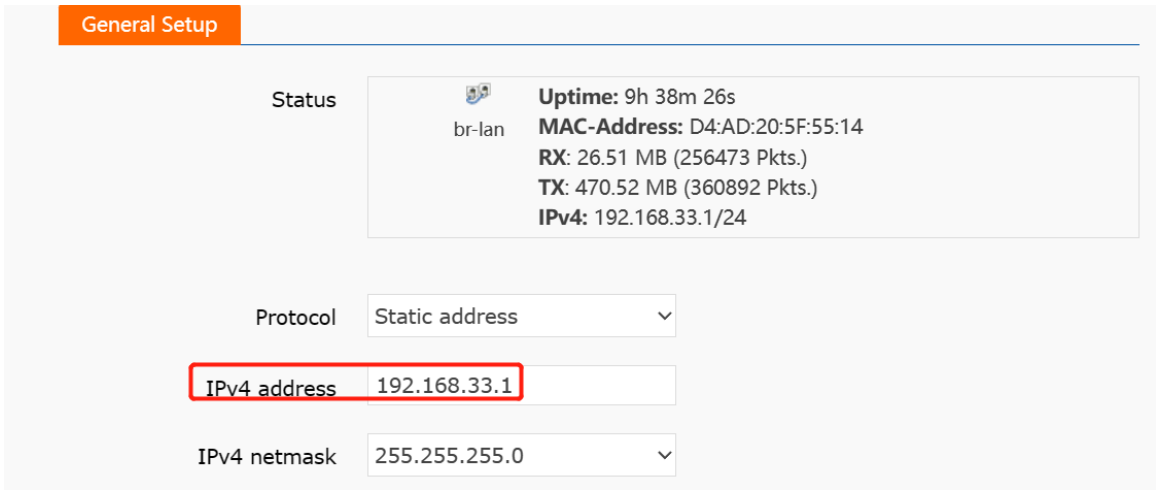


8>Check the routes of router1. This route is very important, without it, the network devices connect to router can’t communicate with each other.



3.2 Configure the second router as OpenVPN Client2

1>The LAN IP of the second router is 192.168.33.1,

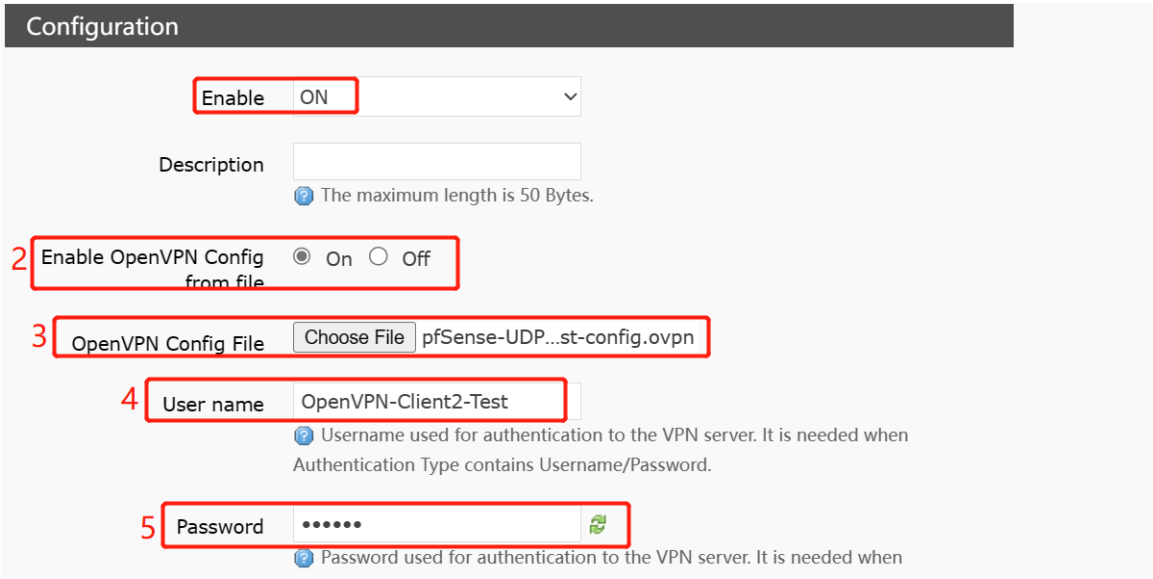


2>OpenVPN Config File: choose the “Client2-Test-config.ovpn” file downloaded in Chapter 2.7

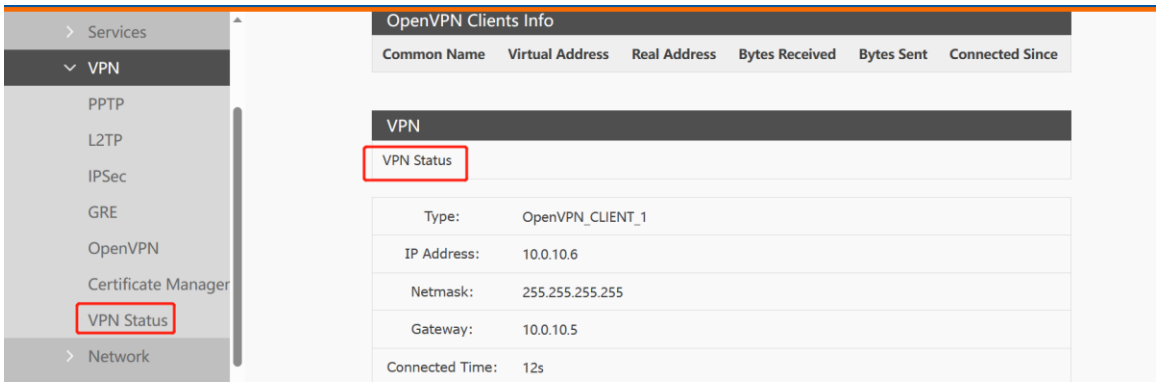
3>User name: The entered name of the “OpenVPN-Client2-Test” in Chapter2.3

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

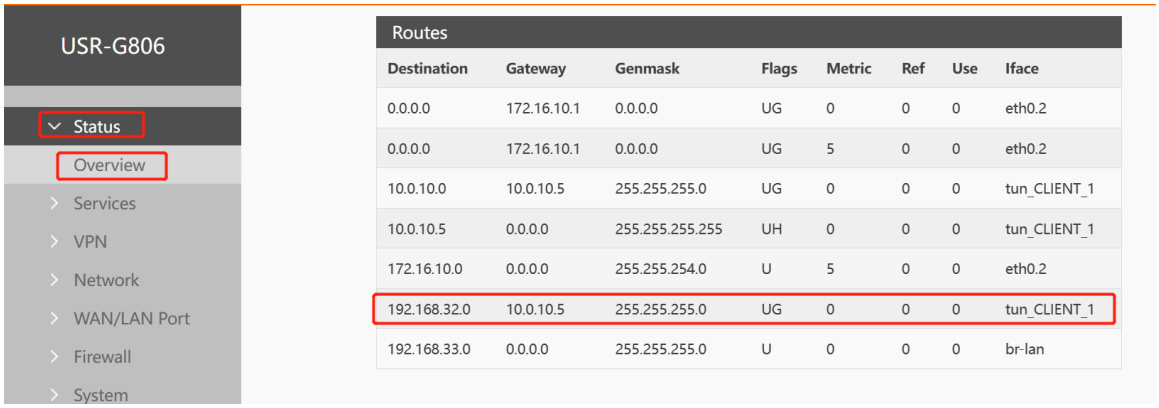
5>Click “Save & Apply” button,



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

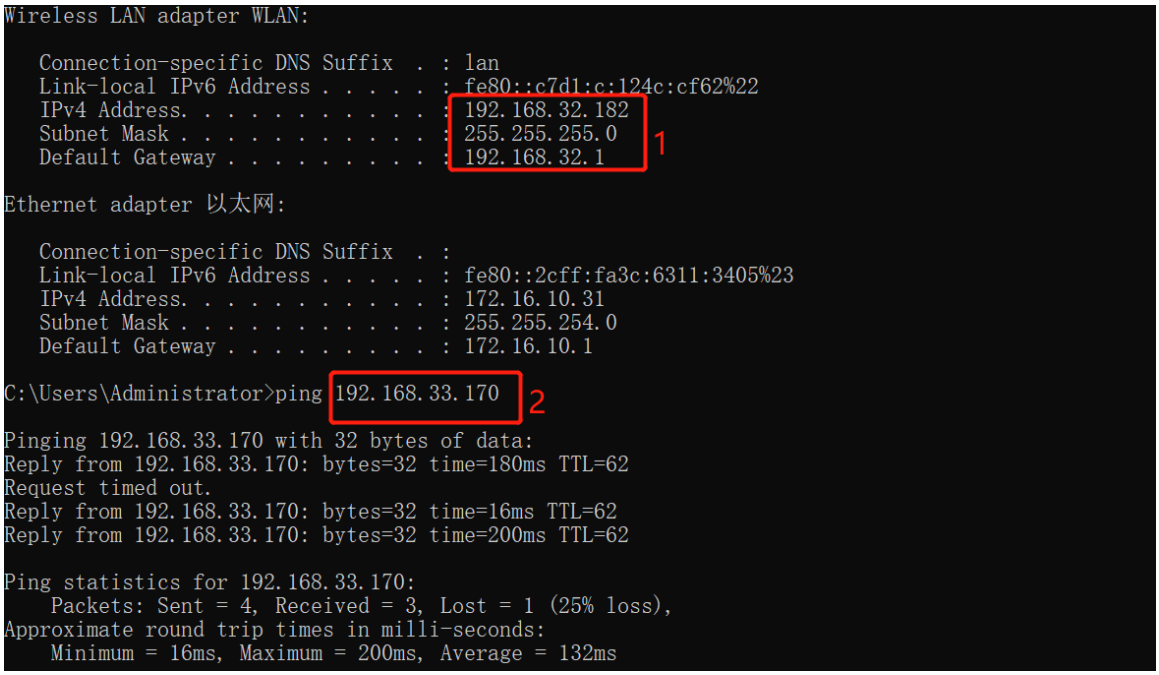


7> Check the routes of router2. This route is very important, without it, the network devices connect to router can't communicate with each other.



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.




搜索
下午 9:14
89%
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=15.777 ms
64 bytes from 192.168.32.182: icmp_seq=1 ttl=32 time=22.384 ms
64 bytes from 192.168.32.182: icmp_seq=2 ttl=32 time=18.423 ms
64 bytes from 192.168.32.182: icmp_seq=3 ttl=32 time=43.237 ms
64 bytes from 192.168.32.182: icmp_seq=4 ttl=32 time=21.842 ms
64 bytes from 192.168.32.182: icmp_seq=5 ttl=32 time=32.511 ms
--- 192.168.32.182 ping statistics ---
6 packets transmitted, 6 received, 0.00% packet loss
round-trip min / avg / max = 15.777 / 25.696 / 43.237 ms