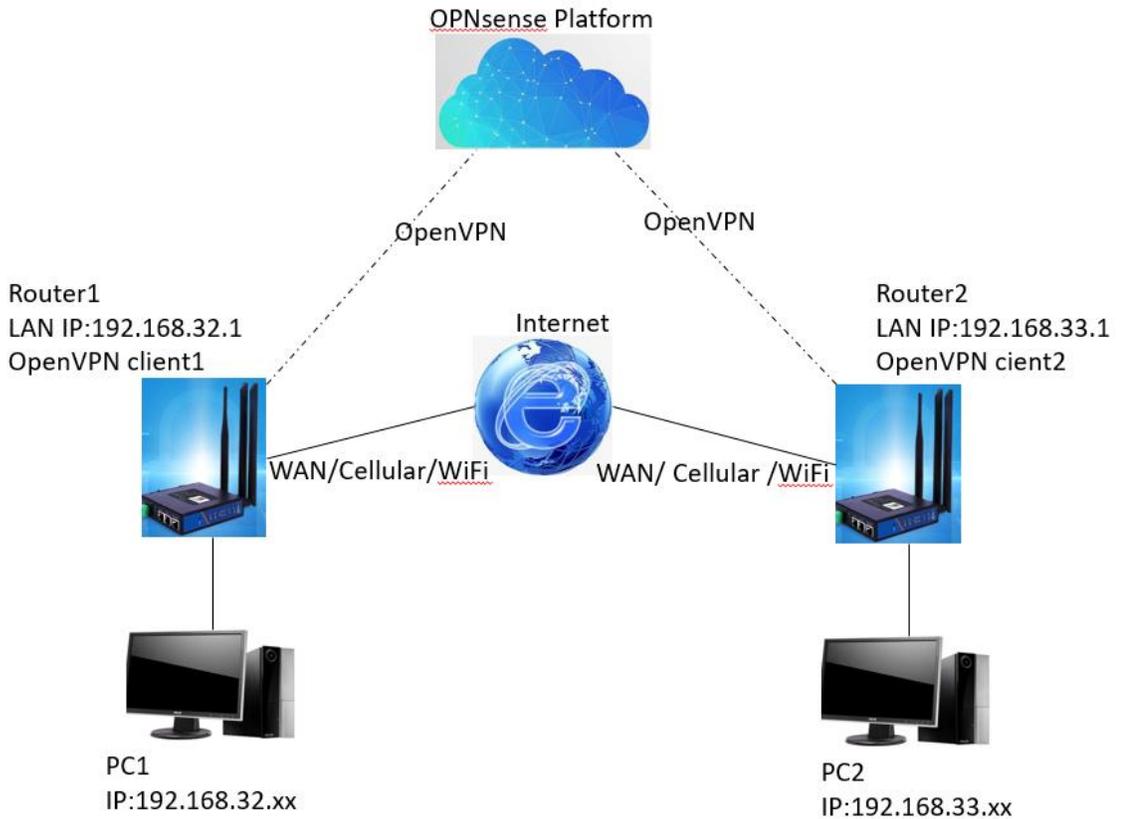


PUSR Routers Connect to OPNsense Server

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.

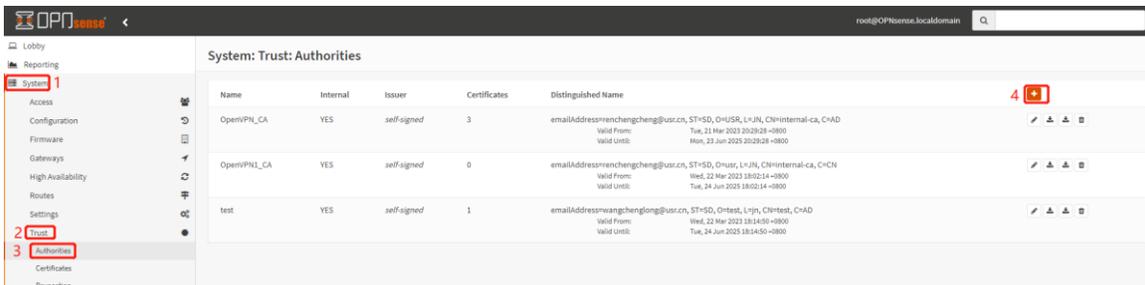
In this case, we configure the OpenVPN server and the OpenVPN clients to achieve the function as the following picture:



2. Create authorities and certificates

2.1 Create a CA certificate.

System->Trust->Authorities



Edit authorities:

System: Trust: Authorities

1 OpenVPN-Test-CA

2 Create an internal Certificate Authority

Internal Certificate Authority

Key Type: RSA

Key length (bits): 2048

Digest Algorithm: SHA256

Lifetime (days): 825

Distinguished name

Country Code: AD (Andorra)

3 State or Province: SD

City: Jinan

Organization: PUSR

Email Address: liumeimei@user.cn

Common Name: internal-ca

4 Save

2.2 Create Server Certificate

System->Trust->Certificates

System: Trust: Certificates

Name	Issuer	Distinguished Name	Valid From	Valid Until	Actions
Web GUI TLS certificate	self-signed	ST=Zuid-Holland, O=OpenSense self-signed web certificate, L=Hillesholm, CN=OpenSense.localdomain, C=NL	Thu, 21 Feb 2023 02:18:57 +0800	Thu, 28 Mar 2024 02:19:57 +0800	+
OpenVPN_Server_Cert	OpenVPN_CA	emailAddress=wangchengsheng@user.cn, ST=SD, O=USR, L=JN, CN=OpenVPN_Server_Cert, C=AD	Thu, 21 Mar 2023 20:30:49 +0800	Sun, 21 Apr 2024 20:30:49 +0800	OpenVPN Server +
test	test	emailAddress=wangchengsheng@user.cn, ST=SD, O=test, L=yn, CN=test, C=AD	Wed, 22 Mar 2023 18:18:11 +0800	Mon, 22 Apr 2024 18:18:11 +0800	User Cert +
OpenVPN_Client1	OpenVPN_CA	emailAddress=wangchengsheng@user.cn, ST=SD, O=USR, L=JN, CN=OpenVPN_Client1, C=AD	Thu, 23 Mar 2023 20:55:23 +0800	Tue, 23 Apr 2024 20:55:23 +0800	User Cert +

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" .

Method	1	Create an internal Certificate
Descriptive name	2	OpenVPN-Test-Sever-Cert
Internal Certificate		
Certificate authority	3	OpenVPN-Test-CA
Type	4	Server Certificate
Key Type		RSA
Key length (bits)		2048
Digest Algorithm		SHA256
Lifetime (days)		397
Private key location		Save on this firewall
Distinguished name		
Country Code :		AD (Andorra)
State or Province :		SD
City :		Jinan
Organization :		PUSR
Email Address :		liumeimei@usr.cn
Common Name :	5	OpenVPN-Test-Sever-Cert

2.3 Add users and create user certificates

System->Access->Users

Username	Full name	Groups
OpenVPN_Client1		
OpenVPN_Client2		
root	System Administrator	admins
test		

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.

System: Access: Users

Defined by: USER

Disabled:

Username: 1 OpenVPN-Test-Client1

Password: 2

Password (confirmation): 3

Group Memberships: Not Member Of

admins

Certificate: Click to create a user certificate.

OTP seed:

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.

System: Trust: Certificates

Method 1 Create an internal Certificate

Descriptive name

Internal Certificate

Certificate authority 2 OpenVPN-Test-CA

Type Client Certificate

Key Type RSA

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" .

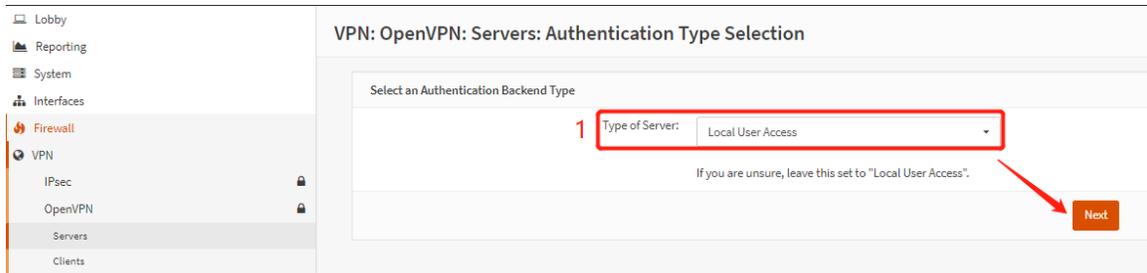
Effective Privileges	Inherited from	Type	Name
User Certificates			
	Name	CA	Valid From
	OpenVPN-Test-Client1	OpenVPN-Test-CA	Mon, 17 Apr 2023 20:21:49 +0800
			Valid To
			Sat, 18 May 2024 20:21:49 +0800
+ [edit] [delete]			
API keys			
	key	+	
OTP seed			
	<input type="text"/>	<input type="checkbox"/> Generate new secret (160 bit)	
Authorized keys			
	Paste an authorized keys file here.		
IPsec Pre-Shared Key			
	<input type="text"/>		
	<input type="button" value="Save"/>	<input type="button" value="Save and go back"/>	<input type="button" value="Cancel"/>

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

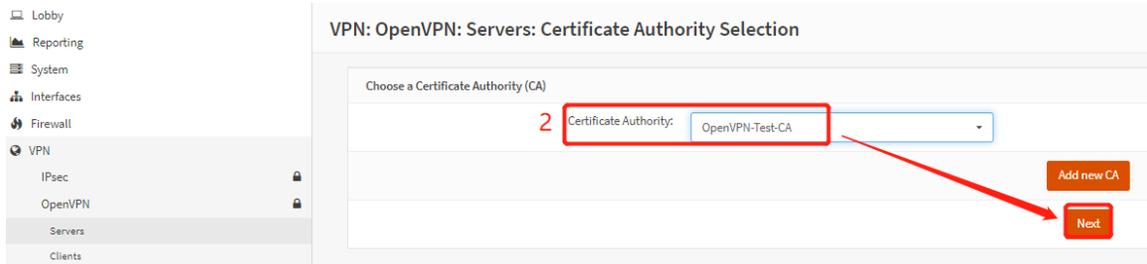
2.4 Configure OpenVPN Server

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

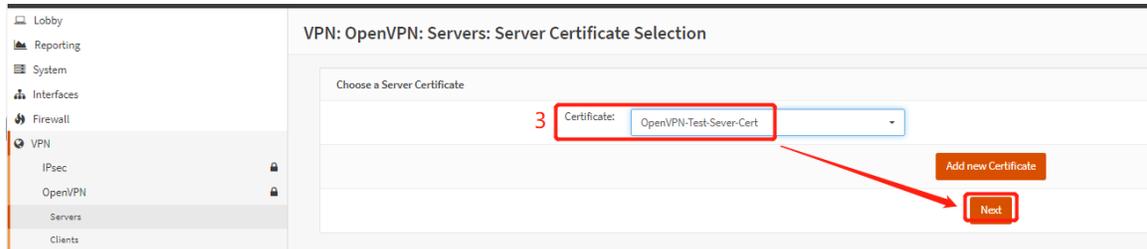
1>Type of Server: Local User Access



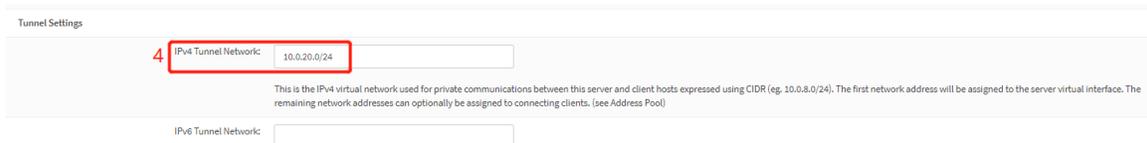
2>Certificate Authority: "OpenVPN-Test-CA" created in Step 2.1



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.

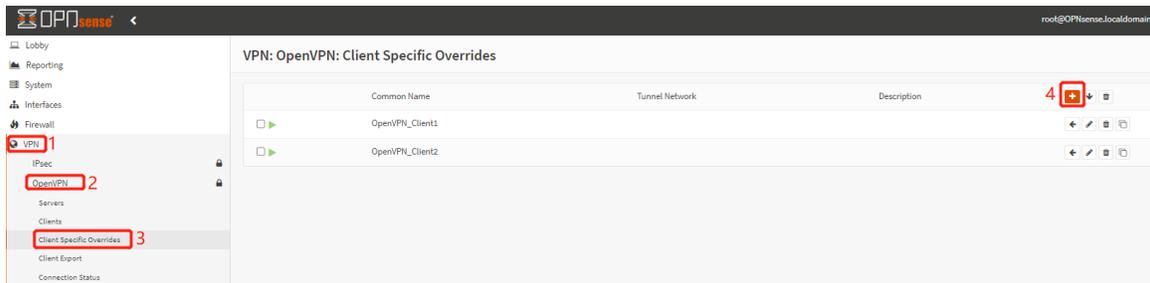


7>Click “Finished” button, the servers are listed. “UDP / 1195” is the server we added.



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” .

VPN: OpenVPN: Client Specific Overrides

General information	
❗ Disabled	<input type="checkbox"/>
❗ Servers	1 (1195 / UDP)
❗ Common name	2 OpenVPN-Test-Client1
❗ Description	<input type="text"/>
❗ Connection blocking	<input type="checkbox"/>
Tunnel Settings	
❗ IPv4 Tunnel Network	<input type="text"/>
❗ IPv6 Tunnel Network	<input type="text"/>
❗ IPv4 Local Network	3 192.168.33.0/24
❗ IPv6 Local Network	<input type="text"/>
❗ IPv4 Remote Network	4 192.168.32.0/24
❗ IPv6 Remote Network	<input type="text"/>

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" .

General information	
Disabled	<input type="checkbox"/>
Servers	1 (1195 / UDP)
Common name	2 OpenVPN-Test-Client2
Description	
Connection blocking	<input type="checkbox"/>
Tunnel Settings	
IPv4 Tunnel Network	
IPv6 Tunnel Network	
IPv4 Local Network	3 192.168.32.0/24
IPv6 Local Network	
IPv4 Remote Network	4 192.168.33.0/24
IPv6 Remote Network	

2.7 Export the OpenVPN client package

VPN->OpenVPN->Client Export

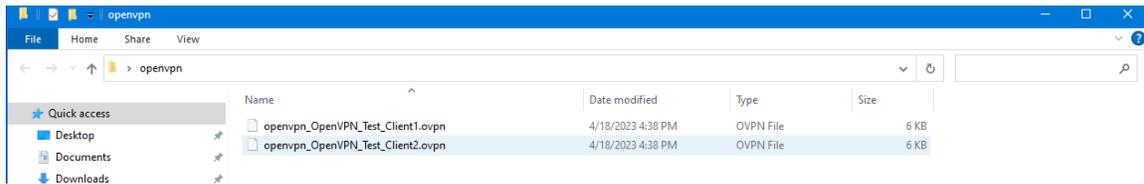
1> Remote Access Server: Server UDP:1195,

2>Download the package of Client1,

3> Download the package of Client2.

The screenshot shows the 'VPN: OpenVPN: Client Export' configuration page. The 'Remote Access Server' is set to 'Server UDP:1195'. The 'Export type' is 'File Only'. The 'Hostname' is '60.208.44.205' and the 'Port' is '1195'. The 'Client Specific Overrides' section is checked. The 'Accounts / certificates' table shows two clients: 'OpenVPN-Test-Client1' and 'OpenVPN-Test-Client2', both linked to the 'OpenVPN-Test-Client2' user.

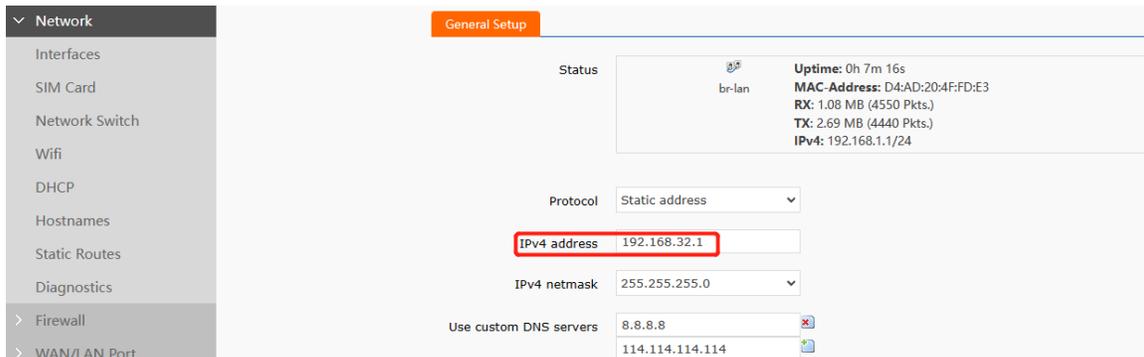
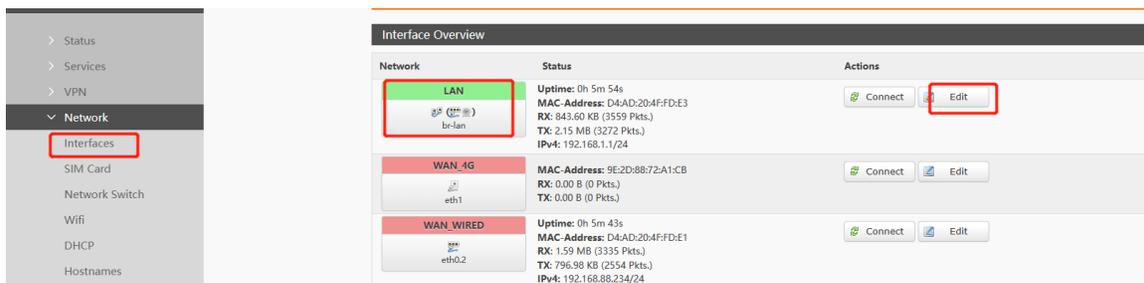
The downloaded file.



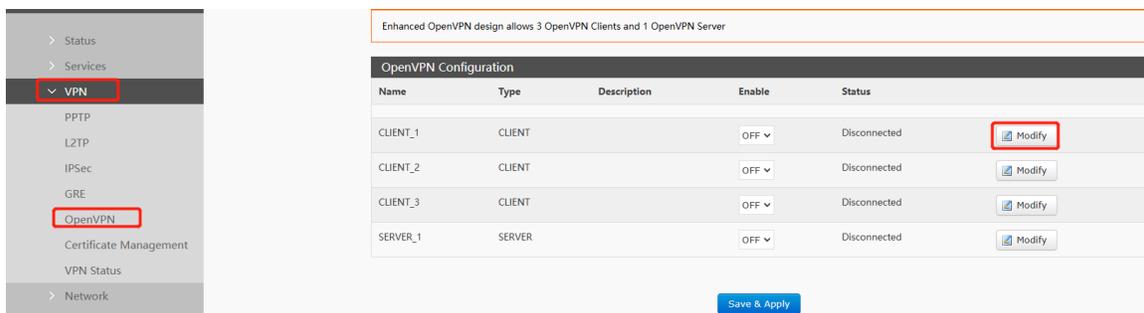
3. Configure router's parameters

3.1 Configure the first router as OpenVPN Client1

1>Change LAN IP to 192.168.32.1



2>Modify the OpenVPN parameter,

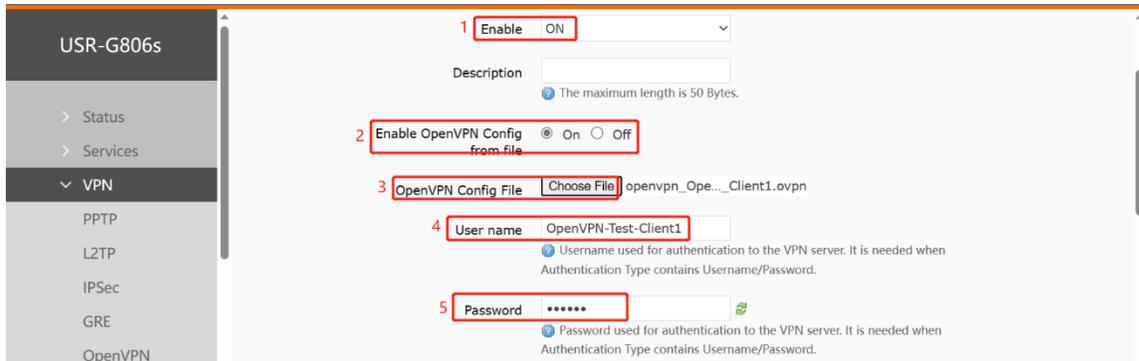


3>OpenVPN Config File: choose the "client1.ovpn" file downloaded in Chapter 2.7,

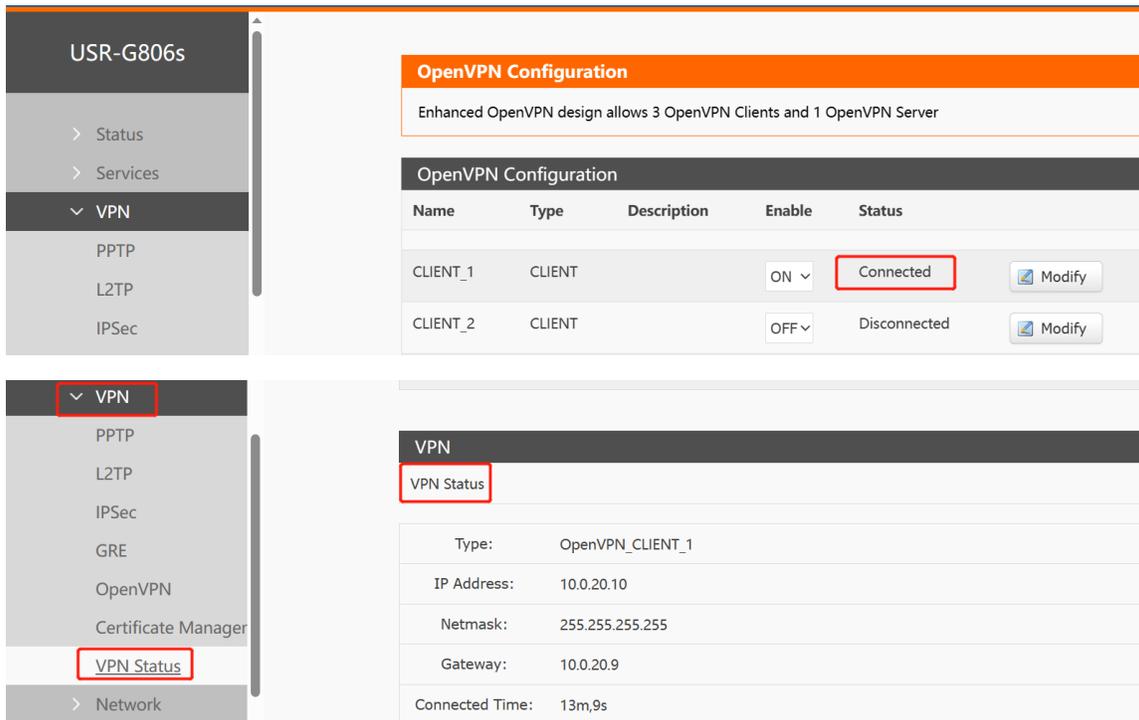
4>User name: The entered name of the OpenVPN-Test-Client1 in Chapter 2.3,

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.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	172.16.10.1	0.0.0.0	UG	0	0	0	eth0.2
0.0.0.0	172.16.10.1	0.0.0.0	UG	5	0	0	eth0.2
10.0.20.0	10.0.20.9	255.255.255.0	UG	0	0	0	tun_CLIENT_1
10.0.20.9	0.0.0.0	255.255.255.255	UH	0	0	0	tun_CLIENT_1
172.16.10.0	0.0.0.0	255.255.254.0	U	5	0	0	eth0.2
192.168.32.0	0.0.0.0	255.255.255.0	U	0	0	0	br-lan
192.168.33.0	10.0.20.9	255.255.255.0	UG	0	0	0	tun_CLIENT_1

3.2 Configure the second router as OpenVPN Client2

1>The LAN IP of the second router is 192.168.33.1

Status: br-lan
 Uptime: 5h 54m 54s
 MAC-Address: D4:AD:20:5F:55:14
 RX: 6.68 MB (34377 Pkts.)
 TX: 38.56 MB (40765 Pkts.)
 IPv4: 192.168.33.1/24

Protocol: Static address

IPv4 address: 192.168.33.1

IPv4 netmask: 255.255.255.0

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,

Configuration

1 Enable: ON

Description: [Empty field]

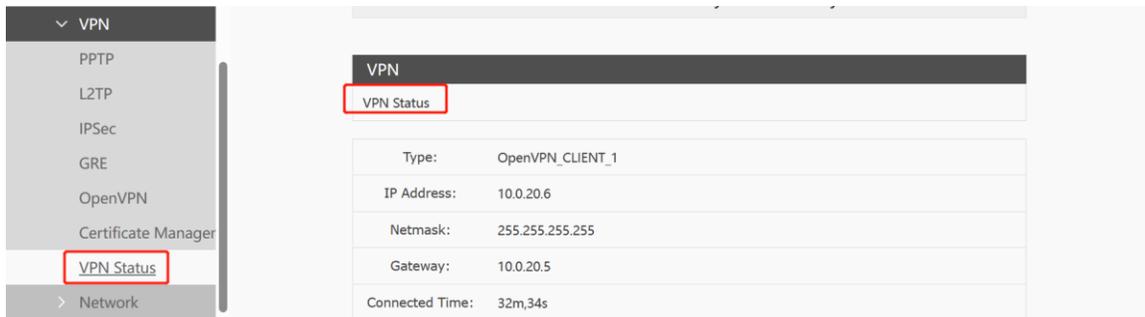
2 Enable OpenVPN Config from file: On

3 OpenVPN Config File: Choose File | openvpn_Ope...Client2.ovpn

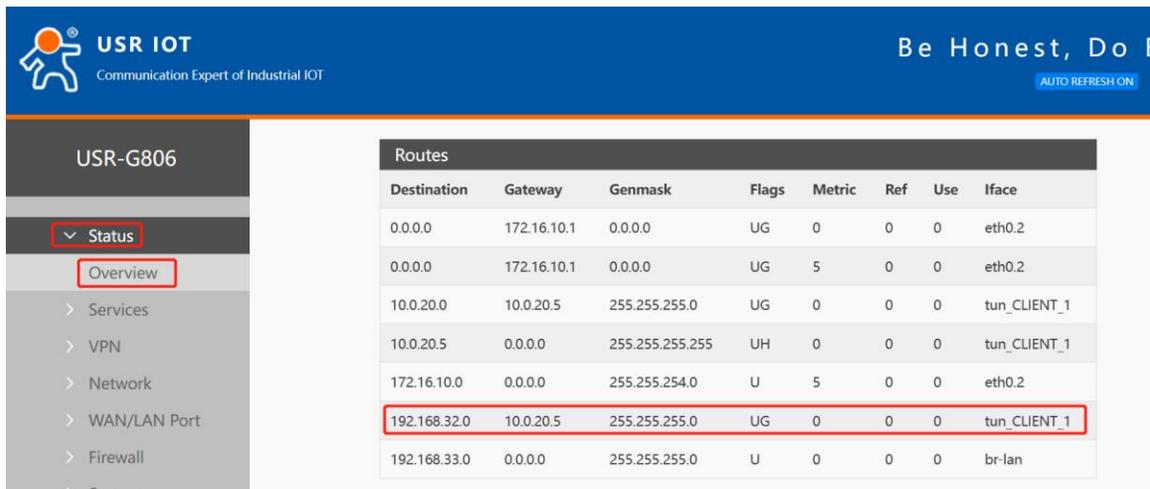
4 User name: OpenVPN-Test-Client2

5 Password: [Masked]

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 is 192.168.32.182, and the IP of PC2(phone) is 192.168.33.170.

```

Administrator: C:\Windows\system32\cmd.exe

Connection-specific DNS Suffix . : lan
Link-local IPv6 Address . . . . . : fe80::c7d1:c:124c:cf62%22
IPv4 Address. . . . . : 192.168.32.182 1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.32.1

Ethernet adapter 以太网:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2cff:fa3c:6311:3405%23
IPv4 Address. . . . . : 172.16.10.31
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 172.16.10.1

C:\Users\Administrator>ping 192.168.33.170 2

Pinging 192.168.33.170 with 32 bytes of data:
Reply from 192.168.33.170: bytes=32 time=19ms TTL=62
Reply from 192.168.33.170: bytes=32 time=38ms TTL=62
Reply from 192.168.33.170: bytes=32 time=25ms TTL=62
Reply from 192.168.33.170: bytes=32 time=38ms TTL=62

Ping statistics for 192.168.33.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 38ms, Average = 30ms

C:\Users\Administrator>

```

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