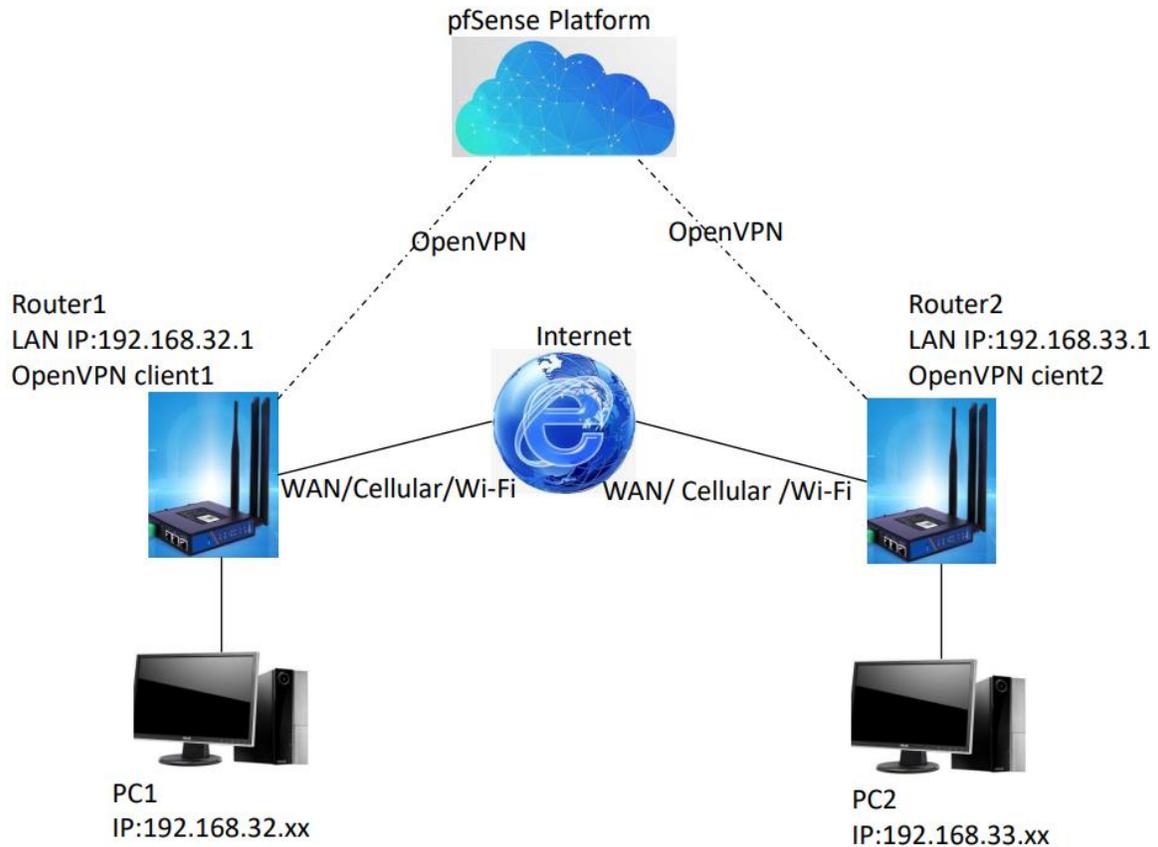


## PUSR Routers Connect to pfSense Server

### 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

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Search

Search term  Both Search Clear

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN_CA	<input checked="" type="checkbox"/>	self-signed	4	ST=SD, OU=znyl, O=usr, L=JiNan, CN=internal-ca, C=CN Valid From: Thu, 23 Mar 2023 15:10:21 +0800 Valid Until: Sun, 20 Mar 2023 15:10:21 +0800	OpenVPN Server	

+ Add

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

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

3>Click "Save" button.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate Manager / CAs / Edit

CA's Certificates Certificate Revocation

Create / Edit CA

Describe the name OpenVPN-Test-CA

Method Create an internal Certificate Authority

Trust Store  Add this Certificate Authority to the Operating System Trust Store  
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial  Use random serial numbers when signing certificates  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type RSA

2048  
The length to use when generating a new RSA key, in bits.  
The key length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256  
The digest method used when the CA is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime (days) 3650

Common Name internal-ca

The following certificate authority subject components are optional and may be left blank.

Country Code CN

State or Province SD

City JiNan

Organization PUSB

Organizational Unit PUSB

Save

CA's   Certificates   Certificate Revocation

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN_CA	✓	self-signed	4	ST=SD, OU=znlly, O=usr, L=JiNan, CN=internal-ca, C=CN Valid From: Thu, 23 Mar 2023 15:10:21 +0800 Valid Until: Sun, 20 Mar 2023 15:10:21 +0800	OpenVPN Server	
OpenVPN-Test-CA	✓	self-signed	0	ST=SD, OU=PUSR, O=PUSR, L=Jinan, CN=internal-ca, C=CN Valid From: Tue, 11 Apr 2023 19:07:56 +0800 Valid Until: Fri, 08 Apr 2023 19:07:56 +0800		

## 2.2 Create Server Certificate

1>System->Cert. Manager->Certificates

System / Certificate Manager / Certificates

CA's   Certificates   Certificate Revocation

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificates**

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (63f5e79b61d3) Server Certificate CA: No Server: Yes	self-signed	O=ySense webConfigurator Self-Signed Certificate, CN=ySense-63f5e79b61d3 Valid From: Wed, 22 Feb 2023 16:30:34 +0800 Valid Until: Tue, 24 Mar 2023 16:30:34 +0800		
OpenVPN_Server56_Cert Server Certificate CA: No Server: Yes	OpenVPN_CA	ST=SD, OU=znlly, O=usr, L=JiNan, CN=OpenVPN_Server56_Cert, C=CN Valid From: Thu, 23 Mar 2023 15:14:18 +0800 Valid Until: Sun, 20 Mar 2023 15:14:18 +0800	OpenVPN Server	
OpenVPN_Client5_Cert User Certificate CA: No Server: No	OpenVPN_CA	ST=SD, OU=znlly, O=usr, L=JiNan, CN=OpenVPN_Client5, C=CN Valid From: Thu, 23 Mar 2023 15:14:59 +0800 Valid Until: Sun, 20 Mar 2023 15:14:59 +0800		
OpenVPN_Client5_Cert User Certificate CA: No Server: No	OpenVPN_CA	ST=SD, OU=znlly, O=usr, L=JiNan, CN=OpenVPN_Client5, C=CN Valid From: Thu, 23 Mar 2023 15:15:41 +0800 Valid Until: Sun, 20 Mar 2023 15:15:41 +0800	User Cert	
OpenVPN_Client5_Cert User Certificate CA: No Server: No	OpenVPN_CA	ST=SD, OU=znlly, O=usr, L=JiNan, CN=OpenVPN_Client5, C=CN Valid From: Thu, 23 Mar 2023 15:16:08 +0800 Valid Until: Sun, 20 Mar 2023 15:16:08 +0800	User Cert	

ySense is developed and maintained by Netgate. © 2023. View license.

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"

**Method** Create an internal Certificate

**Descriptive name** OpenVPN-Server-Test-Cert

---

**Internal Certificate**

**Certificate authority** OpenVPN-Test-CA

**Key type** RSA

**Key length** 2048  
The length to use when generating a new RSA key, in bits. The best practice is to use an algorithm stronger than SHA-1. Some platforms may consider weaker digest algorithms invalid.

**Digest Algorithm** sha256  
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA-1. Some platforms may consider weaker digest algorithms invalid.

**Lifetime (days)** 3650  
The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days on some platforms may consider the certificate invalid.

**Common Name** OpenVPN-Server-Test-Cert  
The following certificate subject components are optional and may be left blank.

**Country Code** CN

**State or Province** SD

**City** Jinan

**Organization** PUSR

**Organizational Unit** PUSR

---

**Certificate Attributes**

**Attribute Notes**  
The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.  
 For Internal Certificates, these attributes are added directly to the certificate as shown.

**Certificate Type** Server Certificate  
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

**Alternative Names**  
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

**Add** [+ Add](#) [Save](#)

## 2.3 Add users and create user certificates

1>System->User Manager->Users

System / User Manager / Users

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

Username	Full name	Status	Groups	Actions
<input type="checkbox"/> OpenVPN_Client5		✓		<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> OpenVPN_Client6		✓		<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> admin	System Administrator	✓	admins	<a href="#">Edit</a> <a href="#">Delete</a>

[+ Add](#) [Delete](#)

pfSense is developed and maintained by Netgate. © 2004 - 2021. [View license.](#)

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" ,

The screenshot shows the pfSense User Manager interface. At the top, the navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is System / User Manager / Users / Edit. The 'Users' tab is selected. The 'User Properties' section includes fields for Username (OpenVPN-Client1-Test), Password, Full name, Expiration date, Custom Settings, Group membership (admins), and Certificate (Click to create a user certificate). Below this is the 'Create Certificate for User' section with fields for Descriptive name and Certificate authority (OpenVPN\_CA).

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

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

This screenshot shows the 'Create Certificate for User' section in detail. The 'Descriptive name' is set to 'OpenVPN-Client1-Test-Cert' and the 'Certificate authority' is set to 'OpenVPN-Test-CA'. The 'Key type' is RSA with a length of 2048 bits. The 'Digest Algorithm' is sha256 and the 'Lifetime' is 3650 days. Below this is the 'Keys' section with fields for Authorized SSH Keys and IPsec Pre-Shared Key. A 'Save' button is visible at the bottom.

#### 4>Add the second user using the same steps

Users Groups Settings Authentication Servers

### User Properties

Defined by: USER

Disabled:  This user cannot login

**Username**: OpenVPN-Client2-Test

**Password**: \*\*\*\*\*

Full name:   
User's full name, for administrative information only

Expiration date:   
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings:  Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Not member of:

Member of:

[Move to "Member of" list](#) [Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

**Certificate**  Click to create a user certificate

### Create Certificate for User

**Descriptive name**: OpenVPN-Client2-Test-Cert

**Certificate authority**: OpenVPN-Test-CA

#### 5>Users are added successfully.

System / User Manager / Users

Users Groups Settings Authentication Servers

Username	Full name	Status	Groups	Actions
<input type="checkbox"/> OpenVPN-Client1-Test		✓		<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> OpenVPN-Client2-Test		✓		<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> OpenVPN-Client5		✓		<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> OpenVPN-Client6		✓		<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> admin	System Administrator	✓	admins	<a href="#">Edit</a>

[Add](#) [Delete](#)

pSense is developed and maintained by Netgate. © 1997-2020. View license.

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

Server: <b>No</b>				
OpenVPN-Server-Test-CA Server Certificate CA: <b>No</b> Server: <b>Yes</b>	OpenVPN-Test-CA	ST=SD, OU=PUSR, O=PUSR, L=Jinan, CN=OpenVPN-Server-Test-CA	Valid From: Tue, 18 Apr 2023 19:14:32 +0800 Valid Until: Fri, 15 Apr 2023 19:14:32 +0800	Server Cert
OpenVPN-Client1-Test-Cert User Certificate CA: <b>No</b> Server: <b>No</b>	OpenVPN-Test-CA	ST=SD, OU=PUSR, O=PUSR, L=Jinan, CN=OpenVPN-Client1-Test	Valid From: Tue, 18 Apr 2023 19:22:50 +0800 Valid Until: Fri, 15 Apr 2023 19:22:50 +0800	User Cert
OpenVPN-Client2-Test-Cert User Certificate CA: <b>No</b> Server: <b>No</b>	OpenVPN-Test-CA	ST=SD, OU=PUSR, O=PUSR, L=Jinan, CN=OpenVPN-Client2-Test	Valid From: Tue, 18 Apr 2023 19:24:25 +0800 Valid Until: Fri, 15 Apr 2023 19:24:25 +0800	User Cert

[+ Add/Sign](#)

## 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

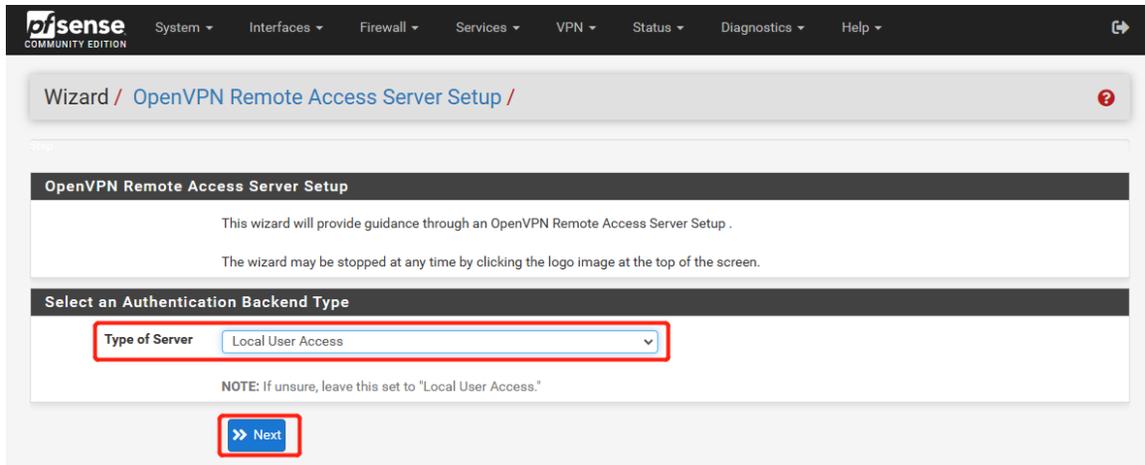
## 2.5 Configure OpenVPN Server

1>VPN->OpenVPN->Wizards

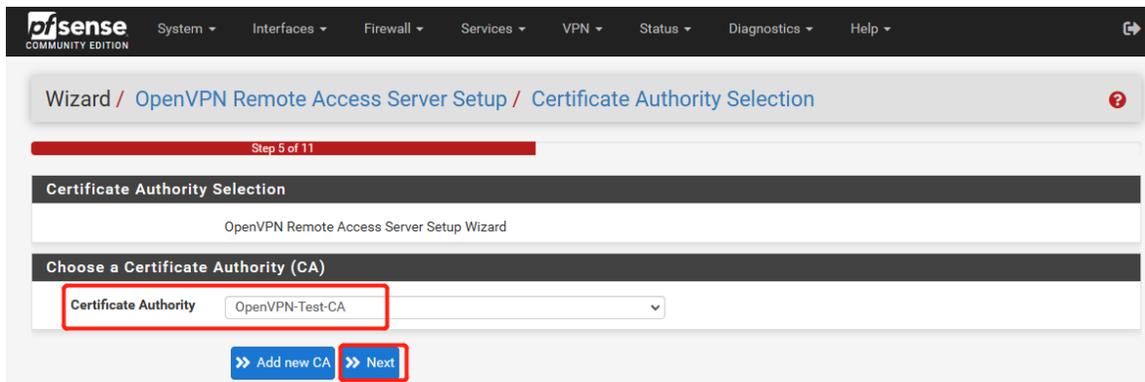
The screenshot shows the pfSense OpenVPN Servers configuration page. The 'Wizards' tab is highlighted with a red box and three red arrows pointing to it. Below the tabs is a table of OpenVPN Servers.

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1193 (TUN)	100.100.100.0/24	Mode: Remote Access ( SSL/TLS ) Data Ciphers: AES-128-GCM, AES-128-CBC Digest: SHA256 D-H Params: 2048 bits		
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	Mode: Remote Access ( SSL/TLS ) Data Ciphers: AES-128-GCM, AES-128-CBC Digest: SHA256 D-H Params: 2048 bits		

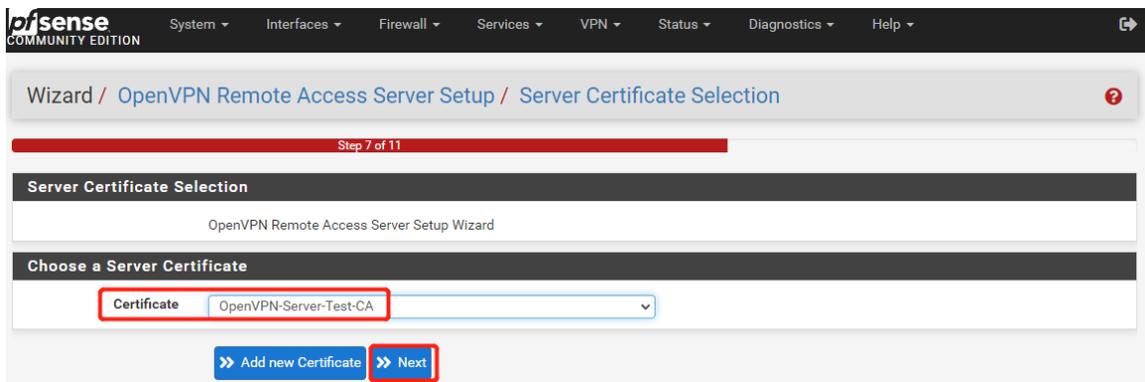
2>Type of Server: Local User Access



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.

### Tunnel Settings

**Tunnel Network**    
 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

**Redirect Gateway**    
 Force all client generated traffic through the tunnel.

**Local Network**    
 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

**Concurrent Connections**    
 Specify the maximum number of clients allowed to concurrently connect to this server.

**Allow Compression**    
 Allow compression to be used with this VPN instance, which is potentially insecure.

**Compression**    
 Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

**Type-of-Service**    
 Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

**Inter-Client Communication**    
 Allow communication between clients connected to this server.

**Duplicate Connections**    
 Allow multiple concurrent connections from clients using the same Common Name.   
 NOTE: This is not generally recommended, but may be needed for some scenarios.

6> Firewall and OpenVPN rules are enabled by default.

### Traffic from clients to server

**Firewall Rule**    
 Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

### Traffic from clients through VPN

**OpenVPN rule**    
 Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[Next](#)

7> OpenVPN server is added successfully.

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

### OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1193 (TUN)	100.100.100.0/24	Mode: Remote Access ( SSL/TLS ) Data Ciphers: AES-128-GCM, AES-128-CBC Digest: SHA256 D-H Params: 2048 bits		
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	Mode: Remote Access ( SSL/TLS ) Data Ciphers: AES-128-GCM, AES-128-CBC Digest: SHA256 D-H Params: 2048 bits		
WAN	UDP4 / 1195 (TUN)	10.0.10.0/24	Mode: Remote Access ( SSL/TLS + User Auth ) Data Ciphers: AES-128-GCM, AES-128-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN Server for Test	

Server mode: Select "Remote Access(SSL/TLS)"

**Mode Configuration**

**Server mode** Remote Access ( SSL/TLS )

**Device mode** tun - Layer 3 Tunnel Mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Select "AES-128-CBC"

**Data Encryption Algorithms**

AES-128-CBC (128 bit key, 128 bit block)

AES-128-CFB (128 bit key, 128 bit block)

AES-128-CFB1 (128 bit key, 128 bit block)

AES-128-CFB8 (128 bit key, 128 bit block)

AES-128-GCM (128 bit key, 128 bit block)

AES-128-OFB (128 bit key, 128 bit block)

AES-192-CBC (192 bit key, 128 bit block)

AES-192-CFB (192 bit key, 128 bit block)

AES-192-CFB1 (192 bit key, 128 bit block)

AES-192-CFB8 (192 bit key, 128 bit block)

Available Data Encryption Algorithms  
Click to add or remove an algorithm from the list

AES-128-CBC

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. ⓘ

## 2.6 Configure the OpenVPN client and subnet

- Add the first OpenVPN client

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

**OpenSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

VPN / OpenVPN / Client Specific Overrides

Servers Clients **Client Specific Overrides** Wizards Client Export Shared Key Export

**CSC Overrides**

Disabled	Common Name	Description	Actions
No	OpenVPN_Client5	OpenVPN_Client5	  
No	OpenVPN_Client6	OpenVPN_Client6	  

 Add

2> Description: OpenVPN-Client1-Test

Common name: OpenVPN-Client1-Test

Server List: Select "OpenVPN Server 3" added in Chapter 2.5

VPN / OpenVPN / Client Specific Overrides / Edit

Servers Clients **Client Specific Overrides** Wizards Client Export Shared Key Export

### General Information

**Description**   
 A description of this override for administrative reference.

**Disable**  Disable this override  
 Set this option to disable this client-specific override without removing it from the list.

### Override Configuration

**Common Name**   
 Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive. Enter "DEFAULT" to override default client behavior.

**Connection blocking**  Block this client connection based on its common name.  
 Prevents the client from connecting to this server. Do not use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.

**Server List**   
 Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.

### 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,

### Tunnel Settings

**IPv4 Tunnel Network**   
 The virtual IPv4 network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.5/24).  
 With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network on the server.  
 With net30 topology, the first network address of the /30 is assumed to be the server address and the second network address will be assigned to the client.

**IPv6 Tunnel Network**   
 The virtual IPv6 network or network type alias with a single entry used for private communications between this client and the server expressed using prefix (e.g. 2001:db9:1:1::100/64).  
 Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.

**IPv4 Local Network/s**   
 These are the IPv4 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases.  
 NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

**IPv6 Local Network/s**   
 These are the IPv6 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more IP/PREFIX networks.  
 NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

**IPv4 Remote Network/s**   
 These are the IPv4 client-side networks that will be routed to this client specifically using iroute, so that a site-to-site VPN can be established. Expressed as a comma-separated list of one or more CIDR ranges. May be left blank if there are no client-side networks to be routed.  
 NOTE: Remember to add these subnets to the IPv4 Remote Networks list on the corresponding OpenVPN server settings.

**IPv6 Remote Network/s**   
 These are the IPv6 client-side networks that will be routed to this client specifically using iroute, so that a site-to-site VPN can be established. Expressed as a comma-separated list of one or more IP/PREFIX networks. May be left blank if there are no client-side networks to be routed.  
 NOTE: Remember to add these subnets to the IPv6 Remote Networks list on the corresponding OpenVPN server settings.

**Redirect Gateway**  Force all client generated traffic through the tunnel.

- 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

VPN / OpenVPN / Client Specific Overrides / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

### General Information

**Description** OpenVPN-Client2-Test  
A description of this override for administrative reference.

**Disable**  Disable this override  
Set this option to disable this client-specific override without removing it from the list.

### Override Configuration

**Common Name** OpenVPN-Client2-Test  
Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive. Enter "DEFAULT" to override default client behavior.

**Connection blocking**  Block this client connection based on its common name.  
Prevents the client from connecting to this server. Do not use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.

**Server List**  
OpenVPN Server 1:  
OpenVPN Server 2:  
OpenVPN Server 3: OpenVPN Server for Test  
Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.

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,

### Tunnel Settings

**IPv4 Tunnel Network**  
The virtual IPv4 network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.5/24).  
With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network on the server.  
With net30 topology, the first network address of the /30 is assumed to be the server address and the second network address will be assigned to the client.

**IPv6 Tunnel Network**  
The virtual IPv6 network or network type alias with a single entry used for private communications between this client and the server expressed using prefix (e.g. 2001:db9:1:1::100/64).  
Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.

**IPv4 Local Network/s** 192.168.33.0/24  
These are the IPv4 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases.  
NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

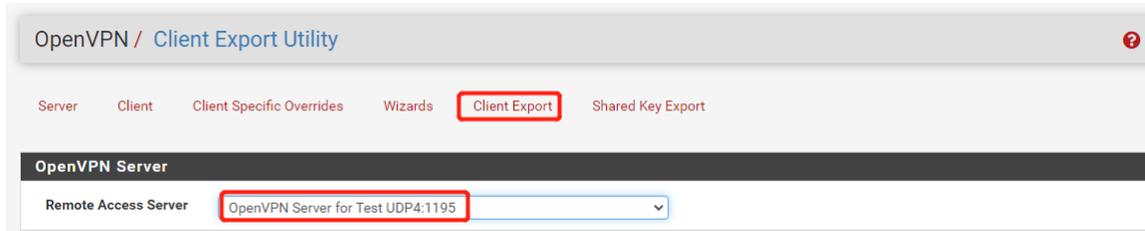
**IPv6 Local Network/s**  
These are the IPv6 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more IP/PREFIX networks.  
NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

**IPv4 Remote Network/s** 192.168.32.0/24  
These are the IPv4 client-side networks that will be routed to this client specifically using iroute, so that a site-to-site VPN can be established. Expressed as a comma-separated list of one or more CIDR ranges. May be left blank if there are no client-side networks to be routed.  
NOTE: Remember to add these subnets to the IPv4 Remote Networks list on the corresponding OpenVPN server settings.

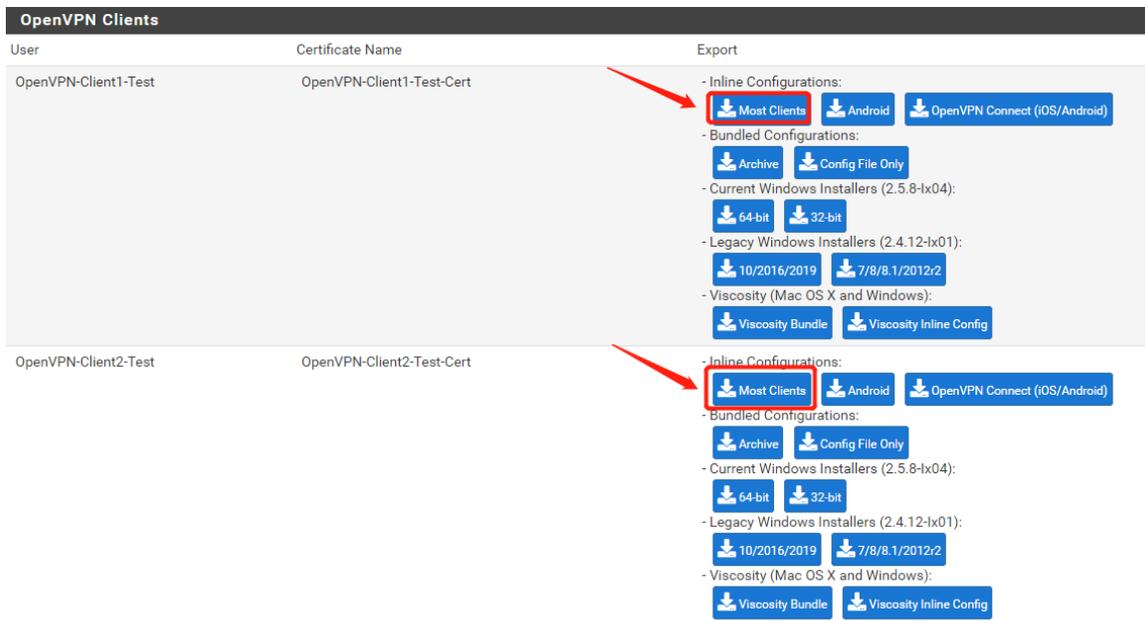
## 2.7 Export the OpenVPN client package

VPN->OpenVPN->Client Export

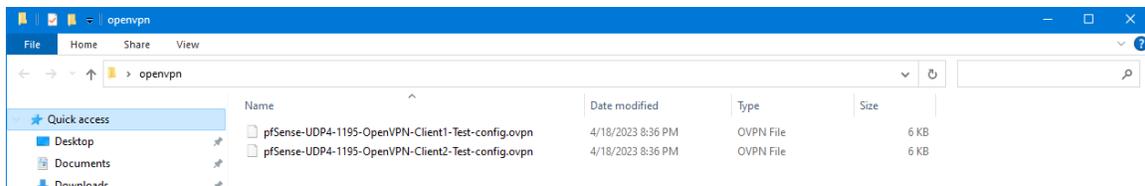
1>Remote Access Server: Select the OpenVPN Server added in chapter 2.5,



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

Interface Overview

Network	Status	Actions
<b>LAN</b> br-lan	Uptime: 0h 5m 54s MAC Address: D4:AD:20:4F:FD:E3 RX: 843.60 KB (3559 Pkts.) TX: 2.15 MB (3272 Pkts.) IPv4: 192.168.1.1/24	Connect Edit
<b>WAN_4G</b> eth1	MAC Address: 9E:2D:88:72:A1:C8 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Edit
<b>WAN WIRED</b> eth0.2	Uptime: 0h 5m 43s MAC Address: D4:AD:20:4F:FD:E1 RX: 1.59 MB (3335 Pkts.) TX: 796.98 KB (2554 Pkts.) IPv4: 192.168.88.234/24	Connect Edit

General Setup

Status: br-lan, Uptime: 0h 7m 16s, MAC Address: D4:AD:20:4F:FD:E3, RX: 1.08 MB (4550 Pkts.), TX: 2.69 MB (4440 Pkts.), IPv4: 192.168.1.1/24

Protocol: Static address

IPv4 address: 192.168.32.1

IPv4 netmask: 255.255.255.0

Use custom DNS servers: 8.8.8.8, 114.114.114.114

2>Modify the OpenVPN parameters

Enhanced OpenVPN design allows 3 OpenVPN Clients and 1 OpenVPN Server

OpenVPN Configuration

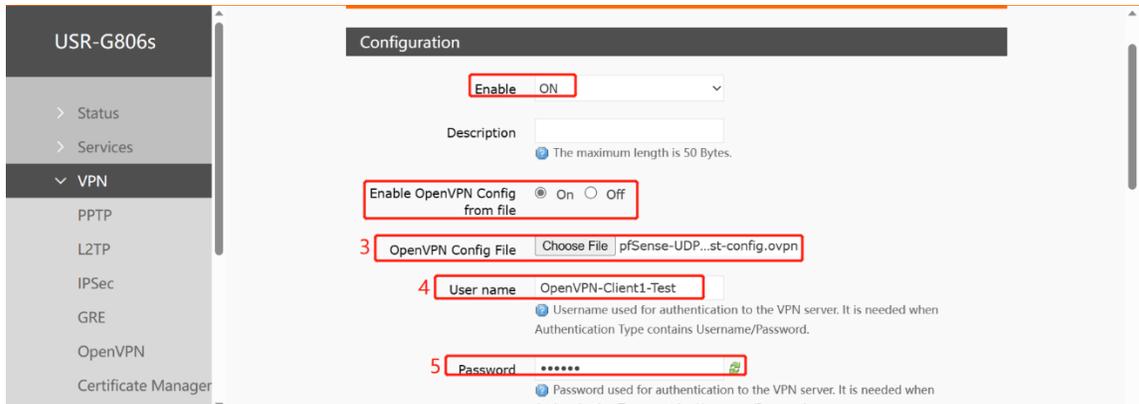
Name	Type	Description	Enable	Status	Actions
CLIENT_1	CLIENT		OFF	Disconnected	Modify
CLIENT_2	CLIENT		OFF	Disconnected	Modify
CLIENT_3	CLIENT		OFF	Disconnected	Modify
SERVER_1	SERVER		OFF	Disconnected	Modify

Save & Apply

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

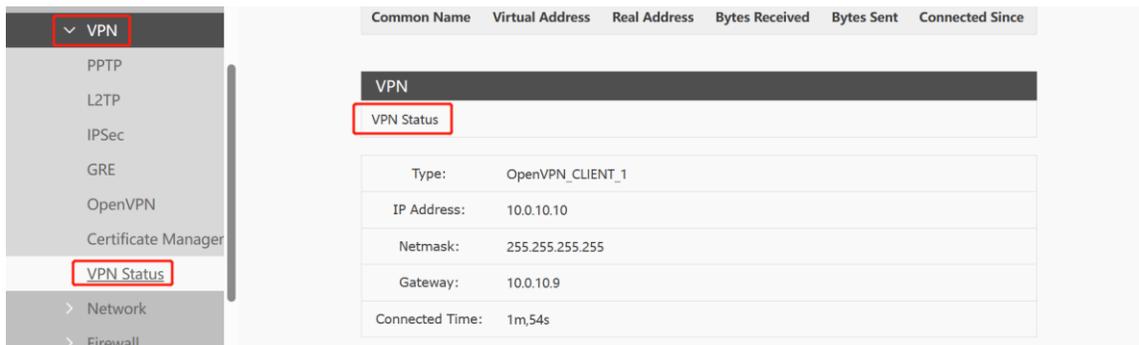
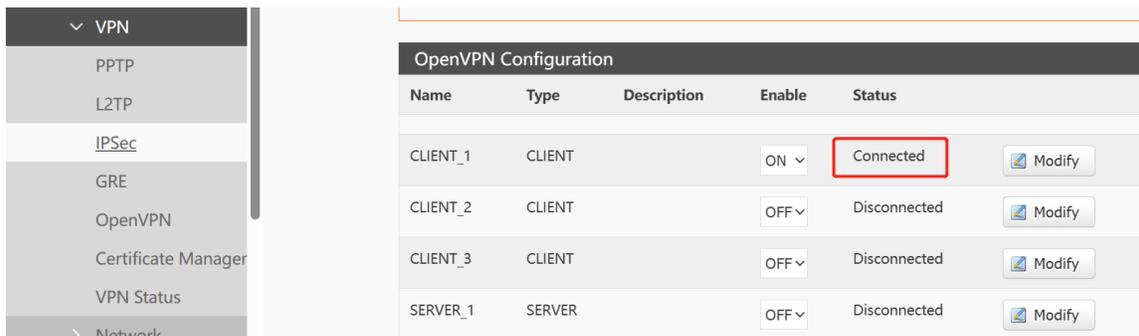
4>User name: The entered name of the OpenVPN-Test-Client1 in Chapter 2.3

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. This route is very important, without it, the network devices connect to router can't communicate with each other.

USR-G806s								
Routes								
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	
10.0.10.0	10.0.10.9	255.255.255.0	UG	0	0	0	tun_CLIENT_1	
10.0.10.9	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	10.0.10.9	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,

General Setup

Status

**Uptime:** 9h 38m 26s

**MAC-Address:** D4:AD:20:5F:55:14

**RX:** 26.51 MB (256473 Pkts.)

**TX:** 470.52 MB (360892 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-Test-config.ovpn" file downloaded in Chapter 2.7

3>User name: The entered name of the "OpenVPN-Client2-Test" in Chapter 2.3

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

5>Click "Save & Apply" button,

**Configuration**

Enable  ON

Description   
The maximum length is 50 Bytes.

2 Enable OpenVPN Config from file  On  Off

3 OpenVPN Config File  pfSense-UDP...st-config.ovpn

4 User name   
Username used for authentication to the VPN server. It is needed when Authentication Type contains Username/Password.

5 Password

Password used for authentication to the VPN server. It is needed when

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

Services

- VPN
  - PPTP
  - L2TP
  - IPSec
  - GRE
  - OpenVPN
  - Certificate Manager
  - VPN Status**
- Network

**OpenVPN Clients Info**

Common Name	Virtual Address	Real Address	Bytes Received	Bytes Sent	Connected Since
<b>VPN</b>					
<b>VPN Status</b>					
Type:	OpenVPN_CLIENT_1				
IP Address:	10.0.10.6				
Netmask:	255.255.255.255				
Gateway:	10.0.10.5				
Connected Time:	12s				

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.

**USR-G806**

- Status**
  - Overview**
  - Services
  - VPN
  - Network
  - WAN/LAN Port
  - Firewall
  - System

**Routes**

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
10.0.10.0	10.0.10.5	255.255.255.0	UG	0	0	0	tun_CLIENT_1
10.0.10.5	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
<b>192.168.32.0</b>	<b>10.0.10.5</b>	<b>255.255.255.0</b>	<b>UG</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>tun_CLIENT_1</b>
192.168.33.0	0.0.0.0	255.255.255.0	U	0	0	0	br-lan

#### 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.

```
Wireless LAN adapter WLAN:
    Connection-specific DNS Suffix . : lan
    Link-local IPv6 Address . . . . . : fe80::c7d1:c:124c:cf62%22
    IPv4 Address. . . . . : 192.168.32.182
    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
Pinging 192.168.33.170 with 32 bytes of data:
Reply from 192.168.33.170: bytes=32 time=180ms TTL=62
Request timed out.
Reply from 192.168.33.170: bytes=32 time=16ms TTL=62
Reply from 192.168.33.170: bytes=32 time=200ms TTL=62

Ping statistics for 192.168.33.170:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 200ms, Average = 132ms
```

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
```