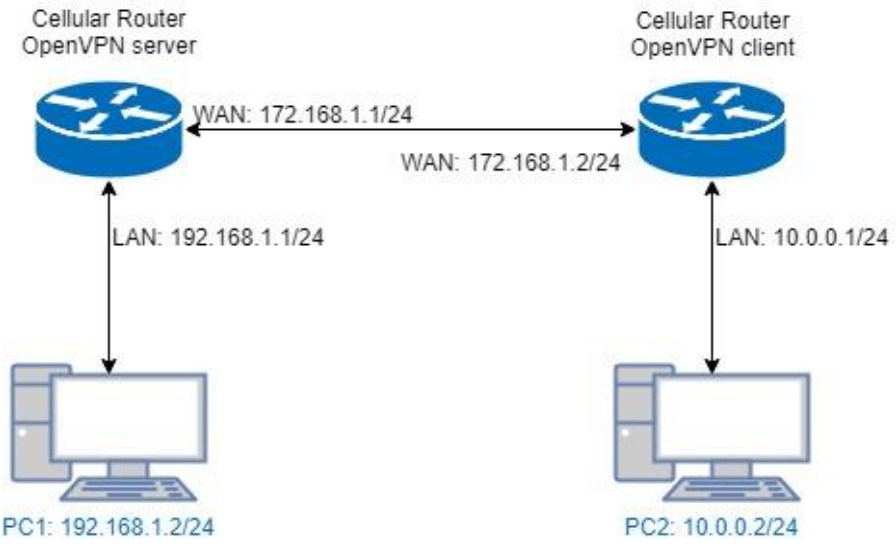
Creating Server/Client Net to Net OpenVPN on Xentino MR4xx Series

Subject	Creating Server/Client Net to Net OpenVPN on Xentino MR4xx Series Quick Guide
Related Models	All Xentino MR4xx Series
Doc Rev	0001
FW Version	All

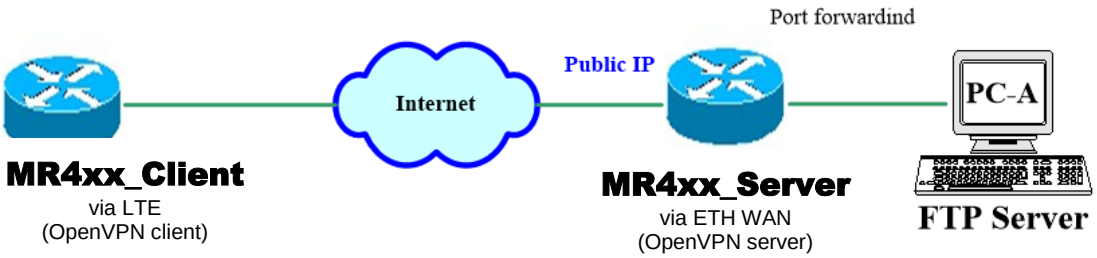
OpenVPN Server /Client Net-to-Net:

Topology:

You can use the OpenVPN VPN tunnel to make the PC1 and PC2 communicate each other.



If you prefer (**with the same configuration and results**):
- The Wan connection can be via LTE on the MR4xx Series OpenVPN client.
- The Wan connection can be via ETH getting a Public IP on the MR4XX OpenVPN Server.



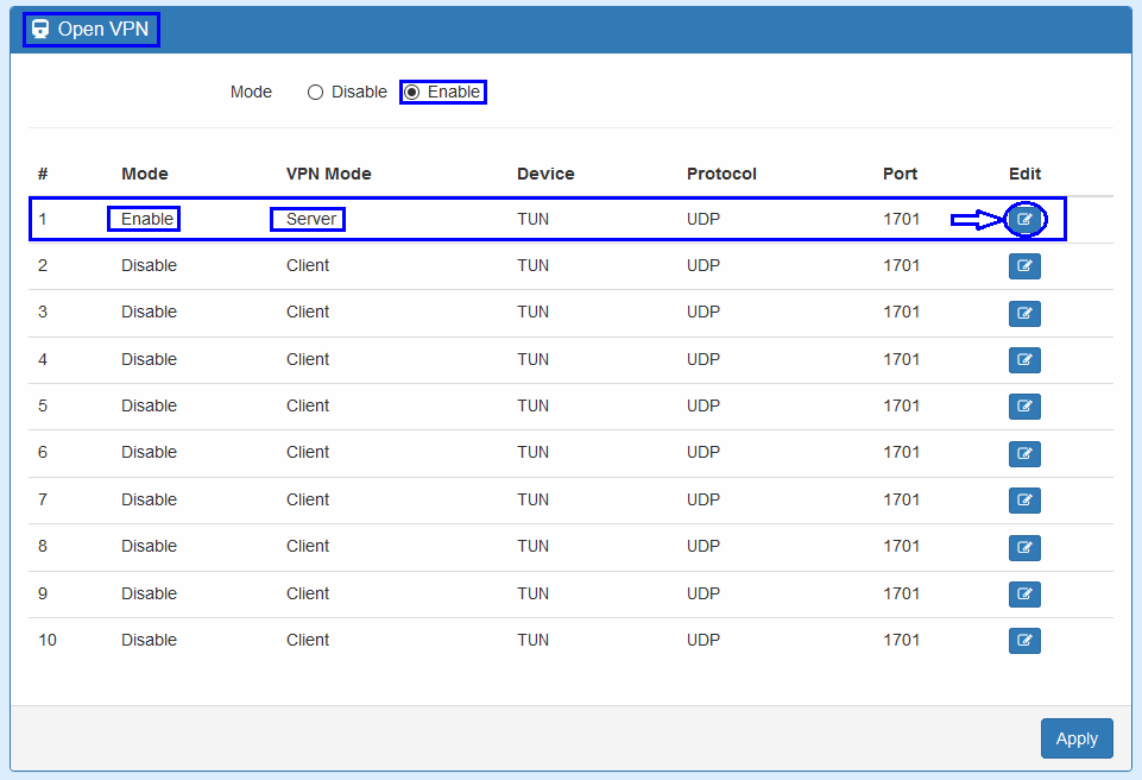
Open VPN Configuration:

Setup:

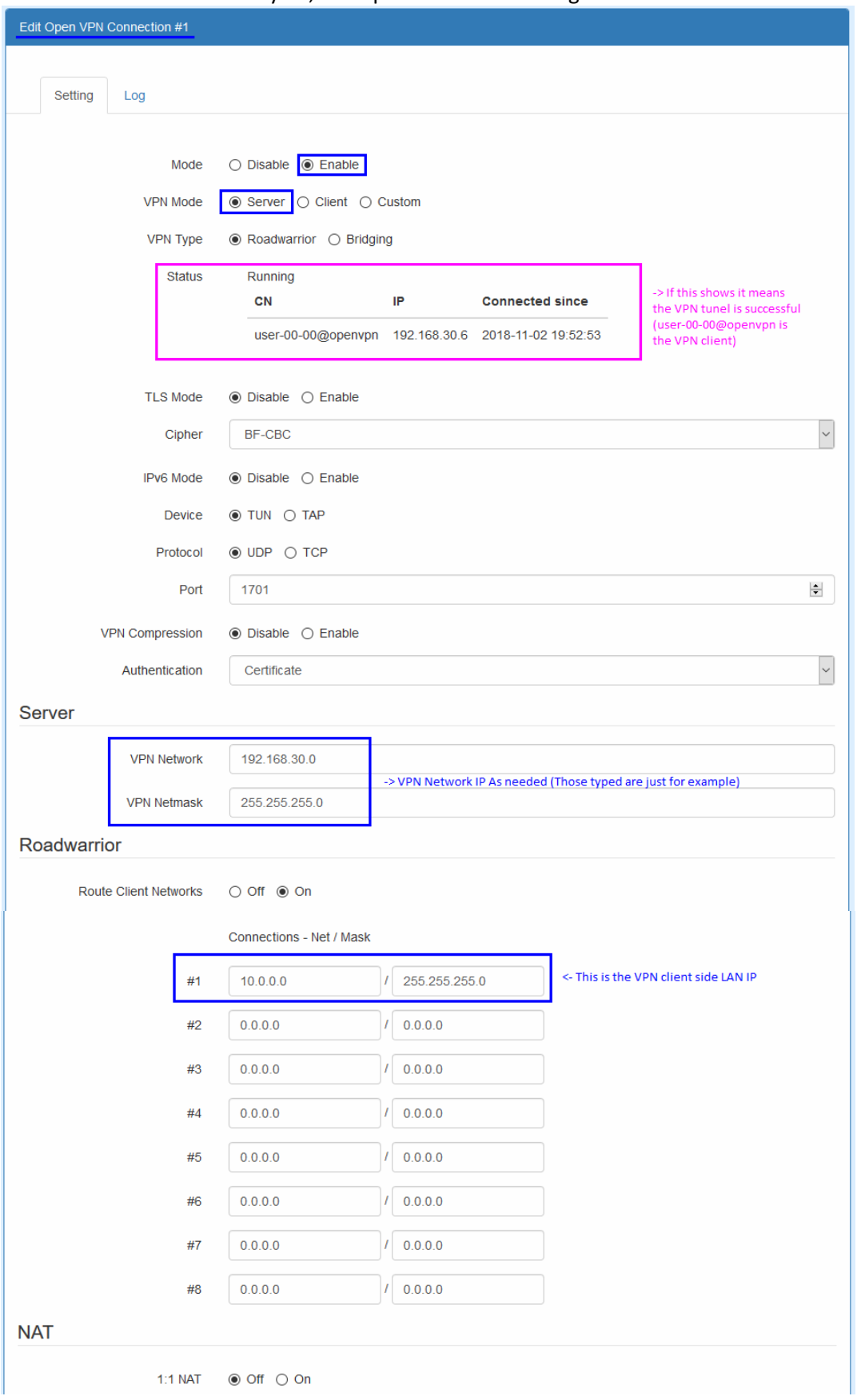
For Open VPN configuration, use the certificate to authenticate the VPN connection.
Thus, you need to generate the required files from the MR4xx Open VPN server and import them to the MR4xx Open VPN client.

(1) MR4xx OpenVPN server configuration

For the Open VPN server side, the basic settings as follows:



When click on the Edit button of entry #1, the OpenVPN Server configuration is like this:



The **VPN Network** and **VPN Netmask** are required fields.

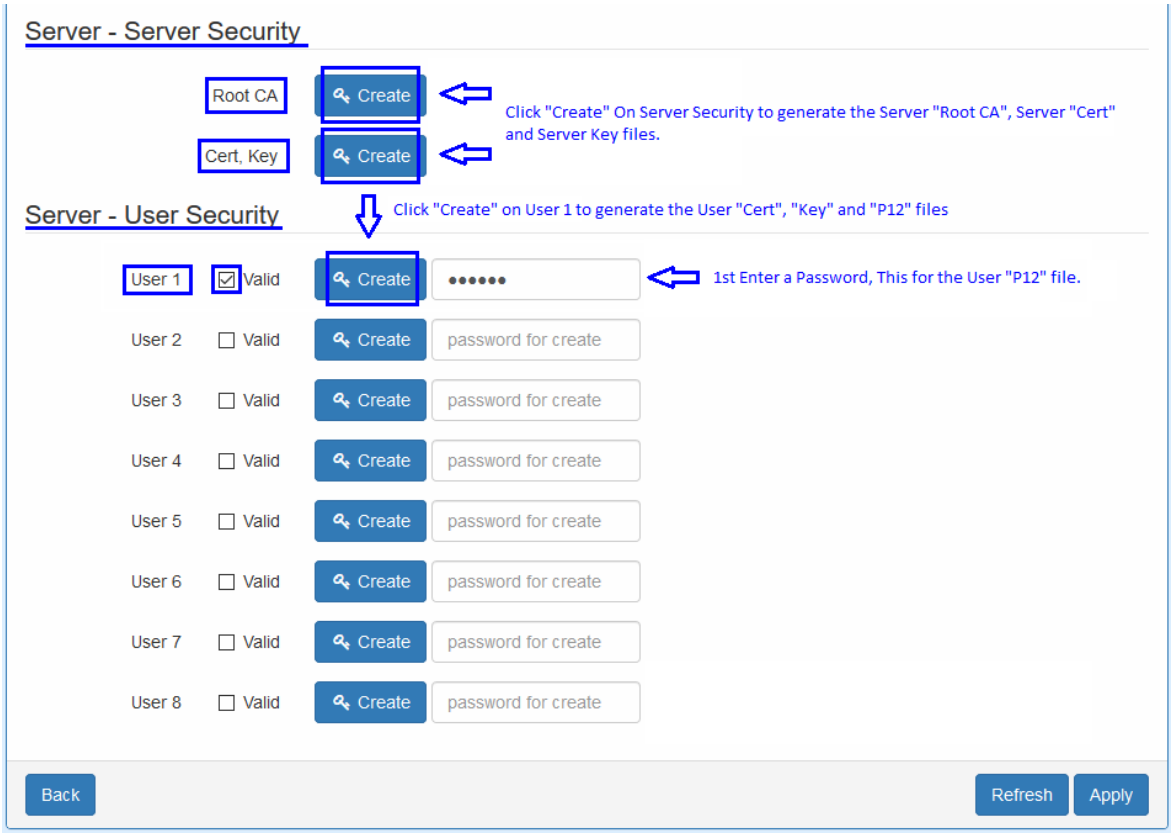
Note: The **VPN Network** should be desired network ID (e.g. **192.168.30.1** could be invalid setting.)

Note: For the PC1 and PC2 to communicate with each other, the "**Route Client Networks**" field should be enabled/On on both the OpenVPN Server and OpenVPN Client configuration.

Now add the LAN information of Open VPN client side, in this case the **#1** route will be **10.0.0.0** and **255.255.255.0** for our reference topology.

Note: The **#1** route means the routing information for **User 1**.

Open VPN server certificate generation:



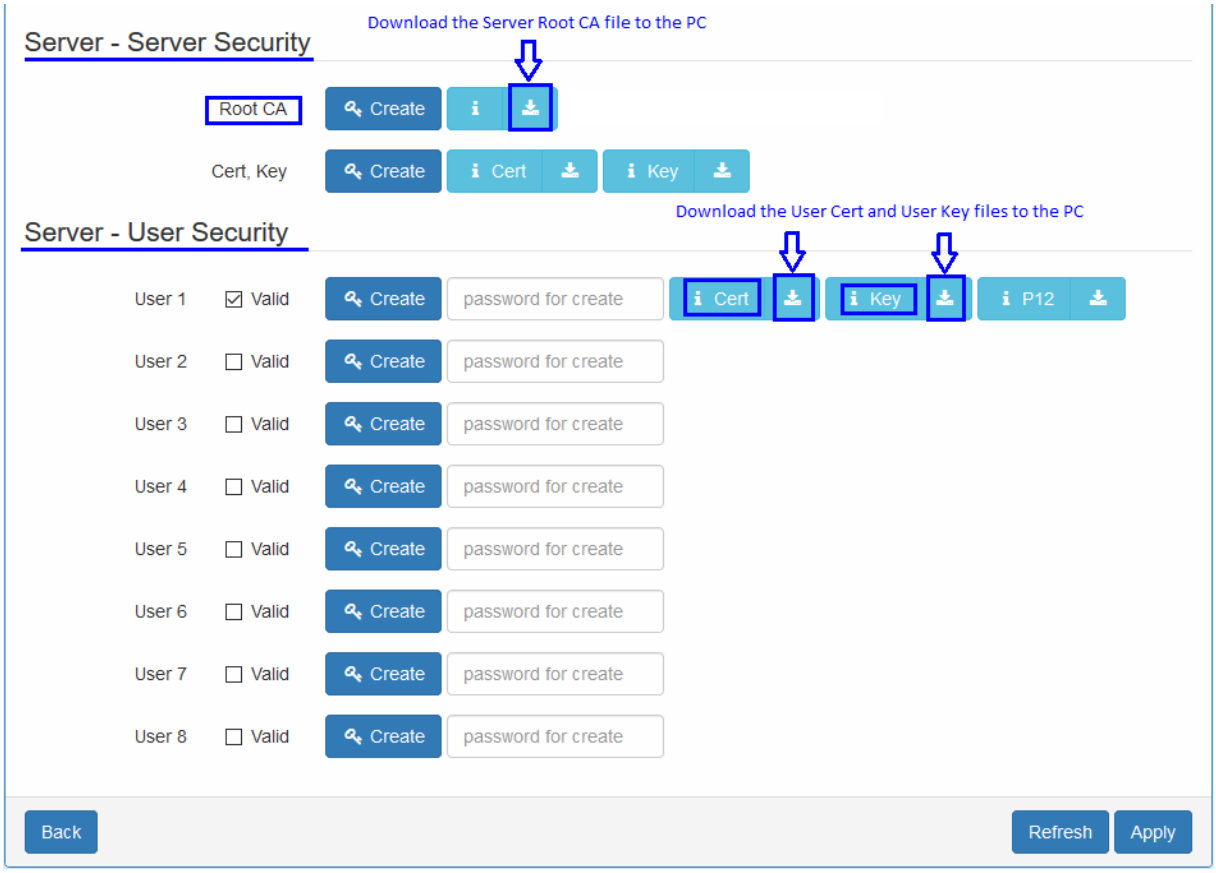
For the OpenVPN Server mode, the OpenVPN web UI provides the buttons to generate the required files. The files include **Root CA**, **Cert**, **Key** and **Open VPN** client files. The file will be generated when you click the corresponded **Create** button.

Note: The **Cert**, **Key** generation will takes around 10 minutes.

To generate the Open VPN client files, you need to type a password to create it.
The password will be used in the OpenVPN client when the client use **PKCS#12** to authenticate the VPN connection.

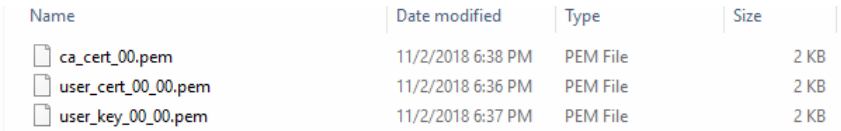
Note: we are not going to use the pkcs #12 Certificate "authentication" field option on the OpenVPN Client for this guide, so this password will not be used in our configuration example later on.

After the generation, the OpenVPN Server web UI shows as Follows:



You can click the info button to show the details for each files.

* Now please click the download button to download the **Server "Root CA" file**, the **User "Cert" file** and the **User "Key" file** to the PC so we can upload them later to the **MR4xx** OpenVPN Client.

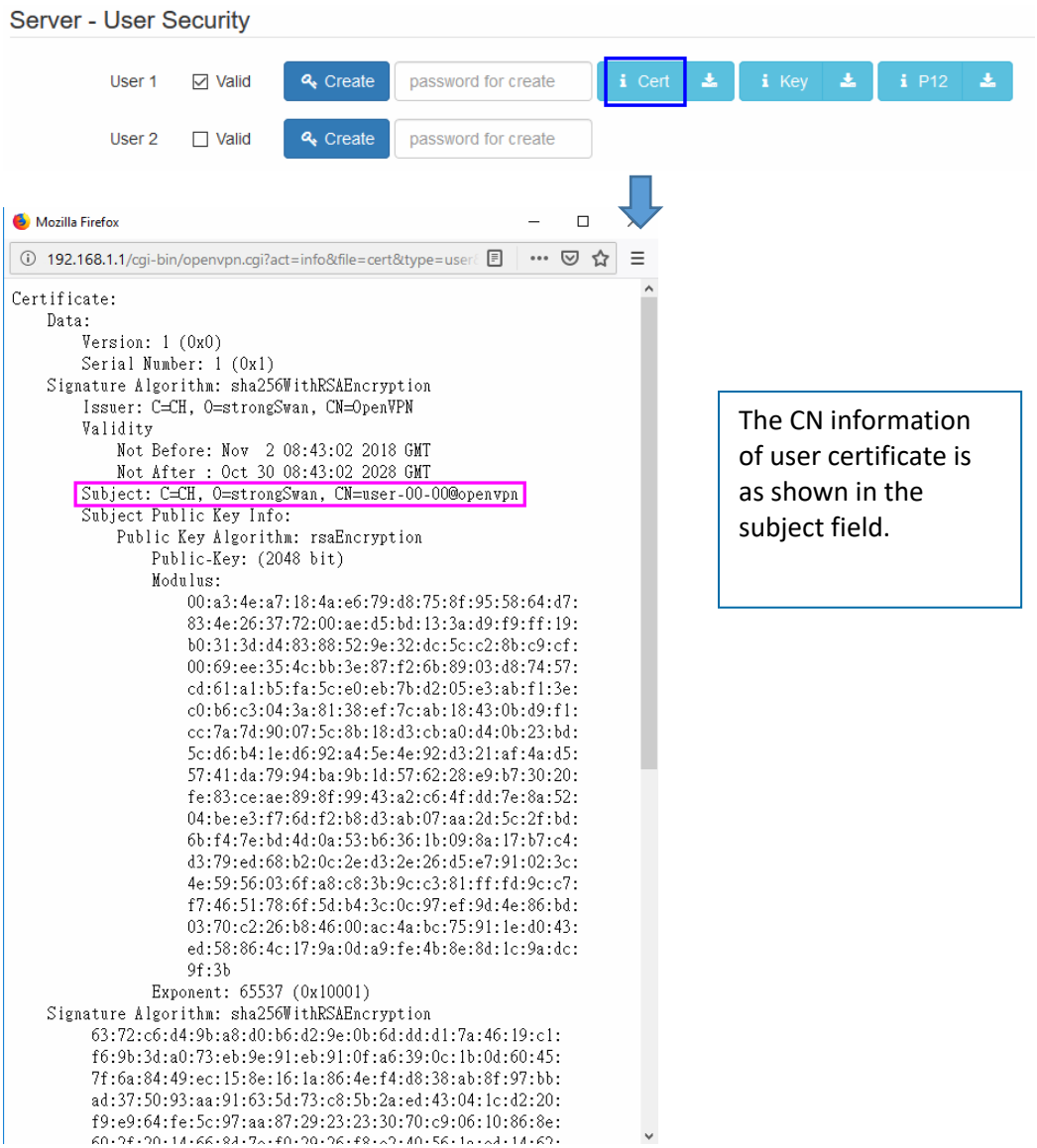


Note: No need to download the User "P12" file as we are not going to use the pkcs #12 Certificate "authentication" field option on the **MR4xx** OpenVPN Client for this guide.

If all settings set up properly, the web UI will show the **Apply OK** and the Open VPN server status should be **Running**. When Open VPN Client mode is connected, the status will show the information which client is connected, IP address and connected time.

In the status, the **CN** field will indicate which client is connected and the **user-00-00@Open VPN** value is from the **User 1** certificate information.

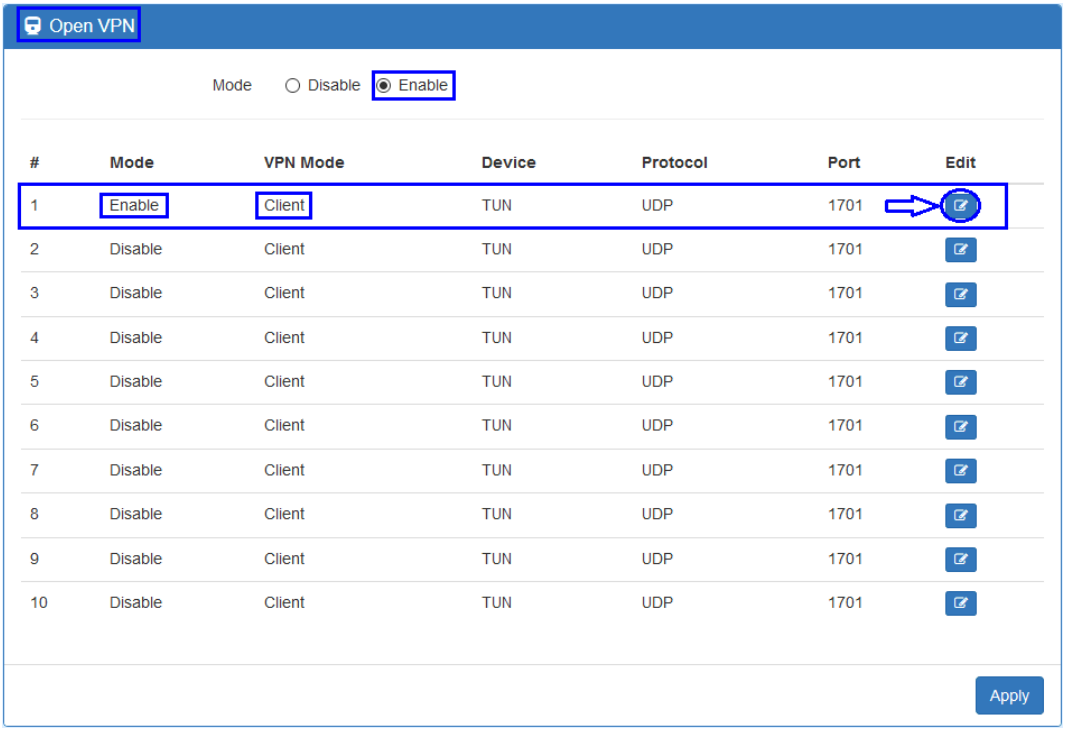
You can check it by clicking the **"i"** (information) button of the Cert, the web UI will display the window as the below figure.



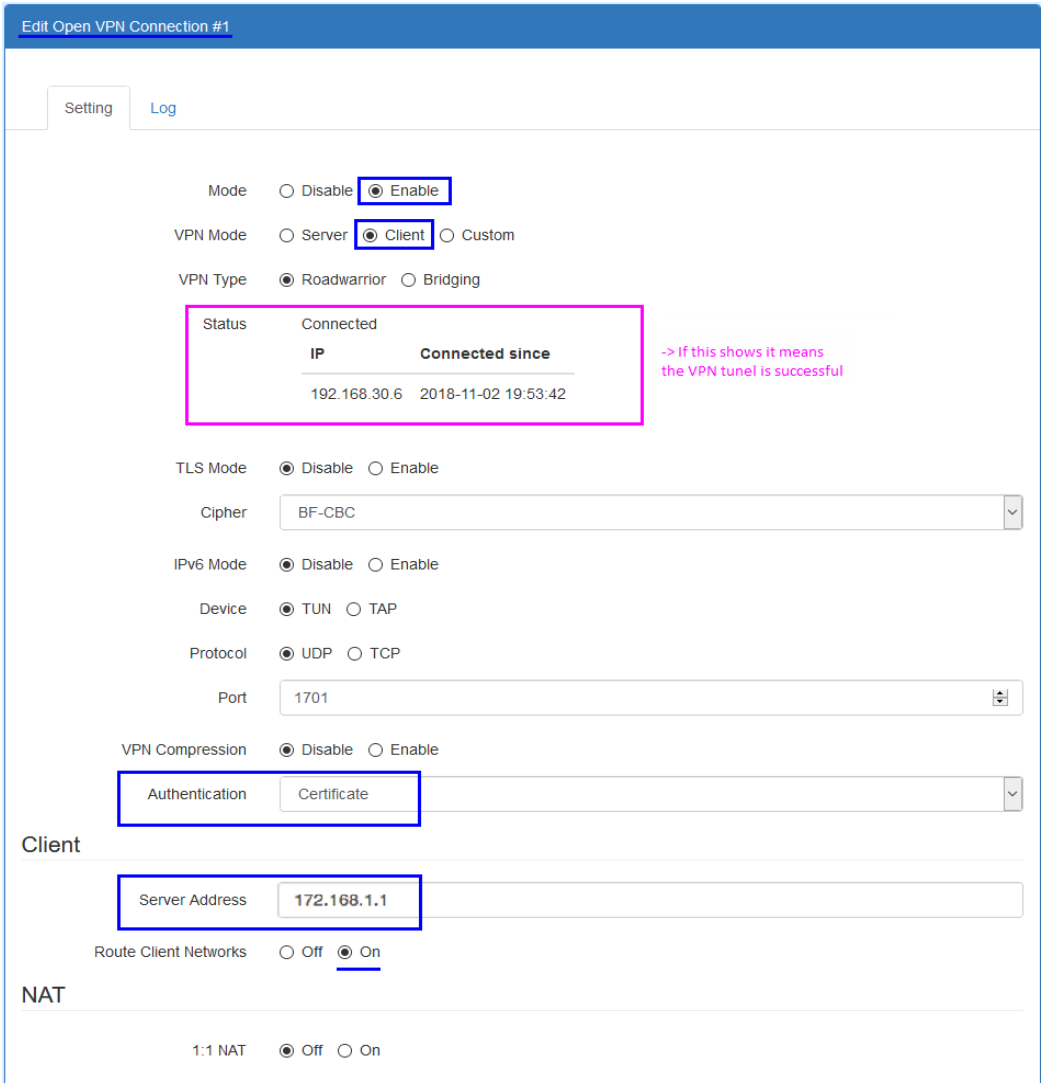
The CN information of user certificate is as shown in the subject field.

(2) MR4xx Open VPN client configuration

For the Open VPN client side, the basic settings as follows:



When click on the Edit button of entry #1, the OpenVPN Client configuration is like this:

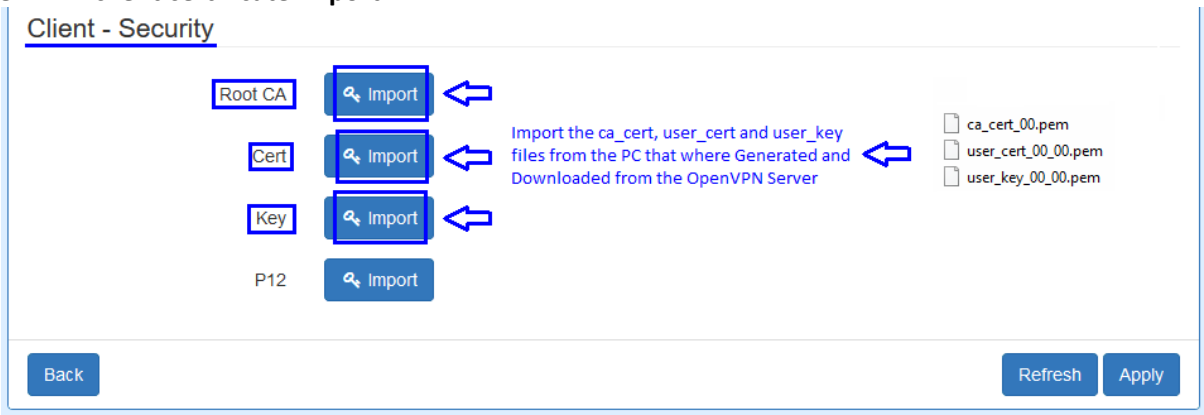


The **Server Address** is required field, which indicate the Open VPN server address which Open VPN client try to connect.

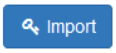
If you use the **Certificate** "**Authentication**" field option, the Open VPN client will require the **Root CA**, **User cert** and **User key** files.
(We are using this Certificate "Authentication" option for this guide, so the OpenVPN client will need the Root CA, User cert and User key files to be imported/Upload. Those files come / can be downloaded from the OpenVPN Server).

(We are not using the pkcs #12 Certificate "authentication" field option for this guide so no need to import the P12 file to the OpenVPN Client from the OpenVPN Server. Also no need to type any PKCS12 password on the OpenVPN Client).

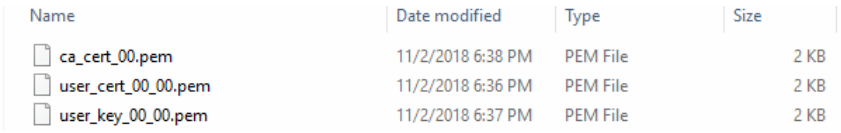
Open VPN client certificate import:



For the OpenVPN client mode, the Open VPN web UI provides the buttons to import the required files. The Open VPN client can use the **Root CA**, **User Key** and **User Cert** files from Open VPN server to authenticate the VPN tunnel. Or just only use the **PKCS#12 (P12)** file from Open VPN server to authenticate it (The PKCS#12 files will contain the Root CA, User Key and User Cert).

* Now please click the 

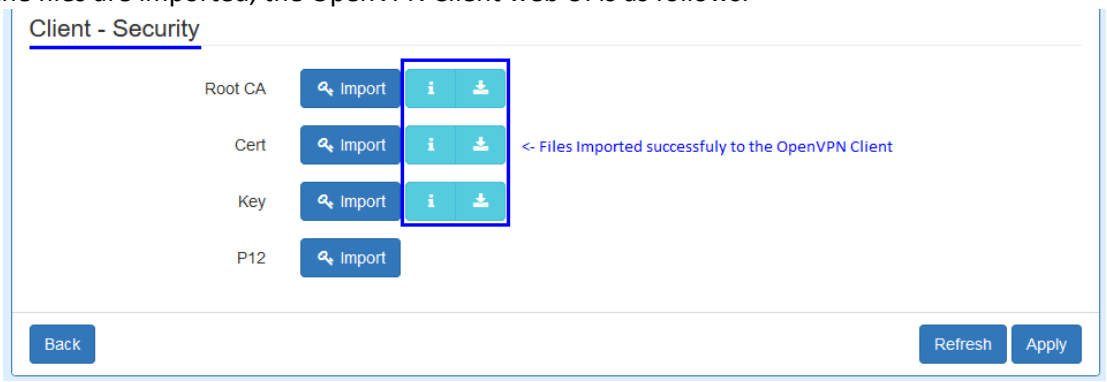
"Import" button to Import the **Server "Root CA" file**, the **User "Cert" file** and the **User "Key" file** from the PC (That comes from the OpenVPN server).



Name	Date modified	Type	Size
ca_cert_00.pem	11/2/2018 6:38 PM	PEM File	2 KB
user_cert_00_00.pem	11/2/2018 6:36 PM	PEM File	2 KB
user_key_00_00.pem	11/2/2018 6:37 PM	PEM File	2 KB

Note: No need to import the User "P12" file as we are not going to use the pkcs #12 Certificate "authentication" field option on the **MR4xx** OpenVPN Client for this guide.

When the files are imported, the OpenVPN Client web UI is as follows:



Same as Open VPN server part, you can use the info/download buttons to get the information of file or download the file to PC. Alike as the Open VPN server configuration part, Open VPN client web UI also provides the status information.

When all settings set up properly, the status will change from **Idle** to **Running**. When Open VPN tunnel is created, the status shows **Connected** and the information for IP address and the time: