

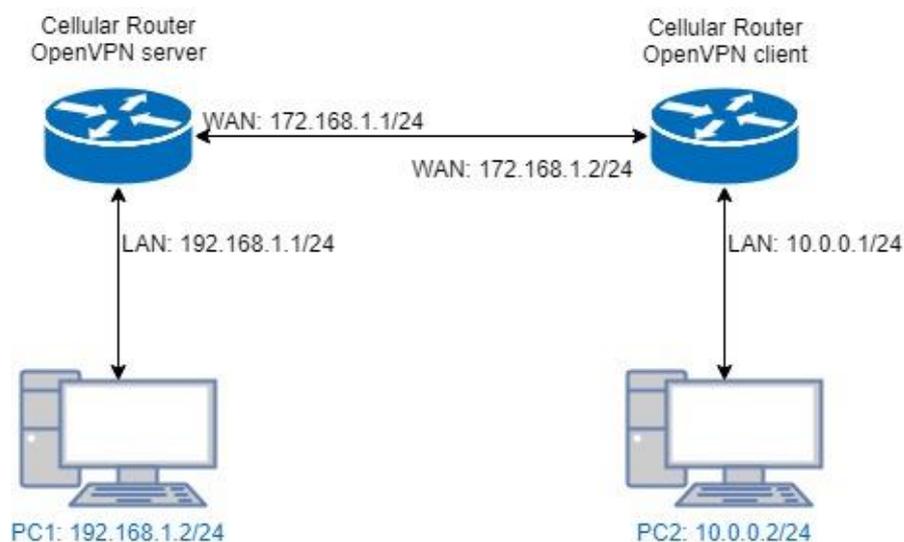
Creating Server/Client Net to Net OpenVPN on Xentino MR4xx Series

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:

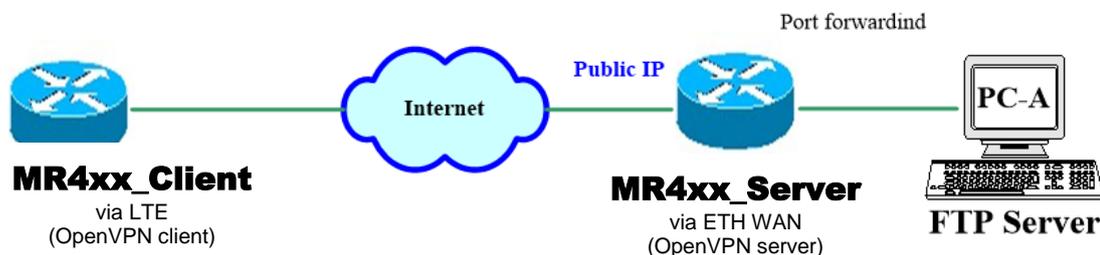
Topology:

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:

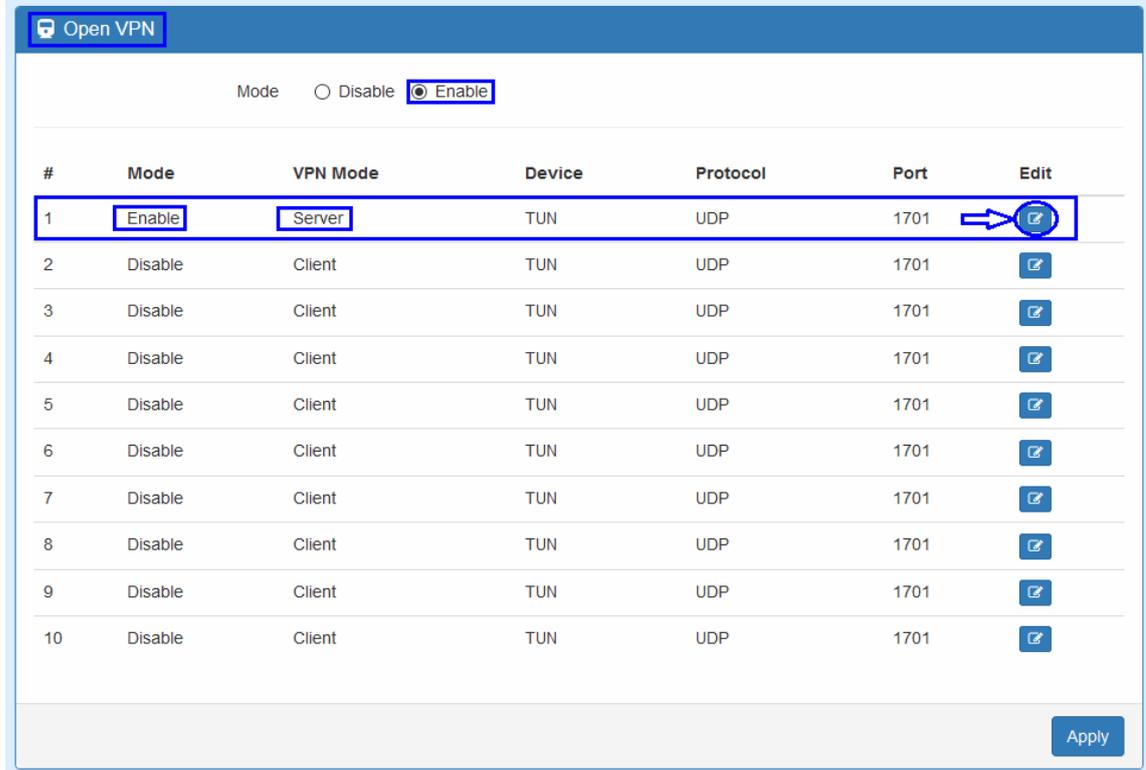
For Open VPN configuration, use the certificate to authenticate the VPN connection.

Thus, you need to generate the required files from the MR4xx Open VPN server and import them to the MR4xx Open VPN client.

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

(1) MR4xx OpenVPN server configuration

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



The screenshot shows the 'Open VPN' configuration interface. At the top, there is a 'Mode' section with radio buttons for 'Disable' and 'Enable', where 'Enable' is selected. Below this is a table with the following columns: '#', 'Mode', 'VPN Mode', 'Device', 'Protocol', 'Port', and 'Edit'. The first row is highlighted with a blue box, and a blue arrow points to the 'Edit' icon in that row. The table contains 10 rows, with the first row being a server profile and the others being client profiles.

#	Mode	VPN Mode	Device	Protocol	Port	Edit
1	Enable	Server	TUN	UDP	1701	
2	Disable	Client	TUN	UDP	1701	
3	Disable	Client	TUN	UDP	1701	
4	Disable	Client	TUN	UDP	1701	
5	Disable	Client	TUN	UDP	1701	
6	Disable	Client	TUN	UDP	1701	
7	Disable	Client	TUN	UDP	1701	
8	Disable	Client	TUN	UDP	1701	
9	Disable	Client	TUN	UDP	1701	
10	Disable	Client	TUN	UDP	1701	

An 'Apply' button is located at the bottom right of the interface.

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

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

Setting Log

Mode Disable Enable

VPN Mode Server Client Custom

VPN Type Roadwarrior Bridging

Status	CN	IP	Connected since
Running	user-00-00@openvpn	192.168.30.6	2018-11-02 19:52:53

-> If this shows it means the VPN tunnel is successful (user-00-00@openvpn is the VPN client)

TLS Mode Disable Enable

Cipher BF-CBC

IPv6 Mode Disable Enable

Device TUN TAP

Protocol UDP TCP

Port 1701

VPN Compression Disable Enable

Authentication Certificate

Server

VPN Network 192.168.30.0

VPN Netmask 255.255.255.0

-> VPN Network IP As needed (Those typed are just for example)

Roadwarrior

Route Client Networks Off On

Connections - Net / Mask

#	Net	Mask
#1	10.0.0.0	255.255.255.0
#2	0.0.0.0	0.0.0.0
#3	0.0.0.0	0.0.0.0
#4	0.0.0.0	0.0.0.0
#5	0.0.0.0	0.0.0.0
#6	0.0.0.0	0.0.0.0
#7	0.0.0.0	0.0.0.0
#8	0.0.0.0	0.0.0.0

<- This is the VPN client side LAN IP

NAT

1:1 NAT Off On

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.)

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

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:

The screenshot displays the OpenVPN Server web UI for certificate generation, divided into two sections:

- Server - Server Security:** Contains two rows. The first row has a box labeled "Root CA" and a "Create" button. The second row has a box labeled "Cert, Key" and a "Create" button. Annotations with arrows point to these buttons, stating: "Click 'Create' On Server Security to generate the Server 'Root CA', Server 'Cert' and Server Key files."
- Server - User Security:** Contains a table of users. The first row is for "User 1", which is checked as "Valid". It has a "Create" button and a password field containing ".....". An annotation with an arrow points to the password field, stating: "1st Enter a Password, This for the User 'P12' file." Below "User 1" are rows for "User 2" through "User 8", each with an unchecked "Valid" checkbox, a "Create" button, and a password field containing "password for create".

At the bottom of the UI, there are three buttons: "Back", "Refresh", and "Apply".

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:

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

Download the Server Root CA file to the PC

Root CA [Create] [i] [Download]

Cert, Key [Create] [i Cert] [i Key] [Download]

Download the User Cert and User Key files to the PC

User 1 Valid [Create] password for create [i Cert] [Download] [i Key] [Download] [i P12] [Download]

User 2 Valid [Create] password for create

User 3 Valid [Create] password for create

User 4 Valid [Create] password for create

User 5 Valid [Create] password for create

User 6 Valid [Create] password for create

User 7 Valid [Create] password for create

User 8 Valid [Create] password for create

Back Refresh Apply

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.

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 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.

Status	Running		
	CN	IP	Connected since
	user-00-00@openvpn	192.168.30.6	2018-11-02 19:52:53

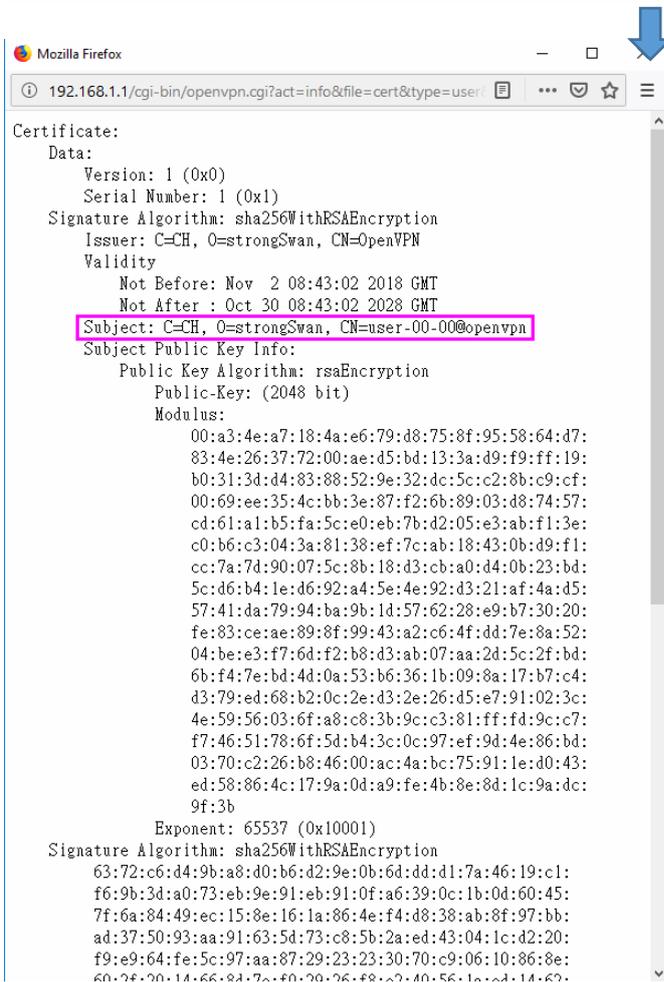
In the status, the **CN** field will indicate which client is connected and the **user-00-00@Open VPN** value is from the **User 1** certificate information.

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

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

Server - User Security

User 1	<input checked="" type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>	<input type="button" value="Cert"/>	<input type="button" value="Key"/>	<input type="button" value="P12"/>
User 2	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>			



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:

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

Open VPN

Mode Disable Enable

#	Mode	VPN Mode	Device	Protocol	Port	Edit
1	Enable	Client	TUN	UDP	1701	
2	Disable	Client	TUN	UDP	1701	
3	Disable	Client	TUN	UDP	1701	
4	Disable	Client	TUN	UDP	1701	
5	Disable	Client	TUN	UDP	1701	
6	Disable	Client	TUN	UDP	1701	
7	Disable	Client	TUN	UDP	1701	
8	Disable	Client	TUN	UDP	1701	
9	Disable	Client	TUN	UDP	1701	
10	Disable	Client	TUN	UDP	1701	

Apply

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

Edit Open VPN Connection #1

Setting Log

Mode Disable Enable

VPN Mode Server Client Custom

VPN Type Roadwarrior Bridging

Status Connected

IP	Connected since
192.168.30.6	2018-11-02 19:53:42

-> If this shows it means the VPN tunnel is successful

TLS Mode Disable Enable

Cipher BF-CBC

IPv6 Mode Disable Enable

Device TUN TAP

Protocol UDP TCP

Port 1701

VPN Compression Disable Enable

Authentication Certificate

Client

Server Address 172.168.1.1

Route Client Networks Off On

NAT

1:1 NAT Off On

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

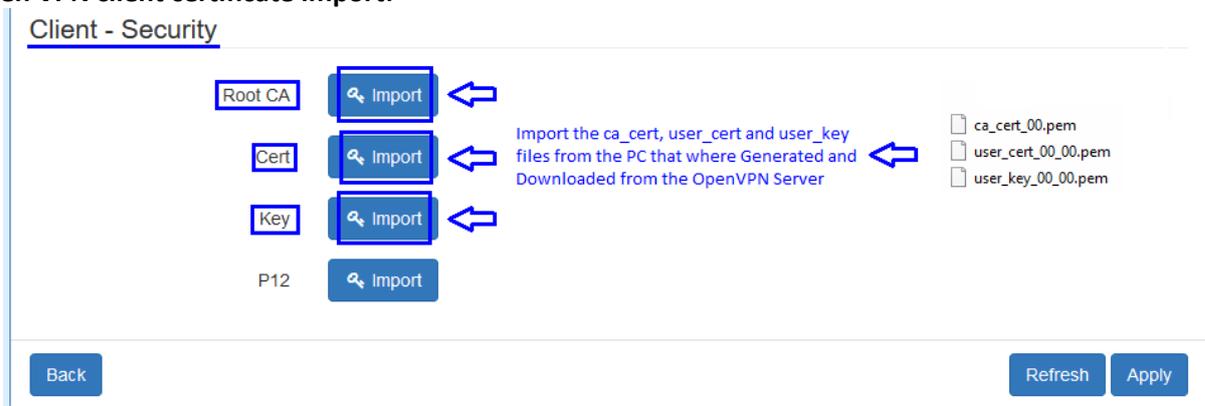
The **Server Address** is required field, which indicate the Open VPN server address which Open VPN client try to connect.

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:



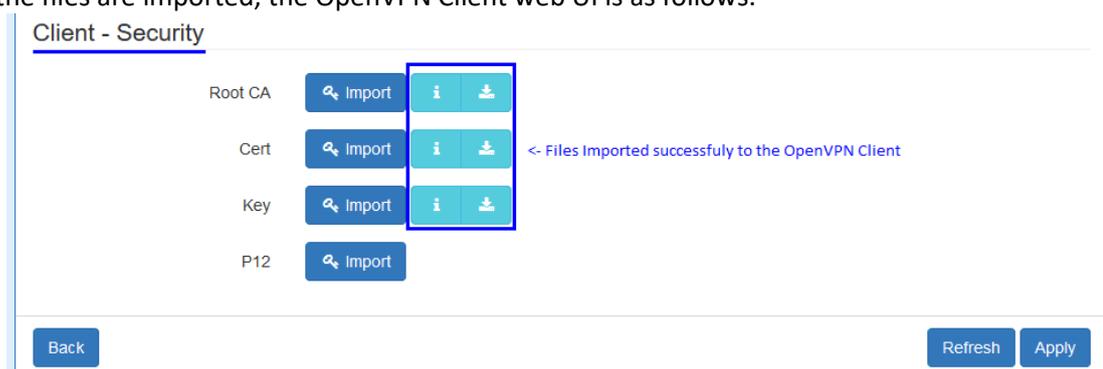
For the OpenVPN client mode, the Open VPN web UI provides the buttons to import the required files. The Open VPN client can use the **Root CA, User Key** and **User Cert** files from Open VPN server to authenticate the VPN tunnel. Or just only use the **PKCS#12 (P12)** file from Open VPN server to authenticate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



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

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:

Status	Connected	
	IP	Connected since
	192.168.30.6	2018-11-02 19:53:42