RUT241 TLS OpenVPN configuration example with Windows client

Prerequisites:

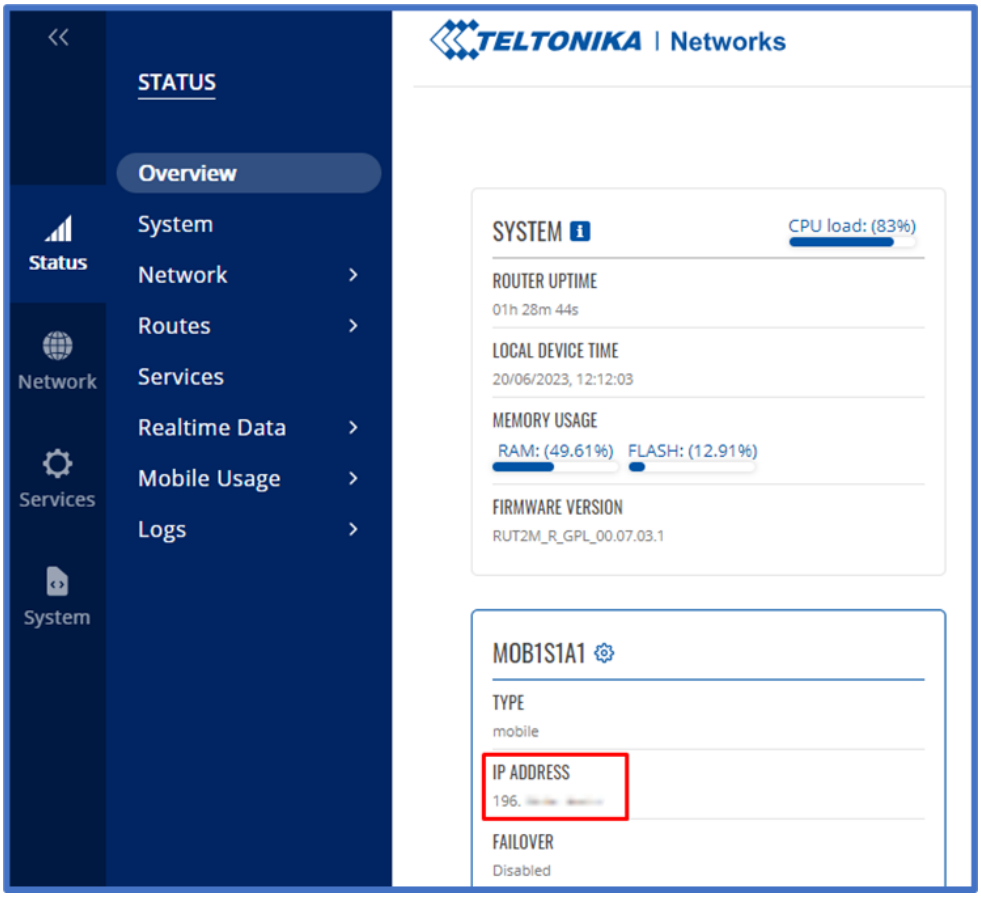
For this configuration example, we will need the following:

- A Teltonika RUT241 router (or any Teltonika RUTxxx router)
- A dynamic public IP address on one of the router's WAN interfaces.
- A free no-ip DDNS account: https://www.noip.com/
- OpenVPN installer file: https://openvpn.net/community-downloads/
- OpenVPN connect client installed on the client machine: https://openvpn.net/client/client-connect-vpn-for-windows/

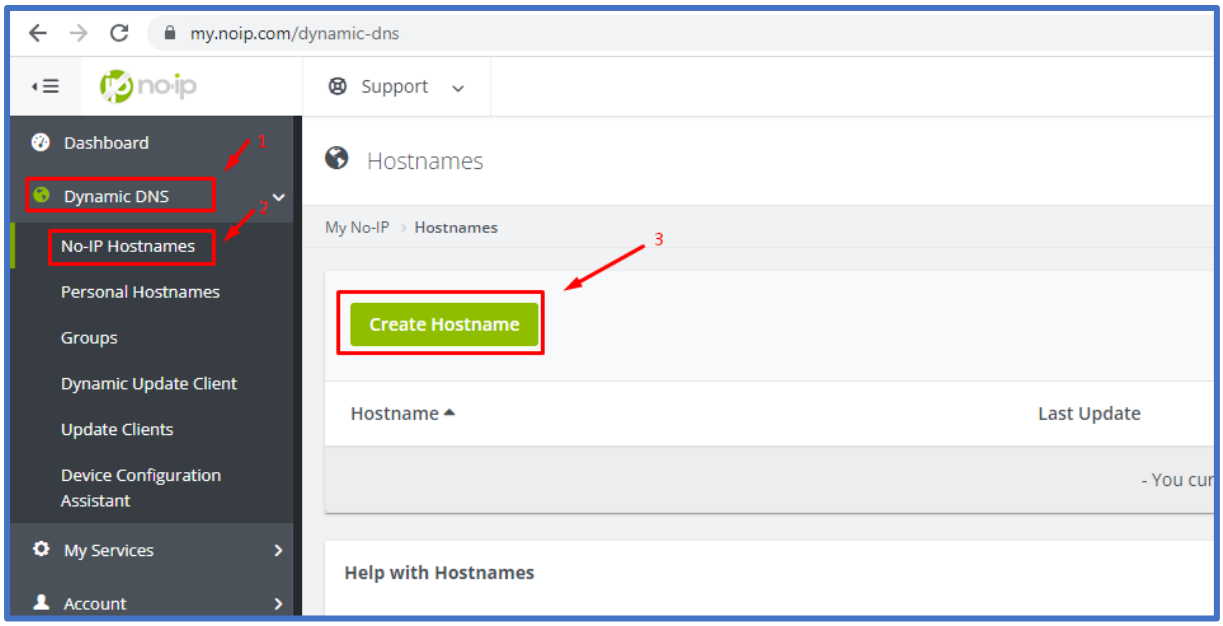
Dynamic DNS configuration (no-ip):

First, log in to your router and turn on "**ADVANCED**" WebUI mode:

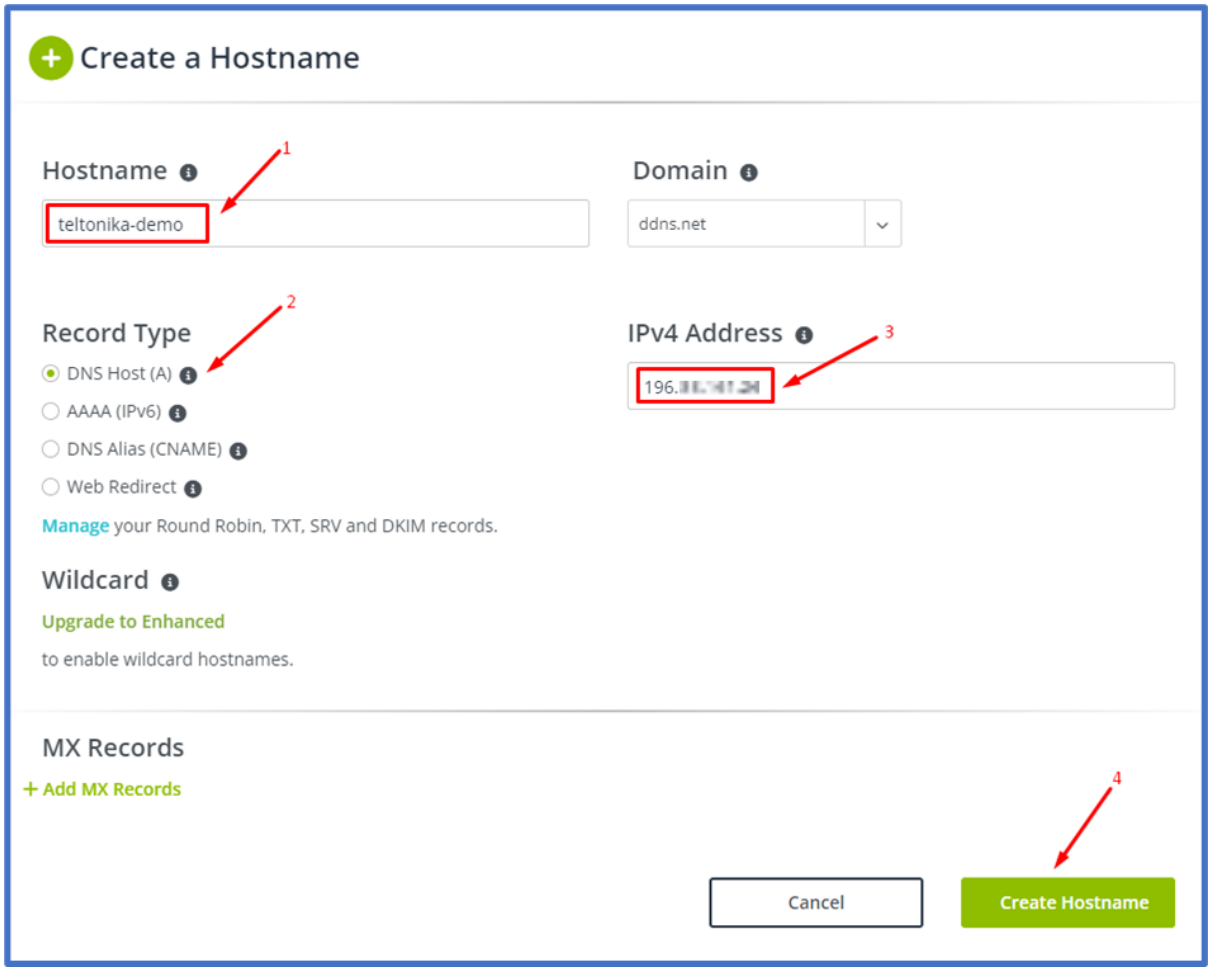
Then go to ***Status → Overview***, and check your WAN interface public IP address (in this case, the main WAN interface is Mobile):



Log in to your no-ip account and create a new hostname:



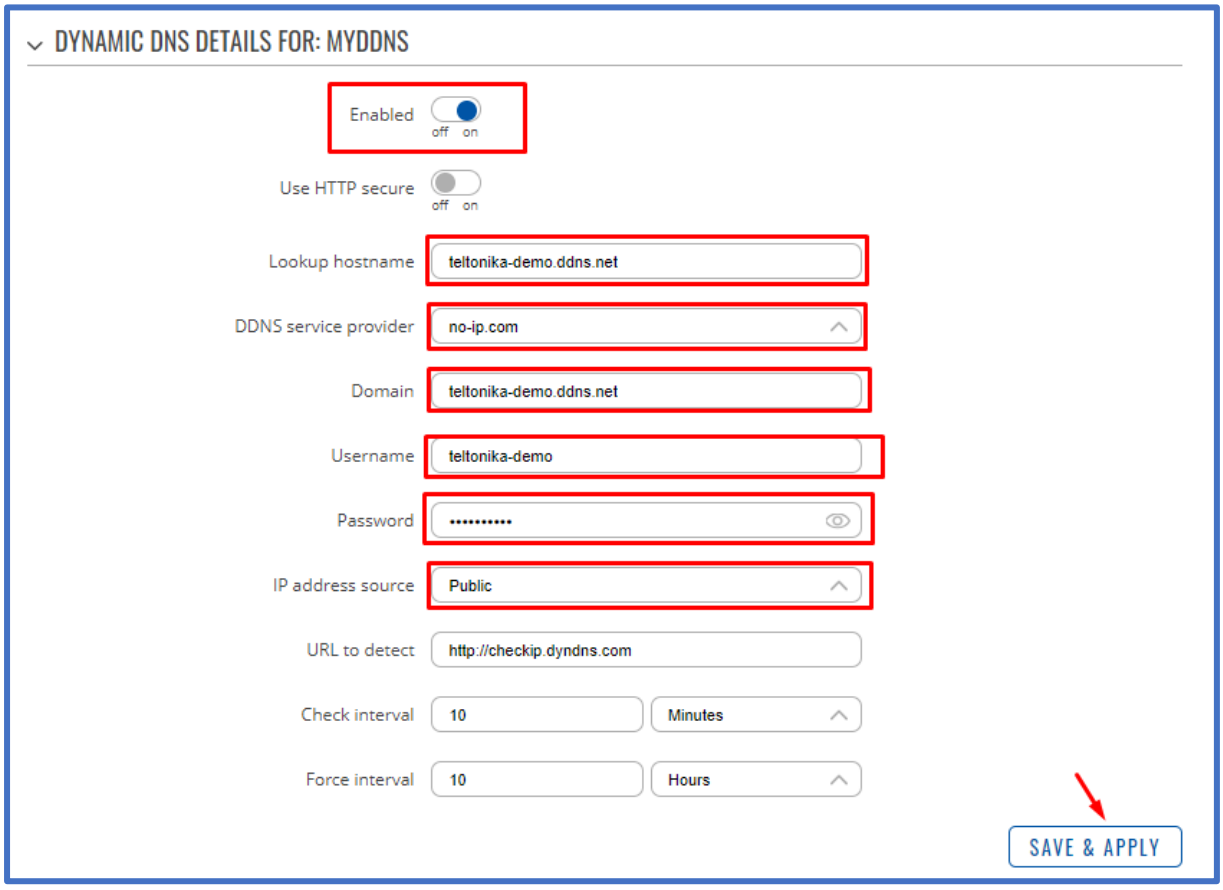
Add a *hostname*, choose *Record type* "DNS Host (A)", and put your router's public IP address in the *IPv4 Address* bar:



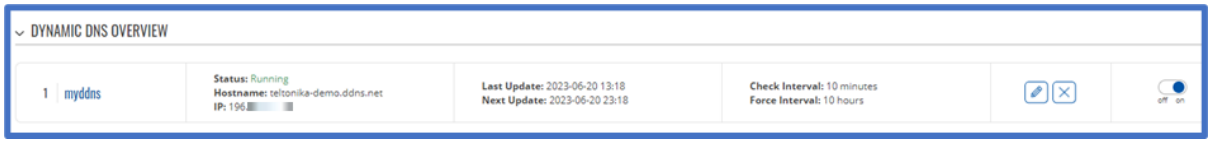
On your router's WebUI, go to ***Services → Package Manager → Packages***, and search for "ddns", click the + button to download and install the package:

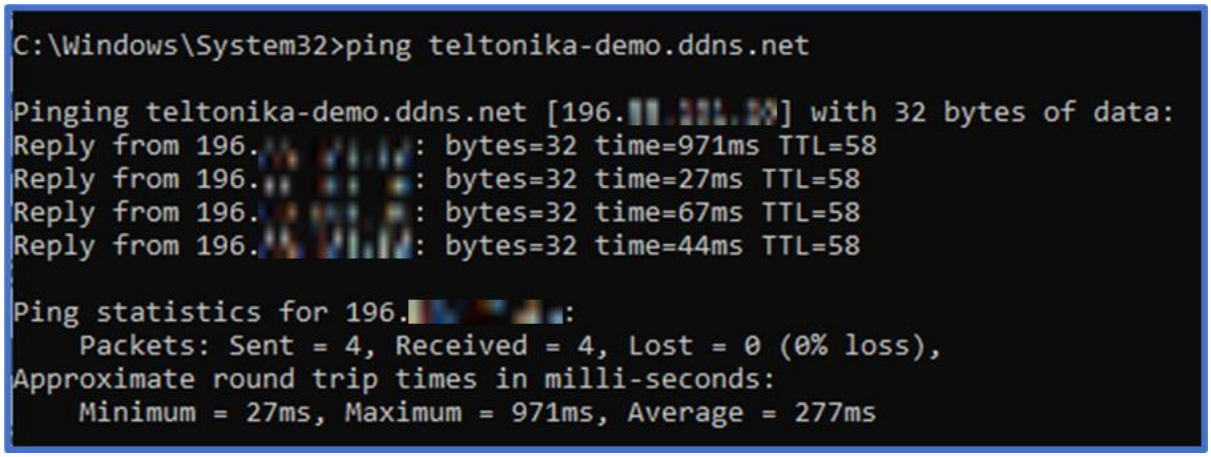
Once the package is installed, go to ***Services-> Dynamic DNS***, click the edit button to edit the DDNS configuration:

- Check the **Enabled** box
- Add your hostname to **Lookup hostname** and **Domain**
- Choose the **no-ip.com** service
- Type your **Username** and **Password**
- Choose Public for **IP address source**
- Click **SAVE & APPLY**



Once the status changes to Running on the DDNS instance, try to ping your hostname from another laptop:





Now, your device is reachable from the internet using the no-ip hostname, and you no longer have to worry about your Public IP address changing.

Generating TLS certificates/keys:

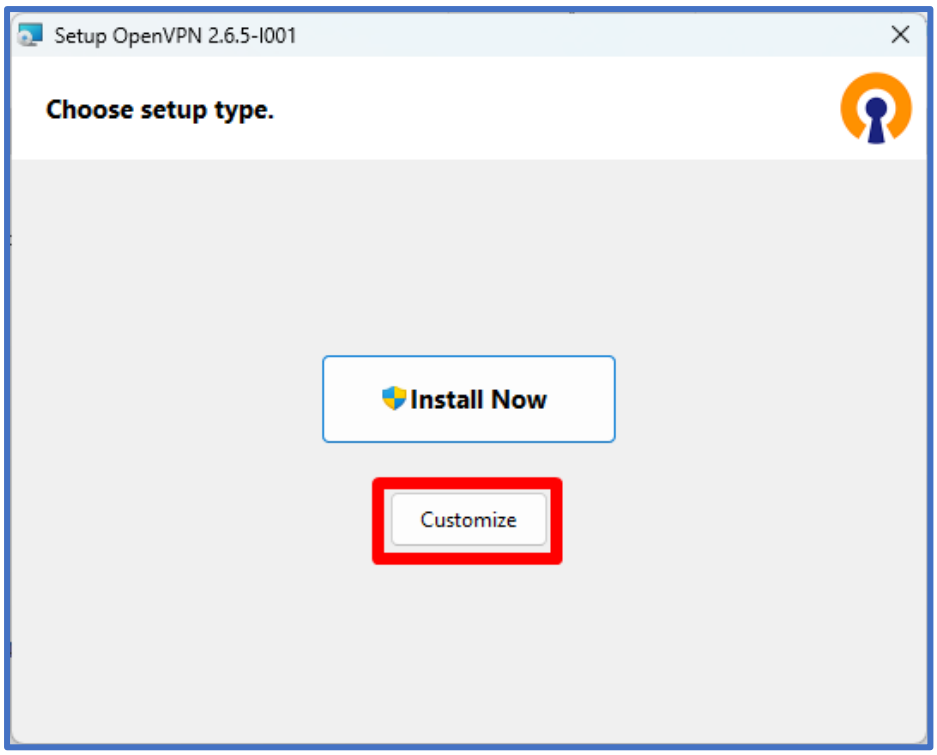
A connection that uses TLS requires multiple certificates and keys for authentication:

- OpenVPN server
    - The root certificate file (Certificate Authority)
    - Server certificate
    - Server key
    - Diffie Hellman Parameters

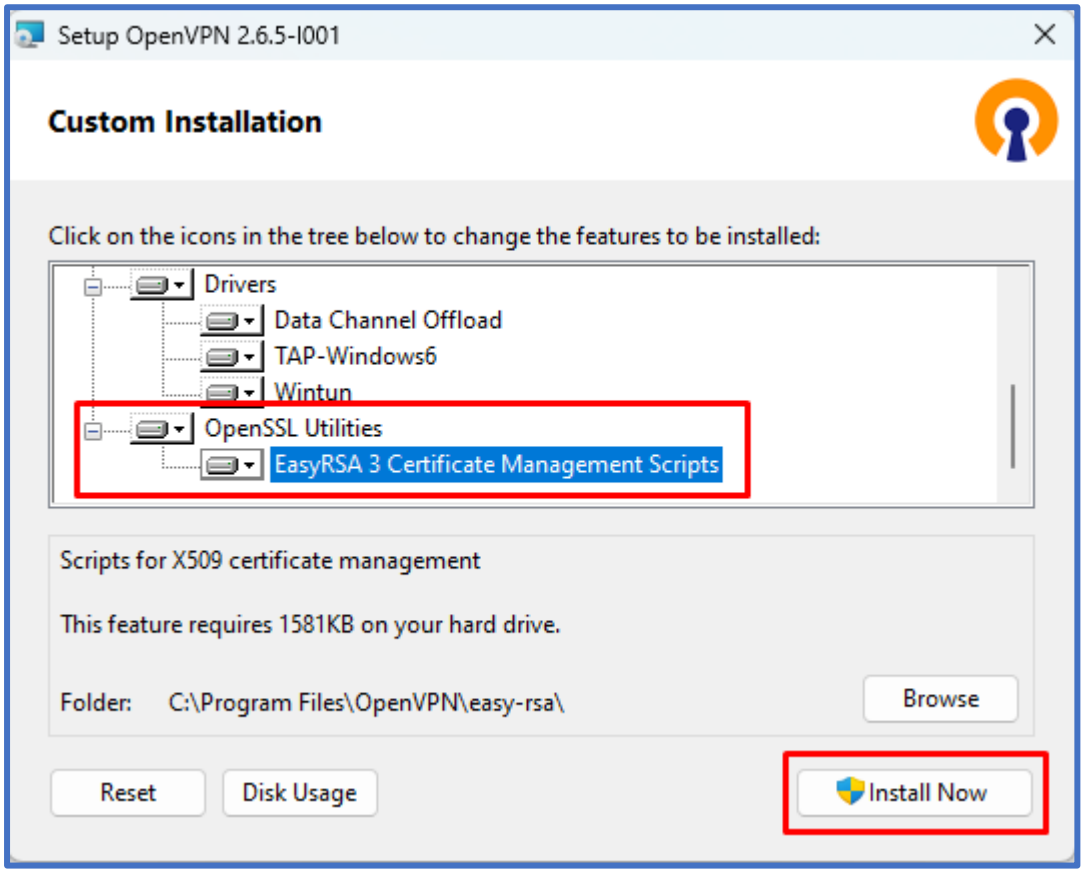
- OpenVPN client
    - The root certificate file (Certificate Authority)
    - Client certificate
    - Client key

Please follow these steps to generate your TLS certificates and Keys:

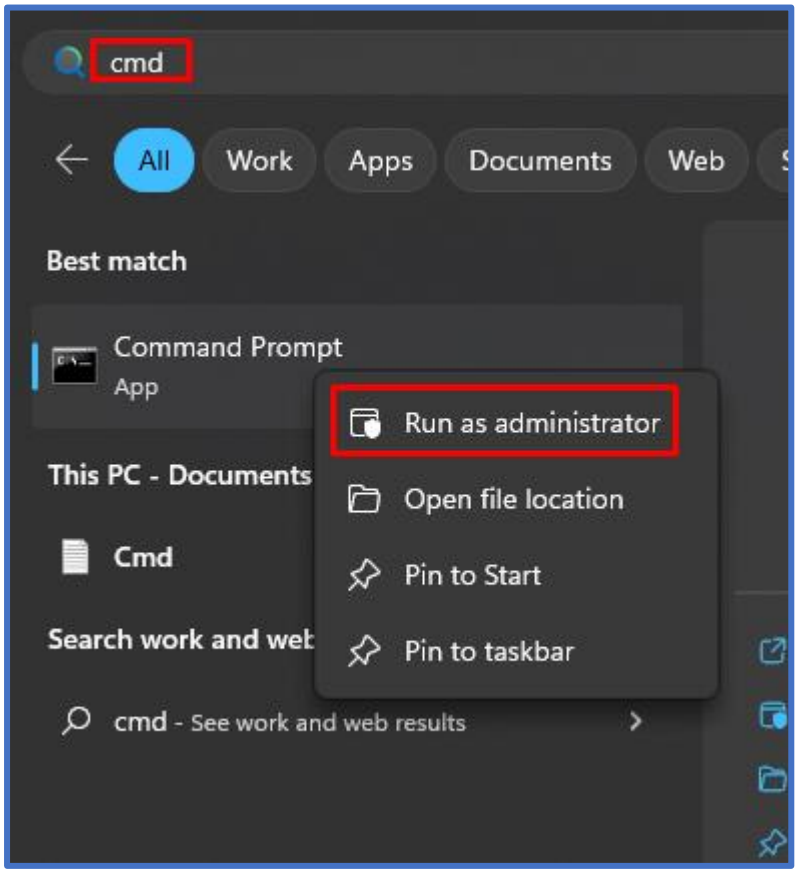
Run the OpenVPN installer file, and before starting the installation process, click **Customize**:



While in the "Custom Installation" window, scroll down to **find OpenSSL Utilities → EasyRSA 3 Certificate Management Scripts**; make sure it is installed along with OpenVPN and **click "Install Now"**:



Launch Windows CMD and make sure you **run it as Administrator**:



Change the current directory to the EasyRSA folder. To do so, execute this command:

```
cd "C:\Program Files\OpenVPN\easy-rsa"
```

Launch EasyRSA:

```
EasyRSA-Start.bat
```

Before you can generate files with EasyRSA, you must first initialize a directory for the Public Key Infrastructure (PKI). This can be done with the following command :

```
./easyrsa init-pki
```

Open the vars.bat file with the Notepad text editor:

```
notepad vars.bat
```

This is the template file for generating certificates, i.e., the information stored here will be offered as default values during certificate generation. Locate and edit the following lines in accordance with your needs:

```
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@host.domain
set DH_KEY_SIZE=2048
```

Once you're done, save the file and close the editor; then run the following commands:

```
vars.bat
./easyrsa clean-all
```

Now we can start generating the certificates and keys. Begin with the **certificate authority (CA)** - the root certificate file that will be used to sign other certificates and keys:

```
./easyrsa build-ca nopass
```

Next, build the **server** certificate and key:

```
./easyrsa build-server-full server nopass
```

Next, build certificates and keys for the **clients**:

```
./easyrsa build-client-full Client1 nopass
```

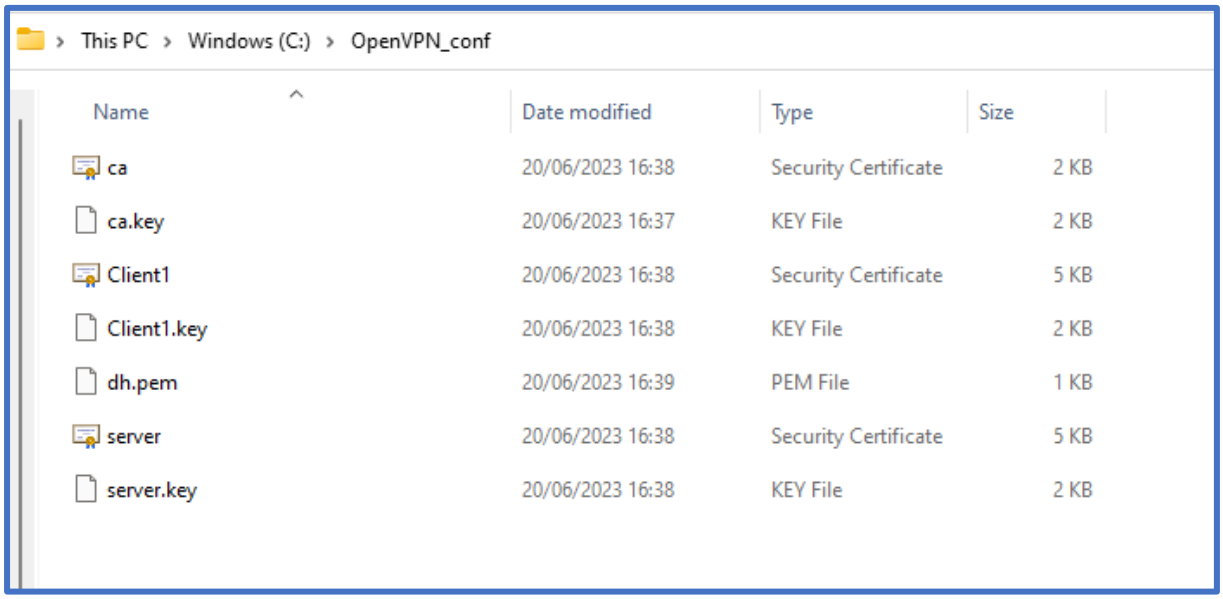
Lastly, generate **Diffie Hellman** parameters:

```
./easyrsa gen-dh
```

The generated and signed files should appear in the following directories (by default):

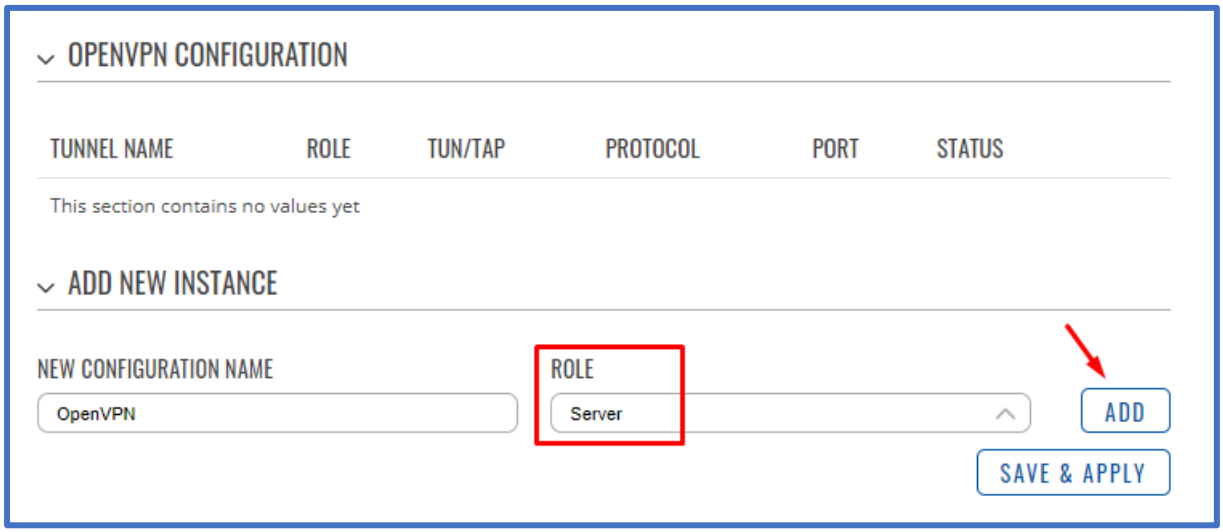
File(s)		Location
CA certificate	→	*C:\Program Files\OpenVPN\easy-rsa\pki*
Diffie-Hellman parameters	→	*C:\Program Files\OpenVPN\easy-rsa\pki*
Client and Server keys	→	*C:\Program Files\OpenVPN\easy-rsa\pki\private*
Client and Server certificates	→	*C:\Program Files\OpenVPN\easy-rsa\pki\issued*

It's recommended to gather all certificates and keys in one folder for easy access, you can create a folder on C:\ hard drive ("C:\OpenVPN_conf"):



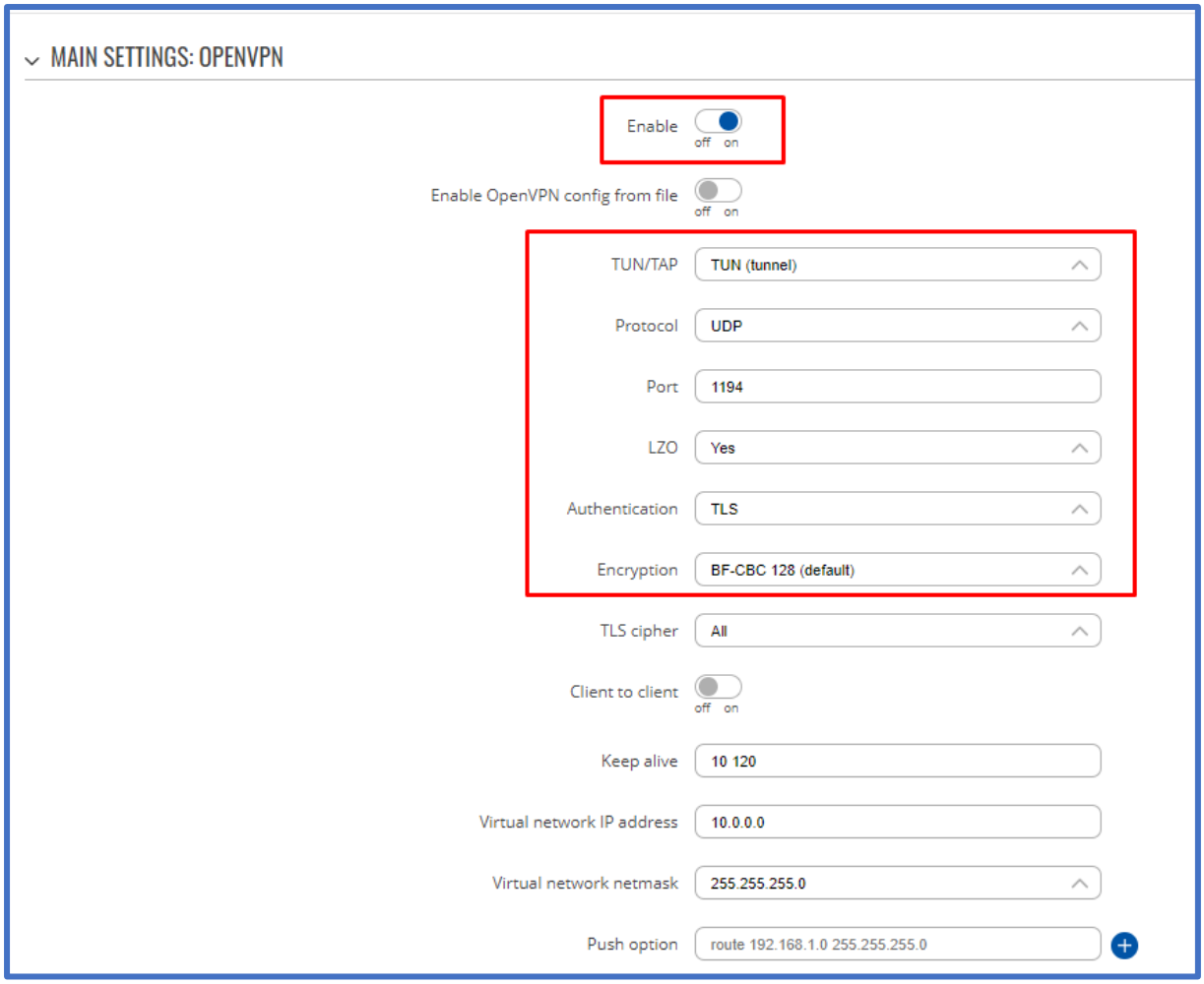
OpenVPN Server configuration:

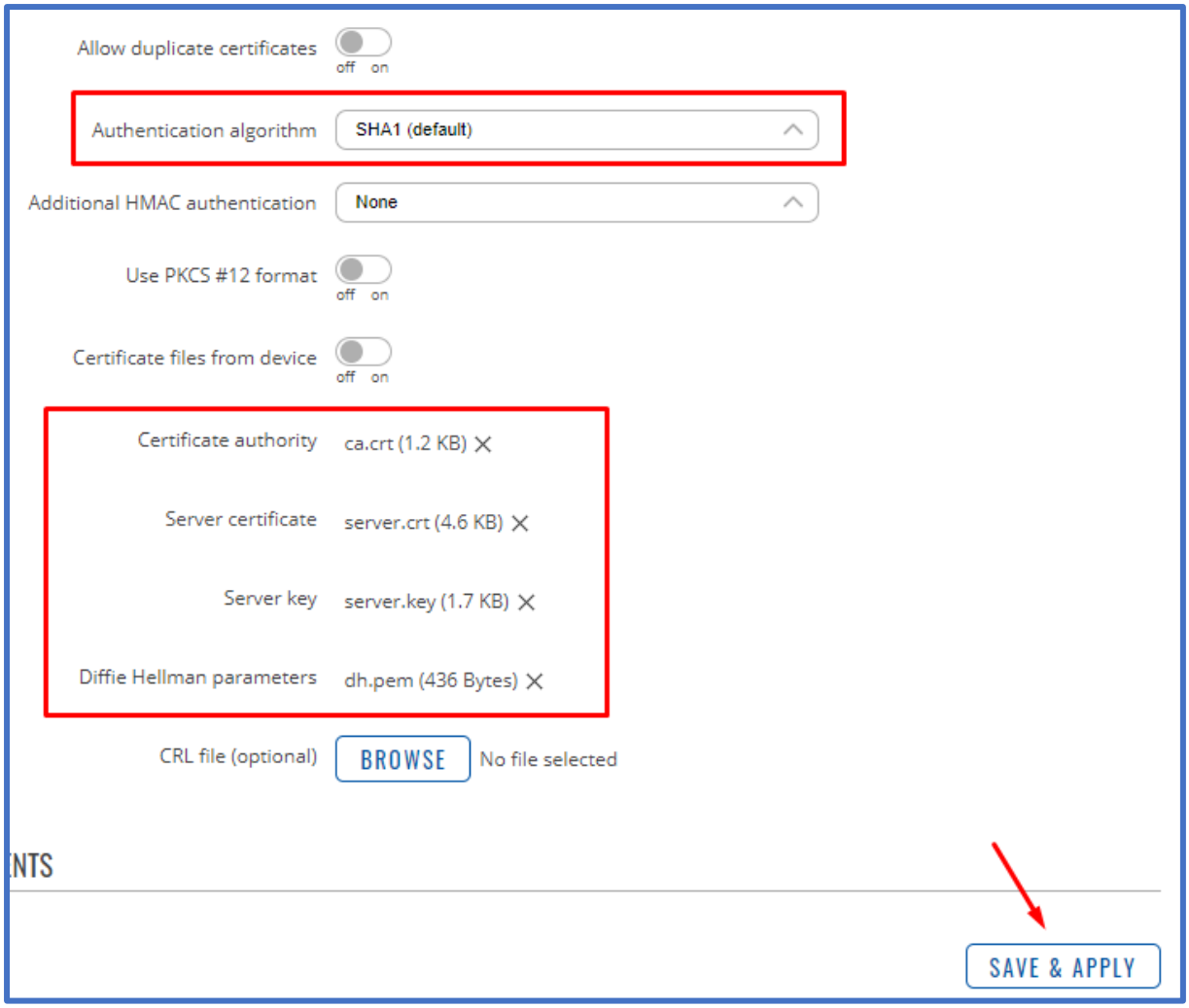
Please go to ***Services → VPN → OPENVPN***, create a new VPN config, set **ROLE** to Server, and click add:



Configure your VPN as follows:

- **Enable** Server
- **TUN/TAP**: TUN (tunnel)
- **Protocol**: UDP
- **Port** : 1194
- **LZO**: Yes
- **Authentication**: TLS
- **Encryption**: BF-CBC 128 (default)
- **Virtual network IP address** : 10.0.0.0
- **Virtual network netmask** : 255.255.255.0
- **Authentication algorithm**: SHA1 (default)
- Upload the following (from certs and keys generated earlier) :
    - **Certificate authority**
    - **Server certificate**
    - **Server key**
    - **Diffie Hellman parameter**
- **Save & Apply**

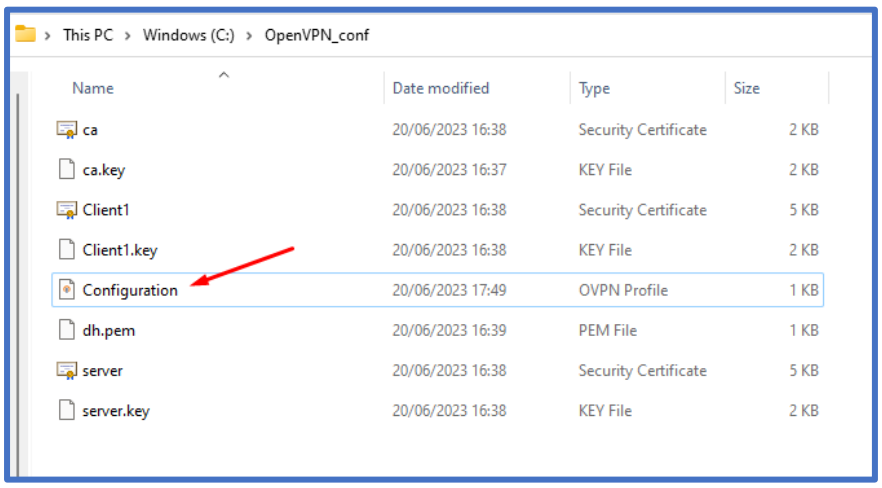




The OpenVPN server is now configured, let's move to the Windows OpenVPN client.

OpenVPN Client configuration:

On the same folder as the OpenVPN Certificate & Keys, create a file "C:\OpenVPN_conf**Configuration.ovpn**" that contains the following:

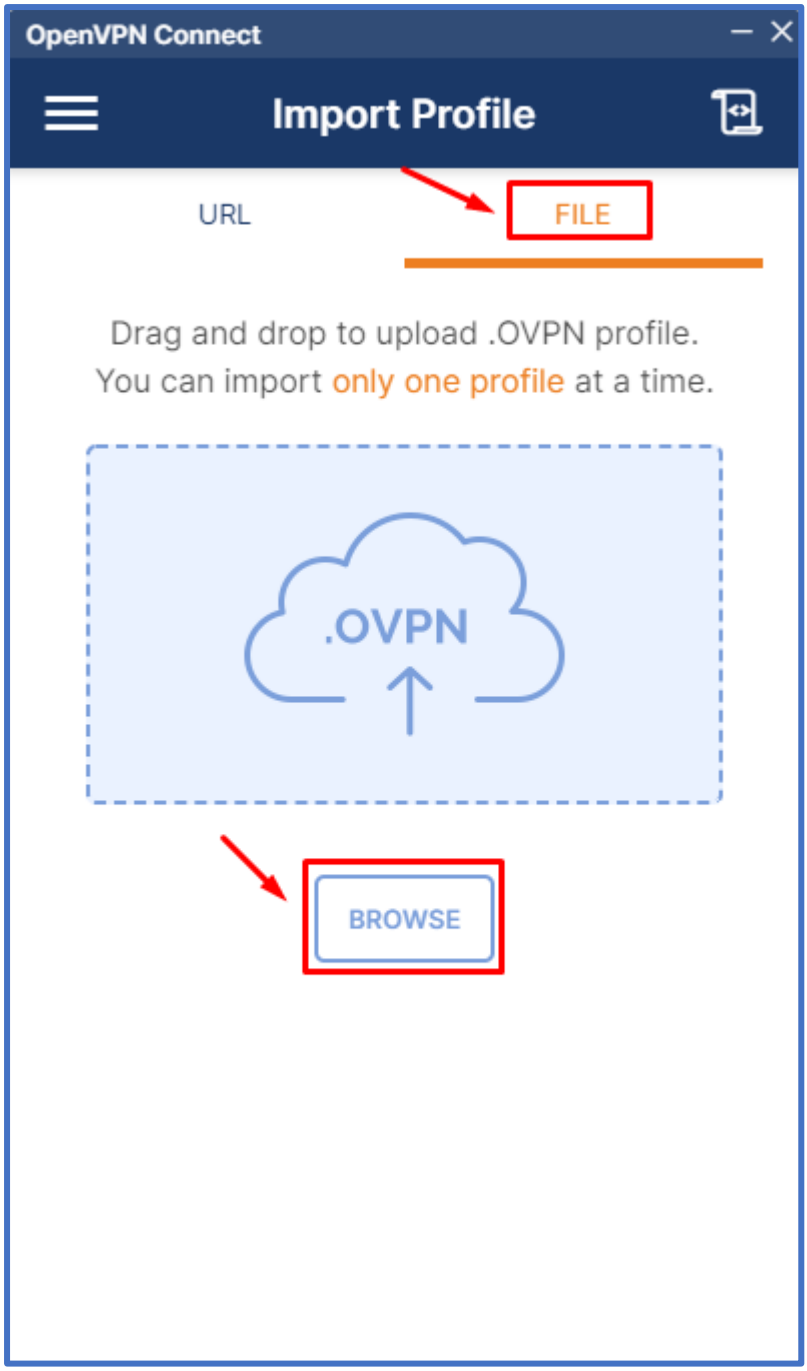


```
client
dev tun
proto udp
auth sha1
remote teltonika-demo.ddns.net 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert Client1.crt
key Client1.key
remote-cert-tls server
data-ciphers BF-CBC
cipher BF-CBC
comp-lzo yes
keepalive 10 120
```

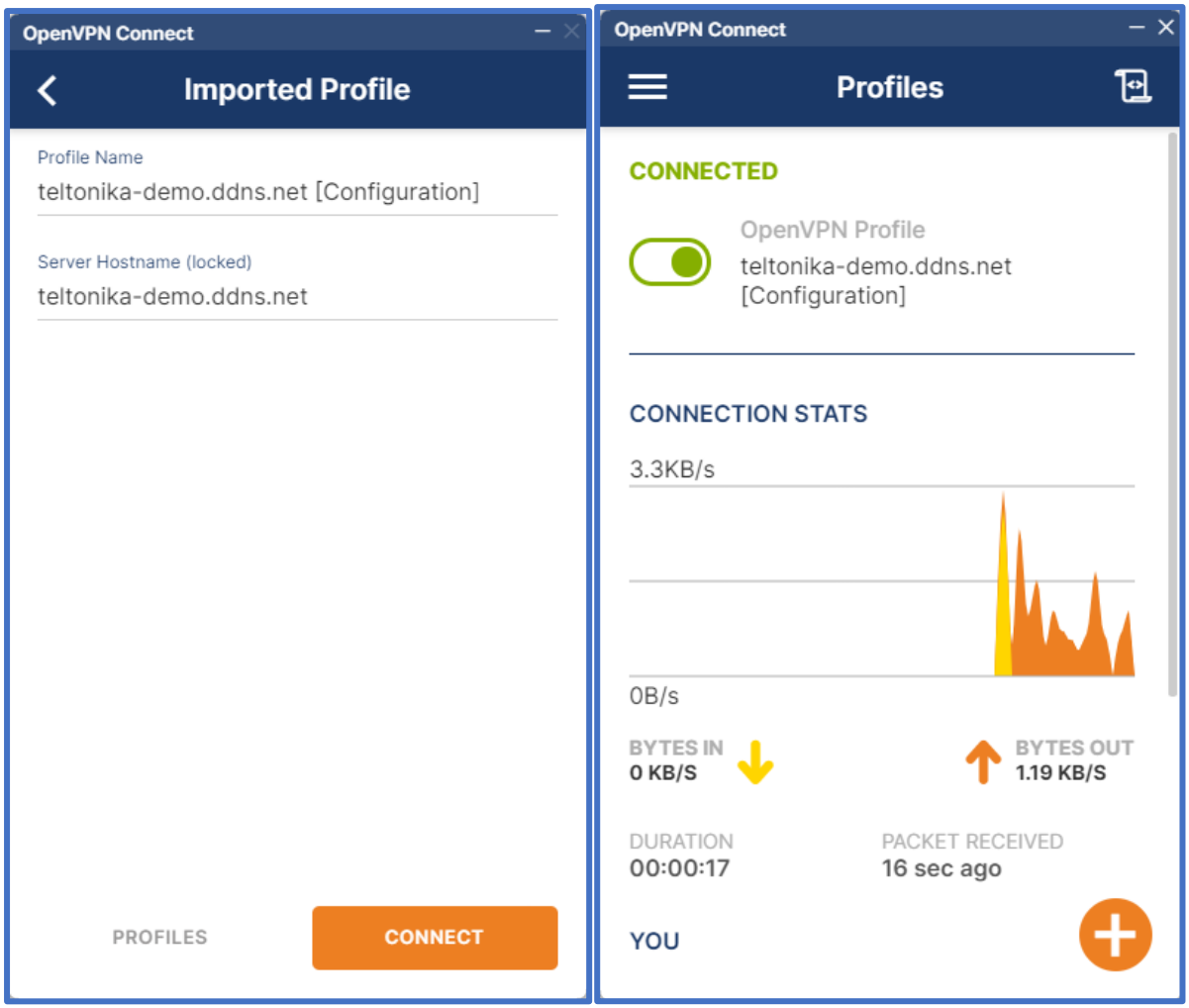
Don't forget to change file names and the OpenVPN hostname to your own.

Now we're going to load this configuration file to the OpenVPN connect software already installed on the client machine (make sure the config and all certificates and keys are in the same folder).

Please open the OpenVPN connect software and choose **FILE**:

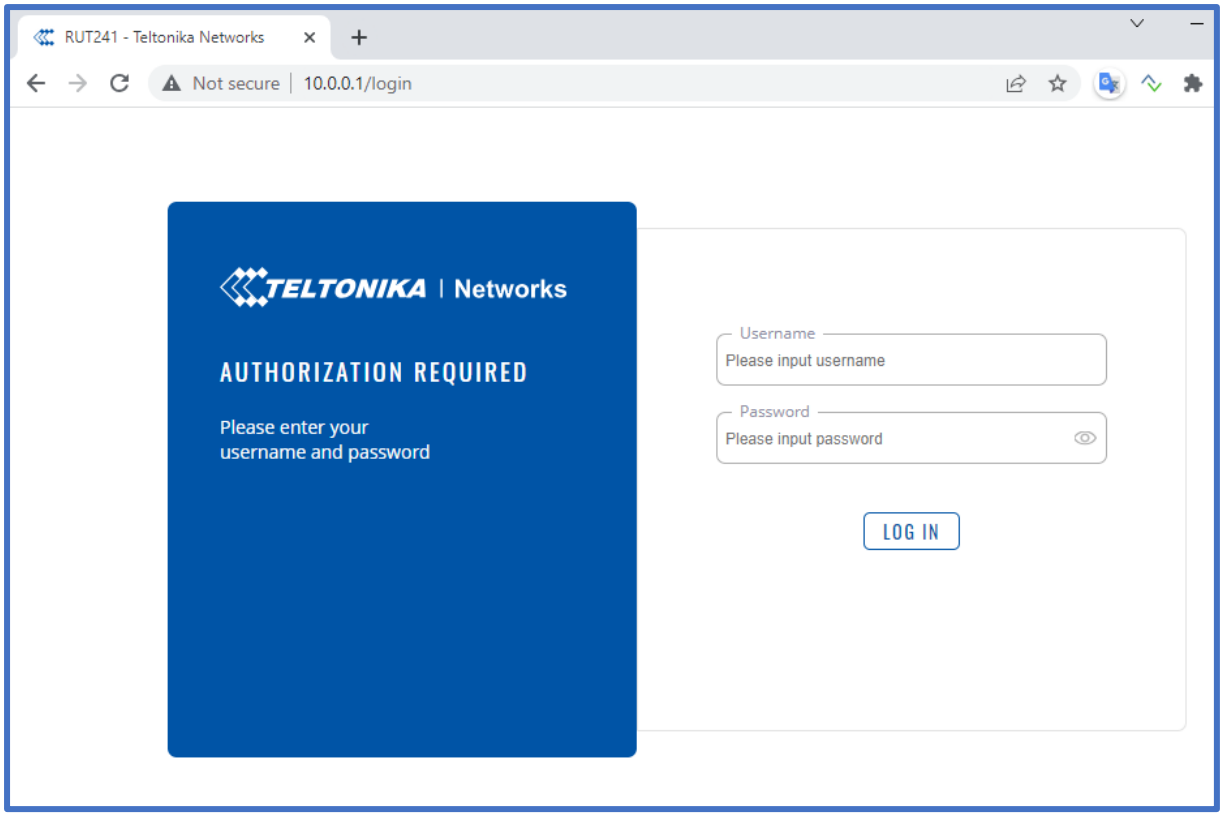


Click **BROWSE**, and select your OpenVPN configuration file, "C:\OpenVPN_conf\Configuration.ovpn", once it is loaded, click **CONNECT**:



Now you're connected to your router via OpenVPN !!!

You can access your router's web interface, using its VPN virtual address (10.0.0.1 in this case) :


RUT241 - Teltonika Networks
Not secure | 10.0.0.1/login
TELTONIKA | Networks
AUTHORIZATION REQUIRED
Please enter your
username and password
Username
Please input username
Password
Please input password
LOG IN

Enjoy !