https://wiki.teltonika-networks.com/view/Template:Connecting_to_the_office_network_remotely_from_your_home_via_VPN_(OpenVPN)

Template:Connecting to the office network remotely from your home via VPN (OpenVPN)

Contents

Configuration overview and prerequisites

Prerequisites:

- One RUTxxx router of any type (In this article RUTX11 will be used)
- A Public Static or Public Dynamic IP addresses
- At least one end device with Windows 10

The topology above depicts the OpenVPN scheme. - The router with the Public IP address (***RUTX11***) acts as the **OpenVPN server** and the **Windows 10 device** acts as a **client**. OpenVPN connects the networks of **RUTX11** and **Windows 10 clients**.

When the scheme is realized, home workers will be able to reach the corporation’s internal network with all internal systems, allowing working from home to be possible.

Configuring OpenVPN from the client-side

TLS Certificates

- Firstly generate TLS certificates on your Windows Computer, you can find instructions on how to do it here.
- After you've successfully generated TLS certificates you will need to create a **.ovpn** file for storing client configurations. Simply open any text editor and follow this tutorial.
- **Important: in your .ovpn file certificates you will need to copy are:**
- In **<ca> </ca>** paste whole certificate from **/easy-rsa/pki/ca.crt**
- IN **<cert></cert>** paste whole certificate from **/easy-rsa/pki/issued/"your_client_name".crt**
- And in the last section **<key></key>** paste whole private key from **/easy-rsa/pki/private/"your_client_name".key**
- One more thing to change in your .ovpn file is to change the IP address to your router's **public IP address**

- Now you can **Save** and **Import** your **.ovpn** file to the OpenVPN client by right-clicking on OpenVPN GUI in the hidden icons tray and navigating to **Import → Import File**.

Do not connect yet to your VPN client, we still have to configure the server.

Configuring OpenVPN from the server-side

Login to the router's WebUI and navigate to the **Services → VPN → OPENVPN** page and do the following:
1. Enter a **custom configuration name**
2. Select **Role: Server**.
3. Click the **Add** button.
4. Click the **Edit** button next to the newly created OpenVPN instance.

---

1. **Enable** OpenVPN instance.
2. Change **Authentication** to **TLS**
3. Change **Encryption** to **AES-256-GCM 256**
4. Change **Keep alive** to **5 10**
5. In **Virtual network IP address** type: **192.168.15.0**
6. **Virtual network netmask** select: **255.255.255.0**
7. Leave everything else default

---

1. The last thing left to do is to upload **Certificates**, firstly upload **Certificate authority** (**ca.crt** file)
2. Upload **Server certificate** (**server.crt** file)
3. Upload **Server key** (**server.key** file)
4. Now upload **Diffie Hellman parameters** (**dh.pem** file)
5. Press **SAVE & APPLY** button

Connecting to the OpenVPN server

If everything was configurated correctly your OpenVPN server should be **Active**:

Now let's try to connect from a **client** to the **server**.

On your Windows machine right-click on **OpenVPN GUI →** Select your client → Press Connect

If the connection was successful then you will get the following notification:

To test if the connection is working properly on your Windows machine open **CMD** and type ping **192.168.15.1** (server's VPN IP) you should get a similar response: