https://wiki.teltonika-networks.com/view/Configuring_clients_to_access_internet_through_office%27s_gateway_from_home_using_VPN_RUTX

Configuring clients to access internet through office's gateway from home using VPN RUTX

Contents

• 1 Configuration overview and prerequisites
• 2 Configuring HQ corporation router
  - 2.1 L2TP
  - 2.2 IPsec
  - 2.3 Firewall
• 3 Home worker’s computer
• 4 Results

Configuration overview and prerequisites

Prerequisites:

- One RUTxxx router (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 L2TP/IPsec scheme. - The router with the Public IP address (***RUTX11***) acts as the **L2TP/IPsec server** and the **Windows 10 device** acts as **client**. L2TP connects the networks of **RUTX11** and **Windows 10 client**, IPsec provides the encryption for the L2TP tunnel.

When the scheme is realized, home workers will be able to reach corporation’s internal network with all internal systems, allowing working from home to be possible. All of the home workers LAN and WAN traffic is going to go through that tunnel.

Configuring HQ corporation router

L2TP

Login to the router's WebUI and navigate to the **Services → VPN → L2TP** page and do the following:
1. Select **Role: Server**.
2. Enter a **custom configuration name**.
3. Click the **Add** button.
4. Click the **Edit** button next to the newly created L2TP instance.

---

1. **Enable** the L2TP instance.
2. Enter a **User name** and **Password** for authentication for the client.
3. Optionaly, set a fixed IP for this client (if left empty, client will receive first free IP from the IP range).
4. Don't forget to **Save** the changes.

IPsec

Go to the **Services → VPN → IPsec** page and do the following:
1. Enter a custom name for the IPsec instance.
2. Click the **Add** button.
3. Click the **Edit** button next to the newly created instance.

In the **IPsec Configuration** page, do the following (and leave the rest as defaults, unless your specific configuration requires otherwise):
1. **Enable** the instance.
2. Enter your **Pre-shared key**.
3. Select **Type: Transport**.
4. **Save** changes.

Firewall

Go to the **Network → Firewall → General Settings** and press edit next to the L2TP zone forwarding rule:

Allow L2TP forward to/from **WAN** and click the **Save & Apply** button:

Home worker’s computer

Type **VPN settings** in the Windows search bar:

Click the **Add a VPN connection** button:

Configure the following parameters:
1. Select **VPN provider: Windows (built-in)**.
2. Enter a custom **Connection name**.
3. Enter the router's WAN IP address into the **Server name or address** field.
4. Select **VPN type: L2TP/IPsec with pre-shared key**.
5. Enter the **Pre-shared key** exactly as it was specified on the router.
6. Select **Type of sign-in info: User name and password**.
7. Enter the **User name** and **Password** exactly as they were specified on the router.
8. Click **Save**

After you are redirected back to the VPN settings page, locate your new connection and click the Connect button. If the connection was successful, you should see the word "connected" appear under the connection name:

Results

Home worker should now be able to access HQ network resources. To verify the connection you can ping some internal HQ server and if you get a reply, you have successfully connected to HQ’s internal network.