Template:Networking rut configuration example l2tp over ipsec work use case

Contents

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

Configuration overview and prerequisites

Prerequisites:

- One RUTxxx routers of any type (excluding RUT850)
- 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 (***RUT955***) acts as the **L2TP/IPsec server** and the **Windows 10 device** acts as **client**. L2TP connects the networks of **RUT955** and **Windows 10 client**, IPsec provides the encryption for the L2TP tunnel. Only LAN traffic is going to go through that tunnel, any other WAN traffic won't go through it. This way the VPN tunnel will not be under a huge load and will provide greater speeds.

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.

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 New** 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. Select **Type: Transport** and **Save** changes.



After saving the changes, you will be redirected back to the main IPsec page. While there, locate the **Pre-shared Keys** section and do the following:
1. Click the **Add** button.
2. Enter your **Pre-shared key**.
3. Enter **%any** under **Secret's ID selector**.
4. Click the **Save** 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**



Type **Network Connections** in the Windows search bar:



Press right mouse click on your newly created VPN instance and select **Properties**:



Navigate to **Networking** section and double click **Internet Protocol Version 4 (TCP/IPv4)**:



Go to **Advanced** settings:



Now disable **Use default gateway on remote network** and save settings:



Go 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.

