L2TP over IPsec PC

Contents

Introduction

Because of the lack of confidentiality inherent in the **Layer 2 Networking Protocol** (**L2TP**), **Internet Protocol Security** (**IPsec**) is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as **L2TP over IPsec** (or simply **L2TP/IPsec**).

This article provides a guide on how to configure L2TP/IPsec on RUTxxx routers, to establish a connection with clients on their personal computers. It should also be noted that this guide is aimed at more advanced users and, therefore, skips some of the more self-explanatory steps in order to preserve the overall coherence of the article. For example, instead of showing how to add new instances step by step, it is only mentioned in a short sentence. If you feel this lack of information impedes your ability to configure the setup, we suggest you check out our separate configuration guides on **IPsec** and **L2TP** for reference.

*Click **Here** for a user's manual based on the old style WebUI (FW version RUT9XX_R_00.06.08.6 and earlier).*

Configuration overview and prerequisites

Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible.

Prerequisites:

- One RUTxxx router of any type (excluding RUT850) with a Public Static or Public Dynamic IP addresses
- At least one end device (PC, Laptop, Tablet, Smartphone) to configure the routers and connect to the VPN.

Configuration scheme:

The figure above shows the L2TP/IPsec scheme. It is quite similar to the L2TP and IPsec configuration schemes - the router with the public IP address (*RUT*) acts as the L2TP/IPsec server and a *PC* acts as the client. L2TP connects the RUT and PC networks and IPsec provides the encryption for the L2TP tunnel.

When tunnel connection is established, the L2TP packets between the endpoints are encapsulated by IPsec. Since the L2TP packet itself is wrapped and hidden inside the IPsec packet, the original source and destination IP address is encrypted inside the packet.

Router configuration

If you have familiarized yourself with the configuration scheme and have all of the devices in order, we can start configuring the router using instructions provided in this section. To summarize, we'll be configuring an L2TP server and an IPsec Transport instance (server) on *RUT*; an L2TP/IPsec client on *PC*.

L2TP

First, it is recommended to start with the L2TP tunnel configuration. This subsection contains instructions on how to do just that. The relevant parameters will be encapsulated **in red rectangles**. Explanations about these parameters will be provided under each example. For more information, you can visit the following wiki pages: **VPN manual page, IPsec section**.

New L2TP instances can be created from the **Services → VPN → L2TP** section of the router's WebUI. Select role as **Server**, enter any name for easy management. Then the configuration window will open up automatically when you press the "Add" button.

- **Server configuration**:

- **Enable** - when checked, enables the instance
- **Local IP** - the server's virtual IP address
- **Remote IP range** parameters - the range of virtual IP addresses that will be assigned to connecting clients
- **User name** and **Password** - authentication information used to authenticate connecting clients

- **L2tp Client's IP** - Optionaly, set a fixed IP for this client (if left empty, client will receive first free IP from the IP range).

IPsec

Next, you must configure a working IPsec transport connection. This subsection contains instructions on how to do just that. The relevant parameters will be encapsulated **in red rectangles**. Explanations about these parameters will be provided under each example. Other used parameters will be defaults; you can find explanations for those parameters in the **VPN manual page, IPsec section**.

Login to the router's WebUI and navigate to **Services → VPN → IPsec**. Enter a custom name for your IPsec instance and click the "Add" button. Then click the "Edit" button located next to the newly created instance after which you will redirected to that instance's configuration window. Adhere to the configurations presented in the figure below:

- **Remote VPN endpoint** - IP address or hostname of the remote IPsec instance. **Leave empty** for the server configuration
- **Enable** - if checked, enables the IPsec instance
- **Authentication method** - different authentication methods between the peers. For this configuration we select **Pre-shared key**
- **Pre shared key** - a shared password used for authentication between the peers. The value of this field must match the other instance
- **Type** - the type of the connection. **Transport** encrypts only the payload and Encapsulating Security Payload (ESP) trailer; so the IP header of the original packet is not encrypted. Transport mode is usually used when another tunneling protocol (such as GRE, L2TP) is used to first encapsulate the IP data packet, then IPsec is used to protect the GRE/L2TP tunnel packets. NAT traversal is not supported with the transport mode.
- **Bind to** - which interface is going to be bind to the IPsec configuration. The L2TP interface must be selected.
- **Custom option** - rekey=0
- **Encryption algorithm** - AES 256
- **Authentication** - SHA1
- **Force crypto proposal** - Enabled
- **DH group** - MODP2048

PC Client

Finally, you need to configure a PC to connect to the VPN configuration. This subsection contains instructions on how to do just that. The relevant parameters will be encapsulated **in red rectangles**. Explanations about these parameters will be provided under each example.

To configure a windows PC as a client, you can use the already developed VPN function. To do this, select the search bar and type "Add a VPN connection". Then select the "Add VPN" option.

- **Client configuration**:

- **VPN provider** - VPN provider to be configured. In our case we select the "Windows (build-in)" option.
- **Connection name** - enter a custom name.
- **Server name or address** - The server with the VPN configuration to which we are going to connect. In this case, the public IP of the server is entered.
- **VPN Type** - Type of VPN to be configured. In our case we select "L2TP/IPsec with pre-shared key".
- **Pre shared key** - a shared password used for authentication between the peers. The value of this field must match the other instance.
- **Type of sign-in info** - VPN authentication configuration. In our case we select "Username and password".
- **User name** and **Password** - authentication information used to authenticate connecting clients. The value of this field must match the other instance.

After the configuration is done, save and select connect. After a few seconds our VPN should be connected.

Testing the setup

If you've followed all the steps presented above, your configuration should be finished. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. The simplest way to test an IPsec connection is using the ipsec status command. You can execute this command via a command line interface (CLI). A CLI is present in all RUTxxx routers' WebUIs. To access it, login to the routers' WebUI and navigate to **Services → CLI** . Login to CLI with the user name root and the router's admin password. Then simply the ipsec status and press the "Enter" key:

As you can see, executing ipsec status displays the number of active/inactive IPsec connections. If the connection you just configured is the only IPsec connection that you're using, you should a 1 up indication next to Security Associations.

To test an L2TP connection. You should then be able to ping the opposite instance, i.e., if you logged in to the server's CLI, you should be able to ping the client's virtual IP address, and vice versa. To use a ping command, type **ping <ip_address>** and press the **Enter** key on your keyboard:

If the ping requests are successful, congratulations, your setup works! If not, we suggest that you review all steps once more.

See also

- Other types of VPNs suported by RUTxxx devices:
  - L2TP configuration examples
  - IPsec configuration examples
  - GRE Tunnel configuration examples
  - OpenVPN configuration examples

- PPTP configuration examples