L2TPv3 over IPsec configuration example

Contents

Introduction

The information on this page is updated in accordance with firmware version **00.07.02.7**.

Because of the lack of confidentiality inherent in the **Layer 2 Networking Protocol** (**L2TP**) protocol, **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 L2TPv3/IPsec on RUTxxx routers. 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.

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:

- Two RUTxxx routers
- At least one router with a Public Static or Public Dynamic IP addresses
- At least one end device (PC, Laptop, Tablet, Smartphone) to configure the routers
- Two VLANs configurated on both devices

Preparation

As mentioned in Prerequisites, you will need to configure two VLANs on both RUT devices, detailed instructions on how to configure them can be found on this page: **VLAN Set Up** Everything else we will configure along the way.

Topology

IPsec configuration

First, 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**.

RUT1

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 be redirected to that instance's configuration window. Adhere to the configurations presented in the figure below:

- **Enable** - if checked, enables the IPsec instance
- **Remote endpoint** - IP address or hostname of the remote IPsec instance. Provide **RUT2** device's **WAN IP** here.
- **Pre shared key** - a shared password used for authentication between the peers. The value of this field must match the other instance
- **Local identifier** - 10.1.0.1
- **Remote identifier** - 10.2.0.2
- **Local subnet** - 10.1.0.0/24
- **Remote subnet** - 10.2.0.0/24
- **IKE liftime** - 3h, make sure you've inserted the same liftime in **Phase 1** and **Phase 2**

RUT2

Create another instance on the second router the same way you created the server (login, add new instance, click **"Edit"**). Adhere to the configurations presented in the figure below:

- **Enable** - if checked, enables the IPsec instance
- **Remote endpoint** - IP address or hostname of the remote IPsec instance. Provide **RUT1** device's **WAN IP** here.
- **Pre shared key** - a shared password used for authentication between the peers. The value of this field must match the other instance
- **Local identifier** - 10.2.0.2
- **Remote identifier** - 10.1.0.1
- **Local subnet** - 10.2.0.0/24
- **Remote subnet** - 10.1.0.0/24
- **IKE liftime** - 3h, make sure you've inserted the same liftime in **Phase 1**and **Phase 2**

Testing IPsec connection

When you're done with the configuration, you should test whether it works before you move on. 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 one of the routers' WebUI (doesn't matter which one) and navigate to **Services → CLI**. Log in 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.

L2TPv3

Next, you must configure a working L2TPv3 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. For more detailed informaton refer to **VPN, L2TPv3**.

New L2TPv3 instances can be created from the **Services → VPN → L2TP → L2TPv3** section of the router's WebUI. Enter a custom name and click the "Add" button to create a new instance. Then click the "Edit" button located next to the newly created instance to enter its configuration page.

RUT1

- **Enable** - if checked, enables the L2TPv3 instance
- **Local address** - IP address of the **local** instance. Provide **RUT1** device's **LAN IP** here.
- **Tunnel ID** - Uniquely identifies the tunnel. The value used must match the peer tunnel **ID** value being used at the peer. For this example **3000**.
- **Session ID** - The value used must match the tunnel ID value being used at the peer. For this example **1000**.
- **Peer address** - IP address of the **remote** instance. Provide **RUT2** device's **LAN IP** here.
- **Peer Tunnel ID** - **RUT2** Tunnel ID: **4000**
- **Peer Session ID** - **RUT2** Session ID: **2000**
- **Bridge to** - you can select an instance that you want to bridge to. In this case select **None**.
- **IPv4 address** - Provide your **RUT1** first **VLAN IP** adress here. In this example **10.10.10.1**
- **Netmask** - netmask for provided IPv4 address above. In this example **255.255.255.0**
- **MTU** - **1488**
- **Encapsulation** - **UDP**
- **UDP source port** - **RUT1** UDP port. In this example **5000**
- **UDP destination port** - **RUT2** UDP port. In this example **6000**

RUT2

- **Enable** - if checked, enables the L2TPv3 instance
- **Local address** - IP address of the **local** instance. Provide **RUT2** device's **LAN IP** here.
- **Tunnel ID** - Uniquely identifies the tunnel. The value used must match the peer tunnel **ID** value being used at the peer. For this example **4000**.
- **Session ID** - The value used must match the tunnel ID value being used at the peer. For this example **2000**.
- **Peer address** - IP address of the **remote** instance. Provide **RUT1** device's **LAN IP** here.
- **Peer Tunnel ID** - **RUT1** Tunnel ID: **3000**
- **Peer Session ID** - **RUT1** Session ID: **1000**
- **Bridge to** - you can select an instance that you want to bridge to. In this case select **None**.
- **IPv4 address** - Provide your **RUT2** first **VLAN IP** adress here. In this example **10.10.10.2**
- **Netmask** - netmask for provided IPv4 address above. In this example **255.255.255.0**
- **MTU** - **1488**
- **Encapsulation** - **UDP**
- **UDP source port** - **RUT2** UDP port. In this example **6000**
- **UDP destination port** - **RUT1** UDP port. In this example **5000**

Firewall rules

Before testing L2TPv3 over IPsec configuration we will need to change **L2TPv3** Firewall rules on both **RUT1** and **RUT2**. To do that Open your device's **Firewall** by navigating to **Network → Firewall → Traffic Rules**. Now on both **RUT1** and **RUT2**, you will need to find two rules called **Allow-your_instance_name-L2TPv3-traffic**

Now **Edit** both of these rules and search for **Destination address** field. In this field, there should be written **0.0.0.0** you need to **delete** this address and **Save** the configuration. Repeat this process on both rules and on both **RUT1** and **RUT2**.

Testing L2TPv3 configuration

The simplest way to test an L2TPv3 connection is using the **ip l2tp show tunnel** 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 one of the routers' WebUI (doesn't matter which one) and navigate to **Services → CLI**. Log in to CLI with the user name **root** and the router's admin password. Then simply the *ip l2tp show tunnel* and press the "Enter" key. IF everything was configurated correctly you should see two L2TPv3 tunnels (example was taken from **RUT1**):

Testing full configuration

TCP Dump

The first way of testing our setup would be to check if the traffic between **RUT1** and **RUT2** devices is encrypted. To do this we will require to utilize **TCP Dump**, **TCP Dump** will let us capture traffic that goes through **RUT2**. In this example, we will install **TCP Dump** on **RUT2** and we will proceed on capturing the data that is going through the device.

Installing TCP Dump on RUT2

Firstly, you will need to connect to the **RUT2** device's **CLI/SSH**. You can connect the **RUT2** device CLI via WebUI by navigating to **Services → CLI**. Log in to **CLI** with the user name **root** and the router's admin password.

Now execute these commands one at a time:

opkg update

opkg install tcpdump

To test if TCP Dump has been installed on your device execute the command *tcpdump*

Installing Wireshark

To see captured data via TCP Dumb we will be using Wireshark, although the data can be seen

directly from CLI/SSH, Wireshark will let you see more information about captured data and it is simpler to understand TCP Dump output. The Wireshark can be downloaded here.

Capturing TCP Dump

Now you will need to login on to both **RUT1** and **RUT2** devices CLI/SSH. Once you have logged on both devices CLI/SSH, on **RUT1** execute command **ping 10.2.0.0**

Leave this command running, the output should be similar:

Now on RUT2 execute the command **tcpdump -i wwan0 -n -w test.pcap** this command will capture all **wwan0 interface (mobile)** traffic and write it into **test.pcap** file. Leave this command running for a minute and after that press **Ctrl + C** to stop this command.

Now in your device (at the directory in that you have executed the TCP Dump command(in this example /root/) you will be able to find **test.pcap** file, extract it to your computer(you can find instructions on how to do that here:**Upload & Download Files from RutOS** and open this file with Wireshark. You should see similar output:

Here you will need to look if your devices communicate with **ESP(Encapsulating Security Payload)** protocol, if so then your configuration is working.

Ping VLANs

Another simple method to check if the configuration is working is to test if **RUT1 VLAN** can reach **RUT2 VLAN** and vice versa. In this example we will execute ping command of **VLAN1** interface of **RUT1** to **VLAN1** of **RUT2**.

Once again login to RUT1 CLI/SSH and execute the command **ping -I 10.10.10.1 10.10.10.2** this will execute a ping from **VLAN1 of RUT1 to VLAN1 of RUT2**. If the configuration is working you should see a similar output of this command:

See also

Other types of VPNs supported by RUTxxx devices:

- L2TP configuration examples
- L2TP over IPsec
- IPsec configuration examples

- GRE Tunnel configuration examples
- OpenVPN configuration examples
- PPTP configuration examples