https://wiki.teltonika-networks.com/view/IPsec_RUTOS_configuration_example

IPsec RUTOS configuration example

Main Page > General Information > Configuration Examples > VPN > **IPsec RUTOS configuration example**

The information in this page is updated in accordance with **00.07.06.3** firmware version.

□

Contents

Introduction

In computing, **Internet Protocol Security** (**IPsec**) is a secure network protocol suite of IPv4 that authenticates and encrypts the packets of data sent over an IPv4 network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

This article provides an extensive configuration example with details on how to create a tunnel connection between two IPsec instances, both of which are configured on RUTxxx routers.

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:

- 1 RUTX11 router
- 1 RUT955 router
- At least one router must have a Public Static or Public Dynamic IP address
- At least one end device (PC, Laptop, Tablet, Smartphone) to configure the routers

---

Configuration topology:

The figure above depicts a RUTX11 with a Public IP connected by an IPsec tunnel via the Internet to a RUT955.

It should also be noted that the connection type used is **Tunnel** and not **Transport**. Tunnel protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by a another set of IP headers. 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.

Tunnel is more widely implemented in site-to-site VPN scenarios and supports NAT traversal. For instructions on how to configure Transport mode, you may want to check out our **L2TP over IPsec** article.

Router configuration

If you have familiarized yourself with the configuration schemes and have all of the devices in order, we can start configuring the routers using instructions provided in this section.

RUTX11

First of all, let's configure the VPN IPsec instance from RUTX11's side:

- Login to the router's WebUI and go to **Services → VPN → IPsec**. Enter a custom name (for this example we use *test*) for the IPsec instance click the "Add" button:

- Click the "Edit" button located next to the newly created instance and set up the configuration according to the network:

- Below are explanations of the parameters highlighted in the figure above. Other parameters (not highlighted) are defaults. You can find descriptions for these parameters in the **VPN manual page, IPsec section**
    - **Enable** - enables the IPsec instance
    - **Local IP address/Subnet mask** - LAN IP address/Subnet mask of the router on which the IPsec instance is configured
    - **Pre shared key** - a shared password used for authentication between the peers. The value of this field must match on both instances
    - **Remote VPN endpoint** - the Public IP address of the opposite router
    - **Remote IP address/Subnet mask** - LAN IP address/Subnet mask of the opposite router

    - **Enable keepalive** - enables the tunnel's keep alive function. When enabled, the instance sends ICMP packets to the specified host at the specified frequency. If no response is received, the instance attempts to restart the connection
        - **Host** - hostname or IP address to which ICMP packets will be sent to. Best to use a hostname/IP address belonging to the opposite instance's LAN. For this example we just use the other router's LAN IP address
        - **Ping period (sec)** - the period (in seconds) at which ICMP packets will be sent to the specified host
    - **XAUTH** - this option is only available when IKEv1 is selected. When enabled, it can be used for additional authentication.
    - **IKEv2 vs IKEv1** - use IKEv2 for better security, speed, and flexibility, especially in dynamic environments. IKEv1 is older but still widely supported in legacy systems. Choose based on specific requirements and compatibility.
    - **Local&Remote identifiers** - there are two types, IP address type - which could describe certain subnet gateways like 192.168.1.1 or whole subnet like 192.168.1.0/24. Hostname type - is when an IP address is subject to change, providing more flexibility, and looks like - " vpngatewayname.yourdomain ".

NOTE: remember to replace certain parameter values (like IP addresses) with your own relevant data.

- IKE lifetime must be added and can be any desired value.

- Phase 1 & Phase 2 details should be the same with that of the RUT955 P1 & P2 details or else the tunnel will not be properly established.

RUT955

Similarly, the configuration for the VPN IPsec instance from RUT955's side is as follows:

- In this case, Remote endpoint should be RUTX11's Public IP:

- The last step in configuring the IPsec instances is **Phase settings**. Make sure they match with the Phase settings (both Phase 1 and Phase 2) of the RUTX11's connection:

After Clicking on “Save & Apply” for both the routers we can try pinging the remote LAN IP to see if it's reachable. Also using the command “ipsec status” in CLI will show the status of the IPsec Connection.

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. To test an IPsec connection, you could use the command “ipsec status” in CLI. It will show the status of the IPsec Connection similar to the ones shown below. You can also **ping** the opposite instance's VPN IP address. To use a ping command, type **ping <ip_address>** and press the "Enter" key on your keyboard:

You can also test if LAN access is working the same way. Instead of pinging the opposite instance's LAN IP address, ping one of the end device's IPs. One common issue that can be encountered here is that the end devices **might need their DHCP leases renewed**. There are many methods of accomplishing this, but the easiest and most accessible way is to simply disconnect and reconnect the LAN cable to device or the router that it's connected to.

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:
  - OpenVPN configuration examples
  - GRE Tunnel configuration examples

- PPTP configuration examples
- L2TP configuration examples