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

Default IPsec route configuration between Teltonika Networks devices

The information on this page is updated in accordance with the **00.07.4** firmware version .

□

Contents

Introduction

Normally we configure IPsec for LAN-to-LAN communication which is also known as split-tunnel VPN when only specific hosts should be reachable via VPN tunnel. However, we may also take a different approach and configure VPN tunnel using full-tunnel method. This means that any non-directly connected network (i.e. lan interface) will be reachable only via IPsec tunnel and not via typical default route.

Configuration overview and prerequisites

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

Prerequisites:

- Two RUT/RUTX series routers with RUTOS firmware;
- An end device (PC, Laptop) for configuration;

If you're having trouble finding any page or some of the parameters described here on your device's WebUI, you should turn on **"Advanced WebUI"** mode. You can do that by **clicking** the **"Basic"** button **under "Mode,"** which is located at the top-right corner of the WebUI.

Topology

RUT1 - RUTX12 as a **hub**. A hub is a server, to which our spoke will be connecting (IPsec responder). It will be our "default gateway" for the spoke device. RUTX12 has a LAN subnet of 192.168.11.0/24 configured on it, which should be reachable by the **spoke**.

RUT2 - RUT955 as a **spoke**. A spoke is a client, that will be connected to the spoke (IPsec initiator). It will be connected to a **hub** for basic internet access. RUT955 has a LAN subnet of 192.168.9.0/24 configured on it.

RUT1 (Hub) configuration

Start by configuring the hub (RUT1) device. Login to the WebUI, navigate to **Services → VPN → IPsec** and **add a new IPsec instance**. Configure everything as follows.

Note: *Not specified fields can be left as is or changed according to your needs.*

Instance configuration

---

1. ***Enable*** instance;
2. Authentication method - ***Pre-shared key;***
3. Pre-shared key - ***your desired password;***

Connection configuration

---

1. Mode - ***Start;***
2. Type - ***Tunnel;***
3. Local subnet - ***0.0.0.0/.0;***
4. Key exchange - ***IKEv2;***

---

1. ***Enable Local firewall;***
2. Remote source IP - ***10.20.30.0/24;***
3. Remote DNS - ***9.9.9.9;***

Proposal configuration

---

1. Encryption - ***AES256;***
2. Authentication - ***SHA512;***
3. DH group - ***ECP521;***
4. Force crypto proposal - **enabled**.

---

1. Encryption - ***AES128;***
2. Authentication - ***SHA256;***
3. DH group - ***ECP521;***
4. Force crypto proposal - **enabled**.

Force crypto proposal option as it simplifies which algorithm suite will be used for both phases.

RUT2 (Spoke) configuration

Login to the RUT2 WebUI, navigate to **Services → VPN → IPsec** and **add a new IPsec instance.** Configure everything as follows.

Note: *Not specified fields can be left as is or changed according to your needs.*

Instance configuration

---

1. ***Enable*** instance;
2. Remote endpoint - ***RUT1 public IP;***
3. Authentication method - ***Pre-shared key;***
4. Pre-shared key - the ***same password*** you have ***set on RUT1*** when configuring ***HUB instance;***

Connection configuration

---

1. Mode - ***Start;***
2. Type - ***Tunnel;***
3. ***Enable default route;***
4. Key exchange - ***IKEv2;***

Proposal configuration

---

1. Encryption - ***AES256;***
2. Authentication - ***SHA512;***
3. DH group - ***ECP521;***
4. Force crypto proposal - **enabled**.

---

1. Encryption - ***AES128;***
2. Authentication - ***SHA256;***
3. DH group - ***ECP521;***
4. Force crypto proposal - **enabled**.

Force crypto proposal option as it simplifies which algorithm suite will be used for both phases.

Testing the configuration

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.

Using the **`ipsec status`** command we can see that IPsec tunnel is successfully established on both routers. The command output on a **hub (RUT1)** device:

The same command output on **spoke (RUT2)** device:

Also, as the hub should be reachable by spoke, we can try pinging the hub using **`ping`**

192.168.11.1:

See also

IPsec on Teltonika Networks devices

External links

OpenWrt IPsec basics