Setting up a GRE over IPsec tunnel between RUTOS devices

Contents

Introduction

This article provides a configuration example with details on how to configure a GRE over IPsec connection between two RUTOS devices.

The information in this page is updated in accordance with the ***R_00.07.01*** firmware version.

If you're having trouble finding this 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 "Advanced" button, located at the top of the WebUI.

Prerequisites

- Two Teltonika routers/gateways with RUTOS support.
- Both devices must have WAN access with a static public IP.
- At least one end device (PC, Laptop) to configure the routers.

Configuration scheme

GRE tunnel configuration

First we will establish a GRE tunnel between our devices.

Router 1 GRE configuration

---

1. Login to the *Router 1* device's WebUI, navigate to the **Services → VPN → GRE** page.
2. Add a new *GRE1* instance by entering custom **New configuration name** and clicking **Add** button.

3. A configuration window should appear. Configure the GRE instance accordingly:
    1. **Enabled** - ON.
    2. **Tunnel source** - select the network interface with Public IP which is used to establish GRE tunnel.
    3. **Remote endpoint IP address** - Public IP address of remote (*Router 2*) device.
    4. **MTU** - 1476
    5. **Outbound key** - 12345 Limit:4294967295 (must match other device's Inbound key)
    6. **Inbound key** - 12345 Limit:4294967295 (must match other device's Outbound key)
    7. **Keep alive** - ON
    8. **Local GRE interface IP address** - 10.0.0.1
    9. **Local GRE interface IP netmask** - 255.255.255.0
    10. **Remote subnet IP address** - 192.168.4.0
    11. **Remote subnet netmask** - 255.255.255.0

Router 2 GRE configuration

Router 2 configuration as very similar except for IP addresses. Create a new *GRE2* instance and configure accordingly:

1. **Enabled** - ON.
2. **Tunnel source** - select the network interface with Public IP which is used to establish GRE tunnel.
3. **Remote endpoint IP address** - Public IP address of remote (*Router 1*) device.
4. **MTU** - 1476
5. **Outbound key** - 12345 Limit:4294967295 (must match other device's Inbound key)
6. **Inbound key** - 12345 Limit:4294967295 (must match other device's Outbound key)
7. **Keep alive** - ON
8. **Local GRE interface IP address** - 10.0.0.2
9. **Local GRE interface IP netmask** - 255.255.255.0
10. **Remote subnet IP address** - 192.168.2.0

11. **Remote subnet netmask** - 255.255.255.0

Testing GRE tunnel

Connect to either device's CLI and run command **ifconfig**. Local GRE interface should be up:

Remote GRE tunnel IP and remote LAN IP should be reachable:

IPsec configuration

Now we will setup an IPsec connection between our devices to encrypt all data going through the GRE tunnel. This configuration will work as a kill switch too as it will automatically disable GRE tunnel in case IPsec connection goes down.

Router 1 IPsec configuration

---

1. Navigate to the **Services → VPN → IPsec** page and add a new *IPSEC1* instance.
2. In the new window, configure accordingly:
    1. **Enabled** - ON.
    2. **Remote endpoint** - public IP address of remote (*Router 2*) device. Only one side needs to have this configured
    3. **Pre shared key** - ipsec123 (must match on both devices)

3. **Connection Settings → General Settings** section:
    1. **Type** - Transport
    2. **Bind to** - GRE1 (GRE)

4. **Connection Settings → Advanced Settings** section:
    1. **Locally allowed protocols** - gre
    2. **Remotely allowed protocols** - gre

5. **Proposal Settings** can be configured personally, but must match on both devices.

Router 2 IPsec configuration

Router 2 configuration is identical to Router 1 configuration, except for:

2.2. **Remote endpoint** - you may leave empty or enter Router 1 WAN IP.

3.2. **Bind to** - GRE2 (GRE)

Testing GRE over IPsec

Connect to either device's CLI and use command **ipsec status**, you should see IPsec tunnel via GRE interface is established.

To test kill switch functionality run command **ipsec stop** and then run command **ifconfig**. GRE interface should be no longer available until IPsec connection comes back up.

After GRE over IPsec connection gets established you should be able to reach all hosts in remote LAN network and vice versa.

Sometimes end devices might be unreachable even though GRE over IPsec connection is successfully established, to resolve this it might be needed to **renew DHCP lease** of end device or if it has multiple network adapters then **increase metric priority** of default gateway associated with RUT device.