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

Default IPsec route configuration between Teltonika and Fortigate devices

The information in this page is updated in accordance with **00.07.07.2** firmware version.

The information in this page is updated in accordance with **Fortigate v7.4.3** firmware version.

□

Contents

Introduction

Normally we configure IPsec for LAN-to-LAN communication, also known as split-tunnel VPN, when only specific hosts or subnets should be reachable via a VPN tunnel. However, we may also take a different approach and configure a VPN tunnel using the 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 the typical default route.

Configuration overview and prerequisites

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

Prerequisites:

- One RUT/RUTX series router or TRB gateway with RUTOS firmware;
- One Fortigate series router;
- An end device (PC, Laptop) for configuration;

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.

Topology

Fortigate – The **Fortigate** will act as a "default gateway" for the RUT device. **Fortigate** has a LAN subnet of 192.168.5.0/24 and WAN subnet of 192.168.10.2/24 configured on it, which should be reachable by the RUT.

RUT – The **RUTX11** in this case will be connected to **Fortigate** for basic internet access. **RUT** has a LAN subnet of 192.168.1.0/24 and WAN subnet of 192.168.10.1/24 configured on it.

Fortigate configuration

Start by configuring the **Fortigate** device. Login to the WebUI, navigate to **1. VPN → 2. IPsec Tunnels → 3. Create new → 4. IPsec Tunnel → 5. Your desired name → 6. Template type: Custom → 7. Click on the button next**.

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

Network configuration

Configure everything as follows. Make the following changes:

1. Remote Gateway – ***Static IP Address;***
2. IP Address – ***192.168.10.1;***
3. Interface – ***wan1;***

Authentication configuration

Make the following changes:

1. Method – ***Pre-shared Key;***
2. Pre-shared Key – ***your desired password;***
3. Version – ***2;***

Phase 1 Proposal configuration

Note: *This is only an example of a secure configuration. Other algorithms or even combinations of them could be used. However, we strongly recommend refraining from using older encryption and hashing algorithms unless support for certain legacy systems is required.*

Make the following changes:

1. Encryption – ***AES256;***
2. Authentication - ***SHA512;***
3. Diffie-Hellman Group – ***16;***
4. Key Lifetime (seconds) – ***86400;***

Phase 2 Selectors configuration

Note: *This is only an example of a secure configuration. Other algorithms or even combinations of them could be used. However, we strongly recommend refraining from using older encryption and hashing algorithms unless support for certain legacy systems is required.*

Make the following changes: ***Click on Advanced settings;***

1. Encryption – ***AES256;***
2. Authentication - ***SHA512;***
3. Diffie-Hellman Group – ***16;***
4. Key Lifetime – ***Seconds;***
5. Seconds – ***86400;***

Firewall configuration

After setting up our IPsec instance, we will need to configure our firewall accordingly. Navigate to **Policy & Objects → Firewall Policy → and click on a Create new button.**. Configure everything as follows.

In this example, we are allowing all types of traffic through the tunnel, but you can restrict certain traffic by specifying the services that are allowed via the tunnel.

Make the following changes:

1. Incoming interface - ***Tunnel interface name (In this case it is Teltonika);***
2. Outgoing interface - ***wan2 (choose WAN port from which Fortigate gets internet);***
3. Source - ***192.168.1.0/255.255.255.0;***
4. Destination - **all;**

5. Service - **ALL;**

Static Routes configuration

After setting up our IPsec instance and firewall, we will need to configure our static route accordingly. Navigate to **Network → Static routes → and click on a Create new button.**. For that we will need to create two static routes, one for blackhole and one for accessing our RUT device, configure everything as follows.

Make the following changes:

1. Destination - ***192.168.1.0/255.255.255.0;***
2. Interface - ***Tunnel interface name (In this case it is Teltonika);***

Then create a new static route for blackhole. Make the following changes:

1. Destination - ***192.168.1.0/255.255.255.0;***
2. Interface - ***Blackhole;***
3. Administrative distance - ***254;***

RUT configuration

Start by configuring the **RUT** 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

Make the following changes:

1. ***Enable*** instance;
2. Remote endpoint - ***Fortigate WAN IP;***
3. Authentication method - ***Pre-shared key;***
4. Pre-shared key - the ***same password*** you have ***set on Fortigate*** when configuring the ***Fortigate IPsec instance;***
5. Local identifier – ***RUT WAN IP;***
6. Remote identifier – ***Fortigate WAN IP;***

Connection general section configuration

Make the following changes:

1. Mode - ***Start;***

2. Type - ***Tunnel;***
3. Local subnet – ***192.168.1.0/24;***
4. Remote subnet – ***0.0.0.0/0;***
5. Key exchange - ***IKEv2;***

Connection advanced section configuration

Make the following changes:

1. ***Enable local firewall***
2. Remote DNS – ***8.8.8.8;***
3. Passthrough subnets – ***192.168.1.0/24;***

Proposal configuration

Note: *This is only an example of a secure configuration. Other algorithms or even combinations of them could be used. However, we strongly recommend refraining from using older encryption and hashing algorithms unless support for certain legacy systems is required.*

Make the following changes:

1. Encryption - ***AES256;***
2. Authentication - ***SHA512;***
3. DH group - ***MODP4096;***
4. IKE lifetime - **86400s**.

---

1. Encryption - ***AES256;***
2. Authentication - ***SHA512;***
3. PFS group - ***MODP4096;***
4. Lifetime – ***86400s;***

Testing the configuration

If you have followed all the above steps, 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`** or we can use **`ipsec statusall`** command for a more verbose output. With these commands we can see that the IPsec tunnel is successfully established on RUT router. The command output on a **RUT** device:

Also, we should be able to access internet routed via Fortigate, we can check it out by pinging

8.8.8.8 and checking what public IP we get by executing this command via command line on RUT device: **`curl icanhazip.com`** and **`ping 8.8.8.8`**:

To check if IPsec tunnel is working properly from **Fortigate**, we can try pinging our **RUT** device by using this command in command line interface on Fortigate**`exec ping 192.168.1.1`**, if you are not able to ping **RUT** device, try changing the source interface from which we try pinging, by executing this command **`exec ping-options source 192.168.5.99`**:

We can also check if IPsec tunnel is working properly from **Fortigate** WebUI, navigate to **VPN → IPSec Tunnels** and there you will see if the tunnel is working:

See also

IPsec on Teltonika Networks devices

External links

OpenWrt Ipsec basics

Fortigate Ipsec configuration