IPsec site to site configuration between Teltonika and Fortinet 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 **Fortinet 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 Fortinet 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.

Site to site configuration RUT public IP

This section provides a guide on how to configure a successful site to site IPsec vpn connection between **RUT** and **Fortinet** devices.

Topology

RUT – **RUT** will act as a **hub**. A hub is a server (IPsec responder), to which our spoke will be connected. It will be our remote endpoint for the spoke device. RUT has a LAN subnet of 192.168.1.0/24 and a WAN with Public IP, which should be reachable by the spoke.

Fortinet – **Fortinet** will act as a **spoke**. A spoke is a client (IPsec initiator), that will be connected to the hub. It will be connected to a **hub** to be able to reach RUT LAN subnet. Fortinet has a LAN subnet of 192.168.5.0/24 and a WAN with private IP.

Fortinet configuration

Start by configuring the **Fortinet** 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 – ***RUT public IP;***
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 - **lan;**
2. Outgoing interface - **IPsec tunnel interface name (In this case it is Teltonika);**
3. Source - **192.168.5.0/255.255.255.0;**
4. Destination - **192.168.1.0/255.255.255.0;**
5. Service - **ALL;**
6. **NAT disabled;**

Then create a second firewall rule.

Make the following changes:

1. Incoming interface - **IPsec tunnel interface name (In this case it is Teltonika);**
2. Outgoing interface - **lan;**
3. Source - **192.168.1.0/255.255.255.0;**
4. Destination - **192.168.5.0/255.255.255.0;**
5. Service - **ALL;**
6. **NAT disabled;**

Our firewall should look like this:

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. Authentication method - ***Pre-shared key;***
3. Pre-shared key - the ***same password*** you have ***set on Fortinet*** when configuring the ***Fortinet IPsec instance;***
4. Local identifier – ***RUT LAN IP;***
5. Remote identifier – ***%any;***

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 – ***192.168.5.0/24;***
5. Key exchange - ***IKEv2;***

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;***

Site to site configuration with multiple LANs

This section provides a guide on how to configure a successful site to site IPsec vpn connection between **RUT** and **Fortinet** devices with multiple LANs.

Topology

RUT – **RUT** will act as a **hub**. A hub is a server (IPsec responder), to which our spoke will be connected. It will be our remote endpoint for the spoke device. RUT has a LAN1 subnet of 192.168.1.0/24, LAN2 subnet of 192.168.2.0/24 and a WAN with Public IP, which should be reachable by the spoke.

Fortinet – **Fortinet** will act as a **spoke**. A spoke is a client (IPsec initiator), that will be connected to the hub. It will be connected to a **hub** to be able to reach RUT LAN1 and LAN2 subnet. Fortinet has a LAN1 subnet of 192.168.5.0/24, LAN2 subnet of 192.168.4.0/24 a WAN with private IP.

Fortinet configuration

As for the configuration of IPsec tunnel, everything is the same, only the Phase 2 Selectors, Firewall and static route sections will be configured additionally, so for other sections refer to the guide site to site.

Phase 2 Selectors configuration

Make the following changes: **Steps 7 8 9 10 are the same for all selectors.**
1. Phase 2 interface - *Fortinet LAN1 to RUT LAN2;*
2. Phase 2 interface - *Fortinet LAN2 to RUT LAN1;*
3. Phase 2 interface - *Fortinet LAN2 to RUT LAN2;*
4. Phase 2 interface – *Fortinet LAN1 to RUT LAN1;*
5. Local address - *Write accordingly with the Fortinet LAN;*
6. Remote address - *Write accordingly with the RUT LAN;*
7. Encryption – *AES256;*
8. Authentication - *SHA512;*
9. Diffie-Hellman Group – *16;*
10. Seconds – *86400;*

Static route 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 four static route interfaces, two for blackholes and two for accessing our RUT device LAN1/LAN2, configure everything the same as for site to site, just add the LAN2. It should look like this:

RUT configuration

Then configure the **RUT** device. Login to the WebUI, navigate to **Services → VPN → IPsec and add a new IPsec instance.** Configure everything the same like site to site configuration, only change the **Connection general section** accordingly.

Connection general section configuration

Make the following changes:
1. Local subnet – *192.168.1.0/24;*
2. *Click + button to add another Local subnet;*
3. Local subnet - *192.168.2.0/24;*
4. Remote subnet – *192.168.5.0/24;*
5. *Click + button to add another Remote subnet;*
6. Remote subnet – *192.168.4.0/24;*
7. Key exchange - *IKEv2;*

Site to site configuration Fortinet public IP

This section provides a guide on how to configure a successful site to site IPsec vpn connection between **RUT** and **Fortinet** when **Fortinet** has a public IP and RUT is behind NAT. This setup will be similiar to Site to site configuration RUT public IP, we will need only to change network section

on Fortinet and on RUT we will need to add Remote endpoint.

Topology

Fortinet – Fortinet will act as a hub. A hub is a server (IPsec responder), to which our spoke will be connected. It will be our remote endpoint for the spoke device. Fortinet has a LAN subnet of 192.168.5.0/24 and a WAN with Public IP, which should be reachable by the spoke.

RUT – RUT will act as a spoke. A spoke is a client (IPsec initiator), that will be connected to the hub. It will be connected to a hub to be able to reach Fortinet LAN subnet. RUT has a LAN subnet of 192.168.1.0/24 and a WAN with private IP.

Fortinet configuration

As for the configuration of IPsec tunnel, everything is the same, only the Network and authentication sections needs to be changed, so for other sections refer to the guide site to site. Start by configuring the **Fortinet** 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

Make the following changes:

1. Remote Gateway – *Dialup User;*
2. Interface – *wan1;*

Authentication configuration

Make the following changes:

1. Method – *Pre-shared Key;*
2. Pre-shared Key – *your desired password;*
3. Version – *2;*
4. Accept Types - *Any peer ID;*

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. For other sections refer to the **"Site to site configuration RUT public IP" 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 - *Public IP of Fortinet device*
3. Authentication method - *Pre-shared key;*
4. Pre-shared key - the *same password* you have *set on Fortinet* when configuring the *Fortinet IPsec instance;*
5. Local identifier – *RUT LAN IP;*
6. Remote identifier – *%any;*

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 ping **Fortinet** device, we can check it out by executing this command via command line on RUT device: `ping 192.168.5.99`:

To check if IPsec tunnel is working properly from **Fortinet**, we can try pinging our **RUT** device by using this command in command line interface on Fortinet`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 **Fortinet** 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](#)

[Fortinet Ipsec configuration](#)