https://wiki.teltonika-networks.com/view/IPsec_Tunnel_with_X.509_Authentication_configuration_example

IPsec Tunnel with X.509 Authentication configuration example

The information in this page is updated in accordance with **00.07.08** 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 authenticating with X.509 Certs 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:

- Two RUTxxx routers of any type;
- One RUTxxx router with public IP address;
- Both RUTxxx routers must be accessible from each other's WAN connection;
- Firmware for the devices must be 00.07.xx.x or above. This is in part to make sure the StrongSwan service is at least version U5.9.6;
- An end device (PC, Laptop) for configuration;
- (Optional) A second end device to test remote LAN access;

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

RUT1 – It will be connected to a **RUT2** to be able to reach **RUT2** LAN subnet. **RUT1** has a LAN subnet of 192.168.3.0/24 and a WAN with private IP.

RUT2 – It will be our remote endpoint for the **RUT1** router. **RUT2** has a LAN subnet of 192.168.14.0/24 and a WAN with Public IP, which should be reachable by **RUT1**.

Router configuration

We will start our configuration with RUT1.

To generate certificates via router, you can refer to this link: Generating certificate via router

IPsec RUT1 Config

- Make sure that you have your certificates generated both for **RUT1** and **RUT2** routers.
- Login to the router's WebUI and go to **System → Services → VPN -> IPsec**
- Add a new instance with your desired name, in my case I will be using **RUT1**

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 - ***RUT2 WAN IP;***
3. Authentication method - ***X.509;***
4. Key - the ***RUT1.key.pem*** that you have generated from certificates;
5. Local certificate - the ***RUT1.cert.pem*** that you have generated from certificates;
6. CA certificate - the ***CA.cert.pem*** that you have generated from certificates;
7. Local identifier – ***RUT1 LAN IP, which is 192.168.3.1 in this case;***
8. Remote identifier – ***RUT2 LAN IP, which is 192.168.14.1 in this case***

We will need to add RUT2 certificate in the **Advanced settings**:

1. Click on **Advanced settings** in the IPsec instance section;
2. Remote certificate - the ***RUT2.cert.pem*** that you have generated from certificates;

Connection general section configuration

Make the following changes:

1. Mode - ***Start;***
2. Type - ***Tunnel;***
3. Local subnet – ***192.168.3.0/24;***
4. Remote subnet – ***192.168.14.0/24;***
5. Key exchange - ***IKEv2;***

Connection advanced section configuration

Make the following changes:

1. Open **Advanced settings**;
2. ***Enable Force encapsulation***;
3. ***Enable Local firewall***;
4. ***Enable Remote firewall***;
5. Inactivity: ***3600*** - Defines the timeout interval, after which the connection is closed;
6. ***Enable Dead peer detection***;
7. DPD action – ***Restart***;

Proposal configuration

Important: Both the RUT1 and RUT2 Encryptions must match in order for this configuration to work.

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;***

IPsec RUT2 Config

- Make sure that you have your certificates generated both for **RUT1** and **RUT2** routers.
- Login to the router's WebUI and go to **System → Services → VPN -> IPsec**
- Add a new instance with your desired name, in my case I will be using **RUT2**

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 - ***X.509;***
3. Key - the ***RUT2.key.pem*** that you have generated from certificates;
4. Local certificate - the ***RUT2.cert.pem*** that you have generated from certificates;
5. CA certificate - the ***CA.cert.pem*** that you have generated from certificates;
6. Local identifier – ***RUT2 LAN IP, which is 192.168.14.1 in this case;***
7. Remote identifier – ***RUT1 LAN IP, which is 192.168.3.1 in this case***

We will need to add RUT2 certificate in the **Advanced settings**:

1. Click on **Advanced settings** in the IPsec instance section;
2. Remote certificate - the ***RUT1.cert.pem*** that you have generated from certificates;

Connection general section configuration

Make the following changes:

1. Mode - ***Start;***
2. Type - ***Tunnel;***
3. Local subnet – ***192.168.14.0/24;***
4. Remote subnet – ***192.168.3.0/24;***
5. Key exchange - ***IKEv2;***

Connection advanced section configuration

Make the following changes:

1. Open **Advanced settings**;
2. ***Enable Force encapsulation***;
3. ***Enable Local firewall***;
4. ***Enable Remote firewall***;
5. Inactivity: ***3600*** - Defines the timeout interval, after which the connection is closed;
6. ***Enable Dead peer detection***;
7. DPD action – ***Restart***;

Proposal configuration

Important: Both the RUT1 and RUT2 Encryptions must match in order for this configuration to work.

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 RUTxxx router. The command output on a **RUT1** device:

Also, we can try to ping the RUT2 device by executing this command **`ping 192.168.14.1`**, by which you should get a response if the IPsec tunnel has been established properly.

To check if the IPsec tunnel is working properly from **RUT2**, we can try pinging our **RUT1** device by using this command in command line interface on RUT2**`ping 192.168.3.1`**:

Also we can check it by executing 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 RUTxxx router. The command output on a **RUT2** device: