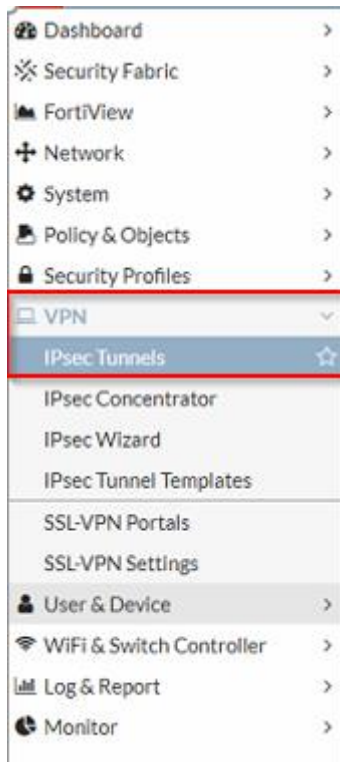


RUT9xx IPsec with Fortigate

1. Setting up IPsec on Fortigate	2
1.1. VPN -> IPsec tunnels > Network	3
2. Setting up IPsec on RUT9XX	6
2.1. Creating an IPsec instance	6
2.2. Creating a pre-shared key:	8
3. Topology	9
4. Testing the connection	9
4.1. On the router	9
4.2. On Fortigate	9

1. Setting up IPsec on Fortigate



1.1. VPN -> IPsec tunnels > Network

- Remote Gateway: **Dialup User**
- Interface: **Select your interface**
- Local Gateway: **Specify**
 - **Fortigate's public IP**
- Mode Config: **Uncheck**
- NAT Traversal: **Enable**
- Dead Peer Detection: **On Idle**

Name: Teltonika-01 100 concurrent user(s) will be supported

Comments:

Network

IP Version: IPv4

Remote Gateway:

Interface:

Local Gateway: Primary IP Secondary IP

Mode Config:

NAT Traversal:

Dead Peer Detection:

1.2. VPN -> IPsec tunnels > Authentication

- Method: **Pre-shared Key**
- Pre-shared Key: **Enter secret key**

Authentication

Method:

Pre-shared Key:

1.3. VPN -> IPsec tunnels > IKE

- Version: **1**
- Mode: **Aggressive**

IKE

Version:

Mode:

1.4. VPN -> IPsec tunnels > Peer Options

- Accept Types: **Specific peer ID**
- Peer ID: **Any string**

Peer Options

Accept Types

Peer ID

1.5. VPN -> IPsec tunnels > Phase 1 Proposal

- Encryption: **3DES**
- Authentication: **SHA1**
- Diffie-Hellman Group: **5**
- Key Lifetime (Seconds): **86400**
- Local ID: **Blank**

Phase 1 Proposal

Encryption Authentication

Diffie-Hellman Group 31 30 29 28 27 21
 20 19 18 17 16 15
 14 5 2 1

Key Lifetime (seconds)

Local ID

1.6. VPN -> IPsec tunnels > XAUTH

- Type: **Disabled**

XAUTH

Type

1.7. VPN -> IPsec tunnels > Phase 2 Selectors

- Name: **Name for your tunnel (Can be anything)**
- Local Address: **Local Fortigate's network address and subnet mask**
- Remote Address: **Teltonika's router local network address and subnet mask**

Phase 2 Selectors

Name	Local Address	Remote Address
Teltonika-01	10.18.0.0/255.255.255.0	10.36.250.0/255.255.255.0

Edit Phase 2

Name: Teltonika-01

Comments:

Local Address: Subnet | 10.18.0.0/255.255.255.0

Remote Address: Subnet | 10.36.250.0/255.255.25

1.8. VPN -> IPsec tunnels > Phase 2 Selectors > Advanced > Phase 2 Proposal

- Encryption: **3DES**
- Authentication: **SHA1**
- Enable Replay Detection: **Check**
- Enable Perfect Forward Secrecy (PFS): **Check**
- Diffie-Hellman Group: **5**
- Local Port: **All**
- Remote Port: **All**
- Protocol: **All**
- Autokey Keep Alive: **Uncheck**
- Key Lifetime: **Seconds**
- Seconds: 43200

Phase 2 Proposal

Encryption: 3DES | Authentication: SHA1

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group:
 31 30 29 28 27 21
 20 19 18 17 16 15
 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 43200

2. Setting up IPsec on RUT9XX

2.1. Creating an IPsec instance

- Log in to router's Web UI, go to **Services -> VPN -> IPsec**
- Enter any **name** for the instance and hit '**Add**'

IPsec

IPsec Configuration				
Name	Enabled	Mode	Dead Peer Detection	Remote VPN endpoint
There are no IPsec configurations yet				
<input type="text" value="Name"/>				<input type="button" value="Add"/>

- Click **Edit** on the newly created instance.
- Select **Enable**
- IKE version: **IKEv1**
- Mode: **Aggressive**
- Type: **Tunnel**
- My identifier type: **FQDN**
- My identifier: same as **Peer ID** on **Fortigate**
- Local IP address/Subnet mask: **LAN IP** address and **prefix** (for ex. 10.36.250.0/24)
- Select **Left firewall**
- Remote VPN endpoint: **Fortigate's Public IP**
- Remote IP address/Subnet mask: **Local address** and **prefix** set up on Fortigate
- Select **Right firewall**

IPsec Configuration

Enable
 IKE version: IKEv1
 Mode: Aggressive
 Type: Tunnel
 My identifier type: FQDN
 On startup: Start
 My identifier: rut9
 Local IP address/Subnet mask: 10.36.250.0/24
 Left firewall
 Force encapsulation
 Dead Peer Detection
 Remote VPN endpoint: **Fortigate's Public IP**
 Remote IP address/Subnet mask: 10.18.0.0/24
 Right firewall
 Enable keepalive
 Host:
 Ping period (sec):
 Allow WebUI access
 Custom options:

- Phase 1:
 - Encryption algorithm: **3DES**
 - Authentication: **SHA1**
 - DH group: **MODP1536**
 - Lifetime (h): **86400 Seconds**

Phase

The phase must match with another incoming connection to establish IPsec

Phase 1

Phase 2

Encryption algorithm: 3DES
 Authentication: SHA1
 DH group: MODP1536
 Lifetime (h): 86400 Seconds

- Phase 2:
 - Encryption algorithm: **3DES**
 - Hash algorithm: **SHA1**
 - PFS group: **MODP1536**
 - Lifetime (h): **43200 Seconds**

Phase

The phase must match with another incoming connection to establish IPsec

Phase 1 Phase 2

Encryption algorithm 3DES

Hash algorithm SHA1

PFS group MODP1536

Lifetime (h) 43200 Seconds

Back to Overview Save

- Hit **Save**

2.2. Creating a pre-shared key:

- Under **Services** -> **VPN** -> **IPsec**, under **Pre-shared keys** hit **Add**
- Put in the **pre-shared key**. It **has to match** the one you put on **step 1.2**
- Secret's ID selector: **Fortigate's Wan IP (Public IP)**
- Hit **Save**

Pre-shared Keys

Pre-shared key	Secret's ID selector	
hello	Fortigate's WAN ip	Delete

Add

Save

3. Topology



4. Testing the connection

4.1. On the router

- Go to **Services -> CLI**
- Username: **root**
- Password: your **router's password**
- Once logged in, put in **ipsec status** and hit **Enter**
- You should see a **tunnel formed** as in the example below:

```
root@Teltonika:~# ipsec status
Shunted Connections:
passthrough0: 192.168.1.0/24 === 192.168.1.0/24 PASS
Security Associations (1 up, 0 connecting):
tetr[1]: ESTABLISHED 4 seconds ago, 117.2[redacted][rut240]...14.9[redacted][amir]
tetr{1}: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c729fe50_i c48178d8_o
tetr{1}: 192.168.1.0/32 === 10.192.0.254/32
```

4.2. On Fortigate

- You should see a **New Dialup Connection** appear besides your ipsec tunnel instance **VPN – IPsec Tunnels**