

Open VPN manual

1. TLS	2
1.1. Download software	2
1.2. Installing software	2
1.3. Creating certificates	2
1.4. Configure RUT9xx as an OpenVPN Tls server	4
1.5. Configure RUT9xx as an OpenVPN Tls client	7
1.6. Configure Computer as an OpenVPN Tls server.....	9
1.7. Configure Computer as an OpenVPN Tls client.....	10
2. Static key	11
2.1. Configure your computer as a Server	11
2.2 Configure RUT9xx as a Client.	11
2.3 Configure your computer as a client.....	14
2.4 Configure Rut9xx as a server	14
2.5 Connect to server	15

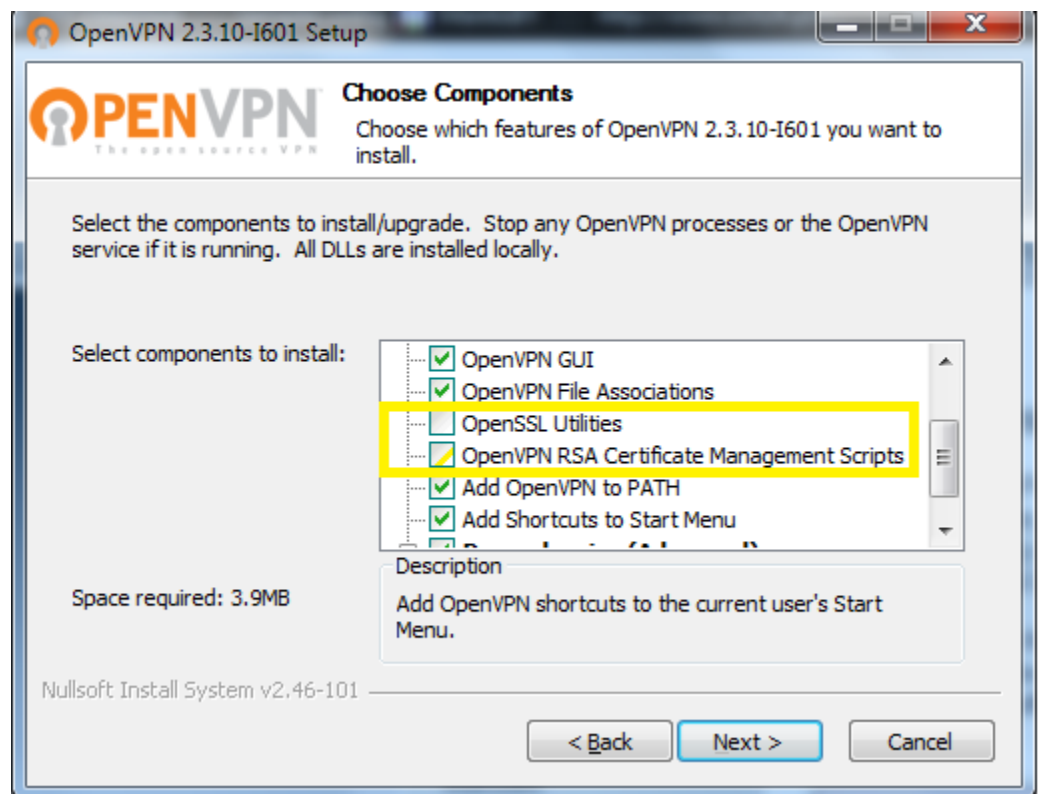
1. TLS

1.1. Download software

- 1.1.1. Download “**OpenVPN windows installer**” 64bit or 32bit software.
(<https://openvpn.net/index.php/open-source/downloads.html>)

1.2. Installing software

- 1.2.1. Press “Next”
- 1.2.2. Press “I Agree”
- 1.2.3. If you want to create certificates using this computer check “OpenSSL Utilities” and “OpenVPN RSA Certificate Management Scripts” checkboxes (should be checked all boxes) otherwise leave default settings .



- 1.2.4. Press “Install” and wait for installation to complete.
- 1.2.5. Press “Next”
- 1.2.6. Press “Finish”

1.3. Creating certificates

- 1.3.1. Open cmd.exe (Start->Run->cmd.exe)
- 1.3.2. If you installed OpenVPN in default folder write
“**cd \Program Files\OpenVPN\easy-rsa**” otherwise use your created file tree.

1.3.3. If you doing it for the first time write command “init-config” it will reset all certificate system. (if you have already created certificates on this computer and if you don’t want to recreate all your certificates skip this step .)

1.3.4. This step is optional (It will help to create certificates easier because you are creating hint for the certificate data). A new file will appear C:\OpenVPN\easy-rsa\vars.bat. Open it with your favorite text editor like notepad and edit these lines: After that save and close vars.bat file.

```
set KEY_COUNTRY= your_text_1
set KEY_PROVINCE= your_text_2
set KEY_CITY= your_text_3
set KEY_ORG= your_text_4
set KEY_EMAIL= your_text_5
```

1.3.5. To build root keys write these commands in cmd.exe: “vars”, “clean-all”, “build-ca”. Now you will be asked to write information (one line at the time) about your certificate:

```
Country Name <2 letter code> [US]:us
State or Province Name <full name> [CA]:ca
Locality Name <eg, city> [SanFrancisco]:san
Organization Name <eg, company> [OpenVPN]:name
Organizational Unit Name <eg, section> [changeme]:name
Common Name <eg, your name or your server's hostname> [changeme]:Unique_name
Name [changeme]:name
Email Address [mail@host.domain]:email@company.com
```

Only “Common Name (eg, your name or your server's hostname) [changeme]:” is important because it must be unique name.

Now you have new file in your C:\OpenVPN\easy-rsa\keys catalog – “ca.crt”

This step should be done once and created file must be used in server and all clients’ settings.

1.3.6. To create server certificate write these commands in cmd.exe: “vars”, “build-key-server server”. Now you will be asked to write information (one line at the time) about your certificate:

```
Country Name <2 letter code> [US]:us
State or Province Name <full name> [CA]:ca
Locality Name <eg, city> [SanFrancisco]:san
Organization Name <eg, company> [OpenVPN]:open
Organizational Unit Name <eg, section> [changeme]:name
Common Name <eg, your name or your server's hostname> [changeme]:Unique_name_2
Name [changeme]:name
Email Address [mail@host.domain]:mail

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:name
```

Only “Common Name (ex. your name or your server's hostname) [changeme]:” (it must be unique) and “A challenge password []” (you’ll have to use it in all clients certificates) are important.

After that you will be asked to agree, press “y” and “enter” two times.

Now you have new files in your C:\OpenVPN\easy-rsa\keys catalog – “server.crt” and “server.key”.

1.3.7. To create Diffie Hellman file write to cmd.exe: “**build-dh**”. Now you have new file in your C:\OpenVPN\easy-rsa\keys catalog – “dh1024.pem” (This is the last file required for server configuration).

1.3.8. To create Client certificate files write to cmd.exe: “vars”, “**build-key <desired unique remote user name>**” (the same user name will be used in certificate data). Now you will be asked to write information (one line at the time) about your certificate:

```
Country Name (2 letter code) [US]:us
State or Province Name (full name) [CA]:ca
Locality Name (eg, city) [SanFrancisco]:sa
Organization Name (eg, company) [OpenVPN]:op
Organizational Unit Name (eg, section) [changeme]:uni
Common Name (eg, your name or your server's hostname) [changeme]:unique
Name [changeme]:name
Email Address [mail@host.domain]:mail

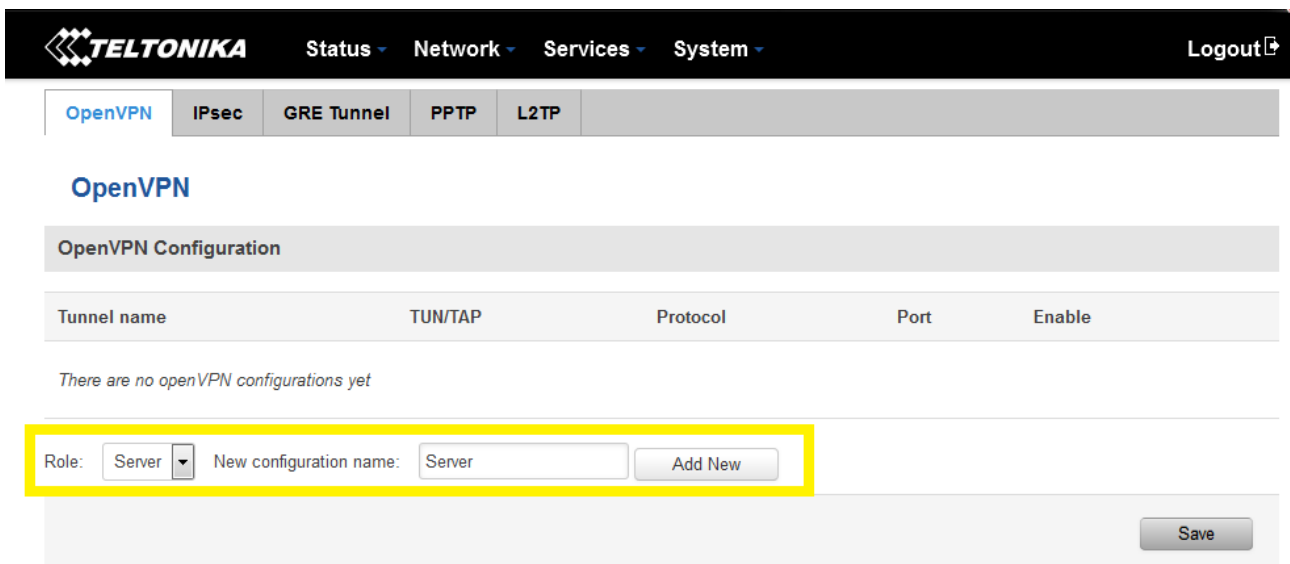
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:name
```

Only “Common Name (eg, your name or your server's hostname) [changeme]:” (it must be unique and the same as in command you entered in cmd.exe <desired unique remote user name>) and “A challenge password []” (you’ll have to use it in all clients certificates) are important. After that you will be asked to agree, press “y” and “enter” two times. Now you have new files in your C:\OpenVPN\easy-rsa\keys catalog – “unique.crt and “unique.key”. (We have named these clients certificates client1.crt and client1.key)

1.4. Configure RUT9xx as an OpenVPN Tls server

1.4.1. Open RUT9xx web GUI and select Services -> VPN -> OpenVPN.

1.4.2. Create new configuration file by selecting role “Server” and typing configuration name which you like. Then press Add New button.



The screenshot shows the TELTONIKA web interface. At the top, there's a navigation bar with 'Status', 'Network', 'Services', and 'System' tabs. The 'Services' tab is active, and the 'OpenVPN' sub-tab is selected. Below the navigation bar, there's a section for 'OpenVPN Configuration'. It contains a table with columns: Tunnel name, TUN/TAP, Protocol, Port, and Enable. Below the table, it says 'There are no openVPN configurations yet'. At the bottom, there's a form to add a new configuration. The 'Role' dropdown is set to 'Server', and the 'New configuration name' field contains 'Server'. The 'Add New' button is highlighted with a yellow box. A 'Save' button is also visible at the bottom right.

1.4.3. After that you will see a line with your tunnel. Press edit button to configure server.

Server_Server	Tun_s_Server	UDP	1194		Edit	Delete
---------------	--------------	-----	------	---	-------------	--------

1.4.4. On the opened page you will see Main Settings. After configuring press save at the bottom of the page.

OpenVPN
IPsec
GRE Tunnel
PPTP
L2TP

OpenVPN Instance: Server_Server

Main Settings

Enable ☒
Check this box if you want to enable OpenVPN service

TUN/TAP TUN (tunnel)

Protocol UDP

Port 1194
Default OpenVPN port

LZO ☒
Check this box if you want to enable data compression (to save data bandwidth)

Encryption BF-CBC 128 (default)

Authentication TLS

TLS cipher All


Client to client ☒
Check if you want that clients could be able to connect to each other
Leave default


Keep alive 10 120


Virtual network IP address 176.16.1.0
Your virtual network IP address.


Virtual network netmask 255.255.255.0

Allow duplicate certificates ☒

Certificate authority Uploaded File (1.33 KB)  ca.crt

Server certificate Uploaded File (3.99 KB)  server.crt

Server key Uploaded File (912.00 B)  server.key

Diffie Hellman parameters Uploaded File (245.00 B)  dh1024.pem

1.4.5. By default everyone who connects to the server will be able to connect to each other by virtual IP address, but if you want to connect to their local IP address you must add client by writing its' name (recommend to write its' unique name, for example PCclient) and pressing "add".

TLS Clients

Here you can add your VPN clients so that they may be reachable from the server.

There are no values created yet

1.4.6. Configure client settings as in picture below and press "save" at the bottom of the page after configuring client settings.

TLS Clients

Here you can add your VPN clients so that they may be reachable from the server.

PCclient

VPN instance name

Endpoint name

Common name (CN)

Virtual local endpoint

Virtual remote endpoint

Private network

Private netmask

Leave default

Write name of your computer (not important)

Client's unique name as in certificate (important)

You should write IP address which client should obtain. Use IP address combinations from table below this picture

Write this client's subnet address with zero in the end

Use this Netmask

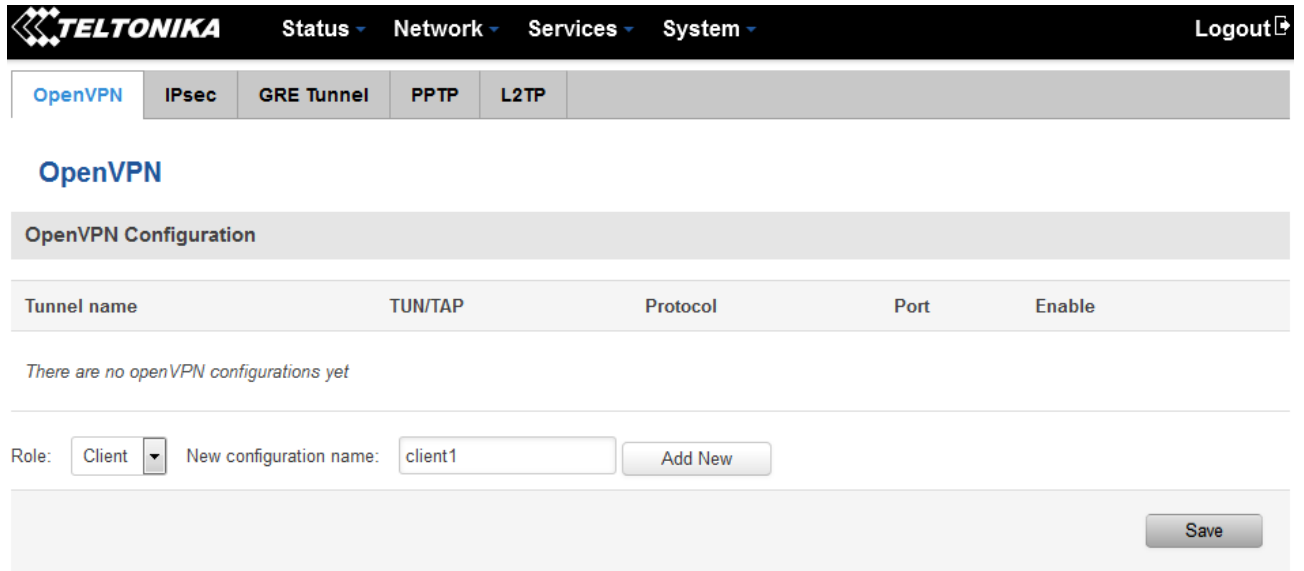
You have to choose virtual local/endpoint from these paired IP endings.

[1, 2]	[5, 6]	[9, 10]	[13, 14]	[17, 18]
[21, 22]	[25, 26]	[29, 30]	[33, 34]	[37, 38]
[41, 42]	[45, 46]	[49, 50]	[53, 54]	[57, 58]
[61, 62]	[65, 66]	[69, 70]	[73, 74]	[77, 78]
[81, 82]	[85, 86]	[89, 90]	[93, 94]	[97, 98]
[101,102]	[105,106]	[109,110]	[113,114]	[117,118]
[121,122]	[125,126]	[129,130]	[133,134]	[137,138]
[141,142]	[145,146]	[149,150]	[153,154]	[157,158]
[161,162]	[165,166]	[169,170]	[173,174]	[177,178]
[181,182]	[185,186]	[189,190]	[193,194]	[197,198]
[201,202]	[205,206]	[209,210]	[213,214]	[217,218]
[221,222]	[225,226]	[229,230]	[233,234]	[237,238]
[241,242]	[245,246]	[249,250]	[253,254]	

1.5. Configure RUT9xx as an OpenVPN Tls client

1.5.1. Open RUT9xx web GUI and select Services -> VPN -> OpenVPN.

1.5.2. Create new configuration file by selecting role “**client**” and typing configuration name (we recommend to write same unique name as in certificate (CN)). Then press Add New button.



TELTONIKA Status Network Services System Logout

OpenVPN IPsec GRE Tunnel PPTP L2TP

OpenVPN

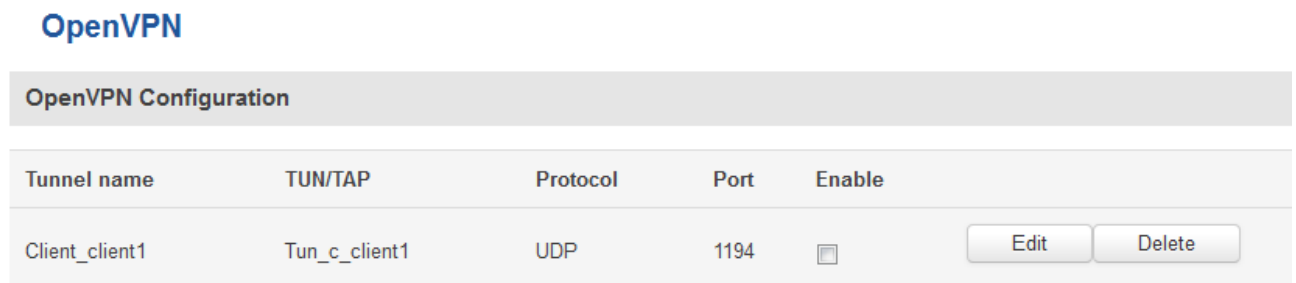
OpenVPN Configuration

Tunnel name	TUN/TAP	Protocol	Port	Enable
There are no openVPN configurations yet				

Role: Client New configuration name: client1 Add New

Save

1.5.3. Now press “**edit**” button.




OpenVPN

OpenVPN Configuration

Tunnel name	TUN/TAP	Protocol	Port	Enable
Client_client1	Tun_c_client1	UDP	1194	<input type="checkbox"/>

Edit Delete

1.5.4. Fill forms as in example and press save.


Status Network Services System Logout

OpenVPN IPsec GRE Tunnel PPTP L2TP

OpenVPN Instance: Client_RUT9xx

Main Settings

Enable ☒
Check if you want to enable this client

TUN/TAP TUN (tunnel)

Protocol UDP

Port 1194
Leave to default or change to your server port

LZO ☒
Check if it is enabled in server

Encryption BF-CBC 128 (default)

Authentication TLS

TLS cipher All

Remote host/IP address 84.15.184.154
Write server IP address

Resolve retry Infinite
Leave default

Keep alive 10 120
Write "10 120"

Remote network IP address 192.168.50.0

Remote network IP netmask 255.255.255.0

Max routes 100

HMAC authentication ☐

Certificate authority Browse... ca.crt

Client certificate Browse... client1.crt

Client key Browse... client1.key

Back to Overview Save

1.6. Configure Computer as an OpenVPN Tls server

1.6.1. In “C:\Program Files\OpenVPN\config” create file “server.ovpn” which contains these settings:

```
## server.ovpn ##
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig 10.8.0.0 255.255.255.0
route 192.168.1.0 255.255.255.0
client-config-dir " C:\Program Files\OpenVPN\config\ccd"
ifconfig-pool-persist ipp.txt
status openvpn-status.log
comp-lzo
keepalive 10 120
persist-key
persist-tun
verb 5
```

Firstly choose your server virtual IP address “10.x.0.0” default is 10.8.0.0, then decide whether you need or not need to use data compression. If you need it leave “comp-lzo” if don’t - delete it.

1.6.2. In 1.6.1. settings you can see four names highlighted in green. These files should be copied in “C:\Program Files\OpenVPN\config” (the same folder as server config file).

1.6.3. Create folder “ccd” in directory in “C:\Program Files\OpenVPN\config\ccd”. In this folder create file with unique client name for example: “unique” (the same name as used for client certificate). In this example we use name “client1”. This file “client1” contains these settings:

```
ifconfig-push 10.8.0.9 10.8.0.10 #push routes prom IP pair table (first IP is to self, second - for client).
iroute 192.168.1.0 255.255.255.0 #example if client's network is .1.0/24
```

1.7. Configure Computer as an OpenVPN Tls client

In “C:\Program Files\OpenVPN\config” create file “unique.opvn” which contains these settings:

```
##remote.ovpn##
client
dev tun
proto udp
remote 84.150.123.101
resolv-retry infinite
nobind
route 192.168.1.0 255.255.255.0
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
comp-lzo
```

In line starting with “**remote**” write your server IP address and port (port is usually default 1194).

“**Route**” – this is RUT9xx (OpenVPN server) LAN subnet.

Files with name highlighted in green should be placed in “C:\Program Files\OpenVPN\config” (the same folder as client config file).

After that open application “**OpenVPN GUI**”. It should be already installed in your computer as bundle of “**OpenVPN windows installer**”. Then you will see this “



” two computers with red displays. Press on it with right mouse button and select “**Connect**”.

2. Static key

2.1. Configure your computer as a Server

2.1.1. Start “Generate a static OpenVPN key” shortcut and press enter. Then check your “C:\Program Files\OpenVPN\config” folder for new file key.txt.

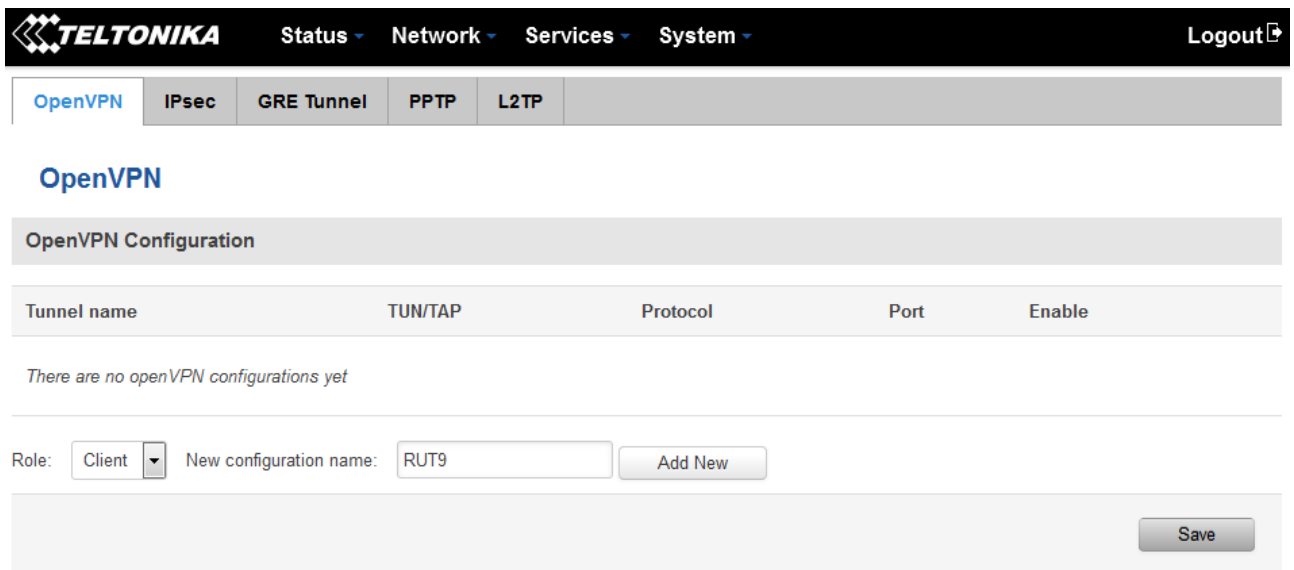
2.1.2. Open “C:\Program Files\OpenVPN\config” and create file “static.ovpn” with content as in example:

```
#server
port 1194
proto udp
dev tun
secret static.key
ifconfig 172.16.0.1 172.16.0.2
comp-lzo
route 192.168.1.0 255.255.255.0
keepalive 10 120
persist-key
persist-tun
resolv-retry infinite
verb 5
```

2.2 Configure RUT9xx as a Client.

2.2.1 Open RUT9xx web GUI and select Services -> VPN -> OpenVPN

2.2.2 Create new configuration file by selecting role “Client” and typing configuration name which you like. Then press Add New button



TELTONIKA Status Network Services System Logout

OpenVPN IPsec GRE Tunnel PPTP L2TP

OpenVPN

OpenVPN Configuration


Tunnel name	TUN/TAP	Protocol	Port	Enable
There are no openVPN configurations yet				

Role: Client New configuration name: RUT9 Add New Save

2.2.3 After that you will see a line with your tunnel. Press edit button to configure server.

OpenVPN Configuration					
Tunnel name	TUN/TAP	Protocol	Port	Enable	
Client_RUT9	Tun_c_RUT9	UDP	1194	<input checked="" type="checkbox"/>	Edit Delete

2.2.4 Fill forms as in example and press save.


Status ▾ Network ▾ Services ▾ System ▾
Logout

[OpenVPN](#)
[IPsec](#)
[GRE Tunnel](#)
[PPTP](#)
[L2TP](#)

OpenVPN Instance: Client_RUT9

Main Settings

Enable ☒

TUN/TAP

TUN (tunnel) ▾

Protocol

UDP ▾

Port

1194

LZO ☒

Encryption

BF-CBC 128 (default) ▾

Authentication

Static key ▾

Remote host/IP address

84.15. XX.YY

Resolve retry

Infinite

Keep alive

10 120

Local tunnel endpoint IP

172.16.0.2

Remote tunnel endpoint IP

172.16.0.1

Remote network IP address

192.168.50.0


Remote network IP netmask

255.255.255.0

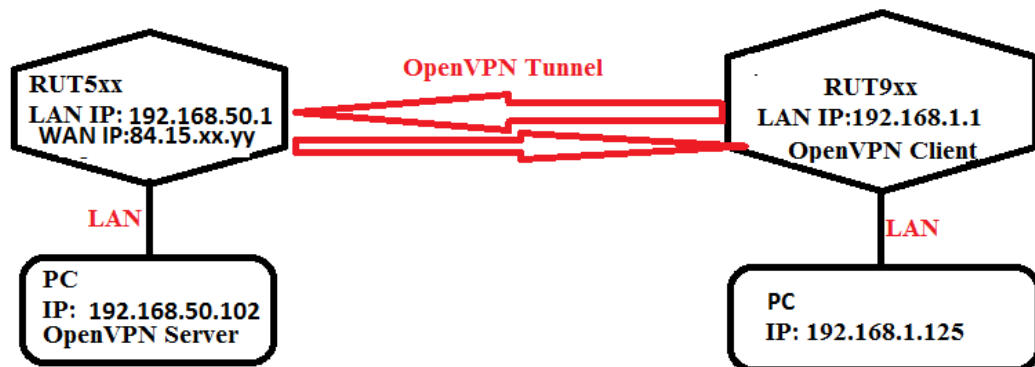
Max routes

100

Static pre-shared key

Uploaded File (636.00 B) 


2.2.5 Network topology of this example:



2.2.6 Port forwarding rule in router RUT5xx for OpenVPN

vpn	TCP, UDP	From <i>any host</i> in <i>wan</i>	To <i>any router IP</i> at port <i>1194</i>	Forward to IP <i>192.168.50.102</i> , port <i>1194</i> in <i>lan</i>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
-----	-------------	---------------------------------------	--	---	-------------------------------------	-------------------------------------	---------------------------------------

2.2.7 After that open application “OpenVPN GUI”. It should be already installed in your computer as bundle of “OpenVPN windows installer”. Then you will see this “

 10:00
2013.04.24” two computers with red displays. Press on it with right mouse button and select “Connect”.

2.3 Configure your computer as a client

2.3.1 Start “**Generate a static OpenVPN key**” shortcut and press enter. Then check your “C:\Program Files\OpenVPN\config” folder for new file key.txt.

2.3.2 Open “C:\Program Files\OpenVPN\config” and create file “**static.ovpn**” with content as in example:

```
remote 84.15.xx.yy
verb 5
proto udp
dev tun
comp-lzo
ifconfig 172.16.0.2 172.16.0.1
route 192.168.1.0 255.255.255.0
secret static.key
keepalive 10 120
persist-key
persist-tun
```

2.3.2.1 In line remote write your server IP address.

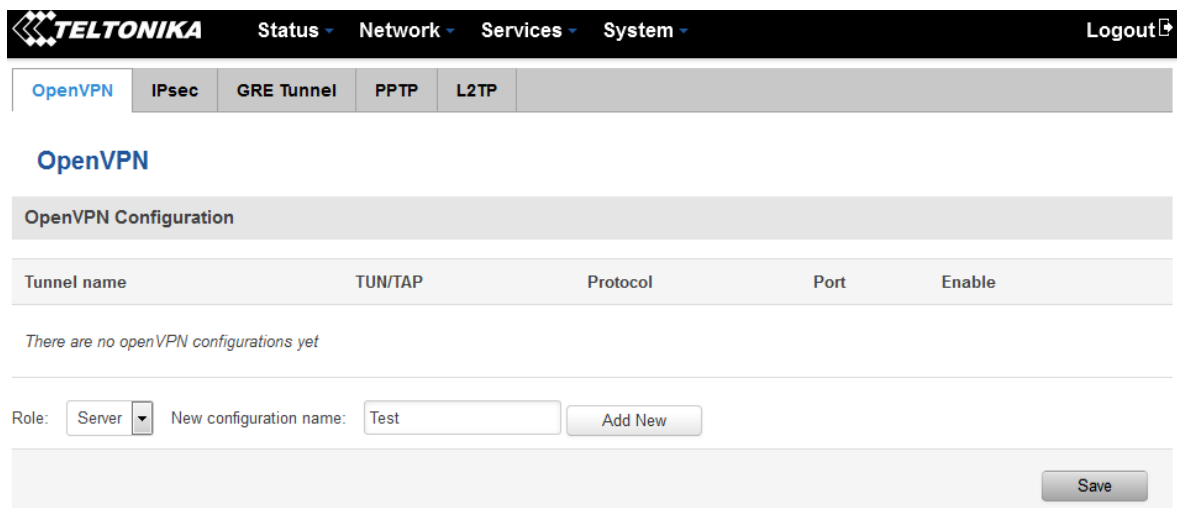
2.3.2.2 In line ifconfig write your virtual remote and local IP address as in example in 1.4.6 item.

2.3.2.3 The last line is the name of your static OpenVPN key, which you generated and have (it should stay here) in “C:\Program Files\OpenVPN\config” folder.

2.4 Configure Rut9xx as a server



2.4.2 Open RUT9xx web GUI and select services -> OpenVPN

2.4.3 Create new configuration file by selecting role “**server**” and typing configuration name which you like. Then press Add New button.



2.4.4 After that you will see a line with your tunnel. Press edit button to configure server.

Tunnel name	TUN/TAP	Protocol	Port	Enable	
Server_Test	Tun_s_Test	UDP	1194	<input checked="" type="checkbox"/>	Edit Delete


Status ▾ Network ▾ Services ▾ System ▾
Logout 

[OpenVPN](#)
[IPsec](#)
[GRE Tunnel](#)
[PPTP](#)
[L2TP](#)

OpenVPN Instance: Server_Test

Main Settings

Enable ☒ Check this box if you want to start OpenVPN

TUN/TAP TUN (tunnel) ▾

Protocol UDP ▾

Port 1194

LZO ☒ Check if you want to compress data

Encryption BF-CBC 128 (default) ▾


Authentication Static key ▾ Choose Static key

Local tunnel endpoint IP 172.16.0.1 Choose local and remote IP as in Client configuration

Remote tunnel endpoint IP 172.16.0.2

Remote network IP address 192.168.50.0 Client IP address

Remote network netmask 255.255.255.0 Client netmask

Static pre-shared key Uploaded File (636.00 B)  Upload generated key

[Back to Overview](#)
[Save](#)

2.5 Connect to server

2.5.2 After that open application “**OpenVPN GUI**”. It should be already installed in your computer as bundle of “**OpenVPN windows installer**”. Then you will see this “



” two computers with red displays. Press on it with right mouse button and select “**Connect**”.