Open VPN manual

1. TLS client to client

1.1. Download software

1.1.1. Download "**OpenVPN windows installer**" 64bit or 32bit software.
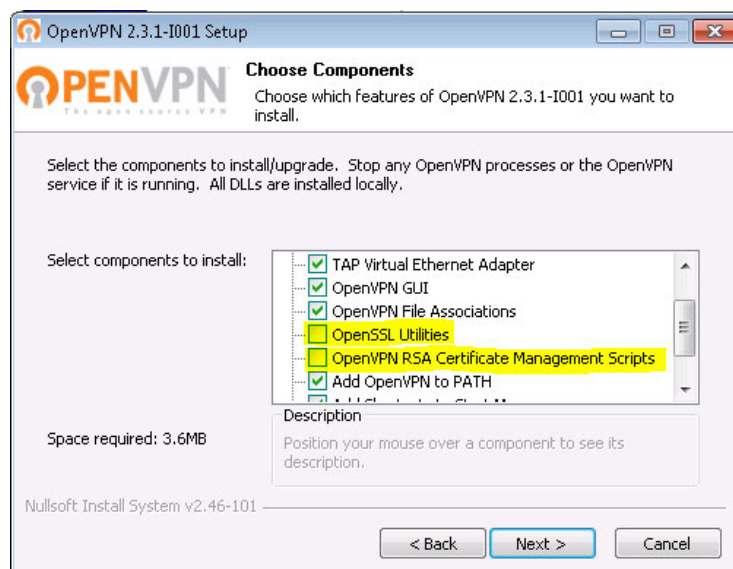(http://openvpn.net/index.php/open-source/downloads.html)

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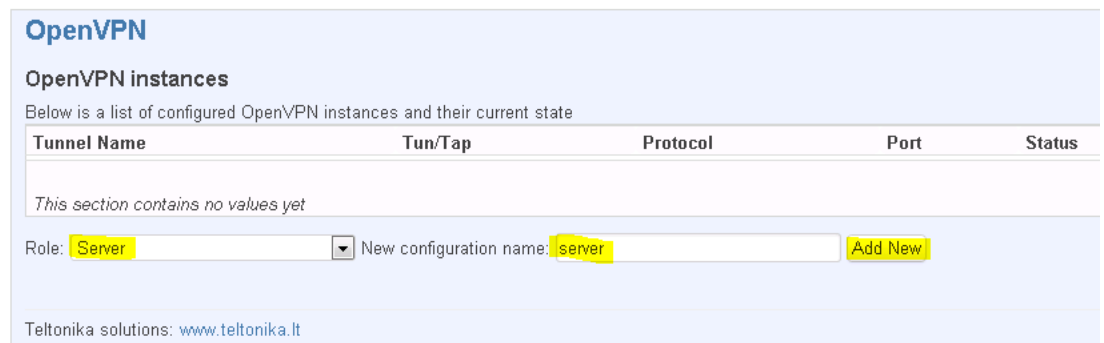
```
Country Name (2 letter code) [US]:us
State or Province Name (full name) [CA]:ca
Locality Name (eg, city) [SanFrancisco]:sa
Organization Name (eg, company) [OpenVPN]:op
Organizational Unit Name (eg, section) [changeme]:uni
Common Name (eg, your name or your server's hostname) [changeme]:unique
Name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

1.4. Configure RUT-500 as an OpenVPN Tls server

1.4.1. Open RUT500 web GUI and select services -> OpenVPN

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

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Tunnel Name	Tun/Tap	Protocol	Port	Status

This section contains no values yet

Role: Server ▼   New configuration name: server   Add New

Teltonika solutions: www.teltonika.lt

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

server_server	TUN	UDP	1194	Disabled	Edit Delete

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

Main settings

Enable	☑ Check this box if you want to enable OpenVPN service
Port	1194 Default OpenVPN port
	❓ TCP/UDP port for both, local and remote
LZO	☑ ❓ Use fast LZO compression Check this box if you want to enable data compresion (to save data bandwidth)
Authentication	Tls ▼ Choose Tls for multiple clients
Client to client	☑ ❓ Allow client-to-client traffic Check this box if you want that clients could be able to connect to each other
Keep alive	10 120 Leave default
	❓ Helper directive to simplify the expression of --ping and --ping-restart in server mod
Virtual network IP address	10.8.0.0 Your virtual network ip adress. You can change only second value 10.x.0.0
Virtual network netmask	255.255.255.0 use 255.255.255.0 network netmask
Certificate authority	Pasirinkti failą ca.crt
Server certificate	Pasirinkti failą server.crt In each upload box, choose to upload files
Server key	Pasirinkti failą server.key as in example from your C:\Program Files\OpenVPN\easy-rsa\keys catalog.
Diffie Hellman parameters	Pasirinkti failą 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) and pressing "add".

TLS Clients

Here you can add your VPN clients so that they may be reachable from the server.
This section contains no values yet

unique   Add

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

unique

VPN Instance name	server_server	Leave default
	With what openVPN Instance should this entry be associated wit	
Endpoint Name	Name	Write name of your computer (not important)
	Your endpoint name. E.g.: "MyHomeComputer"	
Common Name (CN)	unique	Clients' unique name as in certificate (important)
	Client certificate CN field. E.g.: " name.surname@domain.com"	
Virtual Local Endpoint	10.8.0.6	You should write ip adress which client should
	E.g.: "10.8.1.10"	obtain. Use ip adress
Virtual Remote Endpoint	10.8.0.5	combinations from table
	E.g.: "10.8.1.9"	bellow this picture.
Private Network	192.168.5.0	Write this clients' subnet adress with zero in the end.
	The IP of the private **NETWORK**. E.g.: "192.168.1.0"	
Private Netmask	255.255.255.0	Use this Netmask
	The Netmask of the private network. E.g.: "255.255.255.0"	

Delete

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 RUT-500 as an OpenVPN Tls client

1.5.1. Open RUT500 web GUI and select services -> 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.

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Tunnel Name	Tun/Tap	Protocol	Port	Status
This section contains no values yet				

Role: Client   New configuration name: config   Add New

1.5.3. Now press "**edit**" button.

New OpenVPN instance created successfully, configure it

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Tunnel Name	Tun/Tap	Protocol	Port	Status	
client_config	TUN	UDP	1194	Disabled	Edit Delete

Role: Client   New configuration name: Add New

1.5.4. Fill forms as in example and press save.

OpenVPN instance: client_config

Main settings

Enable ☑ check if you want to enable this client

Port 1194   Leave to default or change to your server port
② TCP/UDP port for both, local and remote

LZO ☑ ② Use fast LZO compression   Check if it is enabled in server

Authentication Tls   Use Tls

Remote host/IP address 192.168.99.151   Write server ip adress

Resolve Retry infinite   Leave default

Keep alive 10 120   write "10 120"
② Helper directive to simplify the expression of --ping and --ping-restart

Certificate authority Pasirinkti failą ca.crt   Upload certificates according to names in example from key folder

Client certificate Pasirinkti failą unique.crt   (where your certificates were generated). Upload client certificates

Client key Pasirinkti failą unique.key   according to client name.

1.6. Configure Computer as an OpenVPN Tls server

1.6.1. In "**C:\Program Files\OpenVPN\config**" create file "**server.opvn**" 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-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

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. To create client with static virtual ip, create file with unique client name for example: "**unique**" and put content in it as in this example:

```
ifconfig-push 10.8.0.10 10.8.0.9
iroute 192.168.2.0 255.255.255.0
push route 192.168.99.0 255.255.255.0
push route 192.168.3.0 255.255.255.0
```

1.6.3.1. In the first line write virtual local and endpoint address as in 1.4.6 example.

1.6.3.2. In the second line write this client (which you are configuring now) subnet address and mask address.

1.6.3.3. In the third line write **server** subnet address with mask address

1.6.3.4. In the fourth and other lines write other clients subnet addresses and mask addresses (if you want enable client to connect to these clients subnets), for example: If you have server with subnet 192.168.2.0 and three clients which have subnets like: 192.168.3.0, 192.168.4.0, 192.168.5.0. You configuring client with 192.168.3.0 and want to give him 10.8.0.150 virtual address your configure should look like this:

```
ifconfig-push 10.8.0.150 10.8.0.149
iroute 192.168.3.0 255.255.255.0
push route 192.168.2.0 255.255.255.0
push route 192.168.4.0 255.255.255.0
push route 192.168.5.0 255.255.255.0
```

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 192.168.99.151 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert unique.crt

key unique.key

comp-lzo

verb 3

route-delay
```

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

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 client

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:

```
remote 192.168.99.156

verb 3

proto udp

dev tun

ifconfig 10.8.0.6 10.8.0.5

route 192.168.1.0 255.255.255.0
10.8.0.5

key.txt

persist-key

persist-tun
```
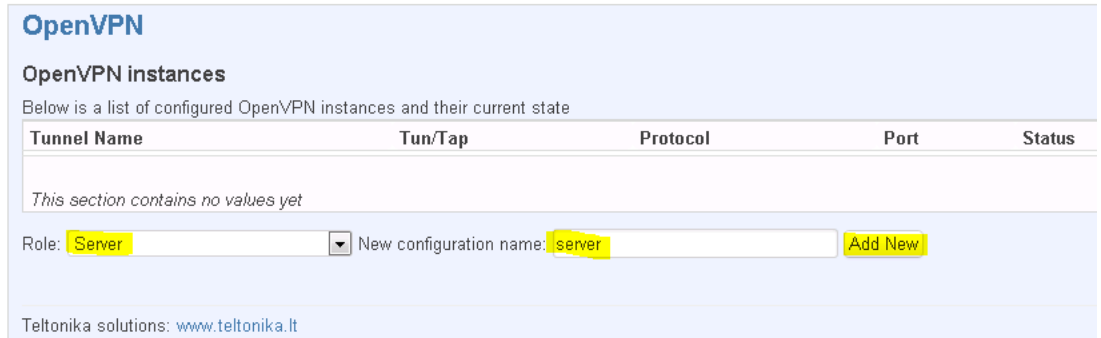
2.1.2.1. In line remote write your server IP address.

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

2.1.2.3. 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.
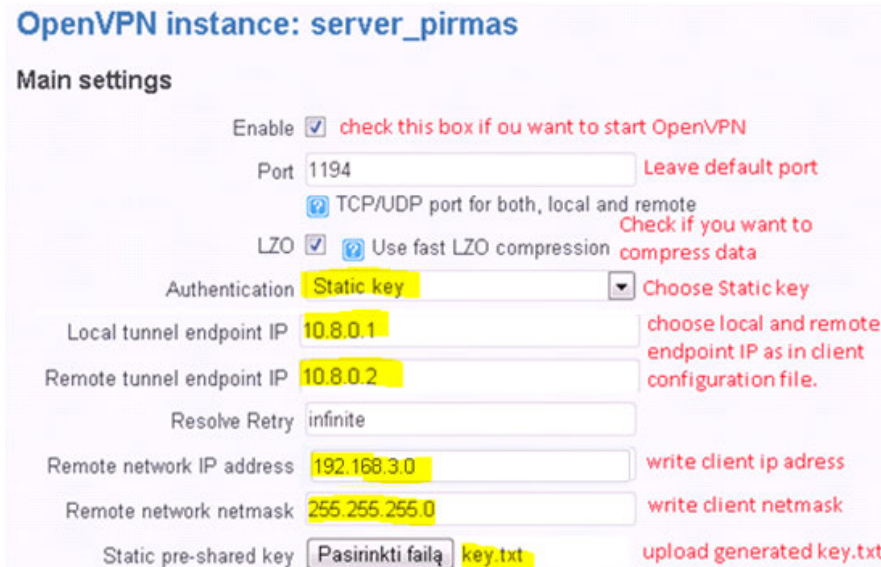
2.2. Configure Rut500 as a server

2.2.1. Open RUT500 web GUI and select services -> OpenVPN

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

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Tunnel Name	Tun/Tap	Protocol	Port	Status

This section contains no values yet

Role: Server ▼ New configuration name: server   Add New

Teltonika solutions: www.teltonika.lt

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

server_server	TUN	UDP	1194	Disabled	Edit Delete

OpenVPN instance: server_pirmas

Main settings

Enable ☑	check this box if ou want to start OpenVPN
Port 1194	Leave default port
ℹ TCP/UDP port for both, local and remote	
LZO ☑ ℹ Use fast LZO compression	Check if you want to compress data
Authentication Static key ▼	Choose Static key
Local tunnel endpoint IP 10.8.0.1	choose local and remote endpoint IP as in client configuration file.
Remote tunnel endpoint IP 10.8.0.2	
Resolve Retry infinite	
Remote network IP address 192.168.3.0	write client ip adress
Remote network netmask 255.255.255.0	write client netmask
Static pre-shared key [Pasirinkti failą] key.txt	upload generated key.txt

2.3. Connect to server

2.3.1. 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 "
![taskbar icon 10:00 2013.04.24]" two computers with red displays. Press on it with right mouse button and select "**Connect**".