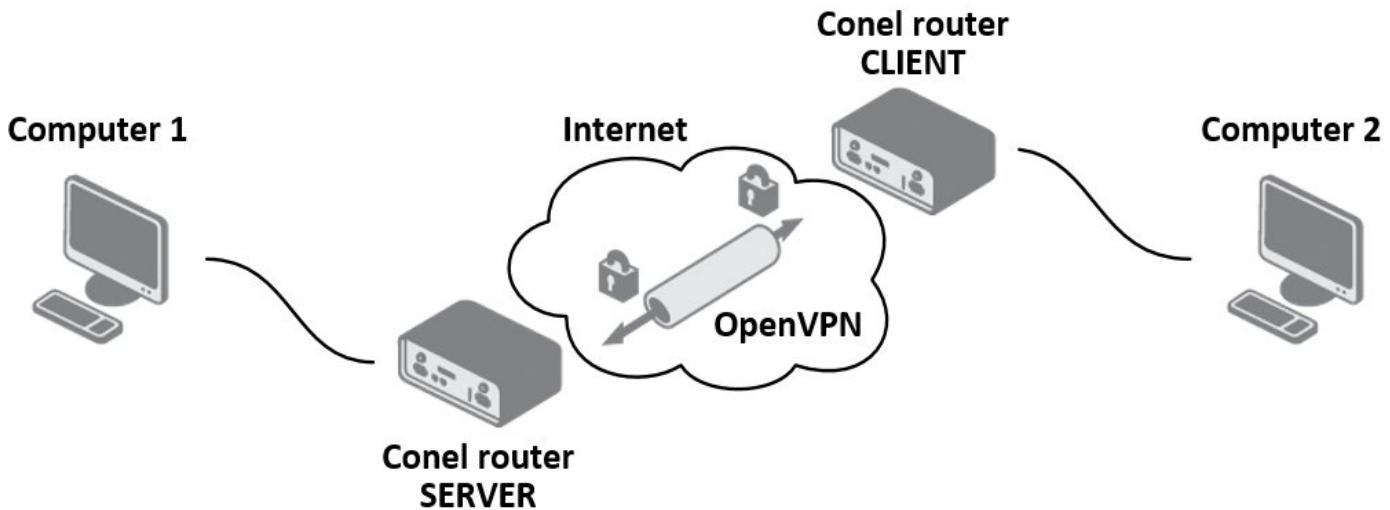


# OpenVPN protocol

Modified on: Thu, 14 Aug, 2014 at 2:29 AM

OpenVPN (Open Virtual Private Network) is a means of interconnection of several computers through an untrusted public network. It is easily possible to reach a situation where connected computers are able to communicate with each other as if they were connected in a single closed private network (this network is consequently trusted). Using client-server architecture, OpenVPN is capable of ensuring a direct connection between computers behind NAT without any need to configure NAT. It has a few ways to authenticate clients – using a pre-shared key, a certificate or a username and password.

OpenVPN uses the officially assigned port 1194, which is applied as a default in newer versions. It offers two types of network interfaces (Universal TUN and TAP driver), which enable creation of an IP tunnel (TUN) on the third layer of the ISO/OSI or on the second layer (layer-2 Ethernet TAP), which is able to transmit any type of data. OpenVPN uses a common network protocols (TCP and UDP) and thus creates an alternative to IPsec protocol.



## Restrictions in Conel routers

- Routers allow to create only two OpenVPN tunnels simultaneously
- Routers only support TUN adapter
- Routers can not be used as a multiclient server

# Configuration of OpenVPN tunnel

Modified on: Fri, 28 Feb, 2014 at 10:05 AM

OpenVPN tunnel allows protected connection of two networks LAN to the one which looks like one homogenous. OpenVPN tunnel configuration can be invoked by pressing *OpenVPN* item in the menu of router web interface. In the *OpenVPN Tunnels Configuration* window are two rows, each row for one configured OpenVPN tunnel. The meaning of individual items is described in the following table:

Item	Description
Create	Enables the individual tunnels
Description	Displays tunnel name (or description) specified in configuration form (of this tunnel)
Edit	OpenVPN tunnel configuration

The screenshot shows a web-based configuration interface titled "OpenVPN Tunnels Configuration". It features a header bar with "Create" and "Description" buttons. Below this are two rows for tunnel configuration. Each row contains a dropdown menu set to "no", an empty text input field, and an "Edit" button. At the bottom of the window is a blue "Apply" button.

After pressing the *Edit* button at one of the tunnels, it will be open a window with a form that can be used to configure the OpenVPN tunel. Individual items have the following meanings:

Item	Description
Description	Description (or name) of tunnel
Protocol	Communication protocol: <ul style="list-style-type: none"><li>• UDP – OpenVPN will communicate using UDP</li><li>• TCP server – OpenVPN will communicate using TCP in server mode</li><li>• TCP client – OpenVPN will communicate using TCP in client mode</li></ul>
UDP/TCP port	Port of the relevant protocol (UDP or TCP)
Remote IP Address	IP address of opposite tunnel side (domain name can be used)
Remote Subnet	IP address of a network behind opposite tunnel side
Remote Subnet Mask	Subnet mask of a network behind opposite tunnel side
Redirect Gateway	Allows to redirect all traffic on Ethernet
Local Interface IP Address	Defines the IP address of a local interface
Remote Interface IP Address	Defines the IP address of the interface of opposite tunnel side
	Defines the time interval after which sends a message to opposite side of tunnel for checking

Ping Interval	the existence of the tunnel.
Ping Timeout	Defines the time interval during which the router waits for a message sent by the opposite side. For proper verification of OpenVPN tunnel, <i>Ping Timeout</i> must be greater than <i>Ping Interval</i> .
Renegotiate Interval	Sets renegotiate period (reauthorization) of the OpenVPN tunnel. This parameter can be set only when <i>Authenticate Mode</i> is set to <i>username/password</i> or <i>X.509 certificate</i> . After this time period, router changes the tunnel encryption to ensure the continues safety of the tunnel.
Max Fragment Size	Defines the maximum size of a sent packet
Compression	<p>Sent data can be compressed:</p> <ul style="list-style-type: none"> <li>• none – no compression is used</li> <li>• LZO – a lossless compression is used (must be set on both sides of the tunnel!)</li> </ul>
NAT Rules	<p>Applies NAT rules to the OpenVPN tunnel:</p> <ul style="list-style-type: none"> <li>• applied – NAT rules are applied to the OpenVPN tunnel</li> <li>• not applied – NAT rules are not applied to the OpenVPN tunnel</li> </ul>
Authenticate Mode	<p>Sets authentication mode:</p> <ul style="list-style-type: none"> <li>• none – no authentication is set</li> <li>• Pre-shared secret – sets the shared key for both sides of the tunnel</li> <li>• Username/password – enables authentication using <i>CA Certificate</i>, <i>Username</i> and <i>Password</i>.</li> <li>• X.509 Certificate (multiclient) – enables X.509 authentication in multiclient mode</li> <li>• X.509 Certificate (client) – enables X.509 authentication in client mode</li> <li>• X.509 Certificate (server) – enables X.509 authentication in server mode</li> </ul>
Pre-shared Secret	Authentication using pre-shared secret can be used for all offered authentication mode.
CA Certificate	Auth. using CA Certificate can be used for <i>username/password</i> and <i>X.509 Certificate</i> modes.
DH Parameters	Protocol for exchange key DH parameters can be used for X.509 Certificate authentication in server mode.
Local Certificate	This authentication certificate can be used for X.509 Certificate authentication mode.
Local Private Key	It can be used for X.509 Certificate authentication mode.
Username	Authentication using a login name and password authentication can be used for <i>username/password</i> mode.
Password	Authentication using a login name and password authentication can be used for <i>username/password</i> mode.
Extra Options	Allows to define additional parameters of OpenVPN tunnel such as DHCP options etc.

The changes in settings will be applied after pressing the *Apply* button.

Tips for working with the configuration form:

- CLIENT routers must have filled in *Remote IP Address* item (IP serveru).
- For SERVER routers we recommend not to fill in *Remote IP Address* item!
- If two routers are situated against each other, one of them is CLIENT and the other is SERVER.
- **It is always recommended to set *Ping Interval* and *Ping Timeout* items.**

**OpenVPN Tunnel Configuration** Create 1st OpenVPN tunnel

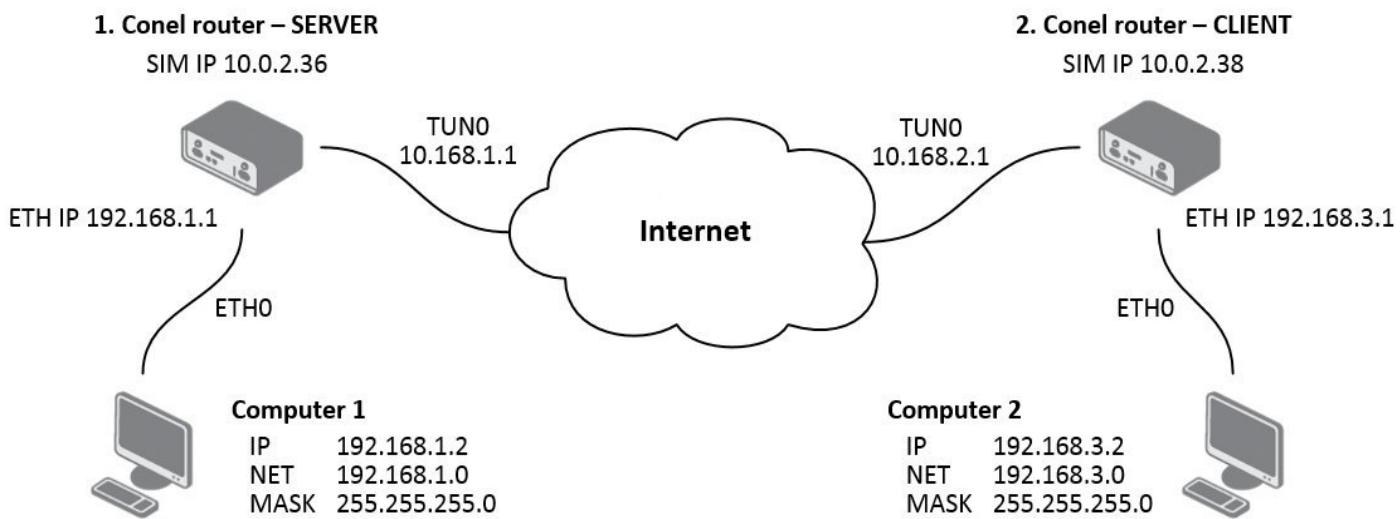
Description *	<input type="text"/>
Protocol	UDP <input type="button" value="▼"/>
UDP port	1194 <input type="button" value="▼"/>
Remote IP Address *	<input type="text"/>
Remote Subnet *	<input type="text"/>
Remote Subnet Mask *	<input type="text"/>
Redirect Gateway	no <input type="button" value="▼"/>
Local Interface IP Address	<input type="text"/>
Remote Interface IP Address	<input type="text"/>
Ping Interval *	<input type="text"/> sec
Ping Timeout *	<input type="text"/> sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO <input type="button" value="▼"/>
NAT Rules	not applied <input type="button" value="▼"/>
Authenticate Mode	none <input type="button" value="▼"/>
Pre-shared Secret	<input type="text"/>
CA Certificate	<input type="text"/>
DH Parameters	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Extra Options *	<input type="text"/>

\* can be blank

## Router on both sides of tunnel

Modified on: Fri, 28 Feb, 2014 at 11:29 AM

The figure below shows a situation where the Conel router is situated on both sides of OpenVPN tunnel. IP address of SIM cards in the router can be static or dynamic.



## OpenVPN tunnel without authentication

Configuration of the first router – SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2

Configuration of the second router – CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1

### OpenVPN Tunnel Configuration

Create 1st OpenVPN tunnel

Description *	<input type="text"/>
Protocol	UDP <input type="button" value="▼"/>
UDP Port	1194 <input type="text"/>
Remote IP Address *	<input type="text"/>
Remote Subnet *	192.168.3.0 <input type="text"/>
Remote Subnet Mask *	255.255.255.0 <input type="text"/>
Redirect Gateway	no <input type="button" value="▼"/>
Local Interface IP Address	10.168.1.1 <input type="text"/>
Remote Interface IP Address	10.168.1.2 <input type="text"/>
Ping Interval *	10 <input type="text"/> sec
Ping Timeout *	30 <input type="text"/> sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO <input type="button" value="▼"/>
NAT Rules	not applied <input type="button" value="▼"/>
Authenticate Mode	none <input type="button" value="▼"/>
Pre-shared Secret	<input type="text"/>
CA Certificate	<input type="text"/>
DH Parameters	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Extra Options *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Note: Configuration of the second router is similar, the difference is only in items listed in table *Configuration of the second router – CLIENT*. If *NAT Rules* parameter is enabled, specified rules (in the configuration form of NAT) are applied to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, an interface tun0 and a route in the routing table of the router are displayed on the *Network Status* page.

**Network Status****Interfaces**

```

eth0      Link encap:Ethernet HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234 Bcast:192.168.2.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB) TX bytes:277877 (271.3 KB)
          Interrupt:23

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

tun0     Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102 P-t-P:172.16.0.101 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

```

**Route Table**

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.2.27	0.0.0.0	UG	0	0	0	eth0
10.0.1.17	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.0	172.16.0.101	255.255.0.0	UG	0	0	0	tun0
172.16.0.1	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.101	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.2.27	0.0.0.0	255.255.255.255	UH	0	0	0	eth0

It is also possible to check successful establishment of OpenVPN tunnel in the system log (*System Log* item in menu). Listings should end with line *Initialization Sequence Completed*.

**System Log****System Messages**

```

2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed

```

**OpenVPN tunnel with pre-shared secret authentication**

Configuration of the first router – SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0

Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2
Authenticate Mode	pre-shared secret
Pre-shared Secret	shared key for both of routers

Configuration of the second router – CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1
Authenticate Mode	pre-shared secret
Local Interface IP Address	shared key for both of routers

The procedure of creating pre-shared key is described in article *Creation of pre-shared key*.

### OpenVPN Tunnel Configuration

Create 1st OpenVPN tunnel

Description *	<input type="text"/>
Protocol	UDP <input type="button" value="▼"/>
UDP Port	1194 <input type="text"/>
Remote IP Address *	<input type="text"/>
Remote Subnet *	192.168.3.0 <input type="text"/>
Remote Subnet Mask *	255.255.255.0 <input type="text"/>
Redirect Gateway	no <input type="button" value="▼"/>
Local Interface IP Address	10.168.1.1 <input type="text"/>
Remote Interface IP Address	10.168.1.2 <input type="text"/>
Ping Interval *	10 <input type="text"/> sec
Ping Timeout *	30 <input type="text"/> sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO <input type="button" value="▼"/>
NAT Rules	not applied <input type="button" value="▼"/>
Authenticate Mode	pre-shared secret <input type="button" value="▼"/>
Pre-shared Secret	<pre># # 2048 bit OpenVPN static key #</pre>
CA Certificate	<input type="text"/>
DH Parameters	<input type="text"/>
Local Certificate	<input type="text"/>
Local Private Key	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Extra Options *	<input type="text"/>
* can be blank	
<input type="button" value="Apply"/>	

Note: Configuration of the second router is similar, the difference is only in items listed in table *Configuration of the second router – CLIENT*. If *NAT Rules* parameter is enabled, specified rules (in the configuration form of NAT) are applied to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, an interface tun0 and a route in the routing table of the router are displayed on the *Network Status* page.

**Network Status****Interfaces**

```

eth0      Link encap:Ethernet HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234 Brdcast:192.168.2.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB) TX bytes:277877 (271.3 KB)
          Interrupt:23

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

tun0     Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102 P-t-P:172.16.0.101 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

```

**Route Table**

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.2.27	0.0.0.0	UG	0	0	0	eth0
10.0.1.17	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.0	172.16.0.101	255.255.0.0	UG	0	0	0	tun0
172.16.0.1	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.101	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.2.27	0.0.0.0	255.255.255.255	UH	0	0	0	eth0

It is also possible to check successful establishment of OpenVPN tunnel in the system log (*System Log* item in menu). Listings should end with line *Initialization Sequence Completed*.

**System Log****System Messages**

```

2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed

```

## OpenVPN tunnel with username/password authentication

Configuration of the first router – SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Authenticate Mode	username/password

CA Certificate	generated certificate from VPN server
Username	username assigned by the VPN server
Password	password assigned by the VPN server

Configuration of the second router – CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Authenticate Mode	username/password
CA Certificate	generated certificate from VPN server
Username	username assigned by the VPN server
password	password assigned by the VPN server

The procedure of creating certificate is described in article *Creation of certificates*.

**OpenVPN Tunnel Configuration**

Create 1st OpenVPN tunnel

Description *	<input type="text"/>
Protocol	UDP ▾
UDP Port	1194
Remote IP Address *	<input type="text"/>
Remote Subnet *	192.168.3.0
Remote Subnet Mask *	255.255.255.0
Redirect Gateway	no ▾
Local Interface IP Address	<input type="text"/>
Remote Interface IP Address	<input type="text"/>
Ping Interval *	10 sec
Ping Timeout *	30 sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO ▾
NAT Rules	not applied ▾
Authenticate Mode	username / password ▾

Pre-shared Secret

CA Certificate

```
-----BEGIN CERTIFICATE-----
MIIFITCCBIsdavFJNcUISZscdscvb1056knsvLSKVNLksvbFSDdbvbVvdfv35DVD
BBBlknklnnmbskhbCSvdSCBVBBDEvvdsFWFEklnmIUIONDFScxC2csdsJKHKmc
```

DH Parameters

Local Certificate

Local Private Key

Username

\*\*\*\*\*

Password

\*\*\*\*\*

Extra Options \*

\* can be blank

**Apply**

Note: Configuration of the second router is similar, the difference is only in items listed in table *Configuration of the second router – CLIENT*. If *NAT Rules* parameter is enabled, specified rules (in the configuration form of NAT) are applied to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, an interface tun0 and a route in the routing table of the router are displayed on the *Network Status* page.

Network Status							
Interfaces							
eth0	Link encap:Ethernet HWaddr 00:55:44:33:52:98						
	inet addr:192.168.2.234 Bcast:192.168.2.255 Mask:255.255.255.0						
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1						
	RX packets:6743 errors:0 dropped:382 overruns:0 frame:0						
	TX packets:532 errors:0 dropped:0 overruns:0 carrier:0						
	collisions:0 txqueuelen:1000						
	RX bytes:541103 (528.4 KB) TX bytes:277877 (271.3 KB)						
	Interrupt:23						
lo	Link encap:Local Loopback						
	inet addr:127.0.0.1 Mask:255.0.0.0						
	UP LOOPBACK RUNNING MTU:16436 Metric:1						
	RX packets:0 errors:0 dropped:0 overruns:0 frame:0						
	TX packets:0 errors:0 dropped:0 overruns:0 carrier:0						
	collisions:0 txqueuelen:0						
	RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)						
tun0	Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00						
	inet addr:172.16.0.102 P-t-P:172.16.0.101 Mask:255.255.255.255						
	UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1						
	RX packets:0 errors:0 dropped:0 overruns:0 frame:0						
	TX packets:0 errors:0 dropped:0 overruns:0 carrier:0						
	collisions:0 txqueuelen:100						
	RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)						
Route Table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.2.27	0.0.0.0	UG	0	0	0	eth0
10.0.1.17	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.0	172.16.0.101	255.255.0.0	UG	0	0	0	tun0
172.16.0.1	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.101	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.2.27	0.0.0.0	255.255.255.255	UH	0	0	0	eth0

It is also possible to check successful establishment of OpenVPN tunnel in the system log (System Log item in menu). Listings should end with line *Initialization Sequence Completed*.

System Log							
System Messages							
2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]							
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194							
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]							
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194							
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this							
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194							
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened							
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255							
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed							
<input type="button" value="Save Log"/>	<input type="button" value="Save Report"/>						

## OpenVPN tunnel with X.509 certificate authentication

Configuration of the first router – SERVER:

Item	Value
Remote Subnet	192.168.3.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.1

Remote Interface IP Address	10.168.1.2
Authenticate Mode	X.509 certificate (server)
CA Certificate	Generated certificate from VPN server
DH Parameters	Diffie-Hellman protocol for key exchange
Local Certificate	Local certificate assigned by the VPN server
Local Private Key	Local private key assigned by the VPN server

Configuration of the second router – CLIENT:

Item	Value
Remote IP Address	10.0.2.36
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Interface IP Address	10.168.1.2
Remote Interface IP Address	10.168.1.1
Authenticate Mode	X.509 certificate (client)
CA Certificate	Generated certificate from VPN server
Local Certificate	Local certificate assigned by the VPN server
Local Private Key	Local private key assigned by the VPN server

The procedure of creating certificate is described in article *Creation of certificates*.

**OpenVPN Tunnel Configuration**

Create 1st OpenVPN tunnel

Description *	<input type="text"/>
Protocol	UDP ▾
UDP Port	1194
Remote IP Address *	<input type="text"/>
Remote Subnet *	192.168.3.0
Remote Subnet Mask *	255.255.255.0
Redirect Gateway	no ▾
Local Interface IP Address	10.168.1.1
Remote Interface IP Address	10.168.1.2
Ping Interval *	10 sec
Ping Timeout *	30 sec
Renegotiate Interval *	<input type="text"/> sec
Max Fragment Size *	<input type="text"/> bytes
Compression	LZO ▾
NAT Rules	not applied ▾
Authenticate Mode	X.509 cert. (server) ▾

Pre-shared Secret

```
-----BEGIN CERTIFICATE-----
MIIFITCCBiIsdavFJNcUISZscdscvb1056knsvbLSKVNLksvbFSDdbvbVvdfv35DVD
BBBlknklnnmbmskhbCSvdSCBVBBDevvdsxFWFEklnmIUIONDFScxC2csdsJKHKmc
```

DH Parameters

```
-----BEGIN DH PARAMETERS-----
MIGHAscdvMGiugNMB56ascVD54Vdsb2vSCxxyLkGUOhcxsiouHIOUGHCIsdCVLsd
vNVBM34SDVOhudoCSN23sdvjsod3DvuVBSDosvCvn56klasdhsdUIBVGIjckVDIUB
```

Local Certificate

```
-----BEGIN CERTIFICATE-----
MIIFITCCBiIsdavFJNcUISZscdscvb1056knsvbLSKVNLksvbFSDdbvbVvdfv35DVD
BBBlknklnnmbmskhbCSvdSCBVBBDevvdsxFWFEklnmIUIONDFScxC2csdsJKHKmc
```

Local Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIABAjsdvhKSDbHVdHCVSDJchidnIOEHVoibvpoUBVUOibpvEUIB6VDAS5xv
9yxxvKSBcsvJSCV3ldjnvLSKnnVBVkBKKBJVkl3SBvklsdvbDJKBVdvkb1KBVbkdvb
```

Username

Password

Extra Options \*

\* can be blank

Note: Configuration of the second router is similar, the difference is only in items listed in table *Configuration of the second router – CLIENT*. If *NAT Rules* parameter is enabled, specified rules (in the configuration form of NAT) are applied to the OpenVPN tunnel.

After establishing an OpenVPN tunnel, an interface tun0 and a route in the routing table of the router are displayed on the *Network Status* page.

**Network Status****Interfaces**

```

eth0      Link encap:Ethernet HWaddr 00:55:44:33:52:98
          inet addr:192.168.2.234 Bcast:192.168.2.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6743 errors:0 dropped:382 overruns:0 frame:0
          TX packets:532 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:541103 (528.4 KB) TX bytes:277877 (271.3 KB)
          Interrupt:23

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

tun0     Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.102 P-t-P:172.16.0.101 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

```

**Route Table**

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.2.27	0.0.0.0	UG	0	0	0	eth0
10.0.1.17	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.0	172.16.0.101	255.255.0.0	UG	0	0	0	tun0
172.16.0.1	172.16.0.101	255.255.255.255	UGH	0	0	0	tun0
172.16.0.101	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.2.27	0.0.0.0	255.255.255.255	UH	0	0	0	eth0

It is also possible to check successful establishment of OpenVPN tunnel in the system log (*System Log* item in menu). Listings should end with line *Initialization Sequence Completed*.

**System Log****System Messages**

```

2013-05-10 18:27:52 openvpn[1338]: Attempting to establish TCP connection with 88.86.101.201:1194 [nonblock]
2013-05-10 18:27:55 openvpn[1338]: TCP connection established with 88.86.101.201:1194
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link local: [undef]
2013-05-10 18:27:55 openvpn[1338]: TCPv4_CLIENT link remote: 88.86.101.201:1194
2013-05-10 18:27:58 openvpn[1338]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2013-05-10 18:28:00 openvpn[1338]: [LT_server] Peer Connection Initiated with 88.86.101.201:1194
2013-05-10 18:28:14 openvpn[1338]: TUN/TAP device tap0 opened
2013-05-10 18:28:14 openvpn[1338]: /sbin/ifconfig tap0 5.11.2.2 netmask 255.255.0.0 mtu 1500 broadcast 5.11.255.255
2013-05-10 18:28:14 openvpn[1338]: Initialization Sequence Completed

```