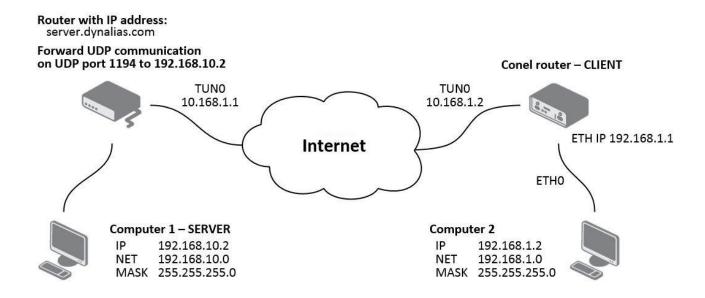
The figure below shows situation, where Conel/Spectre router is on one side of OpenVPN tunnel and device with an operating system Windows/Linux in SERVER mode is on the other side. IP address of the SIM card in the router can be static or dynamic.



OpenVPN tunnel configuration on the router

Item	Value
Remote IP Address	server.dynalias.com
Remote Subnet	192.168.10.0
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 router
DH Parameters	Diffie-Hellman protokol for key exchange
Local Certificate	local certificate assigned by router
Local Private Key	local private key assigned by router

<u> </u>	OpenVPN T	unnel Configuration
	el el	
Description *		
Protocol	UDP	
UDP Port	1194	
Remote IP Address *	server.dynalias.com	
Remote Subnet *	192.168.10.0	
Remote Subnet Mask *	255.255.255.0	
Redirect Gateway	no •	
Local Interface IP Address	10.168.1.2	
Remote Interface IP Address	10.168.1.1	
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO •	
NAT Rules	not applied ▼	
Authenticate Mode	X.509 cert. (client) ▼	
Pre-shared Secret		
CA Certificate		ATE ISZscdscvbl056knsdvLSKVNLksvbFSDdbvbVvdfv35DVD vdSCBVBBDEvvdsvFWFEklnmIUIONDFScxC2csdsvJKHKmc
DH Parameters		
Local Certificate		ATE ISZscdscvbl056knsdvLSKVNLksvbFSDdbvbVvdfv35DVD vdSCBVBBDEvvdsvFWFEklnmIUIONDFScxC2csdsvJKHKmc
Local Private Key		ATE KEY HVdHCVSDJchidnIOEHVoibvpoUBVUOIbpvEUIB6VDAS5xvvLSKnnVBVkBKKBJVkl3SBvklsdvbDJKBVdvkblKBVbkdvb
Username		
Password		
Extra Options *		
* can be blank		
Apply		

Note: 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.

			Netw	rork Sta	tus				
			In	terfaces					
ine UP RX TX col RX	the encap:Ethernet thaddr:192.168.2. BROADCAST RUNNING packets:6743 erro packets:532 error lisions:0 txqueue bytes:541103 (528 errupt:23	234 Bcast:192.16 MULTICAST MTU:1 rs:0 dropped:382 s:0 dropped:0 over len:1000	8.2.25 500 M overru rruns:	5 Mask etric:1 ns:0 fra 0 carrie	ame:0 er:0	5.255	.0		
ine UP RX	k encap:Local Loo t addr:127.0.0.1 LOOPBACK RUNNING packets:0 errors: packets:0 errors:	Mask:255.0.0.0 MTU:16436 Metri 0 dropped:0 overr 0 dropped:0 overr	uns:0		:0				
col	lisions:0 txqueue bytes:0 (0.0 B))						
tun0 Lin ine UP RX TX col		TX bytes:0 (0.0 B Waddr 00-00-00-00- P-t-P:10.168.1.) NG NOARP MULTICAS 0 dropped:0 overro 0 dropped:0 overro len:100	-00-00 2 Mas I MTU uns:0 uns:0	k:255.2 :1500 l frame:0 carrier	55.255.2 (etric:1	255	00-00-00-00		
tun0 Lin ine UP RX TX col	bytes:0 (0.0 B) k encap:UNSPEC H t addr:10.168.1.1 POINTOPOINT RUNNI packets:0 errors: packets:0 errors:	TX bytes:0 (0.0 B Waddr 00-00-00-00- P-t-P:10.168.1.) NG NOARP MULTICAS 0 dropped:0 overro 0 dropped:0 overro len:100	-00-00 2 Mas I MTU uns:0 uns:0	k:255.2 :1500 l frame:0	55.255.2 (etric:1	255	00-00-00-00		
tun0 Lin ine UP RX TX col RX	bytes:0 (0.0 B) k encap:UNSPEC H t addr:10.168.1.1 POINTOPOINT RUNNI packets:0 errors: packets:0 errors: lisions:0 txqueue bytes:0 (0.0 B) Gateway 192.168.2.27	TX bytes:0 (0.0 B Waddr 00-00-00-00- P-t-P:10.168.1.) NG NOARP MULTICAS: 0 dropped:0 overro 1 dropped:0 over	-00-00 2 Mass r MTU uns:0 uns:0) Root	k:255.2 :1500] frame:0 carrier ute Table	55.255 (etric:1 :0 e Ref 0	255 L Use 0	Iface eth0		
col RX tun0 Lin ine UP RX TX col RX Destination 0.0.0.0 10.0.1.17 172.16.0.0 172.16.0.1	bytes:0 (0.0 B) k encap:UNSPEC H t addr:10.168.1.1 POINTOPOINT RUNNI packets:0 errors: packets:0 errors: lisions:0 txqueue bytes:0 (0.0 B) Gateway	TX bytes:0 (0.0 B Waddr 00-00-00-00- P-t-P:10.168.1.) NG NOARP MULTICAS: 0 dropped:0 overro 1 dropped:0 over	-00-00 2 Mas I MTU uns:0 uns:0) Ro Flags UG UGH UG UGH	k:255.2 :1500 lframe:0 carrier ute Table Metric 0 0 0	55.255.1 detric:1 :0 e Ref 0 0 0	Use 0 0 0	Iface eth0 tun0 tun0 tun0		

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 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

Save Log Save Report
```

Tunnel configuration on Computer 1 – Server

It is necessary to perform the following configuration on the computer, which is referred to as *Computer 1 – Server* in the diagram from the beginning of this chapter.

```
local 192.168.10.2
tls-server

dev tun

pull

ifconfig 10.168.1.1 10.168.1.2
route 192.168.1.0 255.255.255.0 10.168.1.2

mute 10

ca cacert.pem
cert client-cert.pem
key client-key2.pem

comp-lzo

verb 3
```