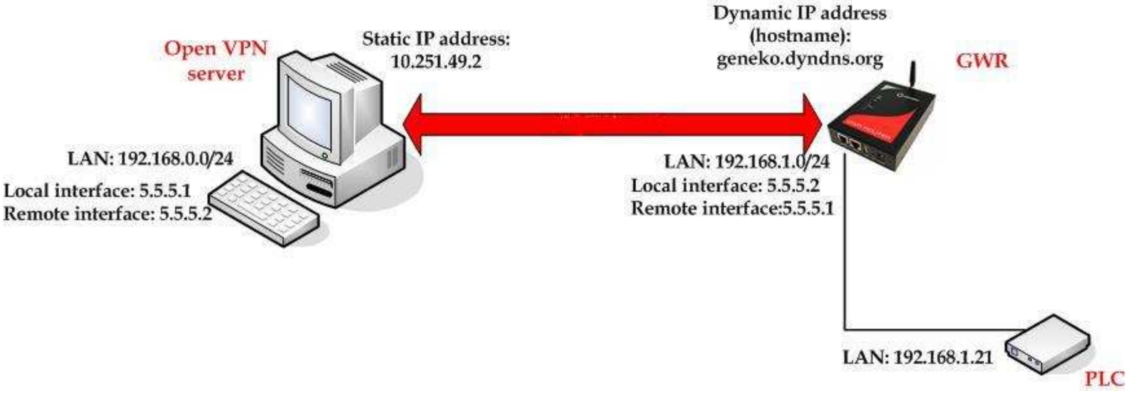
Open VPN Tunnel configuration between GWR Router and OpenVPN server application

OpenVPN site to site allows connecting two remote networks via point–to–point encrypted tunnel. OpenVPN implementation offers a cost–effective simply configurable alternative to other VPN technologies. OpenVPN allows peers to authenticate each other using a pre–shared secret key, certificates, or username/password. When used in a multiclient–server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features. The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also the client can set up the keepalive settings. For successful tunnel creation a static key must be generated on one side and the same key must be uploaded on the opposite side.

OpenVPN tunnel is a type of a VPN tunnels. On the diagram below is illustrated simple network with two sites. Idea is to create OpenVPN tunnel for LAN to LAN (site to site) connectivity.



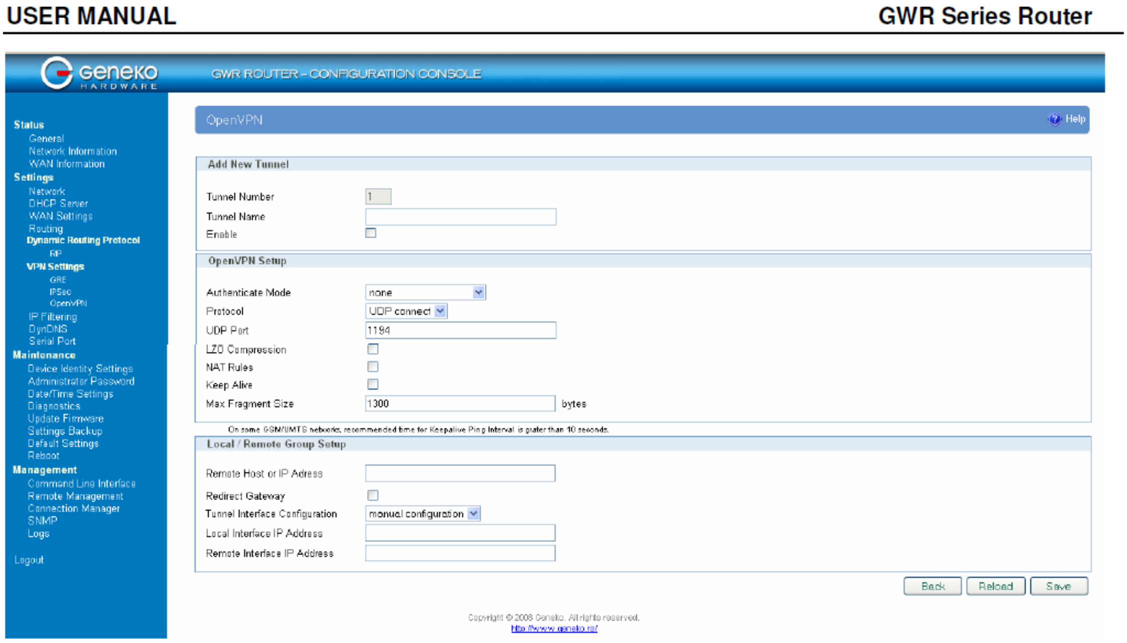
OpenVPN tunnel is created between OpenVPN server application on the central location and the GWR Router on the Remote Network. In this example, it is necessary for both routers to create tunnel interface (virtual interface). This new tunnel interface is its own network. To each of the routers, it appears that it has two paths to the remote physical interface and the tunnel interface (running through the tunnel). This tunnel could then transmit unroutable traffic such as NetBIOS or AppleTalk. The GWR Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. All outgoing traffic uses the GWR Router WAN/VPN mobile IP address. OpenVPN server acts like gateway to remote network for user in corporate LAN. It also performs function of termination of OpenVPN tunnel. The GWR Router act like default gateway for Remote Network and OpenVPN server for tunnel.

1. OpenVPN server requirements:

- OpenVPN server requires static IP WAN address;
- Router or VPN appliance has to support OpenVPN protocol;
- Tunnel peer address will be the GWR Router WAN's mobile IP address. For this reason, a static public IP address is preferred on the GWR Router WAN or you can use dynamic public IP address whith DynDNS client enabled on the router.
- Remote Subnet is remote LAN network address and Remote Subnet Mask is subnet of remote LAN

2. The GWR Router requirements:

- Static IP WAN address;
- Peer Tunnel Address will be the Open VPN server WAN IP address or hostname;
- Remote Subnet is central location LAN IP address and Remote Subnet Mask is subnet mask of its LAN. GSM/UMTS APN Type: For GSM/UMTS networks GWR Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site–to–site VPNs.



Add New Tunnel

Tunnel Number	1
Tunnel Name	
Enable	□

OpenVPN Setup

Authenticate Mode	none
Protocol	UDP connect
UDP Port	1194
LZO Compression	□
NAT Rules	□
Keep Alive	□
Max Fragment Size	1300 bytes

On some GSM/UMTS networks, recommended time for Keepalive Ping Interval is grater than 10 seconds.

Local / Remote Group Setup

Remote Host or IP Adress	
Redirect Gateway	□
Tunnel Interface Configuration	manual configuration
Local Interface IP Address	
Remote Interface IP Address	

Copyright © 2008 Geneko. All rights reserved.
http://www.geneko.rs/

Configuration of GWR Open VPN client is following:

Authenticate Mode: PreShared Key (PSK)
Protocol: TCP Client

TCP port:	1194
LZO Compression:	Enabled
Pre Shared Key:	Generate PSK and paste to OpenVPN server
Remote Host or IP address:	10.251.49.2 (Static IP address)
Redirect Gateway:	Enable
Tunnel interface configuration:	manual configuration
Local interface IP address:	5.5.5.2
Remote interface IP address:	5.5.5.1

Configuration file on the server side should look like this:

```
remote 2.192.116.11
port 1194
proto tcp-server
dev tun
tun-mtu 1500
ifconfig 5.5.5.1 5.5.5.2
ping 10
comp-lzo
verb 4
mute 10
disable-occ
```

Save file in *OpenVPN\config* directory with *key.txt* file which you exported from the router