

Step by Step Instruction for Anonyproz OpenVPN and DD-WRT Firmware Router

Prerequisites:

1. OpenVPN account from <http://www.anonyproz.com>
2. Anonyproz OpenVPN servers details (IP, Port, Tunnel Protocol, Tunnel Device and Certificate).
You can download the server certificate file and settings document for each server from the link below:
<http://www.anonyproz.com/dd-wrt-startup.rar>
3. The right WLAN Router for you.
4. The right DD-WRT firmware version for your router.
5. Knowledge with basic networking.

In this tutorial, let's assume that you have an active OpenVPN account with Anonyproz.com. Take the following steps:

Step1: Choosing a correct WLAN Router

To flash your router firmware with DD-WRT VPN firmware, your device must have at least 4MB of flash. If you already have a router, check with your device manufacturer or go to http://www.dd-wrt.com/wiki/index.php/Supported_Devices to check if your router is supported.

Step 2: Get the right DD-WRT firmware

Download the dd-wrt firmware at <http://www.dd-wrt.com/site/support/router-database> . The setup was tested for **WRT54GL** router. First, install the "mini" version of DD-WRT with filename:

dd-wrt.v24_mini_generic.bin . Then, install the "vpn" version of DD-WRT with filename:

dd-wrt.v24_vpn_generic.bin

Important: You must use these exact firmware versions and names listed above as other versions are not supported!

You can also find these firmware from the archive file you download from:

<http://www.anonyproz.com/dd-wrt-startup.rar>

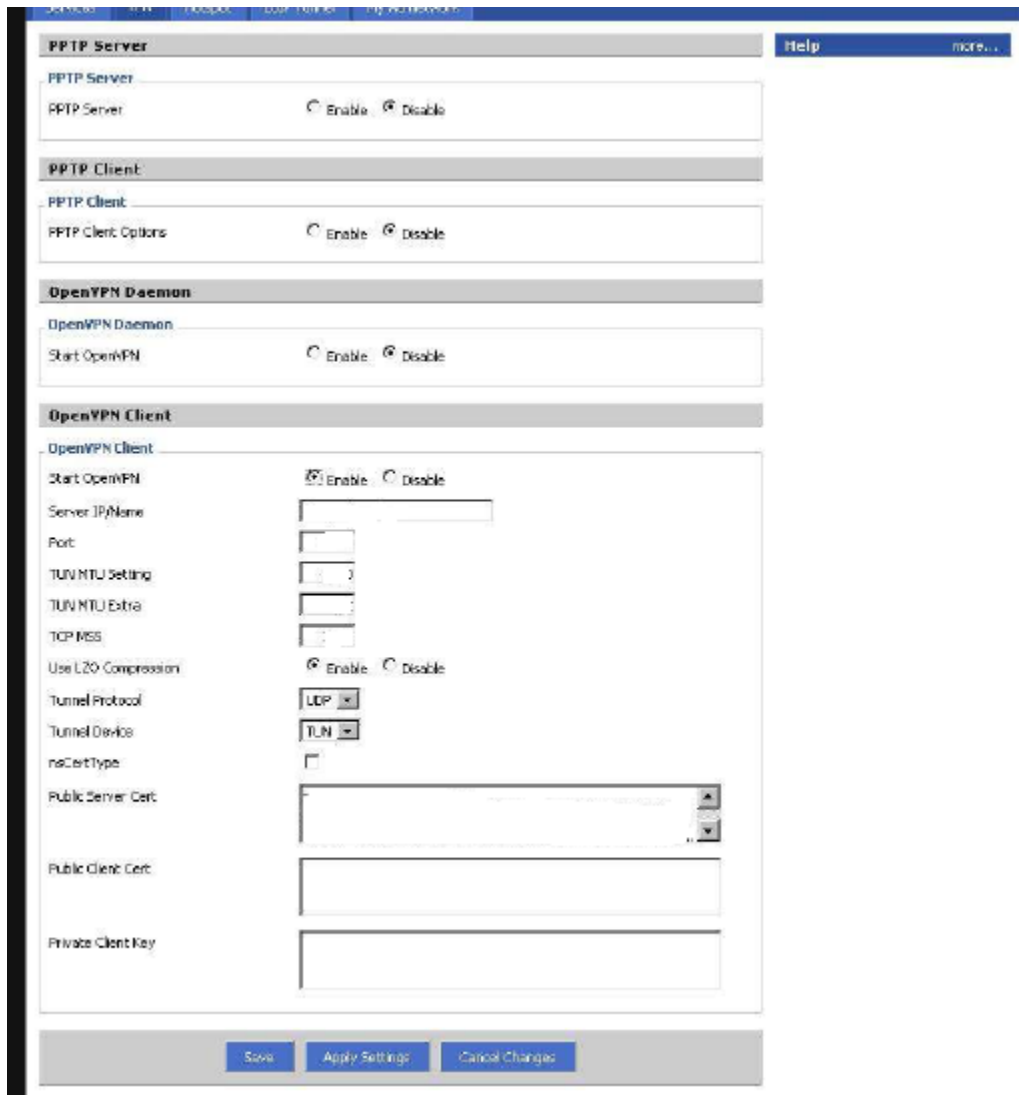
Step 3: Flash your router with DD-WRT firmware

See the instruction to flash your router on dd-wrt website for your specific machine. Use **Microsoft Internet Explorer** to flash your router. **Be cautious**, it can brick your router if the firmware is not correct version for your router.

Step 4: Configuring OpenVPN

We'll connect to a sample Anonymoz OpenVPN server here.

Login to your router via web management. It should look like the screenshot shown below:



i: Go to **Services** > **VPN** tab.



ii: Enable OpenVPN Client.

iii: Configure Parameters as below,

- a. Remote IP : XXX.XXX.XXX.XXX (Replace with the server IP)
- b. Port : 443
- c. TUN MTU Setting:1500
- d. TUN MTU Extra: 32
- e. TCP MSS: 1450
- f. Use LZO Compression : enable
- g. Protocol : TCP
- h. Tunnel Device : TUN

iv: Get the certificate text file named “ca-cert.txt” provided in the archive file you downloaded in the pre-requisite section .

Open the file ca.crt with a text editor and copy the complete key (including „---Begin Certificate---“) into the field for the public server cert.

v: Click on ‘Save’, and ‘Apply Changes’.

Step 5: Go to **Administration > Commands**.



Copy and paste the italicized commands below under the "Startup" form and press the „Save Startup“ button:

```
sleep 30  
echo "USERNAME  
PASSWORD" > /tmp/openvpncl/user.conf  
sleep 10  
echo "client  
dev tun  
proto tcp  
hand-window 30  
port 443  
remote XXX.XXX.XXX.XXX  
resolv-retry infinite  
nobind  
persist-key  
persist-tun  
comp-lzo  
verb 3  
ca /tmp/openvpncl/ca.crt  
auth-user-pass /tmp/openvpncl/user.conf" > /tmp/openvpncl/vpn.conf  
( sleep 10 ; killall openvpn ; /usr/sbin/openvpn --config /tmp/openvpncl/vpn.conf  
--auth-user-pass /tmp/openvpncl/user.conf  
--route-up /tmp/openvpncl/route-up.sh --down /tmp/openvpncl/route-down.sh  
--daemon ) &
```

Note: Make sure you replace the following parameters indicated in red:

- XXX.XXX.XXX.XXX : Replace this with the actual OpenVPN server IP you wish to connect to. You will find all our servers IPs in a word document for each server folder in the link below :

<http://www.anonyproz.com/dd-wrt-startup.rar>

- USERNAME: Replace this with your member username
- PASSWORD: Replace this with your member password

Step 6: Enter Firewall Command

Copy and paste the following commands into the “Firewall” form and click on “Save Firewall”

```
iptables -I FORWARD -i br0 -o tun0 -j ACCEPT  
iptables -I FORWARD -i tun0 -o br0 -j ACCEPT  
iptables -I INPUT -i tun0 -j REJECT  
iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE
```

Step 7: Confirm settings and Reboot Router

Your window should now look like the one shown below. Double check everything and finally click on ‘Save’, ‘Apply Changes’, and Reboot your router.

You can do this as follows. Go to the „Administration“ Tab and select then the „Management“ Tab. At the bottom you will find this selection:



Select the style „brainslayer“, press the button „Preview“ and after that you can select the button „Reboot“ on the left side:



You can also reboot the router by pressing the button directly on the router or you can reset it by getting it without power – plug it off and on.

Note: 60-90 seconds after the reboot of your router, ALL traffic will then be routed via the OpenVPN.

Command Shell

Startup

```

sleep 30
echo '*' > /tmp/openvpncl/user.conf
sleep 10
echo 'client
dev tun
proto udp
hand-window 30
port 1195
route !
resolv-retry infinite
nobind
persist-key
persist-tun
ns-cert-type server
cipher BF-CBC
comp-lzo
verb 3
reneg-sec 0
ca /tmp/openvpncl/ca.crt
auth-user-pass /tmp/openvpncl/user.conf' > /tmp/openvpncl/vpn.conf
( sleep 10 ; killall openvpn ; /usr/sbin/openvpn --config /tmp/openvpncl/vpn.conf
--route-up /tmp/openvpncl/route-up.sh --down /tmp/openvpncl/route-down.sh --ds

```

[Edit](#)

Firewall

```

iptables -I FORWARD -i br0 -o tun0 -j ACCEPT
iptables -I FORWARD -i tun0 -o br0 -j ACCEPT
iptables -I INPUT -i tun0 -j REJECT
iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE

```

[Edit](#)

Run Commands

Save Startup

Save Shutdown

Save Firewall

[Save Custom Script](#)

Commands:
You can run command lines via the web interface. Fill the text area with your command and click [Run Commands](#) to submit.

Step 8: Setting DNS

Follow the steps below to configure DNS on your system. You can use our private DNS servers which support malware Domains sinkhole for blocking all known malware sites which you can find here:

<https://www.anonyproz.com/dnssinkhole/>

If you wish to use our private DNS servers with malware domain sinkhole capability, you need to configure your system DNS to use the IPs below:

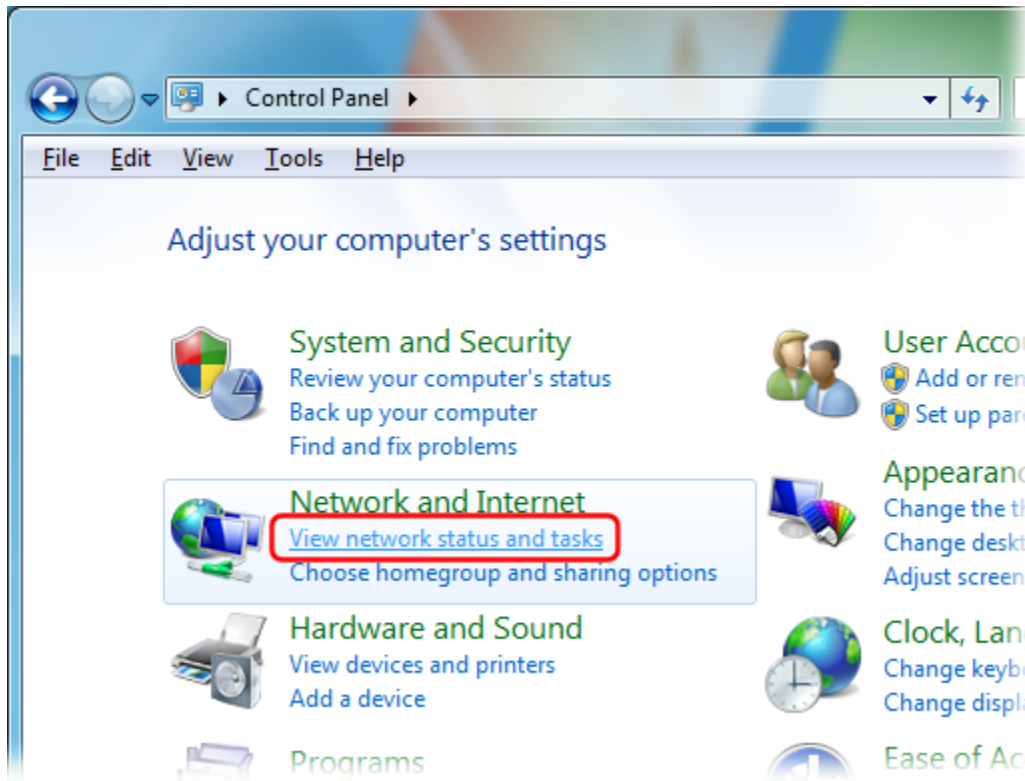
46.166.157.87

46.166.143.110

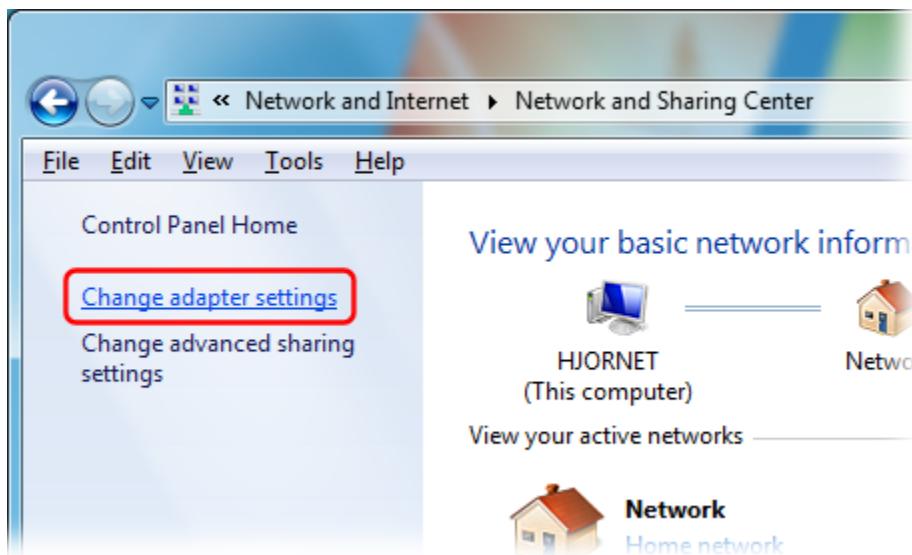
Alternatively, you can use any free Open DNS such as Google public DNS, OpenDNS or COMODO DNS.

The following steps illustrate how to configure Windows 7 system to use Google public DNS servers:

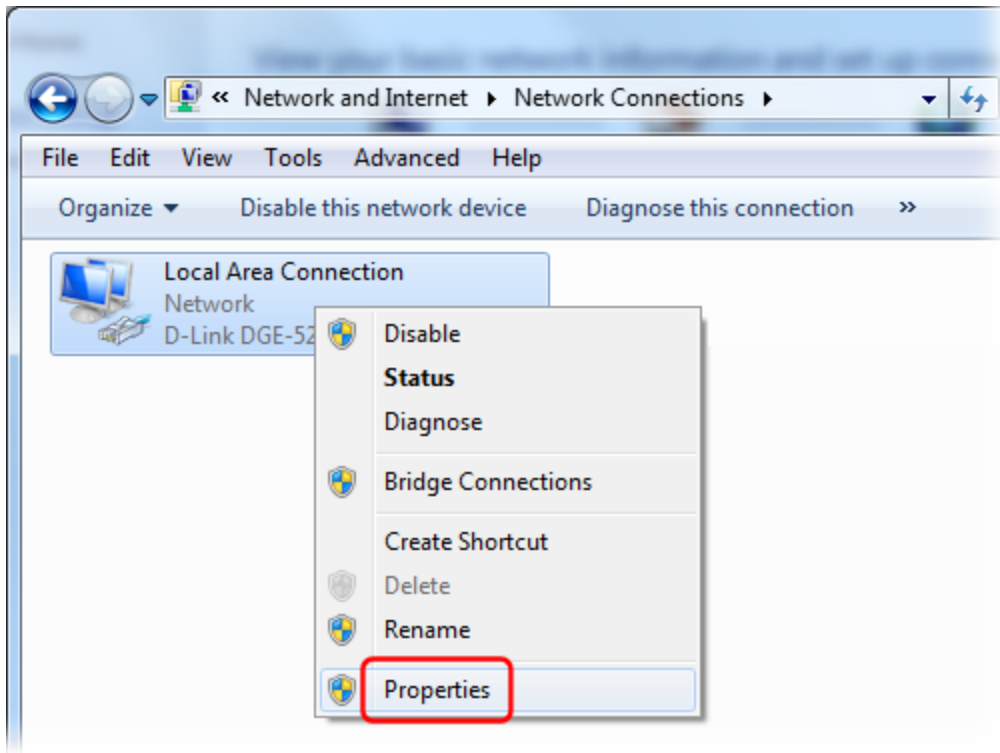
In the Windows Control Panel, under "Network and Internet", select "View network status and tasks":



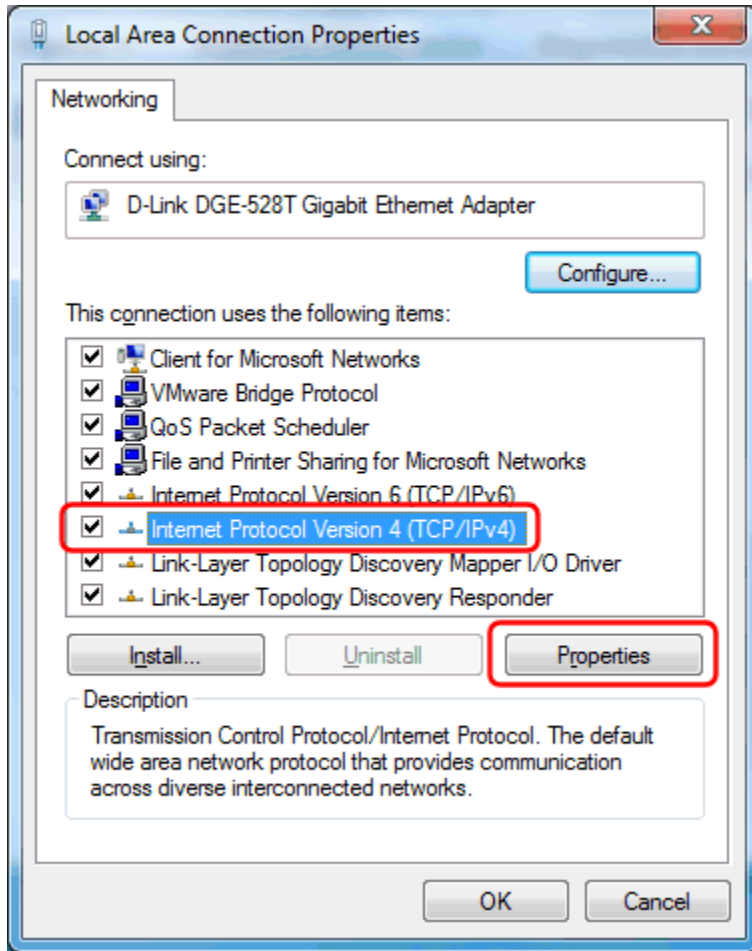
Click "Change adapter settings":



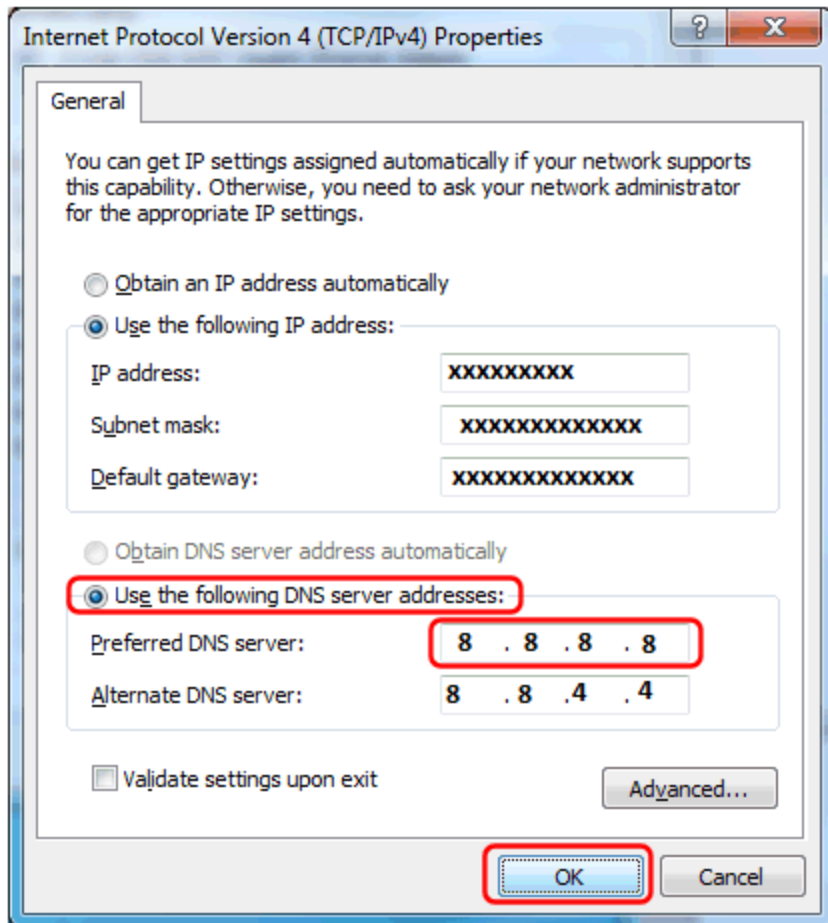
Right-click your Internet connection's icon and select "Properties":



Select the "Internet Protocol Version 4 (TCP/IPv4)" item, and click the "Properties" button:



Select "Use the following DNS server addresses", and enter the IP address of the local DNS server (*) as the Preferred DNS server:



Finally click the "OK" button in this and the previous dialogs to save your changes.

Test your OpenVPN Connection

After successfully Rebooting, wait for 3 minutes to start OpenVPN up.

Open your favorite browser and visit <http://www.geoiptool.com/>.

Be sure, you are not connected to Anonymoz OpenVPN server via Windows GUI OpenVPN client as we are going to test the vpn connection of your router.

Check your IP-Address; it must be correspond to the OpenVPN server IP if you are successfully connected to Anonymoz.

If your External-IP corresponds to the remote OpenVPN server IP, **Congratulation** your router is successfully configured to use Anonymoz OpenVPN.

If your IP address is other than the server IP, see Troubleshooting below.

Troubleshooting & FAQs

- a) Cannot connect to internet.
 - Visit different famous websites such as <http://www.google.com> to check your connection.
 - Check your Client IP is in the same net as your Router IP.
 - Check your DNS setting configuration.
 - Check WAN configuration in your router basic setup.
- b) Cannot connect to Anonyproz OpenVPN server
 - Check your Anonyproz username and password in Startup Command.
 - Check your Anonyproz account is still active.
 - Check your DNS is used Anonyproz DNS.
 - Check OpenVPN process is up and running in your router.
 - Check your NTP service works correctly.
- c) How can I check OpenVPN process is up and running in my router?
 - Login to your router web management console and go to Administration > Commands
 - Type 'ps' without quotes and press 'Run Commands' button
 - You will see a list of running processes.
 - Search for openvpn process in the running processes list.
- d) How can I kill openvpn processes and restart it in my router?
 - Login to your router web management console and go to Administration > Commands
 - Type 'killall openvpn' without quotes and press 'Run Commands' button.
 - Search for openvpn process as above method, to ensure the process was actually killed.
 - Press the „Run commands“ button
- e) How can I check my NTP service works?
 - Login to your router web management console and go to Status > Router
 - Check Current Time is correct.
- f) My NTP service doesn't seem to work properly.
 - If NTP service doesn't work properly, your router won't be able to connect OpenVPN server successfully.
 - Here is a trick in this condition:
 - Add 'date xxxxxxxxxxxx' command on top of the Startup Command.
 - Date format is 'MMDDHHMMYYYY'
 - The new command will look like this:

```
sleep 30
date 010101012011
echo "your-username
.....
```
 - Press 'Save Startup' and Reboot your router.
- g) I want to use another Anonyproz server. What should I do?

- You are free to change Remote IP, Protocol and Port in Startup command. Just use the server IP as provided in the “General Settings” document in the server config folder.
 - Search other configurations in OpenVPN config folder.
 - You are now able to figure out the basic setups for your router with Anonyproz OpenVPN.
- h) Can I login to my router via telnet?
- Yes, you can. Search for articles on dd-wrt website for more details.