**[How To Install and Configure OpenVPN On Your DD-WRT Router](http://www.howtogeek.com/64433/how-to-install-and-configure-openvpn-on-your-dd-wrt-router/%22%20%5Co%20%22How%20To%20Install%20and%20Configure%20OpenVPN%20On%20Your%20DD-WRT%20Router)**

Installing OpenVPN

Now let’s head over to OpenVPN’s [Downloads](http://openvpn.net/index.php/open-source/downloads.html) page and download the OpenVPN Windows Installer. In this guide, we’ll be using the second latest version of OpenVPN called 2.1.4. The latest version (2.2.0) has a [bug](https://community.openvpn.net/openvpn/ticket/125) in it that would make this process even more complicated. The file we’re downloading will install the OpenVPN program that allows you to connect to your VPN network, so be sure to install this program on any other computers that you want to act as clients (as we’ll be seeing how to do that later). Save the openvpn-2.1.4-install .exe file to your computer.



Navigate to the OpenVPN file we just downloaded and double click it. This will begin the installation of OpenVPN on your computer. Run through the installer with all the defaults checked. During the installation, a dialog box will pop up asking to install a new virtual network adapter called TAP-Win32. Click the Install button.



Creating the Certificates and Keys

Now that you have OpenVPN installed on your computer, we have to start creating the certificates and keys to authenticate devices. Click the Windows Start button and navigate under Accessories. You’ll see the Command Prompt program. Right click on it and click Run as administrator.



In the command prompt, type *cd c:\Program Files (x86)\OpenVPN\easy-rsa* if you’re running 64-bit Windows 7 as seen below. Type *cd c:\Program Files\OpenVPN\easy-rsa* if you’re running 32-bit Windows 7. Then hit Enter.

Now type *init-config* and hit Enter to copy two files called vars.bat and openssl.cnf into the easy-rsa folder. Keep your command prompt up as we’ll be coming back to it shortly.



Navigate to *C:\Program Files (x86)\OpenVPN\easy-rsa* (or *C:\Program Files\OpenVPN\easy-rsa* on 32-bit Windows 7) and right click on the file called *vars.bat*. Click Edit to open it up in Notepad. Alternatively, we recommend opening this file with Notepad++ as it formats the text in the file much better. You can download Notepad++ from their [homepage](http://notepad-plus-plus.org/).



The bottom portion of the file is what we are concerned with. Starting at line 31, change the *KEY\_COUNTRY* value, *KEY\_PROVINCE* value, etc. to your country, province, etc. For example, we changed our province to “IL”, city to “Chicago”, org to “HowToGeek”, and email to our own email address. Also, if you’re running Windows 7 64-bit, change the *HOME* value in line 6 to *%ProgramFiles (x86)%\OpenVPN\easy-rsa*. Do not change this value if you’re running 32-bit Windows 7. Your file should look similar to ours below (with your respective values, of course). Save the file by overwriting it once you’re done editing.



Go back to your command prompt and **type *vars*** and hit Enter. Then **type *clean-all*** and hit Enter. Finally, **type *build-ca*** and hit Enter.



After executing the *build-ca* command, you will be prompted to enter in your Country Name, State, Locality, etc. Since we already set up these parameters in our *vars.bat* file, we can skip past these options by hitting Enter, **but!** Before you start slamming away at the Enter key, watch out for the Common Name parameter. You can enter anything in this parameter (i.e. your name). Just make sure you enter *something*. This command will output two files (a Root CA certificate and a Root CA key) in the easy-rsa/keys folder.



Now we’re going to build a key for a client. In the same command prompt **type *build-key* *client1***. You can change “client1” to anything you’d like (i.e. Acer-Laptop). Just be sure to enter the same name as the Common Name when prompted. Run through all the defaults like the last step we did (except for Common Name, of course). However, at the end you will be asked to sign the certificate and to commit. Type “y” for both and click Enter.

Also, don’t worry if you received the “unable to write ‘random state’” error. We’ve noticed that your certificates still get made without a problem. This command will output two files (a Client1 Key and a Client1 Certificate) in the easy-rsa/keys folder. If you want to create another key for another client, repeat the previous step, but be sure to change the Common Name.



The last certificate we’ll be generating is the server key. In the same command prompt, **type *build-key-server* *server***. You can replace “server” at the end of the command with anything you’d like (i.e. HowToGeek-Server). As always, be sure to enter the same name as the Common Name when prompted. Hit Enter and run through all the defaults except Common Name. At the end, type “y” to sign the certificate and commit. This command will output two files (a Server Key and a Server Certificate) in the easy-rsa/keys folder.



Now we have to generate the Diffie Hellman parameters. The Diffie Hellman protocol “allows two users to exchange a secret key over an insecure medium without any prior secrets”. You can read more about Diffie Hellman on RSA’s [website](http://www.rsa.com/rsalabs/node.asp?id=2248).

In the same command prompt **type *build-dh***. This command will output one file (dh1024.pem) in the easy-rsa/keys folder.



Creating the Configuration Files for the Client

Before we edit any configuration files, we should set up a dynamic DNS service. Use this service if your ISP issues you a dynamic external IP address every so often. If you have a static external IP address, skip down to the next step.

We suggest using [DynDNS.com](http://www.dyndns.com/), a service that allows you to point a hostname (i.e. howtogeek.dyndns.org) to a dynamic IP address. It’s important for OpenVPN to always know your network’s public IP address, and by using DynDNS, OpenVPN will always know how to locate your network no matter what your public IP address is. Sign up for a free [hostname](http://www.dyndns.com/services/dns/dyndns/) and point it to your public [IP address](http://www.whatsmyip.org/).

Now back to configuring OpenVPN. In Windows Explorer, navigate to *C:\Program Files (x86)\OpenVPN\sample-config* if you’re running 64-bit Windows 7 or *C:\Program Files\OpenVPN\sample-config* if you’re running 32-bit Windows 7. In this folder you will find three sample configuration files; we’re only concerned with the *client.ovpn* file.



Right click on *client.ovpn* and open it with Notepad or Notepad++. You’ll notice your file will look like the picture below:



However, we want our *client.ovpn* file to look similar to *this* picture below. Be sure to change the DynDNS hostname to your hostname in line 4 (or change it to your public IP address if you have a static one). Leave the port number to 1194 as it is the standard OpenVPN port. Also, be sure to change lines 11 and 12 to reflect the name of your client’s certificate file and key file. Save this as new file .ovpn file in the OpenVPN/config folder.



**OPENVPN INSTRUCTIONS**

I thought I would share this with everyone here how I was able to get this working. I have been trying for sometime to configure my Linksys e4200v1 router with OpenVPN for sometime without success. It seems there is a huge disconnect with the wiki's out there and how the newer builds are configured. However, between reading about bugs in certain builds and improper configs etc I thought I would share this method to get you going.

I don't know much about the technical details around how this all works but I was able to piece together what was required from this important post: <http://www.dd-wrt.com/phpBB2/viewtopic.php?p=641031> as well as the OpenVPN manual/wiki.

A huge thank you to **GTI\_nut** and **maddes.b** for their posts which really helped me to get this all going.

Here are a few things about my setup:

**Router:** Linksys e4200v1
**Build:** king kong r20500 mega <http://www.desipro.de/ddwrt/K26/r20500/>
**OpenVPN version used to generate certs:** 2.2.2 http://swupdate.openvpn.org/community/releases/openvpn-2.2.2-install.exe

**What is working:**

Ipod is able to connect to VPN
Desktop is able to connect to VPN
All VPN clients can access LAN PC's
Internet on LAN PC's works perfectly when clients are connected

Now before I go any further I thought I would also add that there is no need for any addition firewall rules for the router except for a few easy startup Commands which I will outline.

Here we go:

Basic Network Topology:
Server: 192.168.1.0
LAN: 192.168.1.0
VPN: 10.10.10.0

Of course feel free to use whatever IP Addressing you like for your VPN network.

========================================
DD-WRT v24-sp2 (02/03/13) kingkong (SVN revision 20500M) mega

**Services** => VPN tab:
**OpenVpn Server:** enabled
**Start Type:** WAN up
**Config as:** Server
**Server Mode:** Routed (TUN)
**Network:** 10.10.10.0
**Netmask:** 255.255.255.0
**Port:** 443 (you can use the default 1194)
**Tunnel Protocol:** UDP (you can also use TCP just make sure to tweak your client config)
**Encryption Cipher:** Blowfish CBC (I have also played around with this you can use what you want I tried AES-256-CBC and it's fine)
**Hash Algorithm:** SHA1
**Advanced Options:** Enabled
**TLS Cipher:** None
**LZO COmpression:** Yes
**Redirect default Gateway:** Disable
**Allow Client to Client:** Enable
**Allow duplicate cn:** Disable (you can enable if you need this)
**Tunnel MTU setting:** 1500
**Tunnel UDP Fragment:** empty
**Tunnel UDP MSS-Fix:** Disable

Certs that I filled in:
**Public Server Cert:** server cert
**CA Cert:** CA Cert
**Private Server Key:** server key
**DH PEM:** dh1024.pem
**TLS Auth Key:** Leave empty
**Certificate Revoke List:** Leave empty

If you need to know how to generate certs and keys, please look here: <http://www.howtogeek.com/64433/how-to-install-and-configure-openvpn-on-your-dd-wrt-router/> and look under the section Creating the Certificates and Keys

**Additional Config:**

client-client
push "route 192.168.1.0 255.255.255.0"
route 192.168.1.100 255.255.255.0 10.10.10.2

Okay that takes care of the VPN server config and if you have a different LAN address change the IP addresses in the Additional config section to apply to your network. Now to complete the startup commands that I spoke of earlier

Administration => Commands
Startup:
mkdir -p /tmp/openvpn/ccd
echo "iroute 192.168.1.100 255.255.255.0" > /tmp/openvpn/ccd/**ipod**
echo "iroute 192.168.1.100 255.255.255.0" > /tmp/openvpn/ccd/**laptop1**

Okay so these lines that start with **echo** are important the bits that I have bolded need to be the same **common name** that you entered when generating your client keys. If you don't know what I am referring to then please see section where I mention how to create your certs and keys. Also the IP addresses above are the range that the DHCP addresses start from for my network that the router assigns. So if you have something different please change those because I believe that these are the commands that allow the VPN network to speak with your LAN.

-------------------------------------

Now the client config:

client
dev tun
proto udp (if using TCP use "**proto tcp**" instead)
remote your.ipaddress.com 443 (remember port needs to match what you configured so say 1194 if you used the default)
ca ca.crt
cert **ipod.crt**
key **ipod.key**
ns-cert-type server
comp-lzo
verb 3

Now the bolded bits are the names of the client key I generated. So obviously these will change based on what you name your client keys. This config I typed into notepad and then saved it as **client.ovpn**

To import the files into IOS use ITunes and under apps and click on the OpenVPN icon and then add these files:

**client.ovpn**
**ca.crt**
**ipod.crt** (this will change based on what you named your keys)
**ipod.key** (this will change based on what you named your keys)

-----------------------
Now for the laptop running Windows 7 I installed OpenVPN 2.2.2

remote your.ipaddress.com 443 (I put this line first, I read it somewhere that its good to do that)
client
dev tun
proto udp
ca ca.crt
cert **laptop1.crt** (change to your cert name)
key **laptop1.key** (change to your corresponding key name)
ns-cert-type server
comp-lzo
verb 3[/color]

This config I typed into notepad and then saved it as **client.ovpn**

In windows 7 64 bit navigate to this folder:

**C:\Program Files(x86)\OpenVPN\config**

**client.ovpn
ca.crt
laptop1.crt
laptop1.key**

Also run the OpenVPN GUI as "**Administrator**" and then click connect.

-------------------

That's pretty much it. I will try and answer any questions that you may have. I just wanted to share this because it's been really tough to find any tutorials that use the TUN connection and relates to DD-WRT specifically. I have found a few based on TAP but that does not allow for any connections from IOS devices and all of the tutorials I could find were based on older builds which required firewall rules.