



## Setting up a VPN tunnel using OpenVPN

---

Created by : *Hans Camu*  
Date : *23 January 2011*  
<http://camoraict.wordpress.com>

I thank this paper because of good advice of my good friend and colleague Rob den Braber. Rob is a partner at [GRID-IT](#).

I am running an Oracle VM server at home. On this Oracle VM server I am running several Oracle virtual machines. I would like to remotely access these virtual machines when I am not at home. For this purpose a Virtual Private Network (VPN) is a good option. But I have some requirements:

- VPN software must be free
- VPN software must be available for Linux (Oracle Enterprise Linux) and Windows
- No tweaking of my currently used router (Sitecom WL-342 v2)
- VPN software must be easy to configure

After some research I ended up with the following software:

- [OpenVPN](#), software for both running a VPN server and client

## Installing packages on the OpenVPN server

This paragraph will describe the steps to install the packages on the OpenVPN server.

On my Oracle VM server I created a virtual machine and installed Oracle Enterprise Linux 5 update 5 32-bit on it. I performed a minimal installation, because I only will use this server as an OpenVPN server. Because this server is a virtual machine, you must make sure that the network card is bridged to the physical network card in your computer. Give the new server a dedicated IP-address, because you have to make an adjustment in your router. At my home I use the network segment 192.168.0.0 / 255.255.255.0. I gave my OpenVPN server the IP-address 192.168.0.200.

1. Install the following packages:

- [lzo2-2.02-3.el5.rf.i386.rpm](#)
- [openvpn-2.0.9-1.el5.rf.i386.rpm](#)

If you click on the links above, it will lead you to the site where you can download the RPM's. Copy the packages to your server that you're going to use as your OpenVPN server.

2. Install the packages with the rpm command:

```
[root@openvpn ~]# rpm -ivh lzo2-2.02-3.el5.rf.i386.rpm
warning: lzo2-2.02-3.el5.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID
6b8d79e6
Preparing...                               ##### [100%]
 1:lzo2                                     ##### [100%]

[root@openvpn ~]# rpm -ivh openvpn-2.0.9-1.el5.rf.i386.rpm
warning: openvpn-2.0.9-1.el5.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID
6b8d79e6
Preparing...                               ##### [100%]
 1:openvpn                                   ##### [100%]
```

The packages are installed.

## Configuration of the OpenVPN server

This paragraph will describe the steps to install configure the OpenVPN server.

Most of the files of the openvpn package are placed in the directory /usr/share/doc/openvpn-2.0.9.

1. First step is to create the certificates for the OpenVPN server :

```
[root@openvpn ~]# cd /usr/share/doc/openvpn-2.0.9/easy-rsa/2.0
```

2. Change the *Makefile* in this directory and set the *DESTDIR* to */etc/openvpn*.  
After the change the file will look like this:

```
[root@openvpn 2.0]# vi Makefile
DESTDIR=/etc/openvpn
PREFIX=
all:
    echo "All done."
    echo "Run make install DESTDIR=/usr/share/somewhere"
install:
    install -c --directory "${DESTDIR}/${PREFIX}"
    install -c --mode=0755 build-* "${DESTDIR}/${PREFIX}"
    install -c --mode=0755 clean-all list-crl inherit-inter pkitool revoke-full sign-req whichopensslcnf "${DESTDIR}/${PREFIX}"
    install -c --mode=0644 openssl-0.9.6.cnf openssl.cnf README vars
"${DESTDIR}/${PREFIX}"
```

3. Run the *make install* command to install all the necessary files to the directory */etc/openvpn*:

```
[root@openvpn 2.0]# make install
install -c --directory "/etc/openvpn/"
install -c --mode=0755 build-* "/etc/openvpn/"
install -c --mode=0755 clean-all list-crl inherit-inter pkitool revoke-full sign-req whichopensslcnf "/etc/openvpn/"
install -c --mode=0644 openssl-0.9.6.cnf openssl.cnf README vars "/etc/openvpn/"
```

4. Go to the directory */etc/openvpn*:

```
[root@openvpn 2.0]# cd /etc/openvpn
```

5. Change the last 5 lines of the *vars* file in this directory:

```
root@openvpn openvpn]# vi vars
export KEY_COUNTRY="NL"
export KEY_PROVINCE="UT"
export KEY_CITY="dummytown"
export KEY_ORG="Dummy-Org"
export KEY_EMAIL="foo@dummy.org"
```

Specify the Country, Province, City, Organization and an email address.

6. Set the parameters by running the *source* command.  
You can ignore the message about the clean-all script:

```
[root@openvpn openvpn]# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/keys
```

7. Run the *clean-all* procedure to clean the keys directory.  
If this is the first time, than this directory does not exists:

```
[root@openvpn openvpn]# ./clean-all
```

8. Build the certificate authority:

```
[root@openvpn openvpn]# ./build-ca
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [NL]:
State or Province Name (full name) [UT]:
Locality Name (eg, city) [dummytown]:
Organization Name (eg, company) [Dummy-Org]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Dummy-Org CA]:
Email Address [foo@dummy.org]:
```

9. Create the server certificates:

```
[root@openvpn openvpn]# ./build-key-server server
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [NL]:
State or Province Name (full name) [UT]:
Locality Name (eg, city) [dummytown]:
Organization Name (eg, company) [Dummy-Org]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Email Address [foo@dummy.org]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'NL'
stateOrProvinceName  :PRINTABLE:'UT'
localityName         :PRINTABLE:'dummytown'
organizationName     :PRINTABLE:'Dummy-Org'
commonName           :PRINTABLE:'server'
emailAddress         :IA5STRING:'foo@dummy.org'
```

```
Certificate is to be certified until May 11 14:27:28 2020 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

## 10. Create at least one client key:

```
[root@openvpn openvpn]# ./build-key client1
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [NL]:
State or Province Name (full name) [UT]:
Locality Name (eg, city) [dummytown]:
Organization Name (eg, company) [Dummy-Org]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client1]:
Email Address [foo@dummy.org]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'NL'
stateOrProvinceName  :PRINTABLE:'NH'
localityName         :PRINTABLE:'dummytown'
organizationName     :PRINTABLE:'Dummy-Org'
commonName           :PRINTABLE:'client1'
emailAddress         :IA5STRING:'foo@dummy.org'
Certificate is to be certified until May 11 14:28:33 2020 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

## 11. Create the Diffie-Hellman (DH) settings:

```
[root@openvpn openvpn]# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....
```

12. Copy the following files from directory `/usr/share/doc/openvpn-2.0.9/sample-config-files` to directory `/etc/openvpn`:

- `openvpn-shutdown.sh`
- `openvpn-startup.sh`
- `server.conf`

```
[root@openvpn openvpn]# cd /usr/share/doc/openvpn-2.0.9/sample-config-files
[root@openvpn sample-config-files]# cp -pv openvpn-startup.sh openvpn-
shutdown.sh server.conf /etc/openvpn
`openvpn-startup.sh' -> `/etc/openvpn/openvpn-startup.sh'
`openvpn-shutdown.sh' -> `/etc/openvpn/openvpn-shutdown.sh'
`server.conf' -> `/etc/openvpn/server.conf'
```

**Important:** From the `openvpn-startup.sh` and `openvpn-shutdown.sh` files remove the `.sh` extension. The init script in `/etc/init.d/openvpn` uses the filenames `openvpn-startup` and `openvpn-shutdown`.

```
[root@openvpn sample-config-files]# cd /etc/openvpn
[root@openvpn openvpn]# mv -v openvpn-shutdown.sh openvpn-shutdown
`openvpn-shutdown.sh' -> `openvpn-shutdown'
[root@openvpn openvpn]# mv -v openvpn-startup.sh openvpn-startup
`openvpn-startup.sh' -> `openvpn-startup'
```

13. Make the files `openvpn-shutdown` and `openvpn-startup` executable:

```
[root@openvpn openvpn]# chmod u+x openvpn-shutdown openvpn-startup
```

14. Modify the `openvpn-startup` file:

```
[root@openvpn openvpn]# vi openvpn-startup
```

Replace the line containing:

```
$dir/firewall.sh
```

with

```
#$dir/firewall.sh
```

and

```
openvpn --cd $dir --daemon --config vpn1.conf
openvpn --cd $dir --daemon --config vpn2.conf
openvpn --cd $dir --daemon --config vpn2.conf
```

with

```
#openvpn --cd $dir --daemon --config vpn1.conf
#openvpn --cd $dir --daemon --config vpn2.conf
#openvpn --cd $dir --daemon --config vpn2.conf
```

In a future step we will modify the firewall ourselves.

### 15. Modify the *server.conf* file.

It must contain at least the following entries:

```
[root@openvpn openvpn]# vi server.conf
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key # This file should be kept secret
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.0.0 255.255.255.0"
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

### 16. Copy the files *ca.crt*, *server.crt*, *server.key* and *dh1024.pem* from directory */etc/openvpn/keys* to directory */etc/openvpn*:

```
[root@openvpn openvpn]# cd /etc/openvpn/keys
[root@openvpn keys]# cp -pv ca.crt server.crt server.key dh1024.pem /etc/openvpn
'ca.crt' -> `/etc/openvpn/ca.crt'
'server.crt' -> `/etc/openvpn/server.crt'
'server.key' -> `/etc/openvpn/server.key'
'dh1024.pem' -> `/etc/openvpn/dh1024.pem'
```

### 17. Start the openvpn service:

```
[root@openvpn openvpn]# service openvpn start
Starting openvpn: [ OK ]
```

### 18. Make sure that the openvpn service is started on boot:

```
[root@openvpn openvpn]# chkconfig openvpn on
[root@openvpn openvpn]# chkconfig openvpn --list
openvpn          0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

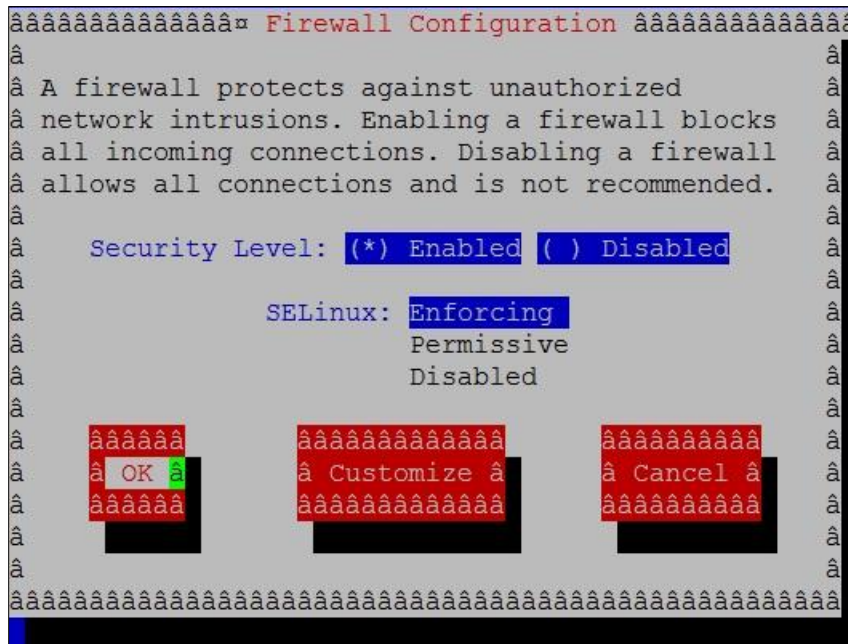
### 19. Check the results of the service startup in */var/log/messages*:

```
Jan  2 19:31:11 openvpn kernel: tun: Universal TUN/TAP device driver, 1.6
Jan  2 19:31:11 openvpn kernel: tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
Jan  2 19:31:11 openvpn openvpn[3840]: OpenVPN 2.0.9 x86_64-redhat-linux-gnu [SSL] [LZO]
[EPOLL] built on Mar  8 2007
Jan  2 19:31:11 openvpn openvpn[3840]: Diffie-Hellman initialized with 1024 bit key
Jan  2 19:31:11 openvpn openvpn[3840]: TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0
EL:0 ]
Jan  2 19:31:11 openvpn openvpn[3840]: TUN/TAP device tun0 opened
Jan  2 19:31:11 openvpn openvpn[3840]: /sbin/ip link set dev tun0 up mtu 1500
Jan  2 19:31:11 openvpn openvpn[3840]: /sbin/ip addr add dev tun0 local 10.8.0.1 peer
10.8.0.2
Jan  2 19:31:11 openvpn openvpn[3840]: /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
Jan  2 19:31:11 openvpn openvpn[3840]: Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135
ET:0 EL:0 AF:3/1 ]
Jan  2 19:31:11 openvpn openvpn[3845]: UDPv4 link local (bound): [undef]:1194
Jan  2 19:31:11 openvpn openvpn[3845]: UDPv4 link remote: [undef]
Jan  2 19:31:11 openvpn openvpn[3845]: MULTI: multi_init called, r=256 v=256
Jan  2 19:31:11 openvpn openvpn[3845]: IFCONFIG POOL: base=10.8.0.4 size=62
Jan  2 19:31:11 openvpn openvpn[3845]: IFCONFIG POOL LIST
```





Add the following to the Other ports section: 1194:udp.  
Click **OK**



Click **OK**

## 22. Check if the new rule is accepted

```
[root@openvpn ~]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination
1  RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination
1  RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination

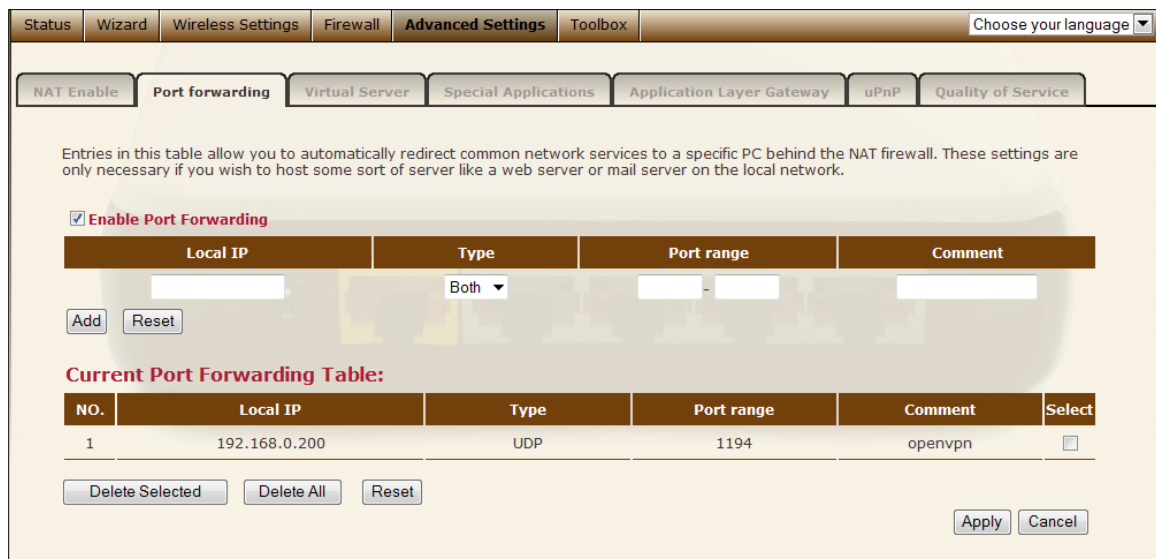
Chain RH-Firewall-1-INPUT (2 references)
num target      prot opt source                destination
1  ACCEPT       all  --  0.0.0.0/0            0.0.0.0/0
2  ACCEPT       icmp --  0.0.0.0/0            0.0.0.0/0            icmp type 255
3  ACCEPT       esp  --  0.0.0.0/0            0.0.0.0/0
4  ACCEPT       ah   --  0.0.0.0/0            0.0.0.0/0
5  ACCEPT       udp  --  0.0.0.0/0            224.0.0.251          udp dpt:5353
6  ACCEPT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:631
7  ACCEPT       tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:631
8  ACCEPT       all  --  0.0.0.0/0            0.0.0.0/0            state
RELATED,ESTABLISHED
9  ACCEPT       udp  --  0.0.0.0/0            0.0.0.0/0            state NEW udp
dpt:1194
10 REJECT       all  --  0.0.0.0/0            0.0.0.0/0            reject-with
icmp-host-prohibited
```

The configuration of the OpenVPN server is finished. The next step is to install and configure the client.

## Opening the OpenVPN port on your Router

To make sure that you can connect to your OpenVPN server from the internet, you must redirect port 1194 on your router to your OpenVPN server. I for example have a Sitecom wireless router. I will describe how I configured this router.

- Login to the administrator page of your router
- Select the Advanced Settings and select Port forwarding
- Tick Enable Port Forwarding
- Fill in the following entries:
  - Local IP: 192.168.0.200 (use the ip-address of your OpenVPN server)
  - Type: UDP
  - Port range: 1194
  - Comment: openvpn
- Click on the Add button to effectuate the changes
- Click on the Apply button
- You're Router will be restarted to make the changes permanent



The screenshot shows the 'Advanced Settings' page of a router, specifically the 'Port forwarding' section. The 'Enable Port Forwarding' checkbox is checked. Below this, there is a form to add a new port forwarding rule. The 'Current Port Forwarding Table' shows one existing rule with the following details:

NO.	Local IP	Type	Port range	Comment	Select
1	192.168.0.200	UDP	1194	openvpn	<input type="checkbox"/>

Buttons for 'Add', 'Reset', 'Delete Selected', 'Delete All', 'Reset', 'Apply', and 'Cancel' are visible at the bottom of the form.

If you're using another router you must check the documentation of that router, how to map ports to particular servers.

## Installation and configuration of OpenVPN on Windows

OpenVPN is an OpenVPN Graphic User Interface (GUI) for Window. The installation is very straightforward can be done just like installing any other program on Windows.

1. Download the program at [OpenVPN](#). I downloaded openvpn-2.1.1-install.exe. Of this version I know it works well op Windows 7.
2. Dubbel-click on the downloaded exe file start the installation. Accept all default values to install successfully.

After the installation a OpenVPN GUI icon is placed on your desktop.

3. The configuration files for OpenVPN are placed in the directory *C:\Program Files (x86)\OpenVPN\config*. Open the file *client.ovpn* in your favorite editor.

Make sure that the configuration file contains at least the following entries:

```
client
dev tun
proto udp
remote <ip-address of your internet connection at home> 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
comp-lzo
verb 3
```

The ip-address of your internet connection can be determined with the help of the website <http://whatismyipaddress.com/>. The ip-address is shown in blue at the right.

4. Copy the following files from your OpenVPN server to your laptop/desktop computer:
  - ca.crt
  - client1.crt
  - client1.key

These files are located at the */etc/openvpn/keys* directory. The must be copied to the directory *C:\Program Files (x86)\OpenVPN\config*. I always use WinSCP for copying files between Linux and Windows.

Once the files are copied to the right location, you can test your VPN connection.

5. On the OpenVPN GUI icon, click with the right mouse on the OpenVPN GUI icon on the taskbar and click on Connect.

If you're tunnel is working, you should see receive a message that a connection is made to an ip-address like 10.8.0.6.

## Remotely connect to your virtual machines

Make sure that on your other systems, which you want to connect to remotely, a route is added. In my example I've added a route for the network segment 10.8.0.0 to 192.168.0.200 (my OpenVPN server).

A route can be created by creating the file `/etc/sysconfig/network-scripts/route-eth0` with the following entries:

```
[root@servername]# vi /etc/sysconfig/network-scripts/route-eth0
GATEWAY0=192.168.0.200
NETMASK0=255.255.255.0
ADDRESS0=10.8.0.0
```

GATEWAY0 is the server you installed the OpenVPN packages on.

NETMASK0 is the netmask of your network network.

ADDRESS0 is the range the OpenVPN uses. Default this is 10.8.0.0.

After you have created the file you can activate it by executing the following command:

```
[root@servername network-scripts]# /etc/sysconfig/network-scripts/ifup-routes eth0
RTNETLINK answers: File exists
```

Check this with the route command:

```
[root@servername network-scripts]# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
10.8.0.0         192.168.0.200  255.255.255.0  UG    0      0      0 eth0
192.168.0.0     *                255.255.255.0  U      0      0      0 eth0
169.254.0.0     *                255.255.0.0    U      0      0      0 eth0
default         192.168.0.1    0.0.0.0        UG    0      0      0 eth0
```

As from now you can remotely connect to your server.