# Open VPN :-

Required machines

1. VPN server - centos - NAT - 192.168.44.160
   Host-only - 10.10.10.132
2. VPN Client1 - Centos - NAT - 192.168.44.139
3. VPN client2 - windows - Host-only - 10.10.10.133

In VPN server machine :-

```
# vi /etc/selinux/config
  ↳ SELINUX= disabled

# echo 1 > /proc/sys/net/ipv4/ip_forward

# vi /etc/sysctl.conf
  ↳ net.ipv4.ip_forward = 1

# yum install epel-release

# yum install openvpn

# cd /etc/openvpn/

# wget https://github.com/OpenVPN/easy-rsa/releases/
  download/V3.0.6/EasyRSA-Unix-v3.0.6.tgz

# tar -xvzf EasyRSA-unix-v3.0.6.tgz

# mv EasyRSA-unix-v3.0.6# easy-rsa
```

```
#cd easy-rsa
 #cat vars.example
 # vi vars
```

↳ copy lines from tech-admin.net open VPN installation parameters.

```
# ./easyrsa init-pki
# ./easyrsa build-ca
```

↳ set password - hpcsa

set Common name - open-vpn-server (CA Name)

pki/ directory will be created

```
# ls pki/
```

↳ there is ca certificate file "ca.crt" & private key "ca.key"

- Now Generate server certificate files.

```
# ./easyrsa gen-req demovpn nopass
```

demovpn → actual server

nopass → (No password while login)

- Now sign the server key using CA

```
# ./easyrsa sign-req server demovpn
```

↳ confirm request = yes

password = hpcsa

```
# cat pki/issued/demovpn.crt
```
↳ now you can see the certificate

```
# openssl verity -CAfile pki/ca.crt pki/issued/
                                       demovpn.crt
```
↳ certificate ok

```
# ./easyrsa gen-dh
```
– generate astrong a strong Deffie-Hellman key use for key exchange

```
# cp pki/ca.crt /etc/openvpn/server/
# cp pki/dh.pem /etc/openvpn/server/
# cp pki/private/demovpn.key /etc/openvpn/server/
# cp pki/issued/demovpn.crt /etc/openvpn/server/
```

Now Generate client certificate & key file

```
# ./easyrsa gen-req client nopass
                    user
```
↳ Enter client host name – vpnclient

Now ~~sino~~ sign the client key using CA certificate

```
# ./easyrsa • sign-req client client
                              user
```
↳ contirm request details = yes

password = hpcsa

Now copy all client certificate to client directory

```
# cp pki/ca.crt /etc/openvpn/client/
# cp pki/issued/client.crt /etc/openvpn/client/
# cp pki/private/client.key /etc/openvpn/client/
```

Now configure VPN server.

```
# vi /etc/openvpn/server/server.conf
```

↳ copy lines from tech-admin.net open vpn installation step-8

```
#systemctl start opevpn-server@server
# systemctl enable openvpn-server@server
```

```
# systemctl start firewalld.service
# systemctl enable firewalld.service
```

```
# firewall-cmd --permanent --add-service=openvpn
# firewall-cmd --permanent --zone=trusted --add-
                                        service=openvpn

# firewall-cmd --permanent --zone=trusted --add-
                                        Interface=tun0

# firewall-cmd --add-masquerade
# firewall-cmd --permanent --add-masquerade
# firewall-cmd --permanent --direct --passthrough
  ipv4 -t nat -A ~~Postr~~ POSTROUTING -s 10.8.0.0/24
  -o ens3 -j MASQUERADE
     Net. interface
```

```
# Firewall-cmd --reload
```

Now Generate client Configuration File

```
# vi /etc/openvpn/client~~-ovpn~~/client.ovpn
```

↳ copy step 10 from techadmin.net open-vpn

```
# scp -r /etc/openvpn/client root@192.168.44.139:/root
```

On centos client machine :-

Now change Network setting to manual ~~give~~ & give ip address same as previous 192.168.44.139 & subnet mask - 255.255.255.0, Dont give DNS & Getwa

then it shouldn't ping to windows client

```
# yum install epel-release
# yum install openvpn
# cd /root/client/
# openvpn --config client.ovpn
```

now open new terminal & run command "ip a" 'tun0' adapter is added. Now press 'Ctrl c'

Now in VPN server

```
# ~~cat~~ vi /etc/openvpn/server/server.conf
```

↳ push "route 10.10.10.0 255.255.255.0"

add this line — 10.10.10.0 windows ip's network

```
# systemctl restart openvpn-server@server.service
```

Now on vpn client linux.

```
# openvpn --config client.ovpn
# route -n
```

↳ now 10.10.10.0 Distination route is reflecting in ip routing table