

Forum:[Hack Forums](#)

Thread: [How to install and setup OpenVPN on CentOS 6 32 bit](#)

Bosto - September 25, 2014, 5:01 pm

Requirements :CentOS 6 32 bit VPS

512 MB RAM

TUN/TAP Support

Putty

Step 1.

Connect to your VPS through putty and check if TUN/TAP is enabled on your virtual private server. Use this command to check. Quote:cat /dev/net/tun
If enabled, it will return "File descriptor in bad state."

Step 2.

You will now have to install OpenVPN which can be completed through this command. Quote:yum install gcc make rpm-build autoconf.noarch zlib-devel pam-devel openssl-devel -y
You will get a response from your virtual private server saying "Complete!."

Step 3.

Now we will have to install LZO RPM and the TPMForge Repo packages. This can be accomplished by this command. Quote:wget <http://openvpn.net/release/lzo-1.08-4.rf.src.rpm>

wget <http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-1.el6.rf.i686.rpm>

Step 4.

After installing the above packages, you will now run these three commands in order. Quote:
rpmbuild --rebuild lzo-1.08-4.rf.src.rpm

rpm -Uvh lzo-*.rpm

rpm -Uvh rpmforge-release*

Now you are able to update your virtual private server by entering "yum update -y"

Step 5.

Now your virtual private server will install OpenVPN. Install by running the command below. Quote:yum install openvpn -y

Next step is to create the security certificate.

Quote:cp -R /usr/share/doc/openvpn-2.2.2/easy-rsa/ /etc/openvpn/ /etc/openvpn/

Step 6.

Now we have to edit the key file but don't worry this is very simple!

Quote:vi /etc/openvpn/easy-rsa/2.0/vars

Now change this line "export KEY_CONFIG=`\$EASY\_RSA/whichopensslcnf \$EASY\_RSA`" to "export KEY_CONFIG=/etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf" Now save the file by hitting ESC and left Shift + ZZ.

Step 7.

We will now need to create the certificate so your users will be able to connect to the OpenVPN through your VPS.

Quote:cd /etc/openvpn/easy-rsa/2.0 give files the permission - chmod 755

Now all you have to do is enter the command "./build-ca" and you have now created the certificate! You will have to enter information but the information doesn't matter so put whatever you want. Now we will need to create the key.

Quote:./build-key-server server

Common Name: your vps hostname

Challenge password: optional

Company name: optional

certificate: y

certificate requests: y

Step 8.

Now enter this command to create the ovpn file.

Quote:./build-dh

Now we need to enable IP Forwarding by doing the following: vi /etc/sysctl.conf

Change "net.ipv4.ip_forward = 0" to "net.ipv4.ip_forward = 1" Use the ESC key and do shift + zz to save. In order to make the changes have effect on the vps, enter "sysctl -p"

Step 9.

Onto the next step! We now need to edit the server configuration file so OpenVPN will work correctly with your VPS. To create the configuration file, enter this.

Quote:touch /etc/openvpn/server.conf

Now edit:

vi /etc/openvpn/server.conf

Copy the text in the configuration file and save it as a .conf file and upload it to your vps /etc/openvpn/ directory through FTP. (FileZilla)

Quote:port 1194 #- port

proto udp #- protocol

dev tun

tun-mtu 1500

tun-mtu-extra 32

mssfix 1450

reneg-sec 0

ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt

cert /etc/openvpn/easy-rsa/2.0/keys/server.crt

key /etc/openvpn/easy-rsa/2.0/keys/server.key

dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem

client-cert-not-required

username-as-common-name

server 10.8.0.0 255.255.255.0

```
push "redirect-gateway def1"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 5 30
comp-lzo
persist-key
persist-tun
status 1194.log
verb 3
```

Now to start OpenVPN, enter this "service openvpn start". You should see an OK! No errors.

Step 10.

Your virtual private server needs iptables in order for users to connect to the VPN. Enter the following to add!

```
Quote:iptables -t nat -A POSTROUTING -o venet0 -j SNAT --to-source YOUREXTERNALIP
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source YOUREXTERNALIP
```

Now enter this command: "service iptables save"

Then enter this command to automatically startup your server: "chkconfig openvpn on"

Now you are done! All you need to do is send your customer or friend the ovpn file and certificate file! Below is the ovpn file you will create!

```
Quote:client
dev tun
proto udp
remote YOURVPSIP 1194 # - Your server IP and OpenVPN Port
resolv-retry infinite
nobind
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
persist-key
persist-tun
ca ca.crt
auth-user-pass
comp-lzo
reneg-sec 0
verb 3
```

Now navigate to the directory "etc/openvpn/easy-rsa/2.0/keys/" to get your certificate. (Use filezilla to accomplish this)

MISC:

Spoiler ([Click to View](#))

Add user:

```
adduser "username" -s /bin/false/nologin
```

Set password:

```
passwd "username"
```

Delete user:

```
userdel "username"
```

Port Forward:

```
iptables -I INPUT -p udp -m udp --dport 1194 -j ACCEPT
```