

Forum:[Hack Forums](#)

Thread: [How to setup an OpenVPN Server](#)

Cyph Jr - December 14, 2014, 2:46 pm

This thread will teach you how to set-up and configure a OpenVPN server on CentOS 6. This tutorial will also teach you how to configure your Windows, OSX, or Linux client to connect to your OpenVPN Server. Before we begin, you'll need to have the Extra Packages for Enterprise Linux (EPEL) Repository enabled on your server. To do this, we're going to want to enter in the following commands on our CentOS Server.

PHP Code

```
<?php
wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
rpm -Uvh epel-release-6-8.noarch.rpm
```

Now that we've downloaded the EPEL Repository we're going to want to install the OpenVPN package from EPEL, to do so, we're going to want to execute the following commands

PHP Code

```
<?php
cp /usr/share/doc/openvpn-*/sample-config-files/server.conf /etc/openvpn
```

Now that we've moved our file in the proper location, we are going to want to open the file for editing to make it configured to our server. To do so, we're going to want to use the text editor of our personal preference, I am going to be using "nano" as it's installed on nearly every GNU/Linux system. We're going to want to execute the following command

PHP Code

```
<?php
nano -w /etc/openvpn/server.conf
```

Our first change we're going to want to make will be to un-comment the "push" parameter which causes traffic on our client systems to be routed through OpenVPN. To do this, we're going to want to execute the following command/line.

PHP Code

```
<?php
push "redirect-gateway def1 bypass-dhcp"
```

Normally that line is commented with a "#" at the beginning, we're going to want to remove it by simply finding the line in our configuration file and removing the "#". We'll also want to change the section that immediately follows route DNS queries to Google's Public DNS servers so our VPNs DNS servers don't go down, Google servers are very reliable to use as DNS servers. You can feel free to use any DNS server although I personally recommend using Google's.

PHP Code

```
<?php
push "dhcp-option DNS 8.8.8.8"
```

```
push "dhcp-option DNS 8.8.4.4"
```

In addition, to enhance security, make sure OpenVPN drops privileges after startup. Uncomment the relevant "user" and "group" lines. This will ensure the fact that no one unless you are root/sudoer can execute root/sudoer commands on our server. Again, this is in the configuration file and we simply change it up a little.

PHP Code

```
<?php
user nobody
group nobody
```

Now that we've finished modifying the configuration file, we'll generate the required keys and certificates. As with the configuration file, OpenVPN places the required scripts in the documentation folder by default. Create the required folder and copy the files over.

PHP Code

```
<?php
mkdir -p /etc/openvpn/easy-rsa/keys
cp -rf /usr/share/openvpn/easy-rsa/2.0/* /etc/openvpn/easy-rsa
```

With the files in the desired location, we'll edit the "vars" file which provides the easy-rsa scripts with required information. Now, following my php codes you can see the commands to execute to do a specific job that I describe in the little disclaimer part or this part instead. Now again, I am using nano in this example because it's pre-installed on nearly every GNU/Linux system, but you can use the text-editor of your choice.

PHP Code

```
<?php
nano -w /etc/openvpn/easy-rsa/vars
```

We're looking to modify the "KEY_" variables, located at the bottom of the file. The variable names are fairly descriptive and should be filled out with the applicable information. After you've done this, your vars folder should look similar to this. Please note that this part is very crucial to follow in-depth, if not, it can ruin your configuration of keys.

PHP Code

```
<?php
export KEY_COUNTRY="US"
export KEY_PROVINCE="NY"
export KEY_CITY="New York"
export KEY_ORG="Organization Name"
export KEY_EMAIL="cyph@nahh.com"
export KEY_CN=cyphjr.example.com
export KEY_NAME=server
export KEY_OU=server
```

Now we're going to want to manually copy the required OpenSSL configuration file. To do so, we're going to want to execute the following command below. Please note that this a precaution so OpenSSL isn't failed to be detected.

PHP Code

```
<?php
```

```
cp /etc/openvpn/easy-rsa/openssl-1.0.0.cnf /etc/openvpn/easy-rsa/openssl.cnf
```

[img]http://remibergsma.files.wordpress.com/2013/01/openvpn-secure-wifi-browsing4.png?w=580[/img]

We'll now change into our working directory and build our Certificate Authority, or CA, based on the information as the information that I've provided above of this..

PHP Code

```
<?php
cd /etc/openvpn/easy-rsa
source ./vars
./clean-all
./build-ca
```

Now that we have our CA, we'll create our certificate for the OpenVPN server. When asked by build-key-server, answer yes to commit. We're also going to need to generate our Diffie Hellman key exchange files using the build-dh script and copy all of our files into /etc/openvpn as follows

PHP Code

```
<?php
./build-key-server server
./build-dh
cd /etc/openvpn/easy-rsa/keys
cp dh1024.pem ca.crt server.crt server.key /etc/openvpn
```

In order to allow clients to authenticate, we'll need to create client certificates. You can repeat this as necessary to generate a unique certificate and key for each client or device.

PHP Code

```
<?php
cd /etc/openvpn/easy-rsa
./build-key client
```

We're going to want to Create an iptables rule to allow proper routing of our VPN subnet and then enable IP Forwarding in sysctl. To do so, we're going to want to execute the following commands as listed.

PHP Code

```
<?php
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
service iptables save
```

This part will create a iptable that allows users to connect to your VPN server and then the iptables save will save iptables so if you re-start your server, it's automatically saved and already configured.

PHP Code

```
<?php
nano -w /etc/sysctl.conf
```

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

Finally, apply our new sysctl settings. Start the server and assure that it starts automatically on boot

PHP Code

```
<?php  
sysctl -p  
service openvpn start  
chkconfig openvpn on
```

Now you finally have a working OpenVPN server. I will be following up with a tutorial shortly on how to configure your OpenVPN client to connect to the OpenVPN server although it's very basic and easy to understand. If you have any questions or concerns regarding this tutorial, please feel free to post below or PM me and I'll assist you to the best of my ability. Thank you and have a fantastic day.

Tirus - December 14, 2014, 2:48 pm

Nice little tutorial you've made, Cyph Jr. Keep up the good work. How about a tutorial on how to secure an OpenVPN Server?

Cyph Jr - December 14, 2014, 2:50 pm

(Dec 14, 2014 03:48 PM)Tirus Wrote: [\[CITE\]](#) Nice little tutorial you've made, Cyph Jr. Keep up the good work. How about a tutorial on how to secure an OpenVPN Server?
I will do a tutorial on that subject next.

Dum De Dum - December 14, 2014, 2:57 pm

Pretty detailed tut there, nice work keep it up.

CatSoup - December 14, 2014, 2:58 pm

Wow this is a really HQ tutorial.

You seem like a hacker. ?

Zen - December 14, 2014, 3:20 pm

very hq guide m8 will help many users out

Billie Joe - December 14, 2014, 3:21 pm

Very hq guide thanks for this cyphy

Cyph Jr - December 14, 2014, 3:30 pm

You can find how to secure an OpenVpn server [here](#)

Arzel - December 14, 2014, 3:40 pm

cyph is very hq very detailed tutorials good job

Crystallmethod - December 14, 2014, 5:22 pm

Working on both of these right now and this was about what I was looking for, Great information here. Thanks alot Cyph, for the in depth tut.

Cyph Jr - December 14, 2014, 5:39 pm

(Dec 14, 2014 06:22 PM)Crystallmethod Wrote: [\[CITE\]](#) Working on both of these right now and this was about what I was looking for, Great information here. Thanks alot Cyph, for the in depth tut.
I'm glad that this tutorial could help you.

Ghostshrimpx - December 14, 2014, 8:29 pm

This was exactly what I was looking for, thanks!

Revamp - December 14, 2014, 9:22 pm

Wow, Nice tut dude.

Note: "iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE"
only works on XEN/KVM VPS.

If someone is installing it on OpenVZ, they would need this command

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to SERVERIP

Cyph Jr - December 15, 2014, 4:19 am

(Dec 14, 2014 10:22 PM)?C??c??? Wrote: [\[CITE\]](#) Wow, Nice tut dude.

Note: "iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE"
only works on XEN/KVM VPS.

If someone is installing it on OpenVZ, they would need this command

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to SERVERIP

Thanks for that I will add it to the thread asap.

The_Defiant_One - December 15, 2014, 3:35 pm

Nice tutorial here. Thanks for sharing.

Cyph Jr - December 16, 2014, 10:11 pm

Thanks for your feedback everyone, looking for ideas on a next guide.

Cyph Jr - December 17, 2014, 6:05 pm

(Dec 17, 2014 01:50 PM)3ggy Wrote: [\[CITE\]](#) nice tut very interesting thanks for this

Thanks for your opinion, I'm happy to help people.

guycheap - December 23, 2014, 11:18 pm

Well done. I did see a few errors and fixes that can make life easier, I'll edit this post once I get a chance.

Cyph Jr - December 24, 2014, 7:01 am

(Dec 24, 2014 12:18 AM)guycheap Wrote: [\[CITE\]](#) Well done. I did see a few errors and fixes that can make life easier, I'll edit this post once I get a chance.

Thanks that would be really appreciated.

guycheap - December 24, 2014, 1:25 pm

You need to make sure these packages are installed:

Code yum install gcc make rpm-build autoconf.noarch zlib-devel pam-devel openssl-devel -y
Transfer all the files over :P:

Code cp -R /usr/share/doc/openvpn-*/easy-rsa/ /etc/openvpn/

You can use this as the default server.conf it makes life much easier:

Code 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
plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so /etc/pam.d/login #- Comment this line if
you are using FreeRADIUS
#plugin /etc/openvpn/radiusplugin.so /etc/openvpn/radiusplugin.cnf #- Uncomment this line if you
are using FreeRADIUS
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
You no longer need this: Code mkdir -p /etc/openvpn/easy-rsa/keys
cp -rf /usr/share/openvpn/easy-rsa/2.0/* /etc/openvpn/easy-rsa
This is not needed:
```

Code nano -w /etc/openvpn/easy-rsa/vars
You can run these commands and be on your way:

```
Code cd /etc/openvpn/easy-rsa/2.0
chmod 755 *
source ./vars
./vars
./clean-all
Quote:cd /etc/openvpn/easy-rsa/keys
It's either /etc/openvpn/2.0/keys OR /etc/openvpn/easy-rsa/2.0/keys.
```

These IPTable commands can make life easier:

Simply open up /etc/sysconfig/iptables by - nano /etc/sysconfig/iptables & look for " Output Accept "
stick these lines right under it remember to change your server IP:

```
Code -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
-A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
-A POSTROUTING -o venet0 -j SNAT --to-source SERVER IP
-A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source SERVER IP
-A POSTROUTING -o eth0 -j MASQUERADE
-A POSTROUTING -o eth0 -j MASQUERADE
Sometimes the PAM package fails and we get the erro
```

Code PLUGIN_INIT: could not load plugin shared object
/usr/share/openvpn/plugin/lib/openvpn-auth-pam.so:
/usr/share/openvpn/plugin/lib/openvpn-auth-pam.so: cannot open shared object file: No such file or
directory
in /var/log/messages while starting up the VPN.

Run wget <https://www.dropbox.com/s/z9lulk005z3qvqj/openvpn-auth-pam.zip?dl=0> to download it (64 bit) and then run unzip openvpn-auth-pam.zip to unzip it. Transfer the files over to the proper folder: mv openvpn-auth-pam.so /etc/openvpn/openvpn-auth-pam.so

then replace the line

Code plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so /etc/pam.d/login with Code plugin /etc/openvpn/openvpn-auth-pam.so /etc/pam.d/login in your server.conf at /etc/openvpn/server.conf by using nano or any other editor. You will also need to kill all OpenVPN Processes, run killall -9 openvpn then service openvpn restart. That should do the trick..

That's all I found for now, sorry for being so messy :P.

Cyph Jr - December 24, 2014, 1:39 pm

(Dec 24, 2014 02:25 PM)guycheap Wrote: [\[CITE\]](#) SnippityI'll make the adjustments when I get the chance. Thanks for the improvements :).

guycheap - December 24, 2014, 1:41 pm

(Dec 24, 2014 02:39 PM)Cyph Jr Wrote: [\[CITE\]](#) I'll make the adjustments when I get the chance. Thanks for the improvements :).

No problem :) glad I could help man.

super666atheist - December 25, 2014, 4:32 am

i'm wondering if this thing works on mobile phones.

n0rtr3x - December 26, 2014, 4:16 am

It's a really useful tut. Thank you :)

Emigrantoz - December 27, 2014, 2:12 pm

Thanks for this! , could u PM me your skype? , I've got a serveral questions.. about your Booter/Stresser.

Much easier then a ticket.

thanks in advance