Control Panel Setup

Once you've purchased a server it takes around 3-4 minutes for an email to arrive with details to access the control panel. After logging in you'll be greeted by this page:

Status	Online		Op	perating System	CentOS 7 64bit Minimal	
IPv4 Address	1			IPv6 Address	1	
IP Address				Disk Space	3 GB	
Virtualization Type	(OpenVZ)			Bandwidth	125 GB	
Hostname				Memory	128 MB	
Node	CA-VZ1			VSwap	0 KB	
Bandwidth Usage			1.05 GB of 125 GB Used / 123.95 GB Free			
Memory Usage	9%		11.65 MB of 128 MB Used / 116.35 MB Free			
VSwap Usage			0 KB of 0 KB Used / 0 KB Free			
Disk Usage	21%		640.03 MB of 3 GE		GB Used / 2.37 GB Free	

If you scroll down, you'll want to make sure TUN/TAP is turned on (It'll most likely be off by default)

Settings	Hostname	Root/Admin Password	Network	API	Statistics
TUN/	TAP				
On		\$			
PPP					
011					

I'd also recommend adding a new hostname and a **strong** root password.

Settings	Hostname	Root/Admin Passwo	Settings	Hostname	Root/Admin Password	Net
New Hostname			New Roo	t Password		
Change	e		Change	9		

Now is when I reinstalled the system OS to make sure all those changes have updated. This can be done via the reinstall button



Now I'd normally use Ubuntu cause that's what I'm most familiar with however after trying multiple times with no success I quickly gave up on Ubuntu and tried Cent OS. The first few attempts didn't work but now I've got it working with "CentOS 7 64bit Minimal"

0



So, pick that one then click "reinstall" at the bottom. You'll be asked to confirm and then you'll need to wait for around 5 minutes before doing anything.

SSH into VPS

Now you should be able to SSH into your VPS. Big thing to note is the port

ssh root@???.???.??? -p ?????

This should now just give you an SSH window logged in as root.



Installing OpenVPN

The first thing that is recommended is a quick update (which might take a while... mine had 271 updates to run)

yum update

Then fetch the script for installing OpenVPN

```
wget https://raw.githubusercontent.com/Angristan/openvpn-
install/master/openvpn-install.sh -0 centos7-vpn.sh
```

Then give the script permissions to run

```
chmod +x centos7-vpn.sh
```

and finally run the script

```
bash ./centos7-vpn.sh
```

You should get something that looks like this: (It'll most likely auto fill with the **internal IP address** and which point I just pressed enter)

```
[[root@ca ~]# bash ./centos7-vpn.sh
Welcome to the OpenVPN installer!
The git repository is available at: https://github.com/angristan/openvpn-install
I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.
I need to know the IPv4 address of the network interface you want OpenVPN listen
ing to.
Unless your server is behind NAT, it should be your public IPv4 address.
IP address:
```

It'll then ask for the Public IPv4 address (this can be found at link provided in the initial setup email)

```
It seems this server is behind NAT. What is its public IPv4 address or hostname?
We need it for the clients to connect to the server.
Public IPv4 address or hostname:
```

It'll then check for IPv6 compatibility and whilst you could run it on IPv6, I said no because neither my fixed ISP or mobile phone plan supports IPv6 so it's pointless to me.

```
Checking for IPv6 connectivity...
Your host appears to have IPv6 connectivity.
Do you want to enable IPv6 support (NAT)? [y/n]: n
```

Then you need to specify the port you wish to use

The setup email will provide a link to your external IP as well as a list of the ports you have access to. This will look something like: "Port Range : XXXXX to XXXXX"

Make sure you tell the OpenVPN server you wish to specify a port (Option 2)

```
What port do you want OpenVPN to listen to?

1) Default: 1194

2) Custom

3) Random [49152-65535]

Port choice [1-3]: 2
```

and then you need to specify the exact port you want to use (pick one from your range):

```
Custom port [1-65535]:
```

Most of the other questions will be the default option where it'll auto fill the value for you

Select number **1** for UDP:

```
What protocol do you want OpenVPN to use?

UDP is faster. Unless it is not available, you shouldn't use TCP.

1) UDP

2) TCP

Protocol [1-2]: 1
```

Pick a DNS provider... you can use the default server one or use something like Google or Cloudflare. Cloudflare (number **3**) is the default and uses the 1.1.1.1 server which you can read more about here https://l.1.1.1/dns/

```
What DNS resolvers do you want to use with the VPN?
1) Current system resolvers (from /etc/resolv.conf)
2) Self-hosted DNS Resolver (Unbound)
3) Cloudflare (Anycast: worldwide)
4) Quad9 (Anycast: worldwide)
5) Quad9 uncensored (Anycast: worldwide)
6) FDN (France)
7) DNS.WATCH (Germany)
8) OpenDNS (Anycast: worldwide)
9) Google (Anycast: worldwide)
10) Yandex Basic (Russia)
11) AdGuard DNS (Russia)
12) Custom
DNS [1-12]: 3
```

Select **no** to compression:

```
Do you want to use compression? It is not recommended since the VORACLE attack m ake use of it.
Enable compression? [y/n]: n
```

no to custom encryption settings:

```
Do you want to customize encryption settings?
Unless you know what you're doing, you should stick with the default parameters
provided by the script.
Note that whatever you choose, all the choices presented in the script are safe.
(Unlike OpenVPN's defaults)
See https://github.com/angristan/openvpn-install#security-and-encryption to lear
n more.
Customize encryption settings? [y/n]: n
```

It will the display the following message at which point you just press any key and then wait for the install

```
Okay, that was all I needed. We are ready to setup your OpenVPN server now.
You will be able to generate a client at the end of the installation.
Press any key to continue...
```

After a minute it will ask for a client name. You can use anything but I've just called mine "main"

```
Tell me a name for the client.
Use one word only, no special characters.
Client name: main
```

You'll then be asked if you want to add a password for the client. Whilst the default is a passwordless client, I'd recommend using a password that way if anyone ever gets hold of your connection file, they'll still need a password to connect to your VPN server.

```
Do you want to protect the configuration file with a password?
(e.g. encrypt the private key with a password)
1) Add a passwordless client
2) Use a password for the client
Select an option [1-2]: 2
```

It will then ask for the password twice (2nd time to verify).

```
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017
Generating a 256 bit EC private key
writing new private key to '/etc/openvpn/easy-rsa/pki/private/main.key
K'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

The server installation is now complete!

You can check the server status using the command

systemctl status openvpn@server

This should spit out that the server is now running:

```
    openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
Loaded: loaded (/etc/systemd/system/openvpn@.service; enabled; vendor preset: disabled)
Active: active (running) since Sat 2019-11-09 01:30:45 UTC; 3min 25s ago
```

Connecting to the server

In the process of installing the server you've just created a connection profile called main.opvn which is saved in the main root directory.

You should be able to see both the install script and the connection file by using the list directory command

ls

Which should display the following: [[root@ca ~]# 1s centos7-vpn.sh main.ovpn

You now need the main.ovpn file on your desktop or phone to connect. Unlike many other VPS servers there is no pre-installed FTP server which makes it harder to get that file and whilst you could setup a FTP server and port forward, I'm lazy and don't want to deal with the extra install involved in that process. Instead I'm just going to copy the text out of the install file. If you have SCP access you could use that however I'm not sure if it'll work with the limited ports available.

Being such a light OS there isn't text editor installed but you can install nano

yum install nano

This will ask you if the download size (around 1.6MB is ok) so just enter y

It should only take a few seconds and it'll then say "complete!"

It's now possible to open the OVPN configuration file with nano by entering

nano main.ovpn

You'll be greeted by the following which you can copy and paste into a text editor. I'm using sublime text and make sure you scroll down to capture it all. Make sure you don't copy the same line twice as it needs to match exactly (scroll down will still show some of the lines that you may have previously copied). Mine has 78 lines and it should be the same assuming you've entered a password for the configuration file.

gient presside dev tun resolv-retry infinite nobidd pressit-to resolv-retry infinite nobidd pressit-to resolv-central server verity	GNU nano 2.3.1	File: main.ovpn			
<pre>general op resolv-retry infinite nobid resolv-retry infinite nobid resolv-retry infinite resolv-retry infinite resolv-retry resolv-retry resolv-retry resolv-retry re</pre>	W1.2				
react and with monitor of the server windows the server wardy with SN256 auth-sace be considered to the server wardy wardy shares and the server	Ellent udp				
dev tun resolv-retry infinite nobid perisis-ky remote-cort-lis server verify- auth SN256 auth-socable cipher 14:18-000 tipher 14:	remote				
resolv-retry infinite nobid persist-key pe	dev tun				
nobid persist-Kup persist-Kup persist-Kup persist-Rup tointer trils erver auth SWA266 auth-Rocate cipher AES-128-CM tis-cipher t	resolv-retry infinite				
persist-Key persist-Key persist-ver verify auth-mozeche cipher AS-128-C0K tis-client tis-version-min 1.2 tis-version-min 1.2 t	nobind				
persat-tun reactive_fit_lis server reactive_fit_lis server reactive_	persist-key				
remote part - Lis server with SNASG auth-morache cipher AS-128-COM tis-client tis-version-sin 1.2 tis-cerision-sin 1.2 tis-ce	persist-tun				
auth SNASS6 cipher AIS-128-CGM tis-cipher tis-cursion=sin 1.2 tis-cipher setenv opt block-outside-dns # Prevent Windows 10 DNS leak verb 3 <begin certificate<br="">END CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE </begin>	verify-				
auth-morache cipher AE-128-COM tis-client tis-version-sin 1.2 tis-version-sin 1.2 tis-ve	auth SHA256				
cipher AES-128-CGM tis-cipher tis-cipher is-cipher seten vopt block-outside-dns # Prevent Windows 10 DNS leak vetb 3 <ca> END CERTIFICATE END CERTIFICATE </ca> BEGIN CERTIFICATE BEGIN CERTIFICATE Certs BEGIN CERTIFICATE	auth-nocache				
tis-client tis-version-sin 1.2 tis-version-sin 1.2 tis-version-sin 1.2 tis-version-sin 1.2 tis-version-sin 1.2 version-sin 1.2 version-	cipher AES-128-GCM				
tla-cupris saterv op t block-outside-dns # Prevent Windows 10 DNS leak verb 3 <a>EBOIN CERTIFICATE EBOIN CERTIFICATE <corts BEOIN CERTIFICATE <corts BEOIN CERTIFICATE </corts </corts 	tls-client				
<pre>Classing of block-outside-dns # Prevent Windows 10 DNS leak Serie 3 Serie 3 Serie 3 Serie 4 Serie</pre>	tls-version-min 1.2				
verb 3 <end certificate<br="">END CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE (cab BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE Composition BEGIN CERTIFICATE BEGIN CERTIFICATE</end>	catery ont block-outside_dos # Prevent Windows 18 DNS leak				
<pre></pre>	verb 3				
BEGIN CERTIFICATE END CERTIFICATE Cot Help Of the Prev Page Cut Text Cut Pos Cut Cut Pos	<ca></ca>				
END CERTIFICATE <certs BEGIN CERTIFICATE BEGIN CERTIFICATE</certs 	BEGIN CERTIFICATE				
Certificate					
END CERTIFICATE <certs BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE</certs 					
<pre>END CERTIFICATE </pre> <cortsbegin begin="" certificate="" certificate<="" td=""><td></td><td></td><td></td><td></td><td></td></cortsbegin>					
END CERTIFICATE <td></td> <td></td> <td></td> <td></td> <td></td>					
<pre></pre>					
END CERTIFICATE BEGIN CERTIFICATE BEGIN CERTIFICATE Cot Help WriteOut Exit Justify Where Is					
CERTIFICATE					
<pre>Capb CERTIFICATE </pre>					
<pre><cert>BEGIN CERTIFICATE BEGIN CERTIFICATE</cert></pre>					
BEGIN CERTIFICATE BEGIN CERTIFICATE G Get Help TO WriteOut RE Read File TO Prev Page RE Cut Text TO Cur Pos SE Exit Justify Where Is NO Next Page LE UnCut Text Ju To Spell	<cert></cert>				
NG Get Help NG WriteOut NG Read File NG Prev Page NG Cut Text NG Cur Pos 20 Exit S Justify NG Where Is NG Next Page NG UnCut Text NG To Spell	BEGIN CERTIFICATE				
TG Get Help TG WriteOut TE Read File TY Prev Page TK Cut Text TG Cur Pos NY Exit Justify TG Where Is NY Next Page TG UnCut Text Ty To Spell					
AG Get Help DG WriteOut BR Read File M Prev Page AK Cut Text AG Cur Pos 20 Exit D Justify AG Where Is MG Next Page AG UnCut Text AG To Spell					
NG Get Help TG WriteGut RE Read File NY Prev Page RK Cut Text NG Cur Pos SE Exit J Justify R Where Is NY Next Page LG UnCut Text NJ To Spell					
Re Get Help NG WriteOut RE Read File NY Prev Page NK Cut Text NG Cur Pos Mg Exit S Justify S Noter Is NN Next Page NU UnCut Text A∏ To Spell					
CG Get Help CG WriteOut CE Read File CM Prev Page CA Cut Text CG Cur Pos SE Exit D Justify CM Where Is CM Next Page CD UnCut Text CM To Spell					
NG Get Help 40 WriteOut 48 Read File 47 Prev Page 48 Cut Text 40 Cur Pos 12 Exit 43 Justify 44 Where Is 40 Next Page 40 UnCut Text 41 To Spell					
X Exit J Justify W Where Is V Next Page 4U UnCut Text 4T To Spell	Get Help WriteOut	Read File	AV Prev Page	AS Cut Text	Cur Pos
	A Justify	AW Where Is	AV Next Page	AU UnCut Text	AT To Spell

Once done you can exit the nano editor by pressing Control-X

Save this file from your text editor making sure to use the same name and extension **.ovpn** as its saved on the VPS.

Save As:	main.ovpn	
Tags:		
	🛅 Desktop	\$ •

Now you can open the file using your preferred OpenVPN client. On a Mac I use Tunnelblick however you can also a Mac or Windows client from the OpenVPN website https://openvpn.net/client-connect-vpn-for-windows/ or use the mobile apps for iOS or Android.

Tunnelblick prompts if you wish to install for all users or just yourself (your preference) and then after pressing connect you'll be asked for the profile password you setup during install.

Tunnelblick: Passphrase Required							
	A passphrase is required to connect to main						
Save in Ke	ychain						
	Cancel OK						

It should then be connected via your VPS server:



Status and Control Commands

If you want to stop the OpenVPN server use: systemctl stop openvpn@server

If you want to start the OpenVPN server use: systemctl start openvpn@server

If you want to restart the OpenVPN server use: systemctl restart openvpn@server

If you want to check the OpenVPN server is running use: systemctl status openvpn@server

Finally, on such a small server performance is often important. In standby (sleep mode) OpenVPN uses around 4% of the memory and 0% of the CPU.

This can be viewed by using the top command:

top

This will show something like this:

top -	02:04	:23 up	1:22	, 3 use	rs, loa	ad_ave	rag	e: 0.	00, 0	.00, 0.00
Tasks: 20 total,			1 r	unning,	19 slee	eping,		0 sto	pped,	0 zombie
%Cpu(s): 0.0 us,		.0 us,	0.0	0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0) hi, 0.0 si, 0.0 st		
KiB M	em :	131072	tota	total. 55952 free. 17828 used. 5				57292 buff/cache		
KiB S	wan:	9	tota	1	A free			A 115	ed.	55875 avail Mem
		-		-,		.,				
PID	USER	PR	NI	VIRT	RES	SHR	s	%CPU	%МЕМ	TIME+ COMMAND
1	root	20	0	43268	2904	1744	S	0.0	2.2	0:00.81 systemd
2	root	20	0	0	0	0	s	0.0	0.0	0:00.00 kthreadd/908
3	root	20		ñ	9		s	0.0	0.0	0:00.00 kbelper/908
82	root	20	ñ	36768	1876	1592	s	0.0	1.4	0:00.15 systemd-jout
126	dhus	20	ñ	26564	908	472	s	0.0	0 7	0:00 27 dbus-daemon
127	root	20		26364	100/	714	6	0.0	0.7	0:00.27 dbds-ddemon
127	1000	20		20346	1004	/10	0	0.0	0.0	0.00.00 systemu-rog+
135	root	20		0404	128	4	2	0.0	0.1	0:00.00 agetty
136	root	20	0	6404	128	4	s	0.0	0.1	0:00.00 agetty
686	root	20	0	41480	1164	760	s	0.0	0.9	0:00.00 systemd-ude+
840	root	20	0	112872	1460	428	S	0.0	1.1	0:00.00 sshd
1062	root	20	0	155300	2412	1052	s	0.0	1.8	0:00.04 sshd
1064	root	20	0	115400	768	372	S	0.0	0.6	0:00.00 bash
1080	root	20	0	113800	1260	332	s	0.0	1.0	0:00.00 bash
1094	root	20	0	155300	2496	1120	s	0.0	1.9	0:00.07 sshd
1096	root	20	0	115400	1436	1032	s	0.0	1.1	0:00.01 bash
1345	nobody	y 20	0	77384	5004	3816	s	0.0	3.8	0:00.39 openvpn
1498	root	20	0	115852	2708	1292	s	0.0	2.1	0:00.04 nano

To quit this screen just press **q**

With a single user connected this increase to around 0.3% of the CPU and still around 4% of the memory. Under a heavier load (a fast.com speedtest pulling 18mbps) this increases to around 7% of the CPU.