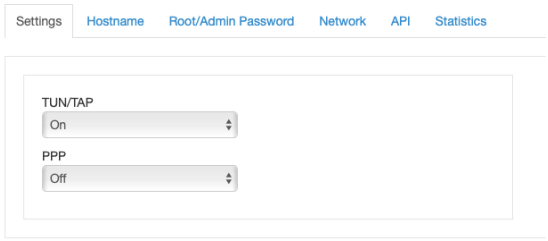
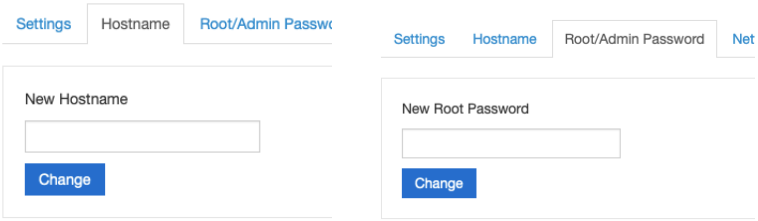
Control Panel Setup

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:

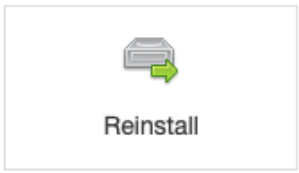
If you scroll down, you'll want to make sure TUN/TAP is turned on (It'll most likely be off by default)



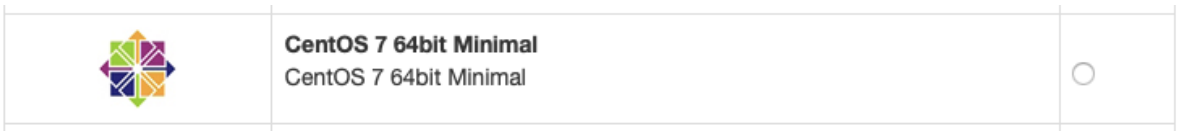
I'd also recommend adding a new hostname and a **strong** root password.



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"



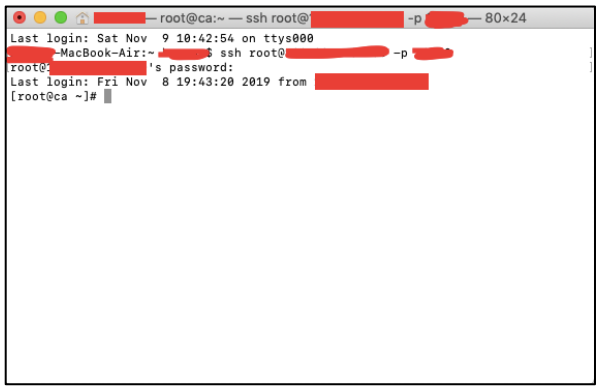
So, pick that one then click "reinstall" at the bottom. You'll be asked to confirm and then you'll need to wait for around 5 minutes before doing anything.

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 -O 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: [redacted]
```

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://1.1.1.1/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 ~]# ls
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
```

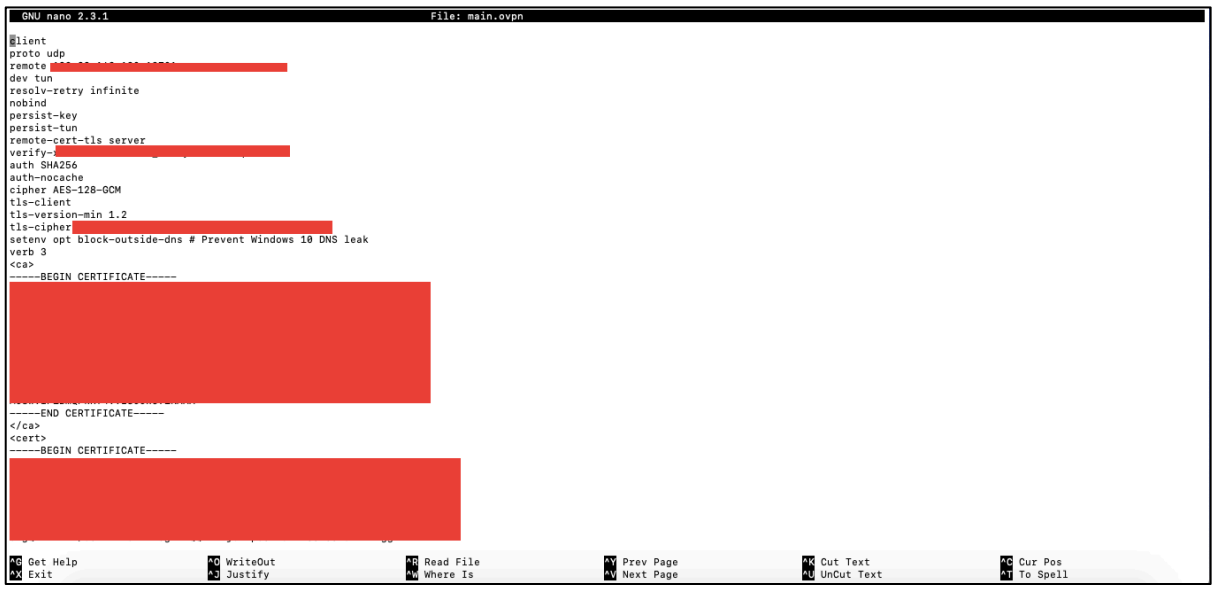
This will ask you if the download size (around 1.6MB is ok) so just enter **y**

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

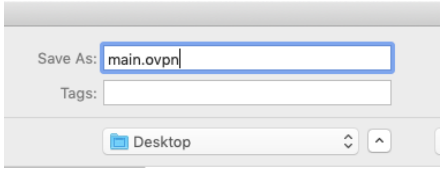
```
nano main.ovpn
```

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.



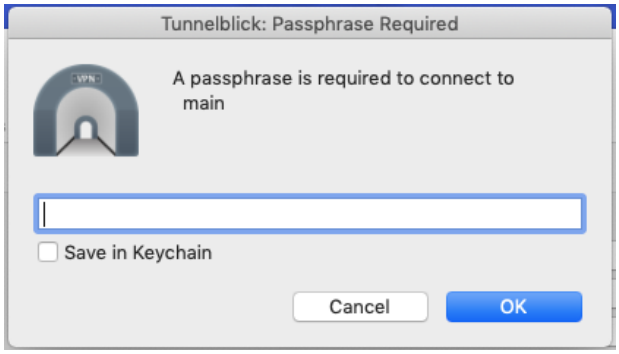
Once done you can exit the nano editor by pressing Control-X

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



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.



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:

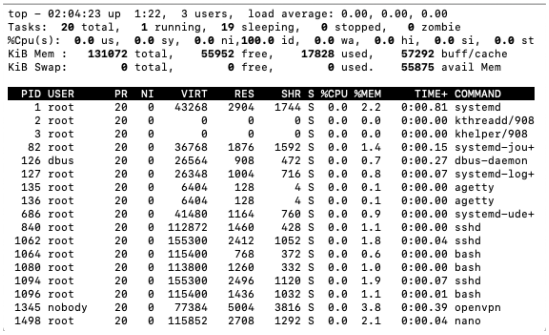
```
systemctl status openvpn@server
```

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 users,  load average: 0.00, 0.00, 0.00
Tasks:  20 total,   1 running,  19 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :   131072 total,    55952 free,    17828 used,    57292 buff/cache
KiB Swap:        0 total,        0 free,        0 used.    55875 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     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   0       0      0      0 S  0.0  0.0   0:00.00 khelper/908
   82 root      20   0   36768   1876   1592 S  0.0  1.4   0:00.15 systemd-jou+
  126 dbus      20   0   26564    908    472 S  0.0  0.7   0:00.27 dbus-daemon
  127 root      20   0   26348   1004    716 S  0.0  0.8   0:00.07 systemd-log+
  135 root      20   0    6404    128      4 S  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    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.