

Forum:[Hack Forums](#)

Thread: [\[Windows/iPhone/Mac/Linux/Android\] How to set up your own VPN server for \\$3 or less](#)

Marxist - July 13, 2017, 12:23 pm

Setting Up your Own Personal VPN And why it's important

With new laws coming into effect concerning digital privacy being behind a VPN is almost a must now, even in your own home. It is ALWAYS a must to use in public wifi, though. We've all seen tools like Cain & Abel, Kismet, the AirCrack suite, etc. You should all know your data is not secure.

Whether you're in a country that censors your internet, or you're in the US and Congress just passed a law allowing ISPs to [Sell your browsing history and much more](#) having a VPN is a must.

I want to compile this quick guide to show how easy it is to set up a cheap and efficient VPN, and how even you could do it too! To protect yourself and your families from security and privacy concerns!

This guide is going to cover Linux servers.

Now, why? Why host your own VPN? In all honesty, can you really trust VPN companies? Yes, there are some trustworthy ones. There are expensive ones, ones that claim to not keep logs or spy on you, etc. But can you really be sure? Paid/free VPNs have their place, but ultimately you do not control the data you are throwing into them. For sketchy activities using another VPN may be viable, as the increased amount of users adds to your entropy, but that is never a full-proof protection and shouldn't be relied on. This is more for protecting privacy, not hiding from law.

Step 1

Finding a host

Firstly, we need to take a look at hosting solutions. For a single user VPN the hardware is a non-issue.

I personally use a \$20 VPS from OVH and host 40+ people. Both CPU and RAM are almost unaffected by this load, added latency is negligible and the server has a 100Mbps throughput/unlimited bandwidth.

I also have several \$3 VPS hosted by OVH for load balancing, which all host anywhere between 10-15 people at a given time with negligible impact on processing.

I also rent from a few other companies around the globe. My users are generally in areas where speeds under 50kb/s, so they come nowhere near my server throughputs.

First, You need to ask yourself:

Do I need unlimited bandwidth?

What speeds am I looking at?

What is my under-load bandwidth requirements?

How much latency increase (ping) is considered negligible?

Why am I looking for protection?

DOES THE HOST HAVE TUN MODE

From here you need to do research on hosting solutions. Find hosts that meet your needs. Are you

looking to maintain privacy with your ISP? You may want to look into a hosting company outside of your country.

Is latency a concern and would hosting outside of your country cause too much of an issue? You can still host within your country and mitigate having your privacy infringed on. Generally hosting companies are in huge data centers with lots of data being sent through them. This at least adds increased entropy to the data you are transmitting and receiving while serving as getting it farther away from you and your ISP. You are still terminating in your country, though.

Really look into your requirements and research these companies. You need to make a security-conscious decision of where your data is going, how it's going to be processed, the laws of where it is exiting, and how much security vs. convenience you are willing to lean toward.

Another HUGE thing is, ask your host if TUN mode is enabled. Most major hosters will allow this. Smaller ones, you may need to ask.

FOR A LIST OF HOSTS THAT ACCEPT BTC:

<http://crypto.net/~joepie91/bitcoinvps.html>

Note: Some hosts may allow anonymous registration, some may not.

Step 2

Preparing your host for a VPN

Once you have your host selected, purchase a server in your desired location using your flavour of Linux. Debian would be a good beginner's choice. This guide is going to cover Linux servers.

First step, you need to update your package manager and upgrade your system. I will be using Debian for all examples after this.

Code # apt-get update # This updates your package manager with current up-to-date software in your repos

apt-get upgrade # This upgrades all packages on your system

reboot # This reboots your server

Step 3 - Installing the OpenVPN Services

And configuring them

Next, we will be using a script created by a Git user named Angristan. This script downloads the most current version of OpenVPN from official repositories, installs it, configures the server with your parameters, generates RSA keys, the certificate authority, creates users and updates the keys.

Here is the link to the official Git. To include source, so you can go through it yourself.

<https://github.com/Angristan/OpenVPN-install>

The above link covers instructions on the install, however I will also cover them here, covering the same topics and using his screenshots, as they would be identical even if I took them.

Firstly, we will need to download the script and run it. The following makes an openvpn directory in your home folder and moves to it. Then it downloads the script from the Git, and makes it executable (chmod). It then executes it.

I have you create its own folder because user .ovpn files are stored in the same directory as the

script. This will keep it neat.

Initially the script must be ran as root. PLEASE DO NOT BLINDLY RUN THIS, READ THROUGH THE SCRIPT. NEVER BLINDLY RUN SCRIPTS AS ROOT.

Code `cd ~/`

`mkdir openvpn`

`cd openvpn`

`wget https://raw.githubusercontent.com/Angristan/OpenVPN-install/master/openvpn-install.sh`

`chmod +x openvpn-install.sh`

`./openvpn-install.sh`

You will be prompted with this lovely screen.

- For most users you can simply press enter when it asks for the IPv4 address.
- When it asks for the port you may change it, and I would actually recommend changing it. Some ISPs or public Wifi spots can block this port, as it is the openVPN default used port.
- I personally select UDP. In today's internet networking there is VERY minimal packet loss. TCP in this situation would significantly increase network overhead and possibly slow down your speeds. We select UDP because TCP is an unneeded protocol in this application in today's world and we are trying to make this as seamless as possible for you.
- Next, it asks you for your DNS server. This is important, especially for privacy. Do your research on these DNS services prior to choosing them and choose the one that aligns to your philosophies and ordeals. For example, OpenDNS is huge on fighting for anti-censorship.

<https://www.opendns.com/about/anti-censorship-policy/>

Step 4

Choosing security options

Now, here's where the magic happens. This is where we decide how your data is secured, why you should make certain choices, and a few links to documentation concerning them.

You will be prompted with these options:

AES-CBC is what I personally recommend. It is less cpu intensive than it's counter parts, and secure. It's an industry standard, and you already use it everyday.

128, 192, or 256? Basically, the higher the blocksize the more "rounds" AES runs your data through to encrypt and decrypt. The more rounds, the longer it takes to do. This is also more intensive on CPU processing on both the client and server, but is extremely negligible. The only instance in which I would foresee a major issue with using a bigger blocksize is on a mobile phone application, where it might drain your battery quite quickly. This can be mitigated by using smaller blocksizes, or only using it when on public Wifi to save your data. I personally choose AES256.

You can, however, research the other encryption methods, but I will not be covering them in this guide.

This video does an excelent job at explaining AES principles:

<https://www.youtube.com/watch?v=7RWP5eO-MPg>

Next, we will be choosing your key sizes for your server and future clients. As shown in the screenshot and on your screen, 2048 is fastest, 4096 is most secure. The NSA in recent years has moved away from 2048 bit keys for encryption protocols, which may raise eyebrows, for obvious reasons. They now recommend 3072 bit key sizes for government applications. Now, will you have to worry about people breaking your encryption if you use 2048bit keys? Probably not, it is highly unlikely. It would take, literally, thousands of years for an average hacker to exploit 2048bit key encrypted data.

As before with selecting the block size, bigger keys slows down the amount of time it takes to encrypt/decrypt. It also uses more processing power, which can have a negative impact on battery life.

Choose your block sizes and key sizes very smartly, but make sure it aligns with your end goal.

Step 5

Create a user and watch paint dry

Now, you will be prompted to create a user. The username doesn't matter, you can name it whatever you wish. It should be noted that only one user can log in with each .ovpn file. This is so another user cannot hijack your session. I will go over creating more files later in the guide.

Now that you have pressed enter, the script will download OpenVPN, all its dependencies, everything for crypto, etc etc. Pretty much everything you need for this. It will also set the OpenVPN service to run at boot, so when the server reboots it will be back up and running.

It will then generate RSA keys, this could take 5 minutes, it could take 3 hours. It depends on how "lucky" you get. It is calculating perfect prime numbers, extremely large prime numbers. Not only that, but it divides the prime number in half, and if the half isn't also a prime number it discards it and calculates a new one. There are arguments that perfect primes and primes are not more or less secure than each other, but I will not go into semantics about that.

Step 6

Setting up the firewall

You have the services running. Now, we need to configure iptables, or your firewall on the server, to forward traffic correctly. Below is everything you'll need to do so.

Code `iptables -A INPUT -i eth0 -m state --state NEW -p udp --dport 1194 -j ACCEPT` #change dport to whatever you selected previously. This allows connections on this port.

`iptables -A INPUT -i tun+ -j ACCEPT` #This allows TUN interfaces on the server

`iptables -A FORWARD -i tun+ -j ACCEPT`

`iptables -A FORWARD -i tun+ -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT`

`iptables -A FORWARD -i eth0 -o tun+ -m state --state RELATED,ESTABLISHED -j ACCEPT` #

These three allow forwarding through the tun interface to the eth0 interface. If "ifconfig" does not have eth0 replace eth0 with your ethernet device name.

`iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE` #This set up NATing

`iptables -A OUTPUT -o tun+ -j ACCEPT` #This is optional if your output line in iptables is not set to DECLINE

Step 7

Adding more users and devices

So, you now have a fully functioning OpenVPN server in the country you desire, with the encryption standards you prefer. But only one user can connect right now. Simply run the script again and you can add a new user, revoke users, or uninstall everything.

Running the script again and creating a user will not take long at all, maybe 5 seconds. It will throw their .ovpn file in the same directory.

The way it is set up right now, it is using TLS for authentication, and your keys for encryption. Only one device per session per key can be connected at a time. So you will need to make one for each device you plan on connecting at the same time.

Step 8

Connecting to the VPN

Now, you need to get the files off of the server. You can use SCP on a Linux box for this.

You can also use FileZilla, or any SSH/SCP enabled software. You simply download the file to your device and connect.

As there are a plethora of devices and operating systems that can be used to connect I will provide a few links to guide on how to connect to OpenVPN servers.

[Official OpenVPN documentation for clients](#)

[OpenVPN official guide for Windows](#)

[Official OpenVPN Guide for Linux](#)

[Official OpenVPN Guide for MacOS](#)

[Unofficial Guide for iOS](#)

NOTE: iOS users MUST either load via iTunes like this example, or you can email them to yourself, and open the attachment in the "Mail" App, then select OpenVPN Connect

[Unofficial Guide for Android](#)

The TL;DR

For people like me

Buy a server/VPS

Code sudo su

apt-get update

apt-get upgrade

reboot

cd ~/

mkdir openvpn

cd openvpn

wget https://raw.githubusercontent.com/Angristan/OpenVPN-install/master/openvpn-install.sh

sudo chmod +x openvpn-install.sh

sudo ./openvpn-install.sh Enter through all the bullshit, should take 5 minutes-3 hours depending on key generation

Download the files

Follow the guides to connect to the server

This is my first guide. If you find any errors let me know. I will fix it promptly.

If you need help with this I can help set it up in my free time for free.
I take people's privacy seriously, and I want to spread this little bit of knowledge with you guys.
I will be fixing formatting on this over time. I know, it's an eye sore.

I'm shit at designing these. I used the following tool to format text:
[https://xadamxk.github.io/ThreadDesignGenerator/\[Beta Release\] Thread Design Generator](https://xadamxk.github.io/ThreadDesignGenerator/[Beta Release] Thread Design Generator)

Travelers - July 13, 2017, 2:25 pm

Excellent guide. Glad to see that you got the formatting taken care of.

Also vouching for Marxist's knowledge. He's a good bro.

StopBackDooring - July 13, 2017, 8:00 pm

This guy just cock blocked all the kids selling vpn "engines" and vpn clients rofl

10x - July 13, 2017, 8:02 pm

Sick guide bro, might consider making my own private VPN but the VPN cracked acct I have [censored] is pretty sick and fast

DARPA - July 13, 2017, 8:08 pm

Where btc could I do this ? nice tutorial

Marxist - July 13, 2017, 11:43 pm

(Jul 13, 2017 02:25 PM)Jinn Wrote: [\[CITE\]](#) Excellent guide. Glad to see that you got the formatting taken care of.

Also vouching for Marxist's knowledge. He's a good bro. Thank you! His formatting program was a life saver. I just need to continue proof reading haha

(Jul 13, 2017 08:00 PM)StopBackDooring Wrote: [\[CITE\]](#) This guy just cock blocked all the kids selling vpn "engines" and vpn clients roflHahaha trust me that's not my intention, I just believe people should know what they're doing, how they don't control their data, and what they can do to give them more Control. People think VPNs are this crazy magic but in reality it's like 5 minutes of work or less.

I just want to help people maintain privacy.

Someone could also use this guide for...the opposite if you know what I'm saying ?

And to learn now this stuff works.

(Jul 13, 2017 08:02 PM)Realest. Wrote: [\[CITE\]](#) Sick guide bro, might consider making my own private VPN but the VPN cracked acct I have [censored] is pretty sick and fastWell if you lose that you know how easy it is now. N-o-r-d is using the same services this is :)

one of the main reasons why I prefer to make my own is because over time most vpn Companies start putting more users than they should per server. It good that you're having good results though.

(Jul 13, 2017 08:08 PM)M3RLIN Wrote: [\[CITE\]](#) Where btc could I do this ? nice tutorial

You could look around for hosters that accept btc. There's a few, I'll look around later today.

You can also find hosters from users here on hf!

edit:

Here is a list of hosting companies and their geographic locations that accept BTC.

Note: some of them may allow anonymous sign up, some may not.

<http://crypto.net/~joepie91/bitcoinvps.html>

Mr J0keR - July 14, 2017, 12:01 am

Thanks a lot SIR, for taking a time, and writing this precious and informative tutorial .

Appreciated ;) :)

azbit - July 14, 2017, 4:43 am

Excellent guide, I'll try to do this today.

Thank you so much !

opentechinfo - July 14, 2017, 9:46 pm

thank you, this helps me lot. although I know about VPN/proxy but I have learnerd something new

J. McCarthy - July 15, 2017, 9:26 am

A very nice guide man

Sticky ;)

Zens - July 15, 2017, 10:31 am

awesome guide, i will bookmark it

Marxist - July 16, 2017, 12:19 am

I might an additional section to this guide that goes over protecting yourself from DCMA's and such as well. I'm glad this has had a positive impact so far. If anyone has any questions let me know

Marxist - July 17, 2017, 12:27 am

Thanks omni :)

Hoping to get the word out so people can protect their privacy, while knowing what happens to their data in the VPN.

Russel_Novagan - July 17, 2017, 1:18 pm

Thanks for this marvellous article. I also wanted to write something like that, but you've outperformed me for sure on that one:)

aana - July 17, 2017, 7:39 pm

I setup this on one of my cheap ubuntu servers it was so easy.... I'm glad this is stickied its very helpful.

goondu - July 18, 2017, 4:58 am

good job mate !!!!

what other scripts are out there?

Marxist - July 18, 2017, 6:17 am

(Jul 18, 2017 04:58 AM)goondu Wrote: [\[CITE\]](#) good job mate !!!!

what other scripts are out there?

What else are you looking for?

James Burnham - July 18, 2017, 7:58 am

A great guide. I am reading it again and again.

Infinity™ - July 19, 2017, 12:15 am

Very detailed and excellent guide. Thanks mate. Btw do you have a script to block user/client downloading movies using p2p and or blocking of p2p and protect yourself from DMCA .

Marxist - July 19, 2017, 12:35 pm

(Jul 19, 2017 12:15 AM)?Properties Wrote: [\[CITE\]](#) Very detailed and excellent guide. Thanks mate.

Btw do you have a script to block user/client downloading movies using p2p and or blocking of p2p and protect yourself from DMCA .

Blocking torrents is a pretty tedious task.

As for protecting from DMCA, that addition to the guide is under works. However, a lot of the tips Tor gives for Exit Nodes apply to VPNs.

<https://blog.torproject.org/running-exit-node>

wlrb2 - July 23, 2017, 12:55 pm

Thank you for posting this, it was easy to follow.

slrslr - July 23, 2017, 2:30 pm

To all who want VPN and are lazy, just buy a Linux VPS and run this on it: [github d0t com/Nyr/openvpn-install](https://github.com/Nyr/openvpn-install)

you will have openvpn server which you can then connect.

If you are ok with normal SSH socks proxy, Google:
[quick-way-turn-linux-vps-into-anonymous-socks-proxy](#)

i used that and it works

Marxist - July 24, 2017, 3:00 am

(Jul 23, 2017 02:30 PM)slrslr Wrote: [\[CITE\]](#) To all who want VPN and are lazy, just buy a Linux VPS and run this on it: [github d0t com/Nyr/openvpn-install](https://github.com/Nyr/openvpn-install)

you will have openvpn server which you can then connect.

If you are ok with normal SSH socks proxy, Google:
[quick-way-turn-linux-vps-into-anonymous-socks-proxy](#)

i used that and it works

This is literally a fork of Nyr's script. Nyr's does not give you the options to change encryption and settings.

I'm not sure if you read the thread.

DA-De-Bufrosa - July 24, 2017, 5:58 am

Very grateful, I would immediately get a new computer, and intends to install Fedora 25, I had considered free vpn but which support Linux very little. I hope that I can successfully build mine vpn according to your introduction.

Marxist - July 29, 2017, 6:18 am

(Jul 24, 2017 05:58 AM)DA-De-Bufrosa Wrote: [\[CITE\]](#) Very grateful, I would immediately get a new computer, and intends to install Fedora 25, I had considered free vpn but which support Linux very little. I hope that I can successfully build mine vpn according to your introduction.

I hope you were able to set this up well.

Also, reminder. If anyone needs any help setting up VPNs or the like, I will help for free and consult you in my free time.

sw0p - August 1, 2017, 5:26 pm

nice guide, well written.
thank you :)

Targus - August 2, 2017, 4:35 am

Discourage people from using NAT VPS if privacy is the main concern here, some happy-go-luck geniuses tend to choose the cheaper alternative without knowing the consequences that come along with it. :)

Marxist - August 3, 2017, 2:59 am

(Aug 2, 2017 04:35 AM)Targus Wrote: [\[CITE\]](#) Discourage people from using NAT VPS if privacy is the main concern here, some happy-go-luck geniuses tend to choose the cheaper alternative without knowing the consequences that come along with it. :)

That's true. I should probably include that, I've been super busy as of late though

The Sales Thrash GOD - August 7, 2017, 9:40 pm

could you possibly start up your own vpn company with this guide?

Marxist - August 10, 2017, 4:19 am

(Aug 7, 2017 09:40 PM)Decree Wrote: [\[CITE\]](#) could you possibly start up your own vpn company with this guide?

I don't see why not. For a smaller operation I'd use rsync over ssh and incron to set up directory-based cron jobs that replicate new pkis to your other servers.

So then there's minimal overhead everytime you create a new user using this script. Example:
rsync -aqz --delete-after /etc/openvpn transferuser@pl1.example.com:/etc/

For the initial use of that command it will transfer everything in the directory to the new server's directory. Everytime it is run after that it will only send files that have changed. (incremental transfers) and it transfers file permissions, etc.

So, for instance, it won't try to transfer your server's certificates everytime it does a back up. It'll only send new files, and delete any that aren't on the original server anymore. It makes an exact mirror between the two servers.

I'm no good at web development and stuff like that, so I couldn't give any advice to any of that, though.

So anything that involves adding more than 5 users a day I'd look at other options for user creation outside of this script.

But for initial installation and configuration this script will save you a lot of time, especially for deploying new servers in your network. just rsync all your configs and pkis from a primary server to the new ones post-installation, then point a subdomain to that IP, and users will be able to connect to it.

For making a small company I recommend making a lot of sub-domains and pointing them to the servers you already have up and including them in the original client configurations, so it doesn't effect the users when new ones are implemented. (like us1.example.com us2.example.com, nl2.example.com etc etc)

hello2 - August 11, 2017, 11:47 am

its amazing to see how much effort people like yourself put into stuff like this, its what makes this community great

Marxist - August 12, 2017, 11:11 pm

Any time. If you need any help if you decide to use this don't hesitate to ask

shabahighrank - August 13, 2017, 11:58 am

(Jul 13, 2017 12:23 PM)Marxist Wrote: [\[CITE\]](#) Setting Up your Own Personal VPN

And why it's important

The TL;DR

For people like me

Buy a server/VPS

Code sudo su

apt-get update

apt-get upgrade

reboot

cd ~/

mkdir openvpn

cd openvpn

wget <https://raw.githubusercontent.com/Angristan/OpenVPN-install/master/openvpn-install.sh>

sudo chmod +x openvpn-install.sh

sudo ./openvpn-install.sh Enter through all the bullshit, should take 5 minutes-3 hours depending on key generation

Download the files

Follow the guides to connect to the server

This will definitely save some time. Thank you for sharing!