# Roll Your Own Open-VPN Server

One of my favorite things about selfhosting is the ability to take back control of your data and as a neat side effect increase your privacy in an ever growing world of data mining and complicated EULAs.

A VPN can be super handy for not allowing prying eyes to view what websites you visit or hijack your dns to point you to a malicious copy of an otherwise legit website. This is especially important on open wifi or networks you don't trust.

Using a VPN provider is certainly an option, but then you're simply moving the trust to yet another 3rd party. Some of these are certainly trustworthy , but ultimately its impossible to know for sure what these services are doing with your data.

Below are some handy resources if you want to use a VPN service rather than roll your own.

- https://thatoneprivacysite.net/vpn-comparison-chart/

- Here is a handy thread as well https://twitter.com/evacide/status/974038707081592832

There are a few options to roll your own personal vpn service, but the first step is picking a virtual server provider (VPS) to run your vpn on. You can of course do this on your own home pc/server , but then you're opening your home to the internet which I generally like to avoid. I peronally use Vultr (<------- disclosure this is an affiliate link) for my outside self hosting playground. Their base VPS price ($3.50 per month) is quite reasonable and I've found their service to be reliable.

After you choose your VPS service, you have a few options for what VPN technology to deploy and how you deploy it. We'll dive into each below.

**Option 1 (my preference) OPENVPN** -
OpenVPN has been around for ages. It is a proven and security audited tech used by many organizations and individuals. There are a few options for deployment here.
-First you'll want to spin up a VPS as listed above. I'd suggest using Ubuntu Server 18.04 LTS as your base OS.

-Login to your server with SSH (putty or mobaxterm) (pick a strong password or better yet use SSH keys

and install Fail2Ban (this will ban IPs who try to bruteforce ssh logins on your box and keep it a bit more secure).

-Use the following script for the easiest deployment https://github.com/angristan/openvpn-install ( **most folks recommend against downloading random bash scripts from the internet and running as root, do not do this unless you know how to read what the script does before deployment**). That being said I've used this on numerous occasions and has my blessing. Once you have run this script it will spit out an openvpn config file. Simply download it from your server and import into your openvpn client on windows, iOS, or, android.

-If you want to avoid the scripting deployment route and get your hands dirty I'd suggest this guide. https://blog.ssdnodes.com/blog/tutorial-installing-openvpn-on-ubuntu-16-04/

**Option 2 (less wide spread support, but I've used it myself without issue) ALGOVPN-**

Algo is a bit more complicated to setup than just using a script, but is still easier than deploying from scratch. It is also a bit harder to setup on your system. The project has been around for a while and the folks there take security seriously. Guide can be found here https://github.com/trailofbits/algo .

In closing. Whatever you decide to do, rolling your own vpn can be a fun afternoon (or even lunch break project) that can help keep you more secure online and learn a bit in the process.

Questions? Comments? Snide remarks? Feel free to spam me using my info on the about page.

---

Revision #1

Created 1 month ago by Biff

Updated 1 month ago by Biff