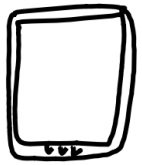
TUNNELS

and

SMARTPHONES



&

A ZINE ABOUT HOW TO CHOOSE A VPN SERVICE
AND HOW TO USE ONE ON A SMARTPHONE

this manual is part of the VPN zines
collection from psaroskalazines.gr

it is made with hand drawn icons by the author
and layout design is done with scribus

cover font:
fontlibrary.org/en/font/sans-quilt-wafer

colophon and content's headers font:
www.wfonts.com/font/erbos-draco-1st-open-nbp

content font:
www.levien.com/type/myfonts/inconsolata.html

many thanks to:
digitaldefenders.org for the financial support
systerserver.net for hosting the git repository of
the vpn zines project

find the author at mastodon
systerserver.town/@mara

INTRODUCTION

This zine informs about how to choose a VPN service and how to install such a service on a smartphone. It is a manual meant for all users who would like to secure their mobile phones with a tunnel. By contrast to the other zines in the VPN collection, here the content does not involve the terminal nor command lines. Instead it navigates through general guides and user interfaces.

Visit the rest of the VPN zine-collection:

Tunnel Up / Tunnel Down
zines.cucu.gr/prints/tunnel-up-tunnel-down-en/

Troubleshooting OpenVPN
zines.cucu.gr/prints/troubleshooting-openvpn-en/

Upcoming
Backups over VPN & raspberry-pi

INDEX

WHY A VPN?

because it helps to avoid tracking, circumvent censorship, and get remote access to intranets!

Putting together pieces of information through our browser or apps activity, is what trackers do to identify users. It is called fingerprinting and is a more persistent tracing method than cookies because it does not store anything on our machine, which can be deleted. While a VPN does not solve entirely the identification of a user's device, it helps to confuse the tracker by hiding our real IP.

However other info, such as screen resolution and browser settings cannot be hidden, that is why using different browsers for different online activities assists in bluring our online id. Also Tor, Firefox and Brave browsers use methods to make all browser instances appear similar, so they are fine options against fingerprinting.

Here we focus on VPN services that can also:

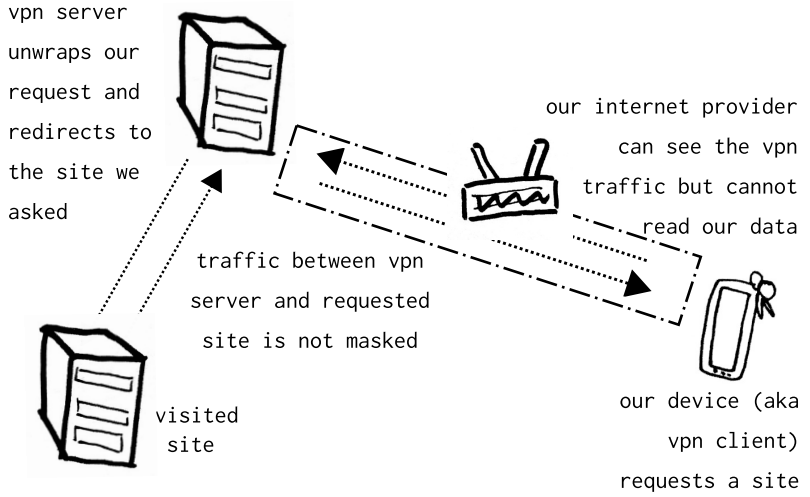
- ensure privacy when connecting to a public WiFi
- circumvent censorship (users need to be informed about local regulations concerning the use of a VPN)
- connect to an intranet (e.x reach our work/organization/home network from outside)

WHAT VPN TO USE?

A VPN masks our data packets on the public internet until it reaches the VPN sever. Since encryption ends at the VPN server, the latter her access to data, such as our IP, destination IP (aka website we visit), our devices' operating systems, which browser we use, etc. So a VPN company could potentially spy on its users by keeping traffic logs, if it wanted to.

Finding a VPN service means that we trust the VPN company's accountability, as well as gather information on any authority enforcements of private data disclosures, such as subpoenas, the company is bound to comply.

So reviewing a company's policies along with its state laws, are parts of the process when we are on the look for a VPN service.



WHAT TO REVIEW EXACTLY?

> If the VPN service accepts payment with bitcoins or disposable or temporary cards, it saves us some privacy. However our IP address can be logged and disclosed on audit requests. If we are at a high risk of surveillance, we may either use the commercial VPN in public spaces such as coffee shops, or use a Tor browser. Usually a VPN company should mention in their privacy policy if they monetize users' data. Yet general claims on their website cannot truly be verified.

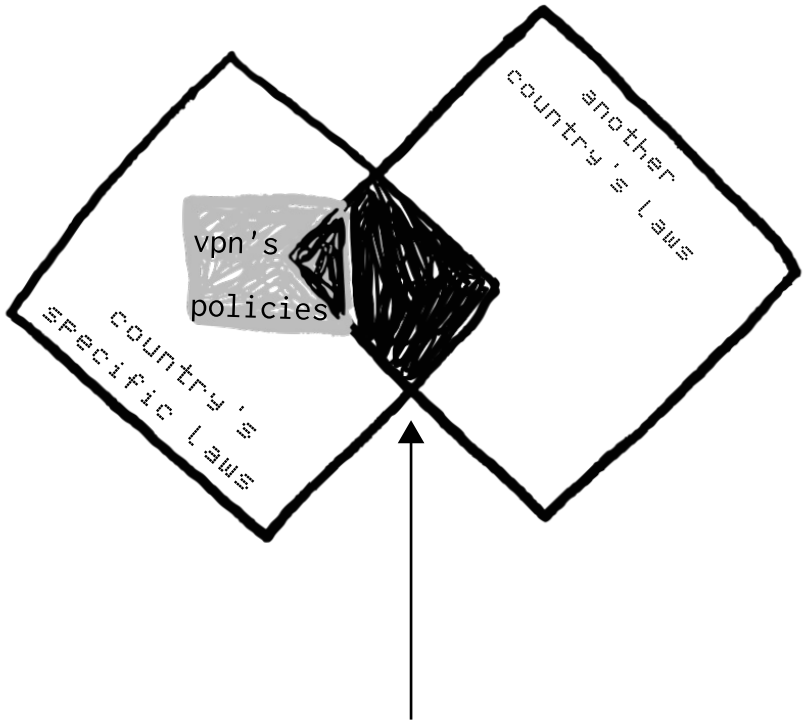
> Review the VPN's business model, what is the income of the VPN, donations, funding, service fees? Too low fees might translate to the company involved in trading users' data.

> Review the organization or company and its people e.x. look for any recommendations from security activists, or from a strong community of activists and journalists.

> Look for the encryption settings, for instance preferable options are OpenVPN software which uses SHA 256 algorithm for authentication, and at least RSA-2048 or AES-256-GCM for data encryption;

> Look if the company provides any security audits from reliable third parties.

STATE LAWS & TREATIES



legal assistance treaty between two countries

> When choosing a VPN service, its geolocation is important. Reiewing the country's data privacy laws, where the VPN is based, should be a priority. Then, any legal assistance treaties that allow other countries to request user data disclosures from the VPN service need to be considered too. And of course reviewing our local laws on using a VPN should be the first thing to look up.

GENERAL TIPS

- Stay away from VPN services located in the 14-eye list including South Korea + Singapore

- VPN providers "no-login' policies cannot be verified.

- Use encrypted DNS if possible (android provide this option in its vpn settings)

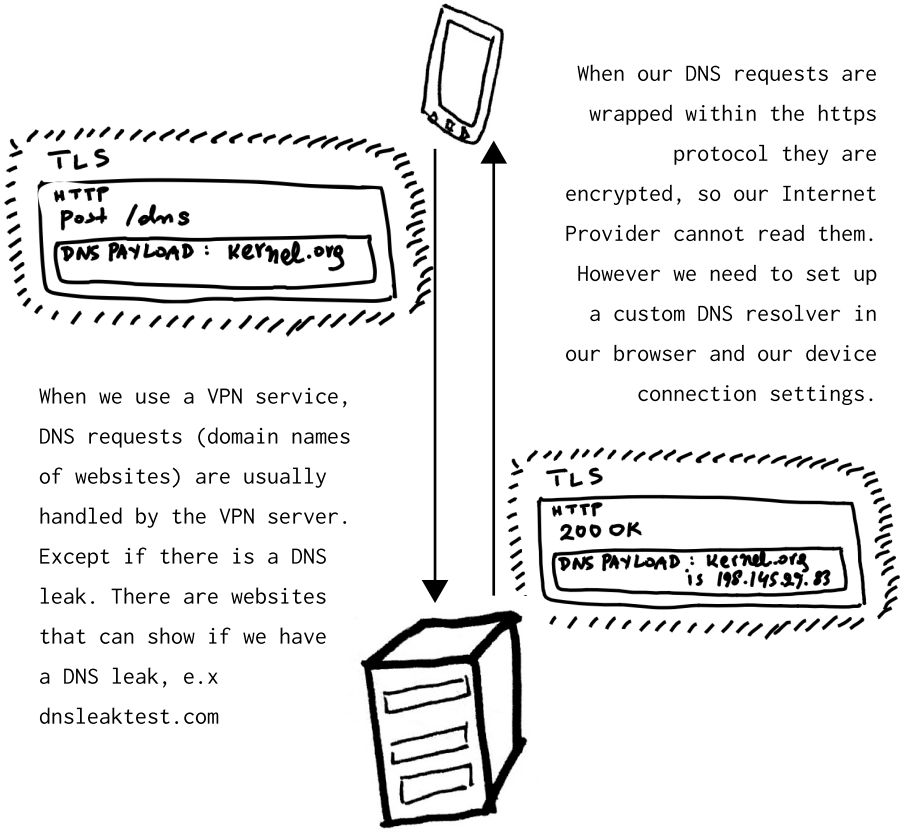
- When we need to provide email and credit card info to the same company, our personal information will be exposed if there is an enforced users' data disclosure.

- If we need a VPN to circumvent censorship, we need a VPN service which provides openVPN software or similar such as WireGuard. Because these software applications allow for communications over no standard ports, they cannot be easily blocked.

- Avoid using a binary installer but obtain a text based configuration file to use for connecting to the VPN service.

- The VPN service should offer a certificate per user, not per group. If group certificate, then many users are at risk when this certificate leaks to wrong hands.

DNS ENCRYPTION OVER HTTPS



When our DNS requests are wrapped within the https protocol they are encrypted, so our Internet Provider cannot read them. However we need to set up a custom DNS resolver in our browser and our device connection settings.

When we use a VPN service, DNS requests (domain names of websites) are usually handled by the VPN server. Except if there is a DNS leak. There are websites that can show if we have a DNS leak, e.x dnsleaktest.com

- We are better off with a DIY VPN setup. See the "troubleshooting openVPN" zine for how to build one.

- Choose the right protocol; PPTP and L2TP are outdated and not secure. Go for IPsec if we want to access a remote server. Use openVPN if we want to evade censorship.

NOTE: see CHEAT-SHEET for the resources of the above list

ANDROID AND VPN

We need a VPN client to connect to a VPN server.

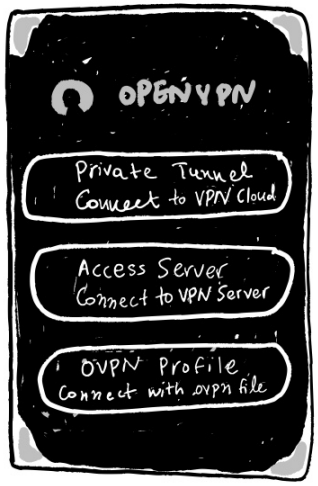
If we choose a commercial VPN, such as Express VPN (see CHEAT-SHEET why this one is widely used in China) they would provide their own client apps for android and iphone.

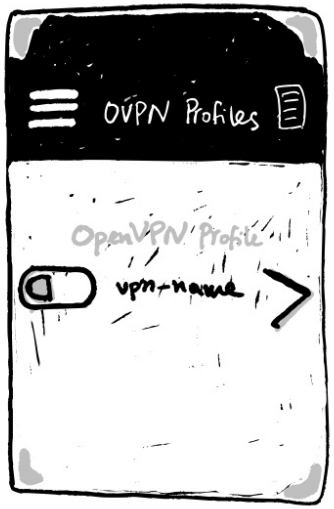
Here we give an example with openVPN's official mobile app, called openVPN Connect. It works with android 4.0 and higher without asking for device root privilege. So we go ahead and install it.

Under settings > "Wireless & Networks" or "Connections" > More settings, there is the option VPN. In the advanced settings, we can provide an encrypted DNS (see more info in the CHEAT-SHEET).Tap the option to start the openvpn connect app.

The first time we connect to the VPN we may need to enter our user/password credentials provided by the VPN service.

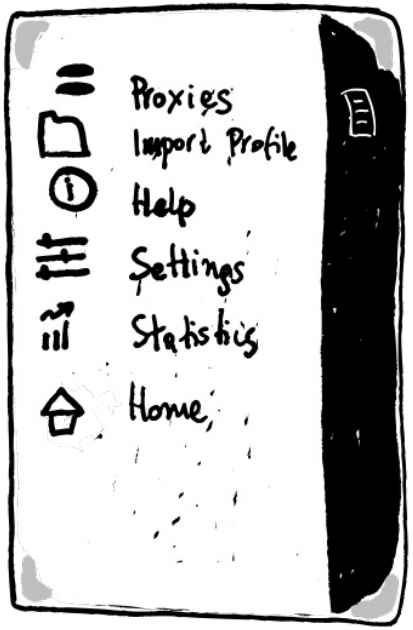
Alternative, if we have an open VPN config file (with .ovpn extension) we chose that option, by going to the openvpn app menu and choose "OVPN Profile connect with .ovpn file". We need to download/transfer the .ovpn file to our phone in advance.





We can give a nickname for the VPN connection. Next we add the IP or the domain name of the VPN server we want to connect.

For extra options, tap on the openvpn app menu > settings, tap on "reconnect on reboot", which will restart the VPN connection automatically when we restart or activate our phone. In the same section, there is also the option to block any connection if it does not go through the VPN.
For any connection errors, tap on the "file" icon at the top right side, which opens the connection log file.



VPN FOR F-DROID & iOS

For f-droid, we can install the same openVPN connect app for Android, and follow the previous steps.

For iPhone we install and open the openVPN Connect app. We can transfer the client config file via iTunes from a Windows or MAC computer. From iTunes choose Apps > file sharing > openvpn and import the config file.

If our computer is Linux, we can install gfs-backends to assist us with mounting iPhone to computer as a storage device and transfer the client config file.

Last, in the openVPN connect app, import the config file and add the new profile, then tap the Connection button and enable it.

EXTRA TIPS

Get the openVPN client config file via a sftp scp (aka secure copy) from the VPN server to a computer, or received via encrypted email. Mount the phone to computer and place the config file under the phone's internal storage.

In openVPN connect settings choose WiFi connection if we want to connect to the VPN also from an internet connection, either public or from home.

Riseup collective offers a donation based VPN for most Operating Systems, including F- droid, but not iOS.
https://riseup.net/en/vpn#why-would-you-want-to-use-the-riseup-vpn

Belgian association Neutrinet offers VPN services on a donation basis https://neutrinet.be/en

This podcast informs about the risk when using a commercial VPN, but also when using a Tor browser. It's from 2017 so take it with a grain of salt. More up-to-date research on Tor is required.
https://georgian.io/the-problem-with-the-tor-network-and-commercial-vpns/

CHEAT SHEET

Choosing the VPN That's Right for You
https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

A thorough introduction on how a VPN works and when to use one
https://www.cucu.gr/prints/tunnel-up-tunnel-down-en/

A list of VPN services which do not keep logs
https://www.privacytools.io/providers/vpn/

Why we should not use commercial VPN services
https://gist.github.com/joepie91/5a9909939e6ce7d09e29

VPN services list comparison
https://thatoneprivacysite.net/#simple-vpn-comparison

VPN on android
https://www.howtogeek.com/135036/how-to-connect-to-a-vpn-on-android/

DNS encryption explained
https://blog.cloudflare.com/dns-encryption-explained/

Configure openvpn client on Android, iOS, Linux, MacOS, Windows
https://www.linode.com/docs/guides/configuring-openvpn-client-devices/

Is your VPN provider in a "14 Eyes" Country?
https://www.my-private-network.co.uk/vpn-provider-14-eyes-country-something-know/

Howto install DNS encryption on Android 9
https://mikaela.info/blog/english/2019/07/11/android-private-dns-in-practice.html