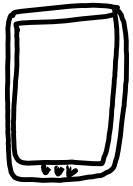
# 穿隧

# 与

# 智能手机



与

一本关于如何选择 VPN
以及在智能手机上应用的小册子

这本指南来自 psaroskalazines.gr
出版的一系列 VPN 小册子

插图由作者手绘
排版设计 scribus 软件完成

字体：
方正 24

致谢：
digitaldefenders.org 的资金资助
systerserver.net 为小册子提供 git 托管服务

在 mastodon 长毛象上联系作者：
systerserver.town/@mara

# 简介

这本小册子解释了如何选择 VPN 服务，以及如何将 VPN 服务安装在智能手机上。

针对所有想在手机上移动电话上安装隧道的用户

与 VPN 系列中别的册子不同，这期内容不包含终端命令行。

这本册子主要围绕通常的用户指南和用户界面展开。

浏览 VPN 系列中其余的册子：

《隧道穿行 / 穿梭指南》

zines.cucu.gr/prints/tunnel-up-tunnel-down-en/

《OpenVPN 故障排除》

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

即将出版

《为 VPN 和树莓派备份》

# 目录


page 1 ..... 为什么要用 VPN?

page 2 ..... 用什么 VPN?

page 3 ..... 怎么选择呢？

page 4 ..... 国家法律和双边协定

page 5 ..... 普适性的建议

page 6 ..... 在 HTTPS 上使用 DNS 加密

page 7,8,9 .... 安卓系统 VPN

page 10 ..... F-DROID 和 iOS 系统 VPN

page 11 ..... 额外建议

page 12 ..... 速查表

# 为什么要用 VPN?

它能够帮助避免被追踪，规避审查机制，还有链接到内联网!

通过分析我们网页或者应用上的用户活动的相关信息，追踪器能够对用户进行辨识。这种方法被称作 “ 指纹 ”，是一种比 cookies 更持续的追踪方法，因为它不在我们的电脑上留下任何能被删除掉的文件。虽然单凭 VPN 不能解决用户识别的问题，但它能通过隐藏我们 IP 真实地址的方法，来混淆追踪器的追踪机制。

但是，其他种类的信息，比如屏幕的分辨度和浏览器的设置不能被隐藏，所以对不同的目的的网页浏览使用不同的对应浏览器能够帮助我们模糊我们的线上身份。另外，洋葱、火狐和 浏览器能够使所有的浏览器活动看起来相似，所以这些浏览器是对抗被 ” 指纹 ” 的好方法。

在这里，我们将关注可以实现下列目的的 VPN 服务

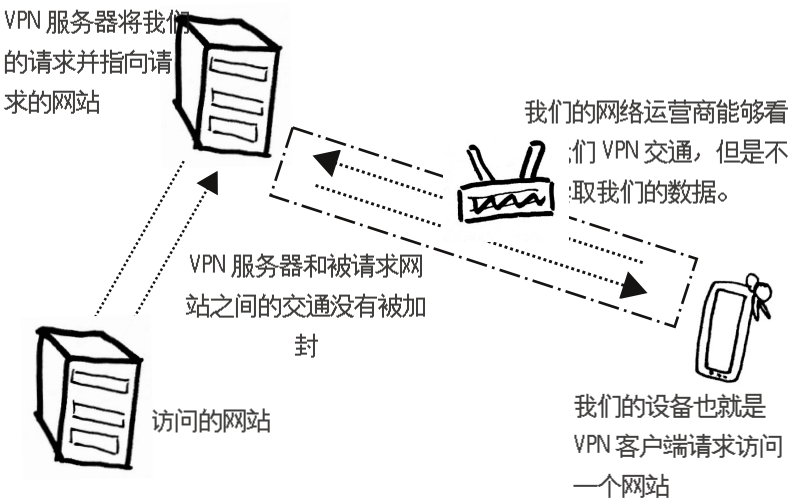
- 在链接公共网络时保证隐私安全
- 规避防火墙（用户需要知晓在本地使用 VPN 的相关规定）
- 链接内联网（比如说从外部链接到我们工作、组织、家庭的内部网络）



# 用什么 VPN?

VPN 能够将我们在公共因特网上传输的数据包在抵达 VPN 服务器之前隐藏起来。因为加密服务在到达 VPN 服务器时就停止了。VPN 服务器能够知晓用户的数据，包括 IP 地址，目的地 IP 地址（也就是我们访问的网站），我们设备的运行系统，我们是用什么浏览器，等等。所以，VPN 公司也有通过保存网络通讯记录的方法来监视用户的嫌疑。

使用 VPN 服务意味着我们信任该 VPN 公司的问责性，包括对任何任何权力执行机构对私人信息的采集，比如说法院传票，该公司有责任服从遵守这些责任。所以审核一家公司的政策和其所在地的法律条规，是选择 VPN 服务的一部分。



# 怎么选择呢?

> 如果 VPN 服务能接受比特币，和能丢弃或临时的支付卡，那么我们能留存一些隐私。但是，我们的 IP 地址还会被记录，也会被审计要求而被公开。如果我们身处高度可能被监视的境况下，我们可以在像咖啡店这样的公共空间使用商业 VPN，或者使用洋葱浏览器。通常一个 VPN 公司会在他们的隐私协议中提到公司是否会利用用户信息进行商业交易。但是，这些公司网站上公布的声明不能真正地被做实。

> 审查 VPN 公司的商业模式，这个公司的收入是通过什么样的来源？捐款，基金，使用费？过低的费用可能表示这个公司有可能对用户的数据进行交易。

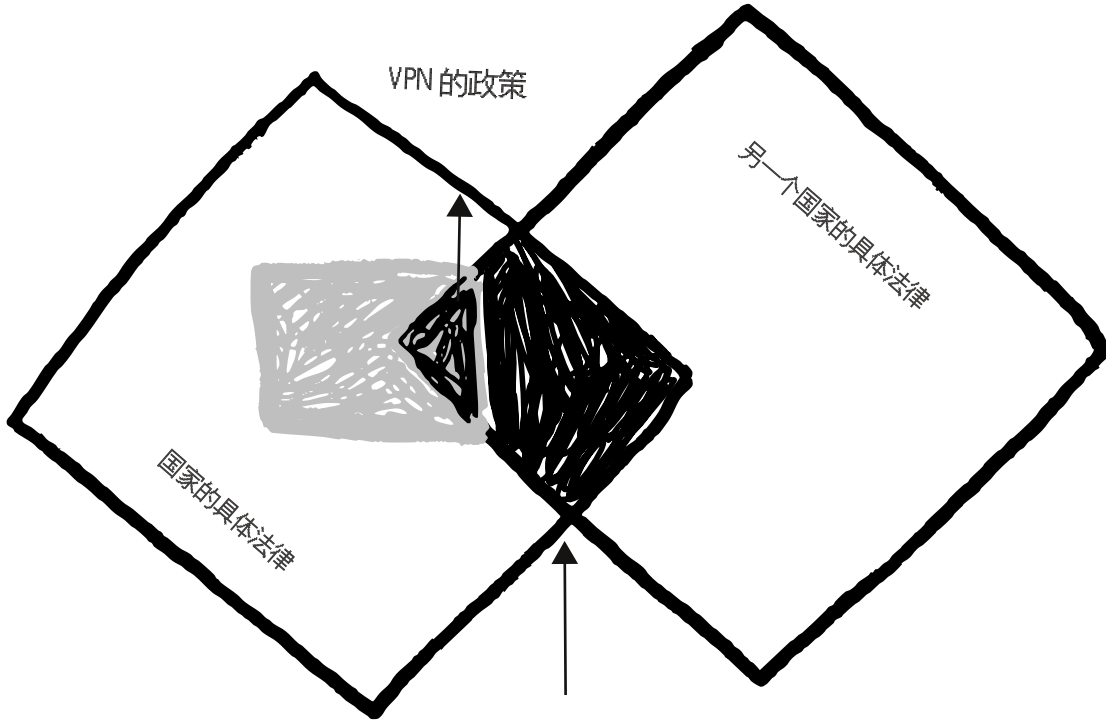
> 审查机构，公司及其任职人员。比如说，咨询网络安全行动者人士，或者来自行动主义者和新闻报告者社群的建议。

> 进行加密配置，比如说使用 SHA 256 算法进行认证的 OpenVPN 软件，或者至少使用 RSA-2048 和 AES-256-GCM 来进行数据加密。

> 审查该公司是否通过可靠的第三方进行安全审计。



# 国家法律和双边协定




> 选择 VPN 服务时，其地理位置十分重要。 审查所在地国家的数据隐私法律应该是一个优先考虑项。 另外，在 VPN 服务条款中，任何能够为其他国家协作提供用户数据公开的双边法律协定也应该被考虑进去。审查 VPN 所处地的本地法律应该是我们要做的第一件事。

# 普适性建议

- 避免使用来自 14 眼列表国家中的 VPN 服务，包括南韩和新加坡。

- VPN 服务商的免登入政策不能被做实。
- 尽可能使用 DNS 加密（安卓系统在 vpn 设置里提供了相应选项）

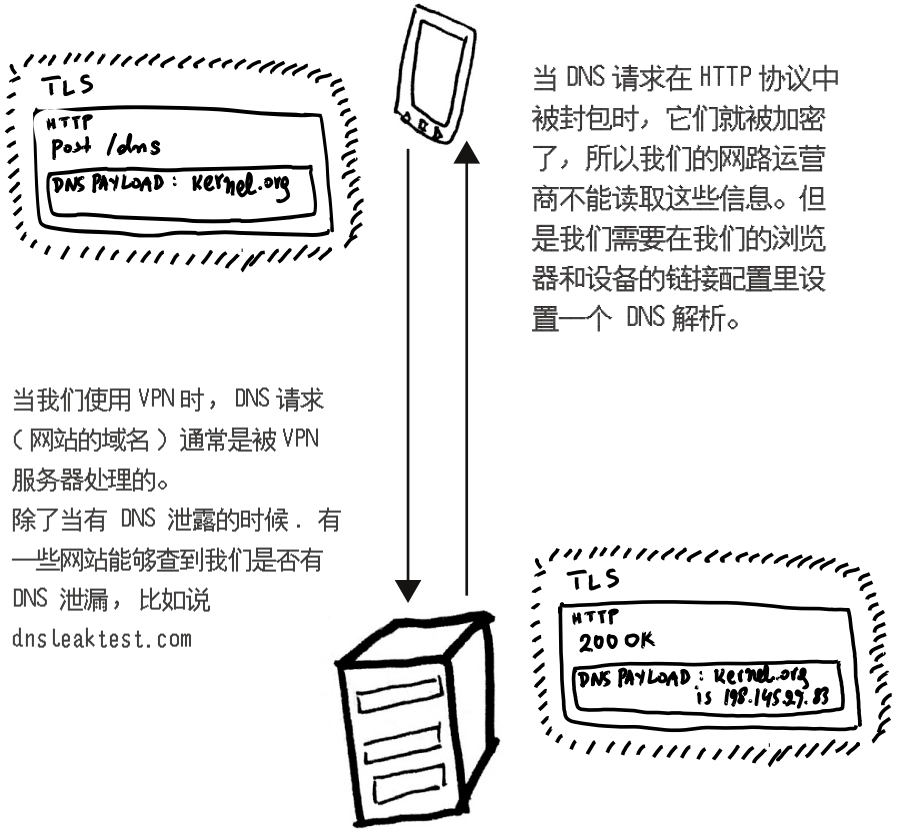
- 当我们需要提供邮件和信用卡提供给同一间公司时，我们的个人信息会在被强制要求信息公开时曝光。
- 如果我们需要使用 VPN 来规避审查机制，我们需要使用提供 openVPN 软件的 VPN 服务，或者相似的，例如 WireGuard。 因为这些软件能够通过非常用的端口通讯，这样就没那么容易被屏蔽。

- 避免使用二进制的安装包，但需要获得一个配置文件来链接 VPN 服务。

- VPN 服务应该为每一个用户提供证书，而不是每一群用户。如果使用群证书的话，那么如果证书落入不当的路径将导致多个用户的风险。



# 在 HTTPS 上进行 DNS 加密




- 我们使用 DIY 的 VPN 配置更好。可以《openVPN 的故障排除》小册子来配置一个

- 选择正确的协议。 PPTP 和 L2TP 已经过时而且不安全。 如果要访问远程的服务器，我们可以使用 IPsec。如果我们想规避审查机制，使用 openVPN。

提醒：阅读速查表来找到上述资源。

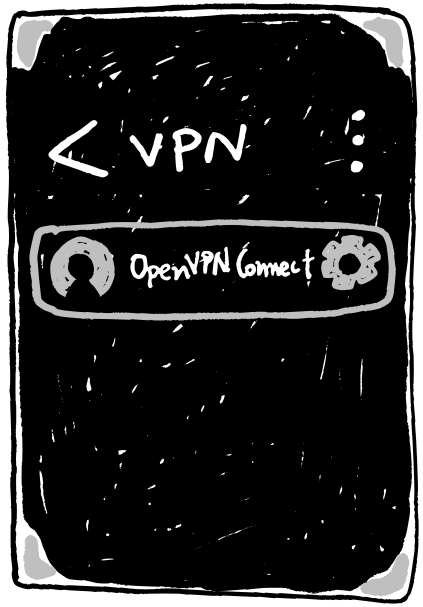
# 安卓和 VPN

我们需要一个 VPN 客户端来链接到 VPN 服务器。

如果我们选择商业的 VPN，比如说 Express VPN（我们能在速查表看到为什么这个在中国被广泛使用）它们会为安卓和 iPhone 提供自己的客户端应用。

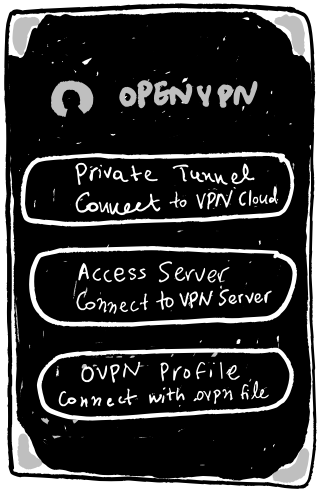
在这里，我们给一个 openVPN's 官方移动应用，叫做 openVPN Connect。它能够在 android 4.0 或者更高的系统上，不使用设备的根授权使用。我们可以下载这个应用。

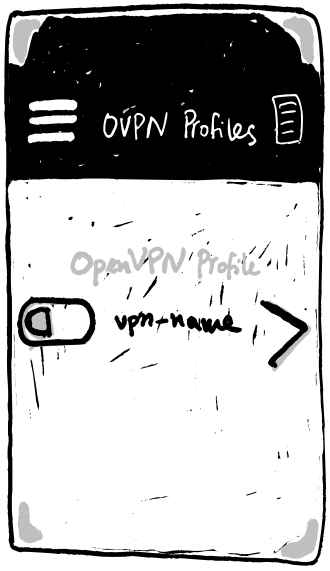
在配置 > "无线和链接" 或者 "链接 > 更多配置，我们能够找到 VPN 选项。在更高级的选项中，我们能配置加密的 DNS（可以在速查表找到相应信息）。点击这个选项来开启使用 openvpn connect 应用。






当我们第一次链接 VPN 时，我们可能会被要求提交我们由 VPN 服务提供的的用户名和密码。或者，如果我们有一个 open VPN 的配置文件（带有 .ovpn 文件后缀）我们可以选择这个选项，通过去 openvpn 应用菜单，然后选择 "OVPN 账户通过 .ovpn 文件链接"。我们需要把 .ovpn 文件提前传输或者下载到我们的手机上。

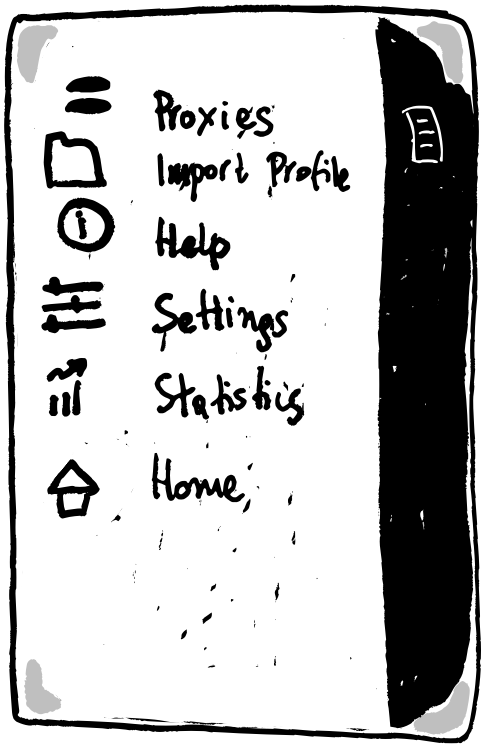



我们可以给 VPN 链接去一个别称。接下来我们可以添加我们想要链接的 VPN 服务器的域名或者 IP 地址。

如果需要更多的选项，可以选择 openvpn 应用的 菜单 > 配置，选择 "重新启动和链接"，这个选项能够在我们重启或重新激活我们手机时自动启动 VPN 链接。在同一个菜单里，也有一个选项能够屏蔽所有如果不经过 VPN 通讯的链接。

如果遇到链接错误，选择右上方的 "文件" 标示 ，来打开链接记录文件。






# F-DROID 和 iOS 使用的 VPN

对于 f-droid，我们可以安装安卓系统使用的同样 openVPN 链接应用。对于安卓，可以遵循前一小节的步骤。

对于 iPhone 我们可以安装并配置 openVPN Connect 应用。我们可以把客户端配置文件通过 iTunes 从 Windows 或者 MAC 电脑传输到手机上。在 iTunes 里选择应用 > 文件共享 > openvpn 然后选择载入配置文件。

如果你的电脑运行 Linux 系统，我们可以安装 gfs-backends 来帮我们把 iPhone
加装到电脑上，作为一个储存设备并把客户端的配置文件传输到上面。

最后，在 openVPN connect 应用里，载入配置文件，添加新的用户配置， 然后选择链接按钮来启动链接。

# 额外建议

通过 sftp scp(也就是安全传输 secure copy)来从 VPN 服务器把 openVPN 客户端的配置文件下载到电脑上，或者通过加密的邮件传输。通过手机连接到电脑，然后把配置文件放置到手机储存空间里。

如果我们想用公共网络或者家庭网络连接 VPN 的话，在 openVPN 的设置里，选择 WiFi 连接。

Riseup 组织为几乎所有的操作系统提供了捐赠使用的 VPN，包括了 F- droid，但不包括 OS。
https://riseup.net/en/vpn#why-would-you-want-to-use-the-riseup-vpn

比利时的 Neutrinet 组织也提供捐赠使用的 VPN 服务
https://neutrinet.be/en

这个播客阐述了使用商业 VPN 的风险，包括在使用洋葱浏览器的情境下。这是在 2017 年录的，所以也值得稍作参考。应该需要做更多关于洋葱浏览器的研究
https://georgian.io/the-problem-with-the-tor-network-and-commercial-vpns/



# 速查表

选择一个适合你的 VPN
https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

一个详尽的 VPN 说明，如何运作，什么时候该使用。
https://www.cucu.gr/prints/tunnel-up-tunnel-down-en/

不留存记录文件的 VPN 服务
https://www.privacytools.io/providers/vpn/

为什么我们不应该使用 VPN 服务
https://gist.github.com/joepie91/5a9909939e6ce7d09e29

VPN 服务比较表
https://thatoneprivacysite.net/#simple-vpn-comparison

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

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

在安卓，iOS，Linux，MacOS，Windows 上安装 openvpn 客户端
https://www.linode.com/docs/guides/configuring-openvpn-client-devices/

你的 VPN 运营商是不是在 “14 眼” 国家？
https://www.my-private-network.co.uk/vpn-provider-14-eyes-country-something-know/

如何在 Android 9 上安装 DNS 加密
https://mikaela.info/blog/english/2019/07/11/android-private-dns-in-practice.html