

重要提醒：

此教程收集自互联网，互联网技术教程，请不要用于非法用途，遵纪守法，拥护党的领导，做合法公民。

目录：

- 1 最简单的现成 app 直连（比如蓝灯，迷雾通… .）
 - 2 使用开源 v2r/clash/ 及其分支（基础）
 - 3 protonvpn
 - 4 开源洋葱网络 tor 相对其他软件最安全 匿名（暗网工具）
orbot/InviZible Pro 使用 tor 网络三次节点跳转 匿名
 - 5 自建节点
- 必读附录：重要提醒

方法 1 自动节点类软软件

首推 geph 迷雾通和 protonvpn ,proton 教程参看方法 3. 这里介绍 geph, 他自由开源且总部位于爱沙尼亚。优点就是免费安全稳定，缺点是免费版限速
迷雾通教程：

安装 geph 迷雾通，并注册登陆

(迷雾通注册过程 可能要用其他软件连国际互联网，如果可以不代理就能刷新验证码，就不需要先用方法 2)

最新版官网 <https://geph.io/zhs>，免代理镜像下载：<https://waa.ai/xiazaimiwutong>，

此软件虽然免费版有限速 但比较稳定，安全性更高，不用每日跟换 订阅，只是 注册 时刷新验证码可能需要连上国际互联网，因此可能需要先用 NEKBOX/v2r/clash 连上国际互联网以后才能使用

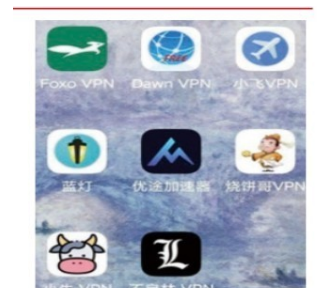
操作流程图： 注意，请开启排除应用程序，排除掉不需要代理的软件，避免国产非开源应用知道你在走代理



注意：

蓝灯 / 快连 / 老王 / 烧饼 等为非开源程序，不推荐，像老王据说背后不干净，有一些 背后是中资或者背后不确定，而且此类免费账户要么限速限流量，要末可能会跑路。

唯一优点只是最简单的



方法 2 v2r/clash 类开源程序

clash for windows 作者因为泄漏个人隐私被开盒删库跑路， clash 内核作者不会再有更新，也删库跑路了，所以 clash, 不会再有更新，不建议使用，可以用 clash verge/clash meta/flclash 等 替代

优点：全平台开源，节点随便换，一般不限速，相对各种商业不开源魔法 app 比较安全，但是最终安全性，看节点本身，相比免费公开节点，更建议使用方法 5。

缺点：可能需要每日换订阅，节点不稳定 / 付费订阅不用（一般几块钱一个月）

注意：软件平台开源安全，不代表节点安全，也可能存在钓鱼节点，因此公开免费的订阅建议做临时使用或者备用，

使用 v2r 和 clash 过程中请务必开启分应用模式或者代理模式，根据需求选择全局代理或规则代理，只让需要翻墙的应用翻墙，尽量使用自由开源程序，不要使用国产 app 使用翻墙服务，比如腾讯浏览器实名 qq 微信，这种等于自爆，有条件的刷机为类原生安卓系统，避免国产系统 监视

下载：

- v2rayng - （安卓）下载地址（更新维护比 nekbox 积极）

<https://github.com/2dust/v2rayNG/releases>

- clash-meta - 安卓 ,clash 使用的订阅为 yaml 而不是下面教程的 txt)

<https://github.com/MetaCubeX/ClashMetaForAndroid>

- flclash- 支持电脑安卓手机 win 和 linux, 或者在 fdroid 应用商店内下载

<https://github.com/chen08209/FlClash>

- clash-verge-rev - 电脑设备

<https://github.com/clash-verge-rev/clash-verge-rev>

- v2raya- 支持电脑设备， windows,linux 等

<https://v2raya.org/>

- v2rayn- 仅支持 win, 下载带 core 核心的 64 位)

<https://github.com/2dust/v2rayN>

- sin-box- 支持安卓和苹果

<https://github.com/SagerNet/sing-box>

- 苹果手机请换区后使用 sinbox，或者使用 ios 版 v2r-OneClick

<https://apps.apple.com/us/app/sing-box/id6451272673?l=zh-cn&platform=iphone>

节点获取方法：

<https://clashgithub.com/>

<https://github.com/aiboboxx/v2rayfree>

<https://github.com/free18/v2ray>

<https://wenode.cc/>

<https://v2rayshare.com/>

<https://onenode.cc/>

获取节点的一个电报群：<https://t.me/zhibeii>
(下载导入 txt 内的所有链接)

.....

打开上面能进入的网址，选择最新日期的帖子进去，找到订阅链接 — v2ray 订阅链接：复制对应客户端的订阅链接

v2r 订阅链接一般以 .txt 结尾

clash 订阅一般以 yam 结尾

这类免费订阅很多，可以在国外搜索上搜索

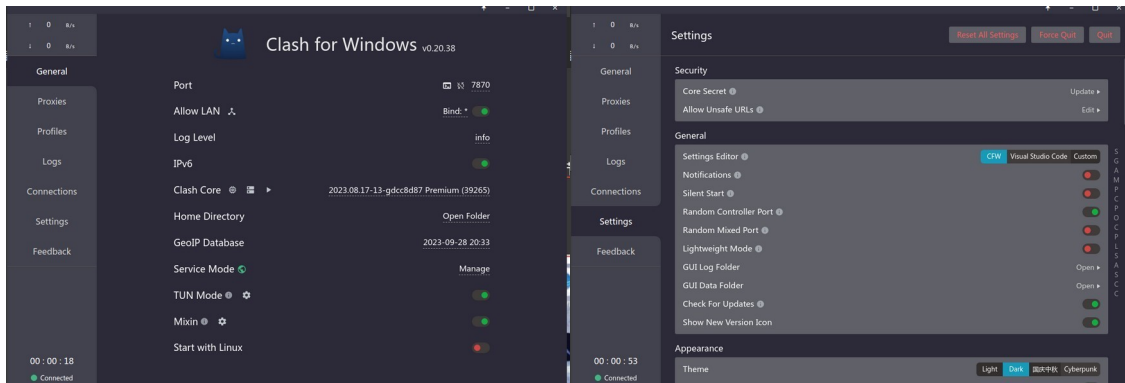
v2r 免费订阅 或者 clash 免费订阅

也可以在 github 上搜索订阅

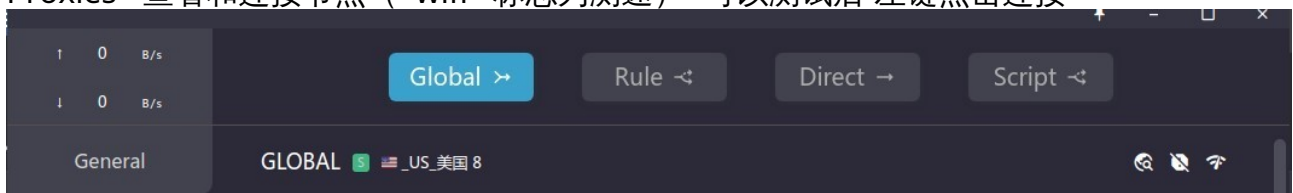


注意：最好使用全局模式而不是默认的规则模式，开源访问控制，禁止不需要代理的软件使用代理或者只允许需要代理的应用使用代理。其他注意事项和 v2r 一样

电脑 clash 操作图示：



如左图 wgeneral 设置好 右图 settings 的 quit 是退出程序
 profiles (添加订阅) 添加后点击 download 然后右键 导入成功的订阅
 update 刷新节点 (有些订阅导入下载需要魔法, 有些开魔法不一定能导入成功, 所以更建议用 v2rayn)
 Proxies 查看和连接节点 (wifi 标志为测速) 可以测试后 左键点击连接



方法三

开源的 protonvpn

软件地点为中立国瑞士，不受美国 / 欧盟 14 眼监管，产品有 proton 匿名邮箱 云盘 vpn 等，vpn 为 fdroid 开源，盈利模式为付费用用户免费，免费用户不限速不限流量。

有 openvpn/wireguard/ 自己 stealth (能流量伪装和混淆) - 免费

Tor 网络 (vip 付费服务，ps 可以使用他免费连接，然后用 orbot/tor 浏览器等连 tor 代理，不用付费走 proton 的 tor)

广告拦截 (付费，浏览器插件也可以拦广告没必要)

专线和额外再加密 (付费，连上之后自己在用 otr 代理来加密，所以此功能也没有必要)

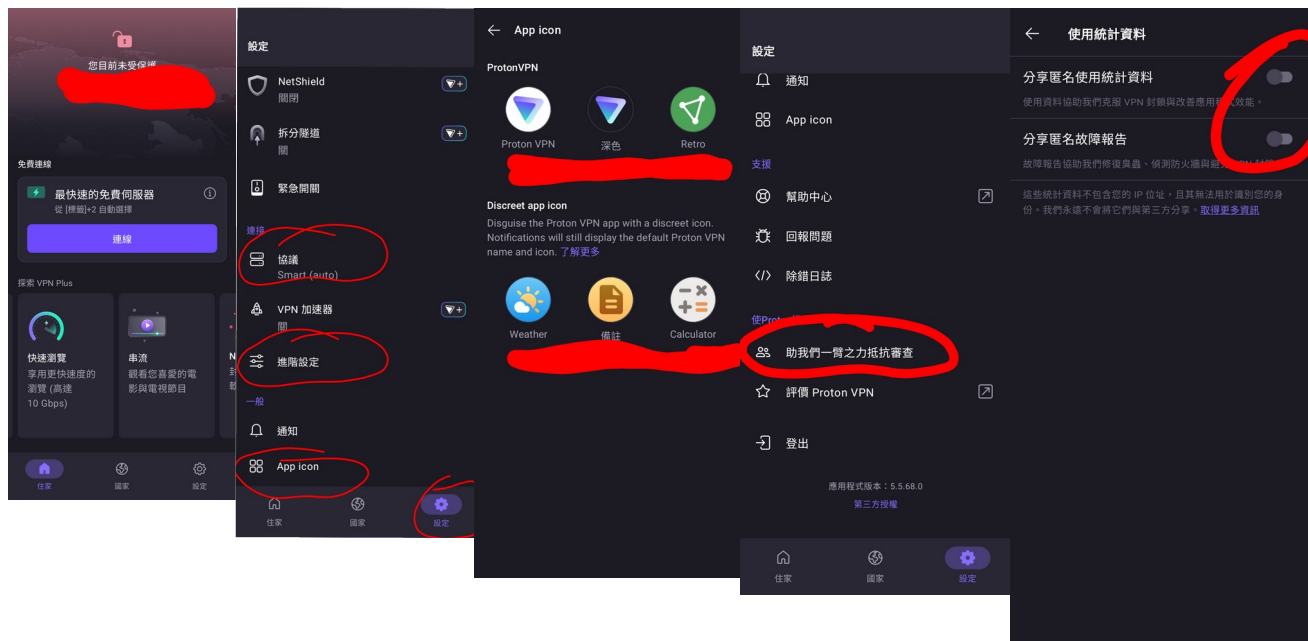
因此免费使用足以

软件注册和第一次登陆需要挂其他魔法，账户和 ptotonmail 匿名邮箱通用，建议使用 gmail，一次性邮箱注册登陆，或者 proton 账户注册 (注册界面下方小字点击就能注册 proton 通用账号)

缺点：新版本免费版只能全局 vpn，不能分应用，因此非类原生设备不能作为主用，除非设备系统和软件环境都为自由开源

操作提醒：设置内关闭用户隐私收集选项，开启图标伪装

操作流程图：



方法四 tor 洋葱匿名网络

(可能需要用方法一二的魔法参与三)

优点：

使用 tor 网络 匿名魔法，中间三次节点跳转，每次一跳转一加密，每个服务器自己也不知道流量内容，即使被知道所有服务器地址，因为采取的是众多服务器随行选三个来跳转，因此相对安全，比较可能的是进出口被抓流量，所以尽量使用未公开网桥连接而非直连，而且要经常性更换网桥

非商业，节点来自各地爱好者，同时也是暗网工具。

缺点：

速度不如一般高速魔法，因为要转三次节点到外网

软件名：

orbot (全局代理) /InviZible Pro (全局) /tor 浏览器 (网页代理)

tor 浏览器为网页内置 tor 代理的网页浏览器

Orbot/InviZible Pro 为移动安卓端 / 苹果端全局 / 指定 app 走 tor 网络代理工具

tor 浏览器全平台客户端官网：<https://www.torproject.org/zh-CN/download/>

inzivible 为安卓上的 tor 代理客户端，在 fdroid 下载，orbot 可以在谷歌应用商店下载，但不如 inzivible 功能全面

Inzivible fdroid 商店下载链接：

https://f-droid.org/zh_Hans/packages/pan.alexander.tordnscrypt.stable/

切忌不要用 tor 访问大陆实名网站服务 ,tor 出口是公开的，来自 tor 出口的流量大陆网站会重点关照

使用 tor 网络连接国际互联网（这种安全性最好），大陆使用需要借助网桥，不能直连（被大陆地区屏蔽），三种网桥模式对比



其他网桥推荐 2024 年推出的 WebTunnel

介绍 :<https://bridges.torproject.org/>

2024 年，Tor 项目正式推出了模拟 HTTPS 流量的新网桥 WebTunnel。网桥是不公开的 Tor 中继。WebTunnel 通过模拟 HTTPS 流量增加屏蔽 Tor 连接的难度。审查者不可能完全屏蔽 HTTPS 连接，因为这会导致绝大部分服务无法访问。Tor 项目称，WebTunnel 的工作原理是将负载（Payload）连接包装成类 WebSocket HTTPS 连接，在网络观察者眼里就像普通的 HTTPS (WebSocket) 连接。使用 WebTunnel 网桥需要用户去获取相关网桥地址，手动添加到 Tor 浏览器

网桥申请需要先连接其他代理，方法如下：

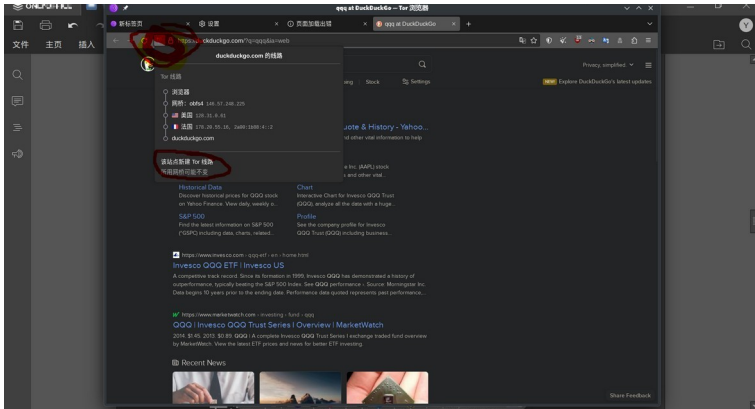
1. 访问 <https://bridges.torproject.org/options/> 并按照说明操作，此方法可以获取 obfs4 网桥和 web 网桥
2. 使用 Gmail 或 Riseup 的邮箱服务发送电子邮件至 bridges@torproject.org, 从 Tor 浏览器内请求网桥
3. 通过 Telegram 向 @GetBridgesBot 发送消息。在聊天中点击“开始”，或者输入 /Start 或 /bridges。

此方法只能获取 obfs4 网桥

安卓手机 fdroid 自由开源应用商店内搜索 invizible 安装启动，快速设置 - 网桥，获取私人网桥 -，选择类似请求网桥 -- 输入验证码确认获取，此方可以获取所有类型网桥

注意事项：如果是获取 web 网桥，可以选择方法 1 或者方法 4, 如果是获取 obfs 网桥，则推荐方法 3, 其次方法 2

将网桥导入软件 tor 网桥设置里，一行一个网桥，可以添加多个
然后连接无速度 点新身份 / 刷新 更换节点
按步骤 A 网桥连接好后，测试网页访问正常（连不上就换网桥或者用非 ofbs4）



B 其他应用走 tor 代理
tor 的默认本地 ip 和端口为 socks5 代理：127.0.0.1 9150/ 或者 9050
代理模式为 socks5
tor 浏览器连接好以后 别关浏览器
（1）系统全局：linux 发行版
系统设置 - 网络 - 代理服务器 - 手动地址 socks5 模式，地址 127.0.0.1
端口：9150 / 连不上就 9050
一般 tor 浏览器用的 9150 端口 ,tor 代理 app 用的 9050



然后所有应用都走 tor 网络

windows 11 实测

(失败案例：win11 设置 - 网络连接 - 代理 - 手动代理 代理 ip 地址：127.0.0.1 端口 9150 结果连不上，因为 windows 系统设置不支持 socks5 代理)

因此选用 v2rayn 软件 来全局代理走 tor

打开 v2rayn(下载链接在 <https://clashnode.com/f/client>)

点击右上角 服务器 添加 socks 服务器 别名随意填

地址 127.0.0.1 端口 9150 (连不上改 9050) 确认

右键点击新添加的服务节点 设为活动服务器

软件最下方 系统代理：自动配置系统代理

路由：全局或者绕过大陆

即可使用全局 tor

(2) 设置应用单独 (让有的走 tor, 有的不走，大陆内容走代理访问比较慢)：

1. 软件设置有 能单独设置代理的软件 (比如火狐浏览器，电报等) - 设置：代理 类型 socks5

地址：地址 127.0.0.1 端口：9150 (或者 9050) 代理类型 socks5

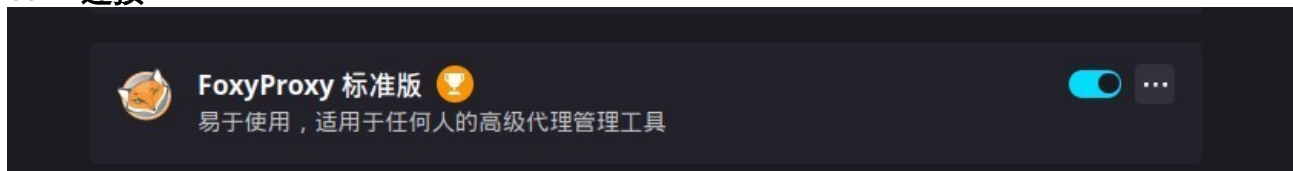
2. 火狐浏览器 (网络的独立的，需要设置代理)

火狐软件设置 代理 同上

建议用火狐代理插件 代理，开关方便，自带设置的代理不一定能连上

火狐浏览器 设置 插件 搜索 foxproxy 下载安装

tor 连接



打开点击插件图标 打开 插件 设置 代理：保存 点击插件图标 连接

编辑代理 127.0.0.1:9150

标题或描述 (可选)	代理类型
<input type="text" value="title"/>	SOCKS5
颜色	代理 IP 地址或 DNS 名称 ★
<input type="text" value="#66cc66"/>	<input type="text" value="127.0.0.1"/>
Send DNS through SOCKS5 proxy	端口 ★
<input checked="" type="checkbox"/>	<input type="text" value="9150"/>
	用户名 (可选)
	<input type="text" value="username"/>
	密码 (可选) 🔒
	<input type="text" value="password"/>
	<input type="button" value="取消"/> <input type="button" value="保存并添加另一个"/> <input type="button" value="保存并编辑模式"/> <input type="button" value="保存"/>

电报单独设置：电报 设置找到代理选项 (原理步骤同火狐)

补充： tor 浏览器连不上怎么办，其他 vpn 加 tor 代理，其他 vpn (全局) 连上，然后 tor 连接

设置 - tor 连接，代理设置 (设置成其他 vpn 的代理 ip 和端口，

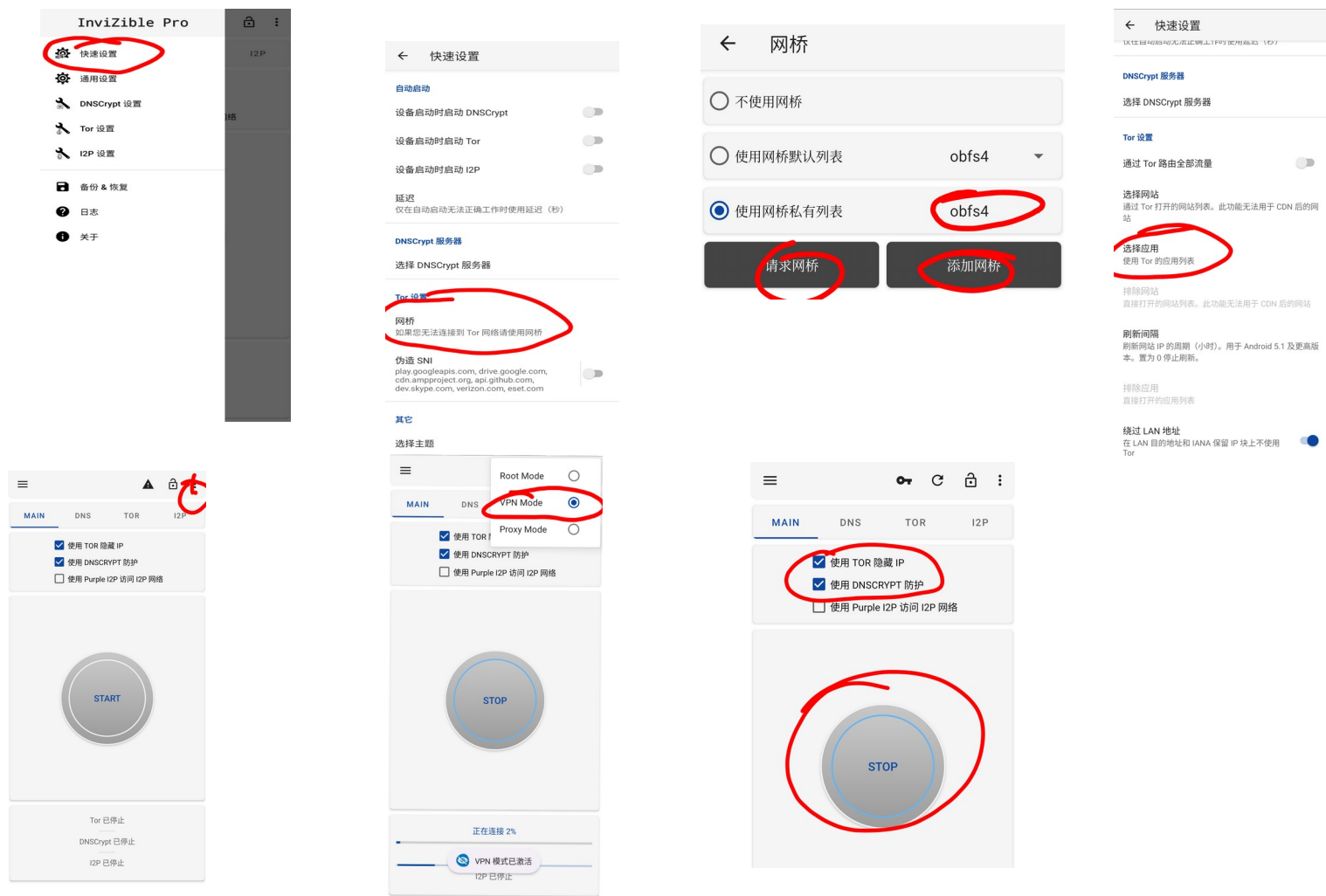
Clash 默认 -socks5 协议，127.0.0.1,7890，v2ryaa 默认 -socks5,localhost,20170

wireguard 不用设置 直接连上然后再连 tor 就行，其他应用走 tor 网络参考前文
但是这种方式会降低匿名性

C 安卓端 / 苹果端：orbot/InviZible Pro/tor 浏览器

打开 invizible，点击 快速设置 配置连接方式 - 定制网桥 - 下一步 -
内置网桥 / 获取网桥 / 手动输入网桥地址（看上文如何获取网桥） - 设置哪些不走代理 -
选择 vpn 模式 - 点击启动
如果会使用代理模式，则优先考虑用它，需要在走代理的软件内开启 sock5 本地代理端口设置

图示流程：



（orbot 不许截图，所以无图文而且新版无代理模式只有 vpn 模式，只有上面的 InviZible Pro，原理和电脑端一样）

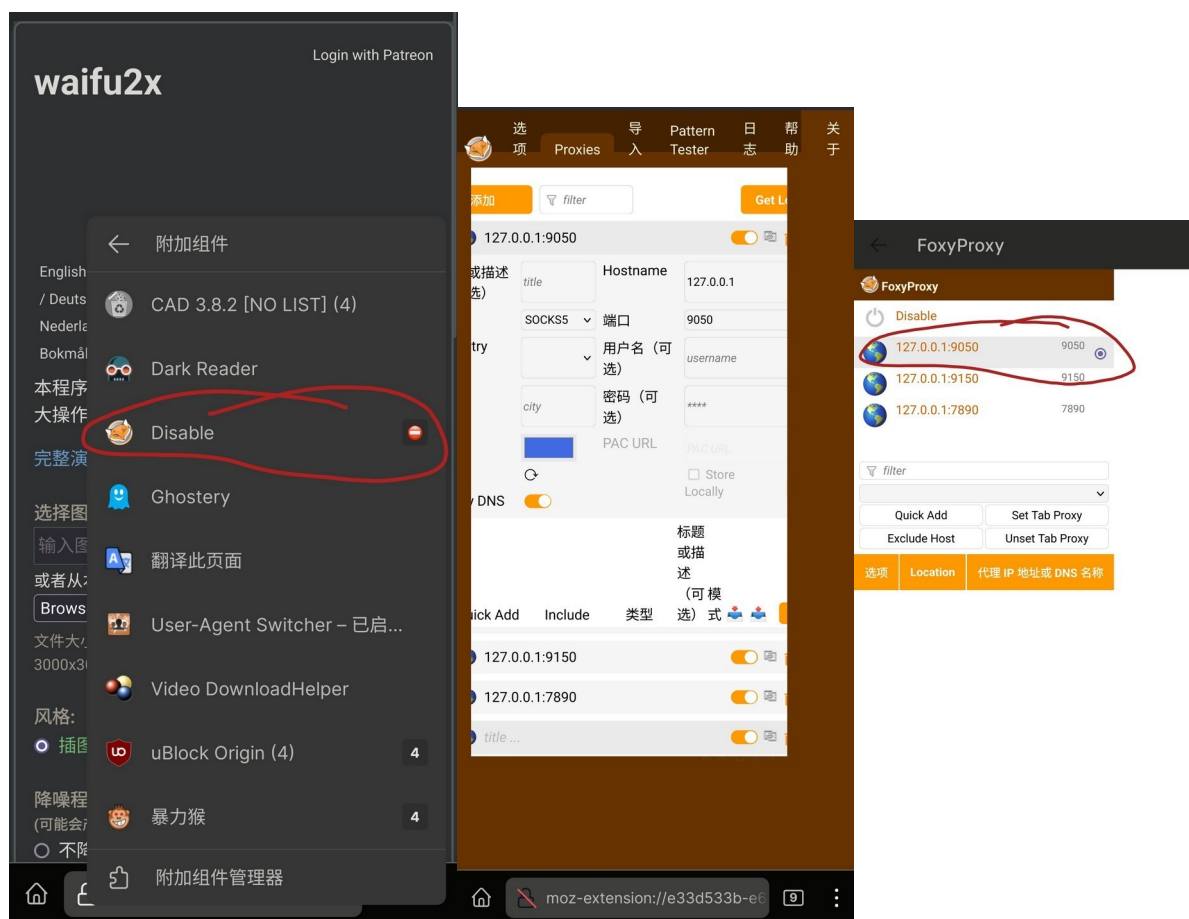
连接后无网速点击刷新 更换节点

注意：设置里有指定 app 走 vpn，或者指定软件绕过，让需要走代理的软件走代理，默认是全局
切忌不要用 tor 访问大陆实名网站服务，tor 出口是公开的，来自 tor 出口的流量大陆网站会重点关照
orbot/invizible 的代理地址和默认端口为 地址 12.0.0.1 端口：9050，如果用的是代理模式为而不是 vpn 模式。
普通软件要走 tor 代理需要在软件内开启本地 tor 代理端口实现代理，代理模式比 vpn 模式更安全，
因为不容易被私有系统和软件检测到设备开启了 vpn 模块，而且 vpn 模式只能运行一个软件开启，
代理模式可以几个代理软件一起使用，
每一个占用不同代理端口

如果任何网桥都连不上只能考虑加前置 vpn，先走普通 vpn 再走 tor，方法为先开启其他带代理 /vpn 软件的 vpn 模式连上
inivible 选择 proxy 代理模式，然后需要代理的软件内开启 tor 的 socks 本地代理端口 (127.0.0.1:9050)，即可使用 tor

代理模式对于手机火狐

火狐浏览器安卓版用火狐代理插件 代理，火狐浏览器 设置 插件 搜索找到 foxproxy 下载安装打开点击插件图标 打开 插件 设置 选项 代理：保存 点击 插件图标 连接



电报单独设置：电报 设置找到代理选项 （原理步骤同火狐）

此种方法实现手机全局代理的办法是

手机设置 - 网络 wifi- 选择自己连的 wifi- 代理（高级设置） - 设置 http 代理 地址为 127.0.0.1 端口号看 软件设置 http 代理那 一般为 8118，跟换 wifi 后得重新设置，此法对火狐浏览器无效，火狐浏览器得单独用 proxy 代理插件设置，参看前文

代理设置

保存

无

手动

✓

代理自动配置

配置项

服务器

127.0.0.1

端口

8118

对以下网址不使用代理

添加

Tor 设置

✓

Tor 设置

Tor 将跟踪最近连接到主机的连接，并尝试重用相同的出口节点。当前，如果两个地址处于同一 /16 区间则“过于接近”。

TrackHostExits

Tor will track recent connections to hosts and attempt to reuse the same exit node for each. This option may help avoid endless captcha.

IsolateDestAddr

不与目的地址不同的流共享链路。

HTTP Tunnel Port

8118

取消 确定

SOCKSPort

打开此端口监听来自使用 SOCKS 的应用的连接。

启用 HTTP 隧道

HTTP Tunnel Port

打开此端口监听使用 HTTP CONNECT 而不是 SOCKS 协议的代理连接。

启用透明代理

Transport

在 gnu linux 安装使用 tor 浏览器后开启全局系统代理方法为

linux 终端输入： export ALL_PROXY=socks5://127.0.0.1:9150

关闭代理指令为：

unset socks5_proxy

unset all_proxy

如果是 kde 或者 gnome 桌面，可在桌面设置 - 代理里直接添加 socks5 代理
127.0.0.1:9150

方法六．自建节点

优点：速度快，超低延迟自建节点大致有三种方法，1 是购买 vps 和域名从零开始搭建节点，2 是使用域名在 cloudflare 上利用 cf 的全球服务器以及 cf pages 部署自己的节点订阅，部署代码有现成的开源项目可用
对于方法 3

- 自建节点订阅教程：

通过 cloudflare 免费自建个人专属 vmess 节点订阅（使用免费域名）并在 v2r/clash/sinbox 代理软件内使用，此方法安全性不如 tor，但是比各种不知商业背景的商业公开节点和不知来源的免费节点安全，高速低延迟优于 tor，可作为 tor 的备用（可用此节点来获取 tor 网桥和高速下载文件）

[1.cf 节点视频教程](https://m.youtube.com/watch?pp=ygUKY2xvdWRmbGFyZQ%3D%3D&v=cqQioz_Kdag)

[2. 官方精简视频教程](<https://m.youtube.com/watch?v=59THrmJhmAw>) 请结合教程 1 一起看

[3. 教程所需 github 源项目网站及文字教程说明](<https://github.com/cmliu/edgetunnel.git>)

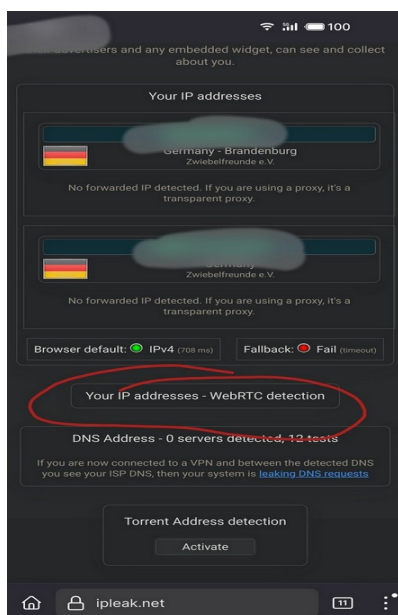
- [cloudflare 国际官网](<https://www.cloudflare.com/>)

- [免费域名申请网站示例](<https://dynv6.com/>)

- 问题故障解决：下面视频 up 主为此节点部署开源项目作者，在他的视频列表能找到所有相关教程

<https://m.youtube.com/watch?v=s91zjpw3-P8&t=1446s&pp=2AGmC5ACaQ%3D%3D> /

- 付费租借 vps 和域名自建节点：（此方法自建节点被墙后更换 ip 可能要额外付费，使用频率高容易被检测，因为一般是固定代理 ip，长期连接固定的 ip 而且高流量一眼看出来是代理节点，出问题解决也较麻烦）油管搜索相关自建节点教程



重要提醒 ip 检测网站 查看是否 ip 泄露，特别是 webrtc

<http://ipleak.net/>

如有 ip 泄漏 请使用火狐浏览器 + webrtc 插件屏蔽

注意事项：

所有翻墙软件使用原则 都是只让要翻墙的软件翻墙，禁止国内实名的软件和服务翻墙来自爆，身份隔离是关键，不要关联任何墙外墙内信息，保护账户，密码，头像，id 等，照片等，墙外不要使用和泄漏 任何真实个人信息，翻墙后尽量减少商业网站访问，多使用自由开源的网站服务，避免被社工

避免使用国产浏览器（比如自带浏览器和腾讯浏览器）和国产输入法（比如 自带输入法和搜狗输入法等），避免他们泄漏个人信息和设备信息

多使用自由开源软件替代非开源商业软件，有条件的请刷机类原生操作系统并做设备信息伪装和地理信息伪装，避免国产系统的跟踪，无条件刷机的 请 自备 shelter（）沙盒和元萝卜沙盒用于环境隔离

Shelter 地址

https://f-droid.org/zh_Hans/packages/net.typeblog.shelter/

元萝卜下载地址 <https://github.com/Katana-Official/Meta>

有条件的最好多准备一台移动设备 刷机类原生系统后作为专用和日常生活用机隔离（不插卡）

学会使用 fdroid 自由软件商店 下载自由开源应用替换 国产 商业应用

https://f-droid.org/zh_Hans/

魔法不能保证绝对安全，勿使用不能确保安全性的公用 wifi（有一些公共 wifi 会钓鱼），勿装反诈类 app，被要求装请放在 shelter 沙盒或 虚拟机如 vmos 里

不要发表冲塔言论，不要用自己手机号码注册海外账户，用虚拟号 / 解码平台注册 sms(接码注册账户或者直接购买，低价) <https://sms-activate.org/>

请用 开源的火狐国际版浏览器家族 上网 比如 安卓手机火狐第三方 iceraven

<https://github.com/fork-maintainers/iceraven-browser/releases>

火狐国际版电脑版

<https://www.mozilla.org/en-US/firefox/all/#product-desktop-release>

设置开启：减少 cookie, 跟踪保护 严格，开启https only,(可选 退出时删除浏览数据)，关闭数据收集和遥测（原版火狐才有）

下载插件 ublock（广告拦截），ghostery/privacy（反跟踪），webRTC(防止 ip 泄漏) 或者基于火狐的 tor 浏览器（自带 tor 网络） <https://www.torproject.org/>

如果要使用谷歌浏览器家族，请使用 开源安全的 brave 浏览器 或 chroimum 浏览器（谷歌浏览器的开源版），不要使用 chrome（非开源）

,

输入法推荐 fcitx5 小企鹅 输入法<https://fcitx5-android.github.io/>