软件版本信息

clash verge V1.7.7

内核v1.18.10 Mihomo

Proxifier for Mac v3.11

macOS Version 14.3

主要解决的问题

渗透测试时, 资产可能比较零散, 小程序和web资产都有.

平常测试小程序采用的是proxifier配置代理, 转发到burp 8080.

但是由于proxifier和clash都设置系统代理会loop, 所以测试小程序时需要退出clash. 但是这样就无法访问google等外网, 进行资料的搜索.

> 经过测试, 由于clash的不知名原因, 导致有时有玄学问题, 所以我clash退出都是先设置直连, 在设置关闭系统代理, 然后退出
>
> 避免出玄学问题, 导致重启burp和proxifier

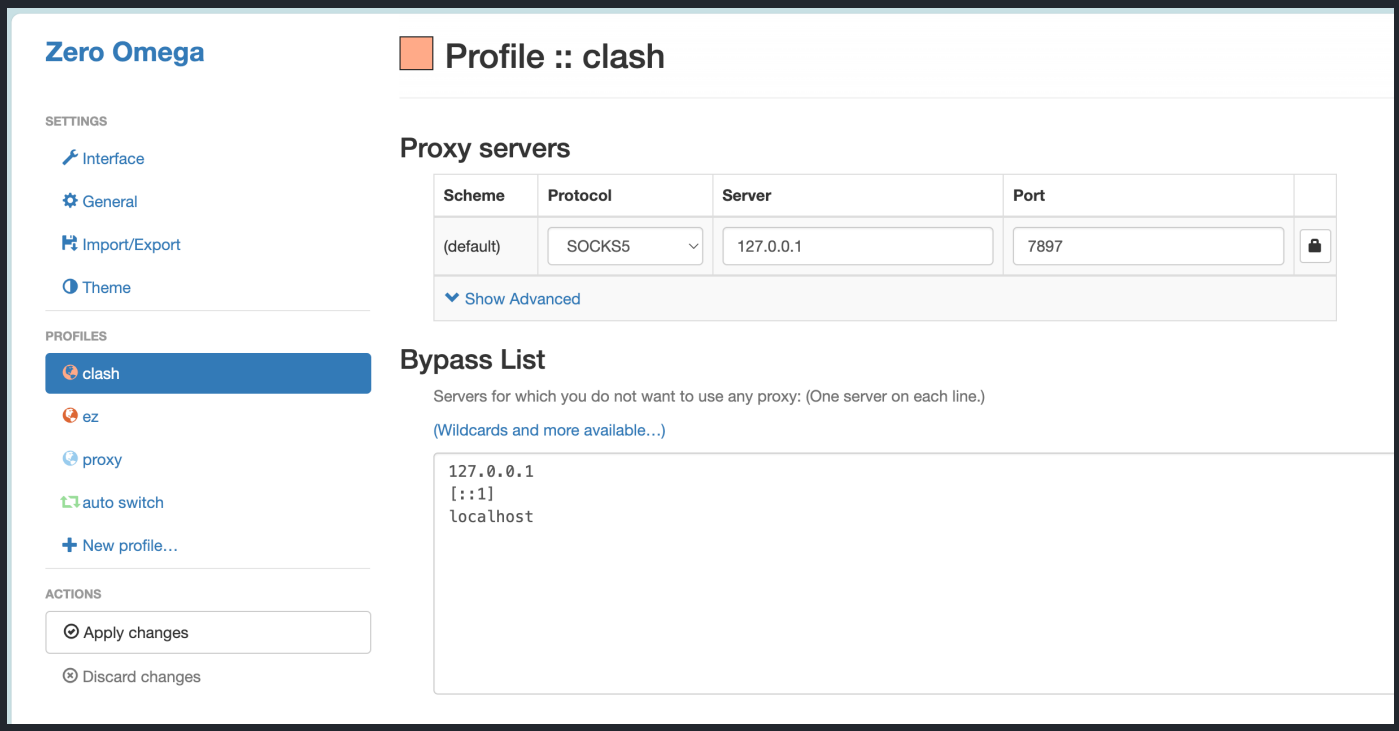
需要走代理的程序

1. 浏览器
2. discord
3. chatgpt

浏览器不是问题, 可以通过ZeroOmega(符合Manifest V3)配置代理

> SwitchyOmega即将被淘汰, 建议更换

配置如下, bypass list可以添加不代理的网站, 当然也可以在clash verge中配置



由于只需要解决两个软件的配置问题, 所以我们分别来解决

1. discord
2. chatgpt

discord

discord由于是走的UDP协议, 所以proxifier不生效, 即使配置了代理, 也无法访问

win的话可以参考github项目, 需要改dll

`https://github.com/aiqinxuancai/discord-proxy`

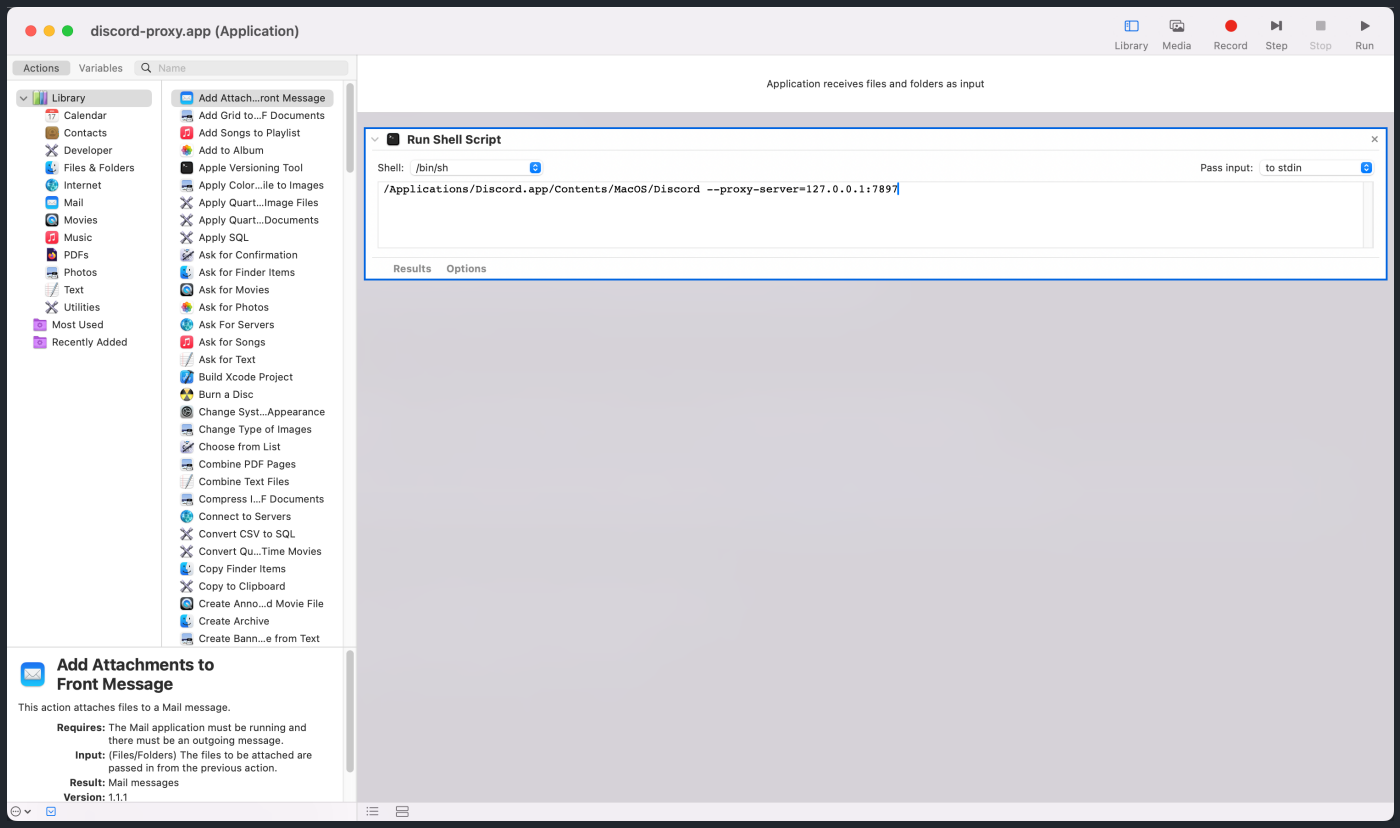
mac经过查询发现有类似的命令, 并且不需要改dll

`https://gist.github.com/Colk-tech/157fd6c81032dde528d3a22434b8f3e6`

实现

使用Automator新建一个.app文件, 命名为discord-proxy.app, 使其运行sh脚本, 端口填自己的.

```
/Applications/Discord.app/Contents/MacOS/Discord --proxy-server=127.0.0.1:7897 --ignore-certificate-errors
```



> 这一步的意义在于不需要保留丑丑的终端界面且更加方便
>
> 运行时, 可以通过spotlight或者raycast一类启动

绕过更新

不绕过的结果就会卡更新界面, 因为discord 更新不走代理. 上面的`--ignore-certificate-errors`参数也是为了防止不更新导致的一些证书错误.

```
nuw4nd4@Nuw4nd4:~
$ cd /Users/nuw4nd4/Library/Application\ Support/discord/
```

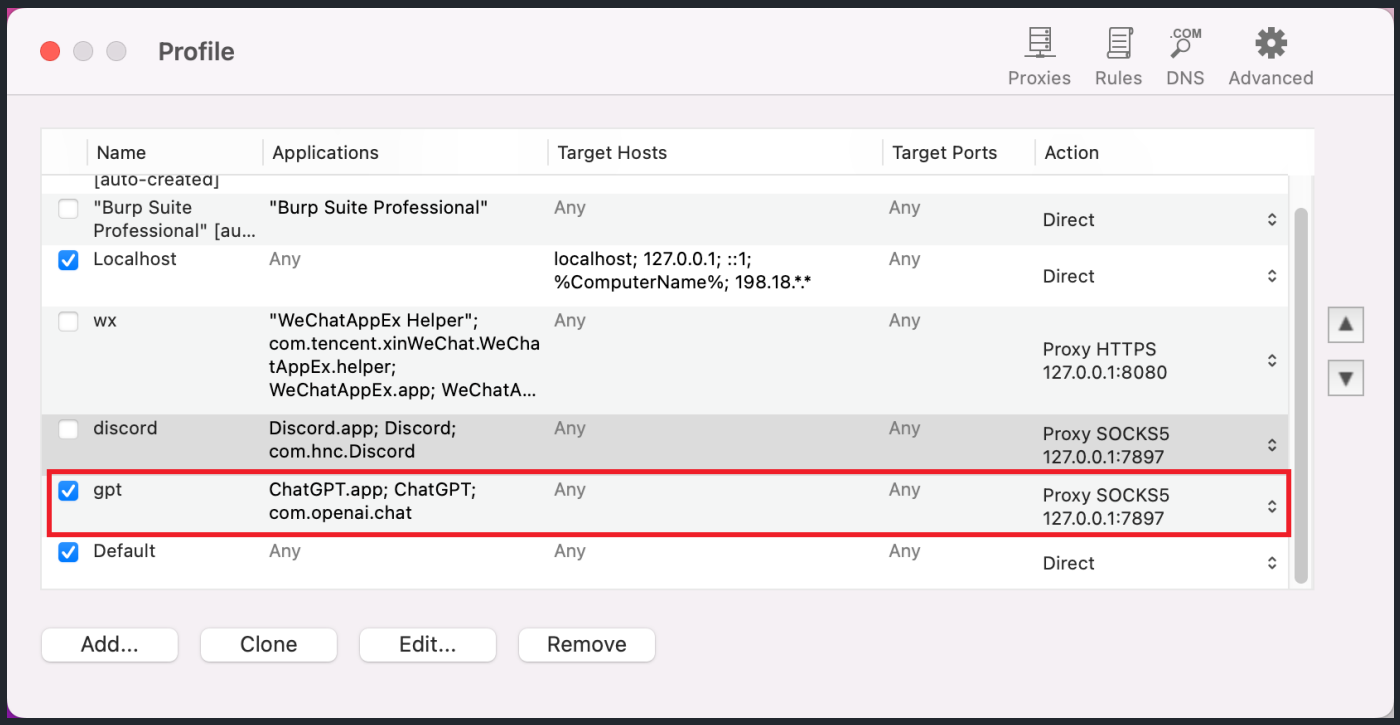
```
nuw4nd4@Nuw4nd4:~/Library/Application Support/discord
$ cat settings.json
{
  "chromiumSwitches": {},
  "IS_MAXIMIZED": true,
  "IS_MINIMIZED": false,

"DANGEROUS_ENABLE_DEVTOOLS_ONLY_ENABLE_IF_YOU_KNOW_WHAT_YOURE_DOING":
true,
  "MIN_WIDTH": 940,
  "MIN_HEIGHT": 500,
  "SKIP_HOST_UPDATE": true,
  "SKIP_MODULE_UPDATE": true
}↵
```

chatGPT

gpt就比较友善, 完全不需要考虑, 直接proxifier配上代理就能正常运行, 包括语音对话功能.

实现

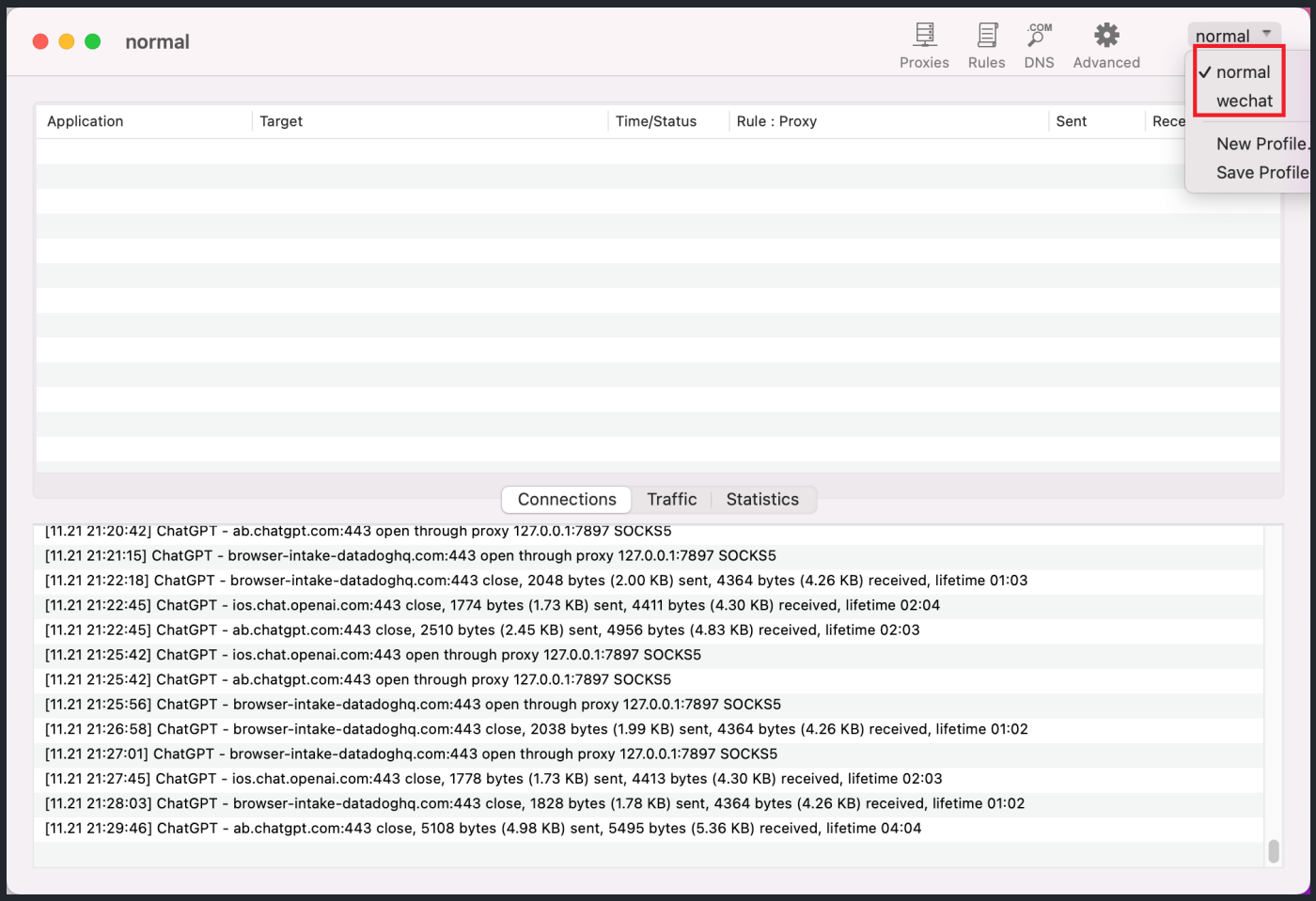
直接在proxifier中配置即可

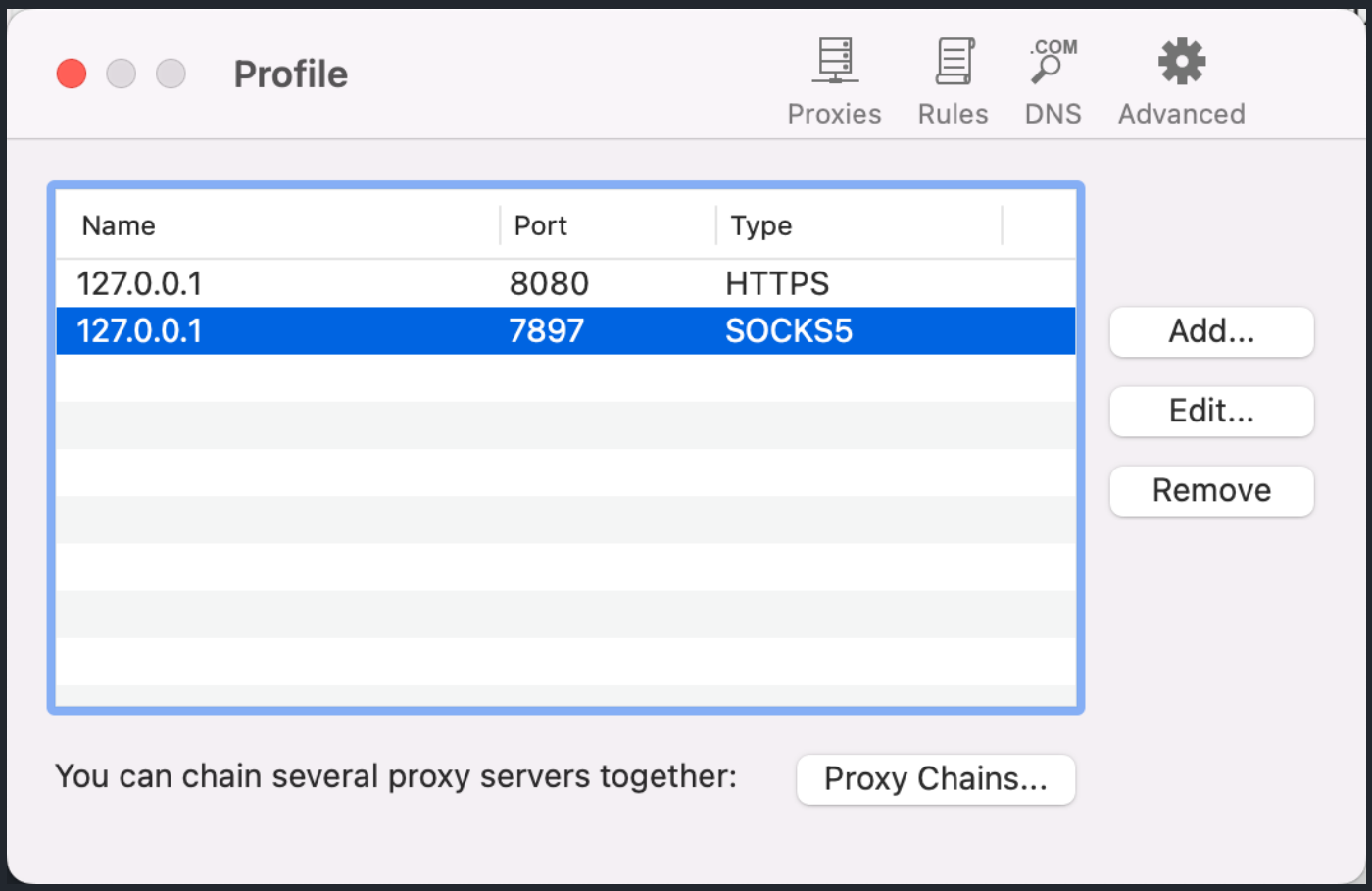


目前的配置

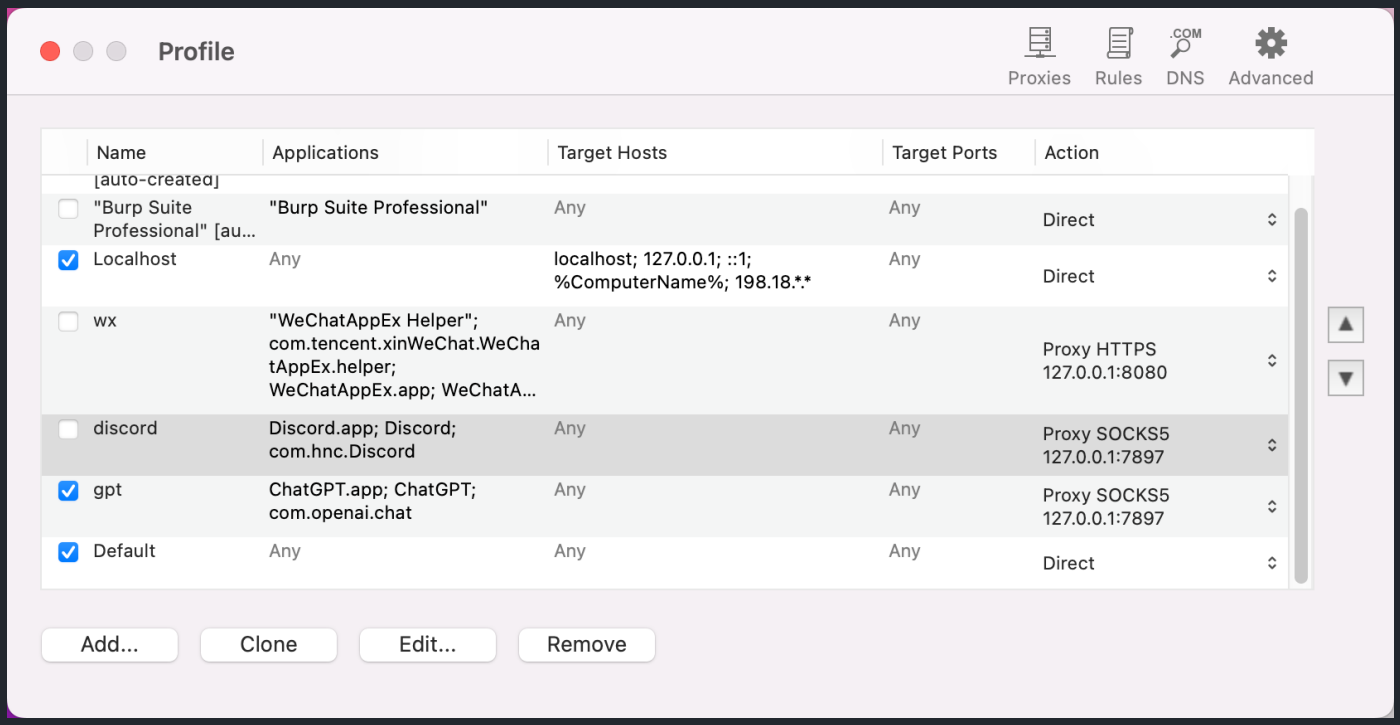
共计两个配置文件, normal(平时使用)和wechat(微信抓包时配置)

需要更改时, 只需要切换右上角的配置文件即可


normal
Proxies
Rules
DNS
Advanced
normal
normal
wechat
New Profile...
Save Profile
Application
Target
Time/Status
Rule : Proxy
Sent
Rece
Connections
Traffic
Statistics
[11.21 21:20:42] ChatGPT - ab.chatgpt.com:443 open through proxy 127.0.0.1:7897 SOCKS5
[11.21 21:21:15] ChatGPT - browser-intake-datadoghq.com:443 open through proxy 127.0.0.1:7897 SOCKS5
[11.21 21:22:18] ChatGPT - browser-intake-datadoghq.com:443 close, 2048 bytes (2.00 KB) sent, 4364 bytes (4.26 KB) received, lifetime 01:03
[11.21 21:22:45] ChatGPT - ios.chat.openai.com:443 close, 1774 bytes (1.73 KB) sent, 4411 bytes (4.30 KB) received, lifetime 02:04
[11.21 21:22:45] ChatGPT - ab.chatgpt.com:443 close, 2510 bytes (2.45 KB) sent, 4956 bytes (4.83 KB) received, lifetime 02:03
[11.21 21:25:42] ChatGPT - ios.chat.openai.com:443 open through proxy 127.0.0.1:7897 SOCKS5
[11.21 21:25:42] ChatGPT - ab.chatgpt.com:443 open through proxy 127.0.0.1:7897 SOCKS5
[11.21 21:25:56] ChatGPT - browser-intake-datadoghq.com:443 open through proxy 127.0.0.1:7897 SOCKS5
[11.21 21:26:58] ChatGPT - browser-intake-datadoghq.com:443 close, 2038 bytes (1.99 KB) sent, 4364 bytes (4.26 KB) received, lifetime 01:02
[11.21 21:27:01] ChatGPT - browser-intake-datadoghq.com:443 open through proxy 127.0.0.1:7897 SOCKS5
[11.21 21:27:45] ChatGPT - ios.chat.openai.com:443 close, 1778 bytes (1.73 KB) sent, 4413 bytes (4.30 KB) received, lifetime 02:03
[11.21 21:28:03] ChatGPT - browser-intake-datadoghq.com:443 close, 1828 bytes (1.78 KB) sent, 4364 bytes (4.26 KB) received, lifetime 01:02
[11.21 21:29:46] ChatGPT - ab.chatgpt.com:443 close, 5108 bytes (4.98 KB) sent, 5495 bytes (5.36 KB) received, lifetime 04:04

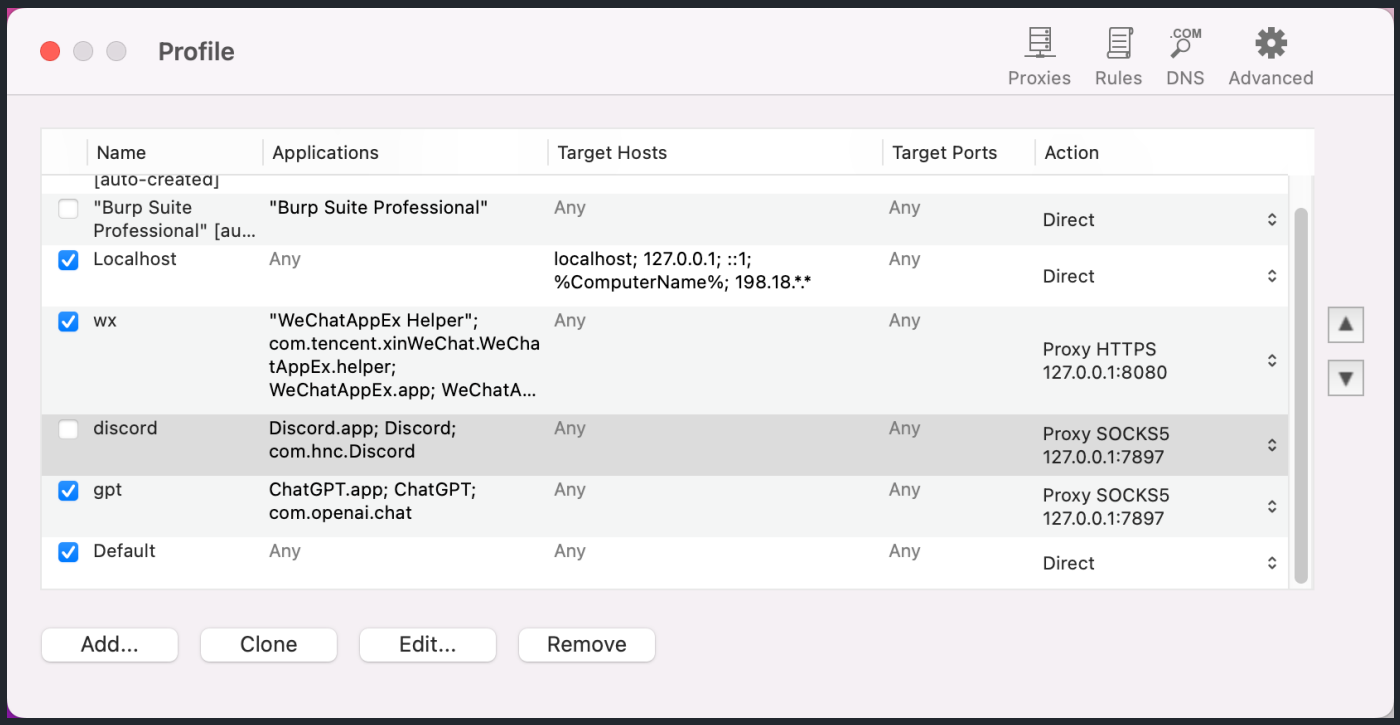

Profile
Proxies
Rules
DNS
Advanced
Name
Port
Type
127.0.0.1
8080
HTTPS
127.0.0.1
7897
SOCKS5
Add...
Edit...
Remove
You can chain several proxy servers together:
Proxy Chains...

normal



wechat

区别就是多了个微信小程序的代理



遇到一些问题

ChatGPT.app显示地域限制

场景:

昨天晚上配置完毕, 测试时GPT正常访问. 第二天移动到单位, 使用随身wifi链接, 在没有改动任何配置的情况下, GPT显示地域限制(浏览器GPT正常可访问).

解决方法:

玄学, 打开然后关闭tun模式.

discord.app卡更新

场景:

discord更新了, 启动时卡在更新界面, proxifier无流量经过

原因在这里也有写, 我一开始没设置后续的

`https://gist.github.com/Colk-tech/157fd6c81032dde528d3a22434b8f3e6`

解决方法:

上面绕过更新有写

steam创意工坊

这里需要有个表情包()

> 你家族有精神病史吗？我有个叔叔买MAC打游戏

场景:

steam创意工坊, 在windows上是通过steamwebhelper.exe控制的, 但是我在mac上没找到.

解决方法:

steam++, 有点背离初衷了.

放弃

到这里决定放弃, 本身是为了解决小程序抓包的繁琐问题, 但是由于clash系统代理的关闭, 导致了更多的问题, 反而使得事情变得更麻烦了.

留下这篇文章给有需要的人.