阅读本文前请认真阅读中华人民共和国网络安全法

国务院《计算机信息网络国际联网管理暂行规定》第6条：任何单位和个人不得自行建立或者使用其他信道进行国际联网。

本文所述均作为一个网络技术爱好者，从技术层面学习相关协议和代理技术，以便更全面地理解网络通信、数据传输、加密技术、抗封锁机制等知识。

从GFW说起

GFW是Great Fire Wall的缩写，即“长城防火墙”，是中国的互联网审查和封锁系统，用于过滤、监控、屏蔽特定的网络内容，控制中国境内用户对全球互联网的访问。他的主要手段如下：

- 直接封锁特定网站IP 或域名。
- 干扰加密通信
- 主动探测和干扰
- DNS污染

详细的信息可以参考https://gfw.report/talks/imc20/zh/这篇论文，文章通过实验证明，GFW会主动检测加密数据包，并会产生与之类似的模拟数据包，并从全国数以万计的服务器向可疑服务器发出数据包进行检测。还会从数据包的发送频率、长度等进行检测。以上文章发表于2020年因此还是非常具有参考价值，同时也不难想象如今的GFW如果结合AI模型会成为更强大的互联网封锁系统。

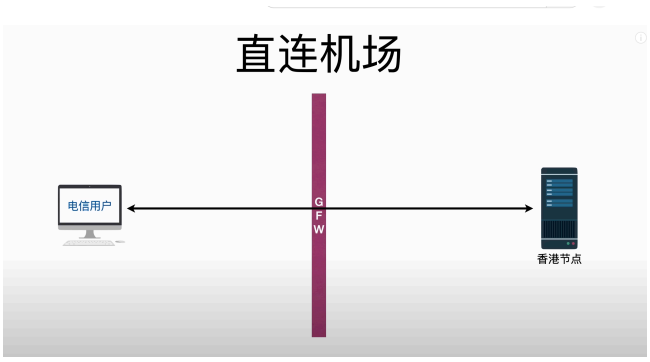
科学上网

基于上一节的内容，广大网民在研究网络通信技术的过程中，探索了各种数据传输和加密方法。

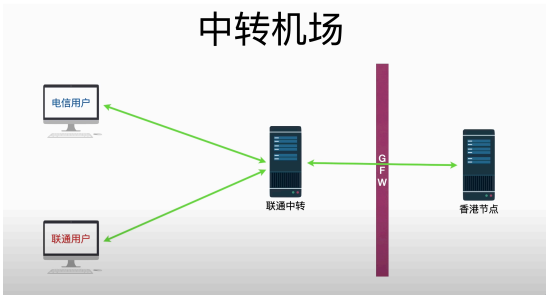
- 机场：顾名思义，是指提供代理服务或中转流量的服务器集群，通常用于绕过网络封锁、加速跨境访问，或者提高网络稳定性。

- VPN客户端：客户端内集成了代理服务器无需额外配置，也无需自找机场，方便快捷。但灵活性低。太依赖客户端的网络环境。

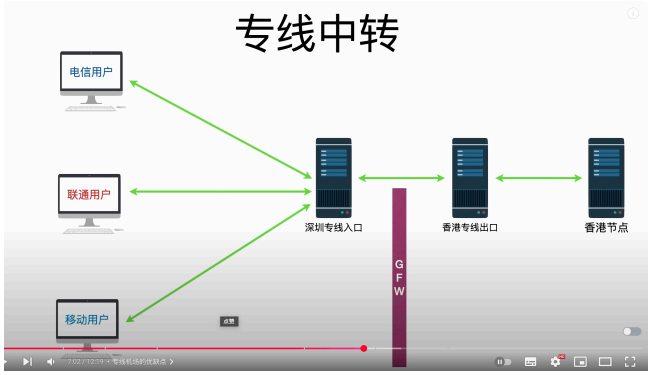
- 直连机场：本地需安装各种代理协议客户端，通过代理协议加密数据包后直接通过GFW和代理服务器直接建立连接。便宜，但大概率会网络拥塞，各运营商的网络出口也不一致，不同的运营商网速可能也不一致。



- 中转机场：境内会有代理服务器，数据包会先发至境内代理服务器，至后由代理服务器突破GFW讲数据包发送到境外代理服务器。避开了网络拥塞路径，减少了路由时间，速度快，是目前大多数机场的策略。



- 专线中转：GFW内的行为与中转机场一致，但是这里的中转机场与境外落地服务器数据发送走的是专线直接避开了GFW的审查，境外落地服务器再将数据包交给境外代理服务器。速度快，避开了GFW，但费用自然也高。



- 原则：

代理协议

通过上一节的内容，我们可以选择出满足自己需求的线路，本节更深入的了解各种代理协议，使得我们可以了解到我们可以在线路上选择那些协议进行数据传输。

- shadowsocks（ss）协议官方文档
  ss是专门设计用于绕过GFW的加密代理协议，ss基于socks5(传输层协议)，对数据包进行加密。在ss的基础上又有ShadowsocksR (SSR)（增强版，支持协议混淆）、Shadowsocks + 插件（如 Cloak、Obfs）（混淆 HTTP/TLS 伪装）。

- VMess
  VMess 是 V2Ray 代理框架中的专用协议，支持**流量加密、动态端口、混淆**，比 Shadowsocks 更难被检测。
  VMess + TCP（基础模式）
  VMess + WebSocket（WS）+ TLS（伪装成普通 HTTPS 流量）
  VMess + mKCP/QUIC（适用于低延迟、高速传输）
  VMess + gRPC（企业级伪装）
  VMess + UDP（适用于游戏）

- VLESS（V2Ray）
  VLESS 是 VMess 的升级版，去掉了认证加密（减少流量特征），适用于 高隐蔽、低延迟 的代理场景。比 VMess 更轻量，几乎无特征。支持 XTLS/Reality，流量像普通 HTTPS 访问。适用于高隐蔽需求，难以被封锁。需要额外配置 TLS 伪装，否则流量特征明显。

- Trojan
  Trojan 是一种 TLS 伪装代理协议，它让流量看起来像普通的 HTTPS 访问，使得防火墙难以检测。流量特征极低，像普通 HTTPS。 支持 TLS 1.3 加密，安全性高。难以被 GFW 检测和封锁。但是需要域名和证书，不适合低配服务器。

- Reality（VLESS+XTLS）
  Reality 是目前最强大的隐蔽代理协议，它通过伪装 HTTPS 证书、SNI、TLS 让流量几乎无法被检测。完全模拟真实 HTTPS 访问，GFW 难以识别。XTLS 低延迟、高性能。比 Trojan/VLESS 伪装能力更强。配置复杂，需要服务器支持。

- Project V
  Project V 是一个工具集合，它可以帮助你打造专属的基础通信网络。Project V 的核心工具称为 V2Ray，其主要负责网络协议和功能的实现，与其它 Project V 通信。关于此项目请直接参考官方文档V2Ray，Project V。

综上，基于上面的信息我们完全可以评估出适合自己的机场方案，对于日常使用的场景来说一家稳定的机场足够满足我们的需求。然后对于跨境电商等更加专业的场景我们需要在高速、稳定的基础上还要对IP的纯净度有更高的需求。

关于IP

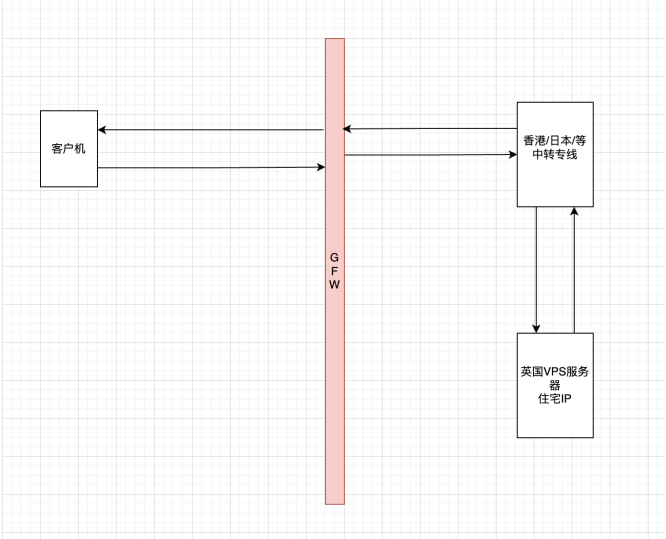
首先给出IP检测网站地址，以下给出我目前在使用机场IP的检测结果，来说明相关问题。

IDC 机房IP：IDC 机房IP特指机房专用的IP，除此外的 IP 均标记为 “家庭宽带IP"。

原生IP：绝大部分的家庭宽带 IP 都属于原生 IP，部分当地的本地 IDC 提供商也会使用原生 IP。 而一些全球性的跨国 IDC 服务商(AWS、GCP、Azure 等)为了方便管理，通常会购买一些大的 IP 段，然后广播到不同的国家, 这些即为 广播 IP。 所以，当一个 IP 显示为 原生 IP 时，通常代表这是一个家庭宽带 IP 或者本地 IDC提供商 IP。 当一个 IP 显示 为广播 IP 时，通常代表这是一个 非家庭宽带 IP，非本地 IDC 提供商 IP。

根据以上这些信息很容易被检测到由代理服务器转发的数据。

解决方案



如上图，给出了我们目前的方案，但是这其中也有不同的实现方式。

A. 购置英国VPS服务器、香港/日本较近的中转VPS服务器，分别在服务器上搭建IP代理协议。优点是稳定低延迟，甚至可以在英国部署一台闲置电脑24H开机，并配置好协议也可作为我们住宅IP服务器且IP绝对纯净，缺点是贵；
B. 仅购置英国住宅IP，使用机场线路中转，路线为客户端——代理协议——->机场——http/socks——>英国住宅IP。优点是价格低廉，缺点是延迟高，机场若不稳定整条线路就会垮掉。

为了更好的生活附上微信监控诠释