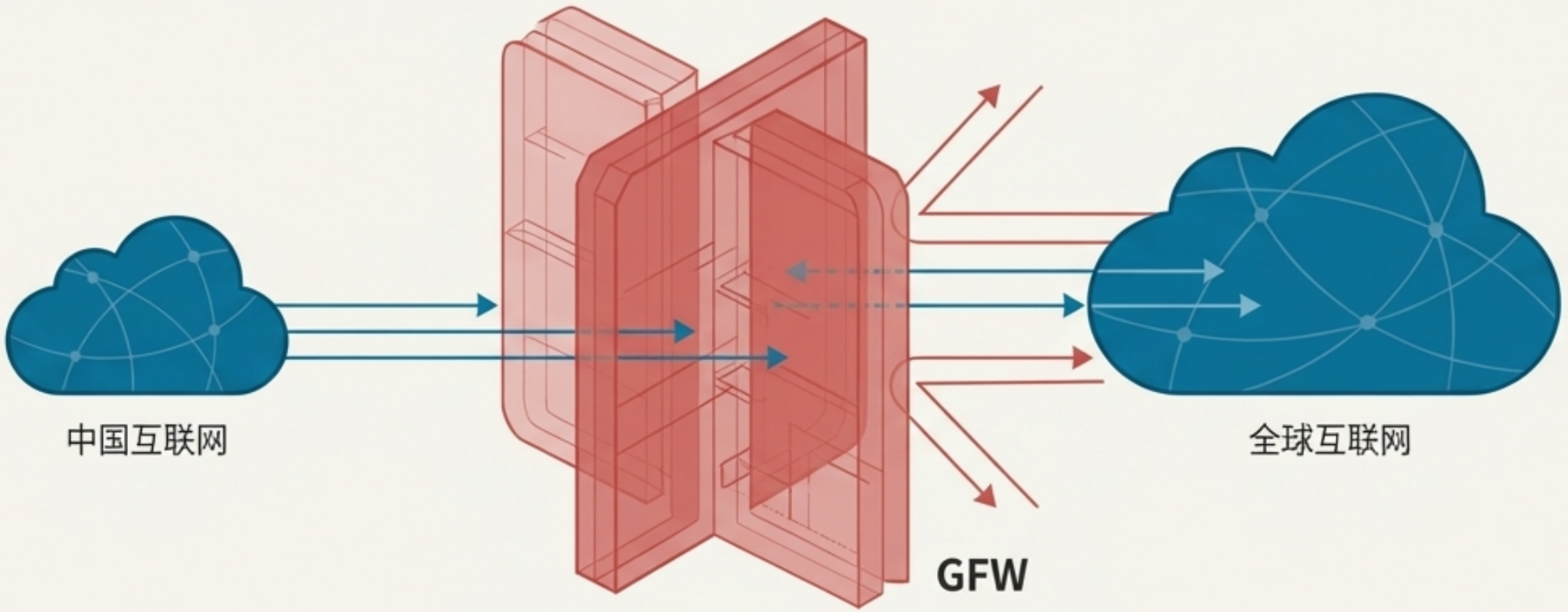


NotebookLM

“墙”：不止是防火墙



核心定义：一个由多个复杂子系统构成的庞大网络监控体系。

核心目标：监控、过滤并限制对特定境外内容的访问，维护国家网络主权。

早期：简单关键词过滤

基于预设黑名单的基础文本匹配

中期：DNS 污染与 IP 封锁

操纵域名解析，直接阻断特定IP访问

后期：深度包检测（DPI）

深入分析数据包内容，实现应用层级的精准识别与阻断

现状：机器学习与主动探测

利用AI识别未知协议与流量，主动探测VPN/代理服务器

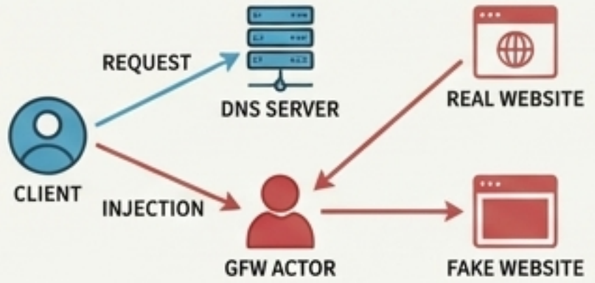
NotebookLM

墙的基石：三种关键封锁技术



DNS 污染

抢在真实的DNS服务器前回应，返回一个虚假的IP地址，让你“走错门”。





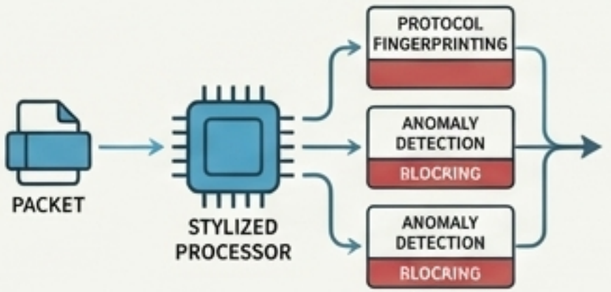
IP 封锁 / TCP 重置

直接在骨干路由器上丢弃数据包，或伪造TCP RST包强制切断连接。

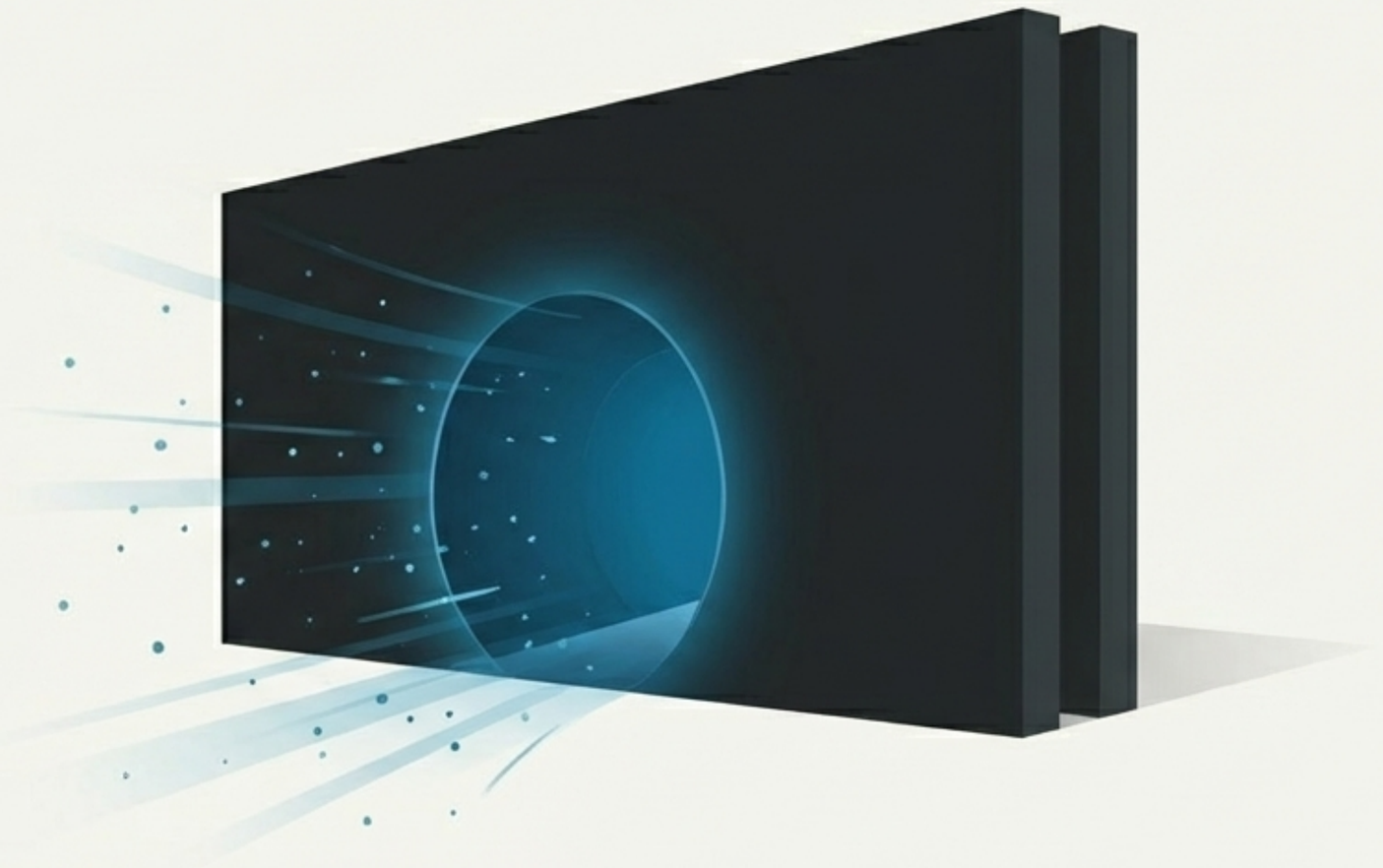


深度包检测（DPI）

深入分析数据包载荷，识别协议指纹与流量统计特征，实现精准打击。



NotebookLM



破壁之道：加密、伪装与中转

NotebookLM

万变不离其宗：正向代理模型



加密（Encryption）：

建立加密通道，让 GFW 看不懂内容。

伪装（Obfuscation）：

将原始请求封装在合法协议中，让 GFW 看不出你在翻墙。

本质：翻墙的本质是一种正向代理行为，通过加密和伪装手段，使 GFW 无法识别流量的真实意图和目标。

NotebookLM

第一回合：从 Shadowsocks 到 Trojan



Shadowsocks (SS)

- **策略：**抛弃传统VPN的复杂握手，采用简洁的对称加密，追求效率。
- **弱点：**原生协议特征明显，易被DPI通过流量统计分析识别。
- **比喻：**穿着“隐身衣”的人



V2Ray / Trojan

- **策略：**V2Ray将流量隐藏在WebSocket等常见Web协议中；Trojan则完全模仿HTTPS流量。
- **优势：**流量与访问普通加密网站的流量几乎完全一致，完美避开特征检测。
- **比喻：**伪装成普通人的特工

NotebookLM

新世代对决：Reality 与 Hysteria 2



Reality（极致隐蔽）

策略：“借用”合法大厂网站的TLS证书和握手特征，彻底消除服务端指纹。

目标：根除一切可识别特征，完美对抗 GFW 的主动探测。



Hysteria 2（极限加速）

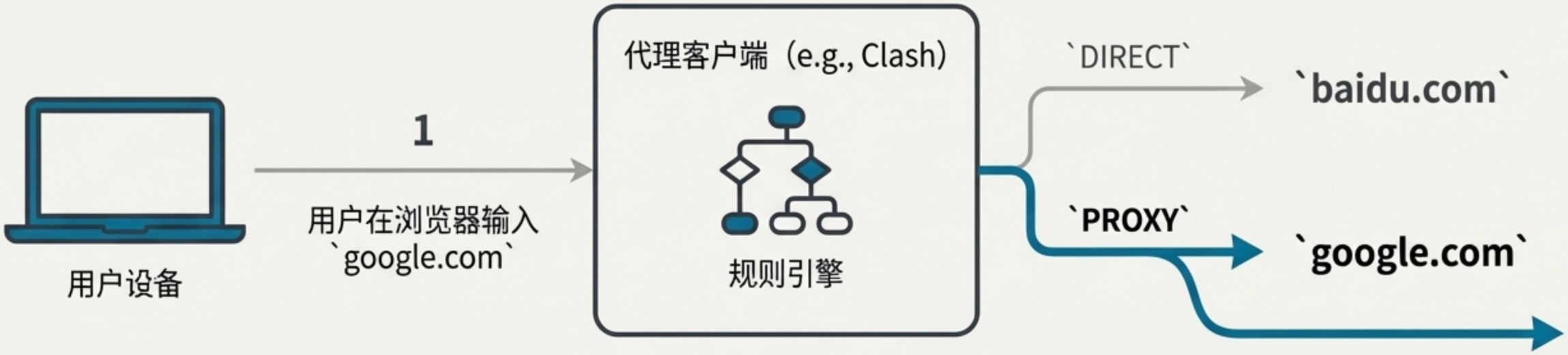
策略：基于 UDP 的 QUIC 协议，采用定制化拥塞控制算法，暴力优化弱网环境。

目标：在高丢包、高延迟的恶劣线路下实现吞吐量最大化。

NotebookLM

一次请求的完整旅程（上）：本地决策

STAGE_01: INITIATION

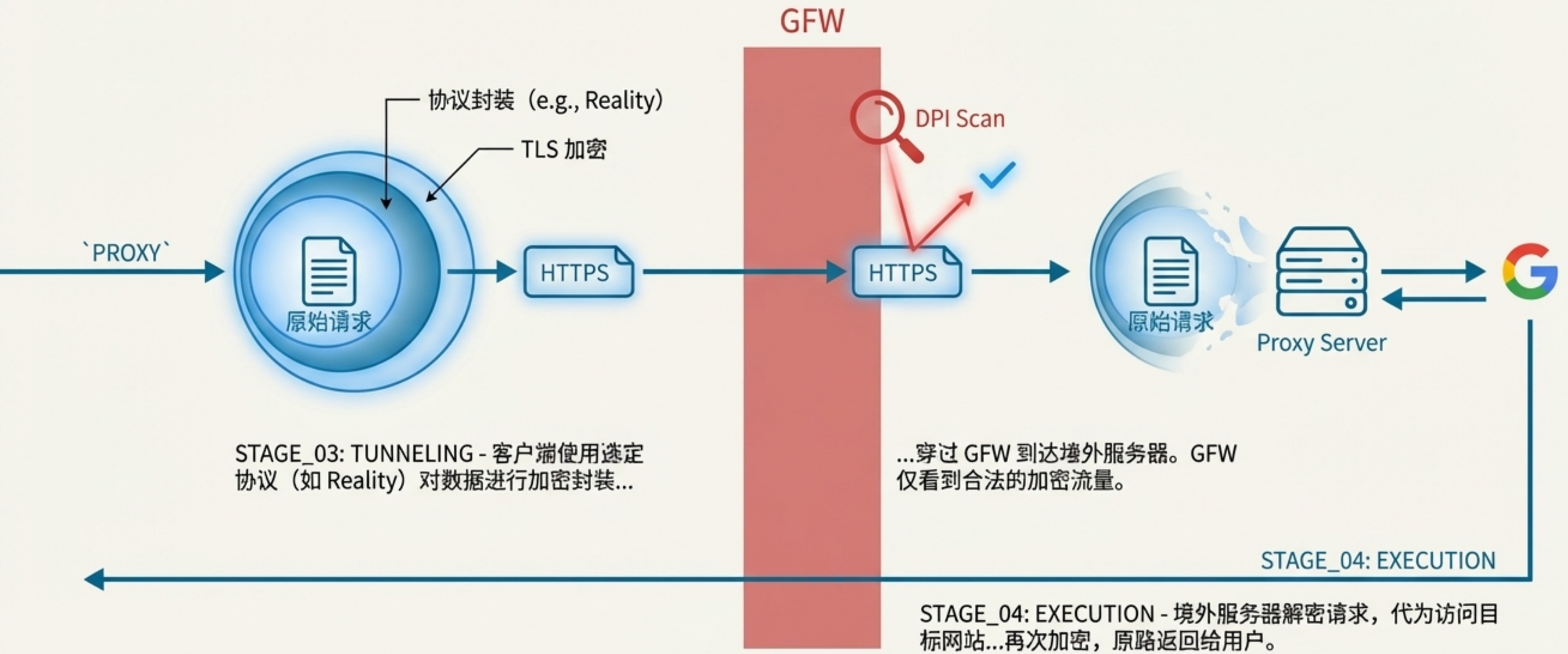


STAGE_02: ROUTING

客户端根据预设规则（域名、IP、GeoIP）判断该请求去向。

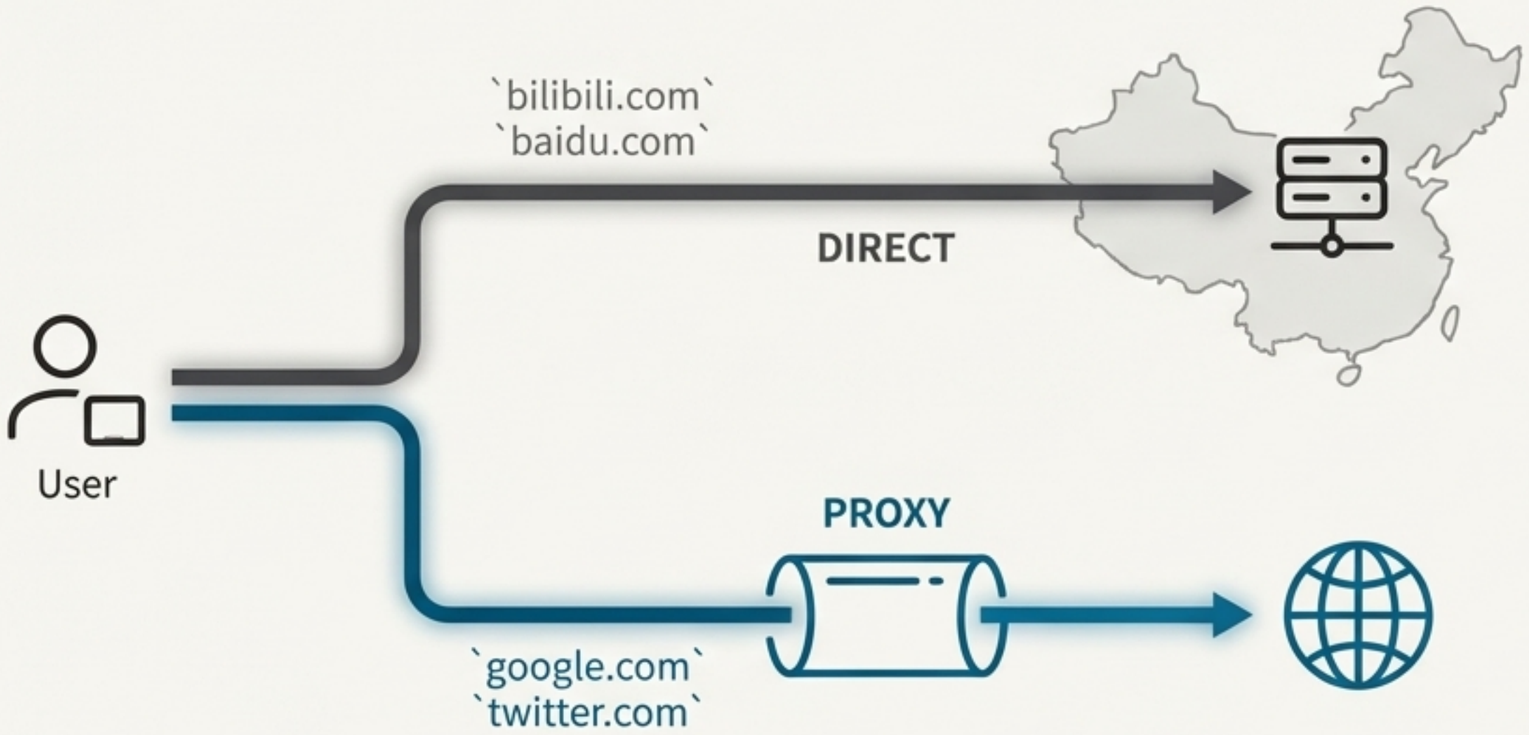
NotebookLM

一次请求的完整旅程（下）：加密穿墙



NotebookLM

规则分流：聪明的网络管家




```
DOMAIN-SUFFIX, google.com -> PROXY
DOMAIN-KEYWORD, baidu -> DIRECT
GEOIP, CN -> DIRECT
MATCH -> PROXY
```

根据域名、IP、地理位置等预设规则，自动决定流量是“直连”、“代理”还是“拦截”，实现内外网访问的无缝切换。

NotebookLM

如何选择？主流协议特性一览

协议（Protocol）	伪装能力（Stealth）	性能表现（Performance）	适用场景（Use Case）
Shadowsocks	较低 	极高 	个人私有节点
VMess/VLESS	中等 	高 	综合性代理环境
Trojan	极高 	中等 	追求稳定性的用户
Reality	顶尖 	高 	对抗深度检测（DPI）
Hysteria 2	中等 	极高（弱网强） 	跨境线路质量差时

NotebookLM

信任，但要验证：安全与隐私风险



警惕免费服务

可能记录用户访问日志、窃取敏感数据，甚至实施中间人攻击（MITM）。



拥抱开源社区

优先选择经过社区审计的协议与客户端（如 Reality, Hysteria）。



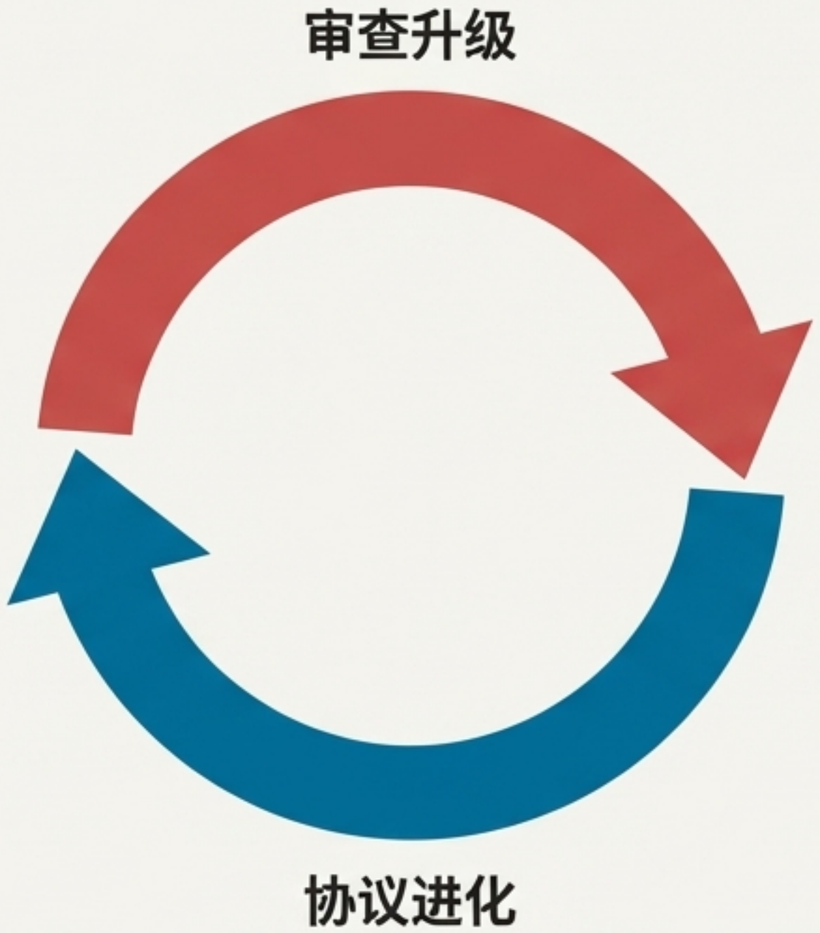
理解法律边界

了解并遵守相关法律法规，用于学习、科研等正当需求。

NotebookLM

永不落幕的博弈

回顾：审查与反审查是一场持续的技术演进，一场长期的“猫鼠游戏”。



未来：对抗将更加依赖机器学习与行为分析，技术也将更加智能化。

基石：加密和伪装是破壁技术的永恒基石。

NotebookLM