

GFW的原理和绕过

——IDS攻防战

GFW是什么？为什么要翻墙？

其中哪些和GFW有关。

- 某某公司的服务器去维修了？
- 全国断网10分钟？
- 有人被政府起诉诽谤罪了？
- 打开facebook时访问超时？
- 打开google.cn时链接被重置？
- 浏览器经常弹出广告？
- 全球twitter无法访问？
- 很多网页打不开？

为什么要翻墙？

- 为了和宇宙人沟通。
- 需要的资料找不到。
- 谷歌粉丝，讨厌百度。
- 好友都在国外，他们让我上facebook。
- 求糟糕物。
- 闲的蛋疼。

GFW的组成

GFW的来历

- 方大师
- Cisco
- IDS

GFW的原理

- 镜像端口转发数据
- IDS集群旁路解析
- 危险连接RST包中断

GFW的位置

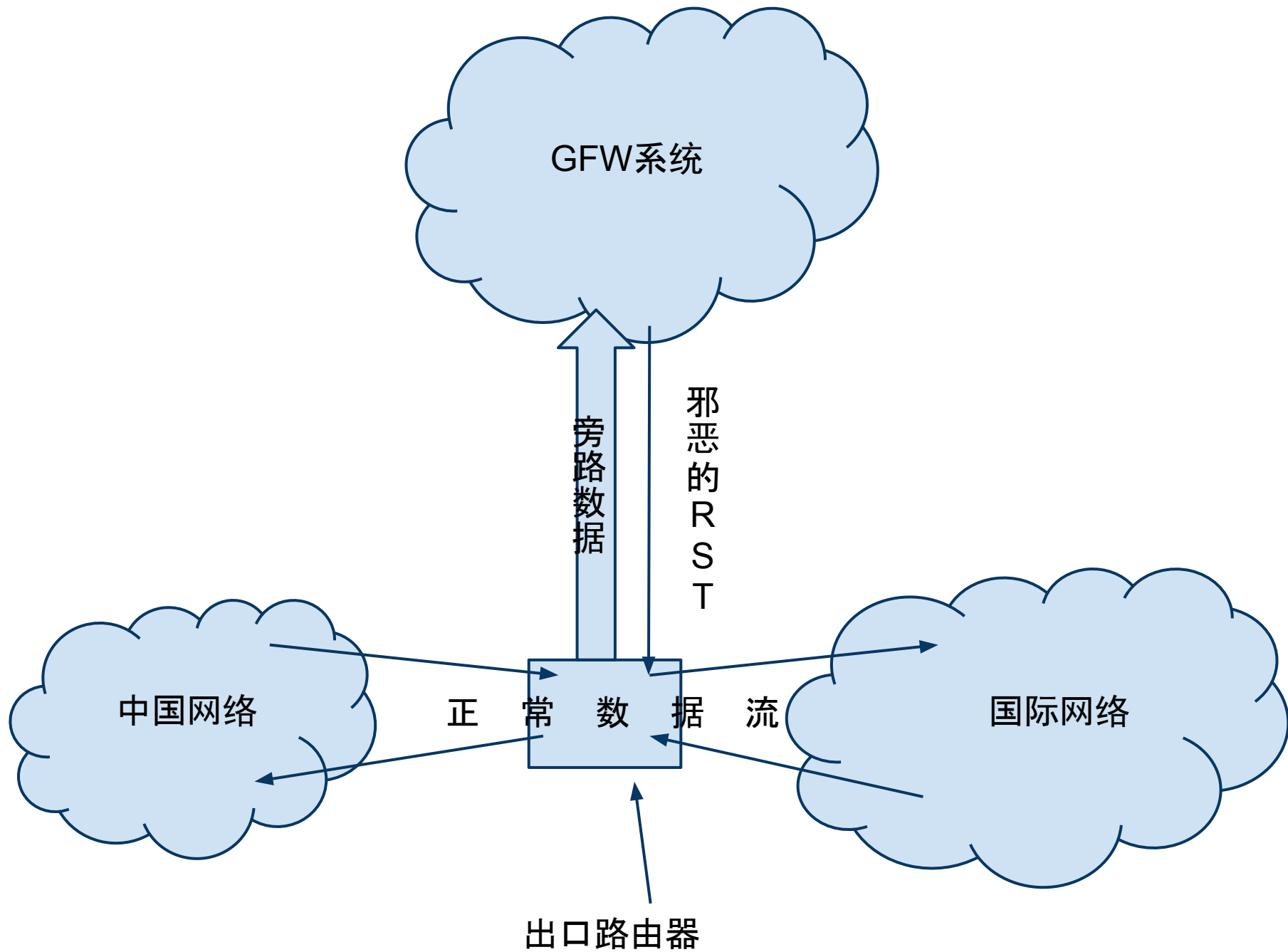
- 中国各大网络出口
- 多数集中在北京, 上海, 广州等城市

GFW的优点

- 成本低, 效果好
- 扩充性好, 运行稳定。

GFW缺点

- 判断智能程度不足, 有漏判
- 目前不支持IPv6



GFW封锁方式一览

- DNS污染
- DNS劫持
- IP路由劫持
- 深度包检测
- (传闻)热点分析
- (传闻)伪造证书
- (传闻)机房白名单制

DNS污染/劫持和IP劫持的解决方案

DNS污染：

- 使用OpenDNS
- 8.8.8.8

DNS劫持：

- 使用/etc/hosts文件
- 直接指定IP地址访问
- 本地DNS缓存

IP路由劫持的解决方案：

- 非加密代理
- twitter API
- 加密网址的代理服务器

以上几个的结合：

如果特定网站没有被列为深度包检测关键字，考虑使用IP地址+非加密代理来访问。

- 速度快
- 代理资源丰富
- 不易被封锁

深度包检测的主流规避方法

加密代理法

- TOR
- ssh -D
- gappproxy
- Psiphon
- 无界
- 自由门
-

变更协议

- UDP
- IPv6
- SDPY(不成熟)

VPN法

- PPTP
- L2TP
- OpenVPN

网络证书原理浅析

证书：

包含了属主信息(网址, Email地址, 公司名称)和公钥的信息集合, 称为证书。

验证：

当访问某个网站时, 某个受信证书上的域名和网站域名一致, 并且使用SSL握手通讯成功。

签署：

客户端持有受信机构A的公钥, A以自身私钥加密关于B的数据。客户端可以解密验证内容, 攻击者无法伪造。以上成为签署。

证书链：

浏览器和系统内置了一些信任证书, 这些验证机构代我们验证其他公司或个人。如果其可信的, 则签署被验证者的证书, 使得浏览器也信任被验证者的证书。

如何挫败嗅探攻击：

由于双方使用证书完成SSL握手, 因此总可以构造嗅探者无法破译的通讯。例如用自己的私钥加密, 用对方的公钥解密。

如何挫败man in middle：

如果man in middle使用原始的证书, 那么浏览器会警告域名和访问目标不符。如果替换证书, 则证书不受信。

防御假证书

借助假证书可以发起的攻击：

- man in middle
- Untrust plugins

假证书的范围：

- Entrust
- CNNIC

CNNIC说：

中国互联网络信息中心(**CNNIC**)是成立于1997年6月3日的非盈利管理与服务机构，行使国家互联网络信息中心的职责。

中央编委说：

不知道**CNNIC**是什么组织，但它肯定不是事业单位。第一，它不符合《中华人民共和国国务院令1998年252号事业单位登记管理暂行条例》所规定的登记条件；第二，它从来也没有向中央编委提出过登记申请。

工商部门说：

不知道**CNNIC**是什么组织，但肯定不是企业。它开不出发票，如果它开了发票，那肯定是在非法无照经营。

民政部门说：

不知道**CNNIC**是什么组织，但肯定不是社团。

调戏GFW

GFW的弱点：

- 依赖于HTTP协议 (RFC2616)。
- 依赖于TCP协议，以及双方对RST包的响应。
- 为了减低负荷，没有追踪TCP SEQ。

调戏GFW的方法：

- 构造畸形HTTP代理请求头。
- 传输双方忽略RST包(西厢计划第二季)。
- 伪造TCP SEQ错误的包欺骗GFW(西厢计划第一季)。

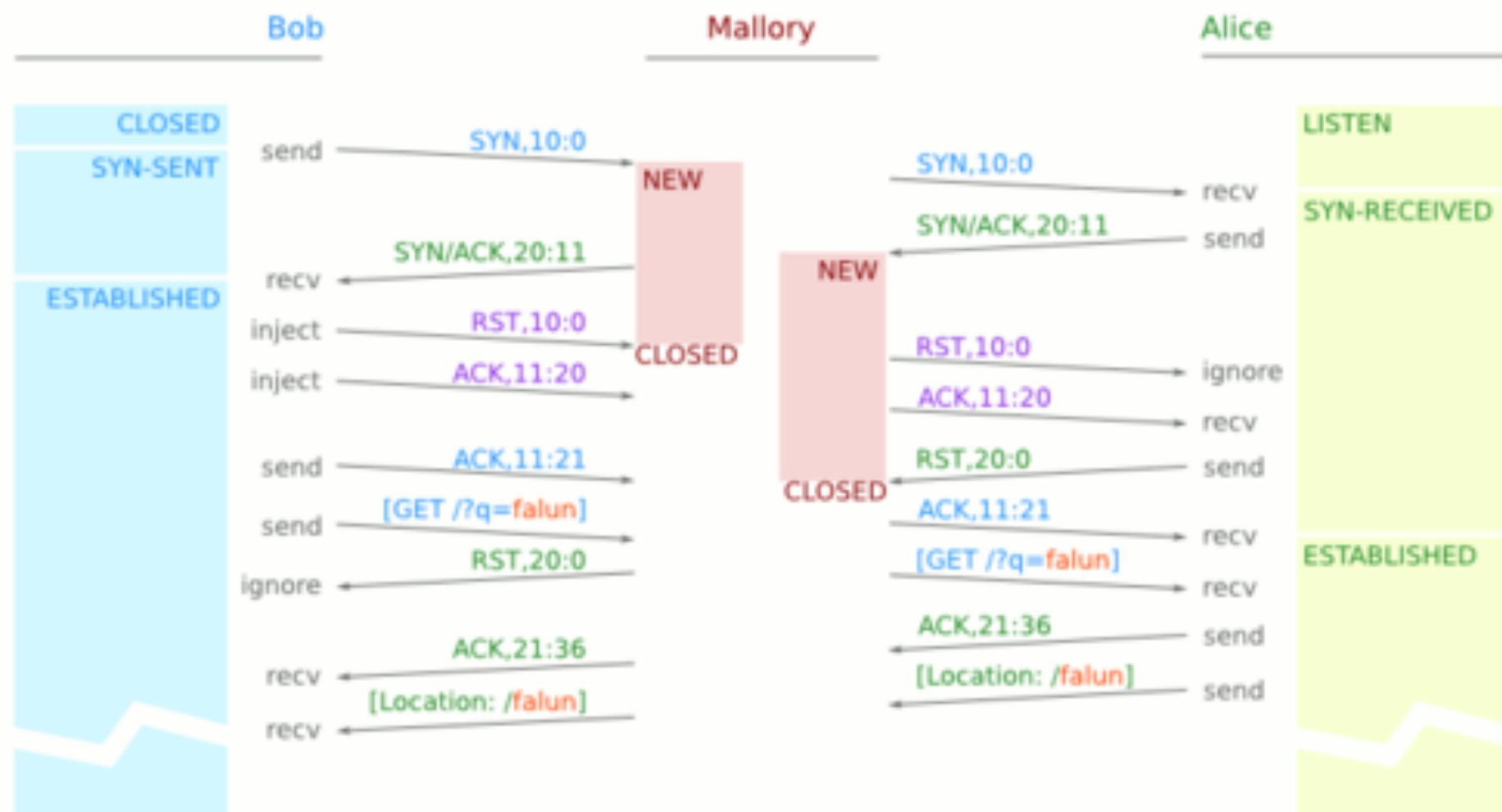
西厢计划第一季

通过构造一个TCP SEQ错误的RST包，欺骗GFW。由于SEQ错误，目标机器忽略此包。而GFW由于没有记录SEQ，导致被骗。认为该TCP连接已经死亡，从而忽略以下所有报文。

优点：TCP连接直走。不需要墙外服务器的支持。速度快，和直接上网几乎无区别。

缺点：GFW很容易修改为不忽略被RST连接的以下报文。该方法需要修改底层的协议栈，因此跨平台特性很差，对客户要求很高。即使花费数倍的代价，此问题总能被修复（最坏情况，修复协议栈）。

张某工作原理示意图



[payload]

tcp-flags,seq:ack



西厢计划第二季

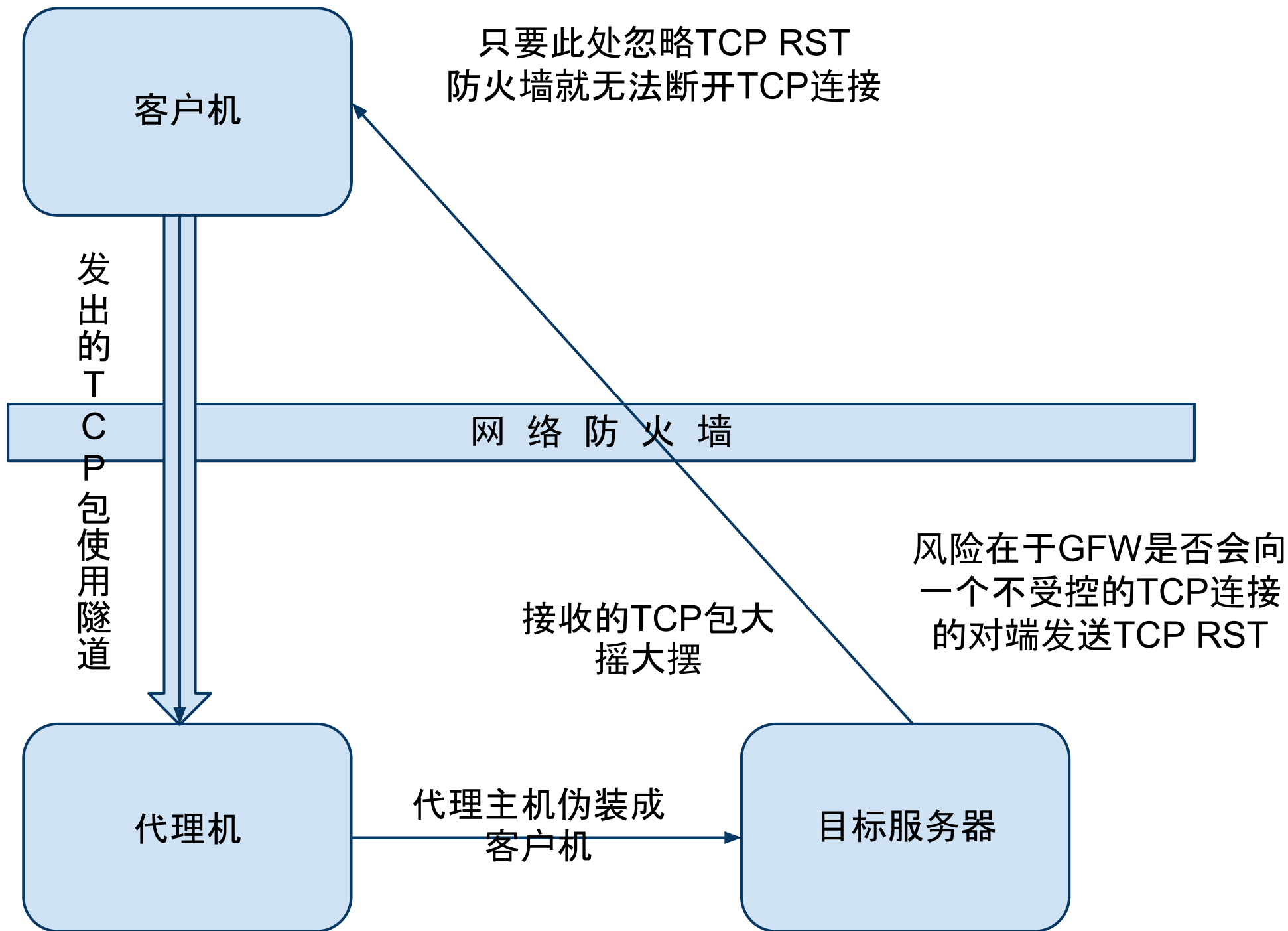
设法忽略RST包。

将一条连接分为出包和入包。对入包全面忽略RST，对出包封装在隧道内发送往墙外的服务器。由远程服务器伪装为本地IP包进行模拟。

由于HTTP协议通常发送数据少而接收数据多，因此一台墙外的转发服务器可以支持相当数量的客户端。

缺陷：需要墙外服务器做转发。如果服务器所在的路由器禁止IP伪装则无法成功。

优点：通常的IDS方案无法阻截。除非将旁路式IDS转为插入式IDS。



组合翻墙系统

规则转发系统：

- **squid**
- **tinyproxy**
- **3proxy**
- **fireproxy**
- **PAC**

规则转发的目的在于分离需要穿墙的和不需要穿墙访问。

(可选)HTTP2SOCK转换：

- **polipo**
- **privoxy**

转换的目的在于换用协议，并且提供其他辅助特性。

(可选)负载均衡系统：

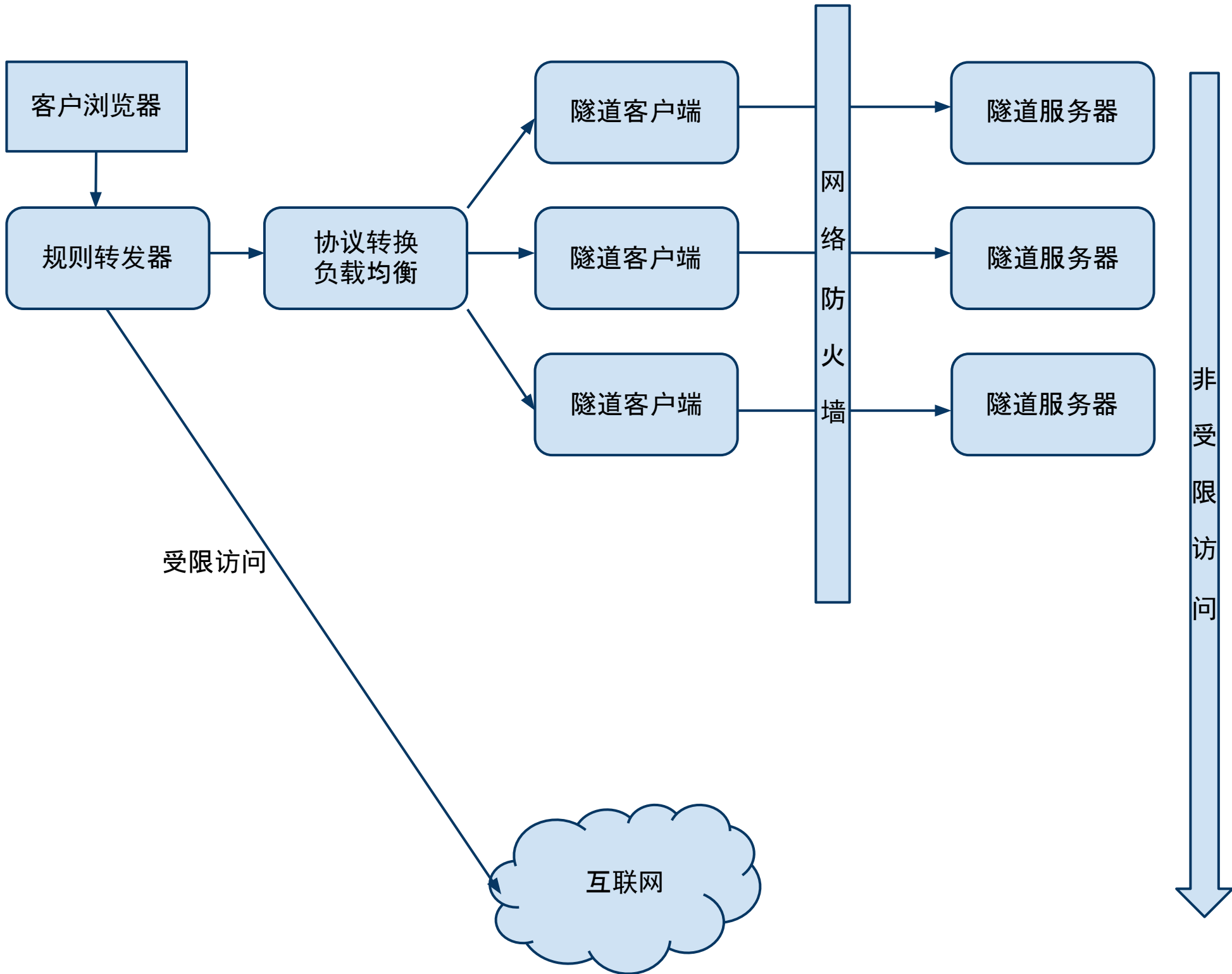
- **haproxy**
- **proxychains**

负载均衡系统将压力调度到多个代理上。

翻墙代理(SOCK5)：

- **Tor**
- **ssh -D**
-

以上方案可以并行，只要支持SOCK5代理协议。



准完美方案：VPN+嵌入设备

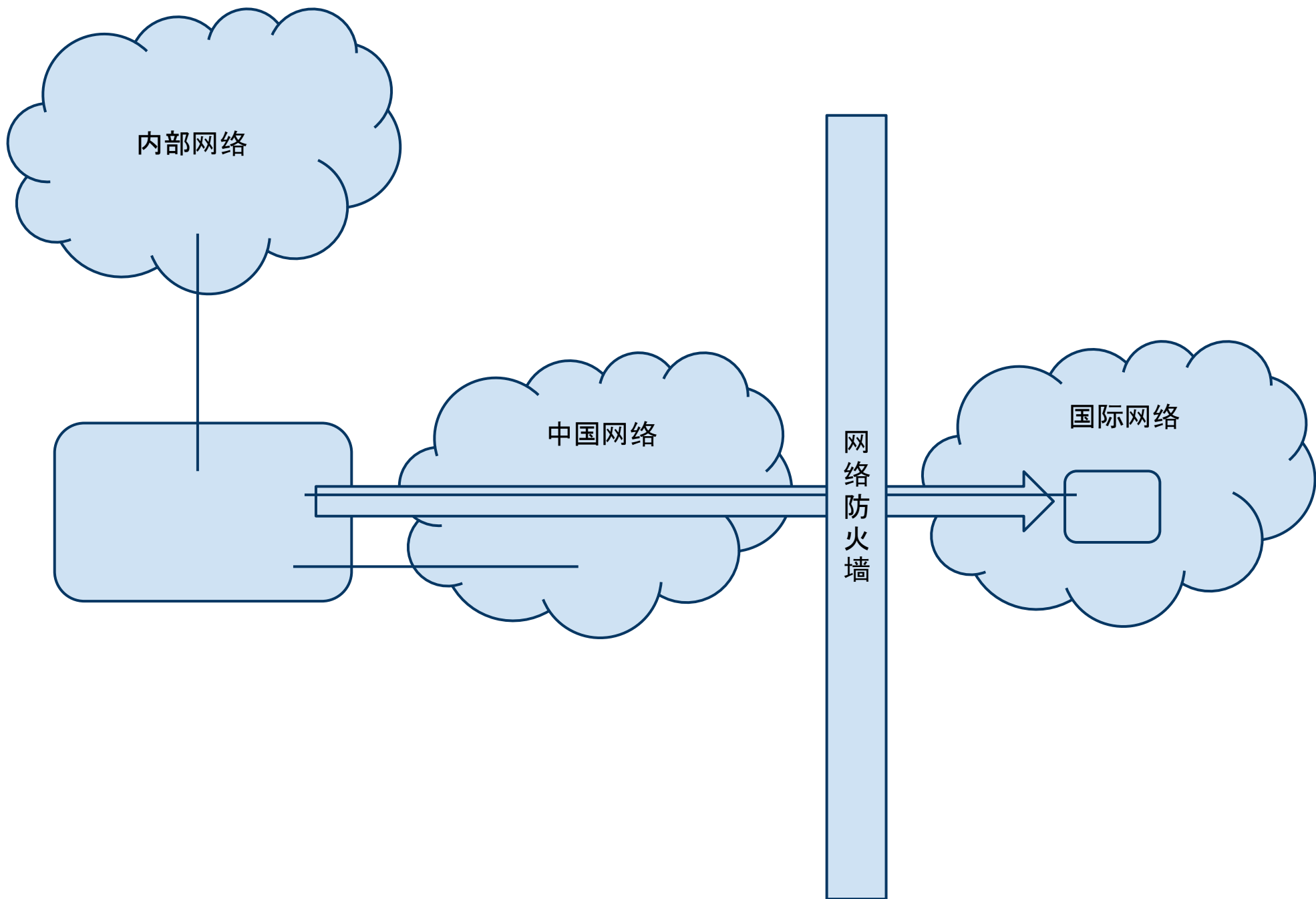
使用一个VPN，加一个支持路由器。通过iptables的路由规则，将需要访问国外内容的数据从VPN内穿出去。

优势：

相当于物理解决，系统稳定可靠。

缺点：

- 需要IP路由数据，并且跟随他的变化。
- 需要额外的路由器设备。
- 需要VPN。
- 由于人工干涉路由，可能造成和其他服务的冲突。



最完美方案

肉身翻墙

卖一套北京上海的房子，投资移民。

优点：终身受益

缺点：你需要一套房子

审查趋势的发展和展望：墙内

- 白名单备案，绑定域名和IP到责任人
- 层层责任制度
- 审查/自我审查
- 五毛技术
- 客户端审查技术
- “儿童黑话”类语言
- 笑孬婊昆
- 隐写术:jpg+rar
- 信息洪水
- 使用Linux

审查趋势的发展和展望：墙外

- IPv6支持, 扩充可控协议
- 增强语义分析技术
- 非受控TCP链接断开
- 工具/方案倒钩, 收集流行方法并屏蔽
- 白名单备案, 绑定域名和IP到责任人
- 全面断网
- 尽量不要将翻墙细节透露给不熟悉的人
- 隐写术
- 加密技术
- 协议混淆
- 小语种
- 社会工程
- 自建通讯系统

*Freedom consists not in doing
what we like, but in having the
right to do what we ought.*

— Pope John Paul II

Thank you all