为什么要翻墙？

前言：

时间进入 2019 年，国内经济下行严重，社会深层次问题的表象化加剧，种种矛盾经过近年的各种维权和抗议活动体现了出来，贸易战进入相持和妥协阶段，短期内中国的舆论环境因习近平 2018 年废除国家主席任期限制和个人崇拜的造神运动急剧下滑，网络封锁和舆论控制将会更加严重，翻墙的技术手段在不断的博弈中又有了一些新的变化。

（国内政治斗争现状及发展请参考：台湾大学政治学系明居正芝加哥演讲视频 https://www.youtube.com/watch?v=lhVDv3HWfm8，需要翻墙才能打开该地址）

由于 2018 年国家对境外网站的大批封锁和 VPN 的强制下架，翻墙的机会也越来越少，中国网民能够深刻体验到上网的不便，想看看外面的世界也更是难上加难，2017 年 1 月 22 日，中国工信部发布通知，自即日起至 2018 年 3 月 31 日，"在全国范围内对互联网网络接入服务市场开展清理规范工作，将依法查处互联网数据中心(IDC)业务、互联网接入服务(ISP)业务和内容分发网络(CDN)业务市场存在的无证经营、超范围经营、层层转租等违法行为"。2019 年开年达沃斯论坛上国际著名金融大鳄乔治.索罗斯发表演讲，点名指责习近平是开放社会的共同敌人。2018 年 9 月，广电总局在网上也发布征求意见稿，严格限制境外新闻节目以个人或企业名义搬运进国内互联网的视频平台。可见将来墙内网民自由上网的情况将持续恶化。

2018 年 12 月 12 日，迅雷以推出支持 IPv6 版本的更新，国家防火墙对于 IPv6 地址的部署已经全面竣工，就算是使用 YouTube 翻墙，但由于 YouTube 的播放视频地址以及 Google Photos 的视频地址内容来源***.googlevideo.com 为随机地址，因此仅靠 host 文件无法解决，需要采用无污染的 DNS 服务器才行。在这里收集并汇总了目前仍然可用的一些免费翻墙方法和翻墙工具，数起来大大小小各有 30 多种，很多都取自 Google十、Facebook、telegram 群分享、维基百科以及 GitHub、一些博客等网站的分享。

一、什么是墙/防火墙

防火长城（英语：Great Firewall (of China)，常用简称：GFW，中文也称中国国家防火墙，中国大陆民众俗称墙、防火墙、功夫网等等），是对中华人民共和国政府在其互联网边界审查系统（包括相关行政审查系统）的统称。此系统起步于 1998 年，其英文名称得自于 2002 年 5 月 17 日 Charles R. Smith 所写的一篇关于中国网络审查的文章《The Great Firewall of China》，取与 Great Wall（长城）相谐的效果，简写为 Great Firewall，缩写 GFW。

随着使用的拓广，中文“墙”和英文“GFW”有时也被用作动词，网友所说的“被墙”即指网站内容被防火长城所屏蔽或者指服务器的通讯被封阻，“翻墙”也被引申为突破网络审查浏览境内外被屏蔽的网站或使用服务（如被 GFW 屏蔽的网盘 Dropbox）的行为。

防火墙的工作原理分以下几种（来自维基）：

1.域名解析服务缓存污染

原理：防火长城对所有经过骨干出口路由的在 UDP 的 53 端口上的域名查询进行 IDS 入侵检测，一经发现与黑名单关键词相匹配的域名查询请求，防火长城会马上伪装成目标域名的解析服务器给查询者返回虚假结果。由于通常的域名查询没有任何认证机制，而且域名查询通常基于的 UDP 协议是无连接不可靠的协议，查询者只能接受最先到达的格式正确结果，并丢弃之后的结果。用户若改用 TCP 在 53 端口上进行 DNS 查询，虽然不会被防火长城污染，但可能会遭遇连接重置，导致无法获得目标网站的 IP 地址。

2.针对境外的 IP 地址封锁

原理：相比起之前使用的访问控制列表（ACL）技术，现在防火长城采用了效率更高的路由扩散技术封锁特定 IP 地址。正常的情况下，静态路由是由管理员根据网络拓扑或是基于其它目的而给出的一条路由，所以这条路由最起码是要正确的，这样可以引导路由器把数据包转发到正确的目的地。而防火长城的路由扩散技术中使用的静态路由其实是一条错误的路由，而且是有意配置错误的，其目的就是为了把本来是发往某个 IP 地址的数据包统统引导到一个“黑洞服务器”上，而不是把它们转发到正确目的地。

这个黑洞服务器上可以什么也不做，这样数据包就被无声无息地丢掉了。更多地，可以在服务器上对这些数据包进行分析和统计，获取更多的信息，甚至可以做一个虚假的回应。这些错误静态路由信息会把相应的 IP 数据包引导到黑洞服务器上，通过动态路由协议的路由重分发功能，这

些错误的路由信息可以发布到整个网络。这样对于路由器来讲现在只是在根据这条路由条目做一个常规数据包转发动作,无需再进行ACL匹配,与以前的老方法相比，大大提高了数据包的转发效率。

一般情况下,防火长城对于中国大陆境外的“非法”网站会采取独立 IP 封锁技术，然而部分“非法”网站使用的是由虚拟主机服务提供商提供的多域名、单（同）IP 的主机托管服务，这就会造成了封禁某个 IP 地址，就会造成所有使用该服务提供商服务的其他使用相同 IP 地址服务器的网站用户一同遭殃，就算是“内容健康、政治无关”的网站，也不能幸免。其中的内容可能并无不当之处,但也不能在中国大陆正常访问。

3.IP 地址特定端口封锁

原理：防火长城配合上文中特定 IP 地址封锁里路由扩散技术封锁的方法进一步精确到端口，从而使发往特定 IP 地址上特定端口的数据包全部被丢弃而达到封锁目的，使该 IP 地址上服务器的部分功能无法在中国大陆境内正常使用。

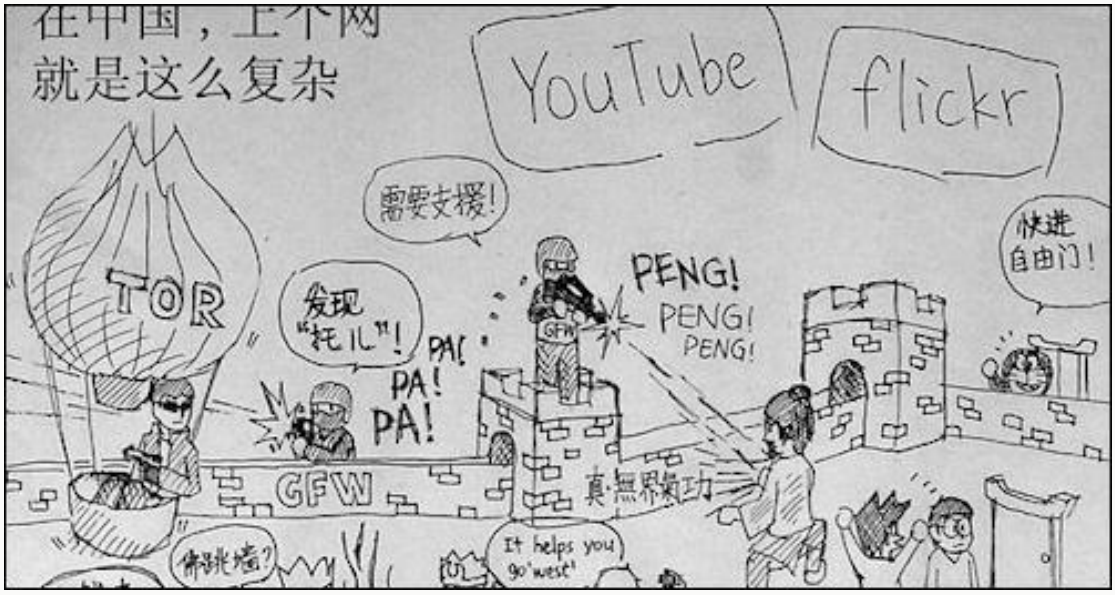
4.无状态 TCP 连接重置

原理：防火长城会监控特定 IP 地址的所有数据包，若发现匹配的黑名单动作（例如 TLS 加密连接的握手），其会直接在 TCP 连接握手的第二步即 SYN-ACK 之后伪装成对方向连接两端的计算机发送 RST 数据包（RESET）重置连接，使用户无法正常连接至服务器。这种方法和特定 IP 地址端口封锁时直接丢弃数据包不一样，因为是直接切断双方连接因此封锁成本很低,故对于 Google 的多项(强制)加密服务例如 Google

文档、Google 网上论坛、Google+和 Google 个人资料等的 TLS 加密连接都是采取这种方法予以封锁。

5.对加密连接的干扰

在连接握手时，因为身份认证证书信息（即服务器的公钥）是明文传输的，防火长城会阻断特定证书的加密连接，方法和无状态 TCP 连接重置一样，都是先发现匹配的黑名单证书，之后通过伪装成对方向连接两端的计算机发送 RST 数据包（RESET）干扰两者间正常的 TCP 连接，进而打断与特定 IP 地址之间的 TLS 加密连接（HTTPS 的 443 端口）握手，或者干脆直接将握手的数据包丢弃导致握手失败,从而导致TLS连接失败。但由于 TLS 加密技术本身的特点，这并不意味着与网站传输的内容可被破译。



Tor 项目的研究人员则发现防火长城会对各种基于 TLS 加密技术的连接进行刺探，刺探的类型有两种：“垃圾二进制探针”，即用随机的二进制数据刺探加密连接，任何从中国大陆境内访问境外的 443 端口的连接都会在几乎实时的情况下被刺探，目的是在用户创建加密连接前嗅探出

他们可能所使用的反审查工具，暗示近线路速率深度包检测技术让防火长城具备了过滤端口的能力。针对 Tor，当中国的一个 Tor 客户端与境外的网桥中继创建连接时，探针会以 15 分钟周期尝试与 Tor 进行 SSL 协商和重协商，但目的不是创建 TCP 连接。

切断 OpenVPN 的连接，防火长城会针对 OpenVPN 服务器回送证书完成握手创建有效加密连接时干扰连接，在使用 TCP 协议模式时握手会被连接重置，而使用 UDP 协议时含有服务器认证证书的数据包会被故意丢弃，使 OpenVPN 无法创建有效加密连接而连接失败。

6.TCP 关键字阻断

Firefox 的“连接被重置”错误消息。当碰触到 GFW 设置的关键词后(如使用 Google 等境外搜索引擎)，即可能马上出现这种画面。TCP 重置是 TCP 的一种消息，用于重置连接。一般来说，例如服务器端在没有客户端请求的端口或者其它连接信息不符时，系统的 TCP 协议栈就会给客户端回复一个 RESET 通知消息，可见 RESET 功能本来用于应对例如服务器意外重启等情况。防火长城切断 TCP 连接的技术实际上就是发送连接重置消息。

对于防火长城而言，发送连接重置数据包比直接将数据包丢弃要好，因为如果是直接丢弃数据包的话客户端并不知道具体网络状况，基于 TCP 协议的重发和超时机制，客户端就会不停地等待和重发，加重防火长城审查的负担，但当客户端收到 RESET 消息时就可以知道网络被断开不会再等待了。而实际上防火长城通过将 TCP 连接时服务器发回的 SYN/ACK 数据包中服务器向用户发送的序列号改为 0 从而使客户端受骗认为服

务器重置了连接而主动放弃向服务器发送请求，故这种封锁方式不会耗费太多防火长城的资源而效果很好，成本也相当的低。

以上是几种主要的手段，其他具体可参考维基百科的介绍：防火长城

二、为什么翻墙？

翻墙早已成为社会主义特色的一部分，不知道儿孙们以后看到我们现在的状态会做何感想，可能会像我们现在不能体会那些莫名其妙的明清文字狱一样。可能吧做过一期中国翻墙网民状况调查。对于为什么要翻墙，可能吧的总结是：

80%的人翻墙仅仅是为了“正常”地使用 Google 等互联网基础服务，他们或许只是想正常地搜索“胡萝卜”。75%的人翻墙会上 Twitter 等社交网站，72%的人会看外媒的新闻。60%的人翻墙是为了娱乐，比如观看 Youtube。因为国内的互联网产品行业相对落后，而优秀的外国互联网产品往往又是被屏蔽，很多人翻墙是为了学习外国的互联网产品，这个比例占了 52%。30%的人翻墙会上成人网站。另外有 26%的人工作必须翻墙。

我们来看一下 GFW 的三大定律：

GFW 第一定律：只要是 “用户产生内容”(User-generated content, UGC)的国外网站都会被和谐。

GFW 第二定律：只要是被和谐的网站，国内一定会有个克隆版。

GFW 第三定律：没有被和谐的网站一定不是同类竞争者中最出色的。

举几个具体例子好了。

GFW 第一定律中“用户产生内容”的意思即用户可以在网站上发布视频、图片、评论等，或者更新自己的内容、而往往这样的发布是面向大量受众，即影响面很大，往往这样的影响不受中国政府控制，比如在 YouTube 上上传涉及政治敏感的视频，发表涉及中国政府的言论，这正是防火墙的作用，即不让我们在上面发表评论或者不希望我们看到这样的评论，因为推特和 Facebook 的言论自由的特点，因此在这些平台上也有许多攻击中国政府的言论。

GFW 第二定律就不必多说了，像我们平常使用的优酷、新浪微博、qq 空间，其实就是从国外的 YouTube、推特、Facebook 那里借鉴来的，不过这些借鉴版本都要配合中国政府的审查制度。

GFW 第三定律，意思是往往那些鲜为人知的国外网站，在中国影响力不大，不会引起什么风波，因此封杀什么的就觉得没有多大必要。

对于翻墙，就我身边的人知道的不多，就我而言经常翻墙也不多。对于原因，鄙人总结如下：

翻墙的动力对于绝大多数人，对于大部分的中国网民，那些 Google 的基础服务，Twitter，Youtube，在国内已经有了山寨的产品出现，他们可以上百度，新浪微博，优酷。在不翻墙的情况下就能满足消费者的需求，奈何还要麻烦翻墙呢。这就造成了翻墙的需求性不高，动力不足。

翻墙的阻碍优秀的互联网服务集中在美国，这些服务的主要语言是英语，操作习惯也是非 China 的。虽然大部分这些网站提供了中文界面，但前期的简单设置还是不可少的，很多人以为国外的网站只有英文怕搞不懂，其实这也是信息封锁下从来没有接触过的误区。

翻墙的体验翻墙毕竟是要经过第三方，一般的翻墙方法速度上比正常要慢，稳定性也不好。翻墙合法性我们已经适应了墙内的其乐融融，一片大好的环境，突然接触到对 Party 不好的评论，都会认为是非法的东西，对合法性的怀疑会造成在浏览的过程中提心吊胆不能畅快淋漓。

翻墙的难度现在的翻墙方法中，简单的不稳定，稳定的不简单。比如自由门和在线代理，几乎不用设置，可过段时间就会发现不能用了。稳定的 Tor、SSH、VPN 在设置上又相对复杂。

*可是为什么会有翻墙？*翻墙的价值为了工作，为了学习，为了感受生活，为了看到墙内没有的东西，为了了解真相，为了知道这个世界究竟是什么样的，为了自己不是一直傻傻地走过这一遭，为了不被儿孙们耻笑…

本段文字摘自这里(需要翻墙)

对于有技术恐惧的同学我想说的是，那些没有走出山洞的人类最终没有机会发现新世界，翻墙是一道天然的门槛，它过滤掉了那些好奇心不强，安于现状和缺乏质疑能力的人。最终世界是属于那些像航海家一样敢于在未知大海不断航行发现新大陆的人。天朝的防火墙和大清的闭关锁国政策是一样的，外媒评价说，21 世纪还在屏蔽互联网的中国，是一个自废武功的国家。

如果你的身边有想看看外面的世界和听到不同声音的朋友，请将本文档转发给他，也许会改变他的人生。

翻墙教程及软件下载地址：

https://github.com/zmike1993/hello-world/tree/hello-world-pdf