为什么你无法访问谷歌

GFW的资料整理

nameless

2024年3月15日

当你在浏览器键入 https://www.google.com/ 时，往往会看到这样的画面（如图1.1）。

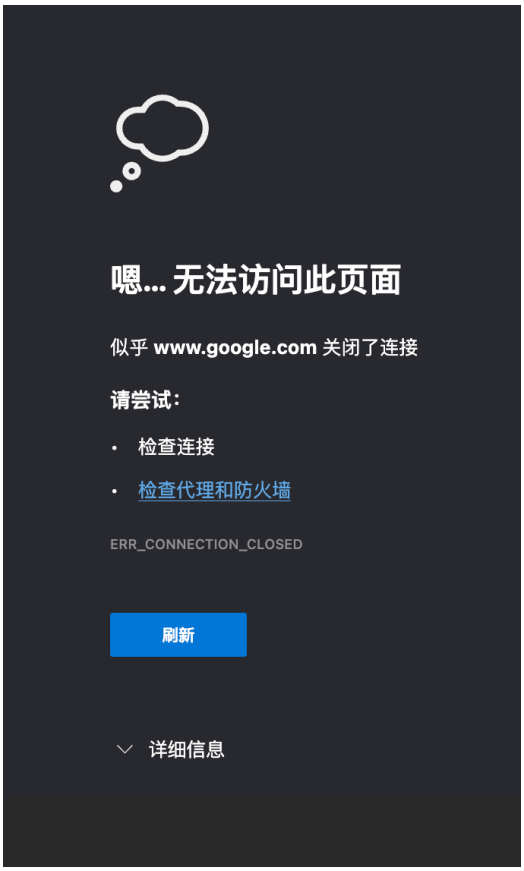

图1.1

为什么会这样？为什么我无法访问这些网站?

这一切的背后，都是"GFW"在操纵一切。

防火长城，即Great Firewall，简称GFW，也称中国国家防火墙，数据跨境安全网关，是中华人民共和国政府过滤国际互联网出口内容的软硬件系统集合。防火长城不是中国特有的一个专门单位，而是由分散部门的各服务器和路由器等设备，加上相关公司的应用程序构成，其监控所有经过国际网关的通讯，对认为不符合中国官方要求的传输内容，进行干扰、阻断、屏蔽。由于中国网络审查广泛，中国大陆内含有"不合适"内容的网站，会受到政府直接的行政干预，故防火长城主要作用在于分析和过滤中国境外网络的信息。

随着1994年中国接入国际互联网，不到两年时间内在发布施行的《计算机信息网络国际联网管理暂行规定》其中第六条规定："计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行创建或者使用其他信道进行国际联网"。

技术手段方面，一开始防火长城仅使用IP封锁，IP封锁是互联网审查的一种方式，防火墙维护一张IP地址的黑名单，一旦发现发往黑名单中地址的请求数据包，就直接将其丢弃，这将导致源主机得不到目标主机的及时响应而引发超时，从而达到屏蔽对目标主机的访问的目的，但是它的缺点也很明显，对被封禁的网站采用黑名单而不是对被允许访问的网站采用白名单的过滤机制，难免会有漏网之鱼的存在。而IP封锁这并不能应对网站时常更换IP的情况。自2002年开始，其能够自动执行针对特定域名的DNS劫持，并能够检测HTTP连接中的特定关键字，使用TCP重

置攻击的方法阻止连接。其中，DNS劫持又称域名服务器缓存污染，指由于防火长城自动执行DNS劫持攻击导致DNS服务器缓存了错误记录的现象。在中国大陆，对所有经过防火长城的在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，会马上伪装成目标解析服务器注入伪造的查询结果。攻击仅出现在DNS查询之路由经过防火长城时。劫持DNS可以做到很多事情，成都市某私立学校很可能使用了DNS劫持的方式ban掉了一些游戏网站，相同地，使用这种方法可以将 https://www.baidu.com 映射到 https://www.google.com。同时，也可以做到ban掉广告网站，将别人的网站替换成自己的网站。

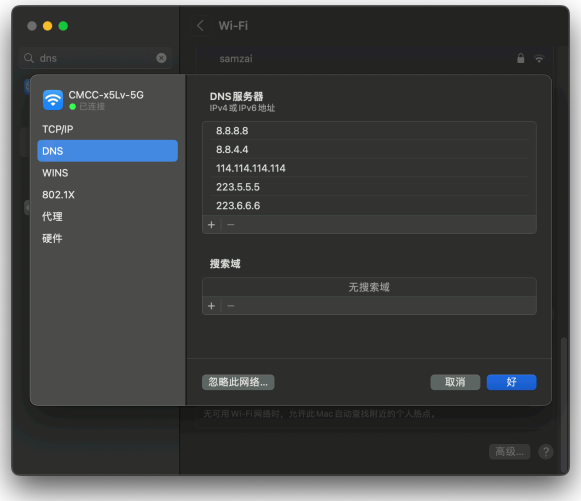

图1.2 DNS设置

防火长城工作在旁路，而非网关。网关是计算机网络中的一种设备或服务器，用于连接不同网络或协议之间进行数据转发和处理。

中国工程院院士、北京邮电大学前校长方滨兴是防火长城关键部分的首要设计师，被称为中国国家防火墙之父。

防火长城随着时代的发展也在不断变化和发展。

自2021年11月初以来，防火长城部署了一种类似白名单的检测方法：应用规则来豁免那些不太可能是完全加密的流量；然后它阻止其余未被豁免的流量。由于翻墙软件的流量多是完全加密的，这种方法十分有效，仅会误伤大约0.6%的非翻墙互联网流量。实现了对破网软件的反制。同时，GFW还在尝试间歇性封锁国际出口来切断对国外网站的访问。

同时，GFW还会尝试TLS站点证书中间人攻击。中间人攻击在密码学和计算机安全领域中是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。

说到GFW之父，这个人非常有趣。下面是一些例子。

2011年2月，方滨兴在接受《环球时报》英文版采访时称在自己的家用电脑上有6个VPN（虚拟专用网）用以测试防火长城。被问到防火长城是如何运作的时候，他拒绝回答，说"It's confidential"（这是机密）。文章发表后民愤强烈，《环球时报》随后在官方网站上撤下了该篇采访，不过文章仍然能从其他转载媒体的网站中找到。

2016年，方滨兴日前在中国超算中心发表演说时，有人询问有关防火长城的问题，方批评了防火墙管理人员不作为的情况。另一方面，他也主张谷歌与旗下YouTube也常会配合政府删除消息，他此次演讲多次称赞美国科技公司发展了令他欣赏的筛选算法，还花了许多时间演示说明其技术的精准高效，并鼓励中国研究员参考学习，莫不思进取。根据网友Maple Whispers录音，方原话如下：

我已经离开这个行当十几年了，这些话我不敢公开说，如果我还在干我就亲自（对他们）说了，我认为现在技术人员的问题是'无能'：什么叫无能呢，这好比说我知道这个楼里有炸弹，我本来可以精确的制导，制导到某一个坏人，但是我们现在仍然要炸掉这栋楼，坏人死了，其他人我不管，这就是技术人员的不作为。

你看谷歌，你看Youtube和刚才我演示的一些网页，都会有审查的制度，他们每天都过滤掉了大量的搜索结果。所以我觉得这件事防火长城应该有一个好的技术去解决。我想放行你们学生（上推特、脸谱），其实很简单，现在都可以，但是没有就说明是我们的技术不作为。

2016年4月3日，方滨兴以杰出校友身份，回到其母校哈尔滨工业大学做题为《定义网络空间安全》的报告。报告中，他试图以韩国政府也架设网络防火墙来论证中国架设网络防火墙的必要性。但由于论证其观点的韩国网页被防火长城阻挡，无法访问，方滨兴只能在众目睽睽之下连接VPN绕过防火长城继续演讲。但连接VPN后，1分钟之内便断线2次，只能在百度搜寻谷歌页面的截图。由于场面尴尬，报告结束后没有安排任何提问环节。

接下来要谈到的就是互联网审查规避技术。

大家"懂得最多"的肯定是**虚拟专用网**（英语：**V**irtual **P**rivate **N**etwork，缩写：**VPN**）。VPN是通过使用专用线路或在现有网络上使用隧道协议创建一个虚拟的点对点连接而形成的。虚拟私人网络不会让互联网变得"私有"。即使IP地址被隐藏，通过跟踪cookie和设备指纹仍然可以找到用户。虚拟私人网络本身并不是一种良好的互联网隐私保护手段——信任负担直接从ISP转移到VPN服务提供商。然而，这只是一种规避技术。

代理（英语：Proxy）也称网络代理，是一种特殊的网络服务，允许一个终端（一般为客户端）通过这个服务与另一个终端（一般为服务器）进行非直接的连接。代理协议有Socks和HTTP。功能有提高访问速度，控制对内部资源的访问，过滤内容，隐藏真实IP（只一个代理很难保证安全，更安全的方法是利用特定的工具创建代理链），突破网站的区域限制，突破网络审查等。

对等式网络（英语：peer-to-peer， 简称**P2P**），又称**点对点技术**，是去中心化、依靠用户群（peers）交换信息的互联网体系。

说到去中心化，是一种非常好的社会关系形态和内容产生形态，是相对于"中心化"而言的新型网络内容生产过程。随着网络服务形态的多元化，去中心化网络模型越来越清晰，也越来越成为可能。Web 2.0内容不再是由专业网站或特定人群所产生，而是由全体网民共同参与、权级平等的共同创造的结果。任何人都可以在网络上表达自己的观点或创造原创的内容，共同生产信息。

未完待续……