維基百科

防火长城

维基百科，自由的百科全书

防火长城[1]（英語：**Great Firewall**，常用简称：**GFW**，中文也称**中国国家防火墙**[2]，中国大陆民众俗称**墙**、**网络长城**、**功夫网**[3]等等），是中华人民共和国政府监控和过滤互联网国际出口内容的软硬件系统集合[4]。隨着使用的拓广，「墙」有时也被用作动词[5][6][7]，中国网友所說的「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中国大陆境外被屏蔽的网站或使用服务的行为。

目录

起源

方滨兴说此系统起步于1998年[8]，然而第一次使用 Great Firewall 这个名字的是Geremie Barmé和桑晔所写的文章《The Great Firewall of China》，文章发表于1997年6月1日，称当时中國金橋信息網和中国公用计算机互联网已经有在屏蔽国外新闻网站，这一审查系统开发开始在 1996 年。[9][10]

简介


中国国家防火墙之父方滨兴

一般情况下，中国国家防火墙，即防火长城，主要指中国政府用于过滤互联网国际出口上内容的软硬件系统的集合。[4]例如中國政府將查獲的特定網點阻斷，造成大家所熟知的連線錯誤現象，因此防火牆不是中國特有的一個專門單位，是由分散部門的各服务器和路由器等设备，加上相关公司的应用程序所构成，是一個軍民合作的大型資訊管制系統，世界其他一些國家也存在網路审查，不過其审查对象、规模、执行主体等均與中國的審查機制有著相當大的不同（参见：互联网审查），例如僅止於金融洗錢、國際詐騙等犯罪行為，或者仅审查儿童色情相关。而防火長城的作用是监控所有经过国际网关的通讯，对认为不符合中国共产党官方要求的传输内容，进行干扰、阻断、屏蔽。由於中國網絡審查廣泛，中國國內含有「不合適」內容的網站，會受到政府直接的行政干預，被要求自我审查、自我监管，乃至關閉，故防火長城主要作用在於分析和過濾中國境外網絡的資訊互相存取。中國工程院院士、北京郵電大學前校長方滨兴是防火长城关键部分的首要设计师[2][8][11][12]，被称为中国国家防火墙之父[13]。

然而，防火长城对网络内容的审查是否没有限制和不违反言论自由，一直是受争议的话题，官方說辭也相當籠統。有报告认为，防火长城其实是一种圆形监狱式的全面监控，以达到自我审查的目的[14]。2007年，人民网转载了题为「百度日本站被GFW屏蔽 疑与色情内容有关」的文章。[15]2011年2月17日有记者在外交部新闻发布会上问及互联网封锁等问题，发言人的回答是：

> 众所周知，中国的互联网发展迅速，网民人数增长很快，已超过4亿。中国政府鼓励和支持互联网发展，依法保障公民言论自由，包括网上言论自由。同时，中国对互联网依法进行管理，这符合国际惯例。我们愿同各国就互联网相关问题加强沟通和交流，共同推进互联网的良性发展，但反对任何国家借口互联网自由等问题干涉中国内政。[16]

次日，方滨兴在接受《环球时报》英文版采访时被问及防火长城是如何运作的，他拒绝回答，说「It's confidential.」(这是机密)[8]

在中國大陸民眾內部，由於內部蓬勃的互聯網企業，牆的存在感也逐漸被忽略，經過18個月的調查研究後，北京大學和斯坦福大學兩名經濟學家在2018年得出了結論，中國大學生對於獲取未經審查的政治敏感信息漠不關心。他們給北京兩所大學的近1000名學生提供了能夠繞過審查的免費工具，但發現近半數學生並沒有使用它。在那些使用了的學生中，幾乎沒人花時間瀏覽遭到屏蔽的外國新聞網站。[17]

主要技术

域名解析服务缓存污染

防火长城對所有经过骨干网国际出口路由的位于TCP与UDP的53端口上的域名查询请求进行IDS检测，一經發現处于黑名單關鍵詞中相匹配的域名查詢請求，防火长城作为中间设备會向查询者返回虚假结果，比真的回复更早到达。由于通常的域名查询没有任何认证机制，而且域名查詢通常基于的UDP協議是无连接不可靠的协议，查询者无法验证返回结果的正确性，而TCP协议则可以使用TCP连接重置来中断连接来阻止获得返回结果。DNSSEC技术为DNS解析服务提供了解析数据验证机制，理论上可以有效抵御劫持。此外，DNSCrypt、DoT、DoH等方法通过将DNS请求封装于安全连接内，以保护DNS请求中的数据不被中间传输设备篡改。

作为DNS系统的组成部分，全球一共有13组根域名服务器（Root Server）。2010年中国大陆有F、I、J這3个根域DNS镜像[18]，但曾因为多次DNS污染外国网络，威胁互联网安全和自由，北京的I根域服务器曾被断开与国际互联网的连接。[19][20]目前已恢复服务。[21]

从2002年左右开始，防火长城在国内进行域名服务器缓存污染。

2012年11月9日下午3点半开始，防火长城对Google的泛域名*.google.com进行了大面积的污染，所有以.google.com结尾的域名均遭到污染而解析错误不能正常访问，其中甚至包括不存在的域名，而Google为各国定制的域名也遭到不同程度的污染（因为Google通过使用CNAME记录来平衡访问的流量，CNAME记录大多亦为.google.com结尾），但Google拥有的其它域名如.googleusercontent.com等则不受影响。有网友推测Google被大面积阻碍连接是因为中共正在召开的十八大。[22]

2014年1月21日下午三点半，中国网站的.com、.net、.org域名解析不正常，网站被错误地解析至65.49.2.178，该IP位于美国北卡罗来纳州的Dynamic Internet Technology，即自由门的开发公司。据推测，可能是操作失误造成的事故。[23][24]

2015年1月2日起，污染方式升级，不再是解析到固定的无效IP，而是随机地指向境外的有效IP。刚开始只是对YouTube影片域名（*.googlevideo.com）进行处理，之后逐渐扩大到大多数被污染的域名。[25]这导致了境外服务器遭受来自中国的DDoS攻击，部分网站因此屏蔽中国IP。[26]使用者在浏览器中会看到无效的TLS证书警告（域名不匹配），但更多情况下是请求超时，因为通常这些IP已经被屏蔽。

这种DNS污染的方式曾经对中国大陆以外的用户造成影响。2010年3月，当美国和智利的用户试图访问热门社交网站如facebook.com和youtube.com还有twitter.com等域名，他们的域名查询请求转交给中国控制的DNS根镜像服务器处理，由于这些网站在中国被封锁，结果用户收到了错误的DNS解析信息，这意味着防火长城的DNS污染影响到国际互联网。[27]2010年4月8日，中国大陆一个小型ISP的错误路由数据，经过中国电信的二次传播，扩散到了整个国际互联网，波及到了AT&T、Level3、德国电信、Qwest和西班牙电信等多个国家的大型ISP。[28]

IP地址或传输层端口封锁

对拦截行为观察发现，在早期技术实现中，会使用访问控制列表（ACL）技术来封锁特定的IP地址，由此延伸可以封锁传输层协议（TCP或UDP）的特定目的端口的网络流量。不过由于大量的ACL匹配会导致网络性能不佳。现在主要是采用了效率更高的路由扩散技术封锁特定IP地址，也就是通过将需要拦截的IP地址配置为空路由、黑洞设备或特别配置的自治域网络上，然后通过动态路由协议将相应配置路由扩散到公众互联网网络中，从将条件匹配拦截行为转为路由器的常规转发行为，从而提高拦截效率。多见于自主拥有大量IP地址段的需要审查的企业中，例如Facebook，Google，Telegram，Twitter等。

> 在大规模自治域的出入口路由器上新接入一个起控管作用的子网或者AS域，将要受控的网络地址配置在这个子网或者AS域内的路由器中，这样利用**动态路由协议的网络拓扑自动识别特性**，在出入口路由器上将生成受控网络地址的路由信息，将自治域内部网络对这些受控网络地址的访问转入到这个控管子网或者AS域的网络中，从而实现对受控网络地址的流量控制 。[29]

针对TCP和UDP连接的封锁

2011年3月，防火长城曾经对Google部分服务器的IP地址实施自动封锁（按时间段）某些端口，按时段对www.google.com（用户登录所有Google服务时需此域名加密验证）和mail.google.com的几十个IP地址的443端口实施自动封锁，具体是每10或15分钟可以连通，接着断开，10或15分钟后再连通，再断开，如此循环，使中国大陆用户和Google主机之间的连接出现间歇性中断，使其各项加密服务出现问题。[30]Google指责中国这样的封锁手法，因为Gmail并非被完全阻断，营造出Google服务“不稳定”的假象，表面看上去好像问题出自Google本身。[31][32]

2014年5月27日起，几乎所有Google服務的80和443端口被封鎖。[33]2014年12月26日起，Google数段IP被路由扩散封锁，直接导致Gmail客戶端所用的IMAP/SMTP/POP3端口也被封鎖。[34][35]

目前防火长城会通过限制QoS优先级的方式干扰向境外的UDP连接，如网站使用HTTP/3（QUIC）协议时。[36]

TCP连接重置

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比连接双方更快地发送连接重置消息，使连接双方认为对方终止了连接而自行关闭连接。有关技术已被申请为发明专利。

Firefox的「連線被重置」錯誤訊息。当碰触到GFW設定的关键词后（如使用Google等境外搜索引擎），即可能马上出现這種畫面。

> 本发明提供了一种阻断TCP连接的方法和装置；方法包括：保存各TCP连接的连接信息；所述TCP连接的连接信息包括该TCP协议连接的：客户端信息、服务端信息、请求方向TCP等待序列号和应答方向TCP等待序列号；抓取TCP封包，找到该TCP封包所属TCP连接的连接信息，根据所抓取的TCP封包更新该连接信息中的请求方向TCP等待序列号和应答方向TCP等待序列号；如果所抓取的TCP封包为需要阻断的TCP封包，则根据更新后的、该TCP封包所属TCP连接的连接信息生成RST封包，并发送给该TCP连接的客户端和服务端。本发明可以进行准确而持续的阻断，从而能在大流量环境下的高效阻断非法TCP连接。[37]

一般这种攻击方法需要结合相应的检测方式来实施，例如：

- HTTP传输是未经过加密的，中间设备可以窃听传输内容。防火长城对 HTTP 回复的检测已经在2008年末终止。[38]目前仅检测HTTP请求的Host字段。
- 早期TLS版本中，服务器握手响应，包括**站点证书**，是未被加密的，所以可以用于识别出访问站点。自TLS 1.3开始，ServerHello之后的握手信息，包括站点证书，也会被加密后传输，一般可以认为能防止对证书信息的检测。[39][40]
- 服务器名称指示（SNI）是TLS的一个扩展协议，该协议下，在握手过程开始时客户端告诉它正在连接的服务器要连接的主机名称。由于SNI信息并未加密，审查者可以识别出使用者访问的网站域名。

有时防火长城也会不加判断地对到特定IP地址特定端口的连接执行TCP重置攻击，比如对GitHub所用的部分CDN节点的IP。

中间人攻击

自2014年8月28日起，原先可以通过IPv6直连Google的中国教育网（CERNET）内试图通过https连接*.google.com.*等网页时，可能收到SSL证书错误的提示，其中以连接https://www.google.com.hk/几乎是每次连接均收到攻击，而其它连接例如https://ipv6.google.com/和https://accounts.google.com/也有受到攻击的报告，但攻击发生的機率相对较低。伪造的SSL证书显示其为google.com，颁发机构即为其本身，与真正的证书不同，顯示谷歌在中国教育网上受到中间人攻击（MITM attack）。[41][42]

其他

对破网软件的反制

因为有防火长城的存在，大量境外网站无法在中国大陆境内正常访问，于是大陆网民开始逐步使用各类翻墙软件突破防火长城的封锁。针对网上各类突破防火长城的翻墙软件，防火长城也在技术上做了应对措施以减弱翻墙软件的穿透能力。通常的做法是利用上文介绍的各种封锁技术以各种途径打击翻墙软件，最大限度限制翻墙软件的穿透和传播。

同时根据中国大陆网民反映，防火长城现已有能力对基于PPTP和L2TP协议的VPN连接进行监控和封锁，这使得大陆网民突破防火长城的封锁变得更加困难。2015年1月起，部分国外VPN服务在中国大陆无法正常使用，这些VPN使用的是L2TP/IPSec和PPTP协议。[43]

对破网软件加密流量的探测

防火长城通过提取加密流量数据包，分析其特征，即可对破网软件中的加密流量进行精准识别，并可进一步进行阻断；[44][45]有研究表明防火长城可基于卷积神经网络对Shadowsocks流量进行探测。[46]

对Tor的刺探

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[47]，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[48]，目的是在用户建立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建立连接时，探针会以15分钟周期尝试与Tor进行SSL协商和重协商，但目的不是建立TCP连接。

间歇性封锁国际出口

从2011年5月6日起，中国大陆境内很多互联网公司以及高校、学院、科研单位的对外网络连接都出现问题，包括中国科学院。有分析指断网可能是因为防火长城已经具有了探测和分析大量加密流量并对用户IP地址执行封锁的能力，而各大机构的出口被封也在其中。具体表现为：当用户使用了破网（翻墙）软件后，其所在的公共网络IP地址会被临时封锁，所有的国际网站都无法访问，包括MSN、iTunes Store等，而访问国内网站却正常，但如果使用境外的DNS解析域名则将会由于DNS服务器被封锁导致无法解析任何域名，国内网站也会无法打开[49]。也有分析指，此举是中国当局在测试逐步切断大部分人访问国际网站的措施，以试探用户反应并最终达到推行网络「白名单」制，也就是凡没有在名单上的企业或团体其网络域名将不能解析，一般用户也无法访问[50]。而中共党机关报《人民日报》旗下的《环球时报》英文版则引述方滨兴指，一些ISP必须为自己的用户支付国际流量费用，因此这些公司「有动机」去阻碍用户访问国外网站。一位不愿留名的工信部官员说，用户碰到这些情况应先检查自己和网站的技术问题。[51][52]

深度包檢測

深度封包檢測（Deep packet inspection, DPI）是一種於應用層對網路上傳遞的資料進行偵測與處理的技術，被廣泛用於入侵檢測、流量分析及數據挖掘。就字面意思考慮，所謂「深度」是相對於普通的報文檢測而言的——相較普通的报文检测，DPI可對报文内容和协议特征进行检测。

在中國大陸，DPI一度被ISP用於追踪用戶行為以改善其廣告推送業務的精準性，而最近則被國外視為防火長城城賴以檢測關鍵詞及嗅探加密流量的重要技術之一[53]。基於必要的硬件設施、適宜的檢測模型及相應的模式匹配算法，防火長城能夠精確且快速地從實時網絡環境中判別出有悖於預期標準的可疑流量，並對此及時作出審查者所期望的應對措施。

针对IPv6协议的审查

IPv6（互联网通信协议第6版）是被指定为IPv4继任者的下一代互联网协议版本。

方滨兴在他的讲话《五个层面解读国家信息安全保障体系》中曾经说道：「比如说Web 2.0概念出现后，甚至包括病毒等等这些问题就比较容易扩散，再比如说IPv6出来之后，入侵检测就没有意义了，因为协议都看不懂还检测什么。」[54]

对电子邮件通讯的拦截

正常情况下，邮件服务器之间传输邮件或者数据不会进行加密，故防火长城能轻易过滤进出境内外的大部分邮件，当发现关键字后会通过伪造RST封包阻断连接。而因为这通常都发生在数据传输中间，所以会干扰到内容。也有網友根據防火长城會過濾進出境郵件的特性，尋找到防火长城部署的位置。[55]

2014年12月26日，有很多中国大陆网民反映说一度无法通过客户端登录到Gmail。在此之前，国内一些用户可以通过IMAP、SMTP和POP3接收、下载邮件；据路透社报道谷歌旗下的Gmail业务已经被当局封锁。[56]12月30日，Gmail的邮件服务器功能已在中国大陆境内恢复部分功能。[57][58]但Gmail网页版至今仍被屏蔽。

洪水攻击

中華人民共和國从2015年3月开始，使用一种被称为“大炮”的網路攻擊攻击方案，对可能涉及违反审查要求的特定网站，进行分散式阻斷服務攻擊（DDoS）。[59][60][61]

其中2015年3月针对Github的攻击，通过包括劫持常见的网站工具脚本植入攻击代码、一些常见浏览器漏洞等方法，持续五天对Github网站进行攻击，导致网站全球访问速度缓慢。[62]中国政府否认有关指责。[63] [64]

硬件

据2010年的估计，防火长城可能拥有数百台曙光4000L服务器[65]。

参与建设

- 美国作家Ethan Gutmann说，思科和一些其他通信设备供应商向中华人民共和国政府提供了具有流量监控和过滤功能的互联网设备，用来封堵网站和追踪网上一些活跃的民运人士。2006年2月，美国国会为此召开听证会，向思科、微软、雅虎、Google四家公司提出质询。美国中国信息中心的亨利·吴（Henry Wu，China Information Center）指责，思科不断主动地与中国中央及各省国家安全部门联系，向其提供最新技术，包括警车间的即时通讯和指挥系统、以及声音识别技术和指纹鉴别技术。[66]记者Sarah Lai Stirland在Wired News发表了一篇文章，并公布了一份泄漏的思科机密PPT文档。该文档详细描述了思科和中国政府在金盾工程上具有商业性质的合作[67]。她还在文章中指责，思科在市场营销中将这些技术明确划分为“镇压工具（A Tool of Repression）”。思科的辩护者声称，实际上，在中国大陆现行的内容过滤系统中，路由器只是作为底层执行设备对人为指定的目的地址进行屏蔽，这是任何一台商用路由器都必须提供的基本功能，思科并没有向中国政府提供特别开发和定制的互联网设备。[68]。

相关事件

参见

中华人民共和国网络审查

- 中华人民共和国审查词汇列表
- 中华人民共和国被封锁网站列表
- 中国大陆封锁维基媒体事件
- 大炮
- 河蟹

突破网络审查（俗称“翻墙”、“破网”、“科学上网”、“番茄”）

- 代理服务器
- VPN
- hosts文件

相关主张与设施

- 網路主權
- 和谐社会
- 國家區域網路
- 国际离岸云计算数据特别管理区
- 第五權
- 禁止网络盗版法案（SOPA，美國提出類似機制的法案）
- 蜻蜓計畫

相关人物

- 方滨兴

参考文献

引用

1. 只剩下门缝的VPN何去何从. 新华网. 北京商报. [2018-12-16]. （原始内容存档于2018-12-16）（中文（简体））.
2. 校长方滨兴:实施过滤计划慎用在线更新输入法. 人民网. 中国信息产业网. 2010-07-09 [2018-12-16]. （原始内容存档于2018-12-16）（中文（简体））.
3. 环球时报：防火墙带给中国互联网哪些影响. 环球时报. 2015-01-28 [2015-01-28]. （原始内容存档于2015-01-31）.
4. 潘永忠谈中国的网络审查制度. 法国国际广播电台（RFI）. 2019-03-20 [2021-07-05]. （原始内容存档于2020-02-26）.
5. Martin Johnson. 纽时多篇文章被“墙”. Greatfire. [2021-06-02]. （原始内容存档于2021-06-02）.
6. 两岸、新疆、六四……被墙前，Clubhouse中文房间在聊哪些公共议题？. 端传媒. [2021-06-02]. （原始内容存档于2021-06-24）.
7. 任琛. WhatsApp“被墙” 因为出事了？. 德国之声.
8. Global Times. Great Firewall father speaks out. SINA English. 2011-02-18 [2011-03-03]. （原始内容存档于2011-02-25）（英语）.
9. Geremie R. Barme; Ye, Sang. The Great Wall: a wonder and a curse!. chinaheritage.net. 2017-07-26 [2021-08-03]. （原始内容存档于2021-02-26）.
10. Geremie R. Barme; Ye, Sang. The Great Firewall of China. Wired. 1997-01-06 [2015-12-29]. （原始内容存档于2016-01-01）.
11. 李永峰. 網民披露方濱興是GFW之父國慶前夕中國網絡再次收緊. 亞洲週刊. 2009-10-04, **23** (39) [2009-09-25]. （原始内容存档于2011-05-15）（中文（繁體））.
12. 方滨兴的墙内墙外. 南方周末. [2013-07-18]. （原始内容存档于2013-07-21）（中文（中国大陆））.
13. 存档副本. [2019-05-02]. （原始内容存档于2018-03-26）.
14. （英文）JR, Crandall; Zinn D; Byrd M; Barr E; East R, ConceptDoppler: A Weather Tracker for Internet Censorship (PDF), Computer and Communications Security, 2007 [2007-09-13], （原始内容存档 (PDF)于2007-10-26）
15. 百度日本站被GFW屏蔽 疑与色情内容有关. 人民网. [2008-09-09]. （原始内容存档于2007-04-18）.
16. 外交部就"北方四岛"、中国互联网发展等答记者问. 2011-02-17 [2021-05-26]. （原始内容存档于2011-03-02）.
17. 那些和「防火長城」一起長大的中國年輕人. 紐約時報中文網. 2018-08-07 [2018-08-30]. （原始内容存档于2018-08-30）（中文）.
18. （英文）Asia Pacific Root servers (http://www.apnic.net/community/support/root-servers/root-server-map)（页面存档备份 (https://web.archive.org/web/20101207000355/http://www.apnic.net/community/support/root-servers/root-server-map)，存于互联网档案馆），亚太互联网络信息中心

19. DNS污染问题发生后中国根服务器被关. Solidot. 2010-03-28 [2021-08-19]. （原始内容存档于2011-05-11）.
20. After DNS problem, Chinese root server is shut down. IT World. 2010-03-26 [2011-05-19]. （原始内容存档于2011-11-24）.
21. Root Server Technical Operations Assn. [2014-01-25]. （原始内容存档于2017-08-24）.
22. 我们的网络为什么这么卡. 2012-11-09 [2021-08-19]. （原始内容存档于2013-01-26）.
23. 中国顶级域名根服务器故障 大部分网站受影响. 新浪科技. 2014-01-21 [2014-01-21]. （原始内容存档于2014-01-27）.
24. 中國網路癱瘓 疑內部作業失誤. 自由時報. 2014-01-23 [2014-01-23]. （原始内容存档于2014-01-23）.
25. 防火长城使用有效IP投毒DNS，其中包括色情网站IP. 2015-01-09 [2021-08-19]. （原始内容存档于2015-04-03）.
26. 遭DNS投毒DDoS攻击的服务器屏蔽中国IP. 2015-01-23 [2021-08-19]. （原始内容存档于2015-04-02）.
27. China censorship leaks outside Great Firewall via root server. Ars Technica. 2010-03 [2011-05-19]. （原始内容存档于2011-06-22）.
28. A Chinese ISP Momentarily Hijacks the Internet. PC World. 2010-04-09 [2011-05-19]. （原始内容存档于2011-06-22）.
29. 刘刚; 云晓春; 方滨兴; 胡铭曾. 一种基于路由扩散的大规模网络控管方法. 通信学报. 2003. ISSN 1000-436X. （原始内容存档于2021-07-07）.
30. 翻墙专题：Google掉包问题. RFA. 2011-03-11 [2011-03-21]. （原始内容存档于2011-03-17）.
31. DAVID BARBOZA; CLAIRE CAIN MILLER. *Google Accuses Chinese of Blocking Gmail Service*. 紐約時報. 2011-03-20 [2015-01-27]. （原始内容存档于2015-10-04）.（英文）
32. Google accuses China of blocking Gmail. 法新社. 2011-03-21 [2013-03-18]. （原始内容存档于2014-02-24）.
33. China Escalating Attack on Google. 紐約時報. 2014-06-02 [2018-08-08]. （原始内容存档于2014-07-14）.（英文）
34. Gmail被中国完全屏蔽. [2014-12-29]. （原始内容存档于2015-01-03）.
35. 社评：中国出于安全考虑“封”Gmail不可信. [2014-12-30]. （原始内容存档于2015-01-20）.
36. 【翻牆問答】互聯網推新傳輸協議UDP 中國網民難受惠. Radio Free Asia. 2020-02-07 [2021-08-07]（中文（香港））. “李建軍：由於中國的電訊公司都是國有企業，他們一定會執行黨的政策，因此，他們必然會在UDP上動手腳。現時大部分中國電訊公司的做法，都是在網絡QoS（中文或者可以稱為服務質素控制）上作出調動，對UDP通訊包的流量和速度作出限制，那麼當你用以UDP為本的技術翻牆時，就會十分之慢，慢至一個不可忍受的程序，那很多人就會放棄使用這種方法。”

37. 专利号2009100850310,《一种阻断TCP连接的方法和装置》, https://patents.google.com/patent/CN101902440A/zh （页面存档备份 (https://web.archive.org/web/20190218020007/https://patents.google.com/patent/CN101902440A/zh)，存于互联网档案馆）, 2018-04-24查阅.
38. Jong Chun Park; Jedidiah R. Crandall. Empirical Study of a National-Scale Distributed Intrusion Detection System: Backbone-Level Filtering of HTML Responses in China. International Conference on Distributed Computing Systems. IEEE. 2020-08 [2021-06-11]. ISBN 978-1-4244-7262-8. doi:10.1109/ICDCS.2010.46. （原始内容存档于2021-06-11） （美国英语）.
39. Rescorla, Eric. The Transport Layer Security (TLS) Protocol Version 1.3. tools.ietf.org. [2019-07-17]. （原始内容存档于2019-06-03） （英语）.
40. Differences between TLS 1.2 and TLS 1.3 (#TLS13) - wolfSSL. 2019-02-18 [2019-07-17]. （原始内容存档于2019-07-17） （美国英语）.
41. 谷歌在中国教育网遭国家级中间人攻击. greatfire.org. 2014-09-04 [2015-02-02]. （原始内容存档于2015-03-27）.
42. 知名网站遭遇SSL中间人攻击 手法很熟业务很忙. 2014-10-21 [2015-02-02]. （原始内容存档于2014-10-24）.
43. 网易. 《环球时报》英文版：部分国外VPN服务在中国无法正常使用_网易财经. money.163.com. [2015-08-21]. （原始内容存档于2016-03-05）.
44. 一种数据包频度分析的网络代理加密流量特征提取方法, 2018-10-10 [2019-08-18], （原始内容存档于2019-08-18）
45. 一种代理上网行为识别与检测方法, 2018-03-15 [2019-08-18], （原始内容存档于2019-08-18）
46. 一种基于卷积神经网络的shadowsocks流量检测方法, 2018-06-04 [2019-08-18], （原始内容存档于2019-08-18）
47. Knock Knock Knockin' on Bridges' Doors. Tor. [2012-01-10]. （原始内容存档于2012-01-13）.
48. China's Great Firewall Tests Mysterious Scans On Encrypted Connections. [2011-11-17]. （原始内容存档于2011-11-18）.
49. 中国网警“修理”翻墙网民中科院也被牵连. 法國國際廣播電台. 2011-05-18 [2011-05-18]. （原始内容存档于2011-05-21）.
50. 中国网络国际访问频故障　温水煮蛙测试断外网反应？. 自由亞洲電台. 2011-05-12 [2011-05-18]. （原始内容存档于2011-05-14）.
51. Theories abound for overseas web access troubles. 环球时报. 2011-05-18 [2011-05-19]. （原始内容存档于2011-05-21）.
52. 方滨兴教授回应国外网站不能拜访事件. Solidot. 2011-05-18 [2021-08-19]. （原始内容存档于2011-05-20）.
53. Internet Filtering in China in 2004-2005: A Country Study. Open Net Initiative. [2014-12-31]. （原始内容存档于2016-04-10）.
54. 方滨兴院士解读国家信息安全保障体系（转载）. 中华人民共和国工业和信息化部. 2009年 [2011-03-21]. （原始内容存档于2011-05-11）.

55. 找出GFW在Internet的位置，全面分析国内到国外邮件受阻的原因 (https://web.archive.org/web/20101028163039/http://www.chinaunix.net/jh/14/838622.html) - ChinaUnix.net
56. Gmail blocked in China. Reuters. 2014-12-29 [2014-12-29]. （原始内容存档于2019-07-13）.
57. 看在中国留学生的面子上 Gmail又能用了 - 好还是不好? - 海外留学 - 人在海外 - 美国华裔教授专家网 ScholarsUpdate.com. scholarsupdate.hi2net.com. [2015-09-15]. （原始内容存档于2015-12-30）.
58. Gmail中国内地服务得以部分恢复. [2015-09-23]. （原始内容存档于2015-09-23）.
59. Perlroth, Nicole. China Is Said to Use Powerful New Weapon to Censor Internet. The New York Times. The New York Times Company. 2015-04-10 [2015-04-11]. （原始内容存档于2015-04-11） （英语）.
60. 路西. 中國採取新方式 網絡封鎖擴大到境外. BBC中文網. 2015-04-11 [2015-04-11]. （原始内容存档于2015-04-14） （中文（繁體））.
61. 秦雨霏. 中共祭出新武器審查網絡 訪問陸網或被監控. 大紀元. 2015-04-10 [2015-04-11]. （原始内容存档于2015-04-11） （中文（台灣））.
62. GitHub. GitHub System Status. [2016-01-02]. （原始内容存档于2017-02-19）.
63. 陳曉莉. GitHub遭遇史上最大規模DDoS攻擊，反中國網路防火牆專案被鎖定. 台灣iThome. 2015-03-30 [2015-03-30]. （原始内容存档于2015-03-31） （中文（台灣））.
64. 海寧. 中共借刀杀人 利用海外华人发起DDoS攻击. 大紀元新聞網. 2015-03-27 [2015-03-30]. （原始内容存档于2015-03-30） （中文（簡体））.
65. 中国GFW预作新技术储备用大奖赛招徕人才（图）. 自由亚洲电台. 2010-06-08 [2010-06-09]. （原始内容存档于2010-09-28）.
66. documentary《The Tank Man》
67. Sarah Lai Stirland. Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers. 2008-05-20 [2009-06-27]. （原始内容存档于2009-06-26）.
68. Earnhardt, John. Cisco Testimony Before House International Relations Subcommittee. Cisco Systems, Inc. 2006-02-16 [2007-01-25]. （原始内容存档于2013-06-02）.

来源

网页

- BLUE的炫影. "连接被重置". 译言. 2008-03-24 [2021-07-16]. （原始内容存档于2011-10-17） （中文（中国大陆））.
- 本文全部或部分内容来自美国联邦政府所属的**美国之音**网站。根据版权条款 (http://www.voachinese.com/p/3874.html)和有关美国政府作品版权的相关法律，其官方发布的内容属于公有领域。

外部链接

- 台灣駭客年會第十四屆 道高一尺，牆高一丈：東亞網絡封鎖和反對鎖技術演進 (https://chinadigitaltimes.net/chinese/2018/07/%e5%8f%b0%e7%81%a3%e9%a7%ad%e5%ae%a2%e5%b9%b4%e6%9c%83%e7%ac%ac%e5%8d%81%e5%9b%9b%e5%b1%86-%e9%81%93%e9%ab%98%e4%b8%80%e5%b0%ba%ef%bc%8c%e7%89%86%e9%ab%98%e4%b8%80%e4%b8%88%ef%bc%9a%e6%9d%b1%e4%ba%9e/)（页面存档备份 (https://web.archive.org/web/20190821204519/https://chinadigitaltimes.net/chinese/2018/07/%e5%8f%b0%e7%81%a3%e9%a7%ad%e5%ae%a2%e5%b9%b4%e6%9c%83%e7%ac%ac%e5%8d%81%e5%9b%9b%e5%b1%86-%e9%81%93%e9%ab%98%e4%b8%80%e5%b0%ba%ef%bc%8c%e7%89%86%e9%ab%98%e4%b8%80%e4%b8%88%ef%bc%9a%e6%9d%b1%e4%ba%9e/)，存于互联网档案馆）（简体中文）
- Chinese bloggers run the gauntlet of forced registration, censorship (http://www.ojr.org/ojr/stories/050621glaser/)（页面存档备份 (https://web.archive.org/web/20061104011520/http://www.ojr.org/ojr/stories/050621glaser/)，存于互联网档案馆）（英文）
- Website Test behind the Great Firewall of China (http://www.websitepulse.com/help/testtools.china-test.html)（页面存档备份 (https://web.archive.org/web/20101229071123/http://www.websitepulse.com/help/testtools.china-test.html)，存于互联网档案馆）, WebSitePulse（英文）
- GreatFire.org (https://zh.greatfire.org/)（页面存档备份 (https://web.archive.org/web/20130527041419/https://zh.greatfire.org/)，存于互联网档案馆）（简体中文）
- 入侵防御系统的评测和问题 (http://www.chinagfw.org/2009/09/gfw_21.html)（页面存档备份 (https://web.archive.org/web/20100430010756/http://www.chinagfw.org/2009/09/gfw_21.html)，存于互联网档案馆）（简体中文）
- 阅后即焚：“GFW” (https://web.archive.org/web/20100507065344/http://freemorenews.com/2009/08/30/burn-after-reading-gfw/)（又名GFW的前世今生）——匿名作者（简体中文）
- 深入理解GFW：内部结构 (http://gfwrev.blogspot.com/2010/02/gfw.html)（页面存档备份 (https://web.archive.org/web/20100223045019/http://gfwrev.blogspot.com/2010/02/gfw.html)，存于互联网档案馆）（简体中文）
- 田小路. “网上长城”攻防战. 凤凰周刊, 腾讯新闻. "vingietang" (责任编辑). 2010-12-22 [2018-04-16]（中文（中国大陆））.
