WIKIPEDIA

防火长城

维基百科，自由的百科全书

防火长城[1]（英语：**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**、**防火墙**、**功夫网**[3]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[4]，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》[5]，取与Great Wall（长城）相谐的效果，简写为Great Firewall，缩写GFW[6]。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的行为。

目录

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监控和过滤互联网国际出口上内容的软硬件系统的集合。例如监视系统就曾与美商合作，构建类似美国的棱镜计划的深度侦查机制，但中国政府并进一步设置将查获的特定网点阻断等，造成大家所熟知的连线错误现象，因此防火墙不是中国特有的一个专门单位，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所构成，是一个跨军民合作的大型信息管制系统，世界其他一些国家也存在网络审查，不过其审查对象、规模、执行主体等均与中国的审查机制有着相当大的不同(参见：互联网审查)，例如仅止于金融洗钱、国际诈骗等犯罪行为，或者仅审查儿童色情相关。而防火长城的作用是监控所有经过国际网关的通讯，对认为不匹配中共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，中国国内含有“不合适”内容的网站，会受到政府直接的行政干预，被要求自我审查、自我监管，乃至关闭，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互相访问。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[2][4][7][8]，被称为**中国国家防火墙之父**[9]。

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，官方说辞也相当笼统。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[10]。而中共当局一直没有正式对外承认防火长城的存在，如当有记者在外交部新闻发布会上问及互联网封锁等问题的时候，发言人的答案基本都是“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，这匹配国际惯例。”方滨兴曾在访问中被问及防火长城是如何运作的时候，他指这是“国家机密”。不过2015年1月与官方有密切关系的《环球时报》则发布报道曾公开宣扬其存在。[11]

在中国大陆民众内部，由于内部蓬勃的互联网企业，墙的存在感也逐渐被忽略，经过18个月的调查研究后，北京大学和斯坦福大学两名经济学家在2018年得出了结论，中国大学生对于获取未经审查的政治敏感信息漠不关心。他们给北京两所大学的近1000名学生提供了能够绕过审查的免费工具，但发现近半数学生并没有使用它。在那些使用了的学生中，几乎没人花时间浏览遭到屏蔽的外国新闻网站。[12]

中国还有一套公开在公安部辖下的网络安全项目——金盾工程，其主要功能是处理中国公安管理的业务，涉外饭店管理，出入境管理，治安管理等，所以金盾工程和防火长城的关系一直没有明确的认定。

主要技术

域名解析服务缓存污染

防火长城对所有经过骨干出口路由的在UDP的53端口上的域名查询会被IDS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虚假查询结果，并丢弃之后的正确查询结果。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。

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等负载于安全连接的DNS访问也能保护DNS的访问数据不被中间传输设备篡改。

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这3个根域DNS镜像[13]，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。[14][15]当前已恢复服务。[16]

从2002年左右开始，中国大陆的网络审查机关开始采用域名服务器缓存污染技术，防止了一般民众访问被过滤的网站。对于含有多个IP地址或经常变更IP地址逃避封锁的域名，防火长城通常会使用此方法进行封锁，具体方法是当用户从境内向境内DNS服务器提交域名请求时，DNS服务器要查询根域名服务器，此过程会受防火长城污染。而用户不做任何保

护措施直接查询境外DNS时，会受防火长城污染。当用户从境外查询境内服务器（不一定是有效DNS服务器），结果也会被污染。

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污染已影响国际互联网。[17]

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。[18]

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。[19]

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。[20][21]

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。[22]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。[23]

IP地址或传输层端口封锁

针对TCP和UDP连接的封锁

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。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。

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。[24]Google指中国这样的封锁手法高明，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。[25][26]

2014年5月27日起，几乎所有Google服务的80和443端口被屏蔽。[27]2014年12月26日起，Google数段IP被路由扩散封锁，直接导致GMAIL客户端所用的IMAP/SMTP/POP3端口也被屏蔽。[28][29]

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。所以基于路由封锁的方法现在主要用于针对自主拥有大量连

续地址段的特定网络服务商，例如Google、Twitter、Facebook等；对于内容分发网络（CDN）的地址段可能不会采用这种地址封锁的方法，以避免误封；基于ACL策略可能会在当地的互联网服务商（ISP）中使用，同时用于控制过度往网络发送数据包的控制。

针对UDP连接的干扰

针对Google的部分域名，在保证IP未被路由扩散技术封锁的情况下，使用HTTP/3(QUIC传输协议）的UDP连接可以有效避开防火长城的审查。但从2019年3月起，出现针对UDP的连接干扰。（错误提示：ERR_QUIC_PROTOCOL_ERROR），当前防火长城仍然无法对UDP连接进行针对性阻拦，但防火长城可以干扰其连接，使得当前所有利用 UDP 翻墙的手段都可能会受到干扰，特别是在针对 QUIC 方面会阻断 UDP 443 端口的连接。[30]

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。

Firefox的“连线被重置”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。

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，其效率被认为比单纯的数据包丢弃更有效，因为后者会令连接双方认为连接超时而不断重试创建连接。

有关技术已被申请为发明专利。

> 本发明提供了一种阻断TCP连接的方法和设备；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数据包，找到该TCP数据包所属TCP连接的连接信息，根据所抓取的TCP数据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数据包为需要阻断的TCP数据包，则根据更新后的、该TCP数据包所属TCP连接的连接信息生成RST数据包，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。[31]

一般这种攻击方法需要结合相应的检测方式来实施。

针对HTTP协议的关键字阻断

2002年左右开始，中国大陆研发了一套关键字过滤系统。这个系统能够从出口网关收集分析信息，过滤、嗅探指定的关键字。普通的关键词如果出现在HTTP请求数据包的标头（如“`Host: www.youtube.com`”）时，则会马上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，进而使请求的内容无法继续查看。如果防火长城在数据流中发现了特殊的内文关键词（如“falun”等）时，其也会试图打断当前的连接，从而有时会出现网页开启一部分后突然停止的情况。在任何阻断发生后，一般在随后的90秒内同一IP地址均无法浏览对应IP地址相同端口上的内容。

2010年3月23日，Google宣布关闭中国服务器（Google.cn）的网页搜索服务，改由Google香港域名Google.com.hk提供后，由于其服务器位于大陆境外必须经过防火长城，所以防火长城对其进行了极其严格的关键词审查。一些常见的中共高官的姓氏，如“胡”、“吴”、“温”、“贾”、“李”、“习”、“贺”、“周”、“毛”、“江”、“令”，及常见姓氏“王”、“刘”、“彭”等简体中文单字，当局实行一刀切政策全部封锁，即“学习”、“温泉”、“李白”、“圆周率”也无法搜索，使Google在中国大陆境

内频繁出现无法访问或搜索中断的问题。2011年4月，防火长城开始逐步干扰Google.com.hk的搜索服务。2012年10月下旬起，防火长城使用更巧妙方式干扰Google搜索，部分用户在点击搜索结果链接跳转时一直被卡住，一直卡了6分钟之后客户端发送RST重置，然后页面一片空白。原因是链接跳转使用的是HTTP，用HTTPS跳转无影响。[32]

这种阻断可以双向工作。在中华人民共和国境外访问位于境内的网站时，如果在数据包头部出现部分关键字，连接也可能会被阻断。两者的关键词列表并不完全相同，比如在境外使用知网搜索“法轮功”连接会被阻断，并且90秒无法访问，搜索“六四”则不会，在中华人民共和国境内访问境外网站时两者都会被阻断。

由于HTTPS采取加密传输，关键词阻断无法对网页传输造成影响。但由于身份认证证书信息是明文传输，因此阻断仍然是有可能的。

后来Google等网站开始采用HTTPS传输数据，针对HTTP协议的关键字阻断对相当一部分网站已经失去作用。

针对TLS的SNI阻断

虽然TLS能保证全程内容加密而且发现连接被干扰时警告并中断，但是对于SNI信息仍然是未加密的，仍可以被识别出访问域名。从2018年8月24日开始，开始出现基于SNI的检测机制，维基百科部分项目、日本亚马逊等启用https服务的网站同样被封锁。[33]

针对TLS的证书传输检测

由于TLS在握手期间，服务器传输站点证书时同样也是明文传输的，防火长城可以对证书的信息进行检测，从而是否需要被拦截的站点而中断TCP连接。

自2017年9月19日起，防火长城开始启用CA证书检测，若经过防火长城时，一旦探测到相关域名如：Google，Facebook，Youtube，Twitter，WhatsApp的CA证书，对应IP通信会被拦截切断。若使用SNI服务器IP反向代理部分域名也会被拦截（网站会提示ERR_CONNECTION_CLOSED 意外终止了连接），但并不是全部IP都会被拦截，可用IP极少。拦截只针对经过出口路由上。

由于TLS 1.3开始，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。

对eD2k协议的连接干扰

从2011年开始，防火长城开始对所有境外eD2k服务器进行审查。当境内用户使用eD2k协议例如eMule使用模糊协议连接境外服务器时会被无条件阻断，迫使eMule使用普通方式连接境外服务器；同时防火长城对所有普通eD2k连接进行关键字审查，若发现传输内容含有关键字，则马上切断用户与境外服务器的连接，此举阻止了用户获取来源和散布共享文件信息，从而阻碍使用eD2k协议软件的正常工作。[34][35]

其他

对破网软件的反制

因为防火长城的存在，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。[36]

针对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[37]，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[38]，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。

间歇性完全封锁

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[39]。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[40]。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。[41][42]

境内骨干路由器间歇性阻断

2012年10月下旬，Google位于北京的服务器被国家级骨干路由器长时间干扰连接，包括中国大陆境内用户在内访问时返回“连接超时”错误，造成大量基于Hosts技术利用Google北京服务器作为反向代理访问Google服务的用户和软件无法正常使用，例如GoAgent。测试指出数据包经过部分国家级骨干路由器时被选择性丢弃，造成与服务器连接的丢包率飙升，甚至有部分用户反映被完全阻断与服务器之间的连接。

深度包检测

深度数据包检测（Deep packet inspection,DPI）是一种于应用层对网络上传递的数据进行侦测与处理的技术，被广泛用于入侵检测、流量分析及数据挖掘。就字面意思考虑，所谓“深度”是相对于普通的报文检测而言的——相较普通的报文检测，DPI可对报文内容和协议特征进行检测。

在中国大陆，DPI一度被ISP用于追踪用户行为以改善其广告推送业务的精准性，而最近则被国外视为防火长城城赖以检测关键词及嗅探加密流量的重要技术之一[43]。基于必要的硬件设施、适宜的检测模型及相应的模式匹配算法，防火长城能够精确且快速地从实时网络环境中判别出有悖于预期标准的可疑流量，并对此及时作出审查者所期望的应对措施。

华为公司曾被媒体指责涉及向伊朗政府提供DPI所依赖的硬件支持以帮助后者开展网络审查工作[44]。

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。在IPv4网络，当时的网络设计者认为在网络协议栈的底层并不重要，安全性的责任在应用层。但是即使应用层数据本身是加密的，携带它的IP数据仍会泄漏给其他参与处理的进程和系统，造成IP数据包容易受到诸如信息包探测（如防火长城的关键字阻断）、IP欺骗、连接截获等手段的会话劫持攻击。虽然用于网络层加密与认证的IPsec协议可以应用于IPv4中，以保护IPv4网络层数据的安全，但IPsec只是作为IPv4的一个可选项，没有任何强制性措施用以保证IPsec在IPv4中的实施。因为防火长城是挂载在国家级骨干路由器的旁路设备，而网络数据传输必须知道数据包来源地与数据包的目的地才能完成路由转发，故在IPv4协议时代实施的针对IP地址封锁技术和特定IP地址端口封锁技术依然对IPv6有效。

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。”[45]

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，但攻击发生的几率相对较低。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google证书不同，显示谷歌在中国教育网上受到中间人攻击（MITM attack）。[46][47]

现阶段防火长城已经具备干扰IPv6隧道的能力[48]，因为IPv6隧道在用户到远程IPv6服务器之间的隧道是创建在IPv4协议上的，因为数据传输分片的问题或者端点未进行IPSec保护的时候很有可能暴露自己正在传输的数据，让防火长城有可乘之机干扰切断连接。另外因为防火长城实行DNS污染，通过域名来访问IPv6服务器时可能也会因错误解析而无法访问。

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数据包阻断连接。而因为这通常都发生在数据传输中间，所以会干扰到内容。也有网民根据防火长城会过滤进出境邮件的特性，查找到防火长城部署的位置。[49]

2007年7月17日，大量使用中国国内邮件服务商的用户与国外通信出现了退信、丢信等普遍现象[50]，症状为：

- 中国国内邮箱给国外域发信收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”
- 中国国内邮箱用户给国外域发信，对方收到邮件时内容均为“aaazzzaaazzzaaazzzaaazzzaaazzz”。
- 中国国内邮箱给国外域发信收到退信，退信提示“Connected to *.*.*.* but connection died.（#4.4.2）”
- 国外域给中国国内邮箱发信时收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”
- 国外域给中国国内邮箱发信后，中国国内邮箱用户收到的邮件内容均为“aaazzzaaazzzaaazzzaaazzzaaazzz”。

对此，新浪的解释是“近期互联网国际线路出口不稳定，国内多数大型邮件服务提供商均受到影响，在此期间您与国外域名通信可能会出现退信、丢信等现象。为此，新浪VIP邮箱正在采取措施，力争尽快妥善解决该问题。”而万网客户服务中心的解释是“关于近期国内互联网国际出口存在未知的技术问题导致国内用户与国外通信可能会出现退信、丢信等普遍现象，万网公司高度重视，一直积极和国家相关机构汇报沟通，并组织了精良的技术力量努力寻找解决方案。”[51]

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。[52]12月30日，Gmail已在中国大陆境内恢复部分功能。[53][54]但Gmail网页版仍被屏蔽。

网络攻击

中华人民共和国从2015年3月开始，使用一种被称为“大炮”的网络攻击攻击方案，对可能涉及违反审查要求的特定网站，进行分布式拒绝服务攻击（DDoS）。[55][56][57]

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。[58]中国政府否认有关指责。[59] [60]

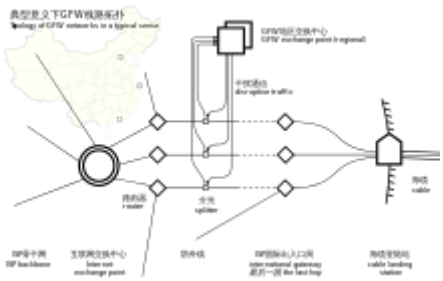
硬件

据2010年的估计，防火长城可能拥有数百台曙光4000L服务器[61]。

- 防火长城（北京）使用曙光4000L机群，操作系统为Red Hat系列（从7.2到7.3到AS 4），周边软件见曙光4000L一般配置
- 防火长城实验室（哈尔滨工业大学）使用曙光服务器，Red Hat操作系统
- 防火长城（上海）使用Beowulf集群。GFW是曙光4000L的主要需求来源、研究发起者、客户、股东、共同开发者。2007年防火长城集群规模进一步扩大，北京增至360节点，上海增至128节点，哈尔滨增至64节点，共计552

节点。机群间星型千兆互联。计划节点数上千。

- 有理由相信防火长城（北京）拥有16套曙光4000L，每套384节点，其中24个服务和数据库节点，360个计算节点。每套价格约两千万到三千万，占005工程经费的主要部分。有3套（将）用于虚拟计算环境实验床，计千余节点。13套用于骨干网络过滤。总计6144节点，12288CPU，12288GB内存，峰值计算速度48万亿次。



典型意义下GFW的线路拓扑

2 GHz CPU的主机Linux操作系统下可达到600Kbps以上的捕包率。通过骨干网实验，配置16个数据流总线即可以线速处理八路OC48（一路OC48约2.5Gbps）接口网络数据。曙光4000L单结点的接入能力为每秒65万数据包，整个系统能够满足32Gbps的实时数据流的并发接入要求。有理由相信GFW的总吞吐量为512Gbps甚至更高（北京）。

相关事件

针对网络封锁的诉讼

北京奥运会

据法新社报道，中国政府曾讨论是否在北京奥运会期间放宽防火长城的屏蔽范围[62]。在奥运前夕，曾一度被限制访问的Blogger、《中国时报》、《明报》等网站陆续被解除封锁，中文维基、BBC中文网和大赦国际网站等网站在8月1日亦被证实解封[63]，但部分被禁网站仍然未被解禁，包括“法轮功”网站、“西藏流亡政府”网站以及和“六四事件”相关的网站[64]。《齐鲁晚报》报道，有外国媒体指责中国政府违背先前全面开放互联网的承诺，奥组委发言人孙伟德表示，奥运期间将提供媒体“充分”的网络使用权，但外国记者上网不会完全不受限制。根据中国的法律，不得通过互联网传播违反法律的信息，如宣扬法轮功，以危害国家利益。希望媒体尊重中国“有关法律法规”。但文中没有解释为何众多与法轮功完全无关的新闻机构、博客、社交和视频网站也无法访问。[65]国际奥委会新闻委员会主席高斯帕也表示，国际奥委会一些官员和中国当局已经达成协议，同意中国封锁一些被认为是敏感的、与奥运无关的网站[66]。

奥运会结束数月后，中国政府对海外新闻网站的封锁又重新开始。至2008年12月，重新被封锁的网站包括德国之声、BBC、美国之音、法广、澳广、加拿大广播电台等新闻机构的中文网站。此外，根据总部在美国的非盈利维权组织“自由之家”16日发布的新闻稿，这次遭中国政府封闭的还有一些被视为敏感的网站，包括无国界记者、《亚洲周刊》和《明报》等。中华人民共和国外交部发言人刘建超表示，中国总体上是采取对外开放的政策，但是中国和其他国家一样，对于网站还是要依法做必要的管理，某些网站确实存在违反中国法律的事情[67]。有评论认为，当局此次收紧舆论控制是为了防止经济危机进一步转化为社会与政治危机[68]。

对谷歌的封锁

对维基百科的封锁

2013年对代码托管网站GitHub的审查和封锁

2013年1月20日，中国大陆政府的防火长城利用域名污染和关键词过滤等手段屏蔽GitHub。但是，由于屏蔽引发了社会的强烈反应，最终解除了对GitHub的屏蔽。

2014年中国网络异常事件

2014年1月21日下午中国发生大范围网络故障。由于中国通用顶级域域名解析出现异常，许多网站域名被解析到了完全没有反应的IP地址 65.49.2.178。

亚太经合组织（APEC）会议

2014年11月，由北京主办的亚太经合组织（APEC）会议的新闻中心，提供的网络服务不过滤任何网站，记者可自由登录Facebook、Twitter、Google、英国广播公司等外国网站，是当局首次在大型国际活动期间全面开放互联网。[69]外交部发言人华春莹在例行记者会上表示："中国互联网是开放的，我们将依法进行管理。如我们承诺过的，有关部门将为峰会圆满举行竭尽全力。媒体中心设施齐全，是专门为高标准提供相关服务而建造，包括互联网服务"。[70]

世界互联网大会

2014年11月，在浙江乌镇举办的第一届世界互联网大会期间，中国电信提供了专用无线网络"iWifi-Wuzhen"，使用该无线网络的嘉宾、记者以至普通游客们都可以正常使用Facebook、Twitter、美国之音、德国之声、自由亚洲电台、BBC中文网等被防火长城封锁的网站。而登记使用"iWifi-Wuzhen"专用无线网络，用户必须在登录页面使用本人的手机号码注册，获取验证码后才可以使用。至于使用普通手机3G、4G数据网络的用户，即使身在乌镇，则仍然受制于防火长城的管制，无法直接使用被屏蔽的网站。[71]

2015年11月第二届世界互联网大会期间，大会组织者向与会者提供了一套特殊的用户名和密码，用此用户名和密码登陆专用无线网络后，同样可以自由浏览境外网站，但如果直接使用当地的互联网络，依然无法浏览这些网站[72]。

2015年加强封锁

自2014年底起，中国官方在网络屏蔽战中逐渐占据上风，大批VPN服务商相继遭到屏蔽[73]，更有甚者提议立法限制VPN服务于大陆网络的注册使用[74]，此举致使民怨沸腾并遭到社会言论指责。《南华早报》报道，在纪念中国人民抗日战争暨世界反法西斯战争胜利70周年大会前夕，多个被用于绕过互联网限制的服务遭到关闭或干扰。[75]

除技术手段外，中国官方通过一系列线下措施，使一些翻墙工具的开发者迫于压力放弃开发，例如2015年1月4日，翻墙软件"枫叶香蕉"开发者许东疑因在网上发布翻墙技术及香港占中消息，被北京西城区警方带走，他的计算机U盘、手机等均被警方取走。警方指控他涉嫌寻衅滋事罪刑拘，关押在北京市第一看守所。同年1月30日获准取保释放[76]。2015年8月下旬，Shadowsocks的作者迫于警方压力[77]删除了自己的项目[78][79]，GoAgent的作者则自行将项目删除[80]。

被美国列为贸易壁垒

美国贸易代表办公室在2016年4月发布的年度特别301报告中称，中国对互联网的审查过滤对外国企业是个严重的贸易障碍。报告中指出，中国在过去一年加紧了对网站的屏蔽，全球25家用户流量最多的网站中有八家被中国屏蔽。

据美联社报道，依赖互联网进行销售、结算以及其它功能的外国和国内企业纷纷抱怨"防火墙"阻碍了公司的运营，以导致部分跨国公司损失严重。

美国商会一月份的调查显示，接受调查的公司中有将近百分之八十的公司表示，他们受到了中国网络屏蔽所带来的"消极影响"。有超过半数的受访企业表示他们在使用网络工具或搜索信息时被屏蔽。很多中国网民也抱怨"防火墙"阻碍了他们与客户或商业伙伴交流以及学生申请海外院校。一些人通过使用虚拟私人网络（VPN）绕开"防火墙"的屏蔽，但现在这些虚拟私人网络也开始遭到北京当局屏蔽，后来在2015年12月前后，GFW突然屏蔽了全部出自国外（不包括ikev2在内）的所有不受控制的VPN连接。

那份年度报告还指出，中国对很多境外网站的屏蔽都显得很武断，有些和社会稳定或国家安全没有关系的网站也被屏蔽，比如美国一家大型家居装饰网站，里面的内容看上去一点都不敏感，但这种却是典型的有可能被防火墙屏蔽的网站。[81]

为此，中国外交部发言人洪磊主持例行记者会，声称：中国互联网蓬勃发展，为各国企业提供了广阔发展空间。中国吸引外资的政策不会变，保护在华外企各方面合法权益的政策不会变，为外企在中国创造良好经营环境的政策也不会变。我们希望各国尊重其他国家自主选择的互联网发展道路、管理模式、公共政策以及参与国际互联网治理的权利。[82]

Steam社区网站被屏蔽

Steam是世界最大的PC数字游戏平台，其社区网站被用于讨论和分享游戏经验。Steam在中国也有着庞大的用户群，根据Steam Spy2017年底的报告，Steam的中国区玩家已经突破3000万[83]，其不受中国监管的社群被认为带来了监管方面的挑战[84][85]。Steam自2015年开启人民币结算以来，曾多次因部分网民在社区发表违反中国法律的内容而遭到屏蔽，在Valve配合删除相关违规言论并封禁违规用户后均解除了屏蔽。但自2017年12月16日起，Steam除了商店，其他功能（社区、市场、库存、创意工坊）均被屏蔽，方法是DNS污染和SNI RST[86]，该屏蔽至今仍未解除，玩家需要使用加速器或在修改hosts的同时使用本地反向代理等工具才能访问，但中国大陆部分地区的用户即使是使用了加速器或本地反向代理，在访问社区的时候仍然会提示“您所在的地区不支持”，原因未知。

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. （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].
4. Great Firewall father speaks out. Global Times. [2011-02-18] （英语）.
5. （英文）Great Firewall of China (https://www.newsmax.com/Pre-2008/The-Great-Firewall-China/2002/05/17/id/666750/)，2008年1月30日新增。
6. （简体中文）百度日本站被GFW屏蔽疑与色情内容有关 (http://media.people.com.cn/GB/40606/5617000.html) 互联网档案馆的存档 (https://web.archive.org/web/20080819043946/http://media.people.com.cn/GB/40606/5617000.html)，存档日期2008-08-19.，人民网（有百度员工指出这是百度自我审查屏蔽内地用户，GFW并没有封锁，详见南方人物周刊：百度搜不到的与索取到的 (http://tech.163.com/08/1203/18/4S8QT3EA000915BF.html)）
7. 李永峰. 网民披露方滨兴是GFW之父国庆前夕中国网络再次收紧. 亚洲周刊. 2009-10-04, **23** (39) [2009-09-25] （中文（繁体））.
8. 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））.
9. http://www.china.org.cn/china/2011-02/18/content_21951602.htm
10. （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]
11. 防火墙给中国互联网哪些影响：成就本土行业崛起. 环球网. 2015-01-28.
12. 那些和“防火长城”一起长大的中国年轻人. 纽约时报中文网. 2018-08-07 [2018-08-30] （中文）.
13. （英文）Asia Pacific Root servers (http://www.apnic.net/community/support/root-servers/root-server-map)，亚太互联网络信息中心
14. DNS污染问题发生后中国根服务器被关. Solidot. 2010-03-28 [2011-02-10].
15. After DNS problem, Chinese root server is shut down. IT World. 2010-03-26 [2011-05-19].
16. Root Server Technical Operations Assn. [2014-01-25].
17. China censorship leaks outside Great Firewall via root server. Ars Technica. 2010-03 [2011-05-19].
18. A Chinese ISP Momentarily Hijacks the Internet. PC World. 2010-04-09 [2011-05-19].
19. 我们的网络为什么这么卡. 2012-11-09 [2012-11-09].
20. 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].
21. 中国网路瘫痪 疑内部作业失误. 自由时报. 2014-01-23 [2014-01-23]. （原始内容存档于2014-01-23）.
22. 防火长城使用有效IP投毒DNS，其中包括色情网站IP. 2015-01-09.
23. 遭DNS投毒DDoS攻击的服务器屏蔽中国IP. 2015-01-23.
24. 翻墙专题：Google掉包问题. RFA. 2011-03-11 [2011-03-21].
25. DAVID BARBOZA; CLAIRE CAIN MILLER. *Google Accuses Chinese of Blocking Gmail Service*. 纽约时报. 2011-03-20.（英文）

26. 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）.
27. China Escalating Attack on Google. 纽约时报. 2014-06-02.（英文）
28. Gmail被中国完全屏蔽. [2014-12-29]. （原始内容存档于2015-01-03）.
29. 社评：中国出于安全考虑“封”Gmail不可信. [2014年12月30日]. （原始内容存档于2015年1月20日）.
30. Github. google.com.hk无法访问，可ping通.
31. 专利号2009100850310，《一种阻断TCP连接的方法和设备》，https://patents.google.com/patent/CN101902440A/zh, 2018-04-24查阅.
32. 防火墙可能采用了更巧妙的方式干扰Google搜索 http://it.solidot.org/article.pl?sid=12/10/31/0510237
33. Github. 一些实验,完成编辑(请仔细阅读说明和说明中给出的链接).
34. 翻墙OK »关于GFW审查eD2k协议的相关内容汇总. [2012-11-29].
35. chengr28. 小盆友的可考证处： （In 2012-11-28）关于eD2k服务遭审查. [2012-11-29].
36. 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.
37. Knock Knock Knockin' on Bridges' Doors. Tor. [2012-01-10].
38. China's Great Firewall Tests Mysterious Scans On Encrypted Connections. [2011-11-17].
39. 中国网警“修理”翻墙网民中科院也被牵连. RFI. 2011-05-18 [2011-05-18].
40. 中国网络国际访问频故障　温水煮蛙测试断外网反应？. RFA. 2011-05-12 [2011-05-18].
41. 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）.
42. 方滨兴教授回应国外网站不能拜访事件. Solidot. 2011-05-18 [2011-05-19].
43. Internet Filtering in China in 2004-2005: A Country Study. Open Net Initiative. [2014-12-31].
44. Special Report: How foreign firms tried to sell spy gear to Iran. Reuters.
45. 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）.
46. 谷歌在中国教育网遭国家级中间人攻击. greatfire.org. 2014年9月4日.
47. 知名网站遭遇SSL中间人攻击 手法很熟业务很忙. 2014年10月21日.
48. （In 2012-11-20）关于近日IPv6隧道被阻断连接. 2012-11-08 [2012-11-08].
49. 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
50. 无耻的GFW，测试GFW工作原理 – MDaemon Server – 邮件服务器-邮件系统-邮件技术论坛（BBS）(http://www.5dmail.net/bbs/thread-167860-1-1.html)，日期为2007年7月6日，有网民在此抱怨GFW的屏蔽
51. （简体中文）万网关于海外邮件通信问题的进展通告 (https://web.archive.org/web/20110510051404/http://www.net.cn/service/a/zytz/200707/2312.html)
52. Gmail blocked in China. Reuters. 2014-12-29.
53. 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.
54. Gmail中国内地服务得以部分恢复.
55. 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]（英语）.
56. 路西. 中国采取新方式 网络封锁扩大到境外. BBC中文网. 2015-04-11 [2015-04-11]（中文（繁体））.
57. 秦雨霏. 中共祭出新武器审查网络 访问陆网或被监控. 大纪元. 2015-04-10 [2015-04-11]（中文（台湾））.
58. GitHub. GitHub System Status.
59. 陈晓莉. GitHub遭遇史上最大规模DDoS攻击，反中国网路防火墙专案被锁定. 台湾iThome. 2015-03-30 [2015-03-30]（中文（台湾））.
60. 海宁. 中共借刀杀人 利用海外华人发起DDoS攻击. 大纪元新闻网. 2015-03-27 [2015-03-30]（中文（简体））.
61. 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].
62. China may relax Internet curbs during the Olympics: official. Google – 法新社. 2008-02-05. （原始内容存档于2008-02-09）（英语）.

63. 胡锦涛接受外国媒体记者采访. BBC. 2008年8月1日 [2008年8月1日]（中文（中国大陆））.
64. 奥运前夕中国解禁国际特赦网站. BBC. 2008年8月1日 [2008年8月1日]（中文（中国大陆））.
65. 外媒指责中国政府未兑现奥运期间网络自由承诺. 齐鲁晚报. [2008-08-31]（中文（简体））.
66. 北京奥组委：外国记者上网不会完全不受限. 联合早报. 2008-07-31. （原始内容存档于2010-02-15）（中文（新加坡））.
67. China 'bans BBC Chinese website'. BBC. 2008年12月16日 [2008年12月16日]（英语）.
68. 中国再屏蔽外国敏感网站引发争议. VOA. 2008年12月17日 [2008年12月17日]（中文（简体））.
69. 中国政府会议期间首度全面开放互联网. 东方报业集团. 2014-11-05 [2014-12-30].
70. 记者手记：从facebook到祷告室 体味自由空间. 文汇报. 2014-11-07 [2014-12-30].
71. 孟航. 中国乌镇互联网大会全面解禁境外网站. BBC中文网. 2014-11-19 [2014-11-19].
72. 乌镇峰会特设上网账户 发小米手机预装大会APP. 南华早报中文网. 2015-12-16 [2015-12-16]. （原始内容存档于2015-12-16）.
73. 中国防火长城再次升级 多数VPN服务失效. UDN. 2015-01-15（中文（台湾））.
74. 中国网络封锁升级大范围屏蔽VPN. 纽约时报中文网. 2015-01-30（中文（中国大陆））.
75. VPN服务受到进一步打击. （原始内容存档于2015-11-08）.
76. 发布占中消息被扣近月IT人许东获释. Radio Free Asia.
77. clowwindy. Adopting iOS 9 network extension points · Issue #124 · shadowsocks/shadowsocks-iOS. GitHub. [2015-08-22]. （原始内容存档于2015-08-22）（英语）. "Two days ago the police came to me and wanted me to stop working on this. Today they asked me to delete all the code from GitHub. I have no choice but to obey."
78. clowwindy. remove · shadowsocks/shadowsocks@938bba3. GitHub. 2015-08-22 [2015-08-22].
79. clowwindy. shadowsocks/shadowsocks. GitHub. 2015-08-22 [2015-08-22].
80. GoAgent开发者删除项目，GitHub再次受到DDoS攻击. Solidot奇客.
81. 美贸易代表办公室：中国网络防火墙是贸易障碍. 美国之音. [2016-04-08].
82. 美国妄称:中国网络防火墙阻碍国际商贸. 搜狐网. [2016-04-09].
83. Steam国区活跃用户突破3000万 玩“吃鸡”的最多 (http://news.zol.com.cn/668/6689734.html).中关村在线. [2017-12-04].
84. Steam 社区网站被屏蔽 (http://www.solidot.org/story?sid=54884).Solidot.[2017-12-17].
85. steamcommunity.com 在中国92%被封锁 (https://zh.greatfire.org/steamcommunity.com).GreatFire.org.
86. Github. steam社区无法打开了，使用hosts也是相同情况 #246.

来源

网页

- Blue的炫影. “连接被重置”. 译言. 2008-03-24 [2008-08-29]（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。根据著作权条款 (http://www.voanews.com/p/5338.html)（英文）和有关美国政府作品著作权的相关法律，其官方发布的内容属于公有领域。

外部链接

- （英文） Chinese bloggers run the gauntlet of forced registration, censorship (http://www.ojr.org/ojr/stories/050621glaser/)
- （英文） Website Test behind the Great Firewall of China (http://www.websitepulse.com/help/testtools.china-test.html), WebSitePulse
- （简体中文） GreatFire.org (https://zh.greatfire.org/)
- （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)

- （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)
- 田路. “网上长城”攻防战. 凤凰周刊, 腾讯新闻. "vingietang" (责任编辑). 2010年12月22日 [2018年4月16日]（中文（中国大陆））.

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

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

- 网络主权
- 和谐社会
- 国家局域网
- 国际离岸云计算数据特别管理区
- 第五权
- 禁止网络盗版法案（SOPA，美国提出类似机制的法案）
- 蜻蜓项目

相关人物

- 方滨兴
