一般来说，一部连上了互联网的电脑都会使用互联网服务供应商提供的域名服务器。这个服务器一般只会服务供应商的客户，通常都会将部分客户曾经请求过的域名暂存起来，这种服务器被称为非权威服务器，其应答称非权威应答。缓存污染攻击就是针对这一种服务器，以影响服务器的使用者或下游服务。

**中国防火长城**[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%BC%93%E5%AD%98%E6%B1%A1%E6%9F%93&action=edit&section=2)]

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](https://zh.wikipedia.org/wiki/%E5%85%A5%E4%BE%B5%E6%A3%80%E6%B5%8B)，一经发现与黑名单关键词相匹配的域名查询请求，会马上伪装成目标域名的解析服务器返回虚假的查询结果。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无连接不可靠的[UDP HYPERLINK "https://zh.wikipedia.org/wiki/UDP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/UDP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/UDP%E5%8D%8F%E8%AE%AE"协议](https://zh.wikipedia.org/wiki/UDP%E5%8D%8F%E8%AE%AE)，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。[[2]](https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%BC%93%E5%AD%98%E6%B1%A1%E6%9F%93)

* 对于不了解相关知识的网民来说，由于系统默认使用的ISP提供的域名查询服务器查询国外的权威服务器时即被防火长城污染，进而使其缓存受到污染，因此默认情况下查询ISP的服务器就会获得虚假IP地址；而用户直接查询境外域名查询服务器（比如 [Google Public DNS](https://zh.wikipedia.org/wiki/Google_Public_DNS)）时有可能会直接被防火长城污染，从而在没有任何防范机制的情况下仍然不能获得目标网站正确的IP地址。[[2]](https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%BC%93%E5%AD%98%E6%B1%A1%E6%9F%93)
* 因为TCP连接的机制可靠，防火长城理论上未对TCP协议下的域名查询进行污染，故现在能透过强制使用TCP协议查询真实的IP地址。而现实的情况是，防火长城对于真实的IP地址也可能会采取其它的手段进行封锁，或者对查询行为使用连接重置的方法进行拦截，故能否真正访问可能还需要其它[翻墙](https://zh.wikipedia.org/wiki/%E7%BF%BB%E5%A2%99)的手段。
* 根据互联网上长期收集到的污染目标的虚假IP地址列表，防火长城会将黑名单内的域名重新导向至不限于以下列表的IP地址：[[3]](https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%BC%93%E5%AD%98%E6%B1%A1%E6%9F%93)

使用 VPN 通常需要先安装客户端软件。当你运行 VPN 客户端，它会尝试联到 VPN 服务器（这点跟加密代理类似）。一旦和 VPN 服务器建立连接，VPN 客户端就会在你的系统中建立了一个虚拟局域网。而且，你的系统中也会多出一个虚拟网卡（在 Windows 下，可以用 ipconfig /all 命令，看到这多出来的网卡）。这样一来，你的系统中就有不止一块网卡。这就引出一个问题：那些访问网络的程序，它的数据流应该通过哪个网卡进出？  
　　为了解决此问题，VPN 客户端通常会修改你系统的**路由表**，让那些数据流，优先从虚拟的网卡进出。由于虚拟的网卡是通往 VPN 服务器的，当数据流到达 VPN 服务器之后，VPN 服务器再帮你把数据流转向到真正的目的地。  
　　前面说了，VPN 为了保证安全，都采用强加密的方式传输数据。这样一来，GFW 就无法分析你的网络数据流，进行敏感词过滤。所以，使用墙外的VPN服务器，无形中就能达到翻墙的效果。

**连接重置**是[TCP HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE"协议](https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE)的一种消息。一般来说，例如[服务器](https://zh.wikipedia.org/wiki/%E6%9C%8D%E5%8A%A1%E5%99%A8)端在没有[客户端](https://zh.wikipedia.org/wiki/%E5%AE%A2%E6%88%B7%E7%AB%AF)请求的[端口](https://zh.wikipedia.org/wiki/%E7%AB%AF%E5%8F%A3)或者其他连接信息不符时，系统的[TCP HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE"协议 HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE" HYPERLINK "https://zh.wikipedia.org/wiki/%E6%A0%88" HYPERLINK "https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE"栈](https://zh.wikipedia.org/wiki/TCP%E5%8D%8F%E8%AE%AE)就会给客户端回复一个RESET通知消息，可见连接重置功能本来用于应对例如服务器意外重启等情况。而发送连接重置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。

中国防火长城的封锁技术[[编辑](https://zh.wikipedia.org/w/index.php?title=%E8%BF%9E%E6%8E%A5%E9%87%8D%E7%BD%AE&action=edit&section=1)]

中华人民共和国在中国内地互联网部署的[防火长城](https://zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E9%95%BF%E5%9F%8E)（GFW）会通过运用伪造“连接重置”技术来作为[互联网审查](https://zh.wikipedia.org/wiki/%E4%BA%92%E8%81%94%E7%BD%91%E5%AE%A1%E6%9F%A5)的封锁措施，当客户端收到伪造的RESET消息时就会断开该连接而不再等待服务器真正的返回信息。而实际上防火长城通过将TCP连接时服务器发回的SYN/ACK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，所以防火长城一般使用此技术对网络数据进行[关键词过滤](https://zh.wikipedia.org/wiki/%E5%85%B3%E9%94%AE%E8%AF%8D%E8%BF%87%E6%BB%A4)。

第一次：

GFW中的主要技术包括国家入口网关的IP封锁、主干路由器的关键字过滤阻断、域名劫持和HTTPS证书过滤等4种

域名劫持：返回错误的ip, 但是可以绕开。比如用这个网站

<http://www.kloth.net/services/nslookup.php> 可以查到google对应的ip为： 216.58.209.68

GFW（great firewall）的几种封锁机制

1.IP封锁 IP封锁是指[防火墙](http://baike.baidu.com/view/3067.htm)维护一张IP黑名单，一旦发现发往黑名单中地址的请求[数据包](http://baike.baidu.com/view/25880.htm)，就直接将其丢弃，这将导致源[主机](http://baike.baidu.com/view/23880.htm)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。

2.dns域名污染

由于一个域名可以对应很多ip地址，仅仅依靠ip地址的封锁是难以阻挡国内人访问某些外国网站，所以应运而生了dns域名污染。原理如下：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。由于默认的dns查询是基于udp协议的，所以防火墙可以轻易的返回错误结果。当然如果使用tcp进行dns查询，是可以防止这种情况的。

但是防火墙还有另一种方法防止这种情况，那就是，tcp协议的连接重置。原理如下：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。

下面通过一个实现来证明

首先我们对[www.facebook.com](http://www.facebook.com/)进行nslookup,查找其对应的ip ,结果如下



从直观上来说，1.2.3.4不可能是facebook的ip,我们在通过用<http://whois.domaintools.com/whois> 查询结果如下



经验证，我们收到了dns的域名污染。

3. **基于关键词内容审查的TCP连接重置**

GFW的内容审查是针对HTTP传输协议的默认80端口的，HTTP传播的内容是明文形式的，没有经过加密。GFW是一个IDS[Intrusion detection system(入侵检测系统)]，持有一个敏感字名单，若在中国大陆访问境外的主机的HTTP的数据流里发现敏感字眼，就在两台主机间伪造一个"reset”信号，导致双方主机以为对方中止了请求。这是我们可以采用基于443端口的https传输协议，因为其是以密文形式传输，可以绕过gfw的内容审查。

**4.SSL证书过滤**

　由于https是加密传输数据的协议，系统无法知道通过https协议传输了什么内容，但又不允许民众使用https访问"有害信息"，除了域名污染和无状态的TCP连接重置防止无法审查内容外，还有SSL证书过滤的审查手段。由于https传输过程中，SSL证书却是明文传输的，所以可以监测SSL证书是否颁发给指定域名的。如果确实如此，那么就强制断开TCP连接，浏览器也会显示"连接被重置"。SSL证书过滤只发生在使用https访问网站的时候。

这次我们来谈一谈翻墙的方法之一

通过修改hosts 文件+https 的翻墙方式。

上回我们介绍了GFW的几种封锁方式，下面我们就修改hosts文件的方法来分析一下它究竟是如何实现翻墙的。

首先，对于IP封锁而言， 由于一个域名对应于很多个IP， 对于GFW而言，谷歌的IP是很难封锁完的，所以我们只要找到那些没有被GFW封锁的IP, 还是可以继续访问谷歌的。那么问题来了，怎么获得没有被墙掉的IP呢？一般是有网页获得的。 当位于国外的可以正常上谷歌的同胞们用谷歌搜索信息并跳转到相关网页上时，网页会记录来源网站（谷歌）的IP信息，经过选择就得到了我们所用的没有被墙掉的IP.我们可以通过ping IP地址的方式来检验IP是否被墙。

其次，对于域名污染/劫持，可以通过hosts文件解决，hosts文件的定义如下：Hosts是一个没有扩展名的系统文件，可以用记事本等工具打开，其作用就是将一些常用的网址[域名](http://baike.baidu.com/view/43.htm" \t "_blank)与其对应的[IP地址](http://baike.baidu.com/view/3930.htm)建立一个关联“数据库”，当用户在浏览器中输入一个需要登录的网址时，系统会首先自动从[Hosts文件](http://baike.baidu.com/view/493742.htm" \t "_blank)中寻找对应的[IP地址](http://baike.baidu.com/view/3930.htm)，一旦找到，系统会立即打开对应网页，如果没有找到，则系统会再将网址提交DNS[域名解析](http://baike.baidu.com/view/30676.htm)服务器进行IP地址的解析。Windows10中，其路径位于C:\WINDOWS\system32\drivers\etc。

最后，对于关键字过滤而言，我们可以通过使用https协议来解决。https协议使用443端口，相对于http而言，在传输过程中使用了加密方式，所以防火墙无法进行关键字的检测。（需要说明的是，https传输需要先获得ssl证书，而获得证书的过程却是非加密的）。

在进行试验的过程中，个人产生了疑惑如下：

157.240.0.17是最新hosts文件里的一个ip,在替换系统hosts之前直接在浏览器输入https://157.240.0.17不能访问网站，是什么原因呢？ 按理说没有经过DNS解析，又使用的是https协议， 效果应该和替换hosts效果一样啊。而且在替换完hosts文件后在这么做就可以了，又是为什么呢？

遗憾的是，这个问题还没有找到答案。

下面再来说一说IPV6 + hosts文件的方式，这种方式在几年前由于ipv6具有速度快，不计流量的特点，曾经风靡一时。但是现在谷歌官方ipv6被墙，国外又很少有用ipv6的人，导致新的IP没有发掘吗，所以已经不再有用。

不过还是想介绍一下怎么使用ipv6

首先看自己是有ipv6, 使用ipconfig命令，由于我使用的是校园网，所以可以获取ipv6

当然ipv4的用户也可以访问ipv6,可以通过在命令行中输入如下指令。

netsh  
netsh>int  
netsh interface ipv6>isatap

netsh interface ipv6> set router isatap.sjtu.edu.cn

netsh interface ipv6>set state enabled

该命令通过isatap隧道技术实现ipv4到ipv6的转换。

Fb:157.240.0.17

Google:61.91.161.217

<http://bgp.he.net/>

test-ipv6.com

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

//上海交通大学DNS服务器：  
//2001:da8:8000:1:202:120:2:100

**C:\>netsh  
  
　　netsh>int  
  
　　netsh interface>IPv6  
  
　　netsh interface>IPv6>install  
  
　　netsh interface IPv6>ISATAP  
  
　　netsh interface IPv6 ISATAP>set router** [www.sjtu.edu.cn](http://www.sjtu.edu.cn)

2404:6800:4008:c02::11 [www.google.com](http://www.google.com)

chrome://net-internals/#quic

服务器密码：jtSHG3NLGGuw

Ssh port 29562

ssserver -c /etc/shadowsocks.json -d start

https://github.com/shadowsocks/shadowsocks/wiki

1080端口：这一协议以[通道方式](http://baike.baidu.com/view/3561891.htm)穿过防火墙，允许防火墙后面的人通过一个IP地址访问INTERNET。