网站怎么被封？科普：上网时背后在发生什么

tutorial, internet, network, firewall, cybersecurity

交大門 (system) 1 August 27, 2023, 12:00am

tl;dr

在Chrome中配置**安全DNS** (DNS over HTTPS) 以解决校园网对 xjtu.men 的DNS污染和DNS劫持（哪怕你设置了使用校外的DNS，依然会给你改成127.0.0.1）问题：

1. 下载安装Chrome，若是Android可直接点击Chrome.apk。

2. 启用安全DNS。PC请在设置中搜索DNS，找到安全DNS设置项，链接：

chrome://settings/security?search=dns

输入的自定安全DNS URL有以下多种选择：

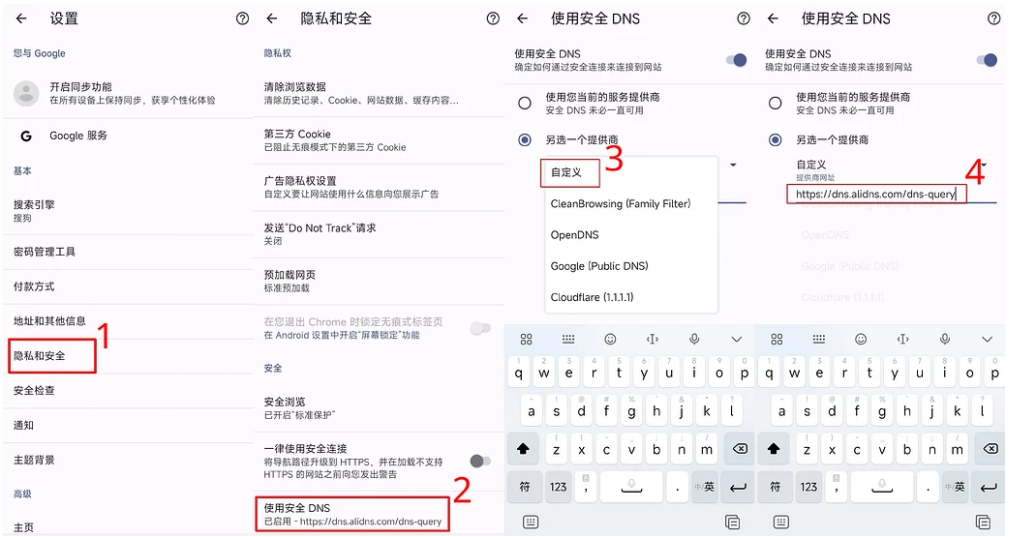
- Tencent DNSPod 安全DNS：

https://1.12.12.12/dns-query

- Ali 安全DNS 的URL为：

https://dns.alidns.com/dns-query

Mobile 操作步骤如下：
隐私与安全 → 使用安全DNS → 另选一个提供商 → 自定义



前情提要

症状描述

> **完了，交大门被校园网ban了？**
>
> 如图，stu校园wifi无法访问，只能4g网络访问。 [图片]

校园网环境下浏览器无法访问本站，而4G网络下可以正常访问。

故障排查

先用ipconfig /all查看网络信息（personal information redacted）：

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   物理地址. . . . . . . . . . . . . :
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2001:250:               (首选)
   获得租约的时间  . . . . . . . . . : 2023年6月
   租约过期的时间  . . . . . . . . . : 2023年6月
   本地链接 IPv6 地址. . . . . . . . : fe80::                      (首选)
   IPv4 地址 . . . . . . . . . . . . : 10.180.       (首选)
   子网掩码  . . . . . . . . . . . . : 255.255.0.0
   获得租约的时间  . . . . . . . . . : 2023年6月
   租约过期的时间  . . . . . . . . . : 2023年6月
   默认网关. . . . . . . . . . . . . : 10.180.0.1
   DHCP 服务器 . . . . . . . . . . . : 10.180.0.1
   DHCPv6 IAID . . . . . . . . . . . :
   DHCPv6 客户端 DUID  . . . . . . . :
   DNS 服务器  . . . . . . . . . . . : 10.6.39.2
                                       10.6.39.3
                                       202.117.0.20
                                       202.117.0.21
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

再nslookup看看这几个校园网自动配置的DNS服务器是否能进行正常域名解析：

```
[root@ubuntu ~]# nslookup xjtu.men 10.6.39.2
Server:         10.6.39.2
Address:        10.6.39.2#53
** server can't find xjtu.men: REFUSED
[root@ubuntu ~]# nslookup xjtu.men 202.117.0.20
Server:         202.117.0.20(陕西省西安市西安交通大学教育网)
Address:        202.117.0.20(陕西省西安市西安交通大学教育网)#53
** server can't find xjtu.men: REFUSED
```

可以看到，服务器拒绝解析xjtu.men。然而此时其他域名的解析正常。

下面来看基于DNS over HTTPS (DoH)的localhost DNS服务器的结果：

```
[root@ubuntu ~]# nslookup xjtu.men 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53
Non-authoritative answer:
Name:   xjtu.men
Address: 104.21.47.144(美国CloudFlare节点)
Name:   xjtu.men
Address: 172.67.171.83(美国CloudFlare节点)
```

Name: xjtu.men
Address: 2606:4700:3030::ac43:ab53(全球 Cloudflare Inc Anycast网段)
Name: xjtu.men
Address: 2606:4700:3036::6815:2f90(全球 Cloudflare Inc Anycast网段)

所以答案很简单，DNS污染。

当你浏览器键入xjtu.men域名的时候后台在发生什么

域名到IP的转换（DNS解析）

- 浏览器会自动把你输入的补全成https://xjtu.men（如果域名在HSTS preload list里，有些浏览器会补全成https://xjtu.men）。
- 做DNS解析，查询域名对应的IP。
  - 对于配置了network.trr.mode=3或2的Firefox，会通过HTTPS进行加密的解析
  - 对于一般的浏览器，会通过操作系统配置的DNS进行解析，如果DNS的IP不在本机，那么查询请求会以明文的形式在网络上传播，中间的任何一个节点都可以窥探并篡改到你查询的域名。
    例如假设你要到8.8.8.8这个DNS服务器上查询：

[root@ubuntu ~]# traceroute 8.8.8.8
traceroute to 8.8.8.8(美国加利福尼亚州圣克拉拉县山景市谷歌公司DNS服务器), 30 hops max, 60 byte
1 <redacted>
2 <redacted>
3 <redacted>
4 <redacted>
5 <redacted>
6 206.72.211.148.any2ix.coresite.com (206.72.211.148(美国加利福尼亚州洛杉矶CoreSite Any2Exchange
7 108.170.247.129(美国加利福尼亚州圣克拉拉县山景市谷歌公司) 10.973 ms 108.170.247.161(美国加
8 108.170.247.161(美国加利福尼亚州圣克拉拉县山景市谷歌公司) 11.043 ms 108.170.247.129(美国加
9 dns.google (8.8.8.8(美国加利福尼亚州圣克拉拉县山景市谷歌公司DNS服务器)) 9.963 ms 10.838 ms

那么从1到9的所有IP上的主机都能看到并篡改这个域名的DNS查询结果，一般是IP。所以在这个环节*污染*正常的DNS解析过程，让你获取不到正确的IP，即可*封网站*。

对于这种最低级的方法，**解决方案**有很多：

- 更换网络环境
- 安装DNS over HTTPS (DoH)软件，例如Cloudflare 1.1.1.1, dnscrypt-proxy。
- 修改电脑的hosts文件，例如：

38.47.117.2 xjtu.men

注意，IP 地址 38.47.117.2 是当前写作时的IP，请用 nslookup / ping 获取最新 IP。
~~如果你有IPv6的话可以加上下面一行~~
~~2604:a880:4:1d0::305:e000 xjtu.men~~

通过传输协议HTTP(S)向位于该IP的(Web)服务器请求内容

0. 首次访问本站时，对于HTTP请求，由于HTTP是不安全的，跟DNS类似，传输路径上的任何主机都看到并篡改你的访问请求和返回的内容，例如这是一个Web服务器的日志：

```
127.0.0.1 - - [05/Jun/2023:20:36:10 +0800] "GET /http/transfer/is/naked HTTP/1.1" 404 385 "" "Mozilla/5.
```

提示你的请求至少泄露了这些信息：

- 你请求的路径/http/transfer/is/naked
- 你的IP：127.0.0.1
- 你的浏览器的User Agent信息：Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36

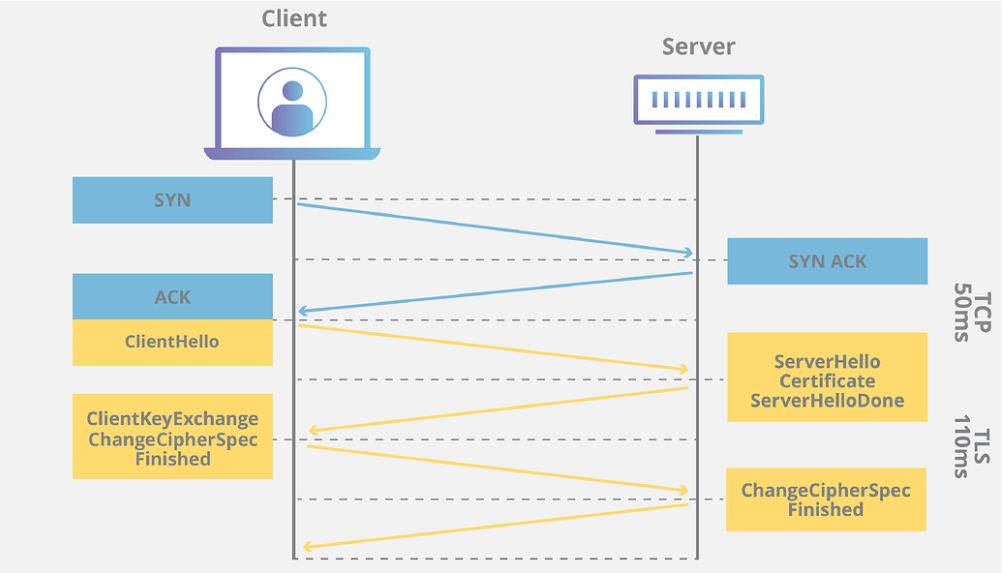
由于HTTP非常不安全，负责地配置的服务器一般会向浏览器回复这样的内容：

```
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://xjtu.men/">here</A>.
</BODY></HTML>
```

提示浏览器改用HTTPS协议。

在这个环节*封网站*也很简单，随便篡改响应头，返回*404*之类的。
解决方案是使用现代浏览器，或者人工输入域名前面的https。

1. 由于本站加入了HTTPS预加载列表， Chrome, Firefox, Safari, Edge 会自动且只能采用HTTPS连接本站，无需上一步的过程且必须验证SSL证书的正确性。
2. 要在服务器和浏览器之间建立端到端加密的HTTPS连接，必须进行TLS握手，需要两者来回发送几次数据，下面是CloudFlare画的一张示意图：



中间的过程涉及公私钥非对称加密的内容，比较复杂，这里只谈怎么在这个环节*封网站*。

TLS握手时，浏览器向服务器发送的客户端Hello包含Server Name Indication (SNI)，这时你要访问的

网站的域名可以被传输路径中途的主机窥探到。
比如你的浏览器地址栏是https://subdomain.xjtu.men/my/little/secret，那么路径中的主机知道你想访问subdomain.xjtu.men这个域名（但是不知道你请求的路径/my/little/secret）。通过TLS的这个缺陷可以*封网站*。

解决方案:
让中间主机无法看到你访问的域名。比如使用**加密/安全SNI**，或者更先进的**加密客户端Hello (ECH)**，或者把你的网络流量包在其他协议里。
可以到**这个网站**测试你的浏览器支持哪些安全功能。

在TLS握手的过程中，网站会发送证明身份的证书给浏览器，TLS1.2协议不加密证书，而证书会泄露域名信息，**解决方案**是：采取激进的TLS设置，只使用TLS1.3，不支持TLS1.2。

另外，如果传输路径上有干扰，把服务器返回的流量给篡改了，比如返回的证书的CA不受信任，或者域名不是你请求访问的域名，$ \ldots\ldots $，那么也会失败，通过这个也可以封网站。解决方案只有*把你的网络流量包在其他协议里*。

3. 在TLS握手成功后，进行HTTPS流量传输，这时候中间路径上的主机只能看到你和远方的服务器之间传输加密流量，可知的只有你们双方的IP和端口号。
   要*封网站*，只需中间路径上的主机把数据包全给扔掉。
   可以选择性封锁，常见的比如封锁某些IP到你的所有流量，或者某些端口，或者某些协议如UDP的流量。

解决方法:

- 对于服务器：使用大公司的CDN服务，即：要么不封IP，只要封就把这个CDN服务商的所有IP给封了。
- *把你的网络流量包在其他协议里*。

11 Likes

最近看点什么书

主域名将变回xjtu.men

真心希望这个网站能做起来

饮水思源型无主题灌水楼精勤求学版1.0

Android App客户端

Android App客户端

校园网wifi无法打开本站，疑似被DNS污染