GFW: Protection or censorship?

A brief overview on China's Great Firewall system

Hengyi Li

January 21, 2024

I Introduction

The Internet has come a long way today. As a bridge for the flow of information, it carries the thoughts, ideas, opinions and needs of all people. However, because of the value attributes of information, the flow of information may inadvertently touch the interests of certain people or groups. This may lead to theft by criminals, or it may be a threat to national security, but in any case, the network firewall has been built as a result. In China, there also exists such a wall, which is not only able to defend against cyber-attacks from outside the country, but at the same time, and most importantly, prevents the flow of network traffic from within the country to outside the country. This is the subject of this article - The Great Firewall.

II Background

Great Firewall (hereinafter referred to as GFW) is a traffic censorship and attack defense system based on Cisco's intrusion detection system [5]. This defense system combines active and passive detection capabilities to censor China's Internet traffic [1]. As far as we know from our testing, the system is running on IPV4, but we have no way of knowing if the system is compatible with IPV6 as well. The main reason for this is that IPV6 is not very popular in China, and even if we could ask the carriers to enable it, they would not be very willing to do so for security reasons, and it would require a series of very complicated procedures to complete.

What's worse, the GFW is still a black box system for outsiders and researchers, and the existence of the system is not recognized at the national level, and there is no official documentation about the system. All research into the system is currently in the "poke around and see what happend" phase, so most of the results and findings below come from community organizations and web forum members. We would like to thank the members and contributors of the gfw. repot [3] website for providing a wealth of documentation and experimental data without which we would not have been able to gain such a deep understanding of GFW. In order to begin to understand how the GFW network in China works, we need to first understand the composition of the network structure in China, which has a huge difference with here in the U.S.

Now, China's Internet is divided into two parts, the national intranet and the international network. Since 2013, China's internet technology companies have grown and expanded into a wide range of industries, creating an ecosystem of apps for every need and an internal loop. For example, we have Bilibili, which is the Chinese version of Youtube. We have Baidu, which is the Chinese version of Google We have Weibo to replace the Twitter, we have WeChat to replace the Facebook and

WhatsApp and the alternate to Apple Pay/Google Pay and a series of other payment tools in China is Alipay and WeChat Pay. Every application you know, we have a alternative version and it's optimized just for Chinese market. Everything we need is in the intranet, so most of people choose to live in a environment like this. But what it brings is the information cocoon. Because the Chinese language is so special, learning English can be much more difficult for Chinese people than it is for Americans learning Spanish. The rising cost of learning means that most people won't bother to learn the language, and thus the breadth of the information stream they receive on a daily basis will become narrower and narrower. Unfortunately, because of the speciality of the Chinese language and its strong historical and cultural ties, the Chinese language media is mostly limited to the territory of China and the GFW exacerbates this situation by making it more difficult to access foreign media.

That's not what we want, and it's not what we want to see the Internet will become. Information should flow freely, and anyone should be able to access as much information as they want without compromising national security. Communication between people should not be hindered by the advent of technology, and unfortunately, GFW is one of the technologies that builds barriers. It didn't come about by accident, but because of a combination of historical legacies and improvisational decisions. For the sake of safety, we will only discuss its technical aspects here, and we would start by discussing the network architecture legacy.

III China's internet architecture

Because of the limited number of IPv4 addresses and China's large population base, China is facing the problem of running out of IPv4 addresses earlier than other countries in the world. At that time, IPv6 protocol had not yet been proposed. As a response, the three major carriers in China coincidentally chose carrier-grade NAT when setting up their networks, which effectively reduced the use of public IPv4 addresses by converting a large number of private IPv4 addresses into a small number of public IPv4 addresses [2].

Therefore, the Chinese network architecture now becomes based on NAT technology. Normal people will not have a public IP address, but all private IP addresses provided by ISPs, and, because China's Internet, cell phone and TV services are monopolized by three state-owned companies, China Mobile, China Telecom and China Unicom. The network architecture has become an onion-like NAT bridging model. Because of this bridging model, network providers can isolate intranet access requests from international access requests very easily. In order to meet the demand for international access, China has set up international line servers in three major cities, Beijing, Shanghai and Guangzhou, and deployed GFWs on them, which can be interpreted as network outbound customs, so that all outbound traffic must pass through the servers in one of the three cities and go through the GFWs' scrutinizing process before going out of the country [6].

Let's simulate a situation for better understanding. Suppose we have a laptop in Chengdu trying to access the ucdavis.edu website, then the request will go through the following process

$$\begin{aligned} &\textit{Laptop} \rightarrow \text{Home Router} \rightarrow \text{Community Server} \rightarrow \text{Distinct Server} \\ &\rightarrow \text{City Datacenter} \rightarrow \text{Province Datacenter} \rightarrow \text{Guangzhou Datacenter} \\ &\rightarrow \text{GFW server} \rightarrow \text{UCDavis server} \end{aligned}$$

As you can see, it takes a long way from Chengdu to connect to the server at UCDavis. At the same time, keep in mind that each hop is accomplished by IP conversion through NAT layer by

layer. And in the final pass through the GFW is also like going through customs, the GFW will review the legal compliance of the destination address, and whether it is on the blacklist. If the address is on GFW's blacklist (e.g. Youtube.com), GFW will reject the connection and send a reset request to both parties or wait until the connection times out. I'll discuss GFW's blocking patterns further in the next section.

IV GFW's Working Principle

The core function of GFW is to block traffic. As a carrier-grade firewall, it mainly uses DNS hijacking and connection reset to prevent users from accessing websites on the banned list. Due to the differences between HTTP and HTTPS, GFW handles these two types of requests differently.

For the HTTP protocol, since the data was being transferred in clear text [4]., which meansthe GFW could just be a middle man and look into the data being transferred, compare it with the black list and see if any of them matched. For the https request, the blacklist change from the keywords to the destination IP address, it works as the same, look into the header to find if the destination IP was on the list, if it founds a match, blocking performed.

Now, there has two types of blocking that the GFW usually used: connection reset and the connection timeout. The connection reset was to send the destination and sender both a connection reset request to end the connection, and the connection timeout, which was the most common one, was to using DNS hijacking to rediect the destination site to some other place that does not exist at all, caused a connection time out error message on the sender side.

IV.I Experiment 1: http connect situation

In this test, we will use a host machine located in Chengdu, Sichuan Province, China to trying to connect to a site using http protocol and it's banned in China. Here is what we found:

todo: Insert results here

IV.II Experiment 2: https connect situation

In this test, we will use a host machine located in Chengdu, Sichuan Province, China to trying to connect to Youtube.com, googl.com and facebook.com. All of those websites were using https protocol to establish the connection and here is our results:

todo: insert results here

V Solutions to bypass the GFW

The most direct way to solve the problem of GFW blocking is to use a VPN for proxy services, but this is a legal risk in China. According to China's "Interim Provisions on the Administration of International Networking of Computer Information Networks": Computer information networks directly for international networking, must use the Ministry of Posts and Telecommunications, the national public telecommunication network to provide the international entrance and exit channels. No unit or individual may establish or use any other channel for international networking, and in case of violation, the public security authorities shall order the cessation of networking, give a warning, and may impose a fine of not more than 15,000 yuan; if there is any illegal income, the illegal income shall be confiscated [7].

There is already a precedent for such behavior in the form of judgments. In 2023, a programmer in Chengde, Hebei province, was convicted of confiscating illegal proceeds for using a VPN to connect to Github for an open source project [8].

Of course, there are legal ways around this policy, and this is the solution for most companies in China that require offshore connectivity - purchase a dedicated line for offshore connectivity from a carrier, and this line is subject to scrutiny by both the carrier and the government. This way the traffic out of the country is legal. For individuals, however, this solution is very expensive and bandwidth is limited. So most of the individuals who go over the wall do so by going through a gray area — VPS for traffic proxy. At present, China does not have explicit legal provisions VPS can not be used in China, so the practice of many people is to set up a VPS proxy server in Hong Kong, China, through which the proxy for access to foreign websites. But one thing to remember is that, because this is an activity in the gray area, so all the behavior may become illegal evidence in the future and be punished, so there is a certain risk.

Another method can also be used to bypass GFW, but it only works for DNS hijacking. That is to bypass the DNS service of the operator by modifying the hosts file in the local machine to connect to the external network. Here is an experiment to show how this can be accomplished

V.I Experiment 3. DNS Hijacking bypass

todo: fill the experimence here.

VI Conclusion

The current architecture of GFW is not as complex as we think. Its cyber-binding effect on citizens comes mainly from the laws and the tedious steps required to bypass this firewall. In the beginning, GFW existed as a politically correct vetting mechanism, but now in today's China, due to the language and the emergence of better, localized alternatives, Chinese people don't need platforms like Twitter, Facebook, etc to get information, and due to the boom of homegrown software, young Chinese people nowadays probably don't know what's going on in the internet. "GFW's influence in China is diminishing as the new generation of Chinese domestic software companies grows, and it will probably be completely forgotten in the near future.

References

[1] Anonymous, et al. *"How China Detects and Blocks Shadowsocks."* GFW Report, 29 Dec. 2019, gfw. report/blog/gfw_shadowsocks. Accessed 11 Jan. 2024.

[2] Cisco.com. "Carrier Grade Network Address Translation." *Information About Carrier Grade Network Address Translation*, www.cisco.com/c/en/us/td/docs/routers en/us/td/docs/routers/ios/config/17-x/ip-addressing/b-ip-addressing/m_iadnat-cgn.pdf. Accessed 11 Jan. 2024

[3] Great Firewall Report. *"Great Firewall Report."* Great Firewall Repor, Dec. 2019, gfw.report. Accessed 11 Jan. 2024.

[4] Hoochanlon. *"Fq-book/Docs/Abc/gfw.md at Master · Hoochanlon/Fq-book."* GitHub, 13 Apr. 2020, github.com/hoochanlon/fq-book/blob/master/docs/abc/gfw.md. Accessed 14 Jan. 2024.

[5] Schaack, Beth Van. *"China's Golden Shield: Is Cisco Systems Complicit?"* Center for Internet and Society, 24 Mar. 2015, cyberlaw.stanford.edu/blog/2015/03/china%E2%80%99s-golden-shield-cisco-systems-complicit. Accessed 11 Jan. 2024.

[6] 聿纾. "国内主流网络运营商国际连接线路简谈." 知乎专栏, zhuanlan.zhihu.com/p/64467370.

[7] 中华人民共和国国务院. "中华人民共和国计算机信息网络国际联网管理暂行规定." 中央网信办, 20 May 1997, www.12377. cn/xzfg/2020/7f441527_web.html. Accessed 21 Jan. 2024.

[8] 承德市公安局双桥分局. 承德市公安局双桥分局行政处罚决定书. Sunshine Police Law Enforcement Inquiry System, 18 Aug. 2023, 111.63.208.144/laws/web/infoqueryxzcf/xzcf/detail/0380da828a06bd69018a07d2be7c530c/1. Accessed 21 Jan. 2024.