GFW: Protection or censorship?

A brief overview on China's Great Firewall system

Hengyi Li

January 11, 2024

1 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.

2 Background

Great Firewall (hereinafter referred to as GFW) is a traffic censorship and attack defense system based on Cisco's intrusion detection system [3]. 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 [2] 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.

3 China's internet architecture

In China, the Internet architecture consists of layers and layers of NATs, and most people do not have public IPs. there are only three Internet Service Providers (ISPs) in China, China Mobile,

China Unicom and China Telecom, all of which are state-owned enterprises. All three are state-owned enterprises. All three companies are state-owned and have a monopoly on the supply of cell phones, TV, and Internet services in China. The reason for these three providers to use Carrier Grade NAT is that China has too many network devices, and IPV4 addresses are limited, coupled with a large population base, which makes China face the problem of insufficient IPV4 addresses earlier than other countries in the world. The use of carrier grade NAT can be a very convenient solution to this problem and also brings more convenient network device management mechanism.

Now, China's Internet is divided into two parts, the national intranet and the international network. Since 2013, China's Internet companies have had a very significant development, the people's daily life can be satisfied with everything, at the same time, the application of international social media platforms China's Internet companies have also launched its replacement products. For example, the Chinese version of Youtube is Bilibili, the Chinese version of Google is Baidu, the Chinese version of Twitter is Weibo, the alternate to Facebook and WhatsApp is WeChat, and the alternate to Apple Pay/Google Pay and a series of other payment tools in China is Alipay and WeChat Pay. It can be said that there is a Chinese app for all the daily needs of the Chinese people, which makes most of the people's online activities only within the Chinese intranet. Without demand, there is no supply, and the concept of the "Internet wall" is becoming less and less relevant to the new generation of Chinese.

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

[3] 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.