Navigating the Great Firewall: A Deep Dive into Chinese Cybersecurity

Through its sophisticated censorship technology, ‘China is able to control such a vast ocean of content through the largest system of censorship in the world’ (Bloomberg. 2018. para.1). This paper discusses the key aspects of the Golden Shield Project.

Aptly known as The Great Firewall of China’, the nationwide censorship and content filtering framework aims to remove ‘undue foreign influence’ on Chinese political, cultural, and ideological policies. The system is administered by the People’s Republic of China.

According to a Stanford report, it the Firewall was described as the ‘most sophisticated internet censorship program’ (Standford. 2011. para.7). The sensor system is implemented primarily for politics, such as curtailing political discourse and censoring events that reflect poorly on the Chinese Community Pary.

Moreover, cross-border internet traffic is slowed down. By sabotaging foreign services, it coerces Chinese citizens to utilize mostly domestic services. Furthermore, it pushes foreign entities to adopt Chinese systems to maintain consumers. Although, this influence likely yields a net positive output to the Chinese economy.

Equally important are popular websites blocked; these include Google, Youtube, Facebook, Wikipedia, Reddit, Netflix, Zoom, Bing, Instagram, Twitch, and Skype Discord. Categories include search engines, social media, music streaming, file sharing, entertainment, and news.

We can obtain statistics about the Great Firewall through GFWatch Dashboard - a measurement platform for the Firewall. From March 2020 the GFWatch reports 265,801 domains were blocked. The primary categories of censored domains are, respectively: new domains, pornographic websites, business, IT information, proxy avoidance domains, personal blogs, entertainment, search engine, and ports, and gambling.

It is possible to view the censorship by using a popular Chinese search engine, Baidu (baidu.com). We can ascertain a clear understanding by using a popular search engine such as Google and comparing its results to its Chinese counterpart.

The censorship system digs deep into citizen’s network packers to identify keywords to find and block. However, Researchers from the University of California at David and the University of New Mexico discovered that the Firewall operates sporadically and much of the censorship is due to self-censorship because citizens are aware their actions are being monitored. This may be due to the inherently difficult task of regulating online content.

The Chinese administration employs a wide range of passive and active filtering functions to regulate connections.

The Firewall maintains a collection of IP addresses that are blacklisted. However, this method is considered a last line of defence, as dynamic IP addresses make it maintain a status list of blocked addresses.

DNS poisoning is another attack. The Firewall maintains a large collection of falsified IP addresses. This means, that if someone attempts to access Facebook.com, the Firewall will provide an incorrect IP address. However, this attack vector can be circumnavigated by simply typing the IP address of the domain. Moreover, encrypted DNS replies are manipulated by the Firewall.

A more sophisticated is Quality of service (Qos) filtering. This method forwards traffic to a Chinese administration branch to analyze the traffic. The packets are then given a score, based on their level of suspiciousness. Low scores then create packet loss which makes effectively stops people from accessing the domain.

Other known methods include Man in the Middle attacks. Furthermore, URL filtering attacks block domains that contain certain sensitive keywords and phrases.

Equally important is the TCP reset attacks used by the Firewall. Also known as SYN flood attack, the packet tampering technique exploits the TCP/IP protocol. We must first understand that in an established connection, each TCP packet contains a header such as the RST flag. Therefore, the Firewall will interrupt the normal communication between a server and a client by sending forged RST packets. The RST packet disrupts the normal ‘conversation’ between the server and the client. This ultimately terminates or slows the communication, which may stop someone from using a website altogether.

Online research indicates there are several methods to bypass the Great Firewall of China. These include using proxy servers, using Virtual Private Networks, and using Tor although it is partially blocked.

As suggested by the name, a ‘proxy’ is an intermediary between the computer and the server; it acts as a representative. In the context of a client to server communication, the server thinks it is communicating with the client. However, the client is represented by the proxy, who is in a different location to the client. Therefore, the client is logically isolated from the proxy server. The process of communication is: the client sends the proxy server a message. Therefore, the identity of the client is disguised.

However, the most popular method of circumvention China’s Internet censorship is by using Virtual Private Networks. Furthermore, VPN traffic may be encrypted, which further obsfucates internet traffic. A VPN works by directing network traffic through a remote server run by a VPN host. We can think of this concept as a virtual tunnel because the VPN server encrypts network traffic.

Despite these efforts, the Chinese Administration continues to crack down on VPN services in China. As noted earlier, many the Firewall blocks proxy avoidance domains, which makes it difficult for people to obtain the actual VPN software. The Chinese government is able to block traffic that appears to be in communication with virtual private network servers. However, some VPNs still work.

Tor is another program that can circumvent the censorship, however ‘nce having had 30,000 users solely from China, the Tor network now is largely inaccessible from within China’s’ (R Esafi. 2015. pg.1)

‘Despite its decreasing prevalence in China, Tor is a program that can be used to circumvent censorship. The Tor system encrypts its packets in multiple layers of encryption to protect its connection. Each layer in the Tor system has instructions for routing to the next place until the packet has arrived at its final destination. The system was originally developed by the U.S navy.

References

GFWatch. 2021. ‘GFWatch Dashboard’ https://gfwatch.org/

Roya Ensaf. 2015. ‘Analyzing the Great Firewall of China Over Space and Time’ https://censoredplanet.org/assets/Ensafi2015a.pdf Accessed 12 April 2022

Bloomberg. 2015. ‘Great Firewall of China’ https://www.bloomberg.com/quicktake/great-firewall-of-china Accessed 12 April 2022

Stanford Projects. 2011. The Great Firewall of China: Background https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the -great-firewall-of-china-background/index.html Accessed 12 April 2022

James Griffiths. 2019. ‘Great wall of China’ https://books.google.com.au/books?hl=en&lr=&id=n_1AEAAAQBAJ&oi=fnd&pg=PP1&dq=great+firewall+of+china&ots=AxwfzAAU6B&sig=AaZ7Uwbdco-6XaUo0vqdADnvBnA#v=onepage&q=great%20firewall%20of%20china&f=false Accessed 14 April 2022

Geeks for Geeks. 2019. ‘TCP handshake’ https://www.geeksforgeeks.org/tcp-3-way-handshake-process/ Accessed 14 April 2022