# In-depth analysis of the Great Firewall of China

Chao Tang
December 14, 2016

Special thanks to Martin Johnson, Charlie Smith from GreatFire and Ming Chow for all the help they have provided.

# Abstract

Created by the Golden Shield Project, the Great Firewall of China (GFW) is the backbone of world's largest system of censorship. As an on-path system, the GFW can monitor traffic and inject additional packets, but cannot stop in-flight packets from reaching its destination. It achieves censorship using three main techniques: First, it inspects all Internet traffic between China and the rest of the world, then terminate connections containing censored content by injecting forged TCP Reset packets to both ends. With the advent of HTTPS, which cannot be decrypted by the GFW, TCP RST has seen fewer use in recent years. Second, the GFW blocks access to specific IP addresses through the gateway routers of all Chinese ISPs. Third, it uses DNS tampering to return false IP addresses in response to DNS queries to blocked domains. This affects queries to both domestic and foreign DNS services. IP blocking and DNS tampering together are the bread and butter of GFW, effectively cutting off all access to blocked websites. But, such draconian methods inevitably cause over-censoring and collateral damage to international web traffic flowing through China and innocent websites. The three main ways a user can bypass the GFW are the use of VPNs, Proxies, and Tor. However, GFW can use deep packet inspection and machine learning to shutdown suspected VPN or proxy tunnels, and use an active probing system to shutdown Tor bridge relays. As of today, few commercial VPN services and the latest Tor protocols using Pluggable Transports are viable approaches.


# INTRODUCTION

In China, the first recorded connection to the global was an email sent to Karlsruher Institut für Technologie in Germany on September 14, 1987. Ironically, the message said "Across the Great Wall, we can reach every corner in the world."[i] True Internet came to China in 1994, as an extension of the "Open Door policy" that opened the country to the Western world. In the following years, as more and more citizens adopted the Internet, the Chinese government found themselves losing control over the spread and availability of information. "Determined to control online content and its citizens with regards to the kinds of information

to which they have accessed. MPS, the branch of the government that deals with this issue, immediately took action by launching the Golden Shield Project."[ii]

Golden Shield Project officially made its debut in 2000, and has been constantly evolving since. "The government initially envisioned the Golden Shield Project to be a comprehensive database-driven surveillance system that could access every citizen's record as well as link national, regional, and local security together."[2] However, the rapid expansion of Internet in China rendered this goal infeasible, and the project pivoted from "generalized content control at the gateway level to individual surveillance of users at the edge of the network."[2] It was this ideology that made the GFW what it is today.

On March 16th, 2015, the Chinese censorship apparatus unveiled a new tool, dubbed the "Great Canon", to the rest of the world. It made its grand entrance by engineering a denial-of-service attack on GreatFire.org, an organization dedicated to collecting data about GFW and sharing it with rest of the world. For the days that followed, GreatFire servers received up to 2.6 billion requests per hour, 2500 more than their normal load. After further research, it was determined that the GC is a separate but related in-path system with the ability to interfere with traffic directly through injection, redirection, and suppression. Since its debut, it has been used to DDOS multiple websites with great success.

## To the community

China has 721,434,547 internet users[iii], most out of any country in the world and 3 times the number in the US. The world must consider the implication of having such a large number of people living under a heavily censored and monitored Internet. Without delving into politics, it is undeniable to say that the relative stability the Chinese Communist Party has enjoyed is due in no small part to the effectiveness of the GFW. All major global social media websites, most of Google's services, any websites with information about civil unrests past and present are only a short list of websites that are blocked by the GFW. Hundreds of thousands of foreign companies operating in China also must operate under the constraints of the GFW and GC, with some altering its business practices to comply with the restrictions imposed, and others constantly finding new ways to circumvent them. Finally, seeing the success of large scale Internet

censorship program in China, other countries such as Cuba, Zimbabwe, and Belarus are considering adopting similar programs.[iv] Thus, computer science students today must keep the capabilities and limitations of the GFW and GC in mind when developing products for the future.

# Great Firewall

## Overview

The name Great Firewall is a misnomer, as traditional firewalls are in-path barriers that control traffic flowing between networks. The GFW is an on-path system, meaning it can passively read all traffic between China and the rest of the world and inject additional packets, but it cannot drop packets already in-flight. Compared to in-path systems, on-path systems are less disruptive and do not dramatically slow down all traffic passing through the network.[v] On the other hand, they are less flexible because they cannot interfere with existing traffic. As a result, they are also less stealthy. One can generally detect when traffic has been altered by the GFW by observing anomalous injected packets using server logs and packet analyzers.

The GFW has three main weapons it employs for censorship: TCP Reset, IP address blocking, and DNS poisoning. They will be individually examined below.

## TCP Reset

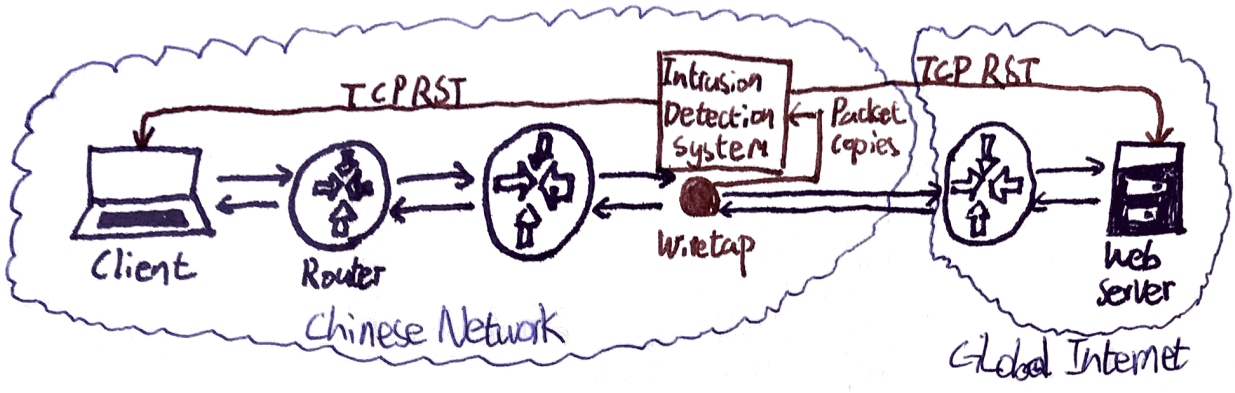
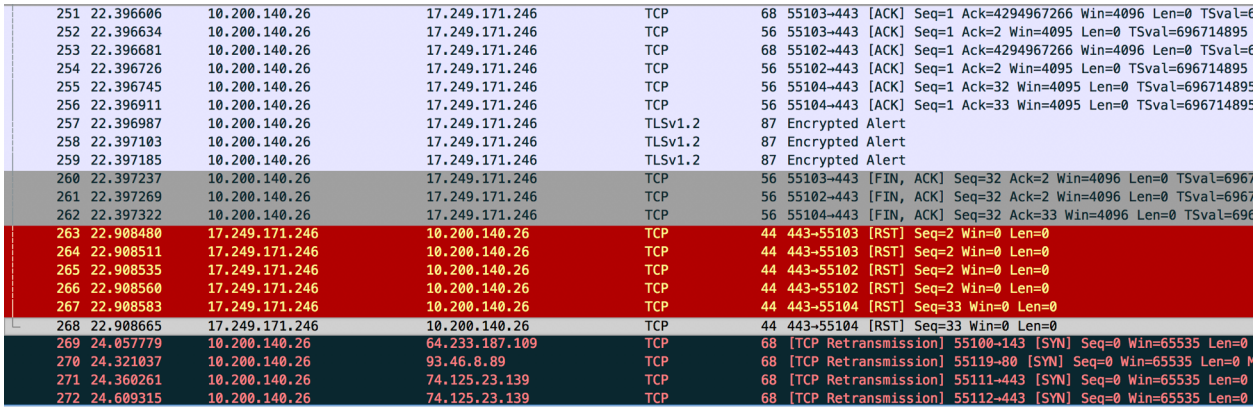



*Figure-1: An illustration of TCP Reset*

Once the crème de la crème of GFW, TCP reset is a direct answer to the limitations of an -path architecture. "Most content inspection schemes work by passing all traffic through a proxy that refuses to serve results for forbidden material. However, a proxy-based system that can cope with the traffic volumes of a major network, or an entire country, would be extremely expensive and difficult to scale."[vi] Instead, the GFW inspects traffic by passing copies to out-of-band devices based on Intrusion Detection Systems.[vii] The original packets are unaffected, while the IDS inspects the content of the packet and the requested URL, matching them against a blacklist of keywords. Since late 2008, only the first HTTP GET request after a TCP handshake is inspected, improving the efficiency of the system without losing too much accuracy.[viii] More impressively, the GFW is now capable of both IP fragments and TCP segments reassembly while maintaining state.[ix] Before this feature was introduced, the inability to reassemble segments was considered a major flaw in the system, and simply breaking down packets was an effective way of by-passing the system.

Once the IDS detects blacklisted keywords, the GFW router injects multiple forged TCP RST packets to both endpoints, forcing the connection to be dropped. Multiple packets with different ACK numbers guarantees that the connection is blocked even if the original packet reaches its destination before the RST. The GFW then maintains the flow state regarding source and destination IP addresses, port number and protocol of denied request to block all further communications for up to hours at a time.



| | | | | | |
|---|---|---|---|---|---|
| 251 | 22.396606 | 10.200.140.26 | 17.249.171.246 | TCP | 68 55103→443 [ACK] Seq=1 Ack=4294967266 Win=4096 Len=0 TSval= |
| 252 | 22.396634 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55103→443 [ACK] Seq=1 Ack=2 Win=4095 Len=0 TSval=696714895 |
| 253 | 22.396681 | 10.200.140.26 | 17.249.171.246 | TCP | 68 55102→443 [ACK] Seq=1 Ack=4294967266 Win=4096 Len=0 TSval= |
| 254 | 22.396726 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55102→443 [ACK] Seq=1 Ack=2 Win=4095 Len=0 TSval=696714895 |
| 255 | 22.396745 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55104→443 [ACK] Seq=1 Ack=32 Win=4095 Len=0 TSval=696714895 |
| 256 | 22.396911 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55104→443 [ACK] Seq=1 Ack=33 Win=4095 Len=0 TSval=696714895 |
| 257 | 22.396987 | 10.200.140.26 | 17.249.171.246 | TLSv1.2 | 87 Encrypted Alert |
| 258 | 22.397103 | 10.200.140.26 | 17.249.171.246 | TLSv1.2 | 87 Encrypted Alert |
| 259 | 22.397185 | 10.200.140.26 | 17.249.171.246 | TLSv1.2 | 87 Encrypted Alert |
| 260 | 22.397237 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55103→443 [FIN, ACK] Seq=32 Ack=2 Win=4096 Len=0 TSval=6967 |
| 261 | 22.397269 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55102→443 [FIN, ACK] Seq=32 Ack=2 Win=4096 Len=0 TSval=6967 |
| 262 | 22.397322 | 10.200.140.26 | 17.249.171.246 | TCP | 56 55104→443 [FIN, ACK] Seq=32 Ack=33 Win=4096 Len=0 TSval=696 |
| 263 | 22.908480 | 17.249.171.246 | 10.200.140.26 | TCP | 44 443→55103 [RST] Seq=2 Win=0 Len=0 |
| 264 | 22.908511 | 17.249.171.246 | 10.200.140.26 | TCP | 44 443→55103 [RST] Seq=2 Win=0 Len=0 |
| 265 | 22.908535 | 17.249.171.246 | 10.200.140.26 | TCP | 44 443→55102 [RST] Seq=2 Win=0 Len=0 |
| 266 | 22.908560 | 17.249.171.246 | 10.200.140.26 | TCP | 44 443→55102 [RST] Seq=2 Win=0 Len=0 |
| 267 | 22.908583 | 17.249.171.246 | 10.200.140.26 | TCP | 44 443→55104 [RST] Seq=33 Win=0 Len=0 |
| 268 | 22.908665 | 17.249.171.246 | 10.200.140.26 | TCP | 44 443→55104 [RST] Seq=33 Win=0 Len=0 |
| 269 | 24.057779 | 10.200.140.26 | 64.233.187.109 | TCP | 68 [TCP Retransmission] 55100→143 [SYN] Seq=0 Win=65535 Len=0 |
| 270 | 24.321037 | 10.200.140.26 | 93.46.8.89 | TCP | 68 [TCP Retransmission] 55119→80 [SYN] Seq=0 Win=65535 Len=0 M |
| 271 | 24.360261 | 10.200.140.26 | 74.125.23.139 | TCP | 68 [TCP Retransmission] 55111→443 [SYN] Seq=0 Win=65535 Len=0 |
| 272 | 24.609315 | 10.200.140.26 | 74.125.23.139 | TCP | 68 [TCP Retransmission] 55112→443 [SYN] Seq=0 Win=65535 Len=0 |

*Figure-2: This is a screenshot taken from Wireshark when the author attempted to trigger TCP RST using a VPN. While connected to a VPN server in Shenzhen, the author used Yahoo to search for the censored string "falun". Although the search returned results, the author was unable to connect to most websites from the results page. The TCP Retransmission shown above is evidence of the failure to connect. The author initially thought the five TCP RST packets in red were the doings of GFW. However, the ACK number of the packets were all 0, which is uncharacteristic of forged TCP RST packets. Thus, although it was a valiant attempt, it is unlikely that GFW was at play here.*

After numerous other attempts at triggering TCP RST without conclusive evidence, the author reached out to GreatFire for advice. Martin Johnson sent back the following response: "Keyword resets matter much less now with most big websites using HTTPS and so many major ones being blocked wholesale anyway. I just tested a couple of sensitive keywords and the connection was not reset, so perhaps the GFW is using it much less now than it used to." HTTPS encrypts all packets in transit, thus the GFW IDS has no way of inspecting HTTPS traffic, rendering TCP RST useless. In addition, creating rules on both endpoints to ignore TCP RST packets can also completely bypass TCP RST. These crippling weaknesses have led to the demise of TCP RST in recent years.

## IP Address Blocking

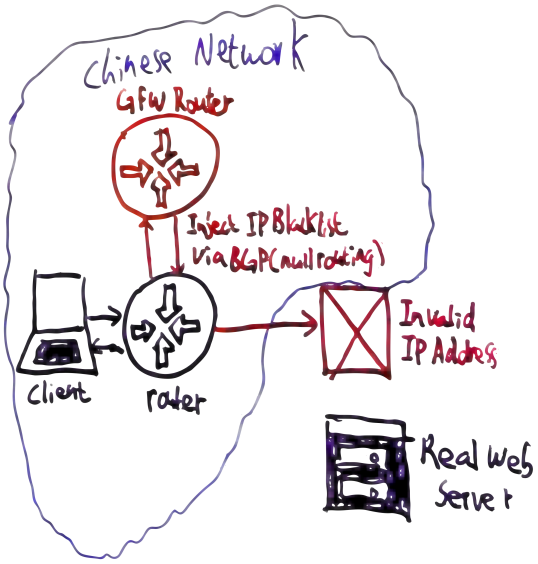
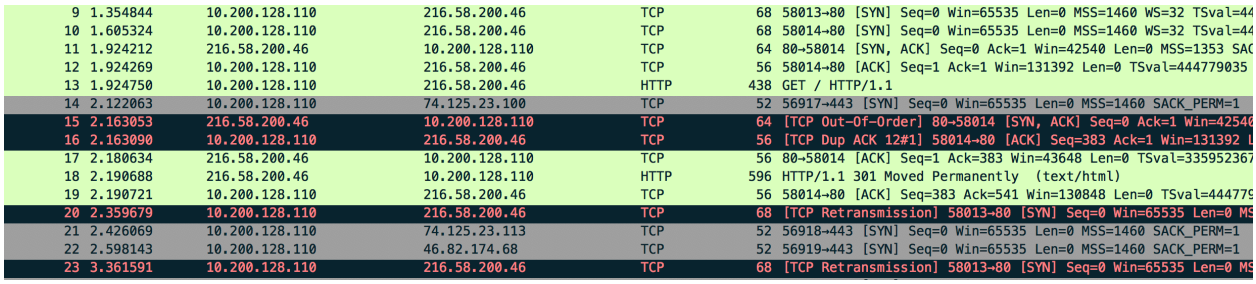



*Figure-3: An illustration of IP Address Blocking.*

IP address blocking is a simple, lightweight, yet extremely effective censorship tool. "By peering with the gateway routers of all Chinese ISPs, GFW injects a list of blacklisted destination addresses into BGP (Border Gateway Protocol) and hijacks all traffic to blocked websites."[x] In other words, the GFW forces routers to drop all traffic for blocked IPs. This technique is called null routing, and can only block outbound traffic from China and permits inbound traffic. This is sufficient in most cases, as most current Internet communication require a three-way-handshake to function.

IP address blocking is a "lightweight solution as the government can maintain a centralized blacklist without much involvement from the ISPs, and thus without much risk of leakage." It also only adds a small load to the gateway router of ISPs, and doesn't require any additional dedicated infrastructure. However, IP blocking does have two key limitations: First, the effectiveness of IP address blocking relies on the accuracy of the blacklist. It needs to be carefully maintained and updated, and websites can keep switching to new IP addresses to stay ahead of the GFW. Second, as many legitimate websites share the same IP addresses or address blocks with banned sites, over-censoring is an unavoidable side effect. This has been exploited

by censored websites to leverage the government into unblocking them in the past. For example, the heavily targeted site www.falundafa.org began resolving to the same IP address as www.mit.edu at one point, which the GFW then blocked. The OpenCourseWare site by MIT was also blocked, and caused such a public outcry that the block was revoked.



| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | 1.354844 | 10.200.128.110 | 216.58.200.46 | TCP | 68 | 58013→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=44 |
| 10 | 1.605324 | 10.200.128.110 | 216.58.200.46 | TCP | 68 | 58014→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=44 |
| 11 | 1.924212 | 216.58.200.46 | 10.200.128.110 | TCP | 64 | 80→58014 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1353 SAC |
| 12 | 1.924269 | 10.200.128.110 | 216.58.200.46 | TCP | 56 | 58014→80 [ACK] Seq=1 Ack=1 Win=131392 Len=0 TSval=444779035 |
| 13 | 1.924750 | 10.200.128.110 | 216.58.200.46 | HTTP | 438 | GET / HTTP/1.1 |
| 14 | 2.122063 | 10.200.128.110 | 74.125.23.100 | TCP | 52 | 56917→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 |
| 15 | 2.163053 | 216.58.200.46 | 10.200.128.110 | TCP | 64 | [TCP Out-Of-Order] 80→58014 [SYN, ACK] Seq=0 Ack=1 Win=42540 |
| 16 | 2.163090 | 10.200.128.110 | 216.58.200.46 | TCP | 56 | [TCP Dup ACK 12#1] 58014→80 [ACK] Seq=383 Ack=1 Win=131392 L |
| 17 | 2.180634 | 216.58.200.46 | 10.200.128.110 | TCP | 56 | 80→58014 [ACK] Seq=1 Ack=383 Win=43648 Len=0 TSval=335952367 |
| 18 | 2.190688 | 216.58.200.46 | 10.200.128.110 | HTTP | 596 | HTTP/1.1 301 Moved Permanently (text/html) |
| 19 | 2.190721 | 10.200.128.110 | 216.58.200.46 | TCP | 56 | 58014→80 [ACK] Seq=383 Ack=541 Win=130848 Len=0 TSval=444779 |
| 20 | 2.359679 | 10.200.128.110 | 216.58.200.46 | TCP | 68 | [TCP Retransmission] 58013→80 [SYN] Seq=0 Win=65535 Len=0 MS |
| 21 | 2.426069 | 10.200.128.110 | 74.125.23.113 | TCP | 52 | 56918→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 |
| 22 | 2.598143 | 10.200.128.110 | 46.82.174.68 | TCP | 52 | 56919→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 |
| 23 | 3.361591 | 10.200.128.110 | 216.58.200.46 | TCP | 68 | [TCP Retransmission] 58013→80 [SYN] Seq=0 Win=65535 Len=0 MS |

*Figure-4: This screenshot is an example of IP blocking. The author tried to access Google via the IP 216.58.200.46. No data was received and the site eventually timed out, as evident by the TCP Retransmission packets in black.*

## DNS Tampering

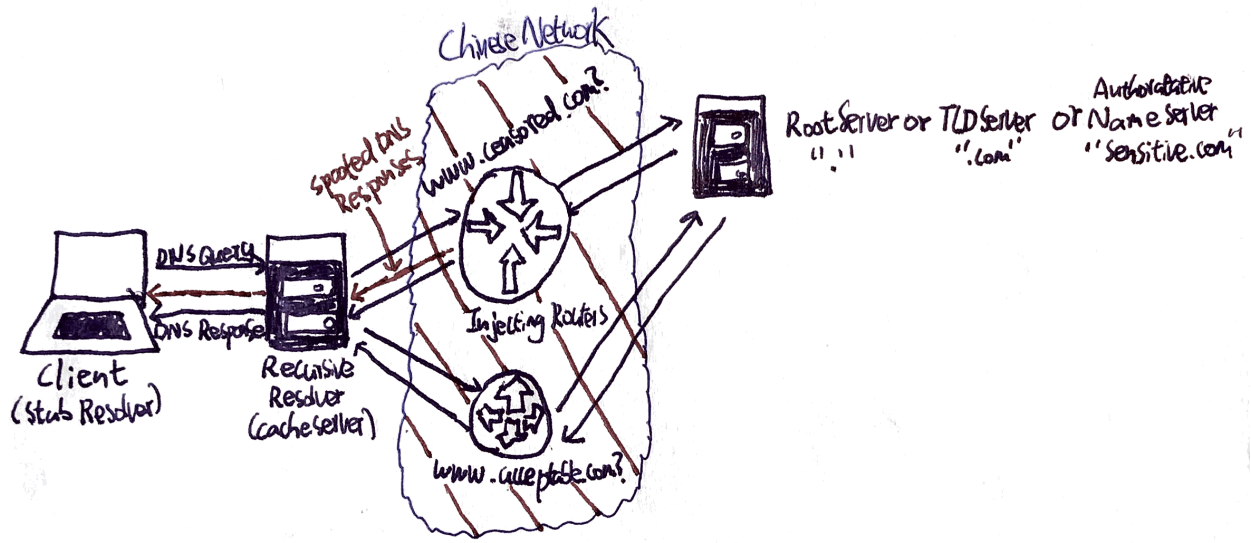



*Figure-5: An illustration of DNS Tampering.*

DNS tampering is used in conjunction with IP address blocking, as changing domain names is much harder than changing IP addresses. The first step in DNS tampering is DNS injection. When a user attempts to connect to a domain, the computer queries DNS servers for the IP address associated with the domain name. GFW monitors each DNS query originating from clients inside China at the border of the Chinese Internet. If it detects a query to a blocked domain name, it injects a fake DNS reply with an invalid IP, or in some rare cases, an IP to another website. This fake DNS reply then trickles down to internal recursive DNS servers in China, with the incorrect pairing cached along the way, achieving DNS poisoning. Thus, almost all DNS resolvers in China have poisoned caches.

When a site's domain name gets blocked in this way, there is little the site can do besides changing it. Therefore, DNS tampering and IP address blocking used together can effectively seal off censored sites at all levels. Similar to IP blocking, there are two major downsides to DNS tampering: first, large-scale collateral damage is unpreventable because GFW does not distinguish between DNS queries that originate from China and those that simply pass through China.[xi] Research showed that "Chinese DNS injection affected 15,225 open resolvers (6% of tested resolvers) outside China, from 79 countries."[xii] Another unintended consequence is that huge volumes of traffic can be suddenly directed to innocent websites,

serious disrupting their normal operation and forcing them to block all communications from China. Craig Hockenberry, a network engineer that maintains a simple web server for Iconfactory, wrote a fascinating blog entry about his encounter with GFW titled “Fear China”.[xiii] On January 20th, 2015, Craig’s single four core server was suddenly hit with traffic that peaked at 52 Mbps, about a third of Google’s global search traffic, assuming each request was 500 bytes. Upon reviewing server logs, he saw that his server was hit with connections targeted at 212 different domains, from www.youtube.com to cdn.gayhotlove.com, all originating from China.[xiv] Essentially, the GFW has inadvertently weaponized its network to DDOS innocent IPs. This has a high potential for abuse by the government, and if this trend continues, more and more websites will have no choice but to block all traffic from China in anticipation.

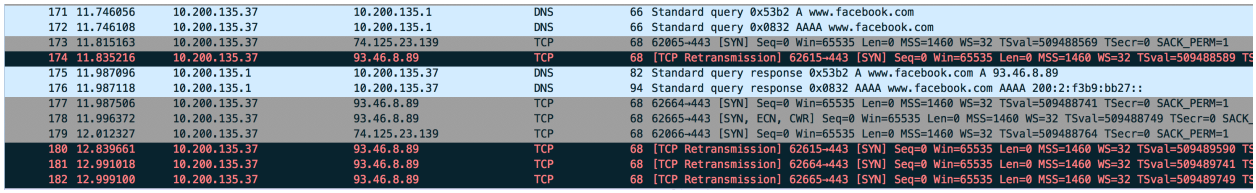



*Figure-6: This screenshot is an example of DNS tampering. The author tried to access www.facebook.com, as can be seen from the standard query. DNS server returned a poisoned address, 93.46.8.89. The TCP retransmissions to that IP is evidence the IP is invalid. Further research revealed that this is one of seven poisoned IPs regularly used by the GFW, and is owned by the company Fastweb in Italy.*[xv]

## Bypassing the GFW

While the majority of Internet users in China are aware of the existence of GFW, few are actually interested in bypassing the censorship and accessing blocked websites. This is mainly due to political propaganda, and the popularity of Chinese "clones" of sites such as Facebook and Twitter. For the few technologically savvy netizens of China, VPN and proxies remain the most accessible ways of avoiding the GFW. Virtual Private Networks work by routing all traffic to and from a computer through a server using many secure protocols. Thus, all connections to the outside web appear to be coming from the location of the VPN server instead of the user's actual location, and the user can effectively bypass the GFW. Proxies function similarly, except only browser traffic is encrypted.

Although the GFW has no way of interpreting encrypted content between the user and the VPN server, the GFW has enough understanding of popular VPN protocols such that it can use deep packet inspection and machine learning to identify and shut down VPN connections.[xvi] If a user sets up his own VPN using a basic OpenVPN setup, he will find that the VPN works fine for a few minutes before latency starts increasing exponentially and eventually timing out. The GFW finds heuristics to guess which TCP/UDP connections are used for VPN, then simply drops all packets when it has enough "proof". One user on Hacker News pointed out that the only way to manually disguise VPN traffic is to make it look like standard HTTPS sessions. "For example in a traditional HTTPS session, if the client browser downloads a 500kB image over HTTPS, it will send periodical empty TCP ACK packets as it receives the data. But when using a VPN that encrypts data at the IP layer, these empty ACK packets will be encrypted, so The Great Firewall will see the client sending small ~80-120 bytes encrypted packets, and will count this as one more sign that this might be a VPN."[xvii]

Considering that the GFW has the capabilities to shutdown VPN connections, it remains a mystery why the government allows commercial VPNs such as ExpressVPN, Astrill VPN, and HMA! to operate freely. The officially accepted answer is that the Chinese government are willing to give legitimate foreign businesses some breathing room, as many firms rely on the use of VPN in their day to day operations. Conspiracy theorists speculate that the Chinese government has already taken control of these commercial VPN services, and are actively

spying on supposedly encrypted connections using man-in-the middle. One blog post by Marc Bevand on Jan 14, 2016 pointed out that ExpressVPN, one of the top 3 VPN services used in China, used a CA certificate RSA key of only 1024 bits.[xviii] It is believed that such a key can be factored by $10 millions of specialized hardware, which is hardly unfeasible considering the benefits it would bring the Chinese government. On February 15, 2016, ExpressVPN upgraded their CA keys from 1024 to 4096-bits, and no one will ever know whether ExpressVPN was compromised or not.

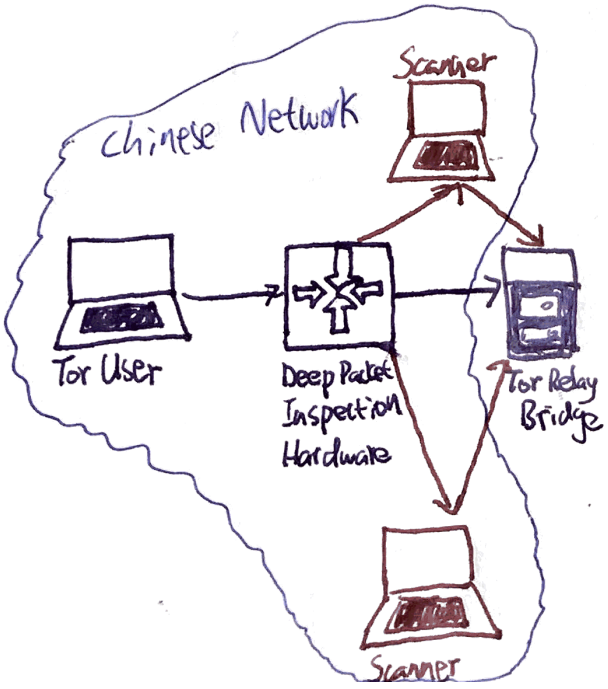



*Figure-7: An illustration of Active Probing System*

The more advanced users can leverage Tor, the infamous anonymity network, to circumvent the GFW. In simple terms, Tor's users employ the Tor network by connecting through a series of virtual tunnels rather than making a direct connection. “It is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content.”[xix] However, Tor has not always been viable in China. In 2012, Chinese users started having issues connecting to the Tor network.[xx] After an extended investigation, it was revealed that the GFW uses an active probing system to dynamically recognize Tor usage.[xxi] Tor relies on a large number of entry guards and bridge relays as end points to offer connections to censored regions. These bridges are Tor relays that aren’t listed in the main Tor directory, so they should

theoretically be untraceable. The GFW implemented a real-time probing system that "searches for bytes that identify a network connection as Tor. If these bytes are found, the firewall initiates a scan of the host which is believed to be a bridge and shuts it down." This works because the GFW "is able to (partially) speak the vanilla Tor protocol, obfs2, and obfs3 to probe bridges", and it functions in real-time: "on average, it takes only half a second after a bridge connection for an active probe to show up".[xxii] The scan is run by seemingly arbitrary computers strewn throughout China, and cannot be predicted by the Tor network.

The situation only changed in 2015, when the Tor project released obfs4 and Meek, two protocols that use Pluggable Transports.[xxiii] Per Tor Project, Pluggable Transports transform the Tor traffic between client and bridge.[xxiv] Specifically, obfs4 is an obfuscation protocol that uses Pluggable Transports to further encrypt the connection between client and bridge. This relies on a shared secret distributed out of band. Since probes do not have access to the secret key, it cannot identify the bridges. Alternatively, Meek is a transport protocol that relay traffic through popular cloud computing services, such as Microsoft Azure, by imitating regular traffic. Instead of taking the HTTPS approach often used against GFW, it uses HTTP and TLS for obfuscation. GFW cannot distinguish between Tor traffic and normal cloud traffic, but it also cannot block the IPs of cloud computing services due to business reasons.

Obfs4 and Meek take opposite approaches to evading the GFW: obfs4 uses an extra layer of encryption to hide in the shadows, while Meek imitates regular traffic to hide in plain sight. Nonetheless, both have contributed to the resurgence of Tor in bypassing GFW in the past year.

## Conclusion

The Great Firewall is a powerful and sophisticated censorship tool unlike any the world has seen before. It uses a combination of DNS tampering and IP address blocking to completely seal off access. In addition, it uses an IDS-like system to inspect traffic for blacklisted keywords and terminate connections by injecting RST packets. While these tools can cause significant collateral damage, they are extremely effective for blocking almost any website for the vast majority of Internet users in China. On the other hand, netizens can use VPN, Proxies, and Tor

to bypass the GFW. Yet, the GFW leverages machine learning and deep packet inspection to shut down VPN and Proxy tunnels, and deploys an active probing system that can shut down Tor relays running everything but the latest Tor protocols. With the recent introduction of the attack oriented Great Cannon, another piece of Golden Shield Project is now complete. Internet censorship will continue to evolve and grow, and many expect the Internet in China to become even more controlled. At the same time, the battle against censorship rages on, but it would be hard to convince anyone that the Chinese government is losing.

## References


[i] http://news.sciencenet.cn/htmlnews/2014/8/301669.shtm
[ii] https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html
[iii] http://www.internetlivestats.com/internet-users-by-country/
[iv] http://networkcultures.org/query/wp-content/uploads/sites/4/2014/06/10.Min_Jiang.pdf
[v] https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf
[vi] https://blog.thousandeyes.com/deconstructing-great-firewall-china/
[vii] https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf
[viii] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.191.206&rep=rep1&type=pdf
[ix] http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/12389-foci13-khattak.pdf
[x] http://queue.acm.org/detail.cfm?id=2405036
[xi] http://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf
[xii] http://ieeexplore.ieee.org/stamp/stamp.jsp?reload=true&arnumber=6814824
[xiii] http://furbo.org/2015/01/22/fear-china/
[xiv] https://gist.github.com/chockenberry/c3e584c28ad6ab6e5faa
[xv] http://viewdns.info/research/dns-cache-poisoning-in-the-peoples-republic-of-china/
[xvi] http://link.springer.com/article/10.1007/s10796-008-9131-2
[xvii] https://news.ycombinator.com/item?id=10101653
[xviii] https://news.ycombinator.com/item?id=10101653
[xix] https://www.torproject.org/about/overview
[xx] https://blog.torproject.org/blog/knock-knock-knockin-bridges-doors
[xxi] http://www.cs.kau.se/philwint/gfw/
[xxii] https://blog.torproject.org/category/tags/gfw
[xxiii] https://plus.google.com/+GhostAssassin/posts/aLcyVfcH7mP
[xxiv] https://www.torproject.org/docs/pluggable-transports.html.en