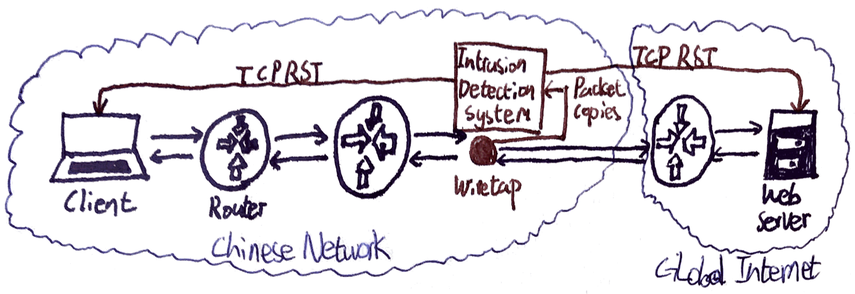
In-depth analysis of the Great Firewall of China

Chao Tang, COMP 116, December 14, 2016

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.

TCP Reset



How It works

The GFW inspects traffic by passing copies to out-of-band devices based on Intrusion Detection Systems. The original packets are unaffected, while the IDS inspects the content of the packet and the requested URL. Once the IDS detects blacklisted keywords, the GFW router injects multiple forged TCP RST packets to both endpoints, forcing the connection to be dropped.

Pros

- On-path architecture is efficient and does not create a bottleneck
- Capable of IP and TCP segments reassembly
- Maintains flow state regarding source and destination to block all further communications for any period of time.

Cons

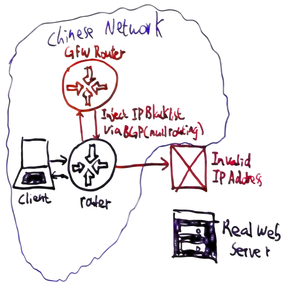
- Not capable of inspecting HTTPS traffic
- Can be bypassed by ignoring RST packets on both endpoints
- **Due to these constraints, TCP RST is now rarely used**

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=69671489
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=69671489
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

Failed Attempt

While connected to a VPN server in Shenzhen, the author used Yahoo to search for the censored string "falun". The author was unable to connect to websites from the results page, evident by TCP Retransmissions. The author initially thought the five TCP RST packets were the doings of GFW. However, the ACK number of the packets were all 0, which is uncharacteristic of forged TCP RST packets. Thus, it is unlikely that GFW was at play here.

IP Address Blocking



How It works

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. This technique is called null routing.

Pros

- Only adds a small load to the gateway router
- No additional infrastructure needed
- Centralized blacklist without further involvement from ISPs

Cons

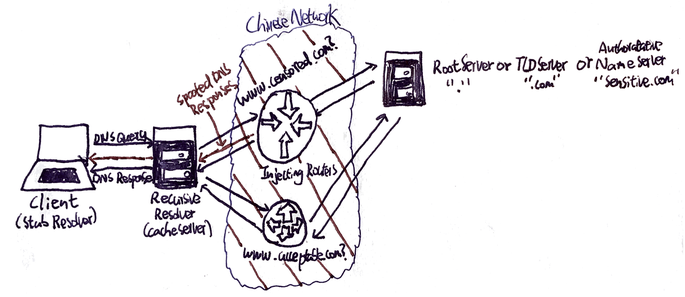
- Blacklist needs to be frequently updated
- Websites can change IP addresses to stay unblocked
- Over-censoring of legitimate websites that share the same IP addresses or address blocks as blocked websites

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	1.685324	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=4254
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
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=444775
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

Successful Attempt

While connected to a VPN server in Shenzhen, 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



How It works

GFW monitors each DNS query originating from any 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. This fake DNS reply then trickles down to internal recursive DNS servers in China. Thus, almost all DNS resolvers in China have poisoned caches.

Pros

- Lightweight yet efficient
- There is little a blocked website can do besides changing domain name
- **Effectively seal off all access when used in conjunction with IP address blocking**

Cons

- Large-scale collateral damage to DNS queries passing through China originating elsewhere
- Can unintentionally redirect huge volumes of traffic to innocent websites

171	11.746056	10.200.135.37	10.200.135.1	DNS	66 Standard query 0x53b2 A www.facebook.com
172	11.746108	10.200.135.37	10.200.135.1	DNS	66 Standard query 0x0832 AAAA www.facebook.com
173	11.815163	10.200.135.37	74.125.23.139	TCP	68 62065→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=5094
174	11.835216	10.200.135.37	93.46.8.89	TCP	68 [TCP Retransmission] 62615→443 [SYN] Seq=0 Win=65535 Len=0 MSS=
175	11.987096	10.200.135.1	10.200.135.37	DNS	82 Standard query response 0x53b2 A www.facebook.com A 93.46.8.89
176	11.987118	10.200.135.1	10.200.135.37	DNS	94 Standard query response 0x0832 AAAA www.facebook.com AAAA 200:2
177	11.987506	10.200.135.37	93.46.8.89	TCP	68 62664→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=5094
178	11.996372	10.200.135.37	93.46.8.89	TCP	68 62665→443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32
179	12.012327	10.200.135.37	74.125.23.139	TCP	68 62066→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=5094
180	12.839661	10.200.135.37	93.46.8.89	TCP	68 [TCP Retransmission] 62615→443 [SYN] Seq=0 Win=65535 Len=0 MSS=
181	12.991018	10.200.135.37	93.46.8.89	TCP	68 [TCP Retransmission] 62664→443 [SYN] Seq=0 Win=65535 Len=0 MSS=
182	12.999100	10.200.135.37	93.46.8.89	TCP	68 [TCP Retransmission] 62665→443 [SYN] Seq=0 Win=65535 Len=0 MSS=

Successful Attempt

While connected to a VPN server in Shenzhen, 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 is evidence the IP is invalid. Further research revealed that this is one of seven poisoned IPs regularly used by the GFW .

Bypassing the Great Firewall

Using VPNs and Proxies

How they work

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. Proxies function similarly, except only browser traffic is encrypted.

Countermeasures by GFW

The GFW has enough understanding of popular VPN protocols such that it can use deep packet inspection and machine learning to identify VPN connections. It finds heuristics to guess which TCP/UDP connections are used for VPN, then simply drops all packets.

Answers to countermeasures

For non-commercial VPN setups, the only way to manually disguise VPN traffic is to make it look like standard HTTPS sessions. There are many details that need to be manually matched. A few commercial VPNs also operate in China, despite the fact that they can be easily shutdown by the government at any time.

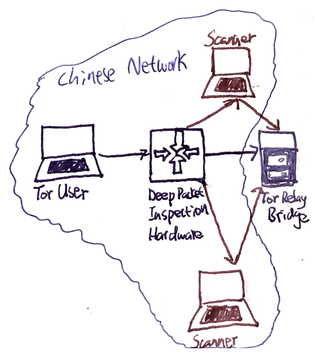
Using Tor

How it works

Tor's users employ the Tor network by connecting through a series of virtual tunnels rather than making a direct connection, allowing them to circumvent the GFW.

Countermeasures by GFW

Tor relies on a large number of entry guards and bridge relays as end points to offer connections to censored regions. 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 rendered Tor completely inaccessible in China for 3 years.



Answers to countermeasures

In 2015, the Tor project released obfs4 and Meek, two protocols that use Pluggable Transports. Pluggable Transports transform the Tor traffic between client and bridge. Obfs4 offers an extra layer of encryption using a shared secret key distributed out-of-band, while Meek disguises Tor traffic as regular cloud computing traffic. Both are currently viable options.