The phrase was first coined by western media in 1997

The firewall of China is a subset of the golden shield project which focuses on ways to censor and block information.

It works by preventing access to IP and domain name blocks.

Internet Café owners were forced to install surveillance software on their computers and report any behavior the government deemed dangerous. ISP’s also had to verify every user’s ID.

In 2006 it introduced keyword blocking technology

After 2008 the main layout of the wall was complete. China started to improve on it.

They began to find ways to detect anonymous proxies and VPN’s which can circumvent the wall

China mobile and China intercom operate internet exchange points which connect to the rest of the world these companies then sell to ISPS. This allows for a controlled internet data stream.

The final part of the wall is a human component. These workers monitor contents and reports on violations.

SLIDE TOPOLOGY:

Internet exchange points are usually located at the border, and they manage all inbound and outbound requests. These internet exchange points are maintained by STATE owned companies. Some examples are as follows: China mobile, China Telecom and China Unicom.

The great firewall of China consists of 3 parts

1. IP ADDRESS BLOCK

Each device that is connected to the Internet has a unique Public IP Address that can roughly map out where that device is connected from. That Ip address is assigned by your internet service provider. Each time you connect to the internet and attempt to access a website, the computer sends internet packets to request access that information.

An Internet packet consists of a header and a payload. The payload is the actual data sent, the header however, is what we are interested in. It contains the source IP address and the destination IP address.

China has a list of blocked IP addresses, and since all connections eventually make their way to your ISP. What ends up happening is all data that makes its way to those access points are checked first. If the destination address is in the blocklist it either reroutes to another address or sends that data to the void which ultimately leaves the sender in constant state of loading.

This can be circumvented using VPNS, we’ll go more in-depth about that later.

2 – DNS POISONING

DNS (Domain Name system) can be thought of as the phonebook of the internet. It used to translate domain names to Ip addresses. Without DNS you’ll have to memorize the Ip address of every website you want to use.

The process goes like this:

- The user enters the domain name in the search bar.

- The request is then sent to a DNS resolver which are servers in charge of tracking down the IP address that corresponds to that domain name.

- The requester then gets routed to that address.

China has a DNS blocklist of over 15000 keywords. Google is one such example. If someone living in China tries to access google. The firewall intercepts the DNS request and sends back an invalid IP(DNS poisoning).

3 – TCP DROP

TCP stands for Transfer control protocol. It’s an agreed upon set of “rules” that govern the transfer of internet packets. As we mentioned an internet packet consists of a header and a payload. The header contains a lot more information than just the source and destination addresses. In a standard TCP packet, there is section for flags. Since we are dealing with bits, those flags will either be 1 or 0. Some notable flags are the FIN and ACK flag, which are used to indicate that the transmission is complete and acknowledged respectively.

For example, if the user has finished sending his data, then the final packet sent will have the bit that corresponds to the FIN flag set to 1. He will also receive a packet back from the host with both ACK and FIN flags set to 1.

Now the flag that causes a TCP drop is the RST flag. It is used by a TCP sender to indicate that it will neither accept nor receive more data. And that’s what the Chinese firewall abuses to forcefully close connections. For example:

1 – A Chinese person enters a website that contains blocked keywords.

2 – On a hardware level an internet packet is sent requesting access.

3 – That packet will propagate throughout the network on it’s way to its destination

4 - subsidiary machines set up by ISP’s will intercept that packet and start scanning the website for blocked keywords

5 – If it detects any blocked keywords and since it’s on the same network it will send a series of packets both ways with the RST flag set to 1.

6 – Both side interpret it as a genuine packet from the other end requesting to kill the connection and thus stops transmitting.

THE SOLUTION:

VPNS

The firewall can be circumvented using a VPN. A VPN encrypts the traffic and sends it to a foreign server and from there routes it to it’s original destination. And since the data is encrypted, the Chinese firewall can’t inspect it so it lets it through. However the firewall has gotten a lot smarter over the years. It has a good understanding of common VPN protocols. It employs the use of AI to detect VPN traffic. For example if 99% of the data stream is routed to 1 address and is encrypted then it’s most likely a VPN and thus shuts down the connection. It can also recognize most free VPNS.

The Chinese government has combated this by regulating the use of VPNS. In 2017 vendors selling illegal VPN’s on TaoBao(Online shopping platform) were fined and some were even jailed. VPN’s in China aren’t outright banned but they are closely monitored.