The Synapse: Intercollegiate science magazine

Volume 28 | Issue 1 Article 8

2021

The Great Firewall of China: The Implementations and Impact of Internet Censorship

Nathan Englehart

The Great Firewall of China

The Implementations and Impact of Internet Censorship

Written by Nathan Englehart
Illustrated by Evelyn Lazen

Currently, China has 751,886,119 internet users, the greatest number of users of any country in the world. As the internet becomes increasingly integral to modern life, internet traffic control has major national security and economic implications for modern China. China's solution to these issues is its nationwide firewall, colloquially referred to as the "Great Firewall of China," which is a combination of various technological implementations responsible for the censorship and content filtering of internet traffic.

In most countries, including the United States, internet content deemed harmful to society is censored (for example, the sale of illegal drugs and child pornography). Much of this censoring takes place using a network security system called a firewall, which monitors and controls incoming and outgoing network traffic. China takes its firewall a step further by screening for sensitive information and political content. China also uses its firewall to block foreign social media websites as a form of domestic trade protection. The Chinese firewall implements various solutions for censorship and content filtering, including network blackholing, quality of service filtering, Domain Name System hijacking, and URL filtering to prevent unwanted internet communications.

The Chinese firewall's most basic censorship implementation is the network blackholing of banned connections. Internet protocol (IP) addresses are numerical names assigned to each computer connected to a computer network. Using IP addresses, computers can be identified and physically located.

Therefore, the Chinese firewall is capable of combating the primary method Chinese internet users utilize to avoid censorship.

Network blackholing is a basic process: the firewall keeps a list of banned IP addresses, and if the firewall detects that a user is attempting to communicate with a banned address, the connection is automatically dropped. Maintaining an updated list of flagged IP addresses is very difficult, so this method is generally a last resort.

Quality of service (QoS) filtering is a more common implementation of censorship used by the Chinese firewall. QoS filtering uses deep packet inspection identification, a data inspection technique that analyzes data being sent over a computer network, according to a survey conducted by Joseph Lorenzo Hall and colleagues in 2018. The Chinese firewall monitors data being sent by users and echos the collected information to a system that then analyzes the data, and scores user requests based on how suspicious it determines the connection to be. The more suspicious the system determines the connection to be, the more it slows down the connection to the request on the client side. If the connection is very suspicious, the client's request will time out, effectively banning the user from the connection.

QoS filtering is commonly utilized to prevent users from employing a Virtual Private Network (VPN) to circumvent the Chinese firewall. A VPN allows for users to theoretically bypass the firewall by sending requests to a VPN server, which then relays the search to the host. This potentially keeps outside parties (such as the government) from being able to access data such as your search history, or where certain searches originate from. Users connect to VPN points outside the local network when sending requests to internet servers. At these VPN points, information is generally encrypted and decrypted. The encryption tunnels implemented by VPNs make it difficult for user information to be intercepted by actors interested in the user's requests. However, QoS filtering catches VPN connections with deep packet inspection before requests can reach VPN points. Therefore, the Chinese firewall is capable of combating the primary method Chinese internet users utilize to avoid censorship.

The Chinese firewall also uses Domain Name System (DNS) hijacking to prevent user connection to a few sites, including Twitter and Facebook. DNS servers match IP addresses with human-recognizable website names. The firewall determines whether users are trying to engage in unwanted connections through flagged domain names and keywords. When users try to engage in unwanted communications through a domestic DNS server, the server will have the user look for the website at the wrong location causing a connection timeout. If a user tries to use a foreign DNS resolver such as Google Public DNS, the firewall mismatches the user-input human-recognizable name with a random blocked IP address.

Similar to DNS hijacking, another method of censorship that China's firewall implements is URL filtering. This implementation of censorship involves proxies. Proxies are intermediaries between connection requests and the connection destinations. Using transparent proxies, the Chinese firewall performs keyword-based scans on requested URLs. Thus, the firewall is able to block web pages based on keywords it finds associated with them. This can lead to interesting cases of web accessibility. For example, "http://en.wikipedia.org" is accessible from within China, but "https://en.wikipedia.org/wiki/Internet_censorship_in_China" is not accessible.

China's firewall filters internet traffic in and out of the country. The firewall uses QoS filtering to prevent users from using VPNs to avoid the firewall. By blocking websites based on target keywords using URL filtering, China can sensor sensitive political material. Using DNS hijacking to prevent users from connecting to foreign social media platforms, China can also promote domestic tech companies (e.g. Twitter vs. Sina Weibo). Thus, the varying methods through which China's firewall implements censorship significantly influences the online habits of Chinese citizens today.