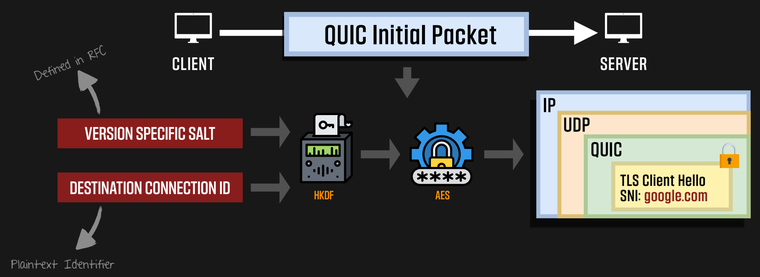
Exposing and Circumventing SNI-based QUIC Censorship of the Great Firewall of China

Ali Zohaib*, Qiang Zao*, Jackson Sippe, Abdulrahman Alaraj, Amir Houmansadr, Zakir Durumeric, Eric Wustrow

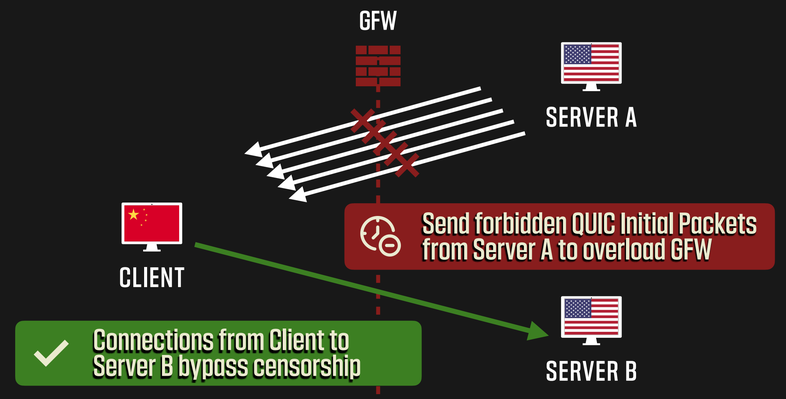
QUIC Protocol

QUIC is a UDP-based transport protocol with built-in encryption



QUIC Initial Packets are encrypted with a key that is derivable by a passive observer

Overwhelming the GFW



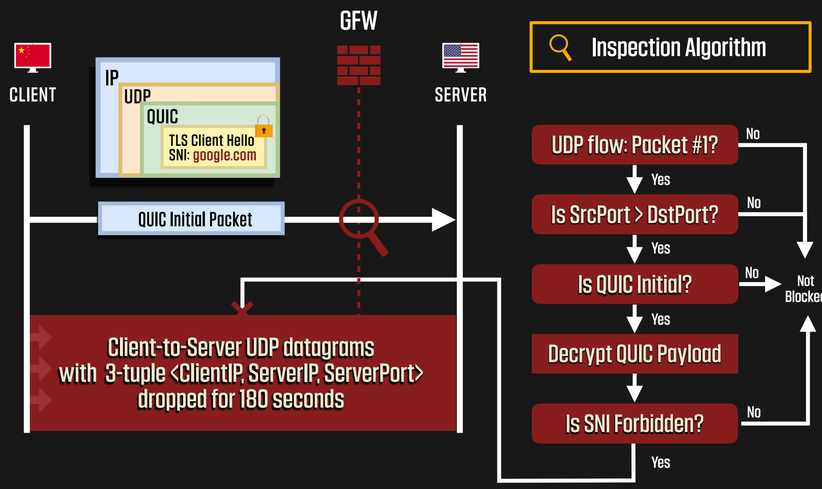
Responsible Disclosure

2025

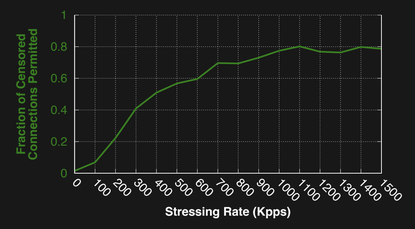
- JANUARY 22nd — Availability attack disclosed to CNCERT.
- JANUARY 24th – FEBRUARY 24th — Multiple visits on our private disclosure webpage. No response received.
- MARCH 13th — Bidirectional QUIC blocking stopped. Attack remains viable from inside China.

In April 2024, the Great Firewall of China began blocking QUIC traffic by inspecting the TLS SNI field

How the GFW Censors QUIC Traffic



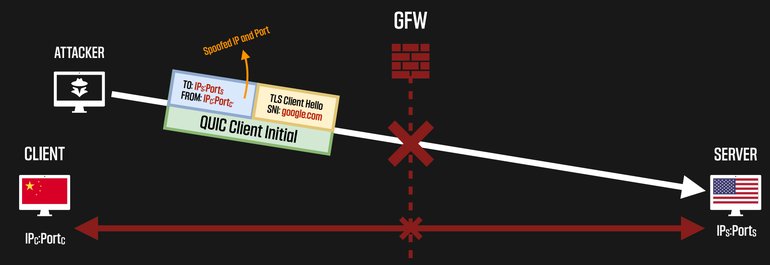
First instance of residual blocking for a UDP-based protocol



The GFW failed to censor 80% of our QUIC connections under moderate-load conditions.

Weaponizing the GFW

Triggering Censorship Between Arbitrary Hosts via IP Address Spoofing



All open/root DNS resolvers outside China can be blocked from access within China

Circumvention Techniques

- Using Source Port <= Destination Port (e.g. listening on port 65535)
- SNI Splitting / QUIC Client Initial Fragmentation
- Sending Random UDP datagram before QUIC Initial
- Post-handshake connection migration
- Use of Encrypted Client Hello (ECH)
- Version Negotiation

Adopted by:

- QUIC-GO
- SING-BOX
- Xray
- Hysteria
- V2Ray

University of Massachusetts Amherst · GFW Report · Stanford University · University of Colorado Boulder