

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

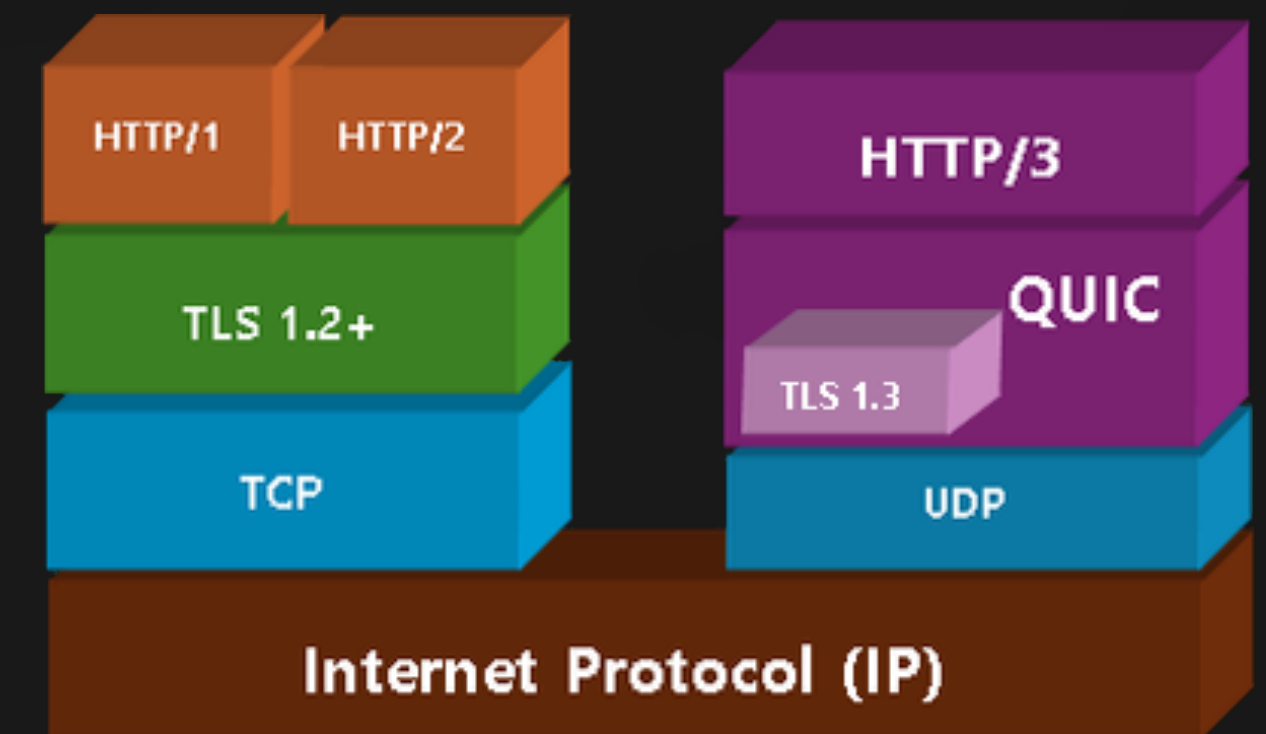
Ali Zohaib^{*}, Qiang Zao^{*}, Jackson Sippe, Abdulrahman Alaraj,
Amir Houmansadr, Zakir Durumeric, Eric Wustrow

USENIX Security 2025

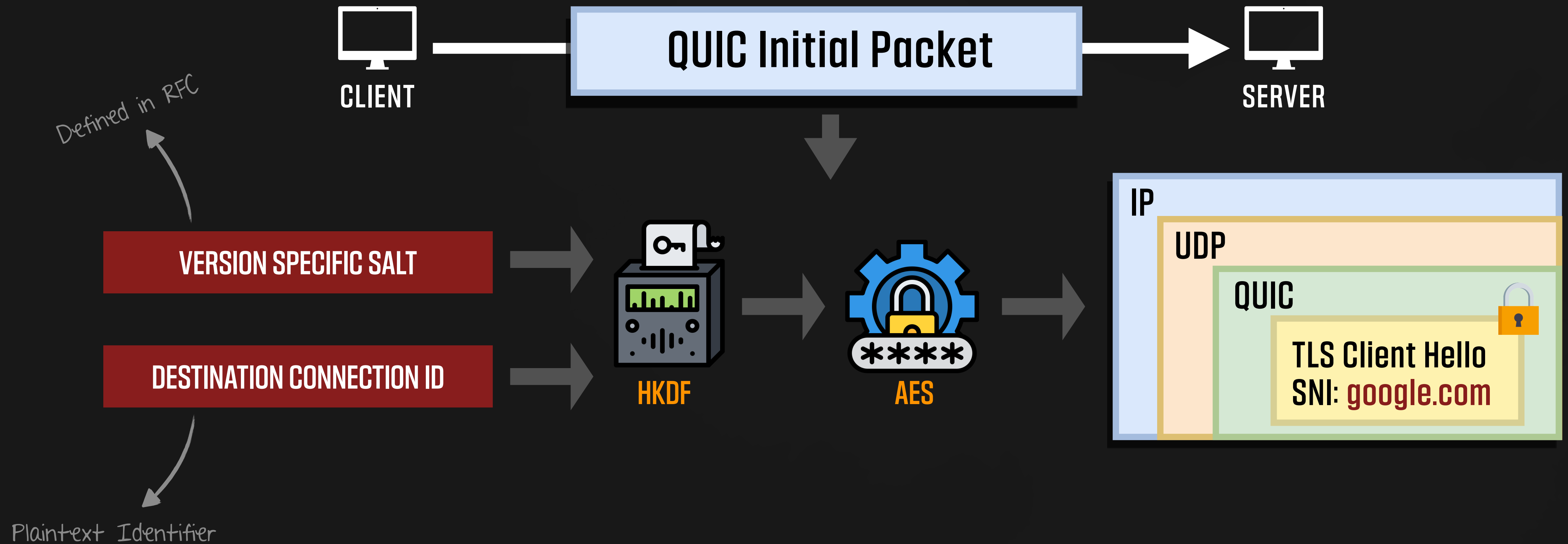


A QUIC Primer

- Transport layer protocol standardized in 2021
- Lower latency & faster connection establishment
- Built-in encryption: all packets are encrypted
- Foundation of HTTP/3
- According to Cloudflare, 30% of their traffic is QUIC



QUIC Initial Packet

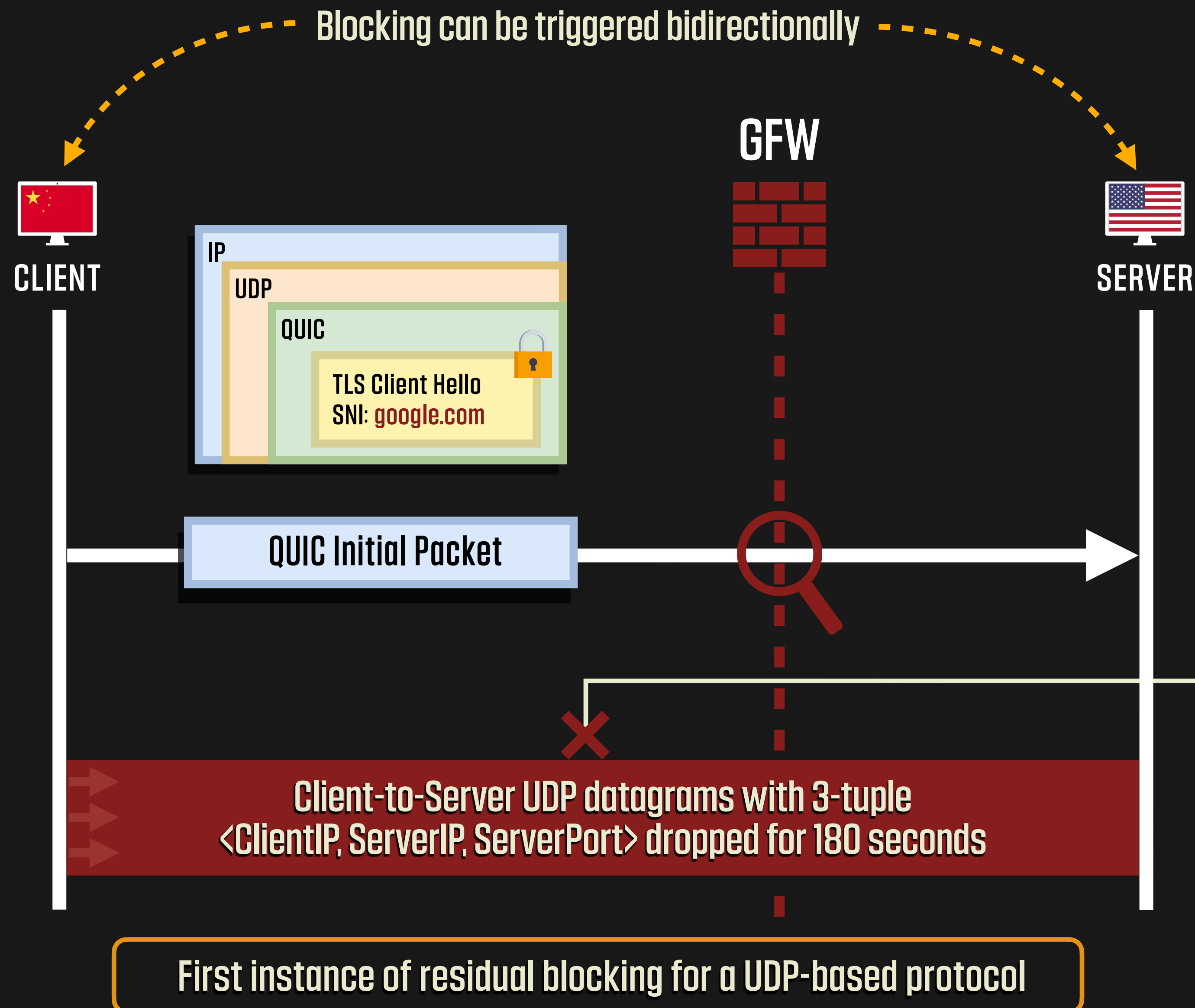


Encrypted with a key that is derivable by a passive observer

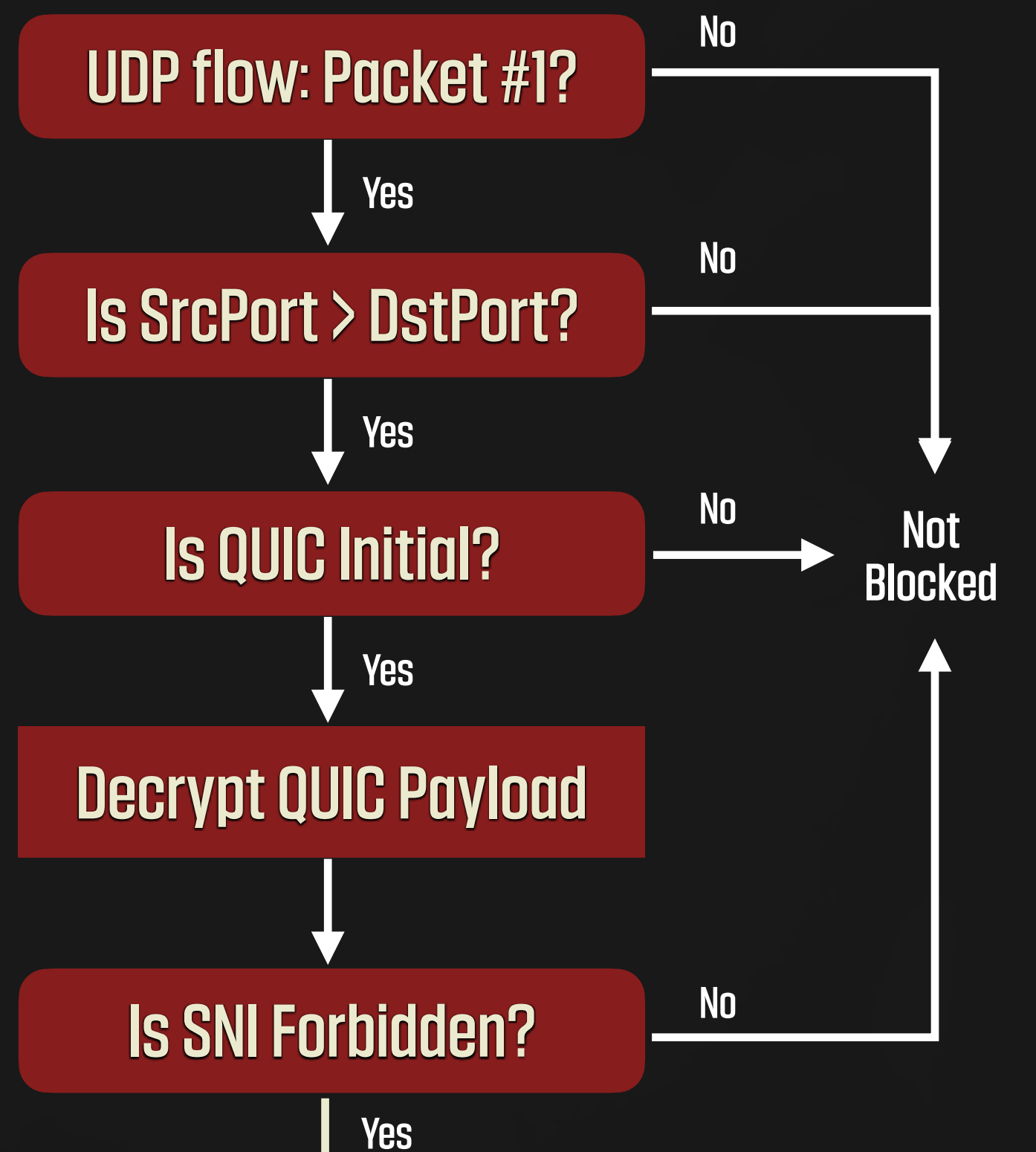


In April 2024, the Great Firewall of China began blocking QUIC traffic by inspecting the TLS SNI field

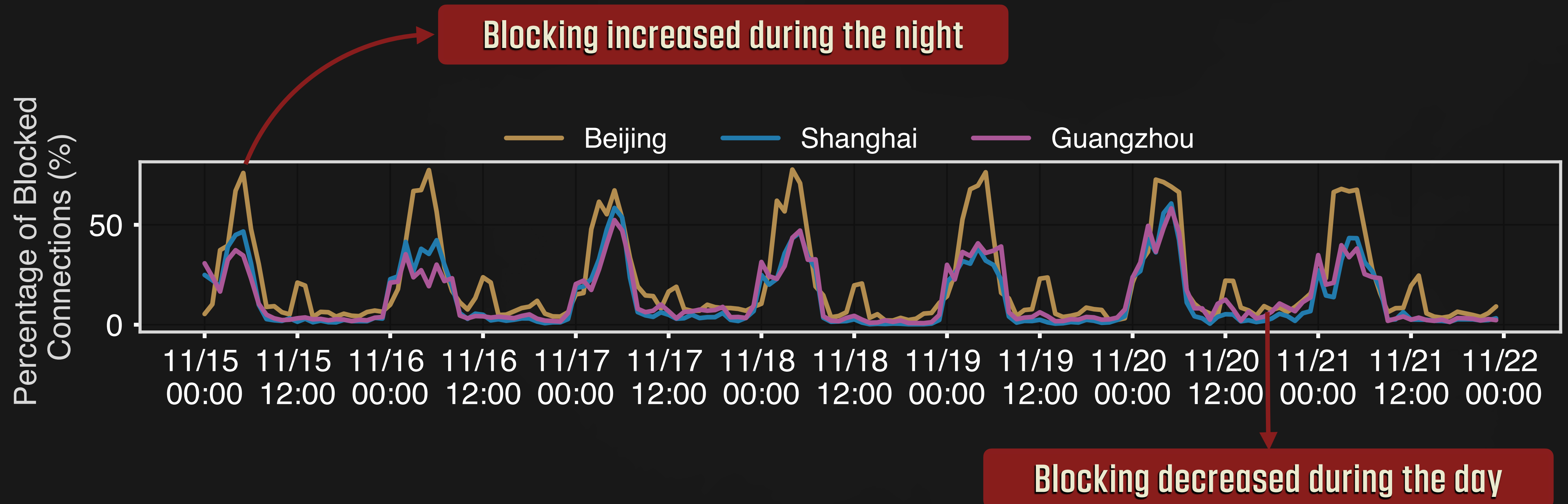
How the GFW Censors QUIC Traffic



Inspection Algorithm

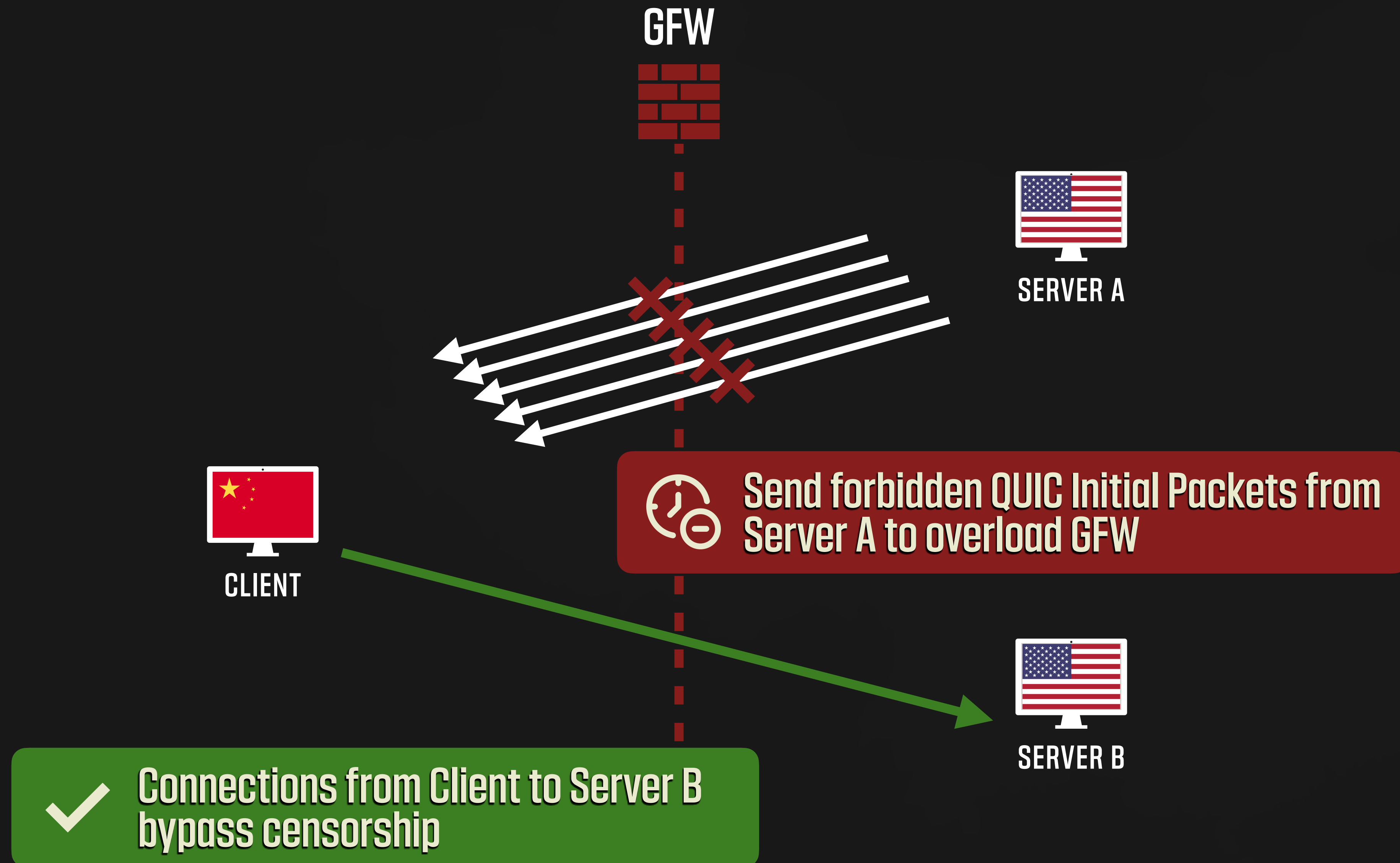


Diurnal Blocking Pattern

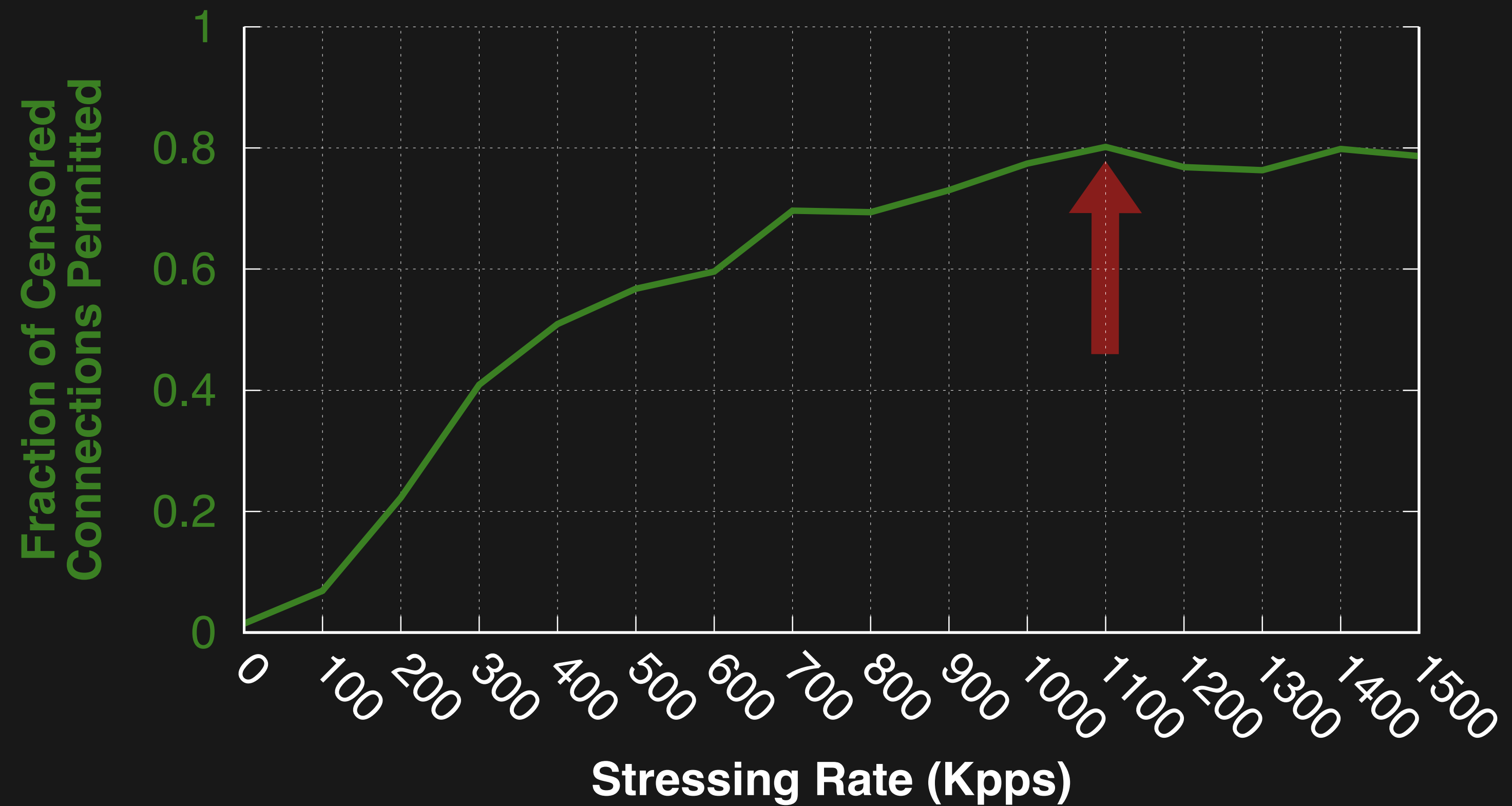


GFW can only block a limited number of concurrent connections. Can we overwhelm its capacity?

GFW Degradation Attack



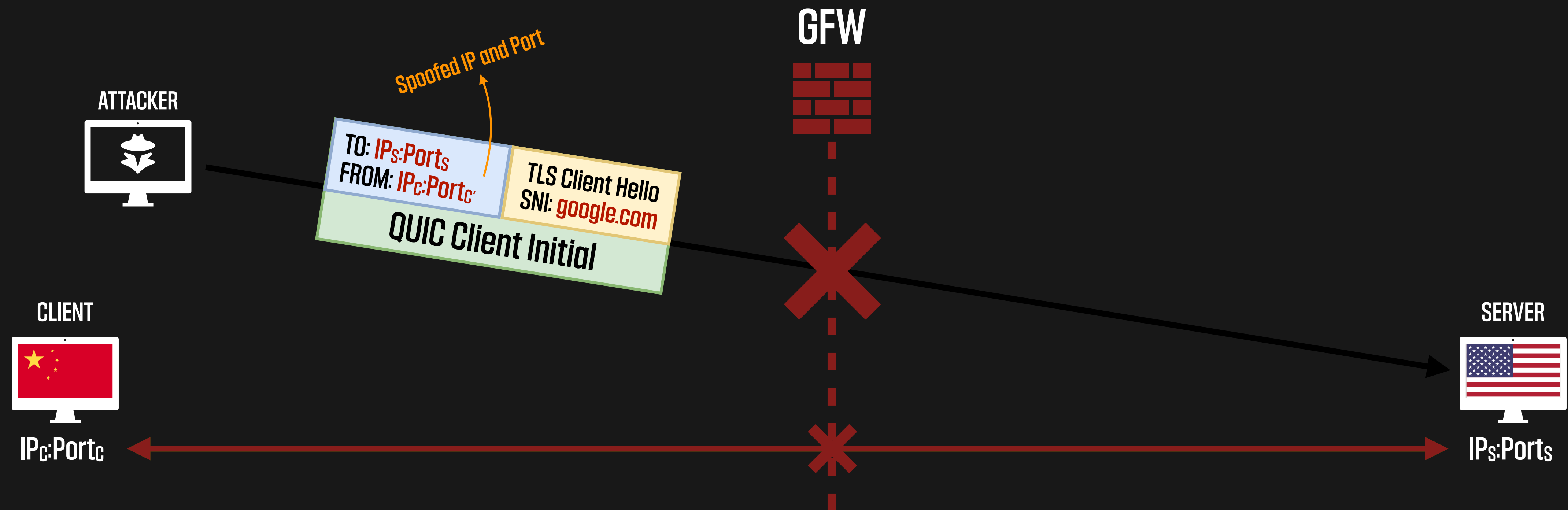
GFW Degradation Attack



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

Weaponizing GFW's QUIC Censorship

Triggering Censorship Between Arbitrary Hosts via IP Address Spoofing



UDP datagrams with 3-tuple $\langle IP_c, IP_s, Port_s \rangle$ dropped for 180 seconds

Blocking is bidirectional → Attacker can be outside China

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

Availability Attack

SETUP

👤 Attacker issues forbidden requests to 🖥️ Victim Server in China spoofing IP addresses of ● Victim Hosts



● Most affected destination host

● Least affected destination host

17 out of the 32 hosts were heavily impacted by our attack

Responsible Disclosure

2025

JANUARY 22nd ●

Availability attack disclosed to CNCERT.

JANUARY 24th ●



FEBRUARY 24th ●

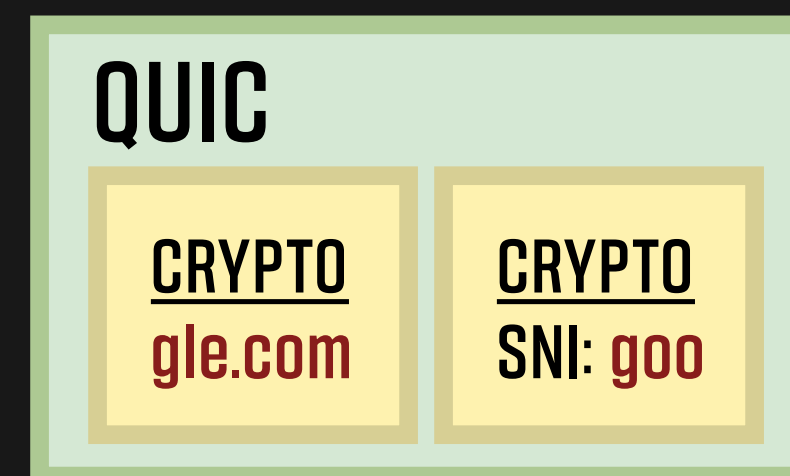
**Multiple visits on our private disclosure webpage.
No response received.**

MARCH 13th ●

**Bidirectional QUIC blocking stopped.
Attack remains viable from inside China.**

Circumvention Techniques

- Using Source Port \leq 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



QUIC-GO

SING-BOX

Xray

Hysteria

V2Ray

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

USENIX Security 2025



Project Webpage



Data and Code

