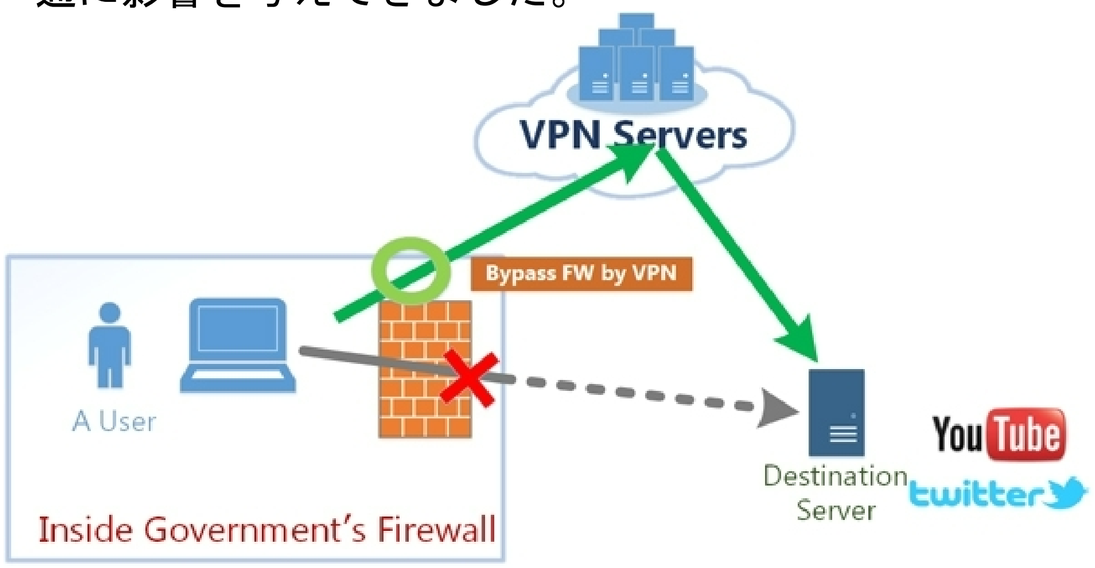
中国Great Firewallの実態解明と回避戦略

1. 研究背景と本研究の目的

■ 中国のGreat Firewall（以下GFW）は、世界最大規模の国家的インターネット検閲・トラフィック制御システムであり、1998 年の運用開始以来、数億人規模の情報流通に影響を与えてきました。



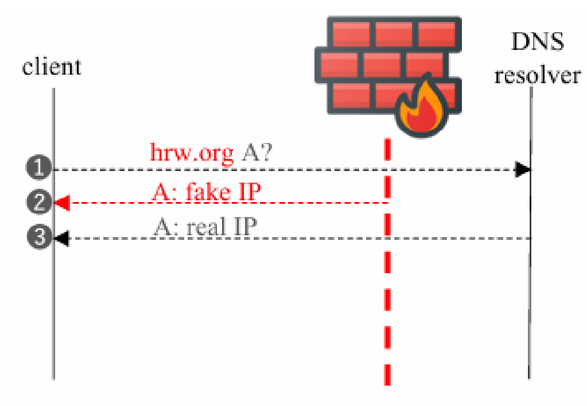
【本研究の目的】

GFWの技術と脆弱性を解明することで、安全で開かれたインターネット設計と国際的な対話を前進させることができます。

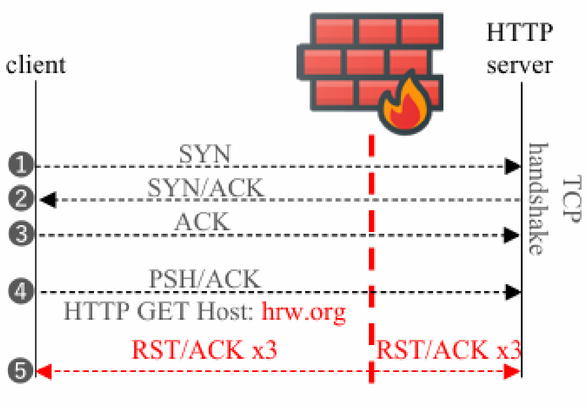
2. GFWのネットワーク干渉手段

DNSレベルの検閲

DNSポイズニング（偽のIPアドレスを返す）を行う。たとえばユーザがhrw.orgにアクセスしようとすると、GFWが正規応答より先に偽応答を返し、接続を誤誘導する。。



(a) DNS filter over UDP



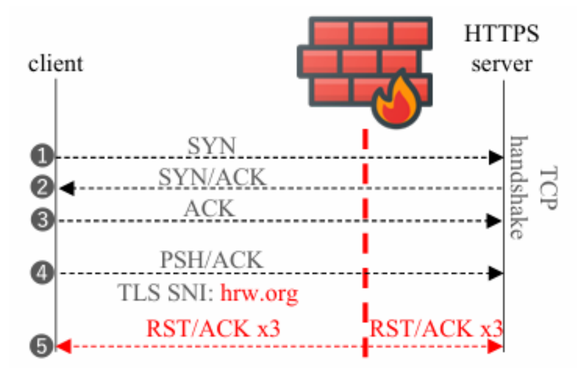
(b) HTTP filter

HTTPレベルの検閲

Hostヘッダ やURLに対してキーワードマッチングを行う。特定キーワードが含まれる場合にはRSTパケットを注入してTCP接続を強制終了させる。平文通信であるため内容ベースの詳細な検閲が可能である。

HTTPSレベルの検閲

通信は暗号化されているため内容を読み取れない。TLSのClient Helloに含まれるSNIを検査し、SNIに「hrw.org」などが含まれる場合に検出・遮断を実施する。



(c) HTTPS filter

3. これまでの研究

年	研究マイルストーン	主な成果
2006	*Ignoring TCP RST*	RST無視で初期キーワード遮断を回避する手法を提示
2023	*Encrypted -Traffic Study*	完全暗号化トラフィックに対するリアルタイム遮断の解析
2024	*GFWeb*	10.2 億ドメインをテストし、HTTP 943 k／HTTPS 55k ドメイン遮断を計測
2024	*河南ファイアウォール*	省レベル防火壁のTLS SNI／HTTP検閲をGFWと比較分析
2025	*Wallbleed*	DNS注入装置のメモリ漏えいを利用し、GFW内部を直接観測

4. GFWを回避する方法

回避手法	説明
VPN	クライアントと国外サーバー間に暗号化トンネルを張り、IP／ドメイン封鎖を回避します。
Tor とブリッジノード	多段暗号化と分散型中継ノード（Obfs4、Snowflakeなど）を用い、DPIや能動探査をすり抜けます。
プラガブル・トランスポート	Obfs3/Obfs4、Meek、FTEなどで通信をランダムデータや一般的プロトコル（HTTP/TLS）に偽装します。
ドメイン前置（Domain Fronting）	大手CDN／クラウドサービスの正当ドメインをホスト名に使い、本来アクセスしたい封鎖ドメインへの経路を隠蔽します。
デコイルーティング（Decoy Routing）	提携ISP側の「おとりルーター」でトラフィックを乗っ取り、封鎖サイトへの迂回ルートを構築します。
プロキシ&P2P系ツール	Freegate、Psiphon、Lantern、I2Pなど、多重プロキシやピアツーピア伝送で検閲を回避します。

5. 研究が直面する主な課題

- **観測拠点の不足と可視性の制約**
- **GFWのブラックボックス化**
- **倫理・法規制リスク**