How China Detects and Blocks Shadowsocks

Alice, Bob, Carol (GFW Report)
Jan Beznazwy
Amir Houmansadr (University of Massachusetts Amherst)

https://gfw.report/publications/imc20/en/

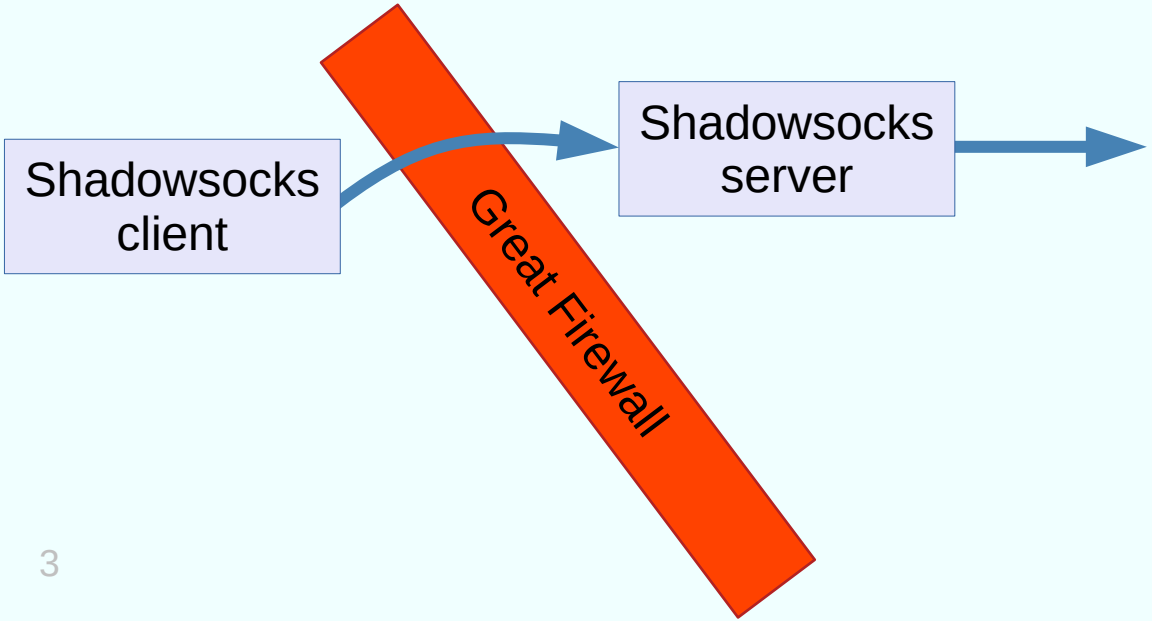
ACM Internet Measurement Conference 2020

Overview

The Great Firewall of China detects and blocks **Shadowsocks** using a combination of **passive traffic analysis** and **active probing**.

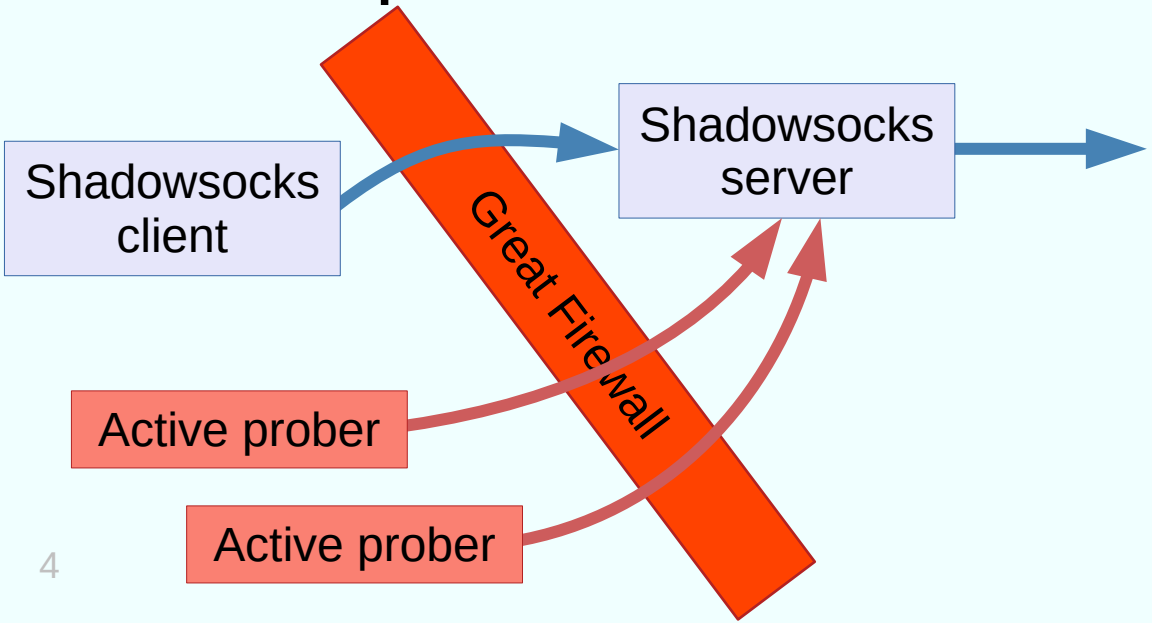
Shadowsocks

Shadowsocks is an encrypted proxy protocol, designed to be difficult to detect.



Active probing

1. Identify *possible* Shadowsocks connections.
2. Send probes to the server to confirm.



Live server experiment

- Run Shadowsocks servers outside China, connect to them from inside.
- Shadowsocks-libev and OutlineVPN.
- September 2019 to January 2020.

Summary of results

- Probing is triggered by the first data packet in a TCP connection, and is more likely when the packet has high entropy and certain lengths.
- There are several probe types, some based on replay and some not.
- Probes come from many source IP addresses, but are evidently centrally managed.
- It is possible to mitigate the effects of active probing by altering packet lengths or changing how servers respond to unauthenticated probes.

Code, data, and contact:

https://gfw.report/publications/imc20/en/

Presentation video with transcripts
in English and Chinese:

https://gfw.report/talks/imc20/en/

https://gfw.report/talks/imc20/zh/

Anonymous pad for questions:

https://pad.riseup.net/p/imc20-shadowsocks-keep