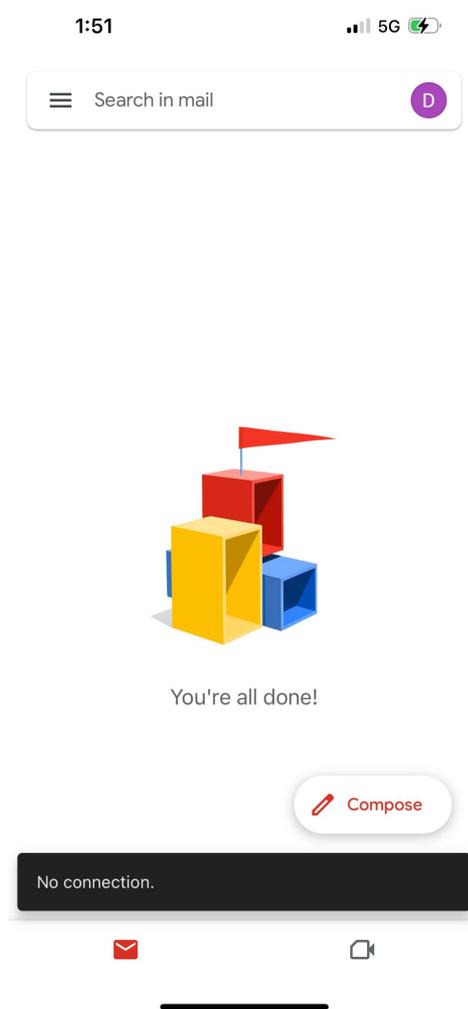
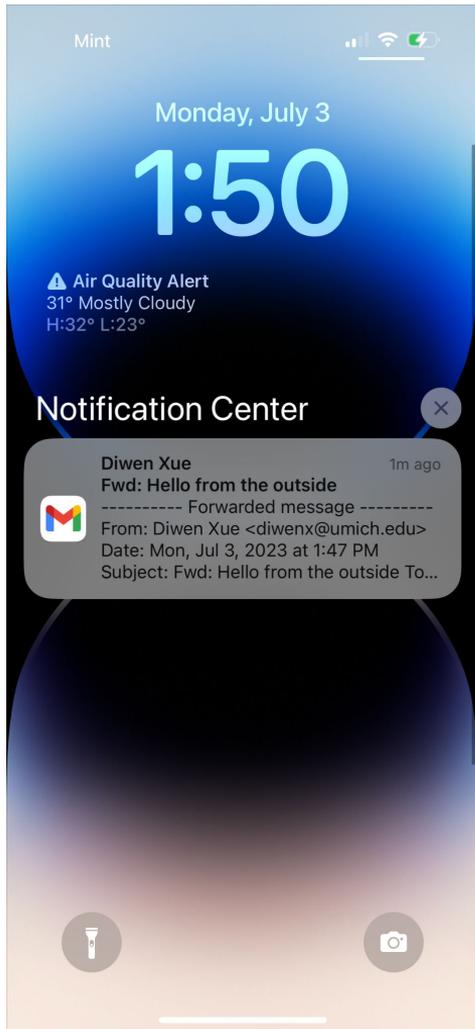


The Use of Push Notification in Censorship Circumvention

Diwen Xue, Roya Ensafi

FOCI 2023

University of Michigan



Example: Gmail in China

Direct connections to/from Google servers are blocked

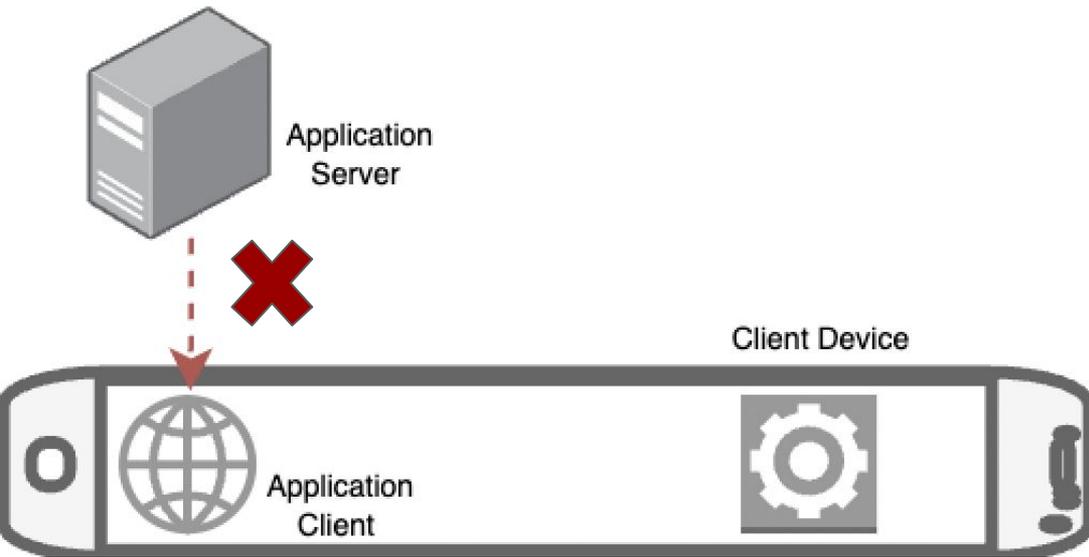
Yet, users are still prompted with push notifications when a new email arrives.

- Includes subject lines and the beginning of the body.

Push Notification

(a.k.a Cloud Messaging)

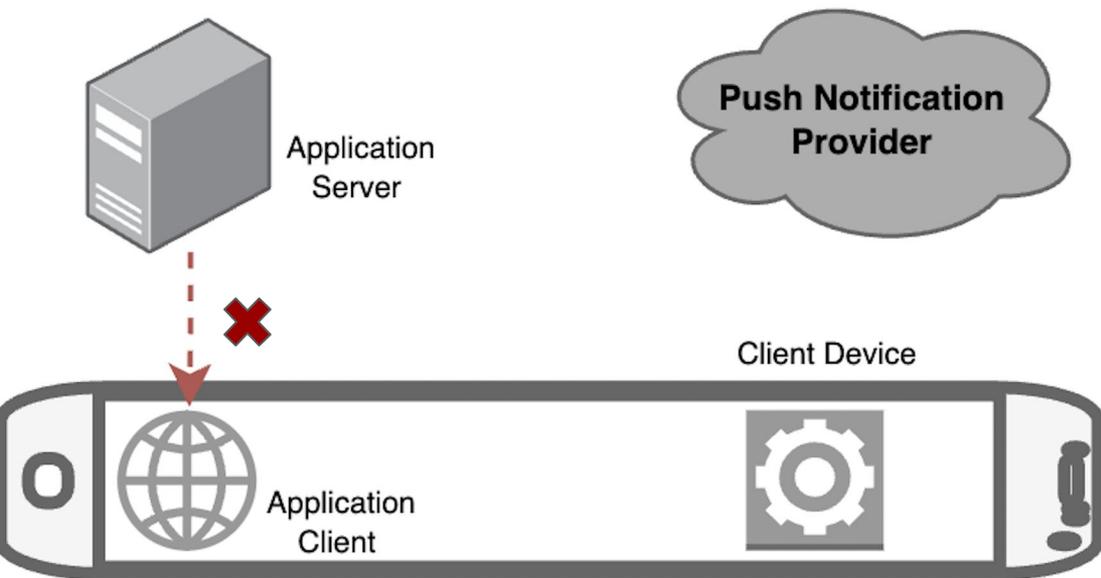
- Apple's APNs, Google's FCM, etc
- Enable applications to transmit time-sensitive information to users



Push Notification

(a.k.a Cloud Messaging)

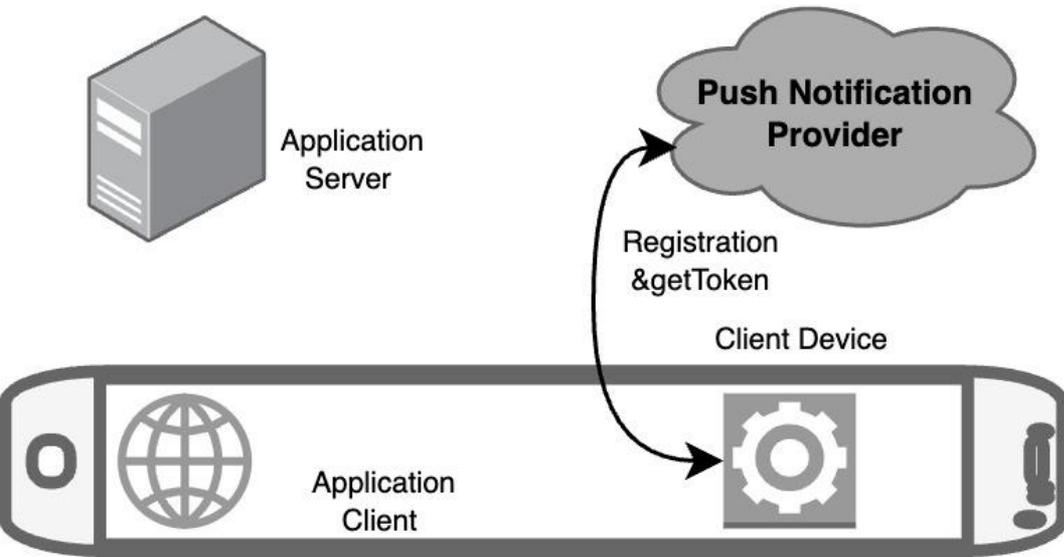
- Apple's APNs, Google's FCM, etc
- Enable applications to transmit time-sensitive information to users



Push Notification

(a.k.a Cloud Messaging)

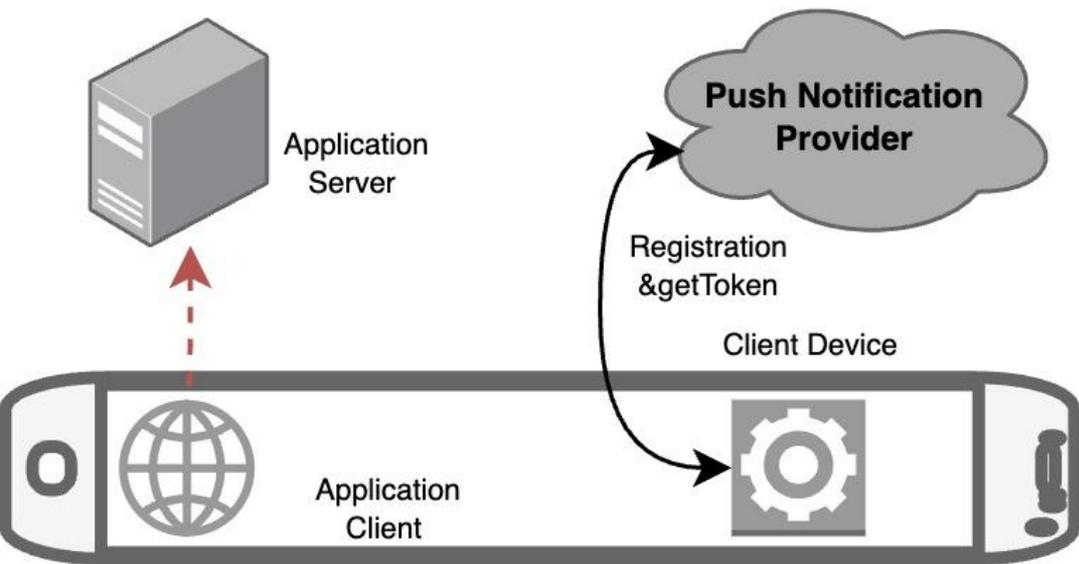
- Apple's APNs, Google's FCM, etc
- Enable applications to transmit time-sensitive information to users
- Messages are **relayed by service providers' networks**
- Publish/Subscribe model



Push Notification

(a.k.a Cloud Messaging)

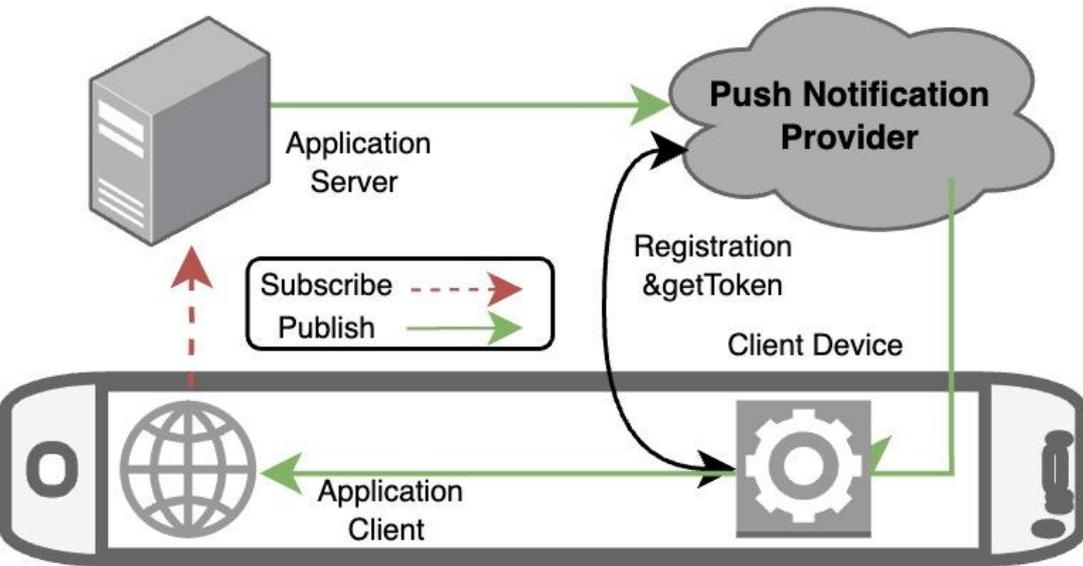
- Apple's APNs, Google's FCM, etc
- Enable applications to transmit time-sensitive information to users
- Messages are **relayed by service providers' networks**
- Publish/Subscribe model



Push Notification

(a.k.a Cloud Messaging)

- Apple's APNs, Google's FCM, etc
- Enable applications to transmit time-sensitive information to users
- Messages are **relayed by service providers' networks**
- Publish/Subscribe model



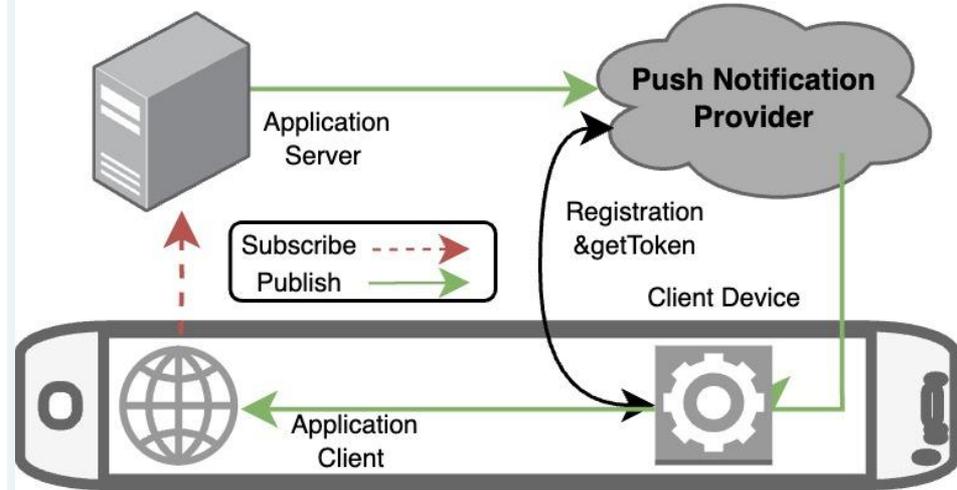
Push Notification

(a.k.a Cloud Messaging)

- Apple's APNs, Google's FCM, etc
- Enable applications to transmit time-sensitive information to users
- Messages are **relayed by service providers' networks**
- Publish/Subscribe model

Push Notifications as One-way Channels

- No direct connection between app server and app client required.
- Functional even when the app is censored down to the IP level.



Push Notifications for Censorship Circumvention

pros:

- **High collateral damage.**
 - Push Notification as a means to reach end-users, no substitute.
 - Blocking one service provider affects all apps relying on it, noticeable effect from end-users.

Push Notifications for Censorship Circumvention

pros:

- **High collateral damage.**
- **Low cost, low latency, acceptable bandwidth.**
 - Operate in real-time
 - Customizable with upto 4KB of payloads for a single notification.

Push Notifications for Censorship Circumvention

pros:

- **High collateral damage.**
- **Low cost, low latency, acceptable bandwidth.**
- **More plausible fingerprints.**
 - No mimicry. Traffic routed through legitimate connections to actual notification endpoints.

Push Notifications for Censorship Circumvention

pros:

- High collateral damage.
- Low cost, low latency, acceptable bandwidth.
- More plausible fingerprints.

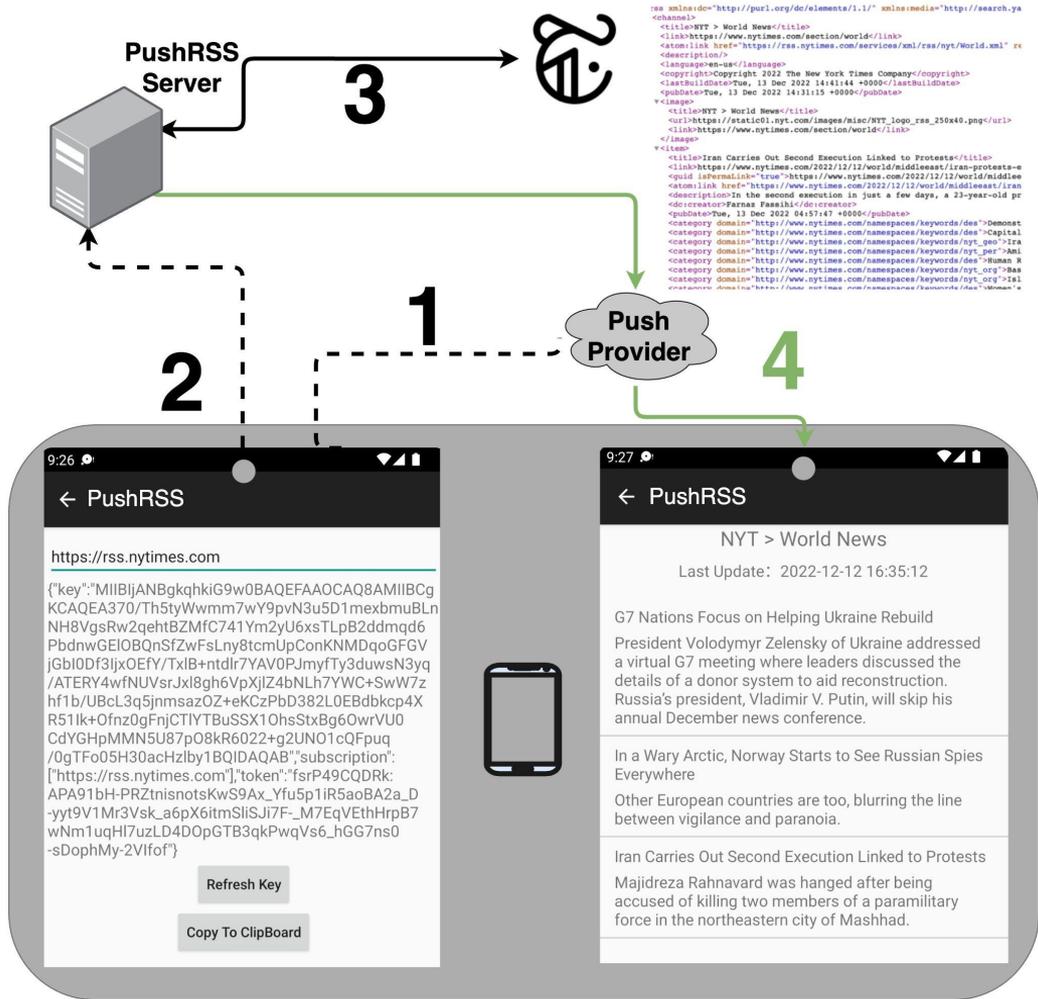
cons:

- Publish/Subscribe model restricts types of communication supported.
- Useful when downstream traffic significantly outweighs upstream.

PushRSS: Blocking-resistant Content Aggregator

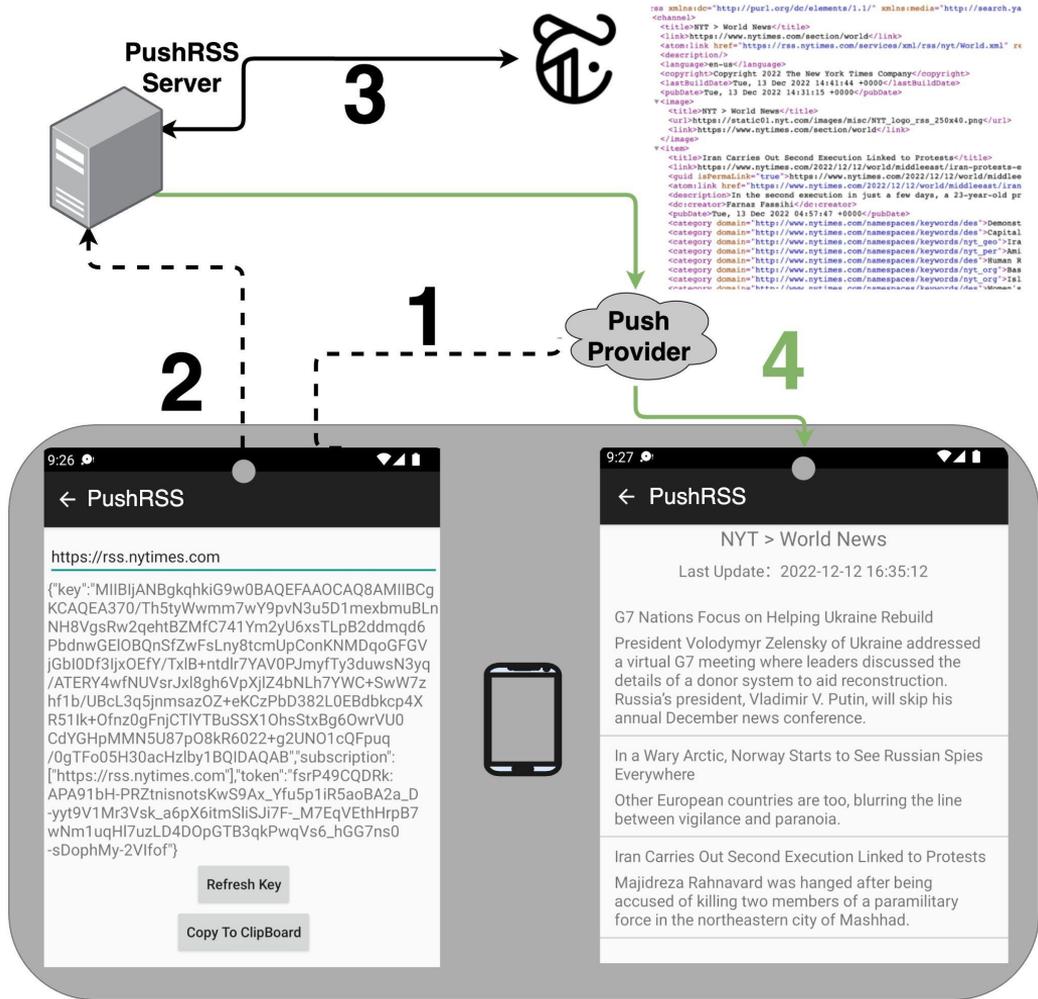
- RSS Aggregator: subscribe to 'feeds', collects latest contents in one place.
- Asymmetric traffic pattern: one-time subscription, regular updates.
- PushRSS routes updates through push notification networks.





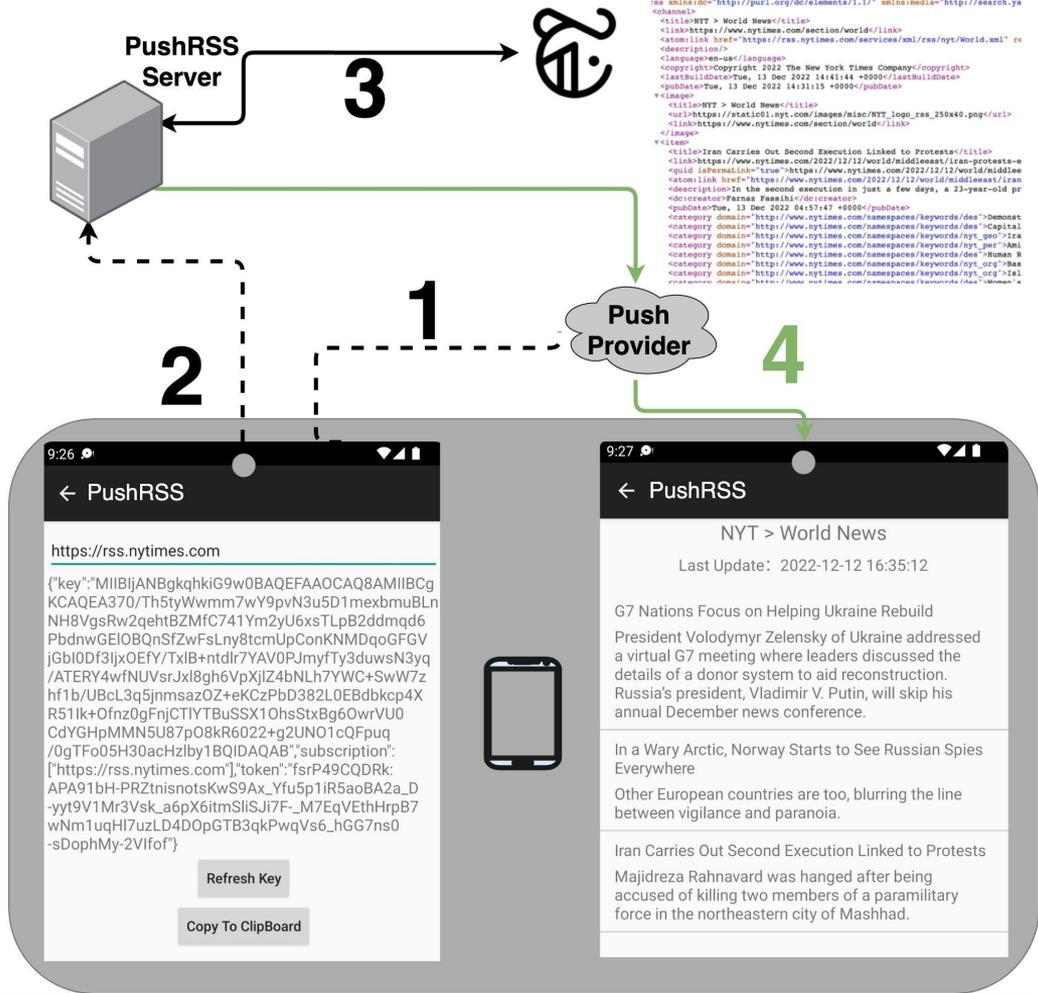
PushRSS: Workflow

1. (One-time only) Registration with push notification providers.
2. (One-time only) Bootstrapping with PushRSS Server



PushRSS: Workflow

1. (One-time only) Registration with push notification providers.
2. (One-time only) Bootstrapping with PushRSS Server.
3. PushRSS server regularly fetches content updates from publishers.
4. Content updates are delivered inside push notification payloads.



PushRSS: Workflow

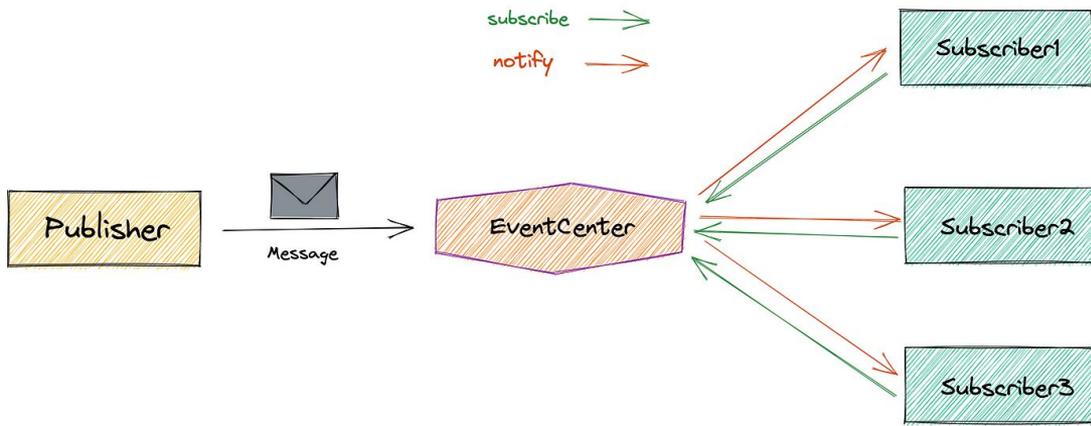
End-to-end Encryption

Reliable Delivery (forward error correction)

Rate limit

----- in the absence of upstream channel

➔ Refer to the paper



PushRSS: Application

- Publish/Subscribe model limits use cases.
- Users cannot request contents on-demand.

RSS Feeds

(Really Simple Syndication) feeds offer another way to get NYTimes.com content. Subscribe to our feeds to get the latest headlines, summaries and links back to full articles - formatted for your favorite feed reader and updated throughout the day.

Terms & Conditions

We allow the use of NYTimes.com RSS feeds for personal use in a news reader or as part of a non-commercial blog. We require proper format and attribution whenever New York Times content is posted on your website, and we reserve the right to require that you cease distributing NYTimes.com content. Please read the Terms and Conditions for complete instructions. Commercial use of the Service is prohibited without prior written permission from NYT which may be requested via email to: nytlg-sales@nytimes.com.

News

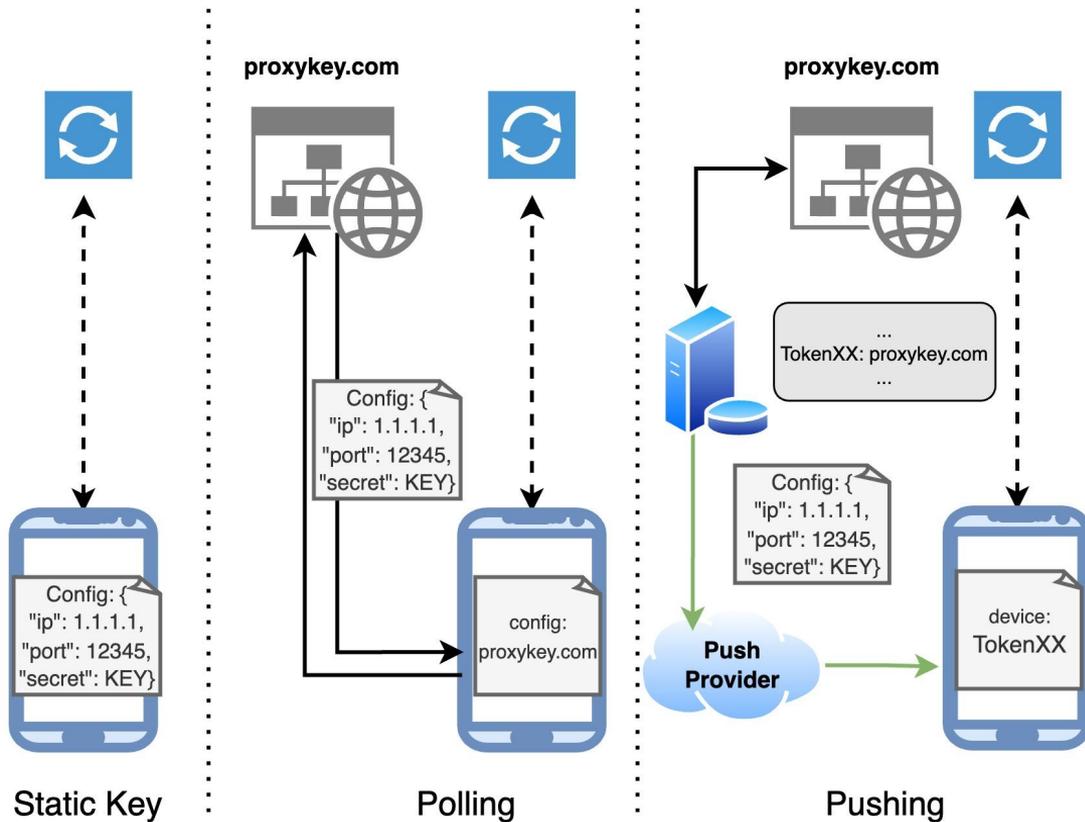
[NYTimes.com Home Page \(U.S.\)](#)

World

World
Africa
Americas
Asia Pacific
Europe
Middle East

PushRSS: Application

- Provide users in censored region continuous feeds from global news agencies / personal blogs.
- Usefulness contingent on the availability of various feeds.
 - Major news publishers already support RSS.
 - Tools exist for individual publishers to convert their contents.



PushRSS: Application

- Facilitate bootstrapping of existing circumvention systems by providing an alternative to “polling”.
- Improved efficiency and blocking resistance.

→ Telegram in Russia

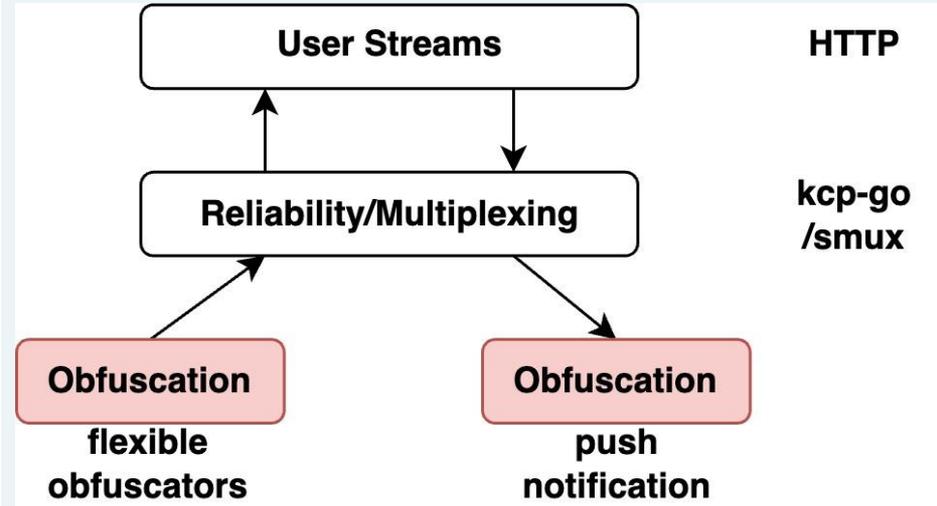
Service notifications

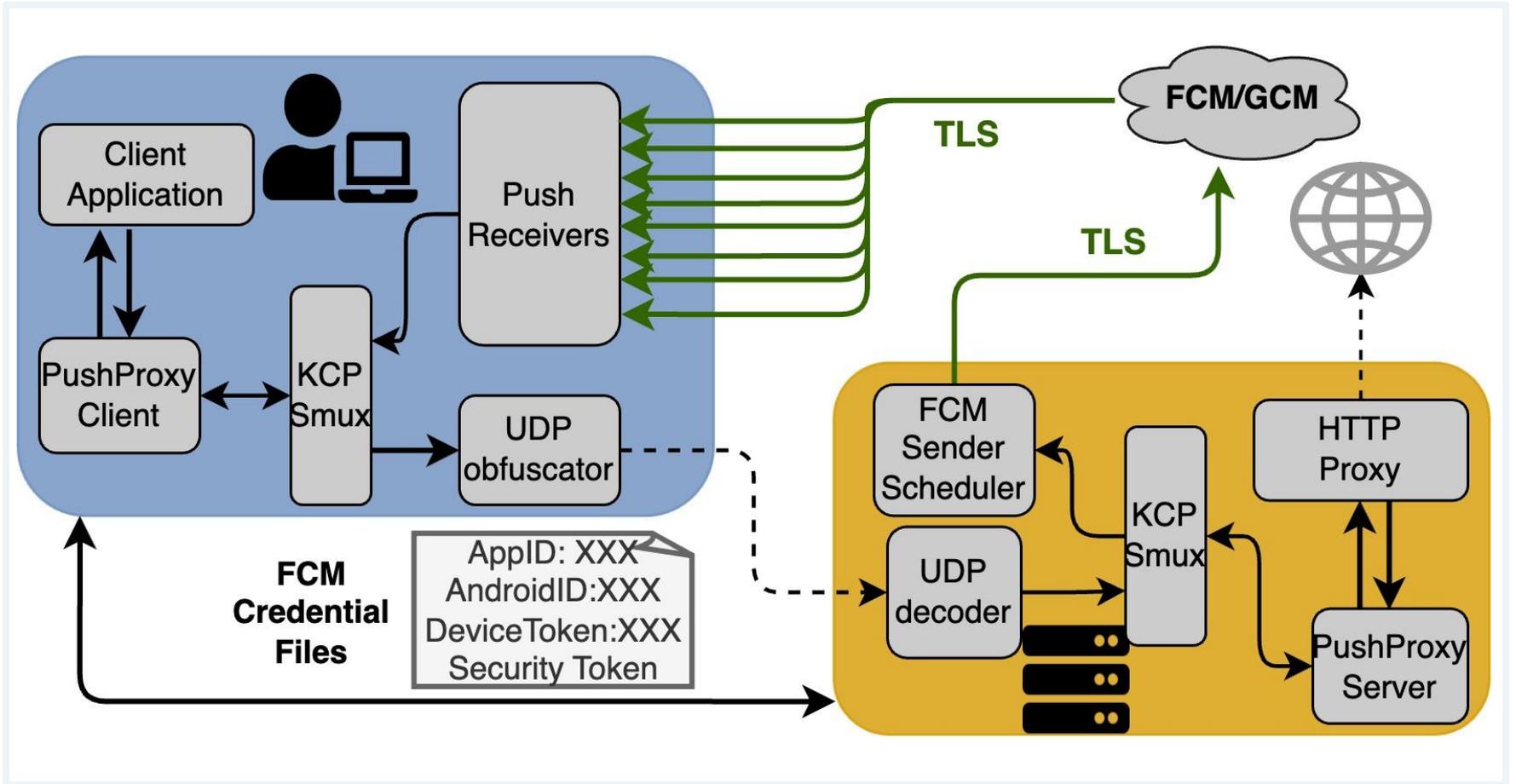
The following notifications can be used to update app settings.

Type	Extra custom arguments	Description
DC_UPDATE	data.custom.dc – number of the data-center data.custom.addr – server address with port number in the format <code>111.112.113.114:443</code>	In case the client gets this notification, it is necessary to add the received server address to the list of possible addresses. In case the address of the first DC was passed (<code>dc=1</code>), it is recommended to call it immediately using <code>help.getConfig</code> to update dc-configuration.

PushProxy: Asymmetric proxy using push notification

- Route downstream traffic through push notification, keep upstream independent.
- The key benefit is to mitigate adversary's ability to perform traffic analysis per-flow.
- Better bandwidth and NAT compatibility, compared to other asymmetric proxy design.





Evaluation: Availability

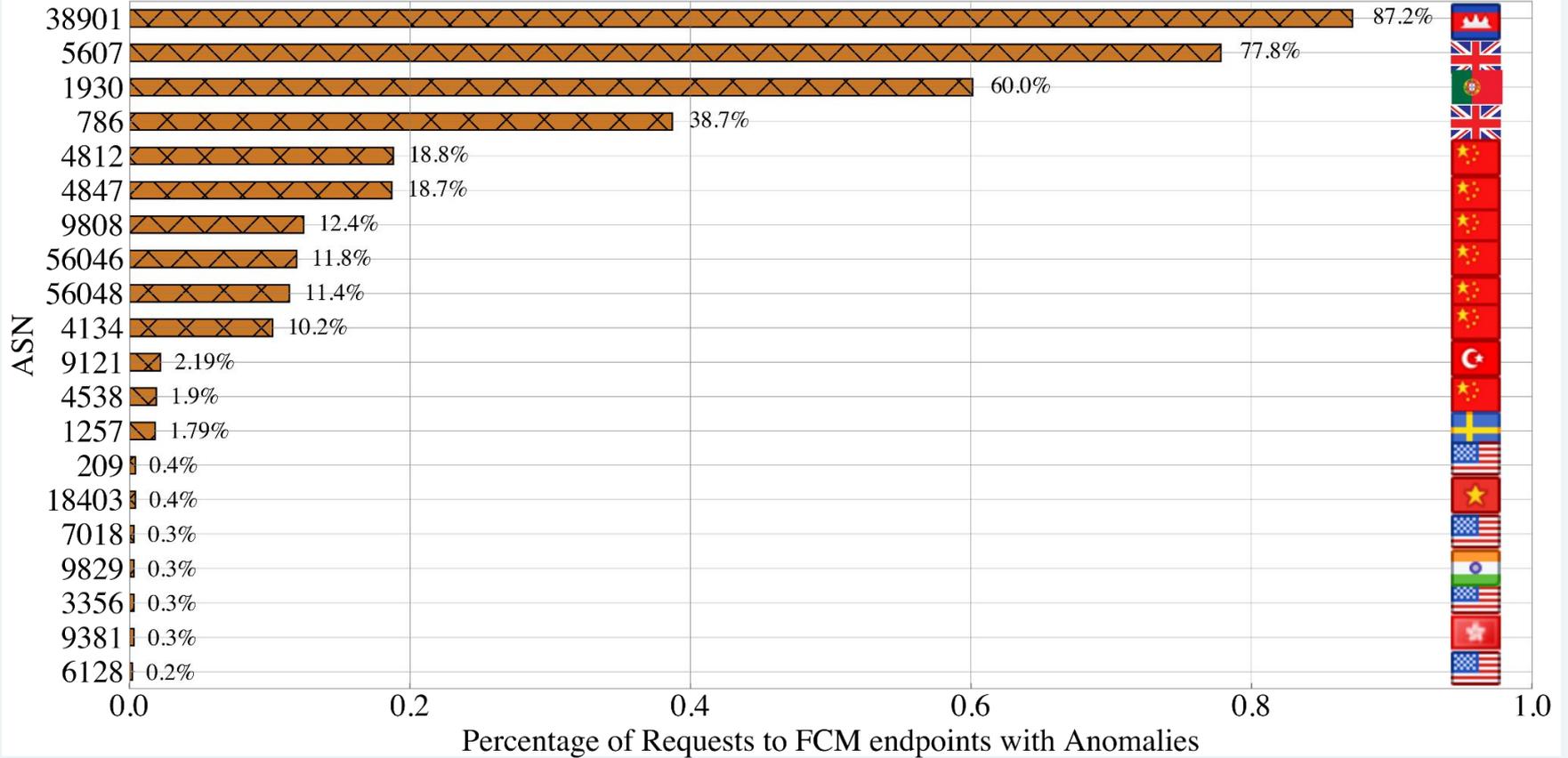
- To use push notification for effective circumvention, the service itself cannot be blocked.

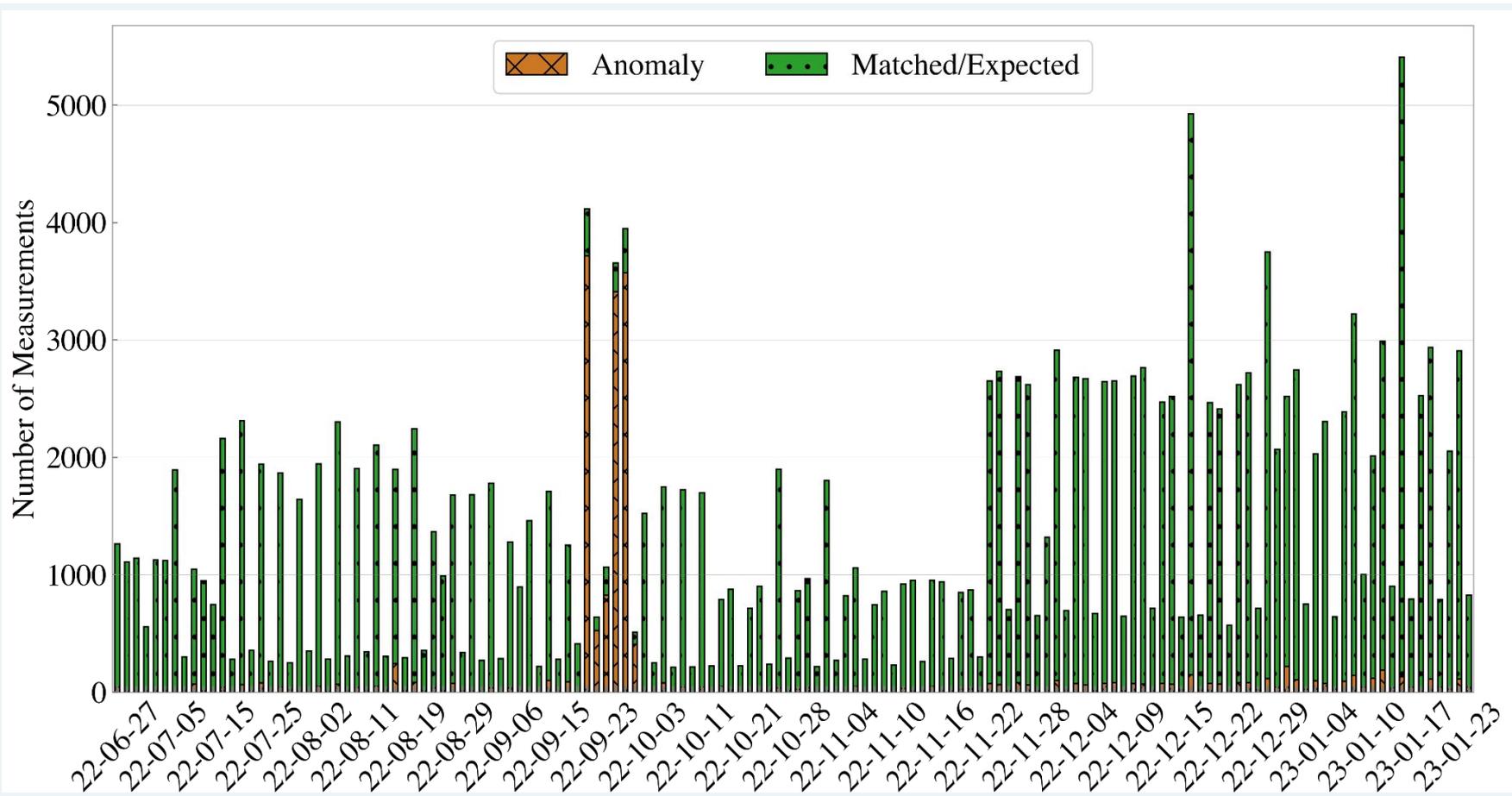
We ask:

- Which networks (ASes) actively block FCM connections? Does FCM offer high availability over time?

Methodology:

- Peer-reviewed technique: Hyperquack
 - First builds a template of expected behaviors, then test for signs of blockings.
 - All FCM domain names, 1632 ASes, over 7 months in 2022.

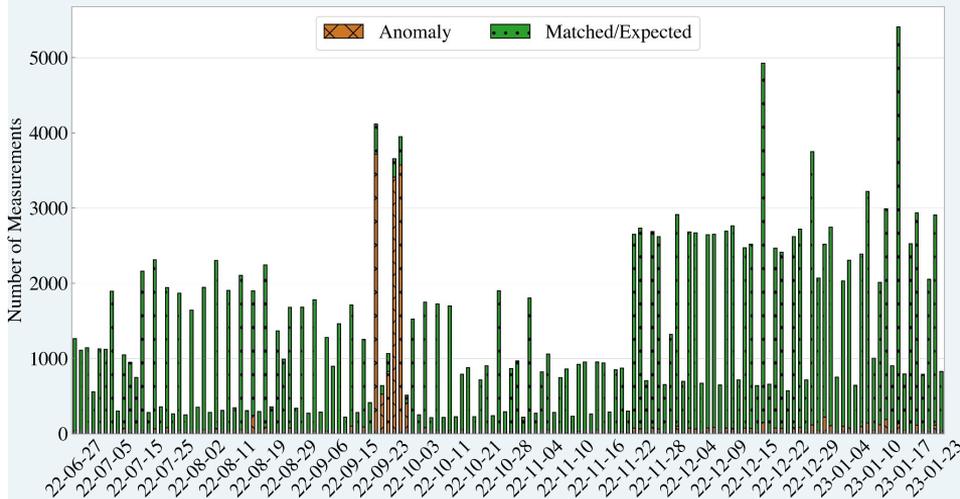




Evaluation: Availability

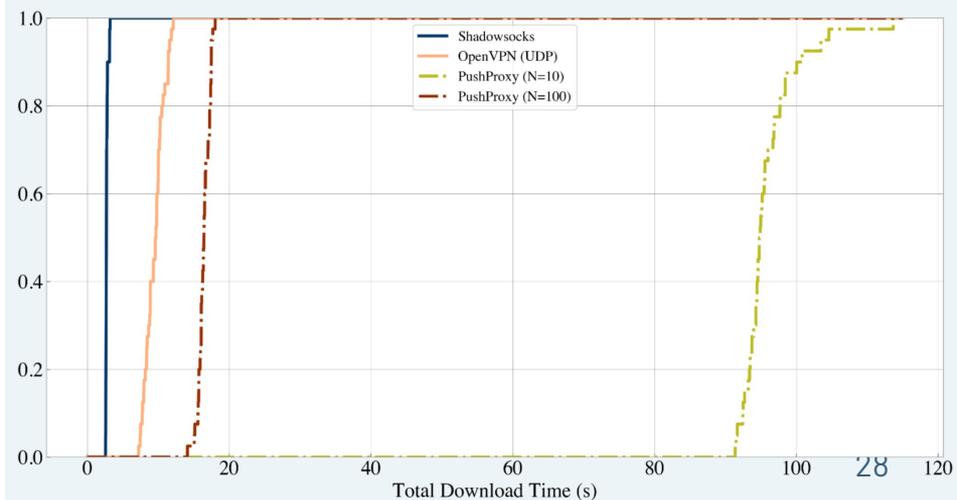
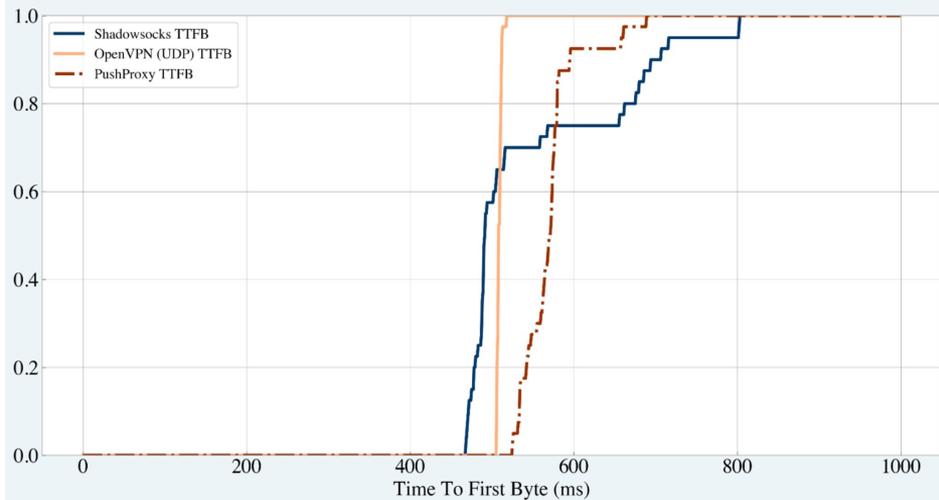
- Blocking in China did not target FCM, but all subdomains of the form ***.google.com**.
- Blocking lifted for FCM on Oct 1, 2022.
- However, ***.google.com** remain blocked as of June 2023 (e.g., {docs/groups/sites}).

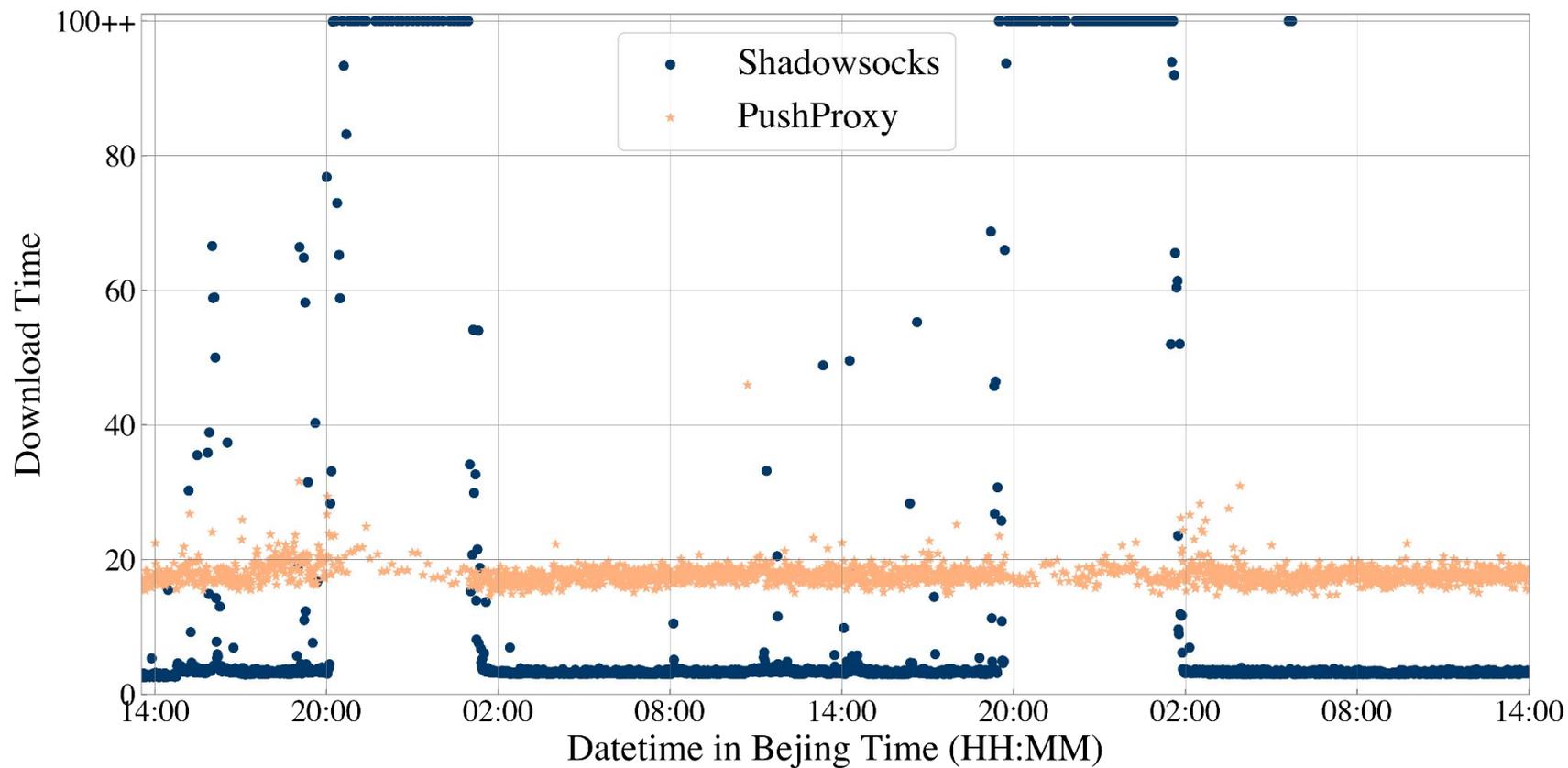
→ Exception was made for FCM, presumably due to high collateral damage.



Evaluation: Performance

- Compare PushProxy with OpenVPN and Shadowsocks for performance.
- Client in China, Proxy and web server in the US. Median RTT = 244ms.
- Comparable in terms of TTFB and bandwidth (with concurrent push notification connections)





Limitations

- **Traffic Analysis**

- High-frequency, high-bandwidth push notifications are atypical.
- De-anonymization of subscribers to sensitive feeds by traffic correlation.

- **Platform Censorship**

- Disable/throttle push notifications for circumvention apps
- Service abuse?

China introduces new regulation forbidding push notifications from unlicensed news sources

 [See all tags](#)

[Read more](#) 

"China to limit news notifications to licensed publishers after weeks of discussion about human trafficking and Ukraine" 3 March 2022

Limitations

- **Traffic Analysis**
 - High-frequency, high-bandwidth push notifications are atypical.
 - De-anonymization of subscribers to sensitive feeds by traffic correlation.
- **Platform Censorship**
 - Disable/throttle push notifications for circumvention apps

→ It has its limitations, but still a **viable circumvention transport** that complements existing approaches.

The Use of Push Notification in Censorship Circumvention

Diwen Xue, Roya Ensafi

FOCI 2023

University of Michigan