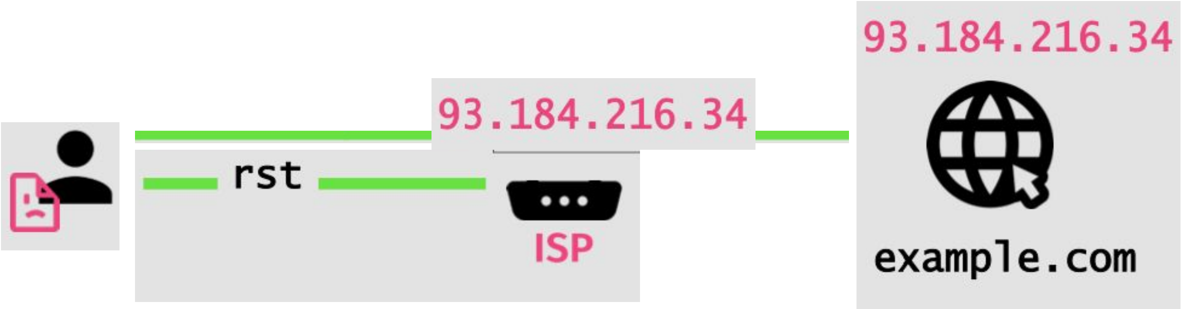
Internet censorship in Iran and how to evade it

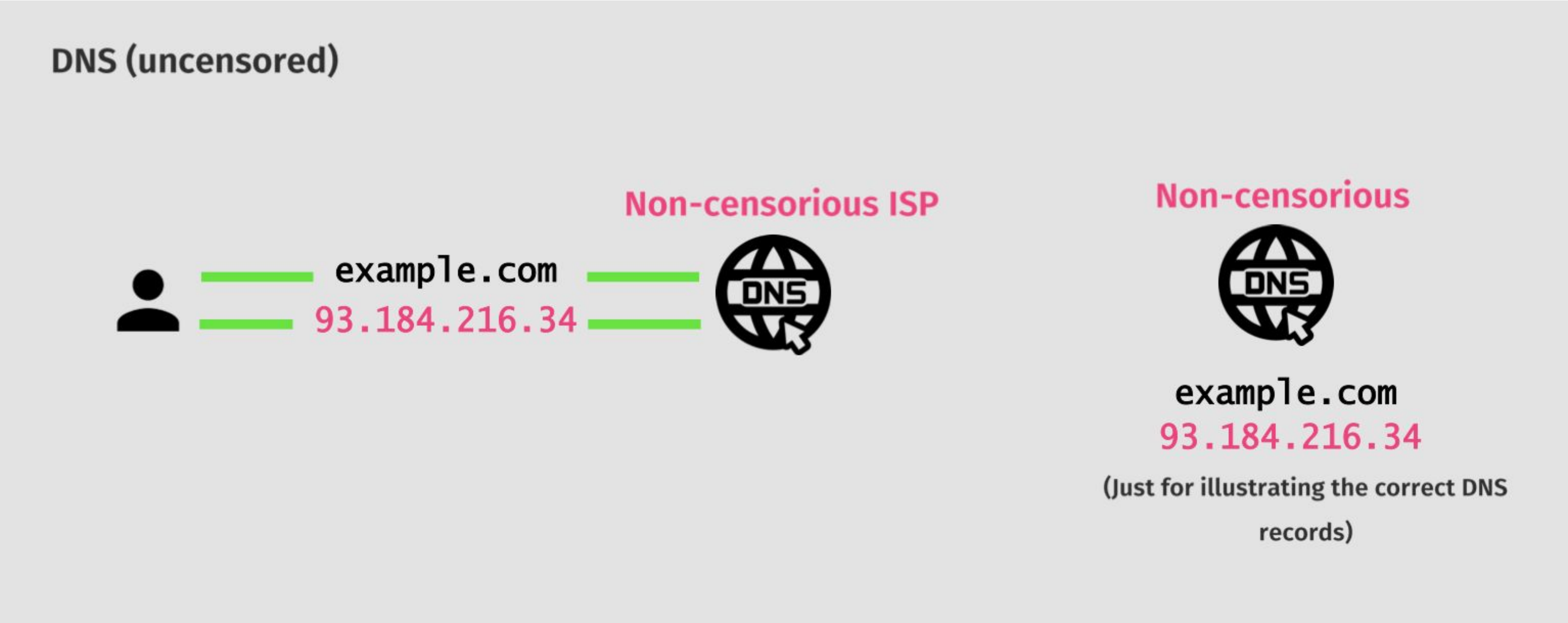
Gurshabad Grover & Alex Linton
12 June 2024

Recap: common methods of online censorship

IP-based censorship

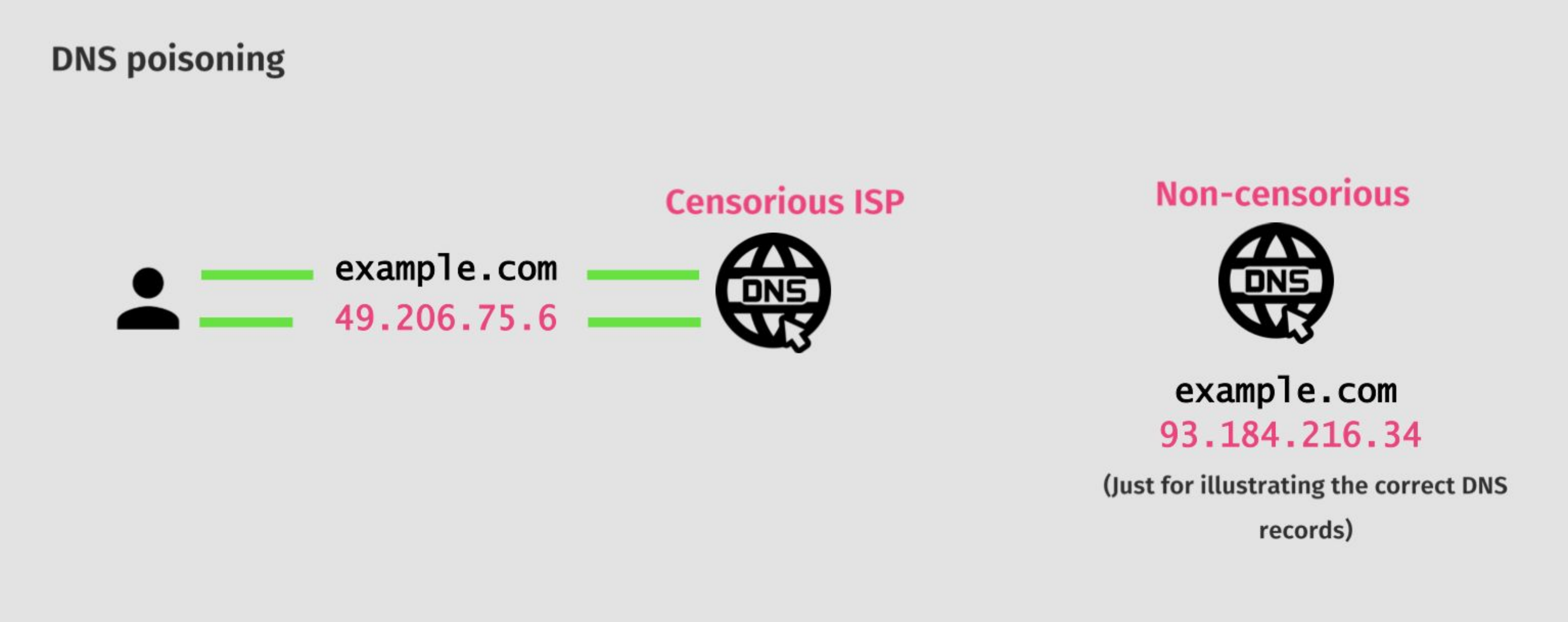


DNS-based censorship

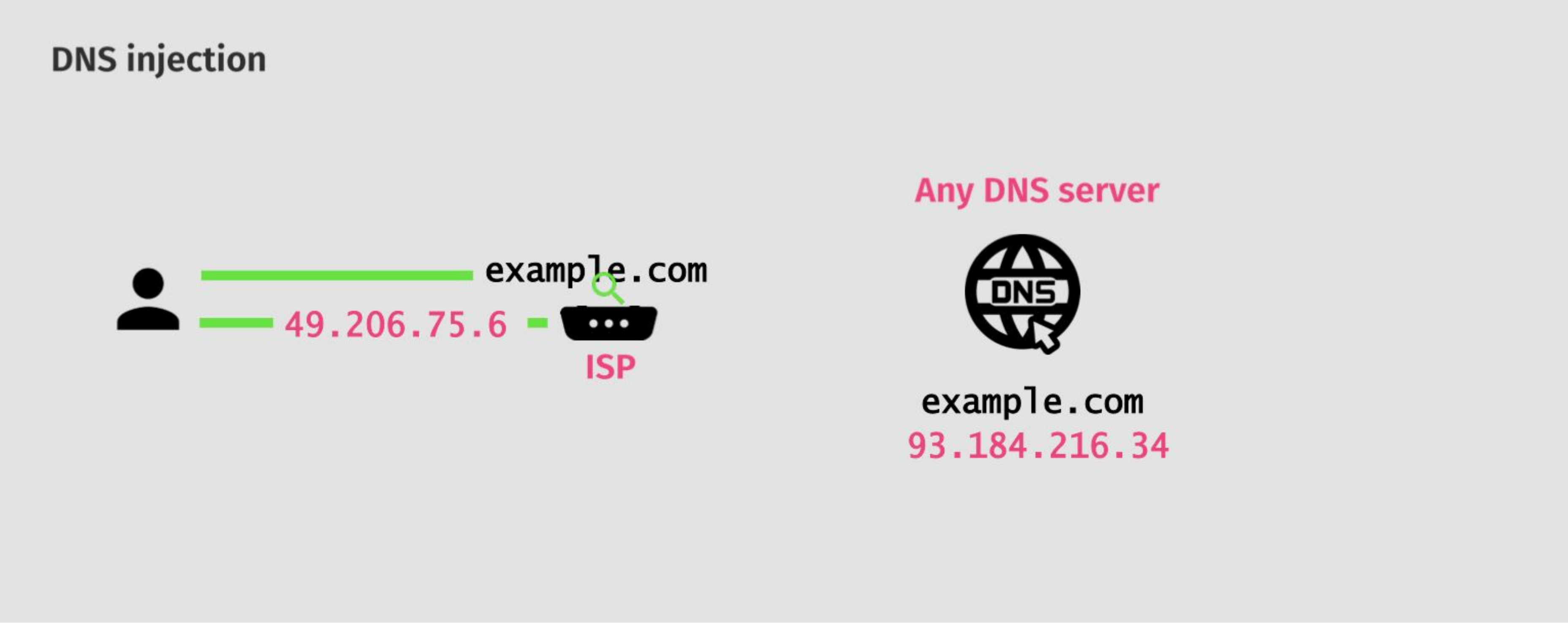


(Just for illustrating the correct DNS records)

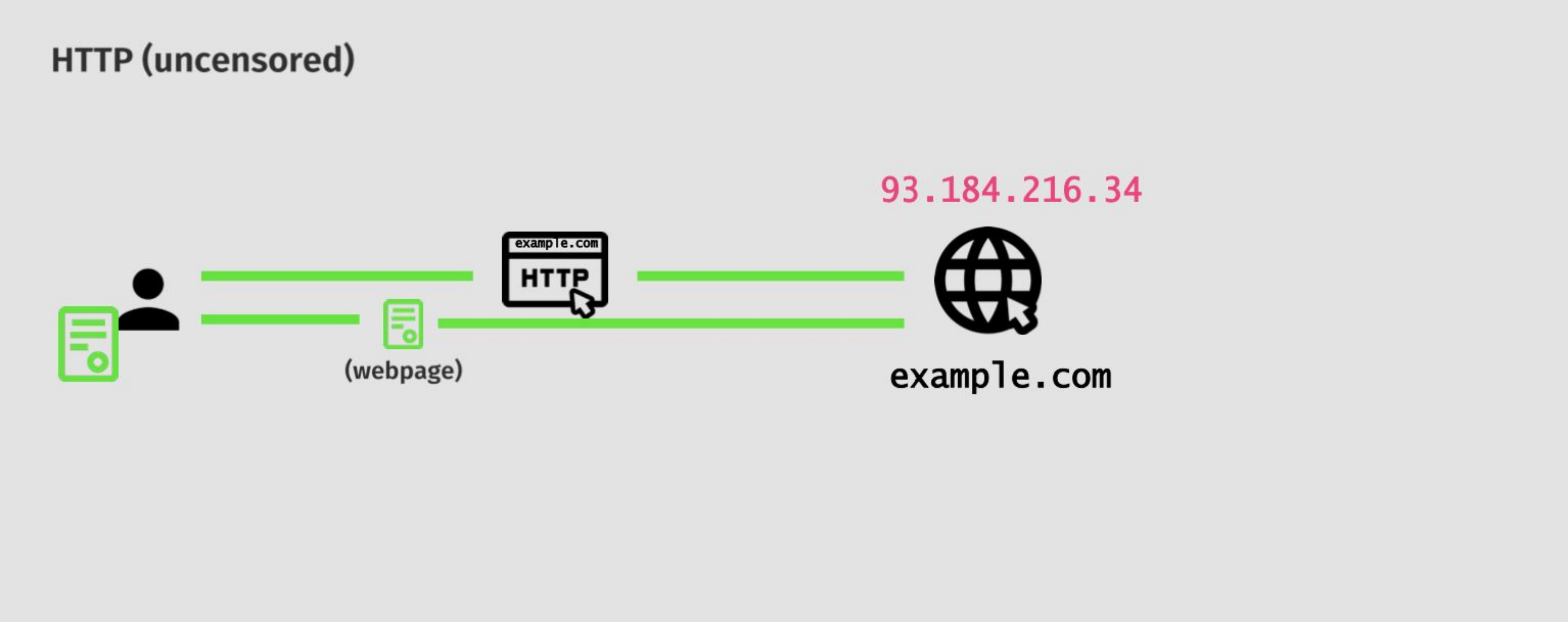
DNS-based censorship



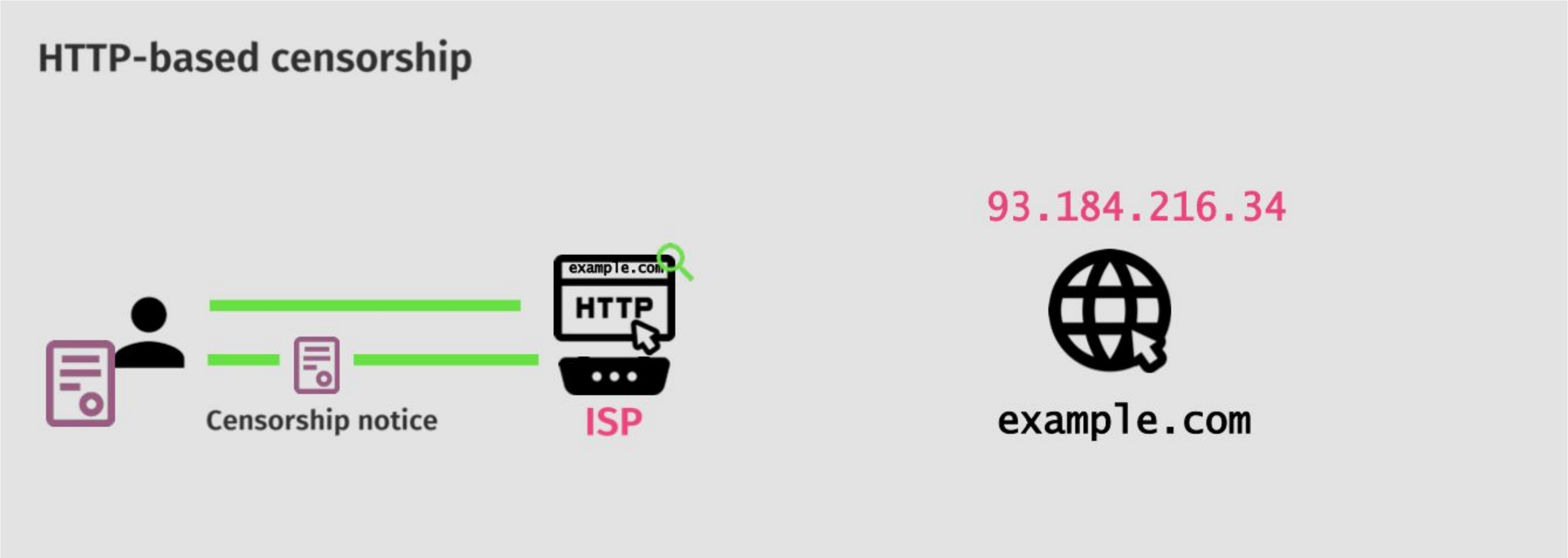
DNS-based censorship



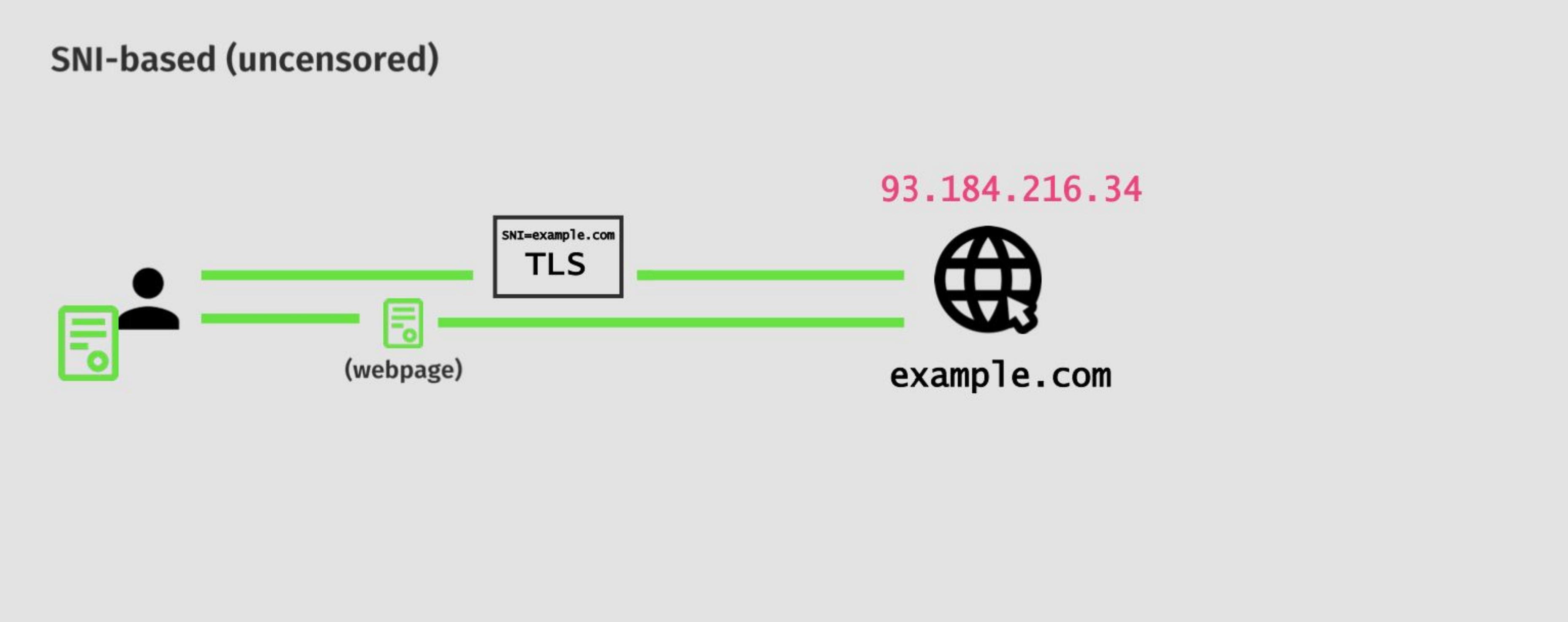
HTTP-based censorship



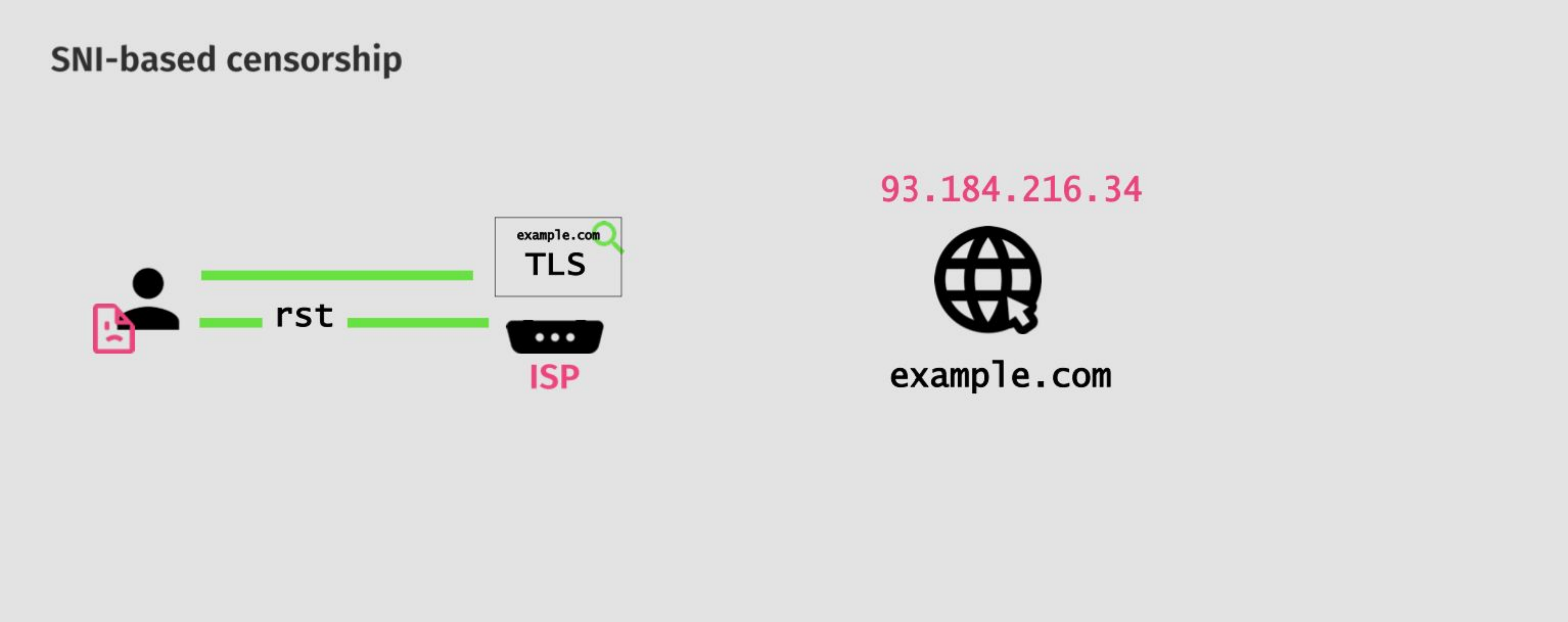
HTTP-based censorship



TLS-based censorship



TLS-based censorship



State of censorship in Iran

- Largely centralized infrastructure
  - All Iran’s ISPs were connected to five international gateways, operating through two entities (2020)
  - Access to the global Internet was centralised to two government-controlled gateways

IRANIAN INTERNET INFRASTRUCTURE MAP 2019

Domestic Peers / ISPs

The majority of the connections we see on this map are the "domestic peers" or domestic Internet Servic Providers (ISPs) that are connecting homes, mobile networks, and institutions to domestic and international networks.

This is the first layer of Internet Service Providers (ISPs) that are connected directly to the international gateways. A second layer smaller ISPs connect through these "first layer" which are major providers, illustrated in this map.

TIC International Gateways

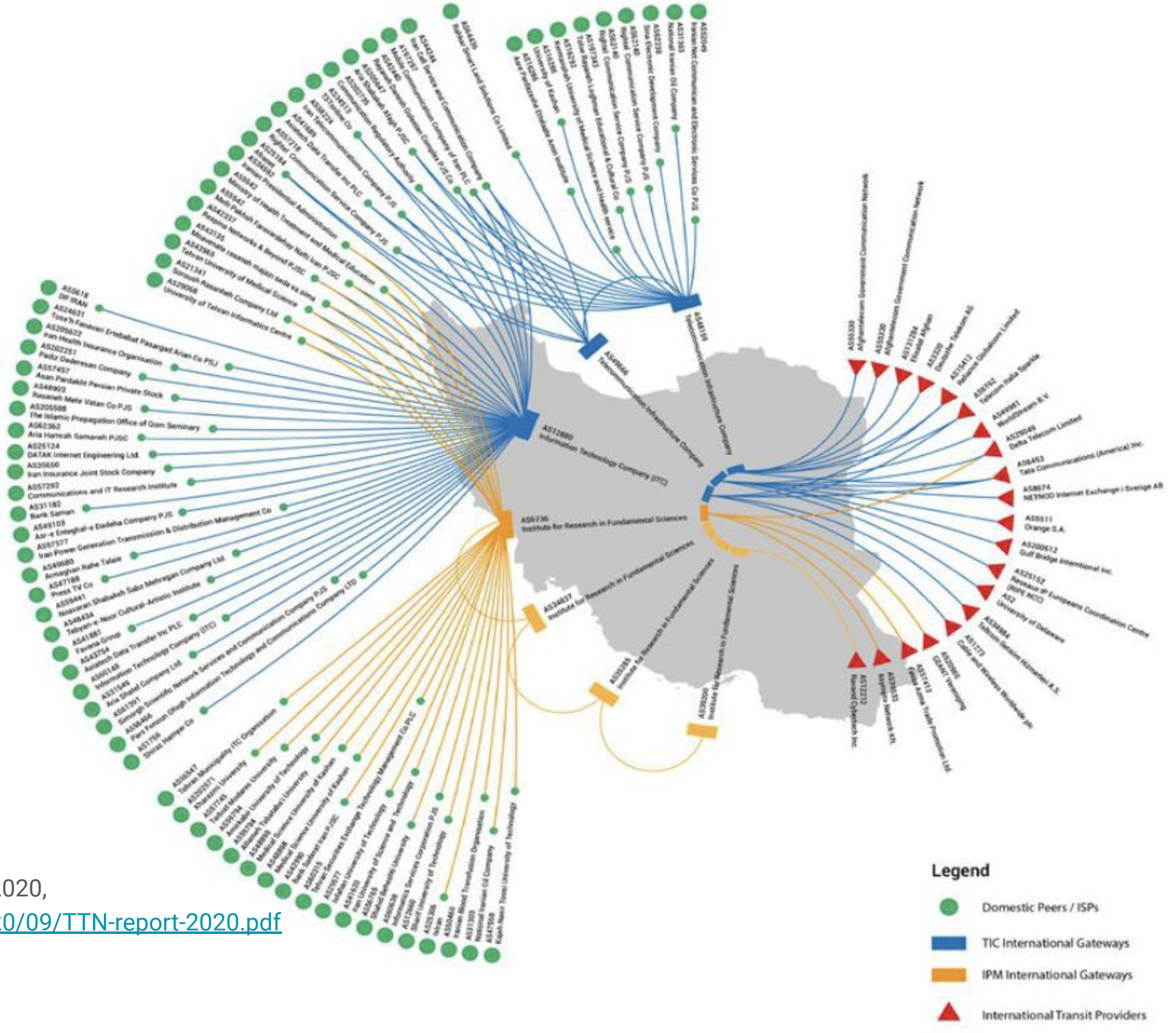
The Telecommunication Infrastructure Company (TIC) is the sole provider of IP communication infrastructure to all private and public operators in the Iran. TIC is also the sole party for all international gateways and IP capacity and connectivity services in the country. It sits under the Ministry of Information, Communication and Technology (ICT), which oversees all IP communication infrastructure across the country.

IPM International Gateways

Although not as large as the TIC Gateway, this older international gateway from the Institute for research in fundamental sciences (IPM), is the only other international gateway in Iran and serves the Internet to research and educational institutes.

International Transit Providers

International transit providers are companies providing international connectivity to the Iranian network, via the two gateways mentioned above.



AS48159 Telecommunication Infrastructure Company
AS49666 Telecommunication Infrastructure Company
AS12880 Information Technology Company (ITC)
AS6736 Institute for Research in Fundamental Sciences
AS34837 Institute for Research in Fundamental Sciences
AS39285 Institute for Research in Fundamental Sciences
AS39200 Institute for Research in Fundamental Sciences
Legend
Domestic Peers / ISPs
TIC International Gateways
IPM International Gateways
International Transit Providers

Source: 'After Blood and Shutdowns', ARTICLE 19, 2020, https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf

State of censorship in Iran

- Censorship at ‘National firewall’:
  - (IP, DNS and HTTP/S)
  - Protocol filter
  - Backup ‘National Internet Network’

- At the ISP level
  - IP, DNS and HTTP/S

Protocol filter

- Exists in tandem with standard censorship
- Monitors for non-standard and obfuscated traffic on ports 53 (DNS), 80 (HTTP) and 443 (HTTPS). DoT and UDP may have been added now.
- Some IP addresses are affected more than others
- **Traffic on other ports is unaffected (for now)**

National firewall

- Centralized facility

- Methods:
  - DNS (injection)
  - HTTP HOST and keyword filtering
  - HTTPS filtering, sometimes SNI and sometimes (SNI, IP)
  - Filtering of HTTP/3 traffic
  - IP-based filtering

At the ISP level

- Some traffic does not reach the ‘national firewall’

- Methods:
  - TLS resets or timeouts, based on SNI and sometimes (SNI, IP)
  - DNS over TLS blocked
  - HTTP HOST and keyword filtering
  - (some) IP-based re-rerouting or blocking

Evasion/circumvention

- Overall strategy must counter:
    - Protocol filter
    - IP-based blocking
    - DNS-based blocking
    - HTTP(S)-based blocking

Censorship circumvention: scope

- Methods do not evade internet shutdowns, only targeted blocking
- Focus on simplicity
  - Methods do not rely on masking traffic as other traffic
  - Rely on advancements in protocols with censorship resilience
  - Ideally, require only server-side changes (or minimal client-side changes)
  - Proxy-less!

Scope and other considerations

- Unavailable due to sanctions:
  - Github, Amazon Cloud, and Google Cloud
  - (US Government exception is helping ease this)

- IP-blocking is the hardest to evade, most methods here rely on the IP not being blocked
  - Using service providers that are not blocked
  - Using not well-known IP addresses

Short-term strategy in Iran

- Hosting HTTPS server on a non-standard port

- Censors make mistakes, and the world is moving!

Method #1: QUIC

- Why?
  - QUIC already encrypts the initial packets of a connection.
  - Keys of this initial encryption are known to observers of the connection, so technically, the SNI is obfuscated (but not encrypted).
  - State-full censorship devices can block, which are not deployed in Iran

- Evades only HTTPS (SNI)-based filtering

- Con: conflicting evidence whether QUIC as a protocol will be entirely blocked or not

Method #2: Encrypted Client Hello (ECH)

- Why?
  - SNI gets encrypted in ECH

- Evades: only HTTPS (SNI)-based filtering

- Con: ECH-enabled TLS traffic 'sticks out', i.e. it can be selectively targeted and blocked. Iran could block all TLS traffic that uses ECH (with large collateral).

Method #3: DNS over TLS

- Why?
  - DNS request gets encrypted
  - Android and iOS ship with DoT support, fairly easy to implement

- Evades: DNS-based censorship

- Cons
  - Already evidence some Iranian ISPs are interfering with DoT requests based on the IP and SNI of the DNS server.
  - Need to select a DoT server instead of the relying on the system/client one (poisoning is still possible!).
  - DoT runs over a specific port (853) and can be easily blocked entirely.

Method #4: DNS over HTTPS

- Why?
  - DNS request gets encrypted
  - Android and iOS ship with DoT support, fairly easy to implement
- Evades: DNS-based censorship
- Cons
  - Already evidence some Iranian ISPs are interfering with DoH requests based on the IP and SNI of the DNS sever.
  - Need to select a DoT server instead of the relying on the system/client one (poisoning is still possible!).
  - (DoH runs on the HTTPS port, so much more censorship resilient!)

Method #5: Domain fronting

- Prerequisites:
    - Need to find a domain hosted on the same hosting service.
    - Say our domain is blocked.com and another domain hosted on the service is notblocked.com.
    - Use notblocked.com in the SNI, but in the (encrypted) HTTP request, use blocked.com in the HOST header. The service will forward the HTTP request to blocked.com
    - Need to find (or host) an innocuous domain name on the same hosting service.

- Evades: SNI-based censorship

- Cons
    - Domain fronting is not supported by most major cloud providers (Google, Amazon, Cloudflare stopped in April 2018, Azure stopped in 2022). Fastly may also drop supporting it by February 2024.(*)
    - We will need to find a service that is promising to offer domain fronting in the long-term.
    - Domain fronting stops working if ECH or ESNI is in play.

Method #6: TCP packet segmentation

- Why?
  - Middleboxes aren’t stateful in Iran (yet!)
  - Reducing the TCP window size of the SYN+ACK packet induces the client to segment a request.
- Evades: SNI and HTTP-based censorship
- Pros
  - This only requires a change to the server, and not the client

Method #7: TLS record fragmentation

- Why?
  - All middleboxes aren’t stateful in Iran (yet!)
  - Split the handshake (specifically the SNI) into two TLS messages. Most TLS servers support fragmented TLS messages.
- Evades: SNI and HTTP-based censorship
- Pros
  - Requires a modification to the client (BUT the server should support fragmented TLS records).

Endnotes

- Use methods in conjunction – check out Outline SDK!

- Things keep changing, practical experience and constant iteration is necessary