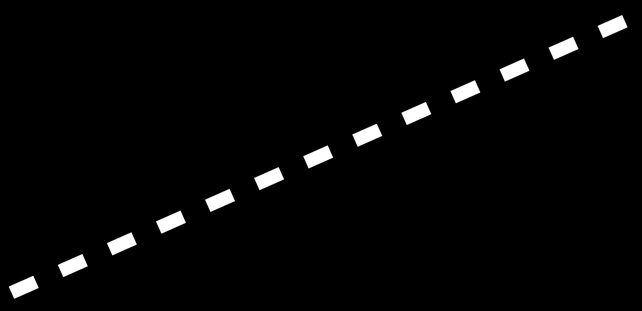
Detecting Network Interference Without Endpoint Participation

Extended Abstract

Sadia Nourin Kevin Bock Nguyen Phong Hoang Dave Levin

Internet Censorship

Internet Censorship



Blockpage

Internet Censorship

RST

Blockpage

Connection
Termination

Internet Censorship

RST

Blockpage

Connection Termination

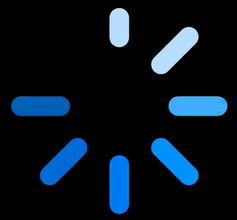
Throttling

Internet Censorship

Blockpage

RST

Connection Termination



Throttling

Packet Drop

Censorship Measurement

- ☐ twitter.com
- ☐ roxypalace.com
- ☑ facebook.com

What is being censored?

How do censors operate?

How does censorship change over time?

Censorship Measurement

- [ ] twitter.com
- [ ] roxypalace.com
- [x] facebook.com

What is being censored?

How do censors operate?

How does censorship change over time?

Censorship Measurement

- [ ] twitter.com
- [ ] roxypalace.com
- [x] facebook.com

What is being censored?

How do censors operate?

How does censorship change over time?

Censorship Measurement

- ☐ twitter.com
- ☐ roxypalace.com
- ☑ facebook.com

What is being censored?

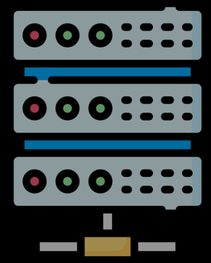
How do censors operate?

How does censorship change over time?

Censorship Measurement

Volunteers

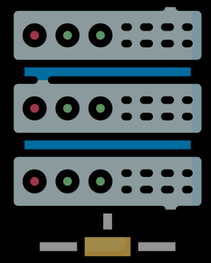
Remote Machines



Censorship Measurement

Volunteers

Remote Machines

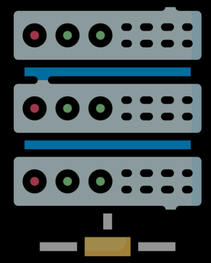


Censorship Measurement

Volunteers

OONI

Remote Machines

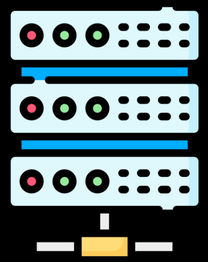


Censorship Measurement

Volunteers

OONI

Remote Machines

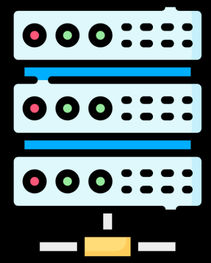


Censorship Measurement

Volunteers

OONI

Remote Machines



Censored Planet

ICLAB

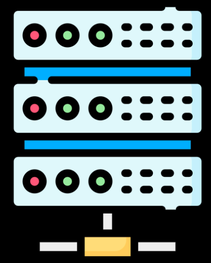
Censorship Measurement

Works great in most countries!

Volunteers

OONI

Remote Machines



Censored Planet

ICLAB

Censorship Measurement

Not great for countries with:

Censorship Measurement

Not great for countries with:

Small Populations

Censorship Measurement

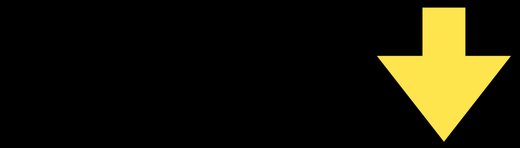
Not great for countries with:

Small Populations

Extremely Repressive Regimes

Censorship Measurement

Not great for countries with:



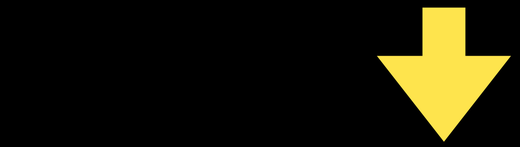
Small Populations

Extremely Repressive Regimes

Low Internet Penetration Rates

Censorship Measurement

Not great for countries with:



Small Populations

Extremely Repressive Regimes

Low Internet Penetration Rates

Poor Internet Infrastructure

Censorship Measurement

We seek to build a new censorship measurement system

- Can longitudinally test millions of domains
- Without needing vantage points or endpoint participation
- Meant to complement NOT replace existing efforts — give insight into hard-to-reach networks or networks not reachable at all

Censorship Measurement

We seek to build a new censorship measurement system

- Can longitudinally test millions of domains
- Without needing vantage points or endpoint participation
- Meant to complement NOT replace existing efforts — give insight into hard-to-reach networks or networks not reachable at all

Censorship Measurement

We seek to build a new censorship measurement system

- Can longitudinally test millions of domains
- Without needing vantage points or endpoint participation
- Meant to complement NOT replace existing efforts — give insight into hard-to-reach networks or networks not reachable at all

Censorship Measurement

We seek to build a new censorship measurement system

- Can longitudinally test millions of domains
- Without needing vantage points or endpoint participation
- Meant to complement NOT replace existing efforts — give insight into hard-to-reach networks or networks not reachable at all

Agenda

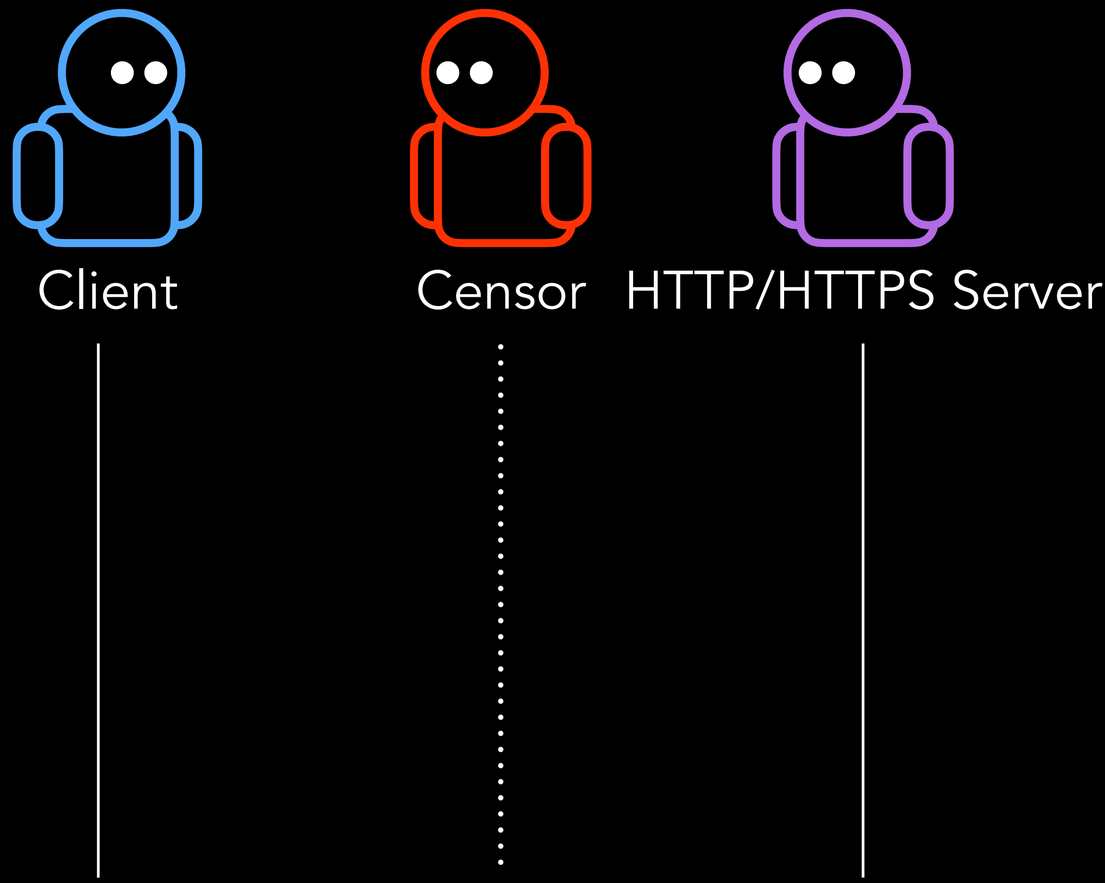
1. Background
2. High-Level Design
3. Preliminary Results

Agenda

1. Background
2. High-Level Design
3. Preliminary Results

Background

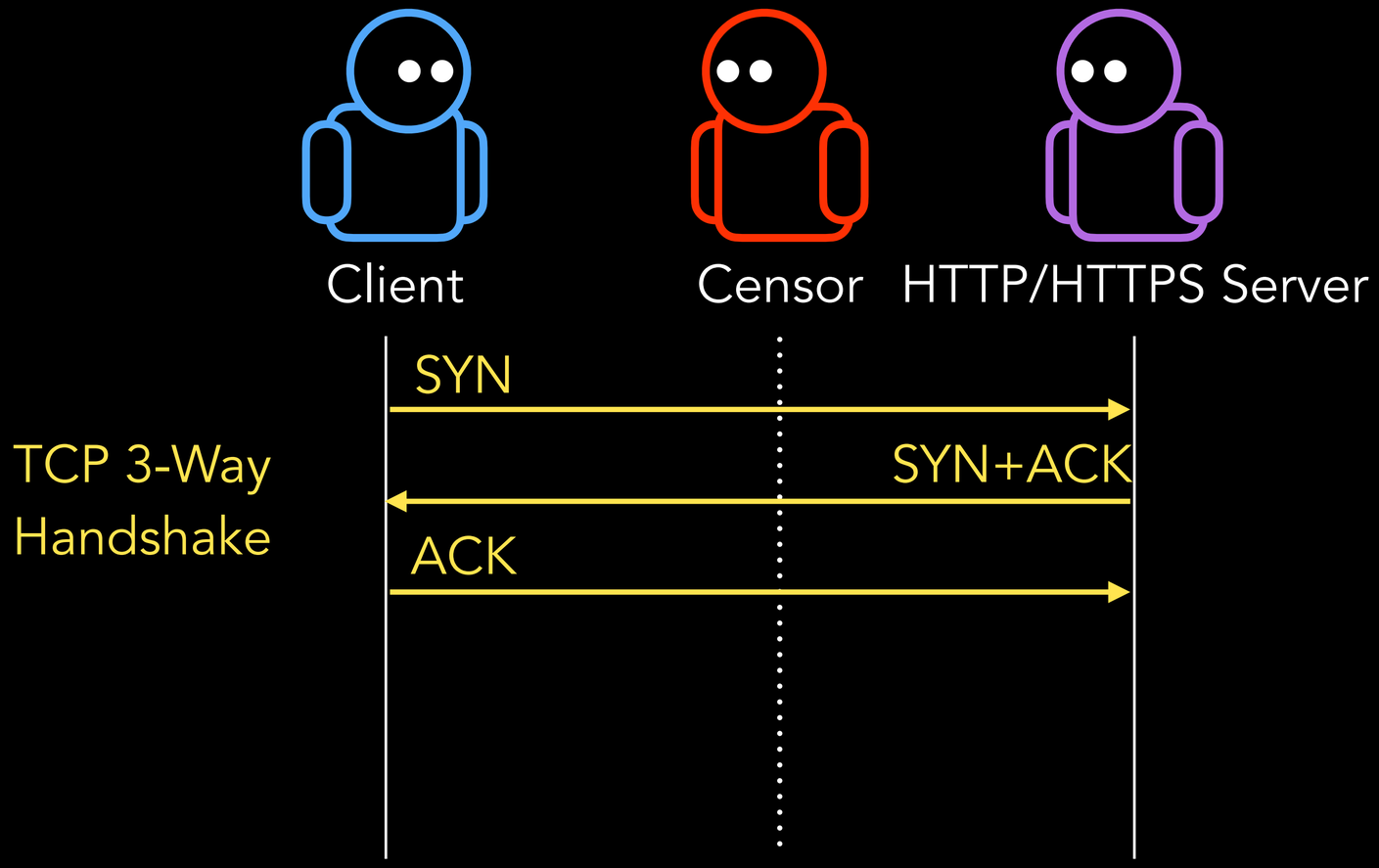
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

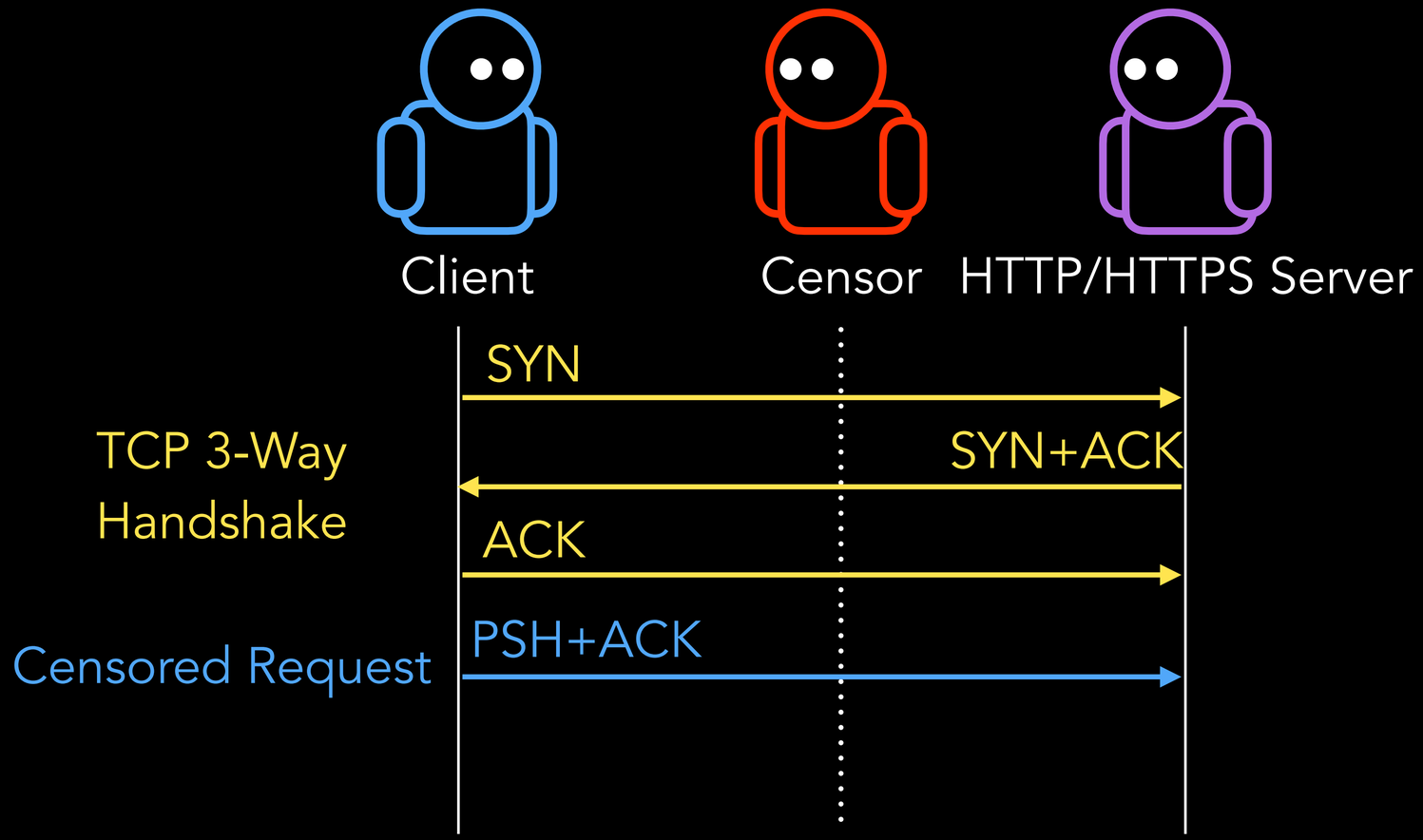
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

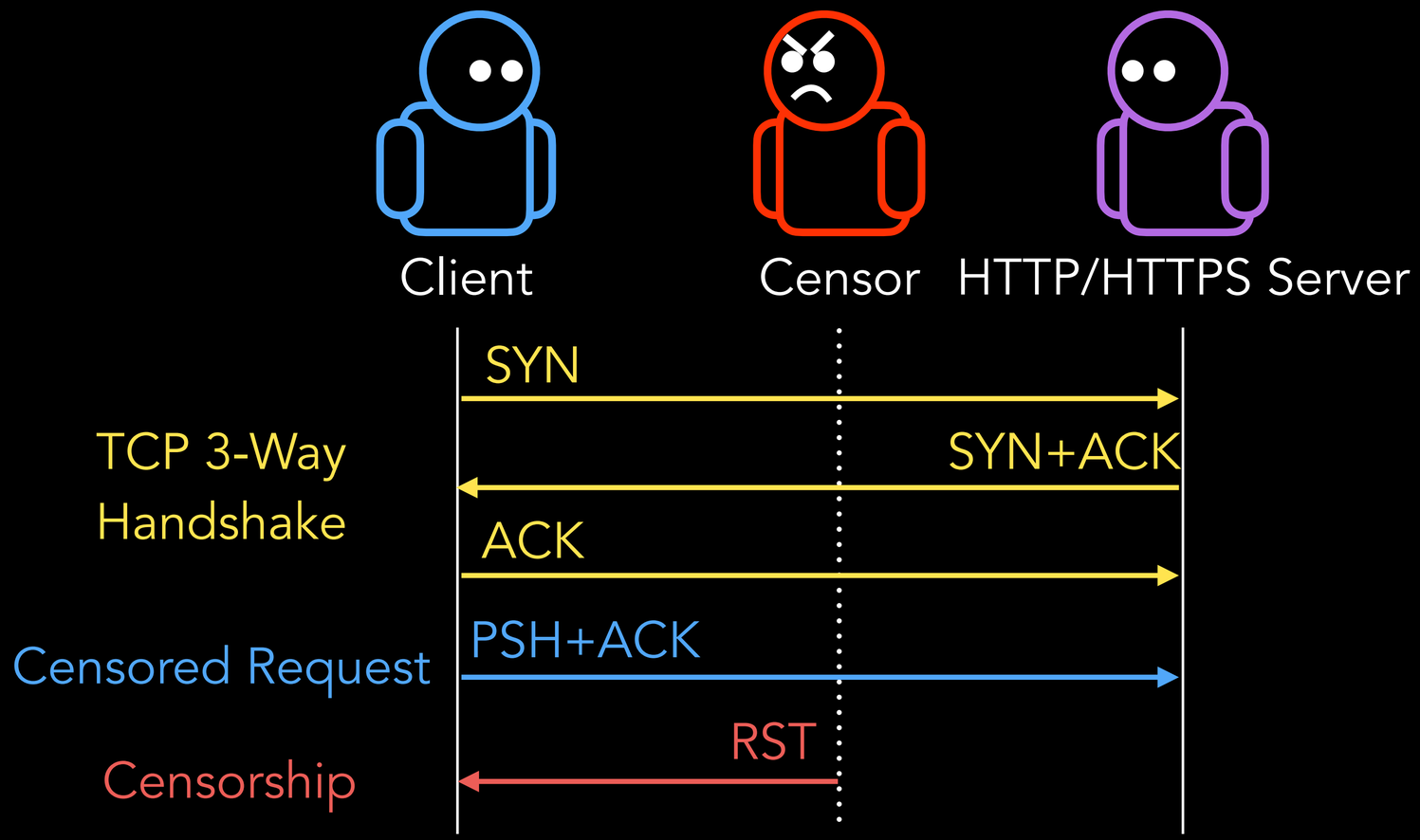
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

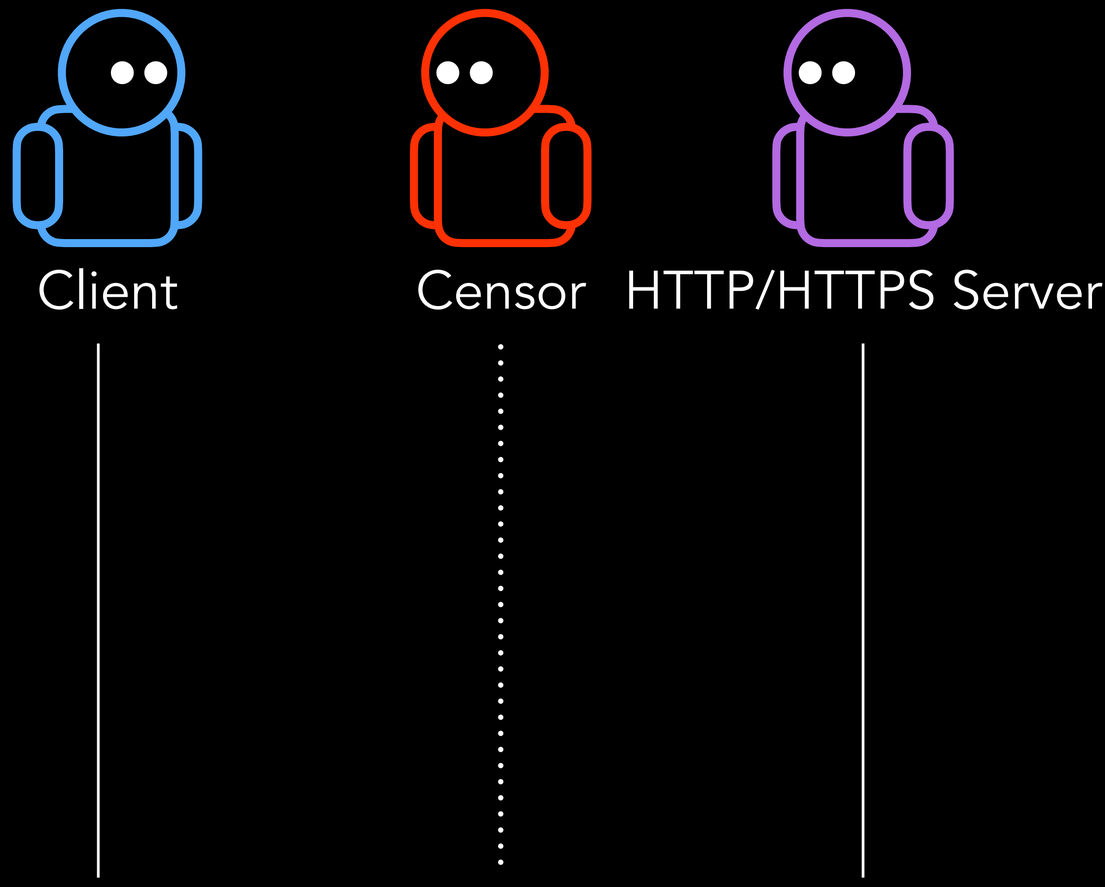
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

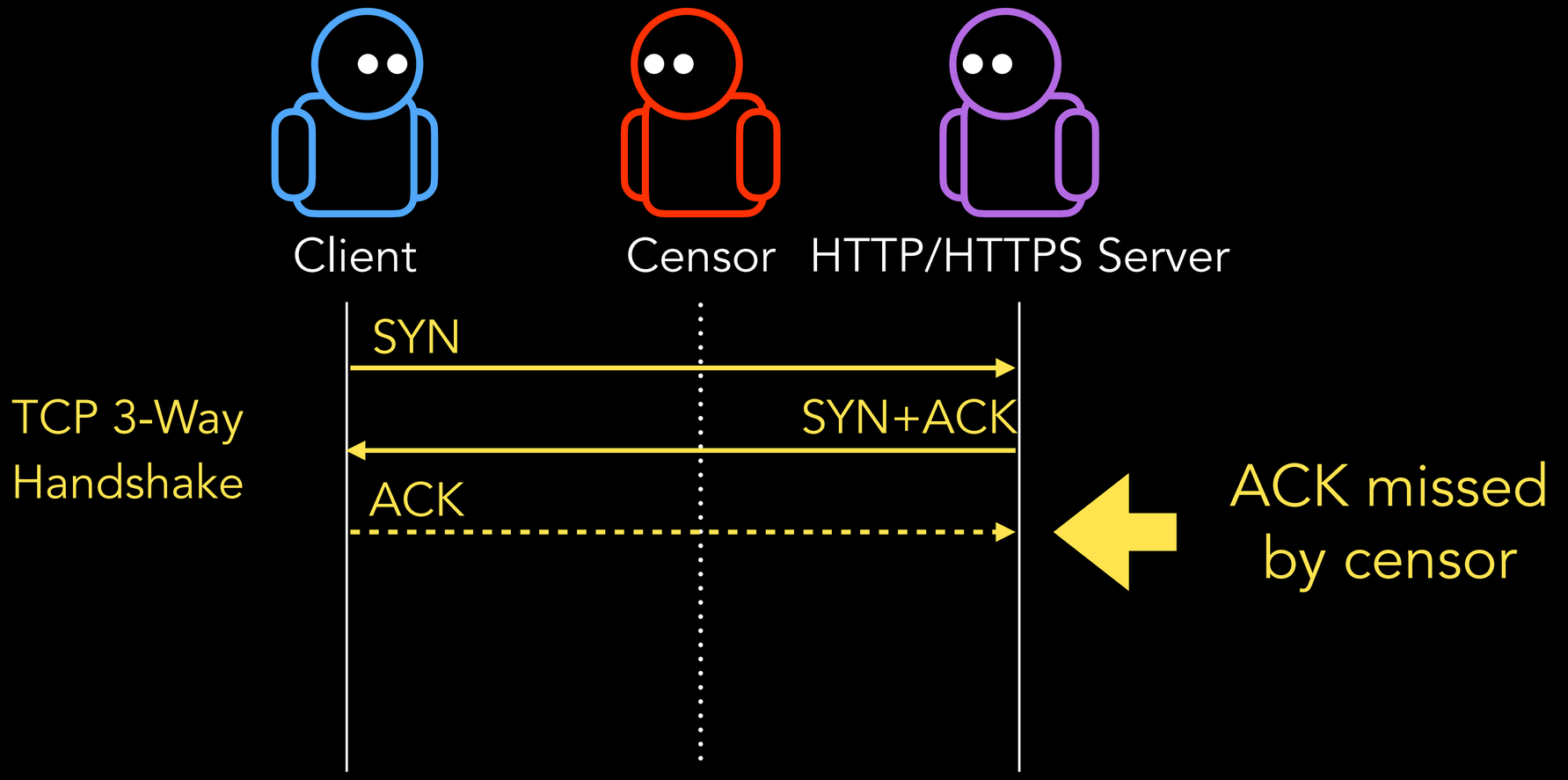
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

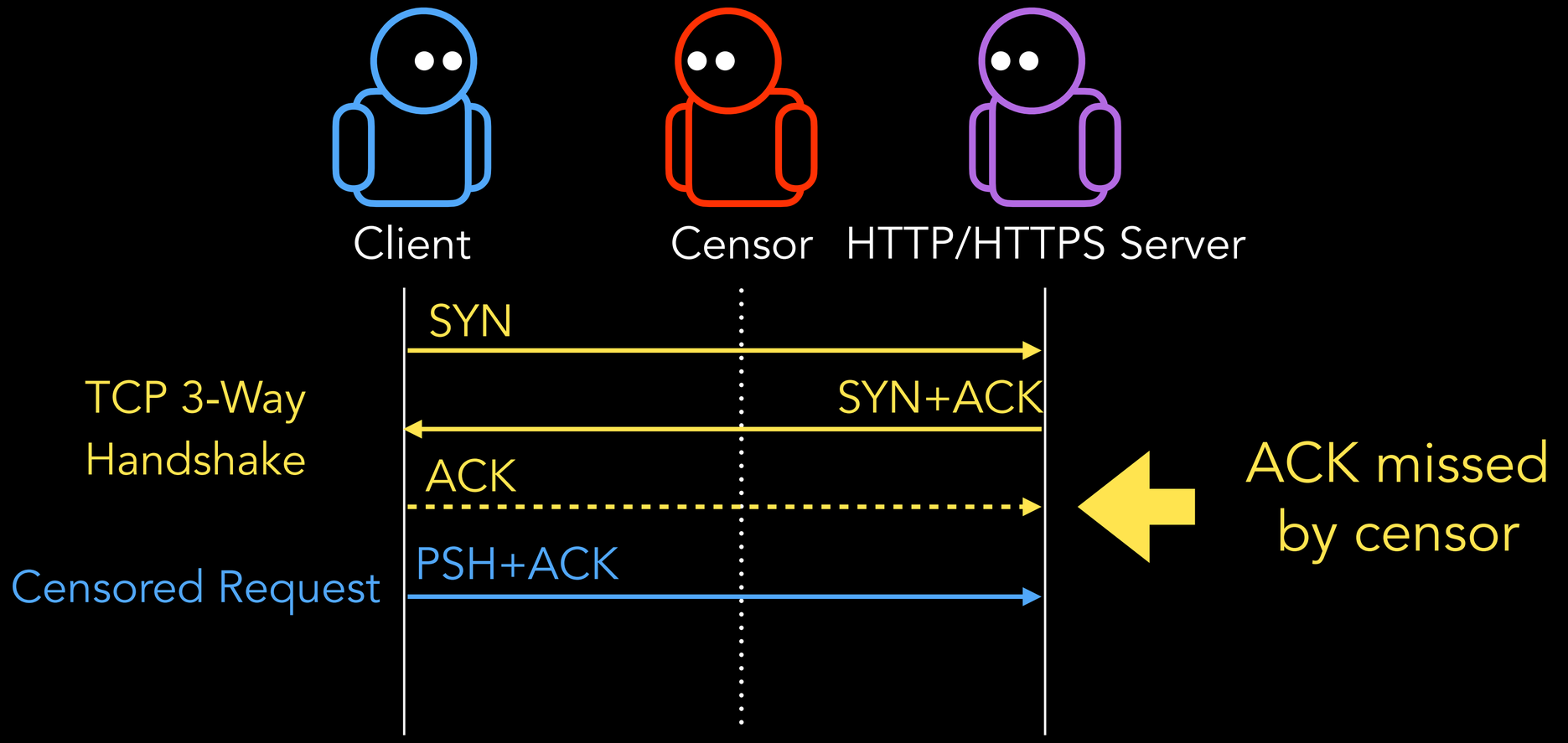
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

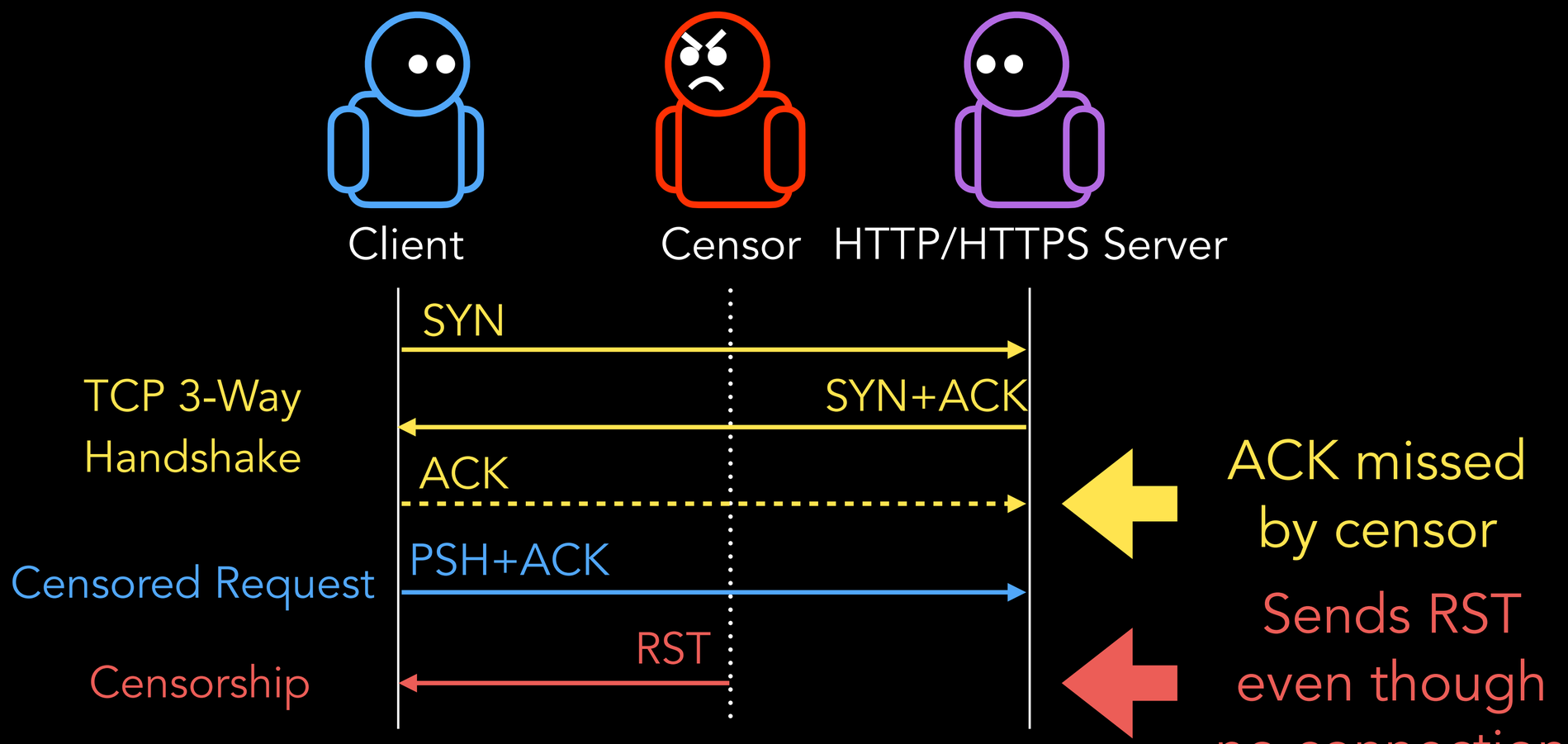
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

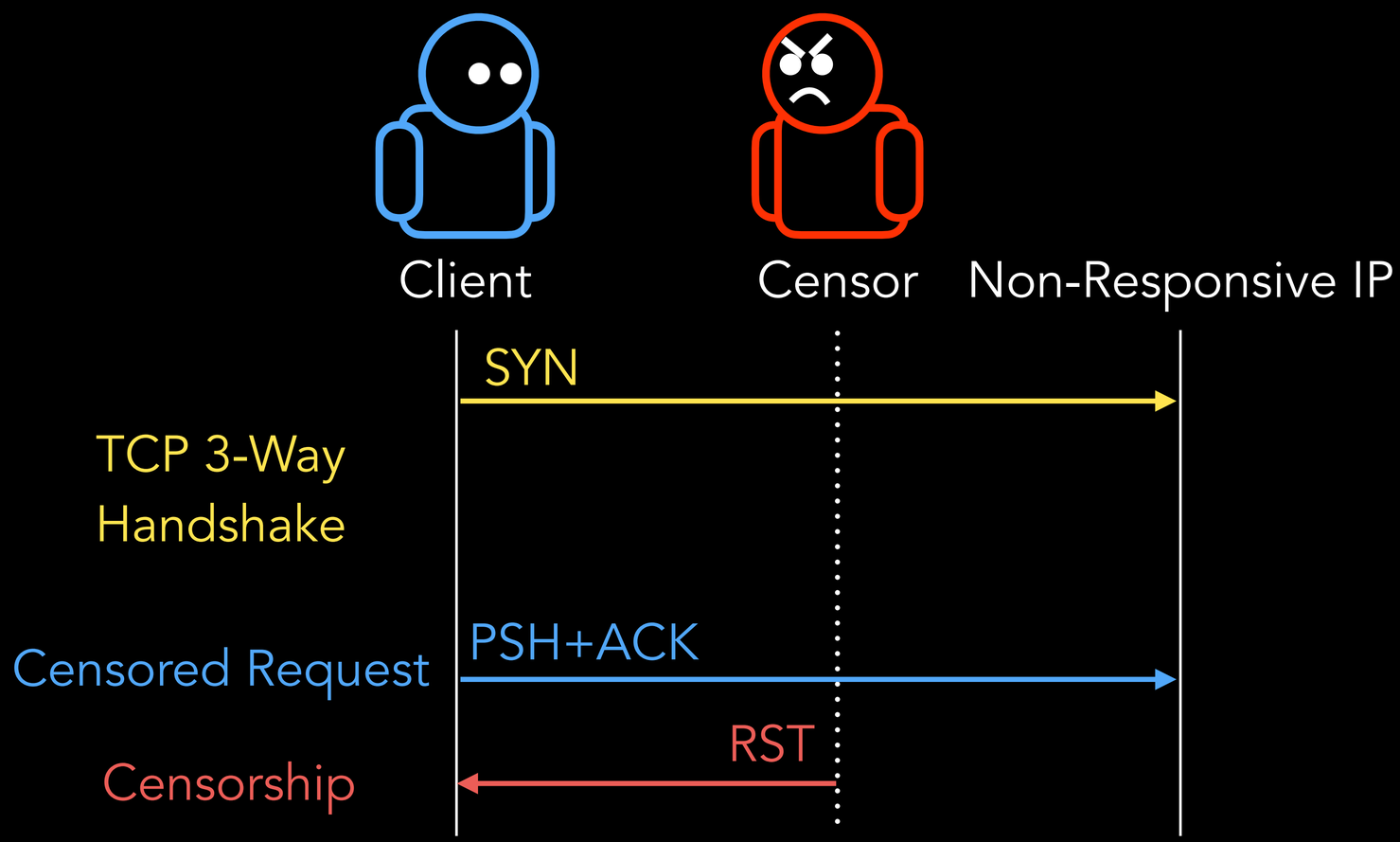
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

Background

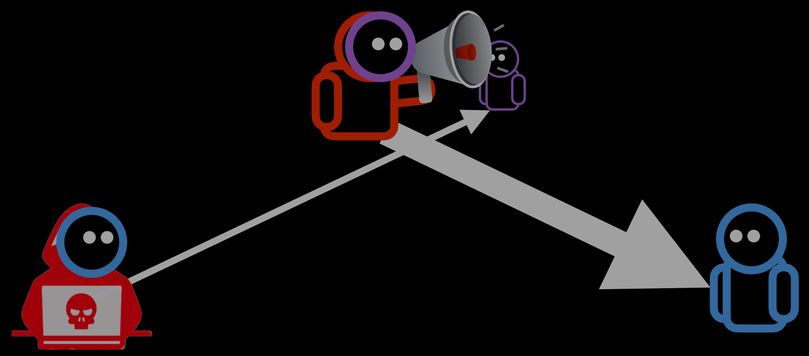
TCP Noncompliance



Triggering HTTP/HTTPS Censorship without Endpoint Participation

Background

TCP Noncompliance



TCP Amplification Attacks

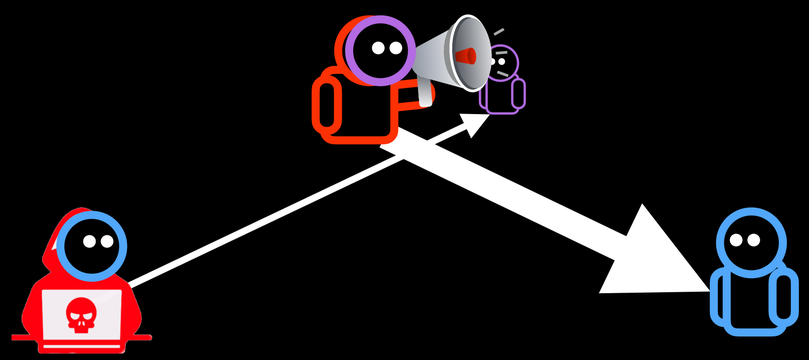
[Bock et al. USENIX 2021]

Measuring Turkmenistan Censorship

[Nourin et al. WWW 2023]

Background

TCP Noncompliance



TCP Amplification Attacks

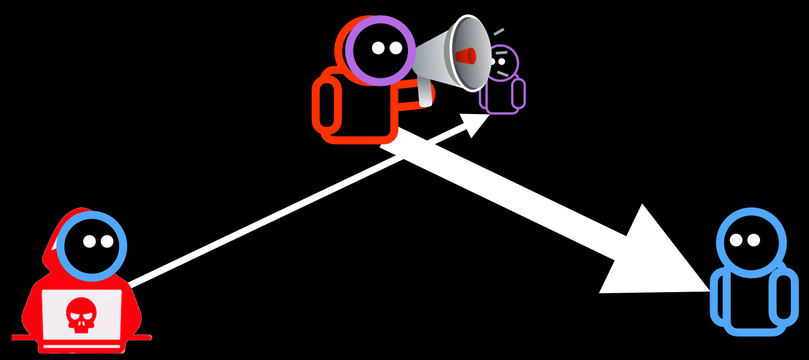
[Bock et al. USENIX 2021]

Measuring Turkmenistan Censorship

[Nourin et al. WWW 2023]

Background

TCP Noncompliance



TCP Amplification Attacks

[Bock et al. USENIX 2021]

Measuring Turkmenistan Censorship

[Nourin et al. WWW 2023]

Background

Geneva

Geneva

Genetic Evasion

[Bock et al. CCS 2019]

Open-source genetic algorithm that trains against
live censors to discover packet sequences that evade censorship

Background

Geneva

Geneva

Genetic Evasion

[Bock et al. CCS 2019]

Open-source genetic algorithm that trains against
live censors to discover packet sequences that evade censorship

Background

Geneva

Geneva

Genetic Evasion

[Bock et al. CCS 2019]

Open-source genetic algorithm that trains against
live censors to discover packet sequences that ~~evade~~ censorship

Background

Geneva

Geneva

Genetic Evasion

[Bock et al. CCS 2019]

Open-source genetic algorithm that trains against live censors to discover packet sequences that ~~evade~~ censorship trigger

Background

Measuring Censorship

- Once we can trigger censorship on one IP address, we can trigger censorship on virtually all IP addresses
- Can not only measure networks current tools cannot access, but can hit more endpoints in other networks too
- Why does this matter? Censorship is not uniformly distributed over IP addresses!

Background

Measuring Censorship

- Once we can trigger censorship on one IP address, we can trigger censorship on virtually all IP addresses
- Can not only measure networks current tools cannot access, but can hit more endpoints in other networks too
- Why does this matter? Censorship is not uniformly distributed over IP addresses!

Background

Measuring Censorship

- Once we can trigger censorship on one IP address, we can trigger censorship on virtually all IP addresses
- Can not only measure networks current tools cannot access, but can hit more endpoints in other networks too
- Why does this matter? Censorship is not uniformly distributed over IP addresses!

Background

Measuring Censorship

- Once we can trigger censorship on one IP address, we can trigger censorship on virtually all IP addresses
- Can not only measure networks current tools cannot access, but can hit more endpoints in other networks too
- Why does this matter? Censorship is not uniformly distributed over IP addresses!

Agenda

1. Background
2. High-Level Design
3. Preliminary Results

Agenda

1. Background
2. High-Level Design
3. Preliminary Results

High-Level Design

Requirements

A country is eligible for our measurement system if it has:

1. Confirmed Censored Domain(s)
2. Bidirectional Censorship
3. Little to No Residual Censorship

High-Level Design

Requirements

A country is eligible for our measurement system if it has:

1. Confirmed Censored Domain(s)
2. Bidirectional Censorship
3. Little to No Residual Censorship

High-Level Design

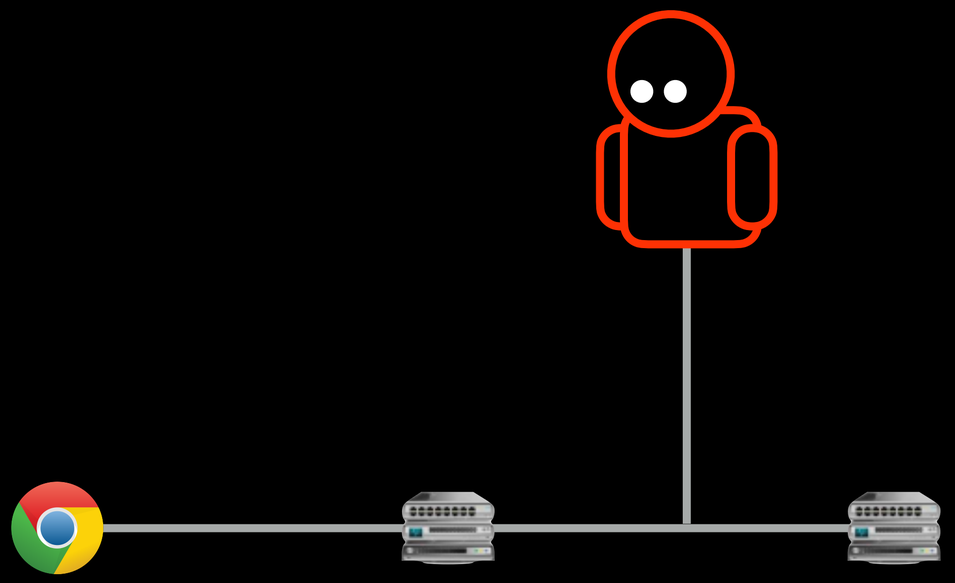
Requirements

A country is eligible for our measurement system if it has:

1. Confirmed Censored Domain(s)
2. Bidirectional Censorship
3. Little to No Residual Censorship

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

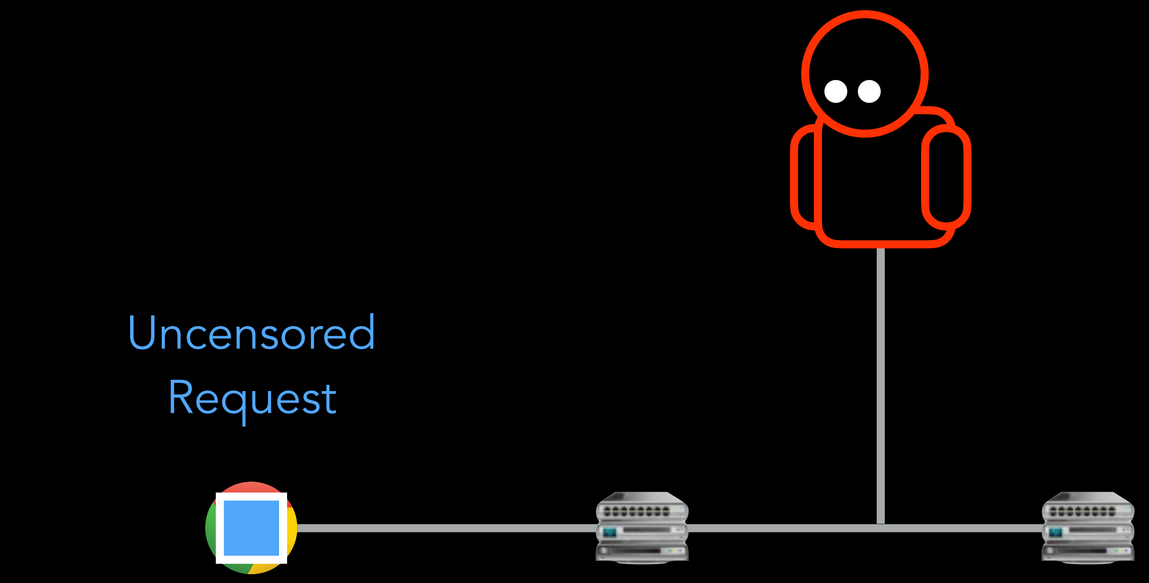
(outside censored country)

Server

(inside censored country)

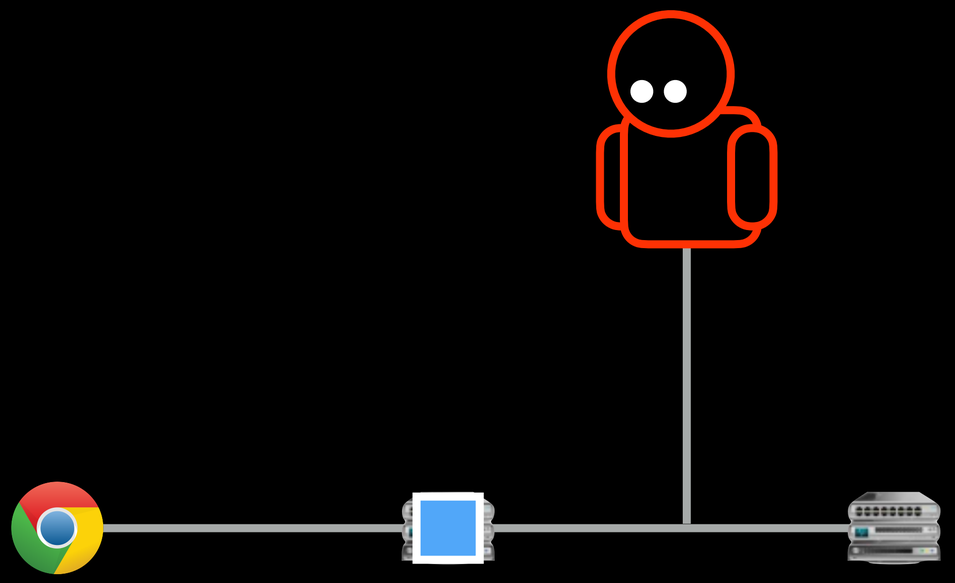
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

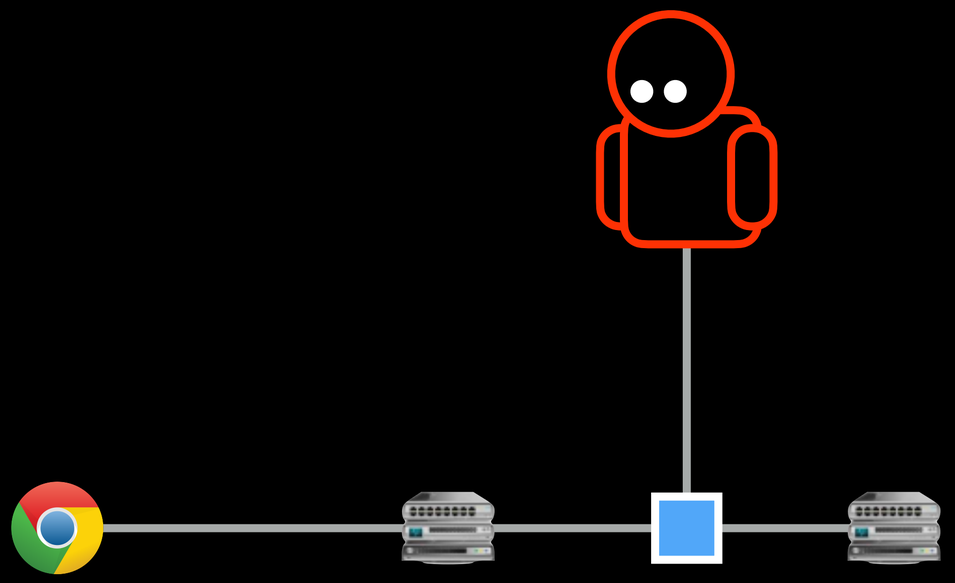
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

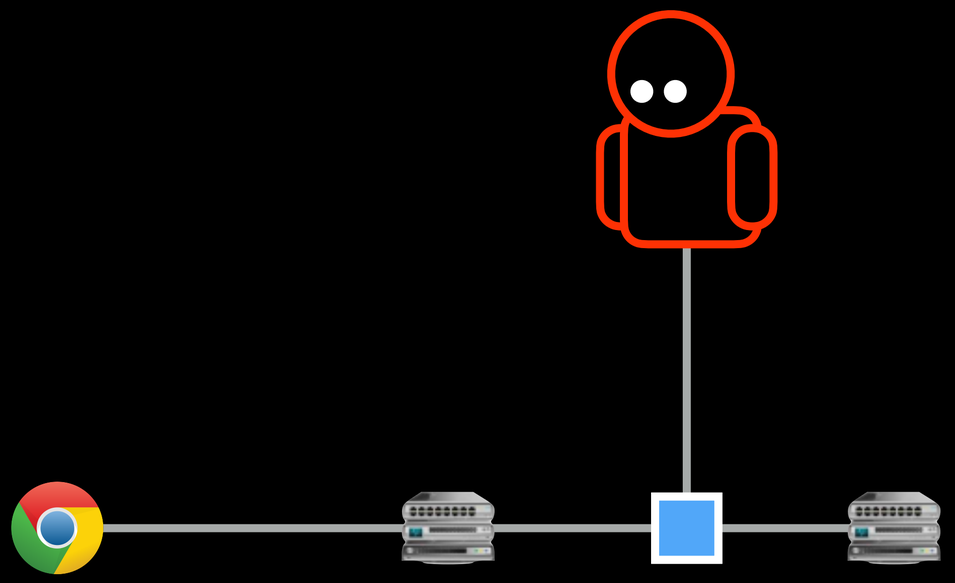
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

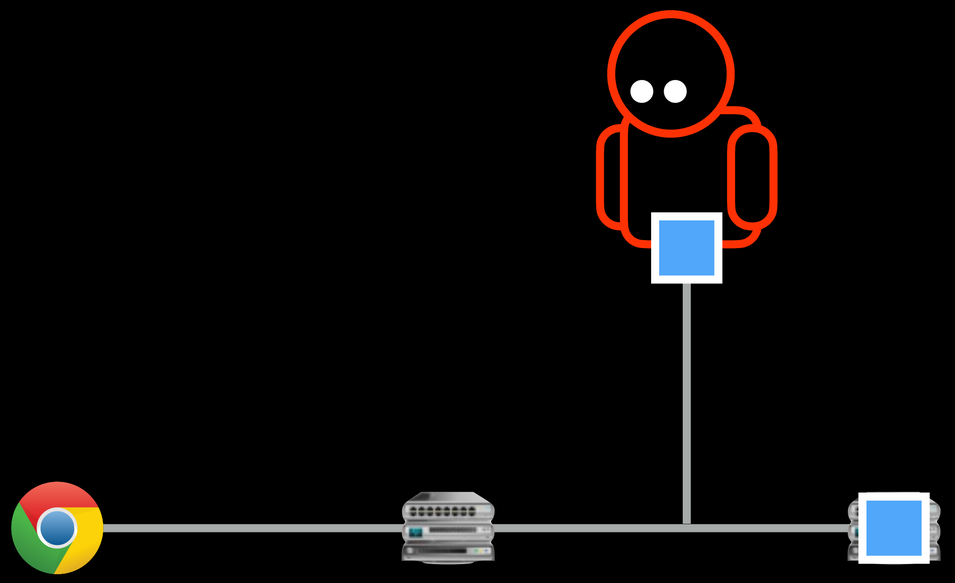
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

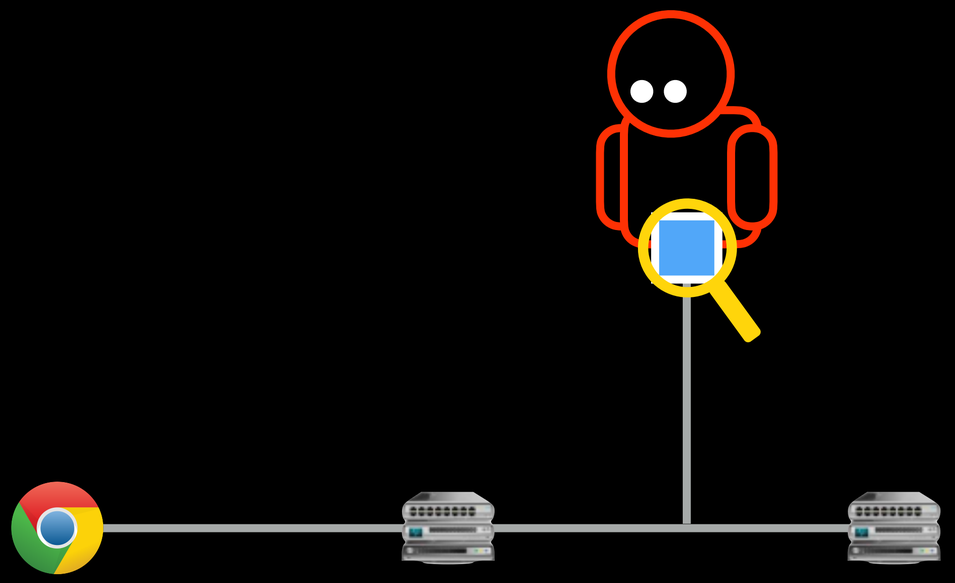
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

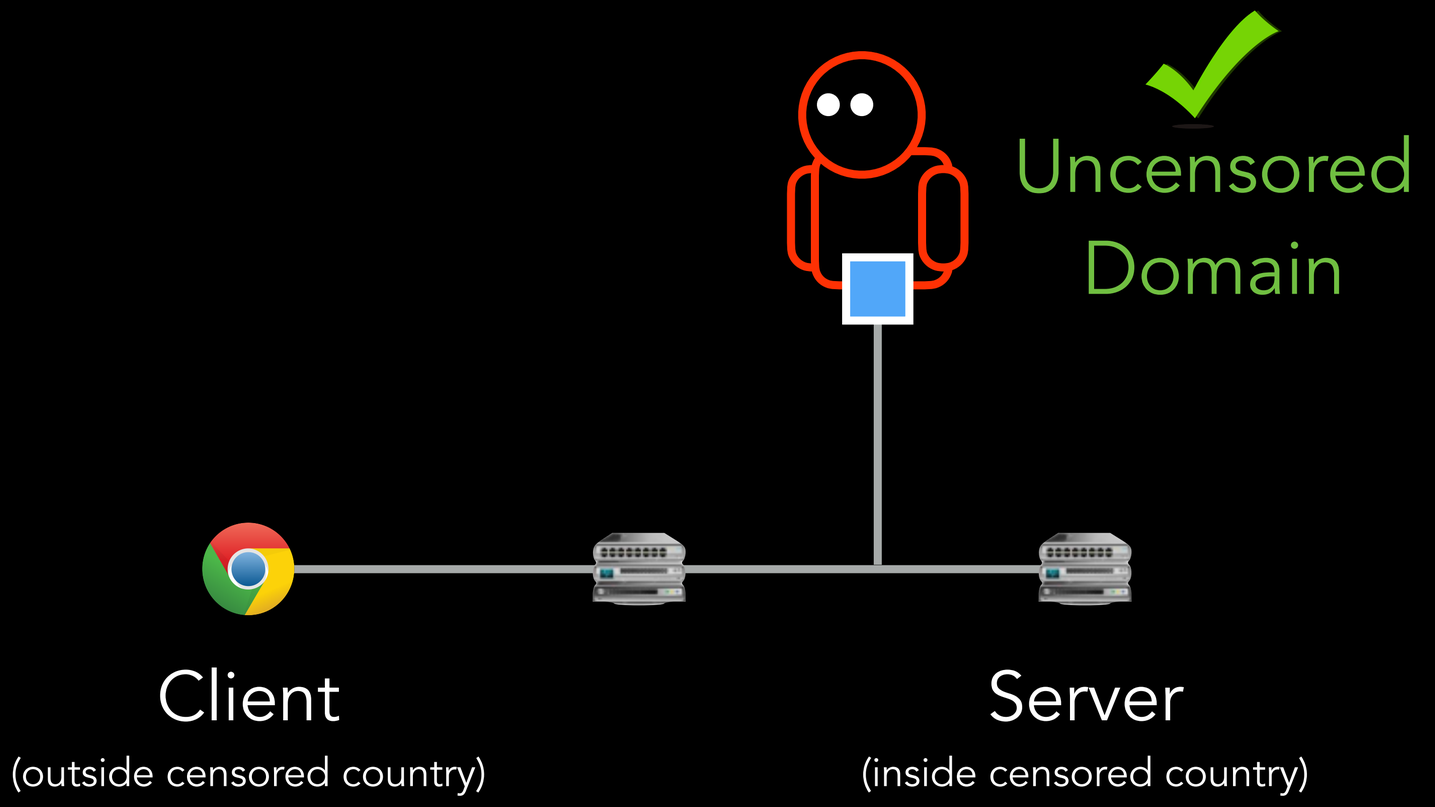
(outside censored country)

Server

(inside censored country)

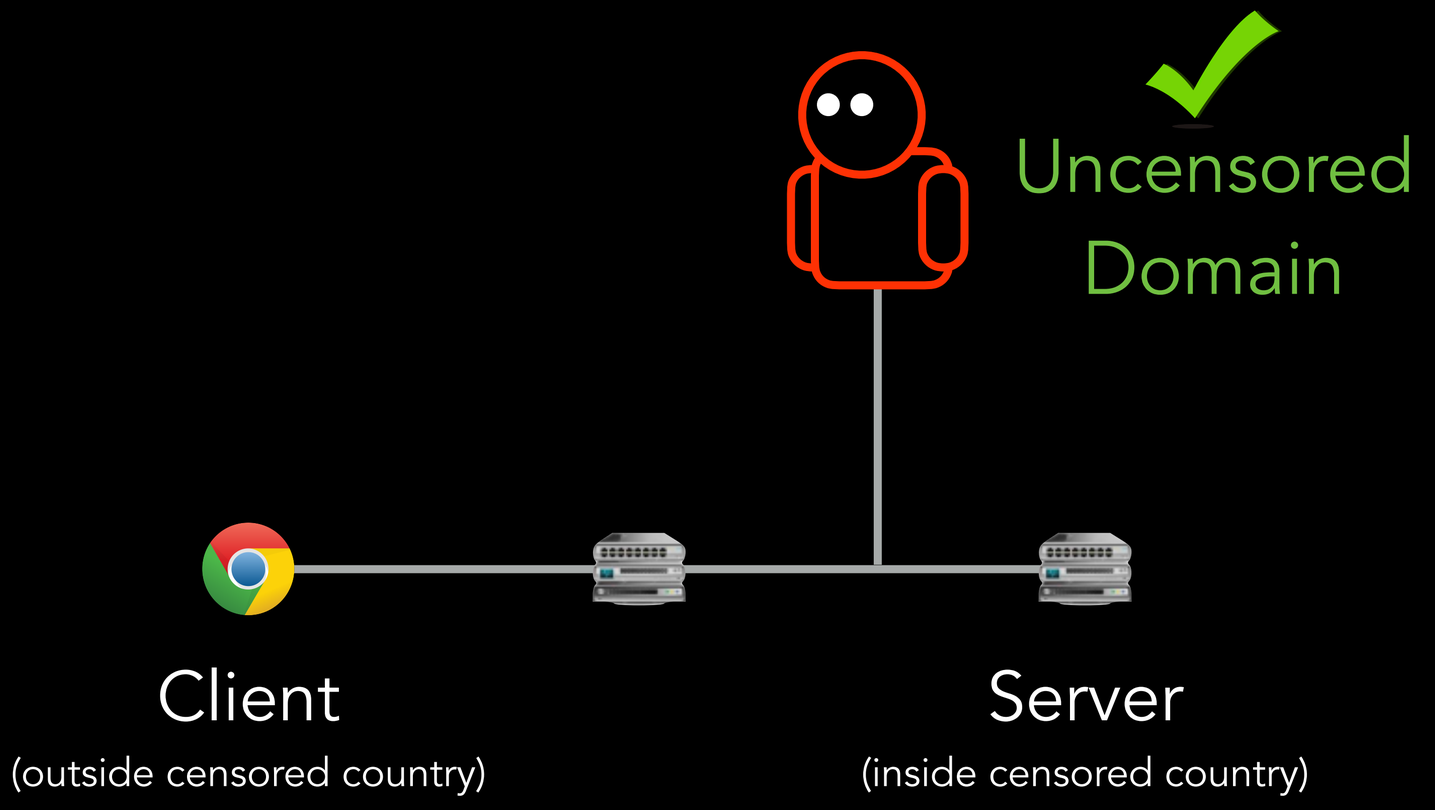
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



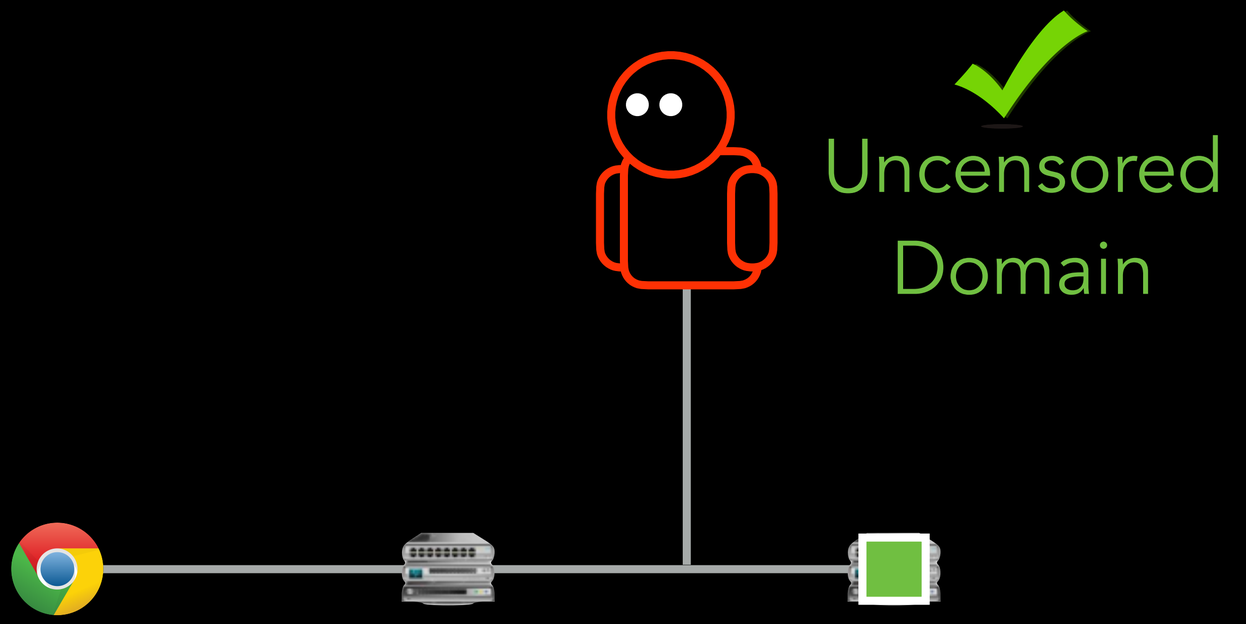
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



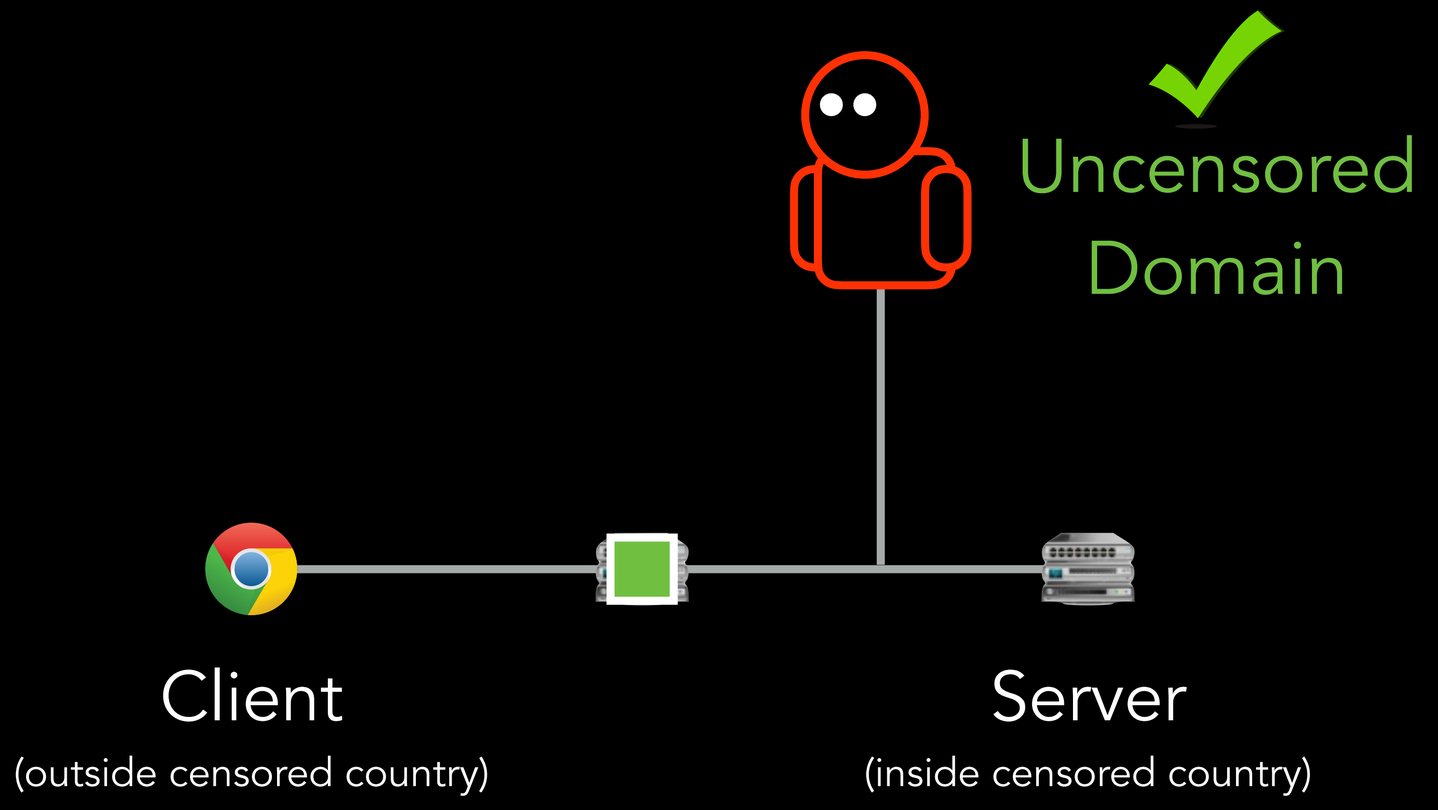
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



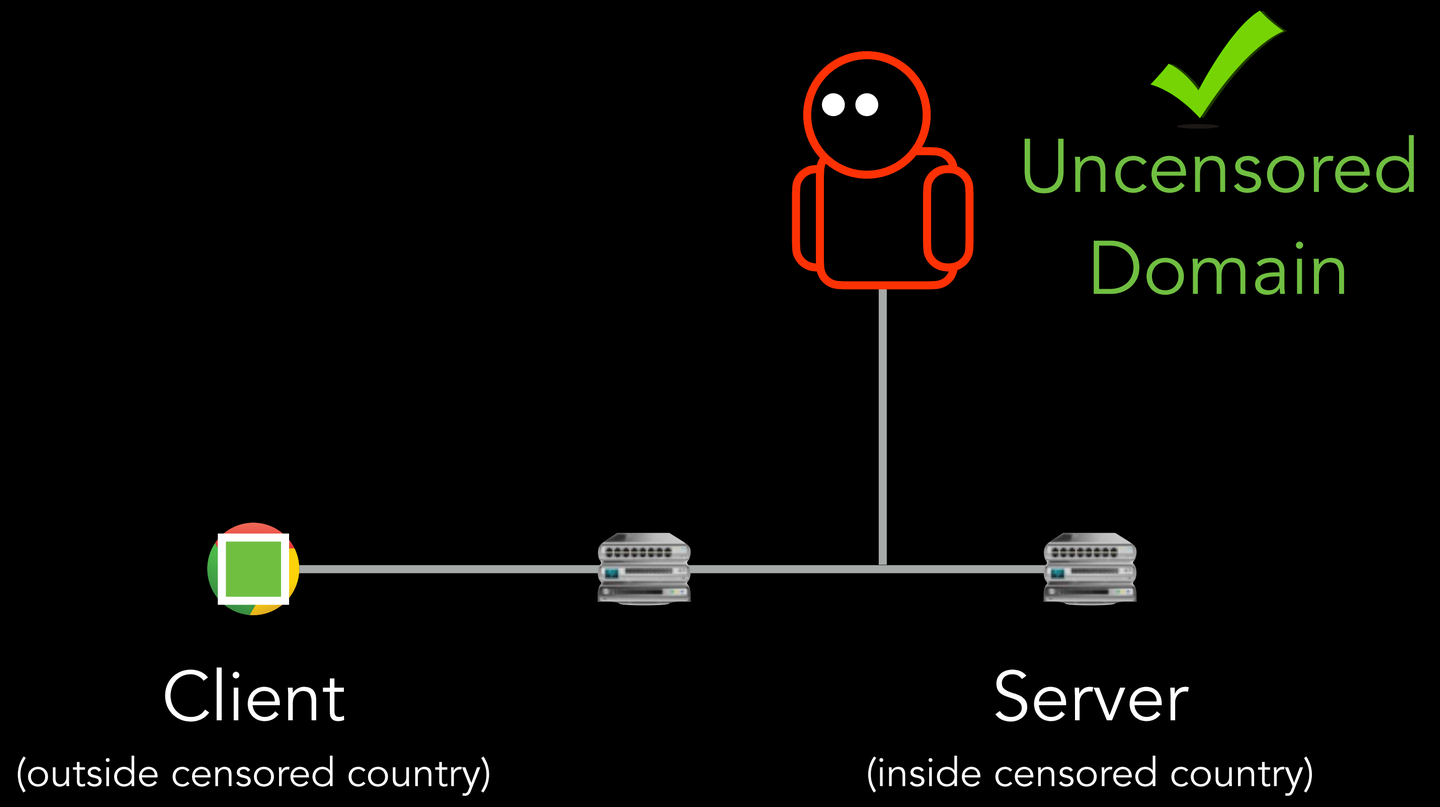
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



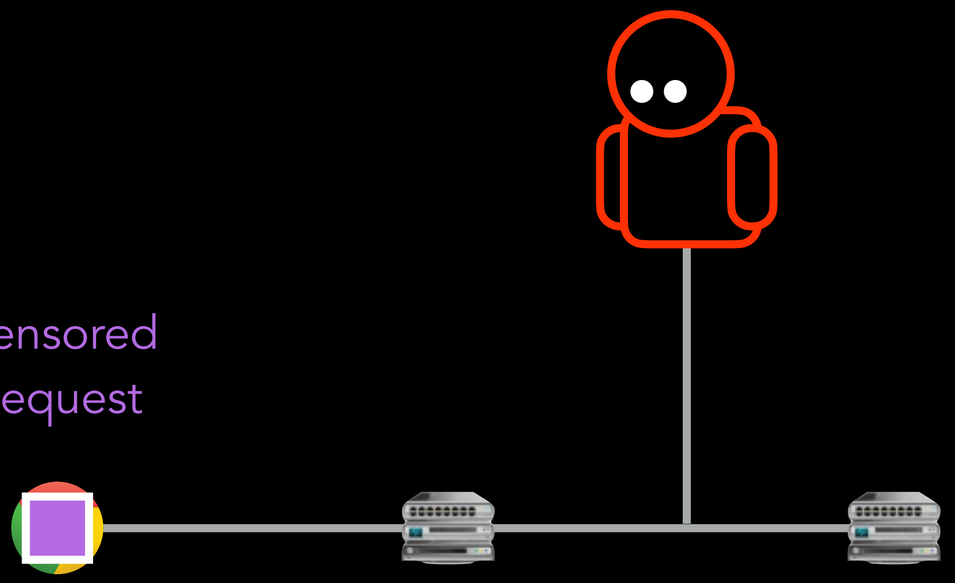
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



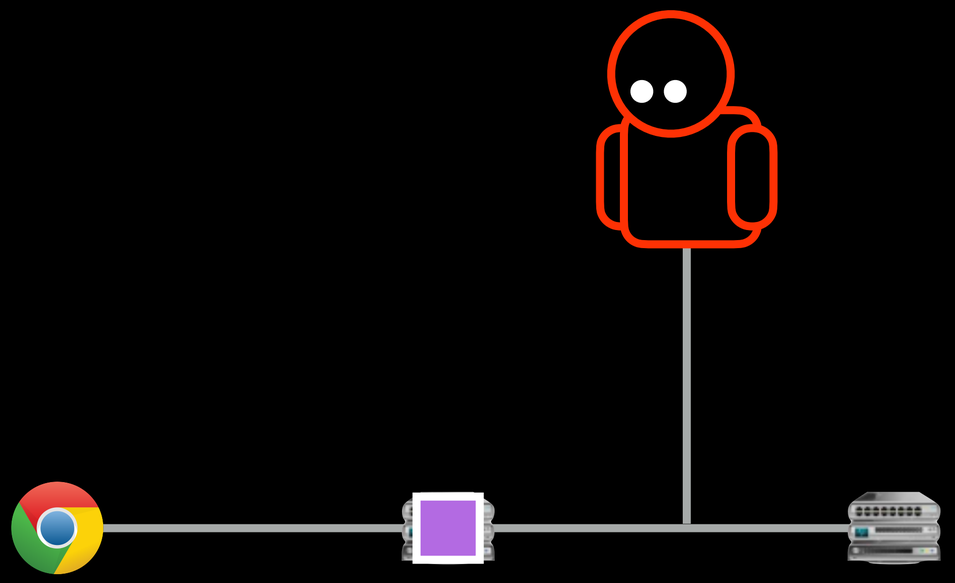
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

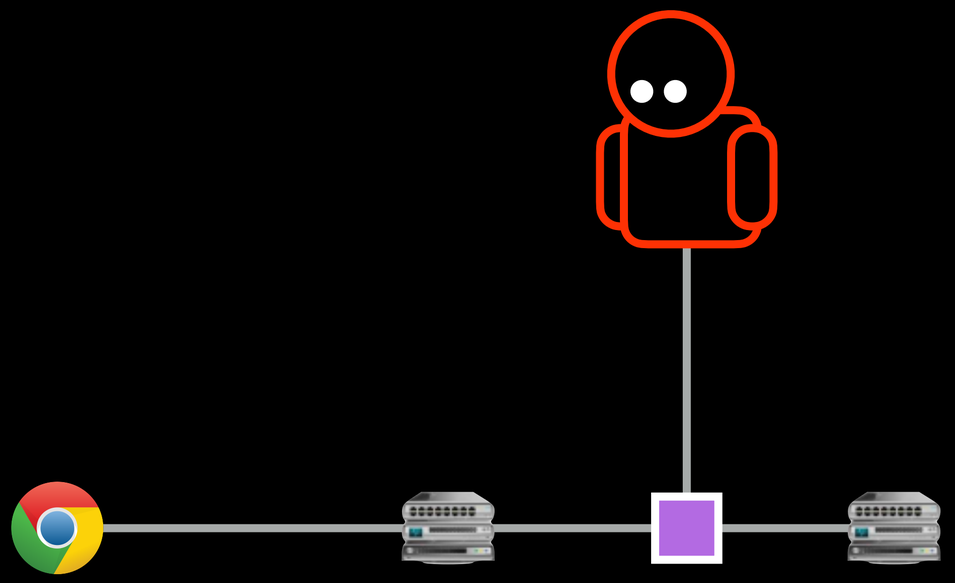
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

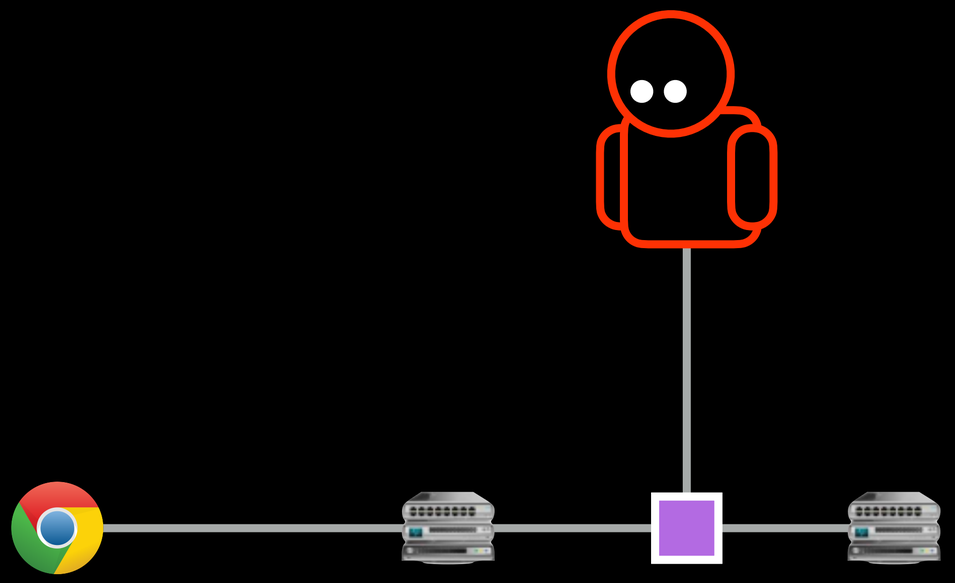
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

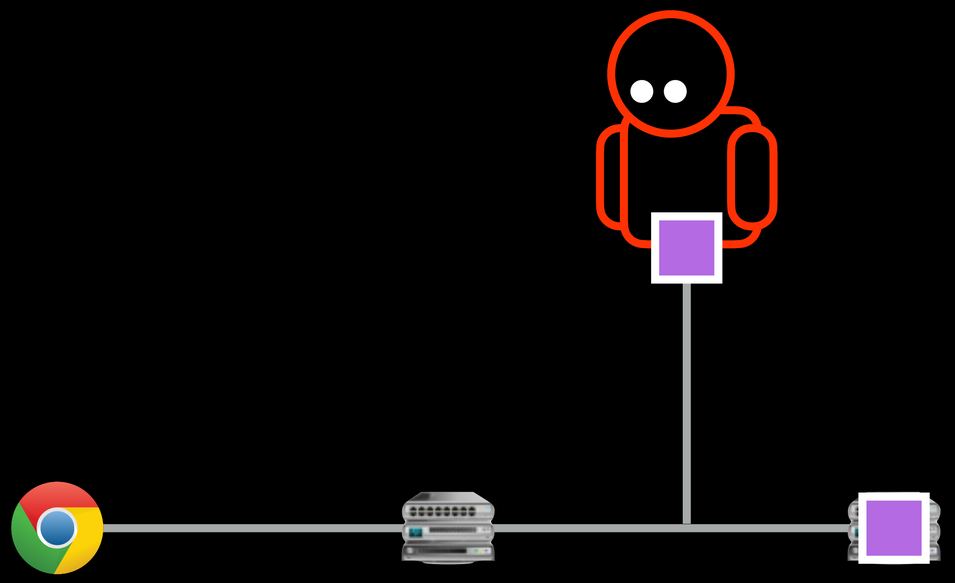
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

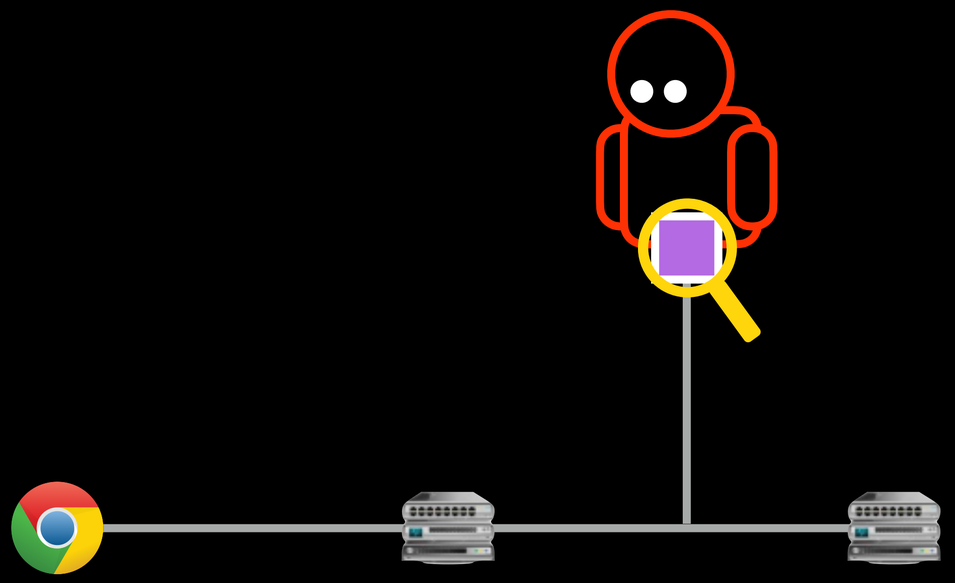
(outside censored country)

Server

(inside censored country)

Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Client

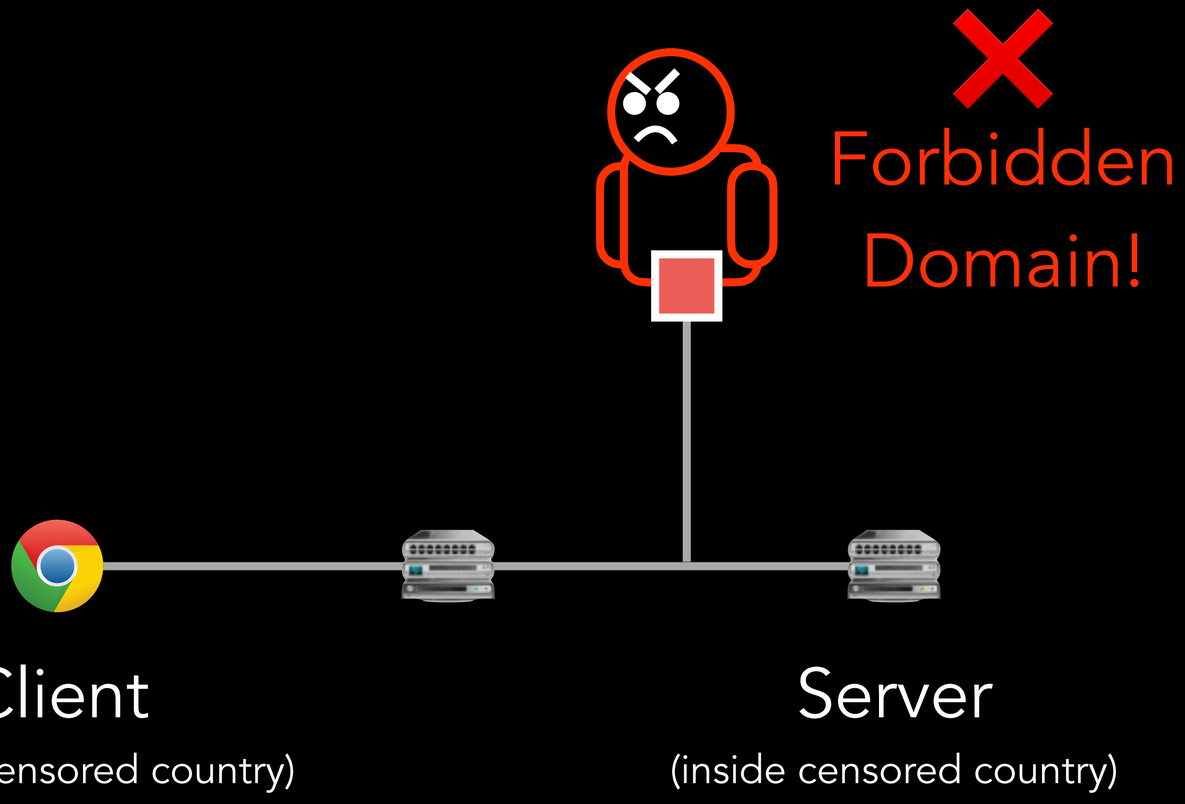
(outside censored country)

Server

(inside censored country)

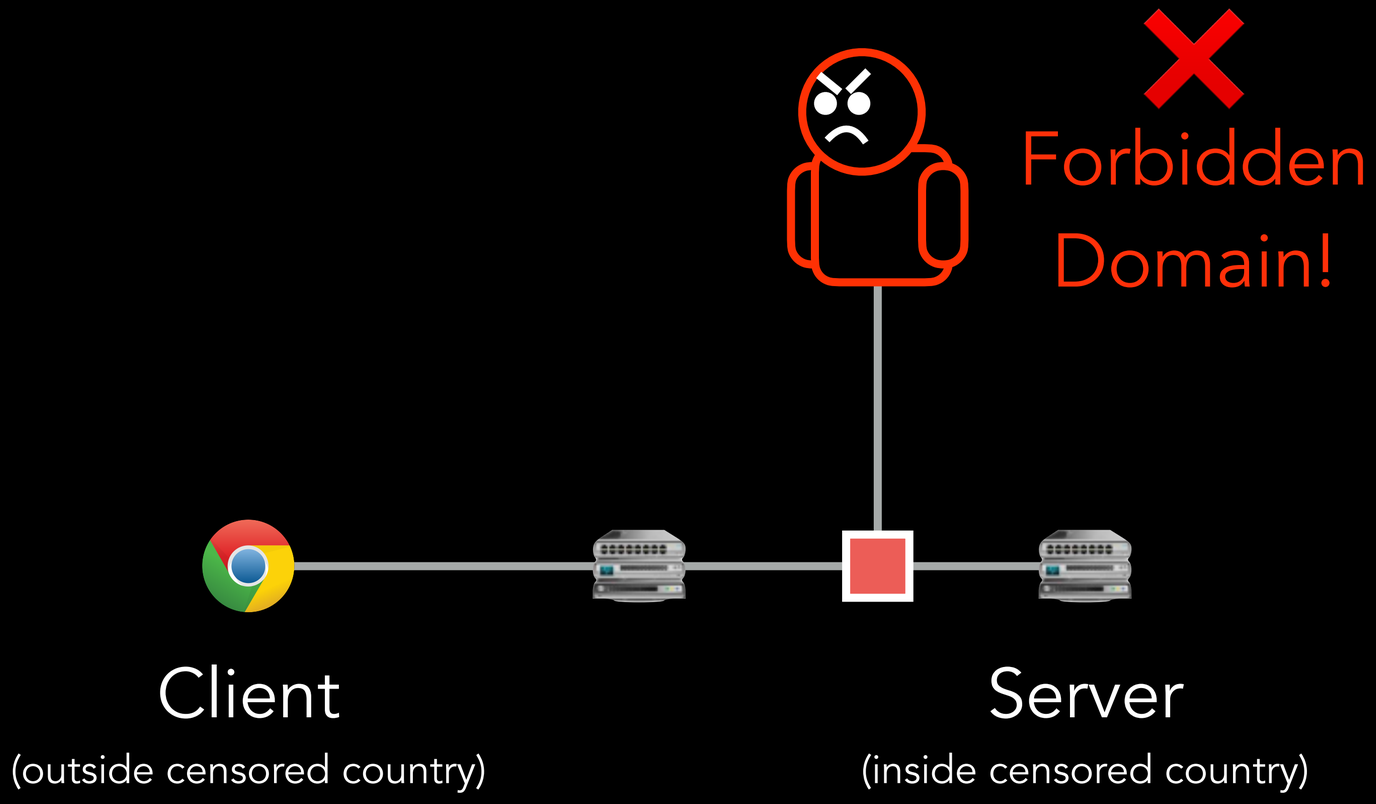
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



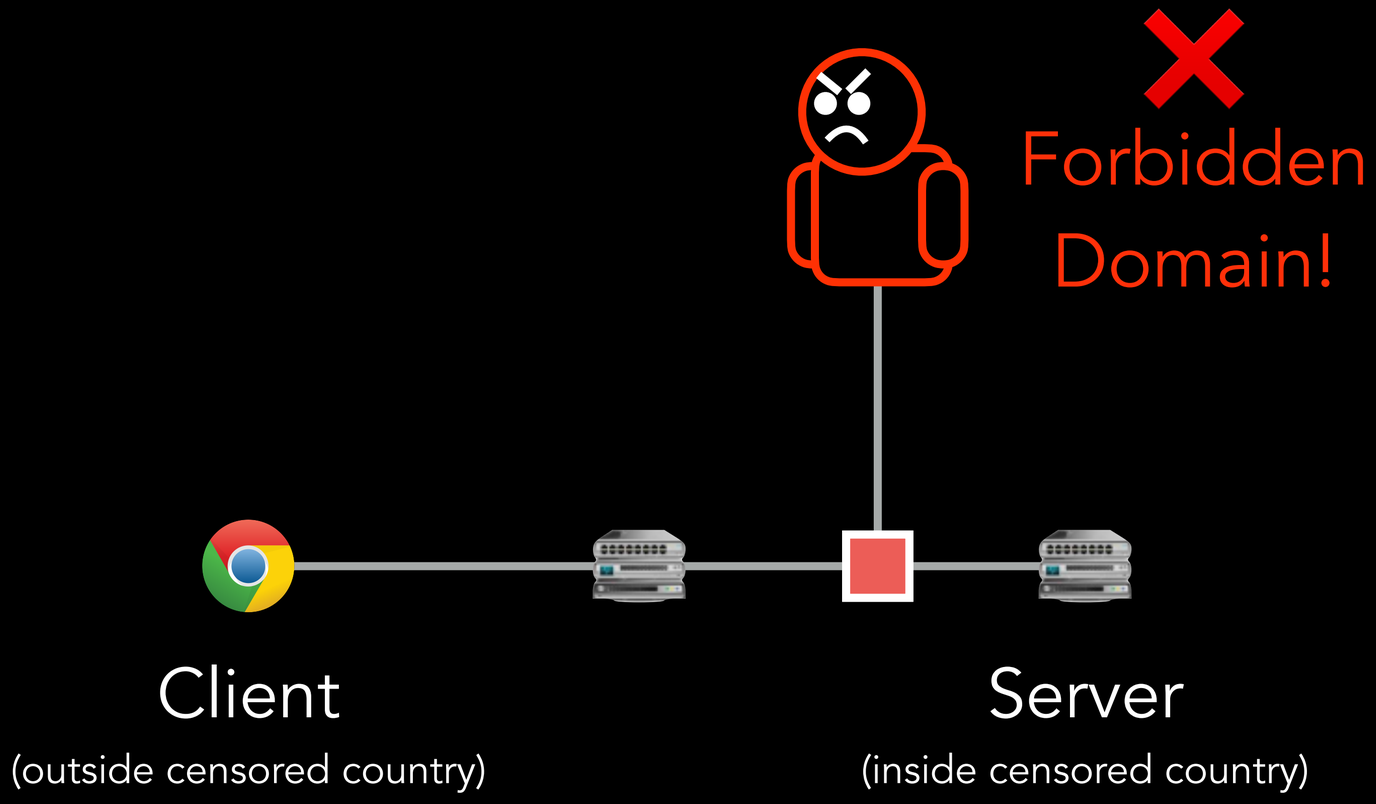
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



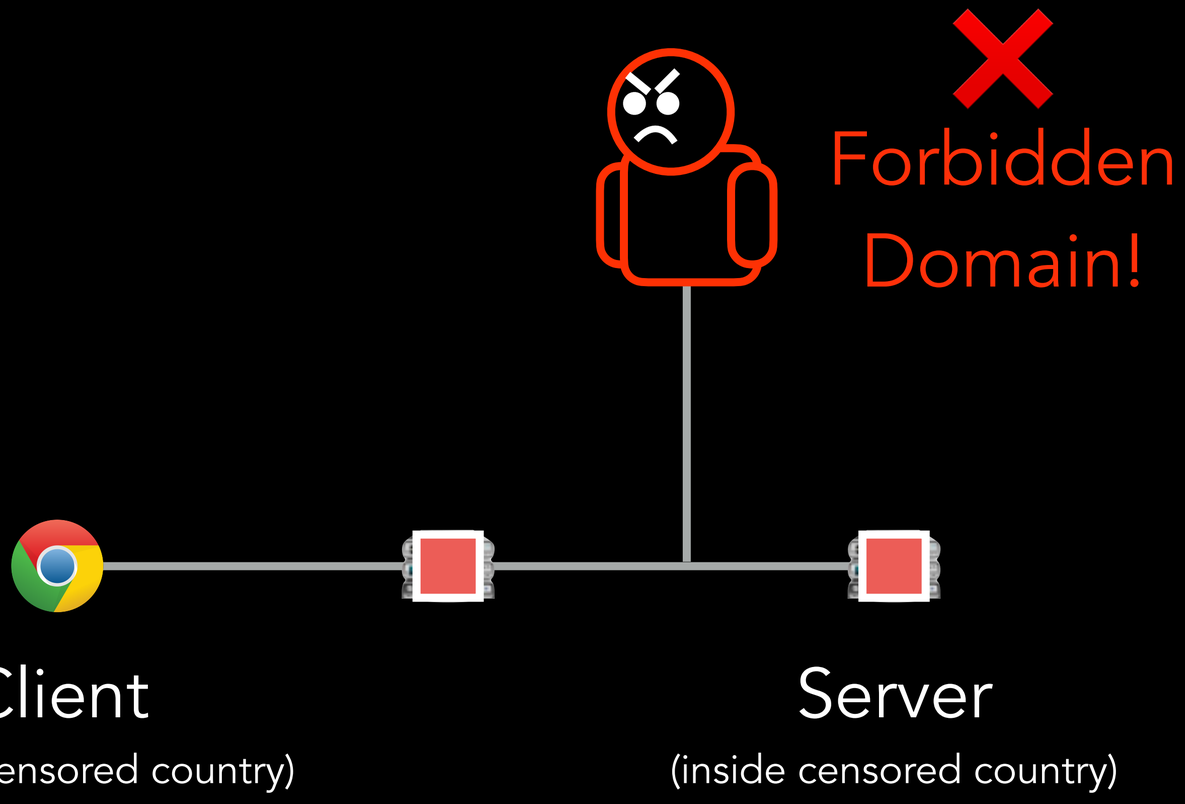
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



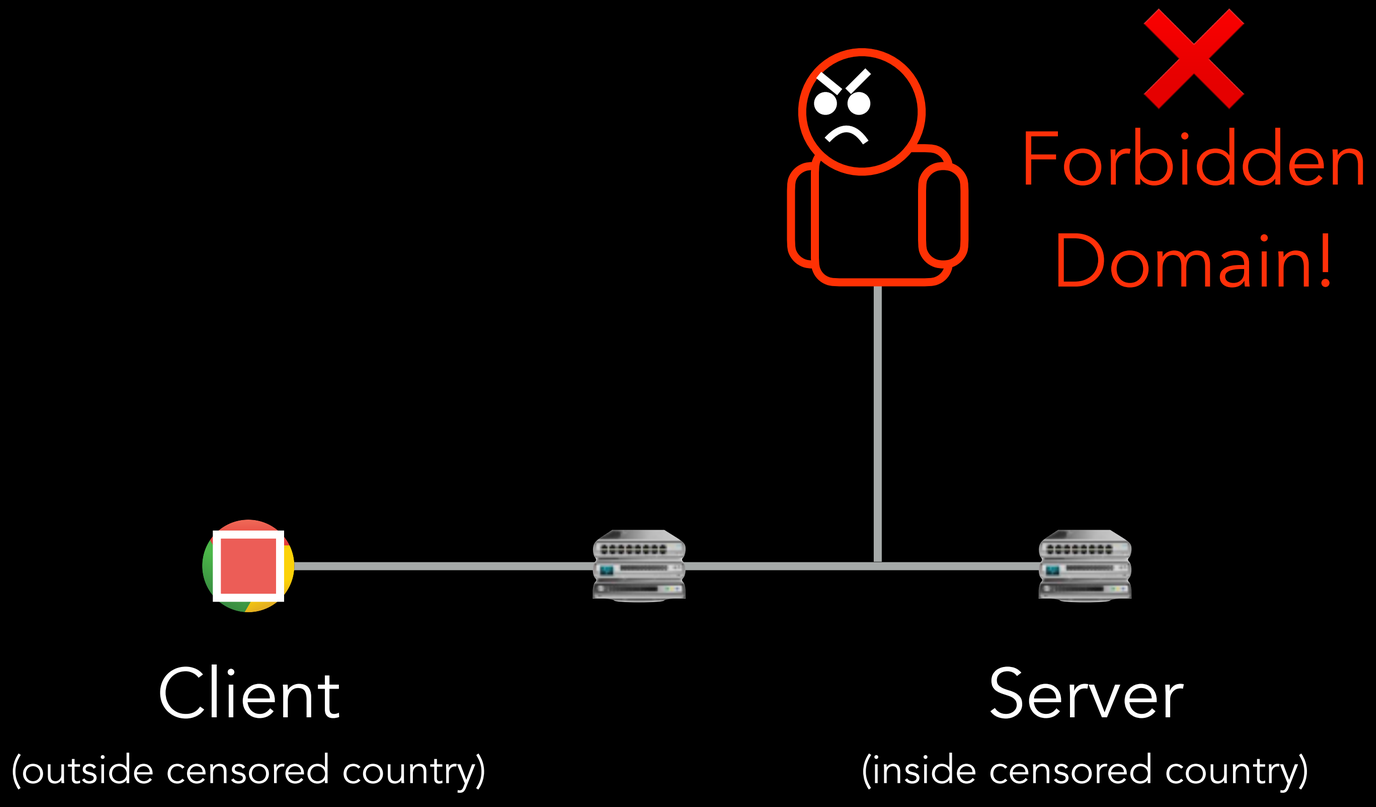
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



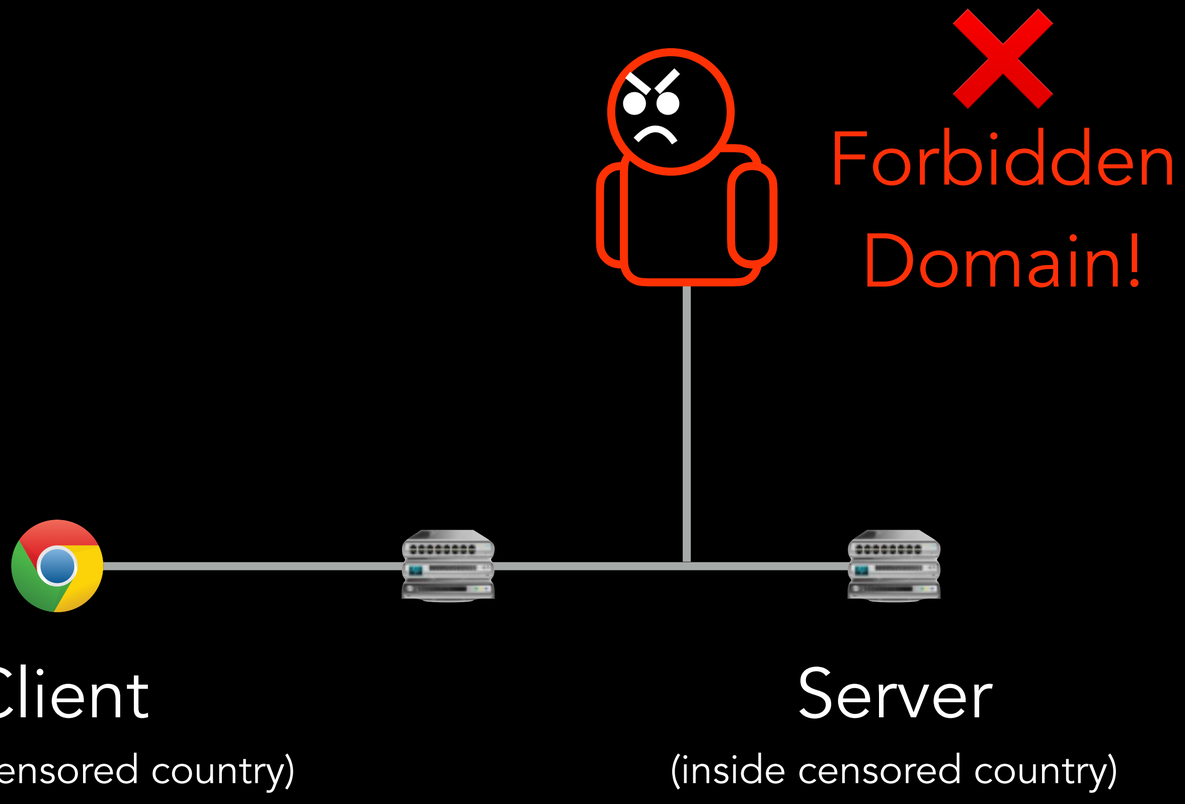
Bidirectional Censorship

Censor filters all traffic regardless of where it originated



Bidirectional Censorship

Censor filters all traffic regardless of where it originated



High-Level Design

Requirements

A country is eligible for our measurement system if it has:

1. Confirmed Censored Domain(s)
2. Bidirectional Censorship
3. Little to No Residual Censorship

High-Level Design

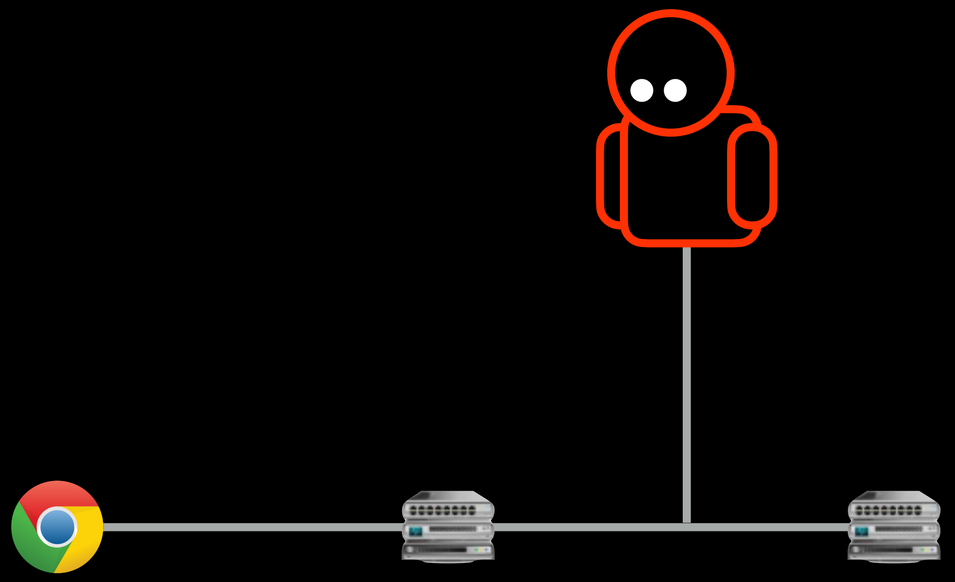
Requirements

A country is eligible for our measurement system if it has:

1. Confirmed Censored Domain(s)
2. Bidirectional Censorship
3. Little to No Residual Censorship

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

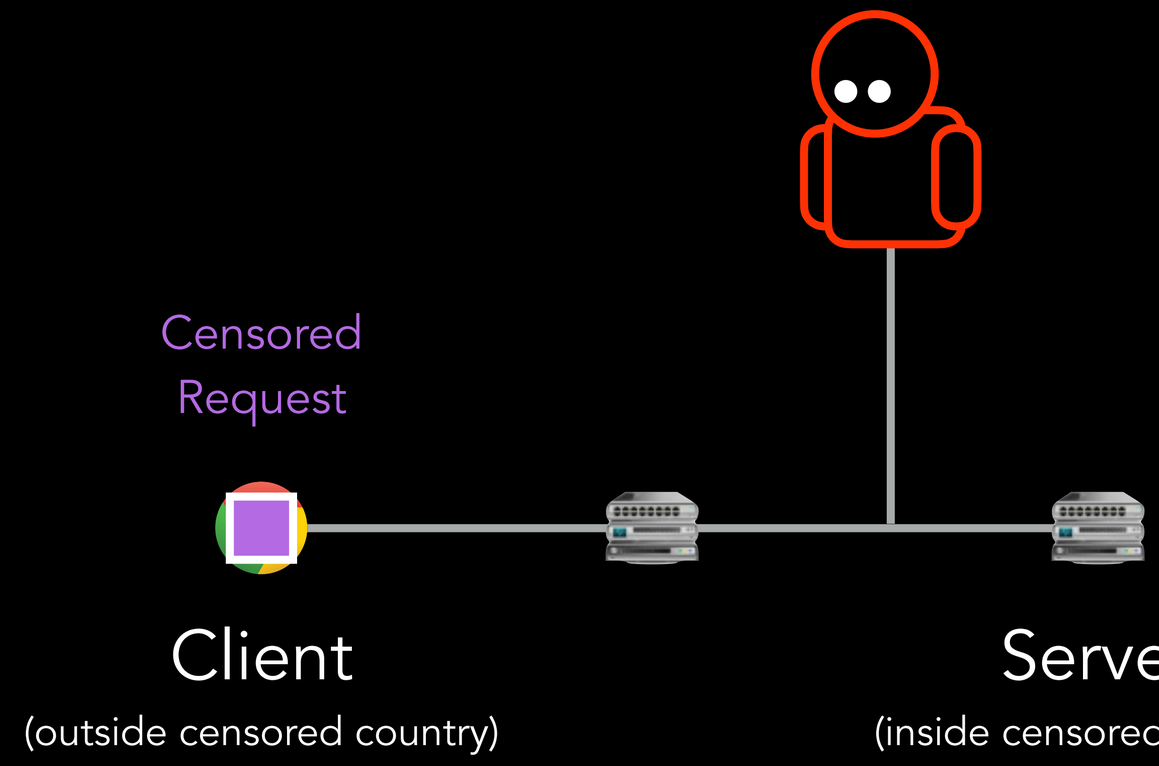
(outside censored country)

Server

(inside censored country)

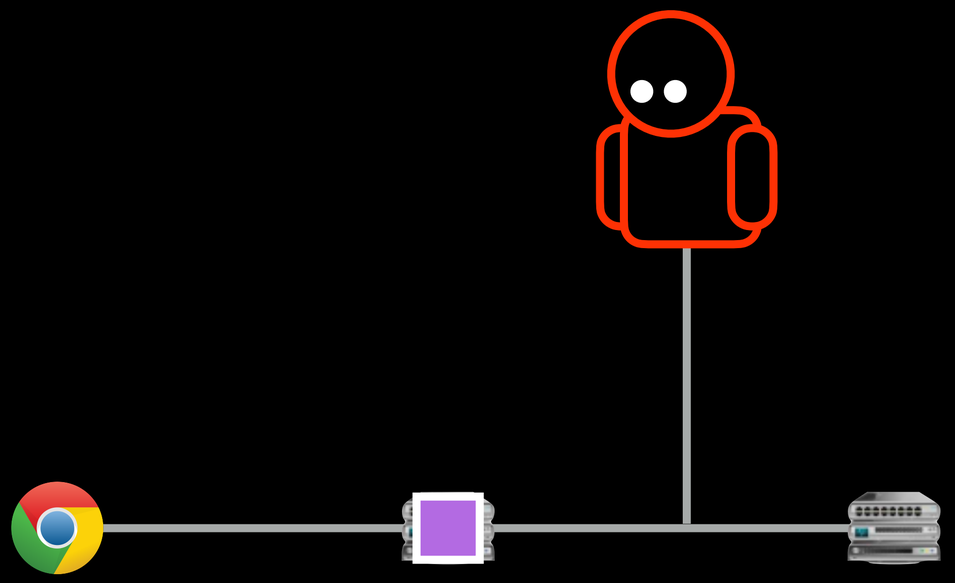
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

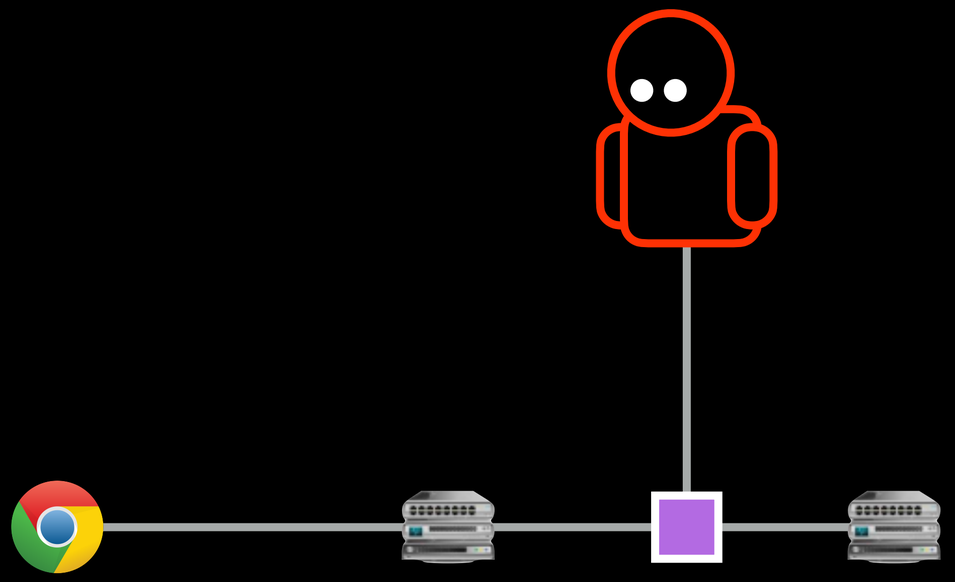
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

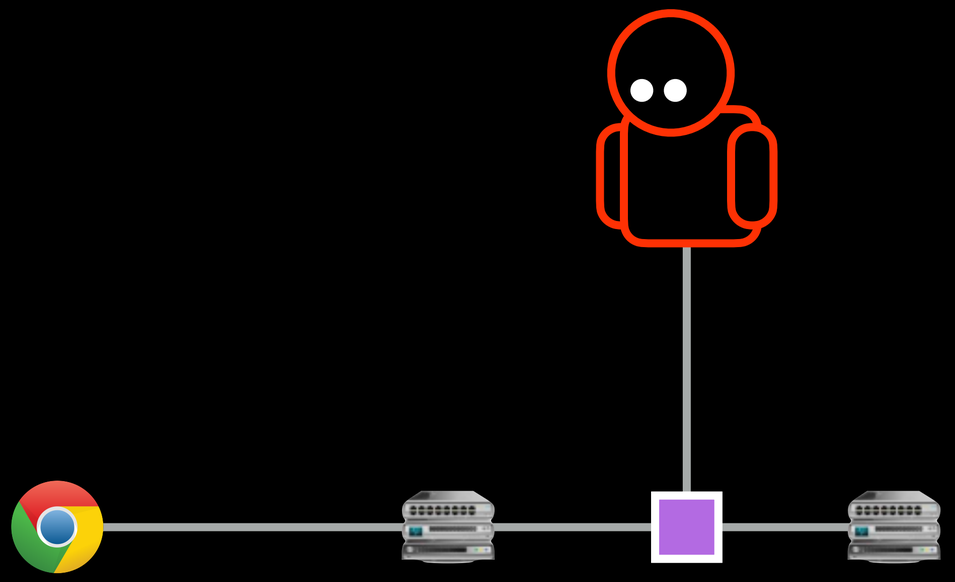
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

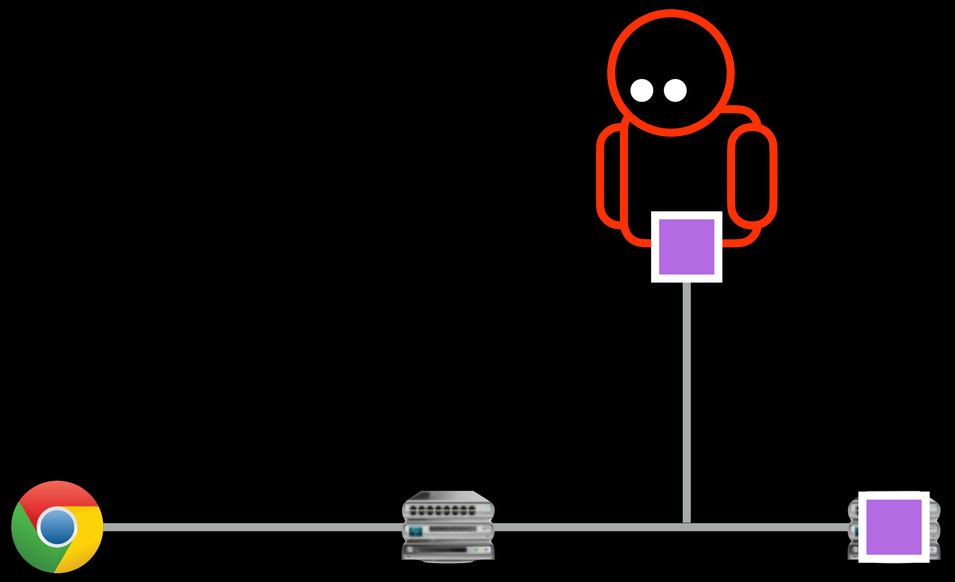
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

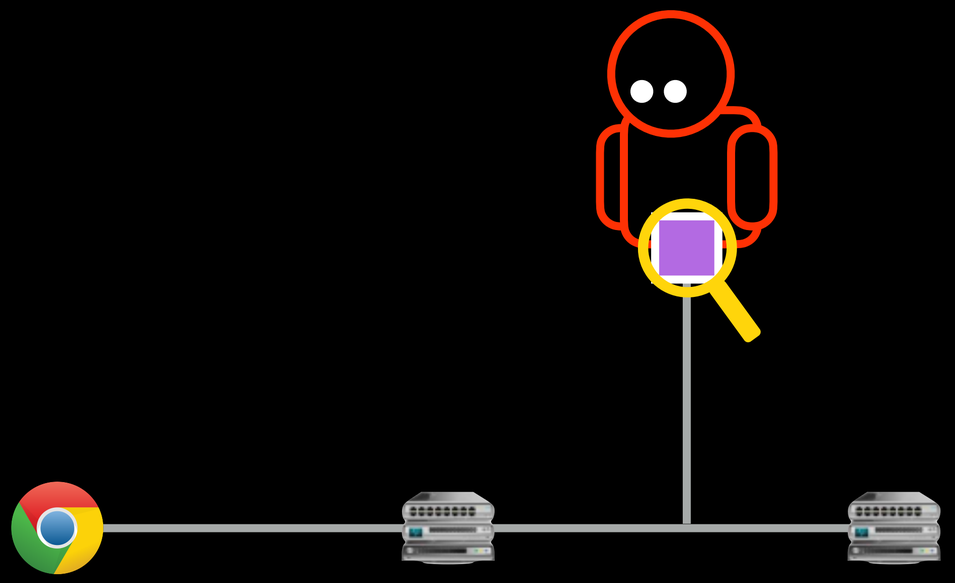
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

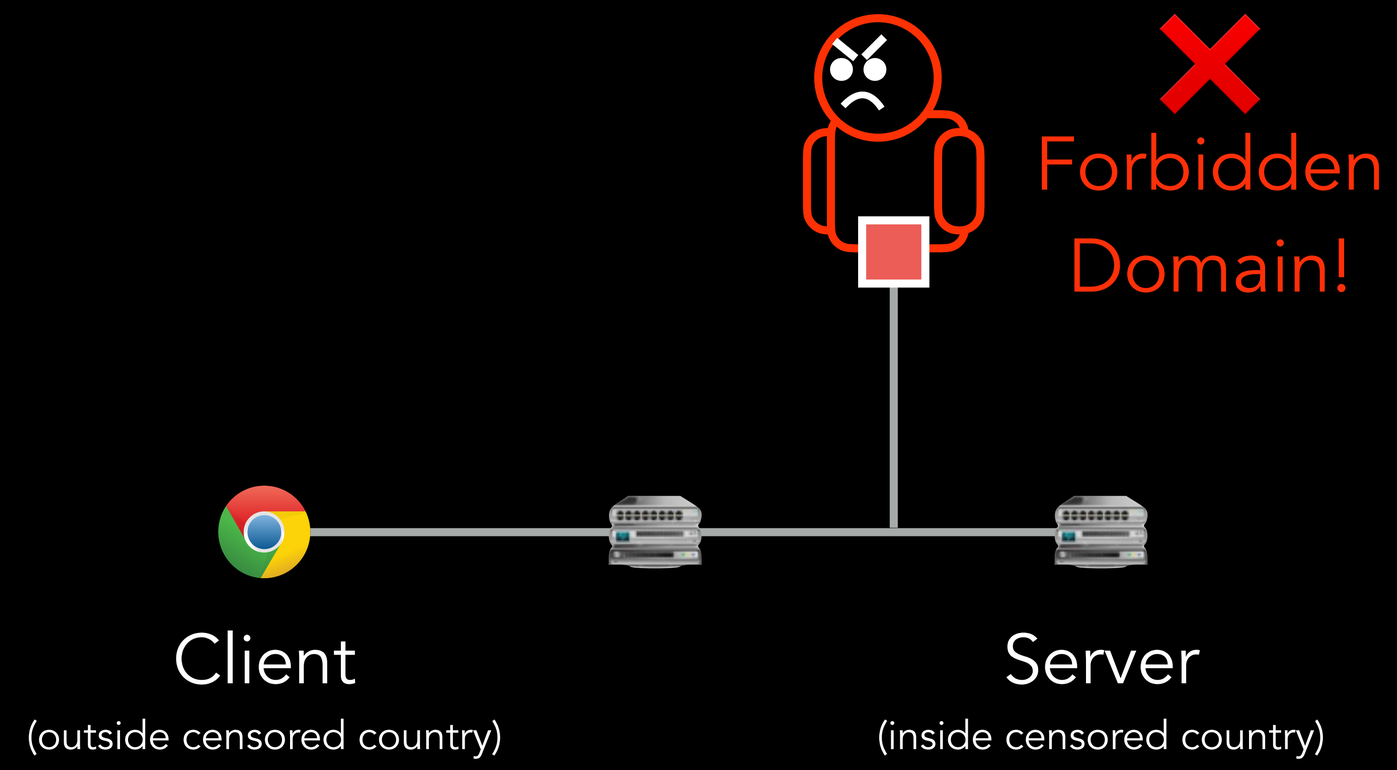
(outside censored country)

Server

(inside censored country)

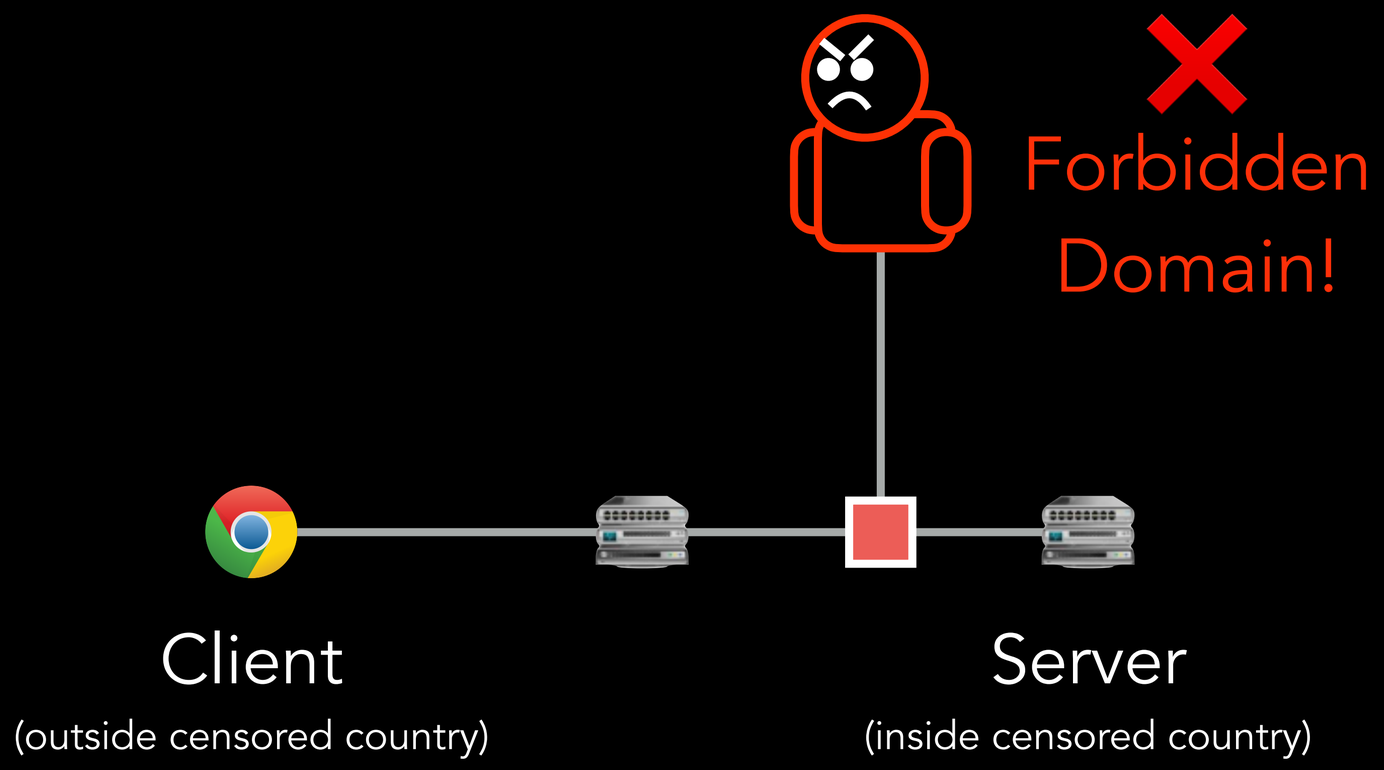
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



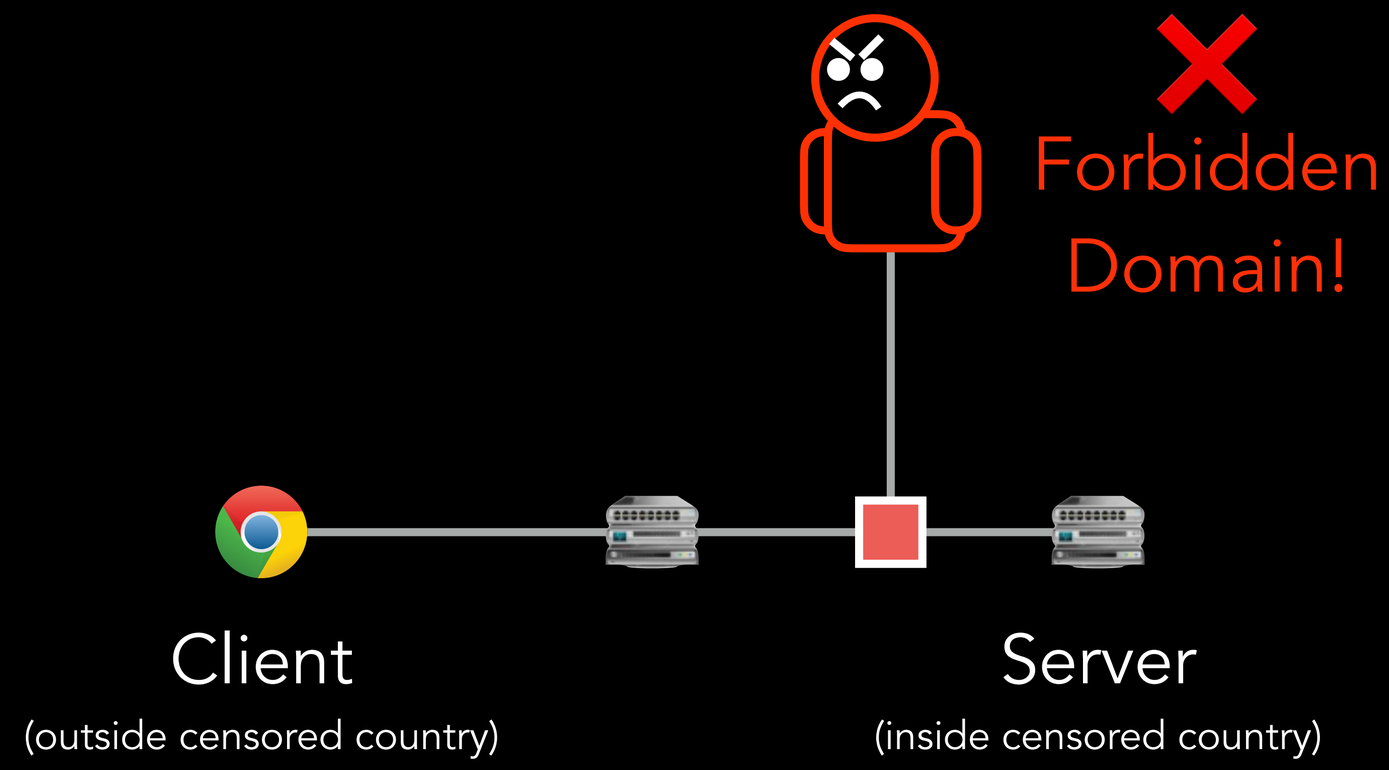
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



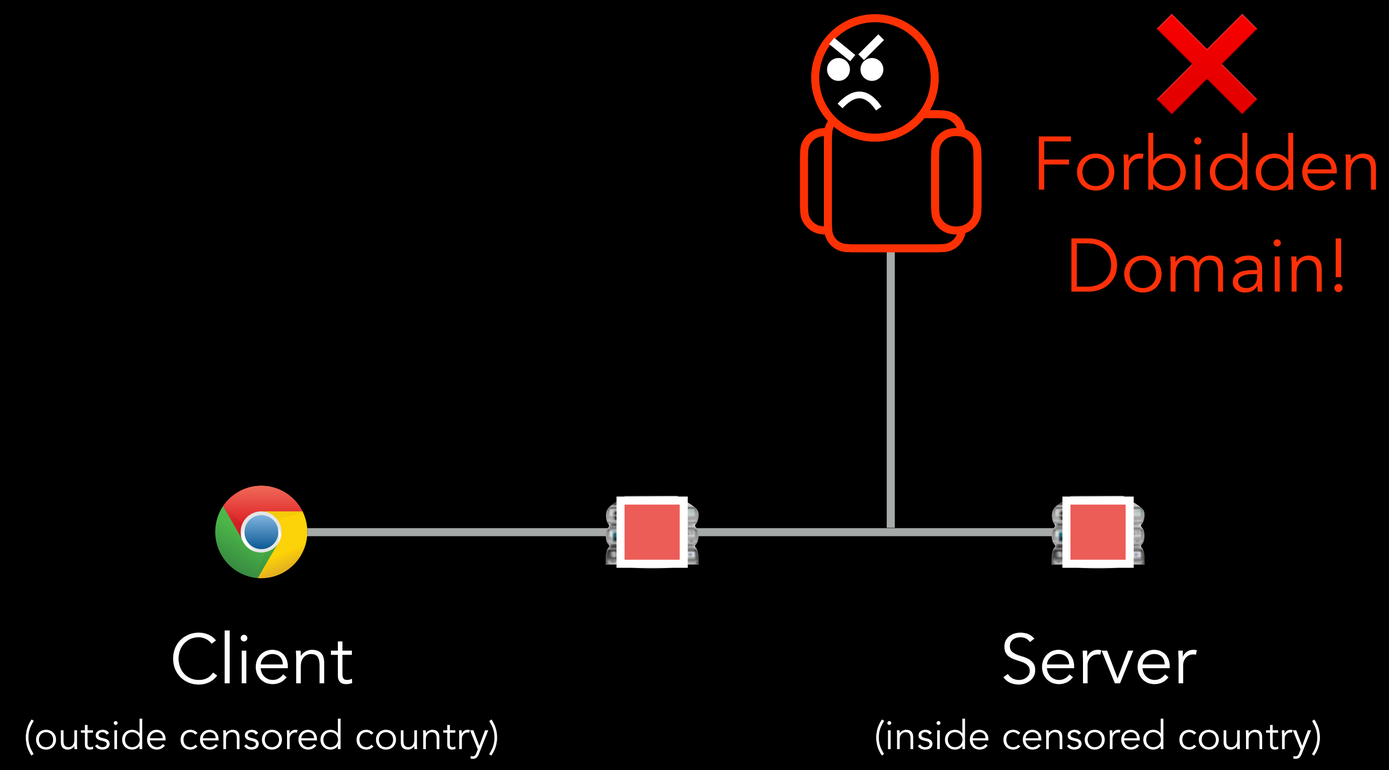
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



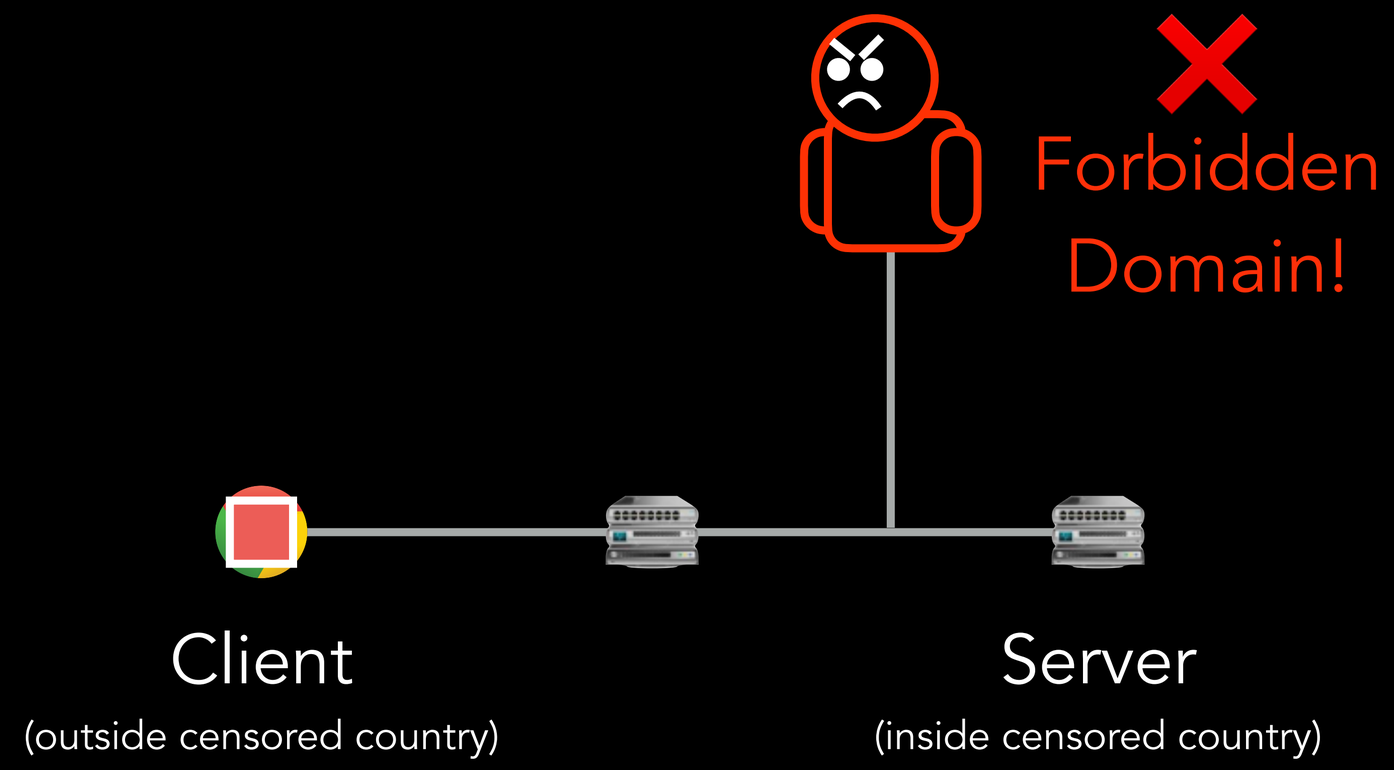
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



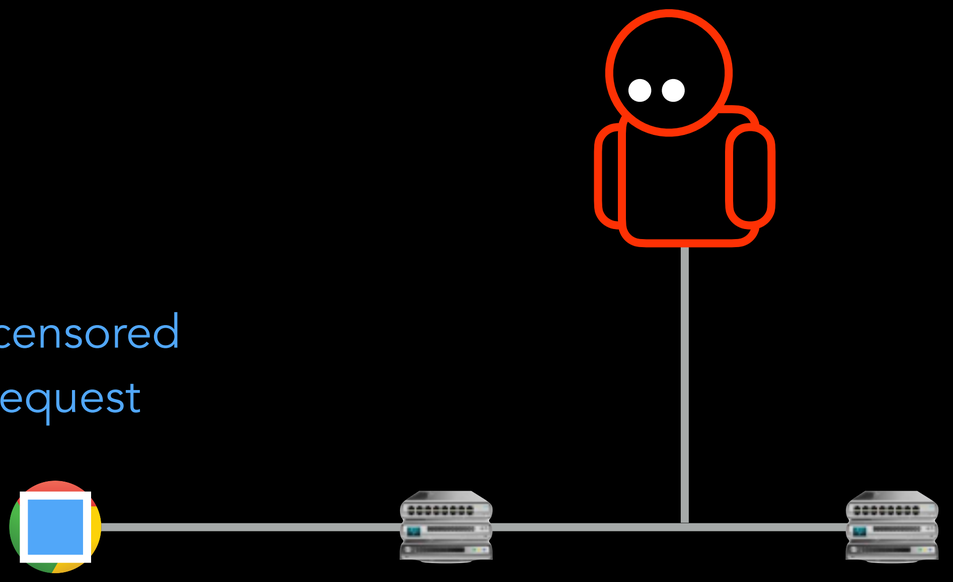
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



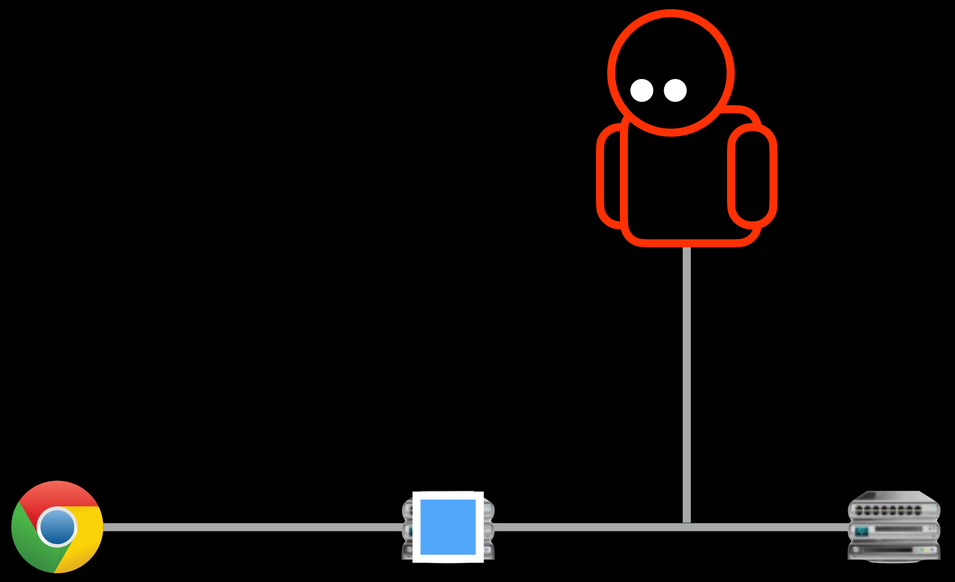
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

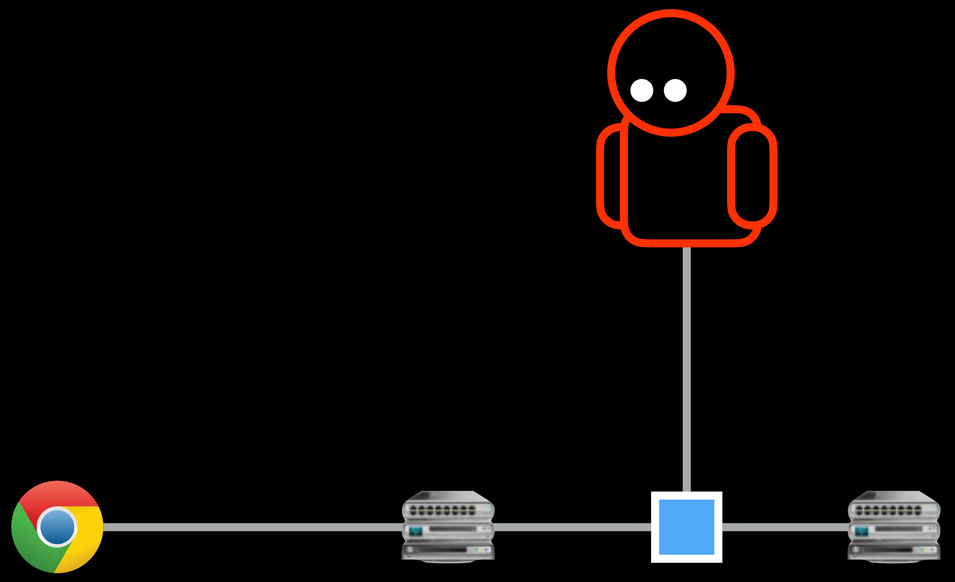
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

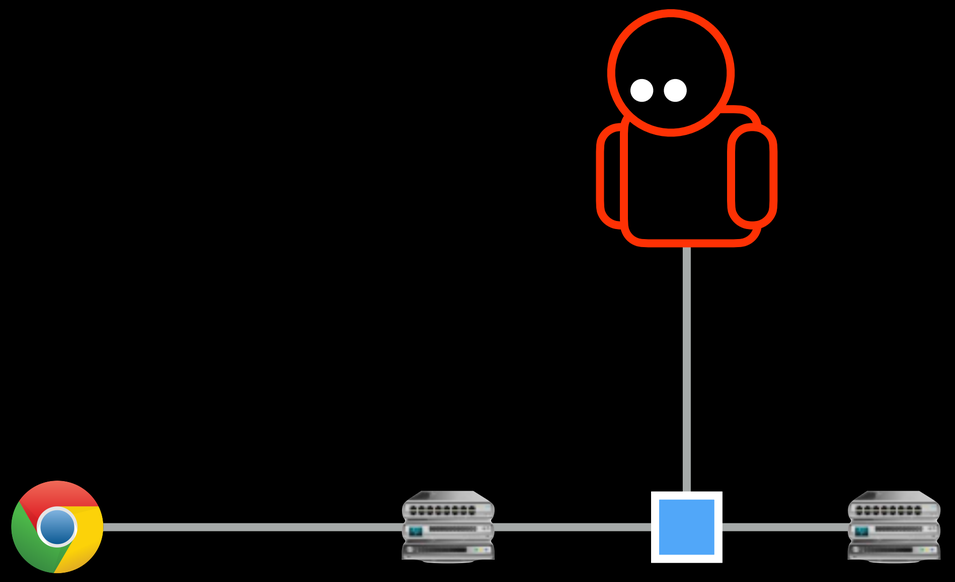
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

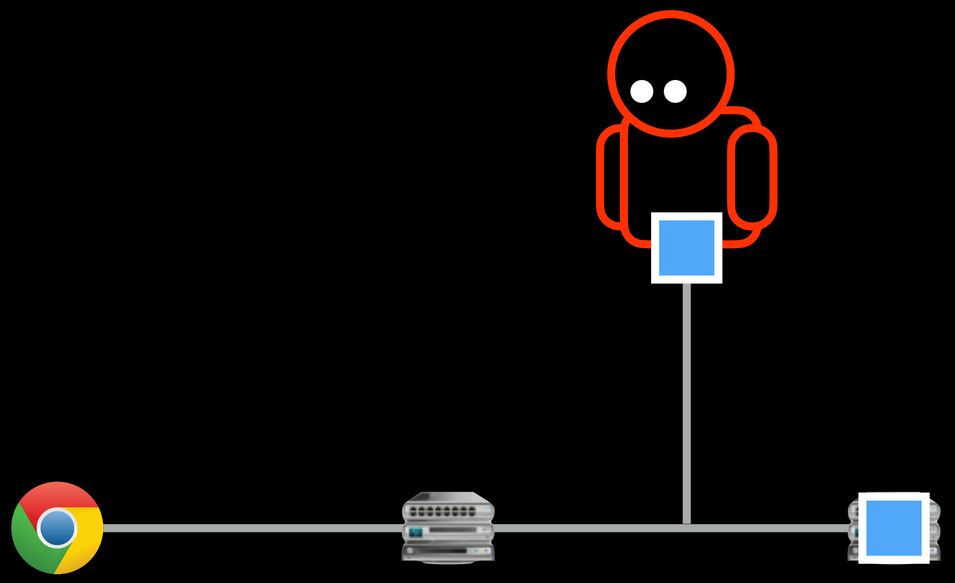
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

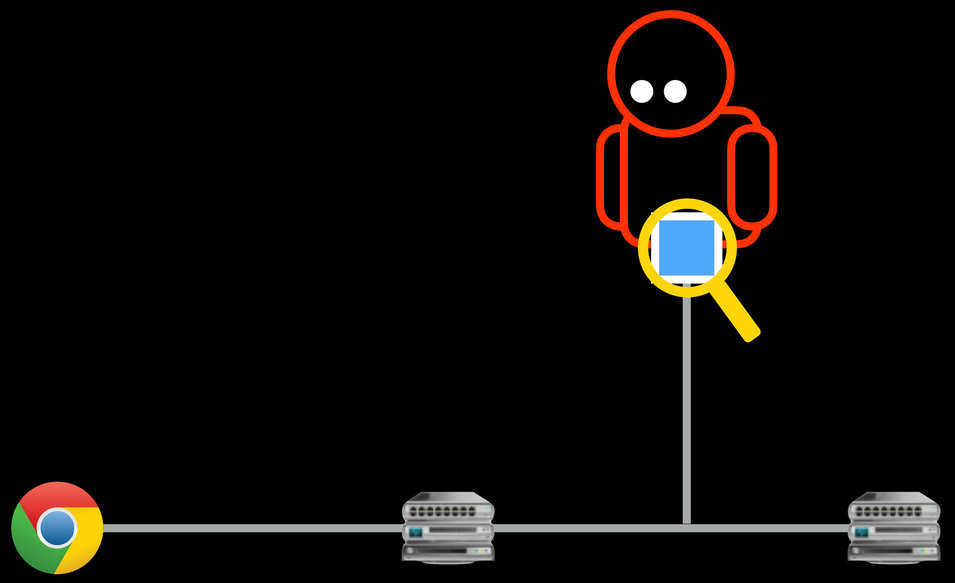
(outside censored country)

Server

(inside censored country)

Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Client

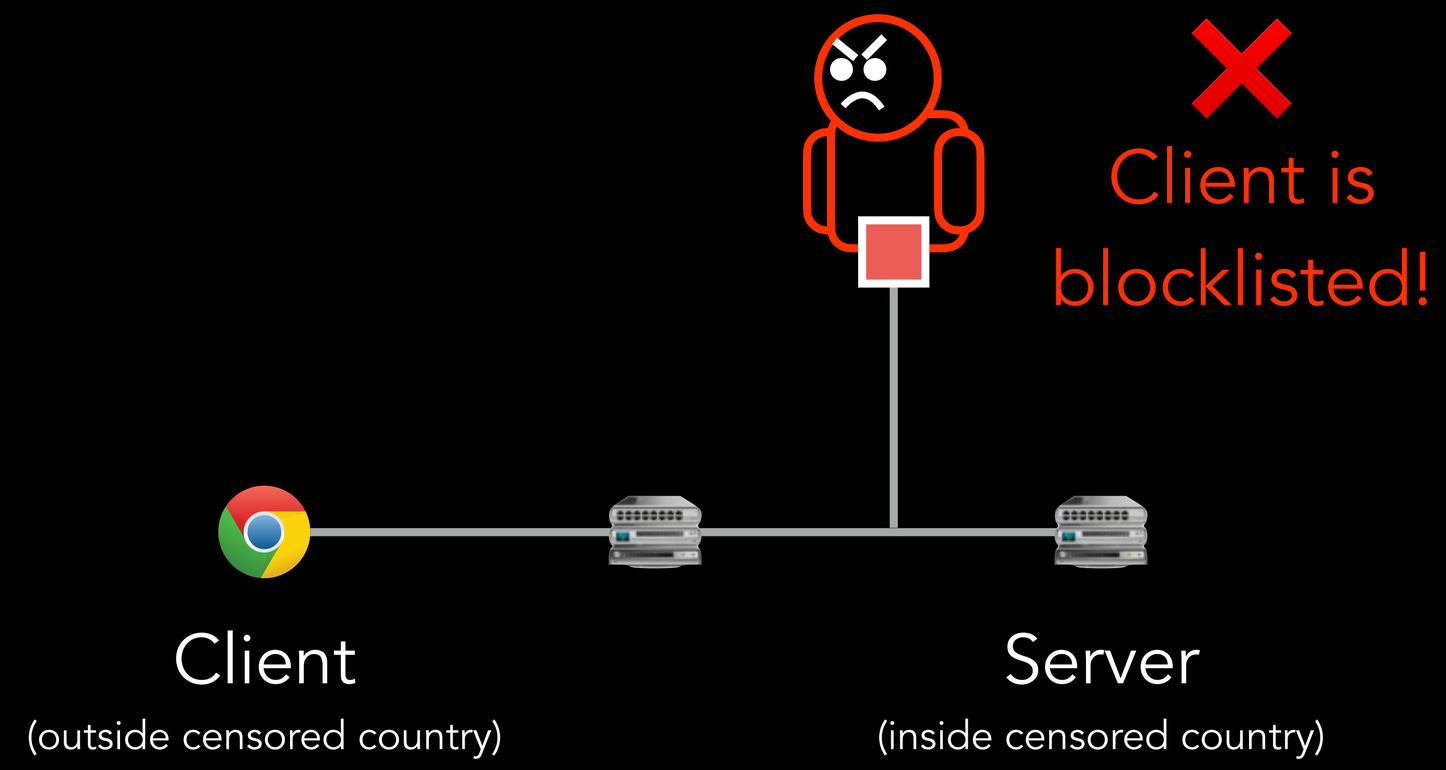
(outside censored country)

Server

(inside censored country)

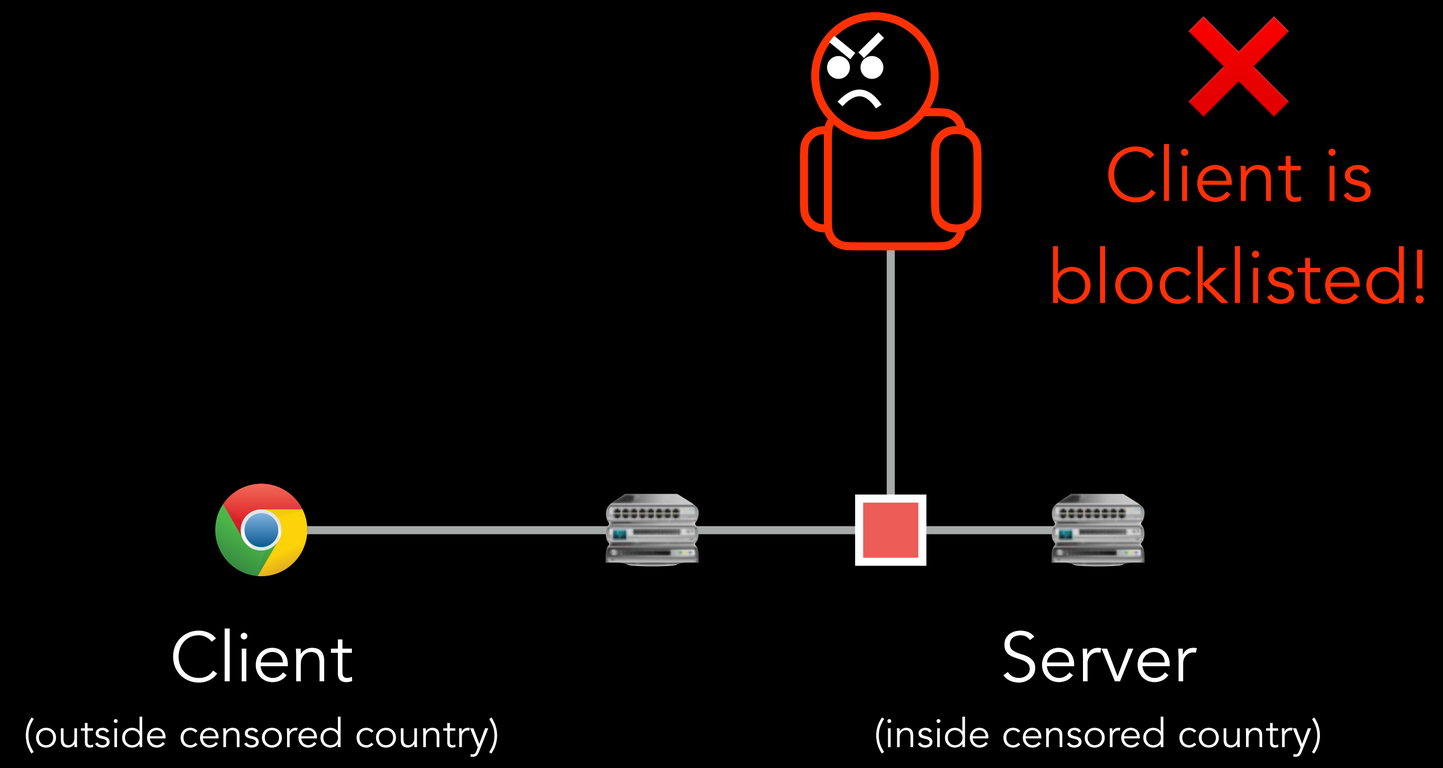
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



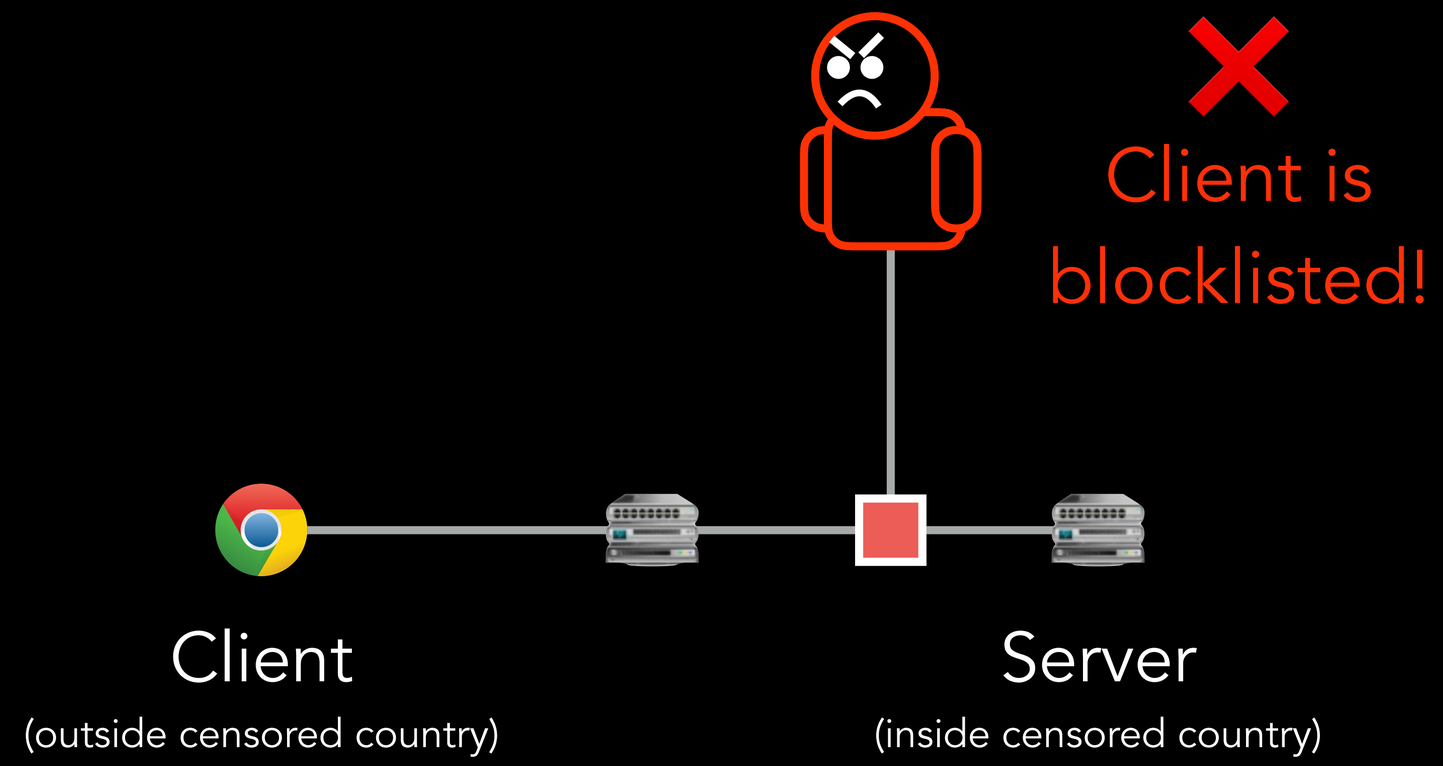
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



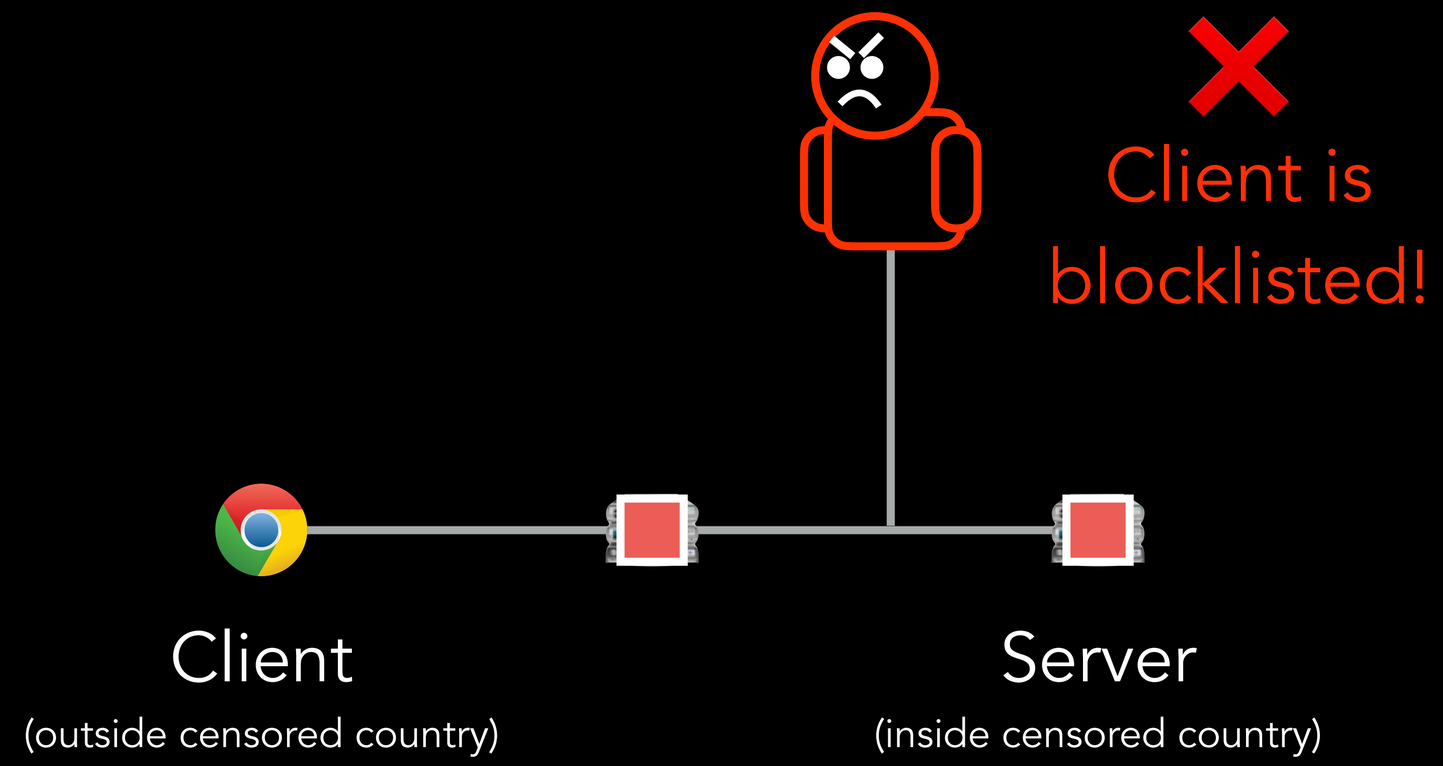
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



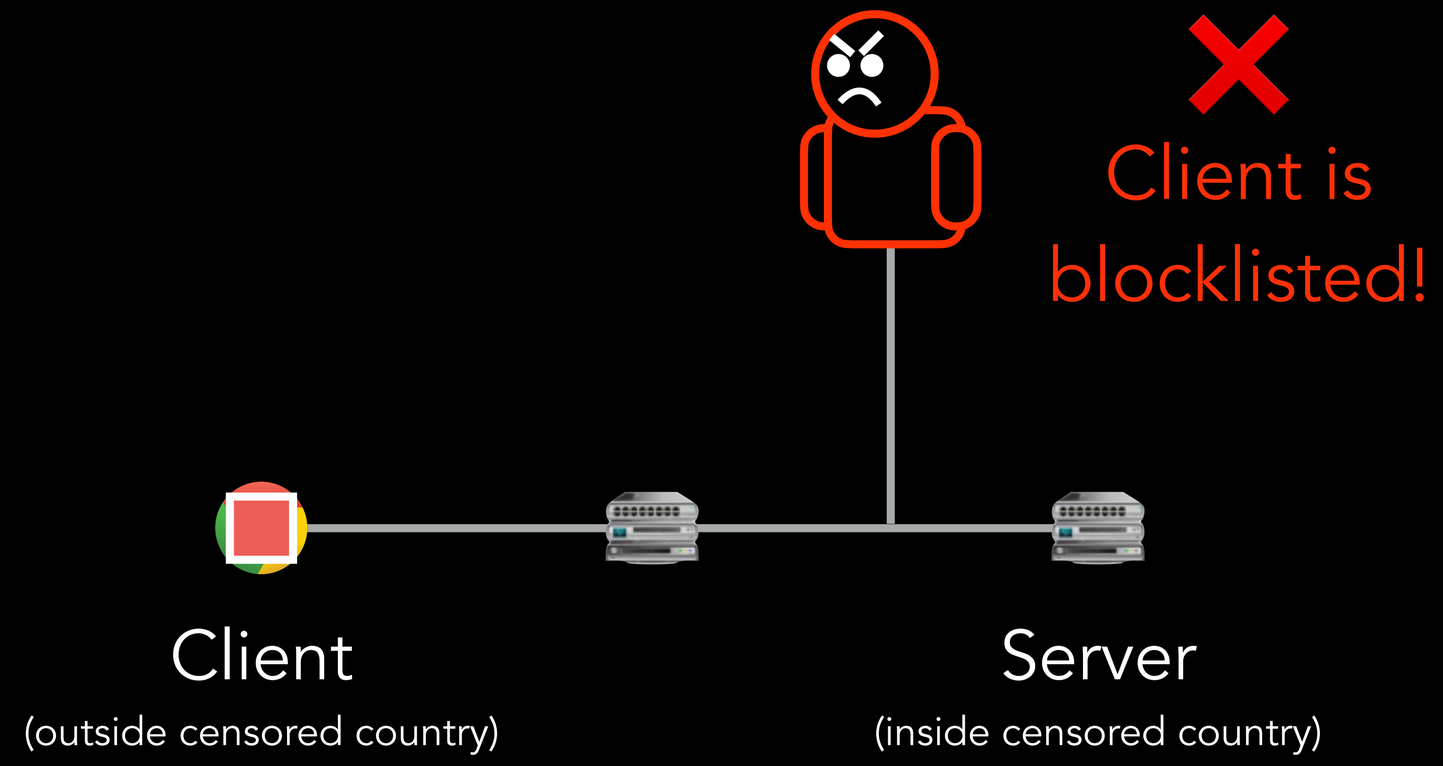
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



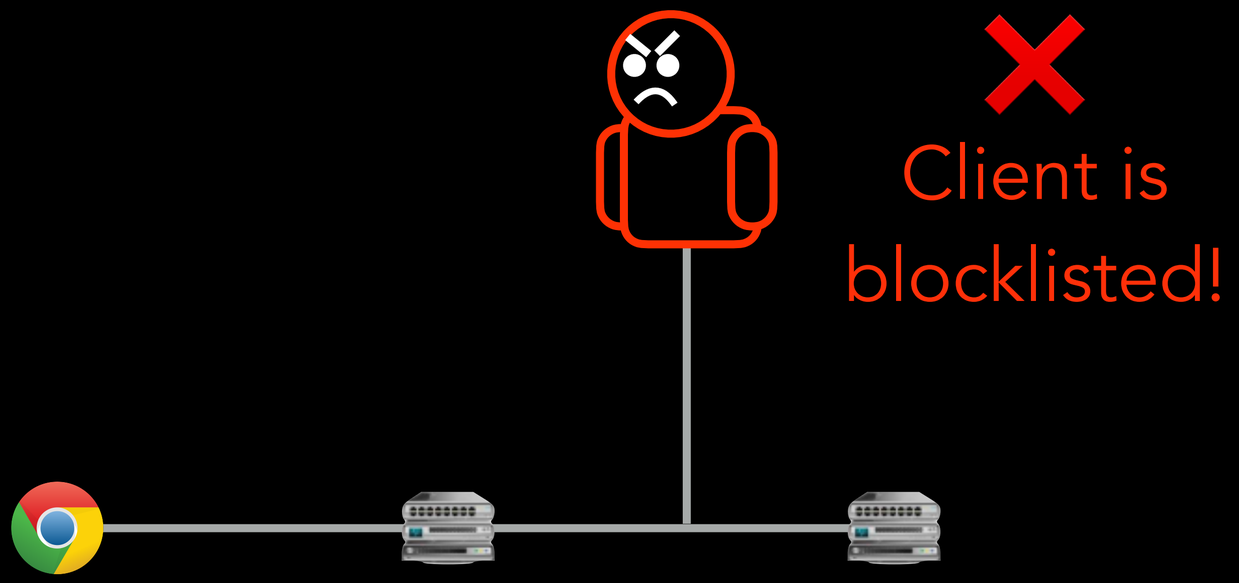
Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



Residual Censorship

Censor filters all requests from a client for an extended period of time due to the client sending a censored request beforehand



High-Level Design

Measurement Probe

Train Geneva on non-responsive IP addresses in the country

If packet sequence Geneva discovers receives a response, it must have come from censor

Send packet sequence with test domains to all other non-responsive IP addresses to conduct measurement

High-Level Design

Measurement Probe

Train Geneva on non-responsive IP addresses in the country

If packet sequence Geneva discovers receives a response,
it must have come from censor

Send packet sequence with test domains to all other
non-responsive IP addresses to conduct measurement

High-Level Design

Measurement Probe

Train Geneva on non-responsive IP addresses in the country

If packet sequence Geneva discovers receives a response, it must have come from censor

Send packet sequence with test domains to all other non-responsive IP addresses to conduct measurement

High-Level Design

Measurement Probe

Train Geneva on non-responsive IP addresses in the country

If packet sequence Geneva discovers receives a response,
it must have come from censor

Send packet sequence with test domains to all other
non-responsive IP addresses to conduct measurement

Agenda

1. Background
2. High-Level Design
3. Preliminary Results

Agenda

1. Background
2. High-Level Design
3. Preliminary Results

Preliminary Results

Brunei

Preliminary Results

Brunei

Bidirectional
Censorship in AS10094

Preliminary Results

Brunei

Bidirectional Censorship in AS10094

SYN followed by PSH+ACK triggers censorship

Preliminary Results

Brunei

Bidirectional Censorship in AS10094

SYN followed by PSH+ACK triggers censorship

No Residual Censorship

Preliminary Results

Tajikistan

Preliminary Results

Tajikistan

Bidirectional
Censorship in AS24722

Preliminary Results

Tajikistan

Bidirectional Censorship in AS24722

Sending a PSH+ACK packet *twice* triggers censorship

Preliminary Results

Tajikistan

Bidirectional Censorship in AS24722

Sending a PSH+ACK packet *twice* triggers censorship

No Residual Censorship

Preliminary Results

Negative Results

We were not able to trigger bidirectional censorship in:

Burundi

Equatorial Guinea

Kyrgyzstan

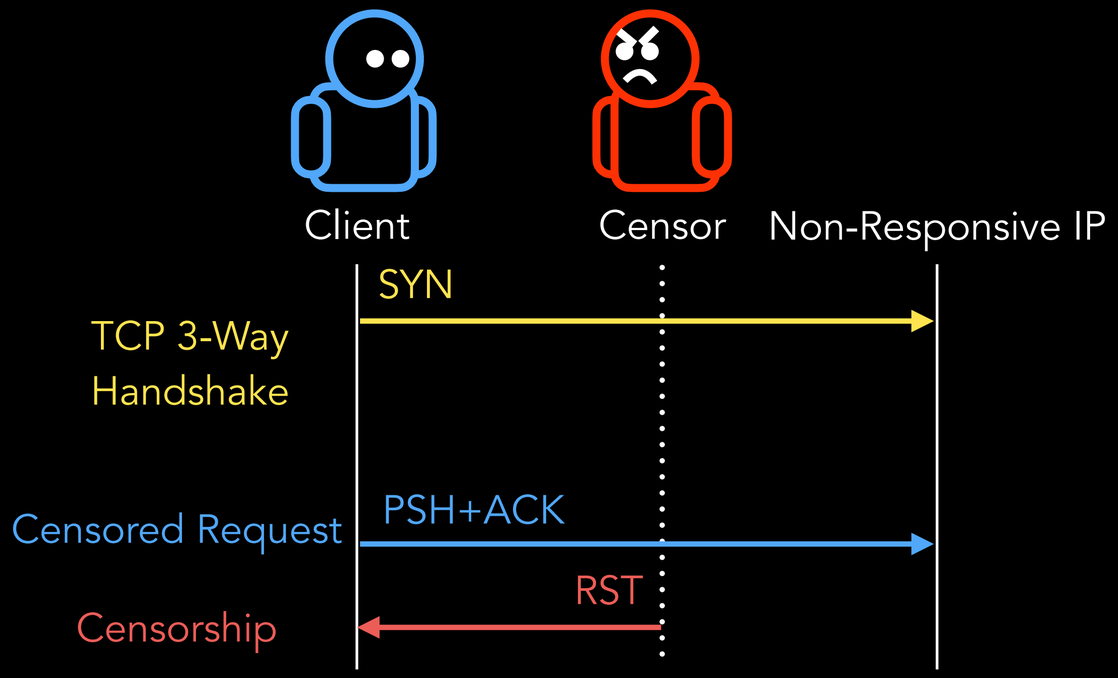
Myanmar

Detecting Network Interference Without Endpoint Participation

Can measure censorship in hard-to-reach networks and hit more endpoints in reachable networks

Limitation — not all ASNs and prefixes in censored countries meets requirements

Open Question — What challenges are we overlooking when implementing this system at a global scale?



Triggering HTTP/HTTPS Censorship Without Endpoint Participation

Website censorship.ai