Measuring and Evading Turkmenistan's Internet Censorship

A Case Study in Large-Scale Measurements of a Low-Penetration Country

Sadia Nourin Van Tran Xi Jiang Kevin Bock
Nick Feamster Nguyen Phong Hoang Dave Levin

UNIVERSITY OF MARYLAND

THE UNIVERSITY OF CHICAGO

Censorship in Turkmenistan

Freedom House Freedom Score: 2/100

RSF Reporters Without Borders "Enemy of the Internet"

Censorship in Turkmenistan

Freedom House — Freedom Score: 2/100

RSF Reporters Without Borders — "Enemy of the Internet"

Censorship in Turkmenistan

Internet Censorship

Freedom House Freedom Score: 2/100

RSF REPORTERS WITHOUT BORDERS "Enemy of the Internet"

Censorship in Turkmenistan

Internet Censorship

Freedom House Freedom Score: 2/100

RSF REPORTERS WITHOUT BORDERS "Enemy of the Internet"

Censorship in Turkmenistan

Internet Censorship

Freedom House Freedom Score: 2/100

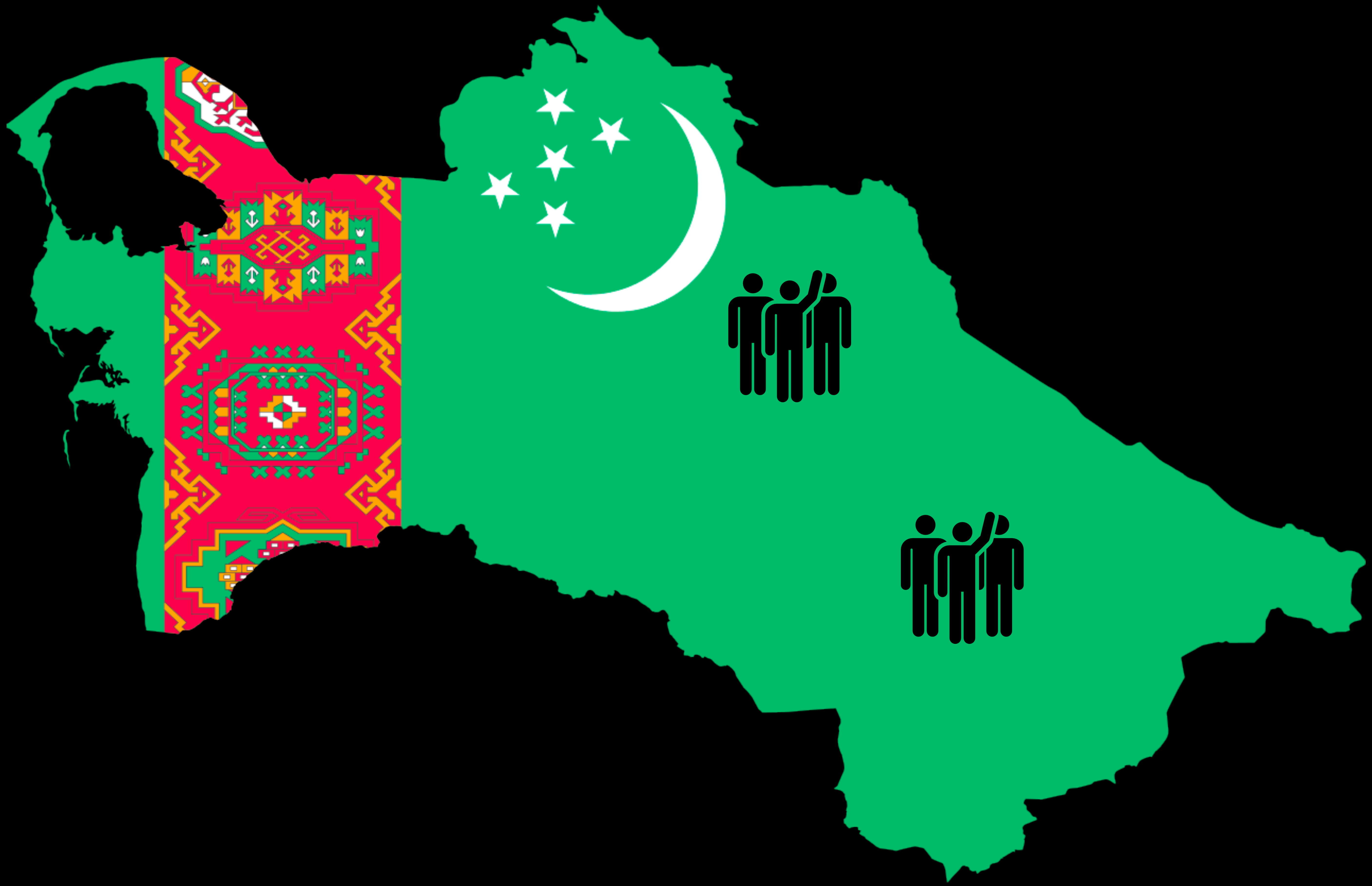
RSF REPORTERS WITHOUT BORDERS "Enemy of the Internet"

Censorship in Turkmenistan

Population =
6 million

Internet Penetration =
38%

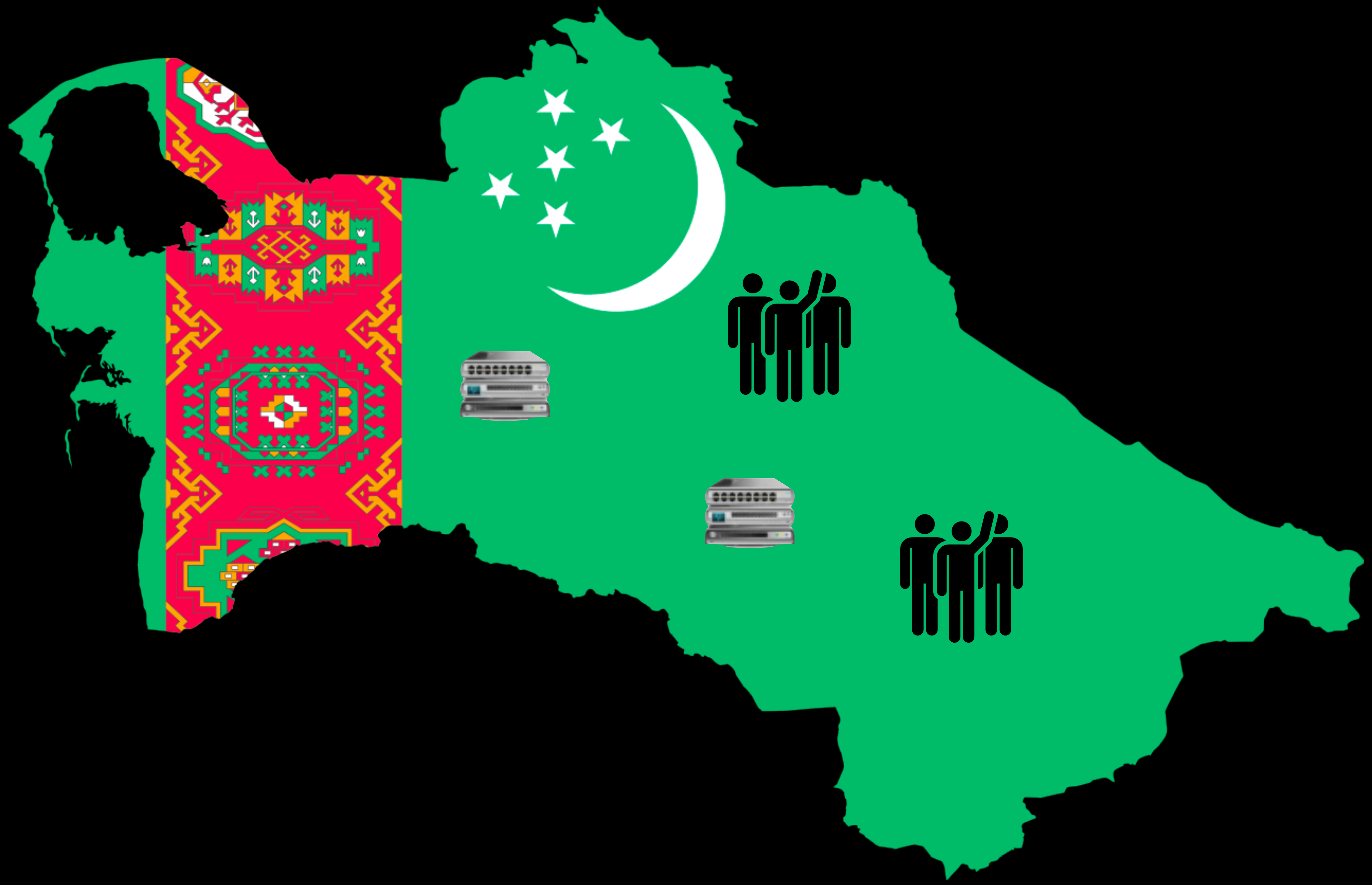
Censorship in Turkmenistan



Population =
6 million

Internet Penetration =
38%

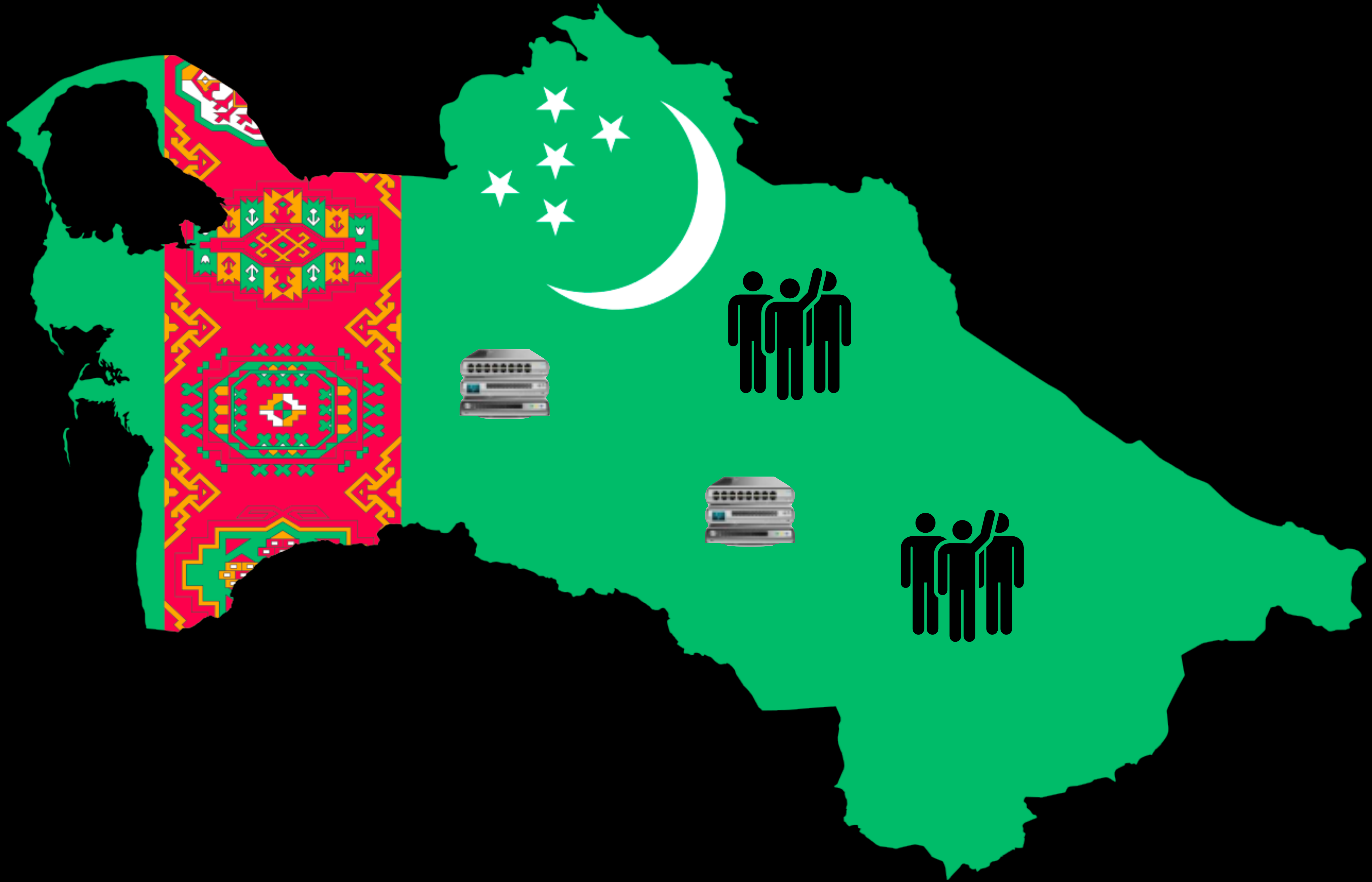
Censorship in Turkmenistan



Population =
6 million

Internet Penetration =
38%

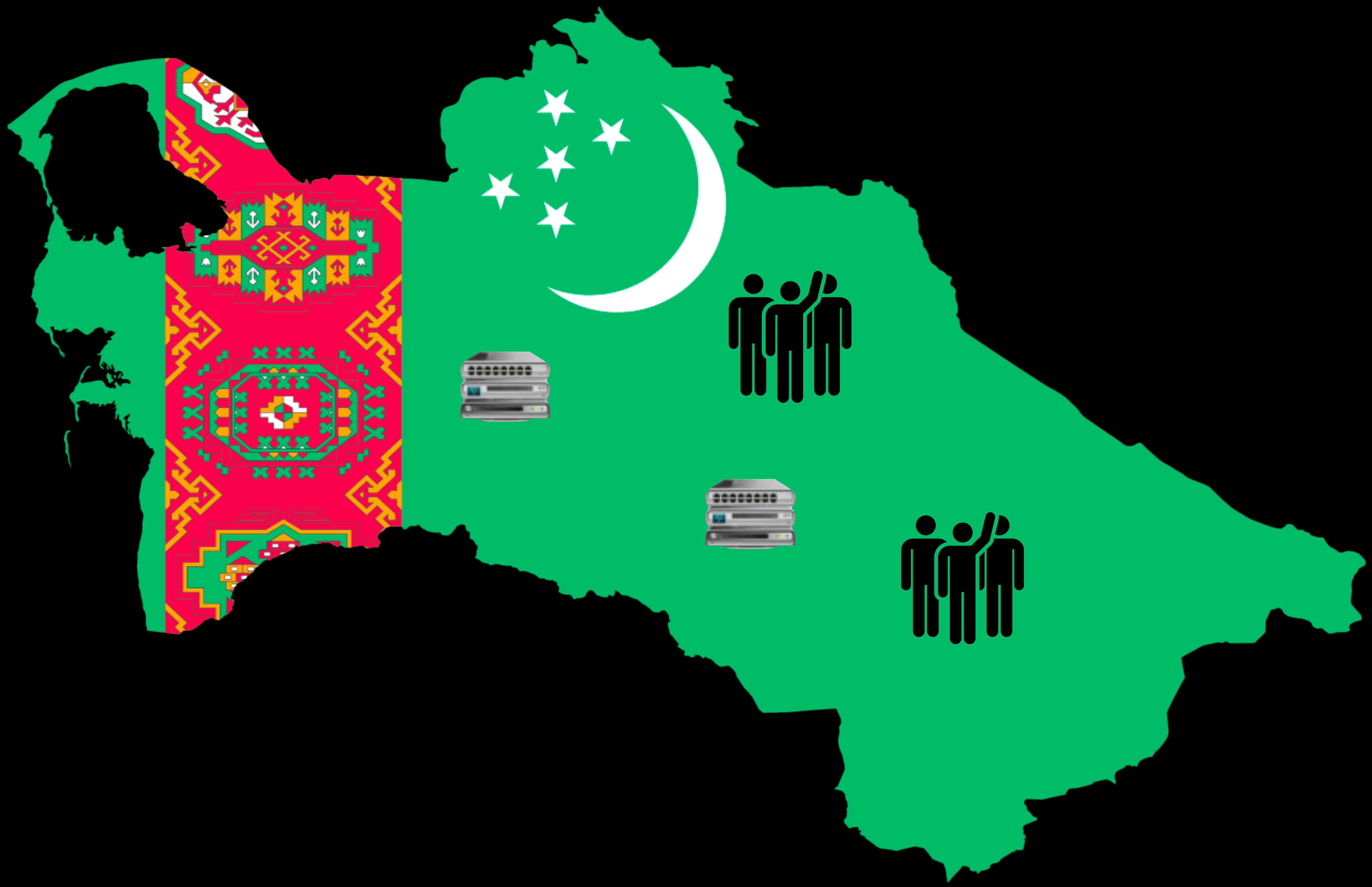
Censorship in Turkmenistan



Population =
6 million

Internet Penetration =
38%

Censorship in Turkmenistan



Population =
6 million

Internet Penetration =
38%

Censorship in Turkmenistan

Population =
6 million

Internet Penetration =
38%

TMC

TurkMenistan Censorship

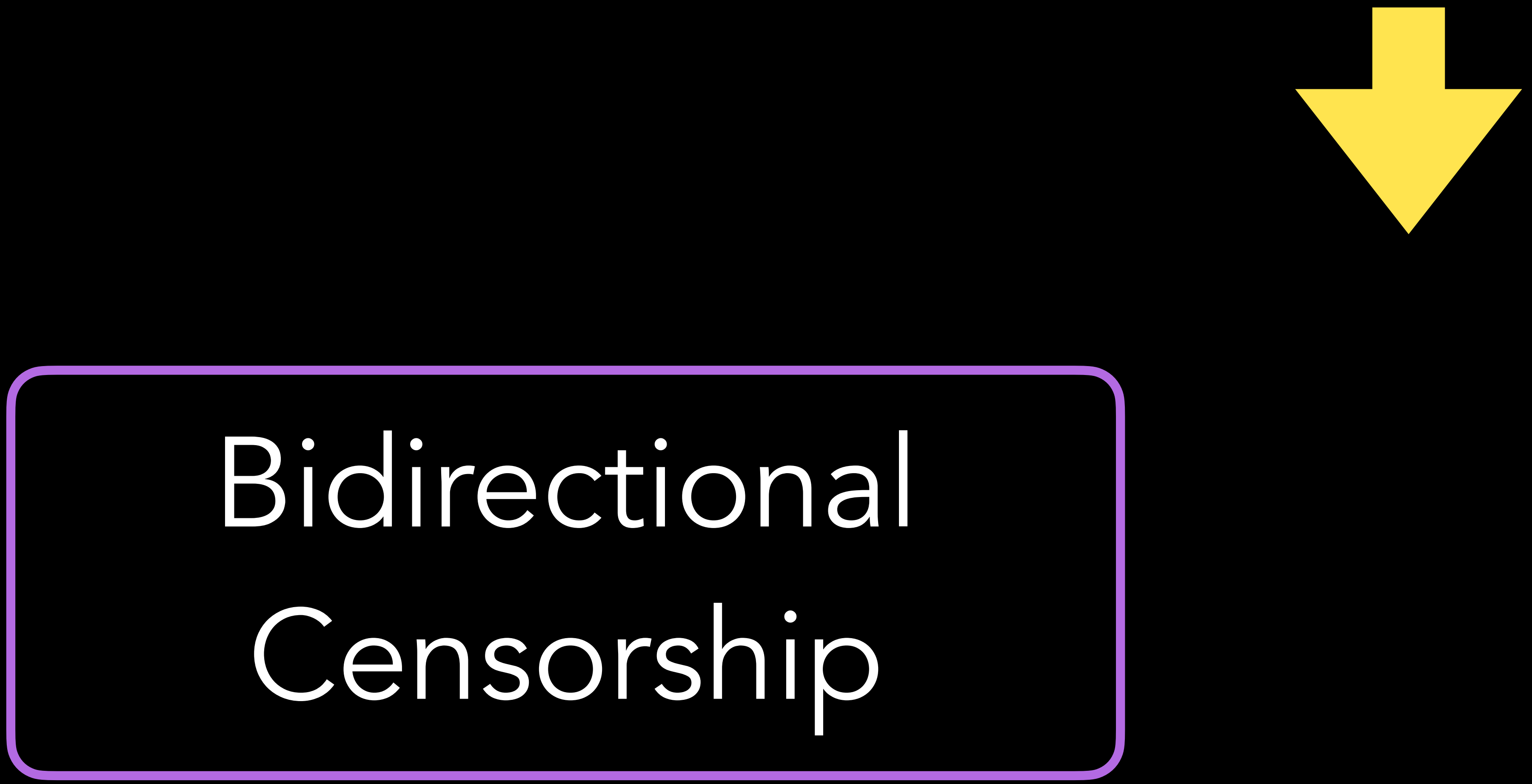
Measures Censorship without Vantage Points

↓

TMC

TurkMenistan Censorship

Measures Censorship without Vantage Points

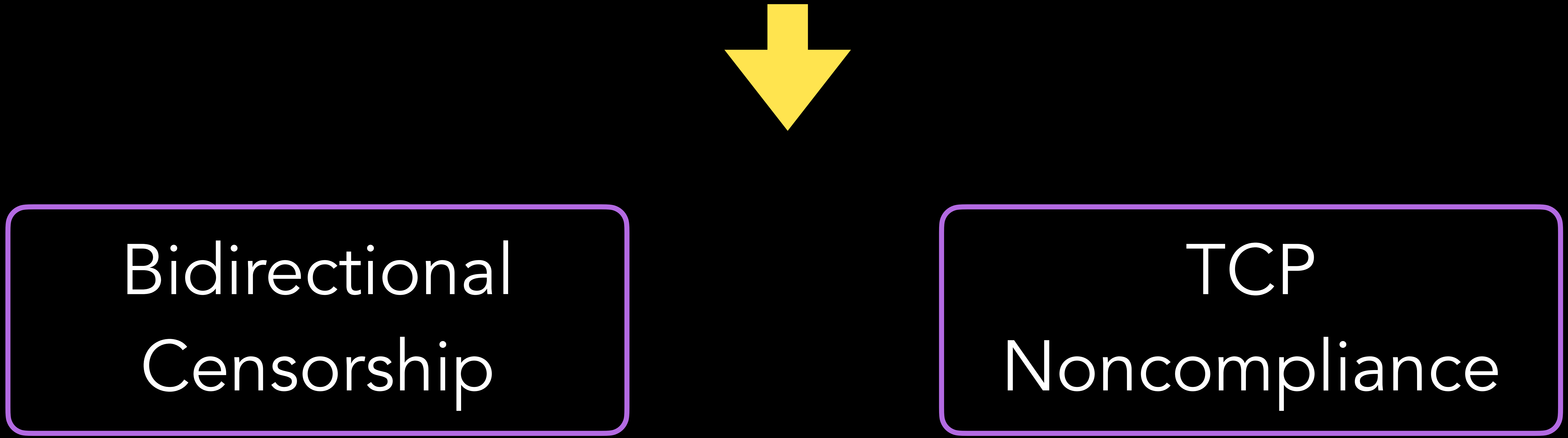


Bidirectional Censorship

TMC

TurkMenistan Censorship

Measures Censorship without Vantage Points



Bidirectional Censorship

TCP Noncompliance

TMC

1. Tests 15.5 million domains
2. DNS, HTTP, and HTTPS filtering
3. No Vantage Points or Endpoint Participation

TMC

1. Tests 15.5 million domains
2. DNS, HTTP, and HTTPS filtering
3. No Vantage Points or Endpoint Participation

TMC

1. Tests 15.5 million domains
2. DNS, HTTP, and HTTPS filtering
3. No Vantage Points or Endpoint Participation

TMC

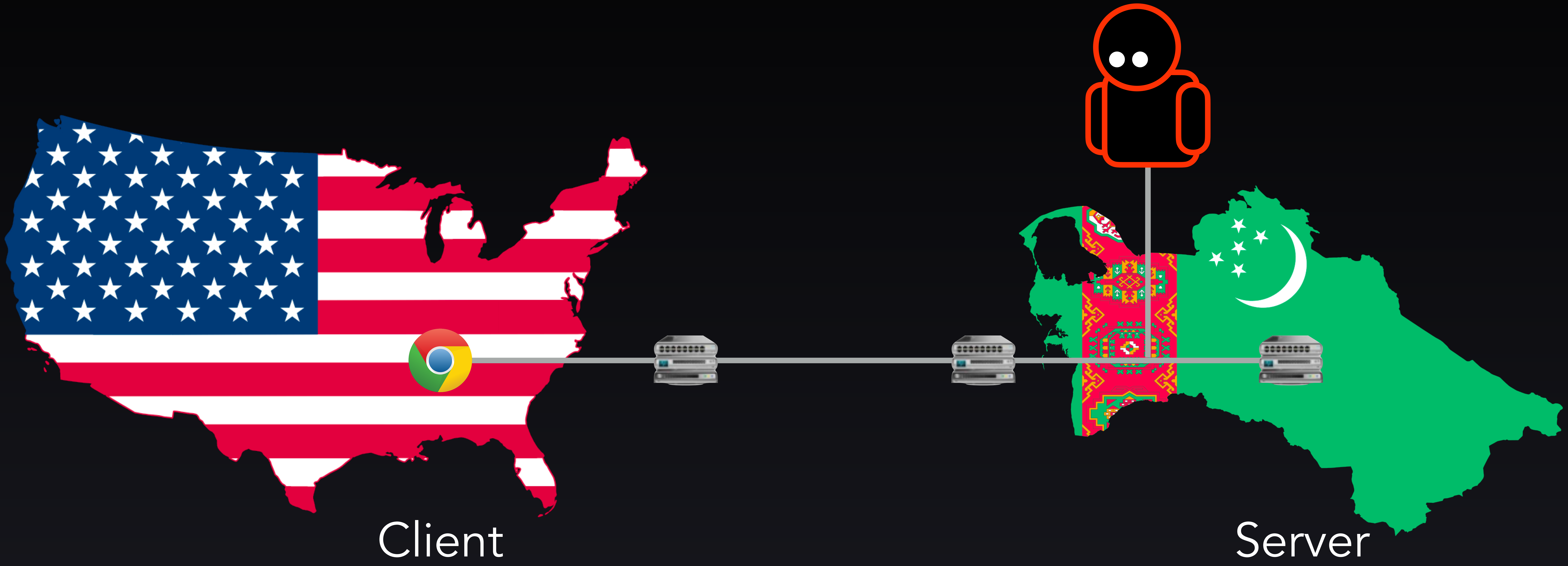
1. Tests 15.5 million domains

2. DNS, HTTP, and HTTPS filtering

3. No Vantage Points or Endpoint Participation

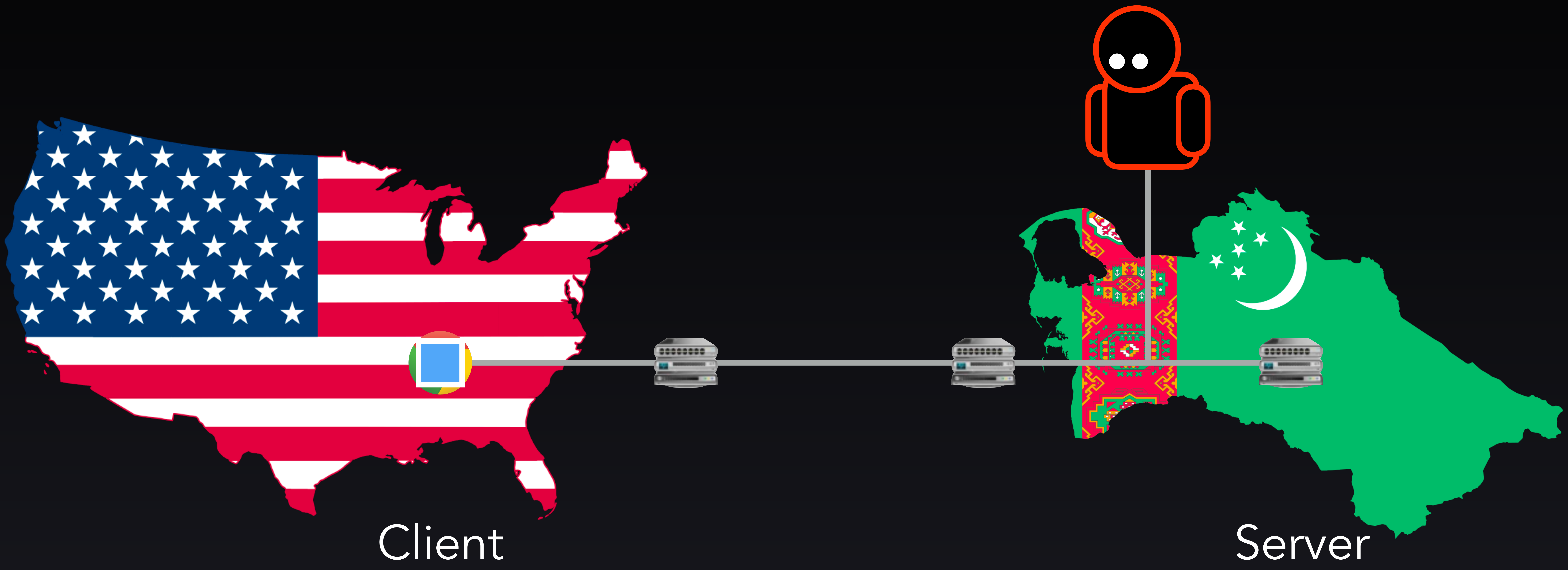
TMC Design

Bidirectional Censorship



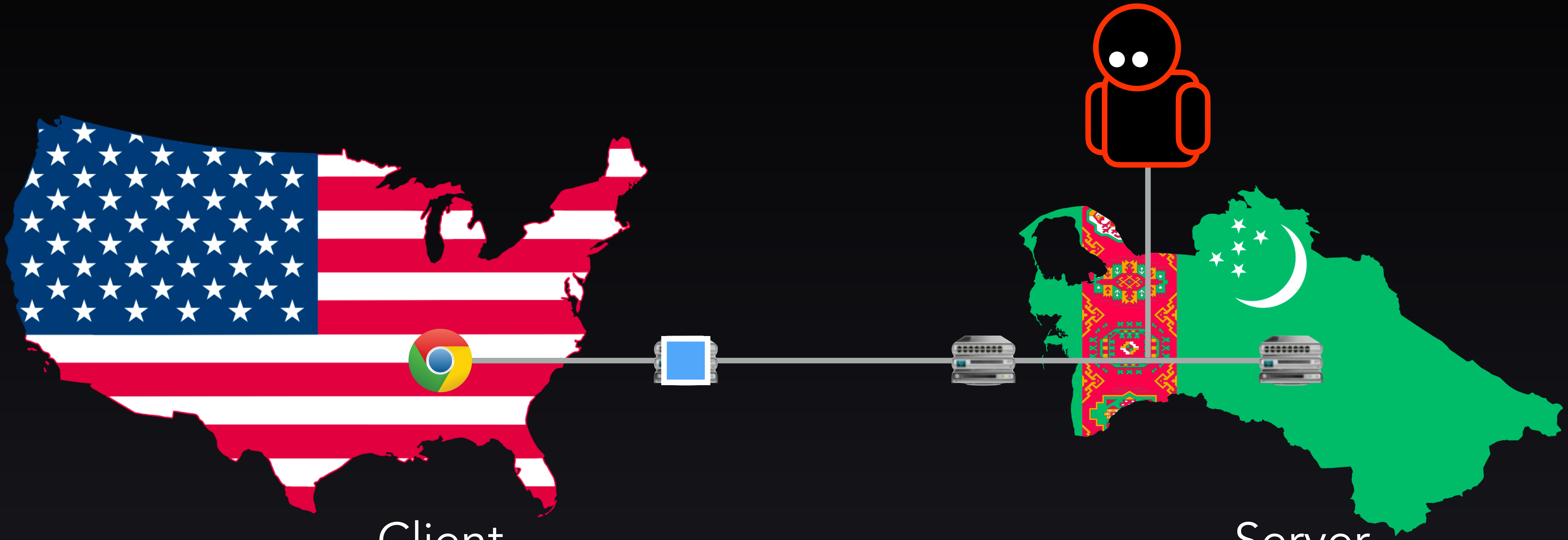
TMC Design

Bidirectional Censorship



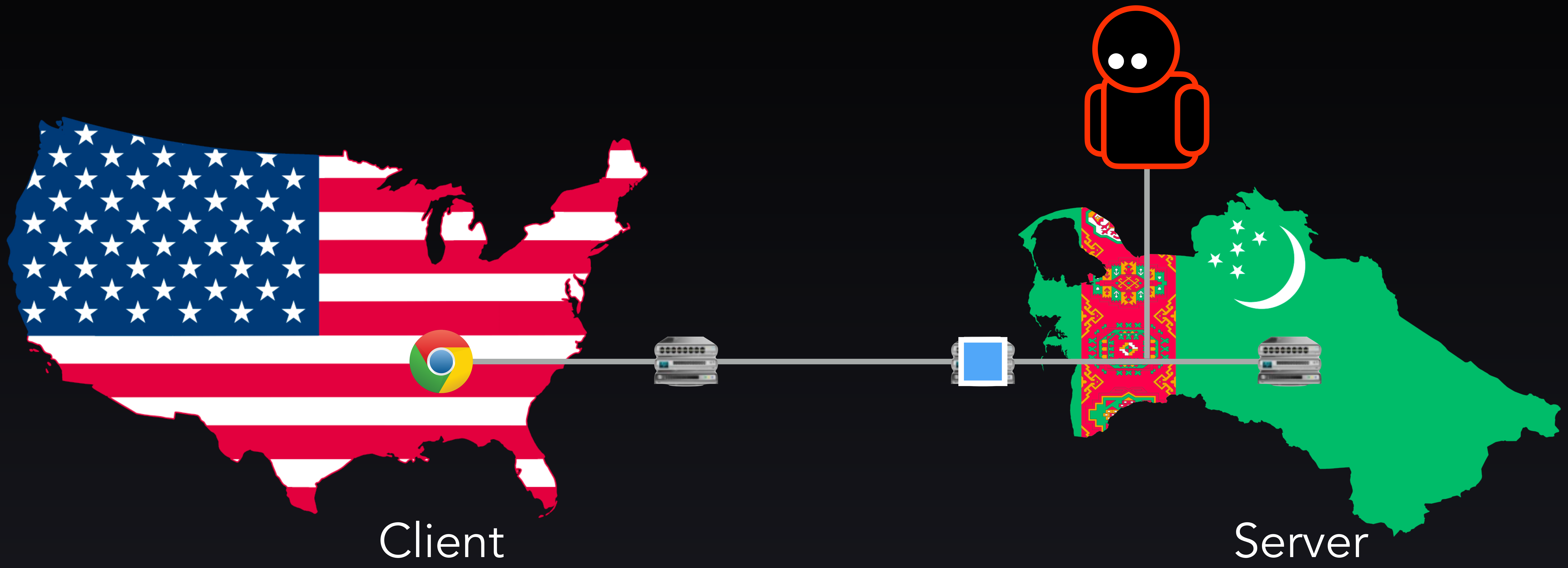
TMC Design

Bidirectional Censorship



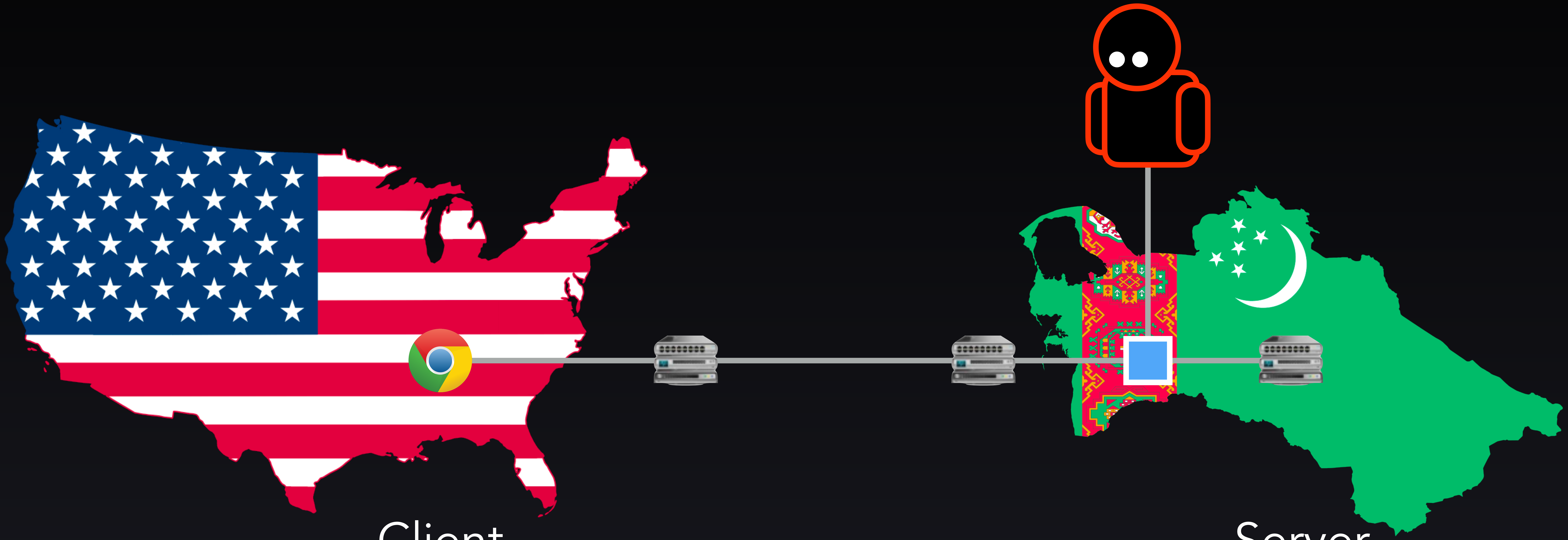
TMC Design

Bidirectional Censorship



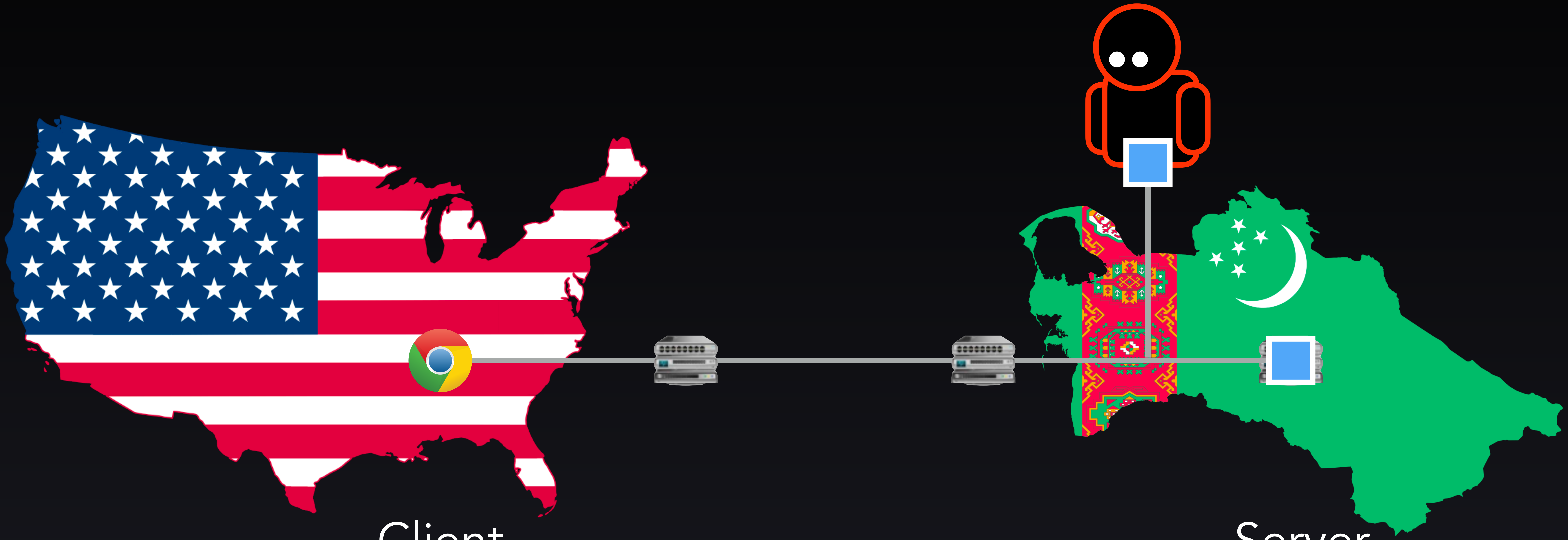
TMC Design

Bidirectional Censorship



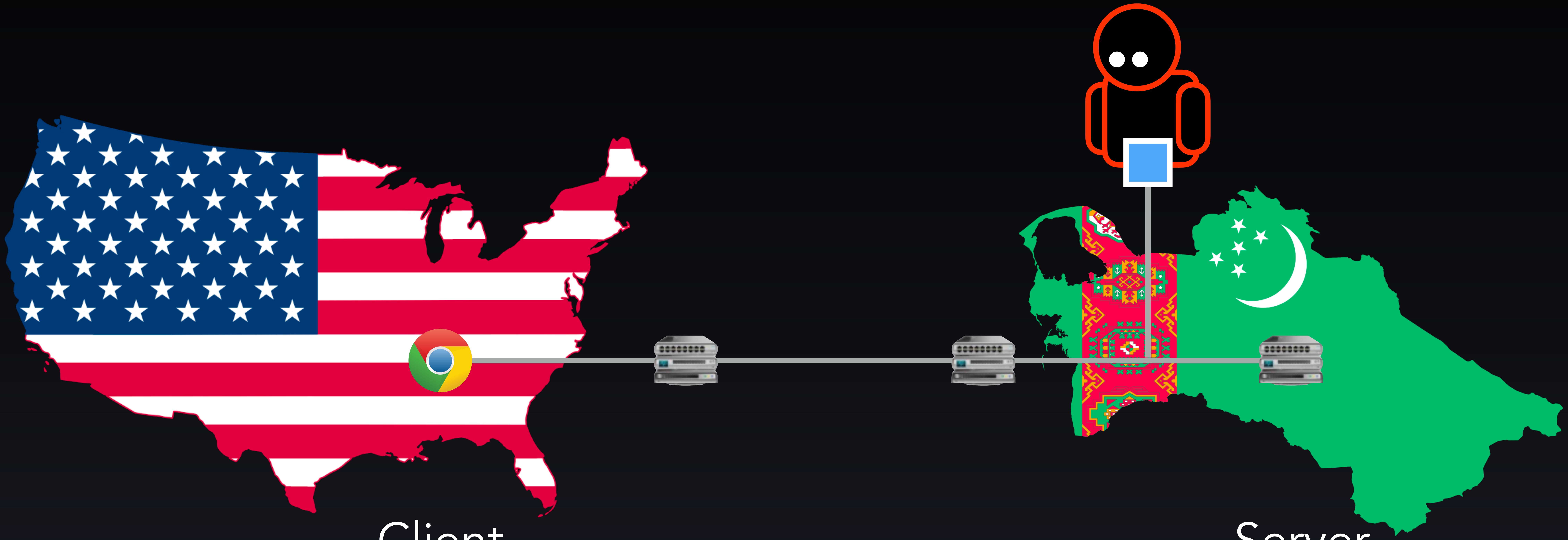
TMC Design

Bidirectional Censorship



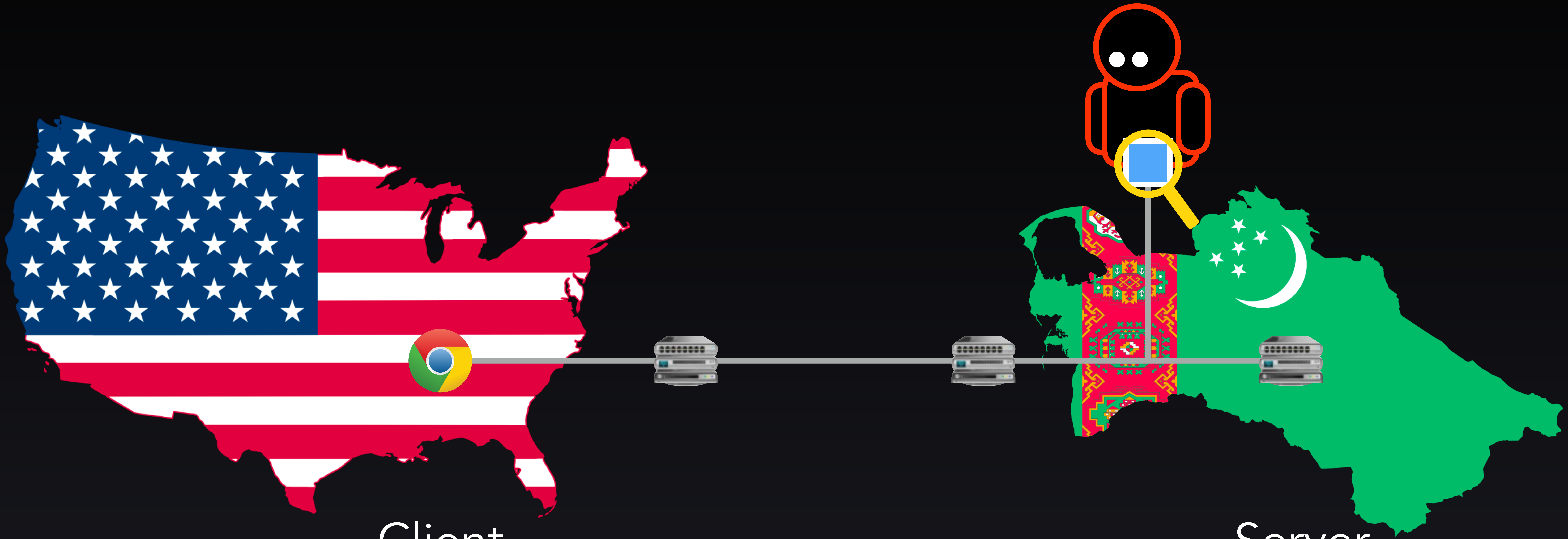
TMC Design

Bidirectional Censorship



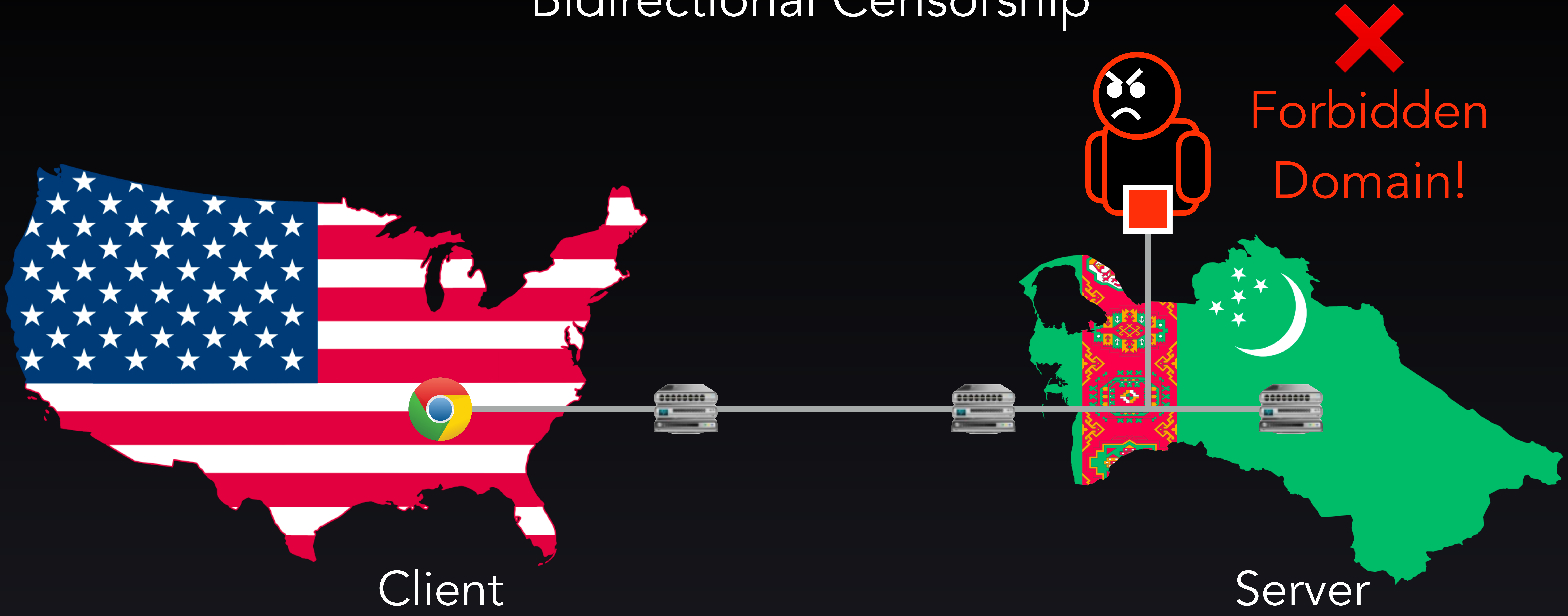
TMC Design

Bidirectional Censorship



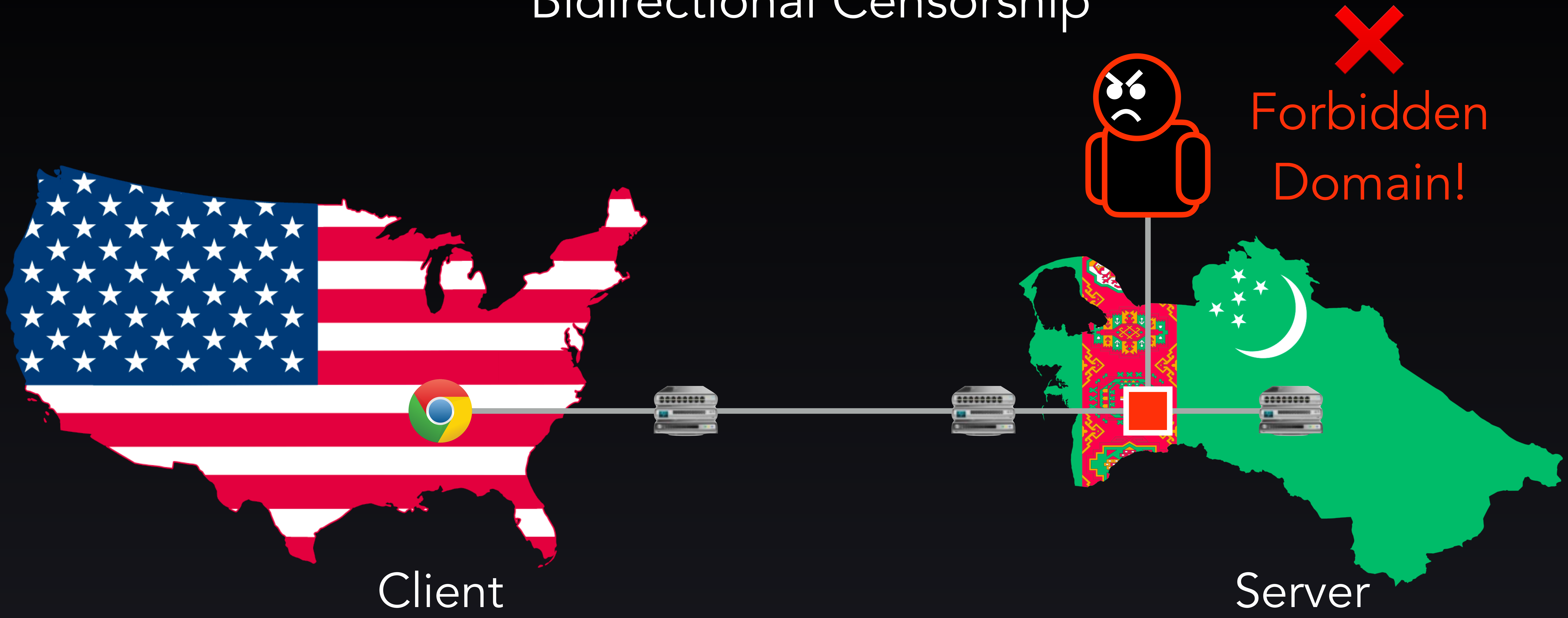
TMC Design

Bidirectional Censorship



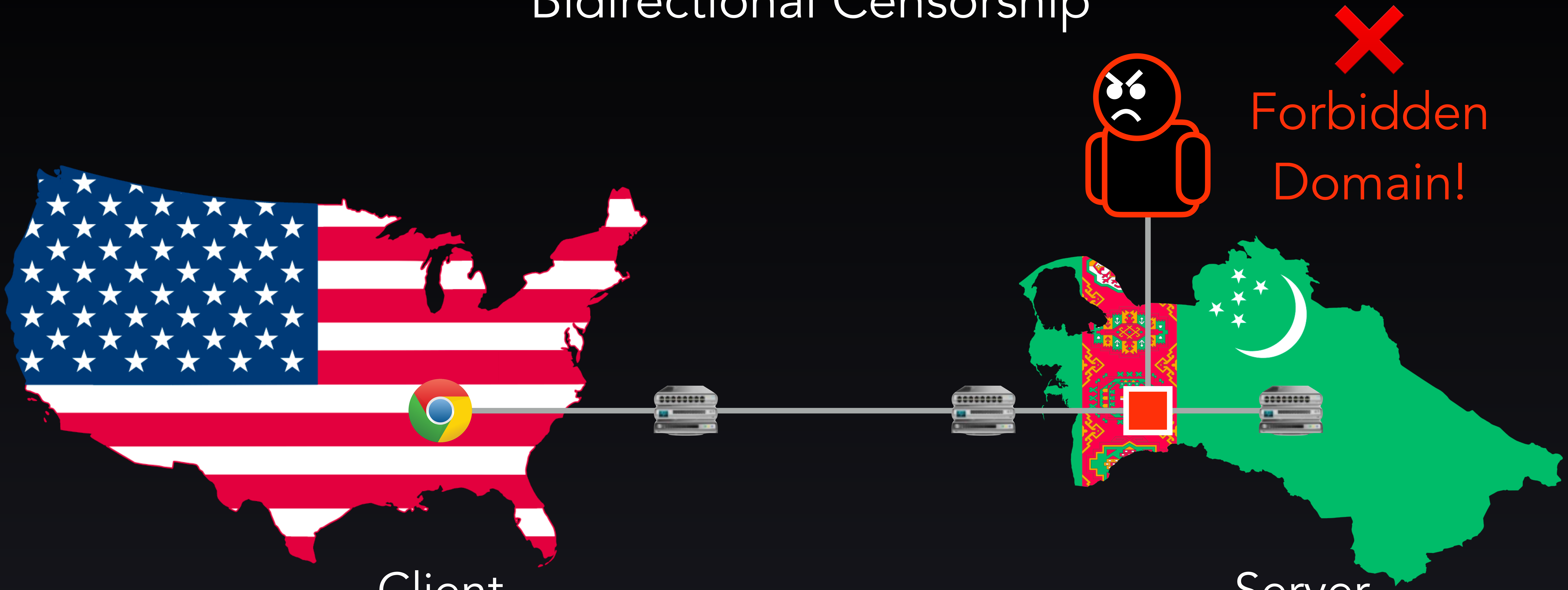
TMC Design

Bidirectional Censorship



TMC Design

Bidirectional Censorship



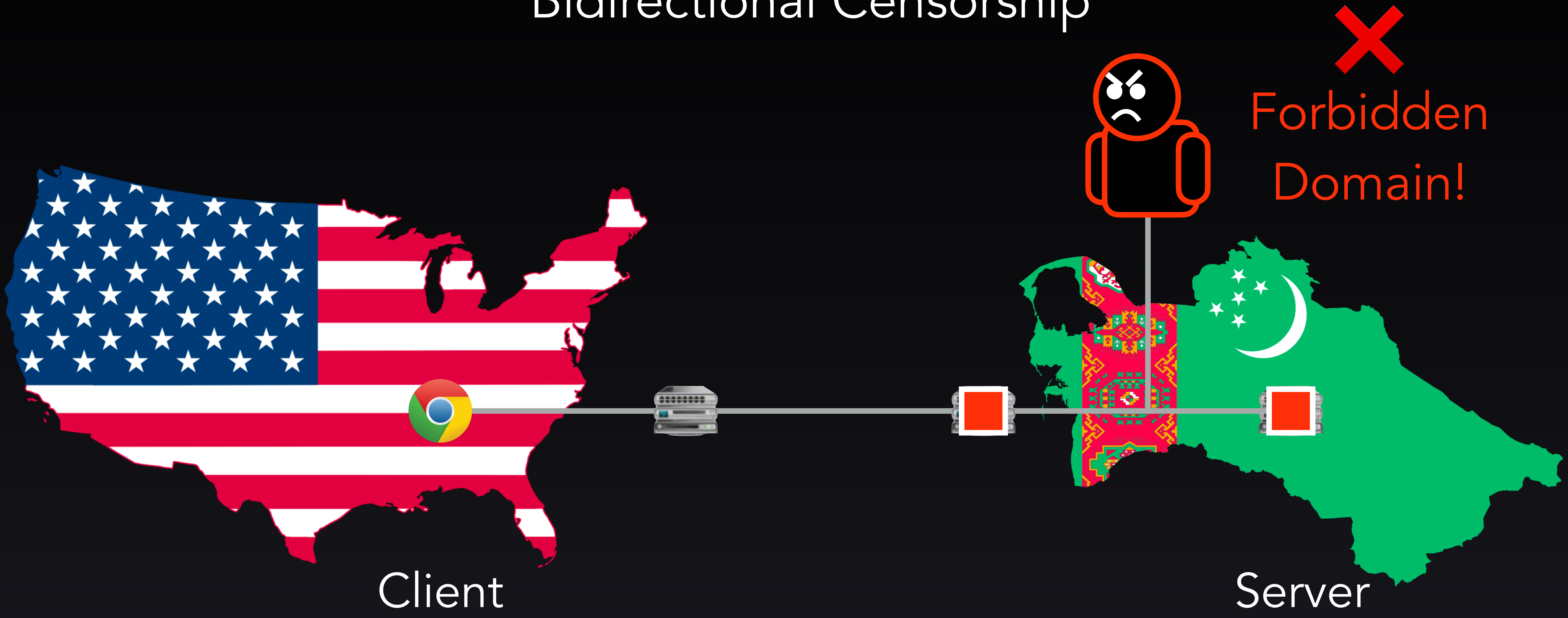
Forbidden Domain!

Client

Server

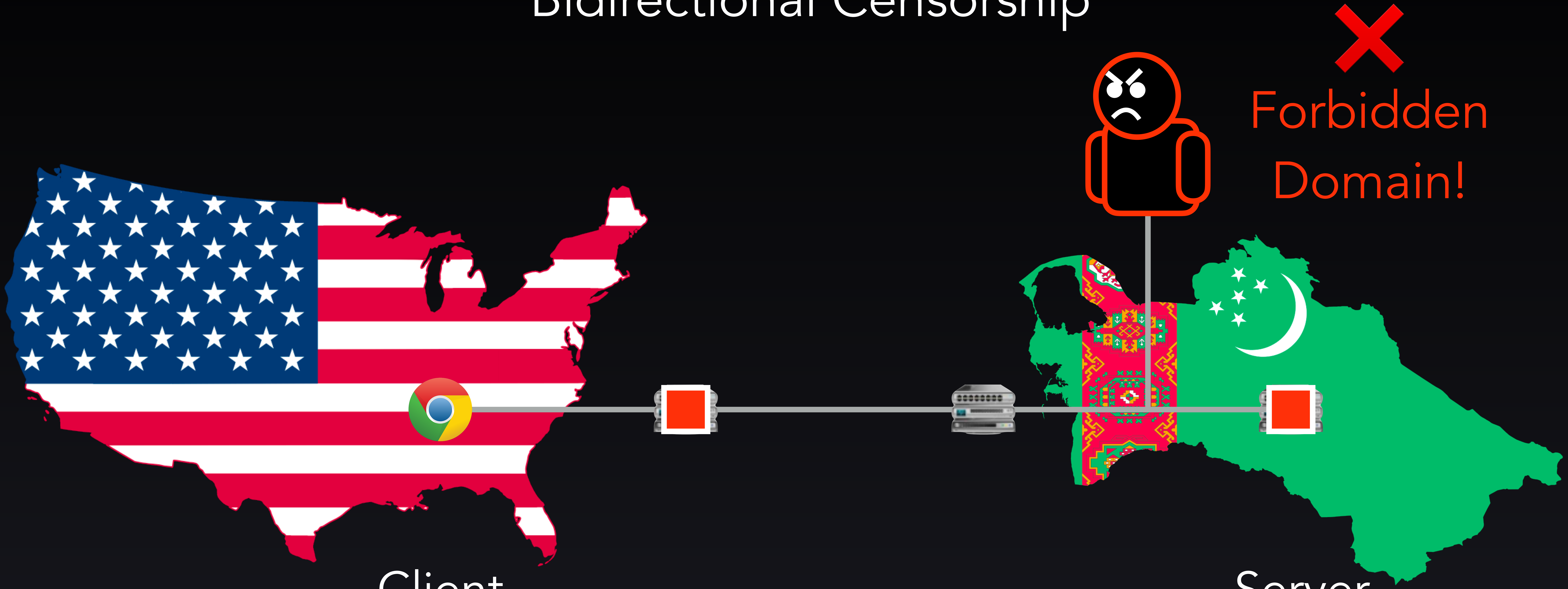
TMC Design

Bidirectional Censorship



TMC Design

Bidirectional Censorship

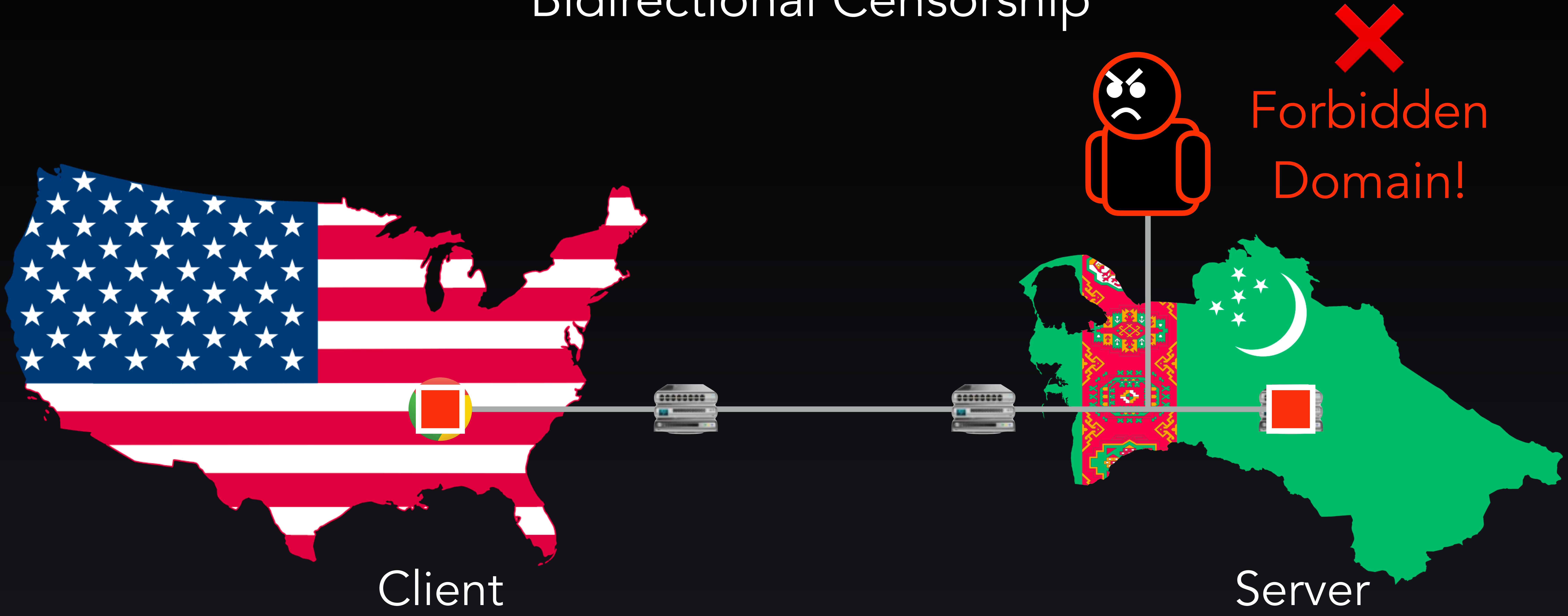


Client

Server

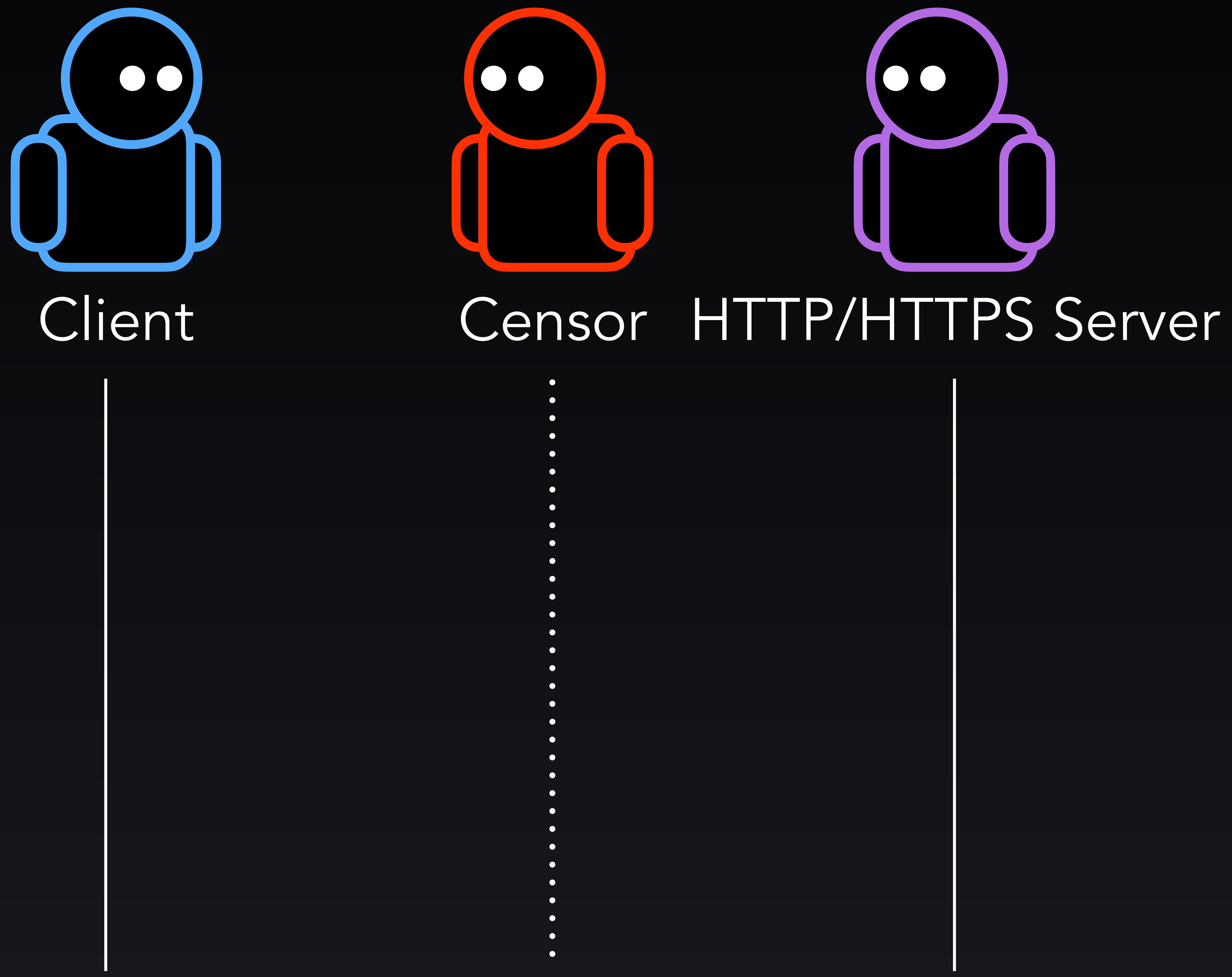
TMC Design

Bidirectional Censorship



TMC Design

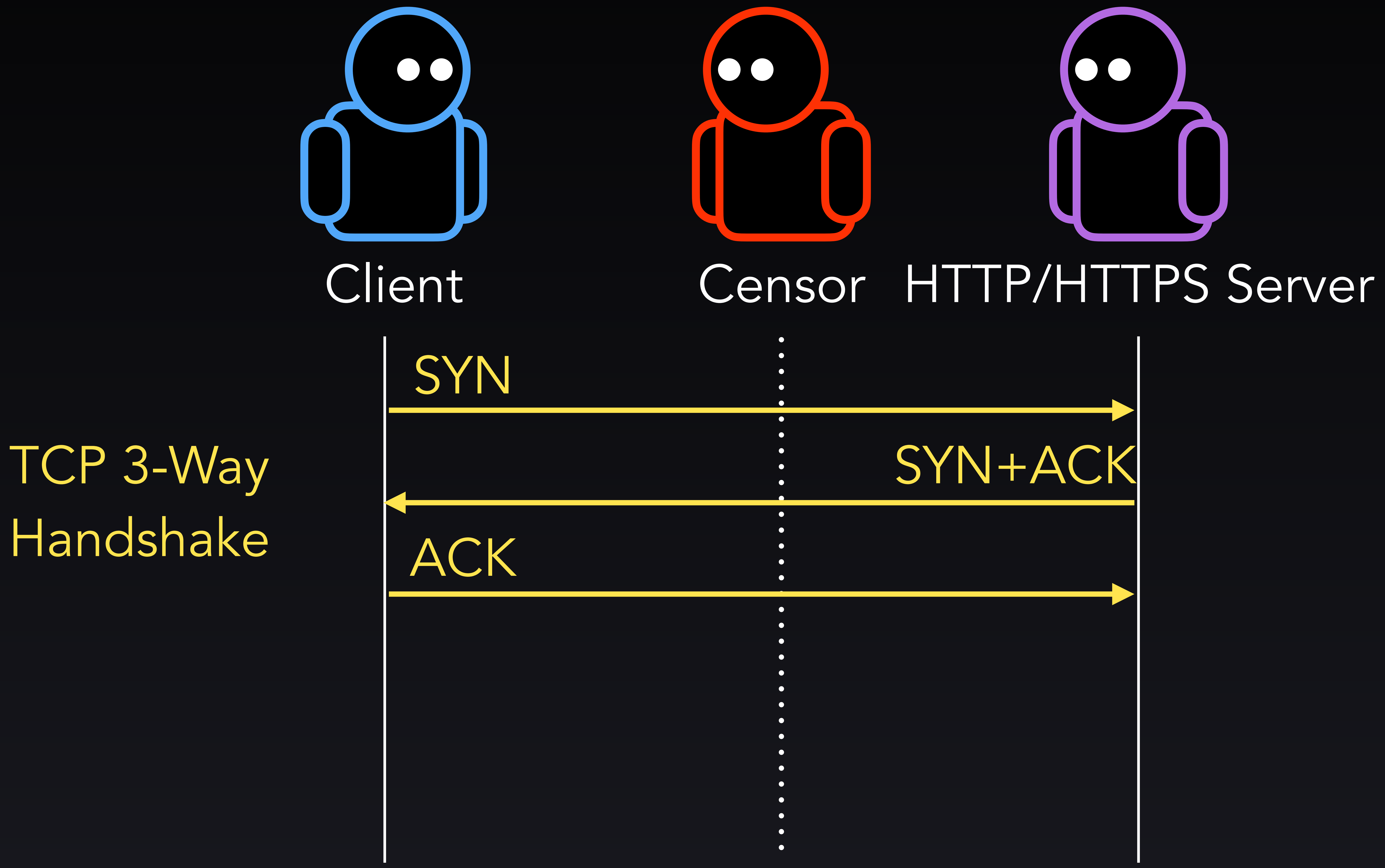
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

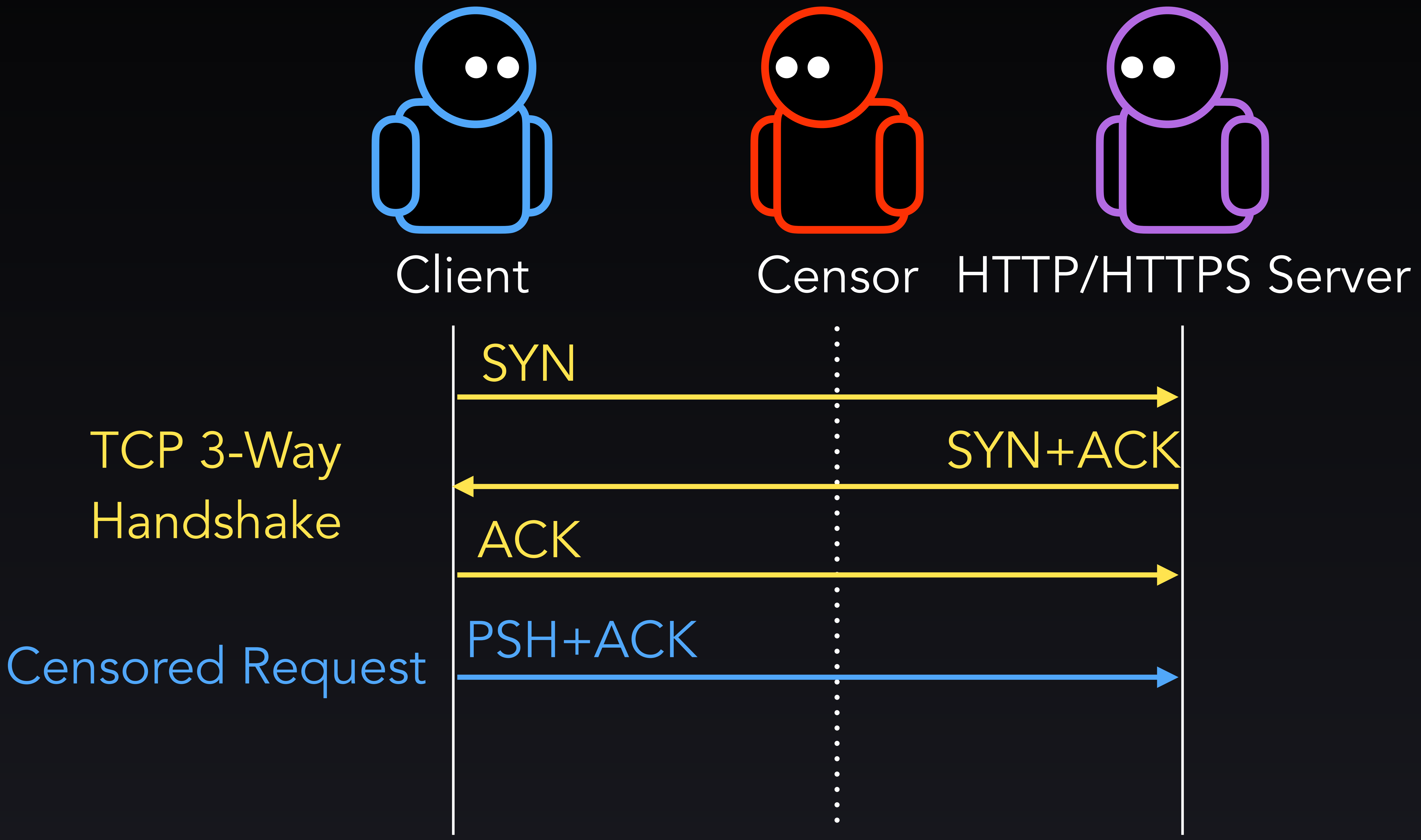
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

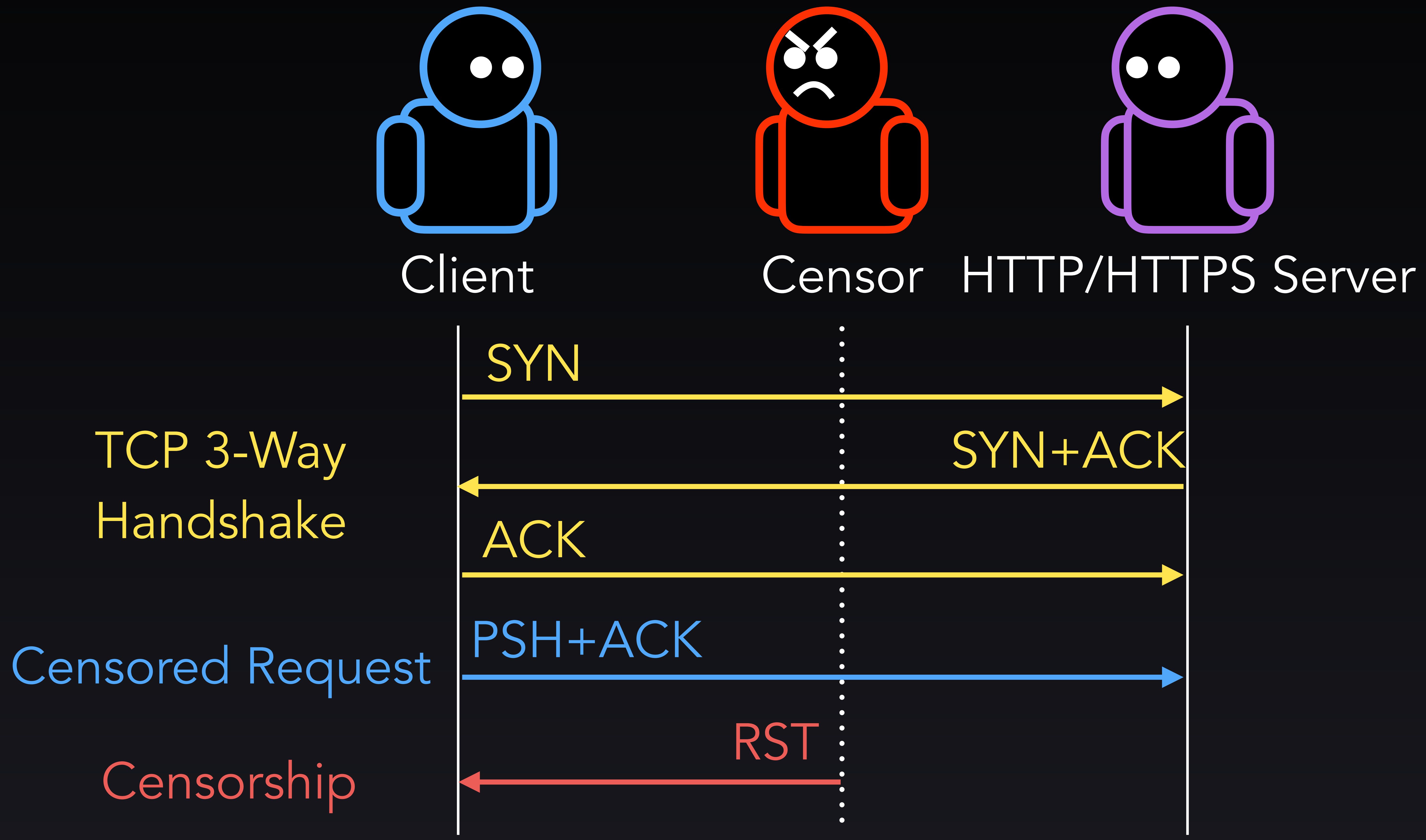
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

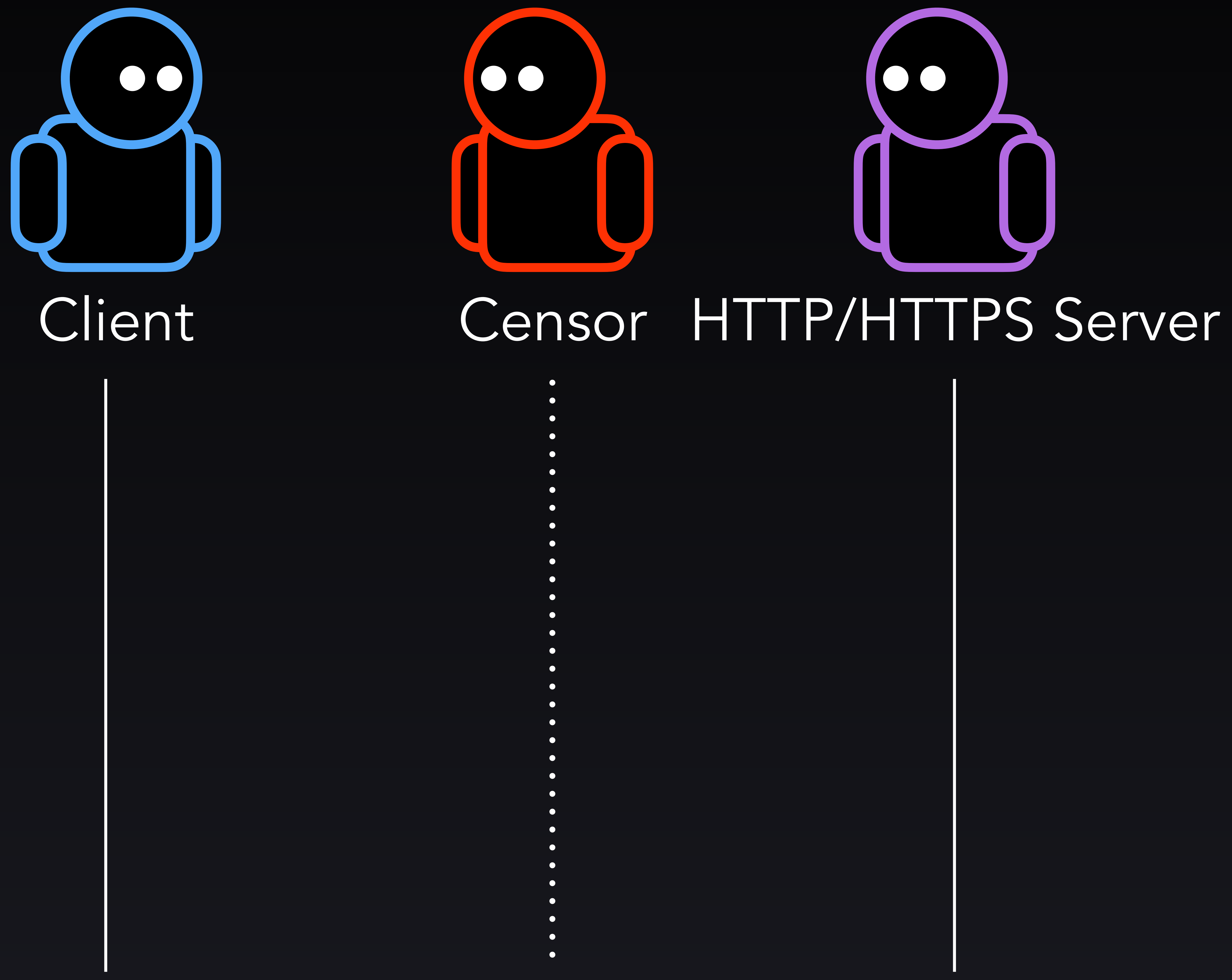
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

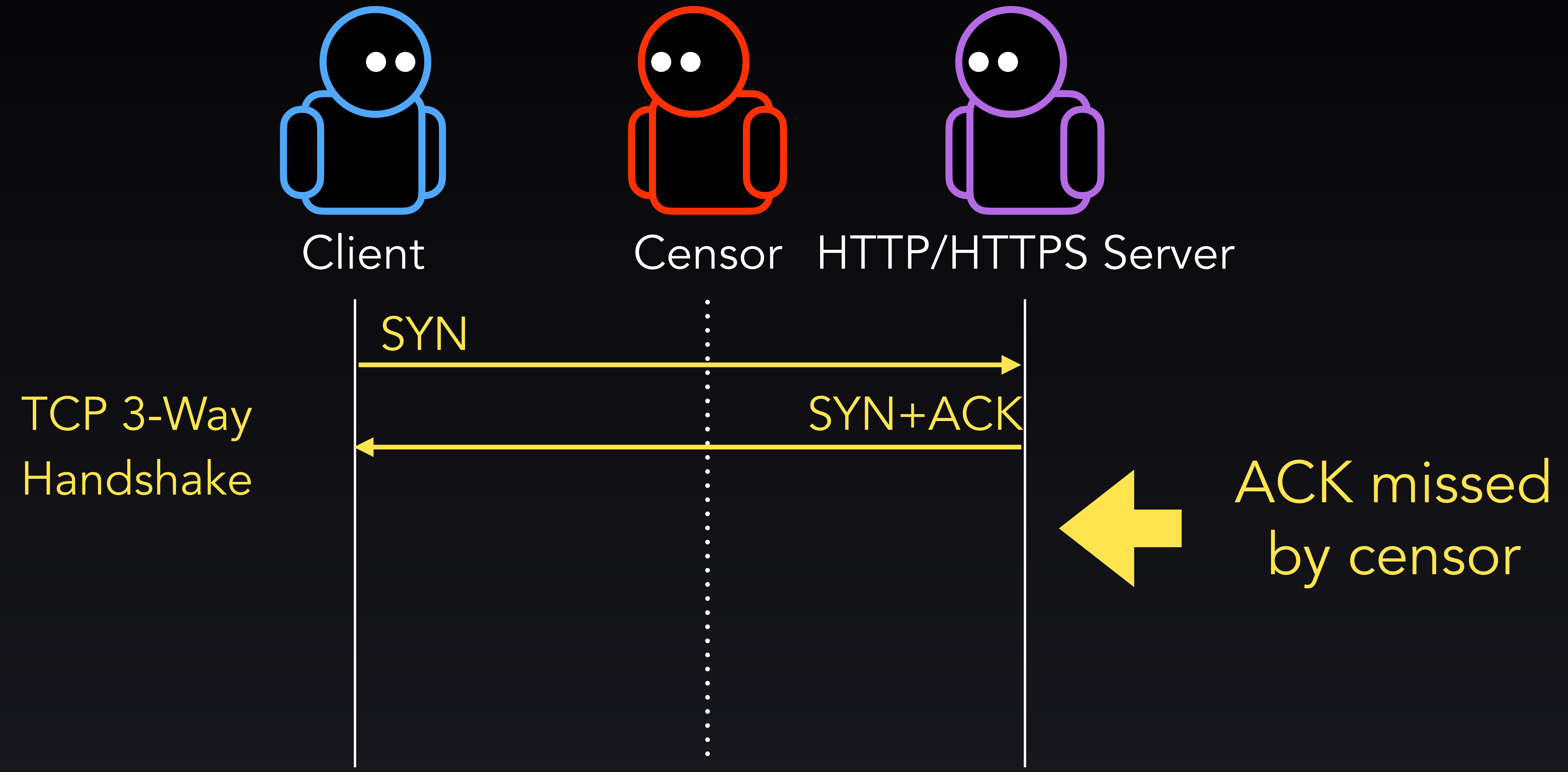
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

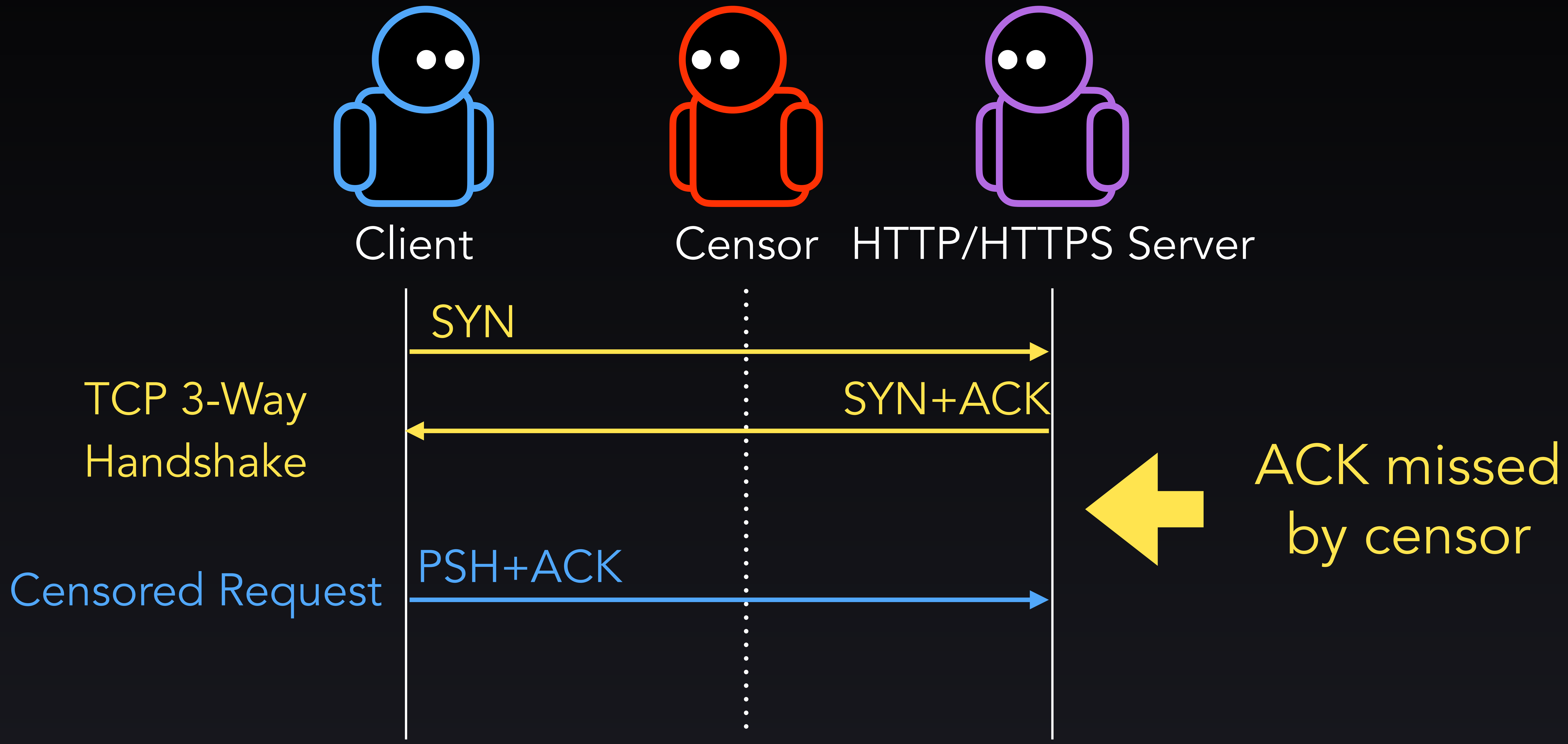
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

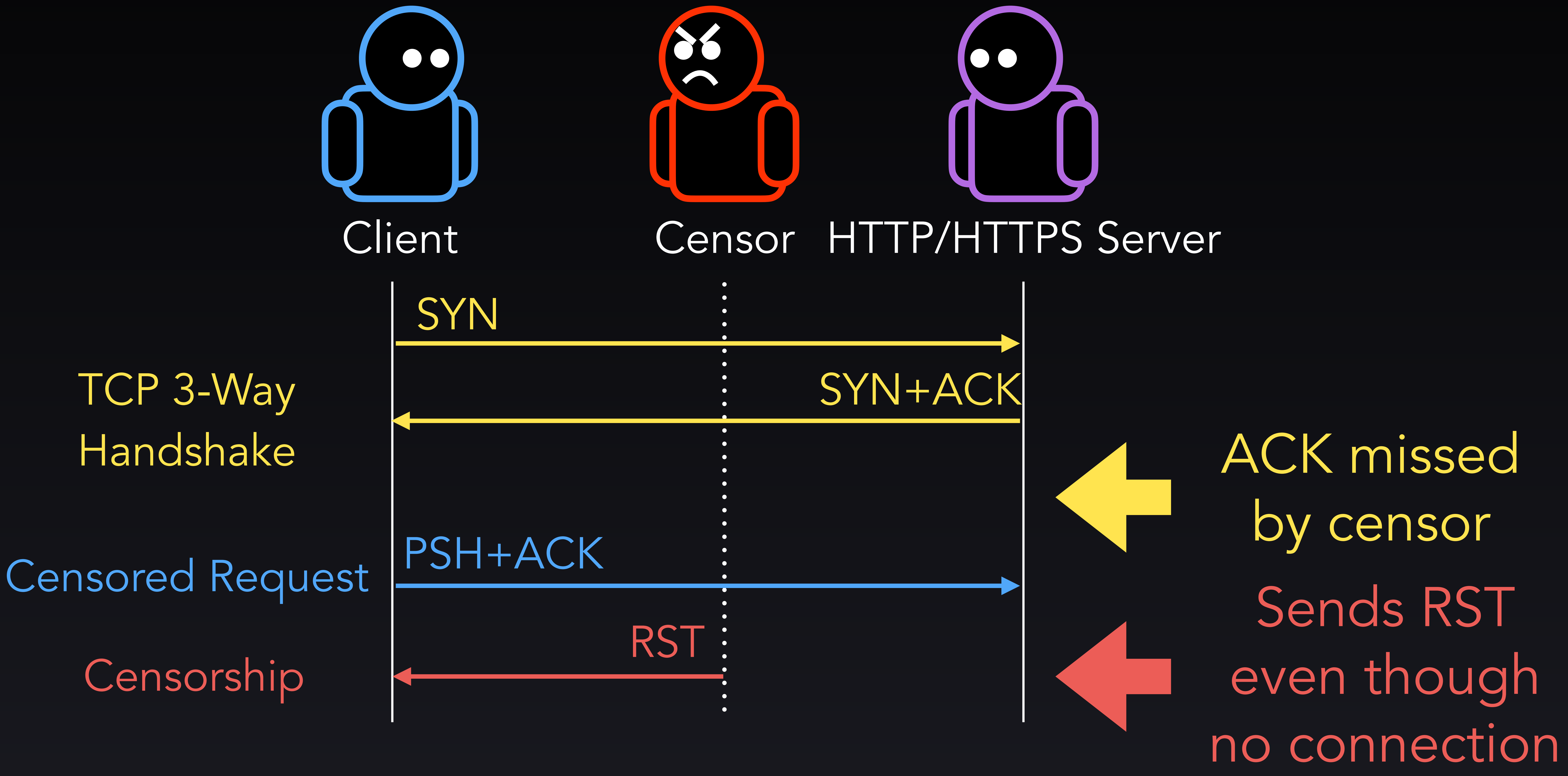
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

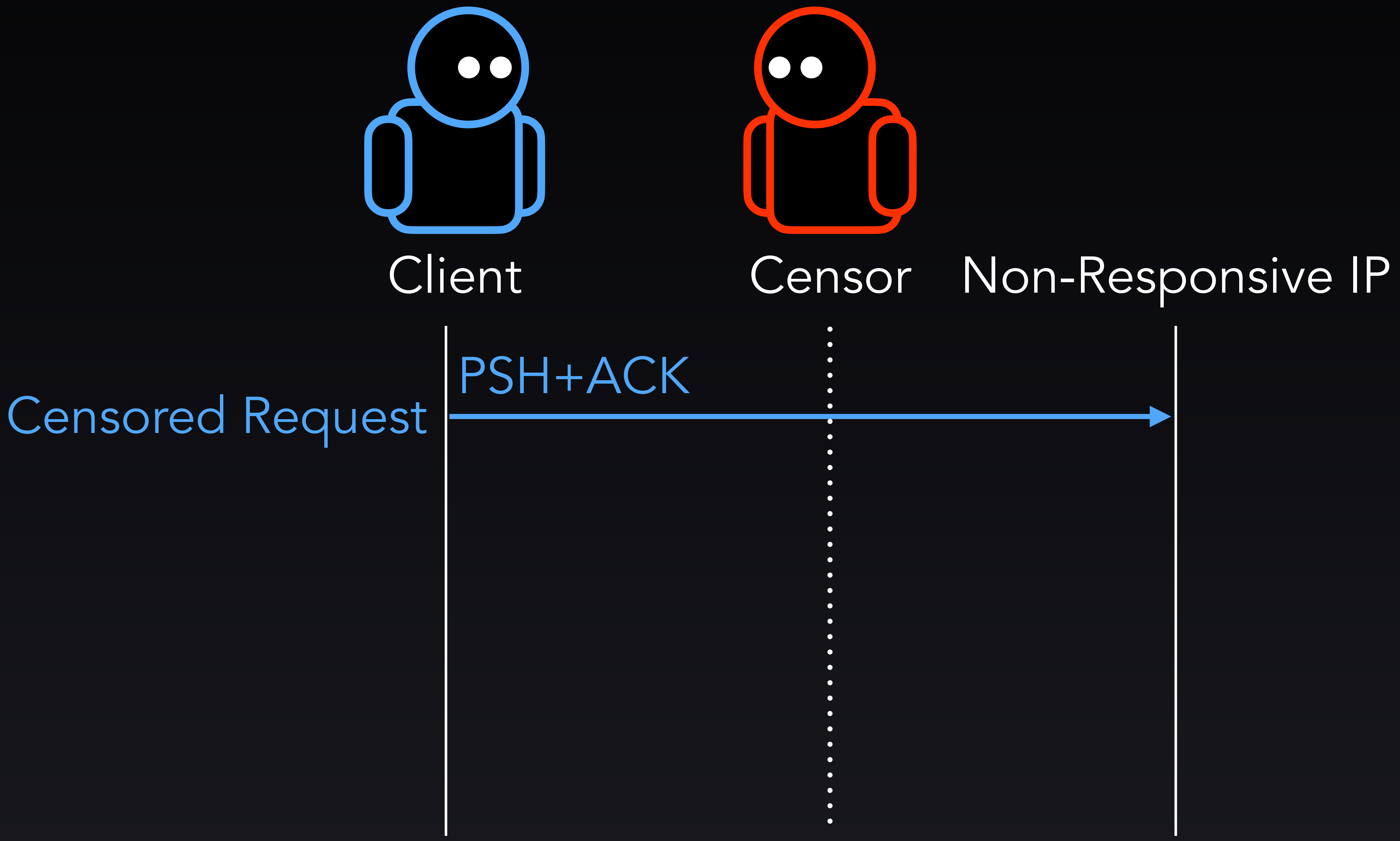
TCP Noncompliance



HTTP/HTTPS Censorship via TCP

TMC Design

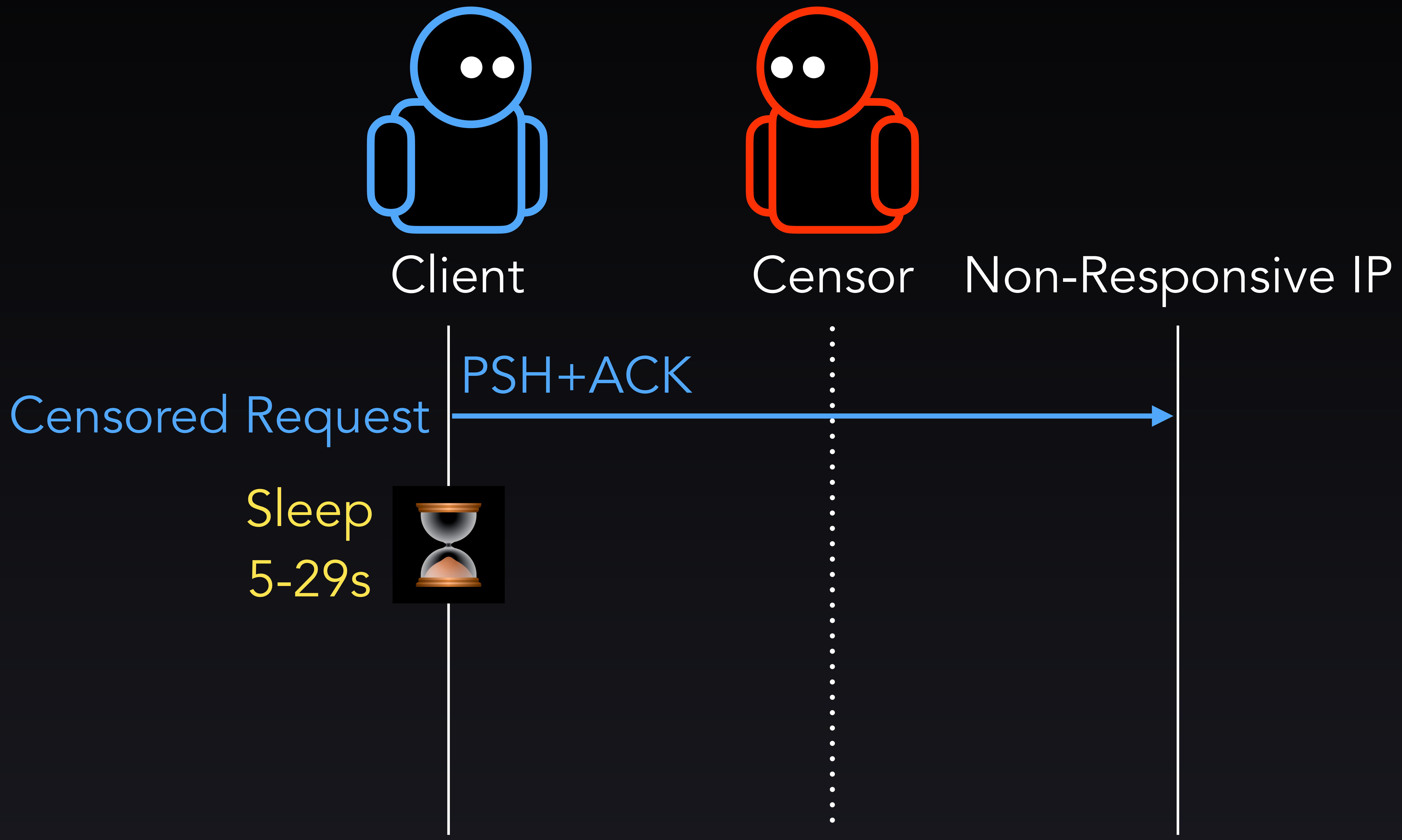
HTTP/HTTPS Censorship



Triggering HTTP/HTTPS Censorship without Endpoint

TMC Design

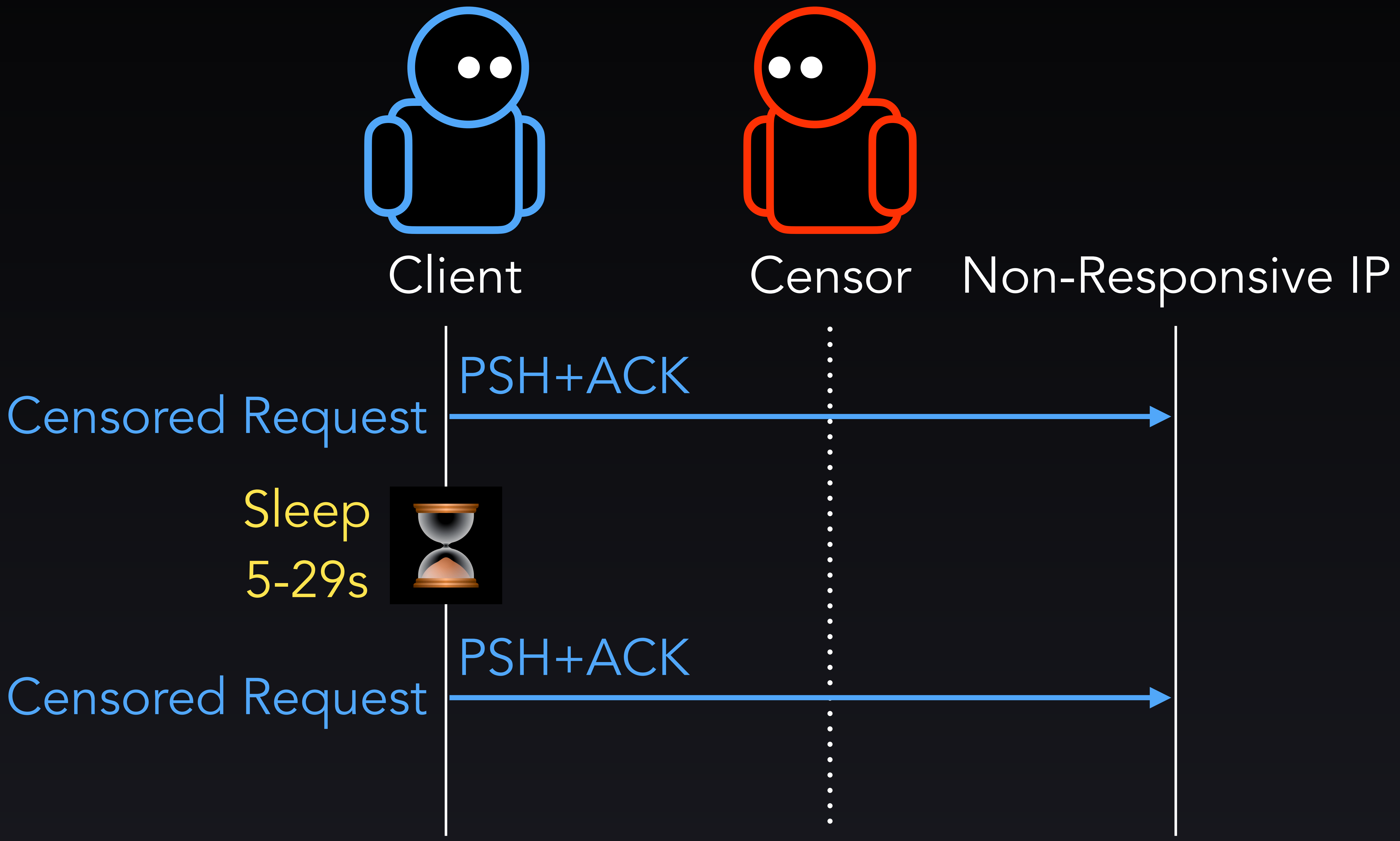
HTTP/HTTPS Censorship



Triggering HTTP/HTTPS Censorship without Endpoint

TMC Design

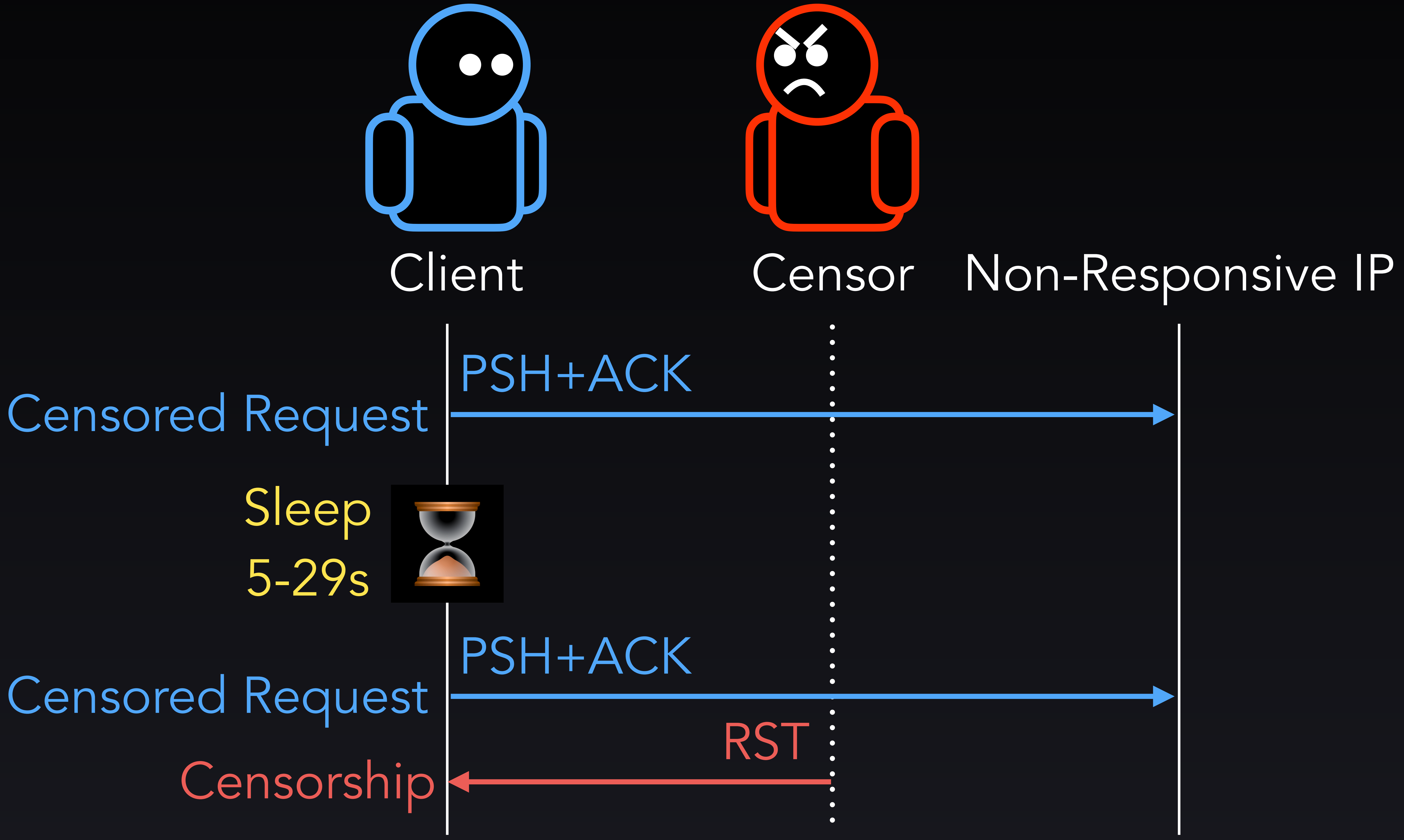
HTTP/HTTPS Censorship



Triggering HTTP/HTTPS Censorship without Endpoint

TMC Design

HTTP/HTTPS Censorship



Triggering HTTP/HTTPS Censorship without Endpoint

Measurement Results

More than 122K FQDNs censored across all three protocols

Discovered 16.5 K regex rules used for filtering

More than 6K rules cause overblocking of unrelated domains

Measurement Results

More than 122K FQDNs censored across all three protocols

Discovered 16.5 K regex rules used for filtering

More than 6K rules cause overblocking of unrelated domains

Measurement Results

More than 122K FQDNs censored across all three protocols

Discovered 16.5 K regex rules used for filtering

More than 6K rules cause overblocking of unrelated domains

Measurement Results

More than 122K FQDNs censored across all three protocols

Discovered 16.5 K regex rules used for filtering

More than 6K rules cause overblocking of unrelated domains

Measurement Results

Extreme Blocking Rules

.*vpn.*

.*porn.*

.*w\.org.*

.*twitter\.com*

^doh\..*

Measurement Results

Extreme Blocking Rules

Sample Overblocked Domains:

.*vpn.*	vpnoverview.com, vpnmentor.com
.*porn.*	antipornography.com, pornphiphit.co.th
.*w\.org.*	w.org, hrw.org, tensorflow.org
.*twitter\.com*	notrealtwitter.com, financetwitter.com
^doh\..*	doh.gov.ae, doh.wa.gov

Censorship Evasion Strategies

Geneva

Genetic Evasion

[Bock et al. CCS 2019]

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

Censorship Evasion Strategies

Geneva

Genetic Evasion

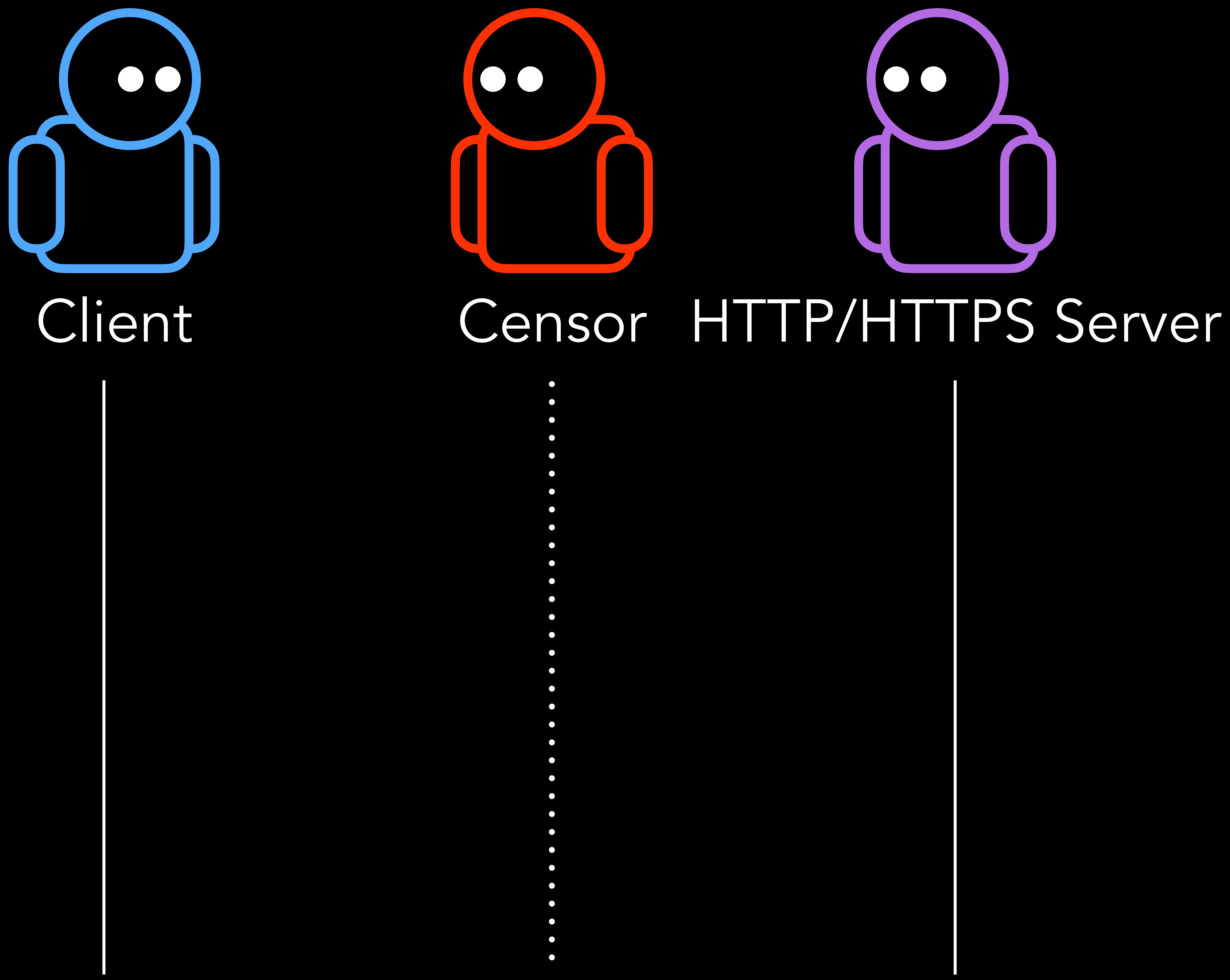
[Bock et al. CCS 2019]

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

Censorship Evasion Strategies

Transport Layer

Free Pass



Client

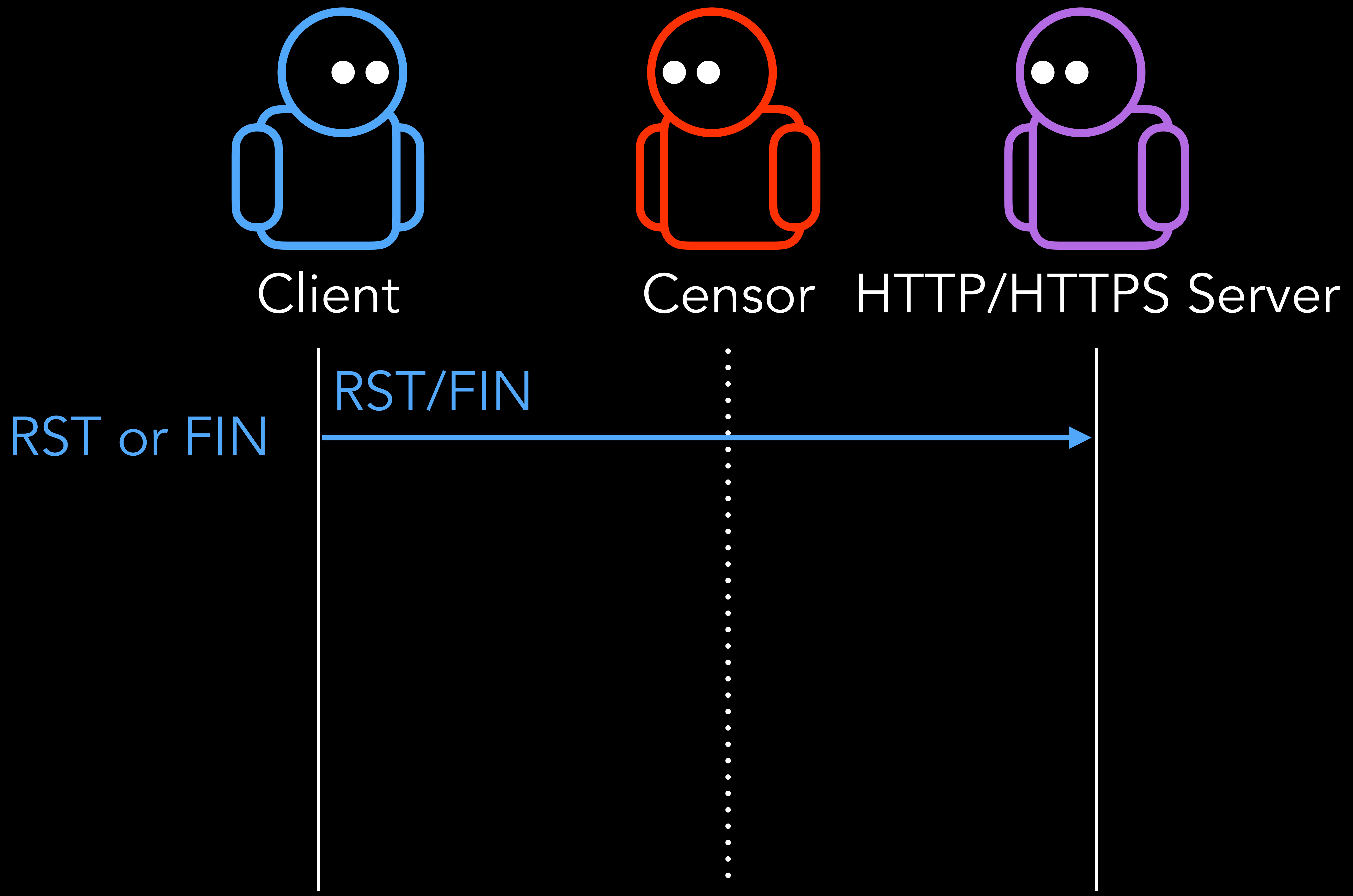
Censor

HTTP/HTTPS Server

Censorship Evasion Strategies

Transport Layer

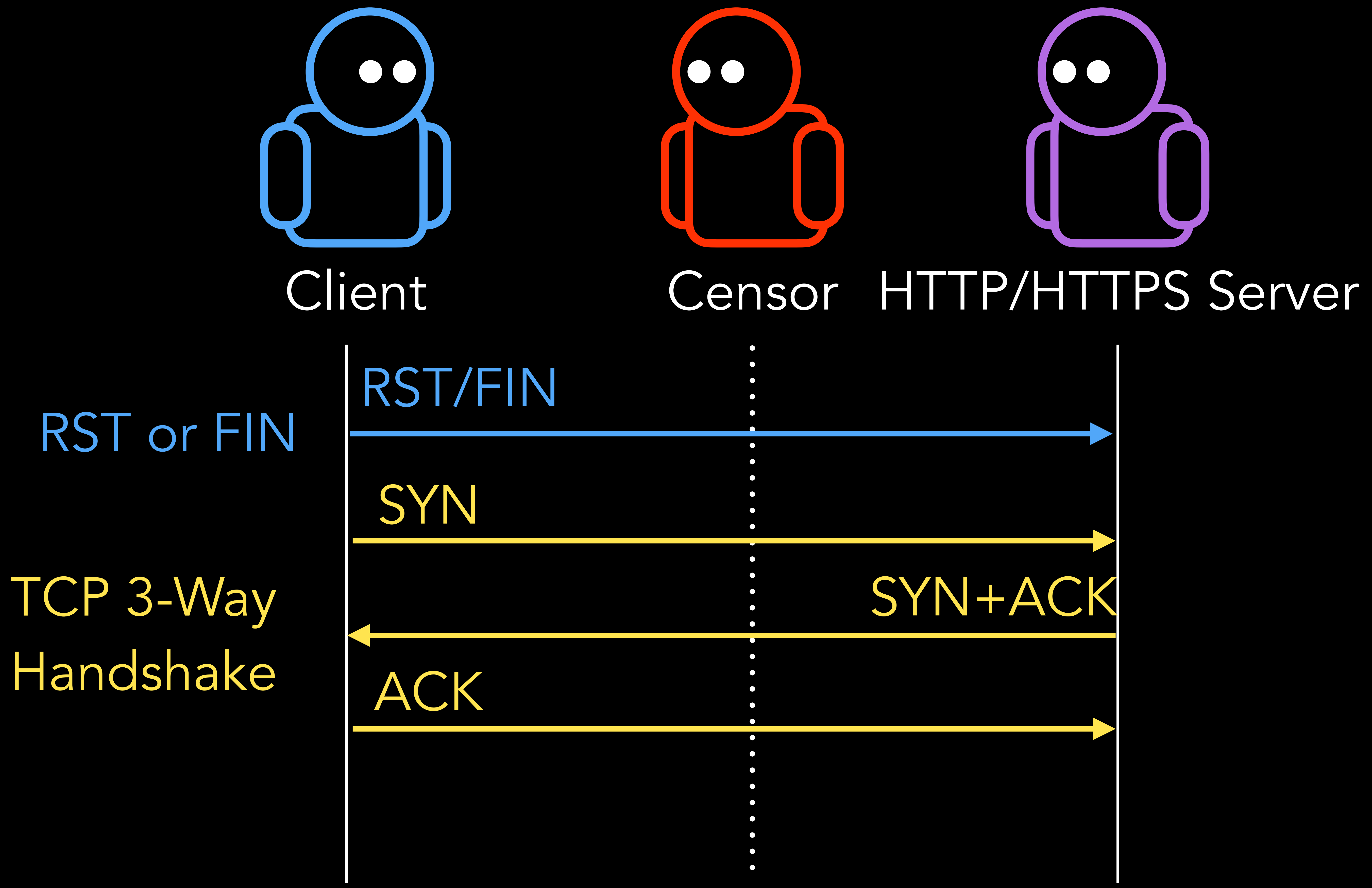
Free Pass



Censorship Evasion Strategies

Transport Layer

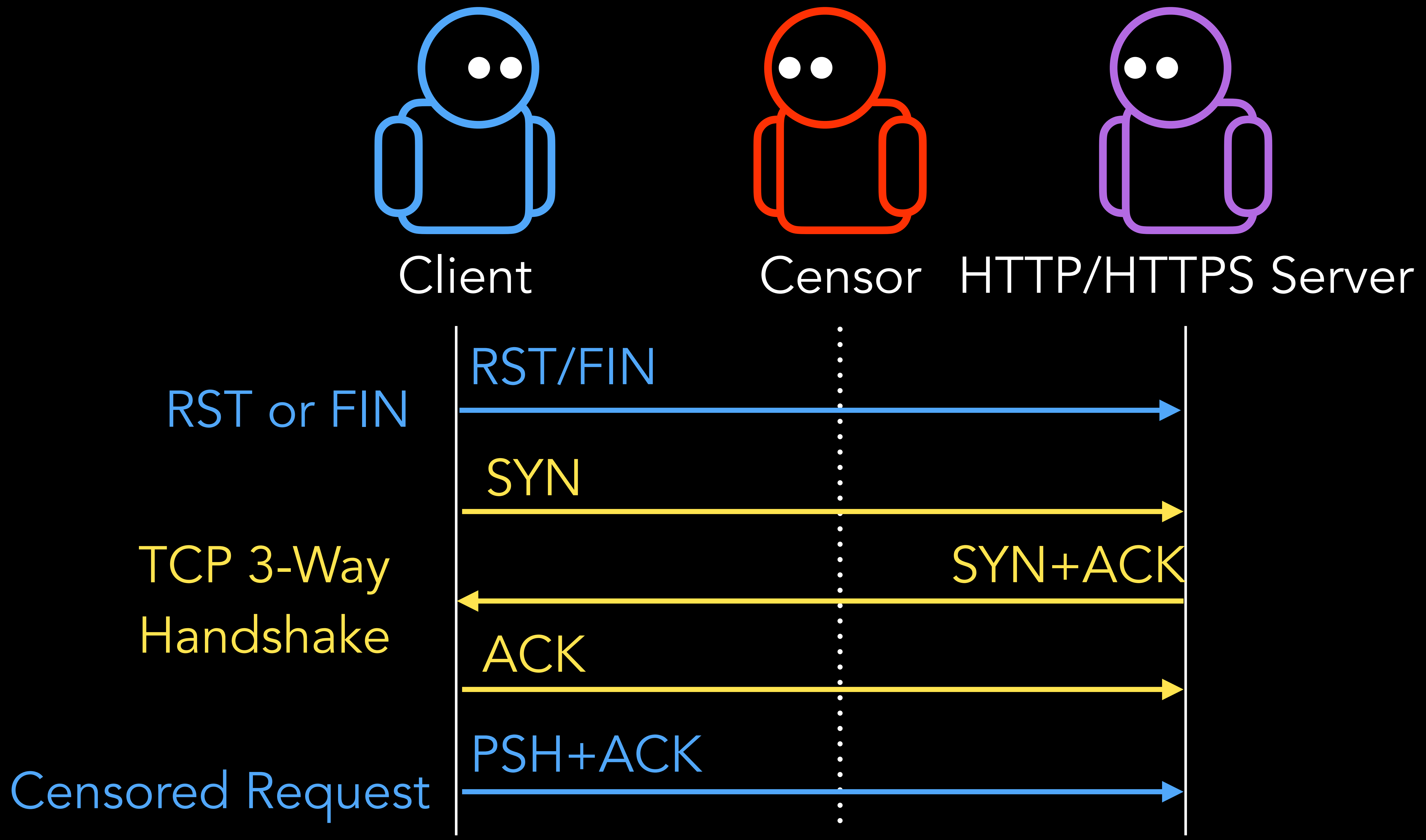
Free Pass



Censorship Evasion Strategies

Transport Layer

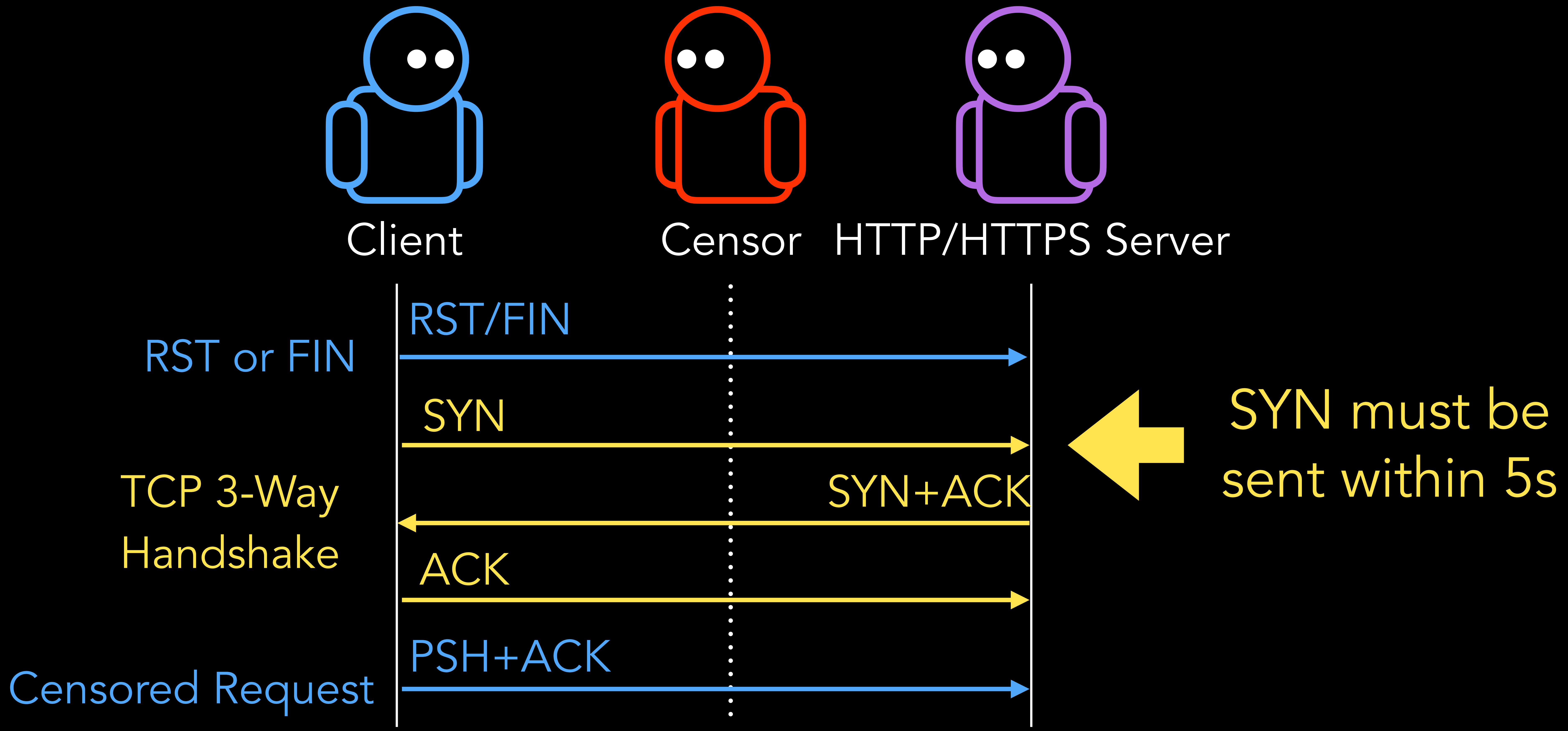
Free Pass



Censorship Evasion Strategies

Transport Layer

Free Pass

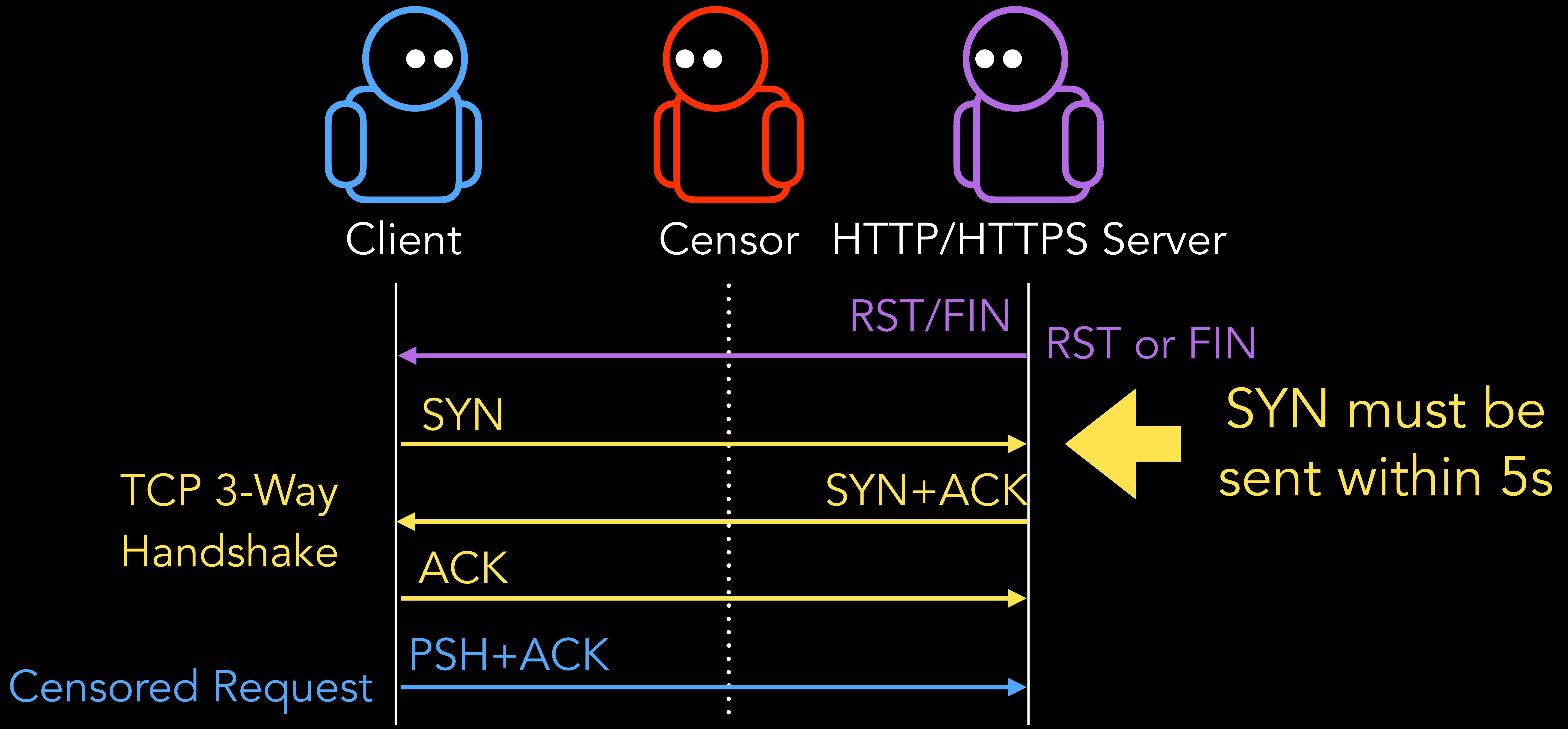


SYN must be sent within 5s

Censorship Evasion Strategies

Transport Layer

Free Pass



SYN must be sent within 5s

Other Details In The Paper

More Evasion Strategies

Evasion strategies for both transport and application layer

DNS Censorship

DNS measurement methodology and results

AS Topology

Routing topology and censorship granularity

Adversarial Censor

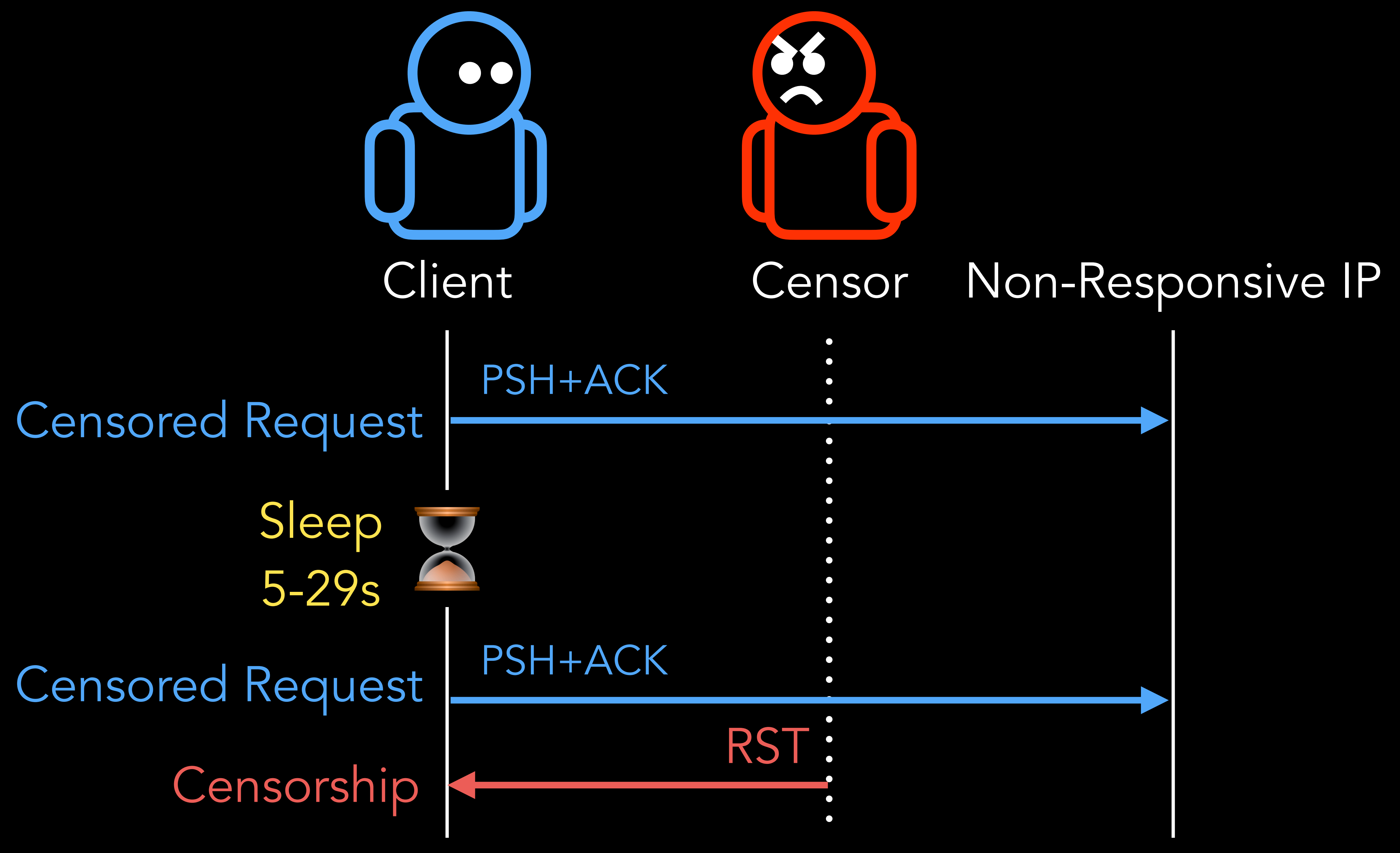
Adversarial nature of Turkmenistan's censoring middleboxes

Measuring and Evading Turkmenistan’s Internet Censorship

TMC can trigger censorship *without vantage points or endpoints*

Turkmenistan’s regex filtering causes significant overblocking

Discovered new transport layer evasion strategy: Free Pass



Triggering HTTP/HTTPS Censorship without Endpoint

Measurement Results tmc.np-tokumei.net