How Low Can You Go: Balancing Performance with Anonymity in Tor'

DC-Area Anonymity,Privacy, and Security Seminar

May 10th, 2013

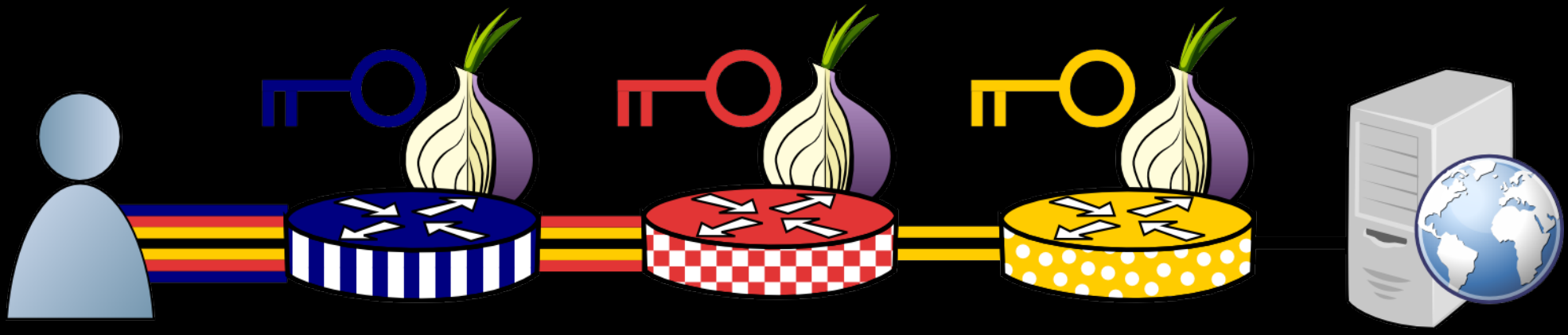
Rob Jansen
U.S. Naval Research Laboratory
rob.g.jansen@nrl.navy.mil

'PETS 2013, joint w/ John Geddes and Nick Hopper, U of Minnesota

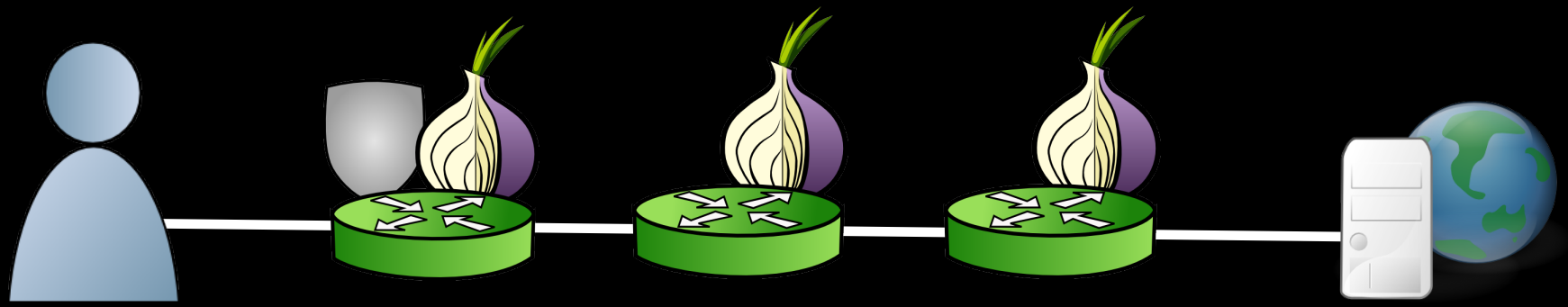
This Talk in a Nutshell

- New class of induced throttling attacks
  - Drastically improves traffic correlation via "stealthy throughput" style attacks
  - Analyze attacks against
    - Traffic admission control algorithms
    - Congestion control algorithms

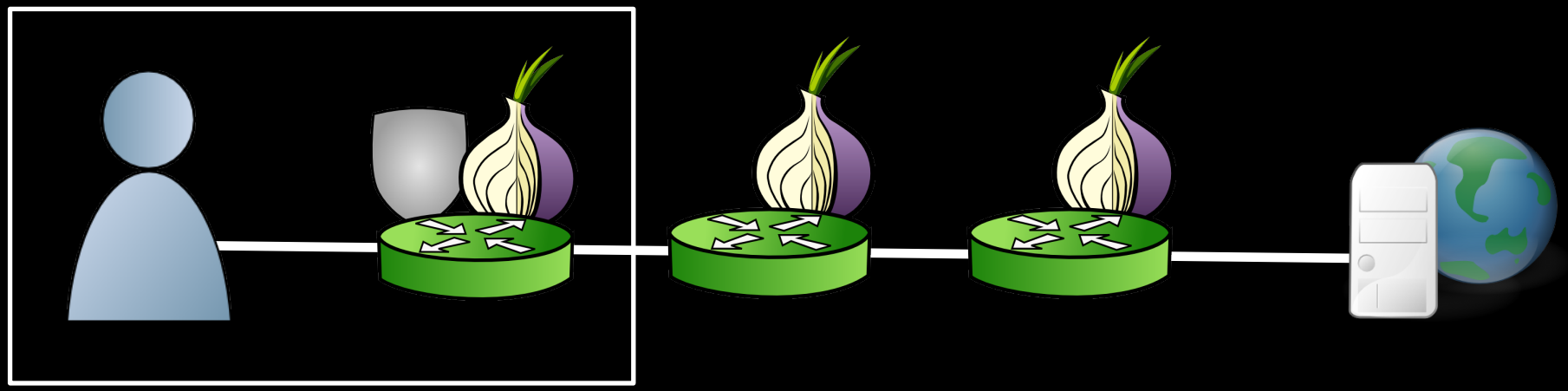
Anonymity with Onion Routing



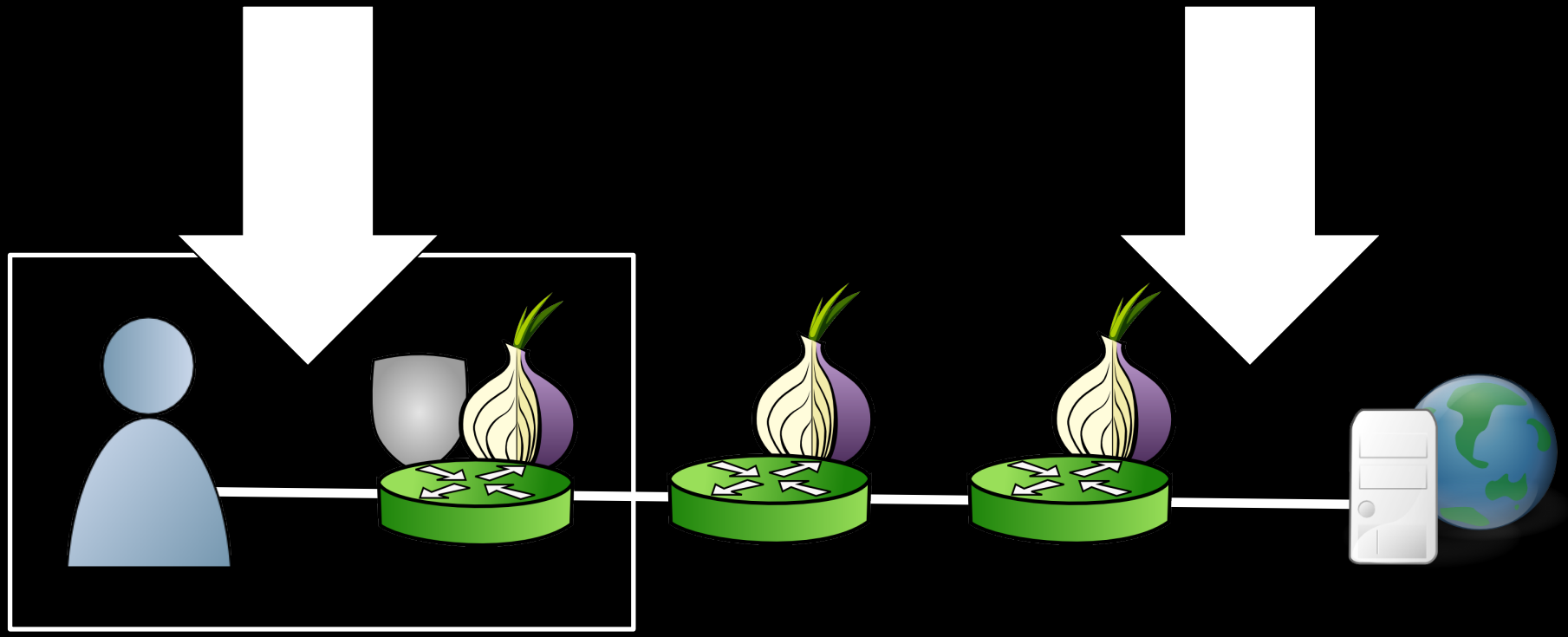
Traffic Correlation



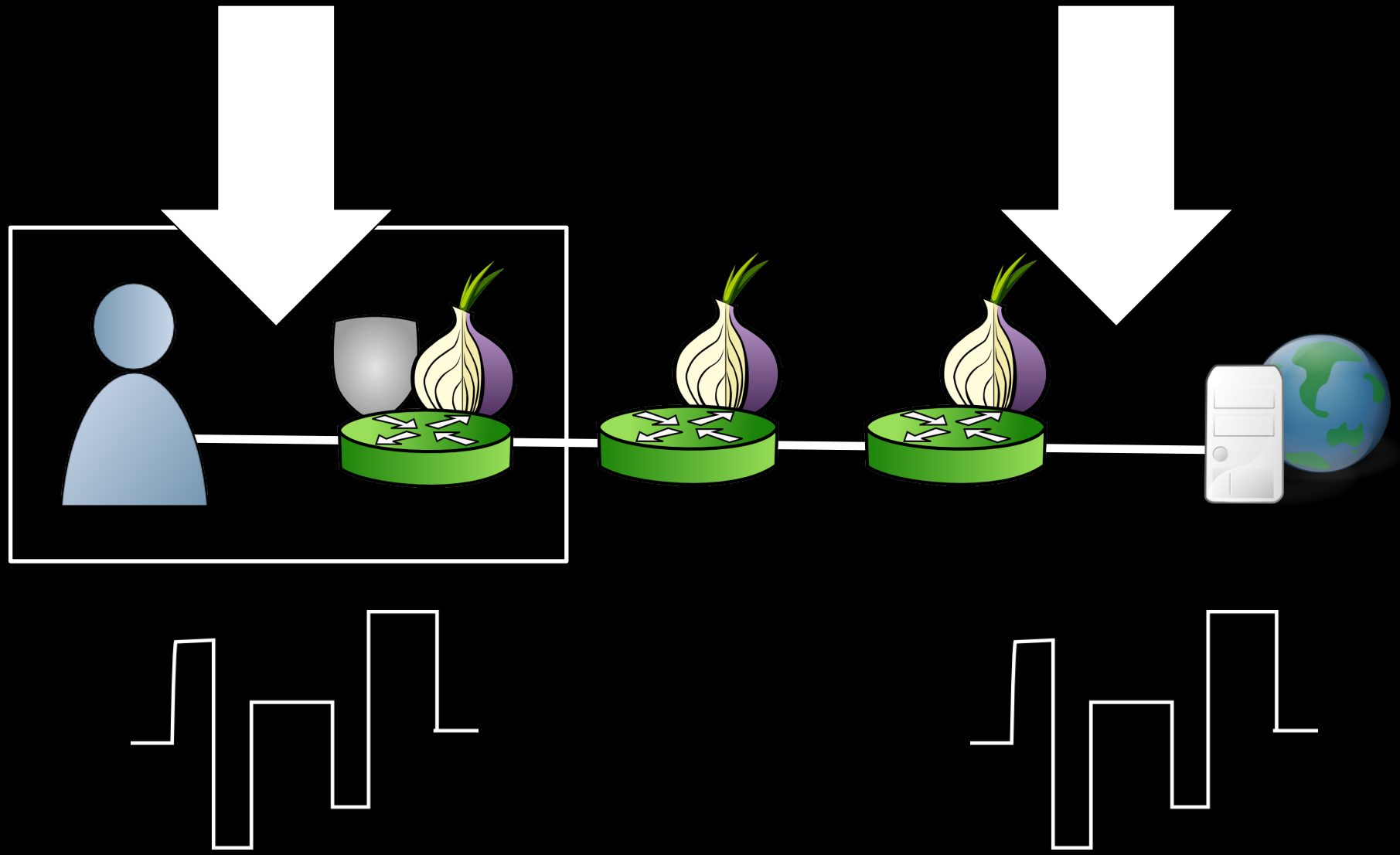
Traffic Correlation



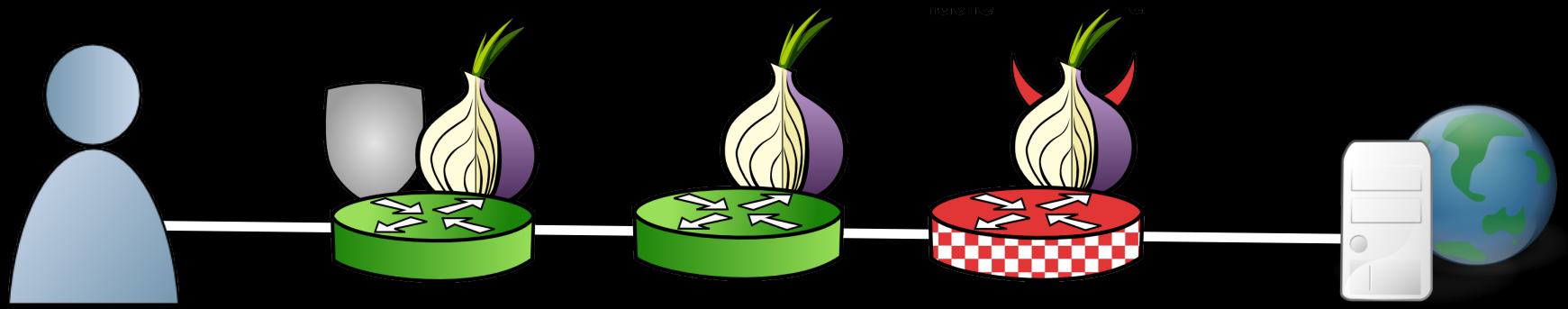
Traffic Correlation



Traffic Correlation

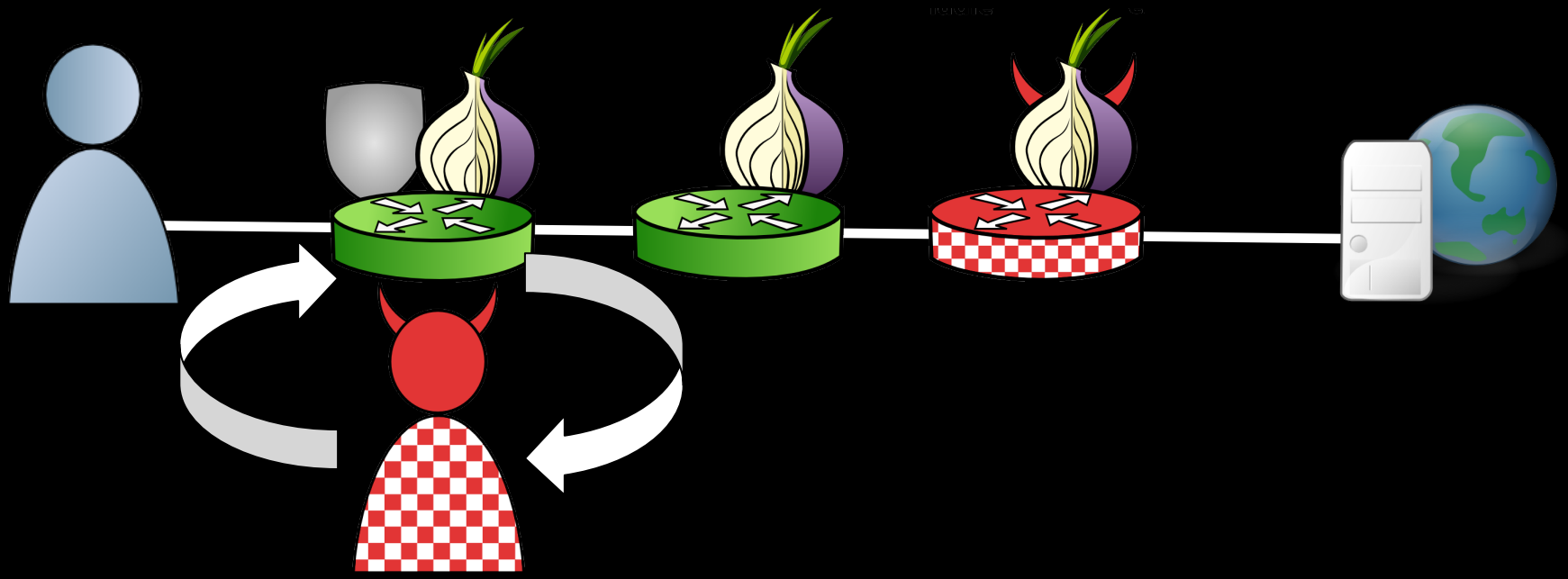


Traffic Correlation: Throughput



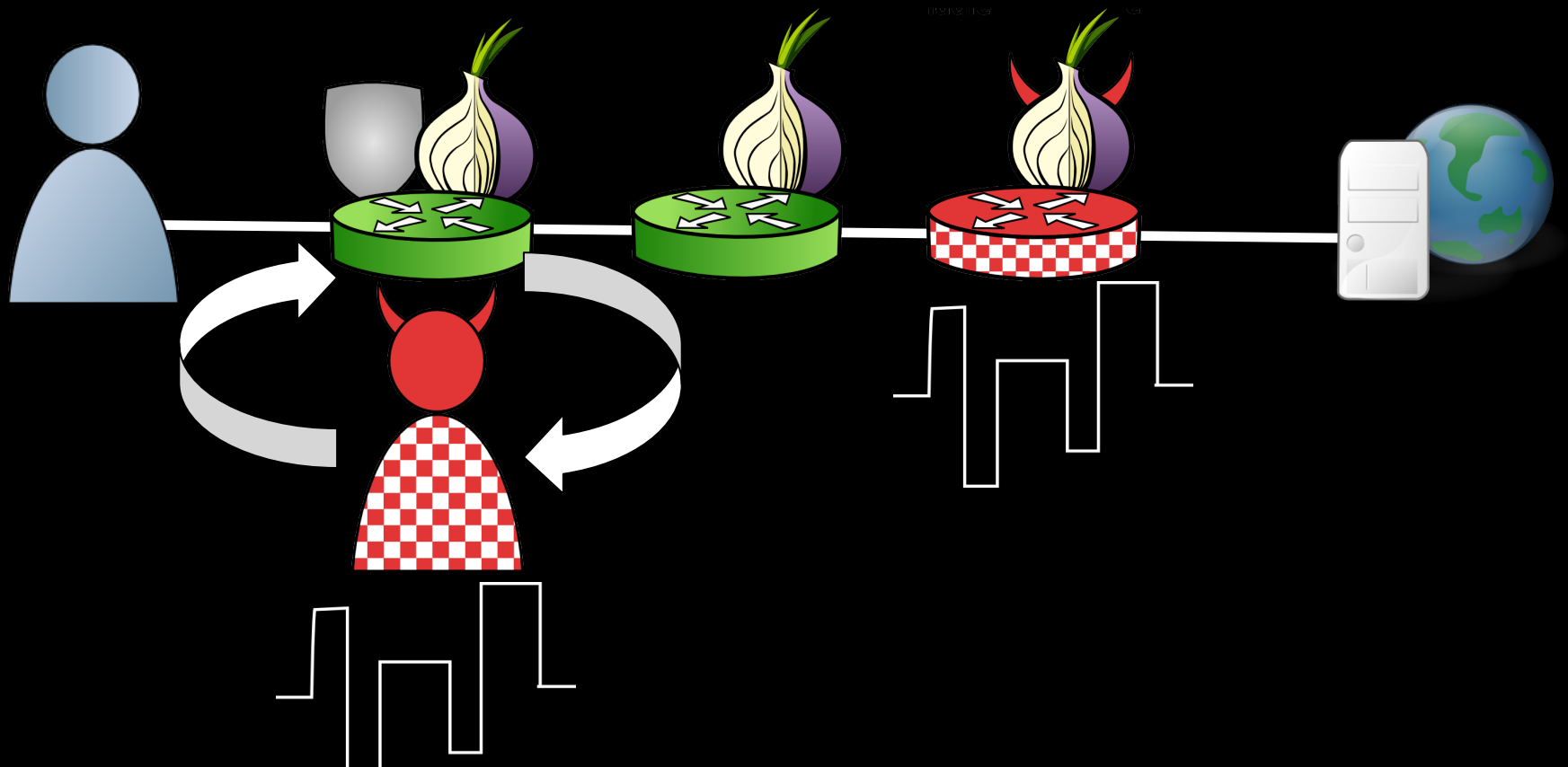
Mittal et.al. CCS'11

Traffic Correlation: Throughput



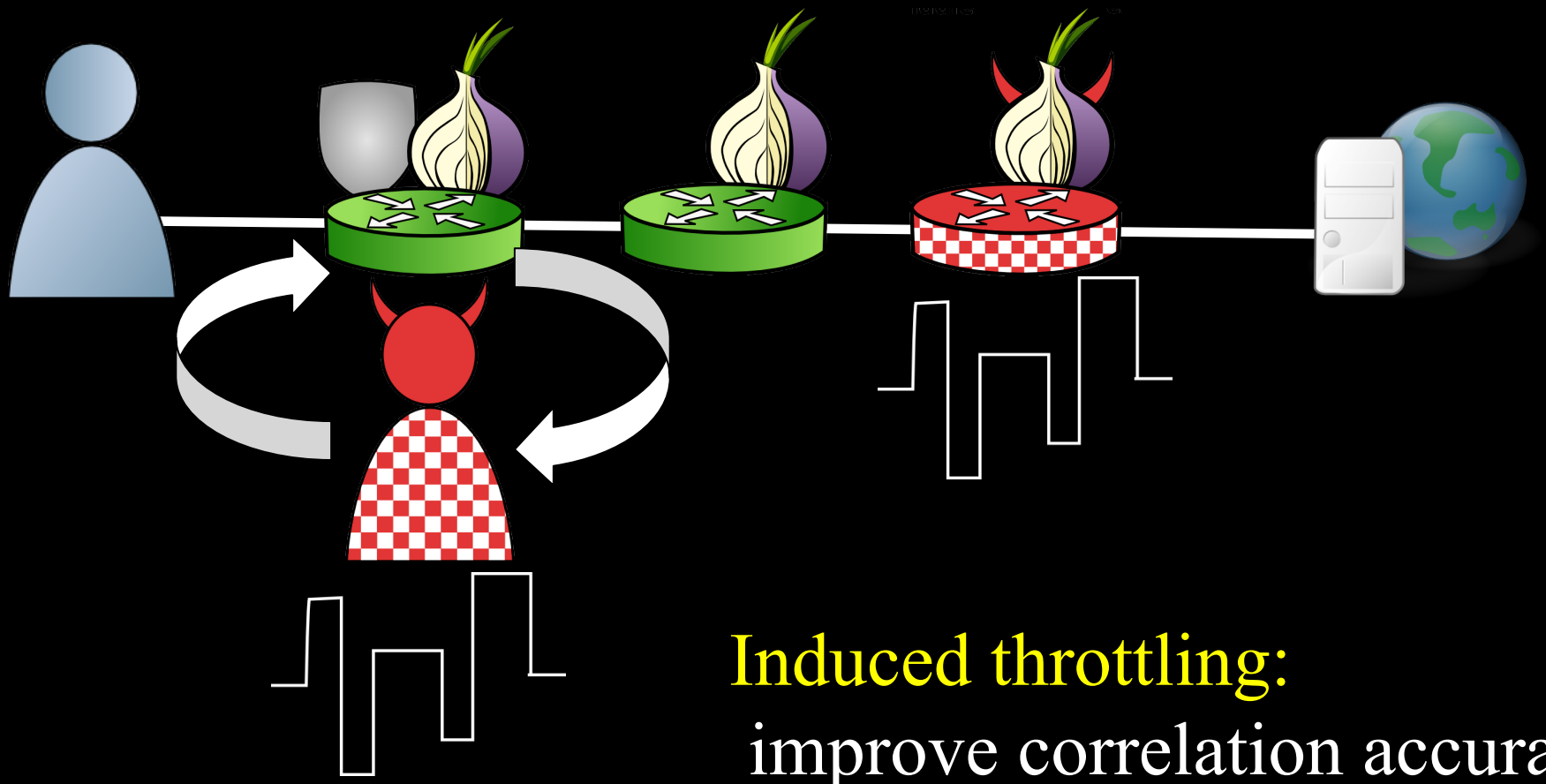
Mittal et.al. CCS'11

Traffic Correlation: Throughput



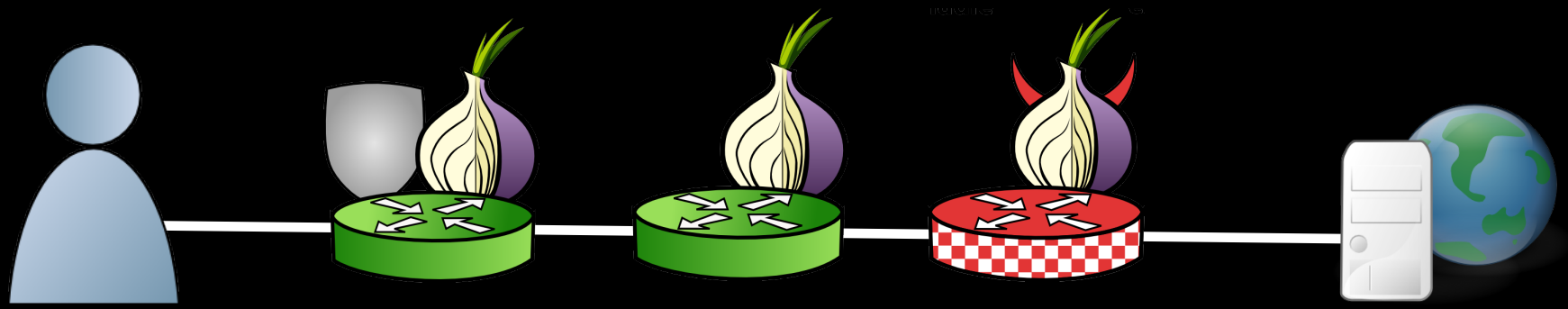
Mittal et.al. CCS'11

Traffic Correlation: Throughput



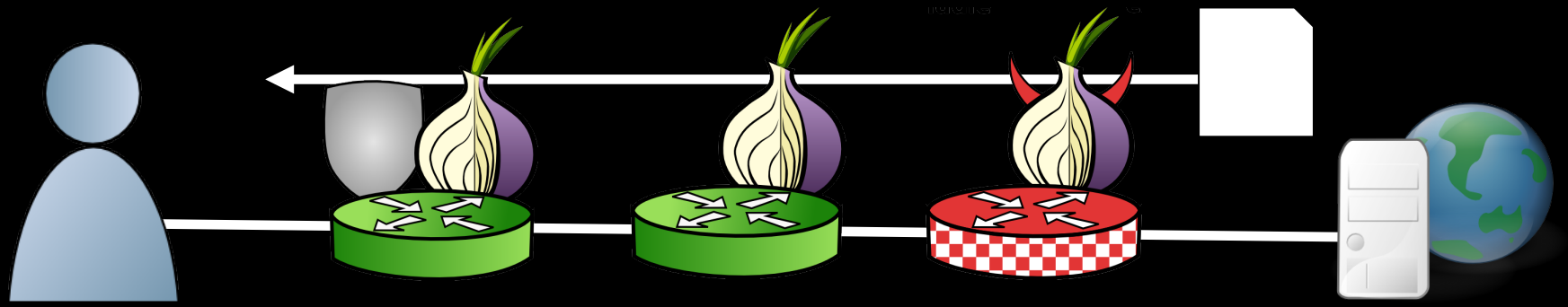
Induced throttling:
improve correlation accuracy

Traffic Correlation: Latency



Hopper et.al. CCS'07

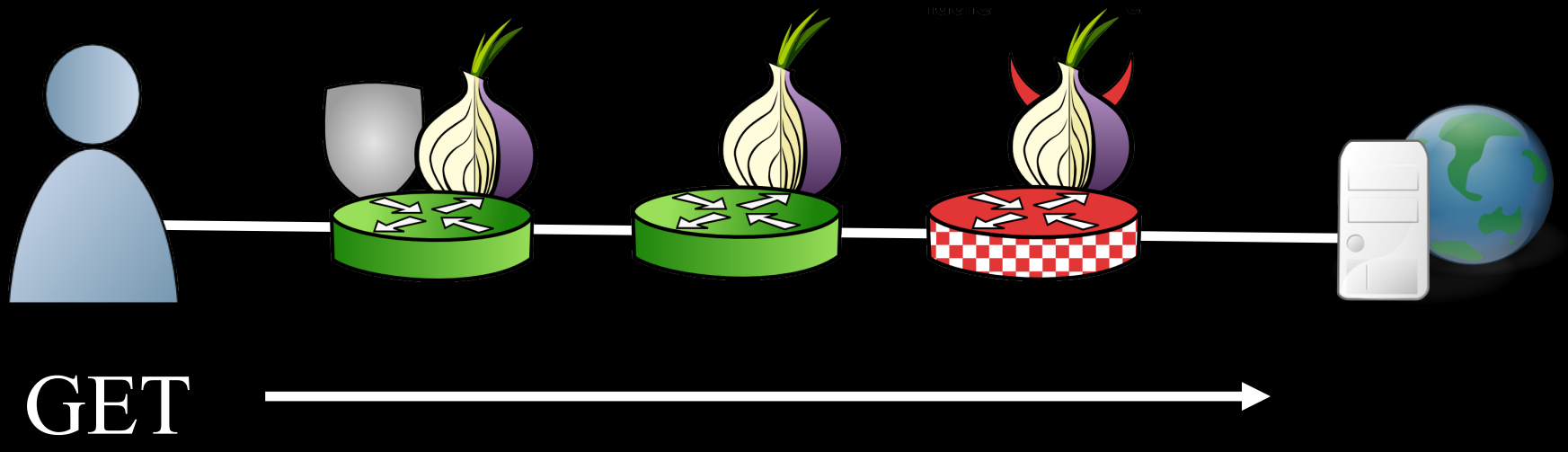
Traffic Correlation: Latency



- Inject redirect or javascript
- Start timer

Hopper et.al. CCS'07

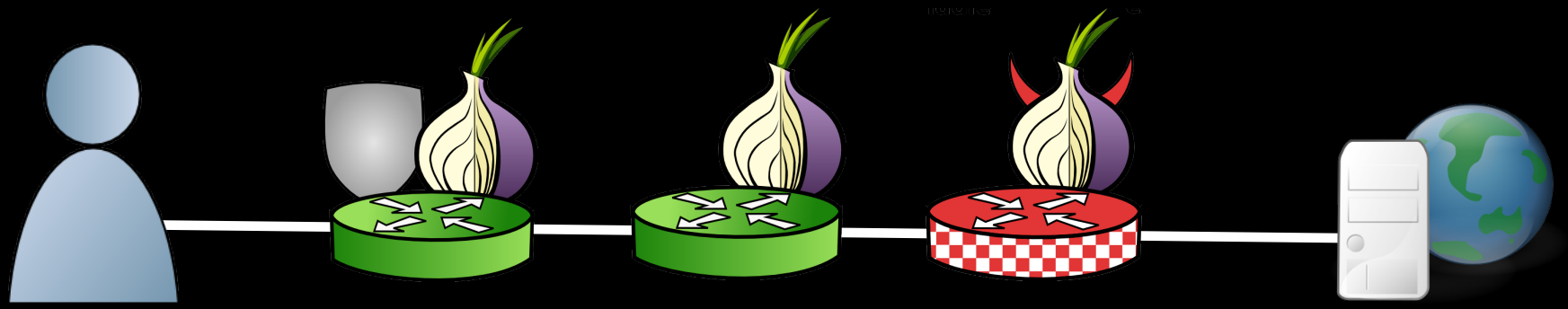
Traffic Correlation: Latency



- Request redirected page

Hopper et.al. CCS'07

Traffic Correlation: Latency



- Stop timer
- Estimate latency

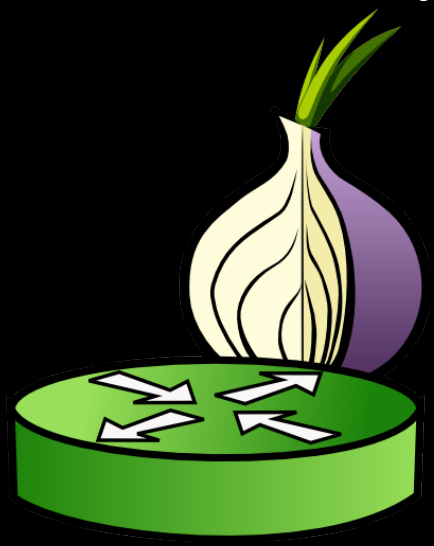
Hopper et.al. CCS'07

Outline

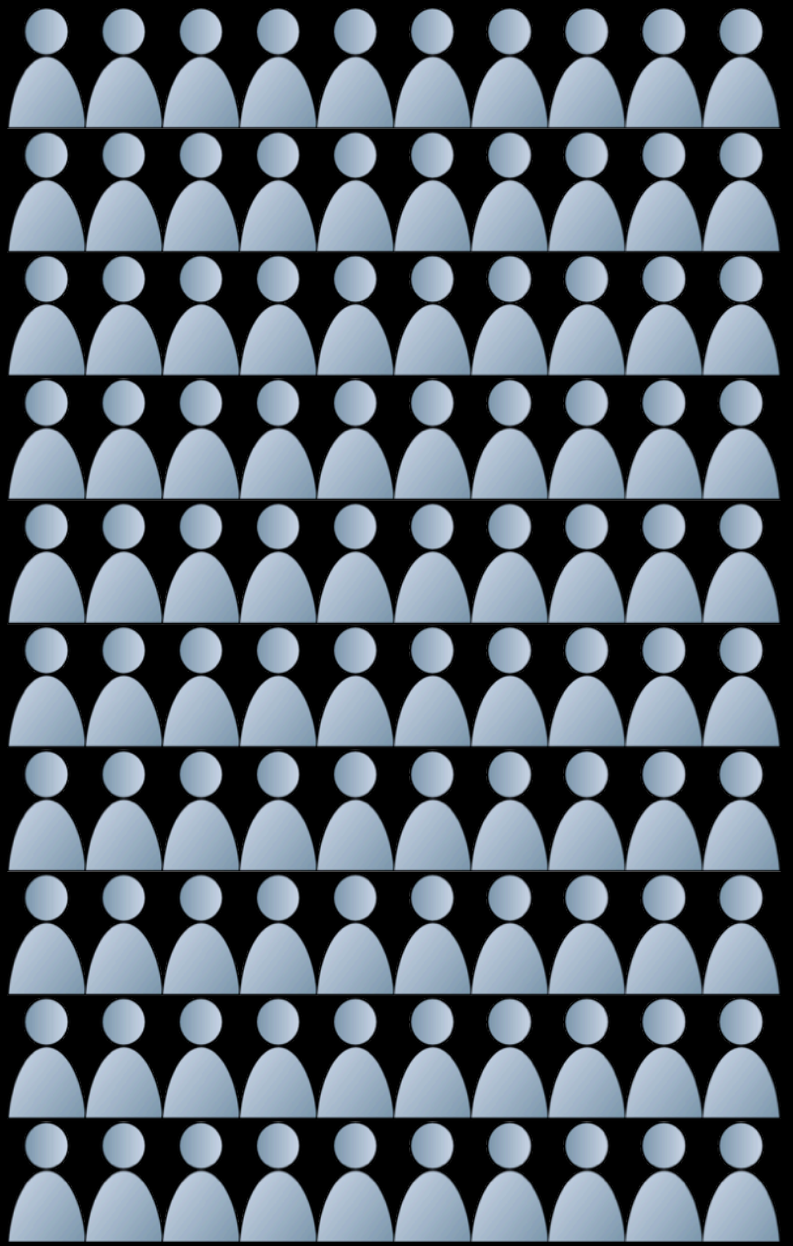
- ~~Tor intro, traffic correlation~~
- Why Tor is slow
- Traffic admission control
  - Induced throttling attack
  - Effects of throughput vs induced throttling
- Congestion control
  - Induced throttling attack
  - Effects of throughput vs induced throttling

Tor's Current Status

~3000 relays

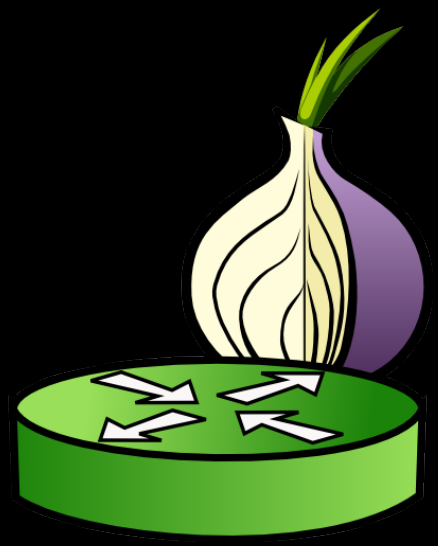


~500,000 clients

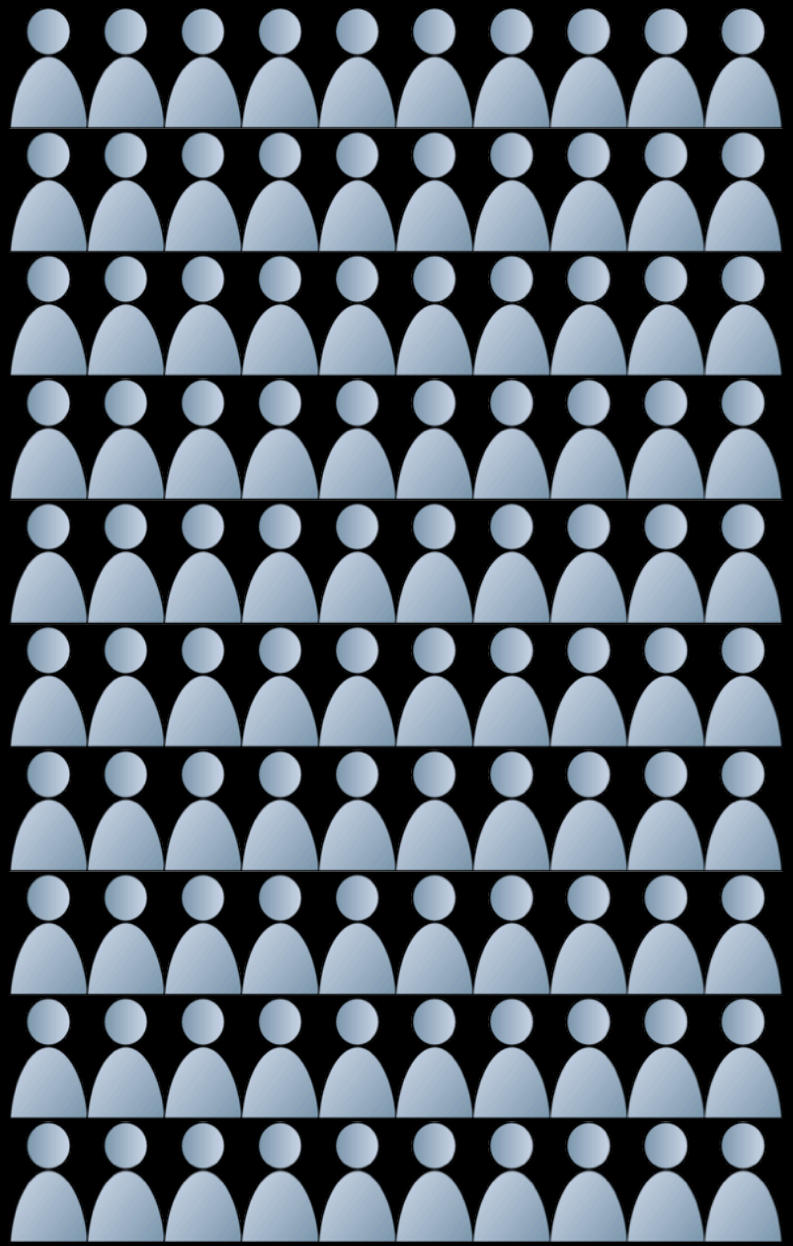


Tor's Current Status

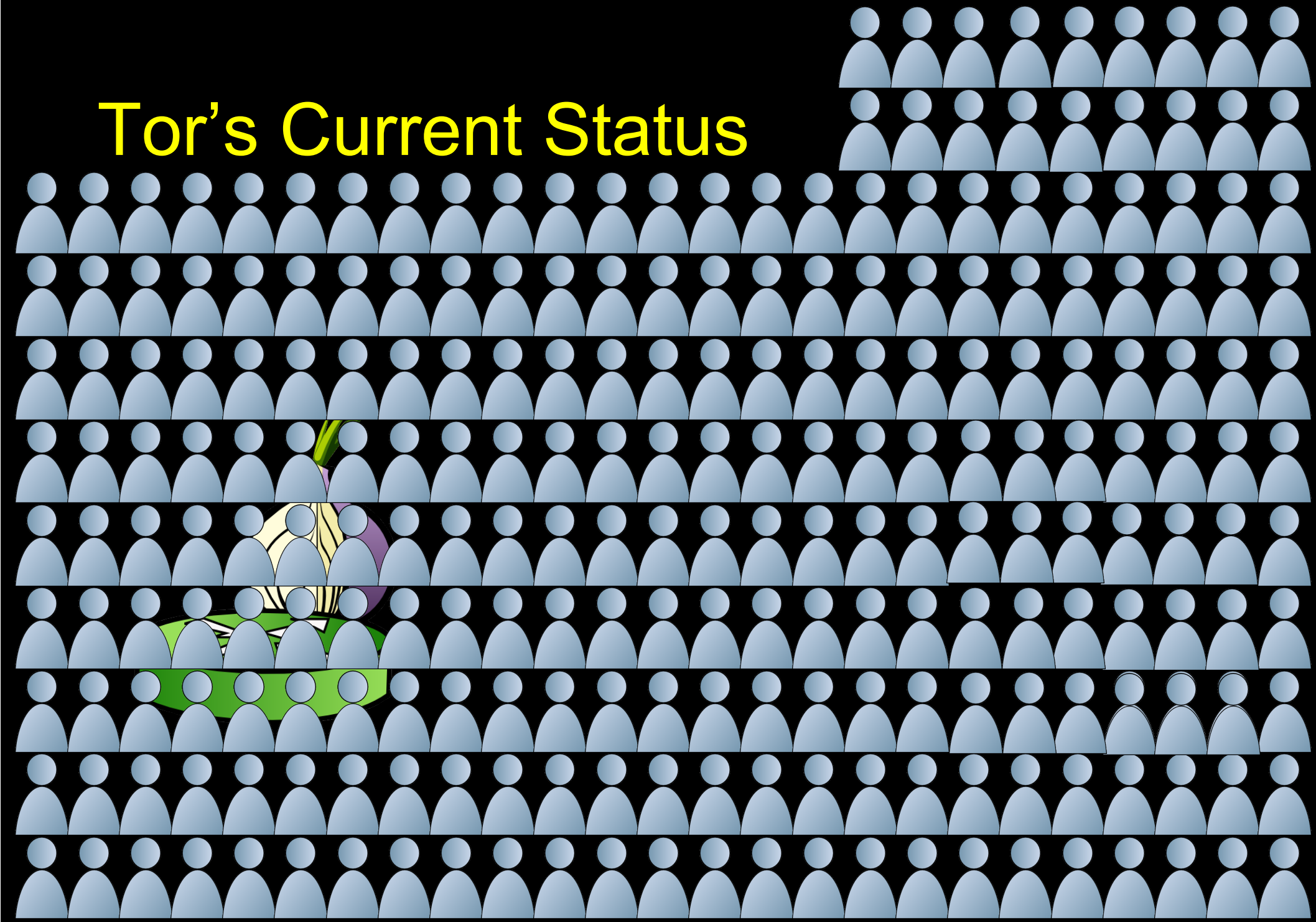
~~3000~~ 1200 relays

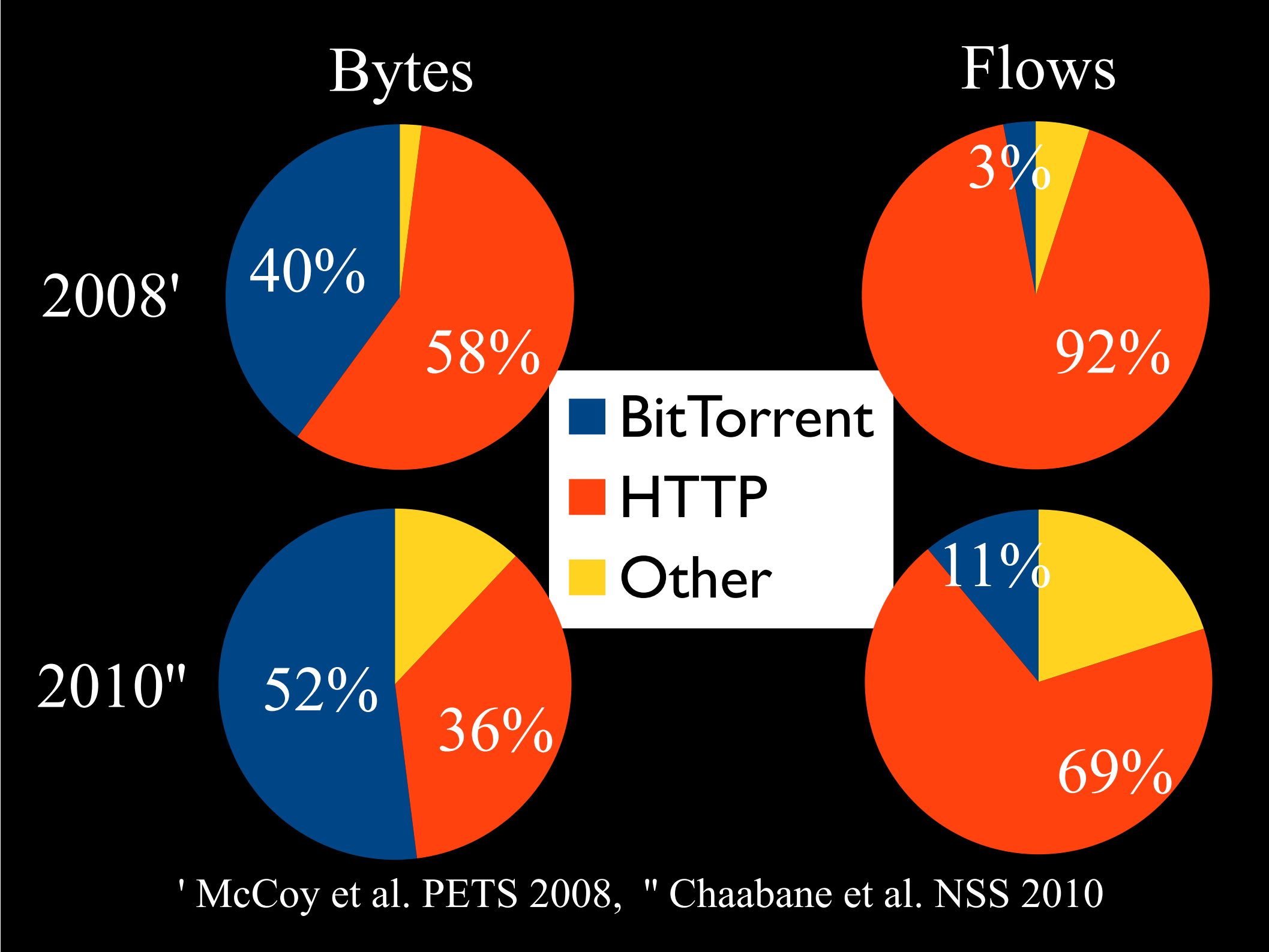


~500,000 clients



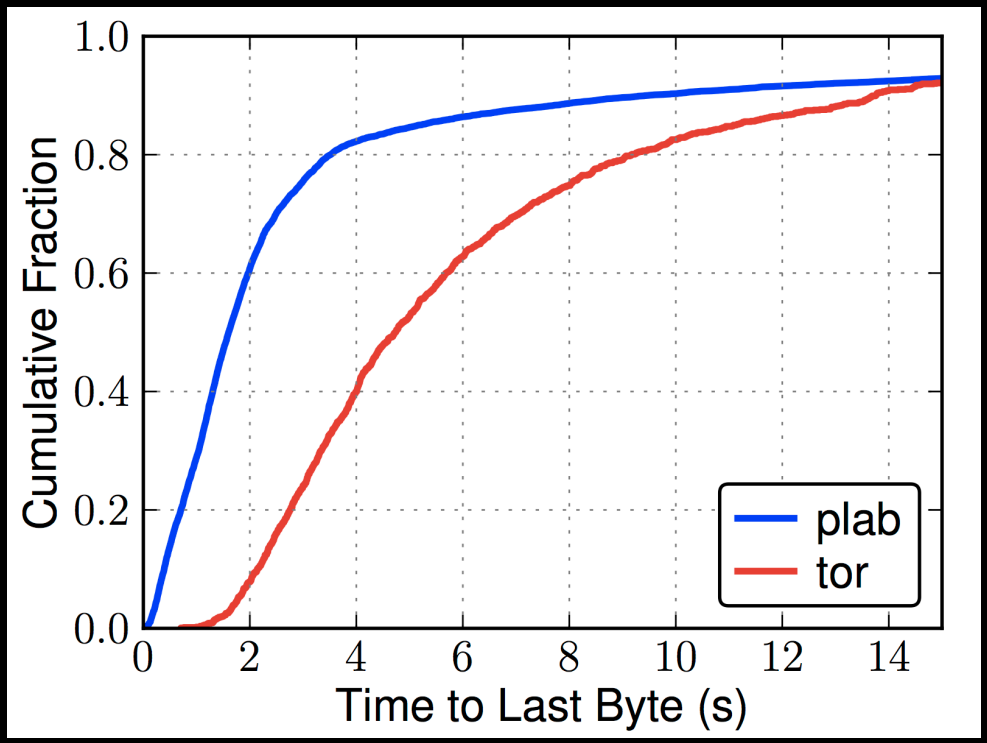
Tor's Current Status



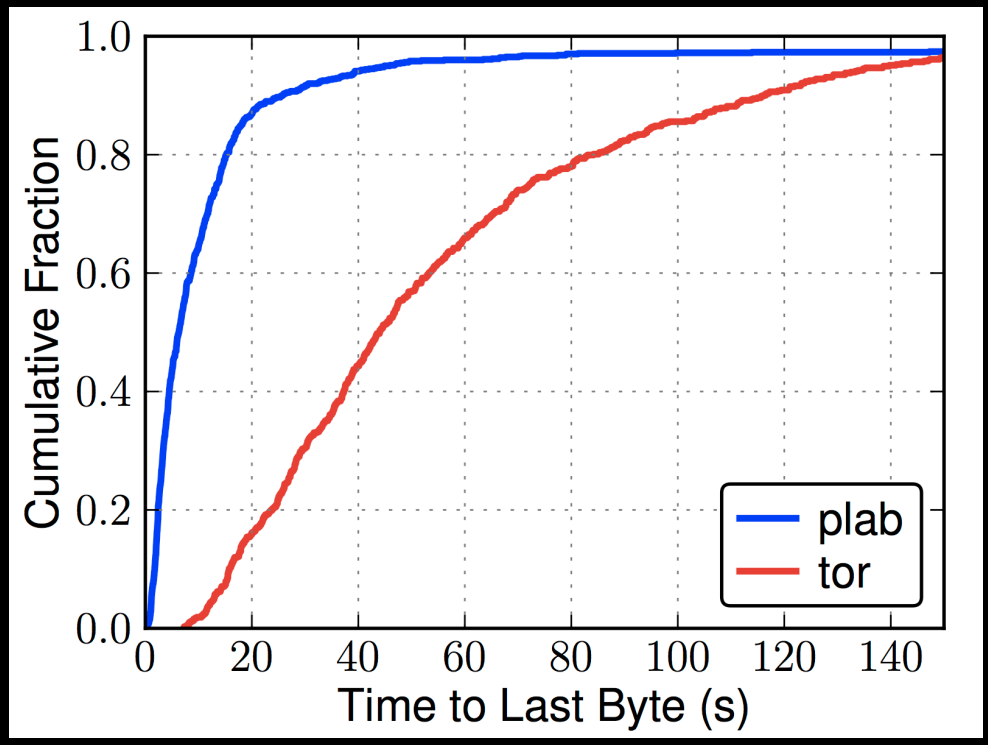

Bytes
Flows
2008'
2010"
40%
58%
3%
92%
52%
36%
11%
69%
BitTorrent
HTTP
Other
' McCoy et al. PETS 2008, " Chaabane et al. NSS 2010

Tor is Slow[er]

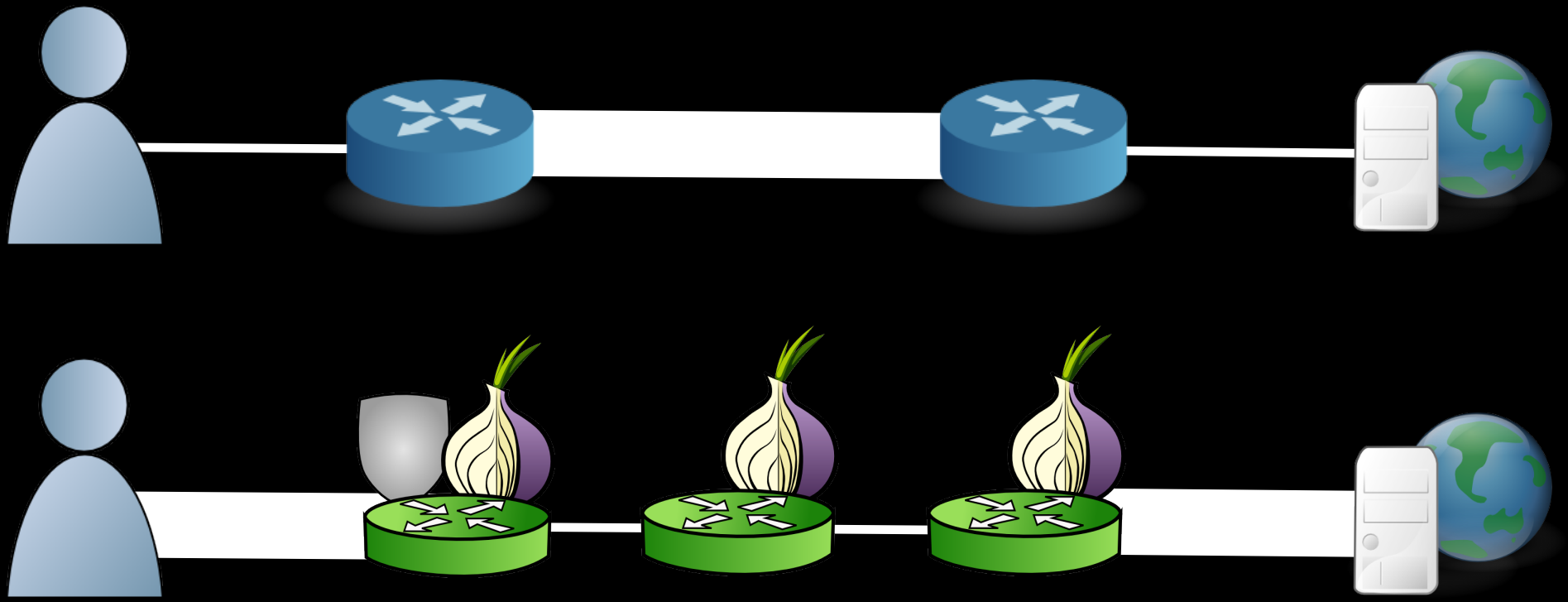
Web (320 KiB)



Bulk (5 MiB)



Tor != Internet

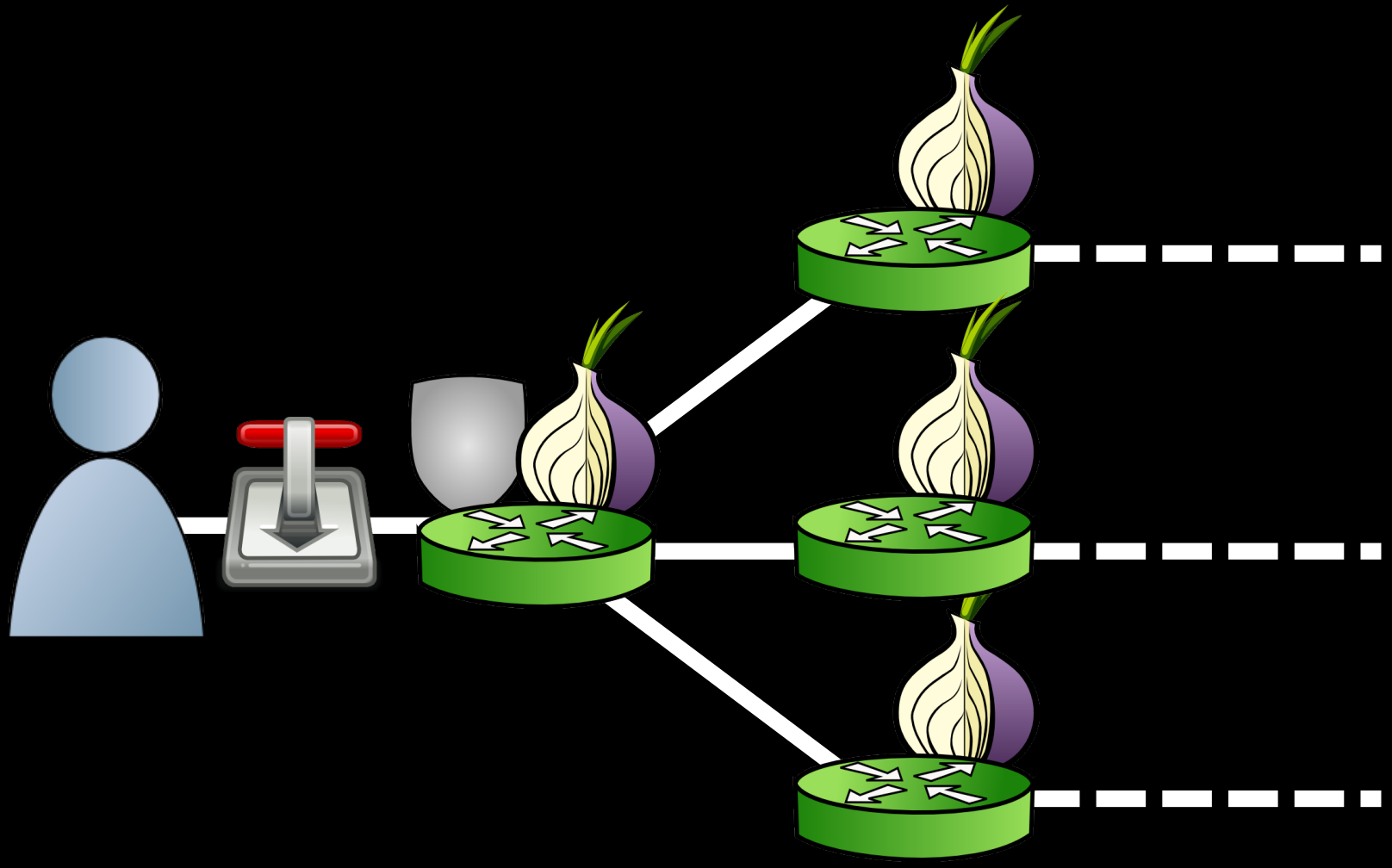


- Specialized Tor performance enhancements
  - Reducing load: traffic admission control
  - Reducing load, improving utilization: congestion control

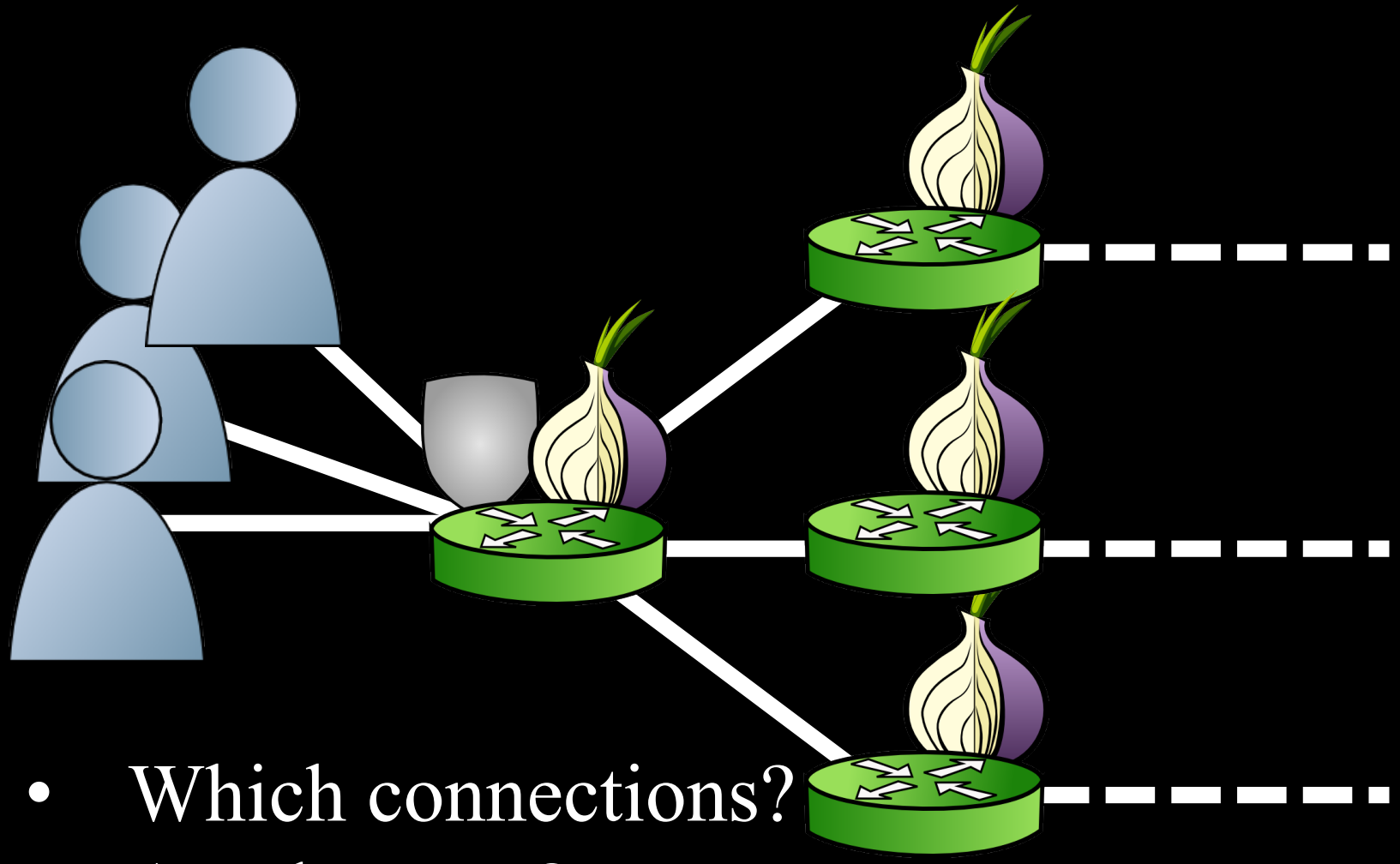
Outline

- ~~Tor intro, traffic correlation~~
- ~~Why Tor is slow~~
- Traffic admission control
  - Induced throttling attack
  - Effects of throughput vs induced throttling
- Congestion control
  - Induced throttling attack
  - Effects of throughput vs induced throttling

Traffic Admission Control

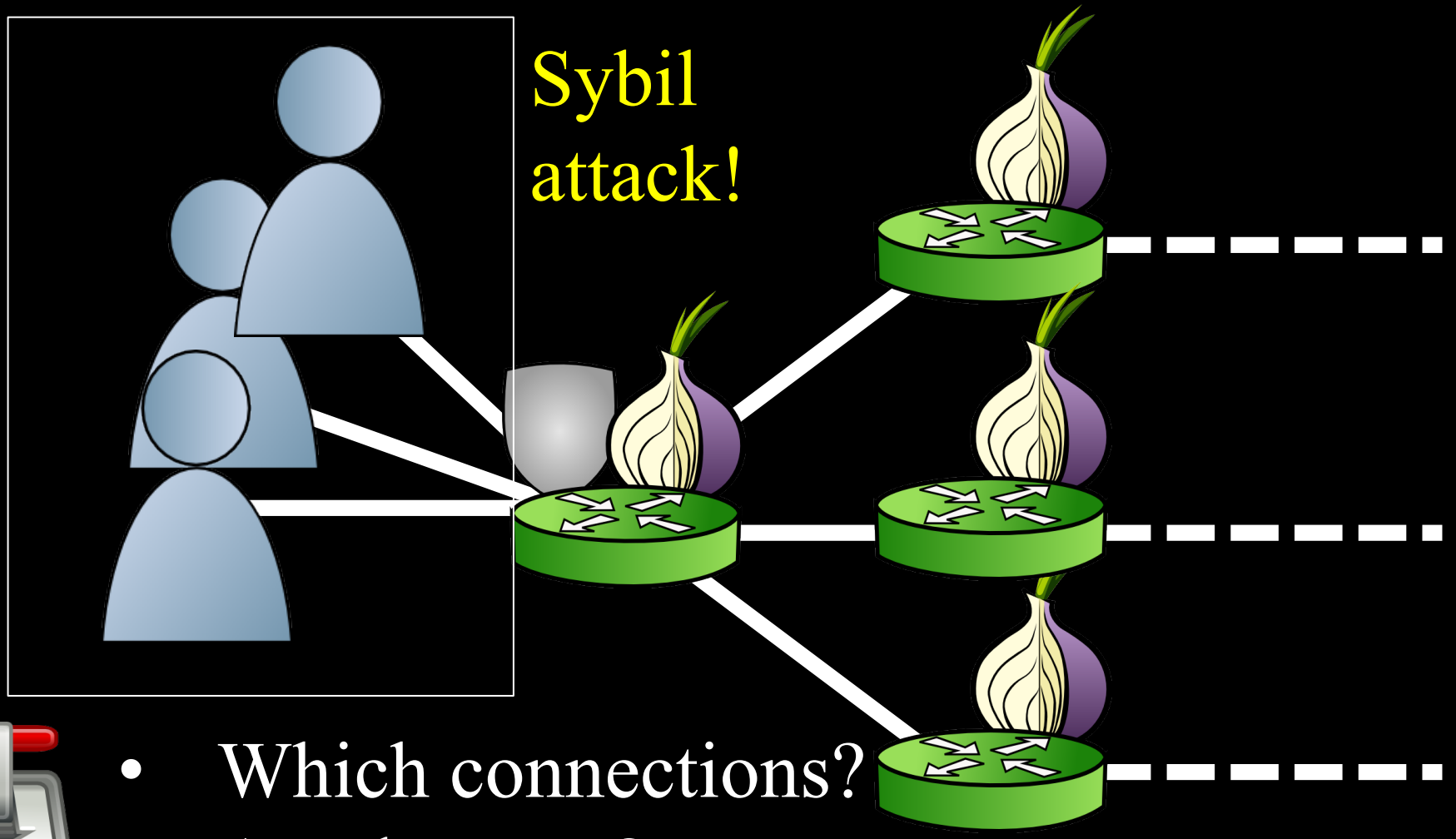


Traffic Admission Control



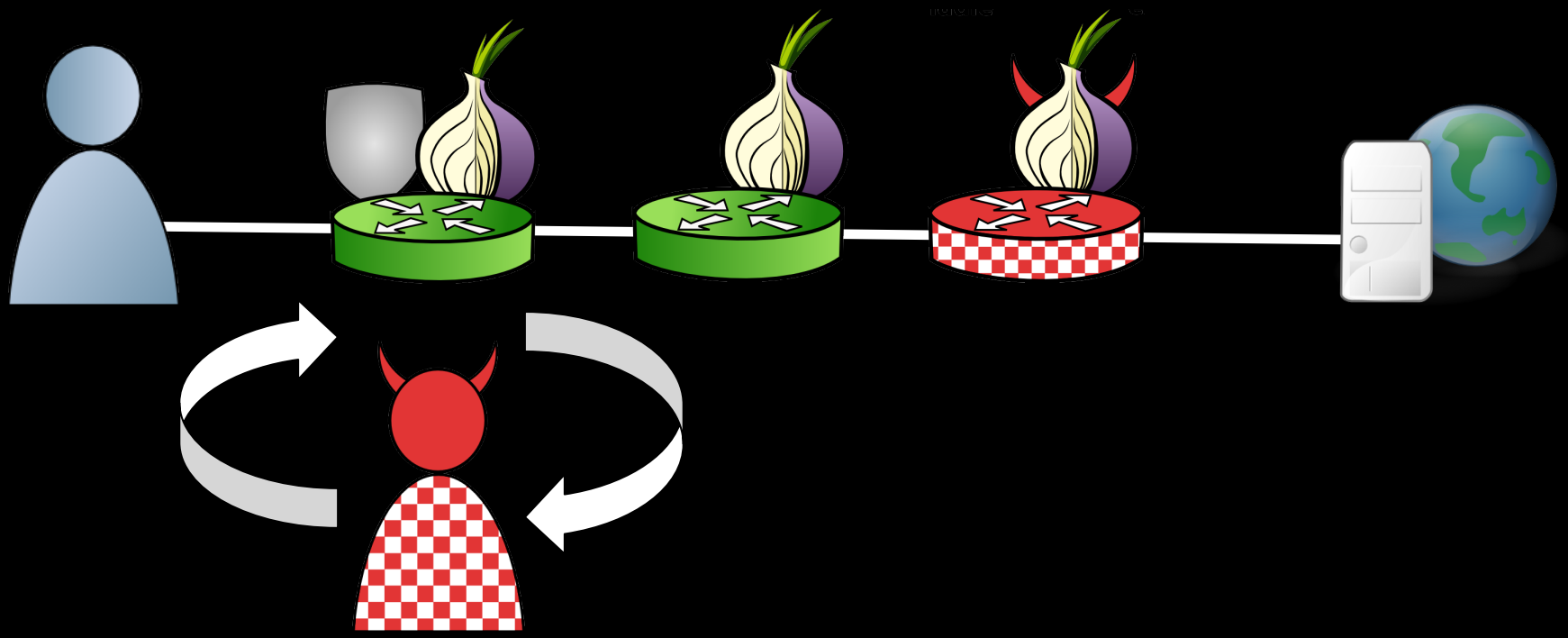
- Which connections?
- At what rate?

Traffic Admission Control



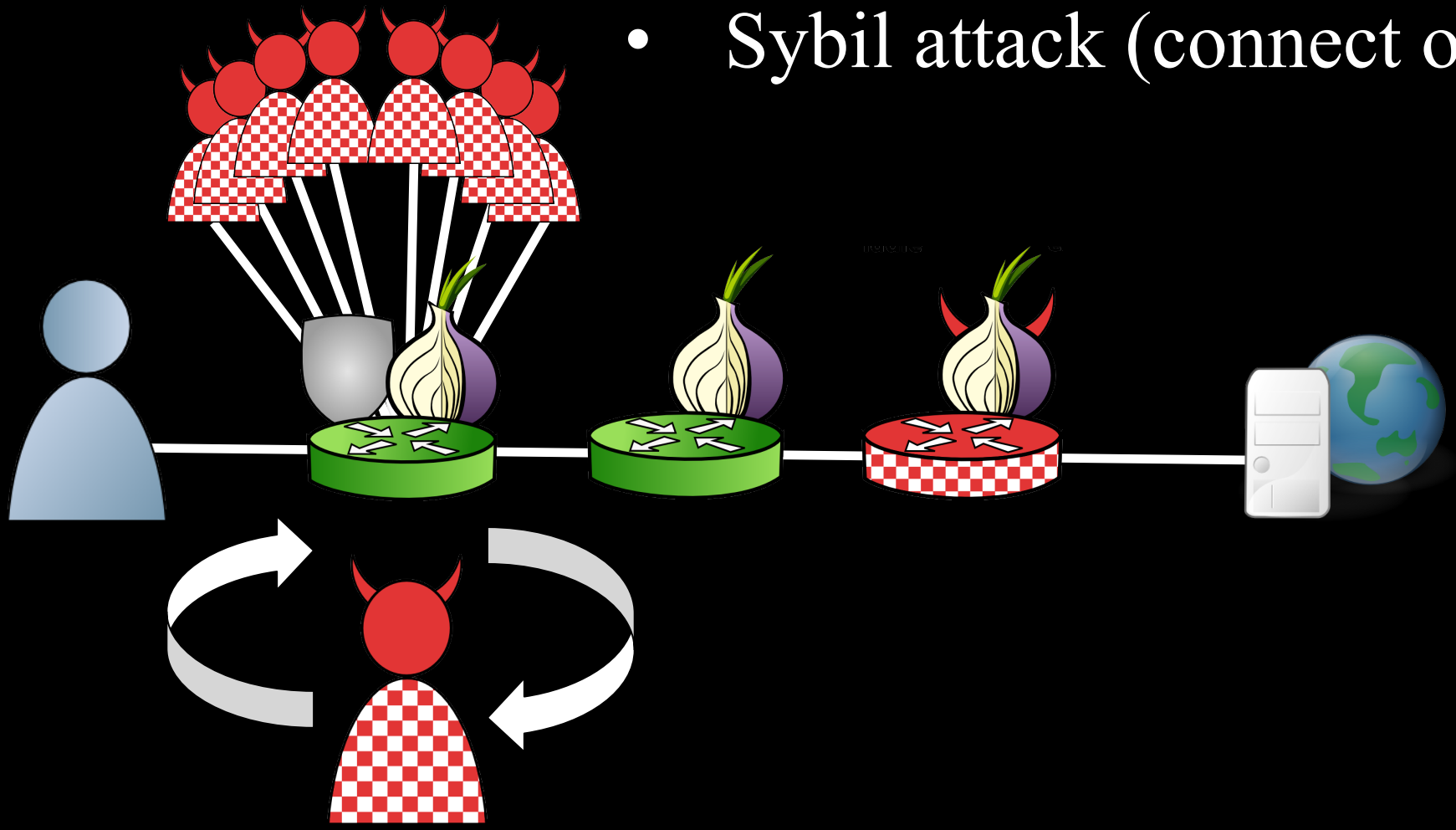
- Which connections?
- At what rate?

Traffic Admission Control

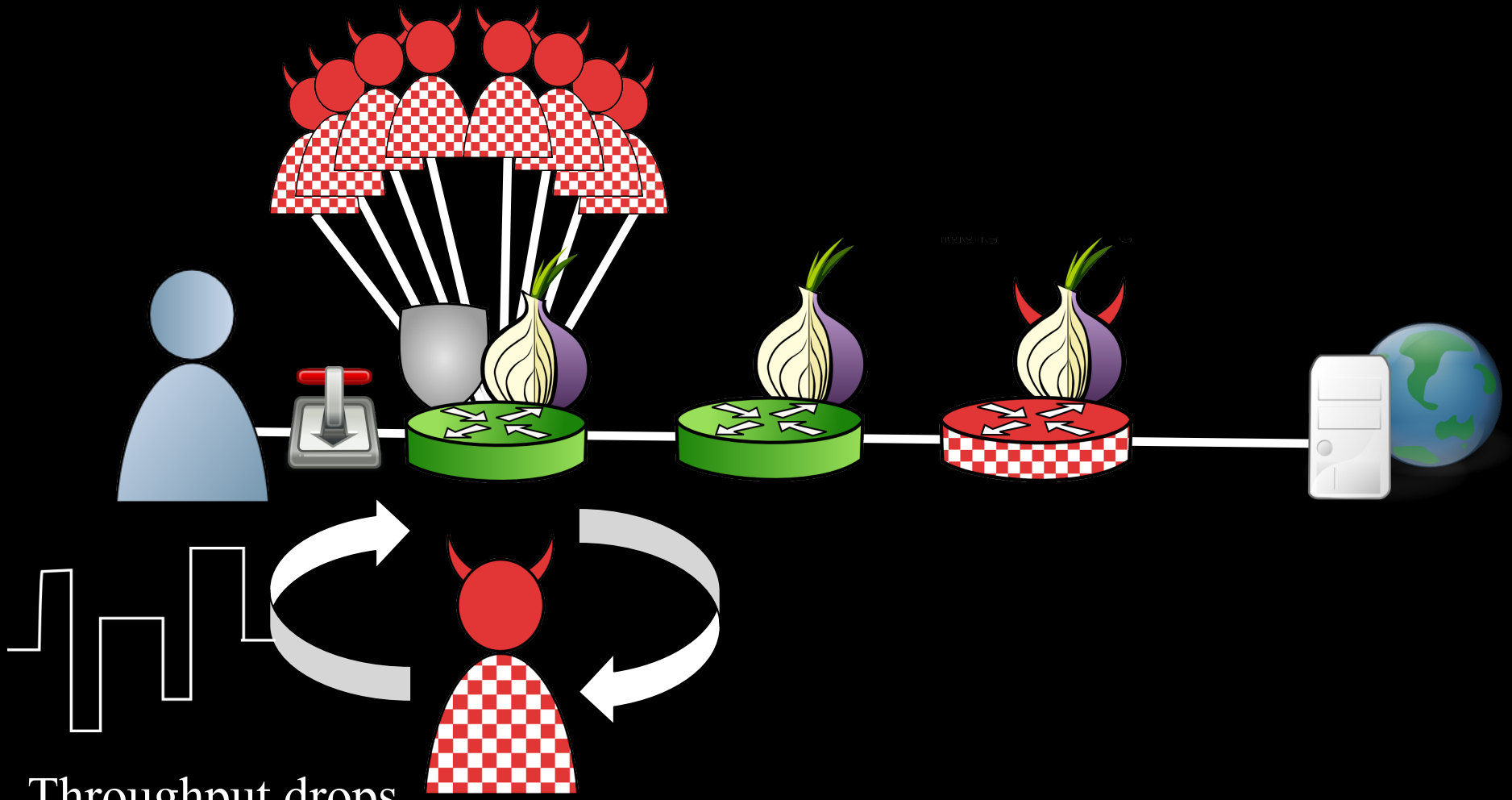


Traffic Admission Control

- Sybil attack (connect only)



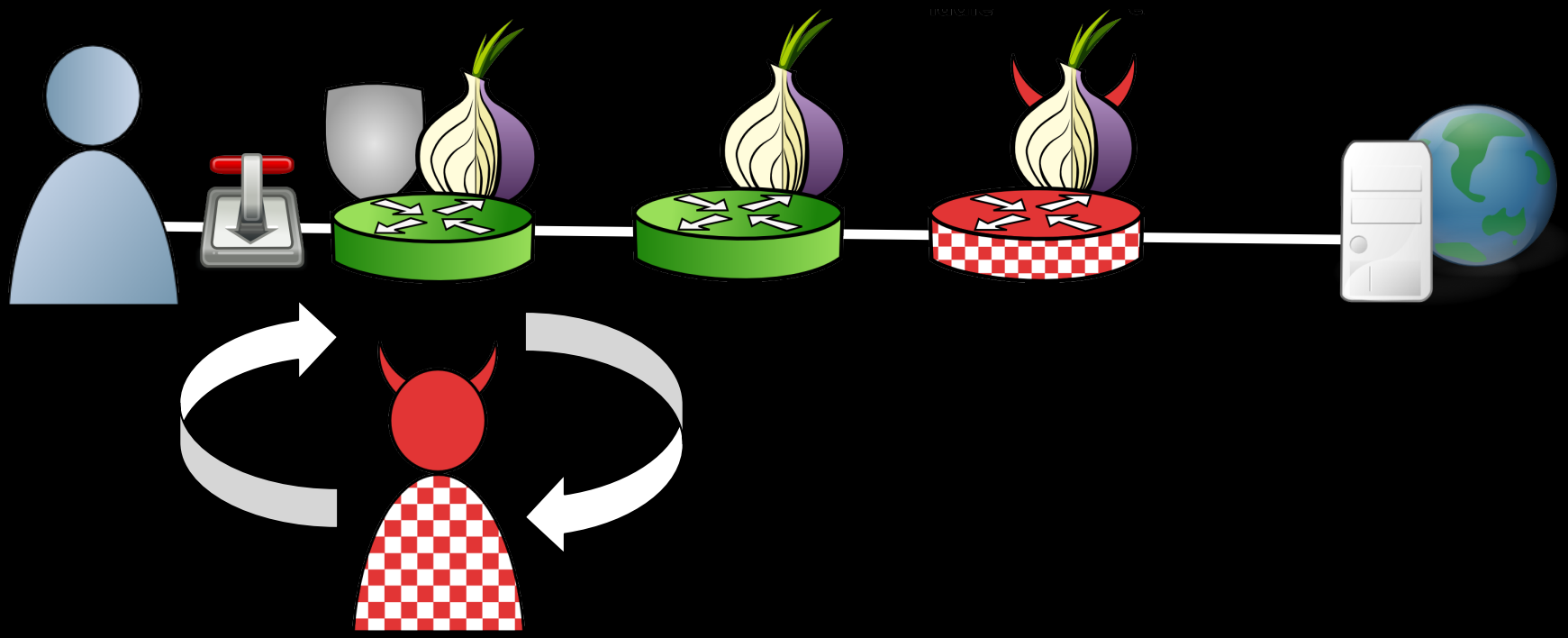
Traffic Admission Control



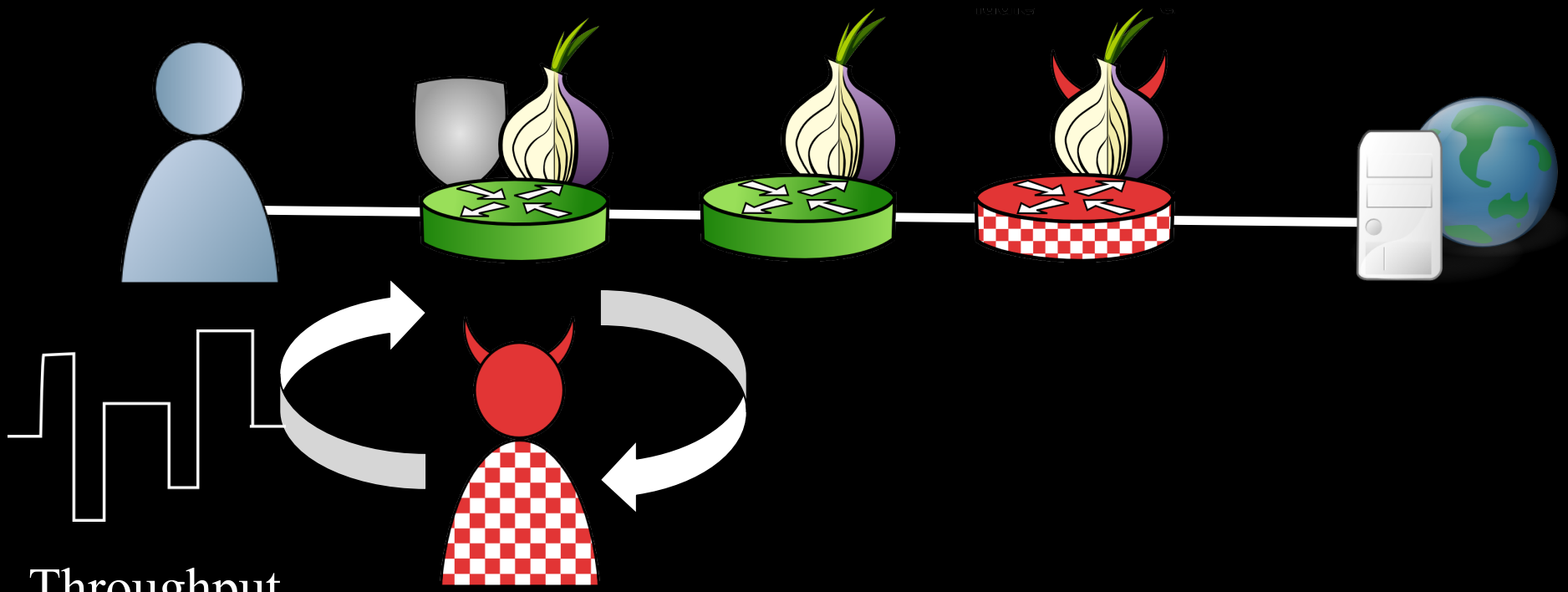
Throughput drops
to throttle rate

Traffic Admission Control

- Disconnect sybils

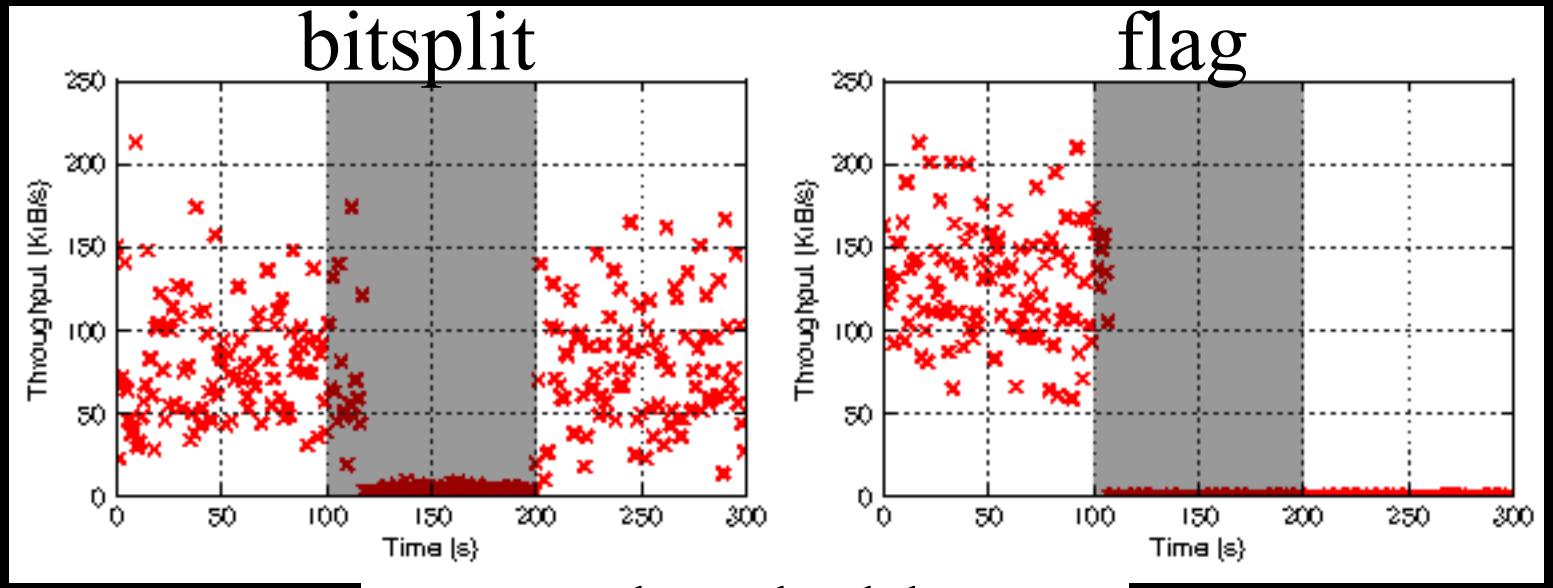


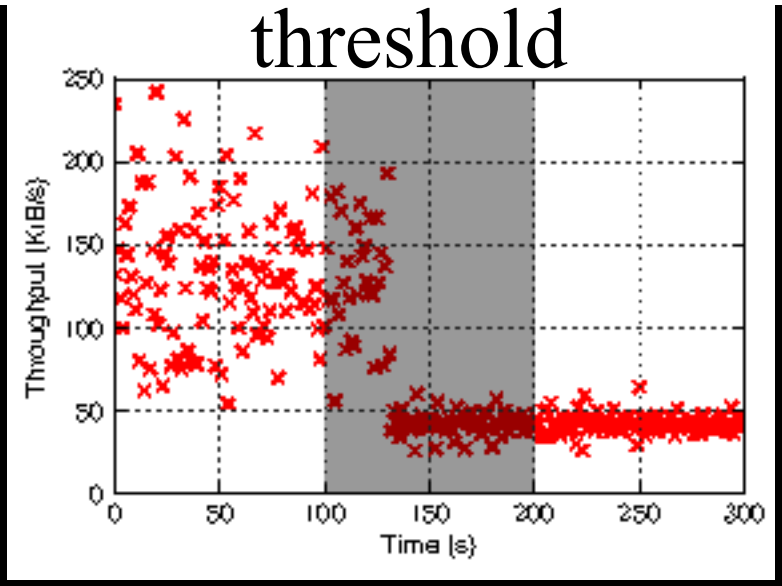
Traffic Admission Control



Throughput increases

Induced Throttling Prototype

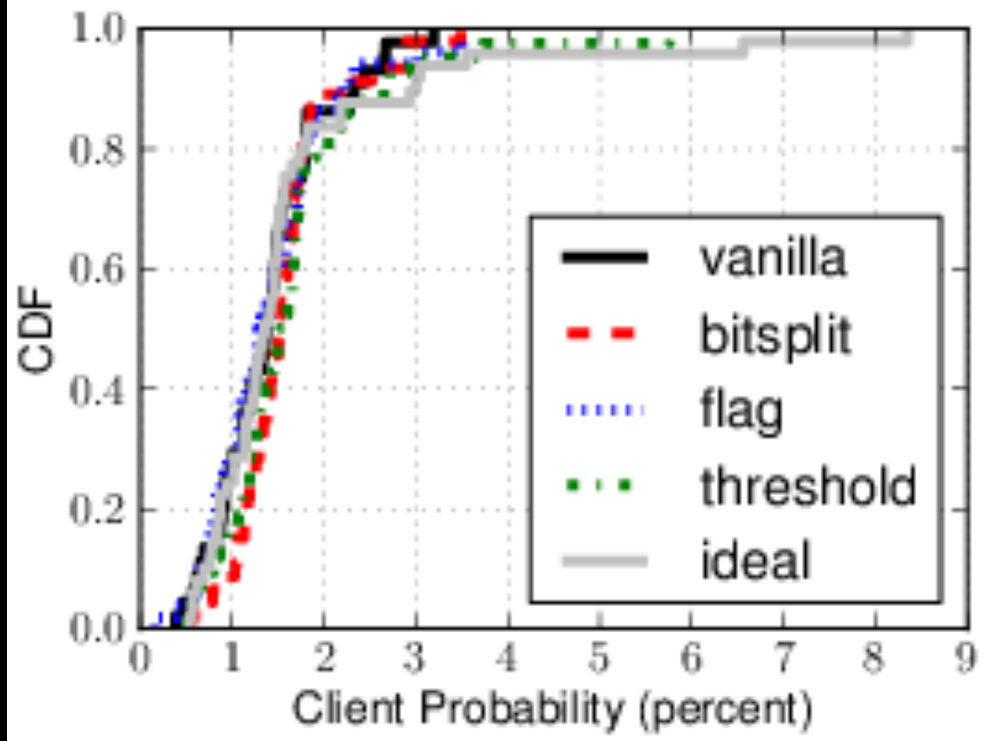


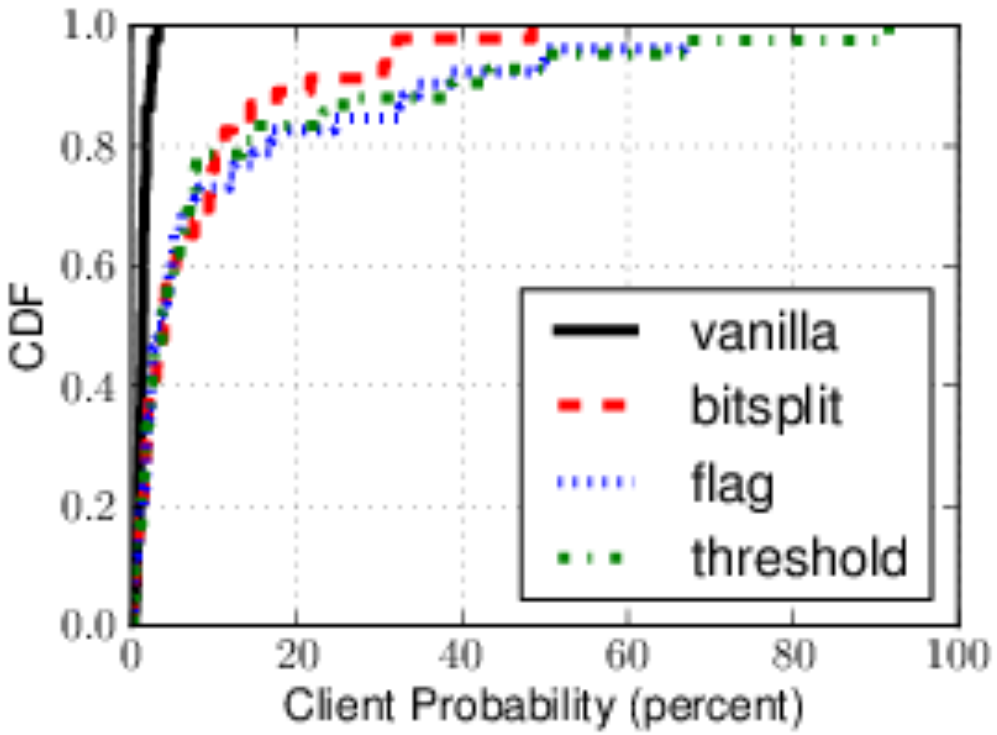


Jansen et.al.
USENIX Sec'12

Induced Throttling Results

$$P[V = C_i] = \sum_j P[V = C_i \mid R_j] P[G = R_j]$$





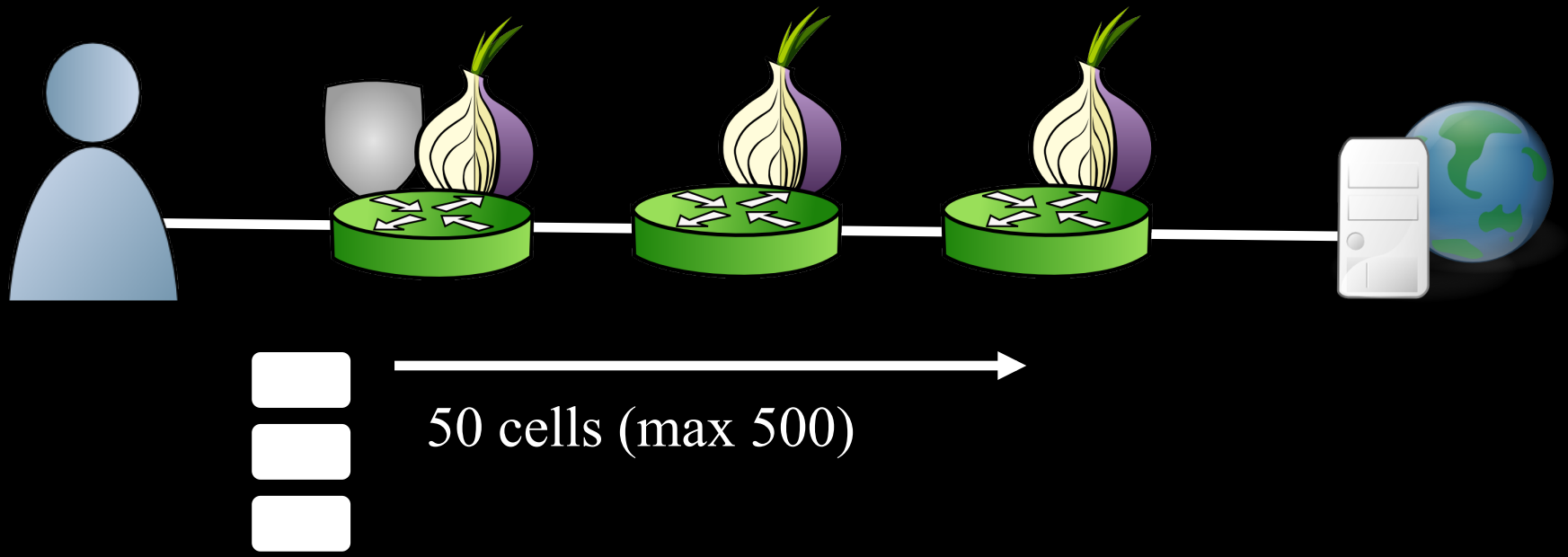
Throughput Attack

Induced Throttling Attack

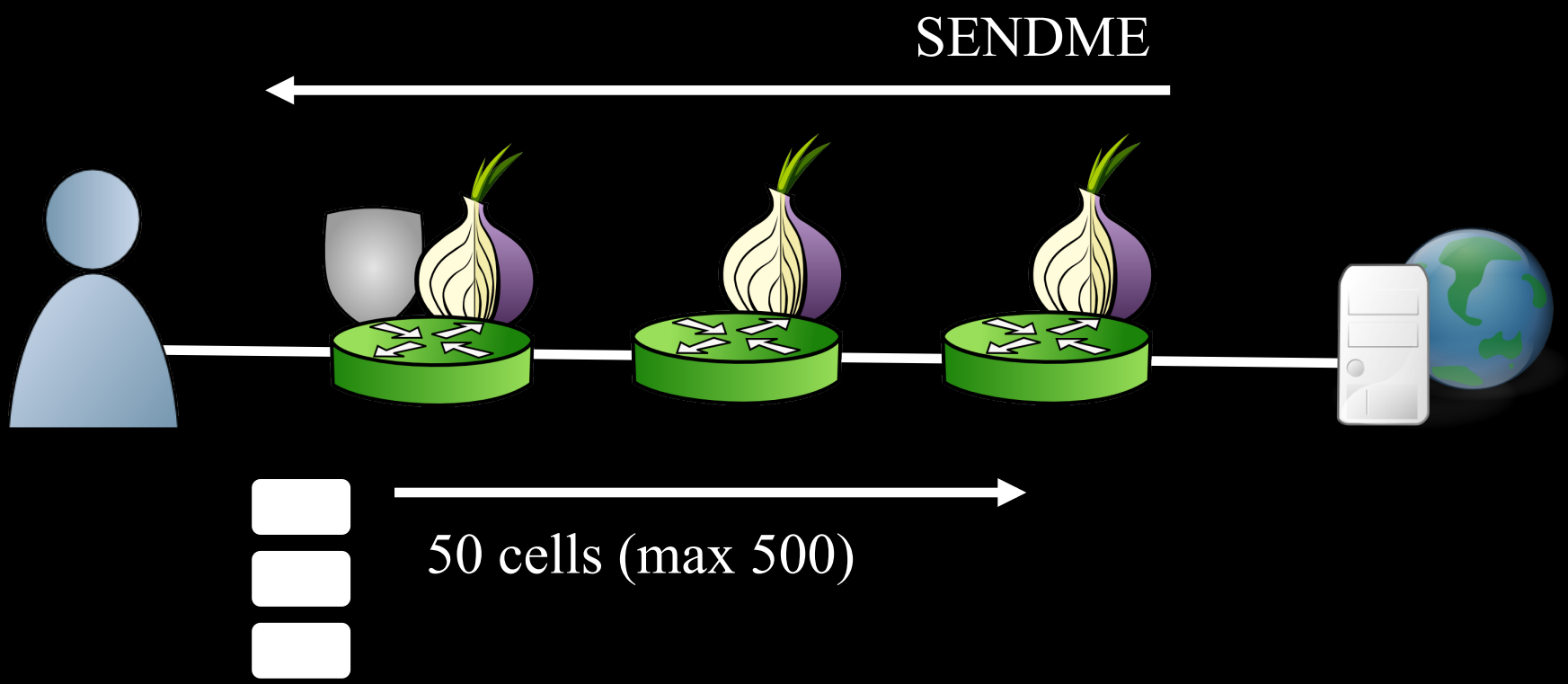
Outline

- ~~Tor intro, traffic correlation~~
- ~~Why Tor is slow~~
- ~~Traffic admission control~~
  - ~~Induced throttling attack~~
  - ~~Effects of throughput vs induced throttling~~
- Congestion control
  - Induced throttling attack
  - Effects of throughput vs induced throttling

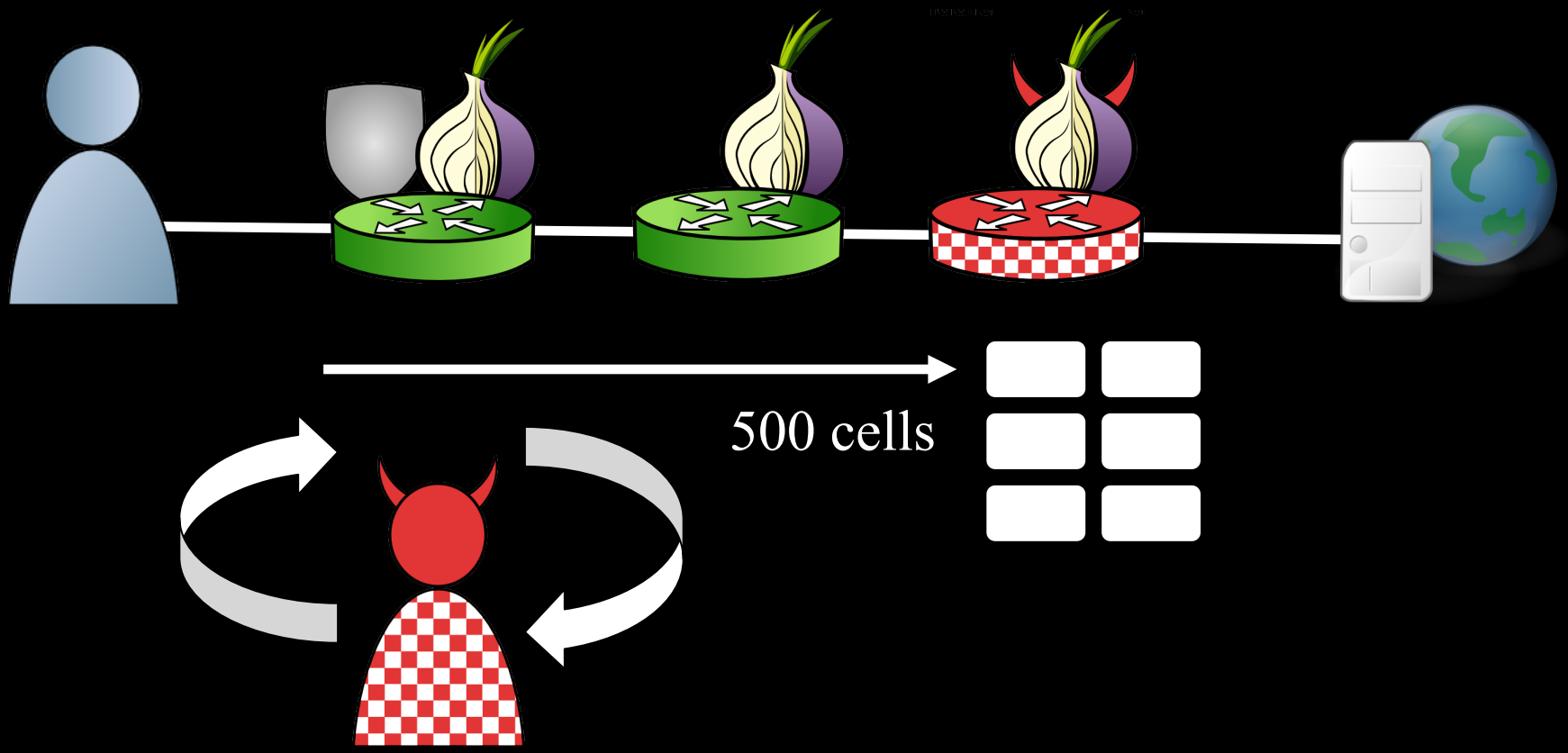
Congestion Control



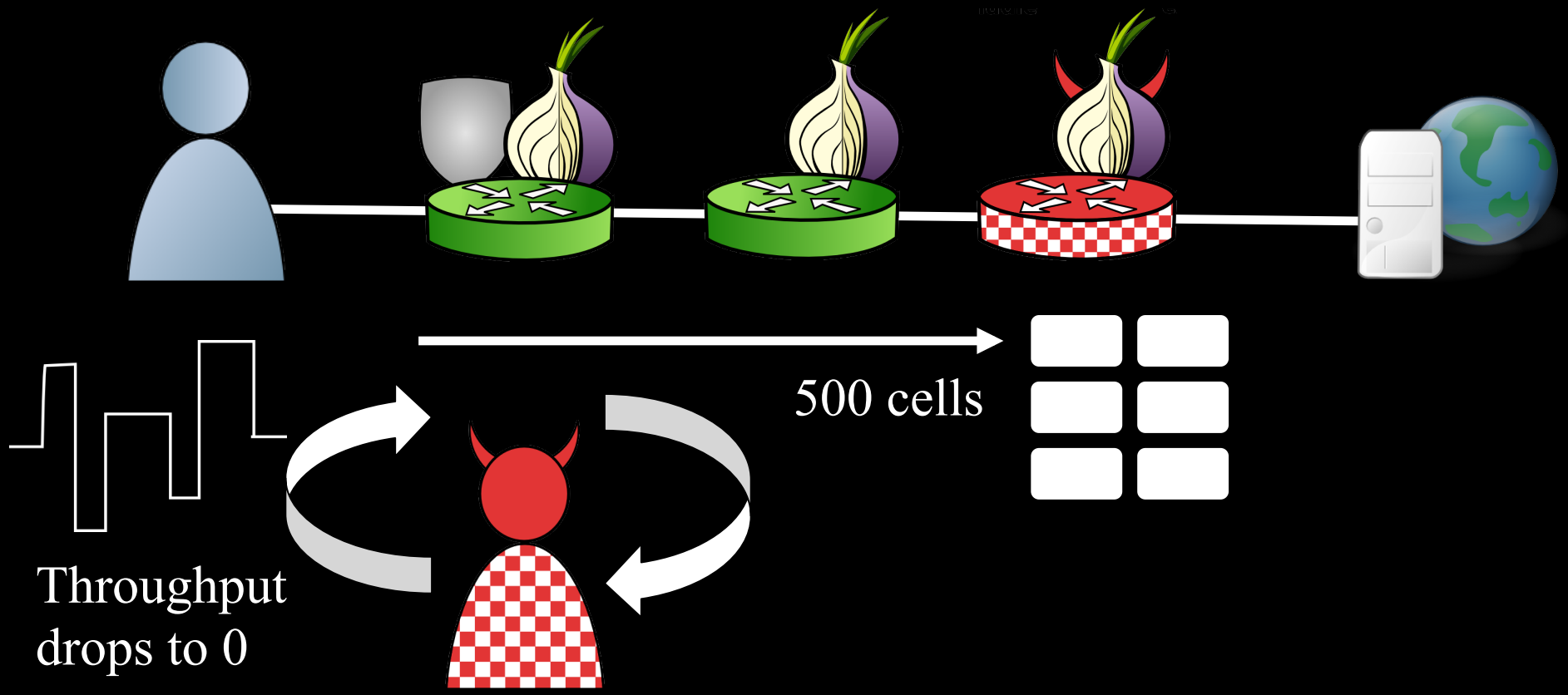
Congestion Control



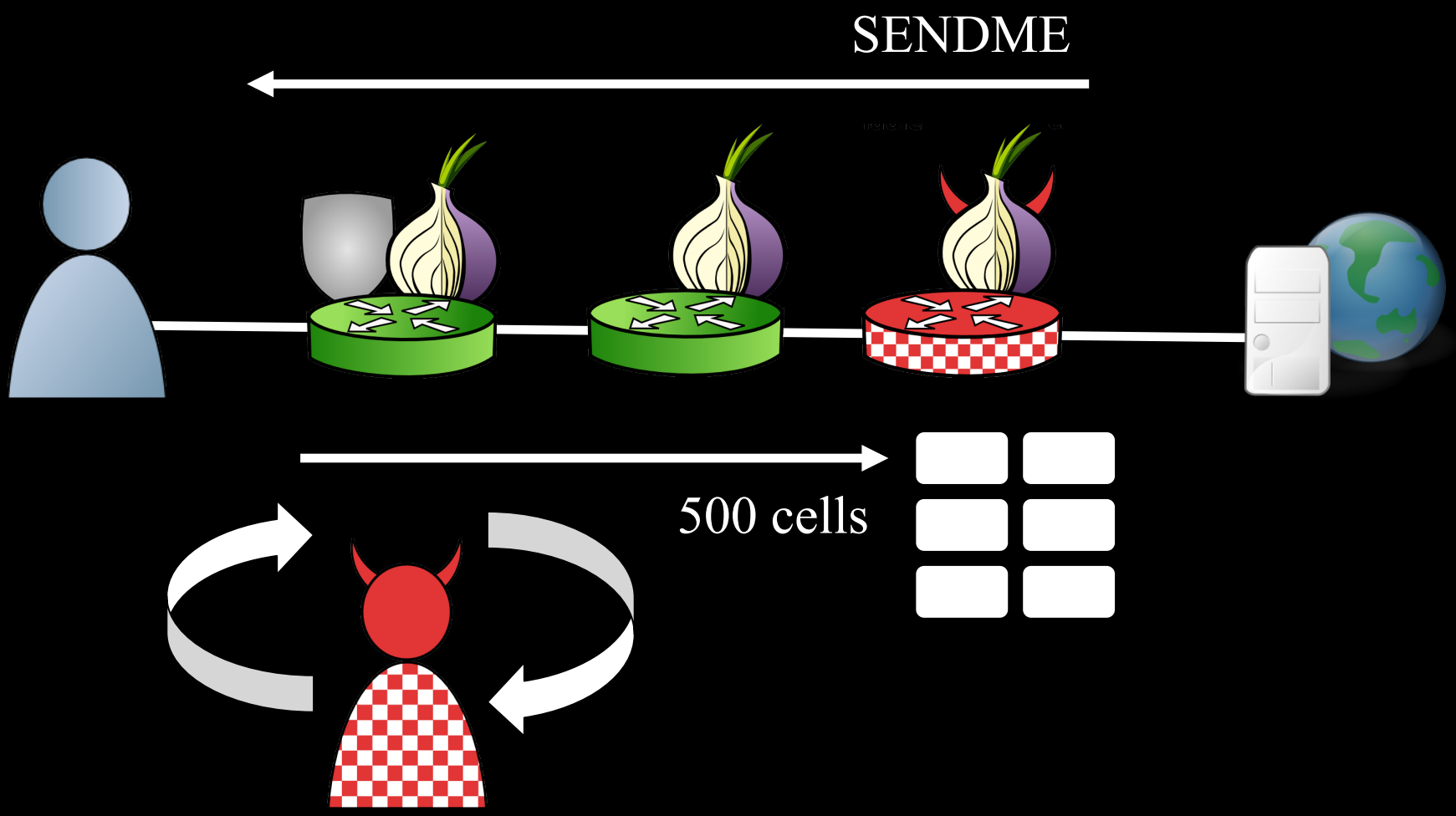
Congestion Control



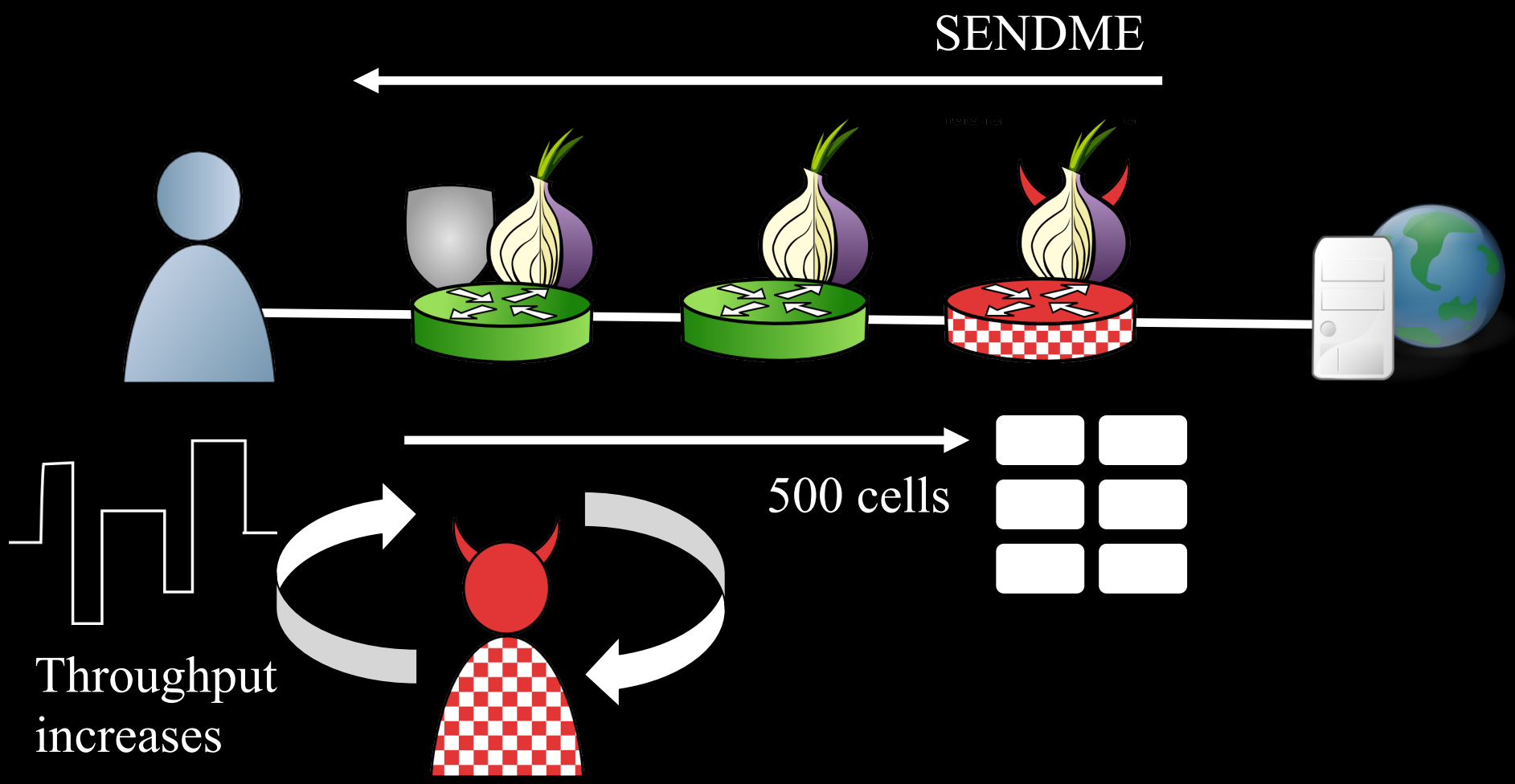
Congestion Control



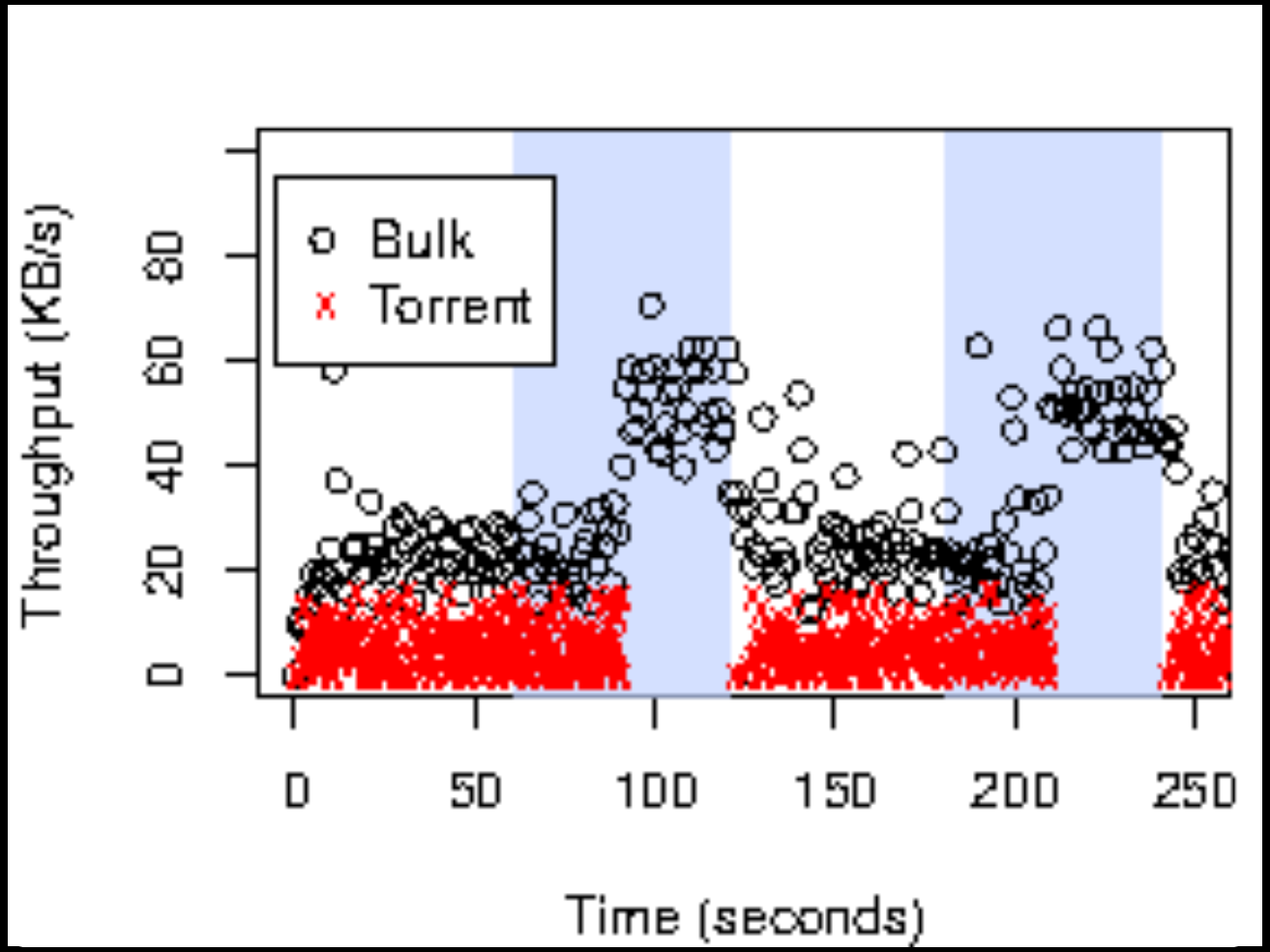
Congestion Control



Congestion Control

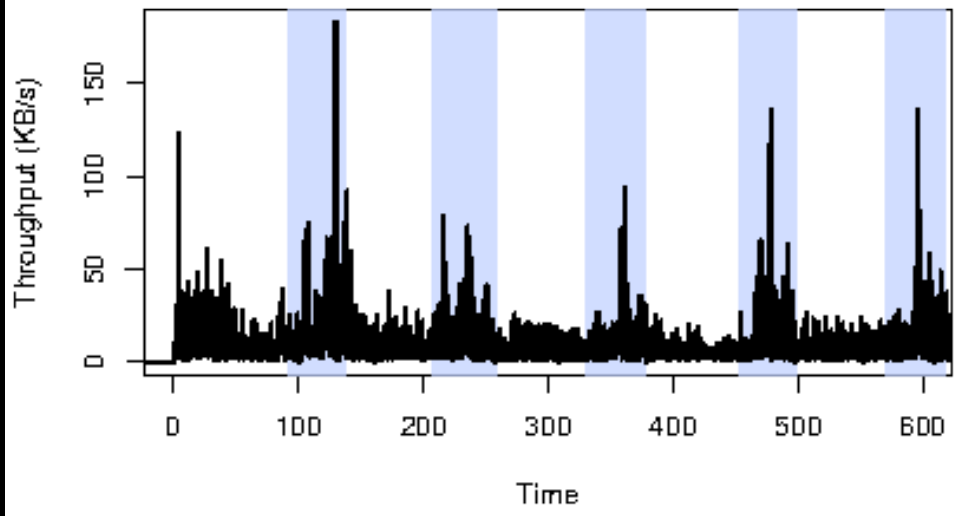


Induced Throttling Prototype

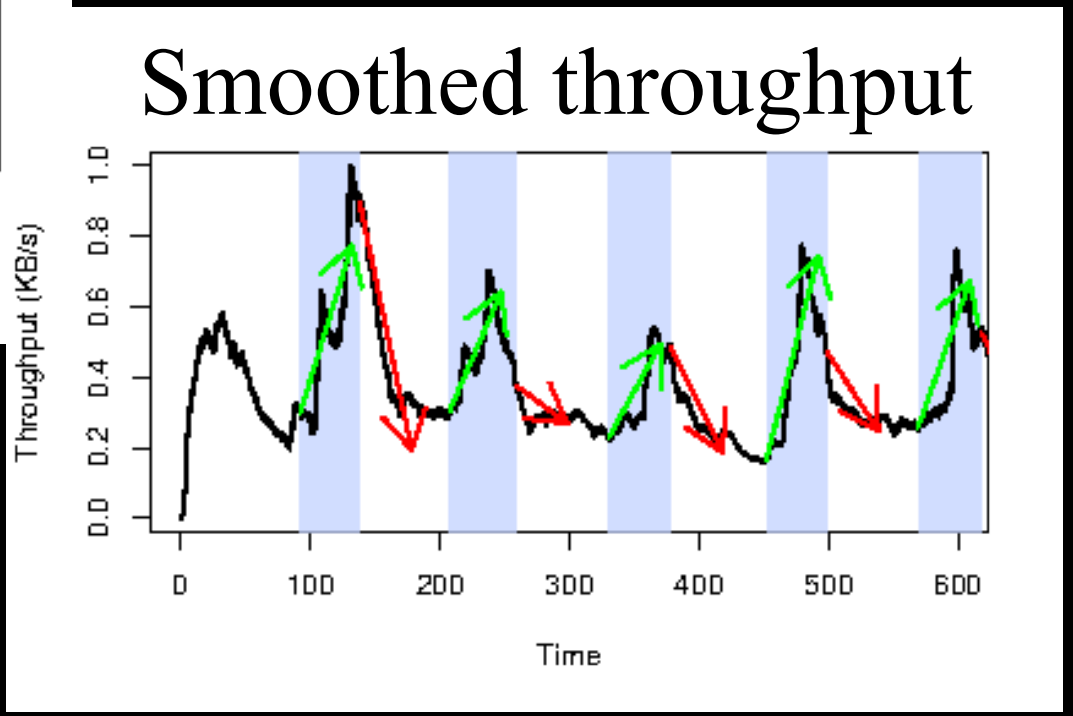


Induced Throttling Results

Raw throughput

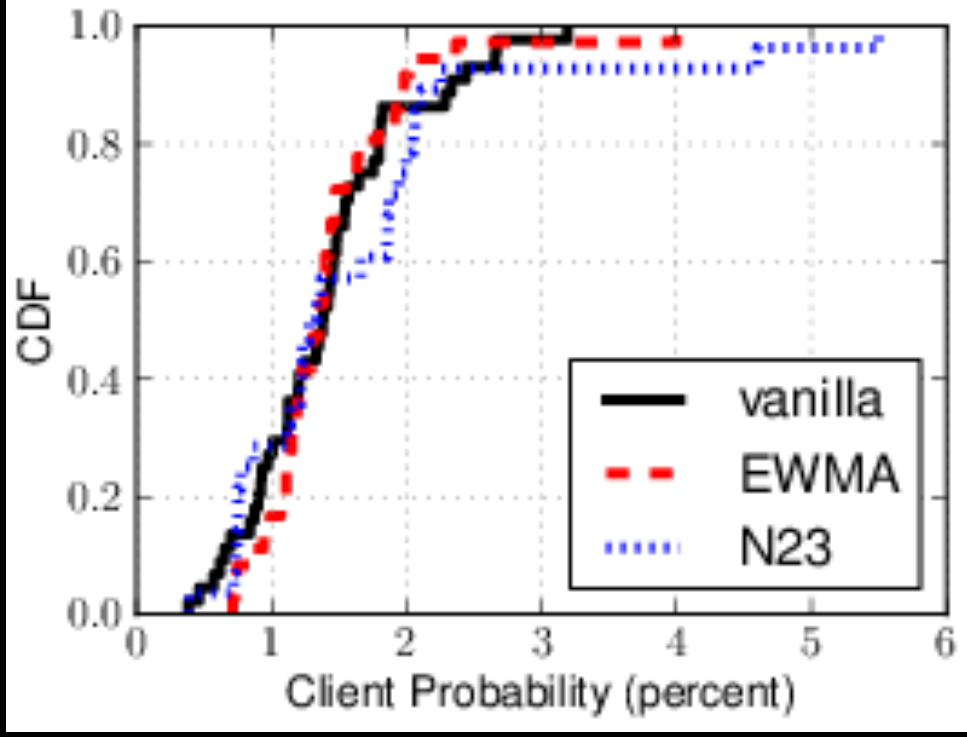


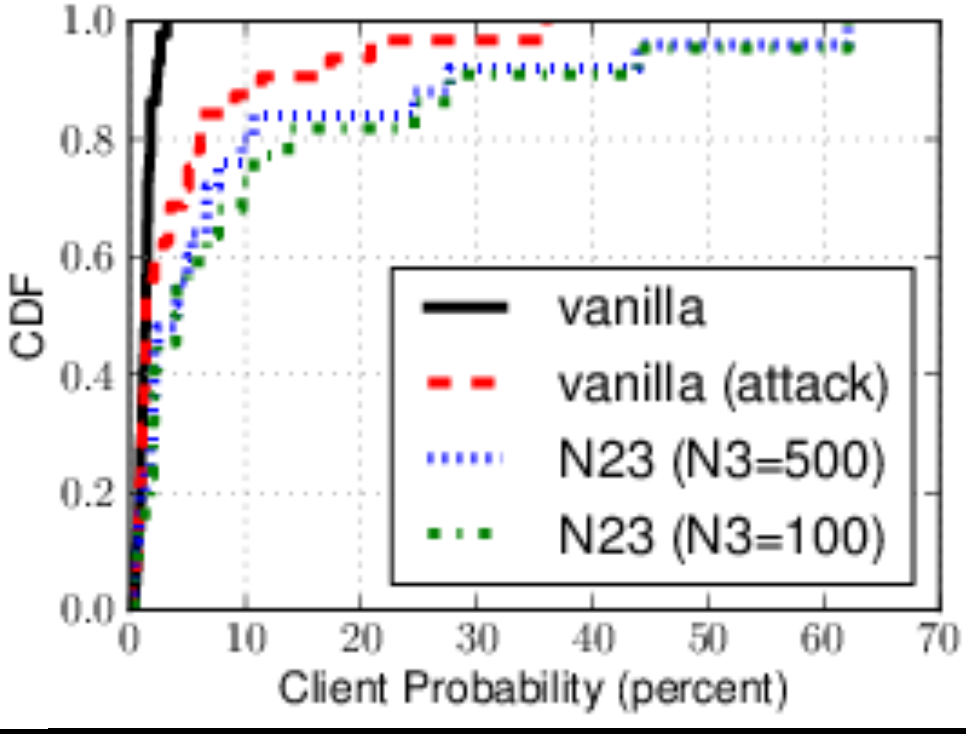
Smoothed throughput



Induced Throttling Results

$$P[V = C_i] = \sum_j P[V = C_i \mid R_j] P[G = R_j]$$





Throughput Attack

Induced Throttling Attack

Questions?

rob.g.jansen@nrl.navy.mil