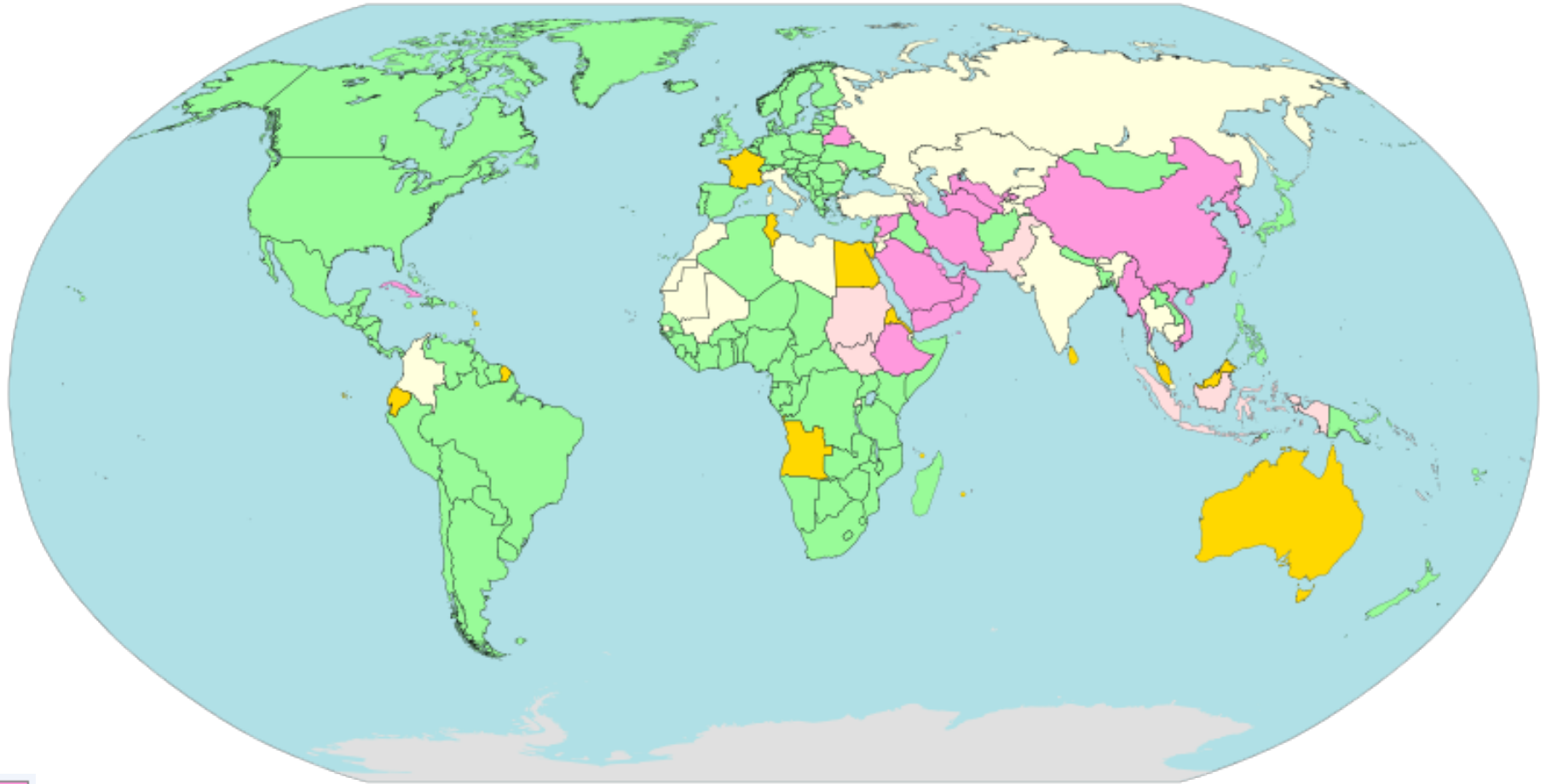


Anticensorship in the Network Infrastructure

Eric Wustrow

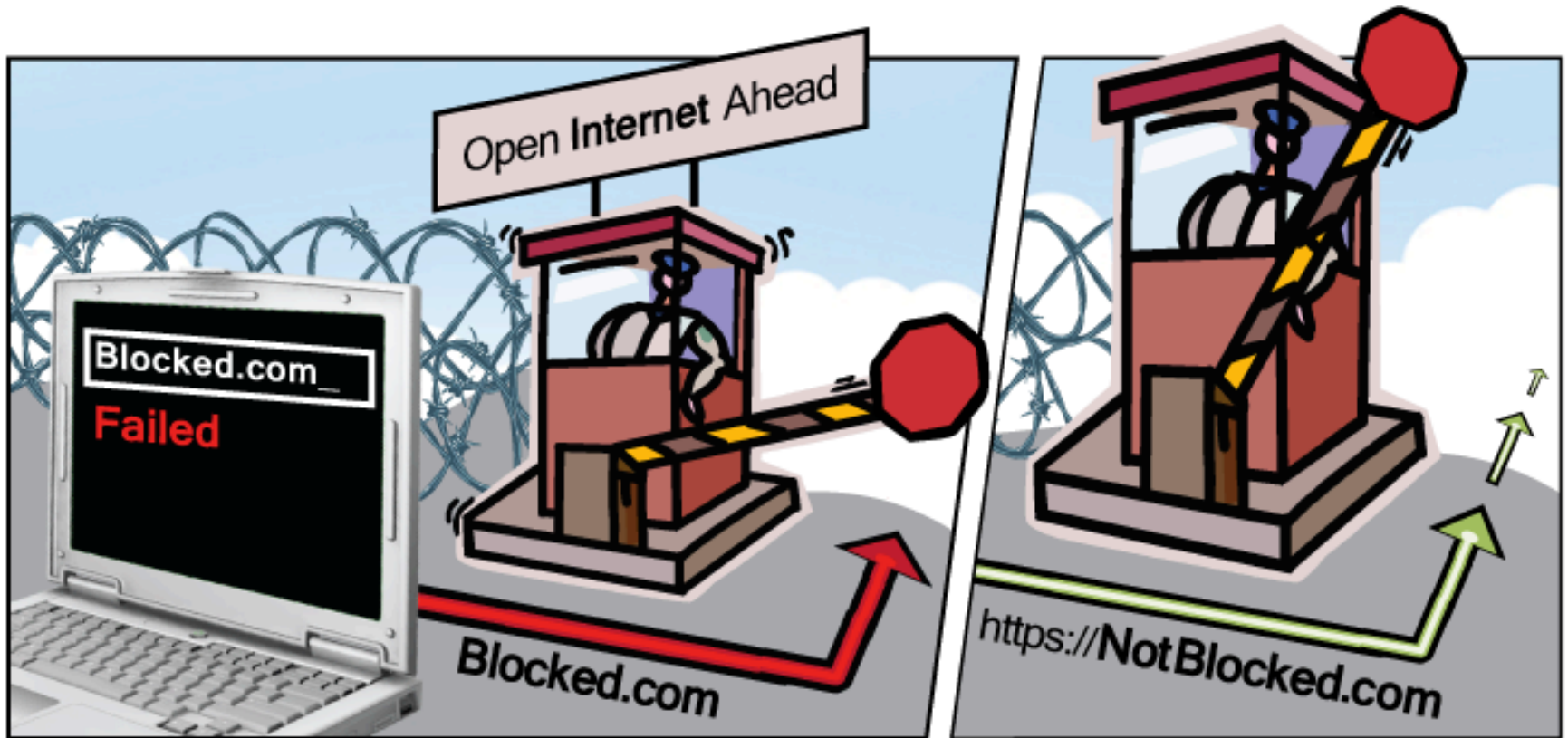
University of Michigan

Background | Internet Censorship



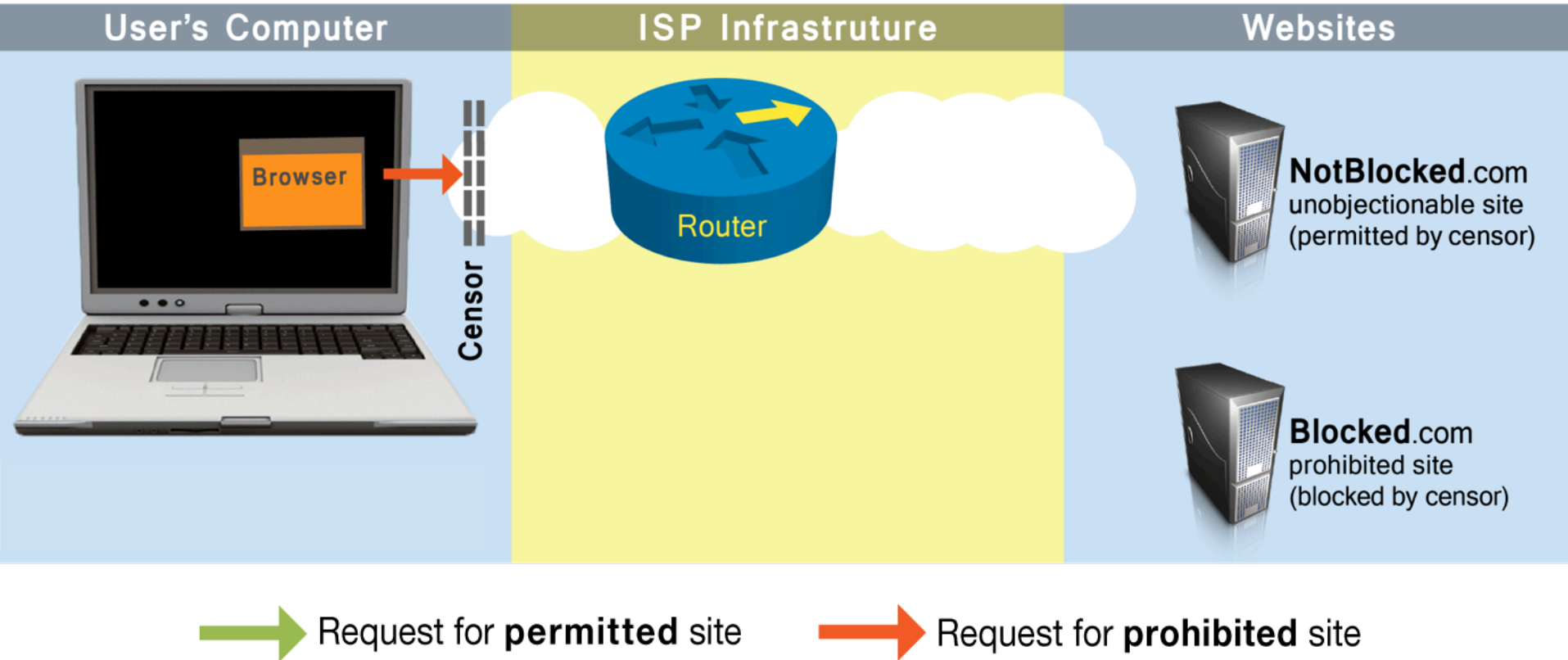
- Pervasive censorship
- Substantial censorship
- Selective censorship
- Changing situation
- Little or no censorship

Threat Model

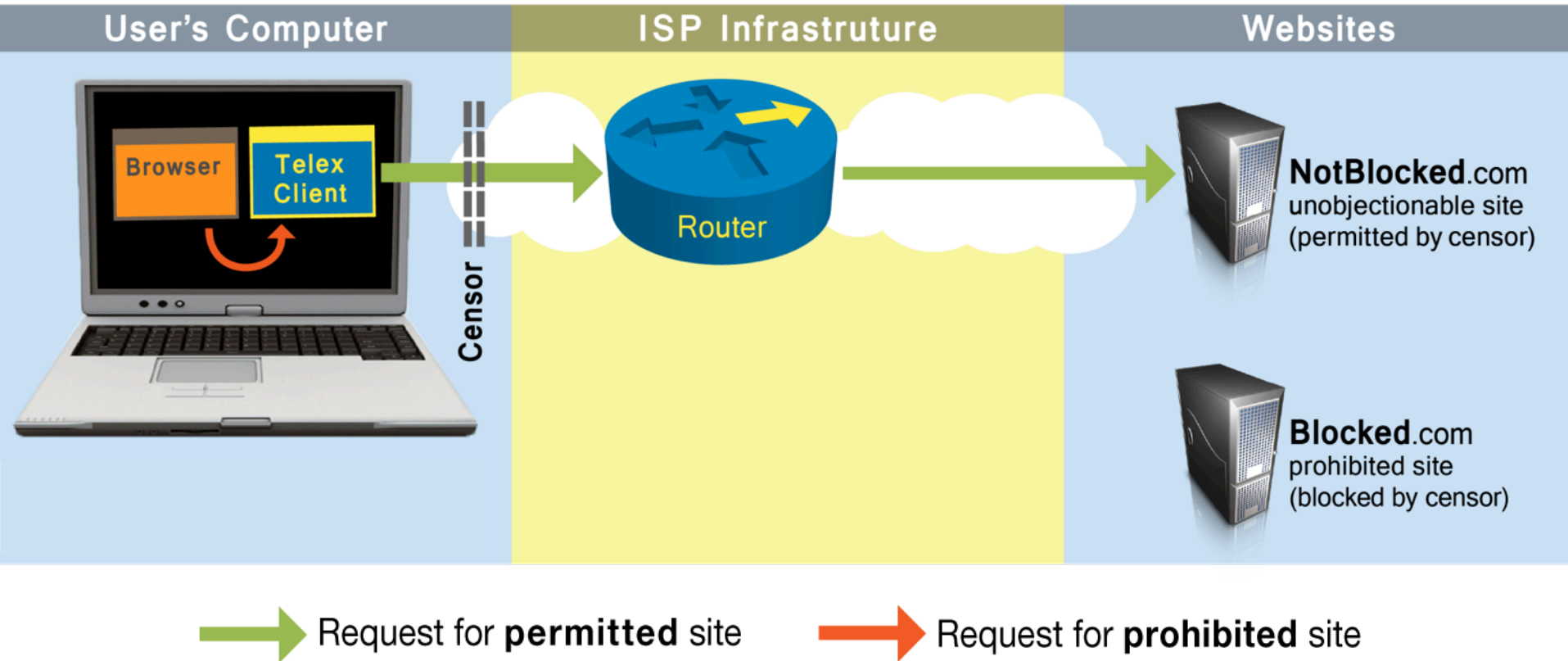


Censor ... controls client's network, but not external network
... blocks according to a blacklist
... allows HTTPS connections to non-blocked sites

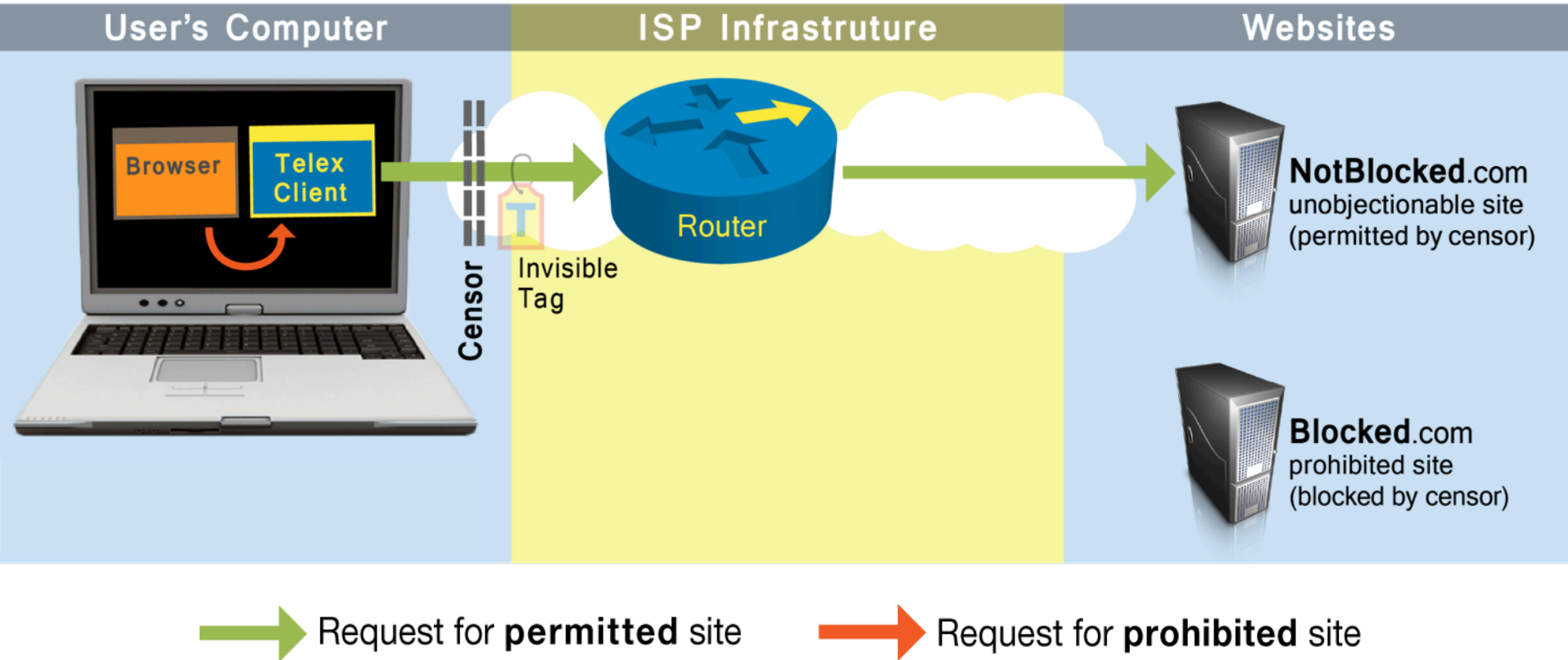
Telex | Overview



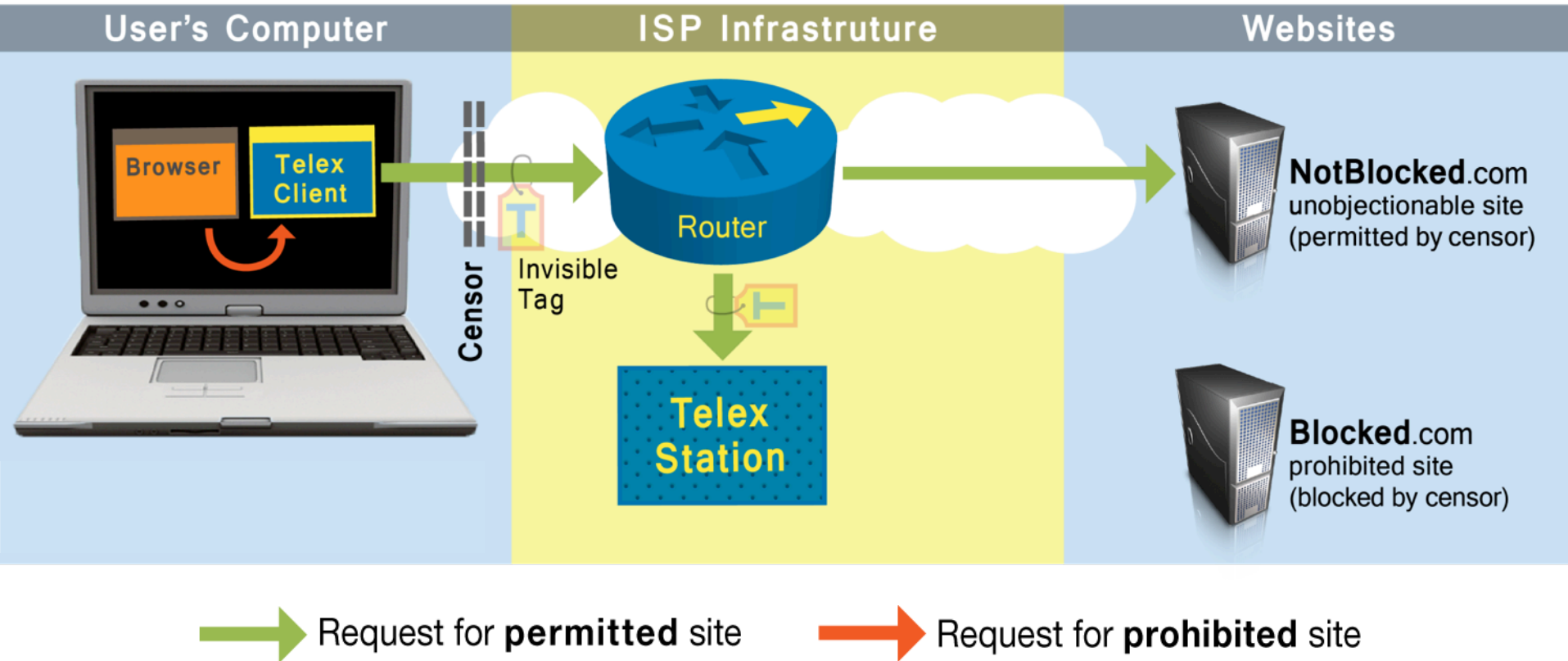
Telex | Overview



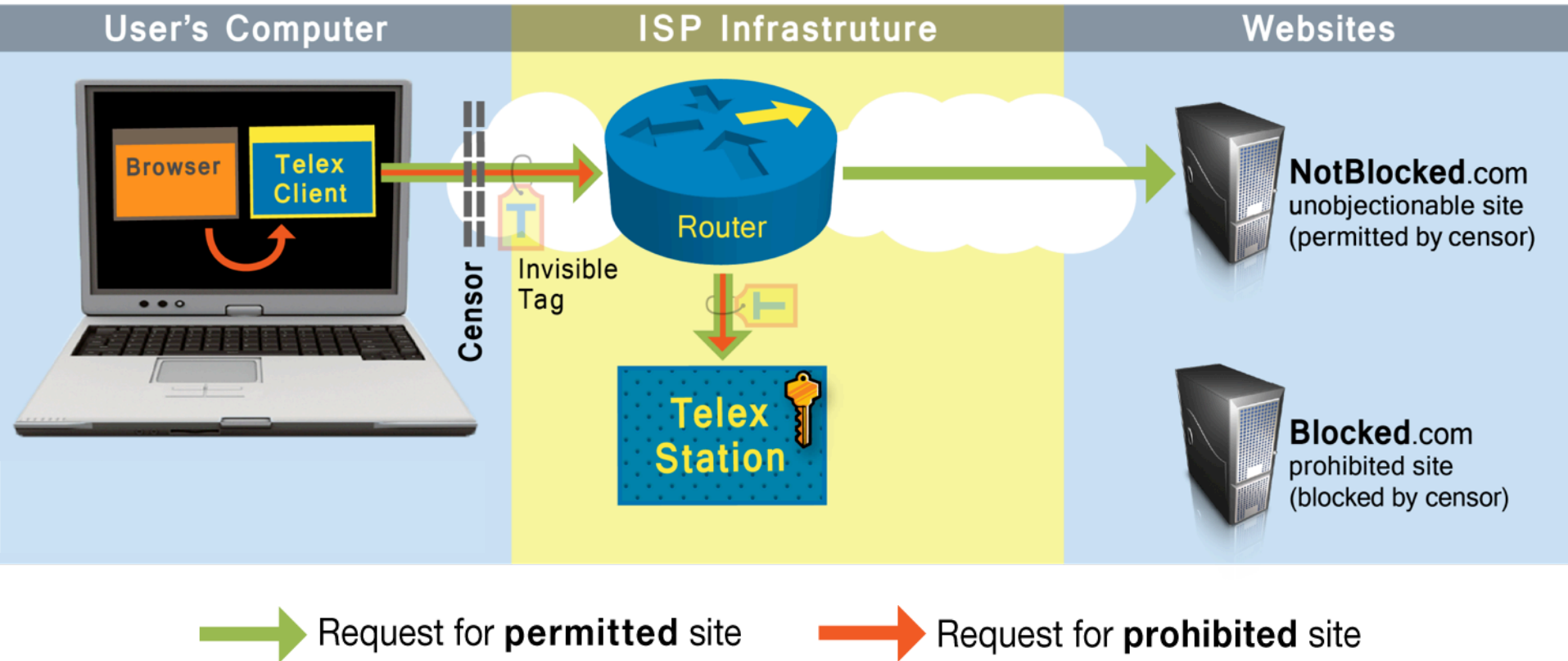
Telex | Overview



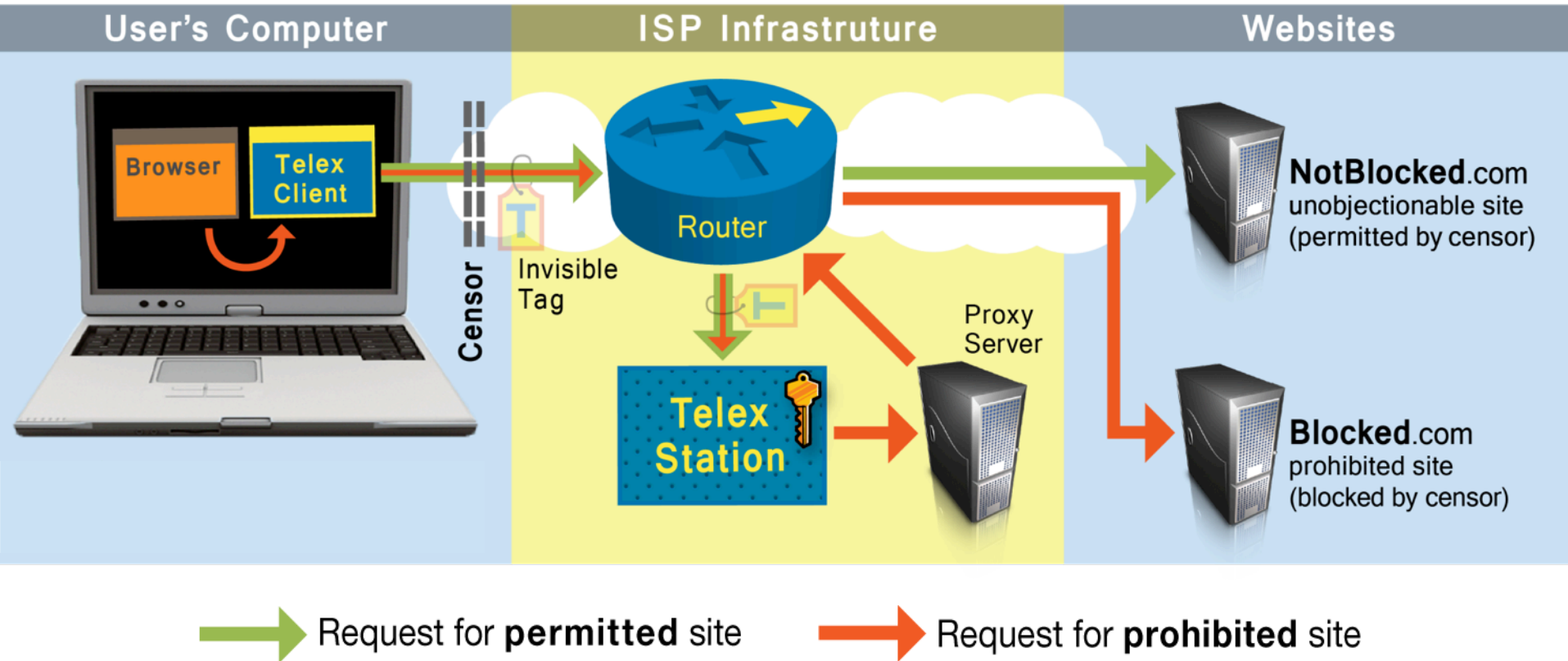
Telex | Overview



Telex | Overview



Telex | Overview



Prototype | Test Deployment

Single Telex Station on lab-scale “ISP” at Michigan

Hosted sites

NotBlocked.telex.cc

Unobjectionable content *

Blocked.telex.cc

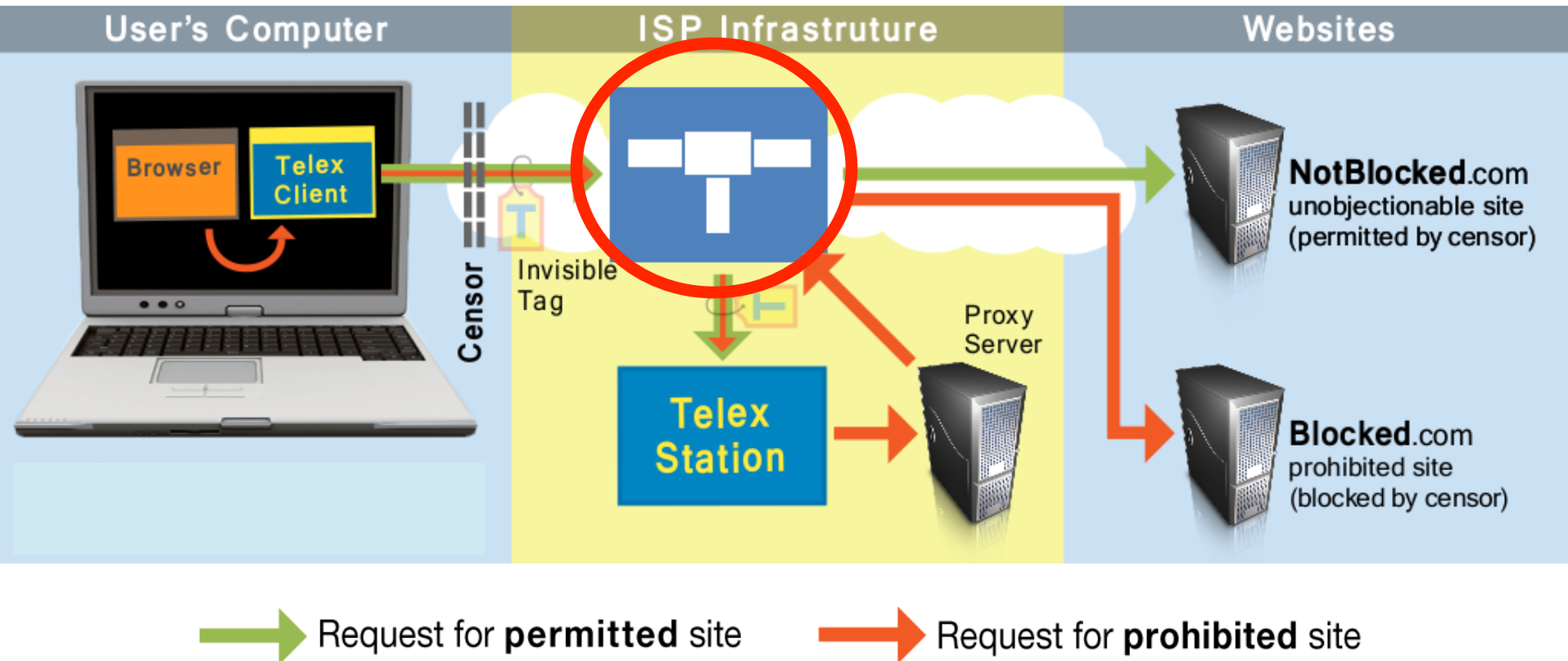
Simulated censored site
only reachable via Telex



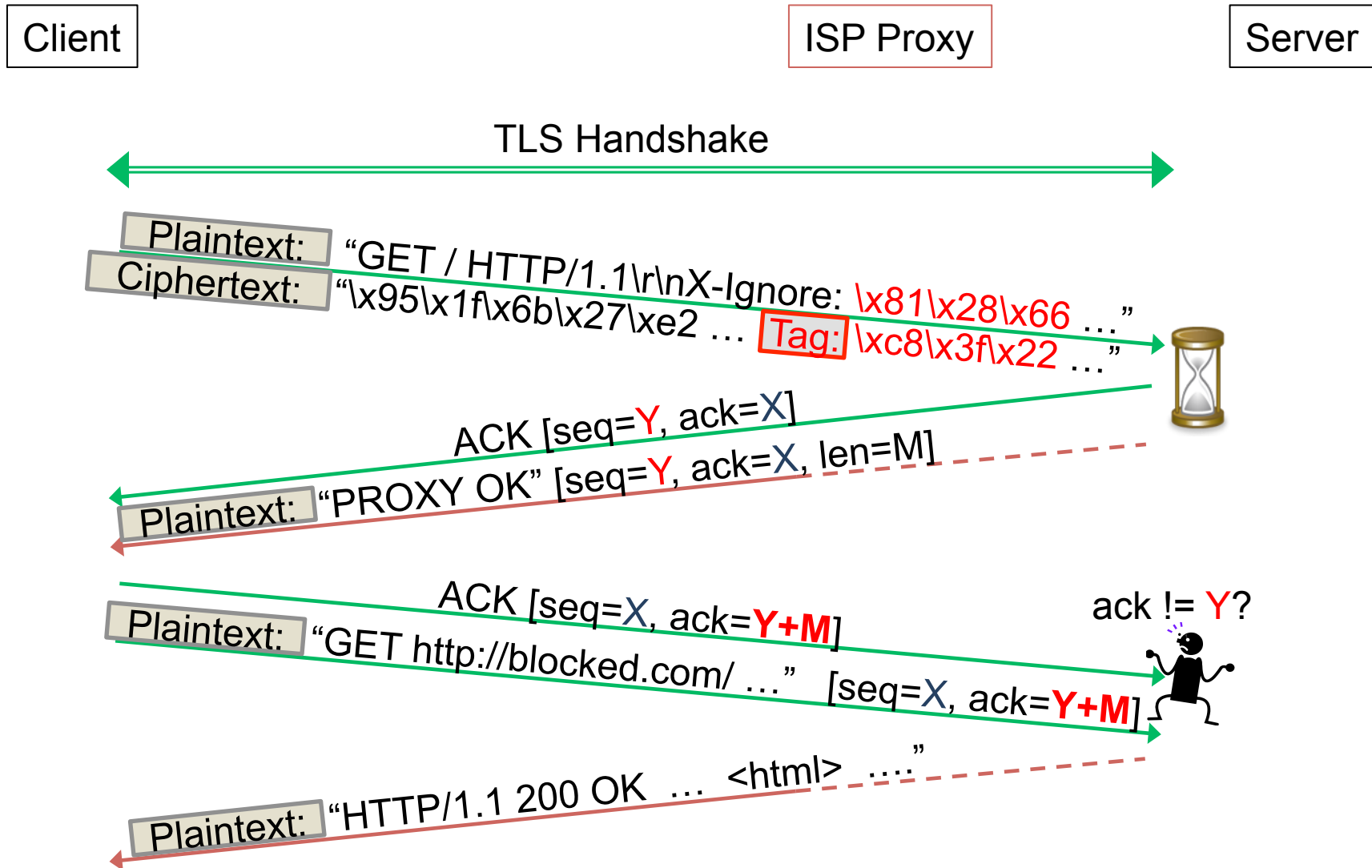
Inline Blocking
Asymmetric flows



Telex v2: Passive tap



New architecture -- passive ISP tap



New architecture -- passive ISP tap

- Pros
 - No inline blocking required, only passive tap
 - Works with asymmetric flows (client -> server)
- Cons
 - Censor can use active attacks
 - (though we can use “active defenses”)

Anticensorship in the Network Infrastructure

- Future work
 - Looking for ISPs willing to help
 - Technical feedback
 - Prototype deployment
 - Strategies for optimal deployment
 - Improving traffic analysis defense

Anticensorship in the Network Infrastructure

<https://telex.cc>

Eric Wustrow
Colleen M. Swanson
Scott Wolchok
Ian Goldberg
J. Alex Halderman