Parldigi Open Hearing, Bern, December 14, 2016

Internet Blocking: A Very Brief Technical Review

Prof. Dr. Burkhard Stiller, Dr. Thomas Bocek
Communication Systems Group CSG, Department of Informatics IfI
University of Zürich UZH
[stiller¦bocek]@ifi.uzh.ch

in collaboration with ***Prof. Dr. Florent Thouvenin, Kento Reutimann***
Rechtswissenschaftliches Institut der UZH
Lehrstuhl für Informations- und Kommunikationsrecht

Universität Zürich[UZH]

Blocking 1
Bypassing 2
Observations 3

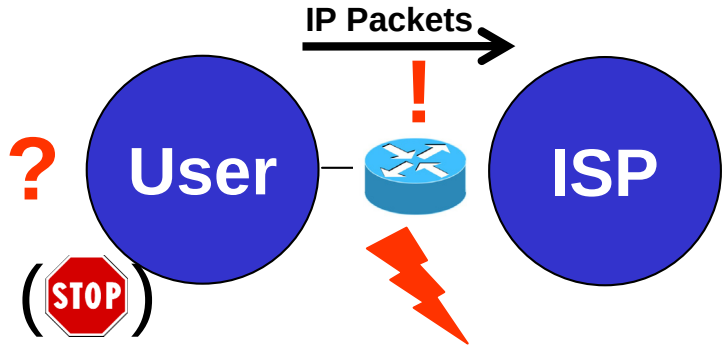
CSG Communication Systems Group

ifi

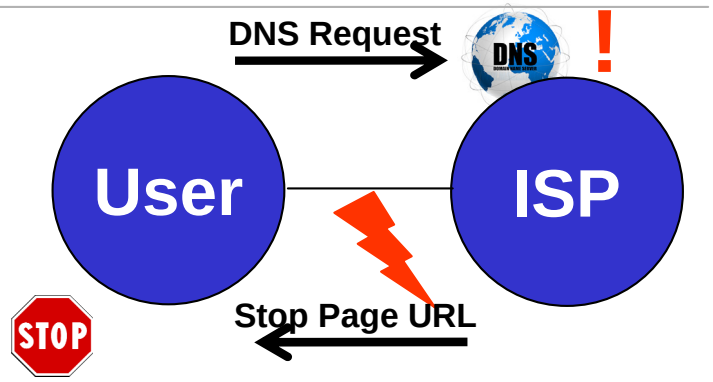
Blocking Alternatives

Major Examples

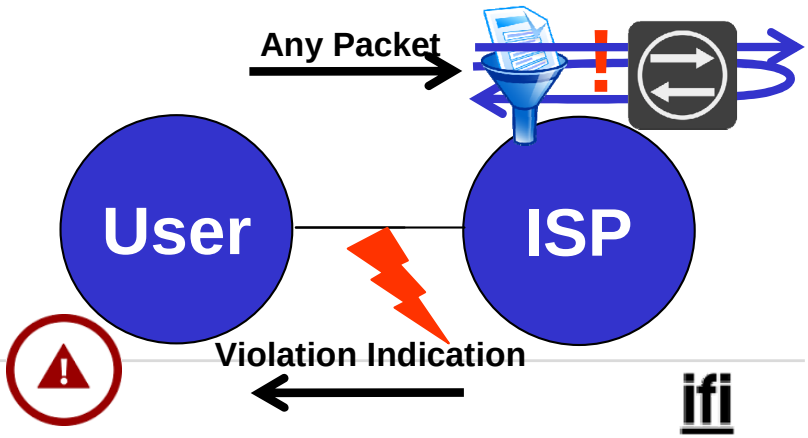
- ISP-based IP Address Blocking
  - Operates on the IP protocol level
  - ISP maintains IP address lists
  - Users (typically) not informed



- ISP-based DNS Blocking
  - Operates on DNS requests (*e.g.*, browsers)
  - ISP maintains DNS name lists
  - Users can potentially be informed



- ISP Application Filters/ Proxy Servers
  - Operates on interpreted content
  - Users can potentially be informed



✘ Blocking not effective
✔ Blocking (partially) effective

Bypassing

Countermeasures	Blocking Approach: IP	Blocking Approach: DNS	Blocking Approach: Filter/ Proxy	Applicability: User	Reaction: ISP
Anonymization of user traffic (Tor)	✘	✘	✘	easy	difficult
Encrypted transmissions (*e.g.* HTTPS)	ESP/AH ✘/✔	✘	✘	easy	governmental certificate
Use of “public” DNS server (not ISP’s)	✔	✘	✔	easy	learning (IP Blocking)
Virtual Private Networks (VPN)	✘	✘	✘	easy	difficult
Content Distribution Networks (CDN)	✘	✘	✘	possible	difficult
Adaptation of user’s sending behavior	✔	✔	-/DPI (✘/✔)	cumber-some	learning
Changing DNS names/IP addresses	before/after ✔/✘	before/after ✔/✘	-/DPI (✘/✔)	cumber-some	learning
Use of IP addresses directly	✔	✘	✔	possible	learning (IP Blocking)

Observations

- Blocking is technically possible
  - Browser and DNS traffic considered here as simpler examples
  - Different traffic types need (partially) different handling
- Technical ISP efforts differ, but are costly
  - Maintenance of to be blocked IP addresses, DNS entries, URLs
    - Data base? Procedures for entering/deleting/changing? Redressing?
  - During operations: loss of “fast path” router capabilities
- Any such blocking can be circumvented legally by technically lower-skilled users (lower user efforts)
  - *E.g.*, Tor, VPN, encryption manuals widely available (Internet)