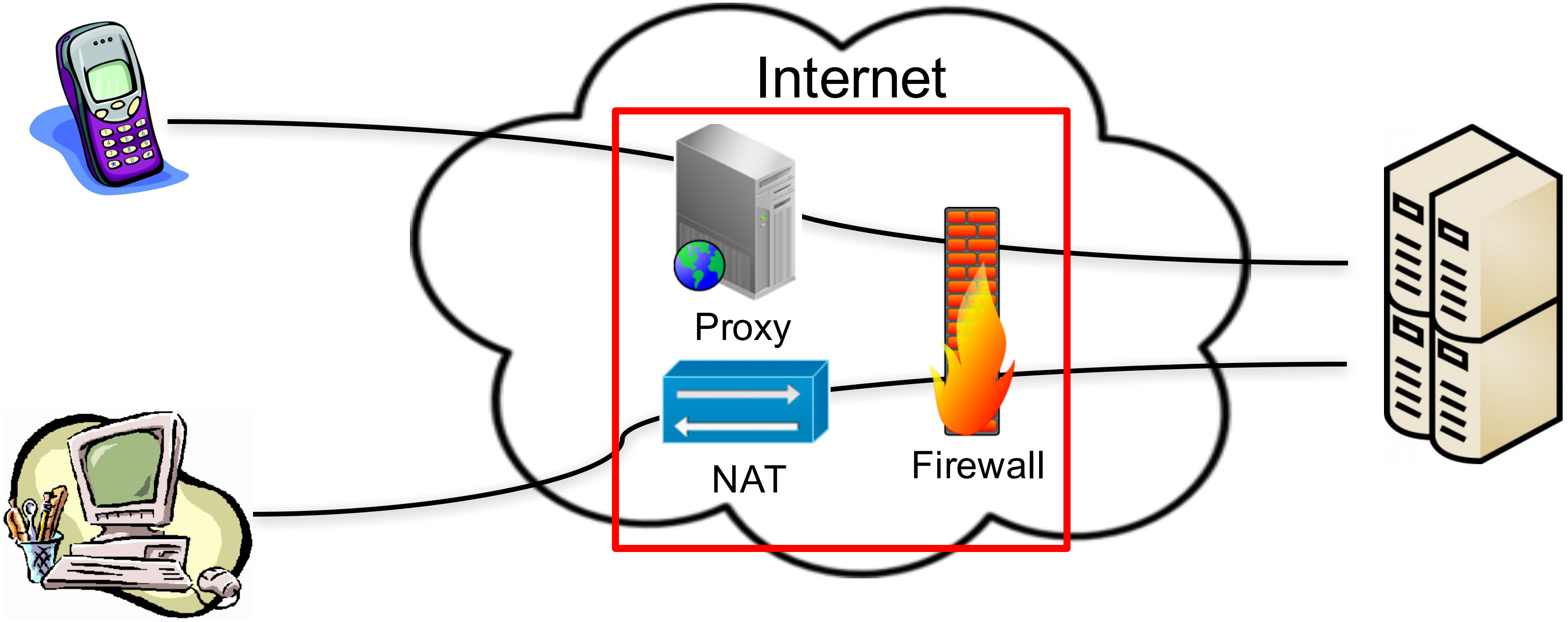
Detecting Middlebox Interference on Applications

Shan Huang

Félix Cuadrado and Steve Uhlig

Queen Mary
University of London

Introduction



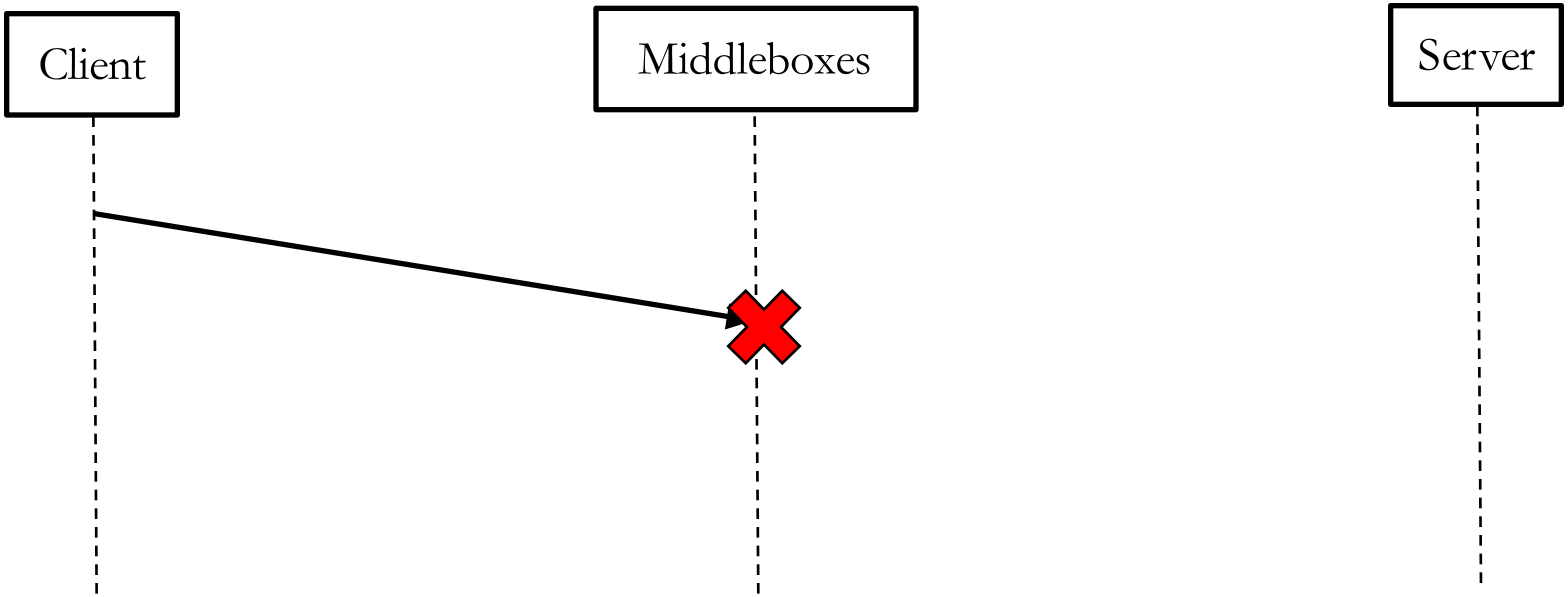
End hosts

Middleboxes

End hosts

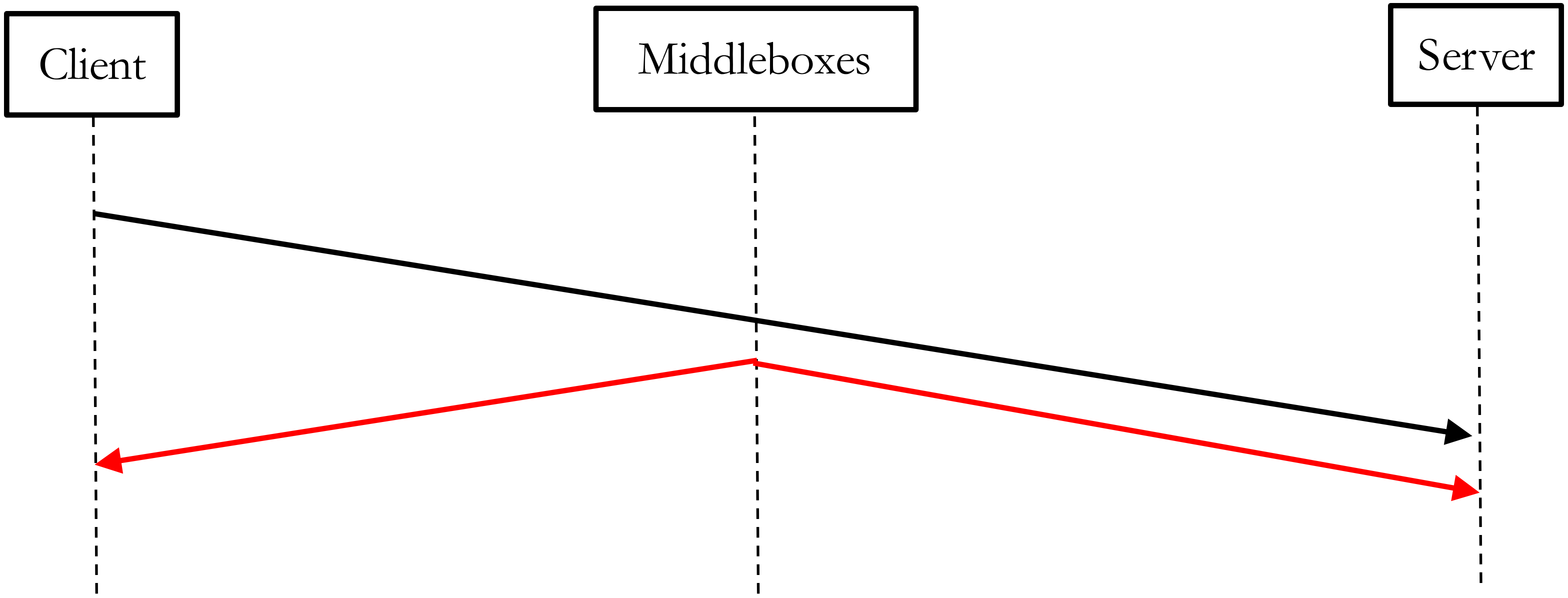
Introduction

- Middlebox interference --- Filtering



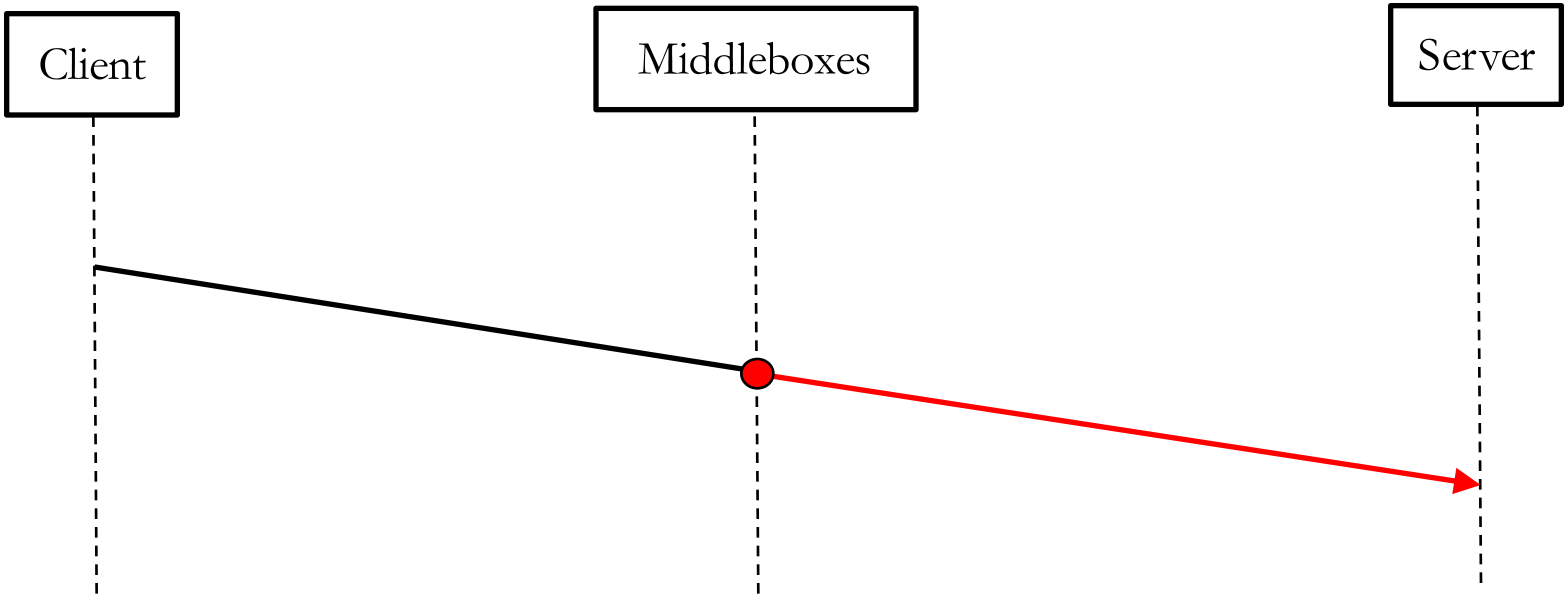
Introduction

- Middlebox interference --- Injection



Introduction

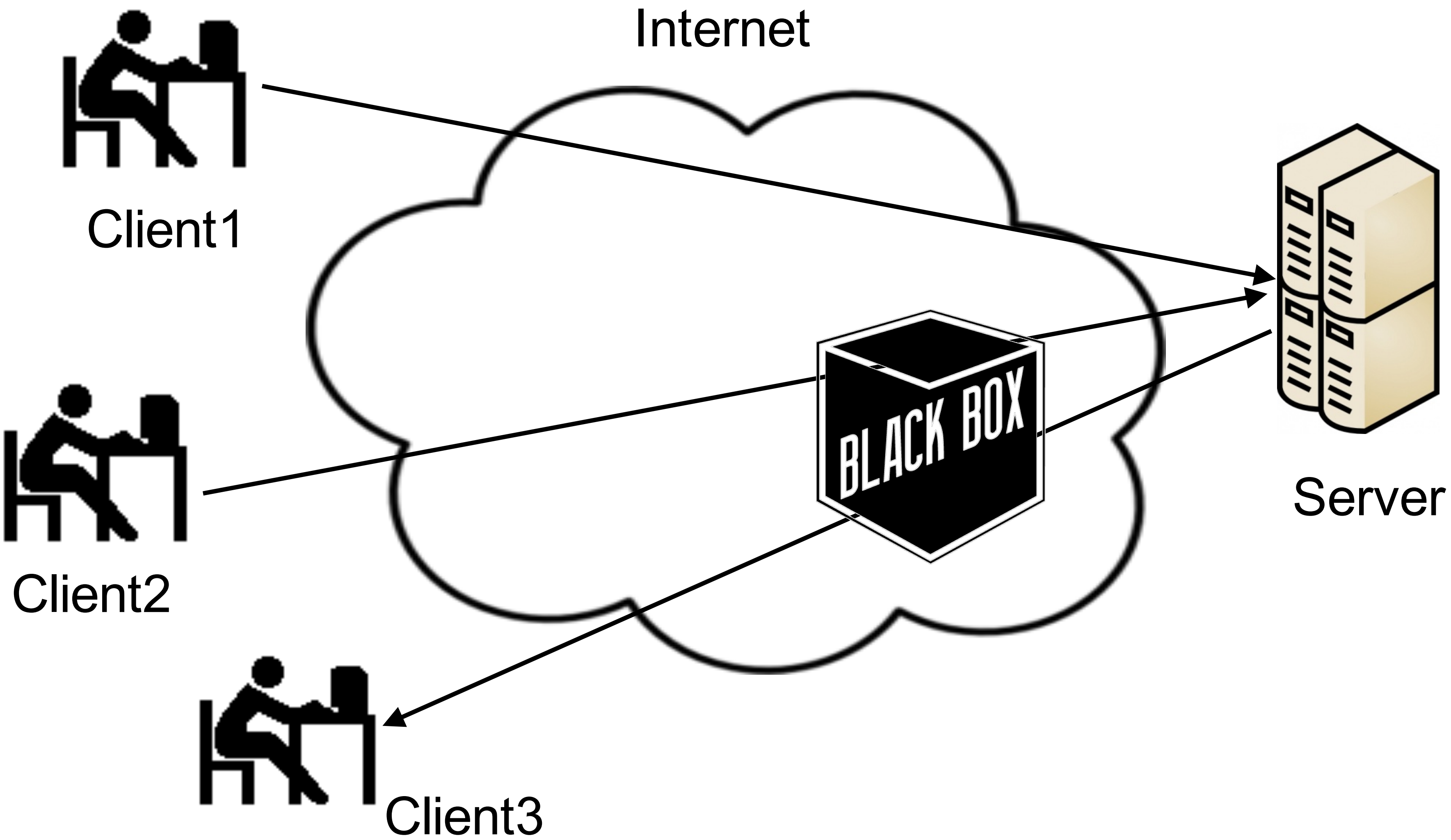
- Middlebox interference --- Modification



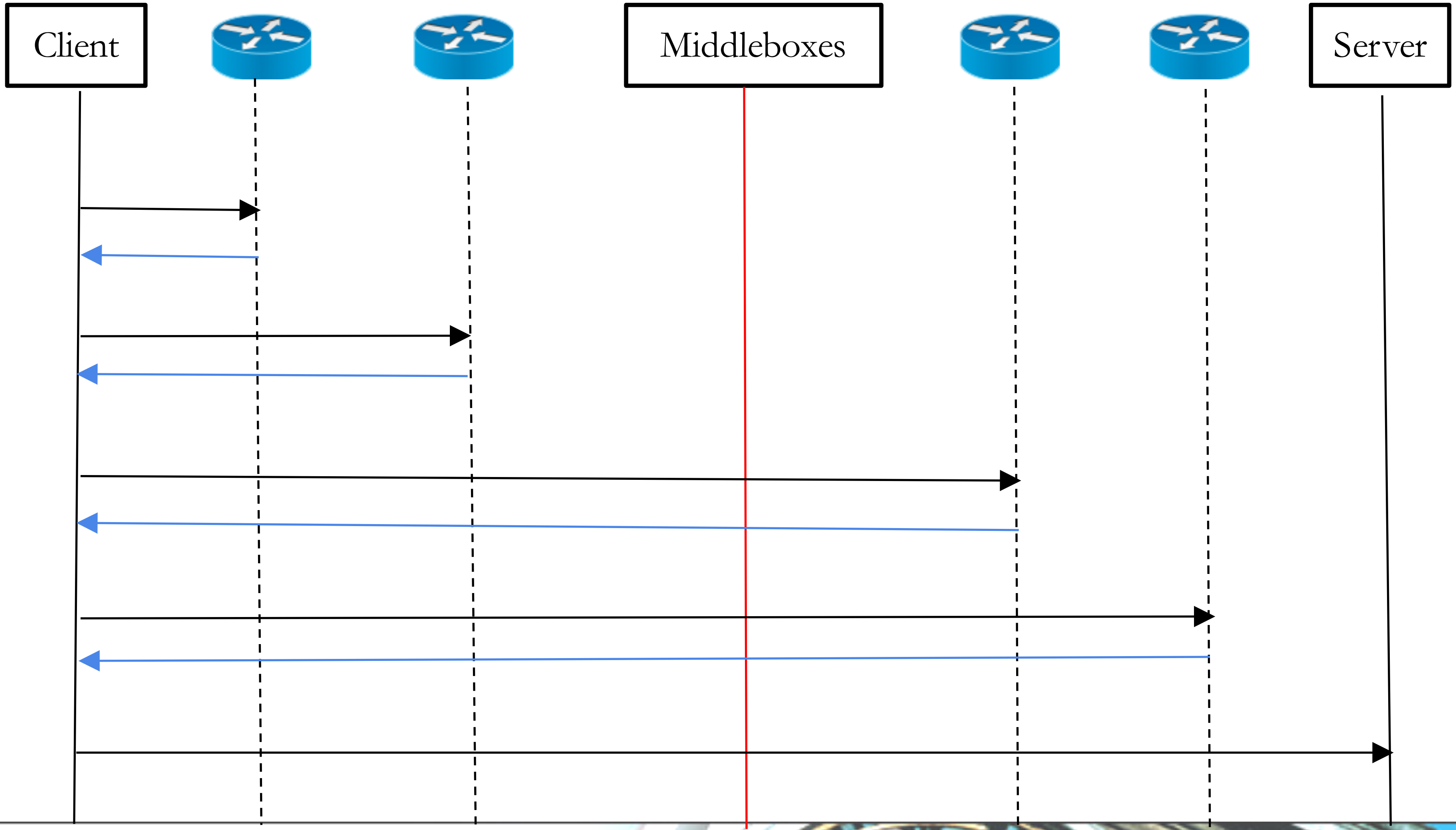
Goal

Develop a system to detect and locate any middlebox interference on applications.

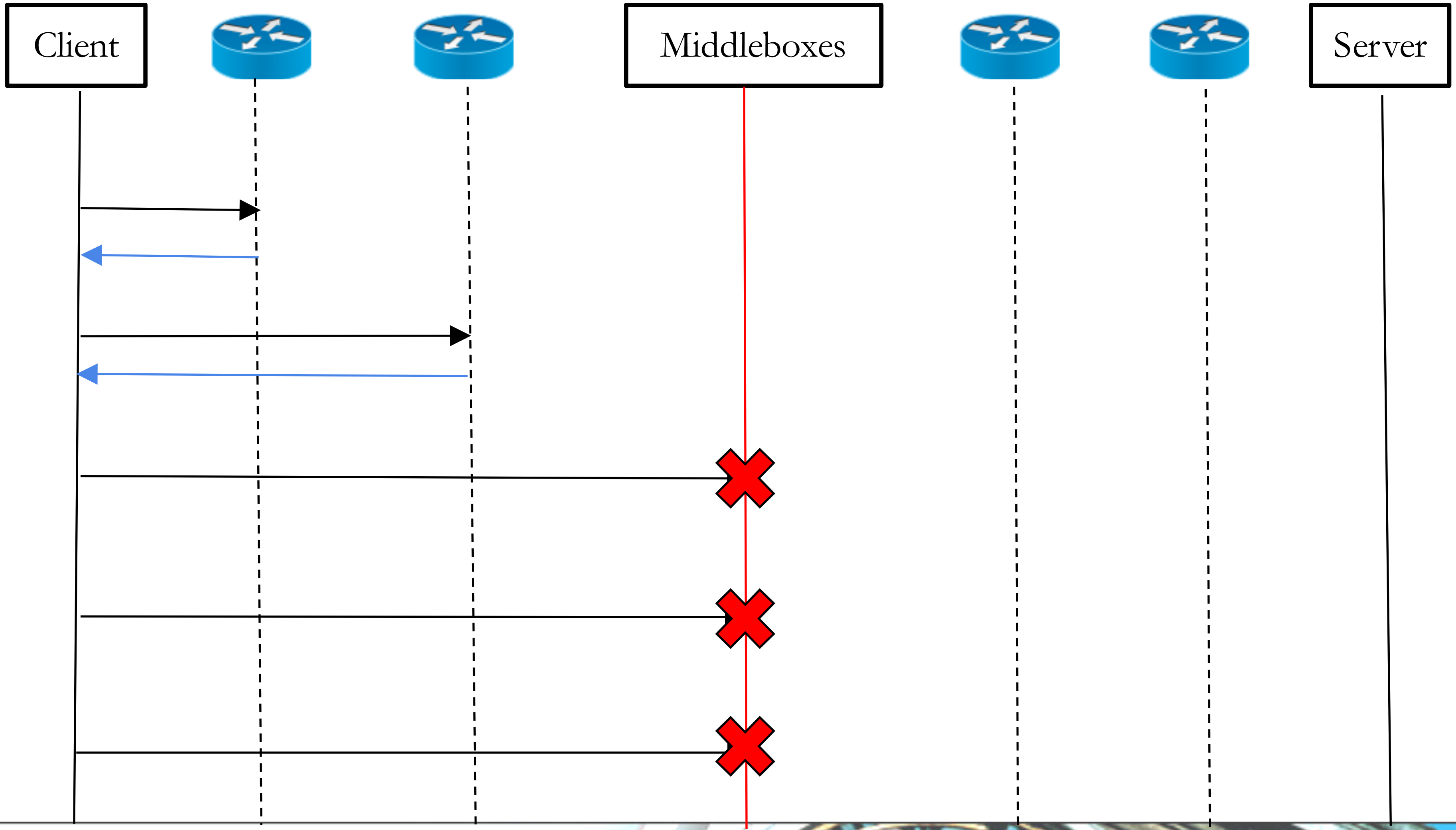
Methodology



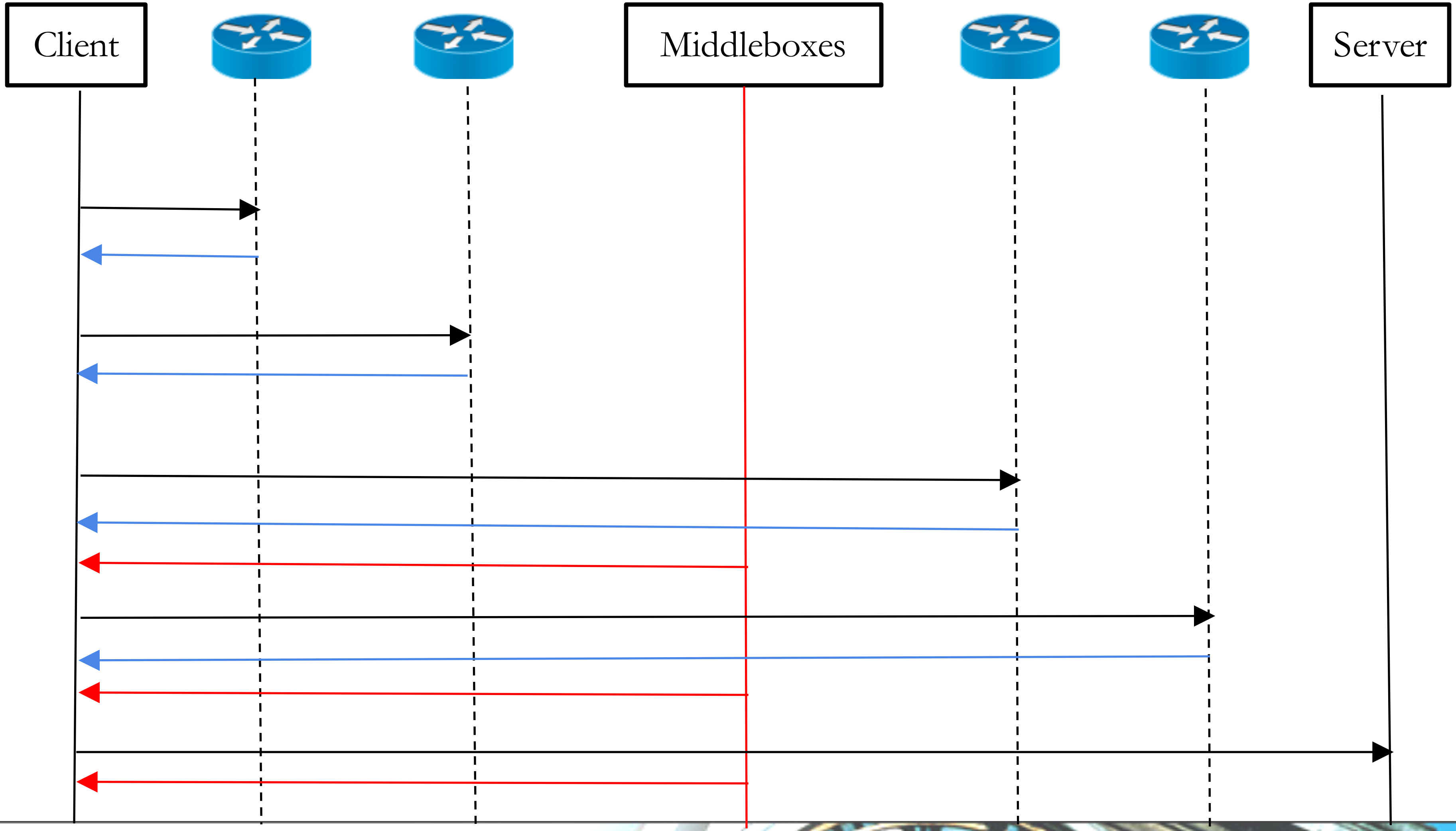
Methodology



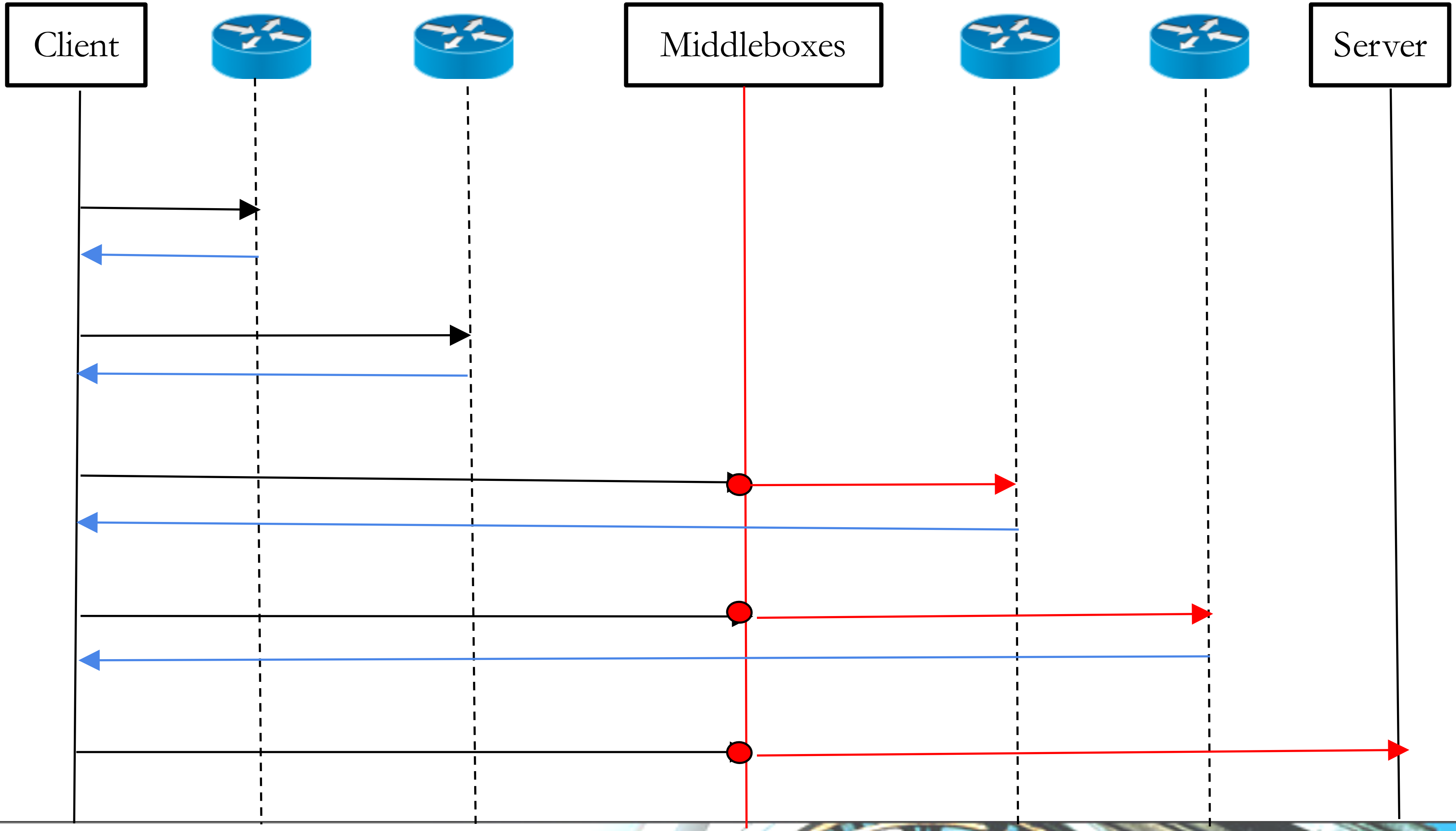
Methodology



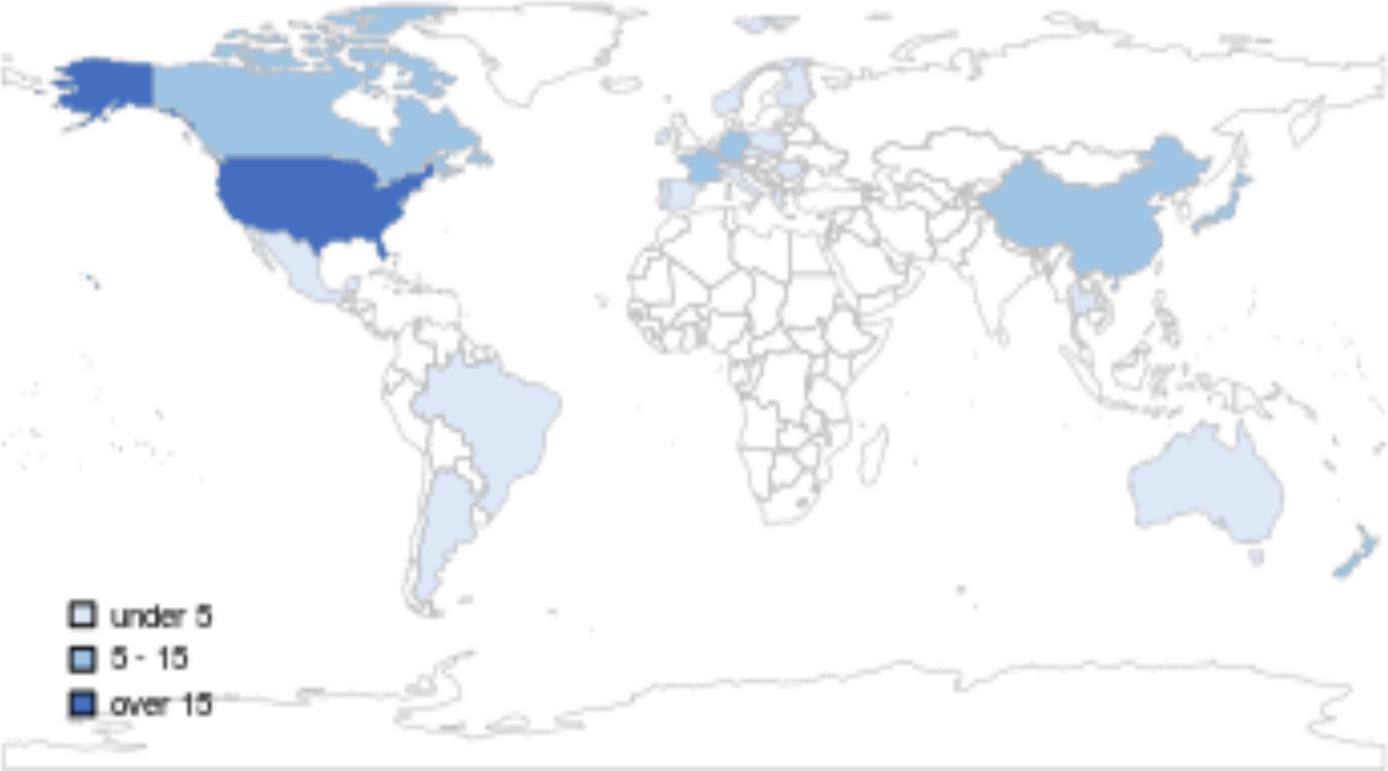
Methodology



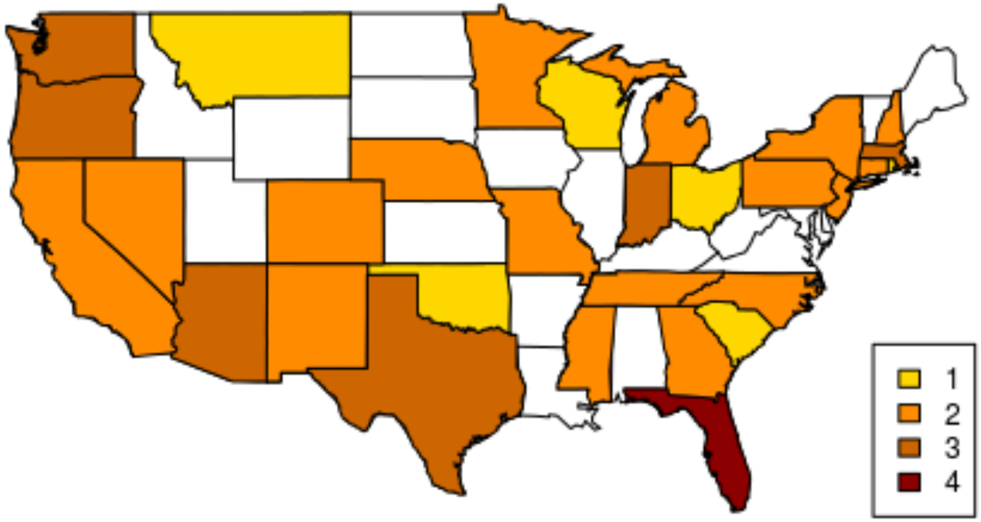
Methodology



Open platform --- PlanetLab



- 152 available PlanetLab nodes
- 28 countries



- 52 available PlanetLab nodes
- 25 states of USA

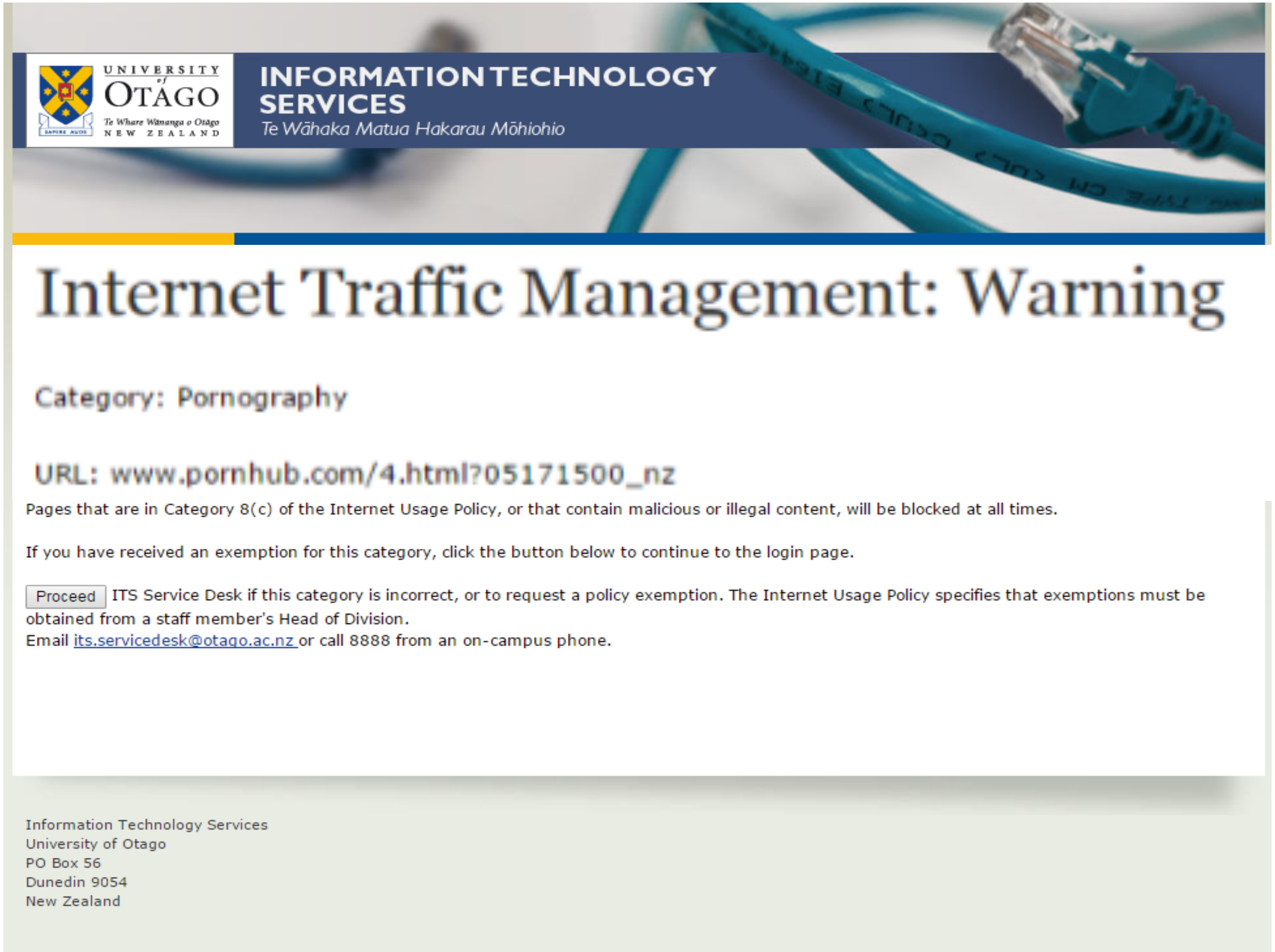
HTTP header manipulation

- National University of Singapore

  HTTP header is manipulated by college proxy.

	Injected HTTP header	Modified HTTP header
Request	X-Forwarded-For Via Connection	Cache-Control
Response	Via Connection	

Injected warning page



UNIVERSITY of OTAGO
Te Whare Wānanga o Otāgo
NEW ZEALAND
INFORMATION TECHNOLOGY SERVICES
Te Wāhaka Matua Hakarau Mōhiohio

Internet Traffic Management: Warning

Category: Pornography

URL: www.pornhub.com/4.html?05171500_nz

Pages that are in Category 8(c) of the Internet Usage Policy, or that contain malicious or illegal content, will be blocked at all times.

If you have received an exemption for this category, click the button below to continue to the login page.

Proceed ITS Service Desk if this category is incorrect, or to request a policy exemption. The Internet Usage Policy specifies that exemptions must be obtained from a staff member's Head of Division.
Email its.servicedesk@otago.ac.nz or call 8888 from an on-campus phone.

Information Technology Services
University of Otago
PO Box 56
Dunedin 9054
New Zealand

Internet censorship in China

- The Great Firewall of China (GFC) injects fake DNS responses to restrict access to domain names.

- The HTTP request with censored host name triggers GFC injects TCP reset packet to both client and server sides.

Future work

- PlanetLab is primary testbed for large-scale measurements

  We would like to use other platform to launch queries from all over the world.

- Other effect on application behaviour

  Whether the middleboxes affect query latency?
  Where the middlebox interference occurs? Close to client ?
  Or close to server?

Questions?
Thanks

Reference

[1] Justine Sherry, Shaddi Hasan, Colin Scott,Arvind Krishnamurthy, Sylvia Ratnasamy, and Vyas Sekar. Making middleboxes someone else’s problem: network processing as a cloud service. In *Proc. ACM SIGCOMM*, 2012.