Great Firewall of China

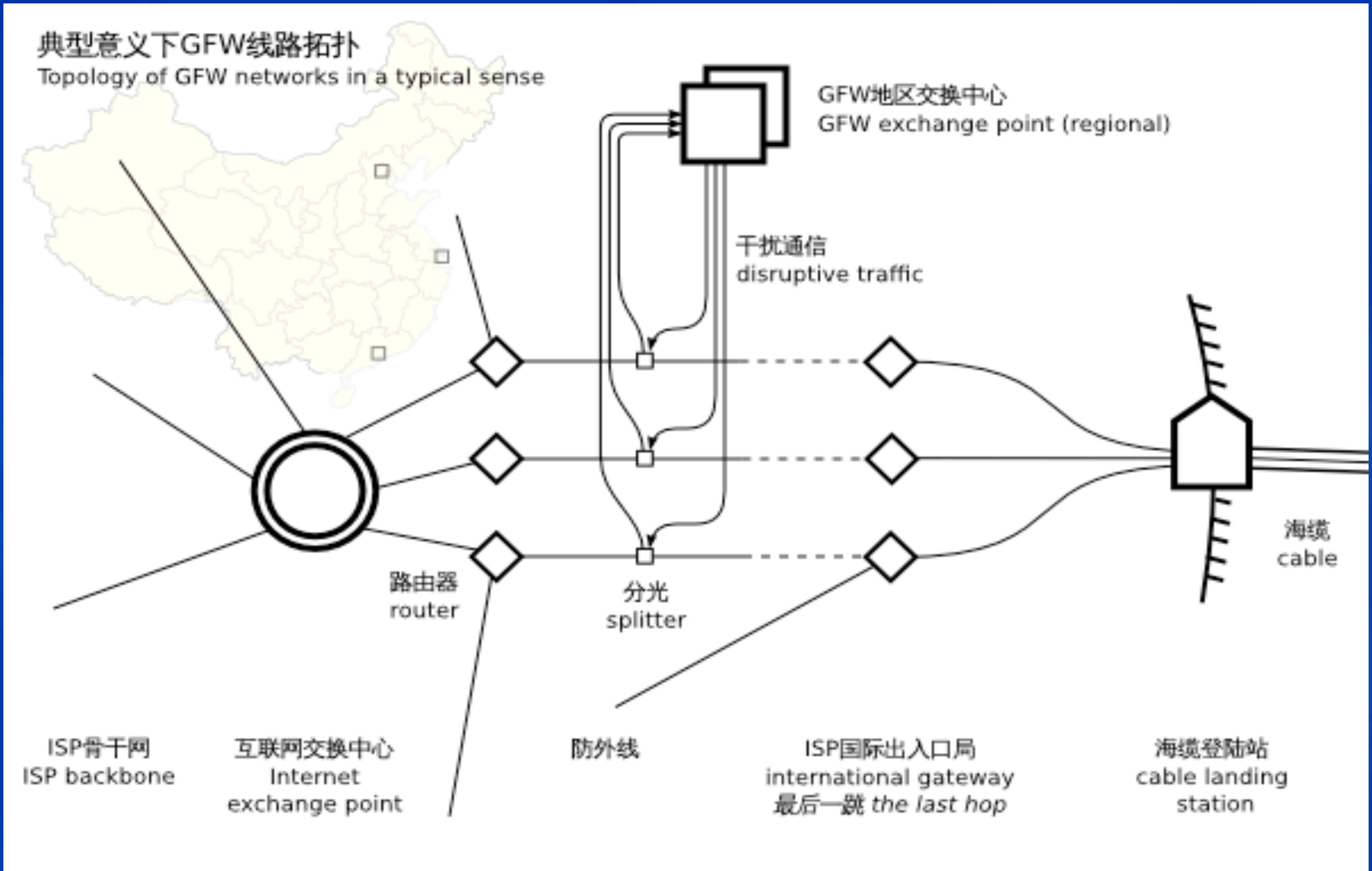
Yipeng Zhang
4/16/2012

What is GFW?

- The Great Firewall of China

  Charles R. Smith
  Friday, May 17, 2002
- It’s a Firewall
- Hardware: Intrusion Detection System - CISCO
- Software: Hundreds of Chinese company

Where is GFW?



典型意义下GFW线路拓扑
Topology of GFW networks in a typical sense
GFW地区交换中心
GFW exchange point (regional)
干扰通信
disruptive traffic
路由器
router
分光
splitter
海缆
cable
ISP骨干网
ISP backbone
互联网交换中心
Internet
exchange point
防外线
ISP国际出入口局
international gateway
最后一跳 the last hop
海缆登陆站
cable landing
station

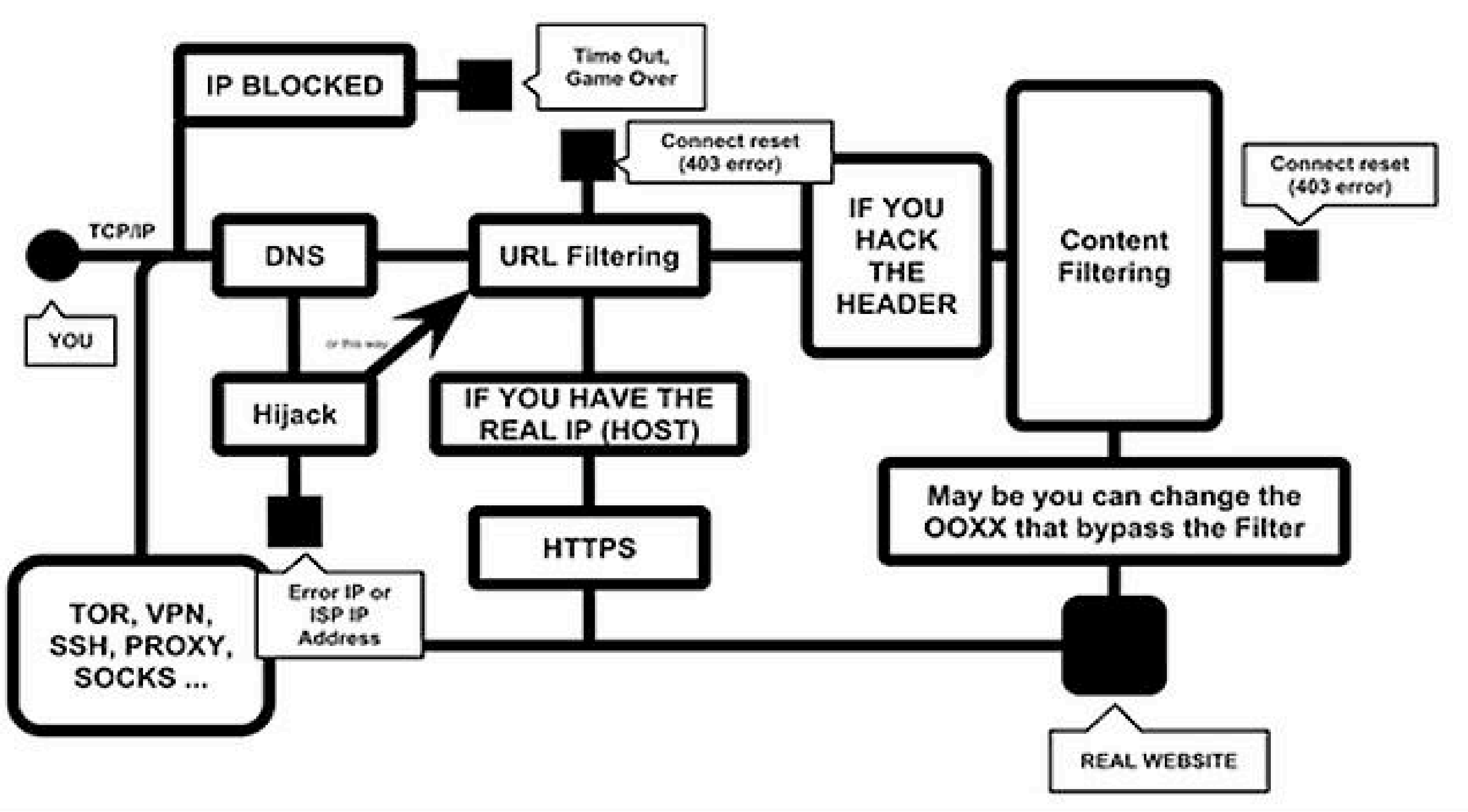
What can GFW do?

- Censor all Chinese Internet traffic
- Make certain webpage unavailable to Chinese and Internet users
- Record all your activities on Internet(at least 2 years)
- Protect Chinese website from DDOS

Target of GFW

- Almost every website with “User Generate Content”, twitter, flickr, blog
- All the information about Chinese government ,
- Chinese Communist Party, even Leader’s name or anything sounds and looks like their name
- National security
- Etc. Basically anything Chinese government don’t want you to know

How Chinese use Internet


IP BLOCKED
Time Out, Game Over
Connect reset (403 error)
TCP/IP
YOU
DNS
URL Filtering
IF YOU HACK THE HEADER
Content Filtering
Connect reset (403 error)
or this way
Hijack
IF YOU HAVE THE REAL IP (HOST)
HTTPS
May be you can change the OOXX that bypass the Filter
TOR, VPN, SSH, PROXY, SOCKS ...
Error IP or ISP IP Address
REAL WEBSITE

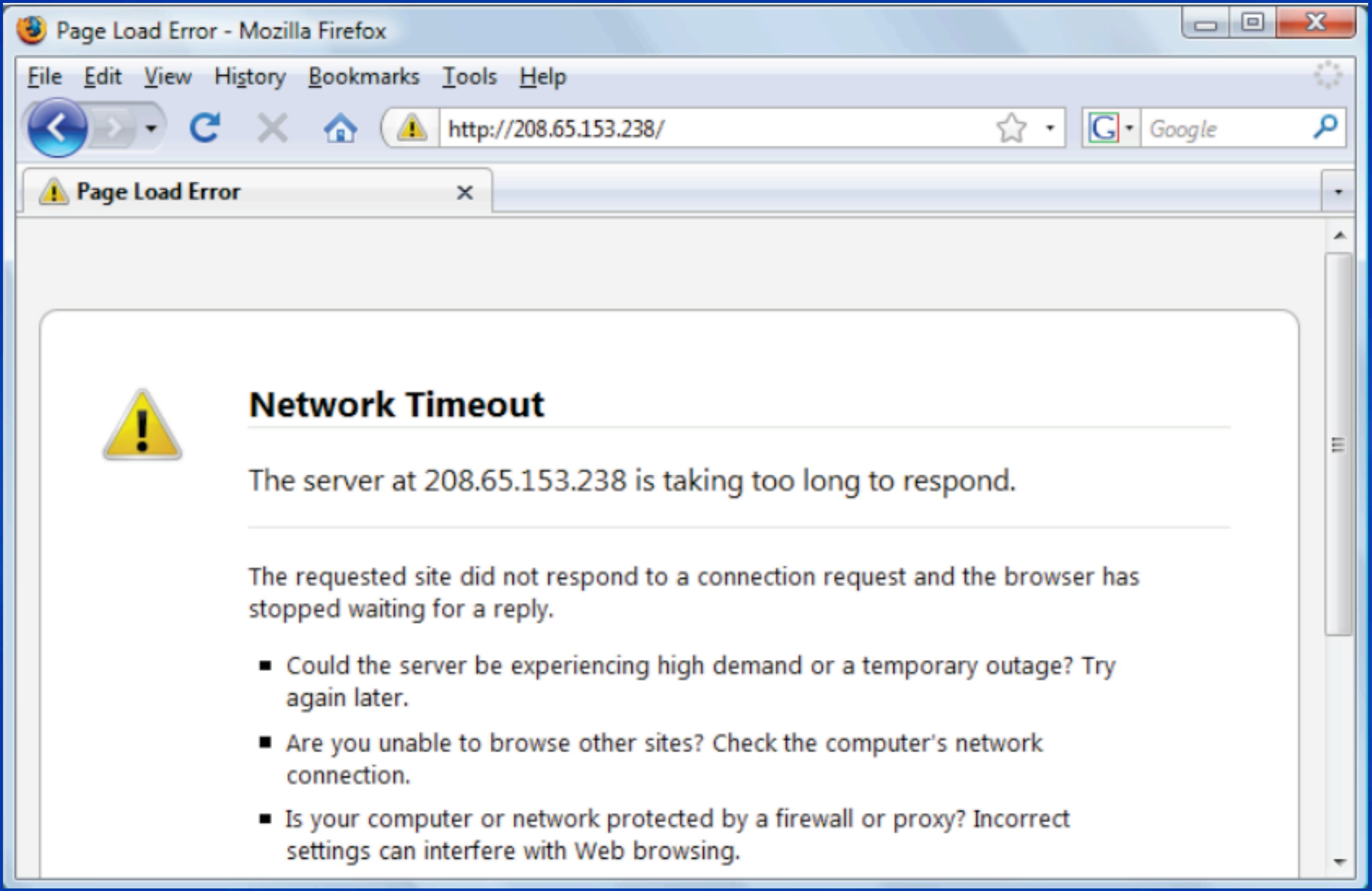
Route of the GFW - This is our Internet (China)

by J.T use Google Docs

What weapons does GFW have?

- IP Blocking
- DNS filtering and redirection
- URL filtering
- Packet filtering
- Connection reset
- SSL certificate filtering
- Fake Tor node and filtering

IP Blocking



Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://208.65.153.238/
Google
Page Load Error

Network Timeout

The server at 208.65.153.238 is taking too long to respond.

The requested site did not respond to a connection request and the browser has stopped waiting for a reply.

- Could the server be experiencing high demand or a temporary outage? Try again later.
- Are you unable to browse other sites? Check the computer's network connection.
- Is your computer or network protected by a firewall or proxy? Incorrect settings can interfere with Web browsing.

IP Blocking

- Simple
- /etc/hosts.deny
- Facebook twitter youtube

Three Principles of GFW

- 1. Any website with User-generated content, UGC, may all be blocked by GFW

  facebook, twitter, youtube
- 2. For all the blocked website, there is a clone version in china.

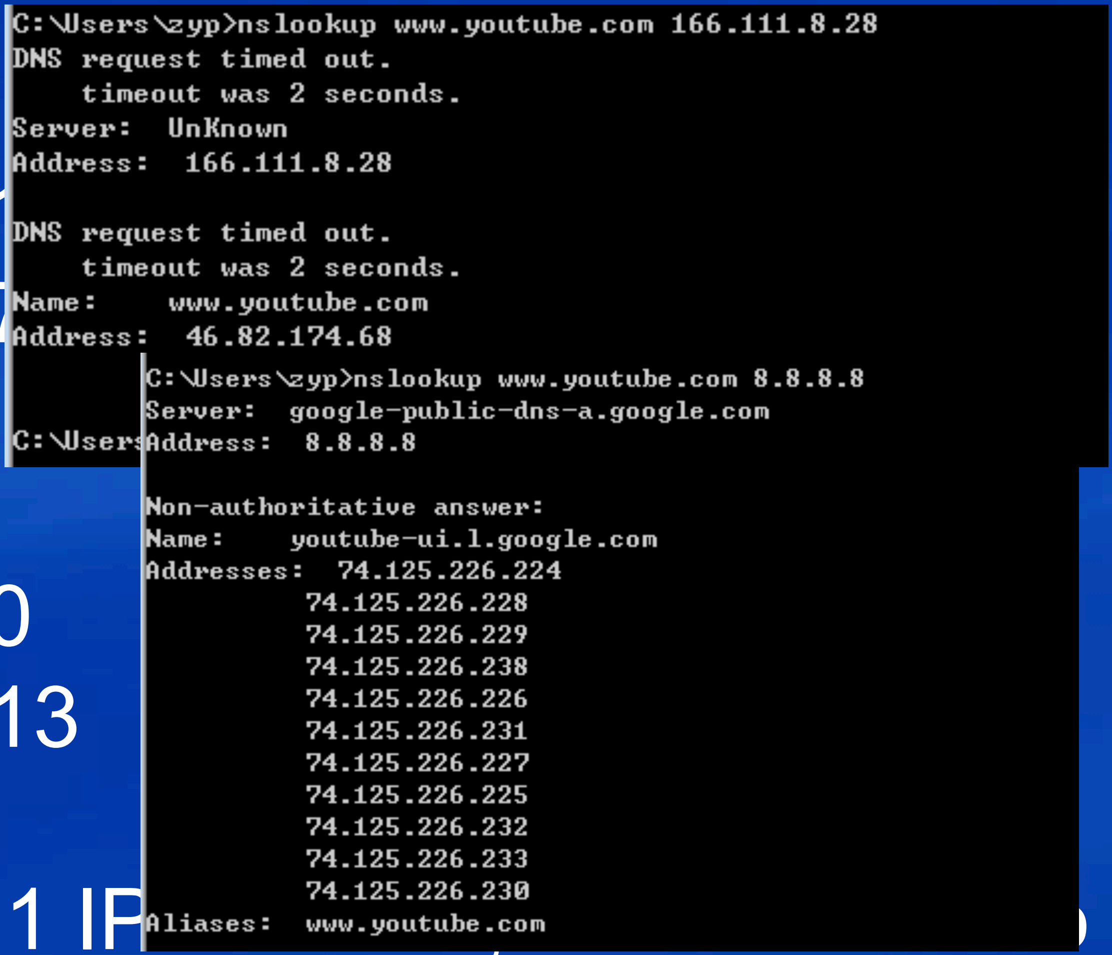
  Renren as facebook, weibo as twitter,
youku as
  youtube
- 3. If you are qualified for the principle 1, and still not blocked by GFW, you are not the best.

IP Blocking – BREAK IT!

- Every now and then, twitter or youtube will add some new IP address.
- VPN/TOR/SSH etc
- Proxy

DNS filtering and redirection

4.36.66.178
203.161.230.1
211.94.66.147
202.181.7.85
202.106.1.2
209.145.54.50
216.234.179.13
64.33.88.161
……(why not 1 IP ,)
DDOS)



```
C:\Users\zyp>nslookup www.youtube.com 166.111.8.28
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  166.111.8.28

DNS request timed out.
    timeout was 2 seconds.
Name:    www.youtube.com
Address:  46.82.174.68

C:\Users
```

```
C:\Users\zyp>nslookup www.youtube.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    youtube-ui.l.google.com
Addresses:  74.125.226.224
          74.125.226.228
          74.125.226.229
          74.125.226.238
          74.125.226.226
          74.125.226.231
          74.125.226.227
          74.125.226.225
          74.125.226.232
          74.125.226.233
          74.125.226.230
Aliases:  www.youtube.com
```

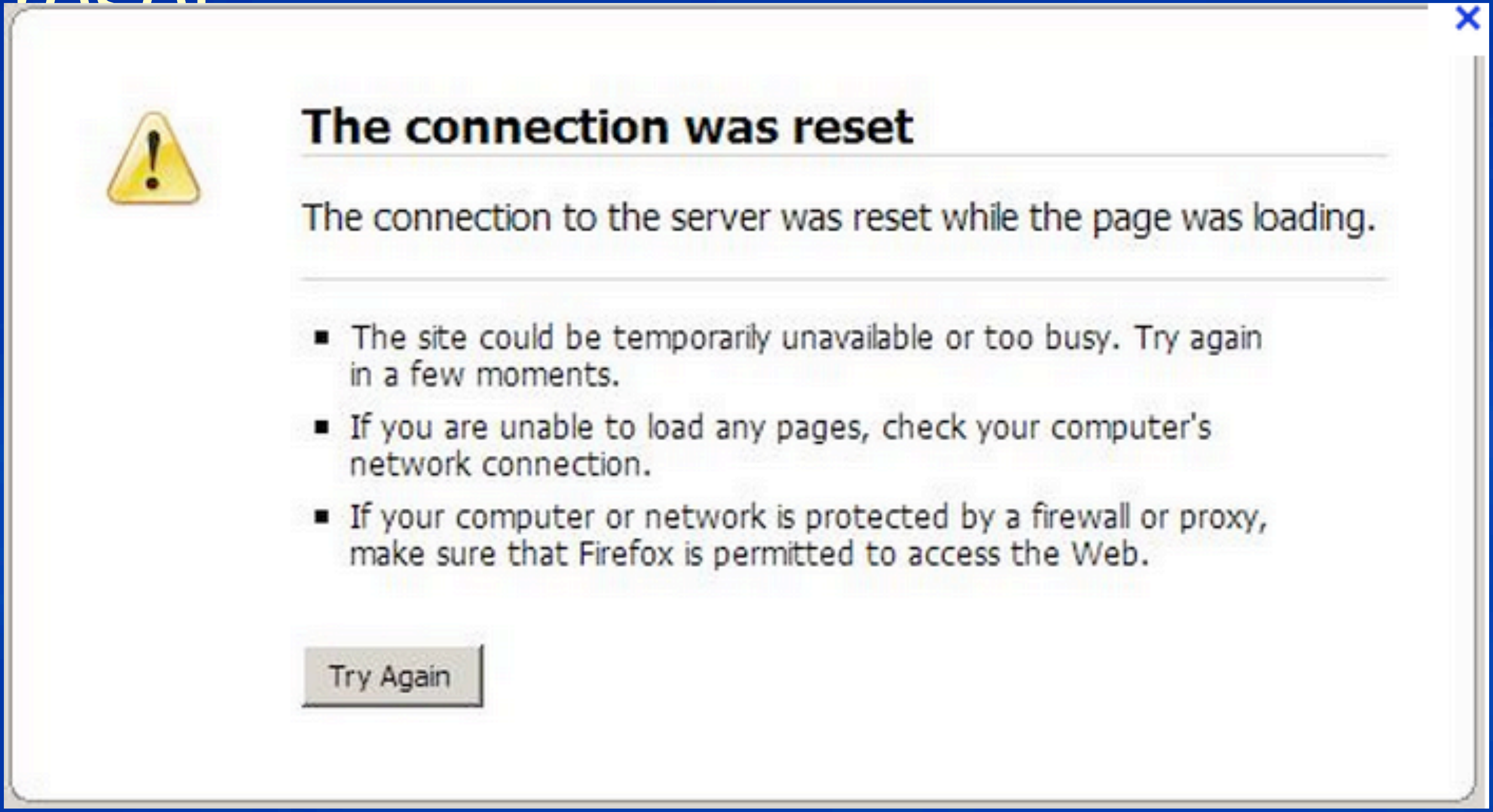
DNS filtering and redirection

- Before GFW, DNS already used by Chinese government to block the Internet
- Now is part of the GFW in 2002
- Even you use DNS outside of GFW
- DNS use UDP packets
- Different TTL number
- OSPF (Open Shortest Path First) protocol

Break DNS

- Use TCP protocol RFC1035
- Only a few support TCP request, like: 8.8.8.8
- Host file
- Ignore the first return result
- Ignore packet with certain TTL(Detect GFW's finger print)
- HEADSUP! There are two types of GFW

URL/Packet filtering and Connection reset



The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

- Also block you in the next 10 ~ 30 mins

URL/Packet filtering and Connection reset

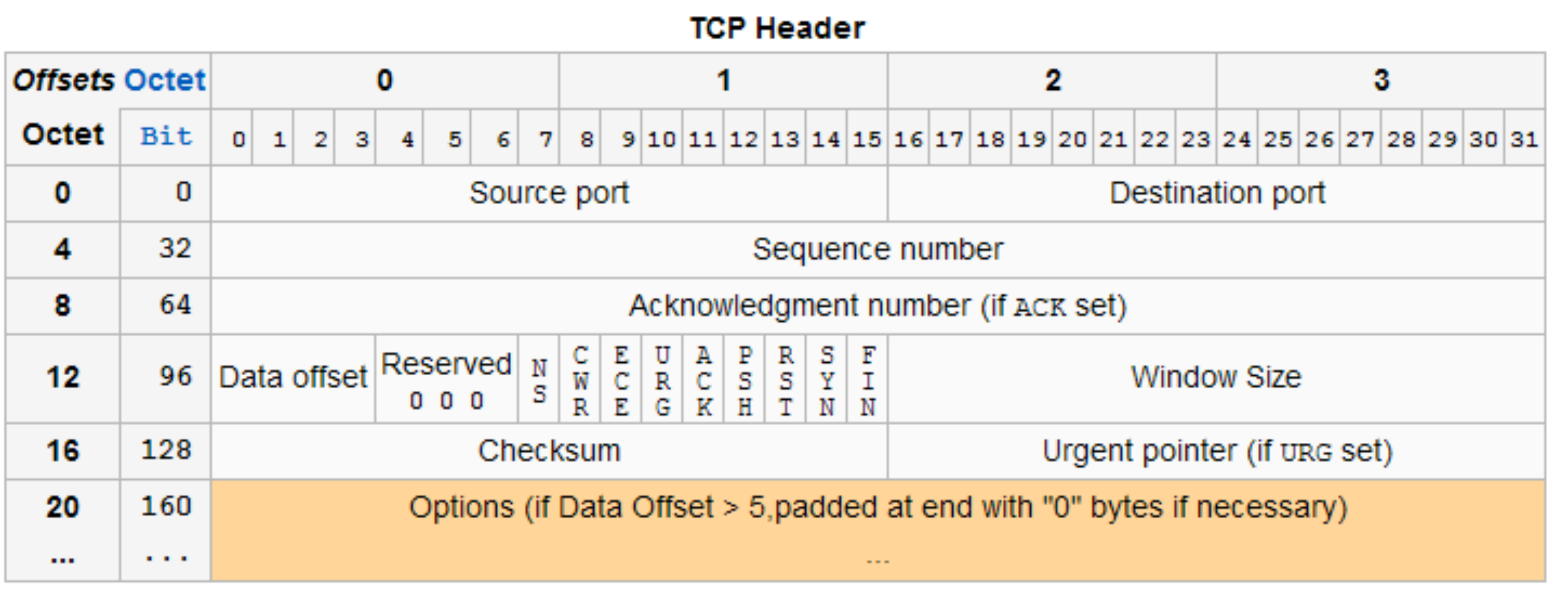
- Plaintext URL: www.youtube.com胡锦涛
- base64、rot13、URL encoded3d3LnlvdXR1YmUuY29tDQo=
  %e8%83%a1%e9%94%a6%e6%b6%9b%0d%0a
- GET /URL HTTP/1.x
- Also censor the return results(works in application layer)

  Packet no.1 DATA:……胡

  Packet no.2 DATA:锦涛….

URL/Packet filtering and Connection reset

- Send RST packet to client



TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if Data Offset > 5,padded at end with "0" bytes if necessary)																															
...	...	...																															

- **Why RST, not FIN?**

URL/Packet filtering and Connection reset

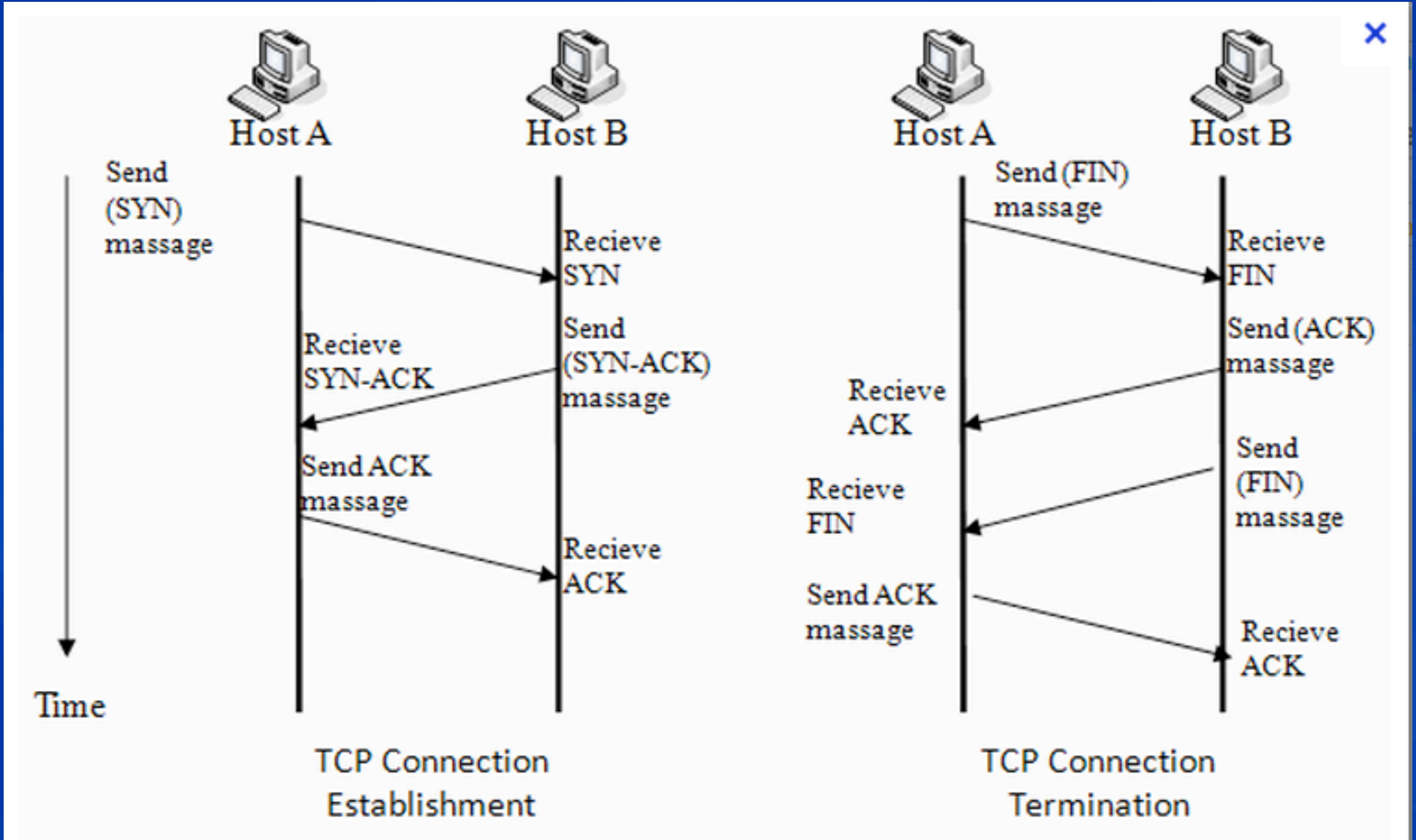


Figure 2.1. TCP session establishment and termination

URL/Packet filtering and Connection reset BREAK IT!

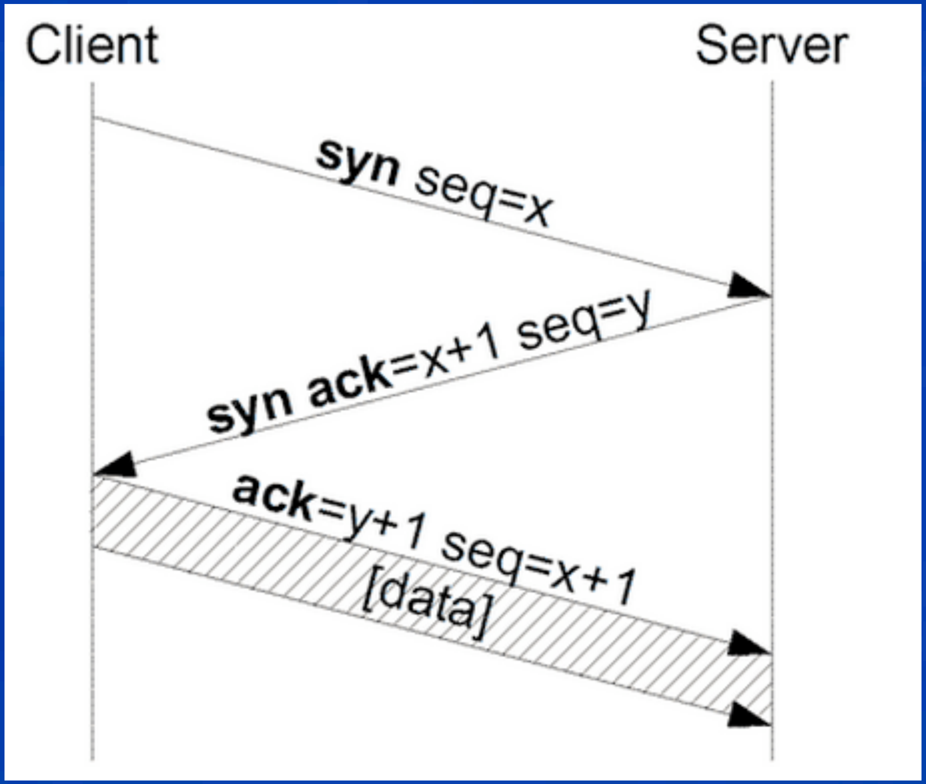
- Ignore all RST packets

```
iptables -A INPUT -p tcp –tcp-flags RST RST -j DROP
```

- Two types of GFW, RST, RST/ACK
- West Chamber Project

URL/Packet filtering and Connection reset

- Three way handshake



URL/Packet filtering and Connection reset

- Three way handshake
- RFC 793

-
  ```
  /*
  * essential part 1
  * inject an FIN with bad sequence number,
  obfuscating the handshake.
  * it will be dropped by rfc-compliant
  endpoint,
  * meanwhile thwarting eavesdroppers on
  the same direction (c -> s).
  */
  ```

URL/Packet filtering and Connection reset

-
  ```
  /*
  * essential part 2
  * inject an ACK with correct SEQ but bad ACK.
  * this causes an RST from server which should have no real impact on
  * the original connection,
  * thus thwarts eavesdroppers on the other direction (s -> c).
  *
  ```

URL/Packet filtering and Connection reset

- ** RFC793:*
  **   2. If the connection is in any non-synchronized state (LISTEN,*
  **   SYN-SENT, SYN-RECEIVED), and the incoming segment acknowledges*
  **   something not yet sent (the segment carries an unacceptable ACK),*
  **   …, a reset is sent.*
  ***
  ***

URL/Packet filtering and Connection reset

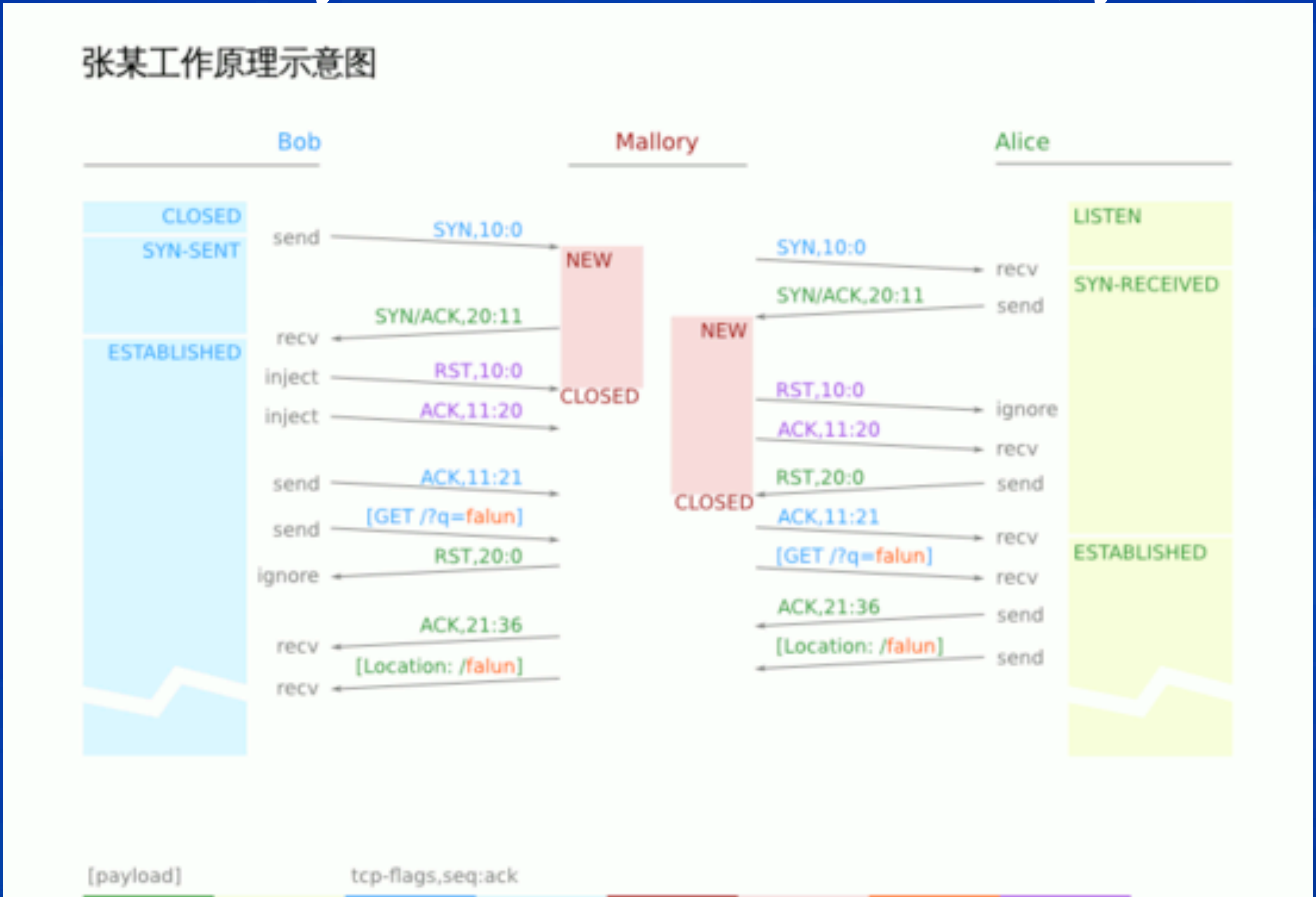
- If the incoming segment has an ACK field, the reset takes its
  * sequence number from the ACK field of the segment, otherwise the
  * reset has sequence number zero and the ACK field is set to the sum
  * of the sequence number and segment length of the incoming segment.
  * The connection remains in the same state.
  *

  * sometimes certain kind of rfc non-compliant tcp stacks or firewalls
  * may have unexpected response or no reply at all.
  *

  * seems that the seq is not nessesarily correct

URL/Packet filtering and Connection reset

- Three way handshake – In China, yeah!



URL/Packet filtering and Connection reset

- Why dose GFW ignore all the traffic after RST or Fin packets?
- DDOS

URL/Packet filtering and Connection reset

- Type2 GFW, send ACK/RST packet 3 times
- With seq number
- N
- N+1460
- N+2920

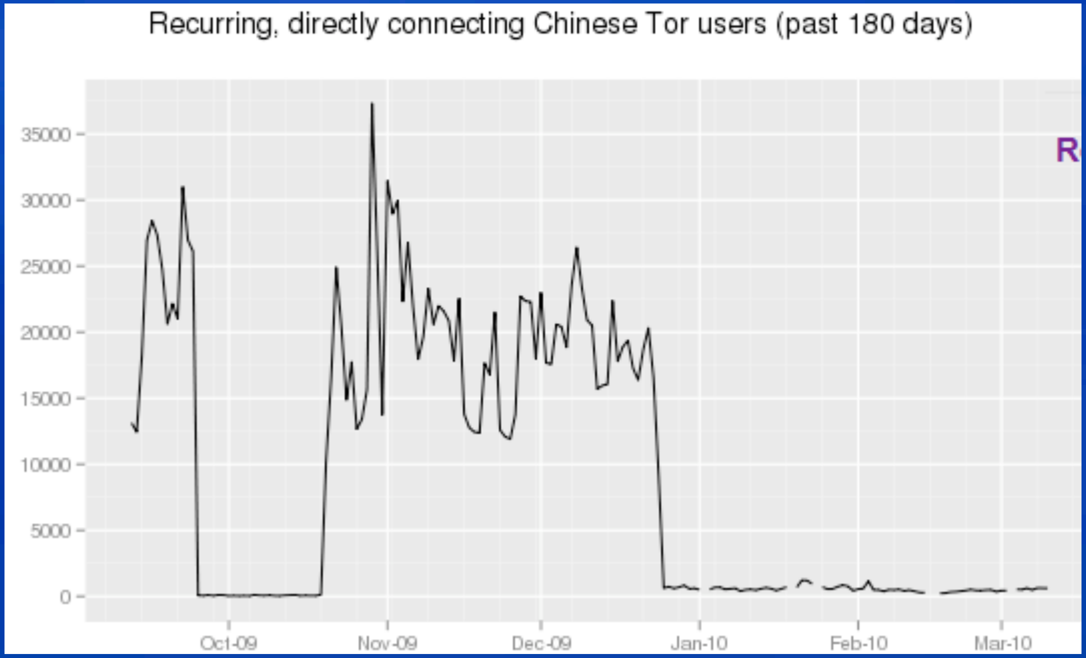
- TCP mss
- The **maximum segment size** (**MSS**) is a parameter of the TCP protocol that specifies the largest amount of data
- This is an example of GFW's finger print

SSL certificate filtering

- Certificate transferred from server doesn’t encrypt
- Block 433 port every 10 mins(gmail)
- Your data still safe

Fake Tor node and filtering

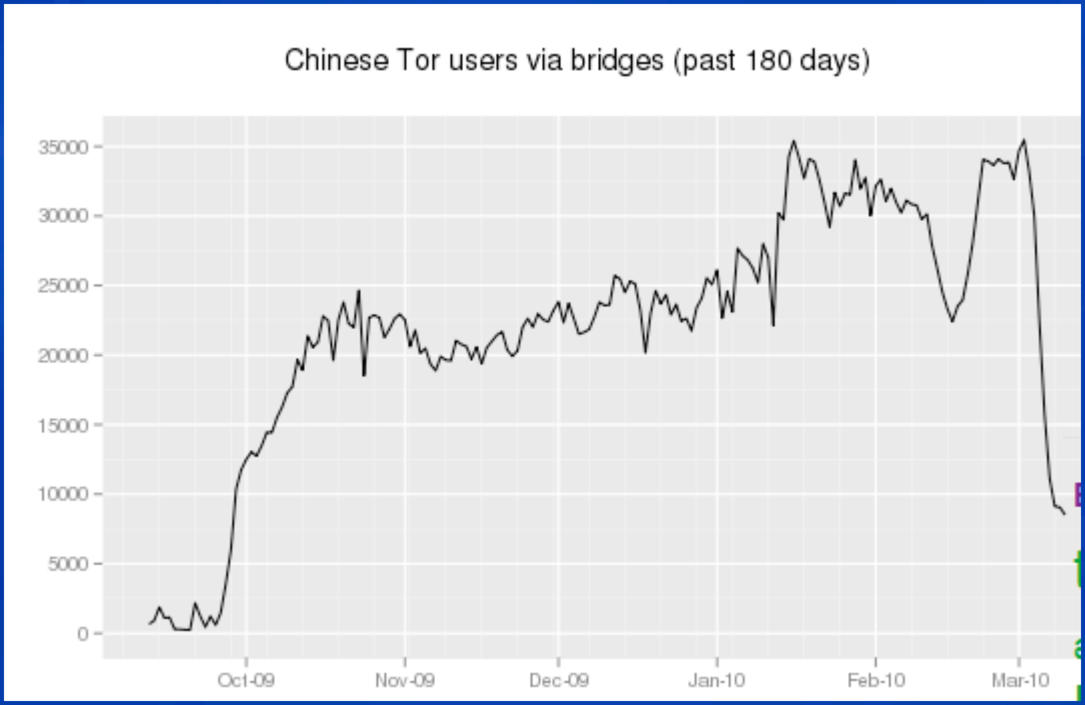
- Round 1
- Not possible to block all Tor nodes
- Put fake Tor nodes in China



Recurring, directly connecting Chinese Tor users (past 180 days)

Fake Tor node and filtering

- Round 2
- non-public relays, use bridges



Any other ways?

- DDOS GFW

- Questions?