中国政府の運用する Great Firewall (GFW) のアーキテクチャ入門 ＆ VPN Gate システムの紹介

登 大遊 (のぼり だいゆう)

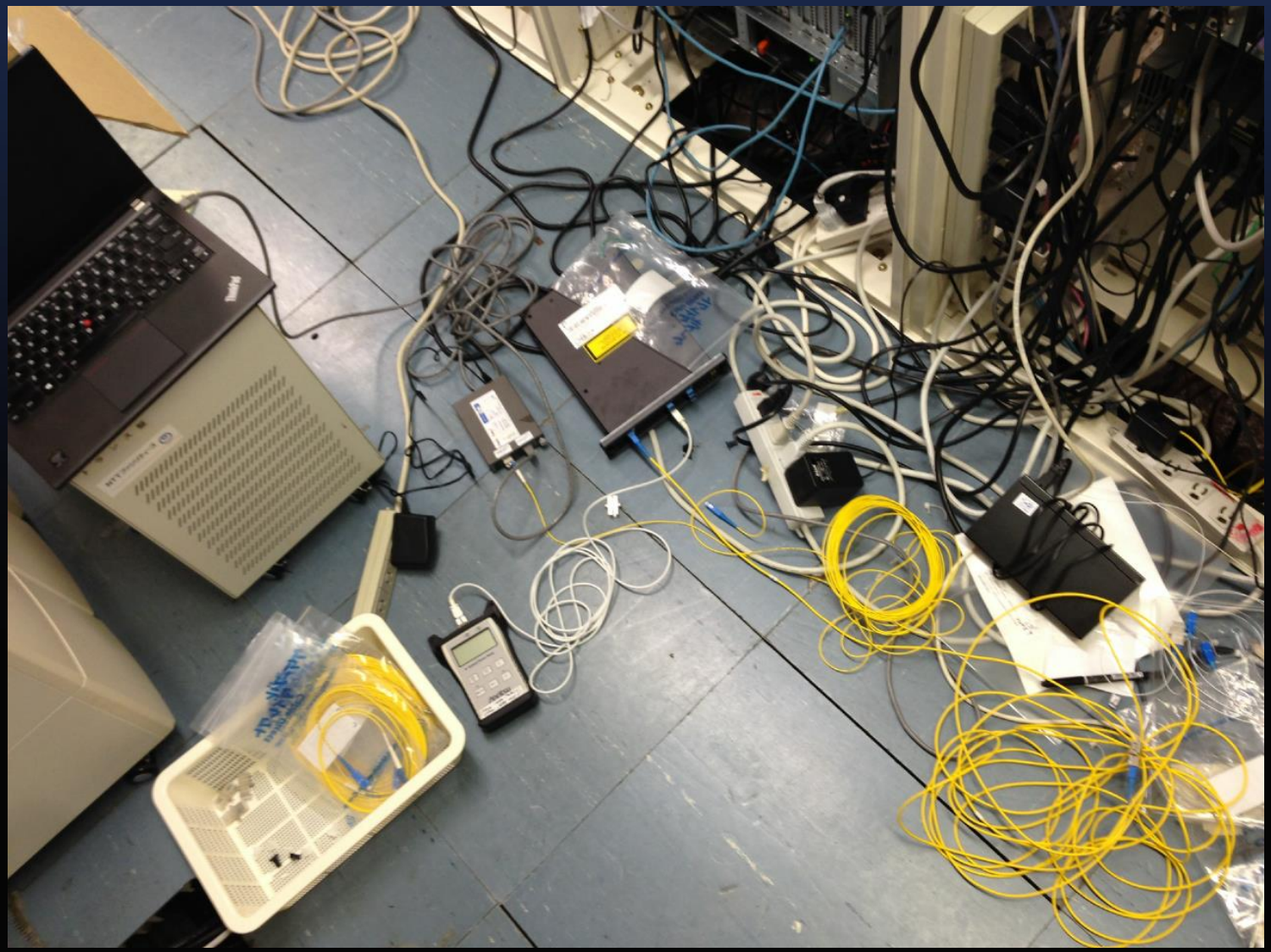
筑波大学大学院システム情報工学研究科
博士後期課程に入院中

ソフトイーサ株式会社 代表取締役

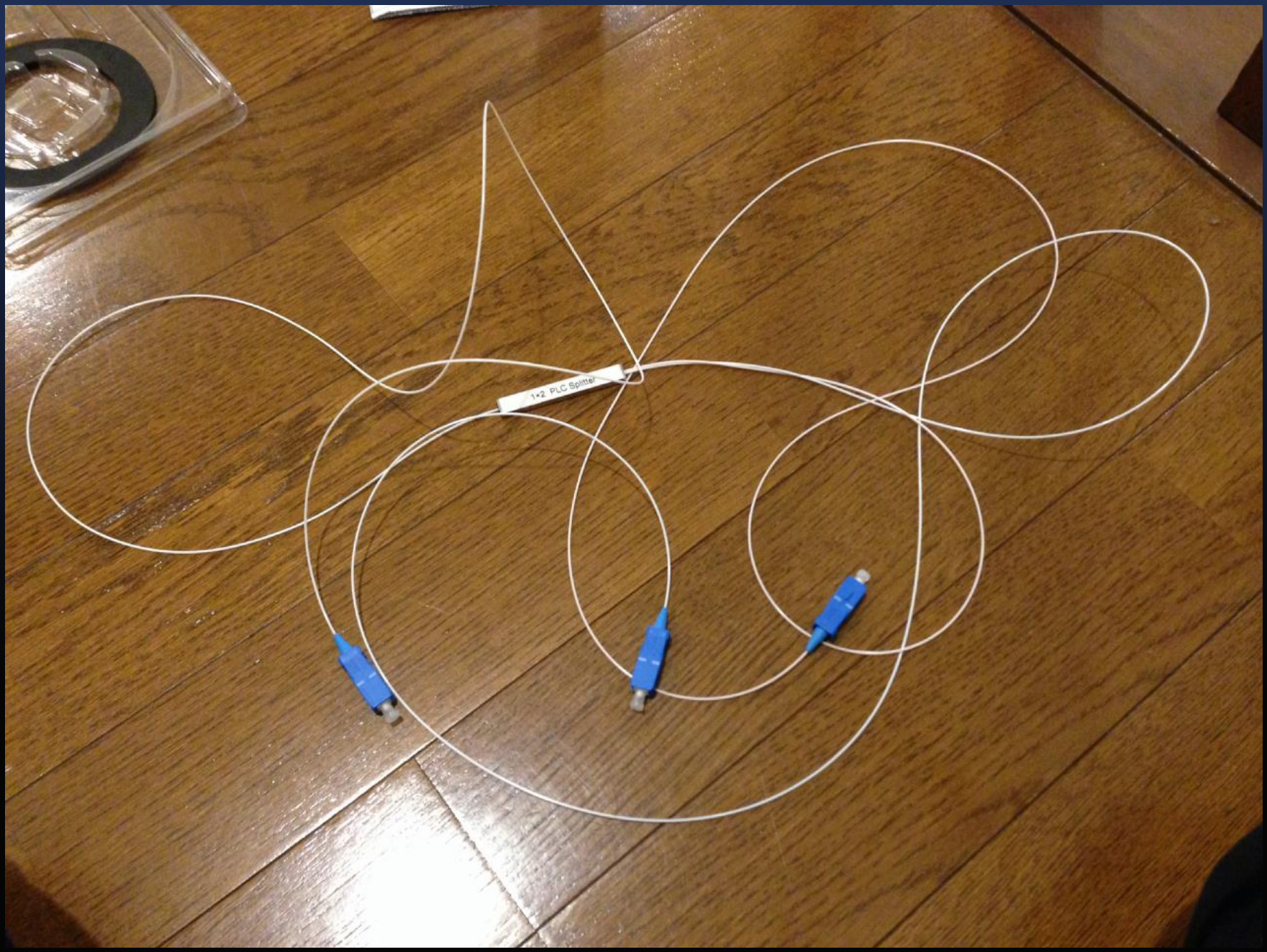
登 大遊 自己紹介

- 2003.4 筑波大学 入学
- **2003.7 IPA未踏ソフトウェア事業採択 SoftEther を開発**
- 2004.4 ソフトイーサ株式会社 設立
- 2007.4 筑波大学大学院 博士前期課程 入院
- 2013.4 筑波大学大学院 博士後期課程 入院
  退院まであと 7 年かかる！ ←イマココ

最近の趣味: フレッツや専用線の安全性の検証

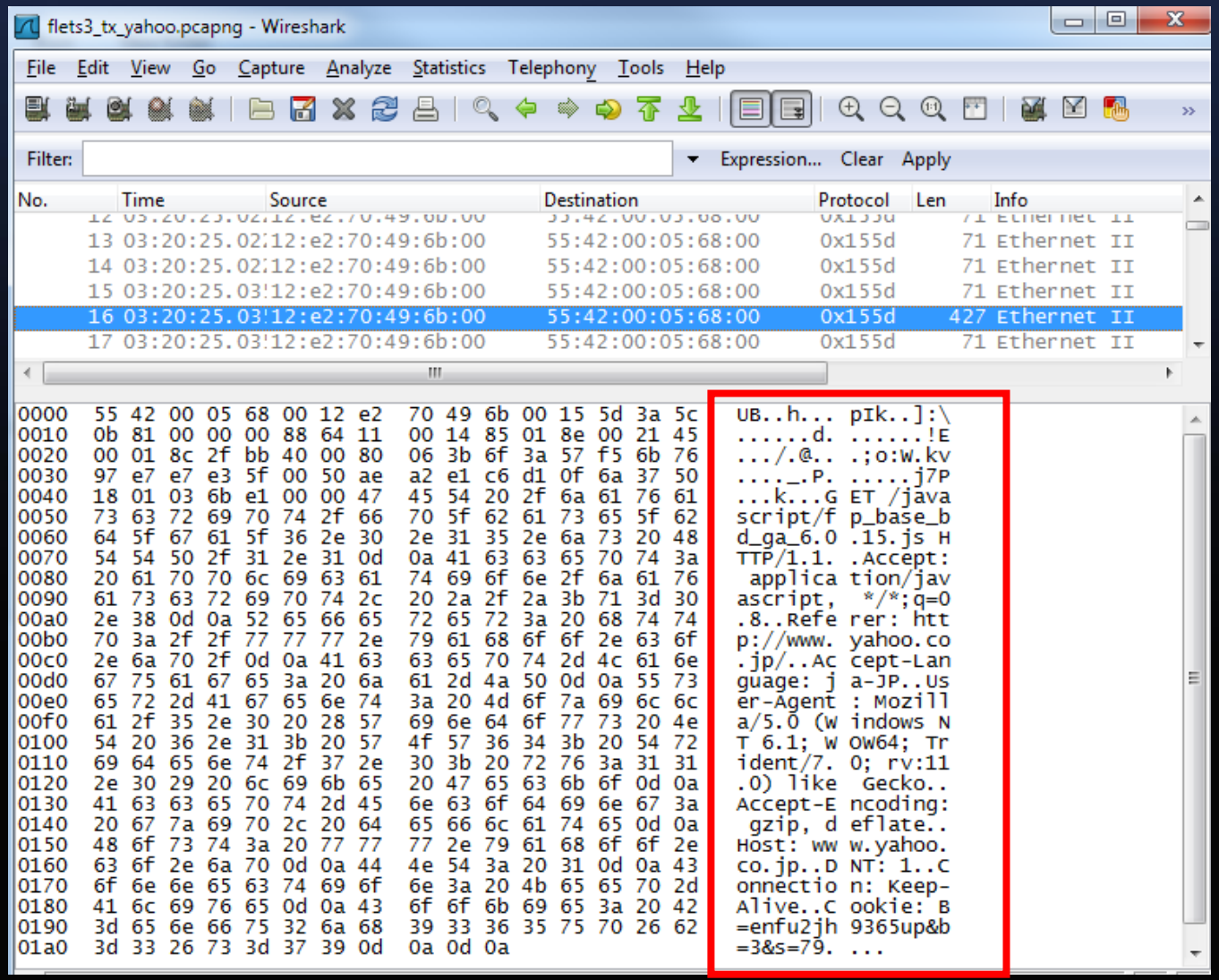


※ 他者の通信の秘密を侵害しないよう、自社専用の回線上で実験しています



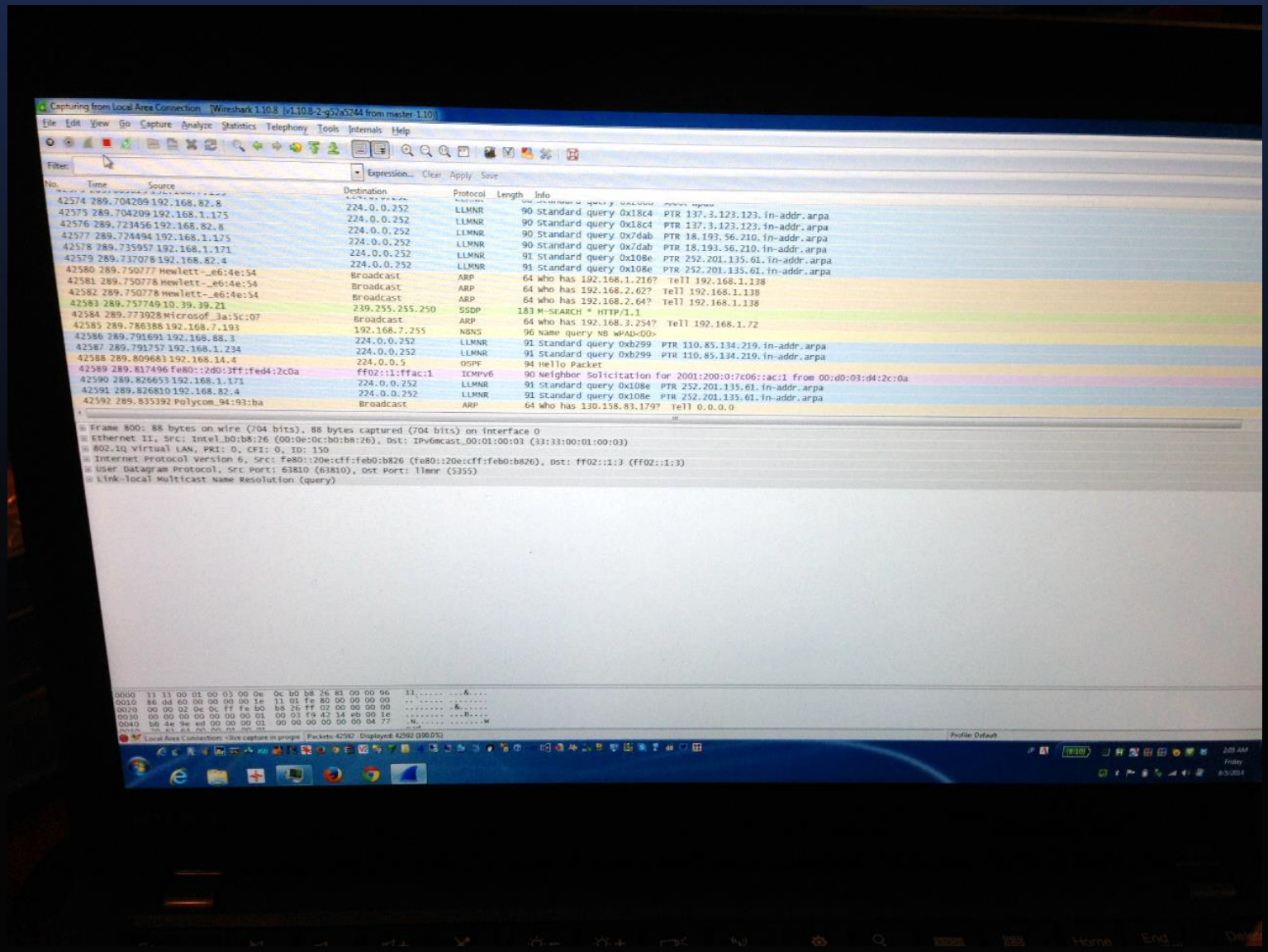
※ 他者の通信の秘密を侵害しないよう、自社専用の回線上で実験しています

フレッツ安全性検証実験結果 (アップロード方向)



※ 他者の通信の秘密を侵害しないよう、自社専用の回線上で実験しています

専用線安全性検証実験結果 (双方向)



※ 他者の通信の秘密を侵害しないよう、自社専用の回線上で実験しています

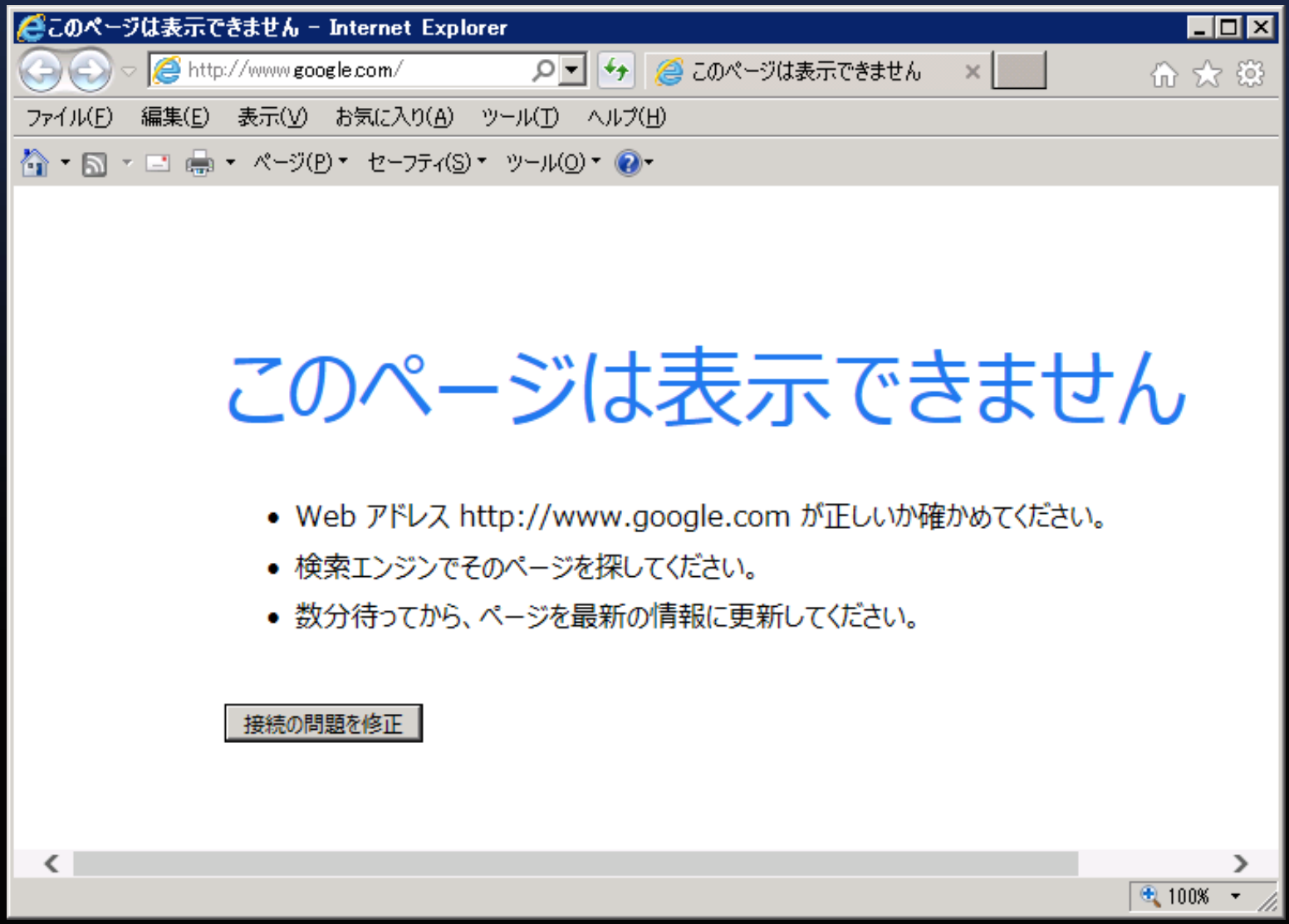
※ 他者の通信の秘密を侵害しないよう、自社専用の回線上で実験しています

中国政府の運用する Great Firewall（GFW）のアーキテクチャ入門

登 大遊
筑波大学大学院システム情報工学研究科
コンピュータサイエンス専攻博士ソフトウェア研究室

筑波大学
University of Tsukuba

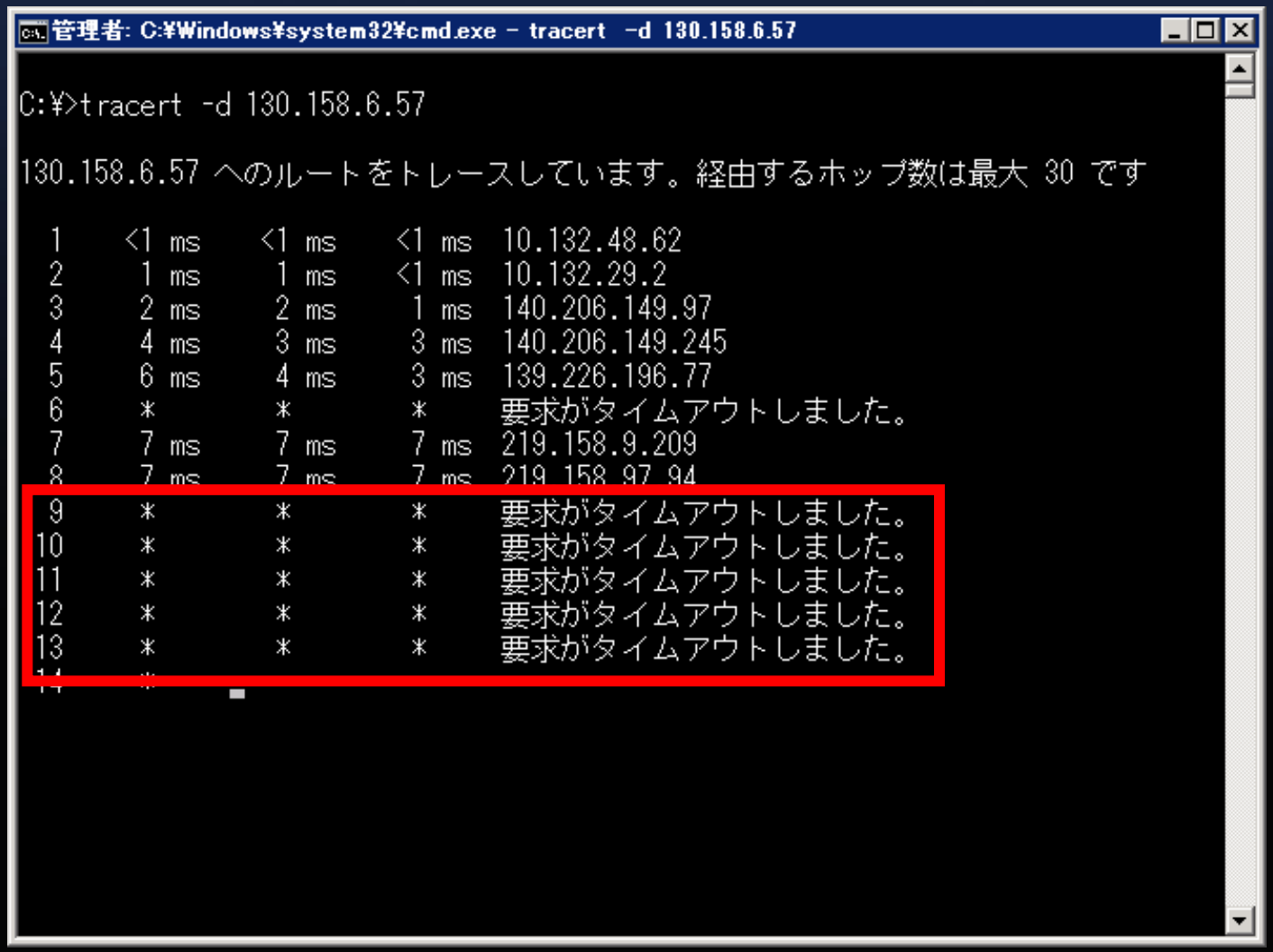
GFW


このページは表示できません - Internet Explorer
http://www.google.com/
このページは表示できません
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
ページ(P) セーフティ(S) ツール(O)
このページは表示できません
Web アドレス http://www.google.com が正しいか確かめてください。
検索エンジンでそのページを探してください。
数分待ってから、ページを最新の情報に更新してください。
接続の問題を修正
100%

GFW が提供する主な遮断機能

- 第 1 世代 (2000年代～)
  - 海外の特定 IP アドレスを対象とした遮断
    - 数千個が限界、共有Webサーバー等でトラブルが発生する
- 第 2 世代 (2000年代～)
  - 偽装 DNS、TCP、SMTP パケットを応答させることによるコネクション遮断
    - 上限がないが DNS および TCP しか対応できない
- 第 3 世代 (2014年6月～)
  - 第1世代を拡張。大量の海外 IP アドレスへの動的フィルタリング機能を搭載
    - 各 L2 スイッチの TCAM (Ternary CAM) が溢れないようにするため 180 秒間のみ ACL を挿入する手法を開発

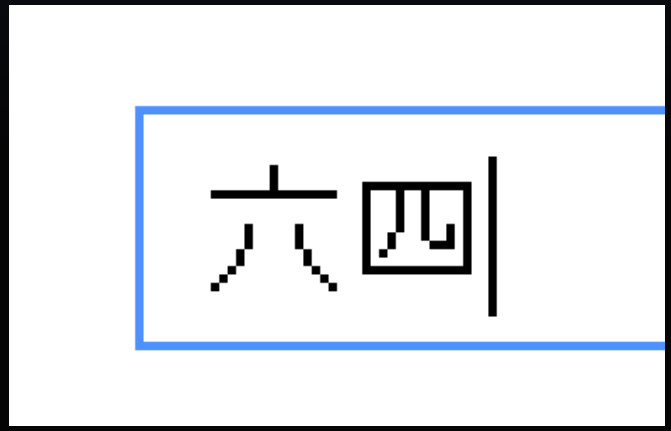
- **第 1 世代 (2000年代～)**
  - 海外の特定 IP アドレスを対象とした遮断
    - 数千個が限界、共有Webサーバー等でトラブルが発生する



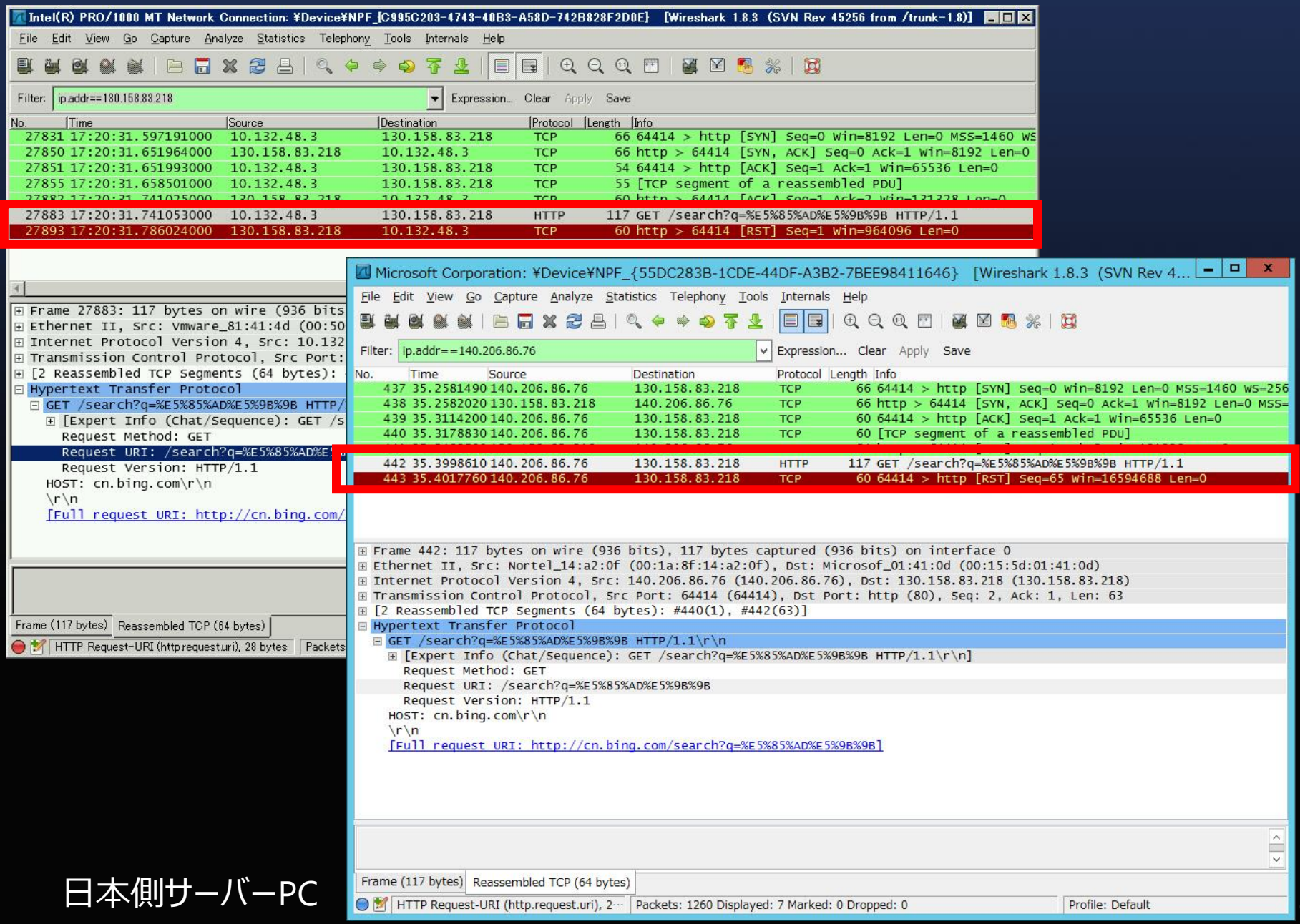
- **第２世代 (2000年代～)**
  - 偽装 DNS、TCP、SMTP パケットを応答させることによるコネクション遮断
    - 上限がないが DNS および TCP しか対応できない

TCP 実験例

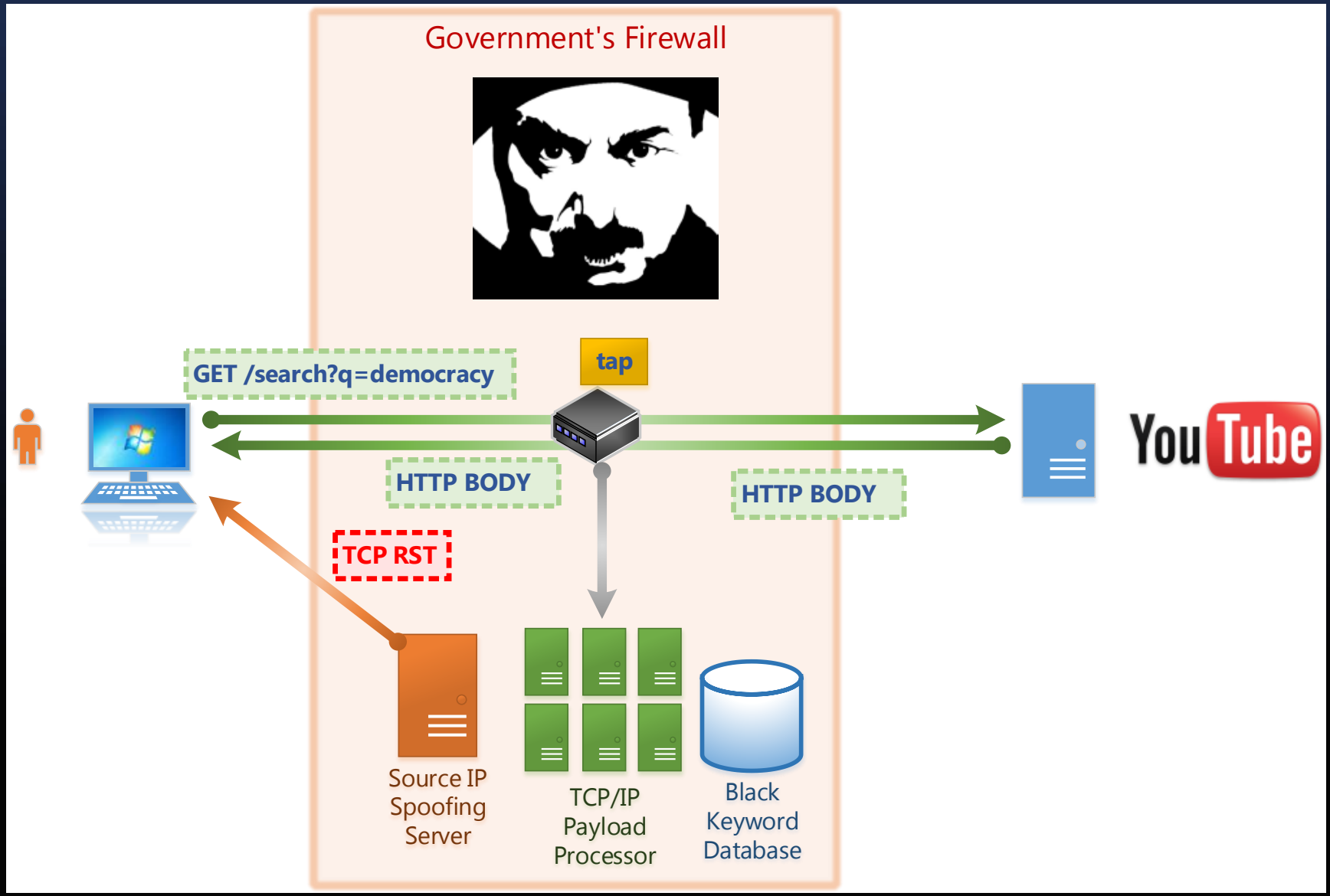
telnet 130.158.83.218 80
GET /search?q=%E5%85%AD%E5%9B%9B
HTTP/1.1
HOST: penguin1.cs.tsukuba.ac.jp



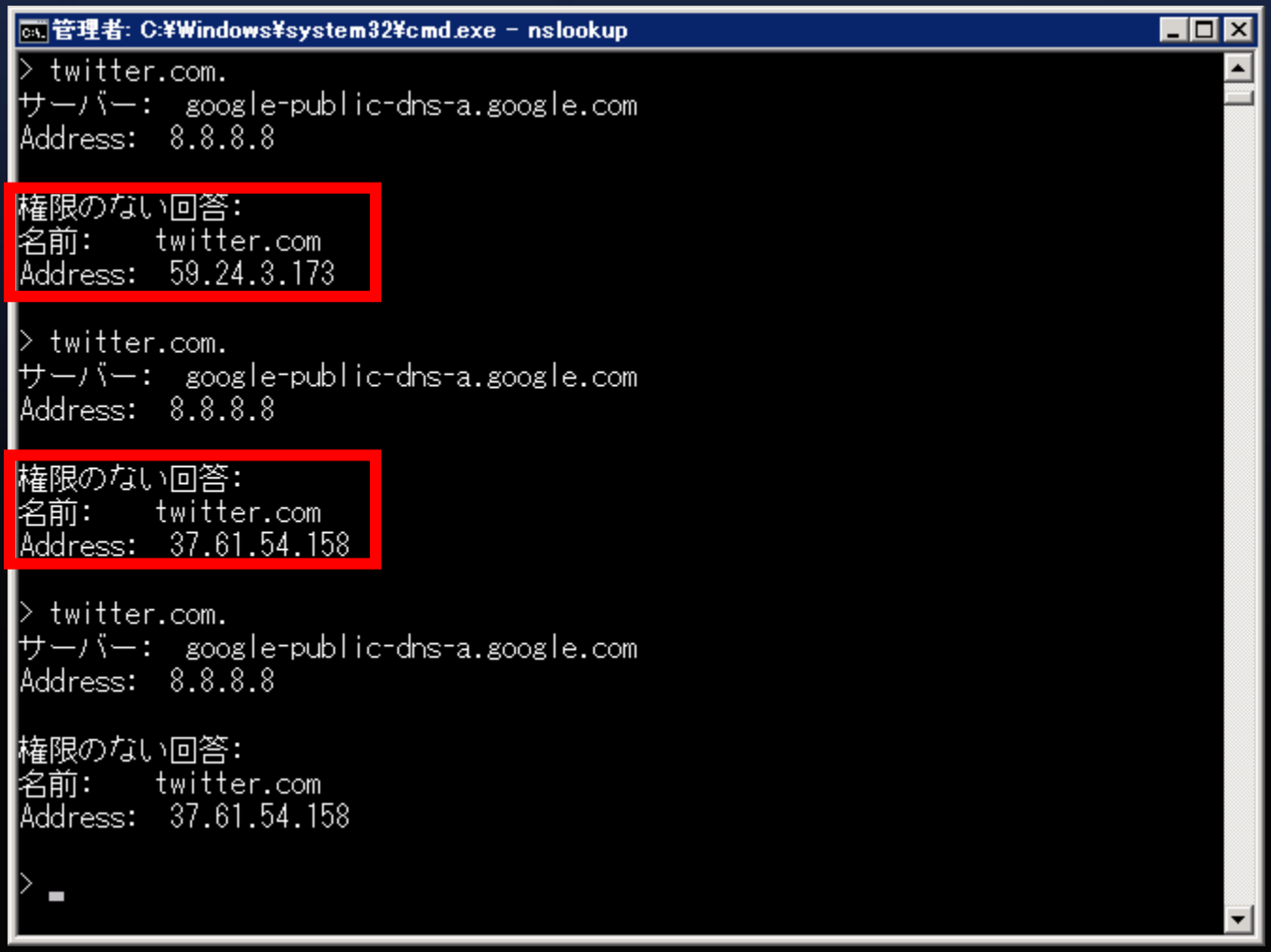
中国側クライアントPC



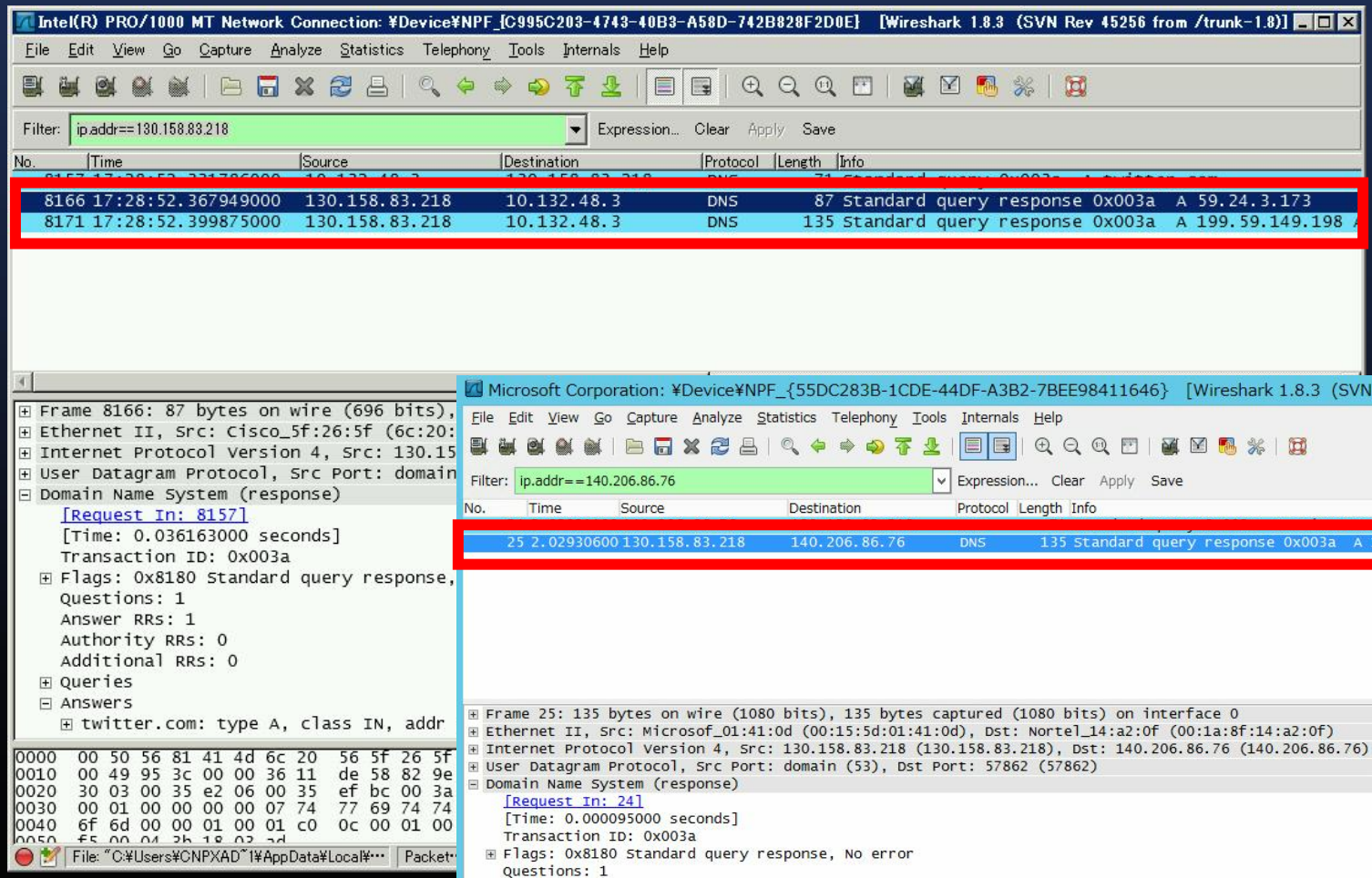
日本側サーバーPC


Government's Firewall
GET /search?q=democracy
tap
HTTP BODY
HTTP BODY
TCP RST
YouTube
Source IP Spoofing Server
TCP/IP Payload Processor
Black Keyword Database

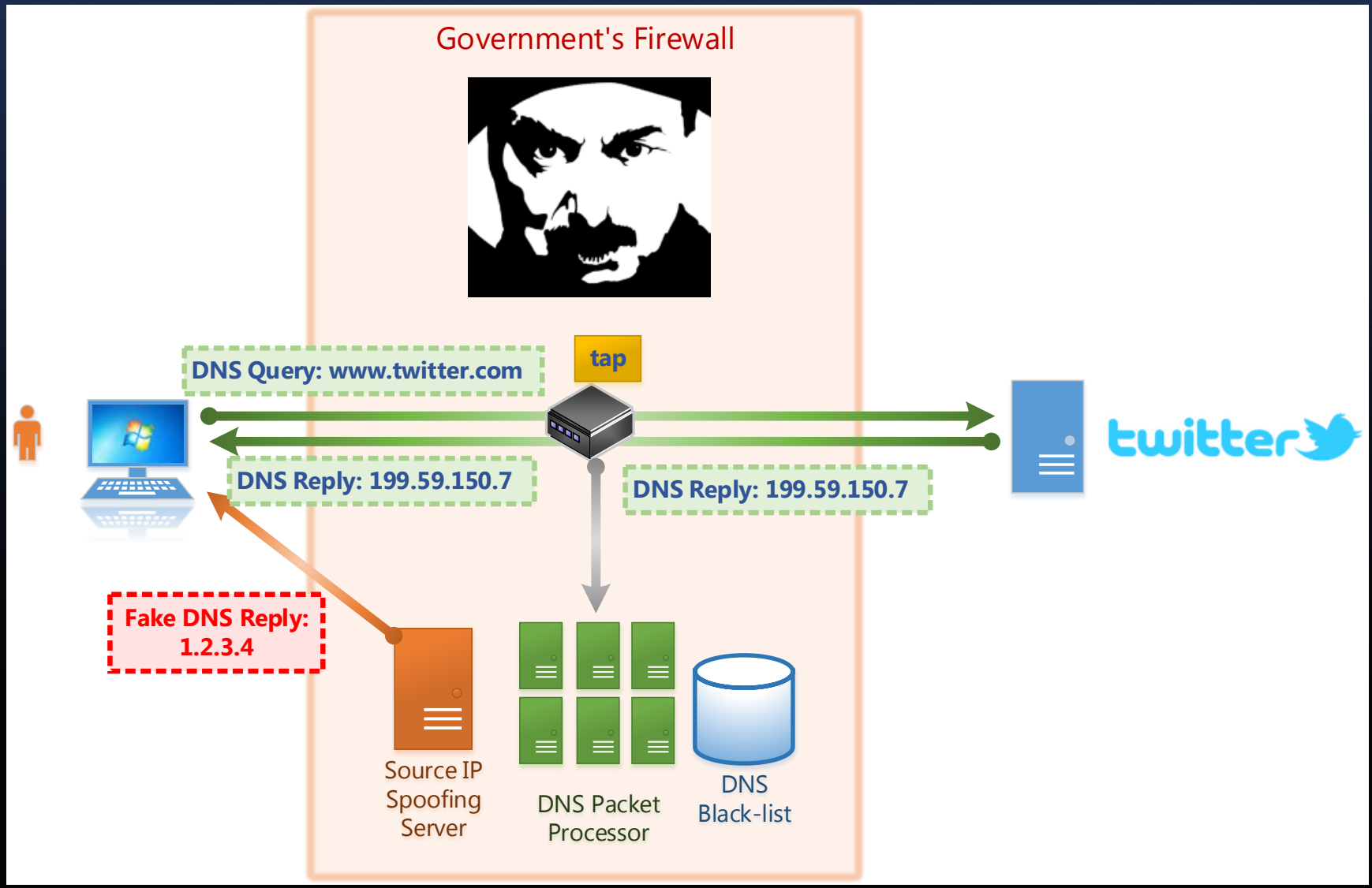
DNS 実験例


管理者: C:¥Windows¥system32¥cmd.exe - nslookup
> twitter.com.
サーバー: google-public-dns-a.google.com
Address: 8.8.8.8
権限のない回答:
名前: twitter.com
Address: 59.24.3.173
> twitter.com.
サーバー: google-public-dns-a.google.com
Address: 8.8.8.8
権限のない回答:
名前: twitter.com
Address: 37.61.54.158
> twitter.com.
サーバー: google-public-dns-a.google.com
Address: 8.8.8.8
権限のない回答:
名前: twitter.com
Address: 37.61.54.158
>

中国側クライアントPC



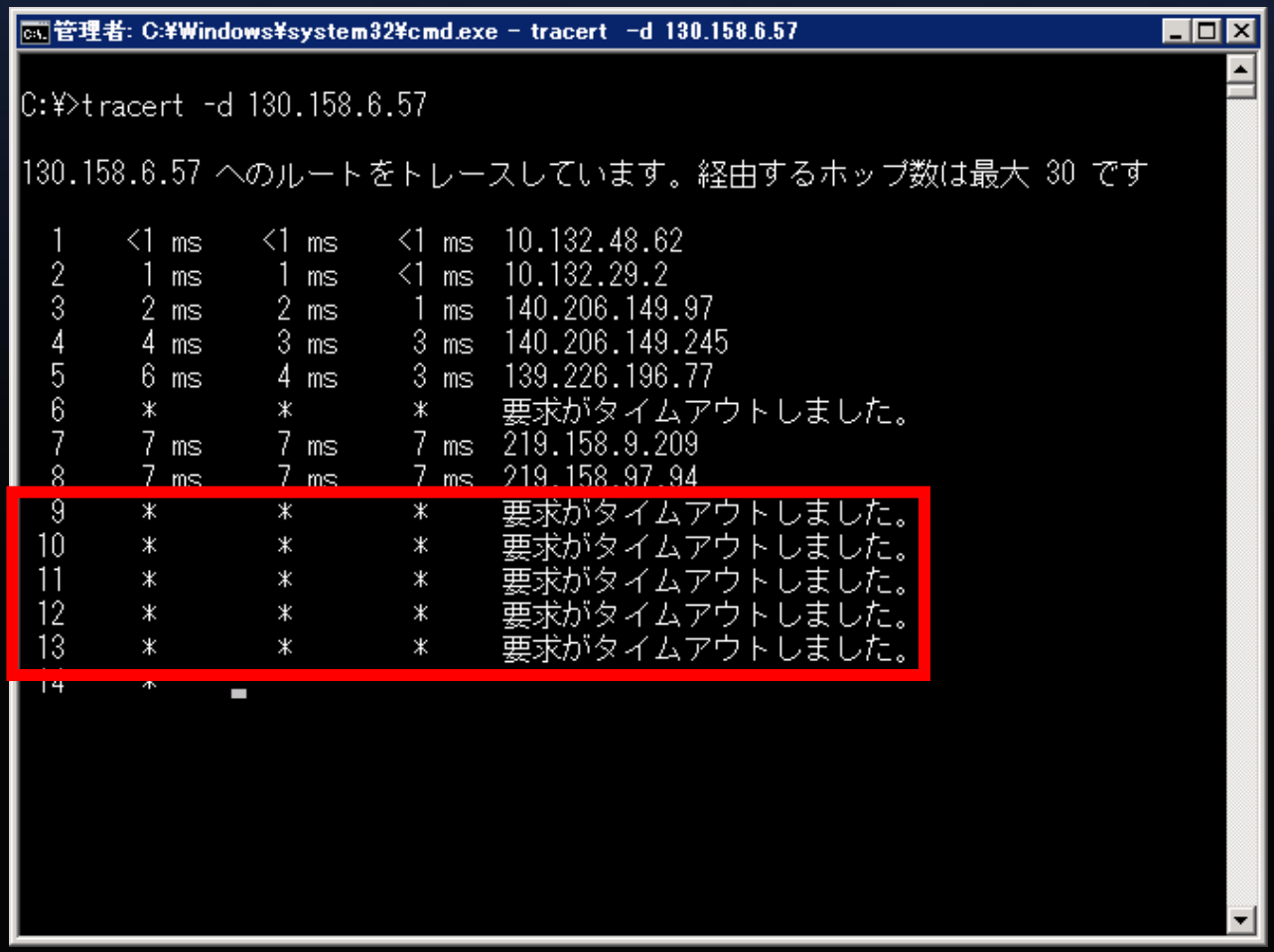
日本側サーバーPC

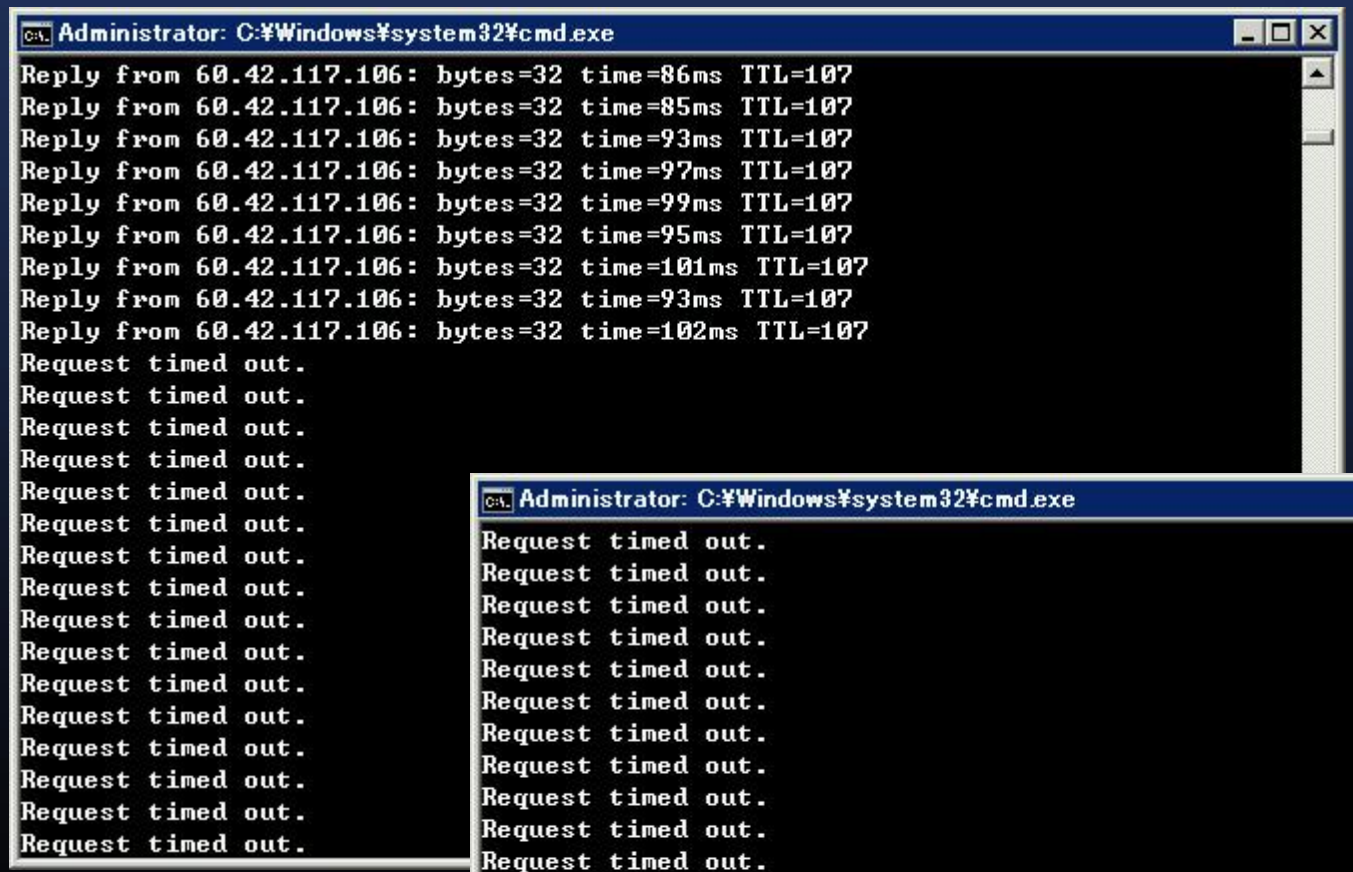

Government's Firewall
DNS Query: www.twitter.com
tap
DNS Reply: 199.59.150.7
DNS Reply: 199.59.150.7
twitter
Fake DNS Reply: 1.2.3.4
Source IP Spoofing Server
DNS Packet Processor
DNS Black-list

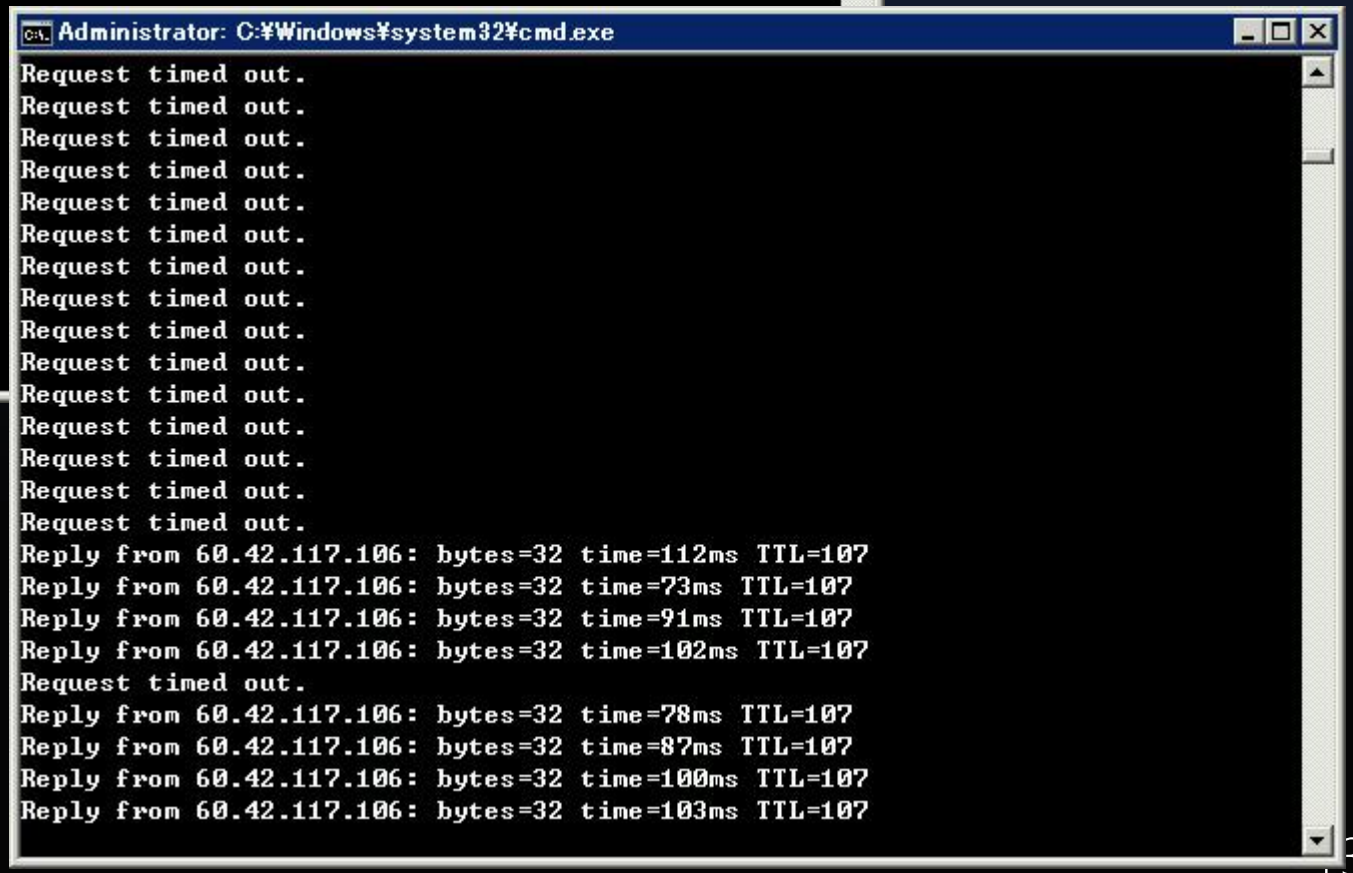
2014/1/21 に GFW の DNS 偽装応答システムで故障が発生

```
> www.yahoo.com.
サーバー:  google-public-dns-a.google.com
Address:  8.8.8.8

権限のない回答:
名前:    ds-fp3.wg1.b.yahoo.com
Address:  65.49.2.178
Aliases:  www.yahoo.com
          fd-fp3.wg1.b.yahoo.com

> www.ascii.co.jp.
サーバー:  google-public-dns-a.google.com
Address:  8.8.8.8

権限のない回答:
名前:    www.ascii.co.jp
Address:  65.49.2.178

> www.tsukuba.ac.jp.
サーバー:  google-public-dns-a.google.com
Address:  8.8.8.8

権限のない回答:
名前:    www.tsukuba.ac.jp
Address:  65.49.2.178

> www.microsoft.com.
サーバー:  google-public-dns-a.google.com
Address:  8.8.8.8

権限のない回答:
名前:    lb1.www.ms.akadns.net
Address:  65.49.2.178
Aliases:  www.microsoft.com
          toggle.www.ms.akadns.net
          g.www.ms.akadns.net
```

- **第３世代 (2014年6月～)**
  - 第1世代を拡張。大量の海外 IP アドレスへの動的フィルタリング機能を搭載
    - 各 L2 スイッチの TCAM (Ternary CAM) が溢れないようにするため 180 秒間のみ ACL を挿入する手法を開発

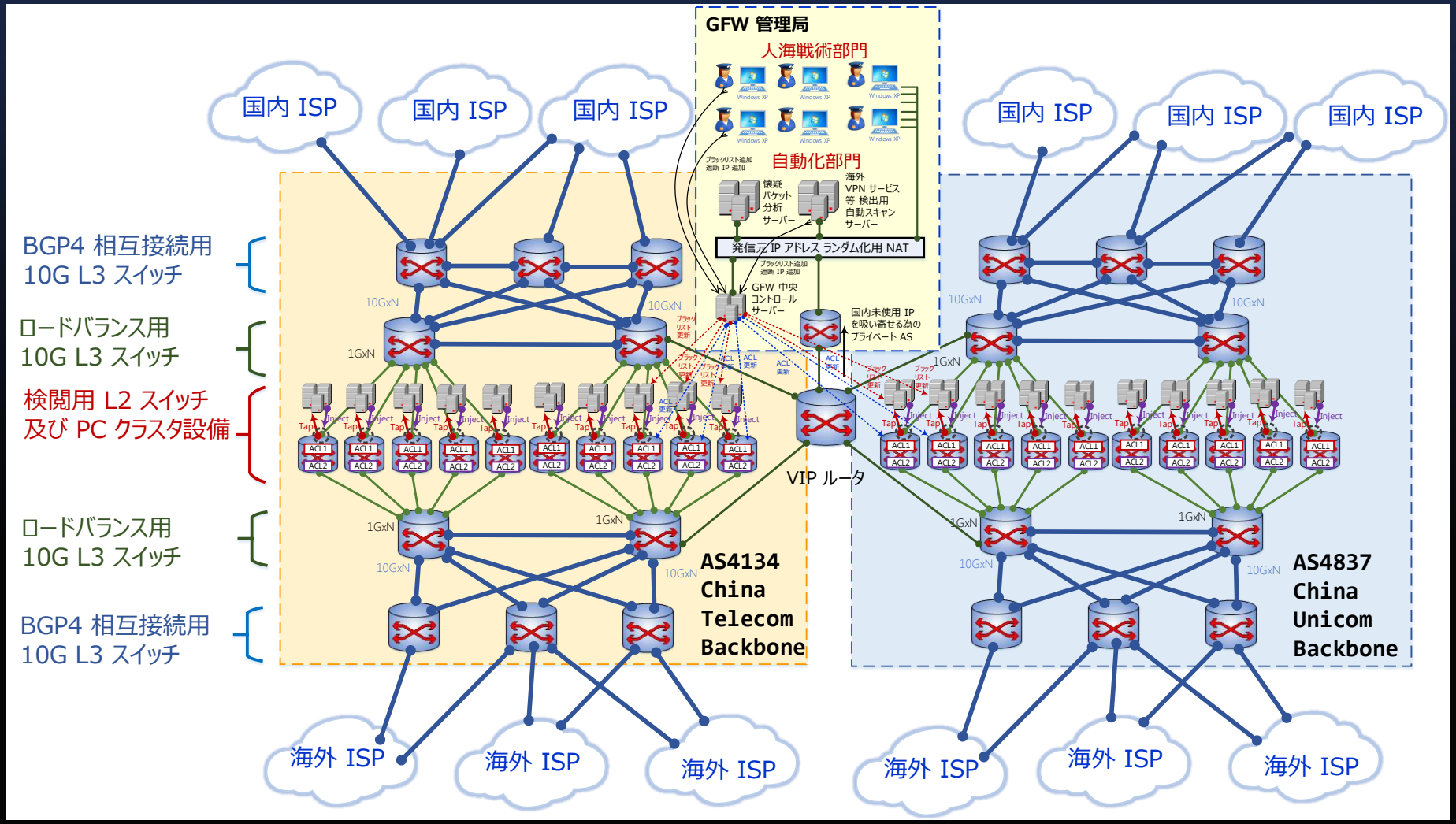




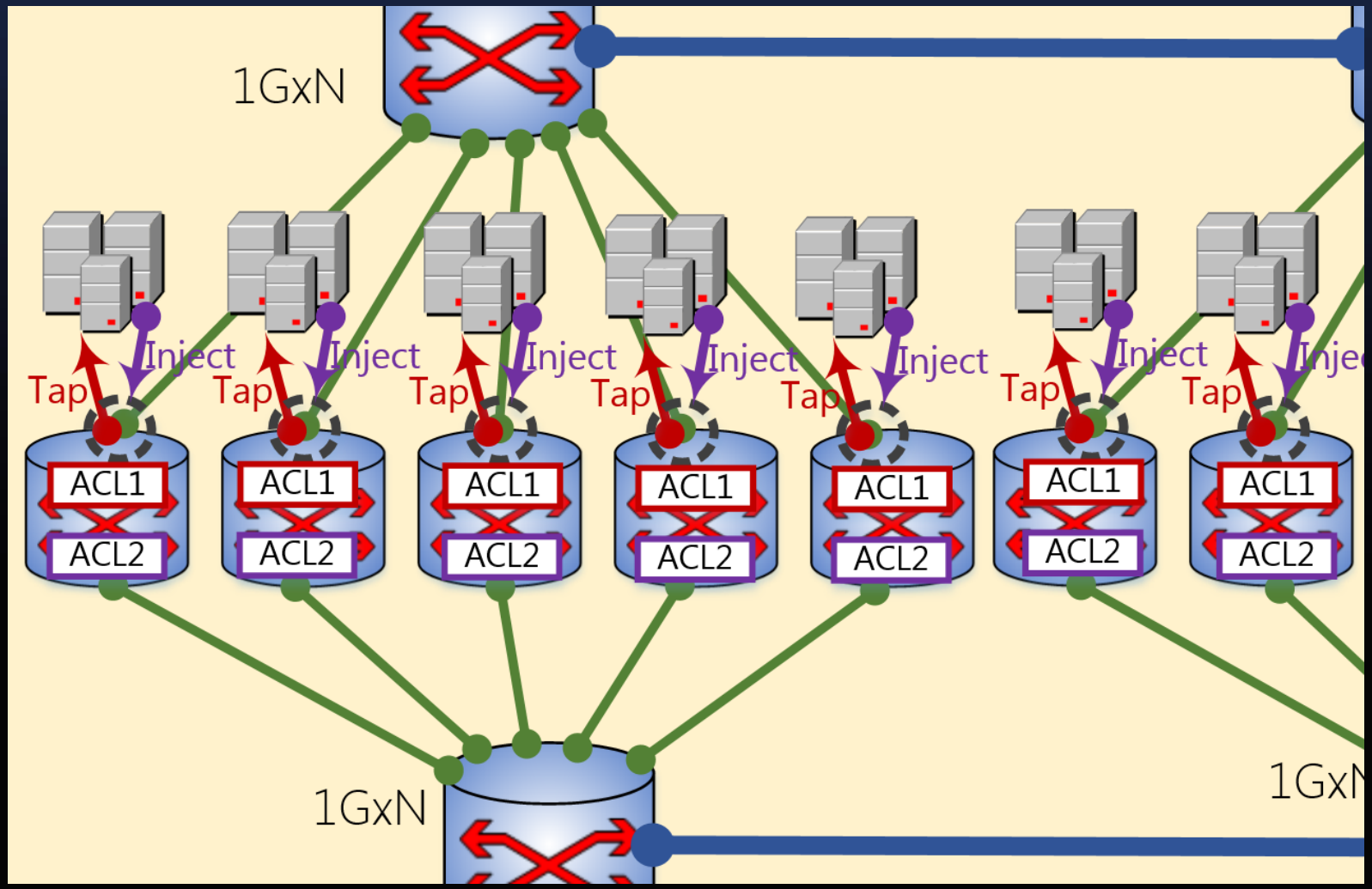


きっちり
180 秒間だけ
遮断。

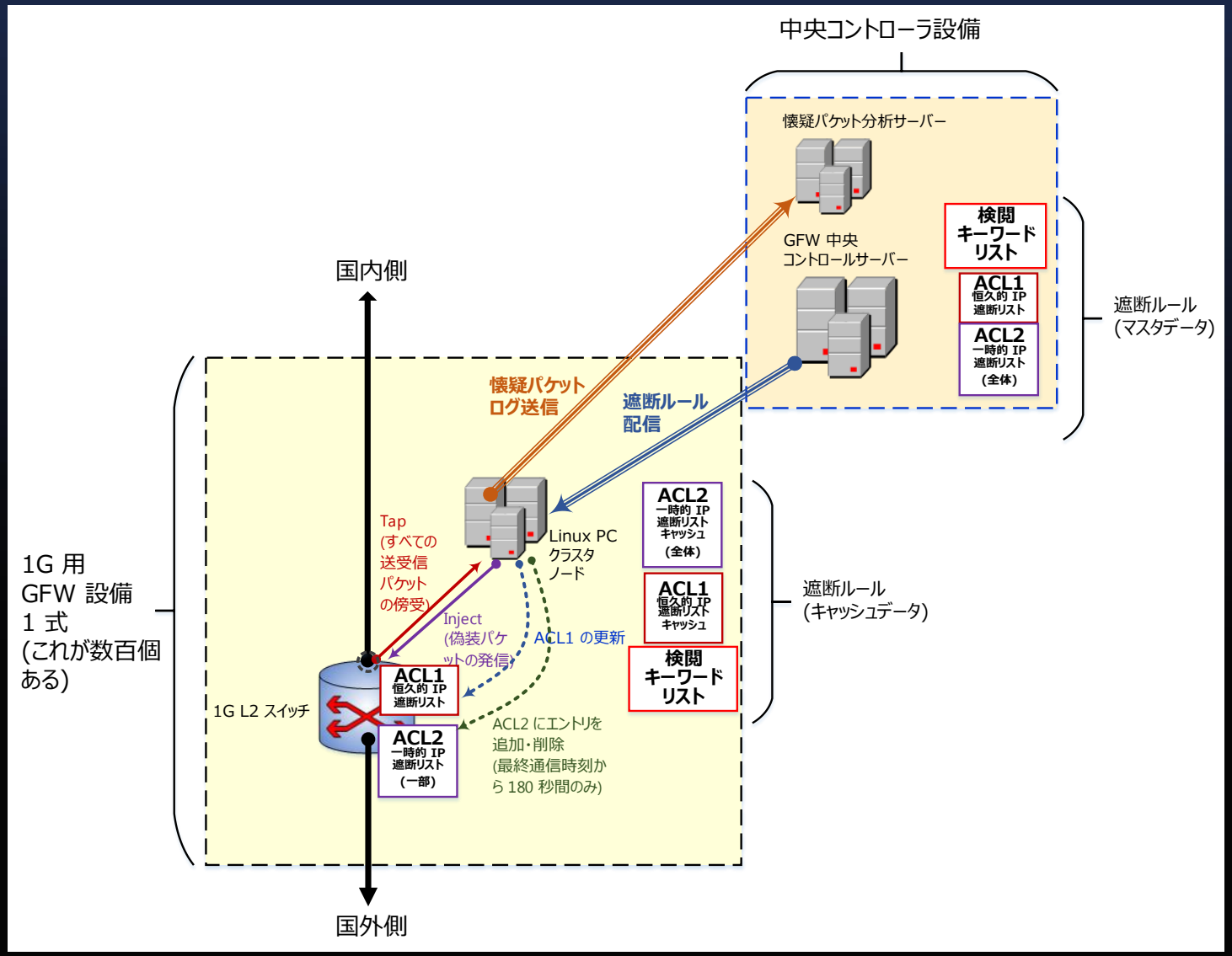
GFW のネットワークトポロジ (挙動から推測)



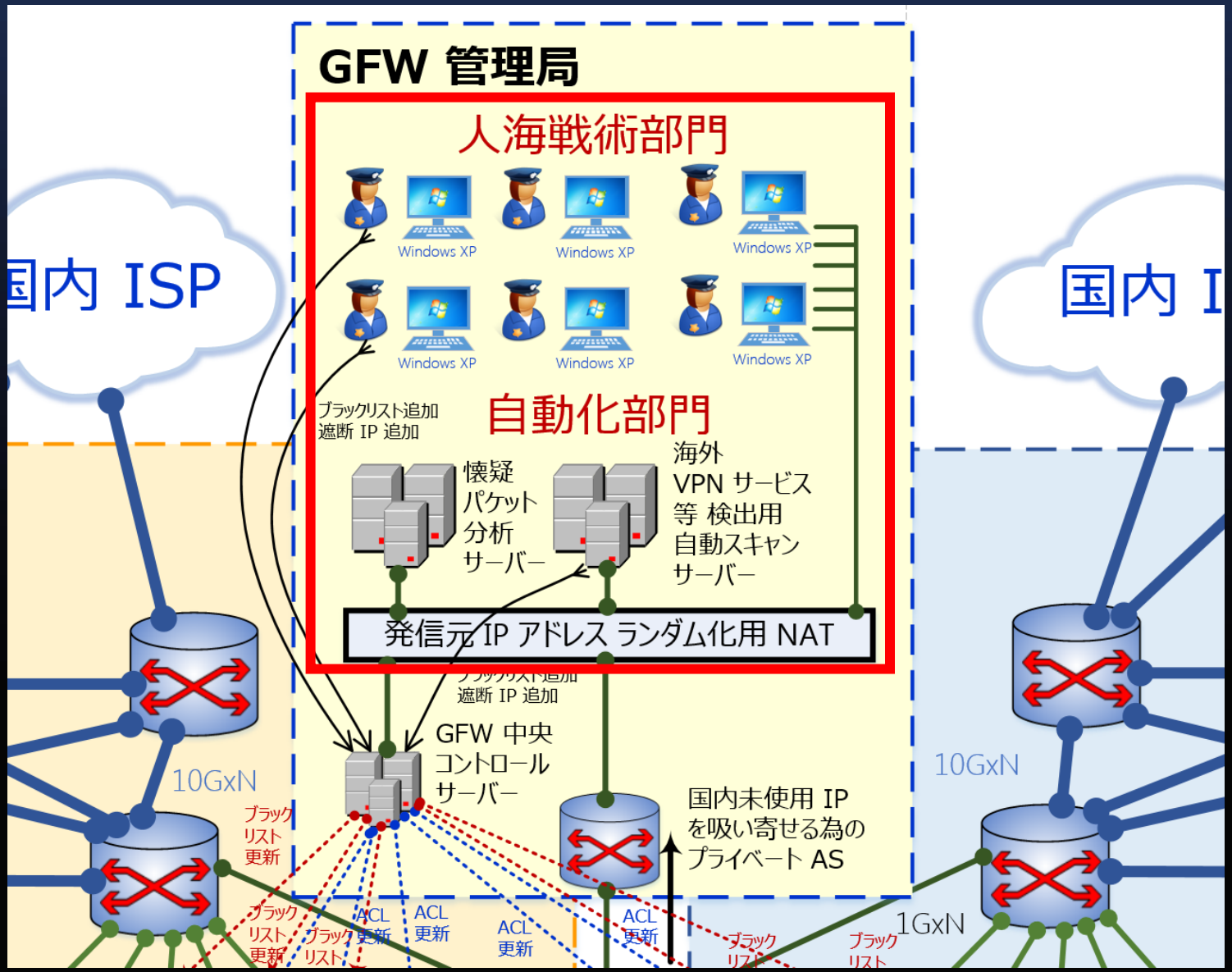
1Gbps 単位に分散し 安価な L2 スイッチおよび Linux PC で検閲・遮断を実施



1Gbps 検閲・遮断用装置



遮断リストの保守業務


GFW 管理局
人海戦術部門
Windows XP
Windows XP
Windows XP
Windows XP
Windows XP
Windows XP
国内 ISP
国内 I
ブラックリスト追加
遮断 IP 追加
自動化部門
懐疑
パケット
分析
サーバー
海外
VPN サービス
等 検出用
自動スキャン
サーバー
発信元 IP アドレス ランダム化用 NAT
ブラックリスト追加
遮断 IP 追加
GFW 中央
コントロール
サーバー
10GxN
10GxN
1GxN
ブラック
リスト
更新
ブラック
リスト
更新
ACL
更新
ACL
更新
ACL
更新
ACL
更新
国内未使用 IP
を吸い寄せる為の
プライベート AS

主な GFW ハードウェアベンダ

- 華為技術有限公司 (Huawei Technologies)
- 曙光信息産業有限公司 (Dawning Information Industry)

他

GFW の開発体制

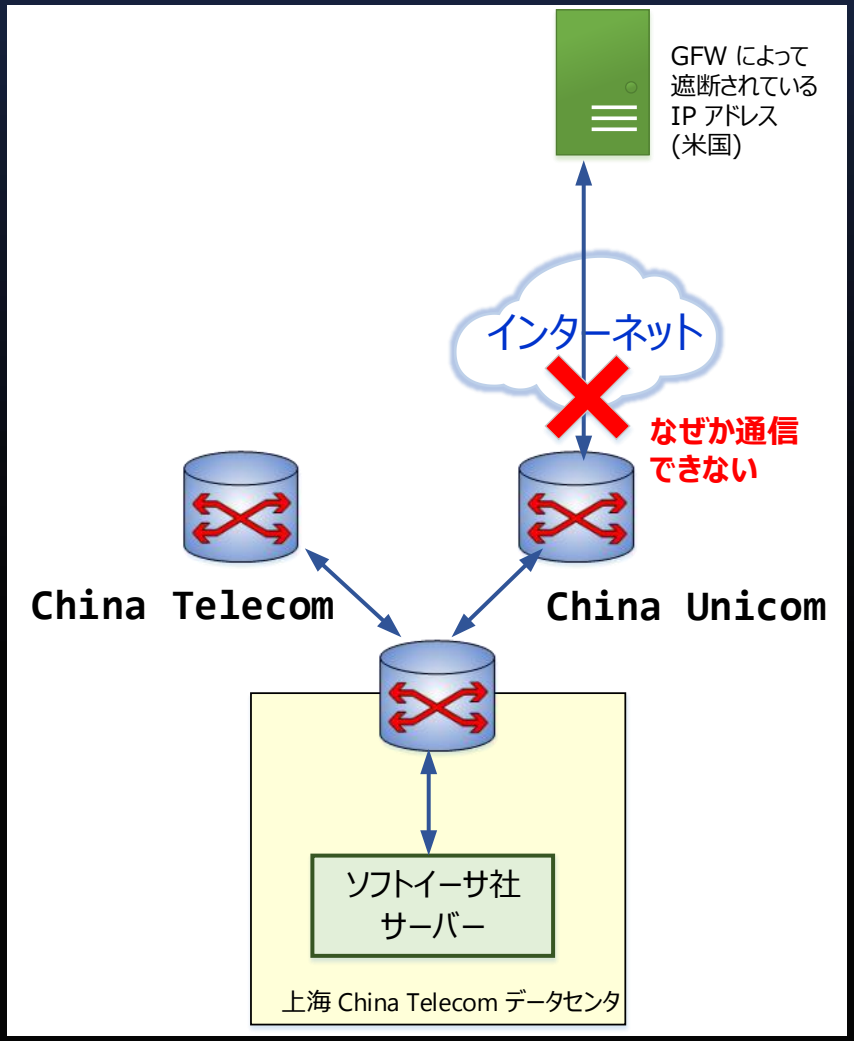
- 「中華人民共和国工業情報化部」の「国家コンピュータネットワーク・情報安全センター」が発注。
- 北京郵電大学の元学長の方濱興氏（Fang Binxing）がプロジェクトリーダーとして企画・開発。
- 現在、十数の大学において合計100人未満の大学院生や研究者によって継続的に実施。

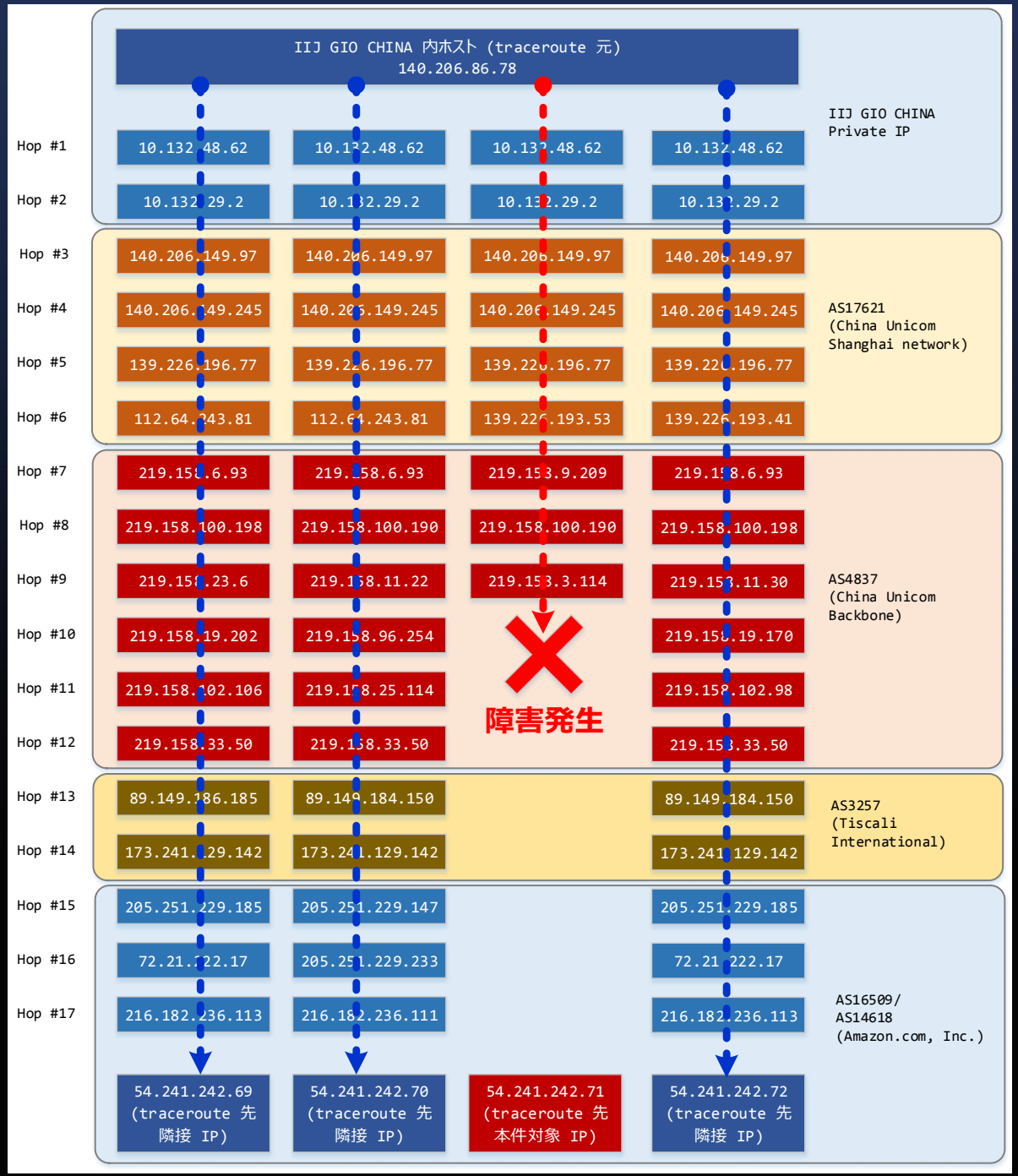
GFW は存在しない

- 中国政府の工業情報化部:
「政府によるファイアウォールというものは存在しない。ISP の装置の故障ではないか?」

- ISP:
「当社設備には故障は存在しない。通信断は、上流 ISP (China Unicom 社内) で発生しているのではないか?」

GFW 遮断を「故障」(＝契約違反)として China Unicom 社に修理を依頼してみる実験




IIJ GIO CHINA 内ホスト (traceroute 元)
140.206.86.78
IIJ GIO CHINA
Private IP
Hop #1
10.132.48.62
10.132.48.62
10.132.48.62
10.132.48.62
Hop #2
10.132.29.2
10.132.29.2
10.132.29.2
10.132.29.2
AS17621
(China Unicom
Shanghai network)
Hop #3
140.206.149.97
140.206.149.97
140.206.149.97
140.206.149.97
Hop #4
140.206.149.245
140.206.149.245
140.206.149.245
140.206.149.245
Hop #5
139.226.196.77
139.226.196.77
139.226.196.77
139.226.196.77
Hop #6
112.64.243.81
112.64.243.81
139.226.193.53
139.226.193.41
AS4837
(China Unicom
Backbone)
Hop #7
219.158.6.93
219.158.6.93
219.158.9.209
219.158.6.93
Hop #8
219.158.100.198
219.158.100.190
219.158.100.190
219.158.100.198
Hop #9
219.158.23.6
219.158.11.22
219.158.3.114
219.158.11.30
Hop #10
219.158.19.202
219.158.96.254
219.158.19.170
Hop #11
219.158.102.106
219.158.25.114
219.158.102.98
Hop #12
219.158.33.50
219.158.33.50
219.158.33.50
障害発生
AS3257
(Tiscali
International)
Hop #13
89.149.186.185
89.149.184.150
89.149.184.150
Hop #14
173.241.129.142
173.241.129.142
173.241.129.142
AS16509/
AS14618
(Amazon.com, Inc.)
Hop #15
205.251.229.185
205.251.229.147
205.251.229.185
Hop #16
72.21.222.17
205.251.229.233
72.21.222.17
Hop #17
216.182.236.113
216.182.236.111
216.182.236.113
54.241.242.69
(traceroute 先
隣接 IP)
54.241.242.70
(traceroute 先
隣接 IP)
54.241.242.71
(traceroute 先
本件対象 IP)
54.241.242.72
(traceroute 先
隣接 IP)

China Unicom 社からの正式回答

- 「該当IPアドレスの疎通の問題については回答できかねる」

GFW の設置方法

- 海外 ISP に直結している商用 ISP は事実上、以下の国有会社 3 社のみ。
  - China Unicom (中国联通)
    AS4837 内に GFW を設置
  - China Telecom (中国电信)
    AS4134 内に GFW を設置
  - China Mobile (中国移動)
    AS8453/AS9394 内に GFW を設置
- その他研究機関
  - AS4538: China Education and Research Network Center)、AS37944 (CHINA SCIENCE AND TECHNOLOGY NETWORK 等も海外 ISP に直結している
- 中国政府の工業情報化部による国際回線の開設時の免許の条件として、GFW を経由した接続義務付けているのではないか?

http://os.51cto.com/art/201009/228379_all.htm

(GFW 設備のイメージ図)

VPN Gate

http://www.vpngate.net/

A Volunteer-Organized Public VPN Relay System
with Blocking Resistance for
Bypassing Government Censorship Firewalls

Daiyuu Nobori and Yasushi Shinjo
Department of Computer Science,
University of Tsukuba, Japan

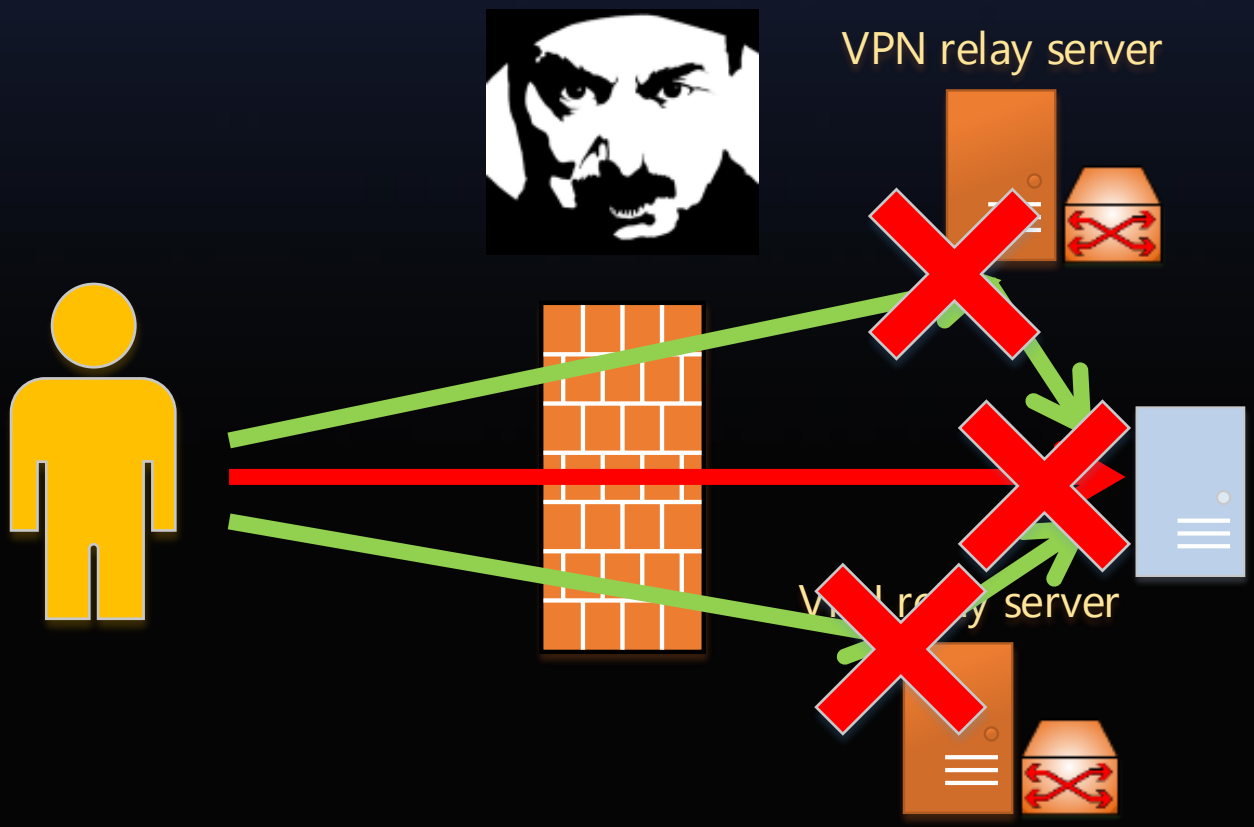
筑波大学
University of Tsukuba

Introduction

- Censorship firewalls restrict Internet access.
  - Great Firewall of China (GFW) is well-known.
- Using relay servers is a popular way to bypass government firewalls.
- Public relays help people behind firewalls to access to the free Internet.
  - Public VPN services
  - Open proxies
  - Tor nodes

Existing problem of public relays

- The censorship authority can easily find public relays and block them soon.



Achieving blocking resistance is difficult

- Blocking resistance:
  - Web MIXes [Berthold 2001]
  - Ignoring the Great Firewall of China [Clayton 2006]
  - Infranet [Feamster 2002]
  - Thwarting web censorship with untrusted messenger discovery [Feamster 2003]
  - How to achieve blocking resistance for existing systems enabling anonymous web surfing [Köpsell 2004]

- Blocking activities by censors:
  - Great Firewall Tor probing Circa 09 [Wilde 2011]
  - How the great firewall of china is blocking Tor [Winter 2012]

Our Goal of VPN Gate

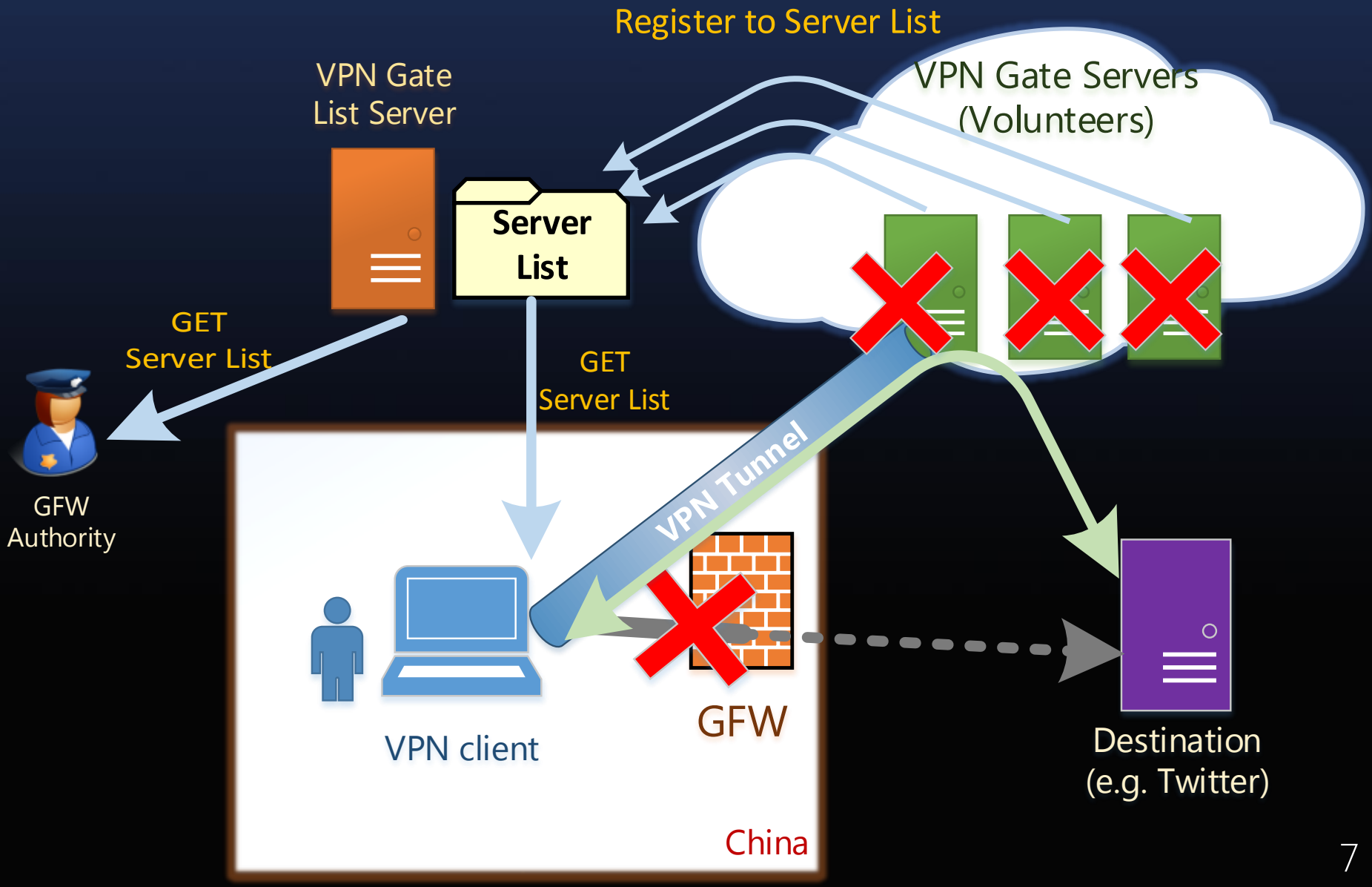
- Make a public VPN relay system with strong blocking resistance against censorship firewalls.

- We have chosen the Great Firewall of China as the first primary target.
  - Because GFW is the most advanced large-scale firewall.

VPN Gate's approach

1. Organize thousands of volunteer relays.
   - Authorities must block all IP addresses.

How we organize volunteers

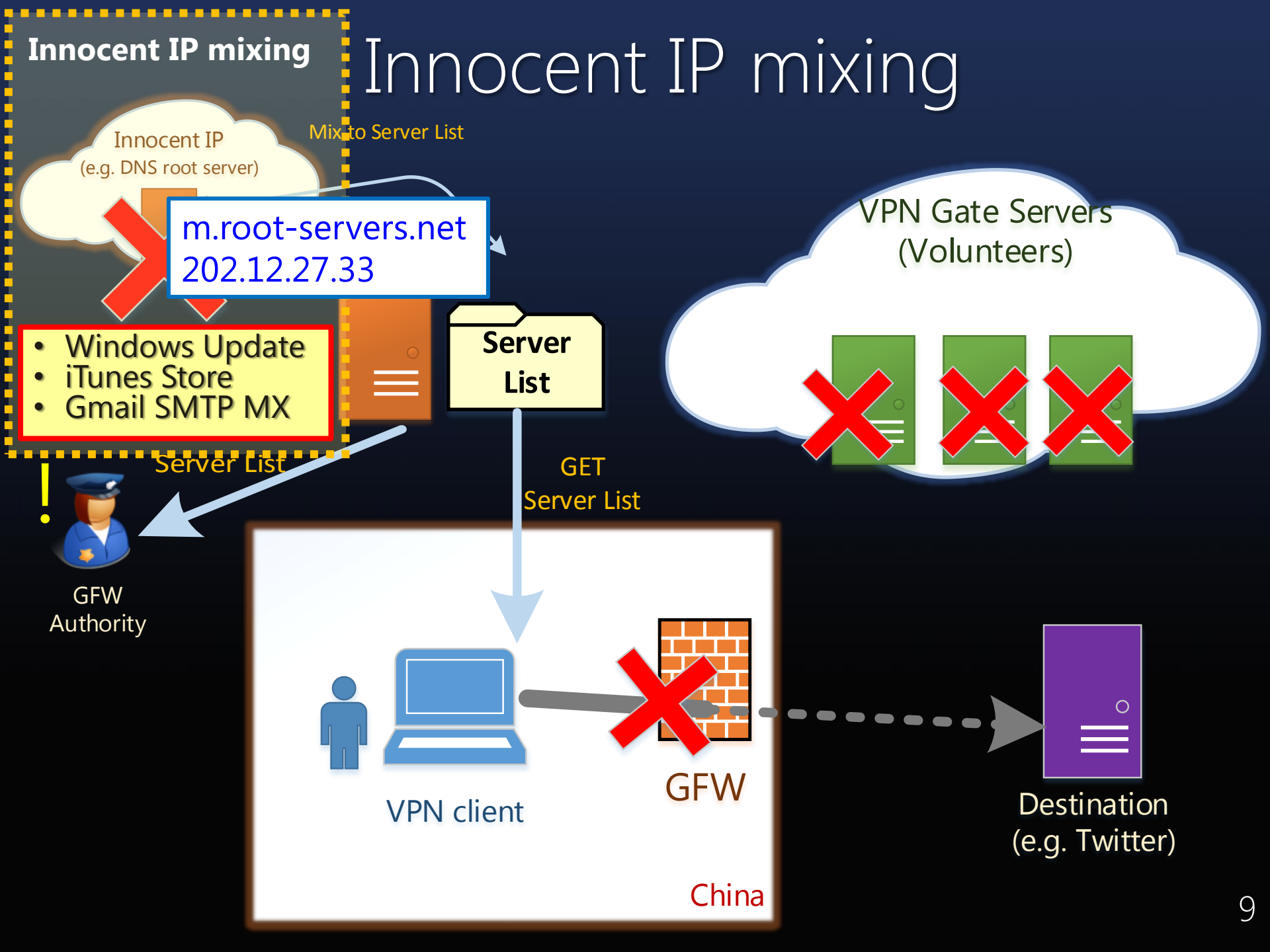


VPN Gate's approach

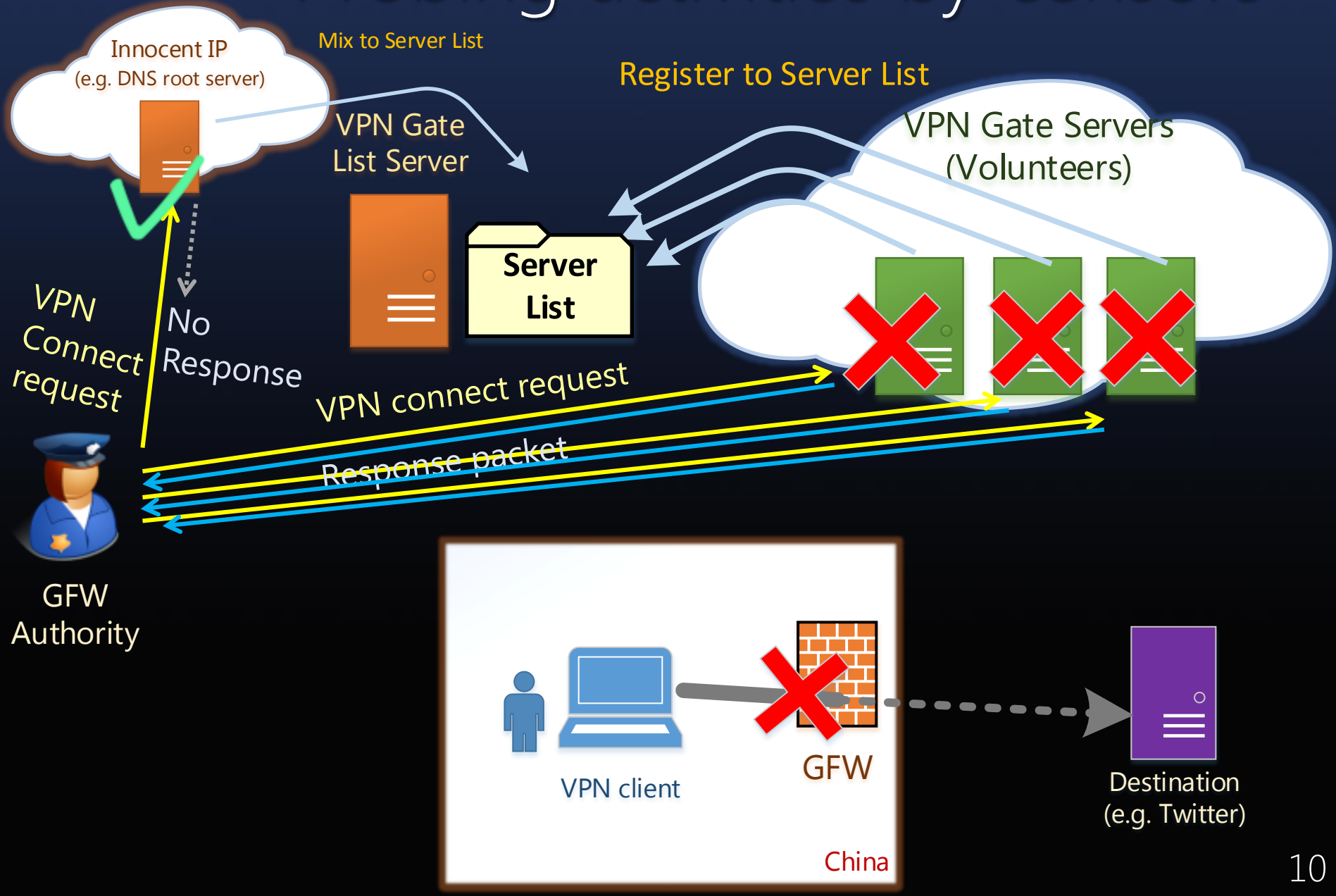
1. Organize thousands of volunteer relays.
   - Authorities must block all IP addresses.

2. Innocent IP mixing technique.
   - Enforce authorities to probe all IPs.

Innocent IP mixing



Probing activities by censors



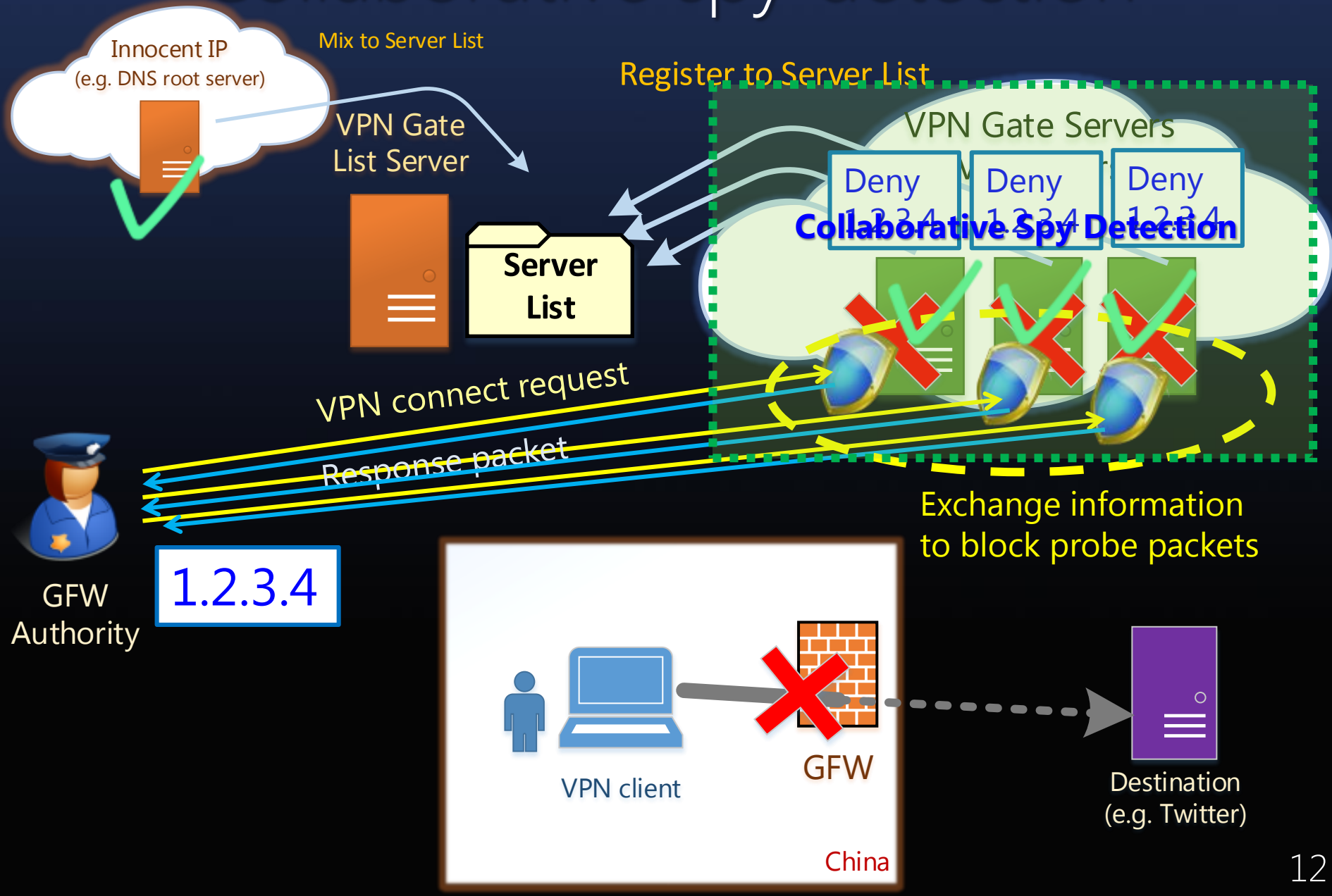
VPN Gate's approach

1. Organize thousands of volunteer relays.
   - Authorities must block all IP addresses.

2. Innocent IP mixing technique.
   - Enforce authorities to probe all IPs.

3. Collaborative spy detection technique.
   - Disallow authorities to complete the probing task.

Collaborative spy detection



Implementation

How to increase the number of VPN Gate volunteer servers

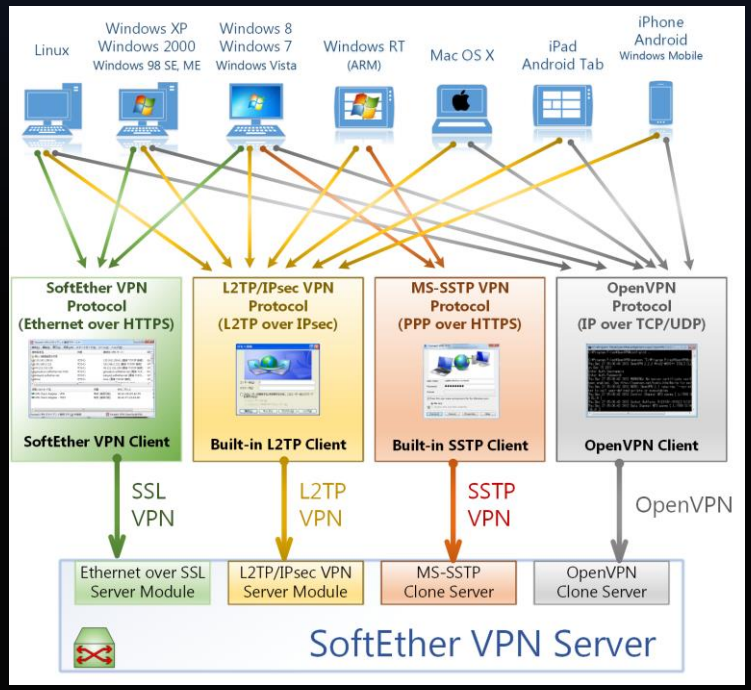
- Installation of the relay program must be easy.
  - It allows casual users to become volunteers.
- The relay program must support running behind NATs.
  - 70% of volunteers are behind NATs.

The VPN Gate Server program

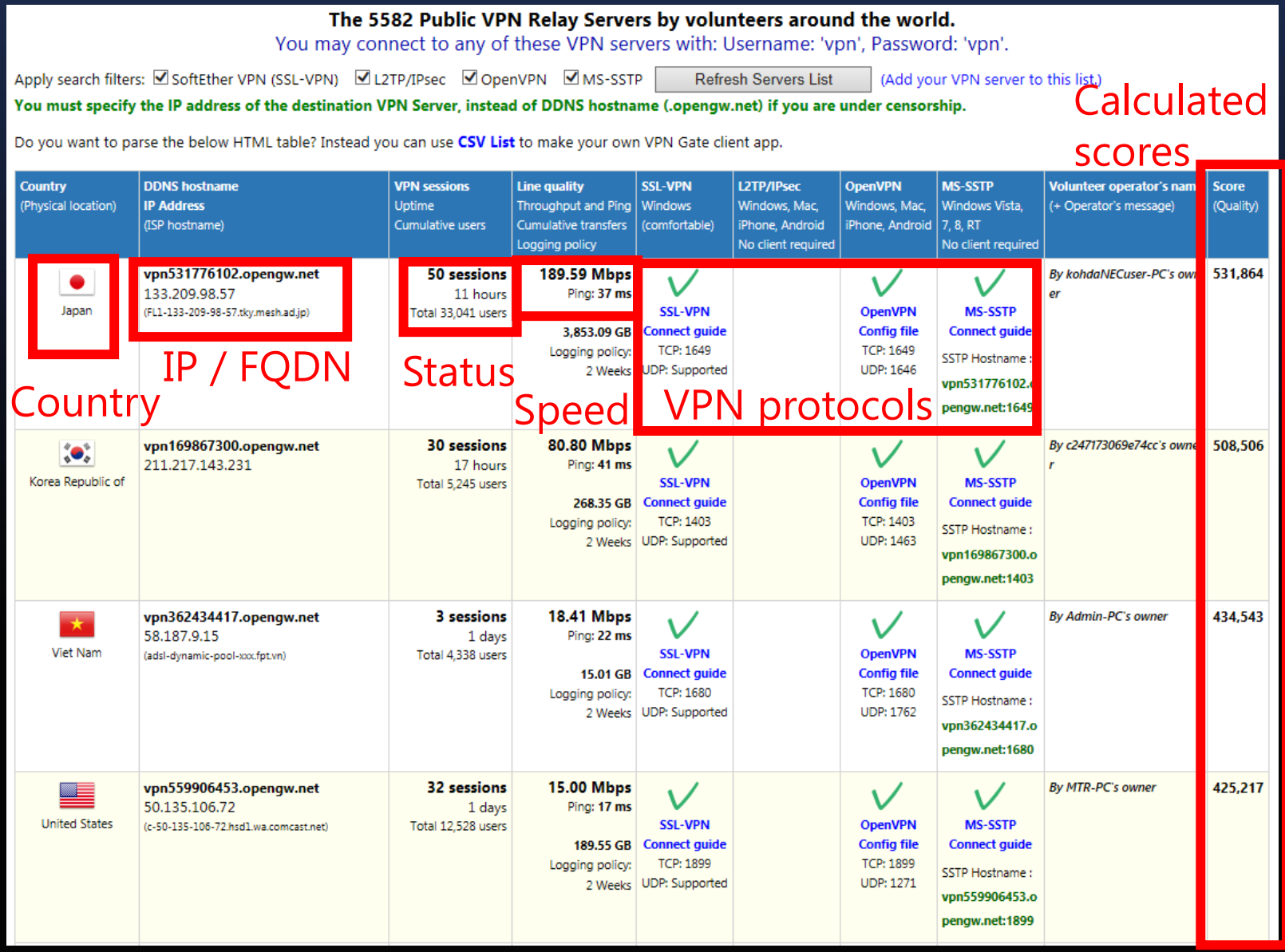
VPN Gate Server supports:

- Multi-VPN protocols
  - L2TP/IPsec
  - OpenVPN
  - Microsoft SSTP
  - SSL-VPN
- NAT Traversal
  - Universal Plug & Play
  - UDP hole punching

Based on our another project
SoftEther VPN Server
http://www.softether.org/



VPN Gate List Server (directory server)



The 5582 Public VPN Relay Servers by volunteers around the world.

You may connect to any of these VPN servers with: Username: 'vpn', Password: 'vpn'.

Apply search filters: ☑ SoftEther VPN (SSL-VPN) ☑ L2TP/IPsec ☑ OpenVPN ☑ MS-SSTP [Refresh Servers List] (Add your VPN server to this list.)

You must specify the IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are under censorship.

Do you want to parse the below HTML table? Instead you can use **CSV List** to make your own VPN Gate client app.

Calculated scores

Country (Physical location)	DDNS hostname / IP Address (ISP hostname)	VPN sessions / Uptime / Cumulative users	Line quality / Throughput and Ping / Cumulative transfers / Logging policy	SSL-VPN Windows (comfortable)	L2TP/IPsec Windows, Mac, iPhone, Android No client required	OpenVPN Windows, Mac, iPhone, Android	MS-SSTP Windows Vista, 7, 8, RT No client required	Volunteer operator's nam (+ Operator's message)	Score (Quality)
Japan	**vpn531776102.opengw.net** 133.209.98.57 (FL1-133-209-98-57.tky.mesh.ad.jp)	**50 sessions** 11 hours Total 33,041 users	**189.59 Mbps** Ping: **37 ms** **3,853.09 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1649 UDP: Supported		✓ OpenVPN Config file TCP: 1649 UDP: 1646	✓ MS-SSTP Connect guide SSTP Hostname : vpn531776102. pengw.net:1649	*By kohdaNECuser-PC's owner*	**531,864**
Korea Republic of	**vpn169867300.opengw.net** 211.217.143.231	**30 sessions** 17 hours Total 5,245 users	**80.80 Mbps** Ping: **41 ms** **268.35 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1403 UDP: Supported		✓ OpenVPN Config file TCP: 1403 UDP: 1463	✓ MS-SSTP Connect guide SSTP Hostname : vpn169867300.o pengw.net:1403	*By c247173069e74cc's owner*	**508,506**
Viet Nam	**vpn362434417.opengw.net** 58.187.9.15 (adsl-dynamic-pool-xxx.fpt.vn)	**3 sessions** 1 days Total 4,338 users	**18.41 Mbps** Ping: **22 ms** **15.01 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1680 UDP: Supported		✓ OpenVPN Config file TCP: 1680 UDP: 1762	✓ MS-SSTP Connect guide SSTP Hostname : vpn362434417.o pengw.net:1680	*By Admin-PC's owner*	**434,543**
United States	**vpn559906453.opengw.net** 50.135.106.72 (c-50-135-106-72.hsd1.wa.comcast.net)	**32 sessions** 1 days Total 12,528 users	**15.00 Mbps** Ping: **17 ms** **189.55 GB** Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 1899 UDP: Supported		✓ OpenVPN Config file TCP: 1899 UDP: 1271	✓ MS-SSTP Connect guide SSTP Hostname : vpn559906453.o pengw.net:1899	*By MTR-PC's owner*	**425,217**

Country

IP / FQDN

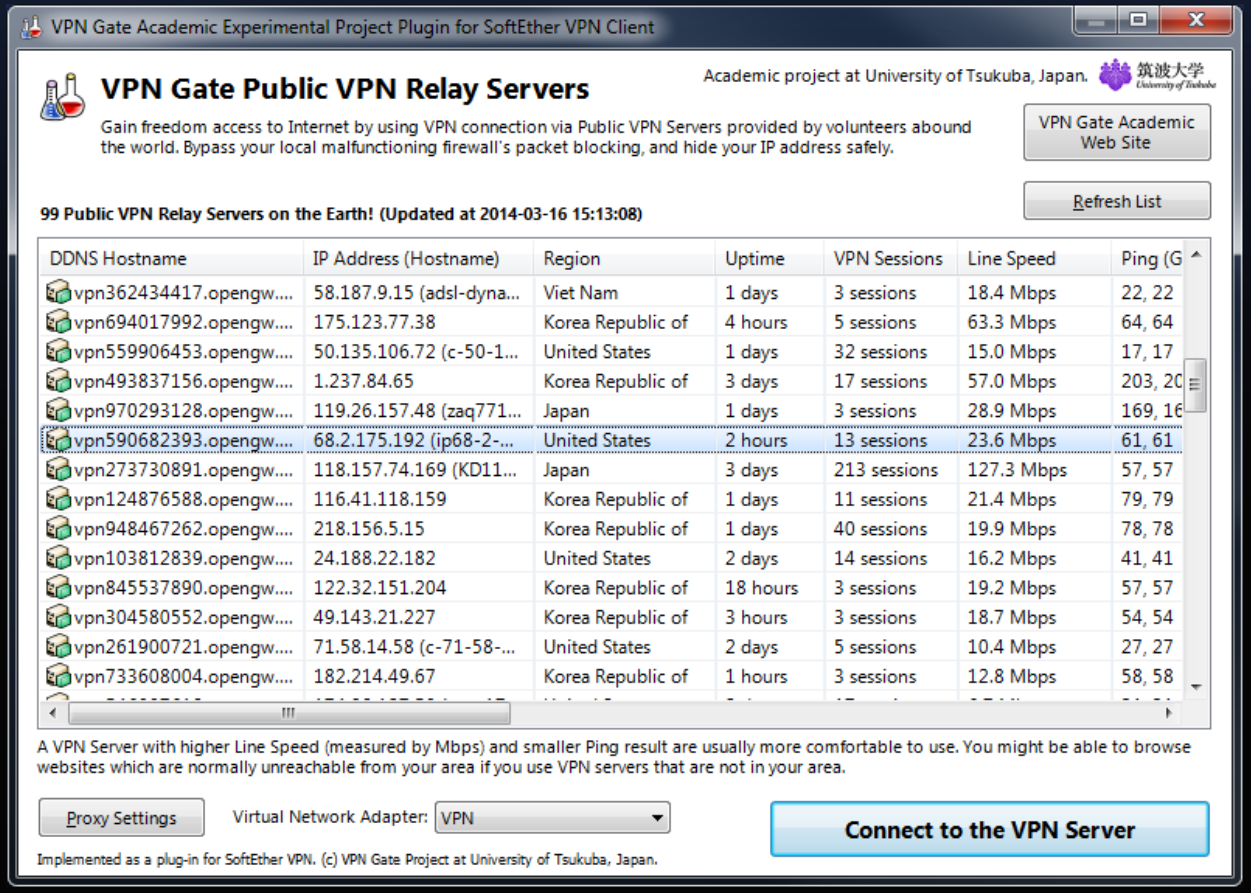
Status

Speed

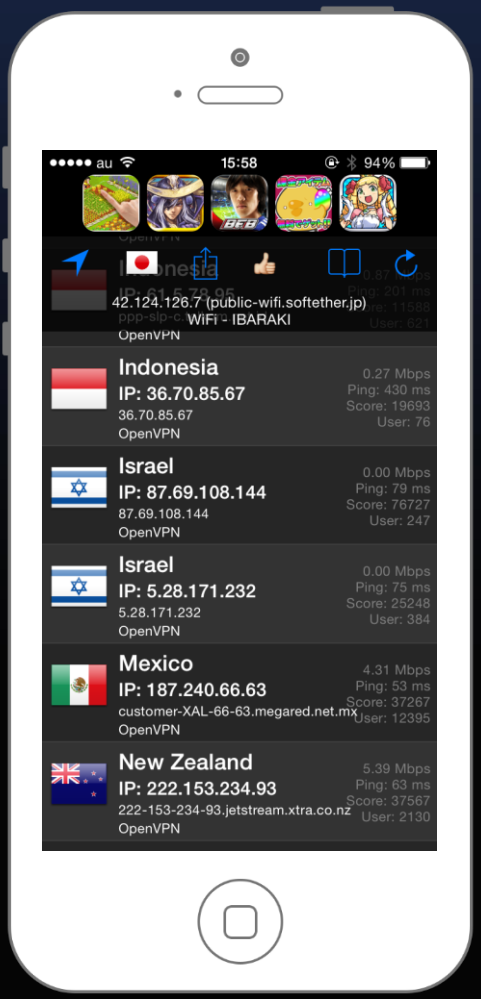
VPN protocols

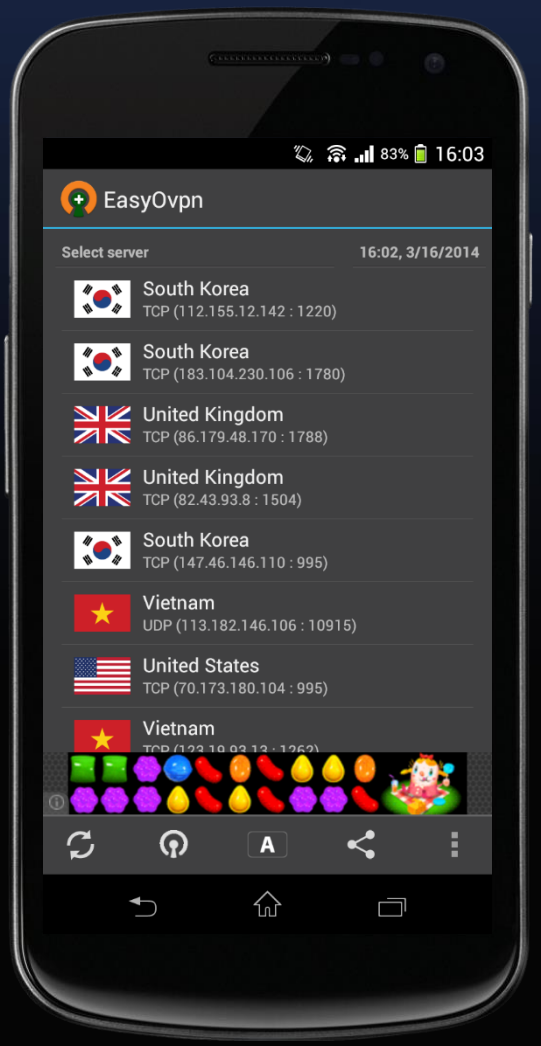
VPN Gate Client for Windows

- One click to connect to a VPN Gate Server.



VPN Gate Clients for iOS and Android (by 3rd parties)

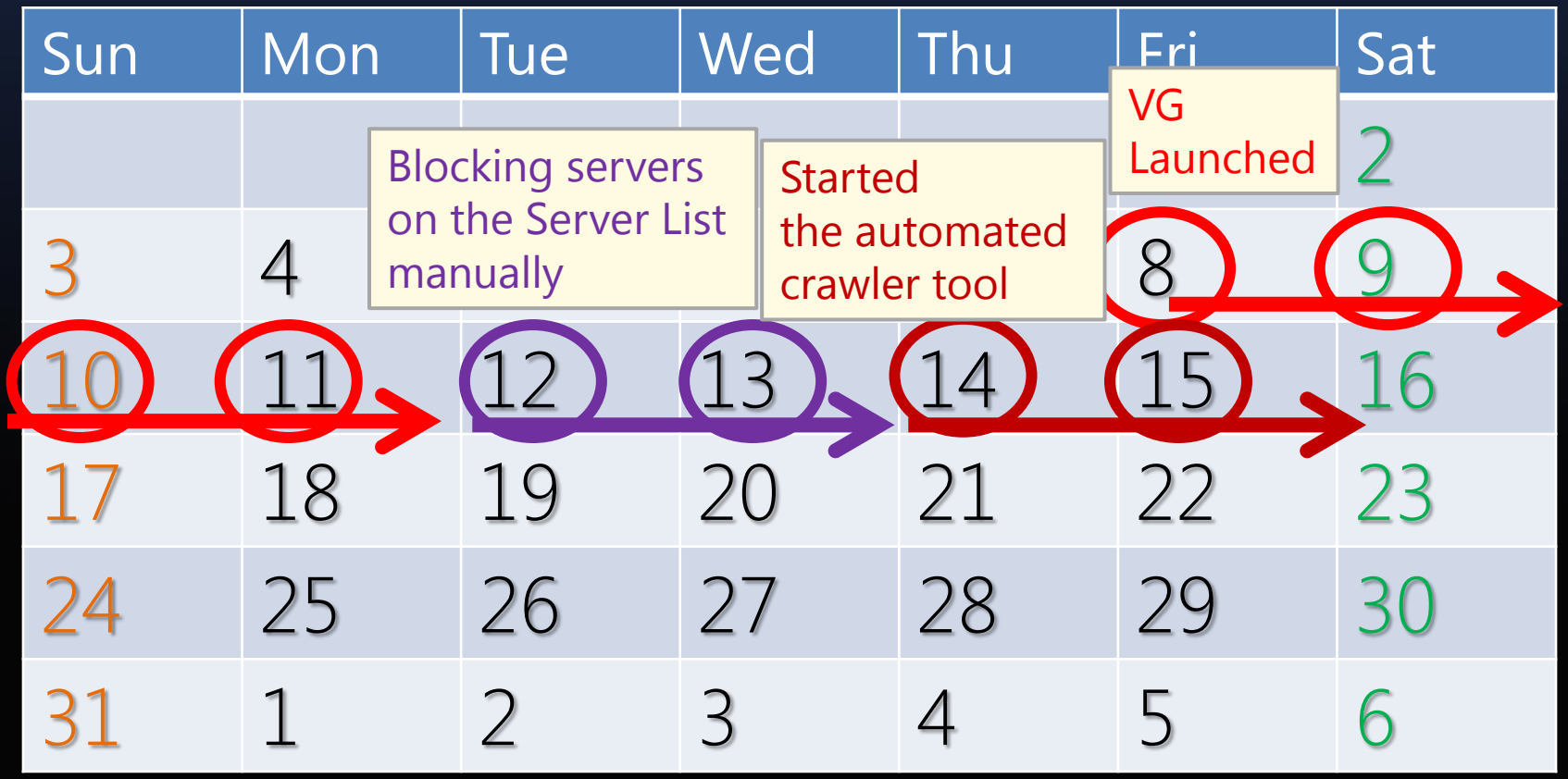




Launched on March 8, 2013
http://www.vpngate.net/

The response of GFW authority

March 2013



The authority developed the crawler in Python

Chinese GFW Authority

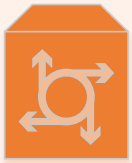
Running 24h (every 5 mins)

HTML Crawler & Table Parser

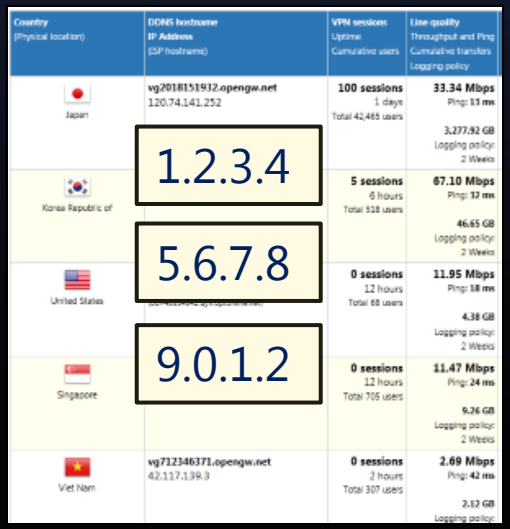
HTTP GET

Automatic IP Blacklist Update

```
body = Get("http://www.vpngate.net/");
servers_list = ParseTable(body);

foreach (server_ip in servers_list)
{
        firewall.Insert(server_ip);
}
```



Government's Black-hole Router



www.vpngate.net VPN Gate Servers List HTML table

VPN Gate List Server access log

ID	Access Date	Client FQDN	URL	User Agent
3312453	3/23/13 7:40 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3312674	3/23/13 7:41 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3313385	3/23/13 7:45 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3313579	3/23/13 7:46 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3314469	3/23/13 7:50 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3314708	3/23/13 7:51 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3315395	3/23/13 7:55 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3315642	3/23/13 7:56 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3316252	3/23/13 8:00 PM	198-136-27-242.static.gorillaservers.com	http://www.vpngate.net/cn/	Python-urllib/1.17
3316383	3/23/13 8:00 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3316570	3/23/13 8:01 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3317306	3/23/13 8:05 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3317533	3/23/13 8:07 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3318339	3/23/13 8:10 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3318553	3/23/13 8:12 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3319072	3/23/13 8:15 PM	198-136-27-242.static.gorillaservers.com	http://www.vpngate.net/cn/	Python-urllib/1.17
3319236	3/23/13 8:15 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3319480	3/23/13 8:17 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3320192	3/23/13 8:20 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3320439	3/23/13 8:22 PM	ec2-50-16-163-135.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17
3321185	3/23/13 8:26 PM	ec2-23-20-4-19.compute-1.amazonaws.com	http://www.vpngate.net/en/	Python-urllib/1.17

GFW authority was trusting our Server List at this time

Chinese GFW Authority

Running 24h (every 5 mins)

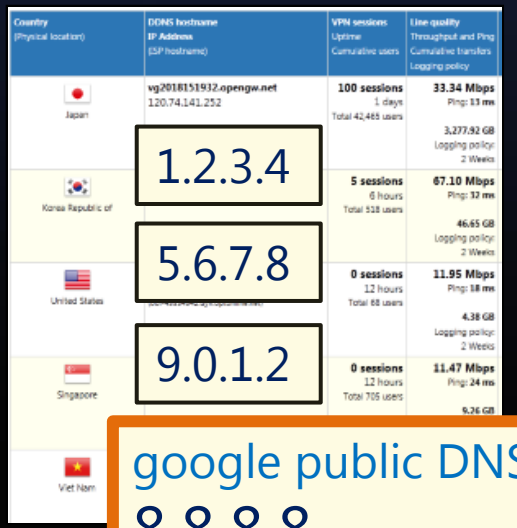
HTML Crawler & Table Parser

HTTP GET

Automatic IP Blacklist Update

```
body = Get("http://www.vpngate.net/");
servers_list = ParseTable(body);

foreach (server_ip in servers_list)
{
        firewall.Insert(server_ip);
}
```

Government's Black-hole Router



google public DNS 8.8.8.8

VPN Gate Servers List HTML table

* This innocent IP address is an example.

GFW blocked the innocent IP in 30 mins

From the computer in China:

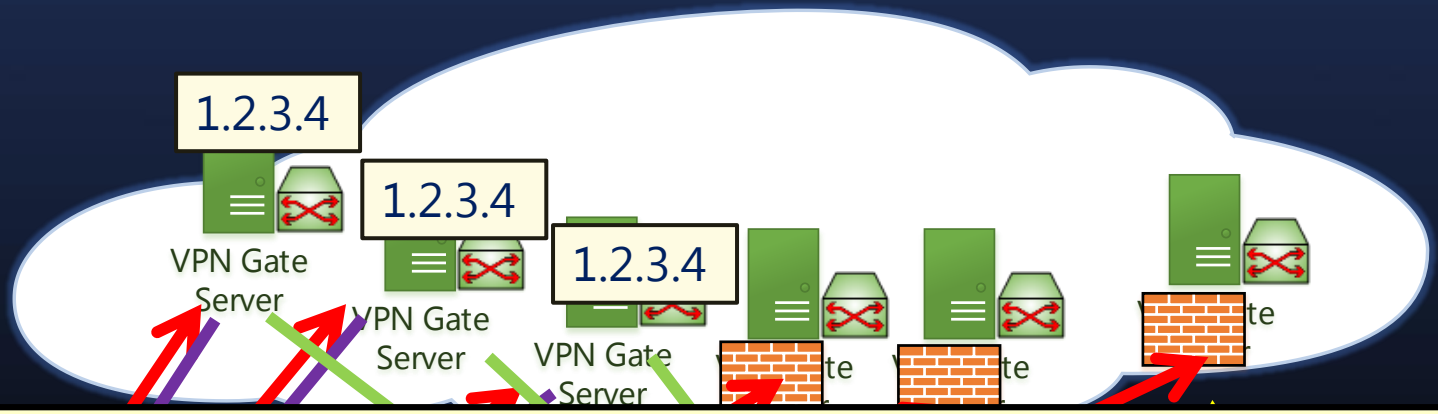
```
>ping 8.8.8.8
Pinging google-public-dns-a.google.com [8.8.8.8] with 32
bytes of data:

Reply from 8.8.8.8: bytes=32 time=159ms TTL=238
Reply from 8.8.8.8: bytes=32 time=143ms TTL=238
Reply from 8.8.8.8: bytes=32 time=141ms TTL=238
Reply from 8.8.8.8: bytes=32 time=148ms TTL=238
Reply from 8.8.8.8: bytes=32 time=144ms TTL=238
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Great Firewall was under our control !

* This innocent IP address is an example.

The GFW authority improved the crawler to probe all IPs.

Collaborative spy detection avoids probing

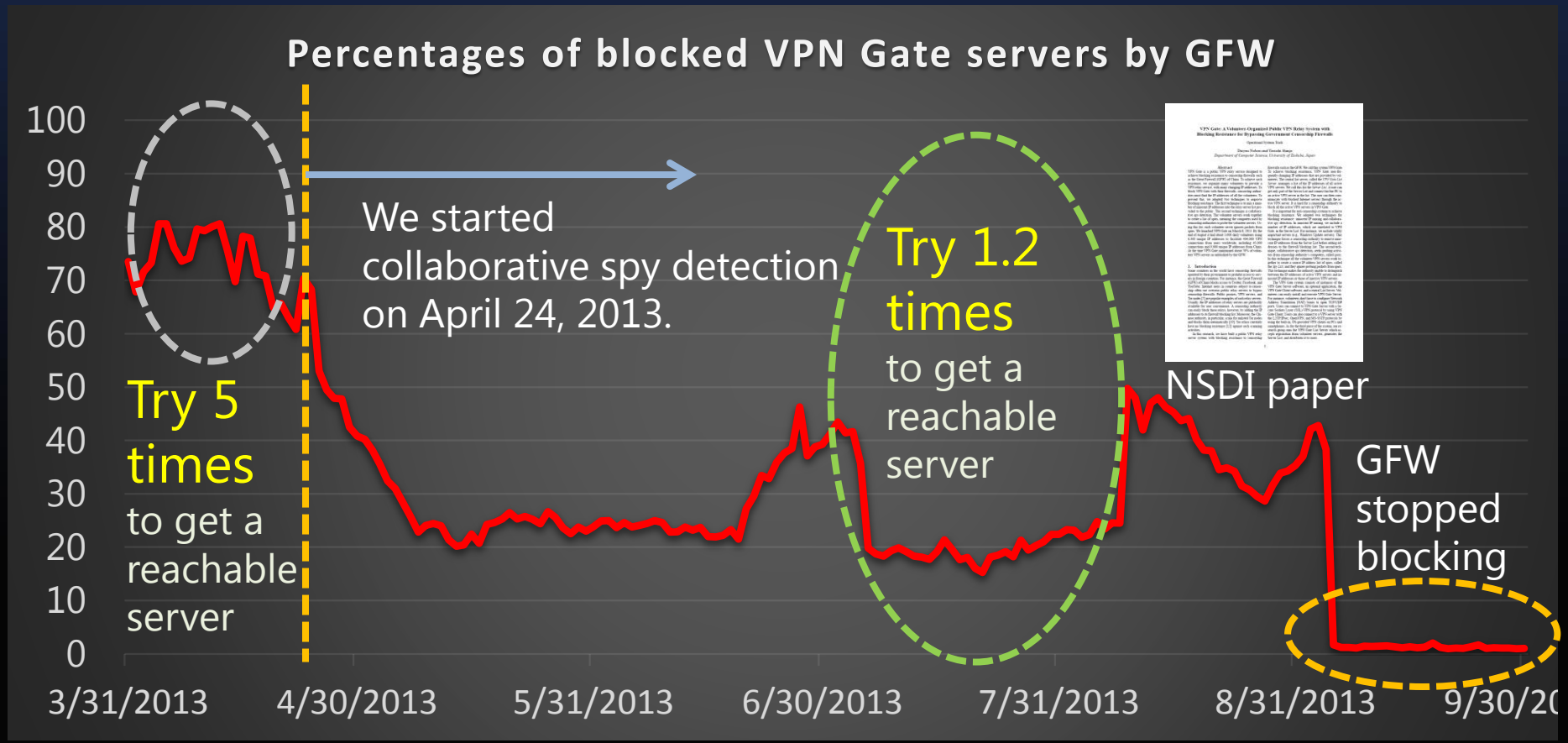


The log analyzer detect spies by looking up source IPs matches to:

1. A single IP address or IP subnet connected to many VPN servers around the same time.
2. The amount of data transfer is too small or the duration is too short.
3. Mixing other complex algorithms.

See our papers for more details.

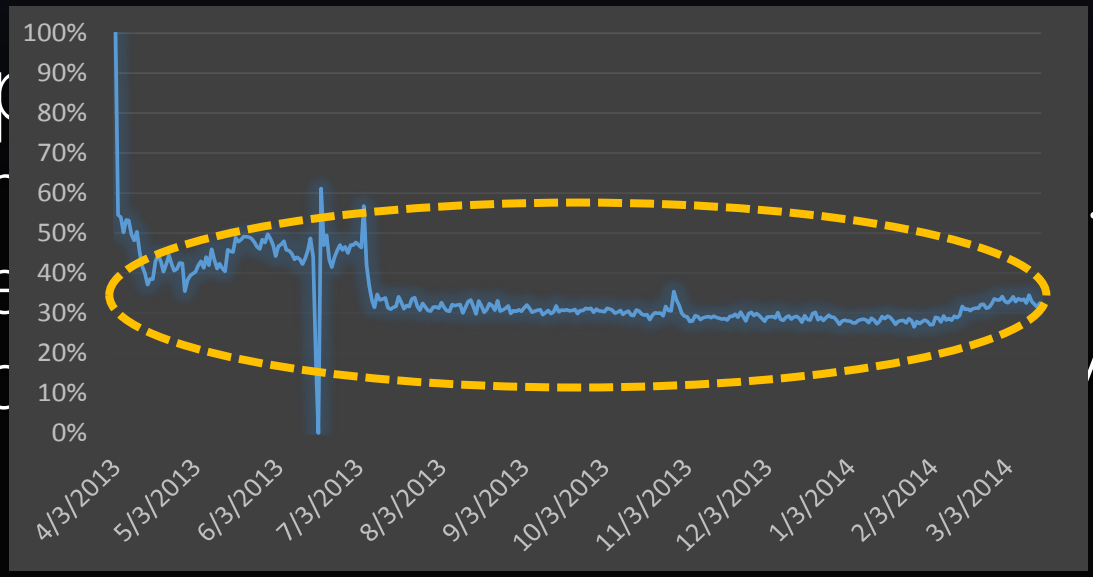
Collaborative spy detection works effectively since April 24, 2013



Why GFW stopped blocking VPN Gate? (hypothesis)

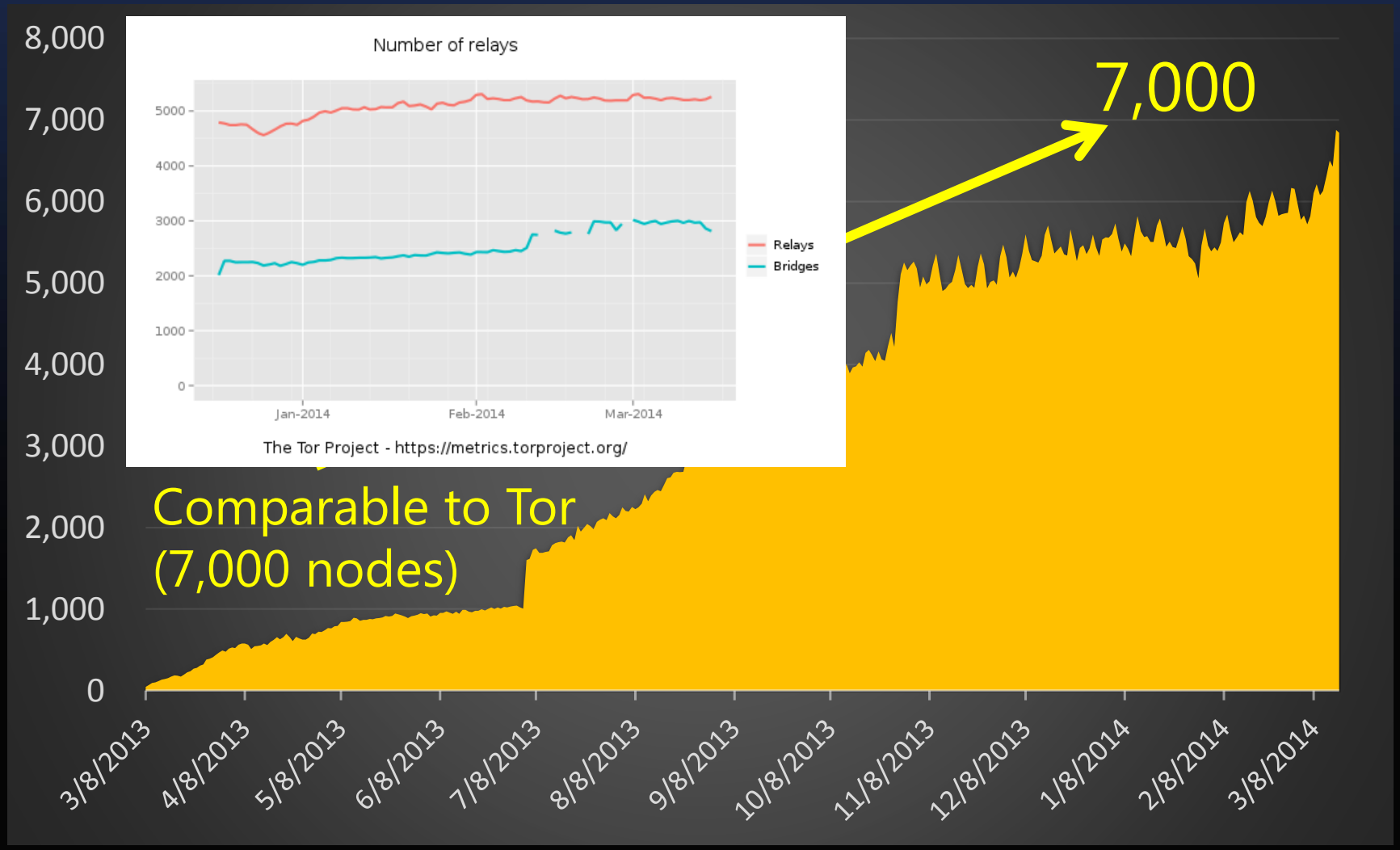
- In August we had 6,000 daily unique server IP addresses.
  - 2,400 (40% of 6,000) new server IP addresses everyday.
  - 17,000 new IP addresses per week.

- We supp
  - GFW r
  - GFW e
  - GFW c

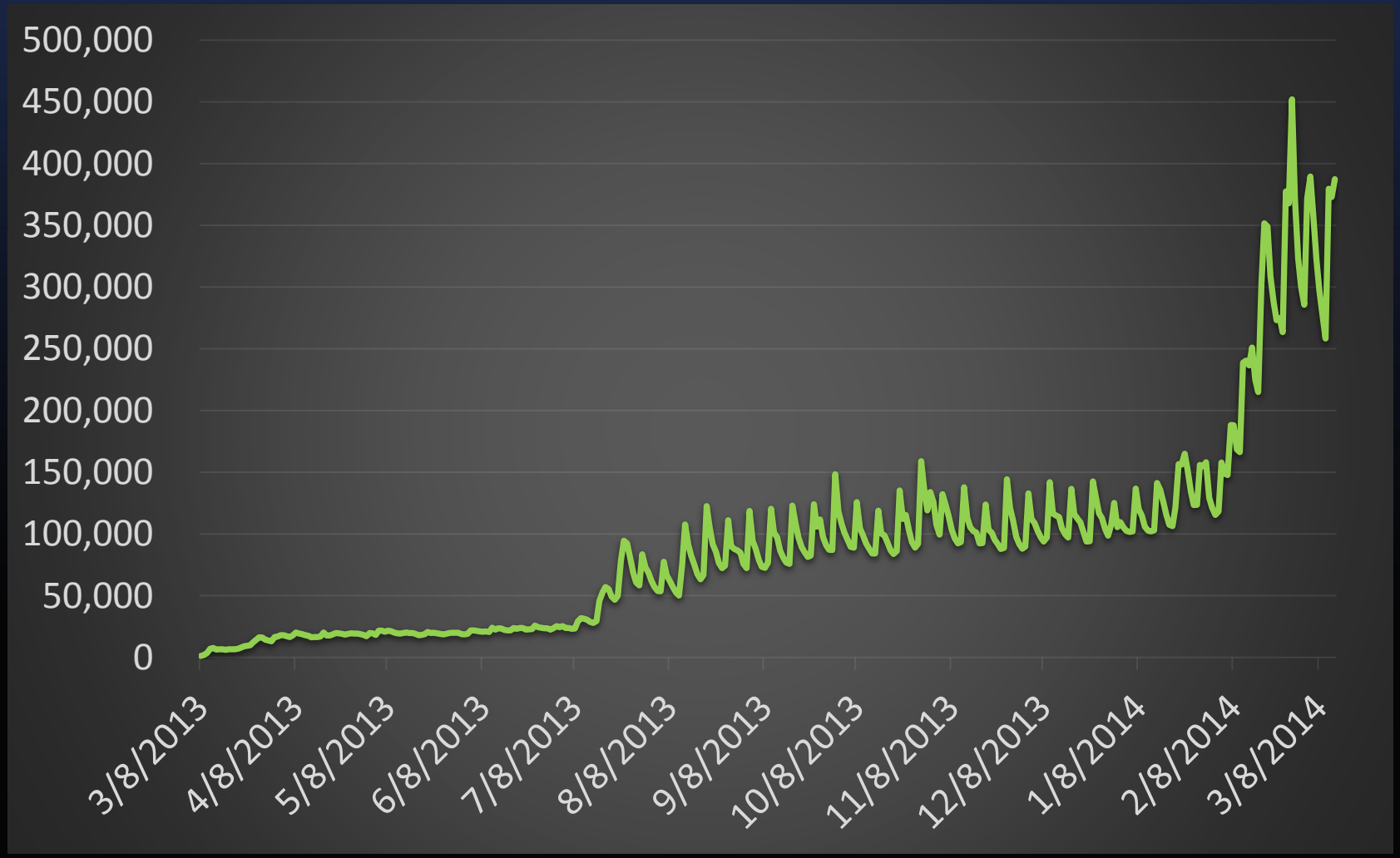


VPN Gate.

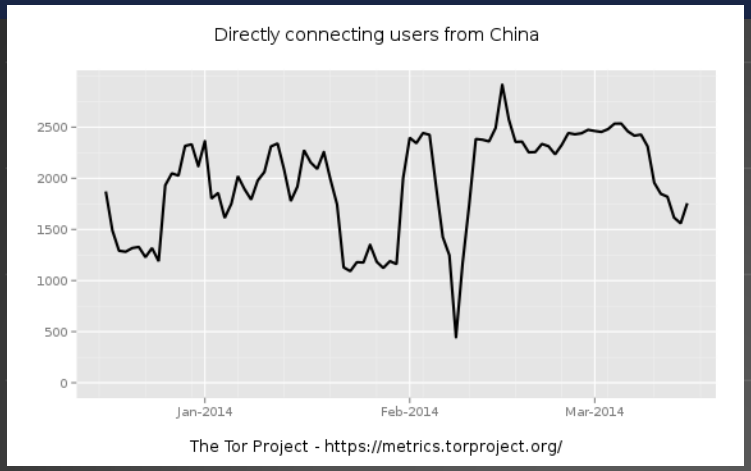
Numbers of active VPN Gate Servers



400,000 daily unique client IPs, world wide



32,000 daily unique client IPs from China



13 times to Tor
(estimated 2,500 users)

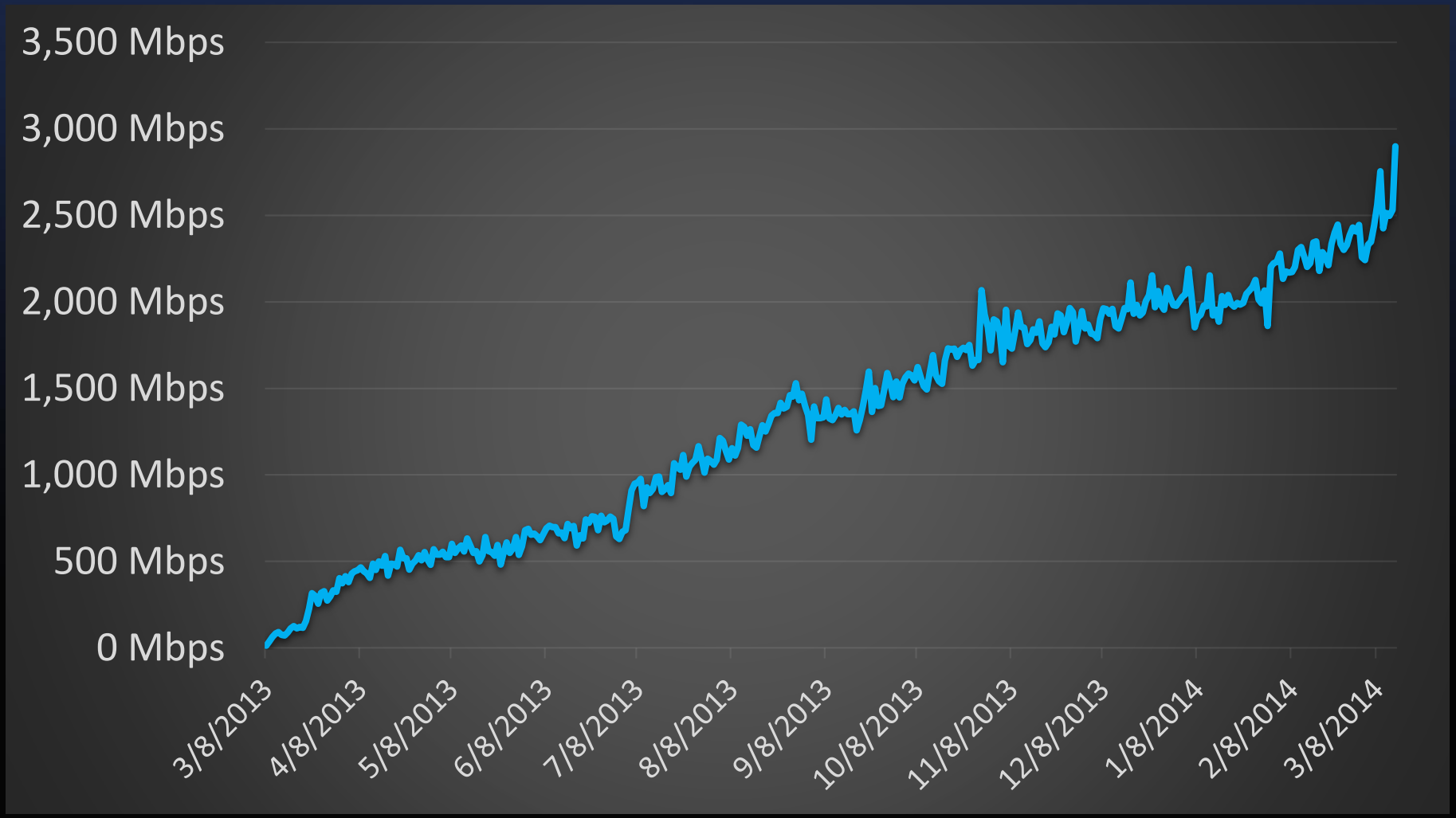
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0

3/8/2013
4/8/2013
5/8/2013
6/8/2013
7/8/2013
8/8/2013
9/8/2013
10/8/2013
11/8/2013
12/8/2013
1/8/2014
2/8/2014
3/8/2014

16,000 daily unique client IPs from Iran

75	Algeria	1,224.2 GB	48,356
76	Latvia	975.3 GB	11,002
77	Comoros	920.5 GB	12,655
78	Korea Democratic People's Republic of	906.8 GB	27,478
79	Lebanon	852.5 GB	13,563
80	Albania	821.2 GB	19,726
81	Serbia	807.7 GB	17,582

VPN Gate's total bandwidth is approaching to 3Gbps



Discussion and Conclusion

Comparison between Tor and VPN Gate

- Tor
  - 7,000 relays
  - 2,500 unique users from China
  - Port forwarding (only TCP)
  - Multi hops
  - Anonymizer
  - Limited FW resistance
- VPN Gate
  - 7,000 relays
  - 32,000 unique users from China
  - VPN tunneling (TCP/UDP/ICMP)
  - Single hop
  - Not an anonymizer
  - Strong FW resistance

https://metrics.torproject.org/

Conclusion

VPN Gate adopted the combination of the three techniques

1. Employ a large number of IP addresses with frequently changing.
   (by volunteered system)

2. Enforce the censor to probe all IP addresses in advance to block.
   (by innocent IP mixing)

3. Make the censor difficult to perform probing.
   (by collaborative Spy detection)

People help oversea people

People in
censored Internet

VPN makes
friendship

People in
free Internet