

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)

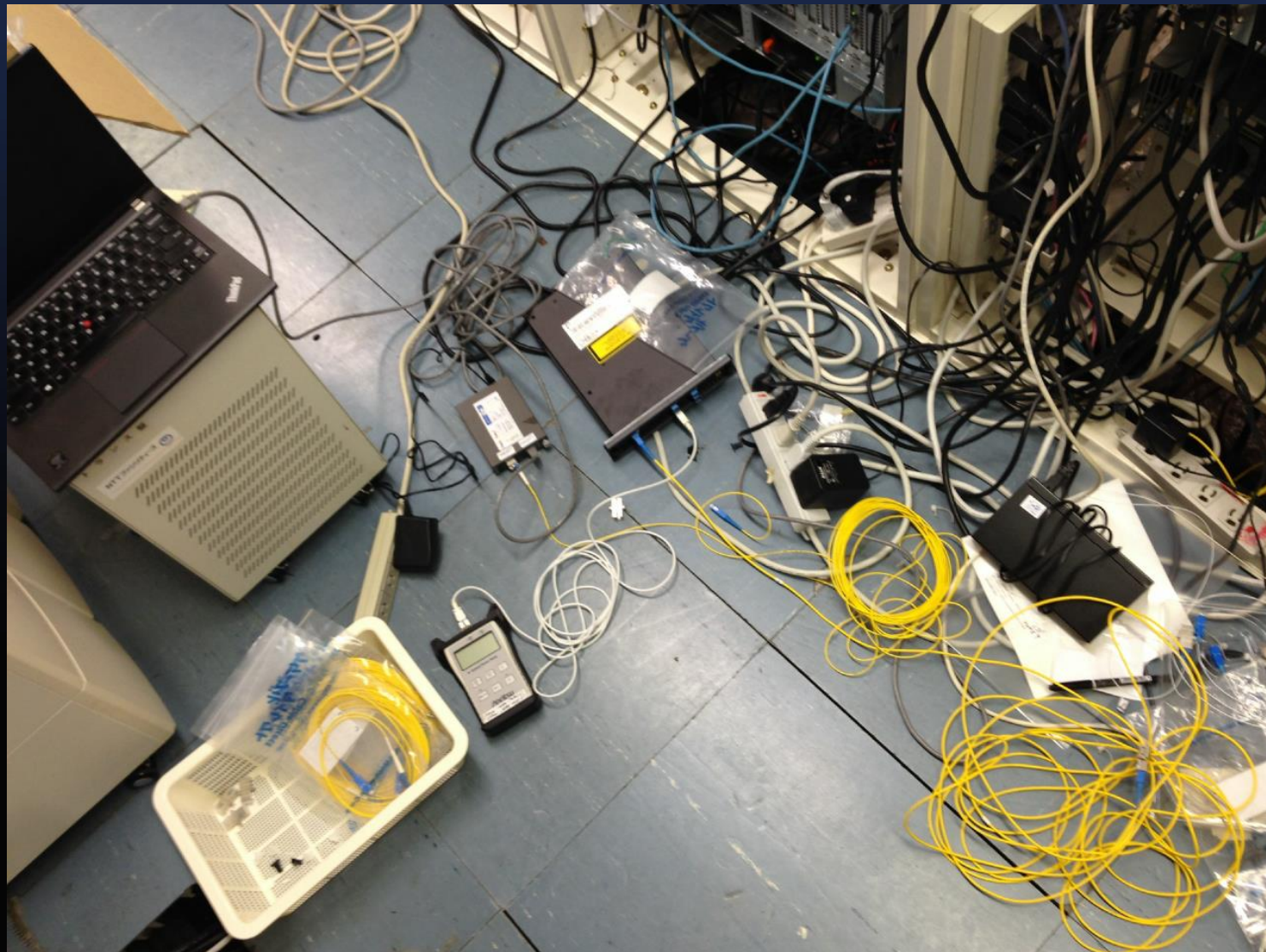
筑波大学大学院システム情報工学研究科
博士後期課程に入院中

ソフトイーサ株式会社 代表取締役

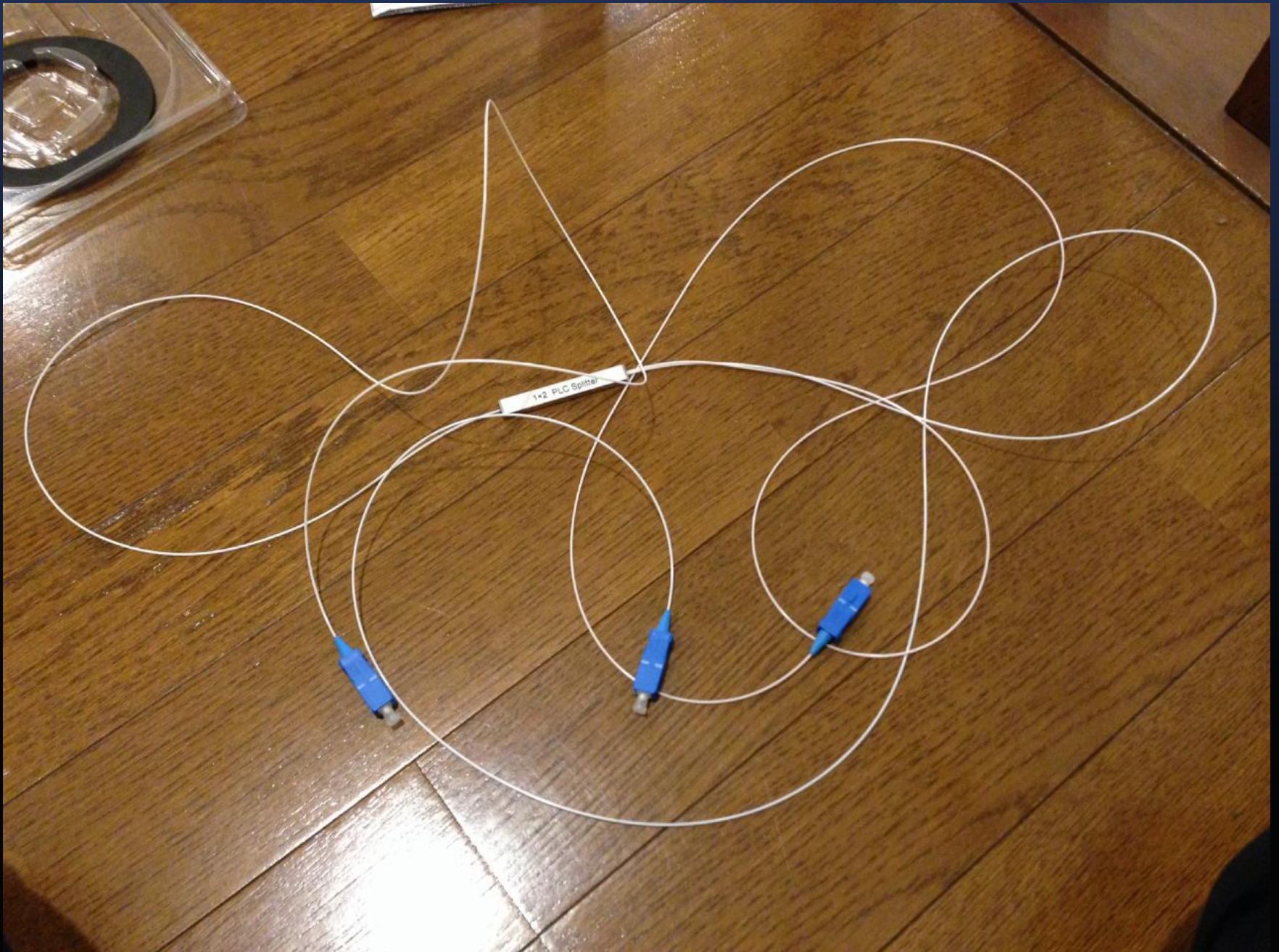
登大遊 自己紹介

- 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

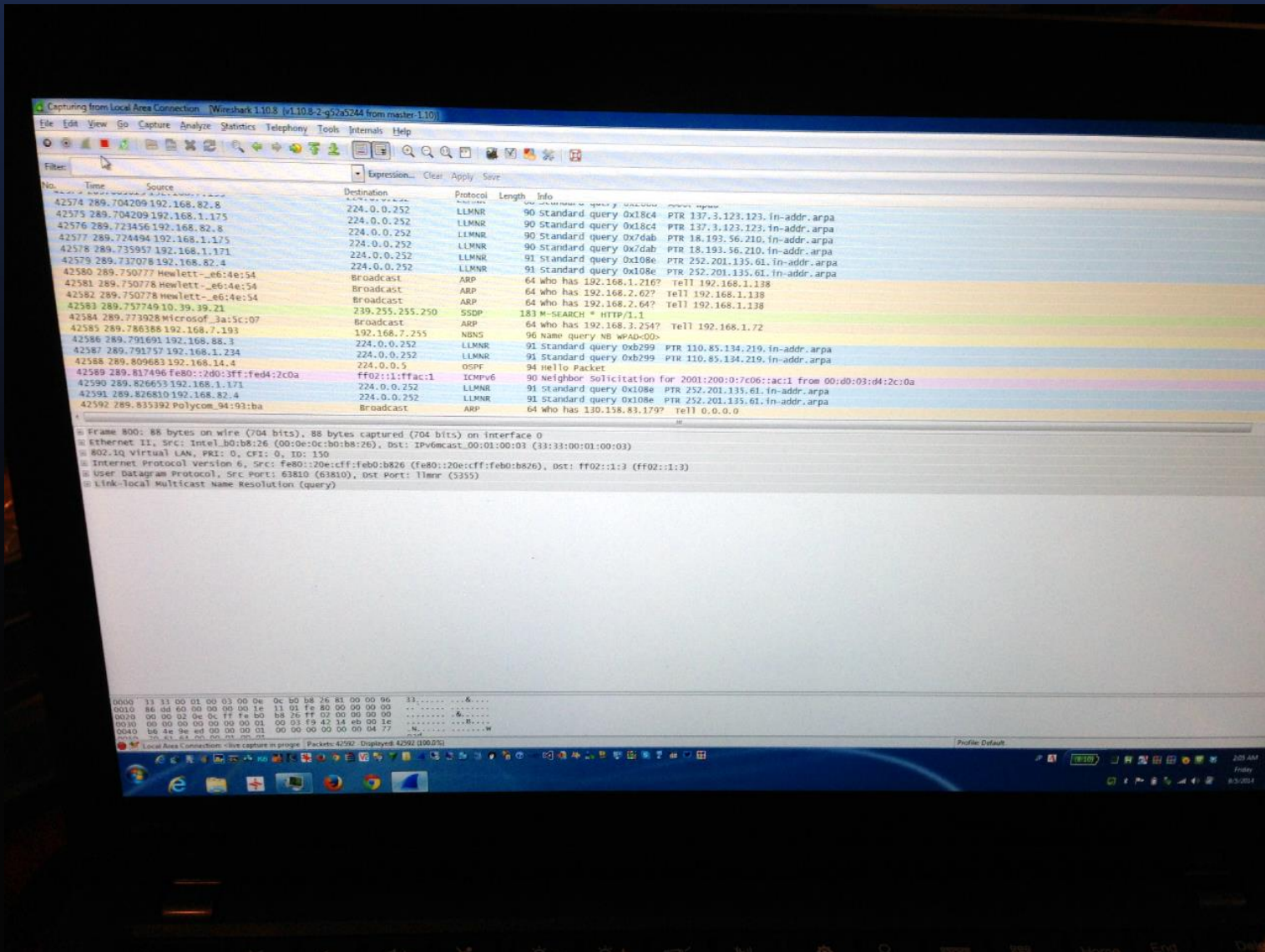
フレッツ安全性検証実験結果 (アップロード方向)

The image shows a Wireshark capture of a network packet. The packet list pane shows a packet of length 427 bytes, protocol 0x155d, and destination 55:42:00:05:68:00. The packet details pane shows the following structure:

Offset	Length	Protocol	Content
0000	55 42 00 05 68 00 12 e2 70 49 6b 00 15 5d 3a 5c		UB..h... pIk..]:\d.!E
0010	0b 81 00 00 00 88 64 11 00 14 85 01 8e 00 21 45		.../.@.. ;o:w.kv
0020	00 01 8c 2f bb 40 00 80 06 3b 6f 3a 57 f5 6b 76	_P.j7P
0030	97 e7 e7 e3 5f 00 50 ae a2 e1 c6 d1 0f 6a 37 50		...k...G ET /java
0040	18 01 03 6b e1 00 00 47 45 54 20 2f 6a 61 76 61		script/f p_base_b
0050	73 63 72 69 70 74 2f 66 70 5f 62 61 73 65 5f 62		d_ga_6.0 .15.js H
0060	64 5f 67 61 5f 36 2e 30 2e 31 35 2e 6a 73 20 48		TTP/1.1. .Accept:
0070	54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a		applica tion/jav
0080	20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 61 76		ascript, */*;q=0
0090	61 73 63 72 69 70 74 2c 20 2a 2f 2a 3b 71 3d 30		.8..Refe rer: htt
00a0	2e 38 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74		p://www. yahoo.co
00b0	70 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f		.jp/..Ac cept-Lan
00c0	2e 6a 70 2f 0d 0a 41 63 63 65 70 74 2d 4c 61 6e		guage: j a-JP..Us
00d0	67 75 61 67 65 3a 20 6a 61 2d 4a 50 0d 0a 55 73		er-Agent : Mozill
00e0	65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c		a/5.0 (w indows N
00f0	61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e		T 6.1; w OW64; Tr
0100	54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 54 72		ident/7. 0; rv:11
0110	69 64 65 6e 74 2f 37 2e 30 3b 20 72 76 3a 31 31		.0) like Gecko..
0120	2e 30 29 20 6c 69 6b 65 20 47 65 63 6b 6f 0d 0a		Accept-E ncoding:
0130	41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a		gzip, d eflate..
0140	20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a		Host: ww w.yahoo.
0150	48 6f 73 74 3a 20 77 77 77 2e 79 61 68 6f 6f 2e		co.jp..D NT: 1..C
0160	63 6f 2e 6a 70 0d 0a 44 4e 54 3a 20 31 0d 0a 43		onnectio n: Keep-
0170	6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d		Alive..C ookie: B
0180	41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 42		=enfujh 9365up&b
0190	3d 65 6e 66 75 3d 6a 68 39 33 36 35 75 70 26 62		=3&s=79. ...
01a0	3d 33 26 73 3d 37 39 0d 0a 0d 0a		

※ 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

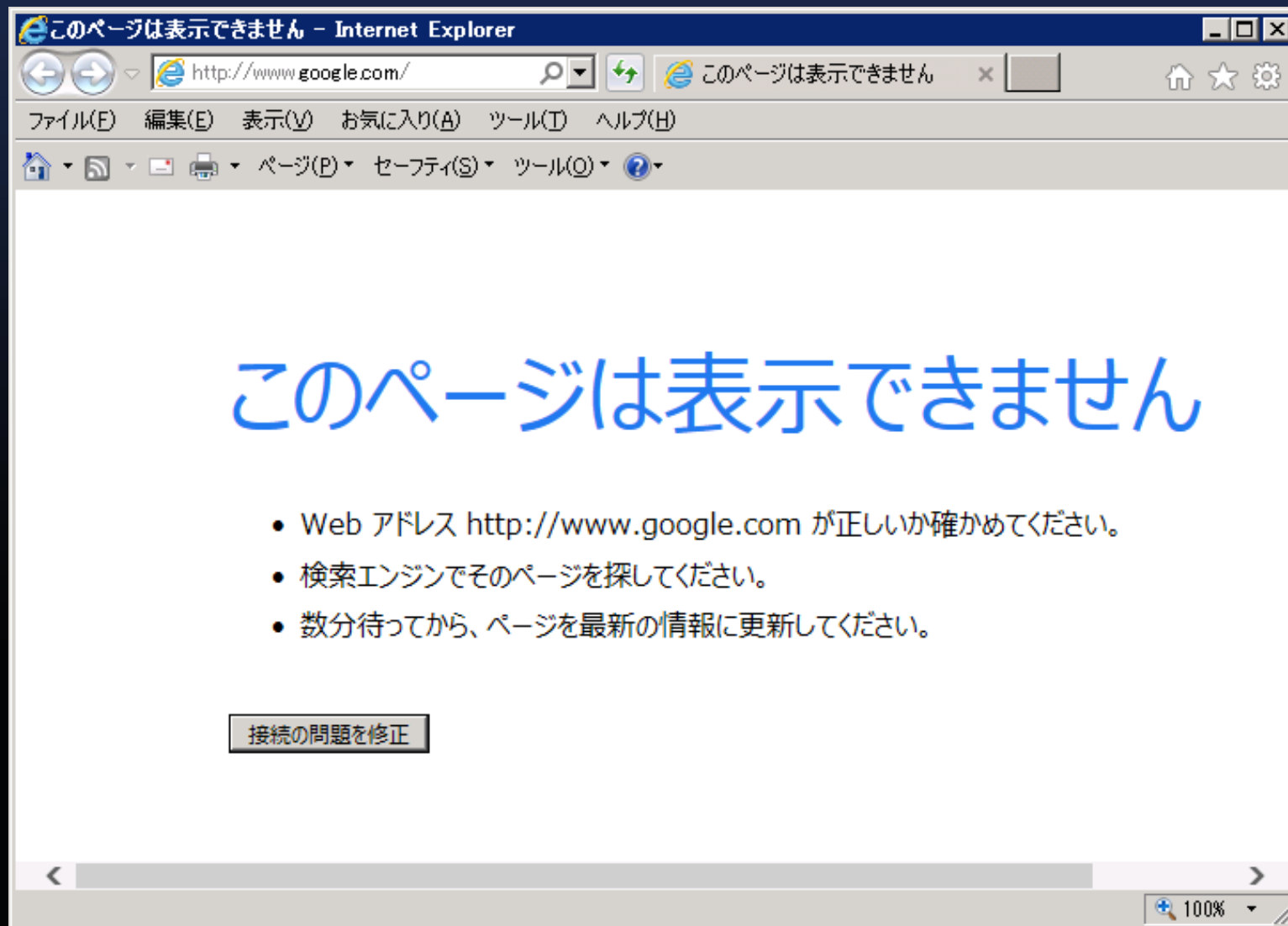
筑波大学大学院システム情報工学研究科
コンピュータサイエンス専攻博士ソフトウェア研究室



筑波大学

University of Tsukuba

GFW



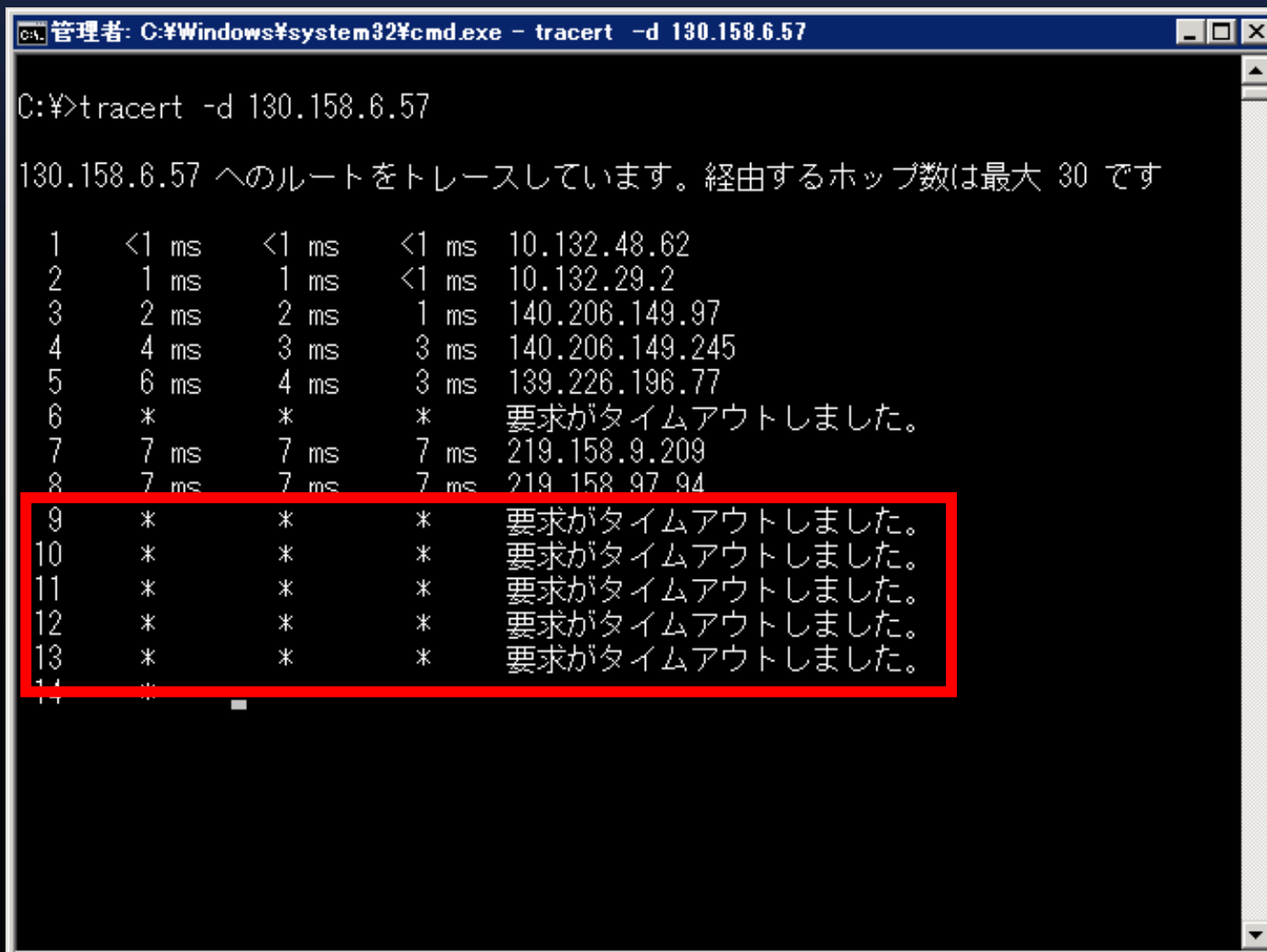
FW が提供する主な遮断機能

- 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



```
管理: C:\Windows\system32\cmd.exe - tracert -d 130.158.6.57
C:\>tracert -d 130.158.6.57

130.158.6.57 へのルートをトレースしています。経由するホップ数は最大 30 です

  1  <1 ms    <1 ms    <1 ms    10.132.48.62
  2   1 ms     1 ms     <1 ms    10.132.29.2
  3   2 ms     2 ms     1 ms    140.206.149.97
  4   4 ms     3 ms     3 ms    140.206.149.245
  5   6 ms     4 ms     3 ms    139.226.196.77
  6   *        *        *        要求がタイムアウトしました。
  7   7 ms     7 ms     7 ms    219.158.9.209
  8   7 ms     7 ms     7 ms    219.158.97.94
  9   *        *        *        要求がタイムアウトしました。
 10  *        *        *        要求がタイムアウトしました。
 11  *        *        *        要求がタイムアウトしました。
 12  *        *        *        要求がタイムアウトしました。
 13  *        *        *        要求がタイムアウトしました。
 14  *        *        *        要求がタイムアウトしました。
```

• 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
```



六四

中国側クライアントPC

Intel(R) PRO/1000 MT Network Connection: ¥Device¥NPF_{C995C203-4743-40B3-A58D-742B828F2D0E} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

Filter: ip.addr==130.158.83.218

No.	Time	Source	Destination	Protocol	Length	Info
27831	17:20:31.597191000	10.132.48.3	130.158.83.218	TCP	66	64414 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256
27850	17:20:31.651964000	130.158.83.218	10.132.48.3	TCP	66	http > 64414 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256
27851	17:20:31.651993000	10.132.48.3	130.158.83.218	TCP	54	64414 > http [ACK] Seq=1 Ack=1 win=65536 Len=0
27855	17:20:31.658501000	10.132.48.3	130.158.83.218	TCP	55	[TCP segment of a reassembled PDU]
27883	17:20:31.741053000	10.132.48.3	130.158.83.218	HTTP	117	GET /search?q=%E5%85%AD%E5%9B%9B HTTP/1.1
27893	17:20:31.786024000	130.158.83.218	10.132.48.3	TCP	60	http > 64414 [RST] Seq=1 win=964096 Len=0

Frame 27883: 117 bytes on wire (936 bits)
Ethernet II, Src: vmware_81:41:4d (00:50:56:81:41:4d), Dst: Intel_14:a2:0f (00:0c:29:14:a2:0f)
Internet Protocol Version 4, Src: 10.132.48.3, Dst: 130.158.83.218
Transmission Control Protocol, Src Port: 64414, Dst Port: http (80), Seq: 1, Ack: 1, Win: 65536, Len: 0
[2 Reassembled TCP Segments (64 bytes): #437(1), #438(63)]
Hypertext Transfer Protocol
GET /search?q=%E5%85%AD%E5%9B%9B HTTP/1.1
[Expert Info (Chat/Sequence): GET /search?q=%E5%85%AD%E5%9B%9B HTTP/1.1] Request Method: GET
Request URI: /search?q=%E5%85%AD%E5%9B%9B
Request Version: HTTP/1.1
HOST: cn.bing.com\r\n\r\n[Full request URI: http://cn.bing.com/search?q=%E5%85%AD%E5%9B%9B]

Microsoft Corporation: ¥Device¥NPF_{55DC283B-1CDE-44DF-A3B2-7BEE98411646} [Wireshark 1.8.3 (SVN Rev 4...)]

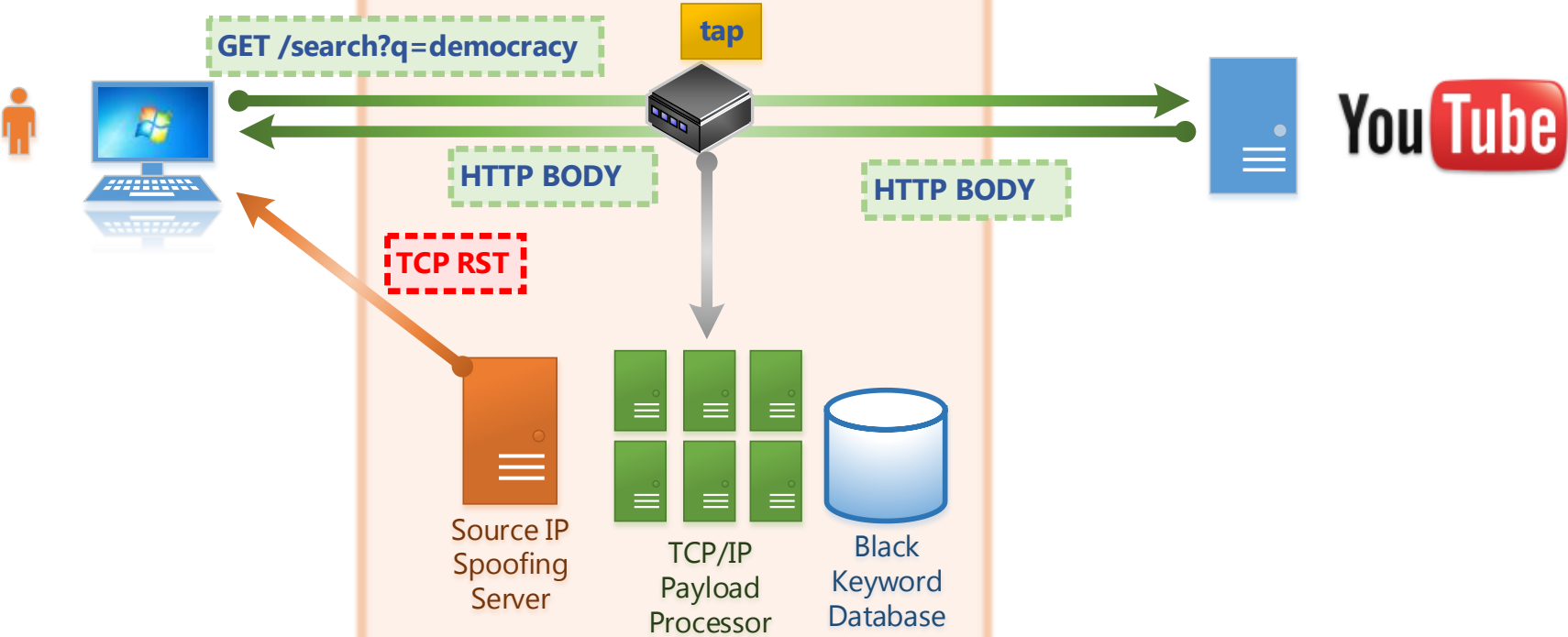
Filter: ip.addr==140.206.86.76

No.	Time	Source	Destination	Protocol	Length	Info
437	35.2581490	140.206.86.76	130.158.83.218	TCP	66	64414 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256
438	35.2582020	130.158.83.218	140.206.86.76	TCP	66	http > 64414 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256
439	35.3114200	140.206.86.76	130.158.83.218	TCP	60	64414 > http [ACK] Seq=1 Ack=1 win=65536 Len=0
440	35.3178830	140.206.86.76	130.158.83.218	TCP	60	[TCP segment of a reassembled PDU]
442	35.3998610	140.206.86.76	130.158.83.218	HTTP	117	GET /search?q=%E5%85%AD%E5%9B%9B HTTP/1.1
443	35.4017760	140.206.86.76	130.158.83.218	TCP	60	64414 > http [RST] Seq=65 win=16594688 Len=0

Frame 442: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
Ethernet II, Src: Nortel_14:a2:0f (00:1a:8f:14:a2:0f), Dst: Microsoft_01:41:0d (00:15:5d:01:41:0d)
Internet Protocol Version 4, Src: 140.206.86.76 (140.206.86.76), Dst: 130.158.83.218 (130.158.83.218)
Transmission Control Protocol, Src Port: 64414 (64414), Dst Port: http (80), Seq: 2, Ack: 1, Len: 63
[2 Reassembled TCP Segments (64 bytes): #440(1), #442(63)]
Hypertext Transfer Protocol
GET /search?q=%E5%85%AD%E5%9B%9B HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /search?q=%E5%85%AD%E5%9B%9B HTTP/1.1\r\n] Request Method: GET
Request URI: /search?q=%E5%85%AD%E5%9B%9B
Request Version: HTTP/1.1
HOST: cn.bing.com\r\n\r\n[Full request URI: http://cn.bing.com/search?q=%E5%85%AD%E5%9B%9B]

日本側サーバーPC

Government's Firewall



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

Intel(R) PRO/1000 MT Network Connection: ¥Device¥NPF_{C995C203-4743-40B3-A58D-742B828F2D0E} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

Filter: ip.addr==130.158.83.218

No.	Time	Source	Destination	Protocol	Length	Info
8166	17:28:52.367949000	130.158.83.218	10.132.48.3	DNS	87	Standard query response 0x003a A 59.24.3.173
8171	17:28:52.399875000	130.158.83.218	10.132.48.3	DNS	135	Standard query response 0x003a A 199.59.149.198

Frame 8166: 87 bytes on wire (696 bits), Ethernet II, Src: Cisco_5f:26:5f (6c:20:00:00:00:00), Dst: Intel_02:00:00:00:00:00 (08:00:00:00:00:00), Internet Protocol Version 4, Src: 130.158.83.218, Dst: 10.132.48.3, User Datagram Protocol, Src Port: domain, Destination Port: 57862, Domain Name System (response)

[Request In: 8157]
[Time: 0.036163000 seconds]
Transaction ID: 0x003a
Flags: 0x8180 Standard query response, Questions: 1, Answer RRs: 1, Authority RRs: 0, Additional RRs: 0

Queries

Answers

- twitter.com: type A, class IN, addr 59.24.3.173

0000 00 50 56 81 41 4d 6c 20 56 5f 26 5f
0010 00 49 95 3c 00 00 36 11 de 58 82 9e
0020 30 03 00 35 e2 06 00 35 ef bc 00 3a
0030 00 01 00 00 00 00 07 74 77 69 74 74
0040 6f 6d 00 00 01 00 01 c0 0c 00 01 00
0050 f5 00 01 3b 18 02 2d

Microsoft Corporation: ¥Device¥NPF_{55DC283B-1CDE-44DF-A3B2-7BEE98411646} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

Filter: ip.addr==140.206.86.76

No.	Time	Source	Destination	Protocol	Length	Info
25	2.029306000	130.158.83.218	140.206.86.76	DNS	135	Standard query response 0x003a A 199.59.149.198 A 199.59.149.198

Frame 25: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0, Ethernet II, Src: Microsof_01:41:0d (00:15:5d:01:41:0d), Dst: Nortel_14:a2:0f (00:1a:8f:14:a2:0f), Internet Protocol Version 4, Src: 130.158.83.218 (130.158.83.218), Dst: 140.206.86.76 (140.206.86.76), User Datagram Protocol, Src Port: domain (53), Dst Port: 57862 (57862), Domain Name System (response)

[Request In: 24]
[Time: 0.000095000 seconds]
Transaction ID: 0x003a
Flags: 0x8180 Standard query response, No error, Questions: 1, Answer RRs: 4, Authority RRs: 0, Additional RRs: 0

Queries

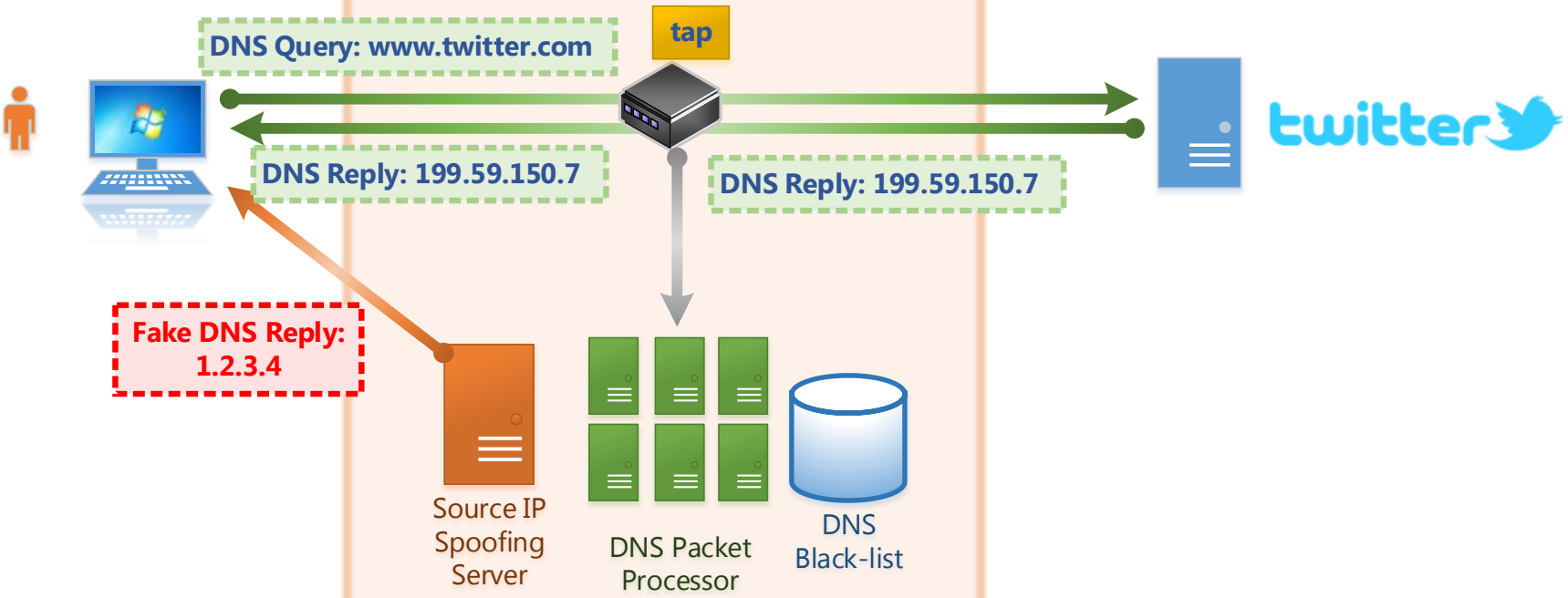
Answers

- twitter.com: type A, class IN, addr 199.59.149.198
- Name: twitter.com, Type: A (Host address), Addr: 199.59.149.198

0000 00 1a 8f 14 a2 0f 00 15 5d 01 41 0d 08 00 45 00].A...E.
0010 00 79 22 85 00 00 80 11 00 00 82 9e 53 da 8c ce .y.....S..
0020 56 4c 00 35 e2 06 00 65 8e 8f 00 3a 81 80 00 01 vL5...e.....
0030 00 04 00 00 00 00 07 74 77 69 74 74 65 72 03 63t witter.c
0040 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 om.....
0050 00 00 01 c7 3b 05 c6 c0 0c 00 01 00 01 00 00 00

日本側サーバーPC

Government's Firewall



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
```



The screenshot shows the FACTA ONLINE website interface. The main header includes the site name "FACTA ONLINE" and navigation links: HOME, ARCHIVES, FREE, BLOG, SHARE, FORUM. A search bar is also present. The article title is "中国が「ネット長城」通信障害で真っ赤な嘘" (China's 'Great Firewall' network outage is a red lie). The article text describes a network outage in China on January 21st, where many websites became inaccessible. It mentions that the outage started at 3 PM and lasted for 2 hours. Popular services like Baidu and Weibo were also affected. The article concludes by mentioning that the Chinese government's network security research center (CNCERT) has identified the cause as a DNS server attack.

• 第3世代 (2014年6月～)

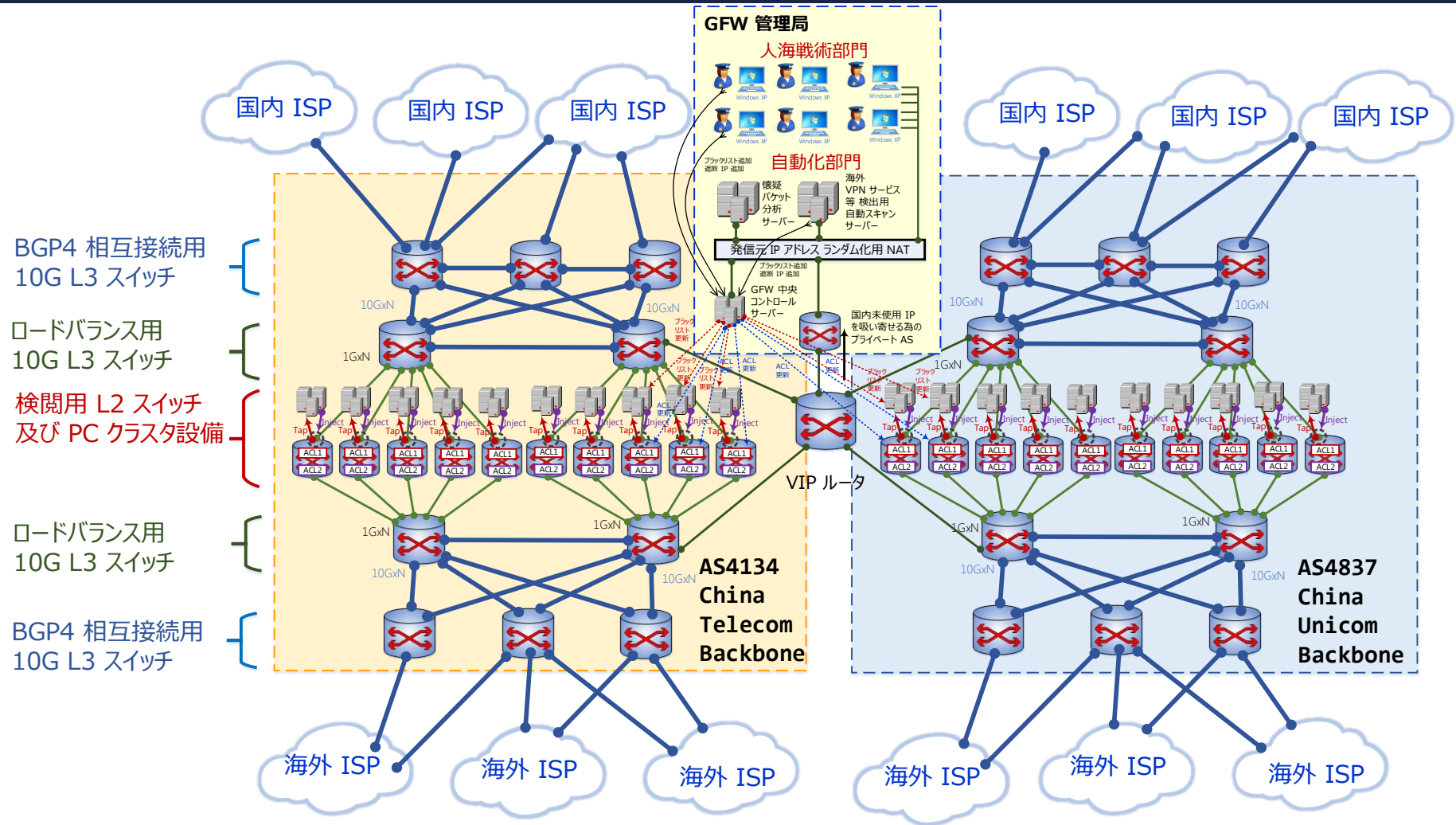
- 第1世代を拡張。大量の海外 IP アドレスへの動的フィルタリング機能を搭載
 - 各 L2 スイッチの TCAM (Ternary CAM) が溢れないようにするため 180 秒間のみ ACL を挿入する手法を開発

```
管理者: C:\Windows\system32\cmd.exe - tracert -d 130.158.6.57
C:\>tracert -d 130.158.6.57

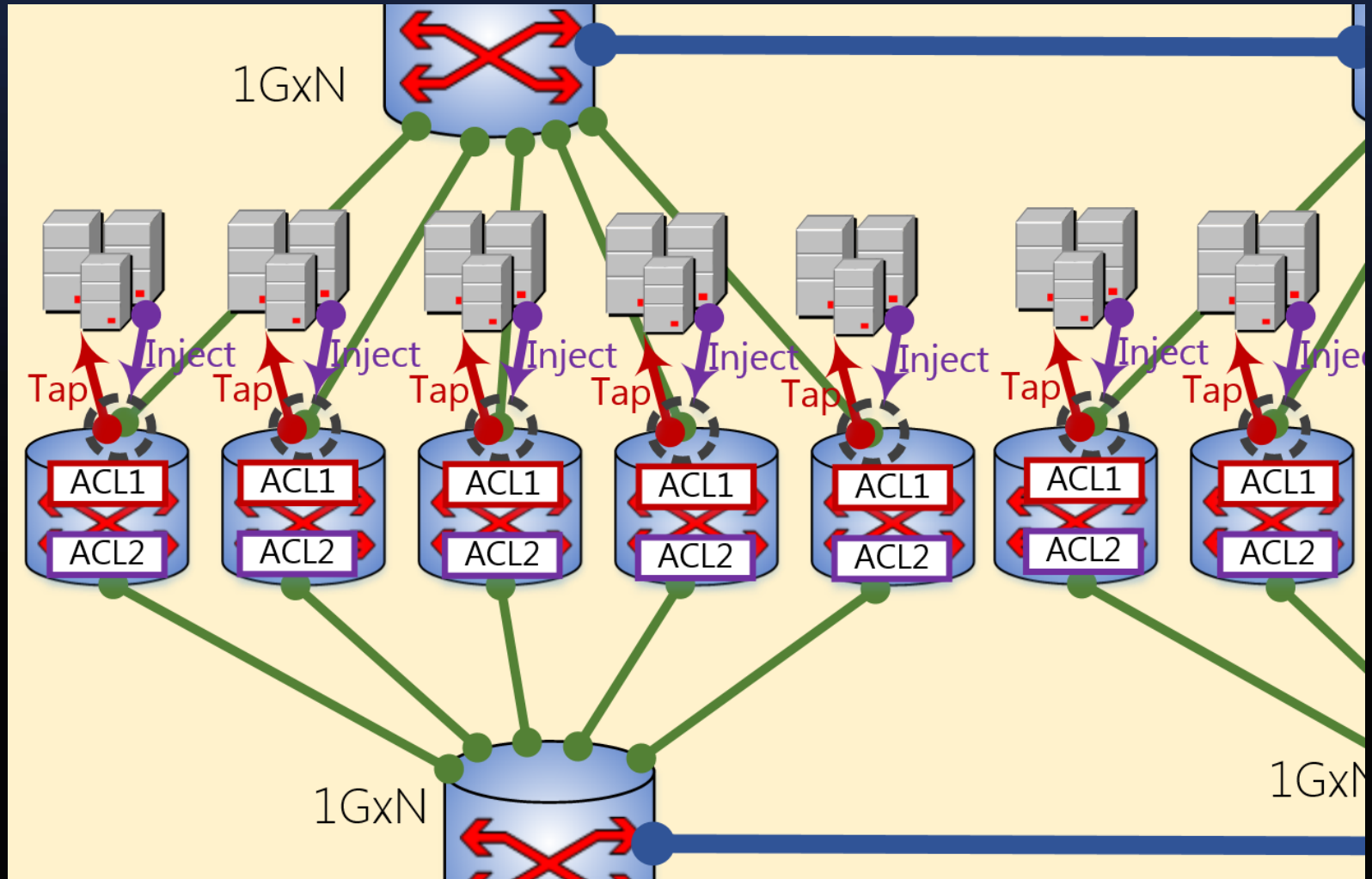
130.158.6.57 へのルートをトレースしています。経由するホップ数は最大 30 です

  1  <1 ms    <1 ms    <1 ms    10.132.48.62
  2  1 ms     1 ms     <1 ms    10.132.29.2
  3  2 ms     2 ms     1 ms    140.206.149.97
  4  4 ms     3 ms     3 ms    140.206.149.245
  5  6 ms     4 ms     3 ms    139.226.196.77
  6  *        *        *        要求がタイムアウトしました。
  7  7 ms     7 ms     7 ms    219.158.9.209
  8  7 ms     7 ms     7 ms    219.158.97.94
  9  *        *        *        要求がタイムアウトしました。
 10  *        *        *        要求がタイムアウトしました。
 11  *        *        *        要求がタイムアウトしました。
 12  *        *        *        要求がタイムアウトしました。
 13  *        *        *        要求がタイムアウトしました。
 14  *        *        *        要求がタイムアウトしました。
```

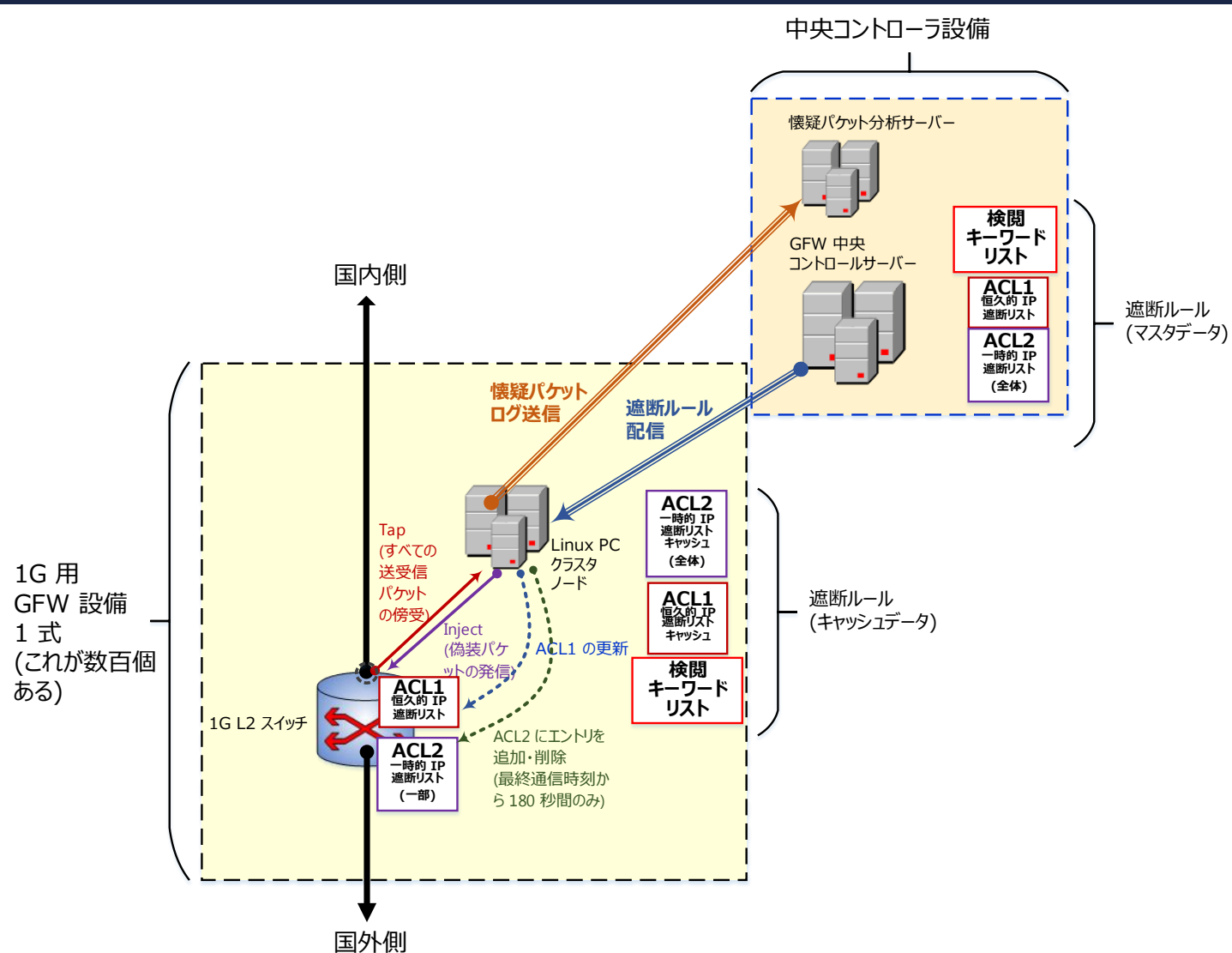

GFW のネットワークポロジ (拳動から推測)



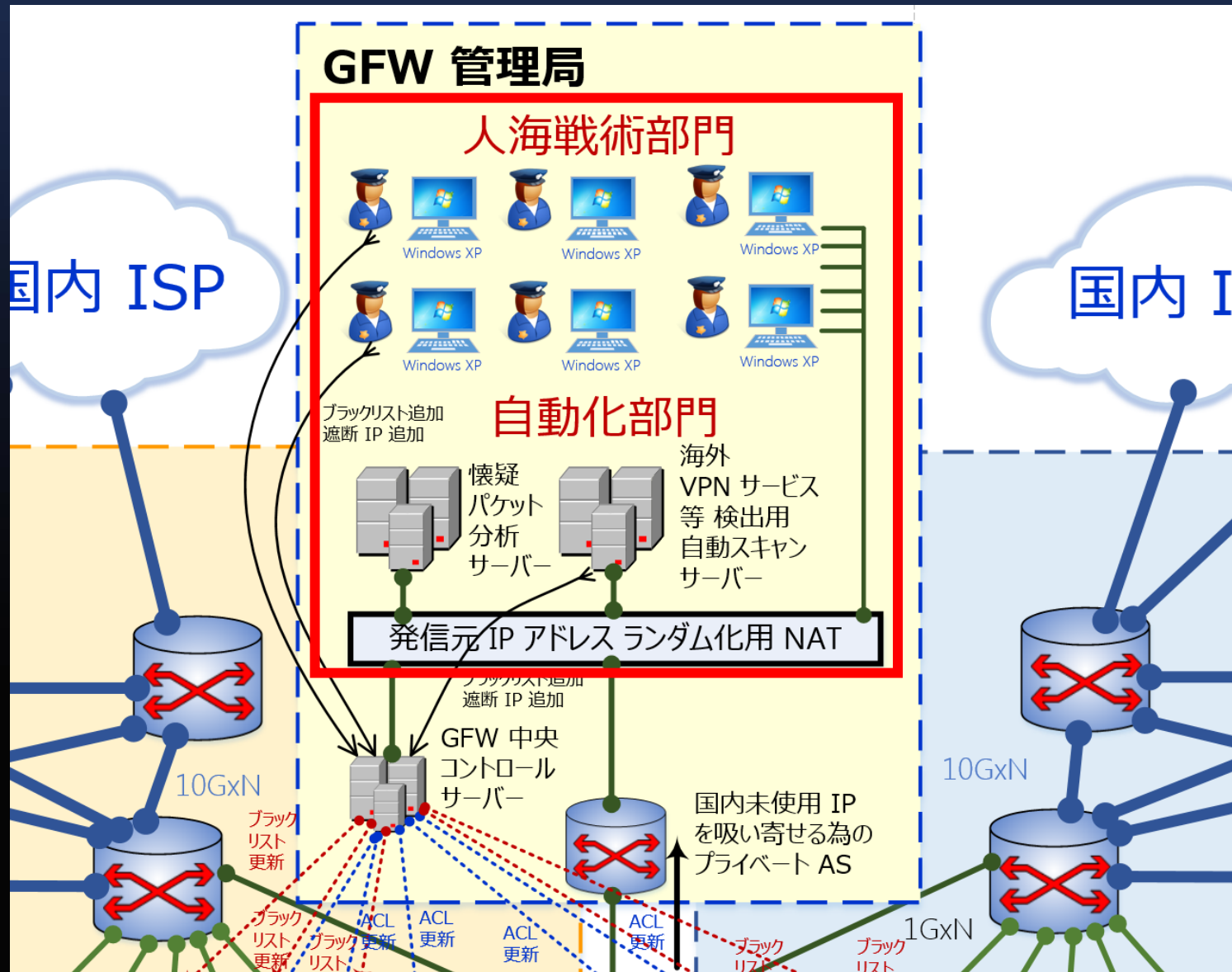
1Gbps 単位に分散し 安価な L2 スイッチおよび Linux PC で検閲・遮断を実施



1Gbps 検閲・遮断用装置



遮断リストの保守業務



主な GFW ハードウェアベンダ

- 華為技術有限公司 (Huawei Technologies)
- 曙光信息产业有限公司 (Dawning Information Industry)

他

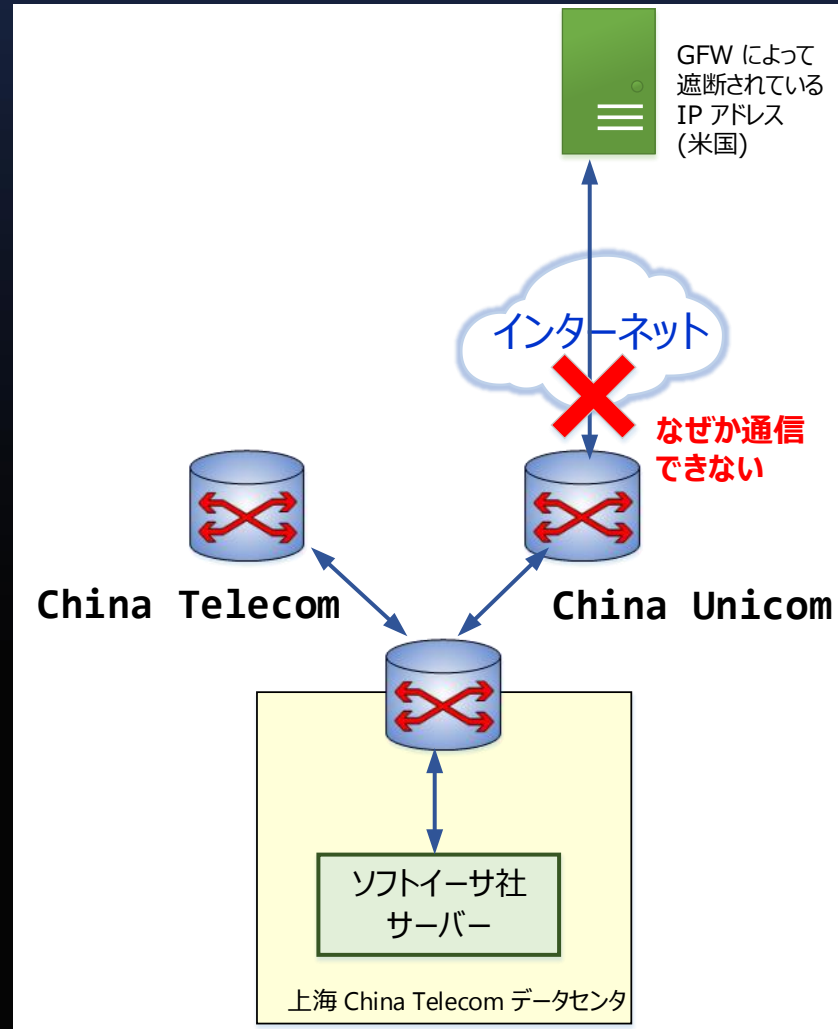
GFW の開発体制

- 「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



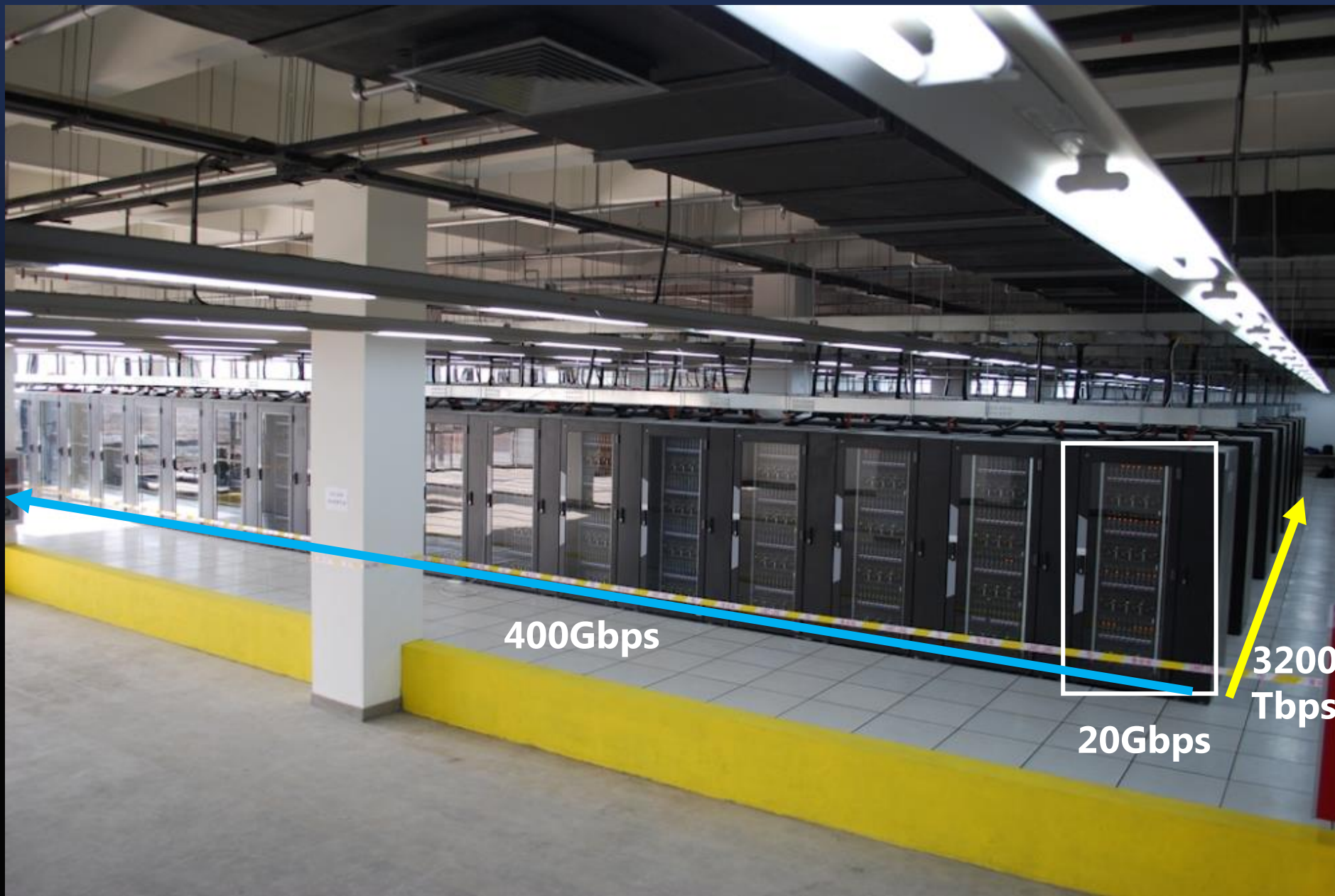


China Unicom 社からの 正式回答

- 「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 (中国移动)
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？



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

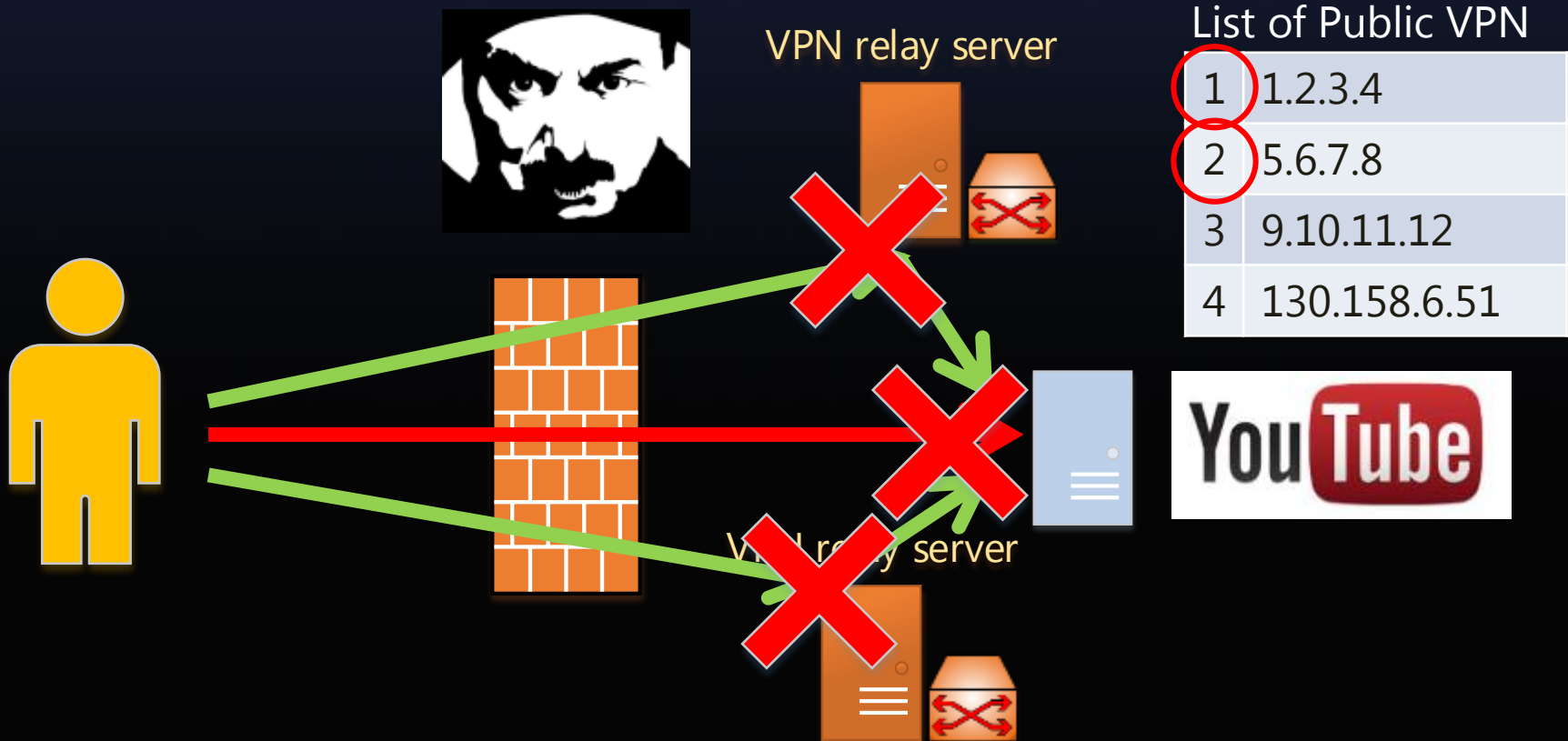
University of Tsukuba

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]

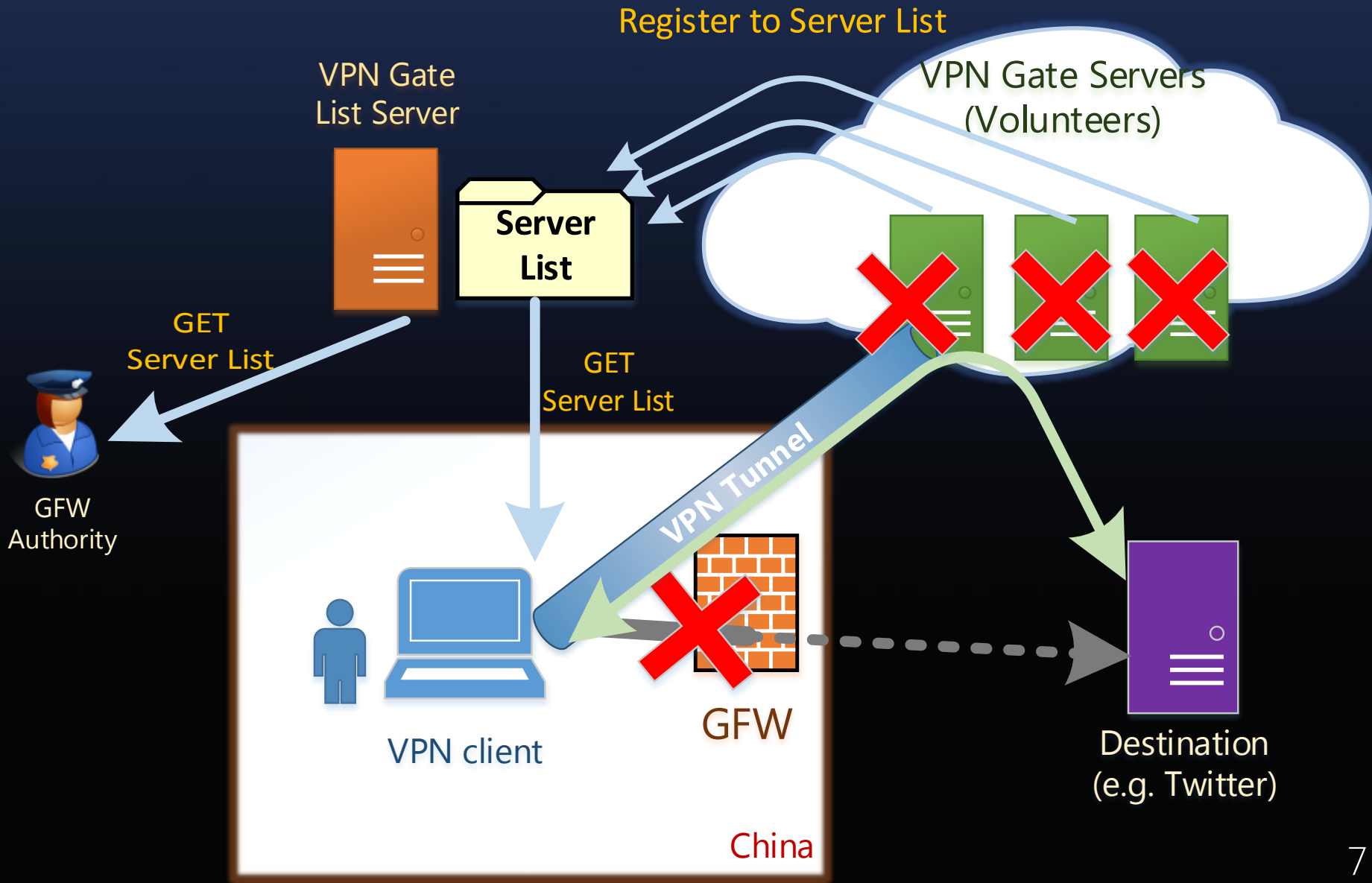
Our Goal of VPN Gate

- 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

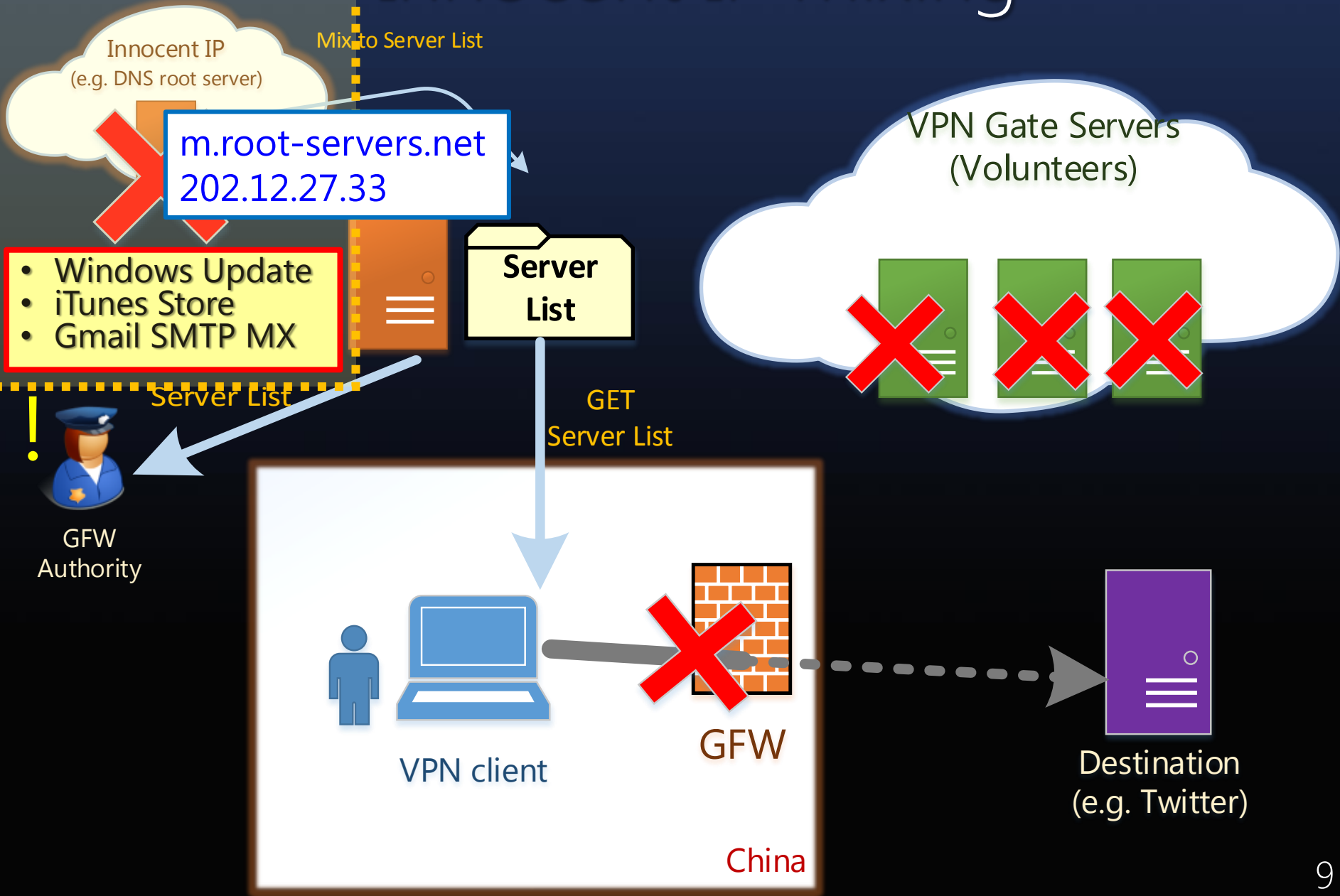


VPN Gate's approach

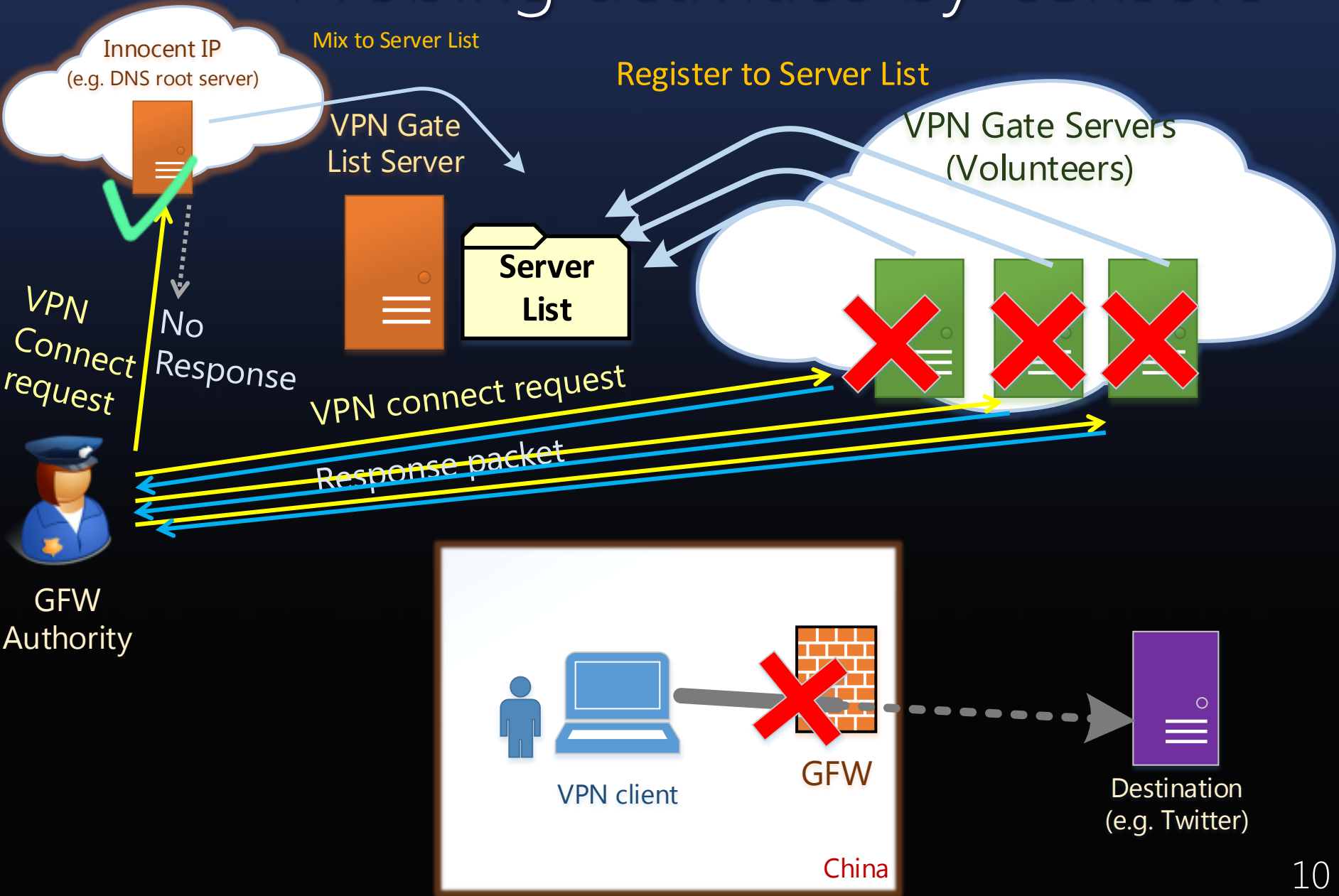
1. Organize thousands of volunteer relays.
 - Authorities must block all IP addresses.
2. Innocent IP mixing technique.
 - Enforce authorities to probe all IPs.

Innocent IP mixing

Innocent IP mixing



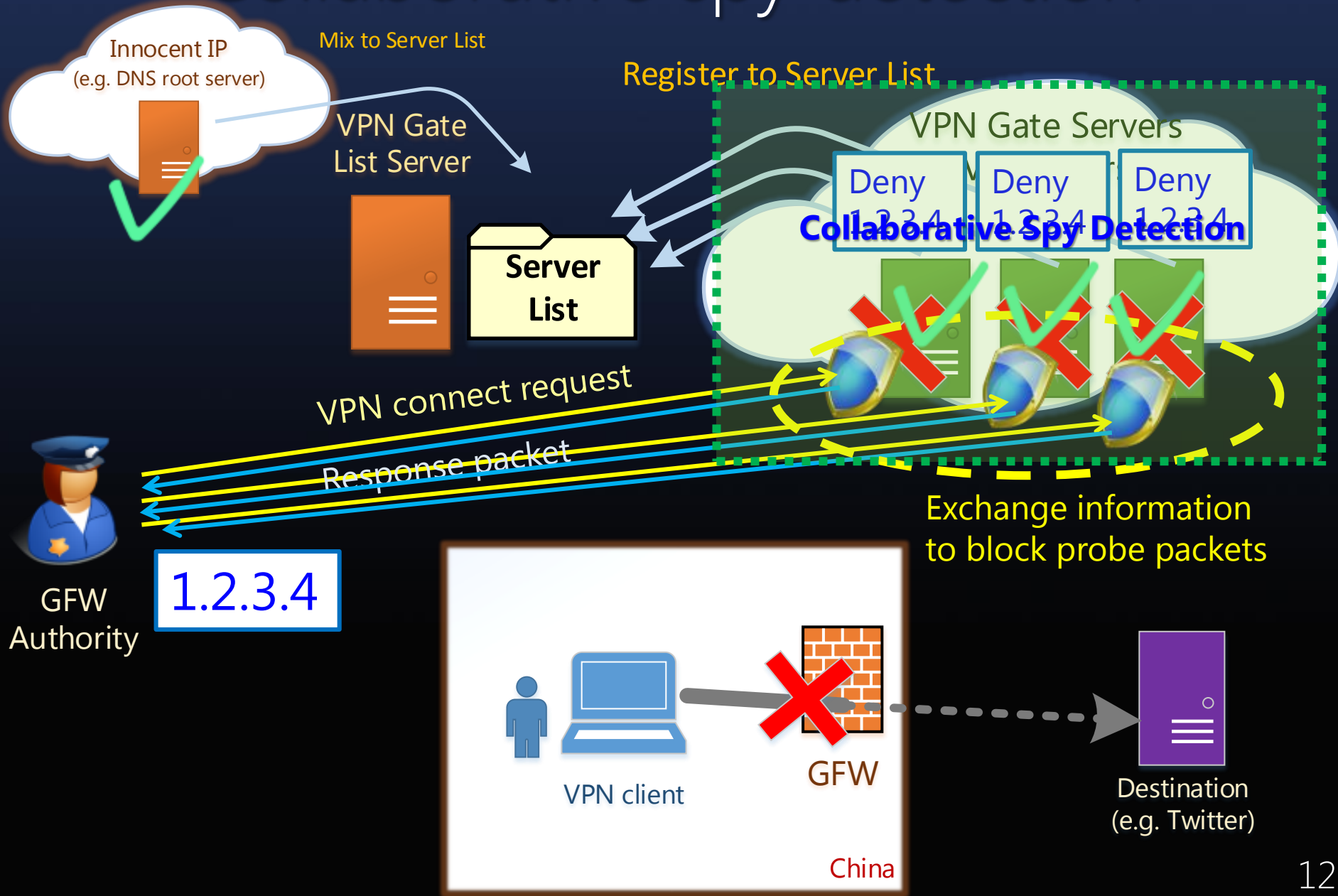
Probing activities by censors



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

The screenshot displays the 'VPN Gate Service Control Panel' window. The main area features a diagram illustrating the VPN Gate architecture. On the left, a 'VPN Gate Client' is shown connected to 'Domestic Internet'. A 'Firewall' is depicted as 'Out of Order by Unknown Reason', with an arrow labeled 'Bypass FW' pointing from the client towards the 'VPN Gate' cloud. The cloud contains 'Public VPN Relay Servers' which are 'Hosted by Volunteers'. An orange arrow labeled 'Liberty!!' points from the cloud to 'Target Servers' on the 'Overseas Internet', which includes logos for YouTube and Twitter. A text box in the top right corner identifies it as 'An Academic Experiment @ Graduate School of University of Tsukuba, Japan.' with the website 'www.tsukuba.ac.jp/english/'. The URL 'www.vpngate.net' is also visible at the bottom of the diagram.

Join the VPN Gate Academic Research Project?

VPN Gate is an academic experiment for the research on the 'Distributed Public VPN Relay Server' technology, operated at the Graduate School on University of Tsukuba, Japan. VPN Gate Client users can connect to VPN Gate Services running on Public VPN Relay Servers, and enjoy unrestricted Internet access via the VPN Relay Server.

When a VPN Gate Client user accesses to a server on Internet, the source IP address will be replaced to the IP address of the relaying Public VPN Server. Consequently, the VPN Gate Client user will be able to browse overseas web sites smoothly even if the user's local firewall is out of order by an unknown reason and unable to pass such an access.

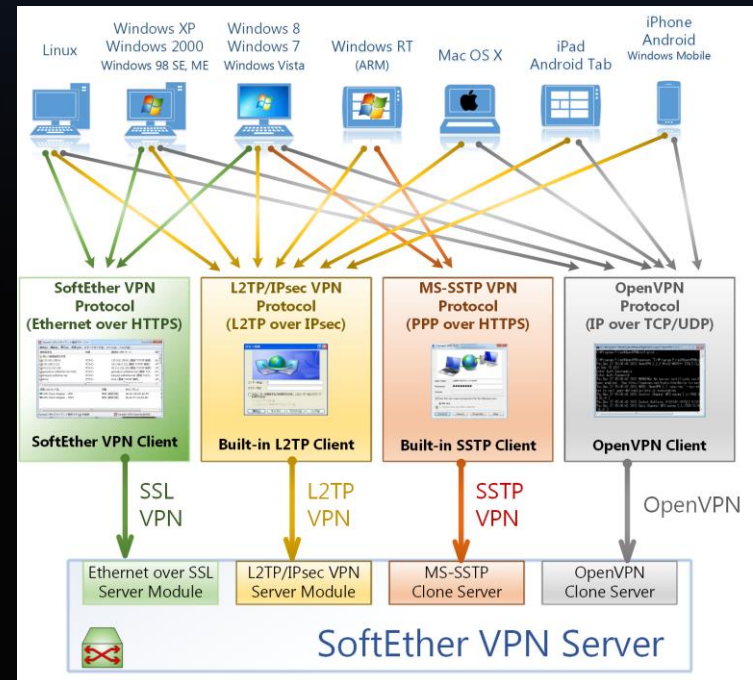
Enable the VPN Gate Relay Service and Join the VPN Gate Research as a Volunteer.

 If you check the above checkbox and press OK, the VPN Gate Relay Service will be activated on this computer. As the result, any VPN Gate Client will be able to communicate towards the Internet via the VPN Gate Relay Service. It is secure even if your computer is on the private network (e.g. corporate network) because any accesses to private IP addresses will not be permitted to pass via the VPN Gate Relay Service.

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 (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 name (+ 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.o 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 Academic Experimental Project Plugin for SoftEther VPN Client

Academic project at University of Tsukuba, Japan. 筑波大学 University of Tsukuba

VPN Gate Public VPN Relay Servers

Gain freedom access to Internet by using VPN connection via Public VPN Servers provided by volunteers around the world. Bypass your local malfunctioning firewall's packet blocking, and hide your IP address safely.

VPN Gate Academic Web Site

Refresh List

99 Public VPN Relay Servers on the Earth! (Updated at 2014-03-16 15:13:08)

DDNS Hostname	IP Address (Hostname)	Region	Uptime	VPN Sessions	Line Speed	Ping (G
vpn362434417.opengw....	58.187.9.15 (adsl-dyna...	Viet Nam	1 days	3 sessions	18.4 Mbps	22, 22
vpn694017992.opengw....	175.123.77.38	Korea Republic of	4 hours	5 sessions	63.3 Mbps	64, 64
vpn559906453.opengw....	50.135.106.72 (c-50-1...	United States	1 days	32 sessions	15.0 Mbps	17, 17
vpn493837156.opengw....	1.237.84.65	Korea Republic of	3 days	17 sessions	57.0 Mbps	203, 20
vpn970293128.opengw....	119.26.157.48 (zaq771...	Japan	1 days	3 sessions	28.9 Mbps	169, 16
vpn590682393.opengw....	68.2.175.192 (ip68-2-...	United States	2 hours	13 sessions	23.6 Mbps	61, 61
vpn273730891.opengw....	118.157.74.169 (KD11...	Japan	3 days	213 sessions	127.3 Mbps	57, 57
vpn124876588.opengw....	116.41.118.159	Korea Republic of	1 days	11 sessions	21.4 Mbps	79, 79
vpn948467262.opengw....	218.156.5.15	Korea Republic of	1 days	40 sessions	19.9 Mbps	78, 78
vpn103812839.opengw....	24.188.22.182	United States	2 days	14 sessions	16.2 Mbps	41, 41
vpn845537890.opengw....	122.32.151.204	Korea Republic of	18 hours	3 sessions	19.2 Mbps	57, 57
vpn304580552.opengw....	49.143.21.227	Korea Republic of	3 hours	3 sessions	18.7 Mbps	54, 54
vpn261900721.opengw....	71.58.14.58 (c-71-58-...	United States	2 days	5 sessions	10.4 Mbps	27, 27
vpn733608004.opengw....	182.214.49.67	Korea Republic of	1 hours	3 sessions	12.8 Mbps	58, 58

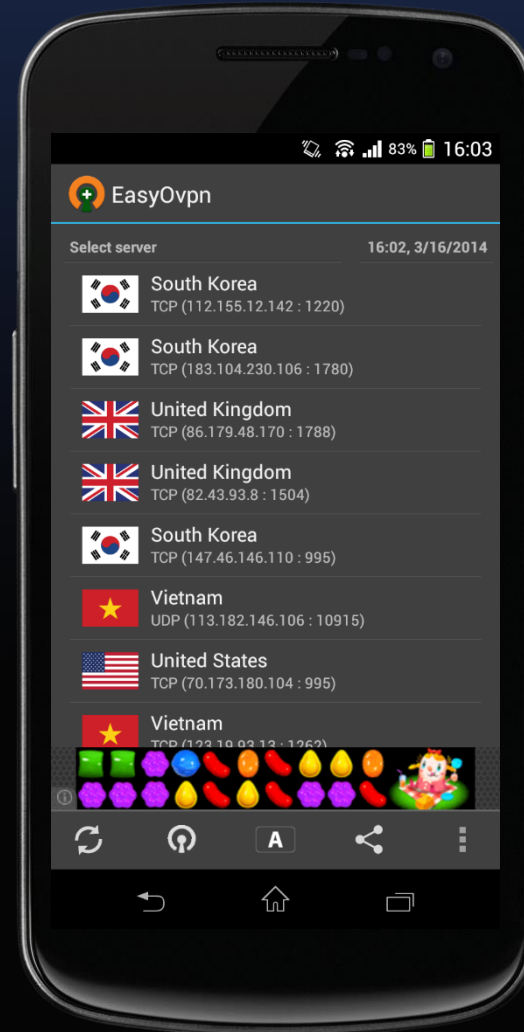
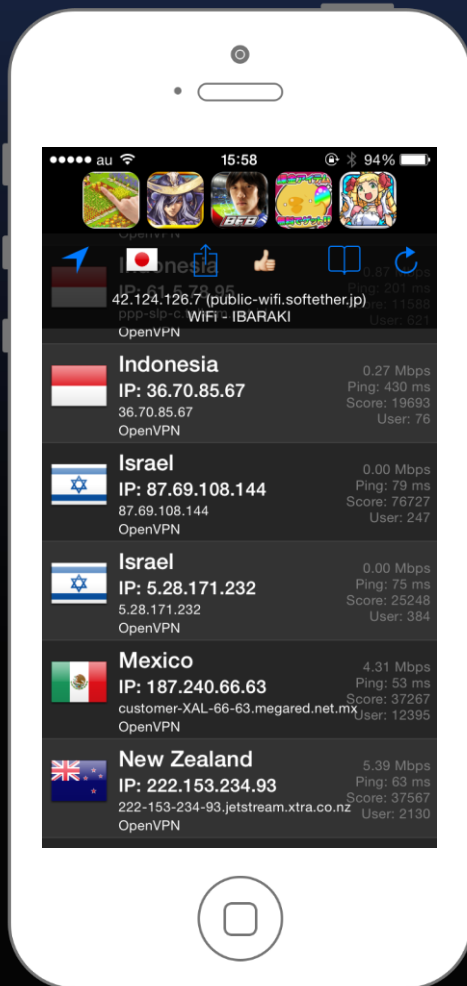
A VPN Server with higher Line Speed (measured by Mbps) and smaller Ping result are usually more comfortable to use. You might be able to browse websites which are normally unreachable from your area if you use VPN servers that are not in your area.

Proxy Settings Virtual Network Adapter: VPN

Connect to the VPN Server

Implemented as a plug-in for SoftEther VPN. (c) VPN Gate Project at University of Tsukuba, Japan.

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



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

VPN Gate
Public VPN Relay Servers

Academic Experiment at University of Tsukuba, Japan.

VPN Servers List | What is VPN Gate | How to Connect | Download | Join Us | Forum | Mirror Sites | Languages

Follow @vpngate

Free Access to World Knowledge Beyond Government's Firewall.

Your IP: 59x121x46x62.ap59.ftth.uxcom.jp (27.121.46.62)

Your country: Japan
Let's change your IP address by using VPN Gate!

Welcome to VPN Gate. (Launched on March 8, 2013.)

- You can get through your government's firewall to browse restricted websites. (e.g. YouTube.)
- You can disguise your IP address to hide your identity while surfing the Internet.
- You can protect yourself by utilizing the strong encryption while using public Wi-Fi. [More Details...](#)

Supports Windows, Mac, iPhone, iPad and Android.

SoftEther VPN
Supports OpenVPN, L2TP/IPsec and SSL-VPN.
An open-source VPN software development project since March 8.

University of Tsukuba, Japan.
www.softether.org

VPN Gate is based on SoftEther VPN, a multi-protocol VPN server.

Today: 2,105,134 connections, Cumulative: 194,323,808 connections, Traffic: 5,415.22 TB. 194,323,808 VPN connections from 220 Countries.

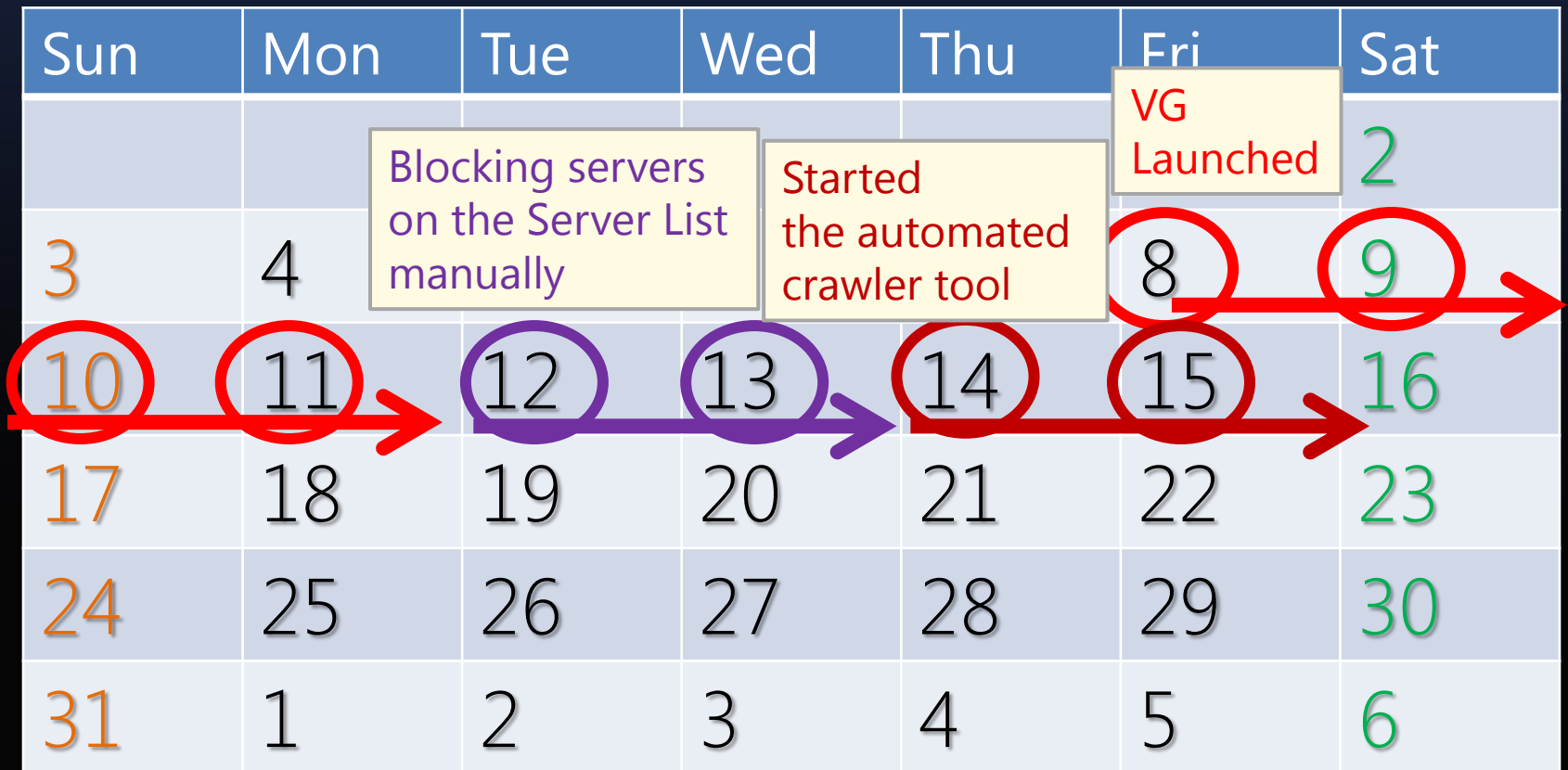
VPN Session ID	Start time (UTC)	VPN source country	VPN destination country	VPN protocol
VPN-194323808	2014/03/17 4:13:39 (0 mins ago)	Taiwan	Korea Republic of	OpenVPN
VPN-194323807	2014/03/17 4:13:38 (0 mins ago)	China	Korea Republic of	OpenVPN
VPN-194323806	2014/03/17 4:13:30 (0 mins ago)	Taiwan	Korea Republic of	OpenVPN

Rank	Country	Traffic	# Connections
1	Korea Republic of	1,739,641.0 GB	7,238,931
2	China	749,661.0 GB	25,300,088
3	Taiwan	660,454.5 GB	65,672,773

<http://www.vpngate.net/en/>

The response of GFW authority

March 2013



The authority developed the crawler in Python

Chinese GFW Authority



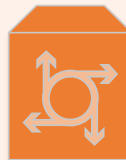

**Running
24h
(every 5 mins)**

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

Country (Physical location)	DNS hostname IP Address (ISP hostname)	VPN sessions Uptime Cumulative users	Line quality Throughput and Ping Cumulative Transfers Logging policy
 Japan	vg2018151932.opengw.net 120.74.141.252	100 sessions 1 days Total 42,465 users	33.34 Mbps Ping: 13 ms 3,277.92 GB Logging policy: 2 Weeks
 Korea Republic of		5 sessions 6 hours Total 518 users	67.10 Mbps Ping: 12 ms 46.65 GB Logging policy: 2 Weeks
 United States		0 sessions 12 hours Total 88 users	11.95 Mbps Ping: 18 ms 4.38 GB Logging policy: 2 Weeks
 Singapore		0 sessions 12 hours Total 705 users	11.47 Mbps Ping: 24 ms 9.26 GB Logging policy: 2 Weeks
 Viet Nam	vg712346371.opengw.net 42.117.139.9	0 sessions 2 hours Total 307 users	2.69 Mbps Ping: 42 ms 2.12 GB Logging policy:

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

Country (Physical location)	DNS hostname IP Address (ISP hostname)	VPN sessions Uptime Cumulative users	Line quality Throughput and Ping Cumulative Transfers Logging policy
Japan	vg2018151932.opengw.net 120.74.141.252	100 sessions 1 days Total 42,465 users	33.34 Mbps Ping: 13 ms 3,277.92 GB Logging policy: 2 Weeks
Korea Republic of	1.2.3.4	5 sessions 6 hours Total 518 users	67.10 Mbps Ping: 12 ms 46.65 GB Logging policy: 2 Weeks
United States	5.6.7.8	0 sessions 12 hours Total 88 users	11.95 Mbps Ping: 18 ms 4.38 GB Logging policy: 2 Weeks
Singapore	9.0.1.2	0 sessions 12 hours Total 705 users	11.47 Mbps Ping: 24 ms 6.26 GB
Viet Nam	google public DNS 8.8.8.8		

VPN Gate Servers
List HTML table

* This innocent IP address is an example. ²⁴

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.
```

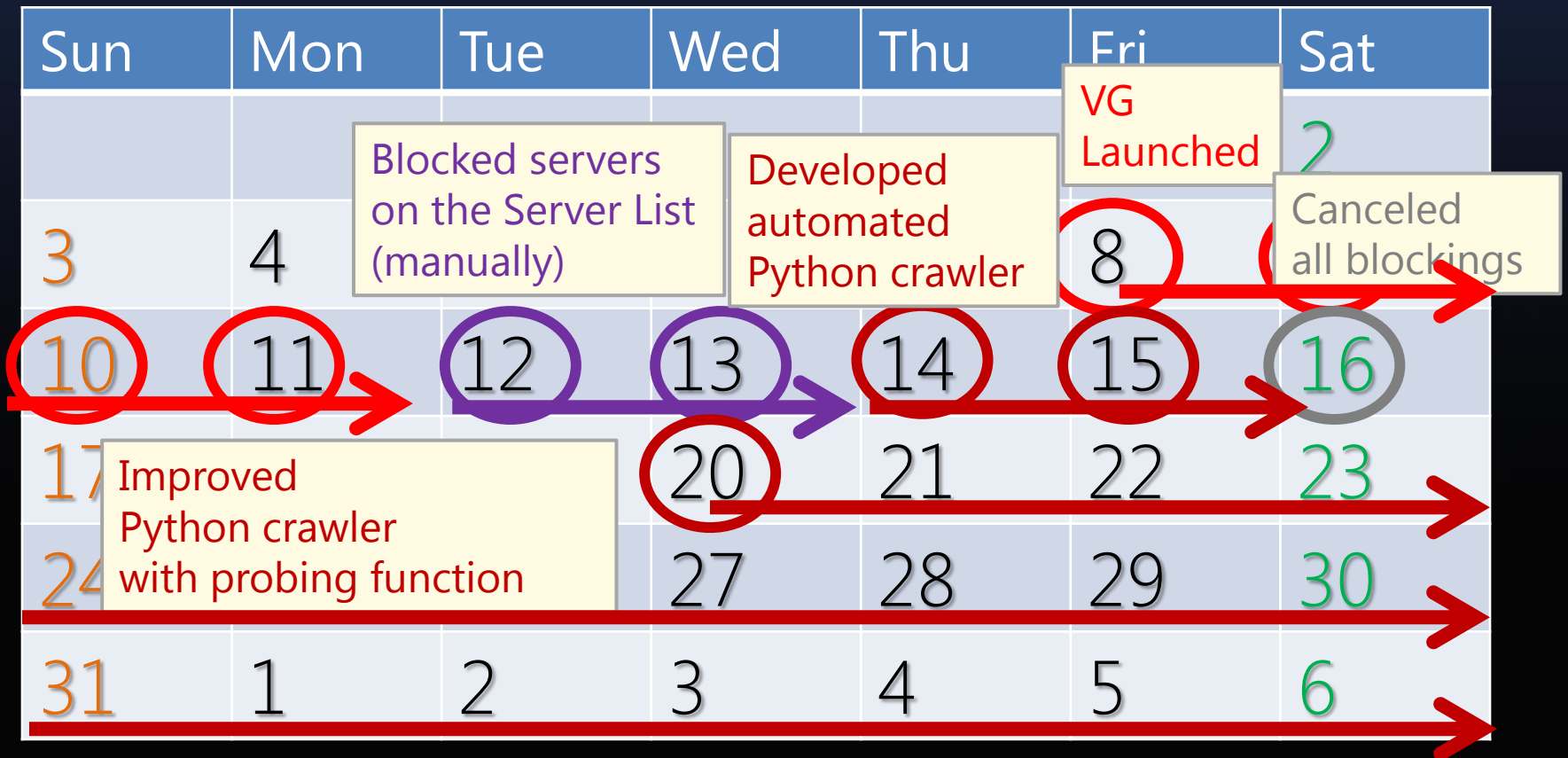
```
Request timed out.
```

Great Firewall was
under our control !

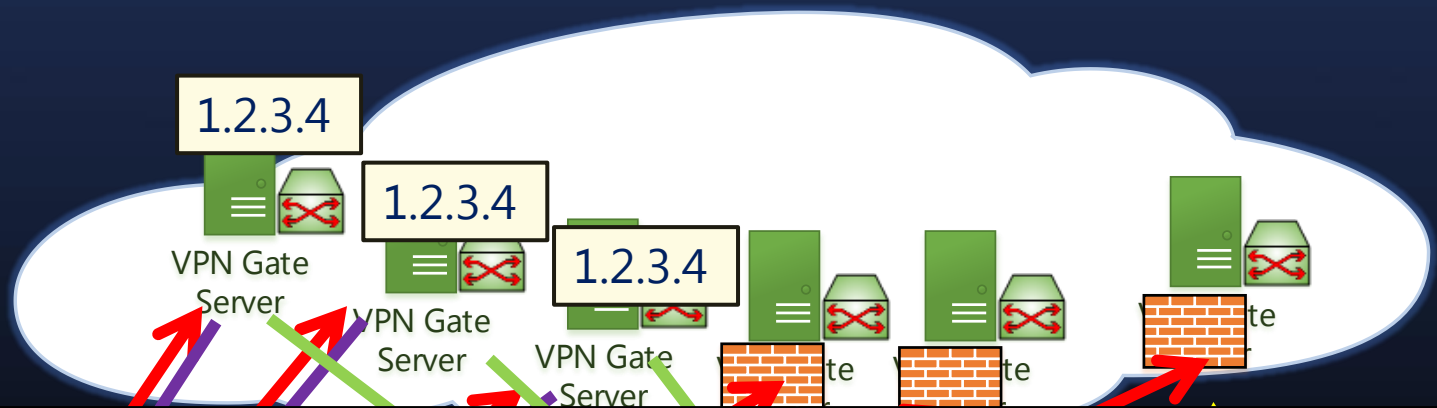
* This innocent IP address is an example.

The GFW authority improved the crawler to probe all IPs.

March 2013



Collaborative spy detection avoids probing



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

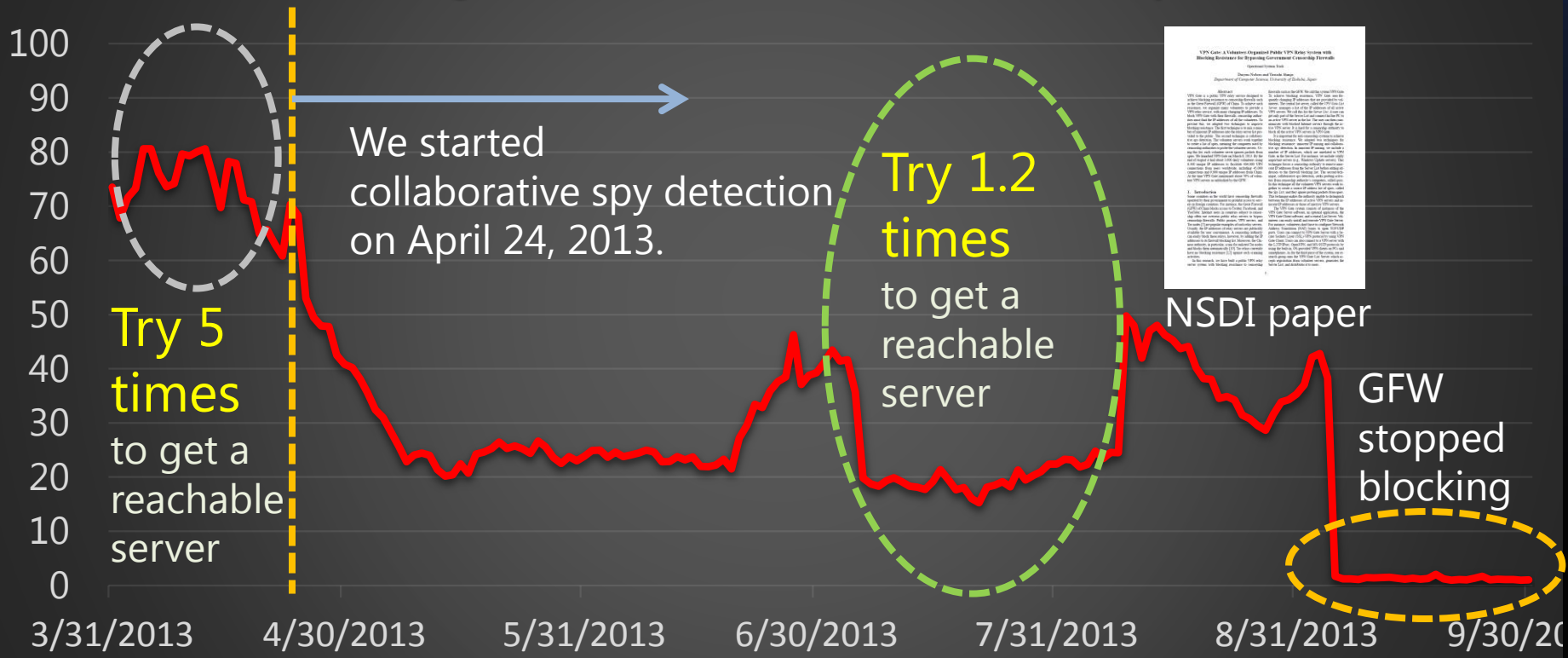
1. A single IP address or IP subnet connected to many VPN servers around the same time.
2. The amount of data transfer is too small or the duration is too short.
3. Mixing other complex algorithms.

See our papers for more details.



Collaborative spy detection works effectively since April 24, 2013

Percentages of blocked VPN Gate servers by GFW



Try 5 times to get a reachable server

We started collaborative spy detection on April 24, 2013.

Try 1.2 times to get a reachable server

NSDI paper

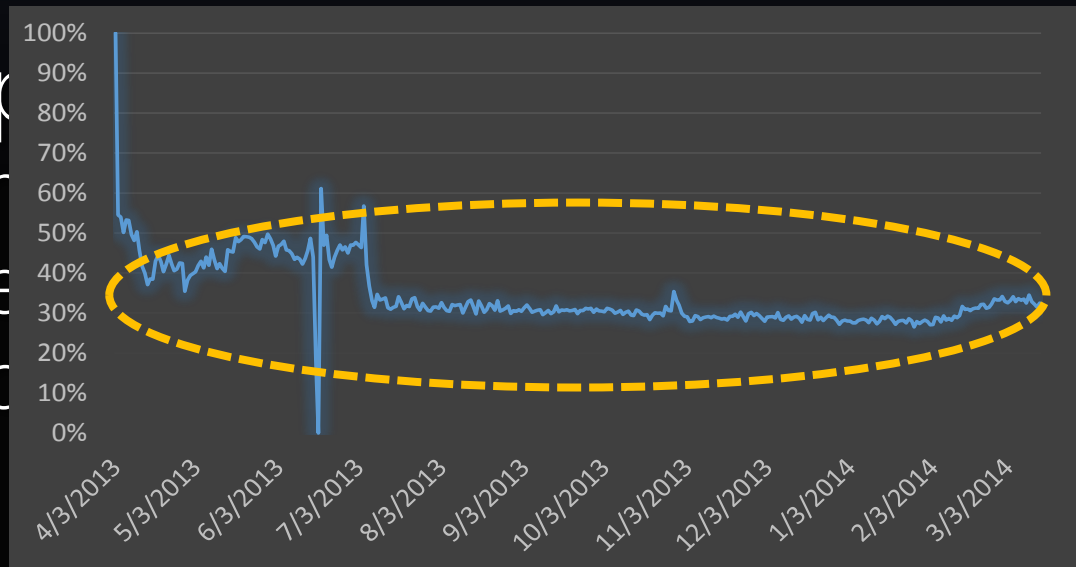
GFW stopped blocking

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.

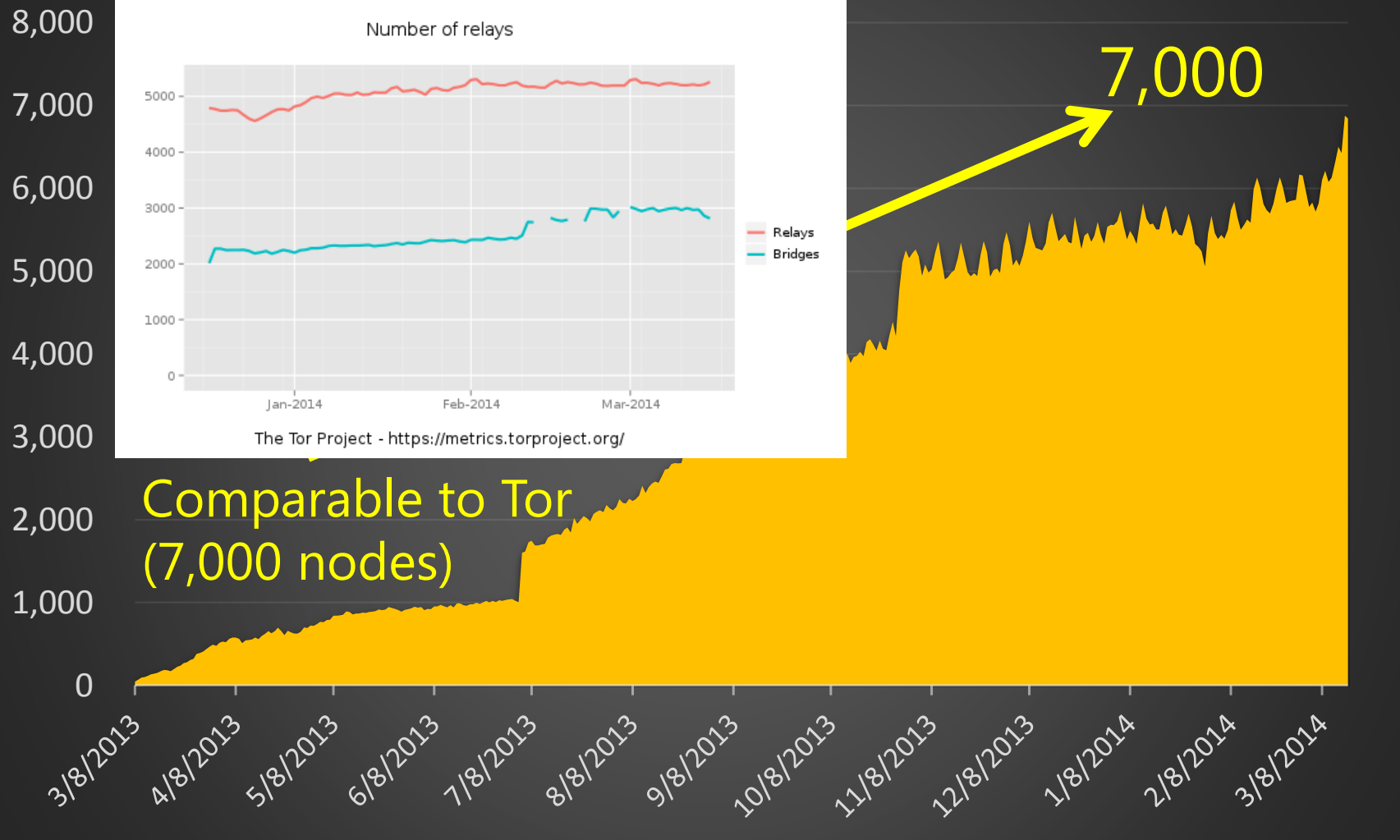
- We support

- GFW r
- GFW e
- GFW c

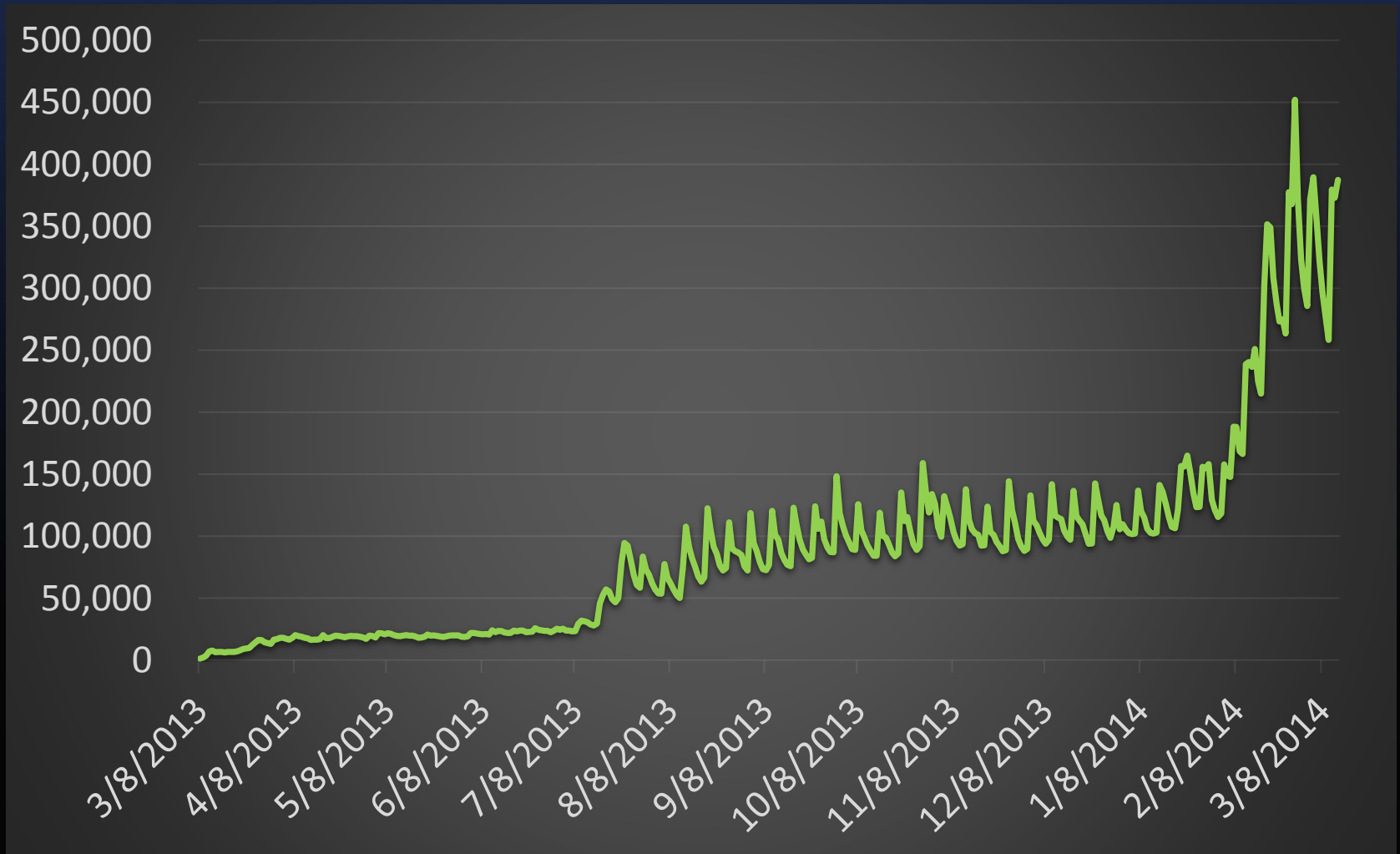


VPN Gate.

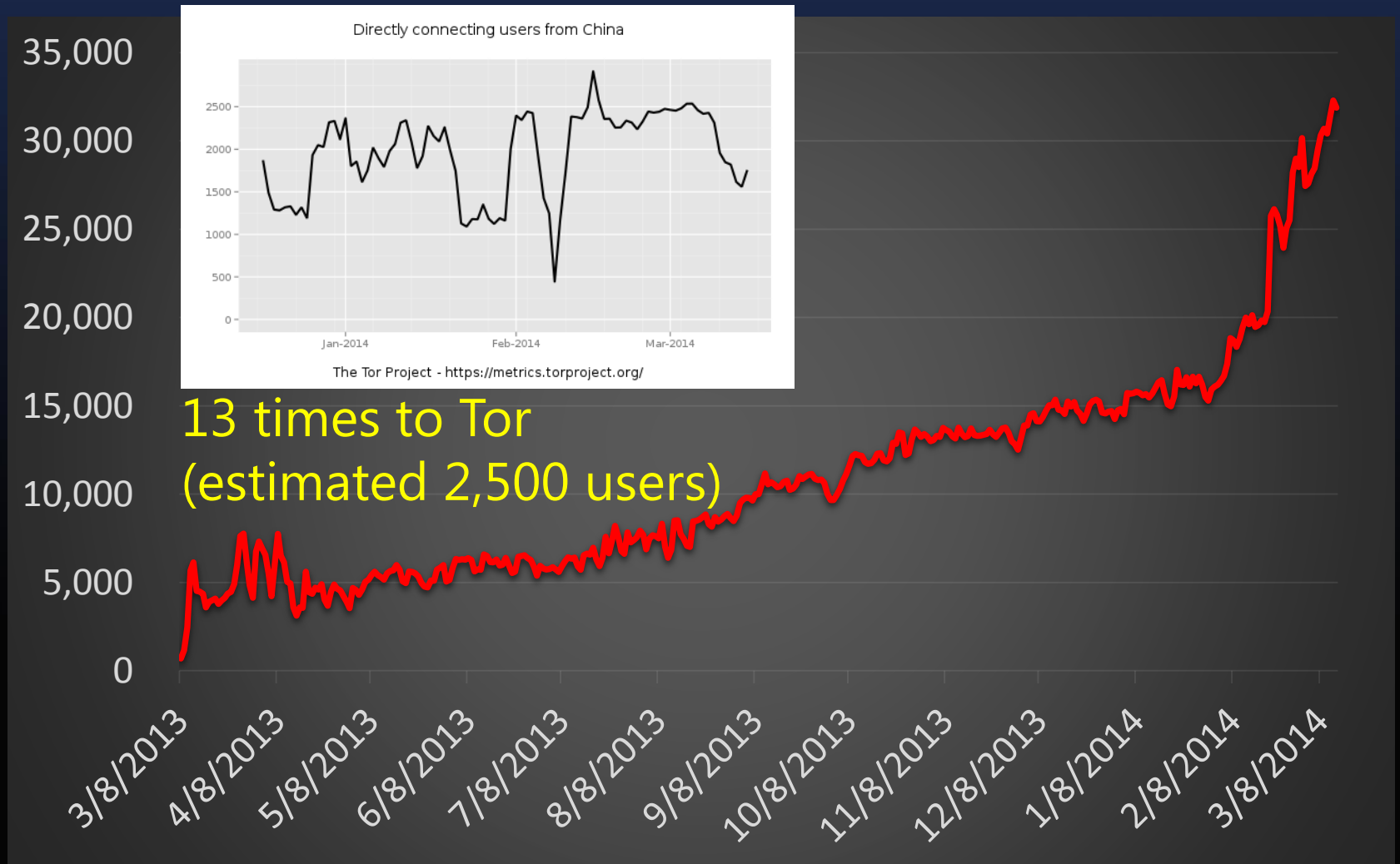
Numbers of active VPN Gate Servers



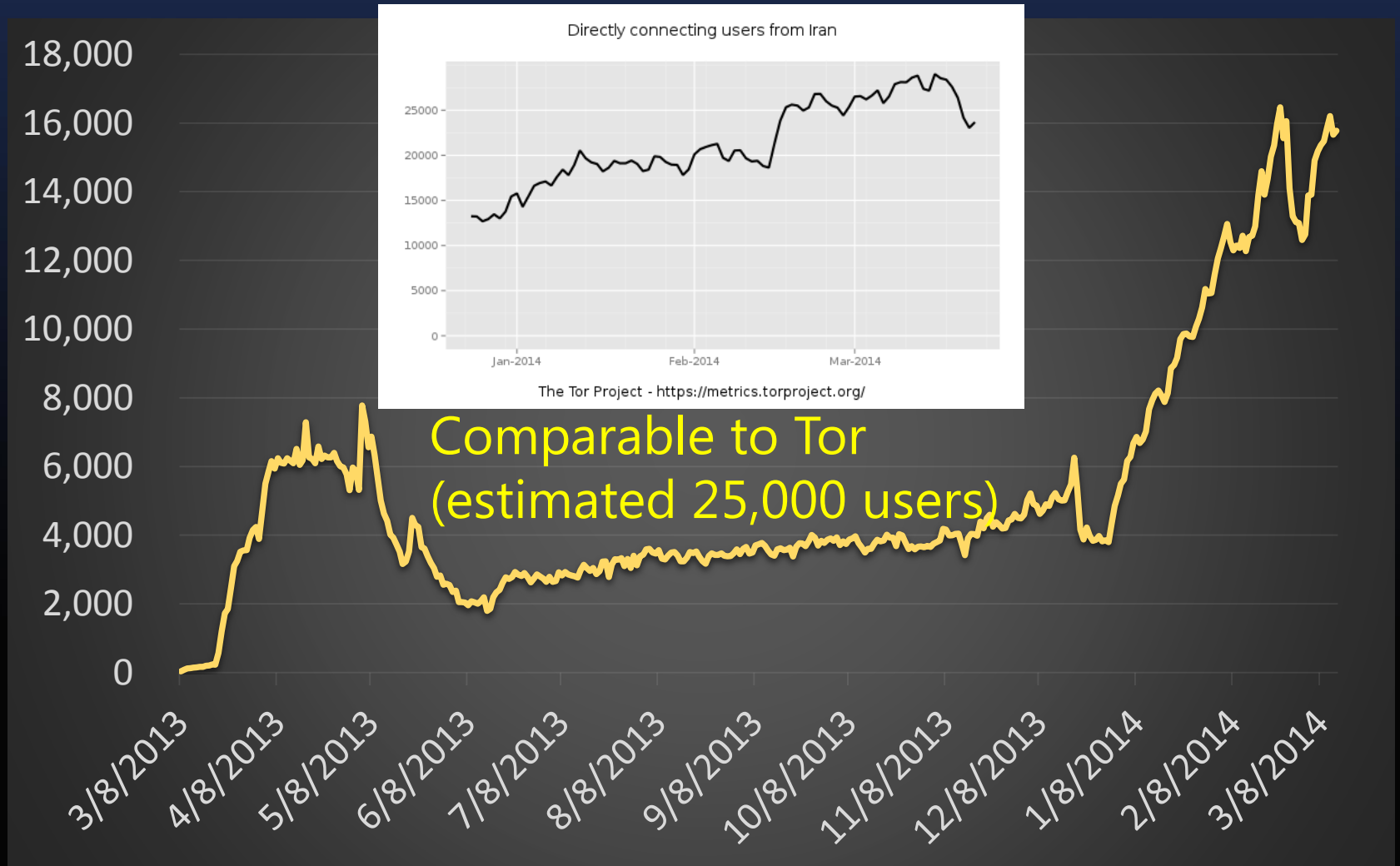
400,000 daily unique client IPs, world wide










32,000 daily unique client IPs from China

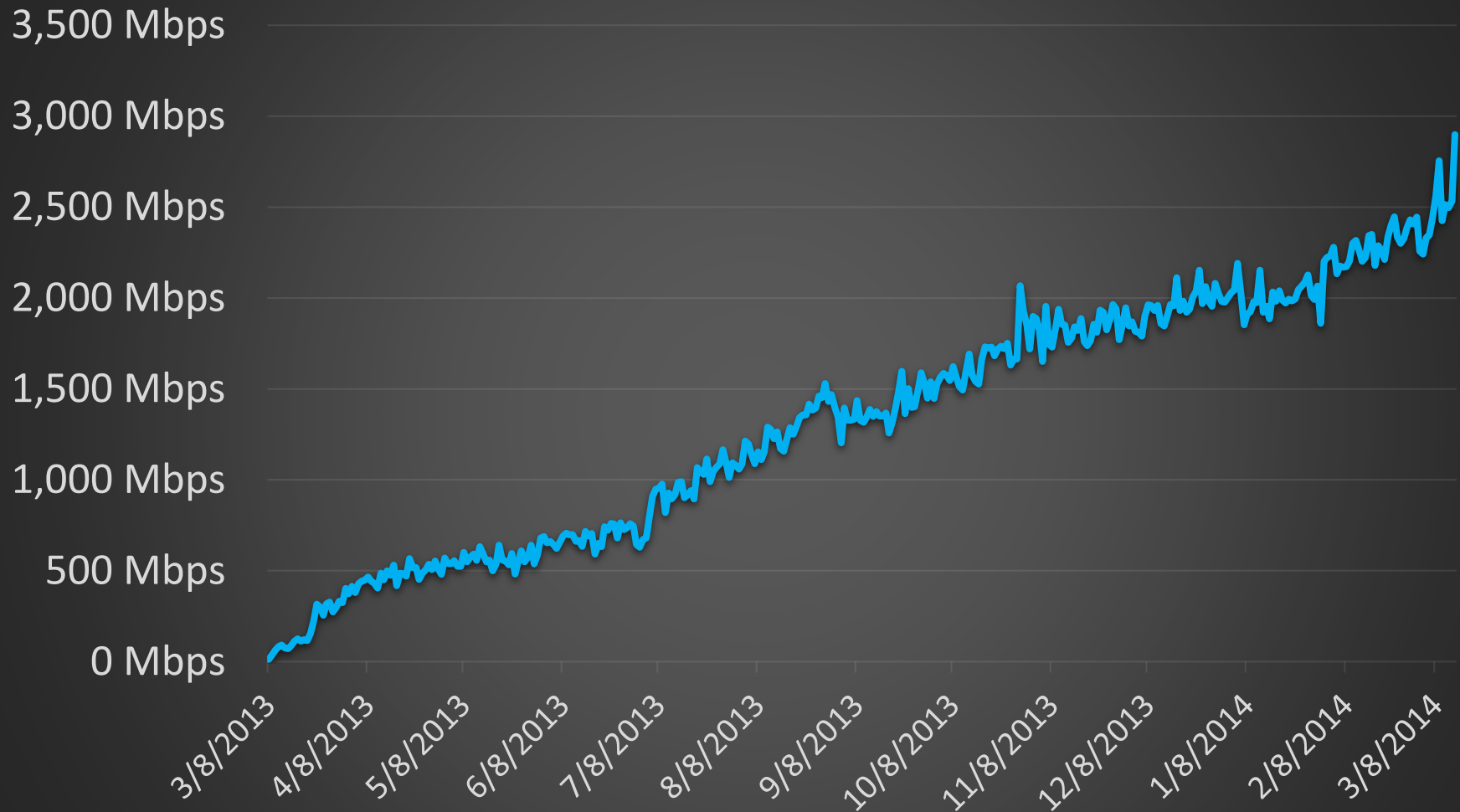


16,000 daily unique client IPs from Iran



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

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