Software Systems for Surveying Spoofing Susceptibility

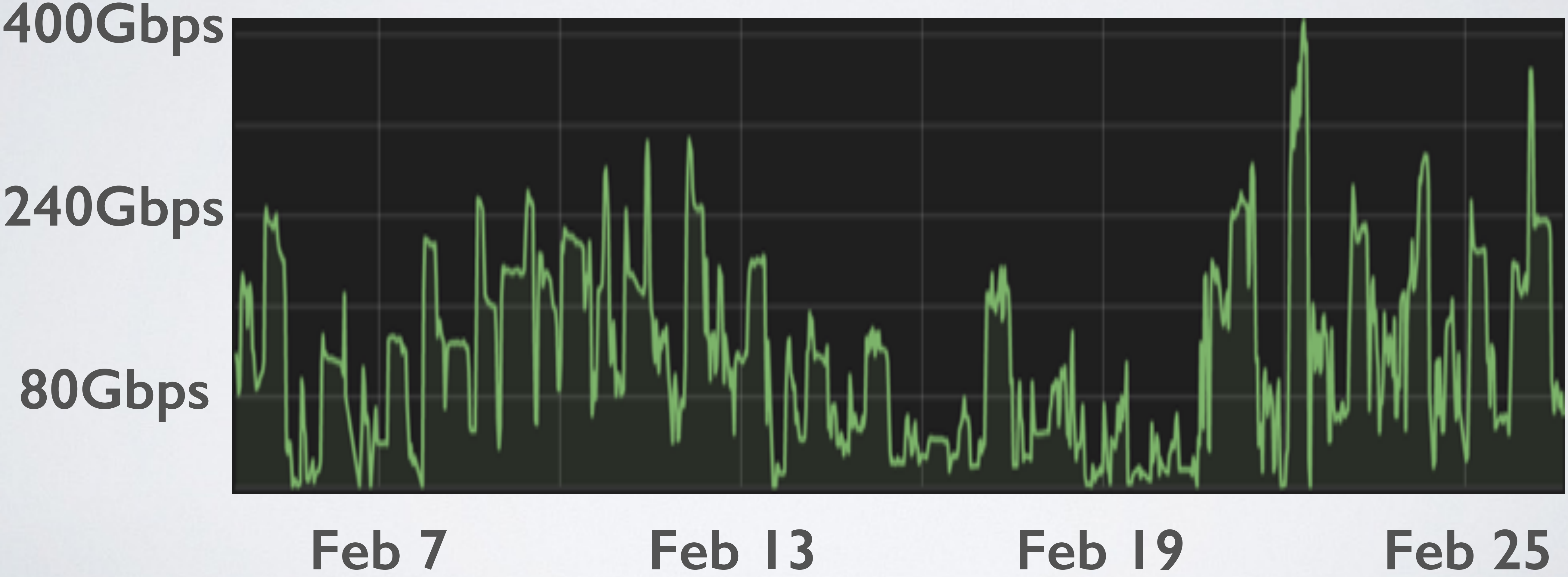
Matthew Luckie, Ken Keys, Ryan Koga, Bradley Huffaker, Robert Beverly, kc claffy

https://spoofer.caida.org/

AusNOG 2016, September 2nd 2016

What is the Problem?

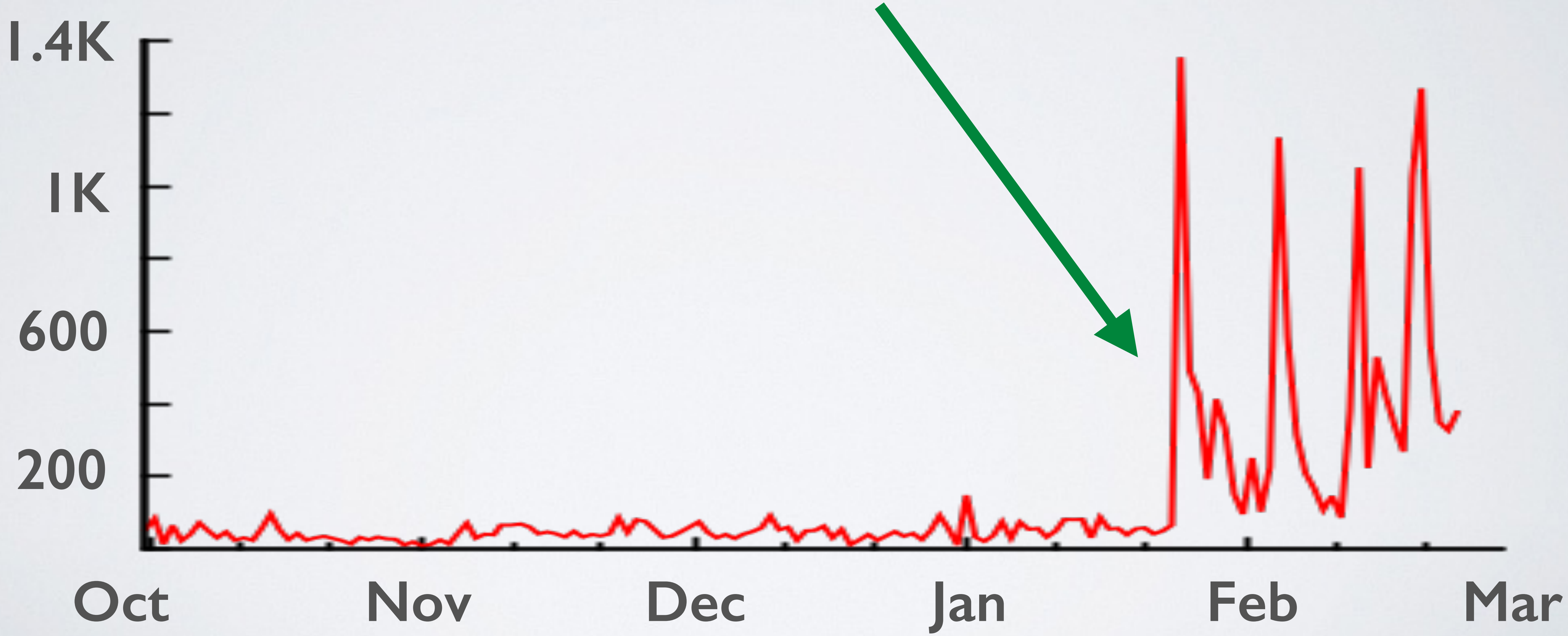
- Lack of filtering allows anonymous denial of service attacks.
- Example: CloudFlare reports **400Gbps attacks** on their systems through 2016



https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/

What is the Problem?

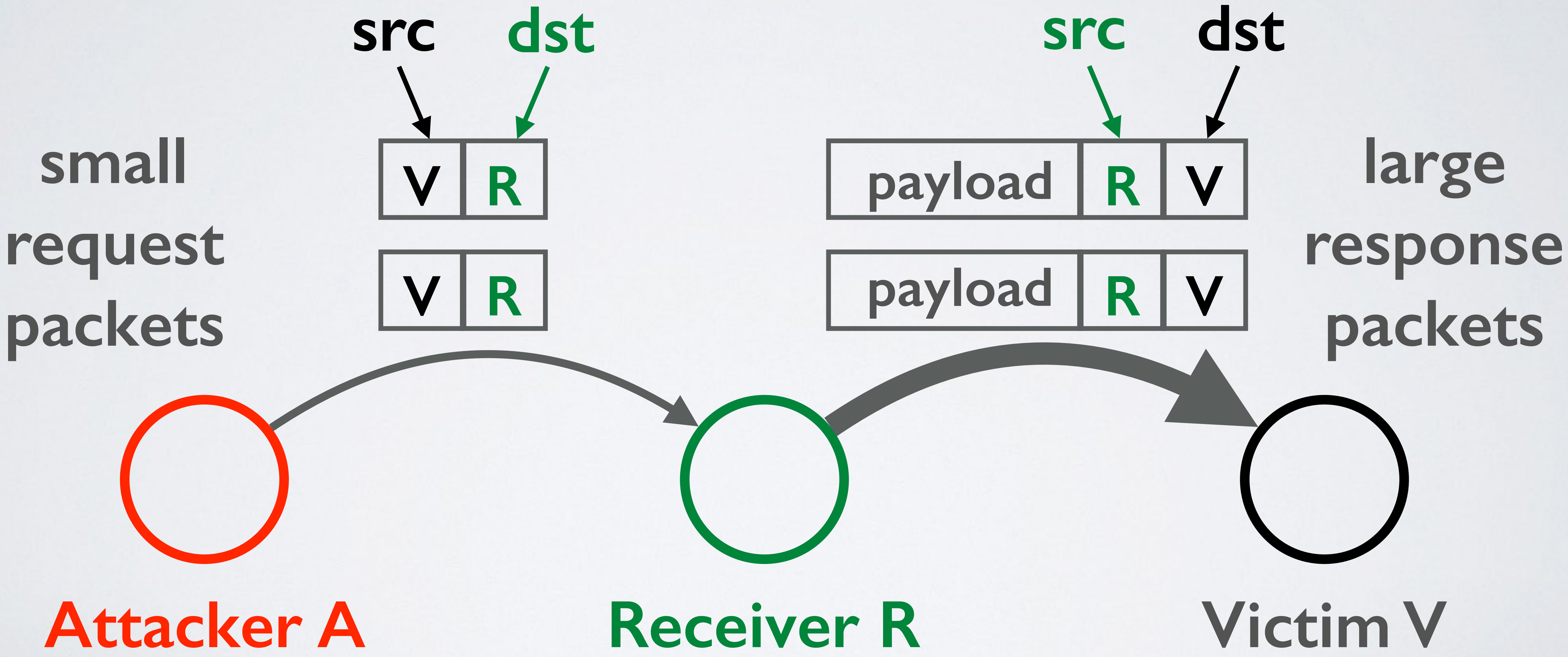
- Lack of filtering allows anonymous denial of service attacks.
- Example: CloudFlare reports **>1K DoS attack events** on their systems, per day, starting **Feb 2016**



https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/

Why does spoofing matter?

- Attacker sends packet with spoofed source IP address
- Receiver cannot always know if packet's source is authentic



Volumetric Reflection-Amplification Attack

Defenses

- **BCP38**: Network ingress filtering: defeating denial of service attacks which employ IP Source Address Spoofing
    - https://tools.ietf.org/html/bcp38
    - May 2000
- **BCP84**: Ingress filtering for multi-homed networks
    - https://tools.ietf.org/html/bcp84
    - March 2004
- Not always straightforward to deploy "source address validation" (SAV): BCP84 provides advice how to deploy

Tragedy of the Commons

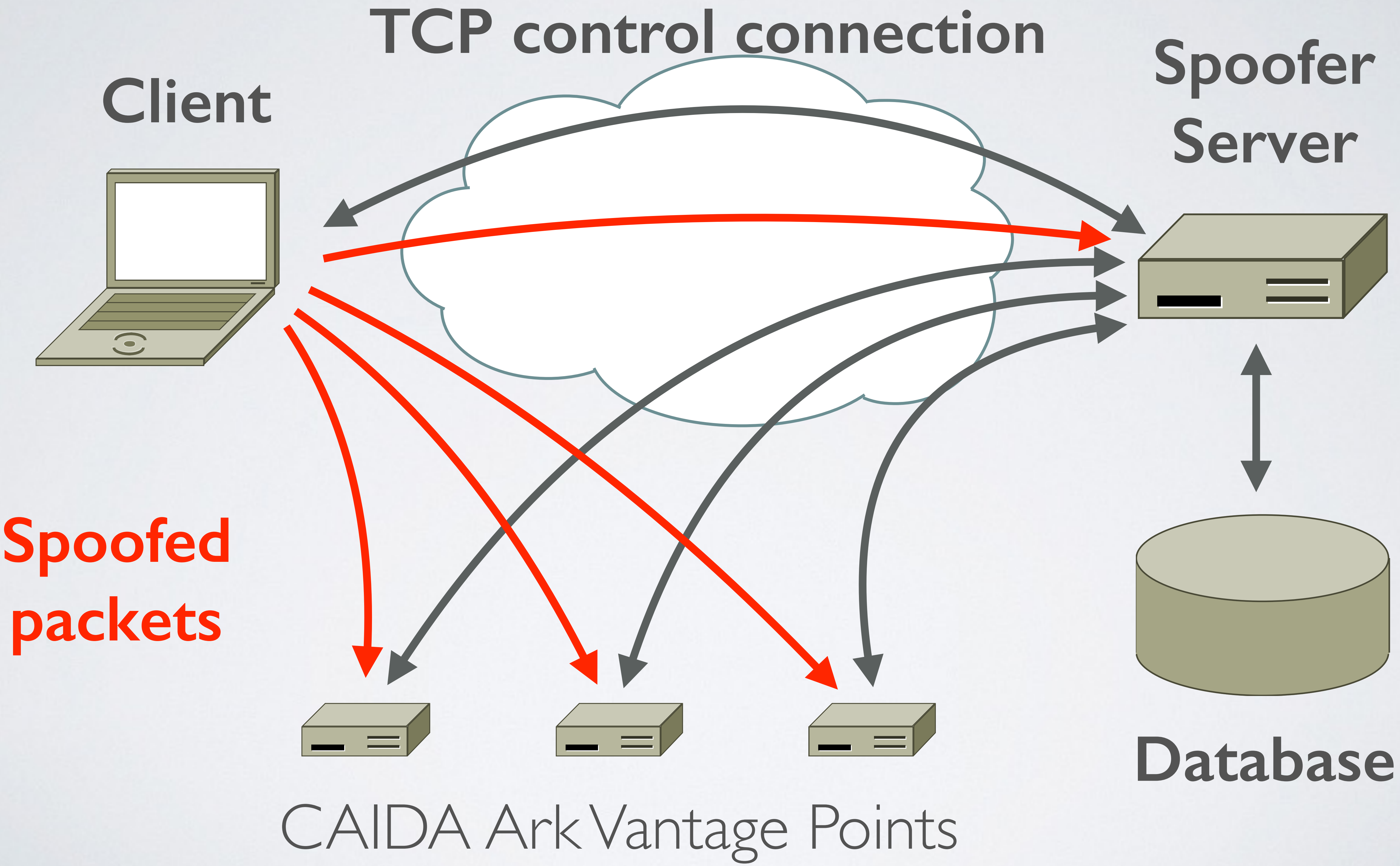
- Deploying source address validation is **primarily for the benefit of other networks**
- **Incentive not clear for some networks**
  - majority of networks do seem to deploy filtering
  - filtering gives an operator moral high-ground to pressure other networks to deploy, which does benefit the operator
  - "Cyber Insurance" takes into account security practice of the network: QuadMetrics.com
- ISOC RoutingManifesto.org: Mutually Agreed Norms for Routing Security (MANRS)

MANRS

Which networks have deployed filtering?

- **No public data that allows a network to show that they have (or have not) deployed filtering**
- **OpenResolverProject**: allows detection of which networks have not deployed filtering based on DNS request forwarding
  - requires a buggy open resolver
  - public reporting at network and AS level
- **MIT/CMAND Spoofer Project**: aggregate statistics of spoofability based on crowd-sourced tests
  - user had to manually run tests
  - no public reporting at network or AS level

Spoofer: Client/Server Overview



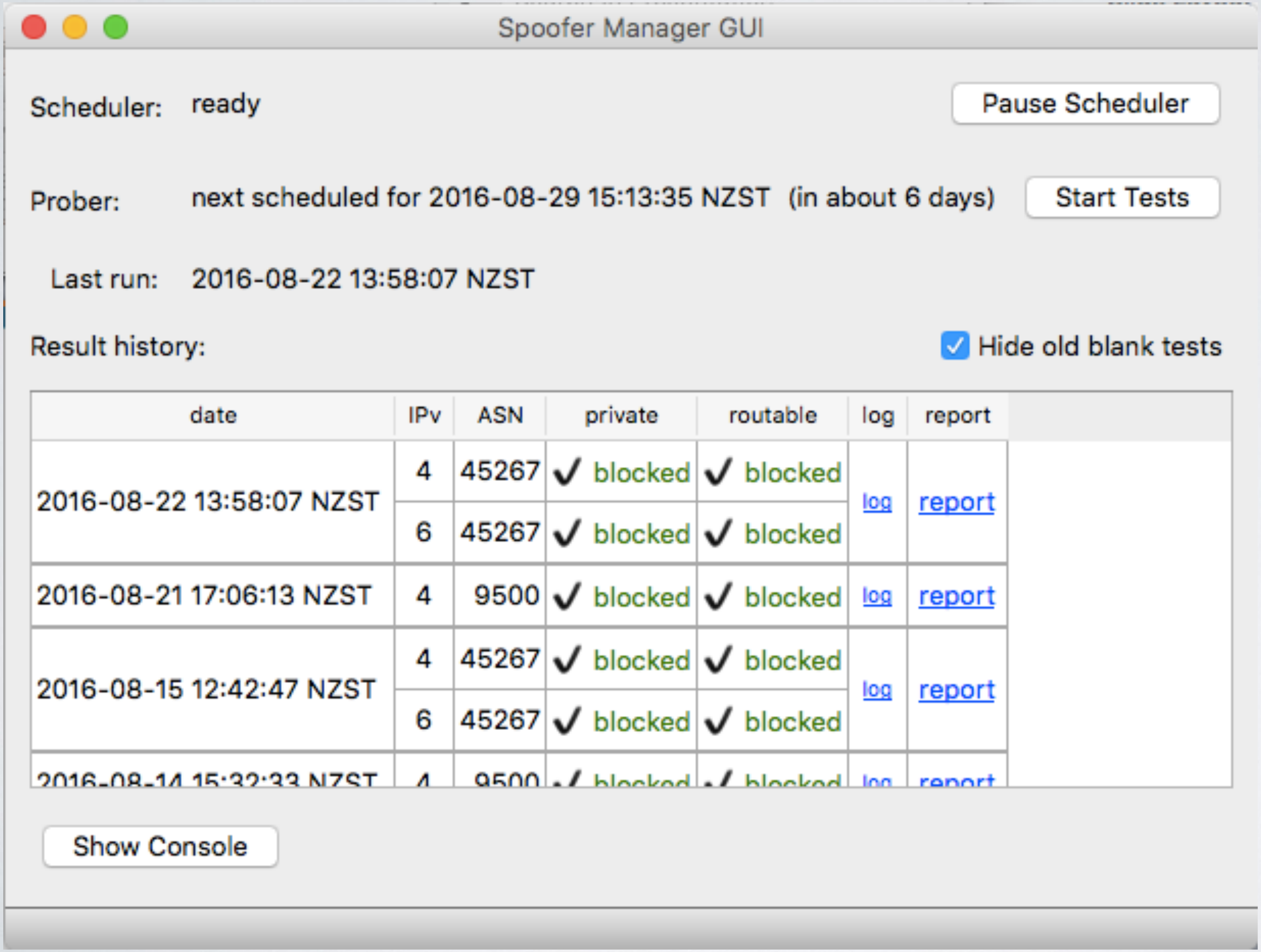
Spoofer: Client/Server Overview

- Client tests ability to spoof packets of different types
  - Routed and Private
  - IPv4 and IPv6
- **`traceroute`** to infer forward path to destinations
- **`tracefilter`** to infer first location of filtering in a path
  - traceroute but with spoofed packets
- Filtering prefix granularity: how many addresses in the same network prefix can be spoofed?

CAIDA Spoofer Project: New Features

- **Client/Server** system provides new useful features
  - **opt-in to publicly share anonymized results, and opt-in to share unanonymized results for remediation**
  - Runs in background, automatically testing new networks the host is attached to, once per week, IPv4 and IPv6
  - GUI to browse test results from your host, schedule tests
- **Reporting Engine** publicly shows outcomes of sharable tests
  - Allows users to select outcomes per country, per ASN
  - **https://spoofer.caida.org/recent_tests.php**

Client GUI



Scheduler: ready

Prober: next scheduled for 2016-08-29 15:13:35 NZST (in about 6 days)

Last run: 2016-08-22 13:58:07 NZST

Result history:

☑ Hide old blank tests

date	IPv	ASN	private	routable	log	report
2016-08-22 13:58:07 NZST	4	45267	✓ blocked	✓ blocked	log	report
	6	45267	✓ blocked	✓ blocked		
2016-08-21 17:06:13 NZST	4	9500	✓ blocked	✓ blocked	log	report
2016-08-15 12:42:47 NZST	4	45267	✓ blocked	✓ blocked	log	report
	6	45267	✓ blocked	✓ blocked		
2016-08-14 15:32:33 NZST	4	9500	✓ blocked	✓ blocked	log	report

Signed Installers

MacOS

Windows

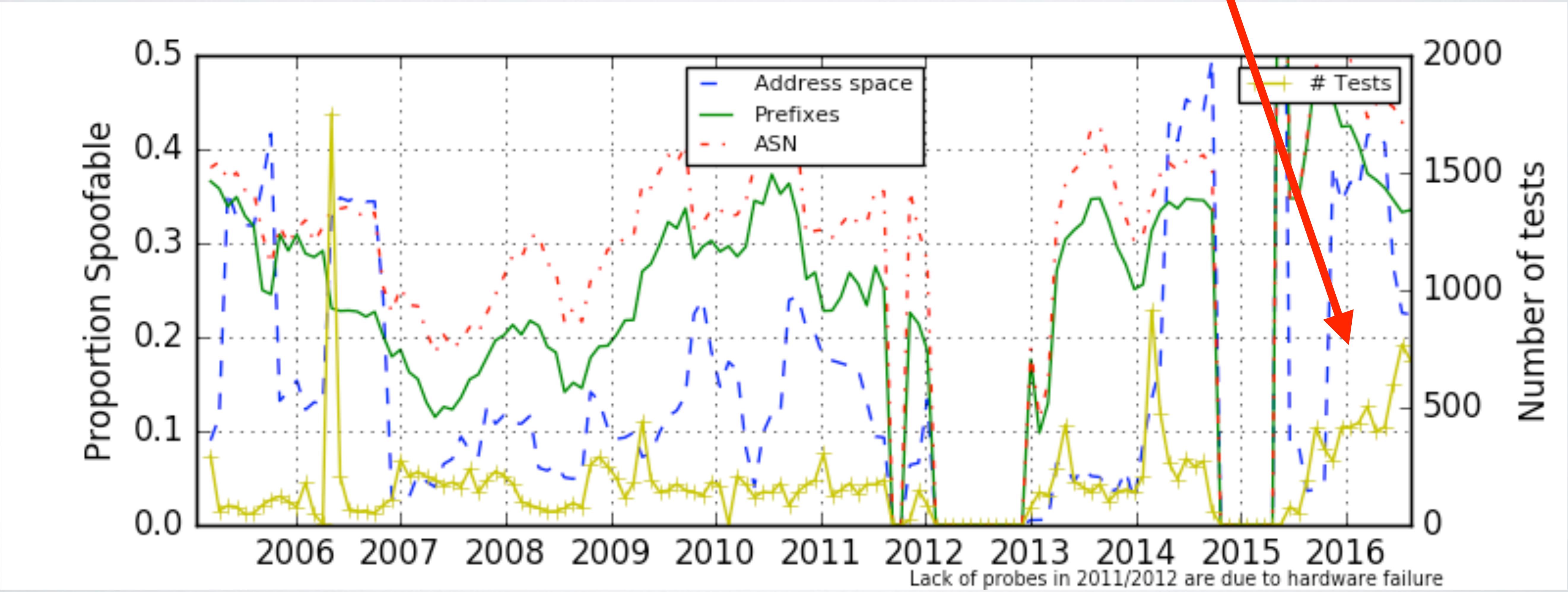
Linux

Open Source

C++

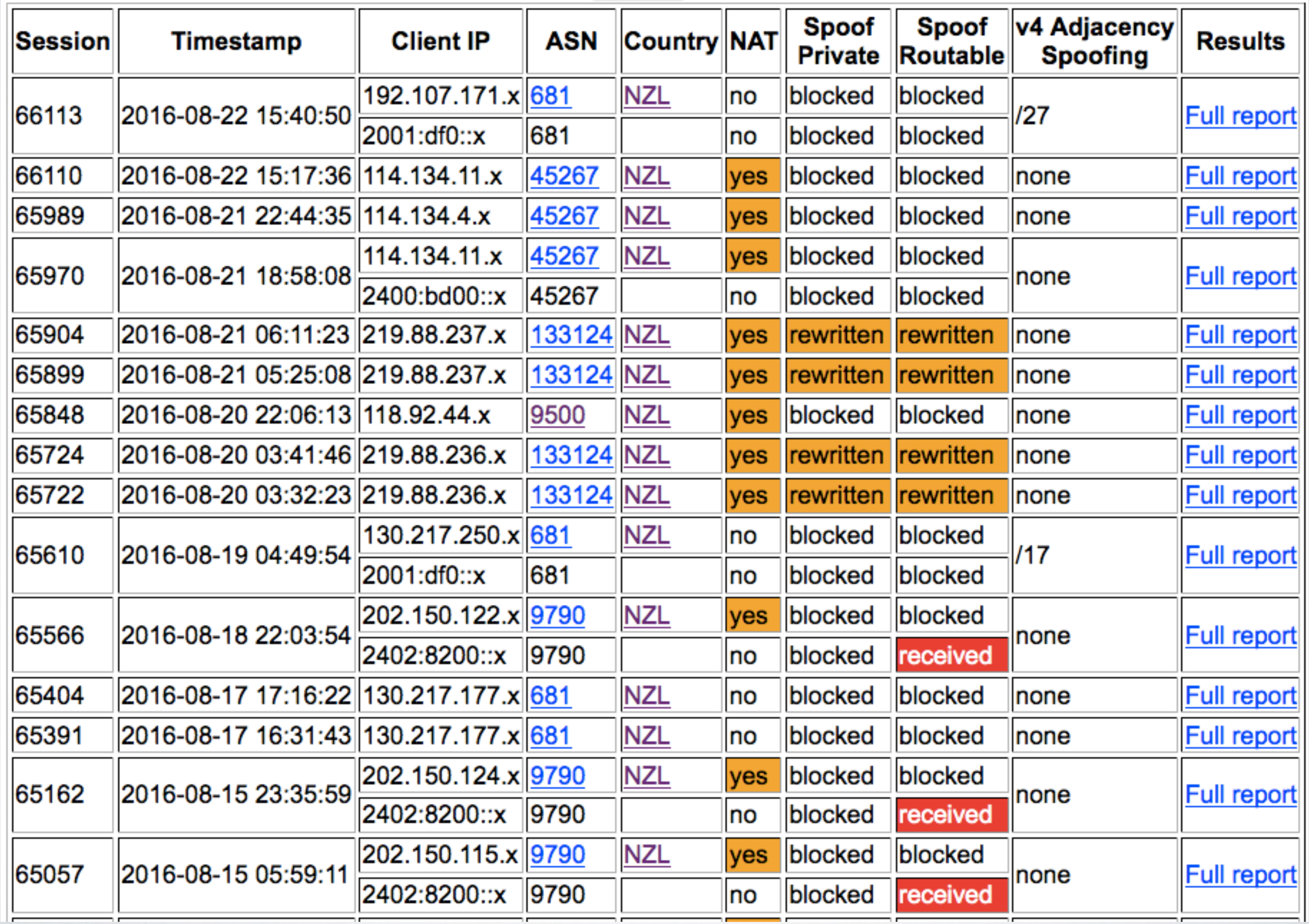
Client/Server Deployment

- Since releasing new client in May, increasing trend of more tests (yellow line)
  - Benefit of system running in background
  - Haven't started deployment push, today is first public talk



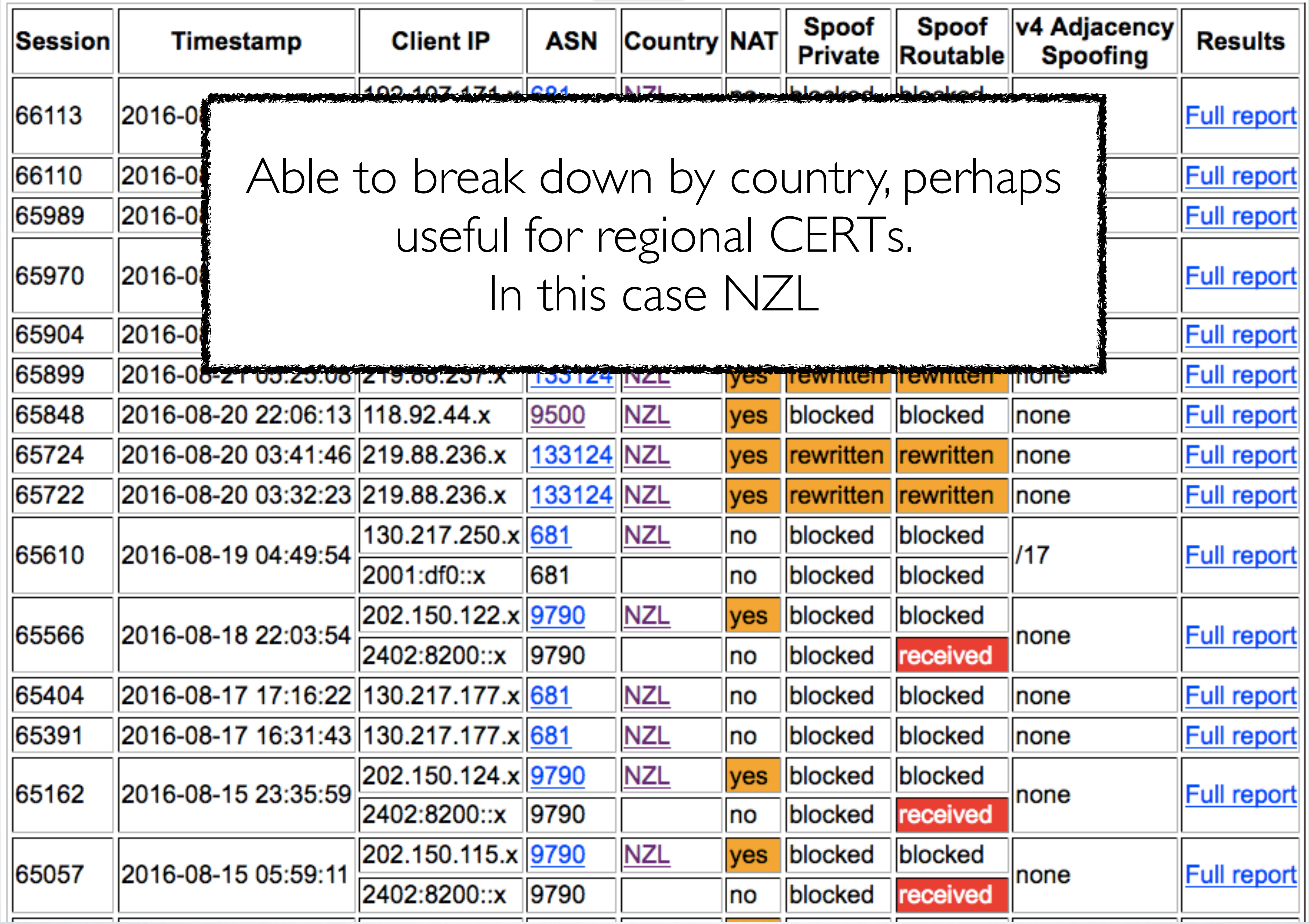
Lack of probes in 2011/2012 are due to hardware failure

Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
66113	2016-08-22 15:40:50	192.107.171.x	681	NZL	no	blocked	blocked	/27	Full report
		2001:df0::x	681		no	blocked	blocked		
66110	2016-08-22 15:17:36	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
65989	2016-08-21 22:44:35	114.134.4.x	45267	NZL	yes	blocked	blocked	none	Full report
65970	2016-08-21 18:58:08	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
		2400:bd00::x	45267		no	blocked	blocked		
65904	2016-08-21 06:11:23	219.88.237.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65899	2016-08-21 05:25:08	219.88.237.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65848	2016-08-20 22:06:13	118.92.44.x	9500	NZL	yes	blocked	blocked	none	Full report
65724	2016-08-20 03:41:46	219.88.236.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65722	2016-08-20 03:32:23	219.88.236.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65610	2016-08-19 04:49:54	130.217.250.x	681	NZL	no	blocked	blocked	/17	Full report
		2001:df0::x	681		no	blocked	blocked		
65566	2016-08-18 22:03:54	202.150.122.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65404	2016-08-17 17:16:22	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65391	2016-08-17 16:31:43	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65162	2016-08-15 23:35:59	202.150.124.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65057	2016-08-15 05:59:11	202.150.115.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		

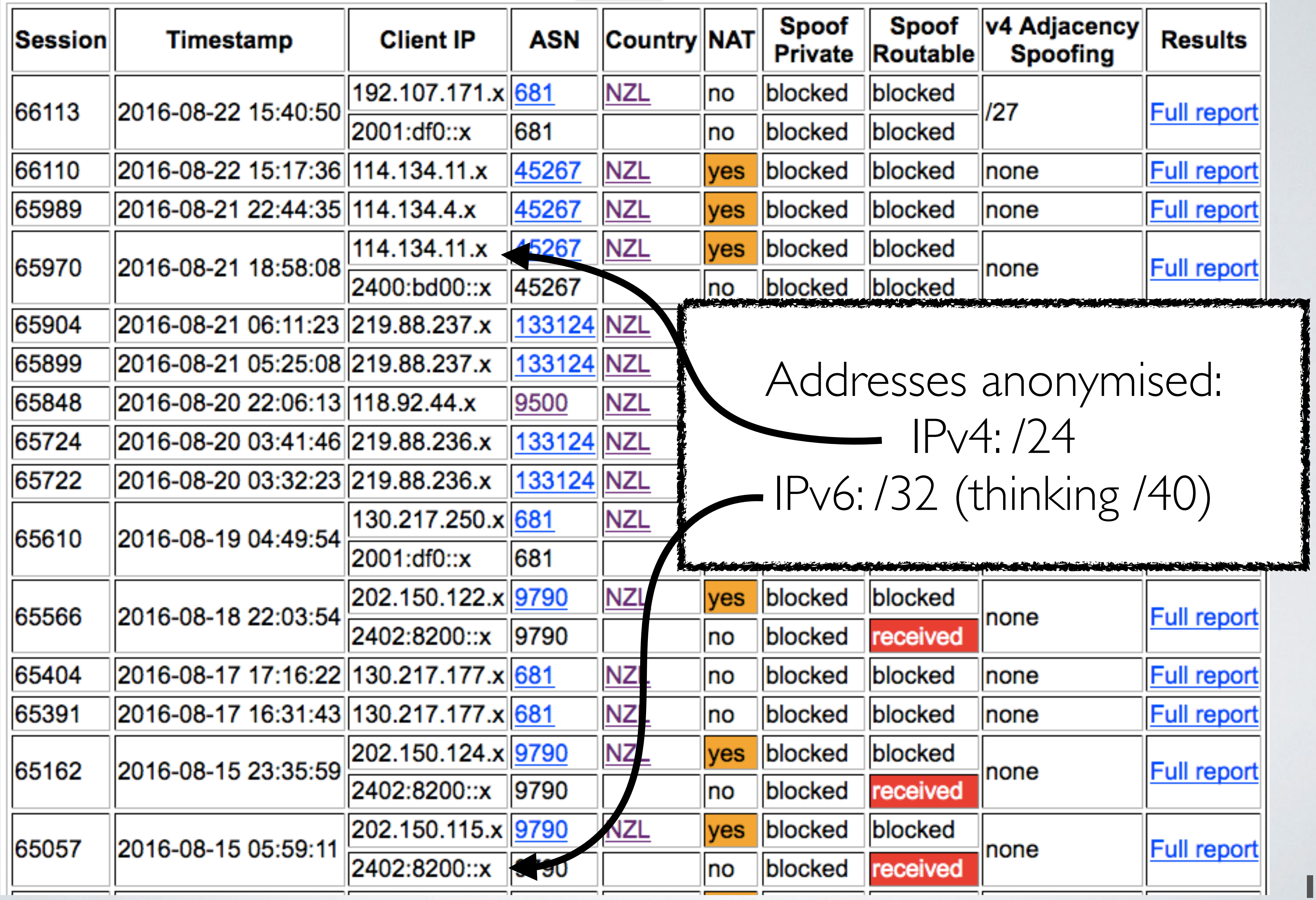
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
66113	2016-0[illegible]	192.107.171.x	681	NZL	no	blocked	blocked	[illegible]	Full report
66110	2016-0[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Full report
65989	2016-0[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Full report
65970	2016-0[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Full report
65904	2016-0[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Full report
65899	2016-08-21 05:25:08	219.88.237.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65848	2016-08-20 22:06:13	118.92.44.x	9500	NZL	yes	blocked	blocked	none	Full report
65724	2016-08-20 03:41:46	219.88.236.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65722	2016-08-20 03:32:23	219.88.236.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65610	2016-08-19 04:49:54	130.217.250.x	681	NZL	no	blocked	blocked	/17	Full report
		2001:df0::x	681		no	blocked	blocked		
65566	2016-08-18 22:03:54	202.150.122.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65404	2016-08-17 17:16:22	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65391	2016-08-17 16:31:43	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65162	2016-08-15 23:35:59	202.150.124.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65057	2016-08-15 05:59:11	202.150.115.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		

Able to break down by country, perhaps useful for regional CERTs.
In this case NZL

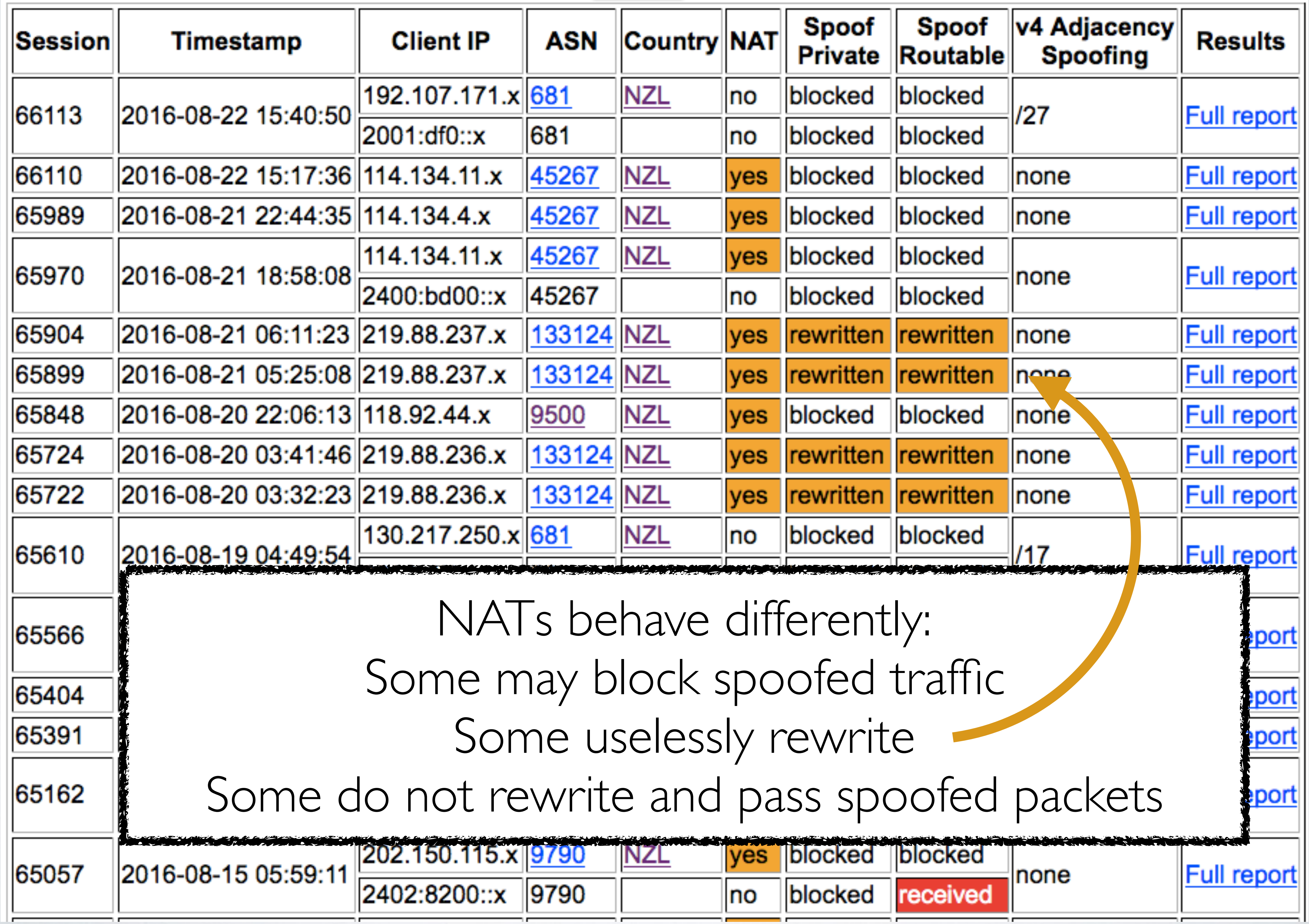
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
66113	2016-08-22 15:40:50	192.107.171.x	681	NZL	no	blocked	blocked	/27	Full report
		2001:df0::x	681		no	blocked	blocked		
66110	2016-08-22 15:17:36	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
65989	2016-08-21 22:44:35	114.134.4.x	45267	NZL	yes	blocked	blocked	none	Full report
65970	2016-08-21 18:58:08	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
		2400:bd00::x	45267		no	blocked	blocked		
65904	2016-08-21 06:11:23	219.88.237.x	133124	NZL					
65899	2016-08-21 05:25:08	219.88.237.x	133124	NZL					
65848	2016-08-20 22:06:13	118.92.44.x	9500	NZL					
65724	2016-08-20 03:41:46	219.88.236.x	133124	NZL					
65722	2016-08-20 03:32:23	219.88.236.x	133124	NZL					
65610	2016-08-19 04:49:54	130.217.250.x	681	NZL					
		2001:df0::x	681						
65566	2016-08-18 22:03:54	202.150.122.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65404	2016-08-17 17:16:22	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65391	2016-08-17 16:31:43	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65162	2016-08-15 23:35:59	202.150.124.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65057	2016-08-15 05:59:11	202.150.115.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		

Addresses anonymised:
IPv4: /24
IPv6: /32 (thinking /40)

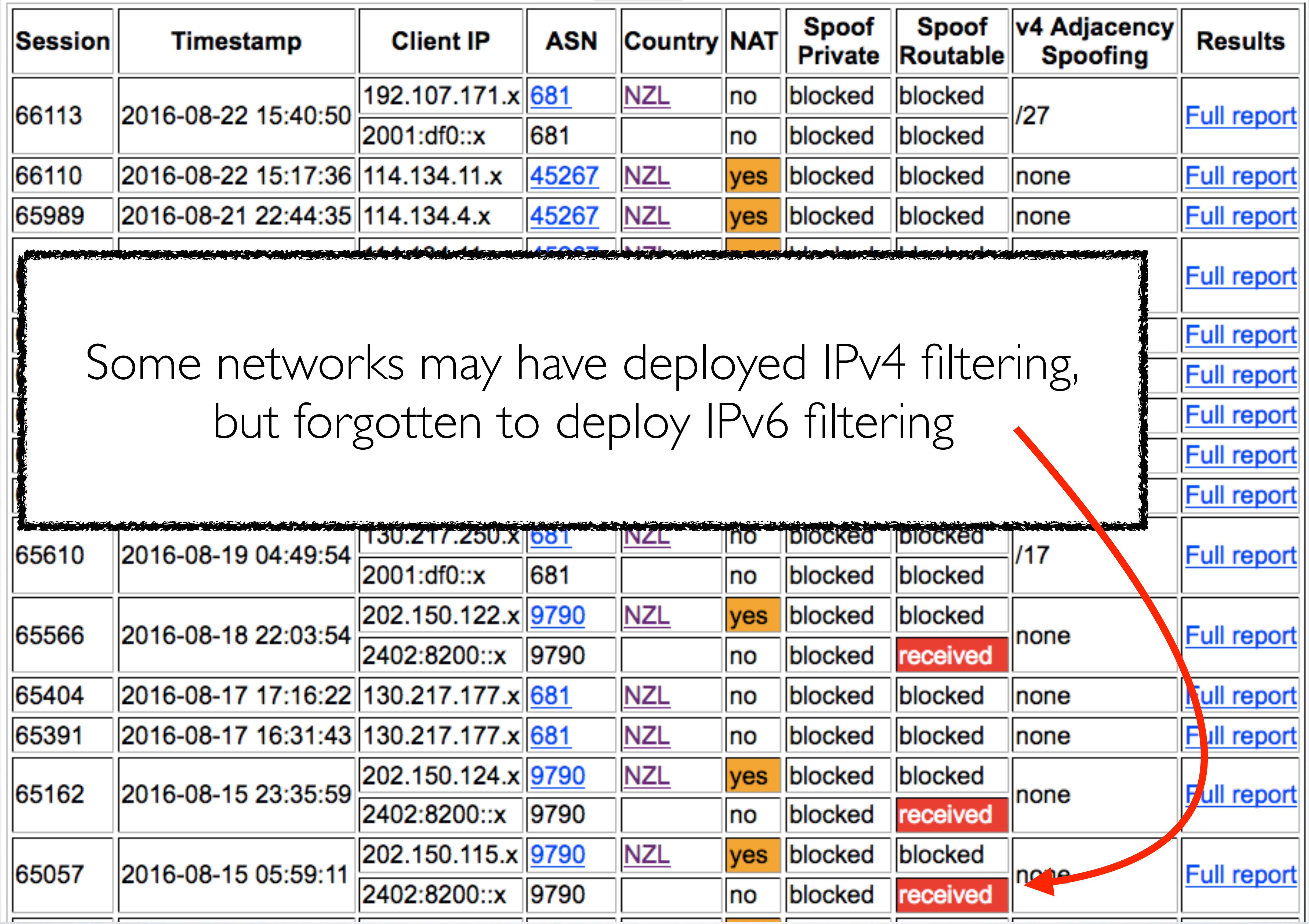
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
66113	2016-08-22 15:40:50	192.107.171.x	681	NZL	no	blocked	blocked	/27	Full report
		2001:df0::x	681		no	blocked	blocked		
66110	2016-08-22 15:17:36	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
65989	2016-08-21 22:44:35	114.134.4.x	45267	NZL	yes	blocked	blocked	none	Full report
65970	2016-08-21 18:58:08	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
		2400:bd00::x	45267		no	blocked	blocked		
65904	2016-08-21 06:11:23	219.88.237.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65899	2016-08-21 05:25:08	219.88.237.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65848	2016-08-20 22:06:13	118.92.44.x	9500	NZL	yes	blocked	blocked	none	Full report
65724	2016-08-20 03:41:46	219.88.236.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65722	2016-08-20 03:32:23	219.88.236.x	133124	NZL	yes	rewritten	rewritten	none	Full report
65610	2016-08-19 04:49:54	130.217.250.x	681	NZL	no	blocked	blocked	/17	Full report
65566									port
65404									port
65391									port
65162									port
65057	2016-08-15 05:59:11	202.150.115.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		

NATs behave differently:
Some may block spoofed traffic
Some uselessly rewrite
Some do not rewrite and pass spoofed packets

Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
66113	2016-08-22 15:40:50	192.107.171.x	681	NZL	no	blocked	blocked	/27	Full report
		2001:df0::x	681		no	blocked	blocked		
66110	2016-08-22 15:17:36	114.134.11.x	45267	NZL	yes	blocked	blocked	none	Full report
65989	2016-08-21 22:44:35	114.134.4.x	45267	NZL	yes	blocked	blocked	none	Full report
									Full report
									Full report
									Full report
									Full report
									Full report
									Full report
65610	2016-08-19 04:49:54	130.217.250.x	681	NZL	no	blocked	blocked	/17	Full report
		2001:df0::x	681		no	blocked	blocked		
65566	2016-08-18 22:03:54	202.150.122.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65404	2016-08-17 17:16:22	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65391	2016-08-17 16:31:43	130.217.177.x	681	NZL	no	blocked	blocked	none	Full report
65162	2016-08-15 23:35:59	202.150.124.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		
65057	2016-08-15 05:59:11	202.150.115.x	9790	NZL	yes	blocked	blocked	none	Full report
		2402:8200::x	9790		no	blocked	received		

Some networks may have deployed IPv4 filtering, but forgotten to deploy IPv6 filtering

Should I install the client?

- **Yes!**

- Room full of laptops and people who travel (use different networks). Great opportunity to collect new users and grow visibility of filtering deployment practice

- What about NAT?

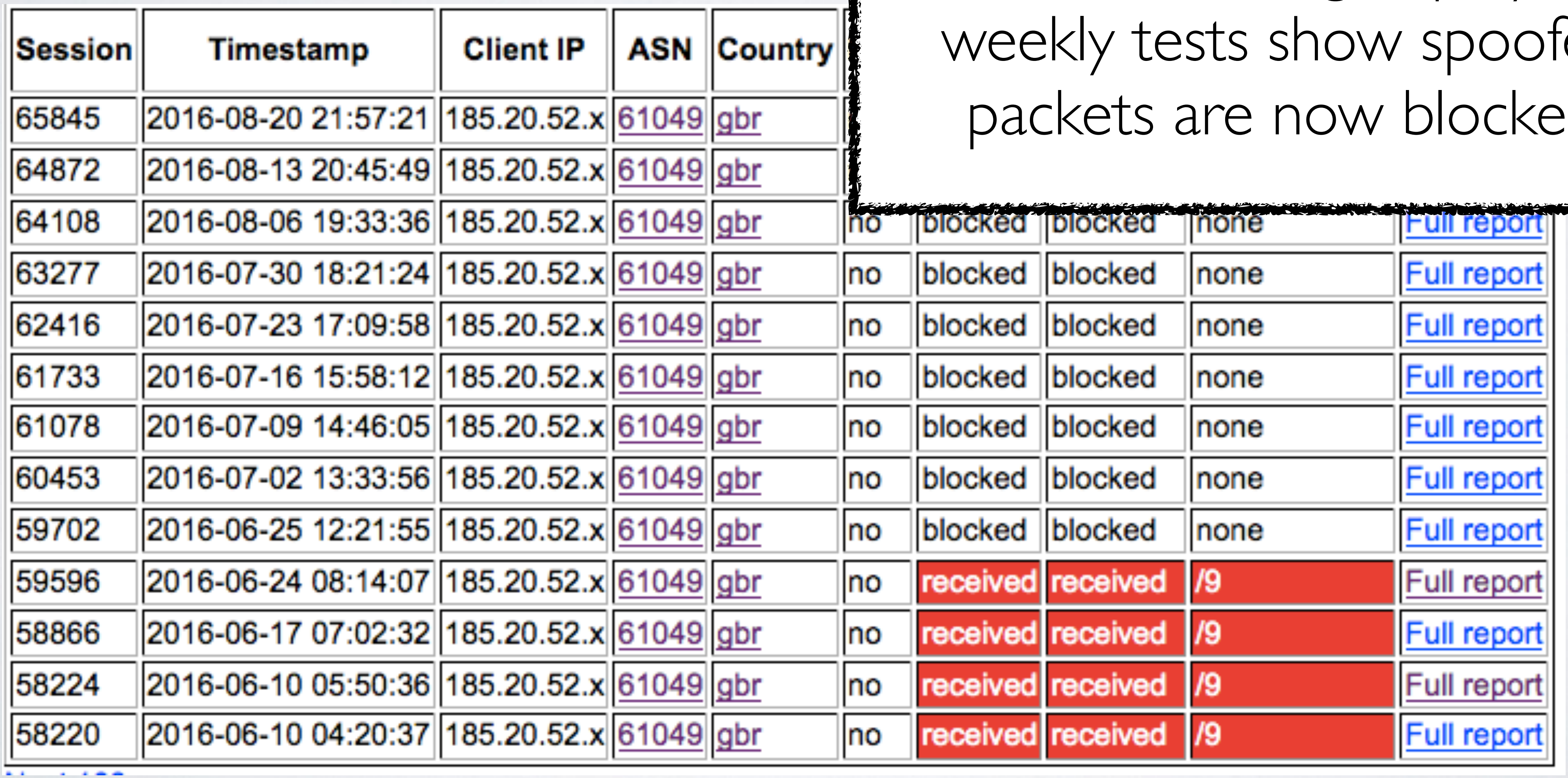
    - Not all NAT systems filter packets with spoofed source addresses

    - Roughly 35% of test results that showed spoof-ability were conducted from behind a NAT

Notifications and Remediation

- Currently, we (mostly I) manually send notifications to abuse contacts of prefixes from which we received spoofed packet

Successful filtering deployment: weekly tests show spoofed packets are now blocked

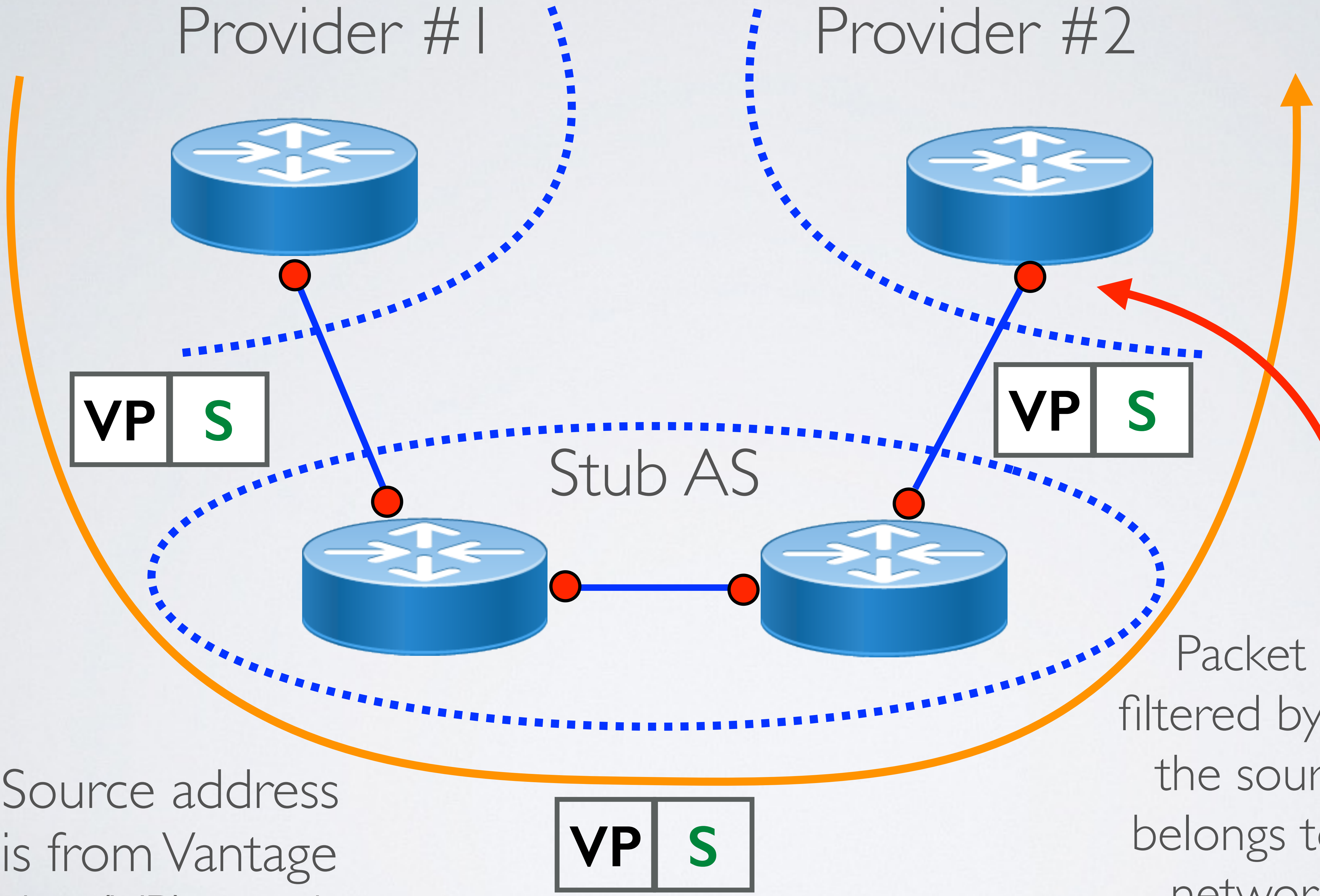


Session	Timestamp	Client IP	ASN	Country					
65845	2016-08-20 21:57:21	185.20.52.x	61049	gbr					
64872	2016-08-13 20:45:49	185.20.52.x	61049	gbr					
64108	2016-08-06 19:33:36	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
63277	2016-07-30 18:21:24	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
62416	2016-07-23 17:09:58	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
61733	2016-07-16 15:58:12	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
61078	2016-07-09 14:46:05	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
60453	2016-07-02 13:33:56	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
59702	2016-06-25 12:21:55	185.20.52.x	61049	gbr	no	blocked	blocked	none	Full report
59596	2016-06-24 08:14:07	185.20.52.x	61049	gbr	no	received	received	/9	Full report
58866	2016-06-17 07:02:32	185.20.52.x	61049	gbr	no	received	received	/9	Full report
58224	2016-06-10 05:50:36	185.20.52.x	61049	gbr	no	received	received	/9	Full report
58220	2016-06-10 04:20:37	185.20.52.x	61049	gbr	no	received	received	/9	Full report

Expanding View of Filtering Policy

- Use CAIDA traceroute data to infer customer-provider links to stub ASes that imply lack of ingress filtering by provider
- Goal: expand view of filtering policy, spur additional deployment of ingress ACLs
- Method suggested by Jared Mauch (NTT), joint work with Qasim Lone (TU Delft)

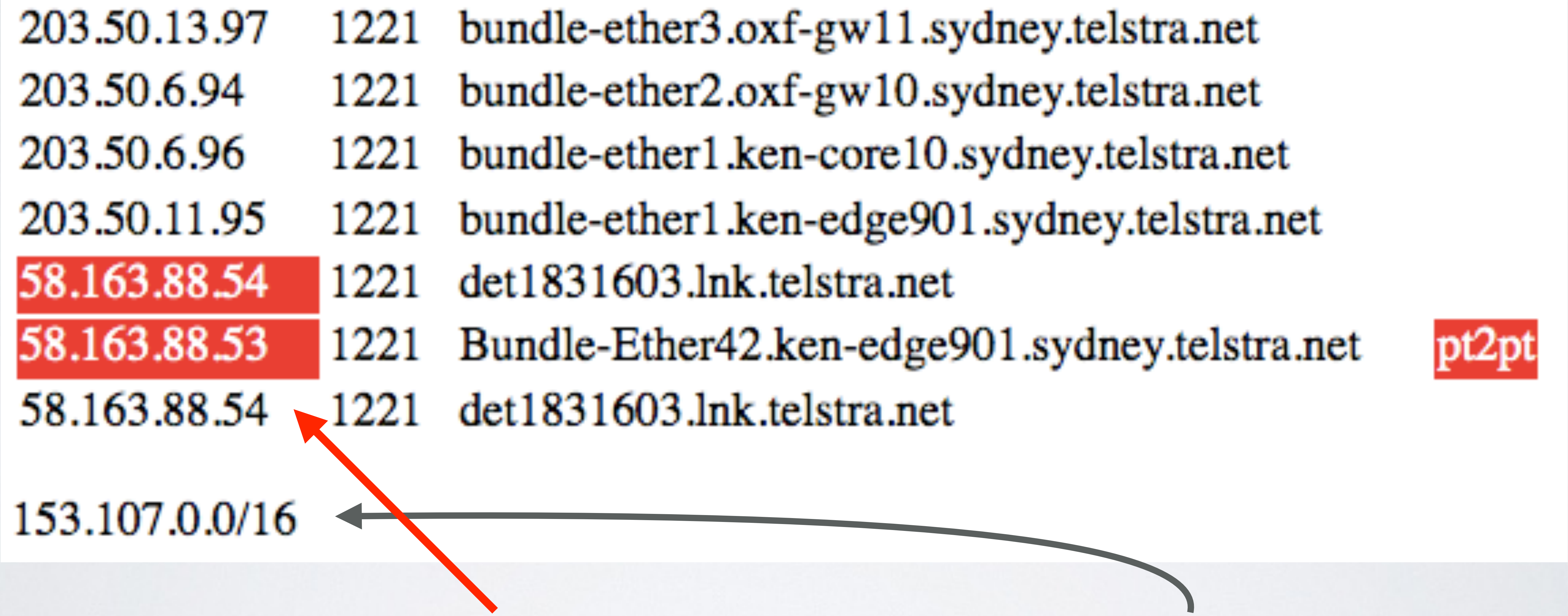
Traceroute Spoofer: Current Work



Source address is from Vantage Point (VP) running traceroute

Packet should be filtered by #2 because the source address belongs to a different network than the stub AS

Traceroute Spoofer: 1221-24313



```
203.50.13.97    1221   bundle-ether3.oxf-gw11.sydney.telstra.net
203.50.6.94     1221   bundle-ether2.oxf-gw10.sydney.telstra.net
203.50.6.96     1221   bundle-ether1.ken-core10.sydney.telstra.net
203.50.11.95    1221   bundle-ether1.ken-edge901.sydney.telstra.net
58.163.88.54    1221   det1831603.lnk.telstra.net
58.163.88.53    1221   Bundle-Ether42.ken-edge901.sydney.telstra.net      pt2pt
58.163.88.54    1221   det1831603.lnk.telstra.net

153.107.0.0/16
```

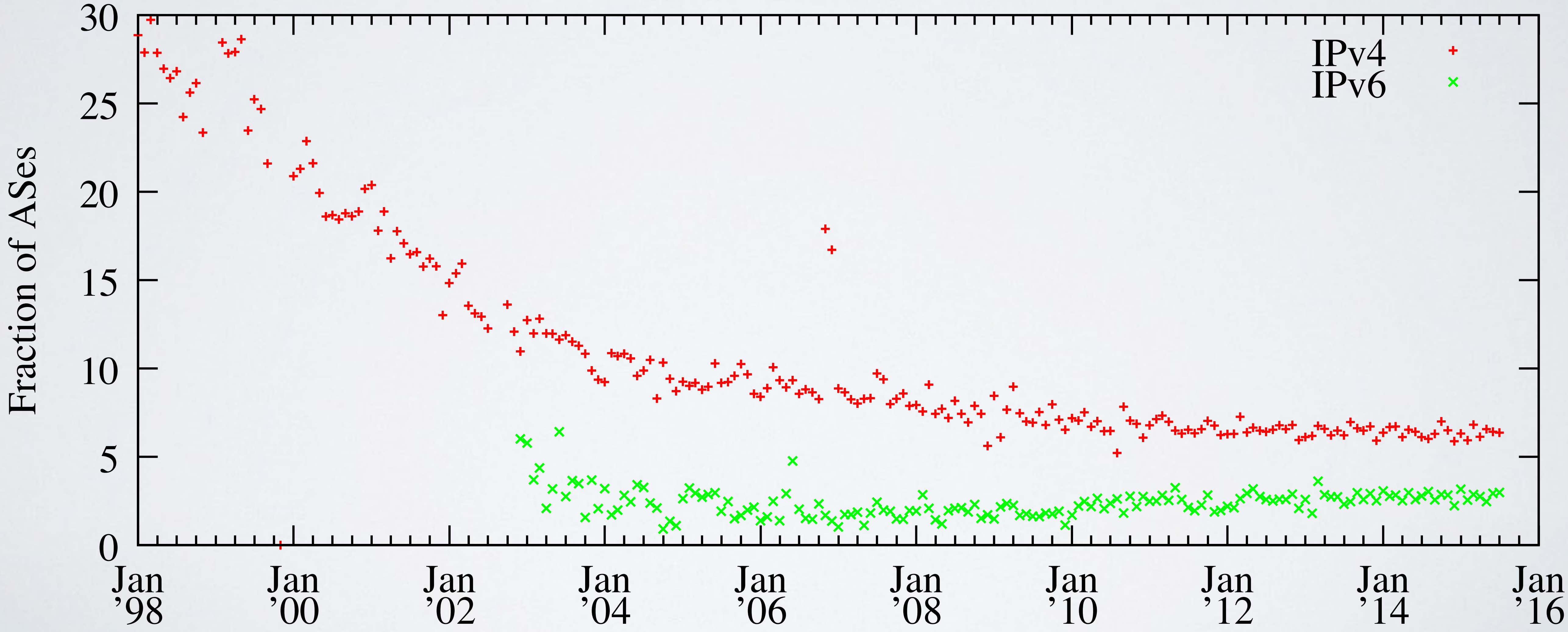
Customer-Provider Link

Suggested Ingress ACL

Goal: develop robust topological method to infer lack of ingress filtering

Use Ingress Access Lists!

During 2015, ~6% and ~3% of ASes announced different IPv4 and IPv6 address space month-to-month, respectively. Increased stability in addressing may make it feasible to use static ingress ACLs



Source Routeviews and RIPE RIS data

Where to from here?

- Would like to see the data have operational impact
  - This is where **you** come in!
  - What problems do you encounter when trying to deploy filtering?
- Currently working on automated notification
  - emails to abuse contacts.
- Working on a per-provider view
  - which of my customer ASes can spoof?
- Working to reduce prober run-time

Acknowledgements

- Project funded by U.S. Department of Homeland Security (DHS) Science and Technology (S&T) directorate

- Contacts:
  - spoofer-info@caida.org