http://commons.wikimedia.org/wiki/File:B1-B_Lancer_and_cluster_bombs.jpg

Coleg Sir Gâr

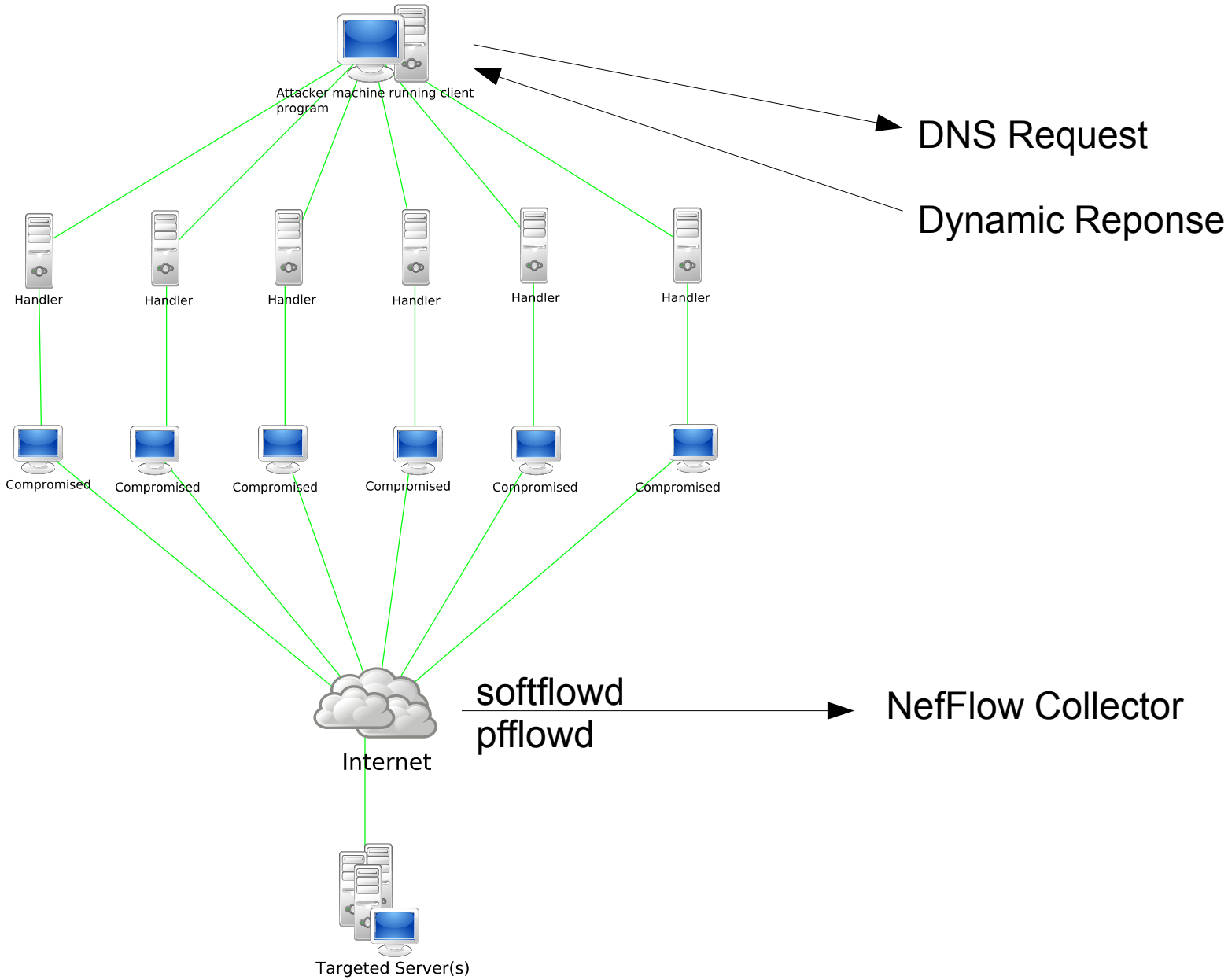
- Further Education (FE) 14+
- Higher Education (HE)
- 5 sites, ~10,000 students, ~850 staff
- 1Gbps Internet at HQ site
- 1Gbps Internet at DR site
- 1Gbps private circuit between sites

DdoS Services

- http://titaniumstresser.net
- http://powerstresser.com
- http://ipstresstest.com
- http://darkbooter.com
- http://pantheonstresser.com
- ....

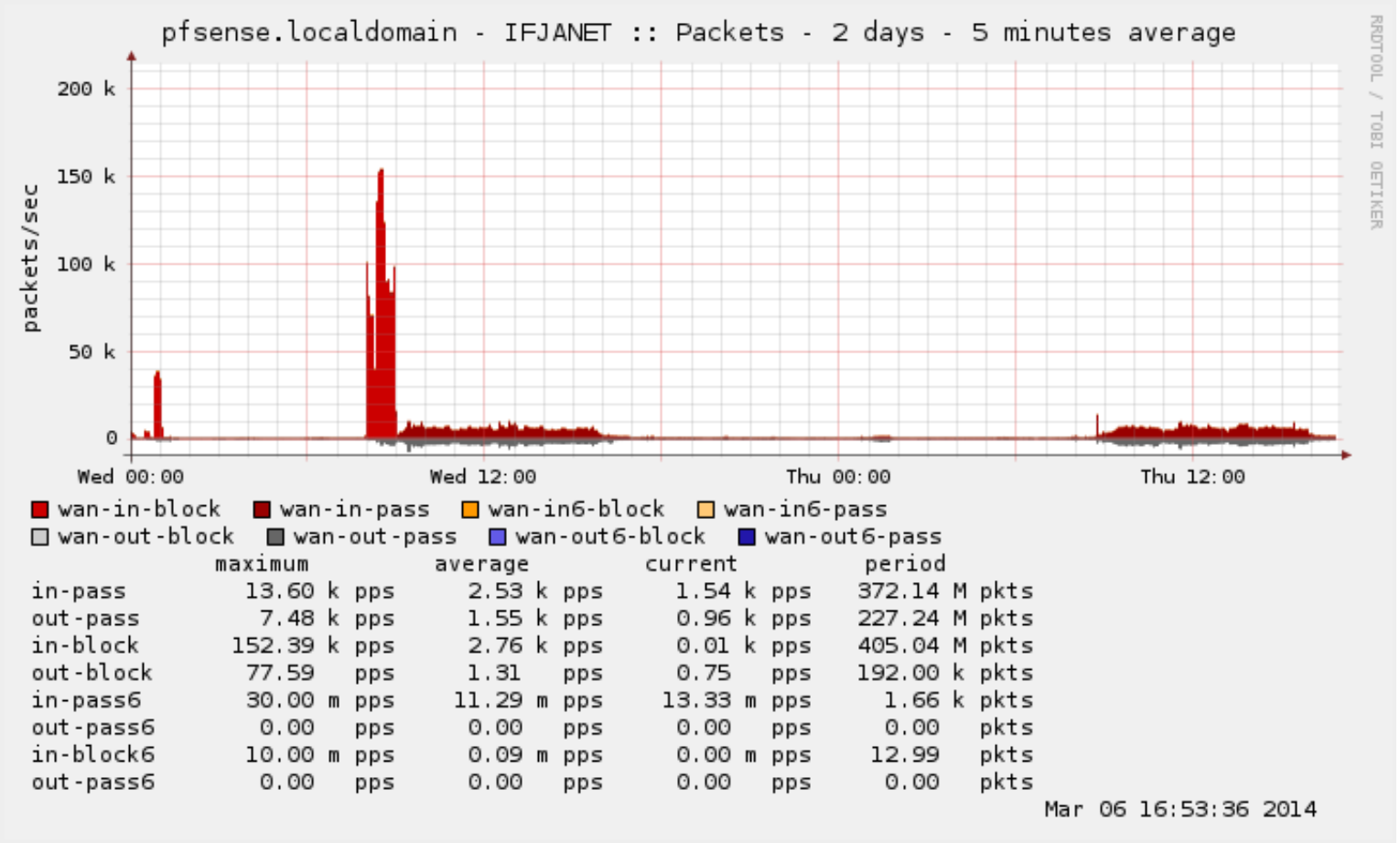
https://www.flickr.com/photos/n3pb/8765646099/in/set-72157634324914351/

```
================================
|| CONTROLLING LOIC FROM IRC ||
================================

As an OP, Admin or Owner, set the channel topic or send a message like the following:
!lazor targetip=127.0.0.1 message=test_test port=80 method=tcp wait=false random=true

To start an attack, type:
!lazor start

Or just append "start" to the END of the topic:
!lazor targetip=127.0.0.1 message=test_test port=80 method=tcp wait=false random=true
start

To reset loic's options back to its defaults:
!lazor default

To stop an attack:
!lazor stop
and be sure to remove "start" from the END of the topic, if it exists, too.

Take a look at source code for more details.
```

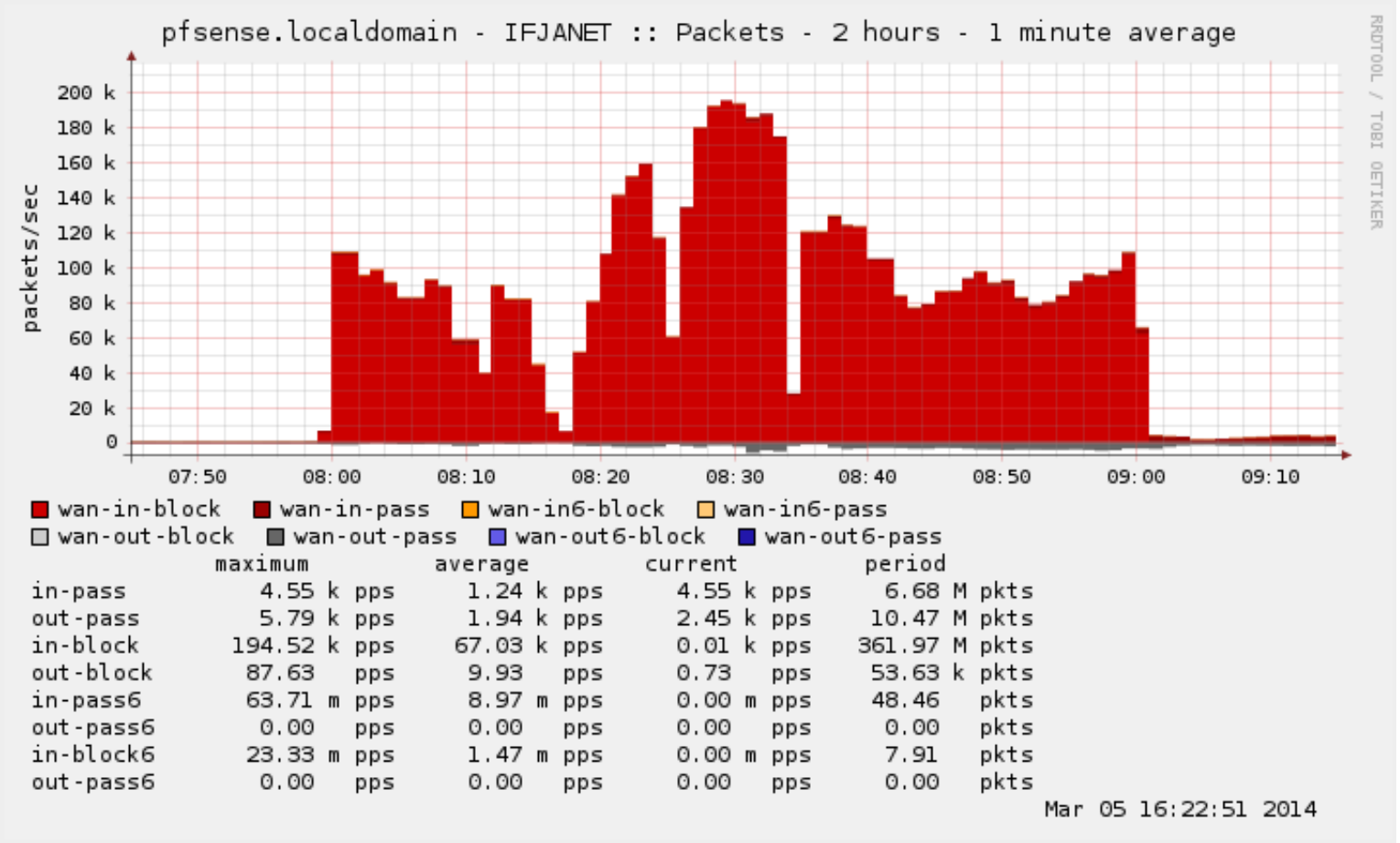


http://en.wikipedia.org/wiki/File:Stachledraht_DDos_Attack.svg

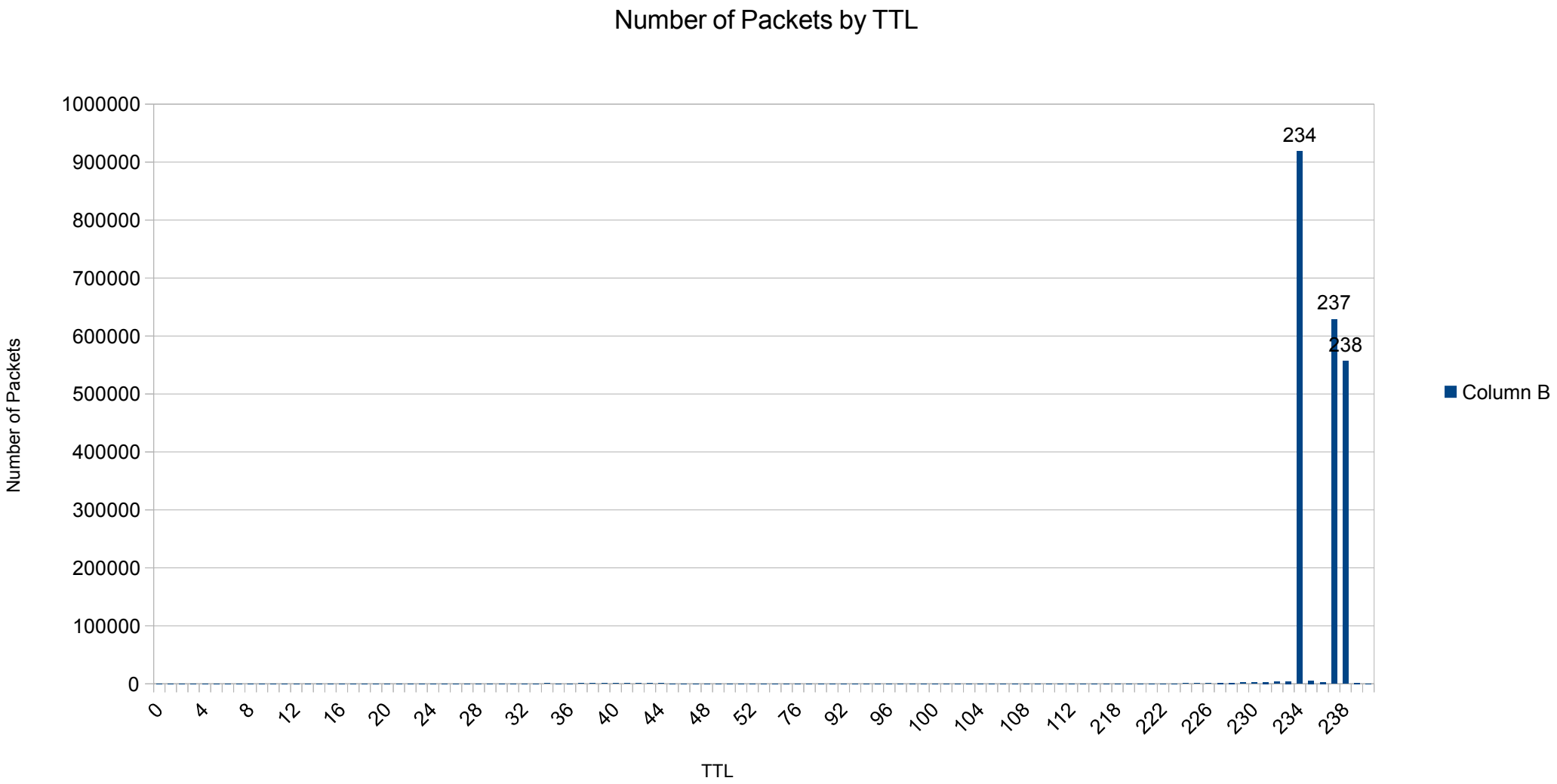
5 March 2014


pfsense.localdomain - IFJANET :: Packets - 2 days - 5 minutes average
packets/sec
200 k
150 k
100 k
50 k
0
Wed 00:00
Wed 12:00
Thu 00:00
Thu 12:00
RRDTOOL / TOBI OETIKER
wan-in-block
wan-in-pass
wan-in6-block
wan-in6-pass
wan-out-block
wan-out-pass
wan-out6-block
wan-out6-pass
maximum
average
current
period
in-pass 13.60 k pps 2.53 k pps 1.54 k pps 372.14 M pkts
out-pass 7.48 k pps 1.55 k pps 0.96 k pps 227.24 M pkts
in-block 152.39 k pps 2.76 k pps 0.01 k pps 405.04 M pkts
out-block 77.59 pps 1.31 pps 0.75 pps 192.00 k pkts
in-pass6 30.00 m pps 11.29 m pps 13.33 m pps 1.66 k pkts
out-pass6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
in-block6 10.00 m pps 0.09 m pps 0.00 m pps 12.99 pkts
out-pass6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
Mar 06 16:53:36 2014

5 March 2014

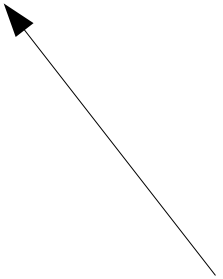

pfsense.localdomain - IFJANET :: Packets - 2 hours - 1 minute average
packets/sec
200 k
180 k
160 k
140 k
120 k
100 k
80 k
60 k
40 k
20 k
0
07:50
08:00
08:10
08:20
08:30
08:40
08:50
09:00
09:10
wan-in-block
wan-in-pass
wan-in6-block
wan-in6-pass
wan-out-block
wan-out-pass
wan-out6-block
wan-out6-pass
maximum
average
current
period
in-pass 4.55 k pps 1.24 k pps 4.55 k pps 6.68 M pkts
out-pass 5.79 k pps 1.94 k pps 2.45 k pps 10.47 M pkts
in-block 194.52 k pps 67.03 k pps 0.01 k pps 361.97 M pkts
out-block 87.63 pps 9.93 pps 0.73 pps 53.63 k pkts
in-pass6 63.71 m pps 8.97 m pps 0.00 m pps 48.46 pkts
out-pass6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
in-block6 23.33 m pps 1.47 m pps 0.00 m pps 7.91 pkts
out-pass6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
Mar 05 16:22:51 2014
RRDTOOL / TOBI OETIKER

5 March 2014
pfSense log (not complete)



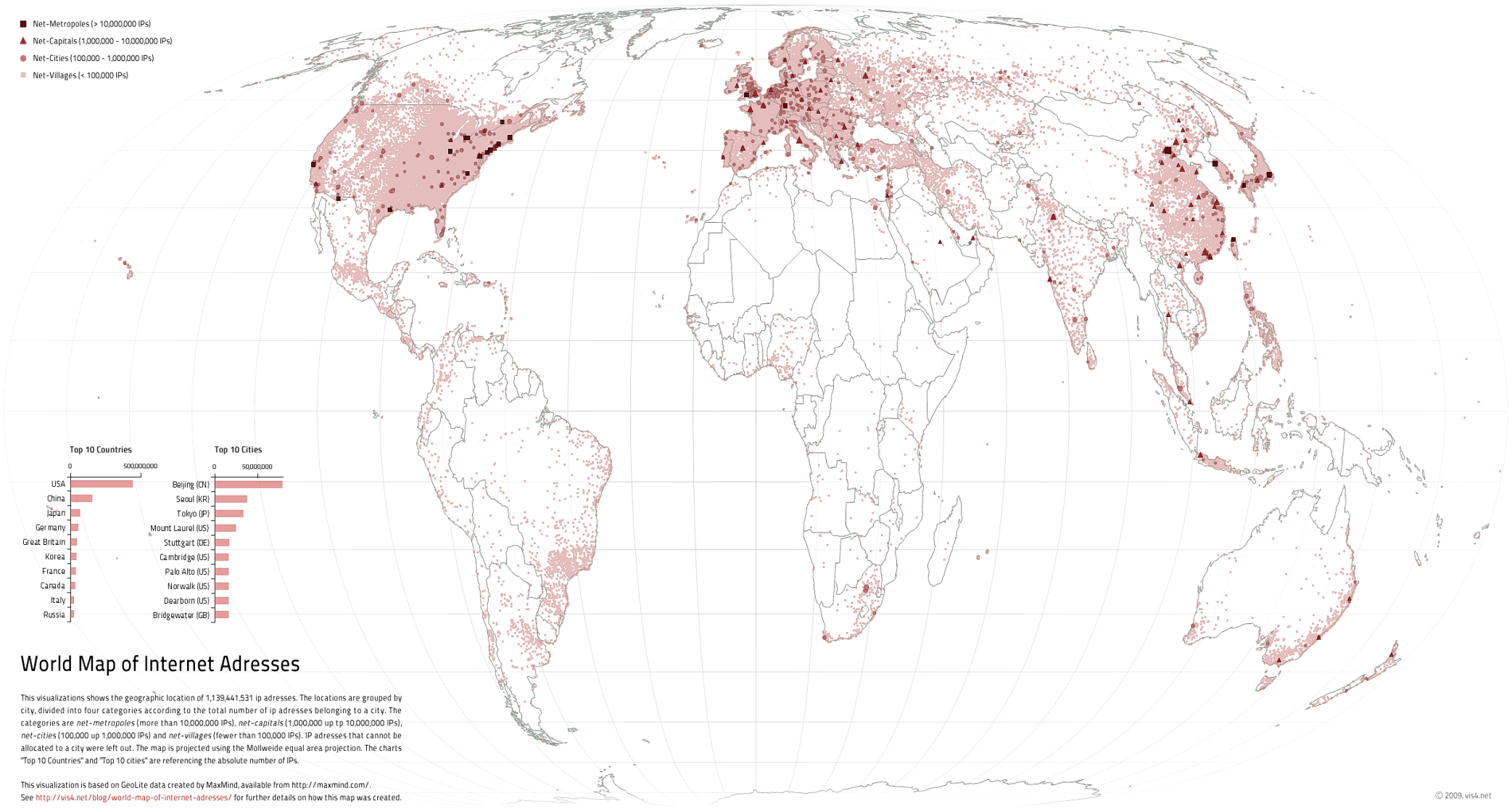
Possible source?

Mar 3, 2014 01:06:16.814944000	178.x.x.66	United Kingdom	5043	secure.colegsirgar.ac.uk0x0001
Mar 3, 2014 01:10:29.281929000	178.x.x.66	United Kingdom	59440	secure.colegsirgar.ac.uk0x001c
Mar 3, 2014 01:10:29.281933000	178.x.x.66	United Kingdom	59440	secure.colegsirgar.ac.uk0x001c
Mar 3, 2014 08:00:17.999137000	178.x.x.66	United Kingdom	57217	secure.colegsirgar.ac.uk0x0001
Mar 3, 2014 08:00:17.999145000	178.x.x.66	United Kingdom	57217	secure.colegsirgar.ac.uk0x0001
Mar 3, 2014 08:04:19.773735000	178.x.x.66	United Kingdom	29299	secure.colegsirgar.ac.uk0x0001
Mar 3, 2014 08:04:19.773737000	178.x.x.66	United Kingdom	29299	secure.colegsirgar.ac.uk0x0001



Dedicated Server...

GeoIP is biased

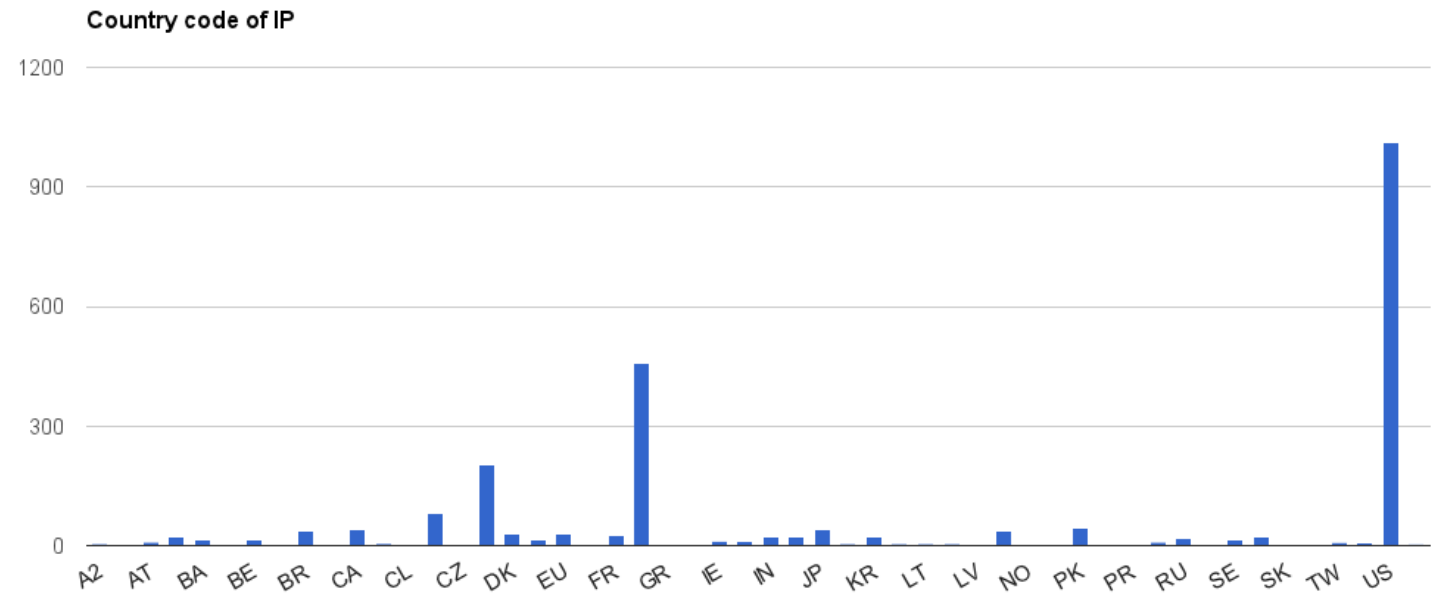


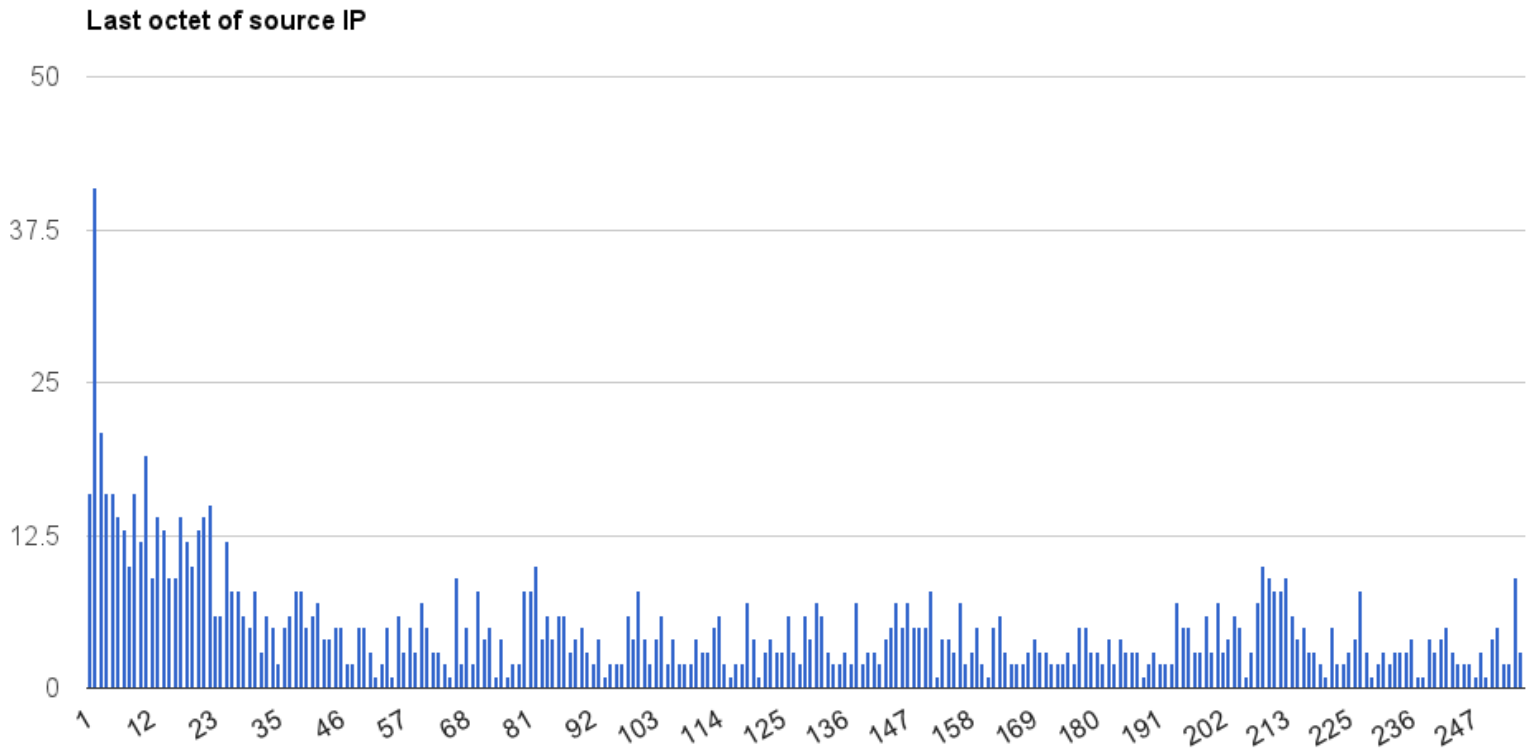
https://www.flickr.com/photos/53260176@N06/4917017613/

Most Attacks from DE and US

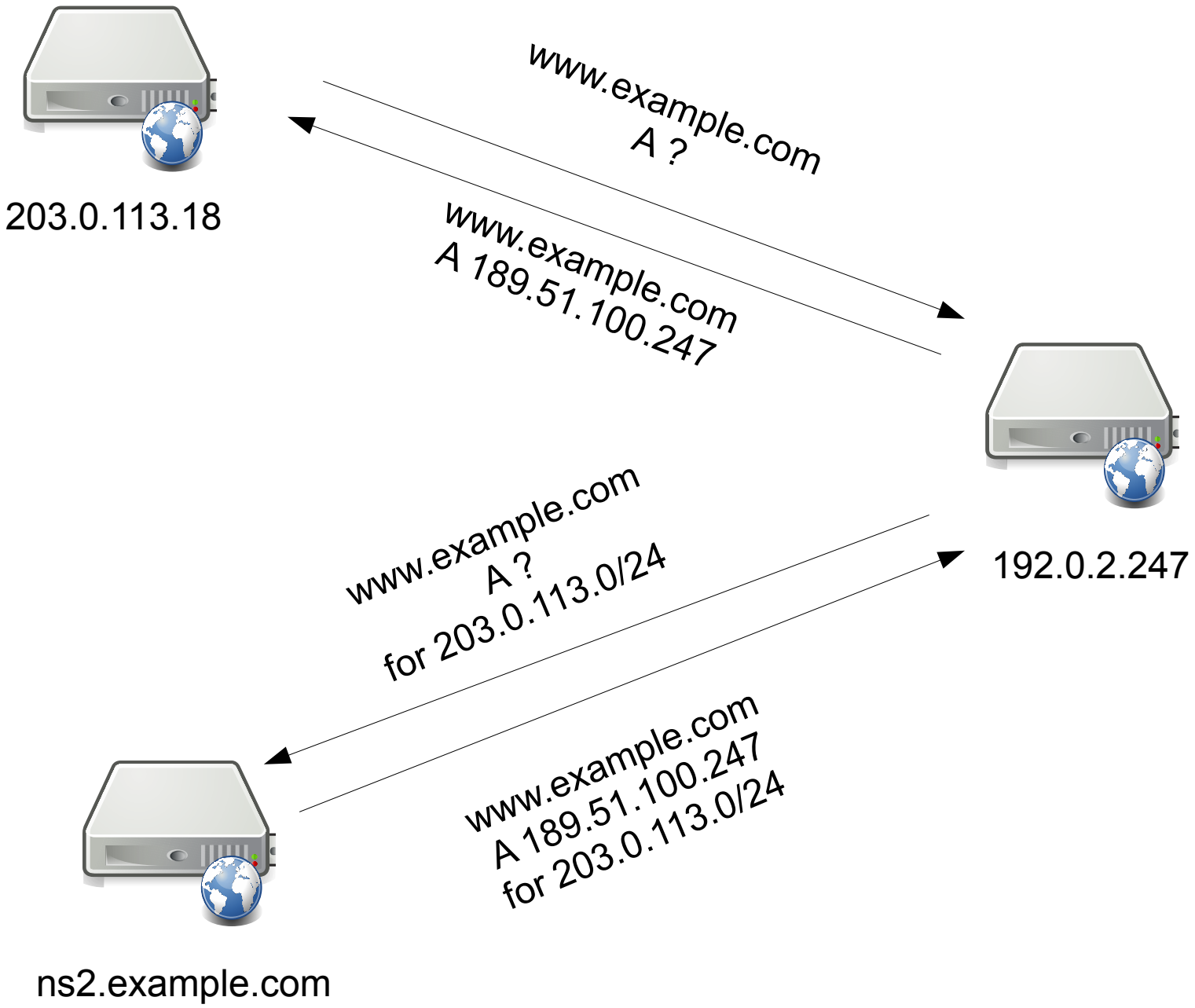
Or should that be Brussles?

- DE – 74.125.17.0/24
- US – 74.125.181.0/24


Country code of IP
1200
900
600
300
0
A2
AT
BA
BE
BR
CA
CL
CZ
DK
EU
FR
GR
IE
IN
JP
KR
LT
LV
NO
PK
PR
RU
SE
SK
TW
US

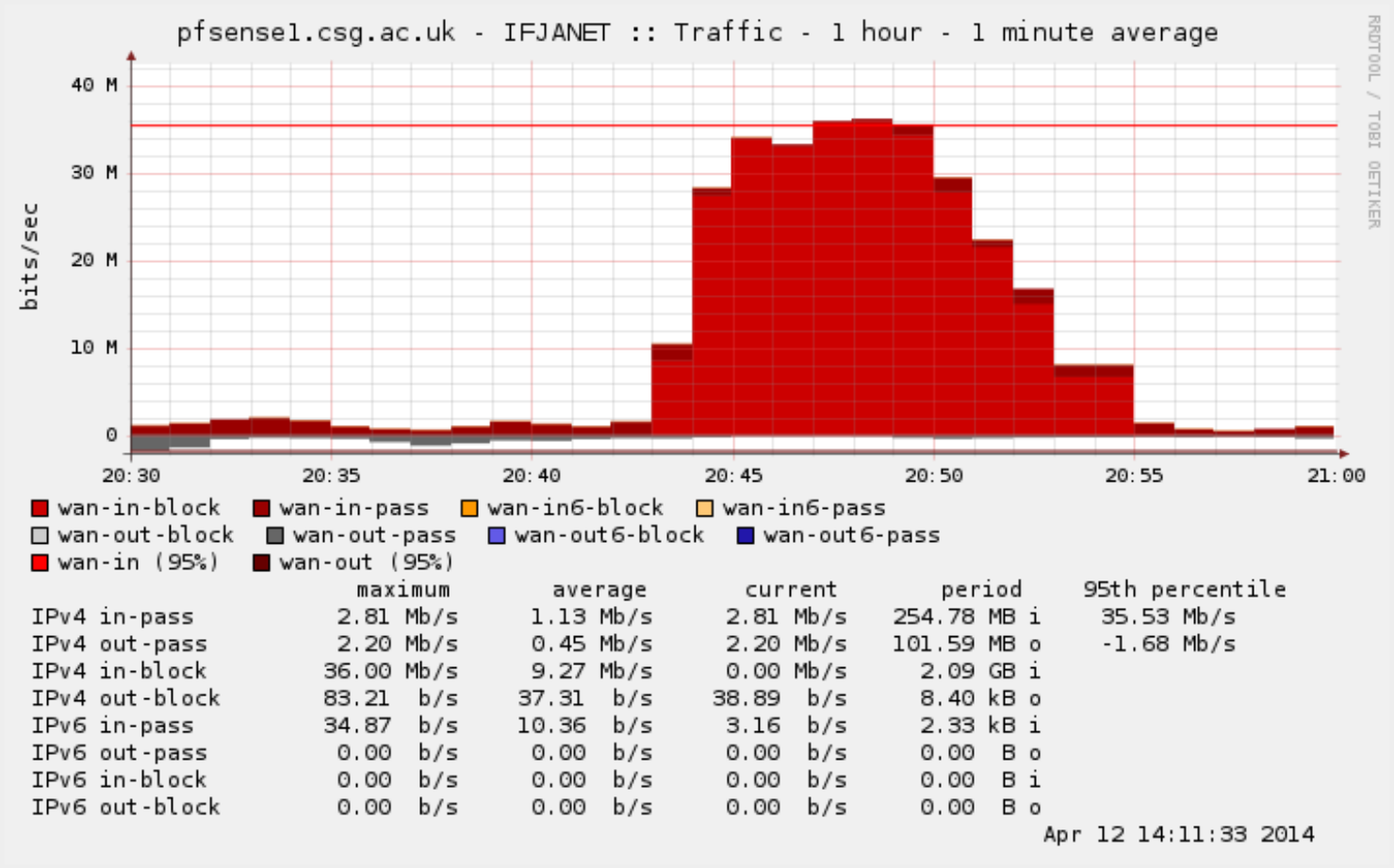

Last octet of source IP
50
37.5
25
12.5
0
1
12
23
35
46
57
68
81
92
103
114
125
136
147
158
169
180
191
202
213
225
236
247

EDNS client subnet



http://commons.wikimedia.org/wiki/File:Server-web.svg

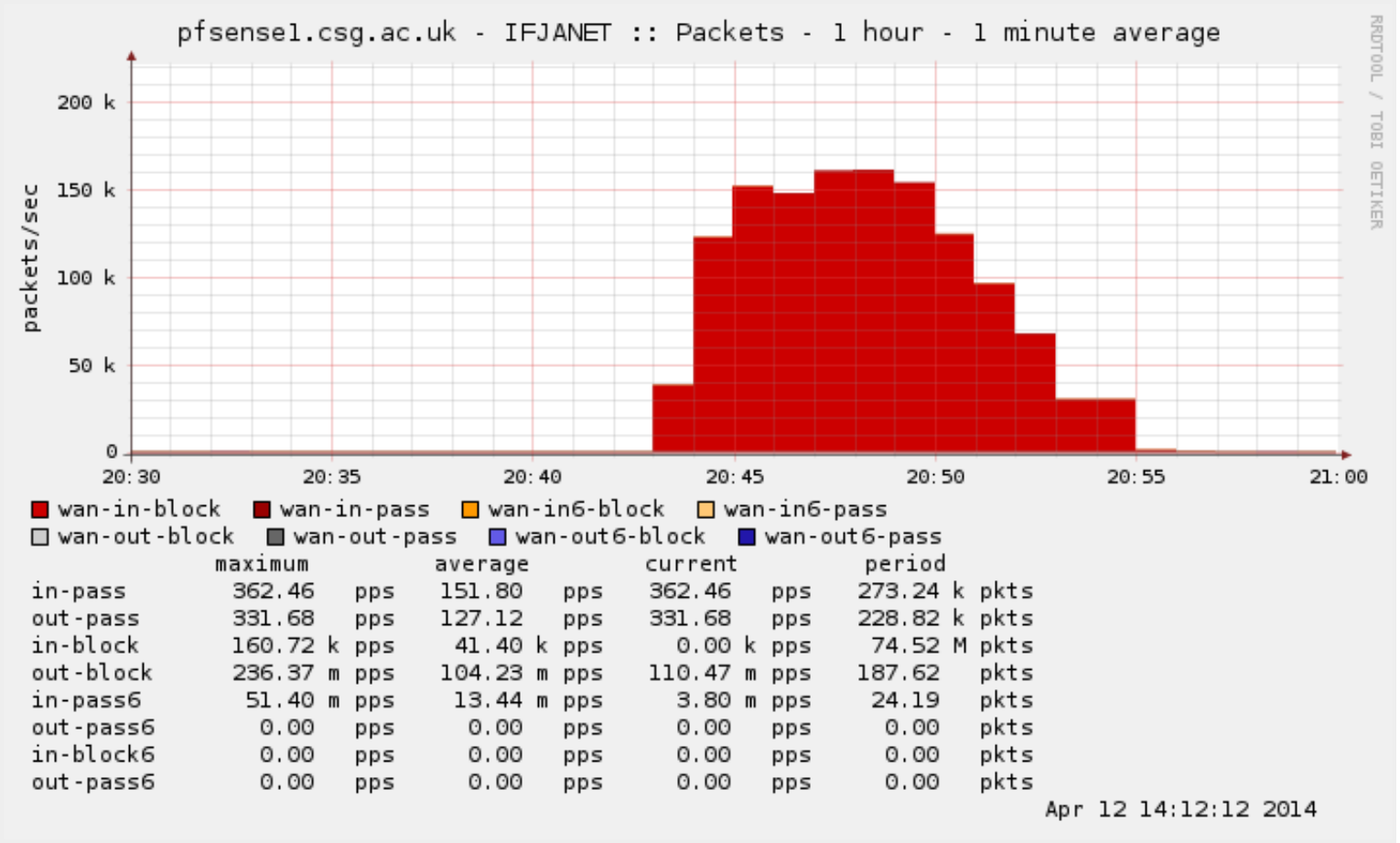
11 April 2014



	maximum	average	current	period	95th percentile
IPv4 in-pass	2.81 Mb/s	1.13 Mb/s	2.81 Mb/s	254.78 MB i	35.53 Mb/s
IPv4 out-pass	2.20 Mb/s	0.45 Mb/s	2.20 Mb/s	101.59 MB o	-1.68 Mb/s
IPv4 in-block	36.00 Mb/s	9.27 Mb/s	0.00 Mb/s	2.09 GB i	
IPv4 out-block	83.21 b/s	37.31 b/s	38.89 b/s	8.40 kB o	
IPv6 in-pass	34.87 b/s	10.36 b/s	3.16 b/s	2.33 kB i	
IPv6 out-pass	0.00 b/s	0.00 b/s	0.00 b/s	0.00 B o	
IPv6 in-block	0.00 b/s	0.00 b/s	0.00 b/s	0.00 B i	
IPv6 out-block	0.00 b/s	0.00 b/s	0.00 b/s	0.00 B o	

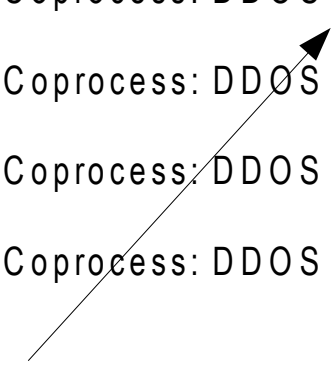
Apr 12 14:11:33 2014

11 April 2014



Attack against 212.219.193.147

```
Apr 11 12:57:45 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147
Apr 11 20:20:12 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147
Apr 11 20:43:51 dns1 pdns[14695]: Coprocess: DDOS Query from 198.51.100.0/24 via 74.125.17.147; returned 212
Apr 11 22:02:20 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.x.147; returned 212.219.193.147
Apr 12 05:00:22 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147
Apr 12 05:44:06 dns1 pdns[14695]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147
```



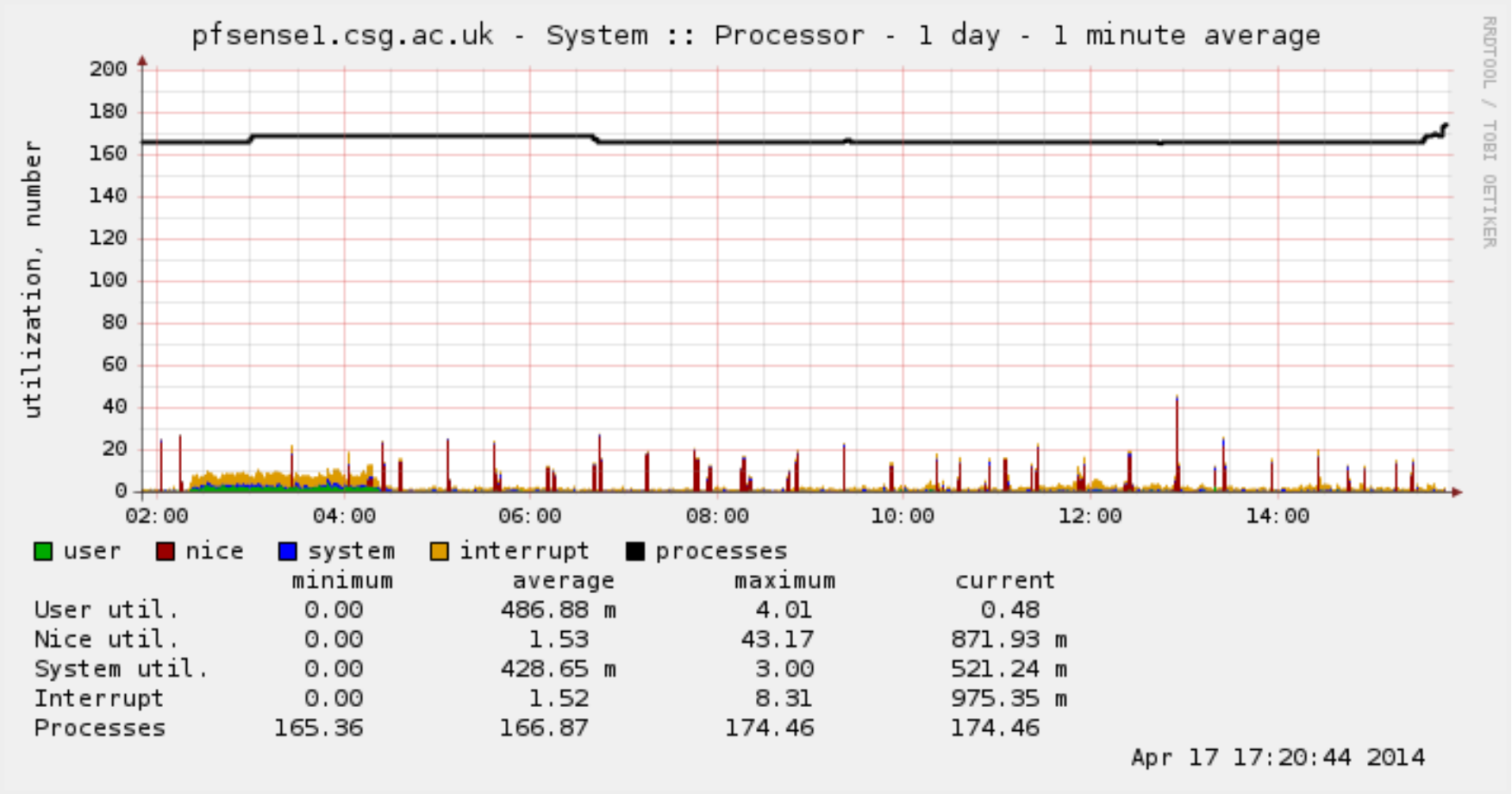
UK VPS provider

2014-04-11 20:43:51.651423000 - DNS request made from Google to dns1

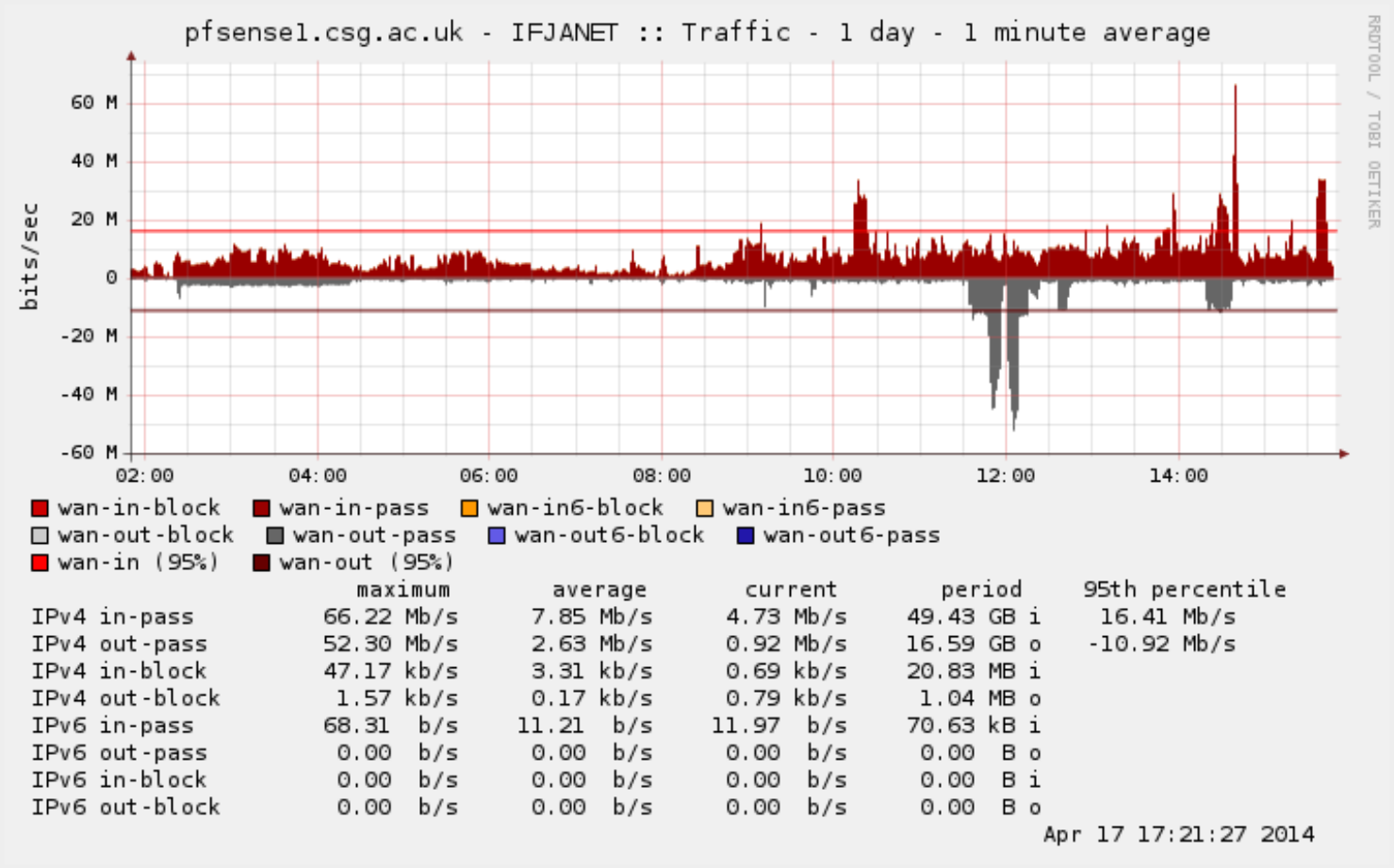
2014-04-11 20:43:51 - response sent to Google DNS

2014-04-11 20:43:58.996 - UDP dst port 80, random src port attack started

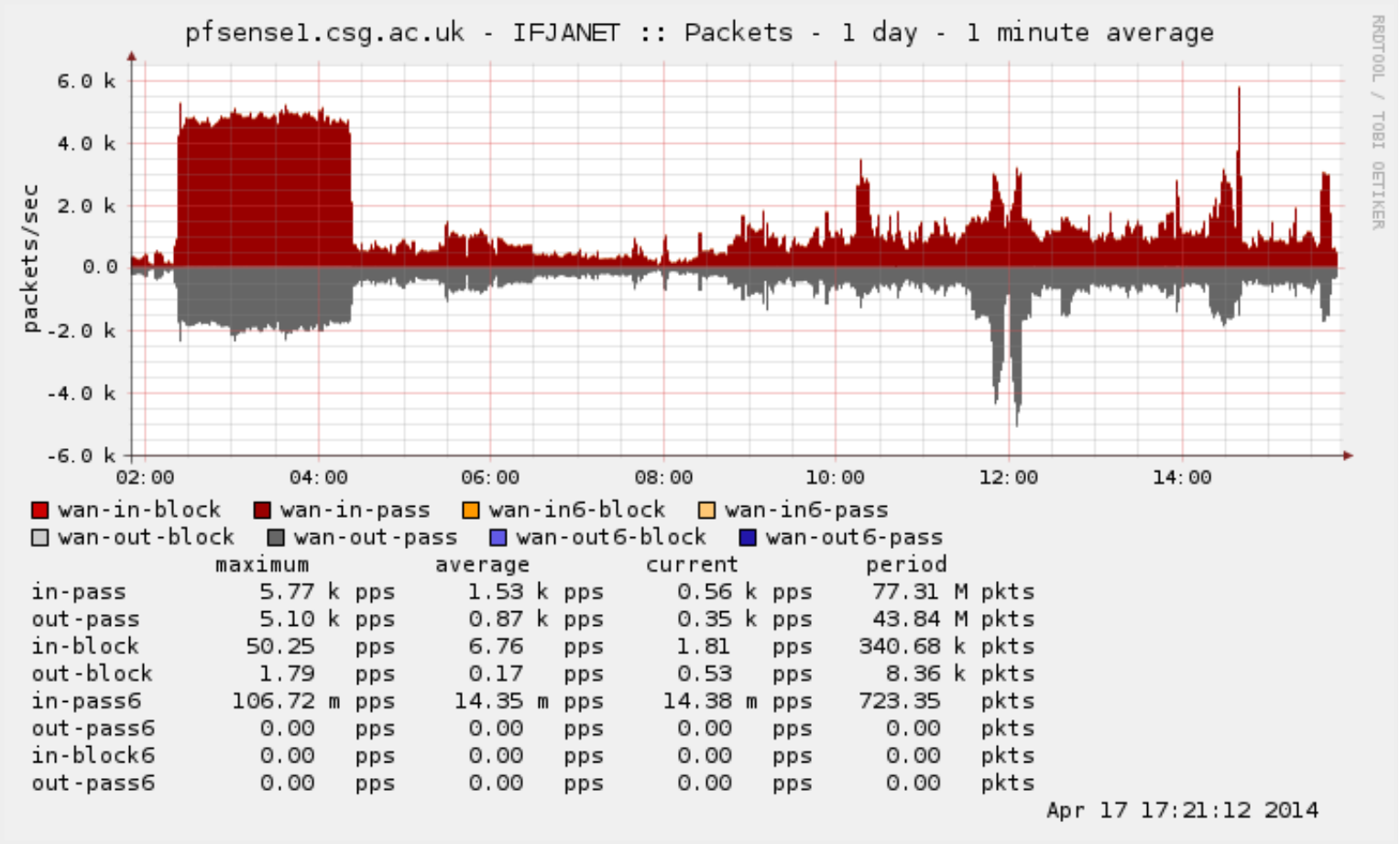
17 April 2014
Distributed HTTPS Flood Attack



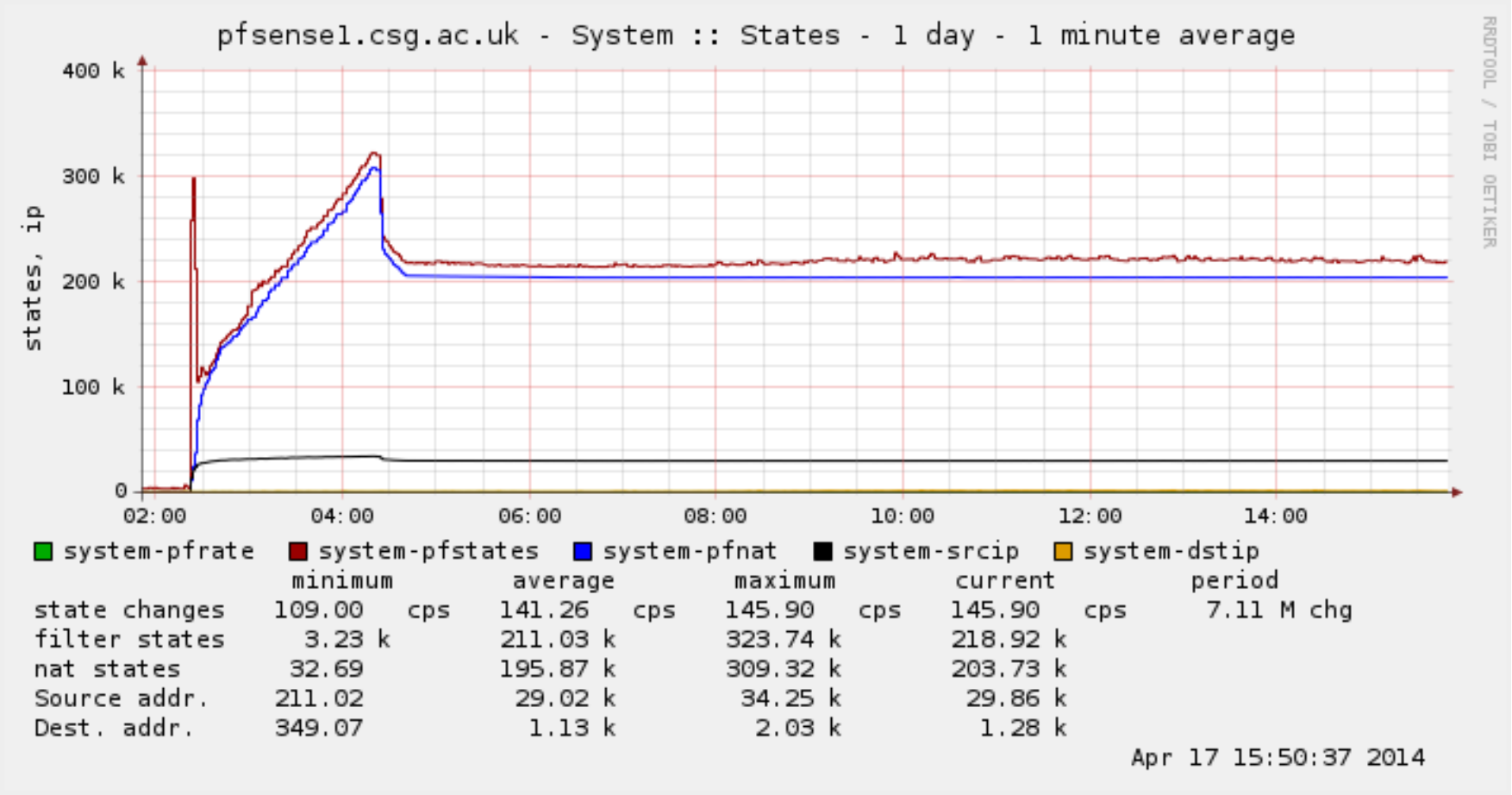
17 April 2014
Minimal Bandwidth



17 April 2014
Small Packets



17 April 2014
Lots of states



Compromised Hosts

- Stateful attack
- ~100,000/hr queries for secure.colegsirgar.ac.uk
- Some 36,000 comprimised/infected hosts
- Mostly hosting providers