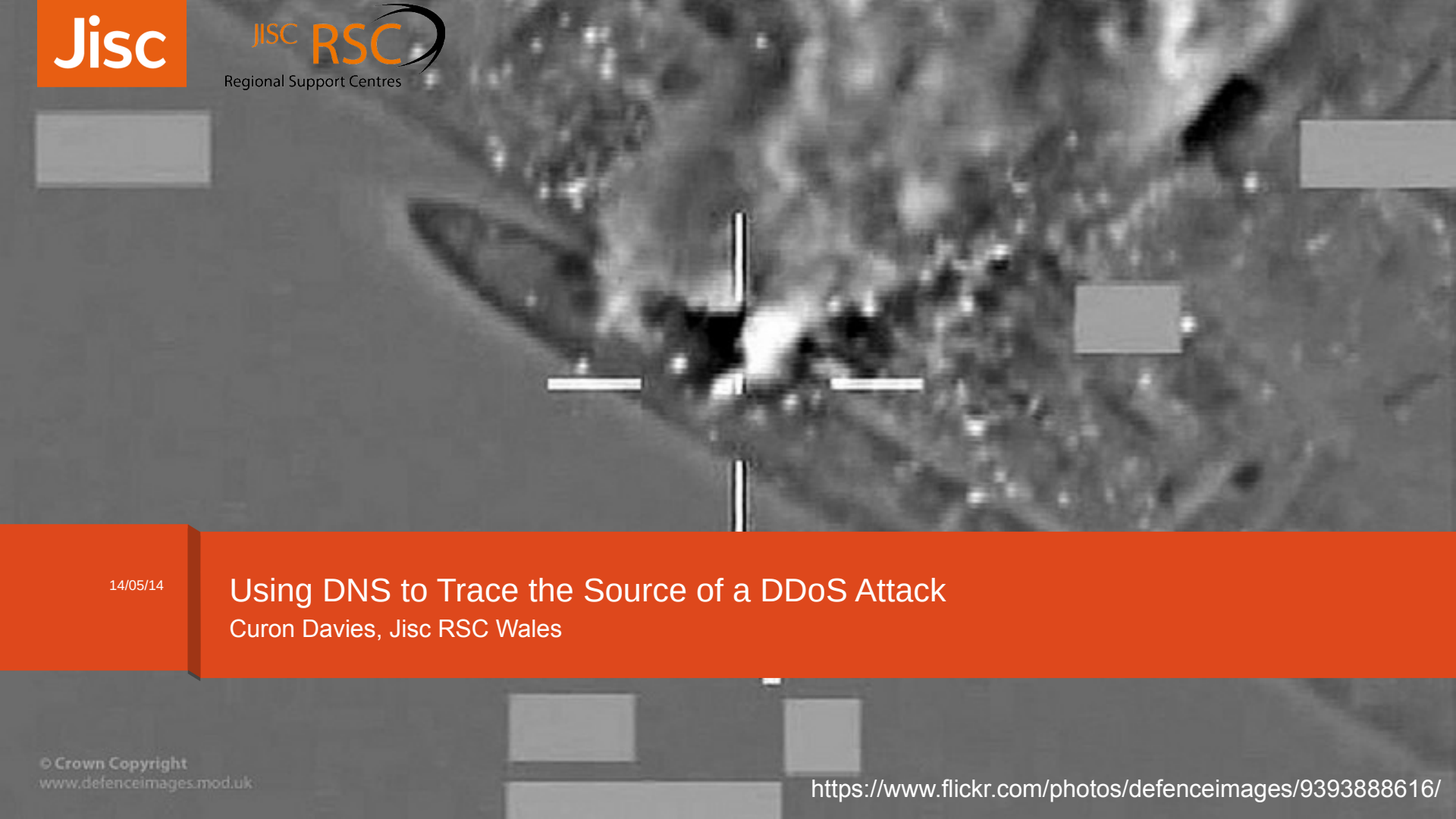


14/05/14

Using DNS to Trace the Source of a DDoS Attack

Curon Davies, Jisc RSC Wales

https://www.flickr.com/photos/defenceimages/9393888616/

Jisc Regional Support Centres

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

The Idea

IPv4

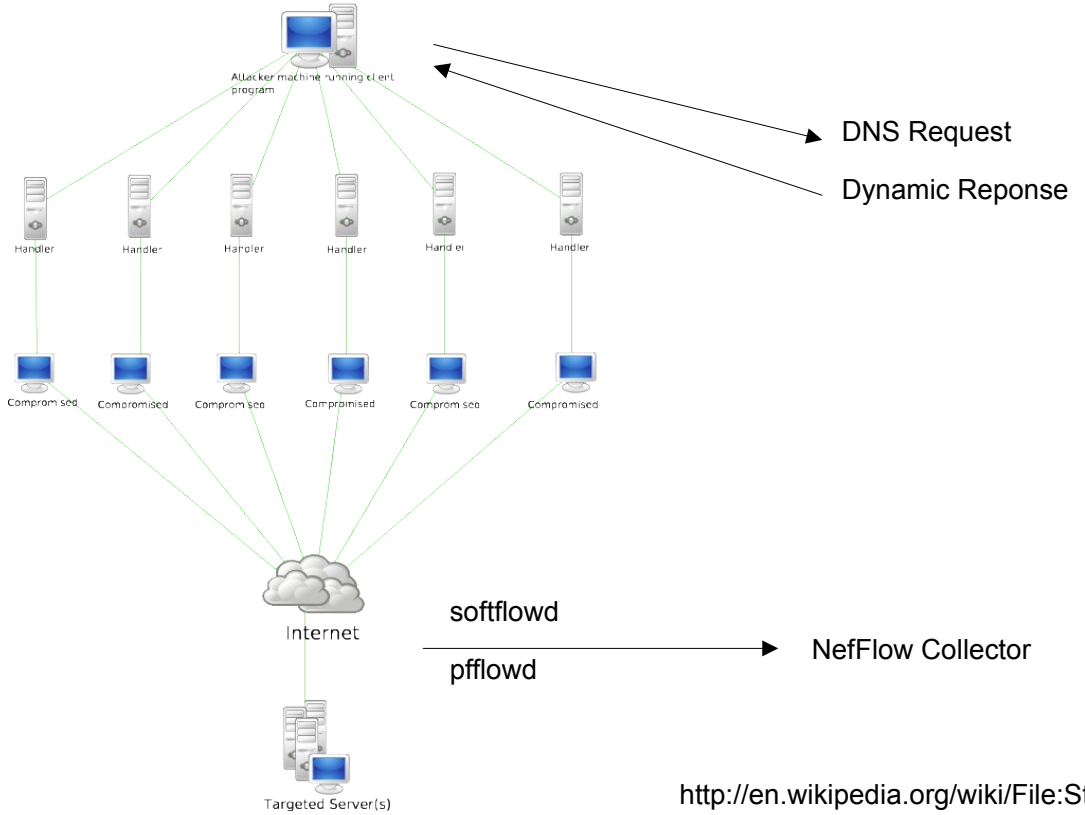
https://www.flickr.com/photos/n3pb/8765646099/in/set-72157634324914351/

Low Orbit Ion Cannon

```
================================
|| 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.
```

DNS RR TTL

DNS Lookup for an Attack

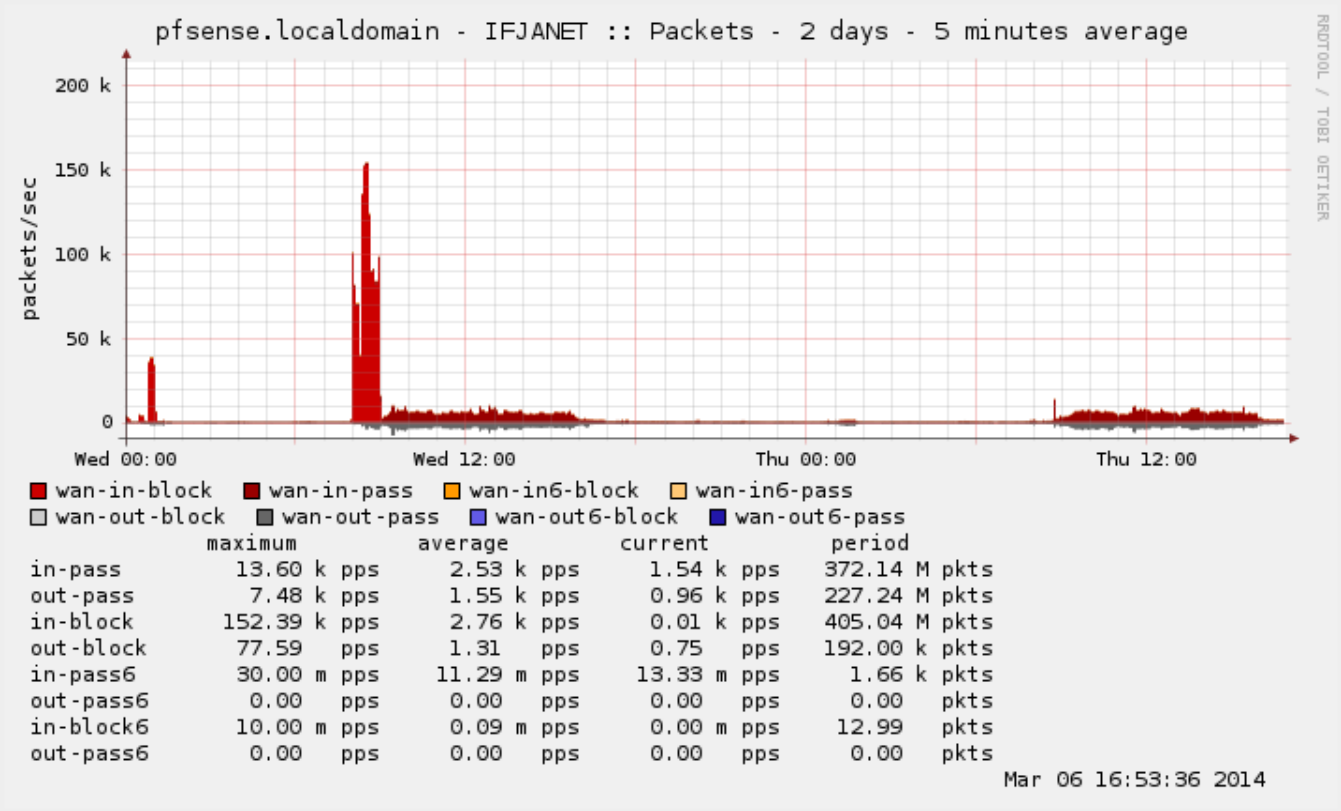


http://en.wikipedia.org/wiki/File:Stachledraht_DDos_Attack.svg

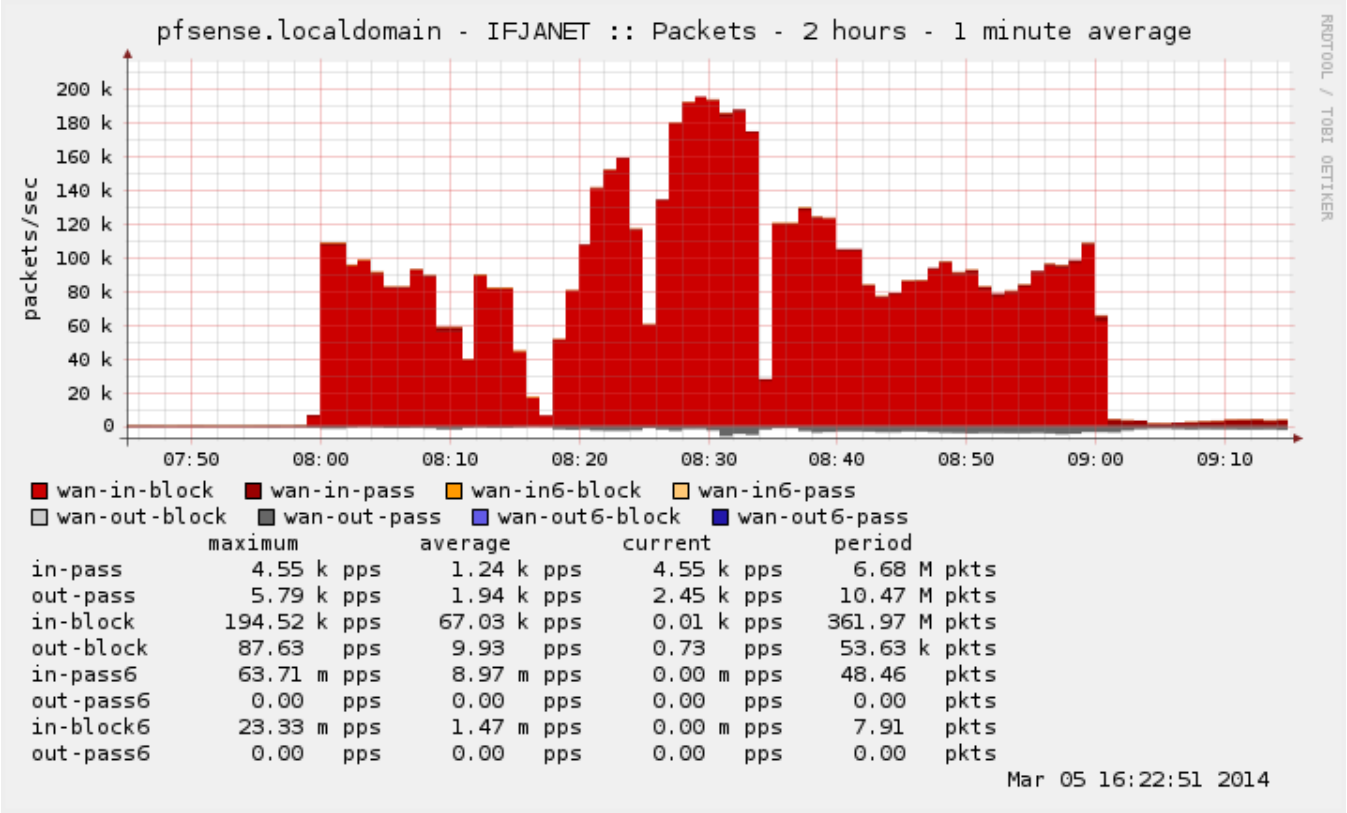
SYN Flood Attacks

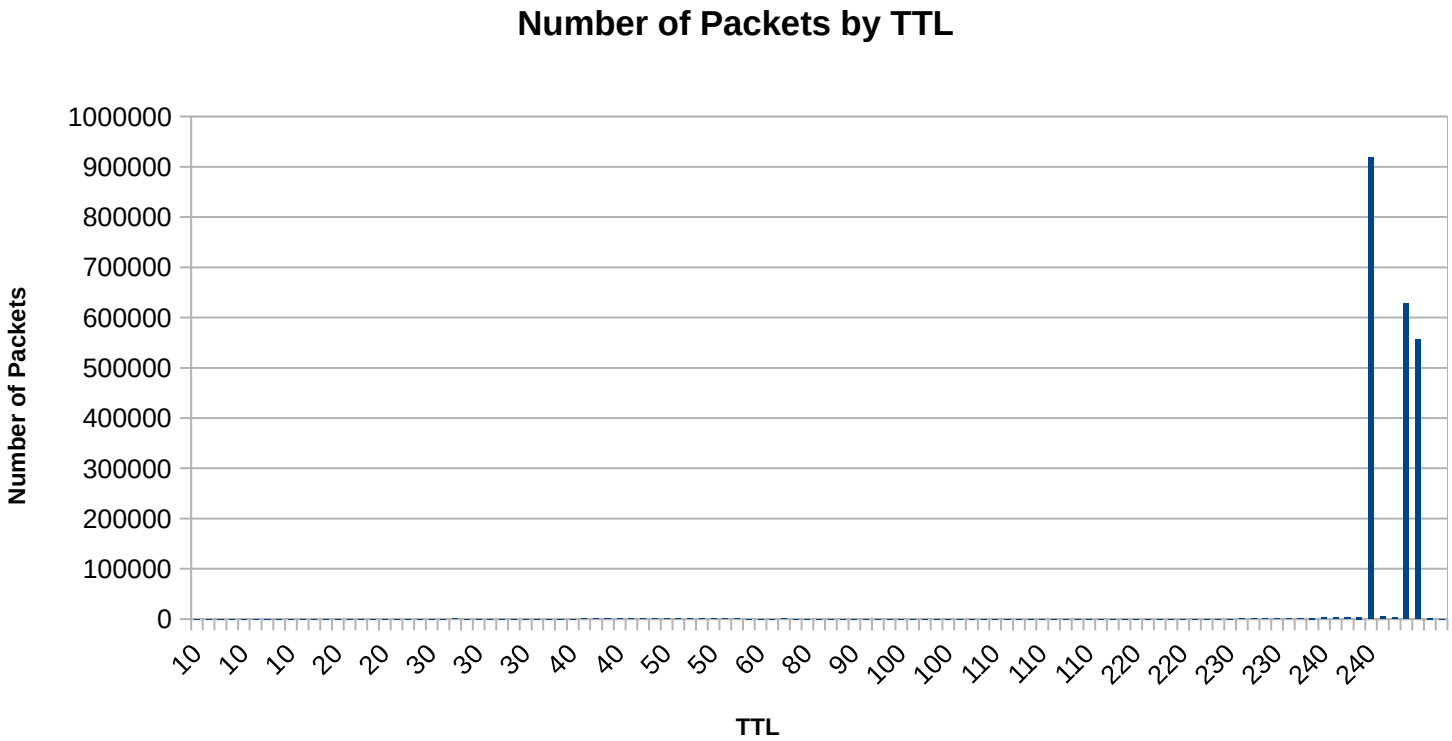
http://commons.wikimedia.org/wiki/File:B1-B_Lancer_and_cluster_bombs.jpg

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

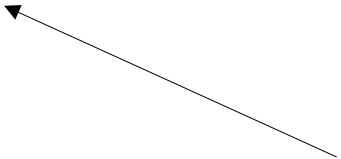
5 March 2014


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
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 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


Number of Packets by TTL
Number of Packets
1000000
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
10
10
10
20
20
30
30
30
40
40
50
50
60
80
90
100
100
110
110
110
220
220
230
230
240
240
TTL

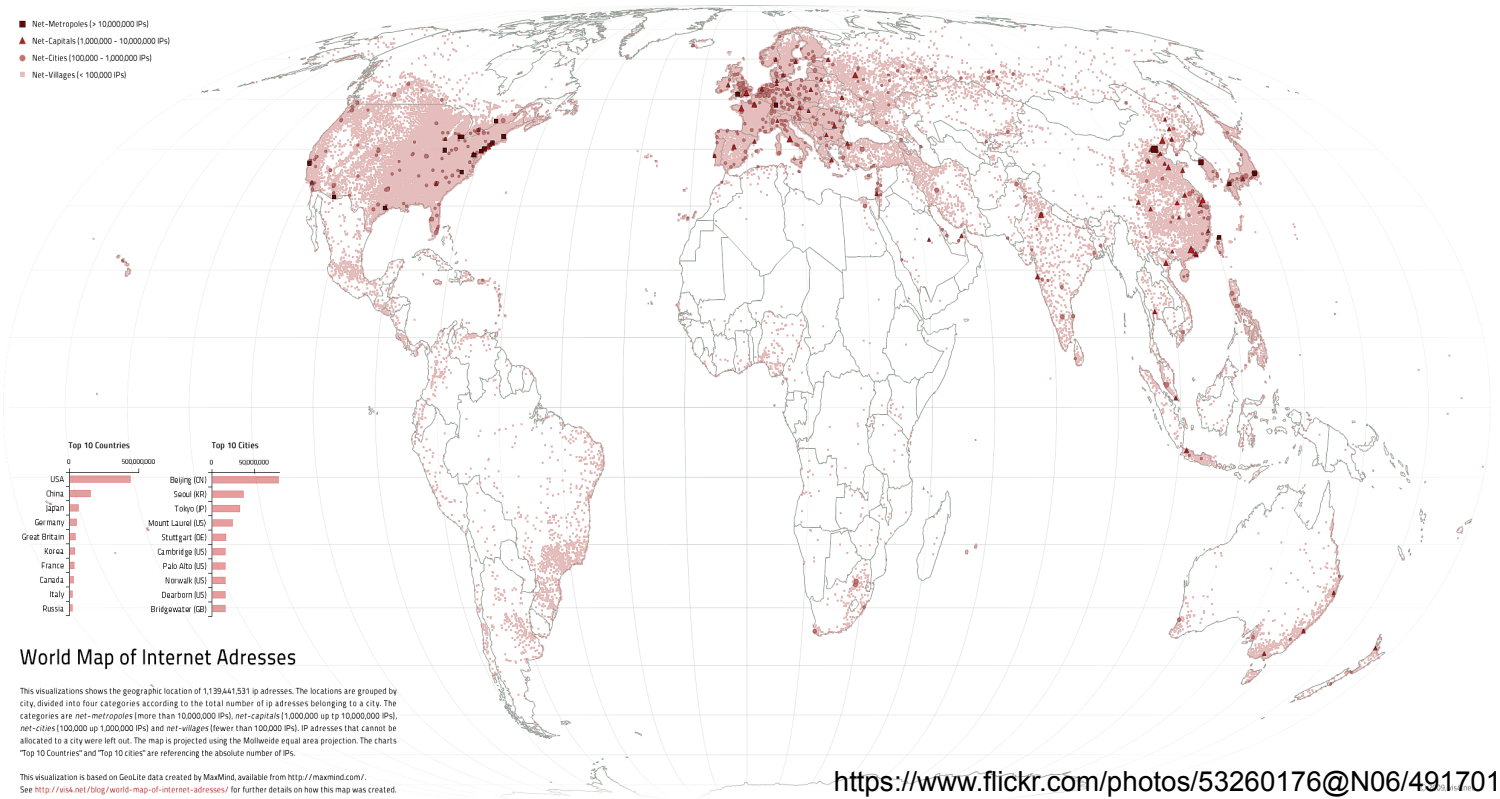
Similar attack 3 March 2014

Mar 3, 2014 01:06:16.814944000	178.x.x.66	United Kingdom	5643	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 01:10:29.281929000	178.x.x.66	United Kingdom	59440	secure.colegsirgar.ac.uk	0x001c
Mar 3, 2014 01:10:29.281933000	178.x.x.66	United Kingdom	59440	secure.colegsirgar.ac.uk	0x001c
Mar 3, 2014 08:00:17.999137000	178.x.x.66	United Kingdom	57217	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 08:00:17.999145000	178.x.x.66	United Kingdom	57217	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 08:04:19.773735000	178.x.x.66	United Kingdom	29399	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 08:04:19.773737000	178.x.x.66	United Kingdom	29399	secure.colegsirgar.ac.uk	0x0001



Dedicated Server...

GeoIP is biased

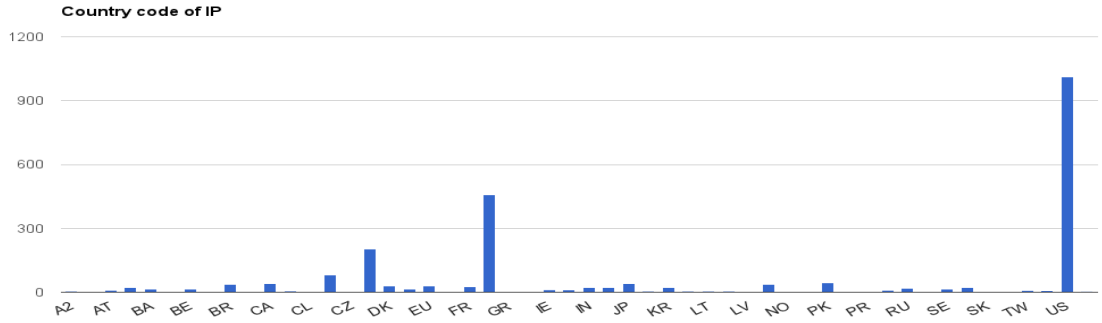


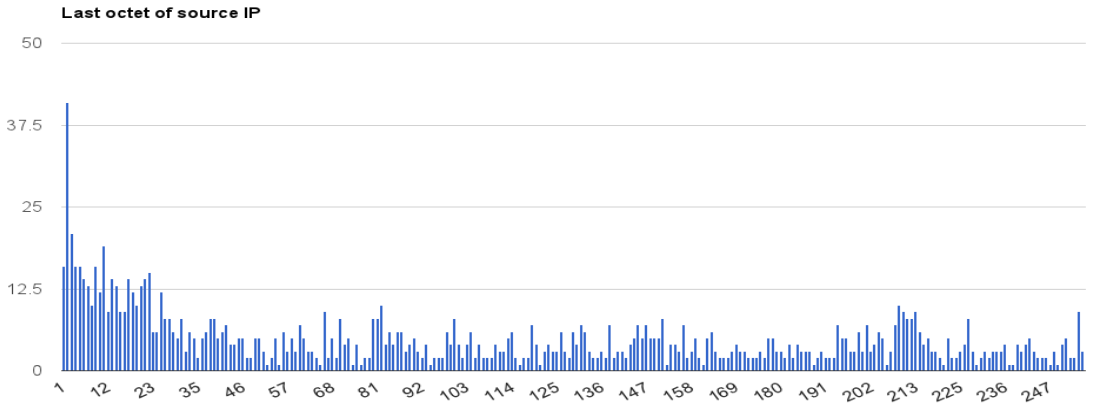
https://www.flickr.com/photos/53260176@N06/4917017613/

Most attacks from US and DE

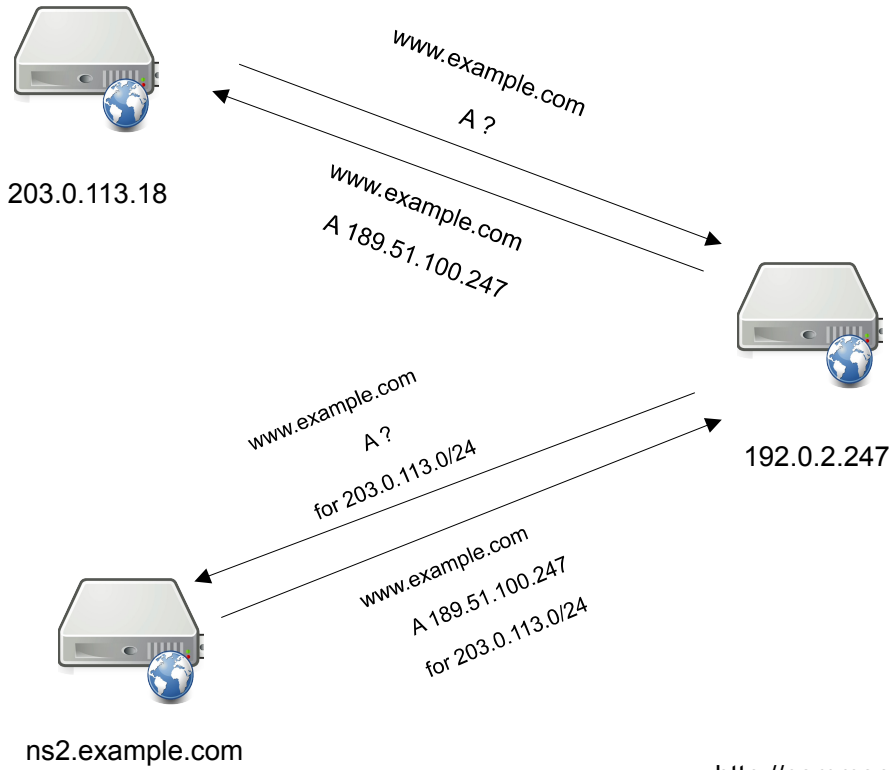
- Or should that be Brussels
  - DE – 74.125.17.0/24
  - US – 74.125.181.0/24

GeoIP is biased – use last Octet instead





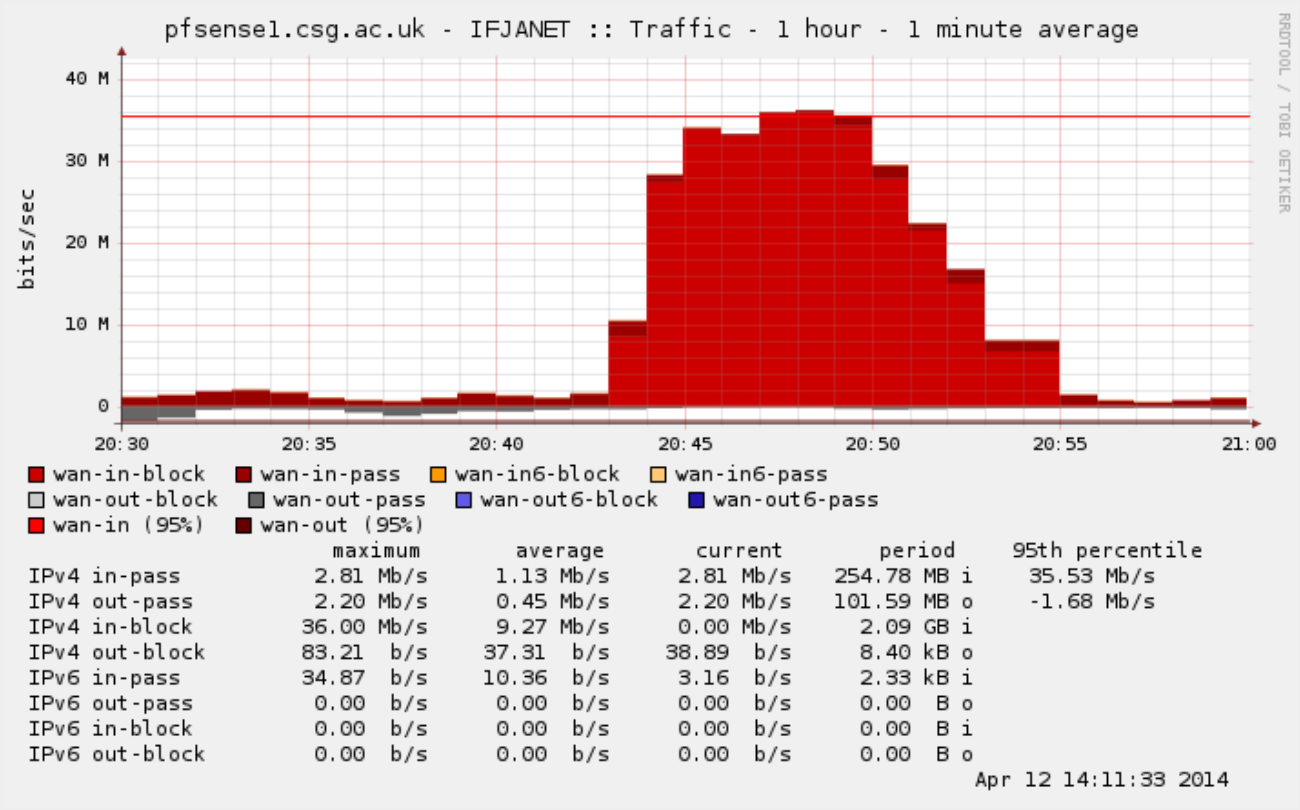
EDNS Client Subnet

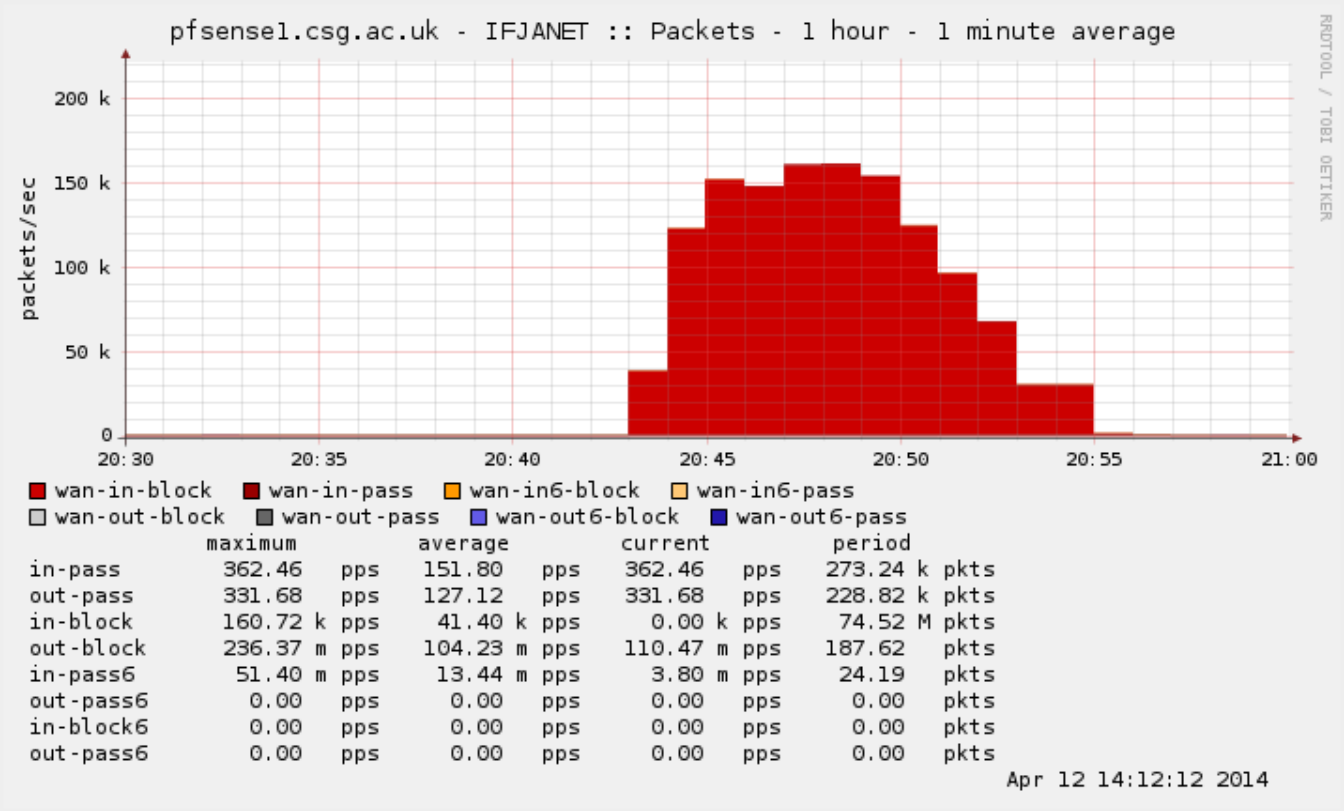


http://commons.wikimedia.org/wiki/File:Server-web.svg

Amplification Attacks

11 April 2014




pfsense1.csg.ac.uk - IFJANET :: Packets - 1 hour - 1 minute average
RRDTOOL / TOBI OETIKER
packets/sec
200 k
150 k
100 k
50 k
0
20:30
20:35
20:40
20:45
20:50
20:55
21:00
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 362.46 pps 151.80 pps 362.46 pps 273.24 k pkts
out-pass 331.68 pps 127.12 pps 331.68 pps 228.82 k pkts
in-block 160.72 k pps 41.40 k pps 0.00 k pps 74.52 M pkts
out-block 236.37 m pps 104.23 m pps 110.47 m pps 187.62 pkts
in-pass6 51.40 m pps 13.44 m pps 3.80 m pps 24.19 pkts
out-pass6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
in-block6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
out-pass6 0.00 pps 0.00 pps 0.00 pps 0.00 pkts
Apr 12 14:12:12 2014

Apr 11 12:57:45 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147

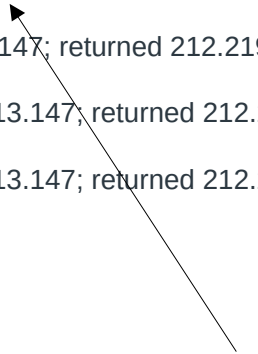
Apr 11 20:20:12 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147

Apr 11 20:43:51 dns1 pdns[14695]: Coprocess: DDOS Query from 198.51.100.0/24 via 74.125.17.147; returned 212.219.193.147

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



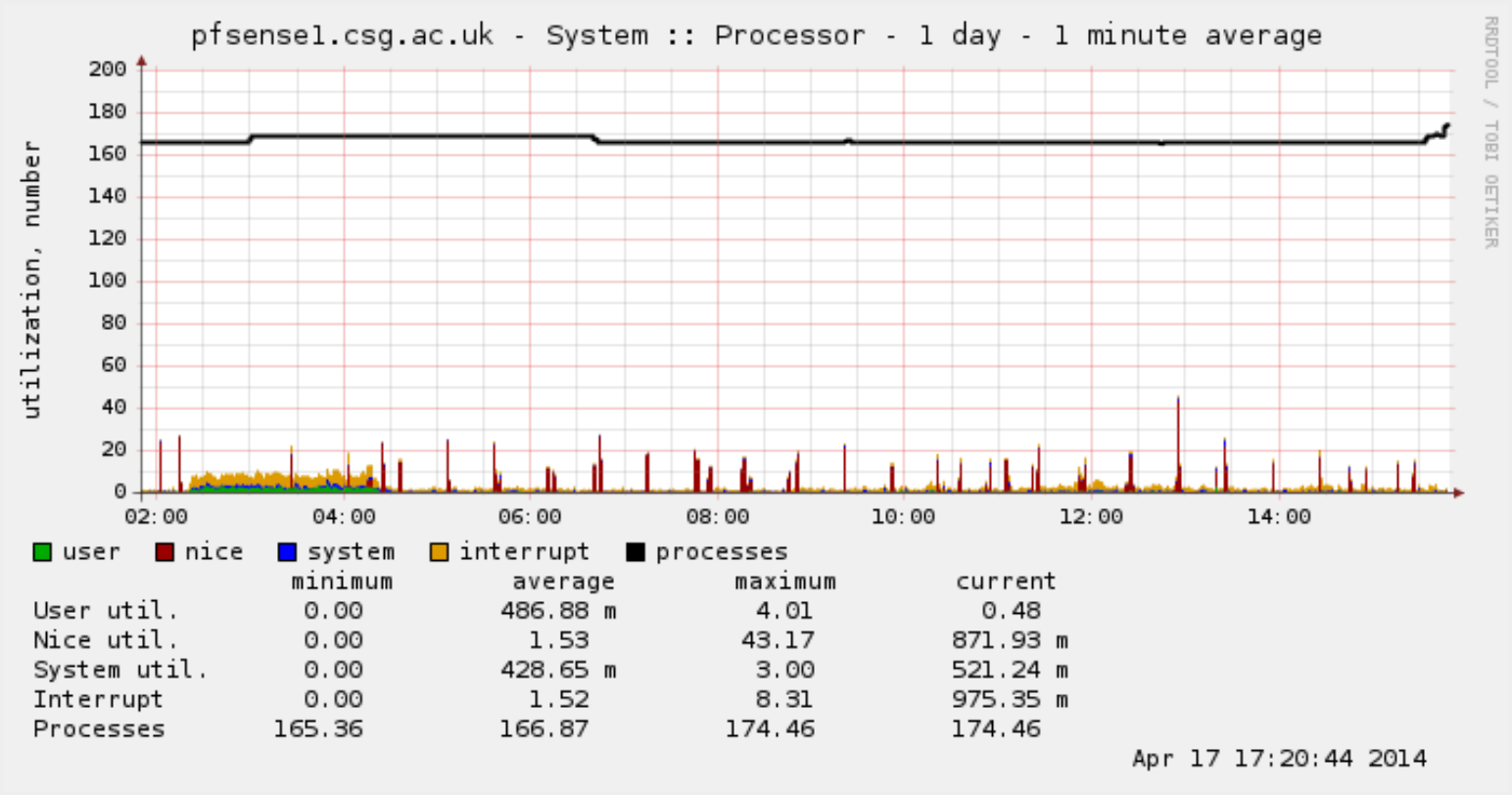
UK VPS provider

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

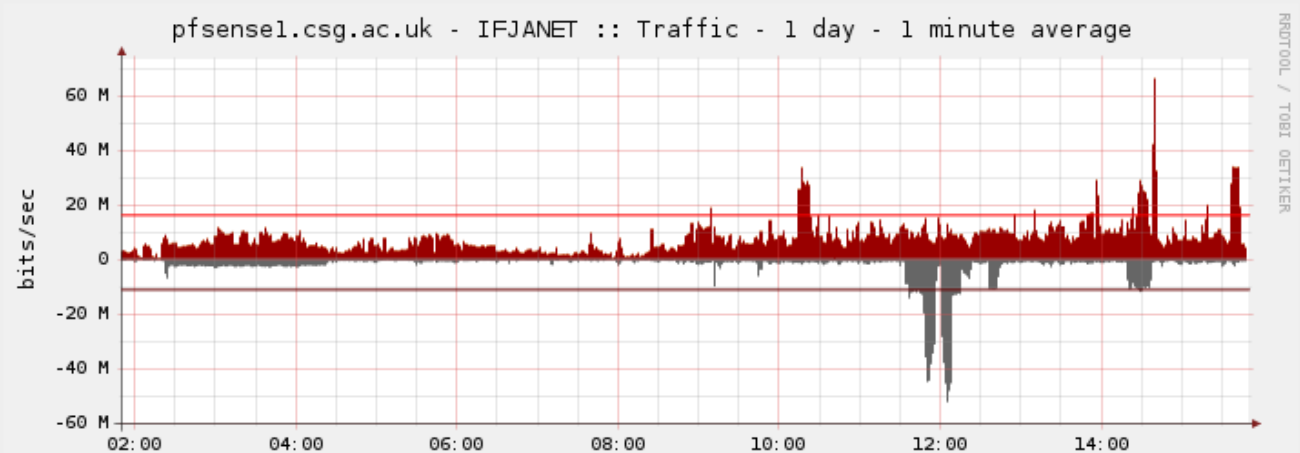
2014-04-11 20:43:51 - response sent to Google DNS

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

Distributed HTTPS Flood Attack



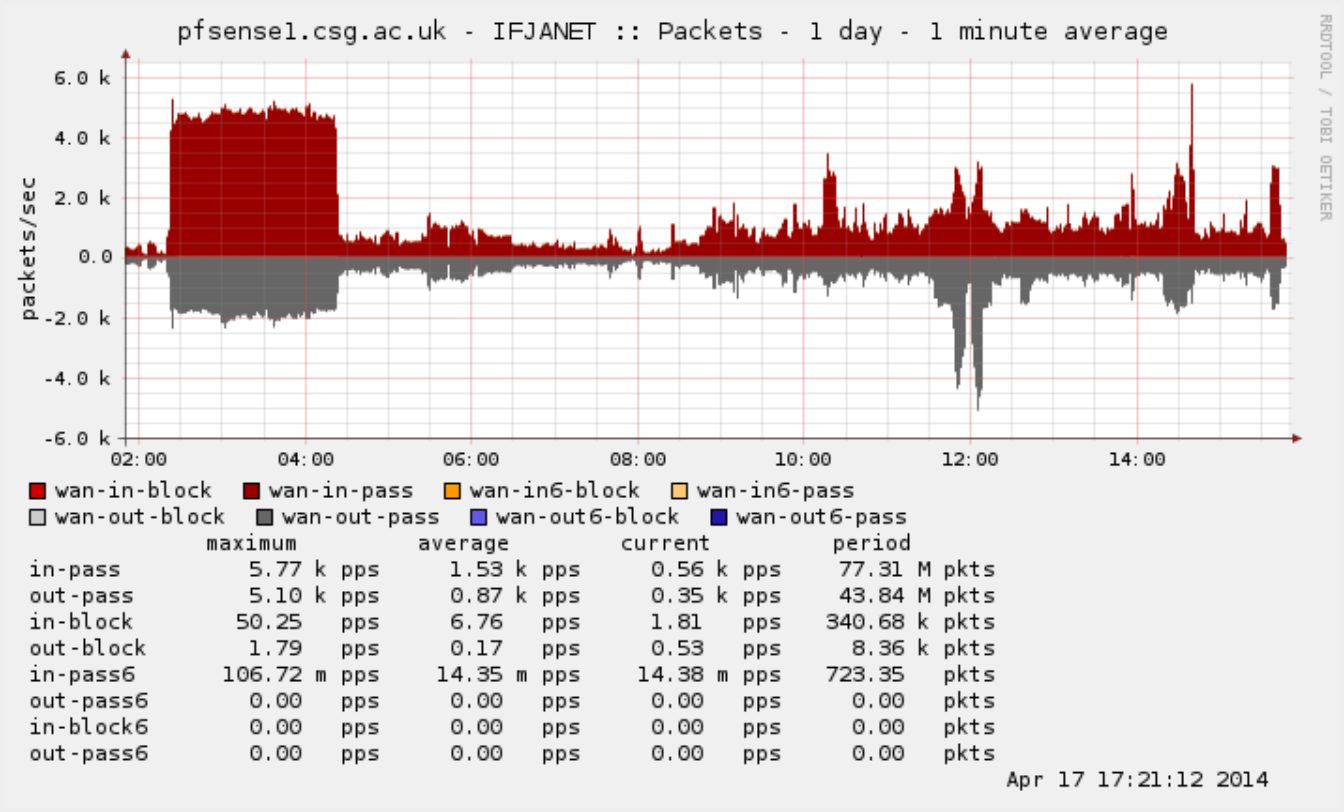
Minimal Bandwidth



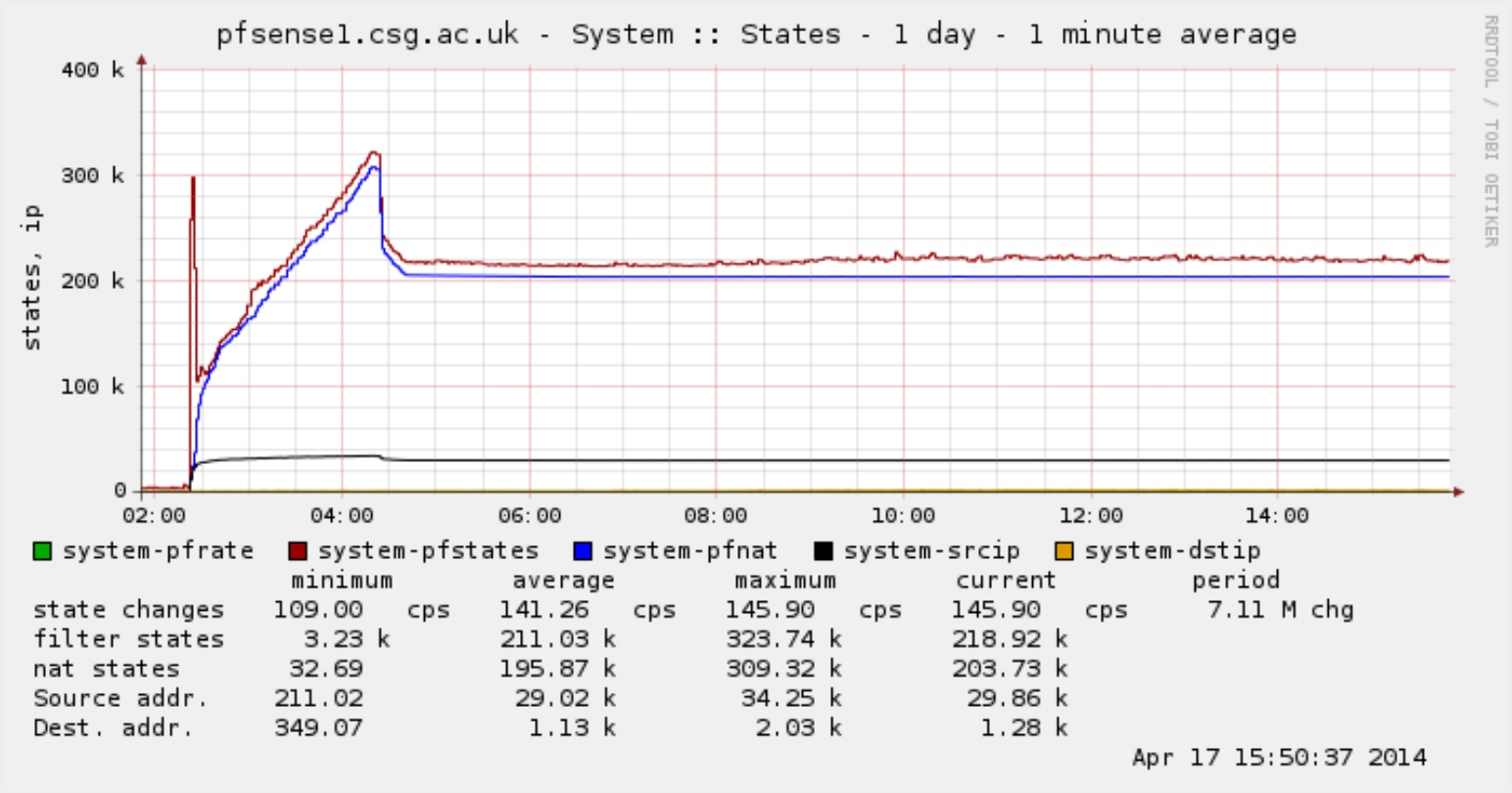
	maximum	average	current	period	95th percentile
IPv4 in-pass	66.22 Mb/s	7.85 Mb/s	4.73 Mb/s	49.43 GB i	16.41 Mb/s
IPv4 out-pass	52.30 Mb/s	2.63 Mb/s	0.92 Mb/s	16.59 GB o	-10.92 Mb/s
IPv4 in-block	47.17 kb/s	3.31 kb/s	0.69 kb/s	20.83 MB i	
IPv4 out-block	1.57 kb/s	0.17 kb/s	0.79 kb/s	1.04 MB o	
IPv6 in-pass	68.31 b/s	11.21 b/s	11.97 b/s	70.63 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 17 17:21:27 2014

Small number of packets

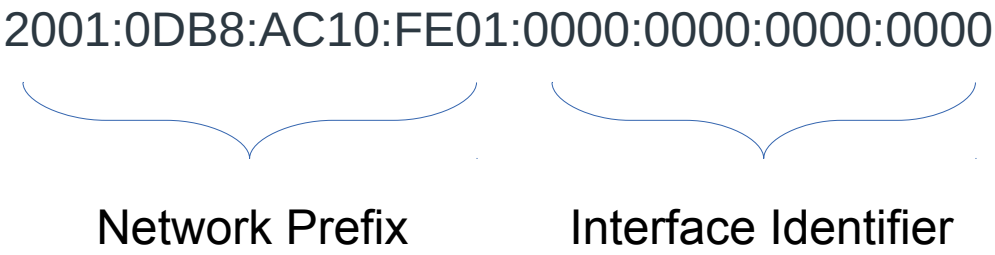


Lots of states



Compromised Hosts

- Stateful Attack
- Data logged in NetFlow (pfflowd)
- States still in memory – dumped via pfctl
- Some 100,000 queries per hour for secure.colegsirgar.ac.uk
- Some 36,000 compromised/infected hosts
- Mostly hosting providers


2001:0DB8:AC10:FE01:0000:0000:0000:0000
Network Prefix
Interface Identifier

Session based hostnames for SSO

~~secure.colegsirgar.ac.uk~~

s-2049dkk3saf87.colegsirgar.ac.uk

s-4598sal4dof40.colegsirgar.ac.uk

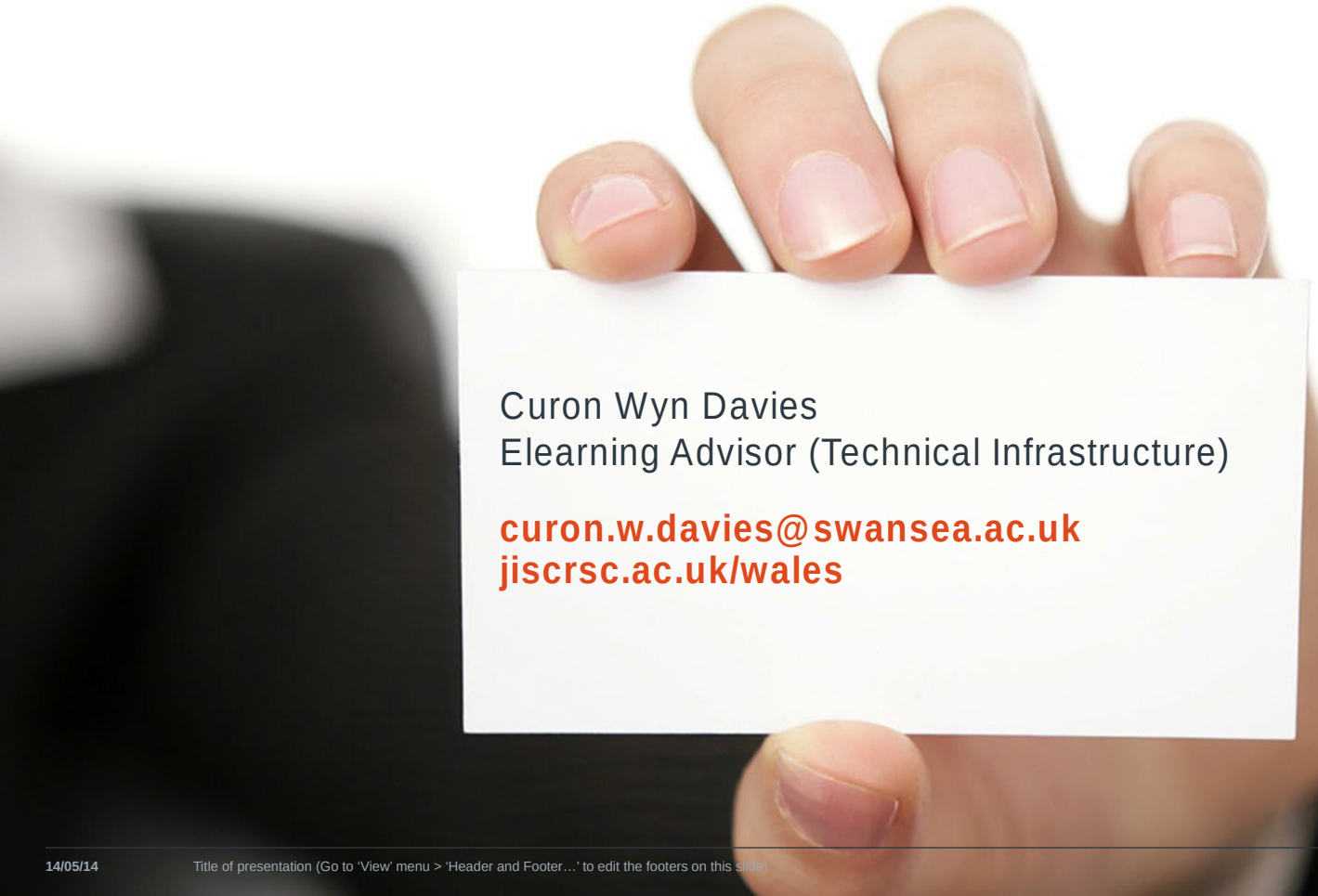
s-3553sge4ive29.colegsirgar.ac.uk

s-3294skd2ifw83.colegsirgar.ac.uk

s-1208oud3lih78.colegsirgar.ac.uk

s-9720dig4kud39.colegsirgar.ac.uk

Find out more…



Curon Wyn Davies
Elearning Advisor (Technical Infrastructure)

curon.w.davies@swansea.ac.uk
jiscrsc.ac.uk/wales