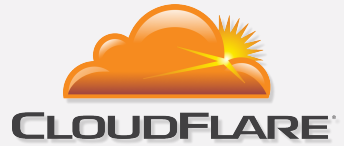
Flowspec

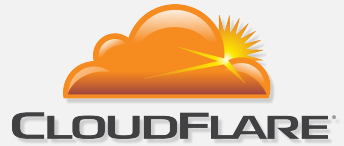
Tom Paseka,
Courtesy of Terry Rodery
Aug 2013

Background



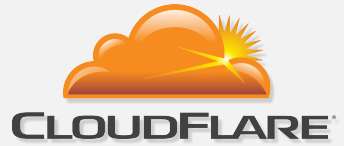
- RFC 5575 (2009)
- Piggybacks on top of existing BGP
- Supported by Juniper (and Alcatel too)
- Available in JunOS since 7.X
- ExaBGP support too.

Operational



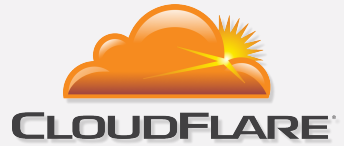
- Configure rules on route server (config so easy a caveman could do it).
- Commit config.
- Rules are pushed via BGP to routers. I typically see the rules appear on my edge routers in a matter of seconds.
- Flowspec counters are available for viewing from CLI using “show firewall”.

Drawbacks



- Flowspec counters ARE NOT available via SNMP! Surely someone can fix this ☺ You'll need to write the necessary poller, database, graphing, etc. to do this.
- Not able to use prefix-lists to define source/destination addresses. Must create multiple rules for multiple prefixes.
- Flowspec is only supported on M,MX,T-Series devices and is not available on EX and SRX.

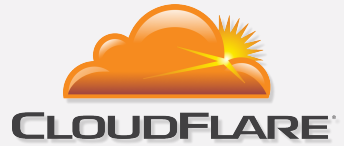
Sample “rule” configs



Discards all traffic to UDP port 80.

```
route DISCARD-80-UDP {
    match {
        protocol udp;
        destination-port 80;
    }
    then discard;
}
```

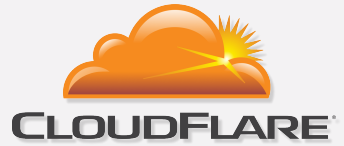
Sample “rule” configs



Rate-limit TCP SYN to 5Mbps. This will be the easiest rate limiting you’ve ever done on JunOS. No more manual policer configuration!

```
route 108.162.203.11-RL {
    match {
        destination 108.162.203.11/32;
        protocol tcp;
        tcp-flags 2;
    }
    then rate-limit 5m;
}
```

Sample “rule” configs

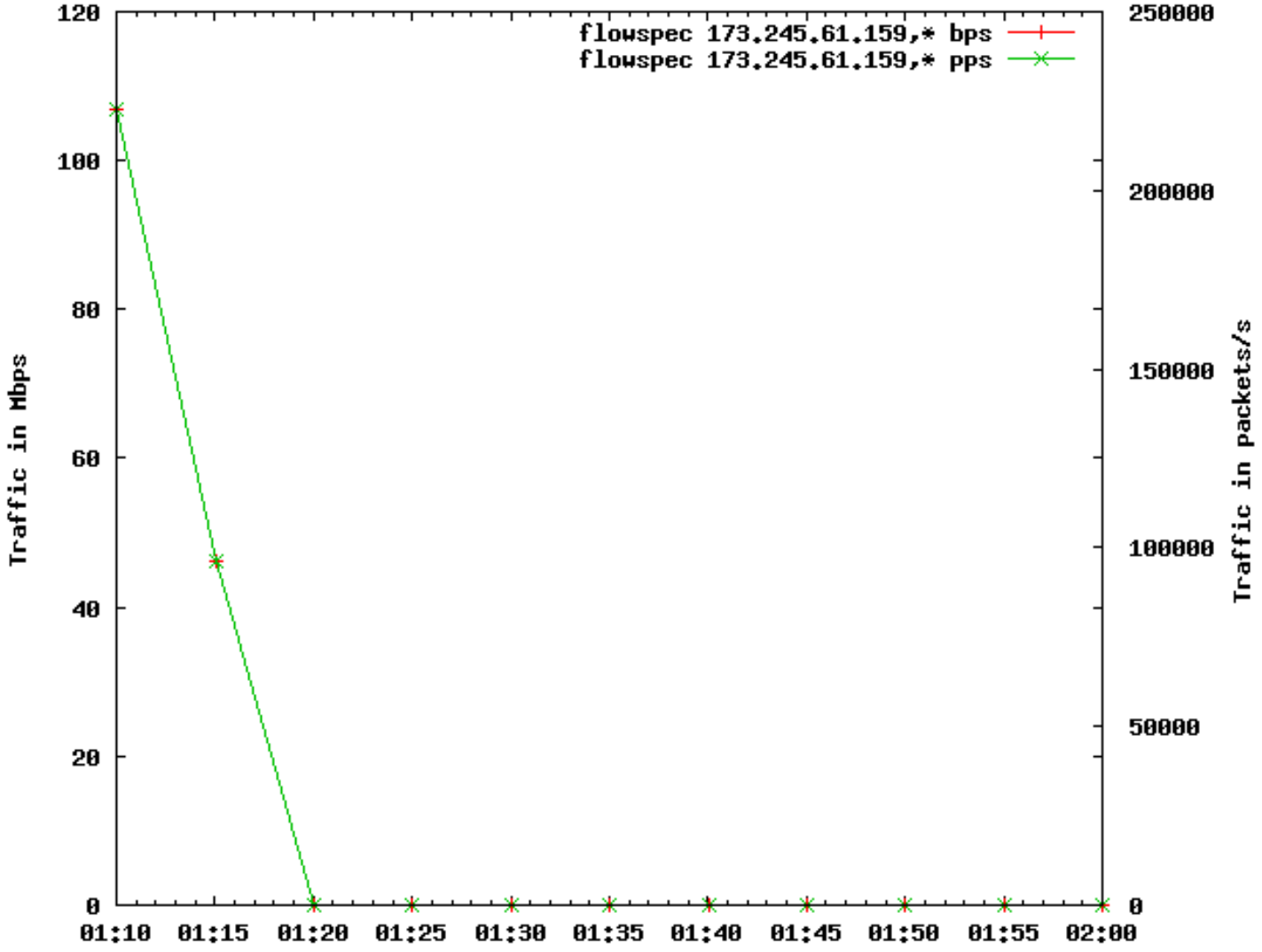



```
route 141.101.124.242-DISCARD {
    match destination 141.101.124.242/32;
    then discard;
}
```

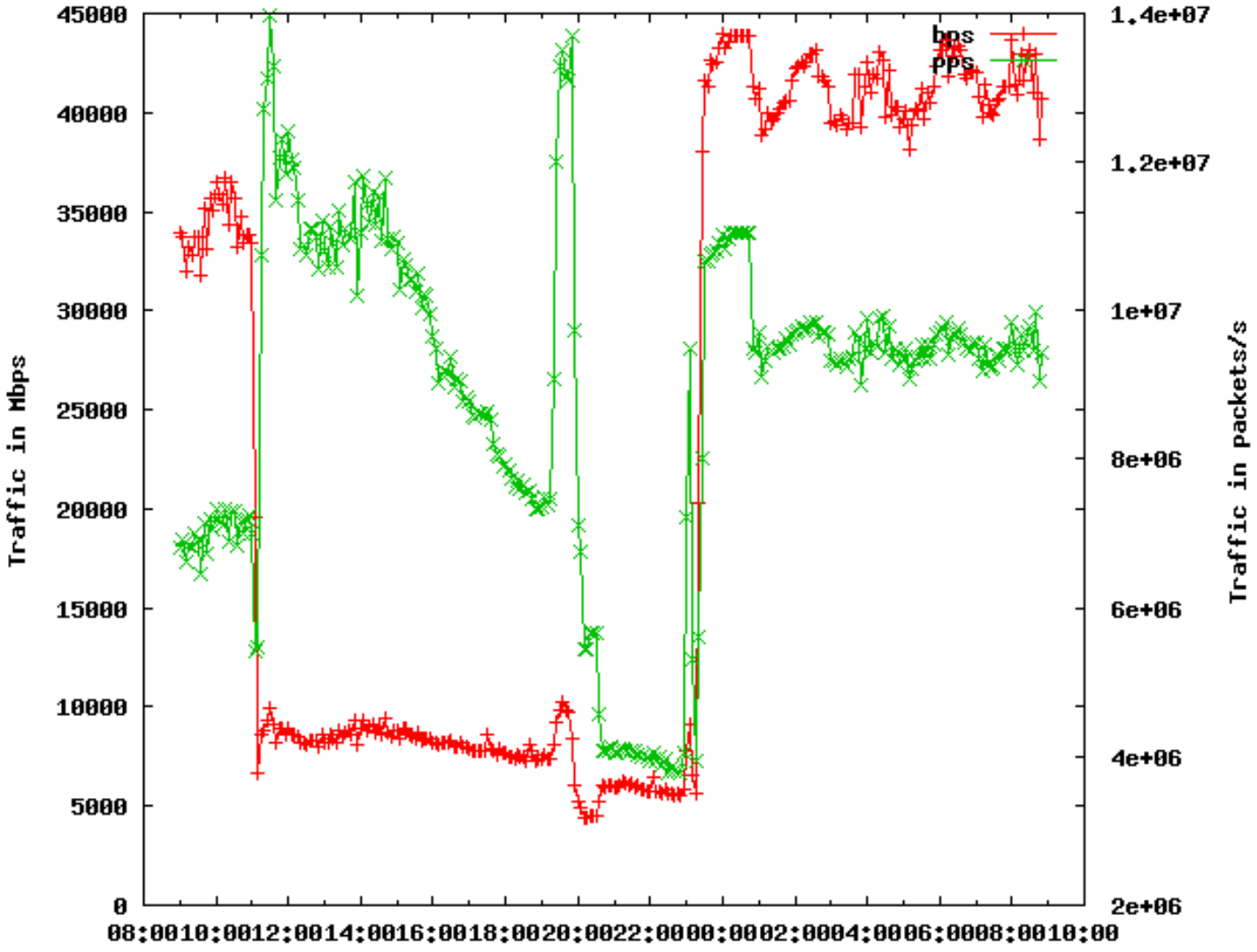
We no longer “nullroute” using BGP triggered blackhole to transit providers so we don’t lose visibility into the attack.

Time for the cool stuff! (Graphs)

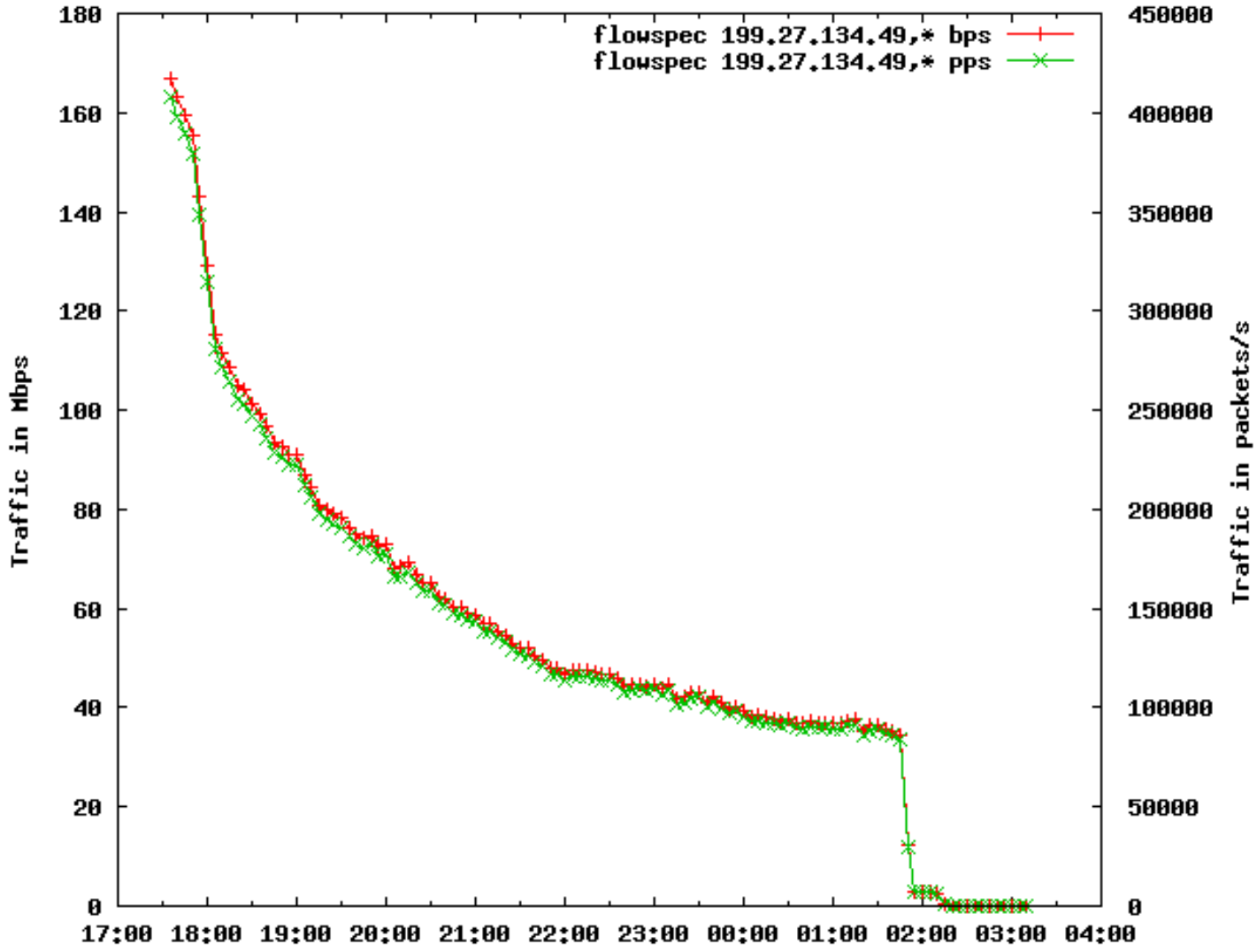
Short Lived Syn Flood



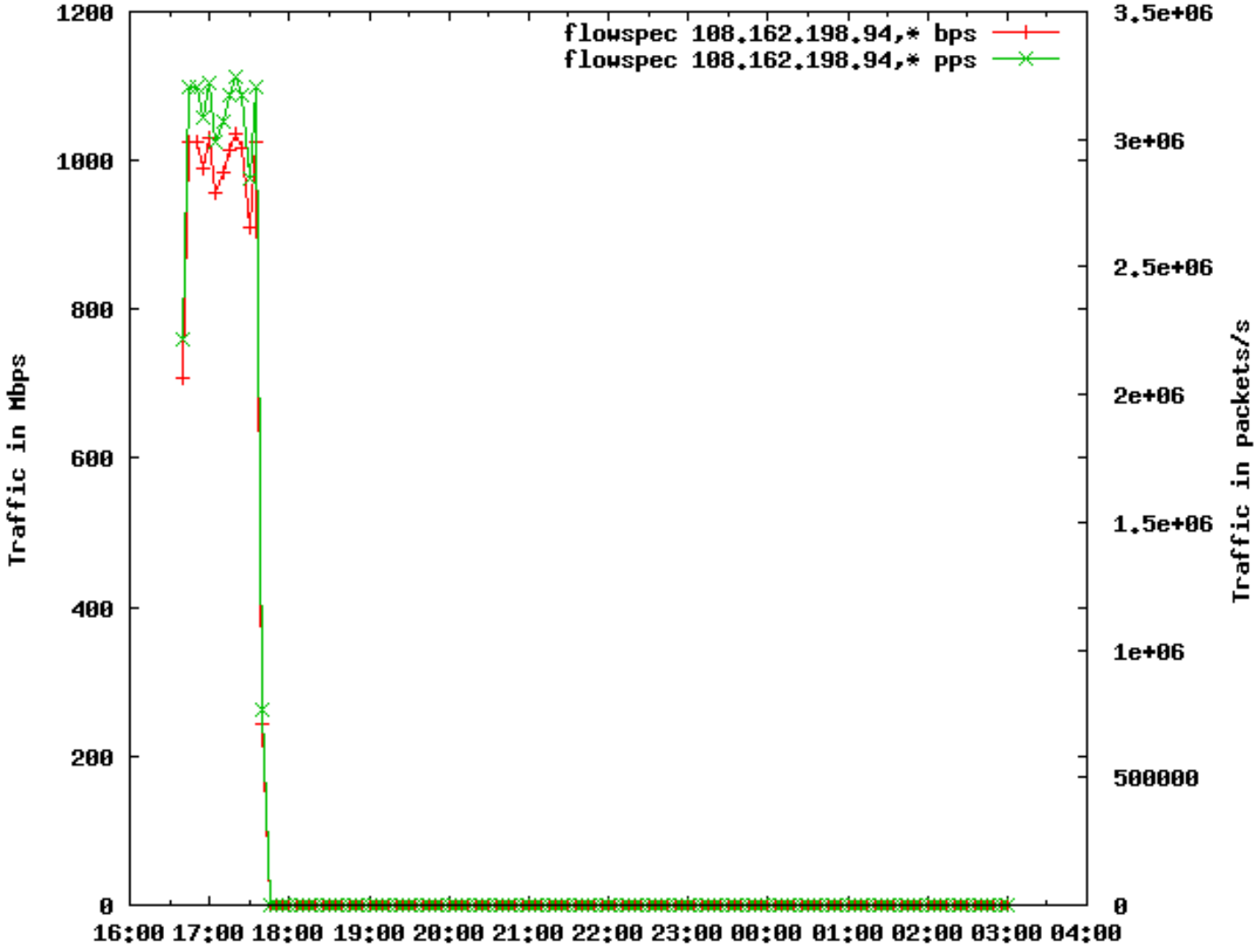
Big attack

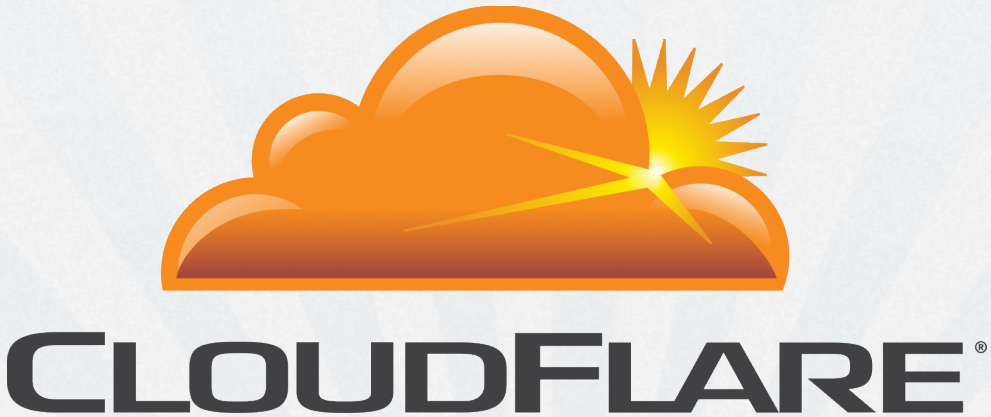

bps
pps
Traffic in Mbps
Traffic in packets/s
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
1.4e+07
1.2e+07
1e+07
8e+06
6e+06
4e+06
2e+06
08:0010:0012:0014:0016:0018:0020:0022:0000:0002:0004:0006:0008:0010:00

Decaying long lived attack



1Gbps attack





Questions?

Thank You