Flow-spec
draft-marques-idr-flow-spec-04

Marques, McPherson, Raszuk

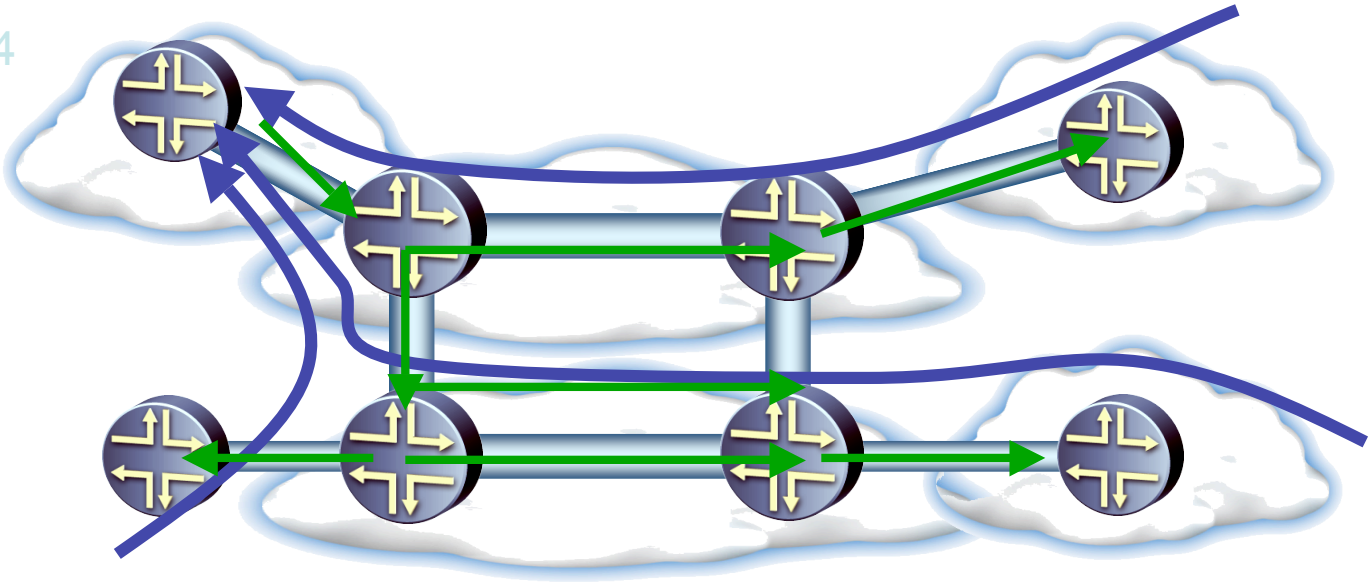
What is a flow-spec ?

- BGP built in propagation of flow specification rules
- Can be used to mitigate DDoS attacks, to rate limit excessive traffic, to monitor specific flows sent and apply policy (e.g., lawful intercept)
- Automates operational headaches (today solved manually), significantly extends BGP-based blackhole routing capabilities

Distributed Traffic Filtering

10.0.1.1,proto=17,port=10000

10.0.1/24



- Attack on 10.0.1.1 with UDP port 10000
- New routing information on existing BGP sessions

Why IDR ?

- It is an extension to BGP (new SAFIs IANA approved 133 & 134) - no new protocol required, employ existing infrastructure for signaling function
- It is application independent, Network and Transport Layer functions – works for IPv4 & IPv6 unicast, but also for VPN routes

Why BGP ?

- Propagation of filtering information should be tightly coupled with the propagation of the original routes
- Automatic verification of the src of the filter must match the src of the original block of prefixes
- Needs to work intra & inter domain
- Defines it’s own NLRI format, but reuses all other BGP attributes for loop free propagation

Next steps

- Three implementations currently, others under development
- Numerous operational deployments
- An application of BGP flow Specification:
  - http://www.nanog.org/mtg-0610/lozano.html

- We would like to ask this group to accept this as a WG document