

Community Flow-spec Project

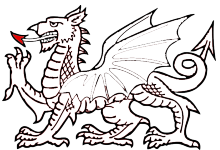


John Kristoff jtk@cymru.com



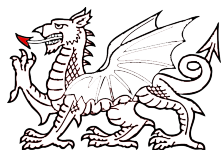
What is Flow-spec?

- IETF RFC 5575
 - Dissemination of Flow Specification Rules
- Think of filters (ACLs) distributed via BGP
- Keyword = flow
 - multiple daddr/saddr prefixes per rule prohibited
- Actions include:
 - accept, discard, rate-limit, sample, redirect
- IMHO, BGP is the wrong mechanism for this, but...



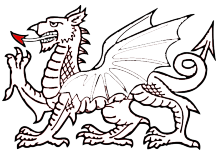
Inter-AS Flow-spec

- Filter state instantiated by other BGP speakers?
 - Import policy or die
- Multi-hop RTBH on steroids
 - saddr/daddr prefix, IP protocol, ICMP type/code, TCP/UDP port, fragment, TCP flag, DSCP
- Complete bogon filtering w/o uRPF
- Real-time black lists
- Abuse Handler + Peering Coordinator
 - = Abeering Coordinator?



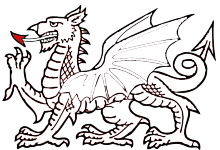
Community Flow-spec Routes

- Traditional bogon feed as source prefix flow routes
- A la carte feeds, e.g.
 - troublesome IP multicast groups
 - community vetted contributions
 - other “bad juju”
- AS path prepend ++
- Feed-specific community + no-export



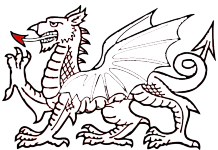
Example: Bogon Flowspec

```
flow {  
  route bogon_s0.0.0.0/8 {  
    match source 0.0.0.0/8;  
    then {  
      discard;  
    }  
  }  
  route bogon_s5.0.0.0/8 {  
    match source 5.0.0.0/8;  
    then {  
      discard;  
    }  
  }  
  route bogon_s10.0.0.0/8 {
```



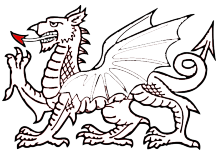
Example: Flow-spec Receiver

```
protocols {
  bgp {
    group flowspec {
      family inet {
        flow {
          prefix-limit {
            maximum 200;
            teardown ...
          }
          no-validate flowspec;
        }
      }
    }
  }
  neighbor 192.0.2.1 {
```



Community Contributed Real-time Flow-spec Routes

- Maybe a nice idea for victim networks
- Not convinced community will trust/want these
- But it might look something like this:
 - Submission via authenticated web form
 - Filters published to f-s community for review
 - Must have originated prefix for 30+ days
 - Must match a source or destination prefix



Want to give it a try?

- You probably want to have JunOS
- This is a research prototype service
 - Could become a production service if warranted
- Test with sampled/accept source bogons feed?

Setup, questions, comments, enhancements to

jtk@cymru.com

<http://www.cymru.com/jtk/>

