Flowspec Indirection-id Redirect
(draft-vandevelde-idr-flowspec-path-redirect-02)
Gunter Van de Velde, Wim Henderickx, Keyur Patel, Arjun Sreekantiah
A logical next step for DDoS

• First there was: Indirection to VRF
  • Recursive look-up inside a VRF to find alternate Next-hop destination
  • RFC5575

• Next there was: Indirection to IP
  • Recursive look-up in Routing Table to alternate next-hop
  • draft-ietf-idr-flowspec-redirect-ip

• Now there is: Indirection to Service-plane
  • Recursive lookup to find alternate chain of next-hops
  • Send DDoS traffic over those links facilitated to transport DDoS
  • draft-vandevelde-idr-flowspec-path-redirect
Technology Summary

• New BGP Flowspec Action -> redirection using “Indirection-ID”

• “Indirection-ID” is a new proposed extended community

• “Indirection-id” is used for a recursive lookup on receiving router

• The flowspec receiving router will use “Indirection-ID” to find out through recursion
  • Tunnel encap information to Next-hop destination
  • Tunnel encap information to Next-Next-hop destination (EPE)
  • Segment Routing Binding SID

• A single Flowspec update from the flowspec controller results in network wide optimized security, application and traffic steering i.e. :
  • Steer to closest IDS or FW or security appliance
  • Steer to engineered path for DDoS mitigation
  • Steer to special regional EPE exit (i.e. for Cloud DDoS handling)
  • Steer to closest Video rendering
  • Steer to path with lowest latency out of the region
  • Steer to None-shared-resource-path (live-live or resilient flow steering)

• Tunnel setup is done out-of-band from flowspec
Changes between -00 and -02

• Added use-case scenario’s:
  • Steer to shortest Path tunnel. Examples could be
    • To regional closest IDS or FW service
    • To best Egress router for the region for flowspec identified traffic
    • To best video rendering device for the region for a particular customer
    • Or simply to a central device in the network
  • Steer to TE-tunnels
    • Steer to RSVP-TE or SR-TE tunnel (to a service)
    • Steer to Segment Routing binding SID
      • i.e. CLI, PCE or BGP based mapping
  • Steer to Next-Next-Hop tunnels
    • Cascaded tunnel tunnel constructs (using “Tunnel ID”)
    • Egress Peer Engineering tunnel constructs
    • Engineered path to egress router and exact egress interface
Changes between -00 and -02

- New co-author: Arjun Sreekantiah
- Revised Community name: “Indirection-id” (to remove purpose confusion)
- Added section to explain “Indirection-id” and “Indirection-id Table”
- Added Validation Procedure
  1. RFC5575 procedures SHOULD be applied
  2. If multiple redirect actions applied, then “Indirection-ID” MUST take priority
  3. When no valid “Indirection-ID” exists, then process as if community was not attached and MUST provide invalid redirection indication
- Added Segment Routing Binding SID context into “Indirection-ID” (using a ‘bit’ in the community local administrator field)
Next steps

• Adopt as a WG document