Flowspec TTL (Time to Live) Match

draft-bergeon-flowspec-ttl-match-00

IETF 111, July 2021

Philippe Bergeon (Nokia)

Use Case

- Main motivation: Flowspec DDoS Mitigation using TTL values. Flowspec v1 RFC 5575, RFC 8955 compatible routers.

- Draft defines a new component to match TTL values. Encoding: <type (1 octet), [numeric_op, value]+>

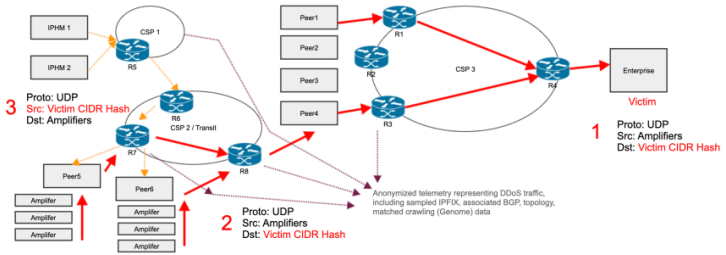
- Studies such as such as the one recently presented at NANOG 82 Tracing DDoS End-to-End in 2021 highlight how filtering traffic based on TTL values can be used as an effective mitigation against volumetric DDoS attacks at the IP edge of the network

Use Case

- The TTL value can be used to differentiate legitimate traffic from DDoS attack traffic generated by DDoS for hire services at the IP edge of the network (direct or reflection/amplification attacks)

Step 1: Trace IPHM

Trace IPHM using fingerprints and real-time IPFIX from across Internet



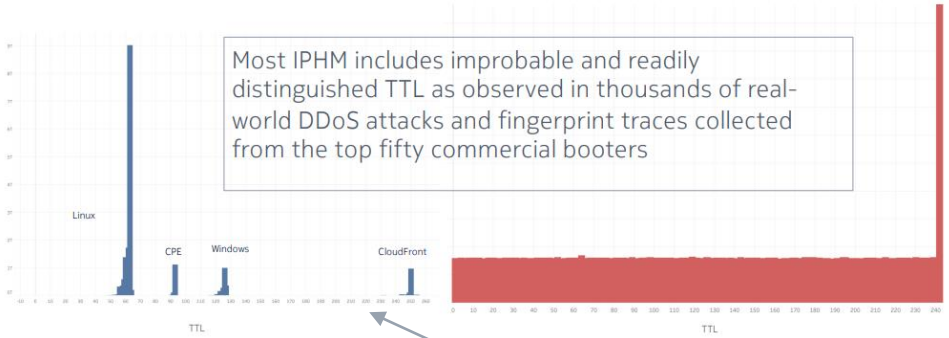
In a process similar to IETF DOTS [39], we use DDoS fingerprint hashes to trace amplified DDoS back to the IPHM hosting origins using [40]. While the victim in step (1) only sees amplifier IPs, we can identify the originating IPHM using fingerprint in step (3)

11

Source: NANOG 82 Tracing DDoS End-to-End in 2021

Step 3: Detect IPHM via Improbable TTL

Sample graph of TTL observed in normal and DDoS traffic



Comment on 5575bis draft

- 5575bis draft up until version 20 included a comment on TTL:

  ```
  The specification of a new Flow Specification Component Type MUST clearly identify what the criteria used
  to match packets forwarded by the router is. This criteria should be meaningful across router hops and
  not depend on values that change hop-by-hop such as TTL or Layer 2 encapsulation.
  ```

- This sentence is not present in RFC 8895 and as seen in Tracing DDoS End-to-End in 2021 the TTL value can be used as an effective filtering match criteria to mitigate DDoS attacks.

- Different IP edge routers (typically peering routers) of a given network under attack may see DDoS attack traffic using slightly different TTL values, however these routers can use a common set of filtering rules propagated via BGP Flowspec as the ranges of known good TTL values can be common.

Thank You