BGP Flowspec Payload Matching

draft-khare-idr-bgp-flowspec-payload-match-08

IETF 110, March 2021

Anurag Khare (Ciena)
Philippe Bergeon (Nokia)
Vijay Kestur (Juniper)
Luay Jalil (Verizon)
Kirill Kasavchenko

Background and Motivations

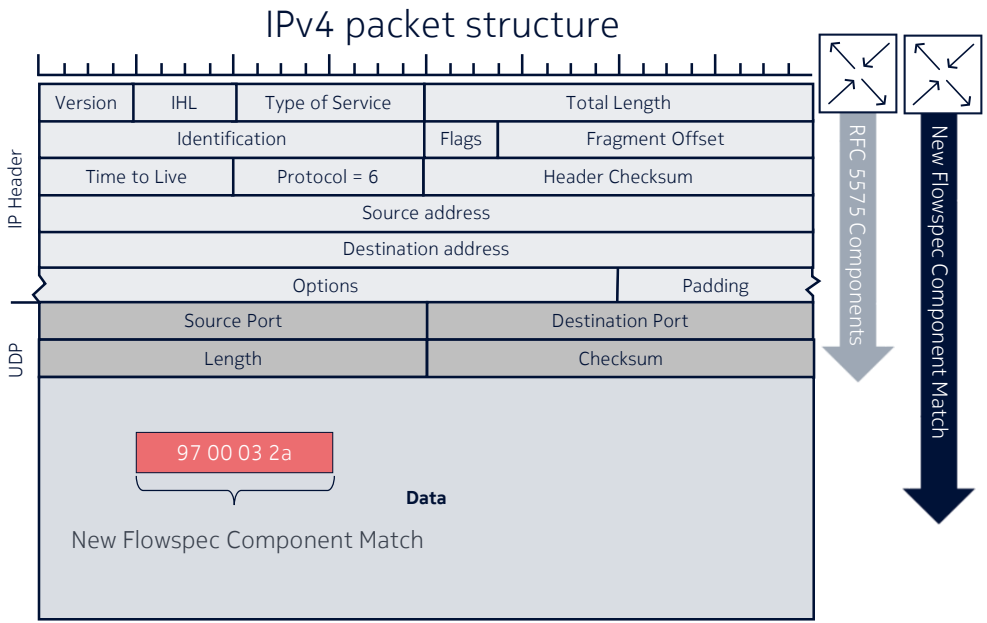
- BGP Flowspec is widely deployed today for n-tuple type filtering using header fields such as IP Prefix, IP protocol, TCP/UDP port number etc…

- Recent advancements to IP router forwarding plane filter implementation can allow matches at arbitrary location within the packet header or payload

- In the context of DDoS mitigation, this new capability can be used to essentially match a signature for the attack traffic and can be combined with traditional n-tuple filter criteria to mitigate volumetric DDoS attacks and reduce false positive to a minimum.

Background and Motivations

- New Flowspec component type for matching a pattern value with the IP packet header or payload
- Enhances DDoS mitigation capability by matching a pattern within the data in addition to IP/Port typical match
- Allow to match header fields not defined in Flowspec RFC yet or across fields
- Allow to match across headers



Component Encoding: **<type (1 octet), length (1 octet), value>**

Value field encoding: **<offset-type (4 bits), offset-value (2 octets), pattern-type (4 bits), pattern-value (variable)>**

Specifications - Offset

Value	Offset Type
0	Layer 3 - IP Header
1	Layer 4 - IP Header Data
2	Payload - TCP/UDP Data

- **Offset-type** and **offset-value** define where the match should begin for the pattern-value
  - Offset type 0 - start of the IP header
  - Offset type 1 - start of the data portion of the IP header after the IP options
  - Offset type 2 - start of the TCP or UDP data

- The **offset-value** defines the number of bytes to ignore in the packet from the offset-type to match the pattern value.

- Examples:
  - The combination of offset-type 0 (Layer 3) and offset-value 0 defines an offset at the very beginning of the IP header.
  - The combination of offset-type 2 (Payload) and offset-value 10 defines an offset ten bytes after the beginning of the TCP/UDP data payload.

Specifications - Pattern

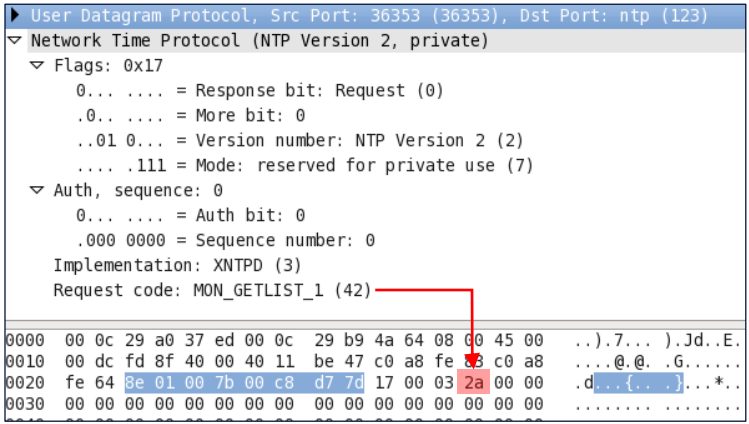
Value	Pattern Type
0	Bitmask match
1	POSIX Regular expression (regex) string match
2	PCRE Regular expression (regex) string match

- The pattern-type defines how the pattern value is matched
  - Pattern Type 0 – Bitmask match
  - Pattern Type 1/2 – Regular expressions (software forwarding planes, appliances …)

- Bitmask match encoded as **{prefix, mask}** of equal length
  - prefix - Provides a bit string to be matched. The prefix and mask fields are bitwise AND'ed to create a resulting pattern.
  - mask - Paired with the prefix field to create a bit string match. An unset bit is treated as a 'do not care' bit in the corresponding position in the prefix field. When a bit is set in the mask, the value of the bit in the corresponding location in the prefix field must match exactly.

Specifications - Example

- Matching on the UDP NTP Request Code value 0x2a can be achieved using:
  - Component type 4 for IP Protocol UDP
  - Component type TBD for Flexible Match Condition with:
    - Offset type = 2 for TCP/UDP Payload
    - Offset value = 3 (for 3 bytes after the beginning of the data)
    - Pattern type = 0 (bitmask)
    - Pattern value Prefix = 0x2a
    - Pattern value Mask = 0xFF



Further Action

- Comments and feedbacks?
- Registration of a new component type?

Thank You