IS-IS Extensions for Flow Specification

draft-you-isis-flowspec-extensions-02

Jianjie You (youjianjie@huawei.com)

Qiandeng Liang
(liangqiandeng@huawei.com)
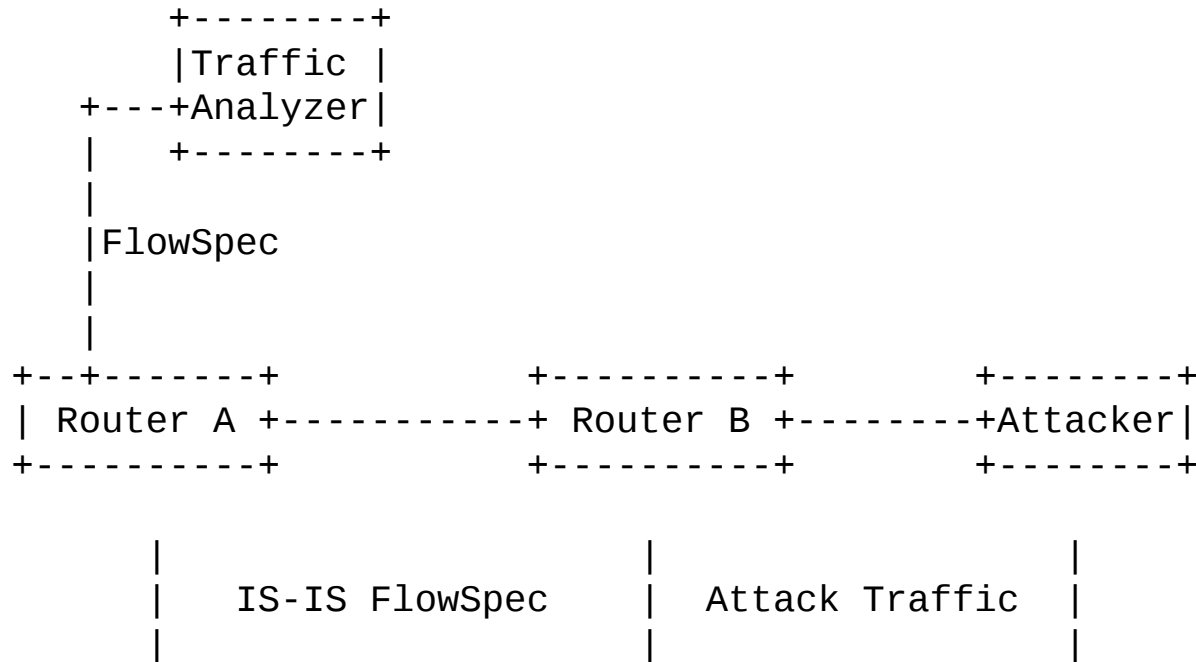
Keyur Patel (keyupate@cisco.com)

Peng Fan (fanpeng@chinamobile.com)

IETF94 Yokohama

Status of this I-D

♦ First presented in IETF 93, Prague meeting

➢ IS-IS is not defined as an IETF PE-CE protocol
Removed BGP/MPLS VPN use case, only keep IS-IS campus network use case.

➢ What happens if multiple routers inject filter components? Defined in section 4.1.1, the order of applying the traffic filter rules is the same as described in Section 5.1 of RFC5575

➢ How to limit these FlowSpec rules in the routing domain? If Flag set, the FlowSpec Reachability TLV SHOULD be flooded across the entire routing domain. Otherwise, it MUST NOT be leaked between levels.

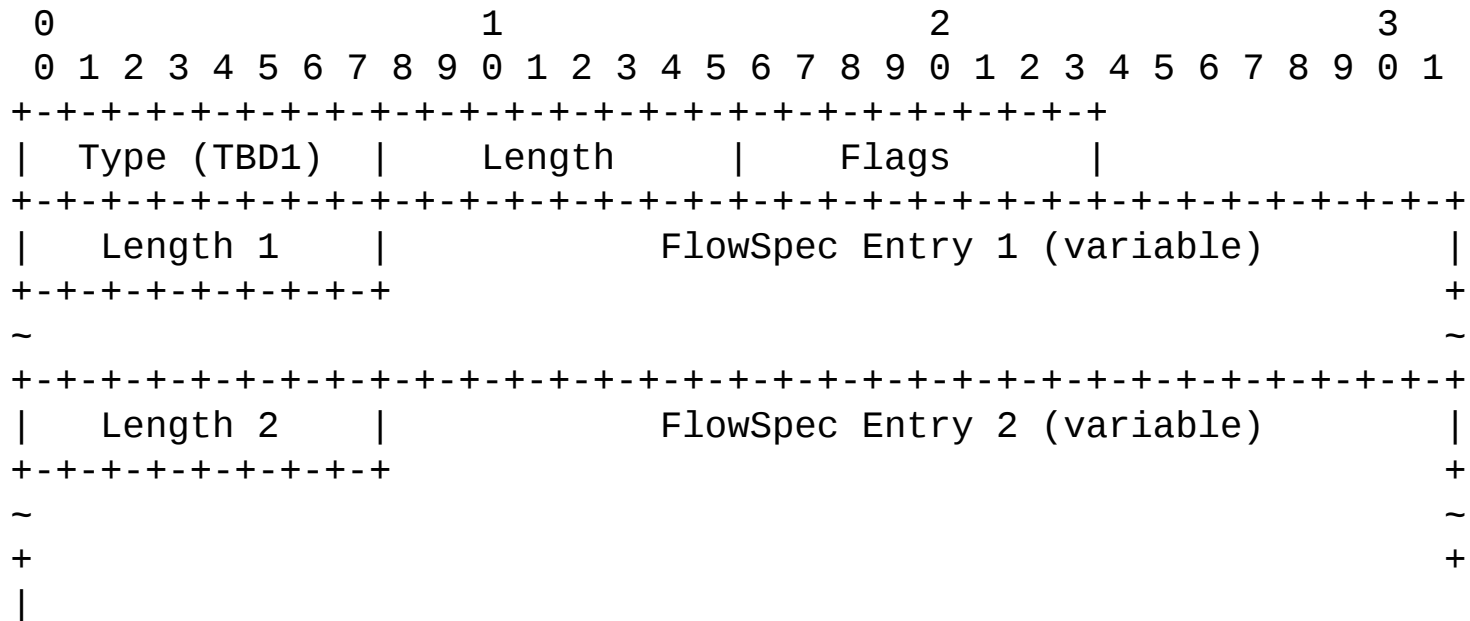♦ The update compared to v-01

➢ Removed section 3.2 BGP/MPLS VPN

Use Case – Campus Network

```
                  +--------+
                  |Traffic |
              +---+Analyzer|
              |   +--------+
              |
              |FlowSpec
              |
              |
        +--+-------+            +----------+            +--------+
        | Router A +-----------+ Router B +--------+Attacker|
        +----------+            +----------+            +--------+

             |                        |                        |
             |     IS-IS FlowSpec     |    Attack Traffic      |
             |                        |                        |
```

For networks not deploying BGP, for example, the campus
network using IS-IS, it is expected to extend IS-IS to distribute
FlowSpec rules as shown in Figure 1.

IS-IS Extensions for FlowSpec

This document defines a new IS-IS TLV, i.e. **the FlowSpec reachability TLV** (TLV type: TBD1), which would be carried in an LSP (Link State Protocol) Data Unit [ISO-10589], to describe the FlowSpec rules.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type (TBD1)  |     Length    |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Length 1    |           FlowSpec Entry 1 (variable)        |
+-+-+-+-+-+-+-+                                                 +
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Length 2    |           FlowSpec Entry 2 (variable)        |
+-+-+-+-+-+-+-+                                                 +
~                                                               ~
+                                                               +
|
```

- **Flags:** One octet Field identifying Flags. The least significant bit L is defined as a Leaking enable bit. If set, the FlowSpec Reachability TLV SHOULD be flooded across the entire routing domain. If the L flag is not set, the FlowSpec Reachability TLV MUST NOT be leaked between levels.
- **FlowSpec Entry:** Each FlowSpec entry consists of FlowSpec filters (FlowSpec filters sub-TLVs) and corresponding FlowSpec actions (FlowSpec Action sub-TLVs).

Next Step

- This document proposes to extend IS-IS to support FlowSpec. It is an equivalent draft to https://tools.ietf.org/html/draft-ietf-ospf-flowspec-extensions-00
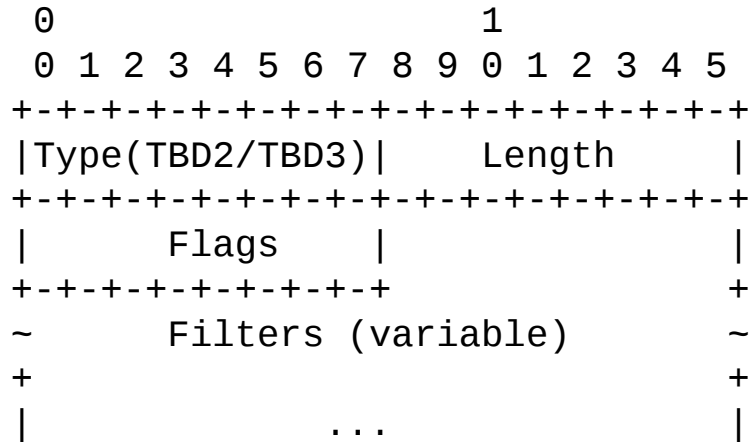
- Accepted as WG doc?

Thank You!

Motivation

❑ FlowSpec rules are used to distribute traffic filtering rules that are used to filter Denial-of-Service (DoS) attacks.

❑ For the networks only deploying IGP (Interior Gateway Protocol) (e.g. IS-IS), it is expected to extend IGP to distribute FlowSpec info.

❑ The IS-IS FlowSpec extensions defined in this document can be used to mitigate the impacts of DoS attacks.

IS-IS Extensions for FlowSpec:

FlowSpec Filters sub-TLV

The FlowSpec Reachability TLV carries one or more FlowSpec entries. Each FlowSpec entry consists of FlowSpec filters (FlowSpec filters sub-TLVs) and corresponding FlowSpec actions (FlowSpec Action sub-TLVs).

```
 0                             1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Type(TBD2/TBD3)|    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Flags     |               |
+-+-+-+-+-+-+-+-+               +
~       Filters (variable)      ~
+                               +
|              ...              |
```

- **Flags:** One octet Field identifying Flags. The least significant bit S is defined as a strict filter check bit. If set, strict validation rules outlined in the validation section (Section 4.1.2) need to be enforced.
- **Filters:** the same as "flow-spec NLRI value" defined in [RFC5575] and [I-D.ietf-idr-flow-spec-v6].
- **Type:** the TLV type (TBD2 for IPv4 FlowSpec filters, TBD3 for IPv6 FlowSpec filters)

IS-IS Extensions for FlowSpec:
FlowSpec Action sub-TLV

There are one or more FlowSpec Action TLVs associated with a FlowSpec Filters TLV. Different FlowSpec Filters TLV could have the same FlowSpec Action TLVs.

```
        Table 2: Traffic Filtering Actions in [RFC5575], etc.
  +-------+----------------+------------------------------------+
  | type  | FlowSpec Action | RFC/WG draft                      |
  +-------+----------------+------------------------------------+
  | 0x8006| traffic-rate   | RFC5575                           |
  |       |                |                                    |
  | 0x8007| traffic-action | RFC5575                           |
  |       |                |                                    |
  | 0x8108| redirect-to-IPv4| I-D.ietf-idr-flowspec-redirect-rt-bis |
  |       |                |                                    |
  | 0x800b| redirect-to-IPv6| I-D.ietf-idr-flow-spec-v6        |
  |       |                |                                    |
  | 0x8009| traffic-marking | RFC5575                          |
  +-------+----------------+------------------------------------+
```