Abstract

This document specifies a new BGP-FS component type to support AS-level filtering. The match field is the origin AS number of the destination IP address that is encoded in the Flowspec NLRI.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 7, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Introduction

BGP Flow Specification (BGP-FS) [RFC5575] defines a new BGP NLRI to distribute traffic flow specification rules via BGP ([RFC4271]). BGP-FS policies have a match condition that may be n-tuple match in a policy, and an action that modifies the packet and forwards/drops the packet. Via BGP, new filter rules can be sent to all BGP peers simultaneously without changing router configuration, and the BGP peer can install these routes in the forwarding table. BGP-FS defines Network Layer Reachability Information (NLRI) format used to distribute traffic flow specification rules. NLRI (AFI=1, SAFI=133) is for IPv4 unicast filtering. NLRI (AFI=1, SAFI=134) is for BGP/MPLS VPN filtering. [I-D.ietf-idr-flowspec-l2vpn] extends the flow-spec rules for layer 2 Ethernet packets.

This document specifies a new BGP-FS component type to support AS-level filtering. The match field is the origin AS number of the destination IP address that is encoded in the Flowspec NLRI.

2. Definitions and Acronyms

- FS: Flow Specification
- Destination-IP-Origin-AS: The origin AS number of the destination IP address

This document proposes a new flow specification rule that is encoded in the NLRI. The following new component type is defined.

- Destination-IP-Origin-AS

Type TBD1 - Destination-IP-Origin-AS

Encoding: <type (1 octet), [op, value]+>

Contains a set of (operator, value) pairs that are used to match the Destination-IP-Origin-AS (i.e. the origin AS number of the destination IP address).

The operator byte is encoded as:

```
0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| e | a | len | 0 |lt |gt |eq |
+---+---+---+---+---+---+---+---+
```

Where:

- e - end-of-list bit. Set in the last (op, value) pair in the list.
- a - AND bit. If unset, the previous term is logically ORed with the current one. If set, the operation is a logical AND. It MUST be unset in the Destination-IP-Origin-AS filter.
- lt - less than comparison between data and value.
- gt - greater than comparison between data and value.
- eq - equality between data and value.

The bits lt, gt, and eq can be combined to produce match the Destination-IP-Origin-AS filter or a range of Destination-IP-Origin-AS filter (e.g. less than AS1 and greater than AS2).

The value field is encoded as:

```
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
+---------------------------------------------------------------+
~       Destination-IP-Origin-AS  (4 octets)                    ~
+---------------------------------------------------------------+
```
4. Use Case

In AS64597’s R1, if the ISP AS64597 wants to redirect all packets from IP Prefix 61 to AS64598, first goto to R3, then forward to AS64598", the ISP can use the traditional method or the method defining in this draft.

```
+---------+
| BGP FS  |
| Server  |
+---------+

IP Prefix 61 * / AS64597 * IP Prefix 83
* / * IP Prefix 84
+---+ +---+ * +---+
AS64596 R1+ AS64598
+---+ 

IP Prefix 81
* 
* / * IP Prefix 91
* 
* 
* 
* R3+AS64599+
* 
* 

Figure 1: Steering the Traffic Using Flowspec
```

Using the traditional method, the ISP AS64597 needs to setup multiple "Destination Prefix + Source Prefix" rules in Router R1 as following:
Figure 2: Steering the Traffic Using Destination Prefix and Source Prefix

Using the method defining in this draft, the ISP AS64597 needs to setup only one "Destination Origin AS + Source Prefix" rule in Router R1 as following:

<table>
<thead>
<tr>
<th>Destination Prefix</th>
<th>Source Prefix</th>
<th>Redirect to IP Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>64598</td>
<td>IP Prefix 61</td>
<td>R3</td>
</tr>
</tbody>
</table>

Figure 3: Steering the Traffic Using Origin AS and Source Prefix

5. Security Considerations

No new security issues are introduced to the BGP protocol by this specification.

6. IANA

IANA is requested to a new entry in "Flow Spec component types registry" with the following values:

<table>
<thead>
<tr>
<th>Type</th>
<th>RFC or Draft</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD1</td>
<td>This Draft</td>
<td>Destination-IP-Origin-AS</td>
</tr>
</tbody>
</table>
7. Contributors

TBD

8. Acknowledgments

The authors would like to acknowledge the review and inputs from Gang Yan, Zhenbin Li, Rainbow Wu and Ziqing Cao.

9. References

[I-D.ietf-idr-flowspec-l2vpn]

[I-D.ietf-idr-rfc5575bis]


Authors’ Addresses

Haibo Wang
Huawei
156 Beiqing Road
Beijing  100095
P.R. China

Email: rainsword.wang@huawei.com
Aijun  
China Telecom  
Beiqijia Town, Changping District  
Beijing 102209  
P.R. China  
Email: wangaj3@chinatelecom.cn

Shunwan Zhuang  
Huawei  
156 Beiqing Road  
Beijing 100095  
P.R. China  
Email: zhuangshunwan@huawei.com