IDR Working Group
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

H. Wang
Huawei
A. Wang
China Telecom
S. Zhuang
J. Dong
T. Qin
Huawei

2 March 2026

Source-IP-Origin-AS Filter for BGP Flow Specification
draft-wang-idr-flowspec-sip-origin-as-filter-00

Abstract

This document defines an extension to the Border Gateway Protocol (BGP) Flow Specification (FlowSpec) to enable filtering based on the Origin Autonomous System (AS) of the source IP address. This extension is particularly useful in mitigating Distributed Denial of Service (DDoS) attacks where the source IP addresses are dynamic but belong to a specific source AS.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 3 September 2026.

Table of Contents

1. Introduction

BGP Flow Specification (FlowSpec), defined in [RFC8955] and [RFC8956], allows for the dissemination of traffic filtering rules. Current FlowSpec components support filtering by destination prefix, source prefix, and various Layer 4 parameters.

In certain DDoS mitigation scenarios, an operator may need to apply rate-limiting or filtering to all traffic sourced from a particular network (Autonomous System), even when the specific souce IP prefixes within that AS are numerous or rapidly changing. Manually updating hundreds of prefix-based FlowSpec rules is inefficient. This document introduces a new FlowSpec component that allows operators to use the Source Origin AS as a matching criterion.

2. Definitions and Acronyms

* FS: Flow Specification

* Source-IP-Origin-AS: The origin AS number of the source IP address

3. The Flow Specification Encoding for Destination-IP-Origin-AS Filter

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

* Source-IP-Origin-AS

Type TBD1 - Source-IP-Origin-AS

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

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

The operator byte is encoded as:

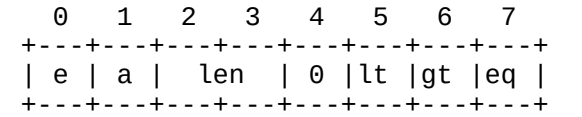

Figure 1: Numeric Operator (numeric_op)

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 Source-IP-Origin-AS filter.

len - The length of the value field for this operator given as (1 << len). This encodes 1 (len=00), 2 (len=01), 4 (len=10), and 8 (len=11) octets.

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 Source-IP-Origin-AS filter or a range of Source-IP-Origin-AS filter(e.g. less than AS1 and greater than AS2).

The value field is encoded as:

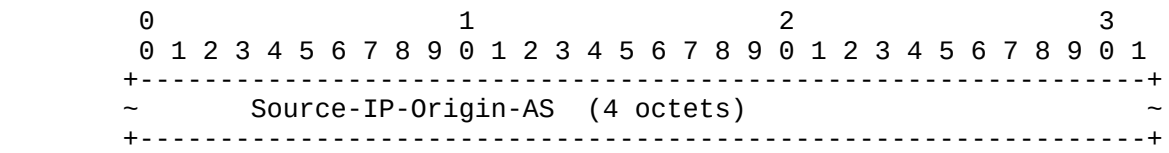

Figure 2: Source-IP-Origin-AS

Per section 10 of [RFC8955] , If a receiving BGP speaker cannot support this new Flow Specification component type, it MUST discard the NLRI value field that contains such unknown components. Since the NLRI field encoding (Section 4 of [RFC8955]) is defined in the form of a 2-tuple <length, NLRI value>, message decoding can skip over the unknown NLRI value and continue with subsequent remaining NLRI.

In cases of multi-homed prefixes with multiple Origin ASes, the match succeeds if any of the valid Origin ASes match the filter.

3.1. Operational Procedures

When a BGP speaker receives a FlowSpec update containing the Source-IP-Origin-AS component:

It MUST determine the Origin AS of the souce IP of the transit packet by performing a lookup in its local BGP RIB.

If the packet’s source IP matches a prefix whose BGP path has an AS_PATH where the rightmost AS (the origin) matches the value in the FlowSpec rule, the action (e.g., rate-limit, discard) MUST be applied.

4. Use Cases

This section describes how to use this function in a simple scenario. Considering the topology shown in Figure 3. In AS64597’s R2, if the ISP AS64597 wants to redirect all packets originating from AS64598 to IP Prefix 61:

"first go to R3, then forward them to IP Prefix 61", the ISP AS64597 can use the traditional method or the method defining in this draft.

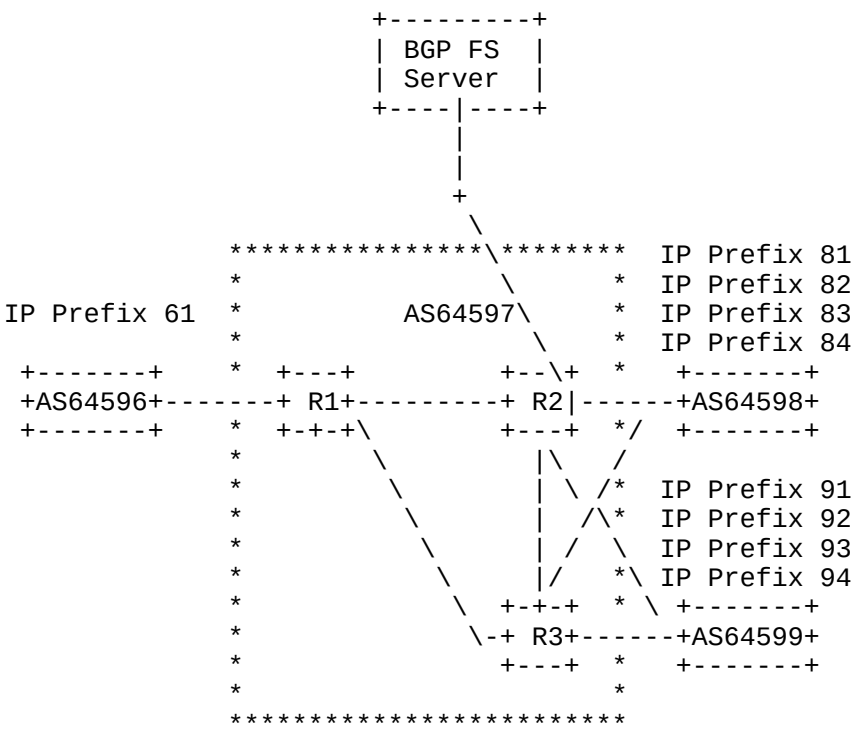

Figure 3: Redirect the traffic using Flowspec

Using the traditional method, the ISP AS64597 needs to setup multiple "Source Prefix + Destination Prefix" rules in Router R2 as following:

Destination Prefix	Source Prefix	Redirect to IP Nexthop
IP Prefix 61	IP Prefix 81	R3
IP Prefix 61	IP Prefix 82	R3
IP Prefix 61	IP Prefix 83	R3
IP Prefix 61	IP Prefix 84	R3
More ...		

Figure 4: Using the traditional method to redirect the traffic

Using the method defining in this draft, the ISP AS64597 needs to setup only one "Source IP Origin AS + Destination Prefix" rule in Router R2 as following:

Soure IP Origin AS	Destination Prefix	Redirect to IP Nexthop
64598	IP Prefix 61	R3

Figure 5: Using the AS-level filtering method to redirect the traffic

Obviously, the new method defining in this draft saves a lot of entry spaces on the control plane and forwarding plane, and it would greatly simplify the operation of the control plane, and the more source prefixes an AS has, the more obvious the benefit.

5. Security Considerations

In addition to the security considerations in [RFC8955], operators must be aware of:

* Routing Inconsistency: If different routers in the network have different views of the BGP table, the "Origin AS" for a given IP may differ, leading to inconsistent filter application.

* AS_PATH Manipulation: An attacker could potentially spoof or prepend ASes to bypass filters if the local BGP table is compromised.

* Validation: Implementations SHOULD ensure that FlowSpec rules are validated against the originating peer to prevent unauthorized AS-based filtering across administrative boundaries.

6. IANA

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

Type	RFC or Draft	Description
TBD1	This Draft	Source-IP-Origin-AS

7. Contributors

TBD

8. Acknowledgments

TBD

9. References

[I-D.ietf-idr-flowspec-l2vpn]
Weiguo, H., Eastlake, D. E., Litkowski, S., and S. Zhuang, "BGP Dissemination of L2 Flow Specification Rules", Work in Progress, Internet-Draft, draft-ietf-idr-flowspec-l2vpn-26, 23 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-flowspec-l2vpn-26>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/info/rfc8955>.

[RFC8956] Loibl, C., Ed., Raszuk, R., Ed., and S. Hares, Ed., "Dissemination of Flow Specification Rules for IPv6", RFC 8956, DOI 10.17487/RFC8956, December 2020, <https://www.rfc-editor.org/info/rfc8956>.

Authors' Addresses

Haibo Wang
Huawei
156 Beiqing Road
Beijing
100095
P.R. China
Email: rainsword.wang@huawei.com

Aijun Wang
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

Jie Dong
Huawei
156 Beiqing Road
Beijing
100095
P.R. China
Email: jie.dong@huawei.com

Tao Qin
Huawei
156 Beiqing Road
Beijing
100095
P.R. China
Email: qintao11@huawei.com