

Inter-Domain Routing  
Internet-Draft  
Intended status: Standards Track  
Expires: 4 January 2026

Z. Li, Ed.  
S. Liu, Ed.  
China Mobile  
3 July 2025

BGP Flowspec Redirects to SR Policy  
draft-li-idr-flowspec-sr-policy-01

## Abstract

Flowspec, an extension to BGP, enables the dissemination of traffic flow specification rules and can be used to steer traffic into SR Policy. However, existing approaches using Flowspec to direct traffic into a SR Policy have certain drawbacks (for details, refer to section 1).

This document defines two new standard actions for the BGP Flowspec V2 protocol (FSv2) [I-D.ietf-idr-flowspec-v2]: Redirect to SR Policy Action and SRv6 SID Action. The former allows traffic to be directed to a designated SR Policy, while the latter allows for the encapsulation of an additional SRv6 SID as required during redirection.

The Redirect to SR Policy Action can be used independently or in conjunction with the SRv6 SID Action, depending on the application scenario. Additionally, the SRv6 SID Action can be used together with other actions defined in FSv2, such as Redirect to IPv6.

## 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 4 January 2026.

## Copyright Notice

Copyright (c) 2025 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 (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Requirements Language . . . . .	4
2. FSv2 Extension . . . . .	4
2.1. Redirect to SR Policy Action . . . . .	4
2.2. SRv6 SID Action . . . . .	6
3. Application Scenario . . . . .	7
4. IANA Considerations . . . . .	8
5. Security Considerations . . . . .	8
6. References . . . . .	8
6.1. Normative References . . . . .	8
6.2. Informative References . . . . .	9
Acknowledgements . . . . .	10
Authors' Addresses . . . . .	10

## 1. Introduction

[RFC8955] and [RFC8956] define the BGP Flow Specification (Flowspec), which allows the conveyance of flow specifications and associated traffic filtering actions (such as rate-limiting, redirect, remark, etc.). BGP flow specifications are encoded within the MP\_REACH\_NLRI and MP\_UNREACH\_NLRI attributes [RFC4760]. Traffic filtering actions are encoded in the Extended Community attribute [RFC4360]. The BGP Flow Specification function enables BGP Flow Specification routes carrying traffic policies to be transmitted to BGP Flow Specification peers for traffic steering.

SR Policy (including SR-MPLS and SRv6 Policy) [RFC9256] is a tunneling technology based on SR-MPLS or SRv6. A SR Policy consists of a set of candidate paths, each of which is composed of one or more segment lists, i.e., segment ID (SID) lists. Each SID list identifies an end-to-end path from the source node to the destination node, instructing a network device to forward traffic along this path

rather than the shortest path computed by an IGP. The header of a packet steered into a SR Policy is augmented with an ordered list of segments associated with that SR Policy, enabling other network devices traversed by the packet to execute the instructions encapsulated in the list.

Regarding the use of BGP Flow specification to steer traffic into a SR Policy, the method proposed in [I-D.ietf-idr-ts-flowspec-srv6-policy] employs the redirect-to-IP action defined in [I-D.ietf-idr-flowspec-redirect-ip]. It carries the endpoint information of the SR Policy in the redirect-to-IP action, and requires the flowspec protocol to carry color information through the BGP attribute in this case, and carry prefix SID information as necessary. This method adds a new action, redirect to SR Policy, to the originally single-action redirect to IP. The newly added redirect to SR Policy action can only be distinguished by whether the BGP attributes carry the color extended community attribute. Since the color extended community attribute is optional, this can lead to errors in the following scenarios: Redirect to SR Policy may fail when the color extended community attribute is absent; Redirect to IP may fail when the color extended community attribute is present. Additionally, [I-D.ietf-idr-ts-flowspec-srv6-policy] is merely an informational document in the IETF, not a standard solution for steering traffic into a SR Policy. To satisfy the requirement for the headend node to encapsulate an SRv6 Service SID when performing the redirect to SR Policy action, [I-D.ietf-idr-ts-flowspec-srv6-policy] suggests using the SRv6 Services TLVs defined for VPN services. These TLVs would be carried in the BGP Prefix-SID Attribute and sent to the headend node along with the redirect to SR Policy action. While this approach of reusing attributes or fields defined for other purposes is easy to implement, it can cause confusion.

[I-D.ietf0-idr-srv6-flowspec-path-redirect] proposes a scheme that indirectly steers traffic into a SR Policy through a Binding SID (BSID). However, this approach requires knowledge of the BSID corresponding to the SR Policy, which poses a high requirement. Moreover, as explicitly stated in [RFC9256], not every SR Policy is required to have a BSID, and the specific value of a BSID may change over time and with state. Therefore, [RFC9256] specifically notes that the BSID should not be used as an identifier for a SR Policy. Consequently, the scheme proposed in [I-D.ietf0-idr-srv6-flowspec-path-redirect] is technically unfeasible.

To address the drawbacks mentioned above, this document extends the BGP Flowspec V2 protocol [I-D.ietf-idr-flowspec-v2] (FSv2) by defining two new standard traffic filtering actions specifically for

steering traffic into a SR Policy: Redirect to SR Policy Action and SRv6 SID Action. The SRv6 SID Action is optional. It can be used in conjunction with the Redirect to SR Policy Action or other actions defined in FSv2 when needed.

The current version of this document focuses on FSv2 extensions for SRv6 Policy. FSv2 extensions for SR-MPLS Policy will be provided in a later version or written in a separate draft.

### 1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "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.

## 2. FSv2 Extension

This document defines a new traffic filtering action: Redirect to SR Policy Action. It is specifically encapsulated and carried through the BGP Community Container Attribute (also known as BGP Wide Communities) defined in [I-D.ietf-idr-wide-bgp-communities].

The definition and format of an action-SubTLV in the BGP Community Container Attribute are illustrated in Figure 1.

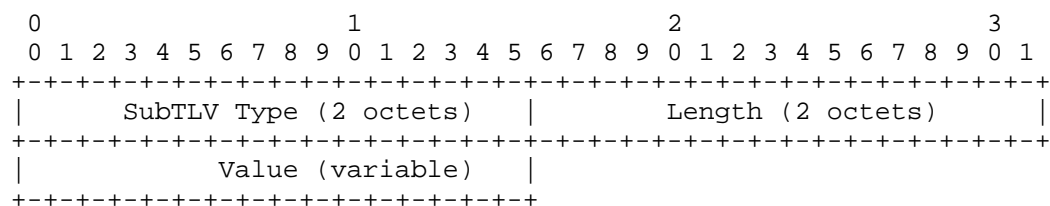


Figure 1: Format of Action-SubTLV

### 2.1. Redirect to SR Policy Action

The newly defined redirect to SR policy Action in this document is represented by the action-SubTLV.

Where:

SubTLV Type (2 octet): Used to indicate that this action-SubTLV is a Redirect to SR policy Action SubTLV. Its value is requested to be assigned by IANA.

Length (2 octet): Measured in byte, used to indicate the total length of the Redirect to SR policy Action.

Value (variable): Used to specify the particular SR policy to which the traffic is to be directed.

The Value field for Redirect to SR policy Action SubTLV is shown in Figure 2.

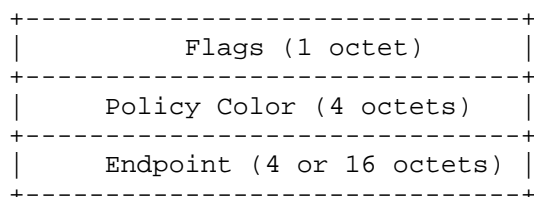


Figure 2: Format of Value Field in Redirect to SR policy Action

Where:

Flags (1 octet): Currently, only two bits are defined: the S bit and the F bit. The other bits are reserved. The S bit and the F bit are used to indicate the type of Endpoint, as shown in Figure 3.

Policy Color (4 octets): The color value of the SR policy [RFC9256] to which traffic is to be directed.

Endpoint (4 or 16 octets): The endpoint of the SR policy [RFC9256] to which traffic is to be directed. When the SR policy's endpoint is represented by an IPv6 address, the Endpoint field is 16 bytes in length, and the S bit in the flags field is set to 1. When the SR policy's endpoint is represented by an IPv4 address, the Endpoint field is 4 bytes in length, and the F bit in the flags field is set to 1.

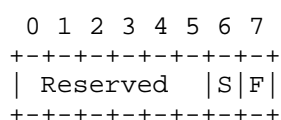


Figure 3: Format of Flags Field

Where:

S Flag (1 bit): Means Six. It indicates that the endpoint is represented by an IPv6 address When it is set to 1.

F Flag (1 bit): Means Four. It indicates that the endpoint is represented by an IPv4 address When it is set to 1.

Reserved (6 bits): These bits are reserved for future use. They are set to 0 when sending and ignored when receiving.

The S bit and F bit can only have one bit set to 1.

## 2.2. SRv6 SID Action

In some scenarios, when redirecting specific traffic to a SR Policy for forwarding, the headend node also needs to encapsulate an additional SRv6 SID. For example, when the last SID of the SR policy path is not USD (Ultimate Segment Decapsulation) flavored [RFC8986], the additional SRv6 SID encapsulated by the headend node is used to instruct the endpoint to decapsulate the outer packet header. To meet this requirement, we define a second new action for the FSv2 protocol, the SRv6 SID Action. This action is used in conjunction with the Redirect to SR Policy Action when necessary. It should be noted that the Redirect to SR Policy Action can be used independently, and the SRv6 SID Action can also be combined with other actions defined in FSv2.

The newly defined SRv6 SID Action in this document is represented using an action-SubTLV (format shown in Figure 1).

Where:

SubTLV Type (2 octet): Used to indicate that this action-SubTLV is a SRv6 SID Action SubTLV. Its value is requested to be assigned by IANA.

Length (2 octet): Measured in byte, used to indicate the total length of the SRv6 SID Action.

Value (variable): Used to carry the specific SRv6 SID information. Its format is shown in Figure 4.

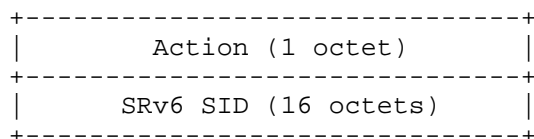


Figure 4: Format of Value Field in SRv6 SID Action

Where:

Action (1 octet): Only the value of 1 is defined. A value of 1 represents encapsulation, indicating that the headend node will encapsulate an additional SRv6 SID when performing the redirect action. The other 255 possible values are reserved for future extensions.

SRv6 SID (16 octets): The value represents a specific SRv6 SID, which can be an SRv6 SID type defined in [RFC8956], such as DT4, DT6, DT46, etc., or END SID with USD flavor.

### 3. Application Scenario

The headend node is enhanced to support the protocol extension defined in this document, being able to receive and parse the extended BGP FSv2 policies and perform the corresponding actions according to the newly defined actions. Specifically, when the headend node receives a policy containing a Redirect to SR policy Action issued through the extended FSv2 protocol, it configures the corresponding policy. Upon receiving traffic matching the policy, the headend node forwards the matching traffic to the corresponding SR Policy as required by the policy, i.e., encapsulates the traffic in SR and forwards the encapsulated traffic to the corresponding forwarding node via the interface specified by the policy. If the policy received by the headend node, issued through the extended FSv2 protocol, contains both Redirect to SR policy Action and SRv6 SID Action, the headend node configures the policy accordingly. Upon receiving traffic matching the policy, the headend node performs both the redirection to the SR policy and the action specified by the SRv6 SID action, such as further encapsulating the SRv6 SID carried in the SRv6 SID action.

The forwarding node forwards the packet based on the header information upon receiving the packet. This document does not introduce any new requirements or extensions for the forwarding node.

When the traffic reaches the endpoint node, the endpoint node processes and forwards the packet based on the header information of the received packet. This document does not introduce any new requirements or extensions for the endpoint node. Even if the received packet contains an SRv6 SID that was additionally encapsulated by the headend node according to the SRv6 SID Action, the endpoint node will perform the corresponding operations as indicated by the SRv6 SID, such as removing the SRv6 Policy encapsulation (decapsulating the outer IPv6 header), looking up in the routing table for the destination address of the inner packet header, and forwarding it accordingly. These are all normal processing procedures for the endpoint node, which is unaware that the SID it is processing was additionally encapsulated by the headend

node according to the SRv6 SID Action. In summary, this document does not introduce any new requirements or extensions for the endpoint node.

#### 4. IANA Considerations

IANA is requested to assign the following code points from the "BGP FSv2 Action types" Registry:

Code Point	Description	Reference
TBD1	Redirect to SR policy Action	This document
TBD2	SRv6 SID Action	This document

Table 1: Code Point for the Actions

#### 5. Security Considerations

TBD

#### 6. References

##### 6.1. Normative References

[I-D.ietf-idr-flowspec-v2]

Hares, S., Eastlake, D. E., Yadlapalli, C., and S. Maduschke, "BGP Flow Specification Version 2", Work in Progress, Internet-Draft, draft-ietf-idr-flowspec-v2-04, 28 April 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-idr-flowspec-v2-04>>.

[I-D.ietf-idr-wide-bgp-communities]

Raszuk, R., Haas, J., Lange, A., Decraene, B., Amante, S., and P. Jakma, "BGP Community Container Attribute", Work in Progress, Internet-Draft, draft-ietf-idr-wide-bgp-communities-12, 17 March 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-idr-wide-bgp-communities-12>>.

[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>>.

- [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>>.

## 6.2. Informative References

- [I-D.ietf-idr-flowspec-redirect-ip]  
Uttaro, J., Haas, J., akarch@cisco.com, Ray, S., Mohapatra, P., Henderickx, W., Simpson, A., and M. Texier, "BGP Flow-Spec Redirect-to-IP Action", Work in Progress, Internet-Draft, draft-ietf-idr-flowspec-redirect-ip-03, 8 September 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-idr-flowspec-redirect-ip-03>>.
- [I-D.ietf-idr-ts-flowspec-srv6-policy]  
Wenying, J., Liu, Y., Zhuang, S., Mishra, G. S., and S. Chen, "Traffic Steering using BGP FlowSpec with SR Policy", Work in Progress, Internet-Draft, draft-ietf-idr-ts-flowspec-srv6-policy-05, 6 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-idr-ts-flowspec-srv6-policy-05>>.
- [I-D.ietf0-idr-srv6-flowspec-path-redirect]  
Van de Velde, G., Patel, K., Li, Z., and H. Chen, "Flowspec Indirection-id Redirect for SRv6", Work in Progress, Internet-Draft, draft-ietf0-idr-srv6-flowspec-path-redirect-12, 21 October 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf0-idr-srv6-flowspec-path-redirect-12>>.
- [RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <<https://www.rfc-editor.org/info/rfc4360>>.
- [RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <<https://www.rfc-editor.org/info/rfc4760>>.
- [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>>.

- [RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <<https://www.rfc-editor.org/info/rfc8986>>.
- [RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <<https://www.rfc-editor.org/info/rfc9256>>.

#### Acknowledgements

The authors would like to express their gratitude for the review and contributions from Cheng Chang and Bo Liu.

Zheng Zhang provides valueable comments to this document.

#### Authors' Addresses

Zhenqiang Li (editor)  
China Mobile  
29 Finance Avenue, Xicheng District  
Beijing  
China  
Email: [lizhenqiang@chinamobile.com](mailto:lizhenqiang@chinamobile.com)

Song Liu (editor)  
China Mobile  
10 Manbai Road, Changping District  
BeiJing  
China  
Email: [liusongwl@chinamobile.com](mailto:liusongwl@chinamobile.com)