OPSAWG
Internet-Draft
Intended status: Standards Track
Expires: 28 August 2026

C. Lin
New H3C Technologies
Z. Li
China Mobile

24 February 2026

Export of Segment Routing Policy Attributes in IP Flow Information Export (IPFIX)

draft-lin-opsawg-ipfix-sr-policy-00

Abstract

This document defines new IP Flow Information Export (IPFIX) Information Elements (IEs) to export attributes of Segment Routing (SR) and Segment Routing over IPv6 (SRv6) policies applied to IP flows, which enables correlation between observed traffic flows and the SR/SRv6 policies that carry them.

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 28 August 2026.

Table of Contents

1. Introduction

Segment Routing (SR) [RFC8402] and Segment Routing over IPv6 (SRv6) [RFC8986] have become widely deployed technologies for source routing and traffic engineering in modern networks. SR Policy [RFC9256] provides a mechanism to steer traffic through an ordered list of segments to meet Service Level Agreements (SLAs) and other operational requirements.

An SR Policy is uniquely identified by the tuple <Headend, Color, Endpoint>, where:

* Headend: The node where the policy is instantiated.

* Color: A 32-bit numerical value representing the policy intent or class.

* Endpoint: The destination address of the policy (IPv4 or IPv6).

While network operators can monitor traffic flows using IP Flow Information Export (IPFIX) [RFC7011] and observe which SR policies are configured in the network, there has been no standardized way to correlate individual IP flows with the specific SR policies that carry them. This correlation is essential for:

* Service Assurance: Verifying that traffic is being forwarded according to the intended policy.

* Troubleshooting: Identifying which flows are affected when a policy fails.

* Routing Planning: Understanding traffic forwarding patterns per policy class.

* Security Monitoring: Detecting policy bypass or hijacking attempts.

This document defines new IPFIX Information Elements (IEs) to export SR and SRv6 policy attributes (color, endpoint, and type) associated with observed IP flows. These IEs enable Exporting Processes to report which SR policy was applied to each flow, providing crucial visibility into the relationship between traffic and network policies.

2. Terminology

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.

This document makes use of the terms defined in [RFC7011], and [RFC8402].

The following terms are used as defined in [RFC7011]:

* IPFIX

* IPFIX Information Elements

The following terms are used as defined in [RFC8402]:

* Segment Routing (SR)

* SR-MPLS

* SRv6

3. IPFIX Information Elements for SR Policy Attributes

This section defines new IPFIX IEs for exporting SR Policy attributes.

srPolicyColor
: The color value of the SR Policy applied to the flow. The color is a 32-bit unsigned integer that identifies the intent or class of the SR Policy.

srPolicyEndpointIPv4
: The 32-bit IPv4 endpoint address of the SR Policy applied to the flow.

srPolicyEndpointIPv6
: The 128-bit IPv6 endpoint address of the SR Policy applied to the flow.

srPolicyType
: The type of SR Policy applied to the flow. It is used to distinguish between SR-MPLS and SRv6 policies.

4. Operational Considerations

For srPolicyColor IE, a value of 0 indicates that no SR Policy was applied to the flow (i.e., the flow was forwarded using conventional routing). Color values are locally significant to the headend node but are often coordinated network-wide to represent consistent service classes.

For srPolicyEndpointIPv4 and srPolicyEndpointIPv6 IE, A value of 0.0.0.0 for IPv4 address and ::0 for IPv6 address indicates that no SR Policy with an IPv4 or IPv6 endpoint was applied, or the endpoint is unknown. When these IEs is used with srPolicyColor IE, this pair uniquely identifies an SR Policy from the perspective of the headend node.

When multiple SR Policies could apply to a flow (e.g., through policy nesting), these IEs defined in this document SHOULD report the value of the outermost or primary policy. These IEs are most meaningfully reported by the headend node of the SR Policy - that is, the node where the policy is instantiated and where packets enter the SR Policy path. To identify the headend node of an SR Policy, the exporterIPv4Address (130) and exporterIPv6Address (131) IEs can be used.

These IEs about SR Policy attributes complement existing IPFIX IEs. When reporting SR Policy attributes, Exporting Processes SHOULD also include basic flow identification IEs such as source/destination addresses, protocol, and ports to provide context for the policy application.

5. Security Considerations

The Security Considerations for IPFIX [RFC7011] apply to this document as well.

SR Policy attributes reveal network engineering decisions and traffic steering policies. Unauthorized access to this information could aid in traffic analysis or network reconnaissance. Export of these IEs SHOULD be protected using IPFIX over TLS [RFC7011] or DTLS [RFC9147].

Manipulation of SR Policy attributes in flow records could mislead network operators about traffic paths, potentially hiding policy violations or attacks. Collecting Processes SHOULD verify data integrity when possible.

While SR Policy attributes themselves don’t directly identify individuals, they could be combined with other flow data to infer sensitive information about network usage patterns.

Exporting additional IEs increases the size of flow records and template definitions. Exporting Processes SHOULD implement appropriate rate limiting and resource controls.

The ability to correlate flows with policies enables verification that traffic is following intended paths, which can help detect policy bypass attacks or configuration errors.

6. IANA Considerations

6.1. New IPFIX IEs for SR Policy Attributes

This document specifies new IPFIX IEs to enable export of SR Policy Attributes along with other flow information. This document requests IANA to add these IPFIX IEs to the "IPFIX Information Elements" registry available at [IANA-IPFIX].

Table 1 lists the new IPFIX IEs for SR Policy Attributes:

Element ID	Name	Reference
TBD1	srPolicyColor	This document
TBD2	srPolicyEndpointIPv4	This document
TBD3	srPolicyEndpointIPv6	This document
TBD4	srPolicyType	This document

Table 1: New IEs in the "IPFIX Information Elements" Registry

6.1.1. srPolicyColor

Name: srPolicyColor

Element ID: TBD1

Description: The color value of the SR Policy applied to the flow. The color is a 32-bit unsigned integer that identifies the intent or class of the SR Policy. A value of 0 indicates that no SR Policy was applied to the flow.

Abstract Data Type: unsigned32

Data Type Semantics: identifier

Status: current

Reference: [this document]

6.1.2. srPolicyEndpointIPv4

Name: srPolicyEndpointIPv4

Element ID: TBD2

Description: The IPv4 endpoint address of the Segment Routing Policy applied to the flow. A value of 0.0.0.0 indicates that no SR Policy with an IPv4 endpoint was applied, or the endpoint is unknown.

Abstract Data Type: ipv4Address

Data Type Semantics: identifier

Status: current

Reference: [this document]

6.1.3. srPolicyEndpointIPv6

Name: srPolicyEndpointIPv6

Element ID: TBD3

Description: The IPv6 endpoint address of the Segment Routing Policy applied to the flow. The ::0 address indicates that no SR Policy with an IPv6 endpoint was applied, or the endpoint is unknown.

Abstract Data Type: ipv6Address

Data Type Semantics: identifier

Status: current

Reference: [this document]

6.1.4. srPolicyType

Name: srPolicyType

Element ID: TBD4

Description: The type of Segment Routing Policy applied to the flow. A value of 0 indicates the policy type is unknown or not applicable. Values are defined in the "SR Policy Types" sub-registry

Abstract Data Type: unsigned8

Data Type Semantics: identifier

Status: current

Reference: [this document]

6.2. IPFIX Sub-Registry for SR Policy Types

IANA is requested to create a new sub-registry titled "SR Policy Types" under the "IPFIX Information Elements" registry.

Value	Description	Reference
0	Unknown or unspecified policy type	This document
1	SR-MPLS policy	This document
2	SRv6 policy	This document
255	Reserved for experimentation	This document

Table 2: SR Policy Types Sub-Registry

7. References

7.1. Normative References

[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>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[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>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[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>.

7.2. Informative References

[IANA-IPFIX] "IP Flow Information Export (IPFIX) Entities", n.d., <https://www.iana.org/assignments/ipfix/ipfix.xhtml>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/info/rfc9147>.

Authors' Addresses

Changwang Lin
New H3C Technologies
Beijing
China
Email: linchangwang.04414@h3c.com

Zhenqiang Li
China Mobile
29 Finance Avenue, Xicheng District
Beijing
China
Email: lizhenqiang@chinamobile.com