SPRING
Internet-Draft
Intended status: Informational
Expires: 20 September 2026

F. Yang
China Mobile
C. Lin
New H3C Technologies

19 March 2026

SID as source address in SRv6
draft-yang-spring-sid-as-source-address-10

Abstract

SRv6 is being rapidly deployed and is currently primarily used in trusted-domain backbone networks. Both the carrier market and the enterprise market are adopting SRv6 for end-to-end service delivery. However, if a firewall exists along an SRv6 path, legitimate SRv6 traffic will be dropped. This proposal addresses this issue by using SID as source address in SRv6 packets.

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 20 September 2026.

Copyright Notice

Table of Contents

1. Introduction

SRv6 is being rapidly deployed and is currently primarily used in trusted-domain backbone networks. Both the carrier market and the enterprise market are adopting SRv6 for end-to-end service delivery. However, if a firewall exists along an SRv6 path, legitimate SRv6 traffic will be dropped. This proposal addresses this issue by using SID as source address in SRv6 packets.

The reason has been elaborated in Section 8.1 of [I-D.draft-ietf-spring-srv6-security]. In brief, SRv6 using loopback as source address will cause asymmetric address, which will be blocked by the firewall. As a result, users are forced to encapsulate traffic with multiple layers of tunnel headers— such as IPSec or L2TP— to ensure it can pass through the firewall. This approach introduces two significant issues: first, it increases overhead— for example, IPSec adds approximately 80 bytes of header overhead; second, it undermines the programmability benefits of SRv6, as forwarding is performed based on IPSec rather than SRv6 itself.

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.

1.2. Terminology

AC: attachment circuit

PE: Provider Edge.

SID: Segment Identifier, defined in [RFC8402].

SRv6: SR over IPv6, defined in [RFC8402].

VPLS: Virtual Private LAN Service.

VPWS: Virtual Private Wire Service.

VPN: Virtual Private Network.

2. Using SRv6 SID as Source Address

Only unicast traffics are eligible for using SID as source address. There are a bunch of SRv6 services specified in [RFC8986], and those End.DT* and End.DX* SIDs are locally allocated and associated SRv6 tunnel operation. All those End.DX* and End.DT* SIDs except End.DT2M SHOULD be used for source address. Put it simple, it SHOULD consider using SID as source address for IPinIP, L3VPN, VPWS, VPLS and EVPN services.

2.1. User Traffic

AC is associated with an SRv6 service, and the SID of that SRv6 service is locally allocated by the PE. Therefore, the traffic received from an AC can always be unambiguously associated with a specific local SRv6 service SID. In other words, the SRv6 service SID to be populated as source address can be naturally determined during the forwarding process.

2.2. Control Traffic

Control traffic will not be terminated by VPN, thus will not be impacted.

2.3. OAM Traffic

OAM traffic terminated by the SRv6 tunnel SHOULD use the SRv6 SID as source address, such as ping, trace. Refer to RFC 8986 4.1.1, Allowing the processing of specific Upper-Layer header types is useful for Operations, Administration, and Maintenance (OAM). As an example, an operator might permit pinging of SIDs. To do this, they may enable permission of Upper-Layer header type 58(ICMPv6).

2.4. Management Traffic

Management traffic will not be terminated by VPN, thus SHOULD not be impacted.

3. Use Cases

3.1. SRv6 Network with SR-aware Stateful Firewall

3.1.1. Problem Statement

To provide VPN service in an SRv6 network [RFC9252], the ingress PE encapsulates the payload in an outer IPv6 header with the Segment Routing Header (SRH) [RFC8754] carrying the SR Policy segment list along with the VPN Service SID. If the VPN service is with best-effort connectivity, the destination address of the outer IPv6 header carries the VPN service SID and the SRH is omitted.

Along the forwarding path in the SRv6 network, firewalls may be deployed to filter the traffics. If a firewall is SR-aware, it will retrieve the final destination of an SRv6 packet from the last entry in the SRH rather than the destination address field of the IPv6 header [I-D.draft-ietf-spring-sr-service-programming].

A stateful firewall keeps a track of the state of the network connections traveling across it. Whenever a packet arrives to seek permission to pass through it, the firewall checks from its state table if there is an active connection between identified by 3 tuple or 5 tuple. Thus only legitimate packets are allowed to be transmitted across it.

Figure 1 and Figure 2 show the bidirectional VPN traffic packets passing through a firewall in an SRv6 network.

The source address of the outer IPv6 header is the IPv6 address of ingress PE. The final destination address of the outer IPv6 header is the VPN Service SID of egress PE. In the SR-Policy-based way, the final destination address is encapsulated in the last entry in the SRH, Segment[0]. In the best-effort way, the SRH is omitted.

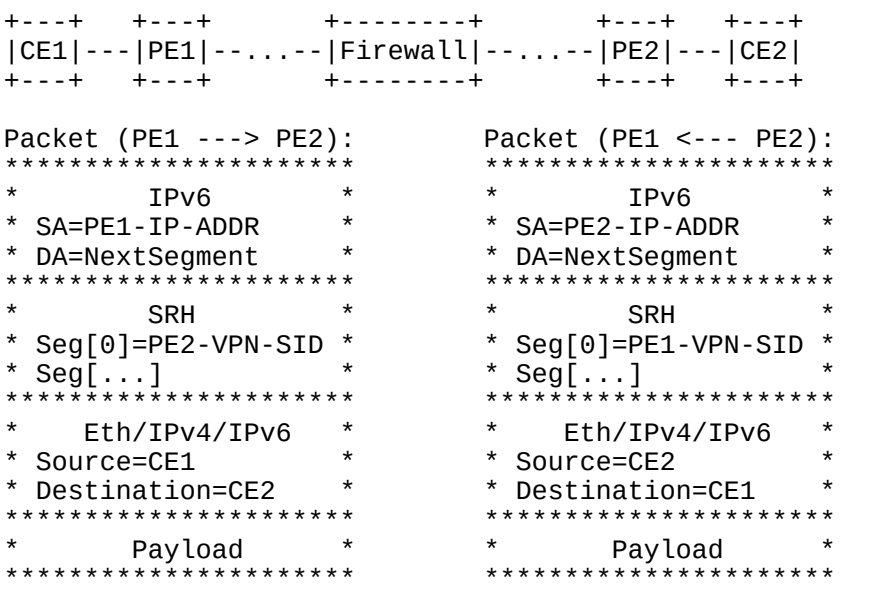


Figure 1: SR-Policy-based VPN Traffic across Firewall

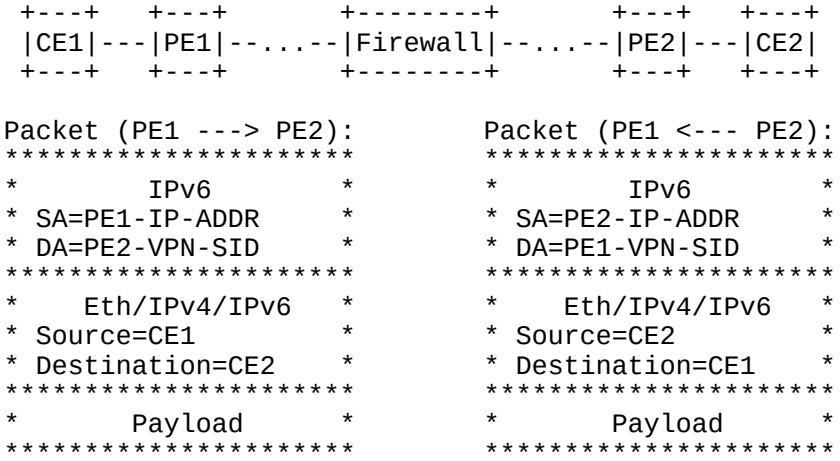


Figure 2: Best-Effort VPN Traffic across Firewall

The stateful firewall will check the association relationships of the bidirectional VPN traffic packets. A common implementation may record the key information of the packets on forward way(internal to external), such as source address and destination address. When receiving a packet on backward way(external to internal), it checks the state table if there is an existing forward packet flow. For example, the firewall may require that the source address of packet on backward way matches the destination address of packet on forward way, and destination address will be checked in the similar way. If not matched, the packet on the backward path will be regarded as illegal and thus dropped.

An SR-aware firewall is able to retrieve the final destination of an SRv6 packet from the last entry in the SRH. The <source, destination> tuple of the packet from PE1 to PE2 is <PE1-IP-ADDR, PE2-VPN-SID>, and the other direction is <PE2-IP-ADDR, PE1-VPN-SID>. However, the source address of the outer IPv6 packet is usually a loopback interface of the ingress PE. Eventually, the source address and destination address of the forward and backward VPN traffic are regarded as different flow, and they may be blocked by the firewall.

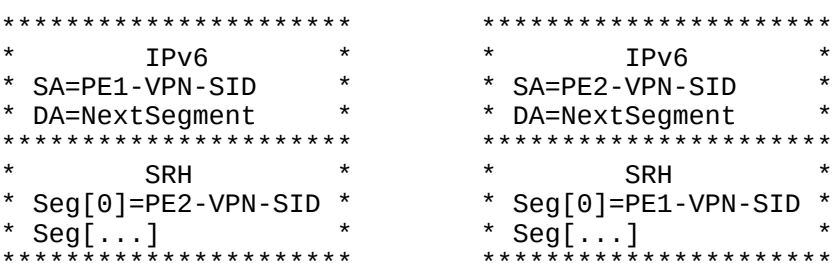
3.1.2. Solution for SRv6 Traffic Pass Thru SR-aware Stateful Firewall

In the SRv6-based VPN service, the final destination of the outer IPv6 header is the VPN-SID of the egress PE, which is associated with that VPN service. But the source address of the outer IPv6 header is usually unrelated to the VPN service. So, it can be difficult for a stateful firewall to establish the association relationship between the bidirectional traffic flows.

The proposed solution is to unify the semantic of the source and destination address thus ensure the symmetry of the bidirectional flow.

When an ingress PE receives the client packet from CE, it checks which L3 VPN service it belongs to, and uses the VPN-SID associated with that L3 VPN service as the source address when encapsulating the outer IPv6 header with the optional SRH.

Outer IPv6 Header of SR-Policy-based VPN Traffic:



Outer IPv6 Header of Best-effort VPN Traffic:

Figure 3: Outer IPv6 Header in the Proposed Solution

According to [RFC8402] and [RFC8986], an SRv6 VPN Service SID is an IPv6 address, and it is routable by its Locator prefix in the SRv6 network. In the proposed solution, when an SRv6 VPN Service SID is used as the source address of the outer IPv6 header in the SRv6 network, it is treated as a normal IPv6 address and does not perform any special behavior.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

TBD.

6. References

6.1. Normative References

[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/rfc/rfc8402>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/rfc/rfc8754>.

[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/rfc/rfc8986>.

[RFC9252] Dawra, G., Ed., Talaulikar, K., Ed., Raszuk, R., Decraene, B., Zhuang, S., and J. Rabadan, "BGP Overlay Services Based on Segment Routing over IPv6 (SRv6)", RFC 9252, DOI 10.17487/RFC9252, July 2022, <https://www.rfc-editor.org/rfc/rfc9252>.

[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/rfc/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/rfc/rfc8174>.

6.2. Informative References

[I-D.draft-ietf-spring-sr-service-programming] Abdelsalam, A., Xu, X., Filsfils, C., Bernier, D., Li, C., Decraene, B., Ma, S., Yadlapalli, C., Henderickx, W., and S. Salsano, "Service Programming with Segment Routing", Work in Progress, Internet-Draft, draft-ietf-spring-sr-service-programming-12, 3 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-service-programming-12>.

[I-D.draft-ietf-spring-srv6-security] Buraglio, N., Mizrahi, T., tongtian124, Contreras, L. M., and F. Gont, "Segment Routing IPv6 Security Considerations", Work in Progress, Internet-Draft, draft-

ietf-spring-srv6-security-11, 2 February 2026,
<https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-security-11>.

Authors' Addresses

Feng Yang
China Mobile
China
Email: yangfeng@chinamobile.com

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