Network Working Group
Internet-Draft
Intended status: Informational
Expires: 18 September 2026

H. Wang
Huawei
L. Dunbar
Futurewei
J. Hu
Y. Xu
Huawei

17 March 2026

ESP Protection for Services over SRv6
draft-wdh-srv6ops-secservice-02

Abstract

This document describes a mechanism for protecting selected service traffic using IPsec ESP while transporting the traffic over an SRv6 domain. The approach enables service payloads to be encrypted prior to SRv6 encapsulation, allowing the SRv6 header to remain visible for segment-based forwarding within the provider network. This mechanism supports services or applications that require additional confidentiality and integrity protection, even when carried over an operator-managed SRv6 domain.

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 RFC 2119 [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 18 September 2026.

Table of Contents

1. Introduction

Segment Routing over IPv6 (SRv6) [RFC8986] is widely deployed within service provider networks to steer traffic across an operator controlled infrastructure. In many deployments, the SRv6 domain is considered operationally secure, and service traffic is transported without additional encryption inside the provider network. However, certain services, such as regulated workloads or sensitive application traffic, may require an additional layer of confidentiality and integrity protection, even when traversing a trusted SRv6 domain

This document describes a mechanism to provide optional IPsec based protection for selected services carried over an SRv6 network. The objective is to allow a subset of services to be encrypted using ESP while preserving SRv6 forwarding semantics. In this approach, the Segment Routing Header (SRH) remains visible to intermediate nodes for path steering, while the service payload is protected by ESP.

This mechanism does not alter SRv6 forwarding behavior. It augments SRv6 service transport by enabling additional security for selected services, while allowing other services to continue using standard SRv6 encapsulation without encryption.

2. Terminology

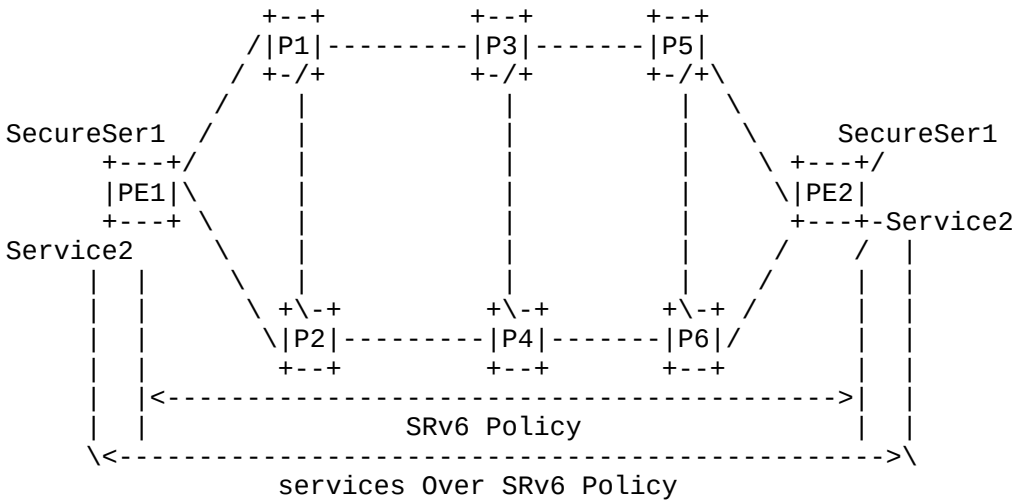
SRv6: Segment Routing over IPv6

ESP: Encapsulating Security Payload

IPsec: Internet Protocol Security

SA: Security Association

3. Scenarios



SecureSer: Secure-Service

As illustrated in the figure above, traffic between PE1 and PE2 traverses the provider backbone and is steered according to an SRv6 policy. The SRv6 policy determines the explicit forwarding path across the core network in order to meet service-level objectives such as performance and resiliency.

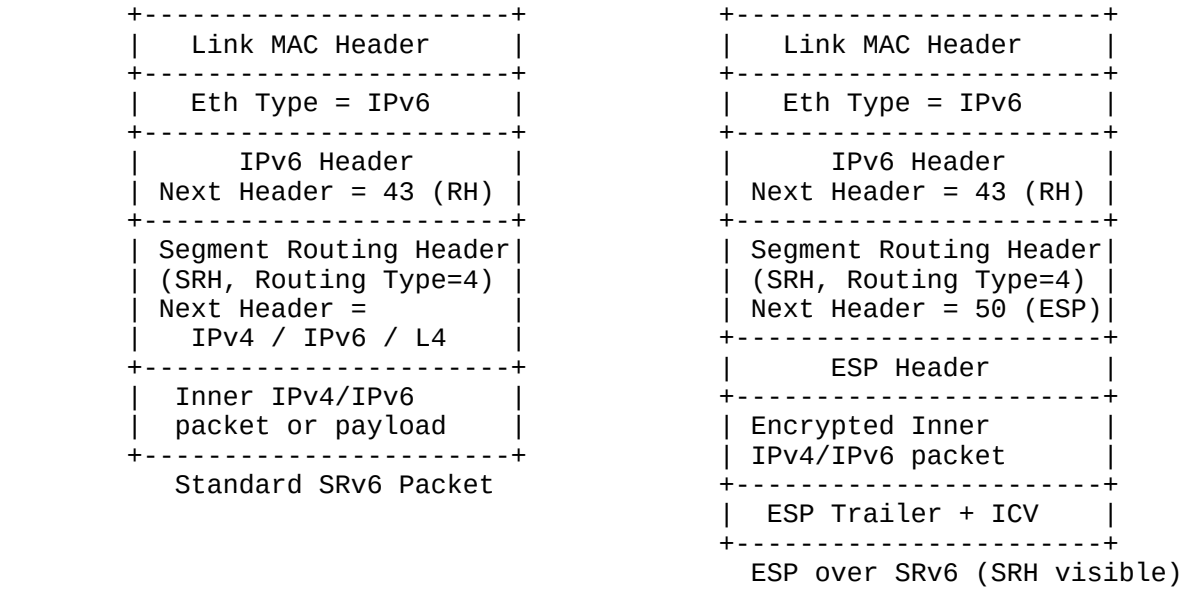
Secure-Service-1 has confidentiality requirements that mandate additional data-plane protection. Accordingly, its packets are protected using ESP prior to being forwarded along the SRv6 policy path. The SRv6 header remains visible to intermediate nodes for segment based forwarding, while the service payload is encrypted to provide confidentiality and integrity across the backbone.

In contrast, Service2 represents regular service traffic that does not require additional protection and is transported using standard SRv6 encapsulation without ESP.

4. Packet Header for Encrypted Payload via SRv6

The SRv6 header [RFC8754] is placed outside the IPsec ESP [RFC4303] encrypted payload to preserve normal SRv6 forwarding behavior within the domain. The Segment Routing Header (SRH) contains the segment list and associated routing information that must remain visible to intermediate nodes in order to enable segment-based forwarding. By keeping the SRH unencrypted, SRv6-capable devices can process the Routing Type 4 header and apply the appropriate forwarding actions. At the same time, ESP protects the inner service payload, providing confidentiality and integrity without interfering with SRv6 path steering. This layering ensures that routing functions and payload protection operate independently and consistently within the SRv6 domain.

The following figure shows the encapsulated packet format:



5. Gap Analysis of the Existing Soluitons

The BGP Tunnel Encapsulation Attribute defined in [RFC9012] allows service routes to carry information about the tunnels that can be used to transport them. However, [RFC9012] does not define how IPsec ESP can be integrated with SRv6 service delivery, particularly when SRv6 policies are used for path steering. Specifically, it does not describe a mechanism for advertising both SRv6 SID information and the IPsec parameters required to protect selected services. As a result, additional specification is required to enable coordinated signaling of SRv6 and ESP-related attributes for a given service route.

The [I-D.ietf-bess-secure-evpn] document defines a method for distributing IPsec-related information for EVPN services using BGP. It introduces a new Tunnel Type, ESP-Transport, within the framework of [RFC9012]. In that approach, VXLAN remains the outer transport encapsulation, and ESP is applied to protect the VXLAN-encapsulated payload. While this model is appropriate for VXLAN-based deployments, it does not directly address SRv6-based service transport. In an SRv6 domain, the Segment Routing Header (SRH) must remain visible to intermediate nodes to enable segment-based forwarding. Encrypting an outer encapsulation in a manner that obscures SRv6 routing information would prevent proper SRv6 policy processing.

n addition, [I-D.ietf-idr-sdwan-edge-discovery] defines sub-TLVs for advertising IPsec-related attributes within the BGP Tunnel Encapsulation Attribute framework. These sub-TLVs provide a mechanism for distributing IPsec parameters associated with specific tunnel types and may be applicable to secure service transport beyond SD-WAN environments. However, the SD-WAN draft primarily associates those IPsec sub-TLVs with SD-WAN tunnel types and hybrid underlay constructs. It does not define a tunnel type or signaling semantics for the case where ESP protection is applied in conjunction with SRv6 encapsulation. In particular, it does not specify how IPsec parameters and SRv6 SID information are to be jointly interpreted when the SRv6 header remains outside the encrypted payload. As a result, while the existing IPsec sub-TLVs could be reused, a clear tunnel type definition and associated processing rules are required to support ESP-protected services transported over an SRv6 policy.

Therefore, a Tunnel Type is required to explicitly indicate that a service route is to be transported over an SRv6 policy while being protected by ESP. Such a definition would clarify the processing semantics when SRv6 encapsulation and IPsec parameters are jointly signaled using the BGP Tunnel Encapsulation Attribute. In particular, it would specify that the SRv6 header remains outside the encrypted payload for forwarding purposes, while the inner service payload is protected by ESP. This preserves SRv6 path steering behavior and ensures consistent interpretation of IPsec-related sub-TLVs when applied to SRv6-based service transport.

6. ESP-Protected-Payload Tunnel Type

This document defines a new Tunnel Type, ESP-Protected-Payload, within the BGP Tunnel Encapsulation Attribute framework specified in [RFC9012]. The ESP-Protected-Payload Tunnel Type, with its value being 28 assigned by IANA, indicates that the service payload is to be protected using IPsec ESP, while being transported over an outer encapsulation such as SRv6. The SRv6 header remains outside the encrypted payload to preserve normal segment-based forwarding behavior within the SRv6 domain.

The IPsec-related sub-TLVs defined in [I-D.ietf-idr-sdwan-edge-discovery], including the IPsec SA Nonce, IPsec Public Key, and IPsec SA Proposal sub-TLVs, MAY be carried under the ESP-Protected-Payload Tunnel Type. These sub-TLVs provide the necessary parameters for establishing ESP protection for the service. This document reuses those sub-TLV definitions without modification, and defines their interpretation when applied to SRv6-based service transport.

When a service route carries additional attributes, such as a color and SRv6 SID information, route resolution is performed according to the local tunnel policy. The service route is resolved to the appropriate SRv6 Provider Edge (PE) or SRv6 Policy based on the color value or as explicitly indicated by the Tunnel Encapsulation Extended Community. The ESP-Protected-Payload Tunnel Type applies to the selected SRv6 transport, indicating that the inner service payload MUST be protected by ESP prior to transmission over the resolved SRv6 policy.

7. Process Illustration

Let’s take the scenario described in section 3 as an example. The following steps illustration the procedure:

1. PE1 obtains IPSec related parameters by configuration, from its management system, or via negotiation, including IPsec SA encryption algorithms, keying material, nonce, and security policies, etc..

2. PE1 detects its attached VPN routes, such as EVPN Type 5 Prefix Routes or others.

3. PE1 adds a Tunnel-Encapsulation Attribute to the routes based on local policies. The Tunnel-Type parameter is ESP-Protected-Payload.

4. PE1 obtains the VPN route and carries tunnel information, such as the VPN SID and Color Extended Community, based on the local policy.

5. PE1 advertises the route to PE2 through RRs.

6. After receiving the route advertised by PE1, PE2 performs IPsec key negotiation based on the ESP-Protected-Payload Tunnel-Encapsulation Attribute carried in the route and indicates that the route needs to be encrypted using IPsec.

7. After PE2 receives the route advertised by PE1 and carries information such as the VPN ID and color, PE2 associates the route with the SRv6 tunnel.

8. When PE2 receives the CE-side traffic that matches the route advertised by PE1. PE2 performs IPsec encryption based on the indicated IPSec sub-TLVs advertised by PE1, encapsulates the traffic into an SRv6 tunnel based on the indicated tunnel information, and sends the traffic to PE1 along the tunnel information.

9. After receiving the traffic from PE2, PE1 finds the corresponding VRF based on the SRv6 tunnel information and decrypts the packets to obtain the original user packet payload. Searches the VRF table and forwards traffic to the CE based on the user packet header.

8. IANA Considerations

Tunnel-Type = 28: ESP-Protected-Payload which has been allocated by IANA.

9. Security Considerations

In this solution, selected service traffic is protected using IPsec ESP prior to transmission over the SRv6 domain. As a result, the inner service payload is encrypted and integrity-protected while traversing the provider backbone. Intermediate nodes that process the SRv6 header for forwarding purposes do not have visibility into the encrypted payload. This mechanism provides confidentiality and data integrity protection for services requiring enhanced security, such as those carrying sensitive or regulated traffic.

10. Acknowledgements

NA

11. Contributors

Yulin Shi
Huawei
Email: shiyulin@huawei.com

Xiangfeng Ding
Huawei
Email: dingxiangfeng@huawei.com

Shunwan Zhuang
Huawei
Email: zhuangshunwan@huawei.com

12. References

12.1. 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>.

12.2. References

[I-D.ietf-bess-secure-evpn]
Sajassi, A., Banerjee, A., Thoria, S., Carrel, D., Weis, B., and J. Drake, "Secure EVPN", Work in Progress, Internet-Draft, draft-ietf-bess-secure-evpn-02, 7 November 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-bess-secure-evpn-02>.

[I-D.ietf-idr-sdwan-edge-discovery]
Dunbar, L., Hares, S., Majumdar, K., Raszuk, R., and V. Kasiviswanathan, "BGP UPDATE for SD-WAN Edge Discovery", Work in Progress, Internet-Draft, draft-ietf-idr-sdwan-edge-discovery-26, 20 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-sdwan-edge-discovery-26>.

[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>.

[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/info/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/info/rfc8986>.

[RFC9012] Patel, K., Van de Velde, G., Sangli, S., and J. Scudder, "The BGP Tunnel Encapsulation Attribute", RFC 9012, DOI 10.17487/RFC9012, April 2021, <https://www.rfc-editor.org/info/rfc9012>.

Authors' Addresses

Haibo Wang
Huawei
Beijing
P.R. China
Email: rainsword.wang@huawei.com

Linda Dunbar
Futurewei
Email: ldunbar@futurewei.com

Junli
Huawei
Beijing
P.R. China
Email: hujunli@huawei.com

YaoYang
Huawei
Beijing
P.R. China
Email: xuyaoyang@huawei.com