Network Working Group
Internet Draft
Intended status: Informational
Expires: June 22, 2024

C. Lin
New H3C Technologies
C.Zhou
China Mobile
M. Chen
New H3C Technologies
December 22, 2023

Considerations for SRv6 across Untrusted Domain
draft-lin-spring-srv6-across-untrusted-domain-02

Abstract

Segment Routing operates within a trusted domain. There are some scenarios in which the whole SRv6 domain is separated by untrusted domain and SRv6 packets need to traverse it. This document describes some use cases of SRv6 across untrusted domain, and proposes a solution using IPSec technology.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on June 22, 2024.

Table of Contents

1. Introduction

Segment Routing (SR) [RFC8402] leverages the source routing paradigm. A node steers a packet through an SR Policy instantiated as an ordered list of instructions called "segments". Segment Routing (SR) can be applied to the IPv6 data plane using Segment Routing Header (SRH) [RFC8754], which is called SRv6.

Due to security concerns, [RFC8402] specifies that SR operates within a trusted domain and Traffic MUST be filtered at the domain boundaries. [RFC8754] describes the deployment model for securing the SRv6 domain:

- External Interface of each edge node: Any packet entering the SR domain and destined to a SID within the SR domain is dropped.

- Internal Interface of each node: Packets to SIDs from source addresses outside the SR domain are dropped.

There are some scenarios in which the whole SRv6 domain is separated by untrusted domain and SRv6 packets need to traverse it. As shown in Figure 1, Domain 1 and Domain 2 are operated by the same administrative entity, but they are connected by a network of

another operator. The two domains can trust each other and may be regarded as one large SRv6 domain. When traffics are forwarded from one of the SRv6 domain to another, SRH is carried in the packets and guides the forwarding path in both the two SRv6 domains. In the meantime, those SRv6 packets need to traverse the intermediate untrusted domain. The mechanism of SRv6 across untrusted domain should comply with the security deployment of SRv6 domain and reduce the risks introduced by the intermediate untrusted domain.

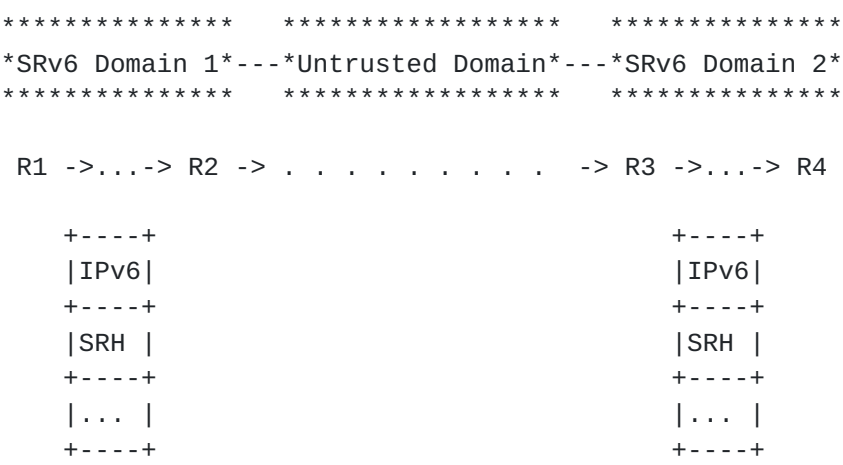

Figure 1: SRv6 across Untrusted Domain

This document describes some use cases of SRv6 across untrusted domain, and proposes a solution using IPSec technology.

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. Use Case

2.1. SRv6 Enterprise Network across Internet

In the enterprise network shown in Figure 2, the branch and center networks are SRv6 capable, but the intermediate network is Internet which is not trusted.

When the host H1 in enterprise branch needs to visit the server S4 in enterprise center, it sends IPv6 packet with SRH carrying SRv6 SIDS, including the SIDs for the forwarding path in the branch and the SIDs for the forwarding path in the center. After the packet is

forwarded to R2, it needs to traverse the Internet and reaches R3. Then it is forwarded from R3 to S4 by the instructions of remaining SRv6 SIDs in SRH.

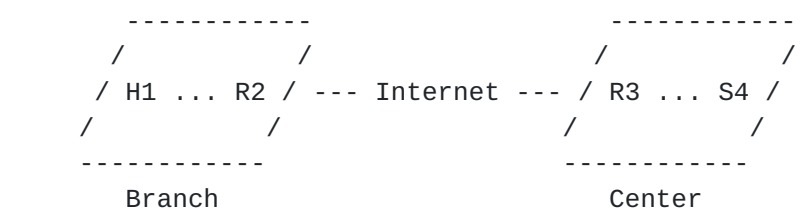

Figure 2: Enterprise Network across Internet

2.2. SRv6 SDWAN to Cloud DC across Third-party Provider

As shown in Figure 3, SRv6 SDWAN provides the connectivity to Cloud Data Center (DC). CPE1 is directly connected to PE1, but CPE2 is connected to PE1 through a third-party ISP.

When a client needs to access the cloud service, CPE encapsulates the client packet with an outer IPv6 Header and SRH. The SRv6 SIDs in SRH may include the Binding SID of PE1, the SID of GW, and the Service SID of cloud service. Both CPE1 and CPE2 are trusted by the service provider, but the packet from CPE2 needs to traverse a third-party ISP which is not untrusted.

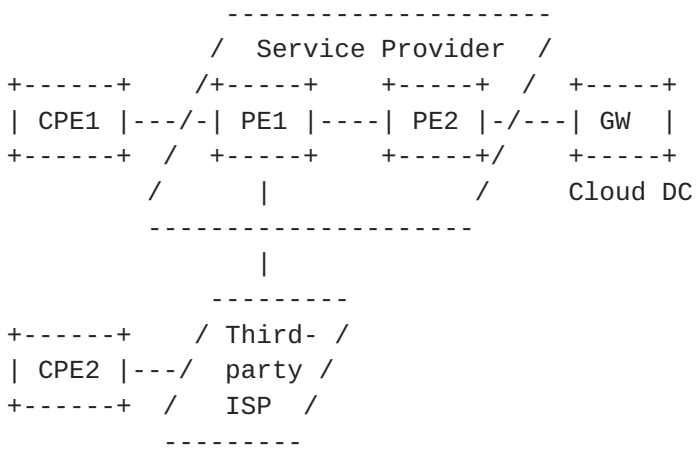

Figure 3: SDWAN to Cloud DC across Third-party Provider

3. Solution

This document proposes a solution for SRv6 across untrusted domain using IPSec technology [RFC4301]. The edge nodes of two separated SRv6 domains are interconnected by an IPSec tunnel. When an SRv6 packets traverse the untrusted domain, it is encapsulated in an

outer IPv6 Header along with AH and ESP, which is the tunnel mode of IPSec. The whole SRv6 packet is encrypted by the ESP. After the packet reaches the other SRv6 domain, the outer IPv6 Header is decapsulated and the inner SRv6 packet continues to be forwarded along the path instructed by the remaining SIDs in SRH.

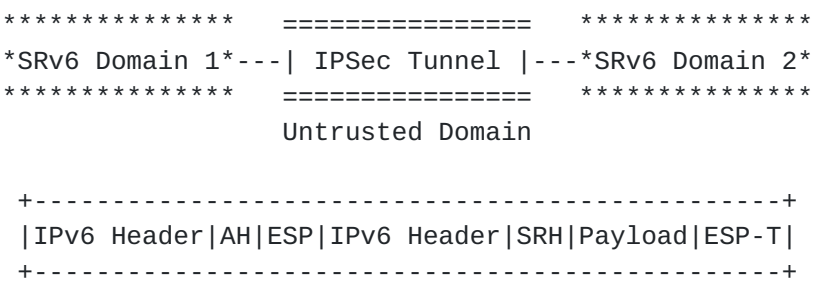

Figure 4: SRv6 over IPSec

The edge node of one SRv6 domain should steer the SRv6 packet towards the other SRv6 domain onto the IPSec tunnel. The steering methods may include, but not limited to, the following ones:

o Config static routes for the SIDs or the locator of the opposite edge node, with the next-hop heading to the IPSec tunnel.

o Allocate an End.X SID for the IPSec tunnel and include it into the SR Policy.

From the perspective of SRv6 domain, the interface facing the untrusted domain on the edge node is external interface. According to [RFC8754], any packet entering the SRv6 domain from the external interface and destined to a SID within the SRv6 domain will be dropped. When the edge node receives a packet from the IPSec tunnel, the destination of the outer IPv6 Header is its tunnel address, not a SID. So, the proposed solution complies with the security deployment of SRv6 domain. In addition, the SRH of inner packet is encrypted by the ESP, hence the source-routing information is not exposed when the packet traverses the untrusted domain, which can reduce the risks introduced by the intermediate untrusted domain.

Note that the security of the proposed solution relies on the IPSec mechanism. If the IPSec tunnel is hacked, the SRv6 domain may be exposed to attacks.

4. Security Considerations

TBD.

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017

[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>.

Authors' Addresses

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

Ce Zhou
China Mobile
China
zhouce@gd.chinamobile.com

Mengxiao Chen
New H3C Technologies
China
Email: chen.mengxiao@h3c.com