SAVNET Working Group
Internet-Draft
Intended status: Standards Track
Expires: 4 June 2026

X. Li
A. Wang
China Telecom

1 December 2025

Segment Routing Policy-Based Source Address Validation (SAV) Mechanism
draft-li-savnet-srsav-02

Abstract

This draft proposes a novel mechanism for Source Address Validation (SAV) message propagation based on Segment Routing policies (SR-policy). Traditional SAV mechanisms often rely on routing tables (RIB) and Policy-Based Routing (PBR), but these methods lack the flexibility and granularity needed for some network environments. By leveraging the flexibility and control capabilities of SR-policy, the proposed mechanism ensures that SAV messages are propagated along well-defined paths, ensuring efficient, secure, and accurate source address validation.

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 June 2026.

Copyright Notice

Table of Contents

1. Introduction

In modern network environments, Source Address Validation (SAV) [SAVNET] mechanisms are critical for ensuring that data packets have legitimate source addresses. Traditional SAV mechanisms typically rely on routing tables (RIB) to control and generate strategies for verifying source addresses. However, these methods often lack flexibility and granular control. While Policy-Based Routing (PBR) [sav-ospf] improves upon these traditional methods by allowing for more customized routing policies, it still falls short in environments where Segment Routing (SR) [RFC8402] policies are employed. This is because SR-policy [RFC8987] allows traffic to be routed along pre-defined paths that may not align with traditional SAV control mechanisms, leading to potential failures in source address validation [SAV].

To address these challenges, this document proposes a novel mechanism for SAV message propagation based on Segment Routing policies (SR-policy). By utilizing the flexibility and control capabilities of SR-policy, we can define explicit paths for SAV messages, ensuring their efficient, secure, and accurate propagation through the network.

The mechanism involves generating SR-policies that specify explicit paths using Segment Identifiers (SIDs). These policies are then disseminated to key nodes within the network. The headend router parses the SR-policy, generates the SAV message, and forwards the SAV message along the specified paths. Routers along the path verify their role using the SID list, if they are key nodes, process the SAV message and create the SAV rule , and then propagate the message to nexthop.

2. Conventions used in this document

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 [RFC2119] [RFC8174].

3. Terminology

The following terms are used in this draft:

* Segment Identifier (SID): An identifier for each path segment used to guide traffic within the network.

* Segment List: An ordered list of SIDs that defines the path for traffic from the source to the destination.

* SR-policy: Segment Routing policy, A policy consisting of one or more Segment Lists, each representing an alternate path.

* FIB: Forwarding Information Base.

* RIB: Routing Information Base.

4. Problem Overview

One of the major challenges in network security is source address spoofing. Attackers can forge source IP addresses to inject malicious traffic or manipulate traffic paths, causing service disruption, data interception, or network resource exhaustion. Traditional intra-domain Source Address Validation (SAV) mechanisms face two main trends:

1. Strict Shortest Path Enforcement: SAV rules are applied strictly along the shortest path computed by IGP (e.g., OSPF/IS-IS), without considering policy-driven routing or dynamic path adjustments. This rigidity can block legitimate alternate paths required for resilience, traffic engineering, or load balancing. When a failure occurs, forcing traffic to follow a new path (e.g., R1 → R3 → R4 → R5 instead of R1 → R2 → R4 → R5), strict SAV enforcement on shortest paths can lead to unnecessary packet drops.

2. Fully Open Interface Policy: This approach removes strict SAV enforcement, allowing all interfaces to accept traffic without path verification. While it provides routing flexibility, it introduces severe security risks, allowing spoofed traffic and malicious injections into the network, undermining SAV’ s purpose.

In addition to the two trends above, different deployment strategies for SAV have been adopted, each with its own limitations:

1.Edge-Only SAV Deployment: SAV is only enforced at the network’s edge, assuming all traffic enters through designated border routers.

Limitations:

* Internal nodes may still propagate malicious traffic if they receive spoofed packets through unexpected routes.

* Failure-induced path changes may cause legitimate traffic to be dropped if edge-based SAV does not recognize the new valid path.

* Attackers can bypass SAV by encapsulating spoofed traffic in tunnels or leveraging alternate entry points.

2. Static Intra-Domain SAV Policies: Some deployments apply SAV within the network but rely on static configurations that do not adapt to topology changes.

Limitations:

* Changes in network topology (e.g., failures, rerouting) require manual intervention to update SAV rules.

* Static enforcement can result in unnecessary packet drops during reconvergence events.

Changes in network topology (e.g., failures, rerouting) require manual intervention to update SAV rules. Static enforcement can result in unnecessary packet drops during reconvergence events.

To address these limitations, we introduce a policy-driven on-demand SAV mechanism using SRv6-Policy:

* Dynamic Interface Control:

  - Interfaces remain closed by default, but SAV rules are dynamically adjusted based on SRv6-policy.

  - If a failure redirects traffic via an alternate path (e.g., R1 → R3 → R4 → R5), the SRv6 policy ensures that R4 dynamically opens the interface facing R3 to allow legitimate traffic.

* Security and Flexibility Balance:

  - Unlike strict shortest-path SAV, our method adapts to topology changes while maintaining security.

  - Unlike fully open interfaces, we only permit necessary paths based on policy enforcement.

Our approach bridges the gap between strict and fully open SAV policies by leveraging SRv6-policy-driven dynamic interface control. This ensures both security and adaptability, preventing spoofing attacks while allowing legitimate network adjustments. By integrating SAV with SRv6-policy, we create a flexible and resilient security model that evolves with network dynamics. The following content is a specific explanation of our approach.

5. The SAV Message Propagation based on SR-policy

In an SR-policy-configured network, SAV messages are propagated according to the paths defined by the SR-policy. Each router along the path uses the SID list specified in the SR-policy to forward SAV messages hop-by-hop.

Consider a network scenario where SR-policy is utilized for SAV message propagation. Take Figure 1 as an example. The network topology consists of several routers, with a source server (S1) sending traffic destined for a destination server (D1). The routers involved in the SR-policy path include R1, R2, R3, R5, and R7.

In this scenario, the SR-policy path for traffic from S1 to D1 is defined to go through R1, R2, R3, R5, and finally R7. The segment list for this SR-policy path includes the segment identifiers (SID) for each router along the path: SID1 for R1, SID2 for R2, SID3 for R3, SID5 for R5, and SID7 for R7.

When Router R1, the head-end router, receives traffic from the source prefix 10.1.1.0/24 destined for the destination prefix 10.7.0.0/16, it generates a SAV message based on the SR-policy. This SAV message includes the source router (R1), the neighbor router (R2), the source prefix (10.1.1.0/24), and the segment list [SID1, SID2, SID3, SID5, SID7].

R1 forwards the SAV message to R2. Upon receiving it, R2 processes the message and designates the interface that received it from R1 as valid for traffic from the source prefix 10.1.1.0/24, creating the SAV rules. After checking the SID list, R2 forwards the message to R3. Similarly, R3 processes the SAV message, designates the interface that received it from R2 as valid for the same source prefix, and creates the SAV rules. This process continues as R3 forwards the message to R5, with R5 designating the interface that received it from R3 as valid, creates the SAV rules.

Then R5 forwards the SAV message to R7. R7 designates the interface that received the message from R5 as valid. Finally, R7, recognizing itself as the destination router, processes the SAV message, creates the SAV rules, and designates its interface for traffic destined 10.1.1.0/24.

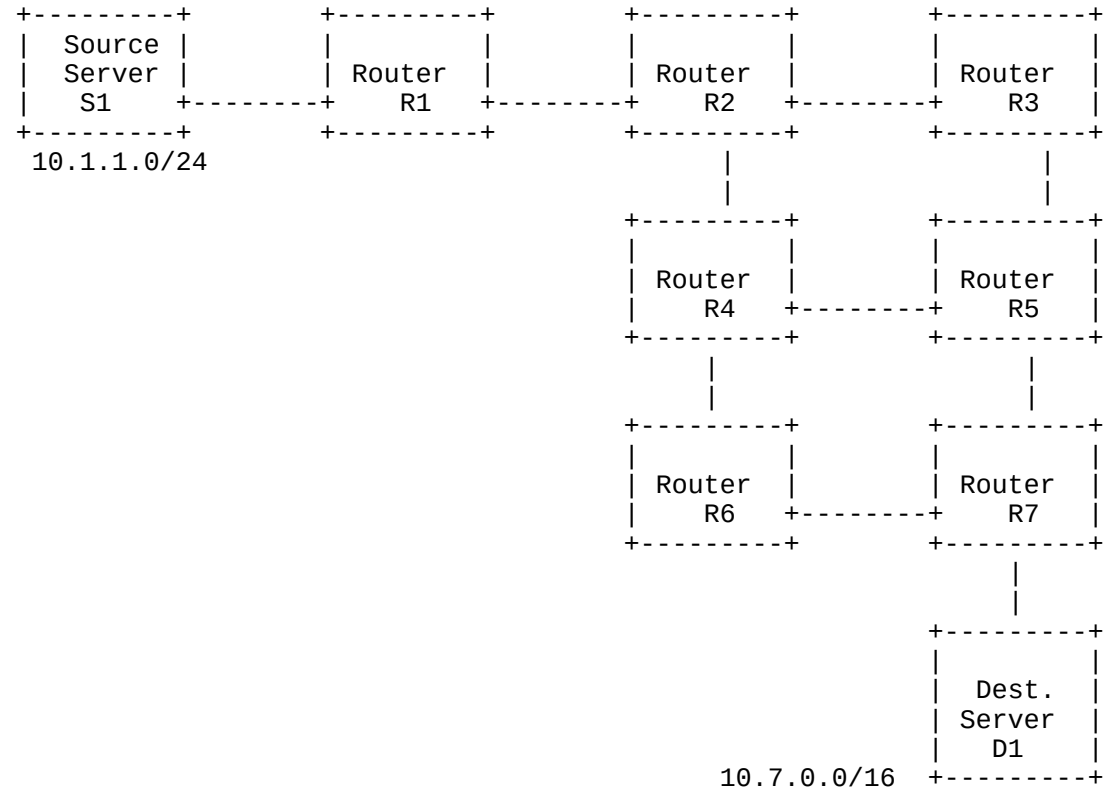

Figure 1 An example of intra-domain network

5.1. SR-policy Generation and Distribution

1. Controller Generation and Distribution: In an SR-policy-configured network, the controller generates SR-policy and distributes it to key nodes such as gateways, core routers, or edge routers. The controller directly delivers the SR-policy to the headend router.

2. SR-policy Parsing: Upon receiving the SR-policy from the controller, the headend router parses the policy to extract the Segment List and associated strategy information, such as path selection and QoS parameters. The headend router parses the segment routing policy sent by the controller to obtain a target segment list; the target segment list is composed of ordered segment identifiers, the segment identifiers in the target segment list are used to represent nodes in the network, and the target segment list is used to define a forwarding path.

3. Message Generation: The headend router generates the SAV message based on the SR-policy.

4. Message Distribution: The headend router forwards the SAV messages according to the forwarding path.

5.2. The SAV Messages Generation and SAV Rule’s Creation

The headend router generates the SAV message based on SR-policy and forwards the SAV message to other routers according to the forwarding path. Then the other routers create SAV rules at the receiving interface after receiving the SAV message, which to ensure accurate and secure traffic forwarding. The SAV rules verify the legitimacy of packet source addresses to prevent malicious or misleading information.

5.2.1. The SAV Messages Fields

The structure of the SAV message was proposed in [ID.draft-zhang-savnet-sav-ospf-00], and we have referenced it, providing the following explanations for each field. It should be noted that [ID.draft-zhang-savnet-sav-ospf-00] assigns field values based on the routing table, while this draft assigns field values based on SR policy. The SAV message includes: Message Type field, Source Router field, Neighbor Router field, Source Prefix field, and Segment List field. The SAV message further includes one or more of a Security Level field and a Quality Of Service field.

* Message Type (MT): Used to indicates the type of message.

* Source Router (SR): Used to identifier of the source router.

* Neighbor Router (NR): Used to identifier of the neighbor router.

* Source Prefix (SP): Used to identify source prefix.

* Segment ID List (SID_list): Used to list of segment IDs defined by the SR-policy.

* Security Level (SEC): Used to indicates security requirements.

* Quality of Service (QoS): Used to indicates quality of service requirements.

5.2.2. Text representation of the SAV message

Based on the SR-policy, this document RECOMMENDED text representation of SAV message through following structure:

1. <srcIP, other, SID_list>:
    * SP: srcIP
    * DR: Updated according to SID_list.
    * SID_list: Segment IDs specified by the SR-policy.
2. <*, other, SID_list>:
    * SP: Default value, representing all source prefixes from the head-end router.
    * DR: Updated according to SID_list.
    * SID_list: Segment IDs specified by the SR-policy.
3. Security and QoS Settings:
    * SEC: Set according to the security requirements defined in the SR-policy.
    * QoS: Set according to the QoS requirements defined in the SR-policy.

Explain and clarify the above structure：

1. When the SR-policy includes source prefixes, the Source Prefix (SP) field in the SAV message can be directly set to srcIP in the policy by the headend router. Specifically:

* The headend router determines the value of the Source Prefix field in the SAV message based on the SR-policy.
* The headend router sets the value of the Segment ID List field in the SAV message to the target Segment List defined by the SR-policy.

2. When the SR-policy does not include source prefixes, the Source Prefix (SP) field in the SAV message is set to the default value by the headend router according to the local traffic control policy. Specifically:

* The headend router sets the default value for the Source Prefix field in the SAV message according to its local traffic control policy.

* The headend router sets the value of the Segment ID List field in the SAV message to the target Segment List defined by the SR-policy.

3. The headend router determines the value of the security level field in the SAV message based on the security requirements in the SR-policy; The headend router determines the value of the quality of service field in the source address verification message based on the quality of service requirements in the SR-policy.

5.2.3. The SAV Rule’s Creation

The headend router generates the SAV message and forwards it to the other forwarding routers. The forwarding routers process the SAV message, identifying the interface receiving the SAV message as a valid interface, creating the SAV rules. Then The forwarding routers forward the SAV message to the next hop based on the Segment List in the SAV message. The SAV rules are created to ensure that the data packets enter the router meet the required SAV rules. To guide routers on how to handle source address verification of actual data packets. The SAV rule includes these fields: SP field and List of valid interfaces field.

* Source prefix (SP): The source prefix that needs to be verified.

* List of valid interfaces: which interfaces can receive data packets from the specified source prefix.

* Security Level (SEC): Define how to handle non compliant data packets (optional).

* Quality of Service (QoS): Quality of Service requirements related to packet processing (optional).

5.3. The SAV Message Forwarding Decisions

1. Basic Forwarding Logic:

When a router receives an SAV message, it must forward the message along the path specified by its SR-policy rules.

The process involves several steps:

* Key Node Matching: Each router has a locally configured SID (or multiple SIDs) that identifies its role in the SR network. When receiving the SAV message, the router will check whether the SIDs in the SAV message matches its local SID. If the SID in the SAV message matches the local SID of the router, it indicates that the router is on the specified path and should handle the SAV message.

* Key Node Handling: If the router is a key node, it processes the SAV message and generates the corresponding SAV rule, then forwards the message to the next key node according to the SID_list.

* Non-Key Node Handling: If the router is not a key node, it floods the SAV message to all neighboring routers to find the next hop, it won’t handle the SAV message and won’t create the SAV rule.

2. Interface Policies:

* Interface Activation: Routers along the SID_list path create the SAV rule at receiving interfaces to ensure legitimate traffic validation.

* Interface Deactivation: If the router is not a key node or the path is broken, it does not create the SAV rule, maintaining interface policy simplicity and security.

3. Message Forwarding:

* Forward to Target: If the router is an intermediate node or the starting point, it forwards the SAV message to the target node specified in the SAV message.

* Update NR Field: Every time traffic passes through a node that matches the SID_list, the current SID in the SAV message is ’ consumed ’ (removed or skipped from the SID_list), and the router updates the SID_list in the SAV message to make the SID of the next node the current segment. And the router also updates the value of the NR field in the SAV message to be the identifier of the next hop in the forwarding path defined by the SID_list.

* Flooding Mechanism: If a router cannot find the next hop which is indicated by the NR field in the SAV message when forwarding the SAV message along the forwarding path, it floods the SAV message to all neighboring routers. This forwarding path is the path specified by SID_list in the SAV message.

5.4. Handling Exceptions

* Path Interruption: If the primary SR-policy path is interrupted, the hand-end router adjusts the SID_list to follow a backup path. Specifically, the segment routing strategy includes a selectable segment list, which is used to define alternative paths; If the forwarding path is interrupted or an unreachable node occurs, the headend router updates the source address verification message based on the alternative path to obtain a new source address verification message; The headend router propagates a new source address verification message according to the alternative path.

* Security and QoS: Ensure that SR-policy security and QoS requirements are met during message forwarding.

5.5. Mechanism Optimization

* Multiple Paths: Define multiple paths in the SID_list for parallel message transmission, enhancing reliability and efficiency. If the target segment list defines multiple forwarding paths, the headend router obtains multiple forwarding paths and propagates messages in parallel on multiple forwarding paths.

* Message Merging: Combine messages with the same source prefix and destination address to reduce communication overhead.

5.6. Usecase: SAV Message Propagation Based on SR-policy

Network Topology Consider a network topology with the following routers and connections: R1: Headend router R2: Intermediate router R3: Intermediate router R4: Intermediate router R5: Destination router. As shown in Figure 2.

The network connections are as follows: R1 is connected to R2 and R3. R2 is connected to R4. R3 is connected to R4. R4 is connected to R5. In this scenario, we have the following SR-policy defined:

* Source Prefix (SP): 10.1.1.0/24

* Destination Prefix (DP): 10.5.0.0/16

* Segment ID List (SID_list): [SID2, SID4, SID5]

The goal is to redirect traffic from the source IP addresses within 10.1.1.0/24 heading towards the destination prefix 10.5.0.0/16 to follow the path defined by the SR-policy: R1 -> R2 -> R4 -> R5. This ensures that all interfaces along the path create appropriate the SAV rule to validate incoming traffic.

Steps:

Control Plane: SR-policy Creation and Distribution:

* The network controller creates the SR-policy with the Segment ID List ([SID2, SID4, SID5]) and distributes it to the headend router, R1.

R1 Control Plane: SAV Message Generation:

* Upon receiving the SR-policy in its control plane, R1 generates the SAV message.

Data Plane: SAV Message Propagation:

* The SAV message is then propagated along the path specified by the SR-policy through the data plane, being forwarded hop-by-hop through each node listed in the SID list.

The SAV message includes:

* MT: SR

* SR: R1

* NR: R2 (first hop according to SID_list)

* SP: 10.1.1.0/24

* SID_list: [SID2, SID4, SID5]

* SEC: As required by the policy

* QoS: As required by the policy

R1 forwards the SAV message to R2. At R2: R2 receives the SAV message from R1. R2 matches the SID2 from the SID_list to its local SID and recognizes itself as a key node. R2 designates the interface for receiving the SAV message from R1 is valid for incoming traffic from 10.1.1.0/24. R2 handles the SAV message and creates the SAV rule at the interface of receiving the SAV message. Then R2 forwards the SAV message to R4 (next hop according to SID_list).

At R4: R4 receives the SAV message from R2. R4 matches the SID4 from the SID_list to its local SID and recognizes itself as a key node. R4 designates the interface for receiving the SAV message from R2 is valid for incoming traffic from 10.1.1.0/24. R4 handles the SAV message and creates the SAV rule at the interface of receiving the SAV message. Then R4 forwards the SAV message to R5 (next hop according to SID_list).

At R5: R5 receives the SAV message from R4. R5 matches the SID5 from the SID_list to its local SID and recognizes itself as the final destination. R5 designates the interface for receiving the SAV message from R4 is valid for incoming traffic from 10.1.1.0/24. R5 handles the SAV message and creates the SAV rule at the interface of receiving the SAV message.

During the SAV message forwarding process, there may be the following situations:

1. Missing Neighbor Router: If a router cannot find NR when forwarding the SAV message along the forwarding path, it floods the SAV message to all neighboring routers. This forwarding path is the path specified by SID_list in the SAV message. This approach ensures that the SAV message does not get dropped due to the missing of a specified NR, allowing the message to continue its propagation and potentially be processed by a router that can provide further direction.

2. Non-path Next-hop Router: If the next hop router does not match in the SID_ list, the router will not handle the SAV message and create the SAV rule since the next-hop router is not part of the predefined path in the SID_ list. The router floods the SAV message to all its neighboring routers. This ensures that only routers on the specified path create the SAV rule, maintaining the integrity and accuracy of the SR-policy.

Results By propagating the SAV message, each router along the path (R1 -> R2 -> R4 -> R5) has validated interfaces for incoming traffic from the source prefix 10.1.1.0/24. This ensures that subsequent traffic can be validated and follow pre-defined paths, thereby enhancing the security and reliability of the network.

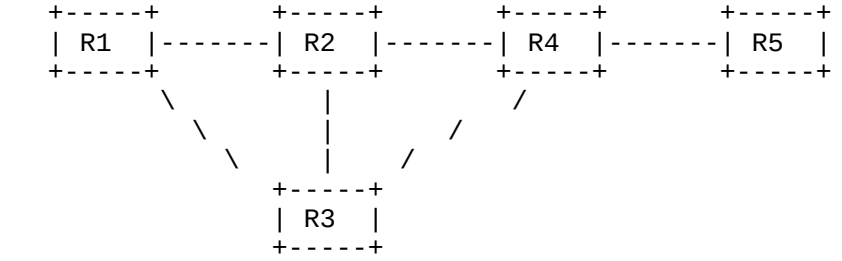

Figure 2 An example of usecase

6. Conclusion

This SR-policy-based SAV message propagation mechanism provides enhanced control and flexibility compared to traditional methods, ensuring efficient, secure, and accurate propagation of source address validation messages. By leveraging SR-policy's capabilities, network administrators can define optimal paths, enforce the SAV rule at key nodes, and maintain high security and QoS standards throughout the network.

This draft creates a flexible and resilient security model that evolves with network dynamics, paving the way for improved network security and performance in SR-policy-configured environments.

7. IANA Considerations

8. Acknowledgement

9. 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>.

[RFC8174] "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words".

[RFC8402] "Segment Routing Architecture".

[RFC8793] Wissingh, B., Wood, C., Afanasyev, A., Zhang, L., Oran, D., and C. Tschudin, "Information-Centric Networking (ICN): Content-Centric Networking (CCNx) and Named Data Networking (NDN) Terminology", RFC 8793, DOI 10.17487/RFC8793, June 2020, <https://www.rfc-editor.org/info/rfc8793>.

[RFC8987] "Segment Routing Policy Architecture.".

[SAV] "General Source Address Validation Capabilities", September 2019.

[sav-ospf] "draft-zhang-savnet-sav-ospf-00", September 2010.

[SAVNET] "Intra-domain Source Address Validation (SAVNET) Architecture".

Authors' Addresses

Xueting Li
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: lixt2@foxmail.com

Aijun Wang
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: wangaj3@chinatelecom.cn