SAVNET Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 January 2026

W. Wang
A. Wang
China Telecom
R. Pang
China Unicom

20 July 2025

Intra-domain Source Address Validation (SAV) Solution Based on BM-SPF
draft-wang-savnet-intra-domain-solution-bm-spf-01

Abstract

This draft proposes a new intra-domain Source Address Validation (SAV) solution. This solution leverages the Bidirectional Metric-based Shortest Path First (BM-SPF) mechanism to avoid the complexity introduced by asymmetric routing for source address validation. It allows intra-domain routers to generate directly the SAV rule from the router's FIB table, based on the reality that the source and destination interface will be same if the IGP domain is symmetric assured.

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 21 January 2026.

Copyright Notice

Table of Contents

1. Introduction

[I-D.ietf-savnet-intra-domain-architecture] proposed two use cases to describe the problems of existing intra-domain SAV mechanisms, and mentioned the intra-domain Source Address Validation (SAV) aims to achieve the following objectives:

* To prevent outbound packets from intra-domain subnets (such as host networks or customer networks) from spoofing the source addresses of other intra-domain subnets or other Autonomous Systems (ASes)

* To prevent inbound packets from external ASes from spoofing the source addresses of the local AS

To achieve these goals, intra-domain SAV needs to focus on the validation mechanisms at three types of routers: Edge Routers (host-facing routers, customer-facing routers), Internal Routers and AS Border Routers. Specifically, Edge Routers (host-facing or customer-facing routers) need to intercept spoofed packets from the connected networks whose source IP addresses do not belong to those networks. Interal Routers, such as spine routers, should also be considered to deploy SAV mechanism to simplify the overall deployment of SAV rules within the network. AS Border Routers need to intercept spoofed packets from other ASes whose source IP addresses belong to the local AS.

It is better to find one general solution that can cover all of the above routers, increase the flexibility of intra-SAV deployment within the operator's network. The main challenge for such general solution is how to assure the symmetric routing on routers within the IGP domain. If such challenge is solved, the behavior of edge router(host-facing, or customer-facing), internal router(the best deployment point for the spine-leaf topology) and AS border router will be same: the SAV can be generated automatically based on the FIB table.

[I-D.wang-lsr-bidirectional-metric-spf] proposes a mechanism to accomplish the Shortest Path First (SPF) calculation based on the bidirectional metrics of the links. Under such mechanism, the bidirectional link metrics that are used by the two neighbors to implement the SPF algorithm to calculate the path will be same, which can avoid the asymmetric routing, and simplify the generation of SAV rule on intra domain IGP routers.

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] .

3. Terminology

The following terms are used in this draft:

BM-SPF: Bidirectional Metric based Shortest Path First Mechanism, defined in [I-D.wang-lsr-bidirectional-metric-spf].

4. The Procedure of this Mechanism

Figure 1 depicts an example of an AS that all routers within it support BM-SPF, the topology is aligned with [I-D.ietf-savnet-intra-domain-architecture]. On Router A, a summarized route 10.0.0.0/16 and a detailed route 10.0.1.0/24 should be configured, with its next hop interface directed to interface "#" of Router A. On Router B, a summarized route 10.0.0.0/16 and a detailed route 10.0.2.0/24 should be configured, with its next hop interface directed to interface "#" of Router B.

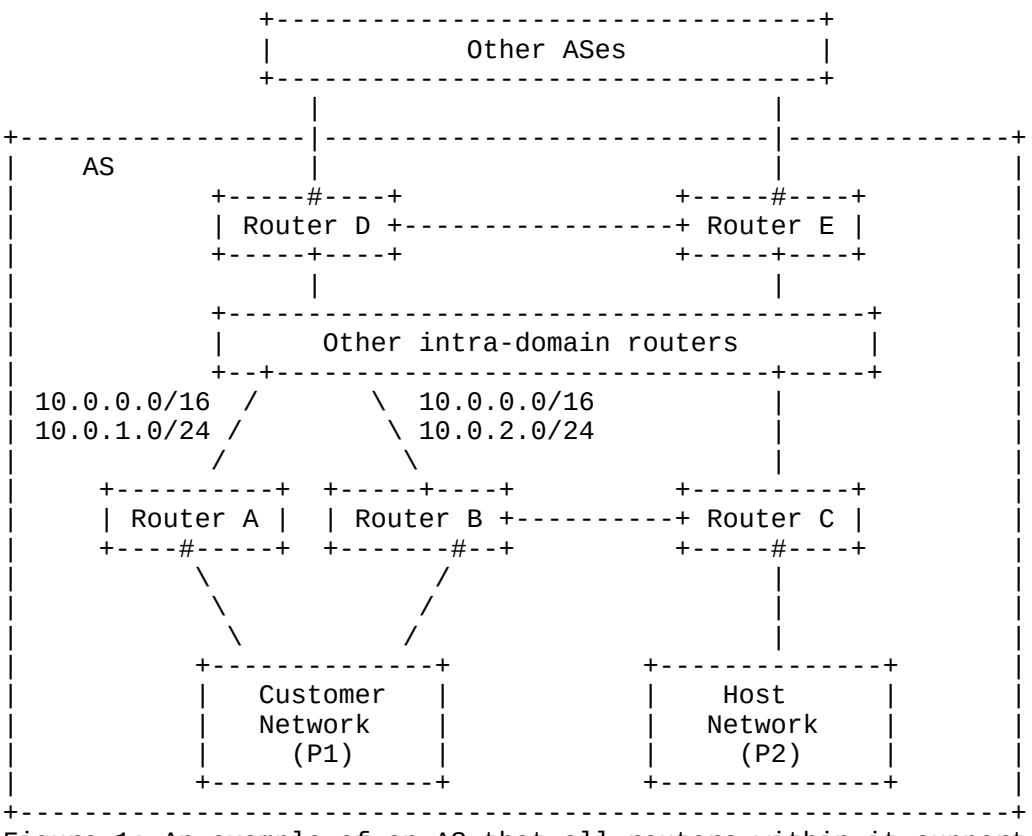

Figure 1: An example of an AS that all routers within it support BM-SPF

4.1. SAV Procedure on AS Border Routers

In Figure 1, the AS Border routers (Router D and Router E) has all the intra-domain prefixes that learned from the IGP protocol. The interface "#" on AS Border Routers enables mode 2 SAV rule (per [I-D.ietf-savnet-general-sav-capabilities]), which can generates an interface-based blocklist containing all these prefixes. For an AS Border Router (such as Router D or Router E), it should performs the following procedures:

1. Traverse all the prefixes in its FIB table;

2. Add all prefixes and the corresponding interface into the blocklist on its interface '#';

When an AS Border Router receives packets with spoofed P1/P2 from interface ‘#’ , the packets will be blocked from entering the AS because the source addresses of these packets are included in the blocklist of the AS Border Router.

If an AS Border Router receives the packet with spoofed source address of the links within the AS, it can also block them automatically.

4.2. SAV Procedure on Edge Routers

In Figure 1, the customer network is multi-homed and the host network is single-homed. Router A and Router B are customer-facing routers, and Router C is host-facing router. The interfaces "#" on Router A, B and C enable mode 1 SAV rule.

For single-homed host network, Router C can prevent other spoofed packets(source address is not from P2) from being accepted.

For multi-homed customer network, to achieve the effect of engineering return traffic based on the granular address space, two kinds of routes(summarized and detailed) should be configured on the customer-facing routers, as shown in Figure 1.

For an Edge Router (such as Router A, Router B or Router C), it should perform the following procedures:

1. Traverse all the prefixes in its FIB table;

2. Add all prefixes and the corresponding interface into the allow list on its interface ’#’;

4.3. SAV Procedure on Internal Routers

Deploying the intra-domain SAV mechanism on Edge Routers and AS Border Router can solve the intra-domain SAV problem. But in some spine-leaf scenario, there is more efficient deployment point to achieve the same goal. For example, in Figure 1, if one spine router within "Other intra-domain routers" connects Router A, Router B and Router C, instead of deploying the intra-domain SAV mechanism on these leaf routers, the operator can select deploy it only on the spine router. With the BM-SPF mechanism (per [I-D.wang-lsr-bidirectional-metric-spf]), only symmetric routes exist in an AS with full BM-SPF deployment. The internal router (such as the spine leaf) can enable mode 1 SAV rule on its interfaces, the SAV procedures is performed in accordance with Section 4.2.

In summary, SAV procedures in Internal Router and Edge Router (such as host-facing router and customer-facing router) are all the same. The procedures in AS Border Router can easily cover the prefixes from host network, customer network and internal links. Then the intra-domain SAV BM-SPF based solution can easily cover all of the scenarios that are described in [I-D.ietf-savnet-intra-domain-problem-statement].

4.4. Overview of BM-SPF

[I-D.wang-lsr-bidirectional-metric-spf] introduces the BM-SPF router capabilities announcement. Once the routers within the IGP domain know all of routers within its domain support and enable the BM-SPF feature, it can safely generate the SAV based on its FIB table.

In an AS that has fully deployed BM-SPF, the bidirectional metric values for SPF calculation on each path are the same. This indicates that when two routers are communicating, the packets between them will be transmitted through the same path. That is to say, when any router within this AS communicates with a peer, whether it is sending packets to that peer or receiving packets from that peer, the same interface is used.

5. Security Considerations

The security considerations described in [I-D.ietf-savnet-intra-domain-problem-statement] and [I-D.ietf-savnet-intra-domain-architecture] also applies to this draft.

6. IANA Considerations

None

7. Normative References

[I-D.ietf-savnet-general-sav-capabilities]
Huang, M., Cheng, W., Li, D., Geng, N., and L. Chen, "General Source Address Validation Capabilities", Work in Progress, Internet-Draft, draft-ietf-savnet-general-sav-capabilities-01, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-general-sav-capabilities-01>.

[I-D.ietf-savnet-intra-domain-architecture]
Li, D., Wu, J., Qin, L., Geng, N., and L. Chen, "Intra-domain Source Address Validation (SAVNET) Architecture",

Work in Progress, Internet-Draft, draft-ietf-savnet-intra-domain-architecture-02, 13 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture-02>.

[I-D.ietf-savnet-intra-domain-problem-statement] Li, D., Wu, J., Qin, L., Huang, M., and N. Geng, "Source Address Validation in Intra-domain Networks Gap Analysis, Problem Statement, and Requirements", Work in Progress, Internet-Draft, draft-ietf-savnet-intra-domain-problem-statement-17, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-17>.

[I-D.wang-lsr-bidirectional-metric-spf] Wang, A., "Bidirectional Metric based Shortest Path First Mechanism", Work in Progress, Internet-Draft, draft-wang-lsr-bidirectional-metric-spf-00, 10 February 2025, <https://datatracker.ietf.org/doc/html/draft-wang-lsr-bidirectional-metric-spf-00>.

[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>.

Authors' Addresses

Wei Wang
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: weiwang94@foxmail.com

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

Ran Pang
China Unicom
9 Shouti South Rd.
Beijing
100089
China
Email: pangran@chinaunicom.cn