SAVNET
Internet-Draft
Intended status: Informational
Expires: 2 August 2026

L. Qin
Zhongguancun Laboratory
N. Geng
Huawei
D. Li
Tsinghua University

29 January 2026

Source Prefix Advertisement for Intra-domain SAVNET
draft-li-savnet-source-prefix-advertisement-06

Abstract

This document describes a mechanism for intra-domain source address validation (SAV), called Source Prefix Advertisement (SPA) for Intra-domain SAVNET (Intra-domain SPA). The mechanism enables intra-domain routers to generate accurate SAV rules by leveraging routing information together with SAV-specific information, including Source Entity Identifiers (SEIs) and Hidden Prefix (HP). Intra-domain SPA improves the precision and reliability of source address validation, addressing challenges such as asymmetric routing and the use of hidden prefixes by legitimate source entities.

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 2 August 2026.

Copyright Notice

Table of Contents

1. Introduction

Existing unicast Reverse Path Forwarding (uRPF) mechanisms (e.g., strict uRPF) [RFC3704] may incorrectly drop legitimate data packets in scenarios involving asymmetric routing or hidden prefixes (see [I-D.ietf-savnet-intra-domain-problem-statement]). Similarly, ACL-based ingress filtering [RFC2827] relies entirely on manual updates, which can be difficult to maintain.

To improve accuracy and enable automatic updates, this document proposes a new intra-domain source address validation (SAV) mechanism, called Source Prefix Advertisement (SPA) for Intra-domain SAVNET (referred to as Intra-domain SPA). Intra-domain SPA allows routers in an intra-domain network to obtain and exchange SAV-

specific information, including Source Entity Identifiers (SEIs) and Hidden Prefixes (HPs), in order to generate more precise SAV rules automatically.

The reader is encouraged to be familiar with [I-D.ietf-savnet-intra-domain-problem-statement] and [I-D.ietf-savnet-intra-domain-architecture].

1.1. Terminology

SAV Rule: The rule that describes the mapping relationship between a source address (prefix) and its valid incoming router interface(s).

SAVNET Router: An intra-domain router that deploys Intra-domain SPA.

Non-BGP Customer Network: A stub network connected to one or more routers of the AS for Internet connectivity. It only originates traffic and does not participate in BGP routing exchanges with the AS.

Source Entity Identifier (SEI): A unique identifier assigned by an operator to represent a specific source entity, such as a non-BGP customer network or a set of hosts within a LAN. Each SEI is associated with one or more interfaces on the SAVNET routers that connect to the corresponding source entity.

Hidden Prefix: A hidden prefix is a prefix legitimately used by a source entity but not visible in the intra-domain routing system.

1.2. 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. Deployment Scope

Intra-domain SPA focuses solely on source address validation (SAV) performed on the external interfaces of an intra-domain network. Each SAVNET router can automatically generate either an allowlist SAV rule (i.e., “Interface-based prefix allowlist” mode in [I-D.ietf-savnet-general-sav-capabilities]) or a blocklist SAV rule (i.e., “Interface-based prefix blocklist” mode in [I-D.ietf-savnet-general-sav-capabilities]) for a specific interface, depending on the role of the connected entity.

* Interfaces facing a set of hosts: The SAVNET router generates an allowlist SAV rule that precisely covers the source address space legitimately used by the connected hosts.

* Interfaces facing a non-BGP customer network: The SAVNET router generates an allowlist SAV rule that precisely covers the source address space legitimately used by the non-BGP customer network.

* Interfaces facing an external AS: The SAVNET router generates a blocklist SAV rule that precisely covers the source address space that is valid only within the local AS and must not be used by external networks.

2.1. Incremental Deployment Considerations

Intra-domain SPA can be deployed incrementally and still provide immediate security benefits within its deployment scope. Each SAVNET router that supports Intra-domain SPA applies SAV rules on its external interfaces — whether facing hosts, non-BGP customer networks, or external ASes.

When an interface is protected by Intra-domain SPA, spoofed traffic with unallowed source addresses cannot enter the domain through that interface. As a result, even partial deployment (e.g., enabling Intra-domain SPA on a subset of external interfaces) effectively reduces the potential attack surface.

By using allowlist SAV rules, SAVNET routers prevent connected hosts or non-BGP customer networks from sending packets with unauthorized source addresses. By using blocklist SAV rules, SAVNET routers prevent connected external ASes from sending packets that use internal-use-only source addresses.

As more SAVNET routers in the AS adopt Intra-domain SPA, the overall protection against source address spoofing attacks increases correspondingly, achieving progressive and cumulative deployment benefits without requiring full coverage from the outset.

3. SAV-specific Information in Intra-domain SPA

Intra-domain SPA uses SAV-specific information to supplement routing data, enabling accurate and automated generation of SAV rules. Two key types of SAV-specific information are used: Source Entity Identifier (SEI) and Hidden Prefix (HP). These serve complementary roles: SEI identifies the source entity originating traffic, while HP provides authoritative information about prefixes legitimately used by the source entity but not visible in the intra-domain routing system.

3.1. Source Entity Identifier (SEI)

A Source Entity Identifier (SEI) is a unique identifier assigned by the network operator to represent a source entity, which may be a non-BGP customer network or a set of hosts within a LAN connected to the SAVNET router.

Each SEI is associated with one or more interfaces of SAVNET routers that connect directly to the corresponding source entity. This binding allows routers to explicitly indicate which entity a specific interface belongs to.

SEIs are propagated within the domain via route advertisements. Upon receiving routes with SEIs, routers can correlate multiple routes belonging to the same entity. This capability is especially useful in asymmetric routing scenarios. For example, when a non-BGP customer network connects to multiple routers and advertises different subsets of its prefixes, uRPF-based filtering may incorrectly drop return traffic. By using SEI, routers can aggregate prefixes for the same entity and generate a unified allowlist, avoiding improper blocks.

3.2. Hidden Prefix (HP)

A hidden prefix is a prefix legitimately used by a source entity but not visible in the intra-domain routing system. Examples include:

* A host that uses a source address not allocated by the operator for Direct Server Return (DSR) or similar applications.

* A non-BGP customer network that uses certain prefixes not announced to the operator.

To avoid improper permits, non-BGP customers or hosts provide their hidden prefixes to the operator, which are then used as SAV-specific information when generating rules on the corresponding interfaces.

Authorization for hidden prefixes may be conveyed through a Traffic Origin Authorization (TOA) object [I-D.qin-savnet-toa] signed by the prefix holder, indicating that traffic from the hidden prefix is legitimate.

SAVNET routers can use this information to allow legitimate traffic from hidden prefixes, even when the prefixes are not visible in intra-domain routing.

4. SAV Rule Generation Procedure

This section describes two approaches for generating SAV rules in Intra-domain SPA. The first approach relies solely on routing information and provides a simple baseline mechanism. The second approach enhances accuracy by combining routing information with SAV-specific information, addressing asymmetric routing and hidden prefix scenarios.

4.1. SAV Using Routing Information

This subsection first describes how routing information can be used to generate more accurate SAV rules than existing intra-domain SAV mechanisms (e.g., strict uRPF and loose uRPF).

Each SAVNET router connected to a set of hosts or a non-BGP customer network generates an allowlist SAV rule. The procedure for allowlist generation is as follows:

1. Extract prefixes from the Forwarding Information Base (FIB) or/ and Routing Information Base (RIB): Select all unique prefixes in the router' s FIB or/and RIB whose next-hop interface points toward the connected set of hosts or non-BGP customer network.

2. Construct the allowlist: Include these prefixes in the allowlist SAV rule for the corresponding interface. The allowlist defines the legitimate source address space that may appear on this interface.

Each SAVNET router connected to an external AS generates a blocklist SAV rule. The procedure for blocklist generation is as follows:

1. Extract internal-use prefixes: Select all unique prefixes from the routing information learned via the intra-domain routing protocol that are originated within the local AS.

2. Construct the blocklist: Include these internal-use prefixes in the blocklist SAV rule for interfaces facing external ASes, preventing incoming traffic that uses internal source addresses.

This routing-based approach works effectively when routing visibility is complete and symmetric. However, in scenarios involving asymmetric routing or hidden prefixes, the allowlist derived solely from routing information may not fully cover the legitimate source address space of a set of hosts or a non-BGP customer network. As a result, legitimate packets may be improperly blocked.

To improve SAV accuracy and avoid such improper blocking, the next subsection introduces an enhanced rule-generation procedure that combines routing information with SAV-specific information (i.e., Source Entity Identifier and Hidden Prefix).

4.2. SAV Using SAV-specific Information and Routing Information

This subsection describes an enhanced rule generation approach that leverages both routing information and SAV-specific information to improve SAV accuracy under conditions such as asymmetric routing and hidden prefixes.

Each SAVNET router connected to a set of hosts or a non-BGP customer network generates an allowlist SAV rule as follows:

1. Identify source entities: For all source entities connected to the router, create a set of their corresponding Source Entity Identifier (SEI) values. Denote this set as Set A.

2. Associate prefixes with SEIs: Using all available SAV-specific information, for each SEI value in Set A, obtain the set of source prefixes associated with the same SEI value.

3. Construct the allowlist: For each interface connected to a source entity, construct an allowlist that includes:

    * all prefixes associated with the SEI configured on that interface; and

    * any hidden prefixes that the source entity has explicitly provided to the operator.

Each SAVNET router connected to an external AS generates a blocklist SAV rule as follows:

1. Extract internal-use prefixes: Select all unique prefixes from the routing information learned via the intra-domain routing protocol.

2. Filter out externally valid prefixes: Exclude any prefix that is considered externally valid, including:

    * prefixes that are observed in routing information learned from external ASes via inter-domain routing; and

    * prefixes that have an external AS number (ASN) listed as the origin in a valid Route Origin Authorization (ROA) or Traffic Origin Authorization (TOA).

3. Construct the blocklist: Include the remaining prefixes in the blocklist SAV rule for interfaces facing external ASes. This prevents traffic from external ASes from using source addresses that are valid only within the local AS.

5. Operational Considerations

5.1. Handling SEIs

5.1.1. SEI Assignment and Configuration

Operators are recommended to use network management or automation tools to assign and maintain SEIs consistently to reduce the risk of misconfiguration.

When a source entity connects to multiple routers, all interfaces MUST use the same SEI to enable correct aggregation of prefixes and accurate identification of the entity across the domain.

5.2. Handling Hidden Prefixes

Hidden prefix information can be incorporated into SAV rule generation on interfaces facing the entities, without requiring a separate synchronization mechanism. Authorization for using hidden prefixes may be conveyed, for example, via a Traffic Origin Authorization (TOA) object [I-D.qin-savnet-toa] or other mechanisms approved by the prefix holder.

Operators can leverage existing operational management and automation tools to record and apply hidden prefix information consistently when generating SAV rules.

6. 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 document.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. 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>.

[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/info/rfc8174>.

8.2. Informative References

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[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-02, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-general-sav-capabilities-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-21, 18 January 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-21>.

[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-03, 13 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture-03>.

[I-D.qin-savnet-toa] Qin, L., Maddison, B., Li, D., and I. Lubashev, "A Profile for Traffic Origin Authorizations (TOAs)", Work in

Progress, Internet-Draft, draft-qin-savnet-toa-00, 3 November 2025, <https://datatracker.ietf.org/doc/html/draft-qin-savnet-toa-00>.

Authors' Addresses

Lancheng Qin
Zhongguancun Laboratory
Beijing
China
Email: qinlc@mail.zgclab.edu.cn

Nan Geng
Huawei
Beijing
China
Email: gengnan@huawei.com

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn