SAVNET
Internet-Draft
Intended status: Informational
Expires: 18 April 2026

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

15 October 2025

Source Prefix Advertisement for Intra-domain SAVNET
draft-li-savnet-source-prefix-advertisement-05

Abstract

This document proposes a new mechanism for intra-domain source address validation (SAV), called Source Prefix Advertisement (SPA) for Intra-domain SAVNET (referred to as Intra-domain SPA). The mechanism enables intra-domain routers to automatically generate more accurate SAV rules by leveraging both routing information and SAV-specific information, including Source Entity Identifiers (SEIs) and Hidden Prefix Registration (HPR). Intra-domain SPA addresses scenarios such as asymmetric routing and hidden prefixes, improving the precision and reliability of 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 18 April 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. Similarly, ACL-based ingress filtering [RFC2827] relies entirely on manual updates, which can be difficult to maintain (see [I-D.ietf-savnet-intra-domain-problem-statement]).

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 Prefix Registration (HPR), 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 Registration (HPR): A registry mechanism maintained by the operator that records hidden prefixes (i.e., prefixes that are legitimately used by source entities but not visible in the intra-domain routing system). Each registered hidden prefix is bound to the SEI of the corresponding source entity.

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 introduces two types of SAV-specific information that supplement routing information to enable accurate and automatic generation of SAV rules: Source Entity Identifier (SEI) and Hidden Prefix Registration (HPR). These two types of information serve complementary roles. SEI identifies the source entity that originates traffic, while HPR provides authoritative information about hidden prefixes legitimately used by the source entity.

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 can be either a non-BGP customer network or a set of hosts within a LAN connected to the SAVNET router.

Each SEI is configured on one or more interfaces of SAVNET routers that directly connect to the corresponding source entity. This binding allows routers to explicitly indicate which entity a specific interface belongs to. The SEI is also associated with the operational account of the source entity in the operator's hidden prefix registration database (HPRD), enabling accountability and controlled hidden prefix registration.

SAVNET routers include the SEI in the routes they advertise within the domain. When other routers receive such route advertisements, they can identify that multiple routes belong to the same source entity by comparing SEIs. This capability allows routers to correlate and aggregate routes associated with the same entity, which is particularly 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 due to path asymmetry. By using SEI, routers can recognize that these prefixes belong to the same source entity and thus generate a unified allowlist for that entity, avoiding false drops.

3.2. Hidden Prefix Registration (HPR)

A Hidden Prefix Registration (HPR) mechanism is maintained by the operator to handle hidden prefixes, i.e., prefixes legitimately used by source entities 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 ensure authenticity, the operator maintains an HPR database that records each registered hidden prefix and binds it to the SEI of the corresponding source entity. When a source entity wishes to register a hidden prefix, it must provide authorization proof that it is legitimately allowed to source traffic from that prefix. One possible proof is a Traffic Origin Authorization (TOA) object [I-D.qin-sidrops-toa] signed by the prefix holder, which authorizes the operator's AS to originate traffic from that prefix.

SAVNET routers can query or periodically retrieve HPR data from the database. Upon learning that a hidden prefix is bound to a specific SEI, routers can augment their allowlists accordingly by ensuring that traffic from the source entity using the hidden prefix is accepted.

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 precisely 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 dropped.

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 Registration).

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 an intra-domain stub network (e.g., a host network 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: Include these prefixes in the allowlist SAV rule of the interface that connects to the corresponding source entity (i.e., the interface associated with the same SEI value). This ensures that all valid source addresses of each connected source entity are properly permitted, even when the prefixes are not visible in the router’s routing information.

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

By incorporating SAV-specific information such as SEI-based mappings and hidden prefix registrations, this enhanced approach ensures comprehensive coverage of legitimate source prefixes while avoiding improper drops caused by asymmetric routing or incomplete routing visibility.

5. Operational Considerations

5.1. Management of the Hidden Prefix Registration Database

The operator is responsible for maintaining a Hidden Prefix Registration Database (HPRD), which stores registered hidden prefixes and their associated Source Entity Identifiers (SEIs). Each entity (e.g., the user of a host or the operator of a non-BGP customer network) registers the prefixes it legitimately uses and binds them to its assigned SEI.

To ensure the authority and authenticity of the registration, each entity MUST provide valid proof of authorization for using the registered prefix. Such proof can be verified by the operator, for example through a valid Traffic Origin Authorization (TOA) or other prefix holder-approved authorization mechanisms.

The operator SHOULD enforce access control to the HPRD. Each registered entity MUST only be able to access and manage its own registration data.

5.2. Synchronization with SAVNET Routers

SAVNET routers obtain SAV-specific information (including SEI and hidden prefix associations) from the HPRD through a secure synchronization mechanism. Synchronization MAY be achieved using a pull or push model, depending on the operator's network management system design.

Operators SHOULD ensure that SAVNET routers are kept up-to-date with recent registration data to prevent either:

* Improper blocking of legitimate traffic due to outdated information; or

* Improper permitting of spoofed traffic due to stale or revoked registrations.

Consistency across all routers participating in Intra-domain SPA is RECOMMENDED to maintain coherent SAV behavior across the network.

5.3. SEI Assignment and Configuration

Each interface connecting to a set of hosts or a non-BGP customer network MUST be configured with the SEI corresponding to that source entity. Operators SHOULD automate SEI assignment through centralized management tools to avoid misconfiguration.

When a source entity connects to multiple routers, all those routers MUST use the same SEI for the entity to enable proper prefix aggregation and identification across the network.

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.

6.1. Authorization of Hidden Prefix Registration

Entities registering hidden prefixes in the HPRD MUST be properly authenticated using credentials issued by the operator. Each entity MUST only be allowed to register prefixes it is authorized to use.

To verify such authorization:

* The operator SHOULD require a Traffic Origin Authorization (TOA) or equivalent proof.

* The HPRD MUST reject or revoke registrations that fail authorization or that have expired.

Operators SHOULD monitor registration activities to detect suspicious or fraudulent registrations.

6.2. SEI Management and Consistency

Incorrect or conflicting SEI assignments can lead to improper SAV rule generation and may open attack vectors for traffic spoofing. Operators MUST ensure:

* Each SEI is uniquely assigned within the domain (i.e., Autonomous System).

* SEI values are consistently configured on all interfaces connected to the same source entity.

* Unauthorized modification of SEI configuration is prevented through access control and configuration management systems.

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-19, 3 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-19>.

[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-sidrops-toa]
Qin, L., Maddison, B., and D. Li, "A Profile for Traffic Origin Authorizations (TOAs)", Work in Progress, Internet-Draft, draft-qin-sidrops-toa-00, 25 June 2025, <https://datatracker.ietf.org/doc/html/draft-qin-sidrops-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