SAVNET
Internet-Draft
Intended status: Informational
Expires: 16 April 2026

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

13 October 2025

Intra-domain Source Address Validation (SAVNET) Architecture
draft-ietf-savnet-intra-domain-architecture-03

Abstract

This document specifies the architecture of intra-domain SAVNET, which aims to achieve accurate source address validation (SAV) at external interfaces of an intra-domain network in an automated manner. It describes the conceptual design of intra-domain SAVNET, along with its use cases and design requirements, to help ensure that the intended objectives are met.

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 16 April 2026.

Table of Contents

1. Introduction

The main task of an intra-domain SAV mechanism is to generate the correct mapping between a source address (prefix) and its valid incoming router interface(s), referred to as SAV rules. The core challenge lies in efficiently and accurately learning this mapping. Existing intra-domain SAV mechanisms (such as strict uRPF [RFC3704] and ACL-based ingress filtering [RFC2827]) suffer from either inaccurate mappings in asymmetric routing or hidden prefix scenarios, or from high operational overhead in dynamic networks (see [I-D.ietf-savnet-intra-domain-problem-statement]). The fundamental cause is that these mechanisms generate SAV rules solely based on a router's local routing information or on manual configuration.

To address this challenge, the intra-domain SAVNET architecture requires routers to generate SAV rules based on SAV-specific information exchanged among routers, rather than relying solely on local routing information or manual configuration. Compared to uRPF [RFC3704], which depends only on a router's local routing information, SAVNET routers generate SAV rules by using both local routing information and SAV-specific information exchanged among routers, resulting in more accurate SAV validation in asymmetric routing and hidden prefix scenarios. Compared to ACL-based ingress filtering [RFC2827], which relies entirely on manual configuration to adapt to network dynamics, SAVNET routers learn SAV rules automatically in a distributed manner.

This document describes the conceptual design of intra-domain SAVNET, along with its use cases and design requirements, to help ensure that the intended objectives are met. The reader is encouraged to be familiar with [I-D.ietf-savnet-intra-domain-problem-statement] and [I-D.ietf-savnet-general-sav-capabilities].

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. Terminology

Local Routing Information: Information in a router's local RIB or FIB that can be used to infer SAV rules.

SAV-specific Information: Information exchanged among routers that is specifically used for SAV rule generation.

SAV-specific Information Communication Mechanism: A mechanism for exchanging SAV-specific information between routers. It can be a new protocol or an extension to an existing one.

SAV Information Base: A data structure within a router that stores both SAV-specific information and local routing information.

SAV Rule: The rule in a router that describes the mapping relationship between a source address (prefix) and the valid incoming interface(s). It is used by a router to make SAV decisions.

SAVNET Router: An intra-domain router that runs the intra-domain SAVNET function.

SAVNET Agent: A component within a SAVNET router that is responsible for exchanging SAV-specific information, processing such information, and generating SAV rules.

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.

Improper Block: The validation results that the packets with legitimate source addresses are blocked improperly due to inaccurate SAV rules.

Improper Permit: The validation results that the packets with spoofed source addresses are permitted improperly due to inaccurate SAV rules.

3. Threat Model

Intra-domain SAVNET assumes the following threat model:

1. Attackers

    * Directly connected hosts: Hosts that are directly attached to an intra-domain router (e.g., in a local LAN).

    * Non-BGP customer networks: Stub networks connected to one or more routers of the AS for Internet connectivity. They only originate traffic and do not participate in BGP routing exchanges with the AS.

    * External ASes: Autonomous systems outside the domain that send traffic to the domain.

2. Attacker Capabilities

   * Attackers may inject packets with spoofed source addresses into the domain.

   * Specifically:

     - At external interfaces facing hosts or non-BGP customer networks, attackers may attempt to send packets with source addresses they are not authorized to use.

     - At external interfaces facing external ASes, attackers may attempt to send packets using internal-use-only source addresses.

3. Assumptions

   * Intra-domain routers are trusted and operate correctly.

   * Spoofing traffic originating from a compromised intra-domain router is out of scope.

4. Scope and Goals

   * Prevent unauthorized source addresses from entering the intra-domain network at external interfaces.

   * Focus is on validating traffic at external interfaces, not on internal interfaces between trusted routers.

   * SAVNET aims to automatically generate and enforce SAV rules to achieve accurate source address validation, even in the presence of asymmetric routing or hidden prefix scenarios.

4. Deployment Scope and Use Cases

To reduce deployment overhead and avoid redundant validation, it is not necessary to include all intra-domain router interfaces within the deployment scope. In general, external interfaces serve as vantage points for deploying intra-domain SAVNET. Intra-domain SAVNET at external interfaces is more effective in identifying and discarding packets with spoofed source addresses because these interfaces are located at the boundary of the intra-domain network and are closer to the source. In addition, Intra-domain SAVNET at external interfaces can more clearly determine the valid incoming direction of specific source prefixes based on the network topology. Intra-domain SAVNET at internal interfaces is currently considered out of scope.

4.1. Use Case 1: Intra-domain SAVNET at External Interfaces Facing Hosts or Non-BGP Customer Networks

At external interfaces facing directly connected hosts or non-BGP customer networks, intra-domain SAVNET prevents these entities from injecting packets into the domain with source addresses they are not authorized to use.

4.2. Use Case 2: Intra-domain SAVNET at External Interfaces Facing External ASes

At external interfaces facing external ASes, intra-domain SAVNET prevents those ASes from injecting packets into the domain that use internal-use-only source addresses.

5. Architecture

5.1. Overview

Figure 1 illustrates the intra-domain SAVNET architecture within an intra-domain network. To generate accurate SAV rules, intra-domain SAVNET enables SAVNET routers to automatically exchange SAV-specific information. Each SAVNET router can independently decide which other SAVNET routers to provide its SAV-specific information to. The arrows in Figure 1 indicate the directions of SAV-specific information flows originating from Router A and Router C. Flows originating from other routers are omitted for clarity.

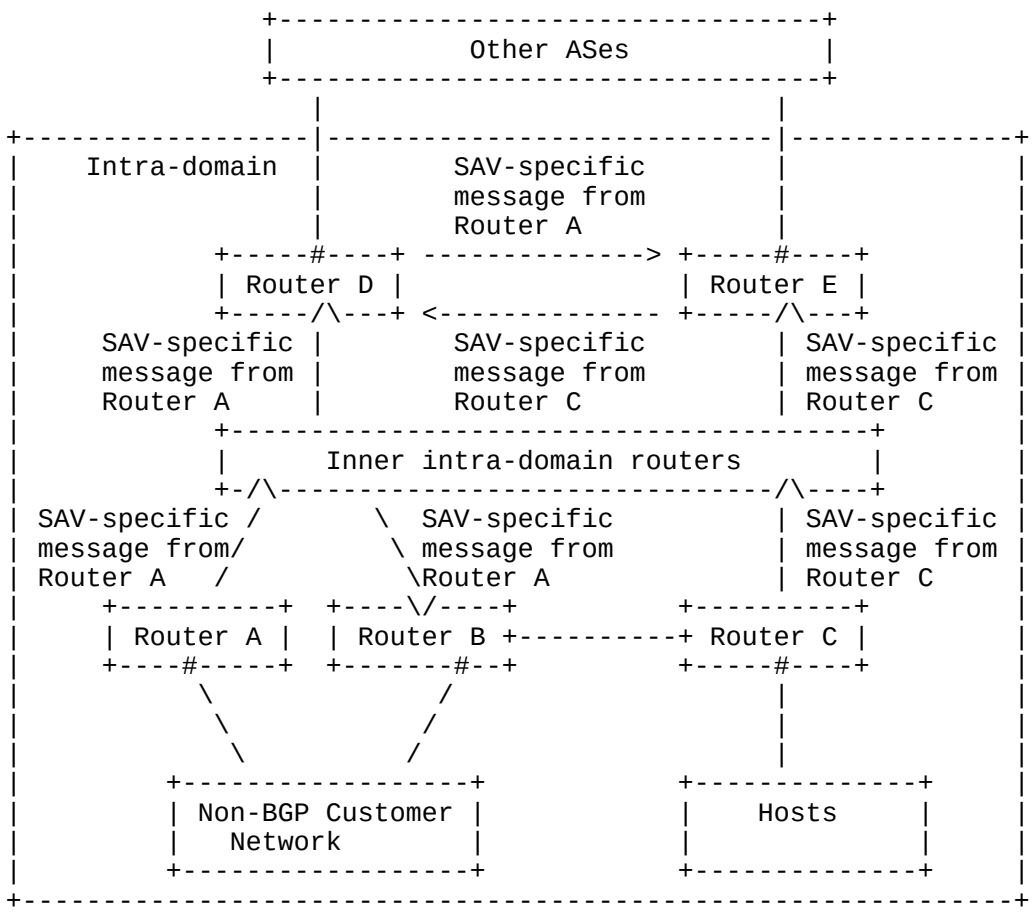

Figure 1: Overview of intra-domain SAVNET architecture

Each SAVNET router includes a SAVNET Agent responsible for SAV-related functions. As shown in Figure 2, a SAVNET router can serve one or both of the following roles in the intra-domain SAVNET architecture:

* Source Entity provides its SAV-specific information to other SAVNET routers.

* Validation Entity receives SAV-specific information from other SAVNET routers.

5.1.1. Source Entity

When a SAVNET router acts as a source entity, the information provider component of its SAVNET Agent supplies SAV-specific information to other SAVNET routers acting as validation entities. A SAVNET router serving as a source entity can obtain SAV-specific information about the hosts and/or non-BGP customer networks attached to it and selectively distribute this information to other SAVNET routers.

5.1.2. Validation Entity

When a SAVNET router acts as a validation entity, the information receiver component of its SAVNET Agent obtains SAV-specific information from other SAVNET routers acting as source entities. The SAVNET Agent then processes the received SAV-specific information, together with its own SAV-specific information and/or local routing information, to generate SAV rules for the corresponding interfaces.

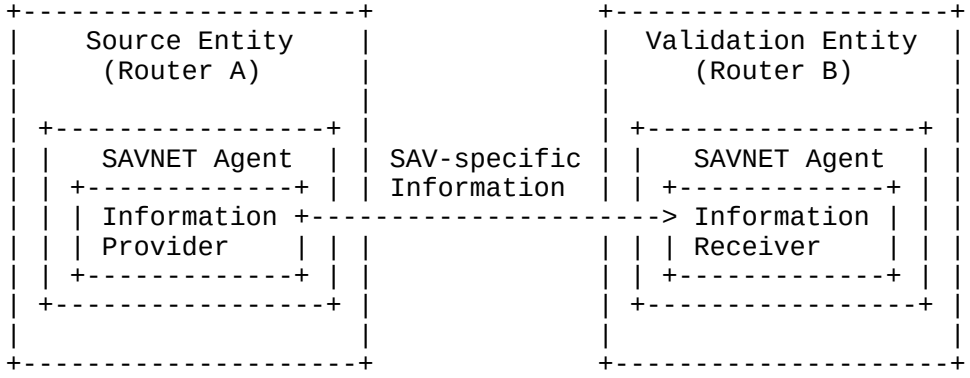

Figure 2: SAV-specific information flow

5.2. SAV-specific Information Communication

New intra-domain SAV solutions are expected to include a SAV-specific information communication mechanism that propagates SAV-specific information from source entities to validation entities. This mechanism may be realized either as a new protocol or as an extension to an existing one. This document does not specify the detailed protocol design or extensions; instead, it identifies the essential features that such a mechanism SHOULD support.

The SAV-specific information communication mechanism SHOULD define the data structure or format of SAV-specific information, as well as the operations related to communication (e.g., session establishment

and termination). In addition, the mechanism SHOULD enable source entities to notify validation entities of SAV-specific information updates in a timely manner, so that validation entities can maintain SAV rules based on the latest information.

5.2.1. Future SAV-specific Information Communication Protocol Requirements

To ensure the convergence and security of the communication, the session of the SAV-specific communication mechanism SHOULD satisfy the following requirements:

* The session MAY be long-lived or temporary, but it MUST provide sufficient assurance of reliability and timeliness to allow validation entities to update SAV rules promptly.

* Authentication SHOULD be supported prior to session establishment. While authentication is optional, the mechanism MUST provide the capability to perform it.

5.3. SAV-related Information

For intra-domain SAV, both SAV-specific information and local routing information can be used to support SAV decision-making.

5.3.1. SAV-specific Information

SAV-specific information is information dedicated to SAV and enables the generation of more accurate SAV rules. A SAVNET router can derive its own SAV-specific information from local routing information, local interface configurations, and/or other local configuration data. In addition, SAVNET routers acting as validation entities can obtain SAV-specific information from other SAVNET routers acting as source entities. By incorporating SAV-specific information provided by other routers, a validation entity can generate more accurate SAV rules than by relying solely on its local routing information.

SAV-specific information MAY also be provided by network operators. In this case, a SAVNET router can obtain the information from an operator-managed database or configuration system and incorporate it into the SAV rule generation process. This allows operators to provide additional guidance or correct information that might not be fully derivable from local routing or interface data.

For example, SAVNET routers connected to the same multi-homed non-BGP customer network can exchange locally known source prefixes of that network through SAV-specific information communication. By

processing both their own SAV-specific information, information received from peer SAVNET routers, and optionally operator-provided information, each router can identify all valid prefixes within the non-BGP customer network and thus avoid improper blocking in cases of asymmetric routing.

5.3.2. Routing Information

Routing information is used to compute packet forwarding rules and is stored in a router's RIB or FIB. Although not specialized for SAV, it has been widely used to infer SAV rules in existing uRPF-based mechanisms, such as strict uRPF and loose uRPF [RFC3704]. A SAVNET router acting as a validation entity can obtain routing information from its local RIB/FIB to generate SAV rules for certain prefixes when the corresponding SAV-specific information is unavailable.

5.4. SAV Rule Generation

Figure 3 illustrates the SAV rule generation process of a SAVNET router acting as a validation entity. The SAV Information Manager of the SAVNET Agent consolidates SAV-specific information received from other routers, the router's own SAV-specific information, and local routing information into the SAV Information Base. It then provides the consolidated information to the SAV Rule Generator. The SAV Rule Generator SHOULD preferentially use SAV-specific information to generate SAV rules for specific source prefixes. Local routing information is RECOMMENDED only when the corresponding SAV-specific information is unavailable.

The SAV Information Manager also supports diagnostic operations. Operators can inspect the contents of the SAV Information Base for monitoring or troubleshooting purposes.

For example, on a SAVNET router facing hosts or non-BGP customer networks, the SAVNET Agent processes SAV-related information to identify the prefixes belonging to the directly connected host or non-BGP customer network, and then generates SAV rules on the interface facing that host or network. Data packets received on that interface are considered invalid and SHOULD be dropped if their source addresses do not belong to the corresponding host or non-BGP customer network.

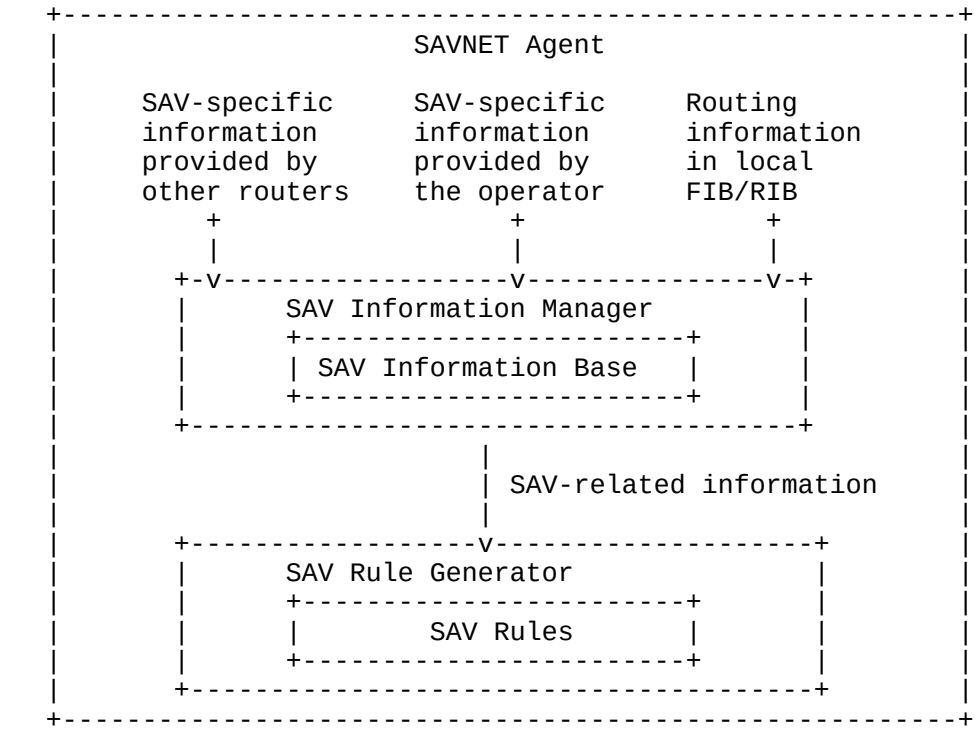

Figure 3: Workflow of SAV rule generation

For a SAVNET router facing an external AS, the SAVNET Agent processes SAV-related information to identify prefixes within the local AS and generates SAV rules on the interface facing another AS. Data packets received on that interface are considered invalid and SHOULD be dropped if their source addresses belong to the local AS.

In addition, if a SAVNET router also implements inter-domain SAVNET, its intra-domain SAVNET Agent SHOULD provide the intra-domain SAV-specific information to the inter-domain SAVNET Agent. This enables the inter-domain SAVNET Agent to generate inter-domain SAV rules or inter-domain SAV-specific information.

5.5. Data Plane SAV Filtering

This document primarily focuses on the SAV rule generation process in the control plane, including the exchange of SAV-specific information, the consolidation of SAV-related information, and the generation of SAV rules. For data-plane SAV filtering, SAVNET routers validate the source addresses of incoming data packets against the locally generated SAV rules and drop packets identified

as using spoofed source addresses. Consequently, the accuracy of data-plane SAV filtering depends entirely on the accuracy of the generated SAV rules. Further considerations for data-plane SAV can be found in [I-D.ietf-savnet-general-sav-capabilities].

6. Meeting the Design Requirements of Intra-domain SAVNET

The intra-domain SAVNET architecture is designed to satisfy the five design requirements defined in [I-D.ietf-savnet-intra-domain-problem-statement].

6.1. Accurate Validation

Existing intra-domain SAV mechanisms (e.g., strict uRPF) that rely solely on local routing information to generate SAV rules may incorrectly block legitimate traffic under asymmetric routing or hidden prefix conditions. Intra-domain SAVNET addresses this limitation by enabling routers to exchange SAV-specific information with one another. Each SAVNET router can use both the SAV-specific information received from other routers and its own SAV-specific information to generate more accurate SAV rules.

6.2. Automatic Update

In real intra-domain networks, the topology or prefixes of networks may change dynamically. The SAV mechanism MUST automatically update SAV rules in response to such network changes. In contrast, ACL-based SAV mechanisms require manual updates to accommodate network dynamics, resulting in high operational overhead.

Intra-domain SAVNET enables SAVNET routers to automatically exchange updates of SAV-specific information with one another. Upon receiving updated SAV-specific information from a source entity, SAVNET routers acting as validation entities can generate and update their SAV rules accordingly.

6.3. Incremental Deployment

Although an intra-domain network is typically under a single administration, incremental or partial deployment may still occur due to phased deployment or multi-vendor environments. In phased deployment scenarios, SAV-specific information from non-deploying routers is unavailable.

As described in Section 5.4, intra-domain SAVNET can adapt to incremental or partial deployment. To mitigate the impact of phased deployment, it is RECOMMENDED that routers facing the same set of hosts or non-BGP customer network adopt intra-domain SAVNET simultaneously so that all routing information of the set of hosts or non-BGP customer network can be identified.

In addition, SAVNET routers acting as validation entities are RECOMMENDED to support flexible validation modes and perform SAV filtering gradually to smooth the transition from partial to full deployment:

* Flexible Validation Modes: SAVNET routers acting as validation entities RECOMMENDED to support modes such as interface-based prefix allowlist, interface-based prefix blocklist, and prefix-based interface allowlist (see [I-D.ietf-savnet-general-sav-capabilities]). The first two modes operate at the interface scale, while the last operates at the device scale. Under incremental or partial deployment, SAVNET routers SHOULD select the appropriate validation mode according to the acquired SAV-specific information. For example, if a SAVNET router can identify all prefixes in its non-BGP customer network using acquired SAV-specific information, an interface-based prefix allowlist containing these prefixes can be applied to that interface. Otherwise, an interface-based prefix blocklist or prefix-based interface allowlist SHOULD be used to avoid improper blocking.

* Gradual SAV-invalid Filtering: Validation entities are RECOMMENDED to apply filtering for invalid packets gradually. Initially, routers may take conservative actions on packets identified as invalid. For instance, packets may not be discarded at the start of deployment; instead, sampling can be conducted for measurement and analysis. Subsequently, rate-limiting or redirecting actions can be applied to packets with invalid results. These conservative actions reduce the risk of incorrectly blocking legitimate traffic while still providing protection for the network. Full filtering actions SHOULD be enabled only after confirming that no improper blocking occurs.

6.4. Convergence

When SAV-related information changes, the SAVNET Agent MUST be able to detect the changes promptly and update SAV rules based on the latest information. Otherwise, outdated SAV rules may cause legitimate packets to be blocked or allow spoofed packets to be accepted.

Intra-domain SAVNET requires routers to update SAV-specific information and refresh SAV rules in a timely manner. Because SAV-specific information originates from source entities, those entities MUST promptly send updated SAV-specific information to validation entities. Therefore, the propagation speed of SAV-specific information is a key factor affecting convergence. Considering that routing information and SAV-specific information can be originated and advertised in similar ways, SAV-specific information SHOULD propagate at least as quickly as routing information.

6.5. Security

Intra-domain SAVNET is designed so that it does not introduce additional security threats to the existing routing architecture or protocols.

7. Manageability Considerations

The architecture provides a general framework for exchanging SAV-specific information between routers and generating SAV rules based on both SAV-specific information and local routing information. Protocol-independent mechanisms SHOULD be provided for operating and managing SAV-related configurations. For example, a YANG data model for SAV configuration and operation is RECOMMENDED to simplify management.

Mechanisms for diagnosis and the collection of necessary logging information SHOULD be provided. The SAV Information Base SHOULD store information that may not be directly used for SAV rule generation but is useful for management purposes.

Furthermore, the SAV-specific information communication mechanism SHOULD include monitoring and troubleshooting capabilities to support the efficient operation of the architecture.

8. IANA Considerations

This document has no IANA requirements.

9. Contributors

Mingqing Huang

Email: huangmq@vip.sina.com

Fang Gao

Email: fredagao520@sina.com

10. Acknowledgements

Many thanks to the valuable comments from: Igor Lubashev, Alvaro Retana, Aijun Wang, Joel Halpern, Jared Mauch, Kotikalapudi Sriram, Rdiger Volk, Jeffrey Haas, Xiangqing Chang, Changwang Lin, Xueyan Song, etc.

11. References

11.1. 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>.

11.2. Informative References

[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>.

[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>.

Authors' Addresses

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

Jianping Wu
Tsinghua University
Beijing
China
Email: jianping@cernet.edu.cn

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

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

Li Chen
Zhongguancun Laboratory
Beijing
China
Email: lichen@zgclab.edu.cn