SAVNET
Internet-Draft
Intended status: Informational
Expires: 28 May 2026

L. Qin
Zhongguancun Laboratory
D. Li
Tsinghua University

24 November 2025

Considerations on Authoritative Information for Source Address Validation
draft-qin-savnet-authoritative-information-00

Abstract

Source Address Validation (SAV) prevents source address spoofing. This document explains that SAVNET relies on authoritative information. It also describes how to handle missing or conflicting data. The guidance minimizes improper blocks and improper permits while supporting reliable SAV enforcement.

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 28 May 2026.

Table of Contents

1. Introduction

Source Address Validation (SAV) prevents source address spoofing and enforces BCP38 [RFC2827], BCP84 [RFC3704], and [RFC8704]. Networks rely on authoritative information to determine which source addresses are legitimate. However, networks may encounter situations where this information is missing or conflicting.

This document provides a conceptual framework for understanding authoritative information in the context of SAVNET, including:

* What constitutes authoritative information and which sources can be trusted.

* How networks should handle missing authoritative information.

* How to reconcile conflicting authoritative sources.

* The role of non-authoritative information as a reference in contextual or policy-based decisions.

By clarifying these principles, the document aims to guide the design and operation of SAV mechanisms that are both secure and operationally reliable, while minimizing improper blocks and improper permits.

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. What Constitutes Authoritative Information

Authoritative information determines which source addresses are legitimate. To be considered authoritative, information should meet the following criteria:

* Organizational authority: The source must be maintained by an entity that has recognized authority over the relevant prefixes or networks.

* Verifiability: The source must provide a mechanism to verify its correctness and authenticity, such as cryptographic validation.

* Timeliness: The information must reflect the current operational state and be updated promptly to avoid reliance on stale or outdated data.

* Integrity and security: The source must be resistant to unauthorized modifications or tampering.

Based on these criteria, authoritative information in SAVNET typically includes:

* RPKI objects: Cryptographically verifiable objects such as ROAs (Route Origin Authorizations) [RFC9582], ASPAs (Autonomous System Provider Authorizations) [I-D.ietf-sidrops-aspa-profile], and TOAs (Traffic Origin Authorizations) [I-D.qin-sidrops-toa] that provide explicit assertions about origin authorization or transit authorization.

* Local or static configuration: Operator-defined rules specifying source address permissions for hosts, non-BGP customer networks, or external ASes.

Note on routing information: Routing information from intra-domain or inter-domain protocols (e.g., IGP, BGP) may indicate reachable prefixes and their origins, but it cannot be considered authoritative by itself because it may include unauthorized or forged routes. If routing information is used to derive SAV rules, it should be validated—such as via RPKI-based Route Origin Validation (ROV)—before being treated as a trusted source.

By defining authoritative information in this way, SAV mechanisms can rely on sources that provide sufficient guarantees of correctness, integrity, and timeliness, reducing the risk of improper blocks or improper permits in filtering.

3. When Authoritative Information Is Missing

Networks may encounter situations where authoritative information about a particular prefix or source entity is unavailable. Such situations can arise for various reasons, including:

* The relevant RPKI objects (e.g., ROAs, ASPAs, TOAs) do not exist or have not yet been published.

* Local configuration has not been defined for a newly connected host, non-BGP customer network, or external AS.

When authoritative information is missing, a network must decide how to handle traffic from the corresponding source addresses. Several approaches can be considered:

* Conservative approach: Treat the source addresses as unauthorized and block traffic. This minimizes the risk of accepting spoofed packets but may lead to legitimate traffic being dropped.

* Permissive approach: Allow traffic from the source addresses by default. This avoids accidental disruption of legitimate communications but increases the risk of accepting spoofed packets.

* Contextual or policy-based approach: Apply local policies or heuristics to determine the appropriate action. In this approach, networks may use non-authoritative information—such as routing information, historical traffic patterns, or operational context—as a reference to make informed decisions. This allows the network to balance security and operational continuity when authoritative information is missing, while still avoiding treating non-authoritative sources as fully trusted.

The choice of approach depends on the operational environment, risk tolerance, and the expected reliability of other sources of authoritative information. Networks should document their chosen strategy and ensure consistency across edge interfaces to maintain predictable and secure SAV behavior.

Note: Only information that meets the criteria for authoritative sources—verifiable, secure, timely, and maintained by an entity with recognized authority—should be used to make definitive filtering decisions. Missing authoritative information highlights the importance of having fallback strategies to balance security and operational continuity.

4. When Authoritative Sources Conflict

Networks may encounter situations where multiple sources of authoritative information provide overlapping or apparently conflicting statements about the legitimacy of a source address or prefix. Such conflicts can arise, for example, when:

* Different RPKI objects (ROAs, ASPAs, TOAs) provide overlapping assertions for the same prefix.

* Local or static configurations overlap with information from other authoritative sources.

Networks should treat all authoritative sources as equally credible and merge information from all sources. Any address or prefix authorized by at least one source should be considered legitimate. This approach ensures that no legitimate source address is incorrectly blocked, reducing improper blocks while maintaining reliable SAV enforcement.

Fallback and reference to non-authoritative information: When authoritative information is incomplete or missing, non-authoritative information—such as routing data—may be used as a reference within a contextual or policy-based approach (see Section 3) to help inform decisions, but it cannot be relied upon as definitive.

5. Discussion and Next Steps

This document provides a conceptual framework for understanding authoritative information in SAVNET, addressing scenarios where information is missing or conflicting. The following points highlight key considerations for SAV design and operations:

* Definition of authoritative information: Networks must rely on sources that are verifiable, secure, timely, and maintained by recognized authorities, such as RPKI objects (ROAs, ASPAs, TOAs), SAV-specific signaling with security guarantees, or operator-defined local/static configuration.

* Handling missing information: When authoritative information is unavailable, fallback strategies— conservative, permissive, or contextual/policy-based using non-authoritative information as reference— should be defined.

* Conflict resolution: Conflicting authoritative sources should be merged to ensure all authorized prefixes and source addresses are preserved.

* Open questions: Additional work may include defining authoritative attributes in greater detail, coordinating with other working groups (e.g., GROW, OSPAWG) for operational guidance, and specifying mechanisms to securely exchange SAV-specific signaling information.

This framework provides a foundation for discussion and standardization of SAV mechanisms that rely on authoritative information, ensuring both security and operational reliability.

6. Security and Operational Considerations

Reliable SAV enforcement depends on correct identification of legitimate source addresses. Inaccurate, missing, or conflicting authoritative information can lead to operational and security risks, including:

* Improper blocks: Legitimate traffic is blocked, potentially disrupting services.

* Improper permits: Spoofed or unauthorized traffic is accepted, increasing vulnerability to attacks.

Mitigation strategies include:

* Validation and cross-checking: Ensure authoritative sources are consistent and verifiable.

* Timely updates and monitoring: Maintain freshness of authoritative information to avoid reliance on stale data.

* Documentation and operational procedures: Clearly define policies for missing, inaccurate, or conflicting authoritative information, including fallback handling.

* Fallback and reference mechanisms: Non-authoritative information (e.g., routing data) may be used as a reference in contextual or policy-based approaches but must never be treated as definitive.

* Merge strategy for conflicts: All authoritative sources should be combined, ensuring that any prefix or source address authorized by at least one source is accepted, minimizing improper blocks.

By implementing these practices, networks can maintain reliable SAV enforcement while reducing both security and operational risks. This approach emphasizes using authoritative information wherever possible and leveraging non-authoritative data only as a reference when necessary.

7. IANA Considerations

This document does not request any IANA allocations.

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>.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

[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>.

[I-D.ietf-sidrops-aspa-profile] Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-20, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20>.

Authors' Addresses

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

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