SAVNET
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

N. Geng
Huawei
L. Qin
Zhongguancun Laboratory
K. Sriram
USA NIST
D. Li
Tsinghua University

2 March 2026

Source Prefix Advertisement for Inter-domain SAVNET
draft-geng-savnet-inter-domain-spa-02

Abstract

This document proposes a mechanism that enables neighboring ASes (Source ASes) to actively advertise their locally observed Customer Cone and prefix information via a new inter-domain message called Source Prefix Advertisement (SPA). The validating AS then combines this SPA-carried information with local source address validation-related information to construct more accurate prefix allowlists for interfaces connected to Source ASes.

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 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The EFP-uRPF technique [RFC8704] performs effective source address filtering on customer interfaces and lateral peer interfaces. It constructs a source prefix allowlist for each customer or lateral peer interface based on the Customer Cone of the neighboring AS. Data packets received from a customer or lateral peer are only permitted if their source addresses fall within the Customer Cone of that neighbor. The enforcement is thus strictly limited to the Customer Cone of the respective neighbor, which includes the AS and the prefixes originated or delegated by the customer or lateral peer.

Building an accurate prefix set representing the Customer Cone is therefore critical to the correct operation of these source address validation mechanisms. However, a locally constructed Customer Cone prefix set may not be accurate and can differ from the actual Customer Cone prefix set observed by the neighbor (i.e., the customer

or lateral peer). This discrepancy can arise due to various factors, including BGP no-export communities, Direct Server Return (DSR), complex inter-domain commercial relationships (e.g., partial transit relationships), and other routing policy differences. Such inaccuracies may result in false positives (legitimate packets being incorrectly filtered) or false negatives (illegitimate packets being incorrectly allowed), which degrade the effectiveness and dependability of the source address validation mechanism. A concrete analysis of existing inter-domain Source Address Validation (SAV) mechanisms can be found in [I-D.ietf-savnet-inter-domain-problem-statement].

To address this problem, this document proposes a mechanism called Inter-domain Source Prefix Advertisement (SPA). A neighboring AS (either a customer or a lateral peer) actively advertise the prefix information and Customer Cone information that it observes locally. The advertised information helps the local AS construct a more accurate prefix allowlist on the corresponding customer or lateral peer interface. This mechanism follows the idea presented in [I-D.ietf-savnet-inter-domain-architecture] regarding the exchange of SAV-specific information between ASes. To carry such source prefix information between ASes, a new inter-domain SPA message is defined.

Protocol extensions for the mechanism proposed in this document are out of scope.

1.1. Terminology

Source Prefix Advertisement (SPA): The process that an AS can actively advertise the prefix information and Customer Cone information that it observes locally to a neighboring AS through the messages called SPA messages.

Source AS: The AS which originates SPA messages to the Validating AS. Source AS is typically the customer or lateral peer of Validating AS.

Validating AS: The AS which receives SPA messages from the Source AS, generates SAV rules, and conducts source address validation. Validating AS is typically the provider or lateral peer of Source AS.

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. Inter-domain Source Prefix Advertisement

The mechanism proposed in this document generally consists of the following three steps:

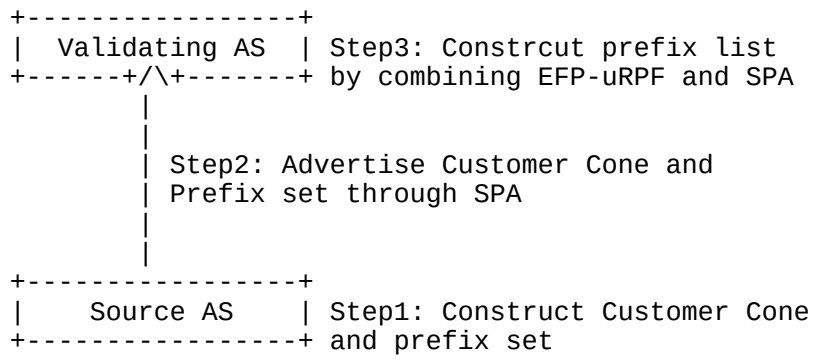

Figure 1: An overview of the inter-domain SPA mechanism.

2.1. Step 1: Construct Customer Cone and Prefix Set at Source AS

First, the neighboring AS, referred to as the Source AS, constructs the Customer Cone and its corresponding prefix set based on its local observations, with specific considerations for the following factors to ensure the comprehensiveness and accuracy of the constructed set:

Step 1.1: The Source AS constructs the Customer Cone (which includes itself) and the corresponding prefix set by integrating multiple authoritative data sources, primarily including local BGP routing information and RPKI data. This integration ensures that the prefix set is initially grounded in verifiable and widely-recognized routing and resource validation information.

Step 1.2: For prefixes hidden in the DSR scenarios where prefixes that are not propagated through standard BGP routing and thus not captured by the above data sources, the Source AS adds such hidden prefixes to the constructed prefix set through administrative configuration. This step addresses the invisibility of DSR-related prefixes in normal routing propagation, preventing their omission from the Customer Cone.

Step 1.3: If the Source AS itself acts as a Validating AS for its downstream neighboring ASes (which serve as Source ASes relative to it), it incorporates the prefix information carried in the SPA messages received from these downstream Source ASes. By integrating this SPA-sourced information with the locally derived Customer Cone and prefix data, the Source AS constructs a complete and accurate prefix set that reflects both its own resource scope and the valid prefixes of its downstream neighbors.

2.2. Step 2: Advertise Customer Cone and Prefix Set through SPA

Second, the Source AS generates SPA messages — a new inter-domain message specifically defined in this document to carry Customer Cone and prefix information between ASes — and advertises the locally observed Customer Cone and its corresponding prefix set to the adjacent Validating AS (the AS responsible for performing source address validation on the interface connecting the two ASes). The detailed implementation of this step is as follows:

The Source AS may transmit the following required information to the Validating AS via one or more SPA messages:

* The set of AS numbers belonging to the Customer Cone observed locally by the Source AS. This set includes the Source AS itself and all ASes within its Customer Cone, providing the Validating AS with the hierarchical scope of the Source AS’s Customer Cone.

* The source prefix set of the Customer Cone observed locally by the Source AS. This set comprises all valid prefixes originated, delegated, or associated with the Customer Cone (including DSR-hidden prefixes added via administrative configuration, as specified in Step 1).

* The AS number of the Source AS. This field serves as an identifier to enable the Validating AS to associate the received SPA message with the correct neighboring AS and the corresponding interface, avoiding confusion when multiple neighbors send SPA messages.

* An Update/Withdraw Flag. This flag is used to explicitly indicate whether the information carried in the SPA message is intended to update the existing Customer Cone or prefix set information (Update Flag) or to withdraw previously advertised Customer Cone or prefix set information (Withdraw Flag). This ensures the Validating AS can dynamically maintain the accuracy of its prefix allowlists as the Source AS’s Customer Cone changes over time.

Upon receiving SPA messages from the Source AS, the Validating AS may propagate the received Customer Cone and prefix information within its own AS. However, the Validating AS MUST NOT propagate the received SPA messages to other ASes.

It should be noted that detailed implementation aspects such as the specific session establishment method between the Source AS and the Validating AS, potential capability negotiation processes (e.g., confirming support for SPA messages), and the encapsulation format of SPA messages are out of the scope of this document and shall be defined in subsequent protocol extension documents.

2.3. Step 3: Construct Prefix List by Combining EFP-uRPF and SPA

Third, the Validating AS constructs an accurate prefix allowlist for the interface connecting to the Source AS, following the core logic of the EFP-uRPF algorithm [RFC8704] and integrating the information received from SPA messages. The detailed implementation of this step is as follows:

Step 3.1: The Validating AS enables the EFP-uRPF algorithm (or some other algorithms like BAR-SAV [I-D.ietf-sidrops-bar-sav]) on the specific interface through which it receives SPA messages from the Source AS. This ensures that the source address validation mechanism is activated for the connection to that neighbor, aligning with the foundational approach of EFP-uRPF for customer and lateral peer interfaces.

Step 3.2: The Validating AS merges two sets of information to form a complete and accurate prefix set for the interface: one is the Customer Cone and its corresponding prefix set generated locally by the Validating AS in accordance with the EFP-uRPF algorithm specified in [RFC8704] (integrating local BGP routing information, RPKI data, and other relevant sources); the other is the Customer Cone and prefix set information carried in the SPA messages advertised by the Source AS.

This merging process supplements the locally generated prefix set with the Source AS’s observed Customer Cone and prefix information— information that the Validating AS may not be able to obtain through existing mechanisms due to factors such as BGP no-export communities or DSR. As a result, the combined prefix set becomes more comprehensive and accurate, effectively mitigating the risks of false positives and false negatives caused by incomplete locally constructed Customer Cone prefix sets.

2.4. Special Usage of Inter-domain SPA

In the descriptions above, the information carried in SPA messages is merged into the information generated by the EFP-uRPF algorithm to enhance the comprehensiveness of the prefix allowlist. This section introduces a special usage of SPA messages: the Source AS may advertise SPA messages to instruct the Validating AS to remove specific AS numbers or source prefixes from the information generated by the EFP-uRPF algorithm on the corresponding interface.

A typical application scenario for this special usage involves partial transit services. Specifically, a customer AS under the Source AS may purchase partial transit services for certain address prefixes from the Source AS. Traffic related to these address prefixes is only forwarded within the Customer Cone of the Source AS and will not access the external Internet through the connection between the Source AS and the Validating AS.

In this scenario, the Source AS will not advertise these address prefixes to the Validating AS via BGP, as the partial transit service does not require propagating these prefixes to the external Internet. However, the Validating AS may still include these prefixes in the prefix allowlist of the interface connected to the Source AS. This can occur in two common cases: first, the customer AS of the Source AS may advertise these prefixes through other ASes, which are then propagated to the Validating AS; second, the customer AS may have registered RPKI ROA data for these prefixes, which the Validating AS obtains and uses to construct the prefix allowlist.

To address this issue, the Source AS can advertise an SPA message carrying these specific address prefixes, explicitly instructing the Validating AS not to include these prefixes in the source prefix allowlist of the connected interface. This approach offers a key benefit: if the Source AS inadvertently leaks the prefixes related to the partial transit service, or if forged traffic using these prefixes originates within the Source AS’s Customer Cone and is sent to the external Internet, the Validating AS can effectively intercept such traffic by excluding these prefixes from the allowlist, thereby enhancing the security of inter-domain source address.

3. Operational and Deployment Considerations

TBD

4. Security Considerations

The mechanism proposed in this document operates between adjacent ASes. For the secure exchange of SPA messages between the Source AS and the Validating AS, existing BGP session protection mechanisms can be adopted, including GTSM/TTL-security [RFC5082], BGP-MD5, and TCP-AO [RFC5925]. These mechanisms help ensure the confidentiality, integrity, and authenticity of SPA messages, preventing unauthorized tampering, eavesdropping, or spoofing of the message content during transmission. More Detailed guidelines can be found in Section 5 of [RFC7454] and Section 3 of [I-D.ietf-grow-bgpopsecupd].

Notably, the scope of influence of the Source AS is strictly limited to the prefix allowlist of the interface on the Validating AS that is directly connected to the Source AS. The information advertised by the Source AS via SPA messages directly determines whether the legitimate traffic sent from the Source AS to the Validating AS can pass source address validation, as well as whether attacks originating from the Source AS can be effectively intercepted by the Validating AS.

This limited scope of influence inherently mitigates the risk of malicious behavior by the Source AS. Specifically, the Source AS has little incentive to intentionally advertise incorrect or malicious SPA information. Any false or malicious SPA advertisements would either result in legitimate traffic from the Source AS being incorrectly filtered (a false positive) or fail to intercept attacks originating from the Source AS (a false negative)—both of which are detrimental to the Source AS’s own network connectivity and security.

5. IANA Considerations

There is no IANA requirement.

Acknowledgements

Thanks a lot for the comments from Jeff Hass and Igor Lubashev.

References

Normative References

[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>.

[I-D.ietf-savnet-inter-domain-problem-statement]
Li, D., Qin, L., Liu, L., Huang, M., and K. Sriram, "Gap Analysis, Problem Statement, and Requirements for Inter-Domain SAV", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-problem-statement-14, 14 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-14>.

[I-D.ietf-savnet-inter-domain-architecture]
Li, D., Chen, L., Geng, N., Liu, L., and L. Qin, "Inter-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-architecture-03, 1 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-architecture-03>.

[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>.

Informative References

[I-D.ietf-sidrops-bar-sav]
Sriram, K., Lubashev, I., and D. Montgomery, "Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)", Work in Progress, Internet-Draft, draft-ietf-sidrops-bar-sav-08, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-bar-sav-08>.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <https://www.rfc-editor.org/info/rfc5082>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <https://www.rfc-editor.org/info/rfc7454>.

[I-D.ietf-grow-bgpopsecupd]
Fiebig, T. and N. Hilliard, "BGP Operations and Security", Work in Progress, Internet-Draft, draft-ietf-grow-bgpopsecupd-12, 12 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bgpopsecupd-12>.

Authors' Addresses

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

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

Kotikalapudi Sriram
USA NIST
Gaithersburg, MD 20899,
United States of America
Email: ksriram@nist.gov

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