

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 15 July 2022

D. Li
J. Wu
Tsinghua University
M. Huang
Huawei
L. Qin
Tsinghua University
N. Geng
Huawei
11 January 2022

Distributed Source Address Validation (DSAV) Framework
draft-li-dsav-framework-01

Abstract

This document provides an overall framework of Distributed Source Address Validation (DSAV) including both intra-domain and inter-domain levels. It also describes related considerations.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 8174](#) [[RFC8174](#)].

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 15 July 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

DSAV Framework

January 2022

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	DSAV Framework	3
3.1.	Separate Source Information Advertisement	5
3.2.	Destination Information Identifier	6
4.	Accuracy	6
5.	Consistency	7
6.	Deployability	8
7.	Security	8
8.	Normative References	8
	Authors' Addresses	9

[1.](#) Introduction

Source address validation (SAV) is important to mitigate source address spoofing and contribute to the Internet security. However, existing SAV mechanisms have limitations in accuracy. Specifically, intra-domain SAV mechanisms (e.g. strict uRPF[RFC3704]) usually improperly block legitimate traffic in the case of routing asymmetry, while inter-domain SAV mechanisms (e.g. loose uRPF[RFC3704] and EFP-uRPF[RFC8704]) provide overly loose SAV rules which can improperly permit spoofed traffic. The root cause of their limitations is that they all achieve SAV based on local forwarding information base (FIB) or routing information base (RIB), which may not match the real forwarding direction from the source. In order to guarantee the accuracy, SAV should follow the real data-plane forwarding path.

This document provides a framework to generate accurate SAV rules on routers at both intra-domain and inter-domain levels. In Distributed Source Address Validation (DSAV) framework, each router or AS originates individual protocol messages to its neighbors, carrying

local source information and corresponding destination information which takes the neighbor as the next hop. Upon receiving a protocol message, the router or AS identifies a valid incoming interface for the related source addresses. After that, it decides whether to terminate the message or further relay new protocol messages to its

neighbors based on the destination information of the received message. In this way, the source information will propagate through all possible forwarding paths originated from the source.

This document also describes basic considerations related to DSAV, including accuracy, consistency, deployability, and security.

[2.](#) Terminology

Some definitions during a propagation process:

- * Node: A router or AS in this document.
- * Initial node: The node generating original protocol messages.
- * Terminal node: The node terminating the received protocol message from a neighbor node.

[3.](#) DSAV Framework

DSAV provides a framework for distributedly generating SAV rules on nodes at both intra-domain and inter-domain levels. Intra-domain SAV avoids source address spoofing within the same AS. Inter-domain SAV prevents source address spoofing among ASes. Despite of different application scenarios and protocol details, DSAVs at the two levels hold the same key idea. The core workflow of DSAV is briefly described as follows:

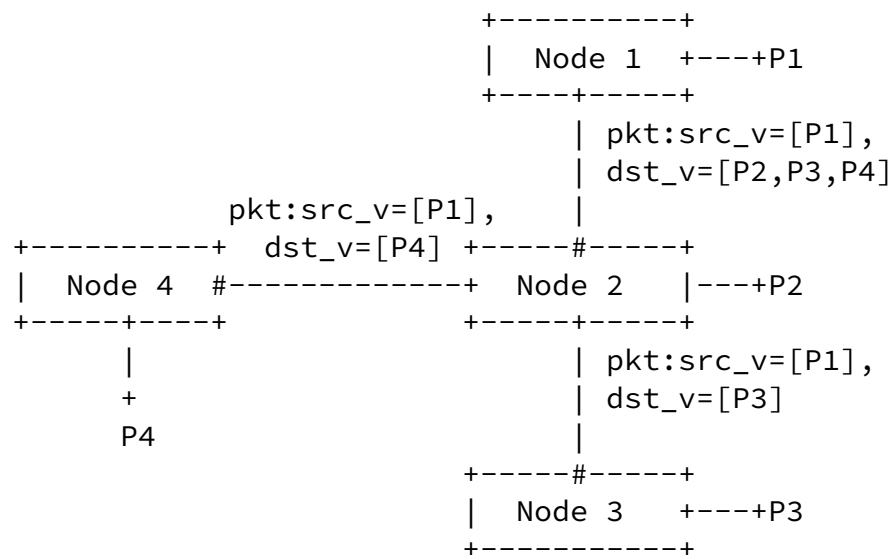
- a. An initial node A generates an original message for each neighbor node, carrying the source prefixes originated locally and the destination prefixes which take the neighbor node as the next hop.

- b. When node B receives a protocol message at interface I, it determines interface I as a valid incoming interface for the source prefixes of the received message. In other words, it generates the SAV rule <source prefixes of A, interface I>.

- c. After that, node B checks the destination prefixes of the received message against its local FIB/RIB. If the next hop of all the destination prefixes point to its local subnets/networks, the message is terminated; otherwise, node B relays new messages. It groups all destination prefixes according to their next-hop node. For each next-hop node C, node B generates a new message destined to C, with the corresponding destination prefixes taking node C as the next hop. The source prefixes in each relayed message should keep the same.
- d. In DSAV, with the exception of some special cases, such as multipath routing, nodes usually receive only one message originated from each source.
- e. The above steps can be executed periodically or when any of source prefixes, destination information, or forwarding paths change. The updated message should add updated SAV rules or delete outdated SAV rules for the affected Nodes. Particularly, to reduce the communication overhead, only the changed information should be propagated again when dynamic updating.

Figure 1 illustrates the workflow of DSAV. The network runs some routing protocols such as OSPF, IS-IS, or BGP among the four nodes. Each node owns a unique source prefix (e.g. P1 for Node 1). Let's consider the propagation process where Node 1 is the initial node. Node 1 sends an original message to the neighbor Node 2, carrying its source prefix (i.e., P1) and destination prefixes whose next-hop node in FIB is Node 2 (i.e., P2, P3, P4). When Node 2 receives the message, it specifies interface '#' as the valid incoming interface

for prefix P1. Then, Node 2 checks the destination prefixes according to its local FIB. Since P3 and P4 are not Node 2's source prefixes, it should relay messages to the corresponding next-hop nodes, i.e. Node 3 and Node 4. The message destined to Node 3 carries the destination prefix P3, while the message destined to Node 4 carries the destination prefix P4. The source prefix in each relayed message keeps the same. When Node 3 or Node 4 receives the message from Node 2, it also learns and enables the SAV rule <P1, interface '#>' but terminates the message.



- P1, P2, P3, and P4 are prefixes belonging to Node 1, 2, 3, and 4, respectively.
- Node 1 is the initial node, and Node 3 and Node 4 are the terminate nodes in this propagation process.
- '#' means the legitimate interface for the data-plane packets with source addresses of P1.

Figure 1: The workflow of DSAV

[3.1.](#) Separate Source Information Advertisement

Containing source prefixes and destination prefixes in a message sometimes induces much unnecessary overhead. For example, a change on a destination prefix or forwarding path will make the initial node advertise its source prefixes again even though no changes happen on its local source prefixes at all. A separate source information advertisement is taken to tackle the above problem.

Particularly, a node can be represented by a node ID (e.g., the router-ID for a router or the ASN for an AS). For each initial node, its source prefixes together with its node ID can be advertised to other nodes through broadcast or existing underlay routing protocols (such as OSPF, IS-IS, and BGP). Then, other nodes will know the mapping from a node ID to a list of source prefixes. Now, the protocol message does not need to carry a long list of source prefixes whose field can be replaced with just one source node ID.

[3.2.](#) Destination Information Identifier

Although separate source information advertisement help reduce communication overhead, including destination prefixes in messages can still be costly, especially in inter-domain scenarios with a large number of destination prefixes.

Similarly, a list of destination prefixes can also be replaced with a destination node IDs (e.g., the router-ID for a router or the ASN for an AS). Considering that a node may have hundreds of different prefixes, this can significantly reduce overhead. However, the replacement of destination prefixes may result in accuracy problems in some scenarios where the destination prefixes belonging to a same destination node have different forwarding paths. Some additional mechanisms need to be imported into these scenarios.

[4.](#) Accuracy

The goal of DSAV is to achieve high accuracy, i.e., avoid improper block problems and try best to reduce improper permit problems. The improper block problem means legitimate traffic is mistakenly dropped. The improper permit problem means spoofed traffic is mistakenly passed.

The accuracy of DSAV is determined by the accuracy of source information advertisement and propagation process. The incompleteness of received source information can compromise the accuracy of SAV. So, each initial node should discover and advertise local source information carefully with the help of either automatic programs or manual configurations. In the case of incomplete source information, the node can take a remedy method at the data plane, i.e., only drop packets with known source addresses but coming from invalid interfaces. Packets with unknown source addresses should be accepted by default. More details will be described in [Section 6](#).

The key of DSAV is to generate SAV rules strictly following the real data-plane forwarding paths. Any factor that can affect forwarding should be considered. Here are three kinds of common forwarding cases:

- * Only FIBs affect forwarding.

- * ECMP (Equal-cost multi-path routing) or UCMP (Unequal-cost multi-path routing). To achieve multi-path routing, hashing functions are usually taken, which map packet header field values (e.g., source/destination IP address, source/destination port number, protocol number) to candidate next hops. Packets with the same destination IP address may be forwarded to different next hops.
- * ACL redirection. An ACL rule can have multiple match fields, and

the match field of destination IP addresses can be included or not in an ACL rule. So, similar to ECMP/UCMP, the packets with the same destination IP address may have different next-hop interfaces.

As described in Section 3, DSAV can work well in the first case. To ensure accuracy in arbitrary routing scenarios, the last two cases should also be considered.

[5.](#) Consistency

The factors influencing the accuracy of DSAV may change with time. Such changes will lower the performance of SAV and lead to improper block or improper permit problems. The SAV rules generated through DSAV should be updated in time so as to keep consistent with routing states. The consistency of DSAV is important for the SAV framework working well in real networks.

A simple method is to send updated messages periodically. An aging mechanism can also be used for SAV rules. That is, SAV rules will expire after a period of time. However, these solutions may take much time before eliminating improper block and improper permit problems. Some quick convergence mechanisms are necessary to achieve consistency of DSAV in time. Here are some preliminary ideas for different cases:

- * Source information changes. A node sends new source information advertisements immediately upon discovering its local source prefixes change.
- * Routing state changes. When route configuration or topology changes, the forwarding path to a destination prefix may change. These changes can trigger the initial node to generate updated messages for the changed forwarding paths. Then, new SAV rules can be added and outdated SAV rules can be withdrawn at other nodes quickly. For the scenarios where fast reroute (FRR) is deployed, the initial node can send message to the backup forwarding paths in advance, and the backup SAV rules can be installed for fast convergence under failures.

[6.](#) Deployability

It is difficult to ensure that all nodes deploy DSAV simultaneously, especially at inter-domain level. In this case, each node only learns partial source address information or incomplete legitimate incoming interfaces for a source prefix, which can lead to improper block problems. Therefore, DSAV should support incremental and partial deployment.

When deployed incrementally or partially, nodes should still avoid improper block problems and minimize improper permit problems based on incomplete SAV tables. The process of data-plane SAV is as follows:

- * For the source address whose source address information and incoming interface information are fully learned, nodes can strictly validate the authenticity by querying <source prefix, interface> in SAV tables.
- * For the source address whose source address information or incoming interface information is only partially learned or even not learned, nodes should pass those packets by default to avoid improper block problems, since it is hard to identify the authenticity with incomplete information.

Since inter-domain topology is greatly complex and ASes are managed by individual network operators, determining whether the incoming interface information for a source prefix is learned completely is a real challenge. Besides, in DSAV framework, neighboring (next-hop) node plays an important role in the propagation of probing packets, namely, a node cannot send or receive any probing packet if its neighboring nodes don't support DSAV. Hence, at inter-domain level, DSAV recommends incremental deployment by customer cones. This deployment pattern ensures that each AS learns complete source address information and incoming interface information for other ASes within the same customer cone. With the merger of different customer cones where DSAV is deployed, the deployment scope of DSAV will gradually expand, and the defense capability against source address spoofing will gradually increase.

7. Security

TBD

8. Normative 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>>.
- [RFC5210] Wu, J., Bi, J., Li, X., Ren, G., Xu, K., and M. Williams, "A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience", [RFC 5210](#), DOI 10.17487/RFC5210, June 2008, <<https://www.rfc-editor.org/info/rfc5210>>.
- [RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", [RFC 7039](#), DOI 10.17487/RFC7039, October 2013, <<https://www.rfc-editor.org/info/rfc7039>>.
- [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>>.
- [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>>.

Authors' Addresses

Dan Li
Tsinghua University
Beijing
China

Email: tolidan@tsinghua.edu.cn

Jianping Wu
Tsinghua University
Beijing
China

Email: jianping@cernet.edu.cn

Internet-Draft

DSAV Framework

January 2022

Mingqing Huang
Huawei
Beijing
China

Email: huangmingqing@huawei.com

Lancheng Qin
Tsinghua University
Beijing
China

Email: qlc19@mails.tsinghua.edu.cn

Nan Geng
Huawei
Beijing
China

Email: gengnan@huawei.com

