Network Working Group
Internet-Draft
Intended status: Informational
Expires: 11 January 2023

D. Li
J. Wu
L. Qin
Tsinghua University
M. Huang
N. Geng
Huawei
10 July 2022

Source Address Validation in Intra-domain Networks (Intra-domain SAVNET) Gap Analysis, Problem Statement and Requirements

draft-li-savnet-intra-domain-problem-statement-00

Abstract

Source Address Validation in Intra-domain Networks (Intra-domain SAVNET) aims to make improvements to existing intra-domain Source Address Validation (SAV). This document provides the gap analysis of existing intra-domain SAV mechanisms, describes the fundamental problems, and defines the requirements for improvements.

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 11 January 2023.

Table of Contents

1. Introduction

Source Address Validation (SAV) is important for defending against source address spoofing attacks and accurately tracing back to the attackers. To be as effective as possible, SAV should be implemented as close to the source as possible. Given numerous access networks managed by different operators, it is difficult to require all access networks to deploy SAV. When some access networks do not deploy SAV,

intra-domain SAV helps filter out spoofed packets as close to the source as possible.

Ingress filtering [RFC2827] [RFC3704] is the current practice of intra-domain SAV. It is recommended to be deployed at the ingress point of each subnet to prevent spoofed packets from entering the intra-domain network. Static Access Control List (ACL) is a typical implementation of ingress filtering. Operators can configure some matching rules to specify which source addresses are acceptable (or unacceptable). The information of ACL should be updated manually so as to keep consistent with the newest filtering criteria, which inevitably limits the flexibility and accuracy of SAV. Strict unicast Reverse Path Forwarding (uRPF) [RFC3704] is another suitable solution to achieve ingress filtering in intra-domain networks. Routers deploying strict uRPF accept a data packet only when i) the local forwarding information base (FIB) contains a prefix encompassing the packet's source address and ii) the corresponding forwarding action for the prefix matches the packet's incoming port. Otherwise, the packet will be blocked. However, in the scenario where data packets are under asymmetric routing, strict uRPF often improperly blocks legitimate traffic. Feasible uRPF and loose uRPF are two other alternative implementations of ingress filtering, but their filtering rules are very loose and generally permit all received packets. Therefore, a new intra-domain SAV mechanism is required to improve accuracy upon current ones.

This document provides the gap analysis of existing intra-domain SAV mechanisms, describes their fundamental problems, and defines the requirements for improvements.

2. Terminology

SAV: Source Address Validation, i.e. validating the authenticity of a packet's source IP address.

SAV rule: The filtering rule generated by the intra-domain SAV mechanism that determines valid incoming interfaces for a specific source prefix.

SAV table: The data structure that stores SAV rules on the data plane. The router queries its local SAV table to validate the authenticity of source addresses.

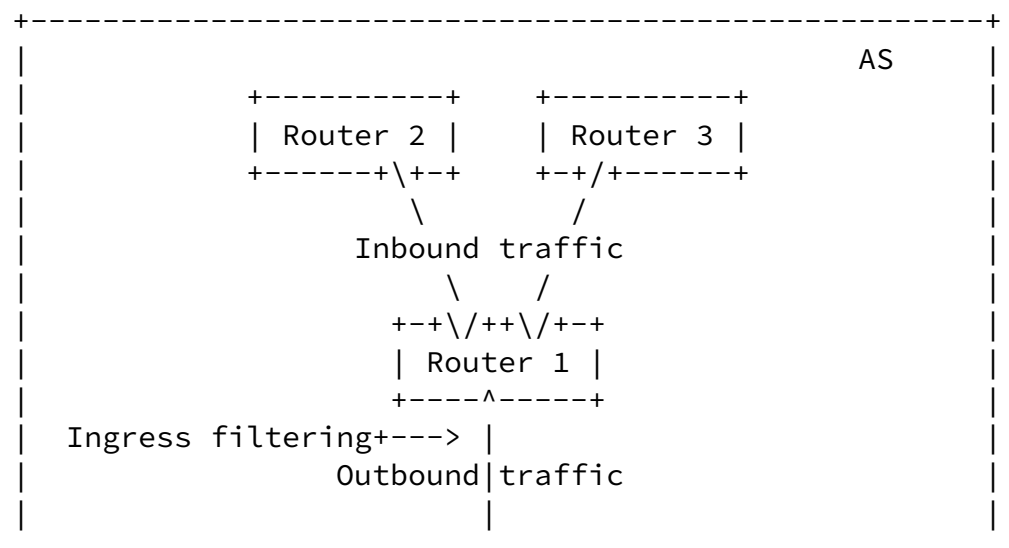
Improper block: Cases when packets with legitimate source addresses are improperly blocked.

Improper permit: Cases when packets with spoofed source addresses are improperly permitted.

3. Gap Analysis

3.1. Vulnerability in Inbound Direction

As shown in Figure 1, ingress filtering is typically deployed at the ingress point of the subnet. It only works for outbound traffic (traffic from subnet to intra-domain network) but does not work for inbound traffic (traffic from intra-domain network to subnet). It prevents the deployed area from sending spoofed packets, but does not protect the deployed area from source address spoofing attacks. Due to the lack of inbound SAV, spoofed packets (even with source addresses of the subnet itself) can easily enter the subnet, although the edge router connected to the subnet has deployed ingress filtering. Therefore, it is generally agreed that ingress filtering only helps when all edge routers in the Autonomous System (AS) have deployed ingress filtering.



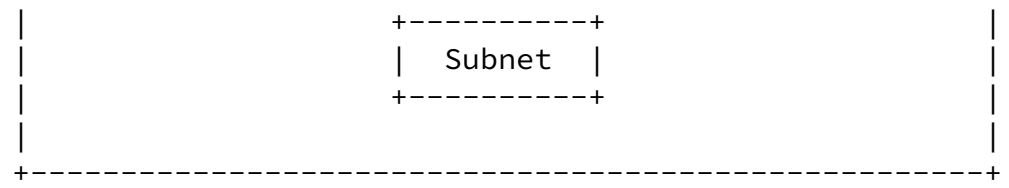


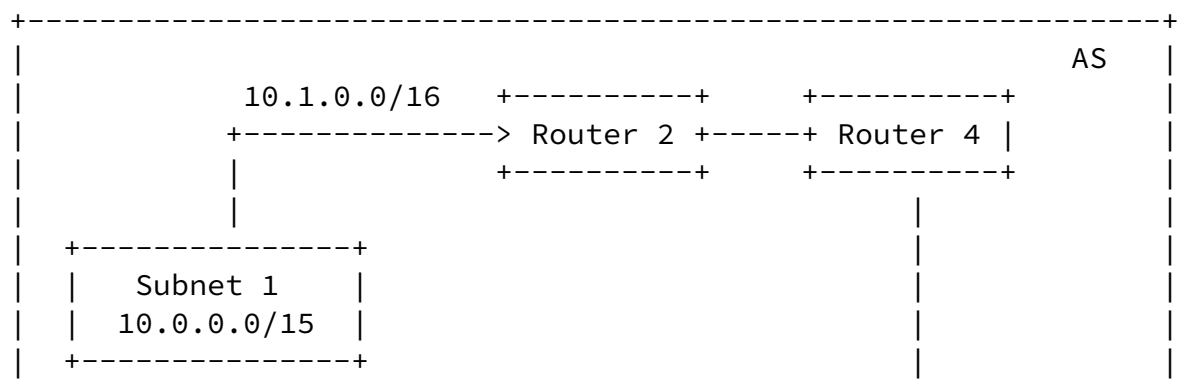
Figure 1: Ingress filtering only works for outbound traffic

3.2. Multi-homed Subnet

Even if all edge routers implement ingress filtering with strict uRPF, strict uRPF may also fail in the case of multi-homed subnet. Figure 2 illustrates a multi-homed subnet scenario. Subnet 1 is attached to two edge routers, i.e. Router 1 and Router 2. Due to the load balance policy of Subnet 1, Subnet 1 advertises 10.0.0.0/16 to Router1 and 10.1.0.0/16 to Router 2, respectively. Then, Router 1 and Router 2 will advertise the learned sub prefixes to other routers in the AS through intra-domain routing protocols such as OSPF and IS-IS. In the end, Router 1 learns the route to 10.1.0.0/16 from Router

3, and Router 2 learns the route to 10.0.0.0/16 from Router 4.

If Router 1 applies strict uRPF at the subnet interface, the SAV rule is that Router 1 only accepts packets with source addresses of 10.0.0.0/16 from Subnet 1. Although Subnet 1 only advertises 10.0.0.0/16 to Router 1, it may send packets with source addresses of prefix 10.1.0.0/16 to Router 1. In this case, strict uRPF at Router 1 will improperly block these legitimate packets. Similarly, when Router 2 with strict uRPF receives packets with source addresses of prefix 10.0.0.0/16 from Subnet 1, it will also improperly block these legitimate packets.



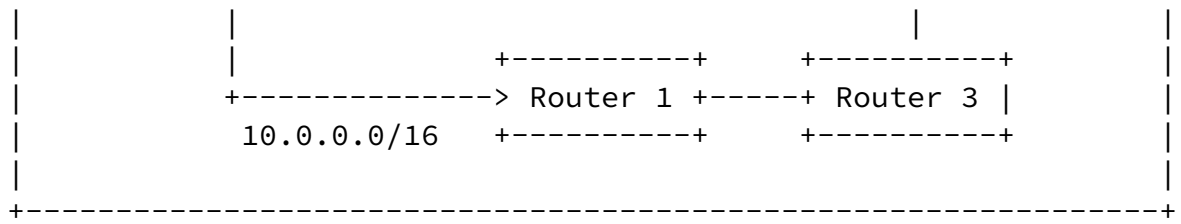
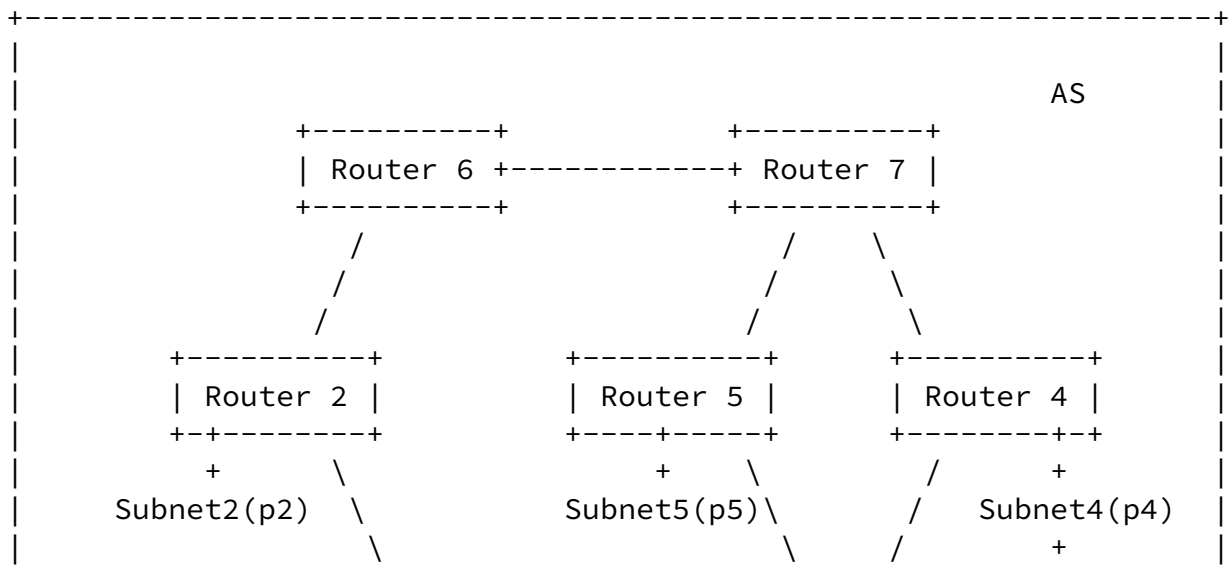


Figure 2: A multi-homed subnet scenario.

3.3. Partial Deployment

Given the technical limitations of existing ingress filtering mechanisms (for example, strict uRPF-based ingress filtering may fail in multi-homed subnet scenario, while ACL-based ingress filtering needs costly manual operation), it is difficult to require all edge routers of an AS to implement ingress filtering simultaneously. Moreover, subnets in a large AS may also be managed by different operators (e.g., subnets in the education network are administered by different campuses). Some operators may not be willing to apply ingress filtering, since ingress filtering does not protect the deployed area from source address spoofing attacks but constrains the behavior of the deployed area.



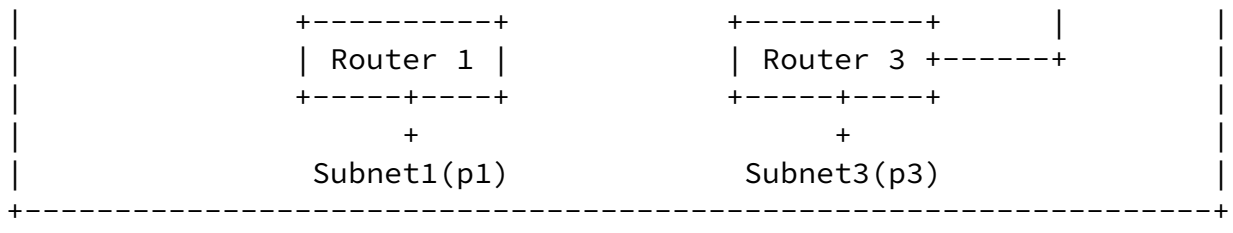


Figure 3: A partial deployment scenario

Figure 3 illustrates a partial deployment scenario. There are seven routers in the AS. Router 1, 2, 3, 4, and 5 are edge routers. Router 6 and 7 are two intra-domain routers located at the aggregation points, which are responsible for transmitting traffic. Assume Router 1 and 2 apply ingress filtering at subnet interfaces, while Router 3, 4, and 5 do not apply ingress filtering. In this case, although Subnet 1 and 2 cannot forge source addresses of other subnets, Subnet 3, 4, and 5 can easily forge source addresses of the deployed area. For example, when Subnet 3, 4, and 5 send spoofed packets with source addresses of p1 or p2 to carry out reflection attacks, Router 1 and 2 may receive these spoofed packets but cannot identify and reject them. To improve the effectiveness of intra-domain SAV when it is partially deployed, it is necessary to perform SAV at more intra-domain routers (at least routers at aggregation points).

To this end, Router 6 and Router 7 apply SAV filtering with strict uRPF at interfaces connected to neighboring routers. However, there will be improper block problems in the case of routing asymmetry. Assume there is asymmetric routing between p2 and p3. The forwarding path from p2 to p3 is Router 2 -> Router 6 -> Router 7 -> Router 5 ->

Router 3. While the forwarding path from p3 to p2 is Router 3 -> Router 4 -> Router 7 -> Router 6 -> Router 2 because of traffic engineering. If Router 7 applies strict uRPF at interfaces connected to the undeployed area, one SAV rule is that packets with source addresses of p3 must arrive from Router 5 since the next hop to p3 in Router 7's FIB is Router 5. In this way, when Router 3 sends legitimate packets with source addresses of p3 to p2, Router 7 will improperly block these packets upon receiving them from Router 4.

3.4. Misbehaved Edge Router

Besides, once an edge router misbehaves, packets with spoofed source addresses can successfully flow from the misbehaved edge router to anywhere in the intra-domain network. To increase the resilience of intra-domain SAV to potential misbehavior, it is desirable to also perform SAV at other intra-domain routers to block spoofed packets as close to the source as possible. However, as mentioned above, existing ingress filtering mechanisms are not competent to perform accurate SAV for packets received from a neighboring router, and can cause traffic disruption.

4. Problem Statement

4.1. Limitation in Accuracy

High accuracy, i.e., avoiding improper block problems while trying best to reduce improper permit problems, is the basic and key problem of an SAV mechanism. However, ACL-based ingress filtering needs manual configuration and thus faces limitations in flexibility and accuracy in dynamic networks. Strict uRPF-based ingress filtering automatically generates SAV tables, but may improperly block legitimate traffic in some cases. The root cause is that strict uRPF leverages the local FIB table to determine the incoming interface for source addresses, which may not match the real data-plane forwarding path from the source, due to the existence of asymmetric routes. Hence, it may mistakenly consider a valid incoming interface as invalid, resulting in improper block problems; or consider an invalid incoming interface as valid, resulting in improper permit problems. Essentially, it is impossible to generate an accurate SAV table solely based on the router's local information due to the existence of asymmetric routes.

4.2. Misaligned Incentive

Currently, ingress filtering is applied at edge routers and only works for outbound traffic but does not work for inbound traffic. This kind of implementation aims to prevent the deployed area from sending spoofed packets, but not to protect the deployed area from attacks. The benefits of the adoption of ingress filtering flow to the rest of the AS, but not to the deployed area itself. As aforementioned, when ingress filtering is partially deployed, the deployed area is still vulnerable to reflection attacks from the undeployed area.

5. Requirements

To improve the accuracy and incentive upon current intra-domain SAV mechanisms, the architecture of intra-domain SAVNET should satisfy the following requirements.

5.1. Accurate Path Discovery

To determine the accurate incoming interfaces for a specific source prefix, routers should be able to learn the real incoming interfaces for packets originated from the subnet which owns the source prefix. In other words, SAV table generation should follow real data-plane forwarding path information. Since this requirement cannot be met by using local FIB information, additional mechanisms are needed to deliver the required information.

5.2. All-round Protection

Intra-domain SAVNET should be deployed in more routers than only the first-hop router (ingress filtering), and should work for traffic coming from all directions (i.e. for traffic from both subnet and neighboring router).

5.3. Incremental Deployment and Incentive

Intra-domain SAVNET should support incremental deployment and can provide direct benefits to the deployed area. When it is partially deployed, it should help the deployed area mitigate reflection attacks from undeployed area.

6. Security Considerations

TBD

7. Acknowledgments

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>.

[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>.

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
Tsinghua University
Beijing
China
Email: qlc19@mails.tsinghua.edu.cn

Mingqing Huang
Huawei
Beijing
China

Email: huangmingqing@huawei.com

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