SAVNET
Internet-Draft
Intended status: Informational
Expires: 10 October 2025

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

8 April 2025

Source Prefix Advertisement for Intra-domain SAVNET
draft-li-savnet-source-prefix-advertisement-04

Abstract

The new intra-domain source address validation (SAV) mechanism requires improving the accuracy (especially avoiding blocking legitimate traffic) and supporting automatic update (see [I-D.ietf-savnet-intra-domain-problem-statement]). To this end, this document proposes an intra-domain SAV mechanism, called source prefix advertisement (SPA) for intra-domain SAVNET (SPA-based SAVNET for short), to advance the technology for intra-domain SAV. SPA-based SAVNET allows routers in an intra-domain network to exchange SPA information. By using SPA information and routing information, intra-domain routers can determine more accurate SAV rules in an automatic manner.

Table of Contents

1. Introduction

The main purpose of intra-domain SAV for an AS is blocking spoofing data packets from host networks and customer networks that use a source address of other networks and blocking spoofing data packets from external ASes that use a source address of the local AS (see [I-D.ietf-savnet-intra-domain-problem-statement]). However, existing uRPF mechanisms [RFC3704] will improperly block legitimate data packets in the case of asymmetric forwarding or asymmetric routing, while ACL-based ingress filtering relies entirely on manual update (see [I-D.ietf-savnet-intra-domain-problem-statement]).

To improve the accuracy and enable automatic update, this document proposes an intra-domain SAV mechanism, called source prefix advertisement (SPA) for intra-domain SAVNET (SPA-based SAVNET for short), to advance the technology for intra-domain SAV. SPA-based SAVNET allows routers in an intra-domain network to exchange SPA information. By using SPA information and routing information,

intra-domain routers can determine more accurate SAV rules in an automatic manner. It is a general intra-domain SAV mechanism that apply to different network topologies (e.g., mesh topology or tree topology) or routing scenarios (e.g., asymmetric routing or symmetric routing).

The reader is encouraged to be familiar with [I-D.ietf-savnet-intra-domain-problem-statement] and [I-D.ietf-savnet-intra-domain-architecture].

1.1. Terminology

SAV Rule: The rule that describes the mapping relationship between a source address (prefix) and its valid incoming router interface(s).

SAVNET Router: An intra-domain router that deploys SPA-based SAVNET.

Host Network: An intra-domain stub network consists of hosts.

Customer Network: An intra-domain stub network consists of hosts and routers.

Host-facing Router: An intra-domain router facing an intra-domain host network.

Customer-facing Router: An intra-domain router facing an intra-domain customer network.

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. Deployment Scope

The deployment scope of SPA-based SAVNET for an AS includes host-facing routers, customer-facing routers, and AS border routers. SPA-based SAVNET allows these routers to exchange SPA information through the existing internal gateway protocol (IGP). By learning SPA information from other SAVNET routers, each SAVNET router can generate an allowlist SAV rule (i.e., "Interface-based prefix allowlist" mode in [I-D.huang-savnet-sav-table]) or a blocklist SAV rule (i.e., "Interface-based prefix blocklist" mode in [I-D.huang-savnet-sav-table]) on the specific router interface:

* For host-facing routers, they generate an allowlist SAV rule on interfaces facing a host network. The allowlist SAV rule exactly covers the space of source IP addresses that are used by data packets of the host network.

* For customer-facing routers, they generate an allowlist SAV rule on interfaces facing a customer network. The allowlist SAV rule exactly covers the space of source IP addresses that are used by data packets of the customer network.

* For AS border routers, they generate a blocklist SAV rule on interfaces facing an external AS. The allowlist SAV rule exactly covers the space of source IP addresses that are used by data packets of the local AS.

By using the generated allowlist SAV rules or blocklist SAV rules, SPA-based SAVNET effectively blocks spoofing data packets from host networks and customer networks that use a source address of other networks and blocks spoofing data packets from external ASes that use a source address of the local AS, while avoiding blocking legitimate data packets.

2.1. Incremental Deployment

SPA-based SAVNET provides incremental benefits when incrementally deployed within the deployment scope. Every SAVNET router that adopts SPA-based SAVNET can identify spoofing data packets coming from a host network, customer network, or an AS. By using allowlist SAV rules, host-facing routers and customer-facing routers that adopt SPA-based SAVNET will block spoofing data packets from host networks and customer networks that use a source address of other networks. By using blocklist SAV rules, AS border routers that adopt SPA-based SAVNET will block spoofing data packets from external ASes that use a source address of the local AS. The network operator can incrementally deploy SPA-based SAVNET in its AS to gradually improve the defense against source address spoofing attacks.

3. SAV Using Routing Information

This document first describes how to use routing information to generate more accurate SAV rules than the existing intra-domain SAV mechanisms (e.g., strict uRPF and loose uRPF).

Each SAVNET router connected to an intra-domain stub network (e.g., a host network or a customer network) generates an allowlist SAV rule. The detailed procedure for allowlist generation is as follows:

1. Extract unique prefixes in the router's routing information base (RIB) that has an outgoing interface towards the stub network.

2. Include these prefixes into the allowlist SAV rule at router interfaces facing the stub network.

Each SAVNET router connected to an external AS generates a blocklist SAV rule. The detailed procedure for blocklist generation is as follows:

1. Extract unique prefixes from routing information learned from the IGP.

2. Include these prefixes into the blocklist SAV rule at router interfaces facing an external AS.

In some asymmetric routing scenario, the allowlist SAV rule generated by using routing information may not cover the whole source IP address space of the stub network. To improve SAV accuracy and avoid improper block, this document further describes using SPA information and routing information to generate the allowlist SAV rules.

4. SAV Using SPA and Routing Information

Each SAVNET router connected to an intra-domain stub network (e.g., a host network or a customer network) generates SPA information:

* Stub Network Identifier (SNI): This identifier indicates the identity of a stub network. Every intra-domain stub network must have a unique SNI value. When advertising the IP information of the stub network, the router carries the SNI value with the IP information.

After generating SPA information, each SAVNET router will provide its SPA information to other SAVNET routers when advertising the IP information of the stub network. SPA information communication can be implemented by using IGP or iBGP. During the propagation of IGP or iBGP messages, SAVNET routers can learn both routing information and SPA information. Specific protocol designs for SPA information communication are not in the scope of this document.

After receiving SPA information from other SAVNET routers, SAVNET routers connected to an intra-domain stub network (e.g., a host network or a customer network) generate allowlist SAV rules as follows:

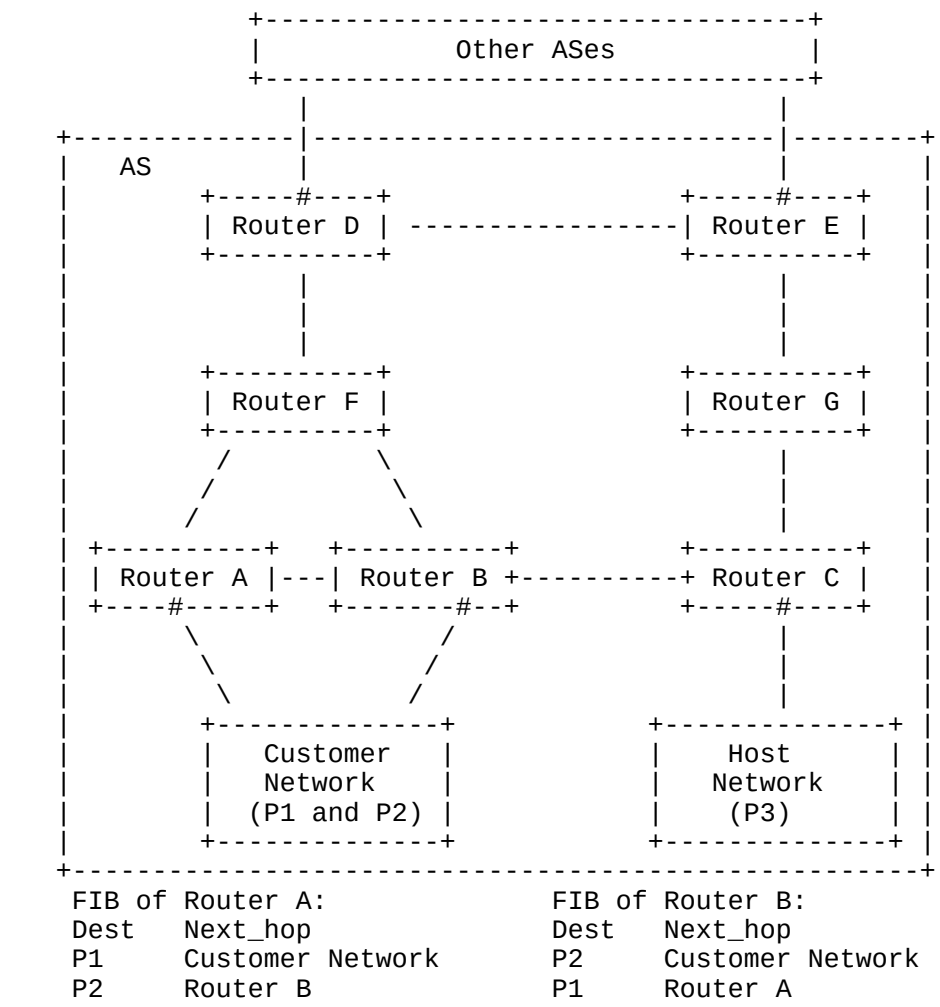
1. Considering all stub networks connected to the router, create a set of SNI values of these stub network. Call it Set A.

2. Considering all SPA information, for each SNI value in Set A, create a set of unique source prefixes that have the same SNI value. Include these prefixes into the allowlist SAV rule at router interfaces facing the stub network which has the same SNI value.

5. Use Case

5.1. SAV on Host-facing Routers, Customer-facing Routers, and AS Border Routers

SPA-based SAVNET is used on host-facing Routers, customer-facing Routers, and AS border routers in an intra-domain network. Figure 1 shows an example. Customer Network is multi-homed to Routers A and B. Host Network is single-homed to Router C. Routers D and E are connected to external ASes. Data packets from Customer Network can use source addresses in prefixes P1 and P2. Data packets from Host Network can use source addresses in prefix P3. P' is the source IP address space for intra-domain router IPs and link IPs. Assume there is an asymmetric forwarding behavior or an asymmetric route among Router A, Router B, and Customer Network due to traffic engineering and load balance. For example, Router A forwards only data packets with destination addresses in prefix P1 to Customer Network while Router B forwards only data packets with destination addresses in prefix P2 to Customer Network. However, Customer Network will sends data packets with source addresses in prefixes P1 and P2 to both routers. In this case, as described in [I-D.ietf-savnet-intra-domain-problem-statement], strict uRPF on Router A's Interface # will improperly block data packets with source addresses in prefix P2 and strict uRPF on Router B's Interface # will improperly block data packets with source addresses in prefix P1.



SAV Rules generated by SPA-based SAVNET:
- Allowlist at Router A's Interface #: [P1, P2]
- Allowlist at Router B's Interface #: [P1, P2]
- Allowlist at Router C's Interface #: [P3]
- Blocklist at Router D's Interface #: [P1, P2, P3, P']
- Blocklist at Router E's Interface #: [P1, P2, P3, P']

Figure 1: An example of the most recommended use case of SPA-based SAVNET

When deploying SPA-based SAVNET in this AS, SAVNET Routers A, B, and C will provide SPA information to other SAVNET routers. By using the SPA and routing information, Routers A and B will include both

prefixes P1 and P2 in the allowlist at the Interface #, because both prefixes have the SNI value of Customer Network, even if the prefix that routers A and B learn from the local route to Customer Network may be different. Router C will include prefix P3 in the allowlist at its Interface #. Routers D and E will include all internal prefixes in the blocklist at their Interfaces #.

5.2. A Special Scenario: Direct Server Return (DSR)

In the case of DSR, the content server in a stub network will send data packets using source addresses of the anycast server in another AS (see [I-D.ietf-savnet-intra-domain-problem-statement]). To avoid blocking these special data packets, these specially used source addresses must be added into the allowlist SAV rule at interfaces facing a stub network where the content server locates. Since routers as well as current routing architecture do not have this information, this may requires manual configuration.

6. Considerations of SAV on Inner Routers

Host-facing routers, customer-facing routers, and AS border routers serve as key vantage points for performing intra-domain SAV. These routers can effectively prevent spoofing traffic from entering the intra-domain router network, ensuring a more secure and reliable routing environment. In addition to these routers, inner routers (such as Routers F and G in Figure 1) may also be able to use SPA information to perform SAV. They can use SPA information together with topology information learned from the IGP to infer the possible incoming directions for a source prefix. However, performing SAV on inner routers may be inefficient in certain network topologies, such as mesh networks. This is because every inner router may receive legitimate data packets with the same source IP address from multiple or even all directions. As a result, the use case of SAV on inner routers is limited.

7. Security Considerations

The security considerations described in [I-D.ietf-savnet-intra-domain-problem-statement] and [I-D.ietf-savnet-intra-domain-architecture] also applies to this document.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. 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>.

9.2. 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>.

[I-D.huang-savnet-sav-table] Huang, M., Cheng, W., Li, D., Geng, N., Liu, Chen, L., and C. Lin, "General Source Address Validation Capabilities", Work in Progress, Internet-Draft, draft-huang-savnet-sav-table-08, 10 December 2024, <https://datatracker.ietf.org/doc/html/draft-huang-savnet-sav-table-08>.

[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-15, 7 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-15>.

[I-D.ietf-savnet-intra-domain-architecture] Li, D., Wu, J., Qin, L., Geng, N., and L. Chen, "Intra-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-ietf-savnet-intra-domain-architecture-01, 14 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture-01>.

Authors' Addresses

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

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

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