SAVNET
Internet-Draft
Intended status: Informational
Expires: 5 January 2026

J. Haas
HPE

4 July 2025

# Inter-domain scaling considerations for source address validation (SAV)
draft-haas-savnet-inter-domain-scaling-00

## Abstract

Source address validation (SAV) covers the general techniques to prevent IP source address spoofing, which is often used in networking attacks. Two primary problem spaces addressed in work on SAV include building the "source of truth" for what IP networks should be permitted to source IP traffic behind a set of network interfaces, and implementing the data plane enforcement for the validation.

Implementing data plane enforcement, especially for inter-domain networking for the Internet carried by BGP-4 [RFC 4271] has a number of scaling considerations. One consideration is the potentially large and often asymmetric sizes of the per-interface SAV tables vs. the Forwarding Information Base (FIB). A second consideration is synchronization issues between SAV enforcement mechanisms and the forwarding state for the FIB where a lack of coordination may result in dropped or mis-forwarded traffic.

This draft explores these two considerations under the title, "The asymmetric contract, and the broken promise."

## 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 5 January 2026.

Table of Contents



## 1. Introduction

This document discusses the implications for when the two parallel control plane inputs for forwarding and for SAV enforcement are not appropriately synchronized, especially at scale.

The IETF SAVNET working group is chartered to address source address validation for Internet Protocol (IP) networking. Spoofing of source IP addresses is a common network attack technique. Such spoofing enhances other network attack techniques by obscuring the attacker and making it more difficult to mitigate such attacks.

Various work has been done over the years to mitigate the use of source address spoofing. A long standing best current practice is using source address filtering ([BCP38]). For edge and access networks, such filtering can be quite successful. Unicast reverse path forwarding checks ([RFC3704]) in many cases is also successful at limiting such spoofing. However, techniques attempting to leverage the routing or forwarding tables (RIB/FIB) for such enforcement are known to be problematic, especially in case of asymmetric routing. [RFC8704] discusses some of these situations for "missing routes".

Within the SAVNET working group, this problem space and also discussion about mitigating such issues are discussed at length in the [I-D.ietf-savnet-inter-domain-problem-statement] and [I-D.ietf-savnet-inter-domain-architecture] documents.

Similarly, much of the work within SAVNET has gone to attempting to address how an operator can construct the appropriate source address enforcement state on a per-device, per-interface basis. This document does not discuss how such a "source of truth" is constructed for enforcement. However, it is presumed that such SAV enforcement state, generally termed the "SAV tables", will be constructed from a variety of inputs, including BGP routing data, RPKI, and local provisioning. [RFC8704] discusses some of this, and so do documents such as [I-D.ietf-sidrops-bar-sav].

Mechanisms to distribute and synchronize these SAV tables to network elements have started to be discussed within the SAVNET working group, but the work is still early. However, it is reasonable to discuss such mechanisms as a component of these devices’ control plane. This helps frame the distribution of the SAV tables as a control plane convergence problem. Comparisons vs. existing routing protocols, even without a specific proposal, helps to frame expectations about convergence time and persistence for this state.

Implementations of SAV enforcement from these SAV tables has also had productive discussion. [I-D.ietf-savnet-general-sav-capabilities] captures at a high level possible enforcement strategies. Note that it is this author’s opinion that there remain gaps in the proposed enforcement capabilities, but that document provides a reasonable starting point for the discussion. The key consideration is that installation of any enforcement mechanism is a programming operation

to instantiate the SAV enforcement for one or more interfaces on the device. Such programming operations have their own latency and thus contribute toward the overall convergence story for SAV enforcement.

This long-winded setup exists to highlight that the distribution of SAV enforcement state and its installation into network elements has a time dimension.

Routing control planes such as BGP also have known time dimensions to distribute the routes and to program the network elements' FIBs.

### 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. The promises of forwarding

### 2.1. The promise of destination-based forwarding

The IPv4 and IPv6 routing technologies have long relied on classless inter-domain routing (CIDR - [RFC1519]). For this document, the critical property of CIDR is the longest-prefix match lookup for destination based routes. Routing protocols, including BGP for Internet use, distribute destination-based prefixes.

Network elements announce destination-based routing state to each other to attract traffic for the covered destinations. Whether that announced state succeeds in attracting the traffic depends on the routing protocol and local configuration of that network element.

The high level "promise" when one network element distributes a destination-based route to another network element is that if it receives IP traffic for an address for that destination that it will be forwarded toward that destination.

While there have always been mitigating circumstances that may prevent forwarding from succeeding, such as firewalls, the implicit promise is that if you accept and use that route, traffic will be delivered. Firewalls "inappropriately" deployed are an illustration of when that promise has been broken. When such situations are detected by an operator, that operator may take measures to not use routes sent by providers that are inappropriately filtering traffic.

### 2.2. The promise of source address validation enforcement

Source address validation becomes involved in this destination-based forwarding promise. SAV enforcement, when the traffic's source address is out-of-profile for the installed enforcement policy, may result in the traffic not being delivered.

The expectation is that the SAV state will fully cover "legitimate" sources. As noted previously in the document, this depends on a fully known "source of truth" to be distributed and installed in SAV enforcing devices.

### 2.3. The broken promise

A significant amount of the current discussion in SAVNET is around how to best calculate the source of truth for SAV enforcement. However, it is simple to distill the situation where the resultant behavior is incorrect and may cause harm to the expectations of users of the involved networks.

If a destination-based route is distributed between two network elements, and both network elements consider the route to be "legitimate", the expectation is that all "legitimately" sourced IP traffic for the covered destinations that can reach that network element MUST be forwarded.

Any technique for calculating a network element's source of truth for SAV enforcement that cannot arrive at the same result as yielded by destination-based routing and locally perceived "legitimate" source addresses has broken the promise of destination-based forwarding.

This property MUST be used as a sanity-check for any technique used to build the source of truth for SAV enforcement.

## 3. The contract between the synchronization of forwarding and SAV enforcement state

Even when the fully known SAV enforcement state has been determined, inconsistencies in the SAV enforcement state vs. forwarding can lead to inappropriately dropped traffic. In order to avoid breaking the promise of destination-based forwarding, there is the contract that SAV enforcement state MUST NOT be installed in such a way as to lead to such dropped traffic.

The core considerations are these:

* SAV enforcement for all legitimate sources MUST be installed prior to attracting traffic to the network element.

* SAV enforcement state MAY be installed but NOT enforced prior to attracting traffic to the network element.

This requirement for synchronization of enforcement and forwarding illustrates several scaling considerations that will be discussed in the following sections.

## 3.1. The asymmetric contract between routing and SAV enforcement

Consider a simple dual-homed BGP stub-AS customer, C, with two providers, P1 and P2. P1 and P2 are Internet Service Providers.

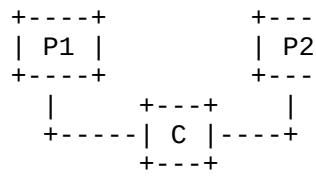


Figure 1: Dual-homed stub-AS customer

Presume that C has a single network, N, it wishes to advertise to the Internet via both P1 and P2.

Presume that C wishes to make load balancing choices for its Internet traffic and thus receives the majority of the current Internet table (approximately 1 million destinations as of the writing of this document) from both P1 and P2.

### 3.1.1. Provider receiving the customer route

If P1 and P2 wish to deploy SAV enforcement for C, their SAV tables for their interfaces towards C contain only "N". Presuming that C always advertises its full set of routes to its providers, unicast-RPF works well as an enforcement mechanism. However, even for this trivial case we can illustrate the synchronization consideration between SAV enforcement and routing.

If C has not yet advertised N to P1, and P1 advertises a single route to C that will start attracting traffic, P1 will drop C’s traffic.

As P1 continues to advertise destinations to C, C advertises its route to P1. During this time, any traffic attracted to P1 prior to C being installed in P1’s FIB will still be dropped. This continues until C’s route is installed in the FIB and u-RPF as the SAV enforcement mechanism stops dropping traffic.

This example highlights that if enforcement occurs prior to programming that traffic is inappropriately dropped.

#### 3.1.2. Customer receiving the provider routes

Consider the somewhat ludicrous opposite scenario: C wishes to deploy SAV enforcement vs. P1 and P2, which send full Internet feeds. Since C is taking full Internet table feeds, it also considers using RPF as its SAV enforcement mechanism.

C has yet to receive any routes from either P1 or P2.

C advertises its route to P1 and P2. These providers install that route into their FIBs and propagate the route to the rest of the Internet. This begins attracting traffic to C.

P1 and P2 start advertising their Internet feeds to C. During the time while the Internet feeds are being advertised to C, traffic may arrive from the Internet for C. Until the covering routes from the providers are received and installed in C’s FIB, traffic is dropped.

#### 3.1.3. Scaling and synchronization considerations

The above two examples illustrate where differences in scaling and a lack of synchronization between routing and SAV enforcement can lead to dropped traffic.

A potentially different conclusion is that RPF as a SAV enforcement mechanism is the wrong tool. Consider instead that in each direction for the network peering that the full source of truth was pre-calculated and is complete. If this is known a priori, and the SAV enforcement state is installed prior to advertising routes that will attract traffic, then traffic will not be dropped. Excellent!

Even with pre-calculated sources of truth, using the two prior examples, there are still properties where scaling considerations are illustrated:

* Your enforcement state MUST be fully installed prior to advertising routing that can attract traffic that will otherwise be dropped.
* The availability of the SAV table state used for enforcement, if distributed dynamically, becomes a convergence consideration that needs to be addressed before routing convergence can start.
* SAV table state is very likely to be significantly greater in scale that routing state. It could vary more on a per-interface basis than similar routing state received by the network element.

* In-band distribution of SAV table state could compete for converging both of these sub-systems - routing and SAV enforcement. The example of RPF as an enforcement mechanism shows how SAV enforcement and routing require full alignment. A mechanism where SAV enforcement is similarly distributed in BGP and competes vs. routing data becomes comparable at a higher scale.

#### 3.1.4. Dynamic updates for SAV enforcement state

SAV enforcement state is likely to require dynamic update mechanisms. Updates to even a single destination's state for "source of truth" require that the entire routing system - e.g., the Internet - need to be able to absorb and install such updates dynamically to avoid dropped traffic. BGP handles the distribution of destinations for the Internet. A similar dynamic mechanism for distributing SAV sources of truth is required. A requirement for Internet-scale SAVE enforcement requires SAV enforcement and forwarding to be synchronized.

The trivial examples (Section 3.1.1, Section 3.1.2) demonstrate how difficult addressing synchronization across the Internet is likely to be, if attempted at scale.

## 4. SAV enforcement scaling considerations for network elements

Most discussion to date about full SAV enforcement makes a highly inappropriate assumption: There are infinite resources to install not only forwarding state, but able to absorb and implement SAV enforcement mechanisms. Instead, it's quite normal for there to be highly asymmetric capabilities in the network elements involved in forwarding.

Using the prior example, for their edge routers, providers P1 and P2 likely have the capacity to carry multiple views of the Internet routing table along with handling all customer routes. If C does indeed wish to carry two full views of the Internet, that's certainly possible. But perhaps it uses a lower capability device where it only can carry 20% of the Internet routing table in its FIB. Stub AS customers can obtain significant benefit for outbound traffic load balancing by only selectively using a portion of the Internet's table and otherwise choosing to "default" its traffic to its upstream providers.

Similarly, it may not be possible for C to do SAV enforcement based on limited hardware resources. RPF as an enforcement mechanism becomes "silly" to do when defaults are involved. In such situations, perhaps it is better to not do SAV enforcement at all?

While the trivial example seems inapplicable to broader scenarios, the discussion above has similar considerations for any device participating in SAV enforcement with constrained resources. If your enforcement policy drops traffic that is out-of-profile, less than perfect and less than fully synchronized enforcement state will lead to inappropriately dropped traffic.

There are two conclusions from these scaling and limiting capacity considerations:

* Using "drop" for out-of-profile SAV traffic is only safe when the devices have both fully synchronized SAV enforcement state, but also all enforcement state.
* Selectively providing SAV enforcement could provide benefit to operators. Developing the forms of selective enforcement and qualifying their benefits is work that should be taken up for future study.

## 5. Violating the contract based on security posture.

The discussion above is written from the general Internet stance that dropping traffic as routing and SAV enforcement is synchronized is always problematic. It’s worth noting that in specific operator scenarios that a "fail closed" model may be appropriate for security reasons. In such cases, until enforcement for the known good source addresses is installed, dropping all traffic that fails to match the SAV enforcement mechanism is permitted.

## 6. The asymmetric contract and the broken promise.

Asymmetry will exist in in device forwarding and SAV enforcement capabilities. Performing aggressive SAV enforcement and dropping out-of-profile traffic requires having perfect sources of truth and tightly coupled procedures to install and enable SAV enforcement state require significant care.

Ordered installation of up to date SAV tables is required before routing information can be disseminated by a SAV enforcing network element.

SAV enforcement "sources of truth" must be fully aligned with any valid distribution of destination based routing state to avoid breaking the promise of destination based forwarding.

Achieving perfection in such a system at Internet scale may prove to be impossible. Benefits of selective enforcement of SAV may prove to be more deployable.

## 7. IANA Considerations

This memo includes no request to IANA.

## 8. Security Considerations

This document discusses the impacts to inappropriately dropped IP traffic when source address validation enforcement is deployed inconsistently routing. This document primarily provides the framework to consider some of the inputs that cause this impact to permit implementors to avoid such issues.

## 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>.

[I-D.ietf-savnet-inter-domain-problem-statement] Li, D., Wu, J., Liu, L., Huang, M., and K. Sriram, "Source Address Validation in Inter-domain Networks Gap Analysis, Problem Statement, and Requirements", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-problem-statement-08, 15 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-08>.

[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-01, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-architecture-01>.

### 9.2. Informative References

[RFC1519] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, DOI 10.17487/RFC1519, September 1993, <https://www.rfc-editor.org/info/rfc1519>.

[BCP38] 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>.

[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-06, 15 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-bar-sav-06>.

[I-D.ietf-savnet-general-sav-capabilities] Huang, M., Cheng, W., Li, D., Geng, N., and L. Chen, "General Source Address Validation Capabilities", Work in Progress, Internet-Draft, draft-ietf-savnet-general-sav-capabilities-01, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-general-sav-capabilities-01>.

## Acknowledgements

TBD

## Contributors

TBD

## Author’s Address

Jeffrey Haas
HPE
1133 Innovation Way
Sunnyvale, CA 94089
United States of America
Email: jhaas@juniper.net