SAVNET Working Group
Internet-Draft
Intended status: Standards Track
Expires: 29 May 2026

X. Li
A. Wang
China Telecom

25 November 2025

Intra-Domain On-Demand Source Address Validation(SAV) Mechanism
draft-li-savnet-intra-domain-od-sav-02

Abstract

Source Address Validation (SAV) mechanisms, such as uRPF, ACLs, and BM-SPF, are applied to prevent IP source address spoofing. However, these mechanisms are typically designed for static routing scenarios and deployed at fixed network boundaries.

With the increasing adoption of dynamic forwarding technologies such as SRv6 Policy and Fast Reroute (TI-FRR), the network’s actual forwarding path may change frequently due to policy-based traffic steering or link failures. In such cases, statically deployed SAV rules may fail to validate traffic on newly activated or alternate paths, creating validation blind spots or even leading to false positives that block legitimate traffic.

This draft proposes an On-Demand Source Address Validation Activation mechanism. It enables routers to dynamically activate or update SAV rules on specific interfaces only when the interface becomes part of an active forwarding path due to policy or failover triggers. This approach enhances SAV coverage, avoids unnecessary resource consumption, and ensures SAV correctness under dynamic path switching scenarios driven by SRv6-policy and TI-FRR.

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 29 May 2026.

Table of Contents

1. Introduction

The security of IP networks depends heavily on the ability to verify the legitimacy of source addresses in data packets. Source Address Validation (SAV) serves as a foundational mechanism to mitigate IP spoofing attacks by enforcing policies that ensure packets originate from expected locations. Common SAV mechanisms include:

* ACL-based filtering, where packet validation rules are manually configured on specific interfaces.

* uRPF, which verifies that a packet' s source address is reachable via the receiving interface according to the FIB.

* BM-SPF, which opens minimal set of interfaces based on IGP.[bmspf]

While effective in static or stable routing environments, these mechanisms face growing limitations in modern networks that adopt path engineering and fast reroute techniques.

In particular, Segment Routing over IPv6 (SRv6) [RFC8987] enables operators to define customized traffic paths (SRv6 Policies) that override shortest-path routing, while Topology-Independent Fast Reroute (TI-FRR) ensures traffic continues during link or node failures by instantly switching to backup paths. These capabilities introduce highly dynamic forwarding behavior, where the actual path of a data packet may change based on traffic type, policy reconfiguration, or network failure—without corresponding updates to the existing SAV rules deployed in the network.

Under such conditions:

* SAV validation may be bypassed if the forwarding path traverses interfaces without validation rules (validation blind spot).

* Legitimate traffic may be dropped if SAV rules mismatch the active path due to delayed or missing updates (false positives).

* Resource overhead increases if operators pre-deploy SAV rules on all possible interfaces to anticipate changes (inefficient and hard to manage).

To address these issues, this draft introduces a mechanism for On-Demand Source Address Validation Activation, which dynamically installs, updates, or revokes SAV rules on interfaces based on real-time detection of path changes. The mechanism supports two representative trigger types:

* SRv6 Policy Routing, where control-plane or application policies initiate path re-selection.

* TI-FRR, where the forwarding plane autonomously switches to a precomputed backup path upon failure detection.

By aligning SAV activation with the actual packet forwarding path, the proposed mechanism improves security robustness, resource efficiency, and operational adaptability in dynamic networks.

2. Conventions used in this document

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 [RFC2119] [RFC8174].

3. Terminology

The following terms are used in this draft:

* Segment Identifier (SID): An identifier for each path segment used to guide traffic within the network.

* Segment List: An ordered list of SIDs that defines the path for traffic from the source to the destination.

* SR-policy: Segment Routing policy, A policy consisting of one or more Segment Lists, each representing an alternate path.

* FIB: Forwarding Information Base.

* SAV: Source Address Validation.

* uRPF: Unicast Reverse Path Forwarding.

* BM-SPF: Bidirectional Metric based Shortest Path First Mechanism.

* FRR: Fast Reroute

* TI-LFA: Topology Independent Loop-Free Alternate.

* SRv6: Segment Routing over IPv6.

* Ingress/Egress: The starting/ending router in a forwarding path.

4. Overview of on-demand SAV activation mechanism

The On-Demand Source Address Validation (SAV) Activation Mechanism is a dynamic and path-aware validation approach designed to ensure precise and efficient spoofing prevention in networks where forwarding paths may change frequently due to control-plane policies or fast reroute events. Unlike traditional SAV mechanisms that rely on static interface bindings or shortest-path assumptions, the on-demand model provides interface-level validation granularity that closely follows actual packet forwarding behavior.

This mechanism is particularly tailored to support intra-domain deployments where advanced routing schemes— such as SRv6 Policy-based traffic steering and Topology-Independent Fast Reroute (TI-FRR)— are actively used to improve performance, availability, and flexibility. In these cases, packet forwarding may dynamically deviate from the IGP shortest path or revert rapidly to backup routes, rendering static SAV rules insufficient or ineffective.

4.1. Design Goals

The on-demand SAV mechanism is designed to meet the following goals:

* Path-Coupled Validation Activation: SAV rules are activated only on interfaces that currently participate in forwarding traffic for protected source prefixes, minimizing resource consumption and false positives.

* Trigger-Based Adaptivity: SAV activation responds in real-time to forwarding path changes triggered by:

  - SRv6 SID list updates in the control plane (e.g., application policy shift).

  - FRR activation upon link or node failure.

* Distributed and Lightweight Propagation: SAV-specific information (such as prefix/interface mappings) is propagated only to affected routers, allowing scalable and incremental rule installation without network-wide updates.

* Fine-Grained Rule Lifecycle: SAV rules are assigned explicit activation conditions and expiry policies (e.g., duration, path reversion), ensuring timely withdrawal and state consistency.

4.2. Mechanism Workflow

The mechanism operates via a coordinated process involving core Workflow:

1. Trigger Detection:

* Path changes are detected through control-plane events (e.g., SRv6 policy change notifications) or data-plane reactions (e.g., TI-FRR activation).

* Each event is associated with a set of source address prefixes that require protection.

2. SAV-specfic information update and SAV rule Generation:

* Local router logic computes the updated validation scope, which includes:
  - Source prefixes to be validated.
  - Interfaces on each router along the active path where validation should be enforced.
* These information is encoded in SAV-specific messages and propagated from source router to validation entities (the routers that need to perform validation).

3. Rule Activation and Enforcement:

* Upon receiving the SAV-specific information, validation routers dynamically create or update SAV rules (e.g., prefix filters, ACL entries, enhanced uRPF modes).
* Rules are scoped in time or bound to session triggers, and are withdrawn when the corresponding path becomes inactive.

4.3. Integration with BM-SPF and Static SAV

The proposed on-demand mechanism is not intended to replace existing SAV methods, but to complement them in scenarios where static validation falls short. In particular:

* BM-SPF (Bidirectional Metric-based Shortest Path First) continues to serve as a reliable default for symmetric or IGP-derived paths.
* On-demand activation is selectively applied only to forwarding paths resulting from:
  - SRv6 Policy-based steering, which diverges from BM-SPF-computed paths.
  - TI-FRR-driven failover, where backup paths are not part of the IGP’s steady-state shortest path.

Through this hybrid approach, operators can retain static validation as a baseline while dynamically extending coverage to alternate or policy-induced routes with minimal operational overhead.

4.4. Applicability Scope

The on-demand SAV mechanism is explicitly scoped to support two types of dynamic forwarding scenarios within a single administrative domain:

* SRv6 Policy Paths: Where the control plane installs an explicit SID list to steer traffic along a non-default path, typically for application-aware routing or SLA enforcement.

* TI-FRR Backup Paths: Where data-plane-level fast reroute mechanisms instantly switch traffic to precomputed backup next hops upon failure, requiring temporary and immediate SAV activation along the backup route.

Table.1 Trigger conditions for on-demand activation

Trigger Type	Example Scenario	SAV Activation Scope
SRv6-policy	SRv6 SID list reroute	Prefixes/Interfaces on new path
FRR Activation	TI-LFA backup engaged after failure	Prefixes backup path interfaces

Other scenarios such as ECMP, BGP-based inter-domain routing, or multicast are outside the scope of this specification, but may be considered in future extensions.

5. Usecases of On-Demand SAV Activation mechanism

The On-Demand SAV mechanism is designed to complement and extend traditional SAV enforcement models in dynamic routing environments. It particularly addresses the validation gaps caused by traffic engineering changes and fast reroute mechanisms by dynamically activating SAV rules only on affected interfaces. Below we present two representative use cases: SRv6-policy based rerouting and TI-FRR based failure recovery.

5.1. SRv6-Policy Based On-Demand SAV

In this intra-domain network, multiple types of traffic coexist, including latency-sensitive voice traffic and high-bandwidth file transfer traffic. These traffic types are routed differently based on service requirements:

* Default Path: The shortest path computed by IGP (BM-SPF) is used: R1 → R2 → R3.

* Policy-Driven Path (File Transfer/High Bandwidth Traffic): A Segment Routing over IPv6 (SRv6) policy instructs routers to use an alternate path with higher bandwidth capacity: R1 → R4 → R3

An SRv6 controller programs this policy using a SID (Segment Identifier) list and updates the forwarding path dynamically.

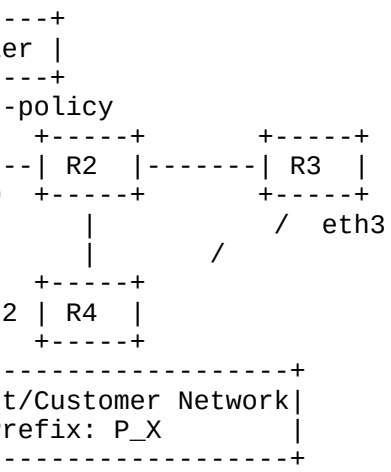

Figure 1 An example of SRv6-Policy Based On-Demand SAV usecase

In this scenario, when the policy change takes effect and traffic is redirected via R1 → R4 → R3, traditional IGP-based SAV at routers like R4 may not permit traffic originating from prefix P_X if that source was not expected on that interface. On-Demand SAV solves this by:

* Dynamically activating SAV rules for prefix P_X on R4' s ingress interface (e.g., eth2) based on the updated SAV-specific information [architecture].

* Ensuring that only traffic matching the expected policy is accepted.

* Avoiding blanket SAV deactivation while preserving forwarding flexibility.

This selective activation protects against spoofing while allowing legitimate policy-driven traffic to be validated correctly.

5.2. TI-FRR Based On-Demand SAV

In a second scenario, the network uses Topology-Independent Loop-Free Alternate (TI-LFA) for fast failure recovery. The default routing path is again: R1 → R2 → R3.

If Router R2 fails, TI-FRR is automatically triggered at R1. Traffic is rerouted via the pre-calculated backup path: R1 → R4 → R3. This fast rerouting is done locally without requiring immediate global convergence.

Under normal conditions, prefix P_X is associated with the primary path. SAV rules are installed accordingly on the primary interfaces (e.g., R2 and R3). When failure occurs:

* Primary Path (eth0) SAV Downgrade: SAV checks may be disabled or relaxed on the now-inactive interface eth0 at R1.

* Backup Path (eth1 → eth2 → eth3) SAV Activation: On-demand SAV is triggered on the interfaces along the backup path based on the updated SAV-specific information:

  - eth1 (R1 → R4).

  - eth2 (R4 ingress).

  - eth3 (R4 → R3).

This ensures that even during transient forwarding path changes, prefix-based source validation continues to be enforced only on relevant interfaces, reducing the risk of spoofing or source address misvalidation.

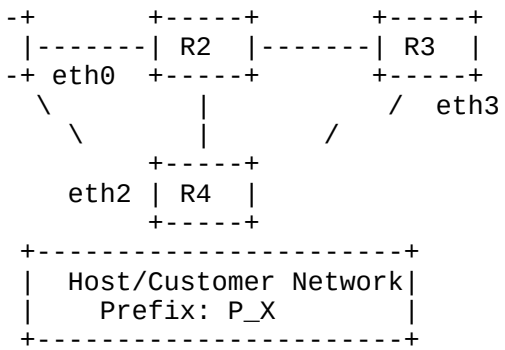

Figure 2 An example of TI-FRR Based On-Demand SAV usecase

5.3. SAV-specific messages propagation

TBD

6. Conclusion

The On-Demand Source Address Validation (SAV) mechanism offers a practical enhancement to existing SAV frameworks by enabling dynamic, policy-aware validation capabilities. Targeting scenarios with dynamic path switching such as SRv6 Policy-based routing and TI-FRR, this mechanism ensures that traffic traversing backup or non-default paths can still undergo precise source address validation, overcoming the limitations of traditional SAV methods.

By coupling route-aware control with dynamic rule activation, this mechanism installs SAV rules only when and where needed—at merge points or policy egress/ingress interfaces—thus reducing the overhead of global static configurations. It also aligns well with the principles of resource efficiency, minimal control plane impact, and fast adaptability to network changes.

As networks increasingly adopt path-aware forwarding and dynamic policy enforcement, the On-Demand SAV mechanism provides a forward-compatible foundation to maintain security guarantees without sacrificing flexibility. Future work may include interoperable signaling extensions, coordination with SRv6 controller behavior, and operational guidelines for real-world deployments.

7. IANA Considerations

TBD

8. Acknowledgement

TBD

9. Normative References

[architecture] "draft-ietf-savnet-intra-domain-architecture".

[bmspf] "draft-wang-savnet-intra-domain-solution-bm-spf".

[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] "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words".

[RFC8793] Wissingh, B., Wood, C., Afanasyev, A., Zhang, L., Oran, D., and C. Tschudin, "Information-Centric Networking (ICN): Content-Centric Networking (CCNx) and Named Data Networking (NDN) Terminology", RFC 8793, DOI 10.17487/RFC8793, June 2020, <https://www.rfc-editor.org/info/rfc8793>.

[RFC8987] "Segment Routing Policy Architecture.".

Authors' Addresses

Xueting Li
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: lixt2@foxmail.com

Aijun Wang
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: wangaj3@chinatelecom.cn