Segment Routing Policy-Based Source Address Validation (SAV) Mechanism

[draft-li-savnet-srsav]

IETF 121

- ***Xueting Li (China Telecom)***
- *Aijun Wang (China Telecom)*
- *Wei Wang (China Telecom)*
- *Yuanyuan Zhang (Zhongguancun Laboratory)*

The contents

- Problem Overview
- Limitations of Intra-domain SAV Mechanisms
- Motivation
- Usecase
- The SAV Message Forwarding Logic
- Conclusion
- References

Problem Overview

- Challenges:
  - Source Address Spoofing: In networks, attackers may forge source IP addresses to bypass security checks and inject malicious traffic into the network.

- Consequences of Spoofing
  - Data Integrity Compromise: Legitimate flows corrupted by malicious data packets.
  - Resource Exhaustion: Illegitimate traffic consumes network resources, impacting performance.

Limitations of Intra-domain SAV Mechanisms

- Option A: Dependence on SPF (IGP)
  - Ignore policy-driven routing and dynamic path adjustments.
  - Prevent use of legitimate alternate paths in complex network environments.

- Option B: Fully Open approach (Least Restrictive)
  - All interfaces are accessible, compromises security.
  - Miss validations and increase risk of spoofing, defeat the purpose of SAV.

- Proposal: On-demand interface open
  - Based on the option A, adding a SAV mechanism of on-demand deployment based on SRv6-policy.

Motivation

- Why integrate SAV with SRv6-Policy?
  - Ensures hop-by-hop validation of traffic sources.
  - Provides granular control over traffic paths.
  - Prevents spoofed source traffic from entering the network.
  - Supports Multi-cloud & Large-scale Networks: Essential for secure traffic management in complex environments.
  - On-demand, policy-driven openness—ensuring controlled yet flexible SAV rules across SR paths and alternate routes as needed.

Usecase

☐ Network Topology Consider a network topology in the figure.

- Scenario:
  - SPF calculation (IGP):
    - •In the network, SAV is deployed to allow traffic only along the shortest path.
    - the shortest path R1 → R2 → R4 → R5
  - Fully Open Control (Least Restrictive)
    - Allows all paths, reducing security.
    - Increases exposure to spoofed or malicious traffic.
    - SAV mechanism loses effectiveness.

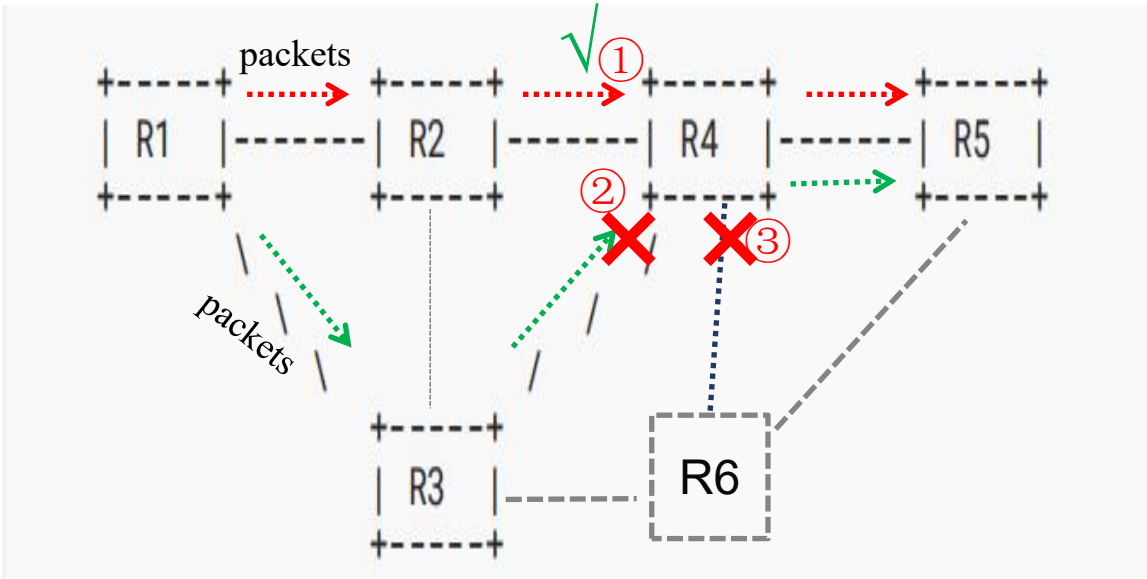

Figure 1 An example of Usecase

Usecase

- On-Demand Interface Control with SRv6-policy (Optimized Approach):
  - Alternate Path (Upon R2 Failure): R1 → R3 → R4 → R5.
    - R4 dynamically opens Interface 2 to accept traffic from R3.
  - Uses SR-policy to dynamically specify and open interfaces only as needed.
  - Ensures security by applying SAV only to defined paths.
- Edge-Only SAV:
  - SAV is applied only at the edge nodes, such as at R1 in this network.
  - Can't protect against malicious traffic from internal nodes that might attempt to exploit alternative paths.

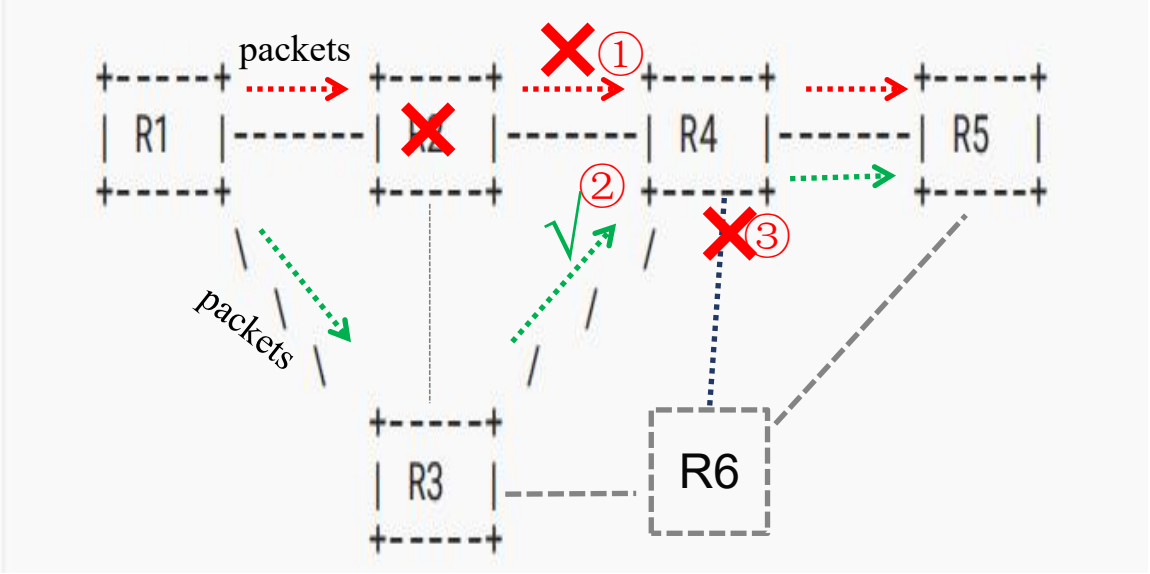

Figure 1 An example of Usecase

The SAV Message Forwarding Logic

1. Basic Forwarding Logic

- SAV Message Propagation on SR-Policy Path
  - SR-policy path (e.g., R1 → R3 → R4 → R5).
  - R1 generates an SAV message, routers set up rules along this path.
- Dynamic Interface Activation:
  - Routers R3 and R4 receive the SAV message.
  - Each checks the segment list, opens required interfaces, and creates SAV rules.
    - The SAV rule includes:
    - Source Prefix: Specifies the allowed source addresses.
    - List of Valid Interfaces: Defines which interfaces are permitted for incoming traffic from this source, per SR-policy.

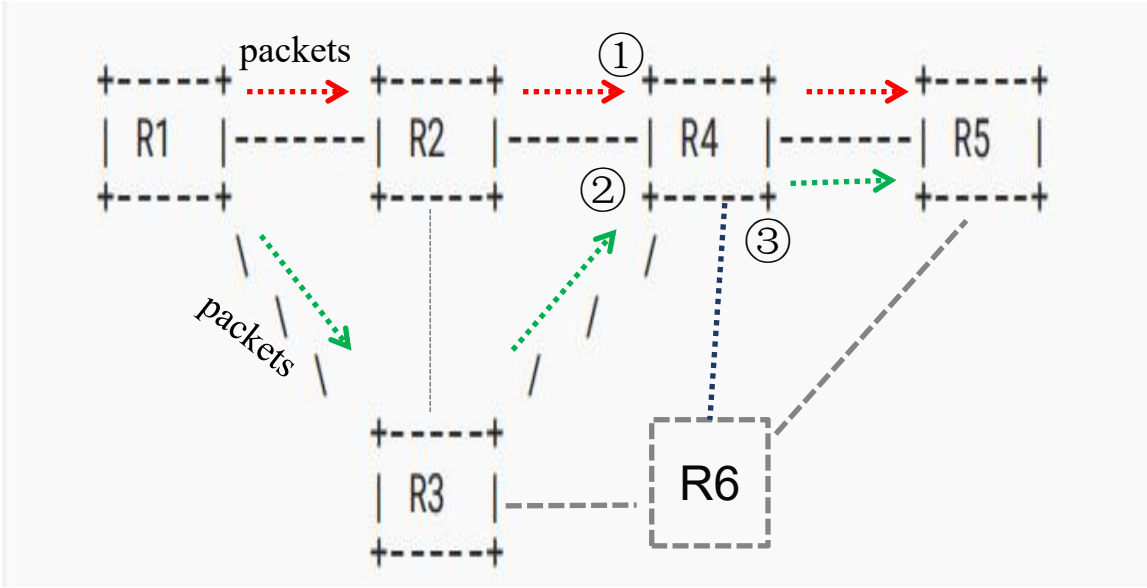

Figure 1 An example of Usecase

The SAV Message Forwarding Logic

- Dynamic Interface Opening at Key Nodes:
  - Each router compares the SID in the SAV message with its locally configured SID(s).
  - R3 processes the SAV message and generates the corresponding SAV rule.
  - Forwards the message to the next key node along the SID_list.
- SAV Rule Enforcement:
  - Along the path R1 → R3 → R4 → R5, each router applies SAV rules at the specified interfaces.
- Non-Key Node Behavior: (e.g., R2)
  - ignores the SAV message.
  - will not establish SAV rules for the traffic.
- Strict Adherence to SR-Policy:
  - Traffic on unauthorized paths will be blocked by routers lacking the corresponding SAV rule.

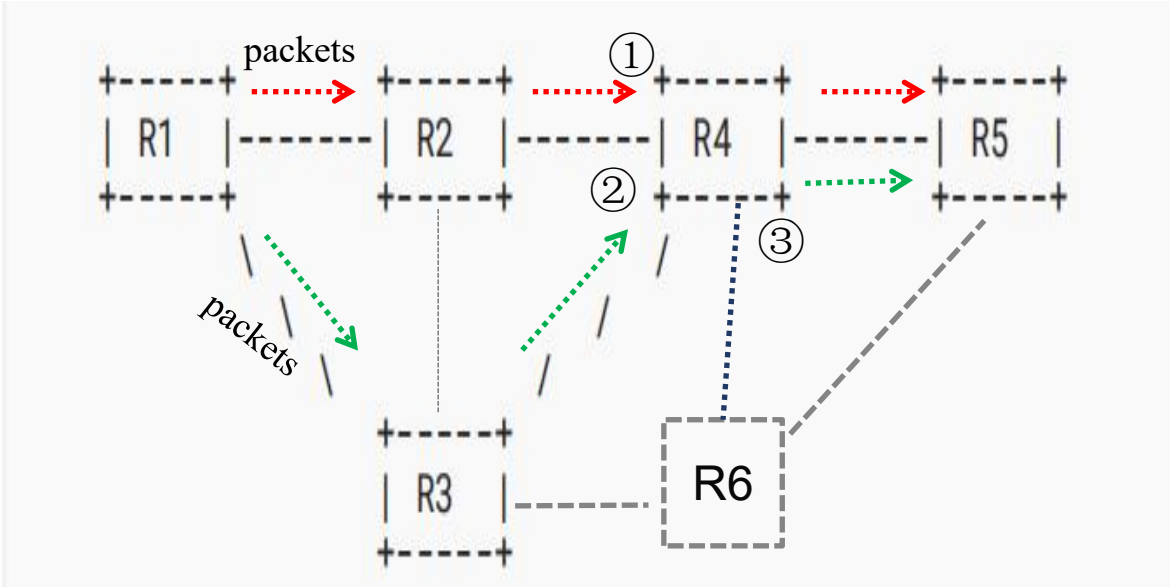

Figure 1 An example of Usecase

Conclusion

- Key Benefits:
  - Open on-demand: Provides controlled flexibility by enabling SAV validation where needed according to the SRv6-policy.
  - Enhanced Security: Traffic is verified for source authenticity at each hop along the SRv6-policy path, preventing unauthorized traffic from bypassing SAV checks.

- Enhanced Control & Flexibility:
  - Provides superior control over message propagation compared to traditional methods.
  - Leverages SR-policy to define optimal paths for SAV message delivery.

- Future Outlook:
  - Ideal for complex network, supporting evolving network demands.

References

- **RFC 2119:** Key words for use in RFCs to Indicate Requirement Levels
- **RFC 8174:** Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words
- **RFC 8402:** Segment Routing Architecture
- **RFC8987:** Segment Routing Policy Architecture.
- **SAV:**General Source Address Validation Capabilities
- **sav-ospf:** draft-zhang-savnet-sav-ospf-00
- **SAVNET:**Intra-domain Source Address Validation (SAVNET) Architecture

Comments ➡

lixt2@chinatelecom.cn
wangaj3@chinatelecom.cn
wangw36@chinatelecom.cn

中国电信
CHINA TELECOM

5G hello

Thank you!