New Intra-domain Source Address Validation (SAV) Solution

[draft-wang-savnet-intra-domain-solution-bm-spf-00]

Wei Wang (China Telecom)
Aijun Wang (China Telecom)
IETF 122, March. 2025

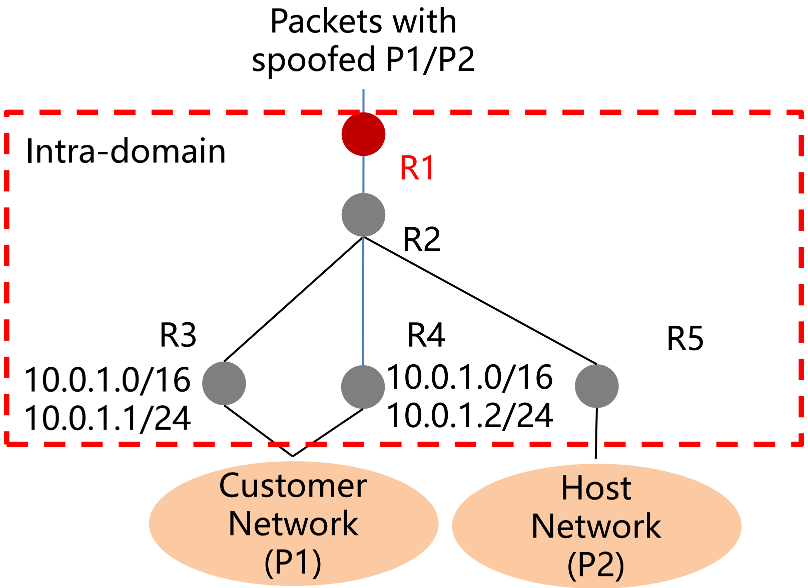
- Background and objectives
- SAV Procedure - AS Border Routers
- SAV Procedure - Customer-facing or Host-facing Routers
- SAV Procedure - Internal Routers
- Overview of BM-SPF mechanism
- Further Action

Background and Objectives

- **Background:** Intra-domain SAV aims to prevent outbound packets from spoofing source addresses of other subnets or ASes, and inbound packets from external ASes from spoofing local AS source addresses.

- **Objectives:** Find a general solution applicable to host-facing, customer-facing, and AS border routers. Simplify SAV rule generation based on FIB table.

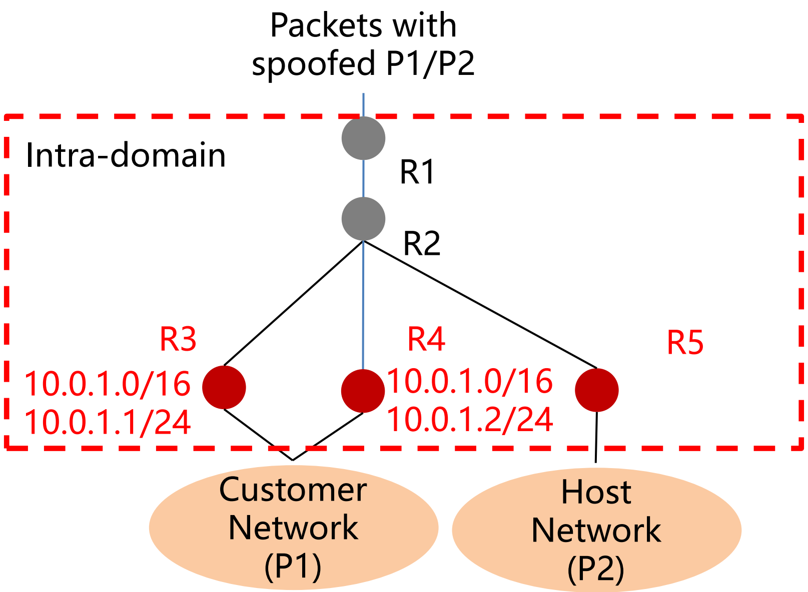
SAV Procedure - AS Border Routers



Intra-Domain SAV Deployment

1. AS border routers (e.g., R1 in Figure) learn all intra-domain prefixes from IGP protocol.
2. **R1 generates a blocklist containing these prefixes on the interface connected to other ASes.**
3. R1 blocks packets with spoofed source addresses from external ASes that match the blocklist. It also block packets with spoofed source addresses of internal links.

SAV Procedure - Customer-facing or Host-facing Routers



Intra-Domain SAV Deployment

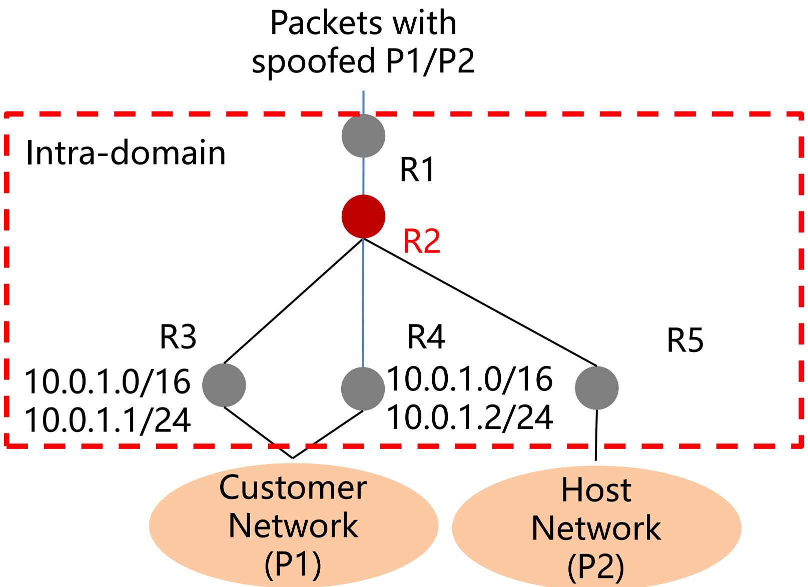
•**Single-homed Host Network (e.g., R5)**: Deploy strict uRPF.

- Interface on R5 prevents acceptance of packets with non-matching source addresses.

•**Multi-homed Customer Network (e.g., R3 and R4)**: Configure two kinds of routes (coarse and granular).

- **Deploy loose uRPF**. Packets are filtered based on both coarse and granular route matching.
- Edge router can determine automatically when to be strict, when to be loose, depending on the summary/detail routes configuration.

SAV Procedure - Internal Routers



Intra-Domain SAV Deployment

- **Deployment in Spine-Leaf Topology**: In some spine-leaf scenarios, like R2.
  - Instead of deploying SAV on leaf routers, deploying strict uRPF on the spine can block spoofed packets from host or customer networks.
- Normally, the routes within one IGP domain will be sysmmetrical, that is, the traffic will come from the interfaces that are the shortest distance to the source address. If not, enable the BM-SPF algorithm within the routers to assure this.

Overview of BM-SPF mechanism

- Based on [I-D.wang-lsr-bidirectional-metric-spf], BM-SPF (Bidirectional Metric based Shortest Path First Mechanism) can **avoid asymmetric routing**. Two neighbors use the same bidirectional link metrics for SPF algorithm path calculation.

- When routers communicate, packets are transmitted through the same path, and the same interface is used for sending and receiving packets between two routers in an AS with fully deployed BM-SPF.

Conclusion & Further Action

- **Summary**: BM-SPF-based SAV solution simplifies intra-domain SAV by leveraging symmetric routing. The new intra-domain SAV solution has the following characteristics:
  - **Consistency**: SAV procedures in internal, host-facing, and customer-facing routers are the same. AS border router procedures cover all relevant prefixes.
  - Covers all types of routers (host-facing, customer-facing, AS border) in different scenarios.
- **Any comments?**

wangw36@chinatelecom.cn
wangaj3@chinatelecom.cn
IETF122