General Source Address Validation Capabilities

M. Huang, W. Cheng, D. Li, N. Geng, L. Chen

Mar. 2025

Progress Since IETF 121

- ✓ Poll on whether SAV Mode 4 should be included
- ✓ WG adoption call
- ✓ Draft updated accordingly

Updates of SAV Modes

- Source address validation Mode 4 (prefix-based interface blocklist) came back based on WG poll

Mode	Scale	SAV rule	validation result
1	interface	1: interface-based source prefix allowlist	invalid if not matched
2	interface	2: interface-based source prefix blocklist	invalid if matched
3	router	3: prefix-based interface allowlist	invalid if not matched
4	router	4: prefix-based interface blocklist	invalid if matched

- Scenario values of Mode 4: A source-prefix-based rule with short interface blocklist works well when we only want block a few interfaces for a specific prefix, while
  - Mode 2 needs to config rules for each interface in the list to block the source prefix
  - Mode 3 needs a rule with much longer interface allowlist to address the requirement
  - Typical scenarios: 1) specific source address based DDoS attack from given directions; 2) block WAN interfaces from receiving traffic with inner source address.....

Updates of Validation Procedures

- Accordingly add mode 4 validation in the precedures
- More details about the relationship between 2 pairs of validation modes

1. Source address and incoming interface are saved while a packet arrives at the router
2. Interface-level validating (rules: interface-based source-prefix allowlist or blocklist)
   - Mode 1 and Mode 2 should not be enabled for an interface at same time. If so, Mode 2 must be ignored.
   - If Mode 1 is enabled, the packet will be only validated based on SAV rule 1, the procedure returns with corresponding validity state.
   - if Mode 2 is enabled, the procedure returns when the validation result is invalid, otherwise continue with route-level validation.
3. Router-level validating (rules: source prefix-based interface allowlist or blocklist)
   - Mode 3 and Mode 4 should not be enabled for a source prefix at same time. If so, Mode 4 must be ignored.
   - Mode 3 or Mode 4 validation based on rule 3 or rule 4, the procedure returns with the validation result.

Acknowledgments

- The authors appreciate the valuable comments from all members of the IETF SAVNET Working Group, especially the guidance and suggestion from Aijun Wang.
- We extend a special thanks to Mingxing Liu (Huawei) and Changwang Lin (New H3C) for their feedback and contributions from vendor implemention point of view.

Thanks!

Any Comments?