draft-huang-savnet-sav-table-07

General Source Address Validation Capabilities

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

Nov. 2024

Brief Review

- Introducing comprehensive SAV modes adaptive for various scenarios
  - Mode 1: general capability for interface-based source prefix allowlist, where FIB-based uRPF strict mode on customer interface does not work in asymmetric routing scenario. Most preferred mode for closed-connected interfaces, where complete knowledge of legitimate source prefix list is required.
  - Mode 2: interface-based source prefix blocklist, a much more efficient SAV tool than current ACL-based source address filtering, in terms of performance and scalability. In case complete knowledge of legitimate source prefix list is infeasible (e.g. for open-connected interfaces), but we do know a bunch of source prefix should not come in through a specific interface, e.g. inner source prefixes for WAN interface, other peer sub-network source prefixes.
  - Mode 3: prefix-based interface allowlist, a powerful tool that could be used to prevent a specific source-spoofing-based DDoS attack from outside networks. This mode could help define which interface will be good to take outside source prefixes.
- Introducing various traffic handling policies to deal with packets with "invalid" validation results, enabling bi-directional interaction with the monitor/security center.
  - Traffic control policies: discard, permit, rate limit, redirect……
  - Traffic monitor policies: sample……

Main Updates 1/2

Further decouple from any implementation implication

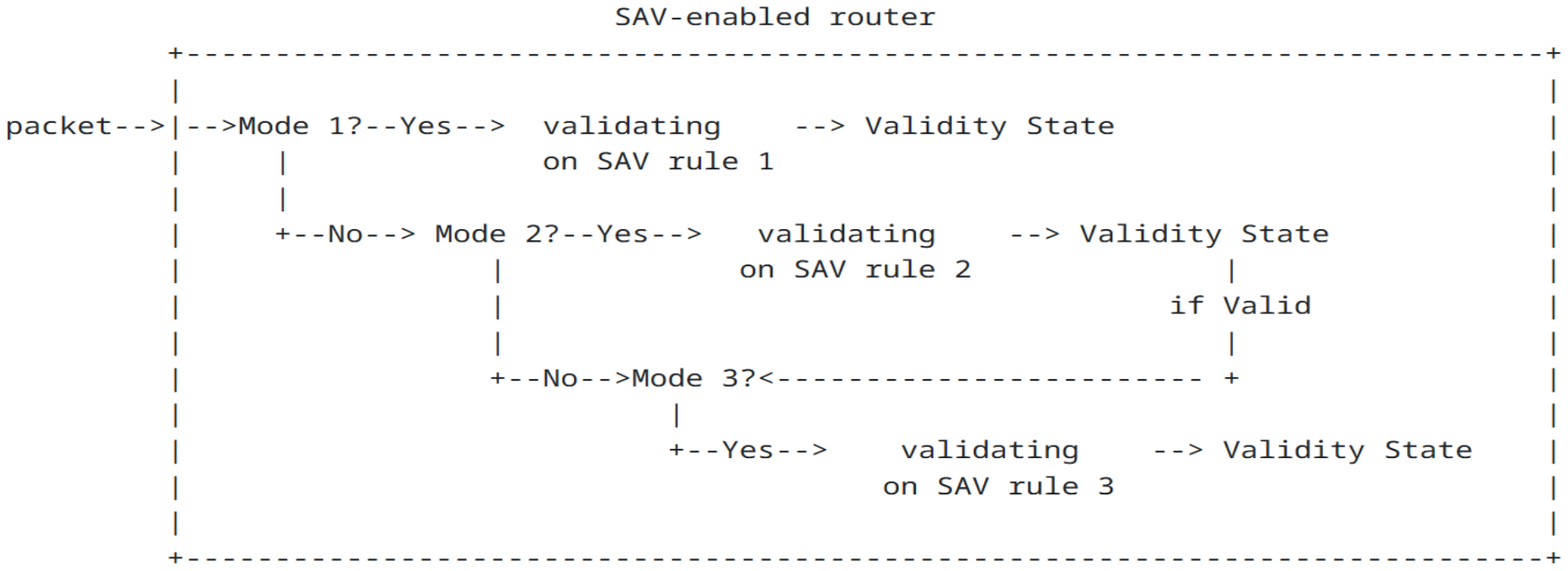
- Before: SAV rule expression for 3 modes shares similar FIB-like expression
- Now: native SAV rule expression for each mode

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

A comparison of 3 validation modes

Main Updates 2/2

- **Revise the validation procedure accordingly**



Note: Procedure illustrated here is more about the logical sequence between the modes from system outside point view, rather than a forwarding plane implementation logic

Some Comments

- Do we need separate memory space for the SAV table? What about the similar way as uRPF which shares FIB space to reduce the memory burden of the forwarding plane implementation?
  - First of all, this is up to vendor implementation, SAV table implementation is not the scope of this draft.
  - SAV table design is tricky for a vendor to balance between scalability (memory) vs performance (look-up efficiency), e.g. reusing some FIB rules might be one design choice . Anyhow, some degree additional cost is kind have to pay if we want make SAV capabilities move forward.
- currently 3 modes: 2 modes for interface-based validation and 1 modes for prefix-based validation. What if treat them equally, i.e. 2 modes for prefix-based validation either?
  - Normally, if we have a long interface list to be blocked for a specific source prefix, the prefix-based interface allowlist will work more efficiently. If we only want block a specific source prefix on a very short interface list, mode 2 might work alternatively, or Mode 4 should be better?
- Shall we provide details for SAV table (SAV rule and policy) segment design?
  - Currently we don't include SAV table segment details design, mainly because it might jump into implemention, especially forwarding plane implementation. It might be right place to design it in other protocols like YANG-based configuration, BGP-based distribution etc.

Summary

- Dedicated SAV tools are required if we want move SAV capabilities forward, rather than those currently just derived from FIB and ACL etc.
- Comprehensive validation modes with native source address based SAV rules, adaptive to various scenarios.
- Flexible traffic control and monitor policies open new possibilities powered by di-directional interaction with security center.
- Just general SAV capabilities, how to implement them is up to vendors.

Next Step

- Any comments are welcome
- Call for WG adoption

Thanks