General Source Address Validation Capabilities

draft-huang-savnet-sav-table-03

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

Nov 2023
Limitations of Existing SAV Capabilities

- **Application Scenario Limitations**
  - **uRPF. FIB-based**
    - **Strict mode.** For closed-connected interfaces, but not applicable to asymmetric routing scenarios, which exists in various scenarios, e.g. intra/inter-domain multi-homing access, inter-domain interconnection etc.
    - **Loose mode.** only for unannounced prefix, massive false negatives
  - **ACL-based source filtering.** Not dedicatedly designed for source prefix filtering
    - **Performance and scalability issue** due to long-key based lookup
    - Usually expert **maintenance efforts** required
  - More focus on outbound filtering, the capabilities are limited for open-connected interface protection

- **Lack of Flexible Traffic Handling Policy Application of Validation Results**
  - Current common practices just silently drop the spoofed packets, we don’t know who benefits from this and who is the attack source

  **Root Cause:** No tools specifically designed for source address filtering
  --the capabilities of current tools are derived from other functions, e.g. FIB, ACL
General Modes for Various Scenarios

- **Closed-connected scenarios** – be able to collect complete list of source prefixes
  - **Mode 1** – interface-based source prefix allowlist
    - Only listed source prefixes are allowed coming into the interface
    - Most preferred mode, mutually exclusive with other 2 modes
    - uRPF strict mode belongs to this mode. However, to overcome the limitation of asymmetric routing, native-source prefix based SAV rule is suggested. This is essential for new SAV architectures like EFP-uRPF(RFC8704), BAR-SAV, Intra-domain/Inter-domain SAVNET etc.

- **For open-connected scenarios** – not be able to collect complete list of source prefixes
  - **Mode 2** – interface-based source prefix blocklist
    - Block specific source prefixes coming into the interface
    - The list can be generated automatically, e.g. one of Intra-domain SAVNET architecture cases, blocking the incoming traffic with local source prefixes.
    - Or operators can configure the specific source prefixes to block from the interface. This is similar to ACL, but more native SAV rule expression with better performance and scalability
  - **Mode 3** – prefix-based interface allowlist/blocklist
    - This mode works in a router global level. For a given source prefix, the traffic only be allowed coming in through the specific interface list
    - Operators can configure the allowed interface list for a specific source prefix, to prevent DDoS attack related to this source prefix
    - Or the allowed interface list for specific prefixes can be generated automatically, e.g. one capability defined by Inter-domain SAVNET architecture
Flexible Traffic Handling Policies

- **Traffic Control Policies.** One and only one of the policies must be chosen for an “invalid” validation result.
  - Discard.
  - Permit. This could be chosen for tentative SAV rule configuration mainly for monitoring purpose
  - Rate Limit. This could be chosen while volumetric attacks happen
  - Redirect. Traffic will be redirected to scrubbing center etc.
  - ......

- **Traffic Monitor Policies.** These policies are options.
  - Sample. NetStream/Netflow could be applied to the “invalid” traffic for threat awareness and further analysis
  - ......
To achieve better source address validation, we need dedicated source prefix based rules rather than those are derived from other functions, e.g. FIB, ACL.

- Asymmetric routing challenge for closed-connected scenarios interface-based source prefix allowlist

- Enhance the source filtering capabilities for open-connected scenarios, i.e. Interface-based source prefix blocklist and source-prefix-based interface allowlist

To encourage operators deploy SAV, we need more policies for flexible traffic handling, visibility, analysis and mitigation closed-loop, rather than just silently dropping.

Adoption?
Thanks!