Updates on Bicone Source Address Validation

Presenter: Lancheng Qin

July 2025

Review of Bicone SAV

☐ Goal #1: Avoid improper block

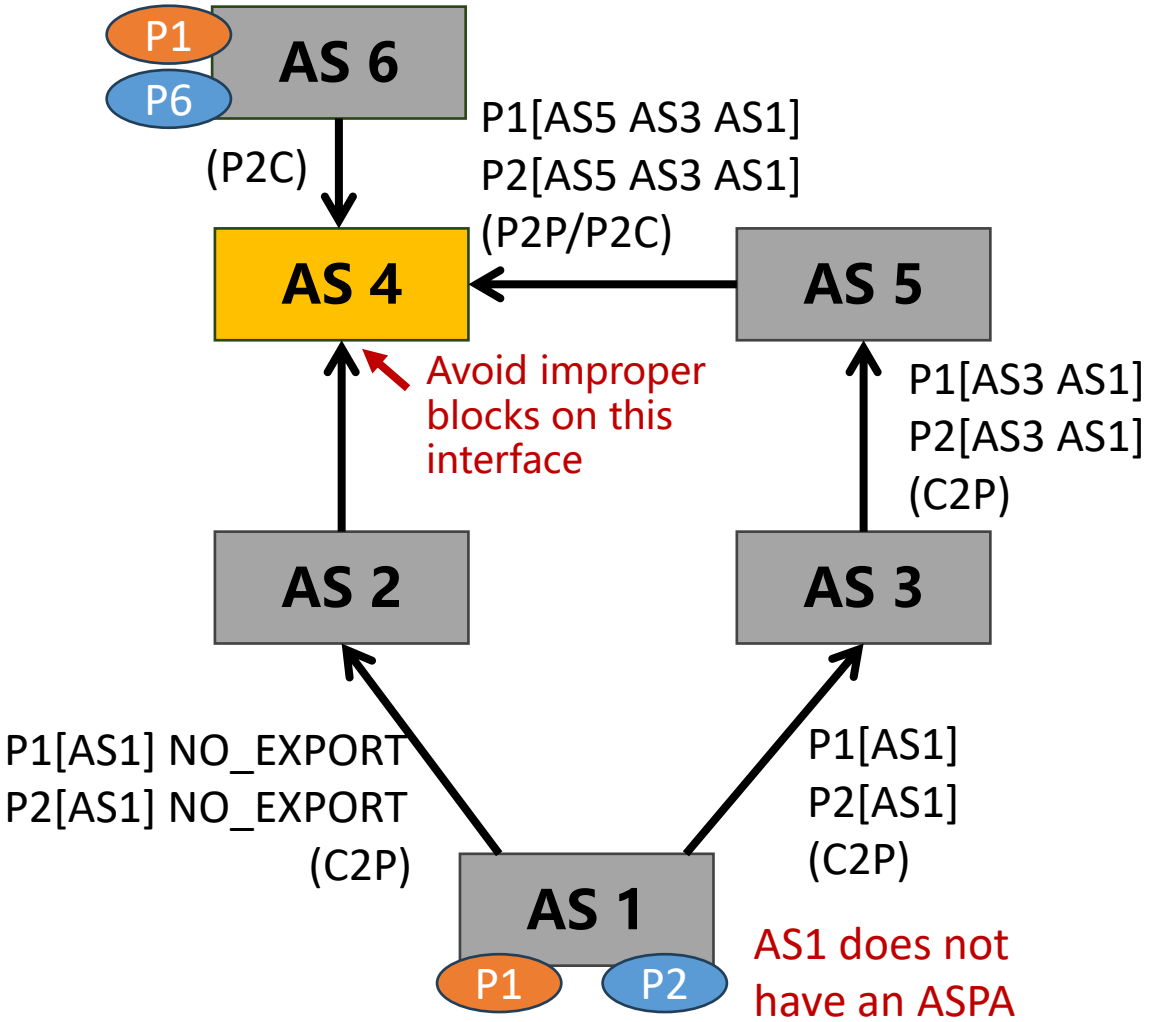
◆Existing allowlist-based SAV solutions have improper block problems in scenarios with limited propagation of prefixes and hidden prefixes, Bicone SAV aims to avoid improper blocks in these cases

◆A conservative way is to use Loose uRPF

☐ Goal #2: Reduce improper permit than solely using Loose uRPF

◆Bicone SAV aims to identify more source-spoofed data packets than solely using Loose uRPF

Review of Bicone SAV



An example of limited propagation of prefixes in the customer cone

- Blocklist contains **prefixes exclusively belonging to the Provider Cone**
  - These prefixes should not be used as source addresses in data packets received from any customer AS or lateral peer AS unless there is a route leak

Main Update: The Usage of TOAs

Using TOAs to improve the accuracy of Bicone SAV

- Step 1: Identify as many ASes in the provider cone as possible by using BGP UPDATES (AS_PATH) and ASPAs

- **Step 2: Identify prefixes exclusively belonging the provider cone by using TOAs (Main update)**

  - ◆TOAs are helpful to discover the hidden prefixes
  - ◆With the increasing prefix coverage of TOAs, the blocklist-based SAV filter progressively enhances its capability to block spoofed traffic

More details can be found in Section 5 of this document

Benefits and Trade-offs of Allowlist and Blocklist

- Allowlist-based filtering requires the completeness
  - If the allowlist is incomplete, it will improperly block legitimate traffic
  - If the allowlist is complete, it ensures zero improper block and zero improper permit
- Blocklist-based filtering does not require the completeness
  - One of its key advantages is that it does not risk blocking legitimate traffic
  - However, its effectiveness depends on how comprehensive the blocklist is
    - Spoofed traffic not covered by the list may still pass through (improper permit)

Recommendations

- If the network operator can determine that the allowlist is complete
  - ◆It is highly recommended to use an allowlist on the interface
- If the network operator cannot
  - ◆It is recommended to use Loose uRPF and the blocklist together
    - ➢Avoid improper block while blocking more spoofing data packets than solely using Loose uRPF or the blocklist
  - ◆Network operators are allowed to manually modify or configure the blocklist according to their local knowledge

Thanks!

Backup

Blocklist Generation Procedure

A detailed description of blocklist generation procedure is as follows:

1. Create the set of all directly connected Provider ASNs. Call it AS-set Z(1).
2. Create the set of all unique AS_PATHs in Adj-RIBs-In of all interfaces facing Providers.
3. For each unique AS_PATH with N (N>1) ASNs, i.e., [ASN_{1}, ASN_{2}, ..., ASN_{i}, ASN_{i+1}, ..., ASN_{N}] where ASN_{i} is the ith ASN in AS_PATH and the first ASN (i.e., ASN_{1}) is a directly connected Provider ASN. If all unique AS_PATHs have been processed, go to Step 8.
4. Let i = N
5. Decrement i to i-1.
6. If ASN_{i} authorizes ASN_{i+1} as a Provider in ASN_{i}'s ASPA, ASNs from ASN_{1} to ASN_{i+1} (i.e., ASN_{1}, ASN_{2}, ..., ASN_{i}, and ASN_{i+1}) are included in AS-set Z(1) and go to Step 3.
7. If i == 1, go to Step 3. Else, go to Step 5.
8. Let k = 1.
9. Increment k to k+1.
10. Create AS-set Z(k) of ASNs that are not in AS-set Z(k-1) but are authorized as Providers in ASPAs of any ASN in AS-set Z(k-1).
11. If AS-set Z(k) is null, then set k_max = k-1 and go to Step 12. Else, form the union of AS-set Z(k) and AS-set Z(k-1) as AS-set Z(k) and go to Step 9.
12. Select all TOAs in which the authorized origin ASN is in AS-set Z(k_max). Form the union of the sets of prefixes in the selected TOAs. Call it Prefix-set S.
13. For each unique Prefix P in Prefix-set S, check origin ASNs of Prefix P by using all TOAs. If all unique Prefixes in Prefix-set S have been processed, go to Step 15.
14. For each prefix of Prefix P and its sub prefixes, if the prefix has at least one origin ASN not in AS-set Z(k_max), remove the prefix from Prefix-set S. Go to Step 13.
15. Apply Prefix-set S as a blocklist on interfaces facing a customer or lateral peer AS.