Provider Interface SAV for Customer Cone Sources

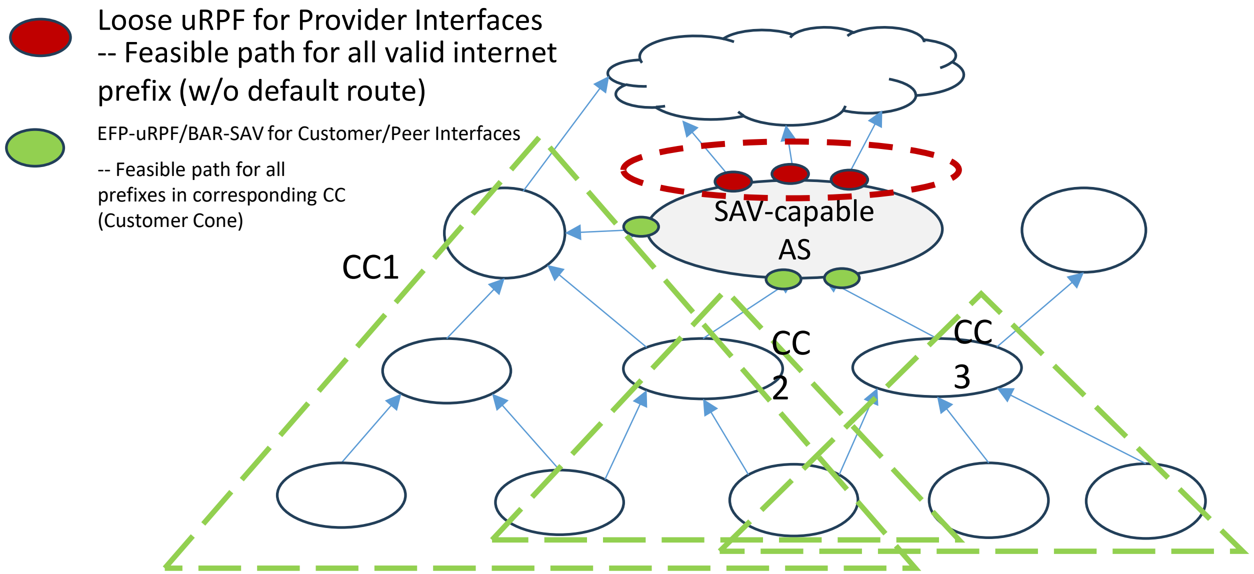
draft-huang-savnet-pi-sav-for-cc-00

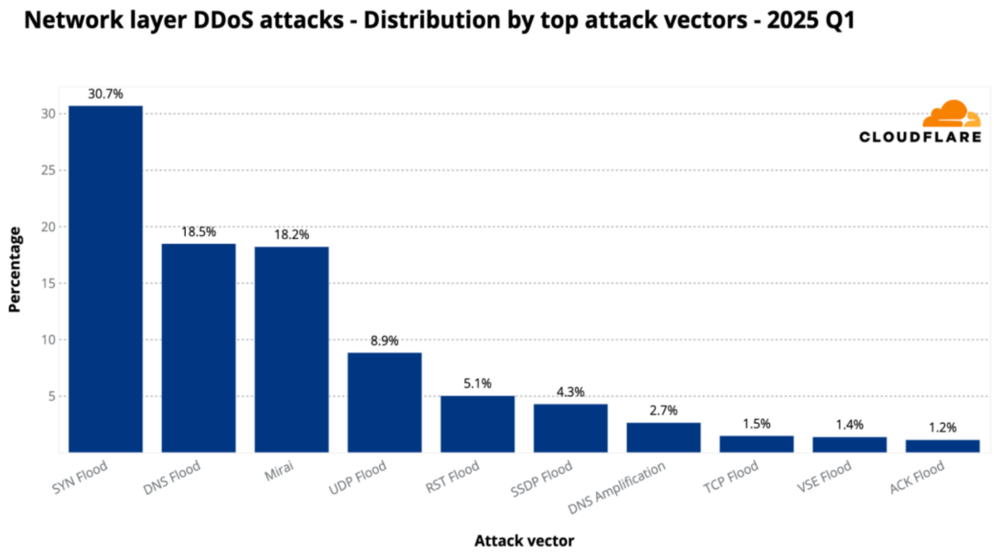
M. Huang, *N. Geng, D. Li*

Nov. 2025

Contents

Provider Interface Side Needs More Sophisticated Inter-Domain SAV Tools





- Works well on close-connected interfaces (customer access side connected with limited range of source).
- Not so well on open-connected interfaces. Meanwhile, from an operator point of view, provider interface sides face more severe source spoofing threats due to much wider source range and more complicated connection topology.

According to Cloudflare DDoS Report 2025Q1

- Majority of top network-layer DDoS attack vectors are directly or indirectly related to source address spoofing.
- The most significant increase was in network-layer DDoS attacks (a 509% YoY increase).

- **In additional to loose uRPF on provider interfaces, new solutions focus on how to narrow the allowed source prefix range by blocking more specific groups of source prefixes under different scenarios.**

PI-SAV Scenarios & Challenges

◆Scenario 1: PI-SAV for CC source.

The traffic between hosts in a customer cone more likely will not detour via the provider interfaces of the CC’ s top AS . Based on this assumption, PI-SAV for CC source can block the traffic with CC source address on the provider interfaces. This can be helpful to protect the reflecitve DDoS attacks aimed to local hosts by leveraging CC local servers.

◻ Key Challenges:

- If a customer AS in the CC has external transit provider, route policies (or transit link failure) may cause the traffic between CC hosts detour via the provider interfaces.

◻ Solutions

- PI-SAV for standalone CC. -- exclude the AS (and its sub-CC) with external provider from the CC.
- PI-SAV for standalone+ CC. -- identify whether there is route policy configuration or transit link failure which may cause the traffic detouring via the provider interfaces.

◆ Scenario 2: PI-SAV for general remote source.

Normally, AS-s will select a BGP AS-path among received path announcements/propagations by/via AS-d, and then reversely, the source traffic of AS-s will follow this path arrive AS-d. At AS-d ASBR, PI-SAV for general remote source can block the traffic with AS-s source address on the provider interfaces rather than active path.

◻ Challenges:

- BGP is uni-directional propagation protocol, routing decision made by AS-s along the propagation path is not awared by the upstream AS-d.
- the AS path via AS-d selected by AS-s for different origin AS/prefix might be different due to route rules and policies (e.g. AS-path prepending) applied in between, and then there might be different provider interfaces for AS-s traffic to visit AS-d. How likely is this scenarios to occur in practice?
- Active path may switch over between feasible paths due to failure or policy configuration.
- Real data plane path might not be aligned with BGP control plane path due to the direct traffic redirection. -- mainly for security scenario applications in limited domain, is not normal and suggested in global domain (BGP attributes based is suggested), and should avoid affect global traffic path.

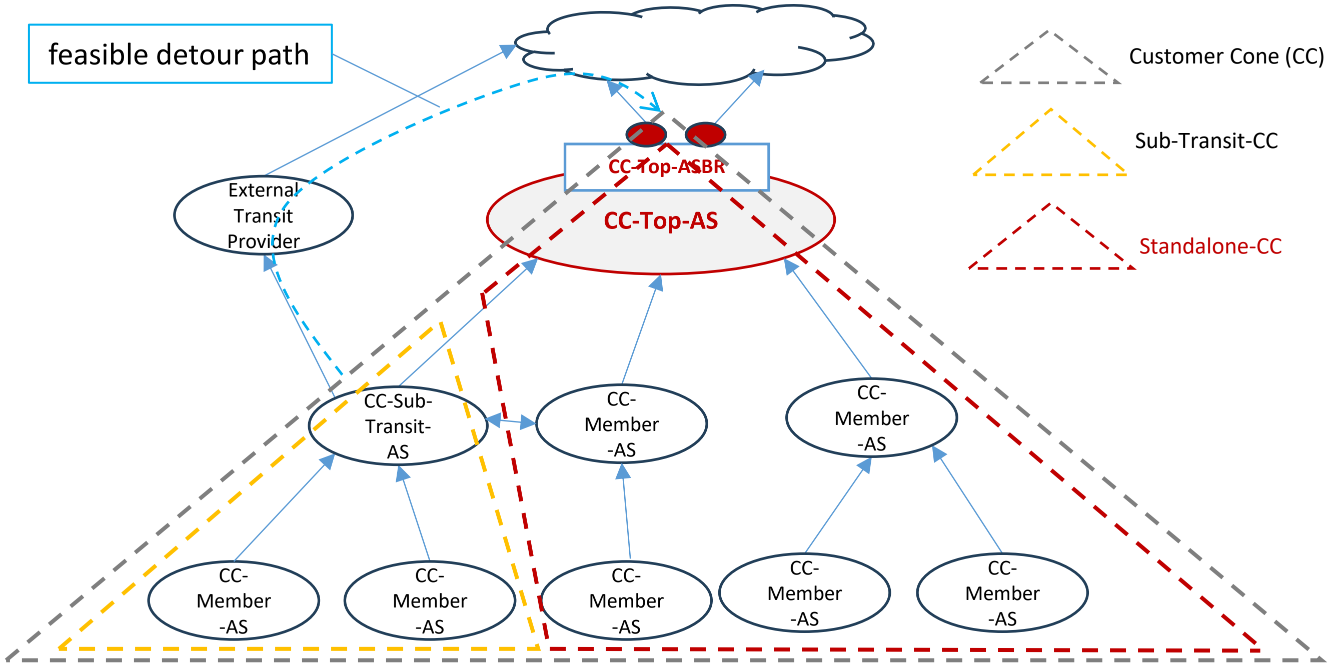
◻ Solutions

- Selected AS-path Notification. – when AS-s selects a BGP path related to AS-d, notify AS-d the selected AS-path by sending a message reversely.
- Active AS-path Self-Recognition. – AS-d detects the active path on provider interfaces by SAV-based traffic analysis.

Contents

- Background
- **PI-SAV for Standalone CC**
- PI-SAV for Standalone+ CC
- Considerations & Follow-ups

Overview of PI-SAV for Standalone CC



What is the Standalone CC of a CC-Top-AS

- Subset of the Customer Cone of CC-Top-AS, excluding Sub-Transit-CC (CC-Sub-Transit-AS and its CC).

Note: CC-Sub-Transit-AS is a CC-Member-AS who has alternative transit provider outside CC.

- All member ASes in the Standalone CC share the transit providers over the CC-Top-AS, no any other transit providers connecting to outside CC.
- According to BGP routing valley-free principle, traffic between members in the standalone CC won't go through the provider interfaces of CC-Top-ASBRs.

Goals of PI-SAV for Standalone CC Solution

- Based on the traffic routing characteristics of Standalone CC, an SAV prefix blocklist can be established at provider interfaces to prevent IP spoofing traffic with corresponding standalone CC source prefixes from entering the CC local networks.

Keys of PI-SAV for Standalone CC Solution

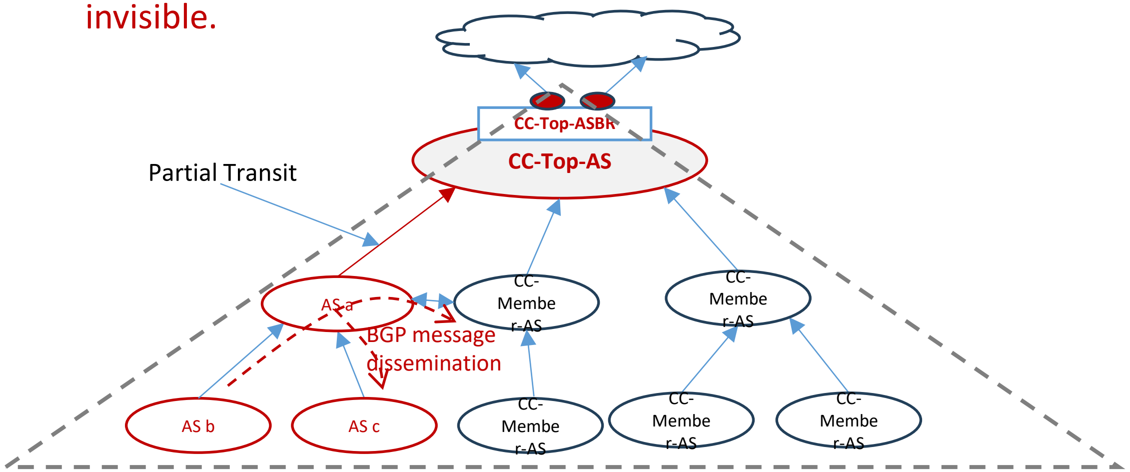
a) Standalone CC construction: identify and exclude all Sub-Transit-CCes without any omissions.

b) Prefix blocklist generation: is there any scenario that legitimate traffic with standalone CC source prefix can go through provider interfaces. Identify the related prefix(es) and remove them from the blocklist.

Construction of Standalone CC

Key Challenge: hidden AS caused by partial transit deployment

- Normally, CC-Top-ASBR can find all CC members in BGP local-RIBs, while partial transit – a special transit relationship, which rarely existing in the wild, can cause related AS (and its CC members) invisible.



Hidden AS scenarios

① Partial transit for all. AS-a receives BGP messages from its customer AS (AS-b, AS-c), then disseminates to its peer ASes and customer Ases, but not to its provider AS (CC-Top-AS) as normal. In this case, AS-a and its CC AS(AS-b, AS-c) are invisible in CC-Top-ASBR local-RIBs.

② Partial transit for specific customer AS (illustrated as above). AS-a receives BGP messages from its customer AS-b, then disseminates to its peer ASes and customer ASes, but not to its provider AS (CC-Top-AS) as normal. In this case, AS-b is invisible in CC-Top-ASBR local-RIBs.

Note: Normally, partial transit can be implemented by direct configuration on router transit link interface. or customer AS BGP messages with NO-EXPORT attributes.

General procedures for Standalone CC construction

--Based on BGP local-RIBs, and pre-registered partial transit information if applicable.

1. CC construction. Identify all CC member ASes for the CC-Top-AS, save transit relationship between them.
   a) Initial CC-Member-ASes: all direct customer Ases, and partial transit AS if any (pre-registration required)
   b) Identify all other CC-Member-ASes by searching BGP local-RIBs with initial member AS in the AS-path. Save the transit relationship between CC-Member-Ases.
2. Check whether each CC-Member-AS has external transit provider.
   a) Get RPKI ASPA and/or SLURM records, mark a CC member AS as CC-Sub-Transit-AS if there is external provider or record not available.
3. Deduct Sub-Transit-CC from the CC
   a) Forming Standalone CC by deducting Sub-Transit-CC (CC-Sub-Transit-AS and its CC) from the whole CC

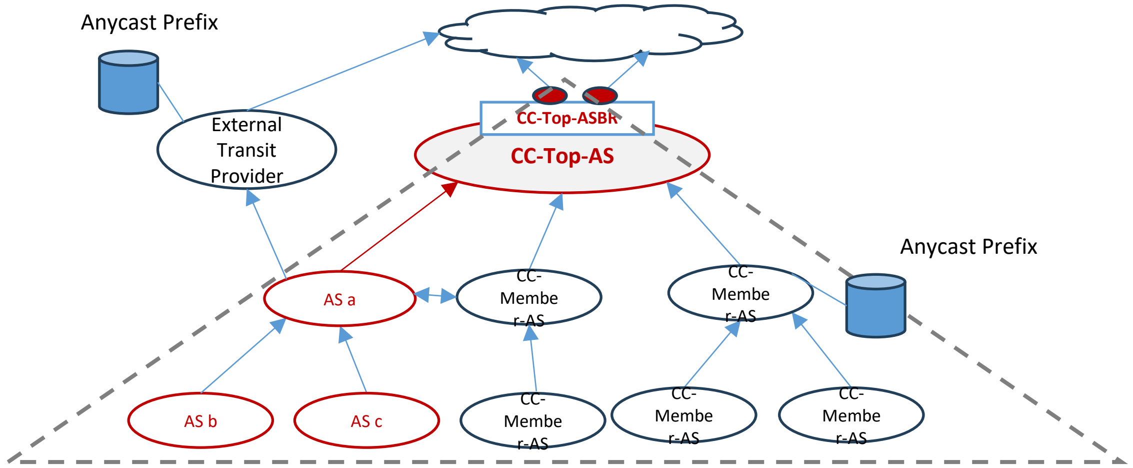
Note: why CC construction not based on RPKI ASPA records.

- It will be long run to get RPKI ASPA registration ubiquitous.
- RPKI can not approve records completeness and partial transit information covered by its own.
- RPKI record updates normal lay behind local-RIBs……

Generation of Prefix Blocklist

Key Challenge: an anycast prefix with multiple origin AS (MOAS) may cause traffic with a CC source prefix arrives CC via provider interfaces

- The situation may happen only when: CC-Top-ASBR chooses the internal origin AS-path, while some other ASBRs in the Standalone CC choose external origin AS-path.
- The prefix under this situation must be removed from the blocklist, but how to identify it?



General procedures for Standalone CC prefix blocklist generation

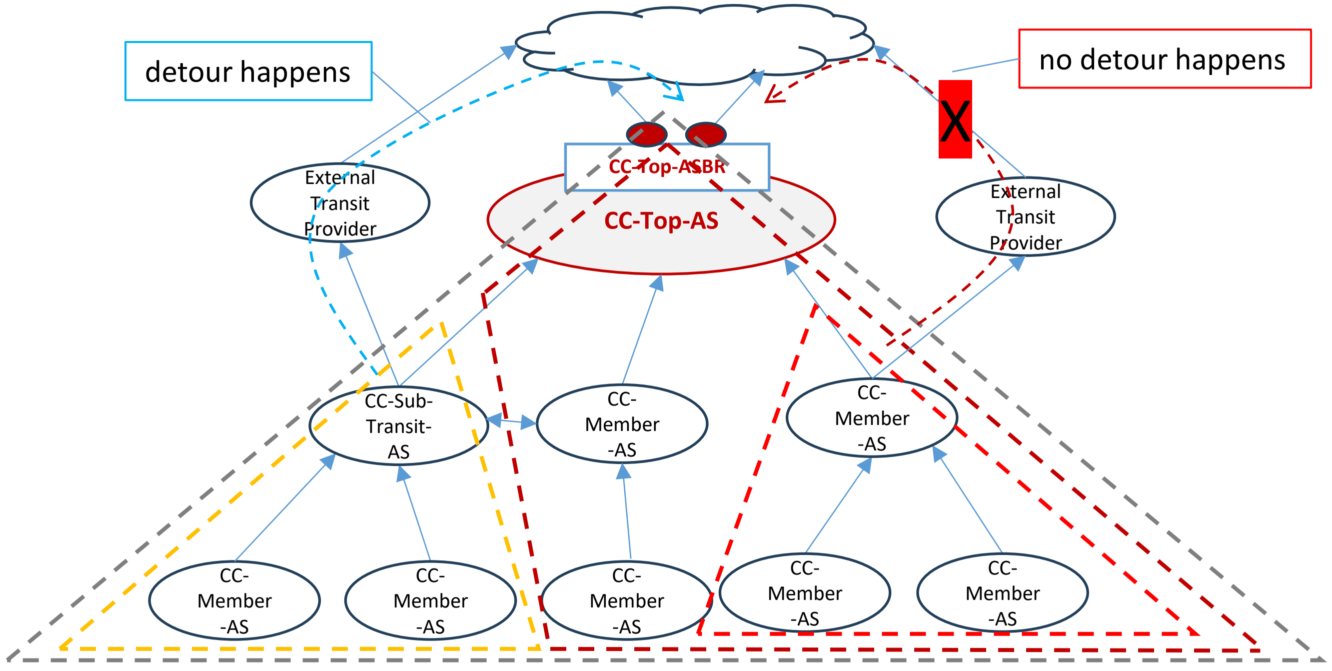
1. Prefix list for Standalone CC generation.
   a) Collect all prefixes initiated by member ASes of Standalone CC in the local-RIBs.
2. Identify the MOAS prefix in the prefix list.
   a) Search adj-RIBs-in for the Standalone CC prefix which is initiated by external AS.
3. Generation the prefix blocklist by deducting the previous MOAS prefix

Note:

- In case CC-Top-ASBR chooses external origin AS-path, the prefix will not be included in the Standalone CC prefix list. No worry about improper block for provider interface SAV.
- Current implementation of some routers may not have adj-RIBs-in local cache. Explicit MOAS prefix pre-registration may be needed.

Contents

Overview of PI-SAV for Standalone+ CC



What is the Standalone+ CC of a CC-Top-AS

- A subset of CC, a superset of Standalone CC.
- The external transit link provides possible detour path via provider interface, but only special policy/event (routing policy, internal transit link failure) can make it happen.
- Sub-Transit-CCes without the detour will be added to Standalone CC – forming Standalone+ CC.

Goals of PI-SAV for Standalone+ CC Solution

- Extend the scope of Standalone CC by dynamically adding Sub-Transit-CC with no detour path. It can generate much more complete prefix blocklist if there are too many CC-Sub-Transit-ASes or high position.
- Improve PI-SAV for Standalone CC solution by providing additional information support via in-band communication between CC member ASes, rather than heavily relying on out-band source (RPKI and/or local SLURM) -- more accurate, complete, and timely information support.

Keys of PI-SAV for Standalone+ CC Solution

a) Communication mechanism for real-time detour path perception between CC-Top-ASBR and CC-Sub-Transit-ASBR

Note:

- This document more focus on general protocol communication mechanism between CC-Top-ASBR and its CC-Member-ASes, not specific protocol design.

General Procedures of Solution

◆ **Conservative Mode** – solution support of all CC members not required

1) CC-Top-ASBR sets **the standalone CC** as the initial standalone+ CC. Then it sends a notification message to all CC-Member-Ases, which includes:
  -- The mode of PI-SAV for standalone+ CC.
  -- CC-Top-ASBR router information for further communication.
  -- The CC-Member-AS and CC provider information.

2) CC-Member-AS receives the notification message. Based on the BGP local-RIBs, CC-Member-AS verifies whether it has preferred an external AS-path via provider interface of CC-Top-ASBR for the BGP updates originated from CC member ASes. Then send response message back to CC-Top-ASBR.

3) CC-Top-ASBR receives the response message. It will add the corresponding CC-sub-transit-AS and its sub-transit-CCs into the standalone+ CC while the message shows no detour through alternative provider.

4) CC-Top-ASBR generates blocklist for Standalone+ CC like standalone CC does, including deduction of MOAS prefixes.

◆ **Aggressive Mode** – solution support of all CC members required

1) CC-Top-ASBR sets **the whole CC** as the initial standalone+ CC. Then it sends a notification message to all CC-Member-Ases, which includes:
  -- The mode of PI-SAV for standalone+ CC.
  -- CC-Top-ASBR router information for further communication.
  -- The CC-Member-AS and CC provider information.

2) CC-Member-AS receives the notification message. Based on the BGP local-RIBs, CC-Member-AS verifies whether it has preferred an external AS-path via provider interface of CC-Top-ASBR for the BGP updates originated from CC member ASes. Then send response message back to CC-Top-ASBR.

3) CC-Top-ASBR receives the response message. It will prune the corresponding CC-sub-transit-AS and its sub-standalone-CCs from the initial standalone+ CC while the message shows detour through alternative provider.

4) Only after CC-Top-AS gets response from all CC-sub-transit-ASes, generates blocklist for Standalone+ CC like standalone CC does, including deduction of MOAS prefixes

Contents

Considerations

- **Deployment Considerations**
  - Deployment location of the solution is recommended to be **at regional hub AS**, rather than a top/high tier AS with complex connection across regions.
  - The solution should allow the incremental deployment, which means some member ASes may not support the solution or some information (e.g. ASPA records for some ASes) may not be fully available.

- **Security Considerations**
  - Communication mechanism for Standalone+ CC solution must be equipped with the reliability and security features inherent in conventional transport protocols, including MITM (Man-in-the-middle) attack protection.
  - The details of security consideration should be covered by further specific protocol design.

Next Steps

- More feedback and discussion are always welcome
  - Overall ideas and solution options……
- Look forward to having more co-authors/contributors join in
- Working on subsequent documents
  - supplementary information provisioning
  - In-band communication protocol
  - ……

Thanks!