BGP Operations for Inter-domain SAV

draft-song-savnet-inter-domain-bgp-ops-03

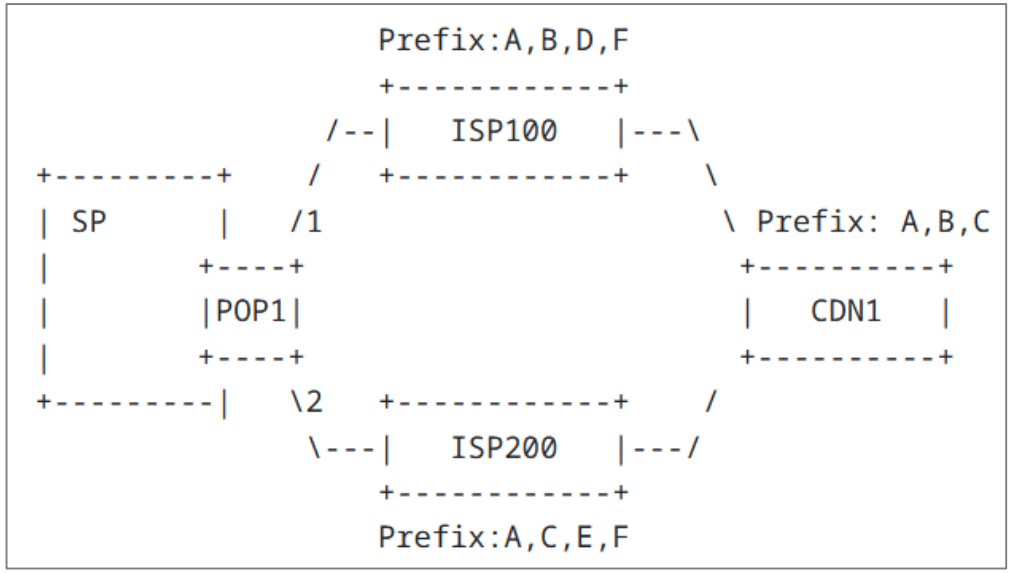
Xueyan Song (ZTE)
Chunning Dai (ZTE)
Shengnan Yue (CMCC)
Changwang Lin (H3C)

IETF 121th Meeting, November 2024

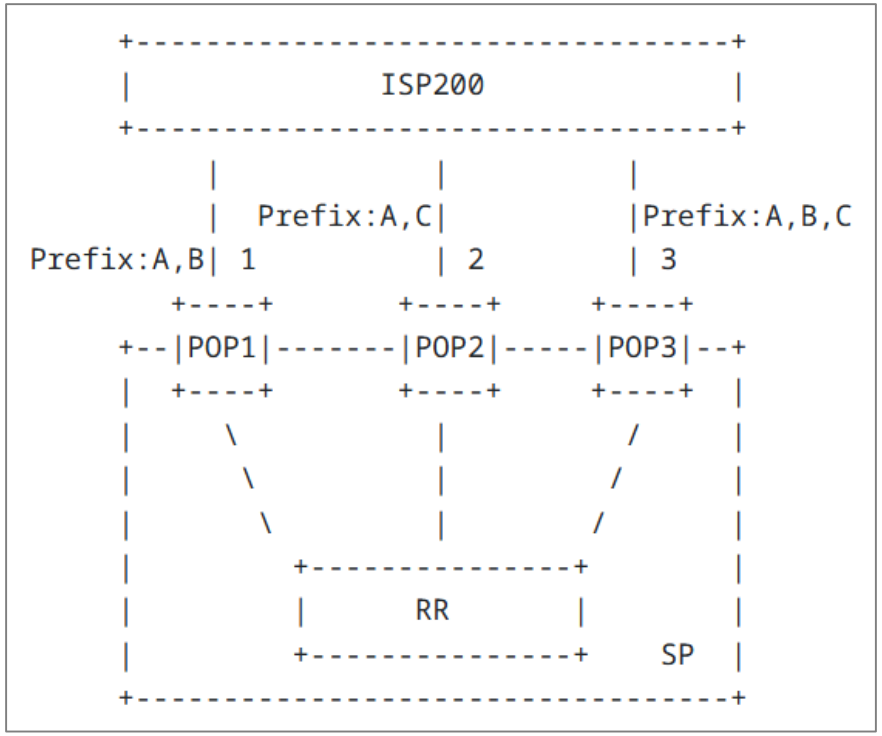
Overview

- This draft presents a BGP policy-based solution for source address validation in inter-domain networks.
- Draft History
  - This draft was presented during Meeting 118, where it received comments from Fang Gao that have been addressed in V02.
  - The V02 was subsequently presented in Meeting 119 and incorporated numerous updates based-on comments from Changwang Lin.
  - The V03 is being presented during this meeting. Key updates include:
    - Changed the method from POI to SDI
    - Updated the BGP policy-based solution
    - Revised figures and made editorial changes

Security Attacks



- **Routing security attack**
  - Route leaks, route prefix hijacking, source address spoofing
- **Filter location**
  - To identify and filter attack traffic at the location closest to the attack



- **Validation policy**
  - RPKI-based BGP POV ([RFC7115]), BGP AS path validation to mitigate route leaks, RPKI-ROA ([RFC6811], [RFC9319]) to prevent prefix hijacking
  - SAVNET resolves source address spoofing
    - To secure the incoming interface received traffic is in fact the right interface

BGP Policy-based Solution

- BGP policy-based solution aspects
  - SDI (Secure Domain Identifier) Assignment
  - BGP Export Policy for SDI Advertisement
  - BGP Ingress Filtering Policy
  - SAV Rule Generation
  - SAV Decision Process

BGP Policy-based Solution

- **Secure Domain Identifier (SDI)**
  - Definition: A tag used for BGP source prefix Secure Domain Identification (SDI).
  - Each secure domain is assigned a unique SDI within the reachable network.
- SDI Communication
  - Mapping secure domain with source prefix for secure communication.
  - SDI information is advertised alongside the source prefix.
- SDI Management
  - SDI is managed by SAVNET Agent, Controller or Management systems.
  - Responsible for the lifecycle management of SDIs, including joining, modifying, and leaving.
- Secure Domain Scope
  - A secure domain encompasses the route prefix and all routers within that.
  - The document acknowledges that the same SDI may span multiple domains.

BGP Policy-based Solution

- **Secure Domain**
  - Each secure domain MUST have a unique SDI within its reachable networks.
  - A secure domain consists of source prefixes with a shared secret
- **BGP Export Policy**
  - Configure SDI mapping with prefix, SDI identification advertised along with prefix advertisement
  - SDIs can be identical or different across multiple mapped domains, implementation dependent
- **BGP Import Policy**
  - Set an interface-to-SDI mapping policy for incoming packets in secure domain filtering
    - Allowing traffic only from trusted SDIs
    - Dropping packets that do not match the expected SDI
- **SAV Rule**
  - Generate SAV rules: prefix-to-interface (using SDI as proxy)
- **Decision Process**
  - Make decision based-on validation state (including parameters: source address, interface, validation status) and take traffic filtering action

Scalability Considerations

- Policies for Secure Domain Identifiers
  - AS Level Secure Domain Identifier (**AS SDI**)
    - Utilizes AS number information obtained from prefix advertisements for SAV filtering policy.
  - Community Level Secure Domain Identifier (**Community SDI**)
    - Uses BGP Community features for source address validation.
    - May require BGP extensions to carry necessary SDI information.
  - Router Level Secure Domain Identifier (**Router SDI**)
    - Reuses existing fields to indicate the directionality or location of source packets.
    - Suggests using router ID as the SDI.
  - Prefix Level Secure Domain Identifier (**Prefix SDI**)
    - Represents the smallest filtering granularity for source address validation.
    - Recommended to be deployed as a local policy due to the management of inter-BGP domains by different operators.

Security Considerations

- Traffic Validation
  - BGP route prefixes in the inter-domain network are treated as trusted.
  - Invalid routes not matching the current BGP route table should be blocked to prevent misuse.
- AS Validation
  - Validation of the originating Autonomous System (AS) for BGP routes is referenced in the BGP POV document (see RFC6811).
- Interface Verification
  - Verification of the incoming interface must confirm that it corresponds to the correct source prefix.
- Inter-domain SAV
  - Refer to [I-D. savnet-inter-domain-architecture] for inter-domain security considerations.
- SDI Communication
  - Communication regarding the assignment and processing of SDIs MUST be secured to ensure confidentiality.

Next Steps

- Feedback and reviews are welcome to help to improve the document further.

Thank You!