BGP Operations for Inter-domain SAV

draft-song-savnet-inter-domain-bgp-ops-01

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

IETF 119 Meeting, March 2024
Context

• This document introduces a BGP validation mechanism to filter invalid address and mitigate traffic spoofing.

• It attempts to collect and present some operational and security considerations to deploy Source Address Validation on routers in inter-domain networks.

• It is proposed at Oct 2023, first presented at IETF 118 meeting, the current revision is 01 which addressed comments received from Fang Gao, added scalability consideration and editorial changes.
Use Case

- **Routing security attack**
  - Route leaks, route prefix hijacking, source address spoofing

- **Filter location**
  - Access, Aggregation, Core Network
  - 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 to address source address spoofing
    - Source address prefix is trusted
    - Incoming interface received traffic is in fact the right interface
Solution Consideration

• Requirement
  • Support the ability to validate the accuracy of incoming interface of the traffic for specific source address prefixes.

• Validation Mechanism
  • Identify the route prefixes advertised by ASBRs as specific POIs
  • Bind POIs to interfaces and generate extended prefix table
  • Implement Source Address Validation to the traffic received in BGP validation entity and take traffic filtering action
Scalability Consideration

• POI policy deployed as different granularity to satisfy scalability requirements for source address validation
  • AS level Prefix Origin Identification (AS POI)
  • Community level Prefix Origin Identification (Community POI)
  • Router level Prefix Originated Indicator (Router POI)
  • Prefix level Prefix Origin Identification (Prefix POI)
Operation Consideration

• The BGP validation mechanism SHOULD support validation done at edge/boarder routers (i.e., ASBR) in a network.
• The BGP Prefix Origination Validation and BGP AS-path validation are out of the scope of the document.
• The BGP validation mechanism SHOULD support backward compatibility with existing routers.
• The BGP validation mechanism SHOULD be hardware friendly, does not require hardware upgrades nor big software updates.
• The BGP validation mechanism SHOULD comply with the routers existing policies and allow for incremental and partial network deployment.
• The BGP validation mechanism SHOULD support actual network implement requirement.

*Note: ZTE and New H3C have deployed the BGP POI method for source address validation in existing routers.
Next Steps

• Comments and suggestions are welcome, and make further refinement to improve the document.

Thank You!