BGP Extensions for Source Address Validation Networks (BGP SAVNET)

draft-geng-idr-bgp-savnet-02

N. Geng, Z. Li, Z. Tan, M. Liu, D. Li, F. Gao

Nov. 2023
Extend BGP protocols to advertise **SAV-specific information** between edge/border routers of one or multiple ASes (Follow the intra- and inter-domain architectures)

**SAV-specific information examples** (Will explain in the following slides)
- 1) Asymmetrically advertised routes; 2) Prefixes tagged as internal ones; 3) Target source prefixes with expected incoming directions

Assist **edge/border routers on the network boundary** to generate SAV rules
- Edge routers connected to subnets or stub customer AS generate rules for validating packets from users
- Border routers connected to other ASes generate rules for validating packets from other ASes

**BGP SAVNET Helps Construct the Validation Boundary for a Network**

- **Local routing information** → **Existing SAV** → **Future SAV**
- **SAV-specific information** → **Extended BGP**
- **Normal BGP**

Sometimes inaccurate SAV rules
More accurate SAV rules and adaptive to various scenarios
BGP SAVNET for Protecting Internal Prefixes

Features:
- **Border routers** can automatically collect internal prefixes and **simplifies operations** compared to manually configuring ACL rules.
- **Edge routers** can exchange asymmetrically advertised routes and **avoids improper block** of strict uRPF.
- **Good deployability**, i.e., upgrading part of routers can also work well.
- **Good convergence**, i.e., 1) similar propagation speed to route and 2) support independent and incremental update (no need to wait for complete information).

### Diagram

- **User’s normal route advertisement**
- **BGP SAVNET advertisement**

**Diagram Elements**
- **R1, R2, R3, R4**: Routers
- **P1, P2**: Subnet or stub AS
- **Deployed AS**: BGP SAVNET advertisement
- **Other ASes**: Block internal source prefixes (P1 and P2) at external interfaces
- **Edge routers automatically notify internal prefixes to border routers**
- **Exchange asymmetrically advertised routes**
- **Only permit internal source prefixes (not only P1 but also P2) at user interfaces**
- **Advertise P1, Advertise P2**
- **Subnet or stub AS**

---

3
BGP SAVNET for Protecting Remote Prefixes

Features:
- Source AS (AS1) can notify target source prefixes that need to be specially protected.
- Source AS (AS1) can notify the legitimate incoming directions of target source prefixes.
- Validation AS (AS4) can provide services like 1) proactive SAV, 2) reactive source address filtering for mitigating DDoS, 3) key source address forwarding path protection.
- Good deployability, i.e., any pair of upgraded ASes can work well.
- Good convergence, i.e., 1) similar propagation speed to route and 2) support independent and incremental update (no need to wait for complete information).
- Simple trust model.

Only permit target source prefixes (P1) at interfaces of AS2 and AS3.

Choose AS_PATHs of [AS4, AS2, AS1] and [AS4, AS3, AS1] in RIB for target source prefixes (P1) to reach AS4 and remote ASes.
Design Considerations

- Extending routing protocols for carrying SAV-specific information is an intuitive method
  - Existing SAV mechanisms primarily rely on local routing information.

- Extending BGP for advertising intra- and inter-domain SAV-specific information
  - Focus on doing validation on the network boundary for protecting internal and remote source prefixes. Using one protocol can adapt to various scenarios and simplify design workload
  - Reuse existing basic design and quality attributes to reduce design and development workload and facilitate application
  - Easy to extend and provide good service isolation
  - Explicit update and withdrawal without unnecessary periodic flooding
Next Step

- Make the design complete
- Comments are welcome
Thanks!