IGP-based Source Address Validation in Intra-domain Network (Intra-domain SAVNET)

Dan Li, Lancheng Qin, Xueyan Song, Changwang Lin, Shengnan Yue

July 23, 2024
Introduction

- [draft-ietf-savnet-intra-domain-problem-statement] summarizes the problems of existing intra-domain SAV solutions [BCP38, BCP84]

- [draft-ietf-savnet-intra-domain-architecture] proposes the architecture of intra-domain SAVNET to address the problems of existing intra-domain SAV solutions

- [draft-li-savnet-source-prefix-advertisement] proposes a protocol-independent SAV solution (i.e., SPA-based SAVNET) under intra-domain SAVNET architecture

- This document proposes an IGP-based method to implement SPA-based SAVNET in an intra-domain network
SPA-based SAVNET requires edge routers provide SAV-specific information to other routers through SPA messages.

- SAV-specific information contains Source Prefix, Interface Type, Subnet Tag, and Only Source Flag.
  - Source prefix is learned through the router’s local route to the facing subnet.
  - Only Source Flag is set by default.

- Edge routers and AS border routers generate prefix allowlists or blocklists by using SPA messages.

How to learn the Interface Type and Subnet Tag, and how to transmit SAV-specific information are not described in SPA-based SAVNET.

The focus of this document...
The Interface Type is configured based on the topology

Each subnet is assigned a unique Subnet Tag value when it first connects to the edge routers

The edge router can automatically match the Interface Type and Subnet Tag to source prefixes of the corresponding subnet

Different from ACL-based SAV, manual configurations are not needed when the source prefix of a subnet changes

- Only Interface Type may need to be updated when the topology changes
  - For example, from Single-homing Interface to Complete Multi-homing Interface
- Require less operational overhead than ACL-based SAV
SAV-specific Information Communication

- The SAVNET Agent of a Sender Router can provide its SAV-specific information to other SAVNET routers by using IGP.
  - When an edge router distributes IP prefix information of its subnet via IGP, it can carry the Interface Type, Subnet Tag, and Only Source Flag with the IP prefix information.
Two Approaches to SAV-specific Information Communication

- Approach #1: Use the existing Administrative Tag Sub-TLV to carry Interface Type, Subnet Tag, and Only Source Flag

- Approach #2: Define a new SAVNET Tag Sub-TLV to carry Interface Type, Subnet Tag, and Only Source Flag
Use the existing Administrative Tag Sub-TLV to carry Interface Type, Subnet Tag, and Only Source Flag

- Administrative Tag Sub-TLV of IS-IS [RFC 5130]
- Administrative Tag Sub-TLV of OSPF [draf-ietf-lsr-ospf-admin-tags]
- Administrative Tag Sub-TLV of OSPFv3 [draf-ietf-lsr-ospf-admin-tags]

Limitation

- Since the Administrative Tag Sub-TLV is not designed for SAV, using the Administrative Tag Sub-TLV may conflict with other routing policies that also use Administrative Tags
  - Additional operations are needed to avoid possible conflicts
Define a new SAVNET Tag Sub-TLV to carry Interface Type, Subnet Tag, and Only Source Flag

- A new SAVNET Tag Sub-TLV for IS-IS
- A new SAVNET Tag Sub-TLV for OSPF
- A new SAVNET Tag Sub-TLV for OSPFv3

Advantage

- Avoid conflicts with routing policies using existing Sub-TLVs and facilitate the operation of SAV
Next Step

- Improve the preliminary design of IGP-based method

- Your comments and suggestions are welcome!
  
  ◆ Which approach is more appropriate?

  ◆ Can Interface Type, Subnet Tag, and Only Source Flag be configured and updated in an automatic way?

  ◆ ......
Thanks!