BGP SPF Extensions for Intra-domain SAVNET
draft-lin-savnet-intra-domain-bgp-spf-extensions-00

Abstract

   This document describes the BGP SPF protocol extension that is
   required for Source Address Validation in Intra-domain. By extending
   BGP SPF and adding the BGP SPF protocol calculation procedure, the
   SAV information can be accurately calculated to realize the source
   address verification.

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   Internet-Drafts are draft documents valid for a maximum of six
   months and may be updated, replaced, or obsoleted by other documents
   at any time. It is inappropriate to use Internet-Drafts as
   reference material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html

   This Internet-Draft will expire on September 14 2023.

Copyright Notice

Table of Contents

[1](#). Introduction

[I-D.li-savnet-intra-domain-method] describes a method based on the
existing IGP routing protocol for the requirement of SAV in the
domain. By extending the message of the routing protocol, adding the
relevant protocol calculation procedure, each node has the ability
to independently calculate the valid incoming interface of a
specific prefix in domain, so as to verify the source address of the
traffic.

[I-D.ietf-lsvr-bgp-spf] describes BGP SPF based on BGP extension. It
uses BGP Link-State distribution and the Shortest Path First (SPF)
algorithm used by Internal Gateway Protocols (IGPs) such as OSPF.
BGP SPF can be effectively used as both the underlay protocol and
the overlay protocol in MSDC.

This document describes the BGP SPF protocol extension that is
required for Source Address Validation in Intra-domain. By extending
BGP SPF and adding the BGP SPF calculation procedure, the SAV

information can be accurately calculated to realize the source
address verification.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

2. Terminology

This document does not introduce more terminologies than [I-D.li-
savnet-intra-domain-problem-statement] and [I-D.lin-savnet-lsr-
intra-domain-method].

3. Calculate SAV Rules based on BGP SPF

The prefix that needs to participate in SAV rule calculation can be
specified through configuration. Using the mechanism introduced in
[I-D.lin-savnet-lsr-intra-domain-method], when BGP advertises such a
prefix, it attaches corresponding information to inform other
routing nodes.

Using the BGP SPF algorithm described in [I-D.ietf-lsvr-bgp-spf],
each routing node that enables the intra-domain SAV function can
take other routers in the SPF domain as the root to calculate the
shortest path tree.

Based on the shortest path tree with each router as the root, the
router can get the legal incoming interfaces of all protected
prefixes in the SPF domain, establish the SAV table, and guide the
verification of the source address of the packet in forwarding plane.

By extending BGP SPF, each routing node that enables the intra-
domain SAV function calculates independently SAV rule which includes
prefixes and valid incoming interfaces. If the source address of the
received packet hits the prefix of a SAV rule, and the interface
belongs to the valid incoming interfaces bound with the prefix, the
source address of the packet is considered legal, otherwise it is
illegal.

In order to identify the protected prefixes, the BGP SPF protocol
needs to be extended accordingly.

4. Advertise Protected Prefix Information in BGP SPF

The BGP SPF protocol is extended to advertise specific prefix
information. Each node that enables the intra-domain SAV function
calculates the SAV information according to the extended routing
message. This document contains the protocol extensions required for
single-area and multi-area scenarios.

4.1. BGP SPF Extension for protected prefixes

A BGP-LS Attribute TLV to BGP-LS-SPF Prefix NLRI called BGP-LS-SPF
Attribute Prefix-SAV TLV is defined to identify the protected
prefixes.

The TLV type value will be assigned by IANA.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Type(TBD)             |        Length(8 Octets)       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |            Flags               |             Reserved          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

> Type: TBD.

> Length: 4.

> Flags: Reserved flag field.

> Reserved: SHOULD be set to 0 on transmission and MUST be
ignored on reception

The BGP-LS-SPF Prefix-SAV TLV MUST be included with the BGP-LS-SPF
SAFI and SHOULD NOT be used for other SAFIs. And the Prefix-SAV TLV
is only relevant to Prefix NLRIs.

If the BGP-LS-SPF Prefix-SAV TLV is advertised and the advertised
value is not defined for all NLRI included in the BGP update, then
the BGP-LS-SPF Prefix-SAV TLV is ignored and not used in SAV
information calculation but is still announced to other BGP SPF
speakers. An implementation MAY log an error for further analysis.

If a BGP SPF speaker received the Prefix NLRI and the Prefix-SAV TLV
is received, it indicates that the prefix is a SAV protection prefix
and will participate in the calculation of SAV rules.

5. Consideration of redirection routing policy

In the actual deployment, some redirected forwarding policies may be used, such as PBR and QoS. The forwarding path of the packets processed by these policies may be inconsistent with the routing table, resulting in a router receiving the packets forwarded based on the routing table and the packets forwarded based on the redirected forwarding policies from different interfaces. Therefore, when calculating SAV rule, the influence of redirected forwarding policy should also be taken into account.

The extension of BGP SPF protocol to redirection routing policy will be improved in the next version.

6. IANA Considerations

This document defines an attribute TLV of BGP-LS-SPF NLRI. We request IANA to assign the type for the Prefix-SAV TLV from the "BGP-LS Node Descriptor, Link Descriptor, Prefix Descriptor, and Attribute TLVs" Registry.

```
+=========================+=================+====================+
| Attribute TLV           | Suggested Value | NLRI Applicability |
+=========================+=================+====================+
| Prefix-SAV              | TBD             | Prefix             |
+-------------------------+-----------------+--------------------+
```
                    Table 1: NLRI Attribute TLVs

7. Security Considerations

This document does not introduce any new security consideration.

8. References

8.1. Normative References

[I-D.li-savnet-intra-domain-problem-statement] Li, D., Wu, J., Qin, L., Huang, M., Geng, N., "Source Address Validation in Intra-domain Networks (Intra-domain SAVNET Gap Analysis, Problem Statement and Requirements", draft-li-savnet-intra-domain-problem-statement-07 (work in progress), 11 March 2023.

[I-D.lin-savnet-lsr-intra-domain-method] Lin, C., Qiu, Y., "Intra-domain SAVNET method", draft-lin-savnet-intra-domain-method-01(work in progress), 3 January 2023.

[I-D.ietf-lsvr-bgp-spf] Patel, K., Lindem, A., Zandi, S.,
           Henderickx, W., "BGP Link-State Shortest Path First (SPF)
           Routing", draft-ietf-lsvr-bgp-spf-21(work in progress), 9
           March 2023.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic
           Engineering", RFC 5305, DOI 10.17487/RFC5305, October
           2008, <https://www.rfc-editor.org/info/rfc5305>.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI
           10.17487/RFC5308, October 2008, <https://www.rfc-
           editor.org/info/rfc5308>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi
           Topology (MT) Routing in Intermediate System to
           Intermediate Systems (IS-ISs)", RFC 5120, DOI
           10.17487/RFC5120, February 2008, <https://www.rfc-
           editor.org/info/rfc5120>.

Contributors

Authors' Addresses

    Changwang Lin
    New H3C Technologies

    Email: linchangwang.04414@h3c.com

    Yuanxiang Qiu
    New H3C Technologies

    Email: qiuyuanxiang@h3c.com