Abstract

This document defines a new BGP non-transitive extended community to carry the BGPsec path validation state inside an autonomous system. Internal BGP (IBGP) speakers that receive this community string can use the embedded BGPsec validation state and configure local policies that allow it being used to influence their decision process. This is especially helpful because Section 5 of RFC 8205 specifically allows putting BGPsec path validation temporarily on hold. This allows reducing the load of validation particularly from IBGP learned routes.

Status of This Memo

This Internet-Draft is submitted to IETF 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/1id-abstracts.html

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

This document defines a new BGP non-transitive extended community to carry the BGPsec path validation state inside an autonomous system. Internal BGP (IBGP) speakers that receive this community string can use the embedded BGPsec validation state and configure local policies that allow it being used to influence their decision process. This is especially helpful because Section 5 of RFC 8205 specifically allows putting BGPsec path validation temporarily on hold. This allows reducing the load of validation particularly from IBGP learned routes.

1.1. Terminology

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. Suggested Reading

It is assumed that the reader understands BGPsec [RFC8205].

3. BGPsec Validation State Extended Community

The origin validation state extended community is a non-transitive extended community [RFC4360] with the following encoding:

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0x43    |      TBD      |             Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Reserved                   |validationstate|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The value of the high-order octet of the extended Type field is 0x43, which indicates it is non-transitive. The value of the low-order octet of the extended Type field as assigned by IANA is TBD. The Reserved field MUST be set to 0 and ignored upon the receipt of this community. The last octet of the extended community is an unsigned integer that gives the BGPsec route’s validation state, see [RFC8205] and [BORCHERT].
It can assume the following values:

+-------+------------------------------+
| Value | Meaning                      |
+-------+------------------------------+
|   0   | Lookup result = "Unverified" |
|   1   | Lookup result = "Valid"      |
|   2   | Lookup result = "Not valid"  |
+-------+------------------------------+

If the router is configured to support the extensions defined in this document, it SHOULD attach the BGPsec path validation state extended community to BGPsec UPDATE messages sent to IBGP peers by mapping the validation state in the last octet of the extended community. A receiving BGPsec speaker, in the absence of a validation state set based on local RPKI data, SHOULD derive a validation state from the last octet of the extended community, if present.

An implementation SHOULD NOT send more than one instance of the BGPsec path validation state extended community. However, if more than one instance is received, an implementation MUST disregard all instances other than the one with the numerically greatest validation state value. If the value received is greater than the largest specified value (2), the implementation MUST apply a strategy similar to attribute discard [RFC7606] by discarding the erroneous community and logging the error for further analysis.

By default, implementations MUST drop the BGPsec validation state extended community if received from an External BGP (eBGP) peer, without processing it further. Similarly, by default, an implementation SHOULD NOT send the community to EBGP peers. However, it SHOULD be possible to configure an implementation to send or accept the community when warranted. An example of a case where the community would reasonably be received from, or sent to, an eBGP peer is when two adjacent ASes are under control of the same administration. A second example is documented in [SIDR-RPKI].

4. Deployment Considerations

As specified in (Section 5) of [RFC8205] "a BGPsec speaker MAY temporarily defer validation of incoming BGPsec UPDATE messages. The treatment of such BGPsec UPDATE messages, whose validation has been deferred, is a matter of local policy". Furthermore one can envision that the operator of a BGPsec router decides to defer BGPsec validation learned via IBGP (including a trusted EBGP peer for instance controlled by the same operator as lined out in Section 3) when already validated by the peer. The router then will use the validation result learned via the community string and apply it the
the route. In case the peer did send the validation state unverified, the receiving router SHOULD apply the validation state "unverified" and perform BGPsec path validation as described in (section 5.2) of [RFC8205].

5. Security Considerations

Security considerations such as those described in [RFC4272] continue to apply. Because this document introduces an extended community that will generally be used to affect route selection, the analysis in Section 4.5 ("Falsification") of [RFC4593] is relevant. These issues are neither new nor unique to the validation extended community.

The security considerations provided in [RFC8205] apply equally to this application of BGPsec path validation. In addition, this document describes a scheme where router A outsources validation to some router B. If this scheme is used, the participating routers should have the appropriate trust relationship -- B should trust A either because they are under the same administrative control or for some other reason (for example, consider [SIDR-RPKI]). The security properties of the TCP connection between the two routers should also be considered. See Section 5.1 of [RFC7454] for advice regarding protection of the TCP connection.

6. IANA Considerations

IANA shall assign a new value from the "BGP Opaque Extended Community" type registry from the non-transitive range, to be called "BGPsec Validation State Extended Community".
6. References

6.1. Normative References


8.2. Informative References


Acknowledgements

The authors wish to thank P. Mohapatra, K. Patel, J. Scudder, D. Ward, and R. Bush for producing [RFC8097], which this document is based on. The authors would also like to acknowledge the valuable review and suggestions from K. Sriram on this document.

Authors’ Addresses

Oliver Borchert  
National Institute of Standards and Technology (NIST)  
100 Bureau Drive  
Gaithersburg, MD 20899  
United States of America

Email: oliver.borchert@nist.gov

Doug Montgomery  
National Institute of Standards and Technology (NIST)  
100 Bureau Drive  
Gaithersburg, MD 20899  
United States of America

Email: dougm@nist.gov