BGPsec Validation State Signaling
draft-sidrops-bgpsec-validation-signaling-01

Abstract

This document updates RFC 8097 by adding the BGPsec path validation state to the reserved portion of the extended community in RFC 8097. BGP 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 or EBGP learned routes when warranted.

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 updates the BGP non-transitive extended community as specified in RFC 8097 to also carry BGPsec path validation state information. BGP speakers that receive this community string can be used to configure local policies that use the signaled BGPsec path validation state to influence their decision process. When used in IBGP sessions, this new community can result in significant reduction in the computational load imposed by BGPsec path validation. When used in EBGP sessions, the new community can provide utility to receivers that are unable to perform BGPsec validation for themselves or put it temporarily on hold as specified in [RFC8205] (Section 5) as well as provides important diagnostic information about a peer’s validation process.
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. Validation State Extended Community

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

```
+-------+---------------------------------+
|      0x43     |      0x0      |              Reserved           |
|              | Path           |Origin         |
|              |validationstate|validationstate|
+---------------------------+-----------------------------+
```

As specified in [RFC 8097] (Section 2.), 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 0x00. The Reserved field MUST be set to 0 by the sender and ignored upon the receipt of this community.

The second to last octet is an unsigned integer that gives the route’s BGPsec path validation state as specified in [RFC8205] and [BORCHERT]. It can assume the following values:

```
+-------+---------------------------------+
|      Value      | Meaning             |
|----------------+---------------------|
| 0              | validation state = "Unverified" |
| 1              | validation state = "Valid" |
| 2              | validation state = "Not valid" |
+----------------+---------------------+
```
As specified in RFC 8097, the last octet of the extended community is an unsigned integer that gives the route’s origin validation state [RFC6811]. It can assume the following values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Validation state = &quot;valid&quot;</td>
</tr>
<tr>
<td>1</td>
<td>Validation state = &quot;not found&quot;</td>
</tr>
<tr>
<td>2</td>
<td>Validation state = &quot;invalid&quot;</td>
</tr>
</tbody>
</table>

If the router is configured to support the extension as defined in this document, it SHOULD attach the path/prefix-origin validation state extended community to UPDATE messages sent to BGP peers by mapping the validation states to the appropriate fields of the extended community as outlined above. This SHOULD be done automatically for IBGP peers and configurable for EBGP peers. Receiving BGP and BGPsec speakers SHOULD in the absence of local BGPsec/RPKI data derive the path validation from the second to last octet and the route origin validation from the last octet of the extended community.

Implementations MUST provide a configuration mechanism to allow the use of this community (both sending and receiving) to be disabled on a per-peer basis. By default, routers performing route origin validation or path validation SHOULD enable use of this community on all IBGP sessions.

By default, routers SHOULD disable the use of this community on all EBGP sessions. Implementations MUST NOT send more than one instance of the origin validation state extended community and MUST drop (without processing) the path/origin validation state extended community if received over an External BGP (EBGP) peering session that has not be explicitly configured to enable processing.

3.1. Error Handling at Peers

If more than one instance of the extended community is received, or if the value received for either origin validation or path validation is greater than the largest specified value (Section 3.), then the implementation MUST disregard all instances and MUST apply a strategy similar to attribute discard [RFC7606] by discarding the erroneous community and logging the error for further analysis.

3.2. Backwards Compatibility to RFC8097
 RFC 8097 originally specified five (5) octets as reserved. These five octets are to be ignored by implementations that receive the community string as specified in RFC 8097. Therefore, drafts such as this one that update RFC 8097 MUST use zero (0) for values whose meaning can be read the same regardless if created by a legacy router or a newer router that implements the respective draft.

As an example, using the value "0" for BGPsec path validation "unverified" accomplishes exactly that. Routers that do not implement BGPsec path validation do not validate and if they only implement RFC 8097 label the path validation state field correctly as "Unverified" and can be correctly read by routers that do implement this draft.

Routers that do BGPsec path validation and talk to legacy routers that do not still can use the path validation value because these legacy routers do ignore the path validation field.

4. Deployment Considerations

As specified in [RFC8205] (Section 5) "a BGPsec speaker MAY temporarily defer validation of incoming UPDATE messages. The treatment of such 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 local BGPsec validation when a validation state value is learned via IBGP or a trusted EBGP peer. The router then will use the validation result learned via the community string and apply it to the route. In case the peer did send the validation state "unverified" for BGPsec, the receiving router SHOULD perform BGPsec path validation as described in [RFC8205] (Section 5.2).

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 reasons as explained earlier. The security properties of the TCP connection between the two routers should also be considered. See [RFC7454] (Section 5.1) for advice regarding protection of the TCP connection.

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

Daniel Kopp
DE-CIX Management GmbH
Lichtstrasse 43i
Cologne  50825
Germany

Email: daniel.kopp@de-cix.net