Internet Engineering Task Force (IETF)
Internet-Draft
Intended status: Standards Track
Expires: January 28, 2021

O. Borchert
D. Montgomery
USA NIST
D. Kopp
DE-IX

July 27, 2020

BGPsec Validation State Signaling
draft-sidrops-bgpsec-validation-signaling-03

Abstract

This document defines a new BGP non-transitive extended community to carry the BGPsec path validation state. BGP speakers that receive this community string can use the embedded BGPsec validation state in conjunction with configured local policies to influence their decision process. The ability to accept and act on BGPsec path validation state from a neighbor allows for a reduction of path validation processing load and/or increased resilience in the event that a router is temporarily unable to perform local path validation.

Table of Contents

1. Introduction

This document defines a new BGP non-transitive extended community to carry the BGPsec path validation state. BGP speakers that receive this community string can use the embedded BGPsec validation state in conjunction with configured local policies to influence their decision process. The ability to accept and act on BGPsec path validation state from a neighbor allows for a reduction of path validation processing load and/or increased resilience in the event that a router is temporarily unable to perform local path validation.

1.1. Terminology

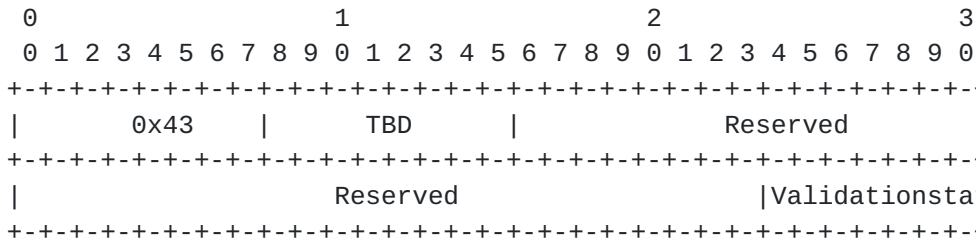
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Suggested Reading

It is assumed that the reader is familiar with BGPsec [RFC8205].

3. BGPsec Validation State Extended Community

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



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 path validation state, see [RFC8205] and [BORCHERT].

The validation state field can assume the following values:

Value	Meaning
0	Validation state = "Unverified"
1	Validation state = "Valid"
2	Validation state = "Not Valid"

If the router supports the extension as defined in this document, it SHOULD attach the BGPsec path validation state extended community to BGPsec UPDATE messages sent to BGP peers by mapping the locally computed validation state into the last octet of the extended community. This SHOULD be done automatically for iBGP peers and configurable for eBGP peers (see below).

Note, if a BGPsec speaker attaches this community to an UPDATE that was not explicitly validated at this router, the signaled validation state MUST be set to "Unverified".

A receiving BGPsec enabled router SHOULD use the received BGPsec path validation state in situations where a locally computed BGPsec validation result is not currently available. In the absence of the extended community, the receiving BGPsec enabled router MUST NOT make any assumption about the validation sate of the UPDATE.

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 SHOULD enable use of this community on all iBGP sessions and 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 BGPsec path 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 is greater than the largest specified value above (Section 3), then the implementation MUST disregard all instances of this community and MUST apply a strategy similar to "Attribute discard" [RFC7606] Section 2 by discarding the erroneous community and logging the error for further analysis.

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 sent the validation state "unverified", the receiving router SHOULD perform BGPsec path validation as described in [RFC8205] (Section 5.2).

5. 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 Path Validation State Extended Community".

6. 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.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <https://www.rfc-editor.org/info/rfc4360>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8205] Lepinski, M., Ed., and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

7.2. Informative References

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/info/rfc4272>.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, DOI 10.17487/RFC4593, October 2006, <https://www.rfc-editor.org/info/rfc4593>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <https://www.rfc-editor.org/info/rfc7454>.

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <https://www.rfc-editor.org/info/rfc7606>.

[RFC8097] Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R. Bush, "BGP Prefix Origin Validation State Extended Community", RFC 8097, DOI 10.17487/RFC8097, March 2017, <https://www.rfc-editor.org/info/rfc8097>.

[BORCHERT] Borchert, O., Montgomery, D., "BGPsec Validation State Unverified", draft-borchert-sidrops-bgpsec-validation-state-unverified-03, <https://tools.ietf.org/html/draft-borchert-sidrops-bgpsec-state-unverified-03>

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