Internet Engineering Task Force (IETF)
Internet-Draft
Intended status: Standards Track
Expires: February 27, 2020

O. Borchert
D. Montgomery
USA NIST

August 26, 2019

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

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.

Table of Contents

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

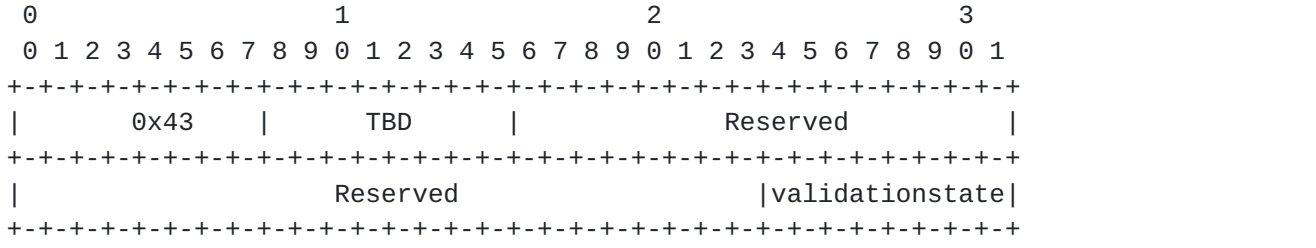
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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:



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

[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>.

[BORCHERT] Borchert, O., Montgomery, D., "BGPsec Validation State Unverified", draft-borchert-sidr-bgpsec-validation-state-unverified-02, <https://tools.ietf.org/html/draft-borchert-sidrops-bgpsec-state-unverified-02>

8.2. 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>.

[SIDR-RPKI] King, T., Kopp, D., Lambrianidis, A., and A. Fenioux, "Signaling Prefix Origin Validation Results from a Route-Server to Peers", Work in Progress, draft-ietf-sidrops-route-server-rpki-light-01, January 2017.

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