Internet Engineering Task Force (IETF)
Request for Comments: 8097
Category: Standards Track
ISSN: 2070-1721

P. Mohapatra
Sproute Networks
K. Patel
Arrcus, Inc.
J. Scudder
Juniper Networks
D. Ward
Cisco
R. Bush
Internet Initiative Japan, Inc.

March 2017

BGP Prefix Origin Validation State Extended Community

Abstract

This document defines a new BGP opaque extended community to carry the origination Autonomous System (AS) validation state inside an autonomous system. Internal BGP (IBGP) speakers that receive this validation state can configure local policies that allow it to influence their decision process.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8097.

Table of Contents

1. Introduction

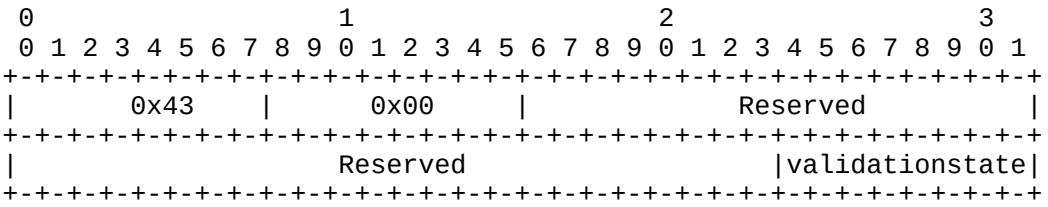
This document defines a new BGP opaque extended community to carry the origination AS validation state inside an autonomous system. IBGP speakers that receive this validation state can configure local policies that allow it to influence their decision process.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Origin Validation State Extended Community

The origin validation state extended community is an opaque 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 0x00. 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 route's validation state [RFC6811]. It can assume the following values:

Value	Meaning
0	Lookup result = "valid"
1	Lookup result = "not found"
2	Lookup result = "invalid"

If the router is configured to support the extensions defined in this document, it SHOULD attach the origin validation state extended community to BGP UPDATE messages sent to IBGP peers by mapping the computed validation state in the last octet of the extended

community. Similarly, a receiving BGP speaker, in the absence of validation state set based on local 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 origin 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 origin 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].

3. Deployment Considerations

In deployment scenarios in which not all the speakers in an autonomous system are upgraded to support the extensions defined in this document, it is necessary to define policies that match on the origin validation extended community and set another BGP attribute [RFC6811] that influences selection of the best path in the same way that an implementation of this extension would.

4. IANA Considerations

IANA has registered the value 0x00, with the name "BGP Origin Validation State Extended Community", in the "Non-Transitive Opaque Extended Community Sub-Types" registry.

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 origin validation extended community.

The security considerations provided in [RFC6811] apply equally to this application of origin 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. 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, <http://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, <http://www.rfc-editor.org/info/rfc4360>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <http://www.rfc-editor.org/info/rfc6811>.

6.2. Informative References

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc7606>.

[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 would like to acknowledge the valuable review and suggestions from Wesley George, Roque Gagliano, and Bruno Decraene on this document.

Authors' Addresses

Pradosh Mohapatra
Sproute Networks
Email: mpradosh@yahoo.com

Keyur Patel
Arrcus, Inc.
Email: keyur@arrcus.com

John Scudder
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089
United States of America
Email: jgs@juniper.net

Dave Ward
Cisco
170 W. Tasman Drive
San Jose, CA 95124
United States of America
Email: dward@cisco.com

Randy Bush
Internet Initiative Japan, Inc.
5147 Crystal Springs
Bainbridge Island, WA 98110
United States of America
Email: randy@psg.com