SIDR
Internet-Draft
Intended status: Standards Track
Expires: July 14, 2017

P. Mohapatra
Sproute Networks
K. Patel
Cisco
J. Scudder
Juniper Networks
D. Ward
Cisco
R. Bush
Internet Initiative Japan, Inc.
January 10, 2017

BGP Prefix Origin Validation State Extended Community draft-ietf-sidr-origin-validation-signaling-11

Abstract

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 allowing it to influence their decision process.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on July 14, 2017.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 2
2. Origin Validation State Extended Community 2
3. Deployment Considerations 3
4. Acknowledgements 4
5. IANA Considerations 4
6. Security Considerations 4
7. References 4
7.1. Normative References 4
7.2. Informative References 5
Authors' Addresses 5

1. Introduction

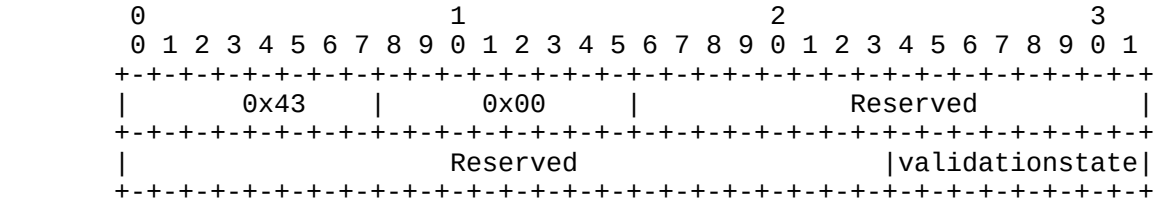
This document defines a new BGP opaque extended community to carry the origination AS validation state inside an autonomous system. IBGP speakers that receive this validation state can configure local policies allowing it to influence their decision process.

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 draft, 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 on the receiving IBGP speakers, the validation state of an IBGP route SHOULD be derived directly 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 EBGP peer, without further processing it. 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 [I-D.ietf-sidr-route-server-rpki-light].

3. Deployment Considerations

In deployment scenarios where 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 the best path selection the same way as what would have been enabled by an implementation of this extension.

4. Acknowledgements

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

5. IANA Considerations

IANA has assigned the value 0x00 from the "Non-Transitive Opaque Extended Community Sub-Types" registry. The value is called "BGP Origin Validation State Extended Community".

6. Security Considerations

Security considerations such as those described in [RFC4272] continue to apply. Since 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 [I-D.ietf-sidr-route-server-rpki-light]). The security properties of the propagation path between the two routers should also be considered. See [RFC7454] Section 5.1 for advice regarding protection of the propagation path.

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, <http://www.rfc-editor.org/info/rfc2119>.

[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, <http://www.rfc-editor.org/info/rfc4271>.

[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>.

7.2. Informative References

[I-D.ietf-sidr-route-server-rpki-light] King, T., Kopp, D., Lambrianidis, A., and A. Fenioux, "Signaling Prefix Origin Validation Results from a Route-Server to Peers", draft-ietf-sidr-route-server-rpki-light-01 (work in progress), December 2016.

[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>.

Authors' Addresses

Pradosh Mohapatra
Sproute Networks

Email: mpradosh@yahoo.com

Keyur Patel
Cisco
170 W. Tasman Drive
San Jose, CA 95124

Email: keyupate@cisco.com

John Scudder
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089

Email: jgs@juniper.net

Dave Ward
Cisco
170 W. Tasman Drive
San Jose, CA 95124

Email: dward@cisco.com

Randy Bush
Internet Initiative Japan, Inc.
5147 Crystal Springs
Bainbridge Island, Washington 98110

Email: randy@psg.com