Network Working Group
Internet-Draft
Updates: 6811 (if approved)
Intended status: Standards Track
Expires: May 2, 2020

R. Bush
Internet Initiative Japan & Arrcus
R. Volk
Deutsche Telekom
J. Heitz
Cisco

October 30, 2019

BGP RPKI-Based Origin Validation on Export
draft-ietf-sidrops-ov-egress-00

Abstract

A BGP speaker may perform RPKI origin validation not only on routes received from BGP neighbors and routes that are redistributed from other routing protocols, but also on routes it sends to BGP neighbors. For egress policy, it is important that the classification uses the effective origin AS of the processed route, which may specifically be altered by the commonly available knobs such as removing private ASs, confederation handling, and other modifications of the origin AS.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without normative meaning.

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 https://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 May 2, 2020.

1. Introduction

This document does not change the protocol or semantics of [RFC6811] of RPKI-based origin validation. It highlights an important use case of origin validation in eBGP egress policies, explaining specifics of correct implementation in this context.

As the origin AS may be modified by outbound policy, policy semantics based on RPKI Origin Validation state MUST be able to be applied separately on distribution into BGP and on egress.

When applied to egress policy, the effective origin AS MUST be used to determine the Origin Validation state. The effective origin AS is that which will actually be the origin AS in the announcement. It might be affected by removal of private AS(s), confederation, AS migration, etc. If there are any AS_PATH modifications resulting in origin AS change, then these MUST be taken into account.

2. Suggested Reading

It is assumed that the reader understands BGP, [RFC4271], the RPKI, [RFC6480], Route Origin Authorizations (ROAs), [RFC6482], RPKI-based Prefix Validation, [RFC6811], and Origin Validation Clarifications, [RFC8481].

3. Egress Processing

BGP implementations supporting RPKI-based origin validation SHOULD provide the same policy configuration primitives for decisions based on validation state available for use in ingress, redistribution, and egress policies. When applied to egress policy, validation state MUST be determined using the effective origin AS of the route as it will (or would) be announced to the peer. The effective origin AS

may differ from that of the route in the RIB due to commonly available knobs such as: removal of private ASs, AS path manipulation, confederation handling, etc.

Egress policy handling can provide more robust protection for outbound eBGP than relying solely on ingress (iBGP, eBGP, connected, static, etc.) redistribution being configured and working correctly - better support for the robustness principle.

4. Operational Considerations

Configurations may have complex policy where the final announced origin AS may not be easily predicted before all policies have been run. Therefore it SHOULD be possible to specify an origin validation policy which MUST BE run after such non-deterministic policies.

An operator SHOULD be able to list what announcements are not sent to a peer because they were marked Invalid, as long as the router still has them in memory.

5. Security Considerations

This document does not create security considerations beyond those of [RFC6811] and [RFC8481].

6. IANA Considerations

This document has no IANA Considerations.

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>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <http://www.rfc-editor.org/info/rfc6482>.

[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>.

[RFC8481] Bush, R., "Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)", RFC 8481, DOI 10.17487/RFC8481, September 2018, <https://www.rfc-editor.org/info/rfc8481>.

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

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <http://www.rfc-editor.org/info/rfc6480>.

Authors' Addresses

Randy Bush
Internet Initiative Japan & Arrcus
5147 Crystal Springs
Bainbridge Island, Washington 98110
US

Email: randy@psg.com

Ruediger Volk
Deutsche Telekom

Email: rv@nic.dtag.de

Jakob Heitz
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: jheitz@cisco.com