

Global Routing Operations
Internet-Draft
Intended status: Standards Track
Expires: May 4, 2017

J. Mauch
J. Snijders
NTT
G. Hankins
Nokia
October 31, 2016

**Default IPv4 and IPv6 Unicast EBGp Route Propagation Behavior Without
Policies
draft-ietf-grow-bgp-reject-02**

Abstract

This document defines the default behavior of a BGP speaker when there is no import or export policy associated with a BGP session for the IPv4 or IPv6 Unicast Address Family.

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](#)].

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 May 4, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Solution Requirements	3
3.	Acknowledgments	3
4.	Security Considerations	3
5.	IANA Considerations	3
6.	Contributors	3
7.	References	4
7.1.	Normative References	4
7.2.	Informative References	4
	Authors' Addresses	4

[1.](#) Introduction

BGP [[RFC4271](#)] speakers have many default settings which need to be revisited as part of improving the routing ecosystem. There is a need to provide guidance to BGP implementers for the default behaviors of a well functioning Internet ecosystem. Routing leaks [[RFC7908](#)] are part of the problem, but software defects and operator misconfigurations are just a few of the attacks on Internet stability we aim to address.

Many BGP speakers send and accept all routes from a peer by default. This practice dates back to the early days of the Internet, where operators were permissive in offering routing information to allow all networks to reach each other. As the Internet has become more densely interconnected, the risk of a misbehaving BGP speaker poses significant risks to Internet routing.

This specification intends to improve this situation by requiring the explicit configuration of a BGP import and export policy for any EBGp speaking session such as customers, peers, or confederation boundaries in a base router or VPN instances. When this solution is implemented, BGP speakers do not accept or send routes without policies configured on EBGp sessions.

2. Solution Requirements

The following requirements for the IPv4 and IPv6 Unicast Address Family apply to the solution described in this document:

- o Software **MUST** consider any routes from an EBGp peer invalid, if no import policy was configured.
- o Software **MUST NOT** advertise any routes to an EBGp peer, if no export policy was configured.
- o Software **SHOULD** provide protection from internal failures preventing the advertisement and acceptance of routes.
- o Software **MUST** operate in this mode by default.
- o Software **MAY** provide a configuration option to disable this security capability.

3. Acknowledgments

The authors would like to thank the following people for their comments, support and review: Shane Amante, Christopher Morrow, Robert Raszuk, Greg Skinner, Adam Chappell, Sriram Kotikalapudi, and Brian Dickson.

4. Security Considerations

This document addresses the basic security behavior of how a BGP speaker propagates routes in a default configuration without policies. Operators have a need for implementers to address the problem through a behavior change to mitigate against possible attacks from a permissive security behavior. Attacks and inadvertent advertisements cause business impact that can be mitigated by a secure default behavior.

5. IANA Considerations

This document has no actions for IANA.

6. Contributors

The following people contributed to successful deployment of solution described in this document:

Jakob Heitz
Cisco

Email: jheitz@cisco.com

Ondrej Filip
CZ.NIC

Email: ondrej.filip@nic.cz

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>>.

7.2. Informative References

[RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", [RFC 7908](#), DOI 10.17487/RFC7908, June 2016, <<http://www.rfc-editor.org/info/rfc7908>>.

Authors' Addresses

Jared Mauch
NTT Communications
8285 Reese Lane
Ann Arbor Michigan 48103
US

Email: jmauch@us.ntt.net

Job Snijders
NTT Communications
Theodorus Majofskistraat 100
Amsterdam 1065 SZ
NL

Email: job@ntt.net

Greg Hankins
Nokia
777 E. Middlefield Road
Mountain View, CA 94043
USA

Email: greg.hankins@nokia.com

