

Global Routing Operations  
Internet-Draft  
Updates: [4271](#) (if approved)  
Intended status: Standards Track  
Expires: November 9, 2017

J. Mauch  
Akamai  
J. Snijders  
NTT  
G. Hankins  
Nokia  
May 8, 2017

**Default EBGp Route Propagation Behavior Without Policies**  
**draft-ietf-grow-bgp-reject-07**

Abstract

This document updates [RFC4271](#) by defining the default behavior of a BGP speaker when there is no Import or Export Policy associated with an External BGP session.

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 November 9, 2017.

Copyright Notice

Copyright (c) 2017 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Changes to <a href="#">RFC4271</a> . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Acknowledgments . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">7.</a>	Contributors . . . . .	<a href="#">4</a>
<a href="#">8.</a>	References . . . . .	<a href="#">5</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">5</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">5</a>
<a href="#">Appendix A.</a>	Transition Considerations . . . . .	<a href="#">5</a>
<a href="#">A.1.</a>	N+1 N+2 Release Strategy . . . . .	<a href="#">5</a>
	Authors' Addresses . . . . .	<a href="#">6</a>

## [1.](#) Introduction

BGP routing security issues need to be addressed in order to make the Internet more stable. Route leaks [[RFC7908](#)] are part of the problem, but software defects or operator misconfiguration can contribute too. This document updates [[RFC4271](#)] in order to improve the default level of Internet routing security.

Many deployed BGP speakers send and accept any and all route announcements between their BGP neighbors by default. This practice dates back to the early days of the Internet, where operators were permissive in sending 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 both BGP Import and Export Policies for any External BGP (EBGP) session such as customers, peers, or confederation boundaries for all enabled address families. Through codification of the aforementioned requirement, operators will benefit from consistent behaviour across different BGP implementations.



BGP speakers following this specification do not use or send routes on EBGp sessions, unless configured to do otherwise.

## 2. Terminology

[RFC4271] describes a Policy Information Base (PIB) which contains local policies that can be applied to the information in the Routing Information Base (RIB). This document distinguishes the type of policy based on its application.

Import Policy: a local policy to be applied to the information contained in the Adj-RIBs-In. As described in [Section 3.2 \[RFC4271\]](#), the Adj-RIBs-In contain information learned from other BGP speakers, and the application of the Import Policy results in the routes that will be considered in the Decision Process by the local BGP speaker.

Export Policy: a local policy to be applied in selecting the information contained in the Adj-RIBs-Out. As described in [Section 3.2 \[RFC4271\]](#), the Adj-RIBs-Out contain information that has been selected for advertisement to other BGP speakers.

## 3. Changes to [RFC4271](#)

This section describes the Updates to [\[RFC4271\]](#) that define the default behavior of a BGP speaker when there are no Import or Export Policies associated with a particular EBGp session. A BGP speaker MAY provide a configuration option to deviate from the following updated behaviors.

The following paragraph is added to [Section 9.1](#) (Decision Process) after the fifth paragraph ending in "route aggregation and route information reduction":

Routes contained in an Adj-RIB-In associated with an EBGp peer SHALL NOT be considered eligible in the Decision Process if no explicit Import Policy has been applied.

The following paragraph is added to [Section 9.1.3](#) (Phase 3: Route Dissemination) after the third paragraph ending in "by means of an UPDATE message (see 9.2).":

Routes SHALL NOT be added to an Adj-RIB-Out associated with an EBGp peer if no explicit Export Policy has been applied.



#### **4. 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, Brian Dickson, Jeffrey Haas, John Heasley, Ignas Bagdonas, Donald Smith, Dale Worley, Alvaro Retana, and John Scudder.

#### **5. Security Considerations**

Permissive default routing policies can result in inadvertent effects such as route leaks [[RFC7908](#)], in general resulting in rerouting of traffic through an unexpected path. While it is possible for an operator to use monitoring to detect unexpected flows, there is no general framework that can be applied. These policies also have the potential to expose software defects or misconfiguration that could have unforeseen technical and business impacting effects.

The update to [[RFC4271](#)] specified in this document is intended to eliminate those inadvertent effects. Operators must explicitly configure Import and Export Policies to achieve their expected goals. There is of course no protection against a malicious or incorrect explicit configuration.

The security considerations described in [[RFC4271](#)] and the vulnerability analysis discussed in [[RFC4272](#)] also apply to this document.

#### **6. IANA Considerations**

This document has no actions for IANA.

#### **7. Contributors**

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

Jakob Heitz  
Cisco

Email: [jheitz@cisco.com](mailto:jheitz@cisco.com)

Ondrej Filip  
CZ.NIC

Email: [ondrej.filip@nic.cz](mailto:ondrej.filip@nic.cz)



## **8. References**

### **8.1. 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>>.

### **8.2. Informative References**

- [RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", [RFC 4272](#), DOI 10.17487/RFC4272, January 2006, <<http://www.rfc-editor.org/info/rfc4272>>.
- [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>>.

## **Appendix A. Transition Considerations**

This appendix is non-normative.

It is anticipated that transitioning to a compliant BGP implementation will require a process that may take several years.

It is understood and acknowledged that operators who are taking advantage of an undefined behavior will always be surprised by changes to said behavior.

### **A.1. N+1 N+2 Release Strategy**

An implementer could leverage an approach described as "the N+1 and N+2 release strategy". In release N+1, the implementer introduces a new default configuration parameter to indicate that the BGP speaker is operating in "ebgp insecure-mode". In addition to the introduction of the new parameter, an implementer could begin to display informational warnings to the operator that certain parts of the configuration are incomplete. In release N+1, operators of the BGP implementation become aware that a configurable default exists in the implementation, and can prepare accordingly. In release N+2 or





later, the inverse of the previous default configuration parameter that was introduced in release N+1 becomes the new default.

As a result, any new installation of release N+2 will adhere to this document. Installations upgraded from version release N+1 will adhere to the previous insecure behavior, if no modification was made to the "ebgp insecure-mode" configuration parameter.

#### Authors' Addresses

Jared Mauch  
Akamai Technologies  
8285 Reese Lane  
Ann Arbor Michigan 48103  
US

Email: [jared@akamai.com](mailto:jared@akamai.com)

Job Snijders  
NTT Communications  
Theodorus Majofskistraat 100  
Amsterdam 1065 SZ  
NL

Email: [job@ntt.net](mailto:job@ntt.net)

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

Email: [greg.hankins@nokia.com](mailto:greg.hankins@nokia.com)

