        Default External BGP (EBGP) Route Propagation Behavior without Policies

Abstract

   This document updates RFC 4271 by defining the default behavior of a
   BGP speaker when there is no Import or Export Policy associated with
   an External BGP session.

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/rfc8212.

Table of Contents

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 also
   contribute. This document updates [RFC4271] so that routes are
   neither imported nor exported unless specifically enabled by
   configuration. This change reduces the consequences of these
   problems and improves 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 behavior across different BGP
   implementations.

   BGP speakers following this specification do not use or send routes
   on EBGP sessions, unless specifically configured to do so.

2. Terminology

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

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Changes to RFC 4271

This section updates [RFC4271] to specify 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, which ends 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, which ends 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. Security Considerations

   Permissive default routing policies can result in inadvertent effects
   such as route leaks [RFC7908], in general resulting in routing 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.

5. IANA Considerations

   This document does not require any IANA actions.

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>.

   [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>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <http://www.rfc-editor.org/info/rfc8174>.

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>.

[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 for BGP Implementers

   This appendix is not normative.

   For an implementer, transitioning to a compliant BGP implementation
   may require a process that can 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.

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, Alvaro Retana, John Scudder, and Dale Worley.

Contributors

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

   Jakob Heitz
   Cisco

   Email: jheitz@cisco.com

   Ondrej Filip
   CZ.NIC

   Email: ondrej.filip@nic.cz

Authors' Addresses

   Jared Mauch
   Akamai Technologies
   8285 Reese Lane
   Ann Arbor Michigan 48103
   United States of America

   Email: jared@akamai.com

   Job Snijders
   NTT Communications
   Theodorus Majofskistraat 100
   Amsterdam 1065 SZ
   The Netherlands

   Email: job@ntt.net

   Greg Hankins
   Nokia
   777 E. Middlefield Road
   Mountain View, CA 94043
   United States of America

   Email: greg.hankins@nokia.com