Internet Engineering Task Force J. Mauch
Internet-Draft J. Snijders
Intended status: Standards Track NTT
Expires: May 4, 2016 November 1, 2015

By default reject propagation when no policy is associated with a BGP peering session.
draft-mauch-bgp-reject-01.txt

Abstract

This document defines the default behaviour of a BGP speaker when no explicit policy is associated with a BGP peering session.

Foreword

A placeholder to list general observations about this document.

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 [1].

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, 2016.

Table of Contents

1. Introduction 2
2. Definitions and Acronyms 3
3. Solution Requirements 3
4. Acknowledgements 3
5. Security Considerations 3
6. References 3
6.1. Normative References 3
6.2. Informative References 4
Authors' Addresses 4

1. Introduction

BGP speakers have many default settings which need to be revisited as part of improving the routing ecosystem. There is a need to provide guidace to BGP implementors for the default behaviors of a well functioning internet ecosystem. Routing leaks [3] 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.

Usually BGP speakers accept all routes from a configured peer or neighbor. This practice dates back to the early days of internet protocols in being very permissive in offering routing information to allow all networks to reach each other. With the core of the internet becoming more densely interconnected the risk of a misbehaving edge device or BGP speaking customer poses signficiant risks to the reachability of critical services.

This proposal intends to solve this situation with the requiring the explicity configuration of BGP policy for any non-iBGP speaking session such as customers, peers or confederation boundaries. When this solution is implemented, devices will no longer pass routes without explicit policy.

2. Definitions and Acronyms

- BGP: Border Gateway Protocol [2]

3. Solution Requirements

The following requirements apply to the solution described in this document:

- Software MUST mark any routes from an eBGP peer as 'invalid' in the Adj-RIB-In, if no explicit policy was configured.
- Software MUST NOT advertise any routes to an eBGP peer without an operator configuring a policy
- Software MUST NOT require a configuration directive to operate in this mode.
- Software MUST provide protection from internal failures preventing the advertisement and acceptance of routes
- Software MAY provide a configuration option to disable this security capability.

4. Acknowledgements

The authors would like to thank the following people for their comments and support: Shane Amante, Christopher Morrow, Robert Raszuk.

5. Security Considerations

This document addresses the basic security posture of a BGP speaking device within a network. Operators have a need for implementors to address the problem through a behavior change to mitigate against possible attacks from a permissive security posture. Attacks and inadvertent advertisements cause business impact necessitating this default behavior.

6. References

6.1. Normative References

[1] 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>.

[2] 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>.

6.2. Informative References

[3] "Methods for Detection and Mitigation of BGP Route Leaks", <https://tools.ietf.org/html/draft-sriram-idr-route-leak-detection-mitigation>.

Authors' Addresses

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

Email: jmauch@us.ntt.net

Job Snijders
NTT Communications, Inc.
Amsterdam
NL

Email: job@ntt.net