Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 30, 2018

A. Azimov
E. Bogomazov
Qrator Labs
R. Bush
Internet Initiative Japan
K. Patel
Arrcus, Inc.
K. Sriram
US NIST

June 28, 2018

Route Leak Prevention using Roles in Update and Open messages
draft-ietf-idr-bgp-open-policy-03

Abstract

Route Leaks are the propagation of BGP prefixes which violate assumptions of BGP topology relationships; e.g. passing a route learned from one peer to another peer or to a transit provider, passing a route learned from one transit provider to another transit provider or to a peer. Today, approaches to leak prevention rely on marking routes according to operator configuration options without any check that the configuration corresponds to that of the BGP neighbor, or enforcement that the two BGP speakers agree on the relationship. This document enhances BGP Open to establish agreement of the (peer, customer, provider, internal) relationship of two neighboring BGP speakers to enforce appropriate configuration on both sides. Propagated routes are then marked with an iOTC attribute according to agreed relationship allowing prevention of route leaks.

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 RFC 2119 [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

Copyright Notice

Table of Contents

1. Preamble

1.1. Peering Relationships

Despite uses of words such as "Customer," "Peer." etc. the intent is not business relationships, who pays whom, etc. These are common terms to represent restrictions on BGP route propagation, sometimes known as Gao-Rexford model. E.g. if A is a "peer" of B and C, A does not propagate B's prefixes to C. If D is a "customer" of E and F, D does not propagate prefixes learned from E to F.

As the whole point of route leak detection and prevention is to prevent vioation of these relationships, they are inescapable.

2. Introduction

This document specifies a new BGP Capability Code, [RFC5492] Sec 4, which two BGP speakers MAY use to ensure that they MUST agree on their relationship; i.e. customer and provider or peers. Either or both may optionally be configured to require that this option be exchanged for the BGP Open to succeed.

Also this document specifies a way to mark routes according to BGP Roles established in OPEN message and a way to create double-boundary filters for prevention of route leaks via new BGP Path Attribute.

For the purpose of this document, BGP route leaks are when a BGP route was learned from transit provider or peer and is announced to another provider or peer. See [I-D.ietf-grow-route-leak-problem-definition]. These are usually the result of misconfigured or absent BGP route filtering or lack of coordination between two BGP speakers.

[I-D.ietf-idr-route-leak-detection-mitigation] The mechanism proposed in that draft provides the opportunity to detect route leaks made by third parties but provides no support to strongly prevent route leak creation.

Also, route tagging which relies on operator maintained policy configuration is too easily and too often misconfigured.

3. Role Definitions

As many of these terms are used differently in various contexts, it is worth being explicit.

A Provider: sends their own routes and (possibly) a subset of routes learned from their other customers, peers, and transit providers to their customer.

A Customer: accepts 'transit routes' from its provider(s) and announces their own routes and the routes they have learned from the transitive closure of their customers (AKA their 'customer cone') to their provider(s).

A Peer: announces their routes and the routes from their customer cone to other Peers.

An Internal: announces all routes, accepts all routes.

Of course, any BGP speaker may apply policy to reduce what is announced, and a recipient may apply policy to reduce the set of routes they accept.

4. BGP Role

BGP Role is new configuration option that SHOULD be configured at each BGP session. It reflects the real-world agreement between two BGP speakers about their peering relationship.

Allowed Role values for eBGP sessions are:

- Provider - sender is a transit provider to neighbor;
- Customer - sender is customer of neighbor;
- Peer - sender and neighbor are peers;
- Internal - sender and neighbor is part of same organization.

For iBGP sessions only Internal role MAY be configured.

Since BGP Role reflects the relationship between two BGP speakers, it could also be used for more than route leak mitigation.

5. Role capability

The TLV (type, length, value) of the BGP Role capability are:

- Type - <TBD1>;
- Length - 1 (octet);
- Value - integer corresponding to speaker' BGP Role.

Value	Role name
0	Sender is Peer
1	Sender is Provider
2	Sender is Customer
3	Sender is Internal

Table 1: Predefined BGP Role Values

6. Role correctness

Section 4 described how BGP Role is a reflection of the relationship between two BGP speakers. But the mere presence of BGP Role doesn't automatically guarantee role agreement between two BGP peers.

To enforce correctness, the BGP Role check is used with a set of constrains on how speakers' BGP Roles MUST corresponded. Of course, each speaker MUST announce and accept the BGP Role capability in the BGP OPEN message exchange.

If a speaker receives a BGP Role capability, it MUST check value of the received capability with its own BGP Role (if it is set). The allowed pairings are (first a sender's Role, second the receiver's Role):

Sender Role	Receiver Role
Peer	Peer
Provider	Customer
Customer	Provider
Internal	Internal

Table 2: Allowed Role Capabilities

In case of any other pair of roles, speaker MUST send a Role Mismatch Notification (code 2, sub-code <TBD2>).

6.1. Strict mode

A new BGP configuration option "strict mode" is defined with values of true or false. If set to true, then the speaker MUST refuse to establish a BGP session with peers which do not announce the BGP Role capability in their OPEN message. If a speaker rejects a connection, it MUST send a Connection Rejected Notification [RFC4486]

(Notification with error code 6, subcode 5). By default strict mode SHOULD be set to false for backward compatibility with BGP speakers, that do not yet support this mechanism.

7. BGP Internal Only To Customer attribute

The Internal Only To Customer (iOTC) attribute is a new optional, non-transitive BGP Path attribute with the Type Code <TBD3>. This attribute has zero length as it is used only as a flag.

There are three rules of iOTC attribute usage:

1. The iOTC attribute MUST be added to all incoming routes if the receiver's Role is Customer or Peer;

2. Routes with the iOTC attribute set MUST NOT be announced by a sender whose Role is Customer or Peer;

3. A sender MUST NOT include this attribute in UPDATE messages if its Role is Customer, Provider or Peer. If it is contained in an UPDATE message from eBGP speaker and receiver's Role is Customer, Provider, Peer or unspecified, then this attribute MUST be removed.

These three rules provide mechanism that strongly prevents route leak creation by an AS.

8. Attribute or Community

Having the relationship hard set by agreement between the two peers in BGP OPEN is critical; the routers enforce the relationship irrespective of operator configuration errors.

Similarly, it is critical that the application of that relationship on prefix propagation using iOTC is enforced by the router(s), and minimally exposed to user misconfiguration. There is a question whether the iOTC marking should be an attribute or a well-known community.

There is a long and sordid history of mis-configurations inserting incorrect communities, deleting communities, ignoring well-known community markings etc. In this mechanism's case, an operator could, for example, accidentally strip the well-known community on receipt.

As opposed to communities, BGP attributes may not be generally modified or filtered by the operator. The router(s) enforce them. This is the desired property for the iOTC marking. Hence, this document specifies iOTC as an attribute.

9. Compatibility with BGPsec

As the iOTC field is non-transitive, it is not seen by or signed by BGPsec [I-D.ietf-sidr-bgpsec-protocol].

10. Additional Considerations

As the BGP Role reflects the relationship between neighbors, it can also have other uses. As an example, BGP Role might affect route priority, or be used to distinguish borders of a network if a network consists of multiple AS.

Though such uses may be worthwhile, they are not the goal of this document. Note that such uses would require local policy control.

As BGP role configuration results in automatic creation of inbound/ outbound filters, existence of roles should be treated as existence of Import and Export policy. [I-D.ietf-grow-bgp-reject]

This document doesn't provide any security measures to check correctness of iOTC usage if role isn't configured.

11. IANA Considerations

This document defines a new Capability Codes option [to be removed upon publication: http://www.iana.org/assignments/capability-codes/capability-codes.xhtml] [RFC5492], named "BGP Role", assigned value <TBD1> . The length of this capability is 1.

The BGP Role capability includes a Value field, for which IANA is requested to create and maintain a new sub-registry called "BGP Role Value". Assignments consist of Value and corresponding Role name. Initially this registry is to be populated with the data in Table 1. Future assignments may be made by a standard action procedure [RFC5226].

This document defines new subcode, "Role Mismatch", assigned value <TBD2> in the OPEN Message Error subcodes registry [to be removed upon publication: http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml#bgp-parameters-6] [RFC4271].

This document defines a new optional, non-transitive BGP Path Attributes option, named "Internal Only To Customer", assigned value <TBD3> [To be removed upon publication: http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml#bgp-parameters-2] [RFC4271]. The length of this attribute is 0.

12. Security Considerations

This document proposes a mechanism for prevention of route leaks that are the result of BGP policy misconfiguration.

Deliberate sending of a known conflicting BGP Role could be used to sabotage a BGP connection. This is easily detectable.

BGP Role is disclosed only to an immediate BGP neighbor, so it will not itself reveal any sensitive information to third parties.

13. Acknowledgments

The authors wish to thank Douglas Montgomery, Brian Dickson, Andrei Robachevsky and Daniel Ginsburg for their contributions to a variant of this work.

14. References

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

[RFC4486] Chen, E. and V. Gillet, "Subcodes for BGP Cease Notification Message", RFC 4486, DOI 10.17487/RFC4486, April 2006, <https://www.rfc-editor.org/info/rfc4486>.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009, <https://www.rfc-editor.org/info/rfc5492>.

14.2. Informative References

[I-D.ietf-grow-bgp-reject]
Mauch, J., Snijders, J., and G. Hankins, "Default EBGP Route Propagation Behavior Without Policies", draft-ietf-grow-bgp-reject-08 (work in progress), May 2017.

[I-D.ietf-grow-route-leak-problem-definition]
Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", draft-ietf-grow-route-leak-problem-definition-06 (work in progress), May 2016.

[I-D.ietf-idr-route-leak-detection-mitigation]
Sriram, K., Montgomery, D., Dickson, B., Patel, K., and A. Robachevsky, "Methods for Detection and Mitigation of BGP Route Leaks", draft-ietf-idr-route-leak-detection-mitigation-03 (work in progress), May 2016.

[I-D.ietf-sidr-bgpsec-protocol]
Lepinski, M. and K. Sriram, "BGPsec Protocol Specification", draft-ietf-sidr-bgpsec-protocol-15 (work in progress), March 2016.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

Authors' Addresses

Alexander Azimov
Qrator Labs

Email: aa@qrator.net

Eugene Bogomazov
Qrator Labs

Email: eb@qrator.net

Randy Bush
Internet Initiative Japan

Email: randy@psg.com

Keyur Patel
Arrcus, Inc.

Email: keyur@arrcus.com

Kotikalapudi Sriram
US NIST

Email: ksriram@nist.gov