Global Routing Operations
Internet-Draft
Obsoletes: 7454 (if approved)
Intended status: Best Current Practice
Expires: 16 May 2026

T. Fiebig
MPI-INF
N. Hilliard
INEX

12 November 2025

BGP Operations and Security
draft-ietf-grow-bgpopsecupd-12

Abstract

The Border Gateway Protocol (BGP) is a critical component in the Internet to exchange routing information between network domains. Due to this central nature, it is important to understand the security and reliability requirements that can and should be ensured to prevent accidental or intentional routing disturbances.

Previously, security considerations for BGP have been described in RFC7454 / BCP194. Since the publications of RFC7454, several developments and changes in operational practice took place that warrant an update of these best current practices. This document obsoletes RFC7454, focusing on the overall goals, and providing a less implementation centric set of best practices.

This document describes security requirements and goals when operating BGP for exchanging routing information with other networks, and explicitly does not focus on specific technical implementations and requirements.

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP), specified in [RFC4271], is the protocol used in the Internet to exchange routing information between network domains. BGP does not directly include mechanisms that control whether the routes exchanged conform to the various guidelines defined by the Internet community. Furthermore, the BGP protocol itself, by its design, does not have any direct way to protect itself against threats to confidentiality, integrity, and availability.

This document summarizes security properties and requirements when operating BGP for securing the infrastructure as well as for security considerations regarding the exchanged routing information. The

document explicitly does not focus on specific technical implementations and requirements. Operators are advised to consult documentation and contemporary informational documents concerning methods to ensure that these properties are sufficiently ensured in their network.

1.1. 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.

2. Scope of the Document

The guidelines defined in this document are intended for BGP when used to exchange generic Internet routing information within the Default-Free Zone (DFZ). It specifically does not cover other uses of BGP, e.g., when using BGP for NLRI exchange in a data-center context. This document does not specify how the outlined requirements and properties can be technically realized at a specific point in time. Instead, operators are advised to consult applicable documentation and contemporary informational documents describing implementation specifics (e.g., [I-D.ietf-grow-routing-ops-sec-inform] and [I-D.ietf-grow-routing-ops-terms]).

3. Protection of the BGP Speaker and Session

The BGP speaker, i.e., the node running BGP to exchange routing information, needs to be protected from external attempts to taint integrity or availability of the BGP session and node alike.

3.1. BGP Session Protection

To protect a BGP speaker on the network layer, an operator MUST ensure the following properties using technical or organizational measures:

* Prevent off-path attackers from injecting BGP messages into existing sessions.

* Prevent off-path attackers from interrupting existing sessions.

* Prevent off-path attackers from preventing the establishment of new sessions.

* Prevent remote systems from overwhelming the BGP speaker by sending large volumes of unsolicited packets or BGP messages.

* Ensure that unstable sessions do not threaten the availability of BGP speakers within the network.

Example technologies to accomplish this include GTSM/TTL-security [RFC5082], BGP-MD5 / TCP-AO [RFC5925], limiting traffic to the control plane via Control Plane Policing (CoPP), and setting maximum prefix limits for the number of prefixes a neighbor may send. When implementing prefix limits, operators SHOULD be aware of the operational implications of exceeding prefix limits, i.e., a loss of an established session. Hence, operators SHOULD appropriately weigh this impact within the specific operational circumstances, and ensure appropriate prefix limits to not cause outages under normal operations.

3.2. BGP Speaker Management Interface Protection

In addition to the control plane / exchange of BGP protocol messages, the management plane of BGP speakers must be appropriately secured. Hence, operators MUST ensure that:

* No unauthorized third-parties can obtain access or connect to the management interface of a BGP speaker in a way that allows tainting confidentiality, integrity, or availability.

* External activity towards the management interface does not interfere with the integrity or availability of BGP sessions.

4. NLRI Filtering

The purpose of BGP is exchanging routing information, i.e., NLRI. Importing or exporting incorrect or malicious NLRI is a security risk for networks themselves, but may also form a threat for connected and/or remote networks. As such, operators MUST ensure the following properties when importing or exporting routing information from their neighbors.

4.1. Importing NLRI

When importing NLRI from a neighbor, an operator MUST ensure that all imported NLRI conform to the following properties by implementing technical or organizational measures:

* The AS originating NLRI for a prefix MUST be globally authorized to originate that prefix. Operators MAY deviate from this for default routes (::/0 and 0.0.0.0/0), if they granted the specific

neighbor permission to announce default routes towards them. Operators SHOULD be aware that ingesting a default route can have opaque negative operational impact, if the announcing upstream is not able to cover the more specific forwarding in the appropriate service provider context. These limitations do not materialize when receiving a full BGP view.

* For received NLRI with an AS_PATH = {AS1, AS2, ..., ASn}, where AS1 is the neighbor that sent the UPDATE and ASn is the originator, for each k in 1..n−1, AS(k+1) MUST be authorized to export the NLRI to ASk according to their bilateral routing policy (e.g., providercustomer, peer, or lateral-peer).

* The AS_PATH MUST NOT contain AS numbers reserved for private [RFC6996] or special-use cases, except for those AS numbers explicitly dedicated to a special-use that requires their presence in the global routing table [IANAASNSpec].

* The number of NLRI received from a neighbor MUST NOT exceed the resources of the local router.

4.2. Originating and Redistributing NLRI

When originating NLRI or redistributing NLRI received from a neighbor, an operator MUST ensure that all NLRI they export conform to the following properties by implementing technical or organizational measures:

* The redistributing AS MUST be authorized to redistribute NLRI for the specific prefix when received from the AS directly to its right in the AS_PATH. Additionally, each AS in the AS_PATH not originating the prefix MUST be authorized to redistribute the prefix when receiving it from the next AS to its right.

* The AS originating NLRI for a prefix MUST be globally authorized to originate that prefix. Operators MAY deviate from this for default routes (::/0 and 0.0.0.0/0), if they originate the default route and the specific neighbor granted them permission to announce default routes towards them. Operators SHOULD be aware that originating a default route without being able to cover the more specific forwarding in the appropriate service provider context can have opaque negative operational impact for a downstream, while sharing a full BGP view with a downstream does not carry this risk.

* The AS_PATH MUST NOT contain AS numbers reserved for private [RFC6996] or special-use cases, except for those AS numbers explicitly dedicated to a special-use that requires their presence in the global routing table [IANAASNSpec].

4.3. Altering Attributes in Received BGP Updates

When processing received BGP updates, an operator SHOULD ensure that attributes which are considered immutable are not altered:

* An operator SHOULD NOT change or remove immutable transitive BGP attributes, e.g., ORIGIN as per [RFC4271]. Furthermore, incremental deployment of new features and technologies relies on the unaltered redistribution of unknown attributes by implementations not yet supporting this feature. Hence, as gratuitously filtering such attributes would harm incremental deployment, filtering unknown attributes SHOULD be avoided by transit providers.

* Please note that occasionally unknown or malformed attributes may cause operational problems, e.g., due to implementation bugs. Hence, in selected cases, if a specific attribute is known to be malicious or disruptive, an operator MAY either temporarily remove that specific attribute from received BGP updates when importing them or filter the BGP update carrying the attribute.

* BGP updates MUST NOT be enriched with transitive attributes subject to change independent of the underlying NLRI, e.g., encoding RPKI validation state in transitive attributes [I-D.ietf-sidrops-avoid-rpki-state-in-bgp].

5. IANA Considerations

This document does not require any IANA actions.

6. Security Considerations

This document is entirely about BGP operational security. It lists requirements and properties operators MUST ensure using technical or organizational measures when operating BGP routers in the DFZ.

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, <https://www.rfc-editor.org/info/rfc2119>.

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

[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>.

[RFC6996] Mitchell, J., "Autonomous System (AS) Reservation for Private Use", BCP 6, RFC 6996, DOI 10.17487/RFC6996, July 2013, <https://www.rfc-editor.org/info/rfc6996>.

[IANAASNSpec] IANA, "Special-Purpose Autonomous System (AS) Numbers", <https://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml>.

7.2. Informative References

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <https://www.rfc-editor.org/info/rfc5082>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <https://www.rfc-editor.org/info/rfc7454>.

[I-D.ietf-grow-routing-ops-sec-inform] Fiebig, T., "Current Options for Securing Global Routing", Work in Progress, Internet-Draft, draft-ietf-grow-routing-ops-sec-inform, 9 April 2025, <https://datatracker.ietf.org/doc/draft-ietf-grow-routing-ops-sec-inform/>.

[I-D.ietf-grow-routing-ops-terms] Fiebig, T., "Currently Used Terminology in Global Routing Operations", Work in Progress, Internet-Draft, draft-ietf-

grow-routing-ops-terms, 9 April 2025,
<https://datatracker.ietf.org/doc/draft-ietf-grow-routing-ops-terms/>.

[I-D.ietf-sidrops-avoid-rpki-state-in-bgp]
Snijders, J., Fiebig, T., and M. A. Stucchi, "Guidance to Avoid Carrying RPKI Validation States in Transitive BGP Path Attributes", Work in Progress, Internet-Draft, draft-ietf-sidrops-avoid-rpki-state-in-bgp, 3 October 2024,
<https://datatracker.ietf.org/doc/draft-ietf-sidrops-avoid-rpki-state-in-bgp/>.

Acknowledgements

This document has been originally based on [RFC7454] and we thank the original authors for their work.

We thank the following people for reviewing this draft and suggesting changes:

* Gert Doerring
* Jeff Haas
* Geng Nan
* Martin Pels
* Job Snijders
* Berislav Todorovic
* Linda Dunbar
* Wolfgang Tremmel
* Florian Obser
* Ben Maddison
* Mohamed Boucadair

Authors' Addresses

Tobias Fiebig
Max-Planck-Institut fuer Informatik
Campus E14
66123 Saarbruecken
Germany
Phone: +49 681 9325 3527
Email: tfiebig@mpi-inf.mpg.de

Nick Hilliard
Internet Neutral Exchange Association
4027 Kingswood Road
Citywest, Dublin
D24 AX96
Ireland
Phone: +353 1 433 205 2
Email: nick@inex.ie