Secure Inter-Domain Routing
Internet-Draft
Intended status: Informational
Expires: 10 December 2025

K. Xu
X. Wang
Z. Liu
Q. Li
Tsinghua University
Y. Guo
Zhongguancun Laboratory

8 June 2025

Transition to Full BGPsec Deployment: Transitive-BGPsec is Incompatible with BGPsec
draft-wang-sidrops-bgpsec-transition-00

Abstract

This document elaborates on the reasons why it is unfeasible to reconstruct the native-BGPsec as a transitive approach, such that a BGP update with a correctly signed BGPsec_PATH attribute can traverse legacy areas and afterwards it can still be properly processed by subsequent native-BGPsec speakers.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://FCBGP.github.io/BGPsec-Transition/draft-wang-sidrops-bgpsec-transition.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-wang-sidrops-bgpsec-transition/.

Source for this draft and an issue tracker can be found at https://github.com/FCBGP/BGPsec-Transition.

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 https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) [RFC4271] is vulnerable to route leaks and hijacking attacks.

Native BGPsec, as defined in [RFC8205], extends BGP to enhance the security of AS path information. Nevertheless, native BGPsec encounters challenges in achieving incremental deployment. It utilizes an optional non-transitive BGP path attribute to deliver digital signatures. Yet, when BGPsec messages traverse BGPsec-

unemployed, the last BGPsec-aware router falls back to native BGP protocol to ensure backward compatibility, by completely removing the BGPsec-related path attribute (i.e., the BGPsec_PATH attribute).

The principal objectives are to make BGPsec transit transparently over BGPsec-unemployed areas, instead of completely falling back to legacy BGP.

In order to transit across areas where BGPsec has not been deployed, the most straightforward approach is to transform the native BGPsec into transitive BGPsec. However, this document will illustrate that it is unfeasible to render BGPsec as a transitive approach for traversing undeployed areas while still being compatible with native BGPsec. In other words, transitive BGPsec is not compatible with BGPsec.

1.1. Conventions and Definitions

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.

BGP: BGP, native BGP, and/or legacy BGP are the BGP version 4 defined in [RFC4271] and/or multiprotocol BGP defined in [RFC4760]. It does not support BGPsec or native BGPsec.

BGPsec: BGPsec, native BGPsec, and/or traditional BGPsec are the BGPsec approach defined in [RFC8205].

T-BGPsec: T-BGPsec or transitive BGPsec means that the transitive BGPsec approach is defined in this document.

2. Transitive BGPsec Modifications

Transitive BGPsec, in essence, describes that the BGPsec_PATh must be transitive and compliant with native BGPsec.

2.1. Transitive BGPsec Negotiation

As stated in Section 2.2 of [RFC8205], for a BGPsec router to successfully negotiate with its peer, it must transmit the BGPsec Capabilities that are in accordance with those of its peers in the BGP OPEN message. A transitive path attribute, instead, does not require the negotiation of capabilities with peers. In the event that a peer fails to comprehend the transitive path attribute, it simply forwards it to downstream BGP speakers.

In transitive BGPsec, negotiating the BGPsec capability is not required. However, a BGPsec router is obligated to inform its peer that it supports transitive BGPsec. In this case, the reuse of the BGPsec capability is essential. Nevertheless, there is no requirement to utilize the Dir field and the AFI field. Transitive BGPsec reuses the native BGPsec capability format. Consequently, the version field of the BGPsec capability must be updated to 1, while the remaining fields should be filled with 0.

If a BGPsec router negotiates with its peers and the version value of the BGPsec capability is set to 1, this implies that the router supports transitive BGPsec. In this scenario, the BGPsec capability serves two purposes. Firstly, it notifies the peer that this particular BGP speaker is capable of supporting transitive BGPsec. Secondly, it differentiates transitive BGPsec from native BGPsec.

For the sake of compatibility, this document designates that it still supports native BGPsec in this version.

2.2. The Transitive BGPsec_PATH Attribute

Given that the objective is to expedite the incremental deployment of BGPsec, this document considers the least possible modifications to BGPsec. Consequently, all of the packet formats of the BGPsec_PATH attribute defined in [RFC8205] are reutilized in the establishment of transitive BGPsec, including the BGPsec_PATH attribute format, Secure_Path format, Secure_Path Segment format, Signature_Block format, and Signature_Block Segment format.

In native BGPsec, the BGPsec_PATH attribute is an optional non-transitive BGP path attribute. However, within this document, the BGPsec_PATH attribute is defined as an optional transitive BGP path attribute. It is important to note that the attribute code should remain the same as that of the native BGPsec_PATH attribute.

2.3. Updating and Receiving BGP UPDATE message

TBD.

3. Question: Compatibility with Native BGPsec

Taking the topology presented in Figure 1 as an example:

* AS A, AS B, and AS C are regions with continuous native BGPsec deployments. Specifically, AS A, AS B, and AS C implement native BGPsec. Additionally, AS C also implements transitive BGPsec.

* AS D and AS E are areas with legacy BGP deployments. These areas do not implement native BGPsec, transitive BGPsec, or any other related security mechanisms.

* AS F deploys native BGPsec.

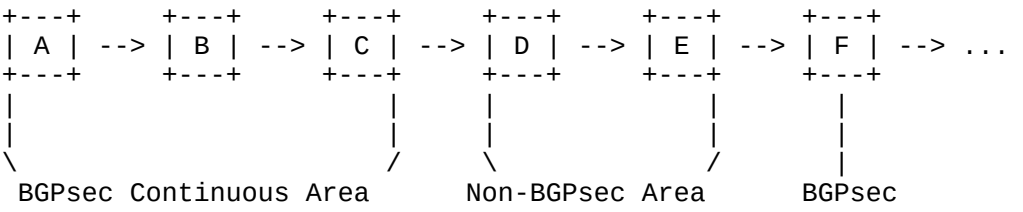

Figure 1: Example: Mix Deployment Scenario

AS A is capable of negotiating the BGPsec Capability with AS B. AS A disseminates a route prefix through a BGPsec UPDATE message to AS B.

AS B can negotiate the BGPsec Capability independently with both AS A and AS C. It receives the BGPsec UPDATE message from AS A and validates it in accordance with the BGPsec specification. Subsequently, it modifies the BGPsec UPDATE message by incorporating its own information and forwards it to AS C.

AS C obtains the BGPsec UPDATE message from AS B. AS C validates the BGPsec UPDATE message and makes the necessary modifications. In this scenario, because AS D is a legacy AS, AS C converts this message into a transitive BGPsec UPDATE message.

AS D and AS E refrain from processing this transitive BGPsec message and instead forward it to the subsequent hop.

AS F receives this transitive BGPsec UPDATE message from AS E. Because AS F deploys the native BGPsec, it will conduct a syntax check. However, the verification will fail because the message is not correctly formatted as a BGPsec UPDATE message.

In summary, any native BGPsec speaker on the downstream of an undeployed region cannot properly process the transitive BGPsec UPDATE messages sent by upstream ASes.

Thus, we conclude that the transitive BGPsec is not a viable option to make BGPsec incrementally deployable.

A new intermediate protocol is required in the transition to full BGPsec deployment.

4. Security Considerations

There are no security considerations in this document.

5. IANA Considerations

This document has no 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, <https://www.rfc-editor.org/rfc/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/rfc/rfc4271>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <https://www.rfc-editor.org/rfc/rfc4760>.

[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/rfc/rfc8174>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/rfc/rfc8205>.

[RFC9774] Kumari, W., Sriram, K., Hannachi, L., and J. Haas, "Deprecation of AS_SET and AS_CONFED_SET in BGP", RFC 9774, DOI 10.17487/RFC9774, May 2025, <https://www.rfc-editor.org/rfc/rfc9774>.

6.2. Informative References

[RFC8374] Sriram, K., Ed., "BGPsec Design Choices and Summary of Supporting Discussions", RFC 8374, DOI 10.17487/RFC8374, April 2018, <https://www.rfc-editor.org/rfc/rfc8374>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Ke Xu
Tsinghua University
Email: xuke@tsinghua.edu.cn

Xiaoliang Wang
Tsinghua University
Email: wangxiaoliang0623@foxmail.com

Zhuotao Liu
Tsinghua University
Email: zhuotaoliu@tsinghua.edu.cn

Qi Li
Tsinghua University
Email: qli01@tsinghua.edu.cn

Yangfei Guo
Zhongguancun Laboratory
Email: guoyangfei@zgclab.edu.cn