SIDR Operations Working Group
Internet-Draft
Intended status: Standards Track
Expires: 22 January 2026

J. Zhang
Zhongguancun Laboratory
Y. Wang
Tsinghua University
M. Matejka
CZ.NIC
M. Xu
Tsinghua University

21 July 2025

ASPA-based AS_PATH Verification for BGP Export
draft-zhang-sidrops-aspa-egress-03

Abstract

This document describes that a BGP speaker may perform AS_PATH verification on the routes it sends to BGP neighbors at external BGP (eBGP) egress based on Autonomous System Provider Authorization (ASPA) objects in the Resource Public Key Infrastructure (RPKI). Before BGP speakers advertise routes to external peers at eBGP egress, performing ASPA-based AS_PATH verification can prevent route leaks to external peers, check for local misconfigurations and detect ASPA registration errors, thus avoiding the advertisement of invalid routes.

Table of Contents

1. Introduction

Autonomous System Provider Authorization (ASPA) objects in the RPKI can be used to verify BGP AS_PATH for detection and mitigation of route leaks and certain prefix hijacks involving forged origins or forged path-segments with some improbable AS paths. The ASPA object profile is defined in [I-D.ietf-sidrops-aspa-profile].

In the procedures of ASPA-based BGP AS_PATH verification defined in [I-D.ietf-sidrops-aspa-verification], ingress external BGP (eBGP) router of an AS receives routes from its BGP peers, and perform ASPA-based BGP AS_PATH verification and mitigation at eBGP ingress, as recomendations specified in Section 8.1 in [I-D.ietf-sidrops-aspa-verification]. BGP AS_PATH verification at eBGP ingress can detect and prevent the route leaks in the routes received from BGP neighbors. However, considering that route leaks may occur within the local AS and that the local AS may modify the AS_PATH, it lacks the ability to prevent the BGP speaker from advertising invalid routes to its external peers at eBGP egress.

This document describes ASPA-based BGP AS_PATH verification at eBGP egress. It does not change the semantics or procedures of ASPA-based BGP AS_PATH verification defined in [I-D.ietf-sidrops-aspa-verification]. It explains important use cases and specifics of correct implementation of ASPA-based path verification in eBGP egress policies, as [RFC8893] did with RPKI origin validation for BGP export. The verification procedure at eBGP egress is a little bit different from the process at the eBGP ingress. By AS_PATH verification before sending routes to BGP neighbors at eBGP egress, a BGP speaker can detect ASPA registration errors and local misconfiguration, and prevent the improper propagation of route leaks.

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. Suggested Reading

It is assumed that the reader understands BGP[RFC4271], RPKI[RFC6480], ASPA object profile[I-D.ietf-sidrops-aspa-profile], ASPA-based BGP AS_PATH verification[I-D.ietf-sidrops-aspa-verification], and RPKI-ROV for BGP export[RFC8893].

3. Procedure of ASPA-based AS_PATH Verification at eBGP Egress

When a BGP speaker advertises a route to an external peer through eBGP egress, the BGP speaker prepends its own AS number to the AS_PATH of the route, and performs ASPA-based AS_PATH verification before sending the route to the external peer.

Suppose the BGP speaker is at AS X, and its external peer is at AS Y, and the AS_PATH P of the route to be advertised to external peer by the BGP speaker is represented by {AS X, AS(N), ..., AS(2), AS(1)}, where AS(1) is the origin AS, and AS X is the local AS number added by the BGP speaker of AS X at eBGP egress.

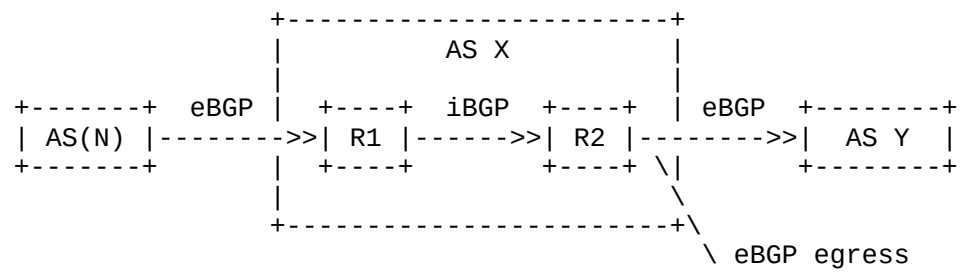

Figure 1: Illustration of the eBGP egress.

The method of ASPA-based AS_PATH verification at the eBGP egress of the BGP speaker is described as follows:

1. Regard the external neighbor AS Y as the virtual receiving/ validating AS point.

2. The BGP roles of AS X and AS Y, including Customer, Provider, Route Server (RS), Route Server Client (RS-client) and Peer, are defined in [RFC9234], and they can be configured locally and used for the path verification.

3. If AS X is the Customer or Peer to AS Y, or AS Y is a (transparent or non-transparent) Route Server (RS) and AS X is a RS-client, or, AS Y is a RS-client and AS X is a (transparent or non-transparent) RS, use the upstream path verification algorithm (described in [I-D.ietf-sidrops-aspa-verification]) to verify the AS_PATH P.

4. If AS X is the Provider to AS Y, use the downstream path verification algorithm (described in [I-D.ietf-sidrops-aspa-verification]) to verify the AS_PATH P.

4. Necessity and Benificial Cases

By performing AS_PATH verification before sending routes to BGP neighbors at the eBGP egress, a BGP speaker can avoid local misconfigurations, prevent local route leaks, and detect ASPA registration errors.

4.1. Prevent Local Misconfigurations

Egress AS_PATH verification will prevent misconfigurations of the egress router. If the local AS has multiple AS numbers, it is necessary to ensure that the AS number added to the AS_PATH at the egress is correct and whether it could lead to neighbors validating it as invalid. Additionally, the local AS needs to check if any modifications to the AS_PATH in export policy are legitimate. Verification at the egress will prevent the local AS from advertising routes with invalid AS_PATHs, allowing for quick detection of issues and correction of local configuration errors.

4.2. Complete ASPA-based Verification Method

The current ASPA-based AS_PATH verification is not a complete solution. Performing AS_PATH verification at the ingress can detect route leaks in the routes received from BGP neighbors, but it cannot prevent local route leaks. Egress AS_PATH verification can detect local route leaks, further completing the overall ASPA-based AS_PATH verification solution.

Even though OTC, defined in [RFC9234], can address local route leaks when used properly, it is tightly coupled with BGP, which increases the likelihood of configuration errors. In contrast, ASPA provides an out-of-band verification solution that decouples from BGP protocol configuration, making the chances of simultaneous configuration errors much lower. Additionally, ASPA has advantages in both security and operability. OTC lacks built-in tamper-proof mechanisms and integrity verification, leaving it vulnerable to malicious attackers or misconfigurations. ASPA achieves secure verification through the distribution of resource certificates and authentication. In terms of operational complexity, OTC requires BGP role configuration per router per session, increasing configuration complexity. Furthermore, to implement OTC as specified in [RFC9234], both the local AS and remote peers need router updates, while ASPA only requires that neighbors have records in ASPA for local verification.

4.3. Detect ASPA Registration Errors

If the local AS or customers have registration errors or omissions, they can be detected at the egress, allowing for quick identification of the issue. This mainly includes the following two scenarios:

(1) Case of local AS: if the local AS has omitted one or more providers in ASPA provider list, the local AS may end up advertising routes with ASPA-invalid AS_PATH to its customers.

(2) Case of Customer: if the Customer of local AS forgets to include the local AS in their ASPA provider list, the local AS may end up advertising their routes with ASPA-invalid AS_PATH to its neighbors.

Performing AS_PATH verification at the egress could detect such registration errors immediately and point to its actual source clearly and noticeably; otherwise, routes advertised by the local AS may be filtered by other ASes, leaving the local AS unaware of the issue.

5. Operational Considerations

The peering relationships between the local AS and its external neighbor ASes, including Customer-Provider/Provider-Customer, Peer-Peer, Route Server (RS) and RS-client, mutual-transit, are used in path verification procedures to determine whether upstream or downstream procedures should be applied. There are the following possible ways to know the relations between the local AS and its external neighbor AS: (1) The first way is to use the BGP Role Capabilities exchanged in the BGP OPEN message as specified in [RFC9234]. (2) The second way is to use ASPA objects registered by the local AS and its external neighbor AS. (3) Another possible way is to use local configuration. When the relation of two neighboring ASes is mutual-transit, they are Customers of each other in BGP roles. It can be confirmed by BGP roles advertised in the BGP OPEN message, or configuration in local file. If a mutual-transit relation is identified as Cutomer-Provider, a false positive of route leak may be generated in path verification.

6. Security Considerations

The security considerations that apply to ASPA-based AS_PATH verification (see [I-D.ietf-sidrops-aspa-verification]) also apply to the procedure described in this document.

7. IANA Considerations

This document has no IANA actions

8. References

8.1. 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>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[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>.

[RFC8893] Bush, R., Volk, R., and J. Heitz, "Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export", RFC 8893, DOI 10.17487/RFC8893, September 2020, <https://www.rfc-editor.org/info/rfc8893>.

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <https://www.rfc-editor.org/info/rfc9234>.

8.2. Informative References

[I-D.ietf-sidrops-aspa-profile] Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-19, 6 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-19>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-22, 23 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-22>.

Acknowledgements

The authors thank Nan Geng, Sriram Kotikalapudi and Randy Bush for their valuable suggestions and comments.

Authors' Addresses

Jia Zhang
Zhongguancun Laboratory
Beijing
China
Email: zhangj@mail.zgclab.edu.cn

Yangyang Wang
Tsinghua University
Beijing
China
Email: wangyy@cernet.edu.cn

Maria Matejka
CZ.NIC
Czechia
Email: maria.matejka@nic.cz

Mingwei Xu
Tsinghua University
Beijing
China
Email: xmw@cernet.edu.cn