Workgroup: SIDR Operations Working Group
Internet-Draft: draft-zhang-sidrops-aspa-egress-04
Published: 20 January 2025
Intended Status: Standards Track
Expires: 24 July 2025
Authors:
J. Zhang, *Zhongguancun Laboratory*
Y. Wang, *Tsinghua University*
M. Matejka, *CZ.NIC*
M. Xu, *Tsinghua University*

ASPA-based AS_PATH Verification for BGP Export

Abstract

This document describes AS_PATH verification based on Autonomous System Provider Authorization (ASPA) for egress eBGP speakers. ASPA is a Resource Public Key Infrastructure (RPKI) object that allows an AS to register its transit provider ASes. Performing ASPA-based AS_PATH verification at egress can prevent the propagation of route leaks to external peers, check for local misconfigurations, and help detect potential ASPA registration errors. This approach complements ingress-side verification; it ensures coverage should ASPA deployment be absent at the ingress eBGP router of the AS.

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/.

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 24 July 2025.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
2. Suggested Reading 3
3. Procedure of ASPA-based AS_PATH Verification at eBGP Egress 3
3.1. Utility of Only to Customer (OTC) Attribute 4
3.2. Consideration of Complex BGP Sessions 5
4. Optimizations 5
5. Necessity and Beneficial Cases 5
5.1. Prevent Local Misconfigurations 6
5.2. Complementing the ASPA-based Ingress Verification Method 6
5.3. Detect ASPA Registration Errors 6
6. Operational Considerations 6
7. Security Considerations 7
8. IANA Considerations 7
9. References 7
9.1. Normative References 7
Acknowledgements 8
Authors' Addresses 8

1. Introduction

Autonomous System Provider Authorization (ASPA) objects in the Resource Public Key Infrastructure (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 [I-D.ietf-sidrops-aspa-verification]. The ASPA object profile is defined in [I-D.ietf-sidrops-aspa-profile].

The procedures described in Section 5 of [I-D.ietf-sidrops-aspa-verification] perform ASPA-based BGP AS_PATH verification at eBGP ingress. Performing BGP AS_PATH verification at eBGP egress (this document) can be beneficial as follows: (1) Ensure coverage should ASPA deployment be absent at the ingress eBGP router of the AS, and (2) Check whether the AS_PATH (with the local AS added) as received by the eBGP neighbor at egress router would be Invalid and, if so, avoid sending the BGP Update. The egress AS_PATH verification inherently detects and alerts the local AS operator if there were any eBGP peering misconfiguration or error in the ASPA registration of the eBGP neighbor on the ingress side.

This document 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 at eBGP egress, as [RFC8893] did with RPKI route origin validation (RPKI-ROV) for BGP export. The verification procedure at eBGP egress is a little different from the procedure at the eBGP ingress.

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 router 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 (see Figure 1). In this AS_PATH, the AS number (ASN) used for AS X MUST be the ASN of the router's BGP configuration (see [RFC8481] [RFC8893]).

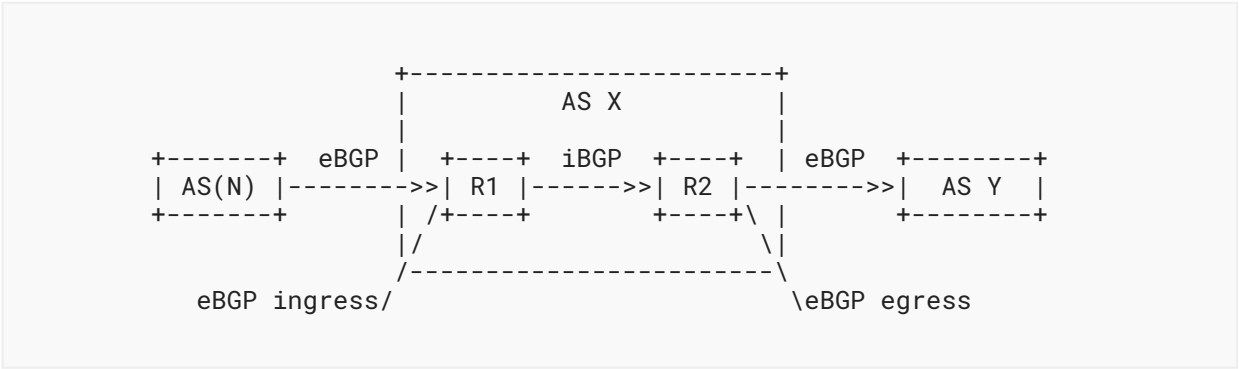

Figure 1: Illustration of the eBGP egress.

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 a Customer or Peer to AS Y, or AS Y is a (transparent or non-transparent) Route Server (RS) and AS X is an RS-client, or, AS Y is an RS-client and AS X is a (transparent or non-transparent) RS, use the algorithm for upstream paths (Sec. 5.4 of [I-D.ietf-sidrops-aspa-verification]) to verify the AS_PATH P.
4. If AS X is a Provider to AS Y, use the algorithm for downstream paths (Sec. 5.5 of [I-D.ietf-sidrops-aspa-verification]) to verify the AS_PATH P.

3.1. Utility of Only to Customer (OTC) Attribute

The egress verification procedure described above can produce incorrect results at R2 in some cases (see Figure 1). This is because at R1 there is direct knowledge (based on local configuration) of AS X's peering relation with the neighbor AS(N) while at R2 the procedure must rely on the ASPA data. But the ASPA data may be absent or insufficient. For example, let the AS(N) to AS X relationship be complex consisting of a C2P session and a p2p session. AS(N) has an ASPA that attests that AS X is a provider (per ASPA specification). Let the AS X to AS Y relationship be C2P or p2p. Then for a route originated by AS(N) and sent to AS X on the p2p session, the egress verification at R2 produces a Valid outcome. Only R1 knows that the route made ingress on a p2p session; R2 does not. In order that R2 does not forward the route to AS Y, it cannot rely on the outcome of the egress verification in this example. It is imperative that R1 attaches the Only to Customer (OTC) Attribute [RFC9234] to the route on ingress. Even if the ingress router R1 is not upgraded to perform ASPA verification (partial deployment of ASPA within an AS), it must be upgraded to do OTC (or minimally an intra-AS BGP Community that emulates the OTC Attribute for route leak prevention).

3.2. Consideration of Complex BGP Sessions

There can be a complex peering relationship on either side of AS X (with AS(N) or with AS Y).

If multiple eBGP sessions can segregate the Complex peering relationship into eBGP sessions with normal peering relationships the receiving/verifying AS SHOULD select the appropriate algorithm (for upstream or downstream paths per Sec. 5.4 or Sec. 5.5, respectively, in [I-D.ietf-sidrops-aspa-verification]) for each of the normal sessions based on its peering relation type.

If a Complex peering relation cannot be segregated (i.e., when a Complex BGP relationship occurs within one single BGP session), an operator may want to achieve an equivalent outcome by applying an appropriate algorithm (for upstream or downstream paths) on a per-prefix basis corresponding to the peering relation for the prefix. If this option is not feasible, then an operator MAY apply the algorithm for downstream paths to avoid false positive outcomes.

4. Optimizations

There would be concerns about the extra workload or redundancy of processing due to performing verification at both ingress and egress. There should be some optimizations implemented or available for use when appropriate so that redundant processing can be minimized. Examples of optimizations are:

1. Consider the full table is received from a provider at an un-upgraded ingress border router and the full tables are advertised to multiple customer ASes. Process egress ASPA verification centrally for all customer AS facing interfaces if possible and then push the verified full table to RIBs-out of all such interfaces. Significant egress ASPA processing savings can result by doing this.
2. Network operators should have a switch that they can use to turn off egress ASPA verification when it is appropriate. For example, when the adoption of ingress ASPA verification + OTC (or an intra-AS BGP community like OTC) is complete on all their border routers.
3. For routes that have OTC (or an intra-AS BGP community like OTC) attached when received from iBGP at an egress router, then the egress ASPA verification must not be performed on them if the egress router is connected only to provider ASes and/or lateral peer ASes.

5. Necessity and Beneficial Cases

Performing ASPA-based egress AS_PATH verification allows an eBGP router, in some cases, to prevent local route leaks and to help diagnose local peering misconfigurations and ASPA registration errors. The cases where these benefits may not materialize are: (1) eBGP peering relations are complex, or (2) the eBGP neighbor on the ingress side has no ASPA registration, or (3) the local AS is in an AS migration state. In the first and second cases, the egress ASPA algorithm (Section 3) could produce a false negative result but never a false positive and hence

the behavior would be conservative (i.e., a valid route is not dropped). When there is AS migration, it is necessary that the local AS has conveyed to its customer ASes all the relevant AS numbers (temporary as well as the global AS ID) for correct ASPA registrations.

5.1. 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.

5.2. Complementing the ASPA-based Ingress Verification Method

Performing AS_PATH verification at the ingress can detect route leaks in the routes received from eBGP neighbors, but additional measures are needed to prevent local route leaks. As discussed in Section 3.1), the OTC Attribute helps prevent local routes leaks . Egress ASPA verification can also detect some (but not all) local route leaks.

5.3. 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 the Set of Provider ASes (SPAS) in its ASPA, the local AS may end up advertising routes with ASPA-invalid AS_PATH to its customers.

(2) Case of Customer AS: If a Customer of the local AS forgets to include the local AS in their SPAS, 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.

6. 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 way is to use the local BGP peering configuration.

7. 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.

8. IANA Considerations

This document has no IANA actions

9. References

9.1. 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>.

[RFC8481] Bush, R., "Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)", RFC 8481, DOI 10.17487/RFC8481, September 2018, <https://www.rfc-editor.org/info/rfc8481>.

[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>.

[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-20, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20>.

[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-24, 19 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-24>.

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