Inter-Domain Routing
Internet-Draft
Intended status: Informational
Expires: 16 August 2026

Y. Guo
Zhongguancun Laboratory
K. Xu
Tsinghua University
X. Wang
Capital Normal University

12 February 2026

Using BGP Community for Inter-AS Security Policy Signaling
draft-guo-idr-bgp-security-policy-community-00

Abstract

This document specifies a set of standardized BGP communities to signal inter-AS routing security policy intent. Current mechanisms such as ROA [RFC6482] [RFC9582] and ASPA [ASPA-Profile] [ASPA-Verification] provide validation outcomes, but leave "NotFound" or "Unknown" states operationally ambiguous.

This document defines transitive communities that allow an Origin AS to explicitly express its security policy expectations, such as a preference for strict handling of ROA or ASPA validation ambiguity, to downstream Autonomous Systems (AS). Unlike validation states, these communities do not assert correctness or authorization. Instead, they communicate origin-declared policy intent to all downstream ASes, enabling them to correlate this intent with locally derived validation results. By enabling explicit signaling of security expectations without exporting validation state, this mechanism allows downstream ASes to make more informed policy decisions while reducing the risk of accidental outages caused by misinterpretation of ambiguous validation outcomes.

This mechanism is orthogonal to existing routing security validation technologies and does not alter their semantics or deployment models.

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/bgp-security-community/draft-guo-idr-bgp-security-community.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-guo-idr-bgp-security-policy-community/.

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

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 3
2. Conventions and Definitions 4
3. Policy Signaling and Transitivity 5
   3.1. Transitive Property Requirement 5
   3.2. Policy Signaling Versus Validation State 5
4. Protocol Operations 6
   4.1. Architecture Overview 6
   4.2. Origin AS Behavior 6
   4.3. Intermediate AS Behavior 7
   4.4. Applicability to Route Leak and Hijack Detection 7
   4.5. Deployment Considerations 7
5. Security Considerations 8
   5.1. Authenticity and Integrity 8
   5.2. Relationship to Validation Mechanisms 9
   5.3. Policy Semantics and Downstream Behavior 9

5.4. Denial-of-Service and Abuse Considerations 9
5.5. Threat Model Summary 10
6. IANA Considerations 10
6.1. Large Community Mapping 10
6.2. Standard Community Mapping 10
7. References 11
7.1. Normative References 11
7.2. Informative References 11
Appendix A. Parameter Field Extensibility 13
Appendix B. Relationship to Existing Mechanisms 13
B.1. Relationship to RPKI, ROA, and ASPA 13
B.2. Relationship to BGPsec 14
B.3. Relationship to BGP Color and Color-Aware Routing 14
B.4. Relationship to Only-To-Customer (OTC) 14
B.5. Summary of Scope Separation 15
Acknowledgments 15
Authors' Addresses 15

1. Introduction

Inter-domain routing security mechanisms intentionally separate validation from policy. While this separation improves robustness, it also creates persistent operational ambiguity.

Internet routing security relies on distributed validation mechanisms like RPKI [RFC6480], ROA [RFC6482] [RFC9582], and ASPA [ASPA-Profile] [ASPA-Verification]. However, there is a functional gap between "knowing a route's validity" and "knowing the origin's policy intent."

These security mechanisms are often locally enforced only. No consistent method exists for an AS to signal its security requirements or expectations for propagated prefixes. [AVOID-RPKI-STATE-IN-BGP] advises against carrying actual RPKI-derived validation state in BGP, in particular using transitive attributes such as BGP Communities. This is an important safeguard, but it leaves downstream ASes with ambiguity. For example, when a Transit AS observes an RPKI "NotFound" state, it cannot distinguish between an Origin AS that has not deployed RPKI and an Origin AS that has deployed RPKI but suffered a configuration error or a hijack attempt. These mechanisms do not allow an Origin AS to express:

* whether it expects strict handling to be applied to ambiguous validation outcomes;

* whether certain propagation behaviors are explicitly expected or operationally acceptable;

* and whether "NotFound" or "Unknown" outcomes are operationally acceptable.

As a result, downstream networks frequently face situations where routing information is technically acceptable, yet operationally unexpected. In large-scale deployments, this ambiguity leads to:

* inconsistent treatment of identical prefixes;

* reliance on bilateral or undocumented conventions;

* and difficulty distinguishing misconfiguration from malicious behavior.

Existing uses of BGP communities partially address this gap, but lack standardized semantics and a clear separation from validation state.

By signaling security policy intent, an Origin AS can explicitly inform the network of its operational expectations regarding routing security. For example, an Origin AS may indicate that it prefers downstream ASes to apply stricter handling for its prefixes when local validation results are ambiguous.

This signaling enables downstream ASes to distinguish between intentional non-deployment and unexpected validation outcomes, and to apply locally appropriate policy decisions without exporting or redefining validation state. The mechanism defined in this document is explicitly designed to follow the guidance in [AVOID-RPKI-STATE-IN-BGP] by avoiding the carriage of RPKI-derived validation state in BGP.

2. 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.

Strict:
: In this document, the term "Strict" as used in community names (e.g., "ROA-Strict") refers solely to the Origin AS’s stated policy preference regarding the handling of ambiguous validation outcomes. It does not imply any mandated filtering, dropping, or preference change by downstream ASes, and it MUST NOT be interpreted as a remote instruction to suppress routes.

Security Policy Community:

A BGP Community or Large Community defined by this document to convey origin-declared routing security policy intent.

Validation State:
A locally derived outcome of a security validation mechanism, such as RPKI Prefix Origin Validation or ASPA-based path validation (e.g., "Valid", "Invalid", "NotFound", "Unknown"). Validation state is explicitly out of scope for the communities defined in this document.

3. Policy Signaling and Transitivity

3.1. Transitive Property Requirement

All communities defined in this document are specified as transitive, with the intent that the origin-declared policy can be observed by all ASes along the AS-PATH.

Intermediate ASes may apply local policy that removes or modifies communities; such behavior is outside the scope of this specification. This specification does not impose any requirement on intermediate ASes to preserve these communities. Preservation is an operational choice intended to maximize the visibility of origin-declared policy intent.

3.2. Policy Signaling Versus Validation State

This document makes a strict distinction between:

* validation state, which is derived locally from cryptographic or registry-based mechanisms; and

* policy intent, which reflects the Origin AS’s operational expectations.

The communities defined herein exclusively signal policy intent. They do not encode validation outcomes, confidence levels, or security posture of any AS other than the origin.

Downstream ASes MUST NOT interpret these communities as an indication that validation has been successfully performed, nor as a substitute for local validation.

Implementations and Operators MUST NOT configure policies that set, clear, or modify the Security Policy Communities defined in this document based solely on per-route validation outcomes (for example, "if validation is Valid, then attach ROA-Strict"). Doing so would effectively re-export validation state in BGP Communities, contrary to the guidance in [AVOID-RPKI-STATE-IN-BGP].

This design explicitly aligns with the guidance in [AVOID-RPKI-STATE-IN-BGP], and avoids propagating dynamic security state within BGP.

4. Protocol Operations

4.1. Architecture Overview

The mechanism defined in this document operates entirely within the BGP control plane and does not alter protocol message formats or path selection procedures.

An Origin AS attaches one or more Security Policy Communities when originating a route. These communities are propagated unchanged unless explicitly removed or modified by policy.

Intermediate and receiving ASes may choose to:

* ignore the communities;

* log or monitor their presence;

* correlate them with local validation results;

* and incorporate them into local policy decisions.

No mandatory processing behavior is defined, and no interoperability dependency is introduced.

4.2. Origin AS Behavior

An Origin AS that chooses to signal security policy intent SHALL attach the appropriate Security Policy Community when originating a route. It MUST ensure that its published RPKI ROAs and ASPA objects are consistent with the signaled community to avoid self-inflicted DoS.

For example, an AS 65001 that wishes to indicate a strict policy posture with respect to ROA-based validation ambiguity for a given prefix may attach the following Large Community:

* 65001:1000:1 (ROA-Strict, default strict posture)

An Origin AS MUST NOT attach the Security Policy Communities defined in this document as a function of per-route validation outcomes (e.g., "attach ROA-Strict only when a particular route is currently Valid"). Instead, the communities are intended to describe a relatively stable per-origin policy posture.

4.3. Intermediate AS Behavior

A receiving AS that chooses to process these communities MUST verify that the Global Administrator ASN in the Large Community matches the rightmost (Origin) AS in the AS_PATH. If they do not match, the community MUST be ignored to prevent unauthorized policy signaling.

If this check succeeds, a receiving AS MAY correlate the presence of ROA-Strict or ASPA-Strict communities with its locally derived validation results as part of its local policy framework.

For example, a local policy may treat a route carrying a ROA-Strict community as less acceptable when the local RPKI validation state is NotFound. Such behavior is illustrative only and is not mandated by this specification.

4.4. Applicability to Route Leak and Hijack Detection

Security policy communities may serve as additional context for routing analysis systems.

For example, a route that violates an origin-authorized export constraint, while also exhibiting abnormal AS path patterns, may be flagged as anomalous with higher confidence when it also carries a strict policy community.

Such signals can reduce false positives in detection systems by providing operator-declared intent, without asserting correctness. This document does not define detection algorithms or mitigation procedures.

4.5. Deployment Considerations

The proposed mechanism is compatible with existing routing policies and does not require changes to BGP implementations. Deployment of this mechanism is expected to be incremental and partial.

The proposed mechanism is intended for gradual deployment and interoperability with existing BGP technologies. Origin ASes may selectively signal policy intent for specific prefixes. In hybrid

networks where both supporting and non-supporting ASes are present, policy communities will simply be ignored by legacy BGP speakers, providing backward compatibility. No coordination between ASes is required.

For environments supporting both Standard [RFC1997] and Large [RFC8092] Communities, implementations SHOULD attach both representations to maximize backward compatibility. Operators are encouraged to monitor for loss or modification of policy communities due to intermediate ASes that filter or rewrite BGP Community attributes, so as to ensure policy expectations are properly signaled end-to-end.

5. Security Considerations

This document defines a policy signaling mechanism using BGP communities. It does not define a security mechanism and does not provide independent security guarantees. It is not intended for real-time attack mitigation or automated incident response.

This document follows the guidance in [AVOID-RPKI-STATE-IN-BGP] by not carrying any RPKI-derived validation state in BGP. The communities defined here do not encode or imply specific validation outcomes (such as Valid, Invalid, or NotFound). Instead, they allow an Origin AS to express a relatively stable policy posture regarding how downstream ASes may treat ambiguous validation results, if they choose to do so.

5.1. Authenticity and Integrity

The communities defined in this document are not cryptographically protected and may be modified, removed, or added in transit. This is consistent with existing BGP community usage and with the design goals of this document.

No attempt is made to ensure integrity or authenticity of community propagation. Accordingly, these communities MUST NOT be treated as authoritative security assertions and MUST NOT be used as a basis for accepting otherwise invalid routes.

The semantics defined herein apply only to communities that are plausibly originated by the Origin AS, as determined by the Global Administrator field matching the rightmost AS in the AS_PATH. This check is intended solely to limit semantic impersonation and does not constitute a security guarantee.

An adversary capable of hijacking a route may also attach, modify, or remove communities.

5.2. Relationship to Validation Mechanisms

The communities defined in this document do not represent validation results, security states, or assertions of route correctness, legitimacy, or authorization.

In particular, the presence or absence of a Security Policy Community MUST NOT be interpreted as indicating whether a route is valid or invalid under RPKI, ASPA, BGPsec, or any other validation mechanism.

These communities MUST NOT override locally derived validation results, including a "Valid" RPKI state. They may be correlated with validation outcomes as part of local policy or analysis, but they do not alter the semantics of those outcomes.

Implementations and Operators MUST NOT use these communities as a reason to skip or short-circuit local validation.

5.3. Policy Semantics and Downstream Behavior

The communities defined in this document express origin-authorized policy intent only. They do not define required actions.

Downstream Autonomous Systems MAY ignore these communities entirely without violating this specification. Any routing, filtering, or preference decisions remain solely a matter of local policy.

The absence of a policy community MUST NOT be interpreted as expressing the opposite intent.

This document does not require or expect consistent interpretation or uniform behavior across Autonomous Systems. Differences in interpretation, deployment, and operational use are expected and acceptable.

5.4. Denial-of-Service and Abuse Considerations

This document intentionally avoids defining communities that directly request route suppression or traffic dropping. As a result, it reduces the risk that a malicious actor could trigger network-wide disruption through abuse of policy signaling.

Nevertheless, operators should be aware that misconfiguration or abuse of these communities may influence local policy decisions if such decisions are explicitly configured to consider them. Operators are encouraged to avoid automated hard actions based solely on the presence of these communities, and to combine them with independently derived validation results and operational context.

5.5. Threat Model Summary

Potential abuse scenarios include, but are not limited to:

* false or misleading signaling of policy intent;

* removal or modification of policy signals during propagation;

* inconsistent signaling across multiple origin points.

These risks are inherent to existing uses of BGP communities and do not introduce new attack vectors. Operators SHOULD correlate these signals with independently verifiable information when making security-related decisions.

6. IANA Considerations

6.1. Large Community Mapping

This document defines new BGP Community values for signaling security policy intent. Compared to Extended Communities, Large Communities are used to avoid ASN exhaustion and ambiguity associated with 16-bit Global Administrator fields.

IANA is requested to create a sub-registry "BGP Security Policy Action IDs" under the "BGP Large Communities" registry.

The format of these communities are "Global-Administrator:Action-ID:Parameter". The Global Administrator MUST be the ASN of the Origin AS.

The "Strict" qualifier expresses only an origin-declared preference and does not define any required downstream behavior.

Action ID	Name	Policy Intent Description
1000	ROA-Strict	Origin expresses a preference for strict handling of routes when RPKI validation results are Invalid or NotFound.
1001	ASPA-Strict	Origin expresses a preference for strict handling of routes when ASPA validation results are Invalid or Unknown.

6.2. Standard Community Mapping

This mapping is provided solely to facilitate incremental deployment in networks that do not yet support BGP Large Communities.

For [RFC1997] support, the following values are assigned from the Well-Known range:

* "65535:1000" (ROA-Strict)

* "65535:1001" (ASPA-Strict)

Operators MUST understand that these Standard Communities cannot encode the Origin AS in the Global Administrator field, and therefore lack the plausibility check described for Large Communities. Their semantics remain the same, but they are more susceptible to impersonation and SHOULD be used with care.

7. References

7.1. Normative References

[RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, DOI 10.17487/RFC1997, August 1996, <https://www.rfc-editor.org/rfc/rfc1997>.

[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>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <https://www.rfc-editor.org/rfc/rfc4360>.

[RFC8092] Heitz, J., Ed., Snijders, J., Ed., Patel, K., Bagdonas, I., and N. Hilliard, "BGP Large Communities Attribute", RFC 8092, DOI 10.17487/RFC8092, February 2017, <https://www.rfc-editor.org/rfc/rfc8092>.

[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>.

7.2. Informative References

[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-22, 6 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-22>.

[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>.

[AVOID-RPKI-STATE-IN-BGP]
Snijders, J., Fiebig, T., and M. 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-03, 26 January 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-avoid-rpki-state-in-bgp-03>.

[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/rfc/rfc6480>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/rfc/rfc6482>.

[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>.

[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/rfc/rfc9234>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/rfc/rfc9582>.

Appendix A. Parameter Field Extensibility

The "Parameter" field in the BGP Security Policy Community is explicitly designed for extensibility. Currently, a value of "1" conveys default strict enforcement for security actions (e.g., ROA-Strict or ASPA-Strict). Future assignments may introduce further parameters to support nuanced policy signaling, such as variant handling levels, time-limited policies, or security requirements specific to more recent routing security enhancements.

Example encodings:

* "65001:1000:1" (ROA-Strict, default strict enforcement)

* "65001:1000:2" (ROA-Strict, but only for prefixes with maxLength constraints, a future possible assignment)

* "65001:1002:1" (hypothetical new Action-ID for a future policy, e.g., "AS-Cones Strict")

The Action-ID and Parameter range is managed through IANA for orderly growth as the community adopts richer security policies.

The extensibility of the Parameter field is intentionally limited to policy refinement and does not introduce conditional logic or dynamic state signaling.

Appendix B. Relationship to Existing Mechanisms

This section clarifies the relationship between the mechanism defined in this document and existing routing policy, traffic engineering, and routing security mechanisms. The goal is to explicitly delineate scope and avoid overlap or semantic ambiguity.

B.1. Relationship to RPKI, ROA, and ASPA

RPKI-based mechanisms such as ROA and ASPA provide cryptographic or registry-backed validation outcomes for routing information. These mechanisms answer the question of whether a route is consistent with registered authorization data.

The communities defined in this document do not provide validation and do not alter validation outcomes. They do not indicate that a route is valid, invalid, or authorized. Instead, they allow an Origin AS to express its operational expectations regarding how ambiguous validation outcomes (e.g., NotFound or Unknown) may be handled by downstream ASes.

This mechanism is therefore complementary to RPKI and ASPA. It operates strictly at the policy signaling layer and does not export validation state, consistent with the guidance in [AVOID-RPKI-STATE-IN-BGP].

B.2. Relationship to BGPsec

BGPsec [RFC8205] provides cryptographic protection of the AS_PATH to ensure path integrity and origin authentication. BGPsec is designed to assert and verify routing correctness.

The mechanism defined in this document does not provide cryptographic protection, path validation, or origin authentication. It does not attempt to replace or replicate BGPsec functionality. Instead, it provides an optional policy signal that may be used in conjunction with BGPsec or in environments where BGPsec is not deployed.

B.3. Relationship to BGP Color and Color-Aware Routing

BGP Color and Color-Aware Routing mechanisms are primarily intended to support traffic engineering and transport-specific constraints, such as latency, bandwidth, or SR policy selection.

While both mechanisms use BGP communities as signaling vehicles, the semantics are fundamentally different. BGP Color expresses forwarding or transport preferences, whereas the communities defined in this document express origin-declared routing security policy intent.

This document does not define path selection behavior, traffic steering, or forwarding constraints, and does not overlap with the objectives of Color-Aware Routing.

B.4. Relationship to Only-To-Customer (OTC)

OTC [RFC9234] is a mechanism designed to assist in route leak prevention by signaling export intent at AS boundaries.

The communities defined in this document differ from OTC in scope and semantics. OTC signals propagation constraints related to business relationships, whereas this document signals security policy expectations related to validation ambiguity.

These mechanisms are complementary and may coexist on the same routes. Neither mechanism subsumes the other.

B.5. Summary of Scope Separation

In summary:

* This document does not export validation state;

* this document does not assert routing correctness or authorization;

* this document does not define forwarding or traffic engineering behavior;

* this document does not mandate filtering or rejection behavior.

The mechanism is limited to expressing origin-declared security policy intent and is designed to coexist with existing routing security and policy mechanisms without semantic conflict.

Acknowledgments

TBD.

Authors' Addresses

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

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

Xiaoliang Wang
Capital Normal University
Email: wangxiaoliang0623@foxmail.com