

# BGP Communities for Security Policy Intent

<https://datatracker.ietf.org/doc/draft-guo-idr-bgp-security-policy-community/01/>

**Yangfei Guo**

IDR

IETF 125

March 2026

# Agenda

- Background
- BGP Security Policy Communities Overview
- Use Cases
- Security Considerations
- Next steps

# Background

- Increasing adoption of RPKI (40%+).
- ROA & ROV
  - Valid, Not-Found, Invalid
- Current security mechanisms verify routing information, but they do NOT express the security expectations of the origin AS.

If ROV Not-Found/Invalid,  
I want you to drop it.



- 1.If ROV valid, I will ...
- 2.If ROV Not-Found, I will ...
- 3.If ROV Invalid, I will ...



# Overview: BGP Security Policy Communities

- **Intent of Origin ASes:** "I have fully deployed security; do not accept anything less than Valid."
- BGP Large Communities:
  - *`Global Administrator : Action : Parameter`*

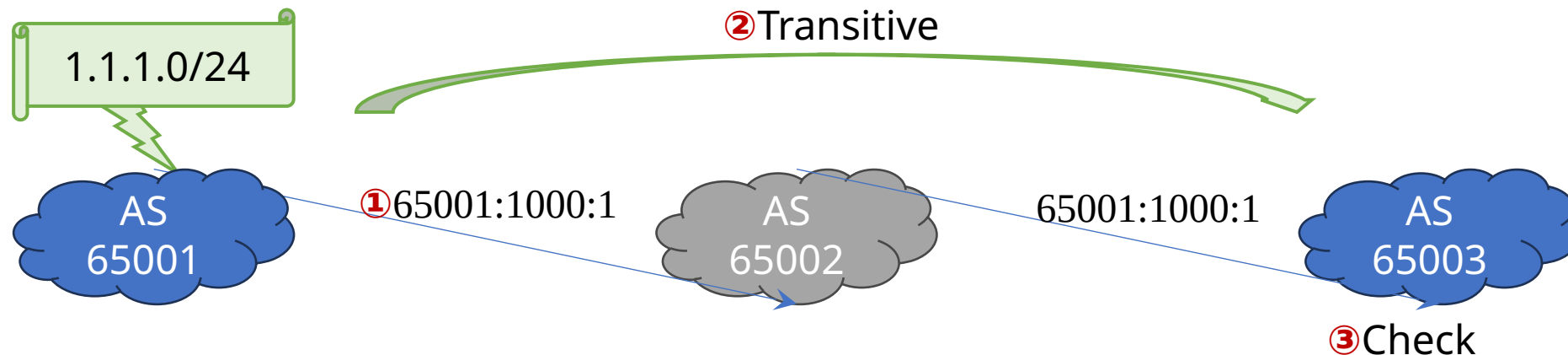
- **Standardized Values:**

Action ID	Name	Description
1000	ROA-Strict	Reject if RPKI state is Invalid OR NotFound.

- **Global Administrator:** MUST be the ASN of the Origin AS (rightmost AS in AS\_PATH) to ensure authenticity.

# Workflow Example

Example: 65001:1000:1 → AS 65001 signals ROA-Strict preference (default level)



- AS 65001 originates 1.1.1.0/24 and attaches 65001:1000:1 to show its `ROA-Strict` intent.
- Non-support ASes pass the community transparently.
- Matches the community's ASN (65001) with the rightmost AS in AS-PATH.
  - If matched, the AS can do ROV and upgrade its local policy from "Permissive" to "Strict."
  - Else, follow its local policy.

# Use Cases

- **Large Content Networks:** when Not-Found is emerged, some attackers may hijack the routes.
  - In practice, there should not be Not-Found window.
- **High value target Networks:** Not-Found exists when their prefixes are re-originated.
  - With ROA-Strict, ISP can deprioritize or reject suspicious re-origination.
- **BGP monitoring:** Build index: 'prefixes with ROA-Strict community'
  - When NotFound appears for indexed prefix → HIGH confidence alert
- etc.

# Security Considerations

- **Implementation**

- **Self-Protection:** Origin ASes must ensure their ROAs/ASPAs are correct before signaling "Strict" to avoid self-inflicted DoS.
- **Verification:** Receivers MUST verify the community ASN against the Origin AS in the AS-PATH to prevent "Signaling Hijacking."
- **Backward Compatibility:** Legacy ASes ignore the community.
  - Does not override Valid RPKI states; it only acts as a "Strictness Toggle" for ambiguous states.

- **Abuse**

- DoS Attack: Victim does not deploy RPKI.
- Pollution: Attackers randomly send ROA-Strict

# Conclusion

- A lightweight, non-disruptive mechanism to show origin AS's expectation.
- Reduces the "Permissive Policy" risk that currently limits the effectiveness of RPKI.
- An out-of-band mechanism, like RPKI object, may be a better choice.

# Questions? Feedback?

Comments are welcomed.

Please email feedback to

[guoyangf19@tsinghua.org.cn](mailto:guoyangf19@tsinghua.org.cn)

# Thank you!

**Let Your Efforts Be Seen!**