

BGP Security State Diagnostic Message (draft-retana-bgp-security-state- diagnostic-00)

Alvaro Retana, Robert Raszuk
{aretana,raszuk}@cisco.com

Motivation

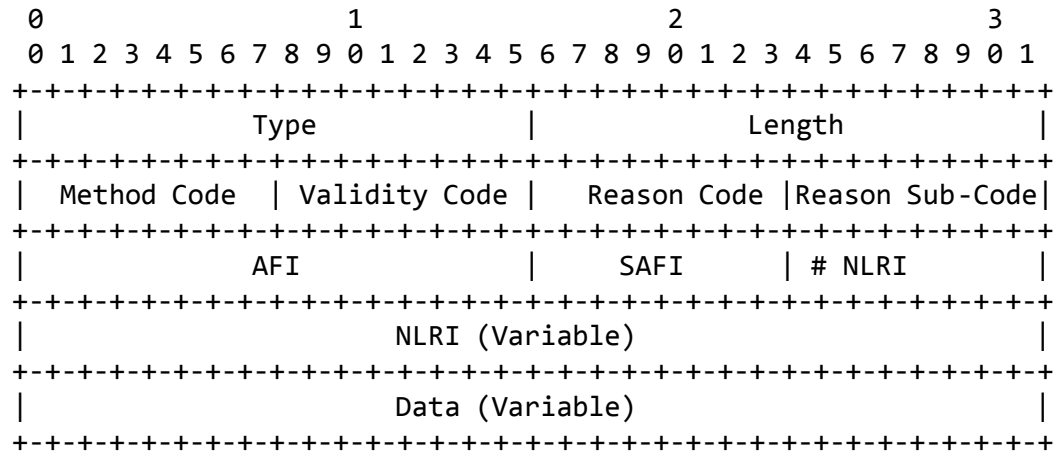
- BGP Prefix Origin Validation [[I-D.ietf-sidr-pfx-validate](#)] defines the interaction between BGP and a database able to map prefixes to their authorized ASes. One of the potential actions resulting from an "invalid" route is to reject it.
- This document describes an extension to the BGP Diagnostic Message [[I-D.raszuk-bgp-diagnostic-message](#)] and its use to communicate information about these "invalid" paths.
- The main motivation is to facilitate troubleshooting, monitoring, logging or even correction of the security mechanisms' operation, especially during initial deployment.

Operation

- **Summary: the receiver of an “invalid” path MAY let the sending ASN of the local state.**
 - The first AS boundary where the “invalid” state is detected may not be at the one with the origin.
- When a BGP speaker receives what considers to be an invalid advertisement it MAY send a BGP Security State Diagnostic Message to the eBGP peer from where it received it.
 - The information can then be used to diagnose and correct any potential local security policy violations.
 - Specific actions taken are outside the scope of this document, but could include withdrawing the original UPDATE or simply logging the information.

Implementation

- TLV in the BGP Diagnostic Message



- Method Code: Security mechanism used
 - 1 BGP Prefix Origin Validation
- Validity Code: Local Security State
 - 1 Not Found
 - 2 Invalid Path
- Reason Code: Why?
 - 1 Invalid Origin
 - 2 Certificate doesn't exist
- Reason Sub-Code + Data: Additional information.

Use of the BGP Diagnostic Message

- Proposed diagnostic communication channel [[I-D.raszuk-bgp-diagnostic-message](#)].
- RECOMMENDATIONS:
 - Rate limit the messages.
 - Messages be built in such a way as to include as many NLRI as possible.
- TLV sent when an invalid prefix is found, or
 - In response to the "Prefix specific BGP query" TLV (type 17) or the "Diagnostic Message Query" TLV (type 3).
 - The BGP Security State Diagnostic Message SHOULD NOT be sent periodically to a peer; to achieve this behavior the "Max frequency permitted" TLV (type 2) should be used to announce a value of 0.

Summary

- Intent: communicate local security state back to eBGP peers with the objective of facilitating the deployment of BGP Prefix Origin Validation.
 - Details of the signaling should be locally controlled.
 - No specific actions expected from the peer.
- The implementation using the BGP Diagnostic Message is independent of the operation.

Next Steps

- Adopt as a WG Document.
 - Defines a mechanism to aid in the deployment of the sidr protocols/extensions.
 - TLV in the BGP Diagnostic Message