Inter-Domain Routing
Internet-Draft
Intended status: Standards Track
Expires: September 8, 2011

A. Retana
R. Raszuk
Cisco Systems, Inc.

March 7, 2011

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

Abstract

This document describes an extension to the BGP Diagnostic Message to communicate the security state of a route. An application of this extension is to propagate information about non-secure advertisements back to the eBGP peer from where the information was received.

Status of this Memo

This Internet-Draft will expire on September 8, 2011.

Copyright Notice

Table of Contents

1. Introduction

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.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. The BGP Security State Diagnostic Message

The BGP Security State Diagnostic Message is a TLV to be carried in the BGP Diagnostic Message and is used to communicate the local security state of a path. It is defined as follows.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              Type             |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Method Code  | Validity Code |  Reason Code  |Reason Sub-Code|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              AFI              |     SAFI      |   # NLRI      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       NLRI (Variable)                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Data (Variable)                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

BGP Security State Diagnostic Message

Type:
Two octet field with a value TBD.

Length:
Two octet field indicating the TLV length in octets.

Method Code:
One octet field. Indicates which security mechanism was used to determine the validity of the path.

Value	Meaning
0	Reserved
1	BGP Prefix Origin Validation [I-D.ietf-sidr-pfx-validate]

Method Codes

Validity Code:
One octet field. Indicates whether the path is considered secure or not by the local AS. The values are to be interpreted relative to the Method defined above.

The following values are defined for Method Code 1:

Value	Meaning
0	Reserved
1	Not Found
2	Invalid Path

Validity Codes

Reason Code:
One octet field. Indicates the reason the security mechanism listed in the Method Code considered the path as indicated in the Validity Code. The values are specific to the Method Code used.

The following Reason Codes are defined for Method Code 1, Validity Code 2:

Value	Meaning
0	Reserved
1	Invalid Origin
2	Certificate doesn't exist

Reason Codes

Reason Sub-Code:
One octet field. Indicates any additional information related to the Reason Code indicated for the specific Method used. At this time no specific values are defined.

AFI (Address Family Identifier):
Two octet field, encoded the same way as in RFC 4760 [RFC4760].

SAFI (Subsequent Address Family Identifier):
Two octet field, encoded the same way as in RFC 4760 [RFC4760].

# NLRI (Number of Network Layer Reachability Information entries):
One octet field indicating the number of NLRI entries to follow.

NLRI:
Variable length field encoded as one or more 2-tuples of the form <length, prefix>, as described in RFC 4760 [RFC4760].

Data:
Variable length field. Indicates any additional information related to the Reason Code indicated for the specific Method used. This is an OPTIONAL field with variable length.

4. Operation

The mechanism described is intended to be primarily applied at autonomous system border routers.

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. It is RECOMMENDED that a BGP speaker limit the number of messages sent to a specific peer over a given period of time and that the messages be built in such a way as to include as many NLRI as possible.

A BGP speaker SHOULD also send the BGP Security State Diagnostic Message 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.

The information contained in the BGP Security State Diagnostic Message 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.

5. IANA Considerations

IANA is asked to create and maintain registries for the fields described in Section 3, and to assign the corresponding TLV type.

6. Security Considerations

The mechanism described in this document doesn't add any new security concerns.

7. Acknowledgements

The mechanism described in this document was influenced by discussions with Dacheng Zhang and Mingui Zhang.

The authors would like to thank the following people for their comments and suggestions: Bertrand Duvivier, Keyur Patel, Roque Gagliano and Russ White.

8. References

8.1. Normative References

[I-D.raszuk-bgp-diagnostic-message]
Raszuk, R., Chen, E., and B. Decraene, "BGP Diagnostic Message", draft-raszuk-bgp-diagnostic-message-00 (work in progress), October 2010.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

8.2. Informative References

[I-D.ietf-sidr-pfx-validate]
Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", draft-ietf-sidr-pfx-validate-01 (work in progress), February 2011.

Authors' Addresses

Alvaro Retana
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

Email: aretana@cisco.com

Robert Razsuk
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Email: raszuk@cisco.com