GROW
Internet-Draft
Updates: 7854 (if approved)
Intended status: Standards Track
Expires: 23 January 2026

H. Sharma
Vodafone
J. Haas
Juniper Networks

22 July 2025

TCP-AO Protection for BGP Monitoring Protocol (BMP)
draft-ietf-grow-bmp-tcp-ao-02

Abstract

This document outlines the utilization of the TCP Authentication Option (TCP-AO), as specified in [RFC5925], for the authentication of BGP Monitoring Protocol (BMP) sessions, as specified in [RFC7854]. TCP-AO provides for the authentication of BMP sessions established between routers and BMP stations at the TCP layer.

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 23 January 2026.

Table of Contents

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. Introduction

The BGP Monitoring Protocol (BMP), as specified in [RFC7854], recommends the use of IPsec [RFC4303] to address security considerations concerning the BMP session between a router and the BMP station managing BGP route collection. This document suggests the use of the TCP Authentication Option (TCP-AO) as an authentication mechanism to ensure end-to-end authentication of BMP sessions between the routers and the BMP stations. TCP-AO is also the choice of authentication for TCP-based network protocols such as BGP and LDP. A comprehensive discussion of TCP-AO is provided in [RFC5925].

3. TCP-AO Protection for BGP Monitoring Protocol (BMP)

The BGP Monitoring Protocol (BMP), defined in [RFC7854], plays a crucial role in network management by allowing routers to share information about their BGP RIBs. This helps operators monitor and troubleshoot their networks effectively. However, the security considerations associated with BMP have become increasingly critical in light of evolving threats. This document proposes that these threats be addressed by utilizing TCP-AO to safeguard BMP sessions.

TCP-AO provides protection against spoofed TCP segments and helps protect the integrity of the TCP session. Further, it provides for the authentication of session endpoints. Similar to BGP, BMP can benefit from these security properties.

TCP-AO helps protect the integrity of BMP session liveness at the TCP layer. As outlined in Section 3.2 of [RFC7854], BMP operates as a unidirectional protocol, meaning no BMP messages are transmitted from the monitoring station to the monitored router. BMP relies on the underlying TCP session, supported by TCP keepalives [RFC1122], to prevent session timeouts from the station to the monitored router.

3.1. Operational Recommendations for BMP

The implementation and use of TCP-AO to protect BMP session is RECOMMENDED in circumstances where the session might not otherwise be protected by alternative mechanisms such as IPsec.

4. Security Considerations

TCP-AO is not intended as a direct substitute for IPsec, nor is it suggested as such in this document. The Security Considerations for TCP-AO in Section 11 of [RFC7854] all apply to its application for BMP.

TCP-AO may inhibit connectionless resets when session keys have been lost or changed. This may cause BMP sessions to linger in some circumstances; however, BGP shares this consideration.

In the presence of NAT, TCP-AO requires additional support as defined in [RFC6978].

TCP-AO does not provide for privacy for the BMP protocol’s contents. When this is desired, IPsec with Encapsulating Security Payload (ESP) can help provide for such privacy.

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. 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/rfc/rfc2119>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/rfc/rfc5925>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/rfc/rfc7854>.

[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>.

6.2. Informative References

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <https://www.rfc-editor.org/rfc/rfc1122>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/rfc/rfc4303>.

[RFC6978] Touch, J., "A TCP Authentication Option Extension for NAT Traversal", RFC 6978, DOI 10.17487/RFC6978, July 2013, <https://www.rfc-editor.org/rfc/rfc6978>.

Acknowledgments

This document is an outcome of the experiences gained through implementing BMP. While TCP-AO safeguards other TCP protocols, BMP currently lacks the same level of protection.

Authors' Addresses

Hemant Sharma
Vodafone
Email: hemant.sharma@vodafone.com

Jeffrey Haas
Juniper Networks
Email: jhaas@juniper.net