GROW
Internet-Draft
Updates: 7854 (if approved)
Intended status: Informational
Expires: 8 February 2026

H. Sharma
S. Clarke
Vodafone

7 August 2025

BMPS: Transport Layer Security for BGP Monitoring Protocol
draft-hmntsharma-bmp-over-tls-03

Abstract

The BGP Monitoring Protocol (BMP) defines the communication between a BMP station and multiple routers, referred to as network elements (NEs). This document describes BMP over TLS, which uses Transport Layer Security (TLS) to ensure secure transport between the NE and the BMP monitoring station. It updates [RFC7854] regarding BMP session establishment and termination.

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 8 February 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 defined in [RFC7854], facilitates communication between NEs and a BMP station. Keeping this communication secure is important because it includes sharing sensitive information about BGP peers and monitored prefixes.

The Section 11 of [RFC7854] , "Security Considerations" acknowledges that while routes in public networks are generally not confidential, BGP is also utilized in private L3VPN [RFC4364] networks where confidentiality is crucial. It highlights that without mutual authentication through secure transport mechanisms, the channel is vulnerable to various attacks and recommends using IPSec [RFC4303] in tunnel mode with pre-shared keys for enhanced security in such scenarios.

Additionally, a recent draft proposal, [I-D.ietf-grow-bmp-tcp-ao], titled "TCP-AO Protection for BGP Monitoring Protocol (BMP)" suggests an alternative approach using the TCP Authentication Option [RFC5925]. This method authenticates the endpoints of the TCP session, thereby safeguarding its integrity. TCP-AO is beneficial in situations where full IPSec security may not be feasible, although unlike IPSec, it does not encrypt the session traffic.

Alternatively, Transport Layer Security (TLS), offers endpoint authentication, data encryption, and data integrity defined in the Transport Layer Security (TLS) Protocol Version 1.3 [RFC8446].

The BGP Monitoring Protocol (BMP) [RFC7854] relies on the TCP protocol to establish BGP sessions between routers. There are ongoing discussions within the IETF [I-D.draft-liu-grow-bmp-over-quic] to replace TCP with the QUIC protocol [RFC9000]. QUIC brings many features compared to TCP including security, the support of multiple streams or datagrams.

QUIC is suitable for BMP transport [I-D.draft-liu-grow-bmp-over-quic] and has the potential to replace a BMP connection for each "logical router" by a single QUIC connection with streams for the messages from each "logical router". However it’s deployment is dependent on the adoption of QUIC in router management stacks which have historically lagged behind server developments due to their cautious approach and slower development rate.

This document describes how BMP can operate over TCP/TLS. Experience in implementing BGP over TLS/TCP [I-D.draft-wirtgen-bgp-tls] showed that this is less costly than porting a BGP implementation over QUIC and the similarities suggest that the same is true for BMP.

This document describes how to utilize TLS to secure BMP sessions between a monitoring station (acting as the server) and a Network Element (acting as the client). Unlike BGP, where either side can act as the server, BMP’s role distinction simplifies the implementation of TLS in a client-server model. Henceforth, the term BMP over TLS will be referred to as BMPS.

3. BMP over TLS (BMPS)

3.1. Operational Summary

The operation of BMPS is virtually the same as the original BMP specification defined in [RFC7854], but with an additional layer of security using TLS.

In BMPS, the BMP station functions as the TLS server, while NEs act as TLS clients. Following the completion of the TCP three-way handshake, as defined in Section 3.4 of [RFC793], each NE, functioning as a TLS client, initiates a TLS handshake with the BMP monitoring station, acting as the TLS server. Once the TLS connection is successfully established, NEs can immediately start transmitting BMP messages, as there is no separate BMP initiation or handshake phase.

The following steps summarize the operational flow of BMPS:

1. The NE initiates and completes a TCP handshake.

2. The NE initiates and completes a TLS handshake with the BMP monitoring station.

3. BMP messages are transmitted by the NE according to [RFC7854].

A BMPS session ends when the underlying TCP or TLS session is terminated for any reason.

The Section 3.2 of [RFC7854] states, "No BMP message is ever sent from the monitoring station to the router." To adhere to this standard, the monitoring station MUST listen on separate ports for BMP (non-TLS) and BMPS (TLS) sessions. This approach also offers a simplified "make before break" migration from BMP to BMPS.

3.2. Transport Layer Security

In regular TLS connections, the server has a TLS certificate along with a public/private key pair, whereas the client does not.

For BMP over TLS (BMPS), it is REQUIRED to implement mutual TLS (mTLS), wherein both the server (BMP station) and the client (network element) have certificates, and both sides authenticate each other using their respective public/private key pairs.

A self-signed "root" TLS certificate is REQUIRED for mTLS, allowing an organization to act as its own certificate authority. The certificates issued to both the BMP station and NEs should correspond to this root certificate.

The operational flow of BMP over TLS is similar to standard TLS operations:

1. The NE initiates the connection to the BMP station.

2. The station presents its TLS certificate.

3. The NE verifies the station’s certificate.

4. The NE presents its TLS certificate.

5. The station verifies the NE’s certificate.

6. The TLS connection is established.

7. The NE begins transmitting BMP data to the station over the encrypted TLS channel.

TLS version 1.3, defined in [RFC8446], streamlines the handshake process and supports more robust cipher suites compared to the previous versions, enhancing both speed and security.

The BMPS is REQUIRED to support TLS 1.3 which has become a dominant standard.

3.3. Operational Recommendations for BMPS

The BMP over TLS (BMPS) is RECOMMENDED as an alternative mechanism to safeguard BMP sessions in scenarios where alternative protections like IPSec may not be feasible or deployed.

4. Security Considerations

The BMPS implementation increases computational demands due to continuous encryption and decryption processes, resulting in high CPU utilization and potential vulnerability to denial-of-service attacks.

The TLS cipher suites that provide only data integrity validation without encryption SHOULD NOT be used by default.

The BMPS implementation SHOULD follow the best practices and recommendations for using TLS, as per the Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) as defined in [RFC7525].

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>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/rfc/rfc7525>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

6.2. Informative References

[I-D.draft-liu-grow-bmp-over-quic] Liu, Y., Lin, C., Graf, T., and P. Lucente, "Using BMP over QUIC connection", Work in Progress, Internet-Draft, draft-liu-grow-bmp-over-quic-02, 19 February 2025, <https://datatracker.ietf.org/doc/html/draft-liu-grow-bmp-over-quic-02>.

[I-D.draft-wirtgen-bgp-tls] Wirtgen, T. and O. Bonaventure, "BGP over TLS/TCP", Work in Progress, Internet-Draft, draft-wirtgen-bgp-tls-03, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-wirtgen-bgp-tls-03>.

[I-D.ietf-grow-bmp-tcp-ao] Sharma, H. and J. Haas, "TCP-AO Protection for BGP Monitoring Protocol (BMP)", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-tcp-ao-02, 22 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-tcp-ao-02>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/rfc/rfc2818>.

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

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/rfc/rfc4364>.

[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>.

[RFC793] Postel, J., "Transmission Control Protocol", RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/rfc/rfc793>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/rfc/rfc8253>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

Acknowledgments

This document is the result of studying all the referenced RFCs and drawing some parallels from PCEPS [RFC8253], leading to the specification for BMP over TLS (BMPS).

We are grateful to the contributors of the RFCs listed in the References section. Their work has been instrumental in shaping and inspiring the development of this specification.

Authors' Addresses

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

Steven Clarke
Vodafone
Email: steven.clarke@vodafone.com