IDR
Internet-Draft
Intended status: Experimental
Expires: 8 January 2026

T. Wirtgen
UCLouvain
O. Bonaventure
UCLouvain & WELRI

7 July 2025

BGP over TLS/TCP
draft-wirtgen-bgp-tls-03

Abstract

This document specifies the utilization of TCP/TLS to support BGP.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-wirtgen-bgp-tls/.

Discussion of this document takes place on the IDR Working Group mailing list (mailto:idr@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/idr/. Subscribe at https://www.ietf.org/mailman/listinfo/idr/.

Source for this draft and an issue tracker can be found at https://github.com/IPNetworkingLab/draft-bgp-tls.

Status of This Memo

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) [RFC4271] relies on the TCP protocol to establish BGP sessions between routers. There are ongoing discussions within the IETF [I-D.draft-retana-idr-bgp-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.

From a security viewpoint, an important benefit of QUIC compared to TCP is that QUIC by design prevents injection attacks that are possible when TCP is used by BGP [RFC4272]. Several techniques can be used by BGP routers to counter this attacks [RFC5082] [RFC5925]. TCP-AO [RFC5925] authenticates the packets exchanged over a BGP session and provides similar features as QUIC. However, it a recent survey [SURVEY] indicates that it remains less used than TCP over MD5 [RFC2385].

The widespread deployment of TLS [RFC8446] combined with the possibility of deriving TCP-AO keys from the TLS handshake [I-D.draft-piraux-tcp-ao-tls] creates an interest in using TLS to secure BGP sessions. While TLS is mainly used to interact with servers that have a certificate bound to a domain name, it is also possible to use TLS certificates bound to IP addresses [IPCERT]. Such certificates are very useful to use BGP over TLS/TCP.

This document describes how BGP can operate over TCP/TLS. Experience in implementing BGP over TLS/TCP [BGPOST] shows that this is less costly than porting a BGP implementation over QUIC.

2. Conventions and Definitions

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.

This document uses network byte order (that is, big endian) values. Fields are placed starting from the high-order bits of each byte.

3. Summary of operation

A BGP over TLS/TCP session is established in two phases:

* establish a transport layer connection using TCP

* establish a TLS session over the TCP connection

The TCP connection SHOULD be established on port TBD1.

During the establishment of the TLS session, the router that initiates the connection MUST use the "botls" token in the Application Layer Protocol Negotiation (ALPN) extension [RFC7301]. The support for other ALPN MUST NOT be proposed during the TLS handshake.

Once the TLS handshake is established and finished, the BGP session is initiated as defined in [RFC4271] and the protocol operates in the same way as a classic BGP over TCP session. The difference is that the BGP session is now encrypted and authenticated using the TLS layer. As in [I-D.draft-retana-idr-bgp-quic], the TLS authentication parameters used for this connection are out of the scope of this draft.

4. Security Considerations

This document improves the security of BGP sessions since the information exchanged over the session is now protected by using TLS.

If TLS encounters a payload injection attack, it will generate an alert that immediately closes the TLS session. The BGP router SHOULD then attempt to reestablish the session. However, this will cause traffic to be interrupted during the connection re-establishement.

If both BGP peer supports TCP-AO, the TLS stack is protected against payload injection and this attack can be avoided. When enabled, TCP-AO counters TCP injection attacks listed in [RFC5082].

Furthermore, if the BGP router supports TCP-AO, we recommend an opportunistic TCP-AO approach as suggested in [I-D.draft-piraux-tcp-ao-tls]. The router will attempt to connect using TCP-AO with a default key. When the TLS handshake is finished, the routers will securely derive a new TCP-AO key from the TLS key.

TCP-MD5 [RFC2385] MAY be used to protect the TLS session if TCP-AO is not available on the BGP router.

5. IANA Considerations

IANA is requested to assign a TCP port (TBD1) from the "Service Name and Transport Protocol Port Number Registry" as follows:

* Service Name: botls
* Port Number: TBD1
* Transport Protocol: TCP
* Description: BGP over TLS/TCP
* Assignee: IETF
* Contact: IDR WG
* Registration Data: TBD
* Reference: this document
* Unauthorized Use Reported: idr@ietf.org

It is suggested to use the same port as the one selected for BGP over QUIC [I-D.draft-retana-idr-bgp-quic].

Acknowledgments

The authors thank Dimitri Safonov for the TCP-AO implementation in Linux. This work has been partially supported by the Walloon Region as part of the funding of the FRFS-WEL-T strategic axis.

Change log

References

Normative References

[I-D.draft-piraux-tcp-ao-tls] Piraux, M., Bonaventure, O., and T. Wirtgen, "Opportunistic TCP-AO with TLS", Work in Progress, Internet-Draft, draft-piraux-tcp-ao-tls-02, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-piraux-tcp-ao-tls-02>.

[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>.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, DOI 10.17487/RFC2385, August 1998, <https://www.rfc-editor.org/rfc/rfc2385>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/rfc/rfc4271>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/rfc/rfc4272>.

[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>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/rfc/rfc7301>.

[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>.

Informative References

[BGPOST] Wirtgen, T., Rybowski, N., Pelsser, C., and O. Bonaventure, "The Multiple Benefits of a Secure Transport for BGP", Association for Computing Machinery (ACM), Proceedings of the ACM on Networking vol. 2, no. CoNEXT4, pp. 1-23, DOI 10.1145/3696406, November 2024, <https://doi.org/10.1145/3696406>.

[I-D.draft-retana-idr-bgp-quic] Retana, A., Qu, Y., Haas, J., Chen, S., and J. Tantsura, "BGP over QUIC", Work in Progress, Internet-Draft, draft-retana-idr-bgp-quic-07, 6 July 2025, <https://datatracker.ietf.org/doc/html/draft-retana-idr-bgp-quic-07>.

[IPCERT] Gable, A., "We've Issued Our First IP Address Certificate", Blog https://letsencrypt.org/2025/07/01/issuing-our-first-ip-address-certificate/ , 2025.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <https://www.rfc-editor.org/rfc/rfc5082>.

[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>.

[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>.

[SURVEY] Wirtgen, T., "Survey on the Configuration of BGP routers", Technical report, http://hdl.handle.net/2078.1/292356 , 2024.

Authors' Addresses

Thomas Wirtgen
UCLouvain
Email: thomas.wirtgen@uclouvain.be

Olivier Bonaventure
UCLouvain & WELRI
Email: olivier.bonaventure@uclouvain.be