Workgroup: IDR
Internet-Draft: draft-wirtgen-bgp-tls-00
Published: 23 October 2023
Intended Status: Experimental
Expires: 25 April 2024
Authors: T. Wirtgen
UCLouvain & WELRI
O. Bonaventure
UCLouvain & WELRI

BGP over TLS/TCP

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/obonaventure/draft-bgp-tls.

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 25 April 2024.

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) [RFC4271] relies on the TCP protocol to establish BGP sessions between routers. A recent draft [I-D.draft-retana-idr-bgp-quic] has proposed 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 provides similar features as QUIC. However, it is notoriously difficult to configure the keys used to protect BGP sessions.

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. This document describes how BGP can operate over TCP/TLS.

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 derive a new TCP-AO key using the TLS key.

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.

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-00, 23

October 2023, <https://datatracker.ietf.org/doc/html/draft-piraux-tcp-ao-tls-00>.

[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>.

[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

[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-02, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-retana-idr-bgp-quic-02>.

[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>.

Authors' Addresses

Thomas Wirtgen
UCLouvain & WELRI

Email: thomas.wirtgen@uclouvain.be

Olivier Bonaventure
UCLouvain & WELRI

Email: olivier.bonaventure@uclouvain.be