

Network Configuration
Internet-Draft
Updates: 7589 (if approved)
Intended status: Standards Track
Expires: 21 July 2024

S. Turner
sn3rd
R. Housley
Vigil Security
18 January 2024

Updates to Using the NETCONF Protocol over Transport Layer Security
(TLS) with Mutual X.509 Authentication
draft-ietf-netconf-over-tls13-04

Abstract

RFC 7589 defines how to protect NETCONF messages with TLS 1.2. This document updates RFC 7589 to update support requirements for TLS 1.2 and add TLS 1.3 support requirements, including restrictions on the use of TLS 1.3's early data.

About This Document

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

The latest revision of this draft can be found at <https://netconf-wg.github.io/netconf-over-tls13/draft-ietf-netconf-over-tls13.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-netconf-over-tls13/>.

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

Source for this draft and an issue tracker can be found at <https://github.com/netconf-wg/netconf-over-tls13>.

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 21 July 2024.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Conventions and Definitions	3
3. Early Data	3
4. Cipher Suites	3
5. Security Considerations	4
6. IANA Considerations	4
7. Normative References	5
Acknowledgments	6
Authors' Addresses	6

1. Introduction

[RFC7589] defines how to protect NETCONF messages [RFC6241] with TLS 1.2 [RFC5246]. This document updates [RFC7589] to update support requirements for TLS 1.2 [RFC5246] and to add TLS 1.3 [I-D.ietf-tls-rfc8446bis] support requirements, including restrictions on the use of TLS 1.3's early data which is also known as 0-RTT data. It also updates the "netconf-tls" IANA Registered Port Number entry to refer to this document. All other provisions set forth in [RFC7589] are unchanged, including connection initiation, message framing, connection closure, certificate validation, server identity, and client identity.

| NOTE: Implementations that support TLS 1.3
| [I-D.ietf-tls-rfc8446bis] should refer to TLS 1.3
| [I-D.ietf-tls-rfc8446bis] in Sections 4 and 5 of [RFC7589].

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.

3. Early Data

Early data (aka 0-RTT data) is a mechanism defined in TLS 1.3 [I-D.ietf-tls-rfc8446bis] that allows a client to send data ("early data") as part of the first flight of messages to a server. Note that TLS 1.3 can be used without early data as per Appendix F.5 of [I-D.ietf-tls-rfc8446bis]. In fact, early data is permitted by TLS 1.3 only when the client and server share a Pre-Shared Key (PSK), either obtained externally or via a previous handshake. The client uses the PSK to authenticate the server and to encrypt the early data.

As noted in Section 2.3 of [I-D.ietf-tls-rfc8446bis], the security properties for early data are weaker than those for subsequent TLS-protected data. In particular, early data is not forward secret, and there is no protection against the replay of early data between connections. Appendix E.5 of [I-D.ietf-tls-rfc8446bis] requires applications not use early data without a profile that defines its use. This document specifies that NETCONF implementations that support TLS 1.3 MUST NOT use early data.

4. Cipher Suites

Implementations MUST support mutually authenticated TLS 1.2 [RFC5246] and they are, as specified in [RFC9325], recommended to support the cipher suites found in Section 4.2 of [RFC9325].

Implementations MAY implement additional TLS 1.2 cipher suites that provide mutual authentication [RFC5246] and confidentiality as required by NETCONF [RFC6241].

Implementations SHOULD support mutually authenticated TLS 1.3 [I-D.ietf-tls-rfc8446bis] and, if implemented, MUST prefer to negotiate TLS 1.3 over earlier versions of TLS.

Implementations that support TLS 1.3 [I-D.ietf-tls-rfc8446bis] are REQUIRED to support the mandatory-to-implement cipher suites listed in Section 9.1 of [I-D.ietf-tls-rfc8446bis].

Implementations that support TLS 1.3 MAY implement additional TLS cipher suites that provide mutual authentication and confidentiality, which are required for NETCONF [RFC6241].

5. Security Considerations

The Security Considerations of [RFC6241], [RFC7589], and [RFC9325] apply here as well.

NETCONF implementations SHOULD follow the TLS recommendations given in [RFC9325].

For implementations that support TLS 1.3, the Security Considerations of TLS 1.3 [I-D.ietf-tls-rfc8446bis] apply.

As specified in [RFC7589], NETCONF over TLS requires mutual authentication.

For implementations that support TLS 1.3 [I-D.ietf-tls-rfc8446bis]:

TLS 1.3 mutual authentication is used to ensure that only authorized users and systems are able to view the NETCONF server's configuration and state or to modify the NETCONF server's configuration. To this end, neither the client nor the server should establish a NETCONF over TLS 1.3 connection with an unknown, unexpected, or incorrectly identified peer; see Section 7 of [RFC7589]. If deployments make use of a trusted list of Certification Authority (CA) certificates [RFC5280], then the listed CAs should only issue certificates to parties that are authorized to access the NETCONF servers. Doing otherwise will allow certificates that were issued for other purposes to be inappropriately accepted by a NETCONF server.

The Security Considerations of [RFC9525] apply to all implementations when the client checks the identity of the server, as is required in Section 6 of [RFC7589].

6. IANA Considerations

IANA is requested to add a reference to this document in the "netconf-tls" entry in the "Service Name and Transport Protocol Port Number Registry". The updated registry entry would appear as follows:

Service Name: netconf-tls
Transport Protocol(s): TCP
Assignee: IESG <iesg@ietf.org>
Contact: IETF Chair <chair@ietf.org>
Description: NETCONF over TLS
Reference: RFC 7589, [THIS RFC]
Port Number: 6513

7. Normative References

- [I-D.ietf-tls-rfc8446bis]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-09, 7 July 2023, <<https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-09>>.
- [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>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <<https://www.rfc-editor.org/rfc/rfc5246>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/rfc/rfc5280>>.
- [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <<https://www.rfc-editor.org/rfc/rfc6241>>.
- [RFC7589] Badra, M., Luchuk, A., and J. Schoenwaelder, "Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication", RFC 7589, DOI 10.17487/RFC7589, June 2015, <<https://www.rfc-editor.org/rfc/rfc7589>>.
- [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>>.

- [RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati,
"Recommendations for Secure Use of Transport Layer
Security (TLS) and Datagram Transport Layer Security
(DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November
2022, <<https://www.rfc-editor.org/rfc/rfc9325>>.
- [RFC9525] Saint-Andre, P. and R. Salz, "Service Identity in TLS",
RFC 9525, DOI 10.17487/RFC9525, November 2023,
<<https://www.rfc-editor.org/rfc/rfc9525>>.

Acknowledgments

We would like to thank Per Andersson, J端rgen Sch旦nw辰lder, Jeff
Hartley, Rob Wilton, and Qin Wu for their reviews.

Authors' Addresses

Sean Turner
sn3rd
Email: sean@sn3rd.com

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA, 20170
United States of America
Email: housley@vigilsec.com