Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: March 30, 2019

J. Fenton
Altmode Networks

September 26, 2018

SMTP Require TLS Option
draft-ietf-uta-smtp-require-tls-04

Abstract

The SMTP STARTTLS option, used in negotiating transport-level encryption of SMTP connections, is not as useful from a security standpoint as it might be because of its opportunistic nature; message delivery is, by default, prioritized over security. This document describes an SMTP service extension, REQUIRETLS, and message header field, RequireTLS. If the REQUIRETLS option or RequireTLS message header field is used when sending a message, it asserts a request on the part of the message sender to override the default negotiation of TLS, either by requiring that TLS be negotiated when the message is relayed, or by requesting that recipient-side policy mechanisms such as MTA-STS and DANE be ignored when relaying a message for which security is unimportant.

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 March 30, 2019.

Copyright Notice

Copyright (c) 2018 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The SMTP [RFC5321] STARTTLS service extension [RFC3207] provides a means by which an SMTP server and client can establish a Transport Layer Security (TLS) protected session for the transmission of email

messages. By default, TLS is used only upon mutual agreement (successful negotiation) of STARTTLS between the client and server; if this is not possible, the message is sent without transport encryption. Furthermore, it is common practice for the client to negotiate TLS even if the SMTP server's certificate is invalid.

Policy mechanisms such as DANE [RFC7672] and MTA-STS [RFC8461] may impose requirements for the use of TLS for email destined for some domains. However, such policies do not allow the sender to specify which messages are more sensitive and require transport-level encryption, and which ones are less sensitive and ought to be relayed even if TLS cannot be negotiated successfully.

The default opportunistic nature of SMTP TLS enables several "on the wire" attacks on SMTP security between MTAs. These include passive eavesdropping on connections for which TLS is not used, interference in the SMTP protocol to prevent TLS from being negotiated (presumably accompanied by eavesdropping), and insertion of a man-in-the-middle attacker exploiting the lack of server authentication by the client. Attacks are described in more detail in the Security Considerations section of this document.

REQUIRETLS consists of two mechanisms: an SMTP service extension and a message header field. The service extension is used to specify that a given message sent during a particular session MUST be sent over a TLS-protected session with specified security characteristics. It also requires that the SMTP server advertise that it supports REQUIRETLS, in effect promising that it will honor the requirement to enforce TLS transmission and REQUIRETLS support for onward transmission of those messages.

The RequireTLS message header field is used to convey a request to ignore recipient-side policy mechanisms such as MTA-STS and DANE, thereby prioritizing delivery over ability to negotiate TLS. Unlike the service extension, the RequireTLS header field allows the message to transit through one or more MTAs that do not support REQUIRETLS.

1.1. 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. The REQUIRETLS Service Extension

1. The textual name of the extension is "Require TLS".

2. The EHLO keyword value associated with this extension is "REQUIRETLS".

3. One MAIL FROM option is defined by this extension.

4. One new SMTP status code is defined by this extension to convey an error condition resulting from failure of the client to send to a server not also supporting the REQUIRETLS extension.

In order to specify REQUIRETLS treatment for a given message, the REQUIRETLS option is specified on the MAIL FROM command when that message is transmitted. This option MUST only be specified in the context of an SMTP session meeting the security requirements that have been specified:

- The session itself MUST employ TLS transmission.

- The certificate presented by the SMTP server MUST either verify successfully in a trust chain leading to a certificate trusted by the SMTP client or it MUST verify succesfully using DANE as specified in RFC 7672 [RFC7672]. For trust chains, the choice of trusted (root) certificates is at the discretion of the SMTP client.

- Following the negotiation of STARTTLS, the SMTP server MUST advertise in the subsequent EHLO response that it supports REQUIRETLS.

3. The RequireTLS Header Field

One new message header field, RequireTLS, is defined by this specification. It is used for messages requesting that recipient TLS policy (including MTA-STS [RFC8461] and DANE [RFC7672]) be ignored.

The RequireTLS header field has a single REQUIRED parameter:

- NO - The SMTP client SHOULD attempt to send the message regardless of its ability to negotiate STARTTLS with the SMTP server, ignoring policy-based mechanisms (including MTA-STS and DANE), if any, asserted by the recipient domain. Nevertheless, the client SHOULD negotiate STARTTLS with the server if available.

More than one instance of the RequireTLS header field MUST NOT appear in a given message.

4. REQUIRETLS Semantics

4.1. REQUIRETLS Receipt Requirements

Upon receipt of the REQUIRETLS option on a MAIL FROM command during the receipt of a message, an SMTP server MUST tag that message as needing REQUIRETLS handling.

Upon receipt of a message not specifying the REQUIRETLS option on its MAIL FROM command but containing the RequireTLS header field in its message header, an SMTP server implementing this specification MUST tag that message with the option specified in the RequireTLS header field. If the REQUIRETLS MAIL FROM parameter is specified, the RequireTLS header field MUST be ignored but MAY be included in onward relay of the message.

The manner in which the above tagging takes place is implementation-dependent. If the message is being locally aliased and redistributed to multiple addresses, all instances of the message MUST be tagged in the same manner.

4.2. REQUIRETLS Sender Requirements

4.2.1. Sending with TLS Required

When sending a message tagged as requiring TLS, the sending (client) MTA MUST:

1. Look up the SMTP server to which the message is to be sent as described in [RFC5321] Section 5.1.

2. Open an SMTP session with the peer SMTP server using the EHLO verb.

3. Establish a TLS-protected SMTP session with its peer SMTP server and authenticate the server’s certificate as specified in [RFC6125] or [RFC7672] as applicable.

4. Ensure that the response to the subsequent EHLO following establishment of the TLS protection advertises the REQUIRETLS capability.

5. The SMTP client SHOULD also require that meaningfully secure cipher algorithms and key lengths be negotiated with the server. The choices of key lengths and algorithms change over time, so a specific requirement is not presented here.

If any of the above steps fail, the client MUST issue a QUIT to the server and repeat steps 2-4 with each host on the recipient domain's list of MX hosts in an attempt to find a mail path that meets the sender's requirements. The client MAY send other, unprotected, messages to that server if it has any prior to issuing the QUIT. If there are no more MX hosts, the client MUST NOT transmit the message to the domain.

Following such a failure, the SMTP client MUST send a non-delivery notification to the reverse-path of the failed message as described in section 3.6 of [RFC5321]. The following status codes [RFC5248] SHOULD be used:

- REQUIRETLS not supported by server: 5.7.x REQUIRETLS needed
- Unable to establish TLS-protected SMTP session: 5.7.10 Encryption needed

Refer to Section 5 for further requirements regarding non-delivery messages.

If all REQUIRETLS requirements have been met, transmit the message, issuing the REQUIRETLS option on the MAIL FROM command with the required option(s), if any.

4.2.2. Sending with TLS Optional

Messages tagged RequireTLS: NO are handled as follows. When sending such a message, the sending (client) MTA MUST:

- Look up the SMTP server to which the message is to be sent as described in [RFC5321] Section 5.1.
- Open an SMTP session with the peer SMTP server using the EHLO verb. Attempt to negotiate STARTTLS if possible, and follow any policy published by the recipient domain, but do not fail if this is unsuccessful.

Some SMTP servers may be configured to require STARTTLS connections as a matter of policy and not accept messages in the absence of STARTTLS. A non-delivery notification MUST be returned to the sender if message relay fails due to an inability to negotiate STARTTLS when required by the server.

Since messages tagged with RequireTLS: NO will sometimes be sent to SMTP servers not supporting REQUIRETLS, that option will not be uniformly observed by all SMTP relay hops.

4.3. REQUIRETLS Submission

An MUA or other agent making the initial introduction of a message has authority to decide whether to require TLS. When TLS is to be required, it MUST do so by negotiating STARTTLS and REQUIRETLS and include the REQUIRETLS option on the MAIL FROM command, as is done for message relay.

When TLS is not to be required, the sender MUST include the RequireTLS header field in the message. SMTP servers implementing this specification MUST interpret this header field as described in Section 4.1.

In either case, the decision whether to specify REQUIRETLS MAY be done based on a user interface selection or based on a ruleset or other policy. The manner in which the decision to require TLS is made is implementation-dependent and is beyond the scope of this specification.

4.4. Delivery of REQUIRETLS messages

Messages are usually retrieved by end users using protocols other than SMTP such as IMAP [RFC3501], POP [RFC1939], or web mail systems. Mail delivery agents supporting the REQUIRETLS SMTP option SHOULD observe the guidelines in [RFC8314].

5. Non-delivery message handling

Non-delivery ("bounce") messages usually contain important metadata about the message to which they refer, including the original message header. They therefore MUST be protected in the same manner as the original message. All non-delivery messages resulting from messages with the REQUIRETLS SMTP option, whether resulting from a REQUIRETLS error or some other, MUST also specify the REQUIRETLS SMTP option unless redacted as described below.

The path from the origination of an error bounce message back to the MAIL FROM address may not share the same REQUIRETLS support as the forward path. Therefore, users requiring TLS are advised to make sure that they are capable of receiving mail using REQUIRETLS as well. Otherwise, such non-delivery messages will be lost.

If a REQUIRETLS message is bounced, the server MUST behave as if RET=HDRS was present as described in [RFC3461]. If both RET=FULL and REQUIRETLS are present, the RET=FULL MUST be disregarded and MAY be transformed to RET=HDRS on relay. The SMTP client for a REQUIRETLS bounce message MUST use an empty MAIL FROM return-path as required by [RFC5321]. When the MAIL FROM return-path is empty, the REQUIRETLS

parameter SHOULD NOT cause a bounce message to be discarded even if the next-hop relay does not advertise REQUIRETLS.

Senders of messages requiring TLS are advised to consider the possibility that bounce messages will be lost as a result of REQUIRETLS return path failure, and that some information could be leaked if a bounce message is not able to be transmitted with REQUIRETLS.

6. Mailing list considerations

Mailing lists, upon receipt of a message, originate new messages to list addresses. This is distinct from an aliasing operation that redirects the original message, in some cases to multiple recipients. The requirement to preserve the REQUIRETLS tag therefore does not necessarily extend to mailing lists, although the inclusion of the RequireTLS header field MAY cause messages sent to mailing lists to inherit this characteristic. REQUIRETLS users SHOULD be made aware of this limitation so that they use caution when sending to mailing lists and do not assume that REQUIRETLS applies to messages from the list operator to list members.

Mailing list operators MAY apply REQUIRETLS requirements in incoming messages to the resulting messages they originate. If this is done, they SHOULD also apply these requirements to administrative traffic, such as messages to moderators requesting approval of messages.

7. IANA Considerations

If published as an RFC, this draft requests the addition of the following keyword to the SMTP Service Extensions Registry [MailParams]:

Textual name:	RequireTLS
EHLO keyword value:	REQUIRETLS
Syntax and parameters:	(no parameters)
Additional SMTP verbs:	none
MAIL and RCPT parameters:	REQUIRETLS parameter on MAIL
Behavior:	Use of the REQUIRETLS parameter on the MAIL verb causes that message to require the use of TLS and tagging with REQUIRETLS for all onward relay.
Command length increment:	11 characters

If published as an RFC, this draft requests the addition of an entry to the Simple Mail Transfer Protocol (SMTP) Enhanced Status Codes Registry [SMTPStatusCodes]:

Code:	5.7.YYY
Sample Text:	REQUIRETLS support required
Associated basic status code:	530
Description:	This indicates that the message was not able to be forwarded because it was received with a REQUIRETLS requirement and none of the SMTP servers to which the message should be forwarded provide this support.
Reference:	(this document)
Submitter:	J. Fenton
Change controller:	IESG

If published as an RFC, this draft requests the addition of an entry to the Permanent Message Header Field Names Registry [PermMessageHeaderFields]:

Header field name:	RequireTLS
Applicable protocol:	mail
Status:	provisional
Author/change controller:	IETF UTA Working Group
Specification document:	(this document)

This section is to be updated for publication by the RFC Editor.

8. Security Considerations

The purpose of REQUIRETLS is to improve communications security for email by giving the originator of a message an expectation that it will be transmitted in an encrypted form "over the wire". When used, REQUIRETLS changes the traditional behavior of email transmission, which favors delivery over the ability to send email messages using transport-layer security, to one in which requested security takes precedence over delivery and domain-level policy.

The following considerations apply to the REQUIRETLS service extension but not the RequireTLS header field, since messages specifying the header field are less concerned with transport security.

8.1. Passive attacks

REQUIRETLS is generally effective against passive attackers who are merely trying to eavesdrop on an SMTP exchange between an SMTP client and server. This assumes, of course, the cryptographic integrity of the TLS connection being used.

8.2. Active attacks

Active attacks against TLS encrypted SMTP connections can take many forms. One such attack is to interfere in the negotiation by changing the STARTTLS command to something illegal such as XXXXXXXX. This causes TLS negotiation to fail and messages to be sent in the clear, where they can be intercepted. REQUIRETLS detects the failure of STARTTLS and declines to send the message rather than send it insecurely.

A second form of attack is a man-in-the-middle attack where the attacker terminates the TLS connection rather than the intended SMTP server. This is possible when, as is commonly the case, the SMTP client either does not verify the server's certificate or establishes the connection even when the verification fails. REQUIRETLS requires successful certificate validation before sending the message.

Another active attack involves the spoofing of DNS MX records of the recipient domain. An attacker having this capability could cause the message to be redirected to a mail server under the attacker's own control, which would presumably have a valid certificate. REQUIRETLS does not address this attack.

8.3. Bad Actor MTAs

A bad-actor MTA along the message transmission path could misrepresent its support of REQUIRETLS and/or actively strip REQUIRETLS tags from messages it handles. However, since intermediate MTAs are already trusted with the cleartext of messages they handle, and are not part of the threat model for transport-layer security, they are also not part of the threat model for REQUIRETLS.

It should be reemphasized that since SMTP TLS is a transport-layer security protocol, messages sent using REQUIRETLS are not encrypted end-to-end and are visible to MTAs that are part of the message delivery path. Messages containing sensitive information that MTAs should not have access to MUST be sent using end-to-end content encryption such as OpenPGP [RFC4880] or S/MIME [RFC5751].

9. Acknowledgements

The author would like to acknowledge many helpful suggestions on the ietf-smtp and uta mailing lists, in particular those of Viktor Dukhovni, Chris Newman, Tony Finch, Jeremy Harris, Arvel Hathcock, John Klensin, John Levine, Rolf Sonneveld, and Per Thorsheim.

10. Revision History

To be removed by RFC Editor upon publication as an RFC.

10.1. Changes since -03 Draft

Working Group Last Call changes, including:

- Correct reference for SMTP DANE
- Clarify that RequireTLS: NO applies to both MTA-STS and DANE policies
- Correct newly-defined status codes
- Update MTA-STS references to RFC

10.2. Changes since -02 Draft

- More complete documentation for IANA registration requests.
- Changed bounce handling to use RET parameters of RFC 3461, along with slightly more liberal transmission of bounces even if REQUIRETLS can’t be negotiated.

10.3. Changes since -01 Draft

- Converted DEEP references to RFC 8314.
- Removed REQUIRETLS options: CHAIN, DANE, and DNSSEC.
- Editorial corrections, notably making the header field name consistent (RequireTLS rather than Require-TLS).

10.4. Changes since -00 Draft

- Created new header field, Require-TLS, for use by "NO" option.
- Removed "NO" option from SMTP service extension.
- Recommend DEEP requirements for delivery of messages requiring TLS.
- Assorted copy edits

10.5. Changes since fenton-03 Draft

- Wording improvements from Rolf Sonneveld review 22 July 2017
- A few copy edits
- Conversion from individual to UTA WG draft

10.6. Changes Since -02 Draft

- Incorporation of "MAY TLS" functionality as REQUIRETLS=NO per suggestion on UTA WG mailing list.
- Additional guidance on bounce messages

10.7. Changes Since -01 Draft

- Specified retries when multiple MX hosts exist for a given domain.
- Clarified generation of non-delivery messages
- Specified requirements for application of REQUIRETLS to mail forwarders and mailing lists.
- Clarified DNSSEC requirements to include MX lookup only.
- Corrected terminology regarding message retrieval vs. delivery.
- Changed category to standards track.

10.8. Changes Since -00 Draft

- Conversion of REQUIRETLS from an SMTP verb to a MAIL FROM parameter to better associate REQUIRETLS requirements with transmission of individual messages.
- Addition of an option to require DNSSEC lookup of the remote mail server, since this affects the common name of the certificate that is presented.
- Clarified the wording to more clearly state that TLS sessions must be established and not simply that STARTTLS is negotiated.
- Introduced need for minimum encryption standards (key lengths and algorithms)
- Substantially rewritten Security Considerations section

11. References

11.1. Normative References

[MailParams] Internet Assigned Numbers Authority (IANA), "IANA Mail Parameters", 2007, <http://www.iana.org/assignments/mail-parameters>.

[PermMessageHeaderFields] Internet Assigned Numbers Authority (IANA), "Permanent Message Header Field Names Registry", 2004, <https://www.iana.org/assignments/message-headers/message-headers.xhtml#perm-headers>.

[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/info/rfc2119>.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <https://www.rfc-editor.org/info/rfc3207>.

[RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, DOI 10.17487/RFC3461, January 2003, <https://www.rfc-editor.org/info/rfc3461>.

[RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced Mail System Status Codes", BCP 138, RFC 5248, DOI 10.17487/RFC5248, June 2008, <https://www.rfc-editor.org/info/rfc5248>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[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/info/rfc8174>.

[RFC8314] Moore, K. and C. Newman, "Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access", RFC 8314, DOI 10.17487/RFC8314, January 2018, <https://www.rfc-editor.org/info/rfc8314>.

[SMTPStatusCodes] Internet Assigned Numbers Authority (IANA), "Simple Mail Transfer Protocol (SMTP) Enhanced Status Codes Registry", 2008, <http://www.iana.org/assignments/smtp-enhanced-status-codes>.

11.2. Informative References

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, DOI 10.17487/RFC1939, May 1996, <https://www.rfc-editor.org/info/rfc1939>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/info/rfc3501>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/info/rfc5751>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <https://www.rfc-editor.org/info/rfc7672>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

Author’s Address

Jim Fenton
Altmode Networks
Los Altos, California 94024
USA

Email: fenton@bluepopcorn.net