Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 December 2026

A. Brotman
Comcast, Inc

4 June 2026

# Domain-Required TLS
# draft-brotman-drtls-00

## Abstract

A mechanism which allows a domain owner to declare their messages should only be accepted via sessions that employ STARTTLS, and otherwise, delivery options to be interpreted by the evaluating/ receiving system.

## 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 6 December 2026.

Table of Contents

1. Introduction . . . . . 2
2. Terminology . . . . . 2
3. Glossary . . . . . 3
4. Policy Discovery via DNS Record . . . . . 3
5. Record Attributes . . . . . 3
5.1. DNS Record Samples . . . . . 4
6. Receiver Evaluation . . . . . 4
6.1. Requested Policy . . . . . 4
6.2. Multi-message SMTP sessions . . . . . 4
7. Security Considerations . . . . . 4
7.1. RequireTLS . . . . . 4
7.2. Non-Participatory Receivers . . . . . 4
8. Other Considerations . . . . . 4
8.1. Multi-hop Delivery . . . . . 5
8.2. Delivery from Sender . . . . . 5
9. IANA Considerations . . . . . 5
10. Appendix . . . . . 5
11. Informative References . . . . . 5
Author’s Address . . . . . 5

## 1. Introduction

In the email ecosystem, messages are transmitted using best-effort STARTTLS, or Opportunistic TLS [?RFC7435]. This generally works well, though, there’s no assurance that messages will be transmitted securely.

There do exist mechanisms which allow receiving domains some control over the transmission, though both parties must support these (DANE/MTA-STS).

This document defines a mechanism whereby the domain owner can require that email messages are transmitted employing TLS, and otherwise the receiving system should evaluate declared and local policy to determine delivery.

## 2. Terminology

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 [RFC2119].

## 3. Glossary

## 4. Policy Discovery via DNS Record

NOTE: TBD 5321 or 5322 or both. Leaning toward 5322. NOTE: OrgDom (and presumably relying on the PSL) may not be an ideal location, TBD

A receiving system should perform this inspection while the SMTP session is open. This allows the receiving system to create an in-line response.

The receiving system should attempt to find discover the Org Domain (or Apex, or Registered Domain). If the message were use the domain 'example.com' to send the message, the record would be:

_drtls.example.com

And the record lookup would be the same if they had used a sub-domain such as 'e.example.com'.

## 5. Record Attributes

v: This MUST always exist, and the value must always be "DRTLSv1". Failure to do so should be treated as an invalid record, and the record MUST be ignored.

tls: This is the mode by which receivers should adhere. Possible values are (r)equired, OthersTBD.

sdo: Sub-domain override. There are three modes, (n)one, (a)llowed, and (s)pecified. None means that no sub-domains are allowed to override the policy specified. Allowed means that any sub-domain can have its own policy that deviates from the OrgDom. Specified will require another tag to specify the domains allowed to have that override.

sdl: A comma-separated list of domains permitted to have an override. Only applicable when the "sdo" flag has been set to "s".

rp: The domain holder may declare a requested policy. Options are (q)uarantine, (d)efer, (r)eject. Default is 'r'. More information below.

NOTE: I think I would be okay to say that there is no 'rp', only reject.

### 5.1. DNS Record Samples

v=DRTLSv1;tls=r;rp=d;

v=DRTLSv1;tls=r;sdo=s;sdl=foo.example.com,bar.example.com

## 6. Receiver Evaluation

Provided the receiving system can retrieve a valid DNS record for the DRTLS, it should apply this to the inbound message. It is local policy for the receiving system to determine if they would prefer to refuse delivery with a permanent (5xx) or temporary (4xx) code. In either case, the refusal should be clear that the system is unwilling to accept the message due to the DRTLS configuration, and failure to negotiate TLS.

### 6.1. Requested Policy

The ’rp’ flag allows the domain owner to request the receiver use the declared policy when a message that does not adhere to the ’tls’ mode is attempted for delivery. The receiving site MAY choose to ignore the policy and instead use a local policy.

### 6.2. Multi-message SMTP sessions

In the event of a session which attempts to deliver multiple messages, the receiving system should take care to recognize when/if the sending domain changes. Each of these distinct domains may have a separate policy.

## 7. Security Considerations

### 7.1. RequireTLS

RequireTLS [?@RFC8689] does exist, and allows for a similar mechanism, though, it is per-message and declared by the MUA, and requires that the sending domain control all infrastructure that might send on behalf of their domain. This method allows the domain to declare the usage for the entirety of the domain.

### 7.2. Non-Participatory Receivers

If a receiver does not utilize this mechanism, the messages may still be transmitted insecurely. There is nothing the domain owner can do in those cases.

## 8. Other Considerations

### 8.1. Multi-hop Delivery

In the case of a multi-hop delivery, the original sender has no control over how a message is delivered on subsequent hops. Declaring this policy implies an understanding that some of those messages may bounce due to non-TLS delivery attempts.

### 8.2. Delivery from Sender

This could allow for a sending system to refuse to attempt delivery if it knows that TLS will not be attempted or cannot be negotiated. For example, if a bulk sender knows that example.org has declared their desire to only be delivered via STARTTLS, and knows that delivering a message to other-site.com will never properly negotiate TLS, it could refuse delivery before the attempt.

## 9. IANA Considerations

IANA

## 10. Appendix

Appendix

## 11. Informative 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/info/rfc2119>.

## Author’s Address

Alex Brotman
Comcast, Inc
Email: alex_brotman@comcast.com