XEP-0368: SRV records for XMPP over TLS

Travis Burtrum
mailto:travis@burtrum.org
xmpp:travis@burtrum.org

2019-08-20
Version 1.1.0

Status	Type	Short Name
Draft	Standards Track	NOT_YET_ASSIGNED

This specification defines a procedure to look up xmpps-client/xmpps-server SRV records (for direct TLS connections) in addition to xmpp-client/xmpp-server and mix weights/priorities.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF’s Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy> or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1 Introduction

XMPP Core [1] specifies the use of xmpp-client/xmpp-server SRV records as the method of discovering how to connect to an XMPP server. This XEP extends that to include new xmpps-client/xmpps-server SRV records pointing to direct TLS ports and combine priorities and weights as if they were a single SRV record similar to RFC 6186 [2]. It also provides an easy way for clients to bypass restrictive firewalls that only allow HTTPS, for servers to host multiple protocols/services on a single port, and for servers and clients to take advantage of less round trips and existing direct TLS loadbalancers.

2 Glossary

Direct TLS Where TLS is attempted immediately on connect to a TCP socket, like how HTTPS works, not like how STARTTLS works with any protocol.

3 Requirements

The following format for DNS SRV resource records is specified in RFC 2782 [3]:

```
_service._proto.name. TTL class SRV priority weight port target.
```

XMPP Core [4] defines SRV records only where 'service' is 'xmpp-client' and 'xmpp-server'. This document specifies two additionally look up records where 'service' is 'xmpps-client' and 'xmpps-server'. This document specifies that the following additional rules apply:

1. Both 'xmpp-' and 'xmpps-' records SHOULD be treated as the same record with regard to connection order as specified by RFC 2782 [5], in that all priorities and weights are mixed. This enables the server operator to decide if they would rather clients connect with STARTTLS or direct TLS. However, clients MAY choose to prefer one type of connection over the other.
2. Where 'service' starts with 'xmpps-' the client or server MUST connect with direct TLS enabled.
3. Where 'service' starts with 'xmpp-' the client or server MUST NOT connect with direct TLS enabled, connection method is unchanged from XMPP Core [6].

[1] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[2] RFC 6186: Use of SRV Records for Locating Email Submission/Access Services <http://tools.ietf.org/html/rfc6186>.
[3] RFC 2782: A DNS RR for specifying the location of services (DNS SRV) <http://tools.ietf.org/html/rfc2782>.
[4] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[5] RFC 2782: A DNS RR for specifying the location of services (DNS SRV) <http://tools.ietf.org/html/rfc2782>.
[6] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.

4. TLS certificates MUST be validated the same way as for STARTTLS. (i.e., as specified in XMPP Core [7]).
5. STARTTLS MUST NOT be used over direct TLS connections.
6. Client or server MUST set SNI TLS extension to the JID's domain part.
7. Client or server SHOULD set the ALPN (RFC 7301 [8]) TLS extension.
8. When ALPN is used, the ALPN protocol MUST be '**xmpp-client**', where the SRV service is '**xmpps-client**'.
9. When ALPN is used, the ALPN protocol MUST be '**xmpp-server**', where the SRV service is '**xmpps-server**'.

4 Use Cases

For server operators, this provides a way to host multiple services on the same port, especially when SNI or ALPN extensions are used. Servers could even host xmpp-client and xmpp-server services on the same TLS port. For clients, this provides a virtually zero overhead way to bypass restrictive firewalls that only allow HTTP over port 80 and HTTPS over port 443, as XMPP-over-TLS is indistinguishable from HTTP-over-TLS when ALPN is not used. For clients and servers, direct TLS saves round trips vs STARTTLS.

5 Implementation Notes

The only overhead is the single additional SRV lookup. All clients that support STARTTLS already have support for direct TLS.
Server operators should not expect multiplexing (via ALPN) to work in all scenarios and therefore should provide additional SRV record(s) that do not require multiplexing (either standard STARTTLS or dedicated direct XMPP-over-TLS). This is a result of relying on ALPN for multiplexing, where ALPN might not be supported by all devices or may be disabled by a user due to privacy reasons.
If the _xmpps-client (or _xmpps-server) target is set to . (dot), this indicates as per RFC 2782 [9] that the service is not provided for the given domain. In this context, this means that Direct TLS is not supported. In this case, the initiating party SHOULD look up _xmpp-client (or _xmpp-server) records. The initiating party MUST NOT perform A/AAAA fallback as per RFC 6120 [10] (since the service provider has already indicated that the SRV protocol is supported).

[7] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[8] RFC 7301: Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension <https://tools.ietf.org/html/rfc7301>.
[9] RFC 2782: A DNS RR for specifying the location of services (DNS SRV) <http://tools.ietf.org/html/rfc2782>.
[10] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.

6 Security Considerations

Direct TLS provides AT LEAST the same level of security as STARTTLS, and more privacy without ALPN as using STARTTLS leaks that the underlying protocol is XMPP, while any direct TLS stream should be indistinguishable from any other direct TLS stream. Direct TLS provides more security than STARTTLS if RFC 7590 [11] is not followed, as it isn't subject to STARTTLS stripping. All security setup and certificate validation code SHOULD be shared between the STARTTLS and direct TLS logic as well. All SRV-based connection methods are subject to DNS modification/stripping/spoofing of SRV records in the absence of DNSSEC.

7 IANA Considerations

ALPN (RFC 7301 [12]) requires registration of new Protocol IDs. This document specifies two Protocol IDs:
Protocol: XMPP jabber:client namespace Identification Sequence: 0x78 0x6d 0x70 0x70 0x2d 0x63 0x6c 0x69 0x65 0x6e 0x74 ("xmpp-client") Reference: [SRV records for XMPP over TLS (XEP-0368) [13]]
Protocol: XMPP jabber:server namespace Identification Sequence: 0x78 0x6d 0x70 0x70 0x2d 0x73 0x65 0x72 0x76 0x65 0x72 ("xmpp-server") Reference: [SRV records for XMPP over TLS (XEP-0368) [14]]
The ALPN registry is currently located here.
Issues with direct TLS ports mentioned in RFC 2595 [15] Section 7 do not apply here for these reasons:

1. URL scheme is unchanged.
2. "Security" is the same between STARTTLS and direct TLS, and post-2014 the general consensus is that no public XMPP server or client should connect without some form of TLS per the ubiquitous encryption manifesto.
3. A "Use TLS when available" security model is possible here because the client could fall back to standard STARTTLS SRV records if the server administrator supplies them.
4. No port numbers are assigned because SRV allows using arbitrary ports at the server administrator's discretion.

[11] RFC 7590: Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP) <http://tools.ietf.org/html/rfc7590>.
[12] RFC 7301: Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension <https://tools.ietf.org/html/rfc7301>.
[13] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.
[14] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.
[15] RFC 2595: Using TLS with IMAP, POP3 and ACAP <http://tools.ietf.org/html/rfc2595>.

8 XMPP Registrar Considerations

This document requires no interaction with the XMPP Registrar [16].

[16] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.