Network Working Group	J. Hildebrand
Internet-Draft	P. Saint-Andre
Intended status: Standards Track	Cisco
Expires: November 9, 2009	May 08, 2009

TOC

Multiplexing of Connections between Extensible Messaging and Presence Protocol (XMPP) Servers Using Transport Layer Security (TLS)
draft-hildebrand-xmpp-tls-multiplexing-00

Status of this Memo

Copyright Notice

Abstract

This document specifies requirements for multiplexing of connections between Extensible Messaging and Presence Protocol (XMPP) servers using Transport Layer Security (TLS).

Table of Contents

---

1. Problem Statement

TOC

The Extensible Messaging and Presence Protocol (XMPP) has been widely deployed over the Internet since publication of [RFC3920] (Saint-Andre, P., Ed., “Extensible Messaging and Presence Protocol (XMPP): Core,” October 2004.) in 2004. One common deployment scenario is for a hosting provider or application service provider to service multiple domains on the same machine or machines. With the increasing popularity of so-called "cloud computing", some of these providers service thousands of domains. Because RFC 3920 specifies that each domain-to-domain "link" shall use two XML streams (one in each direction) and because currently XMPP has no method by which an existing stream can be re-used for additional domains, establishing connectivity between two XMPP "clouds" can quickly necessitate a large number of TCP connections. This is true even if the clouds have authenticated to each other using Transport Layer Security [TLS] (Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” August 2008.) and the Simple Authentication and Security Layer [SASL] (Melnikov, A. and K. Zeilenga, “Simple Authentication and Security Layer (SASL),” June 2006.) with digital certificates issued by trusted roots. Therefore it would be desirable to define a method by which two XMPP clouds could optionally multiplex communications between themselves, so that an existing domain-to-domain stream could be re-used for additional domains. This document defines requirements for such a method. Possible solutions will be defined in separate specifications, potentially for inclusion into [rfc3920bis] (Saint-Andre, P., “Extensible Messaging and Presence Protocol (XMPP): Core,” March 2009.).

---

2. Requirements

TOC

We stipulate the following requirements for server-to-server multiplexing in XMPP:

*The multiplexing method must be backwards-compatible with existing server-to-server connection methods.

*A party that supports multiplexing must also support bidirectional XML streams.

*Each party to a server-to-server communication must be able to determine if the other party supports multiplexing.

*If the addition of a new domain to an existing domain-to-domain stream fails, the existing stream must not be terminated, and the adding party may attempt to add the new domain again.

*Multiplexing shall depend on presentation of a valid digital certificate for the multiplexed domain.

*The certificate for a multiplexed domain should not be same (i.e., have the same subject) as a certificate that has previously been accepted for the stream; however, if it is the same then it shall replace the previous certificate with the same subject (e.g., to present a new certificate with a different expiry time).

*When a multiplexed domain is accepted for the stream, each name on the certificate (e.g., id-on-dnsSRV or id-on-xmppAddr) becomes valid for this stream.

*The protocol for accepting the initial certificate for a stream may be different from the protocol for accepting subsequent ("multiplexed") certificates for the stream.

*The process of adding a subsequent domain shall not affect transmission of application data over the stream.

*If the stream is resumed, all of the certificates that were accepted for the previous session apply to the resumed session.

*It is a security violation to proceed with transmission of application between two domains if multiplexing for those domains failed. It is acceptable for the party that receives such applicatino data to terminate the stream.

*It must be possible to remove a domain from the stream.

TOC

3. Security Considerations

The requirements in this memo are intended to provide guidance regarding solutions to the problem of securely multiplexing domain-to-domain XMPP communications over a single XML stream.

---

4. References

TOC

4.1. Normative References

TOC

[RFC3920]	Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core," RFC 3920, October 2004 (TXT, HTML, XML).
[TLS]	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008 (TXT).

4.2. Informative References

TOC

[rfc3920bis]	Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core," draft-saintandre-rfc3920bis-09 (work in progress), March 2009 (TXT).
[SASL]	Melnikov, A. and K. Zeilenga, "Simple Authentication and Security Layer (SASL)," RFC 4422, June 2006 (TXT).

Appendix A. Copying Conditions

TOC

Authors' Addresses

TOC

	Joe Hildebrand
	Cisco
Email:	jhildebr@cisco.com
	Peter Saint-Andre
	Cisco
Email:	psaintan@cisco.com