TRAM
Internet-Draft
Intended status: Informational
Expires: May 29, 2015

P. Patil
T. Reddy
G. Salgueiro
Cisco
M. Petit-Huguenin
Impedance Mismatch
November 25, 2014

Application Layer Protocol Negotiation (ALPN) Labels for Session Traversal Utilities for NAT (STUN) Usages
draft-ietf-tram-alpn-08

Abstract

Application Layer Protocol Negotiation (ALPN) labels for Session Traversal Utilities for NAT (STUN) usages, such as Traversal Using Relays around NAT (TURN) and NAT discovery, are defined in this document to allow an application layer to negotiate STUN usages within the Transport Layer Security (TLS) connection. ALPN protocol identifiers defined in this document apply to both TLS and Datagram Transport Layer Security (DTLS).

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 http://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 May 29, 2015.

Table of Contents

1. Introduction

STUN can be securely transported using TLS-over-TCP (referred to as TLS [RFC5246]), as specified in [RFC5389], or TLS-over-UDP (referred to as DTLS [RFC6347]), as specified in [RFC7350].

ALPN [RFC7301] enables an endpoint to positively identify an application protocol in TLS/DTLS and distinguish it from other TLS/DTLS protocols. With ALPN, the client sends the list of supported application protocols as part of the TLS/DTLS ClientHello message. The server chooses a protocol and sends the selected protocol as part of the TLS/DTLS ServerHello message. Application protocol negotiation can thus be accomplished within the TLS/DTLS handshake, without adding network round-trips.

STUN protocol usages, such as TURN [RFC5766], can be used to identify the purpose of a flow without initiating a session.

This document proposes the following ALPN labels to identify STUN protocol [RFC5389] usages.

'stun.turn': Label to identify the specific use of STUN over (D)TLS for TURN (Section 4.6 of [RFC7350]).

'stun.nat-discovery': Label to identify the specific use of STUN over (D)TLS for NAT discovery (Section 4.1 of [RFC7350]).

2. IANA Considerations

The following entries are to be added to the "Application Layer Protocol Negotiation (ALPN) Protocol IDs" registry established by [RFC7301].

The "stun.turn" label identifies the use of TURN usage (D)TLS:

Protocol: Traversal Using Relays around NAT (TURN)

Identification Sequence: 0x73 0x74 0x75 0x6E 0x2E 0x74 0x75 0x72 0x6E ("stun.turn")

Specification: This document (RFCXXXX)

The "stun.nat-discovery" label identifies the use of STUN for the purposes of NAT discovery over (D)TLS:

Protocol: NAT discovery using Session Traversal Utilities for NAT (STUN)

Identification Sequence: 0x73 0x74 0x75 0x6E 0x2E 0x6e 0x61 0x74 0x2d 0x64 0x69 0x73 0x63 0x6f 0x76 0x65 0x72 0x79 ("stun.nat-discovery")

Specification: This document (RFCXXXX)

3. Security Considerations

The ALPN STUN protocol identifier does not introduce any specific security considerations beyond those detailed in the TLS ALPN Extension specification [RFC7301]. It also does not impact security of TLS/DTLS session establishment nor application data exchange.

4. Acknowledgements

This work benefited from the discussions and invaluable input by the various members of the TRAM working group. These include Simon Perrault, Paul Kyzivat, Brandon Williams and Andrew Hutton. Special thanks to Martin Thomson and Oleg Moskalenko for their constructive comments, suggestions, and early reviews that were critical to the formulation and refinement of this document.

Barry Leiba, Stephen Farrell, Adrian Farrel and Richard Barnes provided useful feedback during IESG review. Thanks to Russ Housley for his Gen-ART review and Adam Langley for his IETF LC review comments as TLS expert.

The authors would also like to express their gratitude to the TRAM WG chairs Gonzalo Camarillo and especially Simon Perrault, who also acted as document shepherd. Lastly, we also want to thank Transport Area Director Spencer Dawkins for his support and careful reviews.

5. References

5.1. Normative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, July 2014.

[RFC7350] Petit-Huguenin, M. and G. Salgueiro, "Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN)", RFC 7350, August 2014.

5.2. Informative References

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, April 2010.

Authors' Addresses

Prashanth Patil
Cisco Systems, Inc.
Bangalore
India

Email: praspati@cisco.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tireddy@cisco.com

Gonzalo Salgueiro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com

Marc Petit-Huguenin
Impedance Mismatch
USA

Email: marc@petit-huguenin.org