

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

P. Patil
T. Reddy
G. Salgueiro
Cisco
October 26, 2014

Traversal Using Relays around NAT (TURN) Server Selection
draft-patil-tram-turn-serv-selection-00

Abstract

A TURN client may discover multiple TURN servers. In such a case, there are no guidelines that a client can follow to choose or prefer a particular TURN server among those discovered. This document details selection criteria, as guidelines, that can be used by a client to perform an informed TURN server selection decision.

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 April 29, 2015.

Copyright Notice

Copyright (c) 2014 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 (<http://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	2
2. Terminology	3
3. TURN Server Selection Criteria	3
3.1. Local Configuration	3
3.2. Security	3
3.2.1. Location Privacy	4
3.2.2. Authentication	4
3.3. User Experience	5
3.4. Interface	5
3.5. Mobility Support	5
4. Security Considerations	5
5. Acknowledgements	5
6. References	5
6.1. Normative References	6
6.2. Informative References	6
Authors' Addresses	7

1. Introduction

Using any of the discovery mechanisms described in [I-D.ietf-tram-turn-server-discovery], a client may discover multiple Traversal Using Relays around NAT (TURN) servers. The TURN servers discovered could be provided by an enterprise network, an access network, an application service provider or a third party provider. Therefore, the client needs to be able to choose a TURN server that best suits its needs.

Selection criteria could be based on parameters such as:

- o Security
- o Location Privacy
- o Authentication
- o User Experience
- o Interface Selection (if the client is multi-interfaced)
- o Mobility Support

This document describes procedures that a client can use to choose the most appropriate TURN server based on any one or more

combinations of the above parameters. A client could also use the aforementioned selection criteria to prioritize the discovered TURN servers based on these parameters if backup servers are implemented for added resiliency and robustness.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. TURN Server Selection Criteria

The accessibility of possible TURN servers SHOULD be tested and verified prior to beginning Interactive Connectivity Establishment (ICE) [RFC5245]. Any TURN servers that fail such accessibility tests (including credentials verification) SHOULD be excluded. These early tests are an often an optimal opportunity to calculate performance metrics, such as the round-trip time (RTT), that might be used as TURN server prioritization factors, as discussed in Section 3.3. Throughout the lifetime of the application, it is RECOMMENDED to periodically test the entire selection list, in case better TURN servers suddenly appear or connectivity to others is unexpectedly lost.

The parameters described in this Section are intended as TURN server selection criteria or as weighting factors for TURN server prioritization.

3.1. Local Configuration

Local or manual configuration takes precedence for TURN server selection. A client could be configured with an explicit preferred list of TURN servers. Local configuration could list servers in order of preference. For example, a TURN client could opt for a TURN server offered by the Enterprise and fall back to a TURN server offered by the Internet Service Provider (ISP) or a cloud service if the Enterprise TURN server wasn't available.

An implementation MAY give the user an opportunity (e.g., by means of configuration file options or menu items) to specify this preference.

3.2. Security

If a TURN client wants security for its connections, it should opt for a TURN server that supports the usage of Transport Layer Security (TLS) [RFC5246] and Datagram Transport Layer Security (DTLS) [RFC6347] as a transport protocol for Session Traversal Utilities for

NAT (STUN), as defined in [RFC5389] and [RFC7350]. If multiple servers offer this support, the client could use Location Privacy (Section 3.2.1) and Authentication (Section 3.2.2) criteria to determine which among the list is most suitable.

The need for security depends on the type of connected network (i.e., whether the host is connected to a home network versus an Enterprise network versus a coffee shop network). It is recommended that a client always choose security, but this condition could vary depending on the degree of trust with the connected network.

3.2.1. Location Privacy

In addition to security, a TURN client may require additional location privacy from an external peer.

Scenario 1: A client may not wish to use a TURN server in its Enterprise or access network because the client location could be determined by the external peer. In such a case, the client may choose to use a distributed multi-tenant or a cloud-based TURN server that can provide privacy by obscuring the network from which the client is communicating with the remote peer.

Scenario 2: A TURN client that desires to perform Scenario 1, but cannot because of firewall policy that forces the client to pick Enterprise-provided TURN server for external communication, can use TURN-in-TURN through the enterprise's TURN server as described in [I-D.schwartz-rtcweb-return].

Location privacy may not be critical if the client attempts to communicate with a peer within the same domain.

3.2.2. Authentication

A TURN client should prefer a TURN server whose authenticity can be ascertained. A simple certificate trust chain validation during the process of (D)TLS handshake should be able to validate the server.

A TURN client could also be pre-configured with the names of trusted TURN servers. When connecting to a TURN server, a TURN client should start with verifying that the TURN server name matches the pre-configured list of TURN servers, and finally validating its certificate trust chain. For TURN servers that don't have a certificate trust chain, the configured list of TURN servers can contain the certificate fingerprint of the TURN server (i.e., a simple whitelist of name and certificate fingerprint).

DNS-based Authentication of Named Entities (DANE) can also be used to validate the certificate presented by TURN server as described in [I-D.petithuguenin-tram-stun-dane].

3.3. User Experience

All else being equal (or if a TURN client is able to converge on a set of TURN servers based on parameters described in Section 3.2), a TURN client should choose a TURN server that provides the best user experience at that point in time (based on factors such as RTT, real-time clock (RTC), etc).

If using ICE regular nomination, ICE connectivity check round-trip time can influence the selection amongst the valid pairs. This way a candidate pair with relayed candidate could be selected even if it has lower-priority than other valid pairs.

3.4. Interface

With a multi-interfaced node, selection of the correct interface and source address is often crucial. How to select an interface and IP address family is out of scope for this document. A client could account for the provisioning domain described in [I-D.ietf-mif-mpvd-arch] to determine which interface to choose.

3.5. Mobility Support

If a TURN client is aware that the host is mobile, and all other parameters being equal, the client SHOULD choose a TURN server that supports mobility [I-D.wing-tram-turn-mobility].

4. Security Considerations

This document does not itself introduce security issues, rather it merely presents best practices for TURN server selection. Security considerations described in [RFC5766] are applicable to for all TURN usage.

5. Acknowledgements

The authors would like to thank Dan Wing, Marc Petit-Huguenin for their review and valuable comments.

6. References

6.1. Normative References

- [I-D.ietf-mif-mpvd-arch]
Anipko, D., "Multiple Provisioning Domain Architecture", draft-ietf-mif-mpvd-arch-07 (work in progress), October 2014.
- [I-D.ietf-tram-turn-server-discovery]
Patil, P., Reddy, T., and D. Wing, "TURN Server Auto Discovery", draft-ietf-tram-turn-server-discovery-00 (work in progress), July 2014.
- [I-D.petithuguenin-tram-stun-dane]
Petit-Huguenin, M. and G. Salgueiro, "Using DNS-based Authentication of Named Entities (DANE) to validate TLS certificates for the Session Traversal Utilities for NAT (STUN) protocol", draft-petithuguenin-tram-stun-dane-02 (work in progress), October 2014.
- [I-D.schwartz-rtcweb-return]
Schwartz, B., "Recursively Encapsulated TURN (RETURN) for Connectivity and Privacy in WebRTC", draft-schwartz-rtcweb-return-03 (work in progress), September 2014.
- [I-D.wing-tram-turn-mobility]
Wing, D., Patil, P., Reddy, T., and P. Martinsen, "Mobility with TURN", draft-wing-tram-turn-mobility-02 (work in progress), September 2014.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [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.
- [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.

6.2. Informative References

- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

- [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.

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: tiredy@cisco.com

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

Email: gsalguei@cisco.com