DECLARATION

I, Alexa Morris, based on my personal knowledge and information, hereby declare as follows:

1. I am Executive Director of the Internet Engineering Task Force ("IETF") and have held this position since January 1, 2008.
2. Among my responsibilities as Executive Director, I act as the custodian of Internet-Drafts for the IETF and records relating to Internet-Drafts. I am familiar with the record keeping practices relating to Internet-Drafts, including the creation and maintenance of such records.
3. I make this declaration based on my personal knowledge and information contained in the business records of the IETF, or confirmation with other responsible IETF personnel with such knowledge.
4. Since 1998, it has been the regular practice of the IETF to publish Internet-Drafts and make them available to the public on its website at www.ietf.org (the IETF website). The IETF maintains copies of Internet-Drafts in the ordinary course of its regularly conducted activities.
5. Any Internet-Draft published on the IETF website was reasonably accessible to the public and was disseminated or otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence could have located it. In particular, the Internet-Drafts were indexed and searchable on the IETF website.
6. Internet-Drafts are posted to an IETF online directory. When an Internet-Draft is published, an announcement of its publication that describes the Internet-Draft is disseminated. Typically, that dated announcement is made within 24 hours of the

publication of the Internet-Draft. The announcement is kept in the IETF email archive and the date is affixed automatically.

7. The records of posting the Internet-Drafts in the IETF online repository are kept in the course of the IETF's regularly conducted activity and ordinary course of business. The records are made pursuant to established procedures and are relied upon by the IETF in the performance of its functions.

8. It is the regular practice of the IETF to make and keep the records in the online repository.

9. Exhibit 1 is a true and correct copy of draft-rosenberg-midcom-turn-00, titled "Traversal Using Relay NAT (TURN)." The Internet-Draft shows that an announcement of its publication was made on November 14, 2001.

Pursuant to Section 1746 of Title 28 of United States Code, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that the foregoing is based upon personal knowledge and information and is believed to be true.

Date: Sept 19, 2018 By: [signature]

Alexa Morris

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT **CIVIL CODE § 1189**

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California)
County of Santa Clara)

On Sept. 19th, 2018 before me, Sharon J. Chai, Notary Public,
Date — *Here Insert Name and Title of the Officer*

personally appeared Alexa Morris
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that ~~he~~/she/~~they~~ executed the same in ~~his~~/her/~~their~~ authorized capacity~~(ies)~~, and that by ~~his~~/her/~~their~~ signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature [signature]
Signature of Notary Public

SHARON J. CHAI
Notary Public – California
Santa Clara County
Commission # 2224197
My Comm. Expires Jan 3, 2022

Place Notary Seal Above

OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: Declaration
Document Date: 09-19-18 Number of Pages: 2
Signer(s) Other Than Named Above: n/a

Capacity(ies) Claimed by Signer(s)

Signer's Name: Alexa Morris
☐ Corporate Officer — Title(s):
☐ Partner — ☐ Limited ☐ General
☑ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other:
Signer Is Representing: herself

Signer's Name:
☐ Corporate Officer — Title(s):
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other:
Signer Is Representing:

Internet Engineering Task Force MIDCOM WG
Internet Draft Rosenberg,Weinberger,Huitema,Mahy
draft-rosenberg-midcom-turn-00.txt dynamicsoft,Microsoft,Cisco
November 14, 2001
Expires: March 2002

Traversal Using Relay NAT (TURN)

Abstract

Traversal Using Relay NAT (TURN) is a simple protocol that allows for an element behind a NAT or firewall to receive incoming data over TCP or UDP connections. It is most useful for elements behind symmetric NATs or firewalls that wish to be on the receiving end of a connection to a single peer. TURN does not allow for users to run servers on well known ports if they are behind a nat; it supports the connection of a user behind a nat to only a single peer. In that regard, its role is to provide the same security functions provided by symmetric NATs and firewalls, but to "turn" the tables so that the element on the inside can be on the receiving end, rather than the sending end, of a connection that is requested by the client.

1 Introduction

Network Address Translators (NATs), while providing many benefits, also come with many drawbacks. The most troublesome of those drawbacks is the fact that they break many existing IP applications, and make it difficult to deploy new ones. Guidlines have been developed [1] that describe how to build "NAT friendly" protocols, but many protocols simply cannot be constructed according to those guidelines. Examples of such protocols include almost all peer-to-peer protocols, for example.

To handle this, we have documented the Simple Traversal of UDP Through NAT (STUN) protocol [2], which allows for clients behind a NAT to discover the presence of the NAT, and then to allocate an address that is useful for receiving data in the case where they are behind a full-cone or restricted-cone NAT. However, it is acknowledged in that draft that while STUN allows a client to discover that its behind a symmetric NAT, it provides no assistance in traversing symmetric NATs.

This protocol serves as a complement to STUN, handling the case where the user is behind a symmetric NAT. It allows a client to request an IP address and port that it can receive data on from any other host on the Internet. This is accomplished using a server in the service provider cloud, known as a TURN server. When a host on the Internet sends to this IP address and port, the TURN server creates an association between the two. The client behind the NAT will receive this, and any other subsequent data from that host. In addition, the client behind the NAT can send data, and that data will be forwarded by the TURN server to the host which connected. TURN servers purposefully support a single association, so that only a single host can be connected using the IP address and port provided by the turn server. This assures that TURN can't be used to violate the policy that symmetric NAT and firewalls are meant to enforce. All TURN does is allow a client to communicate with a single peer whose address it doesn't know ahead of time. TURN is not a tunneling protocol, and therefore does not allow for a user to send and receive UDP, if, for example, the firewall policy prohibits the usage of UDP. Effectively, a TURN server is a NAT function at the UDP and TCP layer, and thus the name of the protocol - its a "relay NAT".

2 Do we need this Protocol?

Originally, the TURN protocol was integrated with the STUN protocol documented in [2]. The authors yanked it out of that document because it solves a sufficiently different problem, with differing requirements. We also observed that there are many other potential solutions for the symmetric case, including RSIP [3] [4], and more traditional VPN tunnels. We therefore had to ask ourselves why another solution was needed in this space. Here are some of the

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase® Smarter legal research.