Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: September 22, 2018

L. Song
Beijing Internet Institute
P. Vixie
TISF
S. Kerr
March 21, 2018

An Proxy Use Case of DNS over HTTPS
draft-ietf-dnsop-dns-wireformat-http-02

Abstract

This memo introduces a DNS proxy use case to tunnel DNS query and response over HTTPs using DOH, a newly proposed DNS transport. This is useful in some situation where DNS is not working properly and DOH is not widely available for many stub-resolvers.

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 https://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 September 22, 2018.

Copyright Notice

Table of Contents

1. Introduction

RFC 1035 [RFC1035] specifies the wire format for DNS messages. It also specifies DNS transport on UDP and TCP on port 53, which is still used today. To enhance the availability of honest DNS, a new DNS transport DOH is proposed which transport DNS over HTTPs [I-D.ietf-doh-dns-over-https], in a way to cure DNS's long-time suffering from on-path attack by spoofing and blocking.

This memo introduces a DNS proxy use case to leverage the DOH protocol as a substrate to tunnel DNS data over HTTPs which is called called DOH proxy in the rest of the document. It is useful especially when most DNS stub-resolvers and servers are not aware the new DOH protocol, but a public or private proxy using DOH can be deployed and offer DOH capacity to users to bypass the networks where DNS is not working properly.

Just as a normal DNS proxy described in [RFC5625], DOH proxy works as a simple DNS forwarder keeping the transparency principle, so any "hop-by-hop" mechanisms or newly introduced protocol extensions operate as if the proxy were not there. The only difference is DOH proxy consist two part, a proxy client as a initiator of DOH tunnel and a proxy server as a terminator.

In order to keep the transparency of DOH proxy, a new media type is required in DOH proxy use case to allow the proxy client and proxy server use the same transport (UDP or TCP) connecting sub-resolver and far-end server.

May REMOVE BEFORE PUBLICATION: Comparing using a general VPN, the DOH proxy can work on an actual HTTP server, so it can be hosted on a machine that also serves web pages. This means that DNS over HTTP is slightly more "stealthy" than a VPN, in that it can be indistinguishable from normal web traffic.

2. Use case description

As mentioned in introduction, DOH proxy is a special use case to provide to end users with better DNS availability by leveraging the DOH protocol. The proxy client and proxy server speak DOH which served as a tunnel for DNS query and response.

The typical scenario is that a DOH proxy sitting between stub-resolver and the recursive server. The stub-resolver is configured sending DNS query to a proxy client and expected reply from the same proxy client. If proxy client receives the query via UDP, then it will carry the media type "application/dns-udpwireformat" in the HTTP request and includes the DNS query as the message body as defined in DOH protocol. If proxy client receives the query via TCP, then it will carry a new media type defined in this document "application/dns-tcpwireformat" and speak DOH with proxy server with the same DNS query without the two-byte length field defined in DNS over TCP [section 4.2.2 in [RFC1035]].

The proxy server MUST be able to process both "application/dns-udpwireformat" and "application/dns-tcpwireformat" request messages and forward the query to a configured recursive server using the same transport between sub-resolver and proxy client. The response will be delivered back to sub-resolver accordingly. In DOH proxy use case, each DNS query-response pair is mapped into a DOH query-response pair. And the transport for DNS query and response MUST be the same.

It is possible that a proxy client as a module can be deployed in the same host with the sub-client listening to a loop-back address. A proxy server can be implemented that way to host a recursive DNS process as well. The can be combined to form four deployment scenarios of DOH proxy use case.

It is also possible to use the proxy server as a regular web server at the same time that is acting as a proxy server.

Note that the proxy client will face the same bootstrapping problem described in DOH when the HTTPs request needs to resolve the name of server and send the request to on IP address. The strategy is either use the IP directly or use another resolver (like the normal DHCP-supplied resolver) to lookup the IP of the server.

3. Security Considerations

The DOH proxy use case does not introduce new protocol and any new security considerations since it is built on the DNS over HTTPS

protocols. All security considerations and recommendations apply in DOH proxy use case.

Since DOH proxy is a also a special DNS proxy, the security recommendations of DNS proxy RFC 5625 [RFC5625] also apply in DOH proxy use case.

Note that the ability to perform DNS queries in this way may allow users to bypass local DNS policy. This may be problematic in any environment where administrators need to enforce specific DNS behavior, such as an enterprise environment. The protocol outlined here does not introduce any new capabilities in this area, but by creating a more standardized way of doing this it may cause operational problems for enterprise administrators.

4. IANA considerations

4.1. Registration of application/dns-tcpwireformat Media Type

To: ietf-types@iana.org
Subject: Registration of MIME media type
application/dns-tcpwireformat

MIME media type name: application

MIME subtype name: dns-tcpwireformat

Required parameters: n/a

Optional parameters: n/a

Encoding considerations: This is a binary format. The contents are a DNS message as defined in RFC 1035. The format used here is for DNS over UDP, which is the format defined in the diagrams in RFC 1035.

Security considerations: The security considerations for carrying this data are the same for carrying DNS without encryption.

Interoperability considerations: None.

Published specification: This document.

Applications that use this media type:
Systems that want to ship DNS messages via HTTP.

Additional information:

Magic number(s): n/a

File extension(s): n/a

Macintosh file type code(s): n/a

Person & email address to contact for further information:
Linjian Song, songlinjian@gmail.com

Intended usage: COMMON

Restrictions on usage: n/a

Author: Linjian Song, songlinjian@gmail.com

Change controller: IESG

5. Acknowledgments

Thanks to Bob Harold, Paul Hoffman, Julian Reschke, and Erik Kline for review.

6. References

[I-D.ietf-doh-dns-over-https]
Hoffman, P. and P. McManus, "DNS Queries over HTTPS", draft-ietf-doh-dns-over-https-03 (work in progress), February 2018.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <https://www.rfc-editor.org/info/rfc5625>.

Authors' Addresses

Linjian Song
Beijing Internet Institute
2nd Floor, Building 5, No.58 Jing Hai Wu Lu, BDA
Beijing 100176
P. R. China

Email: songlinjian@gmail.com
URI: http://www.biigroup.com/

Paul Vixie
TISF
11400 La Honda Road
Woodside, California 94062
US

Email: vixie@tisf.net
URI: http://www.redbarn.org/

Shane Kerr
Antoon Coolenlaan 41
Uithoorn 1422 GN
NL

Email: shane@time-travellers.org