Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: January 3, 2019

L. Song
Beijing Internet Institute
P. Vixie
TISF
S. Kerr
July 2, 2018

An Proxy Use Case of DNS over HTTPS
draft-ietf-dnsop-dns-wireformat-http-03

Abstract

This memo introduces a DNS proxy use case to tunnel DNS query and response using DNS over HTTPs (DOH) protocol, a newly proposed DNS transport. The proxy use case is useful as a incremental adoption tool when DOH is not widely available in old-transport client and server.

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 January 3, 2019.

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: DNS over HTTPs (DOH) [I-D.ietf-doh-dns-over-https] is proposed which transport 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 DOH proxy in the rest of the document. It is useful especially when most DNS stub-resolvers and far-end 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.

In order to keep the transparency of DOH proxy, a new variable "proto" in URI Template is defined for DOH proxy use case. It allows the proxy server use the same transport protocol (UDP or TCP) to forward DNS query to far-end server just as the stub-client does without DOH proxy.

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

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 DOH proxy and expects reply from the same DOH proxy . Just as a normal DNS proxy described in [RFC5625], DOH proxy works as a simple DNS forwarder keeping the transparency principle. 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. The proxy client speaks DOH with proxy server carrying the same DNS query received from stub-resolver.The proxy server will forward the exact DNS query received from stub-resolver to the configued recursive server.

To keep the transparency principle of DOH proxy, any "hop-by-hop" mechanisms or newly introduced protocol extensions operate as if the DOH proxy were not there. Different from the native DOH protocol, in DOH proxy use case, there should be a indication introduced for proxy client to tell the proxy server original transport (UDP or TCP) the stub-resolver uses to send DNS query to proxy client.

For example if the proxy client receives the query via UDP, then it will notify the proxy server with a "proto=udp" indicator which is defined in Section 3. If proxy client receives the query via TCP, then it will carry a "proto=tcp" indicator with the same DNS query without the two-byte length field defined in DNS over TCP [section 4.2.2 in [RFC1035]].

Besides the original transport indicator, as specified in DOH document, the proxy server MUST be able to process both "application/ dns-message"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. Original transport indicator in DOH proxy

In DOH document[I-D.ietf-doh-dns-over-https], the HTTP request uses a URI defined by the DOH server through the use of a URI Template in which no variables is defined. In this document, a new variable "proto" is defined as the indicator of original transport. For example, The URI "https://example.com/proxy_dns?proto=tcp" will cause the server to make a request using TCP. And the URL "https://example.com/proxy_dns?proto=udp" will cause the server to make a request using UDP.

4. Implementation considerations

The DOH proxy may return TC bit to the sub-resolver which will cause TCP fallback starting from the sub-resolver. An alternative advised is that the proxy has to have sufficient smarts to recognize the returned TC bit and re-issue the request over TCP to the back-end DNS server.

Another implementation is suggested that DOH proxy server has a pool of TCP connections from the proxy to the back-end DNS server(s), over which incoming requests can be multiplexed.

5. 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.

6. IANA considerations

No IANA considerations for DOH proxy

7. Acknowledgments

Thanks to Bob Harold, Paul Hoffman, Julian Reschke, Martin Thomson, Tony Finch ,Ray Bellis and Erik Kline for their review and comments.

8. References

[I-D.ietf-doh-dns-over-https]
Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", draft-ietf-doh-dns-over-https-12 (work in progress), June 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