Network Working Group
Internet-Draft
Expires: December 3, 2021

R. Kobayashi
Hyogo Prefectural Ono High School

June 1, 2021

Effective DNS Service
draft-rintaro-eds-00

Abstract

In DNS Queries over HTTPS [RFC8484], the port that communicates with DNS would change from UDP to TCP 443. This change causes a new problem that makes it difficult to identify which is the name resolution request, so it is difficult to use web filtering, parental controls and so on. Furthermore, a user-agent in a HTTP header that is necessary for HTTPS communications could be a data used to track users. In summary, DNS Queries over HTTPS has some problems that affect users' security and privacy. This draft proposes a system that is set mediation servers between client side and DNS servers. With this proposal, it is expected that those two problems will be solved.

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 December 3, 2021.

Copyright Notice

Table of Contents

1. Introduction

In Effective DNS Service, there is a new server that mediates between client side and DNS servers. Between client side and mediation servers (hereinafter called EDS server) is HTTPS encryption. The FQDN posted from client side is analyzed in an EDS server. After analyzing in the EDS server, when the FQDN posted from client side is matched with the FQDN that is blacklisted, EDS server does not send a DNS request, and is returned to client side with a 403 Error and error messages. If the FQDN is not blacklisted, EDS server starts to communicate with the EDS server by using DNS over HTTPS. In consequence, we can set web filtering by using EDS. Moreover, it is impossible to track user by user-agent because all EDS servers use the same user-agent.

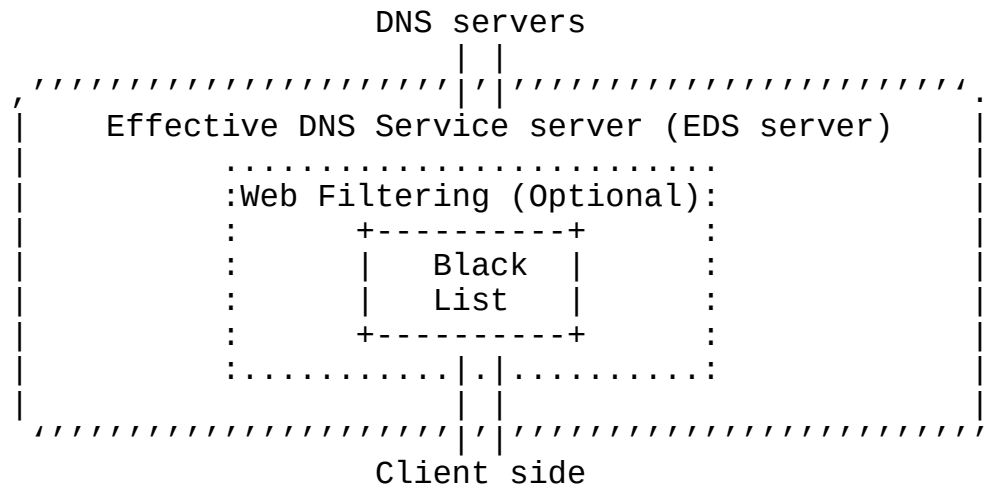
1.1. Terminology

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].

Many of the specialized terms used in this specification are defined in DNS Terminology [RFC7719].

2. Proposed Solution

2.1. The structure of Effective DNS Service



We can realize fast Internet connections because the number of servers is not limited. I accessed the local DNS server and measured the response time by using w/- - write-out. The total response time was 0.2 sec. However, the total response time of the Heroku server in the United States was 1.2 sec. Therefore, the response time is dependant on the location of the EDS server, so EDS servers need to be dispersed widely across the world.

2.2. Web filtering

I tested the web-filtering feature in EDS. First, I created an array that has FQDN needs to block. This array is as a blacklist. Second, when the FQDN is posted from client side, check whether the FQDN is blacklisted or not. Then, make a judgement on starting communication with DNS server or returning a 403 Error.

```
//Node.js v14
//[example: web filtering black list]
 const blacklist = ["www.example.com", "www.rintaro.tech"]
 if (blacklist.includes(FQDN) == false) {
 res.send(kakunouko);
 console.log(kakunouko);
 }else{
 res.status(403);
 res.send({code: 403, error: "EDS sever blocked DNS request because
           the FQDN was blacklisted."})
 console.log(403)
```

3. Additional Considerations

3.1. Safety EDS and Third-party EDS

EDS server should be a distributed system and EDS servers should be set in many countries. These EDS servers are managed by a professional organization directly, and being officially certified by this organization as "Safety EDS". The closest EDS server is set as the default EDS server on browsers, and Safety EDS servers are secured by the organization. By protecting some EDS servers with an official organization, we can assure users' security. To stand up to the crush of demand, all EDS servers are based on AnyCast. In addition to Safety EDS, users can create independent EDS servers as "Third-party EDS". Every EDS server must have "EDS certificate" for a safe connection.

3.2. EDS Certification system

There are two institutions: PA and CA that manage EDS certification. An owner applies for certification to PA, and PA also applies it to CA. CA will issue the certification, and they store it in a repository. The users check the server's certification, and verify the validity by using the repository. By these structures that is similar to SSL certification, we can run this system much more safely.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

Effective DNS Service also uses HTTPS. This mitigates classic amplification attacks for UDP-based DNS. [RFC8484]

About Third-party EDS, the security of connection will be depend on owners' skills. If these servers are for an unspecified large number of people, the feature that users can report the server to a certification organization will be needed.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 7719, DOI 10.17487/RFC7719, December 2015, <https://www.rfc-editor.org/info/rfc7719>.

6.2. Informative References

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

Author’s Address

Rintaro Kobayashi
Hyogo Prefectural Ono High School
518 Nishihommachi-cho
Ono city, Hyogo 6751375
Japan

Email: k.rintaro1@icloud.com
URI: https://www.rintaro.tech