Workgroup: DNSOP WG
Internet-Draft:
draft-wing-dnsop-structured-dns-error-page-00
Published: 9 July 2021
Intended Status: Standards Track
Expires: 10 January 2022
Authors: D. Wing T. Reddy N. Cook M. Boucadair
Citrix McAfee Open-Xchange Orange

Structured Data for DNS Access Denied Error Page

Abstract

It can be valuable to communicate computer-parsable details about DNS filtering to assist troubleshooting and problem resolution. This document describes structured data to provide these details.

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 10 January 2022.

Table of Contents

1. Introduction

DNS clients using services which perform filtering may wish to receive more information about such filtering and the reason for that filtering. To this end, Extended DNS Error Codes [RFC8914] provide information about when different types of filtering have occurred, and DNS Access Denied Error Page [I-D.reddy-dnsop-error-page] provides a URI to give further information to the end-user about the reasons for the filtering. However, the latter draft assumes a client with a user-interface that can display a web page to the end-user, whereas many clients may in fact be "headless", i.e., acting on behalf of other network elements; such clients can include DNS forwarders and proxies. Such clients cannot make use of a web-page designed for presentation to an end-user, but may instead be able to make use of structured data. This draft provides a mechanism for such clients to request and receive structured data from the URI returned by the DNS Access Denied Error Page mechanism.

When a third party provides DNS filtering, there are deployments where disclosing that third party to the host (which originated the DNS query) is desirable but other deployments where such disclosure is not desired. For example, the IT organization might contract filtering to a third party but want trouble-tickets from employees to be handled by IT, rather than having employees interact directly with the third party. As another example, all the employees at a small business or all the members of a household might be informed of the third party so they can troubleshoot filtering with that third party directly.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

This document makes use of the terms defined in [RFC8499].

'Encrypted DNS' refers to any encrypted scheme to convey DNS messages, for example, DNS-over-HTTPS [RFC8484], DNS-over-TLS [RFC7858], or DNS-over-QUIC [I-D.ietf-dprive-dnsoquic].

3. Structured Data

To receive structured DNS error page data, the client MUST query the Error Page URI returned in [I-D.reddy-dnsop-error-page] with Content-Type set to "application/json+structured-dns-error". The JSON has one top-level name, "responsible", containing an array of dictionaries for each party responsible for this particular DNS filter. An array of responsible parties are possible in deployment scenarios where two or more entities are involved in a DNS filtering (the filtering may be for the same or distinct reasons by each involved DNS filter service). The content of the array is structured are as follows:

complaint: Is an array of URIs for the user to report mis-classified DNS filtering. This is likely to solely contain an "https" URI, but an array is provided in case telephone numbers or email or other URIs are necessary. This field is mandatory and MUST contain at least one URI.

justification: Includes the textual justification for this particular DNS filtering. This field is optional.

name: is the human-friendly name of the organization that filtered this particular DNS query. This field is optional.

regulation: the URI of the regulation authority for this DNS query being filtered. This might point at an employment agreement (for an enterprise performing filtering) or a national government regulation (for an ISP performing filtering). This field is optional.

The JSON data can be displayed to the user, logged, or otherwise used to assist the end-user or IT staff with troubleshooting and diagnosing the cause of the DNS filtering.

4. Examples

The examples use the folding defined in [RFC8792] for long lines.

An example with one entity, "example.net", that has filtered a DNS query is shown in Figure 1, below.

```
{
  "responsible": [
    {
      "complaint": [
        "mailto:helpdesk@example.net?subject=\"incorrect filtering\
         of example.org at 1621902483\"",
        "https://mistakes.example.net?domain=example.org?\
         time=1621902483",
        "tel:+18305551212"
      ],
      "justification": "malware present for 23 days",
      "name": "example.net Filtering Service",
      "regulation": "https://laws.example.net?country=atlantis"
    }
  ]
}
```

Figure 1: Example of Filtering with One Entity

An example with two entities, "example.com" and "example.net", that have filtered a DNS query is shown in Figure 2, below.

```
{
  "responsible": [
    {
      "complaint": [
        "mailto:helpdesk@example.net?subject=\"incorrect filtering\
         of example.org at 1621902483\"",
        "https://mistake.example.net?domain=example.org?\
         time=1621902483",
        "tel:+18305551212"
      ],
      "justification": "malware present for 23 days",
      "name": "Example.net Filtering Service",
      "regulation": "https://laws.example.net?country=atlantis"
    },
    {
      "complaint": [
        "mailto:abuse@example.com?subject=\"false positive filtering\
         example.org on 24-May-2021 5:03 GMT\"",
        "https://example.net/report?d=example.org?t=38233",
        "tel:+5305551212"
      ],
      "justification": "command and control malware",
      "name": "Example.com IT department",
      "regulation": "https://hr.example.com?state=CA"
    }
  ]
}}
```

Figure 2: Example of Filtering with Two Entities

5. Deployment Considerations

Over time a domain name may be considered risky, then safe, then risky again, and later can elapse between the DNS EDNS0 error and the user reporting a false positive and the DNS filtering service receiving the user's complaint. Thus the URI is RECOMMENDED to include sufficient detail to determine the state when the DNS EDNS0 response was generated. How this is encoded into the URI is an implementation decision.

As discussed in the Introduction, some deployment models allow the DNS filter provider to be conveyed to the end-user. In such a deployment, state can be avoided in the DNS forwarder by conveying the DNS filter provider's URL in the URL sent to the user. For example, if the upstream DNS filter provider (example.net) indicates their structured DNS error page for a query to example.org is https://example.net?f=example.org&s=38, that URL can be conveyed to the user as the URL-encoded parameter https%3A%2F%2Fexample.net%3Ff%3Dexample.org%26s%3D38229 appended to the DNS forwarder's DNS error page URL.

An array allows multiple DNS filters to be provided by specialized services. For example, one service might filter access to malicious domains and another filters domains due to an internal security policy or court order.

6. Usability Considerations

The JSON values returned SHOULD be returned in the user's preferred language as expressed by the Accept-Language HTTP header.

7. Security Considerations

Security considerations inherent to the use of DNS Error Page URI are discussed in Section 7 of [I-D.reddy-dnsop-error-page].

The structure data includes URLs that may be misused to return infected or compromised websites. Means to detect and avoid such URL are recommended. Likewise, contact URIs and telephone numbers may be misused to return third-party contact points and thus lead to spam these contacts.

8. IANA Considerations

This document requests IANA to register the "application/ json+structured-dns-error" media type in the "Media Types" registry [IANA-MediaTypes]. This registration follows the procedures specified in [RFC6838]:

Type name: application

Subtype name: json+structured-dns-error

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: as defined in Section 3 of [RFCXXXX].

Security considerations: See Section 7 of [RFCXXXX].

Interoperability considerations: N/A

Published specification: [RFCXXXX]

Applications that use this media type: Section 3 of [RFCXXXX].

Fragment identifier considerations: N/A

Additional information: N/A

Person & email address to contact for further information: IETF, iesg@ietf.org

Intended usage: COMMON

Restrictions on usage: none

Author: See Authors' Addresses section.

Change controller: IESG

Provisional registration? No

9. References

9.1. Normative References

[I-D.reddy-dnsop-error-page] Reddy, T., Cook, N., Wing, D., and M. Boucadair, "DNS Access Denied Error Page", Work in Progress, Internet-Draft, draft-reddy-dnsop-error-page-08, 4 June 2021, <https://www.ietf.org/archive/id/draft-reddy-dnsop-error-page-08.txt>.

[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>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC

6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[I-D.ietf-dprive-dnsoquic] Huitema, C., Mankin, A., and S. Dickinson, "Specification of DNS over Dedicated QUIC Connections", Work in Progress, Internet-Draft, draft-ietf-dprive-dnsoquic-02, 22 February 2021, <https://www.ietf.org/archive/id/draft-ietf-dprive-dnsoquic-02.txt>.

[IANA-MediaTypes] IANA, "Media Types", <https://www.iana.org/assignments/media-types>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/info/rfc8792>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

Authors' Addresses

Dan Wing
Citrix Systems, Inc.
United States of America

Email: dwing-ietf@fuggles.com

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park

Bangalore 560071
Karnataka
India

Email: kondtir@gmail.com

Neil Cook
Open-Xchange
United Kingdom

Email: neil.cook@noware.co.uk

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com