Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: 29 October 2026

M. Sivaraman
Banu Systems Private Limited

27 April 2026

EDNS options for filtering information
draft-muks-dns-filtering-05

Abstract

This memo documents EDNS options and methods that can be used to return information about filtered, blocked, or censored DNS responses. It complements the information provided in EDNS Extended DNS Error options [RFC8914].

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 29 October 2026.

Copyright Notice

Table of Contents

1. Introduction

Some DNS nameservers return forged answers with different IP addresses when they filter, block, or censor access to an internet domain name. A service is typically setup to run at the forged address and return information about the filtering that was performed.

This practice causes transport security-related errors at clients, such as the case where a HTTPS server serving at the forged answer's address does not have a valid TLS certificate configured for the domain name. A security error about a certificate mismatch is displayed by the web browser.

This draft introduces EDNS options [RFC6891] for nameservers to provide more information to clients about the filtering as part of the DNS response itself, making the need to return forged answers unnecessary when domain names are filtered. By using these options instead of forged answers, security errors due to forged answers may be avoided at clients, and the information provided in these new EDNS options may be used to diagnose filtering or contact administrators of the DNS nameservers that performed filtering.

2. Requirements notation

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. EDE-EXTRA-TEXT-LANGUAGE EDNS option

This option specifies the language that is used in the EXTRA-TEXT field of EDNS Extended DNS Error options in the same DNS message. It is not limited to DNS filtering, but may be used in any DNS message that contains EDNS Extended DNS Error options. There MAY be zero or one EDE-EXTRA-TEXT-LANGUAGE EDNS option in a message.

If a human-readable message is generated in the EXTRA-TEXT field of EDNS Extended DNS Error options, the nameserver MAY also include an EDE-EXTRA-TEXT-LANGUAGE EDNS option in the response. If the EDE-EXTRA-TEXT-LANGUAGE EDNS option is included, the language in its option data MUST match the language used in the EXTRA-TEXT field of the EDNS Extended DNS Error option.

The EDNS OPTION-CODE of EDE-EXTRA-TEXT-LANGUAGE is provided in Section 12. The OPTION-DATA MUST contain a language tag as described in [RFC5646].

4. FILTERING-CONTACT EDNS option

When DNS queries cause filtering to be performed by nameservers and negative responses to be returned due to it, the nameserver MAY return zero or more FILTERING-CONTACT EDNS options in responses, containing contact information of the party that performed the filtering.

DNS nameservers MAY generate these options as described in Section 7. DNS clients MAY use the information in these options as described in Section 8.

The EDNS OPTION-CODE of FILTERING-CONTACT is provided in Section 12. The OPTION-DATA is a UTF-8 encoded string (that is not nul-terminated) containing a contact URI using a contact URI scheme listed in TBD: add a link to the contact URI scheme registry.

5. FILTERING-ORGANIZATION EDNS option

When DNS queries cause filtering to be performed by nameservers and negative responses to be returned due to it, the nameserver MAY return zero or one FILTERING-ORGANIZATION EDNS option in responses, containing the name of the organization that performed the filtering.

DNS nameservers MAY generate this option as described in Section 7. DNS clients MAY use the information in this option as described in Section 8.

The EDNS OPTION-CODE of FILTERING-ORGANIZATION is provided in Section 12. The OPTION-DATA is a UTF-8 encoded string (that is not nul-terminated) containing the name of the organization that performed the filtering. The language used must match that specified in the EDE-EXTRA-TEXT-LANGUAGE EDNS option if the latter option is also included.

6. FILTERING-DB EDNS option

When DNS queries cause filtering to be performed by nameservers and negative responses to be returned due to it, the nameserver MAY return zero or one FILTERING-DB EDNS option in responses, containing the identifier, name, or description of the filtering database against which a matched query caused the filtering to occur.

DNS nameservers MAY generate this option as described in Section 7. DNS clients MAY use the information in this option as described in Section 8.

The EDNS OPTION-CODE of FILTERING-DB is provided in Section 12. The OPTION-DATA is a UTF-8 encoded string (that is not nul-terminated) containing the identifier, name, or description of the filtering database against which a matched query caused the filtering to occur.

7. DNS nameserver behavior

When DNS nameservers filter/block/censor queries to domain names, it is RECOMMENDED that they do not return forged positive answers (e.g., containing a different IP address) to filtered queries, but instead return negative responses (NODATA or NXDOMAIN) containing an EDNS Extended DNS Error option [RFC8914] with corresponding INFO-CODE accurately indicating the kind of filtering that was performed.

When such negative reponses are returned as a result of DNS filtering, DNS nameservers MAY include in DNS responses zero or more FILTERING-CONTACT EDNS options, and a FILTERING-ORGANIZATION EDNS option to provide information about the party that performed the filtering.

The nameserver MAY return a human-readable message describing the filtering action that was performed in the EXTRA-TEXT field of the EDNS Extended DNS Error option. If a human-readable message is generated in the EXTRA-TEXT field, the nameserver MAY also include an EDE-EXTRA-TEXT-LANGUAGE EDNS option in the response.

8. DNS client behavior

DNS clients do not have to specify anything in their queries to nameservers to receive DNS filtering-related information. Nameservers would automatically return DNS filtering-related information in EDNS responses if they are setup to do so.

When clients query DNS nameservers, they may receive DNS filtering-related information as part of the nameserver’s responses. This information may be contained in the EDNS options described in this draft, as well as EDNS Extended DNS Error option fields (INFO-CODE and EXTRA-TEXT) [RFC8914].

It is strongly RECOMMENDED that clients use DNS transport security protocols to query Privacy-enabling DNS servers as defined in [RFC9499] to protect the authenticity and integrity during transport of the DNS answer as well as the DNS filtering-related information that may be contained in it.

DNS clients may receive zero or more FILTERING-CONTACT EDNS options in reponses. DNS clients MAY make use of the information in these options as they would like to. An example may be to display the contact information in a dialog message with hyperlinks, so that users may contact filtering parties.

DNS clients may receive zero or more FILTERING-ORGANIZATION EDNS options in reponses. DNS clients MAY make use of the information in the first such EDNS option in the OPT RR as they would like to, and ignore any other FILTERING-ORGANIZATION options. An example may be to display the contact information in a dialog message with hyperlinks, so that users may contact filtering parties.

9. Example DNS message

The following is a sample packet dissection by Wireshark of a DNS response message containing the EDE-EXTRA-TEXT-LANGUAGE, FILTERING-CONTACT, FILTERING-ORGANIZATION, and FILTERING-DB EDNS options. This example was taken from the DNS responses generated in one of Loop's system tests. It was generated in response to RPZ processing [I-D.vixie-dnsop-dns-rpz] which returned an NXDOMAIN RCODE because the name being queried was blocked due to response policy.

```
Domain Name System (response)
    Transaction ID: 0x3172
    Flags: 0x8403 Standard query response, No such name
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .1.. .... .... = Authoritative: Server is an authority
                              for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...0 .... .... = Recursion desired: Don't do query
                              recursively
        .... .... 0... .... = Recursion available: Server can't do
                              recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority
                              portion was not authenticated by the
                              server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 2
    Queries
        test1a.example.com: type A, class IN
            Name: test1a.example.com
            [Name Length: 18]
            [Label Count: 3]
            Type: A (1) (Host Address)
            Class: IN (0x0001)
    Additional records
        rpz1.example.com: type SOA, class IN, mname <Root>
            Name: rpz1.example.com
            Type: SOA (6) (Start Of a zone of Authority)
            Class: IN (0x0001)
            Time to live: 300 (5 minutes)
            Data length: 22
            Primary name server: <Root>
            Responsible authority's mailbox: <Root>
```

```
            [Responsible authority's mailbox name: <Root>]
            Serial Number: 1
            Refresh Interval: 600 (10 minutes)
            Retry Interval: 600 (10 minutes)
            Expire limit: 1200 (20 minutes)
            Minimum TTL: 600 (10 minutes)
        <Root>: type OPT
            Name: <Root>
            Type: OPT (41)
            UDP payload size: 4096
            Higher bits in extended RCODE: 0x00
            EDNS0 version: 0
            Z: 0x0000
                0... .... .... .... = DO bit: Cannot handle DNSSEC
                                       security RRs
                .000 0000 0000 0000 = Reserved: 0x0000
            Data length: 180
            Option: Extended DNS Error
                Option Code: Extended DNS Error (15)
                Option Length: 48
                Option Data: 000f5175657279206f7220616e737765722077
                             617320626c6f636b656420627920726573706f
                             6e736520706f6c696379
                Info Code: Blocked (15)
                Extra Text: Query or answer was blocked by response
                            policy
            Option: EDE-EXTRA-TEXT-LANGUAGE
                Option Code: EDE-EXTRA-TEXT-LANGUAGE (22)
                Option Length: 2
                Option Data: 656e
                Language: en
            Option: FILTERING-ORGANIZATION
                Option Code: FILTERING-ORGANIZATION (24)
                Option Length: 24
                Option Data: 546865204578616d706c65204f7267616e697a
                             6174696f6e
                Organization: The Example Organization
            Option: FILTERING-DB
                Option Code: FILTERING-DB (25)
                Option Length: 34
                Option Data: 476f7665726e6d656e7420416e74692d506972
                             61637920506f6c6963696573202331
                Database: Government Anti-Piracy Policies #1
            Option: FILTERING-CONTACT
                Option Code: FILTERING-CONTACT (23)
                Option Length: 26
                Option Data: 6d61696c746f3a737570706f7274406578616d
                             706c652e636f6d
```

```
                Contact: mailto:support@example.com
            Option: FILTERING-CONTACT
                Option Code: FILTERING-CONTACT (23)
                Option Length: 22
                Option Data: 736970733a68656c6c6f406578616d706c652e
                             636f6d
                Contact: sips:hello@example.com
```

For completeness, here is a snippet from a Loop named.conf configuration file, that was used to configure the values returned in the filtering options in the response shown above:

```
options {
    // [snip...]

    edns-filtering-info-contacts {
        "mailto:support@example.com";
        "sips:hello@example.com";
    };

    edns-filtering-info-organization "The Example Organization";

    ede-extra-text-language "en";

    response-policy {
        // The default intent is blocking.
        zone "rpz1.example.com" filtering-db
            "Government Anti-Piracy Policies #1";
        zone "rpz2.example.com" intent blocking;
        zone "rpz3.example.com" intent censoring;
        zone "rpz4.example.com" intent filtering;
    } recursive-only no;

    // [snip...]
};
```

10. Interoperability with Structured Error Data for Filtered DNS JSON

When Structured Error Data for Filtered DNS JSON is explicitly requested by a DNS client by querying with the Structured DNS Error EDNS option as specified in Section 5.4 (Structured DNS Error (SDE) EDNS(0) Option Format) of [I-D.ietf-dnsop-structured-dns-error], a nameserver that also implements [I-D.ietf-dnsop-structured-dns-error] MAY NOT return the EDE-EXTRA-TEXT-LANGUAGE, FILTERING-CONTACT, FILTERING-ORGANIZATION, and FILTERING-DB EDNS options in responses to such queries, and MAY instead process the query as specified in Section 5.2 (Server Generating Response) of [I-D.ietf-dnsop-structured-dns-error].

A nameserver MUST NOT include the EDE-EXTRA-TEXT-LANGUAGE, FILTERING-CONTACT, FILTERING-ORGANIZATION, and FILTERING-DB EDNS options as well as Structured Error Data for Filtered DNS JSON in a single response. It must pick one, and the choice can be made based on whether the DNS client's query contained the Structured DNS Error option.

11. Security considerations

It is strongly RECOMMENDED that clients use DNS transport security protocols to query Privacy-enabling DNS servers as defined in [RFC9499] to protect the authenticity and integrity during transport of the DNS answer as well as the DNS filtering-related information that may be contained in it.

TBD: Any other details that the dnsop WG and authors of draft-ietf-dnsop-structured-dns-error want to include.

12. IANA considerations

IANA has allocated the following code points in the "DNS EDNS0 Option Codes (OPT)" registry in the "Domain Name System (DNS) Parameters" registry group.

Value	Name	Status	Reference
22	EDE-EXTRA-TEXT-LANGUAGE	Optional	See Section 3.
23	FILTERING-CONTACT	Optional	See Section 4.
24	FILTERING-ORGANIZATION	Optional	See Section 5.
25	FILTERING-DB	Optional	See Section 6.

Table 1

13. Acknowledgements

The FILTERING-CONTACT, FILTERING-ORGANIZATION, and EDE-EXTRA-TEXT-LANGUAGE EDNS options are based on the "c", "o", and "l" JSON fields respectively as listed in Section 4 (I-JSON in EXTRA-TEXT Field) of [I-D.ietf-dnsop-structured-dns-error].

14. References

14.1. 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>.

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <https://www.rfc-editor.org/info/rfc5646>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[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>.

[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>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

14.2. Informative references

[I-D.ietf-dnsop-structured-dns-error] Wing, D., Reddy.K, T., Cook, N., and M. Boucadair, "Structured Error Data for Filtered DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-structured-dns-error-19, 6 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-structured-dns-error-19>.

[I-D.vixie-dnsop-dns-rpz] Vixie, P. A. and V. Schryver, "DNS Response Policy Zones (RPZ)", Work in Progress, Internet-Draft, draft-vixie-dnsop-dns-rpz-00, 23 June 2018, <https://datatracker.ietf.org/doc/html/draft-vixie-dnsop-dns-rpz-00>.

Author’s Address

Mukund Sivaraman
Banu Systems Private Limited
6001 Beach Road, #19-09, Golden Mile Tower
SINGAPORE 199589
Singapore
Email: muks@banu.com
URI: https://banu.com/