Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: 27 September 2026

M. Sivaraman
Banu Systems Private Limited

26 March 2026

EDNS options for filtering information
draft-muks-dns-filtering-01

Abstract

This memo documents EDNS options, EDNS Extended DNS Errors INFO-CODE values, 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 27 September 2026.

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. 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 with contact information of the party that performed the filtering.

DNS nameservers MAY generate these options as described in Section 6. DNS clients MAY use the information in these options as described in Section 7.

The EDNS OPTION-CODE of FILTERING-CONTACT is provided in Section 9. The OPTION-DATA contains a single contact URI using a contact URI scheme listed in TBD: add a link to the contact URI scheme registry.

4. 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 more FILTERING-ORGANIZATION EDNS options in responses with the name of the organization that performed the filtering.

DNS nameservers MAY generate these options as described in Section 6. DNS clients MAY use the information in these options as described in Section 7.

The EDNS OPTION-CODE of FILTERING-ORGANIZATION is provided in Section 9. The OPTION-DATA contains 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.

5. 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 9. The OPTION-DATA MUST contain a language tag as described in [RFC5646].

6. 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.

7. 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.

8. 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.

9. IANA considerations

IANA is requested to allocate 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
TBD	FILTERING-CONTACT	TBD	See Section 3.
TBD	FILTERING-ORGANIZATION	TBD	See Section 4.
TBD	EDE-EXTRA-TEXT-LANGUAGE	TBD	See Section 5.

Table 1

10. 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].

11. References

11.1. 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>.

11.2. 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-18, 18 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-structured-dns-error-18>.

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/