

add  
Internet-Draft  
Intended status: Standards Track  
Expires: September 10, 2020

D. Migault  
Ericsson  
March 09, 2020

Signaling resolver's filtering policies  
draft-mglt-add-signaling-filtering-policies-00

## Abstract

This document defines one mechanism that enables a DNS resolver to inform a DNS client that filtering policies are in place and what their concern is. The second mechanism describes how a DNS client can request a resolver whether filtering policies are in place and what their concern is.

## 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 September 10, 2020.

## Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Requirements Notation . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">3.</a>	Filtering semantics . . . . .	<a href="#">3</a>
<a href="#">4.</a>	DNS resolver advertising filtering status . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Requesting DNS resolver filtering status . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Blocking traffic under the policy . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">8.</a>	Privacy Considerations . . . . .	<a href="#">6</a>
<a href="#">9.</a>	IANA considerations . . . . .	<a href="#">6</a>
<a href="#">10.</a>	Acknowledgment . . . . .	<a href="#">7</a>
<a href="#">11.</a>	References . . . . .	<a href="#">7</a>
<a href="#">11.1.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">11.2.</a>	Informative References . . . . .	<a href="#">7</a>
	Author's Address . . . . .	<a href="#">8</a>

[1.](#) 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 [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[2.](#) Introduction

This document defines mechanisms that enable a DNSSEC resolver to signal that filtering policies are enabled by the DNSSEC resolver. There are two distinct mechanisms. The first mechanism enables a resolver to advertise policies that are enabled/disabled without any explicit request from the DNS client. The second mechanism enables a DNS client to request the status of the resolver. Such consideration may be used, by a stub resolver for example to select an appropriated resolver.

The ability for a resolver to provide such information to a DNS client will help a DNS client to appropriately chose its resolver.

The ability to request or signal configuration information has already been done in the past for the TA. [[RFC8145](#)] enables a resolver to advertise an authoritative server via an EDNS option in the OPT RR which TA is used for the DNSSEC validation. The RR is

inserted when DNSKEY RRsets are requested. In addition, the resolver may also request the appropriated TA with a specific DNS query. The RRsets are stored in the authoritative zone.

[RFC8509] describes a sentinel mechanism where the resolver has a specific behavior based on the left side label. This mechanism enable a user to evaluate which KSK the resolver provisioned with.

[RFC6975] describes how resolvers can indicate the supported cryptographic primitives. These are advertised though EDNS0 options in OPT RR.

### [3.](#) Filtering semantics

Filtering can be enforced in various ways, and the resolver should be able to provide some insight of the filtering policies in place. This document considers various filtering policies that may be extended in the future. The filtering policies are informative and are expected to provide a good understanding to the DNS client of the status of the filtering policies. The filtering policy enforced by the resolver may result in a combination of various filtering policies.

Values	Name
0	no_filetring
1	undefined
2	malware
3	illegal
4	child
200-255	unassigned

`no_filetring` indicates no filtering is performed by the resolver. This policy is incompatible with other policies.

`undefined` indicates a filtering policy but does not provide indications on the policies. When used in combination of other filtering policies, it indicates additional filtering policies are considered.

malware sites that are security risks or sources of malware, or that allow users to circumvent policies.

illegal Users may be committing crimes or exposing the organization to legal liability with these sites.

child sites that can be seen by kids.

source: <https://campus.barracuda.com/product/campus/doc/5472264/web-use-categories>  
<https://campus.barracuda.com/product/ContentShield/doc/77401148/how-to-configure-dns-filtering-policies/>

Migault

Expires September 10, 2020

[Page 3]

Internet-Draft

filtering policies by the resolver

March 2020

Note that the client should consider information related to the filtering policies enforced by the resolver cautiously and interpretation of the policies will depend on the trust as well as additional knowledge of the resolver. Typically, illegal categories result in the enforcement of the local jurisdiction which could results in site not being blocked within other jurisdictions.

#### 4. DNS resolver advertising filtering status

The resolver MAY advertise its filtering policy to the DNS client using an OPT RR in an EDNS0 option [[RFC6891](#)]. The variable part of the RDATA to define filtering status is defined below:

```
0                               8                               16
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               OPTION-CODE                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               |                                       |
/                               DATA                                   /
|                               |                                       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

and DATA defined as

```
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               LENGTH                                   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  filtering_policy             |                               ...      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

$$+ - + - + - + - + - + \cdots + - + - + - + - +$$

where:

OPTION-CODE The EDNS0 option code assigned to filtering-policies (TBD1).

LENGTH The length in octets of the filtering policies, that is the number of filtering policies that apply. When RDATA is used in conjunction of EDNS0, LENGTH corresponds to the OPTION-LENGTH field as defined in [\[RFC6891\]](#).

filtering policies the list of filtering policies coded over one octet that apply. When RDATA is used in conjunction of EDNS0, the filtering\_policies corresponds to OPTION-DATA.

The filtering status may be placed by the DNS resolver as an indication to the DNS client. It is recommended the DNS resolve

Migault

Expires September 10, 2020

[Page 4]

Internet-Draft

filtering policies by the resolver

March 2020

place the indication in the first response it provides to the DNS client. When the DNS exchanges are protected by TLS or DTLS, the OPT RR SHOULD be provided in the first DNS response provided after the (D)TLS session establishment. When exchanges are not protected over (D)TLS the resolver MAY insert it at regular time interval. The resolver could also maintain a list of seen IP addresses, and provide the OPT RR anytime a new IP address is noticed.

As EDNS0 is not protected by DNSSEC, it is RECOMMENDED to consider such signaling when the exchanges are protected by (D)TLS.

## 5. Requesting DNS resolver filtering status

This section describes a mechanism that enables the DNS client to request the resolver policies. Policies will be retrieve via a DNS exchange.

The DNS resolver is usually designated by an IP address rather than a name as to get the IP address from a name would involve a DNS resolution. As a result, the DNS client may not necessarily be configured with the associated name of the resolver and a reverse resolution may be required to receive to get this name. In the

remaining of the section, the resolver is designated by example.com

The policies are indicated by the RRset with QTYPE=NULL, QCLASS=IN, QNAME=\_filtering\_policies.example.com. The associated RDATA as defined in [Section 4](#).

The resolver supporting this mechanisms is provisioned with the this record and responds to the query. By this way, the DNS client is aware of the filtering policies implemented. A resolver not supporting this mechanism will return an error (NXDOMAIN) thus informing the DNS client that filtering policies are not provided. The RRsets SHOULD be signed by DNSSEC.

The resolution service is often seen by the end user as a service that may involve multiple parties. How the different parties collaborate is usually out of the DNS client perspective. Typically the downstream point must ensure the provided filtering policies reflects the filtering policies of the upstream parties. In some cases discovery policies of the upstream resolvers might be performed and the response may result in the aggregation of multiple RRsets. At least any party MUST ensure the filtering policies responded reflects the actual the enforced filtering policies. The entry point of a resolving service SHOULD provide its corresponding \_filtering\_policies RRsets as well as RRsets associated to upstream resolvers. These RRsets MAY be added in the additional section or the resolver MAY built its filtering policies according to the

upstream filtering policies. If an upstream resolver does not provide filtering policies, the resolver SHOULD include an undefined filtering p policies.

## [6](#). Blocking traffic under the policy

When a resolution fails because of the filtering policy, the error code returned can be Blocked, Censored or Filtered [[I-D.ietf-dnsop-extended-error](#)]. When filtering policies are requested by the DNS client - such a parental control for example - Filtered SHOULD be returned. When blocking results from a legal enforcement Censored SHOULD be returned. When bocking is performed by the operator's intelligence - such as malware related traffic for example - Blocked SHOULD be returned.

## [7.](#) Security Considerations

Informative only! the DNS client can hardly check. sensitive to chain of resolvers.

## [8.](#) Privacy Considerations

## [9.](#) IANA considerations

IANA has assigned an EDNS0 option code for the filtering option in the "DNS EDNS0 Option Codes (OPT)" registry as follows:

Value	Name	Status	Reference
TBD1	filtering-policies	Optional	RFC-TBD

<https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-14>

### DNS Filtering Policies

Values	Name	Description	Reference
0	no_filetring	no filtering performed	RFC-TBD
1	undefined	undefined filtering	RFC-TBD
2	malware	malware related traffic	RFC-TBD
3	illegal	legal enforcement	RFC-TBD
4	child	unappropriated for kids	RFC-TBD
200-255	unassigned		RFC-TBD

### Underscored and Globally Scoped DNS Node Names

Migault

Expires September 10, 2020

[Page 6]

Internet-Draft

filtering policies by the resolver

March 2020

RR Type	_NODE NAME	Reference
NULL	_filetring_policies	RFC-TBD

## [10.](#) Acknowledgment

## [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>>.
- [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>>.
- [RFC6975] Crocker, S. and S. Rose, "Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)", [RFC 6975](#), DOI 10.17487/RFC6975, July 2013, <<https://www.rfc-editor.org/info/rfc6975>>.
- [RFC8145] Wessels, D., Kumari, W., and P. Hoffman, "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)", [RFC 8145](#), DOI 10.17487/RFC8145, April 2017, <<https://www.rfc-editor.org/info/rfc8145>>.
- [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>>.
- [RFC8509] Huston, G., Damas, J., and W. Kumari, "A Root Key Trust Anchor Sentinel for DNSSEC", [RFC 8509](#), DOI 10.17487/RFC8509, December 2018, <<https://www.rfc-editor.org/info/rfc8509>>.

### 11.2. Informative References

- [I-D.ietf-dnsop-extended-error]  
Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", [draft-ietf-dnsop-extended-error-14](#) (work in progress), January 2020.



Daniel Migault  
Ericsson  
8275 Trans Canada Route  
Saint Laurent, QC H4S 0B6  
Canada

EMail: [daniel.migault@ericsson.com](mailto:daniel.migault@ericsson.com)