Signaling resolver's filtering policies

draft-mglt-dprive-signaling-filtering-policies

Daniel Migault

Motivations

The filtering policies implemented by a resolver are important information for the DNS client.

- can be used for a selection

Currently the detection of parental control is performed through the use of a canary domain.

We believe a standard mechanism as well as the ability to explicitly provide this information is preferred.

Goals

This document defines two mechanisms:

- a DNS resolver informs a DNS client ongoing filtering policies
- a DNS client requests the resolver filtering policies

Multiple Communications between a resolver and a DNS client have already been defined:

- RFC 6975 provides the supported cryptographic primitives of the resolver
    - EDNS0 options
- **RFC 8145** defines the communications of the TA.
    - EDNS0 option
    - specific DNS query
- RFC 8509 defines a sentinel mechanism
    - specific DNS query

Design

Our design is largely inspired by RFC 8145

- (with some differences)

The filtering policies are represented by DATA

- Resolver advertises the filtering by carrying DATA in an EDNSO OPT RR
- Client queries a specific FQDN to request the DATA

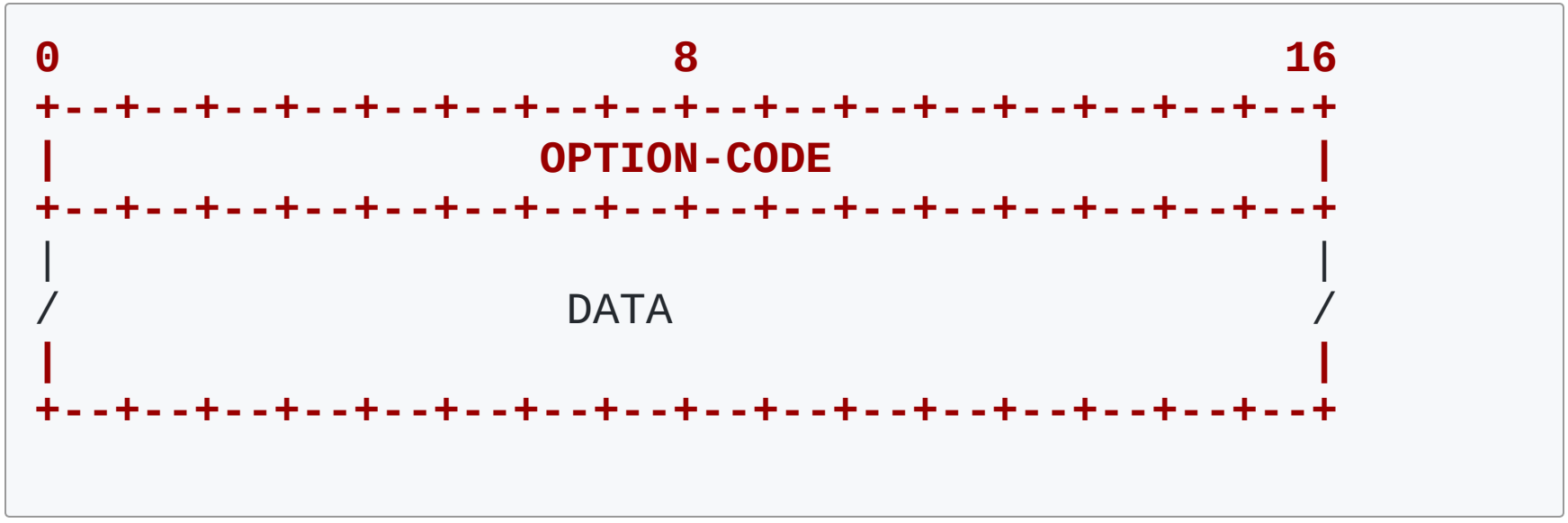
DATA represents the filtering service resulting from several filtering policies:

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

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

Advertisement from the resolver

The resolver advertises filtering policies to the DNS client using an OPT RR in an EDNS0 option



Request by the DNS client

The policies are indicated by the RRset with:

- QTYPE=NULL,
- QCLASS=IN,
- QNAME=_filtering_policies.example.com.

example.com is the domain name of the resolver

- a reverse resolution may be required

Some considerations:

EDNS0 are not DNSSEC protected.

My resolver may depend on one one or more upstream resolvers

- the response should be the agregation of upstream resolvers

Assumes one policy per resolver identity

Thanks!