Best Current Operating Practices for DNS filtering

Asbjørn Sloth Tønnesen

DNS-WG, RIPE90, Lisbon, May 14, 2025

Why do ISPs do DNS filtering?

- Legal reasons
  - Sanctions
  - Copyright
  - Product safety
  - Gambling
- Security (opt-in?)
  - Malware
  - Botnet C&C
  - Phishing

How?

- Use Response Policy Zones (RPZ)
  - `draft-vixie-dnsop-dns-rpz`
- Respond to queries with NXDOMAIN
- Bonus points: add an Extended DNS Error code (EDE).

Respond with a block page

- Is expected/required in some jurisdiction
- Is very fragile (doesn't work with `https://` links / HSTS / preload):

1. Respond DNS query with CNAME pointing to block page server
2. Hope that the client attempts HTTP (really!)
3. Serve a block page with `451 Unavailable For Legal Reasons` (RFC 7725)

Extended DNS error codes

- RFC 8914 specifies the following Extended Error Codes:
  - Forged Answer (4)
  - Blocked (15)
  - Censored (16)
  - Filtered (17)
- Propagations through forwarding resolvers.

Extended DNS error codes

- RFC 8914 specifies the following Extended Error Codes:
  - Forged Answer (4)
  - Blocked (15)
  - Censored (16)
  - Filtered (17)
- Propagation is an implementation detail, but MAY occur.

Example with EDE code

```
$ dig blocked.nx.ede.dn5.dk @1.1.1.1
[...]
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 44427
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
[...]
; EDNS: version: 0, flags:; udp: 1232
; EDE: 15 (Blocked): (You found a blocked page!)
[...]
```

Support for EDE codes related to filtering still missing

- Recursive resolvers (unbound, bind, . . .)
- Caching resolvers (dnsmasq, dnsdist, . . .)
- Stub resolvers (system resolvers + browsers)

Structured DNS errors

- IETF I-D: `draft-ietf-dnsop-structured-dns-error`
- Overloads EDE extratext field as I-JSON.
- MUST discard extratext unless transport is secure (DoT).

Summary

- Many ways to implement:
  - `NXDOMAIN`
  - `CNAME`/`A`/`AAAA` serving STOP pages with HTTP status code ???
  - `A`/`AAAA` to localhost
  - Empty reply
  - Send `EDE` code?
- Block page serving is challenged by `HTTP` support being increasingly deprecated in browsers

RIPE Atlas survey

- Tested resolution on 5378 probes, in EU28/EEA/CH/GB/UA.
- 2505 probes (46.58%) uses a public resolver
- Out of the remaining 2873 probes:
  - 1596 probes (55.55%) resolved both RT and TPB.
  - 2258 probes (78.59%) resolved TPB
  - 1693 probes (58.93%) resolved RT

RIPE Atlas survey - Blocking methods

qtype	resp_class	count
A	nxdomain (no EDE)	463
A	block page (forged A/AAAA)	423
A	blocked (no A)	361
A	blocked (A/AAAA to localhost)	262
A	block page (CNAME)	83
A	nxdomain (+EDE)	16
A	block page (CNAME and EDE)	1
AAAA	blocked (no AAAA)	427
AAAA	blocked (A/AAAA to localhost)	178
AAAA	block page (CNAME)	72
AAAA	nxdomain (no EDE)	41
AAAA	block page (forged A/AAAA)	2

(12 rows)

Where to go from here?

- Block page deprecation?
- Improve EDE support?
- Should we create a BCOP document?
- Any thoughts?