Structured Data for DNS Access Denied Error Page

draft-wing-dnsop-structured-dns-error-page-01

IETF112, November 2021

D. Wing (Citrix)
T. Reddy (Akamai)
N. Cook (Open-Xchange)
M. Boucadair (Orange)
Purpose

• Parsable JSON for user and IT troubleshooting DNS filtering
• Client displays/logs the JSON with its own UI
• Headless devices (IoT)

• Updates to address comments
• Replaces draft-reddy-dnsop-error-page
Design

• Accommodates multiple filtering services

• Protocol permits IT organization to occlude, or pass along, details from upstream DNS filters
  – Correcting upstream filters often requires IT help

  ![Diagram](image-url)
  - Client
  - IT-operated DNS filter: Filters job-searching sites
  - Commercial DNS filter: Filters malware
Structured Error EDNS(0) Option Code

- New EDNS0 option to explain the reason for DNS filtering

```
+-----------------------------------------------+
| STRUCTURED-ERROR-LENGTH (fixed, two octets) |
+-----------------------------------------------+
/                                                                 /
/ STRUCTURED-ERROR-JSON (variable size)         /
/                                               /
+-----------------------------------------------+
```
Example JSON

```
{
    "c": "?time=1621902483",       //Report misclassified filter
    "d": "ns.example.com",        //FQDN of DoH/DoT server
    "j": "malware present for 23 days", //Justification
    "o": "example.net Filtering Service",  //Organization
    "r": "?country=atlantis"       //Regulation
}
```

https://ns.example.com?time=1621902483&type=a&name=example.org

from DNS query
Security Considerations

• Encrypted and Authenticated DNS connection is mandatory
• Free-form text of “o” and “j” fields; no clickable links
• Isolated environment to process the “c” and “r” pages (like captive portals)
  □ Label the page as not trusted
  □ Do not send cookies
  □ Disable JavaScript
  □ Block auto-fill of credentials/personal information
  □ Auto-Enable private browsing mode for the error page. Load the error page in a container isolated from other web activity.
• Processing “c” and “r” is optional; “j” contains text justification
  – Headless devices, IoT, etc.
Discussion Points

• Language of “j” and “o” fields
  – Language tag support removed (privacy, DNS packet has justification)
  – How to handle?

• Isolated browsing environment for “c” and “r”
  – Security vs harm tradeoff (e.g., creating trouble ticket requires login)

• Consider for WG adoption