Internet-Draft
Intended status: Experimental
Expires: April 12, 2026

Rais Ahmed
Independent Submission

October 12, 2025

DNS Policy Redirection Mechanisms: RPZ-EDE Enhancement and URI-R Redirection Record

draft-ahmed-dns-policy-redirect-00

Abstract

This document defines two complementary mechanisms to improve user experience and policy transparency in DNS-based filtering. The first mechanism enhances Response Policy Zone (RPZ) operation through Extended DNS Error (EDE) signaling. The second introduces a new URI-REDIRECT (URI-R) Resource Record to support secure, application-level redirection for both HTTP and HTTPS traffic. Each mechanism can operate independently or together, enabling network operators and resolvers to provide safer, TLS-compliant redirection for policy-enforced domains.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at https://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

This Internet-Draft will expire on April 12, 2026.

Table of Contents

1. Introduction

DNS-based policy enforcement, such as through Response Policy Zones (RPZ), is widely used to protect users from malicious or restricted domains. Traditional redirection methods often substitute an IP address to display a warning page. However, for HTTPS traffic this causes TLS certificate mismatches and security warnings.

This draft introduces two independent but complementary mechanisms to resolve this problem: an RPZ-EDE extension and a URI-REDIRECT record. Each can be implemented separately or together.

2. Problem Statement

When a resolver enforces policy using an RPZ redirect or CNAME substitution, browsers attempting to connect via HTTPS will encounter a certificate mismatch. The redirection IP does not match the queried domain, producing TLS errors such as "Your connection is not private."

There is no existing DNS-based framework that both preserves HTTPS integrity and provides transparent user notification.

3. Overview of RPZ and EDE

Response Policy Zones (RPZ) allow DNS operators to define policies that alter query responses. Extended DNS Errors (EDE), as defined in RFC 8914, allow resolvers to return structured error codes and explanatory text.

Integrating EDE with RPZ provides a mechanism to inform clients why a domain was blocked or altered without modifying the transport or redirection layer.

4. Mechanism 1: RPZ-EDE Policy Signaling

In this approach, RPZ is extended to include optional EDE fields. When a resolver blocks or rewrites a query, it returns an EDE code describing the policy reason (for example, "Malware Domain").

Example:

```
;; ->>HEADER<<- opcode: QUERY; status: REFUSED
;; EDE: 15 (Blocked Due to Policy)
;; EDE Text: "Malicious domain detected by RPZ policy"
```

Clients supporting EDE can render local warnings or internal pages explaining the block reason.

Advantages:

* No TLS handshake errors occur.
* Fully compatible with DNSSEC and RPZ.
* Backward-compatible with existing resolvers.

Limitations:

* Requires EDE-aware clients.
* Cannot display rich HTML warning content.

5. Mechanism 2: URI-REDIRECT (URI-R) Record

The URI-R Resource Record allows resolvers to return a structured URI indicating a redirection target, rather than an IP address. This enables secure, HTTPS-compatible redirects.

Example Record:

```
  blocked.example.com. IN URI-R 10 0 0 "https://safe.example.net/warning"
```

Resolver Behavior:
* On policy match, respond with URI-R instead of A/AAAA records.
* Optionally include EDE for additional context.

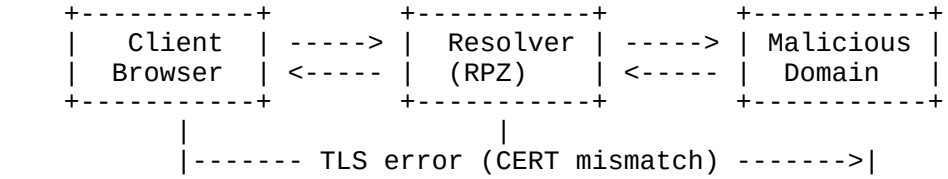
Client Behavior:
* Interpret URI-R as an instruction to redirect to the specified HTTPS URI before establishing any TLS session with the blocked domain.

Advantages:
* Seamless HTTPS redirect without certificate errors.
* Rich user interface and context display possible.

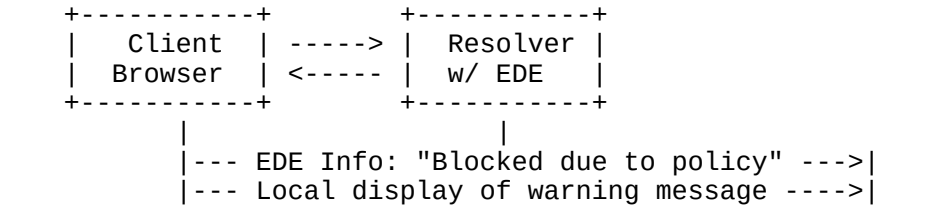
Limitations:
* Requires client/stub resolver support.
* Introduces trust and validation complexity.

6. Illustrative Message Flow

6.1 Current Behavior (Without RPZ-EDE or URI-R)



6.2 RPZ-EDE Enabled Resolver



6.3 URI-R Enabled Resolver

These flows show the difference between the traditional approach, RPZ-EDE signaling, and the new URI-R redirection model.

7. Security Considerations

Both mechanisms require trust in the recursive resolver. URI-R introduces additional considerations because it can alter client navigation behavior. Implementations MUST ensure URI-R responses originate only from trusted, DNSSEC-validated resolvers.

RPZ-EDE and URI-R data MUST NOT be accepted from untrusted or unsigned DNS responses. Clients SHOULD detect and prevent redirect loops and ignore malformed URIs.

8. IANA Considerations

This document requests IANA to allocate a new DNS Resource Record type code for "URI-R" (URI-REDIRECT). It also suggests reserving additional Extended DNS Error codes for policy signaling under RPZ operation.

9. References

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[RFC8914] Kumari, W. and R. Hunt, "Extended DNS Errors (EDE)", RFC 8914, September 2020.

[RPZ-ISC] Internet Systems Consortium, "Response Policy Zone (RPZ) Technical Specification", 2021.

10. Author’s Address

Rais Ahmed
Independent Submission
Email: rais.ahmed@outlook.com