

**EDNS X-Proxied-For
draft-bellis-dnsop-xpf-00**

Abstract

It is becoming more commonplace to install front end proxy devices in front of DNS servers to provide (for example) load balancing or to perform transport layer conversions.

This document defines an option within the EDNS(0) Extension Mechanism for DNS that allows a DNS server to receive the original client source IP address when supplied by trusted proxies.

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 <http://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 July 10, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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

1.	Introduction	2
2.	Terminology	2
3.	Description	3
3.1.	EDNS Option Format	3
3.2.	Proxy Processing	3
3.3.	Server Processing	4
3.4.	Secret Key Transaction Authentication for DNS (TSIG) . .	4
3.5.	Multi-tier Proxies	5
4.	Security Considerations	5
5.	Privacy Considerations	5
6.	IANA Considerations	5
7.	Acknowledgements	5
8.	Normative References	5
	Author's Address	6

[1.](#) Introduction

It is becoming more commonplace to install front end proxy devices in front of DNS servers [[RFC1035](#)] to provide (for example) load balancing or to perform transport layer conversions.

This has the unfortunate side effect of hiding the clients' source IP addresses from the server, making it harder to employ server-side technologies that rely on knowing those address (e.g. ACLs, DNS Response Rate Limiting, etc).

This document defines an option within the EDNS(0) Extension Mechanism for DNS [[RFC6891](#)] that allows a DNS server to receive the original client source IP address when supplied by trusted proxies.

This specification is only intended for use on server-side proxy devices that are under the same administrative control as the DNS servers themselves. As such there is no change in the scope within which any private information might be shared.

[2.](#) Terminology

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 in "Key words for use in RFCs to Indicate Requirement Levels" [[RFC2119](#)].

Bellis

Expires July 10, 2017

[Page 2]

3. Description

3.1. EDNS Option Format

The overall format of an EDNS option is shown for reference below, per [\[RFC6891\]](#), followed by the option specific data:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
0: |                                OPTION-CODE                                |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
2: |                                OPTION-LENGTH                             |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
4: |                                |
/                                /
/                                /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

OPTION-CODE: TBD, with mnemonic "XPF".

OPTION-LENGTH: Size (in octets) of OPTION-DATA.

OPTION-DATA: Option specific, as below:

```

                                +0 (MSB)                                +1 (LSB)
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
0: |      Unused      |  IP Version  |      Address Octet 0      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
2: |      Address Octet 1      |      ...      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      ...      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Unused: Currently reserved. These MUST be zero unless redefined in a subsequent specification.

IP Version: The IP protocol version number used by the client.

Address: The source IP address of the client.

3.2. Proxy Processing

Proxies implementing this specification must append this option to each request packet received before forwarding it to the intended DNS server.

If the proxy has to create a new OPT RR (because none was present in the original request) it MUST strip any OPT RR subsequently seen in the response for conformance with [Section 7 of \[RFC6891\]](#).

Bellis

Expires July 10, 2017

[Page 3]

Author's note: what are the implications of that for TSIG
[Section 3.4](#)?

[3.3.](#) Server Processing

This option MUST be ignored by servers when received from a client that is not white-listed by the server.

When this option is received from a white-listed proxy, the DNS server MUST (SHOULD?) use the address contained therein in preference to the client's source IP address for any data processing logic that would otherwise depend on the latter.

If the length of the client IP address contained in the OPTION-DATA is not consistent with that expected for the given IP version then the server MUST return a FORMERR response.

Author's note: What response for unknown IP version numbers?

Servers MUST NOT send this option in DNS responses.

[3.4.](#) Secret Key Transaction Authentication for DNS (TSIG)

The considerations for TSIG [[RFC2845](#)] from [Section 4.5](#) of "DNS Proxy Implementation Guidelines" [[RFC5625](#)] apply here.

A TSIG-signed request MUST either:

1. be forwarded according to [RFC 5625](#) without addition of this option, or
2. be verified using a secret shared between client and proxy, updated with this option, and then re-signed with a (potentially different) shared secret before sending to the server.

In the case of option 1, the server might still be able to uniquely identify and authenticate the client through its shared key, but not by its IP address.

If option 2 is used, there is an operational trade-off to be considered as to whether the two secrets (between client and proxy, and between proxy and server) are actually the same secret. A potential advantage of three-way sharing of the secret is that the server response (which per above MUST NOT be modified by adding this option) may be returned directly to the client without any further TSIG operations.

Bellis

Expires July 10, 2017

[Page 4]

Author's note: A third alternative exists, which is to append an additional TSIG signature to the packet based on a secret shared only between the proxy and server. If end-to-end TSIG validation is required alongside TSIG validation between proxy and server, the server would have to 1) validate that second signature, 2) strip it, and then 3) perform further validation on the original signature. Feedback is sought on whether this is worth pursuing.

3.5. Multi-tier Proxies

TBD

4. Security Considerations

If the white-list of trusted proxies is implemented as a list of IP addresses, the server administrator MUST have the ability to selectively disable this feature for any transport where there is a possibility of the proxy's source address being spoofed.

This does not mean to imply that use over UDP is impossible - if for example the network architecture keeps all proxy-to-server traffic on a dedicated network and clients have no direct access to the servers then the proxies' source addresses can be considered unspoofable.

5. Privacy Considerations

Used incorrectly, this option could expose internal network information, however it is not intended for use on proxy / forwarder devices that sit on the client-side of a DNS request.

6. IANA Considerations

IANA are directed to assign the value TBD for the XPF option in the DNS EDNS0 Option Codes Registry.

7. Acknowledgements

8. Normative References

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<http://www.rfc-editor.org/info/rfc1035>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

- [RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2845](#), DOI 10.17487/RFC2845, May 2000, <<http://www.rfc-editor.org/info/rfc2845>>.
- [RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", [BCP 152](#), [RFC 5625](#), DOI 10.17487/RFC5625, August 2009, <<http://www.rfc-editor.org/info/rfc5625>>.
- [RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, [RFC 6891](#), DOI 10.17487/RFC6891, April 2013, <<http://www.rfc-editor.org/info/rfc6891>>.

Author's Address

Ray Bellis
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City CA 94063
USA

Phone: +1 650 423 1200
Email: ray@isc.org

