Workgroup: Network Working Group
Internet-Draft:
draft-pauly-masque-dns-proxy-status-00
Published: 4 October 2022
Intended Status: Standards Track
Expires: 7 April 2023
Authors: T. Pauly
Apple, Inc.

HTTP Proxy-Status Parameter for DNS Information

Abstract

This document defines an HTTP Proxy-Status Parameter that contains the IP address and CNAME chain received over DNS that was used to establish the connection to the next hop.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/tfpauly/privacy-proxy.

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 https://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 7 April 2023.

Copyright Notice

Table of Contents

1. Introduction

The Proxy-Status HTTP response field [PROXY-STATUS] allows proxies to convey information about how a proxied request was handled in HTTP responses sent to clients. It defines a set of parameters that provide information, such as the name of the next hop.

The Proxy-Status field can be sent by both forward proxies and gateways (or "reverse proxies"). In the case of forward proxies, clients are requesting to establish TCP connections (using the CONNECT method [HTTP]) and UDP connections (using UDP proxying [CONNECT-UDP]) to a target server. This target server can be specified using either a hostname or an IP address. When using a name instead of an IP address, the forward proxy locally performs DNS resolution to resolve the name to an IPv4 or IPv6 address using A or AAAA queries.

Clients of forward proxies currently don't have visibility into the DNS resolution that is performed on the proxy. If available, this information could be used by clients to help make various decisions that are influenced by IP addresses and CNAME chains. For example, some clients classify specific names and IP addresses as being used for collecting data to track users (which can be used to influence policies for HTTP cookies), or can recognize them as endpoints that ought to be blocked for features like ad blocking or malware blocking. Without this information, proxying using a forward proxy means that clients lose the ability to fully recognize servers based on IP addresses and CNAME chains.

It is possible for clients to perform DNS resolution before using a forward proxy, and proxy using IP addresses, but this has several

drawbacks: performing DNS without using the proxy can lead a privacy regression, or a performance regression if the addresses selected are not optimal for connectivity from the proxy; proxying by IP address prevents the proxy from selecting the best address ([HAPPY-EYEBALLS]); and if clients try to resolve via the proxy using DNS over HTTPS ([DOH]), they can incur a performance hit by requiring an extra round trip before being able to establish a connection.

This document allows clients to receive the IP address and CNAME chain received from DNS, without needing to perform DNS on the client, by including the information in a Proxy-Status parameter (Section 2).

1.1. Requirements

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. dns-used Parameter

The dns-used parameter's value is a String that contains one or more IP addresses and/or DNS names in a comma-separated list. The first item in the list SHOULD be the IP address that was resolved using DNS and was used to open connectivity to the next hop. The remaining items in the list SHOULD include all names received in CNAME records [DNS] or AliasMode SVCB or HTTPS records [SVCB] during the course of resolving the address. Since DNS names can include comma (,) characters in them, any commas that appear in a DNS names MUST be represented using a percent-encoded %2C value instead.

For example:

```
Proxy-Status: proxy.example.net; next-hop=target.example.com
    dns-used="2001:db8::1,tracker.example.com."
```

indicates that proxy.example.net, which used target.example.com as the next hop for this request, used the IP address "2001:db8::1" to connect to the target, and encountered the CNAME "tracker.example.com." in DNS resolution chain. Note that while this example includes both the next-hop and dns-used parameters, dns-used can be included without including next-hop.

The dns-used parameter only applies when DNS was used to resolve the next hop's name, and does not apply in all situations. Clients can use the information in this parameter to determine how to use the

connection established through the proxy, but need to gracefully handle situations in which this parameter is not present.

3. Security Considerations

The dns-used parameter does not include any DNSSEC information or imply that DNSSEC was used. The information included in the parameter can only be trusted to be valid insofar as the client trusts its proxy to provide accurate information. This information is intended to be used as a hint, and SHOULD NOT be used for making security decisions about the identity resource access through the proxy.

4. IANA Considerations

This document registers the "dns-used" parameter in the "HTTP Proxy-Status Parameters" registry <https://www.iana.org/assignments/http-proxy-status>.

Name: dns-used

Description: A string containing the IP address used to establish the proxied connection and the chain of CNAMEs that led to this IP address.

Reference: This document

5. References

5.1. Normative References

[CONNECT-UDP] Schinazi, D., "Proxying UDP in HTTP", RFC 9298, DOI 10.17487/RFC9298, August 2022, <https://www.rfc-editor.org/rfc/rfc9298>.

[DNS] Barr, D., "Common DNS Operational and Configuration Errors", RFC 1912, DOI 10.17487/RFC1912, February 1996, <https://www.rfc-editor.org/rfc/rfc1912>.

[HTTP] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[PROXY-STATUS] Nottingham, M. and P. Sikora, "The Proxy-Status HTTP Response Header Field", RFC 9209, DOI 10.17487/RFC9209, June 2022, <https://www.rfc-editor.org/rfc/rfc9209>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/

RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[SVCB] Schwartz, B. M., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-10, 24 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-10>.

5.2. Informative References

[DOH] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/rfc/rfc8484>.

[HAPPY-EYEBALLS] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/rfc/rfc8305>.

Author's Address

Tommy Pauly
Apple, Inc.

Email: tpauly@apple.com