Workgroup: Network Working Group
Internet-Draft:
draft-pauly-httpbis-alias-proxy-status-00
Published: 30 November 2022
Intended Status: Standards Track
Expires: 3 June 2023
Authors: T. Pauly
Apple, Inc.

HTTP Proxy-Status Parameter for Next-Hop Aliases

Abstract

This document defines an HTTP Proxy-Status Parameter that contains a list of aliases received over DNS when establishing a 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 3 June 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.

[PROXY-STATUS] defines a next-hop parameter, which can contain a hostname, IP address, or alias of the next hop. This parameter can contain only one such item, so it cannot be used to communicate a chain of aliases encountered during DNS resolution when connecting to the next hop.

Knowing the full chain of aliases that were used during DNS resolution is particularly useful for clients of forward proxies, in which the client is requesting to connect to a specific target hostname using the CONNECT method [HTTP] or UDP proxying [CONNECT-UDP]. DNS aliases can be used to "cloak" hosts that perform tracking or malicious activity behind more innocuous hostnames, and clients such as web browsers use the chain of DNS aliases to influence behavior like cookie usage policies [COOKIES] or blocking of malicious hosts.

This document allows clients to receive the chain of DNS aliases for the next hop by including the list of names in a new next-hop-aliases Proxy-Status parameter.

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. next-hop-aliases Parameter

The next-hop-aliases parameter's value is a String that contains one or more DNS names in a comma-separated list. The items in the list include all names received in CNAME records [DNS] or AliasMode SVCB or HTTPS records [SVCB] during the course of resolving the next hop's hostname using DNS. 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=2001:db8::1
    next-hop-aliases="tracker.example.com.,service1.example-cdn.com."
```

indicates that proxy.example.net, which used the IP address "2001:db8::1" as the next hop for this request, encountered the CNAMEs "tracker.example.com." and "service1.example-cdn.com" in the DNS resolution chain. Note that while this example includes both the next-hop and next-hop-aliases parameters, next-hop-aliases can be included without including next-hop.

The next-hop-aliases 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 next-hop-aliases 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 "next-hop-aliases" parameter in the "HTTP Proxy-Status Parameters" registry <https://www.iana.org/assignments/http-proxy-status>.

Name: next-hop-aliases

Description:

A string containing one or more DNS alises used to establish a proxied connection to the next hop.

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-11, 11 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-11>.

5.2. Informative References

[COOKIES] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011, <https://www.rfc-editor.org/rfc/rfc6265>.

Author's Address

Tommy Pauly
Apple, Inc.

Email: tpauly@apple.com