Workgroup:
Multiplexed Application Substrate over QUIC Encryption
Internet-Draft:
draft-schwartz-masque-access-descriptions-00
Published: 7 April 2022
Intended Status: Standards Track
Expires: 9 October 2022
Authors:
B. M. Schwartz
Google LLC

HTTP Access Service Description Objects

Abstract

HTTP proxies can operate several different kinds of access services. This specification provides a format for identifying a collection of such services.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-schwartz-masque-access-descriptions/.

Source for this draft and an issue tracker can be found at https://github.com/bemasc/access-services.

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 9 October 2022.

Copyright Notice

Table of Contents

1. Introduction

In HTTP/1.1, forward proxy service was originally defined in two ways: absolute-uri request form (encrypted at most hop-by-hop), and HTTP CONNECT (potentially encrypted end-to-end). Both of these services were effectively origin-scoped: the access service was a property of the origin, not associated with any particular path.

Recently, a variety of new standardized proxy-like services have emerged for HTTP. These new services are defined by a URI template or path, allowing distinct instances of the same service type to be served by a single origin. These services include:

- DNS over HTTPS [RFC8484]

- CONNECT-UDP [I-D.draft-ietf-masque-connect-udp]

- CONNECT-IP [I-D.draft-ietf-masque-connect-ip]

- Oblivious HTTP [I-D.draft-ietf-ohai-ohttp]

This specification provides a unified format for describing a collection of such access services, and a mechanism for reaching such services when the initial information contains only an HTTP origin.

2. Conventions and Definitions

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.

3. Format

An access service collection is defined by a JSON dictionary containing keys specified in the corresponding registry (Section 6). Inclusion of each key is **OPTIONAL**.

The "dns", "udp", and "ip" keys are each defined to hold a JSON dictionary containing the key "template" with a value that is a URI template suitable for configuring DNS over HTTPS, CONNECT-UDP, or CONNECT-IP, respectively.

The "ohttp" key contains a dictionary with either or both of these keys:

- "proxy", containing a dictionary with a "template" key indicating the Oblivious Proxy's resource mapping. The template **MUST** contain a "request_uri" variable indicating the Oblivious Request Resource.

- "request", containing a dictionary with a "uri" key indicating the Oblivious Request Resource and a "key" key conveying its KeyConfig in base64.

If the Access Description is for a general-purpose proxy, all Oblivious Request Resources and Targets (respectively) are presumed to be supported; otherwise the supported Resources and Targets must be understood from context (but see Section 4).

3.1. Examples

```
{
  "dns": {
    "template": "https://doh.example.com/dns-query{?dns}",
  },
  "udp": {
    "template":
        "https://proxy.example.org/masque{?target_host,target_port}"
  },
  "ip": {
    "template": "https://proxy.example.org/masque{?target,ip_proto}"
  },
  "ohttp": {
    "proxy": {
      "template": "https://proxy.example.org/ohttp{?request_uri}"
    }
  }
}
```

Figure 1: A proxy with UDP, IP, DNS, and Oblivious HTTP support

```
{
  "dns": {
    "template": "https://doh.example.com/dns-query{?dns}",
  },
  "ohttp": {
    "request": {
      "uri": "https://example.com/ohttp/",
      "key": "(KeyConfig in Base64)"
    }
  }
}
```

Figure 2: An Oblivious DNS over HTTPS service

4. Discovery from an Origin

In cases where the HTTP access service is identified only by an origin (e.g. when configured as a Secure Web Proxy), operators can publish an associated access service collection at the path "/.well-known/access-services", with the Content-Type "application/json".

When the "ohttp.request" URI appears in an Access Description at this location, all URIs on this origin (except the Oblivious Request URI) are presumed to be reachable as Oblivious Request Targets.

Clients **MAY** fetch this Access Description and use the indicated services (in addition to any origin-scoped services) automatically. Clients **SHOULD** use the description only while it is fresh according to its HTTP cache lifetime, refreshing it as needed.

5. Security Considerations

TODO Security

6. IANA Considerations

IANA is requested to open a Specification Required registry entitled "HTTP Access Service Descriptors", with the following initial contents:

Key	Specification
dns	(This document)
udp	(This document)
ip	(This document)
ohttp	(This document)

Table 1

IANA is requested to add the following entry to the "Well-Known URIs" registry

URI Suffix	Change Controller	Reference	Status	Related Information
access-services	IETF	(This document)	provisional	Sub-registry at (link)

Table 2

7. Normative References

[I-D.draft-ietf-masque-connect-ip] Pauly, T., Schinazi, D., Chernyakhovsky, A., Kuehlewind, M., and M. Westerlund, "IP Proxying Support for HTTP", Work in Progress, Internet-Draft, draft-ietf-masque-connect-ip-01, 4 March 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-masque-connect-ip-01>.

[I-D.draft-ietf-masque-connect-udp] Schinazi, D., "UDP Proxying Support for HTTP", Work in Progress, Internet-Draft, draft-ietf-masque-connect-udp-08, 21 March 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-masque-connect-udp-08>.

[I-D.draft-ietf-ohai-ohttp] Thomson, M. and C. A. Wood, "Oblivious HTTP", Work in Progress, Internet-Draft, draft-ietf-ohai-ohttp-01, 15 February 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-01>.

[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>.

[RFC8484] 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>.

Acknowledgments

TODO acknowledge.

Author's Address

Benjamin M. Schwartz
Google LLC

Email: bemasc@google.com