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 21 April 2023.

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,
allowing distinct instances of the same service type to be served by
a single origin. These services include:

  *DNS over HTTPS [RFC8484]

  *CONNECT-UDP [RFC9298]

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

  *Modern HTTP Proxies [I-D.draft-schwartz-modern-http-proxies]

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 7). Inclusion of each key is **OPTIONAL**. The corresponding media type is application/access-services+json.

The initially defined keys are "http", tcp", "dns", "udp", and "ip". Each of these keys holds a JSON dictionary containing the key "template" with a value that is a URI template suitable for configuring a Modern HTTP proxy, Modern TCP Transport Proxy, DNS over HTTPS, CONNECT-UDP, or CONNECT-IP, respectively. (Future keys might hold other JSON types.)

If the Access Description is for a general-purpose proxy, all proxy targets are presumed to be supported. Otherwise, the supported targets must be understood from context.

```
{
  "http": {
    "template": "https://proxy.example.org/http{?target_uri}"
  },
  "tcp": {
    "template":
        "https://proxy.example.org/tcp{?target_host,tcp_port}"
  },
  "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}"
  }
}
```

Figure 1: An example proxy with many supported services

4. Client Authentication

General-purpose clients of this specification **SHOULD** also implement support for Popup Authentication [I-D.draft-schwartz-httpapi-popup-authentication] when fetching the Access Description. If Popup Authentication produced any Authorization or Cookie headers for the Access Description, the client **MUST** also apply those headers to any HTTP requests made using the included templates (subject to proxy-specific modifications, see Section 4.3 of [I-D.draft-schwartz-httpapi-popup-authentication]). These headers are applied even if the Access Description and the included services are on different HTTP origins.

This arrangement allows the use of Access Descriptions to describe access-controlled services, and avoids asking the user to authenticate separately with each service.

5. 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/access-services+json".

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.

6. Security Considerations

TODO Security

7. IANA Considerations

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

Key	Specification
http	(This document)
tcp	(This document)
dns	(This document)
udp	(This document)
ip	(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

IANA is requested to add the following entry to the "application" sub-registry of the "Media Types" registry:

Name	Template	Reference
access-services+json	application/access-services+json	(This document)

Table 3

TODO: Full registration template for this Media Type.

8. Normative References

[I-D.draft-ietf-masque-connect-ip]
Pauly, T., Schinazi, D., Chernyakhovsky, A., Kühlewind, M., and M. Westerlund, "IP Proxying Support for HTTP", Work in Progress, Internet-Draft, draft-ietf-masque-connect-ip-03, 27 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-masque-connect-ip-03>.

[I-D.draft-schwartz-httpapi-popup-authentication]
Schwartz, B. M., "Interactive Authentication of Non-Interactive HTTP Requests", Work in Progress, Internet-Draft, draft-schwartz-httpapi-popup-authentication-00, 17 October 2022, <https://datatracker.ietf.org/doc/html/draft-schwartz-httpapi-popup-authentication-00>.

[I-D.draft-schwartz-modern-http-proxies]
Schwartz, B. M., "Modernizing HTTP Forward Proxy Functionality", Work in Progress, Internet-Draft, draft-schwartz-modern-http-proxies-00, 14 October 2022, <https://datatracker.ietf.org/doc/html/draft-schwartz-modern-http-proxies-00>.

[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>.

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

Acknowledgments

TODO acknowledge.

Author's Address

Benjamin M. Schwartz
Google LLC

Email: bemasc@google.com