Workgroup: httpbis
Internet-Draft:
draft-wood-httpbis-ech-coalescing-00
Published: 7 March 2022
Intended Status: Standards Track
Expires: 8 September 2022
Authors: C. A. Wood
Cloudflare

HTTP Connection Reuse Based on TLS Encrypted ClientHello

Abstract

This document specifies new criteria under which HTTP/2 clients may reuse connections. It updates [RFC7540].

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/chris-wood/draft-wood-httpbis-ech-coalescing.

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 8 September 2022.

Copyright Notice

Table of Contents

1. Introduction

The HTTP/2 connection reuse policy requires is stated as follows:

Connections that are made to an origin server, either directly or through a tunnel created using the CONNECT method (Section 8.3), MAY be reused for requests with multiple different URI authority components. A connection can be reused as long as the origin server is authoritative (Section 10.1). For TCP connections without TLS, this depends on the host having resolved to the same IP address.

For "https" resources, connection reuse additionally depends on having a certificate that is valid for the host in the URI. The certificate presented by the server MUST satisfy any checks that the client would perform when forming a new TLS connection for the host in the URI.

Thus, HTTPS connections require that the target resource hostname resolve to an IP address that matches that of the candidate connection for coalescing. This IP address match ensures that clients connect to the same service. If a server changes IP addresses as a means of mitigating hostname-to-IP bindings, clients are less likely to reuse connections. This can have performance problems, due to requiring an extra connection setup phase, as well as privacy problems.

In short, using unauthenticated IP addresses as a signal for connection reuse is fragile. This document relaxes this requirement and introduces another signal based on HTTPS RR answer contents [HTTPS-RR].

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. ECH-Based Coalescing Policy

The HTTPS RR [HTTPS-RR] is a new resource record used for conveying service information about a HTTPS endpoint to clients. Some of this information includes, for example, TLS Encrypted ClientHello (ECH) [TLS-ECH] public key material. The set of hosts behind the same ECH client-facing service provider that share the same ECH and TLS configuration information is referred to as the anonymity set. Client-facing servers SHOULD deploy ECH in such a way so as to maximize the size of the anonymity set where possible. This means client-facing servers should use the same ECH configuration (ECHConfig) for as many hosts as possible.

This type of deployment model means that a given ECHConfig uniquely identifies a given service provider. As a result, clients can use it as a signal to determine if a given resource is hosted by the same service provider. Thus, the HTTP/2 connection reuse policy is modified to use this signal as follows:

> Connections that are made to an origin server, either directly or through a tunnel created using the CONNECT method (Section 8.3), MAY be reused for requests with multiple different URI authority components. A connection can be reused as long as the origin server is authoritative (Section 10.1). For TCP connections without TLS, this depends on the host having resolved to the same service provider. Clients may implement this check in one of two ways: (1) by comparing for equality the resolved IP address to that of the original connection, or (2) by comparing for equality the "ech" SvcParamValue in the resolved HTTPS RR answer. For the latter case, the original connection MUST have successfully used the "ech" parameter to negotiate TLS ECH.

4. HTTP/3 Reuse

The HTTP/3 connection reuse policy [HTTP3] does not require IP addresses to match. However, as HTTP/3 is based on UDP, some clients may fall back to HTTP/2 over TCP in networks where UDP is blocked or otherwise inoperable. Thus, the policy described in this document only applies to HTTP/2.

5. Security Considerations

Existing coalescing policies do not require IP address authentication via DNSSEC. Thus, an adversary which can spoof A or AAAA responses can equally spoof HTTPS responses and ECHConfigList values.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[HTTPS-RR] Schwartz, B., 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-08, 12 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-08>.

[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>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/rfc/rfc7540>.

[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>.

[TLS-ECH] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-14, 13 February 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-14>.

7.2. Informative References

[HTTP3] Bishop, M., "Hypertext Transfer Protocol Version 3 (HTTP/3)", Work in Progress, Internet-Draft, draft-ietf-quic-http-34, 2 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-quic-http-34>.

Acknowledgments

This document was improved based on feedback from David Benjamin, Tommy Pauly, and Martin Thomson.

Author's Address

Christopher A. Wood
Cloudflare

Email: caw@heapingbits.net