Network Working Group
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

D. Schinazi
Google LLC
2 March 2026

The MASQUE Architecture
draft-schinazi-masque-proxy-08

Abstract

MASQUE (Multiplexed Application Substrate over QUIC Encryption) is a set of protocols and extensions to HTTP that allow proxying all kinds of Internet traffic over HTTP. This document describes the architectural principles behind MASQUE, and the properties that MASQUE can provide.

About This Document

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

The latest revision of this draft can be found at https://davidschinazi.github.io/masque-drafts/draft-schinazi-masque-proxy.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-schinazi-masque-proxy/.

Source for this draft and an issue tracker can be found at https://github.com/DavidSchinazi/masque-drafts.

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 September 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

In the early days of HTTP ([HTTP])), requests and responses weren’t encrypted. In order to add features such as caching, HTTP proxies were developed to parse HTTP requests from clients and forward them on to other HTTP servers. As SSL/TLS ([TLS]) became more common, the CONNECT method was introduced ([CONNECT]) to allow proxying SSL/TLS over HTTP. That gave HTTP the ability to create tunnels that allow proxying any TCP-based protocol. While non-TCP-based protocols were always prevalent on the Internet, the large-scale deployment of QUIC ([QUIC]) meant that TCP no longer represented the majority of Internet traffic. Simultaneously, the creation of HTTP/3 ([HTTP/3]) allowed running HTTP over a non-TCP-based protocol. In particular, QUIC allows disabling loss recovery ([DGRAM]) and that can then be used in HTTP ([HTTP-DGRAM]). This confluence of events created both the possibility and the necessity for new proxying technologies in HTTP. This led to the creation of MASQUE (Multiplexed Application Substrate over QUIC Encryption) in 2019.

2. Architectural Principles

Fundamentally, the main design choice for MASQUE was to run atop HTTP. While this choice was initially motivated by privacy benefits (making it harder to distinguish MASQUE traffic from Web browsing), it also facilitated the deployment of MASQUE given the wide availability of HTTP implementations.

2.1. Benefits of HTTP

A large number of Internet-connected services use HTTP. That has led to widespread implementation and adoption of HTTP. For existing deployments of HTTP, adding MASQUE capabilities was possible without reimplementing security or cryptographic protocols, as would have been necessary for other proxying technologies. Similarly, many aspects of the HTTP ecosystem, such as Denial-of-Service protection, load balancing, and monitoring were reused with minimal changes.

Another benefit is the ease of integration with other components of HTTP (such as HTTP Authentication) and extension points (such as HTTP header fields).

2.2. Capabilities

MASQUE allows proxying UDP ([CONNECT-UDP]), IP ([CONNECT-IP]), and even Ethernet ([CONNECT-ETHERNET]) over HTTP. There are also a variety of extensions to these MASQUE protocols to support a wide range of proxying needs.

In the rest of this document, we use the term "MASQUE proxy" to refer to an HTTP proxy (as defined in Section 3.7 of [HTTP]) that implements MASQUE capabilities.

2.3. Privacy Protections

There are currently multiple usage scenarios that can benefit from using MASQUE.

2.3.1. Protection from Web Servers

Connecting directly to Web servers allows them to access the public IP address of the user. There are many privacy concerns relating to user IP addresses ([IP-PRIVACY]). Because of these, many user agents would rather not establish a direct connection to Web servers. They can do that by running their traffic through a MASQUE proxy. The Web server will only see the IP address of the MASQUE proxy, not that of the client.

2.3.2. Protection from Network Providers

Some users may wish to obfuscate the destination of their network traffic from their network provider. This prevents network providers from using data harvested from this network traffic in ways the user did not intend.

2.3.3. Partitioning

While routing traffic through a MASQUE proxy reduces the network provider’s ability to observe traffic, that information is transfered to the proxy operator. This can be suitable for some threat models, but for the majority of users transferring trust from their network provider to their proxy (or VPN) provider is not a meaningful security improvement.

There is a technical solution that allows resolving this issue: it is possible to nest MASQUE tunnels such that traffic flows through multiple MASQUE proxies. This has the advantage of partitioning sensitive information to prevent correlation [PARTITION].

Though the idea of nested tunnels dates back decades ([TODO]), MASQUE now allows running HTTP/3 end-to-end from a user agent to an origin via multiple nested CONNECT-UDP tunnels. The proxy closest to the user can see the user’s IP address but not the origin, whereas the other proxy can see the origin without knowing the user’s IP address. If the two proxies are operated by non-colluding entities, this allows hiding the user’s IP address from the origin without the proxies knowing the user’s browsing history.

2.3.4. Obfuscation

The fact that MASQUE is layered over HTTP makes it much more resilient to detection. To network observers, the unencrypted bits in a QUIC connection used for MASQUE are indistinguishable from those of a regular Web browsing connection. Separately, if paired with a non-probeable HTTP authentication scheme (e.g., [CONCEALED-AUTH]), any Web server can also become a MASQUE proxy while remaining indistinguishable from a regular Web server. This defeats detection tools that operate solely on packet formats.

However, it is still possible to perform statitiscal analyses on the encrypted data. There exist commercially available products that are able to identify visited websites based solely on the timing and size of encrypted packets. While MASQUE increases the cost of such traffic analysis efforts, it doesn’t prevent them from being used at scale.

MASQUE implementations can leverage the ability for HTTP/2 ([HTTP/2]), HTTP/3, TLS, or QUIC to introduce padding inside the encryption. That enables many defensive strategies such as ensuring that all packets are the same size, or introducing variable amounts of cover traffic. From a theoretical perspective, sending data at a constant bitrate is the only way to fully prevent statistical analysis, but it likely introduces too much overhead to be deployable at scale. Finding padding strategies that balance resistance against statistical analysis with overheads remains an open research problem.

3. Related Technologies

This section discusses how MASQUE fits in with other contemporary privacy-focused IETF protocols.

3.1. OHTTP

Oblivious HTTP ([OHTTP]) uses a cryptographic primitive ([HPKE]) that is more lightweight than TLS, making it a great fit for decorrelating HTTP requests. In traditional Web browsing, the user agent will often make many requests to the same origin (e.g., to load HTML, style sheets, images, scripts) and those requests are correlatable since the origin can include identifying query parameters to join separate requests. In such scenarios, MASQUE is a better fit since it operates at the granularity of a connection. However, there are scenarios where a user agent might want to make non-correlatable requests (e.g., to anonymously report telemetry); for those, OHTTP provides better efficiency than using MASQUE with a separate connection per request. While OHTTP and MASQUE are separate technologies that serve different use cases, they can be colocated on the same HTTP server that acts as both a MASQUE proxy and an OHTTP Relay.

3.2. DoH

DNS over HTTPS ([DoH]) allows encrypting DNS traffic by sending it through an encrypted HTTP connection. Colocating a DoH server with a MASQUE IP proxy provides better performance than using DNS over port 53 inside the encrypted tunnel.

4. Security Considerations

Implementers of a MASQUE proxy need to review the Security Considerations of the documents referenced by this one.

5. IANA Considerations

This document has no IANA actions.

6. Informative References

[CONCEALED-AUTH]
Schinazi, D., Oliver, D., and J. Hoyland, "The Concealed HTTP Authentication Scheme", RFC 9729, DOI 10.17487/RFC9729, February 2025, <https://www.rfc-editor.org/rfc/rfc9729>.

[CONNECT] Khare, R. and S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC 2817, DOI 10.17487/RFC2817, May 2000, <https://www.rfc-editor.org/rfc/rfc2817>.

[CONNECT-ETHERNET]
Sede単o, A., "Proxying Ethernet in HTTP", Work in Progress, Internet-Draft, draft-ietf-masque-connect-ethernet-08, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-masque-connect-ethernet-08>.

[CONNECT-IP]
Pauly, T., Ed., Schinazi, D., Chernyakhovsky, A., K端hlewind, M., and M. Westerlund, "Proxying IP in HTTP", RFC 9484, DOI 10.17487/RFC9484, October 2023, <https://www.rfc-editor.org/rfc/rfc9484>.

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

[DGRAM] Pauly, T., Kinnear, E., and D. Schinazi, "An Unreliable Datagram Extension to QUIC", RFC 9221, DOI 10.17487/RFC9221, March 2022, <https://www.rfc-editor.org/rfc/rfc9221>.

[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>.

[HPKE] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/rfc/rfc9180>.

[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>.

[HTTP-DGRAM]
Schinazi, D. and L. Pardue, "HTTP Datagrams and the Capsule Protocol", RFC 9297, DOI 10.17487/RFC9297, August 2022, <https://www.rfc-editor.org/rfc/rfc9297>.

[HTTP/2] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/rfc/rfc9113>.

[HTTP/3] Bishop, M., Ed., "HTTP/3", RFC 9114, DOI 10.17487/RFC9114, June 2022, <https://www.rfc-editor.org/rfc/rfc9114>.

[IP-PRIVACY]
Finkel, M., Lassey, B., Iannone, L., and B. Chen, "IP Address Privacy Considerations", Work in Progress, Internet-Draft, draft-irtf-pearg-ip-address-privacy-considerations-01, 23 October 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-pearg-ip-address-privacy-considerations-01>.

[OHTTP] Thomson, M. and C. A. Wood, "Oblivious HTTP", RFC 9458, DOI 10.17487/RFC9458, January 2024, <https://www.rfc-editor.org/rfc/rfc9458>.

[PARTITION]
K端hlewind, M., Pauly, T., and C. A. Wood, "Partitioning as an Architecture for Privacy", RFC 9614, DOI 10.17487/RFC9614, July 2024, <https://www.rfc-editor.org/rfc/rfc9614>.

[QUIC] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[TLS] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[TODO] "find that 20 year old email about using nested CONNECT tunnels with SSL to improve privacy".

Acknowledgments

MASQUE was originally inspired directly or indirectly by prior work from many people. The author would like to thank Nick Harper, Christian Huitema, Marcus Ihlar, Eric Kinnear, Mirja Kuehlewind, Brendan Moran, Lucas Pardue, Tommy Pauly, Zaheduzzaman Sarker and Ben Schwartz for their input.

In particular, the probing resistance component of MASQUE came from a conversation with Chris A. Wood as we were preparing a draft for an upcoming Thursday evening BoF.

All of the MASQUE enthusiasts and other contributors to the MASQUE working group are to thank for the successful standardization of [HTTP-DGRAM], [CONNECT-UDP], and [CONNECT-IP].

The author would like to express immense gratitude to Christophe A., an inspiration and true leader of VPNs.

Author’s Address

David Schinazi
Google LLC
Email: dschinazi.ietf@gmail.com