Network Working Group
Internet-Draft
Updates: rfc8718 (if approved)
Intended status: Best Current Practice
Expires: 3 September 2026

E. Rescorla

R. Barnes

D. Schinazi

T. Pauly

2 March 2026

Security Requirements for the IETF Network
draft-rescorla-anonymous-network-00

Abstract

This document requires the network at the IETF plenary meeting to protect the security and privacy of its users.

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://ekr.github.io/draft-rescorla-anonymous-network/draft-rescorla-anonymous-network.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-rescorla-anonymous-network/.

Source for this draft and an issue tracker can be found at https://github.com/ekr/draft-rescorla-anonymous-network.

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

IETF meeting participants depend heavily on Internet access during the IETF plenary meeting. The venue selection process defined in [RFC8718] makes a functional network a mandatory criterion:

> It MUST be possible to provision Internet Access to the Facility and IETF Hotels that allows those attending in person to utilize the Internet for all their IETF, business, and day-to-day needs; in addition, there must be sufficient bandwidth and access for remote attendees. Provisions include, but are not limited to, native and unmodified IPv4 and IPv6 connectivity, and global reachability; there may be no additional limitation that would materially impact their Internet use. To ensure availability, it MUST be possible to provision redundant paths to the Internet.

A critical, but implicit requirement in this paragraph is that IETF participants need to be secure in their use of the Internet. It will clearly have a material impact on participants' Internet use if they cannot use the security technologies they require, or if accessing the IETF network requires them to reduce their security or privacy posture (e.g., by revealing sensitive information).

As expressed in [RFC7258], the IETF considers pervasive monitoring an attack, The IETF has a long history of developing protocols to protect the confidentiality and authenticity of Internet communications, such as IPsec, DNSSEC, TLS, and SSH. More recently, there has been a focus on protecting the identities of the endpoints to communication, e.g., MASQUE, OHAI, and ECH. The security properties of the IETF network should be aligned with these principles.

For example:

* IETF attendees often employ mechanisms such as IPsec, HTTPS, Oblivious HTTP, and TLS ECH to protect the security and privacy of their business and day-to-day Internet usage. If these security features cannot be used, attendees will not be able to use the Internet as they need to.

* IETF attendees typically expect that the IETF network will not collect more information about their usage of it than is technically necessary to operate the network. If IETF users need to authenticate in a way that their Internet traffic can be attributed to them by local or upstream network operators, this expectation would be violated, and attendees might not be willing or able to use the Internet under such circumstances.

This document updates the requirements of [RFC8718] to make these security requirements explicit.

1.1. 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.

2. Requirements

This document extends the mandatory criteria as follows:

> The IETF network MUST be compatible with widely-used Internet security technologies, and MUST NOT interfere with their usage. These properties MUST also hold for upstream networks. In other words, in addition to global reachability at the IP layer, the network must provide secure global reachability, in the sense of being able to securely connect to any other endpoint on the Internet using any widely-used security protocol.

This text is intended to ensure that IETF participants can continue to get the level of security that they require when they use the IETF network.

> The IETF network MUST NOT collect information about IETF participants' Internet usage beyond what is technically required to operate the network. If user-linked information needs to be collected, then it MUST NOT be disseminated beyond the immediate IETF network operational team, and MUST be deleted at the end of an IETF meeting.
>
> The IETF network MUST be accessible by any IETF participant without providing authentication information that is tied to their identity. If user-specific authentication is required, it MUST be possible for users to anonymously obtain an arbitrary number of credentials which are not linkable to their identity. The network SHOULD provide unauthenticated access or access via a shared credential if practicable.

This text is intended to maximize user privacy and forbid any authentication mechanisms which would make it possible to attribute traffic to a specific identifiable user.

3. Security Considerations

The requirement in this document enhances user security and privacy by reducing a network observer's ability to track user behavior. The requirement may make it more difficult to manage abusive behavior by network users, however, the IETF network currently routinely operates in a mode without any user-level authentication, so this requirement does not create a security regression.

4. IANA Considerations

This document has no IANA actions.

5. References

5.1. Normative References

[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>.

[RFC8718] Lear, E., Ed., "IETF Plenary Meeting Venue Selection Process", BCP 226, RFC 8718, DOI 10.17487/RFC8718, February 2020, <https://www.rfc-editor.org/rfc/rfc8718>.

5.2. Informative References

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/rfc/rfc7258>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Eric Rescorla
Email: ekr@rtfm.com

Richard Barnes
Email: rlb@ipv.sx

David Schinazi
Email: dschinazi.ietf@gmail.com

Tommy Pauly
Email: tpauly.ietf@gmail.com