SAAG
Internet-Draft
Intended status: Informational
Expires: 6 May 2026

X. Liu
R. Yang
Y. Zhang
Pengcheng Laboratory

2 November 2025

Zero trust standards in IETF: use cases and problem statement
draft-liu-saag-zt-problem-statement-00

Abstract

The traditional "castle-and-moat" security paradigm is no longer effective for some emerging scenarios, such as cloud services, remote workforces and intelligent agents. Zero trust (ZT) has emerged as the new paradigm, holding on the "never trust, always verify" principle, treats every single access request as untrudted and requires veficication.

While a high-level atchitectural guidance exists, notably from NIST in SP 800-207 where thtenants of zero trust are well interperated, the industry lacks the open, interoperable framework and protocol necessary for building multi-vendor zero trust practice enrironment. This document presents the problem statement for zero trust interoperability, outlines the key use cases, and argue for the need for standardization in the IETF. It discusses the possible scope for zero trust standardization work in the IETF, identifying which aspects are well suited for the IETF protocols and which are better addressed by other bodies. The aim of this document is to initiate a discussion in the IETF community on the necessity and prospective of promoting zero trust related work here.

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 6 May 2026.

Table of Contents

1. Introduction

Traditional network security was built on the assumption of that every entity inside the perimeter were trusted by default. This approach is increasingly ineffective in face of new use cases and sophisticateed attackers.

Zero Trust (ZT) offers a fundamentally different approach. As d efined in [NIST-SP-800-207], Zero Trust assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location. Instead, authentication and authorization are discrete, dynamic functions that must be performed before a session is established to an enterprise resource. This is a "never trust, always verify" model.

While this conceptual framework is powerful, its practical implementation is hampered by a lack of open standards. Today’s ZT solutions are largely proprietary, single-vendor ecosystems. An organization cannot easily use a Policy Enforcement Point (PEP) from one vendor with a Policy Decision Point (PDP) from another.

This document provides a gap analysis for zero trust standardization, as well as several typical use cases. In additon, it also discusses the scope of standardization of zero trust in the IETF.

2. Requirements Language

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. Terminology

This document adopts the core terminology defined in [NIST-SP-800-207].

Subject: An entity (e.g., user, device, service, application, AI agent) that requests access to a resource.

Resource: A data source, service, device, or network component that a subject wishes to access.

Policy Engine (PE): The component responsible for the ultimate decision to grant or deny access to a resource for a given subject.

Policy Administrator (PA): The component responsible for establishing and/or shutting down the communication path between a subject and a resource.

Policy Enforcement Point (PEP): A system responsible for enabling,

monitoring, and terminating connections between a subject and a resource. The PEP communicates with the PA to forward requests and/or receive policy updates.

Control Plane: The logical network of communication that is used to manage the ZTA. This includes communication between the PE, PA, and PEPs, as well as the collection of context and signals.

Data Plane: The logical network where subjects and resources communicate after access has been granted.

4. Use cases

In this section we consider several emerging use cases where standardized ZT protocols would provide significant value.

4.1. Use Case 1: Secure Remote Access for Enterprise Resources

A remote employee needs to access an internal application hosted in a private data center of an organization.

1. Subject: The employee’s user identity and the device identity.
2. Resource: The internal application.

4.2. Use case 2: secure service-to-service communication

A front-end web service running in a Kubernetes cluster in Cloud A needs to query a database service running in a VM in Cloud B.

1. Subject: The front-end web service, identified by a workload identity.
2. Resource: The database service.

4.3. Use Case 3: Granular Access to Third-Party SaaS Applications

An organization wants to enforce device posture checks before allowing employees to access a third-party SaaS application .

1. Subject: The employee and their device.
2. Resource: The SaaS CRM application.

4.4. Use Case 4: Secure Access for Autonomous AI Agents

An autonomous AI agent, acting on behalf of a user or system, needs to access a set of APIs to complete a task (e.g., booking travel).

1. Subject: The AI agent, possessing a cryptographically verifiable workload identity.

2. Resource: A set of airline, hotel, and payment gateway APIs.

5. Problem statement

The implementation of zero trust is hindered by several key problems that may be addressed by standardization.

5.1. Lack of interoperability

The core components of ZTA, PE, PA and PEP currently communicate with each other using proprietary protocols. Different components from different vendors can barely communicate and interoperate with each other. This makes an organization wishing to implenment ZTA system probably forced to source all components from one single vendor. This creates silos where the ZT system for employee access is completely separate from the ZT system for cloud service-to-service communication, even though the underlying principles are the same. A unified approach requires common standards.

5.2. Market Confusion

Without clear, protocol-level definitions and specifications, the term "zero trust" is often used as marketing buzzword rather than technology or product langauge. Products with different capabilities and features can be all labeled as "zero trust enabled". Standardization can enhance clarity by clearly document the requirements for components to participate in ZTA system from the protocol and funtionality level.

5.3. Gap Analysis

While the IETF and other SDOs have produced fundamental building blocks, there still lacks a complete, interoperable ZT standard framework. A significant gap exists between the available components and a functioning ZTA control plane. Specifically, the main gaps can be concluded as follows.

1. *A Standardized Control Plane Protocol:* This is the central gap. There is no standard protocol for a PEP to request an access decision from a PE, nor for the PE/PA to return a dynamic policy decision. Today, this critical interaction is implemented with proprietary REST APIs with vendor-specific data models.

2. *A Standardized Signal Exchange Protocol:* A PE’s decisions rely on continuous streams of context (signals). While RATS defines attestation formats, there is no standard protocol for how diverse sources (EDR systems, threat feeds, IdPs) publish these signals and how a PE consumes them. This prevents the creation of a multi- vendor "nervous system" for the ZTA.

3. *A Model for Dynamic, Fine-Grained Authorization:* OAuth scopes are often broad and long-lived. ZT demands just-in-time, least-privilege access. A standard is needed to model a request for, and issuance of, highly specific and ephemeral access rights (e.g., "grant subject X write access to record Y in database Z for the next 30 seconds").

4. *A framework for dynamic and continuous trust evaluation:* The core principle of Zero Trust is continuous verification. This implies a mechanism for dynamically evaluating the trustworthiness of a subject over time. While individual signals (like device posture or user location) are important, there is no standardized framework for aggregating these signals into a dynamic trust score or confidence level. Furthermore, there is no standard protocol for how this trust score is updated in near-real-time and communicated to the Policy Engine to influence access decisions. Defining such a framework would enable interoperable trust assessment modules and allow the PE to make more nuanced, risk-based decisions beyond a simple grant/deny.

6. Proposed Scope of Work for the IETF

To be successful, an IETF effort must have a clearly defined scope. We propose focusing on the communication interfaces between ZTA components, directly addressing the gaps identified in Section 5.3.

6.1. Control Plane Communication Protocol

The highest priority is to define a standard protocol for a PEP to request an access decision from a PE/PA and for the PE/PA to return a decision and policy configuration. This could be a new protocol or a profile of an existing one (e.g., using HTTP APIs with a well-defined JSON data model). It must specify how to represent the subject, resource, and context in a request, and how to represent grant, deny, or step-up authentication decisions in a response.

6.2. Dynamic Context and Signal Exchange Protocol

A ZTA's decisions are only as good as the signals it receives. A standardized protocol is needed for various sensors (e.g., EDR agents, threat intelligence feeds, IdPs) to publish signals to a centralized bus or directly to the PE. This would allow a PE to consume signals from multiple vendors' security tools. This work should align with and leverage concepts from the IETF RATS and SCITT working groups.

6.3. Authenticated Session Establishment and Management

While TLS provides a secure channel, ZTA introduces new challenges. Work could be done to standardize how a PA instructs a PEP to establish a session. This might involve profiling the use of existing protocols or defining mechanisms for securely delivering short-lived, session-specific credentials (e.g., tokens or certificates) to the subject and/or PEP as part of an access grant.

7. IANA Considerations

This memo includes no request to IANA.

8. References

8.1. 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/info/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/info/rfc8174>.

[NIST-SP-800-207] Rose, S., Borchert, O., Mitchell, S., and S. Connelly, "Zero Trust Architecture", August 2020, <https://csrc.nist.gov/publications/detail/sp/800-207/final>.

8.2. Informative References

Authors' Addresses

Xiang Liu
Pengcheng Laboratory
No.2 Xingke 1 Street
Shenzhen
518055
China
Email: liux15@pcl.ac.cn

Rongwei Yang
Pengcheng Laboratory
No.2 Xingke 1 Street
Shenzhen
518055
China
Email: yangrw@pcl.ac.cn

Yu Zhang
Pengcheng Laboratory
No.2 Xingke 1 Street
Shenzhen
518055
China
Email: zhangy08@pcl.ac.cn