NIST Special Publication
NIST SP 800-207A

A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments

Ramaswamy Chandramouli
Zack Butcher

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207A

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-207A

A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments

Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Zack Butcher
Tetrate, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207A

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2023-09-08

How to Cite this NIST Technical Series Publication:

Chandramouli R, Butcher Z (2023) A Zero-Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-207A. https://doi.org/10.6028/NIST.SP.800-207A

Author ORCID iDs

Ramaswamy Chandramouli: 0000-0002-7387-5858

Contact Information

sp800-207A-comments@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

One of the basic tenets of zero trust is to remove the implicit trust in users, services, and devices based only on their network location, affiliation, and ownership. NIST Special Publication 800-207 has laid out a comprehensive set of zero trust principles and referenced zero trust architectures (ZTA) for turning those concepts into reality. A key paradigm shift in ZTAs is the change in focus from security controls based on segmentation and isolation using network parameters (e.g., Internet Protocol (IP) addresses, subnets, perimeter) to identities. From an application security point of view, this requires authentication and authorization policies based on application and service identities in addition to the underlying network parameters and user identities. This in turn requires a platform that consists of Application Programming Interface (API) gateways, sidecar proxies, and application identity infrastructures (e.g., Secure Production Identity Framework for Everyone [SPIFFE]) that can enforce those policies irrespective of the location of the services or applications, whether on-premises or on multiple clouds. The objective of this publication is to provide guidance for realizing an architecture that can enforce granular application-level policies while meeting the runtime requirements of ZTA for multi-cloud and hybrid environments.

Keywords

egress gateway; identity-tier policies; ingress gateway; microservices; multi-cloud; network-tier policies; service mesh; sidecar proxy; SPIFFE; transit gateway; zero trust; zero trust architecture.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Figures

Acknowledgments

The authors would like to express their thanks to Isabel Van Wyk of NIST for her detailed editorial review of the public comment version as well as the final publication.

Executive Summary

The principles of zero trust, as described in NIST Special Publication (SP) 800-207, have become the guiding markers for developing secure zero trust architecture. A well-established class of applications is the cloud-native application class. The generally accepted characterization of a cloud-native application includes the following:

- The application is made up of a set of loosely coupled components called microservices. Each of the microservices can be hosted on different physical or virtual machines (VMs) and even be geographically distributed (e.g., within several facilities that belong to the enterprise, such as the headquarters, branch offices, and in various cloud service provider environments).
- Any transaction involving the application may also involve one or more inter-service (microservice) calls across the network.
- A widespread feature (though not necessarily a requirement for cloud-native applications) is the presence of a software platform called the service mesh that provides an integrated set of all application services (e.g., services discovery, networking connections, communication resilience, and security services like authentication and authorization).

The realization of a zero trust architecture for the above class of cloud-native applications requires a robust policy framework. In order to follow zero trust principles, the constituent polices in the framework should consider the following scenario:

- There should not be implicit trust in users, services, or devices based exclusively on their network location, affiliation, or ownership. Hence, policy definitions and associated security controls based on the segmentation or isolation of networks using network parameters (e.g., IP addresses, subnets, perimeter) are insufficient. These policies fall under the classification of network-tier policies.
- To ensure the presence of zero trust principles throughout the entire application, network-tier policies must be augmented with policies that establish trust in the identity of the various participating entities (e.g., users and services) irrespective of the location of the services or applications, whether on-premises or on multiple clouds.

This document provides guidance for realizing a zero trust architecture that can enforce granular application-level policies for cloud-native applications. The guidance is anchored in the following:

- A combination of network-tier and identity-tier policies
- The components of cloud-native applications that enable the definition and deployment of those policies, such as edge, ingress, sidecar, and egress gateways; the creation, issuance, and maintenance of service identities; and the issuance of authentication and authorization tokens that carry user identities in the enterprise application infrastructure that encompasses multi-cloud and hybrid environments

1. Introduction

Zero trust (ZT) tenets or principles have been accepted as the guide markers for architecting all applications. There are several reasons why adherence to these tenets is critical for obtaining necessary security assurances, especially for cloud-native applications. The enterprise application environments for this class of applications are highly geographically distributed and span multiple cloud and on-premises environments (e.g., headquarters, enterprise-operated data centers, branch offices). Further, the user base consists of both remote and on-premises employees. These two features call for establishing trust in all of the data sources and computing services of the enterprise — irrespective of their location — through secure communication and the validation of access policies.

Apart from geographic distribution, another common feature of cloud-native applications is the presence of many microservices that are loosely coupled and collectively support business processes through extensive inter-service calls. This is augmented by an integrated infrastructure for providing all application services called the service mesh. These features emphasize the concept of identity for the various components of the application in the form of microservices as well as the users who access them through direct calls or clients (other services). This in turn highlights the critical need for authenticating these identities and for providing legitimate access on a per-session basis through a dynamic policy that takes the current status of the user, service, and requested resource into account.

The above requirements can only be met through a comprehensive policy framework. This document provides guidance for developing a policy framework that will form the foundation for realizing a zero trust architecture (ZTA) while incorporating zero trust principles into its design for cloud-native applications. The policy framework should also consist of a comprehensive set of policies that span all critical entities and resources in the application stack, including the network, network devices, users, and services.

1.1. Background — Zero Trust Principles and Zero Trust Architecture

A summary of the zero trust principles and the definition of a zero trust architecture, as described in SP 800-207, *Zero Trust Architecture* [1], are:

- Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users and resources. It is a set of security primitives rather than a particular set of technologies. Zero trust assumes that there is no implicit trust granted to user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or to endpoints (devices) based on their ownership (e.g., enterprise or personally owned). Zero trust focuses on protecting resources (e.g., devices, services, workflows, network accounts) rather than network segments, as the network location is no longer seen as the prime component to the security posture of the resource.
- A zero trust architecture uses zero trust principles to plan industrial and enterprise infrastructures and workflows.