



中华人民共和国国家标准

GB/T 43696—2024



网络安全技术 零信任参考体系架构

Cybersecurity technology—Zero trust reference architecture

2024-04-25 发布

2024-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 典型特征 1

5 参考体系架构 2

6 核心组件 2

 6.1 策略判决组件 2

 6.2 策略执行组件 3

7 支撑组件 3

 7.1 任务管理组件 3

 7.2 身份管理组件 3

 7.3 资源管理组件 3

 7.4 环境感知组件 3

 7.5 密码服务组件 3

参考文献 4

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：奇安信网神信息技术(北京)股份有限公司、中国科学院大学、中国信息通信研究院、中国科学院软件研究所、国家计算机网络应急技术处理协调中心、中国科学技术大学、国家信息技术安全研究中心、北京数字认证股份有限公司、公安部第三研究所、国家信息中心、飞天诚信科技股份有限公司、北京天融信网络安全技术有限公司、江苏易安联网络技术有限公司、国民认证科技(北京)有限公司、启明星辰信息技术集团股份有限公司、深圳竹云科技股份有限公司、格尔软件股份有限公司、海信集团控股股份有限公司、大唐高鸿信安(浙江)信息科技有限公司、腾讯科技(深圳)有限公司、深信服科技股份有限公司、北京芯盾时代科技有限公司。

本标准主要起草人：齐向东、吴云坤、张彬、刘勇、张泽洲、安锦程、荆继武、詹榜华、李新友、张立武、左晓栋、邬怡、韩永刚、金一、孟楠、赵泰、张严、刘丽敏、陈亮、李海玲、陈妍、夏冰冰、国强、黄卉、朱鹏飞、陆舟、刘治平、王龔、秦益飞、杨正权、李俊、韩少波、蒋蓉生、王文路、戴立伟、郑强、何晨迪、高雪松、郑驰、蔡东赞、訾然、孙悦。



网络安全技术 零信任参考体系架构

1 范围

本文件规定了零信任参考体系架构,描述了主体、资源、核心组件和支撑组件以及相互间的关系。
本文件适用于采用零信任体系架构的信息系统的规划、设计、开发、应用、评价。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

零信任 zero trust

一种以资源保护为核心的网络安全理念。

注:该理念认为主体访问资源时,无论主体和资源是否可信,主体和资源之间的信任关系都需要通过持续状态感知与动态信任评估,从零开始进行构建,以实施端到端安全的访问控制。

3.2

零信任体系架构 zero trust architecture

基于零信任建立的信息系统体系架构。

注:包括构成架构的系统组件,以及组件间关系。

3.3

主体 subject

发起访问请求的实体。

3.4

资源 resource

可供主体访问的对象。

4 典型特征

零信任体系架构具有以下典型特征。

- a) 持续状态感知:
持续对主体、资源、环境的相关信息采集、分析安全态势。
- b) 动态信任评估:
在主体访问资源的过程中,根据持续感知到的主体、资源、环境等安全态势的变化,不断进行信

任评估,维持或改变策略决定。

- c) 最小权限：
按照任务要求和策略决定,结合时间窗口和被访问资源粒度,对访问主体授予最小权限。
- d) 加密传输：
采用密码技术建立主体访问资源的端到端的数据安全信道。

5 参考体系架构

零信任参考体系架构由主体、资源、核心组件和支撑组件组成,如图 1 所示。

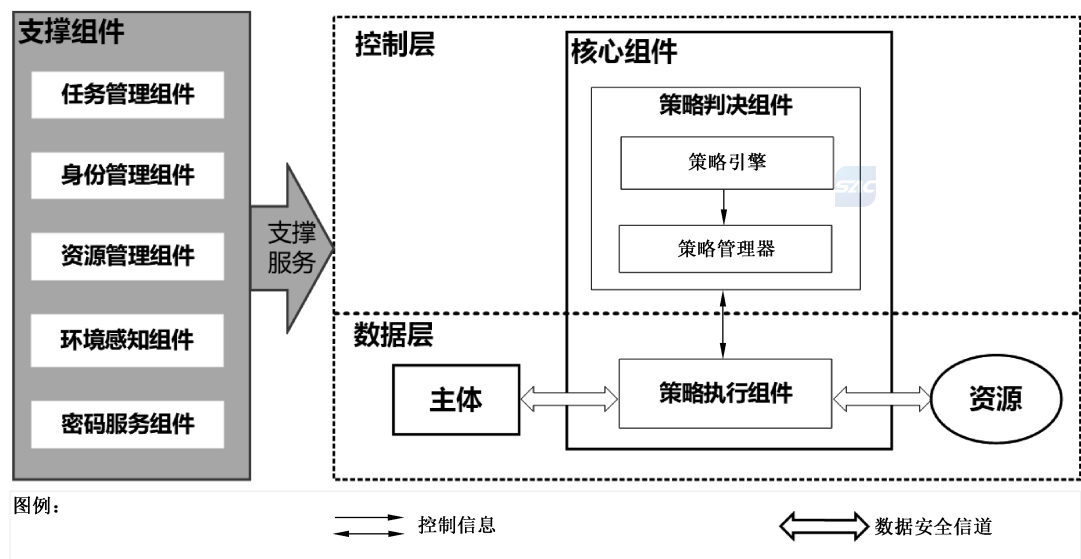


图 1 零信任参考体系架构

核心组件包括策略判决组件和策略执行组件,支撑组件包括任务管理组件、身份管理组件、资源管理组件、环境感知组件和密码服务组件。

主体是用户、设备、信息系统、应用软件等一种或多种的组合。

资源以数据为主,通常也包括设备、信息系统、应用软件、服务、功能接口等。

当主体访问资源时,根据任务管理组件提交的需求,利用身份管理组件、资源管理组件、环境感知组件提供的状态信息进行状态感知,由策略判决组件通过信任评估生成策略判决,策略执行组件执行策略判决,实现最小权限访问控制;在整个访问过程中,通过持续状态感知、动态信任评估、最小权限控制的循环过程,实施对被访问资源的保护。密码服务组件提供全过程密码服务保障。

控制层和数据层是两个逻辑层面。在控制层传输和处理控制信息,在数据层安全传输和处理数据。

6 核心组件

6.1 策略判决组件

策略判决组件由策略引擎和策略管理器组成,主要功能如下。

- a) 策略引擎:负责判决主体对资源的访问权限。根据安全策略和支撑组件提供的信息,持续进行信任评估,做出允许、拒绝或撤销的访问控制判决。
- b) 策略管理器:负责发布主体与资源之间连接的控制指令。依赖策略引擎做出的访问控制判决,向策略执行组件发布建立、维持或阻断数据安全信道的指令。

6.2 策略执行组件

- 策略执行组件在策略判决组件管理下,实施身份鉴别,控制主体与资源之间的数据安全信道。
- a) 身份鉴别:根据策略判决组件指令,与支撑组件协同,对主体实施身份鉴别。
 - b) 控制数据安全信道:按照策略管理器发布指令,启动、监控和终止主体和被授权资源之间的数据安全信道。

7 支撑组件

7.1 任务管理组件

协同主体访问事由,驱动主体访问资源的任务,包括任务目标、任务职责和任务流程等,对接实体权限,为主体、资源、核心组件和其他支撑组件提供关联任务生命周期管理服务、任务与资源权限协同服务、任务审批服务、任务鉴别服务、任务审计服务以及任务相关信息,包括主体任务属性信息、资源任务属性信息、任务状态信息、任务审批信息、任务审计信息等。

7.2 身份管理组件

为主体、资源、核心组件和其他支撑组件提供实体身份标识管理服务、实体身份属性关联服务、个人实体身份鉴别服务、设备身份鉴别服务、实体权限管理服务以及身份相关信息,包括实体身份标识、实体身份信息、实体属性信息、实体权限信息等。

7.3 资源管理组件



为主体、资源、核心组件和其他支撑组件提供数据资源管理服务、设备资源管理服务、网络资源管理服务、计算资源管理服务、应用资源管理服务、资源实体身份鉴别服务、资源属性关联服务、资源业务协同管理服务以及资源相关信息,资源分级分类信息、设备配置信息、资源身份信息、资源访问权限信息、资源访问上下文信息等。

资源管理以资源单元作为最小单位,若干资源单元组合为被访问资源。资源单元关联同一资源标识、具有统一资源属性、执行共同的安全策略。

7.4 环境感知组件

在主体访问资源过程中,通过采集网络流量、资产信息、日志、漏洞信息、用户行为、威胁信息等数据,分析访问过程中的网络行为、用户行为,为主体、资源、核心组件和其他支撑组件获取、理解、回溯、显示主体、资源和访问环境的状态变化和变化趋势。

7.5 密码服务组件

保障主体、资源、核心组件和其他支撑组件的实体身份真实性、数据的机密性和完整性、操作行为的不可否认性,为主体、资源、核心组件和其他支撑组件提供密码相关的网络和通信安全服务,设备和计算安全服务、应用和数据安全服务。

参 考 文 献

- [1] GB/T 11457—2006 信息技术 软件工程术语
 - [2] GB/T 18794.3—2003 信息技术 开放系统互连 开放系统安全框架 第3部分:访问控制
框架
 - [3] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求
 - [4] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
 - [5] GB/T 42453—2023 信息安全技术 网络安全态势感知通用技术要求
 - [6] ISO/IEC 24760-1:2019 IT security and privacy—A framework for identity management—
Part 1: Terminology and concepts
 - [7] ISO/IEC 24760-2:2015 Information technology—Security techniques—A framework for
identity management—Part 2: Reference architecture and requirements
 - [8] ISO/IEC 24760-3:2016 Information technology—Security techniques—A framework for
identity management—Part 3: Practice
 - [9] ISO/IEC 29146:2016 Information technology—Security techniques—A framework for ac-
cess management
 - [10] NIST SP 800-162 Guide to attribute based access control (ABAC) definition and consid-
erations
 - [11] NIST SP 800-207 Zero trust architecture
-

