

基于零信任的省级气象信息网络防护技术研究

刘晓波^{1,2†}, 冯洗¹, 张思睿¹, 郑秋生¹, 周武宁³

(1. 湖南省气象信息中心, 湖南 长沙 410118; 2. 气象防灾减灾湖南省重点实验室, 湖南 长沙 410118;

3. 奇安信科技集团股份有限公司, 湖南 长沙 410000)

摘 要: 随着省级气象部门对外服务统一出口要求, 系统和数据逐步集约化, 部分省级单位建立了专门对外提供数据服务的数据中台, 传统网络安全技术在当前新的业务形态和场景下显得捉襟见肘。零信任作为一种全新的网络安全理念, 为重构网络安全架构提供了理论指引。设计了一种基于零信任的适用于省级气象部门的安全架构体系, 并基于零信任构建了气象网络的可信访问通道解决数据访问管道安全问题, 提出了一种数据动态授权访问的方法解决气象数据安全访问授信问题, 给出终端可信空间方案解决端上数据泄露问题。

关键词: 零信任模型; 动态授权; 可信访问通道; 可信终端空间

中图分类号: TP393.08

文献标识码: A

Research on Provincial Meteorological Information Network Protection Technology Based on Zero Trust

LIU Xiaobo^{1,2†}, FENG Xian¹, ZHANG Sirui¹, ZHENG Qiusheng¹, ZHOU Wuning³

(1. Hunan Meteorological Information Center, Changsha, Hunan 410118, China;

2. Hunan Primary Laboratory of Meteorological Disaster Prevention and Reduction, Changsha, Hunan 410118, China;

3. Qi-Anxin Science and Technology Group Co., Ltd., Changsha, Hunan 410000, China)

Abstract: With the unified export requirements for external services of provincial meteorological departments, the system and data are gradually intensified, and some provincial units have established data centers dedicated to providing external data services, and traditional network security technology is strained under the current new business forms and scenarios. As a new concept of network security, zero trust provides theoretical guidance for reconstructing network security architecture. This paper designs a zero-trust-based security architecture applicable to provincial meteorological departments, constructs a trusted access channel of meteorological network based on zero-trust to solve the security problem of data access pipeline, proposes a method of dynamic data authorization access to solve the problem of meteorological data security access credit, and proposes a terminal trusted space scheme to solve the data leakage problem on the terminal.

Key words: zero trust model; dynamic authorization; trusted access channel; trusted terminal space

当前, 政企机构网络接入方式、接入设备类型越来越多样化, 网络边界变得越来越模糊, 各种突破内网边界的安全事件层出不穷, 传统的边界安全解决方案愈发难以应对这些新的挑战。为应对新 IT 时代的网络安全挑战, 零信任安全应运而生。零信任架构最早由约翰·金德维格(John Kinder-

vag) 在 2010 年提出^[1]。2014 年 Google 提出并实现了基于零信任构建的 BeyondCorp 架构, 为零信任架构提供了可靠的实践背书^[2]。

零信任是一种网络/数据安全的实体到实体的方法, 区别于传统安全方案只关注边界保护, 零信任更关注数据保护的架构方法^[3]。随着近年来零

信任领域在安全业界的逐步升温,国内零信任领域也开始形成相关的趋势和规模。2019 年 9 月,工信部在《关于促进网络安全产业发展的指导意见》中,明确将“零信任安全”列入网络安全重点突破的关键技术^[4]。腾讯在中国通信标准化协会(CCSA)立项《零信任安全技术安全框架》,奇安信等企业推出相应产品原型,全国网络安全标准化技术委员会发布首个零信任国家标准《信息安全技术 零信任参考体系架构》,可以看出零信任技术的先进性以及市场前景^[5]。

现阶段,我国一些大型政企机构对零信任的实践应用主要以特定场景为主,如远程办公场景、远程运维开发场景、内外网一体化接入场景等^[6]。在这些典型场景下,零信任技术主要用于替代原有传统网络安全技术,尤其是远程访问场景下基于零信任技术替换传统 VPN 方案常常作为零信任落地的切入点,这也充分说明零信任技术在保护数据和应用访问安全方面的先进性。为了更好地为政企数字化转型提供保障,越来越多的单位开始以零信任理念来升级传统网络安全架构。

1 零信任网络安全防护模型

1.1 零信任理论模型综述

零信任是一种端到端的网络安全模型,秉承“从不信任并始终验证”的安全原则,通过控制平面和数据平台相互分离的架构设计,在访问主体(人员、设备、应用、系统等)和访问客体(应用、接口、功能、数据等)之间构筑一道新的“边界”,通过对主客体之间持续动态的信任评估验证,最终实现端到端的安全访问。其理论模型如图 1 所示:

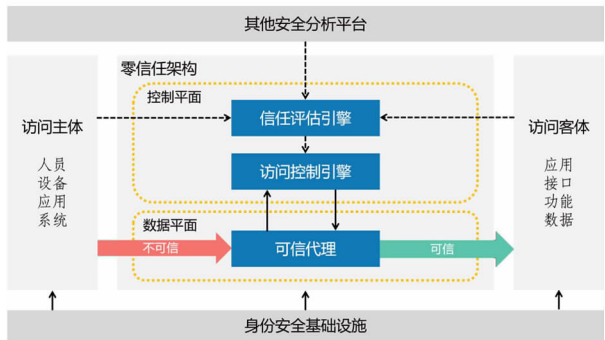


图 1 零信任理论模型

相较于传统安全模型而言,零信任模型具备明显的先进性,主要体现在理念核心、访问模式以及信任评估方式三个方面。

1.1.1 理念核心转变

传统安全架构核心在于建“边界”,设定一个

“边界”对内外网进行隔离,边界内是安全可信的,边界外是不安全、不可信的,为了构建这样一套边界机制,企业通常在网络边界处部署各类防火墙、防毒墙、入侵防御/检测等网络安全设备来构筑内网的安全护城河^[7]。而零信任安全理念始终假设网络内外部都不可信,安全信任的验证不能仅仅依靠网络边界一层措施,信任的验证过程应当覆盖所有的访问主客体之间的所有行为动作,并且验证动作需要持续不断(图 2)。

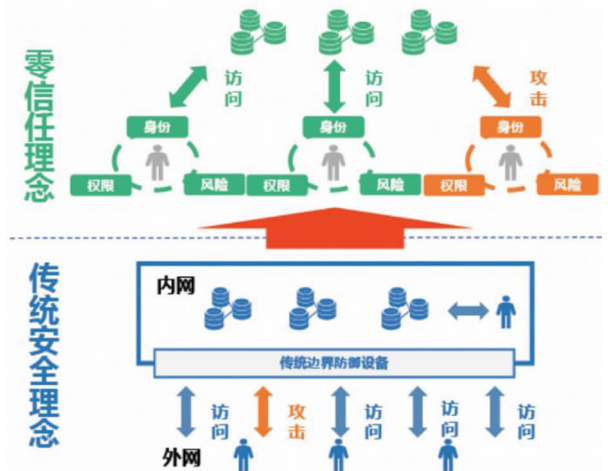


图 2 理念核心转变

1.1.2 访问模式转变

传统网络安全架构中,用户需要通过客户端先建立与服务端的连接,然后再进行认证授权,因此服务端的端口就暴露在公网中,很容易被攻击者利用。在零信任架构中,服务端资源被隐藏在零信任组件中,零信任组件默认关闭所有端口,用户通过验证后登录零信任客户端,才能通过 SPA 敲门的方式和目标服务器连接^[8],将传统先连接后认证模式转变为先认证后连接模式,减少安全暴露面,具备天然的安全防护优势(图 3)。

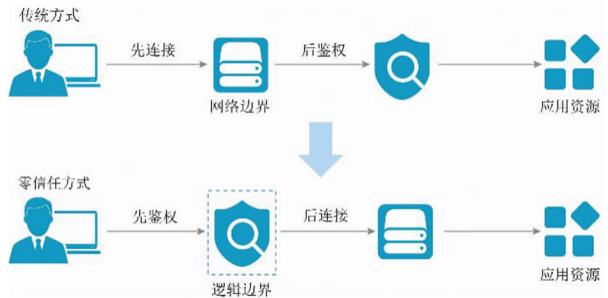


图 3 访问模式转变

1.1.3 信任评估方式转变

传统网络安全架构的信任评估是采用静态单次评估方式,即通过信任评估认证授权后,在后续的持续访问过程中,不再进行信任核实,虽然为了

提高信任评估的可信度,通常会采用多维因素参与评估,但本质上整个评估方式是静态单次的,这种评估方式容易被攻击者利用,通过冒用合法用户身份的方式侵入系统,导致安全机制失效^[9]。而零信任架构采用持续动态信任评估方式,更多地强调过程中的持续动态评估,根据设计好的评估因子,一旦发现非法违规等行为,就能够及时调整该用户的访问动作,避免进一步损失,将信任评估动作贯穿访问全过程^[10]。

1.2 典型零信任应用架构综述

从具体应用实践来看,业内主流零信任技术架构,基本上采用可信访问控制台(TAC)和可信应用代理(TAP)两个组件来分别对应零信任控制平面和数据平面,其技术架构如图 4 所示。

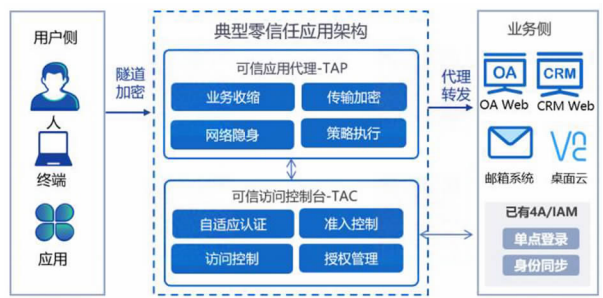


图 4 典型零信任应用架构

张照,王中斌等人所提出的技术架构也证实了这是当前零信任理论模型在实际场景应用的典型技术架构^[8]。该架构是零信任理论落地的最小化版本,适用于大多数典型场景。但是,随着政企机构数字化转型、云原生以及微服务架构等新技术应用,该技术架构也存在应用场景覆盖不全的弊端。

在此背景下,本文将零信任模型引入省级气象部门网络防护体系中,设计了一种基于零信任的、适用于省级气象部门的、全面整体的零信任安全技术架构,并提出构建气象网络的可信访问通道,数据动态授权以及终端可信空间方案。

2 基于零信任的省气象网络安全架构

当前,大多省级气象部门已经搭建国、省、市、州四级纵向网络架构,并横向与各级政府职能部门连通形成综合气象网络。但是,在网络安全方面,大多数气象部门还处于传统网络安全架构阶段。随着气象部门业务服务、数据服务架构的升级和开放,网络安全面临的风险和挑战越来越大,迫切需要对网络安全架构进行迭代升级。

2.1 省级气象部门零信任安全架构

以零信任理论模型为指导,基于省级气象部门

网络架构及业务服务现状,针对当前网络安全面临的主要问题,提出“2+3”架构的省级气象部门零信任安全架构,即通过 2 个控制平面组件和 3 个数据平面组件来实践零信任(图 5)。

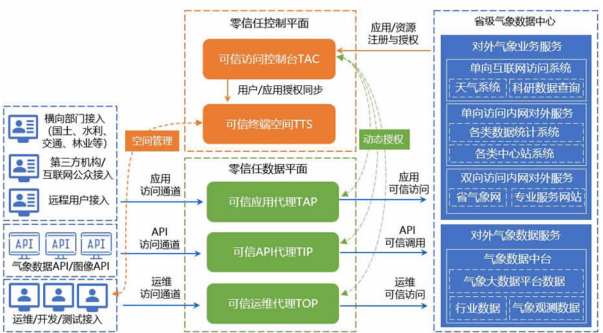


图 5 省级气象部门零信任安全架构

在省级气象部门零信任安全架构中,零信任数据平面的各类可信代理组件将拦截所有访问气象业务服务和数据服务的请求,通过在控制平面采用 RBAC 和 ABAC 的授权方式,实现用户权限的高效分配、授权动态控制和不同粒度的授权控制,在控制内容上有效提升访问控制能力,满足比较复杂的业务系统访问控制要求。

整个架构的核心组件设计如下:

2 个控制平面组件:即可信访问控制台(Trust Access Console, TAC),用于省气象业务和数据资源注册与授权,并统一对接零信任中各个组件,是整个架构的控制中枢,能够提供认证、授权、动态信任评估、细粒度访问控制等能力。另一个控制平面组件为可信终端空间(Trust Terminal Space, TTC),主要用于解决终端落地数据保护问题,面向访问气象业务和数据的运维、开发测试终端提供安全可信的终端数据空间。两个控制平面组件在用户和应用授权数据上保持同步。

3 个数据平面组件:可信应用代理(Trust Application Proxy, TAP),作为应用统一发布的网关,为所有的应用访问提供安全可信的代理转发服务;可信 API 代理(Trust API Proxy, TIP),作为 API 统一发布网关,为所有的 API 接口访问提供安全可信的代理转发服务;可信运维代理(Trust OPS Proxy, TOP),作为统一的运维访问入口,为所有的运维访问提供安全可信的代理转发服务。数据平面所有的组件都是零信任的访问控制策略执行节点,共同构成访问气象业务和数据服务的可信访问通道。

2.2 省级气象部门可信访问通道

2.2.1 可信应用访问通道

为尽可能降低对外气象业务服务系统和数据

服务平台的暴露面,提高访问安全性,通过可信应用代理(TAP)为横向部门(国土、水利、交通、林业等)访问、互联网公众访问、第三方机构访问以及远程访问气象对外业务和数据服务系统提供安全通道。TAP 作为零信任中的策略执行点 PEP(Policy Enforcement Point),为用户访问应用提供代理转发服务,并与 TAC 协同实现用户访问应用的动态访问控制。且能够根据 TAC 的策略开启端口隐藏能力,实现业务端口对用户侧的隐藏,使得业务端口对外不可见,从而保护业务端口无法被扫描到、无法 PING 通、无法发起恶意访问等,进而缓解针对业务端口的恶意嗅探、定向攻击、DDos 攻击等安全风险。可信客户端通过 UDP-TCP 敲门和 TAP 建立隧道,采用 SSL 通信加密,为业务访问提供安全通道,确保访问安全。

2.2.2 可信 API 访问通道

湖南省气象局研制了用于气象信息共享的服务插件,通过标准数据 API 和图形接口等方式提供服务,涉及几十类气象数据,数百个数据接口。为保护各类 API 服务接口安全,通过 TIP 集中代理 API 使用者与 API 服务之间的访问请求与应答,TIP 作为零信任中的策略执行点 PEP,在提供代理服务的过程中,持续与 TAC 协同,接收来自 TAC 的动态访问控制策略,实现对 API 访问过程安全控制。同时,TIP 采用 SSL 通信加密,为数据传输提供安全通道。

2.2.3 可信运维访问通道

省级气象部门各类对外服务系统和气象数据中台在部署和运行期间,面临不同第三方的运维、开发以及测试人员频繁访问系统、数据或设备的需求。为此,省级气象部门零信任安全架构中采用 TOP 对开发、测试和运维人员、B/S 系统、C/S 系统和网络设备、数据库、安全设备和主机系统等资源进行安全访问和运维管理,统一运维访问入口。TOP 作为零信任中的策略执行点 PEP,可通过与 TAC 进行访问控制策略判定,并根据判定结果执行运维访问身份认证和权限控制。同时,TOP 采用 SSL 通信加密,为运维访问提供安全通道。

2.3 省级气象部门数据动态授权

数据安全是省级气象部门当前需要重点关注的问题。就湖南省气象局而言,已经在省气象信息中心 DMZ 区搭建数据中台,统一对外提供气象数据服务,考虑到数据安全隐患,省气象信息中心虽然建立了 MOID 数据标识系统,实现对向外部门提供的气象数据进行安全标记、数据来源追溯、数据流程监控,但是,如何确保数据是被安全可信的人、在可信的时间、可信的地方、因可信必要的业务

需求而进行访问是当前数据被安全访问的关键问题。为了有效解决该问题,本文基于零信任技术架构,提出一种数据动态授权访问的方法(图 6)。



图 6 基于零信任的数据动态授权访问

从图 6 可以看出,构建零信任动态授权能力,需要对请求方的主体、响应方的客体资源、授权方的访问需求和策略进行抽象,建立一套全链路的纵深防御体系,关键举措包括:

(1)构建数据视图。通过 MOID 系统进行客体资源治理,为数据打上标签,作为数据资源属性,建立客体数据资源目录。通过数据中台对原始数据进行处理封装,将数据封装成服务,供主体访问。

(2)构建身份视图。通过 TAC 组件从设备和用户身份认证开始,进行主体身份治理,采用实人认证、设备认证加强认证的强度,保证主体身份可信。判定主体属性(如部门、角色、职责)。

(3)构建统一管控策略体系。基于授权方需求,通过 TAC 对数据的权限进行统一管理,通过基于属性的访问控制机制进行精细化的业务合规控制,保证数据仅供其工作职责访问之内使用。业务规则使用自然语言方式进行描述,再转化为可以进行属性精细化描述的表述性语言(如 XML、接口)。通过零信任数据平台各类代理等进行策略的执行。

(4)持续信任评估与策略治理。在零信任架构中,访问主体由用户、设备和服务三者共同构成,访问主体的信任值包括用户信任值、设备信任值、服务请求信任值以及这三者的综合信任值,同时还需要考虑外部威胁情况对综合值进行动态调整^[1]。因此,持续信任评估与策略治理需要采集主体环境感知数据(包括系统环境、网络环境、软件环境、物理环境、时间、地点等),建立环境信任风险等级,同时还采集用户和应用行为数据,持续对访问会话进行评估,动态调整数据访问安全策略。

2.4 省级气象部门终端可信数据空间

省级气象部门各类对外服务系统和气象数据中台在日常运行过程中,面临第三方开发人员、测试人员、运维人员以及部门内部管理人员因业务需

要访问各类系统和数据中台的场景,如何确保这些人员在访问及业务操作过程中的数据安全,有效防止数据泄露?本文提出了一种基于零信任的终端可信数据空间方案来统一解决上述场景数据安全问题,实现数据“可用不可拿”(图 7)。

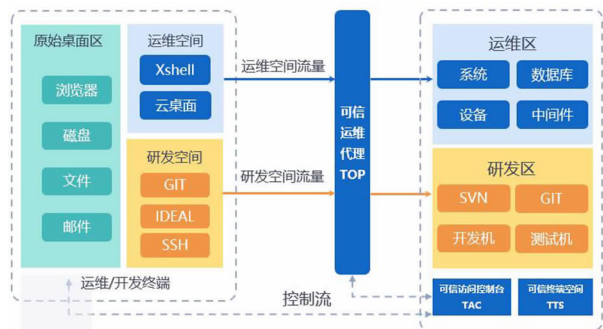


图 6 基于零信任的终端可信数据空间

从图 7 来看,终端可信数据空间设计由 TOP 作为统一的访问入口,为第三方开发人员、测试人员、运维人员以及部门内部管理人员访问气象系统和资源提供可信访问通道,构成第一道数据安全防护线。

终端可信数据空间由可信客户端和 TTS 两大核心组件构成。TTS 作为控制中心,从 TAC 同步用户及应用授权,并下发访问策略至可信客户端。可信客户端部署在第三方开发人员、测试人员、运维人员以及部门内部管理人员终端上,根据 TTS 下发的访问策略,执行网络访问控制、进程隔离、数据隔离以及权限控制等。

通过终端可信数据空间技术,可在相关人员终端上创建单个或多个安全空间,如运维空间、研发空间、测试空间等。安全空间是基于主机操作系统之上的虚拟化,所有安全控件与主机系统共用软硬件资源,安全空间内进程间通信不受限制,安全空间之间进程通信严格受限,包括但不限于文件通信、服务通信、剪贴板进程通信等。每个安全空间可定义不同的安全等级、加密密钥,设置允许/禁止在该安全空间内运行的应用程序列表,设置允许/禁止在该安全空间内访问的网络地址。安全空间内的进程将严格受所属空间限制,在此空间内如果主机进程未经授权,则不能访问任何安全空间内的数据。个人空间与安全空间进程实行严格的 IPC/管道/剪切板单向隔离,安全空间内的进程不能将文件另存到个人空间,个人空间不能以任何方式打开安全空间内的文件。通过内核沙箱驱动,安全空间内进程的所有数据,将被重定向到对应的安全存储空间,即使存储介质丢失也不会导致数据泄密,空间内进程产生的数据只能保存在空间安全盘上,

空间外进程也不能访问空间内的数据。同时,还可以授予不同用户不同的使用权限,如空间内数据的复制/粘贴、打印、截屏、水印、文件导出等,通过空间定义与使用授权的分离,有效防止数据泄露事件的发生。为气象系统重要数据的存储、使用、流转建立安全、易用、可信的工作环境。

3 结 论

主要是对零信任理念及模型在气象部门全面应用的预研,本文所设计的省级气象部门“2+3”零信任安全模型,是基于省级气象部门当前网络安全现状以及未来业务安全需求,以零信任理念为指导设计的一套全新的安全架构,旨在为气象部门当前及未来开展网络安全工作提供新思路、新方案。

不同于典型零信任应用架构,该架构设计面向全局场景,更先进、更全面,能满足省级气象部门当前及未来对网络安全的新需求。同时,也由于架构设计的先进性和全面性,以及省级气象部门当前应用场景条件限制,完整的架构尚未在气象部门实际环境中落地应用。

下一步,将在湖南省气象信息中心以该架构为指导,率先开展落地应用工作,为全国各省气象部门实践零信任提供应用实践样本。

参考文献

- [1] POLALTO. Zero trust network architecture with John Kindervag video [EB/OL]. [2020-05-31]. <https://www.paloaltonetworks.com/resources/videoszero-trust>.
- [2] 王斯梁,冯喧,蔡友保,等. 零信任安全模型解析及应用研究[J]. 信息安全研究,2020,6(11):966-969.
- [3] 余双玻,李春燕,周吉,等. 零信任架构在网络信任体系中的应用[J]. 通信技术,2020,53(10):2533-2537.
- [4] 刘欢,杨帅,刘皓. 零信任安全架构及应用研究[J]. 通信技术,2020,53(7):1745-1749.
- [5] 何国峰. 零信任架构在 5G 云网中应用防护的研究[J]. 应用及终端安全,2020,10(11):1000-1010.
- [6] 魏小强. 基于零信任的远程办公系统安全模型研究与实现[J]. 信息安全研究,2020,4(6):289-295.
- [7] 张刘天,陈丹尾. 基于零信任的动态访问控制模型研究[J]. 信息安全研究,2022,8(10):1008-1017.
- [8] 张照,王中斌,张建伟. 零信任访问解决方案[J]. 信息安全研究,2022,8(增刊):119-122.
- [9] 张宇,张妍. 零信任研究综述[J]. 信息安全研究,2020,6(7):608-614.
- [10] 薛人瑞,吴华佳. HiSec 零信任安全解决方案[J]. 信息安全研究,2021,7(增刊):117-121.