NIST 特别出版物 800-207

零信任架构

斯科特·罗斯
奥利弗·博尔切特
斯图·米切尔
肖恩·康纳利

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-207

计算机安全

National Institute of
Standards and Technology
U.S. Department of Commerce

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

NIST 特别出版物 800-207

零信任架构

斯科特·罗斯
奥利弗·博尔切特
高级网络技术部
信息技术实验室

斯图·米切尔
Stu2Labs
斯塔福德，弗吉尼亚州

肖恩·康纳利
网络安全与基础设施安全局
国土安全部

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-207

2020年8月



美国商务部
威尔伯·L·罗斯二世，部长

美国国家标准与技术研究院
*Walter Copan,NIST*主任兼商务部标准与技术副部长

权限

本出版物由NIST根据2014年《联邦信息安全管理现代化法案》(FISMA),44 U.S.C.3551 *et seq.*，公法(P.L.)113-283所规定的法定职责编写。NIST负责制定信息安全标准和指南，包括联邦信息系统的最低要求，但此类标准和指南在未获得对这些系统行使政策权力的适当联邦官员明确批准的情况下，不适用于国家安全系统。本指南与管理和预算办公室(OMB)A-130号通告的要求一致。

本出版物中的任何内容均不得被视为与商务部长根据法定权力对联邦机构强制实施并具有约束力的标准和指南相矛盾。这些指南也不应被解释为改变或取代商务部长、OMB主任或任何其他联邦官员的现有权力。本出版物可由非政府组织自愿使用，在美国不受版权限制。不过，NIST希望在使用时予以注明出处。

美国国家标准与技术研究院特别出版物 800-207
Natl.Inst.Stand.Technol.Spec.Publ.800-207, 59页(2020年8月)
代码：NSPUE2
本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-207

本文件中可能会提及某些商业实体、设备或材料，以便充分描述实验过程或概念。此类提及并不意图暗示NIST的推荐或认可，也不意图暗示这些实体、材料或设备必然是用于该目的的最佳选择。

本出版物中可能引用了NIST根据其分配的法定职责正在制定的其他出版物。本出版物中的信息，包括概念和方法，即使在此类配套出版物完成之前，联邦机构也可以使用。因此，在每份出版物完成之前，现有的要求、指南和程序(如存在)仍然有效。出于规划和过渡目的，联邦机构可能希望密切关注NIST这些新出版物的制定进展。

鼓励各组织在公开评论期内审阅所有草案出版物并向NIST提供反馈。除上述出版物外，许多NIST网络安全出版物可在https://csrc.nist.gov/publications.获取

对本出版物的评论可提交至：

美国国家标准与技术研究院
收件人：信息技术实验室高级网络技术部
100 局大道（邮件 20899-8920
Email: zerotrust-arch@nist.gov

所有评论均可能根据《信息自由法》(FOIA)予以公开。

计算机系统技术报告

美国国家标准与技术研究院(NIST)的信息技术实验室(ITL)通过为国家的测量和标准基础设施提供技术领导，促进美国经济和公共福利。ITL开发测试、测试方法、参考数据、概念验证实现和技术分析，以推进信息技术的发展和高效使用。ITL的职责包括制定管理、行政、技术和物理标准与指南，以实现联邦信息系统中除国家安全相关信息之外的其他信息的经济高效的安全和隐私保护。800系列特别出版物报告了ITL在信息系统安全方面的研究、指南和外展工作，以及与行业、政府和学术组织的合作活动。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

摘要

零信任(ZT)是指一组不断演进网络安全范式的术语，这些范式将防御从静态的、基于网络的边界转向关注用户、资产和资源。零信任架构(ZTA)使用零信任原则来规划工业和企业基础设施及工作流程。零信任假设不授予资产或用户账户任何隐式信任，这种信任不能仅基于其物理或网络位置(即局域网与互联网)或基于资产所有权(企业所有或个人所有)。身份验证和授权(主体和设备两者)是在建立对企业资源的会话之前执行的离散功能。零信任是对企业网络趋势的回应，这些趋势包括远程用户、自带设备(BYOD)以及不位于企业自有网络边界内的基于云的资产。零信任侧重于保护资源(资产、服务、工作流程、网络账户等)，而不是网络分段，因为网络位置不再被视为资源安全态势的主要组成部分。本文档包含零信任架构(ZTA)的抽象定义，并给出了零信任可以改善企业整体信息技术安全态势的一般部署模型和用例。

关键词

架构；网络安全；企业；网络安全；零信任。

致谢

本文件是多个联邦机构合作的成果，由联邦CIO委员会监督。架构子组负责本文件的编写，但有一些特定个人值得表彰。其中包括联邦CIO委员会ZTA项目项目经理Greg Holden;NIST/国家网络安全卓越中心ZTA工作项目经理Alper Kerman；以及Douglas Montgomery。

受众

本文档旨在为企业安全架构师描述零信任。它旨在帮助理解民用非机密系统的零信任，并提供将零信任安全概念迁移和部署到企业环境的路线图。机构网络安全管理者、网络管理员和管理人员也可从本文档中获得对零信任和ZTA的见解。本文档并非ZTA的单一部署计划，因为企业将拥有需要保护的独特业务用例和数据资产。从对组织业务和数据的扎实理解出发，将形成强有力的零信任方法。

商标信息

所有注册商标或商标均归其各自组织所有。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

专利披露声明

注意：信息技术实验室*(ITL)*已要求，其使用可能为遵守本出版物的指导或要求所必需的专利主张持有人向*ITL*披露此类专利主张。但是，专利持有人没有义务回应*ITL*的专利征集，*ITL*也未进行专利检索以确定是否有任何专利可能适用于本出版物。

在*ITL*征集可能为遵守本出版物的指导或要求所必需的专利主张的标识之后，已收到一项或多项此类主张的通知。

截至发布时，*ITL*不对任何专利主张的有效性或范围或与之相关的任何权利采取立场。然而，已知的专利持有人已向*NIST*提供了一份保证函，声明要么*(1)*一般性免责声明，表明其不持有且目前不打算持有任何必要专利主张，要么*(2)*其将以明显非歧视性的基础、合理的条款和条件与其他方协商免版税或带版税的许可。

详细信息可从**zerotrust-arch@nist.gov 获取**。

未作出或暗示任何陈述表明这是使用本出版物时避免专利侵权可能需要的唯一许可。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

目录

1 **1 引言** 1
1.1 与联邦机构相关的零信任工作历史 2
1.2 本文档的结构 2
2 **2 零信任基础** 4
2.1 零信任原则 6
2.2 网络的零信任视角 8
3 **3 零信任架构的逻辑组件** 9
3.1 零信任架构方法的变体 11
3.1.1 ZTA 使用增强的身份治理 11
3.1.2 ZTA使用微隔离 12
3.1.3 ZTA 使用网络基础设施和软件定义边界 12
3.2 抽象架构的部署变体 13
3.2.1 基于设备代理/网关的部署 13
3.2.2 基于隔离区的部署 14
3.2.3 基于资源门户的部署 15
3.2.4 设备应用沙箱 16
3.3 信任算法 17
3.3.1 信任算法变体 19
3.4 网络/环境组件 21
3.4.1 支持ZTA的网络要求 21
4 **4 部署场景/用例** 23
4.1 拥有卫星设施的企业 23
4.2 多云/云到云企业 24
4.3 拥有合约服务和/或非员工访问权限的企业 25
4.4 跨企业边界的协作 26
4.5 拥有面向公众或客户服务的企业 27
5 **5 与零信任架构相关的威胁** 28
5.1 颠覆ZTA决策过程 28
5.2 拒绝服务或网络中断 28
5.3 窃取凭证/内部威胁 29
5.4 网络可见性 29

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

5.5 系统和网络信息的存储 30
5.6 依赖专有数据格式或解决方案 30
5.7 在ZTA管理中使用非人员实体(NPE) 30
6 零信任架构与现有联邦指南的可能交互 32
6.1 ZTA与NIST风险管理框架 32
6.2 零信任与NIST隐私框架 32
6.3 ZTA 与联邦身份、凭证和访问管理架构 33
6.4 零信任架构与可信互联网连接3.0 33
6.5 零信任架构与EINSTEIN(NCPS--国家网络安全保护系统) 34
6.6 零信任架构与DHS持续诊断和缓解(CDM)计划 34
6.7 ZTA、Cloud Smart 和联邦数据战略 35
7 **7 迁移到零信任架构** 36
7.1 纯零信任架构 36
7.2 混合零信任架构与基于边界的架构 36
7.3 将ZTA引入基于边界的架构化网络的步骤 37
7.3.1 识别企业中的行为主体 38
7.3.2 识别企业拥有的资产 38
7.3.3 识别关键流程并评估与执行流程相关的风险 39
7.3.4 为ZTA候选方案制定策略 39
7.3.5 识别候选解决方案 40
7.3.6 初始部署与监控 40
7.3.7 扩展ZTA 41
参考文献 42

附录列表

附录 A- 缩略语 45
附录 B--ZTA 当前最先进技术中已识别的差距 46
B.1 技术调查 46
B.2 阻碍立即迁移至 ZTA 的差距 47
B.2.1 缺乏ZTA设计、规划和采购的共同术语 47 B.2.2 认为ZTA与现有联邦网络安全

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

政策相冲突 47
B.3 影响ZTA的系统性差距 47
B.3.3 组件间接口的标准化 47
B.3.4 应对过度依赖专有API的新兴标准。48 B.4 ZTA中的知识空白与未来研究领域 48
B.4.5 攻击者对ZTA的响应 49
B.4.6 零信任架构环境中的用户体验 49
B.4.7 零信任架构对企业与网络中断的韧性 49
B.5 参考文献 50

图目录

图1：零信任访问 5
图2：核心零信任逻辑组件 9
图3：设备代理/网关模型 14
图4：飞地网关模型 15
图5：资源门户模型 16
图6：应用程序沙箱 17
图7：信任算法输入 18
图8：拥有远程员工的企业 24
图9：多云用例 24
图10：具有非员工访问权限的企业 25
图11：跨企业协作 26
图 12:ZTA 部署周期 37

表目录

表 B-1：已识别部署差距汇总 46

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

1引言

典型企业的基础设施已变得日益复杂。单个企业可能运营多个内部网络、拥有自己本地基础设施的远程办公室、远程和/或移动个人以及云服务。这种复杂性已超出基于边界的网络安全的传统方法，因为企业不再有单一、易于识别的边界。基于边界的网络安全也已被证明是不够的，因为一旦攻击者突破边界，进一步的横向移动便不受阻碍。

这种复杂的企业催生了一种新的网络安全模型，称为“零信任”(ZT)。ZT方法主要关注数据和服务保护，但可以而且应该扩展到包括所有企业资产(设备、基础设施组件、应用、虚拟和云组件)和主体(最终用户、应用以及从资源请求信息的其他非人类实体)。在本文档中，将使用“主体”，除非该节直接涉及人类最终用户，此时将具体使用“用户”而非更通用的“主体”。零信任安全模型假定环境中存在攻击者，并且企业拥有的环境与非企业拥有的环境并无不同--也不更可信。在这种新范式中，企业必须不假定任何隐式信任，并持续分析和评估其资产和业务功能的风险，然后实施保护措施以缓解这些风险。在零信任中，这些保护措施通常涉及将资源访问(如数据和计算资源以及应用/服务)最小化到仅限那些被识别为需要访问的主体和资产，以及持续认证和授权每个访问请求的身份和安全态势。

零信任架构(ZTA)是一种企业网络安全架构，基于零信任原则，旨在防止数据泄露并限制内部横向移动。本出版物讨论ZTA、其逻辑组件、可能的部署场景和威胁。它还提出了希望迁移到零信任设计方法的组织的一般路线图，并讨论了可能影响或左右零信任架构的相关联邦政策。

ZT不是单一架构，而是一组用于工作流、系统设计和操作的指导原则，可用于改善任何分类或敏感级别[FIPS199]的安全态势。向ZTA过渡是一个关于组织如何在其使命中评估风险的旅程，不能简单地通过整体替换技术来实现。尽管如此，许多组织今天的企业基础设施中已具备ZTA的要素。组织应寻求按用例逐步实施零信任原则、流程变更和技术解决方案，以保护其数据资产和业务功能。大多数企业基础设施将在混合零信任/基于边界的模式下运行，同时继续投资于IT现代化举措并改进组织业务流程。

组织需要实施全面的信息安全和弹性实践，零信任才能有效。当与现有网络安全政策和指南、身份和访问管理、持续监控以及最佳实践相平衡时，ZTA可以保护

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

免受常见威胁，并通过使用受管理的风险方法改善组织的安全态势。

1.1 与联邦机构相关的零信任工作历史

“零信任”这一术语被创造之前，零信任的概念就已存在于网络安全领域。美国国防信息系统局(DISA)和国防部发表了关于更安全的企业战略的研究成果，称为“黑核”[BCORE]。黑核涉及从基于边界的安全模型转向关注单个事务安全的模型。2004年杰里科论坛的工作公开了去边界化的理念--限制基于网络位置的隐式信任，以及在大网段上依赖单一静态防御的局限性[JERICHO]。去边界化的概念演变并改进为更广泛的零信任概念，该术语后来由John Kindervag[1]在Forrester任职期间创造。[2]零信任随后成为描述各种网络安全解决方案的术语，这些解决方案将安全从基于网络位置的隐式信任转移开，转而专注于基于每笔事务评估信任。私营行业和高等教育也都经历了从基于边界的安全到基于零信任原则的安全策略的演变。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

十多年来，联邦机构一直被敦促转向基于零信任原则的安全，建立能力和政策，如《联邦信息安全现代化法案》(FISMA)以及随后的风险管理框架(RMF)；联邦身份、凭证和访问管理(FICAM)；可信互联网连接(TIC)；以及持续诊断与缓解(CDM)项目。所有这些项目都旨在将数据和资源访问限制在授权方。当这些项目启动时，它们受到信息系统技术能力的限制。安全策略基本上是静态的，并在企业可以控制的大“瓶颈点”执行，以最小的努力获得最大的效果。随着技术的成熟，现在有可能以动态和细粒度方式持续分析和评估访问请求，基于“需要访问”的基础，以减轻因账户被攻陷、攻击者监控网络和其他威胁导致的数据暴露。

1.2 本文档的结构

文档的其余部分组织如下：

- **第2节**定义了ZT和ZTA，并列出了为企业设计ZTA时的一些假设。本节还包括ZT设计原则的列表。
- **第3节**记录了ZT的逻辑组件或构建块。独特的实现可能以不同方式组成ZTA组件，但提供相同的逻辑功能。

[1] https://go.forrester.com/blogs/next-generation-access-and-zero-trust/
[2] NIST文件中提及任何商业产品或服务仅供参考；并不暗示NIST的推荐或认可。

- **第4节**列出了一些可能的用例，在这些用例中，ZTA可以使企业环境更安全，更不易被成功利用。这些包括拥有远程员工、云服务和访客网络的企业。

- **第5节**讨论了使用ZTA的企业面临的威胁。其中许多威胁与任何已架构的网络类似，但可能需要不同的缓解技术。
- **第6节**讨论了ZTA原则如何融入和/或补充联邦机构的现有指南。

- **第7节**提出了将企业(如联邦机构)过渡到ZTA的起点。这包括描述在ZT原则指导下规划和部署应用程序及企业基础设施所需的一般步骤。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

2零信任基础

零信任是一种专注于资源保护的网络安全范式，其前提是信任永远不会被隐式授予，而必须持续评估。零信任架构是一种端到端的企业资源和数据安全方法，涵盖身份(人员和非人员实体)、凭证、访问管理、运营、端点、托管环境以及互连基础设施。初始重点应放在将资源限制在有访问需要的主体，并仅授予执行任务所需的最低权限(例如读、写、删除)。传统上，机构(以及一般的企业网络)专注于边界防御，一旦进入内部网络，经过认证的主体就被授予对广泛资源的授权访问。因此，环境内的未授权横向移动一直是联邦机构面临的最大挑战之一。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

可信互联网连接(TIC)和机构边界防火墙提供了强大的互联网网关。这有助于阻止来自互联网的攻击者，但 TIC 和边界防火墙在检测和阻止来自网络内部的攻击方面作用较小，并且无法保护企业边界之外的主体(例如远程工作人员、基于云的服务、边缘设备等)。

零信任和零信任架构的操作性定义如下：

> 零信任(ZT)提供了一组概念和理念，旨在面对被视为已攻陷的网络时，最小化在信息系统和服务中执行准确的、每请求最小权限访问决策的不确定性。零信任架构(ZTA)是企业利用零信任概念的网络安全计划，涵盖组件关系、工作流规划和访问策略。因此，零信任企业是作为零信任架构计划产物的企业网络基础设施(物理和虚拟)及运营策略。

企业决定采用零信任作为其核心策略，并生成零信任架构，作为在考虑零信任原则(见下文第 2.1 节)的情况下制定的计划。然后部署该计划以生成供企业使用的零信任环境。

该定义聚焦于问题的关键，即防止对数据和服务的未授权访问的目标，同时使访问控制执行尽可能细粒度。也就是说，授权和批准的主体(用户、应用(或服务)和设备的组合)可以访问数据，而排除所有其他主体(即攻击者)。进一步说，“资源”一词可以替代“数据”，因此ZT和ZTA是关于资源访问(例如打印机、计算资源、物联网[IoT]执行器)，而不仅仅是数据访问。

为了减少不确定性(因为它们无法被消除)，重点在于身份验证、授权以及缩小隐式信任区域，同时保持可用性并最小化身份验证机制中的时间延迟。访问规则尽可能细化，以强制执行请求中执行操作所需的最小权限。

在图 1 所示的抽象访问模型中，主体需要访问企业资源。访问通过策略决策点(PDP)和相应的策略执行点(PEP)授予。[3]

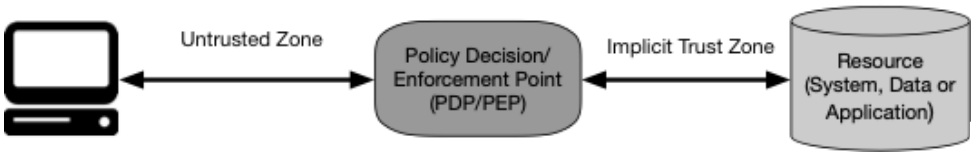


图 1：零信任访问

系统必须确保主体是真实的且请求是有效的。PDP/PEP 通过正确的判断来允许主体访问资源。这意味着零信任适用于两个基本领域：身份验证和授权。对于这个唯一请求，对主体身份的信任级别是多少?鉴于对主体身份的信任级别，是否允许访问该资源?用于请求的设备是否具有适当的安全态势?是否还应考虑其他会改变信任级别的因素(例如时间、主体位置、主体的安全态势)?总体而言，企业需要制定并维护基于风险的动态资源访问策略，并建立一个系统，确保这些策略针对单个资源访问请求得到正确且一致的执行。这意味着企业不应依赖隐含的可信性，即如果主体已达到基本身份验证级别(例如登录到某个资产)，则假定所有后续资源请求都同样有效。

“隐式信任区域”代表所有实体至少被信任到最后一个 PDP/PEP 网关级别的区域。例如，考虑机场的乘客安检模型。所有乘客通过机场安全检查站(PDP/PEP)进入登机口。乘客、机场员工、机组人员等在航站楼区域四处走动，所有个人都被视为可信。在此模型中，隐式信任区域是登机区域。

PDP/PEP 应用一组控制措施，使得 PEP 之后的所有流量具有共同信任级别。PDP/PEP 无法在其流量流中的位置之外应用额外策略。为了使 PDP/PEP 尽可能具体，隐式信任区域必须尽可能小。

零信任提供了一组围绕将 PDP/PEP 移近资源的原则和概念。其理念是显式地对构成企业的所有主体、资产和工作流进行身份验证和授权。

[3] 属于 OASIS XACML 2.0 中定义的部分概念https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

2.1 零信任原则

许多关于 ZT 的定义和讨论都强调将移除广域边界防御(例如企业防火墙)作为一个因素。然而，这些定义中的大多数仍以某种方式相对于边界来定义自身(例如微隔离或微边界；见第 3.1 节)，作为 ZTA 功能能力的一部分。以下尝试根据应涉及的基本原则而非被排除的内容来定义 ZT 和 ZTA。这些原则是理想目标，但必须承认，对于给定策略，并非所有原则都能以其最纯粹的形式完全实现。

零信任架构的设计和部署遵循以下零信任基本原则：

1. **所有数据源和计算服务均被视为资源。**网络可能由多类设备组成。网络还可能具有向聚合器/存储发送数据的小型设备、软件即服务(SaaS)、向执行器发送指令的系统以及其他功能。此外，如果个人拥有的设备能够访问企业拥有的资源，企业可能决定将其归类为资源。

2. **无论网络位置如何，所有通信都是安全的。**仅网络位置并不表示信任。来自位于企业拥有网络基础设施上的资产(例如传统网络边界内部)的访问请求，必须满足与来自任何其他非企业拥有网络的访问请求和通信相同的安全要求。换言之，不应仅因设备位于企业网络基础设施上就自动授予信任。所有通信都应以可用的最安全方式进行，保护保密性和完整性，并提供源身份验证。

3. **对企业单个资源的访问是按-会话授予的。**在授予访问权限之前，会评估对请求者的信任。访问还应以完成任务所需的最小权限授予。这可能仅意味着针对此特定事务“最近某个时间”，并且可能不会直接发生在发起会话或与资源执行事务之前。然而，对一个资源的身份验证和授权不会自动授予对另一不同资源的访问权限。

4. **对资源的访问由动态策略决定--包括客户端身份、应用/服务以及请求资产的可观察状态--并且可能包括其他行为和环境属性。**组织通过定义其拥有哪些资源、其成员是谁(或从联合社区对用户进行身份验证的能力)，以及这些成员需要对这些资源具有何种访问权限来保护资源。对于零信任，客户端身份可以包括用户账户(或服务身份)以及企业分配给该账户的任何关联属性，或用于对自动化任务进行身份验证的工件。请求资产状态可以包括设备特征，例如已安装的软件版本、网络位置、请求的时间/日期、先前观察到的行为以及已安装的凭据。行为属性包括但不限于自动化主体分析、设备分析以及相对于观察到的使用模式所测得的偏差。策略是组织基于分配给主体、数据资产或应用的属性而设定的一组访问规则。环境属性可能包括请求者等因素

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

网络位置、时间、报告的活跃攻击等。这些规则和属性基于业务流程的需求和可接受的风险水平。资源访问和操作权限策略可能因资源/数据的敏感性而异。应用最小权限原则以限制可见性和可访问性。

5. **企业监控并测量所有自有及相关资产的完整性和安全态势。**任何资产均不被固有信任。企业在评估资源请求时评估资产的安全态势。实施ZTA的企业应建立持续诊断与缓解(CDM)或类似系统以监控设备和应用的状态，并应按需应用补丁/修复。被发现已被攻陷、存在已知漏洞和/或不受企业管理的资产，其处理方式可能不同于被视为处于最安全状态的企业自有或相关设备(包括拒绝所有与企业资源的连接)。这也可能适用于相关设备(例如个人拥有的设备)，这些设备可能被允许访问某些资源但不允许访问其他资源。这同样需要健全的监控和报告系统，以提供关于企业资源当前状态的可操作数据。

6. **所有资源身份验证和授权都是动态的，并在允许访问前严格执行。**这是一个获取访问、扫描和评估威胁、适应并持续重新评估持续通信中信任的恒定循环。实施ZTA的企业应具备身份、凭证和访问管理(ICAM)及资产管理系统。这包括使用多因素身份验证(MFA)访问部分或全部企业资源。持续监控及可能的重新身份验证和重新授权贯穿用户交易全过程，由策略定义并执行(例如基于时间、请求新资源、资源修改、检测到异常主体活动)，力求实现安全性、可用性、可用性和成本效益的平衡。

7. **企业尽可能多地收集有关资产、网络基础设施和通信当前状态的信息，并利用这些信息改善其安全态势。**企业应收集有关资产安全态势、网络流量和访问请求的数据，处理这些数据，并利用获得的任何洞察来改进策略创建和执行。这些数据还可用于为主体访问请求提供上下文(见第 3.3.1 节)。

上述原则力求与技术无关。例如，“用户标识(ID)”可包括多种因素，如用户名/密码、证书和一次性密码。这些原则适用于组织内部完成的工作或与一个或多个合作伙伴组织协作完成的工作，不适用于匿名公共或面向消费者的业务流程。组织不能对外部行为者(例如客户或普通互联网用户)施加内部策略，但可能能够对与组织有特殊关系的非企业用户(例如注册客户、员工家属等)实施某些基于ZT的策略。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

2.2 零信任视角下的网络

任何组织在网络规划和部署中使用ZTA时，都存在一些关于网络连接的基本假设。其中一些假设适用于企业拥有的网络基础设施，另一些适用于在非企业拥有的网络基础设施(例如公共Wi-Fi或公共云提供商)上运行的企业拥有资源。这些假设用于指导ZTA的构建。实施ZTA的企业中的网络应按照上述ZTA原则并基于以下假设进行开发。

1. **整个企业专用网络不被视为隐式信任区。**资产应始终假设攻击者存在于企业网络上，并应以可用的最安全方式进行通信(参见上文原则2)。这需要采取诸如对所有连接进行身份验证和对所有流量进行加密等操作。

2. **网络上的设备可能并非由企业拥有或配置。**访客和/或合同服务可能包括需要网络访问以履行其职责的非企业拥有的资产。这包括允许企业主体使用非企业拥有的设备访问企业资源的自带设备(BYOD)策略。

3. **没有任何资源是天然可信的。**每个资产在获得对企业拥有资源的请求授权之前，必须通过PEP评估其安全态势(类似于上述第6条原则，同样适用于资产和主体)。只要会话持续，这种评估就应持续进行。企业拥有的设备可能具有支持身份验证的工件，并提供比来自非企业拥有设备的相同请求更高的置信级别。仅凭主体凭据不足以完成对企业资源的设备身份验证。

4. **并非所有企业资源都在企业拥有的基础设施上。**资源包括远程企业主体以及云服务。企业拥有或管理的资产可能需要利用本地(即非企业)网络进行基本连接和网络服务(例如DNS解析)。

5. **远程企业主体和资产不能完全信任其本地网络连接。**远程主体应假设本地(即非企业拥有的)网络是敌对的。资产应假设所有流量都在被监控且可能被修改。所有连接请求都应经过身份验证和授权，所有通信都应以尽可能安全的方式进行(即提供保密性、完整性保护和源身份验证)。参见上述ZTA原则。

6. **在企业与非企业基础设施之间移动的资产和工作流应具有一致的安全策略和安全态势。**资产和工作负载在移入或移出企业拥有的基础设施时应保持其安全态势。这包括从企业网络移动到非企业网络的设备(即远程用户)。这也包括从本地数据中心迁移到非企业云实例的工作负载。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

3逻辑组件ofZeroTrustArchitecture

企业中构成ZTA部署的逻辑组件众多。这些组件可以作为本地服务运行，也可以通过基于云的服务运行。图2中的概念框架模型展示了组件之间的基本关系及其交互。请注意，这是一个展示逻辑组件及其交互的理想模型。从图1中可以看出，策略决策点(PDP)被分解为两个逻辑组件：策略引擎和策略管理器(定义如下)。ZTA逻辑组件使用单独的控制平面进行通信，而应用数据则在数据平面上通信(见第3.4节)。

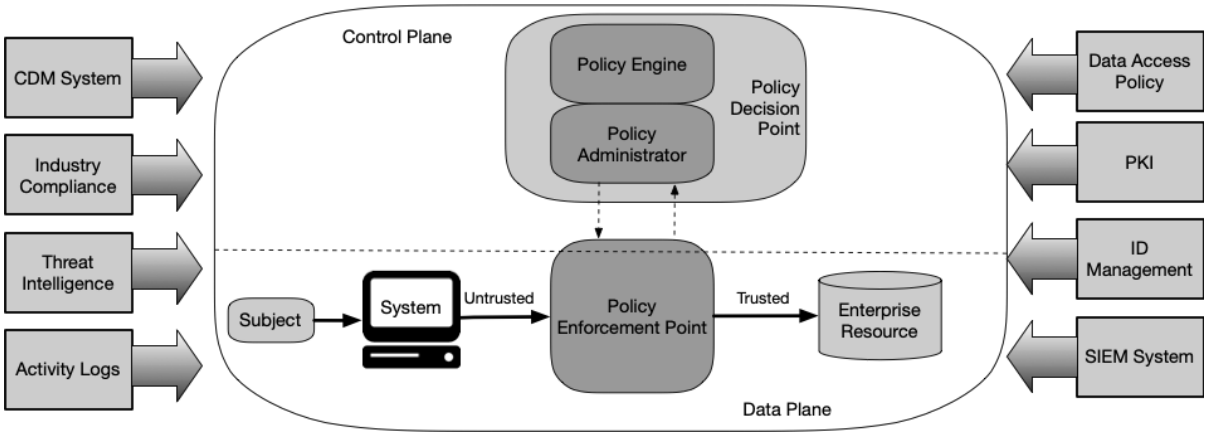


图2：核心零信任逻辑组件

组件描述：

- **策略引擎(PE):**该组件负责为给定主体授予资源访问权限的最终决策。PE使用企业策略以及来自外部来源的输入(例如下文所述的CDM系统、威胁情报服务)作为信任算法的输入(更多细节见第3.3节)，以授予、拒绝或撤销对资源的访问。PE与策略管理器组件配对。策略引擎做出决策并记录日志(批准或拒绝)，策略管理器执行该决策。

- **策略管理器(PA):**该组件负责建立和/或关闭主体与资源之间的通信路径(通过向相关PEP发送命令)。它将生成客户端访问企业资源所使用的任何会话特定身份验证和身份验证令牌或凭证。它与PE紧密关联，并依赖其最终允许或拒绝会话的决策。如果会话已获授权且请求已通过身份验证，则PA配置PEP以允许会话开始。如果会话被拒绝(或先前的批准被撤销)，则PA向PEP发出信号以关闭连接。某些实现可能将PE和PA视为单一服务；此处将其分为

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

两个逻辑组件。PA在创建通信路径时与PEP通信。此通信通过控制平面完成。

- **策略执行点(PEP):**该系统负责启用、监控并最终终止主体与企业资源之间的连接。PEP与PA通信以转发请求和/或接收来自PA的策略更新。这是ZTA中的单一逻辑组件，但可能分为两个不同的组件：客户端(例如，笔记本电脑上的代理)和资源侧(例如，资源前端控制访问的网关组件)，或作为通信路径守门人的单一门户组件。PEP之外是承载企业资源的信任区(见第2节)。

除了实施ZTA的企业中的核心组件外，若干数据源为策略引擎在做出访问决策时提供输入和策略规则。这些包括本地数据源以及外部(即非企业控制或创建的)数据源。这些可以包括：

- **持续诊断与缓解(CDM)系统：**该系统收集有关企业资产当前状态的信息，并对配置和软件组件应用更新。企业CDM系统向策略引擎提供有关发出访问请求的资产的信息，例如该资产是否运行了适当修补的操作系统(OS)、企业批准的软件组件的完整性或是否存在未批准的组件，以及该资产是否存在任何已知漏洞。CDM系统还负责识别并可能对企业基础设施上活跃的非企业设备强制执行一部分策略。

- **行业合规系统：**这确保企业始终遵守其可能所属的任何监管制度(例如FISMA、医疗保健或金融行业信息安全要求)。这包括企业为确保合规而制定的所有策略规则。

- **威胁情报源：**该组件提供来自内部或外部来源的信息，帮助策略引擎做出访问决策。这些可能是多个服务，从内部和/或多个外部来源获取数据，并提供有关新发现的攻击或漏洞的信息。这还包括新发现的软件缺陷、新识别的恶意软件，以及向其他资产报告的、策略引擎将希望拒绝企业资产访问的攻击。

- **网络和系统活动日志：**该企业系统聚合资产日志、网络流量、资源访问操作以及其他事件，提供关于企业信息系统安全态势的实时(或近实时)反馈。

- **数据访问策略：**这些是关于访问企业资源的属性、规则和策略。这组规则可以在策略引擎中编码(通过管理接口)或由策略引擎动态生成。这些策略是授权访问资源的起点，因为它们为企业中的账户和应用程序/服务提供基本访问权限。这些策略应基于已定义的任务角色和组织的需求。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

- **企业公钥基础设施(PKI):**该系统负责生成和记录企业向资源、主体、服务和应用程序颁发的证书。这还包括全球证书颁发机构生态系统和联邦PKI,[4]其可能与企业PKI集成，也可能不集成。这也可以是不基于X.509证书的PKI。

- **身份管理系统：**该系统负责创建、存储和管理企业用户账户和身份记录(例如，轻量级目录访问协议(LDAP)服务器)。该系统包含必要的主体信息(例如，姓名、电子邮件地址、证书)以及其他企业特征，如角色、访问属性和分配的资产。该系统通常利用其他系统(如PKI)来获取与用户账户相关的工件。该系统可能是更大联邦社区的一部分，并可能包括非企业员工或与非企业资产的链接以进行协作。

- **安全信息和事件管理(SIEM)系统：**该系统收集以安全为中心的信息以供后续分析。然后使用这些数据来完善策略并警告针对企业资产的可能的攻击。

3.1 零信任架构方法的变体

企业可以通过多种方式为工作流实施零信任架构。这些方法在所使用的组件以及组织策略规则的主要来源上有所不同。每种方法都实现了零信任的所有原则(见第2.1节)，但可能以一个或两个(或一个组件)作为策略的主要驱动因素。完整的零信任解决方案将包含所有三种方法的要素。这些方法包括增强的身份治理驱动、逻辑微隔离和基于网络的分段。

某些方法比其他方法更适合某些用例。希望为其企业开发ZTA的组织可能会发现，其选择的用例和现有策略指向某一种方法而非其他方法。这并不意味着其他方法不可行，而是其他方法可能更难实施，并且可能需要对企业的当前业务流方式进行更根本的改变。

3.1.1 使用增强身份治理的ZTA

开发零信任架构的增强身份治理方法使用行为主体的身份作为策略创建的关键组件。如果不是因为主体请求访问企业资源，就没有必要创建访问策略。对于这种方法，企业资源访问策略基于身份和分配的属性。资源访问的主要要求基于授予给定主体的访问权限。其他因素，如所使用的设备、资产状态和环境因素，可能会改变最终的置信度计算(和最终访问授权)，或以某种方式调整结果，例如基于网络位置仅授予对给定数据源的 partial 访问权限。单个资源或PEP

[4] https://www.idmanagement.gov/topics/fpki/

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

保护资源的组件必须有一种方式将请求转发到策略引擎服务，或在授予访问权限之前对主体进行身份验证并批准请求。

企业基于增强身份治理的方法通常采用开放网络模型或具有访客访问权限或网络上频繁出现非企业设备的企业网络(如下文第4.3节中的用例)。网络访问最初授予所有资产，但对企业资源的访问仅限于具有适当访问权限的身份。授予基本网络连接存在一个缺点，因为恶意行为者仍可能尝试网络侦察和/或利用网络发起内部或针对第三方的拒绝服务攻击。企业仍然需要监控并响应此类行为，然后才能影响工作流。

身份驱动方法非常适合资源门户模型(见第3.2.3节)，因为设备身份和状态为访问决策提供辅助支持数据。其他模型也可以使用，取决于所实施的策略。身份驱动方法也适用于使用基于云的应用程序/服务的企业，这些应用程序/服务可能不允许使用企业拥有或运营的零信任安全组件(例如许多SaaS产品)。企业可以使用请求者的身份在这些平台上制定和执行策略。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

3.1.2 使用微隔离的零信任架构

企业可以选择基于将单个或一组资源放置在由网关安全组件保护的唯一网络段上来实施零信任架构。在这种方法中，企业部署基础设施设备，如智能交换机(或路由器)或下一代防火墙(NGFW)或专用网关设备，作为保护每个资源或一小组相关资源的PEP。或者(或另外)，企业可以选择使用软件代理(见第3.2.1节)或端点资产上的防火墙来实施基于主机的微隔离。这些网关设备动态地授予来自客户端、资产或服务的单个请求的访问权限。根据模型的不同，网关可以是唯一的PEP组件，也可以是由网关和客户端代理组成的多部分PEP的一部分(见第3.2.1节)。

此方法适用于各种用例和部署模型，因为保护设备充当PEP，而所述设备的管理充当PE/PA组件。此方法需要身份治理计划(IGP)才能完全发挥作用，但依赖网关组件充当PEP，保护资源免受未授权访问和/或发现。

此方法的关键必要性在于PEP组件受到管理，并且应能够根据需要做出反应和重新配置，以应对威胁或工作流的变化。使用不太先进的网关设备甚至无状态防火墙来实现微隔离企业的一些功能是可能的，但管理成本和快速适应变化的难度使其成为一个非常糟糕的选择。

3.1.3 使用网络基础设施和软件定义边界的ZTA

最后一种方法使用网络基础设施来实现ZTA。ZTA实现可以通过使用覆盖网络(即第7层，但也可以设置在OSI网络栈的较低层)来实现。

OSI网络栈)。这些方法有时被称为软件定义边界(SDP)方法，并且经常包含软件定义网络(SDN)[SDNBOOK]和基于意图的网络(IBN)[IBNVN]的概念。在此方法中，PA充当网络控制器，根据PE做出的决策设置和重新配置网络。客户端继续通过PEP请求访问，PEP由PA组件管理。

当该方法在应用网络层(即第7层)实施时，最常见的部署模型是代理/网关(参见第3.2.1节)。在此实现中，代理和资源网关(充当单个PEP并由PA配置)建立用于客户端和资源之间通信的安全通道。此模型可能还有其他变体，以及用于云虚拟网络、非基于IP的网络等。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

3.2 抽象架构的部署变体

上述所有组件均为逻辑组件。它们不一定需要是独立的系统。单个资产可以承担多个逻辑组件的职责，同样，一个逻辑组件也可以由多个硬件或软件元素组成以执行任务。例如，企业管理的PKI可能由一个负责为设备颁发证书的组件和另一个用于向最终用户颁发证书的组件组成，但两者都使用从同一企业根证书颁发机构签发的中间证书。在当前市场上一些可用的ZT产品中，PE和PA组件合并在一个单一服务中。

架构中选定组件的部署有几种变体，概述如下各节。根据企业网络的设置方式，一个企业中可能针对不同的业务流程使用多种ZTA部署模型。

3.2.1 基于设备代理/网关的部署

在此部署模型中，PEP分为两个组件，分别驻留在资源上或作为资源正前方的组件。例如，每个企业发放的资产都安装有一个设备代理，用于协调连接，而每个资源都有一个直接放置在其前方的组件(即网关)，使得资源仅与网关通信，实质上充当资源的代理。代理是一个软件组件，它将部分(或全部)流量引导至适当的PEP以便对请求进行评估。网关负责与策略管理器通信，并仅允许策略管理器配置的已批准通信路径(见图3)。

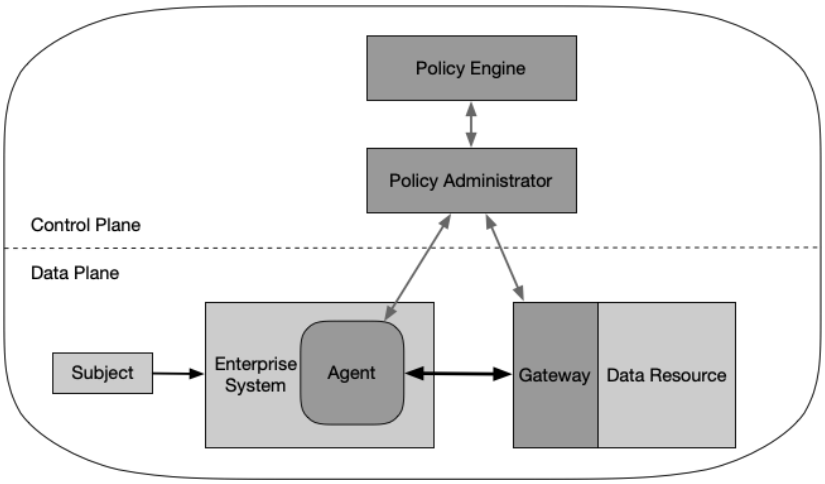


图 3：设备代理/网关模型

在典型场景中，拥有企业发放笔记本电脑的主体希望连接到企业资源(例如人力资源应用/数据库)。访问请求由本地代理接收，并将请求转发给策略管理器。策略管理器和策略引擎可以是企业本地资产或云托管服务。策略管理器将请求转发给策略引擎进行评估。如果请求被授权，策略管理器通过控制平面在设备代理和相关资源网关之间配置通信通道。这可能包括互联网协议(IP)地址、端口信息、会话密钥或类似安全工件等信息。然后设备代理和网关连接，加密的应用/服务数据流开始。当工作流完成或由于安全事件(例如会话超时、重新认证失败)由策略管理器触发时，设备代理和资源网关之间的连接终止。

此模型最适合已建立强大设备管理计划以及可与网关通信的离散资源的企业。对于大量使用云服务的企业，这是云安全联盟(CSA)软件定义边界(SDP)[CSA-SDP]的客户端-服务器实现。此模型也适用于不希望实施BYOD政策的企业。仅可通过设备代理进行访问，该代理可放置在企业拥有的资产上。

3.2.2 基于飞地的部署

此部署模型是上述设备代理/网关模型的变体。在此模型中，网关组件可能不驻留在资产上或单个资源前方，而是驻留在资源飞地(例如本地数据中心)的边界处，如图4所示。通常，这些资源服务于单一业务功能，或者可能无法直接与网关通信(例如，没有可用于与网关通信的应用程序编程接口[API]的遗留数据库系统)。此部署模型也可能对使用基于云的微服务处理单一业务流程(例如用户通知、数据库查询、薪资发放)的企业有用。在此模型中，整个私有云位于网关之后。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

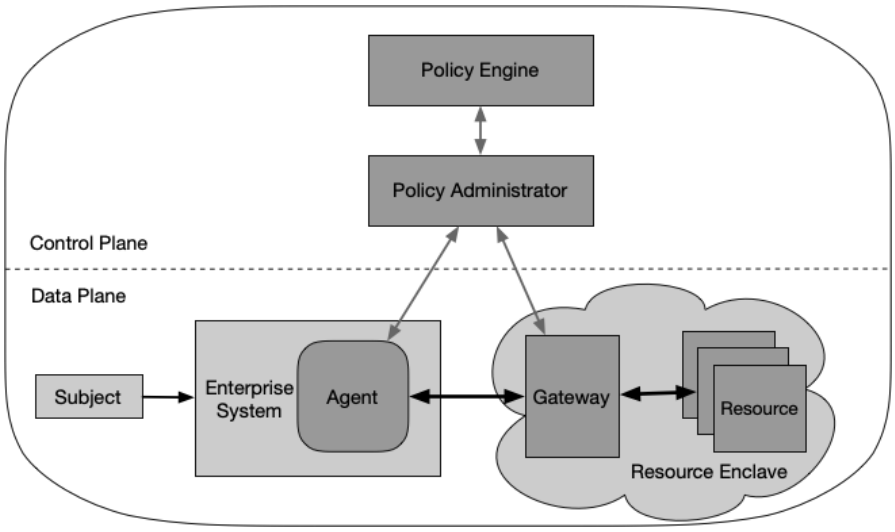


图 4：飞地网关模型

此模型可以与设备代理/网关模型形成混合。在此模型中，企业资产具有用于连接到飞地网关的设备代理，但这些连接使用与基本设备代理/网关模型相同的过程创建。

此模型适用于拥有无法单独设置网关的遗留应用程序或本地数据中心的企业。企业需要健全的资产和配置管理计划来安装/配置设备代理。缺点在于网关保护一组资源，可能无法单独保护每个资源。这也可能允许主体看到其无权访问的资源。

3.2.3 基于资源门户的部署

在此部署模型中，PEP是充当主体请求网关的单个组件。网关门户可以是用于单个资源的，也可以是用于单个业务功能的一组资源的安全飞地。一个示例是进入包含遗留应用程序的私有云或数据中心的网关门户，如图5所示。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

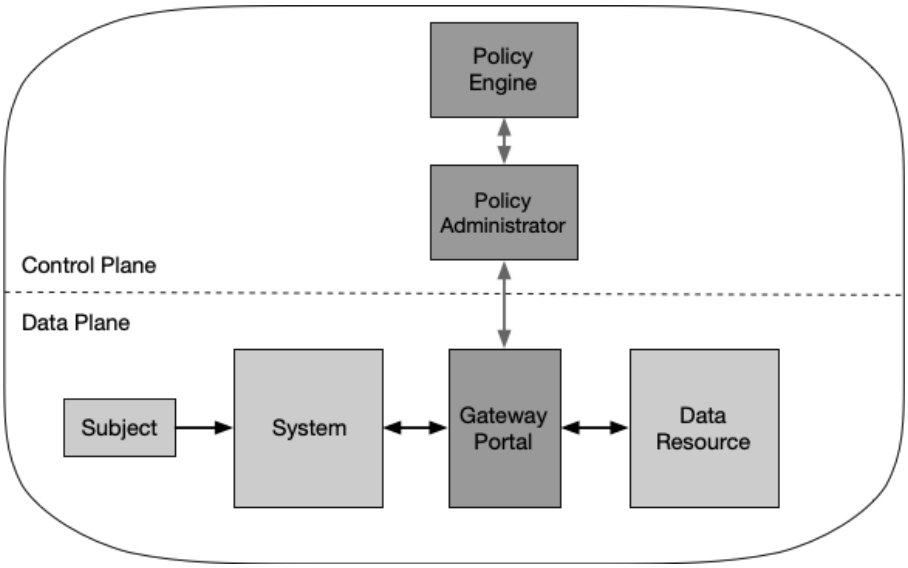


图5：资源门户模型

与其他模型相比，该模型的主要优势在于软件组件无需安装在所有客户端设备上。该模型对于BYOD策略和组织间协作项目也更加灵活。企业管理员无需确保每台设备在使用前都安装了适当的设备代理。然而，从请求访问的设备中能够推断出的信息有限。该模型只能在资产和设备连接到PEP门户后对其进行扫描和分析，可能无法持续监控它们是否存在恶意软件、未修补的漏洞以及适当的配置。

该模型的主要区别在于没有处理请求的本地代理，因此企业可能无法对资产拥有完全的可见性或任意控制权，因为只有在资产连接到门户时才能看到/扫描它们。企业可能能够采用浏览器隔离等措施来缓解或补偿。在这些会话之间，这些资产对企业可能是不可见的。该模型还允许攻击者发现并尝试访问门户，或尝试对门户发起拒绝服务(DoS)攻击。门户系统应做好充分配置，以提供抵御DoS攻击或网络中断的可用性。

3.2.4 设备应用沙盒

代理/网关部署模型的另一种变体是让经过审查的应用程序或进程在资产上分区运行。这些分区可以是虚拟机、容器或其他实现，但目标相同：保护应用程序或应用程序实例免受可能受损的主机或资产上运行的其他应用程序的影响。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

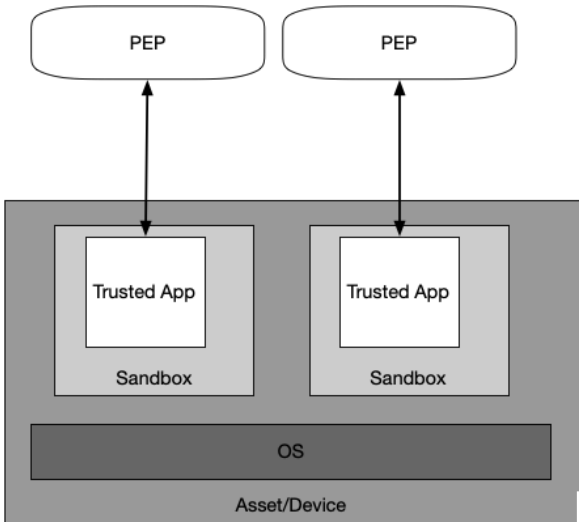


图 6：应用程序沙箱

在图6中，主体设备在沙箱中运行经过批准、审查的应用程序。这些应用程序可以与PEP通信以请求访问资源，但PEP将拒绝来自资产上其他应用程序的请求。在此模型中，PEP可以是企业本地服务或云服务。

该模型变体的主要优势在于单个应用程序与资产的其余部分进行了隔离。如果无法对资产进行漏洞扫描，这些单独的沙箱化应用程序可能受到保护，免受主机资产上潜在恶意软件感染的影响。该模型的缺点之一是，企业必须为所有资产维护这些沙箱化应用程序，并且可能无法完全了解客户端资产。企业还需要确保每个沙箱化应用程序都是安全的，这可能比简单地监控设备需要更多的精力。

3.3 信任算法

对于部署了ZTA的企业，策略引擎可以被视为大脑，而PE的信任算法则是其主要思维过程。信任算法(TA)是策略引擎用于最终授予或拒绝对资源访问的过程。策略引擎从多个来源获取输入(见第3节)：包含关于主体、主体属性和角色、历史主体行为模式的可观察信息的策略数据库、威胁情报来源以及其他元数据来源。该过程可以归入广泛的类别，并在图7中可视化。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

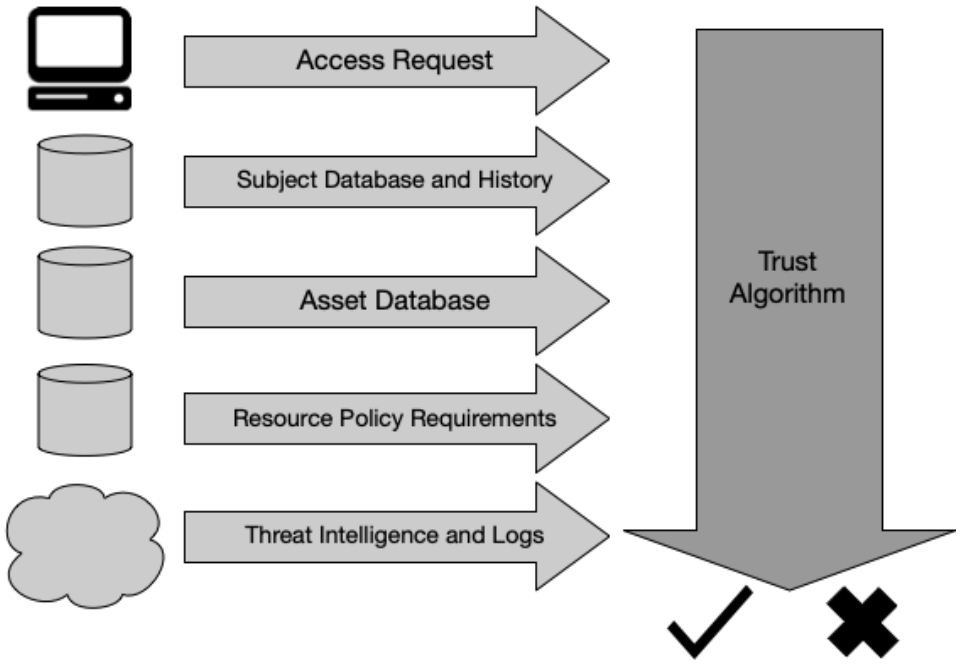


图 7：信任算法输入

在图中，输入可以根据它们向信任算法提供的内容分为不同类别。

- **访问请求：**这是来自主体的实际请求。所请求的资源是使用的主要信息，但关于请求者的信息也会被使用。这可以包括操作系统版本、使用的软件(例如，请求应用程序是否出现在已批准应用程序列表中?)和补丁级别。根据这些因素和资产安全态势，对资产的访问可能受到限制或被拒绝。

- **主体数据库：**这是请求访问资源的“谁”[SP800-63]。这是企业或协作方的主体(人员和进程)集合以及所分配的主体属性/权限的集合。这些主体和属性构成了资源访问策略的基础[SP800-162] [NISTIR 7987]。用户身份可以包括逻辑身份(例如账户ID)和PEP执行的身份验证检查结果的混合。可纳入置信水平推导的身份属性包括时间和地理位置。分配给多个主体的权限集合可以被视为一个角色，但权限应基于个体分配给主体，而不是仅仅因为他们可能适合组织中的某个特定角色。该集合应编码并存储在ID管理系统和策略数据库中。在某些(TA)变体中，这还可能包括关于过去观察到的主体行为的数据(见第3.3.1节)。

- **资产数据库(及可观察状态):**这是包含每个企业拥有(以及可能已知的非企业/BYOD)资产(在某种程度上包括物理和虚拟)已知状态的数据库。将其与发出请求的资产的可观察状态进行比较，可以包括操作系统版本、存在的软件及其完整性、

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

位置(网络位置和地理位置)以及补丁级别。根据资产状态与此数据库的比较，对资产的访问可能受到限制或被拒绝。

- **资源要求：**这组策略补充了用户ID和属性数据库[SP800-63]，并定义了对资源访问的最低要求。要求可能包括身份验证器保证级别，例如MFA网络位置(例如，拒绝来自海外IP地址的访问)、数据敏感性以及对资产配置的请求。这些要求应由数据保管人(即负责数据的人员)和负责使用数据的业务流程的人员(即负责任务的人员)共同制定。

- **威胁情报：**这是关于互联网上一般威胁和活跃恶意软件的信息源或信息源集合。这还可能包括从设备上看到的可能可疑的通信的具体信息(例如对可能的恶意软件命令与控制节点的查询)。这些信息源可以是外部服务或内部扫描和发现，并且可以包括攻击签名和缓解措施。这是唯一一个最有可能由服务而非企业控制的组件。

每个数据源的重要性权重可以是专有算法，也可以由企业配置。这些权重值可用于反映数据源对企业的重要性。

最终判定随后被传递给PA以执行。PA的职责是配置必要的PEP以启用授权通信。取决于ZTA的部署方式，这可能涉及向网关和代理或资源门户发送身份验证结果和连接配置信息。PA还可以暂停或搁置通信会话，以根据策略要求重新验证和重新授权连接。PA还负责根据策略发出终止连接的命令(例如，在超时后、工作流已完成时、由于安全警报)。

3.3.1 信任算法变体

实现TA有不同的方式。不同的实现者可能希望根据上述因素的重要性对其赋予不同的权重。还有两个主要特征可用于区分TA。第一个是这些因素如何评估，是作为二元决策还是作为整体“评分”或置信水平的加权部分。第二个是请求如何与同一主体、应用/服务或设备的其他请求相关联进行评估。

- **基于标准与基于评分：**基于标准的TA假定一组合格属性，在授予对资源的访问权限或允许某个操作(例如读/写)之前必须满足这些属性。这些标准由企业配置，并且应为每个资源独立配置。只有当所有标准都满足时，才授予访问权限或对资源应用操作。基于评分的TA根据每个数据源的值和企业配置的权重计算置信度。如果分数大于为该资源配置的阈值，则授予访问权限或执行该操作。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

否则，请求被拒绝，或访问权限被降低(例如，授予读访问权限但不授予对文件的写访问权限)。

- **单一式与上下文式：**单一式TA单独处理每个请求，并在进行评估时不考虑主体历史。这可以实现更快的评估，但如果攻击保持在主体的允许角色范围内，则存在攻击可能未被检测到的风险。上下文式TA在评估访问请求时会考虑主体或网络代理的近期历史。这意味着PE必须维护所有主体和应用程序的某种状态信息，但可能更有可能检测到使用被破坏的凭据以不同于PE针对给定主体所见的典型模式访问信息的攻击者。这也意味着PE必须由与主体在通信时交互的PA(和PEP)告知用户行为。对主体行为的分析可用于提供可接受使用的模型，偏离此行为可能触发额外的身份验证检查或资源请求拒绝。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

这两个因素并不总是相互依赖的。可以有一个TA为每个主体和/或设备分配置信级别，并且仍然独立地(即单一地)考虑每个访问请求。然而，基于上下文、基于评分的TA将能够提供更动态和更细粒度的访问控制，因为评分提供了请求账户的当前置信级别，并且比由人工管理员修改的静态策略更快地适应变化因素。

理想情况下，ZTA信任算法应是上下文相关的，但这在企业可用的基础设施组件下可能并不总是可行。上下文TA可以缓解攻击者针对被入侵主体账户或内部攻击保持接近“正常”访问请求集的威胁。在定义和实施信任算法时，平衡安全性、可用性和成本效益非常重要。针对与主体在组织内任务职能和角色的历史趋势和规范一致的行为，持续提示主体重新身份验证可能会导致可用性问题。例如，如果某机构HR部门的员工在典型工作日内通常访问20到30条员工记录，那么如果访问请求在一天内突然超过100条记录，上下文TA可能会发送警报。如果有人在正常工作时间之后发出访问请求，上下文TA也可能发送警报，因为这可能是攻击者利用被入侵的HR账户窃取记录。这些是上下文TA能够检测到攻击而单一TA可能无法检测到新行为的示例。在另一个示例中，一名通常在正常工作时间访问财务系统的会计现在试图在半夜从无法识别的位置访问系统。上下文TA可能触发警报，并要求主体满足更严格的置信级别或NIST Special Publication 800-63A[SP800-63A]中概述的其他标准。

为每个资源制定一组标准或权重/阈值需要规划和测试。企业管理员在ZTA初始实施期间可能会遇到问题，即本应批准的访问请求因配置错误而被拒绝。这将导致部署的初始“调优”阶段。可能需要调整标准或评分权重，以确保策略得到执行，同时仍允许企业业务流程运行。此调优阶段持续多长时间取决于企业定义的指标

用于工作流中所使用资源的进展和容忍不正确的访问拒绝/批准。

3.4 网络/环境组件

在ZT环境中，用于控制和配置网络的通信流与用于执行组织实际工作的应用/服务通信流之间应当存在分离(逻辑上或可能是物理上的)。这通常被分解为用于网络控制通信的控制平面和用于应用/服务通信流的数据平面[Gilman]。

控制平面由各种基础设施组件(企业自有和来自服务提供商的组件)使用，以维护和配置资产；判断、授予或拒绝对资源的访问；并执行任何必要操作以在资源之间建立通信路径。数据平面用于软件组件之间的实际通信。在通过控制平面建立路径之前，可能无法进行此通信通道。例如，PA和PEP可以使用控制平面来建立主体与企业资源之间的通信路径。然后，应用/服务工作负载将使用已建立的数据平面路径。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

3.4.1 支持零信任架构的网络要求

1. **企业资产具有基本网络连接性。**局域网(LAN)，无论是否由企业控制，提供基本路由和基础设施(例如DNS)。远程企业资产不一定使用所有基础设施服务。

2. **企业必须能够区分哪些资产由企业拥有或管理以及设备的当前安全态势。**这由企业颁发的凭证确定，而不使用无法认证的信息(例如可被欺骗的网络MAC地址)。

3. **企业可以观察所有网络流量。**企业记录在数据平面上看到的的数据包，即使它无法对所有数据包执行应用层检查(即OSI第7层)。企业过滤出关于连接的元数据(例如目的地、时间、设备身份)，以动态更新策略并在PE评估访问请求时通知PE。

4. **不访问PEP就不应能够访问企业资源。**企业资源不接受来自互联网的任意传入连接。资源仅在客户端经过身份验证和授权后才接受自定义配置的连接。这些通信路径由PEP建立。如果不访问PEP，资源甚至可能无法被发现。这可以防止攻击者通过扫描识别目标，和/或对位于PEP后面的资源发起DoS攻击。请注意，并非所有资源都应以这种方式隐藏；某些网络基础设施组件(例如DNS服务器)必须可访问。

5. **数据平面和控制平面在逻辑上分离。**策略引擎、策略管理器和PEP在逻辑上分离且企业资产和资源无法直接访问的网络上通信。数据平面用于

应用/服务数据流量。策略引擎、策略管理器和PEP使用控制平面来通信和管理资产之间的通信路径。PEP必须能够从数据平面和控制平面发送和接收消息。

6. **企业资产可以到达PEP组件。**企业主体必须能够访问PEP组件以获得对资源的访问。这可以采取Web门户、网络设备或企业资产上启用连接的软件代理的形式。

7. **PEP是作为业务流的一部分访问策略管理器的唯一组件。**在企业网络上运行的每个PEP都与策略管理器有连接，以建立从客户端到资源的通信路径。所有企业业务流程流量通过一个或多个PEP。

8. **远程企业资产应当能够访问企业资源而无需首先穿越企业网络基础设施。**例如，远程主体不应被要求使用回连到企业网络的链路(即虚拟专用网络[VPN])来访问由企业使用并由公共云提供商托管的服务(例如电子邮件)。

9. **用于支持ZTA访问决策过程的基础设施应具备可扩展性，以应对流程负载的变化。** ZTA中使用的PE、PA和PEP成为任何业务流程中的关键组件。延迟或无法到达PEP(或PEP无法到达PA/PE)会对工作流的执行能力产生负面影响。实施ZTA的企业需要为预期工作负载配置组件，或者能够在需要时快速扩展基础设施以处理增加的使用量。

10. **企业资产可能由于策略或可观察因素而无法到达某些PEP。**例如，可能存在策略规定如果请求资产位于企业所在国之外，则移动资产可能无法到达某些资源。这些因素可以基于位置(地理位置或网络位置)、设备类型或其他标准。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

4部署场景/使用案例

任何企业环境都可以在设计中考虑零信任原则。大多数组织已经在企业基础设施中具备零信任的某些要素，或者正在通过实施信息安全与弹性策略及最佳实践来推进。若干部署场景和用例天然适合零信任架构。例如，ZTA源于地理上分散和/或拥有高度移动员工队伍的组织。尽管如此，任何组织都可以从零信任架构中受益。

在以下用例中，ZTA未被明确指示，因为企业可能同时具有基于边界的和可能的ZTA基础设施。如第7.2节所讨论的，很可能存在一个时期，ZTA组件和基于边界的网络基础设施在企业中同时运行。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

4.1 拥有卫星设施的企业

最常见的场景涉及一个拥有单一总部和一个或多个地理上分散位置的企业，这些位置之间没有通过企业拥有的物理网络连接相连(见图8)。远程位置的员工可能没有完整的企业自有本地网络，但仍需要访问企业资源以执行任务。企业可能有一条到企业总部网络的MPLS链路，但可能没有足够的带宽承载所有流量，或者可能不希望发往基于云的应用/服务的流量经过企业总部网络。同样，员工可能正在远程办公或处于远程位置，并使用企业自有或个人拥有的设备。在这种情况下，企业可能希望授予对某些资源(例如员工日历、电子邮件)的访问权限，但拒绝对更敏感资源(例如HR数据库)的访问或限制操作。

在此用例中，PE/PA通常作为云服务托管(云服务通常提供更优的可用性，并且不要求远程工作人员依赖企业基础设施来访问云资源)，终端资产安装有代理(见第3.2.1节)或访问资源门户(见第3.2.3节)。将PE/PA托管在企业本地网络上可能响应性不是最佳，因为远程办公室和工作人员必须将所有流量发送回企业网络才能到达由云服务托管的应用/服务。

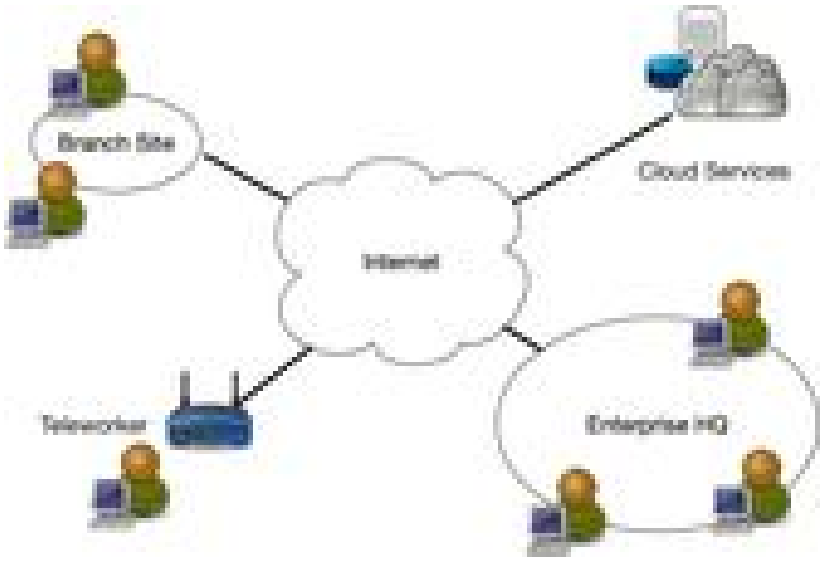


图8：拥有远程员工的企业

4.2 多云/云到云企业

部署ZTA的一个日益常见的用例是企业使用多个云提供商(见图9)。在此用例中，企业拥有本地网络，但使用两个或多个云服务提供商来托管应用/服务和数据。有时，应用/服务托管在与数据源分离的云服务上。为了性能和易于管理，托管在云提供商A中的应用应能够直接连接到托管在云提供商B中的数据源，而不是强制应用通过企业网络隧道回传。

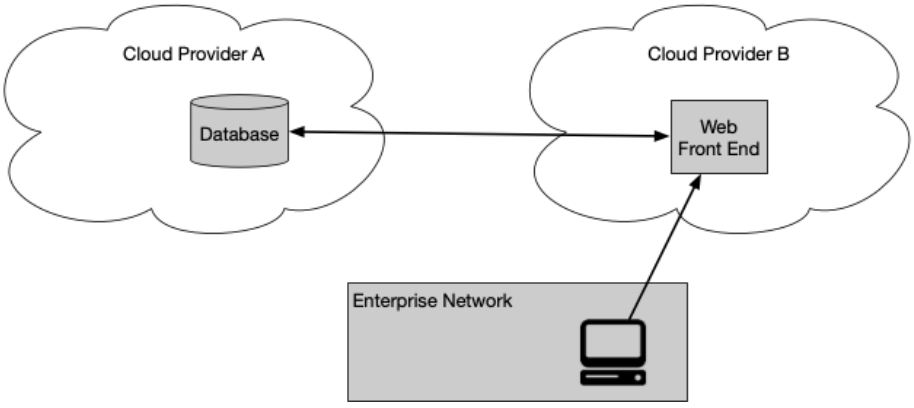


图 9：多云用例

此用例是CSA软件定义边界(SDP)规范[CSA-SDP]的服务器-服务器实现。随着企业迁移到更多云托管的应用和服务，依赖企业边界进行安全防护变得明显是一种负担。如第2.2节所述，ZT原则认为企业拥有和运营的网络基础设施与任何其他服务提供商拥有和运营的基础设施之间不应有区别。多云的零信任方法是将PEP放置在

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

每个应用/服务和数据源的接入点。PE和PA可以是位于任一云中甚至第三方云提供商上的服务。然后，客户端(通过门户或本地安装的代理)直接访问PEP。这样，即使资源托管在企业外部，企业仍然可以管理对资源的访问。一个挑战是不同云提供商有独特的实现类似功能的方式。企业架构师需要了解如何针对他们使用的每个云提供商实施企业ZTA。

4.3 采用外包服务和/或非员工访问的企业

另一个常见场景是企业包含需要有限访问企业资源以完成工作的现场访客和/或签约服务提供商(见图10)。例如，企业拥有自己的内部应用/服务、数据库和资产。这些包括外包给可能偶尔现场提供维护的提供商的服务(例如，由外部提供商拥有和管理的智能供暖和照明系统)。这些访客和服务提供商需要网络连接来执行任务。零信任企业可以通过允许这些设备和任何来访服务技术人员访问互联网同时隐藏企业资源来促进这一点。

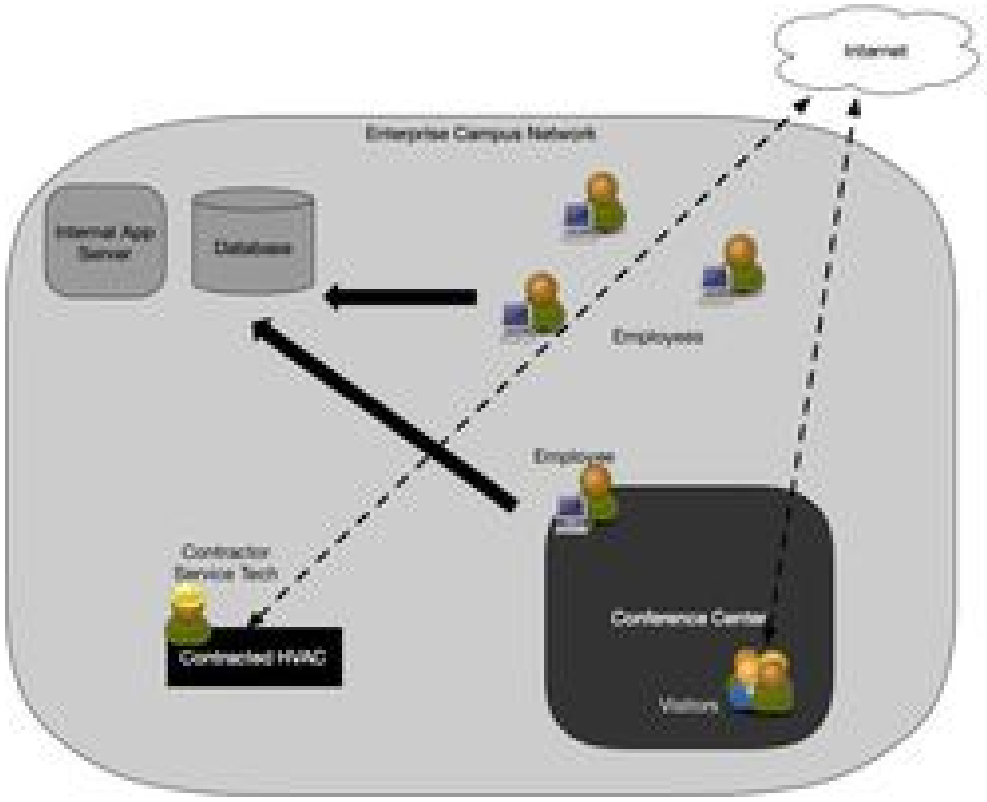


图10：拥有非员工访问权限的企业

在此示例中，组织还设有一个会议中心，访客在此与员工互动。同样，采用SDP的ZTA方法，员工设备和主体被区分开来，并且可能能够访问适当的企业资源。园区访客可以访问互联网，但不能访问企业资源。他们甚至可能无法

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

通过网络扫描发现企业服务(即防止主动网络侦察/东西向移动)。

在此用例中，PE和PA可以托管为云服务或托管在LAN上(假设很少或根本不使用云托管服务)。企业资产可以安装代理(见第3.2.1节)或通过门户访问资源(见第3.2.3节)。PA确保所有非企业资产(那些未安装代理或无法连接门户的资产)不能访问本地资源，但可以访问互联网。

4.4 跨企业边界的协作

第四个用例是跨企业协作。例如，有一个涉及企业A和企业B员工的项目(见图11)。这两个企业可能是独立的联邦机构(G2G)，甚至可能是联邦机构和私营企业(G2B)。企业A运营用于项目的数据库，但必须允许企业B的某些成员访问数据。企业A可以为企业B的员工设置专用账户以访问所需数据并拒绝访问所有其他资源，但这很快会变得难以管理。让两个组织都注册到联邦身份管理系统中，将允许更快地建立这些关系，前提是两个组织的PEP都能在联邦身份社区中对主体进行身份验证。

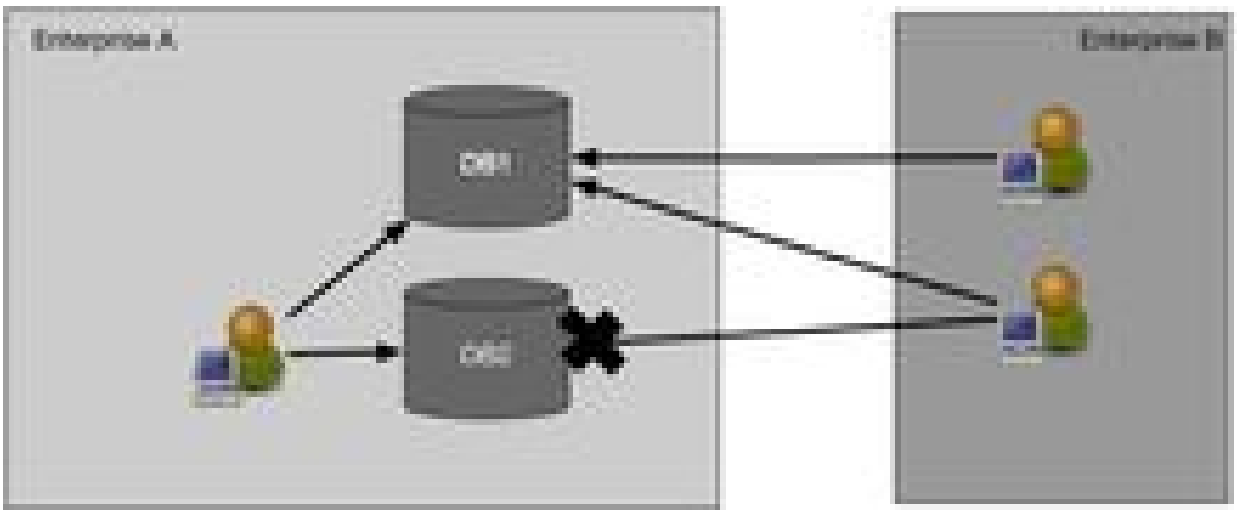


图11：跨企业协作

此场景可能类似于用例1(第4.1节)，因为两个企业的员工可能并不位于其组织的网络基础设施上，并且他们需要访问的资源可能位于某个企业环境内或托管在云中。这意味着无需复杂的防火墙规则或企业范围的访问控制列表(ACL)来允许属于企业B的特定IP地址基于企业A的访问策略访问企业A中的资源。如何实现这种访问取决于所使用的技术。与用例1类似，作为云服务托管的PE和PA可以为所有各方提供可用性，而无需建立VPN或类似机制。企业B的员工可能被要求在其实产上安装软件代理，或通过Web网关访问必要的数据资源(见第3.2.3节)。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

4.5 面向公众或客户服务的企业

许多企业的一个常见特征是面向公众的服务，该服务可能包含也可能不包含用户注册(即，用户必须创建或已被发放一组登录凭证)。此类服务可能面向一般公众、具有现有业务关系的一组客户，或特殊的一组非企业用户(如员工家属)。在所有情况下，请求资产很可能并非企业所有，企业在可强制执行哪些内部网络安全策略方面受到限制。

对于不需要登录凭据即可访问的通用、面向公众的资源(例如公共网页),ZTA的原则不直接适用。企业无法严格控制请求资产的状态，而匿名公共资源(例如公共网页)不需要凭据即可访问。

企业可为注册的公共用户(如客户，即具有业务关系的用户)和特殊用户(如员工家属)制定策略。如果要求用户提供或被发放凭证，企业可制定关于密码长度、生命周期和其他细节的策略，并可提供MFA作为选项或要求。然而，企业对此类用户可实施的策略是有限的。关于传入请求的信息可能有助于确定公共服务状态并检测伪装成合法用户的可能攻击。例如，已知注册用户门户由注册客户使用一组常见Web浏览器之一进行访问。来自未知浏览器类型或已知过时版本的访问请求突然增加可能表明某种自动化攻击，企业可采取措施限制来自这些已识别客户端的请求。企业还应了解关于可收集和记录哪些请求用户及资产信息的任何法规或规定。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

5与零信任架构相关的威胁

没有企业能够消除网络安全风险。当与现有的网络安全策略和指南、身份和访问管理、持续监控以及一般网络卫生相结合时，正确实施和维护的ZTA可以降低整体风险并防范常见威胁。然而，在实施ZTA时，某些威胁具有独特特征。

5.1 颠覆ZTA决策过程

在ZTA中，策略引擎和策略管理器是整个企业的关键组件。除非经PE和PA批准并可能由其配置，否则企业资源之间不会发生通信。这意味着这些组件必须得到正确配置和维护。任何具有PE规则配置访问权限的企业管理员都可能执行未经批准的更改或犯错，从而扰乱企业运营。同样，被攻陷的PA可能允许访问原本不会被批准的资源(例如，访问被颠覆的个人拥有设备)。缓解相关风险意味着必须正确配置和监控PE和PA组件，并且任何配置更改都必须记录并接受审计。

5.2 拒绝服务或网络中断

在ZTA中，PA是资源访问的关键组件。未经PA许可并可能未经其配置操作，企业资源无法相互连接。如果攻击者扰乱或拒绝访问PEP或PE/PA(即DoS攻击或路由劫持)，则可能对企业运营产生不利影响。企业可通过将策略执行置于适当安全的云环境中，或按照网络弹性指南[SP 800-160v2]在多个位置进行复制来缓解此威胁。

这降低了风险但并未消除风险。像Mirai这样的僵尸网络会对关键互联网服务提供商发起大规模DoS攻击，并中断对数百万互联网用户的服务。[5]攻击者也有可能拦截并阻断来自企业内部分或全部用户账户(例如分支机构甚至单个远程员工)发往PEP或PA的流量。在这种情况下，只有部分企业主体受到影响。这在传统远程访问VPN中也有可能发生，并非ZTA所独有。

托管提供商也可能意外地使基于云的PE或PA离线。云服务过去曾经历过中断，包括基础设施即服务(IaaS)[6]和SaaS。[7]如果策略引擎或策略管理器组件无法从网络访问，操作错误可能会阻止整个企业运作。

5 https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

6

7 https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12286870

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

还存在企业资源可能无法从PA到达的风险，因此即使授予主体访问权限，PA也无法配置来自网络的通信路径。这可能由于DDoS攻击或仅仅由于意外的高使用率而发生。这类似于任何其他网络中断，即部分或所有企业主体由于该资源因某种原因不可用而无法访问特定资源。

5.3 凭据被盗/内部威胁

正确实施的ZT、信息安全与弹性策略以及最佳实践可降低攻击者通过窃取凭据或内部攻击获得广泛访问权限的风险。ZT基于网络位置不提供隐式信任的原则意味着攻击者需要攻陷现有账户或设备才能在企业中获得立足点。正确开发和实施的ZTA应能防止被攻陷的账户或资产访问其正常权限范围或访问模式之外的资源。这意味着，围绕攻击者感兴趣的资源设有访问策略的账户将成为攻击者的主要目标。

攻击者可能使用网络钓鱼、社会工程或组合攻击来获取有价值账户的凭据。“有价值”可能因攻击者的动机而有不同含义。例如，企业管理员账户可能有价值，但以经济利益为动机的攻击者可能认为有权访问财务或支付资源的账户具有同等价值。对访问请求实施MFA可降低因账户被攻陷而导致信息丢失的风险。然而，拥有有效凭据的攻击者(或恶意内部人员)仍可能访问该账户已被授予访问权限的资源。例如，拥有有效人力资源员工凭据和企业自有资产的攻击者或被攻陷员工仍可能访问员工数据库。

ZTA降低风险并防止任何被攻陷的账户或资产在网络中横向移动。如果被攻陷的凭据未被授权访问特定资源，它们将继续被拒绝访问该资源。此外，上下文信任算法(见第3.3.1节)比在传统的基于边界的网络中更有可能检测并快速响应此类攻击。上下文TA可以检测偏离正常行为的访问模式，并拒绝被攻陷账户或内部威胁访问敏感资源。

5.4 网络可见性

如第3.4.1节所述，所有流量都在网络上被检查和记录，并进行分析以识别和响应针对企业的潜在攻击。然而，如前所述，企业网络上的部分(可能是大部分)流量对第3层网络分析工具可能是不透明的。这些流量可能来自非企业自有资产(例如使用企业基础设施访问互联网的承包服务)或抗拒被动监控的应用程序/服务。无法执行深度包检测或检查加密流量的企业必须使用其他方法来评估网络上可能的攻击者。

这并不意味着企业无法分析其在网络上看到的加密流量。企业可以收集关于以下内容的元数据（例如源地址和目的地址等）

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

加密流量的元数据(例如源地址和目的地址等)，并利用其检测网络上通信的活跃攻击者或可能的恶意软件。机器学习技术[Anderson]可用于分析无法解密和检查的流量。采用此类机器学习将使企业能够将流量分类为有效或可能恶意并需修复。

5.5 系统和网络信息的存储

企业网络流量监控与分析面临的一个相关威胁是分析组件本身。如果监控扫描、网络流量和元数据被存储用于构建上下文策略、取证或后续分析，这些数据就会成为攻击者的目标。就像网络拓扑图、配置文件和其他各类网络架构文档一样，这些资源应当受到保护。如果攻击者能够成功获取这些信息，他们可能借此深入了解企业架构，并识别资产以进行进一步的侦察和攻击。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

在ZT企业中，攻击者的另一个侦察信息来源是用于编码访问策略的管理工具。与存储的流量一样，此组件包含对资源的访问策略，并可以向攻击者提供哪些账户最值得入侵的信息(例如，那些有权访问所需数据资源的账户)。

对于所有有价值的企业数据，应实施充分的保护措施以防止未经授权的访问和访问尝试。由于这些资源对安全至关重要，它们应具有最严格的访问策略，并且只能从指定或专用管理员账户访问。

5.6 依赖专有数据格式或解决方案

零信任架构依赖多种不同的数据源来做出访问决策，包括有关请求主体、所用资产、企业和外部情报以及威胁分析的信息。通常，用于存储和处理这些信息的资产缺乏关于如何交互和交换信息的通用开放标准。这可能导致企业因互操作性问题而被锁定在部分提供商之中。如果某个提供商出现安全问题或服务中断，企业可能无法在不付出极高成本(例如更换多个资产)或不经历漫长过渡过程(例如将策略规则从一种专有格式转换为另一种)的情况下迁移到新的提供商。与拒绝服务攻击一样，这一风险并非零信任架构所独有，但由于零信任架构高度依赖信息的动态访问(包括企业和 service providers)，中断可能影响企业的核心业务功能。为缓解相关风险，企业应在整体基础上评估 service providers，除性能、稳定性等更典型的因素外，还应考虑供应商安全控制、企业切换成本和供应链风险管理等因素。

5.7 非人员实体(NPE)在ZTA管理中的使用

人工智能和其他基于软件的代理正被部署用于管理企业网络上的安全问题。这些组件需要与ZTA的管理组件(例如策略引擎、策略管理器)交互，有时替代人类管理员。这些组件在实施

ZTA的企业中如何自我身份验证是一个开放问题。假设大多数自动化技术系统在使用API访问资源组件时会使用某种方式进行身份验证。

使用自动化技术进行配置和策略执行时的最大风险是误报(无害操作被误认为攻击)和漏报(攻击被误认为正常活动)影响企业安全态势的可能性。这可以通过定期重新调整分析来纠正错误决策并改进决策过程来减少。

相关风险在于，攻击者可能诱导或胁迫某个 NPE 执行攻击者无权执行的某些任务。与人类用户相比，软件代理在执行管理或安全相关任务时可能具有较低的身份验证门槛(例如 API 密钥而非 MFA)。如果攻击者能够与该代理交互，理论上可以诱骗该代理允许攻击者获得更大访问权限，或代表攻击者执行某些任务。还存在一种风险，即攻击者可能获取软件代理的凭据，并在执行任务时冒充该代理。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

6 零信任架构与现有联邦指南可能的交互

若干现有联邦政策和指南与ZTA的规划、部署和运营相交。这些政策并不禁止企业转向更面向零信任的架构，但可以影响机构零信任策略的制定。当与现有的网络安全策略和指南、ICAM、持续监控以及一般网络卫生相结合时，ZTA可以强化组织的安全态势并防范常见威胁。

6.1 ZTA与NIST风险管理框架

零信任架构部署涉及围绕指定任务或业务流程的可接受风险制定访问策略(见第 7.3.3 节)。可以拒绝对某资源的所有网络访问，仅允许通过连接的终端访问，但在大多数情况下这种限制过于严格，可能妨碍工作完成。联邦机构为履行其使命，存在可接受的风险水平。必须识别和评估与执行给定任务相关的风险，并予以接受或缓解。为协助完成这一工作，NIST 制定了风险管理框架(RMF) [SP800-37]。

ZTA规划和实施可能会改变企业定义的授权边界。这是由于增加了新组件(例如策略引擎、策略管理器和PEP)以及减少了对网络边界防御的依赖。RMF中描述的总体流程在ZTA中不会改变。

6.2 零信任与 NIST 隐私框架

保护用户隐私和私人信息(例如个人可识别信息)是组织的首要关切。隐私和数据保护被纳入 FISMA 和《健康保险携带与责任法案》(HIPAA)等合规计划。为此，NIST 制定了供组织使用的隐私框架 [NISTPRIV]。该文件提供了一个框架，用于描述隐私风险和缓解策略，以及企业识别、衡量和缓解用户隐私及组织存储和处理的私人信息所面临风险的流程。这包括企业用于支持零信任架构运营的个人信息，以及访问请求评估中使用的任何生物特征属性。

ZT核心要求的一部分是，企业应检查并记录其环境中的流量(或至少在处理监控系统无法解密的流量时记录并检查元数据)。其中一些流量可能包含私人信息或存在相关隐私风险。组织需要识别与拦截、扫描和记录网络流量相关的任何可能风险[NISTIR 8062]。这可能包括告知用户、获取同意(通过登录页面、横幅或类似方式)以及教育企业用户等行动。NIST隐私框架[NISTPRIV]有助于制定正式流程，以识别和缓解企业开发零信任架构时任何与隐私相关的风险。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

6.3 ZTA与联邦身份、凭据和访问管理架构

主体配置是ZTA的关键组成部分。如果PE没有足够的信息来识别相关主体和资源，策略引擎就无法确定尝试的连接是否被授权连接到资源。在转向更符合零信任的部署之前，需要制定强有力的主体配置和身份验证策略。企业需要一套清晰的主体属性和策略，供PE用于评估访问请求。

管理和预算办公室(OMB)发布了M-19-17，旨在改进联邦政府的身份管理。该政策的目标是制定“.....一个共同愿景，将身份作为任务交付、信任和国家安全的使能因素”[M-19-17]。该备忘录呼吁所有联邦机构成立ICAM办公室，以治理与身份发放和管理相关的工作。其中许多管理政策应使用NIST SP 800-63-3《数字身份指南》[SP800-63]中的建议。由于ZTA严重依赖精确的身份管理，任何ZTA工作都需要整合机构的ICAM政策。

6.4 零信任架构与可信互联网连接 3.0

TIC是一项由OMB、DHS和总务管理局(GSA)共同管理的联邦网络安全倡议，旨在为联邦政府建立网络安全基线。历史上，TIC是一种基于边界的网络安全策略，要求机构整合并监控其外部网络连接。TIC 1.0和TIC 2.0固有的假设是边界内部是“可信的”，而ZTA假设网络位置不能推断“信任”(即机构内部网络上不存在“信任”)。TIC 2.0提供了一系列基于网络的安全能力(例如内容过滤、监控、身份验证等)，部署在机构边界的TIC接入点；其中许多能力与ZT原则一致。

TIC 3.0已更新以适应云服务和移动设备[M-19-26]。在TIC 3.0中，认识到“信任”的定义可能因具体计算环境而异，且机构对定义信任区域有不同的风险容忍度。此外，TIC 3.0更新了TIC安全能力手册，定义了两种类型的安全能力：(1)适用于企业级别的通用安全能力，以及(2)PEP安全能力，即根据TIC用例定义，应用于多个策略执行点(PEP)的网络级能力。PEP安全能力可应用于给定数据流沿途的任何适当PEP，而非仅应用于机构边界的单一PEP。TIC 3.0的许多安全能力直接支持ZTA(例如加密流量、强身份验证、微隔离、网络和系统清单等)。TIC 3.0定义了具体用例，描述跨特定应用、服务和环境的信任区域和安全能力的实施。

TIC 3.0侧重于基于网络的安全保护，而ZTA是更包容的架构，涉及应用、用户和数据保护。随着TIC 3.0用例的发展，很可能会开发ZTA TIC用例，以定义在ZTA执行点部署的网络保护。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

6.5 ZTA与EINSTEIN(NCPS - 国家网络安全保护系统)

NCPS(在操作层面称为EINSTEIN)是一个集成的系统之系统，提供入侵检测、高级分析、信息共享和入侵防御能力，以保护联邦政府免受网络威胁。NCPS的目标与零信任的总体目标一致，即管理网络风险、改善网络保护并赋能合作伙伴保障网络空间安全。EINSTEIN传感器使CISA的国家网络安全和通信集成中心(NCCIC)能够防御联邦网络并响应联邦机构的重大事件。

NCPS传感器用于DHS态势感知的部署基于联邦政府的边界网络防御，而ZTA将保护措施移至更靠近资产、数据及所有其他资源的位置。NCPS项目正在演进，以确保通过利用基于云的流量的安全信息来保持态势感知，帮助为来自ZTA系统的扩展态势感知遥测奠定基础。NCPS入侵防御功能也需要演进，以便能够在当前NCPS位置以及ZTA系统上为策略执行提供信息。随着ZTA在联邦政府中的采用，NCPS的实施将需要持续演进，或者需要部署新能力以实现NCPS目标。事件响应人员可能利用已实施零信任架构的联邦机构可获得的身份验证、流量检查和机构流量日志信息。ZTA中生成的信息可能更好地为事件影响量化提供信息；机器学习工具可以使用ZTA数据来改进检测；来自ZTA的额外日志可保存下来，供事件响应人员进行事后分析。

6.6 ZTA与DHS持续诊断和缓解(CDM)计划

DHS CDM计划是改善联邦机构信息技术(IT)的一项努力。该态势的关键是机构对自身资产、配置和主体的洞察。为了保护系统，机构需要建立流程来发现和理解其基础设施中的基本组件和参与者：

- **连接了什么?**组织使用了哪些设备、应用和服务?这包括在发现漏洞和威胁时观察并改善这些工件的安全态势。
- **谁在使用网络?**哪些用户属于组织或属于被允许访问企业资源的外部人员?这些包括可能执行自主操作的NPE。
- **网络上发生了什么?**企业需要洞察系统之间的流量模式和消息。
- **数据如何受到保护?**企业需要制定关于信息在静态、传输和使用中如何保护的既定策略。

拥有强大的CDM计划实施是ZTA成功的关键。例如，要转向ZTA，企业必须拥有发现和记录物理及虚拟资产的系统，以创建可用的清单。DHS CDM计划已启动多项努力，以构建联邦机构内部转向ZTA所需的能力。例如，DHS

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

硬件资产管理(HWAM)[HWAM]计划旨在帮助机构识别其网络基础设施上的设备，以部署安全配置。这类似于制定零信任架构路线图的第一步。机构必须能够了解网络上活跃的资产(或远程访问资源的资产)，以便对网络活动进行分类、配置和监控。

6.7 ZTA、Cloud Smart 和联邦数据战略

Cloud Smart [8]战略、更新的数据中心优化倡议 [M-19-19] 政策以及联邦数据战略[9]都影响着机构规划零信任架构的部分要求。这些政策要求机构对本地和云端数据的收集、存储和访问方式进行清点和评估。

这一清点对于确定哪些业务流程和资源将从实施零信任架构中受益至关重要。主要以云为基础或主要由远程工作人员使用的数据资源以及应用和服务是零信任架构方法的良好候选对象(见第7.3.3节)，因为主体和资源位于企业网络边界之外，并且很可能在使用、可扩展性和安全性方面获得最大收益。

联邦数据战略的另一个考虑因素是如何使机构数据资产可供其他机构或公众访问。这与跨企业协作零信任架构用例相对应(见第4.4节)。将这些资产用于零信任架构的机构在制定战略时可能需要考虑协作或发布要求。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

[8] ategy/

[9]联邦数据战略：https://strategy.data.gov/

7迁移到零信任架构

实施ZTA是一个旅程，而不是对基础设施或流程的整体替换。组织应寻求渐进式实施零信任原则、流程变更和技术解决方案，以保护其最高价值的数据资产。大多数企业将在无限期内继续以零信任/基于边界的混合模式运营，同时继续投资于正在进行的IT现代化举措。拥有包含向基于ZT原则的架构迁移的IT现代化计划，可能有助于企业形成小规模工作流迁移的路线图。

企业如何迁移到某种策略取决于其当前的网络安全态势和运营。企业应达到能力基线，之后才有可能部署重要的以ZT为重点的环境[ACT-IAC]。该基线包括为企业识别并编目资产、主体、业务流程、流量和依赖关系映射。企业需要这些信息，才能制定候选业务流程清单以及该流程中涉及的主体/资产。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

7.1 纯零信任架构

在绿地方法中，可以从头构建零信任架构。假设企业知道其希望用于运营的应用程序/服务和工作流，它就可以基于这些工作流的零信任原则生成架构。一旦识别出工作流，企业就可以缩小所需组件的范围，并开始映射各个组件如何交互。从那时起，就是构建基础设施和配置组件的工程和组织工作。这可能包括额外的组织变更，具体取决于企业当前的设置和运营方式。

在实践中，这对于联邦机构或任何拥有现有网络的组织来说很少是可行选项。然而，有时组织可能被要求履行新的职责，从而需要构建自己的基础设施。在这些情况下，可能在一定程度上引入ZT概念。例如，某个机构可能被赋予一项新职责，需要构建新的应用程序、服务或数据库。该机构可以围绕ZT原则和安全系统工程[SP8900-160v1]设计新所需的基础设施，例如在授予访问权限之前评估主体的信任，并围绕新资源建立微边界。成功程度取决于该新基础设施对现有资源(例如ID管理系统)的依赖程度。

7.2 混合零信任架构与基于边界的架构

任何重要的企业都不太可能在单个技术更新周期内迁移到零信任。在企业中，ZTA工作流与非ZTA工作流共存的时间可能会无限期延长。向ZTA方法的迁移可能一次只针对一个业务流程进行。企业需要确保通用元素(例如，ID管理、设备管理、事件日志记录)足够灵活，以便在ZTA和基于边界的安全混合架构中运行。企业架构师可能还希望将ZTA候选解决方案限制为那些能够与现有组件接口的方案。

将现有工作流迁移到零信任架构很可能需要(至少)进行部分重新设计。企业可以利用这一机会采用安全系统工程[SP800-160v1]实践，前提是它们尚未在工作流中采用这些实践。

7.3 将零信任架构引入基于边界的架构网络的步骤

迁移到零信任架构要求组织对其资产(物理和虚拟)、主体(包括用户权限)和业务流程有详细的了解。策略引擎在评估资源请求时会访问这些知识。知识不完整通常会导致业务流程失败，即策略引擎因信息不足而拒绝请求。如果组织内存在未知的“影子IT”部署，这尤其是一个问题。

在着手将ZTA引入企业之前，应当对资产、主体、数据流和工作流进行调查。这种认知构成了实现ZTA部署之前必须达到的基础状态。如果对当前运营状态一无所知，企业就无法确定需要建立哪些新流程或系统。这些调查可以并行进行，但两者都与对组织业务流程的审查相关联。这些步骤可以映射到RMF[SP800-37]中的步骤，因为任何ZTA的采用都是降低机构业务功能风险的过程。实施ZTA的路径可以在图12中可视化。

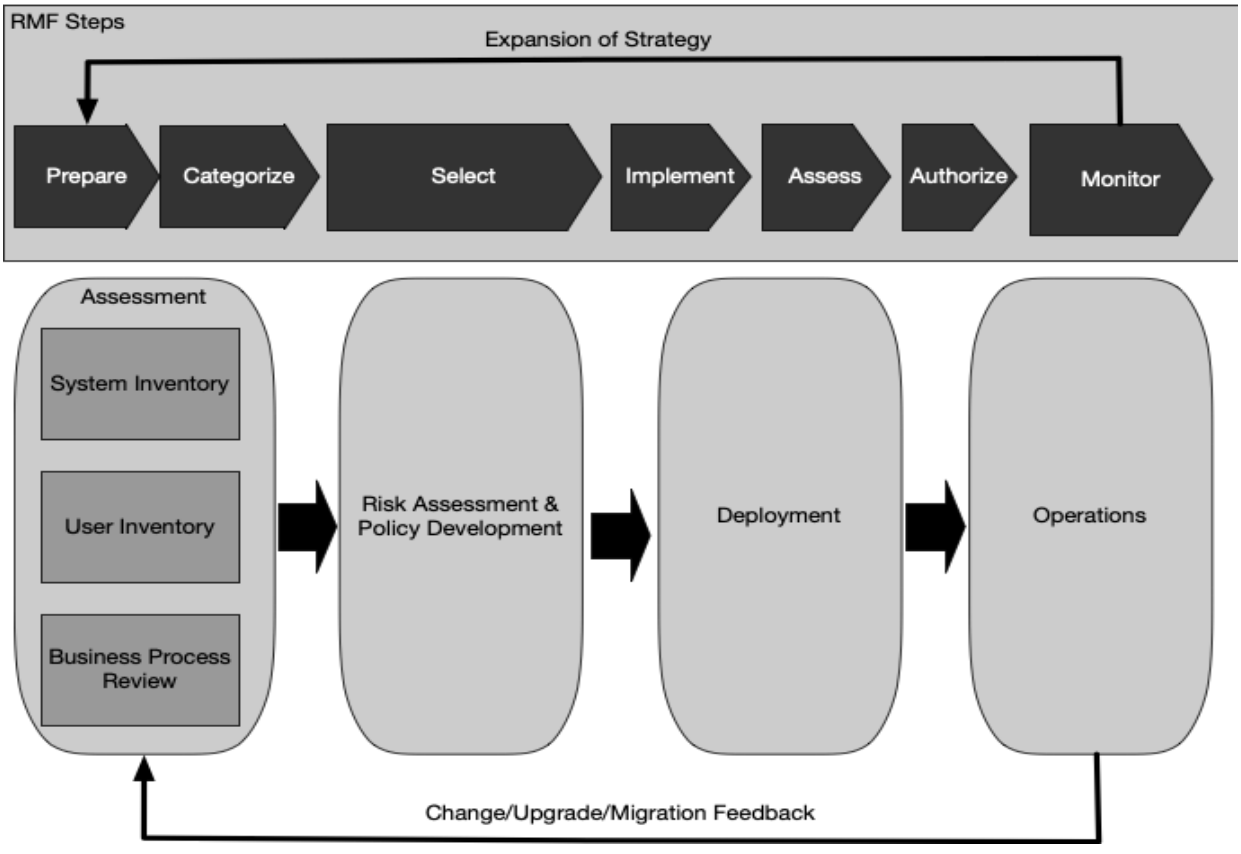


图 12:ZTA 部署周期

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

在创建初始清点之后，存在定期的维护和更新周期。这种更新可能改变业务流程，也可能没有任何影响，但应当对业务流程进行评估。例如，数字证书提供商的变化可能看起来没有重大影响，但可能涉及证书根存储管理、证书透明度日志监控以及其他起初不明显的因素。

7.3.1 识别企业中的行为主体

零信任企业要运作，策略引擎必须了解企业主体。
主体可以包括人类以及可能的非人类实体(NPE)，例如与资源交互的服务账户。

拥有特殊权限的用户，例如开发人员或系统管理员，在分配属性或角色时需要额外的审查。在许多传统安全架构中，这些账户可能拥有访问所有企业资源的全面权限。ZTA应允许开发人员和管理员拥有足够的灵活性以满足其业务需求，同时使用日志和审计操作来识别访问行为模式。ZTA部署可能要求管理员满足NIST SP 800-63A第5节[SP800-63A]中概述的更严格的置信水平或标准。

7.3.2 识别企业拥有的资产

如第2.1节所述，ZTA的关键要求之一是识别和管理设备的能力。ZTA还要求能够识别和监控可能位于企业拥有的网络基础设施上或访问企业资源的非企业拥有的设备。管理企业资产的能力是成功部署ZTA的关键。这包括硬件组件(例如，笔记本电脑、手机、IoT设备)和数字制品(例如，用户账户、应用程序、数字证书)。可能无法对所有企业拥有的资产进行全面普查，因此企业应考虑建立快速识别、分类和评估企业拥有基础设施上新发现资产的能力。

这不仅仅是编目和维护企业资产数据库。这还包括配置管理和监控。观察资产当前状态的能力是评估访问请求过程的一部分(见第2.1节)。这意味着企业必须能够配置、调查和更新企业资产，例如虚拟资产和容器。这还包括其物理位置(尽可能估计)和网络位置。这些信息应为PE在做出资源访问决策时提供依据。

非企业所有的资产和企业所有的“影子IT”也应尽可能编入目录。这可能包括企业可见的任何信息(例如MAC地址、网络位置)，并由管理员数据录入加以补充。这些信息不仅用于访问决策(因为协作者和BYOD资产可能需要联系PEP)，还用于企业的监控和取证日志记录。影子IT带来一个特殊问题，即这些资源为企业所有，但不像其他资源那样受到管理。某些ZTA方法(主要是基于网络的方法)甚至可能导致影子IT组件变得不可用，因为它们可能不为人知，也未纳入网络访问策略。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

许多联邦机构已经开始识别企业资产。已建立CDM计划能力(如HWAM[HWAM]和软件资产

管理(SWAM)[SWAM])的机构在实施零信任架构时有丰富的数据可供利用。机构还可能有一份涉及高价值资产
(HVA)[M-19-03]的零信任架构候选流程清单，这些资产已被确定为机构任务的关键。在任何业务流程能够以零信任架构进行(重新)设计之前，这项工作需要在企业或机构范围内存在。这些计划必须设计为可扩展并能适应企业的变化，不仅是在迁移到零信任架构时，而且在考虑成为企业一部分的新资产、服务和业务流程时也是如此。

7.3.3 识别关键流程并评估与执行流程相关的风险

机构应开展的第三项清点是识别并排列业务流程、数据流及其在机构使命中的关系。业务流程应说明资源访问请求被授予和拒绝的情形。企业可能希望从低风险业务流程开始首次向ZTA过渡，因为中断可能不会对整个组织产生负面影响。一旦获得足够经验，更关键的业务流程就可以成为候选对象。

利用基于云的资源或由远程工作人员使用的业务流程通常是ZTA的良好候选对象，并且可能会看到可用性和安全性的改善。企业客户端可以直接请求云服务，而不是将企业边界投射到云中或通过VPN将客户端带入企业网络。企业的PEP确保在向客户端授予资源访问权限之前遵循企业策略。规划者还应考虑在为给定业务流程实施ZTA时可能出现的性能、用户体验以及可能增加的工作流脆弱性方面的潜在权衡。

7.3.4 为零信任架构候选方案制定策略

识别候选服务或业务工作流的过程取决于几个因素：流程对组织的重要性、受影响的主体群体以及用于该工作流的资源的当前状态。资产或工作流基于其风险的价值可以使用NIST风险管理框架[SP800-37]进行评估。

在识别资产或工作流之后，识别该工作流使用或受影响的所有上游资源(例如身份管理系统、数据库、微服务)、下游资源(例如日志记录、安全监控)和实体(例如主体、服务账户)。这可能影响作为首次向ZTA迁移的候选选择。由已识别的企业主体子集使用的应用/服务(例如采购系统)可能比对企业整个主体群至关重要的应用/服务(例如电子邮件)更受青睐。

然后，企业管理员需要为候选业务流程中使用的资源确定一组标准(如果使用基于标准的信任算法)或置信水平权重(如果使用基于评分的信任算法)(见第3.3.1节)。管理员可能需要在调优阶段调整这些标准或值。这些调整对于确保策略有效但不妨碍对资源的访问是必要的。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

7.3.5 识别候选解决方案

一旦制定了候选业务流程列表，企业架构师就可以编制候选解决方案列表。某些部署模型(见第3.1节)更适合特定的工作流和当前企业生态系统。同样，某些供应商解决方案比其他解决方案更适合某些用例。以下是一些需要考虑的因素：

- **解决方案是否要求在客户端资产上安装组件?**这可能限制使用或期望使用非企业所有资产的业务流程，例如BYOD或跨机构协作。

- **解决方案是否在业务流程资源完全存在于企业场所内的情况下工作?**某些解决方案假设请求的资源将驻留在云中(所谓的南北向流量)，而不是在企业边界内(东西向流量)。候选业务流程资源的位置将影响候选解决方案以及该流程的ZTA。

- **解决方案是否提供记录交互以供分析的手段?**ZT的一个关键组件是收集和使用与流程流相关的数据，这些数据在做出访问决策时反馈给PE。

- **解决方案是否提供对不同应用程序、服务和协议的广泛支持?**某些解决方案可能支持广泛的协议(web、secure shell[SSH]等)和传输(IPv4和IPv6)，而其他解决方案可能仅适用于狭窄的焦点，例如web或电子邮件。

- **解决方案是否要求更改主体行为?**某些解决方案可能需要额外步骤来执行给定工作流。这可能改变企业主体执行工作流的方式。

一种解决方案是将现有业务流程建模为试点项目，而不仅仅是替换。该试点项目可以通用化以适用于多个业务流程，也可以针对一个用例具体化。该试点可以作为ZTA的“试验场”，在将主体过渡到ZTA部署并远离传统流程基础设施之前。

7.3.6 初始部署与监控

一旦选择了候选工作流和ZTA组件，初始部署就可以开始。企业管理员必须通过使用所选组件来实现已制定的策略，但可能希望首先在观察和监控模式下运行。很少有企业策略集在其第一次迭代中就是完整的：重要的用户账户(例如管理员账户)可能被拒绝访问他们需要的资源，或者可能不需要他们被分配的所有访问权限。

新的ZT业务流程可以在仅报告模式下运行一段时间，以确保策略有效且可行。这也允许企业了解基线资产和资源访问请求、行为和通信模式。仅报告意味着大多数请求应被授予访问权限，并且连接的日志和跟踪应与初始制定的策略进行比较。基本策略如

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

应强制执行并记录拒绝未通过 MFA 或来自已知攻击者控制或被破坏的 IP 地址的请求，但在初始部署后，访问策略应更为宽松，以便从 ZT 工作流的实际交互中收集数据。一旦建立了工作流的基线活动模式，异常行为就更容易被识别。如果无法以更宽松的方式运行，企业网络运营者应密切监控日志，并准备根据运营经验修改访问策略。

7.3.7 扩展零信任架构

当获得足够的信心且工作流策略集得到完善后，企业进入稳定运营阶段。网络和资产仍受到监控，流量被记录(见第 2.1 节)，但响应和策略修改以较低的节奏进行，因为它们不应是严重的。所涉及资源和流程的主体及利益相关方也应提供反馈以改进运营。在此阶段，企业管理员可以开始规划 ZT 部署的下一阶段。与之前的推广一样，需要确定候选工作流和解决方案集，并制定初始策略。

然而，如果工作流发生变化，运行中的 ZT 架构需要重新评估。系统的重大变化--例如新设备、软件的重大更新(尤其是 ZT 逻辑组件)以及组织结构的转变--可能导致工作流或策略的变化。实际上，应在假设部分工作已完成的前提下重新考虑整个过程。例如，已购买新设备，但未创建新用户账户，因此只需更新设备清单。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

参考文献

[ACT-IAC] 美国技术委员会与产业咨询委员会(2019) 零信任网络安全当前趋势。可访问于 https://www.actiac.org/zero-trust-cybersecurity-current-trends

[安德森] Anderson B, McGrew D(2017) 加密恶意软件流量分类的机器学习：考虑噪声标签与非平稳性。第*23*届*ACM SIGKDD*知识发现与数据挖掘国际会议论文集(ACM，加拿大新斯科舍省哈利法克斯)，第1723-1732页。 https://doi.org/10.1145/3097983.3098163

[BCORE] 国防部首席信息官(2007)。国防部全球信息网格架构愿景 1.0 版 2007 年 6 月。可查阅于 http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,2007年6月.pdf

[CSA-SDP] https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[FIPS199] 美国国家标准与技术研究院(2004)《联邦信息和信息系统的安全分类标准》(美国商务部，华盛顿特区)，联邦信息处理标准出版物(FIPS)199。 https://doi.org/10.6028/NIST.FIPS.199

[吉尔曼] Gilman E, Barth D(2017) 零信任网络：在不可信网络中构建安全系统(O'Reilly Media, Inc., Sebastopol, CA)，第1版。

[HWAM] 国土安全部(2015) 硬件资产管理*(HWAM)*能力描述。可访问于https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf

[IBNVN] Cohen R, Barabash K, Rochwerger B, Schour L, Crisan D, Birke R, Minkenberg C, Gusat M, Recio R, Jain V(2013)《一种基于意图的网络虚拟化方法》。*2013 IFIP/IEEE* 综合网络管理国际研讨会*(IM 2013)*。(IEEE，比利时根特)，第42-50页。可访问于 https://ieeexplore.ieee.org/document/6572968

[杰里科] The Jericho Forum(2007) *Jericho Forum Commandments*，版本1.2。可在以下网址获取 https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

[M-19-03] 管理和预算办公室(2018)加强通过增强高价值资产来保障联邦机构的网络安全

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

计划。(白宫，华盛顿特区),OMB 备忘录 M-19-03,2018 年 12 月 10 日。可在 https://www.White House.gov/wp-获取 content/uploads/2018/12/M-19-03.pdf

[M-19-17] 管理和预算办公室(2019)赋能任务交付 通过改进身份、凭证和访问管理。(白宫，华盛顿特区),OMB 备忘录 M-19-17,2019 年 5 月 21 日。可在https://www.White House.gov/wp-获取 content/uploads/2019/05/M-19-17.pdf

[M-19-19] 管理和预算办公室(2019)数据中心更新 Optimization Initiative(DCOI)。(The White House, Washington, 在以下网址获取 https://datacenters.cio.gov/assets/files/m_19_19.pdf

[M-19-26] 管理和预算办公室(2019)更新至可信互联网 Connections(TIC) Initiative。(The White House, Washington, DC),OMB // www.White House.gov/wp-content/uploads/2019/09/M-19-26.pdf

[NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W(2015) 策略机：特性， 架构与规范。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 机构 间或内部报告(IR)7987，第 1 版。https://doi.org/10.6028/NIST.IR.7987r1

[NISTIR 8062] 布鲁克斯 SW， 加西亚 ME， 莱夫科维茨 NB， 莱特曼 S， 纳多 EM (2017) 联邦系统中的隐私工程与风险管理导论。(美国国家标准与技术研究院，马里兰 州盖瑟斯堡),NIST 机构间或内部报告(IR)8062。https://doi.org/10.6028/ NIST.IR.8062

[NISTPRIV] 美国国家标准与技术研究院(2020)隐私 框架：通过企业风险管理提升隐私的工具，版本1.0。(美国国家标准与 技术研究院，马里兰州盖瑟斯堡)。https://doi.org/10.6028/ NIST.CSWP.01162020

[SDNBOOK] Nadeau T, Gray K(2013) *SDN*：软件定义网络：一种 网络可编程技术权威评述。(O'Reilly) 第1版。

[SP800-37] 联合工作组(2018)信息风险管理框架 Systems and Organizations: A System Life Cycle Approach for Security and Privacy.(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-37, Rev.2. https://doi.org/10.6028/NIST.SP.800-37r2

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

[SP800-63] Grassi PA, Garcia ME, Fenton JL(2017) 数字身份指南。(National Institute of Standards and Technology, Gaithersburg, MD),NIST 包含截至2020年3月2日的更新。https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] 格拉西 PA， 芬顿 JL， 莱夫科维茨 NB， 丹克 JM， 钟 Y-Y， 格林 KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63A

[SP800-160v1] Ross R, McEvilley M, Oren JC(2016) 系统安全工程：值得信赖的安全系统工程中多学科方法的考量。(美国国家标准与技术研究院 Technology, Gaithersburg, MD),NIST Special Publication(SP) 800-160,Vol.1，包含截至2018年3月21日的更新。https://doi.org/10.6028/NIST.SP.800-160v1

[SP800-160v2] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2019) 开发网络弹性系统：系统安全工程方法。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP)800-160，第 2 卷。https://doi.org/10.6028/NIST.SP.800-160v2

[SP800-162] 胡VC，费拉伊奥洛DF，库恩R，施尼策A，桑德林K，米勒R，Scarfone KA(2014)基于属性的访问控制(ABAC)定义与考量指南。(NIST, 马里兰州盖瑟斯堡),NIST 特别出版物(SP)800-162，包含截至 2019 年 8 月 2 日的更新。https://doi.org/10.6028/NIST.SP.800-162

[SWAM] 国土安全部(2015)软件资产管理(SWAM)能力描述。可访问https://www.us- cert.gov/sites/default/files/cdm_files/SWAM_Capability Description.pdf

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

附录A-缩略语

API	应用程序编程接口
BYOD	自带设备
CDM	持续诊断与缓解
DHS	国土安全部
DoS	拒绝服务
G2B	政府对企业(私营行业)
G2G	政府间
NIST	美国国家标准与技术研究院
NPE	非人类实体
PA	策略管理器
PDP	策略决策点
PE	策略引擎
PEP	策略执行点
PKI	公钥基础设施
RMF	NIST 风险管理框架
SDN	软件定义网络
SDP	软件定义边界
SIEM	安全信息与事件监控
TIC	可信互联网连接
VPN	虚拟专用网络
ZT	零信任
ZTA	零信任架构

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

附录B--已识别的差距在ZTA当前最先进水平中

在编写本文件的研究过程中，对零信任组件和解决方案的当前成熟度进行了调查。该调查得出结论，ZTA 生态系统的当前状态尚不够成熟，无法广泛采用。虽然可以使用 ZTA 策略来规划和部署企业环境，但没有单一解决方案能提供所有必要组件。此外，当今可用的 ZTA 组件很少能用于企业中存在的所有各种工作流。

以下是对 ZTA 生态系统中已识别差距以及需要进一步调查领域的总结。其中一些领域已有一定的工作基础，但由于缺乏针对多样化 ZTA 企业环境的经验，ZTA 原则如何改变这些领域尚不为人所知。

B.1 技术调研

多家供应商受邀展示其产品和对零信任的看法。此次调查的目的是找出阻碍机构现在迁移到基于零信任的企业基础设施或维护现有 ZTA 实施的缺失部分。这些差距可分为立即部署(即时或短期)、影响维护或运营的系统性差距(短期或中期)以及知识缺失(未来研究领域)。它们总结在表 B-1 中。

表 B-1：已识别部署差距汇总

类别	示例问题	已识别差距
即时部署	• 采购应如何需求应如何编写？ • ZTA 计划如何与TIC、FISMA及其他需求？	• 缺乏通用的框架和词汇用于ZTA • 认为ZTA与现有政策冲突
系统性	• 如何实现供应商锁定被防止？ • 不同的ZTA环境如何交互？	• 过度依赖供应商API
需要关注的领域更多研究	• 威胁将如何演变ZTA？ • 业务流程将如何变化面对ZTA？	• 成功的入侵在具有ZTA的企业中是什么样子 • 记录在案的最终用户在采用ZTA的企业中的经验

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

B.2 阻碍立即迁移至零信任架构的差距

这些是目前减缓 ZTA 采用的问题。这些问题被归类为即时问题，本类别未考虑未来维护或迁移。具有前瞻性的企业也可能将维护类别视为防止 ZTA 组件初始部署的即时关注事项，但在本分析中这些问题被视为单独类别。

B.2.1 零信任架构设计、规划与采购缺乏通用术语

零信任作为企业基础设施设计和部署的策略仍是一个正在形成的概念。业界尚未就描述 ZTA 组件和操作的一套统一术语或概念达成一致。这使得组织(例如联邦机构)难以制定连贯的需求和政策，以设计零信任企业基础设施并采购组件。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

第2.1节和第3.1节的驱动因素是初步尝试构建一套中立的术语和概念基础，用以描述零信任架构(ZTA)。抽象的ZTA组件和部署模型旨在作为基本术语和思考ZTA的方式。其目标是在制定企业需求和进行市场调研时，提供一种通用的方式来审视、建模和讨论ZTA解决方案。随着联邦机构在ZTA方面积累更多经验，上述章节可能会被证明是不完整的，但它们目前构成了通用概念框架的基础。

B.2.2 认为 ZTA 与现有联邦网络安全政策冲突的看法

有一种误解认为ZTA是一个单一的框架，包含一套与现有网络安全观念不兼容的解决方案。相反，零信任应被视为当前网络安全策略的演进，因为许多概念和思想已经流传了很长时间。联邦机构已被鼓励通过现有指南(见第6节)采取更加零信任的网络安全方法。如果一个机构拥有成熟的ID管理系统和强大的CDM能力，它就在通往ZTA的道路上(见第7.3节)。这种差距源于对ZTA及其如何从先前网络安全范式演变而来的误解。

B.3 影响零信任架构的系统性差距

这些是影响 ZTA 初始实施和部署以及持续运营/成熟度的差距。这些差距可能减缓机构对 ZTA 的采用，或导致 ZTA 组件行业碎片化。系统性差距是开放标准(由标准开发组织[SDO]或行业联盟制定)可以发挥作用的领域。

B.3.3 组件间接口的标准化

技术调研表明，没有单一供应商能提供实现零信任的完整方案，且采用单一供应商方案可能并不可取。

这导致组件之间不仅需要在购买时实现互操作性，还需要随时间推移保持互操作性。

更广泛企业内的组件范围极为广泛，许多产品专注于零信任中的单一细分领域，并依赖其他产品为另一组件提供数据或某种服务(例如，为资源访问集成MFA)。供应商往往依赖合作伙伴公司提供的专有API，而非标准化的、供应商无关的API来实现这种集成。这种方法的问题在于这些API是专有的且由单一供应商控制。控制供应商可以改变API行为，集成商则必须相应更新其产品。这需要供应商社区之间建立紧密的合作关系，以确保API修改的早期通知，因为这些修改可能影响产品之间的兼容性。这给供应商和消费者增加了额外负担：供应商需要投入资源更改其产品，而当一个供应商更改其专有API时，消费者需要对多个产品应用更新。此外，供应商需要为每个合作伙伴组件实现和维护包装器，以实现最大程度的兼容性和互操作性。例如，许多MFA产品供应商需要为每个云提供商或身份管理系统创建不同的包装器，以便在不同类型的客户端组合中使用。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

在客户方面，这在制定产品采购需求时产生了额外问题。购买者没有可依赖的标准来识别产品之间的兼容性。因此，由于无法确定组件的最低兼容性要求，制定迈向 ZTA 的多年路线图非常困难。

B.3.4 应对过度依赖专有 API 的新兴标准

由于开发 ZTA 没有单一解决方案，零信任企业也没有单一的工具或服务集合。因此，不可能有单一协议或框架能够使企业迁移到 ZTA。目前，有各种各样的模型和解决方案试图成为 ZTA 的主导权威。

这表明存在一个机会，即开发一套开放、标准化的协议或框架，以帮助组织迁移到ZTA。像互联网工程任务组(IETF)这样的SDO已经规定了可能有助于交换威胁信息的协议(称为XMPP-Grid[1])。云安全联盟(CSA)已经制定了一个软件定义边界(SDP)[2]框架，这可能对ZTA也有用。应致力于调查ZTA相关框架的现状或有用ZTA所需的协议，并确定需要开展工作以产出或改进这些规范的地方。

B.4 零信任架构中的知识空白与未来研究领域

此处列出的差距并不妨碍组织为其企业采用 ZTA。这些是关于运营性 ZTA 环境知识的灰色地带，大多数源于缺乏对成熟零信任部署的时间和经验。这些是研究人员未来工作的领域。

B.4.5 攻击者对零信任架构的响应

为企业正确实施的 ZTA 将比传统的基于网络边界的安全改善企业的网络安全态势。ZTA 的原则旨在减少资源对攻击者的暴露，并在主机资产被攻陷时最小化或防止企业内部的横向移动。

然而，坚定的攻击者不会坐以待毙，而是会在面对ZTA时改变行为。悬而未决的问题是攻击将如何变化。一种可能性是，旨在窃取凭证的攻击将扩展到针对MFA(例如，网络钓鱼、社会工程)。另一种可能性是，在混合ZTA/基于边界的企业中，攻击者将聚焦于尚未应用ZTA原则的业务流程(即遵循传统的基于网络边界的安全)--实际上，就是针对最容易得手的目标，试图在ZTA业务流程中获得某种立足点。

随着 ZTA 成熟、出现更多部署并积累经验，ZTA 在缩小资源攻击面方面的有效性可能会变得明显。还需要制定 ZTA 相对于旧网络安全策略的成功指标。

B.4.6 零信任架构环境中的用户体验

目前尚未对最终用户在使用 ZTA 的企业中的行为进行严格审查。这主要是由于缺乏可供分析的大型 ZTA 用例。然而，已有研究关注用户对 MFA 以及作为 ZTA 企业一部分的其他安全操作的反应，这项工作可以作为预测企业中使用 ZTA 工作流时最终用户体验和行为的基础。

一组能够预测ZTA如何影响最终用户体验的研究是关于企业中使用MFA和安全疲劳的研究。安全疲劳[3]是指最终用户面临过多的安全策略和挑战，以至于开始对他们的生产力产生负面影响的现象。其他研究表明，MFA可能会改变用户行为，但总体变化是混合的[4][5]。如果流程简化并且涉及用户习惯使用或随身携带的设备(例如智能手机上的应用程序)，一些用户会欣然接受MFA。然而，一些用户对必须使用个人拥有的设备进行业务流程感到不满，或者觉得他们因可能违反IT政策而受到持续监控。

B.4.7 零信任架构对企业与网络中断的韧性

对ZTA供应商生态系统的调查显示了部署ZTA的企业需要考虑的广泛基础设施。如前所述，目前没有单一供应商提供完整的零信任解决方案。因此，企业将购买多种不同的服务和产品，这可能导致组件之间形成复杂的依赖网络。如果一个关键组件被中断或无法访问，可能会引发级联故障，影响一个或多个业务流程。

大多数接受调查的产品和服务依赖云存在来提供稳健性，但即使云服务也曾因攻击或简单错误而变得不可达。发生这种情况时，用于做出访问决策的关键组件可能不可达，或可能

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

无法与其他组件通信。例如，位于云中的 PE 和 PA 组件在分布式拒绝服务(DDoS)攻击期间可能可达，但可能无法到达与资源位于同一位置的所有 PEP。需要研究 ZTA 部署模型可能的瓶颈点，以及 ZTA 组件不可达或可达性受限时对网络运营的影响。

企业在采用ZTA时，其运营连续性(COOP)计划可能需要修订。ZTA使许多COOP因素变得更容易，因为远程工作人员可以拥有与在本地时相同的资源访问权限。然而，如果用户未接受适当培训或缺乏经验，MFA等策略也可能产生负面影响。在紧急情况下，用户可能会忘记或无法访问令牌和企业设备，这将影响企业业务流程的速度和有效性。

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.SP.800-207

B.5 参考文献

[1] Cam-Winget N(编),Appala S,Pope S,Saint-Andre P(2019)使用用于安全信息交换的可扩展消息与存在协议(XMPP)。(互联网工程任务组(IETF)),IETF 征求意见稿(RFC)8600。https://doi.org/10.17487/RFC8600

[2] 软件定义边界工作组“SDP 规范 1.0”云安全联盟。2014 年 4 月。

[3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. IT Professional 18(5):26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D, Shechtman GM, Alsop AS(2009)使用双因素安全系统对生产力和可用性的影响。*SAIS 2009* 论文集(AIS，南卡罗来纳州查尔斯顿)，第 37 页。可访问http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J(2017) 我喜欢它但我讨厌它：员工对机构向 BYOD 第二因素身份验证过渡的看法。第*33*届年度计算机安全应用会议*(ACSAC 2017)*论文集(ACM，佛罗里达州奥兰多)，第212-224页。https://doi.org/10.1145/3134600.3134629

这份文件是怎么做出来的

本译本是《零信任架构（SP 800-207）》的中文全译本，共 59 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/nist-800-207-zh

支持私有化部署（需按贵方模型与合规要求评估）

扫码关注服务号
咨询定制交付

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。