安全加社区

公益译文项目

2020

零信任架构

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

NIST 800-207 特刊

2020 年 8 月

NSFOCUS

文档信息			
原文名称	Zero Trust Architecture		
原文作者	Scott Rose Oliver Borcher Stu Mitchell Sean Connelly	原文发布日期	2020 年 8 月
原文发布单位	美国国家标准与技术研究院		
原文出处	https://doi.org/10.6028/NIST.SP.800-207		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

授权

本文由 NIST 依据《2014 年联邦信息安全现代化法案》（FISMA）（美国法典第 44 卷第 3551 节、113–283 公法）规定的 NIST 法定职责拟定。NIST 负责开发信息安全标准和指南，包括联邦信息系统的最低要求。但是，未经相关系统决策联邦官员的明确许可，这些标准和准则不得用于国家安全系统。该指南符合美国行政管理和预算局（OMB）A-130 通告的要求。

由商务部长依法授权制定的标准和指南具有强制性与约束力，本文内容与其冲突时，以前者为准。本文所述准则并不会更改或取代商务部长、行政管理和预算局局长或其他联邦官员的现有权力。 本刊不受美国版权保护，非政府组织可自愿使用，但组织在使用本文时提及作者，NIST 将不胜感激。

美国国家标准与技术研究所
800-207 特刊

美国标准与技术研究所 800-207 特刊，共 59 页（2020 年 8 月）

分类编号：NSPUE2

本特刊可从以下地址免费获取：https://doi.org/10.6028/NIST.SP.800-207

本文中可能提到的商业实体、设备或资料，仅为准确描述规程（procedure）或概念之用，并非暗示 NIST 推荐或者认可，也不表明这些实体、资料或设备是实现目的的最佳选择。

本文提及的 NIST 依据法定职责制定的其他文档，有些可能处于开发过程中。也就是说，联邦机构在使用本文信息（包括概念和方法）时，所提及的同系列其他文档可能并未完成。这种情况下，在上述文档完成之前，现有的要求、指南和规程依然有效。为满足规划及过渡需要，联邦机构或会密切追踪 NIST 新文档的开发。

欢迎各组织在公开征求意见期间评审所有文档草案，并向 NIST 提供反馈意见。欲了解 NIST 有关网络安全的其他刊物，请访问：https://csrc.nist.gov/publications。

国家标准与技术研究院

收件人：美国马里兰州盖瑟斯堡 Bureau Drive 大道（邮递点代号：8920）

信息技术实验室计算机安全部
邮编：20899-8920

Email：zerotrust-arch@nist.gov

发表意见应受到信息自由法案（FOIA）的约束。

计算机系统技术报告

《实施指南》包含总体指导（第 1 卷）和概念验证（PoC）方案示例，展示在制造环境中如何按照《网络安全框架制造篇》中的低影响性要求来部署使用开源产品和商用现成（COTS）品。PoC 方案示例为流程型制造环境（第 2 卷）和离散型制造环境（第 3 卷）提供了可量化的网络、设备和业务性能影响指标。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用以管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用的网络安全标准和行业指南的补充而非替代。

摘要

零信任（Zero trust，ZT）是一种不断发展的网络安全范式的术语，将网络防御从静态的、基于网络边界的防护转移到关注用户、资产和资源。零信任体系结构（ZTA）使用零信任原则来规划企业基础架构和工作流。零信任假定不存在仅仅基于物理或网络位置（即局域网与互联网）或基于资产所有权（企业或个人拥有的）即授予资产或用户帐户的隐式信任。身份认证和授权（用户和设备）是在建立与企业资源的会话之前执行的独立功能。ZTA 是为了响应企业网络发展趋势。企业网络包括远程用户、自带设备（BYOD）和位于企业网络边界之外的云端资产。ZTA 的重点是保护资源（资产、服务、工作流、网络帐户等），而不是网段，因为网络位置已不再被视为资源安全态势的主要组成部分。本文给出了 ZTA 的抽象定义，并给出了 ZTA 可以改善企业整体 IT 安全状况的一般部署模型和用例。

关键词

架构，网络空间安全，企业，网络安全，零信任

致谢

本文由多个联邦机构合作著成，接受联邦首席信息官委员会监督。架构小组负责本文档的开发，但仍需认可其他人的贡献。他们是：联邦首席信息官委员会的 ZTA 项目经理格雷格·霍顿（Greg Holden）、NIST/NCCoE ZTA 项目经理阿尔珀·科尔曼（Alper Kerman）和道格拉斯·蒙哥马利（Douglas Montgomery）。

读者对象

本文旨在为企业安全架构师描述零信任（ZT）。本文旨在帮助理解民用非保密系统中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。机构网络安全经理、网络管理员、经理也可通过本文了解零信任和零信任架构。本文并不是作为 ZTA 的单一部署规划，因为企业将拥有独一无二的业务用例和数据资产，这些业务用例和数据资产是需要保护的。充分了解组织的业务和数据将有助于获得建立零信任的强有力的方法。

审稿须知

本刊旨在开发出一套技术中立的术语、定义和逻辑组件，它们可用于开发和支持 ZTA 的逻辑架构组件中。本文不提供关于如何在企业中部署零信任组件的具体指导或建议。审阅者可基于本文目的发表评论。

商标信息

专利公开公告

注意：信息技术实验室（ITL）已要求可能需要遵守本刊指南或要求而使用的专利权利要求的持有人向 ITL 披露此类专利权利要求。但是，专利持有人没有义务响应 ITL 对专利的号召，ITL 也没有进行专利检索，以确定哪些专利（如果有的话）可能适用于本刊物。

继 ITL 要求识别可能需要遵守本刊指南或要求而使用的专利权利要求之后，我们已收到一项或多项此类权利要求的通知。

经公布，ITL 对任何专利权利要求或与之相关的任何权利的有效性或范围不采取任何立场。然而，已知专利持有人已向 NIST 提供了一份保证书，声明（1）一般免责声明，声明其不持有且目前不打算持有任何基本专利权利要求，或（2）其（他们）将与其他各方在明显不存在不公平歧视的合理条款条件的基础上就交付或不交付版权费用的许可证进行协商。

详情可从 zerotrust-arch@nist.gov 获取。

我们并未明示或暗示这是避免在使用本刊中出现专利侵权所需的唯一许可证。

目录

1. 介绍

典型的企业网络基础设施变得日益复杂。一个企业可以运行多个内部网络、拥有自己的本地基础设施远程办公室、远程和/或移动个人，以及云服务。这种复杂性超越了网络边界安全的传统方法，因为企业网络边界并不是单一的存在，且难于识别。基于边界的网络安全也被证明是不够的，因为一旦攻击者突破边界，进一步的横向移动便会畅通无阻。

针对复杂的企业，形成了一种新型网络安全模式，称为“零信任”（ZT）。ZT 方法主要侧重于数据保护，但也可以且应该扩展到包括所有企业资产（设备、基础架构组件、应用、虚拟和云组件）和主体（从资源请求信息的终端用户、应用以及其他非人类实体）。在本文中，“主体”用于不直接涉及人类终端用户的章节，而“用户”用于直接涉及人类终端用户的章节，因为“主体”更通用。在零信任安全模型中，我们假设环境中存在攻击者，而且企业环境和任何非企业环境毫无二致，并没有更值得信赖。在这种新范式下，企业必须不能隐性信任，必须不断地分析和评估其内部资产和业务功能的风险，然后制定防护措施来缓解这些风险。在零信任中，这些防护措施通常尽可能减少对资源（如数据、计算资源和应用/服务）的访问，只允许那些被确定为需要访问的用户和资产访问，并对每个访问请求的身份和安全态势进行持续认证和授权。

零信任架构（ZTA）是一种基于零信任原则的企业网络安全架构，旨在防止数据泄露和限制内部横向移动。本文不仅提供了 ZTA 的定义、逻辑组件、可能的部署场景和威胁，还为希望迁移到网络基础架构的零信任网络架构设计方法的组织提供了一个总体路线图，并讨论了可能影响零信任架构的相关联邦政策。

ZT 不是单一的架构，而是一套关于工作流和系统设计运营的指导原则，可用于改善任何密级或敏感级别的安全态势[FIPS199]。向 ZTA 过渡是一个过程，只有进行大刀阔斧的技术革新才能实现。向 ZTA 过渡是关于组织如何评估其任务中的风险的过程，而不仅仅是简单地通过全面的技术替换就能实现。也就是说，现在许多组织的企业基础设施中已经有了 ZTA 元素。组织应逐步实施零信任原则、流程变更，通过用例保护其数据资产和业务功能的技术解决方案。在此期间，大多数企业基础设施将以零信任/基于边界模式的混合模式运行，同时继续投资于正在进行的 IT 现代化计划和改进业务流程。

组织需要实施全面的信息安全和弹性实践，才能使零信任有效。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、最佳实践相平衡时，ZTA 能够使用风险管理方法增强组织的安全状况，防御常见威胁。

1.1 与联邦机构有关的零信任发展历史

在“零信任”一词出现之前，零信任的概念就一直存在于网络安全中。国防信息系统局（DISA）和国防部（DOD）公布了他们在更安全的企业战略方面的工作，称之为“black core”[BCORE]。Black core 中涉及了从基于边界的安全模型转移到关注单个事务安全的模型。1994 年 Jericho 论坛的工作公开了去边界化的思想—限制基于网络位置默认的信任，以及在一张大网上依赖单一的、静态的防御的局限性[JERICHO]。去边界化的概念不断演进为一个更大的概念，被称为零信任。后来，John Kindervag 在 Forrester[1]创立了“零信任”[2]一词。零信任后来成为一个术语，用来描述各种网络安全解决方案，这些解决方案将安全性从基于网络位置的默认信任转移到基于每个事务的信任评估上来。私人企业和高等教育行业也经历了从基于边界的安全到基于零信任原则的安全战略的演变。

[1] https://go.forrester.com/blogs/next-generation-access-and-zero-trust/
[2] NIST 文档中提及的任何商业产品或服务仅供参考，并不意味着 NIST 的推荐或认可。

十多年来，在很多方面美国联邦机构一直在积极转向基于零信任原则的网络安全。联邦机构一直在推进相关能力建设和政策，从《联邦信息安全管理法案》（FISMA）开始，然后是风险管理框架（RMF）、联邦身份凭证和访问管理（FICAM）、可信互联网连接（TIC）、持续诊断和缓解（CDM）计划。所有这些计划均是为了限制授权方的数据和资源访问。这些计划在启动时都受到了信息系统技术能力的限制。安全策略基本上是静态的，并在企业可控制的大“瓶颈”上执行，以获得最佳效果。随着技术的成熟，以细粒度的方式动态地持续分析和评估访问请求，将成为可能，以“需要访问”为基础，减轻由于帐户受损、攻击者监视网络和其他威胁而导致的数据暴露。

1.2 本文结构

下文结构划分如下：

第 2 章：定义 ZT 及 ZTA 并列出设计 ZTA 企业网络时的一些网络假设。本章还介绍了一系列 ZT 设计原则。

第 3 章：描述 ZT 的逻辑组件或构建模块。各种独特的实现可以不同的方式组合 ZTA 组件而提供相同的逻辑功能。

第 4 章：列出一些通过 ZTA 使企业网络更加安全、更不易被攻击利用的用例，包括远程办公、云服务和客户网络等企业场景。

第 5 章：讨论使用 ZTA 策略的企业所面临的威胁。其中许多威胁与传统架构的网络相似，但需要采用不同的缓解技术。

第 6 章：讨论 ZTA 原则如何适用于和/或补充联邦机构的现有指南。

第 7 章：提出企业（如联邦机构）如何着手向 ZTA 过渡，并描述在 ZT 原则指导下规划和部署应用程序和网络基础设施的一般步骤。

2. 零信任基础知识

零信任是一种以资源保护为核心的网络安全范式，其前提是信任从来不是隐式授予的，而是必须进行持续评估。零信任体系架构是一种端到端的企业资源和数据安全方法，包括身份（人和非人的实体）、凭证、访问管理、操作、端点、宿主环境和互联基础设施。初始关注重点应该是将资源仅限于“需要访问和仅授予执行任务所需的最小权限（如读取、修改、删除）”的人。传统上，机构（和一般的企业网络）都专注于边界防御，授权主体可广泛地访问内网资源。因此，环境内未经授权的横向移动一直是联邦机构面临的最大挑战之一。

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。这有助于阻止互联网攻击者，但 TIC 和边界防火墙在检测和阻断内部网络攻击方面的用处不大，并且也无法保护企业边界外的主体（例如，远程工作者、基于云的服务、边缘设备）。

零信任及零信任架构的定义为：

零信任（Zero trust，ZT）提供了一系列概念和思想，旨在面对被视为受损的网络时，减少在信息系统和服务中执行准确的、权限最小的按请求访问决策时的不确定性。零信任架构（ZTA）是一种企业网络安全规划，它利用零信任概念，并囊括其组件关系、工作流规划与访问策略。因此，零信任企业作为零信任架构规划的产物，是指为企业准备的（物理和虚拟的）网络基础设施及操作策略。

一个企业决定采用零信任作为它的核心战略，并将零信任架构作为一个以零信任原则（见第 2.1 节）开发的计划。然后部署此计划以生成一个零信任环境，供企业使用。

该定义聚焦于问题的关键，即防止未经授权访问数据和服务以及使访问控制的实施尽可能精细。也就是说，授权和获准主体（用户、应用（或服务）和设备的组合）可以访问数据，但不包括其他主体（即攻击者）。更进一步，“资源”一词可以代替“数据”，因此 ZTA 与资源访问（例如打印机、计算资源、IoT 执行器等）有关，而不仅仅是数据访问。

为了减少不确定性（因为它们不能完全消除），零信任在认证机制中维持可用性、减少时间延迟的同时更加关注认证、授权以及可信域。访问规则尽可能精细化，以强制执行请求中执行操作所需的最小权限。

在图 1 中，主体需要访问企业资源，可通过策略决策点（PDP）和相应的策略执行点（PEP）授予访问权限。[3]

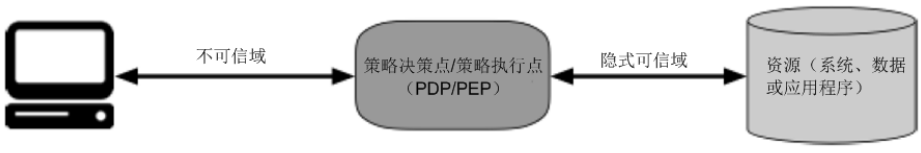

图 1：零信任访问

系统必须确保主体是“真实的”且请求有效。PDP/PEP 提供适当的判断，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。对于这个唯一的请求，主体的身份的可信度是多少？考虑到对主体身份的信任程度，是否允许访问资源？用于请求的设备是否具有正确的安全态势？是否有其他因素需要考虑，这些因素可能改变可信度（如时间、主体位置、主体安全态势）？总的来说，企业需要为资源访问制定和维护动态的基于风险的策略，并建立一个系统来确保针

[3] 概念部分定义见 OASIS XACML 2.0 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf。

对单个资源访问请求来正确、一致地执行这些策略。这意味着企业不应依赖于隐式可信性。如果主体符合基本身份验证级别（如登录到资产），则所有资源请求都视为同等有效。

“隐式可信域”是指一个区域内的所有实体都至少被信任为上一个 PDP/PEP 网关的级别。例如，在机场的乘客筛选模型中，所有乘客通过机场安检点（PDP/PEP）进入登机口。乘客、机场工作人员、机组人员等可以在航站区内闲逛，所有个人都被认为是可信的。在这个模型中，隐式可信域就是登机区。

PDP/PEP 采用一系列公共的控制措施，使通过检查点的所有流量都具有相同的信任级别。PDP/PEP 不能将策略应用于流量位置之外。为了使 PDP/PEP 尽可能具体，隐式可信域必须尽可能小。

零信任提供了一套原则和概念，使 PDP/PEP 更接近资源。其思想是明确地验证和授权组成企业的所有主体、资产和工作流。

2.1 零信任的原则

许多关于 ZT 的定义和讨论都强调从方程式中去掉边界防御（如防火墙等）的概念。然而，大部分仍然以某种方式定义自己与边界的关系（例如微分段或微边界；见第 3.1 节），将边界防护作为“零信任架构功能的一部分”。根据应遵循的基本原则而不是应排除的基本原则，我们尝试定义 ZT 及 ZTA。这些宗旨是理想目标，尽管必须承认，并非所有的宗旨都可以在给定的战略中以其最纯粹的形式得到充分实现。

*零信任架构的设计和部署*遵循以下零信任基本原则：

1. 所有的数据源和计算服务都被认为是资源。网络可以由多种类别的设备组成。网络可能还具有占用空间小的设备，这些设备将数据发送到聚合器/存储，“软件即服务”（SaaS），还有将指令发送到执行器的系统等。此外，如果个人设备有权限访问企业资源，则企业可决定将这些设备归类为资源。

2. 所有的通信都是安全的，与网络位置无关。仅网络位置并不意味着信任。来自企业自有网络基础设施上的系统的访问请求（例如，在传统网络边界内）的安全要求，必须与来自任何其他非企业自有网络的访问请求和通信的安全要求相同。换言之，不应对企业自有网络基础设施上的设备自动授予任何信任。所有通信应以最安全的方式进行，保护机密性和完整性，并提供源身份认证。

3. 对单个企业资源的访问的授权基于每个连接授予的。在授予访问权限之前评估请求者信任级别。访问权限还应授予完成任务所需的最小权限。这可能意味着权限授予只能在“最近某个时间”发生，并且在启动会话或使用资源执行事务之前不会直接发生。但是，对一个资源的身份认证和授权并不是自动授予对另一个不同资源的访问权限。

4. 对资源的访问是由策略决定，包括客户身份、应用/服务和请求资产的可观察状态，可能还包括其他行为及环境属性。通过定义其拥有的资源、成员（或对来自联邦的用户进行身份认证的能力）、成员需要的资源访问权，组织可进行资源保护。用户身份包括所用的用户帐户（或服务身份）和由企业分配给该帐户或工件以认证自动化任务的任何相关属性。请求资产状态可包括设备特征，例如已安装的软件版本、网络位置、请求的时间/日期、之前观察到的行为、已安装的凭证等。行为属性包括但不仅限于自动化主体分析、设备分析、实际测量到的与已观察到的使用模式的偏差。策略是基于组织分配给主体、数据资产或应用的属性的访问规则集。环境属性可能包括请求者网络位置、时间、报告的活跃攻击等因素。这些规则和属性是根据业务流程需求和可接受的风险水平而定。资源访问和操作权限策略可根据资源/数据的敏感性而变化，可采用最小特权原则来限制可视性和可访问性。

5. 企业对所有自有和相关的资产的完整性和安全态势进行监控和测量。没有资产是天生可信的。企业评估资源请求时，也评估资产的安全态势。实施 ZTA 战略的企业应建立一个 CDM 或类似的系统来监控设备和应用的状态，并根据需要应用补丁/修复程序。被发现为被颠覆、具有已知漏洞和/或不受企业管理的资产可能会受到不同的对待，与那些企业所有或与企业相关的被视为处于最安全状态的系统相比，可能会被区别对待（包括拒绝与企业资源的所有连接）。这也可能适用于允许访问某些资源但不允许访问其他资源的关联设备（例如，个人拥有的设备）。这也需要一个强大的监控和报告系统来提供关于企业资源当前状态的可操作数据。

6. 所有资源身份认证和授权是动态，并且在允许访问之前严格执行。这是一个不断的循环过程，包括访问、扫描和评估威胁、调整、在通信中进行持续信任评估。实现 ZTA 的企业应该具有身份、凭证和访问管理（ICAM）以及资产管理系统。这包括使用多重身份验证（MFA）访问某些（或所有）企业资源。根据策略（如基于时间、请求的新资源、资源修改、检测到的异常用户活动等）的定义和实施，在整个用户交互过程中，会持续监视可能的重新认证和重新授权，努力实现安全性、可用性、使用性和成本效益之间的平衡。

7. 企业尽可能收集有关资产、网络基础架构和通信现状的信息，并利用这些信息改善其安全态势。企业应该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，然后使用获得的任何洞察力来改进策略的创建和实施。此数据还可用于为来自主体的访问请求提供上下文（请参阅第 3.3.1 节）。

上述原则尽可能做到与技术无关（technology-agnostic）。例如，“用户识别（ID）”可包括用户名/密码、证书、一次性密码等多个因素。此类原则适用于在一个组织内或与一个或多个合作伙伴组织协作完成的工作，而不适用于面向公众或消费者的业务流程。组织不能将内部政策强加给外部参与者（例如，客户或普通互联网用户），但可以对与组织有特殊关系的非企业用户（如注册客户、员工家属等）实施一些基于 ZT 的政策。

2.2 零信任视角下的网络

在网络规划和部署中使用 ZTA 的组织都有一些关于网络连通性的基本假设。其中一些假设适用于企业自有的网络基础设施，另一些适用于非企业自有的网络基础设施上使用的企业资源（例如公共 Wi-Fi 或公共云提供商）。这些假设用于指导 ZTA 的形成。在实施 ZTA 战略的企业中，网络开发应遵循上述 ZTA 原则和以下假设。

1. 整个企业专网不被视为隐式信任区。系统应始终假设企业网络上存在攻击者，通信应以最安全的方式进行（见上述原则 2）。这需要对所有连接进行身份验证，并对所有流量进行加密。

2. 网络上的设备可能不归企业所有或不可配置。访客和/或外包服务可能包括非企业所有系统，它们需要网络访问才能履行其职责；还包括自带设备（BYOD）政策，允许企业主体使用非企业所有的设备访问企业资源。

3. 没有资源是天生可信的。在将请求授予企业资源之前，每个资产都必须通过 PEP 评估其安全态势（与针对资产和主体的上述原则 6 相似）。该评估应在会话期间持续进行。与来自非企业拥有设备的相同请求相比，企业拥有设备可具有启用身份验证并提供高于同一请求的信任程度的构件。主体凭证并不足以对企业资源进行设备认证。4. 并非所有的企业资源都在企业拥有的基础设施上。这包括远程主体和云服务。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（如 DNS 解析）。

5. 远程企业主体和资产不能信任本地网络连接。远程主体应假设本地网络（即非企业所有的网络）都是恶意的。系统应假设所有流量都被监控并可能被修改。所有连接请求都应经过身份认证和授权，所有通信都应尽可能以最安全的方式完成（即提供机密性、完整性保护和源身份认证）（见上述 ZTA 原则）。

6. 在企业和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态势。在移动到企业拥有的基础设施或从企业拥有的基础设施进行移动时，资产和工作负载应保持其安全态势。这包括从企业网络移动到非企业网络（即远程用户）的设备，还包括从本地数据中心迁移到非企业云实例的工作负载。

3. 零信任架构的逻辑组件

《在企业中，构成 ZTA 网络部署的逻辑组件很多。这些组件可以作为现场服务或通过云服务来操作。图 2 中的概念框架模型显示了组件基本关系及其相互作用。注意，图中展示的是理想模型中的逻辑组件及其相互作用。从图 1 中，策略决策点（PDP）可分为两个逻辑组件：策略引擎（PE）和策略管理器（PA）（定义如下）。ZTA 逻辑组件使用单独的控制平面进行通信，而应用数据在数据平面上进行通信（见第 3.4 节）。

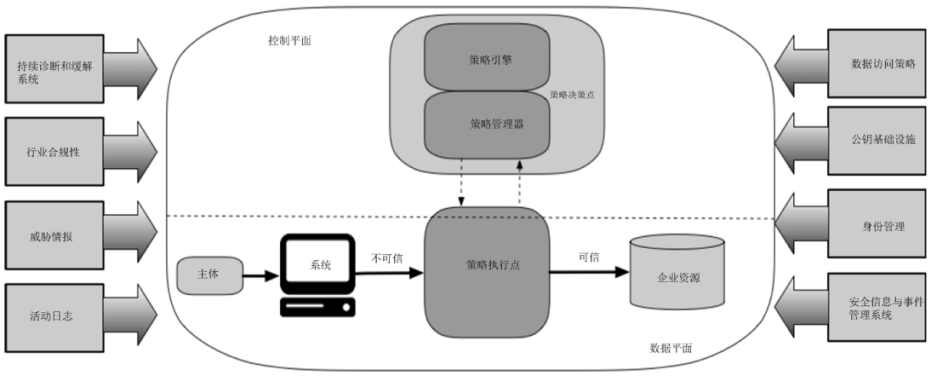

图 2：核心零信任逻辑组件

组件描述如下：

- **策略引擎（PE）：**该组件负责最终决定是否授予特定访问主体对资源的访问权限。策略引擎使用企业安全策略以及来自外部源（例如持续诊断和缓解系统、下述威胁情报服务）的输入作为“信任算法”（更多详情，见第 3.3 节）的输入，以决定授予、拒绝或撤销对该资源的访问权限。策略引擎常与策略管理器组件搭配使用。策略引擎做出决定并加以记录（批准或拒绝），策略管理器执行该决定。
- **策略管理器（PA）：**该组件负责建立和/或切断主体与资源之间的通信路径（通过与策略执行点相关的指令）。它将生成针对具体会话的身份验证令牌或凭证，供客户端用于访问企业资源。它与策略引擎密切相关，并依赖策略引擎最终做出允许或拒绝会话的决定。如果会话被授权并且请求通过身份验证，PA 将配置策略执行点（PEP）以允许会话启动。如果会话被拒绝（或先前的批准被否决），PA 将向 PEP 发出信号切断连接。策略引擎和策略管理器可分别作为单项服务来实施；这里，二者被划分成两个逻辑组件。在创建通信路径时，策略管理器与策略执行点通过控制平面保持通信。
- **策略执行点（PEP）：**该组件负责启用、监控并最终结束访问主体和企业资源之间的连接。PEP 与 PA 通信以转发请求和/或从 PA 接收策略更新。策略执行点是 ZTA 中的一个逻辑组件，但可分为两个不同的组件：客户端组件（例如笔记本电脑上的代理）、资源端组件（例如资源前控制访问的网关）或保护通信路径的单个门户组件。在 PEP 之外是托管企业资源的隐

式信任区域（请参阅第 2 节）。

除了在执行 ZTA 策略的企业中的核心组件之外，还有多个能够提供输入和策略规则的数据源。策略引擎在做出访问决策时可使用这些输入和策略规则。这些数据源包括本地数据源和外部（即非企业控制或创建的）数据源，包括：

- **持续诊断和缓解（CDM）系统：**该系统收集企业系统当前状态信息，并将更新应用到配置和软件组件中。企业 CDM 系统为策略引擎提供关于发送访问请求的系统信息，例如系统运行的是否是打过补丁的操作系统和应用程序、企业认可的软件组件是否完整或是否存在未经批准的组件、系统是否存在任何已知漏洞。CDM 系统还负责识别和潜在地对活跃在企业基础设施上的非企业设备执行策略子集。
- **行业合规系统：**该系统确保企业可满足可能归入的任何监管制度（如 FISMA、医疗或金融行业信息安全要求等）的合规性要求，包括企业为确保合规性而制定的所有策略规则。
- **威胁情报源：**该系统提供内部源或外部源信息，帮助策略引擎做出访问决策。这些可以是从多个外部源获取数据并提供关于新发现的攻击或漏洞信息的多个服务，还包括新发现的软件缺陷、新识别的恶意软件或策略引擎拒绝从企业系统访问的报告的对其他资产的攻击。
- **网络和系统活动日志：**这是一个企业系统，它聚合了资产日志、网络流量、资源访问操作和其他事件，这些事件提供关于企业信息系统安全态势的实时（或接近实时）反馈。
- **数据访问策略：**这是企业为企业资源创建的关于数据访问的属性、规则和有关访问企业资源的策略的集合。策略规则集可以编码（通过管理界面）在策略引擎中或由策略引擎动态生成。这些策略是授予资源访问权限的起点，因为它们为企业中的参与者和应用/服务提供了基本的访问权限。这些策略应以本组织确定的任务角色和需要为基础。
- **企业公钥基础设施（PKI）：**该系统负责生成和记录企业对资源、主体、服务和应用等发布的证书，还包括全局 CA 生态系统和联邦 PKI。联邦 PKI[4] 可与企业 PKI 集成，二者也可互不集成。这也可能是不是建立在 X.509 证书上的 PKI。
- **身份管理系统：**该系统负责创建、存储和管理企业用户帐户和身份记录（例如，轻量级目录访问协议（LDAP）服务器）。该系统中包含必要的主体信息和其他企业特征，比如角色、访问属性或分配的系统。该系统通常利用其他系统（如上述 PKI）来处理与用户帐户相关联的工件。该系统可能是一个更大的联邦社区的一部分，可能包括非企业员工或链接到非企业资产进行协作。
- **安全信息与事件管理（SIEM）：**它收集以安全为中心的信息以供以后分析。然后，这些数据将用于完善策略并警告可能对企业资产发起的攻击。

3.1 零信任架构方法的变化

企业可以通过多种方式为工作流制定 ZTA。这些方法因使用的组件和组织的策略规则的主要来源而异。每种方法都达成了 ZT 的全部宗旨（见第 2.1 节），但可以使用一个或两个（或一个组件）作为策略的主要驱动因素。一个完整的 ZT 解决方案将包括所有三种方法的要素。这些方法包括增强的身份治理驱动、逻辑微分段以及基于网络的分段。

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

对于某些用例来说，某些方法会显得比其他方法更适合。为企业研发 ZTA 的组织部门可能会发现，其选择的用例和现有策略指向某一种特定方法而不是其他方法。这并不意味着其他方法不起作用，而是意味着其他方法可能更难实施，并且可能需要对企业当前如何进行业务流造成更根本的更改。

3.1.1 使用增强身份治理的 ZTA

实现 ZTA 的增强身份治理方法使用参与者身份作为策略创建的关键组件。如果不是针对请求访问企业资源的主体，则无需创建访问策略。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，如使用的设备、资产状态和环境因素，可以改变最终信任程度算（和最终访问授权），或者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部分访问。保护资源的单个资源或 PEP 组件必须具有将请求转发到策略引擎服务或认证主体并在授予访问权限之前批准请求的方法。

针对企业的基于增强身份治理的方法通常使用开放网络模型或有访客访问的企业网络或非企业设备常接入网络的情况（如下面第 4.3 节中的用例）。网络访问最初被授予对资源具有访问权限的针对企业的基于增强身份治理的方法通常使用开放网络模型或有访客访问的企业网络或非企业设备常接入网络的情况（如下面第 4.3 节中的用例）。网络访问最初被授予所有资产，但企业资源的访问仅限于具有适当访问权限的身份。授予基本网络连接有一个缺点，因为恶意参与者仍然可以尝试网络侦察和/或使用网络在内部或针对第三方发起拒绝服务攻击。企业仍然需要在此类行为影响工作流之前对其进行监视和响应。

身份驱动的方法与资源门户模型很好地配合（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。其他模式也可以工作，这取决于现有的策略。身份驱动的方法也适用于使用基于云的应用/服务的企业，这些应用/服务可能不允许使用企业拥有或运营的 ZT 安全组件（如许多 SaaS 产品）。企业可以使用请求者的身份在这些平台上形成和实施策略。

3.1.2 使用微分段的 ZTA

企业可以选择通过将单个或资源组部署在由网关安全组件保护的自身网段上来实现 ZTA。在这种方法中，企业放置基础设施设备，如智能交换机（或路由器）或下一代防火墙（NGFWs）或专用网关设备作为 PEP 来保护每个资源或相关资源小组。或者（或者另外），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现基于主机的微分段。这些网关设备为来自客户端、资产或服务的每个请求动态的授予访问权。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 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，而管理所述设备充当 PE/PA 组件。这种方法需要一个身份治理程序（IGP）来完全发挥作用，但依赖于网关组件作为 PEP，以保护资源免受未经授权的访问和/或发现。

这种方法的关键必要性在于，PEP 组件是受管理的，并且应该能够根据需要进行响应和重新配置，以响应工作流中的威胁或更改。虽然通过使用不太先进的网关设备甚至无状态防火墙，可以实现微分隔企业的某些功能，但管理成本和快速适应变化的困难使这成为一个非常糟糕的选择。

3.1.3 使用网络基础架构和软件定义边界的 ZTA

第三种方法使用网络基础架构来实现 ZTA。ZTA 可以通过使用 overlay 网络实现（即，第 7 层，但也可以设置在 ISO 网络堆栈的较低层）来实现。这些方法有时被称为软件定义边界（SDP）方法，通常包括来自软件定义网络（SDN）[SDNBOOK]和基于意图的网络（IBN）[IBNVN]的概念。在这种方法中，PA 充当网络控制器，根据 PE 所做的决策建立和重新配置网络。客户端继续通过由 PA 组件管理的 PEPs

请求访问。

当该方法在应用网络层（即第 7 层）实现时，最常见的部署模型是代理/网关（见第 3.2.1 节）。在这种实现方法中，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。这个模型可能还有其他变体，对于云虚拟网络、非 IP 网络等也是如此。

3.2 抽象架构的部署变体

所有这些组件都是逻辑组件，但不一定都是唯一的系统。一个系统可以履行多个逻辑组件的职责。同样地，一个逻辑组件可以由多个硬件或软件元素组成，以执行任务。例如，企业 PKI 可以由两个组件组成，一个负责为设备颁发证书，另一个用于向最终用户颁发证书，但两者均使用从同一企业根证书颁发机构颁发的中间证书。在目前市场上提供的许多 ZT 网络产品中，PE 和 PA 组件组合在一个服务中。

在架构所选定组件的部署上有多个变体，下文中将加以概述。根据企业网络的建立方式，企业中的不同业务流程可使用多个 ZTA 部署模型。

3.2.1 基于设备代理/网关的部署

在基于设备代理/网关的部署模型中，策略执行点被分为两个组件，它们位于资源上或者作为一个组件直接位于资源之前。例如，每个企业发布的系统上都安装了一个用于协调连接的设备代理，而每个资源都一个前置组件（即网关），以便资源只与网关通信，实质上充当了资源的反向代理。代理是一个软件组件，它将一些（或全部）通信量定向到适当的 PEP，以便对请求进行评估。网关负责与策略管理器进行通信，并且只允许策略管理器批准的连接（见图 3）。

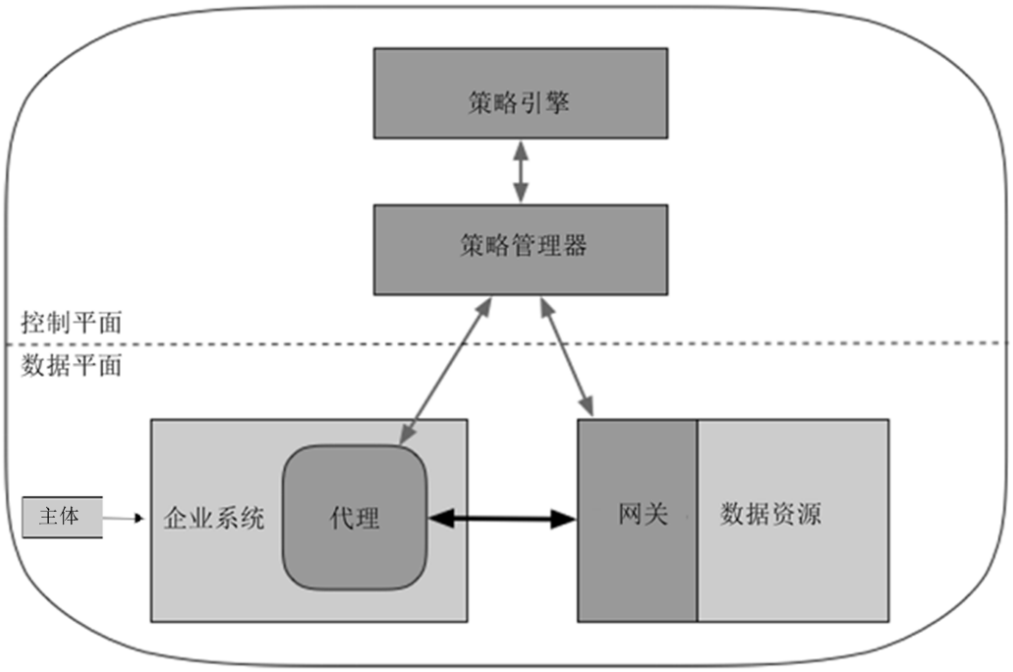

图 3：设备代理/网关模型

在典型的连接场景中，企业的笔记本电脑用户希望连接到企业资源（如 HR 应用程序/数据库）。本地代理接收连接请求并将其转发给策略管理器。策略管理器（和策略引擎）可以是企业本地系统或云托管服务。策略管理器将请求转发给出来引擎进行评估。如果请求被授权，策略管理器将通过控制平面在设备代理和相关的资源网关之间配置通信通道，包括 IP 地址/端口信息、会话密钥或类似安全构件等信息。然后，设备代理和网关二者连接，开始传输经过加密的应用/服务数据流。当工作流完成或因安全事件（如会话超时、重新认证失败等）而被策略管理器触发时，设备代理和资源网关之间的连接将会被终止。

对于具备健壮的设备管理程序和可与网关通信的离散资源的企业而言，这种模型最为适合。对于大量使用云服务的企业而言，这是一项云安全联盟软件定义周界（CSA-SDP）的客户端-服务器实现。对于不计划执行 BYOD（自带设备）策略的企业而言，这种模式也很好。访问权限只能通过设备代理来授予。设备代理可部署在企业自有系统中。

3.2.2 飞地部署

基于微边界的部署模型是上述设备代理/网关模型的变种。在该模型中，网关组件可能并不位于系统上或在单个资源之前，而是位于资源飞地（如本地数据中心）的边界，如图 4 所示。通常，这些资源是作为单个业务功能，并不直接与网关通信（例如，传统数据库没有可用于与网关通信的应用程序编程接口[API]）。对于使用基于云的微服务进行业务处理（如用户通知、数据库查询或工资发放）的企业而言，该部署模型也很有用。在该模型中，企业私有云位于网关之后。

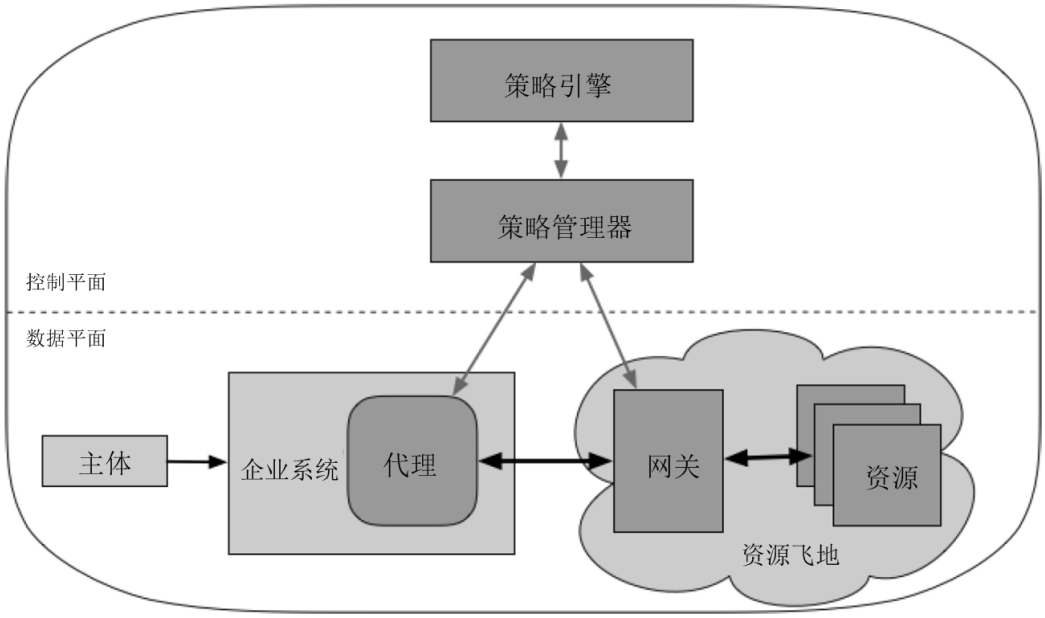

图 4：飞地网关模型

该模型可与设备代理/网关模型混合。在该模型中，企业系统中具备用于连接飞地网关的设备代理，但是这些连接的创建过程与基本设备代理/网关模型的创建过程是一样的。

对于具有遗留应用程序的企业或无法部署独立网关的现场数据中心而言，这种模型很有用。企业需要具备稳健的资产和配置管理计划来安装/配置设备代理。这种模型的缺点在于：网关保护的是资源集，而不是单个资源。这种模型可能还会允许主体查看其原本无权访问的资源。

3.2.3 基于资源门户的部署

在基于资源门户的部署模型中，策略执行点是一个组件，可作为主体用户请求网关。网关门户可以是单个资源，也可以是单个业务功能集合的安全飞地。以下以私有云或包含遗留应用程序的数据中心的网关门户为例，如图 5 所示。

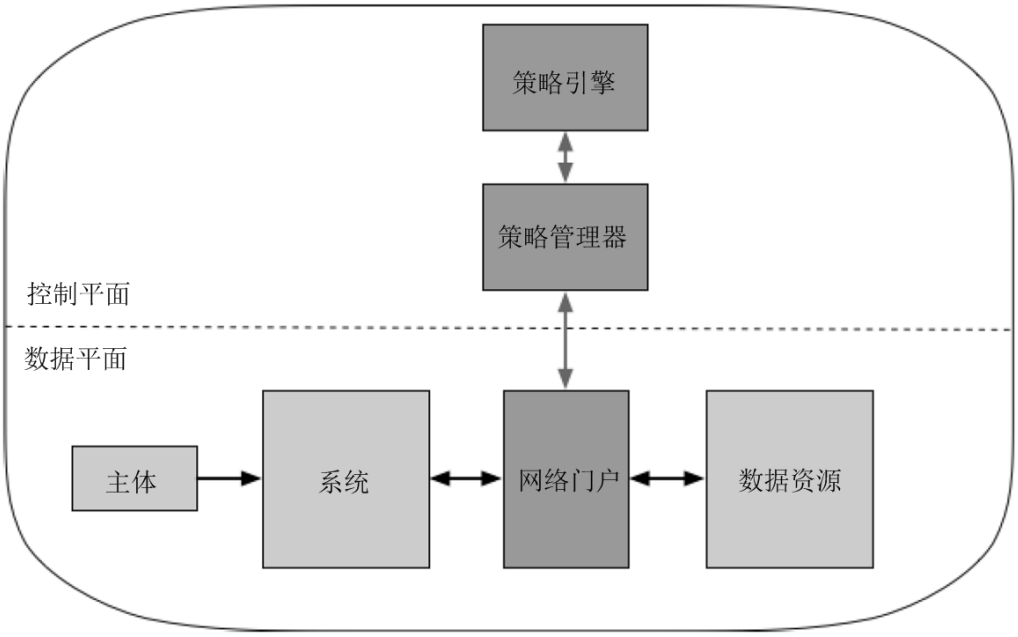

图 5：资源门户模型

与其他模型相比，该模型的主要优势是不需要在所有客户端设备上都安装软件组件。对于 BYOD 政策和组织间协作项目而言，这种模型也更加灵活。在使用前，企业管理员不需要确保每个设备都有适当的设备代理。然而，可以根据请求访问的设备推断出有限的信息。这种模型可用于扫描和分析连接到策略执行点门户的系统和设备，但可能无法持续监控这些系统和设备是否存在恶意软件和未修补的漏洞，也无法持续监控它们的配置。

该模型的主要不同之处在于它没有处理请求的本地代理。该模型的缺点在于：企业可能无法完全查看或控制自有系统，因为只有在这些系统连接到门户时企业才能看到/扫描这它们。企业可以采取浏览器隔离等措施来缓解或补偿。在这些连接会话之间，这些系统对企业而言可能是不可见的。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。门户系统应配置好，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

让经审查的应用或进程在系统上隔离运行是代理/网关部署模型的另一个变种。这种隔离的部分可以是虚拟机、容器或其他实现方式，但目的都是为了保护应用或应用实例不受可能受损的主机或资产上运行的其他应用的影响。

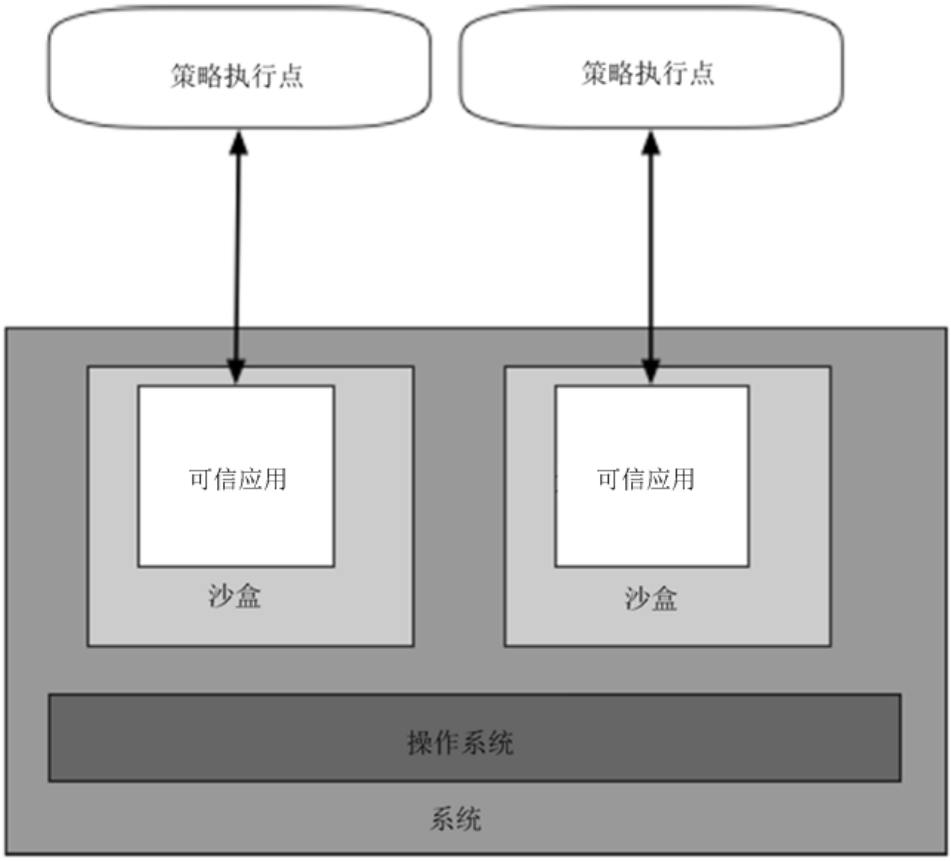

图 6：应用沙盒

如图 6 所示，主体系统在沙盒中运行经批准、审查的应用。这些应用可以与 PEP 通信以请求对资源的访问，但 PEP 将拒绝来自系统上其他（不可信）应用程序的连接。在该模型中，PEP 可以是企业本地服务，也可以是云服务。

该模型变种的主要在于它将单个应用程序与系统的其他部分隔离开来。若无法扫描系统脆弱性，则可以保护沙盒应用程序，使其免受主机系统上潜在的恶意软件感染。这种模式的缺点之一在于：企业必须在所有系统上维护这些沙盒应用程序，并且可能无法完全查看客户端系统。企业还需要确保每个沙箱应用都是安全的，这可能需要比简单地监视设备需要花费更大精力。

3.3 信任算法

对于部署了 ZTA 的企业，可将策略引擎视为大脑，将信任算法视为其主要的思维过程。信任算法（TA）是策略引擎用来最终授予或拒绝资源访问权限的过程。策略引擎接受来自多个源的输入：策略数据库（包含主体、主体属性和角色等可观察的信息）、历史主体行为模式、威胁情报源和其他元数据源。具体流程可分为几大类别，如图 7 所示。

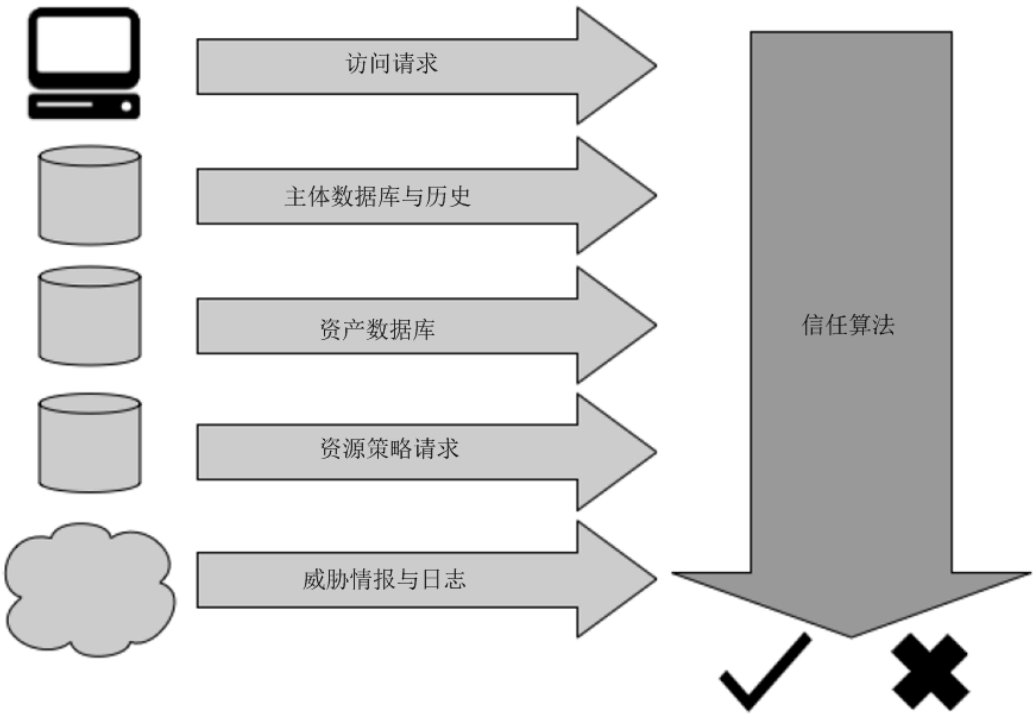

图 7：信任算法的输入

如图 7 所示，基于提供给信任算法的内容，这些输入可分为以下类型：

- **访问请求：**指来自主体的实际请求。被请求的资源是使用的主要信息，但也会用到请求者信息，包括操作系统版本、使用的应用程序、使用的软件（例如，请求应用程序是否出现在批准的应用程序列表中？）和补丁级别。根据这些因素和资产安全态势，资产访问请求可能会受限或遭拒。
- **主体数据库：**这是回答“谁”在请求访问资源[SP800-63]。这是企业或合作者用户组（人员和进程）和已分配主体属性/权限集合。这些主体和属性构成了资源访问策略的基础[SP800-162][NISTIR 7987]。用户身份包含以下信息：逻辑身份（如帐户标识）和 PEP 执行的认证检查结果。身份属性应被纳入计算信任度，包括时间和地理因素。授予多个用户的权限集合可被视为一个角色，但应将每个主体作为单独的个体进行权限分配，而不仅仅是因为他们可能适合组织中某个特定角色而进行权限分配。这应该被编码并存储在身份管理系统和策略数据库中。这个集合应该被编码并存储在 ID 管理系统和策略数据库中。这也可能包括一些（TA，trustalgorithm，信任算法）变化中过去观察到的用户行为的数据（见第 3.3.1 节）。
- **系统数据库（和可观察状态）：**系统数据库中包含了每个企业自有（和可能已知的非企业/自带设备）资产（在某种程度上是物理的和虚拟的）的已知状态。这些状态与发送请求的系统的可观察状态相比较。这可以包括操作系统版本、当前软件及其完整性、位置（网络位置和地理位置）和补丁级别。根据资产状态与此数据库进行比较，资产访问请求可能会受限或遭拒。
- **资源请求：**这是对用户身份和属性数据[SP800-63]的策略补充。它定义了访问资源的最低要求，包括认证器的保证级别（例如多因素认证（MFA））、网络位置（例如，拒绝来自海外 IP 地址的访问）、数据敏感性、系统配置请求。这些要求应由数据管理员（即数据负责人）和使用数据的业务流程负责人（即任务/使命责任人）共同制定。

- **威胁情报：**威胁情报是指在互联网上运行的一般威胁和活跃恶意软件的信息源。威胁情报还可能包括有关从可能可疑的设备上看到的通信相关的特定信息（例如查询可能的恶意软件命令和控制节点）。这些信息源可以是外部服务，也可以是内部扫描和发现，可以包括攻击签名和缓解措施。这是唯一一个极少受到企业控制但极有可能是一种服务的组件。

关于每个数据源的重要性权重，可以使用专有算法，也可以由企业来配置。这些权重值可反映出数据源对企业的重要性。

最终决策交由策略管理器来执行。策略管理器的职责是配置必要的策略执行点，启用连接。根据 ZTA 的部署方式，这可能涉及向网关和代理或资源门户发送验证结果和连接配置信息。策略管理器还可以对通信会话进行保持或暂停，以便根据策略要求重新认证和重新授权连接。策略管理器还负责根据策略终止连接（例如，在超时后、工作流完成时或出于安全告警而终止连接）。

3.3.1 信任算法的变种

实施 ZTA 信任算法（TA）的方法有很多种。不同的实施者可能希望根据其感知到的重要性，对上述因素进行不同的权衡。以下两个主要特征可用于区分信任算法：一是如何评估这些因素，无论是二元决策，还是整体“得分”或信任度的加权部分；二是如何根据同一主体、应用或者设备的身份评估一些请求与其他请求的关联。

- **基于条件与基于分值：**基于条件的信任算法的前提是在授予资源访问权限或允许操作（例如读/写）之前必须满足一组属性。这些条件由企业来配置，并且应独立配置给每个资源。只有在满足所有条件时，才能授予访问权限或对资源应用操作。基于分值的信任算法是根据每个数据源的值和企业配置的权重来计算“信任度”。如果分值大于所配置的资源阈值，则授予访问权限，或执行操作。否则，请求被拒绝，或访问权限降低（例如，授予读取权限，但不授予对文件的写入权限）。

- **单一（Singular）与上下文（Contextual）：**单一信任算法会单独处理每个请求，在评估时不考虑主体的历史情况。这样可以加快评估速度，但如果攻击使用的是主体被允许的角色，则存在无法检测到该攻击的风险。上下文信任算法会在评估访问请求时考虑主体（或网络代理）的最近历史记录。这意味着策略引擎必须维护所有主体和应用程序的某些状态信息，但更可能检测到攻击者使用被攻陷的凭证访问信息。这种访问方式与特定主体所采用的方式不同。这也意味着，通信时，与主体互动的 PA（和 PEP）必须将用户行为告知 PE。主体行为分析可用于提供可接受使用的模型，与此行为的偏差可能会触发额外的身份认证检查或资源请求拒绝。

这两种因素相互独立。可能有这样一种信任算法：它将信任度分配给每个主体和/或设备，并分别对待每个访问请求（即单一化）。但是，基于分数的、上下文的信任算法会提供更动态和更细粒度的访问控制的能力，因为分数为请求帐户提供了当前的信任度，并且比人工管理员修改的静态策略更快地适应变化的因素。

理想情况下，ZTA 信任算法应该是上下文的，但对于企业可用的基础设施组件，这并不总是行得通的。上下文信任算法可以缓解这类威胁：当攻击者使用一组“正常”的访问请求用于主体帐户攻击（或内部攻击）。在定义和实现信任算法时，必须平衡安全性、可用性和成本效益。若用户行为符合其在组织中关于任务功能和角色的历史趋势和规范，仍不断地提示主体重新认证，这可能会导致可用性问题。例如，如果人力资源部门员工在一个工作日内通常访问 20–30 条员工记录，那么当访问请求在某天突然超过 100 条记录时，上下文信任算法就会发送告警。如果有人在正常工作时间后提出访问请求，上下文可信算法也可能发送警报，因为这可能是攻击者在使用盗取的人力资源帐户进行信息渗透。这个例子说明上下文信任算法可检测到攻击，而单一信任算法可能无法检测到新型行为。再举一个例子：会计人员

通常在正常工作时间内访问财务系统，而现在他正试图在午夜时分从一个无法识别的位置访问财务系统。这种情况下，上下文信任算法会触发告警并要求用户满足NIST SP 800-63A [SP800-63A]中规定的更严格的分值或其他标准。

为每个资源开发一套标准或权重/阈值是需要经过规划和测试的。在 ZTA 的初始部署过程中，企业管理者可能会遇到这样的问题：由于配置错误导致本该获准的访问请求被拒绝，这带来了部署的初始“优化”阶段。需要调整标准或分值权重，确保在执行策略的同时保证企业业务流程的正常运转。此优化阶段持续多长时间取决于企业定义的进度度量和对工作流中使用的资源的错误访问拒绝/批准的容忍度。

3.4 网络/环境组件

在 ZTA 网络中，应将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/服务通信流隔离开来（逻辑隔离或物理隔离）。这种隔离通常可分为控制平面（用于网络控制通信）和数据平面（用于应用/服务通信流）[吉尔曼（Gilman）]。

各类基础架构组件（企业所有和服务提供商提供）将控制平面用于资产维护与配置；判断、授予或拒绝访问资源权限；以及执行任何必要的操作以建立资源之间的连接。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连接之前，不可能有这样的通信信道。例如，策略管理器和策略执行点可使用控制平面在主体和企业资源之间建立连接。然后，应用/服务工作负载才能使用已建立的数据平面连接。

3.4.1 支持 ZTA 的网络需求

1. 企业系统应具有基本的网络连接性。局域网，无论是否由企业控制，提供基本的路由和基础设施（如 DNS 等）。远程企业系统未必会使用所有的基础设施服务。

2. 企业必须能够区分企业拥有或管理的资产及设备当前的安全态势。这些根据企业发放的凭据而定，而不使用未经验证的信息（例如可以伪造的网络 MAC 地址等）。

3. 企业能够捕获所有网络流量。企业记录在数据平面上看到的数据包，即使可能无法对所有数据包执行应用层检查（即，ISO 第 7 层）。企业过滤出关于连接的元数据（例如目的地址、时间、设备标识等），在评估访问请求时动态更新策略并通知 PE。

4. 除非访问策略执行点，否则企业资源是不可被访问的。企业资源不接受来自互联网的任意传入连接。仅在客户端经过身份验证后，资源可接受自定义配置的连接。这些连接是由策略执行点建立的。如果不访问策略执行点，资源甚至不可能被发现。这可防止攻击者通过扫描 PEPs 后面的资源和/或对其发起 DoS 攻击来识别目标。请注意，并非所有资源都应以这种方式隐藏；某些网络基础结构组件（如 DNS 服务器）必须可访问。

5. 数据平面和控制平面在逻辑上是分开的。策略引擎、策略管理器和策略执行点都是在逻辑上独立、企业系统和资源无法直接访问的网络上进行通信。数据平面用于应用/服务数据通信。策略引擎、策略管理器和策略执行点使用控制平面进行通信和管理系统之间的连接。策略执行点必须能够发送和接收来自数据平面和控制平面的信息。

6. 企业系统可以访问策略执行点组件。企业用户必须能够访问策略执行点组件，从而访问资源。访问方式包括在企业系统上启用连接的 Web 门户、网络设备或软件代理。

7. 策略执行点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策略执行点都可与策略管理器连接，以便从客户端建立连接。所有

企业业务流程流量都通过一个或多个策略执行点。

8. 远程企业系统应该能够不通过基础设施去访问企业资源。例如，不应要求远程用户使用安全链接连接到企业网络（即 VPN），从而访问由公共云提供商托管的企业服务（例如邮件服务）。

9. 用于支持 ZTA 访问决策过程的基础架构应具有可扩展性，以考虑过程负载的变化。ZTA 中使用的策略引擎、策略管理器和策略执行点成为任何业务流程中的关键组成部分。延迟或无法联系到策略执行点（或策略执行点无法联系到策略管理器/策略引擎）对执行工作流的能力产生负面影响。实现 ZTA 的企业需要为预期的工作负载提供组件，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. 由于策略或可观察因素，企业系统可能无法达到某些策略执行点。例如，可能有一项策略规定，如果请求的资产位于企业之外，移动资产可能无法访问到某些资源。这些因素可能涉及到位置（地理位置或网络位置）、设备类型等。

4. 部署场景/用例

任何企业网络都可基于零信任原则进行设计。如今，大多数组织的企业基础架构已经具备了零信任的某些要素，或者正在通过实施信息安全、弹性策略和最佳实践来实现零信任。有几种场景可以更轻松地实施零信任体系架构。例如，零信任架构易于在地理广泛分布和/或具有高度移动性的员工队伍的组织中扎根。也就是说，任何组织都可以从零信任架构中获益。

在下面的用例中，没有明确指出零信任架构，因为企业可能同时拥有遗留和（可能）零信任架构基础设施。零信任架构组件和遗留网络基础设施在企业中可能会同时运行一段时间，见第 7.2 节。

4.1 拥有多分支机构的企业

最常见的情况是，企业只有一个总部和一个或多个地理分散的位置，这些位置没有企业拥有的物理网络连接（见图 8）。远程员工可能没有完全由企业拥有的本地网络，但仍需要访问企业资源才能执行其任务。企业可能有一个多协议标签交换（MPLS）链接到企业总部网络，但可能没有足够的带宽用于所有通信量，或者可能不希望以基于云的应用/服务为目的地的通信量在企业总部网络中穿越。同样，员工也可以使用企业设备或个人设备，进行远程访问网络或远程工作。在这种情况下，企业可能希望授予对某些资源（如员工日历、邮件）的访问权限，但拒绝访问更敏感的资源（如人力资源数据库）。

在这个用例中，策略引擎/策略管理器通常作为云服务（通常提供更高的可用性，不需要远程工作者依赖企业基础设施来访问云资源）托管，终端资产具有已安装的代理（见第 3.2.1 节）或访问资源门户（见第 3.2.3 节）。由于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访问由云服务托管的应用/服务，因此将策略引擎/策略管理器托管在企业本地网络上可能不是响应最迅速的。

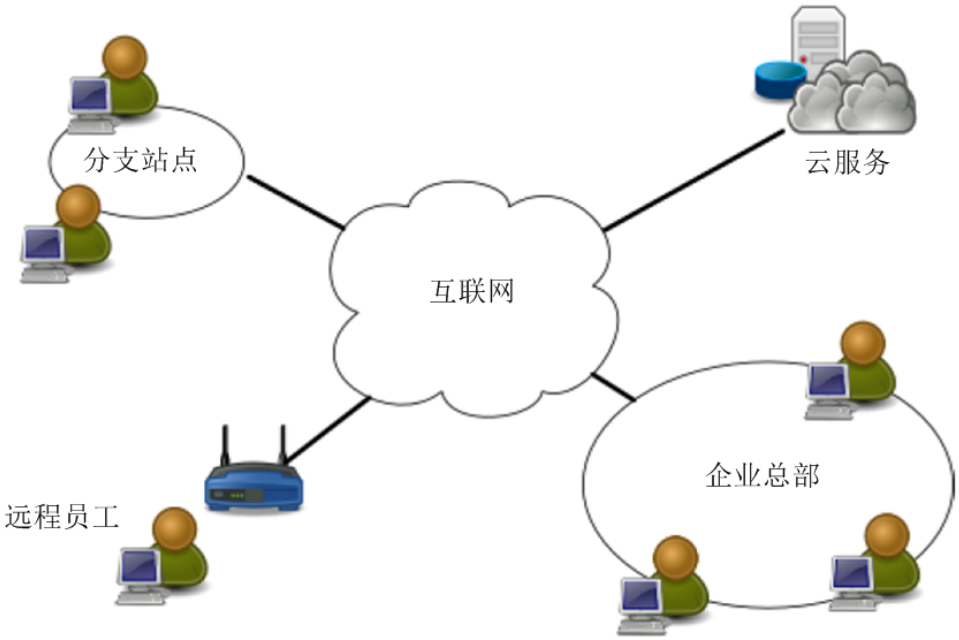

图 8：拥有远程员工的企业

4.2 多云/云到云的企业

关于部署零信任架构策略的日益常见的用例是使用多个云提供商的企业（见图 9）。在这个用例中，企业有一个本地网络，但使用两个（或更多）云服务提供商来承载应用/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。为了提高性能和便于管理，托管在云提供商 A 中的应用程序应该能够直接连接到托管在云提供商 B 中的数据源，而不是强制应用程序通过企业网络返回。

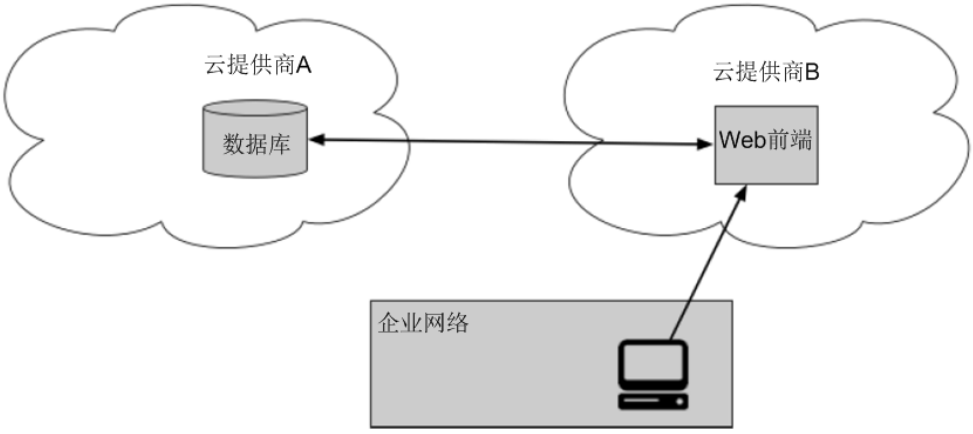

图 9：多云用例

这个多云用例是 CSA-SDP 规范的服务器到服务器实现。随着企业转向更多的云托管应用程序和服务，依赖企业边界进行安全保防护显然已成为一种负担。如第 2.2 节所述，零信任架构认为，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没有区别。多云使用的零信任方法是在每个应用/服务和数据源的访问点放置策略执行点。策略引擎和策略管理器可以位于是云或甚至第三个云提供商上的服务。然后，客户端（通过门户或本地安装的代理）直接访问策略执行点。这样，即使托管在企业外部，企业仍然可以管理对资源的访问。一个挑战是，不同的云提供商有独特的方法来实现类似功能。企业架构师需要知道如何在他们使用的每个云提供商上实现他们的企业 ZTA。

4.3 存在外包服务和/或非员工访问的企业

另一个常见的场景是，企业包含需要有限访问企业资源才能完成工作的现场访问者和/或外包服务提供商（见图 10）。例如，企业有自己的内部应用/服务、数据库和资产。这些包括外包给偶尔在现场提供维护任务的供应商的服务（例如，由外部供应商拥有和管理的智能暖通空调（HVAC）系统和照明系统）。这些访客和服务提供商将需要网络连接来执行他们的任务。零信任架构网络可以通过允许这些设备（以及任何来访的服务技术人员）访问互联网来实现这一点，同时还可以屏蔽企业资源。

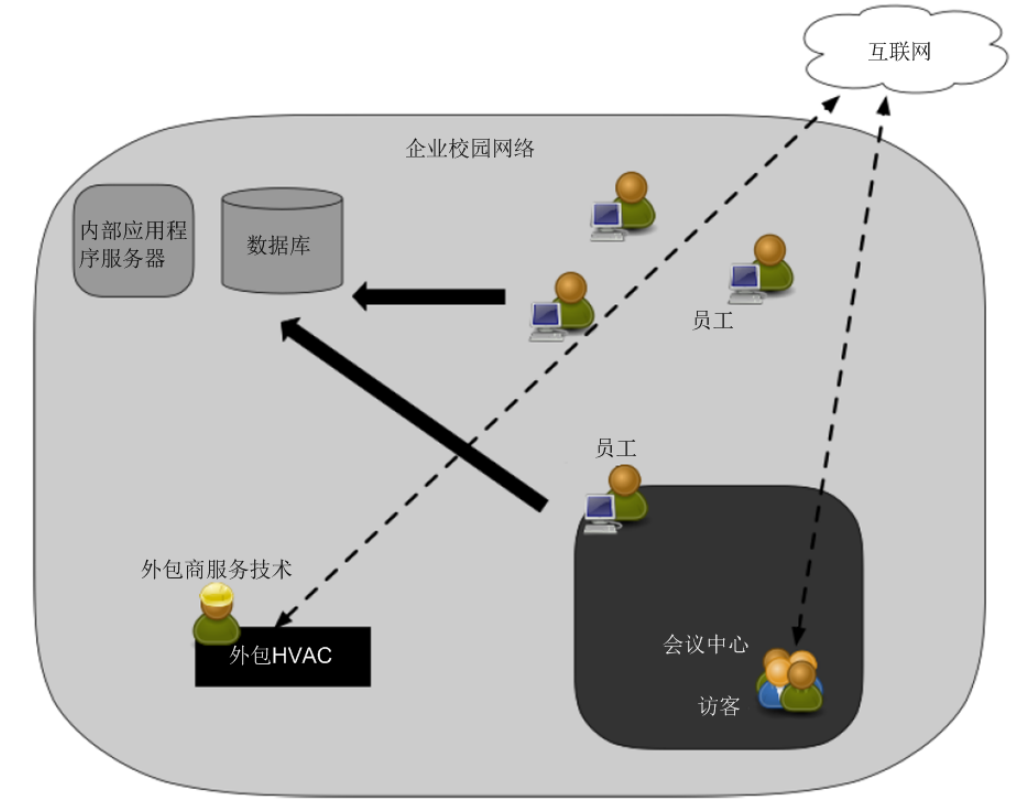

图 10：具有非员工访问的企业

在本例中，该组织还有一个会议中心，访客可以在会议中心与员工进行交互。同样，通过零信任架构的 SDP 策略，员工设备和主体是有区别的，可以分别访问恰当的企业资源。进入校园的访客可以访问互联网，但不能访问企业资源。他们甚至可能无法通过网络扫描发现企业服务（即，阻止主动网络侦察/东西移动）。

在这个用例中，策略引擎和策略管理器可以作为云服务或在 LAN 上托管（假设很少或根本没有使用云托管服务）。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 策略管理器所有非企业系统（那些没有安装代理或无法连接到门户的系统）不能访问本地资源，但可以访问互联网。

4.4 跨企业协作

第四个用例是跨企业协作。例如，有一个项目涉及企业 A 和企业 B 的员工（见图 11）。这两个企业可以是独立的联邦机构（G2G），甚至是可以是一个联邦机构和一个私营企业（G2B）。企业 A 运行用于项目的数据库，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 的员工设置专用帐户，以访问所需的数据并拒绝访问所有其他资源。但这很快就会变得难以管理。如果两个组织的策略执行点都可以在联合身份证社区中对主体进行身份认证，那么让两个组织都注册到联合身份证管理系统中可以更快地建立这些关系。

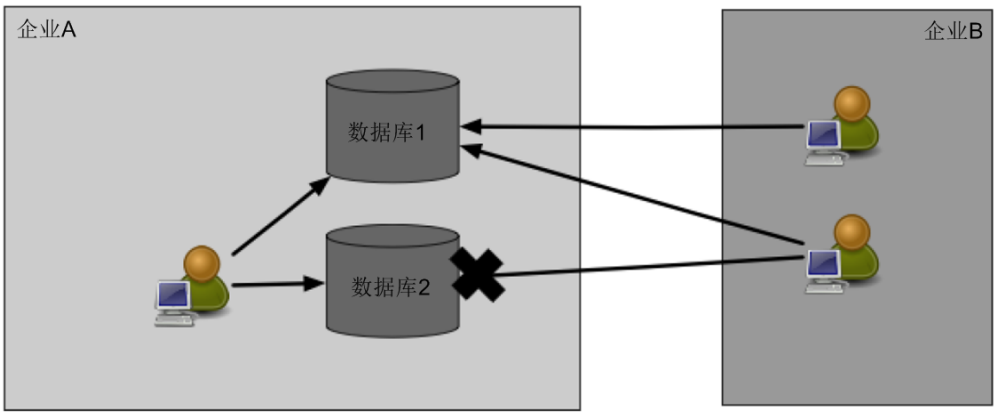

图 11：跨企业协作

此场景类似于上面的用例 1，因为两个企业的员工可能不在其组织的网络基础设施上，并且他们需要访问的资源可能在其中一个企业网络的内部或托管在云中。这意味着不需要复杂的防火墙规则或企业范围的访问控制列表，允许属于企业 B 的某些 IP 地址基于企业 A 的访问策略访问企业 A 中的资源。如何完成此访问，取决于使用的技术。与用例 1 类似，作为云服务托管的策略引擎和策略管理器可以向所有各方提供可用性，而无需建立 VPN 或类似的服务。企业 B 的员工可能会被要求在其系统上安装软件代理或通过 Web 代理网关访问必要的数据资源（见第 3.2.3 节）。

4.5 面向公众或客户提供服务的企业

许多企业的一个共同特点是面向公众的服务，可能包括也可能不包括用户注册（即，用户必须创建或已获得一组登录凭据）。这类服务可以面向公众、一组与现有业务关系的客户，或者一组特殊的非企业用户（如员工家属）。在所有情况下，请求的资产很可能不是企业所有的，并且企业在哪些内部网络安全策略可以实施方面受到限制。

对于不需要登录凭据才能访问的一般面向公共的资源（例如，公共网页），ZTA 的原则并不直接适用。企业无法严格控制请求资产的状态，匿名公共资源（例如，公共网页）不需要凭据才能访问。

企业可以为注册公共用户（如客户（即与企业有业务关系的用户）和特殊用户（如员工家属）制定策略。如果要求用户出示或获得颁发的凭据，企业可以制定有关密码长度、生命周期和其他详细信息的策略，并可以提供 MFA 作为选项或要求。然而，企业在为这类用户实现策略方面受到限制。有关传入请求的信息可能有助于确定公共服务的状态并检测伪装为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通用 web 浏览器中的一个访问。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示某种自动攻击，企业可以采取措施限制来自这些已标识客户端的请求。企业还应了解有关可收集和记录请求用户和资产的哪些信息的任何法规或条例。

5. 零信任架构相关的威胁

任何一家企业都不可能百分百防范网络安全风险。若与现有的网络安全策略和指南、身份和访问管理、持续监控和常规网络卫生措施相结合，ZTA 可减少总风险，防御常见威胁。然而，在实施 ZTA 时，面临一些特有的威胁。

5.1 ZTA 决策过程的维护

在 ZTA 中，策略引擎（PE）和策略管理器（PA）组件是整个企业的关键组件。企业资源之间不存在连接，除非经过 PE 和 PA 批准以及可能由其进行配置。这意味着必须对这些组件进行正确配置和维护。任何具有 PE 规则配置访问权限的企业管理员均可在未经批准的情况下进行更改（或误操作），这些更改可能会中断企业运营。同样，若 PA 遭遇入侵可能允许访问未经批准的资源（例如，被入侵的自带设备）。要防范相关风险，必须对 PE 和 PA 组件进行合理配置和监控，对任何配置更改进行记录和审计。

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 许可及可能进行的配置操作，企业资源无法相互连接。如果攻击者中断或拒绝对 PEP 或 PE/PA 的访问（即拒绝服务攻击或路由劫持），则可能对企业运营造成不利影响。假设大多数企业可通过在安全可靠的云环境中执行策略或按照网络弹性指南[SP800-160v2]在多个位置重复执行策略来缓解此威胁。

这会缓解风险，但却无法彻底消除风险。Mirai 等僵尸网络对关键互联网服务发起大规模 DoS 攻击，造成数百万互联网用户的服务中断。[5]此外，攻击者也可能监听和中断企业（如分支办事处或某个远程员工）中的一些（或全部）用户帐户向 PEP 或 PA 发送的流量。在这些情况下，仅有一部分企业用户受影响。这种情况并不仅在 ZTA 中出现，在传统的基于 VPN 的访问中也存在。

托管提供商也可能意外地使基于云的 PE 或 PA 离线。云服务在过去经历过中断，包括基础设施即服务（IaaS）[6]和软件即服务（SaaS）。[7]若策略执行组件无法通过网络访问，操作失误会导致整个企业无法正常运转。

同时，这也存在企业资源无法通过 PA 访问的风险。因此，即使授予了主体访问权限，PA 仍无法配置来自网络的访问连接。这可能是由于分布式拒绝服务攻击或只是由于意外的大量使用。这与任何其他网络中断类似，即由于资源因某种原因不可用导致一些或所有企业主体无法访问这些特定资源。

5.3 被盗凭据/内部威胁

合理实施 ZT 策略、信息安全和弹性策略以及最佳实践可降低攻击者通过被盗凭据或内部攻击获得广泛访问权限的风险。ZT 基于网络位置的无隐式信任原则意味着攻击者只能靠破坏某个已有帐户或设备才能在企业中站住脚。ZTA 确实可以阻止被入侵的帐户或系统访问其正常权限之外或正常访问模式之外的资源。这意味着针对攻击者感兴趣的资源具有访问策略的帐户将成为攻击者的主要目标。

攻击者可以使用网络钓鱼、社会工程或攻击组合来获取有价值帐户的凭据。基于攻击者的动机，“有价值”可能意味着不同的事情。例如，企业管理员帐户可能是有价值的，但对财务收益感兴趣的攻击者可能会考虑访问同等价值的财务或支付资源的帐户。为访问请求实施多因素认证（MFA）可以降低从受损帐户丢失信息的

---

[5] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
[6] https://aws.amazon.com/cn/message/41926/
[7] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12286870

风险。但是，具有有效凭据的攻击者（或恶意内部人员）可能仍然能够访问已授予帐户访问权限的资源。例如，具有有效人力资源员工的凭据和企业拥有的资产的攻击者或受损员工可能仍然能够访问员工数据库。

ZTA 可降低风险并防止任何被入侵的帐户或系统在整个网络中横向移动。如果遭破坏的凭据未被授权访问特定资源，则它们将继续被拒绝访问该资源。此外，基于上下文的信任算法（请参见 3.3.1 节）相对于传统网络更容易检测到此类攻击并快速响应。上下文信任算法可以检测出超出正常行为的访问模式，并拒绝被入侵的帐户（或内部威胁）访问敏感资源。

5.4 网络可见性

3.4.1 节中提到需检查并记录网络上的所有流量，并对其进行分析，从而识别和应对针对企业的潜在攻击。然而，如前所述，企业网络中的一些（可能是大多数）流量对于第 3 层网络分析工具来说可能是不透明的。此流量可能来自非企业所有的资产（例如，使用企业基础设施访问 Internet 的外包服务）或可防止被动监控的应用/服务。企业无法执行 DPI 或检查加密的流量，必须使用其他方法评估网络中可能存在的攻击者。

这并不意味着企业无法分析网络上检测到的加密流量。企业可以收集加密流量相关的元数据（例如，源地址和目标地址等），并使用这些元数据检测网络上可能存在的恶意软件通信或活跃的攻击者。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允许企业将流量归类为有效或可能存在恶意且需要修复。

5.5 系统和网络信息的存储

分析数据是公司在监控和分析网络流量威胁时需考虑的一方面。若存储了监视器、网络流量和元数据用于构建上下文策略、取证或后期分析，则这些数据将成为攻击者的目标。这些资源与网络图、配置文件和其他各种网络架构文档一样也应该受到保护。若攻击者能成功访问该信息，则可能会深入了解企业架构并识别资产进行进一步侦察和攻击。

对访问策略进行编码的管理工具是攻击者从 ZT 企业中获取侦察信息的另一个来源。与存储的通信流量一样，此组件包含对资源的访问策略，可向攻击者提供最有入侵价值的帐户信息（例如，对所需的数据资源有访问权限的帐户）。

与所有有价值的企业数据一样，这些资源应得到足够的保护以防止未经授权访问和访问尝试。由于这些资源对安全至关重要，因此它们应具有最严格的访问策略且仅来自指定或专用管理员帐户。

5.6 对专有数据格式或解决方案的依赖

ZTA 依赖多个不同的数据源来做出访问决策，包括关于请求主体的信息、使用的资产、企业和外部情报、威胁分析等。通常，用于存储和处理这些信息的资产在信息交互和交换方式方面没有一个通用的开放的标准。这样就造成了企业由于互操作性问题拘泥于一些提供商。若某个提供商存在安全问题或发生中断，企业可能因未预留特殊情况支出费用（如替换数个资产）无法迁移至另外一个提供商或经历一个漫长的过渡过程（如将策略规则从一种方式转换为另一种方式）。如同 DoS 攻击一样，这种风险并非 ZTA 特有，但由于 ZTA 严重依赖信息的动态访问（企业和服务提供商双方），中断可能会影响企业的核心业务职能。为缓解相关风险，企业除了应考虑性能、稳定性等比较典型的因素，还应综合考虑供应商安全控制、更换企业成本、供应链风险管理等因素，从而对服务提供商进行全面评估。

5.7 ZTA 管理中非个人实体（NPE）的使用

企业目前正在部署人工智能（AI）和其他基于软件的代理管理网络安全问题。这些组件需与 ZTA 的管理组件（例如，PE、PA 等）进行交互，有时会代替管理员。在实施 ZTA 策略的企业中，这些组件如何对自身进行身份验证是一个待解决的问题。我们假设大多数自动化技术系统在使用资源组件的 API 时会采取某种方式进行身份验证。

在使用自动化技术进行配置和策略实施时，最大的风险是可能出现影响企业安全态势的假阳性误报（无害操作被误认为是攻击）和假阴性误报（攻击被误认为是正常活动）。这可以通过定期的重新调整分析来减少，以纠正错误的决策并改进决策过程。

存在的风险是攻击者将能够诱导或强制 NPE 代理执行其无权执行的某些任务。与人类用户相比，软件代理可能在执行管理或安全相关任务时采取较低的认证标准（例如，API 密钥和 MFA）。理论上说，若攻击者可与代理进行交互，可能会诱骗代理为攻击者获得更高访问权限或代表攻击者执行某些任务。另一个潜在风险是攻击者可在执行任务时获得软件代理的凭证并模拟该代理。

6. 零信任架构与现有联邦指南的可能关联

一些现有的联邦政策和指南与 ZTA 战略的规划、部署和实施相交叉。这些策略不会阻止企业采取更加倾向于零信任导向的网络战略，但会影响一个机构的零信任框架的发展。若与现有的网络安全政策和指南、身份、凭证和访问管理（ICAM）、持续监测和通用网络卫生相结合时，ZTA 可提升组织的安全状况，防护常见威胁。

6.1 ZTA 和 NIST 风险管理框架

ZTA 部署涉及围绕指定任务或业务流程（见 7.3.3 节）的可接受风险制定访问策略。可以拒绝对某个资源的所有网络访问，仅允许通过连接的终端访问。不过，在大多数情况下，这一点限制性太大，可能阻碍工作的完成。为使联邦机构执行其任务，需允许存在可接受程度的风险。必须对执行特定任务相关的风险进行识别、评估，并接受或缓解。为此，NIST 风险管理框架应运而生[SP800-37]。

在 ZTA 的规划和实施过程中，由于添加新组件（例如，PE、PA 和 PEP）并减少对网络边界防御的依赖，可能会改变企业定义的授权边界。在 ZTA 的网络安全战略中，RMF 中描述的过程不受影响。

6.2 ZT 和 NIST 隐私框架

保护用户和私人信息（如个人身份信息（PII））通常是企业的首要关注。隐私和数据保护纳入了 FISMA 和 HIPAA 等合规计划中。作为回应，NIST 制定了供企业使用的隐私框架[NISTPRIV]。该框架提供了用于描述隐私风险和缓解战略的框架以及公司对所存储和处理的用户隐私和私有信息进行风险识别、评估和缓解的流程。这包括企业用于支持 ZTA 操作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 的核心要求之一是，企业应该检查并记录其环境中的流量（或者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）。这些流量可能含有私人信息或存在隐私风险。组织需对网络流量拦截、扫描和记录相关的任何潜在风险进行识别[NISTIR 8062]，例如，通知用户、采取认证（通过登录页面、条幅等类似措施）和对企业的用户进行培训。NIST 隐私框架[NISTPRIV]可帮助制定用于识别和缓解 ZTA 网络的任何隐私相关风险的规范流程。

6.3 ZTA 和联邦身份、凭证和访问管理架构（FICAM）

主体配置是 ZTA 的关键部分。如果 PE 没有足够的信息识别关联的主体和资源，则 PE 无法确定建立失败的连接是否被允许连接到资源。在迁移到采取更倾向于零信任标准的部署之前，需制定完善的主体配置和认证策略。因此，企业要有一套清晰的主体属性和策略供 PE 评估访问请求。

近期，管理和预算办公室（OMB）发布了 M-19-17 谅解备忘录，提升联邦政府的身份管理。该政策旨在“就任务交付、信任和国家安全的推动者身份达成共识”[M-19-17]。该谅解备忘录呼吁联邦机构成立 ICAM 办公室负责身份签发和管理。很多这些管理政策应采取 NIST SP 800-63-3《数字身份指南》[SP800-63]中的建议。由于 ZTA 严重依赖于精确的身份管理，ZTA 的任何活动都需要与机构的 ICAM 政策相结合。

6.4 ZTA 和可信互联网连接（TIC）3.0

TIC 是由 OMB、国土安全部（DHS）和总务管理局（GSA）联合管理的一项联邦网络安全计划，旨在建立联邦政府的网络安全基线。从历史角度看，TIC 是一项基于边界的网络安全战略，要求各机构对其外部网络连接进行监控和加固。TIC 1.0

和 TIC 2.0 内部假设边界内部是“可信的”，而 ZTA 认为该网络位置是“不可信的”（即机构的内部网络不“可信”）。TIC 2.0 为机构边界的 TIC 访问点提供一系列网络安全能力（如内容过滤、监控、认证及其他能力），其中很多这些能力与 ZT 原则一致。

TIC 3.0 将进行更新以适配云服务和移动服务[M-19-26]。在 TIC 3.0 中，人们意识到，“可信”的定义在特定的计算环境中可能会有所不同，机构在定义信任区时有不同的风险承受能力。此外，TIC 3.0 还具有更新的《可信互联网连接安全能力手册》。该手册定义了两种类型的安全能力：（1）适用于企业级的通用安全能力，以及（2）PEP 安全能力，即应用于多个策略执行点的网络级能力，如 TIC 用例中定义的。PEP 安全能力可应用于任何既定数据流边缘的策略执行点，而非机构边界的单个 PEP 上。很多这些 TIC 3.0 安全能力直接为 ZTA 提供支持（例如，加密的流量、强认证、微分段、网络和系统库存及其他）。TIC 3.0 定义了特定用例，用于描述如何对多个特定应用、服务和环境实现信任区和安全能力。

TIC 3.0 主要提供网络安全保护，而 ZTA 则是一个更具包容性的架构，用于解决应用程序、用户和数据的保护问题。随着 TIC 3.0 用例的发展，很可能会开发 ZTA TIC 用例用于定义 ZTA 执行点部署的网络保护。

6.5 ZTA 和 EINSTEIN（NCPS-国家网络安全保护系统）

NCPS（又名 EINSTEN（爱因斯坦））是一个集成的分散系统，提供入侵检测、高级分析、信息共享和入侵防御能力，保护联邦政府免受网络威胁。NCPS 的目标与零信任的首要目标一致，即管理网络风险，提升网络保护，使合作伙伴能够保护网络空间。EINSTEN 传感器可使 CISA 的国家网络安全和通信集成中心（NCCIC）保护联邦网络，对联邦机构的重大事件做出响应。

适用于美国国土安全部态势感知的 NCPS 传感器的部署基于联邦政府的边界网络防御，而 ZTA 使保护更贴近数据和资源。NCPS 项目正在不断发展，以确保通过利用云流量的安全信息来保护态势感知，从而为 ZTA 系统扩展的态势感知遥测技术奠定基础。NCPS 入侵预防功能还需要改进，以便能够通报当前 NCPS 位置和 ZTA 系统的政策执行情况。如果整个联邦政府都采用 ZTA，则 NCPS 的实现需持续改进或需部署新能力实现 NCPS 目标。事件响应者可能会利用采取了 ZTA 的联邦机构的认证、流量监测和流量记录信息。ZTA 中生成的信息可能会更好地展示量化的事件影响；机器学习工具可利用 ZTA 数据提升检测；可对 ZTA 的其他日志进行保存用于事件响应者在对发生的事件进行分析。

6.6 ZTA 和持续诊断和缓解（CDM）计划

国土安全部 CDM 计划旨在改进联邦机构信息技术（IT），关键是机构要深入了解其系统、配置和主体。若要对系统进行保护，机构需制定进程，发现和了解其基础设施的基本组件和攻击者。

- **哪些设备接入了网络？**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，对这些物件的安全状况进行监控和提升。
- **谁在使用网络？**哪些用户是组织的内部用户，哪些是外部用户，哪些允许访问企业资源？这包括可进行自动行为的非个人实体。
- **网络中发生了什么？**企业需深入了解系统之间的流量模式和消息。
- **数据保护是如何实现的？** 企业需配置策略对静态信息、传输中的信息和使用中的信息进行保护。

制定完备的 CDM 计划是 ZTA 成功的关键。例如，企业若迁移至 ZTA 必须有一个系统来发现和记录物理和虚拟资产，以创建可用的库存。国土安全部的 CDM

计划已启动了数项工作构建联邦机构转向 ZTA 战略所需的能力。例如，国土安全部的硬件资产管理（HWAM）[HWAM]计划帮助机构识别其网络架构中的设备，从而部署安全配置。这类似于制定 ZTA 路线图的第一步。机构必须了解网络（或远程访问资源的网络）中活跃的资产，从而对其活动进行分类、配置和监控。

6.7 ZTA、云智能和联邦数据战略

《云智能战略》[8]更新了《数据中心优化计划》[M-19-19]策略。在企业规划 ZTA 战略时，《联邦数据战略》[9]会对机构的一些需求产生影响。要实现这些策略，机构需清点并评估如何收集、存储和访问本地和云端数据。

该清单对于确定哪些业务流程和资源会从实施 ZTA 中受益至关重要。因为数据资源、应用和服务位于企业网络边界之外，他们最能体会到在易用性、可扩展性和安全性方面的益处。主要基于云或由远程用户使用的数据资源和应用对于实现 ZTA 方案（请参见 7.3.3）来说不错的选择。

对于《联邦数据战略》来说，还需考虑如何将机构的数据资产开放给其他机构或公众使用。这与跨企业合作的 ZTA 用例（参见 4.4 节）一致。对资产采取 ZTA 的机构，在制定战略时需考虑协作（或发行）需求。

[8] 《联邦云计算战略》https://cloud.cio.gov/strategy/
[9] 《联邦数据战略》https://strategy.data.gov/

7. 迁移到零信任架构

实施 ZTA 战略是一个过程，而非对基础设施或流程的大规模替换。组织应逐步实施零信任原则、进行流程变更、并采取保护其最高价值数据资产的技术解决方案。大多数企业在持续投资当前 IT 现代化方案的同时，在很长一段时间内会出现零信任和现有模式并存的局面。制定一个 IT 现代化计划（包括迁移到基于 ZT 原则的体系结构）可以帮助企业形成小规模工作流迁移的路线图。

企业如何迁移到 ZTA 战略取决于其当前的网络安全状况和运营情况。企业在部署以 ZT 为核心的重要网络[ACT-IAC]时应达到一个能力基线，即对企业的资产、主体、业务流程、流量和依赖关系映射进行识别和编目。企业在整理 ZTA 备选业务流程和参与此流程的主体/资产的列表之前需要此信息。

7.1 纯零信任架构

在绿地方法中，可从头开始构建零信任架构网络。假设企业清楚其运营所需的应用/服务和工作流，那么企业可为这些工作流制定基于零信任策略原则的架构。一旦确定了工作流，企业即可缩小所需组件的范围，并开始规划各组件的交互方式。从这点上看，构建网络基础设施和配置组件是一项工程和组织工作。这可能会带来额外的组织变更，具体取决于企业当前的设置和运行方式。

实际上，这种方案对于联邦机构或任何组织的当前网络并不可取。然而，组织有时可能因履行一项新职责而需要构建自己的架构。在这些情况下，可能需在某种程度上引入 ZT 概念。例如，机构在履行一项新职责时需构建新应用、服务或数据库，可围绕 ZT 原则和安全系统工程[SP8900-160v1]（为授予访问权限前对评估主体信任，对新资源划分微边界）设计所需的新架构。机构在多大程度上取得成功取决于该新架构对当前资源（如 ID 管理系统）的依赖程度。

7.2 ZTA 和传统架构并存

任何一家大企业都不可能在一次技术更新周期内迁移至 ZT 网络。在传统企业中，ZTA 工作流在一段时间（也许是无限期）内会与企业的非 ZTA 工作流并存。企业向 ZTA 方法迁移时，可采取每次迁移一个业务流程的方式。企业需确保公共元素（例如 ID 管理、设备管理、事件日志等）足够灵活，可在 ZTA 和当前模式并存的安全架构中运行。企业架构师可能也希望只采取那些可与现有元素相交互的 ZTA 备选解决方案。

将现有工作流迁移到 ZTA 可能需要（至少）部分重新设计。如果企业尚未在工作流中采用安全系统工程[SP800-160v1]实践，则可以借此机会采用一番。

7.3 在基于传统架构的网络中引入 ZTA 的步骤

要迁移到 ZTA，组织需对其资产（物理和虚拟）、主体（包括用户权限）和业务流程有详细了解。PE 在评估资源请求时会使用这些信息。若这些信息不完整，通常会导致业务流程失败，即 PE 由于信息不足而拒绝请求。如果组织中有未知的“影子 IT”部署在运行，就明显会成为一个问题。

企业实施 ZTA 之前，应对资产、主体、数据流和工作流进行调查。这是 ZTA 部署前必须要了解的基本情况。如果不了解当前的操作状态，企业就无法确定需要准备哪些新流程或系统。这些调查可并行进行，但都与对组织的业务流程检查相关。这些步骤可与风险管理框架（RMF）[SP800-37]中的步骤相对应，因为 ZTA 迁移相关的任何举措均可被视为是降低机构的业务功能风险的过程。ZTA 迁移路径如图 12 所示。

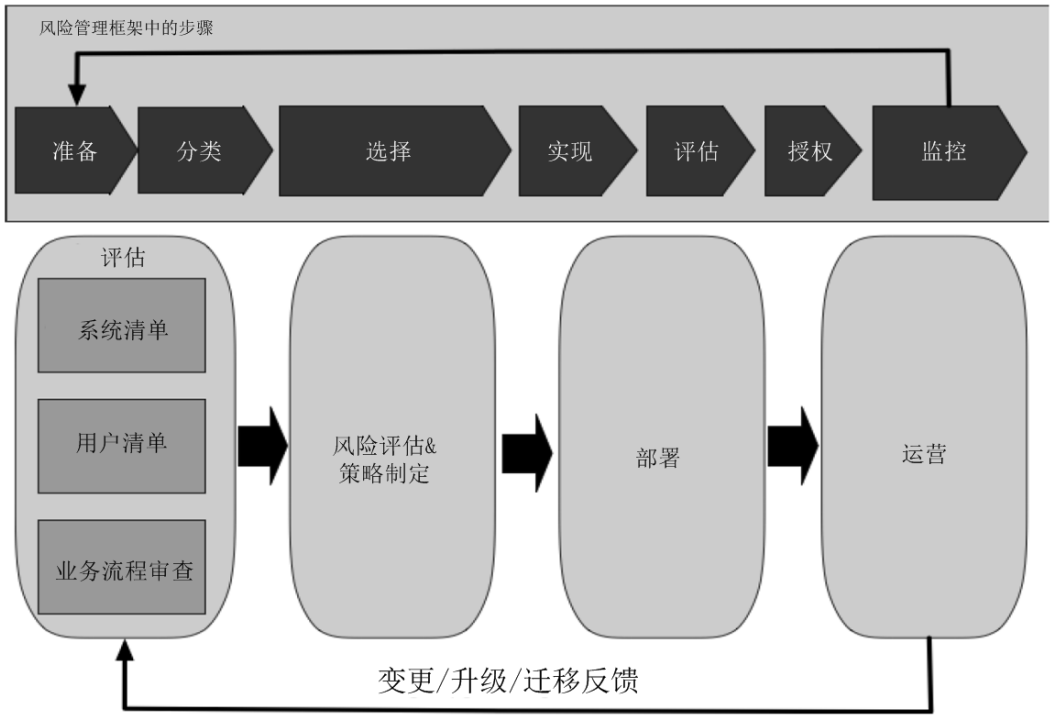

图 12 ZTA 部署周期

初始库存清单创建后，需定期维护和更新。此更新可能会更改业务流程或不产生任何影响，但应对业务流程进行评估。例如，数字证书提供商中的变更看似不会产生重大影响，但可能会涉及证书根存储管理、证书透明度日志监控和其他最初不大明显的因素。

7.3.1 识别企业中的攻击者

为确保 ZTA 网络正常运行，PE 必须了解企业中的研究对象。“研究对象”包括人类实体和可能存在的非人类实体（NPE），例如与资源交互的服务帐户。

在对具有特殊权限的用户（如开发人员或系统管理员）分配属性或角色时需要额外的检查。在许多传统的安全架构中，这些帐户可能具有访问企业所有资源的总体权限。ZTA 应允许开发人员和管理员有足够的灵活性以满足他们的业务需求，同时使用日志和审核操作来标识访问行为模式。要部署 ZTA，可要求管理员获得 NIST SP 800-63A，第五节[SP800-63A]中概述的更高分数或符合更严格的标准。

7.3.2 识别企业拥有的资产

正如 2.1 节中介绍的，ZTA 的一个关键要求是具备识别和管理设备的能力。ZTA 还要求能够识别和监控企业拥有的网络基础设施上部署的或访问企业资源的非企业拥有的设备。企业资产管理能力是 ZTA 成功部署的关键，这些资产包括硬件组件（例如笔记本电脑、电话、物联网设备等）和数字工件（例如用户帐户、应用程序、数字证书等）。可能无法对所有企业拥有的资产进行全面的普查，因此企业应考虑建立快速识别、分类和评估企业拥有的基础设施上新发现的资产的能力。

这不仅仅是对企业资产数据库进行编目和维护，还包括配置管理和监控。对当前系统状态的监控能力是评估访问请求过程的一部分（请参见 2.1 节）。也就是说，企业必须能够配置、调查和更新包括虚拟系统和容器在内的企业系统，这还涉及这些系统的物理位置（作为最佳估计）和网络位置。该信息应在做出资源访问决策时通知给 PE。

应尽可能对非企业所有的资产和企业所有的“影子 IT”进行编目。这可能包括企业可见的任何内容（例如，MAC 地址和网络位置）以及管理员的输入。这些信息不仅用于访问决策（因为合作方和自带系统可能需要联系 PEP），还用于企业监

控和取证日志记录。“影子 IT”提出了一个特殊的问题，因为这些资源是企业拥有的，而不是像其他资源一样管理。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，因为它们可能不知道并包含在网络访问策略中。

许多联邦机构已开始执行企业资产识别任务。已构建了硬件资产管理（HWAM）[HWAM]和软件资产管理（SWAM）[SWAM]的机构在制定 ZTA 战略时有一套丰富的数据可供参考。各机构还可能有一份高价值资产相关的 ZTA 备选流程清单，这些高价值资产(HVA) [M-19-03]已被确定为机构任务的关键所在。这些工作需在 ZTA 战略纳入任何业务流程之前在企业或机构范围内开展。必须对这些计划进行扩展，适应企业的变化，除了向 ZTA 迁移，在企业引入新系统、服务和业务流程时均需开展该工作。

7.3.3 识别关键流程并评估执行流程相关的风险

机构应进行的第三项清查是对机构任务中的业务流程、数据流及其关系进行识别和排序。业务流程应考虑在何种情况下允许和拒绝资源访问请求。企业可能希望在最初过渡到 ZTA 时从低风险的业务流程着手，因为这样一旦发生中断可能不会对整个组织产生负面影响。在积累了足够的经验后，就可以选择更关键的业务流程。

基于云的资源或远程工作人员使用的业务流程通常是切换到 ZTA 的不错选择，而且可能会看到易用性和安全性的改善。企业客户端可以直接请求云服务，而不是通过虚拟专用网（VPN）将企业边界映射到云中或将客户端加入企业网络。企业的 PEP 确保为客户端分配资源访问权限之前符合企业策略。规划者还应该考虑在性能、用户体验以及在为给定的业务流程实现 ZTA 时可能出现的工作流脆弱性增加方面的潜在折衷。

7.3.4 为 ZTA 候选制定策略

明确候选服务或业务工作流的过程取决于以下几个因素：流程对组织的重要性、受影响的主体组、工作流所用资源的当前状态。可利用 NIST 风险管理框架[SP800-37]从风险角度评估资产或工作流的价值。

明确资产或工作流后，确定使用或受工作流影响的所有上游资源（如 ID 管理系统、数据库、微服务）、下游资源（如日志记录、安全监控）和实体（如主体、服务帐户）。这可能会对首批迁移到 ZTA 的备选者的选择产生影响。相对于对企业的整个主体群至关重要的应用/服务（例如，电子邮件）来说，一部分指定的企业主体使用的应用/服务（如采购系统）可能会优先迁移至 ZTA。

企业管理员需为候选业务流程中使用的资源明确一组标准（若使用基于标准的 TA）或可信的分数权重（若使用基于分数的 TA）（见第 3.3.1 节）。管理员可能需要在优化阶段对这些标准或值进行调整。这些调整对于确保策略有效非常必要，但又不妨碍对资源的必要访问。

7.3.5 定候选解决方案

在开发一系列备选业务流程后，企业架构师即可编写各种候选解决方案。一些部署模型（见 3.1 节）更适用于特定的工作流和当前的企业生态系统。同样，一些厂商解决方案比其他方案更适合于特定用例。需要考虑的因素有：

- **解决方案是否要求在客户端资产上安装组件？**这可能会对那些使用或需要非企业拥有的资产（如 BYOD 或跨机构协作）的业务流程有限制。
- **解决方案是否适用于所有的业务流程资源均位于企业的办公场所的情况？**一些解决方案假设所请求的资源位于云中（所谓的“南北”流量），而不在企业范围内（“东西”流量）。候选业务流程资源的定位将对该流程的备选解决方案以及 ZTA 有影响。
- **解决方案是否提供了记录交互以进行分析的方法？**ZT 的一个关键组成部

分是收集和使用与在做出访问决策时反馈到 PE 的过程流相关的数据。

- **解决方案是否为不同的应用、服务和协议提供了广泛支持？**一些解决方案可能支持广泛的协议（网络、安全外壳[SSH]等）和传输（IPv4 和 IPv6），而其他解决方案的支持范围可能比较狭隘，比如只支持网络或邮件。
- **解决方案是否需要改变主体的行为？**某些解决方案可能需要额外的步骤来执行给定的工作流。这可能会改变企业主体执行工作流的方式。

其中一种解决方案是将现有业务流程的建模作为试点计划，而不仅仅进行替换。该试点计划可实现通用化用于多个业务流程或专门用于某个用例。该试点方案可作为将用户过渡为 ZTA 部署前的 ZTA 试验田，避开传统流程架构。

7.3.6 初始部署和监测

一旦选择了候选工作流和 ZTA 组件，即可启动初始部署。企业管理员必须使用选定的组件来实现制定的策略，但可能希望首先以观察和监视模式进行操作。很少有企业策略集在第一次迭代时就是完整的：重要的用户帐户（例如，管理员帐户）可能会被拒绝访问所需资源，也可能不需要他们具备的某些访问特权。

新的 ZT 业务工作流可在“报告模式”下运行一段时间，确保策略的有效性和可行性。这还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”意味着应为大多数请求分配访问权限且应将连接的日志和踪迹与最初制定的策略进行比较。应执行并记录基本策略（拒绝多因素身份认证（MFA）失败的请求或来自攻击者控制或破坏的已知 IP 地址的请求）。不过，在初始部署后，访问策略应更宽松些，以收集 ZT 工作流的实际交互相关的数据。一旦建立了工作流的基线活动模式，就可以更容易地识别异常行为。如果无法以更宽松的方式运行，企业网络运营人员应密切监视日志并准备根据运营经验修改访问策略。

7.3.7 扩大 ZTA

当获得足够的信任并细化工作流策略集时，企业进入稳定运行阶段，仍对网络和系统进行监控，对流量进行记录（请参见第 2.1 节），不过响应和策略修改的节奏放慢，原因是这方面的任务不应那么严峻。相关资源和流程的主体和利益相关者也应提供反馈，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。与上次发布一样，需确定候选工作流和解决方案集并制定初始策略。

但是，如果工作流发生变更，则需重新评估正在运行的 ZT 架构。对系统的重大变更，如新设备、软件（特别是 ZT 逻辑组件）的重要更新或组织结构的变化，都可能导致工作流或策略的变更。实际上，我们应在假定在某些工作已完成的情况下重新审视公司流程，例如，我们购买了新设备，但没有创建新用户帐户，因此只需更新设备资源清单。

附录 参考

[ACT-IAC] American Council for Technology and Industry Advisory Council (2019) *Zero Trust Cybersecurity Current Trends*. Available at https://www.actiac.org/zero-trust-cybersecurity-current-trends

[Anderson] Anderson B, McGrew D (2017) Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non- Stationarity. *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM, Halifax, Nova Scotia, Canada), pp 1723-1732. https://doi.org/10.1145/3097983.3098163

[BCORE] Department of Defense CIO (2007). Department of Defense Global Information Grid Architecture Vision Version 1.0 June 2007. Available at http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural% 20Vision,%20June%2007.pdf

[CSA-SDP] Cloud Security Alliance (2015) SDP Specification 1.0. Available at https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[FIPS199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[Gilman] Gilman E, Barth D (2017) *Zero Trust Networks: Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., Sebastopol, CA), 1st Ed.

[HWAM] Department of Homeland Security (2015) *Hardware Asset Management (HWAM) Capability Description*. Available at 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) An Intent-based Approach for Network Virtualization. *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*. (IEEE, Ghent, Belgium), pp 42-50. Available at https://ieeexplore.ieee.org/document/6572968

[JERICHO] The Jericho Forum (2007) *Jericho Forum Commandments*, version 1.2. Available at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

[M-19-03] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M- 19-03, December 10, 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[M-19-17] Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[M-19-19] Office of Management and Budget (2019) Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019. Available at https://datacenters.cio.gov/assets/files/m_19_19.pdf

[M-19-26] Office of Management and Budget (2019) Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB Memorandum M-19-26, September 12, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

[NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W (2015) Policy Machine: Features, Architecture, and Specification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. https://doi.org/10.6028/NIST.IR.7987r1

[NISTIR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[NISTPRIV] National Institute of Standards and Technology (2020) Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[SDNBOOK] Nadeau T, Gray K (2013) *SDN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies*. (O'Reilly) 1st Ed.

[SP800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST

Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene 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) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP800-160v2] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[SWAM] Department of Homeland Security (2015) *Software Asset Management (SWAM) Capability Description*. Available at https://www.us- cert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

附录 A 缩略语

API	应用程序编程接口
BYOD	自带设备
CDM	持续性诊断和缓解
DHS	美国国土安全部
DoS	拒绝服务
G2B	私营企业
G2G	独立的联邦机构
NIST	国家标准与技术研究院
NPE	非个人实体
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	安全信息与事件管理
TIC	可信互联网连接
VPN	虚拟专用网
ZT	零信任
ZTA	零信任架构
ZTE	零信任生态系统

附录 B 明确当前 ZTA 存在的缺口

在本文档编写时的背景研究期间，我们对对零信任组件和解决方案当前的成熟度进行了调查。调查结果显示，目前，ZTA 生态系统还不成熟，不适用于广泛部署。尽管我们可采取 ZTA 战略对企业网络进行规划和部署，但现在任何一种方案都不可能提供所有必要组件。同时，目前没有几个 ZTA 组件适用于企业中的所有各类工作流程。

我们在下面总结了当前的 ZTA 生态系统存在的缺口以及需进一步调查的方面。这些方面已做了一些基础工作，但 ZTA 原则会对这些方面带来哪些影响尚不明确，原因是目前关于各类以 ZTA 为核心的企业网络的经验还不是很丰富。

B.1 技术调查

多个供应商受邀介绍了其关于零信任的产品和观点。本次调查的目的是找出各机构因在哪些方面有疏漏而阻碍其现在迁移到 ZTA 基础框架或妨碍其对现有 ZTA 部署的维护。这些缺口可分为即时部署（即时或短期）、影响维护或运行的系统性问题（短期或中期）和知识缺失（未来研究领域）。表 B-1 总结了这些内容：

类别	问题示例	存在缺口
即时	• 如何编写采购要求。 • ZTA战略如何与TIC、FISMA等结合。	• 缺乏ZTA通用框架和词汇。 • 认为ZTA与现行政策存在冲突。
系统性	• 如何防止拘泥于某个厂商。 • 不同的ZTA环境如何互通。	• 过于依赖厂商API。
研究领域	• 若引入ZTA，威胁将如何演进； • 若引入ZTA，业务流程将面临怎样的变化；	• 对于采用ZTA的企业，成功的入侵是什么样子？ • 采用ZTA的企业中，最终用户的体验如何。

表 B-1 存在的缺口

B.2 哪些缺口会阻碍立即迁移至 ZTA

有些问题目前会阻碍 ZTA 战略的实施，称为“即时”问题，并没有考虑针对此类问题开展后续维护或迁移。有前瞻力的企业可能也会将维护视为启动 ZTA 组件初始部署的首要阻碍，但我们在本文会对此类企业进行单独分析。

B.2.1 缺乏 ZTA 设计、规划和采购的通用术语

目前业界还没有形成一套零信任战略，描述企业架构的设计和部署，也没有一套术语或概念描述 ZTA 的组件和运行。这样，组织（如联邦机构）就很难针对 ZTA 基础设施设计和组件采购制定一致的要求和政策。

2.1 节和 3.1 节的驱动因素是初步尝试构建关于 ZTA 术语和概念的可行基础。开发了抽象的 ZTA 组件和部署模型，作为考虑 ZTA 的基本条件和方案，目的是在制定企业需求和进行市场调查时，采取一种通用方法对 ZTA 方案进行审核、建模和讨论。随着联邦机构会积累越来越多的 ZTA 战略经验，以上章节可能会显得不全面，但目前来看这些内容是构建通用概念框架的基础。

B.2.2 对于 ZTA 与现有联邦网络安全政策冲突的看法

ZTA 是个单一框架，提供一套与现有网络安全观不兼容的解决方案。这是一种误解。实际上，应将零信任看作是当前网络安全战略的一种演进，因为许多概念和想法都已传播了很长时间。目前，鼓励联邦机构基于现有指南（参见第六章）采取

倾向于零信任的方案解决网络安全问题。若机构已具备成熟的 ID 管理系统和强大的 CDM 能力，那么该机构正在朝着实施 ZTA 战略（参见 7.3 节）迈进。ZTA 缺口是对 ZTA 及其如何从之前的网络安全模式演进的错误看法导致的。

B.3 影响 ZTA 的系统性缺口

这些缺口会对 ZTA 战略的最初实施和部署以及持续运营/成熟度产生影响，减缓机构的 ZTA 战略的推行进度，造成 ZTA 组件产业的分裂。这些系统性缺口可通过采取开放性标准（标准制定组织或行业联盟制定）进行弥补。

B.3.3 组件之间接口的标准化

技术调查期间显示，没有任何一家厂商能提供一种支持零信任的方案。此外，采取一种厂商方案实现零信任且冒险拘泥于某一厂商，可能并不可取。这会导致各组件之间存在互联互通问题，并且该问题不仅在采购时存在而会持续存在。

在较庞大的零信任生态系统（ZTE）中，组件范围非常广泛，很多产品都专注于 ZTE 中的某一方面，依赖其他产品向其他组件（如集成资源访问的多因素认证（MFA））提供数据或服务。厂商通常依赖合作伙伴公司提供的专有 API，而非独立于厂商的非标准化 API 实现这种集成。这种方法的问题在于这些专有的 API 由单个供应商控制。一旦供应商更改 API 的行为，集成商需更新他们的产品。这就需要厂商群体进行密切合作，确保尽早通知可能影响产品之间的互通的 API 修改。这进一步增加了厂商和消费者的负担：若某个厂商对其专有 API 进行修改，厂商需投入资源对其产品进行修改，而且消费者需更新多个产品应用。此外，厂商应对每个合作伙伴的组件进行封装并对封装进行维护，实现最大化兼容和互联互通。例如，很多 MFA 产品厂商须对每个云提供商或身份识别系统进行个性化封装，以便将其用于各种不同的客户端组合中。

在客户方面，这会为拟定产品采购需求带来其他问题。采购商在确定产品兼容性时没有任何标准可参考，也就无法明确组件的最低兼容需求，很难制定多年的 ZTA 迁移路线图。

B.3.4 解决过度依赖专有 API 的新兴标准

由于没有任何一种方案可实现 ZTA 战略部署，也就没有任何一套工具或服务用于零信任架构。因此，企业无法采取某一种协议或框架迁移至 ZTA 战略。目前推出了多种模型和方案，试图在 ZTA 方面的树立权威。

这表明可开发一套开放的标准化协议（或框架），帮助组织迁移至 ZTA 战略。Internet 工程任务组（IETF）等标准开发组织（SDO）已提出了对威胁信息交换可能有用的协议（称为 XMPP-Grid）。云安全联盟（CSA）为软件定义边界（SDP）开发的框架可能在 ZTA 中也很有用。应投入精力对实施有用的 ZTA 战略来说非常必要的 ZTA 相关框架或协议的当前状态进行评估，明确要制定和改进这些规范需在哪些方面下功夫。

B.4 ZTA 的知识缺口与未来研究领域

此节列出的缺口并不妨碍组织为其企业采用 ZTA 战略。这些是关于 ZTA 运行环境知识的灰色区域，主要归因于在实现成熟的零信任部署方面缺乏时间和经验，这些是未来研究人员的研究方向。

B.4.5 攻击者对 ZTA 的反击

对于企业来说，正确实施 ZTA 战略相对于传统的基于网络边界的安全而言，会改善其网络安全态势。ZTA 的宗旨是减少对攻击者的资源暴露，并在主机系统失陷时尽量降低（或防止）企业内部的横向移动。

然而，顽固的攻击者不会坐视不管，而是在 ZTA 引入时会调整其行为。目前需要解决的问题时攻击将会作何调整。其中，由于 ZTA 的一个主要原则是在访问资源之前进行频繁的身份验证，因此旨在窃取凭证的攻击（例如网络钓鱼和社会工程）可能会变得更加普遍。此外，对于 ZTA 和现有方案并存的企业，攻击者将重点关注尚未应用 ZTA 原则的业务流程（即遵循传统的基于网络边界的安全）——实际是攻破容易下手的目标试图在 ZTA 业务流程中获得一些立足点。

随着 ZTA 逐渐成熟，其部署越来越广泛且积累了更多经验，ZTA 相对于基于网络边界安全的传统方法的有效性将会变得显而易见。此外，还需要制定 ZTA 与较老网络安全策略相比具备的“成功”指标。

B.4.6 ZTA 环境中的用户体验

目前尚未对采取 ZTA 战略的企业的最终用户反响进行严格审查。这主要是因为缺乏可供研究的大量 ZTA 用例。已有研究表明，用户对 MFA 和其他安全运营的反应作为 ZTA 企业战略的一部分。这项工作可作为采取 ZTA 工作流的企业中预测最终用户体验和行为的基础。

目前已就 ZTA 对最终用户体验的影响开展了一系列的研究，包括 MFA 在企业中的使用和“安全疲劳”。安全疲劳指最终用户面临的很多安全策略和挑战开始对其生产力产生负面影响的现象。一些研究表明，MFA 可能会改变用户行为，但总体变化是非常复杂的。一些用户很容易接受 MFA，若流程简化且涉及到他们习惯于使用或拥有的设备（例如，智能手机上的应用程序）。然而，有些用户不喜欢在业务流程中使用自己的设备，或者感到他们经常被监视是否违反了 IT 政策。

B.4.7 ZTA 对企业和网络中断的适应能力

ZTA 厂商生态系统的调查显示了企业部署 ZTA 战略需要考虑的各种基础设施。正如上述内容所示，没有一家提供商提供完善的零信任方案，这样企业就需采购多种不同的服务和产品，造成组件之间存在多种依赖关系。在这种情况下，一旦关键组件运行中断或无法连接，就会造成一系列的运行中断，影响一个或多个业务流程。

大多数被调查的产品和服务都依赖于云服务提供健壮性，但众所周知即使是云服务在遭遇攻击或出现简单错误也会变得不可用。当这种情况发生时，用于做出访问决策的关键组件可能会无法访问或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）攻击期间也许可供访问，但可能并非资源中的所有 PEP 都可访问。因此，我们需要研究如何发现 ZTA 部署模式可能存在的“瓶颈”以及 ZTA 组件不可访问或可访问性有限时对网络运行的影响。

采用 ZTA 战略时可能会对企业的运行连续性（COOP）计划进行调整。ZTA 战略简化了许多 COOP 因素，这是因为用户在远程情况下可能与在本地时具备相同的资源访问权限。然而，如果用户未接受适当培训而缺乏经验，像 MFA 这样的策略也可能产生负面影响。用户可能会在突发情况下忘记（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效率。

B.5 参考

[1] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Software Defined Perimeter Working Group “SDP Specification 1.0” Cloud Security Alliance. April 2014.

[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) Productivity and Usability Effects of Using a Two-Factor Security System. *SAIS 2009 Proceedings* (AIS, Charleston, SC), p 37. Available at http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)* (ACM, Orlando, FL), pp 212-224. https://doi.org/10.1145/3134600.3134629

安全加社区

公益译文项目

2020

小蜜蜂翻译公益译文项目，旨在分享国外先进网络安全理念、规划、框架、技术标准与实践，将网络安全战略性文档翻译为中文，为网络安全从业人员提供参考，促进国内安全组织在相关方面的思考和交流。

“安全加”社区

小蜜蜂公益翻译组