【ZTA 101】NIST SP 800-207

第一章：简介

在2020年8月，美国国家标准与技术研究院（NIST）公布了关于[零信任架构（**Zero Trust Architecture**，**ZTA**）的**SP 800-207**]，这是一个美国政府采用ZTA的重要参考标准文件，提供架构面的建议与实施概念，其目的是希望能帮助更多组织能够采用零信任架构并受益。

这份白皮书用了7大章节来介绍NIST所认为的零信任架构的基本内涵，同时，也让日后各界在探讨ZTA时，能够有一致、共通的语言来沟通。因此，我们将针对这份文件的一些重点做介绍，提供简体中文化的内容并补充相关概念信息，让国内对于网络安全零信任能有清楚的认识，同时我们也感谢台湾科技大学教授查士朝协助此系列内容的校正。

第一章：简介

第一章就是相关背景介绍，说明什么是“零信任”。

前两段主要说明一件事：在现今的复杂的企业环境之下，无论是BYOD、云端服务与远程工作等新兴访问方式，加上数字转型议题，都一再冲击着传统边界防护策略。因此，网络安全架构必须要有所改变。

毕竟，传统典型的企业网络基础架构变得日益复杂：例如，单一企业内部就有多个内部网络、远程办公室，并拥有本地端的基础设施，还有远程与个人移动应用，以及云端服务等。

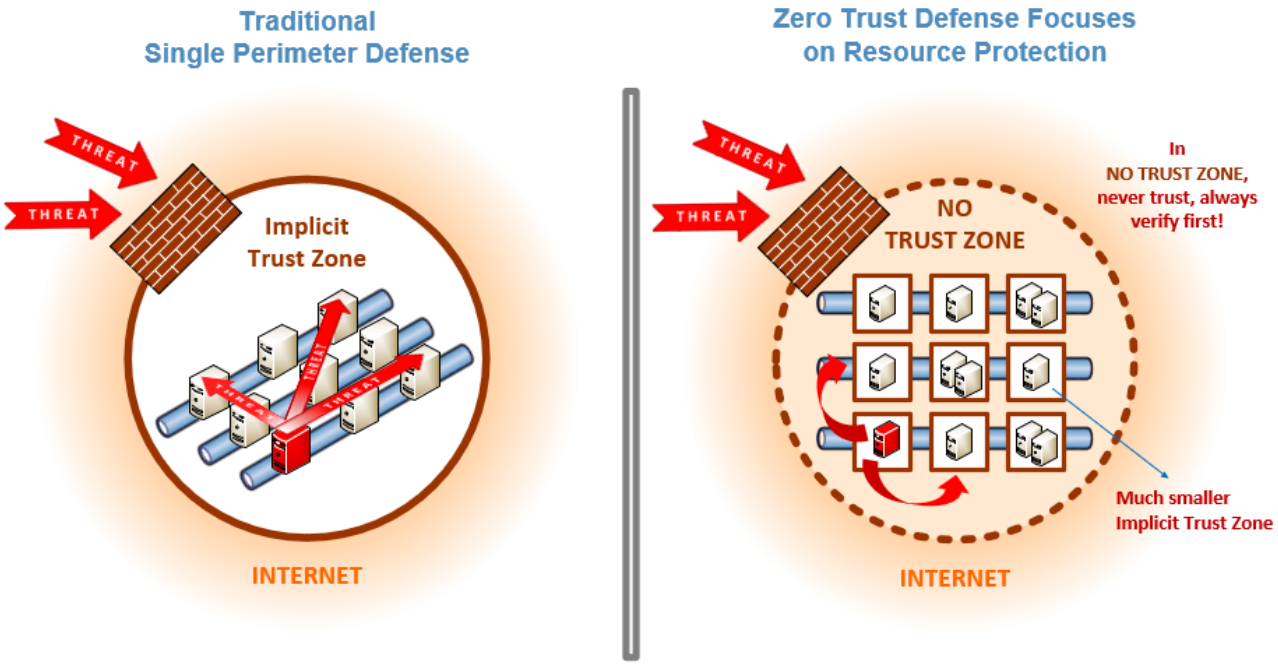
这样的复杂性，显然超越了传统网络边界安全的防护方法，因为，现在的企业网络边界相当难识别。而且，基于边界的网络安全防护也被证明是不够的，因为一旦攻击者突破了原本的边界防护，进入内网的横向移动就变得畅通无阻。

虽然这里NIST没有举例说明，不过从现实世界来看，黑客入侵与数据泄露事件不断，而过往大家也已听过很多这样的事件。例如，黑客一旦窃取企业组织的VPN帐密或凭证，往往就能轻易突破目标的内网防护，而进入内网后就有可能攻击重要系统而传播勒索病毒或是窃取重要数据。因此，对于复杂企业环境而言，需要新型网络安全的模型，也就是“零信任”。

或许，有人对于NIST 800-207中谈及的企业网络安全架构，并不是那么清楚，其实我们看到资安界已有很多比喻与说明，也在此一并补充。

例如，以往的网络安全是怎么做？基本上，企业的网络安全是通过边界防护概念而形成，具象化一点来形容，就如同石墙、护城河与城门保护的堡垒概念，保护着企业内部的数据，避免受到恶意攻击，这是因为当时的基本假设是，在堡垒内的活动是相对安全的，也就是企业边界内部的资源都是可信任的概念。

但是，这种边界防护的方法，其实存在着严重的限制。例如，随着BYOD与云端服务的兴起，这些都不是原先边界防护策略会面临的状况，而这些新兴访问方式，也让企业需要设法通过不同解决方案去应对，除此之外，还有远程访问、数字转型的需求存在，再加上这两年疫情下大幅带动了远程工作，在这些种种原因之下，都让企业对于网络边界防护变得更加困难。



> 此外，美国国家网络安全卓越中心（*NCCoE*）资安工程师与项目经理*Alper Kerman*，也曾用一张简单的图表，说明零信任架构网络安全策略与传统边界网络防护策略的区别，就是不再有信任的内部网络。图片来源：*NIST:零信任网络安全 (A. Kerman/NIST)*

接下来，NIST介绍了所谓的零信任方法，主要的面向就是数据保护，但也应该延伸到包含：

- 所有企业资产（实体资安设备、基础架构组件、应用程序、虚拟以及云端组件）
- 主体（来自终端用户、应用程序及非用户操作的资源请求信息）

这里强调的重点在于，我们要假设环境中存在攻击者，而且企业环境与任何非企业环境都该是一样，不值得信赖。

换言之，现在所谈的零信任，是将原本的信任视为弱点。而在一个零信任架构中，不再是建构出可被信任的网络，取而代之的是，消除了信任这个概念。毕竟，现在企业环境其实分散各地，不该再以内部或外部来区分。

因此，NIST明确指出，在零信任安全模型中，企业不能再有隐性的信任，对于内部资产和业务功能的风险，必须经过不断地分析与评估，并且制定防护措施来缓解这些风险。

在零信任中，这些防护措施通常要尽可能减少对资源（如数据、运算资源与应用程序/服务）的访问，只允许那些被确定为需要访问的用户与资产访问，并对考量访问请求的身份和安全态势，进行持续的身份识别与授权。

关于零信任架构，NIST先简单介绍其特性，后面的章节还会再细谈。

基本上，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，目的是要尽可能去防止数据泄露与限制内部横向移动。而为了帮助实现，因此这里将谈论到的内容包括：ZTA的定义、逻辑组件、可能的部署场景和威胁，希望为组织提供零信任网络架构设计方法、以及迁移过程的总体路线图，同时也讨论了可能影响零信任架构的相关联邦政策。

NIST强调，零信任（ZT）不是单一的架构，而是一套关于工作流程与系统设计运营的指导原则，其用途就是可改善任何机密分类或敏感数据层级的安全现状。

特别的是，朝向ZTA网络安全迈进之际，企业与组织可要先有心理准备。因为，朝向ZTA过渡是一段漫长过程，需要持续的技术革新才能实现，而过渡到ZTA也是组织评估其任务中分享的过程，并不只是全面技术替换。NIST继续说明：其实现在企业的IT基础架构中，就已经有ZTA元素，组织对于零信任原则与流程上的变动，应该要逐步实施，并采用保护数据资产与业务功能的技术解决方案。因此，迈向零信任网络安全策略的期间，大多数企业应该都是同时以零信任与以传统边界模式的方式来进行，通过持续投资以改善。

而为了要让零信任能有效运行，组织必须要全面考量信息安全并灵活实践。当与现有的网络安全政策和指南、身份和访问控制管理、持续监控和最佳实践相平衡时，ZTA可以通过使用风险管理方法来防范常见威胁并改善组织的安全状况。

综合而言，我们可以了解到：零信任网络安全，或是简称的零信任、零信任模型、零信任架构，谈的就是一种企业网络安全的方法。

另外，我们要补充的是，由于零信任一词在字面上容易造成误解，因此在含义上要能够澄清：关于这里的零信任一词，网络安全是一大前提。但在普遍情境下的直接联想，只说零信任，有人可能只想到“默认都不信任”，此假设不仅是在网络安全领域，在许多不同资安领域或构面中，常常也都隐含这样的概念。最简单的例子，以白名单机制而言，就是除了白名单上列出的标的外，默认都不允许访问。这部分的道理是相通的，还有许多情境也都是如此。但网络安全零信任包含的内涵不仅于此，也因此，普遍大众首次听到零信任一词，每个人想象到的轮廓可能不同，就容易搞混。而且，零信任的概念与精神，也会延伸套用到许多资安领域与场景。

网络安全零信任发展至今，对应的是传统边界防护策略，概念是不因内网或外网而有信任或不信任，当中并具有相当多的内涵，包括：从默认都不信任出发，以及持续验证、动态评估等，架构面还需具备零信任的原则、核心组件与必要技术等。

第一章第一节：联邦机构致力于零信任的历史

在这一章节中，主要说明的是与美国联邦机构有关的零信任发展历史。当中重点包括：

关于ZT一词，美国国防部旗下国防信息系统局（Defense Information Systems Agency，DISA）之前已经提出，理念是由传统基于边界的传统防御模式，进化到每次访问请求都要检查的架构概念。

对于NIST本身，早在2018年发布的NIST网络安全框架（Cybersecurity Framework），已在实施层级之中提到零信任安全模型。

而白皮书所讲的内容背景，源自于美国白宫在2019年发布的联邦政府数据战略（Federal Data Strategy），该战略要求美国政府对其数据采取更具现代化、更加开放与更加隐私保护的措施，并且结合创新的管理技术（例如：微分隐私）以达到安全目标。而零信任理念，也正是其中的关键之一。此战略的目标，就是要让联邦机构能更好地保护数据、降低网络攻击风险，并确保数据安全和隐私的管理。

其实，联邦机构对零信任的探索，并不是一朝一夕的。早在2018年，美国联邦首席信息官（Federal CIO）就已提出相关建议，强调了企业架构视角下的零信任概念，而美国国防部则在其2018年的“云计算策略”中也提到了零信任方法的采用。

而如今，这份SP 800-207指南，正式确立了ZTA的定义，并为如何实施与设计提供了详细的指南。

第一章第二节：介绍此文件的结构

此章节的作用，主要是公布后续章节的内容简介。

第二章 定义ZTA、列出设计ZTA企业网络的一些网络架设，同时介绍设计零信任架构的原则。

第三章 将零信任逻辑元件内容文件标准化，并且提到不同ZTA元件组合且提供相同逻辑功能的各种独特实践方式。

第四章 列出通过ZTA使企业网络更加安全的使用案例，包括远距办公、云端服务与访客访问等企业场景。

第五章 讨论采用ZTA网络安全策略之下，企业可能面临的威胁。

第六章 讨论ZTA原则如何与美国政府联邦现有指南结合呼应。

第七章 说明企业可以如何朝向ZTA过渡。

第二章 零信任基础认知

在第二章开头的第一句话中，强调了零信任是一种网络安全范例，聚焦于资源保护，并指出信任的前提在于持续评估而不是隐性授予权限。

这里说明了不少零信任的基础认知，例如，零信任架构可以实现端到端的企业资源与数据安全，方法包括：身份、账户和凭证管理、访问管理，以及操作、端点、托管环境与互联基础设施等。最初的重点应放在限制资源的访问，只有需要访问的人才能访问该资源，并且仅给予执行任务所需的最低权限。

同时，这里提出了对零信任与零信任架构的有效定义：

零信任（*Zero Trust*）是面向信息系统与服务在被视为已被入侵的网络环境中运行时，为了让每个访问请求决定的不确定性最小化，并在执行准确且最小权限下运行，所提供的一系列概念与想法。

就零信任架构（*Zero Trust Architecture*）而言，这是一种企业网络安全计划，其中利用了零信任概念，包括元件关系、工作流程规划与访问政策。

对于整个网络安全策略而言，当企业决定采用零信任作为网络安全核心战略，就需要根据零信任原则来制定计划，以产生零信任架构。之后，需要部署与打造零信任环境，让企业使用。

值得关注的是，这里说明了零信任所要解决的问题症结：第一，防止未经授权访问数据与服务；第二，使访问控制尽可能做到更精细。

因此，这里谈到零信任架构的目的，是要让未经授权访问的风险降到最低。

也就是说，只让经过授权与允许的主体可以访问数据，而不让攻击者等其他主体能访问。而这里的主体，包括用户、应用程序或服务，以及设备。

进一步而言，在零信任（ZT）与零信任架构（ZTA）所指的资源访问，不仅包含数据访问，也包含如打印机、计算资源与物联网设备等。

该如何判断是否允许访问？以及该如何做到访问控制细化？这里先从基本概念开始说起，同时借由一个简要的访问模型，让外界可以更容易理解。

由于访问控制有其不确定性，因此访问决策的重点将放在身份验证、授权与限制默示信任区域。同时，需要尽可能减少身份验证机制的时间延迟，以保持可用性，并尽可能让访问规则更精细，让每次资源访问请求的操作，只提供所需的最小权限。

关于访问模型的概念，NIST绘制了图1（如下图）来说明：当用户或机器需要访问企业资源时，需要经过政策落实点（Policy Enforcement Point，PEP）进行把关，并由相应的政策决策点（Policy Decision Point，PDP）来决定权限。

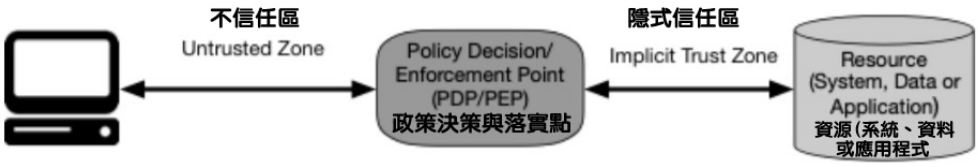


Figure 1: Zero Trust Access

以上图为例，系统必须确保左边的主体是真实的，以及请求是有效的，而中间的政策决策点（PDP）与政策落实点（PEP）需提供适当的判断，允许主体访问资源。

在此当中，将考虑主体身份的信任程度，如请求设备的安全现况等各种因素。

同时，这里也提到PDP/PEP的重要性，因为在PDP/PEP与资源之间，将会形成默示信任区（Implicit Trust Zone）。在NIST的解释中，这如同机场航站位于登机区的概念，通过机场安全检查站（PDP/PEP）进入登机口的人员与旅客，将被视为是可信的。

综合来说，如何让PDP/PEP做到严谨的决策，就需要通过实时且基于风险评估的结果，给出适当的判断，以决定是否能够访问。

换言之，企业需要为资源访问，制定与维护一个基于风险的动态政策，并建立一个这样的系统，以确保每次的资源访问请求，都能通过这个动态政策来执行。**NIST**也强调，为了使**PDP/PEP**尽可能具体明确，隐式信任区必须尽可能小。

整体而言，零信任提供了一套原则与概念，并围绕在让PDP/PEP与资源更靠近，其想法是对企业所有主体、资产与工作流程，都做到明确的验证与授权。

第二章 第一节 零信任原则

有了零信任基本认知后，接下来就是理解零信任的原则。这部分的重点是具体描绘出零信任架构（ZTA）的设计与部署所需遵循的基本原则，也可以说是ZTA的精神，或者是信念、信条。

基本上，这些原则尽可能与技术无关，NIST共统整出7项：

1. 所有的数据来源与运算服务，都要被当作是资源。
2. 无论与哪个网络位置的设备通信，都需确保安全。
3. 对于个别企业资源的访问要求，应以连接为基础判断是否允许。

4. 对资源的访问需要有动态政策来决定，包括基于客户端识别、应用服务，以及要求访问资产可观察到的状态，可能还包括其他行为或环境属性。
5. 企业对于所有自有与相关的资产，需监控与衡量其完整性与安全状况。
6. 在允许访问之前，所有资源的身份鉴别与授权机制，都要依监控结果动态决定，并且严格落实。
7. 企业应该尽可能收集有关资产、网络基础架构与通信的现况信息，并用这些信息来增强安全状态。

关于上述零信任所需遵循的原则，简单来说，网络上每个服务与可被访问的设备，都应被视为资源并要管控其访问，且所有通信都需要确保安全。

对资源的访问请求，是要基于每次连接请求来进行，并要先评估请求者的可信度，以及仅给予完成任务所需的最低权限。在此过程中，需要建立相关系统来监控与评估资产的安全状况，并要有动态政策来判断是否能够访问。

因此，这将是获得访问权限、扫描、威胁评估、适应与不断重新评估的持续循环，并依照每次监控结果来动态决定是否允许访问。也就是说，企业必须要有身份凭证与访问管理（ICAM）系统，以及资产管理系统，其中包括多因素身份验证（MFA）的采用，而在访问管控策略的定义与执行上，将包含基于时间的因素，以及新资源的请求、资源修改、检测到的异常活动等。这样的策略需要在安全性、可用性与成本效益上取得平衡。

此外，为了支持动态政策，以做到更细致的访问控制，需要尽可能从外部收集信息来改进政策。

第二章 第二节 零信任视角下的网络

在阐述零信任原则之后，NIST列出零信任角度下对于网络的六大假设。换言之，这其实是指出ZTA将建立在相关假设前提之下。包括：

1. 企业私有网络不能预设为信任的区域。
2. 网络中的设备可能不是企业所有，也不能被企业设置。
3. 没有资源是原本就可信赖。
4. 并非所有企业资源都位于企业拥有的基础架构上。
5. 远程用户访问企业主体与资产时，不能完全信赖自身的网络。
6. 在企业与非企业基础建设之间移动的资产与工作流程，应具有一致的安全政策与安全状态。

从上述假设来看，我们可以了解到一些观念：必须设想攻击者存在于企业网络中。因此要以尽可能安全与可行的方式进行沟通，这将需要对所有连接做鉴别，并加密所有流量。

有些假设也与上述原则呼应，例如，没有资源是原本就可信赖的，因此在访问企业拥有的资源之前，每个资产都必须经过PEP评估其安全状况，确保所有设备尽可能是在最安全的状态。

最后，也必须考虑企业环境的复杂性，像是并非所有设备都是企业所拥有，资源也不都是在自己拥有的基础建设上，以及企业不同据点的连接，资产与工作流程的迁移等。

第三章：零信任逻辑元件

在理解了零信任的基础认知与原则后，接下来NIST进一步阐述了零信任架构的核心元件与构成，以便让外界具体了解其运作方式。

NIST指出，企业ZTA的部署是由许多逻辑元件所构成，这些元件可以是本地端的服务，也可以是云端服务。而各元件间可能有其关联。

这里也具体描绘了ZTA核心逻辑元件的架构图（如图2），以便更清楚地呈现ZTA核心元件彼此的关系，也让外界可以更明白如何实现零信任架构。NIST提醒，这只是一个理想的模型架构。
零信任架构核心元件

在前一章节的图1中，我们可以大致理解存取模型的重要核心，即PDP/PEP，也就是政策决策点与政策落实点。

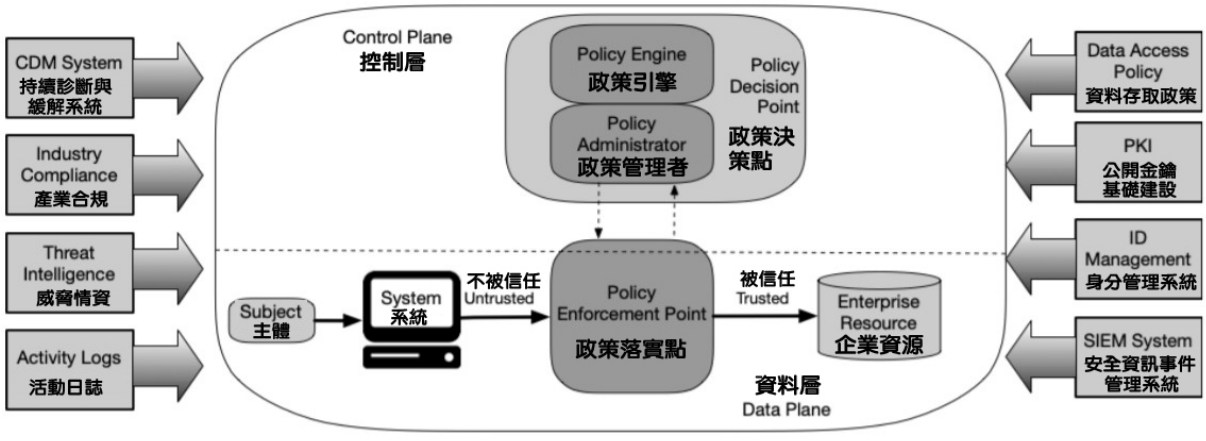


Figure 2: Core Zero Trust Logical Components

上图呈现了零信任逻辑元件的核心架构，在此当中，NIST对这个PDP/PEP做出了更深入的解析。

基本上，当任何主体通过系统要访问企业资源前，需经过存取控制的政策落实点（PEP），以决定是否给予权限，这样的动作发生在网络环境的数据层（Data Plane）。

而在PEP的背后，将通过控制层的相应政策决策点（PDP）来判断。PDP是由两个逻辑元件配对构成，包括政策引擎（Policy Engine, PE）与政策管理者（Policy Administrator, PA）。

其中，政策引擎（PE）负责决定是否给予资源访问权限。当PE做出允许或拒绝的决策时，将由政策管理者（PA）执行决策。

简言之，PE负责运算，而判断的依据则来自两方面：一是企业政策，另一是外部信息，例如CDM系统与威胁情报等。

政策引擎（PE）的运作

在决策过程中，政策引擎不仅依据企业制定的资料访问政策，同时也引入多方外部信息作为考量因素，进行基于风险的评分决策运算，实现即时调整控制权限。

NIST列出了8种信息来源以帮助PE进行更好的访问控制动态决策，包括：

1.美国政府推动的持续诊断与缓解（CDM）系统
2.产业合规系统
3.威胁情报
4.网络与系统的活动日志
5.资料访问政策
6.企业公开密钥基础设施（PKI）
7.身份管理系统
8.安全事件信息管理系统（SIEM）

政策管理者（PA）的角色

政策管理者（PA）负责执行政策引擎的决策。具体而言，PA负责建立或关闭主体与资源之间的通信路径，并生成客户端访问企业资源时所需的身份验证、验证Token或凭证。

简言之，当PE允许时，PA设置PEP允许Session连接；反之，当PE拒绝时，PA向PEP发出信号关闭连接。这些过程都在控制层进行。

政策落实点（PEP）的组成

对于PEP的组成形式，NIST表示，PEP本身也可能分为两个不同的元件，像是以客户端与资源端的形式呈现。例如，PEP可分成两部分，一是笔电上的代理程序，另一是资源前面的访问控制网络闸道元件。

通过上述逻辑元件的解析，我们可以更加深入地了解零信任架构的具体实现方式，以及各个元件在ZTA中的角色和作用。

第三章第一节：不同的零信任架构方法

接下来，NIST说明了零信任逻辑元件的组成方式有很多种，并指出企业组织可通过多种方式为工作流程制定ZTA，只要每种方法都符合全部的零信任原则。这其实也呼应了第一章中所强调的：“零信任（ZT）不是单一的架构”。

特别值得关注的是，这里探讨了ZTA所必需的三个重要关键技术。NIST指出，一个完整的零信任解决方案具备3项要素，包括：先进的身份治理（Enhanced Identity Governance）、网络微分割（Micro-Segmentation），以及软件定义边界（Software Defined Perimeters）。

针对这三项关键技术，NIST有简单的说明。例如，关于先进身份治理的方法，可与资源入口部署的模型（稍后会提到）有很好的配合；使用网络微分割的零信任架构，企业可通过智能交换机、次世代防火墙或特定用途的网络网关器，用以作为PEP，以保护每个资源或相关小组资源；而使用网络基础架构与软件定义边界的零信任架构，在此方法中，PA可作为网络控制器，根据PE所做的决策，以重新建立或配置网络。

对于上述提到的各种不同方法，NIST认为，当企业组织在设计零信任架构时，可能发现某些方法比其他方法适合，这并不表示其他方法不管用，只是意味着其他方法更难执行，可能需要针对现行业务流程进行根本上的改变。

第三章第二节：部署方式的抽象架构

在部署方式上，由于每个公司与组织的环境不同，因此NIST指出，根据企业网络的建立方式，以及企业中的不同业务流程，可使用多个ZTA部署模型。

对于ZTA部署模型，NIST这里简要提出4种情境，分别是：

- （一）装置基于代理/网关的部署

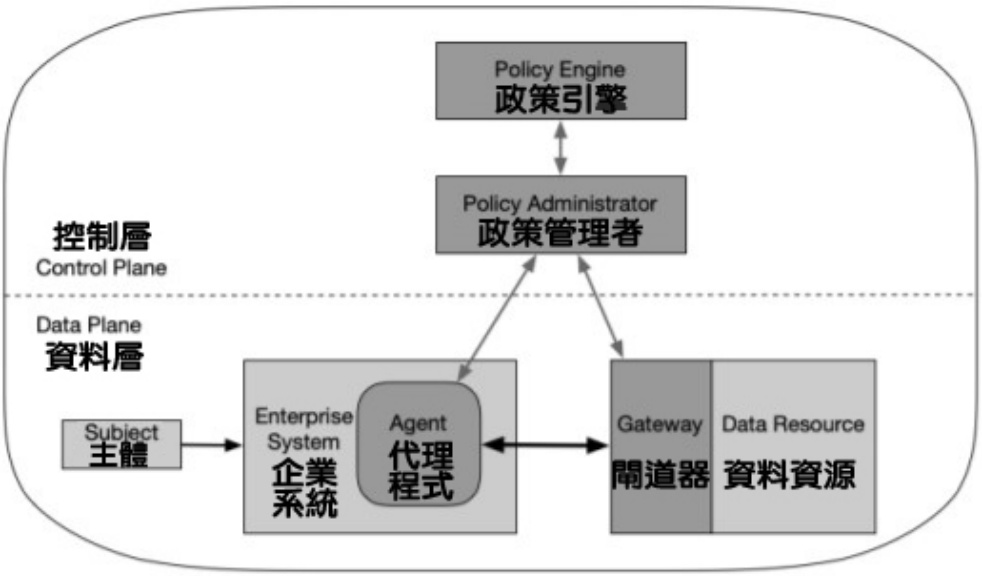


Figure 3: Device Agent/Gateway Model

- （二）基于Enclave区域的部署

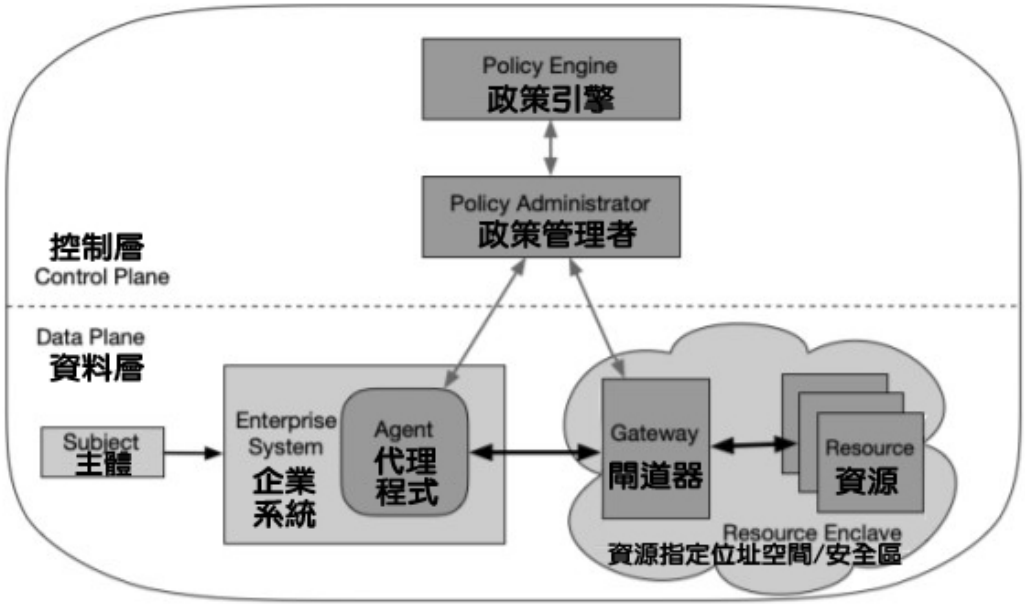


Figure 4: Enclave Gateway Model

- （三）基于资源入口的部署

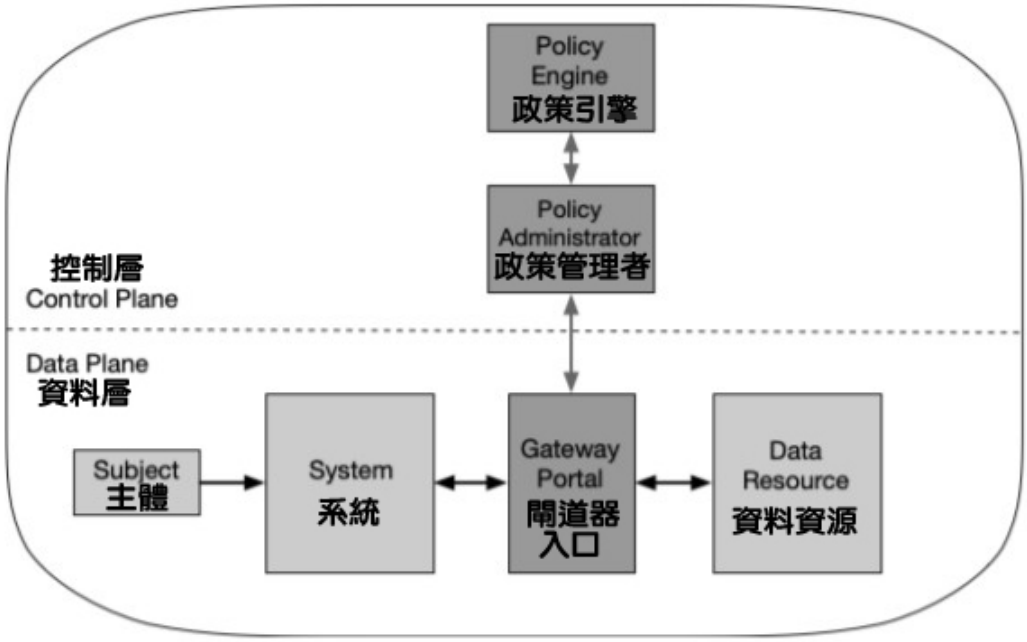


Figure 5: Resource Portal Model

- （四）装置应用程序沙箱

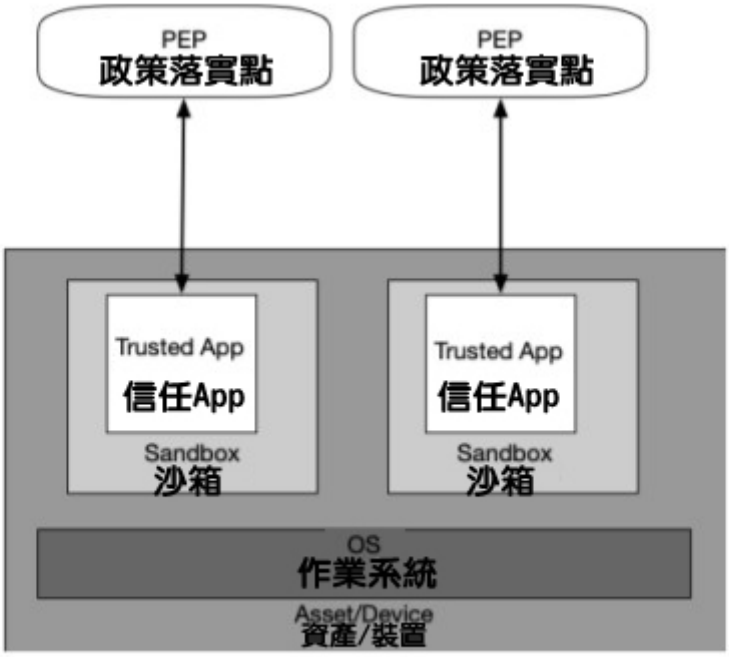


Figure 6: Application Sandboxes

简单来说，前两种是基于代理程序（Agent）的模式。第一种是访问每个资源时，经过单独的网络网关器，第二种是将很多资源部署在同个网段，访问这些资源时，将经过同一个网络网关器；后两种则是没有Agent的模式，第三种是经过网页入口，第四种则是通过沙箱。

NIST同时也提到一些注意事项或优缺点，例如，第三种基于网页入口的部署方式，可能要注意浏览器隔离与DoS防护。第四种沙箱方式需确保每个应用程序沙箱的安全等等。

第三章第三节：信任算法

在第二章提到，企业需要为资源访问制定和维护基于风险的动态策略。在本章的前半部分，也指出了 Zero Trust Architecture（ZTA）逻辑组件的组成。在决策点背后的访问决策点（PEP）中的访问评估（PE）是负责运算的元件，是最终决定是否授予资源访问权限的元件。这样的过程实际上是对访问请求进行风险分析。

关于存在策略引擎（PE）中的信任算法（Trust Algorithm），NIST提出了更多的说明与探讨。内容涵盖了两个方面：一方面是关于决策所需的多方信息来源，另一方面是决策所需的算法方式。

NIST使用了简单的比喻来说明，对于部署 ZTA 的企业而言，PE 可视为大脑，信任算法可视为思考过程。就像人脑一样，会通过综合考虑许多信息并做出决定。因此，PE 需要接收多方信息来做出决策。

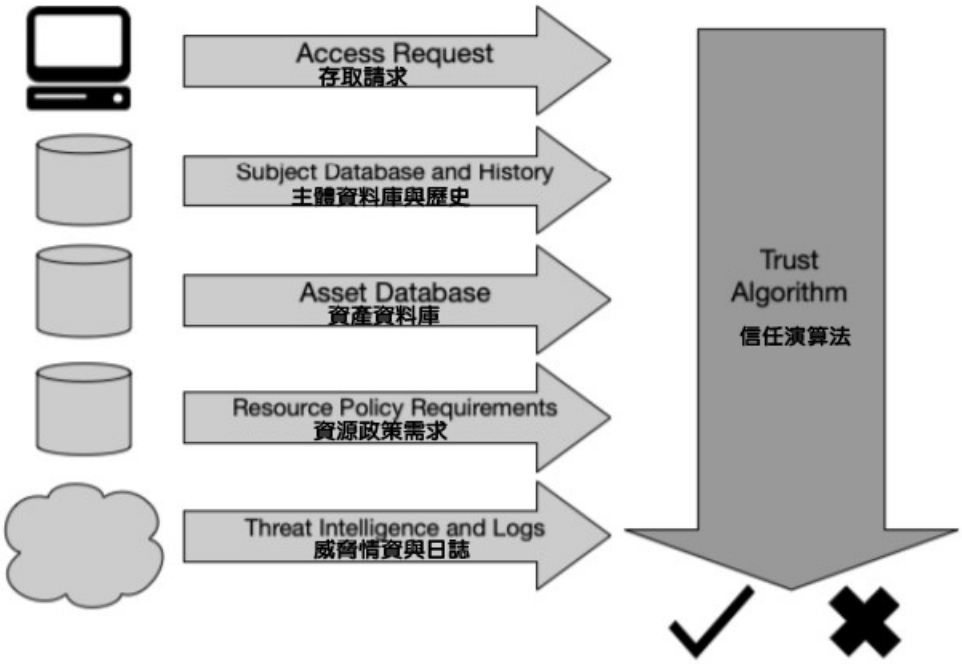


Figure 7: Trust Algorithm Input

特别的是，这里重新将信息归纳为5大类别，分别是访问请求、主体数据库与主体历史行为记录、资产数据库、资源策略需求，以及威胁情报与日志。

NIST 也做了一些解释，例如，在访问请求的类别中，包括操作系统版本、使用的软件，以及更新修补的水平，将根据这些因素与资产安全现状进行评估。

基本上，PE 所依赖的就是信任算法。至于每个数据来源的重要性与权重，将根据专有的算法或企业设置的标准进行。当然，这些权重将反映数据来源对企业的重要性。

更进一步，这里还探讨了不同的信任算法规则，因为实施 ZTA 信任算法的方法可以有很多种。不同的 ZTA 设计者，对于各因素的重要性，可能会希望有不同的权衡。因此，这里将信任算法规则区分出两种类型：

一种是基于条件与基于分数的方法；另一种是根据单一与上下文的方法。前者是每次都会独立评估，后者则是会评估历史记录，将比单一信任算法规则更能检测到异常访问行为。

同时，这些算法方式可以搭配使用，例如，基于分数与上下文的方法，将可提供更动态与更精细的访问控制能力。

这其实相当于 NIST 已经给出了建议，但是，这里 NIST 在此还提供了更务实的见解。

理想上，ZTA 的信任算法应该都要是上下文的方式，不过，可能受限于当前企业采用的基础设施元件，而不一定能行得通。

因此，在定义与实现信任算法时，最重要的是，必须从安全性、易用性与成本效益来考量，再逐步朝目标迈进，因为，上下文的方式将能让潜伏公司内部攻击者的风险减到最低。

最后 NIST 表示，要为每个资源开发一套标准或权重值，需要经过规划与测试。在实际部署过程中，企业可能遇到问题，例如因为配置错误导致原本该允许的访问被拒绝，因此企业在部署初期会经过优化的阶段，调整标准或权重，以确保政策执行下，同时企业业务流程可正常运作，至于优化阶段需要经历多长时间，将取决于企业对于错误允许或拒绝的容忍度。

第三章第四节：网络 / 环境元件

普遍而言，网络设备可分为控制层（Control Plane）与数据层（Data Plane）。在此章节最初有简单提到，而这里对于网络环境有更多说明。

在零信任环境中，控制层将与数据层是分开的，逻辑上或可能是物理上的分离。这方面，与软件定义网络（SDN）所谈的概念相同。

在 ZTA 中，PA 与 PEP 就是在控制层建立主体与企业资源之间的通讯，而应用程序或服务工作负载将使用建立的数据层路径。

构建 ZTA 的网络需求是什么？这里共列出10项：

一、企业资产需要基础的网络连接。（包含LAN与DNS等。）

二、企业必须要能够区分资产是自己拥有还是企业代管，并能识别设备的安全现状。

三、企业要能监控内部网络流量。（从连接中，依照数据的描述（或 metadata），取筛出目的、时间等所需数据，以便动态决定权限）

四、所有企业资源不应在没有PEP访问控制下被获取。（这也使相关网络扫描或攻击都不会直接接触到资源）

五、ZTA 中的数据层与控制层是逻辑上分开的。（因此在控制层的 PE、PA 与 PEP 的通讯，不会存取到企业资产与资源）

六、企业资产可以接触到 PEP 元件。（企业主体必须透过 PEP 元件才能存取资源）

七、作为业务流程的一部分，PEP 是唯一可存取 PA 的元件。

八、远距企业资产应能访问企业资源，且无需经过企业网络架构。（例如，不应要求远距主体透过 VPN 来访问企业采用的公有云电子邮件服务。）

九、提供 ZTA 存取决策流程所需的基础架构，应具有可扩展性，以因应流程负载的变化。（在 ZTA 中使用的 PE、PA、PEP 是任何业务流程中都需要的关键元件，因此延迟、问题，或弹性扩增，都需有所考量。）

十、由于政策或可见的因素，企业资产可能无法连接到 PEP。（例如，可能有一项政策是规定，如果请求的资产位于企业之外，将无法访问到某些资源）

第四章　ZTA部署场景与使用案例

基本上，任何企业网络环境都可采取基于零信任原则设计。NIST指出，事实上，大多数的企业组织基础架构已具备零信任的某些要素，或是透过各种最佳资安实践做法来达到零信任。

接下来，这里将通过5个小章节，以说明不同的部署情境与使用案例。但要注意的是，在企业实际迈向ZTA的过程中，应该会是基于传统边界防护或与零信任架构并存，且会持续运行一段时间的状态。

第四章第一节　拥有卫星工厂的企业

第一种类型，就是拥有卫星工厂的企业。

这是大多数企业的场景，企业拥有一个总部以及多个分散不同地理位置的据点，这些据点并不与企业实体网络相连，而这些员工在工作上仍有需求要存取企业资源，因此，普遍会依赖电信服务供应商提供的专线，通过MPLS（Multiprotocol Label Switching）来连接这些据点，以建立安全连接。

基本上，企业可能因为没有足够的带宽，因此不希望云服务的流量经过公司总部网络，员工也希望可以通过企业或个人设备，实现远程存取。在此情形下，企业希望提供用户某些资源的存取权限，包括员工日历、邮件等，同时也要拒绝用户存取更敏感的数据，包括HR人力资源的数据库。

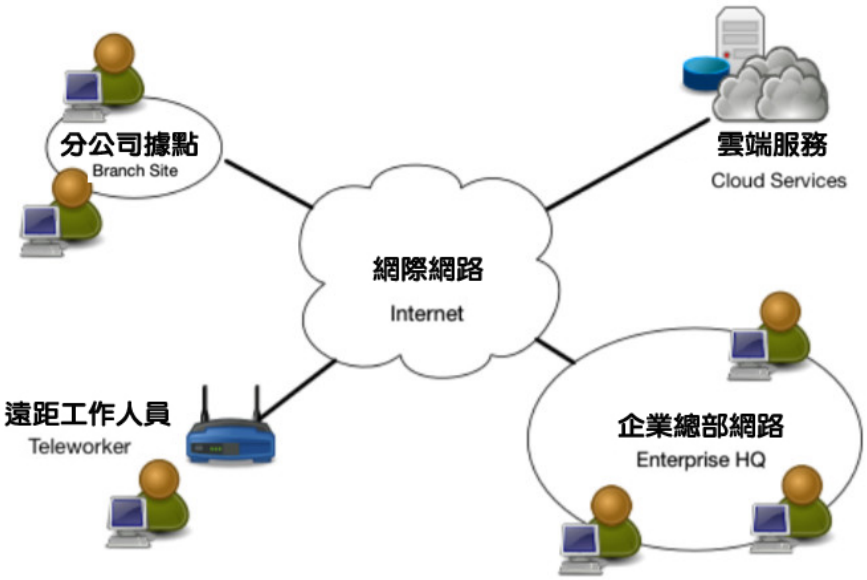


Figure 8: Enterprise with Remote Employees

在这样的场景中，策略引擎（PE）/ 策略管理器（PA）通常以云端服务方式来托管，具有更高的可用性，远程工作也不需要经过企业基础设施来存取云端信息。

而用户端将需要安装代理程序，或是通过网页入口进而存取资源，这部分在第三章第一节已有提到。

基本上，企业不用将策略引擎（PE）/ 策略管理器（PA）设置于企业本地网络环境，否则远程办公室的人员还要经由企业网络才能存取云端服务上的应用，响应上可能就不是那么迅速。

第四章第二节　使用多种云端服务的企业

第二种类型，是使用多种云端服务或云端对云端的企业，而使用多个云服务商的企业也是日益常见的场景。

在此种案例导入ZTA时，企业本身用有自己的本地端网络，并使用多个云端服务提供商托管应用程序、服务与数据，而且，有时应用服务与数据是托管在不同的云端服务上。而为了效能与便于管理，在A云端平台的应用程序应能直接连到B云端平台的数据来源，而不是强制应用程序存取须经由企业网络。

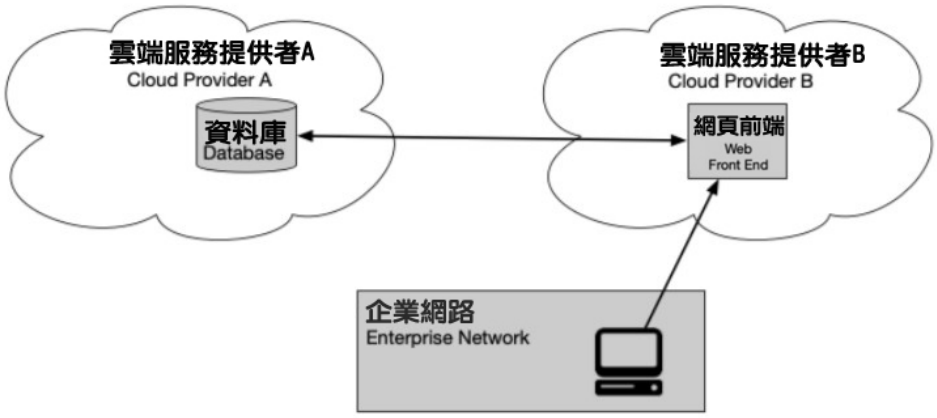


Figure 9: Multi-cloud Use Case

在这样的场景中，以多云环境使用的零信任方法而言，是在每个应用程序／服务与数据来源都设置策略落实点（PEPs）。

基本上，策略引擎（PE）与策略管理器（PA）可以位于云端或是第三方云端服务供应商，安装代理程序或经由网页入口的用户端，将能直接存取策略落实点（PEPs），如此一来，企业仍然可以管理资源的存取。

不过，这里有一个挑战，不同的云端平台提供商会有各自独特的方式，来实践类似的功能。因此，企业架构师需懂得利用各业者的机制才能实现企业ZTA。

第四章第三节　拥有外包与非员工存取的企业

第三种类型是另一种普遍常见的情境，与企业合作的驻点工作者或外包服务提供商需要有限的权限以存取企业资源。

例如，一家企业拥有内部的应用程序／服务、数据库与资产，其中包括偶尔在现场提供维护的外包供应商服务，比如由外部供应商拥有与管理的智能空调、照明系统，而这些人员将需要连接网络来进行他们的工作。在零信任的企业环境中，将能够遮蔽企业资源，并允许这些设备与技术人员存取互联网。

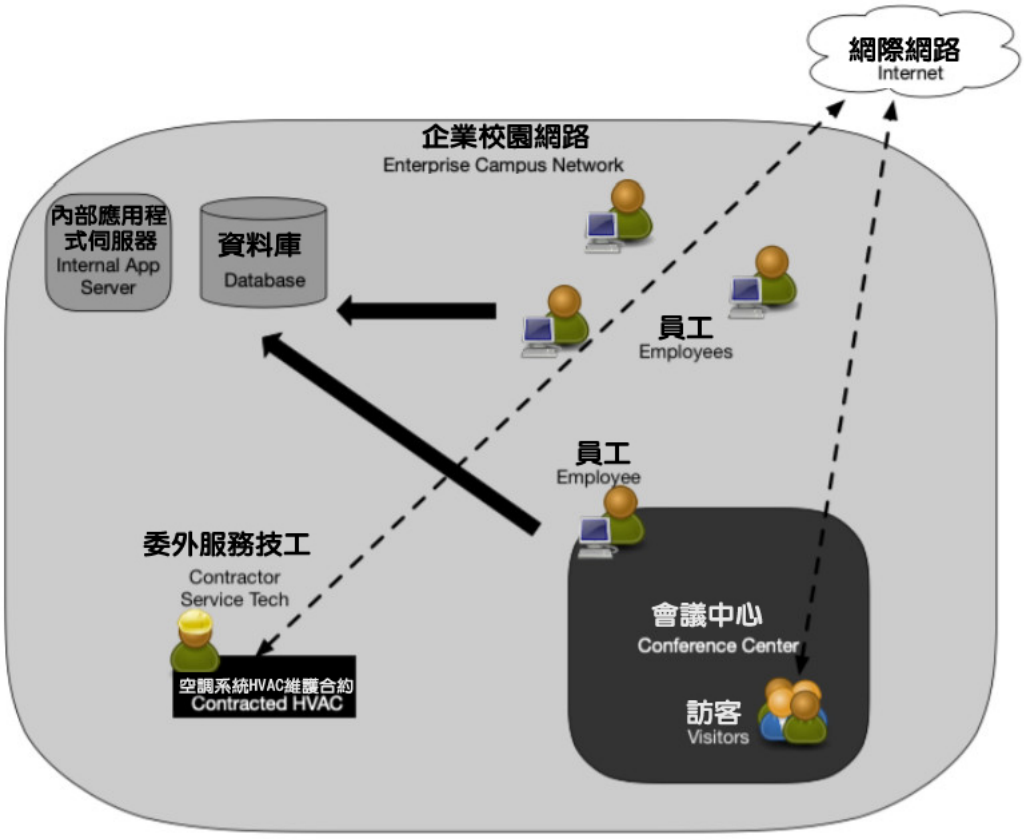


Figure 10: Enterprise with Nonemployee Access

在这个例子中，企业还有一个供访客与员工互动的会议中心。同样地，在零信任架构的软件定义边界方法中，员工设备与主体是有区别的，并且可能有能力以适当方式存取企业资源。例如，进入校园的访客可以存取互联网，但不能存取企业资源，甚至无法通过网络扫描发现企业服务。

在此场景下，策略引擎（PEs）与策略管理器（PAs）可以托管在云端服务，如果很少使用云的话或也能设置于区域网络LAN上。企业资产同样可以安装代理程序或经过网页入口存取，在此当中，策略管理器（PA）须确保所有非企业系统，也就是没有安装代理程序或连到网页入口的系统，不能存取本地资源，但可以存取互联网。

第四章第四节 跨企业边界协作的企业

第四种类型属于跨企业间的协作。例如，涉及A公司与B公司的项目。这两个企业可以是独立的联邦机构（G2G），也可以是联邦机构与民间企业。例如，A公司运营的项目数据库必须让B公司的员工存取。

在这种情况下，企业A可以设立专用帐户，供企业B员工存取需要的数据，并拒绝存取其他所有资源。但是，这种做法很快就会变得难以管控。如果企业双方建立联合身份识别管理系统，提供双方组织可使用的策略执行点（PEP）以进行认证，可以更快速地建立起关系。

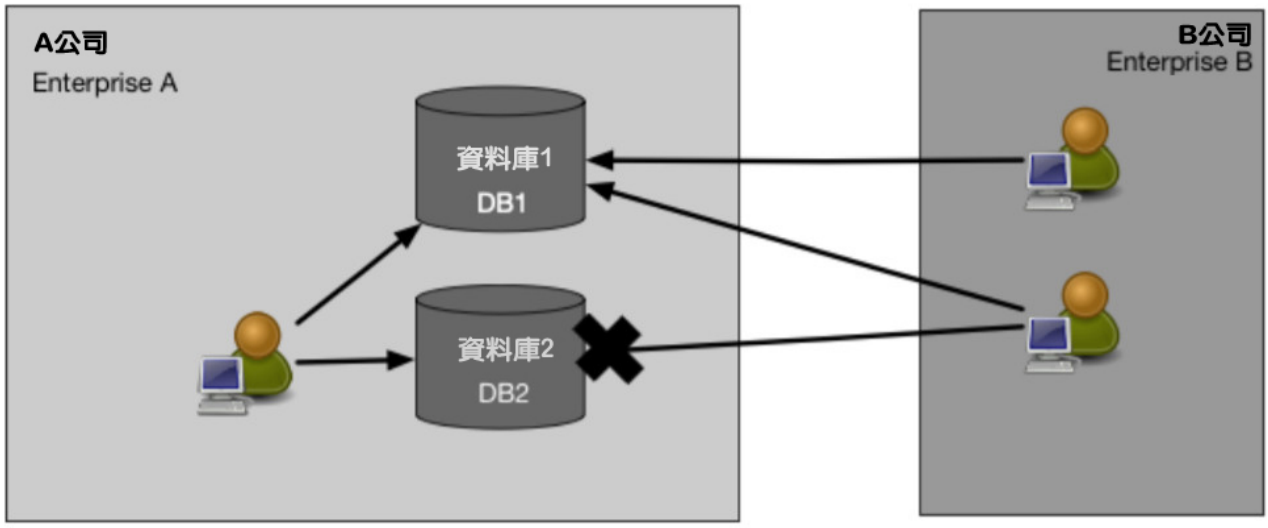


Figure 11: Cross-Enterprise Collaboration

这样的场景有点类似于上述第一节提到的使用案例1，双方员工可能不在本地组织网络架构中，并且需要存取一个企业网络或托管于云端的资源。

因此，策略引擎（PE）/ 策略管理器（PA）可以托管于云端服务来进行，而无需建立VPN或类似的服务。可能需要企业B员工在其系统上安装代理程序，或通过网页入口存取必要资源。

第四章第五节 面向公众或客户服务的企业

第五种类型是许多企业的一个共同特点，会提供对外的公众服务。这类服务可能是针对广泛大众，或是针对业务关系的客户，甚至是针对特殊的非企业客户，比如员工家属之类。在这当中，或者也包含需要用户注册的服务。

在上述所有情形下，请求的资源可能不是企业所拥有的，并且企业在内部网络安全政策，在应用到非企业拥有的资源时会受到限制。

基本上，不需要登录就能存取的对外服务，比如公开网站等，零信任原则并不直接适用。

针对注册的会员用户，或是商业客户与特殊用户，企业可以建立限制政策，包括针对在线服务帐密安全，要求密码长度、生命周期，以及提供多因素验证等选项或要求。并要注意，要限制那些来自未知浏览器类型与过时版本的存取请求，这很可能是伪装合法用户的攻击行为。同时，也应了解使用者请求与资产的信息收集与记录方面的法规。

总体而言，这里介绍了5种常见的企业场景，主要只是简单概述了ZTA部署的可行方式。

第五章 零信任架构相关威胁

在SP 800-207的第五章中，NIST希望用户对于网络安全及零信任的概念要有正确的认知。因此，他们一开始就强调，任何企业都不可能完全防范网络安全风险，也不会有百分之百的安全。

在现有的网络安全政策与指南之下，加上身份识别与存取管控、持续监控、普遍网络卫生的相辅相成，实施ZTA的主要目标就是降低总体风险，防范共同威胁。

然而，在导入ZTA时，也将面临一些特定的风险。NIST共归纳出七大威胁面，并说明其风险，这将成为企业与业者在设计或导入ZTA时，可以考量或注意的方面。

第五章第一节 **ZTA**决策过程遭破坏

零信任架构的第一个风险是存在于策略引擎（PE）与策略管理器（PA）中，因为它们是整个系统的关键组成，企业资源的请求都需要经由此机制来存取放行。这意味着，这些元件必须要被正确的设置与维护。

据理来说，若是可存取PE政策的任一企业的系统管理员，执行了未经授权的变更或是犯了错，都可能扰乱企业的运行；同样地，遭入侵的PA可能允许存取未经核准的资源，例如个人装置遭入侵。

因此，要防范PE与PA的相关风险，就必须具有适当的设置与监控，对于任何变更设置，都要做到记录与审计。

第五章第二节 遭遇**DoS**阻断服务或网络中断

如上所述，PE与PA是整个系统的关键，而零信任架构的第二个风险，就是若是攻击者透过DoS攻击，或是路由劫持等方式，造成与PEP或PE/PA连接的中断或拒绝存取，也可能对企业系统运行造成影响。

基本上，企业可以遵照SP800-160v2网络弹性指南，将策略落实放在安全可靠的云端环境或是设于多个位置，来缓解这样的威胁。

然而，这并不能完全消除风险，毕竟，过去Mirai等僵尸网络曾发起大规模的服务阻断攻击，而攻击者也可能只拦截或中断部分流量，使部分用户受影响。此外，还有像是云端服务提供者也可能发生意外，使设于云端的PE或PA离线。

第五章第三节 帐密被盗 / 内部威胁

由于零信任原则是不再有隐性的信任，攻击者只能靠入侵既有的帐户或装置，才能在企业中获得立足点。因此，对于企业组织而言，要能正确开发与实施ZTA，应防止遭入侵的帐户或资产以超出其正常权限或存取模式的行动。这意味着，具有资源存取权限的有价值帐户，将成为攻击者的主要目标。

攻击者将如何获取这类具有价值的帐户？一般而言，攻击者惯用网络钓鱼、社交工程，以及两者合并使用的手法。对于成为目标的具有价值帐号，NIST提醒，这需要从攻击动机来看，企业管理者的帐号通常被认为很有价值，但对于财务有兴趣的攻击者，可能还会考虑具有财务与支付资源存取权限的帐号。

在应对上，NIST表示，实施多因子身份验证（MFA），将可降低数据遭被入侵帐户存取的风险。不过，一旦攻击者或是恶意的内部人员获得了有效凭证，仍然能够存取已授予权限的资源。因此，这样的风险仍需要注意。

NIST强调，零信任架构可降低风险，以及防止被入侵帐户或资产在整个网络中的横向移动。

防止横向移动攻击是关键。因此，被入侵帐户若原本没有的存取权限，其实依然会被继续拒绝存取。而且，在第三章说明ZTA算法时，曾提到基于装置情境的信任算法，这将比传统的边界防护策略，更容易检测出超出正常存取模式的攻击行为，并拒绝遭入侵帐户或内部威胁去存取敏感资源。

第五章第四节 网络可视性

在第三章介绍ZTA网络环境元件时，NIST提到对于网络上的所有流量，都需要经过检查、记录与分析，目的是要识别与应对潜在的攻击活动。

然而，企业网络中的多数流量，对于第三层（Layer 3）的网络分析工具而言，可能并不透明，加上这些流量可能并非来自所有企业资产，或是应用程序与服务本身可抵抗这类被动监控。因此，企业无法执行深度封包检测（DPI）或检查加密流量，必须使用其他方法来评估，网络上是否可能存在攻击者。

但NIST指出，这并不代表企业无法分析这些加密流量，企业仍然可以收集加密流量元数据，并使用这样的数据来检测网络上的攻击者活动，或是可能存在的恶意软件通讯行为。此外，机器学习技术将有助于分析这类无法被解密的流量。

在此，NIST提及了2017年由Blake Anderson与David McGrew发表的研究报告，名为「用于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」，并说明使用此类型的机器学习，将帮助企业将流量分类，包括有效的流量，以及可能存在恶意待补救的流量。

第五章第五节 系统与网络信息的存储

当企业针对网络流量进行监控与分析时，这里同样存在一个相关的威胁，那是分析组件本身的安全性。

如果有监控机制进行的扫描结果、网络流量、备用作装置情境（Contextual）算的元数据、鉴识结果，以及后续调查等数据，这些数据也将成为攻击者的目标。这就如同网络拓扑、配置文件，以及各种网络架构文件一般，这些信息也都应受到保护。一旦攻击者能够访问这些信息，意味着对方能够深入了解企业架构并识别资产，帮助他们未来进一步的侦测与攻击。

在零信任企业环境中，另一个攻击者信息侦察的来源，是编码存取政策的管理工具，这如同网络流量的存储，这个元件包含资源存取政策，将提供给攻击者信息，了解哪些帐号最有价值被入侵，例如，知晓可访问特定资源的帐户。

因此，对于所有具有价值的企业数据，都应采取适当保护措施，防止未经授权的访问与尝试访问的行为。由于这些资源的安全性更是至关重要，因此需采取最严格的存取政策，只能通过指定或专用的管理者帐户去访问。

第五章第六节 依赖专有数据格式或解决方案

从ZTA核心元件来看，零信任架构会根据多方数据做出存取决策，这其中包括请求的主体、使用的资产，以及企业与外部威胁情报等信息。

普遍而言，这些信息的交换并没有一个通用的开放标准，这样的互动性问题，将导致企业可能被限制在同一供应商。如此一来，当该供应商出现安全问题或服务中断时，可能无法转移到新的供应商，除非是要付出高昂成本更换多项资产，或是需要经历漫长的转换计划。

基本上，这样的风险并非ZTA特有的问题，但因为ZTA非常依赖动态存取政策控管，因此，这样的问题将会影响到企业核心业务功能。

因此，NIST指出了供应链安全的议题。为了要降低相关风险，企业需要对服务提供商进行整体评估，不只是考量效能、稳定性，并要考量供应商资安控管，以及企业转换成本与供应链风险管理等因素。

第五章第七节 ZTA管理者采非人实体的风险

随着AI和其他基于软件的代理程序在企业网络安全中的部署，这些组件将与ZTA的核心元件（如PE、PA）互动，有时还将代替人工管理者执行任务。在这种情况下，这些元件如何进行身份验证是一个尚未解决的问题。

一般来说，大多数自动化技术系统在使用资源组件的API时，会进行某种形式的身份验证。但是，当政策设置和执行涉及自动化技术时，最大的风险是“误报”，其中包括两种情况，一种是将无害行为错误地识别为攻击，另一种是将攻击行为错误地判定为正常活动。

因此，相关风险是攻击者可能通过诱使或强迫方式，让NPE执行攻击者无权执行的操作。NIST解释说，与人类用户相比，软件代理程序在执行管理或安全相关任务时，可能采用较低的身份验证标准，例如API密钥和多因素验证。一旦攻击者能够与代理程序互动，理论上可以欺骗代理程序，允许攻击者获得更大的访问权限，或执行某项任务。另外，还有一种风险需要注意，即攻击者可以获得软件代理程序的凭证，并在执行任务时冒充代理程序。

第六章 零信任架构与美国现有联邦指引的相关性

NIST指出，零信任架构与一些现有的联邦政策与指引，在规划、部署与运作上，都有着交互的作用。

基本上，这些政策虽然会影响零信任战略的制定，但不是要禁止企业朝向零信任导向的架构。在与现有的网络安全政策与指南、ICAM、持续监控，以及一般网络卫生相结合的情况下，ZTA可以强化组织的安全现况，防范常见威胁。

第六章第一节 零信任架构（**ZTA**）与风险管理框架（**RMF**）

首先，NIST谈到的是现有的NIST SP 800-37风险管理框架（Risk Management Framework，RMF）。

在ZTA部署中，主要焦点围绕在指定任务或业务流程的可接受风险，并制定存取政策，因此有可能允许连接的终端进行存取资源，但拒绝所有网络存取。但在大多数情况下，这种不平衡地限制，可能会阻碍工作的完成。

过去，NIST已发展出NIST SP 800-37风险管理框架（RMF），对于联邦机构执行其任务，必须识别、评估与缓解执行任务的相关风险，需要可接受风险层级。

而在ZTA的导入与实施中，这会改变企业对于认证边界的定义，主要因为增加了PE、PA与PEP等新元件，以及减少了对于边界网络防护的依赖，但在整个过程中，RMF的描述并不会改变。

第六章第二节 零信任（**ZT**）与**NIST**隐私框架

对于用户个人信息的隐私保护，一直是企业与组织关注重点，以法规面向来看，包括联邦信息安全管理法（FISMA），以及美国医疗信息保护法规（HIPAA），为此，NIST 制定了供组织使用的隐私框架「NISTPRIV」，这份文件提供一个框架以描述隐私风险与缓解策略，这将包含企业组织对于用户隐私的识别、评估与缓解，以及隐私信息的存储与处理的过程。

而ZTA的核心要求之一，在于企业应在其网络环境中，检查并记录所有流量，在这其中，有些流量可能包含了隐私信息，以及相关隐私风险。

因此，当企业在开发零信任架构时，通过NIST隐私框架将有助于开发一个正式的流程，可用以识别与缓解任何隐私相关的风险。

第六章第三节 零信任架构（**ZTA**）与联邦身份识别、认证与存取管理（**FICAM**）

主体是ZTA的关键组成之一，若政策引擎（PE）没有足够信息来识别关联的使用者与资源，则PE将无法确定尝试的连接，是否应被授权连接到资源。在迈向更为零信任的部署之前，需要针对主体制定严格的身份验证策略，因此企业需要清晰的使用者属性与政策，才能让PE能够评估存取请求。

针对联邦政府的身份识别管理，美国行政管理和预算局（OMB）发布M-19-17的备忘录，在此其中，该备忘录呼吁所有联邦机构成立一个ICAM办公室，目的是治理与身份发放与管理相关的工作，而其中许多的管理策略，主要建议是依循NIST SP 800-63-3 Digital Identity Guidelines的指引。

由于ZTA需要精确的身份管理，在ZTA上所进行各项努力，都将需要与机构的ICAM政策相结合。

第六章第四节 零信任架构（**ZTA**）与可信互联网连接第三版（**TIC 3.0**）

基本上，TIC是一项由OMB、DHS与GSA联合管理的网络安全计划，期望建立联邦政府的网络安全最低基准。

从其历史来看，TIC是一种基于边界防护的网络安全策略，要求机构整合与监控其外部网络连接，在早期的TIC 1.0与TIC 2.0中，主要假设周边内部都是受信任的，其中TIC 2.0提供一系列基于网络的安全功能，包括内容过滤、监控、身份验证等，并部署于机构周边的TIC接入点，其中许多功能都符合ZTA原则。

到了TIC 3.0，新版扩展到云端服务与移动设备，不仅如此，人们意识到「信任」的定义，可能因特定运算环境条件而异，且每个机构有不同的风险承受能力。

简单来说，TIC 3.0聚焦在基于网络的安全保护，相对地，ZTA是更广泛的架构，不仅针对网络，同时还强调应用程序、使用者与资料保护。而随着TIC 3.0使用案例的发展，ZTA TIC使用案例很可能也会出现，开发出关于部署ZTA强制点的网络保护定义。

第六章第五节 零信任架构（**ZTA**）与国家网络安全保护系统（**NCPS**）

关于国家网络安全保护系统（National Cybersecurity Protection System，NCPS），也就是爱因斯坦计划（EINSTEIN），这是一个多系统的整合，主要提供入侵侦测、进阶分析、信息共享与入侵防御功能，目的是帮助美国联邦政府防御网络威胁。

基本上，NCPS的总体目标与零信任一致，都是要管理网络风险、改善网络保护能力，通过该系统感知器，可供CISA旗下的国家网络安全与通讯整合中心（NCCIC）帮助联邦机构应对重大资安事件。

美国国土安全部（DHS）同样运用这些感知器，主要基于边节网络防护的做法，相对地，ZTA是将防护更贴近资产、资料与所有其他资源的所在位置。

随着NCPS计划的发展，将可帮助ZTA系统扩展感知与遥测能力的基础。但也因此，NCPS的入侵防御功能应该需要进化。

随着ZTA被整个联邦政府采用，NCPS的实施需要不断发展，或是需要具备新的能力来实现NCPS的目标。

第六章第六节 零信任架构（**ZTA**）与国土安全部持续诊断与缓解计划（**CDM**）

关于国土安全部（DHS）的持续诊断与缓解计划（Continuous Diagnostics and Mitigations，CDM），目的是要改进联邦机构的IT技术，关注的重点在于机构对自身资产、设置配置与主体的洞察力。这包括：企业连接了什么？谁在使用网络？网络发生什么情况？以及数据如何保护？

NIST指出，能实施高强度的CDM计划，将是零信任架构成功的关键。例如，要朝向ZTA发展，企业必须有一套系统能发现并记录实体与虚拟资产，以建立可用清单。

这其实类似于制定零信任路线图的第一步，机构必须对于网络上的资产与活动具有可视性，才能分类、设置配置与监控网络活动。

第六章第七节 零信任架构（**ZTA**）与云端智能策略、联邦数据策略

最后，NIST谈到联邦云端计算策略（简称云端智能策略）、数据中心优化政策的更新（备忘录M-19-19），以及联邦数据策略，都会影响机构在ZTA规划上的一些需求，在这些政策中，对于数据收集、存储，以及本地与云端的存取，均有要求机构盘点与评估。

这样的清单至关重要，可确定商业流程与资源，对ZTA导入带来帮助。对于主要基于云端或远端的使用者而言，ZTA方案将是不错的选择。因为数据资源、应用程序与服务位于企业网络边界之外，这些企业最能体会其扩展性与安全性的益处。

第七章 迈向零信任架构

在第一章中，NIST已经指出，朝向ZTA过渡会是一个漫长过程，不是全面的技术更换。在企业的IT基础设施中，实际上已经存在着ZTA的元素。在第七章的开头，NIST再次强调这一点，指出导入ZTA是一段旅程，而不是大规模更换基础设备或流程。

对于零信任原则的实施、流程的变化以及保护高价值数据资产技术解决方案的采用，企业组织需要寻求一个渐进的方式。

基本上，大多数企业的网络安全策略会以零信任与传统边界防护混合的模式进行，并持续很长一段时间。这期间将持续投资于IT基础设施的现代化。换言之，制定IT现代化的计划将包含基于零信任原则的架构，这将有助于企业为小规模的工程流程制定未来发展蓝图。

当然，每家企业导入零信任的策略都取决于当前的网络安全运作与现状。

NIST指出，企业应该在部署零信任环境之前，就能达到一个基本的安全水平。而这个基本安全水平的方面将包含资产、主体、业务流程与流量，以及对应的识别与分类，也就是对于这些信息要有详细的了解。这是因为企业需要这些信息，才能有助于后续工作的进行。

第七章第一节 纯粹的零信任架构

若以一个全新的环境而言，企业可以从头开始构建零信任架构。

因此，这里需要假设企业知道，运作中会有哪些应用程序、服务与工作流程，因此可以为这些工程流程，建立一个基于零信任原则的架构。

一旦确定了工作流程，企业就可以缩小所需元件的范围，并开始描绘每个元件的互动关系。

从这一刻开始，建立架构与设置配置元件将是企业一大工程，同时可能也要关注额外的组织性变动，具体还是取决于企业运作与配置的现状。

当然，对于普遍企业组织来说，这很少是可行的选项，毕竟已经拥有既有网络环境。不过，一旦要建立新的应用程序、服务或数据库时，是可以在某种程度上，引入零信任的概念。

第七章第二节 混合零信任架构与传统边界防护的架构

基本上，对于普遍企业而言，零信任与传统企业边界防护架构共存的情况，可能会需要一段时间。在NIST的建议中，导入零信任的方法上，企业可以每次只针对一个业务流程的方式去进行。

但同时，企业需要确认是否有足够且灵活的共同元素，例如身份识别管理、设备管理与事件日志记录等，以支撑混合式安全架构的运行。对于征选的ZTA解决方案，企业架构师也可能希望是，限制为可以与现有元件接口连接的解决方案。

要让既有业务流程邁向到ZTA，可能有些部分需要重新设计，相对地，企业也可趁着这样的机会，遵循SP800-160v1的系统安全工程的内容去实践。

第七章第三节 介绍从边界网络架构邁向零信任架构的步骤

基本上，本章节是最关键的部分，这里提供了导入ZTA的步骤建议，让企业对于ZTA的导入更有方法。

前面多少都有提到，邁向ZTA的过程中，企业组织需要详细了解自身在实体与虚拟的资产，以及包含用户权限的主体，还有业务流程。

因为这些知识内容，将是策略引擎（PE）在评估资源请求存取时所需。一旦这些知识内容不完整，将会导致业务流程失败，也就是PE因为信息不足的原因，而拒绝存取请求。

换言之，企业组织如果不了解当前的业务运作状况，当然也就无法确定需要采用哪些新流程或系统。因此，企业应在努力将ZTA引入企业之前，对于资产、主体、数据流与工作流程进行调查。

NIST表示，这些相关的调查，都与组织业务流程的检查有关，其实是可以同时进行的。同时这里还特别强调一点，这些步骤是可与NIST风险管理框架（RMF）的SP 800-37相对应的，这是因为，采用ZTA的任何过程，就是要降低组织业务功能风险的过程。

还要注意的是，在初始的盘点清单建立后，需要定期维护与更新，并要注意更新之际，可能更改业务流程也可能不产生影响，但都应该要对业务流程进行评估。

在此，NIST提供了一个可视化的图表，让外界可以了解导入ZTA的步骤与路线。

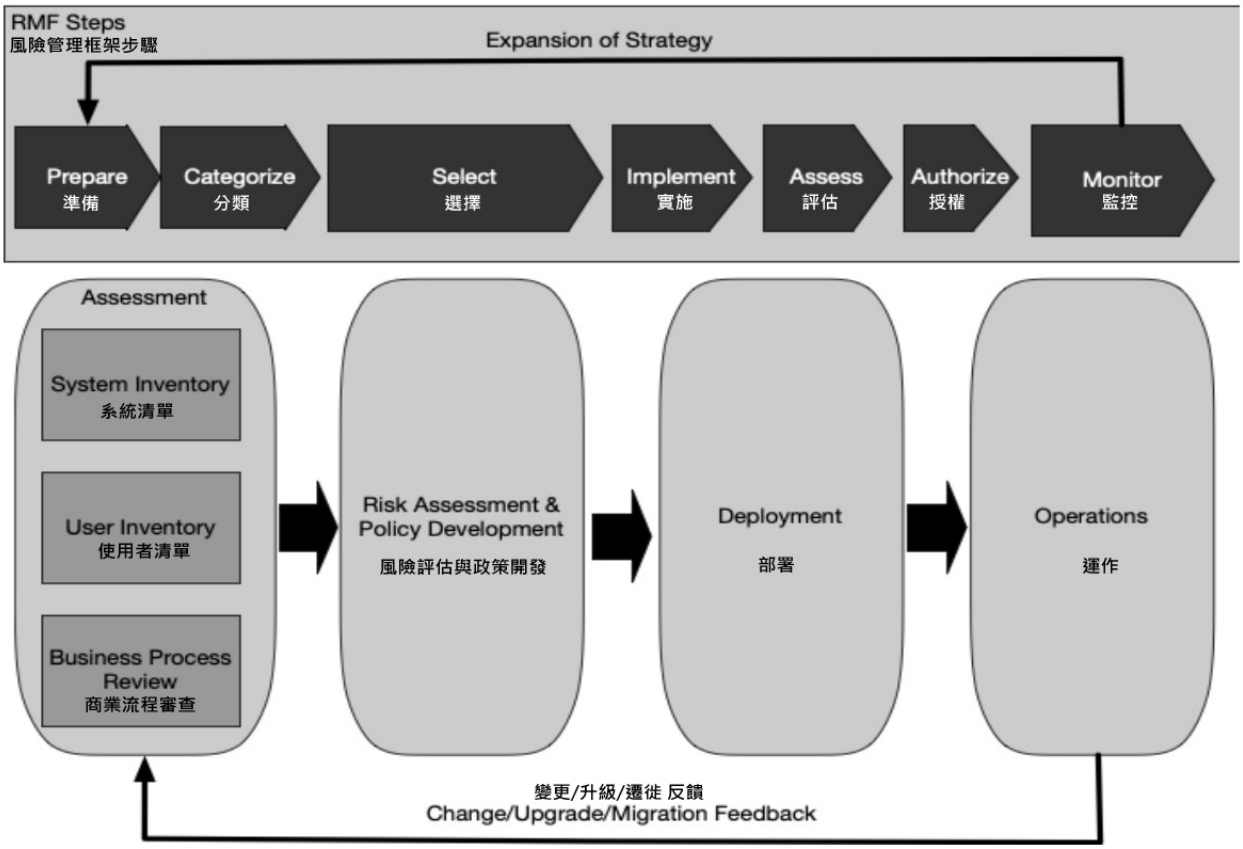


Figure 12: ZTA Deployment Cycle

具体而言，NIST提供了7大建议步骤，分别是：（一）识别企业中的角色，（二）识别企业中的资产，（三）识别关键流程，并要评估与流程执行相关的风险，（四）针对ZTA候选者制定政策，（五）识别候选的解决方案，（六）初期部署与监控，（七）扩展零信任架构。
一、识别企业中的角色

为了使零信任企业得以运行，以策略引擎（PE）的角度来看，必须对于企业主体先有所认识。

这里指的主体，包含了人类，也有可能是非人类实体（Non-person Entities，NPE），比如与可资源互动的服务账号。

至于特权账号使用者，如开发人员或系统管理员，在分配属性与角色时，需要具有额外的审查。在许多传统安全架构中，这些账号可能有用访问所有企业资源的能力，而在ZTA架构之下，应该允许开发人员与管理员有足够的灵活性，以满足他们的业务需求，同时使用日志和审计机制来标识访问行为模式。

此外，关于ZTA的部署上，可要求管理员在NIST SP 800-63A中满足更高分数或符合更严格的标准。

二、识别企业中的资产

前面章节提到ZTA的关键要求之一，是要有能力识别与管理设备，同时ZTA还要求针对非企业拥有的设备，同样要有能力去识别与监控，因为这些设备可能存在于企业拥有的网络基础设施上，或是访问企业的资源。简而言之，部署ZTA的成功关键，就是要有能力管理企业资产。

具体而言，这些企业资产包括硬件元件，例如笔记本电脑、手机与IoT装置，还有数字artifacts，例如用户账号、应用程序与数字证书等。或许我们不可能对所有企业拥有的资产，进行完整的普查与盘点，因此，所以企业或许应考虑建立一套机制，可在企业基础设施上，将新发现的设备资产，做到快速识别、分类与评估。

需要注意的是，这不仅仅是对企业资产进行简单的归类与维护数据库，还须包括配置管理与监控。

毕竟，观察资产当前状态的能力，是评估访问请求过程的一部分。这意味着企业需要企业必须能够配置、调查与更新企业资产，譬如虚拟资产与容器，以及实体与网络位置，当进行资源访问决策时，这些信息需要通知到PE。

此外，非企业拥有的资产，以及企业拥有的影子IT，也应该尽可能的纳入分类。这方面可能包括企业内可见的任何东西，例如MAC地址、网络位置，并通过管理员的数据输入加以补充。这些信息不仅可用于访问决策，也将用于企业的监控与日志鉴定。

还要注意的是，影子IT会带来一个特殊的问题，因为这些资源是企业所拥有，但却不像其他资源那样被管理。因此也要注意，有些ZTA方法可能会导致影子IT变得不可用。

三、识别关键流程，并要评估与流程执行相关的风险

第三个清查项目，机构应对业务流程、信息流，以及对于机构任务中的关系，做到识别排序。

基本上，业务流程应通知资源访问请求被批准或拒绝的情况。对于企业而言，建议可从低风险的业务流程开始朝向ZTA迈进，因为一旦业务中断，还不致于让对整个组织带来负面的影响，一旦获取了足够的经验，就可以选择其他重要的业务流程继续进行。

同时，利用基于云端的资源，或是由远端工作人员使用的业务流程，对于ZTA也是相当不错的方式，并可能会看到可用性与安全性上的改善。
此外，企业用户可以直接请求云端服务，而不是投射企业边界到云端，或是将用户通过VPN带入企业网络。因为，通过企业的政策落实点（PEP），可确保向用户授予资源访问权之前已遵循企业政策。

但这里还强调一点，规划ZTA的人，还要考虑一些潜在的因素，当实施ZTA时可能会出现的问题，包括效能、用户体验，以及可能增加工作流程脆弱性等，需要做出权衡取舍。四、识别引入 ZTA 候选程序的政策

在选择服务或业务工作流程以实施 ZTA 的过程中，有几个重要因素必须注意：包括流程对组织的重要性，受影响的群体对象，以及在工作流程中资源使用的当前状态。

而要评估资产的价值，或是资产与工作流程的相关风险，在 NIST 的建议中，NIST 风险管理框架可为企业带来帮助，也就是 NIST SP 800-37。

在识别了资产与工作流程之后，也就是识别工作流程中所使用或影响的所有上游资源、下游资源与实体。

上游资源：如 ID 管理系统、数据库、为服务

下游资源：如日志、资安监控

实体：如主体、服务帐号

这些都会使企业第一次迁徙 ZTA 时，在选择上带来影响。NIST 并举例说明，一部分企业主体使用的应用程序或服务（如采购系统），可能比整个企业群体至关重要的应用程序或服务（如电子邮件）更适合。

接下来，企业管理者需确认要使用的信任算法（Trust Algorithm），并且调整权重标准，以确保不阻碍资源的访问，并且访问管控政策是有效的。

五、识别可行的解决方案

当确定了业务流程的清单后，企业架构师将可制定解决方案选择的清单，这部分 NIST 指出可从五个关键因素去考量

● 解决方案是否要求在客户资产上安全元件？

在非企业资产使用或需求上，这可能会限制业务流程，像是 BYOD 或跨机构合作的情境。

● 解决方案在业务流程完全存在于企业场所的情况下是否有效？

因为有一些解决方案预设请求的资源是存放云端（所谓的南北向数据流），而不是在企业的周边（东西向数据流），因此业务流程资源的位置，将影响解决方案与 ZTA 流程的选择。

● 解决方案是否提供了可互动的 Log 记录供分析？

毕竟零信任的关键元件，就是要收集与使用流程相关的数据，提供给政策引擎以做出访问决策。

● 解决方案是否针对不同应用程序、服务与协议提供广泛支持？

有些解决方案可能支持广泛的协议（如网络、SSH 等）、协议（IPv4、IPv6），但一些解决方案可能只适用于特定范围，像是网络或电子邮件。

● 解决方案是否需要改变主体的行为？

有些解决方案可能在执行特定工作流程时需要额外的步骤，这可能会改变企业主体执行工作流程的方式。

总体而言，这一解决方案是先将现有业务流程建立模型，作为试点计划，而不仅仅是一个替代方案。而这样的试点方案可以具通用性，也就是能适用与多个业务流程，或是当成特定的使用案例。基本上，在过渡到 ZTA 部署之前，试点计划可视为 ZTA 的验证场域，之后再脱离传统的流程基础架构。

六、初期部署与监控

在选择了工作流程与 ZTA 元件后，就可以开始进入初期部署阶段。

一开始企业可能遇到的问题是，希望先以观察或监控模式来进行。只是很少有企业可以在第一次就能完善，像是重要的帐户可能在访问资源时被拒绝，或是可能不需要具备某些访问权限。

因此，在新的 ZT 业务流程之下，可在「仅报告」（Reporting-only）模式下先执行一段时间，以确保政策是有效且可行，并让企业可以理解其运行。在 Reporting-only 模式之下，这意味着对于大多数访问请求给予访问许可，应将日志与连接的踪迹，进而比对最初制定的管理政策。

不过，这里也指出初始部署时，访问政策可以更宽松一点，以便收集 ZT 工作流在实际交互过程下的相关数据，一旦建立工作流程下活动例子的基准，就可以更容易识别异常行为。若无法以更宽松的方式运作，企业网络维运人员需要密切监控日志，并随时准备根据运作经验修改访问政策。

七、扩展零信任架构

在初期实际部署运作之后，完善了工作流的所有政策，企业就进入稳定运行阶段。

此时，网络与资产仍然被监控，流量也都被记录，但响应与政策调整的节奏放慢，持续从各式问题反馈做到改进。接下来，企业管理者可以规划ZT部署的下一循环，也就是回到上述第四步骤，选定下一个工作流程与解决方案，并进行部署。

同时，也要注意如果工作流程发生变化，需要重新评估运行中的零信任架构。这包括新设备、软件（特别是零信任逻辑元件）的重大更新，以及组织架构的转变，都可能导致工作流程与政策产生变化。实际上，应假设有些工作已经完成的情况，重新审视整个流程。