# 零信任架构在网络安全运维中的实践与效果评估

张 磊
浙江省数据管理有限公司 浙江 杭州 310000

**摘 要：**随着云计算、大数据、移动互联的飞速发展，远程办公、异地分支的大量应用，网络边界变得越来越模糊，传统的网络安全架构已难以满足安全新需求。零信任架构作为一种新兴的网络安全范式，通过打破传统边界防护思维，以身份为中心，构建动态的、自动化的、自适应的安全网络，为网络安全运维提供了新的解决方案。本文旨在探讨零信任架构在网络安全运维中的实践与效果评估，以期为相关领域的实践提供参考。

**关键词：**网络安全运维；零信任架构；实践应用；效果

## 引言

零信任架构最早由约翰·金德维格（John Kindervag）在2010年提出，其核心思想是“永不信任，持续验证”。在零信任架构下，任何实体都必须在访问任何资源之前通过验证，且这种验证是持续进行的。随着网络环境的日益复杂，零信任架构在网络安全运维中的实践与效果评估成为了一个重要课题。

## 1 零信任架构在网络安全运维中的实践应用

### 1.1 架构模型构建

在零信任架构的部署中，架构模型的精细化构建是确保整个安全体系有效运行的关键步骤。这一过程不仅涉及对关键数据、应用程序、资产和服务（DAAS）的深入理解和分类，还要求在技术实现、策略制定和持续优化上做到细致入微。

#### 1.1.1 数据分类与保护策略

首先，需根据数据的敏感性、法律合规要求及业务价值，将数据细分为多个级别，如高度敏感（包含个人身份信息、财务信息）、敏感（业务策略、客户数据）、内部使用（日常运营数据）和公开（可对外分享的信息）。每个级别数据对应不同的保护措施和访问权限。针对不同级别的数据，设计差异化的加密策略、存储位置和访问控制规则[1]。例如，高度敏感数据应采用强加密算法，存储于受限访问区域，并实施严格的访问审计。

#### 1.1.2 应用程序、资产与服务评估

评估每个应用程序的安全性，包括其代码安全、更新频率、漏洞管理情况以及对敏感数据的处理方式。基于评估结果，为应用分配相应的安全等级，并采取相应的防护措施，如应用安全加固、Web应用防火墙（WAF）部署等。识别企业关键资产，如服务器、数据库、云服务实例等，评估它们对业务连续性的重要性及潜在的安全风险。对于高价值资产，实施更为严格的安全监控和访问控制。

#### 1.1.3 安全控制链的构建

采用多因素认证机制，结合用户身份、设备信息、网络环境等多维度数据，确保访问请求的真实性。利用单点登录（SSO）技术简化用户访问流程，同时保持高安全性。基于用户角色、数据分类、设备健康状态及实时威胁情报，动态调整访问权限。采用策略即服务（PaaS）模式，实现策略的快速部署和灵活调整。实施细粒度的授权策略，确保用户仅能访问完成工作所必需的资源。建立全面的审计日志系统，记录所有访问活动，便于追踪和合规性检查。部署持续监测工具，如安全信息和事件管理（SIEM）系统，实时分析网络流量、用户行为及系统日志，及时发现异常并触发响应机制。结合人工智能和机器学习技术，提升威胁检测的准确性和效率。

#### 1.1.4 持续优化与迭代

定期回顾和调整安全策略，根据最新的威胁情报、业务变化及合规要求，优化访问控制规则，确保策略的有效性和适应性。定期对员工进行零信任安全理念的培训，提高其对安全政策的理解和执行力，形成全员参与的安全文化。

### 1.2 信任评估算法应用

信任评估算法作为零信任架构的核心组件，扮演着智能决策者的角色，确保每一次访问请求都经过严格而全面的评估，从而维护网络的安全性和稳定性。这一算法的应用不仅涉及多源数据的整合与分析，还包括动态风险评估与实时策略调整。

#### 1.2.1 多维度数据融合与分析

（1）用户信息：整合用户身份验证数据、历史访问记录、角色权限及行为模式，构建用户信任档案。利用机器学习技术，分析用户行为模式，识别异常登录或访

问行为。（2）设备状态：收集设备健康信息，如操作系统版本、安全补丁状态、防病毒软件更新情况，以及设备是否被标记为已知的可信或不受信任设备。（3）访问信息：分析访问请求的具体内容，包括请求的资源类型、访问时间、地理位置等，以评估请求的合理性。（4）行为属性：监控用户在网络中的实时行为，如文件操作、数据传输、网络浏览等，结合历史行为模式，识别潜在的安全威胁[2]。（5）访问策略：根据企业安全政策、合规要求及业务需要，动态调整访问控制策略，确保策略的灵活性和适应性。（6）外部威胁情报：整合全球安全威胁数据、已知漏洞信息、恶意IP地址库等，实时更新威胁情报库，提升系统对外部攻击的防御能力。

1.2.2 动态风险评估与策略调整

基于上述多维度数据，算法实时计算访问请求的风险评分，对高风险请求进行拦截或要求额外的验证步骤。根据风险评估结果，自动调整访问控制策略，如限制访问时间、降低权限等级、要求二次认证等，确保策略的动态适应性。算法通过持续学习用户行为、设备状态变化及威胁情报更新，不断优化风险评估模型，提高评估的准确性和效率。

1.3 微隔离与细粒度访问控制

微隔离作为零信任架构的关键技术之一，其核心在于将网络划分为多个微小的、逻辑上隔离的安全区域，也称为“微段”或“微隔离区”。每个区域仅包含完成特定业务功能所必需的资源，如服务器、应用程序、数据等。这种细粒度的资源分割策略，显著降低了攻击者利用单个突破口在网络中横向移动和扩散的风险，有效遏制了潜在的安全威胁。

1.3.1 微隔离的实践应用

根据业务逻辑和安全需求，将网络中的资源精细划分到不同的微隔离区中。每个区域实施独立的访问控制策略，确保只有经过授权的流量才能通过。微隔离策略需根据业务变化和安全威胁动态调整，确保策略的时效性和适应性。例如，当新业务上线或旧业务下线时，及时调整隔离策略，以维持网络的安全隔离状态。通过可视化工具，实时监控微隔离区的网络流量、访问行为及安全事件，为安全运维团队提供直观的监控视图，便于快速响应和处置潜在威胁。

1.3.2 细粒度访问控制的实现

细粒度访问控制是微隔离策略的重要补充，它强调对用户权限的精确管理，确保用户仅能访问完成工作所必需的资源。一是基于角色的访问控制（RBAC）：根据用户的职责和角色，分配相应的访问权限。每个角色对应一组特定的权限，用户通过角色获得访问资源的权限，简化了权限管理过程，提高了管理效率。二是基于属性的访问控制（ABAC）：相比RBAC，ABAC提供了更细粒度的控制。它根据用户属性（如职位、部门、地理位置）、资源属性（如数据分类、敏感级别）及环境属性（如时间、网络条件）综合评估访问请求，动态决定是否授予访问权限[3]。三是最小权限原则：无论是RBAC还是ABAC，都遵循最小权限原则，即用户仅获得完成工作所需的最小权限集，减少了因权限过大而导致的安全风险。

1.4 多因素身份认证与单点登录

1.4.1 多因素身份认证（MFA）

多因素身份认证（MFA）作为零信任架构中访问控制的关键环节，其核心价值在于通过要求用户提供多个独立且难以复制的认证因素，显著提升帐户的安全性，有效抵御未经授权的访问尝试。这些认证因素通常包括以下几类：（1）知识因素：如密码、PIN码或安全问题答案，这类因素基于用户记忆，是传统的认证方式。（2）拥有因素：如手机短信验证码、电子邮件中的一次性密码（OTP）或硬件令牌生成的动态密码，这类因素基于用户所持有的物理或虚拟物品。（3）生物特征因素：如指纹识别、面部识别或声纹识别，这类因素基于用户独特的生物特征，难以复制且使用便捷。MFA的实施，要求用户在登录时提供上述因素中的两个或更多，从而大大增加了攻击者绕过认证机制的难度，即使其中一个因素被破解，也还有其他因素作为安全屏障。

1.4.2 单点登录（SSO）

单点登录技术则解决了用户在多应用环境中频繁登录的问题，它通过统一的认证入口，实现了对用户身份的一次性验证和跨应用的无缝访问。SSO的优势主要体现在：用户只需登录一次，即可访问所有授权的应用，无需重复输入用户名和密码，大大简化了登录流程。IT管理员可以通过SSO系统集中管理用户身份和访问权限，降低了管理复杂度，提高了工作效率。SSO系统通常集成有强认证机制，如MFA，确保了用户身份的真实性和可信度，同时，通过集中审计和监控，能够及时发现并响应安全事件。

## 2 零信任架构在网络安全运维中应用的效果评估

2.1 安全性提升

零信任架构在网络安全运维中的应用，显著提升了系统的整体安全性。其核心理念——持续验证与最小权限原则，为防御网络攻击筑起了一道坚实的防线。在网络钓鱼等社会工程学攻击面前，零信任架构要求用户通

过多因素身份认证，即使攻击者获取了用户的部分登录信息，也难以绕过强认证机制，有效阻断了钓鱼攻击的链路。对于恶意软件和勒索软件，零信任架构通过微隔离技术，将网络划分为多个细粒度的安全区域，每个区域实施独立的访问控制策略。即使某个区域被恶意软件感染，也无法轻易横向移动到其他区域，大大限制了恶意软件的扩散范围。在DDoS攻击场景下，零信任架构通过实时监控网络流量和访问行为，结合行为分析和威胁情报，能够迅速识别异常流量，及时采取防御措施，如限制访问速率、阻断恶意IP等，有效缓解了DDoS攻击对系统的影响。此外，细粒度访问控制的应用，确保了用户仅能访问完成工作所必需的资源，减少了不必要的权限分配，降低了因权限过大而导致的安全风险。这种精细的权限管理，不仅提升了系统的安全性，还促进了合规性的提升。

2.2 运维效率提高

零信任架构在提升网络安全性的同时，也极大地提高了运维管理的效率。其内部终端资产的可视化管理功能，为运维工程师提供了前所未有的便捷。通过零信任架构的集中管理平台，运维人员可以实时查看网络中每一台设备的运行状态，包括设备类型、操作系统版本、安全补丁状态、防病毒软件更新情况等关键信息。这种全面的资产视图，使得运维人员能够迅速定位问题设备，及时采取修复措施，显著提高了运维响应速度。此外，零信任架构的自动化策略调整功能，也大大减轻了运维人员的工作负担。系统能够根据用户的角色、行为、设备状态及外部威胁情报，动态调整访问控制策略，确保策略的时效性和适应性[4]。这种自动化管理，不仅减少了手动配置的错误率，还释放了运维人员的时间和精力，使其能够专注于更高层次的网络优化和安全策略规划。同时，零信任架构的细粒度访问控制，通过精确管理用户权限，减少了不必要的权限分配，降低了因权限管理不当而引发的安全风险。这不仅提升了系统的安全性，也简化了权限管理流程，提高了运维管理的效率。

2.3 适应性增强

零信任架构的灵活性和可扩展性，使其成为应对不断变化的网络环境和业务需求的有力武器。其设计之初就充分考虑了网络的动态性和复杂性，能够轻松适应各种规模和结构的网络环境。随着企业业务的不断拓展，网络规模和复杂度也随之增加。零信任架构通过模块化设计和松耦合架构，能够方便地扩展新的安全功能和策略，以满足不断变化的业务需求。无论是新增的业务系统、网络设备，还是新的安全威胁，零信任架构都能迅速适应并作出响应。同时，零信任架构的动态策略调整能力，是其适应性的重要体现。系统能够根据用户的角色、行为、设备状态及外部威胁情报，实时分析并调整访问控制策略。这种动态调整，不仅确保了策略的时效性和准确性，还提高了系统的安全性和灵活性。此外，零信任架构还支持与其他安全技术和工具的集成，如SIEM（安全信息和事件管理）、威胁情报平台等，进一步增强了其适应性和防御能力。通过集成这些技术，零信任架构能够更全面地感知网络中的安全事件和威胁，更快速地作出响应和处置。

**结语**

零信任架构作为一种新兴的网络安全范式，在网络安全运维中展现出了显著的优势。通过构建以资源为中心的安全模型、应用信任评估算法、实现微隔离与细粒度访问控制以及采用多因素身份认证与单点登录等措施，零信任架构有效提升了系统的安全性、运维效率和适应性。随着网络环境的日益复杂，零信任架构将成为未来网络安全运维的重要趋势。

**参考文献**

[1]刘波,廖游.基于零信任架构的网络安全防护技术分析[J].网络空间安全,2024,15(04):172-175.

[2]陈念标,杨亮,唐立明,等.企业零信任网络安全架构的应用实践研究[J].中国宽带,2023,19(09):157-159.

[3]庞浩,何渊文.基于零信任的网络安全架构研究与应用[J].广东通信技术,2022,42(02):63-67.

[4]翟福龙.基于零信任的网络安全模型架构与应用研究[J].电脑知识与技术,2022,18(03):37-40.