局域网络多层防御体系构建与优化策略研究

郭世凡
贵州省贵阳市花溪区潮苗族布依族乡　贵州贵阳　550031

摘　要：在信息技术高速发展的今天，局域网络已经深入到社会生产和生活的每一个阶层。从日常企业办公，数据存储和传输到工业控制系统稳定工作，局域网络可靠性和安全性非常关键。基于此，文章分析局域网络多层防御体系概念，从多方面入手探讨局域网络多层防御体系构建以及优化策略。

关键词：局域网络；多层防御体系；构建；优化策略

如今，随着云计算和物联网等新兴技术的广泛运用，局域网络已经不是一个孤立的体系，它和外部网络之间进行着频繁的互动。这就使局域网络在防止外界恶意入侵的同时，也必须处理好内部可能存在的隐患，比如员工的误操作和内部人员的恶意损害。与此同时，各行业对局域网络的安全要求也不尽相同，而单一的安全防护策略并不能适应这种多元化的要求。因此，对局域网络多层防御体系建设和优化策略进行深入研究，并通过融合各种防御技术对其进行有层次，有情景的保护，是提高局域网络总体安全性的必然选择。

1 局域网络多层防御体系概述

1.1 定义

局域网络多层防御体系以系统论和网络安全工程思想为基础，通过从物理层，网络层和系统层建立层次化的防御架构、应用层和管理层布设差异化防御机制形成涵盖进攻前防范，进攻时阻断和进攻后追溯的全周期保护体系。它以突破单一防御边界限制为核心，以跨层协同的方式动态应对已知和未知威胁，其实质就是以防御维度立体化（空间维度）和防御阶段连续性（时间维度）增强网络系统弹性抗毁能力。该体系强调“分层不割裂、协同不冗余”，要求各层防御策略既独立承载特定安全功能，又通过威胁情报共享形成有机整体，这种技术主要用于满足企业园区网络、工业控制网络等高度安全的应用场景[1]。

1.2 特点

深度防御：在网络的各个层面，从物理层、网络层至应用层都部署相关安全防护措施。物理层上通过建立门禁系统和监控设备来阻止非法人员与网络硬件设备的接触，从而实现对潜在攻击路径的物理上的屏蔽。在网络层，我们利用防火墙的规则和路由器的访问控制列表等先进技术，对网络数据包进行筛选和过滤，以阻止来自外部的非法网络侵入。在应用层上，采用应用程序防火墙和网页防篡改系统来检测应用程序输入和输出，以防止应用层面上如 SQL 注入和跨站脚本攻击所带来的威胁。每一层的防护都是相互补充的，构建一个纵深的防御体系。当一个层面的防护措施失效时，其他层面仍然能够继续发挥其作用，有效地阻止攻击的渗透。

动态自适应：能实时感知网络环境的变化以及遭受的攻击态势，并自动调整防御策略。在流量监测工具和安全情报收集系统的支持下，对网络上各种数据信息进行实时采集。当发现零日漏洞攻击等新型攻击类型时，系统会马上启动应急响应机制迅速更新入侵监测系统特征库或对防火墙规则进行调整以阻断此类攻击流量。当攻击强度发生变化时，例如在很短的时间内有大量恶意流量流入时，系统将自动加大资源的投入并增强检测和过滤能力，例如提高服务器带宽等、启用备用防护设备等以提高应对新兴威胁和保障防御时效性。

2 局域网络多层防御体系构建策略

2.1 网络边界防御

网络边界作为联系局域网络和外部网络的中枢，无时无刻不暴露在恶意扫描，非法入侵，DDoS 攻击的复杂威胁中。为加强网络的边界防护，我们可以从多个角度出发，其中部署结合深度包检测（DPI）和入侵防御系统（IPS）功能的下一代防火墙（NGFW）是关键的策略之一。NGFW 以其优秀的应用层协议解析能力实现网络流量的深度剖析和恶意流量的准确筛选与屏蔽[2]。

以 HTTP 协议漏洞攻击为例，NGFW 通过确定恶意 HTTP 请求的具体字符组合，异常请求头信息以及其他特征可以达到精准拦截攻击流量的目的。同时，网络地址转换（NAT）技术在网络边界防御中也扮演着重要角色，它将内部网络的真实 IP 地址隐藏于公网 IP 之后，极大地降低内部网络遭受直接攻击的概率。此外，我们精心设计访问控制列表（ACL），并根据源 IP、目的 IP 和端口号等详细数据，对网络流量进行细致的管理和控制，仅允许符合安全策略的合法流量穿越边界进入内部网络，从源头上杜绝非授权访问。

2.2 主机和服务器防御

主机及服务器是局域网络运转过程中最核心的支持，它们的安全与否直接关系到整个网络系统运行的稳定可靠性。在网络攻击技术不断迭代的过程中，对主机、服务器等设备的攻击行为变得越来越隐蔽，破坏力也越来越大。为筑牢主机与服务器之间的安全防线，可以在上面部署以机器学习为核心的高级防病毒软件。该类软件在深度分析大量正常和恶意软件样本的基础上，建立具有较高准确性的行为模型，既可以有效地鉴别传统病毒，更能对不断出现的未知新病毒，恶意软件进行实时监控与拦截。

与此同时，打开操作系统及应用程序自动更新功能也是必不可少的一环，操作系统及应用程序开发者将定期推出安全补丁，及时修补已知漏洞并打开自动更新，可以保证系统及应用时刻保持最新安全状态并将被攻击面减少到最低。此外，我们利用主机入侵检测系统（HIDS）对主机系统中的核心文件、注册表和进程活动进行全面的实时监测，当发现异常修改，未经许可接入或疑似行为时，HIDS 立即报警并根据预设策略进行相应阻断，全力确保主机与服务器之间系统完整性和数据安全性。

2.3 身份认证与访问控制

身份认证和访问控制作为局域网络安全体系建设的重要基石，核心目的是保证仅有合法用户才能对网络资源进行访问。在人员频繁流动和网络应用越来越多元化的复杂背景下，传统的单一因素身份认证方式已经在安全性上显得力不从心。多因素身份认证（MFA）技术应运而生，它融合用户所知（如密码）、用户所拥有（如手机验证码）、用户所是（如指纹、面部识别）等多种不同类型的认证因素，显著提升身份认证的准确性与安全性，能够有效防范身份冒用风险 [3]。

在访问控制这一领域中，采纳基于属性的访问控制（ABAC）模型成为实现细致访问管理的核心要素。ABAC 模型依据用户的属性（比如所属的部门，职位级别，安全权限等级）、资源的属性（例如数据的密级，文件的类型，资源的重要性等等）以及环境属性（例如，访问时间，访问地点，网络接入方式），动态、灵活地授予用户访问权限。该方法突破传统静态访问控制中存在的限制，可以根据实际情况实时调节，保证用户仅能在权限内获取对应的网络资源，从而有力地减少权限滥用所带来的安全风险。

2.4 数据加密

数据作为公司的核心资产在网络环境下的保密性，完整性以及可用性都受到空前的考验。近年来数据泄露现象频繁发生，对企业造成重大经济损失以及声誉损害，所以数据加密已经成为确保数据安全的一种核心方法。

数据传输环节使用 SSL/TLS 加密协议加密网络流量是业界的普遍做法。当企业内部网络与外部合作伙伴进行数据交互时，通过 SSL/TLS 加密建立起安全可靠的通信通道，确保数据在传输过程中不被窃取、篡改或监听。对于存储在主机和服务器上的数据，全面加密（FDE）技术可以有效地防止设备丢失或被盗导致的数据泄露，例如使用 BitLocker 等成熟的全面加密工具，对硬盘中的所有数据进行加密处理。同时，针对关键数据文件，基于密钥管理系统（KMS）的文件级加密方案能够根据数据的重要性和实际使用场景，灵活管理加密密钥。不同层次的数据可以对应于不同加密密钥，密钥的产生，存储，发布及使用均处于 KMS 严格控制下，从各方面确保数据存储及使用时的安全。

2.5 内部网络安全

内部网络安全在局域网络的多层防御系统中起着不容忽视的作用，虽然内部网络较为闭塞，但是仍然存在很多安全隐患，例如内部人员误操作，内部网络中恶意软件传播蔓延。为增强内部网络的安全性，可以在内部网络中部署一套专业流量监控系统，利用先进的流量分析技术来实时监控和分析网络流量情况。通过构建一个正常的流量行为模型，该系统能够准确地识别出异常的流量模式，例如在内部网络中出现的大规模端口扫描、异常的数据传输速度或方向等，从而及时识别出潜在的安全风险。同时，合理地划分虚拟局域网（VLAN）是一种隔离内部网络、降低安全风险传播的有效方法。把不同部门或者业务区域内的网分成不同的 VLAN

可以约束广播域范围和降低安全事件影响程度，如把财务部门和研发部门网单独分成不同 VLAN 以避免安全问题向不同业务区域间扩散。另外，强化内部网络设备安全管理也很关键，要定期更新设备固件，修补已知漏洞并建立强密码策略，避免设备被攻破，并严格审核设备访问情况，对设备操作日志做详细的记录与审核，以保证内部网络设备时刻保持在安全、平稳的状态下 [4]。

3 局域网络多层防御体系优化策略

3.1 各层防御措施协同工作

局域网络多层防御体系各层防御措施并不是孤立的，它们是一个密切相连的有机整体。在网络威胁手段越来越复杂和多变的情况下，单一防御措施所带来的限制越来越明显。比如只靠防火墙来防止外部非法访问很难处理内部网络恶意软件的扩散。所以需要建设各层防御措施的协同工作机制。可以通过统一的安全管理平台的部署来实现防火墙 \ 入侵监测系统和防病毒网关的不同级别防御设备的整合。再者，利用平台联动功能可以在入侵检测系统检测到异常流量后快速给防火墙下达命令、调整访问控制策略、屏蔽攻击路径。同时，防病毒网关实时监测文件传输，一旦检测到病毒，立即通知其他防御设备对相关网络连接进行限制，实现各层防御措施在信息共享基础上的协同响应，提升整体防御效能。

3.2 系统评估与测试

局域网络的安全状况是动态变化的，各种新漏洞、新威胁层出不穷，需要系统地评价和检验多层防御体系。以往的静态评估方式已经不能适应现在复杂网络环境的需要。在目前广泛使用云计算和大数据的大环境中，可以利用动态评估技术模拟真实网络攻击场景来实现防御体系的全方位渗透测试。例如，通过使用自动化渗透测试工具，可以定期扫描网络系统，模拟黑客可能采用的多种攻击方式，包括端口扫描、漏洞利用、恶意软件植入等。通过采集试验期间防御体系响应数据，对不同攻击场景进行薄弱环节分析。根据评价结果对入侵检测系统规则库等防御策略进行有针对性地优化，提高识别新型攻击模式和保证多层防御体系始终处于高效防护状态等措施。

3.3 安全社区与同行交流

局域网络多层防御体系的优化过程中安全社区和同行之间的沟通非常关键。网络安全领域的知识更新快，单一的机构很难掌握全部的最新资讯与技术。积极地参与各种安全社区的活动，例如著名的网络安全技术论坛，并组织安全专家与行业同仁分享他们的经验和观点。从论坛上，我们可以解其他机构对新型网络攻击的有效对策，例如对零日漏洞采取紧急处置办法等。另外还参加行业安全联盟和同行的共同研究项目。比如，联合分析某一行业所面临的常见网络安全威胁、共同开发有针对性防御解决方案等。通过这种跨组织间的沟通与协作，可以获得更多的安全资源及信息，从而为局域网络多层防御体系的优化提供一种新的思路与方法，增强其在复杂网络背景下的安全防护能力。

4 结语

在信息技术高度迭代的今天，建设和优化局域网络多层防御体系是确保网络安全的中心工作。它将系统论和网络安全工程理念有机地结合在一起，凭借其深度，动态和协同等防御特性构建局域网络全周期防护屏障。该系统既是一种技术上的融合，也是网络安全战略布局中的重点表现。通过不断探索各层防御协同，加强评估测试，跟上技术革新及推动安全交流等措施，不断提高自身的弹性抗毁能力和总体安全，为局域网络在复杂多变的数字生态中稳健运行提供坚实支撑，成为抵御网络威胁、守护数字资产的有力保障。

参考文献：

[1] 裴辰晔 . 电力系统网络安全中的多层协同防御模型分析 [J]. 电子技术 ,2024,53(12):240–241.

[2] 赵一畅 . 大数据时代的网络空间安全风险与防御 [J]. 数字通信世界 ,2024,(10):75–77+80.

[3] 简丽琼 . 基于大数据及人工智能技术的计算机网络安全防御 [J]. 软件 ,2024,45(09):7–9.

[4] 王勇亮 , 谭远波 , 郑学通 . 基于深度学习的网络安全主动防御策略研究 [J]. 工业信息安全 ,2024,(04):59–66.