电子政务网微隔离技术应用的安全域划分与访问控制策略研究

李志飞

内蒙古自治区大数据中心，内蒙古自治区呼和浩特市新城区，010010；

摘要：信息技术在政府管理中广泛应用，使电子政务网成为提升政府工作效率、优化公共服务的重要支撑，但它面临的安全威胁日益复杂，传统安全防护手段已无法满足需求。本文深入研究微隔离技术在电子政务网中的应用，通过合理划分安全域、精准制定访问控制策略来构建更具弹性和适应性的安全防护体系，先阐述电子政务网的安全挑战和微隔离技术原理，详细分析安全域划分原则与方法，探讨访问控制策略制定和实施要点，再结合实际案例评估应用效果，为提升电子政务网安全性提供理论支持和实践参考。

关键词：电子政务网；微隔离技术；安全域划分

DOI：10.69979/3041-0673.26.01.007

引言

政府部门实现信息化办公、信息共享与对外服务关键得靠电子政务网这个涵盖政务办公自动化、信息发布、在线服务等核心业务的平台。近年来，云计算、大数据等新技术融入使电子政务网业务范围不断扩大、数据交互更频繁，虽然政府工作效能提升了，但网络安全也面临着前所未有的挑战。外部网络攻击手段不断出新，黑客、恶意软件对电子政务网攻击越来越猖獗，他们企图窃取敏感政务数据、破坏系统运行，内部而言电子政务网各部门业务系统众多、网络结构复杂，不同安全级别的数据和应用混在一起，传统靠边界防护的安全措施无法应对内部安全威胁的扩散。这种情况下，引进先进的微隔离技术科学划分电子政务网安全域并制定有效的访问控制策略对保障电子政务网安全稳定运行是很急迫的需求。

1 电子政务网安全现状与挑战

1.1 安全现状

多数电子政务网目前初步构建起包含防火墙、入侵检测系统（IDS）、防病毒软件等的基础安全防护体系，在网络边界防火墙挡住外部非法网络访问、IDS 实时监测网络流量中的攻击行为且防病毒软件使终端和服务器免遭病毒侵害，部分地区还按业务类型、涉密程度等将网络分成政务内网、政务外网、互联网接入区等不同区域进行安全域划分并在区域边界设置安全设备控制访问，不过实际运行中这些传统安全措施的局限性慢慢暴露出来。

1.2 面临的挑战

1.2.1 内部威胁扩散

电子政务网内部有着大量业务系统和数据且安全级别各有不同，内部某一终端或者服务器要是遭受攻击，传统边界防护设备很难拦住攻击在内部网络横向扩散，就像一台普通办公终端感染了恶意软件，该恶意软件也许会借助网络共享、未授权端口之类的在内部网络快速传播从而感染其他重要业务系统，导致严重的数据泄露或者系统瘫痪。

1.2.2 云化与虚拟化带来的新问题

电子政务网朝着云平台迁移且虚拟化技术被广泛运用，这使网络边界模糊起来，虚拟机在虚拟网络里通信，而传统安全防护设备基于物理网络边界，对虚拟机间流量难以有效监控和管控，云平台是多租户环境，底层基础设施可能被不同租户业务共享，若某一租户被攻击，安全风险就容易殃及其他租户。

1.2.3 复杂网络结构下的访问控制难题

众多部门和业务系统被电子政务网涵盖且其网络结构复杂，各部门业务需求不同访问权限设置繁杂，在实际运行时业务变更、人员调整等因素常使权限管理陷入混乱进而部分用户权限超出工作所需且安全风险增加，传统的访问控制策略基于 IP 地址和端口号难以适应这种复杂且动态变化的网络环境而无法实现精准的访问控制。

2 微隔离技术原理及优势

传统网络边界防护理念被微隔离技术摒弃，它以应用和工作负载为核心在网络内部实现细粒度安全防护，并且通过在服务器、虚拟机等计算节点部署轻量级代理来实时采集网络流量、学习业务系统正常访问关系以构

建动态访问模型，网络流量产生时代理按照模型实时检测，合法流量才被允许通过，异常或未授权流量则被拦截，就像精准限定业务系统与指定数据库的交互端口那样。

传统安全技术和微隔离比起来，微隔离有着明显的优势，传统技术在访问控制这块靠的是 IP 地址、端口号，粒度很粗，而微隔离深入到应用层，依据应用标识、用户身份等多维度信息，把每个进程和网络连接都精准管控起来，从而让安全漏洞少很多；在动态网络环境里，传统策略配置是静态的，业务一变就难以适应，微隔离能一直学习流量，自动察觉环境变化并实时调整策略，从而保障新应用部署安全；在应对内部威胁时，微隔离把网络划分成好多微小安全区域，若某个区域被攻击，它能严格限制范围，防止恶意软件横向传播，有效保护核心业务和数据安全。

3 基于微隔离技术的电子政务网安全域划分

3.1 划分原则

电子政务网运用微隔离技术划分安全域得遵循三大原则，业务相关性原则是要根据业务系统功能、流程和数据交互关系，把关联紧密的系统划到同一个安全域，行政审批系统和相关的信息查询、共享系统，从而保证业务连贯、数据流转顺利，方便制定统一安全策略，安全等级相似性原则需按照数据敏感程度、系统重要性和安全风险等级，将安全需求差不多的系统和数据归在同一域，涉及国家机密等核心系统分到高安全等级域严格防护，一般性公开系统设为低安全等级域适度防护，以做到精准防护和资源合理分配，最小化通信原则是减少安全域之间不必要的通信，保证各域相对独立，必要通信要经过严格授权，降低风险传播，非关键业务域和核心业务域只在必要时通过特定安全接口通信，严格控制访问，有效控制攻击范围。

3.2 划分方法与步骤

电子政务网可这样实施基于微隔离技术的安全域划分：第一步梳理分析业务，全面知晓各业务系统功能、数据流向、用户群体以及系统交互关系，通过绘制业务流程图、数据交互图等弄明白系统关联，为划分打基础；第二步评估安全等级，按照数据敏感程度、系统重要性以及潜在威胁构建含数据保密性、完整性等指标的评估体系，量化评估后将系统分成高、中、低不同安全等级；第三步基于业务相关性和安全等级相似性原则，综合网络拓扑、现有防护和业务发展情况合理划分安全域，确定各域边界、所含资源并绘制拓扑图；第四步规划安全域间隔离与通信，利用微隔离技术实现逻辑隔离，依据业务需求明确通信类型、协议、地址等要素并配置访问控制策略，限制公共服务域对核心域的数据查询请求以保障通信安全。

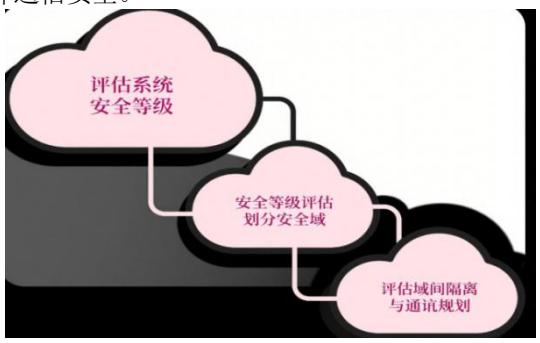

图 1 基于微隔离技术的电子政务网安全域划分步骤示意图

4 基于微隔离技术的访问控制策略制定与实施

4.1 策略制定依据

4.1.1 业务需求分析

电子政务网各业务系统的具体业务流程和操作要求需要深入了解并且明确不同用户角色在业务开展时对各类资源（如数据、应用程序、服务器等）的访问需求，以政府审批人员处理行政审批业务为例，他们需要访问审批系统、相关政策法规数据库以及企业申报信息库等资源，按照这种业务需求制定出相应的访问控制策略，审批人员工作才能顺利开展并且防止越权访问。

4.1.2 用户角色与权限划分

电子政务网用户要依据工作职责、职位级别等因素分类确定不同用户角色，如管理员、普通办公人员、公众用户之类的，并且要明确每个用户角色在不同安全域对各类资源的操作权限，如读取、写入、修改、删除等，管理员一般在所有安全域内资源有最高管理权限，能进行系统配置、用户管理等操作，普通办公人员只有跟自己工作相关业务系统和数据的特定操作权限，只能读取处理本部门业务数据而不能修改其他部门数据，公众用户只能访问公共服务安全域内公开信息而无法访问内部业务数据。

4.1.3 安全风险评估结果

依据电子政务网安全风险评估结果，考虑不同资源面临的安全威胁和遭受攻击可能产生的损失来调整优化访问控制策略，高风险资源像存有敏感政务数据的服务器需实行更严格的访问控制策略，对访问源、访问时间加以限制并采用多因素认证等法提升访问安全性，低风险资源在保证基本安全的条件下可适当放宽访问控制来提高工作效率，就好比某个安全域内存储大量公民个人隐私数据的数据库近期网络攻击风险较高，就可以

临时强化对这个数据库的访问控制，除限制特定用户角色访问外再增添动态验证码、指纹识别等多因素认证方式防止非法访问。

4.2 策略实施要点

4.2.1 策略部署与更新

微隔离技术的管理平台可把制定好的访问控制策略精准部署到对应的安全域和计算节点，并且要确保策略在网络里一致有效，防止策略冲突或者遗漏，在业务发展、网络环境变化和新安全威胁出现时，得及时更新调整访问控制策略，建立策略更新机制并定期审查优化策略，使其一直满足电子政务网的安全需求，电子政务网新增业务功能且有新用户角色和数据访问需求时，就要及时在微隔离管理平台更新相关访问控制策略，保障新业务安全运行。

4.2.2 多因素认证与身份管理

要增强访问控制的安全性就得引入多因素认证机制，除了传统的用户名与密码认证外，还要结合短信验证码、硬件令牌、生物识别（像指纹识别、人脸识别）等多种方式验证用户身份，并且要加强身份管理，建立完善的用户身份信息数据库，做好用户身份信息集中管理与维护，实时监控用户账号使用情况，及时发现与处理异常登录行为，用户登录电子政务网核心业务系统时，系统不仅让用户输入正确的用户名和密码，还会向用户绑定手机发送验证码进行二次验证，若用户账号有异地登录等异常情况，系统马上就会警报并采取冻结账号等措施保障安全。

4.2.3 实时监控与审计

微隔离技术的流量监测功能被利用起来以实时监控安全域内和安全域之间的网络流量，记录与审计所有访问行为。经分析审计日志，可及时发现潜在安全风险与违规访问行为，如未经授权的访问尝试、异常流量模式等并建立安全事件预警机制，一旦检测到异常行为就马上将警报信息发给安全管理员以便及时采取应对措施，审计日志若显示某个普通办公用户非工作时间频繁试图访问高安全等级域内的敏感数据，系统就触发警报，安全管理员迅速介入调查，判断是否有安全威胁，采取冻结该用户账号、进行安全排查等相应处理措施。

5 案例分析

某省电子政务网覆盖省、市、县多级政府部门并承载政务办公自动化、行政审批、公共服务等众多核心政务业务，随着业务不断拓展、网络环境日益复杂，该电子政务网面临严峻安全挑战且内部安全威胁频频发生，传统安全防护体系难以满足实际需求，于是某省为提升网络安全性引入微隔离技术来进行电子政务网的安全域划分和访问控制策略优化。

表 1 某省电子政务网微隔离技术应用前后效果对比表

评估维度	实施前情况	实施后效果
内部安全威胁事件数量	内部威胁频发	大幅下降 78%
攻击拦截情况	传统防护手段拦截效果有限	三个月内外部非法访问尝试被拦截达 12.6 万次且内部违规访问行为被拦截 8900 余次，拦截准确率达 99.2%。
用户权限违规操作	权限管理混乱，违规操作较多	普通办公人员越权访问减少 92%，公众用户恶意访问内部数据行为下降 95%
账号安全	用户账号存在被盗用风险	账号被盗用实施非法访问的风险降低 85%以上

6 结论

微隔离技术在电子政务网中的应用是本文的核心，文中深入研究了安全域划分与访问控制策略。微隔离技术具有细粒度访问控制、能适应动态网络环境、有效遏制内部威胁扩散等优势，凭借这些优势可构建更高效更灵活的电子政务网安全防护体系。安全域划分要遵循业务相关性、安全等级相似性、最小化通信等原则，访问控制策略需依据业务需求、用户角色与权限、安全风险评估结果制定，再结合多因素认证、实时监控审计等实施要点就能显著提升电子政务网的安全性，实际案例应用效果评估也证实了该技术和策略在减少安全威胁事件数量、提升攻击拦截率、规范用户权限管理等方面是有效的。

参考文献

[1]王淼.电子政务系统安全域划分与等级保护方法的研究与应用[D].广东工业大学,2010.DOI:10.7666/d.y1745626.

[2]佚名.基于微隔离的企业内网流量保护方法及系统:CN202410456171.9[P].CN118101325A[2025-06-19].

[3]杜虹.电子政务中安全域和网络划分与控制[J].信息安全与通信保密,2003,000(007):48-50.DOI:10.3969/j.issn.1009-8054.2003.07.018.