云计算环境下的网络安全技术应用研究

季凌云
（宁夏建设职业技术学院，宁夏 银川 750001）

摘要：在信息技术领域，云计算是一种极为重要的服务模式，正在随着各个领域的信息化发展而成为支撑相关企业正常运行的重要支撑。这一服务模式具有可靠、灵活、高效等优势，为企业发展带来更多新的可能，同时也带来了更为严峻的网络安全问题。故而，文章在分析网络安全运维技术需求的基础上，结合云计算环境探讨网络安全面临的各种不同类型威胁，提出网络安全技术及其应用策略，以期能够为云计算的安全应用提供借鉴。

关键词：云计算环境；网络安全技术；应用路径

引言

人随着云计算这一服务模式逐渐深入各行各业，云计算技术在数据处理与存储方面的优势逐渐凸显，受到了企业的广泛青睐。鉴于云计算技术的诸多优势，越来越多的企业开始将业务迁移到云端，网络安全技术应用不仅关系着企业业务流程的正常运行，而且可能对企业决策与发展造成一定影响。近年来，网络安全问题也日益严峻，基于云环境的隐私保护与数据安全已然成为用户需要深入研究的重要问题。

一、网络安全运维技术需求

（一）网络漏洞检测

在网络安全运维工作中，网络漏洞监测是极为重要的环节，用户通过实时监测网络系统与设备的漏洞，能够及时发现潜在的安全风险，继而采取相应的防范与修复措施。云计算环境下，网络漏洞检测工作更为重要和复杂，需要满足以下几个方面的要求。其一，漏洞扫描技术需要满足大规模网络系统与设备的扫描需求，适应处于动态变化之中的网络环境，所以该技术应兼具实时、准确、高效等特点。网络漏洞监测中，漏洞扫描处于基础地位，用户可以通过实时或者定期扫描网络系统与设备发现其中的安全漏洞。其二，漏洞挖掘技术需要与云计算平台架构及其应用保持适应性，帮助用户及时发现配置文件、源代码、网络设备中潜在的安全风险。其三，漏洞扫描技术需要满足预警和应急响应需要，通过实时收集、分析、处理漏洞信息，及时发现并启动相应应急机制应对潜在的网络攻击，对安全漏洞进行修复。

（二）网络流量管理

网络流量管理是网络安全运维工作中的另一项重要内容，需要用户通过实时监控、分析、控制网络流量对规范网络攻击进行有效防范，从而保证网络安全运行。在网络流量管理领域，流量监控技术是基础，先进的流量监控技术能够帮助用户更好地应用云计算环境下的复杂网络拓扑、多种类型应用以及大规模网络流量，实现对网络流量的更全面、有效实时监控，及时发现异常流量，继而选择相应的防范策略。云计算环境下，流量控制技术应具有实时、高效、灵活的优势，满足深度分析网络流量，及时发现异常行为、潜在网络攻击的需求，保证异常流量检测的效率与准确性。

二、云计算环境下网络安全威胁分析

（一）常见的网络安全威胁类型

跨站脚本攻击（XSS）、SQL 注入以及分布式拒绝服务（DDoS）攻击等是云计算环境下常见的网络安全威胁类型，对用户网络完全的威胁较大。其中，跨站脚本攻击（XSS）是一种在网页中注入恶意脚本的攻击方式。当用户受到该类型攻击，并浏览受污染页面时将会执行该恶意脚本，导致用户信息被窃取或者执行其他恶意操作。SQL 注入是一种针对数据库驱动的攻击方式，攻击者通过在应用或者网站的数据库入恶代码，绕过其安全机制，执行数据查询或者其他操作。云计算环境下的用户数据库中的数据高度集中，一旦被注入恶意 SQL 代码往往会导致大量重要信息泄露。分布式拒绝服务（DDoS）攻击通过向目标服务器发出大量请求造成拥堵，从而使合法用户难以访问，对攻击对象运行情况影响较大。云计算环境下，用户通常选择将服务托管于集中式的数据中心，造成这种攻击时不仅会影响目标服务器运行，而且可能会严重影响整个云平台，致使其瘫痪，无法提供服务。

（二）云计算环境下特有的安全威胁

在云计算环境下，需要通过虚拟机对不同的用户与应用进行隔离，一旦虚拟机软件出现漏洞，非法人员就可能抓住漏洞乘机“逃逸”出虚拟机，继而对宿主机和其他虚拟机进行攻击，对云计算环境隔离性甚至是整个云平台进行破坏，导致其无法正常运行。此外，云计算平台还会受到侧信道攻击，这是一种通过分析软件或者硬件系统运行过程中形成的物理泄露信息（如功耗变化、电磁辐射等）非法获取文件信息的攻击方式，相较于其他攻击方式更为隐蔽，更难以被传统安全防护措施识别、防范。云计算环境下，同一物理硬件往往承载着大量虚拟机，而且侧信道攻击方式五花八门，令人防不胜防。

三、云计算环境下的网络安全防护技术应用

（一）传统网络安全技术的适用性评估

1. 防火墙技术

随着云计算技术在各个领域的广泛应用，网络信息安全防护

工作责任更加重大，用户需要合理使用防火墙技术将病毒与黑客攻击屏蔽在外。防火墙技术是一种将网络外部与网络内部隔离开来的基础防护措施，通常用于控制与监控网络流量，对未授权访问行为进行阻止，继而保证网络安全。在云计算环境下，这种基础性网络安全防护技术仍然发挥着重要作用，但是需要用户对防火墙技术应用方式进行合理选择。相对而言，云计算环境具有弹性大、动态性强的特点，基于固定规则的传统防火墙技术往往难以适应应用环境，用户应采用动态化、智能型防火墙技术，以便更有效应对各种攻击，维护网络信息安全，比如应用层防火墙、基于行为的防火墙等都是云计算环境中较为常用的网络安全防护技术。同时，由于云计算环境中同一物理硬件往往承载着大量虚拟机，技术人员还需要充分考虑不同虚拟机之间的隔离问题，保证它们的网络流量被有效隔离，从而隔绝一些潜在风险。

2. 入侵检测系统（IDS）/ 入侵防御系统（IPS）

IDS/IPS 是基于云计算环境进行网络安全防护工作的重要技术手段，用户可以通过人工智能、机器学习技术提升其检测能力，加强对网络流量的分析与学习，从而更为精准地辨别潜在攻击与异常流量。另外，为了进一步提升响应、处置安全事件的速度，提升网络安全性，用户还要重视 IDS/IPS 和云平台的安全管理系统的集成，使安全防护措施更为适应云计算环境。考虑到云计算环境弹性强的特点，用户可以选择具有灵活性、可扩展性的 IDS/IPS，进而能够结合具体需求作出迅速调整与部署，比如具备灵活配置安全策略、动态删除或者添加检测节点等功能的 IDS/IPS 能够更好地满足云计算环境下的网络安全防护需求。

3. 数据加密技术

数据加密技术主要由加密技术与解密技术组合而成，能够根据用户前期所设定好的规则为整个网络中的数据与信息提供保护。其中，数据加密技术要求用户在前期设定好相关规则，为网络安全防护提供依据；数据解密技术能够依据译文规则对网络信息进行反向还原操作，使合法用户获得目标信息。当前，这种网络安全防护技术已经较为成熟，能够对一些较为重要的数据信息进行加密处理，提高其安全防护等级。在云计算环境下，它具有良好的适应性，是一种关键性数据安全保障措施。云计算服务涉及的数据存储与传输量较为庞大，用户采用数据加密技术进行网络安全防护工作时，一方面要充分考虑加密性能对系统性能形成的影响，以及加密密钥管理、加密算法强度等方面因素，另一方面要考虑多租户共享同一物理平台的需求，对用户数据进行有效隔离，并选择相应访问控制机制和隔离技术防止非法访问，降低数据破坏或者泄漏的风险。

（二）针对云计算环境的特殊安全防护技术

1. 虚拟机安全隔离技术

在云计算环境下，虚拟机安全隔离技术是一项较为常用，且十分关键的安全防护技术。由于云计算环境下的同一物理服务器上可能同时运行多个虚拟机，需要保证它们之间彼此隔离，此处所讨论的“隔离”既包括网络层面的隔离，又包括内存、CPU、存储等资源的隔离。为了达到“隔离”效果，用户需要采用 AMD 的 V 技术或者 Intel 的 VT-x 技术实现硬件层面的隔离。它们是基于硬件辅助的虚拟化技术，能够通过虚拟机监视器（VMM）或者容器化技术进一步实现虚拟机之间的资源隔离，提升网络运行安全性。此外，用户管理策略的选择也十分重要，可以通过落实最小权限原则、定期对虚拟机安全补丁进行更新、监控虚拟机系统行为与网络流量等多种方式加强管理，加强对网络的安全防护。

2. 虚拟化环境下的安全策略

为了维护云计算环境安全运行，用户要基于虚拟化环境采用有效的安全策略，预防各种网络攻击。其一，是对虚拟机的镜像进行安全审核与验证，保证其来源可靠而且未被篡改。其二，是对虚拟机进行定期的漏洞评估和安全扫描，旨在及时发现潜在的安全问题，并进行修复。其三，是采用合理网络访问控制策略，从而对虚拟机之间的非必要通信进行限制，达到减少攻击面的目的。其四，是对数据的隐私保护与安全性进行特别关注，比如通过加密技术进一步保护存储或者传输中的数据，利用多因素身份验证与强密码策略对访问控制进行强化。

3. 云安全访问控制机制

它通常基于身份与访问管理（IAM）系统实现网络安全防护，能够保证只有经过授权的用户才可以访问云计算资源，避免数据信息泄漏。IAM 系统具备细粒度的访问控制功能，支持管理员结合用户角色、需要、职责进行权限分配，达到降低潜在安全风险的目的。此外，云安全访问控制机制还包括联合身份验证、单点登录（SSO）、多因素身份验证等身份验证措施，用户联合采取不同云安全访问控制措施能够更有效保证云计算资源访问者身份的合法性，将数据泄露与未经授权访问等风险降到更低。

（三）新兴技术在云计算安全防护中的应用

1. 人工智能（AI）与机器学习（ML）在云安全防护中的应用

随着信息技术不断创新发展，AI 与 ML 等先进技术得到广泛应用，为云计算安全防护带来了新的技术支持。其一，是异常检测，机器学习模型能够通过分析用户行为、系统日志、网络流量等数据，自动检测出可疑活动和异常模式，从而加强云计算安全防护。比如，当某用户的登录行为与其历史行为模式差异性较大时，系统可以作出相应判断，并自动启动警报，进一步验证其身份。其二，是威胁预测，机器学习模型能够根据历史数据与目前的安全态势，对未来可能发生的威胁类型进行预测，继而提前采取相应的防范措施，减少网络的安全风险。其三，是自动化响应，AI 能够结合自动化工具进行对安全事件的自动响应，维护云计算安全运行，比如它检测到恶意攻击时，能够自动将被感染的数据或者系统隔离开来，阻止攻击扩散。

2. 区块链技术在提升云安全中的作用

区块链是基于现代信息技术形成的数字分类账本，能够对任何有价值的信息进行记录，其在提升云安全防护等级方面发挥着十分重要的作用。首先，区块链技术的应用，更有效地保证了存储在云中的数据免受篡改。区块链准确地对每次数据变更进行记录，形成不可更改的历史记录，该记录为溯源、追踪安全事件提供可靠依据，更大程度上确保数据完整且真实。其次，区块链技术的应用能够实现分布式访问控制与身份验证，区块链基于加密技术与智能合约控制用户访问行为，保证唯有经过授权的用户才可以访问敏感数据或者执行关键操作。最后，区块链具备可追溯性与透明性优势，让安全审计更为便捷，用户利用其记录、验证客户合规性，能够在满足监管要求的同时，提高客户信任度。

（四）安全意识培训的开展

云计算环境下，用户要增强防范意识，对网络安全防护工作引起足够重视，并采用相应防护手段应对各种不同攻击，确保网络信息和数据的安全使用。一方面，各个单位与企业要定期开展网络安全培训活动，强化员工主体的安全防范意识与技能。通常而言，员工网络安全意识与技能培训主要涉及以下几个方面：首先，是普及网络安全基本概念、常见攻击类型，以及不同攻击类型可能造成的破坏，促使员工对网络安全引起足够重视；其次，是讲解强密码设置方法，降低密码被破解或猜测的风险；再者，指导员工对网络钓鱼邮件、社交过程攻击进行识别与防范，比如讲解典型案例，以及当前常见的攻击手法与特征；最后，对个人与组织数据重要性进行讲解，指导员工如何妥善处理敏感信息，避免相关数据发生泄漏。另一方面，各个单位与企业要通过相应培训活动强化员工识别和应对网络威胁的技能。比如，在培训活动中模拟网络攻击的真实场景，促使员工结合实践体验学习如何应对威胁，确保其在遭遇类似情况时迅速且正确地做出反应；介绍入侵检测系统、杀毒软件、防火墙等常用安全防护工具，使员工充分了解、掌握它们的使用范围和方法。

（五）移动设备安全管理的强化

近年来，各种移动设备在个人与企业中迅速普及，平板电脑、手机等已然成为人们工作、生活中不可或缺的伙伴。它们为人们工作、生活带来各种便捷的同时，也为网络安全带来了新的隐患。云计算环境下，用户要加强移动设备安全管理，通过各种有效性、针对性的安全管理措施对一些潜在风险进行防范。比如，用户可以为移动设备安装防恶意攻击程序和杀毒软件，实时监测设备的安全状态，从而及时发现并消除潜在威胁；定期更新应用程序与操作系统，利用其搭载的最新安全防护功能降低被攻击风险。此外，用户还可以通过远程擦除功能与密码锁加强数据安全防护，比如在移动设备上设置较为复杂的密码锁，增加非法用户访问难度，或者在设备被盗或者遗失后采用远程擦除功能命令设备清除所有数据。

（六）定期安全审计的实施

1. 对网络系统、软件、设备进行定期审计

为了增强云计算环境下的网络安全防护，用户可以对网络系统、软件、设备进行定期审计，其具体操作步骤如下。第一，拟定审计计划：明确审计目标、范围，并列出时间表，保证后续审计工作得到有序开展。用户要注意审计计划覆盖所有网络设备、软件以及系统，能够做到全面检查、深入剖析，有效识别、防范潜在风险。第二，组建专业审计团队，团队由具备网络安全知识与技能的专业人员组成，主要负责执行审计计划并出具审计报告。通常而言，该团队成员包括软件开发人员、系统管理员、网络安全专家，以便审计计划得到全面、顺利执行。第三，通过自动化审计工具开展相关工作，提升审计准确性与工作效率。最后，记录并分析审计结果，该环节需要详细记录审计过程中发现的问题与漏洞，并对记录的内容进行深入分析。用户通过对比分析结果与历史审计结果，能够发现安全状况变化趋势，做出相应判断，为后续修复与改进工作提供指导。

2. 及时发现并修复潜在的安全漏洞

用户在对网络系统、软件、设备进行定期审计的基础上，要采取相应措施修复潜在的安全漏洞，加强对网络的安全防护。为了及时发现并修复潜在的安全漏洞，用户需要做好以下几个方面的工作：首先，制定清晰、明了的漏洞管理流程，该流程包括漏洞的发现、报告、修复、验证等 4 个环节，以及各个环节的责任人与完成时间；其次，根据发现的安全漏洞开展风险评估与分析工作，即结合漏洞的严重性与影响范围提出相应修复方案；再次，依据风险评估结果拟定修复计划，并尽快落实；最后，在完成修复工作之后，全面测试、验证系统，保证修复漏洞过程中未产生新的安全问题。

结语

综上所述，随着云计算这一服务模式逐渐深入各行各业，并成为支撑相关企业正常运行的重要支撑，网络安全问题也日益严峻，用户需要深入研究云计算环境下的网络安全技术应用路径，为企业经营与发展提供安全网络环境。具体到网络安全维护工作实践中，用户要明确网络安全运维技术需求，了解云计算环境下网络安全面临的各种不同类型威胁，并根据实际情况选择相应的网络安全技术，以提升网络安全等级，营造安全网络环境。

参考文献：

[1] 高松涛 . 新时代病毒防护技术在计算机网络安全中的运用 [J]. 木工机床 ,2024,(04):35-39.

[2] 万静静 . 基于网络安全防护技术的智控平台应用研究 [J]. 机械工程与自动化 ,2024,(06):205-207.

[3] 苟伟 . 应对生成对抗网络与自然语言处理技术驱动下的网络安全策略与防护方法 [J]. 中国信息界 ,2024,(07):86-88.