本文引用格式：张红金,刘维.国产云平台安全体系策略探究[J].自动化与信息工程,2022,43(2):23-28.

ZHANG Hongjin, LIU Wei. Research on security system strategy of domestic cloud platform[J]. Automation & Information Engineering, 2022,43(2):23-28.

国产云平台安全体系策略探究

张红金[1,2]　刘维[1,2]

（1.工业和信息化部电子第五研究所，广东 广州 510610

2.基础软硬件性能与可靠性测评工业和信息化部重点实验室，广东 广州 510610）

摘要：针对国产云平台的安全性既要应对传统 IT 技术带来的安全威胁，又要面对虚拟化等技术带来的新风险问题，进行安全体系策略探究。首先，提出构建以安全策略、防护策略、检测策略和响应策略为核心的国产云安全防御模型；然后，从物理、网络、主机、应用、数据 5 个层面阐述国产云平台安全体系构建的关键技术，以期为国产云平台安全体系策略的相关研究提供有益探索。

关键词：国产云；云平台；安全体系；安全防御模型

中图分类号：TP393.4　　**文献标识码：**A　　**文章编号：**1674-2605(2022)02-0004-06

DOI：10.3969/j.issn.1674-2605.2022.02.004

0　引言

信息技术应用创新产业的蓬勃发展催生了国产云平台快速成长，但随之而来的风险也不容小觑。随着云计算攻击逐年增多，我国云平台的安全事件也逐渐增长；同时软件定义网络、人工智能等技术的引入，使云计算的安全保障任务更加艰巨[1]。新的云计算攻击方式层出不穷，原有的安全措施存在失效的风险，且云计算系统也因种类多、数量大、环境差异大等因素而管控日渐困难，安全体系面临新的挑战[2]。因此，根据国产云平台特点，构建其安全体系已迫在眉睫。

1　安全防御模型

国产云平台安全体系遵循“水桶效应”，即最脆弱部分决定系统的整体安全。为此，本文构建一种基于国产云的安全防御模型——SPDR 模型，即以安全策略（security）、防护策略（protection）、检测策略（detection）和响应策略（response）为核心的安全模型。SPDR 模型以安全策略为重心，根据事前防护（事前制定相应的防护策略）、事中检测（事中按所制定的检测策略进行实时检测，发现潜在的安全威胁）、事后响应（事后及时启动对应的响应策略）的工作模式，打造国产云平台的整体防御体系。基于国产云的技术特点，构建国产云平台整体防御体系时需遵循云原生、安全功能模块化、纵深防御、可运营 4 个基本原则。

1）云原生。国产云平台中，根据业务资源和业务系统实际状况有针对性地部署安全防范措施。

2） 安全功能模块化。各功能模块既可独立执行自身的安全任务，又可与其他模块组成安全防御面。

3） 纵深防御。为应对多样化的攻击方式和攻击途径，构建纵深防御体系，增加攻击难度与攻击成本。

4） 可运营。国产云平台安全体系能够为用户提供安全运营的工具和服务。

2　安全体系构建

2.1　整体构建策略

网络入侵/攻击绕不开物理、网络、主机、应用和数据这 5 种路径中的一种或多种。为此，着重针对上述 5 种路径构建安全防护能力，实现可运营的目的。以安全策略为核心的国产云平台安全体系框图如图 1 所示。

AUTOMATION & INFORMATION ENGINEERING

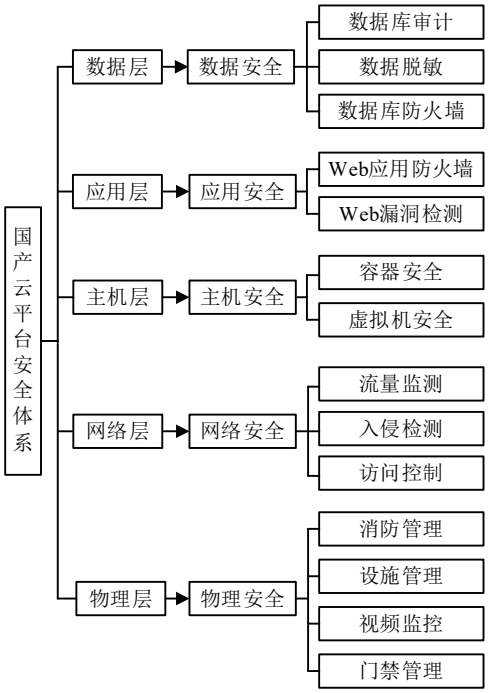

图 1　国产云平台安全体系框图

2.2　网络安全

国产云平台的数据节点较多，功能复杂，为实现网络安全简化设计的目的，阻断网络攻击波及到其他层面，将攻击影响降为最低，需要科学划分或隔离网络安全区域与业务层，实现边界高级防护[3]。

2.2.1　安全区域划分

为阻断网络攻击在云数据中心网络蔓延，将攻击影响最小化，对云数据中心网络进行安全区域划分和隔离，如图 2 所示。

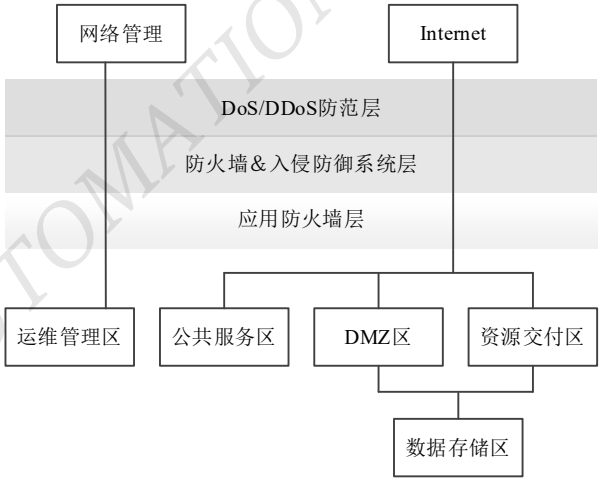

图 2　云数据中心网络安全区域划分和隔离示意图

1） 运维管理区。部署运维设施，运维管理员通过 VPN 接入本区域后，再通过此区域访问其他运维区域，但其他运维区域不能访问本区域。

2） 公共服务区。本区域内部署 IaaS、PaaS、SaaS 服务的相关控制部件、DNS、NTP 等。所有部件根据业务需求开放相应的权限，管理员通过内网访问管理本区域，用户通过 DMZ 区访问本区的部件和服务。

3） DMZ 区也称“非军事化区”。为解决安装防火墙后外网用户无法访问内网服务器而设立的一个安全系统与非安全系统之间的缓冲区。缓冲区位于内网和外网之间，在区内部署一些公开的服务器等设施，如企业 Web 服务器、FTP 服务器等。通过 DMZ 区既保护了内网，又对外网的恶意攻击设置了一道关卡。即使 DMZ 中的硬件设备遭到破坏，也不会对内网中的机密信息造成影响。

4） 资源交付区。提供计算、存储和网络等基础设施资源给用户，但用户彼此之间的基础设施资源相互隔离，任何一个用户未经允许无法访问其他用户的基础设施资源。

5） 数据存储区。部署存储系统，为用户提供隐私数据或私密信息的存储服务，但本区域同样要进行分区隔离。外网访问本区域必须通过 DMZ，其他访问也需执行相关的访问控制规则。

2.2.2　业务层划分

为确保用户业务不影响管理操作，确保设备不会脱离有效监管，在每个安全区域内，根据业务的隔离要求将国产云平台网络的通信平面划分为数据平面、业务平面、运维管理平面、数据存储平面等，保证不同业务的网络通信流量可合理分流[4]。

2.2.3　边界安全防护

国产云平台的网络安全防护除考虑网络安全措施外，还需考虑边界的安全防护。

1） DDoS 防护。在国产云平台的数据中心边界部署 Anti-DDoS 设备，用于检测异常或大流量攻击。为了给用户提供 DDoS 高防服务，用户根据业务类型设置 Anti-DDoS 设备的阈值参数，定期查询攻击和防御信息。DDoS 工作原理流程图如图 3 所示。

AUTOMATION & INFORMATION ENGINEERING

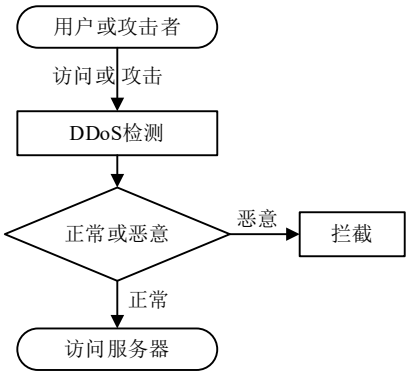

图 3　DDoS 工作原理流程图

2） 网络入侵防护。为感知和拦截恶意攻击，需在外网、安全区域等边界处部署 IPS 设备，进行实时在线监测、流量分析以及阻断等。另外，IPS 还提供信息定位和异常监测功能，充分保障应用程序与网络基础设施的安全。

3） Web 安全防护。为应对 Web 的各类攻击，Web 安全防护可保护 Web 应用服务和系统。

2.3　主机安全

国产云平台通过虚拟化平台对 CPU、内存、I/O 等物理资源抽象，并将这些物理资源统一分配、管理和调度。一个服务器上可构建多个虚拟云主机的运行环境，多个虚拟云主机既能独立运行也能同时运行，但彼此间相互隔离[5]。

为保证主机及其环境安全，主机操作系统实行最小化原则，对系统管理员执行访问控制权限，对其登录、退出、运维等操作实行严格的日志审计。

统一虚拟化平台（unified virtualization platform，UVP）确保虚拟机正常工作，严禁某一虚拟机对其他虚拟机或 UVP 进行攻击。UVP 通过 CPU、内存和 I/O 等隔离技术实现云主机操作系统之间相互隔离，确保云主机运行安全。

2.3.1　CPU 隔离管理

虚拟化平台通过硬件辅助虚拟化技术实现。CPU 隔离有多种途径，包括 Root 和 Non-Root 的切换、权限分配、VCPU 虚拟资源的分配与切换等。虚拟 CPU 隔离包括虚拟机与虚拟机之间隔离、虚拟机与虚拟化平台之间隔离、虚拟机内的权限划分与分配。基于 CPU 的隔离机制，通过 UVP 控制虚拟机对物理基础设备、设施及虚拟化环境等的访问，实现虚拟机与虚拟机、虚拟机与虚拟化平台之间信息和资源的隔离。

2.3.2　内存隔离管理

任何一台虚拟机只能访问自身的内存资源，且虚拟机内存资源与实际物理内存之间为一一对应的映射关系。虚拟机需通过虚拟层的地址转换才能访问其内存，且只能访问指定的物理内存，不可访问虚拟化平台的内存。

2.3.3　I/O 隔离管理

虚拟机所需的虚拟化磁盘、虚拟化网卡以及键盘、鼠标等 I/O 设备均由虚拟化平台提供，并且这些设备相对独立，避免共享同一设备造成信息泄露的风险。虚拟磁盘与虚拟化平台上的镜像文件一一对应，虚拟机之间无法访问彼此的 I/O 等物理设备，实现 I/O 设备真正意义上的隔离。

2.3.4　用户主机安全管理

用户主机安全管理通过国产云平台主机实现，需要重点防护云主机内的系统和软件。云主机安全工作示意图如图 4 所示。

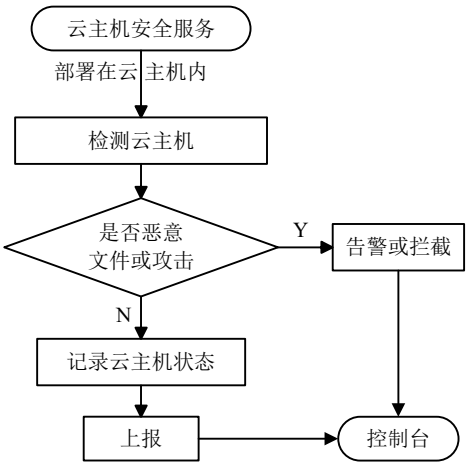

图 4　云主机安全工作示意图

国产云平台主机安全功能：

1） 基本安全功能，包括账户口令破解、恶意程序、漏洞等检测功能；

AUTOMATION & INFORMATION ENGINEERING

2） 其他安全管理功能，包括主机管理、基线配置管理、漏洞管理等高级安全风险；

3） 文件目录变更检测和文件完整性保护等功能，检测业务系统是否满足相关标准要求。

2.4 应用安全

Web 安全威胁在整个应用安全中达 70%左右，但大多数的Web安全威胁可通过Web应用防火墙消除，工作原理如图 5 所示。

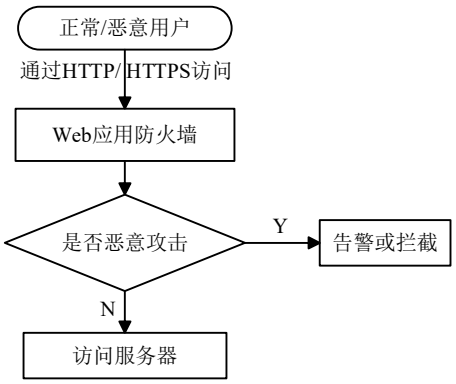

图 5 Web 应用防火墙工作示意图

Web 应用安全功能：

1） Web 攻击防御，能防御多数 Web 攻击，包括 XSS 攻击、CSRF 攻击、SQL 注入攻击、文件上传漏洞、DDoS 攻击等常见攻击类型；

2） 编码还原，实现混合编码还原、递归还原等；

3） CC 攻击防护，CC 攻击占用大量业务资源，影响正常业务，Web 应用防火墙对用户标识，通过设置阈值进行访问控制，拒绝阈值外的访问请求；

4） Webshell 防范，通过检测 HTTP(S)传输通道的信息，覆盖 Webshell 各类型，防止其带来威胁；

5） 自定义控制，借助 Web 应用防火墙的接口设置自定义的检测规则；

6） 隐私过滤，用户可自定义过滤规则，避免泄露自身的隐私、用户名、密码等相关信息，实现隐私过滤功能。

2.5 数据安全

国产云平台安全体系的核心任务是保护用户数据信息的机密性、完整性、可用性等，同时需要遵照数据相关安全管理标准，着重在身份认证、权限管理、访问控制、数据隔离、传输安全等方面采用安全技术、流程等保证用户数据安全[6]。

2.5.1 访问隔离策略

1） 统一身份认证访问控制。统一身份认证可集中管理用户和访问密钥等，对用户的管理和访问云资源权限进行控制。管理员使用统一身份认证管理和控制用户账号的操作权限。在多用户协同操作的情况下，统一身份认证可避免与其他用户共享账号密钥的风险。通过设置用户登录验证、用户密码、访问权限等策略以及配置用户最小权限，确保用户账户安全。

2） 数据隔离。对不同用户间的网络实行深度隔离，用户完全控制自己的虚拟网络，且无法获取其他用户的数据。实现不同用户在网络层上的完全隔离：① 结合 VPN 实现虚拟私有云与用户内网传数据中心之间的相互连接，应用和数据可从内网迁移到云端；② 在虚拟私有云上，实现用户更深层次的网络隔离需要配置一定的安全访问规则。

2.5.2 安全传输策略

客户端到客户端、客户端到服务端、服务端到服务端之间的信息数据通过公共通道传输。为此，信息数据的安全保护尤为重要，通过 VPN、传输层安全协议与证书管理服务等进行保护。

1） VPN 属于远程访问，是远程访问用户与虚拟私有云之间的一条安全加密通道，将数据无缝扩展到国产云平台，确保数据传输过程中的机密性。数据中心与虚拟私有云之间通过 VPN 通道，可避免机密数据扩散风险。

2）传输层安全协议（transport layer security，TLS）与证书管理服务。数据主要通过 REST 和 Highway 两种方式传输。REST 通道根据 RESTful 标准向外发布服务，实现数据传输；Highway 是一种私有协议通道，性能高，适用于性能需求较特殊的场景。证书管理服务可实现可信身份认证与数据安全传输功能，提供一站式 SSL 证书的全生命周期管理。

2.5.3 安全存储策略

通过硬件安全模块为用户创建、管理密钥并保障

AUTOMATION & INFORMATION ENGINEERING

其安全，密钥的所有操作都需要控制、跟踪、记录，并符合审计。硬件安全模块是负责产生、管理、使用密钥并提供加密服务的一套硬件设备组合，用户可根据自身的需求在国产云平台上选择厂商、加密算法以及不同强度的云硬件安全模块[7]。

2.5.4 数据删除与销毁

1） 写“零”操作。在云操作系统中给新用户重新分配内存前，需对原内存进行清零处理，即写“零”操作，确保新启动的虚拟机中无法检测到原来的相关信息，即使通过软件工具也无法恢复物理内存中已删除的数据，最大程度地避免信息泄露。

2） 磁盘清零。防止利用数据恢复软件恢复磁盘中的数据。

3） 数据泄漏。采用机密数据加密存储功能，直接销毁数据的加密密钥来销毁或废弃该数据。

4） 数据删除功能。支持对原有废弃数据逻辑删除功能。

5） 硬盘报废处理。通过消磁、折弯或粉碎等方式清除物理硬盘中的数据，再报废物理硬盘，但要保存数据清除操作记录。

2.6 运维安全管理

运维安全管理主要包括账号管理、漏洞管理、日志和事件管理、业务管理与灾难恢复 4 个方面。

2.6.1 账号管理

1） 账号登录认证。运维人员登录个人账号管理系统时需进行双重认证，如密码+Ukey 认证等。个人账号用于登录 VPN，执行深度审计和日志审计功能，确保主机上的任何操作都能追溯到个人[8]。

2） 接入安全管理。内、外网运维人员通过运维平台统一管理数据中心的堡垒主机系统，对网络、服务器等进行本地与远程操作，实行设备资源统一管理。

3） 权限控制。权限控制分为账号生命周期管理和授权管理。其中账号生命周期管理包括开户、使用、口令、销户等管理；授权管理是根据业务的职责需求，实行基于角色权限的访问管理，登录人员无权访问其他，只能访问自身角色管辖的权限范围。

2.6.2 漏洞管理

1） 收集漏洞。鼓励产品供应商、网络公司及漏洞管理组织等定期提交产品的漏洞汇总明细信息，建立完善、科学的漏洞收集渠道；建立漏洞库，保证各个漏洞都能有效记录、溯源和闭环等；对漏洞库、安全论坛等实时在线监控，确保瞬时感知国产云平台漏洞相关信息；同时，安装漏洞扫描工具确保漏洞实时监测。

2） 漏洞的响应管理。建立漏洞感知、响应、修复的服务系统。当接收到上报的漏洞信息时，根据漏洞修复服务等级协议要求，按漏洞的严重程度确定处理优先级。为降低漏洞被利用的风险，也可通过修改配置、制定 Web 应用防火墙规则或暂停服务等方式对受影响的服务进行隔离。

3） 提醒修复漏洞功能。对于国产云平台、云服务存在的安全漏洞，及时向用户发送漏洞规避方法、技巧以及修复方案或建议等。

2.6.3 日志和事件管理

国产云平台安全事件包括网络攻击、信息破坏、信息泄露、数据篡改或入侵及其他可能影响云服务的安全事件，如后门攻击、窃听、DDoS 攻击、数据泄漏/窃取/丢失等。

1） 日志管理及审计。建立一套完善的日志审计系统，用以收集汇总所有物理设备、网络、应用、数据库和安全系统的日常操作日志及相关信息，确保所有操作都被记录，并提供在线查询、事后追溯等功能。

2）发现与定界。关联各种安全设备及告警日志，通过大数据安全分析系统，统一分析、快速识别已发生的攻击，实现快速发现与定界，并预测潜在威胁。借助海量的原始告警日志，大数据安全分析系统可以实时在线检测攻击、威胁行为，缩短人工分析的时间。

3） 隔离策略与恢复管理。当恶意攻击发生时，迅速启动隔离与恢复功能，边界的安全设备为第一道防线。大数据安全分析系统与各种安全设备联动能快速发现并迅速阻断攻击，实现快速隔离与恢复的第二道防线作用。

AUTOMATION & INFORMATION ENGINEERING

2.6.4　业务管理与灾难恢复

1） 基础设施管理策略。通过多数据中心的技术架构、异地备份等方式对数据进行容灾与备份。另外，也可采取两地互为容灾备份中心的方式，若某一地出现故障，系统自动将用户应用及数据转移到另一地无故障区域，确保用户业务的连续性及稳定性。如果某一数据中心发生故障，用户应用也会被负载均衡到其他的数据中心。

2） 灾备复制策略。为数据中心制定一套灾后恢复计划，将用户数据复制并存放在一个数据中心的多个节点内。如果某一节点发生故障，确保用户数据不会丢失；单区域内或多区域之间通过光纤技术实现数据中心互联、多区域之间数据复制的功能。

3） 测试及业务计划。对重大灾难，如地震，为确保云服务正常运行、用户业务和数据的安全，需要制定业务计划或连续性业务计划，并定期对其测试。同时制定灾难恢复计划并定期对其测试，将测试结果记录归档，用以逐步完善持续改进的业务计划。

3　结语

本文详细梳理并借鉴已有的安全体系结构设计经验，设计一种能定义、可重构、可演进的结构方案，再逐步优化，最终成为适合的国产云安全体系结构方案，以满足用户需求。

参考文献

[1] 荣喜丰.云计算网络环境下的信息安全研究[J].网络安全技术与应用,2021(7):83-84.

[2] 刘隐.云计算网络环境下的信息安全问题探讨[J].电脑知识与技术,2021,17(18):64-65.

[3] 张勇,郭骏,刘金波,等.调控云平台 IaaS 层技术架构设计和关键技术[J].电力系统自动化,2021,45(2):114-121.

[4] 王承明,白连万,王健,等.基于云平台的计算机公共实验教学中心建设的研究与实践[J].实验技术与管理,2020,37(11):269-272.

[5] 王佐捷.云计算网络环境下的信息安全问题探究[J].数码世界,2019(3):247-248.

[6] 麦伟明.基于 4G-DTU 的用水信息管理系统[J].自动化与信息工程,2020,41(3):37-40.

[7] 贺敏超,刘思洋,霍朝宾.基于云计算的软件测试平台架构设计[J].信息技术与网络安全,2019,38(4):63-66.

[8] 李冀东,张进猛,苏健.基于云平台的教学系统的设计与实现[J].实验技术与管理,2019,36(6):176-180.

Research on Security System Strategy of Domestic Cloud Platform

ZHANG Hongjin　LIU Wei

(1.The 5th Electronics Research Institute of the Ministry of Information Industry of China, Guangzhou 510610, China　2.The Ministry of Industry and Information Technology Key Laboratory of Performance and Reliability Testing and Evaluation for Basic Software and Hardware, Guangzhou 510610,China)

Abstract: For the security of domestic cloud platforms, we should not only deal with the security threats brought by traditional IT technology, but also face the new risks brought by virtualization and other technologies. Firstly, a domestic cloud security defense model with security strategy, protection strategy, detection strategy and response strategy as the core is proposed; Then, the key technologies for the construction of domestic cloud platform security system are described from the five levels of physics, network, host, application and data, in order to provide useful exploration for the relevant research of domestic cloud platform security system strategy.

Keywords: domestic cloud; cloud platform; security system; security defense model

作者简介：

张红金，男，1976 年生，本科，高级工程师，信息系统项目管理师，主要研究方向：软件测试、信息系统安全研究、科研项目管理及质量管理。E-mail: zhanghongjin@ceprei.com

AUTOMATION & INFORMATION ENGINEERING