电信云安全方案研究

Research on Security Scheme of Telecom Cloud

张世华[1]，文湘江[2]，张　奎[1]，胡　祎[1]，赵以爽[1]，申　佳[1]（1. 中讯邮电咨询设计院有限公司郑州分公司，河南 郑州 450007；2. 中国联合网络通信集团有限公司，北京 100033）

Zhang Shihua[1], Wen Xiangjiang[2], Zhang Kui[1], Hu Yi[1], Zhao Yishuang[1], Shen Jia[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd. Zhengzhou Branch, Zhengzhou 450007, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

随着新基建和数字经济的推进，云计算作为网络、计算和应用的重要结合点，给电信运营商带来了新的发展机遇。深入分析了国家安全政策要求，结合工信部和公安部颁布的法律法规，梳理出了云资源安全防护手段；其次根据电信运营商云资源池类型和承载业务需求，给出了各类云资源池安全部署建议。

关键词：

安全方案；云计算；业务云；IT云；CT云

doi：10.12045/j.issn.1007-3043.2023.04.006

文章编号：1007-3043（2023）04-0024-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the development of new infrastructure and digital economy, as an important combination of network, computing and application, cloud computing brings new development opportunities to telecom operators. It analyzes the national security policy requirements in depth, and combs out the cloud computing security protection schemes in combination with the laws and regulations issued by the Ministry of industry and information technology and the Ministry of public security. Secondly, according to the service requirements of telecom operators, the security deployment suggestions of various cloud computing pools are given.

Keywords：

Safety scheme; Cloud computing; Business cloud; IT cloud; CT cloud

引用格式：张世华，文湘江，张奎，等. 电信云安全方案研究[J]. 邮电设计技术，2023（4）：24-28.

1 概述

随着新基建和数字经济的推进，云计算作为整合网络与计算技术能力的平台，成为通信网络、算力与新应用技术协同配合的关键契合点。云计算产业的蓬勃发展也给电信运营商带来了新的发展机遇，电信运营商在纷纷推出天翼云、移动云、联通云等公有云服务的同时，也在积极推动网络设备和平台业务的云化部署[1-2]。

与此同时，网络边界的扩大化和模糊化也给业务安全增加了困难。首先，新技术的演进增大网络安全威胁暴露面，网络云化导致整体架构的变化，业务系统从分散和独立向集中化、融合化发展，增加了安全防御难度[3]；与此同时，攻击手段和外部环境不断升级、恶化，国家关键基础设施和重要信息系统成为跨国网络攻击的重要目标。网络安全上升为国家战略，以《国家安全法》作为基础性法律，国家又相继颁布了《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等一系列法律法规。在国家引导、信息化资产重要性提升、重大安全事件影响下，服务提供商和使用方逐渐认识到安全的重要性。

因此，本文从国家安全政策分析入手，探讨电信运营商部署的各类云资源池的安全方案建议。

收稿日期：2023-02-22

2 云资源安全政策要求分析

2.1 工信部安全政策要求

在国家法律法规的要求下,主要由工信部和公安部对电信运营商的云资源池安全做进一步细化要求。其中工信部主导颁布了《电信网和互联网信息服务业务系统安全防护要求》(YD/T 2243-2016)、《互联网数据中心安全防护要求》(YD/T 2584-2013)以及《移动通信网安全防护要求》(YD/T 1734-2009)等关于电信网和互联网安全防护体系的一系列通信行业标准[4-7]。其中对云资源池的安全要求主要有以下几个方面。

a) 业务及应用安全。业务及应用在实现技术、管理和控制等方面的安全要求,分为业务逻辑安全和Web安全两大类,包括身份鉴别、访问控制和安全审计等相关要求。

b) 网络安全。业务系统内部网络鲁棒性和抗攻击的安全要求,包括结构安全、安全检测和入侵防范等相关要求。

c) 设备及软件系统安全。业务系统所使用的设备和软件系统的安全要求,包括网络设备、安全设备、操作系统等软硬件设备在资源和访问控制、入侵防范、安全审计等方面的相关要求。

d) 物理安全。业务系统所部署的物理环境的安全要求,包括机房物理位置、电力供应、防水和防火等相关要求。

e) 管理安全。业务系统在建设和维护阶段的安全管理要求,包括管理制度、人员和技术支持能力、运行维护管理能力、灾难恢复预案等相关要求。

2.2 公安部安全政策要求

为配合国家网络安全法实施,适应大数据、物联网、云计算等新型技术和应用,由公安部主导对原国家标准进行修订,形成新的标准《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019),也被称为等保2.0,根据保护对象不同分为安全通用要求和安全扩展要求2个部分,其中对云资源池的安全要求主要有以下几个方面[8-9]。

a) 安全通信网络要求。对网络架构和通信传输的安全要求,保障通信过程中数据的完整性和安全性,包括网络架构、通信传输、可信验证等相关要求。

b) 安全区域边界要求。在不同的网络之间实现数据交换的同时,对网络边界的安全控制要求,包括边界防护、访问控制、入侵防范等相关要求。

c) 安全计算环境要求。对系统内部所有对象的安全要求,例如网络设备、服务器、应用系统等,包括身份鉴别、访问控制、可信验证等相关要求。

d) 安全管理类要求。技术层面的安全管控,通过技术工具实现集中管理,包括审计管理、系统管理和集中管控等相关要求。

e) 安全物理环境要求。对物理机房的安全控制要求,包括物理位置选择、物理访问控制、电力供应、防盗窃和防破坏等相关要求。

工信部和公安部对云资源池的安全要求从不同方面和角度出发,最终梳理出的安全设备/能力大致相同,其中公安部针对公有云场景,适用性更强,而工信部针对各类业务系统进行了细化。对外服务云池需按照公安部安全要求建设,以满足政企客户业务的安全需要,对内业务云池需按照工信部安全要求建设,以满足通信管局的管理要求。其中主要的安全设备包括:

a) 防火墙。基于对五元组进行访问策略控制,保障同一区域内各个逻辑网络平面间按需互通和阻断。

b) IPS。入侵防御系统,监视网络中的数据传输行为,能够及时中断、调整或隔离一些具有伤害性或者不正常的数据转发行为。

c) 防病毒网关。用于保护网络内进出数据安全,支持阻止垃圾邮件、杀除病毒、过滤关键字等功能。

d) WAF。Web应用防火墙,专门为Web应用提供HTTP/HTTPS安全策略,对各类请求进行内容检查,确保Web请求的合法和安全性,对不合规请求进行阻断。

e) 抗DDoS。对网络中流量攻击、资源耗尽等类型的攻击进行安全防护。

f) 4A。包括认证、授权、账号、审计,又称为统一安全管理平台解决方案,一般将身份认证、授权、账号称为3A,集中部署,审计称为1A,部署到各个节点,对用户所有的操作日志记录管理和分析。

g) 接入VPN。一种采用SSL协议来实现远程接入的VPN技术。

h) EDR。端点检测与响应,通过采集终端的行为和网络事件,根据自身系统的攻击指示器、行为分析的数据库,借助机器学习等智能化技术来监测终端的安全威胁,并做出快速响应。

i) 漏扫。即漏洞扫描,通过对本地或远端的计算机系统、网络设备等对象扫描,进行安全脆弱性检测分析,并出具相关的扫描结果和整改报告。

云资源池中部署的对象主要包括：

a）计算节点。部署各种类型的计算能力，主要包括计算型服务器/GPU服务器等。

b）存储节点。部署各类存储能力，主要包括集中式存储和分布式存储设备。

c）网络节点。主要采用Spine-leaf架构，部署网络路由、交换设备。

d）安全设备。部署资源池所需各类安全设备，满足资源池安全合规要求。

e）其他。包括运营支撑系统、监控平台、虚拟化软件等。

根据安全防护要求，防护手段包含漏洞检测、基线检测、抗DDoS等总计约20种，依据安全防护手段，云资源池中各类对象可以分为网络设备、服务器、存储、云平台、操作系统、账号、IP地址、应用等8类，具体安全防护的对应关系如表1所示。

3 云资源池安全部署方案建议

电信运营商云资源池根据承载业务不同可以分为业务云、IT云和CT云，以下将分别对它们的安全方案进行介绍。

表1 云资源池安全防护的对应关系

序号	类别	设备对象	防护手段																			统计
			漏洞检测	基线核查	抗DDOS	堡垒机	防火墙	入侵检测/APT	蜜罐	VPN	日志审计	防病毒网关	WAF	SOC综合管理平台	微隔离	云镜像安全	主机防病毒	数据脱敏	数据加密	数据防泄漏	态势感知	资产安全管理平台	20种
1	云资源池	网络设备	√	√	√	√	√	√	–	√	√	√	–	√	–	–	–	–	–	√	√	√	13
2		服务器	√	√	√	√	√	√	–	√	√	√	–	√	–	–	–	–	–	–	√	√	12
3		存储	√	√	√	√	√	√	–	√	√	√	–	√	–	–	–	–	–	–	√	√	12
4		云平台	√	√	√	√	√	√	√	√	√	√	–	√	√	√	–	–	–	–	√	√	15
5		操作系统	√	√	√	√	√	√	√	–	√	√	–	√	√	–	√	–	–	–	√	√	14
6		账号	–	√	–	√	√	√	–	√	√	–	–	–	–	–	–	√	–	√	–	–	7
7		IP地址	–	–	√	√	√	√	–	–	–	–	–	–	–	–	–	√	–	–	–	√	5
8		应用	√	√	√	√	√	√	√	–	–	–	√	√	–	√	√	√	√	√	√	√	15

3.1 业务云安全部署方案

业务云指对外提供服务的云资源池，如公有云、政务云和行业云等。安全建设内容分为面向云平台的安全建设和面向租户的安全建设，面向平台的安全建设建议根据设备处理能力和性价比选用硬件安全设备或安全资源池来实现，面向租户的安全建设建议使用安全资源池来实现，以满足客户自定义安全配置、差异化提供安全防护能力和快速开通服务的要求。如图1所示，基于等保2.0分级分域的原则，面向平台安全建设在公网出口区建议部署抗DDoS、负载均衡、防火墙、接入VPN、防病毒网关等设备进行网络边界的安全防护；在核心交换区建议部署网络及数据库审计系统和APT设备，对资源池内部东西向流量和出口南北向流量进行安全检测；在平台运维区建议部署漏扫、堡垒机、日志审计、态势感知等设备，对终端设备和管理平台进行安全防护；在存储区建议部署备份一体机进行重要数据的备份保护。面向租户的安全建设建议部署安全资源池，可实现不同租户的不同安全需求，也可协助租户通过等级保护测评，安全资源池需涵盖多种类型安全网元，如防火墙、漏扫、WAF等虚拟化安全网元。

3.2 IT云安全部署方案

IT云指承载运营商内部信息化系统相关业务的云资源池，资源池内划分为多个区域，不同区域间设备物理隔离，不同业务根据网络连接需求分布部署到对应区域，并根据安全需要在同一区域内划分不同AZ/HA区进行资源和网络隔离，资源池通过IT承载网、互联网对外连接。如图2所示，IT云相关安全部署建议如下。

a）将互联网视为不可信网络，IT承载网视为可信网络，根据公网连接情况，资源池内划分为DMZ区、用户区、核心区、安全区等多个区域。

b）互联网出口设备串接防火墙，旁挂抗DDoS、流量分析、IDS/IPS、防病毒网关、WAF、非法外联检测等防护设备，用于网络边界安全防护。

c）IT承载网为可信网络，通过此接口访问的业务需通过各区域的防火墙进行安全隔离。

d）资源池内不同区域/不同资源池之间互访需要通过防火墙进行安全隔离；同一AZ/HA区内根据分域

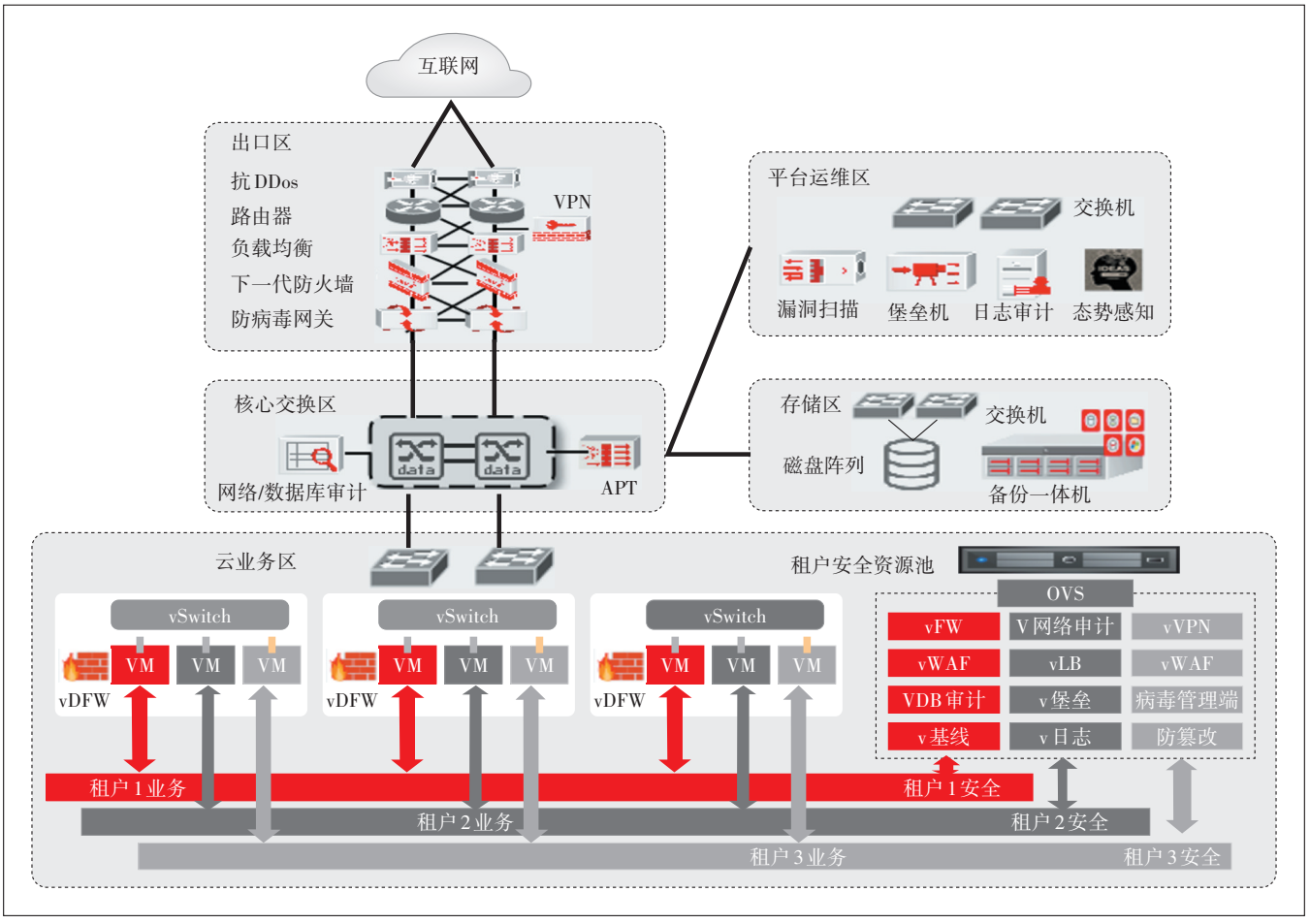

图1　业务云资源池安全方案示意图

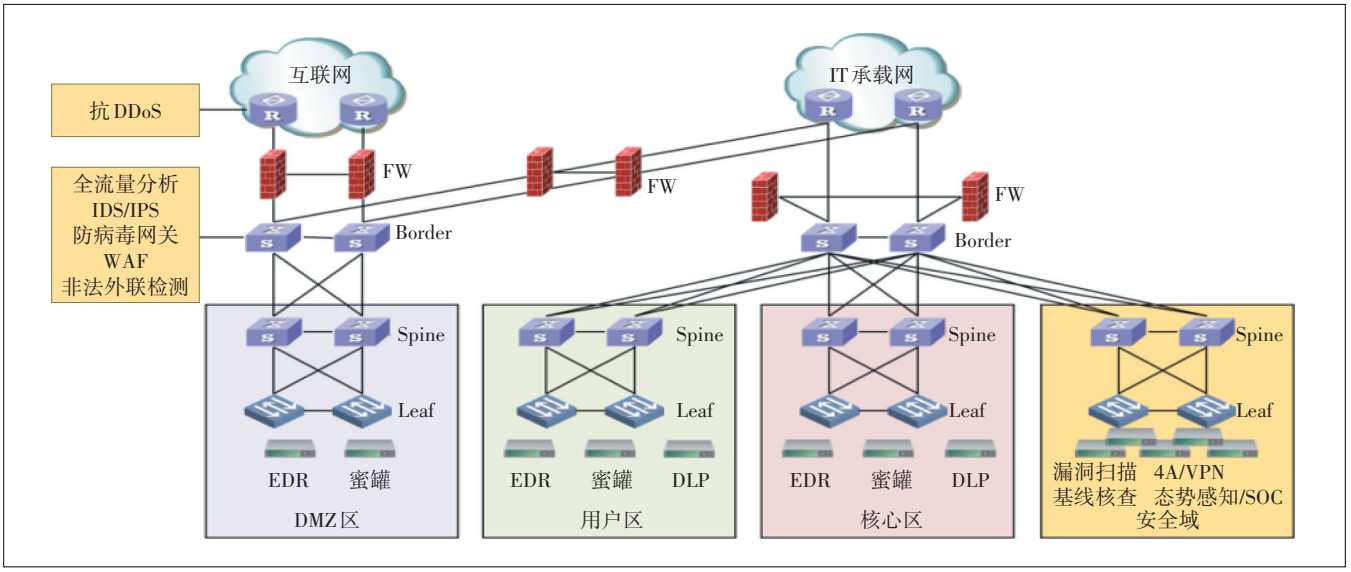

图2　IT云资源池安全方案示意图

分区的原则可通过路由策略进行管控。

e）资源池内各逻辑区部署主机防护EDR、蜜罐、DLP，实现主机安全、数据防泄漏。

f）资源池内安全域部署漏洞扫描、基线检查、

VPN、4A、态势感知平台等,进行安全能力统一管控。

3.3 CT云安全部署方案

CT云也被称为通信云/网络云,采用NFVI架构,主要承载虚拟化的通信网元。考虑到业务的复杂性、高可靠性以及解耦程度的不同,建议根据需要分为网络能力域和平台业务域资源池,2类资源池单独部署。

网络能力域资源池承载5GC、vIMS等路由型业务,目前已实现了硬件设备和云平台软件之间的软硬解耦,为保证业务高可靠性,云平台和上层业务网元需同厂商部署。如图3所示,由于业务无公网访问需求,资源池可不再划分安全区,出口处按需部署防火墙、IPS/IDS等设备用于网络边界和DC内管理流量的访问控制,部署4A系统提供远程安全接入和审计功能,此外在资源池内部署日志审计系统满足日志查询和管理的需求,漏扫软件以定期/按需等周期进行安全扫描,保障通信云计算环境安全。资源池内东西向流量隔离防护,可根据业务需求选择划分不同VLAN和VRF进行网络隔离。

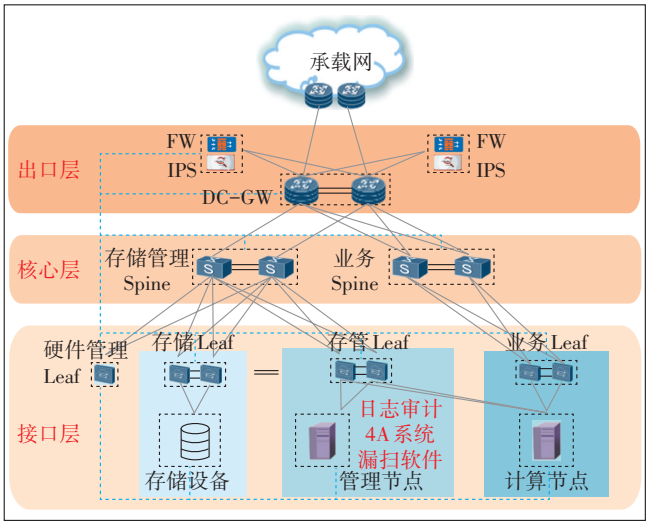

图3　CT云网络能力域资源池安全方案示意图

平台业务域资源池承载短、彩信等主机型业务,基本实现了硬件设备、云平台、业务网元间的3层解耦。由于部分业务要求与互联网连接,需将资源池划分为可信区和DMZ区,整体方案与IT云大体相同,因此不再赘述。

经过以上分析可知,业务云因需满足用户安全要求,需部署安全资源池,向客户提供灵活可定制的安全能力;IT云目前仍以硬件安全为主,分区分域进行了隔离和安全部署;CT云由于承载业务和架构的特殊性,仍较为封闭。

4 未来展望

本文基于国家安全政策要求,结合电信运营商云资源池需求,明确提出了各类云资源池安全部署建议,旨在提高电信云安全能力和方案标准化。

在网络演进过程中新技术、新应用层出不穷,可能会重构网络安全防护能力,容易出现未知风险,同时5G与各类垂直行业的融合放大了安全影响和威胁程度;而目前配套的安全策略和解决方案研究相对滞后,仍然以被动防御为主,缺少APT攻击防御能力,主动感知、自动探测的水平不高。基于以上情况,建议在满足国家监管要求的基础上,加强业务和数据安全风险防护研究,聚焦大数据、可视化等技术,提高安全防护效率和智能化,保障网络演进,不断丰富安全服务产品。

参考文献:

[1] 刘艳红,黄雪涛,石博涵. 中国"新基建":概念、现状与问题[J]. 北京工业大学学报(社会科学版),2020,20(6):1-12.
[2] 张天魁,骆晓亮,朱禹涛. 面向新基建的通信网络发展现状与趋势研究[J]. 通信管理与技术,2022(1):9-11.
[3] 卢磊,张玲. 运营商网络云化架构演进分析[J]. 电信快报,2020(3):24-27,45.
[4] 中华人民共和国工业和信息化部. 互联网数据中心安全防护要求:YD/T 2584-2013[S]. 北京:人民邮电出版社,2013.
[5] 中华人民共和国工业和信息化部. 电信网和互联网信息服务业务系统安全防护要求:YD/T 2243-2016[S]. 北京:人民邮电出版社,2016.
[6] 中华人民共和国工业和信息化部. 移动通信网安全防护要求:YD/T 1734-2009[S]. 北京:北京邮电大学出版社,2010.
[7] 中华人民共和国工业和信息化部. 互联网数据中心安全防护检测要求:YD/T 2585-2013[S]. 北京:人民邮电出版社,2013.
[8] 国家市场监督管理总局,国家标准化管理委员会. 信息安全技术网络安全等级保护基本要求:GB/T 22239-2019[S]. 北京:中国标准出版社,2019.
[9] 国家市场监督管理总局,中国国家标准化管理委员会. 信息安全技术网络安全等级保护测评要求:GB/T 28448-2019[S]. 北京:中国标准出版社,2019.

作者简介:
张世华,助理工程师,硕士,主要从事核心网、通信云咨询、规划和设计工作;文湘江,高级工程师,硕士,主要从事通信云架构设计、技术选型等工作;张奎,高级工程师,硕士,主要从事核心网、通信云咨询、规划和设计工作;胡祎,高级工程师,硕士,主要从事核心网、通信云咨询、规划和设计工作;赵以爽,高级工程师,硕士,主要从事核心网、通信云咨询、规划和设计工作;申佳,助理工程师,学士,主要从事核心网、通信云咨询、规划和设计工作。