国家电子政务外网标准

GW0013—2017

政务云安全要求

Security Requirements for Government Cloud

2017-03-30 发布　　2017-05-01 实施

国家电子政务外网管理中心
电子政务云集成与应用国家工程实验室　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则及政务云安全的实际需求起草。

本标准由电子政务云集成与应用国家工程实验室提出。

本标准由国家电子政务外网管理中心归口。

本标准主要起草单位：国家电子政务外网管理中心、新华三集团、华为技术有限公司、曙光信息产业股份有限公司、中国科学院信息工程研究所、中国电子技术标准化研究院、中电长城网际系统应用有限公司、中电科华云信息技术有限公司、北京中软华泰信息技术有限责任公司、杭州迪普科技股份有限公司、兴唐通信科技有限公司、北京江南天安科技有限公司、上海汉邦京泰数码技术有限公司、华信咨询设计研究院有限公司、阿里云计算有限公司、杭州合众数据技术有限公司、太极计算机股份有限公司。

本标准主要起草人：周民、杨绍亮、邵国安、徐云、梁鹏、韩帅、任飞、李彦宾、史翔宇、黄敏、张云星、陈驰、杨瑛、闵京华、葛超、朱星、赵勇、路剑华、孟斌、李国、肖国玉、栗金芬、陈雪秀、李丹丹、钱春巍、郭峰、陈楠、陈龙、曹亮、毛群飞、任伟。

引　言

政务云在管理、建设和运维过程中有其自身的安全要求，需要在国家标准的基础上提出有针对性的安全要求。本标准是相关云计算国家标准在电子政务应用方面的安全要求补充，在遵守国家相关法律法规、中央网信办相关管理办法及等级保护的前提下，为指导全国各级政务部门开展政务云服务提供安全和管理依据，保证政务云服务的安全要求。本标准主要包括政务云概述及安全功能区域划分、安全参考模型、政务云安全技术要求和管理要求等内容。

政务云安全要求

1 范围

本标准适用政务云规划设计、设备选型、建设实施、运行维护和管理。为各级政务部门建设政务云提供指导和参考。

本标准规定了云服务客户及政务云服务方应满足的安全基本要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注明日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇（ISO/IEC 27000）

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

ISO/IEC 17788 信息技术 云计算 概述和词汇

3 术语与定义

下列术语和定义适用于本文件。

3.1

政务云 Government Cloud

用于承载各级政务部门开展公共服务、社会管理的业务信息系统和数据,并满足跨部门业务协同、数据共享与交换等的需要，提供IaaS、PaaS和SaaS服务的云计算服务。

3.2

云服务客户 Cloud Tenant

在政务云中，云服务客户指使用政务云的各级政务部门（指各级党委、人大、政府、政协、法院和检察院等政务部门），即使用云计算基础设施开展电子政务业务和处理、存储数据的组织（或机构）及相关事业单位。包括单位内部业务使用人员及对云相关云资源和安全的管理人员。

3.3

云服务方 Cloud Service Party

管理、运营、支撑云计算的计算基础设施及软件，通过服务方式将云计算的资源交付给客户。在政务云中，云服务方指为各级政务部门提供计算、存储、网络及安全等各类云计算基础设施资源、相关软件和服务的提供商，及负责执行云服务方业务运营和相关管理工作。

3.4

政务云管理单位 Government Cloud Management Unit

是政务云的行政监管单位，负责政务云平台的规划、应用、监督、管理及对云服务方的考核，审核云服务客户的政务云平台使用需求，受理政务云平台建设方案备案及服务费用的审核。

3.5

云管理平台 Cloud Management Platform

为整个云计算基础设施提供资源管理和服务管理，能够对存储/计算/网络/系统等基础设施资源（IaaS）、应用/开发/数据平台（PaaS）和软件架构整合服务（SaaS）进行管理。一般情况下，由云计算基础设施服务方提供，也可由第三方提供云管理平台。

3.6

云计算基础设施 Cloud Computing Infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。硬件资源包括所有的物理计算资源，即服务器（CPU、内存等）、存储组件（硬盘等）、网络组件（路由器、防火墙、交换机、网络链路和接口等）及其他物理计算基础元素。资源抽象控制组件对物理计算资源进行软件抽象，云服务方通过这些组件提供和管理对物理计算资源的访问。

3.7

虚拟专有云 VPC- Virtual Private Cloud

提供一个逻辑隔离的区域，搭建一个安全可靠、可自主定义的环境。在该区域中部署独立的服务资源，并根据业务需求定义虚拟环境，包括定义网络拓扑、创建子网、虚拟机存储资源和划分安全组等。部门业务区每个云服务客户有一个VPC，公共区和互联网区可以是多个云服务客户共享的VPC。

3.8

控制器 Controller

包括虚拟化监视器、SDN控制器、存储虚拟化控制器和策略管理控制器等进行物理资源抽象管理的资源管理和策略管理系统。

3.9

跨网数据交换系统 Data Exchange Across Regional Networks

跨网数据交换是一种基于网络隔离技术的无协议数据同步系统，综合利用设备认证、数据格式检查、病毒检查等安全措施，实现两个不同网络业务区服务器之间数据同步。可由外交换服务器和内交换服务器及相关隔离设备组成，支持数据库、文件、图像数据及请求响应数据的安全交换。

4 缩略语

IaaS	基础设施即服务（Infrastructure as a Service）
PaaS	平台即服务（Platform as a Service）
SaaS	软件即服务（Software as a Service）
VM	虚拟机（Virtual Machine）
VPC	虚拟专有云 (Virtual Private Cloud)
MPLS	多协议标签交换 (Multi-Protocol Label Switching)
VPN	虚拟专用网络（Virtual Private Network）
SDN	软件定义网络（Software Defined Network）
API	应用程序编程接口（Application Programming Interface）
NFV	网络功能虚拟化（Network Function Virtualization）
RTO	恢复时间目标 (Recovery Time Objective)
RPO	恢复点目标（Recovery Point Objective）

5 政务云概述及业务区域划分

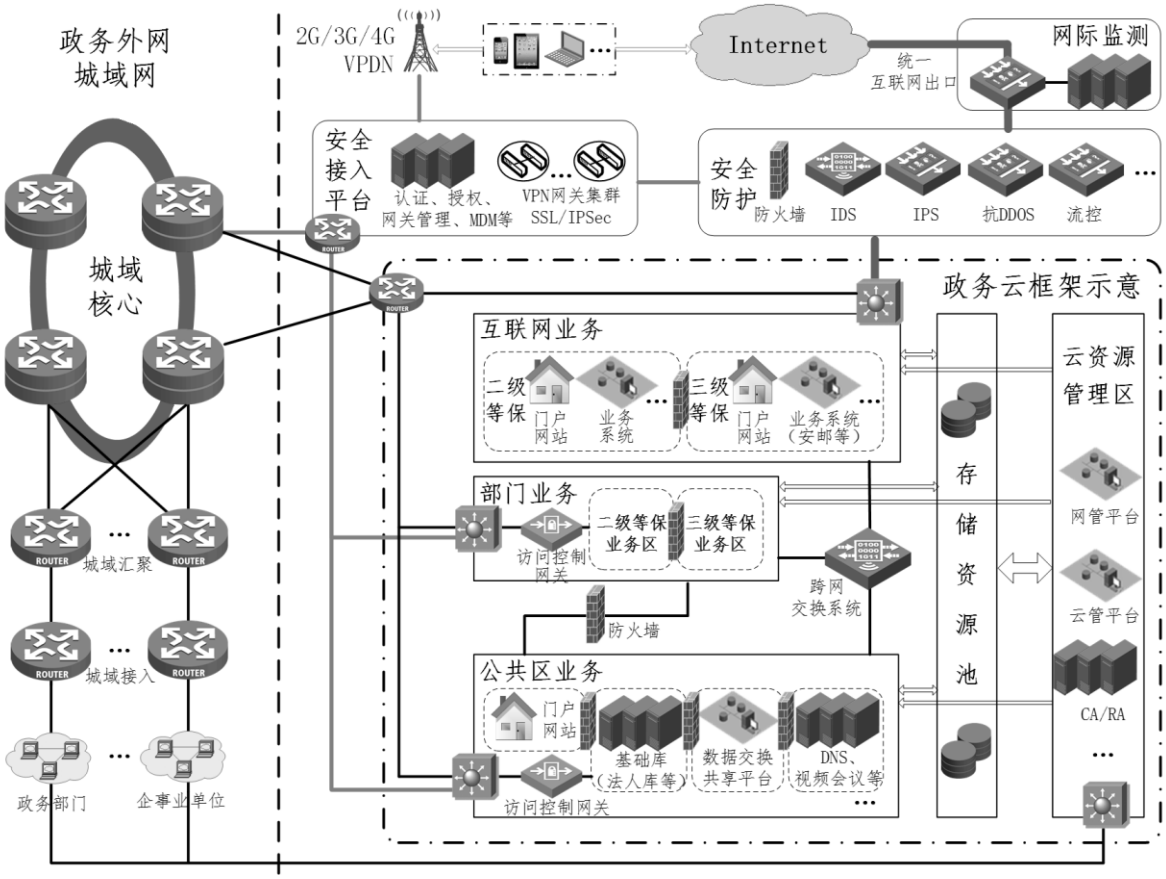


图1　政务云业务区域划分图

5.1 政务云概述

政务云是承载各级政务部门的门户网站、政务业务应用系统和数据的云计算基础设施，用于政务部门公共服务、社会管理、数据共享与交换、跨部门业务协同和应急处置等政务应用。政务云对政府管理和服务职能进行精简、优化、整合，并通过信息化手段在政务上实现各种业务流程办理和职能服务。政务云的建设有利于减少各部门分散建设，提升信息化建设质量，提高资源利用率和减少行政支出等优势。

政务云的服务对象是各级政务部门，通过政务外网连接到各单位，使用云计算环境上的计算、网络和存储资源，承载各类信息系统，开展电子政务活动。

5.2 政务云功能区域划分

5.2.1 政务外网城域网

政务外网城域网连接同级各政务部门，云服务客户可通过城域网各自的MPLS VPN分别访问政务云内部相关部门内部的信息系统和公共区信息系统。各政务部门通常以专线接入当地政务外网城域网，并通过城域网不同VPN实现政务云及互联网的访问。

5.2.2 安全接入平台

安全接入平台是政务用户通过互联网或移动专线网络访问政务云的部门业务和公共区业务的唯一接入通道，接入平台应具备数字认证、授权管理、VPN接入、移动设备管理和移动应用管理等功能，为各类智能移动终端和远程办公用户提供可信的安全接入和实时的业务访问。

5.2.3 安全防护

本防护区是互联网用户访问政务云上的门户网站、部署在互联网上的应用系统和政务人员统一访问互联网的安全防护区域，其安全防护要求按网络安全等级保护第三级的国家标准要求进行保护。

5.2.4 政务云

a) 互联网业务区

互联网业务区主要为公众和企业提供互联网门户网站服务和政务服务，由于门户网站群分属各不同的政务部门，其安全要求各有不同，对网站和信息系统可根据不同的安全级别进行分等级防护。

b) 公共业务区

公共业务区主要实现跨部门、跨地区的信息共享、数据交换及业务协同，提供政务部门内部的公共服务。禁止从互联网直接访问本区域的各信息系统和数据，与部门业务区逻辑隔离并应做好相应的访问控制，本区域部署的信息系统可结合自身实际情况按国家等级保护要求进行分级并实施保护。

c) 部门业务区

部门业务区主要承载各云服务客户部署或迁移的信息系统，云服务客户可按要求部署在不同的VPC，VPC之间采用VPN技术隔离，应根据信息系统的安全等级进行防护。可按云服务客户对信息系统的安全要求分为二级信息系统等级保护区域和三级信息系统等级保护区域，若云服务客户同时拥有二级业务和三级业务，应确保不同等级的信息系统采用访问控制策略。

d) 存储资源池

云计算中的存储池一般是以存储块或分布式存储方式，将数据离散的存储在资源池中，并按要求可对相关重要数据进行加密存储，并将互联网区的业务和政务业务在计算资源及网络资源物理分开，如存储资源池共用，则需保证数据安全可控，对存储资源池进行统一管理和调度。

e) 云资源管理区

为整个政务云系统提供云资源管理和物理资源抽象，以及日常运维所必须的运维系统和认证管理系统。通过资源管理区实现对各类云资源的实时监控、管理、预警和应急处置，并对虚拟机迁移、资源弹性扩展、业务使用情况及运维操作人员进行实时监控和审计。

6 政务云安全参考模型

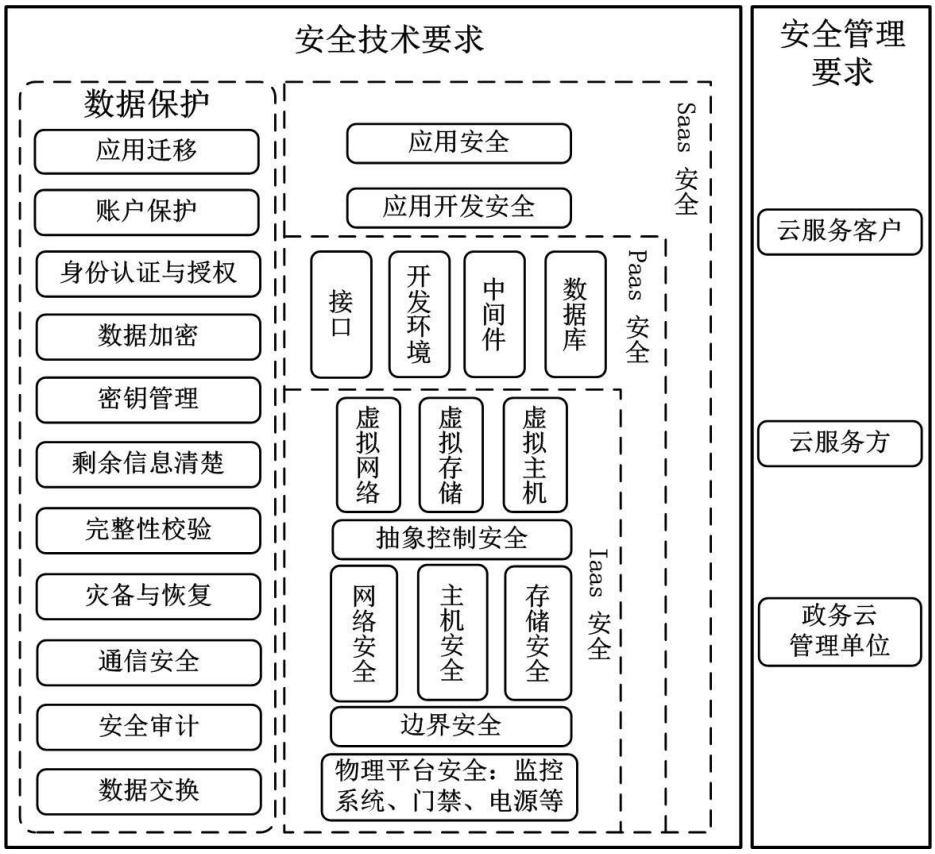


图 2：政务云安全参考模型

6.1 政务云服务模式概述

a) IaaS服务模式下，云服务方向客户提供计算资源、存储、网络等资源，提供访问云基础设施的服务接口。客户可在这些资源上部署或运行操作系统、中间件和应用软件等。客户通常不能管理或控制云基础设施，但能控制自己部署的操作系统、存储、应用和数据，也能部分控制使用的网络组件，如虚拟防火墙。IaaS安全主要包括物理平台安全、边界安全、物理资源安全（网络安全、主机安全、存储安全）、抽象控制安全、虚拟网络安全、虚拟存储安全、虚拟主机安全等。

b) PaaS服务模式下，云服务方向客户提供的是运行在云基础设施之上的软件开发和运行平台，如：标准的开发语言与工具、数据访问、中间件、数据库及通用接口等。云服务客户可利用该平台开发和部署自己的软件。云服务客户通常不能管理或控制支撑平台运行所需的底层资源，如网络、服务器、操作系统、数据库和存储等，但可对应用的运行环境进行配置，控制自己部署的应用。PaaS位于IaaS之上，用以与应用开发框架、中间件以及数据库、消息队列等功能集成。PaaS层增加的安全主要包括接口安全、开发环境安全、中间件安全、数据库安全等。

c) SaaS服务模式下，云服务方向客户提供的是运行在云基础设施之上的应用软件。云服务客户不需要购买、开发软件，即可利用不同设备上的客户端（如WEB浏览器）或程序接口进行网络访问并使

用云服务方提供的应用软件，如电子邮件系统、协同办公系统等。云服务客户通常不能管理或控制支撑应用软件运行的底层资源，如网络、服务器、操作系统、存储等，但可对应用软件进行有限的配置管理。SaaS位于IaaS和PaaS之上，它能够提供独立的运行环境，用以交付完整的用户体验，包括内容、展现、应用和管理能力。SaaS层增加的安全主要是应用开发安全和应用安全。

6.2 数据保护要求概述

无论采用何种政务云服务模式，政务云中的政务数据保护是关系到政务云能否提供安全可靠的服务交互的关键，从信息系统迁移开始就要考虑应用系统和数据的安全问题，迁移到云上后，对应用系统的访问，应采取身份认证、授权管理、账户保护、数据加密、密钥管理、剩余信息清除、完整性校验、灾备与恢复、通信安全、安全审计、数据交换安全等技术手段实现应用和数据的保护要求。

6.3 政务云安全管理要求概述

政务云的安全管理角色分为云服务客户、政务云管理单位和云服务方，在政务云的安全管理过程中，应结合三方的角色，合理划分权限和责任，充分考虑各方在政务云安全管理和使用工作中的互补性，实现各方的职能定位，共同协作，保障政务云整体的安全防护能力。云服务提供方应与政务云管理单位、政务部门（云服务客户）签订安全保障协议，明确责任及管理边界，云计算资源使用情况，资源配套管理、安全策略制定和业务连续性等要求。

7 政务云安全技术要求

7.1 总体要求

a) 各类政务业务应部署在物理设施独立的政务云上，不得部署在公有云上；
b) 政务云计算基础设施应按网络安全等级保护国家标准中的第三级等级保护要求建设和保护；
c) 政务云上承载互联网门户网站及部署在互联网上的信息系统计算和网络资源，从云计算核心交换机以下，在物理上（宿主机和交换机）与其他VPC分开部署，根据系统预设的调度策略进行资源调度和迁移。对于已建的政务云，应对互联网VPC的业务实时监测、控制和管理，尤其是对跨VPC数据共享与交换访问控制的实时监控；
d) 所有对各类资源的操作必须通过云资源管理区，并对管理员操作进行审计。要求业务流量与管理流量分开，应能实现并区分运维管理人员、云服务客户管理员及公务人员访问业务和对各类资源的管理和控制；
e) 云服务方应提供对各信息系统的核心或敏感数据加密存储的功能，应按照国家密码管理有关规定使用和管理政务云平台的密钥设施，并按规定生成、使用和管理密钥；
f) 应对云服务客户管理员账户及政务云的管理数据单独加密存储，重点保护。其密钥的使用和管理应符合国家密码管理局的有关规定；
g) 重要部门的信息系统在分地域部署云计算基础设施时，可将计算、网络和存储设施采用分布式部署方式部署在远端并进行统一管理；
h) 明确远程管理责任，云服务方需要对计算资源进行远程管理时，云管理单位有权对所有远程维护和诊断活动进行审计并进行定期或不定期审查；
i) 云计算环境应具备基于行为的实时安全监控、策略控制、安全事件主动发现和预警、态势感知及安全事件及时处置的能力；
j) 云服务方应定期向政务云管理单位提交各云服务客户安全情况及资源使用率情况的报告；
k) 对重点云服务客户的信息系统和数据应能重点进行安全保障，实时监控异常情况并预警；

l) 政务云应具备分级管理和控制的能力，VPC内部信息系统之间的访问控制及数据使用等管理权限应开放给云服务客户，云服务方应具备对资源使用情况实时监测、发现异常、预警和协助处置的能力；
m) 所有应用系统正式迁移或部署到政务云上前应进行测试、其应用系统源代码的定制化部分应向政务云管理单位备案；
n) 云服务客户拥有本单位VPC内部信息系统和数据完整的使用权和管理权。

7.2 IaaS 安全

政务云IaaS平台各云服务客户的业务应用系统根据自身信息系统的安全要求确定信息系统安全保护的等级，并按照相应等级基本要求实施不同安全级别的保护。

7.2.1 物理平台安全

环境安全、设备安全、介质安全、冗余备份及隔离等基本安全防护要求应按国标《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239）中的相关要求执行。

7.2.2 边界安全

7.2.2.1 ISP 边界

政务云与互联网服务提供商（ISP）的边界安全防护应由云服务提供商负责，并满足信息安全等级保护对三级系统的防护标准，同时采取有效措施及基于行为和实时的监控手段，保证政务云、互联网门户网站、相关信息系统的网络和数据的安全。

7.2.2.2 电信运营商专线

通过互联网实现移动智能终端安全接入政务云时，应部署安全接入平台，如使用电信运营商的VPDN专线时，云服务提供商应负责维护和管理，并满足如下技术要求。

a) 安全接入平台的要求可参照《国家电子政务外网安全接入平台技术规范》(GW0202-2014)；
b) 根据云服务客户的业务需求，通过安全接入平台，可实现政务人员通过移动网络访问政务云相关业务的需求及满足政务业务主动推送到指定终端的需求。

7.2.2.3 互联网边界防护

a) 应提供异常流量清洗服务，具备防范来自互联网的DDoS攻击、webshell攻击、木马病毒等各类恶意攻击。同时，外部和内部网络应提供冗余连接和带宽预留，进行流量控制和过滤；
b) 应具有基于恶意行为攻击实时监控和安全态势感知能力；对跨境数据传输等异常情况进行拦截、告警并溯源，协助云服务客户分析原因并处置；
c) 应能对云主机主动散播和被操纵主机的被动有害信息散播行为进行防护、清除并告警；
d) 应具有对未知威胁进行检测发现的能力，并且具有对web应用安全漏洞进行检测发现和攻击防御的能力；
e) 应能对已发现的攻击行为制定并执行安全策略，发现问题及时通知信息系统的责任单位并配合采取措施，消除安全隐患。

7.2.3 网络安全

a) 访问控制、攻击防范、网络审计、安全检测等要求按等级保护第三级要求中的网络与通信部分的要求执行；
b) 提供网络访问控制使云服务客户实现网络分段和隔离，包括网络过滤功能，禁止云服务客户的远程管理能够访问到非其VPC的IP地址；

c) 数据远程传输保护：用户客户端到政务云平台之间的远程数据传输应采取保护和隔离措施；
d) 除了部署传统的基于特征库的防御手段外，政务云环境应具备针对APT、零日漏洞利用、定向攻击等高级威胁检测能力，识别在政务云环境中的渗透、扩散、数据窃取等行为；
e) 应具备防火墙与安全监控系统的联动与防火墙策略迁移的能力，以方便云服务客户违规行为的及时阻断、清除安全威胁；
f) 除了部署传统的基于特征库的防御手段外，政务云环境还需要具备基于大数据技术的威胁检测、判断和关联分析能力，从而能够从全攻击链整体对安全威胁发生发展进行识别、分析和评估；
g) 应具备安全分析和可视化能力，至少可以提供安全事件展示、攻击路径展示等，并提供多维分析展示（例如：IP地址、邮件、文件、域名、受威胁资产等多个维度）。

7.2.4 主机安全

a) 政务云所有宿主机和虚拟机采用的操作系统均应满足国家标准《信息安全技术 信息安全等级保护基本要求》（GB/T22239）的相关安全要求；
b) 采用双因子认证方式对物理主机（数字证书IP地址或FC端口地址）或用户（数字证书和口令）进行身份认证；
c) 对主机的管理、操作等应通过堡垒机等技术手段，对管理员进行权限控制和审计。

7.2.5 存储安全

a) 为防止数据的永久丢失，云服务方应积极采取措施，与云服务客户一起提出可行的信息系统和数据迁移方案，明确数据镜像（或副本）及数据备份的要求，满足云服务客户对数据安全的要求；
b) 如果云服务客户的服务终止，云服务方应通知云服务客户，并应给云服务客户提供至少一个月的时间进行数据的迁移或下载，并保证删除后的数据不可恢复；
c) 按云服务客户的要求，对重要信息系统和数据在政务云上应采用加密的方式存储和备份，存储在云服务客户端或存放在其他备份云平台上的数据，应采用多因素认证配合才允许进行修改或删除，同时政务云服务方应至少每年对重要信息系统的数据配合云服务客户进行数据恢复的测试；
d) 应对用户鉴别信息、审计日志等关键信息予以完整性和保密性保护；
e) 应能针对政务云平台内不同云服务客户的存储数据进行有效隔离，防止政务云不同云服务客户间非授权访问敏感数据；
f) 由云服务客户决定自身业务数据是否加密；
g) 存储设备应具有工业级的高可靠性设计，支持并发访问，保证政务云平台各云服务客户的业务不间断，并可防止非授权访问；
h) 对物理主机或用户、密钥生成签名进行身份认证；
i) 采用访问控制机制，云服务客户所持有资源的任何访问需要检测资源的请求者是否具备访问的权限，防止多云服务客户间的非授权访问；
j) 应采取相应技术措施对存储资源池或分布式存储集群的访问进行实时的控制，对异常情况应能实时告警，并及时通知云服务提供商、运维人员和云服务客户管理人员。

7.2.6 抽象控制安全

a) 控制器安全主要包括身份认证、授权管理和操作审计，具有行为的鉴别、访问控制及异常行为的实时预警功能，并应通过安全审计进行分析、溯源、定位及安全预警；
b) 针对云服务方管理员和云服务客户管理员，分别设置不同的职责和权限，对管理员的身份进行多因素认证，所有操作应进行审计；

c) 云服务方提供的控制器（如虚拟化和SDN）应开放标准的API接口供云服务客户自行选择通用的安全解决方案；
d) 控制器（如SDN控制器）应具备冗余能力，保证政务云中的管理系统提供持续使用的能力；
e) 云服务客户的管理员对资源调度使用应具备与云服务方管理员联合审批及安全接入的功能，如专用终端、堡垒机、专用账户、强密码和多因素身份验证。

7.2.7 虚拟网络

a) 应实现云计算环境业务网络与管理网络的有效隔离，包括云服务客户使用的基础设施、云服务方的管理网络以及内部局域网。应制定各应用系统的访问控制策略并实时监控策略的有效性；
b) 部门业务区中，云服务方应为不同的云服务客户分配不同的VPC，每个VPC之间不能直接进行通信，同时解决不同云服务客户间可能产生的地址重叠问题；
c) 云服务客户的局域网边界通过接入路由器接入电子政务外网的城域网，在网络上可将各云服务客户用MPLS VPN进行隔离，在政务云侧为每个VPN接入的云服务客户分配不同的路由表。通过路由或ACL访问控制列表对应每个云服务客户的VPN，实现云服务客户网络的隔离；
d) 云服务方应具备为每个云服务客户提供独立安全服务的能力，明确安全服务的功能、性能、实现的安全目标及在政务云上的部署位置，如虚拟防火墙、虚拟IPS等，其安全防护设备的安全策略应与云服务客户共享，应对安全策略实施的有效性进行监测和控制；
e) 云服务客户拥有VPC内部信息系统和数据完整的使用权和管理权。

7.2.8 虚拟主机

a) 虚拟机的隔离、漏洞发现与修复、安全配置及访问控制等策略，应满足不同云服务客户信息系统的安全需求。其安全策略及访问控制权限应由云服务客户自行决定；
b) 云服务客户内部信息系统虚拟机之间的访问控制及实时安全监测应能发现异常，通知云服务客户并及时处置。对虚拟机的访问、迁移、动态扩展及使用状态应做好审计和记录；
c) 云服务方应根据云服务客户要求开通虚拟机，并保证虚拟机的正常使用。应具备实时监测的能力，及时向云服务客户提供安全事件取证、溯源、定位及处置的能力；
d) 云服务方应提供虚拟机之间可配置的访问控制机制，使同一云服务客户的不同虚拟机之间可以设置访问控制策略；
e) 虚拟机出现异常，云服务方应及时采取有效措施，保证云服务客户业务不中断；
f) 应为云服务客户提供配置安全和完成补丁修复的虚拟机模板，避免新的虚拟机被分配同样的弱口令；
g) 承载信息系统安全等级第三级的虚拟机，应对其进行加固，并对重要信息资源进行标记；
h) 虚拟机迁移或动态扩展时，应做好资源变更记录和审计；
i) 云服务客户应确认云服务方或应用开发方对虚拟机的操作系统（包括操作系统补丁升级）、虚拟网络配置以及虚拟安全配置的修复；
j) 应确保每个云服务客户都有独立的计算资源，其中包括CPU、内存、存储、外设和地址空间等；
k) 云服务方应根据云服务客户需求，具备对VPC内部虚拟机所承载的不同业务进行划子区域或安全组的能力，及时发现并阻断VPC内部的恶意攻击；
l) 应具备将VPC内部流量通过隧道等技术导出到物理或虚拟安全防护设备的能力；
m) 安全防护设备应具备根据业务可弹性、快速生效和可被软件定义的池化安全处理能力。

7.2.9 虚拟存储

a) 所有云服务客户的信息系统应按照安全要求，挂载到存储资源池相应的逻辑分区中；
b) 云服务客户拥有VPC内部信息系统和数据完整的使用权和管理权。

7.3 PaaS 安全

PaaS安全除满足7.2节对IaaS安全的要求外，还应满足如下要求：

7.3.1 接口安全

a) 应采用密码技术，保障资源访问的API接口安全；
b) 应对开放的API接口的调用行为及数据异常情况的监控和告警，发现问题及时通知云服务客户，并协助云服务客户及时处置；
c) 政务云中间件接口，对应用开发的API接入进行安全测控和异常分析，以及对开发环境的安全检测；
d) 应对中间件、数据库及应用开发的API接口标准化，并通过政务云管理单位正式发布。

7.3.2 开发环境安全

a) 应对开发环境提供给云服务客户的数据库、中间件等服务进行定期的漏洞监测，及时执行补丁更新；
b) 应对云服务客户的应用系统软件及使用情况进行监测，对应用系统代码漏洞或异常应及时通知云服务客户，并督促其及时整改；
c) 应对开发环境中数据库/中间件服务的使用，端口的开放及使用过程进行实时监测和控制，保证政务云的安全；
d) 应对云服务客户上传的文件、镜像和开发工具进行安全检测，防止其VPC内部的扩散，影响云环境安全运行。

7.3.3 中间件安全

a) 安装其适用的所有安全补丁；
b) 启用访问控制功能，依据安全策略控制云服务客户对中间件服务的访问；
c) 对应用部署的中间件服务状态进行实时监控，并对云服务客户访问中间件服务的过程进行实时监控；
d) 应对云服务客户登录访问中间件服务的所有访问和操作行为进行审计，以便事后追查。

7.3.4 数据库安全

a) 应及时验证并更新安全补丁；
b) 通过保障帐号和密码安全、服务配置安全、审计安全，管理扩展存储过程、传输保护配置、服务端口和网络连接安全配置、数据库应用系统的安全设置提高数据库的安全性；
c) 提供应用部署的数据库服务状态实时监控；
d) 通过建设数据库审计系统对数据库访问和操作行为进行审计，以便事后追查；
e) 提供应用部署的中间件服务状态实时监控，并对云服务客户访问中间件服务的过程进行实时监控；
f) 在云服务客户访问敏感数据服务时，应调用加密算法模块，对整个报文或会话过程进行加密，保证通信保密性；
g) 启用访问控制功能，依据安全策略控制云服务客户对数据库服务的访问；
h) 通过设置系统、网络、安全管理员和安全审计员等管理人员及职责，按照最小权限的安全策略明确各自的职责。

7.4 SaaS 安全

SaaS安全除满足7.3节所述的PaaS安全外，还应满足如下要求：

7.4.1 应用安全

a) 应用安全防护要求按国标《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239）中的相关要求执行。

7.4.2 应用开发安全

a) 应用开发安全防护要求按国标《信息安全技术 信息系统通用安全技术要求》（GB/T 20271）中的相关要求执行。

7.5 数据保护要求

7.5.1 应用迁移安全

a) 云服务客户应对拟迁移至云计算平台应用系统的敏感度和业务重要性进行分析和评估，按照应用系统敏感度和业务重要性要求云服务方提供相应的安全防护能力，禁止将涉密数据迁移至云平台；
b) 云服务方应配合云服务客户对云计算平台进行全面风险评估，确保云平台的安全防护能力不低于拟迁移信息系统的安全保护等级；
c) 应采用专线或加密隧道技术承载云服务客户业务数据的迁移，数据迁移时应对云服务客户的身份进行认证识别，采用访问控制措施保证迁移路径的安全可靠并对迁移来的数据执行恶意代码检测和清除；
d) 应采用密码技术保证云服务客户终端与云环境通信过程中的完整性；
e) 云服务客户应优先将备份系统中的数据迁移至云计算平台；
f) 云服务方应提供应用测试环境，在云服务客户迁移完成后对部署在云计算平台上的业务进行全面的可用性测试。

7.5.2 身份认证与授权

a) 对登录访问应用服务（技术服务、业务服务、数据服务）的云服务客户进行身份识别和鉴别；
b) 应启用身份鉴别、云服务客户身份标识唯一性检查、云服务客户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；
c) 应启用访问控制功能，依据安全策略控制云服务客户对应用服务（技术服务、业务服务、数据服务）、文件（配置文件、日志文件、镜像文件）等客体的访问；
d) 基于单位、角色控制的资源访问权限，并支持细度的权限控制（修改、只读、无权限），仅授予云服务客户所需的最小权限；
e) 授予不同角色为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
f) 应对重要信息资源设置敏感标签，并依据安全策略严格控制云服务客户对有敏感标记重要信息资源的操作，并做好相关审计记录。

7.5.3 账户保护

a) 定期针对数据保护、重要信息资源访问进行测试，并验证政务云具备相关的取证和分析能力，包括实时事件的记录，磁盘镜像，内存快照和自身的元数据（包括存储位置、历史数据、文件记录等）；
b) 云服务客户的账户和密码不得泄露给第三方，至少三个月应更改一次密码，使用复杂密码且密码位数不少于14位；
c) 云服务客户应使用安全受控的终端、双因子认证，受限的访问权限和传输加密的方式访问并管理云上的资源；

d) 云服务客户应禁止或避免给云服务方提供自己的账号权限（或开放接入能力）及密钥口令，让云服务方能够接入云服务客户自己的重要信息系统中，例如云服务客户的高等级业务；
e) 云服务方在对云进行管理或对云服务客户资产进行故障诊断或技术支持及远程操作时应控制管理员的权限，及系统和数据的访问特权，防止云服务的滥用。对于已经批准的临时特权，应有记录并在3个月内予以撤销；
f) 根据业务特点，云服务方应区分系统管理员、安全管理员及安全审计员等各管理员角色，不可兼任；
g) 平台不可明文存储口令数据；
h) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

7.5.4 数据加密

a) 应保证系统管理数据（如索引文件、云服务客户信息及密钥等）、鉴别信息和重要业务数据（如用户隐私数据）存储和传输的完整性和保密性；
b) 云服务客户管理员客户端到政务云平台之间的远程数据传输应采取加密机制保护和隔离措施；
c) 对应用系统中的重要数据应采取密码机制保护措施，以保证数据的保密性和完整性；
d) 应支持基于硬件密码设备的数据加密机制，所使用的硬件密码设备和密码算法应当符合国家标准和国家密码管理局的相关要求；
e) 云服务客户数据加密所使用的密钥应由用户管理；
f) 政务云平台可在云平台中构建硬件密码资源池，供云服务客户使用；
g) 政务云平台负责硬件密码资源的分配，并确保只有云服务客户的VPC才能访问所分配的密码资源；
h) 云服务客户的硬件密码资源应为独占方式，禁止不同云服务客户共享硬件密码资源，政务云应确保不同云服务客户间的隔离；
i) 云服务客户可以通过远程网络管理自己的密码资源和密钥，在管理时应经过基于硬件介质的身份认证，所有通讯数据应被加密；
j) 政务云应提供一种或多种技术手段，使云服务客户可以使用密钥基础设施对敏感数据进行加密，可选的方式包括卷加密、数据库加密、应用系统调用API加密等。

7.5.5 密钥管理

a) 密钥的生成、存储、使用和管理应符合国家密码管理局关于商用密码的相关管理要求和国家标准；
b) 政务云可以自建统一的密钥管理系统，也可以选择支持第三方密钥管理系统（如电子政务外网CA），或支持用户自行管理密钥，所使用的密钥管理系统应当符合国家密码管理局的相关要求；
c) 政务云平台应对云服务客户提供密码设备服务，平台负责密钥基础设施的资源分配和网络连通，云服务客户负责对密钥基础设施进行配置，政务云平台所提供的密钥基础设施服务应当设置严格的鉴别机制，保证只有云服务客户才能对密钥基础设施进行配置，且只有云服务客户的应用才能使用云服务客户的密钥基础设施；
d) 加密密钥应在专门的密钥生成系统或密钥基础设施中生成，密钥数据必须密文存储且与业务数据存储分离，关键密钥如主密钥、签名密钥等需存放在安全介质中或密钥基础设施中。且关键密钥在云平台上使用时，必须存放于密钥基础设施中。非关键密钥信息如会话密钥等可以以密文形式保存在密码资源外部，但不能在任何情况下以明文形式出现在密码资源外部；
e) 政务云平台应确保云服务客户密钥在使用中处于独立的安全环境或云服务客户专用密钥基础设施中；

f) 政务云平台应提供安全的证书更新机制，确保云服务客户加密资源释放时，云服务客户证书被撤销；
g) 政务云自建的统一密钥管理系统，应确保不同云服务客户间的密钥隔离，政务云平台所使用的密钥和云服务客户密钥不得在同一系统中进行管理，政务云平台的服务管理人员和密钥管理人员不得兼任；
h) 未经云服务客户明确授权，政务云平台不得查询、修改、删除云服务客户密钥及相关信息；
i) 密钥在停止使用后，必须及时销毁且不可恢复。

7.5.6 剩余信息清除

a) 用户存储空间清除：应保证虚拟机用户的磁盘存储空间被释放或再分配给其他用户前得到完全清除，不能通过软件工具恢复；
b) 管理文件空间清除：应确保虚拟机监视器（Hypervisor）和云管理平台内的文件、目录、数据库记录和其他资源等所在的存储空间，被释放或重新分配给其他用户前得到完全清除；
c) 鉴别信息清除：应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除；
d) 快照信息清除：在迁移或删除虚拟机后应确保镜像文件、快照文件等数据的清除以及备份数据清除；
e) 虚拟机内存清除：应保证虚拟机的内存被释放或再分配给其他虚拟机前得到完全清除；
f) 设备置零：集中存储过重要信息的存储部件在报废、维修、重新利用前，应采取技术手段进行硬件置零处理；
g) 云服务客户将信息系统和数据退租后，云服务方应清除相关数据且不可恢复。

7.5.7 备份与灾难恢复

a) 同城系统备份的两个数据中心之间距离在50公里以内，信息系统能迅速恢复使用；
b) 异地数据备份与主用数据中心之间距离在200公里以外，只做数据级备份；
c) 应满足数据恢复和重建目标的需求。通过确定备份时间、技术、介质和场外存放方式，以保证达到RPO和RTO的要求，具体标准应通过云服务方，云服务客户和云管理单位三方确定；
d) 政务云数据备份及灾难恢复要求遵循 GB/T 30285 《信息安全技术 灾难恢复中心建设与运维管理规范》及 GB/T 31500 《信息安全技术 存储介质数据恢复服务要求》。

7.5.8 数据完整性校验

a) 应提供虚拟机镜像文件完整性校验功能，对虚拟机镜像被篡改应能及时发现并告警；
b) 应对虚拟机配置文件、虚拟机模板、云服务客户账户数据、管理员及权限等管理数据采取数据保护措施，经完整性校验后方能部署使用。

7.5.9 通信安全

a) 应采用由密码技术支持的完整性校验机制或具有相应安全强度的其他安全机制，以实现通信网络数据传输完整性保护；
b) 采用由密码技术支持的保密性保护机制或具有相应安全强度的其他安全机制，以实现网络数据传输保密性保护；
c) 通过对连接到通信网络的设备进行认证，确保接入通信网络的设备真实可信，防止设备的非法接入。

7.5.10 安全审计

政务云的审计也是政务云能正常应用的关键，除了对传统的行为、数据库、运维人员等审计外，还需要根据云计算的特点，对远程操作管理、资源调度和弹性扩展等进行审计，其审计应通过第三方的审计产品进行独立审计，审计要求包括：

a) 所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致；
b) 确保日志存储中有足够的存储空间可保存半年以上，且必须定期归档并予以标记；
c) 对于异常的审计结果需要定期提供报告，并验证异常事件；
d) 云服务客户通过连接到政务外网城域网的线路访问互联网时，其互联网出口的安全防护应具备URL过滤能力。云服务方应提供URL分类服务，以确保最新的网站类别定义；
e) 确保日志包括日期，时间戳，源地址，目的地址，各种可分析的元素，同时对于收集的日志的格式，需要具备统一规范化的手段；
f) 从云服务客户行为审计、资源变更审计和管理操作审计等三方面，保证政务云处于可控状态。

7.5.11 数据同步

a) 互联网区VPC内信息系统和数据与部门VPC内部数据或公共区VPC数据实施数据同步时，应采取严格的安全隔离和访问控制策略；
b) 安全数据交换系统中的数据格式、内容及流量等应做到实时监测和实时控制。其访问控制策略的制定、实施和管理由云服务客户与云服务方管理员共同负责；
c) 安全数据交换系统应满足云环境下的各类弹性要求。如前后端部门/业务非对称性的接入，要求安全接入系统可以提供灵活的部署方式，提供弹性的资源调度模式，提供基于部门/业务的强安全隔离的安全数据交换方式。政务云跨VPC数据同步方法见附录A。

7.5.12 数据共享与交换

部门间VPC之间和公共区VPC之间的数据共享与交换，应制定不同信息系统及数据库相关字段级的共享与交换规则，按政务信息资源目录的要求，实现不同虚拟专有云（VPC）之间的应用系统、数据库、视频等需要通过细粒度的路由策略进行访问范围限制，同时在路由可达的基础之上，利用防火墙或虚拟防火墙对跨VPC的访问流量进行访问控制。达到跨部门的数据共享与交换。

8 政务云管理要求

8.1 云服务客户

a) 云服务客户单位向政务云进行信息系统迁移时或部署信息系统时，应制定相关的技术方案，明确安全责任边界及基于风险分析基础之上的安全计划和控制策略，从网络、主机、应用和数据安全及备份恢复等方面提出具体要求，满足信息系统安全等级保护技术要求；
b) 接受政务云管理部门对云服务客户安全工作的指导、监督、检查和考核；
c) 云服务客户承担应用系统部署及管理，以及自身业务和数据安全、客户端安全等相关责任；
d) 云服务客户应用迁移时，应对拟迁移至云计算平台的应用系统的敏感度和业务重要性进行分析和评估，按照应用系统敏感度和业务重要性要求云服务方提供相应的安全防护能力，禁止涉密数据迁移至云平台；
e) 云服务客户的局域网及终端安全由各云服务客户自行负责；
f) 云服务客户在政务云上的信息系统及内部系统之间的访问控制由云服务客户负责；
g) 完成风险评估和损失评估后，安全策略应明确数据安全的要求，如数据副本的数量、存储的物理位置，根据数据的重要程度明确数据备份的RPO和RTO，明确数据是否需要加密存储；
h) 云服务客户管理员应使用安全受控的终端、多因素认证、复杂密码（至少14位），受限的访问权限和传输加密的方式访问并管理政务云上的资源。

8.2 政务云管理单位

a) 云管理单位监督云服务方执行安全配置，持续的脆弱性管理，及时修补漏洞，定期邀请第三方安全评估和渗透测试机构对云服务和基础设施进行评估；
b) 云管理单位应组织审查云服务方和云服务客户的网络安全应急预案并确保云服务方进行应急演练，相互配合，以满足云服务客户对业务连续性的要求，例如制定关于云服务遭遇网络攻击造成基础设施损失等事件的应对措施；
c) 审定各云服务客户单位向政务云进行信息系统迁移时或部署信息系统时的技术方案、安全责任边界及基于风险分析基础之上的安全计划和控制策略；
d) 对政务云建设及运营开展行政监管，指导政务云服务机构开展对政务云的运维（安全监管）工作，并负责监督检查、考核及相关服务费用审定；
e) 在云服务客户退出云计算服务时，监督云服务方履行相关责任和义务，确保退出云计算服务阶段的数据和业务安全；
f) 应定期组织对云服务客户的技术、安全及业务等方面的培训；
g) 应明确政务云与政务外网的边界，云服务客户信息系统与政务云的边界，及政务云上云服务客户之间的边界，以及相应边界访问控制的策略、责任和安全要求。

8.3 云服务方

a) 为云管理单位提供各类资源的使用报告，指导云服务客户的资源申请和退订；
b) 对云服务客户定制培训计划并提供定期的培训，培训内容至少包括数据维护、系统维护和安全管理及事件处理流程要求等；
c) 为云服务客户制定应急预案及安全事件处置响应计划，对数据的使用进行实时的监测及审计；
d) 对开放云管理系统的API接口应实时监测，发现异常及时告警；
e) 为避免云计算管理员账户和云服务客户管理员账户被恶意劫持，应予重点保护，对管理员信息、登录密码等数据进行加密保护，并做好备份；
f) 应定期向政务云管理部门提交各云服务客户安全情况TOP排名，资源使用率高、低的TOP排名及对重点云服务客户的安全保障情况；
g) 云服务方应有针对政务云服务的安全责任书面承诺，尤其对政务云上所有的数据不出省或按省政务云管理部门的要求作出承诺；
h) 应对所有设备相关的安全策略定期或不定期备份，并制定管理办法；
i) 云服务客户终止服务后，对云服务客户的信息系统、数据的处置，应有书面协议，说明信息系统、数据、管理员的账号密码的处理过程及安全要求；
j) 要求政务云服务方对政务云应进行7*24小时的实时行为监测，对已知特征的网络攻击行为进行预警。能够利用入侵节点的告警进行汇总分析，发现不同告警日志内在联系，并对相关云服务客户提出预警信息，对确定的信息安全事件，协助云服务客户及时处置并形成事件处置报告报政务云管理部门和相关云服务客户；
k) 在对政务云进行管理或对云服务客户资产进行故障诊断、技术支持、远程操作或管理时应严格限制管理员的管理权限，按职能划分系统管理员、网络管理员、安全管理员及审计员等，明确各管理员的岗位职责和作业流程。需要远程管理时，应限制权限，并进行审计，防止云服务的滥用；
l) 接受政务云管理部门对云计算环境使用及安全工作的指导、监督、检查和考核；
m) 应保证政务云计算、网络、存储及其他各基础设施安全并满足云服务客户业务的需要；
n) 应提供实时的网络、系统和业务实时监测、分析、预警和应急处置的服务，保证各类业务的连续性；

o) 应主动提供基于应用的漏洞检测、行为及数据异常情况的告警，发现问题及时通知云服务客户，并协助云服务客户及时处置；

p) 应与其技术员或其指派的代维机构和人员签订保密协议，确保不泄露政务云平台承载的信息；

q) 已经形成的安全事件分类分级要遵从国家标准《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986），在对政务云实时监测过程中，应对各类安全事件进行分类分级，不论是被安全设备阻断的各类网络攻击行为，还是国家信息安全主管部门网络安全检查及第三方相应机构授权检测，或云服务方主动扫描检测发现的异常等，均需要进行归类分析、预警及统一的报告。政务云的安全事件分类分级见附录 B。

附录 A

（资料性附录）

政务云 VPC 之间跨网数据交换方法示例

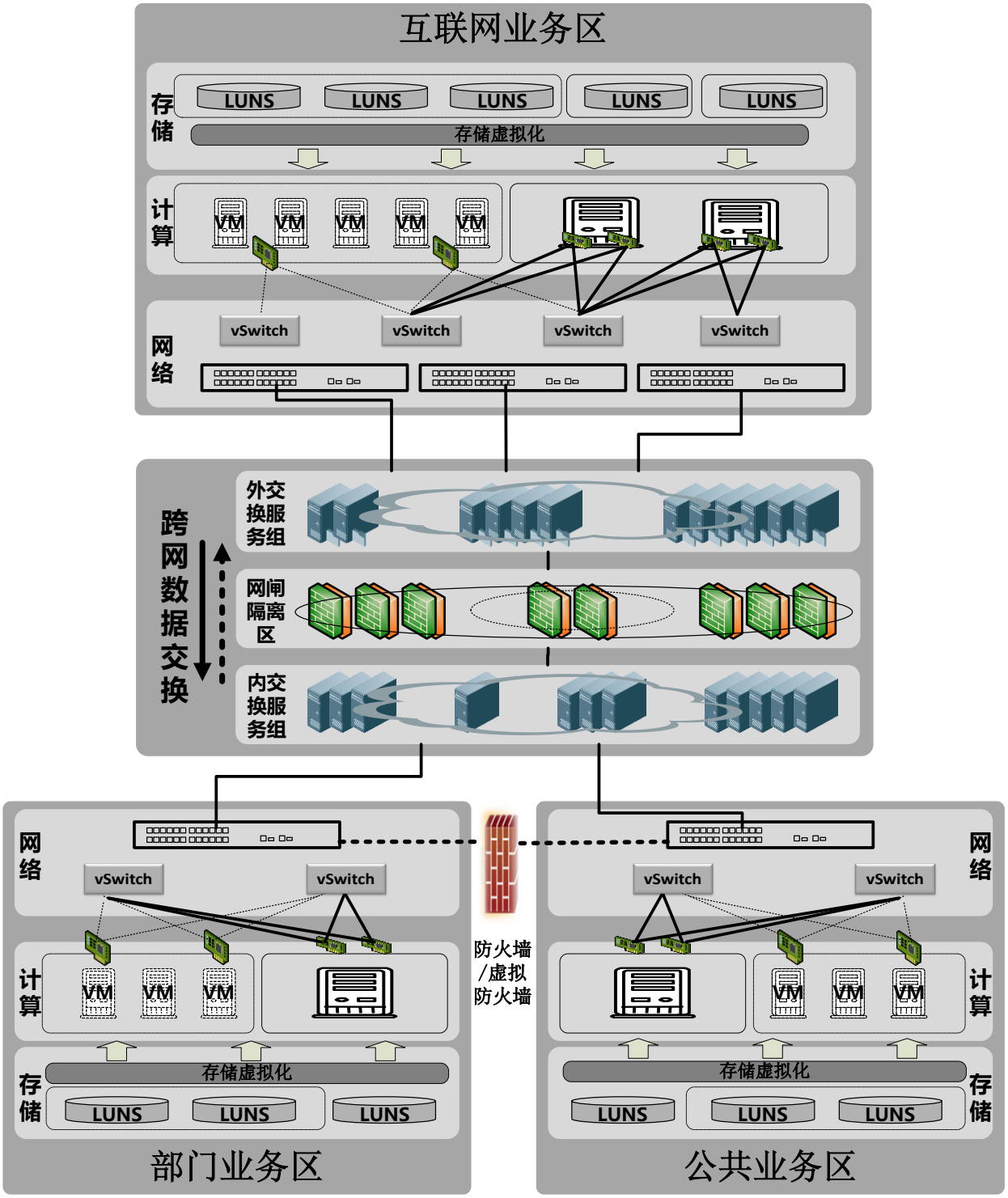
互联网业务区与部门业务区或公共业务区的跨网数据交换：云服务客户有一台或多台VM的数据需要向互联网业务区同步数据，配置一台至多台宿主机，宿主机上面配备2块以上的物理网卡，分别与业务核心交换机、数据隔离区相连。一块负责虚拟前置机组的前端业务实时同步交互，一块负责系统向互联网业务区处的虚拟或物理后端机同步数据。

跨网数据交换系统集群支持基于业务的部署模式，支持非对称的接入方式。

具体包括内网交换服务器组：部署于各部门业务区或公共业务区；外网交换服务器组：部署于互联网业务区；网闸隔离组：部署于非互联网区域；支持多部门多业务接入，允许单独根据部门构架其基于内部应用的资源池，并支持资源扩容等功能。

具体技术要求及部署方式可参照国家电子政务外网管理中心印发的《国家电子政务外网跨网数据安全交换技术要求与实施指南》（GW0205）。

详见下图：


互联网业务区
存储
LUNS
LUNS
LUNS
LUNS
LUNS
存储虚拟化
计算
VM
VM
VM
VM
VM
网络
vSwitch
vSwitch
vSwitch
vSwitch
跨网数据交换
外交换服务组
网闸隔离区
内交换服务组
网络
vSwitch
vSwitch
计算
VM
VM
VM
存储
存储虚拟化
LUNS
LUNS
LUNS
部门业务区
防火墙/虚拟防火墙
网络
vSwitch
vSwitch
计算
VM
VM
VM
存储
存储虚拟化
LUNS
LUNS
LUNS
公共业务区

附录B

（规范性附录）

政务云安全事件分类分级规范

已形成的安全事件分类分级要遵从国家标准《信息安全技术　信息安全事件分类分级指南》（GB/Z 20986），政务云的安全事件分类分级见下表：

政务云安全事件分类分级规范		
类别	**一级分类**	**二级分类**
0	授权训练、演习、调查	授权的渗透测试、漏洞扫描等。
1	成功入侵	木马入侵、病毒入侵、后门入侵、漏洞入侵、猜口令成功、网络攻击等。
2	不成功的入侵行为企图	猜口令、SQL 注入尝试、非授权访问等。
3	拒绝服务攻击	短包、流量、DNS 放大攻击等。
4	违规行为	非法外联、安全策略不正确、误操作等。
5	嗅探踩点	非授权漏洞扫描、常用服务探测等。
6	可识别的异常	异常跨境数据传输、软件后门（尚未受控）、系统漏洞、不当使用等。
7	其他未知异常	0day，网络攻击及所有未知异常的行为。