1. **项目名称**：自治区机关事务信息化平台房地产管理系统云服务器租赁服务项目采购需求

**2.项目单位：**新疆维吾尔自治区机关事务管理局

**3.项目需求**：自治区机关事务信息化平台房地产管理系统云服务器租赁服务项目采用购买服务方式建设，房地产管理系统云服务器为私有云性质，全部由专网区服务器组成，本项目服务内容包含房地产管理系统云服务器专网区承载服务、房地产管理系统云服务器运维服务、房地产管理系统云服务器数据灾备服务、房地产管理系统云服务器网络安全运维服务以及与机关事务专属云互联网区数据对接服务。提供400核vCPU，800G内存和250T存储空间，提供云服务器网络安全服务，提供数据备份服务，数据定期备份至异地数据中心，包含30T可用备份空间以及100M链路，具备通过《信息安全技术网络安全等级保护基本要求》第三级安全保护标准测评和《信息安全技术信息系统密码应用基本要求》第三级标准测评；提供云服务器资源服务的供应商须按照中央网信办相关工作要求，通过云计算服务安全评估。提供的云服务器基础设施具有连续性，确保自治区机关事务局房地产管理系统现有业务不间断，安全有效运行。

根据财政部令《政府购买服务管理办法》中第二十四条，政府购买服务合同履行期一般不超过1年；在预算保障的前提下，对于购买内容相对固定、连续性强、经费来源稳定、价格变化幅度小的政府购买服务项目，可以签订履行期限不超过3年的政府购买服务合同。自治区机关事务管理局对中标方服务期内的服务内容和质量等进行评估。如符合条件，待一年服务期届满再续签两年。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | | 数量 | 单位 | 货物/服务 | 备注 |
| 1 | 云服务器  资源服务 | | 1 | 项 | 提供独立的专属云资源，CPU 240核，内存480G，150T存储空间，含机柜、云安全等基础配套。 |  |
| 2 | 网络安全服务 | | 1 | 项 | 提供防火墙、入侵防御、WAF产品服务 |  |
| 3 | 数据灾备服务 | | 1 | 项 | 提供独立的专属云资源，CPU 160核，内存320G，100T存储空间，含机柜、云安全等基础配套；提供数据备份服务，数据定期备份至异地数据中心，包含30T可用备份空间以及配套软硬件、100M链路。 |  |
| 工期要求 | | 服务自合同签订之日3个日历日内完成项目交付。 | | | | |
| 总预算 | |  | | | | |
| 备注 | |  | | | | |

**4.项目要求：**

**云服务器资源服务要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **具体要求** | | |
| ★资源要求 | CPU（核） | 内存（GB） | 存储空间（TB） |
| 240 | 480 | 150 |
|  | ★投标人提供的云服务器资源，招标人享有独立使用权，独立的网络，不接受公有云模式； | | |
| 基本要求 | 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等。 | | |
| 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。 | | |
| 提供统一的虚拟机管理界面，在同一界面上提供虚拟机启动、暂停、恢复、休眠、重启、安全关闭、关闭电源、克隆、迁移、备份、快照、克隆为模板、修改等生命周期管理功能。 | | |
| 支持虚拟机规格的在线和离线调整，包括CPU、内存、硬盘、网卡等资源，当虚拟机操作系统本身的前提下，热添加的CPU/内存可以即时生效。 | | |
| 资源管理能力 | 支持批量修改虚拟机的配置参数，包括：CPU调度优先级、CPU个数、内存大小、I/O优先级、启动优先级、是否自动迁移、tools自动升级等，提供产品截图证明。 | | |
| 支持集群动态资源调度功能，可基于主机的CPU、内存、网络流量、连接数、磁盘IO、存储容量等资源利用率对虚拟机进行动态资源调度，实现全自动化的资源分配和负载平衡功能，主动确保云环境的服务水平，提供产品截图证明。 | | |
| 支持配合负载均衡设备根据业务的负载情况实现业务系统虚拟机的动态扩展和回收，能够根据虚拟机CPU、内存、连接数、存储容量、磁盘IO等参数动态的克隆虚拟机或删除虚拟机，满足业务突发流量响应需求，实现资源的随需而动，提升资源利用率，节约投资，提供产品截图和至少3份用户使用证明。 | | |
| 支持当虚拟机的CPU、内存利用率超过设置的阈值时，在虚拟机操作系统本身支持资源热添加的前提下，系统将自动为该虚拟机增加相应的CPU和内存资源，无需人工干预。 | | |
| 数据安全 | 提供虚拟机快照功能，支持设置手工和定时快照将虚拟机磁盘文件和内存状态信息保存到镜像文件中。 | | |
| 提供虚拟机回收站功能，统一管理被删除的虚拟机，防止因虚拟机误删除导致数据丢失，支持设置回收站文件保存周期，超期的文件将被自动删除，支持批量销毁或还原虚拟机。 | | |
| 支持虚拟机迁移历史记录功能，记录中包含迁移的操作员、迁移方式、源主机、目的主机、开始时间、迁移耗时等信息，便于对虚拟机的迁移路径进行回溯。 | | |
| 运维能力 | 支持使用一键鼠标按钮分析虚拟机、主机历史资源使用情况，提供规划决策数据支撑。提供产品功能截图。 | | |
| 支持使用一键鼠标按钮分析后端存储上的无效镜像文件，并提供一键清理和释放存储空间能力，提升资源利用率，保障投资。要求提供CNAS认可的检测机构出具的检测报告检测结果及检测结果截图页并有制造商盖章作为证明材料，未提供视为不满足。 | | |
| 支持使用一键鼠标按钮快速查看、启动、删除、批量启动和批量删除长时间未使用且处于关闭状态的虚拟机，进行资源利用率统计，降低运维工作量与难度，保障投资。要求提供CNAS认可的检测机构出具的检测报告检测结果并有制造商盖章作为证明材料，未提供视为不满足。 | | |
| 支持一键切换大屏展示功能，直观展示虚拟化资源池的健康度、告警、资源使用情况等虚拟化环境，同时支持展示内容用户自定义，方便用户日常监控。 | | |
| 防病毒能力 | 支持虚拟化内核集成虚拟化安全防护功能模块为虚拟机提供防护，无需单独占用虚拟机资源安装安全防护功能模块，只需在虚拟化环境底层安装安全防护功能模块，不需要在每台虚拟机上安装，对每个虚拟机没有资源占用。 | | |
| 支持主流Windows和Linux操作系统无代理底层防病毒能力，不需要在虚拟服务器或虚拟桌面中部署安全防护代理。 | | |
| 杀毒授权 | 配置杀毒AV和DPI授权，配置不限主机数量授权。 | | |
| 信息安全技术网络安全等级保护 | 投标人所提供的云平台需要满足《信息安全技术网络安全等级保护基本要求》第三级安全保护标准，等保测评得分需在85分及以上并提供测评报告。 | | |
| 商用密码应用安全性评估 | 投标人所提供的云平台在通过《信息安全技术 网络安全等级保护基本要求》第三级安全保护标准评测后，需要通过商用密码应用安全性评估，密码测评得分需到70分及以上并提供测评报告。 | | |

**云安全管理平台要求**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 基本要求 | ★投标人所提供的云安全管理平台需要与招标人互联网区实现共管共用，且不额外收取费用，提供承诺。 |
| 功能要求 | ★产品具备综合日志审计功能、漏洞扫描功能、运维审计、数据库审计、终端杀毒功能 |
| [★可统一在管理平台进行版本升级、授权激活、账户密码配置等（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_可统一在管理平台进行版本升级、授权激活、账户密码配置等) |
| [★可统一在管理平台展示CPU、内存、磁盘的资源使用情况，统计展示一天、一周、30天内设备告警情况，并对重要告警信息进行展示（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_可统一在管理平台展示CPU、内存、磁盘的资源使用情况，统计展示一天、一) |
| [★可统一在管理平台对各个组件的运维数据进行集中统计展示（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_可统一在管理平台对漏扫、日志审计、运维审计、数据库审计、终端杀毒等各个) |
| [★可在管理平台进行各个组件的基础安全业务策略配置的免跳转下发（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_可在管理平台进行漏扫、日志审计、运维审计、数据库审计、终端杀毒等各个组) |
| [★具备脆弱性大屏展示功能，直观展示内网各类设备漏洞情况（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_具备脆弱性大屏展示功能，直观展示内网各类设备漏洞情况) |
| [★具备安全合规大屏展示功能，直观展示内网各类设备安全现状，并对各类设备的安全情况进行打分评定，帮助用户直观感受内网安全情况（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_具备安全合规大屏展示功能，直观展示内网各类设备安全现状，并对各类设备的) |
| [★具备数据库安全大屏展示功能，直观展示数据库安全现状（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_具备数据库安全大屏展示功能，直观展示数据库安全现状) |
| 日志审计功能要求：满足功能项“综合日志审计系统功能”的要求 |
| 漏洞扫描功能要求：满足功能项“漏洞扫描系统功能”的要求 |
| 运维审计功能要求：满足功能项“运维审计系统功能”的要求 |
| 数据库审计功能要求：满足功能项“数据库审计系统功能”的要求 |
| 终端杀毒功能要求：满足功能项“终端杀毒功能”的要求 |
| 部署模式 | 设备采用旁路部署模式，系统与目标资源IP可达，协议互通即可，不需要改变网络拓扑结构 |
| 日志查看 | [★支持按照日志类型进行查询，支持操作日志、审计日志、流量日志、威胁日志、主机日志等11大类70子标签进行分类；支持多条件查询，包含开始时间、结束时间、动作类型、设备名称、日志等级、用户名、源IP、目的IP、协议等条件进行过滤查询展示（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持按照日志类型进行查询，支持操作日志、审计日志、流量日志、威胁日志、) |
| 全文检索 | [★支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式（需提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容) |
| 主机漏洞扫描 | [★主机漏洞知识库可检测漏洞数量51000+，其中可检测CVE漏洞数不低于48400+个，非CVE漏洞数不低于3000+个,漏洞信息全中文支持，提供漏洞名称、威胁类型、风险级别等漏洞信息详细描述及其对应的解决方案（提供界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_主机漏洞知识库_2) |
| [★支持针对多种协议进行口令猜测，系统应内置至少包括SMB、SSH、TELNET、RDP、POP3、SNMP等多种协议的用户字典与口令字典，允许用户使用自定义的用户字典与口令字典（提供界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_口令破解_1) |
| [★支持IPV4、IPV6双协议栈地址扫描（提供界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持IPV4、IPV6双协议栈地址扫描) |
| 数据库漏洞扫描 | [★数据库漏洞知识库可检测漏洞数量1560+，提供漏洞名称、威胁类型、风险级别等漏洞信息详细描述及其对应的解决方案（提供界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_数据库漏洞知识库_1) |
| [支持对数据库进行帐户口令认证登陆，登陆到相应的数据库中对特定应用进行深入扫描，其中主流数据库类型支持包括不局限于Oracle、Mysql、MSSQL、DB2、Informix、Sybase、达梦等7种数据库类型（提供界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_各种主流数据库类型认证深度扫描_1) |
| 性能要求 | 最大图形并发连接数不少于150，最大字符并发连接数不少于300 |
| 账号同步 | [★支持AD账号的自动化同步，可将未纳管的AD账号自动添加到系统中并自动赋予指定角色，无需管理员干预（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持AD账号的自动化同步，可将未纳管的AD账号自动添加到系统中并自动赋) |
| IPv6资产管理与审计 | [支持对IPv6资产进行统一管理，同时可完整记录用户对IPv6资产的运维操作行为（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持管理IPv6资产) |
| 访问权限 | [★支持不同资产之间的联动配置，彼此之间可实现自动跳转访问（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持不同资产之间的联动配置，彼此之间可实现自动跳转访问) |
| [★支持动态权限管控，管理员可基于用户属性、设备属性、系统账号属性来创建弹性动态权限规则，只要满足相关属性的用户、设备、账号即会被自动赋予对应访问权限（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持动态权限管控，管理员可基于用户属性、设备属性、系统账号属性来创建弹) |
| [支持变更单管理功能，管理员可以基于使用人、资源、系统账号、到期时间，来上传、创建值班表模式的权限变更单，变更单无需审批，但可以自动生成时效性的访问权限（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持变更单管理功能，管理员可以基于使用人、资源、系统账号、到期时间，来) |
| [★支持基于A/B角管理模式的双人复核，当用户登录到目标设备时，必须经过复核人的复核确认后才能正常操作当会话复核人发现操作存在风险，可实时暂停（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持基于A/B角管理模式的双人复核，当用户登录到目标设备时，必须经过复) |
| 密码工单 | [支持密码工单管理，可通过工单申请相应资源的明文密码，审批通过后可通过邮件方式向申请人发送相应提示信息，有效期后平台会自动回收相应账号密码，并自动触发密码变更操作（提供截图证明）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持密码工单管理，可通过工单申请相应资源的明文密码，审批通过后可通过邮) |
| 审计能力 | [支持在IPV6环境下部署和管理，且支持在纯IPV4环境、纯IPV6环境及IPV4与IPV6混杂环境下对数据库进行审计（需提供产品配置界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_IPV6环境管理与审计_1) |
| [★支持VXLAN环境下数据库的审计，且需支持指定源IP审计功能（需提供产品配置界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_VXLAN环境审计) |
| [★支持因子监测功能，对数据库中突发增加的内容提供独立展示页面。因子内容包括：IP地址、应用程序名、计算机名、存储过程、数据库用户名、数据名、数据库主机。系统记录因子出现次数，且能排序，可多维快速定位因子（需提供产品配置界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_因子监测) |
| [★支持SQL模板，系统能自动识别并抽取数据库句式语意相同但参数不同的语句，并通过独立页面展示，同时记录该模板的状态、触发规则名、总记录数、总告警数、上次告警记录数、上次出现时间、最后出现时间，并能设置该模板别名，通过模板直接进行过滤操作（需提供产品配置界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_SQL模板) |
| [支持审计数据中敏感数据的模糊化处理，系统内置常见敏感数据的掩码规则（需提供产品配置界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_敏感数据掩码) |
| 结果查询 | [★支持对审计数据结果进行多条件组合查询，查询条件不少于27类。所支持的查询条件包括时间范围、源IP地址、操作方式、规则名、操作内容、排序方式、查询方式、排除内容、操作对象、计算机名、目标IP、应用程序名、数据库用户名、数据名、协议类型、会话流水号、语句流水号、长语句总耗时、长语句平均耗时、会话语句种类数、会话重复程度、最大单条耗时、会话语句数量、会话重复程度；支持对审计数据按关键词进行模糊查询，支持查询结果的二次过滤（需提供产品配置界面截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_查询方式) |
| 病毒、恶意代码、木马防护 | 支持内存病毒监控，可以自动清除或者删除病毒文件，并在隔离区中备份 |
| 支持查杀DOS、Windows等系统的ZIP、GZIP、ARJ、CAB、RAR、LZH、UPX、ASPACK、FSG、ZOO、ARC等多种压缩包裹格式的文件 |
| 支持移动设备自动监控，接入后提示病毒检测等 |
| 支持终端访问网络共享文件时的实时病毒检测 |
| 可以定时查杀，并且对病毒文件进行查毒或查毒 |
| [★支持文件、目录和数字签名自定义白名单的方式来管理全网终端的文件（需提供界面配置截图）](file:///D:\\Program%20Files%20(x86)\\Tencent\\WeChat\\WeChat%20Files\\niexin4125\\FileStorage\\File\\2021-10\\机关事务管理局参数(1).xlsx" \l "RANGE!_支持文件、目录和数字签名自定义白名单的方式来管理全网终端的文件) |
| 补丁分发与漏洞修复 | 可以定时修复漏洞功能，可以筛选高危补丁、可选补丁进行修复 |
| 产品资质要求 | 产品具备公安部《计算机信息系统安全专用产品销售许可证》,提供证书复印件证明 |
| 产品具备国家版权局颁发的《计算机软件著作权登记证书》,提供证书复印件证明 |

**网络安全要求**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| **服务要求** | |
| 物理安全 | ★投标人需要提供多种服务措施，保障机房的物理安全； |
| 网络安全 | ★投标人需要提供针对安全域内外的边界防护和访问控制服务； |
| ★投标人需要提供针对平台及网络的入侵检测和防御服务； |
| ★投标人需要提供针对平台的web安全防护服务和web漏洞扫描服务； |
| **产品要求（入侵防御）** | |
| 硬件架构 | 采用非X86多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块； |
| 存储 | 支持双硬盘，单块SSD硬盘不小于480G； |
| 接口要求 | 万兆光口不少于4个，千兆光口不少于4个，不少于4个千兆电口。配置4个万兆多模光模块。 |
| 性能要求 | 全威胁业务UDP吞吐不小于40G；并发连接数不小于500万，新建连接数不小于20万。 |
| 授权配置 | 配置3年IPS、AV升级授权License。 |
| 部署模式 | 同时支持串接部署的IPS模式以及旁路部署的IDS模式 |
| 防御能力 | 支持深入七层的分析检测技术，能检测防范的攻击类型包括：蠕虫/病毒、木马、后门、DoS/DDoS攻击、探测/扫描、间谍软件、网络钓鱼、利用漏洞的攻击、SQL注入攻击、缓冲区溢出攻击、协议异常、IDS/IPS逃逸攻击等 支持P2P、IM、视频等网络滥用协议的检测识别，支持的网络滥用协议至少包括迅雷、BT、eDonkey/eMule、Kugoo下载协议、多进程下载协议（网络快车、网络蚂蚁）等P2P应用， MSN、QQ、ICQ等IM应用， PPLive、PPStream、HTTP下载视频文件、沸点电视、QQLive等网络视频应用；可在识别的基础上对这些应用流量进行阻断或限流。 |
| 采用全面深入的分析检测技术，结合模式特征匹配、协议异常检测、流量异常检测、事件关联等多种技术，能识别运行在非标准端口上的协议，准确检测入侵行为。 |
| IPS检测到攻击报文或攻击流量后，支持阻断、限流、捕获原始报文等常规响应方式。 |
| IPS支持对不同的网段运用不同的入侵防御策略； |
| **产品要求（WAF）** | |
| 硬件要求 | 机架式硬件架构，8内存，1T硬盘，2个以太网千兆管理接口，支持至少4以太网千兆电口及4个以太网千兆光口. |
| 性能要求 | HTTP吞吐量不低于3Gbps，HTTP并发连接数不低于80万、HTTP每秒新建连接数不低于7万，保护网站站点数量无限制 |
| 部署方式 | 支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式； |
| 支持旁路镜像模式下，对检测到的攻击进行旁路阻断；（提供截图证明） |
| 网络适用性 | 支持通过BGP方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置SNAT策略；（提供截图证明） |
| 支持Trunk链路部署，自动识别VLAN，支持链路聚合，提升网络接口的性能，支持配置静态路由 |
| ★支持端口联动，一组业务接口中上下行接口同步UP/DOWN状态 |
| 系统管理 | 系统采用B/S设计架构，并采用SSL加密通信方式，通过浏览器方便对产品进行远程管理； |
| 产品界面友好，简洁大方，所有的图形界面、报警信息、报表与文档、技术资料要求均支持简体中文； |
| 支持系统配置的手工备份、自动备份（自动备份以日、周、月区分）； |
| Web安全防护 | 支持HTTP协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据；（提供截图证明） |
| 支持HTTPS防护，支持上传证书及密钥；应能识别和阻断注入攻击； |
| ★支持设置扫描陷阱，防止恶意扫描；（提供截图证明），支持爬虫防护；（提供截图证明），支持文件上传、下载过滤；（提供截图证明） |
| 支持LDAP、XPATH、struct2/xworks检测和防护；应能识别阻断跨站脚本(XSS)注入式攻击；应能识别阻断跨站请求伪造攻击； |
| 应能识别和防止敏感信息泄露；且可自定义敏感信息特征，如用户名、密码、邮箱、身份证信息、MD5密码等 |
| 支持敏感词防护并可自定义敏感词库；（例如：反动，色情类） |
| 支持页面访问顺序规则防护；（提供截图证明） |
| 支持虚拟补丁功能，支持导入appscan等第三方扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护； （提供截图证明） |
| 支持网站自学习建模，可通过学习URL、host等信息展示网站结构树形图，并支持对URL的访问量和响应健康度进行图形化统计； 支持通过自学习的URL参数的长度、类型、范围及请求方法等数据特点创建黑白名单模型，如果参数违反模型则判断为非法流量，直接执行阻断或封禁动作；（提供截图证明） |
| ★支持自定义防护模板，提供通用、增强、专家的初始防护策略模板； |
| 监控及报表 | ★支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标服务器、攻击类型、攻击趋势、流量趋势及实时事件的动画统计； |
| 态势监测支持对监测范围、防护区域和防护对象的自定义设置； |
| 系统须能够对遭受攻击按照攻击次数、防护的网站、遭受攻击的网页、攻击类型、攻击时间（或者发现攻击的时间）等进行统计并排名； |
| Web漏洞扫描 | 提供Web站点安全扫描功能； |
| 支持自定义Web安全扫描任务，定期进行Web安全扫描； |
| 产品管理及运维 | 支持HTTPS、SSH、Console、WebShell多种管理方式； |
| 支持Web管理端口自定义，保证产品访问的安全性； |

**机柜资源参数要求**

| **序号** | **指标项** | **指标要求** |
| --- | --- | --- |
| 1 | 机房总 体要求 | ★投标方提供的机房建设标准必须满足《信息安全等级保护管理办法》第三级安全保护标准，提供公安机关出具的证书文件。 |
| ★投标方提供的机房建设标准必须满足《通信行业数据中心基础设施认证技术规范》（YD/T5235-2019）A 级机房标准或国际T3标准，提供相关证明材料。 |
| 2 | 机房所在地应交通方便，周边 500 米范围内不得有下列危险：水灾、泥石流等灾害威胁、国家重点基础设施或重大军事目标、强腐蚀源、污染源、强电磁、有害气体、强震动源、容易发生群体事件场所、易燃易爆源； |
| 3 | 投标方提供服务的数据中心应具有极高的安全性、可用性设计，包括建筑结构、系统冗余能力、物理安全考虑、人员设备控制、消防安全考虑、应急能力、防电磁辐射、防雷、防水、防静电等； |
| 4 | 投标机房产权所有人应提供房屋所有权证明文件或由政府批复的土地使用确认证明，并提供相应的证明文件； |
| 5 | 机房定 制化要 求 | ★提供租赁机房区域要求为独立连续的空间内（须提供图纸）。  所在专有区域需安装视频监控录像装置，连续视频监控记录应保存至少90天，机房实行封闭式管理，并按照门禁系统，机房应设置防盗报警系统。应对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录应保存至少365天。 |
| 6 | 机柜要 求 | **★**提供同模块连续机柜（含电费），单机柜额定功率不低于4.5KW（如不满足，可根据功率核算，调整机柜数量），机柜须满足标准19英寸机架设备安装上架要求，机柜尺寸不小于600×1200×2000mm，可用空间不小于42U。（须提供图纸）。 |
| 7 | 机房综 合布线 要求 | 投标方须提供根据招标方需求在机柜所在机房区域内完成综合布线，线缆敷设在所在区域桥架机柜内，对强弱电进行分离，规范整齐。所在区域内的线缆按照招标方要求进行标签标识； |
| 8 | 缆线采用线槽或桥架敷设时，线槽或桥架的安装位置应与建筑装饰、电气、空调、消防等专业协调一致。应将通信线缆铺设在专用线槽内，强弱电缆需隔离铺设间隔不小于300mm，并进行统一标识； |
| 9 | 综合布线系统应选用有质量保证产品；综合布线系统应满足ANSI/TIA/EIA 568B、ANSI/TIA/EIA 569A、NSI/TIA/EIA-606、ANSI/TIA/EIA-607/《综合布线系统工程设计规范》GB50311-2016/《综合布线系统工程验收规范》GB50312-2016等标准要求； |
| 10 | 机房建 筑要求 | 机房所在建筑物须为机房专用的独栋建筑，建筑内不含有数据中心以外其他不相关业务用途；并根据信息系统机房应用的特点和特殊需要，在功能分区划分和平面布置、建筑结构上采取相应的技术措施； |
| 11 | **★**机房所在建筑物抗震等级为 8 级；建筑结构安全等级为 A 级；机房耐火等级不低于乙级； |
| 12 | 机房活荷载承重量不低于标准值 8-10（kN/㎡）； |
| 13 | 供配电 要求 | 机房采用双路市电供电，两路市电应该来自不同的供电站； |
| 14 | IT系统供电与空调等动力供电分开。 |
| 15 | 末端配电：每台机柜配置 A\B 双路 PDU（来自不同的 UPS 系统供电）； |
| 16 | 机房 UPS 及电池均应采用有质量保证的产品，并至少采用 3N 冗余方式。 |
| 17 | 满载情况下电池后备时间应不低于 15 分钟，招标人租赁机房区域内每个机柜要求由分别来源于两路 UPS 的两路电力供应（提供竣工验收资料）； |
| 18 | 柴油发电机配备 (N+X)冗余（X=1～N）后备柴油发电机系统（提供竣工验收资料）； |
| 19 | 投标方提供服务的数据中心内应设置有大容量油库，发电机燃油储备应能满足所有发电机组满载运行不低于 8 小时，并可不停机加油。此外，投标方应与附近油站签署有优先供油保障协议，可确保发电机燃油在 8 小时内获得补充。储油设施应符合国家相关标准规范要求（提供供油保障协议）； |
| 20 | 柴油发电机组应具有自动启动、自动切换、自动停机功能，应急电源与正常电源之间必须采取防止并列运行的措施。发电机组自启动到具备供电条件的时长原则上应小于 5 分钟； |
| 21 | 制冷要 求 | 机房精密空调应配备 N+X 冗余（X=1～N）机房专用空调（提供竣工验收资料）； |
| 22 | 保持机房温度（开机时）23℃±1℃ ，相对湿度（开机时）40%-60%，不结露。按冷、热通道分离布置。空调机房需独立，与IT机房物理隔离； |
| 23 | 防雷接 地要求 | 机房建筑设置有避雷装置，能够防范直击雷的危害； |
| 24 | 机房应设置交流电源地线，应设置通过国家认证的防雷装置，投标方须提供相关资质证明。防止感应雷，采用共用接地系统，在供电系统做好三级防雷措施。（提供专业检测机构出具的《机房防雷接地检测报告》）； |
| 25 | 消防要 求 | 机房区域的消防系统采用极早期火灾探测报警系统，火灾探测点应采取多层部署方式并应具有地址编码及电子地图，接入到火灾自动报警系统，提供集中式灭火报警系统； |
| 26 | 投标方提供服务的机房场地及配电室应设置感温、感烟双重报警系统。采用 IG541 或 FM200 环保洁净气体灭火系统。气体释放喷头应采取多路部署，分区灭火方式。无水管经过 IT 设备放置的机房区域； |
| 27 | 消防中控室应配置有 7×24 小时专职消防监控人员，实时监控火灾自动报警系统； |
| 28 | 机房内应设置有独立的消防排烟系统； |
| 29 | **★**投标方提供服务的数据中心的消防设施及管理应符合消防规范要求，并通过主管部门验收和年检，投标方应提供相关证明材料； |
| 30 | 多运营 商线路 接入 | 应满足全部基础运营商和运营商互联网、专线、裸光纤以及政务外网接入路由空间，满足招标人未来的网络接入； |
| 31 | 各运营商节点机房为独立空间，传输设备、管井等资源满足多条专线布设开通条件并具备后期扩展能力，传输设备应便于维护； |
| 32 | 承诺机房能够支持国家电子政务外网的接入，并提供相应的配合服务； |
| 33 | 机房运 维要求 | 机房所在建筑物入口处应安装出入控制和安全防护装置，并对出入人员和所带物品应进行安全检查； |
| 34 | 机房应配备 7×24 小时值班保安人员，负责机房的安全保卫工作； |
| 35 | 数据中心设有环境监控系统，并配备监控大屏，屏幕尺寸不低于20 m2，对机房相关基础设施运行状态和故障进行 7×24 小时监控； |
| 36 | 机房应配备 7×24 小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作；机房的基础设施日常巡检工作，每日巡检次数不少于六次； |
| 37 | 机房区域应为独立、封闭区域，并配置有门禁访问控制措施、视频监控、安全检查措施，并有 7×24 小时安保人员值班对进出机房的人员、设备进行检查、核实、放行。有多个出入口时，每个出入口都应有周全的人员、设备进出控制措施，以确保机房安全； |
| 38 | 应为招标人租赁区域出入口设置门禁控制系统，划分不同人员进出不同区域的权限。未经招标人授权的人员（包括投标方机房工作人员）不得进入；门禁控制系统应保存有完整的人员进出记录，人员进出记录要求至少保留一年； |
| 39 | 投标方须保证招标人及备案的项目组成员无条件（含封网期间）随时进入所租赁机房区域进行操作，并提供配合； |
| 40 | 应为招标人租赁机房区域部署高清视频监控系统，实现对所有通道、区域、设备的监控，且监控区域无死角。视频监控数据应至少保存 90 天且供招标人随时调阅查看； |
| 41 | 向招标人租赁机房区域提供包括供变配电、UPS、电池、空调及新风系统的设备系统监测服务、运行区温湿度及漏水监测、末端配电监测； |
| 42 | 在进行重大变更时，应提前至少 20 个工作日通过书面方式通知可能受到影响的招标人； |
| 43 | 应至少每季度一次向招标人提供服务报告，包括监控及巡检、日常维护、应急处理工作等； |
| 44 | 应提供数据中心保洁、卫生等日常工作，随时保持数据中整洁。 |

**链路资源参数要求**

|  |  |
| --- | --- |
| **指标内容** | **参数指标** |
| 带宽 | 端到端的数据传输速率不低于1G，预留电路扩容空间，保证后期电路带宽平滑升级 |
| 时延 | 端到端不丢包情况下的网络转发数据所用时间，包括传输时延和传输节点处理时延。跨省、跨市时延：0.8ms/百公里（单向时延）；本地网内≤10ms |
| 丢包率 | 在网络稳定状态下由于网络资源缺乏造成的不能转发的数据帧和总数据帧的百分比。从客户端PING至少1000个IP包，丢失的IP包与所有IP包的比值，在正常带宽负荷下（负荷小于70％）≤0.1%（挂表测试为准） |
| 可用率 | 挂表测试、网管监控，按单条电路使用情况计算：≥99.96% |
| 组网保障 | 提供的AAA级别的传输电路能够确保骨干层及局间网络两个层面的自愈保护及可监控，接入层做到物理双路由及自愈保护 |
| 性能监控 | 监控层面可以提供针对客户的365\*24\*7小时监控，确保传输设备性能、告警及业务性能如发生故障及性能下降时提前进行处理 |
| 设备巡检 | 提供应急演练及日常巡检，来随时确保业务的可用性 |
| 故障处理 | 如发生故障，在2小时内对业务进行抢通恢复（除不可抗力原因外） |
| 重点业务保障 | 提供故障的绿色通报申报途径，如遇到用户需重点保障及业务高峰期，可提供7\*24\*365小时的重点保障 |

**容灾备份服务要求：**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| **备份要求** | 投标人提供30T数据备份存储容量，包含配套的备份软硬件及一条100M链路。 |
| **选址要求** | 数据灾备机房应满足建设在距离生产中心300公里范围以外。  数据灾备机房建设标准必须满足《信息安全等级保护管理办法》第三级安全保护标准，提供公安机关出具的证书文件。  投标方提供的机房建设标准必须满足国家标准《数据中心设计规范》（GB 50174-2017）A级机房标准或国际T3标准，提供相关证明材料。 |
| **主控平台(Acesure/Boxsure)** | 灾备服务端主控平台，基于Web方式管理，对整个灾备平台软硬件资源统一管控，平台包含计算、存储节点功能；通过组合授权实现对物理机、虚拟机、云主机的操作系统、业务应用、数据等的整体实时容灾保护；可选择主机数实现业务应用的备份、仿真测试、容灾功能；支持Oracle RAC、微软双机的集群数据一致性保护；支持本/异地容灾复制功能，实现异地容灾；支持多个主控平台间级联。 |
| **备份容量授权** | 提供基于X86物理机、虚拟机、云主机的操作系统、业务应用、数据等的整体备份容量的授权使用；选择备份容量不限备份服务器数量。 |
| **集群支持模块** | Windows/Linux平台下Oracle RAC数据库的一致性保护；微软双机系统数据一致性保护；以主控平台为单位，平台内不限Oracle RAC、微软MSCS数量。 |
| **产品基础服务** | 1.软件升级服务：在服务年限内提供免费产品版本升级。 2.技术支持服务：提供技术咨询，产品使用培训，安装指导，容灾恢复演练。 3.产品基础服务提供支持形式包括：电话咨询，邮件等，提供7\*24小时支持响应； |
| **安装服务** | 根据交付场景需要提供远程或现场首次安装交付服务，提供交付方案，完成设备上架，客户端和管理平台安装，首次安装灾备配置和部署，完成首次灾备演练测试，完成交付报告。 |
| **现场专家服务** | 提供现场技术支持服务，24小时到达现场；现场专家服务根据需求提供：技术培训，故障排除，巡检，灾备演练，紧急救援等服务。 |
| **安全服务** | 提供基础风险评估服务、每年4次以上的漏洞扫描服务、每半年1次的安全基线检查服务、每年4次以上的Web扫描服务、每年1次的渗透测试服务、安全值守服务、安全应急响应服务、安全培训服务、技术支持服务、网络安全规划服务、网络安全标准建设服务、网络安全知识转移服务、安全加固指导服务、优化建议服务、网络整改及优化和信息安全体系构建服务。 |
| **数据备份** | 提供数据备份服务，数据定期备份至异地数据中心，包含60T可用备份空间，链路以及配套软硬件。 |

**容灾备份云服务器资源环境及能力要求：**

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **具体要求** | | |
| **资源要求** | CPU（核） | 内存（GB） | 存储空间（TB） |
| 160 | 320 | 100 |
| 投标人提供的云资源，招标人享有独立使用权，独立的网络，不接受公有云模式； | | |
| **基本要求** | 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等。 | | |
| 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。 | | |
| 提供统一的虚拟机管理界面，在同一界面上提供虚拟机启动、暂停、恢复、休眠、重启、安全关闭、关闭电源、克隆、迁移、备份、快照、克隆为模板、修改等生命周期管理功能。 | | |
| 支持虚拟机规格的在线和离线调整，包括CPU、内存、硬盘、网卡等资源，当虚拟机操作系统本身的前提下，热添加的CPU/内存可以即时生效。 | | |
| **资源管理能力** | 支持批量修改虚拟机的配置参数，包括：CPU调度优先级、CPU个数、内存大小、I/O优先级、启动优先级、是否自动迁移、tools自动升级等，提供产品截图证明。 | | |
| 支持集群动态资源调度功能，可基于主机的CPU、内存、网络流量、连接数、磁盘IO、存储容量等资源利用率对虚拟机进行动态资源调度，实现全自动化的资源分配和负载平衡功能，主动确保云环境的服务水平，提供产品截图证明。 | | |
| 支持配合负载均衡设备根据业务的负载情况实现业务系统虚拟机的动态扩展和回收，能够根据虚拟机CPU、内存、连接数、存储容量、磁盘IO等参数动态的克隆虚拟机或删除虚拟机，满足业务突发流量响应需求，实现资源的随需而动，提升资源利用率，节约投资，提供产品截图和至少3份用户使用证明。 | | |
| 支持当虚拟机的CPU、内存利用率超过设置的阈值时，在虚拟机操作系统本身支持资源热添加的前提下，系统将自动为该虚拟机增加相应的CPU和内存资源，无需人工干预。 | | |
| **数据安全** | 提供虚拟机快照功能，支持设置手工和定时快照将虚拟机磁盘文件和内存状态信息保存到镜像文件中。 | | |
| 提供虚拟机回收站功能，统一管理被删除的虚拟机，防止因虚拟机误删除导致数据丢失，支持设置回收站文件保存周期，超期的文件将被自动删除，支持批量销毁或还原虚拟机。 | | |
| 支持虚拟机迁移历史记录功能，记录中包含迁移的操作员、迁移方式、源主机、目的主机、开始时间、迁移耗时等信息，便于对虚拟机的迁移路径进行回溯。 | | |
| **运维能力** | 支持使用一键鼠标按钮分析虚拟机、主机历史资源使用情况，提供规划决策数据支撑。提供产品功能截图。 | | |
| 支持使用一键鼠标按钮分析后端存储上的无效镜像文件，并提供一键清理和释放存储空间能力，提升资源利用率，保障投资。要求提供CNAS认可的检测机构出具的检测报告检测结果及检测结果截图页并有制造商盖章作为证明材料，未提供视为不满足。 | | |
| 支持使用一键鼠标按钮快速查看、启动、删除、批量启动和批量删除长时间未使用且处于关闭状态的虚拟机，进行资源利用率统计，降低运维工作量与难度，保障投资。要求提供CNAS认可的检测机构出具的检测报告检测结果并有制造商盖章作为证明材料，未提供视为不满足。 | | |
| 支持一键切换大屏展示功能，直观展示虚拟化资源池的健康度、告警、资源使用情况等虚拟化环境，同时支持展示内容用户自定义，方便用户日常监控。 | | |
| **防病毒能力** | 支持虚拟化内核集成虚拟化安全防护功能模块为虚拟机提供防护，无需单独占用虚拟机资源安装安全防护功能模块，只需在虚拟化环境底层安装安全防护功能模块，不需要在每台虚拟机上安装，对每个虚拟机没有资源占用。 | | |
| 支持主流Windows和Linux操作系统无代理底层防病毒能力，不需要在虚拟服务器或虚拟桌面中部署安全防护代理。 | | |
| **杀毒授权** | 配置杀毒AV和DPI授权，能够实现虚拟主机无代理杀毒，配置不限主机数量授权。 | | |
| **迁移服务** | 投标人需要提供迁移服务，负责招标人现有业务系统虚拟机和数据迁移，需要保障业务和数据的完整性。 | | |
| **信息安全技术网络安全等级保护** | 投标人所提供的容灾备份云服务器资源需要满足《信息安全技术网络安全等级保护基本要求》第三级安全保护标准，等保测评得分需在85分以上并提供测评报告。 | | |
| **商用密码应用安全性评估** | 投标人所提供的容灾备份云服务器资源在通过《信息安全技术 网络安全等级保护基本要求》第三级安全保护标准评测后，需要通过商用密码应用安全性评估，密码测评得分需到70分及以上并提供测评报告。 | | |

**容灾备份云服务器资源硬件环境要求：**

| **指标项** | **指标要求** |
| --- | --- |
| **机房总 体要求** | ★投标方提供的机房建设标准必须满足《信息安全等级保护管理办法》第三级安全保护标准，提供公安机关出具的证书文件。 |
| ★投标方提供的机房建设标准必须满足国家标准《数据中心设计规范》（GB 50174-2017）A 级机房标准或国际T3标准，提供相关证明材料。 |
| 机房所在地应交通方便，周边 500 米范围内不得有下列危险：水灾、泥石流等灾害威胁、国家重点基础设施或重大军事目标、强腐蚀源、污染源、强电磁、有害气体、强震动源、容易发生群体事件场所、易燃易爆源； |
| 投标方提供服务的数据中心应具有极高的安全性、可用性设计，包括建筑结构、系统冗余能力、物理安全考虑、人员设备控制、消防安全考虑、应急能力、防电磁辐射、防雷、防水、防静电等； |
| 投标机房产权所有人应提供房屋所有权证明文件或由政府批复的土地使用确认证明，并提供相应的证明文件； |
| **机房定  制化要  求** | ★提供租赁机房区域要求为独立连续的空间内（须提供图纸）。  所在专有区域需安装视频监控录像装置，连续视频监控记录应保存至少90天，机房实行封闭式管理，并按照门禁系统，机房应设置防盗报警系统。应对机房所在区域出入人员身份执行审批审核流程，并记录出入人员信息、进出时间、工作内容等，相关记录应保存至少365天。 |
| **机柜要求** | 提供同模块连续机柜（含电费），单机柜额定功率不低于4.5KW（如不满足，可根据功率核算，调整机柜数量），机柜须满足标准19英寸机架设备安装上架要求，机柜尺寸不小于600×1200×2000mm，可用空间不小于42U。（须提供图纸）。 |
| **机房综  合布线  要求** | 投标方须提供根据招标方需求在机柜所在机房区域内完成综合布线，线缆敷设在所在区域桥架机柜内，对强弱电进行分离，规范整齐。所在区域内的线缆按照招标方要求进行标签标识； |
| 缆线采用线槽或桥架敷设时，线槽或桥架的安装位置应与建筑装饰、电气、空调、消防等专业协调一致。应将通信线缆铺设在专用线槽内，强弱电缆需隔离铺设间隔不小于300mm，并进行统一标识； |
| 综合布线系统应选用有质量保证产品；综合布线系统应满足ANSI/TIA/EIA 568B、ANSI/TIA/EIA 569A、NSI/TIA/EIA-606、ANSI/TIA/EIA-607/《综合布线系统工程设计规范》GB50311-2016/《综合布线系统工程验收规范》GB50312-2016等标准要求； |
| **机房建  筑要求** | 机房所在建筑物须为机房专用的独栋建筑，建筑内不含有数据中心以外其他不相关业务用途；并根据信息系统机房应用的特点和特殊需要，在功能分区划分和平面布置、建筑结构上采取相应的技术措施； |
| 机房所在建筑物抗震等级为 8 级；建筑结构安全等级为 A 级；机房耐火等级不低于乙级； |
| 机房活荷载承重量不低于标准值 8-10（kN/㎡）； |
| **供配电  要求** | 机房采用双路市电供电，两路市电应该来自不同的供电站； |
| IT系统供电与空调等动力供电分开。 |
| 末端配电：每台机柜配置 A\B 双路 PDU（来自不同的 UPS 系统供电）； |
| 机房 UPS 及电池均应采用有质量保证的产品，并至少采用 3N 冗余方式。 |
| 满载情况下电池后备时间应不低于 15 分钟，招标人租赁机房区域内每个机柜要求由分别来源于两路 UPS 的两路电力供应（提供竣工验收资料）； |
| 柴油发电机配备 (N+X)冗余（X=1～N）后备柴油发电机系统（提供竣工验收资料）； |
| 投标方提供服务的数据中心内应设置有大容量油库，发电机燃油储备应能满足所有发电机组满载运行不低于 8 小时，并可不停机加油。此外，投标方应与附近油站签署有优先供油保障协议，可确保发电机燃油在 8 小时内获得补充。储油设施应符合国家相关标准规范要求（提供供油保障协议）； |
| 柴油发电机组应具有自动启动、自动切换、自动停机功能，应急电源与正常电源之间必须采取防止并列运行的措施。发电机组自启动到具备供电条件的时长原则上应小于 5 分钟； |
| **制冷要求** | 机房精密空调应配备 N+X 冗余（X=1～N）机房专用空调（提供竣工验收资料）； |
| 保持机房温度（开机时）23℃±1℃ ，相对湿度（开机时）40%-60%，不结露。按冷、热通道分离布置。空调机房需独立，与IT机房物理隔离； |
| **防雷接  地要求** | 机房建筑设置有避雷装置，能够防范直击雷的危害； |
| 机房应设置交流电源地线，应设置通过国家认证的防雷装置，投标方须提供相关资质证明。防止感应雷，采用共用接地系统，在供电系统做好三级防雷措施。（提供专业检测机构出具的《机房防雷接地检测报告》）； |
| **消防要求** | 机房区域的消防系统采用极早期火灾探测报警系统，火灾探测点应采取多层部署方式并应具有地址编码及电子地图，接入到火灾自动报警系统，提供集中式灭火报警系统； |
| 投标方提供服务的机房场地及配电室应设置感温、感烟双重报警系统。采用 IG541 或 FM200 环保洁净气体灭火系统。气体释放喷头应采取多路部署，分区灭火方式。无水管经过 IT 设备放置的机房区域； |
| 消防中控室应配置有 7×24 小时专职消防监控人员，实时监控火灾自动报警系统； |
| 机房内应设置有独立的消防排烟系统； |
| 投标方提供服务的数据中心的消防设施及管理应符合消防规范要求，并通过主管部门验收和年检，投标方应提供相关证明材料； |
| **多运营  商线路  接入** | 应满足全部基础运营商和运营商互联网、专线、裸光纤以及政务外网接入路由空间，满足招标人未来的网络接入； |
| 各运营商节点机房为独立空间，传输设备、管井等资源满足多条专线布设开通条件并具备后期扩展能力，传输设备应便于维护； |
| 承诺机房能够支持国家电子政务外网的接入，并提供相应的配合服务； |
| **机房运  维要求** | 机房所在建筑物入口处应安装出入控制和安全防护装置，并对出入人员和所带物品应进行安全检查； |
| 机房应配备 7×24 小时值班保安人员，负责机房的安全保卫工作； |
| 数据中心设有环境监控系统，并配备监控大屏，屏幕尺寸不低于20 m2，对机房相关基础设施运行状态和故障进行 7×24 小时监控； |
| 机房应配备 7×24 小时值班基础设施管理员，负责机房的日常维护、事件应急、故障处置等工作；机房的基础设施日常巡检工作，每日巡检次数不少于六次； |
| 机房区域应为独立、封闭区域，并配置有门禁访问控制措施、视频监控、安全检查措施，并有 7×24 小时安保人员值班对进出机房的人员、设备进行检查、核实、放行。有多个出入口时，每个出入口都应有周全的人员、设备进出控制措施，以确保机房安全； |
| 应为招标人租赁区域出入口设置门禁控制系统，划分不同人员进出不同区域的权限。未经招标人授权的人员（包括投标方机房工作人员）不得进入；门禁控制系统应保存有完整的人员进出记录，人员进出记录要求至少保留一年； |
| 投标方须保证招标人及备案的项目组成员无条件（含封网期间）随时进入所租赁机房区域进行操作，并提供配合； |
| 应为招标人租赁机房区域部署高清视频监控系统，实现对所有通道、区域、设备的监控，且监控区域无死角。视频监控数据应至少保存 90 天且供招标人随时调阅查看； |
| 向招标人租赁机房区域提供包括供变配电、UPS、电池、空调及新风系统的设备系统监测服务、运行区温湿度及漏水监测、末端配电监测； |
| 在进行重大变更时，应提前至少 20 个工作日通过书面方式通知可能受到影响的招标人； |
| 应至少每季度一次向招标人提供服务报告，包括监控及巡检、日常维护、应急处理工作等； |
| 应提供数据中心保洁、卫生等日常工作，随时保持数据中整洁。 |

**容灾备份服务链路资源要求：**

|  |  |
| --- | --- |
| **指标内容** | **参数指标** |
| **带宽** | 端到端的数据传输带宽不低于100m，预留电路扩容空间，保证后期电路带宽平滑升级 |
| **时延** | 端到端不丢包情况下的网络转发数据所用时间，包括传输时延和传输节点处理时延。跨省、跨市时延：0.8ms/百公里（单向时延）；本地网内≤10ms |
| **丢包率** | 在网络稳定状态下由于网络资源缺乏造成的不能转发的数据帧和总数据帧的百分比。从客户端PING至少1000个IP包，丢失的IP包与所有IP包的比值，在正常带宽负荷下（负荷小于70％）≤0.1%（挂表测试为准） |
| **可用率** | 挂表测试、网管监控，按单条电路使用情况计算：≥99.96% |
| **组网保障** | 提供的AAA级别的传输电路能够确保骨干层及局间网络两个层面的自愈保护及可监控，接入层做到物理双路由及自愈保护 |
| **性能监控** | 监控层面可以提供针对客户的365\*24\*7小时监控，确保传输设备性能、告警及业务性能如发生故障及性能下降时提前进行处理 |
| **设备巡检** | 提供应急演练及日常巡检，来随时确保业务的可用性 |
| **故障处理** | 如发生故障，在2小时内对业务进行抢通恢复（除不可抗力原因外） |
| **重点业务保障** | 提供故障的绿色通报申报途径，如遇到用户需重点保障及业务高峰期，可提供7\*24\*365小时的重点保障 |