**郑州市中医院郑州市区域中医药信息系统升级项目**

**变更内容**

1. **第五章项目需求第二条建设规模中：**

**原文件：**

| **建设名称** | **规模数量** | **度量单位** |
| --- | --- | --- |
| **一、应用系统开发** |  |  |
| 智慧共享中药房 | 1 | 套 |
| 数据整合交换与数据集成服务系统 | 1 | 套 |
| 中医针灸数智服务平台 | 1 | 套 |
| 中医药诊疗服务质控系统 | 1 | 套 |
| 中医药业务智能监管驾驶舱 | 1 | 套 |
| 中西医结合数智类脑系统 | 1 | 套 |
| **二、成品软件** |  |  |
| 操作系统 | 55 | 套 |
| 数据库 | 25 | 套 |
| 中间件 | 30 | 套 |
| 项目管理系统 | 1 | 套 |
| 统一运维管理系统 | 1 | 套 |
| 统一门户 | 1 | 套 |
| **三、硬件设备** |  |  |
| **1.服务器** |  |  |
| 大数据服务器 | 18 | 台 |
| 应用服务器 | 15 | 台 |
| 边缘超融合节点 | 2 | 套 |
| 高性能存储节点 | 2 | 台 |
| 中心智算节点 | 4 | 台 |
| 边缘智算节点 | 6 | 台 |
| 备份一体机 | 2 | 台 |
| 云平台管理软件 | 1 | 套 |
| **2.网络设备** |  |  |
| 互联网核心交换机 | 2 | 台 |
| 互联网接入交换机 | 2 | 台 |
| 核心交换机 | 2 | 台 |
| 接入交换机 | 2 | 台 |
| 存储互联交换机 | 1 | 台 |
| 超融合接入交换机 | 2 | 台 |
| 高速互联交换机 | 2 | 台 |
| 管理交换机 | 2 | 台 |
| 应用负载均衡器 | 1 | 台 |
| **3.安全设备** | 1 |  |
| 万兆防火墙（专网区） | 2 | 台 |
| 万兆防火墙（互联网区） | 1 | 台 |
| 千兆防火墙 | 1 | 台 |
| WEB应用防火墙 | 2 | 台 |
| 漏洞扫描 | 1 | 台 |
| 入侵防御（专网区） | 1 | 台 |
| 入侵防御（互联网区） | 1 | 台 |
| 网络安全审计 | 1 | 台 |
| 堡垒机（互联网） | 1 | 台 |
| 堡垒机（专网区） | 2 | 台 |
| 数据库审计 | 2 | 台 |
| 服务密码机 | 2 | 台 |
| 签名验签服务器 | 2 | 台 |
| 安全隔离与信息交换系统 | 2 | 台 |
| 态势感知平台 | 2 | 套 |
| 态势感知探针 | 1 | 套 |
| 杀毒软件 | 2 | 台 |
| 日志审计（互联网区） | 2 | 台 |
| 日志审计（专网区） | 2 | 台 |
| 抗DDOS攻击设备 | 1 | 台 |
| 互联网VPN接入设备 | 2 | 台 |
| **4.机房设备** |  |  |
| 微模块机柜 | 15 | 台 |
| 列头机柜 | 1 | 台 |
| 智慧机柜侧板 | 2 | 套 |
| 机柜锁具 | 16 | 套 |
| 智慧机柜M型走线槽 | 20 | 套 |
| 快开盲板 | 150 | 个 |
| 水平理线器 | 15 | 条 |
| 智慧机柜轻载托盘 | 15 | 块 |
| L型托架 | 15 | 对 |
| 智慧机柜专用普通PDU | 30 | 个 |
| 列间空调 | 4 | 套 |
| 盲柜 | 4 | 套 |
| 机柜监控主机 | 1 | 台 |
| 微动环监控平台系统软件 | 1 | 套 |
| 电话,短信告警模块 | 1 | 个 |
| 手机APP客户端接入接口 | 1 | 套 |
| 温湿度传感器 | 4 | 个 |
| 烟雾探测器 | 4 | 个 |
| 声光报警器 | 1 | 个 |
| 水浸探测绳 | 4 | 根 |
| 智慧模块化通道电源控制箱 | 1 | 套 |
| 机房强弱电设备安装及配套辅材 | 1 | 套 |
| **5.其他设备** |  |  |
| 指挥中心大屏 | ≥20 | m² |
| 可视化综合管控一体机 | 1 | 台 |
| 拼接屏处理器 | 1 | 个 |

变更为：

| **建设名称** | **规模数量** | **度量单位** |
| --- | --- | --- |
| **一、应用系统开发** |  |  |
| 智慧共享中药房 | 1 | 套 |
| 数据整合交换与数据集成服务系统 | 1 | 套 |
| 中医针灸数智服务系统 | 1 | 套 |
| 中医诊疗服务质控系统 | 1 | 套 |
| 中医药业务智能监管驾驶舱 | 1 | 套 |
| 中西医结合数智类脑系统 | 1 | 套 |
| **二、成品软件** |  |  |
| 操作系统 | 55 | 套 |
| 数据库 | 25 | 套 |
| 中间件 | 30 | 套 |
| 项目管理系统 | 1 | 套 |
| 统一运维管理系统 | 1 | 套 |
| 统一门户 | 1 | 套 |
| **三、硬件设备** |  |  |
| **1.服务器** |  |  |
| 大数据服务器 | 18 | 台 |
| 应用服务器 | 15 | 台 |
| 边缘超融合节点 | 2 | 套 |
| 高性能存储节点 | 2 | 台 |
| 中心智算节点 | 4 | 台 |
| 边缘智算节点 | 6 | 台 |
| 备份一体机 | 2 | 台 |
| 云平台 | 1 | 套 |
| **2.网络设备** |  |  |
| 互联网核心交换机 | 2 | 台 |
| 互联网接入交换机 | 2 | 台 |
| 核心交换机 | 2 | 台 |
| 接入交换机 | 10 | 台 |
| 存储互联交换机 | 2 | 台 |
| 超融合接入交换机 | 4 | 台 |
| 高速互联交换机 | 1 | 台 |
| 管理交换机 | 4 | 台 |
| 应用负载均衡器 | 4 | 台 |
| **3.安全设备** |  |  |
| 万兆防火墙（专网区） | 2 | 台 |
| 万兆防火墙（互联网区） | 2 | 台 |
| 千兆防火墙 | 2 | 台 |
| WEB应用防火墙 | 2 | 台 |
| 漏洞扫描 | 1 | 台 |
| 入侵防御（专网区） | 2 | 台 |
| 入侵防御（互联网区） | 2 | 台 |
| 网络安全审计 | 2 | 台 |
| 堡垒机（互联网） | 1 | 台 |
| 堡垒机（专网区） | 1 | 台 |
| 数据库审计 | 2 | 台 |
| 服务密码机 | 1 | 台 |
| 签名验签服务器 | 1 | 台 |
| 安全隔离与信息交换系统 | 2 | 台 |
| 态势感知平台 | 1 | 台 |
| 态势感知探针 | 1 | 套 |
| 杀毒软件 | 1 | 套 |
| 日志审计（互联网区） | 1 | 台 |
| 日志审计（专网区） | 1 | 台 |
| 抗DDOS攻击设备 | 2 | 台 |
| 互联网VPN接入设备 | 2 | 台 |
| **4.机房设备** |  |  |
| 微模块机柜 | 15 | 台 |
| 列头机柜 | 1 | 台 |
| 智慧机柜侧板 | 2 | 套 |
| 机柜锁具 | 16 | 套 |
| 智慧机柜M型走线槽 | 20 | 套 |
| 快开盲板 | 150 | 个 |
| 水平理线器 | 15 | 条 |
| 智慧机柜轻载托盘 | 15 | 块 |
| L型托架 | 15 | 对 |
| 智慧机柜专用普通PDU | 30 | 个 |
| 列间空调 | 4 | 套 |
| 盲柜 | 4 | 套 |
| 机柜监控主机 | 1 | 台 |
| 微动环监控平台系统软件 | 1 | 套 |
| 电话,短信告警模块 | 1 | 个 |
| 手机APP客户端接入接口 | 1 | 套 |
| 温湿度传感器 | 4 | 个 |
| 烟雾探测器 | 4 | 个 |
| 声光报警器 | 1 | 个 |
| 水浸探测绳 | 4 | 根 |
| 智慧模块化通道电源控制箱 | 1 | 套 |
| 机房强弱电设备安装及配套辅材 | 1 | 套 |
| **5.其他设备** |  |  |
| 指挥中心大屏 | ≥20 | m² |
| 可视化综合管控一体机 | 1 | 台 |
| 拼接屏处理器 | 1 | 个 |

1. **招标文件第五章项目需求5、建设需求中：**

**原文件：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **一** | **服务器** |  |  |  |
| 1 | 大数据服务器 | 1、规格：≥12个3.5英寸硬盘盘位； 2、CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，支持超线程； 3、内存：配置≥16\*32GB DDR5 内存条； 4、系统盘：配置≥2\*960GB SSD； 5、数据盘：配置≥6\*4TB SATA； 6、缓存盘：配置≥2\*3.2TB NVMe SSD； 7、网口：配置≥4个GE，≥2个10GE光口（含光模块），≥2个25GE光口（含光模块）； 8、RAID卡：配置独立RAID卡； 9、配置冗余电源，冗余风扇； 10、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 18 |
| 2 | 应用服务器 | 1、规格：≥12个3.5英寸硬盘盘位； 2、CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，支持超线程； 3、内存：配置≥16\*32GB DDR5内存条； 4、系统盘：配置≥2\*960GB SSD； 5、网口：配置≥4个GE，≥2个10GE光口（含光模块），≥2个25GE光口（含光模块）； 6、RAID卡：配置独立RAID卡； 7、配置冗余电源，冗余风扇； 8、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 15 |
| 3 | 边缘超融合节点 | 1、通过服务器节点构建，同一节点内实现计算存储融合，可配置副本（2副本或3副本）或EC（纠删码），可满足不同可靠性要求的业务场景。 2、支持图形化界面划分存储资源池，每个存储资源池即为一个故障域，保证可靠性。 3、配置超融合管理授权及分布式存储授权，共配置≥3个节点，单节点配置如下： 1）规格：≥12个3.5英寸硬盘盘位； 2）CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，或支持超线程； 3）内存：配置≥16\*32GB DDR4 内存条或DDR5内存条； 4）系统盘：配置≥2\*960GB SAS SSD； 5）数据盘：配置≥5\*4TB SATA； 6）缓存盘：配置≥1\*3.2TB NVMe SSD； 7）网口：配置≥4个GE，≥4个10GE光口（含光模块）； 8）RAID卡：配置独立RAID卡； 9）配置冗余电源，冗余风扇； 10）为保证项目正常交付，须提供服务器厂家的质保函； | 套 | 2 |
| 4 | 高性能存储节点 | 1、控制器规格：≤5U机架式双控制器存储； 2、缓存：≥768GB缓存，交流电源； 3、处理器：国产化处理器，总核数≥128核； 4、端口：≥4\*100Gb RDMA； 5、端口：≥2\*4端口25Gb ETH(含模块)； 6、端口：≥2\*4端口 1Gb ETH ； 7、硬盘：配置≥16块7.68 TB NVMe SSD ，≥77块16TB 7.2K RPM NL SAS，RAID6后可得容量不低于1PB； 8、线缆：配置≥8根多模光跳线； 9、线缆：配置≥4\*高速电缆-48G Mini SAS -3m； 9、配置SAN许可(含存储管理软件,瘦分配,数据迁移,快照,远程复制,克隆,服务质量管理,智能运维软件,主机多路径,异构虚拟化,双活,CDP)； 10、配置NAS许可(含CIFS,NFS,NDMP,瘦分配,快照,远程复制,克隆,服务质量管理,双活,CDP,智能运维软件,NAS备份)； 11、存储系统为对称AA架构，LUN无控制器归属，在多控配置下，能够负载到所有控制器，CPU利用率差异小于5%，提供CNAS检测证明，并加盖厂商公章。 | 台 | 2 |
| 5 | 中心智算节点 | 1、单节点国产化AI算力：≥2.2 PFLOPS FP16，单节点≥512GB HBM高带宽显存。单个AI处理器/加速卡支持≥280TFLOPS@FP16算力，单卡≥64GB HBM高带宽内存。 2、单节点CPU：≥4颗国产化处理器，单颗物理核心数≥48，主频≥2.6GHz。 3、单节点内存：容量 ≥512G DDR4，内存频率≥3200MHZ。 4、单节点硬盘：≥2\*960GB SSD，≥2\*3.2TB SSD；。 5、单节点网络：≥2个10GE光口（含光模块），≥4\*25Gbps端口(含光模块)，≥8\*200G光口（含光模块）。 6、根据网络信息安全要求，主板管理控制器为国产管理芯片，该芯片能提供基于Web的远程管理控制、配备硬件监控、远程管理功能，支持IPMI2.0标准，提供IKVM功能，实现远程KVM功能。 7、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 4 |
| 6 | 边缘智算节点 | 1、规格：≥12个3.5英寸硬盘盘位； 2、CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，或支持超线程； 3、内存：配置≥8\*32GB DDR4 内存条； 4、系统盘：配置≥2\*960GB SAS SSD； 5、网口：配置≥4个GE，≥4个10GE光口（含光模块）； 6、RAID卡：配置独立RAID卡； 7、加速卡：≥4\*AI加速卡；单卡≥140T FP16、≥96GB； 8、配置冗余电源，冗余风扇； 9、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 6 |
| 7 | 备份一体机 | 1、支持对Oracle、MySQL、SQL Server、GaussDB OLTP、OpenGauss、Postgre SQL、达梦、KingBase、DB2、SAP HANA、GoldenDB、HCS GaussDB数据库进行在线备份保护。 2、支持Oracle、MySQL数据库的永久增量备份功能，合成副本支持数据重复删除、备份副本异地复制、备份副本长期保留到对象和带库功能，支持备份副本即时挂载和恢复。 3、支持HDFS、HBase、Hive、ElasticSearch、Redis、ClickHouse等大数据组件的数据备份功能。备份任务配置过程全部图形化操作，无需编写脚本，且支持HDFS单文件、HDFS目录、HBase单表、HBase NameSpace级、Hive表级、ElasticSearch索引级、ClickHouse表级细粒度备份和恢复能力。 4、提供按备份任务细粒度复制，支持设置立即复制和周期性复制，支持设置复制副本保留时长（支持永久保留、按年/月/周/天保留）； 5、双控,SSD&HDD,≥256GB 缓存,采用国产化处理器，主频≥2.6GHz，总核心数≥40core；实配≥4\*960GB SSD SAS硬盘；≥8\*8TB 7.2K RPM NL SAS硬盘；配置≥32T备份许可；提供≥8个GE，≥4个10GE光口（含光模块）； | 台 | 2 |
| 8 | 云平台 | 1、平台云软件支持对存储、交换机、服务器、超融合、虚拟化资源的统一管理，无需多个软件界面分散管理，管理能力包括设备基本信息查询、配置信息查询、历史性能信息、资源利用率查询、设备告警信息查询等； 2、支持在同一界面配置交换机设置，块存储、文件存储快速发放，实现虚拟机端到端的发放。 3、提供了虚拟机视角的IO路径全链路故障诊断：一个界面展示虚拟盘、虚拟机、主机、交换机、存储设备的IO路径级的拓扑信息。 4、基于应用视角，提供了包含虚拟机、主机、LUN、存储等对象实例的多维度的关联对象分析，快速定界定位问题。 5、支持通过设置快照策略任务对虚拟机进行定时快照，满足日常运维管理诉求。运维人员可设置不同的虚拟机快照策略，可按天、周、月设置执行计划。 6、提供预见式运维，支持管理员可自定义检查条件，对存储、计算、网络的配置、容量、性能、可用性、低负载、可回收资源进行检查，在匹配到违规条件时，产生事件，帮助管理员实现风险提前识别与闭环。 7、支持用户针对指定的虚拟机配置检查策略，达到策略定义的阈值后自动扩容虚拟机的CPU或者内存。过程中虚拟机正常运行不需要重启。 8、支持批量对多个虚拟机的CPU、内存、磁盘硬件参数做变更配置，提升运维效率。 9、支持大屏展示，预置超过3种大屏；预置超过20种图表控件，可支持用户自定义大屏内容。 10、支持租户管理，提供资源配额管理。 11、支持报表统计，支持周期性自动生成报表，预置容量、资源性能，告警等30多种典型业务场景的报表。支持用户自定义报表统计内容。 12、配置≥42颗CPU计算虚拟化高级版/企业版授权、≥1800核容器授权及≥110颗CPU云平台授权； | 套 | 1 |
|  |  |
| **二** | **网络设备** |  |  |  |
| 1 | 互联网核心交换机 | 1.交换容量≥170Tbps，包转发率≥128000Mpps； 2.主控槽位≥2个；整机业务板槽位数≥8个，主控槽位与业务线卡槽位宽度相同，为全宽槽位，电源槽位≥4个； 3.要求设备采用国产化CPU芯片和转发芯片； 4.支持VxLAN 分布式网关、集中式网关，BGP-EVPN，通过 Netconf配置VxLAN； 5.支持整机MAC地址≥380K；MAC学习速率≥16000/s;整机ARP表项≥140000，整机ND表项≥80000，IPv4 路由表以及 FIB表≥256000， IPv6 路由表以及 FIB表≥80000； 6.支持 Telemetry 技术，实时采集设备数据并上送至网络分析组件平台，通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，及时定界故障以及故障发生原因，精准保障用户体验； 7.配置要求: 双主控引擎，≥2个独立风扇框，≥2个交流电源，≥2个100G光口，≥24个万兆光口，≥32个千兆光口，≥48个千兆电口，≥24个万兆多模模块，≥1根5米万兆集群线缆。为满足后期扩容需求，满足上述配置后空余业务槽位≥4个； | 台 | 2 |
| 2 | 互联网接入交换机 | 1.交换容量≥2.5Tbps，转发性能≥1500Mpps； 2.万兆光接口≥24个，100G光接口≥2个，交流电源≥2个，≥24个万兆多模模块，40G堆叠线缆≥1根； 3.支持VXLAN分布式网关，集中式网关，支持BGP-EVPN，支持VXLAN 路由交换； 4.支持RIP、RIPng、OSPF、OSPFV3、ISIS、ISISV6、BGP、BGP4+； 5.设备关键芯片(CPU、转发芯片)均为国产化芯片； 6.MAC 地址表容量≥128K， ARP 地址容量≥64K， FIBv4 表容量≥128K， FIBv6 表容量≥64K； 7.为了方便后期维护，要求设备支持外置复位按钮，可在忘记密码或清空配置时使用，使设备快速恢复出厂配置； | 台 | 2 |
| 3 | 核心交换机 | 1.交换容量≥800Tbps，包转发率≥230000Mpps； 2.整机主控槽位≥2个，业务槽位数≥4个，交换网板与业务槽位垂直正交CLOS架构； 3.设备关键芯片(CPU、转发芯片)均为国产化芯片； 4.支持Vxlan协议，且支持BGP EVPN协议； 5.MAC地址表容量≥250K，ARP地址容量≥250K，FIBv4表容量≥250K，FIBv6表容量≥80K； 6.配置要求：冗余主控，交换网板≥6个，电源≥2个，40G光接口≥36个，10G光接口≥48个，万兆多模模块≥48个，5米40G高速线缆≥2根； | 台 | 2 |
| 4 | 接入交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.固定接口交换机，独立风扇模块≥3个，电源槽位≥2个； 3.设备CPU芯片和转发芯片均采用国产自研芯片； 4.支持配置回滚，在系统运行过程中发现配置错误、业务运行不正常，可以通过该命令将系统回退到指定的历史配置状态； 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维ID指示灯，现场定位用指示灯，运维人员可远程控制ID灯开启和关闭； 6.配置：10GE光接口≥48个，100GE光接口≥8个 ，万兆多模模块≥48个，40G多模模块≥4个，配置冗余电源； | 台 | 10 |
| 5 | 存储互联交换机 | 1.交换容量≥8Tbps，包转发率≥2300Mpps； 2.固定接口交换机，独立风扇模块≥5个，电源槽位≥2个； 3.支持智能无损网络特性，支持PFC死锁预防，支持识别流量模型动态调节ECN门限功能即AI ECN功能； 4.设备CPU芯片和转发芯片均采用国产自研芯片； 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维ID指示灯，现场定位用指示灯，运维人员可远程控制ID灯开启和关闭； 6.配置：25GE光接口≥48个（不可通过接口拆分提供），100 GE光接口≥8个，≥48个25G多模模块，≥4个40G多模模块，配置冗余电源； | 台 | 2 |
| 6 | 超融合接入交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.固定接口交换机，独立风扇模块≥3个，电源槽位≥2个； 3.设备CPU芯片和转发芯片均采用国产自研芯片； 4.支持配置回滚，在系统运行过程中发现配置错误、业务运行不正常，可以通过该命令将系统回退到指定的历史配置状态； 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维ID指示灯，现场定位用指示灯，运维人员可远程控制ID灯开启和关闭； 6.配置：10GE光接口≥48个，100GE光接口≥8个 ，万兆多模模块≥48个，40G多模模块≥4个，配置冗余电源； | 台 | 4 |
| 7 | 高速互联交换机 | 1.交换容量≥25.6Tbps ，包转发率≥8000Mpps； 2.固定接口交换机，电源模块槽位≥2个，支持电源1+1备份，风扇模块槽位≥6个； 3.400GE QSFP-DD光接口≥32个，10GE SFP+光接口≥2个，配置≥24个400G光模块以及配套400G一分二线缆； 4.设备CPU芯片、转发芯片均为国产自研芯片，满足自主可控； 5.支持AI ECN，可以根据现网流量模型智能调整无损队列的ECN门限，可以保障零丢包下的低时延和高吞吐，让无损业务达到最优性能； 6.支持M-LAG或vPC或DRNI等跨机箱链路捆绑技术； 7.支持RDMA,RoCEv2,可提供“无丢包、低时延、高吞吐”的网络环境； 8.支持Vxlan，且支持 EVPN VxLAN，支持VxLAN网络与VLAN网络互通； | 台 | 1 |
| 8 | 管理交换机 | 1.交换容量≥660Gbps，包转发率≥200Mpps； 2.固定接口交换机，电源槽位≥2个； 3.设备支持复位按钮，忘记密码可以通过按钮恢复出厂设置； 4.设备CPU芯片和转发芯片均采用国产自研芯片； 5.支持配置回滚不重启，在系统运行过程中发现配置错误、业务运行不正常，可以通过该命令将系统回退到指定的历史配置状态； 6.设备支持ID指示灯，便于快速定位设备位置； 7.配置：千兆电接口≥48个，10GE光接口≥4个，支持≥2个专用堆叠口，≥4个万兆多模模块，配置冗余电源； | 台 | 4 |
| 9 | 应用负载均衡器 | 1、千兆电口≥8个，万兆光口≥8个，万兆多模光模块≥4个，冗余电源,含国密和商密芯片加速卡；采用国产化CPU和操作系统； 2、吞吐量≥40G；并发连接数大于等于2500万，新建连接数≥20万；支持多存储介质，可同时支持EMMC卡≥4GB，SSD硬盘≥512GB； 3、支持TCP、HTTP、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、SIP、RADIUS、自定义等健康监测方式；支持源IP、目的IP、SIP、HASH、http cookie、http header、URL、Radius、DHCP、SSL ID、自定义等多种会话保持方式； 4、单一设备可同时支持包括链路负载均衡、服务器负载均衡、全局负载均衡的功能；（需提供设备功能界面截图证明) 5、支持TCP、HTTP、HTTPS、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、SIP、RADIUS、自定义健康监测脚本等健康监测方式； 6、支持轮询、加权轮询、最小流量、最小连接、加权最小连接、加权最佳性能、每源IP轮询、源地址源端口哈希散列等服务器负载均衡调度算法； 7、支持主备真实服务组功能，在缺省实服务组内的成员均不可用时，启用备份实服务组对外提供服务，无需单独配置真实服务的优先级； 8、支持手动方式的双机配置一致性检查功能，在日常运维中，可以通过手动的方式检查双机之间的配置是否保持一致，并且显示上次检查时间以及检查结果是否为一致，在不一致的情况下，可以详细展示出双机在地址池、NAT、真实服务、真实服务组、虚拟服务、健康检查、会话保持、HTTP内容调度、SSL策略等模块的配置差异化对比；（提供设备功能界面截图并加盖原厂商公章） 9、支持一键跳转至命令行CLI功能，支持通过设备WEBUI页面，一键跳转至命令行CLI界面，无需通过远程管理工具登录命令行CLI界面； | 台 | 4 |
| **三** | **安全设备** |  |  |  |
| 1 | 万兆防火墙（专网区） | 1、机框式插卡设备，主控≥2，支持N+1冗余备份，业务槽位数≥3，具有良好的扩展性；支持扩容业务功能板卡数量，实现整机业务性能叠加，满配整机业务吞吐量≥1080Gbps，最大并发连接数≥2亿，每秒新建连接数≥1440万，支持扩展万兆接口≥96个，100G接口≥8或40G接口≥16； 2、本次实配国产化主控，电源模块≥2块，主控≥2，风扇模块≥2个，千兆电口≥4个，万兆光口接口≥16个，万兆多模光模块≥16个，业务吞吐量≥80Gbps； 3、支持丰富的VPN特性，如 IPSec VPN、SSL VPN、L2TP VPN、MPLS VPN、GRE等；支持国用商用密码对数据进行加密。 4、支持L2～L7的全面安全防御，包括防火墙、NAT、LB、IPS、AV、ACG、VPN等； 5、支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护；支持SYN Flood、ICMP Flood、UDP Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； 6、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作； 7、支持主机和业务模块统一IP管理和统一的配置界面，支持统一网管功能，支持紧耦合部署； 8、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙； 9、支持同一块板卡、跨板卡的链路聚合，支持多台物理设备完成虚拟化之后，不同物理设备的物理端口进行聚合； 10、支持自动生成安全策略，统一运维管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率（提供和统一管理平台的对接的承诺函）； 11、支持 802、1Qbg、DCB 等；支持 VXLAN 等 Overlay 主流标准技术；支持 Openflow1、3 协议标准；具备SDN 及专网区特性； 12、支持设备在线状态监测机制，实现对包括主控引擎，背板，芯片和存储等关键元器件进行检测； | 台 | 2 |
| 2 | 万兆防火墙（互联网区） | 1、具备千兆电口≥8个，千兆光口≥2个，万兆光口≥4个，千兆多模光模块≥2个，万兆多模光模块≥4个，支持扩展槽≥1个，冗余交流电源； 2、整机吞吐量≥10Gbps，每秒新建连接数≥23万，最大并发连接数≥500万，含5年病毒、IPS、应用识别、URL特征库及升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持一体化安全策略配置，可以通过一条策略实现五元组、应用、服务、时间、长连接、IP限速、IPS、AV、URL过滤、行为审计等功能配置,简化用户管理； 5、具备防火墙、应用识别、链路负载均衡、IPV6、VPN等功能，支持扩展URL过滤、IPS、AV、IP信誉库、区域特征库、威胁情报等功能； 6、支持IPv4／IPv6 NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT66地址转换；支持多种应用协议，如FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT的NAT ALG功能； 7、支持通过命令查询数据流在设备上的处理流程，可以看到报文经过设备的处理流程，包含不限于入接口、会话创建、NAT匹配结果、路由查询结果、安全策略匹配、出接口等以及数据包在设备中最终的处理结果等信息，便于进行故障排查； 8、支持在一台物理设备上划分出≥30个并发相互独立的虚拟系统，并可以查看虚拟系统的CPU和内存利用率、新建、并发和吞吐等信息，并支持单独重启一个虚拟系统，其他虚拟系统以及公共系统的业务不受影响。； | 台 | 2 |
| 3 | 千兆防火墙 | 1、具备千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个，支持扩展槽≥2个，冗余交流电源； 2、整机吞吐量≥4Gbps，每秒新建连接数≥9万，最大并发连接数≥390万，含5年病毒、IPS、应用识别、URL特征库及升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持一体化安全策略配置，可以通过一条策略实现五元组、应用、服务、时间、长连接、IP限速、IPS、AV、URL过滤、行为审计等功能配置,简化用户管理； 5、具备防火墙、应用识别、链路负载均衡、IPV6、VPN等功能，支持扩展URL过滤、IPS、AV、IP信誉库、区域特征库、威胁情报等功能； 6、支持IPv4／IPv6 NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT66地址转换；支持多种应用协议，如FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT的NAT ALG功能； 7、支持通过命令查询数据流在设备上的处理流程，可以看到报文经过设备的处理流程，包含不限于入接口、会话创建、NAT匹配结果、路由查询结果、安全策略匹配、出接口等以及数据包在设备中最终的处理结果等信息，便于进行故障排查； 8、支持在一台物理设备上划分出≥30个并发相互独立的虚拟系统，并可以查看虚拟系统的CPU和内存利用率、新建、并发和吞吐等信息，并支持单独重启一个虚拟系统，其他虚拟系统以及公共系统的业务不受影响； | 台 | 2 |
| 4 | WEB应用防火墙 | 1、具备千兆电口≥8个，千兆光口≥2个，千兆多模光模块≥2个，支持扩展槽≥2个，冗余交流电源； 2、整机吞吐≥9Gbps，HTTP吞吐≥1Gbps，最大并发连接数≥300万，每秒新建连接数≥3万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持透明模式、代理模式、网关模式和旁路模式，且模式之间切换不需要重启设备或者检测引擎，可多种模式共同运营；  5、支持对Web流量的镜像阻断功能，并且支持指定阻断报文发送接口； 6、支持通过虚拟化技术实现将一台物理设备虚拟成≥30个并发虚拟WAF；并且可对每个虚拟WAF使用的资源进行限制，例如会话数、新建速率、吞吐量、CPU及内存使用率； 7、支持流量自学习，可以自动学习IP、域名、端口等信息，将学习到的服务添加到防护策略；  8、支持内置规则弱口令防护功能，支持自定义表单模式对弱口令登录表单进行识别和校验； 9、支持通过设定前置参数名、正则表达式、参数范围等匹配特定的主机名、URL，对容易被篡改或者篡改会产生重大风险的参数名的取值进行限定； | 台 | 2 |
| 5 | 漏洞扫描 | 1、 配置千兆电口≥8个，万兆光口≥2个，万兆多模光模块≥2个，USB接口≥2个，冗余交流电源； 2、 采用国产化CPU和操作系统，内存≥16GB，硬盘存储≥1T； 3、采取旁路部署模式，支持分级部署与集中管理，IP可达即可进行检测，无需改变网络架构，基于WEB进行管理； 4、支持资产盘点，可下发资产盘点任务导出专用资产盘点报告，支持自定义资产指纹； 5、支持漏洞检测及弱口令的识别能力，支持高危漏洞的专项检测，支持对高危漏洞的自动化验证，可生成专业安全检测报告； 6、产品具备边界完整性检测能力，可检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为； 7、产品具备违规内联检测能力，可检测出随身WI-FI、BYOD设备、向日葵； 8、产品具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测； 9、支持配置主机漏洞模板，内置漏洞库数量≥300000种，可兼容CVE、CNNVD、CNVD等主流标准，同时支持自定义扫描漏洞库，漏洞库类型可基于操作系统、数据库、中间件等进行分类； 10、产品需集成安全漏洞验证知识库（提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库）以及手工漏洞验证工具集； 11、产品具备高危预警能力，能够对最新发布的高危漏洞及时更新推送平台，对最新高危漏洞预警进行立即检测； 12、产品可以联动统一运维管理平台实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验；（提供和统一管理平台的对接的承诺函） | 台 | 1 |
| 6 | 入侵防御（专网区） | 1、具备千兆电口≥4个，千兆光口≥4个，千兆多模光模块≥4个，支持扩展SSD硬盘；冗余交流电源； 2、整机网络层吞吐≥4Gbps，IPS吞吐≥600Mbps，最大并发连接数≥200万，每秒新建连接数≥2万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持丰富的路由协议，例如静态路由、策略路由（路由前策略、路由后策略、本地报文发包策略）、RIP、OSPF、ISIS、BGP； 5、内置丰富的IPS特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量≥9000条； 6、入侵防御日志支持聚合发送，聚合条件包括源IP聚合、目的IP聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器≥10个； 7、支持将设备划分成多台虚拟的IPS分给不同的租户使用，租户管理各自策略，相互隔离，虚拟IPS数量≥30个并发； 8、支持对邮件协议进行访问管控，包括对SMTP命令（至少包含EXPN、MAIL、RCPT、SAML、SEND、SOML、TURN、VRFY等命令）、邮件大小、邮件主题、收发件人、以及文件类型进行控制； 9、支持跨物理设备的端口聚合，扩展带宽节省链路资源以及方便部署。 | 台 | 2 |
| 7 | 入侵防御（互联网区） | 1、具备千兆电口≥8个，千兆光口≥6个，千兆多模光模块≥6个，支持扩展SSD硬盘；冗余交流电源； 2、整机网络层吞吐≥9Gbps，IPS吞吐≥1Gbps，最大并发连接数≥300万，每秒新建连接数≥3万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持丰富的路由协议，例如静态路由、策略路由（路由前策略、路由后策略、本地报文发包策略）、RIP、OSPF、ISIS、BGP； 5、内置丰富的IPS特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量≥9000条; 6、入侵防御日志支持聚合发送，聚合条件包括源IP聚合、目的IP聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器≥10个； 7、支持将设备划分成多台虚拟的IPS分给不同的租户使用，租户管理各自策略，相互隔离，虚拟IPS数量≥30并发； 8、支持对邮件协议进行访问管控，包括对SMTP命令（至少包含EXPN、MAIL、RCPT、SAML、SEND、SOML、TURN、VRFY等命令）、邮件大小、邮件主题、收发件人、以及文件类型进行控制； 9、支持跨物理设备的端口聚合，扩展带宽节省链路资源以及方便部署。 | 台 | 2 |
| 8 | 网络安全审计 | 1、具备千兆电口≥8个，千兆光口≥2个，千兆多模光模块≥2个；冗余交流电源； 2、网络层吞吐量≥9Gbps，并发连接数≥200万，每秒新建连接数≥1.5万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理； 5、支持策略路由协议、动态路由协议，包括RIP、OSPF、ISIS、BGP；  7、支持自定义应用：支持通过IP+端口方式自定义网络应用及基于深度检测方式（应用特征）自定义网络应用； 8、支持应用会话审计，包括IP、端口、应用类型、会话包数、字节数、时间等的审计； 9、支持用户时长分析：支持分析用户总时长、总流量以及用户具体应用的时长和流量，可通过饼状图或柱状图展示； 10、支持记录portal认证账号的最后一次的登陆时间，方便管理员清理长期未使用的账号，避免设备策略冗余； | 台 | 2 |
| 9 | 堡垒机（互联网） | 1、千兆电口≥6个，千兆光口≥4个，千兆多模光模块≥4个，USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥1T；内存≥16G，管理点数≥60个；采用国产化CPU和操作系统； 2、支持SSHv1、SSHv2、TELNET等字符协议；支持RDP、VNC等图形协议；支持FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议； 3、支持运维用户对未授权的资源、资源账号申请授权工单，授权工单通过后可运维申请的资源； 4、支持通过协议前置机进行协议扩展，可支持扩展 KVM、Vmware等虚拟平台上的资源、数据库、B/S应用、C/S 应用等； 5、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，对动作流配置即可实现单点登录和审计接入； 6、提供运维、监控、回放屏幕水印功能，并可根据实际需求场景选择开启范围，运维本地无法篡改水印内容，震慑不规范的运维和审计行为，提升运维过程数据安全性； 7、支持 linux 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息，支持手动添加、删除、编辑、检索资源，支持变更默认运维端口；支持资源的动态图表管理，系统可自动生成动态全景视图，支持资源的分类统计，提供资源分类可视化页面； 8、支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT 、 Xshell 、 Putty 、 WinSCP 、 FileZilla 、xftp、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯； 9、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期；用户登录认证方式支持静态口令认证、手机动态令牌认证、Usbkey（国密数字证书）认证、吉大正元网关认证、华测Ukey认证、北京CA认证、信安CA认证、中安云科认证、503CA认证、AD/LDAP认证、Radius认证、短信认证、指纹识别等认证方式，并支持组合形成双因子认证； | 台 | 1 |
| 10 | 堡垒机（专网区） | 1、千兆电口≥6个，千兆光口≥4个，千兆多模光模块≥4个，USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥4T；内存≥16G，冗余交流电源；管理点数≥300个；采用国产化CPU和操作系统； 2、支持SSHv1、SSHv2、TELNET等字符协议；支持RDP、VNC等图形协议；支持FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议； 3、支持运维用户对未授权的资源、资源账号申请授权工单，授权工单通过后可运维申请的资源； 4、支持通过协议前置机进行协议扩展，可支持扩展 KVM、Vmware等虚拟平台上的资源、数据库、B/S应用、C/S 应用等； 5、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，对动作流配置即可实现单点登录和审计接入； 6、提供运维、监控、回放屏幕水印功能，并可根据实际需求场景选择开启范围，运维本地无法篡改水印内容，震慑不规范的运维和审计行为，提升运维过程数据安全性； 7、支持 linux 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息，支持手动添加、删除、编辑、检索资源，支持变更默认运维端口；支持资源的动态图表管理，系统可自动生成动态全景视图，支持资源的分类统计，提供资源分类可视化页面； 8、支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT 、 Xshell 、 Putty 、 WinSCP 、 FileZilla 、xftp、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯； 9、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期；用户登录认证方式支持静态口令认证、手机动态令牌认证、Usbkey（国密数字证书）认证、吉大正元网关认证、华测Ukey认证、北京CA认证、信安CA认证、中安云科认证、503CA认证、AD/LDAP认证、Radius认证、短信认证、指纹识别等认证方式，并支持组合形成双因子认证； | 台 | 1 |
| 11 | 数据库审计 | 1、业务接口：千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个，USB host接口≥2个，Console口≥1个，扩展槽≥2个，采用国产化CPU和操作系统； 2、SQL流量吞吐≥500Mb/秒，业务流量吞吐≥2Gb/秒，SQL语句吞吐≥20000条/秒，数据库实例数≥10； 3、CPU ≥8核，内存≥16G，硬盘≥2T； 4、支持Oracle、SQLserver、DB2、MySQL、Cache、Sybase、Informix、Teradata、PostgreSQL、Hive、MongoDB、HANA、HBASE、ES、CacheWeb、Solr、HDFS、Redis、EsgynDB、Tibero、SSDB等国际主流数据库；支持DM7、神通、人大金仓、南大通用、湖南上容、浪潮KDB、HWMPP、翰高等国产数据库； 5、支持扫描网络中的开放的服务，自动发现网络中存在的数据库系统，能够能够对这些数据库系统进行安全审计； 6、支持自动发现敏感数据如身份证号、银行账号等信息，便于进行用户权限控制，支持将扫描到的敏感表信息进行导出； 7、支持自学习功能，能够基于自学习机制的模型策略，审计未授权的客户端ip地址，未授权的表操作访问、未授权的数据库用户、未授权的特权操作等; 8、支持跨包的SQL语句进行拼接功能，能够完整解析与审计超长SQL语句（≥1460字节），屏蔽逃逸审计通道； 9、支持查看数据库系统的监视器信息、软件版本信息、补丁信息、表空间情况、会话信息、回退信息、权限等信息来判断数据库系统运行是否正常，保证数据库系统的可用性和响应能力； 10、支持扫描以下系统风险：数据库表级访问的安全性设置，SGA共享池分配私有空间的限制，每次调用读入的数据块数目的限制，一次会话读入的数据块总数的限制，是否启用资源限制等数据库系统配置等； | 台 | 2 |
| 12 | 服务密码机 | 采用国产化CPU和操作系统； 网络接口≥2个千兆电口，不支持扩展，其他接口≥6个USB口、≥2个COM口 性能参数： SM4算法加解密：≥540Mbps；SM2密钥对≥12000对/秒；SM2加密：≥2600次/秒；SM2解密：≥3400次/秒；SM2签名：≥12000次/秒；SM2验签：≥4300次/秒；SM3杂凑运算：≥520Mbps | 台 | 1 |
| 13 | 签名验签服务器 | 采用国产化CPU和操作系统； 提供基于数字证书的数据签名与验证、加解密服务，支持SM2等签名算法； 硬件规格:≥2个100/1000M自适应网口。主要性能参数: SM2签名≥1600次/秒。 | 台 | 1 |
| 14 | 安全隔离与信息交换系统 | 1、业务接口：（内机）千兆电口≥6个，万兆光口≥2个，万兆多模光模块≥2个，满足接口基础要求上扩展槽≥1个；（外机）千兆电口≥6个，万兆光口≥2个，万兆多模光模块≥2个，满足接口基础要求上扩展槽≥1个；冗余交流电源；采用国产化CPU和操作系统； 2、网络层吞吐量≥1.5Gbps；并发连接数≥40W；视频并发路数≥450路D1视频；数据库同步速率≥3000条/秒； 3、带液晶屏，液晶菜单可显示内外网机IP地址、CPU使用率和内存使用率等整机信息； 4、支持远程ftp、远程SMB、远程NFS、远程sftp、本地ftp、本地sftp、客户端方式进文件交换同步; 5、可查看系统每日CPU、内存、负载使用率以及会话连接数变化情况，提供至少近7日变化图查询； 6、提供API管理接口，API管理接口支持访问密钥数字签名验证，确保访问请求身份认证以及数据未被非法篡改；接口支持授权管理，可针对访问请求进行访问权限控制； 7、支持移动网络接入，搭配外置4G/5G硬件模块实现电信、移动、联通移动网络拨号接入； 8、多机热备支持自定义服务监测对象，可对关键IP、服务进行监测，发现服务连接异常，及时进行主备切换； 9、支持批量数据表智能匹配配置，可自动匹配表名、字段相同的数据表建立同步关系，满足大批量数据表同步场景下的快速配置需求; 10、支持SMTP\POP3协议，支持发件人、收件人地址过滤；支持主题关键字、正文关键字、附件文件名、附件正文过滤；支持文件类型过滤；病毒扫描; | 台 | 2 |
| 15 | 态势感知平台 | 1.千兆电口≥4个，万兆光口≥2个，万兆多模光模块≥2个，USB接口≥4个，扩展槽≥2个；硬盘≥8T；CPU≥8核；冗余交流电源； 2.单台最大流量处理能力≥1G；采用国产化CPU和操作系统； 3.支持5G协议解析和威胁检测，可查看5G威胁的日志统计数据，包括攻击级别分布，攻击名称Top5和手机号Top5统计图以及5G威胁事件的列表；支持查看5G威胁日志的攻击列表展示，包括攻击者、受害者、所属机构、攻击类型、攻击名称、关键字、发现时间； 4.支持从外连地址和受害者的维度展示外连威胁，查看单条外连威胁详情时将外连攻击行为信息进行展示； 5.支持自定义攻击事件分析模型，包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置38种及以上安全事件分析模型，如冰蝎webshell通信、利用Sqlmap上传webshell、Acunetix安全工具扫描、APPSCAN工具扫描等； 6.支持自定义配置的分析条件，包括：URL、HTTP方法、HTTP域名、HTTP状态码、DNS解析域名、TLS指纹、TLS版本、SSH服务端协议版本、SSH客户端协议版本、文件类型、文件哈希值、恶意文件家族、SMTP发件人等； 7.支持时间轴溯源分析，以时间轴的形式展示攻击者在入侵全过程中各个入侵时间节点中的攻击目标、攻击次数、攻击手段以及攻击阶段，同时提供各攻击手段安全处置建议； 8.支持基于ATT&CK框架的模型分析； 9.支持多层溯源功能，开启多层溯源后，默认展示两层溯源信息，攻击手段在展示图中消失，右侧展示攻击手段TOP5及描述信息； 10.支持攻击关系分析，以攻击者视角展示针对每个攻击目标所采用的攻击手段的攻击关系视图，同时展示攻击事件的攻击手段TOP统计，以及每种攻击手段的描述说明，并支持下钻； 11.支持攻击详情分析，基于受害者、目的端口、时间段、攻击手段、攻击类型、攻击级别、攻击名称等七个维度进行网络攻击日志检索，可查看本次攻击事件涉及的网络攻击的详细情况，以及下载原始攻击数据包； 12.支持AI判真功能，存在多个攻击手段的攻击事件显示为AI判真事件，AI判真事件存在AI判真标识； 13.支持AI自动处置功能，支持攻击事件按照昨天的处置历史信息进行处置，攻击事件被盖上相应的处置标签；历史处置记录按时间轴形式显示处置时间、设备信息或备注信息；处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息； 14.支持展示安全风险评级、攻击事件类型TOP5、攻击事件级别分布、外部攻击类型TOP5、外部攻击者TOP5等信息，支持在全球地图上展示攻击者到受害者的攻击视图，展示主要攻击类型，展示资产受害者TOP5，支持展示攻击者数量、受害者数量、攻击总数、已沦陷资产数量和活跃攻击源TOP5等信息，同时支持实时滚动攻击日志，每条攻击至少包括攻击者、受害者、攻击类型、攻击等级、攻击名称和时间。 | 台 | 1 |
| 16 | 态势感知探针 | 1、千兆电口≥4个，万兆光口≥2个，万兆多模光模块≥2个，USB接口≥4个，扩展槽≥2个；硬盘≥4TB；冗余交流电源； 2、流量采集能力≥1G； 3、支持设置标准模式、增强模式、深度模式、专家模式等流量分析策略，可设置不同策略类型，包括攻击策略、审计策略、采样等级、高级设置； 4、支持多种漏洞攻击检测，至少包括：信息泄露、文件包含、文件上传、目录遍历、跨站脚本、代码注入、反序列化、命令执行、未授权访问、模板注入、文件下载、XML外部实体注入、越权访问、XPATH注入、SQL注入、跨站请求伪造、服务端请求伪造、逻辑绕过、缓冲区溢出、DoS攻击、其它漏洞、可以的User-Agent等； 5、支持对5G协议解析和威胁检测，可以通过平台查看5G威胁的日志统计数据，包括攻击级别分布，攻击名称Top5和手机号Top5 统计图以及5G威胁事件的列表； 6、支持基于机器学习的提取攻击者真实访问的URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者IP、攻击者URL、访问行为的原始报文等； 7、支持多种恶意软件检测，至少包括：勒索病毒、挖矿软件、僵尸网络、shellcode、蠕虫病毒、木马病毒、黑客工具、Rootkit、BootKit、恶意文件投放等； 8、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS等协议的隧道通信； 9、可自定义弱口令规则，低、中、高三种密码规则，结合预定义弱口令字典，对弱口令威胁的检测更准确;界面可展示检测的弱口令威胁日志，有关键字的会展示关键字。 | 套 | 1 |
| 17 | 杀毒软件 | 1、产品以纯软件交付，本次配置≥100点服务器资源且提供不少于三年的软件升级服务，包含管理控制中心软件及终端客户端软件，其中管理控制中心支持云化或者本地化管理平台交付； 2、Windows桌面支持：Windows XP（32位）、Windows 7、Windows 8/8.1、Windows 10等；Windows服务器：Windows Server 2003（32位）/2008/2012/2016/2019等，支持国产化操作系统； 3、单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器和国产化操作系统的客户端软件； 4、采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； 5、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量。 | 套 | 1 |
| 18 | 日志审计（互联网区） | 1、 千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个；USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥2T+mSATA 128G；内存≥16G； 2、 日志处理能力≥2000条/秒，日志存储能力≥1.7亿条/天，审计授权≥60；  3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、 支持日志查询，可根据接收时间、源目IP、严重级别等信息进行查询，可针对查询到的日志结果进行导出；支持普通模式查询，并且可以根据查询的条件进行模板保存，以便于后续使用；支持专家模式查询，可通过编写表达式进行对日志信息进行更加全面的查询，并且可以根据查询的条件进行模板保存，以便于后续使用； 5、 审计策略：内置审计分析策略，包含：DDoS攻击、Webshell攻击、XSS跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换root用户、系统重启、硬件故障等。 6、 采集方式：支持基于TCP和UDP的syslog协议、kafka、snmp trap、ftp、smb、wmi、sftp等采集协议格式的模式解析； 7、 采集策略：支持被采设备无需安装代理；支持同一资产多种采集策略；支持从不同类型系统采集到的日志进行标准化分析，将不同格式日志映射到固定的解析字段中，标准化处理后的字段细粒度≥90； 8、支持将采集到的日志进行过滤，可以根据自身业务需求定制过滤策略，做到将无关日志进行丢弃；支持将采集到的日志进行归并，可以根据自身业务需求定制归并策略，做到在一定条件下将接收到的相同日志归并为一条，并且显示该日志的接收次数，使日志信息简明易看；  9、 支持三权分立原则，可设置安全管理员、安全审计员、系统管理员等角色。通过赋予不同角色不同的权限，以达到配置权力、审计权力、运维权力的相互制约； | 台 | 1 |
| 19 | 日志审计（专网区） | 1、 千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个；USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥4T+mSATA 128G；内存≥32G；冗余交流电源； 2、 日志处理能力≥3000条/秒，日志存储能力≥2.5亿条/天，审计授权≥110； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、 支持日志查询，可根据接收时间、源目IP、严重级别等信息进行查询，可针对查询到的日志结果进行导出；支持普通模式查询，并且可以根据查询的条件进行模板保存，以便于后续使用；支持专家模式查询，可通过编写表达式进行对日志信息进行更加全面的查询，并且可以根据查询的条件进行模板保存，以便于后续使用； 5、 审计策略：内置审计分析策略，包含：DDoS攻击、Webshell攻击、XSS跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换root用户、系统重启、硬件故障等。 6、 采集方式：支持基于TCP和UDP的syslog协议、kafka、snmp trap、ftp、smb、wmi、sftp等采集协议格式的模式解析； 7、 采集策略：支持被采设备无需安装代理；支持同一资产多种采集策略；支持从不同类型系统采集到的日志进行标准化分析，将不同格式日志映射到固定的解析字段中，标准化处理后的字段细粒度≥90； 8、支持将采集到的日志进行过滤，可以根据自身业务需求定制过滤策略，做到将无关日志进行丢弃；支持将采集到的日志进行归并，可以根据自身业务需求定制归并策略，做到在一定条件下将接收到的相同日志归并为一条，并且显示该日志的接收次数，使日志信息简明易看；  9、 支持三权分立原则，可设置安全管理员、安全审计员、系统管理员等角色。通过赋予不同角色不同的权限，以达到配置权力、审计权力、运维权力的相互制约； | 台 | 1 |
| 20 | 抗DDOS攻击设备 | 1、业务接口：千兆电口≥8个，千兆光口≥2个，千兆多模光模块≥2个，万兆光口≥4个，万兆多模光模块≥4个，冗余交流电源； 2、网络层吞吐量≥10Gbps，最大并发连接数≥800w，最大每秒新建连接数(HTTP) ≥12w； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持针对网络层、应用层分别设置清洗策略，包括不限于：SYN Flood、UDP Flood、ICMP Flood、DNS Query/Reply Flood、HTTP Flood、HTTPS Flood; 5、支持针对不同防护对象，分别设置不同的异常流量清洗参数、算法等； 6、支持抓包溯源功能，支持抓取清洗前、清洗后、清洗丢弃的报文进行分析；针对抓包文件可以进行攻击源IP溯源，并提取攻击报文中的攻击特征下发到清洗设备过滤； 7、支持连接数新建及并发限制功能，可对TCP等协议设置阈值及周期； 8、支持会话数限制，可对源地址/目的地址做会话数限制，设置维度包括：服务类型（可定义服务类型）、用户、新建速率、总会话数、每IP会话数、生效时间等； 9、支持针对协议头中各字段配置自定义策略，字段包括但不限于：Method、Cookie、Host、Referer、Request URI、Verion、User-Agent等； 10、为保障异常流量安全清洗和业务系统稳定运行，抗DDOS攻击设备可以被统一运维管理平台监控。（提供和统一管理平台的对接承诺函并加盖抗DDOS攻击设备厂商公章） | 台 | 2 |
| 21 | 互联网VPN接入设备 | 1、具备千兆电口≥8个，千兆光口≥2个，万兆光口≥4个，万兆多模光模块≥4个，冗余交流电源；采用国产化CPU和操作系统； 2、整机吞吐量≥9Gbps，每秒新建连接数≥10万，最大并发连接数≥500万； VPN加密性能：IPsec VPN吞吐量≥1Gbps，IPsec VPN隧道数≥2000个；SSL VPN吞吐量≥1Gbps，SSL VPN并发用户数≥3000个，总用户数不限； 3、支持集群：双机模式下，支持主备两台设备采用同一套IP地址，简化配置，节约公网地址； 4、内网攻击防护：基于内网用户流量模型和会话连接、新建连接的异常行为识别攻击，有效防护内网病毒传播、僵尸网络、木马等安全威胁； 5、支持静态路由、RIP v1/2、OSPF、策略路由等。支持MPLS VPN；支持MPLS静态标签转发；支持LDP协议，支持LDP引入OSPF路由、BGP路由、RIP路由、静态路由、ISIS路由、GUARD 路由，支持环路检测；支持LDP邻居，MPLS转发表查看；支持SVC方式、CCC方式、MARTINI方式、VPLS方式的L2VPN；支持MPLS TE； 6、提供设备的可靠性试验证明，(设备厂商提供证明材料)； 7、支持自动和手动备份，能够保存5个以上的文件，支持整机配置文件在线回滚功能，未变化的业务连续不中断； 8、登录公告：支持VPN登录前和登录后公告信息显示，登录前后公告内容可配置多条； 9、产品需要支持国密算法，具备商用密码产品认证证书；（提供证书复印件并加盖原厂商公章） | 台 | 2 |
| **四** | **机房设备** |  |  |  |
| 1 | 微模块机柜 | 1.外形尺寸：服务器机柜规格（W\*D\*H）：600mm\*2000mm，前门为玻璃门，后门为钢板门。 2.机柜涂覆层应表面光洁、色泽均匀、无流挂、无露底；金属件无毛刺、无锈蚀。机柜门板、侧板平整，无扭曲、无变形、也不明显抖动；门板开孔均匀。 3.机柜由主框架、顶板、内嵌底板、前后门、侧横梁、矩形管、内立柱和固定层板组成。其中主框架、内立柱的、侧横梁的材料厚度不小于2.0mm，后门、顶板、和侧板的材料厚度不小于1.2mm。 4.为方便设备安装及维护，门板为可拆卸式结构，门的开合转动灵活、锁定可靠、施工安装和维护方便。 5.为了保障用电安全，要求机柜内各带电回路对地（或柜体）绝缘电阻不小于100MΩ。 6.机柜耐电压强度：要求机柜内各带电回路以及两个非电气连接的带电回路之间，应能承受2500V，50HZ正弦试验电压1min，并不出现击穿或者飞弧现象，漏电流不超过1mA。 7.机柜附件：每个机柜含接地组件（接地线6mm²）、左后各1条垂直理线板、19英寸安装接地铜排（3\*15mm²）、运输脚轮、LED灯管+行程开关。 | 台 | 15 |
| 2 | 列头机柜 | 1.外形尺寸：服务器机柜规格（W\*D\*H）：600mm\*2000mm，前门为玻璃门，后门为钢板门。 2.要求配电柜主路开关不小于2\*160A/3P，防雷模块不低于C级防雷模块。 3.要求配电柜支路开关不小于且不少于两路24\*32A/1P，支路监测参数要求包含：支路额定电流、实际电流，支路负载百分比，支路开关状态。 | 台 | 1 |
| 3 | 智慧机柜侧板 | 机柜配件,侧板,1400mm(D)\*2000mm(H) | 套 | 2 |
| 4 | 机柜锁具 | 机柜配件,电子锁\*2,刷卡一体,带钥匙和IC卡1张,包含配套线缆 | 套 | 16 |
| 5 | 智慧机柜M型走线槽 | 顶部M型走线槽,600mm(W)\*300(D)\*150(H),强弱分离,带隔板 | 套 | 20 |
| 6 | 快开盲板 | 1U免工具安装盲板,快开方式,钣金 | 个 | 150 |
| 7 | 水平理线器 | 水平理线器,482\*44\*80MM | 条 | 15 |
| 8 | 智慧机柜轻载托盘 | 100kg承重开孔托盘,19",适配600宽1100深以上机柜-微模块 | 块 | 15 |
| 9 | L型托架 | 50kg承重L型托架1副(2只,左右各1) | 对 | 15 |
| 10 | 智慧机柜专用普通PDU | 1.每个机柜标配2条PDU，为设备A/B路供电使用。两条PDU应为同一规格，互为备份。 2.交流PUD采用黑色涂层，外壳选用优质型材或钢板，应具备强度高，坚固耐用，抗压性能、装配性能、耐蚀性能和装饰性能良好，表面喷涂效果好，工艺先进，纹路平整，美观大方等特点。 3.机柜PDU输出接口具有GB标准类型，10A的插座不少于16个，16A的插座不少于4个。 | 个 | 30 |
| 11 | 列间空调 | 1.总冷量≥35kw，显冷量≥35kw，风量≥6100m³/h，加湿量≥1.5kg/h，加热量≥4kW，水平送风模式； 2.可以实现常温情况下最低10%的IT负载（即制冷量的10%）稳定除湿量功能，降低高湿环境下数据中心低载运行的IT设备结露风险。 3.精密空调室内机采用高效工业用直流变频压缩机，可实现10%～100%宽冷量输出； 4.为了相应国家节能节耗政策，要求空调全年能效比应大于3.5； 5.具有LCD的真彩触摸显示屏，可以显示设备的运行模式与状态，并可设定设备参数，实现良好的人机交互 6.机组具备联动与群控功能，群控采用高速、灵活的CAN通讯协议，同一区域可以将≥32套机组进行统一控制管理； 7.室内风机：要求采用高效后倾离心式EC风机。 8.要求空调机组设备符合GB19413相关标准。 | 套 | 4 |
| 12 | 盲柜 | 规格：≥300\*1400\*2000mm(W\*D\*H),黑色 | 套 | 4 |
| 13 | 机柜监控主机 | 1.通道动环监控主机，ARM架构，Linux系统；双交流供电，支持多路温湿度、烟雾、漏水、端门、天窗、空调、UPS、配电单元、消防、声光告警器等的监测和/或控制。 | 台 | 1 |
| 14 | 微动环监控平台系统软件 | 1.安装在服务器或PC端，通过有线连接，后台软件展示模块机房温湿度、通道门禁状态、能耗等动环实时监控数据； 2.为了保证机房健康运行，要求平台软件具有告警管理功能，可实现实时告警查看、待处理告警统计、历史告警查看以及可自定义设置告警阀值和告警等级等功能，且可自主远程邮件和短信发送相关负责人，可及时发现告警，并能及时处理，保障机房健康安全运行； 3.要求在本软件可实时查看行级空调运行状态和配电模块以及UPS电压、电流、电功率、负载百分比以及电池容量等运行状态。 | 套 | 1 |
| 15 | 电话,短信告警模块 | 可通过电话或短信的形式对告警内容进行通知。 | 个 | 1 |
| 16 | 手机APP客户端接入接口 | 手机APP客户端接入接口,须能够支持安卓4.0及以上智能设备-微模块 | 套 | 1 |
| 17 | 温湿度传感器 | 磁吸式温湿度传感器,测温范围:-20℃-70℃,测湿范围:0%-100%RH,12V接线端子供电 | 个 | 4 |
| 18 | 烟雾探测器 | 机柜专用光电烟感探测器,磁吸式,工作电压:DC12V | 个 | 4 |
| 19 | 声光报警器 | 磁吸式电子蜂鸣器,声压105db,声频1500±500Hz,60mA,DC12V | 个 | 1 |
| 20 | 水浸探测绳 | 非定位式水浸探测绳,配合非定位水浸传感器使用(5米) | 根 | 4 |
| 21 | 智慧模块化通道电源控制箱 | 一体柜控制箱,350W12V开关电源,含照明灯,背景灯电源,2U | 套 | 1 |
| 22 | 机房强弱电设备安装及配套辅材 | 机房强弱电设备安装费及配套辅材费，包括网线、电缆等。 | 套 | 1 |
| **五** | **其它设备** |  |  |  |
| 1 | 指挥中心大屏 | 面积≥20m²； 点间距：1.2mm； 封装方式： COB； 亮度：≥800cd 分辨率：≥4K; | m² | 20 |
| 2 | 可视化综合管控一体机 | CPU：≥16核，≥2.0GHz； 内存：≥16GB; 硬盘：≥2TB； 显卡：显存≥4GB； 可实现对视频拼接处理的集中统一管理，控制各屏的输出内容。设备带有话筒、投屏器、控制台等外设。 另需包含管理软件。 | 台 | 1 |
| 3 | 拼接屏处理器 | 1.1920x1080p@60Hz信号，处理平台内部不进行任何抽帧，满帧输出至显示设备。支持场景轮循， 2.信号支持：4096x2160@60hz，4096x2160@30hz，3840x2160@30hz，3840x2400@30hz，2560x1600@60hz分辨率，向下兼容其他分辨率， 3.支持在输出通道上打开高达16个高清信号窗口，且每个窗口支持大小任意调整，图层顺序调整。支持多组屏硬回显，可同时将4组不同大屏的整体显示画面通过回显板卡传输至显示器，进行高清显示，回显帧率可达60hz。可以在控制端实时回显大屏整体画面。 4.配置双控制卡，双电源 | 个 | 1 |

| **序号** | **名称** | **主要性能（技术）指标** | **单位** | **数量** |
| --- | --- | --- | --- | --- |
| **一** | **系统软件** |  |  |  |
| （一） | 操作系统 | 具备文件管理、设备管理、日志管理、服务管理、进程和监控管理、网络管理、资源管理、软件包管理、硬件管理等基本功能，提供语言支持工具、文件共享服务工具、集成开发平台等常用工具，支持KVM、Docker虚拟化技术。 硬件支持‌：支持 X86 和 ARM 架构的处理器，如海光、鲲鹏 、飞腾等；符合国家信创要求； 授权方式：按节点授权。 | 套 | 55 |
| （二） | 数据库 | 符合国家信创要求；具备数据存储、访问控制、身份鉴别、安全审计和数据备份恢复等功能。产品部署在服务器，以后台服务形式运行，数据库管理员及用户在管理主机上通过图形化管理工具或命令行工具，可实现对数据对象（表、视图、约束、索引、触发器、存储过程等）的配置管理；开发人员可通过标准化数据库访问接口，开发基于数据库的应用系统和软件产品。 授权方式：按节点授权。 | 套 | 25 |
| （三） | 中间件 | 用于为上层应用提供运行环境，实现对上层应用的部署和动态管理。主要功能包括Web容器、EJB容器、数据源服务、集群管理等。产品可部署在信创服务器，以后台服务形式运行，用户通过管理控制台或者命令行工具完成上层应用的部署、启动、停止等操作。符合国家信创要求。 授权方式：按节点授权。 | 套 | 30 |
| **二** | **应用软件** |  |  |  |
| （一） | 项目管理系统 | 项目管理系统可完整覆盖项目管理的各个过程，帮助企业建立研发管理体系，提高企业管理流程的稳健性和项目管理成熟度，大大提升项目成功的概率。 本系统主要提供标准化模板（如敏捷、瀑布模型），支持项目拆解子任务，设置任务的优先级和依赖性关系，制定预算并关联任务成本，设置交付物和验收标准。 | 套 | 1 |
| （二） | 统一运维管理系统 | 统一运维平台可以将本项目涉及的网络和安全设备进行集中管理，对网内安全设备、网络设备、服务器等进行实时运行状态监控，分析研判各类安全事件，通过访问控制策略的配置，实现大规模部署环境下灵活、便捷的安全策略管理，阻止敏感信息外泄和非核心业务的滥用；同时还可以联动现网扫描设备实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验，确保网络的整体安全。设备含设备管理、网络监控、攻击监控、系统管理、通用图标等≥65种大屏展示组件，可以以折线图、环形图、柱状图等形式进行展示。 | 套 | 1 |
| （三） | 统一门户 | 统一门户平台集成了本项目的所有应用（除智慧共享药房、针灸数智服务平台以外），实现一键登录，支持his集成，用户同步认证。 系统主要功能包括身份认证、身份管理、统一权限、单点登录、信息共享、应用管理与注册、门户管理、页面管理、部件管理导航管理、内容管理等。 | 套 | 1 |

**现变更为：**

**硬件类**

| **序号** | **名称** | **主要性能（技术）指标** | **单位** | **数量** |
| --- | --- | --- | --- | --- |
| **一** | **服务器** |  |  |  |
| 1 | 大数据服务器 | 1、规格：≥12个3.5英寸硬盘盘位； 2、CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，支持超线程； 3、内存：配置≥16\*32GB DDR5 内存条； 4、系统盘：配置≥2\*960GB SSD； 5、数据盘：配置≥6\*4TB SATA； 6、缓存盘：配置≥2\*3.2TB NVMe SSD； 7、网口：配置≥4个GE，≥2个10GE光口（含光模块），≥2个25GE光口（含光模块）； 8、RAID卡：配置独立RAID卡； 9、配置冗余电源，冗余风扇； 10、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 18 |
| 2 | 应用服务器 | 1、规格：≥12个3.5英寸硬盘盘位； 2、CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，支持超线程； 3、内存：配置≥16\*32GB DDR5内存条； 4、系统盘：配置≥2\*960GB SSD； 5、网口：配置≥4个GE，≥2个10GE光口（含光模块），≥2个25GE光口（含光模块）； 6、RAID卡：配置独立RAID卡； 7、配置冗余电源，冗余风扇； 8、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 15 |
| 3 | 边缘超融合节点 | 1、通过服务器节点构建，同一节点内实现计算存储融合，可配置副本（2副本或3副本）或EC（纠删码），可满足不同可靠性要求的业务场景。 2、支持图形化界面划分存储资源池，每个存储资源池即为一个故障域，保证可靠性。 3、配置超融合管理授权及分布式存储授权，共配置≥3个节点，单节点配置如下： 1）规格：≥12个3.5英寸硬盘盘位； 2）CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，或支持超线程； 3）内存：配置≥16\*32GB DDR4 内存条或DDR5内存条； 4）系统盘：配置≥2\*960GB SAS SSD； 5）数据盘：配置≥5\*4TB SATA； 6）缓存盘：配置≥1\*3.2TB NVMe SSD； 7）网口：配置≥4个GE，≥4个10GE光口（含光模块）； 8）RAID卡：配置独立RAID卡； 9）配置冗余电源，冗余风扇； 10）为保证项目正常交付，须提供服务器厂家的质保函； | 套 | 2 |
| 4 | 高性能存储节点 | 1、控制器规格：≤5U机架式双控制器存储； 2、缓存：≥768GB缓存，交流电源； 3、处理器：国产化处理器，总核数≥128核； 4、端口：≥4\*100Gb RDMA； 5、端口：≥2\*4端口25Gb ETH(含模块)； 6、端口：≥2\*4端口 1Gb ETH ； 7、硬盘：配置≥16块7.68 TB NVMe SSD ，≥77块16TB 7.2K RPM NL SAS，RAID6后可得容量不低于1PB； 8、线缆：配置≥8根多模光跳线； 9、线缆：配置≥4\*高速电缆-48G Mini SAS -3m； 9、配置SAN许可(含存储管理软件,瘦分配,数据迁移,快照,远程复制,克隆,服务质量管理,智能运维软件,主机多路径,异构虚拟化,双活,CDP)； 10、配置NAS许可(含CIFS,NFS,NDMP,瘦分配,快照,远程复制,克隆,服务质量管理,双活,CDP,智能运维软件,NAS备份)； 11、存储系统为对称AA架构，LUN无控制器归属，在多控配置下，能够负载到所有控制器，CPU利用率差异小于5%，提供CNAS检测证明，并加盖厂商公章。 | 台 | 2 |
| 5 | 中心智算节点 | 1、单节点国产化AI算力：≥2.2 PFLOPS FP16，单节点≥512GB HBM高带宽显存。单个AI处理器/加速卡支持≥280TFLOPS@FP16算力，单卡≥64GB HBM高带宽内存。 2、单节点CPU：≥4颗国产化处理器，单颗物理核心数≥48，主频≥2.6GHz。 3、单节点内存：容量 ≥512G DDR4，内存频率≥3200MHZ。 4、单节点硬盘：≥2\*960GB SSD，≥2\*3.2TB SSD；。 5、单节点网络：≥2个10GE光口（含光模块），≥4\*25Gbps端口(含光模块)，≥8\*200G光口（含光模块）。 6、根据网络信息安全要求，主板管理控制器为国产管理芯片，该芯片能提供基于Web的远程管理控制、配备硬件监控、远程管理功能，支持IPMI2.0标准，提供IKVM功能，实现远程KVM功能。 7、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 4 |
| 6 | 边缘智算节点 | 1、规格：≥12个3.5英寸硬盘盘位； 2、CPU：配置≥2颗国产化处理器，主频≥2.6GHz，≥64core处理器，或支持超线程； 3、内存：配置≥8\*32GB DDR4 内存条； 4、系统盘：配置≥2\*960GB SAS SSD； 5、网口：配置≥4个GE，≥4个10GE光口（含光模块）； 6、RAID卡：配置独立RAID卡； 7、加速卡：≥4\*AI加速卡；单卡≥140T FP16、≥96GB； 8、配置冗余电源，冗余风扇； 9、为保证项目正常交付，须提供服务器厂家的质保函； | 台 | 6 |
| 7 | 备份一体机 | 1、支持对Oracle、MySQL、SQL Server、GaussDB OLTP、OpenGauss、Postgre SQL、达梦、KingBase、DB2、SAP HANA、GoldenDB、HCS GaussDB数据库进行在线备份保护。 2、支持Oracle、MySQL数据库的永久增量备份功能，合成副本支持数据重复删除、备份副本异地复制、备份副本长期保留到对象和带库功能，支持备份副本即时挂载和恢复。 3、支持HDFS、HBase、Hive、ElasticSearch、Redis、ClickHouse等大数据组件的数据备份功能。备份任务配置过程全部图形化操作，无需编写脚本，且支持HDFS单文件、HDFS目录、HBase单表、HBase NameSpace级、Hive表级、ElasticSearch索引级、ClickHouse表级细粒度备份和恢复能力。 4、提供按备份任务细粒度复制，支持设置立即复制和周期性复制，支持设置复制副本保留时长（支持永久保留、按年/月/周/天保留）； 5、双控,SSD&HDD,≥256GB 缓存,采用国产化处理器，主频≥2.6GHz，总核心数≥40core；实配≥4\*960GB SSD SAS硬盘；≥8\*8TB 7.2K RPM NL SAS硬盘；配置≥32T备份许可；提供≥8个GE，≥4个10GE光口（含光模块）； | 台 | 2 |
| 8 | 云平台 | 1、平台云软件支持对存储、交换机、服务器、超融合、虚拟化资源的统一管理，无需多个软件界面分散管理，管理能力包括设备基本信息查询、配置信息查询、历史性能信息、资源利用率查询、设备告警信息查询等； 2、支持在同一界面配置交换机设置，块存储、文件存储快速发放，实现虚拟机端到端的发放。 3、提供了虚拟机视角的IO路径全链路故障诊断：一个界面展示虚拟盘、虚拟机、主机、交换机、存储设备的IO路径级的拓扑信息。 4、基于应用视角，提供了包含虚拟机、主机、LUN、存储等对象实例的多维度的关联对象分析，快速定界定位问题。 5、支持通过设置快照策略任务对虚拟机进行定时快照，满足日常运维管理诉求。运维人员可设置不同的虚拟机快照策略，可按天、周、月设置执行计划。 6、提供预见式运维，支持管理员可自定义检查条件，对存储、计算、网络的配置、容量、性能、可用性、低负载、可回收资源进行检查，在匹配到违规条件时，产生事件，帮助管理员实现风险提前识别与闭环。 7、支持用户针对指定的虚拟机配置检查策略，达到策略定义的阈值后自动扩容虚拟机的CPU或者内存。过程中虚拟机正常运行不需要重启。 8、支持批量对多个虚拟机的CPU、内存、磁盘硬件参数做变更配置，提升运维效率。 9、支持大屏展示，预置超过3种大屏；预置超过20种图表控件，可支持用户自定义大屏内容。 10、支持租户管理，提供资源配额管理。 11、支持报表统计，支持周期性自动生成报表，预置容量、资源性能，告警等30多种典型业务场景的报表。支持用户自定义报表统计内容。 12、配置≥42颗CPU计算虚拟化高级版/企业版授权、≥1800核容器授权及≥110颗CPU云平台授权； | 套 | 1 |
|  |  |
| **二** | **网络设备** |  |  |  |
| 1 | 互联网核心交换机 | 1.交换容量≥170Tbps，包转发率≥128000Mpps； 2.主控槽位≥2个；整机业务板槽位数≥8个，主控槽位与业务线卡槽位宽度相同，为全宽槽位，电源槽位≥4个； 3.要求设备采用国产化CPU芯片和转发芯片； 4.支持VxLAN 分布式网关、集中式网关，BGP-EVPN，通过 Netconf配置VxLAN； 5.支持整机MAC地址≥380K；MAC学习速率≥16000/s;整机ARP表项≥140000，整机ND表项≥80000，IPv4 路由表以及 FIB表≥256000， IPv6 路由表以及 FIB表≥80000； 6.支持 Telemetry 技术，实时采集设备数据并上送至网络分析组件平台，通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，及时定界故障以及故障发生原因，精准保障用户体验； 7.配置要求: 双主控引擎，≥2个独立风扇框，≥2个交流电源，≥2个100G光口，≥24个万兆光口，≥32个千兆光口，≥48个千兆电口，≥24个万兆多模模块，≥1根5米万兆集群线缆。为满足后期扩容需求，满足上述配置后空余业务槽位≥4个； | 台 | 2 |
| 2 | 互联网接入交换机 | 1.交换容量≥2.5Tbps，转发性能≥1500Mpps； 2.万兆光接口≥24个，100G光接口≥2个，交流电源≥2个，≥24个万兆多模模块，40G堆叠线缆≥1根； 3.支持VXLAN分布式网关，集中式网关，支持BGP-EVPN，支持VXLAN 路由交换； 4.支持RIP、RIPng、OSPF、OSPFV3、ISIS、ISISV6、BGP、BGP4+； 5.设备关键芯片(CPU、转发芯片)均为国产化芯片； 6.MAC 地址表容量≥128K， ARP 地址容量≥64K， FIBv4 表容量≥128K， FIBv6 表容量≥64K； 7.为了方便后期维护，要求设备支持外置复位按钮，可在忘记密码或清空配置时使用，使设备快速恢复出厂配置； | 台 | 2 |
| 3 | 核心交换机 | 1.交换容量≥800Tbps，包转发率≥230000Mpps； 2.整机主控槽位≥2个，业务槽位数≥4个，交换网板与业务槽位垂直正交CLOS架构； 3.设备关键芯片(CPU、转发芯片)均为国产化芯片； 4.支持Vxlan协议，且支持BGP EVPN协议； 5.MAC地址表容量≥250K，ARP地址容量≥250K，FIBv4表容量≥250K，FIBv6表容量≥80K； 6.配置要求：冗余主控，交换网板≥6个，电源≥2个，40G光接口≥36个，10G光接口≥48个，万兆多模模块≥48个，5米40G高速线缆≥2根； | 台 | 2 |
| 4 | 接入交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.固定接口交换机，独立风扇模块≥3个，电源槽位≥2个； 3.设备CPU芯片和转发芯片均采用国产自研芯片； 4.支持配置回滚，在系统运行过程中发现配置错误、业务运行不正常，可以通过该命令将系统回退到指定的历史配置状态； 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维ID指示灯，现场定位用指示灯，运维人员可远程控制ID灯开启和关闭； 6.配置：10GE光接口≥48个，100GE光接口≥8个 ，万兆多模模块≥48个，40G多模模块≥4个，配置冗余电源； | 台 | 10 |
| 5 | 存储互联交换机 | 1.交换容量≥8Tbps，包转发率≥2300Mpps； 2.固定接口交换机，独立风扇模块≥5个，电源槽位≥2个； 3.支持智能无损网络特性，支持PFC死锁预防，支持识别流量模型动态调节ECN门限功能即AI ECN功能； 4.设备CPU芯片和转发芯片均采用国产自研芯片； 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维ID指示灯，现场定位用指示灯，运维人员可远程控制ID灯开启和关闭； 6.配置：25GE光接口≥48个（不可通过接口拆分提供），100 GE光接口≥8个，≥48个25G多模模块，≥4个40G多模模块，配置冗余电源； | 台 | 2 |
| 6 | 超融合接入交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps； 2.固定接口交换机，独立风扇模块≥3个，电源槽位≥2个； 3.设备CPU芯片和转发芯片均采用国产自研芯片； 4.支持配置回滚，在系统运行过程中发现配置错误、业务运行不正常，可以通过该命令将系统回退到指定的历史配置状态； 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维ID指示灯，现场定位用指示灯，运维人员可远程控制ID灯开启和关闭； 6.配置：10GE光接口≥48个，100GE光接口≥8个 ，万兆多模模块≥48个，40G多模模块≥4个，配置冗余电源； | 台 | 4 |
| 7 | 高速互联交换机 | 1.交换容量≥25.6Tbps ，包转发率≥8000Mpps； 2.固定接口交换机，电源模块槽位≥2个，支持电源1+1备份，风扇模块槽位≥6个； 3.400GE QSFP-DD光接口≥32个，10GE SFP+光接口≥2个，配置≥24个400G光模块以及配套400G一分二线缆； 4.设备CPU芯片、转发芯片均为国产自研芯片，满足自主可控； 5.支持AI ECN，可以根据现网流量模型智能调整无损队列的ECN门限，可以保障零丢包下的低时延和高吞吐，让无损业务达到最优性能； 6.支持M-LAG或vPC或DRNI等跨机箱链路捆绑技术； 7.支持RDMA,RoCEv2,可提供“无丢包、低时延、高吞吐”的网络环境； 8.支持Vxlan，且支持 EVPN VxLAN，支持VxLAN网络与VLAN网络互通； | 台 | 1 |
| 8 | 管理交换机 | 1.交换容量≥660Gbps，包转发率≥200Mpps； 2.固定接口交换机，电源槽位≥2个； 3.设备支持复位按钮，忘记密码可以通过按钮恢复出厂设置； 4.设备CPU芯片和转发芯片均采用国产自研芯片； 5.支持配置回滚不重启，在系统运行过程中发现配置错误、业务运行不正常，可以通过该命令将系统回退到指定的历史配置状态； 6.设备支持ID指示灯，便于快速定位设备位置； 7.配置：千兆电接口≥48个，10GE光接口≥4个，支持≥2个专用堆叠口，≥4个万兆多模模块，配置冗余电源； | 台 | 4 |
| 9 | 应用负载均衡器 | 1、千兆电口≥8个，万兆光口≥8个，万兆多模光模块≥4个，冗余电源,含国密和商密芯片加速卡；采用国产化CPU和操作系统； 2、吞吐量≥40G；并发连接数大于等于2500万，新建连接数≥20万；支持多存储介质，可同时支持EMMC卡≥4GB，SSD硬盘≥512GB； 3、支持TCP、HTTP、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、SIP、RADIUS、自定义等健康监测方式；支持源IP、目的IP、SIP、HASH、http cookie、http header、URL、Radius、DHCP、SSL ID、自定义等多种会话保持方式； 4、单一设备可同时支持包括链路负载均衡、服务器负载均衡、全局负载均衡的功能；（需提供设备功能界面截图证明) 5、支持TCP、HTTP、HTTPS、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、SIP、RADIUS、自定义健康监测脚本等健康监测方式； 6、支持轮询、加权轮询、最小流量、最小连接、加权最小连接、加权最佳性能、每源IP轮询、源地址源端口哈希散列等服务器负载均衡调度算法； 7、支持主备真实服务组功能，在缺省实服务组内的成员均不可用时，启用备份实服务组对外提供服务，无需单独配置真实服务的优先级； 8、支持手动方式的双机配置一致性检查功能，在日常运维中，可以通过手动的方式检查双机之间的配置是否保持一致，并且显示上次检查时间以及检查结果是否为一致，在不一致的情况下，可以详细展示出双机在地址池、NAT、真实服务、真实服务组、虚拟服务、健康检查、会话保持、HTTP内容调度、SSL策略等模块的配置差异化对比；（提供设备功能界面截图并加盖原厂商公章） 9、支持一键跳转至命令行CLI功能，支持通过设备WEBUI页面，一键跳转至命令行CLI界面，无需通过远程管理工具登录命令行CLI界面； | 台 | 4 |
| **三** | **安全设备** |  |  |  |
| 1 | 万兆防火墙（专网区） | 1、机框式插卡设备，主控≥2，支持N+1冗余备份，业务槽位数≥3，具有良好的扩展性；支持扩容业务功能板卡数量，实现整机业务性能叠加，满配整机业务吞吐量≥1080Gbps，最大并发连接数≥2亿，每秒新建连接数≥1440万，支持扩展万兆接口≥96个，100G接口≥8或40G接口≥16； 2、本次实配国产化主控，电源模块≥2块，主控≥2，风扇模块≥2个，千兆电口≥4个，万兆光口接口≥16个，万兆多模光模块≥16个，业务吞吐量≥80Gbps； 3、支持丰富的VPN特性，如 IPSec VPN、SSL VPN、L2TP VPN、MPLS VPN、GRE等；支持国用商用密码对数据进行加密。 4、支持L2～L7的全面安全防御，包括防火墙、NAT、LB、IPS、AV、ACG、VPN等； 5、支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护；支持SYN Flood、ICMP Flood、UDP Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； 6、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作； 7、支持主机和业务模块统一IP管理和统一的配置界面，支持统一网管功能，支持紧耦合部署； 8、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙； 9、支持同一块板卡、跨板卡的链路聚合，支持多台物理设备完成虚拟化之后，不同物理设备的物理端口进行聚合； 10、支持自动生成安全策略，统一运维管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率（提供和统一管理平台的对接的承诺函）； 11、支持 802、1Qbg、DCB 等；支持 VXLAN 等 Overlay 主流标准技术；支持 Openflow1、3 协议标准；具备SDN 及专网区特性； 12、支持设备在线状态监测机制，实现对包括主控引擎，背板，芯片和存储等关键元器件进行检测； | 台 | 2 |
| 2 | 万兆防火墙（互联网区） | 1、具备千兆电口≥8个，千兆光口≥2个，万兆光口≥4个，千兆多模光模块≥2个，万兆多模光模块≥4个，支持扩展槽≥1个，冗余交流电源； 2、整机吞吐量≥10Gbps，每秒新建连接数≥23万，最大并发连接数≥500万，含5年病毒、IPS、应用识别、URL特征库及升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持一体化安全策略配置，可以通过一条策略实现五元组、应用、服务、时间、长连接、IP限速、IPS、AV、URL过滤、行为审计等功能配置,简化用户管理； 5、具备防火墙、应用识别、链路负载均衡、IPV6、VPN等功能，支持扩展URL过滤、IPS、AV、IP信誉库、区域特征库、威胁情报等功能； 6、支持IPv4／IPv6 NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT66地址转换；支持多种应用协议，如FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT的NAT ALG功能； 7、支持通过命令查询数据流在设备上的处理流程，可以看到报文经过设备的处理流程，包含不限于入接口、会话创建、NAT匹配结果、路由查询结果、安全策略匹配、出接口等以及数据包在设备中最终的处理结果等信息，便于进行故障排查； 8、支持在一台物理设备上划分出≥30个并发相互独立的虚拟系统，并可以查看虚拟系统的CPU和内存利用率、新建、并发和吞吐等信息，并支持单独重启一个虚拟系统，其他虚拟系统以及公共系统的业务不受影响。； | 台 | 2 |
| 3 | 千兆防火墙 | 1、具备千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个，支持扩展槽≥2个，冗余交流电源； 2、整机吞吐量≥4Gbps，每秒新建连接数≥9万，最大并发连接数≥390万，含5年病毒、IPS、应用识别、URL特征库及升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持一体化安全策略配置，可以通过一条策略实现五元组、应用、服务、时间、长连接、IP限速、IPS、AV、URL过滤、行为审计等功能配置,简化用户管理； 5、具备防火墙、应用识别、链路负载均衡、IPV6、VPN等功能，支持扩展URL过滤、IPS、AV、IP信誉库、区域特征库、威胁情报等功能； 6、支持IPv4／IPv6 NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT66地址转换；支持多种应用协议，如FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT的NAT ALG功能； 7、支持通过命令查询数据流在设备上的处理流程，可以看到报文经过设备的处理流程，包含不限于入接口、会话创建、NAT匹配结果、路由查询结果、安全策略匹配、出接口等以及数据包在设备中最终的处理结果等信息，便于进行故障排查； 8、支持在一台物理设备上划分出≥30个并发相互独立的虚拟系统，并可以查看虚拟系统的CPU和内存利用率、新建、并发和吞吐等信息，并支持单独重启一个虚拟系统，其他虚拟系统以及公共系统的业务不受影响； | 台 | 2 |
| 4 | WEB应用防火墙 | 1、具备千兆电口≥8个，千兆光口≥2个，千兆多模光模块≥2个，支持扩展槽≥2个，冗余交流电源； 2、整机吞吐≥9Gbps，HTTP吞吐≥1Gbps，最大并发连接数≥300万，每秒新建连接数≥3万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持透明模式、代理模式、网关模式和旁路模式，且模式之间切换不需要重启设备或者检测引擎，可多种模式共同运营；  5、支持对Web流量的镜像阻断功能，并且支持指定阻断报文发送接口； 6、支持通过虚拟化技术实现将一台物理设备虚拟成≥30个并发虚拟WAF；并且可对每个虚拟WAF使用的资源进行限制，例如会话数、新建速率、吞吐量、CPU及内存使用率； 7、支持流量自学习，可以自动学习IP、域名、端口等信息，将学习到的服务添加到防护策略；  8、支持内置规则弱口令防护功能，支持自定义表单模式对弱口令登录表单进行识别和校验； 9、支持通过设定前置参数名、正则表达式、参数范围等匹配特定的主机名、URL，对容易被篡改或者篡改会产生重大风险的参数名的取值进行限定； | 台 | 2 |
| 5 | 漏洞扫描 | 1、 配置千兆电口≥8个，万兆光口≥2个，万兆多模光模块≥2个，USB接口≥2个，冗余交流电源； 2、 采用国产化CPU和操作系统，内存≥16GB，硬盘存储≥1T； 3、采取旁路部署模式，支持分级部署与集中管理，IP可达即可进行检测，无需改变网络架构，基于WEB进行管理； 4、支持资产盘点，可下发资产盘点任务导出专用资产盘点报告，支持自定义资产指纹； 5、支持漏洞检测及弱口令的识别能力，支持高危漏洞的专项检测，支持对高危漏洞的自动化验证，可生成专业安全检测报告； 6、产品具备边界完整性检测能力，可检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为； 7、产品具备违规内联检测能力，可检测出随身WI-FI、BYOD设备、向日葵； 8、产品具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测； 9、支持配置主机漏洞模板，内置漏洞库数量≥300000种，可兼容CVE、CNNVD、CNVD等主流标准，同时支持自定义扫描漏洞库，漏洞库类型可基于操作系统、数据库、中间件等进行分类； 10、产品需集成安全漏洞验证知识库（提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库）以及手工漏洞验证工具集； 11、产品具备高危预警能力，能够对最新发布的高危漏洞及时更新推送平台，对最新高危漏洞预警进行立即检测； 12、产品可以联动统一运维管理平台实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验；（提供和统一管理平台的对接的承诺函） | 台 | 1 |
| 6 | 入侵防御（专网区） | 1、具备千兆电口≥4个，千兆光口≥4个，千兆多模光模块≥4个，支持扩展SSD硬盘；冗余交流电源； 2、整机网络层吞吐≥4Gbps，IPS吞吐≥600Mbps，最大并发连接数≥200万，每秒新建连接数≥2万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持丰富的路由协议，例如静态路由、策略路由（路由前策略、路由后策略、本地报文发包策略）、RIP、OSPF、ISIS、BGP； 5、内置丰富的IPS特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量≥9000条； 6、入侵防御日志支持聚合发送，聚合条件包括源IP聚合、目的IP聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器≥10个； 7、支持将设备划分成多台虚拟的IPS分给不同的租户使用，租户管理各自策略，相互隔离，虚拟IPS数量≥30个并发； 8、支持对邮件协议进行访问管控，包括对SMTP命令（至少包含EXPN、MAIL、RCPT、SAML、SEND、SOML、TURN、VRFY等命令）、邮件大小、邮件主题、收发件人、以及文件类型进行控制； 9、支持跨物理设备的端口聚合，扩展带宽节省链路资源以及方便部署。 | 台 | 2 |
| 7 | 入侵防御（互联网区） | 1、具备千兆电口≥8个，千兆光口≥6个，千兆多模光模块≥6个，支持扩展SSD硬盘；冗余交流电源； 2、整机网络层吞吐≥9Gbps，IPS吞吐≥1Gbps，最大并发连接数≥300万，每秒新建连接数≥3万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持丰富的路由协议，例如静态路由、策略路由（路由前策略、路由后策略、本地报文发包策略）、RIP、OSPF、ISIS、BGP； 5、内置丰富的IPS特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量≥9000条; 6、入侵防御日志支持聚合发送，聚合条件包括源IP聚合、目的IP聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器≥10个； 7、支持将设备划分成多台虚拟的IPS分给不同的租户使用，租户管理各自策略，相互隔离，虚拟IPS数量≥30并发； 8、支持对邮件协议进行访问管控，包括对SMTP命令（至少包含EXPN、MAIL、RCPT、SAML、SEND、SOML、TURN、VRFY等命令）、邮件大小、邮件主题、收发件人、以及文件类型进行控制； 9、支持跨物理设备的端口聚合，扩展带宽节省链路资源以及方便部署。 | 台 | 2 |
| 8 | 网络安全审计 | 1、具备千兆电口≥8个，千兆光口≥2个，千兆多模光模块≥2个；冗余交流电源； 2、网络层吞吐量≥9Gbps，并发连接数≥200万，每秒新建连接数≥1.5万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理； 5、支持策略路由协议、动态路由协议，包括RIP、OSPF、ISIS、BGP；  7、支持自定义应用：支持通过IP+端口方式自定义网络应用及基于深度检测方式（应用特征）自定义网络应用； 8、支持应用会话审计，包括IP、端口、应用类型、会话包数、字节数、时间等的审计； 9、支持用户时长分析：支持分析用户总时长、总流量以及用户具体应用的时长和流量，可通过饼状图或柱状图展示； 10、支持记录portal认证账号的最后一次的登陆时间，方便管理员清理长期未使用的账号，避免设备策略冗余； | 台 | 2 |
| 9 | 堡垒机（互联网） | 1、千兆电口≥6个，千兆光口≥4个，千兆多模光模块≥4个，USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥1T；内存≥16G，管理点数≥60个；采用国产化CPU和操作系统； 2、支持SSHv1、SSHv2、TELNET等字符协议；支持RDP、VNC等图形协议；支持FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议； 3、支持运维用户对未授权的资源、资源账号申请授权工单，授权工单通过后可运维申请的资源； 4、支持通过协议前置机进行协议扩展，可支持扩展 KVM、Vmware等虚拟平台上的资源、数据库、B/S应用、C/S 应用等； 5、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，对动作流配置即可实现单点登录和审计接入； 6、提供运维、监控、回放屏幕水印功能，并可根据实际需求场景选择开启范围，运维本地无法篡改水印内容，震慑不规范的运维和审计行为，提升运维过程数据安全性； 7、支持 linux 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息，支持手动添加、删除、编辑、检索资源，支持变更默认运维端口；支持资源的动态图表管理，系统可自动生成动态全景视图，支持资源的分类统计，提供资源分类可视化页面； 8、支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT 、 Xshell 、 Putty 、 WinSCP 、 FileZilla 、xftp、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯； 9、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期；用户登录认证方式支持静态口令认证、手机动态令牌认证、Usbkey（国密数字证书）认证、吉大正元网关认证、华测Ukey认证、北京CA认证、信安CA认证、中安云科认证、503CA认证、AD/LDAP认证、Radius认证、短信认证、指纹识别等认证方式，并支持组合形成双因子认证； | 台 | 1 |
| 10 | 堡垒机（专网区） | 1、千兆电口≥6个，千兆光口≥4个，千兆多模光模块≥4个，USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥4T；内存≥16G，冗余交流电源；管理点数≥300个；采用国产化CPU和操作系统； 2、支持SSHv1、SSHv2、TELNET等字符协议；支持RDP、VNC等图形协议；支持FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议； 3、支持运维用户对未授权的资源、资源账号申请授权工单，授权工单通过后可运维申请的资源； 4、支持通过协议前置机进行协议扩展，可支持扩展 KVM、Vmware等虚拟平台上的资源、数据库、B/S应用、C/S 应用等； 5、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，对动作流配置即可实现单点登录和审计接入； 6、提供运维、监控、回放屏幕水印功能，并可根据实际需求场景选择开启范围，运维本地无法篡改水印内容，震慑不规范的运维和审计行为，提升运维过程数据安全性； 7、支持 linux 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息，支持手动添加、删除、编辑、检索资源，支持变更默认运维端口；支持资源的动态图表管理，系统可自动生成动态全景视图，支持资源的分类统计，提供资源分类可视化页面； 8、支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT 、 Xshell 、 Putty 、 WinSCP 、 FileZilla 、xftp、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯； 9、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期；用户登录认证方式支持静态口令认证、手机动态令牌认证、Usbkey（国密数字证书）认证、吉大正元网关认证、华测Ukey认证、北京CA认证、信安CA认证、中安云科认证、503CA认证、AD/LDAP认证、Radius认证、短信认证、指纹识别等认证方式，并支持组合形成双因子认证； | 台 | 1 |
| 11 | 数据库审计 | 1、业务接口：千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个，USB host接口≥2个，Console口≥1个，扩展槽≥2个，采用国产化CPU和操作系统； 2、SQL流量吞吐≥500Mb/秒，业务流量吞吐≥2Gb/秒，SQL语句吞吐≥20000条/秒，数据库实例数≥10； 3、CPU ≥8核，内存≥16G，硬盘≥2T； 4、支持Oracle、SQLserver、DB2、MySQL、Cache、Sybase、Informix、Teradata、PostgreSQL、Hive、MongoDB、HANA、HBASE、ES、CacheWeb、Solr、HDFS、Redis、EsgynDB、Tibero、SSDB等国际主流数据库；支持DM7、神通、人大金仓、南大通用、湖南上容、浪潮KDB、HWMPP、翰高等国产数据库； 5、支持扫描网络中的开放的服务，自动发现网络中存在的数据库系统，能够能够对这些数据库系统进行安全审计； 6、支持自动发现敏感数据如身份证号、银行账号等信息，便于进行用户权限控制，支持将扫描到的敏感表信息进行导出； 7、支持自学习功能，能够基于自学习机制的模型策略，审计未授权的客户端ip地址，未授权的表操作访问、未授权的数据库用户、未授权的特权操作等; 8、支持跨包的SQL语句进行拼接功能，能够完整解析与审计超长SQL语句（≥1460字节），屏蔽逃逸审计通道； 9、支持查看数据库系统的监视器信息、软件版本信息、补丁信息、表空间情况、会话信息、回退信息、权限等信息来判断数据库系统运行是否正常，保证数据库系统的可用性和响应能力； 10、支持扫描以下系统风险：数据库表级访问的安全性设置，SGA共享池分配私有空间的限制，每次调用读入的数据块数目的限制，一次会话读入的数据块总数的限制，是否启用资源限制等数据库系统配置等； | 台 | 2 |
| 12 | 服务密码机 | 采用国产化CPU和操作系统； 网络接口≥2个千兆电口，不支持扩展，其他接口≥6个USB口、≥2个COM口 性能参数： SM4算法加解密：≥540Mbps；SM2密钥对≥12000对/秒；SM2加密：≥2600次/秒；SM2解密：≥3400次/秒；SM2签名：≥12000次/秒；SM2验签：≥4300次/秒；SM3杂凑运算：≥520Mbps | 台 | 1 |
| 13 | 签名验签服务器 | 采用国产化CPU和操作系统； 提供基于数字证书的数据签名与验证、加解密服务，支持SM2等签名算法； 硬件规格:≥2个100/1000M自适应网口。主要性能参数: SM2签名≥1600次/秒。 | 台 | 1 |
| 14 | 安全隔离与信息交换系统 | 1、业务接口：（内机）千兆电口≥6个，万兆光口≥2个，万兆多模光模块≥2个，满足接口基础要求上扩展槽≥1个；（外机）千兆电口≥6个，万兆光口≥2个，万兆多模光模块≥2个，满足接口基础要求上扩展槽≥1个；冗余交流电源；采用国产化CPU和操作系统； 2、网络层吞吐量≥1.5Gbps；并发连接数≥40W；视频并发路数≥450路D1视频；数据库同步速率≥3000条/秒； 3、带液晶屏，液晶菜单可显示内外网机IP地址、CPU使用率和内存使用率等整机信息； 4、支持远程ftp、远程SMB、远程NFS、远程sftp、本地ftp、本地sftp、客户端方式进文件交换同步; 5、可查看系统每日CPU、内存、负载使用率以及会话连接数变化情况，提供至少近7日变化图查询； 6、提供API管理接口，API管理接口支持访问密钥数字签名验证，确保访问请求身份认证以及数据未被非法篡改；接口支持授权管理，可针对访问请求进行访问权限控制； 7、支持移动网络接入，搭配外置4G/5G硬件模块实现电信、移动、联通移动网络拨号接入； 8、多机热备支持自定义服务监测对象，可对关键IP、服务进行监测，发现服务连接异常，及时进行主备切换； 9、支持批量数据表智能匹配配置，可自动匹配表名、字段相同的数据表建立同步关系，满足大批量数据表同步场景下的快速配置需求; 10、支持SMTP\POP3协议，支持发件人、收件人地址过滤；支持主题关键字、正文关键字、附件文件名、附件正文过滤；支持文件类型过滤；病毒扫描; | 台 | 2 |
| 15 | 态势感知平台 | 1.千兆电口≥4个，万兆光口≥2个，万兆多模光模块≥2个，USB接口≥4个，扩展槽≥2个；硬盘≥8T；CPU≥8核；冗余交流电源； 2.单台最大流量处理能力≥1G；采用国产化CPU和操作系统； 3.支持5G协议解析和威胁检测，可查看5G威胁的日志统计数据，包括攻击级别分布，攻击名称Top5和手机号Top5统计图以及5G威胁事件的列表；支持查看5G威胁日志的攻击列表展示，包括攻击者、受害者、所属机构、攻击类型、攻击名称、关键字、发现时间； 4.支持从外连地址和受害者的维度展示外连威胁，查看单条外连威胁详情时将外连攻击行为信息进行展示； 5.支持自定义攻击事件分析模型，包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置38种及以上安全事件分析模型，如冰蝎webshell通信、利用Sqlmap上传webshell、Acunetix安全工具扫描、APPSCAN工具扫描等； 6.支持自定义配置的分析条件，包括：URL、HTTP方法、HTTP域名、HTTP状态码、DNS解析域名、TLS指纹、TLS版本、SSH服务端协议版本、SSH客户端协议版本、文件类型、文件哈希值、恶意文件家族、SMTP发件人等； 7.支持时间轴溯源分析，以时间轴的形式展示攻击者在入侵全过程中各个入侵时间节点中的攻击目标、攻击次数、攻击手段以及攻击阶段，同时提供各攻击手段安全处置建议； 8.支持基于ATT&CK框架的模型分析； 9.支持多层溯源功能，开启多层溯源后，默认展示两层溯源信息，攻击手段在展示图中消失，右侧展示攻击手段TOP5及描述信息； 10.支持攻击关系分析，以攻击者视角展示针对每个攻击目标所采用的攻击手段的攻击关系视图，同时展示攻击事件的攻击手段TOP统计，以及每种攻击手段的描述说明，并支持下钻； 11.支持攻击详情分析，基于受害者、目的端口、时间段、攻击手段、攻击类型、攻击级别、攻击名称等七个维度进行网络攻击日志检索，可查看本次攻击事件涉及的网络攻击的详细情况，以及下载原始攻击数据包； 12.支持AI判真功能，存在多个攻击手段的攻击事件显示为AI判真事件，AI判真事件存在AI判真标识； 13.支持AI自动处置功能，支持攻击事件按照昨天的处置历史信息进行处置，攻击事件被盖上相应的处置标签；历史处置记录按时间轴形式显示处置时间、设备信息或备注信息；处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息； 14.支持展示安全风险评级、攻击事件类型TOP5、攻击事件级别分布、外部攻击类型TOP5、外部攻击者TOP5等信息，支持在全球地图上展示攻击者到受害者的攻击视图，展示主要攻击类型，展示资产受害者TOP5，支持展示攻击者数量、受害者数量、攻击总数、已沦陷资产数量和活跃攻击源TOP5等信息，同时支持实时滚动攻击日志，每条攻击至少包括攻击者、受害者、攻击类型、攻击等级、攻击名称和时间。 | 台 | 1 |
| 16 | 态势感知探针 | 1、千兆电口≥4个，万兆光口≥2个，万兆多模光模块≥2个，USB接口≥4个，扩展槽≥2个；硬盘≥4TB；冗余交流电源； 2、流量采集能力≥1G； 3、支持设置标准模式、增强模式、深度模式、专家模式等流量分析策略，可设置不同策略类型，包括攻击策略、审计策略、采样等级、高级设置； 4、支持多种漏洞攻击检测，至少包括：信息泄露、文件包含、文件上传、目录遍历、跨站脚本、代码注入、反序列化、命令执行、未授权访问、模板注入、文件下载、XML外部实体注入、越权访问、XPATH注入、SQL注入、跨站请求伪造、服务端请求伪造、逻辑绕过、缓冲区溢出、DoS攻击、其它漏洞、可以的User-Agent等； 5、支持对5G协议解析和威胁检测，可以通过平台查看5G威胁的日志统计数据，包括攻击级别分布，攻击名称Top5和手机号Top5 统计图以及5G威胁事件的列表； 6、支持基于机器学习的提取攻击者真实访问的URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者IP、攻击者URL、访问行为的原始报文等； 7、支持多种恶意软件检测，至少包括：勒索病毒、挖矿软件、僵尸网络、shellcode、蠕虫病毒、木马病毒、黑客工具、Rootkit、BootKit、恶意文件投放等； 8、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS等协议的隧道通信； 9、可自定义弱口令规则，低、中、高三种密码规则，结合预定义弱口令字典，对弱口令威胁的检测更准确;界面可展示检测的弱口令威胁日志，有关键字的会展示关键字。 | 套 | 1 |
| 17 | 杀毒软件 | 1、产品以纯软件交付，本次配置≥100点服务器资源且提供不少于三年的软件升级服务，包含管理控制中心软件及终端客户端软件，其中管理控制中心支持云化或者本地化管理平台交付； 2、Windows桌面支持：Windows XP（32位）、Windows 7、Windows 8/8.1、Windows 10等；Windows服务器：Windows Server 2003（32位）/2008/2012/2016/2019等，支持国产化操作系统； 3、单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器和国产化操作系统的客户端软件； 4、采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； 5、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量。 | 套 | 1 |
| 18 | 日志审计（互联网区） | 1、 千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个；USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥2T+mSATA 128G；内存≥16G； 2、 日志处理能力≥2000条/秒，日志存储能力≥1.7亿条/天，审计授权≥60；  3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、 支持日志查询，可根据接收时间、源目IP、严重级别等信息进行查询，可针对查询到的日志结果进行导出；支持普通模式查询，并且可以根据查询的条件进行模板保存，以便于后续使用；支持专家模式查询，可通过编写表达式进行对日志信息进行更加全面的查询，并且可以根据查询的条件进行模板保存，以便于后续使用； 5、 审计策略：内置审计分析策略，包含：DDoS攻击、Webshell攻击、XSS跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换root用户、系统重启、硬件故障等。 6、 采集方式：支持基于TCP和UDP的syslog协议、kafka、snmp trap、ftp、smb、wmi、sftp等采集协议格式的模式解析； 7、 采集策略：支持被采设备无需安装代理；支持同一资产多种采集策略；支持从不同类型系统采集到的日志进行标准化分析，将不同格式日志映射到固定的解析字段中，标准化处理后的字段细粒度≥90； 8、支持将采集到的日志进行过滤，可以根据自身业务需求定制过滤策略，做到将无关日志进行丢弃；支持将采集到的日志进行归并，可以根据自身业务需求定制归并策略，做到在一定条件下将接收到的相同日志归并为一条，并且显示该日志的接收次数，使日志信息简明易看；  9、 支持三权分立原则，可设置安全管理员、安全审计员、系统管理员等角色。通过赋予不同角色不同的权限，以达到配置权力、审计权力、运维权力的相互制约； | 台 | 1 |
| 19 | 日志审计（专网区） | 1、 千兆电口≥8个，千兆光口≥4个，千兆多模光模块≥4个；USB接口≥2个，Console口≥1个，扩展槽≥2个；硬盘≥4T+mSATA 128G；内存≥32G；冗余交流电源； 2、 日志处理能力≥3000条/秒，日志存储能力≥2.5亿条/天，审计授权≥110； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、 支持日志查询，可根据接收时间、源目IP、严重级别等信息进行查询，可针对查询到的日志结果进行导出；支持普通模式查询，并且可以根据查询的条件进行模板保存，以便于后续使用；支持专家模式查询，可通过编写表达式进行对日志信息进行更加全面的查询，并且可以根据查询的条件进行模板保存，以便于后续使用； 5、 审计策略：内置审计分析策略，包含：DDoS攻击、Webshell攻击、XSS跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换root用户、系统重启、硬件故障等。 6、 采集方式：支持基于TCP和UDP的syslog协议、kafka、snmp trap、ftp、smb、wmi、sftp等采集协议格式的模式解析； 7、 采集策略：支持被采设备无需安装代理；支持同一资产多种采集策略；支持从不同类型系统采集到的日志进行标准化分析，将不同格式日志映射到固定的解析字段中，标准化处理后的字段细粒度≥90； 8、支持将采集到的日志进行过滤，可以根据自身业务需求定制过滤策略，做到将无关日志进行丢弃；支持将采集到的日志进行归并，可以根据自身业务需求定制归并策略，做到在一定条件下将接收到的相同日志归并为一条，并且显示该日志的接收次数，使日志信息简明易看；  9、 支持三权分立原则，可设置安全管理员、安全审计员、系统管理员等角色。通过赋予不同角色不同的权限，以达到配置权力、审计权力、运维权力的相互制约； | 台 | 1 |
| 20 | 抗DDOS攻击设备 | 1、业务接口：千兆电口≥8个，千兆光口≥2个，千兆多模光模块≥2个，万兆光口≥4个，万兆多模光模块≥4个，冗余交流电源； 2、网络层吞吐量≥10Gbps，最大并发连接数≥800w，最大每秒新建连接数(HTTP) ≥12w； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持针对网络层、应用层分别设置清洗策略，包括不限于：SYN Flood、UDP Flood、ICMP Flood、DNS Query/Reply Flood、HTTP Flood、HTTPS Flood; 5、支持针对不同防护对象，分别设置不同的异常流量清洗参数、算法等； 6、支持抓包溯源功能，支持抓取清洗前、清洗后、清洗丢弃的报文进行分析；针对抓包文件可以进行攻击源IP溯源，并提取攻击报文中的攻击特征下发到清洗设备过滤； 7、支持连接数新建及并发限制功能，可对TCP等协议设置阈值及周期； 8、支持会话数限制，可对源地址/目的地址做会话数限制，设置维度包括：服务类型（可定义服务类型）、用户、新建速率、总会话数、每IP会话数、生效时间等； 9、支持针对协议头中各字段配置自定义策略，字段包括但不限于：Method、Cookie、Host、Referer、Request URI、Verion、User-Agent等； 10、为保障异常流量安全清洗和业务系统稳定运行，抗DDOS攻击设备可以被统一运维管理平台监控。（提供和统一管理平台的对接承诺函并加盖抗DDOS攻击设备厂商公章） | 台 | 2 |
| 21 | 互联网VPN接入设备 | 1、具备千兆电口≥8个，千兆光口≥2个，万兆光口≥4个，万兆多模光模块≥4个，冗余交流电源；采用国产化CPU和操作系统； 2、整机吞吐量≥9Gbps，每秒新建连接数≥10万，最大并发连接数≥500万； VPN加密性能：IPsec VPN吞吐量≥1Gbps，IPsec VPN隧道数≥2000个；SSL VPN吞吐量≥1Gbps，SSL VPN并发用户数≥3000个，总用户数不限； 3、支持集群：双机模式下，支持主备两台设备采用同一套IP地址，简化配置，节约公网地址； 4、内网攻击防护：基于内网用户流量模型和会话连接、新建连接的异常行为识别攻击，有效防护内网病毒传播、僵尸网络、木马等安全威胁； 5、支持静态路由、RIP v1/2、OSPF、策略路由等。支持MPLS VPN；支持MPLS静态标签转发；支持LDP协议，支持LDP引入OSPF路由、BGP路由、RIP路由、静态路由、ISIS路由、GUARD 路由，支持环路检测；支持LDP邻居，MPLS转发表查看；支持SVC方式、CCC方式、MARTINI方式、VPLS方式的L2VPN；支持MPLS TE； 6、提供设备的可靠性试验证明，(设备厂商提供证明材料)； 7、支持自动和手动备份，能够保存5个以上的文件，支持整机配置文件在线回滚功能，未变化的业务连续不中断； 8、登录公告：支持VPN登录前和登录后公告信息显示，登录前后公告内容可配置多条； 9、产品需要支持国密算法，具备商用密码产品认证证书；（提供证书复印件并加盖原厂商公章） | 台 | 2 |
| **四** | **机房设备** |  |  |  |
| 1 | 微模块机柜 | 1.外形尺寸：服务器机柜规格（W\*D\*H）：600mm\*2000mm，前门为玻璃门，后门为钢板门。 2.机柜涂覆层应表面光洁、色泽均匀、无流挂、无露底；金属件无毛刺、无锈蚀。机柜门板、侧板平整，无扭曲、无变形、也不明显抖动；门板开孔均匀。 3.机柜由主框架、顶板、内嵌底板、前后门、侧横梁、矩形管、内立柱和固定层板组成。其中主框架、内立柱的、侧横梁的材料厚度不小于2.0mm，后门、顶板、和侧板的材料厚度不小于1.2mm。 4.为方便设备安装及维护，门板为可拆卸式结构，门的开合转动灵活、锁定可靠、施工安装和维护方便。 5.为了保障用电安全，要求机柜内各带电回路对地（或柜体）绝缘电阻不小于100MΩ。 6.机柜耐电压强度：要求机柜内各带电回路以及两个非电气连接的带电回路之间，应能承受2500V，50HZ正弦试验电压1min，并不出现击穿或者飞弧现象，漏电流不超过1mA。 7.机柜附件：每个机柜含接地组件（接地线6mm²）、左后各1条垂直理线板、19英寸安装接地铜排（3\*15mm²）、运输脚轮、LED灯管+行程开关。 | 台 | 15 |
| 2 | 列头机柜 | 1.外形尺寸：服务器机柜规格（W\*D\*H）：600mm\*2000mm，前门为玻璃门，后门为钢板门。 2.要求配电柜主路开关不小于2\*160A/3P，防雷模块不低于C级防雷模块。 3.要求配电柜支路开关不小于且不少于两路24\*32A/1P，支路监测参数要求包含：支路额定电流、实际电流，支路负载百分比，支路开关状态。 | 台 | 1 |
| 3 | 智慧机柜侧板 | 机柜配件,侧板,1400mm(D)\*2000mm(H) | 套 | 2 |
| 4 | 机柜锁具 | 机柜配件,电子锁\*2,刷卡一体,带钥匙和IC卡1张,包含配套线缆 | 套 | 16 |
| 5 | 智慧机柜M型走线槽 | 顶部M型走线槽,600mm(W)\*300(D)\*150(H),强弱分离,带隔板 | 套 | 20 |
| 6 | 快开盲板 | 1U免工具安装盲板,快开方式,钣金 | 个 | 150 |
| 7 | 水平理线器 | 水平理线器,482\*44\*80MM | 条 | 15 |
| 8 | 智慧机柜轻载托盘 | 100kg承重开孔托盘,19",适配600宽1100深以上机柜-微模块 | 块 | 15 |
| 9 | L型托架 | 50kg承重L型托架1副(2只,左右各1) | 对 | 15 |
| 10 | 智慧机柜专用普通PDU | 1.每个机柜标配2条PDU，为设备A/B路供电使用。两条PDU应为同一规格，互为备份。 2.交流PUD采用黑色涂层，外壳选用优质型材或钢板，应具备强度高，坚固耐用，抗压性能、装配性能、耐蚀性能和装饰性能良好，表面喷涂效果好，工艺先进，纹路平整，美观大方等特点。 3.机柜PDU输出接口具有GB标准类型，10A的插座不少于16个，16A的插座不少于4个。 | 个 | 30 |
| 11 | 列间空调 | 1.总冷量≥35kw，显冷量≥35kw，风量≥6100m³/h，加湿量≥1.5kg/h，加热量≥4kW，水平送风模式； 2.可以实现常温情况下最低10%的IT负载（即制冷量的10%）稳定除湿量功能，降低高湿环境下数据中心低载运行的IT设备结露风险。 3.精密空调室内机采用高效工业用直流变频压缩机，可实现10%～100%宽冷量输出； 4.为了相应国家节能节耗政策，要求空调全年能效比应大于3.5； 5.具有LCD的真彩触摸显示屏，可以显示设备的运行模式与状态，并可设定设备参数，实现良好的人机交互 6.机组具备联动与群控功能，群控采用高速、灵活的CAN通讯协议，同一区域可以将≥32套机组进行统一控制管理； 7.室内风机：要求采用高效后倾离心式EC风机。 8.要求空调机组设备符合GB19413相关标准。 | 套 | 4 |
| 12 | 盲柜 | 规格：≥300\*1400\*2000mm(W\*D\*H),黑色 | 套 | 4 |
| 13 | 机柜监控主机 | 1.通道动环监控主机，ARM架构，Linux系统；双交流供电，支持多路温湿度、烟雾、漏水、端门、天窗、空调、UPS、配电单元、消防、声光告警器等的监测和/或控制。 | 台 | 1 |
| 14 | 微动环监控平台系统软件 | 1.安装在服务器或PC端，通过有线连接，后台软件展示模块机房温湿度、通道门禁状态、能耗等动环实时监控数据； 2.为了保证机房健康运行，要求平台软件具有告警管理功能，可实现实时告警查看、待处理告警统计、历史告警查看以及可自定义设置告警阀值和告警等级等功能，且可自主远程邮件和短信发送相关负责人，可及时发现告警，并能及时处理，保障机房健康安全运行； 3.要求在本软件可实时查看行级空调运行状态和配电模块以及UPS电压、电流、电功率、负载百分比以及电池容量等运行状态。 | 套 | 1 |
| 15 | 电话,短信告警模块 | 可通过电话或短信的形式对告警内容进行通知。 | 个 | 1 |
| 16 | 手机APP客户端接入接口 | 手机APP客户端接入接口,须能够支持安卓4.0及以上智能设备-微模块 | 套 | 1 |
| 17 | 温湿度传感器 | 磁吸式温湿度传感器,测温范围:-20℃-70℃,测湿范围:0%-100%RH,12V接线端子供电 | 个 | 4 |
| 18 | 烟雾探测器 | 机柜专用光电烟感探测器,磁吸式,工作电压:DC12V | 个 | 4 |
| 19 | 声光报警器 | 磁吸式电子蜂鸣器,声压105db,声频1500±500Hz,60mA,DC12V | 个 | 1 |
| 20 | 水浸探测绳 | 非定位式水浸探测绳,配合非定位水浸传感器使用(5米) | 根 | 4 |
| 21 | 智慧模块化通道电源控制箱 | 一体柜控制箱,350W12V开关电源,含照明灯,背景灯电源,2U | 套 | 1 |
| 22 | 机房强弱电设备安装及配套辅材 | 机房强弱电设备安装费及配套辅材费，包括网线、电缆等。 | 套 | 1 |
| **五** | **其它设备** |  |  |  |
| 1 | 指挥中心大屏 | 面积≥20m²； 点间距：1.2mm； 封装方式： COB； 亮度：≥800cd 分辨率：≥4K; | m² | 20 |
| 2 | 可视化综合管控一体机 | CPU：≥16核，≥2.0GHz； 内存：≥16GB; 硬盘：≥2TB； 显卡：显存≥4GB； 可实现对视频拼接处理的集中统一管理，控制各屏的输出内容。设备带有话筒、投屏器、控制台等外设。 另需包含管理软件。 | 台 | 1 |
| 3 | 拼接屏处理器 | 1.1920x1080p@60Hz信号，处理平台内部不进行任何抽帧，满帧输出至显示设备。支持场景轮循， 2.信号支持：4096x2160@60hz，4096x2160@30hz，3840x2160@30hz，3840x2400@30hz，2560x1600@60hz分辨率，向下兼容其他分辨率， 3.支持在输出通道上打开高达16个高清信号窗口，且每个窗口支持大小任意调整，图层顺序调整。支持多组屏硬回显，可同时将4组不同大屏的整体显示画面通过回显板卡传输至显示器，进行高清显示，回显帧率可达60hz。可以在控制端实时回显大屏整体画面。 4.配置双控制卡，双电源 | 个 | 1 |

**软件服务类**

| **序号** | **名称** | **主要性能（技术）指标** | **单位** | **数量** |
| --- | --- | --- | --- | --- |
| **一** | **系统软件** |  |  |  |
| （一） | 操作系统 | 具备文件管理、设备管理、日志管理、服务管理、进程和监控管理、网络管理、资源管理、软件包管理、硬件管理等基本功能，提供语言支持工具、文件共享服务工具、集成开发平台等常用工具，支持KVM、Docker虚拟化技术。 硬件支持‌：支持 X86 和 ARM 架构的处理器，如海光、鲲鹏 、飞腾等；符合国家信创要求； 授权方式：按节点授权。 | 套 | 55 |
| （二） | 数据库 | 符合国家信创要求；具备数据存储、访问控制、身份鉴别、安全审计和数据备份恢复等功能。产品部署在服务器，以后台服务形式运行，数据库管理员及用户在管理主机上通过图形化管理工具或命令行工具，可实现对数据对象（表、视图、约束、索引、触发器、存储过程等）的配置管理；开发人员可通过标准化数据库访问接口，开发基于数据库的应用系统和软件产品。 授权方式：按节点授权。 | 套 | 25 |
| （三） | 中间件 | 用于为上层应用提供运行环境，实现对上层应用的部署和动态管理。主要功能包括Web容器、EJB容器、数据源服务、集群管理等。产品可部署在信创服务器，以后台服务形式运行，用户通过管理控制台或者命令行工具完成上层应用的部署、启动、停止等操作。符合国家信创要求。 授权方式：按节点授权。 | 套 | 30 |
| **二** | **应用软件** |  |  |  |
| （一） | 项目管理系统 | 项目管理系统可完整覆盖项目管理的各个过程，帮助企业建立研发管理体系，提高企业管理流程的稳健性和项目管理成熟度，大大提升项目成功的概率。 本系统主要提供标准化模板（如敏捷、瀑布模型），支持项目拆解子任务，设置任务的优先级和依赖性关系，制定预算并关联任务成本，设置交付物和验收标准。 | 套 | 1 |
| （二） | 统一运维管理系统 | 统一运维平台可以将本项目涉及的网络和安全设备进行集中管理，对网内安全设备、网络设备、服务器等进行实时运行状态监控，分析研判各类安全事件，通过访问控制策略的配置，实现大规模部署环境下灵活、便捷的安全策略管理，阻止敏感信息外泄和非核心业务的滥用；同时还可以联动现网扫描设备实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验，确保网络的整体安全。设备含设备管理、网络监控、攻击监控、系统管理、通用图标等≥65种大屏展示组件，可以以折线图、环形图、柱状图等形式进行展示。 | 套 | 1 |
| （三） | 统一门户 | 统一门户平台集成了本项目的所有应用（除智慧共享药房、针灸数智服务平台以外），实现一键登录，支持his集成，用户同步认证。 系统主要功能包括身份认证、身份管理、统一权限、单点登录、信息共享、应用管理与注册、门户管理、页面管理、部件管理导航管理、内容管理等。 | 套 | 1 |
| **三** | **应用系统开发软件** |  |  |  |
| （一） | 智慧共享中药房 | 结合当前中医药数字化的要求和医院的实际情况，为了更好地提高院内管理数字化水平尤其是中医药场景的管理，发挥区域医共体中心医院的带头作用，方案主要从饮片调剂、煎煮等全流程可追溯范畴入手，满足中药房的数字化管理，将日常繁琐的工序进行优化，通过互联网、物联网等适宜的数字化手段的应用，在整体质量管理、高效管理等方面提高医院的整体数字化管理水平。 系统主要功能包括区县共享中账套管理，煎煮审核，煎药流程管理，流程预警管理，煎药业务查询和汇总，人员绩效管理，药房药库日常管理等。 | 套 | 1 |
| （二） | 数据整合交换与数据集成服务系统 | 数据整合交换与数据集成服务系统是一个集数据采集、治理与监控管理为一体的综合性数据处理平台，旨在为医疗业务和管理提供全面、精准、高效的数据支撑。通过构建灵活多样的数据采集机制，包括批量、定时及实时采集，系统可快速整合来自多源业务系统的数据资源，确保数据的及时性与完整性。通过系统建设打通市县乡村各级数据共享和数据交换通道，为分级诊疗体系做好必要的基础准备。 系统主要功能包括大数据基础底座，分布式存储系统，批流一体化计算引擎，医疗数据存储计算，数据采集子系统，数据管理子系统，数据分类分级子系统，数据开放子系统，数据处理子系统，AI数据中台等。 | 套 | 1 |
| （三） | 中医针灸数智服务系统 | 以针灸领域权威著作以及大规模临床数据为数据源，构建针灸大模型、针灸知识图谱，并将时空针灸融入其中，形成时空针灸知识图谱，从疾病和症状等多个维度构建针灸处方推荐算法，搭建针对中医针灸诊疗综合服务平台，以针灸大模型技术为特色，支撑针灸辅助诊断、处方审核、诊疗方案推荐、知识学习及查询、患者随访等功能。 系统主要功能包括针灸知识体系，针灸知识管理，针灸处方诊断与治疗决策智能体，针灸处方分析，临床应用服务，针灸疗效评价，针灸患者管理与服务等。 | 套 | 1 |
| （四） | 中医诊疗服务质控系统 | 通过对海量已完成的中医诊断案例进行流程与结果分析，系统能够识别出共性的诊疗模式与潜在的优化点，为推动中医诊疗流程的标准化提供数据支持。系统将对历史诊疗数据中的关键指标进行统计分析与趋势预警，帮助管理者识别系统性风险，从而在宏观层面指导医疗质量的持续改进，保障患者长远利益。 系统主要功能包括中医诊疗行为规范监控，医疗服务过程追踪与回溯，多模态疗效评价，中医医生实时监控管理分布图，AI质控，人工质控，门诊病历质控，病案首页质控，住院病历质控，多维度质控结果分析，分类搜索引擎等。 | 套 | 1 |
| （五） | 中医药业务智能监管驾驶舱 | 中医药业务智能监管驾驶舱整合全市医疗机构中医诊疗与运营数据，主要面向区域卫生监管部门和医疗机构管理者，以“数据赋能中医药管理，智慧驱动业务决策”为核心目标，构建覆盖中医药服务全流程的智能监管体系，通过整合区域中医药机构运营数据、疾病监测数据及患者行为数据并进行可视化呈现，管理者能够迅速掌握区域医疗资源的分布、利用情况，以及医疗服务的质量与效率，从而实现精准监管、科学决策，推动区域医疗服务的持续优化与升级。 系统主要功能包括自定义报表分析工具，数据填报，仪表板可视化编辑，组件配置，数据分析报表，业务运营主题分析，患者就诊行为分析，中医健康画像数据应用等。 | 套 | 1 |
| （六） | 中西医结合数智类脑系统 | 中西医结合数智类脑系统结合前沿AI模型搭建理念及技术，深度融合中医“理法方药”理论与西医诊疗理论，构建“中医为主、西医辅助”的智能诊断体系，通过多源数据获取与处理模块解析中西医临床文献、病历及标准规范，经文本分类、清洗、去重等加工形成高质量训练语料，基于渐进式预训练策略与指令微调、强化学习等技术，将中医经典理论与西医病理指标转化为模型算法，实现“中医辨证—西医验证”的协同推理；借助知识图谱构建中西医结合知识体系，通过混合检索与生成技术关联舌象脉象、检验指标等多模态数据，形成动态诊疗路径，既能基于中医辨证思维生成治法治则，又能调用西医检查数据辅助验证用药安全性，为中医智能辅助诊断服务系统、中医诊疗服务质控系统等应用系统提供模型能力支撑。 系统主要功能包括中西医结合基础大模型，临床智能对话大模型，中西医知识检索增强生成技术，中西医临床诊疗大模型，大模型应用服务系统，分布式程序数据搜索引擎，多云平台API资源批量化采集引擎，西医临床标准word文档处理套件，临床数据处理、非结构化pdf文件解析等。 | 套 | 1 |
| 四 | 其他 |  |  |  |
| （一） | 网络租赁 | 提供5年网络带宽 | 年 | 5 |
| （二） | 数据治理服务 | 语料库建设 采集计划 历史数据采集范围 数据采集标准编制 技术准备 历史数据采集 增量数据同步范围 实时数据采集 数据预处理 采集数据质量验证 问题反馈与处理 数据汇聚 ODS层模型设计和存储 数据质控规则配置 实时质量监控 定期质量评估 问题处理与改进 数据落标开发 数据标准规范 数据接口规范 | 项 | 1 |