**睢宁县精神病医院智慧医疗系统服务项目**

**更正（澄清）内容（一）**

**一、以下为澄清或者修改的内容**

****1、原招标文件**第六章《采购需求》“四、建设清单及技术需求”中**

**1.5硬件部分技术参数需求**

**1.5.1防火墙**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 基本规格 | 标准机架式设备，国产化硬件平台，配置8个10/100/1000M Base-TX；2个万兆口，16G内存，4T硬盘，吞吐量≧10G，并发连接数≧400万，默认支持IPSec VPN和SSL VPN模块（含200个并发用户授权）；开通AV模块，IPS模块；三年IPS特征库升级，三年AV病毒库升级，三年硬件质保。 |
| 工作模式 | 支持国产操作系统，可在Web界面完成系统备份、系统恢复、指定启动系统操作 |
| 模版式配置管理 | ▲支持系统主要防护功能的统一化模版设置，模版分为高、中、低三个级别，对应不同防护强度，可通过Web界面单击选择切换及扩展通过设备面板外置按键一键切换（提供面板外置按键照片证明） |
| 网络适应性 | 支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路、支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。 |
| 要求支持将任意接口数据完全镜像到设备自身的其他接口，用于抓包分析 |
| 网络访问控制 | 支持策略命中数显示，并支持通过安全策略命中数范围查询 |
| IPSEC VPN | 支持DMVPN，在增加一个新的分支节点网关后，不需要在中心网关更改任何配置，且支持路由推送，实现spoke to spoke互通，不必建立额外隧道 |
| 支持多NAT环境下的多用户L2TP认证加密接入 |
| 入侵防御 | 支持基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略 |
| 支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析 |
| 防病毒 | 支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略 |
| 支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性 |
| 加密算法 | ▲TLS加密算法支持选择TLS1.0、TLS1.1、TLS1.2和TLS1.3，并支持国密TLS；(要求提供具有第三方检测机构报告) |
| 抗拒绝服务攻击 | 支持主流ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD攻击防护，采用专业高效攻击防护算法，非采用简单的阈值进行攻击防护 |
| 统一认证管理 | 支持对入网终端的系统版本和运行进程进行准入检查 |
| 支持显示详细的用户在线信息，包括用户名称、真实姓名、所属组、认证源、接入方式、认证方式、登录IP/MAC、在线时间、登录时间和可对其进行相关操作 |
| 漏洞扫描 | 支持包括后门、服务探测、文件共享、Windows系统补丁、认证等主动式扫描、支持周，月定时漏洞扫描设置,及一次性漏洞扫描设置、支持同多台漏扫服务器联动同步，并根据安全策略对漏扫服务器高等级漏洞进行处理 |
| 资产风险评估 | 支持全方位、多角度的风险趋势呈现。支持以曲线图形的方式呈现全网和核心资产的风险变化趋势。支持以柱状堆叠图形（按安全事件分类）的方式呈现全网和核心资产安全事件的趋势统计，每类安全事件是否参与统计可调节。支持以处理动作（如阻断/放行）的趋势统计 |
| 安全日志 | 支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器 |
| 审计中心 | 可支持内置或外置数据存储介质；支持根据存储时间或硬盘使用率发送告警邮件；支持智能优化存储空间，保证近期数据的可追溯性，且必须支持手动删除保存时间较长的数据 |
| 升级维护 | ▲支持自动创建和手动创建两种方式创建快照，数量不少于16个，自动创建可根据客户的预设置时间，每周或每月自动创建系统快照；（提供功能截图） |
| 高可用性 | 自动同步、心跳接口多级（≥2级）物理备份 |
| ▲资质要求 | 厂商为相关部门网络安全威胁和漏洞信息共享平台-通用网络安全产品漏洞库三星级支持单位 |
| 厂商具备相关测评中心颁发的信息安全服务资质（安全工程类三级） |
| 产品通过相关检验中心的电磁兼容性、浪涌（冲击）抗扰度、雷击型式测试； |

**1.5.2日志审计**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架设备；设备配置≥6个千兆电口，≥4个千兆光口,，≥3个扩展槽； |
| ▲性能要求 | 使用国产化操作系统和CPU，内存不小于16G，硬盘不小于2T，设备开通不小于50个资源管理数授权，此次提供三年硬件质保。 |
| ▲硬件架构 | 要求采用设备硬件状态监测技术对网络资产进行安全监控，提供权威第三方机构出具的证明复印件并加盖原厂公章 |
| 管理范围 | 能对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 操作系统 | 无需安装任何其他软件和组件，用户只需要安装审计中心即可实现对日志的采集、分析； |
| 日志分析 | 支持对日志提供在线/离线地图定位、支持源IP与目的IP分布走向的视网膜图展示、支持事件拓扑分析用于描述整个事件的访问关系及过程、支持多维分析； |
| 部署方式 | 支持单级部署，无需安装任何其他软件和组件，用户只需要安装审计中心即可实现对日志的采集、分析；支持级联部署，两个审计中心之间可以进行级联，形成大规模统一审计。 |
| 资产管理 | 要求系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；要求拓扑视图可以显示被审计资产之间的网络连接关系。 |
| 日志采集 | 要求采用先进的设备统一控制技术，可针对设备的日志进行统一的采集控制，有证明材料。 |
| 日志传输和存储转发 | 系统需支持加密压缩方式转发，定时转发。 |
| 日志综合显示 | 系统可以提供传统的线形图、饼图、条状图等多种方式来显示信息。 |
| 产品证书 | 产品具有网络关键设备和网络安全专用产品安全认证证书。 |
| ▲厂商资质 | 为了保证信息安全产品的售后服务，要求厂商通过商品售后服务评价体系认证，具有售后服务认证证书（五星级），提供相关证书复印件加盖厂商公章。 |

**1.5.3堡垒机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架设备；设备配置≥6个千兆电口，≥4个千兆光口，≥3个扩展槽； |
| ▲性能要求 | 使用国产化操作系统和CPU，内存不小于8G，硬盘不小于4T，设备开通不小于50个被管理资源数授权，此次提供三年硬件质保。 |
| 部署方式 | 支持NAT地址映射部署，通过映射后的IP地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境。 |
| 分权分域 | 支持管理员帐号设置双因认证、IP/MAC限制，提升帐号安全性。 |
| 资源管理 | 支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问。 |
| 帐号托管 | 支持数据库协议自动改密，改密类型支持：Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE、Mssql(2005,2008,2012)以及主流的国产数据库。 |
| 技术能力 | 采用网络安全设备命令行的解析技术，对设备进行运维管理，提供第三方权威机构出具的相关证明材料。 |
| 运维方式 | 支持windows终端调用国产化应用发布工具运维，支持国产化终端调用应用发布工具运维。 |
| 字符、文件传输协议审计 | 支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放。 |
| ▲审计查询 | 审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS\_C\_5601\_1987,Shift\_JIS,Window-874)，由审计管理员自主选择（产品具有CNAS、CMA、ilac-MRA认证的权威检测机构出具的检测报告复印件）。 |
| IPV4/IPV6 | 支持在IPV4与IPV6网络环境下部署。 |
| 产品证书 | 产品具有网络安全专用产品安全检测证书。 |
| ▲厂商资质 | 为保障产品成熟度，要求设备厂商具有CMMI5证书。 |

**1.5.4杀毒软件**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 杀毒软件 | 1.支持查看资产的安全态势，并进行统一任务下发、策略配置，对资产进行统一管理； 2.支持采集、展示多种日志，包括防护日志、操作日志、运维日志，并支持一键导出。  3.支持对终端进行详细信息展示，包括网络信息、环境信息等。并支持远程关闭、重启主机；  4.支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据。 5.配置：一个管理中心，服务器端杀毒50点，三年病毒库升级。 |

**1.5.5数据库审计**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架设备；设备配置≥6个千兆电口，≥4个千兆光口，≥3个扩展槽； |
| ▲性能要求 | 使用国产化操作系统和CPU，内存不小于16G，硬盘不小于4T，设备开通不小于10个数据库授权，此次提供三年硬件质保。 |
| 产品部署 | 支持对部署在vmware、KVM、Xen等虚拟化环境中的数据库进行审计，审计系统可虚拟化部署。 |
| 数据审计 | 支持对针对数据库的SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 |
| 数据审计 | 支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨杉、虚谷、OceanBase、AnalyticDB MySql 、AnalyticDB PostgreSQL、RDS MySql、RDS PostgreSQL等数据库的审计。 |
| 审计能力与效果 | 数据库审计策略支持频次统计，某一操作在周期时间内达到设定的次数阀值后可以进行单独记录和展示，周期事件和次数可按需配置。 |
| 业务关联审计 | 支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯。 |
| ▲统一管理 | 采用设备控制技术，可对设备进行统一安全管理，提供第三方权威机构证明材料复印件，加盖原厂公章。 |
| 智能发现 | 支持基于网络流量的资产发现功能，能够发现数据库表和资源账号，其中数据库表的自动发现支持表名、数据库名、发现次数和发现日期，资源账号自动发现支持在线天数、首次发现日期、末次发现日期，提供截图证明并盖原厂公章。 |
| 多样审计访问 | 支持审计访问数据库的时间，源/目的IP，源/目的端口，源/目的mac，资源账号，数据库名，规则名称，表名，命令，SQL语句、级别，响应时间、错误码，影响行数，连接方式，客户端程序名，模式名，客户端用户，SQL执行结果。 |
| ▲厂商资质 | 为了保证信息安全产品的售后服务，要求厂商通过相关商品售后服务评价体系认证，具有售后服务认证证书（五星级）和《数据安全服务能力-数据安全“评估”能力二级》，提供相关证书复印件加盖厂商公章。 |

**1.5.6 VPN网关**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架式设备，国产化硬件平台，设备配置1个RJ-45 Console口，8个10/100/1000M自适应电口，4个千兆SFP插槽，2个网络接口扩展槽位，2个USB口，交流单电源；设备配置硬件加密卡，支持国家商用密码算法SM2、SM3、SM4，产品具有国家密码管理局发布的商用密码产品认证证书，此次提供三年硬件保修和基础型技术支持服务。 |
| ▲性能要求 | IPSec/SSL国密加解密吞吐不小于300Mbps，推荐并发用户数不小于1000，整机吞吐不小于5Gbps；此次提供不小于50点SSL VPN授权。 |
| 基本功能： | 客户端支持龙芯、兆芯、飞腾、鲲鹏等国产化平台，支持中标麒麟，银河麒麟，普华、深度（deepin）、优麒麟、UOS统信操作系统、中科方德等国产化操作系统客户端 |
| 多系统引导 | 产品支持多系统引导，即系统A、系统B和备份系统，可在管理员界面直接配置启动顺序，支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且配置文件分别支持加密导入导出，备份系统用于应急恢复。 |
| SSL VPN | 支持设置SSL代理模式，可选择用户以VPN 接口IP、客户端源地址、或为用户分配独立虚拟IP 模式，来访问应用便于对用户访问行为进行审计溯源。 |
| 用户认证 | 支持IPSec、SSL 、PPTP、L2TP VPN的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部VPN类型接入，无需分别购买不同类型VPN接入授权。 |
| IPv6 | IPSec VPN支持网关、单臂部署模式，IPSec VPN支持透明、路由、冗余等网络接入方式。 |
| ▲支持终端认证功能， | 包含硬件特征码、IP、MAC、主机绑定，特征码信息无需用户手动设置输入可自动生成，支持自定义用户绑定终端数量。支持硬件特征码批量导入导出。（产品具有相关部门出具的检测报告复印件） |
| IPSec VPN | 支持IPSec手动隧道，手动输入密钥参数，无需协商，可以满足IPSec VPN跨越单向光闸传输加密要求。 |
| 访问控制 | 采用滤除网络攻击流量的方法。 |
| 产品证书 | 产品具有网络安全专用产品安全检测证书。 |
| ▲厂商资质 | 为保障信息系统建设和服务能力，要求设备厂商具有信息系统建设和服务能力等级证书和《数据安全服务能力评定资格证书》证书，提供相关证书复印件加盖厂商公章。 |

**1.5.7 备份一体机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 国产化平台 | 支持基于国产化平台（国产CPU架构或国产操作系统）部署备份存储服务器； |
| 硬件要求 | 配置：CPU:≥2颗国产处理器，单颗主频≥2.6GHz，单颗物理核数≥32核，≥内存：128GB，16个DIMM插槽，最大支持2T 内存；系统盘：≥2\*480GB SSD 数据盘：≥6\*8TB SATA 阵列卡：≥2GB缓存RAID卡（含掉电保护） 网络接口：≥4\*1GE 电口，≥4\*10GE 光口（含多模光纤模块）；扩展槽位：≥3个可用PCIe插槽；国产，非OEM品牌，备份软件授权≥14TB； |
| ▲虚拟化和云操作系统保护 | 支持国产虚拟化或云平台的备份恢复，包括但不限于KVM、FusionCompute、FusionCloud（Huawei Cloud Stack）、H3C CAS、OpenStack、CNware、RHV、易捷行云EasyStack、腾讯云TStack、ZStack、品高云等虚拟化平台或云平台的备份恢复（提供不少于6家虚拟化或云平台厂商的产品兼容性互认证证书复印件，并加盖公章） |
| 数据库保护基本功能要求 | 支持国产主流的数据备份恢复，包括但不限于达梦（DM）、人大金仓（Kingbase）、南大通用（GBase）、GBase 8a MPP、神舟通用（ShenTong）、优炫（UXDB）、瀚高（Highgo）、虚谷、openGauss、Vastbase（海量）、SG-RDB-PG、GoldenDB、HotDB、TDSQL-PG、AntDB（亚信）、FusionDB、MogDB、TBase、GaussDB（DWS）和 GaussDB（for openGauss）等数据库。（提供不少于6家上述国产数据库产品的兼容性互认证证书复印件，并加盖公章） |
| ▲针对Oracle的redo log和archive log提供连续日志备份方式，实现RPO达到秒级的安全保护要求。（提供产品功能截图） |
| ▲支持华为GaussDB，原 GaussDB(for openGauss)非侵入式备份，无需在GaussDB节点安装Agent，即可实现备份恢复。同时兼容 Roach 与 TPOPS 方案，Roach 支持完全备份、增量备份、累积增量备份，TPOPS 支持完全备份、增量备份、日志备份和任意时间点恢复。支持将GaussDB实例7、恢复至原集群和同构异集群。（提供产品功能截图） |
| 数据重删复制冗余基本功能要求 | 支持固定块、变长块的数据重删技术，在创建重删存储空间时，需要提供变长和固定长度的块大小选择。 |
| 支持源端重删和目标端重删技术。 |
| 支持重删池的状态检查，显示各重删池的指纹库大小、已用空间等信息。支持重删池的空间使用图表，显示空间使用和节省率趋势。 |
| 支持指纹库异常修复和优化，包括指纹库重建和重分片、碎片自动整理机制等，保障重删备份恢复性能。 |
| 厂商资质 | 厂商提供投标产品必须具有IPV6认证。（提供原厂盖章的证书复印件） |
| ▲厂商具有相关部门颁发的《源代码安全审计证书》（提供原厂盖章的证书复印件） |
| 质保服务 | 三年原厂硬件质保服务，三年原厂软件质保服务； |

**1.5.8前置服务器**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 前置服务器 | 国产化CPU:≥2颗，单颗主频≥2.4GHz，单颗物理核数≥16核，内存：≥128GB，内存；系统盘：≥2\*480GB SSD 数据盘：≥3\*8TB SATA； 阵列卡：≥2GB缓存RAID卡（含掉电保护）； 网络接口：≥4\*1GE 电口，≥2\*10GE 光口（含多模光纤模块） |

**1.5.9业务超融合**

|  |  |
| --- | --- |
| 名称 | 技术要求 |
| 云资源要求 | 1、 国产化CPU,单节点提供两颗C86 CPU,主频不少于2.5GHz，核数不少于64核，内存不少于512GB, 不少于960GB SATA SSD系统盘， 不少于3.84TB NVMe SSD缓存盘，不少于32TB 数据盘，RAID卡（带4GB缓存），冗余电源。为保证软硬件兼容性，以及后期售后服务一致性，要求硬件与云软件为同一品牌。 |
| 软件授权 | 1、每台服务器提供不少于2颗CPU授权的计算虚拟化、存储虚拟化、网络虚拟化、云计算管理平台授权.  2、为保障国产化替代进程，云软件需兼容国产C86、ARM架构处理器。  3、提供3年软件升级服务。 |
| 功能要求 | 支持健康巡检功能，用于快速查看系统健康情况 |
| 统一运维要求：针对云资源整体软硬件故障问题，提供统一的可视的监控管理中心，可视化实时监控中心从硬件可靠性、系统可靠性、服务可靠性三大层面进行实时监控、分层展示，运维人员可以直观查看集群的整体运行情况，可以快速诊断集群的健康状态，同时支持对无需关注的检测异常启用屏蔽功能，启用屏蔽功能的检测异常将不会上报显示。 |
| ▲资源扩容要求：可以依据资源的使用情况，云资源支持按需选择扩容计算存储融合型节点、计算虚拟化型节点、存储虚拟化型节点，满足后期按业务对资源的需求进行灵活扩容，并节省采购成本要求；（需提供产品功能截图） |
| 内置迁移工具：云资源管理平台内置在线p2v、v2v迁移工具，支持业界主流的操作系统、公有云平台、虚拟化平台。包括但不限于VMware、华为、Hyper-V等平台的迁移功能，提升被迁移业务平台的普适性、降低业务上云的难度，降低运维工作量 |
| ▲投资保障需求：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（提供具有CNAS及CMA认证的第三方权威机构出具的测试报告） |
| 支持一键切换展示大屏功能，直观展示虚拟化资源池的健康度、告警、资源使用情况等，同时展示内容支持用户自定义 |
| ▲容量故障预测：支持资源容量预测服务，管理平台自动化实现数据检索预测，提供用户易用的数据预测服务，服务支持呈现实时的CPU、内存和 存储容量资源使用数据信息展示，并给出基于AI机器学习算法预测分析得到的预警时间点的提示，帮助用户做好资源扩容、成本预算等，提升业务可靠性。（需提供产品功能截图） |
| 自动部署要求：管理平台对于新上线节点设备可基于链路层协议、被管理节点自动发现，自动分配其IP地址，降低管理难度 |
| 支持安装在通用的x86、ARM架构服务器，支持现有市场上主要国内外操作系统，包括Windows、CentOS、Fedora、RedHat、SUSE、Ubuntu、FreeBSD、中标红旗、中标麒麟、中标普华、深度、一铭、凝思等 |
| 运维管理要求：支持虚拟机桌面预览功能，无需登录虚拟机即可在虚拟化管理平台上看到虚拟机当前桌面的状态。 |
| 采用分布式的软件定义存储架构，在通用服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务 |
| ▲投资保障需求：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。（提供具有CNAS及CMA认证的第三方权威机构出具的测试报告） |
| ▲在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。（需提供产品功能截图） |
| 质保服务 | 原厂质保三年，提供原厂三年质保函并加盖公章。 |

**1.5.10 PACS存储**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲国产操作系统 | 所投存储底层操作系统采用欧拉、统信、麒麟等国产操作系统，使用成熟稳定的国产品牌自主研发CPU，并且CPU通过国家保密科技测评中心最新的安全可靠测评，提供投标产品使用CPU型号、主频等证明材料以及中国信息安全测评中心官网安全可靠测评结果截图并加盖投标人公章。 |
| ▲硬件配置 | 本次配置≥3个存储节点，单节点配置：CPU:≥2颗国产处理器，单颗主频：≥2.6GHz，单颗物理核数：≥32核，内存：≥8\*32GB DDR4 内存，硬盘：≥2\*480GB SSD 硬盘，≥1\*3.2TB NVME SSD 硬盘，≥12\*8TB SATA 硬盘；网口：≥4\*GE网口，≥4\*25GE 网口（含万兆光模块），软件：配置对应可得容量的存储软件授权； |
| 分布式架构 | 采用全对称分布式架构，无独立元数据节点，随着存储节点数的增加，分布式存储性能和容量也随着近线性增长，扩容过程中业务不中断； |
| 具备大规模横向扩展能力，单集群规模最大可扩展至≥4096节点，支持横向扩展能力，新增节点带来的集群性能提升不低于单节点性能的80％； |
| 支持在线缩容和扩容；支持存储软件在线升级，升级操作均不影响前端业务的连续性； |
| CIFS协议 | 支持创建目录、删除目录、创建文件、删除文件、拷贝文件、查看文件、修改文件等； |
| 业务连续能力 | 支持Failover,支持在接入节点发生故障时业务不中断； |
| ▲并行客户端功能 | 为大幅提升医生客户端阅片性能，降低访问时延，所投存储产品支持并行客户端功能，支持MPI-IO，兼容OpenMPI， MPICH2，提供具备CNAS或CMA资质的第三方权威评测机构签字盖章的测试报告复印件并加盖设备厂商原厂公章； |
| 文件访问控制 | 支持对文件多种访问控制，只读、只读写、完成控制（读/写/删除/创建）、禁止（无权限访问）权限； |
| ▲目录文件数要求 | 单个目录支持的文件数不低于3000万，单个文件最大支持1PB，提供具备CMA和CNAS认证资质且隶属国家部委的认证机构的认证报告； |
| ▲数据完整性校验 | 支持数据完整性校验功能(DIF)，数据静默错误可自动校验并修复。提供具备CMA和CNAS认证资质且隶属国家部委的认证机构的认证报告； |
| 质保服务 | 原厂质保三年，提供原厂三年质保函并加盖公章。 |

**1.5.11数据中心交换机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 转发性能 | 交换容量≥4.8Tbps，以官网所列最低参数为准；包转发率≥2000Mpps，以官网所列最低参数为准； |
| 硬件规格 | 高度≤1U，固定接口交换机，电源1+1备份，风扇模块3+1备份； |
| ▲CPU | 国产芯片，自主可控，提供第三方测试报告； |
| 特性 | 4、设备缓存≥32M，支持前后、后前风道； |
| 5、支持M-LAG或vPC或DRNI等跨机箱链路捆绑技术; |
| 6、支持BFD3.3ms检测间隔 |
| 端口配置要求 | 48个10GE光端口数量，6个100GE 光接口； |
| 模块 | 配置20个万兆多模光模块； |
| 质保服务 | 原厂质保三年。 |

**1.5.12千兆交换机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 端口 | 24个10/100/1000M以太网电口，4个千兆 SFP接口； |
| 性能 | 交换容量：≥672Gbps/6.72Tbps；包转发率：126Mpps； |
| CPU | 国产芯片，自主可控，提供权威第三方测试报告; |
| MAC地址 | ≥32K，预留可支持到64K的能力; |
| 质保服务 | 原厂三年质保。 |

**1.5.13核心交换机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 自主可控 | 采用国产芯片，自主可控，提供权威第三方测试报告; |
| ▲可靠性 | 主控上的业务端口，在主控复位时，依然可以正常工作； |
| 性能 | 包转发率：≥100/460 Tbps，交换容量：≥76800 Mpps； |
| ▲配置要求 | 主控板槽位数：≥2； |
| 业务板槽位数：≥6； |
| 支持颗粒化电源，整机电源槽位数≥6； |
| 为了部署的方便性，POE电源模块须内置于机框内，不使用外置电源模块 |
| ▲实际配置 | 板卡：两个主控；网口：≥48个万兆光口，≥48个千兆电口；光模块：≥12个10GE多模光模块，≥1个10GE高速电缆-3m； |
| 电源 | 冗余电源 |
| 质保 | 原厂三年质保。 |

**1.5.14配套软件**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 软件 | 国产化操作系统、国产化数据库 |

**1.5.15运维服务**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 运维服务 | 一、运维服务要求  如需要，供应商需提供标准机柜，空间需满足招标设备安装需求。同时机柜所在机房环境需满足如下要求：  1、动环要求  ①两组UPS，切换时间小于10ms，UPS电源的供电时间不小于4小时；  ②一组油机，额定功率不低于500Kw；  ③两路市电；  ④机房内空调制冷量不低于320Kw；  2、驻场服务  提供2名专业技术人员（人员须为资深工程师），24小时\*365天驻场服务，驻场期间由采购人提供办公场所，驻场人员要自行提供工作工具，按照采购人的作息时间进行工作，接受管理和工作安排。  3、巡检要求  必须对维护范围内的信息化软硬件设备每4小时进行一次巡检且必须提供记录，及时发现系统存在的隐患与安全漏洞，提出书面报告，并与采购人共同解决存在的问题与隐患。每次巡检应提供书面巡检报告，并根据巡检报告及时与采购人进行交流，及时协调解决维护工作中的问题。  4、咨询服务  应对用户信息系统进行定期的维护管理和配置优化，确保用户整个信息系统运转的高效、稳定和安全，减少和避免系统性能瓶颈，杜绝信息系统安全事故，并且能根据用户需要，提供信息系统运行的合理化建议和方案。   1. 运维周期   供应商承诺对所投软硬件产品原厂质保三年，整体项目免费运维服务三年。  6、如甲方提供机柜、机房，供应商需无条件将设备迁移至指定位置。 |

**1.5.16配套链路**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 专线链路 | 供应商需提供2条不低于1G带宽的的专线链路。 |

**现更正为：**

**1.5硬件部分技术参数需求**

**1.5.1防火墙**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 基本规格 | ▲标准机架式设备，国产化硬件平台，配置8个10/100/1000M Base-TX；2个万兆口，16G内存，4T硬盘，吞吐量≧10G，并发连接数≧400万，默认支持IPSec VPN和SSL VPN模块（含200个并发用户授权）；开通AV模块，IPS模块；三年IPS特征库升级，三年AV病毒库升级，三年硬件质保。 |
| 工作模式 | 支持国产操作系统，可在Web界面完成系统备份、系统恢复、指定启动系统操作 |
| 模版式配置管理 | 支持系统主要防护功能的统一化模版设置，模版分为高、中、低三个级别，对应不同防护强度，可通过Web界面单击选择切换及扩展通过设备面板外置按键一键切换（提供面板外置按键照片证明） |
| 网络适应性 | 支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路、支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。 |
| 要求支持将任意接口数据完全镜像到设备自身的其他接口，用于抓包分析 |
| 网络访问控制 | 支持策略命中数显示，并支持通过安全策略命中数范围查询 |
| IPSEC VPN | 支持DMVPN，在增加一个新的分支节点网关后，不需要在中心网关更改任何配置，且支持路由推送，实现spoke to spoke互通，不必建立额外隧道 |
| 支持多NAT环境下的多用户L2TP认证加密接入 |
| 入侵防御 | 支持基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略 |
| 支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析 |
| 防病毒 | 支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略 |
| 支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性 |
| 加密算法 | TLS加密算法支持选择TLS1.2和TLS1.3，可支持国密TLS； |
| 抗拒绝服务攻击 | 支持主流ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD攻击防护，采用专业高效攻击防护算法，非采用简单的阈值进行攻击防护 |
| 统一认证管理 | 支持对入网终端的系统版本和运行进程进行准入检查 |
| 支持显示详细的用户在线信息，包括用户名称、真实姓名、所属组、认证源、接入方式、认证方式、登录IP/MAC、在线时间、登录时间和可对其进行相关操作 |
| 漏洞扫描 | 支持包括后门、服务探测、文件共享、Windows系统补丁、认证等主动式扫描、支持周，月定时漏洞扫描设置,及一次性漏洞扫描设置、支持同多台漏扫服务器联动同步，并根据安全策略对漏扫服务器高等级漏洞进行处理 |
| 资产风险评估 | 支持全方位、多角度的风险趋势呈现。支持以曲线图形的方式呈现全网和核心资产的风险变化趋势。支持以柱状堆叠图形（按安全事件分类）的方式呈现全网和核心资产安全事件的趋势统计，每类安全事件是否参与统计可调节。支持以处理动作（如阻断/放行）的趋势统计 |
| 安全日志 | 支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器 |
| 审计中心 | 可支持内置或外置数据存储介质；支持根据存储时间或硬盘使用率发送告警邮件；支持智能优化存储空间，保证近期数据的可追溯性，且必须支持手动删除保存时间较长的数据 |
| 升级维护 | ▲支持自动创建和手动创建两种方式创建快照，数量不少于16个，自动创建可根据客户的预设置时间，每周或每月自动创建系统快照； |
| 高可用性 | 自动同步、心跳接口多级（≥2级）物理备份 |

**1.5.2日志审计**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架设备；设备配置≥6个千兆电口，≥4个千兆光口,，≥3个扩展槽； |
| ▲性能要求 | 使用国产化操作系统和CPU，内存不小于16G，硬盘不小于2T，设备开通不小于50个资源管理数授权，此次提供三年硬件质保。 |
| 硬件架构 | 要求采用设备硬件状态监测技术对网络资产进行安全监控，提供权威第三方机构出具的证明复印件。 |
| 管理范围 | 能对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 操作系统 | 无需安装任何其他软件和组件，用户只需要安装审计中心即可实现对日志的采集、分析； |
| 日志分析 | 支持对日志提供在线/离线地图定位、支持源IP与目的IP分布走向的视网膜图展示、支持事件拓扑分析用于描述整个事件的访问关系及过程、支持多维分析； |
| 部署方式 | 支持单级部署，无需安装任何其他软件和组件，用户只需要安装审计中心即可实现对日志的采集、分析；支持级联部署，两个审计中心之间可以进行级联，形成大规模统一审计。 |
| 资产管理 | 要求系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；要求拓扑视图可以显示被审计资产之间的网络连接关系。 |
| 日志采集 | 要求采用先进的设备统一控制技术，可针对设备的日志进行统一的采集控制，有证明材料。 |
| 日志传输和存储转发 | 系统需支持加密压缩方式转发，定时转发。 |
| 日志综合显示 | 系统可以提供传统的线形图、饼图、条状图等多种方式来显示信息。 |
| 产品证书 | 产品具有网络关键设备和网络安全专用产品安全认证证书。 |

**1.5.3堡垒机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架设备；设备配置≥6个千兆电口，≥4个千兆光口，≥3个扩展槽； |
| ▲性能要求 | 使用国产化操作系统和CPU，内存不小于8G，硬盘不小于4T，设备开通不小于50个被管理资源数授权，此次提供三年硬件质保。 |
| 部署方式 | 支持NAT地址映射部署，通过映射后的IP地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境。 |
| 分权分域 | 支持管理员帐号设置双因认证、IP/MAC限制，提升帐号安全性。 |
| 资源管理 | 支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问。 |
| ▲帐号托管 | 支持数据库协议自动改密，改密类型支持：Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE、Mssql(2005,2008,2012)以及主流的国产数据库。 |
| 技术能力 | 采用网络安全设备命令行的解析技术，对设备进行运维管理，提供第三方权威机构出具的相关证明材料。 |
| 运维方式 | 支持windows终端调用国产化应用发布工具运维，支持国产化终端调用应用发布工具运维。 |
| 字符、文件传输协议审计 | 支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放。 |
| 审计查询 | 审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS\_C\_5601\_1987,Shift\_JIS,Window-874)，由审计管理员自主选择（产品具有CNAS、CMA、ilac-MRA认证的权威检测机构出具的检测报告复印件）。 |
| IPV4/IPV6 | 支持在IPV4与IPV6网络环境下部署。 |
| 产品证书 | 产品具有网络安全专用产品安全检测证书。 |

**1.5.4杀毒软件**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 杀毒软件 | 1.支持查看资产的安全态势，并进行统一任务下发、策略配置，对资产进行统一管理； 2.支持采集、展示多种日志，包括防护日志、操作日志、运维日志，并支持一键导出。  3.支持对终端进行详细信息展示，包括网络信息、环境信息等。并支持远程关闭、重启主机；  4.支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据。 5.配置：一个管理中心，服务器端杀毒50点，三年病毒库升级。 |

**1.5.5数据库审计**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架设备；设备配置≥6个千兆电口，≥4个千兆光口，≥3个扩展槽； |
| ▲性能要求 | 使用国产化操作系统和CPU，内存不小于16G，硬盘不小于4T，设备开通不小于10个数据库授权，此次提供三年硬件质保。 |
| 产品部署 | 支持对部署在vmware、KVM、Xen等虚拟化环境中的数据库进行审计，审计系统可虚拟化部署。 |
| 数据审计 | 支持对针对数据库的SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 |
| ▲数据审计 | 支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨杉、虚谷、OceanBase、AnalyticDB MySql 、AnalyticDB PostgreSQL、RDS MySql、RDS PostgreSQL等数据库的审计。 |
| 审计能力与效果 | 数据库审计策略支持频次统计，某一操作在周期时间内达到设定的次数阀值后可以进行单独记录和展示，周期事件和次数可按需配置。 |
| 业务关联审计 | 支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯。 |
| 统一管理 | 采用设备控制技术，可对设备进行统一安全管理。 |
| 智能发现 | 支持基于网络流量的资产发现功能，能够发现数据库表和资源账号，其中数据库表的自动发现支持表名、数据库名、发现次数和发现日期，资源账号自动发现支持在线天数、首次发现日期、末次发现日期，提供截图证明并盖原厂公章。 |
| 多样审计访问 | 支持审计访问数据库的时间，源/目的IP，源/目的端口，源/目的mac，资源账号，数据库名，规则名称，表名，命令，SQL语句、级别，响应时间、错误码，影响行数，连接方式，客户端程序名，模式名，客户端用户，SQL执行结果。 |

**1.5.6 VPN网关**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲硬件外观 | 1U标准机架式设备，国产化硬件平台，设备配置1个RJ-45 Console口，8个10/100/1000M自适应电口，4个千兆SFP插槽，2个网络接口扩展槽位，2个USB口，交流单电源；设备配置硬件加密卡，支持国家商用密码算法SM2、SM3、SM4，产品具有国家密码管理局发布的商用密码产品认证证书，此次提供三年硬件保修和基础型技术支持服务。 |
| ▲性能要求 | IPSec/SSL国密加解密吞吐不小于300Mbps，推荐并发用户数不小于1000，整机吞吐不小于5Gbps；此次提供不小于50点SSL VPN授权。 |
| ▲基本功能： | 客户端支持龙芯、兆芯、飞腾、鲲鹏等国产化平台，支持中标麒麟，银河麒麟，普华、深度（deepin）、优麒麟、UOS统信操作系统等国产化操作系统客户端。 |
| 多系统引导 | 产品支持多系统引导，即系统A、系统B和备份系统，可在管理员界面直接配置启动顺序，支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且配置文件分别支持加密导入导出，备份系统用于应急恢复。 |
| SSL VPN | 支持设置SSL代理模式，可选择用户以VPN 接口IP、客户端源地址、或为用户分配独立虚拟IP 模式，来访问应用便于对用户访问行为进行审计溯源。 |
| 用户认证 | 支持IPSec、SSL 、PPTP、L2TP VPN的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部VPN类型接入，无需分别购买不同类型VPN接入授权。 |
| IPv6 | IPSec VPN支持网关、单臂部署模式，IPSec VPN支持透明、路由、冗余等网络接入方式。 |
| 支持终端认证功能， | 包含硬件特征码、IP、MAC、主机绑定，特征码信息无需用户手动设置输入可自动生成，支持自定义用户绑定终端数量。支持硬件特征码批量导入导出。 |
| IPSec VPN | 支持IPSec手动隧道，手动输入密钥参数，无需协商，可以满足IPSec VPN跨越单向光闸传输加密要求。 |
| 访问控制 | 采用滤除网络攻击流量的方法。 |
| 产品证书 | 产品具有网络安全专用产品安全检测证书。 |

**1.5.7 备份一体机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 国产化平台 | 支持基于国产化平台（国产CPU架构或国产操作系统）部署备份存储服务器； |
| ▲硬件要求 | 配置：CPU:≥2颗国产处理器，单颗主频≥2.6GHz，单颗物理核数≥32核，≥内存：128GB，16个DIMM插槽，最大支持2T 内存；系统盘：≥2\*480GB SSD 数据盘：≥6\*8TB SATA 阵列卡：≥2GB缓存RAID卡（含掉电保护） 网络接口：≥4\*1GE 电口，≥4\*10GE 光口（含多模光纤模块）；扩展槽位：≥3个可用PCIe插槽；国产品牌，备份软件授权≥14TB； |
| ▲虚拟化和云操作系统保护 | 支持国产虚拟化或云平台的备份恢复，包括但不限于KVM、FusionCompute、FusionCloud（Huawei Cloud Stack）、H3C CAS、OpenStack、CNware、RHV、易捷行云EasyStack、腾讯云TStack、ZStack、品高云等虚拟化平台或云平台的备份恢复（提供不少于4家虚拟化或云平台厂商的产品兼容性互认证证书复印件，并加盖公章） |
| 数据库保护基本功能要求 | 支持国产主流的数据备份恢复，包括但不限于达梦（DM）、人大金仓（Kingbase）、南大通用（GBase）、GBase 8a MPP、神舟通用（ShenTong）、优炫（UXDB）、瀚高（Highgo）、虚谷、openGauss、Vastbase（海量）、SG-RDB-PG、GoldenDB、HotDB、TDSQL-PG、AntDB（亚信）、FusionDB、MogDB、TBase、GaussDB（DWS）和 GaussDB（for openGauss）等数据库。（提供不少于4家上述国产数据库产品的兼容性互认证证书复印件，并加盖公章） |
| ▲针对Oracle的redo log和archive log提供连续日志备份方式，实现RPO达到秒级的安全保护要求。（提供产品功能截图） |
| ▲支持GaussDB，原 GaussDB(for openGauss)非侵入式备份，无需在GaussDB节点安装Agent，即可实现备份恢复，Roach 支持完全备份、增量备份、累积增量备份，TPOPS 支持完全备份、增量备份、日志备份和任意时间点恢复。支持将GaussDB实例7、恢复至原集群和同构异集群。（提供产品功能截图） |
| 数据重删复制冗余基本功能要求 | 支持固定块、变长块的数据重删技术，在创建重删存储空间时，需要提供变长和固定长度的块大小选择。 |
| 支持源端重删和目标端重删技术。 |
| 支持重删池的状态检查，显示各重删池的指纹库大小、已用空间等信息。支持重删池的空间使用图表，显示空间使用和节省率趋势。 |
| 支持指纹库异常修复和优化，包括指纹库重建和重分片、碎片自动整理机制等，保障重删备份恢复性能。 |
| 质保服务 | 三年原厂硬件质保服务，三年原厂软件质保服务； |

**1.5.8前置服务器**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 前置服务器 | 国产化CPU:≥2颗，单颗主频≥2.0GHz，单颗物理核数≥16核，内存：≥128GB，内存；系统盘：≥2\*480GB SSD 数据盘：≥3\*8TB SATA； 阵列卡：≥2GB缓存RAID卡（含掉电保护）； 网络接口：≥4\*1GE 电口，≥2\*10GE 光口（含多模光纤模块） |

**1.5.9业务超融合**

|  |  |
| --- | --- |
| 名称 | 技术要求 |
| ▲云资源要求 | 1、 国产化CPU,单节点提供两颗C86 CPU,主频不少于2.3GHz，核数不少于32核，内存不少于512GB, 不少于960GB SATA SSD系统盘， 不少于3.84TB NVMe SSD缓存盘，不少于32TB 数据盘，RAID卡（带4GB缓存），冗余电源。为保证软硬件兼容性，以及后期售后服务一致性，要求硬件与云软件为同一品牌。 |
| ▲软件授权 | 1、每台服务器提供不少于2颗CPU授权的计算虚拟化、存储虚拟化、网络虚拟化、云计算管理平台授权.  2、为保障国产化替代进程，云软件需兼容国产C86、ARM架构处理器。  3、提供3年软件升级服务。 |
| 功能要求 | 支持健康巡检功能，用于快速查看系统健康情况 |
| 统一运维要求：针对云资源整体软硬件故障问题，提供统一的可视的监控管理中心，可视化实时监控中心从硬件可靠性、系统可靠性、服务可靠性三大层面进行实时监控、分层展示，运维人员可以直观查看集群的整体运行情况，可以快速诊断集群的健康状态，同时支持对无需关注的检测异常启用屏蔽功能，启用屏蔽功能的检测异常将不会上报显示。 |
| 资源扩容要求：可以依据资源的使用情况，进行计算资源、存储资源不中断业务扩容，支持分布式存储集群在线扩容节点、缩减节点，扩缩容后支持数据重均衡； |
| ▲内置迁移工具：云资源管理平台内置在线p2v、v2v迁移工具，支持业界主流的操作系统、公有云平台、虚拟化平台。包括但不限于VMware、华为、Hyper-V等平台的迁移功能，提升被迁移业务平台的普适性、降低业务上云的难度，降低运维工作量。 |
| 投资保障需求：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. |
| 支持切换展示大屏功能，直观展示虚拟化资源池的健康度、告警、资源使用情况等，同时展示内容支持用户自定义 |
| ▲容量故障预测：支持资源容量预测服务，管理平台自动化实现数据检索预测，提供用户易用的数据预测服务，服务支持呈现实时的CPU、内存和存储容量资源使用数据信息展示。（需提供产品功能截图） |
| 自动部署要求：管理平台对于新上线节点设备可基于链路层协议、被管理节点自动发现，自动分配其IP地址，降低管理难度 |
| ▲支持安装在通用的x86、ARM架构服务器，支持现有市场上主要国内外操作系统，包括Windows、CentOS、Fedora、RedHat、SUSE、Ubuntu、FreeBSD、中标红旗、中标麒麟、中标普华、深度、一铭、凝思等 |
| 运维管理要求：支持虚拟机桌面预览功能，无需登录虚拟机即可在虚拟化管理平台上看到虚拟机当前桌面的状态。 |
| 采用分布式的软件定义存储架构，在通用服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务 |

**1.5.10 PACS存储**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲国产操作系统 | 所投存储底层操作系统采用欧拉、统信、麒麟等国产操作系统，使用成熟稳定的国产品牌自主研发CPU，并且CPU通过国家保密科技测评中心最新的安全可靠测评，提供投标产品使用CPU型号、主频等证明材料以及中国信息安全测评中心官网安全可靠测评结果截图并加盖投标人公章。 |
| ▲硬件配置 | 本次配置≥3个存储节点，单节点配置：CPU:≥2颗国产处理器，单颗主频：≥2.3GHz，单颗物理核数：≥32核，内存：≥8\*32GB DDR4 内存，硬盘：≥2\*480GB SSD 硬盘，≥1\*3.2TB SSD 硬盘，≥96T SATA 硬盘；网口：≥4\*GE网口，≥4\*25GE 网口（含万兆光模块），软件：配置对应可得容量的存储软件授权； |
| 分布式架构 | 采用全对称分布式架构，无独立元数据节点，随着存储节点数的增加，分布式存储性能和容量也随着近线性增长，扩容过程中业务不中断； |
| 具备大规模横向扩展能力，单集群规模最大可扩展至≥4096节点，支持横向扩展能力，新增节点带来的集群性能提升不低于单节点性能的80％； |
| 支持在线缩容和扩容；支持存储软件在线升级，升级操作均不影响前端业务的连续性； |
| CIFS协议 | 支持创建目录、删除目录、创建文件、删除文件、拷贝文件、查看文件、修改文件等； |
| 业务连续能力 | 支持Failover,支持在接入节点发生故障时业务不中断； |
| ▲并行客户端功能 | 为大幅提升医生客户端阅片性能，降低访问时延，所投存储产品支持客户端功能，支持MPI-IO等，兼容OpenMPI， MPICH2等；（需提供产品功能截图） |
| 文件访问控制 | 支持对文件多种访问控制，只读、只读写、完成控制（读/写/删除/创建）、禁止（无权限访问）权限； |

**1.5.11数据中心交换机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲转发性能 | 交换容量≥4.8Tbps，以官网所列最低参数为准；包转发率≥2000Mpps，以官网所列最低参数为准； |
| 硬件规格 | 高度≤1U，固定接口交换机，电源1+1备份，风扇模块3+1备份； |
| CPU | 国产芯片，自主可控，提供第三方测试报告； |
| 特性 | 4、设备缓存≥32M，支持前后、后前风道； |
| 5、支持M-LAG或vPC或DRNI等跨机箱链路捆绑技术; |
| 6、支持BFD3.3ms检测间隔 |
| 端口配置要求 | 48个10GE光端口数量，6个100GE 光接口； |
| 模块 | 配置20个万兆多模光模块； |
| 质保服务 | 原厂质保三年。 |

**1.5.12千兆交换机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| ▲端口 | 24个10/100/1000M电口，4个千兆 SFP接口； |
| 性能 | 交换容量：≥672Gbps/6.72Tbps；包转发率：126Mpps； |
| CPU | 国产芯片，自主可控，提供权威第三方测试报告; |
| MAC地址 | ≥32K，预留可支持到64K的能力; |
| 质保服务 | 原厂三年质保。 |

**1.5.13核心交换机**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 自主可控 | 采用国产芯片，自主可控，提供权威第三方测试报告; |
| 可靠性 | 主控上的业务端口，在主控复位时，依然可以正常工作； |
| 性能 | 包转发率：≥100/460 Tbps，交换容量：≥76800 Mpps； |
| ▲配置要求 | 主控板槽位数：≥2； |
| 业务板槽位数：≥6； |
| 支持颗粒化电源，整机电源槽位数≥6； |
| 为了部署的方便性，POE电源模块须内置于机框内，不使用外置电源模块 |
| ▲实际配置 | 板卡：两个主控；网口：≥48个万兆光口，≥48个千兆电口；光模块：≥12个10GE多模光模块，≥1个10GE高速电缆-3m； |
| 电源 | 冗余电源 |
| 质保 | 原厂三年质保。 |

**1.5.14配套软件**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 软件 | 国产化操作系统、国产化数据库 |

**1.5.15运维服务**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 运维服务 | 一、运维服务要求  如需要，供应商需提供标准机柜，空间需满足招标设备安装需求。同时机柜所在机房环境需满足如下要求：  1、动环要求  ①两组UPS，切换时间小于10ms，UPS电源的供电时间不小于4小时；  ②一组油机，额定功率不低于500Kw；  ③两路市电；  ④机房内空调制冷量不低于320Kw；  2、驻场服务  提供2名专业技术人员（人员须为资深工程师），24小时\*365天驻场服务，驻场期间由采购人提供办公场所，驻场人员要自行提供工作工具，按照采购人的作息时间进行工作，接受管理和工作安排。  3、巡检要求  必须对维护范围内的信息化软硬件设备每4小时进行一次巡检且必须提供记录，及时发现系统存在的隐患与安全漏洞，提出书面报告，并与采购人共同解决存在的问题与隐患。每次巡检应提供书面巡检报告，并根据巡检报告及时与采购人进行交流，及时协调解决维护工作中的问题。  4、咨询服务  应对用户信息系统进行定期的维护管理和配置优化，确保用户整个信息系统运转的高效、稳定和安全，减少和避免系统性能瓶颈，杜绝信息系统安全事故，并且能根据用户需要，提供信息系统运行的合理化建议和方案。   1. 运维周期   供应商承诺对所投软硬件产品原厂质保三年，整体项目免费运维服务三年。  6、如甲方提供机柜、机房，供应商需无条件将设备迁移至指定位置。 |

**1.5.16配套链路**

|  |  |
| --- | --- |
| **名称** | **技术要求** |
| 专线链路 | 供应商需提供2条不低于1G带宽的的专线链路。 |

**二、其他内容不变。**