**采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **采购项目** | **数量** | **单位** |
|  | 模块化机房一体化建设（含装修） | 1 | 套 |
|  | 供配电系统 | 1 | 套 |
|  | 机柜系统 | 1 | 套 |
|  | 动力环境监控管理系统 | 1 | 套 |
|  | 消防系统 | 1 | 套 |
|  | 装饰装修及其他 | 1 | 套 |
|  | 楼层交换机 | 33 | 个 |
|  | 安全网关 | 1 | 套 |
|  | 主机安全管理系统 | 1 | 套 |
|  | 日志审计系统 | 1 | 套 |
|  | 运维审计系统 | 1 | 套 |
|  | 数据库审计系统 | 1 | 套 |
|  | 态势感知平台 | 1 | 套 |
|  | 安全服务 | 1 | 套 |
|  | 网络安全等级保护测评 | 2 | 套 |
|  | VPN | 1 | 套 |
|  | 核心交换机 | 1 | 套 |
|  | 超融合一体机 | 6 | 套 |
|  | 备份一体机 | 1 | 套 |
|  | 超融合专用交换机1 | 2 | 套 |
|  | 超融合专用交换机2 | 2 | 套 |
|  | 互联网医院 | 1 | 套 |
|  | 系统集成 | 1 | 套 |

1. **模块化机房一体化建设**

1.1 **供配电系统**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 蓄电池 | 电池厂商要求国内大规模主流工业铅酸电池企业，交货能力强，通过UL/CE/IEC/TLC认证，提供证明材料  蓄电池容量：C20，25℃不低于100AH  蓄电池功率重量比（电池15分钟功率/重量）不低于：10.4W/Kg·单元，功率容量比：W15/C10≥3.0W/AH\*单元。  应采用长效密封免维护电池，蓄电池的连续浮充工作寿命不少于10年，25℃条件  循环使用寿命应满足：80%放电深度时≥400次；  30%浅充放电≥1000次。电池再充电时间：10~12小时电池容量达到90%以上。  蓄电池除排气阀外，其他各处均要保持良好的密封性，应能承受50kPa的正压或负压而不破裂、不开胶，压力释放后壳体无残余变形。  蓄电池组容量：蓄电池20小时放电容量C20，20h率容量在第一次循环不低于0.95C20，第五次循环达到C20，放电终止电压10.5V。  浮充蓄电池组电压偏差值：蓄电池组在正常浮充下运行3~6个月，单个蓄电池端电压与平均值的偏差为±0.3V。 | 只 | 32 |
| 2 | 电池架 | 1、根据现场实际空间定制电池架、  2、元器件采用直流开关盒、  3、汇流盒  4、35mm²电池连接线 | 个 | 1 |
| 3 | 160A交流配电单元 | 【主路输入】单路市电输入，配置250A/3P\*1塑壳开关；  【防雷要求】C级防雷设计；  【市电输出】UPS输入输出开关配置160A/3P\*2微型断路器，UPS维护旁路开关带锁配置160A/4P\*1微型断路器；空调输入开关配置63A/3P\*3微型断路器；照明开关32A/1P\*1微型断路器；备用开关32A/1P\*1微型断路器，备用开关16A/1P\*5微型断路器，备用开关10A/1P\*5微型断路器； B路IT机柜开关配32A/1P\*15微型断路器；  【UPS输出】A路IT机柜开关配置32A/1P\*15微型断路器；监控32A/1P\*1微型断路器，备用开关10A/1P\*5微型断路器；  【断路器要求】采用施耐德品牌  【其他】配置三相电子式电能表（斯菲尔），可监测主路供电电压、电流、功率等参数；配置电源输入指示灯； | 台 | 1 |
| 4 | 配电柜 | 1、定制，根据设计系统图结合施工实际要求进行深化  2、柜体尺寸：与机房服务器机柜品牌和选型要一致，根据元器件选型和设计系统图深化箱内元器件布置图  3、所有元器件应选择国际知名的产品  4、所配电器元件应满足有关规程、规范的要求，均应有合格证，强制认证的产品应有认证标志  5、浪涌保护器防雷保护装置：内置D级防雷器  6、同型号同规格的元器件应采用同一生产厂生产的同一安装尺寸的产品  7、 输出开关（支路）：具有可在线热插拔功能，每个断路器的输入端设有一个电流互感器进行电流测量。所有电流互感器连接到监控模块上，并向主模块发送有关测量数据的信息  8、配套监控系统，能数据处理及显示主开关全部电参量及支路电参量，提供与机房环境监控系统的联接端口，采用开放式通讯协议接口：RS485 或SNMP 接口，通讯协议为MODBUS RTU 协议等  9、配电柜的开关位置均应留有足够的接线空间，如无法满足现场接线要求，则由中标人负责免费整改直至满足安装要求。配电柜内中性零线（N 线）和相线（L线）的安装方式为同向，尽量减少出现交叉的情况  10、所有的对外引接电缆均应通过接线端子连接至接线排，每组端子排应留有备用端子。导线两端均应标以编号，导线的任何连接部分不能焊接  11、配电柜内所有电气连接电线电缆均采用无卤低烟阻燃型  12、必须进行成套装配，应符合成套相关要求  13、柜体配置接地装置和相关线缆，符合接地要求  14、其他要求：柜体的标识标贴要完整且符合要求，包含底部支撑架及所有安装所需要辅件  15、环境温度：－5℃～＋40℃ | 套 | 1 |
| 5 | 竖直PDU普通型 | 单相32A输入，输出12位国标10A插孔+4位国标16A；不带电源线，带接线盒；带总输入开关电源指示灯；竖直安装，区分AB路。 | 件 | 26 |

**1.2机柜系统**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 综合柜 | 1、服务器机柜尺寸规格（W×D×H）：600mm×1350mm×2000mm，42U；  2、机柜应采用高强度的优质冷轧钢板，防护等级不低于IP20，主体骨架采用≥2.2mm厚冷轧钢板材料，其它≥1.5mm厚冷扎钢板材料 4、机柜前后门须采用具有良好透风性能网状结构，前门采用单开平板网孔门，后门采用双开平板门，为了便于安装、拆装，要求单块侧板分两段设计；开门角度不低于120°，需提供第三方权威机构检测报告；  5、机柜800KG承载8、9级烈度抗震能力，提供权威第三方检测报告。 | 台 | 1 |
| 2 | IT柜 | 1、服务器机柜尺寸规格（W×D×H）：600mm×1350mm×2000mm，42U；  2、机柜应采用高强度的优质冷轧钢板，防护等级不低于IP20，主体骨架采用≥2.2mm厚冷轧钢板材料，其它≥1.5mm厚冷扎钢板材料；需提供第三方检测报告  3、且机柜要有良好的承重能力，机柜净重≥320KG，静态承重≥2550KG，动态承重≥1200KG；需提供防护等级、板材和承重的第三方权威机构检测报告； 4、机柜前后门须采用具有良好透风性能网状结构，前门采用单开平板网孔门，后门采用双开平板门，为了便于安装、拆装，要求单块侧板分两段设计；开门角度不低于120°，需提供第三方权威机构检测报告；  5、机柜800KG承载8、9级烈度抗震能力，提供权威第三方检测报告。 | 台 | 10 |
| 3 | 左侧板组件 | 上下两段式侧门，适配1350mm(D)\*2000(H)机柜，机柜左侧内部螺钉固定。 | 件 | 2 |
| 4 | 右侧板组件 | 上下两段式侧门，适配1350mm(D)\*2000(H)机柜，机柜左侧内部螺钉固定。 | 件 | 2 |
| 5 | 层板 | 用于承载机架空调以及其他重要设备，适用于800mm安装深度，T=1.5mm，承重不小于80KG。 | 件 | 33 |
| 6 | L型导轨 | 定制用于承载机架UPS等，适用于800mm安装深度，T=2.0mm，承重不小于50KG。（1件含左右2个） | 件 | 10 |
| 7 | L型导轨（UPS专用） | 定制用于承载机架UPS等，适用于800mm安装深度，T=2.0mm，承重不小于50KG。（1件含左右2个） | 件 | 1 |
| 8 | 1U塑胶假面板 | 1.配置1U封板，用于机柜冷热风道隔离，免工具、快拆设计。  2.采用阻燃材料，需提供非金属件阻燃报告。 | 件 | 100 |
| 9 | IT柜照明包 | 单纯照明、开关控制灯、门开灯亮，门关灯关。 | 套 | 10 |
| 10 | 蓝色LED灯带 | 单色LED灯带-2000mm | 条 | 20 |

**1.3动力环境监控管理系统**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 监控系统总成 | 1) 嵌入式Linux监控主机，配套监控软件，支持实时数据、告警通知、基本报表、WEB页面访问等；整体的环境和动力监控接口，实现对模块内供配电、UPS、空调、温湿度、漏水检测、烟雾，发现部件故障或参数异常，即时采取 E-mail、短信告警、声光报警等多种报警方式，记录历史数据和报警事件；  2) 水浸：通过检测接口连接至采集器，当检测到有漏水发生时，监控系统发出报警提示；  3) 温湿度：NTC 温度传感器；  4）烟雾传感器： 红外光电传感器: LED灯光闪烁指示/输出电信号至联网控制主机、自动复位；。  5) 控制器显示屏(≥9.7 英寸)，微模块显示屏为电容屏，支持多点触控；  6）具备空调、配电、UPS、消防、新风等状态显示功能.  7）声光报警器；  8）声光报警、温湿度、烟雾传感器等采用强磁固定方式，可随意改变安装位置。  9) 提供软件著作权证书以及3C认证及检测报告，空调、UPS、配电、监控系统为同一品牌。 | 台 | 1 |
| 2 | 监控一体机 | 台 | 1 |
| 3 | 电控盒部件 | 台 | 1 |
| 4 | 温湿度传感器 | 个 | 2 |
| 5 | 烟雾传感器 | 个 | 2 |
| 6 | 不定位漏水套装 | 套 | 1 |
| 7 | 综合柜蓝色LED灯带 | 条 | 1 |
| 8 | 综合柜机柜照明包 | 个 | 1 |
| 9 | 综合柜内监控布线总成 | 套 | 1 |
| 10 | 综合柜内动力布线总成 | 套 | 1 |

**1.4 消防系统**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 点型光电感烟火灾探测器 | 1、火灭自动报警系统和灭火控制系统组成完整的灭火系统  2、气体要求：七氟丙烷  3、本次消防系统要求采用无害七氟丙烷全淹没灭火系统，喷放时间不大于20秒。  4、在抱回区域外及机房监控中心设置声、光报警及释放信号标志，并在机房监控中心设置灭火控制系统紧急启用与停止开关。  5、消防系统需保证机房内人员安全。  6、符合国家固定灭火系统标准审查委员会审查的Q/HSB07-2011《七氟丙烷自动灭火系统设计》国际标准的指标和要求。 | 只 | 4 |
| 2 | 点型光电感温火灾探测器 | 只 | 4 |
| 3 | 探测器底座 | 只 | 4 |
| 4 | 手持编码器 | 个 | 1 |
| 5 | 气体喷洒指示灯 | 个 | 1 |
| 6 | 紧急启停按钮 | 只 | 1 |
| 7 | 指示灯及启停按钮底座 | 只 | 2 |
| 8 | 火灾声光警报器（4线制） | 只 | 4 |
| 9 | 火灾声光警报器底座 | 只 | 4 |
| 10 | 通讯模块 | 只 | 1 |
| 11 | 通讯模块底座 | 只 | 1 |
| 12 | 柜式七氟丙烷灭火装置 | 瓶组 | 1 |
| 13 | 七氟丙烷药剂 | KG | 150 |
| 14 | 泄压口 | 套 | 1 |
| 15 | 气体灭火火灾报警控制器 | 套 | 1 |

**1.5 装饰装修及其他**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 双联开关 | 国标86型双开双控开关 | 个 | 5 |
| 2 | 应急照明指示灯 | 国标机房应急照明灯 | 台 | 4 |
| 3 | 机房专用吊顶灯 | 国标600\*600机房吊顶专用灯 | 台 | 12 |
| 4 | 防盗门 | 国标 | 樘 | 2 |
| 5 | 指纹密码锁 | 国标指纹、密码、ID卡一体锁 | 台 | 2 |
| 6 | 操作台 | 1、4联操作台，参考尺寸：3600\*900\*750mm（长\*宽\*高）  2、材质：冷轧钢板，厚度不低于1.2mm，表面防锈，酸洗，磷化，静电喷塑  4、结构：拼装结构，缝隙不大于3mm  5、键盘抽屉抽拉不小于10000次  6、前面板通风率不少于50%，支持前后开门  7、操作台外观、颜色、尺寸须按装饰要求进行定制  8、符合国标，提供权威检测报告 | 台 | 1 |
| 9 | 安装调试费 | 【新建机房】  1、机房新址选用走廊，四面无墙，需提供专业设计  2、墙体做法需要全部天地生根  3、不可影响消防验收，以及消防卷帘的开启与闭合  4、中标人需配合业主方完成消防验收  【顶面天花主龙骨】  1、采用U38系列镀锌轻钢龙骨，厚度不小于0.8毫米。吊筋采用镀锌轻钢材质，吊杆直径不小于0.6毫米。  【顶面微孔铝板】  1、600×600，采用的基材为1001H24、3003H24国家标准铝材热扎优质铝合金板材，基材厚度不小于0.8mm，误差不超过20um；表面平整无痕，拼接无缝；板面涂层采用静电粉末喷涂，正面涂层厚度不小于60μm；背面贴高级吸音无纺布；整板采用一次冲压成型，不采用间歇式翻折工艺加工。含收边。  2、不支持国标负偏差  提供权威第三方检测报告  【75系列轻钢龙骨（防火岩棉填充）+彩钢板封面（内含防火石膏板）】  1、75系列轻钢龙骨（防火岩棉填充）+彩钢板封面（内含防火石膏板）22、不支持国标负偏差  【75系列轻钢龙骨（防火岩棉填充）+12mm防火石膏板】  1、75系列轻钢龙骨（防火岩棉填充）+12mm防火石膏板。  2、不支持国标负偏差  【墙面刷白色无机涂料】  1、白色无机涂料（A级，2道）  2、不支持国标负偏差  【踢脚线不锈钢包边】  1、高度：100mm，材质304不锈钢  2、不支持国标负偏差  【地面防尘防静电漆】  1、A及防静电漆，三遍成活  2、完工验收时需要提供三遍成活的依据  【全钢静电地板】  1、机房专用复合静电活动地板（无边框）  2、地板支承系统：横梁支角和钢轨支角（支角分成上、下托，螺杆可以调节，以调整地板面水平）。地板的撑脚可以调节高度  3、 厚度：35mm，颜色一致，无色差，无气泡现象  4、 单元尺寸：600×600×35mm，无缝，极限偏差≤0.2mm  5、 集中承受力：≥450kg/㎡  6、 分散承受力：≥23000N/㎡，撬曲度小于2mm（承载3000N）  7、 阻抗：1×105Ω～1×109Ω  8、网络机房内风口地板位置由施工单位进行深化，风口地板透风率不小于40%，主要设置在冷通道内及其他相应设备区，  9、机房主入台阶，5号角钢基础，防静电地板饰面， 10、架空高度综合考虑。  12、不支持国标负偏差  【等电位均压环】  1、40\*4接地铜排  【接地网格】  1、25mm²编织铜带  2、不支持国标负偏差  【接地线】  1、BVR-16m2  2、不支持国标负偏差  【等电位接地箱体】  1、参考尺寸300\*200\*100mm，含18位接地汇流排  2、不支持国标负偏差 | 项 | 1 |

1. **楼层交换机**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 楼层交换机 | 1、端口类型：≥24 \*10/100/1000TX以太网端口，≥2个SFP光口，≥2个SFP+光口。  2、交换容量(G) ：396Gbps  3、转发性能(Mpps)：108Mpps  4、MAC地址表：最多支持MAC（Media Access Control）地址：16K  支持手工配置静态MAC：1000项  5、静态MAC配置：  支持端口镜像和流镜像功能  支持端口聚合(聚合组端口最大8个端口)  支持10GE口聚合  支持端口隔离  支持STP/RSTP/MSTP  支持IEEE 802.3ad（动态链路聚合）、静态端口聚合  支持Jumbo Frame  6、VLAN：支持基于端口的VLAN  支持MAC VLAN  支持Guest VLAN  7、ARP：支持ARP Detection功能  支持ARP限速  8、DHCP：支持DHCP Client  支持DHCP Snooping  支持 DHCP Relay  支持DHCP Option82  9、IPv4、IPv6：支持IPv4/IPv6静态路由、双协议栈  支持DHCPv6 Client、DHCPv6 Snooping  支持ND、PMTU  支持IPv6 Ping、IPv6 Telnet、IPv6 SSHv2、IPv6域名解析  10、管理：支持命令行接口（CLI）配置  支持Telnet远程配置  支持通过Console口配置  支持SNMP（EImple Network Management Protocol）  支持RMON（Remote Monitoring）告警、事件、历史记录  支持iMC网管系统  支持WEB网管  支持系统日志  支持分级告警  支持NTP | 个 | 33 |

# 安全设备技术要求

**3.1 安全网关**

1. 安全网关性能要求：吞吐量不低于8Gbps，最大并发连接数不低于300万，每秒新建连接数不低于10万。工作接口标配12\*GE电口（含1组Bypass电口），12\*SFP光口；支持千兆接口总数不低于24个。配置双电源。
2. 要求配置3年防病毒许可（AV），3年入侵检测与防御许可（IPS），3年上网行为管理许可（APP&URL），并提供三年原厂质保及软件、规则库升级服务，默认提供1500个SSLvpn用户许可。
3. 要求支持基于7元组、域名的链路负载均衡策略；支持过载保护、会话保持和健康检查，会话保持可实现用户的访问请求均分配至同一出口。
4. 要求支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能。
5. ▲内置不少于8000条IPS规则库，包含安全漏洞、CGI攻击、缓存溢出、木马后门、网络数据库攻击、蠕虫病毒、间谍软件、欺骗劫持等安全类型，提供此功能证明材料。
6. 要求支持本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证、微信认证、APP认证、二维码认证、互联网钉钉认证、混合认证和免认证，其中微信认证支持通过小程序获取手机号。
7. 要求支持虚拟路由转发功能，使用VRF功能可以从系统层面隔离不同VRF组里的流量信息和路由信息，可作为MPLS组网环境中的MCE设备。提供此功能证明材料。
8. 内置Web防护特征库，提供SQL注入攻击、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于10种的防护类型，支持手动和自动特征库升级。
9. 提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询。
10. 求支持对20级的压缩文件进行解压查杀。以上参数提供相关证明截图及第三方检测证明材料。
11. 要求支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限；

**3.2 主机安全管理系统**

1. 求提供主机安全管理系统1套，管控终端数不低于250个，提供三年软件使用许可、特征库升级、技术支持服务。
2. ▲要求支持可视化态势大屏展示，包括终端安全管控大屏和安全概况大屏，安全概况展示内容包括防护概况、检测概况、入侵检测概况、防护风险趋势、安全动态；终端管控包括终端状态、分组分类、版本状态、安装量、防护率、在线率等，提供此功能证明材料。
3. 要求支持Windows PC防护以及主流信创PC防护如中标麒麟、银河麒麟及统信uos等系统。
4. 要求支持各类型服务器防护；支持Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 +、Suse11 +、Ubuntu 14 +等操作系统。
5. 要求支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时招标人端进行熔断；支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控；支持网络通信全时监控。
6. 要求支持对恶意文件进行自动化动静态分析，获取样本行为分析、样本同源性等分析。支持IP&域名&文件&邮箱的信誉判断，可以对应急响应事件进行处置溯源分析，还可以获取可视化数据形成黑客团伙画像及获取实时的热门威胁情报，提供此功能证明材料。
7. 提供告警类型包括：异常文件、网站防护、性能监控、登录防护。告警内容至少包括事件发生时间、事件类型、访问的资源、IP源地址等详细内容。告警方式包括：Email，短信，syslog，snmptrap，自定义。
8. 要求支持文件实时监控，在文件执行、文件修改、存储介质连接时自动触发；支持对压缩包扫描及深度进行设置，默认9层深度；支持对文件扫描进行跳过，默认50M以上文件；支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并且将修复前的病毒文件进行备份；支持对顽固流行病毒进行智能拦截提供专门的勒索风险评估功能。
9. 要求支持网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，支持资产自主切换不同网络访问域，提供此功能证明材料。

**3.3 日志审计系统**

1. 要求产品能够审计不少于55个日志源，平均日志处理能力不低于2000EPS（峰值不低于4000EPS），硬盘不少于2T，内存不低于8G。
2. ▲产品采用解决方案包上传对产品进行功能扩展，无需要代码开发，提供此功能证明材料。
3. 要求支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。
4. 要求支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持使用代理(Agent)方式提取日志并收集。
5. 安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件，提供此功能证明材料。
6. 内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景。
7. 要求通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息，提供能力检测证明材料。
8. 要求支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、攻击类型、地理城市进行过滤查询。
9. 要求内置合规性报表1000+种；内置SOX、ISO27001、WEB安全等解决方案包。
10. 要求支持双因子认证登录，双因子认证令牌支持绑定至具体用户。
11. 要求支持三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件，提供能力检测证明材料。
12. 要求设备制造商具备国家信息安全测评信息安全服务资质证书（安全工程类三级）。提供证书复印件或扫描件。

**3.4 运维审计系统**

1. 要求产品硬盘空间不少于2T，可管理设备数量不低于100个，运维用户无限制。
2. 要求支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。
3. 求支持AD、LDAP、RADIUS、吉大正元、北京CA、深圳CA认证系统联动登录堡垒机；支持多个AD域认证源；支持自动同步AD/LDAP用户，提供此功能证明材料。
4. 要求设备支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；也可通过应用发布的方式进行协议扩展以及IE代填应用发布等协议。
5. 要求支持标准化对接CAS、JWT、SAML2、OAuth2单点登录认证，且支持配置是否自动创建堡垒机中不存在用户，提供此功能证明材料。
6. 要求支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能；要求支持完善的自动改密安全保护机制。支持发送方式，包括邮件、FTP、SFTP等要求支持自动密码恢复、手工验证密码、密码强度控制等。
7. 要求支持使用IE、谷歌、火狐三种浏览器打开远程运维审计设备的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维招标人端工具。
8. 要求支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志；要求支持保存SSH的sz/rz命令（zmodem）传输的原始文件，提供此功能证明材料。
9. 要求支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表。
10. ▲要求支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。提供此功能截图证明材料。
11. 要求设备制造商具备国家信息安全测评信息安全服务资质证书（风险评估二级）证书，提供证书复印件或扫描件。

**3.5 数据库审计系统**

1. 要求产品支持的数据库实例个数不低于4个；设备SQL处理能力不低于6000条/秒;吞吐量不低于500Mbps。
2. 要求支持在云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；支持IPv4/IPv6双栈审计；支持和ES平台对接，将审计日志和告警日志存储在ES系统中，并支持通过页面查询日志。
3. 要求可在云环境操作系统中安装软件代理，要求提供证明材料。
4. ▲要求支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB等主流数据库审计；支持PostgreSQL、GuassDB、HANA、greenplum、librA、graphbase、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、Redis审计，提供此功能证明材料；支持MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Canssandra、greenplum、LibrA、graphbase、cache等数据库审计。
5. 要求支持数据库操作表、视图、索引、存储过程等[各种对象的所有SQL操作审计](#_支持各种对象的SQL审计_1)；支持数据库请求和返回的双向审计。
6. 要求支持基于数据库[访问日期、时间、源/目的IP、来源](#_多维度查询)、数据库名、数据库表名、字段值、数据库登录账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询。
7. 求支持B/S业务系统三层关联审计，提供此功能证明材料。
8. 要求支持用户界面告警、SNMP、邮件、短信、钉钉、SYSLOG方式告警。
9. 要求设备内置独立的故障排错系统，可以支持一键导出加密的系统调试日志。
10. 要求设备制造商具有中国通信企业协会通信网络安全风险评估（二级）资质证书，提供证书复印件或扫描件。

**3.6 态势感知平台**

1.要求数据采集和处理性能不低于8000EPS，CPU不低于24核，内存不低于128GB，配置企业级存储磁盘总容量不低于48TB；千兆电口不少于5个。

2.要求工作台首页支持自定义个性化配置，支持以拖拽方式进行画布页面设置，页面可选组件包括原始告警、资产管理、组件管理、风险资产、安全事件、安全日志、平台概览、快速搜索、安全设备、SOAR、系统消息、通报预警、工单、告警监控等，每个组件均支持点击“收藏”按钮进行自定义收藏。

3.要求支持立体、平面、球面等多种维度的网络实体关系透视，点击每个实体可展示资产名称、风险评级、告警TOP3、最近异常发生时间等，点击实体间的访问连线可展示实体间访问方向、访问类型、累计流量、最近访问时间等。

4.要求内置包括规则模型、关联模型、统计模型、情报模型等多种安全分析模型，提供此功能证明材料。

5.要求安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容，提供此功能证明材料。

6.要求原始日志或原始告警支持多种语法查询，语法至少包括但不限于AND、OR、NOT、==、!=、>、<、>=、<=、exist、notexist、in，语法可任意组合并支持利用中括号和小括号的嵌套查询。

7.要求支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，保留检索语句历史记录；检索语句可直接发布成统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警。

8.要求实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展，提供此功能证明材料。

9.要求支持设置3层递进阻断策略，支持选择多台联动设备下发阻断策略；支持查看封禁设备数、封禁IP数、自动封禁IP数、本日解禁IP数、封禁订阅规则数，支持查看最近7天封禁IP趋势及防护设备封禁IP分布；支持封禁策略批量删除、解禁、导出。

10.要求支持拓扑图的增加、修改、删除、导入、导出，拓扑图支持平面和3D两种方式，拓扑图内容可基于单个资产、安全域、安全设备、WEB业务系统、网络设备等多种方式组成。

11.要求系统获得公安部颁布的“安全管理平台”类销售许可证，提供证书复印件或扫描件。

**3.7 安全服务**

1、安全漏洞扫描服务（三年）

1.1、实施要求：使用知名厂商远程漏洞评估产品，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议。服务人员及用时要求：专业服务工程师工程师2人。服务工具要求：人工+硬件。频率要求：1次/每季。

2、日志审计分析服务（三年）

2.1、实施要求：通过部署服务器收集内网系统路由器、交换机防火墙等网络设备和服务器操作系统、数据库日志信息，对日志记录进行分析，查找和发现系统安全事件和安全问题，并分析问题原因，给出相应的解决方案。服务人员及用时要求：审计分析师2人。服务工具要求：人工+硬件。频率要求：1次/每季。

3、紧急响应服务（三年）

3.1、实施要求：远程或现场方式及时响应和处理信息安全事件，协助招标人降低影响，分析问题产生的原因，提供应急响应报告和改进建议。服务人员及用时要求：安全服务工程师2人。服务工具要求：人工+硬件。频率要求：依据实际发生频率开展。

4、安全巡检服务（三年）

4.1、实施要求：检查内容包括端口状况扫描、端口监听检查、用户列表检查、进程检查、病毒检查、系统木马检查等安全检查与分析工作。服务人员及用时要求：安全服务工程师2人。服务工具要求：人工。频率要求：1次/每季。

5、安全制度完善服务（三年）

5.1、实施要求：协助用户完善系统安全管理制度。服务人员及用时要求：安全服务工程师1人。服务工具要求：人工。频率要求：1次/每年。

6、安全培训服务（三年）

6.1、实施要求：提供网络安全法、网络安全意识、日常办公防护等内容。服务人员及用时要求：资深安全培训工程师1人。频率要求：1次/每年。

# **网络安全等级保护测评**

|  |  |  |
| --- | --- | --- |
| **测评系统名称** | **安全保护等级** | **备注** |
| HIS系统 | 2级 | 协助完成等保定级备案，测评整改并通过测评。 |
| LIS系统 | 2级 |

# **VPN**

1. 桌面型
2. 内存256MB
3. 1个千兆WAN口
4. 4个千兆LAN口
5. 单电源
6. 整机吞吐280M
7. VPN加密吞吐36M
8. 产品硬件保修3年

# **核心交换机**

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 业务插槽数 | 业务插槽数≥3 |
| 交换容量 | 23.04Tbps/64Tbps |
| 转发能力 | 2880Mpps/22500Mpps |
| 主控引擎 | 主控引擎支持固化万兆光业务口≥12个（16电+12万兆光） |
| 主控引擎支持固化万兆光业务口≥12个（16光+12万兆光） |
| 主控引擎支持固化千兆光业务口≥24个（24光+4万兆主控） |
| 主控引擎支持固化千兆电业务口≥24个（24电+4万兆主控） |
| 电源冗余 | 电源模块冗余 |
| 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| 板卡 | 单槽位线速万兆端口密度≥16 |
| 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性，提供商用板卡公开手册的官网链接证明（24电+20光+4万兆） |
| 链路聚合 | 聚合组数≥128组，每组成员≥8个 |
| 支持跨设备链路聚合 |
| 支持对广播、组播、单播报文的均匀分担 |
| 支持链路聚合+ECMP情况也可以对报文均匀分担，即等价路由的链路是由聚合链路组成情况下的报文分担 |
| ACL | 支持双向ACL |
| ACL≥4K |
| 支持端口ACL |
| 支持VLAN ACL |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、WFQ三种队列调度算法 |
| 支持精细化的流量监管，粒度可达8K |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 可靠性 | 双引擎快速倒换，主备切换时候板内转发无丢包 |
| 支持热补丁功能，可在线进行补丁升级 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。 |
| BFD收敛时间<100ms |
| MAC | MAC表≥64K |
| 路由表 | 路由表≥8K |
| ARP | ARP表≥16K |
| MPLS | 支持MCE |
| 支持VLPS |
| SDN/OPENFLOW | 支持OPENFLOW 1.3， |
| 支持多控制器（EQUAL模式、主备模式） |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| ▲安全特性 | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持IP Source Guard |
| 支持广播风暴抑制 |
| 支持EAD |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 管理特性 | 支持Console/AUX/Telnet/SSH2.0 |
| 支持风扇管理 |
| 支持电源管理 |
| 支持在线诊断 |
| 支持SNMPv1/v2 |
| 支持 SNMPv3 |
| 支持RMON(RFC2819) |
| 支持端口镜像 |
| 支持VLAN镜像 |
| 支持RSPAN |
| 支持流镜像 |
| NAS | 支持802.1x |
| 支持mac认证 |
| 支持Portal |
| 支持本地认证 |
| 支持Radius认证 |
| 支持Tacacs+认证 |
| 实配 | 实配千兆电口≥16，万兆光口≥12口，所有端口均分在不同槽位，提高业务可靠性 |

|  |  |
| --- | --- |
| 端口类型 | ≥24 \*10/100/1000TX以太网端口 |
| ≥2个SFP光口，≥2个SFP+光口 |
| 交换容量(G) | 396Gbps（提供官网截图） |
| 转发性能(Mpps) | 108Mpps |
| MAC地址表 | 最多支持MAC（Media Access Control）地址：16K |
| 支持手工配置静态MAC：1000项 |
| 以太网特性 | 静态MAC配置 |
| 支持端口镜像和流镜像功能 |
| 支持端口聚合(聚合组端口最大8个端口) |
| 支持10GE口聚合 |
| 支持端口隔离 |
| 支持STP/RSTP/MSTP |
| 支持IEEE 802.3ad（动态链路聚合）、静态端口聚合 |
| 支持Jumbo Frame |
| VLAN | 支持基于端口的VLAN |
| 支持MAC VLAN |
| 支持Guest VLAN |
| ARP | 支持ARP Detection功能 |
| 支持ARP限速 |
| DHCP | 支持DHCP Client |
| 支持DHCP Snooping |
| 支持 DHCP Relay |
| 支持DHCP Option82 |
| IPv4、IPv6 | 支持IPv4/IPv6静态路由、双协议栈 |
| 支持DHCPv6 Client、DHCPv6 Snooping |
| 支持ND、PMTU |
| 支持IPv6 Ping、IPv6 Telnet、IPv6 SSHv2、IPv6域名解析 |
| 广播/多播/单播风暴抑制 | 支持基于端口速率百分比的风暴抑制 |
| 支持基于PPS的风暴抑制 |
| QoS | 支持Diff-Serv QoS |
| 支持802.1p、DSCP优先级映射 |
| 支持SP/WRR/SP+WRR |
| 流量限速 |
| 镜像 | 支持端口镜像 |
| 支持流镜像 |
| 安全特性 | 支持用户分级管理和口令保护 |
| 支持SSH2.0 |
| 支持端口隔离 |
| 支持 802.1X |
| 支持端口安全 |
| 支持MAC地址认证 |
| 支持IP Source Guard |
| 支持HTTPs |
| 加载与升级 | 支持FTP（File Transfer Protocol）加载升级 |
| 支持TFTP（Trivial File Transfer Protocol）加载升级 |
| 管理 | 支持命令行接口（CLI）配置 |
| 支持Telnet远程配置 |
| 支持通过Console口配置 |
| 支持SNMP（EImple Network Management Protocol） |
| 支持RMON（Remote Monitoring）告警、事件、历史记录 |
| 支持iMC网管系统 |
| 支持WEB网管 |
| 支持系统日志 |
| 支持分级告警 |
| 支持NTP |
| 维护 | 支持调试信息输出 |
| 支持Ping、Tracert |
| 支持Telnet远程维护 |
| 支持NQA |
| 支持DLDP |
| 支持虚拟电缆检测(Virtual Cable Test) |

# **超融合一体机**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标名称 | 技术参数和性能指标 |
|  | 硬件参数 | ▲硬件参数：规格：2U，CPU≥2颗，单CPU核数≥24C，单CPU主频≥2.2GHz，内存≥4\*32GB ，系统盘≥2\*240GB SATA SSD，缓存盘≥2\*960GB-SSD，数据盘≥6\*6T，电源：冗余，冗余电源，接口：6千兆电口+2万兆光口。 |
|  | 云管软件 | 为保证使用体验及产品成熟度，产品需完全自研，非OEM，需提供云计算管理平台的软件著作权证书 |
|  | 云管平台应具备大规模资源池的纳管能力，可支持跨地域的多集群管理，多集群的物理节点纳管规模应超过1000台 |
|  | 云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络和安全虚拟化（虚拟应用防火墙、虚拟应用负载均衡等）功能组件，以保障平台的扩展性和兼容性 |
|  | 支持可靠中心以提供持续数据保护CDP、本地备份、异地容灾等高可用服务，当主平台发生故障时，能够切换到备平台，保障云平台稳定运行 |
|  | 支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件 |
|  | 计算虚拟化 | 为保证使用体验及产品成熟度，虚拟化软件非OEM或贴牌产品，禁止借用第三方软件的整合，以保证功能的可靠性和安全性（提供相应的软件著作权） |
|  | 支持对超融合平台的硬件进行监控和大屏展示，包含CPU、内存、网卡、硬盘、存储、RAID等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议 |
|  | 支持漏洞及版本信息巡检，推送补丁及升级信息，并支持补丁管理、更新、回滚 |
|  | 为了更好的保护用户数据，支持设置定期全量备份、增量备份、差异备份（支持增量差异即基于上次增量做差异备份，不支持累积差异即基于首次全备做差异增量），支持用户灵活配置备份策略，备份文件保留时间最高可以达到15年，支持将虚拟机的备份文件定期归档到第二存储 |
|  | 支持UPS联动，为尽可能保障数据中心断电场景下的业务，可在市电断电时通过UPS临时供应电量，当UPS电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机 |
|  | 为保证整体的可靠性及安全性，要求提供CDP能力的厂商与云厂商为同一家，禁止借用第三方软件的整合（提供相应持续数据保护软件著作权证书）为保证整体的可靠性及安全性。 |
|  | 存储虚拟化 | 为保证使用体验及产品成熟度，虚拟化软件非OEM，需提供存储虚拟化软件著作权证书 |
|  | 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能 |
|  | 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响 |
|  | 支持选择多种克隆方式，包括快速全量克隆、全量克隆和链接克隆，可查看通过链接克隆的虚拟机是否运行正常，可以设置克隆完成后自动启动克隆虚拟机操作（提供带有CMA、CNAS标识的检测报告证明，至少包含报告首页，对应功能测试页和报告尾页） |
|  | 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响 |
|  | 支持对虚拟机或虚拟磁盘设置数据分布策略，当采用副本聚合策略时，可以保证以性能优先为原则，实现IO本地读效果，当采用副本散列策略时，可以保证虚拟机以分布均匀优先为原则，打散分布均匀在各物理主机上 |
|  | 网络虚拟化 | 为保证使用体验及产品成熟度，虚拟化软件非OEM，需提供网络虚拟化软件著作权证书 |
|  | 在管理平台上可以通过拖拽连线完成网络拓扑的构建，可以在网络拓扑页面通过功能键实现虚拟网络连接、开启和关闭等操作（提供带有CMA、CNAS标识的检测报告证明，至少包含报告首页，对应功能测试页和报告尾页） |
|  | 超融合需提供网络可视化组件，可在图形化界面上观察到所有虚拟机的流量走向与访问关系，包括源对象、源IP、目标对象、目的IP、访问次数、服务类型、动作等。 |
|  | 支持跳转连通性探测页面，可以设置探测对象信息，包括网口、对象类型、IP地址，可以点击开始探测按钮查看探测页面信息，可以在网络连通性探测页面查看网络探测是否成功 |
|  | 可以支持手动指定虚拟路由器运行在固定的物理主机上，可以自动将虚拟路由器规划到高性能和高吞吐的物理主机上 |

# **备份一体机**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标名称 | 技术参数和性能指标 |
|  | 硬件参数 | 硬件参数：规格为2U，CPU≥1颗，单CPU核数≥10C，单CPU主频≥2.4GHz，内存≥2\*32GB ，系统盘≥2\*240GB SATA SSD，缓存盘≥2\*480GB-SSD，数据盘≥6\*8T，电源为冗余电源，接口≥4千兆电口+4万兆光口。 |
|  | 备份容量 | ▲提供36TB备份容量授权； |
|  | 分组功能 | 支持文件备份代理分组功能，提高创建批量文件备份任务的效率； |
|  | 数据库备份 | 支持Oracle、SQL Server、MySQL、达梦等主流数据库的在线备份，支持全量、增量、差异或日志备份，支持数据库原机或异机恢复； |
|  | 支持Oracle、SQLServer、MySQL数据库实时备份，拥有高细粒度恢复功能，可以将数据库回滚到某个时间点的某一步操作；支持Oracle数据库多通道备份策略，提高数据库备份效率； |
|  | 记录查询 | 支持按时间段或指定时间点查询实时备份数据库的详细操作记录，可以精确到数据库SQL语句，提供1秒内5条以上数据库日志查询记录； |
|  | 日志管理 | 数据库实时备份支持多种日志管理方式，如按时间保留，按恢复条数保留等； |
|  | 虚拟机无代理备份 | 支持虚拟机无代理备份，兼容VMware vSphere、Microsoft Hyper-V、Citrix XenServer、深信服HCI、H3C CAS/UIS，云轴ZStack、Huawei FusionCompute等主流KVM架构虚拟化平台，支持虚拟机批量备份及恢复，满足数据中心级业务保护需求 |
|  | 运维工具 | 支持高级智能运维工具，提供备份系统服务控制工具以及网络连通判断运维工具等； |
|  | 备份效率 | 支持配置滚动备份任务，备份时最小可以设置15分钟滚动备份间隔，提高数据备份频率； |
|  | 显示界面 | 系统全中文界面，能实时展示备份系统的CPU、内存使用率，当前任务以及历史任务运行状态，以便实时掌握备份系统运行情况； |
|  | 备份限速 | 支持备份限速策略，可以提供策略限速或永久限速，可以指定时间段进行限速，减少备份对生产业务系统的影响； |

# **超融合专用交换机1**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标名称 | 技术参数和性能指标 |
| 1 | 交换机性能 | ▲交换容量≥2.5Tbps；包转发率≥700Mpps； |
| 2 | 端口类型 | 万兆SFP+光口≥24个；40G QSFP+光口≥2个；Console口≥1个；Manage口≥1个； |
| 3 | 冗余性 | 支持双交流电源模块1+1冗余（热插拔）； |
| 4 | 二层功能 | 支持MAC地址≥32K；  支持4K个VLAN； |
| 5 | 虚拟化 | 支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面。 |
| 6 | 工作模式 | 支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时灵活的进行切换。 |
| 7 | 管理维护 | 支持以下上线方式：支持二层广播自动发现网管中心平台；支持配置静态IP地址三层发现网管中心平台；支持DHCP Option43方式发现网管中心平台；支持DNS域名发现网管中心平台。 |
| 8 | 智能终端类型识别 | 支持终端类型库，基于指纹自动识别PC、路由器、摄像头设备、无线AP等。 |

# **超融合专用交换机2**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标名称 | 技术参数和性能指标 |
| 1 | 交换机性能 | ▲交换容量≥400Tbps；包转发率≥150Mpps； |
| 2 | 端口类型 | 千兆电口≥24个，万兆SFP+光口≥4个；Console口≥1个； |
| 3 | 冗余性 | 支持双交流电源模块1+1冗余（热插拔）； |
| 4 | 二层功能 | 支持MAC地址≥16K；  支持4K个VLAN； |
| 5 | 虚拟化 | 支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面。 |
| 6 | 工作模式 | 支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时灵活的进行切换。 |
| 7 | 管理维护 | 支持以下上线方式：支持二层广播自动发现网管中心平台；支持配置静态IP地址三层发现网管中心平台；支持DHCP Option43方式发现网管中心平台；支持DNS域名发现网管中心平台。 |
| 8 | 智能终端类型识别 | 支持终端类型库，基于指纹自动识别PC、路由器、摄像头设备、无线AP等。 |

# **互联网医院**

**11.1建设清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块** | **功能清单** | **备注** |
| 1 | 管理端  （超级管理员） | 菜单管理 |  |
| 2 | 医疗机构维护 |  |
| 3 | 医疗机构科室维护 |  |
| 4 | 医疗机构人员维护 |  |
| 5 | 部门管理 |  |
| 6 | 管理端（医院管理员） | 医疗机构人员维护 |  |
| 7 | 医疗机构科室维护 |  |
| 8 | 出诊时段维护 |  |
| 9 | 挂号费用维护 |  |
| 10 | 医生职称维护 |  |
| 11 | 医生排班设置 |  |
| 12 | 用户管理 |  |
| 13 | 订单管理 |  |
| 14 | 医院报表 |  |
| 15 | 对账报表 |  |
| 16 | 图文配置管理 |  |
| 17 | 图文医生管理 |  |
| 18 | 患者端(新建小程序) | 实名认证 |  |
| 19 | 联系客服 |  |
| 20 | 消息中心 |  |
| 21 | 切换就诊人 |  |
| 22 | 图文咨询 |  |
| 23 | 视频问诊 |  |
| 24 | 视频诊室 |  |
| 25 | 在线挂号 |  |
| 26 | 统一支付 |  |
| 27 | 条件搜索 |  |
| 28 | 电子医保凭证 |  |
| 29 | 医生评价 |  |
| 30 | 专属医生开方 |  |
| 31 | 医生关注 |  |
| 32 | 挂号记录 |  |
| 33 | 问诊记录 |  |
| 34 | 处方记录 |  |
| 35 | 地址维护 |  |
| 36 | 线上购药（自提/配送） |  |
| 37 | 药品物流 |  |
| 38 | 查看电子处方单 |  |
| 39 | 医生端（支持小程序及PC端） | 医生登录 |  |
| 40 | 我的处方 |  |
| 41 | 患者列表 |  |
| 42 | 我的评价 |  |
| 43 | 消息提醒 |  |
| 44 | 意见反馈 |  |
| 45 | 视频问诊 |  |
| 46 | 图文问诊 |  |
| 47 | 在线开处方 |  |
| 48 | 在线开医嘱 |  |
| 49 | 处方流转 |  |
| 50 | 快速处方 |  |
| 51 | 排班管理（8小时外） |  |
| 52 | 药房端 | 消息提醒 |  |
| 53 | 药品维护 |  |
| 54 | 库存维护 |  |
| 55 | 处方审核 |  |
| 56 | 线下收费 |  |
| 57 | 处方驳回 |  |
| 58 | 药房维护 |  |
| 59 | 第三方接口 | 自治区互联网监管平台对接（11个接口） |  |

**11.2 功能要求**

1、互联网医院平台

互联网医院平台包含4个端：管理端、患者端、医生端、药房端。

1.1、管理端

管理端包括系统管理端和医疗机构管理端。系统管理端提供给超级管理员使用，用于区域内医疗机构入驻、分配医院管理员账号；医疗机构管理端提供给医疗机构管理员使用，用于院内医生的管理、互联网医院业务的配置。

1.1.1、系统管理端

系统管理端的功能包含菜单管理、医疗机构维护、医疗机构科室维护、医疗机构人员维护、部门管理等。

（1）菜单管理

支持管理端菜单的配置，包括菜单名称、权限标识、组件路径的新增、修改和删除等。

（2）医疗机构维护

支持医疗机构基础数据维护，医疗机构的详细信息支持从区域全民健康信息平台的医疗机构信息同步，也可在系统中进行新增、修改和导入医疗机构信息。

（3）医疗机构科室维护

支持医疗机构科室基础数据维护，用于医疗机构科室入驻系统时进行科室信息绑定，可在基础管理模块中新增、修改、删除、导入和导出科室信息。

（4）医疗机构人员维护

支持医疗机构人员基础数据维护，用于用户管理模块创建用户时进行医生信息绑定，可在基础管理模块中新增、修改、删除、导入和导出医疗机构人员信息。

（5）部门管理

支持为每个入驻的医疗机构和科室创建部门，用于医疗机构内科室、医生的管理。

1.1.2、医疗机构管理端

医疗机构管理端的功能包含医疗机构人员维护、医疗机构科室维护、出诊时段维护、挂号费用维护、医生职称维护、医生排班设置、用户管理、订单管理、医院报表、对账报表、图文配置管理、图文医生管理等。

（1）医疗机构人员维护

支持医疗机构管理员创建医生账号，医生的详细信息支持从区域全民健康信息平台的医护人员信息同步；支持为医生分配角色的功能。

（2）医疗机构科室维护

支持医疗机构管理员创建机构内的科室，科室的详细信息支持从区域全民健康信息平台的医疗机构科室信息同步。

（3）出诊时段维护

支持医生出诊时段维护用于医生排班配置，医疗机构管理员可维护出诊时段的名称、时段类型、开始时间、结束时间、退号提前天数、挂号最早提前天数、挂号最晚提前天数等。

（4）挂号费用维护

配置各档次的挂号费。

（5）医生职称维护

配置医生职称的收费标准。

（6）医生排班设置

为每位医生配置排班信息，包括医生的挂号职称、出诊的时段、时段间隔时间、时段内的号数等。

平台可按照医生的排班信息生成指定时间段的详细排班信息。

（7）用户管理

支持医疗机构管理员维护用户账号，医生的详细信息支持从区域全民健康信息平台的医护人员信息同步。

（8）订单管理

支持医疗机构进行订单信息查询，包括交易笔数、应收金额及明细。

（9）医院报表

支持医疗机构查询某时间段内的报表信息的查询和导出，包括支付来源、日期、交易笔数、金额等信息。

（10）对账报表

支持指定医疗机构、科室在某时间段内的对账报表信息的查询和导出，包括医院、科室、医生、挂号费、日期、收入和退费等信息。

（11）图文配置管理

可配置图文问诊的最低消息条数、图文问诊一次挂号的有效截止时间、挂号患者的年龄下限及上限。

（12）图文医生管理

可为每位提供图文问诊服务的医生配置挂号职称及图文问诊配置。

1.2、患者端

患者端支持微信小程序的模式，支持患者使用微信号进行登录。患者端支持患者进行实名认证、视频问诊预约挂号、针对复诊进行视频就诊、图文问诊、慢病续方、查看预约信息、问诊信息以及在线开方等。

实名认证

患者登录微信小程序需要实名认证，采用“国家电子健康卡”校验进行认证。

联系客服

在微信小程序“我的”菜单中可以点击联系客服进行问题反馈。

消息中心

患者端微信小程序支持消息的搜索与查看。

切换就诊人

患者端微信小程序支持新增就诊人和切换已增加的就诊人，通过“国家电子健康卡”进行校验。

图文咨询

居民进行图文咨询挂号后，可随时向医生问询诊疗信息，医生可根据时间安排答复居民咨询的问题。

视频问诊

居民可按照预约的视频问诊时间，进入视频诊室进行视频就诊，小程序能够提供多种方式进入视频就诊：

1）可通过小程序 “视频问诊候诊室”，居民可提前5分钟进入，等待医生进行就诊。

2）可从问诊记录中找到待就诊的记录，点击进如候诊室，等待医生进入进行就诊。

（7）视频诊室

居民可按照预约的视频问诊时间，进入视频诊室等待医生进入进行就诊。

（8）在线挂号

复诊患者登录居民端小程序后，可以选择医院、医生进行视频问诊/图文问诊挂号，其中，视频问诊还需要选择就诊的时间。小程序支持患者使用微信支付进行线上支付挂号费。

1）视频问诊挂号

视频问诊挂号可以预约具体的就诊日期和就诊时间，预约成功后即可锁定号源，患者可简要的填写病情信息并在线支付挂号费。

2）图文咨询挂号

患者可简要描述病情、上传诊疗相关的附件、简述需要医生提供的帮助及问诊的疾病，患者也可线上支付问诊费用。

（9）统一支付

患者在进行在线挂号的时候可以通过统一支付的方式进行在线支付挂号费。

（10）条件搜索

患者可以通过条件搜索功能进行相关信息的搜索。

（11）医生评价

居民就诊后，可对医生就行评价。

（12）专属医生开方

为线下患者提供开药服务，患者正按方用药且病情稳定。

（13）医生关注

支持患者关注自己想要关注的医生，可在我的医生菜单查看已关注的医生。

（14）挂号记录

小程序可为患者提供查看挂号记录的功能。

（15）问诊记录

小程序可为患者提供查看问诊记录的功能。

（16）地址维护

小程序支持患者进行地址维护功能。

（17）线上购药（自提/配送）

小程序支持为患者提供线上购药功能，支持药品自提和送药上门两种方式。

（18）药品物流

药品物流功能为患者提供送药上门订单和药品自提订单的物流信息查询。

（19）查看电子处方单

医生开具处方后，小程序为患者提供电子处方单的查询功能。

1.3、医生端

医生端支持PC端和小程序端两种接诊模式。

1.3.1、PC端

（1）首页

登录视频诊室医生端后，可以查看待就诊患者列表，蓝色卡片为接诊中的患者、灰蓝色卡片为已进入候诊室候诊的患者、灰色卡片为未上线的患者，医生可查看患者视频问诊预约挂号时填写的病情信息。视频问诊结束后，医生可记录病程并开具处方。

（2）视频问诊

医生和患者都进入视频诊室，医生可以开始视频问诊。

（3）疾病诊断

视频问诊结束后，医生可根据患者病情书写诊断。诊断界面可根据医生输入的信息模糊匹配ICD10疾病字典，供医生选择。

（4）开具处方

医生书写完诊断信息，可以为患者开具处方，医生可输入处方的拼音手写字母或者药品的名称，系统支持模糊检索药品库，列出符合条件的药品信息，供医生选择。

（5）接诊记录

医生可查看自己的在线接诊记录，可按照患者名称或者诊断日期进行检索，也可查看患者的诊断信息及处方信息。

1.3.2、小程序端

（1）医生登录

打开医生端小程序，输入账号、密码及验证码后可登录小程序，也可以通过手机号码登录。

（2）我的处方

支持医生查看已经开过的处方，包括审核未通过、审核中和审核通过的。

（3）我的评价

可以在我的评价菜单中查看患者对医生的评价。

（4）视频问诊

接诊后，医生可进入视频诊室，对患者进行视频问诊。

（5）图文问诊

医生可以点击图文问诊菜单查看待接诊、接诊中、已结束和异常订单信息，并在待接诊的患者列表中选择患者进行接诊。

在线开处方

视频问诊或图文问诊结束后，医生可针对病人的病情书写诊断并开具处方。

在线开医嘱

视频问诊或图文问诊结束后，医生可针对病人的病情在线开医嘱。

处方流转

医生开具处方后，处方信息会同步到处方流转平台。

（10）快速处方

支持医生在常用处方选择处方进行编辑重新开具处方，还可以将历史处方设为快速处方。

1.4、药房端

（1）消息提醒

处方流转平台药房端支持消息的搜索与查看。

（2）药品维护

药房管理员登录系统后可以进行药品维护，包括分类名称、分类编码、药品编码、药品名称、药品厂家等信息的维护。

（3）库存维护

库存维护包括药品库存维护、入库管理和出库管理。

药房管理员登录系统后可以进行药品库存维护，包括入库和出库，入库就是将药品信息添加到该药店，出库主要是销售出库，将销售出去的药品进行出库操作。

入库管理主要是将药品进行入库操作，和库存维护的入库是相同的含义。

出库管理主要是将药品进行出库操作，和库存维护的出库是相同的含义。

（4）处方审核

药师可根据情况，审批处方通过或者驳回，需要填写审批意见。

（5）线下收费

药房可以进行线下收取购买药品的费用。

（6）处方驳回

药师可根据情况，审批处方驳回，需要填写审批意见。

（7）药房维护

药房维护包括支付商户维护和药房库存维护。

**11.3 互联网医院牌照申请服务**

依据《互联网诊疗管理办法（试行）》、《互联网医院管理办法（试行）》、《远程医疗服务管理规范（试行）》等相关要求，结合内蒙古自治区互联网医院牌照申请相关要求，协助医院申请互联网医院牌照，包括但不限于提供以下服务：

协助医院通过自治区互联网医疗服务监管系统申请互联网医院牌照（医疗机构执行许可证增加第二机构名称）。

**11.4 互联网医疗服务监管系统对接**

（1）配合医院完成申请书、可行性研究报告、互联网医院规章制度等材料上传；

（2）配合完成互联网医疗服务监管系统API接口对接；

（3）协助提供互联网医疗信息系统三级等保备案及测评证书；

（4）配合医院完成自治区信息中心技术审核、医政医管局行政审批等流程；

（5）提供互联网医疗服务系统演示环境的准备

**11.5 医疗机构执业许可证变更**

（1）协助指导医疗机构完成政务服务执业登记变更流程；

（2）协助配合完成内蒙古自治区卫生健康委员会（内蒙古自治区中医药管理局）技术初审/材料复审、完成电子证照系统执业许可证变更、协助完成医疗机构执业许可证打印、政务局执业许可证盖章等一系列流程；

供应商需提供在牌照申请变更过程中的咨询服务、技术支持以及指导材料的准备等服务，确保医疗机构能够在要求的期限内尽快完成互联网医院牌照申请及执业许可证变更等业务流程。

# **系统集成**

　　把硬件、软件、数据和信息按照行业标准和医院实际需求统一集成。