# 苏北人民医院信息安全设备采购技术参数要求

**一、设备采购一览表：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **推荐品牌** |
| 1 | 终端安全管控系统 | 1 | 启明星辰、亚信、绿盟 |
| 2 | WEB防火墙 | 1 | 启明星辰、铱迅、绿盟 |
| 3 | 日志审计 | 2 | 启明星辰、铱迅、绿盟 |
| 4 | 运维平台 | 1 | 启明星辰、中宜通信，德塔精要 |

**二、技术参数要求（带★号为必须满足项）：**

## 1.终端安全管控系统（1套）

| **序号** | **指标项** | **技术指标** | | | **指标要求** |
| --- | --- | --- | --- | --- | --- |
| 1 | **系统要求** | 操作系统支持 | | | 支持windows 2000/XP/2003/vista/7/8/10等系列操作系统，支持windows2003/2008等服务器系列，包括32/64位系统 |
| 系统架构 | | | 支持C/S架构 |
| 系统部署 | | | 1、服务器支持地区分布式级联部署，实现跨区域管理； 2、服务器支持集中式部署，分区域进行管理； 3、客户端支持跟准入联动下载安装、手动安装、域脚本安装、管理员远程安装等方式； 4、支持与AD域/LDAP结合，实现组织架构同步； |
| **★**许可数量 | | | 授权许可数量≥2000 |
| 管理模式 | | | 1. 支持按“计算机模式”和“用户模式”进行管理； 2. 支持终端服务器、云桌面、虚拟化等工作模式； |
| 2 | **基础框架** | 机构分级管理 | | 账户管理 | 管理员分级管理，超级管理员可以新增下级管理员，并对下级管理员的管理范围和权限进行分配。 |
| 机构管理 | 可以针对系统内计算机、员工和机构进行管理。每个计算机对应着一个员工，并对应相应的机构。 |
| 机器管理 | 设置录入终端机器信息，监控终端机器在线情况 |
| 基本报警 | | 资产异动报警 | 可统计计算机基本信息，包括：计算机名称、IP/MAC地址、操作系统、当前状态、离线天数、开机时间、最后在线时间、最后活动时间、安装时间、最后登录用户等。 |
| 程序违规访问报警 | 对违规程序使用行为进行自动报警。 |
| 客户端管理 | | 客户端控制 | 可对客户端计算机进行锁定、解锁、关闭、注销、重启及发送通知消息等。 |
| 客户端密码设置 | 可以设置客户端的管理密码 |
| 与准入基本联动 | | | 需要配合使用准入设备 |
| 3 | **终端桌面管理模块** | **资产管理** | **★**硬件资产管理 | | 管理者可以查询硬件资产统计报表，自动收集硬件资产的变更情况。包括CPU、内存、硬盘、打印设备、串口设备等。可以对于硬件资产信息进行自定义操作，包括设置维保日期，责任人，机器品牌，配备时间，配备方式。 |
| 软件资产管理 | | 管理者可以查询软件统计报表，自动收集软件的变更情况。可以统计安全软件名称、安装日期、版本号、发布者 |
| 资产异动报警 | | 当客户端硬件资产出现变动时，管理端会即时报警。支持软件界面报警和邮件报警 |
| 杀毒软件检测 | | 管理员可以按计算机模式查看所有客户端的杀毒软件状况，包括是否安装杀毒软件、杀毒软件状态、杀毒软件版本号等。 |
| Windows服务 | | 查看客户端的windows服务状况，可以设置WINDOWS服务端状态，如禁用、启用服务等。可以禁止、禁用、启用服务 |
| **程序管控** | 程序访问控制 | | 管理者可以设置员工禁止访问的程序。可以根据动态链接库名称对于程序使用进行控制。也可以根据程序的MD5进行控制 |
| 黑白名单管理 | | 管理员可以设置进程黑名单禁止访问程序；也可以设置白名单允许运行的程序； |
| 应用程序统计 | | 可以形成多种类型的程序统计报表。包括访使用程序最多的前20名的计算机、使用次数最多的程序前20名，使用时间最多的程序前20名。形成饼状图、柱状图和列表 |
| 程序违规访问报警 | | 对违规程序使用行为进行自动报警。 |
| 程序MD5搜集 | | 客户端开机可以自动搜集网络内部程序的MD5值，上传到服务器，形成MD5库 |
| 进程运行管理 | | 可以查看客户端正在运行的程序 |
| **设备管控** | U盘管理 | | 可以设置禁止使用U盘，可以为U盘设置只读，只写权限。U盘插入报警。对于鼠标键盘等USB非存储设备不禁用。支持制作注册U盘，制作后的例外U盘，可以在单位内部按权使用。 |
| 保密U盘 | | 支持制作保密U盘，制作好的保密U盘只能在认证的计算机中使用，插入到任何非认证的计算机都不能使用。 |
| 禁用光驱 | | 禁止客户端使用光驱 |
| 禁用外设 | | 禁止终端计算机使用软驱，光驱，红外，蓝牙，MODEM，声卡，COM口，禁用图形图像设备，禁用便携式设备，禁用无线网卡。 |
| 禁止使用打印机 | | 禁止使用打印机，或者只允许使用制定的打印机。 |
| **打印管控** | 打印内容备份 | | 可对打印内容进行备份，以图片形式进行备份 |
| 水印控制 | | 可自定义打印文字浮水印功能 |
| 支持对各类打印机（包括本地打印、网络打印、共享打印、虚拟打印）进行水印控制 |
| **文档安全管控** | 文件外发控制 | | 客户端会自动记录用户文档外发行为。包括QQ外发、USB外发、浏览器外发等，同时可以记录外发的源文件。禁止用户通过浏览器外发文件。禁止QQ外发文件。禁止阿里旺旺外发文件。禁止MSN外发文件。禁止U盘外发文件。禁止拷贝文件到USB设备。禁止拷贝文件到共享目录。禁止拷贝文件到网络硬盘。禁止从USB拷贝文件到本地计算机。禁止从共享目录拷贝文件到本地计算机。从网络硬盘拷贝文件到本地计算机。限制USB设备拷贝文件的大小。 |
| 文件删除操作备份 | | 支持对设定文件在删除前进行备份，防止文档破坏并保留证据，并可对备份文件大小进行设置 |
| **网络管控** | IP地址禁用 | | 管理员通过设置IP地址范围设置，禁止对特定IP地址的访问。 |
| 端口禁用 | | 管理员可以设置禁止员工访问的端口 |
| 非法IP接入报警 | | 可以发现网络内是否有非法（非授权）计算机接入 |
| 网络使用控制 | | 管理员可以设置指定的计算机禁止访问外网。内网访问不受控制。 |
| 实时网络状态 | | 可以查看每台计算机的网络状态，包括使用协议、本地地址、远程地址、本地端口、远程端口、当前状态、占用进程、进程ID等信息 |
| **流量管理** | 实时流量查看 | | 管理者随时查看当前时间网络内所有客户端的实时流量 |
| 历史流量 | | 可以详细记录员工任意时段的使用的外网流量。 |
| 流量控制 | | 可以设置企业内部网络的连接Internet网络的流量，包括总流量、上行流量和下行流量。 |
| 4 | **终端远程运维管理** | **★补丁管理** | 可以自动在服务端下载补丁，识别客户端需要安装的补丁，然后将补丁推送给客户端进行安装，并对于安装状态进行统计。该功能不接受第三方模块集成。管理员可以设置安装补丁的分组，也可以设置补丁推送的速度和时间。可以显示客户端的当前漏洞数目和漏洞和漏洞明细。可以以折线图的方式展示过去5天内的每天发现的漏洞数量和修复的漏洞数量。 | | |
| **操作系统维护** | 系统盘自动还原 | | 对于终端计算机提供系统盘还原功能，每次计算机重启，对于系统盘的写入信息，全部丢弃，系统盘恢复原状。 |
| 操作系统备份/还原操作系统 | | 管理员可以向终端计算机发送命令，实现远程备份操作系统，生成备份文件。该备份文件可以存储在服务器上，并可以将该文件直接给相同配置的终端计算机进行系统还原，该功能支持磁盘为UEFI启动方式启动，该操作只在管理段进行，无需在客户端进行任何操作。 |
| **系统运维** | 开机启动项 | | 查看并管理开机启动项 |
| 开机时间统计 | | 可以统计计算机使用时间最长的前二十名计算机，详细计算出每个计算机的开机时间。成饼状图、柱状图和列表。 |
| 虚拟工作桌面 | | 终端登录后自动进入用于工作的虚拟桌面，虚拟桌面中的内容与功能可以定制。包括定制虚拟桌面中的会计方式，以及快捷方式在桌面的第几列，第几个 |
| 系统用户 | | 可以查看终端计算机的系统用户 |
| 共享目录 | | 查看客户端的共享目录情况。 |
| 磁盘信息 | | 查看客户端的磁盘信息，可以设置磁盘空间小于一定的磁盘大小时，系统及时报警。 |
| 窗口信息 | | 查看客户端的窗口信息，管理与可以对与非常规窗口进行远程关闭。 |
| 终端权限控制 | | 终端计算机禁止修改MAC、禁止使用任务管理器、禁止使用添加删除程序、禁止进入安全模式、禁止使用注册表 |
| **远程管理** | 远程执行命令 | | 管理员可以对远程计算机执行命令 |
| 远程电源管理 | | 对远程计算机执行开机、关机、重启、注销等操作 |
| 文件分发 | | 管理员可以对远程计算机进行文件传送。可以自定义文件分发位置。支持多人传送。以任务的形式提交到服务器，对于在线的计算机立刻分发，对于不在线的计算机，开机后自动执行分发任务 |
| 软件安装 | | 管理员可以对计算机实行远程推送安装软件。以任务的形式提交到服务器，对于在线的计算机立刻安装，对于不在线的计算机，开机后自动执行安装任务 |
| 系统信息 | | 管理端可以查看客户端的系统信息、IP地址、MAC地址、客户端版本号。 |
| 远程文件传送 | | 支持远程文档传输，提供管理控制台与客户端相互传送文件的功能 |
| 发送消息 | | 管理员可以给终端计算机发送消息，支持批量发送。 |
| **屏幕监控** | 屏幕快照 | | 可以查看整个部门当前屏幕快照。 |
| 远程屏幕协助 | | 管理员可以远程监看或者控制客户端的计算机。当对终端计算机进行远程控制时，可以锁定终端计算机的鼠标。 |
| 多屏墙 | | 管理员可以实时查看多个计算机的电脑屏幕，最大支持64屏同时监看。 |
| 5 | **网络准入控制** | **网络准入设备配置要求** | ★配置 | | 1U机架式结构，带2组bypass，SAST-500G，单电，标配6个10/100/1000Mbps千兆，RJ-45端口，1个可插拨的扩展槽 |
| **★**性能 | | 采用嵌入式Linux系统，并发数≥100000；最大吞吐量5Gbps,，支持Bypass功能 |
| **功能** | 接入方式 | | 设备支持干路接入、旁路接入、策略路由方式接入。 |
| 网络访问隔离 | | 可以在内网设备不同的组，不同组之间的网络是不可以互相访问的。没装客户端的计算机不能访问装了客户端的计算机。 |
| 合规检测 | | 系统自带默认安全合规检测库：操作系统版本检测，系统防火墙开启检测，来宾帐户检查，系统垃圾文件检查，系统共享检测，机器名称检测检测；软件合规包括本地安装软件检测，本地安装软件库的管理，支持软件安装检测的黑白名单管理及检测。不符合规则的终端不能入网。在入网后，计算机使用的过程中，合规检测也及时生效，在这个过程中，当发现终端计算机合规检测不合格时，立即阻止终端接入网络，同时在终端计算机上有详细的违规信息弹窗提示，在系统的管理界面中也有该违规信息的详细展示。 |
| 跟OSCE联动，检测OSCE版本，补丁和病毒码信息。 |
| 接入服务器控制 | | 针对单位内部服务器上的办公系统访问进行控制，没安装客户端的计算机不能访问该办公系统，可以提供WEB认证页面，输入用户名、密码，可以进行临时认证。 |
| 802.1X准入控制 | | 支持通过计算机和域用户下发加密策略 |
| Radius认证服务器 | | 软件自带自主研发的radius服务器实现用户认证，不接受调用第三方的认证服务器。 |
| Wifi白名单 | | 只允许终端设备连接单位内部wifi的SSID，具备SSID方冒充功能 |
| 访客入网 | | 对于访客入网，用户打开浏览器会自动跳到认证页面，入网者输入姓名，单位，电话及受访者姓名，部门，电话，计划入网时长，点击申请按钮提交入网审计，管理员可以在后台管理界面对于此次入网进行审批。 |
| USBKEY入网 | | 未入网用户可以插入USBKEY后入网，所有入网信息系统中有记录。 |
| 入网认证 | | 未认证的入网用户，打开浏览器会自动跳转到认证页面。管理员可以设置用户下载安装客户端入网或者通过PORTAL认证入网 |
| 用户名/密码入网 | | 管理者可以添加或者导入用户名、密码，终端使用者输入正确的用户名、密码即可入网。 |
| AD域账号入网 | | 管理者设置好域服务器的IP、端口、域名等信息后，终端用户可以输入域用户名、密码，准入设备与域服务器联动，认证输入的用户名、密码，认证成功即可入网。 |
| 入网信息查询 | | 管理员可以查询所有入网用户的信息，包括：姓名、部门、入网时间、入网认证方式（用户名/密码、UKey认证，手机短信认证，指纹仪认证）等信息。 |
| 审批信息查询 | | 管理员可以查询所有访客申请入网信息以及审批信息。包括：入网者姓名、单位、电话，受访者姓名、部门、电话，审批者信息等。 |
| 6 | ★资质要求 | | | | 产品具有公安部销售许可证 |
| 7 | ★授权和服务要求 | | | | 不少于3年原厂售后服务，服务级别7x24，要求出具原厂盖章的授权函和服务承诺函。 |

## 2.WEB防火墙(1台)

|  |  |  |
| --- | --- | --- |
| **序号** | **技术指标** | **指标要求** |
| 1 | ★品牌 | 启明星辰、铱迅、绿盟 |
| 2 | 系统架构 | 采用专用机架式硬件设备。专业WEB应用防护设备，非OEM、NGFW、NGAF等下一代防火墙或UTM安全网关产品。 |
| 3 | ★接口数量 | 标配千兆电口≥6个，支持4进4出，2路同时防护，带2路电口BYPASS |
| 4 | webshell扫描工具 | 提供同品牌windows平台webshell检测工具一套搜索网站里面的网页木马，并生成统计报表。 |
| 5 | ★性能要求 | 吞吐量≥2000Mbps |
| 单向应用层（HTTP）吞吐量≥1000Mbps |
| 最大并发会话数≥50万 |
| HTTP请求速率≥12000次/秒 |
| 网络延迟≤0.06毫秒 |
| 不限防护网站数量 |
| 6 | 部署方式 | 支持纯透明部署，需即插即用（无需绑定域名、IP及端口号）即可防护 |
| 支持端口汇聚（Trunk），显著提高设备间的吞吐能力 |
| 7 | 安全特性 | 能够同时支持IPv6/IPv4环境下的攻击检测和访问策略 |
| 支持隐藏Web服务器的类型名称 |
| 支持对恶意扫描行为开启防扫描功能，用户可自定义防护等级。 |
| 支持任意碎片组包、支持超长报文组包设置，功能界面上可以对报文大小优先进行设置。（报文大小设置不低于30M） |
| 8 | 攻击防御手段 | 支持多虚拟web主机同时防护 |
| SQL注入攻击：攻击者通过输入数据库查询代码窃取或修改数据库中的数据 |
| XSS跨站攻击：跨站脚本攻击利用网站漏洞攻击那些访问该站点的用户，常见目的是采取窃取该站点访问者相关的用户登陆或认证问博信息 |
| 关键文件下载：攻击者通过工具或特殊命令下载网站系统的数据库文件、配置文件信息 |
| 木马上传：攻击者利用黑客工具上传Webshell以达到控制服务器的目的 |
| 具有智能化阻断功能：基于智能用户行为识别的动态防护机制，识别并彻底阻断黑客的攻击行为 |
| 关键字过滤：支持敏感关键字过滤功能，用户可自定义关键字内容 |
| 支持备案检查功能：检测网站的ICP备案情况，对于通过备案网站优先放行，未通过备案才禁止访问。 |
| 支持数据库防篡改功能，无需安装任何数据库代理插件。 |
| 智能防扫描功能：通过扫描器“行为特征”智能判断扫描器 |
| 网站统计功能：能统计每天不同时段后端防护网站各个时段的访问博次数、攻击次数并绘制成图表 |
| 9 | 交互式统计视图 | 可以生成攻击访问地域视图，可按国家、省份、市交互式呈现。统计客户端访问来自于哪些搜索引擎、搜索词以及访客排行，以便用户更好的了解自己网站的访问信息 |
| 10 | 报表功能 | 安全报表（入侵统计、按入侵类别统计、被攻击主机、攻击来源IP和地理位置、页面访问次数、网络接口流量趋势） |
| 报表中可以统计URL访问的次数，可记录最后访问者的浏览器类型者 |
| Webshell提示：生成的报表中需提供对防护Web网站中已经存在Webshell文件的告警功能 |
| 11 | 管理功能 | 提供接入即防护的能力 |
| 针对高级用户，对于访问控制、防篡改等功能，支持灵活时间段的计划任务 |
| 支持基于HTTPS的B/S管理 |
| 12 | ★资质要求 | 产品具有公安部销售许可证。 |
| 13 | ★授权和服务要求 | 不少于3年原厂售后服务，服务级别7x24，要求出具原厂盖章的授权函和服务承诺函。 |

## 3.日志审计(2台)

|  |  |  |
| --- | --- | --- |
| 序号 | 技术指标 | 指标要求 |
| 1 | ★品牌 | 启明星辰、铱迅、绿盟 |
| 2 | ★硬件规格 | 软硬件一体化产品，采用专用千兆多核硬件平台和安全操作系统； |
| 标准1U机架设备 |
| 设备标配6个千兆电口，2TB存储空间；此次包含30个审计对象授权； |
| 3 | ★性能要求 | 采集性能≧4000条； |
| 4 | ★功能要求 | 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； |
| 针对文本格式的日志采集，支持本地文件、Windows共享和FTP获取三种采集方式； |
| 支持日志范式化，实现对异构日志格式的统一化；在范式化的时候能够对日志进行分类，分类需按照安全事件的类型，而不是日志的设备类型，并提供日志分类的类型清单； |
| 支持加密压缩方式转发，定时转发； |
| 可实现统计计数关联，能够设定一段时间内的事件发生次数的阈值，还能指定重复事件的属性特征，提供截图证明； |
| 根据需要结合应用场景，系统可重定义关联事件中一个或多个字段的值，比如某些原始事件触发了某一关联规则而产生新的关联事件，原本是一个自动不可干预的过程，关联事件重定义可以凭借安全专家经验，重定义及补全像事件类型、事件名称、摘要描述信息，起到修正、补正信息的作用； |
| 告警动作支持告警重定义、弹出提示框、发出警示音、发送邮件、发送SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送Syslog等方式；。 |
| 提供丰富的报表管理功能，提供自定义报表，用户可根据自身需要进行定制；报表可根据设置生成日报、周报和月报。 |
| 系统内置内置Cisco PIX和交换机的事件编码知识库、Windows、Linux、Solaris、AIX操作系统的事件ID知识库、Oracle、SQL Server、MySQL、Informix、DB2数据库的事件编码知识库。 |
| 5 | ★产品资质 | 产品具有公安部销售许可证。 |
| 6 | ★授权和服务要求 | 不少于3年原厂售后服务，服务级别7x24，要求出具原厂盖章的授权函和服务承诺函。 |

## 4. 运维平台

|  |  |  |
| --- | --- | --- |
| 序号 | 技术指标 | 指标要求 |
| 1 | 系统架构 | 1、综合运维平台的所有微服务组件全部支持多副本运行，具备负载自动均衡、弹性负载、运行状态监控、故障自动定位、无感知快速升级、故障服务自动拉起等功能  2、综合运维平台聚焦于异构系统、异构数据的统一收集、标准化、存放、以及查询分析，为用户提供实时在线分析平台. |
| 2 | 页面管理 | 1、系统可自定义各类业务面板，通过拖拽的方式实现各种Portal自定义配置，并可自定义页面的刷新频度。  2、系统需具有一键换肤功能，根据应用场景不同可一键切换界面背景、图表配色、主题样式。  3、系统应可自定义组件内容、组件布局，组件标题文字可编辑。提供用户将自己创建的页面分享给指定角色人员或指定用户。 |
| 3 | ★智能资产管理 | 1、系统应具有对网络设备、无线设备、主机、数据库、中间件、应用、机房环境资源、虚拟机设备、存储设备的一体化管理，并能实现各IT资源的相互影响分析管理及联动系统需自动发现单个和多个资产并自动生成拓扑关系，可采集IT资产本地日志文件和物联网资产运行状态。  2、系统具有对各主流厂家各平台的主机、服务器、有线无线网络设备、数据库、中间件、邮件服务、WEB服务、虚拟化、存储、物联网等资产的运行状态、告警信息和日志进行统一采集，并对其他标准协议设备提供扩展对接支持。  3、具有对主流的思科、锐捷、华为、华三、中兴、Juniper、HP等主流网络设备的监控。具有对网络设备的可用状态、性能指标、配置指标和信息指标进行监控，具有对CPU利用率、内存利用率、ping时延、发送广播包数、广播包速率、吞吐量、总流量、网卡数量、电源类型等进行监控。  4、系统可以显示资产的名称、类别、IP、厂商、位置、维保时间、管理员、告警次数、资产编号等信息，提供类别、位置、告警三种列表模式并具有快速搜索、批量维护、批量关注，协助对各类资产的统一监控、统一管理。  5、系统需配置多种资产关注主题，可自定义关注的资产、可对资产的告警按严重程度和发生频次进行归纳排序、可显示资产调拨变更的状态。  6、具有对主流的思科、锐捷、华为、华三的WLan、AC、AP等无线设备进行监控包括设备配置信息、热点用户数、退服率等。系统需具有对资产采集并显示资产详细的基本信息如可用性、性能、配置、进程、分区、端口、在线用户、表空间、告警、变更等  7、系统需具有资产变更记录，对资产的维修、调拨、迁移、延保、报废全过程的事件记录和查询，直接通过资源管理、告警可以关联相关资产变更记录、信息。  8、系统提供对物联网资产管理功能，可实现对各物联（视频、门禁、安防报警、机房监控、电动窗帘、投影幕、照明等）系统运行状态的自动监控，通过物联网网关可以实时采集系统的运行状态、开关状态、实时数值、布撤防情况、触发报警、故障、日志等信息。 |
| 4 | 拓扑管理 | 1、系统需提供斜30度透视基于集成电路排线效果的拓扑展示方式，可清晰的描述有线、无线、物联网设备的层级连接关系、运行状态，可灵活配置设备详细运行指标。  2、系统需提供斜30度透视基于集成电路排线效果的拓扑展示方式，可清晰的描述业务系统与中间件、数据库及应用服务器、交换机之间的连接关系及详细指标，可自动进行拓扑连线。  3、系统拓扑需实时反应资产的告警状态以及故障后对其他设备、业务、链路的影响范围。 |
| 5 | 告警管理 | 1、系统具备统一的告警管理平台，告警需提供基于告警级别、资产类别、资产位置等类型，便于运维人员快速识别告警信息。  2、系统需根据不同资产的各自特性，灵活配置告警的触发和阈值；  3、系统需配置多种告警关注主题，可以反映出资产告警的时间分布、级别分布、类型分布和位置分布等。  4、系统需具有邮件、手机APP、微信自动故障事件推送  5、具有告警搜索，可在告警界面对需要关注的资产进行快速搜索，了解该资产的历史告警信息、发生告警时该资产的关键指标、当前资产的同类告警信息及其他指标告警信息，方便运维人员快速了解资产的故障情况。 |
| 6 | 报表管理 | 1、系统需提供多种报表模板，如资产指标模板、资产分析模板、资产SLA模板、资产运行趋势模板、资产位置模板、排序模板等。  2、系统需提供多种报表主题，如资产统计报表、资产指标报表、告警统计报表等 |
| 7 | ★配置要求 | 1、为保证系统运行的稳定性，系统需部署在Linux环境上。  系统包含括全息发现架构引擎、智能资产管理、异常告警管理、智能关系图谱等功能。  2、配置高资监控授权节点：123个（包括智能整机设备、智能工控设备、网关设备、主机、数据库、中间件等）  3、配置网元监控节点授权数70个（包括交换机、路由器、防火墙等）。  4、配置存储阵列监控授权：7个  5、配置低资产管理授权100个，包括环境传感、智能基础设施（照明、窗帘、门禁、插座等）、穿戴设备、车载智能终端、无线AP、电器等 |
| 8 | ★授权和服务要求 | 不少于3年原厂售后服务，服务级别7x24，要求出具原厂盖章的授权函和服务承诺函。 |