**信息化基础设施建设**

信息化基础设施建设作为承载平台运行的软硬件和网络设施，基于二职已经建设的基础上进行补充必要的建设和对学院老校区原有信息化相关设备和平台进行系统集成，保证学院信息安全和信息化建设的基础。详见附件说明

1、IPS 入侵防御系统

|  |  |  |  |
| --- | --- | --- | --- |
| **指标项** | **规格要求** | **数量** | **推荐品牌** |
| ★硬件配置要求 | 具备8个千兆电口，16个千兆光口，支持2个扩展插槽，可扩展万兆端口，并含2个高速USB2.0接口，1个RJ45串口 ，提供设备配置的实物图片提供设备配置的实物图片，配置冗余电源； | 1套 | 迪普、安恒、深信服 |
| 性能要求 | 应用层吞吐量≥2Gbps |
| 并发连接数≥320万 |
| 每秒新建连接数≥8万 |
| 架构 | 根据机房机柜资源实际情况，要求设备≤1U架构，提供设备安装手册说明 |
| 设备生命周期 | 投标产品必须为现有平台销售产品，并在制造商官方网站上能找到相对应的投标产品型号（提供官网截图及链接并加盖公章） |
| 安全态势 | 要求所投产品厂商密切关注全球的安全态势，以安全周报的形式进行通告，提供官网链接及截图证明。 |
| 部署方式 | 支持透明、透明桥接等工作模式，透明桥接模式下可支持带内管理 |
| 基本攻击防护 | 内置IPS特征库，特征规则数量不少于5900条 |
| 可根据IT资源的类型定义保护规则，支持对操作系统、应用软件、数据库、WEB应用、浏览器、邮件服务器等IT资源进行保护 |
| 支持对漏洞利用类、恶意代码类、信息搜集类、拒绝服务类、WEB类的攻击防护。 |
| 支持IPv4、IPv6环境下的攻击检测，支持基于多种协议类型的深度攻击防御。 |
| ▲支持根据报文特征进行自定义攻击防护类型，可以灵活的定义特征流的出入方向、协议类型（需提供产品配置截图证明，并加盖原厂鲜章） |
| DDoS攻击防护 | 支持IPv4、IPv6环境下对每个IP的新建速率设置阈值并进行监控，支持对SYN Flood、UDP Flood、ICMP Flood等攻击设置防护策略 |
| ▲支持对会话生成确认时间和会话维持时间参数进行调整，以优化系统资源利用率，避免设备本身被拒绝服务攻击（需提供产品配置截图证明，并加盖原厂鲜章） |
| ▲具备DDOS自定义指纹防护，可根据报文长度、TTL值、源目的端口和IP、序列号、flag标记等指纹信息构成的正常流量模型进行防护（需提供产品配置截图证明，并加盖原厂鲜章） |
| 防病毒 | ▲集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于10000条（需提供产品配置截图证明，并提供与防病毒厂商的合作证明，并加盖原厂鲜章） |
| 网络特性 | ▲可以在IPv4/IPv6双栈、MPLS等复杂网络环境下良好的工作，可以识别并检测QinQ、PPPoE、MPLS、GRE、Vlan等特殊封装的网络报文，具备面向下一代网络的各种特性（需提供产品配置截图证明，并加盖原厂鲜章） |
| 攻击取证 | 支持攻击取证功能：支持查看攻击事件明细，分析攻击源目的IP及端口，并可针对攻击事件分析攻击报文内容，便于分析提取关键攻击特征（需提供产品配置截图证明，并加盖原厂鲜章） |
| 系统功能 | 系统具备健康状态异常告警机制，发现异常状态时可通过邮件、短信等各种方式及时通知管理员，告警触发条件可设置； |
| ▲支持基于物理接口或vlan配置虚拟引擎，每个虚拟引擎能够根据用户业务需要分配吞吐量、CPU使用率、内存使用率等资源，且可由超级管理员分配独立的用户名和密码，独立用户登录后可配置防护策略（需提供产品配置截图证明，并加盖原厂鲜章） |
| ▲IPv4、IPv6环境下，设备可以作为NTP时钟同步可Server提供Server、Client两种模式（需提供产品配置截图证明，并加盖原厂鲜章） |
| 报表展示 | ▲支持攻击取证，可以基于攻击事件、攻击时间等维度查询具体的攻击事件明细，并可获取到相应攻击的报文内容，便于分析攻击特点（需提供产品配置截图证明，并加盖原厂鲜章） |
| ▲系统应具备地址簿功能，在报表中可直观显示所有攻击事件的攻击源IP所处省份或某个运营商等信息（需提供产品配置截图证明，并加盖原厂鲜章） |
| 日志管理 | 支持网管软件统一网管，支持SNMPv1，SNMPv2c和SNMPv3；支持通过SNMP用户进行认证，支持认证加密和数据传输加密功能； |
| ▲支持告警和日志管理功能：支持攻击事件触发告警、支持告警通知（短信，邮件、声音）、支持告警过滤、支持自定义日志存储时间、支持告警日志和操作日志支持转储功能（提供需提供产品配置截图证明，并加盖原厂鲜章） |
| 设备管理及运维 | 支持病毒库、特征库平滑升级，在设备运行时，升级病毒库、特征库不会导致网络丢包。 |
| 产品资质 | 具备国家版权局颁发的《计算机软件著作权登记证书》； |
| 具备国际CVE兼容证书 |
| 具备IPv6 Forum《IPv6 Ready Logo Phase-2证书》 |
| 公司资质 | ▲具备中国信息安全测评中心颁发的《信息安全服务资质-安全工程类二级》资质； |
| ▲为确保设备系统稳定安全，需提供CMMI5软件成熟度证书证明 |
| 具备中国信息安全认证中心颁发的《信息安全应急处理一级》资质； |
| 具备中国国家认证认可监督管理委员会颁发的《ISO14001：2004（GB/T24001-2004）环境管理体系认证》资质； |
| 具备通信企业协会颁发的《风险评估一级》资质； |
| ▲信息安全设备、系统软件的开发、生产符合TL9000-HS R5.5/R5.0标准，提供相关证明； |
| 国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（一级） |
| 售后服务 | ★提供原厂三年技术支持以及保修服务，中标后提供原厂商针对本次项目的授权书和售后服务承诺函。 |
| 生产厂商在省内有售后服务人员及机构（需提供相关证明），并设有产品备件库，厂家能够提供快速本地化现场技术支持10分钟内响应，提供7\*24小时技术服务支持 |
| ★其他 | 中标后七个工作日内需提供样机对上述功能进行逐一测试，测试通过后才能执行合同流程，测试中若发现有虚假应标行为，业主保留追究法律责任的权力 |

2、日志管理综合审计系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指标名称 | 指标项 | 详细描述 | 数量 | 推荐品牌 |
| 资质要求 | 产品资质 | 1. 提供产品的《计算机软件著作权登记证书》； 2. 国家公安部计算机信息系统安全专用产品销售许可证； 3. 通过国家保密局涉密信息系统产品认证； 4. ISCCC国家信息安全产品3C证书（增强型认证）； 5. 产品必须是自主研发而不是OEM产品； | 1套 | 思福迪、谐润、金电网安 |
| 厂商资质  要求 | 1. 拥有省级以上高新技术企业资质； 2. 通过ISO9001:2008质量管理体系认证； |
| 系统架构 | 产品结构 | 要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁； |
| 产品架构 | 采用标准1U机架式硬件； |
| 操作系统 | 深度定制优化的Linux系统； |
| 管理方式 | B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 设备部署 | 提供旁路接入模式，设备部署不影响原有网络结构； |
| 数据存储 | 1. 所供系统设备必须自带本地存储功能； 2. 提供专业的高性能日志及行为审计系统的技术先进性证明； 3. 提供基于海量日志专用存储的文件系统著作权证书，禁止采用通用关系型数据库来存储日志； 4. 物理磁盘空间≥1TB；日志存储量至少十亿条；（指标以原厂公开资料为准）； 5. RAID架构以保证数据可靠性,（指标以原厂公开资料为准）； 6. 支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)； |
| 网络接口 | 1. 至少提供千兆RJ45\*4（三路数据传输口；一路系统管理口）； 2. 网络接口支持电口，可升级为光口； |
| 处理性能 | 日志采集能力：5000条/秒以上 |
| 功能要求 | 数据采集 | 1. 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]； 2. 支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神] 3. 支持Opsec Lea日志采集；（提供产品页面截图证明） 4. 支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控； 5. 支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储；（提供产品页面截图证明） 6. 支持文本型日志原始文件管理，可将系统作为日志服务器使用；（提供产品页面截图证明） 7. 支持FTP行为审计并提供FTP二次登陆系统及实现文件传输和过程监控的方法技术先进性证明； 8. 支持Telnet行为审计并提供一种安全终端仿真协议监控时实现会话复制和跟踪的方法技术先进性证明； |
| 基本功能 | 监控功能 | 1. 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况； 2. 支持自定义配置实时监控的日志类型； 3. 支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警； 4. 支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况； 5. 支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作； |
| 报表分析功能 | 1. 系统内置多种类报表模板； 2. 支持动态\静态（日报、周报、月报）两种系统生成方式； 3. 支持报告的邮件转发、生成提醒功能；支持多人邮件接收； 4. 支持自定义审计报告； 5. 支持导出html、Excel、PDF； 6. 支持管理员自定义审计报表模板；（提供相关产品截图证明） |
| 查询分析功能 | 1. 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；（提供产品页面截图证明） 2. 支持以日志类型、时间范围及条件字段快速检索过滤； 3. 支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询； 4. 支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件； 5. 支持查询模版创建、修改、删除功能；（提供产品页面截图证明） 6. 支持查询结果导出； |
| 策略管理功能 | 1. 支持内置归并策略，对HTTP数据进行自动归并处理；（提供产品页面截图证明） 2. 支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件； 3. 支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问；（提供产品页面截图证明） 4. 支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略； 5. 规则条件设定支持逻辑运算符与支持正则表达式；（提供产品页面截图证明） 6. 支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；（提供产品页面截图证明） 7. 支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息； |
| 数据管理功能 | 1. 支持按日志属性、日志类型、时间范围进行数据备份；（提供产品页面截图证明） 2. 支持WEB界面备份及日志恢复导入工作； 3. 支持自动与手动两种备份归档方式； 4. 系统支持以FTP上传方式将归档文件存储到第三方存储系统中；（提供产品页面截图证明） |
| 系统配置功能 | 1. 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）； 2. 支持资产管理，即所有采集日志源管理维护； 3. 支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略； 4. 支持证书页面生成下载； 5. 支持系统配置备份恢复； 6. 支持时间同步页面配置； 7. 支持页面方式系统升级以及设备关闭、重启； 8. 支持从WEB界面查看网卡IP设置，修改静态路由设置等内容； 9. 支持安全页面（SSL）证书下载；（提供相关产品截图证明） |
| 系统安全 | 系统自身安全 | 1. 系统内置安全防火墙；支持控制访问审计主机范围； 2. 必需提供内部通讯检查机制，传输128加密； 3. 管理接口支持串口或电口的方式管理； 4. 管理界面与其他功能模块分离； |
| 日志数据安全 | 1. 审计日志文件方式存储； 2. 审计日志加密导出审计系统； 3. 支持对所有审计管理员操作审计系统的动作进行审计； |
| 日志权限 | 1. 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；（提供产品页面截图证明） 2. 支持日志类型、IP地址权限设置； 3. 支持页面功能模块权限设置； |
| 其他要求 | 系统升级 | 1. 在设备维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本； |
| 系统许可方式 | 永久许可方式，再增加审计用户的情况下不用增加授权许可； |
| 产品授权及服务 | 1. 提供原厂三年7\*24小时的售后服务承诺； 2. 提供三年原厂保修及原厂免费现场服务，产品的安装、培训由原厂工程师完成实施。 |

3.灾备存储一体机

|  |  |  |  |
| --- | --- | --- | --- |
| 产品类型 | 参数要求 | 数量 | 推荐品牌 |
| 参数要求 | 私有云存储RS3617xs+16 CPU: Intel Xeon D-1531 六核 2.2GHz，最高可超频到 2.7GHz  内存:16GB DDR4 ECC  内部硬盘数:8T X 5块 ，自带M.2 SSD缓存加速卡和500G缓存加速盘2块;  最大外部扩展:支持外接二个12硬盘位扩展柜,支持到最大36硬盘槽位;  硬盘热拔插:支持硬盘热拔插  RJ-45 1GbE 网络接口数 4 个 (支持 Link Aggregation / 故障移转)  无线网络:支技外接USB无线网卡  10G网卡扩展支持:支持扩展万兆光纤网卡  账号数:自带用户授权16000个  自带并发数:512  ISCSI:最大 iSCSI Target数：256 最大 iSCSI LUN数：512  AC输入电压 100V ~ 240V AC  尺寸:机架式  网络唤醒:Wake on LAN/WAN  电源唤醒:电源自动回复  PCIe 扩充:1 x Gen3 x8 slot (x8 link)  开关机支持定时及自动开关机  工作状态灯:网卡、电源、状态、硬盘  检查系统状态:显示硬盘、CPU、内存、带宽流量、存储及各账号使用，按日、周、月报表分析；  双机热备:支持双机热备功能(如配备俩套同样硬件情况下)、自动切换  不断电系统:支持UPS, USB/SNMP 独立模式  负载均衡/链路切换:Link Aggregation、实现对主机的多通道路径访问以及对应用透明的自动故障通道切换及负载均衡  语言:支持17种语言管理界面，支持17种语言文件应用  质保及服务:五 年保修、原厂服务；  具体功能要求:  自带文件共享  UPnP 探索服务  WebDAV 共享文件夹内直接编辑存取档案，建立私有云存储  支持 FTPS (FTP over SSL/TLS)  可以启用回收站，避免误删文件，并可设备自动定时清除  支持 SMB/CIFS、AFP 及 NFS 传输协议  电脑终端操作系统支持 MAC 、WINDOWS、LINUX  移动终端手机、平板 ,Android 、 IOS  通过网页就可访问、上传、下载文件；  ISO镜像文件存储及分享  文件夹同步  256位文件夹加密  ISCSI及虚拟化 获得VMware® Ready™ 、Citrix® Ready™ 认证支持，并兼容于Microsoft® Hyper-V™  支持 ISCSI 和Target  支持 LUN 快照技术，提升存储空间的使用效率，并且提供多一层的保护  LUN 备份服务，可直接在存储设备上进行 LUN 备份  支持 Link Aggregation、负载均衡及故障移转  具备 VMware VAAI 支持认证  备份终端支持 Windows PC 安卓和苹果端  支持支持 Apple Time Machine  支持第三方备份软件  支持做为虚拟化备份服务器  支持RTRR 或 rsync 实时远程备份  备份至外接设备  备份至远程 RTRR 服务器或 rsync 服务器  备份至云端存储  备份方式：排程备份、增量备份、自动备份，并可设备份数量  系统备份，还原系统设置并灵活可选相应的设置  支持完整的 RAID 组态设定  弹性 RAID 组态迁移  扩充期间无需暂停系统  在线 RAID 容量扩充  弹性的存储空间扩充  加强的只读模式数据保护，保护重要数据  RAID 恢复功能,避免误拔插硬盘  支持旧机到新机系统迁移，系统迁移过程，数据保持完好  系统管理 图形式的操作界面  网络浏览器管理  电子邮件及手机短信实时警示通知  自动侦测固件更新  系统资源监控  支持TFTP服务器  系统日志，（实用的系统事件纪录及联机纪录, 在线用户清单帮助访问权限设定；  支持 SSH 及 Telnet  流量控管；  利用 SNMP 协助 IT 管理  支持硬盘 S.M.A.R.T. 检查、硬盘坏轨扫描  应用服务器 网站服务器  支持 MySQL 数据库服务器  支持打印服务器  支持Directory 服务器  支持DHCP 服务器  支持VPN 服务器  支持Syslog 日志服务器  支持苹果 iTunes 服务器  支持媒体服务器  支持邮件服务器  支持RADIUS 服务器  支持DNS 服务器  权限管理: 网页式用户界面   与Windows AD环境结合  整合LDAP 目录功能  支持 Windows AD 环境  提供个人资料夹给每位网域用户 ( 主目录 )  权限管理  网络环境 可设定专属于用户的个人资料夹  支持大量用户及群组账号管理  支持 window acl  支持并可结合 RADIUS 服务，集中化管理及符合802.1x 安全机制  共享文件夹访问控制，只读、写、禁止访问，进阶文件权限设置  可以限制用户容量上限  提供 DDNS 服务  支持建立多组无线网络联机设定  可同时在IPv4 与IPv6 的双协议网络环境中运行  支持 PPTP 及 OpenVPN  多网络端口，Port-trunking，负载平衡，网络容错  网络环境  安全性 支持PPOE 拔号  SSL, HTTPS 提供安全性的档案存取与传输、连机管理  SMB 3 加密  整合防毒软件  整合防火墙，并可条件式设定自动封锁 IP  将系统服务指定到一个或多个有线或无线网络接口  支持 PPTP 及 OpenVPN  存取文档  上传档案或照片  可以移动、复制、重新命名或删除 NAS 里的档案  可通过NAS 上下载到移动设备中离线阅读  分享的档案建立下载链接，通过电子邮件或是手机短信传送给他人；您也可以直接利用电子邮件夹带档案来分享出去  支持iOS® 系列: iPhone, iPod 支持Android™ 系列: Android OS 2.3.4+ 多种远程监控模式  单一屏幕可监看最多 4 台摄像机画面  支持摄像机巡逻  智能型 PTZ（上下／左右／远近）摄像机操控  网页式管理界面  安全监控 支持众多知名网络摄像机品牌  支持H.264、MPEG-4、M-JPEG 及MxPEG格式高画质录像  手动录像  排程录像  支持电子地图  多种回放影像搜寻模式  附件工具软件  应用软件 WINDOWS MAC LINUX 安装向导  Windows 终端电脑数据备份及同步  WINDOWS MAC LINUX 安装向导,升级程序及固件  移动终端手机、平板 ,Android 、 IOS文件查阅及下载应用软件  杀毒软件 防火墙  具备附加套件（需要具备以下最低配置套件服务或更高功能）：  Antivirus Essential  Antivirus by McAfee (Trial)  Audio Station  Central Management System  Cloud Station  Cloud Sync  Directory Server  DNS Server  Download Station  Glacier Backup  HiDrive Backup  iTunes Server  Java Manager  Mail Server  Mail Station  Media Server  DLNA Compliance  Note Station  Photo Station  RADIUS Server  Surveillance Station  最大摄像机支持数 (须安装摄像机授权)为76个（本次含 2 组免费摄像机授权）  Video Station视频转码  VPN Server最大联机数 30个 | 1套 | 群晖、EMC、NETAPP |

4、机房桌面虚拟化系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 详细参数 | 数量 | 推荐品牌 |
| 1. 1 | 桌面云终端 | |  |  | | --- | --- | | 数量要求 | ★本项目要求配备60台桌面云终端，与桌面云控制平台、桌面一体机同一品牌。 | | 硬件规格 | ★ARM架构，CPU≥四核1.6Ghz、内存≥1G、存储≥4G、USB≥6个、1个VGA或HDMI、1个以太网口、1对音频口。 | | 其他要求 | 采用嵌入式操作系统，比如Android、Linux。  ★要求云终端管理控制台与桌面云控制器同一界面。  ★云终端权限管理：支持配置是否允许显示本地桌面和是否允许安装应用、支持开启“修改云终端配置和登录信息需要密码”功能、支持配置是否允许新的云终端接入或者接入需要密码。  ★云终端易用性管理：支持配置自定义开机画面、支持云终端分组管理、支持配置云终端定时开关机计划、支持开启“云终端加电自启”功能、支持配置是否自动下载并安装更新、支持批量移动/删除/关闭云终端、支持配置是否允许自动登录和保存密码。（提供功能截图）  通过CCC产品质量管理认证、节能环保认证。所有授权的软件必须正版原厂盖章。 | | 60台 | 深信服、思杰、vmware |
| 1. 2 | 桌面云控制平台 | |  |  | | --- | --- | | 配置要求 | ★为提升桌面云接入性能及稳定性，本项目要求桌面云控制平台与桌面云终端、桌面云一体机同一品牌，且提供60个VDI用户授权，支持发布专有桌面、还原桌面、池化桌面、共享桌面、远程应用至少5种桌面资源，满足不同场景的应用需求。所需软件产品为正版原厂盖章授权 | | 部署模式 | 为了简化部署环节，本项目要求桌面云控制器所有组件完全集成化，不需要过多的安装调试步骤，后台导入一个镜像就可以完成部署，提升上线效率。  ★桌面云控制器自带高可用性技术方案，在不增加第三方负载均衡工具的情况下，支持双机（主备）和集群（主主）2种模式，如果选择集群模式部署，要求桌面云控制器宕机切换会话不中断。（提供功能截图）  ★支持分布式部署、集中管理模式，桌面云一体机部署在各个分支本地数据中心，总部通过一套集中管理平台实现对分支桌面云的统一管理，包括统一授权、统一升级、统一监控等，本项目要求免费提供集中管理平台所需软件。  ★桌面控制器内置DHCP功能，部署时无需额外搭建DHCP服务器，可实现终端和虚拟机IP的动态分配。  ★支持将桌面云控制器直接映射到互联网，要求自带SSL VPN功能，不要借助第三方设备，并且能够用于固定IP线路和动态IP线路2种方式，其中动态IP不依赖第三方插件，降低部署复杂度。 | | 用户体验 | 支持PC、笔记本、云终端（含ARM和X86）、iPad、iPhone、Android移动终端等设备接入访问虚拟桌面。  支持Windows XP/7/10、iOS、Android、Linux等客户端操作系统。  支持Windows XP/7/10、Windows Server，支持两种以上的Linux虚拟桌面操作系统，其中要包含国产Linux操作系统。  ★支持池化桌面，该模式下虚拟机不固定关联给用户，当用户需要时从桌面资源池中随机获取一个闲置虚拟机，退出后自动归还（即还原到“未关联用户状态”），其他用户仍然可以使用。  ★支持PC磁盘映射，即PC本地硬盘可直接映射到虚拟桌面上使用，并可根据策略进行文件读写权限设置和数据读写审计。  ★PC（或笔记本）接入虚拟桌面支持通过导航条或快捷键切换为窗口化模式，用户可随意改变窗口大小且分辨率会自动适应。  支持USB外设映射，兼容高拍仪、扫描枪、扫描仪、摄像头、密码小键盘、指纹收集器、身份证读卡器、手写板、打印机、USB-key等不同外设。  ★支持云盘存储方案，包括个人云盘和公共云盘，可设置配额和读写权限，其中个人云盘绑定用户，只允许特定用户访问，公共云盘允许所有人访问。  支持本地、AD域等多种情况下的单点登录，用户登录VDI客户端和虚拟桌面操作系统只有1次账号密码输入动作，保持和PC使用习惯一致。  ★支持联动关机，用户可以跟使用PC一样，打开操作系统“开始”菜单、点击“关机”按钮，云终端和操作系统将会一体化关闭，没有多余的操作步骤。  ★支持针对用户应用软件的黑白名单控制。  支持显示虚拟机开关机画面；支持分辨率自适应和更改分辨率，操作时要求与PC一样，即在桌面右键点击“个性化分辨率”进行设置。  支持桌面会话保持功能，在多桌面切换、更换不同终端接入、临时性网络中断（自动重连）等情况下，用户重新登录后不会影响原先的桌面操作行为。  ★客户端连接虚拟桌面无需依赖虚拟机IP，具体表现为禁用虚机网卡或者随意更改IP，桌面会话不会中断，用户可以正常办公和播放视频，避免因误操作而导致业务中断。  支持视频重定向，视频文件不在服务器解码，直接重定向到终端本地解码，提升播放体验，能够兼容Media Player、暴风影音等多种本地播放器，以及优酷、土豆、腾讯等多种在线视频网站。  ★针对广域网接入虚拟桌面的场景可配置缓存级别、有损压缩比率、启用帧控等策略，降低流量、提升体验。（提供功能截图） | | 运维功能 | ★支持模板链接克隆，克隆时可指定虚拟机数量、运行位置、存储位置、网口信息、磁盘大小，本项目要求60个虚拟机派时间不超过5分钟。  支持在原磁盘上扩容或添加新的磁盘，扩大磁盘容量。  支持模板升级，可以统一安装所需要升级的软件/补丁，一键更新到对应的虚拟机，满足标准化场景的软件和补丁更新需求。  ★支持软件分发，通过创建软件库并关联给虚拟机，实现应用软件、驱动程序的增量式更新，不需要在每个虚拟机执行安装过程，整个分发过程秒级完成，且分发后不会覆盖原虚拟机的个性化配置和自主安装的软件，本项目要求支持应用软件、USB打印机和网络打印机驱动、网页快捷方式和页面控件、办公文件的分发。（提供使用说明和功能截图）  支持批量完成如下配置：创建用户、删除用户、禁止/踢除用户、关联虚拟机、导入导出用户、用户分组。  支持删除用户时，可选择是否删除关联的虚拟机，如果不删除，虚拟机处于闲置状态，可重新关联给其他用户。  ★支持与上网行为管理系统联动认证，用户成功登录VDI后，上网行为管理自动同步用户认证信息，后台记录用户ID, 后续上网无需再次认证登录。  支持虚拟机自由分组、支持修改计算机名称、支持虚拟机名称搜索。  支持批量删除虚拟机、批量设置虚拟机IP地址、批量关联/解关联虚拟机用户。  支持开机状态下编辑虚拟机配置，重启生效。  支持设置虚拟机开关机计划，一方面可避免并发开机IO风暴问题，另一方面可释放服务器资源，支持关机前会弹框提醒用户，如果用户正在使用不想关机可手动选择“取消”。  ★支持外置数据中心报表功能，能够查询一段时间的并发用户会话、用户使用时长、服务器负载情况、存储利用率、存储性能情况等。支持报表导出。  支持升级前和升级后的健康检查，确保升级不出问题。 | | 安全管理 | ★支持客户端准入检测，可根据用户接入的终端类型、操作系统版本、接入IP和时间、软件安装情况等条件设置接入访问策略，如客户端不满足安全检测要求则不允许接入。（提供功能截图）  ★支持USB黑白名单技术，能够精准识别每一款不同类型的外设（包括高拍仪、摄像头、USB光驱、认证key等），并设置放通或者限制策略，提高管控粒度和安全性。  ★支持多种认证方式随需组合，包括本地账号密码、usb-key认证、短信认证、硬件特征绑定、动态口令、ldap认证、raduis认证、AD域认证等多种方式，满足不同级别用户的安全接入需求。  支持设置首次登录强制修改密码、定时修改密码、图形校验码和软键盘等密码安全策略，以保障认证密码安全性，避免越权访问行为。（提供功能截图）  支持虚拟门户，不同用户通过不同地址接入虚拟桌面，适用于互联网访问场景，可以指定特定账号在外网访问桌面云，而其他用户只能在内网访问。  支持U盘、PC本地桌面到虚拟桌面这2种情况的双向拷贝管控，可控制U盘的只读和读写权限，可控制本地桌面和虚拟桌面双向拷贝、单向拷贝。  支持个人盘加密技术，对云桌面个人数据进行加密保存，保障个人隐私安全。  支持虚拟机快照技术，当数据误删或系统故障时可实现回滚，快照只保存增量数据，节省存储空间。（提供功能截图）  支持虚拟机回收站功能，避免误操作导致虚拟机数据丢失，当虚拟机删除后，会自动进入回收站，支持恢复到原位置，可设置回收站自动清理时长。  ★桌面云控制器内置防火墙，包括设置过滤规则、NAT设置、访问监控、防DOS攻击、QOS上传下载规则等。  兼容国内外多款虚拟化防病毒软件，防止虚拟机中毒。  ★支持PC防截屏，在PC利旧场景下，支持设置PC客户端桌面不能窗口化，且无法截屏。  ★支持满屏水印，水印内容颜色和边框颜色反色调设置，防止背景颜色与水印颜色一致，覆盖水印，支持水印内容、透明度、水印字体大小、倾斜度调整。  ★支持文件导出内容审计，开启文件安全导出后，虚拟机通过剪切板、PC设备和USB设备外发文件的操作将被禁止，用户可以使用虚拟机内部的文件导出工具实现文件外发，所有外发的文件内容都可以加密备份到数据中心，以备后续审计使用，可疑的导出行为会产生告警。  ★支持临时权限，管理员为部分用户临时在某个时间段内放通usb和pc剪切板等权限，并在到期后自动回收该权限，保证数据安全。 | | 其他要求 | 本项目要求所投桌面云产品厂商具备CMMI5证书（提供证书复印件加盖公章）  为保障云平台的领先性和成熟度，云平台厂商入围2016 X86服务器虚拟化基础架构魔力象限（提供Gartner魔力象限报告证明）  云厂商通过数据中心联盟颁布的可信云评估（提供相应的可信云认证报告）  要求桌面云平台厂商在温州设有直属办事处等服务机构，以便于为客户提供完善、及时的售后服务。（官网可查询网址链接、直属办事处截图证明） | | 60节点 |  |
| 1. 3 | 桌面云一体机 | |  |  | | --- | --- | | 硬件规格 | ★本项目要求桌面云一体机与桌面云终端、桌面云控制平台同一品牌，出厂时必须预装各类桌面云软件（如服务器虚拟化软件），不允许提供祼机设备，且CPU核数≥14（主频不低于2.4Ghz）、内存≥128G、千兆网口≥6个、万兆网口≥2个，冗余双电源，至少配备1块64G SSD硬盘、1块480G SSD硬盘，1块1T机械盘 | | 功能要求 | ★兼容市场上主流x86服务器和存储设备，支持品牌不局限于IBM、联想、戴尔、浪潮等。  ★单集群管理时无需部署集中管理平台，通过Web方式接入集群主服务器，实现对服务器、虚拟机、网络、存储等进行统一管理。  ★支持服务器端口汇聚技术（管理口、业务口、存储口），将多个网络端口聚合起来，提高网络带宽和容错能力。  ★支持虚拟机集中备份与恢复，可按需选择多个虚拟机或全部虚拟机备份至外置服务器（NAS、FTP、CIFS等），支持设置备份策略，实现全自动化备份。  ★支持自动/手动将配置文件备份到FTP服务器。  虚拟机损坏无法启动时，支持将虚拟机磁盘挂载到新虚拟机上，用户可登录新虚拟机将磁盘内容备份出来。  ★支持主机和磁盘故障后不停机替换。  ★支持全局热备盘技术，管理员可配置在集群中保留多块磁盘作为热备盘，分布在不同主机上，当任何一台主机的任意一块硬盘出现故障后，会自动选择其中1块热备盘进行替换和重建。 | | 其他要求 | 要求具备ISO9001质量管理体系认证证书，以确保整套桌面云方案的成熟稳定，投标时需提供资质复印件。  通过CCC产品质量管理认证。 | | 1台 |  |
| 1. 4 | 云课堂控制软件 | |  |  | | --- | --- | | 配置要求 | ★本项目要求配备60套软件授权，所提供的软件必须能够兼容本次采购的桌面云平台。所需产品为正版原厂盖章授权 | | 基本功能 | ★支持屏屏和视频广播，广播画面不需要经过学生虚拟机，可从教师机直接推送到云终端，这样不仅能够提供更流畅的屏幕广播和学生演示效果，而且能够有效节省广播流量。  支持离线教学，在这种情况下，教师机必须是物理PC，即使服务端网络中断，教师PC依然可以将屏幕广播画面推送给云终端，确保教学业务不中断。  ★支持课程切换，管理员先根据上课需求创建对应类型及数量的虚拟机（比如计算机课虚拟机、公共课虚拟机等），可通过控制台按上课时间表配置“计划课表”，实现不同课程自动化切换，也可通过电子教室软件手动选择启动对应课程的虚拟机，切换时会先关闭上一节课的虚拟机，再自动启动本节课的虚拟机。  文件分发和提交支持拖拽添加文件，可添加不同目录下的文件或文件目录。  文件分发和提交支持拖拽添加，教师或学生一次分发或提交多个文件夹或多个文件目录下的文件。  教师机对学生机可设定网络浏览、程序应用策略，对不同学生应用不同策略，策略支持开放、白名单、黑名单，任意限制或仅开放某个网页或程序，网页浏览支持QQ、IE、谷歌、360、遨游等浏览器。  ★上网限制：设定学生访问网站的黑名单或白名单，对学生可以访问的Internet站点进行管理。支持多浏览器限制，如QQ、IE、谷歌、360、遨游等浏览器。  ★程序限制：通过各种策略的应用，可防止学生在教学过程中打游戏，或使用QQ，MSN等聊天工具。 | | 课堂教学 | 学生演示：教师可选定一台学生机作为示范，由此学生代替教师进行示范教学。  分组教学：教师分派组长执行指定的功能，组长代替教师进行小组教学，小组不需要再临时创建，可以直接使用既有分组信息，教师可以监控每个分组的教学过程，以了解分组教学的进度。  分组讨论：教师可以创建多个小组进行讨论活动，并可任意选择分组加入讨论活动。同组师生支持多种方式进行交流，包括文字，表情，图片等。  文件分发：允许教师将教师机不同盘符中的目录或文件一起发送至生机的某目录下。目录不存在自动新建此目录；盘符不存在或路径非法不允许分发；文件已存在选择自动覆盖或保留原始文件。  作业提交：学生把做好的作业直接提交到教师机，方便教师批改作业要收取的麻烦。通过特殊设置，学生提交作业时必需经过教师审批通过后才可提交，教师可以选择接收和拒绝学生提交的文件。并且教师可以限制学生提交文件的数目和大小。  网络快照：教师可以在监控学生的时候，对学生画面拍快照，保存学生画面的截图。  屏幕监视：教师机可以监视单一、部分、全体学生机的屏幕，教师机每屏可监视多个学生屏幕（最多36个）。可以控制教师机监控的同屏幕各窗口间、屏幕与屏幕间的切换速度。可手动或自动循环监视。  多频道教学：支持多达32个频道的划分，一个教师可对单个班级或多个班级同时上课；多个教师可同时对多个班级进行不同内容的教学。 | | 教学评测 | 随堂小考：教师启动快速的单题考试或随堂调查，限定考试时间，学生答题后立即给出结果，结果显示学生答案柱状图分析和答题时间，可作为抢答依据。 | | 课堂管理 | 签到：提供学生名单管理工具，为软件和考试模块提供实名验证。提供点名功能，支持保留学生多次登录记录、考勤统计、签到信息的导出与对比。  班级模型：有单独的管理界面，实现对班级模型的统一管理，并能够导入、导出，调用不同网络教室中的班级模型。  ★上网限制：设定学生访问网站的黑名单或白名单，对学生可以访问的Internet站点进行管理。支持多浏览器限制，如QQ、IE、谷歌、360、遨游等浏览器。  ★程序限制：通过各种策略的应用，可防止学生在教学过程中打游戏，或使用QQ，MSN等聊天工具，  学生端属性查看：教师可以获取学生端计算机的名称、登录名和其它常用信息，并可以列出学生端的应用程序、进程和进程 ID，教师还可以远程终止学生端的进程。  系统日志：显示和自动保存系统运行过程中的关键事件，包括学生登录登出，资源不足，提交文件等。  黑屏肃静：教师可以对单一、部分、全体学生执行黑屏肃静来禁止其进行任何操作，达到专心听课目的，教师可自定义黑屏的内容与图片。  远程命令：可以进行远程开机、关机、重启等操作，远程关闭所有学生正在执行的应用程序功能。  分组管理：教师可以新建，删除，重命名分组，添加和删除分组中的成员，设置小组长。分组信息随班级模型永久保存，下次上课可以直接使用保存的分组。  ★图标监看：班级模型中可以显示学生机桌面的缩图。以定期更新，更新的快慢可由教师机程序定制，缩图显示大小也可自由设定。  自动锁屏：独有的断线保护自动锁屏技术，通过网卡的是否激活来锁定屏幕，避免学生拔掉网线违反纪律。  防杀进程：为安全起见，学生端程序运行后，防止学生通过任务管理器结束学生端程序进程来逃脱教师控制。  请求帮助：学生端遇到问题可请求帮助，教师端可远程遥控帮助学生解决问题。  远程消息：教师与学生能够使用远程消息进行交流，并可以允许和阻止学生发送文字消息。  远程设置：远程设置学生桌面主题、桌面背景、屏幕保护方案、学生的频道号和音量、学生的卸载密码，是否启用进程保护，断线锁屏，热键退出等。 | | 60套 |  |

5、waf防火墙

|  |  |  |  |
| --- | --- | --- | --- |
| 指标项 | 指标要求 | 数量 | 推荐品牌 |
| 资质 | 明御®WEB应用防火墙WAF-1000AG  \*通过公安部检测并获得公安部计算机信息系统安全专用产品销售许可证  \*中国信息安全认证中心《IT产品信息安全认证证书》  \*通过军用信息安全产品检测并获得认证证书  \*通过国家保密局检测中心检测并获得检测证书  \*原厂商注册资金不少于5000万，需提供经年检合格的营业执照副本  \*原厂商具有EAL3+资质证书  \*原厂商应具有CMMI3及以上等级资质证书 | 1套 | 安恒、深信服、思科、 |
| 规格 | 标准2U专用千兆硬件平台  标配1+1冗余电源，电源可热插拔 |
| 网口数量 | 标配：2\*GE电管理口，8\*工作口（4\*GE电口，4\*GE光口）  扩展：工作口最大可扩展16\*GE光/电口 |
| 性能参数 | 应用吞吐量不小于4000Mbps  HTTP并发连接不小于30万  HTTP新建连接(CPS)不小于3万 |
| 部署方式 | 透明桥部署：防护口不占用IP地址，实现完全透明部署，无需以先终结用户的TCP会话后再发起新的TCP会话到服务器方式处理，并支持路由不对称场景 |
| 透明代理部署：防护口不占用IP地址，实现应用层透明部署，支持TCP连接复用，并优化服务器会话处理改善服务器处理性能 |
| 端口镜像部署：镜像服务器流量即可实现安全审计和告警 |
| \*反向代理部署：可支持代理和路由牵引两种模式，客户端源IP可采用透明和非透明两种转发机制，非透明可指定字段进行识别，支持前后端口分离，支持多台WAF设备冗余和集群部署，提供界面截图并加盖公司公章 |
| \*支持虚拟化部署，支持KVM、Xen、VMWare等虚拟机环境，并支持WAF镜像导入，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告 |
| 支持链路聚合，提升网络带宽、增加容错性和链路负载均衡 |
| 支持VLAN子接口，业务口可承载多个VLAN通道 |
| 高可用性 | 支持全透明集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS |
| 保护对象 | 支持多条链路数据的防护，防护网段数量不限 |
| 支持以域名和IP多种方式进行防护 |
| 支持ipv4/ipv6双协议栈 |
| WEB服务自发现 | \*支持WEB站点服务自动侦测功能，支持自动识别VLAN信息，提供界面截图并加盖公司公章 |
| 防御功能 | 能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入、代码注入、LDAP注入、SSI注入文件注入等）、跨站请求伪造等应用攻击行为 |
| 支持对HTTP请求分割攻击和HTTP响应报文截断攻击的防护 |
| 能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |
| 能基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力 |
| 能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问 |
| 内置主流Webshell特征库，对上传内容进行检查，防止恶意Weshell上传 |
| WAF能自动识别扫描器的扫描行为，并智能阻断如Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为 |
| 内置开源CMS漏洞和WEB服务器插件漏洞防护规则 |
| 支持阻断提交政冶敏感、违反法规相关的言论信息 |
| 支持丰富的自定义规则，可以针对多个条件组合，形成深度的WEB防护规则 |
| 支持服务器隐藏，可配置删除服务器响应头信息 |
| \*内置身份证、银行卡等服务器敏感信息库，对服务器响应敏感内容进行隐藏，并支持自定义，提供界面截图并加盖公司公章 |
| 支持Cookie安全机制，支持Cookie自学习，防止Cookie被篡改和劫持，并支持Cookie Httponly |
| 智能自学习功能 | 支持网站自学习建模功能，能通过自学习形成网站URL树；  通过自学习能生成安全防护策略；  通过自学习能发现参数的名称、类型、匹配频率；  可配置匹配到自学习特征后放行；  可配置匹配不到自学习特征直接阻断请求；  \*提供界面截图并加盖公司公章 |
| 智能攻击者锁定 | 支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站  可配置攻击者识别策略和算法  可配置攻击者锁定时间  可配置将攻击者直接加入网络黑名单  可展示攻击者发生的时间和攻击者所在的地理位置  \*提供界面截图并加盖公司公章 |
| 基于时间的访问控制 | 可基于时间对客户端IP进行黑白名单控制  \*提供界面截图并加盖公司公章 |
| 防御动作 | 针对触发安全规则的行为进行阻断并发出告警页面 |
| 告警页面支持重定向至其它URL |
| 能将攻击者列入网络黑名单进行网络阻断该IP的访问 |
| 对攻击报文丢弃 |
| WEB访问行为合规 | \*可实现访问流程的校验，向网站提交表单前必须先访问指定的网页，并等待可配置的时间长度后才能正常提交表单，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告 |
| CC防护功能 | \*可根据URL、请求头字段、目标IP、请求方法等多种组合条件对CC攻击进行检测，检测指标为URL访问速率和URL访问集中度；可根据IP、IP+URL和IP+User\_Agent等算法对客户端进行检测，并支持应用层字段解析和自定义检测字段功能，支持挑战模式，支持基于地址位置的识别，支持对特定的IP地址进行CC规则白名单放行，支持CC慢攻击防护，通过学习业务流量模型，在业务流量异常时开启CC防护，并支持启动配置阈值，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告 |
| 地图态势分析 | \*按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP的访问，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告 |
| IP信誉库 | \*根据国际权威机构提供的恶意IP名单库，对恶意 IP的访问实施告警或阻断，提供界面截图并加盖公司公章 |
| 篡改监控 | 系统提供防篡改功能，能够防止被篡改内容被浏览者访问到,一旦检测到被篡改，实时发送告警信息给管理员。 |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容 |
| 能详细记录服务器响应头信息，服务器响应内容 |
| 日志分析 | \*根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率，提供界面截图并加盖公司公章 |
| 报表 | 根据PCI-DSS要求，对用户的应用进行合规性评估，生成合规报表 |
| 支持自定义报表、定时报表、支持各类导出格式（WORD,PDF等） |
| 报表可自动发至管理员邮箱 |
| 告警方式 | 支持Syslog、手机短信、邮件等多种告警方式 |
| 访问审计 | 具备审计网站正常访问流量的能力，提供按小时，日期、月份生成报表 |
| 能记录、查询所有用户对网站的访问情况 |
| 能分析出访问量最大的URL，IP地址 |
| 能分析出访问流量最大的文件类型 |
| 加速功能 | 系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，提高访问速度 |
| 支持响应内容压缩，并支持对压缩的响应内容识别 |
| SSL透明代理 | 支持HTTPS服务器的防护，可支持第三方认证机构颁发的证书链，WEB应用防火墙前端与后端均为HTTPS加密链路，实现HTTPS应用系统的防御 |
| 支持对HTTPS站点上传的公钥、私钥、证书链的内容格式进行检查，同时自动检测公钥和私钥是否配对、公钥和证书链是否配对，避免无效证书引起的业务不通的问题 |
| 一个保护站点支持上传多个域名证书 |
| \*可以选择需要支持的SSL/TLS协议版本，提供界面截图并加盖公司公章 |
| 部署在SSL网关后面，能够解析到真实的访问者IP，并能对真实的IP进行防护和阻断 |
| 移动安全运维 | 可通过移动端实现设备安全运维监控，APP具备以下功能：  支持查看当前WAF的告警数量包括最近24小时内以及总的告警数量  支持对攻击的服务器IP以及客户端IP进行统计  \*提供界面截图并加盖公司公章 |
| 智能联动 | \*支持与同品牌的APT设备进行联动，对未知威胁流量进行检测和拦截，提供界面截图并加盖公司公章 |
| 设备管理 | 规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保WAF能够针对新型的、突发型的Web攻击进行防护 |
| 支持HTTPS方式进行设备管理 |
| 设备管理采用管理员与审计员分离 |
| 操作界面支持全中文界面 |
| 支持LDAP认证 |
| 支持标准网管 SNMPv3，并且兼容SNMP v1和v2c |
| 支持NTP时间同步 |
| 服务要求 | 提供不少于三年产品原厂商质保服务，提供原厂质保函； |
| 提供不少于三年的原厂商7\*24小时上门现场服务支持； |
| 原厂商工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂商常驻浙江省内不少于7个CISP-CSE工程师（须提供杭州近三个月社保证明），以便提供快速的售后服务。 |

6、动力机房监控系统

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **动力环境监控** | 漏水监控 | 定位漏水检测器 | 采用独创双源轮检算法，可精确定位，它是通过检测前端预先在保护区范围内布好的漏水检测绳来定位漏水位置，并能发出声光报警，同时可控制一路开关信号，起到联动作用。具有RS485通讯端口，可与电脑连接，配套定位漏水软件，可在CAD图上自动定位漏水位置，并通过网络远程监控和邮件报警。  ▲采用LCD显示屏，可直接显示泄漏位置，信息直观，按键操作容易；可检测长达300米的漏水传感电缆，进行泄漏检测、定位和跟踪，精确度误差可达±0.2m，提供AOV检测证书 | 1 | 定制 |
| 15米定位漏水检测绳 | 15米长定位漏水感应绳 |
| 引出线 | 配套辅件 |
| 终止端 | 配套辅件 |
| 固定胶贴 | 固定漏水绳缆专用 |
| 智能通讯转换器 | RS485转TCP/IP以太网转换,用于将检测仪数据接入以太网传送至监控服务器。  ▲提供CE检测证书 |
| 漏水监控软件接口 | 实现漏水监控数据软件接入 |
| 温湿度监控 | 温湿度传感器 | 集成了温湿度检测，1路RS485通讯接口，面板上带LCD显示屏，可直观显示现场温湿度参数，当敏感元件被监测到环境温度、湿度，输出智能数字信号。测湿范围：5～95%RH，精度±3%RH（20%RH～80%RH）；测温范围：-20%RH～70℃，精度±0.3（25℃）  ▲提供CNAS证书 |
| 智能通讯转换器 | RS485转TCP/IP以太网转换,用于将检测仪数据接入以太网传送至监控服务器。  ▲提供CE检测证书 |
| 温湿度监控软件模块 | 实现温湿度数据软件接入 |
| UPS监控 | 智能通讯转换器 | RS232转TCP/IP以太网转换。  ▲提供CE检测证书 |
| UPS监控软件接口 | 二次应用开发，采购方协助提供UPS原厂通信协议 |
| UPS智能通讯卡 | 与采购方现有UPS型号相匹配 |
| 闭路监视及数字录像系统 | 视频监控软件模块 | SMT\_vidio |
| 通信转换模块 | NCS1-1 |
| 红外半球式摄像机 | 红外半球式摄像机，红外探头LH-905A-2 |
| 嵌入式硬盘录像机 | DS-7204HV-ST |
| 硬盘 | 2T |
| 摄像机 | DS-2CD855F-E，200万像素1/3" CMOS ICR 日夜型枪型网络摄像机 |
| 支架 | DS-1212ZJ壁装支架 |
| 机房空调监控 | 智能通讯转换器 | RS485转TCP/IP以太网转换。  ▲提供CE检测证书 |
| 机房空调监控软件接口 | 二次应用开发，采购方协助提供空调原厂通信协议 |
| 机房空调智能通讯卡 | 与采购方现有机房空调型号相匹配 |
| 智能通讯转换器 | RS485转TCP/IP以太网转换,用于将检测仪数据接入以太网传送至监控服务器。  ▲提供CE检测证书 |
| 硫化物监控软件模块 | 实现硫化物监测数据软件接入 |
| 监控平台 | LINUX嵌入式管理服务器 | ▲系统必须采用基于LINUX或UNIX类操作系统平台，由于windows系统的稳定性、容易受病毒黑客的攻击以及软件版权纠纷等原因，基于windows操作系统平台的监控系统不予考虑。  全中文B/S设计，内嵌入LINUX系统与自主研发的动环监控系统，用户使用不需要购买第三方系统版权，安全可靠。提供现场数据采集、数据处理功能，包含告警、监控、管理、报表、远程WEB查询及自诊断模块(VGA显示器接口，WEB浏览）BS架构，无需在客户机上安装任何软件，通过浏览器访问实时采集的数据；监控项历史曲线图显示，历史数据可导出为Excel文件;支持短信、语音电话、邮件、声光等报警；可通过短信查询设备实时的运行状态及数据；可集成其它基于WEB管理的设备例。方便管理人员通过内网、外网使用浏览器进行监控或管理。系统整体设计采用分布式结构，以提高系统整体工作效率，并为将来的维护和扩展提供便利。系统平台需提供专用传输网与GPRS/CDMA无线网络的两种接入方式，方便用户野外通信基站的接入。鼠标控制，操作简单，可根据现场情况定制主界面。系统软件平台各监控子系统之间相对独立，以方便维护和扩展；机房内某一监控子系统设备出现故障时需更进行维护时，无需停止系统运行，对其它监控子系统也不产生任何影响。系统软件平台应具备有日后增加设备的扩容接口能力，具有随发展变化持续扩容能力；可以在不停止监控系统运行的情况下进行监控对象的增加和监控点的增加，避免出现升级时的监控盲点。支持对服务器、交换机、数据库、存储等运行状态及属性的网管系统监控；内置视频播放器，可通过页面直接观看现场视频；与其他系统整合的技术支持与开发服务，支持二次开发，提供开放的开发接口；支持用户机房定制专用软件以及根据用户的使用习惯量身制作界面，根据机房现场实际情况的定制三维图 。▲提供商标注册、发明和外观专利、软件著作权、软件登记证书 |
|  | 零功耗备用主机 | 集成了温湿度检测、市电停电检测、1路DI（可连接消防、防盗、漏水等设备）、1路RS485，面板上带LCD显示屏，可直观显示现场温湿度参数，当相关参数出现异常时可自动拨打预设的6组电话号码，并告知具体异常内容。当相关参数恢复正常时，设备会再次拨打恢复正常通知  ▲直接通过普通电话线进行供电，无需外接电源和后配电池，零功耗节能环保，装在机房内当主机故障时，能够代替主机所有功能 |
| 其他 | 电话/多媒体语音报警模块 | 提供短信、电话线拔号/多媒体中文语音报警功能 |
| 烟雾传感器 | HM-602PC-4 |
| 声光报警器 | RS485接口进行远程管理报警 |
| 多媒体音箱 | 现场播放多媒体中文语音报警 |
| 采集箱 | 开关电源 | DC12V/8.5A直流供电，给前端设备供电 |
| 以太网交换机 | 桌面8口百兆、铁壳、每个设备箱安装1个 |
| 设备箱 | 放置传感器、电源等 |

7、系统集成

|  |  |  |  |
| --- | --- | --- | --- |
| 系统集成 | 对整个系统进行集成和对原来老校区搬迁的信息化系统进行安装调试保证老校区的信息化系统能正常使用。 | 1 | 定制 |

商务要求

|  |
| --- |
| 1、★所有产品必须经正规渠道供货，不得提供旧货、水货、假货，产品原厂备案最终用户为温州技师学院；并须提供详细配置清单，签订合同之前提供原厂授权质保函原件，否则作废标处理。  2、在设备保修期内，由于设备质量因素而造成的损坏，均由中标商负责免费维修和更换配件；在保修期结束前，须与买方、中标商进行一次全面检查，任何缺陷必须由中标商负责修理或更换。3、为保证项目系统良好运行及今后售后服务的及时性, 要求供应商在温州地址设有自营服务机构（以工商营业执照为准），接到报修电话2小时内到场维修，质保期内能够提供免费的上门服务（7\*8小时）。  4、本项目为交钥匙工程,以上参数带★号必须完全满足不接受偏离，中标后，用户方可以无条件要求中标人提供全新未拆封的且和投标型号一致的设备根据招标要求进行软件功能及硬件参数逐一测试验证，并按招标要求提供全部相关资料，否则作废标处理.  5、预中标后，中标方需在3个工作日提供中标价的5%做质保金，不提供则视为自动放弃该项目，如果虚假应标则没收质保金且报价作废。  6、要求整个项目实施验收通过后提供1次针对项目相关维护人员的集中培训.  7、本次项目涉及到新旧网络设备及安全设备数据等无缝链接问题，所以要求中标公司要有一定的实施能力，包括中标公司要有网络交换ccie或者H3CSE 工程师；虚拟化VCP认证工程师，数据库ocp认证工程师等，要求供应商免费提供驻点人员维护一年， 直至项目顺利接割。驻点人员工作时间和学院上班时间同步，如有需要必须接受临时加班要求。驻点人员无故不来上班的每日扣处千分之一的履约保证金。  8、本次采购不接受非推荐品牌产品，要求中标供应商提供机房服务工作。  9、中标后3个工作日内用户有权要求对产品功能进行逐项测试（如果功能、性能要求上理解与用户有不同，责任有投标人承担），如有虚假应标，用户有权取消其中标资格并按规定追求相应责任；招标所有参数作为实质性条款必须满足，否则视为无效投标。采购人若有疑问时投标人在成交确认前需提供样品逐项演示产品功能。 |