1. **总体要求**
2. 本部分内容是根据本项目实际情况制定的。
3. 投标人必须仔细阅读本部分的全部条款。对本部分中存在的任何疑问、遗漏或相互矛盾之处，或是对于相关要求不清楚，认为存在歧视、限制的情况，投标人可以向采购人或采购中心寻求书面澄清。
4. 本部分所列明的工艺、材料和设备的标准以及参照的分类号仅起说明作用，并没有任何限制性，投标人在投标中可以选用替代标准或分类号，但这些替代应当等于或优于文件技术要求。
5. **项目概述及需求一览表**

**1.需求一览表**

| **项目** | **品目号** | **品目名称** | **数量** | **单位** | **交货期** | **服务期限** |
| --- | --- | --- | --- | --- | --- | --- |
| 硬件采购 | A01-01 | 汇聚交换机 | 6 | 台 | 合同签订后2个月内 |  |
| A01-02 | 南校区核心交换机 | 2 | 台 |
| A01-03 | 48口接入交换机 | 440 | 台 |
| A01-04 | 24口接入交换机 | 60 | 台 |
| A01-05 | 24口POE交换机 | 10 | 台 |
| A01-06 | 超融合服务器 | 20 | 台 |
| A01-07 | 信创应用服务器 | 4 | 台 |
| A01-08 | 备份一体机 | 1 | 套 |
| A01-09 | 防DDOS | 2 | 台 |
| A01-10 | 链路负载均衡 | 1 | 台 |
| A01-11 | 核心防火墙 | 1 | 台 |
| A01-12 | 边界防火墙 | 2 | 台 |
| A01-13 | 上网行为管理系统 | 1 | 台 |
| A01-14 | 网络防病毒软件 | 1 | 套 |
| A01-15 | 主机安全审计 | 1 | 台 |
| A01-16 | 数据库审计 | 2 | 台 |
| A01-17 | 漏洞扫描 | 1 | 台 |
| A01-18 | 终端安全管理系统 | 1 | 套 |
| A01-19 | 安全管理平台（SOC） | 1 | 套 |
| A01-20 | 虚拟化云教室 | 1 | 套 |
| A01-21 | 精密空调 | 2 | 台 |
| A01-22 | UPS | 1 | 台 |
| A01-23 | 服务器机柜 | 6 | 台 |
| A01-24 | 关系型数据库 | 12 | 套 |
| A01-25 | 操作系统 | 40 | 套 |
| A01-26 | 应用中间件 | 12 | 个 |
| A01-27 | 综合运维管理系统 | 1 | 套 |
| A01-28 | 数据交换 | 1 | 套 |
| A01-29 | 内容管理 | 1 | 套 |
| A01-30 | 报表软件 | 1 | 套 |
| A01-31 | 工作流及表单 | 1 | 套 |
| A01-32 | 全文检索 | 1 | 套 |
| 安全服务 | A01-33 | 等级保护测评服务 | 1 | 套 | 1年 |
| 软件定制开发 | A01-34 | 展现门户建设 | 1 | 套 |  |
| A01-35 | 网络学习平台 | 1 | 套 |
| A01-36 | 移动应用平台 | 1 | 套 |
| A01-37 | 云应用支撑平台 | 1 | 套 |
| A01-38 | 信息资源目录服务 | 1 | 套 |
| A01-39 | 安全邮件系统 | 1 | 套 |
| 标准规范编制 | A01-40 | 标准规范编制 | 1 | 套 |  |  |

品目A01-01至A01-20、A01-24至A01-27、A01-39，提供原厂售后服务承诺函（承诺函的内容包括：原厂提供技术服务期限为3年，从竣工验收开始3年内，针对软硬件使用过程中出现的技术问题，需要提供7\*24小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对软件的调节/优化提供建议，提供24小时带备件现场保修，3年原厂免费上门服务）

**2.项目概述**

**2.1项目背景**

中共中央党校是是党中央培训全国高中级领导干部和优秀中青年干部的学校，是研究宣传习近平新时代中国特色社会主义思想、推进党的思想理论建设的重要阵地，是党和国家哲学社会科学研究机构和中国特色新型高端智库，是党中央直属事业单位。

加强信息化服务党校教学培训、科研咨询、党校发展的能力和水平，采取有力措施，全面加强智慧党校建设，充分利用“互联网+干部教育培训、新一代信息技术、数据应用、智慧党校”等技术，推进干部教育培训改革、丰富培训内容、创新教学方式、改进教学方法，为党中央、国务院提供科学的决策咨询服务，中央党校教学科研咨询智慧服务系统工程建设项目势在必行。

2.2现状描述

近年来，党校信息化建设已经初步形成规模。党校已建成万兆为核心、千兆到桌面架构的网络系统，分布式存储系统和现有机房设备，为本项目的建设提供稳定的基础环境支撑条件。本次项目建设，将基于南北校区软硬件及基础设施等信息化建设成果，开展进一步的项目建设实施工作。

2.3建设内容

2.3.1信息化基础设施建设。优化党校网络中心机房建设、搭建党校私有云支撑平台、促进党校各区域高速接入校园网、完善党校网络安全防护系统、建设智慧校园示范智能教室。

2.3.2 信息安全测评服务。

2.3.3 应用系统开发建设。提高学员认知水平和解决实际问题的能力。

2.3.4 标准规范体系建设。编制相关的标准规范，形成标准规范体系。

1. **技术规格、参数及要求**

指标按重要性分为“★”、“#”和一般无标识指标。★代表必要指标项， #代表重要指标项，无标识则表示一般指标项。

**A01-01 汇聚交换机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★1 | ★ | 业务插槽数 | 业务插槽数≥8 |
| ★2 | ★ | 交换性能 | 交换容量≥19Tbps  转发能力≥2880Mpps |
| ★3 | ★ | 配置 | 主控引擎模块≥2，满足1+1冗余  独立交换网板模块≥2，满足1+1冗余（交换网板与业务板卡90°正交）  配置冗余电源模块  实配≥96个万兆光口, 实配堆叠带宽40G（单向）实配堆叠线缆  实配96个万兆单模光模块 |
| 1 |  | 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇等关键部件可热插拔 |
| 2 |  | 链路聚合 | 聚合组数≥512组，每组成员≥32个 |
| 支持跨设备链路聚合 |
| #1 | # | 可靠性 | 支持主控板冗余，倒换时间为0ms |
| 支持NSF/GR for OSFP/BGP/IS-IS |
| 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<50ms |
| 支持IP FRR，满足网络收敛<50ms |
| 3 |  | IPv6 | 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议 |
| 支持IPv6策略路由； |
| 支持DHCPv6功能、IPv6 portal功能、IPv6管理功能； |
| 支持基于IPv6的VXLAN二三层互通； |
| 支持基于IPv6的VRRP功能 |
| 4 |  | 虚拟化 | 多虚一技术(N:1) |
| 5 |  | 安全特性 | 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 |
| 6 |  | 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SNMPv3、支持端口镜像、支持VLAN镜像、支持RSPAN、支持流镜像 |

**A01-02 南校区核心交换机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★4 | ★ | 业务插槽数 | 业务插槽数≥10 |
| ★5 | ★ | 交换性能 | 交换容量≥28Tbps  转发能力≥4000Mpps |
| ★6 | ★ | 配置 | 主控引擎模块≥2，满足1+1冗余  独立交换网板模块≥4，满足N+1冗余（交换网板与业务板卡90°正交）  实配40G堆叠端口，堆叠带宽达到160G  配置冗余电源模块  实配48口万兆光口板≥4  192个万兆单模光模块 |
| 7 |  | 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇等关键部件可热插拔 |
| 8 |  | 链路聚合 | 聚合组数≥512组，每组成员≥32个 |
| 支持跨设备链路聚合 |
| #2 | # | 可靠性 | 支持主控板冗余，倒换时间为0ms |
| 支持NSF/GR for OSFP/BGP/IS-IS |
| 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<50ms |
| 支持IP FRR，满足网络收敛<50ms |
| 9 |  | IPv6 | 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议 |
| 支持IPv6策略路由； |
| 支持DHCPv6功能、IPv6 portal功能、IPv6管理功能； |
| 支持基于IPv6的VXLAN二三层互通； |
| 支持基于IPv6的VRRP功能 |
| 10 |  | 虚拟化 | 支持多虚一技术(N:1) |
| 11 |  | 安全特性 | 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 |
| 12 |  | 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SNMPv3、支持端口镜像、支持VLAN镜像、支持RSPAN、支持流镜像 |

**A01-03 48口接入交换机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★7 | ★ | 交换性能 | 交换容量≥590Gbps  转发能力≥250Mpps |
| ★8 | ★ | 配置 | 端口：48个10/100/1000 Base-T自适应以太网口，4个万兆SFP+口，配置两个万兆单模光模块，≥2扩展槽  模块化双电源 |
| 13 |  | CPU保护功能 | 支持CPU保护功能 |
| 14 |  | 组播协议 | 支持IGMP v1/v2/v3，MLD v1/v2 |
| 支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2 |
| 15 |  | 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 16 |  | 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)； |
| 支持RRPP或ERPS（快速环网保护协议），环网故障恢复时间不超过200ms； |
| 17 |  | 性能指标 | MAC地址表>=32K |
| ARP：8K |
| 18 |  | 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| 支持IPv6手动隧道、6to4隧道和ISATAP隧道 |
| 19 |  | 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 |

**A01-04 24口接入交换机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★9 | ★ | 交换性能 | 交换容量≥590Gbps  转发能力≥210Mpps |
| ★10 | ★ | 配置 | 24个10/100/1000Base-T自适应以太网端口），4个万兆SFP+口，配置两个万兆单模光模块，≥2个扩展槽，模块化双电源 |
| 20 |  | CPU保护功能 | 支持CPU保护功能 |
| 21 |  | 组播协议 | 支持IGMP v1/v2/v3，MLD v1/v2 |
| 支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2 |
| 22 |  | 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 23 |  | 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)； |
| 支持RRPP或ERPS（快速环网保护协议），环网故障恢复时间不超过200ms； |
| 24 |  | 性能指标 | MAC地址表>=32K |
| ARP：8K |
| 25 |  | 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| 支持IPv6手动隧道、6to4隧道和ISATAP隧道 |
| 26 |  | 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 |

**A01-05 24口POE交换机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★11 | ★ | 交换性能 | 交换容量≥330Gbps  转发能力≥90Mpps | |
| ★12 | ★ | 配置 | 24个10/100/1000Base-T自适应以太网端口，4个万兆SFP+口，配置两个万兆单模光模块，实配POE功能，总输出功率≥370W | |
| 27 |  | ERPS | 实现ERPS功能，能够快速阻断环路，链路收敛时间≤50ms | |
| 28 |  | POE | 支持802.3at/POE+供电标准 | |
| 29 |  | 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； | |
| 支持流镜像 | |
| 同时支持N：M的端口镜像（M大于1） | |
| 30 |  | 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)； | |
| 支持RRPP或ERPS（快速环网保护协议），环网故障恢复时间不超过200ms； | |
| 31 |  | 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF | |
| 支持IPv6静态路由、RIPng | |
| 32 |  | 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 | |

**A01-06 超融合服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★13 | ★ | 产品外形 | 机架式服务器 |
| ★14 | ★ | 配置 | 处理器：配置4颗处理器,性能相当或优于GOLD 5120：主频≥2.2GHz，核心数≥14核  内存：具备48个内存插槽，本次配置1T DDR4-2666MHz 内存。  硬盘：配置2块2.5寸480GB 热插拔SSD硬盘，≥5块900GB 10K RPM SAS盘  RAID卡：配置PCI-E接口独立RAID卡，1G缓存，支持0/1/5/10/50/60等  网络：配置4个千兆网口（RJ45）,2块双端口万兆网卡（光纤接口含光模块）  HBA卡：配置2个16Gb FC口  电源：配置4个电源， 2+2冗余  风扇：配置冗余风扇 |
| 33 |  | 硬盘扩展性 | 最大支持≥24块3.5寸热插拔SAS接口硬盘； |
| 34 |  | PCI-E扩展 | 最大可扩展支持≥10个PCI-E插槽 |
| 35 |  | 管理 | 支持IPMI2.0、KVM over IP等方式远程管理控制； |

**A01-07 信创应用服务器**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★15 | ★ | 规格 | 标准机架式2U服务器 |
| ★16 | ★ | 配置 | 处理器：国产CPU，主频≥1.4GHZ |
| 内存：实配≥32GB DDR3内存 |
| 硬盘：实配≥2块240GB企业级SSD硬盘，实配≥3块900GB企业级热插拔SAS硬盘 |
| 操作系统：兼容中标麒麟高级服务器操作系统软件（龙芯64位）V7.0 |
| RAID卡：实配≥1块独立八通道Raid卡 |
| 网卡：实配≥4个千兆网络接口（RJ45） |
| 电源配置1+1冗余电源 |
| 风扇：配置冗余热拔插风扇 |

**A01-08 备份一体机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| #3 | **#** | 机型 | 机架式软硬一体化设备 |
| ★17 | ★ | 配置 | 处理器：配置2颗性能相当或优于xeon Silver 4110系列CPU，单CPU核心数≥8  内存：配置128GB DDR4-2400内存，  支持高级内存纠错、内存镜像、内存热备等高级功能；  要求内存插槽数≥16，内存扩展能力≥384GB  系统盘：配置2块240GB 2.5寸 SSD硬盘作为系统盘  备份容量：配置≥72块3.5寸 7200RPM 8TB企业级SATA硬盘，配置与实际可用容量相当的容量授权，备份不限制客户端类型和数量  RAID级别：支持RAID0、1、5、6、10、50、60  主机接口：配置2个千兆以太网口，要求可扩展≥10个千兆以太网口，并可扩展万兆网口  I/O扩展能力：支持≥7个标准PCI-E 3.0插槽  配置双冗余、热插拔电源和风扇 |
| ★18 | ★ | 操作系统支持 | 支持Windows、Linux、AIX、HP-Unix、Solaris等主流操作系统平台的各类数据备份保护，支持国产中标、普华、红旗等系统平台 |
| ★19 | ★ | 数据库支持 | 支持Oracle、SQL Server、MySQL、Exchange Server、Active Directory、DB2、Domino、人大金仓、达梦等主流数据库的备份和恢复 |
| #4 | # | 虚拟机支持 | 支持主流虚拟机备份，支持对VMware vSphere、XenServer、FusionComputer、CAS、FusionCloud和TStack等主流虚拟化应用的备份，支持单机和集群部署环境。以上虚拟化应用均支持以虚拟机、资源池和整个集群为单位进行备份保护保护，无需在虚拟机内部安装任何代理软件。 |
| ★20 | ★ | 重复数据删除 | 配置重删功能，多个备份任务可以共享同一个重复数据删除指纹池，也可以根据数据的不同单独设置专属指纹池，最大限度的提升重复数据删除效率，减轻带宽压力，降低传输数据量和备份数据存储成本。 |
| 36 |  | D2D2T备份 | 支持D2D2T备份 |
| 37 |  | 外部备份介质 | 支持连接主流物理带库等异构硬件备份介质 |
| #5 | **#** | 备份方式 | 支持完全、增量、差分等多种备份方式，支持实时备份，实时备份数据的应急接管和容灾演练功能，基于虚拟磁盘快照和实时备份的日志数据，通过图形化界面快速生成生产服务器在历史某一时间完整状态的完整虚拟磁盘，时间选择精度为微秒（0.000001）级。在时间精度选择时，系统界面提供对应时间状态的生产服务器的磁盘IO负载波形图，以辅助选择合适的IO状态。同时，通过图形化界面为该虚拟机磁盘配置相关的存储、计算和网络资源后形成一个完整的虚拟机，可使用备份设备内置的企业级虚拟化软件启动该虚拟机。 |
| #6 | **#** | 远程复制 | 支持2台备份一体机间的远程复制 |
| 38 |  | 灾难恢复能力 | 要求备份管理具有灾难恢复能力，支持数据复制验证功能，复制到目标端备份系统的备份数据，如果需要查看和恢复，必须输入源端备份系统原操作员的账号和密码，避免数据泄密 |
| 39 |  | 统一监管 | 可实现所有备份节点的统一监管，具备拓扑图、多租户、监控告警、报表等特性，提供API实现二次开发对接 |

**A01-09 防DDOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★21 | ★ | 性能 | 整机抗攻击能力≥4Gbps |
| ★22 | ★ | 配置 | 万兆光纤端口≥2 |
| 40 |  | 抗攻击功能 | 防御流量型flood攻击 ：SYN Flood 、SYN-ACK Flood、 ACK Flood、FIN/RST Flood、ICMP Flood、UDP Flood、IP Fragment Flood、Stream flood等。 |
| 41 |  | 防御UDP Flood攻击：必须提供2层防护，要求包括UDP防御阈值设置以及丢弃UDP碎片。 |
| 42 |  | ACK Flood攻击提供TCP防御阈值设置，同时必须提供ACK限速手段进行防护，开启时不影响客户在线业务。 |
| 43 |  | 防御HTTP get /post Flood 攻击、CC应用层攻击，必须能够自定义web防护端口，同时要求至少有set-cookie、javaScript、mouse click、flash、encrypt javaScript、encrypt set-cookie 6种验证方式。 |
| 44 |  | 针对HTTP 攻击、CC应用层攻击必须提供如下防护手段：连接缓存、屏蔽HTTP代理、屏蔽搜索引擎、源IP连接数限制、源IP新建连接速率限制、源IP GET请求速率限制、源IP POST请求速率限制、源IP OTHER请求速率限制。 |
| 45 |  | 防御DNS query/reply Flood攻击， 提供TCP、CNAME和Passive 3种验证机制，多维度限制查询及请求速率。 |
| 46 |  | HTTPS攻击专项防护模块，必须能够对HTTPS协议数据包进行解密，然后防护，必须具有redirect、JavaScript和flash 三种验证方式，有效防御HTTPS类型的DDoS攻击。 |
| 47 |  | 必须支持导入SSL证书对HTTPS流量进行防护 |
| 48 |  | 支持自动防护，系统开启自动防护后，无需撰写任何规则对所有服务器进行DDoS防护，也可针对特定服务器撰写特定防护规则。 |
| 49 |  | 异常流量管理 | 支持IP黑白名单，支持智能动态黑/白名单；支持静态黑/白名单，支持批量导入、导出静态黑白名单。 |
| 50 |  | 支持域名黑/白名单，支持域名黑/白名单批量导入、导出，可自定义拦截页面。 |
| 51 |  | 支持自定义包大小限制，自定义数据包大小、特征字符出现的频率限制，必须提供数据匹配或正则匹配选项，对匹配的数据包进行丢弃、放行、对源目IP加黑名单等操作。 |
| 52 |  | 防御策略必须提供攻击防御模式、直通模式、信任模式、清洗模式、屏蔽模式、透明模式6种防御策略。 |
| 53 |  | 支持动态黑名单抓包功能。 |
| 54 |  | 支持基于源IP、目的IP、源端口、目的端口、协议的五元组抓包功能；必须支持对输入滤前/滤后、输出滤前/滤后、输入拦截、输出拦截、双向滤前、双向滤后、双向拦截等条件抓取指定数据包，指定抓包数量和抓包比例 |
| 55 |  | 产品必须具备抓取数据包的功能，必须能够进行在线分析，同时提供下载功能。 |
| 56 |  | 必须支持GEOIP功能，针对特定国家或区域的IP批量执行拦截、放行或防护等操作，有效阻止境外IP发起的攻击。 |
| 57 |  | 支持UDP限速，通过源IP、源IP+源端口、目的IP、目的IP+目的端口、目的IP+源端口等方式进行UDP限速。 |
| 58 |  | 支持对服务器总流量、TCP流量、UDP流量、FRAG流量、ICMP流量以及其他协议的流量限制。 |
| 59 |  | 串行部署时进行双向会话管控，能够设置从外到内的连接阈值，同时必须能够设置从内到外的连接阈值。 |
| 60 |  | 通过CC防御模块动态加入黑名单的客户端再次访问web服务器时有提示信息。 |
| 61 |  | 支持流量超过设定阈值后web页面提示告警。 |
| 62 |  | 支持牵引屏蔽，当攻击流量过大时，能与上层交换机或路由器联动，直接屏蔽攻击流量。 |
| 63 |  | 支持针对服务器出/入流量、出、入包数、出/入连接数的TOPN排名。 |
| 64 |  | 部署方式 | 支持透明串行部署、旁路部署和集群部署 |
| 65 |  | 支持BGP牵引，OSPF牵引；  支持策略路由、二层回注。 |
| 66 |  | 日志报表 | 提供攻击事件和攻击详情。提供攻击源IP、被攻击IP、防护域、攻击类型、攻击事件、总流量、攻击流量、峰值流量等信息；支持按被攻击IP、防护域、攻击时间等查询特定的攻击事件；支持导出PDF格式的攻击事件和攻击详情。 |
| 67 |  | 提供攻击报表，攻击报表中包含全局流量、攻击流量、攻击类型、被攻击IP流量TOP10、源国家攻击次数TOP10、目的端口流量TPO10、攻击事件峰值TOP10、攻击类型峰值流量区间统计、协议流量统计、协议概览等信息；支持攻击报表定时发送给指定管理员邮箱；支持导出PDF格式的攻击报表。 |
| 68 |  | 设备管理 | 支持Web图形化界面配置，支持http和https登录方式；支持SSH、串口管理。 |
| 69 |  | 可设置访问客户端IP黑白名单，对客户端IP进行访问控制，提供允许访问和不允许访问两种方式。 |
| 70 |  | 恢复出厂保护设置，进行系统恢复出厂设置时必须输入管理员密码，防止误操作删除所有配置数据。 |
| 71 |  | 支持通过SNMP方式输出内存、CPU、磁盘、接口状态和物理网卡信息，支持V1、V2C和V3版本，支持snmp trap。 |
| 72 |  | 支持web页面上传升级包一键升级。支持在线备份恢复。 |
| 73 |  | 提供网络诊断工具，必须支持ping、traceroute、TCP诊断及故障信息一键收集。 |
| 74 |  | 支持自定义添加账号，必须支持自定义功能按钮权限。支持Radius认证。 |
| 75 |  | 操作日志、攻击事件、攻击详情可通过SFTP/SSH方式上传至备份服务器。 |
| 76 |  | 支持查看系统网卡的状态，包括网卡up/down信息，流量信息，网卡速率等。 |
| 77 |  | 高可靠性 | 支持多台设备集群部署，支持在大流量攻击发生时手动或自动启动集群，保证整个系统可用性；支持集群设备间数据状态同步、配置同步，支持集群无限扩容。 |
| #7 | # | 资质要求 | 具有《计算机信息系统安全专用产品销售许可证》；  具有软件著作权证书； |

**A01-10 链路负载均衡**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★23 | ★ | 产品形态 | 采用x86硬件架构，必须是独立专业负载均衡设备，非插卡式负载均衡设备，高度≤2U，冗余电源，开通3条多线路授权模块 |
| ★24 | ★ | 配置 | 千兆电口≥6 个  千兆光口≥8个（满配光模块）  万兆光口≥4个（满配光模块）  冗余电源 |
| ★25 | ★ | 性能要求 | 四层最大并发≥900万；  四层每秒新建连接数≥35万  四层最大有效吞吐≥20G |
| 78 |  | 多合一功能集成 | 单一设备可同时提供包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。 |
| #8 | # | IPV6改造 | 提供双栈模式，支持NAT46、NAT64、NAT66。 |
| 79 |  | IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题 |
| 80 |  | 提供通过syslog的方式实现IPv4/IPv6协议转换日志功能，累积存储和查询3个月内数据；提供IPv6/IPv4协议翻译和互通的日志信息，包括源/目的IP地址和端口，被访问的URL等信息，并在需要的情况下，回溯查询用户信息 |
| #9 | # | IP地址库 | 内置完备的IP地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能 |
| 81 |  | 支持链路数量 | 支持对不少于20条的线路进行流量选路调度，最多可扩展支持到200条线路 |
| 82 |  | DNS透明代理 | 提供DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率 |
| 83 |  | 应用识别和引流 | 支持应用引流，可识别游戏、视频、网银等应用，并根据应用类型进行流量调度分发 |
| 84 |  | 动态反馈 | 支持对服务端的CPU、I/O、Memory进行SNMP的探测，基于探测结果向访问端反馈访问请求的最优访问调度信息 |
| 85 |  | 会话保持 | 支持基于消息的长连接负载（MBLB），对于非HTTP协议的长连接应用，可通过分析议特征来识别消息的开始和截止，以消息为对象进行七层访问和流量的调度。同时能支持在软件界面上更改会话保持时间 |
| 86 |  | 自定义方式 | 支持多种编程语言（如Python、Java等） |
| 87 |  | 负载均衡算法 | 提供轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法 |
| 88 |  | URL链路调度 | 支持基于URL的链路调度功能，内置不少于1000条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路 |
| 89 |  | 图片格式转化 | 通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果 |
| 90 |  | 压缩格式 | 至少支持DEFLATE、GZIP等压缩格式 |
| 91 |  | 告警 | 内置智能告警系统, 支持E-mail、短信 、SNMP Trap三种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（包括服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息 |
| 92 |  | 慢速HTTP攻击防护 | 提供应对慢速HTTP攻击防护的更改缓存模式的软件脚本包，可以实现慢速HTTP攻击导致缓存沾满，导致正常用户访问无法响应或是响应慢的问题 |
| 93 |  | 可视化 | 业务可视化：支持通过大屏展示所有业务的运行情况，包括新建连接数、并发连接数、实时吞吐量、压缩优化效果、缓存优化效果、SSL卸载效果、业务在线离线情况等等 |

**A01-11 核心防火墙**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★26 | ★ | 产品形态 | 采用x86硬件架构，必须是独立专业防火墙设备，非插卡式防火墙设备，高度≤2U，冗余电源，开通WEB防护等增强级防火墙功能模块 |
| ★27 | ★ | 配置 | 千兆电口≥6个；  千兆光口≥4个（满配光模块）  万兆光口≥4个（满配光模块）  冗余电源 |
| ★28 | ★ | 整机性能 | 整机吞吐量≥18 Gbps；  每秒新建连接数≥30万；  并发连接数≥400万； |
| 94 |  | 部署方式 | 支持路由，网桥，以及混合部署方式 |
| 95 |  | 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口；支持链路聚合功能；  支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路； |
| 96 |  | 基础功能 | 支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录；  访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；  访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况； |
| 97 |  | 访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； |
| 98 |  | 内容安全 | 内置病毒样本数量超过200万；  支持URL过滤和文件过滤功能； |
| 99 |  | 支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤； |
| 100 |  | DoS/DDoS攻击防护 | 支持内网访问控制，配置内网区域只允许指定的IP地址或IP范围对外进行访问 |
| 101 |  | 蜜罐功能 | 支持蜜罐功能 |
| 102 |  | 入侵防护功能 | 设备具备独立的入侵防护漏洞规则特征库 |
| 103 |  | 安全审计 | 当发生安全事件可记录攻击源IP、攻击类型、攻击目的IP、攻击时间等关键信息； |
| 104 |  | 安全可视化 | 支持对检测到的攻击行为按照IP地址的地理位置信息进行信息展示 |
| 105 |  | 支持自动生成安全风险报表 |
| 106 |  | 支持受保护业务和用户的关联安全事件展示；  支持以攻击链方式来匹配和展示资产遭受到的攻击行为； |
| 107 |  | 支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证； |
| 108 |  | 安全风险报表 | 双机支持A/S，A/A方式部署；  支持配置同步，会话同步和用户状态同步；  支持双机心跳线冗余； |
| 109 |  | 高可用性 | 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式；  支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限； |
| 110 |  | 系统配置管理 | 支持自动备份配置，最大支持十五天内的配置恢复；  支持修改TCP，UPD和ICMP协议的连接超时时间；  支持内置规则库的手动/自动更新；  支持邮件、短信和微信告警； |
| #10 | # | 产品资质要求 | 产品应具备计算机信息系统安全专用产品销售许可证； |

**A01-12 边界防火墙**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★29 | ★ | 产品形态 | 采用x86硬件架构，必须是独立专业防火墙设备，非插卡式防火墙设备，高度≤2U，冗余电源。 |
| ★30 | ★ | 网络接口 | 千兆电口≥6个；  千兆光口≥4个（满配光模块）  万兆光口≥2个（满配光模块） |
| ★31 | ★ | 整机性能 | 整机吞吐量≥18Gbps；  应用层吞吐量≥8Gbps；  每秒新建连接数≥30万；  并发连接数≥400万； |
| 111 |  | 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口；支持链路聚合功能；  支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路； |
| 112 |  | 基础功能 | 访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试 |
| 113 |  | 内容安全 | 内置病毒样本数量超过200万 |
| 114 |  | 蜜罐功能与应急 | 支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址 |
| 115 |  | 未知威胁检测 | 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； |
| 116 |  | 入侵防护功能 | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上； |
| 117 |  | 安全审计 | 当发生安全事件可记录攻击源IP、攻击类型、攻击目的IP、攻击时间等关键信息； |
| 118 |  | 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别 |
| 111 |  | 支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； |
| 112 |  | 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； |
| 121 |  | 安全运营中心 | 支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险； |

**A01-13 上网行为管理系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★32 | ★ | 硬件基本要求 | 千兆电口≥4个；  千兆光口≥4个（满配光模块）  万兆光口≥2个（满配光模块）  冗余电源 |
| ★33 | ★ | 整机性能 | 支持带宽≥2.5Gb；  支持用户规模≥25000； |
| 122 |  | 多主模式 | 必须支持两台及两台以上设备同时做主机的部署模式； |
| 123 |  | 用户密码强度 | 可设置用户密码不能等于用户名；  新密码不能与旧密码相同；  可设置密码最小长度；  可设置密码必须包括数字或字母或特殊字符 |
| 124 |  | 网页过滤 | 支持根据访问的URL、网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为； |
| 125 |  | 上网时长控制 | 支持统计和控制用户终端每天上网时间，并支持排除应用或特殊端口后的灵活流量统计方法； |
| 126 |  | 用户行为报表 | 支持查询和导出基于指定时间段/用户/用户组的文件审计、邮件收发、访问网站、即时通讯、发帖/微博、搜索关键字等详细用户行为的报表 |
| 127 |  | SSL加密内容审计和过滤 | 针对SSL加密的网站、论坛发帖、web邮箱的内容进行关键字过滤和内容审计 |
| 128 |  | 带宽管理 | 必须支持在不同线路上，根据不同的应用、用户/用户组、位置、终端类型来保证或者限制流量 |
| 129 |  | 文件外发审计 | 支持审计用户通过HTTP、FTP、Email当方式外发的文件内容；必须能审计记录无后缀名的文件外发行为； |
| 130 |  | 日志分级审查 | 管理员登录数据中心只能审计指定用户组的上网行为日志； |
| 131 |  | 趋势报表 | 支持基于时间段/用户/用户组/终端类型/位置等多种维度的流速趋势报表、流控通道趋势报表、应用行为趋势报表、网站分类行为趋势报表等 |
| 132 |  | 报表功能 | 支持从流量分析、时长分析、用户行为分析、网站分类分析、终端接入分析、终端接入安全等多维度下选择具体的基于用户/用户组/终端/网站/域名/应用/通道/搜索关键字等细粒度的排行、趋势等报表，整合成一个自定义报表进行订阅； |

**A01-14 网络防病毒软件**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★34 | ★ | 软件 | 提供防病毒策略管理、下发以及病毒告警分析、报表等功能，可管理win系列客户端、Linux系列客户端、麒麟系列客户端，可安装在centos7.0及以上操作系统。 |
| ★35 | ★ | 配置 | 1套管理端、不少于2000台主机终端管理能力。 |
| 133 |  | 管理要求 | 符合安全产品的三员分立要求，支持按功能模块配置管理策略和日志查看策略，提供多种预定义的统计报表和图形报表 |
| 134 |  | 产品运行不能对系统本身和网络的正常运行产生影响，占用系统主机极少的CPU和内存 |
| 135 |  | 系统架构：管理方式采用B/S、客户端采用C/S架构。 |
| #11 | # | 兼容性 | 服务端支持平台  操作系统支持国产化操作系统服务器版本（中标麒麟、银河麒麟、中科方德等）以及CentOS系统；同时支持主流国产化CPU平台（龙芯、飞腾、兆芯、海光、申威等）以及X86 CPU |
| 客户端支持平台  操作系统支持国产化操作系统，如中标麒麟、银河麒麟、中科方德等；同时支持主流国产化硬件（龙芯、飞腾、兆芯等）以及X86 CPU。 |
| 136 |  | 查杀能力 | 本地查杀能力：  要求产品具备多个自主研发的本地引擎  能够对已知、未知病毒、木马、恶意程序等进行检测、清除。  能够对各种加壳的病毒文件进行病毒查杀，支持的加壳种类不少于100种  支持族群式变种病毒的查杀 |
| 主动防御：  须具备基于多步行为判断的主动防御技术，能够根据样本一系列的行为特征来进行综合的风险判定。  能够实时监控和清除病毒、木马、恶意程序等， |
| 实时防护：  具备系统文件监控能力，能够监控计算机系统所有活跃文件的安全性  具备边界防护能力，对网页访问、浏览器下载、U盘拷贝等系统入口实时监控，拦截危险文件的落地 |
| 压缩包查杀：  具备压缩包查杀功能，支持25种解压缩格式，涵盖压缩包、安装包、文档格式解析能力。支持安装脚本级查杀，拦截流氓软件捆绑。 |
| 137 |  | 管理能力 | 威胁管理：  展示全网威胁统计情况，包括威胁类型、感染范围、最后活跃时间以及MD5  具备病毒文件审计追踪能力，可智能定位病毒，及早处理感染源，减少病毒爆发造成的损失。  可自定义展示数据范围，以面积图、折线图、饼状图、柱形图、表格等方式进行展示 |
| 138 |  | 终端信息展示：  展示全网终端杀毒相关的状态信息，包括计算机名、IP地址、所属部门、计算机所在地、风险病毒统计等  可自定义展示数据范围，以面积图、折线图、饼状图、柱形图、表格等方式进行展示 |
| 139 |  | 审计日志：  具备提供多维度，多粒度的日志汇总报表与分析报表的能力。并提供两种展示方式，图形报表和详细日志。 |
| 140 |  |  | 图形报表：可折线图，饼状图等图表导出终端部署情况，日活统计，病毒库版本统计，病毒排名，感染情况统计等数据。  详细日志：可展示所有终端的操作日志，通过触发原因，操作类型，操作状态，时间戳，操作员账户，终端名等搜索条件来筛选用户需要的信息，筛选完成后，可导出报表。  可自定义展示数据范围，以面积图、折线图、饼状图、柱形图、表格等方式进行展示 |
| #12 | # | 产品资质 | 1、具有《信息系统安全专用产品销售许可证》  2、产品须具有《计算机软件著作权登记证书》 |

**A01-15 主机安全审计**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★36 | ★ | 硬件规格 | ≤2U机箱，标配双电源，支持RAID1，存储空间≥2T、≥4个10/100/1000M Base-TX网络接口，≥4个千兆SFP接口插槽（包含光模块），1个RJ45串口，含2个监听口授权，最大支持≥4个千兆口监听 |
| ★37 | ★ | 性能 | 入库速度≥25000条/秒，日处理事件数≥15000万条 |
| 141 |  | 部署方式 | 支持旁路部署和透明桥接部署，支持分布式部署与集中管理 |
| 142 |  | 支持Lan、MPLS、GRE、PPPOE、VLAN等网络接入环境 |
| 143 |  | 行为审计 | 能够全面详实地记录网络内流经监听出口的各种网络行为，并根据国家有关法规规定保存至少60天，以便进行事后的审计和分析。日志以加密的方式存放，只有管理者才能调阅读取 |
| 144 |  | 支持GRE(通用路由协议封装）、MPLS（Multi-Protocol Label Switching，多协议标签交换）、L2TP、PPPoE等封装协议的网络数据审计还原。 |
| 145 |  | Windows远程桌面等远程登录事件 |
| 146 |  | 能够审计的网络协议或应用类型包括：标准协议及其衍生应用（HTTP-GET、HTTP-POST、HTTPS、TELNET、FTP、SMTP、POP3、Samba等）； |
| 147 |  | 内容审计 | 支持WEBMAIL、网页论坛、网页聊天、网页登录等网页提交内容审计，对不能自动识别类型的网页提交应用能自动归到其他类型 |
| 148 |  | 支持对Google, baidu, sogou, soso等常见搜索引擎的搜索关键字记录，并具备良好的扩展能力，支持用户自定义其它搜索引擎 |
| 149 |  | 支持文件还原及下载备份功能 |
| 150 |  | 网页提交内容审计不限站点 |
| 151 |  | 支持邮件附件下载备份功能 |
| 152 |  | 上网认证 | 支持触发式WEB认证，除免认证用户外，其他用户必须经过认证后才可上网 |
| 153 |  | 支持多种认证方式并存，不同终端PC可分别使用不同的认证方式 |
| 154 |  | 实名审计 | 支持三层交换环境下的MAC地址获取，能够将IP/MAC地址等信息与实际用户进行对应，并在审计结果中体现实际用户， |
| 155 |  | 支持PPPoE、Radius协议的拨号帐号与上网日志关联；支持在网络环境中存在多种代理服务器时能够准确捕获还原网络日志数据，包括ISA代理、Socks4/5、Squid等HTTP Proxy；支持代理服务器与AD域控制器、LDAP帐号的联动，自动获取代理帐号信息并与上网日志关联，以实现审计实名 |
| 156 |  | 应用阻断 | 可以设置禁止通过HTTP/FTP下载指定类型文件，在封堵日志里可以查看请求被拒绝的记录，并可以开放指定可信任网站下载文件；可以设置禁止或只能通过指定的邮件服务器收发邮件，包括webmail邮件，；支持URL关键字阻断功能 |
| 157 |  | 行为告警 | 支持弹出页面、手机短信、发送邮件 |
| 158 |  | 可以对HTTP（GET/POST）、SMTP、POP3、TELNET、FTP、MSN、YahooMessenger、数据库（SQL SERVER、Oracle）等常见协议或应用进行内容关键字告警 |
| 159 |  | 系统管理 | 管理员登陆支持基于Radius协议的集中身份验证，能够自动检测和指定登录密码强度；支持在指定IP地址的计算机上才能登录管理机界面  支持关联管理账号功能，多个管理账号关联之后必须依次输入账号密码才能登录 |
| #13 | # | 产品资质 | 1、具有《计算机信息系统安全专用产品销售许可证》  2、具有《信息技术产品安全测评证书》EAL3+级别 |

**A01-16 数据库审计**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★38 | ★ | 硬件规格 | ≤2U上架专用设备，≥4电口（含1个管理口），≥4个千兆SFP光口（包含光模块），1个RJ45串口，支持RAID1，≥2T存储空间，默认≥3个监听口授权，默认≥13个被审计DB服务数，可扩充，双电源 |
| ★39 | ★ | 性能要求 | 系统审计事件每秒入库速度至少在25000条/秒以上，日处理审计事件数至少15000万条； |
| 160 |  | 部署和管理 | 支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行 |
| 161 |  | 审计协议 | 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache数据库审计。 |
| ★40 | ★ | 支持国产数据库人大金仓、达梦、南大通用、神通数据库的审计。 |
| 162 |  | 对网盘文件传输的审计，可记录百度网盘、360云盘等传输的文件名、文件大小、IP地址、MAC地址、传输时间等信息 |
| 163 |  | 支持RDP协议审计，可审计关键的键盘输入，记录会话过程 |
| 164 |  | 支持FTP、Rlogin、Radius、NFS、X11等协议审计支持 |
| 165 |  | 支持对常用网络游戏、股票软件、IM软件、P2P软件、流媒体的审计 |
| 166 |  | 审计能力与效果 | 系统应内置规则集，对数据库DML、DCL、DDL等语句及FTP、Telnet等协议中的命令进行归类，便于用户定制审计策略。 |
| 167 |  | 支持数据库服务器、资源账号以及表名的自动发现，简化配置 |
| 168 |  | 支持ftp、http服务器的自动发现，ftp、http、telnet账号的自动发现，在线时间以及上报事件条数等； |
| 169 |  | 支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计 |
| 170 |  | 支持对超长SQL语句的审计 |
| 171 |  | 支持访问数据库的源主机名、源主机用户、SQL操作响应时间、数据库操作成功、失败的审计； |
| 172 |  | 支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的SQL操作审计 |
| 173 |  | 支持审计Radius协议的认证用户MAC、认证用户名、认证IP、NAS服务器IP |
| 174 |  | 基于场景的审计 | 支持对相同账号下班时间操作多于上班时间的异常操作自动发现和审计 |
| 175 |  | 支持访问操作的全审计，自动生成审计策略，自动生成报表； |
| 176 |  | 支持对于短时间内相同账号多个IP地址登陆的自动发现与审计，用以发现账号被盗用等异常； |
| 177 |  | 事件查询统计与报表 | 支持用户操作轨迹图展示，轨迹图维度可自定义，包括：资源账号、源ip、客户端程序名、命令、表名、错误码等，可根据昨天、最近七天、最近30天以及自定义时间进行轨迹显示，可显示关联数量，可在某一维度中进行筛选， |
| 178 |  | 支持按时间、级别、源\目的IP、协议名、源\目的MAC、源\目的端口为条件进行查询 |
| 179 |  | 系统应内置统计分析模板，统计模板包括且不限于：趋势分析、统计分析、性能分析等，且支持自定义模板，自定义条件包括源IP、目的IP、资源账号、客户端名称、协议等10几种。 |
| 180 |  | 支持生成Word、PDF、xls、HTML格式的报表导出 |
| 181 |  | 响应方式 | 记录审计事件、记录会话数据、忽略、界面告警、Syslog告警、SNMP trap告警、邮件告警、短信告警 |
| 182 |  | 第三方扩展接口与联动功能 | 支持SNMP方式，提供系统运行状态给第三方网管系统 |
| 183 |  | 支持Syslog方式向外发送审计日志 |
| 184 |  | 支持Syslog方式接收第三方审计日志 |
| 185 |  | 支持snmp服务器配置自定义，不同策略可选择不同snmp服务器 |
| 186 |  | 提供CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能 |
| #14 | # | 资质 | 1、具有《计算机信息系统安全专用产品销售许可证》增强级  2、具有《信息技术产品安全测评证书》EAL3+级别 |

**A01-17 漏洞扫描**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★41 | ★ | 硬件规格 | 1U上架设备，标配≥1个10/100/1000M管理口（可做扫描口）、≥9个100/1000M扫描电口、≥4个千兆SFP接口插槽（含SFP光收发模块），1个RJ45 Console口，2个USB接口，≥1个接口扩展插槽 |
| ★42 | ★ | 性能 | 不限制扫描的IP地址，并发扫描70IP。  Web应用检测模块可扫描50个域名地址，具体地址名称不限制 |
| 187 |  | 系统扫描能力 | 支持对Apple软件和应用进行扫描，包括MAC OS，Safari，itunes等  支持对主流ftp应用服务进行扫描，覆盖serv-u、pcman、core等ftp服务软件  支持对主流邮件系统服务应用进行扫描，覆盖sendmail、InetServ，Atmail等  支持对网站开源架构类扫描：支持phpmyadmin、WordPress 等的扫描  支持对主流数据库的识别与扫描，包括：Oracle、Sybase、SQL Server、DB2、MySQL等，能够扫描的数据库漏洞扫描方法不小于2400种。 |
| 188 |  | 策略管理 | 支持35种以上默认扫描策略模板，如常规安全扫描，中高危漏洞扫描，高危漏洞扫描，web服务组件扫描，网络设备扫描，云平台漏洞扫描，虚拟化扫描，主机信息收集，攻击性扫描，SQL SERVER 数据库扫描，Apple类扫描，视频监控类扫描等等，同时针对市场应急响应的漏洞提供应急响应策略模板。 |
| 189 |  | 资产管理 | 支持对部门和资产的添加、删除、编辑等操作，以及对资产的属性自定义功能； |
| 190 |  | 支持每个资产历史扫描的风险趋势图显示，缺省显示最后24次扫描结果的趋势显示； |
| 191 |  | 报表功能 | 支持输出单独的系统漏扫报表，报告中的漏洞应具备统一的CVSS国际标准评分，以准确衡量漏洞的危险级别，为漏洞修补工作的优先级提供指导。 |
| 192 |  | HTML离线报表能够通过点击主机ip链接，自动跳转至该主机的详细报告。 |
| 193 |  | 支持任务扫描完成后，支持自动将HTML、Word、Excel、PDF、xml格式扫描结果上传至ftp服务器。 |
| 194 |  | 用户管理 | 支持登录验证码，并可以设置是否启用。  支持跨网段登录g限制开关设置； |
| 195 |  | 产品升级、维护 | 支持实时提醒当前的系统消息，包括报表下载消息、升级内容消息、日志下载消息等 |
| 196 |  | Web漏扫功能要求 | 支持检测SQL注入漏洞、命令注入漏洞、CRLF注入漏洞、LDAP注入漏洞、XSS跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等。  支持漏洞验证功能，在扫描结束后，能够对结果中的重要漏洞进行现场验证，展示漏洞利用过程和风险  支持灵活的扫描任务制定功能，可设定检测开始时间、检测入口地址、网站COOKIE、检测周期、任务模式、User\_Agent设置、发包限速设置、最大检测页面数、漏洞类型设置等 |
| #15 | # | 资质 | 1、具有《计算机信息系统安全专用产品销售许可证》增强级  2、具有《信息技术产品安全测评证书》EAL3+级别 |

**A01-18 终端安全管理系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★43 | ★ | 规格参数 | 1个服务器端，至少提供2000个桌面运维终端管理 |
| ★44 | ★ | 平台管理 | 桌面运维包含终端桌面管理，终端审计，移动存储设备管理，网络准入等功能。 |
| 197 |  | 支持管理员分级管理，不同的管理员可以授权不同的区域或部门 |
| 198 |  | 支持系统策略进行导入和导出。  支持基于部门管理，支持面向不同的终端组织机构下发不同的策略 |
| 199 |  | 事件管理 | 事件能够按类别管理，包括安全基线、终端DLP、非法外联、终端杀毒事件。 |
| 200 |  | 能够对终端各事件行为进行查询和统计，且支持时间、状态等条件过滤。 |
| 201 |  | 事件支持条件过滤查询和统计，且每个事件可进行事件快照查看详细内容。 |
| 202 |  | 基于权限的报告和报表管理，管理员只能够查看和导出自己有权限的报告和报表 |
| 203 |  | 性能监控 | 可以对安装系统的服务器性能状况进行实时监控，可以监控和显示管理服务器的CPU使用率、内存使用率、系统所在硬盘分区使用率和数据库可用磁盘空间的状况。 |
| 204 |  | 注册管理 | 对于未提交注册信息的客户端，管理员可以在管理控制台集中进行手工注册。能够从客户端报表及文件导入进行注册，并可以进行批量注册。 |
| 205 |  | 桌面运维 | 能够准确统计计算机终端数量。能够自动收集计算机终端资产状况。 |
| 206 |  | 能够识别安装多操作系统的终端，方便用户对终端操作系统安装情况进行了解和统计。 |
| 207 |  | 支持离线补丁升级，对不能连接互联网的网络环境，可以使用工具对补丁分发信息及文件进行导入。 |
| 208 |  | 补丁分发支持在空闲时进行，也支持在指定的时间段内进行。 |
| 209 |  | 补丁分发前和分发后自定义提示消息补丁分发支持P2P。 |
| 210 |  | 支持客户端软件安装包的自动分发和安装，且支持MSI、EXE、BAT、脚本等格式的安装程序，支持自定义安装包 |
| 211 |  | 终端审计 | 能够对终端的非法外联行为进行监控和告警，一旦探测发现终端发生非法外联行为，即可根据设定的告警对象和告警方式，进行告警，直至非法外联行为中止后才会解除。 |
| 212 |  | 安全防护 | 能够对终端访问的目的地址、服务以及发起访问的进程进行管理，只有允许的进程才能对指定目的地址和服务进行访问 |
| 213 |  | 移动存储 | 能够对接入终端的移动存储进行认证，对未认证的移动存储设备，能给用户弹出认证和注册窗口，提示用户对设备进行认证，确保只有认证过的移动存储设备才能够在终端使用。提交认证时，除了可以填写移动设备的使用人相关信息之外，还可以选择使用人所在的部门。 |
| 214 |  | 准入控制 | 支持仅验证客户端的准入控制。 |
| 能够通过与支持802.1x协议的接入交换机互动，实现有线局域网网络准入，对接入的计算机及接入的用户进行认证。 |
| 215 |  | 基于802.1x的网络准入支持终端可信MAC认证管理。通过可信MAC认证，确保只有合法的MAC的终端通过网络准入认证接入内网。同时，系统支持管理员在线对申请接入的终端，进行可信MAC实时认证和授权。 |
| 216 |  | 防病毒 | 支持防病毒功能启用状态统计查询，能够查询已启用防病毒功能的终端和未启用防病毒功能的终端 |
| 217 |  | 支持终端杀毒概况查询，可查询全网终端病毒木马感染状态描述和感染时间 |
| #16 | # | 产品资质 | 1、具有《计算机信息系统安全专用产品销售许可证》  2、产品须具有《计算机软件著作权登记证书》；  3、具有《信息技术产品安全测评证书》EAL2级别 |

**A01-19 安全管理平台（SOC）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★45 | ★ | 硬件规格 | ≤2U标准机架式，冗余电源，专用千兆硬件平台和安全操作系统，≥6个千兆电口，≥1个管理口，≥2个USB接口，存储容量≥2TB。默认支持≥200个管理对象授权。 |
| ★46 | ★ | 运行环境 | 系统采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作用户的浏览器客户端无需安装JRE或者JAVA Web Start即可访问管理中心；  产品集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 |
| 218 |  | 部署方式 | 支持单级部署和级联部署，支持分布式部署。 |
| 219 |  | 综合展示 | 用户登录即可进入综合展示界面。通过该界面，能够快速的导航到各个功能；  用户可以自定义一级功能菜单，可以根据自身需要调整一级功能菜单的顺序；  在综合展示界面中能够显示系统的基本管理信息，包括最近30分钟告警状态雷达图、最近1小时事件趋势图、最近24小时的10条告警列表，能够显示最新1小时内的事件总数、各等级事件数量，以及事件量曲线 |
| 220 |  | 工作台 | 工作台为用户提供了一个从用户自身业务需要出发使用本系统的快速入口。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为不同角色的用户建立不同维度的仪表板；  仪表板中的每个显示区域都能够放大、缩小、拖动；  系统必须内置基本的仪表板； |
| 221 |  | 资产建模 | 用户可以自定义资产类型，并且可以针对每个资产类型自定义资产扩展属性；  用户在录入资产的时候，一旦指定该资产为某种资产类型，则会自动显示该资产的扩展属性，供用户录入和维护。 |
| 222 |  | 日志采集 | 无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能； |
| 223 |  | 日志范式化 | 系统必须具备日志范式化功能，实现对异构日志格式的统一化；  针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成；  支持长安全事件格式；  对日志设备类型、日志类型、日志级别等可进行重定义。  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。 |
| 224 |  | 日志传输和存储转发 | 日志可加密压缩传输，保证数据的完整性和机密性；  日志可加密存储。支持大数据量存储；  可根据转发条件，将采集范式化后的数据转发到其他的目标地址；  支持加密压缩方式转发，定时转发 |
| 225 |  | 日志过滤 | 要支持对无用日志的自动过滤，减少垃圾数据数量；  可以建立日志过滤条件； |
| 226 |  | 日志合并 | 要支持对无用信息的自动合并，减少垃圾数据数量；  可以建立日志合并条件，设定合并的时间范围。 |
| 227 |  | 弱点管理 | 系统具有弱点管理功能，能够导入资产的弱点信息，并计算资产/安全域/业务系统的脆弱性值。  至少支持导入启明星辰、绿盟、榕基等的漏扫结果；  系统能够通过多种方式展示资产/安全域/业务系统的弱点信息，可以查看单个资产的弱点，可以查看某个安全域的弱点值最高的10个资产；  系统具备漏洞库，所有导入的漏洞信息都可以检索，用户可以编辑漏洞信息。 |
| 228 |  | 虚拟化监控 | 能监控虚拟机名称、IP、描述、节点状态、运行时间、CPU利用率、内存利用率、网络状况、数据存储、磁盘IO、虚拟机列表  能监控每个名称、IP、描述、节点状态、运行时间、CPU利用率、内存利用率、网络状况、数据存储、磁盘IO |
| 229 |  | 虚拟化拓扑 | 能够展示虚拟化环境的概览，包括数据中心、集群、主机、数据存储、虚拟机和资源池的总体运行状况；  能够显示关键性能指标排名；  能够以拓扑图的方式可视化地自动地展示主机集群视图，能够形象展示数据中心的构成、能够实时显示每个虚拟节点的当前工作状态，能够对虚拟节点进行监控、开机、挂起、关机、重启、删除，能够远程登录到虚拟节点上；  能够自动展示出虚拟网络拓扑反映虚拟网络与虚拟节点之间的关系，可以看到虚拟交换机； |
| 230 |  | 热点分析 | 系统采用聚类算法持续地从事件的源IP、目的IP、资产类型、事件等级、事件数目5个维度（向量）朝终端、网络和应用三个群组进行聚类运算，找到当前一段时间的事件热点；  能够展示一幅热点分析图，以三个同心圆的方式展示应用层、网络层和终端层的热点信息  系统支持对热点事件进行钻取分析；  系统支持热点的历史回放。 |
| 231 |  | 事件查询 | 系统允许管理员以查询策略的形式查看安全事件；  用户可自定义查询策略，并以树形结构进行组织，形成一个查询树  可对安全事件进行模糊搜索查询；  采用任务的方式响应用户查询请求，用户不必在线等待查询结果。 |
| 232 |  | 预警管理 | 通过发布内部及外部的早期预警信息，分析可能受影响的资产，提前了解业务系统可能遭受的攻击和潜在的安全隐患。  系统的预警分为内部预警和外部预警；  内部预警支持规则自动产生，外部预警支持手工录入；  在录入预警信息的时候，可以关联到受影响的资产；  预警类型包括安全通告、攻击预警、漏洞预警和病毒预警；  系统具有预警的生命周期管理，预警信息的状态至少包括预备预警、正式预警和归档预警三种。 |
| 233 |  | 集中设备运行监控 | 系统能够对各种不同厂商的安全设备、网络设备、主机的性能与可用性进行集中化实时监控 |
| 234 |  | 集中应用运行监控 | 系统能够对各种主流厂商数据库、中间件、网络服务、以及各种应用系统的性能与可用性进行集中化实时监控 |
| 235 |  | 基于情报的事件关联分析 | 系统可提供通过导入或者主动自动抓取的方式获取外部相关网络威胁情报信息，并能将这些威胁情报用于关联分析  网络威胁情报至少包含恶意IP和恶意URL |
| 236 |  | 告警管理 | 告警动作支持告警重定义、弹出提示框、播放警示音、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、设置观察列表等方式；  告警内容可以自定义，可以根据日志的实际情况将参数传递给命令行脚本；  系统允许管理员以告警统计策略的形式从各个维度进行告警信息进行统计分析；  用户可自定义告警统计策略，并以树形结构进行组织，形成一棵告警统计策略树  告警统计策略的条件和时间段可自由设定  根据告警统计结果可直接钻取符合条件的告警信息； |
| 237 |  | 报表管理 | 系统应包含资产、事件、监控、风险等报表报告；提供内置报表模板；持按照天、月度、季度、年度等时间周期生成报表，并支持邮件自动投递；  支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况；  支持报表报告的导出，导出的格式支持EXCEL、PDF、DOC、XML、HTML、RTF等，支持Office 2007格式；  系统应包含报表编辑器，可以自定义报表。 |
| 238 |  | 系统管理 | 可记录系统自身日志，可查询；  可对系统自身的CPU、内存、数据库空间大小等进行监控；可以对自身运行的CPU、内存和磁盘空间等的使用率设置告警阈值  支持系统时间同步，确保安管平台系统与用户网络环境的时间保持同步。 |
| 239 |  | 权限管理 | 实现基于角色的权限管理，所有的用户的权限都通过角色来赋予；  要求系统管理员、审计管理员和用户管理员三权分立；系统应包含上述三类管理员。 |
| #17 | # | 产品资质 | 1、具有《计算机信息系统安全专用产品销售许可证》  2、产品须具有《IT产品信息安全认证证书》；  3、具有《信息技术产品安全测评证书》EAL3+级别 |

**A01-20 虚拟化云教室**

###### 云终端控制器（数量，1台）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★47 | ★ | 基本要求 | 软硬件一体化设备，设备到用户现场开机即用；  CPU：性能不低于1颗Xeon E3 12XX V5；  内存：≥1根16GB DDR4 ECC 2133MHz内存，且预留内存扩展槽位≥3个；  存储：企业级SSD固态硬盘≥240GB，SATA3.0企业级机械硬盘≥8TB；内外置硬盘槽位不低于4块3.5寸和2块2.5寸硬盘；  网络：≥2个10/100/1000 RJ45电口；  实配1000个云终端管理，满足学校后续云终端扩容； |
| 240 |  | 基本功能 | 出厂预装云终端控制器虚拟化软件，无需单独购买； |
| 241 |  | 云终端控制器应提供B/S架构的云终端控制器统一管理界面，提供向导式的部署方法，在部署完成后要求体检，自动生成体检报告及分数； |
| #18 | # | 提供虚拟教室功能，能够按照教室规模创建不同的虚拟教室，每个虚拟教室独立管理和配置，在云终端控制器后台能够实现对独立教室的学生终端、教师云终端分别进行配置和管理，包括镜像管理、网络访问限制、网络白名单的设置。 |
| #19 | # | 通过云终端控制器能够对教室中学生云终端和教师终端进行统一管理，能够在同一管理界面同时查看到学生云终端和教师终端；能够在云终端控制器端平台后台界面内实现对所有学生云终端批量配置，桌面批量新建、设置和删除，同时也能对教师终端进行镜像下发、配置。 |
| 242 |  | 智能云终端控制器提供云桌面的统一管理功能，能统一监控云桌面，包含但不限于以下参数：在线情况、IP地址、终端MAC地址；并可新建、修改、删除、批量生成云桌面； |
| 243 |  | 云终端控制器需要能够实现共享磁盘自动挂载功能，学生与老师共享一块虚拟磁盘，为学生设置下载权限，老师设置上传和下载权限； |
| 244 |  | 提供教学镜像隐藏功能，在云终端控制器后台对教学镜像设置后，可实现部分教学镜像对学生可见，部分镜像（如考试镜像）对学生不可见，当需要使用的时候，只需一键设置学生即可看到镜像，保证重要镜像的安全性； |
| 245 |  | 云终端控制器后台提供消息管理功能，能够对接收的消息进行存储和查看，当信息未读时能够在后台进行标识提醒； |
| 246 |  | 支持设置定时任务，能够定时关闭云终端控制器、重启云主机、关闭云终端，可按照每天或者每周设置周期性任务，具体时间点能够设置到时分秒； |
| 247 |  | 提供作业空间管理功能，对作业空间的学生与老师账号进行统一管理，可以对学生使用的作业空间存储空间进行管理； |
| #20 | # | 云终端控制器底层虚拟化系统为自主研发系统，要求提供中华人民共和国国家版权局颁发的云终端控制器底层操作系统的软件著作权登记证证书扫描件； |

###### 教学管理软件（数量：1套）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| #21 | # | 产品要求 | 为便于课堂多位老师使用，要求提供C/S架构教学管理软件平台，平台至少需要包含教师端和学生端，并且教师端和学生端能够进行互动教学。 |
| 248 |  | 支持作业空间授权，支持屏幕广播、学生监控、文件分发等教学常用功能，支持在线升级和教学应用扩展，实配软件本体及105个云终端授权； |
| ★48 | ★ | 基本功能 | 一套教学管理软件能够实现教学业务，同时能够提供部分终端管理功能，比如禁网、教室终端一键部署、终端参数配置、终端编号等，不接受在教师机上安装多个软件来实现教学管理和终端管理功能； |
| #22 | # | 提供教室环境体检工具，并根据体检结果打分和输出体检报告，如果体检分数不合格，必须给出修复项辅助进行设备健康维护。 |
| #23 | # | 能够配合云终端控制器实现当云终端开启时自动进入多种独立教学镜像选择界面，学生可以根据需求选择相应的教学镜像进行使用，不同云终端之间系统互不影响。 |
| 249 |  | 能够根据教学需要选择相应的教学镜像，并可以通过镜像选择实现所有终端一键切换到教学镜像环境中，云终端无需重新启动，老师也无需登录云终端控制器后台进行操作； |
| 250 |  | 教学管理软件能够实现一键关闭所有云终端（终端物理机和虚拟机），一键关闭教学云终端控制器，不需要访问云终端控制器后台进行繁琐操作，只需要在C/S教学管理软件上完成即可； |
| 251 |  | 支持实时监看功能，老师通过教学管理软件能够实现对学生机屏幕的监看，要求满足同时监看多个屏幕或放大监看某个特定学生屏幕细节，细节学生终端上打开的软件，使用的操作以及鼠标变化和移动轨迹； |
| 252 |  | 支持远程终端编号功能，并与云桌面编号一一对应，方便上课前的学生点名等； |
| 253 |  | 支持老师对单一、部分、全体学生广播教师机屏幕，实现多媒体教学，并且可以选择是否将教师机的麦克风声音或系统声音广播给学生；支持老师将指定学生的屏幕图像广播给其他所有学生，老师也能看到该指定学生的屏幕图像。 |
| 254 |  | 支持老师将选中的文件分发给学生，可以分发给所有学生，也可以分发给指定学生；同时，学生也可以直接将文件提交给老师； |
| 255 |  | 支持老师在作业空间为多个或单个班级的学生布置作业，布置内容可支持各种文件格式。老师可以对作业上交截止时间限制。学生端可以看到老师布置完的作业； |
| #24 | # | 产品资质 | 提供中华人民共和国国家版权局颁发的软件著作权登记证证书扫描件； |

###### 云终端（数量，80台）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★49 | ★ | 基本要求 | 云终端为一体机样式：  1、云终端要求内置虚拟桌面系统；  2、配置≥1颗四核四线程处理器（处理器主频≥3.6GHz）或更好；内存容量≥4GB，本地存储≥256 GB SSD；  3、配置≥21.5寸显示器，分辨率≥1920×1080；  4、配置USB接口≥6个（包含≥2个USB 3.0接口），≥1个千兆网口，≥1个HDMI接口，≥1对音频输入输出接口；  5、配置≥1个内存扩展槽（最大可扩展4GB内存条），≥1个SATA扩展接口，可扩展1个2.5英寸硬盘； |
| #25 | # | 具备独立的关屏功能键，可实现一键关闭屏幕显示，但系统不会休眠或者关机，方便用户打开显示器后的流畅使用体验；具备屏幕亮度调节功能键，可实现屏幕亮度增加、减弱功能； |
| #26 | # | 基本功能 | 支持多种系统的教学镜像，提供给不同课程教学使用，不同的教学镜像可供学生自由选择，上课期间老师可以要求所有云终端统一进同一个镜像进行教学。 |
| ★50 | ★ | 支持完全离线模式，即在云终端控制器连接中断时，依然可使用当前正在使用的镜像环境，保障业务连续性； |
| 256 |  | 支持终端显卡透传，能够将终端物理显卡透传至虚拟机中； |
| 257 |  | 支持主流图形设计类软件，如autoCAD、3DMAX、PS等流畅运行，保障业务平稳开展； |
| ★51 | ★ | 支持4k清晰度高清视频流畅播放。 |
| 258 |  | 云终端提供公共存储空间，该空间可供不同课程学生上课使用，可存储部分临时文件，在云终端控制器端能够对所有云终端的公共空间提供统一管理功能，并能进行批量删除； |
| 259 |  | 对于云终端控制器所提供的虚拟桌面提供关机还原模式，保证系统不会中毒且易于管理，且个人数据盘数据不得丢失； |
| 260 |  | 对于云终端控制器所提供的虚拟桌面提供个性化模式，可保证用户数据和操作系统完全保存，用户安装的软件及数据在重启后均可保留； |
| 261 |  | 支持镜像断点续传功能。当用户关闭终端时，暂停下载更新任务，当终端再次启动时，应用断点续传技术，继续下载未完成的更新任务； |
| #27 | # | 提供中华人民共和国国家版权局颁发的操作系统的软件著作权登记证证书扫描件； |

**A01-21 精密空调**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 262 |  | 空调类型 | 风冷 |
| 263 |  | 机械性能要求 | 外观工艺：机柜表面喷涂均匀、无破损；信号灯、开关、测量显示装置布局合理。  结构工艺：部件排列合理、整齐；导线颜色和截面合理，布放平整；接插件牢固；进出线符合工程需要；具备抗震措施。  输入电压允许波动范围：380V +15%-10%。（说明：适应电网电压变化范围宽）  频率：50Hz  2Hz。 |
| 264 |  | 总制冷量（kW）（回风24℃，RH50%） | ≥65KW |
| 送风方式 | 地板下送风 |
| 室内风机类型 | 后曲叶片式离心风机 |
| 室内风机送风量（m3/h） | ≥15600/26000 |
| 室内风机数量 | 2个 |
| 265 |  | 过滤器类型 | 中效EU4 |
| 266 |  | 压缩机数量 | 2 |
| 压缩机类型 | 涡旋式压缩机 |
| 适应制冷剂类型 | 环保制冷剂 |
| 制冷回路 | 2 |
| 267 |  | 加热器 | 全铝制电极 |
| 加热量 | 不小于15kW/24KW |
| 调节量 | 三级 |
| 加湿器 | 电极式 |
| 加湿量 | 不小于8kg/h |
| 湿度 | ≤95%RH |
| 室外工作温度 | -20℃~ +50℃ |
| 268 |  | 性能要求 | 能按要求自动调节室内温、湿度，具有制冷、加热、加湿、除湿等功能；  温度调节范围：24℃  温度调节精度：±1℃；温度变化率< 5℃/小时；  湿度调节范围：40% ~ 60%RH；  湿度调节精度： ±5 %RH；  具有高效节能性，压缩机采用具有较高的能效比的涡旋式压缩机；  具有LCD大屏幕显示器，能显示温湿度及各组件的运行状态的功能，并能显示蒸发器出口过热度和压力；应具有大容量的故障报警记录储存的功能；机组应具有过压 、欠压等报警及故障诊断，告警记录功能，自动保护，自动恢复，自动重启动等功能。控制系统应具有密码保护功能；控制器具有主被控制功能；  当室内热湿负荷增加时自动启动备用机组；  机房专用空调机组的送风余压能自动调整，且送风余压的自动调整不会改变机组的送风量；  室外机组应该采用耐腐蚀的铝合金外壳结构，室外机组选用无级变速控制器； |
| 269 |  | 压缩机性能 | 为了增高设备的高效节能性，机组设备应采用电子式膨胀阀，随着环境的要求，自动调整制冷量 |
| 270 |  | 安全性 | 空调机组标准配置储液罐和干燥过滤器以提高系统的安全可靠性 |
| 271 |  | 机组维护 | 机房专用空调机组应满足不同工况和负荷下的应用；应保证零配件在10年内都能得到随时更换。  机组的维护性：提供100%正面完全维护。 |
| ★52 | ★ | 质保 | 提供原厂3年质保 |

**A01-22 UPS**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 272 |  | UPS | 模块化UPS系统。UPS模块并联采用分散控制技术，确保整机可靠性； |
| 273 |  | 总体要求 | UPS主机系统柜体分为功率模块柜和开关接线柜两部分，其中功率模块柜最多可承载不少于10个可热插拔的UPS功率模块；开关接线柜中包括主路输入开关、旁路输入开关、手动维修旁路开关、输出开关及可插拔式静态旁路模块等。单个功率模块不小于30KVA,整机框架不小于300KVA。 |
| 274 |  | 整流器 | 满载时，输入谐波电流总含量＜3%；输入功率因数＞0.99；  半载时，输入谐波电流总含量＜5%；输入功率因数＞0.98。 |
| 输出因数 | 输出功率因数1，带超前0.5～滞后0.5负载不降额。 |
| 效率η | 50%以上负载时，≥95%；  25％负载时≥94％； |
| 输出波形为连续的正弦波，在带100%不均衡负载时，电压波形失真度 | 100%线性负载 ≤1％  100%非线性负载 ≤3％。 |
| 逆变器过载能力 | 110%额定电流 60min  125%额定电流 10min  150%额定电流 60s  短路限流能力≥2.9In  旁路过载能力： （1000%额定电流 100ms） |
| 275 |  | 输出电压相位偏差 | 在100%不平衡整流性负载时，三相输出电压相位差≤1°。 |
| 设备操作界面要求 | 设备应能提供全中文监控及操作界面和全中文远程监控管理界面，应提供全中文显示的LCD显示器，尺寸不小于80mm×80mm，能够显示输入输出电池电压、电流和相关运行状态以及故障告警信息等。 |
| 276 |  | 外观设计要求 | 采用标准服务器机架外观设计，冗余模块化UPS系统（不含电池）的总体外观尺寸满足：高度≤2000mm，深度≤1100mm，宽度≤1200mm。 |
| #28 | # | 安全 | 投标方所提供的UPS设备必须通过7、8、9烈度的抗震性能检测，并提供相应的抗震性能检测合格证和检验报告资料。 |
| 277 |  | 其它 | 投标方需要提供所提供的UPS设备系列产品的设备可靠性MTBF计算书 |
| CQC节能证书和节能测试报告 |
| ★53 | ★ | 质保期 | 提供原厂3年质保 |

**A01-23 服务器机柜**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 278 |  | 机械设计要求 | 1. 重载设计，每个机柜最大静态和动态可承重1000kg以上。 2. 机柜尺寸为：高42U x 宽600mm x 深1070mm或以上。 3. 喷塑表面处理，黑色。 4. 材料为冷轧钢板，防护等级IP20。 5. NEMA 1 级机柜。 6. 机柜前后标准配置安装设备的黑色角轨，上面喷涂白色U标识。 7. 移动脚轮设计，标配可调整式支撑脚。 8. 每面侧板为整板设计，具备加强筋，可保证机柜的稳定性。 9. 可选装门磁锁。 10. 双开后门设计有助于优化地板空间的使用，后门的开关只需要占用 300 mm 的操作空间，方便对设备进行维护、操作。 11. 标准配置并柜附件，利于机柜成排摆放后的稳定和美观，同时提供机柜的抗震性能。 12. 机柜的顶盖、侧面板和前后门通过机柜架接地。机柜架上至少有八个电气接地插头用于外部接地。 |
| 279 |  | 机柜功能要求 | 1. 机柜采用冷轧钢主体重型加硬框架焊接结构，框架立柱由厚度不小于1.5MM(采用九折型材工艺)冷轧钢板制成；水平支撑不少于3对。 2. 机柜底部预留与安装基座固定的孔位。按招标要求，部分机柜需要和底座固定安装，保证稳定性，,机柜必须符合现场已施工完成的底座的安装条件。 3. 四根安装立柱双面打孔，可任意调节托板高度，也可前后灵活调整。 4. 机柜表面必须经过防静电喷粉等喷涂工艺处理，保证机柜拥有高强度的防腐蚀性、防静电性、防盐雾性； 5. 机柜箱体表面折角处不带有皱纹、裂纹、毛刺、焊接等痕迹。门与门框的缝隙不超过1.5mm，且四周缝隙均应保持一致。门开启灵活，不会产生卡阻现象； 6. 机柜前后门采用超级通透六角网孔门，网孔呈蜂窝状高密度有序排列，网孔通风率不低于75% |
| ★54 | ★ | 承重 | 机柜应确保高刚性、轻量化，静态承重不低于1600公斤（证明文件）； |
| 280 |  | 立柱 | 机柜中间增加2根辅助方孔条，安装与前后方孔条中间位置，增加2根后立柱，增加机柜的承重性能，立柱不少于8根 |
| 281 |  | 安装方式 | 机柜可以并列安装，随机配有并机连接件。两台机柜间前后共6点并柜，机柜应采用专用并柜件从侧面锁螺钉拉紧，稳定可靠。机柜并柜后，柜体之间无明显的透光缝隙；并柜件合理设置，便于拆卸，不影响其他配件的安装及冷热通道的封闭。 |
| 282 |  | 工艺 | 柜制造工艺符合国际IEC标准，通过UL认证或者RoHS认证或者是同等级别的其它国际认证 |
| 283 |  | 安全 | 符合《通信设备安装抗震设计规范》，机柜达到抗震设防烈度8度，并提供投标产品第三方机构专项的抗震检测报告 |
| ★55 | ★ | 质保 | 提供原厂3年质保 |

**A01-24 关系型数据库**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★56 | **★** | 基本要求 | 采用当前成熟技术的数据库管理系统产品，提供软件著作权证书 |
| 284 |  | 支持Linux主流操作系统。支持国产操作系统和国产芯片、国产中间件。 |
| 285 |  | 支持ODBC、JDBC、OLEDB、.Net Data Provider(NDP)、PHP、Perl、ESQL等开发接口，提供与Oracle OCI、Pro\*C、C++、PL/SQL兼容的开发接口； |
| ★57 | **★** | 针对信息系统中文字符要求，数据库需要支持UNICODE、GBK和GB18030字符集；产品必须符合GB18030-2005强制性部分的要求，可提供相关认证证书。 |
| 286 |  | 支持水平范围分区和水平列表分区技术，支持组合分区技术，支持两种以上的垂直分区技术。 |
| #29 | **#** | 具备高性处理能力，单机数据库事务处理能力TPMC值能达到100万级、在线连接数能达到10万级和并发连接数达到万级处理。 |
| 287 |  | 可靠性要求 | 支持多种备份还原方式，包括物理和逻辑的备份与还原、全部/增量的备份与还原、基于时间点的备份与还原、联机与脱机的备份与还原等，支持并行的逻辑备份还原。 |
| 288 |  | 产品不依赖第三方HA软件部署双机集群部署，实现主备故障自动切换高可靠性。 |
| ★58 | **★** | 产品支持读写分离集群，支持一主多备，实现数据零丢失且支持故障自动切换、失败节点自动加入。 |
| 289 |  | 安全性要求 | 产品安全级别应达到《GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求》第四级。 |
| 290 |  | 产品支持三权分立、身份认证、系统权限、数据对象权限、列级权限的自主存取控制；支持语句审计、特权审计、对象审计、用户审计等多种审计策略手段； |
| 291 |  |  | 产品支持数据存储加密、SSL传输加密、快速数据销毁能力，支持基于覆写技术擦除手段； |
| 292 |  | 管理性要求 | 提供命令行客户端及基于跨平台技术的风格统一的全图形化客户端管理维护工具，同时支持基于Web的管理工具，可进行本地和远程联机管理。 |
| #30 | **#** | 产品支持数据库健康检查，提供在线检查和离线检查、数据库文件、数据文件、事务日志、控制文件、数据字典等文件的完整性检查、CPU、内存、磁盘等信息的检查。 |

**A01-25 操作系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★59 | ★ | 总体要求 | 64位企业版国产操作系统； |
| 293 |  | CPU支持 | 最大逻辑CPU支持数量：x86-64：288(4096) |
| 294 |  | 内存支持 | 最大内存支持：  x86-64：12TB（64TB） |
| 295 |  | 单个文件大小 | 单个文件最大支持：  Ext4：16TB  GFS2：100TB  XFS：100TB |
| 296 |  | 文件系统大小 | 文件系统最大支持：  Ext4：16TB  GFS2：100TB  XFS：100TB |
| CPU架构支持 | 支持多种硬件架构，包括Intel 及 AMD 的x86/x86-64架构，国产龙芯、兆芯、申威等架构，以及PPC架构、IBM公司Power8架构技术； |
| ★60 | ★ | 硬件兼容性 | 支持主流服务器硬件产品； |
| ★61 | ★ | 数据库兼容性 | 支持国内外主流数据库产品，包括人大金仓、达梦、神通、南大通用、Oracle、DB2等数据库产品 |
| ★62 | ★ | 中间件兼容性 | 支持国内外主流中间件产品，包括东方通、金蝶、中创、普元、汇金、Weblogic、Websphere等中间件产品； |
| 297 |  | 无商业限制 | 无CPU、用户数的商业限制； |
| 中文支持 | 提供中文化的图形操作界面，支持多种输入法，支持多种安装方式，提供一键式快速安装部署支持； |
| 便捷管理 | 提供一体化图形运维工具集，包括多网卡绑定工具，对网卡、IB卡实现快捷直观的网卡绑定，提高网络性能；存储链路配置工具，有效解决存储多链路问题； |
| 298 |  | 备份恢复 | 提供安全备份恢复工具，支持对整个已安装操作系统及数据分区的镜像备份和恢复；支持主流备份软件厂商产品。 |
| 299 |  | 安全要求 | 提供安全策略定制功能，包括Root权限限制、双因子认证体系、核心数据加密存储、加密文件系统、入侵检测、防火墙等，能够有效防范系统漏洞与各种攻击方法； |
| 300 |  | 集群支持 | 提供对高可用集群的良好支持，并有方便的管理及配置工具； |
| 301 |  | 虚拟化支持 | 提供对 KVM、Xen、VMware、VirtualBox、Hyper-V等虚拟化技术的支持，可作为host OS 或guest OS 实现对云计算管理平台的管理支持； |
| 302 |  | 集成基于KVM的服务器虚拟化功能，只需设置密码即可一键式安装部署，高效快捷；为满足管理员在 Windows上对虚拟化日常管理，提供虚拟化的 Windows客户端，提升管理便捷性； |
| 303 |  | 提供对虚拟化组件的安全加固技术，提供可信引导、文件数字签名、虚拟机镜像加密、入侵检测及快速恢复功能，全面提升虚拟化物理节点的安全性。 |

**A01-26 应用中间件**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 304 |  | 开放性标准 | 支持HTTP、XML、LDAP、Web Services等多种开放性标准。 |
| 305 |  | 主流硬件平台 | 支持主流硬件平台，列出所支持的硬件平台。 |
| 306 |  | 主流数据库 | 支持多种数据库，如Oracle、MS SQL Server、DB2、Informix、Sybase等，并对国产数据库如达梦、金仓有良好的支持。 |
| 307 |  | 主流操作系统 | 支持Linux、UNIX、Windows等平台的最新发行版本,并对国产操作中标、红旗等有良好的支持。 |
| 308 |  | 微内核体系 | 支持微内核体系，可以更节省的使用资源。 |
| 309 |  | 类加载 | 提供多种可配置的类加载策略，支持动态类加载。 |
| 310 |  | 多级缓存 | 支持多级缓存技术，能够对Web静态内容、实体Bean等对象进行缓存。 |
| 311 |  | 分布式事务 | 支持分布式的事务，能够跨越多种的资源类型（如数据库、消息等）。 |
| 312 |  | 事务恢复 | 支持JTA事务恢复功能，即使在执行事务的过程中出现停电等导致服务器不正常关闭的情况，在服务器重启后，会自动恢复事务的执行，保证业务数据的完整性和一致性。 |
| 313 |  | 消息集群和智能路由 | 支持JMS消息集群和智能路由功能。 |
| 数据库连接 | 支持数据库连接池，具备连接配置向导；能够对连接进行健康性检查，提供数据访问优化。 |
| 314 |  | 部署方式 | 支持热部署、远程部署等多种部署方式。 |
| 315 |  | WebSocket规范 | 支持规范WebSocket JSR-356。 |
| 316 |  | SIP Servlets规范 | 支持SIP Servlets 规范（JSR289）。 |
| 317 |  | 异构集群 | 支持异构集群技术。 |
| 负载均衡器 | 支持纯Java编写的负载均衡器，支持随机选择策略、轮询策略和权重策略等负载策略，支持对负载均衡策略进行第三方扩展 |
| 318 |  | 动态扩展 | 在业务系统不宕机的情况下，支持动态增加服务器，扩充系统性能。 |
| 319 |  | 负载均衡种类和方式 | 内置并支持第三方负载均衡，如Apache、微软的IIS等，请说明所支持的负载均衡的种类和方式。 |
| 320 |  | 客户端缓存 | 支持客户端缓存（CSC）技术。 |
| 291 |  | 命令行管理工具 | 提供命令行管理工具可以完成通过图形管理工具的管理和配置功能，可对服务器中的服务进行配置，并可察看各配置项的帮助信息。 |
| 292 |  | 开发工具 | 提供基于EClipse体系的开发工具，必须支持可视化、拖拽式的Web应用开发。 |
| 293 |  | 域管理 | 提供基于应用服务器域概念的管理，一个应用服务器安装能够实现多个域的创建和启动。 |
| 集群管理 | 提供集群管理控制工具，管理集群中的任意一个节点服务器。支持图形化集群管理、集群应用部署、集群数据源配置等功能。 |
| 294 |  | 性能监测及分析工具 | 提供性能监测及分析工具，通过多种图形化展示方式，观察最近自定义时间段内应用服务器组件及服务的运行状况，如JavaEE组件、数据源、用户会话、JTA事务、HTTP链接、JVM内存、线程和类加载等，同时还能提供故障诊断及分析、实时活动服务监控、请求事务分析、获取动态StackTrace、应用程序SQL优化、警报和例外监控、监控扩展适配器、统计分析及报告、基于域的综合监控等额外监控内容。 |
| 295 |  | 认证方式 | 提供安全机制，能保证数据传递的安全性；支持JSSE，提供单向的和双向的SSL配置方式，兼容want认证方式。 |
| 296 |  | 安全证书 | 全面支持多认证中心、级联证书。 |
| 297 |  | LDAP目录集成 | 支持在LDAP目录基础之上的内置安全性数据存储，并能与主流的第三方LDAP服务器集成。 |
| 298 |  | IP过滤配置 | 提供访问过滤配置功能，拒绝ip或者ip段的机器访问web应用，达到防攻击效果。 |

**A01-27 综合运维管理系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★63 | ★ | 总体要求 | 系统应支持对网络设备、主机、数据库、中间件、应用、存储设备、CMDB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。功能包含业务服务、事件告警中心、资源管理、网络拓扑、配置管理、统一门户展现等。实配1000个资源管理授权。 |
| 299 |  | 架构要求 | 平台应采用分层、模块化的设计技术，模块与模块、层与层之间松散耦合，在不同的管理层次均有相应的处理模块，各管理模块既相互独立工作，也具备良好的耦合性，能够形成一体化运维平台。 |
| 300 |  | 兼容性要求 | 支持对多厂商、多类型、多版本资源的统一管理，包括各品牌的网络设备、安全设备、服务器、虚拟化资源、存储设备、应用等，能显示所有资源列表，可按照资源状态、事件级别、资源类别、资源组等条件快速筛选查看； |
| 301 |  | 配置要求 | 提供IT资源的统一监控，包括网络监控、业务监控、可视化展示平台、CMDB、配置管理、统一权限控制、流程自定义、报表、统一门户、移动门户等。可管理交换机、路由器、防火墙、无线AC、服务器、数据库、应用、AP资源 |
| 302 |  | 业务服务 | 为反应业务系统运行情况，应提供业务系统与IT资源之间自定义建模的功能，可自定义业务所关联的关键IT资源，包括服务器、网络设备、应用平台软件等。 |
| 业务系统的可用性、健康度、繁忙度等关键指标支持自定义计算规则。 |
| 为从宏观和整体角度掌握所有IT系统的运行情况，系统应提供IT整体健康指数的量化指标，使运维部门的管理人员清晰了解当前整体IT系统的好坏，以及IT整体健康情况的历史走势。通过分析IT整体健康指数了解其影响因素是哪些业务系统； |
| 业务系统的运行情况不仅仅通过IT基础架构的运行数据来体现，还需要将业务系统自身的业务数据纳入统计范畴。因此系统应提供对外的API接口，可对接业务系统推送的自定义业务指标，或通过执行脚本等形式主动获取用户所关心的业务数据； |
| 303 |  | 网络拓扑 | 自动发现网络拓扑，拓扑图应能直接提供设备状态、链路带宽流量、告警故障信息，查看拓扑对象的事件信息；使用不同方式展示管理对象的状态信息，如颜色、粗细、图标等方式，并能支持数据下钻功能，查看每个设备和链路的详细信息，如设备的详细信息、告警详情、面板信息、网络接口、业务结构图、配置管理、下联设备等； |
| 304 |  | 告警管理 | 支持告警与知识库的关联，受理后的告警解决方案能够直接生成知识，支持关键字的设定，根据关键字，今后出现类似的问题，直接提供知识解决； |
| 305 |  | 支持基于业务应用视角进行故障告警管理；基于业务系统可用性事件及性能事件进行故障判断并设定告警级别。 |
| 306 |  | CMDB | 配置项要支持多种构建方式以方便构建配置管理数据库，包括自动发现、手动录入、批量导入等。CMDB要具备按用户分权管理功能。 |
| 为了定期掌握配置项信息的变化情况，系统应支持配置审计功能。支持对加入到CMDB中的资源进行配置审计，可以根据设定的时间周期定期自动比对，并生成审计报告，提醒CMDB中发生变化的数据对应的配置项；支持添加、删除、修改和导出配置审计的操作。 |
| 307 |  | 统计报表 | 作为运维管理系统决策分析的依据，系统应提供报表查询的功能。支持自动生成报表和实时查询报表的功能。系统内置多纬度多视角报表模版，包括：资源报表模版、告警报表模版、流量报表模版、存储报表模板等； |
| 308 |  | 安全运维一体化 | 支持syslog、文件、WMI、SNMPTrap、数据库等多种接入方式，目标机无需安装任何代理； |
| 支持主流厂商安全设备、服务器、网络设备、中间件等设备日志自识别接入；并支持非主流设备日志的自定义接入解析 |
| 支持为安全事件收集功能设置过滤条件，可过滤无关安全事件，满足根据实际业务需求减少减少对网络带宽和数据库存储空间地占用 |
| 支持接收安全事件告警。1、可接收安全事件（无需二次开发），并将安全事件转为告警。2、支持在告警台、网络拓扑、业务拓扑上查看监控资源的安全事件告警； |
| 309 |  | 统一门户展现 | 不同角色的人员因为管理层次、管理范围的差异，关注点各有差异。系统应支持根据不同角色，定义不同的主界面，可将资源、拓扑、告警、流量、报表等信息在统一门户展示；支持自定义每个页面的展示内容和窗体标题；支持拖拽方式布局每个窗体的大小和位置。 |
| #31 | # | 产品资质 | 要求提供中华人民共和国国家版权局颁发的软件著作权登记证证书； |
| 投标产品提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

**A01-28 数据交换**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| ★64 | ★ | 工业标准要求 | Web服务：WS-I Basic Profile、SOAP、WSDL、WS-Attachment、MTOM、WS-Security、JAX-WS、JAX-RPC、JAAS、SAAJ、REST  通讯协议：JMS、HTTP/s、JDBC、SOAP、REST  数据类型与格式：CSV、XML、JSON、JAVASCRIPT  监控管理及其他：JMX、JNDI |
| 310 |  | 全面支持Web服务 | 既支持对各种系统提供的Web Service进行访问，又能够将常用业务流程或组件封装成Web Service供外部应用访问。  既支持对SOAP消息包进行解析，方便消息格式转换，又支持不对SOAP消息包进行解析，直接穿透代理的模式。  提供完善的安全保障，包括支持HTTPs协议、消息加密/解密、消息签名/验签、用户身份认证等，并提供基于JAAS方式的身份验证和授权扩展机制。  提供Web Service 附件处理能力，支持将超大附件转储成临时文件的功能。  支持Web服务的常用协议，如SOAP、WSDL、WS-Security、WS-Attachment、UDDI、RESTful API等。  支持和Axis、Axis2、CXF、.NET等多种开发平台进行交互。 |
| #32 | # | 丰富的协议适配能力 | 支持多种通讯协议和外部系统应用系统进行交互，如File、JDBC、JMS、HTTP/s、SOAP、REST等，通过流程编排，轻松实现任意两者之间的协议转换功能。  应包含多种适配器，如支持结构化和非结构化文件读写的文件类适配器、能根据文件名的特点将文件夹下的文件分成不同的类，每类文件调用不同的文件处理服务；支持异步传输协议的JMS适配器、HTTP/s适配器、Web服务适配器等，通过现成的适配器，减少程序员开发工作量，实现快速应用集成能力。  应具备数据库处理组件，支持和主流关系型数据库如Oracle、SQLServer、DB2、Sybase，开源数据库MySQL、国内数据库金仓、达梦等进行交互。支持和主流非关系型数据库如Hive、HBase、MongoDB等进行交互。所有适配过程均需通过可视化界面进行配置。  此处需要针对功能指标进行产品演示。 |
| #33 | # | 完善的数据加工能力 | 支持数据库、文件、XML、JSON、NoSQL(Hive、MongoDB)、Web服务、JSM等之间的转换加工处理。支持基于时间戳、标志位回写、数据库日志CDC的增量加工处理。  支持多种转换加工方法，能通过web界面可视化配置包括不限于字符串转换、时间类转换、数据比对与翻译、数学运算、身份证格式转换等转换方法。  支持多种逻辑处理方法，能通过web界面可视化配置包括不限于：格式匹配检查、字符串逻辑检查、空检查、重复记录检查、范围内检查、逻辑检查、复合逻辑检查、自定义逻辑检查等。  支持加工过程中的数据质量检查，根据数据逻辑判断规则，将干净的数据装载到目标中，将判断有问题的数据路由到数据库表或者数据文件中。  支持数据脱敏处理，支持在保留数据原始特征的条件下，对某些敏感信息通过脱敏规则进行数据的混洗、值变换、加密、遮挡、空值插入等处理，实现敏感数据及个人隐私的可靠保护。  所有配置过程均需通过可视化界面进行配置。  此处需要针对功能指标进行产品演示。 |
| #34 | # | 数据传输与多样调度能力 | 提供数据传输功能。支持将数据、文件、文件夹下的文件传输到目标中。支持变化文件传输，支持按条件选择文件传输，支持加密、压缩等处理，可以设定规则对文档归档或者清理。  支持在一个可视化配置界面内实现跨网段的两个交换节点之间的交换，交换的数据源和目标可以是文件、数据库、接口。为了安全考虑被交换的数据库通讯端口不对外开放，只能通过交换节点获得表的结构信息，要求通过简单配置能实现数据库表之间的相互交换。  为了安全的考虑，支持基于中心节点中转（可以不在中心保存数据）的数据交换能力，两个交换节点分别对应两个部门（或系统），中转节点对应中心，两个节点通过中心中转交换（不在中心保存数据）。要求经过简单可视化配置实现两个交换节点通过中转节点交换数据，交换的数据源和目标可以是文件、数据库、接口。该交换服务支持长连接情况下的大数据量交换，保证事务的完整性。  为了安全的考虑，要求支持单向连接通讯方式，如中心和前置节点交换重要数据时，只允许中心单向连接前置节点，不允许前置节点连向中心，只能由中心节点通过推、拉方式交换文件和数据库的数据。要求提供数据库表之间交换的服务配置界面，拉方式交换等。  所有配置过程均需通过可视化界面进行配置。  支持基于菜单的交互调度、定时调度。要求提供可视化界面。支持文件分类调度。能根据文件名的特点将文件夹下的文件分成不同的类，每类文件调用不同的文件处理服务；要求提供可视化界面。支持流程调度功能。支持平行处理、顺序执行、条件处理、意外处理；可根据CPU、I/O、网络等情况调整并行处理的并发数。当流程运行出意外时，可选择补偿运行、断点续运行、间隔检查运行等处理方式。要求提供可视化界面。  此处需要针对功能指标进行产品演示。 |
| #35 | # | 数据共享支持能力 | 提供数据共享功能，基于web能可视化配置出数据交换共享服务，包括数据查询服务、订阅比对服务、数据操作服务。提供服务目录管理，支持服务的发布、变更等管理。提供服务流程管理，包括服务的申请、审核/审批等。  可视化配置出交换共享服务的转换加工、逻辑处理、交换过程中的数据质量检查等功能。  可视化配置出数据交换共享服务的数据安全脱敏功能，支持加密、遮挡、混淆、值替换等脱敏处理方法。  提供服务的安全授权功能，授权用户允许访问的服务，支持白名单、IP约束等功能。  提供访问控制，只有通过身份验证、访问控制的用户才能访问，对于不允许的IP，拒绝访问。  提供服务运行池管理，能设置允许并发访问数。  此处需要针对功能指标进行产品演示。 |
| 311 |  | 数据集成组件支持 | 消息处理组件  数据转换组件  协议适配器 |
| #36 | # | 产品资质 | 具备国家版权局颁发的数据交换共享平台或数据处理交换平台类著作权证书。 |

**A01-29 内容管理**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 312 |  | 设计及扩展性要求 | 投标方所提供的内容管理系统，应采用模块化、组件化设计，成熟稳定，可用性强。可实现网站信息更新的灵活性、方便性、一致性、动态性和可扩展性。 |
| 313 |  | 需求理解 | 网站用户应分为前端用户和后台维护人员，两类用户各自独立。前端用户为一般浏览者，后台维护人员为信息维护员。不同的信息维护员有不同的权限和界面，支持远程信息维护，并使用系统管理员分配的用户名及密码登录，从而保证信息维护的方便性和安全性。  网站内容管理系统要求是对整个网站及网站的用户、部门、菜单、权限等进行管理。网站后台信息维护人员负责网站的信息发布、维护、修改等工作。网站内容管理系统提供统一的平台界面，实现对网站的整个内容管理 |
| 314 |  | 功能要求 | 站点（群）管理、栏目管理、模板管理、可视化内容编辑器、一键转载、信息发布、多终端信息发布、热词管理、专题管理、资源库管理、系统管理、统计分析 |

**A01-30 报表软件**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | | **指标要求** |
| 315 |  | 多表体控件式报表设计 | | 软件应提供报表设计工具，采用图形化设计界面，实现控件式、多表体设计，支持选项卡切换展现，可独立制作报表。支持工字型、田字型、上下型、左右型，并可嵌套展现，支持表格、图片、统计图、GIS地图、富文本等混合展示，表格编辑上支持合并拆分单元格、任意表头、多级斜线、字体设置、序列填充、格式刷等，能实现各种复杂报表的快速设计。 |
| 316 |  | 拖拽式多维分析 | | 系统应提升报表分析的交互能力，通过鼠标拖拽操作就实现数据的分析展现，拖拽式多维分析的结果可以保存为固定方案持续使用。 |
| 317 |  | 分布式数据库 | | 软件支持分布式数据库，并可通过适配基于hadoop框架hive架构下的其他分布式数据库，在分布式数据库上运行软件。 |
| 318 |  | Word分析报告 | | 软件可以提供WORD式分析报告的功能，分析报告中的动态内容如数字、文字、统计图、表格等可从其他报表中获取，可以像编辑WORD文件那样编辑自己的分析报告。 |
| 319 |  | 中间件集成 | | 可以与现有J2EE项目进行JAR包方式无缝集成，不依赖单点登录或者跨系统调用方式 |
| 320 |  | 填报 | 支持不依赖于数据库基于填写的数据由业务人员自行生成统计表，将数据结构化后保存，可保存为二进制文件，不占用数据库资源，填写报结果分析控件，提供源代码 | |

**A01-31 工作流及表单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 321 |  | 软件环境兼容性 | 需支持国产麒麟等国产主流操作系统 |
| 322 |  | 硬件环境兼容性 | 需支持基于X86的pc服务器 |
| 323 |  | 权限要求 | 工作流系统提供完善的权限控制体系，按照最小授权原则进行授权；支持用户可根据实际情况将模块、流程、组织机构、按钮等系统资源经由严密的权限审批流程分配给不同的角色。工作流系统支持分配的权限包括访问、管理以及分级授权等。 |
| 324 |  | 标准及规范要求 | 1.工作流定义、引擎模型设计和接口设计方面遵循WFMC工作流标准。  2.引擎建模实现支持BPMN规范，通过对流程对象类型的扩展，可以实现各种BPMN规范的建模对象。  4.在管理工具中的权限管理方面遵循RBAC规范，在与组织机构接口方面支持LDAP规范。 |
| ★65 | ★ | 系统接口要求 | 支持XML和Web Service技术，实现与第三方系统之间的数据交换与集成。 |
| ★66 | ★ | 可用性要求 | 支持7\*24小时不间断运转，可用性达到99.99%。 |
| 325 |  | 子流程 | 1.支持启动一个、多个子流程；  2.支持子流程与主流程同步、异步流转；  3.支持主子流程之间的数据相互传递。 |
| 326 |  | 操作权限要求 | 可以按照主办、协办、读者、创建者、管理者不同身份，给用户指定不同的操作权限。 |
| 327 |  | 表单访问权限要求 | 可以按照主办、协办、读者、创建者、管理者不同身份，给用户指定不同的表单访问权限。 |
| 328 |  | 字段访问权限控制要求 | 可以按照主办、协办、读者、创建者、管理者不同身份，给用户指定针对每个表单中不同字段的访问权限。 |
| 329 |  | 流程定义接口 | 1.提供流程建模定制接口。  2.支持主流工作流建模导入。  3.支持流程导出为BPML规范描述。  4.提供图形化流程定制工具，同时提供流程建模和定义API供第三方程直接创建流程 |
| 330 |  | 流程任务接口 | 1.提供流程引擎工作列表调用接口。  2.显示待办、草稿、撤办、代理办理等数据列表。  3.提供用户有权访问的所有流程启动入口。 |
| 331 |  | 工单分配 | 工单可自动分配或手动分配。告警可触发工单，并实现告警工单的自动分配或手动领取。 |
| 332 |  | 工单分级 | 工单可以关联SLA级别，定义每个级别的工单完成时间。 |

**A01-32 全文检索**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 333 |  | 功能要求 | 提供搜索功能，系统管理人员可以根据网站数据更新情况配置触发器的最短更新周期，达到实时搜索效果。即网站只要发布了最新文章，通过实时触发机制，第一时间（如5分钟内）将网站数据导入到检索系统中，确保搜索结果与网站内容更新保持一致。 |
| 334 |  | 支持拼音联想、关键词联想、智能纠错等人性化引导用户搜索的功能； |
| 335 |  | 支持有按需加权、智能排序的功能，管理员可根据当前业务重点或关注热点进行设置，在搜索结果页面中优先呈现重要的服务信息，提高网站的服务效果。 |
| 336 |  | 支持信息自动聚合功能； |
| 337 |  | 支持快速服务功能，可以实现在搜索页直接展示热门服务与功能，网络用户无需点击搜索结果链接跳转查看，直接在搜索结果页面即可完成所有操作，给用户提供更佳的用户访问体验。 |
| 338 |  | 支持全文检索功能，对网站信息进行标题、关键词、正文内容、附件内容等进行全文检索，并实现对学校所在地等信息进行动态查询。 |
| 339 |  | 支持分类检索、自定义推荐链接、自定义词库管理、搜索系统自优化功能。 |

**A01-33 等级保护测评服务**

按照采购人要求完成咨询工作，按照采购人要求在一年内协助完成等级保护定级、备案、整改、测评等工作，测评费用由中标人承担，包含在投标报价中。

等级保护测评服务内容包括：针对等保对应级别要求的自评估、自评估所发现问题的加固与整改、等保测评的实施及现场配合；

中标人应承诺协助采购人指定的系统通过等级保护测评机构的测评；

等级保护测评服务的提交物包括：《XX系统等级保护自评估报告》、《XX系统等级保护加固与整改计划》、《XX系统等级保护加固与整改报告》、《XX系统等级保护测评报告》等。

**A01-34 展现门户建设**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 340 |  | 技术路线要求 | 遵循J2EE多层框架设计，利用统一门户技术，集成性、扩展性强 |
| 341 |  | 门户需求 | 需要根据中央党校业务实际情况与需求，设计不同用户的展现门户 |
| 342 |  | 总体设计要求 | 打造中央党校统一门户系统，作为面向全体不同用户的门户网站建设统一的集成平台，同时，支持与移动应用平台的协同互动。 |
| 343 |  | 门户展现要求 | 包括网站风格设计、界面布局设计、内容结构设计、网站SEO和栏目规划等方面进行系统设计与建设 |
| 344 |  | 门户构建平台要求 | 主要包括统一视图、个性化定制、应用整合、业务协同、安全控制等功能 |

**A01-35 网络学习平台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 345 |  | 技术路线要求 | 遵循J2EE多层框架设计，集成性、扩展性强 |
| 346 |  | 需求 | 需要根据中央党校业务实际情况与需求，设计符合用户需求的网络学习平台 |
| 347 |  | 总体设计要求 | 通过中央党校网络学习平台为全国的党员领导干部提供网络学习园地，通过网络学习平台，能够使学员根据各自业务领域学习相关课程，系统会根据学习情况进行教学资源推荐及学习记录跟踪管理，并能够按班次或学员统计学习兴趣倾向为教师为学员提供个性化支持服务。 |
| 348 |  | 功能设计 | 支持网络培训功能，覆盖中央党校日常培训业务领域。 |
| 349 |  | 支持课堂直播功能，覆盖远程教学、直播课堂等多种形式的教学方式。 |
| #37 | # | 直播活动 | 直播活动垫片，支持校内活动直播应急垫片功能，支持断流自动播放垫片，支持手动切换垫片播放；直播课程监控，不依赖客户端插件，以B/S结构H5的方式，在浏览器上支持多路直播课程流实时监控可对黑场、断流、白屏、蓝屏等IP流故障报警；视频课程快编，支持对视频课程文件进行分段，支持视频场景分析，可注识视频的的转场镜头时间点并以当前帧的缩略图显示，支持视音频分离，可在时间轴上显示音频的波形，支持掐头、去尾、删除功能，支帧精确分段物理文件。  需要针对课程直播垫片、直播课程监控、课程视频快编进行产品演示。 |
| #38 | # | 课程安全保护 | 点播课程防录屏，支持节目内容保护在播放视频时，可以在视频上以浮层的方式显示登录用户名访止截屏录制；点播课程防盗链，支持防盗链即使获取到视频课程地址也不能下载视频内容。课程加密保护，支持课程切片加密，在非法下载到视频切片也不能进行线下播放。  需要针对课程防录屏、课程防盗链、课程加密进行产品演示。 |
| #39 | # | 点直播课程流服务 | 点直播课程流服务，提供国产化流服务软件需具备自主知识产权采用C++开发，支持中文操作界面，可创建多个点、直播课程播出发布点，支持UDP、RTMP、HTTP多种视频课程传输协议输入播出（推流、拉流），支持点播课程实时生成预览视频片段，根据播放器的HTTP截图，实时生成片段视频给请求方。  需要针对中文操作界面，个点、直播播出发布点状态监看；支持UDP、RTMP、HTTP多种视频传输协议输入播出（推流、拉流）；点播实时生成预览视频片段，根据播放器的HTTP请求，实时生成片段视频给请求方进行产品演示。 |

**A01-36 移动应用平台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 350 |  | 扩展性要求 | 集成性、扩展性强 |
| 351 |  | 需求 | 需要根据中央党校业务实际情况与需求，利用先进技术，开发移动端应用 |
| 352 |  | 总体设计要求 | 基于党校原有的硬件支撑环境与软件现状为基础，结合党校业务需求，设计移动端应用平台，应充分考虑集成性、实用性、界面友好性等 |
| 353 |  | 功能要求 | 支持信息查询、信息发布等功能 |
| #40 | # | 设备管理安全性要求 | 配置登录是否校验、是否自动绑定、绑定是否审批、绑定设备数、解绑校验、设备的拉黑、挂失、白名单处理等；移动端提交自定义设置、管理员可以定义特定用户的设置、停用、删除、查看用户的自定义设置等功能。可以根据用户姓名模糊过滤查询设置信息。  此功能需要产品演示。 |
| #41 | # | 架构部署要求 | 支持多单位多层级架构。统一部署一套平台，满足分处多个层级的总部以及下属部门同时使用的要求。在使用过程中，总部以及每个部门所使用的移动门户显示风格、系统功能、通讯录、即时通讯等均不相同，形成个性化的移动工作门户集合。支持在云端部署，支持多租户应用，支持租户数量动态扩展。  此功能需要产品演示。 |
| #42 | # | 多门户设计要求 | 用户手机端只装一个APP，根据用户身份、权限不同，动态切换不同的门户，每一个门户的展现功能和操作均不相同。具体到本项目，系统内角色可以区分为领导及工作人员等不同角色，有的用户同时属于几种角色，为方便用户，需要实现在用户不退出系统的前提下，灵活切换领导门户及员工门户，查看不同的界面及数据，使用不同的功能（包括通讯录在内）。\*\*基于门户提供可视化设计工具，门户各区域（首页、菜单、导航栏等）都能以所见即所得方式进行拖拉式发布；  提供磁贴风格的首页自定义配置功能，可以根据需要随时上传更换磁贴图片；  提供首页横幅图片的配置，可以配置需要显示的图片数量，上传或更换横幅图片，配置横幅图片点击行为；  在管理平台完成设计或配置后，一键发布，移动端无需升级就能实时显示门户新设计的结果、使用门户最新发布的应用。  此功能需要产品演示。 |
| #43 | # | 快速实现业务移动化 | 平台作为移动信息化基础支撑架构，要求快速实现业务在移动端上的横向扩展。在已经实现移动端与PC端接口的情况下，对于原有流程调整，能够同步在手机端进行展现；对于新建流程，能够在5分钟以内实现移动手机的业务办理。  管理员可以灵活配置某些流程或流程节点在手机上不能够办理，手机显示对应的提示信息。  此功能需要产品演示。 |
| #44 | # | 多样化手写签批 | 产品原生支持移动签批功能，支持用户在移动端原生表单以及HTML5表单中实现手写签批，支持放大、缩小签批，支持签批定位，支持正文签批，支持用户在移动端OFD版式文件中手写签批。  此功能需要产品演示。 |
| #45 | # | 产品资质 | 具备在本项目招标公告发布时间前，由国家版权局颁发的移动应用开发平台类著作权、由信息化管理部门颁发的移动RSS聚合平台类软件产品登记证书，提供相关证明材料。 |

**A01-37 云应用支撑平台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 354 |  | 统一用户管理 | 支持组织分层和配置管理，支持群组自定义配置 |
| 355 |  | 提供身份认证功能，支持单点登录、统一认证等 | 提供身份认证功能 |
| 支持单点登录 |
| 356 |  | 提供统一的应用开发框架，支持前端和后端的开发 | 支持x86平台的应用开发框架，同时支持国产化平台 |
| 357 |  | 提供日志等审计类服务组件 | 支持日志输出、日志查看、导出、统计等功能的服务组件 |
| 358 |  | 提供统一消息处理服务组件 | 提供对消息处理构件，满足公共消息处理能力，实现远程消息服务 |
| 359 |  | 提供统一外部适配接口服务 | 提供通过webservice等数据接口实现和集成平台、外围系统的对接服务 |
| 360 |  | 提供微服务资源池服务 | 对业务系统中的应用服务进行提炼，形成微服务并进行发布，统一融入到微服务资源池，为各应用系统提供所需的业务支撑公共服务，从而整体提升应用支撑平台的业务支撑能力 |

**A01-38 信息资源目录服务**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 361 |  | 技术路线要求 | 遵循J2EE多层框架设计，集成性、扩展性强 |
| 362 |  | 需求理解要求 | 需要根据中央党校业务实际情况与需求，分析业务问题，进行产品定位 |
| 363 |  | 总体设计要求 | 结合党校的数据化现状与未来的业务需求，设计详细合理的信息资源目录规划与数据资源架构 |
| #46 | # | 功能指标 | 实现资源目录管理功能，具有信息资源数据元、代码集的管理能力，支持逐级审核和发布功能；实现业务关联功能，具有业务事项与承载系统的一对一关联匹配功能，支持图形化展现业务关联结果的功能，具有将一个事项的多个材料分别与特定信息类的关联匹配功能，且自动计算匹配程度；共享需求管理支持面向主题的资源申请，针对事项，提出一个或多个信息类（项）需求，形成需求清单；在需求开发全流程中，必要环节要求支持“退回”操作，达到业务与规则要求，具备需求概览功能，直观展示当前需求的开发进展情况，及具体需求项所处环节。此处需要针对功能指标进行产品演示。 |
| #47 | # | 产品资质 | 具备在本项目招标公告发布时间前，由国家版权局颁发的政务信息资源目录系统类著作权，提供相关证明材料。 |

**A01-39 安全邮件系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 364 |  | 外网电子邮件（含反垃圾模块）系统（4000用户） | 基本要求：  邮件系统需要具备体系化的安全设计，能够实现从用户登录、收信、发信、存储到归档的全生命周期的安全防护；  邮件系统需要对邮件协议有广泛的支持，包括但不限于IMAP、POP3、SMTP、MIME协议等，且需要支持SSL加密传输；  邮件系统需满足1000用户同时在线并发收发邮件时，系统无明显延迟；以个人用户2万封信件为基准，用户查询特定信件时间不大于500ms。 |
| ★67 | ★ | 数据存储：  邮件数据应采用安全性和性能更佳的块文件存储，且对存储的数据进行加密。不应采用一个用户一个目录或文件的存储方式；  邮件数据应采用单副本技术存储，即针对同一封邮件应只保留一份存储数据，以节省存储空间。 |
| 365 |  | 易用性：  系统应支持Webmail，有良好的人性化交互操作，界面可以根据要求定制；  系统需与主流的邮件客户端程序有良好的兼容性，支持Outlook, Foxmail等常用邮件客户端。 |
| 366 |  | Webmail：  支持邮件接收、发送、回复，且支持包含原附件的全部回复；  用户可以直观的查询邮件的收发踪迹；支持域内邮件撤回功能；发送失败的邮件要有详细的退信；  具备邮件摘要能力，即邮件前段正文能够在列邮件时显示；  要求能够支持多标签页,比如可以写信同时打开邮件夹、阅读邮件，操作地址簿等，可通过页标签快速切换；  要求具备多标签的状态自动恢复能力，即用户正常或异常退出后重新登录时能够恢复上次打开的内容，保障工作连续性；  支持2GB以上的大附件文件上传和发送。为保障良好的兼容性，附件上传不允许使用浏览器插件；  要求支持附件批量上传和断点续传，即一次选中多个附件文件上传，且网络中断重新上传时可自动接续；  别名登录：为保证用户的登录安全，系统需要支持邮箱别名登陆功能（区别于别名邮箱账号），别名可设置为中文或者英文，当存在别名时必须使用别名登陆  要求支持鼠标拖拽，用户可方便的将邮件拖拽到相应邮件夹中；  要求支持邮件备注，用户对邮件添加备注信息，且备注信息可被检索；  要求支持邮件标色，用户可对邮件标记不同颜色，便于对邮件的管理；  要求支持用户自建文件夹，且支持来信分类策略，可将满足特定特征的邮件分拣到不同邮件文件夹中 |
| 367 |  | 系统管理功能：  应有全中文的管理界面，良好的人性化交互操作；  系统需要支持用户组织管理和邮件域管理，实现系统的分级管理，分公司可管理自己辖区内的邮箱；  管理员可以建立服务等级，全局和个别配置邮箱存储大小、邮件收发大小的功能；  系统应提供审计员角色，具备对用户及管理员操作行为日志记录和安全审计回溯功能；  对管理员帐号，可实现绑定IP登陆设置。 |
| 368 |  | 安全性：  邮件系统应采用沙箱技术架构，确保系统访问入口的唯一性，保护系统对攻击最大程度的安全防护；  WebMail前端JS一次载入，不可多次、动态载入，以保障JS前端的安全性，前后端会话仅传递必须的变化内容，不可按帧传递以防劫夺；  系统应通过使用随机图片验证码或随机问题等类似方法防止密码暴力破解。应具有登录失败处理功能，可采取结束回话、限制非法登录次数和当网络登录连接超时自动退出等措施；  系统应对HTTP、SMTP、IMAP、POP3、HTTPS登陆错误次数均作限制，比如：增验证码机制，几次输入密码错误限制IP等；  支持邮件备份，数据库备份，邮件恢复最小颗粒为单封邮件，邮件恢复功能要有良好的查询定位邮件的功能。 |
| #48 | # | 反垃圾防病毒：  具有反垃圾邮件引擎，内嵌到邮件系统各个模块中，非网关形式应用，使用和邮件系统统一管理界面。  要求具有垃圾邮件智能识别和学习功能，识别垃圾邮件，智能计算，无须各级管理员干预。  防病毒系统需采用双重或三重杀毒引擎，提高病毒识别力；并要求病毒防护成本与并发用户数、用户数、域数量无关，病毒库更新成本与并发用户数、用户数、与数量无关。  需支持SMTP、HTTP、POP3、IMAP4、SMTPS、HTTPS、POP3S、IMAP4S全协议的防病毒能力。 |
| 369 |  | 实施要求：  投标方在系统实施前，需要依据招标人情况，制订并提交详细的实施和迁移方案。 |
| 370 |  | 外邮件归档系统（4000用户） | 基础技术要求：  为保障未来扩展升级便利，产品必须为纯软件形态，不接受软硬一体的产品形态。  为保障安全和高效，产品须运行在Linux操作系统。  产品须采用B/S架构。  支持双机HA部署架构，且具备向高端集群架构的平滑升级能力。 |
| 371 |  | 即时归档：要求实现即时归档功能，能够在收发邮件的同时完成到归档系统的邮件归档操作。 |
| 372 |  | 单副本：要求使用或支持附件单副本存储技术，支持邮件附件级单副本存储，即相同附件文件只保留一份。 |
| 373 |  | 数据存储：要求支持数据固化技术，归档的内容在服务器端不允许删除、改写，用户也不能删除、改写。 |
| 374 |  | 安全性：  邮件数据应采用安全性和性能更佳的块文件存储，且对存储的数据进行加密。  为保障产品安全性、易用性和使用性能，产品应采用Web 2.0架构，其AJAX引擎必须为自主技术，不允许使用开源AJAX引擎。  归档系统需具有安全的访问权限控制。  登录账号密码要求与邮件服务器统一验证。  要求支持支持多种认证方式，如数据库认证、LDAP认证、第三方认证机制。 |
| 375 |  | 归档功能：  要求能够归档所有传入、传出以及内部的电子邮件。  能够根据归档策略实现对所有用户邮箱的自动归档，也同时支持选择性归档。  电子邮件归档系统应不限用户归档存储空间。  能够提供对历史邮件统一归档的功能，保证对所有历史数据进行归档。  提供用户级归档邮件访问入口，允许/限制用户访问自己的归档电子邮件。 |
| 376 |  | 信息检索：  提供高效的搜索引擎，保证快速检索。  支持对邮件正文及附件的全文检索功能。  支持对压缩附件的直接检索功能。  提供智能化的模糊查询和精确查询功能，保证快速高效的调取归档数据。  要求提供对整体邮件搜索和对特定用户邮件搜索两种模式。  检索速度，在标准服务器下（4核CPU、16GB内存），百万封归档邮件中检索任意一封邮件。检索时间不超过1秒。检索的附件格式支持不限于doc、txt、html、pdf、zip、rar等格式。  能够将从归档系统中检索出来的邮件恢复、下载和转发等功能。 |
| 377 |  | 管理功能：  多角色分级用户管理，有普通用户、审计与管理员账号等多种角色。  具有审计功能，用户或管理员登录时记录登录痕迹。  所有管理操作均记录完整的日志。  具备日志固化技术，保障日志不被删除。  提供多种系统日志功能，能监控系统的运行状态。 |
| 378 |  | 扩展能力：  支持SNMP/API扩展。  应具有无限存储空间扩展能力，可以加入新的存储空间，扩容后应可自动使用新的存储空间，并对所有存储进行搜索查看邮件。  要求邮件归档系统支持分布式集群架构，可同时将邮件归档系统部署在多台物理机器上。 |
| #49 | # | 边界内容审计系统  （4000用户） | 关键字过滤：支持对外发邮件进行关键字检测和过滤，支持组合关键词、正则表达式、字典。 |
| 策略设置：支持中心统一策略和分支补充策略的两级策略设置。可设置附件检查策略。 |
| 文件检测：  附件内容检查可自动识别格式，支持嵌套附件内容检查。  支持压缩和多次压缩的附件内容检查。  可禁止外发加密或不能识别的附件。  识别文件MD5，进行特定扫描和例外。 |
| 379 |  | 处理动作：  扫描后自动隔离或放行。  可审批后放行，并提示相关用户。具备通知信功能，可在通知信中展现审批员的审批意见。 |
| 审计和检索：  支持对历史邮件及附件数据的合规性检查。  提供高效的邮件归档搜索引擎，可实现对归档邮件的邮件头及附件全文搜索。 |
| #50 | # | 产品要求 | 具备公安部计算机信息系统安全专用产品销售许可证（增强级） |

**A01-40 标准规范编制**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
| 380 |  | 标准规范编制要求 | 从技术、管理等角度，充分考虑标准规范的体系性、指导性，支撑中央党校整体的信息化建设。 包括但不限于：  1）中央党校（国家行政学院）信息化总体技术标准  2）云管理规范  3）信息资源标准  4）数据交换标准  5）应用支撑技术标准  6）工程管理规范 |

1. **方案设计及项目实施要求**

投标人应在投标文件中提出满足项目需求的项目详细实施方案。方案内容包括但不限于投标人对整个工程的：

**1、方案设计**

投标人在充分理解采购人现状基础上，结合采购人具体需求，提供设计方案，包括但不限于：

1. 信息化基础设施改造建设方案；
2. 应用系统设计方案：针对软件定制开发部分，提供业务需求分析、设计方案等；
3. 安全服务方案；
4. 标准规范体系设计方案。

**2、项目实施的组织结构保障**

投标人必须有详细项目管理组织架构、参与本项目实施的职员姓名、职务、职责，主要资历、经验及承担过的项目，具有三年以上类似项目经验（提供人员简历、相应的资质和证明文件）。

**3、施工组织方案**

方案主要内容要求（但不限于下列要求）：

1）项目实施进度计划

对项目实施的各个阶段：工程设计阶段、设备订货阶段、工程实施准备阶段、系统建设阶段（包括软件开发、系统安装调试、设备开箱验货、设备安装调试、设备安装、加电测试、设备调试配置、系统调试等）、系统验收阶段的进度做出详细的计划；

2）项目组人员安排

3）项目质量保障措施

4）项目进度保障措施

1. **培训要求**

培训内容周详、合理、培训范围广、有合理的培训计划、二次培训计划和持续培训计划安排，可实施，有针对性，包括但不限于应用系统使用培训及相关产品培训。

1. 应用系统使用培训：培训课程安排、培训内容、培训达到预期结果；

2、相关产品培训，说明课程安排、培训内容、培训达到预期结果；

3、所有培训必须有3-5名培训学员熟练掌握所培训内容；

4、培训地点按采购人指定地点。

1. **售后服务要求**
2. **硬件产品安装及技术支持**

中标人提供软硬件的配置安装及集成工作，产品原厂商提供设备安装的技术支持。中标人提供详细的安装规划文档包括系统补丁列表、系统参数调整列表、安装软件组件列表、以及系统环境变量列表。

从竣工验收开始3年内，针对硬件使用过程中出现的技术问题，需要提供7\*24小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对软件的调节/优化提供建议，提供4小时带备件现场保修。

1. **软件产品安装及技术支持**

在软件安装部署完毕后，需要对软件的安全性和稳定性进行测试，包括软件可调节参数修改。

从竣工验收开始3年内，投标方针对软件运行过程中出现的技术问题，需要提供7\*24小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对软件的调节/优化提供建议。

**相关资质要求：**

投标人具有中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类二级及以上）、中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书（信息系统安全集成服务资质二级及以上）、中国网络安全审查技术与认证中心颁发的信息系统灾难备份与恢复服务资质-灾难备份与恢复（B类）。

项目经理具有中国电子信息行业联合会颁发的高级项目经理证书、人社部门颁发的信息系统项目管理师证书、工信部电子工业标准化研究院颁发的ITAIP（信息技术应用创新专业人员）证书。

技术负责人具有中国电子技术标准化研究院颁发的ITSS认证工程师证书、人社部门或工信部教育考试中心颁发的高级系统分析师证书。

系统分析师具有人社部门或工信部教育考试中心颁发的系统分析师证书、工信部教育考试中心颁发的高级软件工程师证书、工信部教育考试中心颁发的高级数据库管理工程师证书。

本项目团队总人数要求不少于15人。并且除项目经理、技术负责人外，项目团队成员具有以下证书：国产厂商认证的网络工程师证书、工信部教育考试中心颁发的软件测试工程师证书、工信部电子工业标准化研究院颁发的ITAIP（信息技术应用创新专业人员）证书、中国信息安全测评中心频发的CISP认证证书。

**讲标与演示要求：**

**每家投标人讲标与演示时间应控制在10分钟以内。**

1. **整体设计方案：**项目整体设计方案应描述清晰准确、满足本项目实施要求。
2. **网络割接方案：**网络割接设计方案应描述清晰准确、满足本项目实施要求。
3. **项目重难点分析：**对本项目实施的重难点进行分析。
4. **产品演示：**产品演示应把重点功能描述清晰准确、满足本项目实施要求。

产品演示包含如下产品功能：

1. **移动应用平台**

* **设备管理安全性要求：**配置登录是否校验、是否自动绑定、绑定是否审批、绑定设备数、解绑校验、设备的拉黑、挂失、白名单处理等；移动端提交自定义设置、管理员可以定义特定用户的设置、停用、删除、查看用户的自定义设置等功能。可以根据用户姓名模糊过滤查询设置信息。
* **架构部署要求：**支持多单位多层级架构。统一部署一套平台，满足分处多个层级的总部以及下属部门同时使用的要求。在使用过程中，总部以及每个部门所使用的移动门户显示风格、系统功能、通讯录、即时通讯等均不相同，形成个性化的移动工作门户集合。支持在云端部署，支持多租户应用，支持租户数量动态扩展。
* **多门户设计要求：**用户手机端只装一个APP，根据用户身份、权限不同，动态切换不同的门户，每一个门户的展现功能和操作均不相同。具体到本项目，系统内角色可以区分为领导及工作人员等不同角色，有的用户同时属于几种角色，为方便用户，需要实现在用户不退出系统的前提下，灵活切换领导门户及员工门户，查看不同的界面及数据，使用不同的功能（包括通讯录在内）。基于门户提供可视化设计工具，门户各区域（首页、菜单、导航栏等）都能以所见即所得方式进行拖拉式发布；

提供磁贴风格的首页自定义配置功能，可以根据需要随时上传更换磁贴图片；

提供首页横幅图片的配置，可以配置需要显示的图片数量，上传或更换横幅图片，配置横幅图片点击行为；

在管理平台完成设计或配置后，一键发布，移动端无需升级就能实时显示门户新设计的结果、使用门户最新发布的应用。

* **快速实现业务移动化：**平台作为移动信息化基础支撑架构，要求快速实现业务在移动端上的横向扩展。在已经实现移动端与PC端接口的情况下，对于原有流程调整，能够同步在手机端进行展现；对于新建流程，能够在5分钟以内实现移动手机的业务办理。

管理员可以灵活配置某些流程或流程节点在手机上不能够办理，手机显示对应的提示信息。

* **多样化手写签批：**产品原生支持移动签批功能，支持用户在移动端原生表单以及HTML5表单中实现手写签批，支持放大、缩小签批，支持签批定位，支持正文签批，支持用户在移动端OFD版式文件中手写签批。

1. **数据交换**

* **协议适配能力：**支持多种通讯协议和外部系统应用系统进行交互，如File、JDBC、JMS、HTTP/s、SOAP、REST等，通过流程编排，轻松实现任意两者之间的协议转换功能。

应包含多种适配器，如支持结构化和非结构化文件读写的文件类适配器、能根据文件名的特点将文件夹下的文件分成不同的类，每类文件调用不同的文件处理服务；支持异步传输协议的JMS适配器、HTTP/s适配器、Web服务适配器等，通过现成的适配器，减少程序员开发工作量，实现快速应用集成能力。

应具备数据库处理组件，支持和主流关系型数据库如Oracle、SQLServer、DB2、Sybase，开源数据库MySQL、国内数据库金仓、达梦等进行交互。支持和主流非关系型数据库如Hive、HBase、MongoDB等进行交互。所有适配过程均需通过可视化界面进行配置。

完善的数据加工能力：支持数据库、文件、XML、JSON、NoSQL(Hive、MongoDB)、Web服务、JSM等之间的转换加工处理。支持基于时间戳、标志位回写、数据库日志CDC的增量加工处理。

支持多种转换加工方法，能通过web界面可视化配置包括不限于字符串转换、时间类转换、数据比对与翻译、数学运算、身份证格式转换等转换方法。

支持多种逻辑处理方法，能通过web界面可视化配置包括不限于：格式匹配检查、字符串逻辑检查、空检查、重复记录检查、范围内检查、逻辑检查、复合逻辑检查、自定义逻辑检查等。

支持加工过程中的数据质量检查，根据数据逻辑判断规则，将干净的数据装载到目标中，将判断有问题的数据路由到数据库表或者数据文件中。

支持数据脱敏处理，支持在保留数据原始特征的条件下，对某些敏感信息通过脱敏规则进行数据的混洗、值变换、加密、遮挡、空值插入等处理，实现敏感数据及个人隐私的可靠保护。

所有配置过程均需通过可视化界面进行配置。

* **数据传输与多样调度能力：**提供数据传输功能。支持将数据、文件、文件夹下的文件传输到目标中。支持变化文件传输，支持按条件选择文件传输，支持加密、压缩等处理，可以设定规则对文档归档或者清理。

支持在一个可视化配置界面内实现跨网段的两个交换节点之间的交换，交换的数据源和目标可以是文件、数据库、接口。为了安全考虑被交换的数据库通讯端口不对外开放，只能通过交换节点获得表的结构信息，要求通过简单配置能实现数据库表之间的相互交换。

为了安全的考虑，支持基于中心节点中转（可以不在中心保存数据）的数据交换能力，两个交换节点分别对应两个部门（或系统），中转节点对应中心，两个节点通过中心中转交换（不在中心保存数据）。要求经过简单可视化配置实现两个交换节点通过中转节点交换数据，交换的数据源和目标可以是文件、数据库、接口。该交换服务支持长连接情况下的大数据量交换，保证事务的完整性。

为了安全的考虑，要求支持单向连接通讯方式，如中心和前置节点交换重要数据时，只允许中心单向连接前置节点，不允许前置节点连向中心，只能由中心节点通过推、拉方式交换文件和数据库的数据。要求提供数据库表之间交换的服务配置界面，拉方式交换等。

所有配置过程均需通过可视化界面进行配置。

支持基于菜单的交互调度、定时调度。要求提供可视化界面。支持文件分类调度。能根据文件名的特点将文件夹下的文件分成不同的类，每类文件调用不同的文件处理服务；要求提供可视化界面。支持流程调度功能。支持平行处理、顺序执行、条件处理、意外处理；可根据CPU、I/O、网络等情况调整并行处理的并发数。当流程运行出意外时，可选择补偿运行、断点续运行、间隔检查运行等处理方式。要求提供可视化界面。

* **数据共享支持能力：**提供数据共享功能，基于web能可视化配置出数据交换共享服务，包括数据查询服务、订阅比对服务、数据操作服务。提供服务目录管理，支持服务的发布、变更等管理。提供服务流程管理，包括服务的申请、审核/审批等。

可视化配置出交换共享服务的转换加工、逻辑处理、交换过程中的数据质量检查等功能。

可视化配置出数据交换共享服务的数据安全脱敏功能，支持加密、遮挡、混淆、值替换等脱敏处理方法。

提供服务的安全授权功能，授权用户允许访问的服务，支持白名单、IP约束等功能。

提供访问控制，只有通过身份验证、访问控制的用户才能访问，对于不允许的IP，拒绝访问。

提供服务运行池管理，能设置允许并发访问数。

1. **信息资源目录服务**

* 实现资源目录管理功能，具有信息资源数据元、代码集的管理能力，支持逐级审核和发布功能；
* 实现业务关联功能，具有业务事项与承载系统的一对一关联匹配功能，支持图形化展现业务关联结果的功能，具有将一个事项的多个材料分别与特定信息类的关联匹配功能，且自动计算匹配程度；
* 共享需求管理支持面向主题的资源申请，针对事项，提出一个或多个信息类（项）需求，形成需求清单；在需求开发全流程中，必要环节要求支持“退回”操作，达到业务与规则要求，具备需求概览功能，直观展示当前需求的开发进展情况，及具体需求项所处环节。

1. **网络学习平台**

* **直播活动：**直播活动垫片，支持校内活动直播应急垫片功能，支持断流自动播放垫片，支持手动切换垫片播放；直播课程监控，不依赖客户端插件，以B/S结构H5的方式，在浏览器上支持多路直播课程流实时监控可对黑场、断流、白屏、蓝屏等IP流故障报警；视频课程快编，支持对视频课程文件进行分段，支持视频场景分析，可注识视频的的转场镜头时间点并以当前帧的缩略图显示，支持视音频分离，可在时间轴上显示音频的波形，支持掐头、去尾、删除功能，支帧精确分段物理文件。

需要针对课程直播垫片、直播课程监控、课程视频快编进行产品演示。

* **课程安全保护：**点播课程防录屏，支持节目内容保护在播放视频时，可以在视频上以浮层的方式显示登录用户名访止截屏录制；点播课程防盗链，支持防盗链即使获取到视频课程地址也不能下载视频内容。课程加密保护，支持课程切片加密，在非法下载到视频切片也不能进行线下播放。需要针对课程防录屏、课程防盗链、课程加密进行产品演示。
* **点直播课程流服务：**点直播课程流服务，提供国产化流服务软件需具备自主知识产权采用C++开发，支持中文操作界面，可创建多个点、直播课程播出发布点，支持UDP、RTMP、HTTP多种视频课程传输协议输入播出（推流、拉流），支持点播课程实时生成预览视频片段，根据播放器的HTTP截图，实时生成片段视频给请求方。

需要针对中文操作界面，个点、直播播出发布点状态监看；支持UDP、RTMP、HTTP多种视频传输协议输入播出（推流、拉流）；点播实时生成预览视频片段，根据播放器的HTTP请求，实时生成片段视频给请求方进行产品演示。