滁州市机电工程学校数据中心及安全等保项目

拟采购产品规格型号和参数清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 规格型号 | 数量 | 单位 | 备注 |
| 1 | 超融合资源池 | （一）计算存储融合节点要求： 本次配置计算存储融合节点≥6个,每节点要求如下： 1、处理器不低于2.2GHZ，24核，数量≥2； 2、内存配置容量≥256GB； 3、配置≥12块4TB SATA硬盘，≥2 块 600GB 10K SAS 硬盘，≥1块NVMe 3200G SSD； 4、配置RAID卡，2G缓存，支持 RAID 0、1、5，配置超级电容； 5、网卡≥4\*10GE光口（满配光模块），≥2\*GE电口。 （二）超融合系统软件要求： 本次配置1套满足此次项目需求的计算虚拟化软件、分布式存储软件、超融合管理软件的授权；包含云平台管理软件、管理平台主备机制软件，数据中心管理平台软件，含三年专享升级服务； 1、虚拟化软件、分布式存储软件、超融合管理软件必须具有国产软件自主知识产权，具有自主研发能力，保障后续产品的连续性。 2、在同一个管理界面中监控和管理计算、存储、交换机、虚拟化平台等。 3、分布式存储软件构筑在x86/ARM标准硬件之上，非开源软件开发，如不能使用开源Lustre和Ceph软件等，通过软件层面的去中心化架构和数据冗余技术，来达到高可伸缩性和高可用性； 4、实现管理节点的管理数据定期自动备份到远端FTP服务，以便出现重大事故导致管理数据丢失时，可以利用备份的数据进行恢复。 5、实现在图形界面上一键式完成存储、计算、网络的扩容，对于扩容节点自动完成操作系统和虚拟化平台软件安装与初始配置。 6、在全SSD配置及SSD+HDD混合配置下，实现EC（Erasure Code）算法实现数据冗余存储的功能， 4+2冗余配置；本次配置EC（Erasure Code）算法实现数据冗余存储； 7、实现虚拟机资源调整功能，根据实际需要修改虚拟机的属性，包括vCPU个数、内存大小、硬盘数量和网卡个数。 8、实现创建精简配置卷的功能，系统应该根据精简配置卷的实际使用情况动态分配空间，提供存储资源利用率。  9、实现SSD磨损寿命识别的功能，提前告警及隔离处理；  10、实现全局自适应重删压缩的功能，可根据业务负载自动在在线重删和后重删之间进行切换，压缩比达3:1；  11、本次配置可用容量不低于145TB。 | 1 | 套 |  |
| 2 | 数据中心万兆交换机 | 1、交换容量≥40T，包转发率≥1000Mpps； 2、固定端口10GE SFP+≥48,40/100GE QSFP28≥6；配置20个万兆光模块。 3、可插拔电源模块≥2、独立风扇模块≥4； 4、实现RIP、RIPng、OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+等动态路由协议； 5、实现BFD for OSPF，BGP，IS-IS，Static Route的功能； 6、实现IGMP、PIM-SSM、IGMP Snooping、IGMP Proxy、MBGP等组播路由协议的功能； 7、实现缓存的微突发检测功能； 8、实现Netstream、sFlow、Telemetry、ERSPAN流量分析技术； | 2 | 台 |  |
| 3 | 迁移服务 | 我校一卡通、教务处教学诊改平台、总务处资产管理、教务处青果等现有业务系统迁移至本次项目建设的超融合资源池中。 | 1 | 套 |  |
| 4 | 数据中心接入防火墙 | 1、标准机架式1U设备； 2、吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万，IPSec吞吐量≥20Gbps； 3、设备实现前后风道，支持风扇、电源冗余、可热插拔； 4、能够基于IP、IPv6、MAC地址、时间进行访问控制策略控制;实现自定义安全策略，安全策略组功能；实现策略冗余/命中分析； 5、实现静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 6、实现基于地理位置的流量和威胁分析；每IP，每用户的最大连接数限制； 7、要求防火墙具备AI引擎，用于DGA域名请求检测、用于恶意C&C流量检测、用于ECA恶意加密流量识别； 8、本次配置要求：千兆电口≥12，千兆光口≥8，万兆光口≥4，实配三年威胁防护服务（含IPS/AV/URL/云沙箱授权），SSL VPN并发数实配100，配置2个电源； | 2 | 台 |  |
| 5 | 备份一体机 | 1、2U机架式，配备64位Intel八核处理器、32GB高速缓存、千兆网口≥2、万兆口≥2；提供RAID0,1,10,5,50,6,60等多种RAID级别，并具备热备盘；提供Raid掉电保护，防止突然断电造成RAID系统数据及缓存数据丢失，掉电保护时间需≥72小时，并支持全局热备盘；本次配置≥12块6TB企业级SATA硬盘； 2、要求设备系统和软件安装在2块（RAID 1）≥240GB企业级SSD磁盘上，不允许占用前面板的槽位。 3、实现Windows文件系统的卷级备份功能，以整卷为单位进行数据备份，提升海量小文件环境下的备份效率。实现整卷恢复和单文件目录级别的细粒度恢复； 4、实现对VMware vSphere、XenServer、H3C CAS、华为Fusionsphere等主流虚拟化应用的备份，实现单机和集群部署环境。以上虚拟化应用均实现以虚拟机、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；  5、Oracle数据库备份支持自定义脚本，实现RMAN备份参数的图形化配置；  6、实现虚拟机并发备份和恢复功能，实现在WEB页面中设置单个备份和恢复任务中的虚拟机并发备份和恢复数量，可设置≥10个虚拟机并发数量，可大幅提高备份恢复效率； 7、虚拟机恢复时实现选择目标集群、资源池和存储资源，实现原位置恢复和恢复为新虚拟机，能够设置恢复后虚拟机的CPU、内存和网络配置。实现保留源虚拟机MAC地址恢复，实现恢复后自动打开虚拟机； 8、实现永久增量备份技术，初次备份对所有数据进行完全备份，之后只对新增加或改动过的数据做增量备份。每个增量备份的数据副本将自动合成为完全副本，能够大幅度减少备份时间，节省备份数据所需的存储空间，且提升了恢复效率； 9、实现对备份数据进行加密传输和存储，至少实现AES256和SM4两种加密算法，提升传输过程以及存储的安全性； 10、所有数据恢复任务最后一步，均需要操作者在提示界面确认，避免误操作； 11、实现系统管理员，审计管理员、安全管理员、租户,操作员和巡检员六类角色，通过分权管理，提升备份系统的管理安全性； 12、软件许可：Windows和Linux平台下的定时备份，不限制需要备份的服务器、PC机、虚拟机的数量，不限制数据库的数量与类型； | 1 | 台 |  |
| 6 | Web应用防火墙 | 1、网络层吞吐量≥6Gbps，HTTP新建连接数≥6万，HTTP并发连接数≥180万，内存≥4G，配置不少于6个10/100/1000M Base-TX接口；4个SFP接口； 2、产品采用多核并行处理架构； 3、实现虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求； 4、实现通过被动扫描功能，业务系统进行黑链检测、Webshell检测、漏洞风险检测、配置风险检测、弱口令账户检测。 5、实现口令暴力破解防护，至少包含FTP、Web、Weblogic、Zabbix、Wordpress、Tomcat等组件，并实现自定义FTP和Web的爆破阈值设置； 6、实现业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因WEB应用中因代码不规范和安全检测功能冲突导致的业务误判问题； 7、实现主动扫描功能，实现识别网站目录结构，实现自定义扫描模板，实现在扫描模板中自定义扫描限制、扫描代理、自定义404页面规则、爬虫限制、测试项目。 8、实现识别HTTP异常，包含HTTP方法过滤、HTTP头部字段Referer、User-Agent等注入检测、Host检测、URL溢出检测、POST实体溢出检测、HTTP头部溢出检测、range字段防护、multipart头部字段异常检测、Content-Type头部字段异常检测； 9、实现超过3700种Web应用防护规则。 10、实现网站防篡改功能，实现Windows和Linux双平台操作系统，防止攻击者篡改文件系统； 11、实现针对业务风险汇总，实现展示业务安全状态分布，包括已失陷业务、正在遭受攻击的业务、存在漏洞但暂时未被攻击的业务，以及最近7天内的漏洞风险分布情况； 12、实现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； | 1 | 台 |  |
| 7 | 堡垒机 | 1、包含运维授权数≥50，可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200。内存大小≥4G，硬盘容量≥1T SATA，配置6个10/100/1000M Base-TX接口； 2、物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构； 3、实现字符协议：SSHv1、SSHv2、TELNET，图形协议：RDP、VNC，文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板等； 4、实现通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入； 5、用户登陆认证方式实现静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并实现各种认证方式和静态口令组合认证； 6、内置三员角色的同时实现角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴； 7、实现RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别； 8、实现配置资源访问时间规则，即使授权范围内的资源，需在指定时间范围内才可发起访问，确保运维在可信时间范围； 9、实现倍速播放、拖动、暂停、停止、重新播放等播放控制操作，并可以指定时间点定位播放位置； 10、实现跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问； 11、全面实现Windows、linux、国产麒麟系统、Android、IOS、Mac OS等客户端操作系统下的H5页面一站式运维，实现跨终端适应性BYOD（Bring Your Own Device）； | 1 | 台 |  |
| 8 | 漏洞扫描 | 1、系统漏扫授权IP数≥100，主机漏扫最大并发IP数≥70，内存大小≥8G，硬盘容量不低于128GB SSD，1TB SATA，配置6个10/100/1000M Base-TX接口，2个SFP接口； 2、采用有自主知识产权的安全操作系统，采用B/S设计架构，并采用SSL加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理； 3、实现全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情； 4、实现同时开启全插件系统漏洞扫描、WEB漏洞扫描、弱口令扫描、基线配置核查，扫描速度不低于1000ip/h； 5、实现从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况； 6、实现从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，实现以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情； 7、实现信息泄漏类漏洞检测，如：mail地址、敏感目录暴露、内部IP地址、会话令牌、源码、数据库备份文件、SVN文件、系统重要配置、日志文件向外网泄漏等； 8、实现快速扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中快速扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行； 9、实现对Windows、Linux等操作系统按照等保二级、等保三级要求实施基线配置核查； 10、实现报表过滤功能，实现从任务类型、任务/资产、风险等级、漏洞/基线类型等角度筛选和过滤报表生成条件； 11、实现查看系统CPU、内存、磁盘资源的使用情况，实现系统设备状态的实时监控、一键式关机和重启； 12、系统实现ping、curl、traceroute、dig、nmap等工具； 13、产品实现对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表； | 1 | 台 |  |
| 9 | 日志审计 | 1、机架式,6个千兆电口，50日志源授权，综合采集处理均值3000EPS 2、实现根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数； 3、实现百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s；数据存储能力：压缩加密存储，压缩比不低10:1，日志存储不低于10000条/M； 4、实现安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集； 5、实现对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；  6、实现主动、被动相结合的数据采集方式；支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；实现通过Agent采集日志数据； 7、实现日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者； 8、实现首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息； 9、实现实时自动刷新每个日志源的实时日志列表，实现在实时日志界面通过选择过滤器来监视所关注的特定类型的日志； 10、实现首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出； 11、实现独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，实现独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态； 12、实现对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击； 13、实现IPv6/IPv4双栈环境部署，对IPv6/IPv4日志源的日志进行采集，实现标准协议下（Syslog）的IPv6日志采集，实现IPv6日志的查询、统计和存储。 14、实现对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； 15、实现基于拓扑图的日志源相关数据信息快速查看；实现通过拓扑下钻查看对应日志源的日志、报表、告警数据； | 1 | 台 |  |
| 10 | 数据库审计 | 1、2U机架式结构， 默认包含1个10/100/1000BASE-TX管理口，5个10/100/1000BASE-T电口采集口，4个SFP插槽，2个USB接口，1个Console接口，2个可插拔扩展插槽；1T存储空间，配置双电源，带有液晶屏；含3年攻击检测规则库、僵尸主机规则库升级许可 2、实现sql错误统计，多维度展示错误占比及趋势，从源IP维度以柱状图展示SQL错误数（TOP10），可以列表形式给出出错原因、出错信息以及解决办法； 3、实现SQL效率分析，以饼图展示正常SQL与慢SQL占比情况、TOP10慢SQL的详细分析：TOP排名信息、事件ID、数据库名、目的ip、协议类型、源ip、sql响应时间、操作类型、具体sql语句等要素； 4、实现Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata、HANA、Hive、Hbase、ES（elaticsearch）、Redis、浪潮KDB、MongoDB等数据库系统。 5、实现按数据库实例、数据库名、用户名、数据库表名、表字段名、操作类别、SQL语句、响应时间、连接时长、会话ID、关联规则ID、操作结果、SQL返回结果集、数据库客户端程序、数据库服务器端程序等作为查询和统计条件。 6、实现会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节； 7、实现等保、萨班斯法案报表模板以及自定义报表，可以按日、周、月等周期自动生成报表； 8、实现手动、自动方式的磁盘清理，可根据剩余空间、保存时限等条件灵活设置，磁盘空间占用情况的检查频率可灵活设置：10min、30min、1h、3h、6h、24h等时长； 9、安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统； 10、实现数据库监控，支持数据库名、实例名、数据库类型、数据库服务器负载、活跃会话数以及CPU、硬盘、内存等信息的展示；  11、实现系统配置文件和系统策略的明文或密文的导入导出；  12、对无法镜像流量的审计场景，实现多种类型操作系统的探针部署，适配的操作系统至少包括以下几种： WinSer2003/2008/2012/2016、Centos、opensuse、redhat、Ubuntu、中标麒麟SV1.2-龙芯、银河麒麟SV1.3-飞腾、银河麒麟server-飞腾； | 1 | 台 |  |
| 11 | 防火墙特征库升级 | ★现有华为USG6620防火墙特征库3年升级； | 1 | 套 |  |
| 12 | 上网行为管理特征库升级 | ★现有天融信上网行为管理ACM-51638特征库3年升级； | 1 | 套 |  |
| 13 | iPv6升级 | ★现有核心交换机华为S12704进行iPv6功能授权 | 1 | 套 |  |
| 14 | 二级等保测试 | ★委托有测评资质的第三方机构进行测评后，进行整改，确保达到二级等保要求，所产生费用由中标方承担。 | 2 | 系统 | 对2个现有业务系统测评。 |
| 15 | 辅材 | 本次项目所用到的所有的配件及辅材 | 1 | 项 |  |