**安徽商贸职业技术学院教科研一体化平台**

**采购项目（第一包）需求方案**

1. **项目名称**

安徽商贸职业技术学院教科研一体化平台采购项目（第一包）

1. **项目背景**

安徽商贸职业技术学院于2018年购买了数据库审计、负载均衡、态势感知平台、安全感知系统、潜伏威胁探针、WAF、基线核查等安全设备。随着当前高校业络系统日益复杂，外部攻击、内部资源滥用、木马和病毒等不安全因素越来越显著，当前设备已无法满足信息化建设需求，根据《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例》等法律法规和网络安全类产品规定，拟采购一批设备用于保护校本数据安全和网络安全。

**三、技术需求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **技术参数及要求** | **数量（单位）** | **所属行业** | **备注** |
| 1 | 教科研数据安全设备1--网络安全防护与态势管理设备 | **功能一（数据库审计）：**  ★1、标准2U机架设备，内存≥32G，机械硬盘≥32T，千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，扩展槽位≥2个，冗余电源，配置液晶屏；  2、整机吞吐量≥8Gbps，可审计流量≥800Mbps，峰值SQL处理能力≥50000条/s，日处理能力≥4000万条；  3、支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统；支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统；支持KingBase、DaMeng、Oscar、GBase、浪潮\_KDB、Highgo、GaussDB等国内主流数据库系统；  ★4、支持HTTP、Telnet、FTP、Rlogin的解析；支持工控协议Modbus的解析，规则条数不少于10000条，支持对僵尸网络、木马控制、蠕虫、挖矿、勒索等僵尸主机行为检测告警；**（投标文件中须提供产品功能截图证明）**  5、内置默认控制规则，包括用户登录、低中高风险操作、数据库DML、DCL、DDL等操作语句等规则定义，方便用户引用和制定控制规则；支持内置规则一键复制，可基于复制后的标准规则模板进行优化配置，满足用户精细化场景下审计需求；  ●6、数据库审计系统能够正确的展示近5分钟的审计数据，能够正确的弹出会话回放对话框，能够正确回放选中事件的整条会话信息，能够正确的展示实例的轨迹显示，并可以显示不同节点的信息；**（投标文件中须提供第三方检测机构出具的带有CMA或CNAS标志的检测报告扫描件，至少包含报告首页，对应功能测试页和报告尾页）**  7、支持查看会话回放，支持倍速回放，至少包括2倍速、3倍速、4倍速等，完整还原数据库操作情况；  8、产品支持SQL错误页面正常展示SQL错误及解决方法；支持以饼状图展示正常 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；  9、支持系统阈值设置，支持CPU报警设置、硬盘报警、内存报警功能，支持抓包工具；  10、支持记录数据库操作的源/目的 IP、源/目的端口、源/目的 MAC、源操作系统账号、表名、SOL 语句、客户端程序、客户端用户名、源计算机名、预处理 SQL、响应时间、影响行数、错误码等；  **功能二（负载均衡）：**  ★1、标准2U机架设备，内存≥64G，CF卡≥2G ，机械硬盘≥1T，千兆电口≥10个，万兆光口≥4个，双电源，扩展槽位≥4个，配置液晶屏；  2、负载均衡吞吐量≥120G，并发连接≥7000万，四层新建≥200万，七层新建≥220万；  3、支持多功能合一同时支持链路负载均衡、服务器负载均衡和全局负载均衡的功能，无需额外购买相应授权；支持IPV6/IPV4双栈，支持NAT66、NAT64、NAT46、DNS64可对过渡型网络进行负载均衡；  3、支持轮询算法、比率算法、带宽比率算法、首个有效算法、随机算法、加权随机算法、丢包算法、最小连接数算法、加权最小连接数算法、最小流量算法、加权最小流量算法、观察者算法、最小包速率算法、最小带宽算法、最小连接速率算法、静态就近算法、动态就近算法、静态就近（HA）算法、源地址算法、目的地址算法、源地址和源端口算法；  ●4、DNS server支持A记录,AAAA记录，CNAME记录，MX记录、NS记录、TXT记录、CAA记录、SRV记录。支持主域名服务器、从域名服务器和转发域名服务器；**（投标文件中须提供产品功能截图）**  ★5、地址库包含国内ISP地址库、全国地址库和全球地址库，支持地址库手动导入，支持地址库查询；**（投标文件中须提供产品功能截图）**  6、支持主动健康检查和被动健康检查相结合的方式，健康检查类型包括ICMP、TCP、TCP\_ECV、UDP、TCP被动、HTTP、HTTPS、FIX、SSL、SOAP、HTTP被动、RADIUS、LDAP、WAP、DNS、IMAP、POP3、SMTP、FTP、EXTERNAL、数据库等；  7、利用读写分离技术实现数据库负载且无需在服务器上安装任何插件或软件。通过对数据库操作请求做内容解析，将其中的写操作调度到指定服务器，减少服务器压力，提高数据库资源利用率，提升业务响应速度；  8、支持CSS加速功能，支持内嵌CSS,合并CSS,最小化CSS。支持JavaScript加速功能，支持内嵌JS，合并JS，最小化JS。支持HTML加速功能，支持去除空白，去除注释。支持图片加速功能，支持内嵌图片，转换图片格式；  **功能三（潜伏威胁探针）：**  ★1、标准2U机架设备，网络层吞吐量≥2Gbps，内存大小≥8G，千兆电口≥8个，万兆光口≥2个；  2、产品旁路部署支持探针接入多个镜像口，每个接口相互独立且不影响；  3、支持敏感信息检测功能，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于IP统计和连接统计2种方式进行命中次数统计；  4、支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用，针对命令注入检测、SQL注入检测等类型支持自定义高检出、低误报模式；  5、支持多种类型弱口令策略可选；支持自定义FTP弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB登录）的爆破次数；  ●6、支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Media漏洞攻击、Network Device、Shellcode漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击、IPS云防护等服务漏洞攻击检测；**（投标文件中须提供产品功能截图）**  7、支持FTP、IMAP、MS Sql、Mysql、Oracle、Discuz、Basic Authorization、Glassfish、POP3、RDP、Sip 、Jboss、Redis 、Ldap 、SMTP、SSH、Telnet、Tomcat、Sybase、Weblogic 、Wordpress 、VNC等73种协议暴力破解检测；  8、支持检测出网络中的网络拓扑设备进行绘制，更直观可视化查看网络整体情况；  9、支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测；  10、为提升学校现有设备利用率，本次所投探针需同步支持与学校现有态势感知平台数据对接；  **功能四（态势感知平台）：**  ★1、标准2U机架式设备，存储容量≥21T，内存≥4\*32GB DDR4 3200，数据盘≥8\*4TB，标配盘位数≥12，配备冗余电源，接口≥4千兆电口。  2、本次新增态势感知平台，需能与我单位现有态势感知平台组件集群化运行，通过同一个管理平台统一管理，原有资产信息、脆弱性信息、安全告警、安全事件信息自动同步到现有平台；  ●3、支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合安全态势、物联网安全态势、分支安全态势、安全事件、通报预警态势、脆弱性态势、资产态势、全球网络攻击态势、资产监控、告警实时监控、设备运行态势、重大活动网络安全指挥调度大屏、正常外连监控等不少于17块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；**（投标文件中须提供产品功能截图）**  4、支持主机类资产识别，能够识别资产数据来源、IP地址、主机名、MAC地址、基线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP类型、识别方式、首次发现时间等；  5、支持EBA实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括DGA解析请求、外联C&C服务器、异常协议利用、下载可疑文件、异常横向访问等；  6、支持挖矿专项检测页面，帮助客户更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者IP、攻击次数、威胁情报等信息；  7、实时检测到关注告警类型的威胁可以发出声音告警提醒用户。支持受害者IP/攻击者IP/代理服务器IP/威胁描述/威胁类型等维度自定义告警复制，支持基于威胁定性、重点关注资产以及威胁类型排行等维度对告警进行筛选；  8、支持自定义分支管理权限，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等；  9、支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它4个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置；  10、支持对下级平台和探针设备进行统一运维监控，支持对网卡，内存，raid卡，磁盘的硬件异常进行故障监控；支持故障告警在横幅优先展示，提升设备安全性；  11、支持整体展示服务器脆弱性风险分析、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web明文传输、可用性风险）；  ★以上所有功能项需提供原厂商5年质保及相关配套升级服务。 | 1套 | 工业 |  |
| 2 | 教科研数据安全设备2--网络安全边界与访问管理设备 | **功能一（出口防火墙）：**  ★1、标准机架式1U设备，防火墙吞吐量≥35Gbps，最大并发连接数≥2000万，每秒新建连接数≥50万;  2、整机提供千兆Combo接口≥8个，千兆电口≥4个，万兆光口≥10个，配置双电源，240G SSD硬盘≥1块，SSL VPN并发数≥100个；  3、产品采用国产自主研发的关键芯片(CPU) ；  4、支持设备的WEB管理页面中直接打开CLI控制命令；  5、支持基于源IP/目的IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置；  6、支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议，支持SRv6协议，支持IPv6协议栈、IPV6穿越技术、IPV6路由协议；  7、系统预定义签名数量≥20000，并支持特征库自动更新；  ●8、支持应用识别，预置应用≥6000，支持自定义应用，支持50+的分类和20+的风险标签，可基于分类及标签进行访问控制;**（投标文件中须提供官网截图证明）**  9、在识别业务应用的基础上，可管理每IP使用的带宽,确保关键业务和关键用户的网络体验，管控方式包括限制最大带宽或保障最小带宽、修改应用转发优先级等；  ●10、支持DNS恶意域名过滤,基于海量的威胁信息,利用AI等技术发现恶意DNS请求，本地最大支持200万的DNS恶意域名库；**（投标文件中须提供官网截图证明）**  **功能二（内网防火墙）：**  ★1、标准2U机架设备，内存≥16G，机械硬盘≥4T，千兆电口≥8个，万兆光口≥10个，千兆光口≥2个，扩展槽位≥2个，冗余电源；  2、吞吐量≥35G，应用层吞吐量≥16G，并发连接≥2000万，每秒新建连接≥50万；  3、支持路由、交换、虚拟线、Listening、混合工作模式；支持RIP、OSPF、BGP4、QinQ（VLAN VPN）、PIM-SM、PIM-DM等；  4、支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换。  ●5、支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、数据库防护、防代理、APT等功能配置；**（投标文件中须提供第三方检测机构出具的带有CMA或CNAS标志的检测报告扫描件，至少包含报告首页，对应功能测试页和报告尾页）**  6、提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析、宽泛策略分析，可在WEB界面显示检测结果；  7、访问控制策略执行动作支持放行、阻断、认证、收集，对需要认证的流量进行Web认证，策略中可设置用户 Web 认证的门户地址或收集策略流量访问记录，生成更细粒的策略；  8、支持IPv4/IPv6双栈安全控制策略，支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；  9、具有恶意代码防护引擎，能够对各种协议传输的恶意代码进行监测；具备恶意网站库，能够根据分类对恶意网站进行过滤；能够拦截带有恶意代码的HTTP访问和电子邮件收发；具备恶意加密流量检测功能，可自动添加恶意加密流量的阻断策略，防火墙上可以产生相应的访问控制日志；  10、支持配置文件本地备份和回滚，支持≥3个配置文件备份，支持配置定时保存，支持配置导入及明文/密文导出，支持对访问控制策略；  **功能三（基线核查）：**  ★1、标准2U机架式设备，双电源，千兆电口≥6个，千兆光口≥4个，硬盘≥2T，支持最大并发扫描主机数≥120个，IP、域名扫描数量无限制；  2、漏洞库数量≥30万个，兼容CVE、CNVD、CNNVD、CWE、Bugtrap、微软KB等主流漏洞标准，并提供CNNVD兼容性证明，其中自研PoC漏洞数量 5000+；  3、支持自定义漏洞PoC功能，自定义内容包括但不限于漏洞名称、漏洞等级、漏洞类型、漏洞危害、CVSS信息、检测脚本等，用于日常突发漏洞应急；  4、支持针对系统漏洞扫描功能，包含但不限于操作系统、数据库、应用软件、网络设备、安全设备、移动设备等；  5、支持Web漏洞检查能力，包括但不限于SQL注入、XSS、CSRF、反序列化、LDAP注入、XPath注入、文件上传、水平权限绕过、信息泄露等；  6、具备Web应用被动扫描能力，通过代理监听Web应用运行状态，自动识别和发现漏洞；  ★7、支持全局视角分析漏洞状态，包括漏洞的新增分析、漏洞修复分析、资产运行状况分析、资产数据统计分析、资产风险等级分析、风险组织单位分析、业务系统漏洞排名分析、漏洞等级、弱口令漏洞排名分析；**（投标文件中须提供功能截图）**  ★8、支持盲打平台反连配置，fastjson、SSRF、log4j、代理未授权等需要反向连接确定的漏洞；**（投标文件中须提供功能截图）**  9、提供基线管理功能，内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板；支持Word、Excel、HTML、PDF、JSON等多种格式报表导出；  10、通过周期性的监控，持续对网站的文本内容进行检测，以保障网站的安全性和合规性。一旦检测到敏感关键字的存在，则发出告警；  11、提供主机扫描（主动）扫描策略，包含主机资产发现模块、系统漏洞检测模块、系统漏洞库、基础服务漏洞扫描策略；  12、Web扫描(主动)扫描策略，包含爬虫引擎、Web漏洞检测模块、Web漏洞库、基础Web漏洞扫描策略；  **功能四（行为管理）：**  ★1、标准2U机架设备，整机提供千兆电口≥4个、千兆光口SFP≥4个、万兆光口SFP+≥2个，配置冗余电源；  2、网络层吞吐量≥20Gb，应用层吞吐量≥9Gb，支持用户数≥50000，包转发率≥1Mpps，每秒新建连接数≥50000，最大并发连接数≥3200000；  3、支持路由模式（NAT、路由转发、DHCP、GRE、OSPF）、网桥模式（多路桥接模式）、旁路模式；  4、可设置四类管理员，分别为系统管理员、安全管理员、审计管理员，以及多种权限的超级管理员；管理员支持分级，高级别管理员的策略配置优先生效，并可修改低级管理员的策略；  ●5、支持网络故障排查，支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况；提供图形化排障工具，便于管理员排查策略错误等故障;支持针对用户认证的故障进行分析，给出错误详情以及处置建议；**（投标文件中须提供产品功能截图）**  6、支持从本地导入和扫描导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息；用户分组支持树形结构，支持父组、子组、组内套组等；  7、支持代理控制功能，不允许使用外部HTTP代理，不允许使用外部SOCKS4/5代理，不允许在HTTP，SSL一些的标准端口上使用其他协议；  8、支持根据IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标IP组提供的服务；支持根据不同的应用类型或具体的某种应用设置允许或拒绝；  9、支持SSL中间人解密和客户端解密，确保数据传输的透明性与安全性，客户端会自动推送根证书安装，支持记录全部或者指定类别URL、网页标题、网页内容等信息，支持网页内容审计后的网页快照功能；  10、支持基于用户组、位置、终端类型、URL类型配置流量管控策略，支持基于IP或用户名灵活配置流控单位；  ●11、提供Web访问质量检测功能，针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；**（投标文件中须提供产品功能截图）**  12、支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率，空闲值可自定义；  13、提供原厂商5年质保及特征库升级服务。  **功能五（WAF）：**  ★1、标准2U机架式设备，CPU≥6核，内存≥32G，固态硬盘≥128G，机械硬盘≥2T，，USB接口≥2个，RJ45串口≥1个，GE管理口≥2个，GE业务口≥10个（含5组bypass），10GE业务口≥2个（bypass，满配光模块），冗余电源；  2、整机吞吐量≥30G，每秒连接数≥1.4W，并发连接数≥500W；  3、具备HTTP/1.X、HTTP/2和HTTPS报文解码能力，可对攻击者编码绕过行为进行有效识别。解码能力包括但不限于：HTML解码、Unicode解码、十六进制转换、斜杠反转义、二进制解码等不少于10种，能对10层的嵌套编码绕过行为进行有效检测与防护；  ●4、无需规则配置，可通过语义分析技术识别OWASP TOP 10所公布的WEB应用程序安全风险，如SQL注入、XSS、PHP反序列化、Java反序列化、PHP代码注入、Java代码注入、命令注入、CSRF、SSRF、ASP代码注入、模版注入、文件包含、文件上传等13种常见攻击类型，可根据攻击语法特征，智能生成攻击威胁等级；**（投标文件中须提供产品功能截图）**  5、检测引擎支持自动区分注入型/非注入型攻击，可自动放行非注入型SQL、XSS等，避免业务请求包含完整SQL语言从而导致WAF大量误报；  6、支持对性质可疑的复杂攻击进行多维度关联攻击验证，支持同一时刻平行检查，可对攻击按照规则进行穷举遍历匹配，并在攻击检测日志中完整记录请求命中的所有攻击检测信息，有效阻止多阶段、隐匿性Web攻击；  7、支持自定义规则检测前对请求进行解码，解码类型包括：Base64解码、十六进制解码等不少于5种，可根据业务系统编码类型进行配置，快速实现新爆发漏洞的防护；  8、支持CC攻击防护，可通过限制IP、Session和用户指纹实现对异常访问行为的限制，限制时间及限制路径可灵活定义；  9、支持自定义拦截状态码和阻断页面，可以根据不同的状态码响应不同的阻断页面，便于安全人员基于业务场景精细化配置拦截页面；  10、支持误报消除功能，可在日志告警界面一键添加例外白名单，自动在后续检测中消除同类型误报，避免人为输入错误；  11、具备0day漏洞防护能力，能够自动检测攻击特征，实现告警和拦截，可提供实际防护案例说明及原理说明；  12、支持WAF能力原子化可编排，支持可视化显示WAF检测流程，可在不同的检测点直接插入业务规则，可按照业务场景自动调整检测流程，满足业务差异化防护需求；  13、支持对记录并存储全量访问日志，并可通过Syslog外发，便于安全管理员分析异常事件；**（投标文件中须提供产品功能截图）**  ★以上所有功能需提供原厂商5年质保及相关服务升级服务。 | 1套 | 工业 |  |

**四、评分办法**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **评分内容** | **评分标准** | **分值范围** |
| 技术资信分  （70分） | 所投产品技术参数及要求响应情况 | 根据投标人所投产品对招标文件技术参数及要求的响应情况进行综合评分：  1、标注“★”的技术参数及要求，每满足或优于一项，得2分，共15项，满分30分；  2、标注“●”的技术参数及要求，每满足或优于一项，得1分，共10项，满分10分；  3、无标识项的技术参数及要求，有3条及以上不满足要求的，将导致投标无效。  **注：以投标响应表和“技术参数及要求”中要求提供的证明材料作为评审依据。**  **合同签订前中标人须根据采购人要求对招标产品要求响应情况逐条测试，如发现虚假响应的，采购人有权终止合同采购，并报相关部门依规处理。** | 0-40分 |
| 安装调试及培训方案 | 由评标委员会根据投标人提供的实施方案及培训方案、安装施工质量保证及质量控制方及技术培训方案进行综合评分。  1、安装实施及技术培训计划周密、合理，调试仔细、确保设备正常使用，制定了具体可行的保证措施的，得5分；  2、安装实施及技术培训计划较为详实、实施各种风险考虑较为充分，能够满足采购人的实际需要的，得3分；  3、提供的方案内容较为简单，细节有待进一步完善的，得 1分；  4、差或者未提供任何内容的不得分。 | 0-5分 |
| 售后服务方案 | 由评标委员会根据投标人提供的售后服务方案进行综合评审：  1、售后服务体系科学、健全，故障响应时间、到场时间合理，人员培训措施得当，有利于项目顺利实施的，得5分；  2、售后服务体系比较健全，故障响应时、到场时间基本合理，人员培训措施较为得当，对项目实施有一定积极作用的，得3分；  3、售后服务方案有待进一步细化提升的，得1分；  4、差或未提供任何内容不得分。 | 0-5分 |
| 投标人认证 | 1、投标人具有经中国国家认证认可监督管理委员会认可的认证机构颁发的有效期内的：质量管理体系认证、环境管理体系认证、职业健康安全管理体系认证证书的，得2分，缺一项不得分。  2、投标人具有经中国国家认证认可监督管理委员会认可的认证机构颁发的有效期内的：信息技术服务管理体系认证证书、信息安全管理体系认证证书的，每提供一个得2分，本小项满分4分。  3、投标人具有有效的信息技术服务运行或维护类证书，得1分，满分1分；  **注：投标文件中提供上述证书扫描件，其中第1-2项须同时提供全国认证认可信息公共服务平台官网证书信息查询截图。** | 0-7分 |
| 投标人技术实力 | 1、投标人为本项目配备的项目经理具有计算机技术与软件专业技术资格的系统集成项目管理工程师认证证书的，得3分，本小项满分3分；  2、投标人为本项目配备的服务人员具有计算机技术与软件专业技术资格的网络工程师认证证书的，得2分，本小项满分4分；  注：  3、投标文件中须提供：  （1）上述人员名单（格式自拟）；  （2）上述人员有效期内证书扫描件；  （3）投标人为上述人员缴纳的近3个月内任意1个月的社保证明材料。社保证明材料形式详见投标人须知前附表，提供任意五险之一即可；  （4）投标人所提供的人员证书及社保必须真实可靠，如发现弄虚作假,则取消其本项目的中标资格,并报相关部门依规处理。 | 0-7分 |
| 投标人业绩 | 自2022年1月1日以来（以合同签订时间为准），投标人具有网络安全建设业绩（合同内容须包含网络安全产品且必须是与最终用户直签的业绩合同），每提供一个业绩得2分，满分6分。  注：  （1）投标文件中同时提供合同、验收证明材料（如验收报告等）扫描件。如提供的上述材料无法体现业绩类别等关键信息的，须另附业主单位（合同甲方）提供的相关证明材料，且该证明材料须经评标委员会认可，否则不予计分。  （2）提供的业主验收证明材料（如验收报告等）须加盖业主单位公章（或部门章），否则不予认可。  （3）投标人需确保业绩合同真实有效，投标人须提供业绩合同原件供招标人核查，若业绩合同存在伪造、篡改等虚假情形，招标人将作废标处理，相关违规行为将上报行政监督部门记入信用档案，并依法追责。 | 0-6分 |
| 价格分  （30分） | 价格分统一采用低价优先法，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分 30 分。其他投标人的价格分统一按照下列公式计算：  投标报价得分＝（评标基准价/投标报价）×30％×100 | | |