

绍兴市公共交通集团有限公司物联网卡和网络线路、网络安全技术服务和设备采购等项目

报  
价  
文  
件  
部  
分

浙江省通信产业服务有限公司

2024年12月30日

# 目录

一、 开标一览表（报价表） .....	1
二、 中小企业声明函.....	1

## 一、 开标一览表（报价表）

（绍兴市公共交通集团有限公司）、（浙江天源工程管理咨询有限公司）：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下开标一览表（报价表）的价格完成（绍兴市公共交通集团有限公司物联网卡和网络线路、网络安全技术服务和设备采购等项目）【招标编号：（CGSHZJ-2024-N001094）】的实施。

开标一览表（报价表）（单位均为人民币元）

序号	名称	品牌（如果有）	规格型号	数量	单价	合计	备注（如果有）
第一部分：网络安全技术服务部分							
1	安全咨询与规划服务	国产优质	规格：服务描述： 依据等级保护 2.0 相关标准，结合绍兴市公共交通集团有限公司信息系统具体情况，建立完整的信息安全管理体 系，达到动态的、系统的、制定化的、以预防为主的信息管理方式，用最低的成本，达到可接受的信息安全水平，最大限度保证业务的持续性。 服务方式：现场/远程 服务范围：绍兴市公共交通集团 服务频率：1 次 服务输出：《安全规划方案》 型号：定制	3	20000.00	60000.00	
2	漏洞分析与加固服务	国产优质	规格：服务描述： 网络安全讲一百遍不如打一遍，实战	3	20000.00	60000.00	

			<p>化是检验网络安全防护能力的唯一标准。一个漏洞的存在给业务系统带来的危害是致命的，不可想象的。漏洞被利用导致的信息安全事件不胜枚举，轻者业务系统运行缓慢和中断，重则敏感数据泄露或丢失。发现高（中）风险问题后，涉及到相关业务系统的提出加固整改建议。</p> <p>服务内容：</p> <p>1) 安全漏洞检测：如操作系统、中间件、B/S 业务系统、数据库等漏洞；</p> <p>2) 业务逻辑漏洞检测：如后台登录处存在逻辑错误，登陆时没有错误次数限制用户登录，并且没有判断验证码过期，导致验证码可以重复使用，可被爆破用户名密码或撞库；</p> <p>3) Webshell 检测：如网页后门程序、线程插入后门程序、扩展后门程序；</p> <p>4) 弱口令核查，复用口令核查。</p> <p>服务人数：2 人</p> <p>服务方式：现场</p> <p>服务对象：绍兴市公共交通集团重要信息系统</p> <p>服务频率：2 次/年</p> <p>服务输出：《漏洞评估报告》</p> <p>工具要求：</p> <p>支持检测的漏洞数大于 230000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准。</p> <p>支持国产操作系统的漏洞扫描，包括麒麟（Kylin）、统信（UnionTech</p>				
--	--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			<p>OS)、中兴新节点(NewStart CGSL)等。</p> <p>支持操作系统、网络设备、数据库、中间件等漏洞扫描。</p> <p>支持采用SMB、RDP、Telnet、SSH等协议对系统进行登录扫描。</p> <p>支持全面扫描、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,其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。</p> <p>提供检测结果综述分析,按照等保2.0的检测项要求,统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项,直观了解自身业务系统合规情况。</p> <p>产品支持对系统漏洞、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。</p> <p>型号:定制</p>				
3	应急演练服务(桌面推演)2个演练剧本	国产优质	<p>规格:服务描述:</p> <p>网络安全应急演练服务覆盖演练准备工作、演练环境搭建、演练剧本编写、演练彩排工作、正式演练大会活动、应急演练总结等各个阶段,帮助绍兴市公共交通集团实现全面有效的应急演练。通过应急演练工作,进一步明确各应急小组在应急响应工作中的职责,熟练掌握应急响应的处置程</p>	3	40000.00	120000.00	

			<p>序、方法和注意事项，有效提高绍兴市公共交通集团整体应急响应的反应能力、指挥水平和实战能力，增强各部门应急人员之间的协调性，检验单位应急救援预案的可行性和可操作性，使其达到应急演练的预期效果。</p> <p>服务方式：现场演练  服务范围：绍兴市公共交通集团  服务频率：1次  演练脚本：2个  服务输出：《应急演练方案》、《应急演练总结报告》  型号：定制</p>				
4	应急响应与溯源服务	国产优质	<p>规格：工作内容：  在发生确切的网络安全事件时，应急响应实施人员应及时采取行动，限制事件扩散和影响的范围，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件解决方案，追查事件来源，协助后续处置。</p> <p>服务人数：2人  服务方式：现场或远程  服务对象：绍兴市公共交通集团重要信息系统  服务频率：按需响应，不限次数  时间要求：不限次数。1小时内抵达客户现场，2小时内定位问题，4小时内控制风险、事件。  服务输出：《应急响应处置报告》  型号：定制</p>	3	40000.00	120000.00	

第二部分：网络维护服务部分

1	集团机房日常网络系统维护（机房及服务器及网络系统等信息化系统）	国产优质	<p><b>规格：基础设施管理：</b>1. 确保网络通信传输畅通。2. 负责网络布线架的管理，确保配线的合理有序。3. 掌握客户端设备接入网络情况，以便+发现问题可迅速定位。4. 采取技术措施，对网络内经常出现的用户需要变更位置和部门的情况进行管理。5. 掌握与外部的链接配置，监督网络通信状况，发现问题后与有关机构及时联系。6. 实时监控局域网的运行河网络通信情况；</p> <p><b>应用系统管理：</b>1. 确保各种网络应用服务运行的不间断性和工作性能的良好性。出现故障时应将造成的损失和影响控制在最小范围；2. 对于要求不可中断的关键型网络应用系统，除了在软件手段上要掌握，备份系统参数和定期备份系统、业务数据外，必要时在硬件手段上要建立和配置系统的热备份；</p> <p><b>路由、局域网环境检查：</b>1. 测试到路由、交换机以及外部网络的连通性。2. 查看所有路由、交换机端口以及状态灯的工作状态，保证设备工作正常。3. 检查网关设备（防火墙、路由）工作状态，确保外网连接正常。4. 检查网络线缆，确保网络线缆完好无损</p>	3	100000.00	300000.00	
---	---------------------------------	------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	-----------	-----------	--

			相关资质：中标后提供机房安全设备（防火墙等）维护授权资质 型号：定制				
<b>第三部分：一网统管部分</b>							
1	一网通智能监控平台 (国产软件)	北塔	<p>规格： 总体要求：产品架构支持中台+微应用架构，支持运维运营化管理，支持扩展为整个多产品的支持服务平台，根据安全原则，系统用户权限定义原生支持三员分立</p> <p>CMDB：▲可自定义不同业务资源主题，覆盖全运维领域，包括监控、IoT、自动化、资产、视频、DevOps，不同业务主题可通过各自视图查看模型（要求提供功能截图）</p> <p>▲提供配置项（CI项）的变更历史查询，可查看原配置项变更到新值的全历史记录，包括变化时间、变更人属性值。（要求提供功能截图）</p> <p>运维场景自动化管理：编排语句采取拖拽式、自然语言语句编排</p> <p>▲提供多种触发执行场景的能力，包括周期执行、告警驱动、手工执行、指标驱动执行。通过指标驱动执行，可以将场景实现的统计指标作为指标，应用到告警、历史记录、自定义首页部分。（要求提供功能截图）</p> <p>告警管理：▲提供告警信息所属的事件标签分类，并标识出告警持续时间显示，对手工撤销告警的操作，要求</p>	1	390000.00	390000.00	



			<p>标注和展示手工撤销理由、撤销人信息。（要求提供功能截图）</p> <p>支持屏幕颜色告警、告警邮件提醒、和短信猫告警、企业微信、钉钉机器人、数据库输出。</p> <p>报表管理：支持多个不同指标在同一时间轴中进行对比分析；支持历史记录任意时段拖拽查看，对于超过3个月的历史数据，支持原始采集颗粒度（5分钟）的对比分析。</p> <p>主机管理：支持系统拓扑图，一张图可以展现所有主机承载的数据库、中间件和标准应用之间的实时状态监控，为主机监控提供全景视图。</p> <p>▲提供操作系统的CPU、内存、流量、存储进行涨势分析，主动识别涨势过快的设备。（要求提供功能截图）</p> <p>支持IPMI方式监控主流国产服务器厂商的硬件，监控内容包括温度、电源、风扇、电压等硬件状态；</p> <p>数据库管理：支持ODBC和JDBC取数方式取数，对SQLServer、Oracle、Sybase、Mysql、Informix、DB2、神通、瀚高等数据库的各项运行参数进行监控；</p> <p>支持对于各个数据库实时运行状态的实时统计，包含数据库会话数、死锁数实时排行，支持对表空间大小和会话数、缓存信息、锁信息进行重点监管。</p> <p>支持Oracle Rac的管理，支持集群分</p>				
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			<p>成操作系统、clusterware、实例方式展现，支持动态数据对比，检测各个承载主机的性能表现</p> <p>中间件管理：中间件管理必须支持对WEBLogic、Tuxedo、WebSphere、EAServer、Cognos、MQ、Apache、Tomcat、Jboss、IIS、TongWeb、中创、TAS 等中间件实时监控。</p> <p>支持图形化方式显示应用的承载主机状态和应用的基本性能信息，同时展示相关的运维负责人和联系方式。</p> <p>标准应用管理：支持FTP、SFTP、HTTP、HTTPS、POP3、SMTP、DHCP、JVM、Exchange 的监控。</p> <p>网络管理：系统能支持各大设备厂商的各型号设备，支持多厂商设备组成的混合网络自动发现。拓扑图的生成必须支持网络设备的SNMP V1、V2、V3这三个版本的混和生成，并能对SNMP V3 设备进行管理；要求在拓扑图上快速定位 IP 地址的接入端口，包括服务器 IP 和 PC 机 IP，并且通过图标进行显示。拓扑图设备间的连线除直线形式外，还可支持以折线、合并线等线型，并可将网络拓扑按照线路图、地域分布图、逻辑关系图等方式呈现；拓扑图线路支持带有流动效果方式展现，支持定义虚实线、粗细、速度等线形设置。；支持在拓扑图上直接调用 webssh 工具，访问设备和主机。允许保存上一次登陆使用账号密码。支</p>				
--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			<p>支持查询接入 IP 的历史变更情况查询。支持异常接入终端的告警通知，可以针对未规划设备、未分配 IP、未在指定位置接入等多种异常进行自动检测。支持网络拓扑中快速定位 PC，并以下标方式显示其使用人信息</p> <p>虚拟化管理：实现宿主机配置、状态、性能信息的一体化管理。实现虚拟机配置、状态、性能信息的一体化管理。要求以图形化方式展现虚拟化拓扑，显示宿主机、虚拟机、虚拟网络、数据存储关系，动态显示管理对象负载、告警。</p> <p>存储管理：支持存储设备硬件管理，以统一的视图展现被管的各个硬件子项的运行详情，清晰展现各个管理设备的各类型管理状态，并以颜色显著标示出现问题的硬件类型；涉及到磁盘阵列的电源、电池、风扇、温度、磁盘、控制器等各个关键硬件信息；支持存储设备性能管理，提供 LUN 读 IOPS TOP 排行；提供 LUN 写 IOPS TOP 排行；提供 LUN 总 IOPS TOP 排行；提供 LUN 的总传输字节数 TOP 排行；提供按照传输流量的存储线路排行</p> <p>知识库管理：支持自定义知识库的分类。新增知识时，支持对知识设置共享范围，公有知识对所有人可见，私有知识可按人员选定。对于非知识库管理员提交的知识有知识库的审核功能。知识库可在各服务管理流程中被</p>				
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			直接引用，支持知识的引用次数统计。 型号：BeCloud MD V1.0				
2	内外专网终端防非法外联技术参数（国产设备）	新华三	规格： 性能要求：网络层吞吐量（大包）：3Gb，带宽性能：250Mb，新建连接数：30000，最大并发连接数：2000000。 硬件要求：规格：1U，内存大小：8G，硬盘容量：500G HDD，电源：单电源，接口：4千兆电口，2个 combo 口。 特征库数量：产品支持应用特征库数量不低于 7100+，提供产品界面截图 精细化控制：支持用户上网应用的精细化控制，例如微信的：“微信”“微信语音”“微信发消息”“微信收消息”“微信登录”“微信发文件”“微信收文件”并提供 web 配置截图 支持移动终端发现管理，可一键添加为信任终端、发现终端后可邮件告警/冻结等，支持趋势图呈现移动终端接入趋势及列表详情等 ▲用户画像：支持用户虚拟身份画像，以时间轴的形式展示用户上网行为轨迹；支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如 QQ 号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分	1	85000.00	85000.00	

			<p>布、全天关键网络行为轴等信息，支持对单用户进行网站访问质量检测，提供 web 界面截图（提供第三方测试报告证明，并加盖 CNAS 章）</p> <p>文件缓存：支持文件缓存，支持安卓和 IOS 形式的文件，主动缓存文件形式包含 APP 应用等，提供 web 配置截图</p> <p>资产梳理：支持对内网资产的 IP、用户、部门、操作系统、重要程度、可用服务、是否可信进行统一梳理，发现问题资产支持阻断 IP，提供产品截图</p> <p>型号：ACG1000-AI-15-G</p>				
3	内外网专网政务网及一公司防火墙（国产设备）	新华三	<p>规格：</p> <p>性能要求：网络层吞吐量：≥6Gbps。 TCP 新建连接速率：≥200w。 TCP 并发连接数：≥5w。 硬件要求：≥4 个千兆电口和 4 个千兆光口，冗余电源，≥2 个扩展槽位</p> <p>NAT 功能：支持 NAT44、NAT46、NAT64、NAT66</p> <p>VPN：可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阈值进行细颗粒度的管控。（提供功能截图）</p> <p>支持 IPsec VPN 智能选路，根据隧道质量调度流量。（提供功能截图）</p> <p>应用识别：支持至少 9000 条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。（提供截图）</p>	3	60000.00	180000.00	

			<p>安全策略：支持基于域名的安全策略模糊匹配（提供功能截图）</p> <p>支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图）</p> <p>加密流量检测：支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供截图）</p> <p>▲虚拟化能力：所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功能要求提供功能截图</p> <p>支持 Context+VRF 二级虚拟化技术，支持 CPU、内存、存储等硬件资源划分的完全虚拟化</p> <p>支持 vSys 虚拟防火墙技术，可以将一台物理设备虚拟成 N 台相互独立的虚拟设备</p> <p>产品资质：所投产品须具备国芯证明材料</p>				
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			具备中国网络安全审查技术与认证中心颁发的 EAL4 增强级认证证书 型号：F1000-CN-G35				
4	流控交换机（国产设备）	新华三	规格： 1. 交换容量≥672Gbps，包转发率≥171Mpps，以官网所列最低参数为准，提供官网清晰截图及链接证明； 2. ≥28 个 10/100/1000Base-T 以太网端口，≥8 个万兆 SFP+，提供设备官网截图和链接证明； ▲3. CPU 和 LSW 要求国产化，提供国产测试报告 ▲4. 支持硬件 BFD，支持 BFD 3ms 最小探测间隔，提供封面具备 CMA 或 CNAS 标识的检测报告复印件证明 5. 支持 IPv4 静态路由、RIP、OSPF 6. 支持 IPv6 静态路由、OSPFv3 及加密 7. 支持 SP、WRR 等队列调度方式 三年质保 型号：S5130S-36S-EI-G	6	10000.00	60000.00	
5	内网核心交换机（国产）	新华三	规格： 采用国产化芯片 交换容量≥76.8Tbps，包转发率≥57600Mpps，若官网存在两个指标，以官网所列最低参数为准； 配置冗余主控，冗余电源，≥72 千兆电口≥20 千兆光口≥4 万兆光口，≥6 个业务槽位 ▲支持 FW 防火墙和 IPS 防火墙业务卡，提供第三方测试报告； 支持横向虚拟化技术，具备四虚一	1	60000.00	60000.00	

			<p>支持 16 条 40G 堆叠链路，堆叠带宽能达到双向 1.28T，提供第三方测试报告；</p> <p>支持 VxLAN ，能够实现基于 IPv4/IPv6 的 VxLAN 二三层互通（包括分布式网关或集中式网关），支持 VxLAN OAM ping 和 tracert，提供第三方测试报告；</p> <p>支持融合 AC 功能，无需额外配置单独硬件，在交换机上实现对 AP 的接入控制和管理，有线无线用户的统一认证管理，提供第三方测试报告；</p> <p>▲支持内置智能图形化管理功能，对于下联设备具备统一管理的功能，能够通过图形化界面对组内设备进行配置文件一键下发，对拓扑内的设备或设备组批量进行版本升级，提供第三方测试报告；</p> <p>型号：S7506X-G</p>				
6	外网核心交换机（国产）	新华三	<p>规格：</p> <p>采用国产化芯片</p> <p>交换容量≥76.8Tbps，包转发率≥57600Mpps，若官网存在两个指标，以官网所列最低参数为准；</p> <p>配置冗余主控，冗余电源，≥72 千兆电口≥20 千兆光口≥4 万兆光口，≥6 个业务槽位</p> <p>▲支持 FW 防火墙和 IPS 防火墙业务卡，提供第三方测试报告；</p> <p>支持横向虚拟化技术，具备四虚一</p> <p>支持 16 条 40G 堆叠链路，堆叠带宽能</p>	1	60000.00	60000.00	



			<p>达到双向 1.28T, 提供第三方测试报告;</p> <p>支持 VxLAN, 能够实现基于 IPv4/IPv6 的 VxLAN 二三层互通 (包括分布式网关或集中式网关), 支持 VxLAN OAM ping 和 tracert, 提供第三方测试报告;</p> <p>支持融合 AC 功能, 无需额外配置单独硬件, 在交换机上实现对 AP 的接入控制和管理, 有线无线用户的统一认证管理, 提供第三方测试报告;</p> <p>▲支持内置智能图形化管理功能, 对于下联设备具备统一管理的功能, 能够通过图形化界面对组内设备进行配置文件一键下发, 对拓扑内的设备或设备组批量进行版本升级, 提供第三方测试报告;</p> <p>型号: S7506X-G</p>				
7	48 口交换机 (国产)	新华三	<p>规格:</p> <p>采用国产化芯片</p> <p>交换容量<math>\geq</math>672Gbps, 转发性能<math>\geq</math>207Mpps, 提供官网截图证明</p> <p><math>\geq</math>48 个 10/100/1000Base-T 自适应以太网接口, 6 个万兆 SFP+接口, 左右通风</p> <p>支持静态路由, RIP, RIPng, OSPF, 等价路由, VRRP/VRRPv3</p> <p>支持集群或堆叠多虚一技术 (4 台), 实现单一界面管理多台设备</p> <p>支持 6 个万兆口堆叠</p> <p>支持 ECA (加密流量分析)</p>	4	15500.00	62000.00	

			VOQ 功能 CPU 保护 所有端口线速转发 端口平均时延小于 2us 硬件 BFD 3ms 最小间隔 型号: S5130S-54S-EI-G				
8	专网交换机 (国产)	新华三	规格: 采用国产化芯片 交换容量 $\geq 248\text{Gbps}$ , 转发性能 $\geq 120\text{Mpps}$ , 提供官网截图证明 主控转发合一 端口 $\geq 8*10\text{GE}$ 且 $\geq 29*1\text{GE}$ 支持静态路由, RIP, RIPng, OSPF, 等价路由, VRRP/VRRPv3 支持虚拟化特性, 将物理上两台设备虚拟化成一台逻辑设备, 提供第三方机构的测试报告 支持在一个物理网络上实现多个逻辑拓扑, 指定不同业务流量走不同的逻辑拓扑路由转发, 提供第三方机构的测试报告 随流检测技术, 提供第三方机构的测试报告 支持记录终端用户访问互联网的日志, 包括: 用户名、源/目的 IP 地址、时间、访问的域名、URL 等, 提供第三方机构的测试报告 型号: MSR3600-28-G	1	30500.00	30500.00	
9	信息系统安全等级保护测评	安信	规格: 等保二级, 根据国家网络安全等级保护相关标准, 实施方对信息系	2	50000.00	100000.00	

			统安全等级保护测评，并出具该系统的等级保护测评报告。 型号：定制				
10	等保一体机（信创设备）	迪普	规格： 高度 2U，千兆电口≥8 个，USB 接口≥2 个，Console 口≥1 个，扩展槽≥3 个；硬盘≥4T；内存≥96G，350W 冗余电源； 首页支持查看账号、产品、方案、待办事项等项目的数量信息，同时能以列表形式展示月订单、待办事项、账户明细等信息 一、安全运营： 支持风险资产 TOP5、攻击源地区 TOP5、攻击类型 T05 等信息的图表化呈现，进行不同安全级别的综合判定 二、报表中心 支持以自定义周期方式生成综合分析报表和资源运行报表，报表内容可自定义，其中综合分析报表包括安全分析、资产分析、告警分析等内容，资源运行报表包括资源使用情况、运行情况等内容 三、日志中心 1) 支持提供包括下一代防火墙、Web 应用防火墙、堡垒机、数据库审计、日志审计等安全组件的日志展示界面 一、资源管理 可查看等保一体机所有安全组件的在线/离线状态，cpu、内存、磁盘使用率，流入带宽趋势、流出带宽趋势等	1	155000.00	155000.00	

			<p>信息</p> <p>二、组件管理</p> <p>1) 支持对安全组件进行全生命周期管理，包括安全模块创建、开机、扩容、重启、关机、删除等操作</p> <p>2) 支持安全组件的流量编排，可按需对流量的来源与目标节点进行策略配置，实现安全模块先后顺序与是否启用的灵活调整</p> <p>一、监控可视化</p> <p>支持提供监控概览页面，直观呈现组件数量、总 CPU 核数与使用率、总内存与使用率、总磁盘空间与使用率等信息</p> <p>二、智能告警</p> <p>1) 支持告警列表展示，内容至少包括告警时间、告警规则、告警类型、告警等级、区域等内容，并能按照区域、告警类型、告警等级进行筛选与批量删除等操作</p> <p>三、网络拓扑</p> <p>1) 支持以拖拽的方式进行拓扑的编辑与展示，内置多种拓扑模板</p> <p>2) 支持拓扑的导入与导出，支持格式至少包括 PNG、Json 文件</p> <p>1) 支持防护资产列表展示，根据资产状态划分为高风险、中风险、低风险、比较安全，根据资产价值划分为核心、重要、一般、边缘、未知</p> <p>2) 支持对安全组件进行策略分析，策略分析内容包括隐藏策略、冗余策</p>				
--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			<p>略、过期策略、合并策略、未命中策略</p> <p>1) 支持三权分立</p> <p>2) 支持创建平台角色，并对角色的菜单权限与操作权限进行自定义设置</p> <p>3) 支持平台操作审计，对用户名称、IP、操作内容、操作结果、时间等进行展示与查询，并支持操作日志的导出</p> <p>▲1) 平台内的虚拟磁盘支持内核级 I/O 加速，将虚拟磁盘的 I/O 驱动从用户态迁移到内核态，支持异步 I/O 加速功能（提供具备 CNAS 标识的第三方检测报告）</p> <p>▲2) 平台支持 B/S 和 C/S 两种架构的安全虚拟机控制台，且 C/S 客户端无任何授权限制，支持将本地文件拖拉拽到安全虚拟机内部且支持和本地共享粘贴板（提供具备 CNAS 标识的第三方检测报告）</p> <p>▲3) 平台具备数据中心全局服务器损坏恢复能力，数据中心内服务器发生不可恢复灾难时，通过存储池容灾功能即可立即恢复对应业务虚拟机（提供具备 CNAS 标识的第三方检测报告）</p> <p>▲4) 平台支持对接远端存储时，可配置对接存储的 IP 以及端口号、是否启用 iSER 协议，为保护数据安全，可支持单向和双向验证 CHAP 身份信息（提供具备 CNAS 标识的第三方检测报告）</p>				
--	--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

			<p>▲5) 平台支持配置和一键部署大数据集群,快速提供大数据集群服务,管理平台支持以大数据镜像方式创建 manager 和 worker 节点,并支持配置大数据服务 CPU、内存、磁盘规格和磁盘数量(提供具备 CNAS 标识的第三方检测报告)</p> <p>1) 具备公安部第三研究所颁发的《云应用安全可信认证》</p> <p>▲2) 具备与飞腾、鲲鹏、海光芯片的兼容性证明</p> <p>▲5) 具备与麒麟操作系统的兼容性证明</p> <p>型号: CSSMP-BSS-GA-HG+LIC1</p>				
投标报价(小写)			1842500.00				
投标报价(大写)			壹佰捌拾肆万贰仟伍佰元整				

注:

1、投标人需按本表格式填写,否则视为投标文件含有采购人不能接受的附加条件,投标无效。

2、有关本项目实施所涉及的一切费用均计入报价。采购人将以合同形式有偿取得货物或服务,不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务,不得出现“0元”“免费赠送”等形式的无偿报价,否则视为投标文件含有采购人不能接受的附加条件,投标无效;采购内容未包含在《开标一览表(报价表)》名称栏中,投标人不能作出合理解释的,视为投标文件含有采购人不能接受的附加条件的,投标无效。

3、特别提示：采购代理机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的名称、品牌（如果有）、规格型号、数量、单价等予以公示。

4、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

## 附：报价明细表

### 标项二报价表

#### 一、招标项目清单

第一部分：网络安全技术服务部分				
序号	服务项目	服务年限	型号和规格（或具体服务）	分项报价
1	安全咨询与规划服务	3	<p>服务描述： 依据等级保护 2.0 相关标准，结合绍兴市公共交通集团有限公司信息系统具体情况，建立完整的信息安全管理体系，达到动态的、系统的、制定化的、以预防为主的信息管理方式，用最低的成本，达到可接受的信息安全水平，最大限度保证业务的持续性。</p> <p>服务方式：现场/远程</p> <p>服务范围：绍兴市公共交通集团及下属单位</p> <p>服务频率：1 次</p> <p>服务输出：《安全规划方案》</p>	60000.00



2	漏洞分析与加固服务	3	<p>服务描述： 网络安全讲一百遍不如打一遍，实战化是检验网络安全防护能力的唯一标准。一个漏洞的存在给业务系统带来的危害是致命的，不可想象的。漏洞被利用导致的信息安全事件不胜枚举，轻者业务系统运行缓慢和中断，重则敏感数据泄露或丢失。发现高（中）风险问题后，涉及到相关业务系统的提出加固整改建议。</p> <p>服务内容：</p> <p>1) 安全漏洞检测：如操作系统、中间件、B/S 业务系统、数据库等漏洞；</p> <p>2) 业务逻辑漏洞检测：如后台登录处存在逻辑错误，登陆时没有错误次数限制用户登录，并且没有判断验证码过期，导致验证码可以重复使用，可被爆破用户名密码或撞库；</p> <p>3) Webshell 检测：如网页后门程序、线程插入后门程序、扩展后门程序；</p> <p>4) 弱口令核查，复用口令核查。</p> <p>服务人数：2 人</p> <p>服务方式：现场</p> <p>服务对象：绍兴市公共交通集团重要信息系统</p> <p>服务频率：2 次/年</p>	60000.00
---	-----------	---	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------

		<p>服务输出：《漏洞评估报告》</p> <p>工具要求：</p> <p>支持检测的漏洞数大于 230000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准。</p> <p>支持国产操作系统的漏洞扫描，包括麒麟（Kylin）、统信（UnionTech OS）、中兴新节点（NewStart CGSL）等。</p> <p>支持操作系统、网络设备、数据库、中间件等漏洞扫描。</p> <p>支持采用 SMB、RDP、Telnet、SSH 等协议对系统进行登录扫描。</p> <p>支持全面扫描、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，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。</p> <p>提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。</p> <p>产品支持对系统漏洞、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。</p>	
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

3	应急演练服务（桌面推演）2个演练剧本	3	<p>服务描述： 网络安全应急演练服务覆盖演练准备工作、演练环境搭建、演练剧本编写、演练彩排工作、正式演练大会活动、应急演练总结等各个阶段，帮助绍兴市公共交通集团实现全面有效的应急演练。通过应急演练工作，进一步明确各应急小组在应急响应工作中的职责，熟悉掌握应急响应的处置程序、方法和注意事项，有效提高绍兴市公共交通集团整体应急响应的反应能力、指挥水平和实战能力，增强各部门应急人员之间的协调性，检验单位应急救援预案的可行性和可操作性，使其达到应急演练的预期效果。</p> <p>服务方式：现场演练</p> <p>服务范围：绍兴市公共交通集团及下属单位</p> <p>服务频率：1次</p> <p>演练脚本：2个</p> <p>服务输出：《应急演练方案》、《应急演练总结报告》</p>	120000.00
4	应急响应与溯源服务	3	<p>工作内容： 在发生确切的网络安全事件时，应急响应实施人员应及时采取行动，限制事件扩散和影响的范围，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件解决方案，追查事件来源，协助后续处置。</p>	120000.00

			<p>服务人数：2人</p> <p>服务方式：现场或远程</p> <p>服务对象：绍兴市公共交通集团重要信息系统</p> <p>服务频率：按需响应，不限次数</p> <p>时间要求：不限次数。1小时内抵达客户现场，2小时内定位问题，4小时内控制风险、事件。</p> <p>服务输出：《应急响应处置报告》</p>	
--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------	--

第二部分：网络维护服务部分

序号	服务项目	服务年限	型号和规格（或具体服务）	分项报价
1	集团机房日常网络系统维护（机房及服务器及网络系统等信息化系统）	3	<p><b>基础设施管理：</b>1. 确保网络通信传输畅通。2. 负责网络布线架的管理，确保配线的合理有序。3. 掌握客户端设备接入网络情况，以便+发现问题可迅速定位。4. 采取技术措施，对网络内经常出现的用户需要变更位置和部门的情况进行管理。5. 掌握与外部的链接配置，监督网络通信状况，发现问题后与有关机构及时联系。6. 实时监控局域网络的运行河网络通信情况；</p> <p><b>应用系统管理：</b>1. 确保各种网络应用服务运行的不间断性和工作性能的良好性。出现故障时应将造成的损失和影响控制在最小范围；2. 对于要求不可中断</p>	300000.00

			<p>的关键型网络应用系统，除了在软件手段上要掌握，备份系统参数和定期备份系统、业务数据外，必要时在硬件手段上要建立和配置系统的热备份；</p> <p><b>路由、局域网环境检查：</b>1. 测试到路由、交换机以及外部网络的连通性。2. 查看所有路由、交换机端口以及状态灯的工作状态，保证设备工作正常。3. 检查网关设备（防火墙、路由）工作状态，确保外网连接正常。4. 检查网络线缆，确保网络线缆完好无损</p> <p>相关资质：中标后提供机房安全设备（防火墙等）维护授权资质</p>	
<b>第三部分：一网统管部分</b>				
序号	设备项目	单位	型号和规格（或具体服务）	分项报价
1	一网通智能监控平台（国产软件）	1	<p>总体要求：产品架构支持中台+微应用架构，支持运维运营化管理，支持扩展为整个多产品的支持服务平台，根据安全原则，系统用户权限定义原生支持三员分立</p> <p>CMDB：▲可自定义不同业务资源主题，覆盖全运维领域，包括监控、IoT、自动化、资产、视频、DevOps，不同业务主题可通过各自视图查看模型（要求提供功能截图）</p>	390000.00

		<p>▲提供配置项（CI 项）的变更历史查询，可查看原配置项变更到新值的全历史记录，包括变化时间、变更人属性值。（要求提供功能截图）</p> <p>运维场景自动化管理：编排语句采取拖拽式、自然语言语句编排</p> <p>▲提供多种种触发执行场景的能力，包括周期执行、告警驱动、手工执行、指标驱动执行。通过指标驱动执行，可以将场景实现的统计指标作为指标，应用到告警、历史记录、自定义首页部分。（要求提供功能截图）</p> <p>告警管理：▲提供告警信息所属的事件标签分类，并标识出告警持续时间显示，对手工撤销告警的操作，要求标注和展示手工撤销理由、撤销人信息。（要求提供功能截图）</p> <p>支持屏幕颜色告警、告警邮件提醒、和短信猫告警、企业微信、钉钉机器人、数据库输出。</p> <p>报表管理：支持多个不同指标在同一时间轴中进行对比分析；支持历史记录任意时段拖拽查看，对于超过 3 个月的历史数据，支持原始采集颗粒度（5 分钟）的对比分析。</p> <p>主机管理：支持系统拓扑图，一张图可以展现所有主机承载的数据库、中间件和标准应用之间的实时状态监控，为主机监控提供全景视图。</p>	
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		<p>▲提供操作系统的 CPU、内存、流量、存储进行涨势分析，主动识别涨势过快的设备。（要求提供功能截图）</p> <p>支持 IPMI 方式监控主流国产服务器厂商的硬件，监控内容包括温度、电源、风扇、电压等硬件状态；</p> <p>数据库管理：支持 ODBC 和 JDBC 取数方式取数，对 SQLServer、Oracle、Sybase、Mysql、Informix、DB2、神通、瀚高等数据库的各项运行参数进行监控；</p> <p>支持对于各个数据库实时运行状态的实时统计，包含数据库会话数、死锁数实时排行，支持对表空间大小和会话数、缓存信息、锁信息进行重点监管。</p> <p>支持 Oracle Rac 的管理，支持集群分成操作系统、clusterware、实例方式展现，支持动态数据对比，检测各个承载主机的性能表现</p> <p>中间件管理：中间件管理必须支持对 WEBLogic、Tuxedo、WebSphere、EAServer、Cognos、MQ、Apache、Tomcat、Jboss、IIS、TongWeb、中创、TAS 等中间件实时监控。</p> <p>支持图形化方式显示应用的承载主机状态和应用的基本性能信息，同时展示相关的运维负责人和联系方式。</p>	
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		<p>标准应用管理：支持 FTP、SFTP、HTTP、HTTPS、POP3、SMTP、DHCP、JVM、Exchange 的监控。</p> <p>网络管理：系统能支持各大设备厂商的各型号设备，支持多厂商设备组成的混合网络自动发现。拓扑图的生成必须支持网络设备的 SNMP V1、V2、V3 这三个版本的混和生成，并能对 SNMP V3 设备进行管理；要求在拓扑图上快速定位 IP 地址的接入端口，包括服务器 IP 和 PC 机 IP，并且通过图标进行显示。拓扑图设备间的连线除直线形式外，还可支持以折线、合并线等线型，并可将网络拓扑按照线路图、地域分布图、逻辑关系图等方式呈现；拓扑图线路支持带有流动效果方式展现，支持定义虚实线、粗细、速度等线形设置。；支持在拓扑图上直接调用 webssh 工具，访问设备和主机。允许保存上一次登陆使用账号密码。支持查询接入 IP 的历史变更情况查询。支持异常接入终端的告警通知，可以针对未规划设备、未分配 IP、未在指定位置接入等多种异常进行自动检测。支持网络拓扑中快速定位 PC，并以下标方式显示其使用人信息</p> <p>虚拟化管理：实现宿主机配置、状态、性能信息的一体化管理。实现虚拟机配置、状态、性能信息的一体化管理。要求以图形化方式展现虚拟化拓扑，显示宿主机、虚拟机、虚拟网络、数据存储关系，动态显示管理对象负载、告警。</p>	
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--



			<p>存储管理：支持存储设备硬件管理，以统一的视图展现被管的各个硬件子项的运行详情，清晰展现各个管理设备的各类型管理状态，并以颜色显著标示出现问题的硬件类型；涉及到磁盘阵列的电源、电池、风扇、温度、磁盘、控制器等各个关键硬件信息；支持存储设备性能管理，提供 LUN 读 IOPS TOP 排行；提供 LUN 写 IOPS TOP 排行；提供 LUN 总 IOPS TOP 排行；提供 LUN 的总传输字节数 TOP 排行；提供按照传输流量的存储线路排行</p> <p>知识库管理：支持自定义知识库的分类。新增知识时，支持对知识设置共享范围，公有知识对所有人可见，私有知识可按人员选定。对于非知识库管理员提交的知识有知识库的审核功能。知识库可在各服务管理流程中被直接引用，支持知识的引用次数统计。</p>	
2	内外专网终端防非法外联技术参数 (国产设备)	1	<p>性能要求：网络层吞吐量（大包）：≥3Gb，带宽性能：≥250Mb，新建连接数：≥30000，最大并发连接数：2000000。</p> <p>硬件要求：规格：≥1U，内存大小：≥8G，硬盘容量：≥500G HDD，电源：单电源，接口：≥4 千兆电口，≥2 个 combo 口。</p> <p>特征库数量：产品支持应用特征库数量不低于 7100+，提供产品界面截图</p> <p>精细化控制：支持用户上网应用的精细化控制，例如微信的：“微信”“微信语音”“微信发消息”“微信收消息”“微信登录”“微信发文件”“微信收</p>	85000.00

			<p>文件”并提供 web 配置截图</p> <p>支持移动终端发现管理，可一键添加为信任终端、发现终端后可邮件告警/冻结等，支持趋势图呈现移动终端接入趋势及列表详情等</p> <p>▲用户画像：支持用户虚拟身份画像，以时间轴的形式展示用户上网行为轨迹；支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如 QQ 号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息，支持对单用户进行网站访问质量检测，提供 web 界面截图（提供第三方测试报告证明，并加盖 CNAS 章）</p> <p>文件缓存：支持文件缓存，支持安卓和 IOS 形式的文件，主动缓存文件形式包含 APP 应用等，提供 web 配置截图</p> <p>资产梳理：支持对内网资产的 IP、用户、部门、操作系统、重要程度、可用服务、是否可信进行统一梳理，发现问题资产支持阻断 IP，提供产品截图</p>	
3	内外网专网 政务网及一 公司防火墙	3	<p>性能要求：网络层吞吐量：≥6Gbps。TCP 新建连接速率：≥200w。TCP 并发连接数：≥5w。</p> <p>硬件要求：≥4 个千兆电口和 4 个千兆光口，冗余电源，≥2 个扩展槽位</p> <p>NAT 功能：支持 NAT44、NAT46、NAT64、NAT66</p>	180000.00

	(国产设备)	<p>VPN：可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阈值进行细颗粒度的管控。（提供功能截图）</p> <p>支持 IPsec VPN 智能选路，根据隧道质量调度流量。（提供功能截图）</p> <p>应用识别：支持至少 9000 条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。（提供截图）</p> <p>安全策略：支持基于域名的安全策略模糊匹配（提供功能截图）</p> <p>支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图）</p> <p>加密流量检测：支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供截图）</p> <p>▲虚拟化能力：所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功</p>	
--	--------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

			<p>能要求提供功能截图</p> <p>支持 Context+VRF 二级虚拟化技术，支持 CPU、内存、存储等硬件资源划分的完全虚拟化</p> <p>支持 vSys 虚拟防火墙技术，可以将一台物理设备虚拟成 N 台相互独立的虚拟设备</p> <p>产品资质：所投产品须具备国芯证明材料</p> <p>具备中国网络安全审查技术与认证中心颁发的 EAL4 增强级认证证书</p>	
4	流控交换机 (国产设备)	6	<p>1. 交换容量<math>\geq 672\text{Gbps}</math>，包转发率<math>\geq 171\text{Mpps}</math>，以官网所列最低参数为准，提供官网清晰截图及链接证明；</p> <p>2. <math>\geq 28</math> 个 10/100/1000Base-T 以太网端口，<math>\geq 8</math> 个万兆 SFP+，提供设备官网截图和链接证明；</p> <p>▲3. CPU 和 LSW 要求国产化，提供国产测试报告</p> <p>▲4. 支持硬件 BFD，支持 BFD 3ms 最小探测间隔，提供封面具备 CMA 或 CNAS 标识的检测报告复印件证明</p> <p>5. 支持 IPv4 静态路由、RIP、OSPF</p> <p>6. 支持 IPv6 静态路由、OSPFv3 及加密</p> <p>7. 支持 SP、WRR 等队列调度方式</p>	60000.00

			三年质保	
6	内网核心交换机（国产）	1	<p>采用国产化芯片</p> <p>交换容量<math>\geq 76.8\text{Tbps}</math>，包转发率<math>\geq 57600\text{Mpps}</math>，若官网存在两个指标，以官网所列最低参数为准；</p> <p>配置冗余主控，冗余电源，<math>\geq 72</math> 千兆电口<math>\geq 20</math> 千兆光口<math>\geq 4</math> 万兆光口，<math>\geq 6</math> 个业务槽位</p> <p>▲支持 FW 防火墙和 IPS 防火墙业务卡，提供第三方测试报告；</p> <p>支持横向虚拟化技术，具备四虚一</p> <p>支持 16 条 40G 堆叠链路，堆叠带宽能达到双向 1.28T，提供第三方测试报告；</p> <p>支持 VxLAN ，能够实现基于 IPv4/IPv6 的 VxLAN 二三层互通（包括分布式网关或集中式网关），支持 VxLAN OAM ping 和 tracert，提供第三方测试报告；</p> <p>支持融合 AC 功能，无需额外配置单独硬件，在交换机上实现对 AP 的接入控制和管理，有线无线用户的统一认证管理，提供第三方测试报告；</p> <p>▲支持内置智能图形化管理功能，对于下联设备具备统一管理的功能，能够通过图形化界面对组内设备进行配置文件一键下发，对拓扑内的设备或设备组批量进行版本升级，提供第三方测试报告；</p>	60000.00

7	外网核心交换机（国产）	1	<p>采用国产化芯片</p> <p>交换容量<math>\geq 76.8</math>Tbps，包转发率<math>\geq 57600</math>Mpps，若官网存在两个指标，以官网所列最低参数为准；</p> <p>配置冗余主控，冗余电源，<math>\geq 24</math>千兆电口<math>\geq 20</math>千兆光口<math>\geq 4</math>万兆光口，<math>\geq 6</math>个业务槽位</p> <p>▲支持FW防火墙和IPS防火墙业务卡，提供第三方测试报告；</p> <p>支持横向虚拟化技术，具备四虚一</p> <p>支持16条40G堆叠链路，堆叠带宽能达到双向1.28T，提供第三方测试报告；</p> <p>支持VxLAN，能够实现基于IPv4/IPv6的VxLAN二三层互通（包括分布式网关或集中式网关），支持VxLAN OAM ping和tracert，提供第三方测试报告；</p> <p>支持融合AC功能，无需额外配置单独硬件，在交换机上实现对AP的接入控制和管理，有线无线用户的统一认证管理，提供第三方测试报告；</p> <p>▲支持内置智能图形化管理功能，对于下联设备具备统一管理的功能，能够通过图形化界面对组内设备进行配置文件一键下发，对拓扑内的设备或设备组批量进行版本升级，提供第三方测试报告；</p>	60000.00
8	48口交换机（国产）	4	<p>采用国产化芯片</p> <p>交换容量<math>\geq 672</math>Gbps，转发性能<math>\geq 207</math>Mpps，提供官网截图证明</p>	62000.00

			<p>≥48 个 10/100/1000Base-T 自适应以太网接口，6 个万兆 SFP+接口，左右通风</p> <p>支持静态路由，RIP，RIPng,OSPF,等价路由,VRRP/VRRPv3</p> <p>支持集群或堆叠多虚一技术（4 台），实现单一界面管理多台设备</p> <p>支持 6 个万兆口堆叠</p> <p>支持 ECA(加密流量分析)</p> <p>VOQ 功能</p> <p>CPU 保护</p> <p>所有端口线速转发</p> <p>端口平均时延小于 2us</p> <p>硬件 BFD 3ms 最小间隔</p>	
9	专网交换机 (国产)	1	<p>采用国产化芯片</p> <p>交换容量≥≥248Gbps，转发性能≥120Mpps，提供官网截图证明</p> <p>主控转发合一</p> <p>端口≥ 8*10GE 且 ≥ 29*GE 电</p> <p>支持静态路由，RIP，RIPng,OSPF,等价路由,VRRP/VRRPv3</p> <p>支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备，提供第三方机构的测试报告</p>	30500.00

			<p>支持在一个物理网络上实现多个逻辑拓扑，指定不同业务流量走不同的逻辑拓扑路由转发，提供第三方机构的测试报告</p> <p>随流检测技术，提供第三方机构的测试报告</p> <p>支持记录终端用户访问互联网的日志，包括：用户名、源/目的 IP 地址、时间、访问的域名、URL 等，提供第三方机构的测试报告</p>	
8	信息系统安全等级保护测评	2	<p>等保二级，根据国家网络安全等级保护相关标准，实施方对信息系统安全等级保护测评，并出具该系统的等级保护测评报告。</p>	100000.00
9	等保一体机（国产设备）	1	<p>高度 2U，千兆电口<math>\geq</math>8 个，USB 接口<math>\geq</math>2 个，Console 口<math>\geq</math>1 个，扩展槽<math>\geq</math>3 个；硬盘<math>\geq</math>4T；内存<math>\geq</math>96G，350W 冗余电源；</p> <p>首页支持查看账号、产品、方案、待办事项等项目的数量信息，同时能以列表形式展示月订单、待办事项、账户明细等信息</p> <p>一、安全运营：</p> <p>支持风险资产 TOP5、攻击源地区 TOP5、攻击类型 T05 等信息的图表化呈现，进行不同安全级别的综合判定</p> <p>二、报表中心</p> <p>支持以自定义周期方式生成综合分析报表和资源运行报表，报表内容可自定</p>	155000.00



		<p>义，其中综合分析报表包括安全分析、资产分析、告警分析等内容，资源运行报表包括资源使用情况、运行情况等内容</p> <p>三、日志中心</p> <p>1) 支持提供包括下一代防火墙、Web 应用防火墙、堡垒机、数据库审计、日志审计等安全组件的日志展示界面</p> <p>一、资源管理</p> <p>可查看等保一体机所有安全组件的在线/离线状态，cpu、内存、磁盘使用率，流入带宽趋势、流出带宽趋势等信息</p> <p>二、组件管理</p> <p>1) 支持对安全组件进行全生命周期管理，包括安全模块创建、开机、扩容、重启、关机、删除等操作</p> <p>2) 支持安全组件的流量编排，可按需对流量的来源与目标节点进行策略配置，实现安全模块先后顺序与是否启用的灵活调整</p> <p>一、监控可视化</p> <p>支持提供监控概览页面，直观呈现组件数量、总 CPU 核数与使用率、总内存与使用率、总磁盘空间与使用率等信息</p> <p>二、智能告警</p>	
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		<p>1) 支持告警列表展示，内容至少包括告警时间、告警规则、告警类型、告警等级、区域等内容，并能按照区域、告警类型、告警等级进行筛选与批量删除等操作</p> <p>三、网络拓扑</p> <p>1) 支持以拖拽的方式进行拓扑的编辑与展示，内置多种拓扑模板</p> <p>2) 支持拓扑的导入与导出，支持格式至少包括 PNG、Json 文件</p> <p>1) 支持防护资产列表展示，根据资产状态划分为高风险、中风险、低风险、比较安全，根据资产价值划分为核心、重要、一般、边缘、未知</p> <p>2) 支持对安全组件进行策略分析，策略分析内容包括隐藏策略、冗余策略、过期策略、合并策略、未命中策略</p> <p>1) 支持三权分立</p> <p>2) 支持创建平台角色，并对角色的菜单权限与操作权限进行自定义设置</p> <p>3) 支持平台操作审计，对用户名称、IP、操作内容、操作结果、时间等进行展示与查询，并支持操作日志的导出</p> <p>▲1) 平台内的虚拟磁盘支持内核级 I/O 加速，将虚拟磁盘的 I/O 驱动从用户态迁移到内核态，支持异步 I/O 加速功能（提供具备 CNAS 标识的第三方检测报告）</p>	
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		<p>▲2) 平台支持 B/S 和 C/S 两种架构的安全虚拟机控制台，且 C/S 客户端无任何授权限制，支持将本地文件托拉拽到安全虚拟机内部且支持和本地共享粘贴板（提供具备 CNAS 标识的第三方检测报告）</p> <p>▲3) 平台具备数据中心全局服务器损坏恢复能力，数据中心内服务器发生不可恢复灾难时，通过存储池容灾功能即可立即恢复对应业务虚拟机（提供具备 CNAS 标识的第三方检测报告）</p> <p>▲4) 平台支持对接远端存储时，可配置对接存储的 IP 以及端口号、是否启用 iSER 协议，为保护数据安全，可支持单向和双向验证 CHAP 身份信息（提供具备 CNAS 标识的第三方检测报告）</p> <p>▲5) 平台支持配置和一键部署大数据集群，快速提供大数据集群服务，管理平台支持以大数据镜像方式创建 manager 和 worker 节点，并支持配置大数据服务 CPU、内存、磁盘规格和磁盘数量（提供具备 CNAS 标识的第三方检测报告）</p> <p>1) 具备公安部第三研究所颁发的《云应用安全可信认证》</p> <p>▲2) 具备与飞腾、鲲鹏、海光芯片的兼容性证明</p> <p>▲5) 具备与麒麟操作系统的兼容性证明</p>	
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

注：

★1. 采购单位将根据以上附表中的报价与中标单位进行结算。如中标单位不遵守此项规则，采购单位在沟通无果的情况下有权立即终止合同，并由中标单位承担期间产生的全部费用。

## 二、中小企业声明函

无