**本询价文件经我方审核确认，同意按此发布。**

**采购人代表签字：**

**询 价 文 件**

**招标编号: PTXX2021033**

**项目名称:信息安全管理与评估实训系统采购项目**

**采购人: 湄洲湾职业技术学院（盖章）**

**招标代理人:** **福建莆田兴鑫招标代理有限公司(盖章）**

**二○二一年十二月**

**目 录**

一、询价公告

二、报价人须知

三、招标内容及要求

四、合同文本

五、报价文件（格式）

**第一部分 询价公告**

**[福建莆田兴鑫招标代理有限公司]**受**[湄洲湾职业技术学院]**委托，对下列所述货物以**询价采购**方式进行招标，现欢迎国内合格的意向报价人前来提交密封的报价。

**1、项目编号：**PTXX2021033

**2、项目内容：**信息安全管理与评估实训系统采购项目

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **合同包** | **项目名称** | **数量** | **详细要求** | **最高限价（元）** |
| 1 | 信息安全管理与评估实训系统采购项目 | 1项 | 详见第三章招标内容及要求 | 489815.00 |
| **1.合同签订时间：**中标通知书发出后3个工作日内签订合同。  **2.交货地点：**按招标人指定地点。  **3.交货期：**中标方在合同签订后3天内完成。  **4.付款方式：**全部货物交货、安装调试正常并经验收合格后支付95%，在验收合格之日满一年后且未发现质量问题无合同未了事宜后支付剩余5%。 | | | | |

**备注：本次询价采购设最高限价，超过最高限价的报价将被拒绝。**

**3、确定成交供应商方法：**采用最低价法。

**4、资格要求：**

1）投标人须在中国境内注册并具有独立法人资格，提供**三证合一的企业法人营业执照复印件并加盖公章**。

2）投标代表必须经投标人的法定代表人关于参与本项目投标的授权，请提供法定代表人授权投标代表的授权委托书原件(投标代表是法定代表人无需)，法定代表人和投标代表的身份证复印件。

3）**需提供无行贿犯罪记录承诺（说明）函（供应商自行对其有无行贿犯罪情形进行说明或承诺，格式自拟）**

4）本次招标不允许联合体进行投标。

5）投标人参加本次投标的前三年内，在经营活动中没有重大违法记录书面承诺函。

**5、报名方式及标书费：**

5.1上门报名：即供应商直接到我司购买招标文件。

5.2邮寄方式报名：即投标人先将标书费和邮购费转账或电汇至我司指定账户，再将转账或电汇的银行回单、报名人全称、地址、电话、传真、联系人、手机、E-mail、报名项目编号、项目名称等传真至我司，我司再将招标文件通过快递和发电子邮件方式寄给报名人。

5.3询价文件售价为100元/份(含电子文档)，邮购费50元，本招标代理公司不对邮寄过程中可能发生的延误或丢失负责，本文件售后不退。

**6、时间安排、地点：**

（1）报名时间：2021年12月2日至2021年12月7日（节假日及公休日除外）上午08：00—12：00，下午14：30—17：30（北京时间，以下同）；

（2）报价文件递交截止时间和报价时间：2021年12月8日下午15：00时；逾期收到的或不符合规定的报价文件将被拒绝，并将其原封不动地退回报价人。

（3）报价地点：莆田市城厢区龙桥街道东园西路1133号西山小区A区2号楼9梯323室，投标文件由招标代理人的工作人员接收。

**7、投标保证金：**投标保证金为**合同包一：人民币肆仟捌佰元整（￥4800元）；**投标保证金以转账或电汇形式提交，不直接接受现金或汇票，以投标文件递交截止时间前到帐为准。

**8、指定帐户**：

（1）**投标保证金缴纳帐户**：开户名--福建莆田兴鑫招标代理有限公司，开户行—中国邮政储蓄银行股份有限公司莆田市城厢区支行，帐号—935002010016936699。

（2）**标书工本费、中标服务费缴纳帐户**：开户名--福建莆田兴鑫招标代理有限公司，开户行—招商银行股份有限公司莆田分行，帐号—6232625940080501。

**9、本批采购确定成交人的办法：**

采取最低评标价法确定成交供应商。即在全部满足文件实质性要求前提下，依据统一的价格要素评定最低报价，以提出最低报价的报价人作为成交供应商。若出现报价相同的，则按服务要求高低及售后服务优劣的顺序推荐成交供应商。

**10、**意向报价人对本次询价活动事项提出疑问的，请在报价截止时间3日之前， 以信函或传真的形式与招标代理人联系。

**11、**我司将在中国政府采购网和福建招标采购网上发布本项目的询价公告、更改通知、答疑纪要、评标结果等信息，请意向报价人及时关注，意向报价人若没有在以上网站上查询相关更改通知和答疑纪要等信息而影响报价的，意向报价人自行承担相关责任。

**12、采购单位和招标代理机构的名称和地址**

(1) 采购人：湄洲湾职业技术学院

联系人\电话：陈老师\15960752583

(2) 招标代理人：福建莆田兴鑫招标代理有限公司

地址：莆田市城厢区龙桥街道东园西路1133号西山小区A区2号楼9梯323室

联系人：小陈

电话：18030342382

公司邮箱：xxzb2020@126.com

**第二部分 报价人须知**

|  |  |
| --- | --- |
| **项号** | **编 列 内 容** |
| 1 | **项目名称：**信息安全管理与评估实训系统采购项目  **招标人名称：**湄洲湾职业技术学院  **项目内容：**第三部分《采购内容及技术要求》  **项目编号：**PTXX2021033 |
| 2 | **资格标准：**  1）投标人须在中国境内注册并具有独立法人资格，提供**三证合一的企业法人营业执照复印件并加盖公章**。  2）投标代表必须经投标人的法定代表人关于参与本项目投标的授权，请提供法定代表人授权投标代表的授权委托书原件(投标代表是法定代表人无需)，法定代表人和投标代表的身份证复印件。  3）**需提供无行贿犯罪记录承诺（说明）函（供应商自行对其有无行贿犯罪情形进行说明或承诺，格式自拟）。**  4）本次招标不允许联合体进行投标。  5）投标人参加本次投标的前三年内，在经营活动中没有重大违法记录书面承诺函。 |
| 3 | **确定成交供应商方法：采用最低价法**。 |
| 4 | **招标代理费：**  招标代理服务费由中标人在领取中标通知书的同时支付按中标价的1.5%向招标代理机构缴纳。  **代理费账户：**开户名--福建莆田兴鑫招标代理有限公司，开户行—招商银行股份有限公司莆田分行，帐号—6232625940080501。 |
| 5 | **项目监督部门：**采购人相关主管部门 |
| 6 | **报价文件份数：**按要求制作报价文件，统一用A4纸装订后（格式见第五部分），一正叁副本密封，报价文件的正本和副本必须用不褪色的墨水填写或打印，并注明“正本”和“副本”字样。正本、副本必须内容必须一致。 |
| 7 | **报价文件装订及封面：**报价文件装订胶装成册，封面应加盖报价人公章，并经报价人的法定代表人或其委托代理人签字或盖章。由委托代理人签字或盖章的报价文件中须同时提交报价文件签署授权委托书。报价文件必须按照询价文件的规定和要求签字、盖章。未经报价人法定代表人或未经法定代表人正式授权签署的报价人代表在“询价文件”要求的地方签字或加盖印章的报价文件，属无效文件，作无效处理。 |
| 8 | **报价文件外层密封袋的标注：**报价文件全部正副本报价文件整体密封成一袋。包封上应写明项目编号、项目名称、报价人名称、并注明“开标时启封”字样；所有包封口处应加盖报价人公章及由法定代表人盖章。如果报价人未按上述要求密封及加写标记，招标代理人对报价文件的误投和提前启封概不负责。 |
| 9 | **报价过程的纪律：**  1.报价开启之后，直至确定成交供应商为止，凡是属于审查的有关资料以及授标意向等，均不得向报价人或其他无关人员透露，对任何违反者均将按有关规定处理；  2.在报价期间，报价人企图影响招标人的任何活动，将导致报价被拒绝，并不予退还其保证金；  3.报价人不得串通报价。报价人和采购人不得相互勾结，以排挤其他报价人的公平竞争。任何单位和个人在报价活动中，不准以任何方式行贿受贿。违者由行政主管部门按有关法律、法规规定处理。  **4.报价截止时间结束后参加报价的报价人不足三家的，本次询价程序终止，除采购任务取消情形外，采购单位将依法重新组织询价或者采取其他方式采购。**  5.成立询价采购小组，由采购人的代表和有关专家共3人以上的单数组成，采购小组人员必须遵循公平、公正原则进行评标，并接受监督。  6.询价。询价小组要求被询价的供应商一次报出不得更改的价格。  7.确定成交供应商。采购人根据符合采购需求、质量和服务相等且报价最低的原则确定成交供应商，并将结果通知所有被询价的未成交的供应商。 |

**第三部分 招标内容及技术要求**

**一、采购人：湄洲湾职业技术学院**

**二、采购项目名称：信息安全管理与评估实训系统采购项目**

**三、技术参数**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **技术指标及要求** | 数量 | 备注 |
| **1** | 虚拟化交换机 | 1. 1U高，固化10/100/1000M以太网电接口≥24个，固化SFP千兆光接口≥4个，固化SFP+万兆光接口≥4个，机身固化内置双AC电源 2. 机身支持Console口（RJ45）、带外管理口（MGMT端口，RJ45）、USB接口、Reset键 3. 满负荷情况下功耗≤30W 4. 要求设备1U高，深度≤330mm 5. 交换容量≥598Gbps，包转发率≥270Mpps 6. 支持RIP V1/2、RIPng、OSPF、OSPFv3、IS-IS、IS-ISv6、BGP、BGP4+ 7. 支持OpenFlow 8. 支持MPLS VPN 9. 支持虚拟化，优雅重启（GR），CPU安全防护； 10. 支持sflow，以太网OAM功能，支持CFM-OAM功能，当ULPP组成员端口收到与配置匹配的CFM（超时或恢复超时）时，能够进行联动操作。 11. 支持专业级IPv4/v6 VLAN ACL，IPv6 port-range ACL。 12. 支持FULL EAPS功能，支持多进程MSTP进程。 13. 支持BFD for VRRP/静态路由/RIP/OSPF/BGP，拓扑变化时，设备能够快速收敛，收敛时间小于等于50ms。 14. Pv6 SAVI接入网源地址验证。 15. IPv6 DHCP Server。 16. 此次所投网络与安全产品均为同一厂商 17. 要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。   可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项规程要求 | 1套 |  |
| **2** | 信息安全攻防竞技平台 | 1. 标准X86服务器架构，内存≥16GB，千兆电口≥6个。 2. 采用“系统+数据”双硬盘架构。数据硬盘容量配置不低于1TB，系统硬盘SSD不低于120GB。 3. 单台设备虚拟机并发数量≥20个，单台虚拟机的启动速度小于20秒。 4. 为了便于用户灵活访问平台进行攻防实操，系统采用B/S架构设计，通过浏览器访问平台即可开展实训操作。 5. 平台支持多台设备集群管理，在管理页面进行权重设置，即可实现所有设备的负载均衡。 6. 可以在主设备后台直接查看所有设备的硬件使用情况和虚拟机数量。 7. 系统提供管理员、观众、学员三种账号 8. 管理员能够对账户进行批量操作，包括导入、导出、编辑、新增等； 9. 系统提供三种比赛模式，夺旗模式、单兵模式、混战模式 10. 提供观摩模式，可以通过大屏输出，实时查看比赛过程。 11. 提供场景管理，同时可创建多个比赛主题场景，让老师轻松管理任意切换。快速满足举办各种竞赛的需要。 12. 支持对实验场景进行新增、删除、修改等操作；可以进行磁盘镜像和光盘镜像管理，对每个服务器的状态进行控制和编辑，对光盘镜像文件启动进行设置。至少提供10种以上的虚拟化主机系统，至少包括Windows2000、Windows2003、Windows2008、Windowsxp、Windows7、Windows8、CentOS、Redhat、BT5、KALI等操作系统，并且用户可自定义。 13. 支持场景、靶机、竞赛内容的新建和编辑，管理员可以根据自己的要求进行场景、靶机、场景介绍、场景规则、场景拓扑等内容的创建和编辑 14. 提供支持一键快速部署，系统自行根据参赛组成员数量部署比赛环境 15. 场景一键部署后，可以实时监控参加该场景实训的任意学员的靶机状态和操作，在靶机故障时可以帮助其重置环境； 16. 可扩展加载全国高职大赛的第三阶段信息安全管理与评估的大赛扩展包。 17. 夺旗竞速模式为每个用户提供1-2台攻击渗透机，通常在实验室进行集中部署，只要网络可达，学员可以在任何地点任何时间可以开展攻防实操实验，夺旗模式是考验学员的解题速度。 18. 单兵闯关模式，每个用户拥有完全独立的多台靶机资源，不同用户之间环境隔离，某个用户环境故障，管理员20S即可快速帮助学员恢复环境； 19. 分组混战模式，平台通过集群可以支持上百支队伍同时比赛，每组可以有1-5台漏洞靶机，参赛队伍在比赛中可以加固自己的漏洞主机得分，也可以攻击其他队伍的漏洞靶机进行得分。 20. 单兵闯关提供内置不少于30个关卡 21. 提供一套网络混战赛题，参赛队伍可以通过平台默认赛题快速开展混战比赛； 22. 夺旗竞速态势展示：平台通过集群可以支持200人以上同时比赛，态势展示可以显示参赛学员ID、头像、得分、排名、实时夺旗得分情况。 23. 单兵闯关态势展示：平台通过集群可以支持200人以上同时比赛，态势展示可以显示参赛学员ID、头像、得分、排名、个人闯关进度以及单个关卡过关率。 24. 分组混战态势展示：平台通过集群可以支持100支队伍以上同时网络混战，包含参赛队伍昵称、队旗、得分、排名，实时攻击流量、FLAG得分流量 25. 支持三种模式态势展示定制，可以提供标准化接口； 26. 此次所投网络与安全产品均为同一厂商   要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。  可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项平台要求 | 1 |  |
| **3** | 下一代防火墙 | 设备硬件要求：  专有硬件平台：硬件采用非X86多核架构，处理器为采用64位MIPS多核处理器  操作系统：必须为具有自主知识产权的64位安全操作系统  接口数量：配备至少9个千兆电口  USB接口：至少配置1个USB2.0接口 ,支持不依赖网络的外接U盘方式进行系统升级和外接移动硬件存储日志。  性能要求：  吞吐量≥2Gbps；  IPS吞吐量≥400Mbps；  防病毒吞吐量≥300Mbps；  IPsec VPN吞吐率≥500Mbps（AES256+SHA-1）；  最大并发会话数≥20万；  每秒新建会话数≥2万；SSL VPN用户数最大需支持不少于128并发用户  网络功能：  接入模式：必须支持透明、路由、混合、旁路四种工作模式，旁路模式下对流量进行统计、扫描、记录和会话重置  路由协议：  OSPF、BGP和RIPv1/v2（动态路由协议非透传）支持策略路由、并内置ISP路由表，支持ISP路由功能，支持ISIS路由协议；  IPv6静态路由、IPv6 BGP动态路由、OSPFv3、RIPng等  必须支持基于角色、用户、用户组、服务协议、APP应用等的条件策略路由；  802.3ad 链路聚合：透明、路由模式下支持将多条链路带宽进行捆绑，支持LACP动态聚合  NAT技术：  要求必须支持SNAT、DNAT、PAT等功能。  要求必须支持NAT full cone模式、NAT的端口扩展技术，突破传统单个公网地址64512个端口的瓶颈。  支持多种NAT技术，包括源地址NAT，目的地址NAT，支持一对一、一对多、多对一、多对多的NAT等多种方式。  NAT地址有效性检测：支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断  高可用性（HA）：支持AP模式，AA模式，且透明模式下可支持AP模式  防火墙：  必须支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、Winnuke  必须支持并发、新建会话控制功能，要求能够基于源、目的、应用协议三种条件做会话数限制  支持按照应用、时间、用户帐号、IP地址、服务端口、物理端口、安全域等方式对数据进行访问控制  支持对防火墙策略命中次数的统计功能  支持通过策略列表中的冗余和无用策略进行检测  基于国家地理的威胁识别与控制  链路负载均衡：  支持电信和联通的ISP路由表，并支持自定义的ISP创建  基于应用的健康监测：支持HTTP GET、DNS请求和TCP端口的方式探测被监控链路或被监控服务器的健康状态。  支持多出口线路的链路质量就近探测（带宽使用率、延时影响等条件）、实现择优选路的负载均衡功能  支持SmartDNS功能。  入侵防御：  支持基于源、目的、规则集、动作的入侵防御规则；  具备丰富的木马特征库，能对当前主流的RPC漏洞攻击做检测和阻断，支持识别针对FTP、Netbios、IMAP、Samba等应用安全漏洞的攻击；支持识别多种IIS、Apache、RPC、Oracle、SQL等应用系统类溢出攻击；支持专业的 Web Server 防护功能，含 CC 攻击防护和外链防护等  支持抵御所列所有攻击类型，在保障合法应用正常运转的前提下，提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破2解等恶意流量的检测和阻断。可有效抵御SQL注入、XSS注入，外链检查、CC防护等  支持自定义入侵防御特征，方便用户根据自身业务系统设置防护策略；  入侵防护特征库不少于7000种且特征库支持自动更新；  防病毒：  具备专业的病毒扫描引擎技术，被检测文件大小不受限制；支持对压缩文件类型的病毒检测，支持对多重压缩文件的病毒检测，且不小于5层压缩；  支持对HTTP、FTP、SMTP、POP3、IMAP协议的应用进行病毒扫描和过滤；  支持对GZIP、EXE、ZIP、RAR、PE、JPEG、MAIL、HTML、PE、BZIP2、RIFF和TAR文件类型进行病毒过滤；  支持恶意网站访问控制，针对恶意网站可执行重置连接、告警和记录日志动作；  具备病毒过滤特征库不少于300万，且支持特征库每日自动更新升级；  应用引流：  支持TCP/UDP的应用牵引功能，可以将URL、HTTP视频、HTTP下载、P2P下载、P2P视频、游戏和IM软件等应用基于策略引导到指定链路上，可以识别进行引流的应用数在3000种以上。  能对P2P软件下载、P2P在线视频、Web视频进行应用引流    虚拟化：支持虚拟交换机、虚拟路由器等虚拟化功能  流量管理：  必须支持基于用户，ip地址以及7层应用进行保证带宽，最大带宽的控制，支持针对7层应用的优先级转发控制  多层QoS功能要求包含应用QoS 和IP QoS 是两个独立的数据流控制功能，应用QoS下可以嵌套IP Qos策略，IP QoS可以嵌套应用QoS。  可支持3000种以上应用协议的识别分类，包括P2P下载、P2P在线、WEB视频、网络游戏、炒股软件等  必须支持弹性带宽功能，可自定义阀值来上弹或回收带宽，充分利用网络带宽资源  上网行为管理：  支持对FTP登陆账号名及上传、下载文件名进行记录或控制  可支持对主流IM、主流网络游戏、主流炒股软件、主流视频、P2P下载应用进行识别或控制；  对用户访问含有某关键字的网页（包括HTTPS加密网页）、邮件和web外发关键字进行行为控制；  支持加权算法，包括定义关键字的权重和出现次数等条件做控制；  支持2000万以上，至少60个分类web页面库，且支持自定义URL分类过滤。  支持基于文件类型、文件大小、文件名称进行文件传输安全控制  SSL VPN：  支持硬件USB-key、手机短信的认证方式  支持双因素认证(用户名/口令＋USB-Key)  支持客户端硬件特征码绑定认证  多出口链路下支持选择最快响应链路建立SSL连接  支持本地用户修改密码功能  IOS下支持XAuth的IPSEC服务，Android系统拥有独立客户端系统  必须支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、指定进程、系统补丁、浏览器版本、杀毒软件等方面  IPSEC VPN：  支持对VPN隧道中的应用进行控制  支持速连VPN部署技术，中心端自动下发配置到分支设备而无需手工配置  基于策略的VPN和基于路由的VPN  配套管理：  管理功能：必须支持2个系统软件并存，并支持系统软件回滚，防止配置不当或系统故障造成的网络中断，充分保证系统的稳定性。  网页浏览日志：必须支持记录通过设备的访问详细URL、IM上下线日志等日志信息。  高性能日志记录：必须支持基于secure-tcp的日志记录格式  实名认证审计：支持与深澜、城市热点等知名计费系统进行实名审计关联，包括user+IP+MAC。  此次所投网络与安全产品均为同一厂商  要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。  支持全国及福建省职业院校技能大赛高职组“信息安全管理与评估”赛项。 | 1 |  |
| **4** | 信息安全实训平台 | 硬件配置及性能指标：   1. 多核平台，内存≥16G，千兆电口≥10个，采用SSD+SATA双硬盘架构； 2. 存储容量配置不低于1TB，SSD系统盘不低于120GB; 3. 单台设备虚拟机并发数量≥14个；   基本功能：   1. 支持基于WEB的用户注册功能，并支持学生、教师和管理员三种用户，并支持用户自己修改用户信息； 2. 提供学生、老师、管理员三种角色管理，支持组织结构管理； 3. 设备必须支持虚拟化管理，支持查看当前云平台自动调用的虚拟化资源； 4. 平台采用B/S结构   课程管理：   1. 提供支持必修课和选修课两种类型的课程； 2. 提供支持课程导入导出，包含课程所有信息，如虚拟机、课件等内容； 3. 提供用户课件的上传，提供用户上传课件内容后在线浏览功能，同时可以在线下载课件。支持HTML、PPT、WORD、PDF、SWF、scom等格式； 4. 提供上传的课件支持HTTP和FTP两种方式； 5. 支持不同课程之间虚拟机环境的隔离 6. 教师角色支持课程和学员的关联，学员只能学习关联的课程 7. 支持课程体系管理、课程分类管理、课程管理和实验调度管理； 8. 提供学习课程时对虚拟机进行截图、录屏功能、提供实验报告撰写功能； 9. 提供超过200个以上课件资源列表，每个课程提供虚拟模板，实验操作手册，实验视频和WORD版本的操作手册； 10. 虚拟化设备支持根据用户需求定制虚拟机，便于学生学习各种课件。必要时按照用户要求进行现场测试，不满足的视为非实质性响应；   考试管理：   1. 支持题库管理定义课程题库； 2. 支持综合考试管理通过详细流程来定制综合考试相关试题； 3. 支持课程考试管理 4. 支持考题题型、难度搜索，支持考题导入导出；   查询统计：   1. 查看学生学习情况及进展； 2. 支持查看学生考试结果 3. 支持在线用户数   云平台管理：   1. 提供虚拟机模板定制功能，新建虚拟机模板、删除虚拟机模板。支持基础镜像、增量镜像的设置。支持导入虚拟机模板。支持导入光盘镜像文件。 2. 提供集群管理，支持多台主机集群管理，通过弹性云计算方法自动轮询调度虚拟主机。 3. 提供虚拟机使用状态情况，能够看到各个节点资源使用情况，如虚拟机、课程、学生关联情况。提供关闭各个节点的虚拟机功能。提供远程协助各个虚拟机功能。 4. 提供HTML5技术的虚拟机管理方式，支持对于虚拟机暂停、恢复、关闭、重启等操作。 5. 至少提供16种以上的虚拟化主机系统，至少包括Windows2003、Windows2008、Windows2012、Windowsxp、WindowsVista、Windows7、Windows8、Windows10、Linux Mint、CentOS、Redhat、BT5、KALI、Ubuntu、debian、kylin等操作系统，并且用户可自定义。   学习内容：   1. 该平台必须满足以下实验教学内容，应包括密码学与应用、信息系统安全、网络安全、数字内容安全、软件安全、信息安全工程实践、计算机取证与司法鉴定等200个实训场景，可以通过扩展到800个实训场景，并提供配套电子实验教学文档。   实验数量：   1. 实验数量必须含有Web应用安全11个、网络安全15个、安全攻防分析6个、密码破解技术6个、VPN6个、防火墙实验8个、网络扫描与嗅探19个、BT5实验9个、安全风险评估3个、入侵检测6个、网络攻防分析2个、 windows取证和司法见证4个、linux系统10个、操作系统安全11个、安全审计3个、容灾备份5个、应用系统安全6个、数据库安全4个、恶意代码分析10个、缓冲区溢出与漏洞分析7个、网络渗透4个、操作系统渗透3个、Web应用渗透5个、拒绝服务7个、数据保密与安全4个、密码学14个、密码学应用5个、PKI6个、安全编程11个； 2. 要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。 3. 提供正规出版配套信息安全教材一套，包含（网络攻击防范与协议分析、网络渗透与设备安全、数据库与WEB安全、信息安全产品配置）。 4. 提供互动式虚拟仿真平台公有云账号3个（一年）。内容包括（近年赛项真题解析、缓冲区溢出渗透测试、运用Python进行渗透测试、Web应用程序安全攻防等）   提供10方竞赛培训云视频服务（一年），云视频服务由全球领先云计算平台承载，采用全虚拟化部署方式，实现分布式集群式媒体资源池架构，支持异地多活，支持大规模接入、无限弹性扩展，保证系统高可靠性。支持媒体录制服务，支持会议录制、内容分享录制，云端存储，支持录制权限管理。支持通过视频线缆、网络和无线方式发送双流，共享PC桌面、Office、PDF、图片、视频等文件。  可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项平台要求 | 1 |  |
| **5** | web应用防火墙 | 网络配置：   1. 接口地址配置：   具备默认网关、网络接口地址配置；  支持透明模式下网桥配置功能，包括IP/MASK/GATEWAY配置；  支持反向代理模式下外网口，内网口配置IP地址配置，支持外网口默认网关地址设置；   1. DNS配置：支持网关主、从DNS配置； 2. WAN口多IP配置：支持反向代理模式下WAN口（外网口）多个IP配置功能； 3. 网桥配置：   支持网桥下接口的灵活配置，可以将多个接口配置到一个网桥下；  支持多个网桥添加、修改、删除；  支持网桥上IP设置；   1. VLAN配置：支持802.1q协议标准VLAN设置，通过VLAN设置实现对VLAN服务实行服务； 2. 静态路由配置：支持对指定接口添加，删除静态路由； 3. 策略路由配置：支持对指定接口添加，删除策略路由； 4. 应用模式：部署方式支持反向代理、透明代理部署模式   服务接入：   1. 接入方式：   支持对添加的不同服务采用不同的策略；不同的服务通过是IP，PORT，域名组合的唯一性来确定；支持IP,PORT相同域名不同的服务采用不同的防护策略  支持客户端到WAF网关的HTTP/HTTPS连接；  支持WAF网关到WEB服务器的HTTP/HTTPS连接；  支持添加透明、反向代理模式下服务，服务配置包括：服务名称，服务类型(HTTP,HTTPS),主机地址，端口，域名  支持透明模式下的服务直通功能；  支持网关证书管理，包括根证书、网关证书、证书密钥等；  支持添加服务时指定关联的防护策略；  支持透明和反向代理模式下，添加HTTPS服务，用于防护HTTP的WEB服务；   1. 证书管理：   支持证书上传功能，包括CA，网关证书，通过上传证书，提供HTTPS服务网关证书功能，验证客户端证书和WEB服务器证书功能；  支持证书有效期，证书内容查看功能；  支持pem，pfx格式的网关证书和CA证书上传；  安全策略：   1. 黑白名单：黑白名单实现对指定客户端IP或者是URI,参数等设置黑名单或者白名单，黑名单优先于白名单。该用于实现用户特定的一些业务需求，同时也是在系统误报时进行白名单设置，不影响用户的正常业务访问。 2. 协议规范检测：   支持设置HTTP请求头域值的最大长度  支持设置HTTP请求头名称的最大长度  支持设置HTTP请求头域的最大个数  支持设置HTTP请求体的最大长度  支持设置表单参数值的最大长度  支持设置表单参数名称的最大长度  支持设置HTTP请求行的最大长度   1. 安全策略：   支持设置查询参数值的最大长度  支持设置查询参数名称的最大长度  支持设置查询参数的最大个数  支持设置COOKIE最大个数  支持设置禁止的请求方法  支持设置禁止的HOST   1. 输入参数验证：   支持查询参数值，查询参数名称，查询参数值和名称组合，表单参数值，表单参数名称，表单参数值和名称组合的参数验证；  支持字符串匹配和正则匹配的输入参数匹配方式；  支持上传文件后缀检查；  支持允许,阻断动作；   1. 基本攻击防护：实现对基本攻击的防护，包括HTTP请求和回复，通过本功能实现对常见攻击如SQL注入，跨站脚本，目录遍历，系统命令注入等防护，支持对OWASP攻击类型防护，且提供规则的高级配置，用户可以配置复杂的用户自定义的规则。 2. 暴力浏览攻击防护：实现阻止暴力浏览防护，对单个IP来访请求根据设定相应的限制 3. HTTP CC防护：实现CC 攻击防护,拦截多IP、会话CC攻击 4. 网站隐身 本实现通过HTTP回复头的处理，实现对网站信息，如网站操作系统类型，web服务器类型的隐身 5. 站点转换：实现对HTTP请求头和回复头域的添加，修改操作,对访问URL的重定向功能 6. 数据防窃取：本实现对HTTP回复内容敏感信息过滤和隐藏。 7. 错误码过滤：本实现对web服务器回复4XX，5XX时，进行过滤和定制回复页面用以隐藏泄漏服务器信息 8. 篡改保护：防篡改——实现基于FTP的防篡改保护 9. 漏洞发现：漏洞扫描——至少实现敏感信息发现，目录泄漏，网站信息泄漏的漏洞发现 10. 高可用：双机热备——实现双机热备，一台主机宕机，另一台能够自动切换所有的防护服务 11. 此次所投网络与安全产品均为同一厂商 12. 要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。   可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项规程要求 | 1 |  |
| **6** | 网络日志系统 | 物理端口：6个千兆电口，1个扩展插槽，1个Console ，存储 1T硬盘，机箱 1U。内置常用的攻击工具库，重点针对网络层，可以用于教学和比赛使用；能够详细识别、记录所有的用户数据，有详细的日志信息，可以导出，可以让学生动手分析   1. 部署模式   旁路模式：支持旁路部署，以镜像方式接收流量用于分析  桥接模式 支持以二层桥接模式部署，包括单桥和多桥的部署模式。   1. 网管方式与网管策略   WEB管理：支持以HTTP及SSL加密的WEB图形化接口进行设备配置和管理，支持英语、简体中文  SSH管理：支持 SSH 命令行管理方式。  Console管理：支持Console管理。   1. 网管策略   管理权限分立：系统默认有超级管理员、审计管理员、只读管理员，可根据需要灵活定制管理员角色。  支持密码强度、口令尝试死锁、账户激活等安全管理功能。  通过网管策略，可允许部分IP能网管设备，以限制非法管理员访问设备。   1. 网络功能   静态路由：支持IPv4、IPv6静态路由功能。  子接口：支持物理接口添加子接口功能。  聚合接口：支持将多个以太网物理端口捆绑成一条逻辑端口，不仅增加链路带宽，同时增加链路备份。  网口模式：支持WEB页面改变网口的排列顺序   1. 基础防火墙功能   防火墙：支持基于状态监测的防火墙，不仅保障网关设备安全，还能保护组织内网安全。  安全策略：支持包过滤检测功能，默认情况下，拒绝所有的数据包通过，以保证网络的安全性，且不能修改、移动和删除。  NAT转换：支持多对一的PAT转换、一对一的地址转换、多对多等多种 NAT转换策略。   1. IPS入侵检测   防dns漏洞攻击：DNS类规则识别各种DNS服务器漏洞，防止攻击者通过DNS服务器漏洞攻击用户。  防mail漏洞攻击：邮件库类规则识别各种邮件服务器漏洞，如Sendmail、Foxmail、MS Exchange等，防止攻击者通过邮件服务器漏洞攻击用户。  防worm漏洞攻击：蠕虫程序是一种可以自我复制的恶意程序，可以通过网络进行传播，消耗网络和系统资源。蠕虫规则识别蠕虫程序的传播，防止攻击者通过蠕虫程序破坏目标系统。  防tftp漏洞攻击 ：Tftp类规则识别各种tftp服务器漏洞，如3CDeamon、FutureSoft等防止攻击者通过tftp服务器漏洞攻击用户。  防snmp漏洞攻击：snmp类规则识别各种snmp服务器漏洞，防止攻击者通过snmp服务器漏洞攻击用户。  防 ftp漏洞攻击：Ftp类规则识别各种ftp服务器漏洞，如Serv-U、WU-FTPD、WS\_FTP、3CDeamon等，防止攻击者通过ftp服务器漏洞攻击用户。  防 shellcode漏洞攻击：Shellcode是一段小的程序，作为漏洞执行的负载，执行某种功能。Shellcode规则识别shellcode代码，防止攻击者远程执行shellcode代码。  防rpc漏洞攻击：rpc类规则识别各种rpc服务器漏洞，如tooltalk、sadmind等，防止攻击者通过rpc服务器漏洞攻击用户。  防database漏洞攻击：数据库类规则识别各种数据库服务器漏洞，如Oracle、Sql server、Mysql等，防止攻击者通过数据库服务器漏洞攻击用户。  防web漏洞攻击：Web类规则识别各种web服务器漏洞，如IIS、Apache等，防止攻击者通过web服务器漏洞攻击用户。  防system漏洞攻击：系统类规则识别各种操作系统漏洞，如Windows、Linux、Unix等操作系统，防止攻击者通过操作系统漏洞攻击用户。  防 malware漏洞攻击：Malware就是植入你电脑中的恶意代码，它可以完全控制、破坏你的PC、网络以及所有数据。malware类规则识别各种malware程序，防止攻击者利用malware漏洞攻击用户。  防 trojan漏洞攻击：木马软件是一种恶意软件，可以安装在用户计算机上，通过木马软件远程操控目标系统并执行各种操作。木马规则类识别木马软件的网络操作，防止攻击者通过木马软件控制目标系统。  防 telnet漏洞攻击：Telnet类规则识别各种Telnet服务器漏洞，防止攻击者通过Telnet服务器漏洞攻击用户。  防 botnet漏洞攻击：botnet类规则识别各种客户端botnet行为，防止攻击者通过botnet漏洞控制用户。  防 web\_browse漏洞攻击：Web浏览器类规则识别各种web浏览器漏洞，如IE、Firefox、Chrome等，防止攻击者通过web浏览器漏洞攻击用户。  防 web\_activex漏洞攻击：ActiveX是可以重用的软件组件程序，可以嵌入到web浏览器中使用。Web\_activeX类规则识别各种嵌入到浏览器的ActiveX控制漏洞，防止攻击者通过ActiveX控件漏洞攻击用户。   1. 攻击知识库   攻击库：攻击库列表展示和查询，攻击库字段包括：攻击编码、攻击名称、攻击类型、风险等级、CVE编码、攻击标签、影响产品、发布时间、更新时间  CVE库：CVE库列表展示和查询，CVE库字段包括：名称、类型、描述、来源、解决方案、影响硬件、参考URL、漏洞分值、风险等级、发布日期、修改日期、攻击向量、攻击复杂度、机密性影响、完整性影响、可用性影响  常用服务端口：常用端口列表展示和查询，端口信息字段包括：端口号、端口类型、端口名称、端口说明  常用网络层协议说明：网络协议列表展示和查询，协议信息字段包括：协议号、协议简称、协议名称、协议说明、参考来源   1. DOS/DDOS防护   DOS/DDOS防护：支持ARP洪水攻击防护、IP和端口扫描防护、 DOS/DDOS防护（ ICMP洪水、UDP洪水、SYN洪水、DNS洪水攻击防护）、未知协议类型防护、TearDrop攻击防护、IP数据块分片传输防护、LAND攻击防护、WinNuke攻击防护、Smurf攻击防护、异常报文侦测防护等  9、Web服务攻击防护  支持Web网站隐藏，包括HTTP响应报文头出错页面的过滤，web响应报文头可自定义；  支持FTP服务应用信息隐藏包括：服务器信息、软件版本信息等；  支持OWASP定义10大web安全威胁，保护服务器免受基于Web应用的攻击，如SQL注入防护、XSS攻击防护、CSRF攻击防护、支持根据网站登录路径保护口令暴力破解；支持web站点扫描、web站点结构扫描、漏洞扫描等扫描防护；  可严格控制上传文件类型，检查文件头的特征码防止有安全隐患的文件上传至服务器，并支持结合病毒防护、插件过滤等功能检查文件安全性；   1. 流量实时监控   TOP 50服务流量监控：查看前五十名服务流量的实时监控。  服务组流量监控：将各服务分类统计，实时查看服务组流量监控图。  活跃服务统计：查看当前活跃服务的最新速率、最近一小时流量、最近一小时平均速率、每个服务对应有哪些用户在使用，及每个用户的使用情况。  所有服务统计：查看当前活跃服务的最新速率、最近一小时流量、最近一小时平均速率。  TOP 50 用户流量监控：查看前五十名用户的传输速率、新建会话速率、活跃会话数。  在线用户统计：实时查看当前在用户的详细信息：在线流量、最新速率、会话数、上线时间等信息。  上网行为：实时查看在线用户的访问网站、搜索引擎、邮件收发、账号登录等上网行为记录。  物理端口：查看物理端口接收报文的情况，以及每个端口传输流量的趋势图。  动态更新实时监控图 支持动态显示网络流量监控图。  11、流量控制  流量优先级：  可将应用流量划分为 高、中、低等共三个优先级，优先级越高的流量，优先传送，以提升带宽的高使用率。  支持流量父子通道技术，支持三级父子通道；  结合最大带宽和流量优先级，可为某些关键应用或者VIP客户保障一定带宽。  流控黑名单：基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中，或者强制用户下线。  策略流控：支持基于终端类型，线路，应用，URL的流控，文件类型，IP，用户组，时间段的流控  基于单个用户的流控：  可根据主机的IP地址或者用户名称，对单个主机进行如下控制：  （1）最大上行/下行带宽限制；  （2）最大上行/下行会话控制；  （3）分类服务的带宽控制，即限制单主机的总带宽的同时，再对某些服务进行控制。如限制单个主机的上行/下行带宽分别为500K/1M的同时，再限制P2P的带宽为100K/200K、网络电视为100K/100K等；  以上参数均可分时段管理。   1. 自身安全防护   高可靠性(HA)：支持一主一备、主/主模式的HA功能。  会话加速老化：对某些会话进行快速老化，防止会话表被写满。   1. 告警配置   设备告警：支持设备事件日志告警、黑名单告警、CPU、内存、活跃会话数、入侵事件、攻击事件等告警。  14、抓包分析：调试信息下载——一键下载调试信息，以便学生分析学习分析。  15、统计分析  设备资源：分时段对设备资源，包括 CPU使用率、内存使用率、活跃会话数、在线用户数等信息进行统计分析。  物理接口：分时段对物理接口的收发的流量、速率等进行统计分析。  用户统计：基于用户，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个用户使用了哪些服务、访问了哪些网站、通过了哪些链路等更加详细的信息。  用户组统计 基于用户组，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个用户组使用了哪些服务、访问了哪些网站、通过了哪些链路等更加详细的信息。  服务统计：基于服务名称，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务在各条链路上的分配情况。  服务类型统计：基于服务类型，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种类型的服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。  线路统计：基于出口链路，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每条链路上的用户、用户组、服务、服务类型、网站、网站类型的详细信息。  网站访问量排名：  基于用户/用户组对URL的访问次数，进行统计排名。  基于网站/网站类型被访问的次数，进行统计排名。  上网时长统计：统计用户上网的总时长，并统计每类服务使用时间的情况。  流量统计-网站排名：支持对网站流量进行排名，能生成趋势图，并能深入分析该URL基于用户的统计，该URL基于用户组的统计，该URL基于线路的统计  流量统计-网站类型排名：支持对网站类型流量进行排名，能生成趋势图，并能深入分析该URL类型基于URL的统计，该URL类型基于用户的统计，该URL类型基于用户组的统计，该URL类型基于线路的统计  热点分析-热点网站：支持对网站访问次数进行排名，能生成趋势图，并能深入分析该网站基于用户的统计，该网站基于用户组的统计  热点分析-热门网站类型：支持对网站类型访问次数进行排名，能生成趋势图，并能深入分析该网站类型基于用户的统计，该网站类型基于用户组的统计   1. 日志查询   DoS攻击日志：记录DoS攻击日志，包括攻击类型、源区域、源目IP地址、目的IP地址、匹配策略名、描述、严重级别、记录时间。  IPS日志：记录IPS日志，包括攻击类型、源区域、源目IP地址、目的端口、漏洞ID、漏洞名称、匹配策略名、描述、严重级别、记录时间。  WEB应用防护日志：记录WEB应用防护日志，包括攻击类型、协议、URL/目录、源/目的区域、源/目的IP、源/目的端口、详细信息、规则名称、严重等级、动作、时间等  病毒查杀：记录病毒查杀日志，包括应用类型、行为、协议、文件名、文件类型、病毒名称、源目区域、源目IP、源目端口、所属组、记录时间。  网页URL日志：能够记录用户所访问网站的URL地址。  会话记录：详细记录每一个会话的信息，包括：用户名、用户组、源IP/端口、目的IP/端口、转换IP/端口、MAC地址、协议类型、协议名称、发送流量、接收流量、会话持续时间、会话结束时间。并可导出为EXCEL或者HTML格式的报表。  告警记录：记录入侵事件、攻击事件、设备运行状态异常的告警日志。  高级检索：可查询以上日志类型，支持模糊查询。   1. 应用审计   网页标题：记录用户所访问网页的标题内容。  网页快照：支持记录网站网页快照，进行网页预览。  记录网站的 URL：能够记录用户所访问网站的 URL 地址。  记录引擎搜索关键词：对在搜索引擎中搜索的关键词进行记录。  邮件收发记录：SMTP,POP3，IMAP,WebMail邮件审计，包含发件人、收件人、邮件主题、正文、附件、日期、邮件大小等。  IM聊天内容审计：记录QQ、MSN、Skype、Yahoo、飞信、阿里旺旺等聊天内容信息，包括发送账号、接受账号、聊天内容、用户名、主机IP、所属组以及对应时间。  论坛微博信息：记录天涯、搜狐、新浪等论坛及微博的发帖、博客记录，审计信息包括标题、正文、发帖网站、用户名、组名、日期等。  账号登录审计：记录购物、微博、博客、论坛、网盘、邮箱、社交娱乐、即时通讯、游戏、手机ID等类别的应用的登录账号。包括web和客户端两种登录方式的账号审计。  外发文件审计：记录网易网盘、百度云盘、金山快盘等网盘文件的http上传文件，记录QQ、Skype、MSN、阿里旺旺等聊天工具外发文件，记录FTP上传、下载文件，WebMail发送邮件，SMTP发送邮件，POP3接收邮件包括文件名、文件大小、用户名、组名、主机IP、目标IP地址、上传URL、日期、附件个数和下载。  外发post审计：记录购物、微博、博客、论坛、网盘、邮箱、搜索引擎、游戏、综合、手机ID等外发post信息。  Telnet行为记录：记录用户Telnet操作的详细信息。  数据库审计：支持MYSQL,SQL SERVER 等数据库命令审计  会话记录：详细记录每一个会话的信息，包括：用户名、用户组、源IP/端口、目的IP/端口、转换IP/端口、MAC地址、协议类型、协议名称、发送流量、接收流量、会话持续时间、会话结束时间。并可导出为EXCEL或者HTML格式的报表。  应用识别库：支持常用协议，HTTP应用，FTP应用，视频网站浏览，WEB视频，P2P下载，流媒体，网络游戏，即时通讯，股票行情，股票交易，网上银行，网络电话，网络存储，移动应用，网页邮箱，软件更新，远程控制，数据库等应用分类等2000多种。   1. 数据管理   数据存储策略：支持按磁盘百分比、按保留天数、系统硬盘最大化三种存储方式。  数据列表查询：支持查询磁盘空间使用和剩余空间、百分比，包括每一种数据类型的使用空间、磁盘占用率，时间范围。  数据删除：基于时间范围、数据类型明细、系统日志明细删除日志。  数据备份：支持备份本地存储日志到FTP服务器，为日志审计提供冗余备份。   1. 此次所投网络与安全产品均为同一厂商 2. 要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。   可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项规程要求 | 1 |  |
| **7** | 无线交换机 | 1.为独立的盒式AC。支持对所有AP(a/b/g/n/ac)进行统一管理。  2.具备交换路由功能，支持基于ASIC芯片的二层交换和三层交换功能，支持基于ASIC芯片的ACL和QoS控制功能  3.支持N+1或1+1热备冗余机制；  4.最大支持256个 AP管理；  5.每台AC支持最大并发用户数不少于8K；  6.支持双 image功能，主用image损坏时备份image可以启动；  7.支持不少于368Gbps的交换容量，支持不少于274Mpps的IPv4、IPv6包转发速率；  8.24个10/100/1000Mbps接口，4个复用千兆SFP光口，2个万兆扩展插槽；  9.支持AC及DC电源；  10.支持802.11a/b/g/n/ac、802.11i、802.11e、WMM；  11.支持频谱分析功能，实现对2.4G的频谱分析功能，能识别微波炉、无绳电话、蓝牙、单音多音干扰等非wifi干扰；  12.支持WEP、TKIP、CCMP、SMS；  13.支持Portal和MAC双因子认证，即同一个SSID下部分终端采用Portal认证方式，部分终端采用MAC认证方式；  14.支持WAPI的加解密功能、支持WAPI认证方式；  15.支持IPV6接入和转发功能：支持在IPv4网络中构建IPv6的WLAN接入服务；支持在IPv6网络中提供IPv4的WLAN接入服务；支持在IPv6网络中构建私有的IPv6的WLAN网络服务；  16.支持MAC，IPv4，IPv6各种类型报文的QOS Policy控制；  17.支持MAC，IPv4，IPv6各种类型报文的ACL访问控制；  18.支持AP向AC注册的如下安全接入方法：支持AP mac地址的认证；支持AP口令密码的认证；支持AP、AC双向数字证书的认证；  19.支持Static Routing，RIPv1/v2、OSPF、BGP；  20.支持IGMP v1/v2/v3，PIM-SM、PIM-DM、PIM-SSM；  21.AC和AP之间的管理支持CAPWAP协议；  22.IPV4/V6双栈、手工隧道、ISATAP等隧道、DHCPv6、DNSv6、ICMPv6、ACLv6、IPv6 QoS、静态路由、OSPFv3；  23.此次所投网络与安全产品均为同一厂商  24.要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。  可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项规程要求 | 1 |  |
| **8** | 无线交换机POE模块 | 无线AP配件：10/100/1000Mbps单端口802.3at PoE模块，最高输出功率为30W | 1 |  |
| **9** | 无线接入点 | 基础规格：   1. 要求产品形态为室内双频放装式AP，发射功率≥20dBm 2. 可同时工作在802.11a/n/ac、802.11b/g/n模式 3. 支持802.11ac wave2的MU-MIMO技术 4. 2.4G射频支持3\*3 MIMO，2.4G射频最大速率450Mbps 5. 5G射频支持2\*2 MIMO，5G射频最大速率867Mbps   硬件规格   1. 支持10/100/1000BASE-T 端口≥1个 2. 支持外置USB接口，便于扩展蓝牙、物联网、外置存储等应用 3. 内置天线设计，支持壁挂、放装、吸顶等安装方式 4. 支持标准PoE（802.3af）供电，并支持本地适配器供电   功能要求   1. 支持SSID数≥32 2. 支持FIT/FAT模式可切换，可被本次招标的所有型号的无线控制器管理 3. 支持AP逃生功能，AP-AC链接断开后AP可继续工作不影响用户使用 4. AP向AC注册支持AP mac地址认证，支持AP口令密码认证，支持AP、AC双向数字证书的认证 5. 支持基于SSID和Radio的无线服务定时开启和关闭控制 6. 支持wifi定位功能和wifi探针功能 7. 支持频谱导航功能，能够自动引导双频无线终端工作在5GHz频段上 8. 此次所投网络与安全产品均为同一厂商 9. 要求所有配件原厂完整包装；货物由原厂直接发货到采购人现场，包装箱上注明采购人的单位名称，否则不予验收。   可以满足2022年福建省职业院校技能大赛“信息安全管理与评估”赛项规程要求 | 1 |  |
| **10** | 定制服务 | 设备平台安装调试、设备及平台的使用培训辅导、产品维护 | 1 |  |

1. **商务条件**

**包：1  
1、交付地点：采购人指定地点**

**2、交付时间：中标方在合同签订后3内完成。**

**3、交付条件：现场交付。  
4、是否收取履约保证金：否  
5、是否邀请投标人参与验收：否  
6、验收方式数据表格**

| **验收期次** | **验收期次说明** |
| --- | --- |
| 1 | 1、验收时中标人代表必须在场，招标人将根据招标文件要求、中标人所供货物的规格和产品标准及我国相关技术规范和技术标准进行验收。2、结构、外观、制造、装配材料及工艺要求应符合招标采购要求及投标文件承诺，招标人在验收时如发现不符合招标采购要求的，招标人有权要求中标人进行换货或退货。3、在招标人安装现场进行，最终检验所发生的一切费用由中标人承担。 |

**7、支付方式数据表格**

| **支付期次** | **支付比例(%)** | **支付期次说明** |
| --- | --- | --- |
| 1 | 95 | 全部货物交货、安装调试正常并经验收合格后支付95%。 |
| 2 | 5 | 在验收合格之日满一年后且未发现质量问题无合同未了事宜后支付剩余5%。 |

**五、设备交货与安装调试**

1、交货。签订合同后，按合同约定时间把货物全部运抵现场。设备运抵安装现场后，招标方将与中标方共同开箱验收，如中标方届时不派人来，则验收结果应以招标方和当地商检人员的验收报告为最终验收结果。验收时发现短缺、破损，招标方有权要求投标人立即补发和负责更换。中标方应提供主要设备厂家供货证明。

2、安装和调试

中标人应按照采购人指定的地点进行安装调试；

设备调试由中标方负责，中标方调试前应提出完整的调试计划并经采购人确认，包括设备调试的内容、项目、指标、方法和进度；并提供相应的仪器和工具。中标方有责任对采购方的技术人员提出的问题作出解答。调试应进行详细记录，系统调试结束后，由中标方技术人员签字后交给采购人验收。

3、技术培训：提供两名日常操作及简单维护保养人员的免费培训服务，并指派专人负责与采购人联系售后服务事宜，主要培训内容包括但不限于货物及主要部件的基本构造、功能、日常使用操作、保养与管理、常见故障的排除，紧急情况的处理等；

4、售后服务承诺：

  1）在招标货物详细要求中有特殊要求的除外，所有货物均要求在验收合格之日起**免费质保期为一年或以上(厂家或国家有更长免费质量保修期限规定的从其规定）**。保质期内中标人必须保证对所有设备非人为破坏而损坏的免费保修保养。

2）所有产品保修服务方式均为中标供应商上门保修，即由中标供应商派人员到招标人产品使用现场维修。由此产生的一切费用均由中标供应商承担。

3）售后服务必须符合国家规定的标准，招标人欢迎中标供 应商提供切合实际的更优惠的服务承诺。中标供应商必须在售后服务条款中列明售后服务的标准、条件和服务响应时间等；

4）中标供 应商必须提出保修期内的维修、维护内容和范围（产品、技术、模块、部件）。提供全面的中文版培 训使用资料、产品说明书（原件）、保修卡、合格证。

5）中标人应根据招标人指定的地点免费提供所有货物的送货、安装服务。

6）验收不合格的货物，招标人可以要求中标人无条件免费更换或退货，并赔偿由此造成用户的损失。

7）投标人可视自身能力在投标文件中提供更优、更合理的售 后服务承诺。

8）投标人应针对本次投标提供详细的售 后服务方案及承诺，内容应涉及：维护机构、人员、地址、电话、维修方式、保修方式、保修期满后的维修保养费用、时间保证、零配件及易损件费用及优惠措施等。

**注：招标货物一览表中有相关保修和售后服务规定的从其规定，没有规定的按以上售 后服务要求。**

**第四部分 采购合同(参考文本)**

合同号：

甲方(招标人)： 签定地点：

乙方(中标人)： 签定日期： 年 月 日

见证单位(招标代理机构)：

根据甲方申请并经主管部门核准，甲方委托福建莆田兴鑫招标代理有限公司对以下货物进行招标采购(招标编号： )的招标结果，乙方为中标人，现依照招标文件、投标文件及相关文件的内容，双方达成如下协议：

* 1. **合同标的和合同价格**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 合同包 | 品目号 | 货物名称 | 品牌型号 | 配置和技术参数 | 生产厂家 | 数量 | 单价 | 小计 | 交货期 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 总价： 圆整(大写) ￥： (小写)  (合同总金额包含备件、安装、调试、检验和运输保险等费用) | | | | | | | | | |

* 1. **交货方式、地点和时间**

1. 交货方式：
2. 交货地点：
3. 交货时间：
   1. **供货清单**
   2. **付款方式与条件**
4. 货物交货付款

全部货物交货并经验收合格后，甲方凭收讫货物的验收凭证和货物验收合格文件等材料以 方式向乙方一次性支付 %的货物价款。(若乙方有支付履约保证金的，可在支付货款时予以扣除。)

现场交货条件下，乙方要求付款应提交下列单证和文件。

* 1. 金额为有关合同货物价格 %的正式发票。
  2. 生产厂家出具的货物质量合格证书。
  3. 甲方已收讫货物的验收凭证。
  4. 甲方签发的验收合格文件。

1. 分期支付货款的，余下的货款应于 (时间)支付。
   1. **质量要求和技术标准**

质量条款可细分为产品质量、包装质量、技术资料质量等内容。

(质量要求和技术标准应按招标文件要求填列。)

* 1. **安装调试、技术服务、人员培训及技术资料**

(安装调试、技术服务、人员培训及技术资料应按招标文件要求填列。)

* 1. **验收**

(货物验收标准和方法应按招标文件要求填列。)验收结果经双方确认后，双方代表必须按规定的验收交接单上的项目对照本合同填好验收结果并签名盖章。

* 1. **质量保证和售后服务：**

所有货物质保期要求均为货物经最终验收合格后 个月，在质量保证期内设备运行发生故障时，乙方在接到甲方故障通知后 小时内应委派专业技术人员到现场免费提供咨询、维修和更换零部件等服务，并及时填写维修报告(包括故障原因、处理情况及甲方意见等)报甲方备案。其中发生一切费用由乙方承担。

质量保证期后乙方应承担以下售后服务：

* 1. **知识产权：**

乙方须保障甲方在使用该货物或其任何一部分时不受到第三方关于侵犯专利权、商标权或工业设计权等知识产权的指控。如果任何第三方提出侵权指控与甲方无关，乙方须与第三方交涉并承担可能发生的责任与一切费用。如甲方因此而遭致损失的，乙方应赔偿该损失。

* 1. **违约责任**
     1. 因乙方原因造成货物延误，每延误满一周，应向甲方支付延期交货货物总值5%的违约金。但违约金总值不超过该批(次)货物总值的20%。当乙方的某一批货物交货时间延迟超过一个月时，除应按规定向甲方支付延迟交货违约金外，甲方有权通知终止本合同并要求赔偿因此而造成的损失。
     2. 当乙方发生违约时，乙方的质量合格证金或甲方未支付的货款可以作为上述违约金的一部份、由甲方直接扣抵。
  2. **违约终止合同**

在补救违约而采取的任何其他措施未能实现的情况下，即在甲方发出的违约通知后30天内(或经甲方书面确认的更长时间内)仍未纠正其下述任何一种违约行为，甲方有权向乙方发出书面违约通知，甲方终止本合同：

* + - 1. 如果乙方未能在合同规定的期限内或双方另行确定的延期交货时间内交付合同约定的货物。
      2. 乙方未能履行合同项下的任何其它义务。
  1. **不可抗力**

因不可抗力造成违约的，遭受不可抗力一方应及时向对方通报不能履行或不能完全履行的理由，并在随后取得有关主管机关证明后的15日内向另一方提供不可抗力发生以及持续期间的充分证据。基本于以上行为，允许遭受不可抗力一方延期履行、部分履行或者不履行合同，并根据情况可部分或全部免于承担违约责任。

本合同中的不可抗力指不能预见、不能避免并不能克服的客观情况。包括但不限于：自然灾害如地震、台风、洪水、火灾；政府行为、法律规定或其适用的变化或者其他任何无法预见、避免或者控制的事件。

* 1. **合同纠纷处理方式：**

因本合同或与本合同有关的一切事项发生争议，由双方友好协商解决。协商不成的，任何一方均可选择以下方式解决：

1. 向 (甲方所在地)仲裁委员会申请仲裁；
2. 向有管辖权的人民法院提起诉讼。
   1. **其他约定**
3. 若在交付使用过程中，因乙方的质量或安装工艺等原因而造成甲方人员安全或其他损失的，乙方应承担全部赔偿责任。
4. 本采购项目的招标文件、中标人的投标文件以及相关的澄清确认函(如果有的话)均为本合同不可分割的一部分，与本合同具有同等法律效力。
5. 本合同未尽事宜，双方另行补充。
6. 本合同一式陆份，经双方授权代表签字并盖章后生效。甲方、乙方各执贰份，送(招标文件投标人须知前附表第8项所述的招标项目行政监督部门) 备案一份，送招标代理人存档一份，具有同等效力。

甲 方： 乙 方：

单位地址： 单位地址：

商务代表： 法定代表人：

委托代理人： 委托代理人：

手机/电话： 手机/电话：

开户银行： 开户银行：

账 号： 账 号：

见证单位：福建莆田兴鑫招标代理有限公司(盖章)

见证日期： 年 月 日

**第五部分 响应文件格式**

**响应报价投标文件**

**(封面)**

**项目名称：**

**项目编号：**

**(正本/副本)**

**投标人名称 ：**

**法定代表人姓名：**

**地址： 邮编：**

**电话： 传真：**

**网址：**

**电子邮箱：**

**投标代表(印刷体)： 签字：**

**手机： 日期 ：20 年 月 日**

**1.报价一览表**

**(报价部分需单独胶装成册密封)**

招标编号：

投标人名称：(全称并加公章) 货币单位：元人民币

|  |  |  |  |
| --- | --- | --- | --- |
| 合同包号 | 品目号 | 品目号投标总价 | 备注 |
| n |  |  |  |
|  |  |
| 合同包n投标总价 | (大写) 　　　　　(小写)￥： | |

投标人代表签名：

**响应技术商务文件**

**(封面)**

**项目名称：**

**项目编号：**

**(正本/副本)**

**投标人名称 ：**

**法定代表人姓名：**

**地址： 邮编：**

**电话： 传真：**

**网址：**

**电子邮箱：**

**投标代表(印刷体)： 签字：**

**手机： 日期 ：20 年 月 日**

**附件1**

**投标函**

**致：** (招标代理人)

根据贵方为 (项目名称) 项目及服务的报价邀请 (项目编号) ，签字代表 (全名、职务)经正式授权并代表报价人 (报价人名称、地址) 提交以下文件正本一份和副本叁份。

(1)报价一览表**(本表投标时需单独密封，技术商务部分不得体现)**

(2)简要说明一览表

(3)服务承诺

(4)资格证明文件

(5)按文件要求提供的全部文件

据此函，签字代表宣布同意如下：

1、报价人将按文件规定履行合同责任和义务。

2、报价人已详细审查全部文件，包括修改文件(如有的话)以及全部参考资料和相关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

3、本报价有效期自报价有效截止时间起90个日历日。

4、报价人在报价有效期内撤回报价，将按规定给予处罚。

5、报价人同意提供按照招标人可能要求的与其报价有关的一切数据或资料，完全理解招标人不一定要接受最低价的报价或收到的任何报价。

6、与本报价有关的一切正式往来通讯请寄：

地址： 电话： 传真：

手机： 报价代表姓名、职务：

报价人(加盖公章)： 日期： 年 月 日

**附件2**

**货物详细说明一览表**

项目编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 合同包 |  | 货物名称 |  | 规格 |  | 数量 |  |
| 详细配置、技术参数与性能说明： | | | | | | | |

报价人全称(加盖公章)：

供应商代表签字：

日期：

**附件3**

**技术货物要求和商务偏离表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 合同包 | 商品品目 | 技术要求货物内容 | 响应文件内容的技术要求服务内容 | 偏离说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：

1．只须对比偏离情况。

2．有规格、技术参数偏离的必须提供本表，如无偏离可不提供。

3．无提供偏离表的投标文件视为所提供产品完全满足询价文件要求；如在供货过程中发现产品与询价文件要求不符的，供应商必须承担所有责任。

报价人全称(加盖公章)：

供应商代表签字：

日期：

**附件4**

**质量及服务承诺**

福建莆田兴鑫招标代理有限公司：

我方针对项目编号为： 的 (项目名称) ，承诺以下售后服务：

1. 服务方面的其他承诺：
2. 其他优惠条件：

报价人名称：(全称并加盖公章)

报价人代表签名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

年 月 日

**附件5**

**5资质证明文件**

1.提供合格的营业执照副本、税务登记证、组织机构代码证或营业执照三证合一的复印件(需加盖单位公章)

**附件6**

6.1 近三年无重大违法记录承诺书

项目名称：

项目编号：

致： 有限公司

根据中华人民共和国国务院第658号文件的规定，特作如下声明：

一、我方在投标前3年内在经营活动中没有重大违法记录。

二、我方若被采购人确定为成交人，同意并接受各单位或个人的监督审查。

三、经查实我方若有虚假声明，同意采购单位对其保证金不予退还；并自觉接受政府采购管理部门的处罚，因在采购活动中出现违反本声明行为的给其他当事人造成经济损失的，按规定予以赔偿。如保证金不能弥补我方对采购人造成的损失，我方同意另行支付相应的赔偿。

四、我方自愿将本声明作为响应文件的组成内容。

五、本声明自签署之日起生效。

此声明是由（投标供应商全称） 以（法定代表人或其委托代理人） 为全权代表的身份提交的。

投标单位（全称并加盖公章）：

投标供应商代表签字：

日 期：

**6.2 需提供无行贿犯罪记录承诺（说明）函（供应商自行对其有无行贿犯罪情形进行说明或承诺，格式自拟）**

投标单位（全称并加盖公章）：

投标供应商代表签字：

日 期：

**附件7**

**法定代表人授权书(原件)**

兹有 (单位名称) 法定代表人 (姓名)，授权 (被授权人姓名)为 (项目编号及项目名称) 的报价代理人，以本公司名义处理一切与之有关的事宜。

本授权书仅对该项目有效，特此声明。

法定代表人签字：

被授权人签字：

被授权人身份证号码：

被授权人职务：

报价单位全称(加盖公章)：

日期： 年 月 日

**法定代表人身份证复印件**

**被授权人身份证复印件**

**附件8**

**投标人提交的其它资料**

投标人认为应提交的其他材料，可在此附件中提交。

报价人名称：(全称并加盖公章)

报价人代表签名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

年 月 日