**医院网络安全设备采购项目预算价调研公示**

**第一部分 须知前附表**

|  |  |
| --- | --- |
| **序号** | **主　　　要　　　 内　　　 容** |
| 1 | 调研报名公示开始时间： 2022年 9月　26　日上午9点00分北京时间  调研报名截止时间：2022年　9 月　30　日下午17点30分北京时间  (报名请携带加盖公章的项目文件回执单、营业执照复印件、公司简介)  调研会时间：具体调研会时间将另行通知 |
| 2 | 项目：医院网络安全设备采购项目预算价调研公示 |
| 3 | 文件正本　 1　份，副本　1 　份。 |
| 4 | 文件递交处：　福建省肿瘤医院 网络办会议室 |
| 5 | 上述时间、地点如有变动，以单位届时通知为准。 |

**地　址： 福建省福州市福马路420号省肿瘤医院科研楼四楼网络办**

**邮　编： 350001**

**电　话： 0591-83660063-8822**

**联系人：金工**

**一、采购内容**

|  |  |  |  |
| --- | --- | --- | --- |
| **合同包** | **项目名称** | **数量** | **预算价** |
| **1** | **医院网络安全设备采购项目** | **1项** | **215万元** |

**二、采购要求：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备规格** | **主要参数** | **数量** |
| **1** | **核心防火墙** | 1.2U标准机架式设备，模块化设计，最大支持30个千兆接口；标配6个千兆电口，4个千兆SFP接口，3个扩展槽，2个USB口，1个COM口，2T企业级硬盘，单电源；最大吞吐量≥20Gbps，并发会话≥500万，新建会话≥10万，VPN吞吐量≥800Mbps，三年质保。双电源  2.支持路由、网桥、单臂、虚拟网线以及混合部署方式；支持源地址转换、目的地址转换；  3.双机热备：支持VRRP协议，支持主主模式、主备模式，支持会话同步、策略同步、报文同步；  4.支持用户和用户组管理，支持批量添加用户，支持对不同用户配置不同的安全策略，包括访问控制、应用控制、入侵防护、病毒防护等安全策略；  5.支持网络资源分级管控，根据不同的资源等级分配不同的安全控制级别，只允许具有相应级别权限的用户访问；  6.支持抵御网站扫描、SQL注入、XSS、命令注入、CSRF、远程代码执行、JAVA反序列化、文件上传、目录跳转、WebsShell上传等Web应用攻击；  7.支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等；  8.支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测；提供预定义、自定义敏感信息的特征库。预订义特征应内置常见敏感信息的特征，且可自定义敏感信息特征，如身份证信息、邮箱、银行卡号、手机号等  9.支持丰富的WEB防护功能，能够对web源代码进行扫描，检查代码中的网页木马，网页挂马以及网页暗链，并支持自定义规则  10．与我院现有态势感知系统联动，实现主动式网络防御 | **2** |
| **2** | **无线防火墙** | 1.2U标准机架式设备，模块化设计，最大支持26个千兆接口+2个万兆接口；标配6个千兆电口，4个千兆SFP接口，2个SPF+万兆接口，2个扩展槽，2个USB口，1个COM口，1T硬盘，单电源；双电源；三年IPS、AV、应用识别特征库升级服务。三年硬件质保，三年系统软件升级服务。最大吞吐量≥15Gbps，并发会话≥240万，新建会话≥6万，VPN吞吐量≥400Mbps，IPS吞吐量≥1.5Gbps，防病毒吞吐量≥1.5Gbps，IPS+防病毒吞吐量≥1.3Gbps  2.支持路由、网桥、单臂、虚拟网线以及混合部署方式；支持源地址转换、目的地址转换；  3.双机热备：支持VRRP协议，支持主主模式、主备模式，支持会话同步、策略同步、报文同步；  4.支持用户和用户组管理，支持批量添加用户，支持对不同用户配置不同的安全策略，包括访问控制、应用控制、入侵防护、病毒防护等安全策略；  5.支持网络资源分级管控，根据不同的资源等级分配不同的安全控制级别，只允许具有相应级别权限的用户访问；  6.支持抵御网站扫描、SQL注入、XSS、命令注入、CSRF、远程代码执行、JAVA反序列化、文件上传、目录跳转、WebsShell上传等Web应用攻击；  7.支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等；  8.支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测；提供预定义、自定义敏感信息的特征库。预订义特征应内置常见敏感信息的特征，且可自定义敏感信息特征，如身份证信息、邮箱、银行卡号、手机号等  9.支持丰富的WEB防护功能，能够对web源代码进行扫描，检查代码中的网页木马，网页挂马以及网页暗链，并支持自定义规则  10．与我院现有态势感知系统联动，实现主动式网络防御 | **1** |
| **3** | **边界防火墙** | 1.2U标准机架式设备，模块化设计，最大支持26个千兆接口；标配6个千兆电口，4个千兆SFP接口，2个扩展槽，2个USB口，1个COM口，1T企业级硬盘，单电源；最大吞吐量≥10Gbps，并发会话≥150万，新建会话≥6万，VPN吞吐量≥400Mbps，IPS吞吐量≥1.5Gbps，防病毒吞吐量≥1.5Gbps，IPS+防病毒吞吐量≥1.3Gbps三年IPS、AV、应用识别特征库升级服务。三年硬件质保，三年系统软件升级服务。双电源  2.支持路由、网桥、单臂、  3.虚拟网线以及混合部署方式；支持源地址转换、目的地址转换；  4.支持链路聚合、支持PPPoE接入，支持ARP代理，VLAN子接口、VLAN、Trunk、802.3ad、STP。  5.支持和IDS/IPS联动、安全准入系统、数据库审计系统SAS联动，形成完善的安全防御体系，提供界面截图；  6.支持多ISP线路接入，支持链路主备切换和自动负载均衡，支持ARPing、Ping、HTTPing等多种方法进行链路状态检测  7．与我院现有态势感知系统联动，实现主动式网络防御 | **2** |
| **4** | **WEB墙** | 1.1U标准机架，标准配置6个千兆电口、2个扩展槽；整机最大可支持14个千兆接口；2个USB，1个控制口，1T硬盘。HTTP吞吐：400Mbps；HTTP新建连接（CPS）：4000/s；HTTP最大并发连接：50万；WEB防护：32个站点；DDOS防护：100个站点；防篡改：32个节点；三年质保,双电源  2.支持通过BGP方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置SNAT策略。  3.支持HTTP访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，过滤非法请求。  4.应能识别和阻断注入攻击，支持防扫描陷阱、爬虫防护，支持文件上传、下载过滤。  5.支持通过移动终端管理，不需要安装APP和第三方插件，通过手机浏览器即可,并可管理设备实现网站快速应急处置；  6．与我院现有态势感知系统联动，实现主动式网络防御 | **1** |
| **5** | **安全审计系统** | 1.1U标准机架，标准配置6个千兆电口，2个扩展槽、2个USB,1个控制口，1T硬盘；适用带宽≥400M，适用用户数≥800人，网络吞吐量4G，最大并发连接数120万，每秒最大新建连接数40000；三年质保。双电源  2．可通过策略对IP或用户进行白名单的控制，符合白名单规则的IP或用户不做行为控制和审计。  3．可自定义基于协议和端口的对象，可根据协议、端口、报文长度、报文特征、目的IP等信息自定义特征识别规则。  4．支持将特殊协议（如L2TP、GRE、LWAPP、CAPWAP等）的协议头剥离掉，对特殊协议封装内的原始数据进行认证、审计和控制。  5.支持基于组织结构的个人行为监控，包括：网页标题记录、发贴记录、网页评论记录、在搜索引擎上的搜索记录、网页文件上传记录、URL访问记录、即时通讯的登录信息/聊天内容/文件传输记录、邮件记录（详细内容、附件）、FTP登录信息/上传记录/下载记录。 | **1** |
| **6** | **数据库安全审计** | 1.2U,模块化设计，标配6个千兆电口，4个千兆SFP接口，3个扩展槽；可支持扩展4口/8口的千兆光或电模块、2口/4口万兆光模块，整机最大可支持34个1000M接口，4T硬盘，默认支持8个数据库实例；最大日处理10000W条SQL明细；入库速度：8000(条/秒)；峰值事务处理能力：40000(条/秒)；日志存储量:16亿条  2.支持在IPV6环境下部署和管理，且支持在纯IPV4环境、纯IPV6环境及IPV4与IPV6混杂环境下对数据库操作行为进行审计，同时产品自身支持以IPV6方式进行管理。  3.除支持Oracle，Microsoft SQL Server，DB2，Sybase, Informix、MySQL、Caché、Teradata、MongoDB等数据库以外，还需支持人大金仓（Kingbase）、达梦(DM)、南大通用、神通等国产自主数据库的审计。可准确分析出这些数据库的协议，并支持对多种不同类型和不同版本的数据库的同时审计  4.支持对审计数据的多种响应方式，包含过滤、记录、windows消息、邮件、syslog、SNMP、屏幕录像、网关联动等多种事件告警和提示方式，第一时间向负责人发送告警信息  5.支持事件告警，发现异常或非法行为。提供事件追踪页面，通过事件关联追踪排查事件，多维度定位事件状态，包括地点追踪、屏幕录像，且屏幕录像与改事件一样对应。支持快捷规则配置，如，将此类语句设为安全、设为统方等； | **1** |
| **7** | **网络入侵检测系统** | 1.2U标准机架式设备，模块化设计，标配6个千兆电口，4个SFP接口，3个扩展槽；2个USB口，1个COM口，128G SSD固态盘，4T企业级硬盘；包含威胁监测、资产发现、资产风险分析、黑客画像功能。每秒TCP新建连接数≥18万，最大TCP并发会话数≥200万，整机吞吐率≥10Gbps，IDS吞吐率≥5Gbps。  2展示选定时间内的攻击趋势、攻击总数、攻击源IP Top10、攻击目的IP Top10、攻击协议统计、攻击严重性统计、攻击类型统计、攻击详情；  3展示选定时间内的文件检测威胁趋势、危险文件总数、危险文件下载源IP Top10、危险文件下载目标IP Top10、病毒文件类型、文件关联邮箱、文件关联URL、文件报告列表，提供病毒文件样本下载功能；  4展示选定时间内的扫描探测趋势、扫描探测总数、扫描探测源IP Top10、扫描探测目的IP Top10、扫描探测详细信息；  5支持展示选定时间内的恶意外联趋势、恶意外联总数、恶意外联活跃域名统计 Top10、恶意外联源IP Top10、恶意外联关系图、恶意外联类型、恶意外联详细信息  5、与我院现有态势感知系统联动，实现主动式网络防御 | **1** |
| **8** | **双因素认证设备** | 2\*10核 CPU，64G内存，4T\*4机械硬盘，标配4千兆电口，2万兆光口（含2个多模光模块），冗余电源，提供3个扩展槽位，可扩展：2千兆电、4千兆电、2万兆光；支持本地身份管理、权限管理、会话管理、资源统一发布、风险响应等功能，支持与第三方认证服务、权限服务对接实现零信任体系的身份和权限控制，支持与AiThink等平台对接实现零信任体系的持续信任评估，支持高可用集群部署 | **1** |

**三、为保障网络稳定性与兼容性，**

上述序号1-7设备为同一品牌，本次预算调研设备品牌为安恒、启明星辰、黑盾。

上述序号8设备,本次预算调研设备品牌为安恒、启明星辰、黑盾。

**四、调研说明：**

1、本次报名截止时间为2022年9月30日下午17点30分北京时间；(报名请携带加盖公章的项目文件回执单、营业执照复印件、公司简介)

2、调研会时间：具体调研会时间将提前3个工作日另行通知；

3、本预算价调研会的会议结论仅做为本项目公开招标的预算限价；

4、本预算价调研会不做参与投标的限制条件；

5、上述各参数将做为本项目招标的主要参数，不代表本项目公开招标的最终参数；

6、本项目实施主要工作为：上述各设备及信息的所需线缆与配件的安装调试、上架、设备集成等硬件安装工作，同时必须结合医院现有网络拓扑，实施等保安全配置等各项工作；

7、本预算价应包含设备价格、实施费用、集成费用及3年保修期内的维修及服务费用等，本预算价为含税开票价格；

8、必须对所有设备进行报价，不得缺项。报价格式见附件；

10、参加公司应准备PPT材料（含产品介绍、服务及集成能力、应用案例等），文件正本1份，副本1份，每公司讲解时间30分钟；

11、欢迎供应商、集成商、厂商前来参与，每一品牌限前2名报名。

**项目文件回执单**

**请各公司在一周内将此项目文件回执单送到“福建省肿瘤医院网络办”。**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **公司名称** | **产品名称** | **报价** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

**公司名称：**

**联系人：**

**联系电话：**

**邮箱号：**

**公司盖章：**

**2022年　月　日**报价格式

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备规格 | 主要参数 | 是否满足 | 品牌 | 数量 | 单价 | 金额 | 备注 |
|  |  |  |  |  |  |  |  |  |
| 工程实施费 | | | | | |  | |  |
| 合计（上述金额为含税开票金额） | | | | | |  | |  |

注：表格项目应按主要参数表中的序号、设备规格顺序进行对应报价。