**[信息安全等级保护整改]**

**采购项目市场调查公告**

各供应商：

我院信息安全等级保护整改采购项目现进入市场调查阶段，欢迎符合资格条件的供应商前来报名参与。我院将根据市场调查的结果，邀请符合我院需求的供应商进行院内邀请论证（谈判）会，具体时间另行通知。本项目不属政府采购类。

**一、采购项目概况：**

1、项目名称：信息安全等级保护整改

2、项目编号：FSSZYYZWCG2023110601

3、项目预算金额：63万元。

4、用户需求：详见附件1

**二、报名供应商资格要求：**

1、供应商必须具有独立法人资格，能独立承担民事责任和合同义务。

2、供应商必须具有有效的中华人民共和国企业法人营业执照，执照中必须具有本项目的经营范围。

3、具有良好的商业信誉和健全的财务会计制度。

4、供应商须具备履行合同的设备和专业技术能力。

5、供应商须未被列入“信用中国”网站(www.creditchina.gov.cn)以下任何记录名单之一：①失信被执行人；②重大税收违法案件当事人名单；③政府采购严重违法失信行为。

6、供应商应遵纪守法、诚信经营，近三年内（自本公告发布之日起往前推三年）无违规违法行为或采购活动中无不良记录。

7、本项目不接受联合体参与。

**三、网上公告时间及报名时提交的文件要求**

1、公告时间：公告时间：自发布次日起5个工作日内。

2、报名时需提交的文件（A4纸，双面打印并按照以下顺序装订完整并每页加盖公章）：

（1）报名资料封面（格式见附件2）。

（2）报名文件目录（格式见附件3）。

（3）企业法人营业执照（副本）复印件。营业执照经营范围如注明“具体经营项目请登录商事主体信息公示平台查询”的，须打印商事主体信息公示平台查询页。

（4）税务登记证书（国、地税）复印件。

（5）组织机构代码证复印件。

（6）如已办理营业执照、税务登记证、组织机构代码证三证合一的企业，请提交加载法人和其他组织统一社会信用代码的营业执照复印件。

（7）自行登录“信用中国”网站([www.creditchina.gov.cn](http://www.creditchina.gov.cn))，下载并打印《信用信息报告》（下载日期应在本公告发布日期之后）。

（8）参与人如为法人代表，须提交供应商法人代表证明书（格式见附件4）法人代表第二代居民身份证复印件（原件备核）。参与人如为授权代理人，须提交供应商法人代表证明书及法人代表第二代居民身份证复印件、法人授权书（格式见附件5）、授权代理人第二代居民身份证复印件（原件备核）及授权代理人近三个月社保缴费证明。

（9）提供遵纪守法、诚信经营、近三年内（自论证公告发布之日起往前推三年）无违规违法行为或采购活动中无不良记录的承诺书。（格式见附件6）。

**四、响应文件的递交（文件随谈判会当日自行携带入场提交）**

**（1）提供详细的《信息安全等级保护整改方案书》，请严格按照以下排序内容进行编制，需编制封面（封面需包含项目名称和项目编号、供应商名称、授权代表姓名及联系电话）、目录及页码；本方案书一式五份（一正四副，加盖公章），随论证（谈判）会当日自行携带入场提交；方案书内容需包含但不限于以下内容：**

①技术响应表（格式见附件9，标记“▲”的技术参数需提供相关材料）

②项目设计方案 （供应商提供技术方案，项目背景理解与分析，设计方案包括但不限于整体流程、技术方法和服务方案设计等。）

③实施方案（供应商提供实施方案，实施方案包括但不限于安装调试人员安排、 安装调试计划、流程、安装调试、安全服务执行方案、阶段性文档提交、验收标准、质量保证和风险规避措施等。）

④售后服务（供应商提供售后服务内容，包含服务措施、后期维护服务措施、售后响应时间、售后服务承诺等。）

⑤资质证书（供应商提供资质证书包含ISO9001质量管理体系认证、ISO27001信息安全管理体系认证、ISO20000信息技术服务管理体系认证证书、CCRC信息系统安全运维服务资质认证、CCRC信息系统安全集成服务资质认证。）**注：须提供有效证书复印件或扫描件并加盖供应商公章，不提供不得分。**

⑥供应商拟投入本项目的人员情况（A.项目经理：具备高级信息系统项目管理师证书、具有注册信息安全专业人员CISP、信息安全保障人员证书CISAW认证（认证范围为：风险管理、安全集成、安全运维）、系统规划与管理师、ITIL Managing Professional认证;

B.技术负责人：本科或以上的学历、高级信息系统项目管理师、具有注册信息安全专业人员CISP、信息安全保障人员证书CISAW认证（认证范围为：风险管理、安全集成、安全运维）；C.其他技术人员：信息安全保障人员认证、ITIL 认证证书、中级网络工程师、系统集成项目管理工程师）；**注：供应商必须提供该成员有效资质证书复印件材料并加盖供应商公章，并提供该成员在项目公告截止时间前半年内连续三个月的社保证明复印件材料并加盖供应商公章。**

⑦供应商自2020年1月1日至今同类信息安全服务业绩复印件，最少提供4份（格式见附件7），须提供合同关键页，关键页包括采购内容、签订日期 、双方盖章等;且针对每项合同（或业绩），需提供由客户签名盖章的验收合格资料或者由客户签名盖章的用户满意度评价，且必须为验收合格或满意程度为满意以上或类似的好评。

**备注：**

**1、供应商提交的材料必须真实可靠，如经核实为虚假材料的，将取消其报名资格并列入医院供应商诚信黑名单。**

**2、请供应商按照上述第三点第2条要求，提交纸质资料（一式一份），所提交的文件资料必须在有效期内，复印件需清晰并加盖公章，否则将会被取消资格。**

**3、供应商不得串通围标，如发现有串通围标行为将取消其参与项目资格并列入医院供应商诚信黑名单。（串通定义见《政府采购法实施条例》第七十四条,中华人民共和国财政部令第87号--政府采购货物和服务招标投标管理办法第三十七条）。**

**五、报名交资料时间**

公告时间：自发布次日起5个工作日内。

**六、联系方式**

1、采购人：佛山市中医院

2、地 址：佛山市禅城区亲仁路6号自编10号楼二楼采购办公室

3、联系电话：(0757)83067026传真：(0757)83067026

4、电子邮箱：740329062@qq.com

5、联系人：李小姐

佛山市中医院

2023年11月7 日

**附件1：**

**[信息安全等级保护整改]项目用户需求书**

**一、项目概述**

根据《信息安全等级保护管理办法》要求，佛山市中医院对相关信息系统进行年度测评整改，进一步增强医院信息系统安全防护能力，确保系统安全稳定运行。

现拟对我院备案系统进行整改服务，主要服务内容如下：

1. 现场协助医院完成等级保护测评资产收集、资料准备、项目整体协调等工作，为信息系统开展等级保护定级备案、安全风险梳理、指导等级保护安全整改和加固。等级保护辅助服务需供应商全程协助医院完成等级保护测评工作，直至完成测评。
2. 医院信息安全管理制度、应急预案的修订服务；
3. 硬件设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品类型 | 数量 | 维保年限 |
| 1 | 下一代防火墙 | 2台 | 含三年软硬件维保升级服务 |
| 2 | Web防火墙 | 1台 | 含三年软硬件维保升级服务 |
| 3 | IDS入侵检测 | 1台 | 含三年软硬件维保升级服务 |

**二、技术要求**

1、整改服务要求：

（1）协助测评

供应商的安全顾问或项目经理需配合测评机构的现场测评工作。安全顾问需陪同用户技术人员配合现场测评工作，协助回答测评人员问题，协助完成信息系统通过国家等级保护的相应测评。

（2）准备资料

在用户向测评机构申请测评后，安全顾问需根据测评要求，协助补充和准备测评所需的文档资料，如机房安全管理制度及相关记录、安全职责书说明、安全漏洞检测和系统升级管理制度及相关记录、权限管理制度及相关记录、备份制度及相关记录、防病毒管理制度和记录、第三方人员管理制度、安全事件报告制度、应急管理制度和应用预案等，确保符合国家等级保护测评需要。

（3）测评问题单整改

供应商根据测评机构提出的不符合项问题单进行梳理，提供技术服务并落实安全设备对医院的信息系统实施整改工作使之符合测评要求。

（4）问题整改确认

供应商在根据医院信息系统的测评不符合项逐一整改完成后，提供整改确认服务，具体至少包含：安全漏洞扫描、安全基线核查、渗透测试复查和再次测试、安全管理体系落地性审核、非应用系统的整改包括但不限于操作系统补丁、数据库补丁等（若涉及停机则医院协调停机时间）。整改确认过程中所需使用的工具由供商提供并出具购买证明或远程授权证明，避免实施过程产生的授权纠纷。

（5）现场协助

安全顾问需陪同医院技术人员配合现场测评工作，协助回答测评人员问题，协助医院完成主要信息系统通过国家等级保护的相应测评。

2、硬件设备清单参数要求

1. 下一代防火墙

|  |  |
| --- | --- |
| **技术指标** | **指标项** |
| ▲硬件和性能要求 | 标准架式设备，网络吞吐率≥20Gbps，IPS入侵防御吞吐量≧10Gbps；防病毒吞吐≧5Gbps；最大并发连接数≧300万；每秒新建会话数≥16万，配置业务端口≥8个千兆电口，≥4个千兆光口，≥8个万兆光口，1个空置扩展槽，1个console口，配置≥4T 硬盘，标配冗余电源。**（请提供截图证明）**  本次配置需开通≥3年病毒防护特征库、入侵防御特征库、URL分类特征库、应用识别库等升级服务，IPSec VPN（并发隧道数）≥25个，SSL VPN（并发用户数）≥25个。**（请提供截图证明）** |
| 部署模式 | 支持路由模式、透明（网桥）模式、混合模式、旁路模式； |
| ▲智能链路负载均衡 | 必须支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发；必须支持智能DNS提供入站负载均衡；必须支持基于源、基于源和目的、基于会话等多种负载均衡模式**（请提供截图证明）** |
| IPv6支持 | 设备接口支持配置IPv6地址，并可使用IPv6地址管理设备；支持IPv6手动及自动的IP/MAC探测及绑定； |
| 支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别、反间谍软件等安全功能 |
| VPN | SSLVPN支持安卓、IOS、MAC OS、windows、linux等平台的客户端 |
| 入侵防御 | 支持漏洞防护功能，并且漏洞特征库能细化分类，例如跨站脚本、SQL注入等，其中漏洞特征库可以至少查看攻击名称、CWEID、类型以及对应解决方案建议等信息，以及能针对发现的入侵行为至少满足记录日志、阻断、放行、重置等行为。 |
| Web防护 | 所投产品必须支持web防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类； |
| 病毒防护 | 支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持压缩文件查杀，支持设置例外特征，对特定的病毒特征不进行查杀。 |
| 数据包路径检测 | 防火墙支持数据包路径检测，可模拟数据包穿越设备，对设备的各个功能模块进行有效性检测，非传统意义的debug功能。  兼容并通过图形化以及文字描述的方式将检测过程及检测结果呈现给用户，以便快速的进行故障定位。  可检测的数据包来源包含模拟数据包、实时在线数据包。支持对检测结果以报告的形式导出，供管理员分析。 |
| 云端智能威胁检测 | 具有已知以及未知威胁的检测能力，支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能。 |
| SSL解密 | 所投产品必须支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计 |
| 高可用 | 支持A-S模式，A-A模式；支持NAT场景的非对称流量，同时支持BFD for static，ospf，BGP，保证网络的快速收敛 |
| ▲运维管理 | 支持将告警信息以SNMP Trap、邮件、声音、短信、安全运维APP等形式通知管理员，告警信息的范围不限于配置变更、病毒事件、攻击事件、失陷主机告警、CPU利用率、内存利用率、硬盘利用率等**（请提供截图证明）** |
| 支持在线抓包功能，可基于源地址、目的地址、协议、应用等参数配置抓包条件；**（请提供截图证明）** |
| 产品资质 | 要求提供国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）资质证书扫描件 |

1. Web应用防火墙

|  |  |
| --- | --- |
| **技术指标** | **指标项** |
| ▲硬件和性能要求 | 专用Web硬件防火墙，非防火墙、UTM、IPS设备，具备独立自主知识产权，标准机架式设备**（请提供截图证明）** |
| 管理接口：10/100/1000Mbps RJ45口\*1、RJ45 Console\*1，USB接口\*2,1个HA口**（请提供截图证明）**  业务接口：≥2个万兆光；≥8个千兆光；≥1个空闲接口扩展槽位，冗余电源，硬盘配置≥128GB SSD；**（请提供截图证明）** |
| 网络层最大吞吐量≥40Gbps；http最大吞吐量≥4.5Gbps；  http每秒新建事务数≥95,000；http最大并发连接数≥5000,000。**（请提供截图证明）** |
| 提供至少三年产品升级维保质保服务**（请提供截图证明）** |
| 部署要求 | 支持旁路镜像、透明代理、透明桥、路由代理和反向代理部署 |
| 支持双机HA模式。支持配置信息同步。 |
| 功能要求 | 具备http协议深层解码能力，支持递归解码，解码方式包括：URL解码、JSON解码、Base64解码、16进制转换、斜杠反转义、XML解析、PHP反序列化解析、UTF-7解码；  支持从 XFF 中解析 ‘[IPv6]’ 格式的地址信息 |
| ▲具备网页防篡改功能。配置静态网页缓存和篡改监控功能，在检测到篡改发生时，可以将篡改前的缓存页面返回给用户。**（请提供截图证明）** |
| 攻击检测：  具有独立防护能力的具有自主知识产权的智能分析检测引擎 |
| 支持SQL注入攻击检测； |
| 支持SQL非注入型攻击检测； |
| ▲具有漏洞扫描及防护功能，所投WAF应具备WEB漏扫功能，并且能够在扫描完成之后，根据扫描结果，新建虚拟补丁策略。**（请提供截图证明）** |
| 支持XSS注入检测，通过分析Html片段的DOM结构，解析存在的JS片段，进行智能分析，根据分析结果评估威胁等级并阻断； |
| 支持机器人检测，能够识别扫描器检测、爬虫检测、非浏览器请求； |
| 支持文件上传、文件包含攻击检测；  支持代码注入、命令注入攻击检测，支持检测上传文件中是否包含Java、Php代码注入信息； |
| 支持服务器响应信息检测，防止响应错误信息包含服务器列目录、SQL报错、服务器异常信息等； |
| ▲具备0day漏洞防护能力，实现告警和拦截；**（请提供截图证明）** |
| 支持访问审计功能，能够记录、查询所有用户对网站的访问情况 |
| 支持反序列化攻击检测，支持PHP、JAVA语言的反序列化攻击检测，能够识别相关程序语言的序列化流并进行分析、解码，进行告警和阻断； |
| 支持CSRF和SSRF检测，通过分析Payload代码特征，告警并阻断相关请求； |
| 支持深度检测功能，可在站点详情中的防护配置页面开启深度检测，即使该请求已在检测过程中已被判断为拦截，仍可继续进行所有攻击检测模块的检测，完整地记录攻击检测信息记录，便于进行更完整的分析 |
| 支持自定义基于正则表达式的防护规则；  支持设置检测前解码，在自定义规则时，支持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。 |
| 支持访问IP溯源，能够从Socket、X-Forwarded-For和任意Http头中获取访问源IP； |
| 支持在线查看报告，支持PNG、PDF、HTML等多种格式的报告下载和外发。 |
| 支持站点全量访问日志的完整记录功能，属性包括：站点信息、访问地址、源IP、请求方法、响应码、请求开始时间；查看详情功能提供分类查看日志详情，可分为访问日志详情、请求检测信息、响应检测信息、HTTP响应展现。 |
| 支持IP组功能，进行配置的模块包括：自定义规则-匹配条件、访问频率控规则、不限制这些用户以及源IP获取方式-信任IP； |
| 支持Cookie防篡改，可配置三种防护方式，结合“观察”和“拦截”两种响应方式； |
| 支持设备信息实时监控，监控数据包括CPU使用率、内存使用率、磁盘使用率、网络读写、每秒新建连接数、每秒检测请求数； |
| 管理界面可见bypass状态；  支持流量镜像阻断功能，按照实际防护监测选择是否开启流量阻断； |
| 透明代理支持主动链路探测，链路故障时主动进行bypass，保障主备场景下链路切换时业务正常。 |
| 支持后端Web服务器集群的负载均衡，支持加权轮训法、最小连接数法和源地址哈希法三种调度策略； |
| 报表功能 | 支持定时报表，并外发至FTP服务器或管理员邮箱 |
| 提供大屏展示功能，可展示地理威胁分布、威胁事件类型、热点威胁事件、风险站点排名、WEB整机流量等内容。 |
| 产品成熟度 | 产品具有《计算机信息系统安全专用产品销售许可证》  （须提供以上有效期内的资质证书） |

1. IDS入侵检测要求

|  |  |
| --- | --- |
| **技术指标** | **指标项** |
| ▲硬件规格 | 标准机架式硬件设备，自适应电口≥8个10/100/1000，千兆SFP插槽≥8个千兆SFP插槽，万兆SFP+插槽≥4个，网络层吞吐量≥20Gbps，IDS吞吐量为≥12.5Gbps，最大并发连接数≥500万，硬盘配置≥1T ，冗余电源**（请提供截图证明）** |
| 产品部署 | 产品具备接口配置IPv6地址功能，包括接口名称、IP地址/掩码、地址类型和IPv6路由通告，并可以显示当前本机的IPv6邻居信息 |
| 产品具备透明接入、旁路部署等多种部署模式 |
| ▲入侵检测 | 支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测；**（请提供截图证明）**  支持HTTP Get、Head、Put、Post等多种协议方法检查；**（请提供截图证明）** |
| 支持自定义入侵检测特征：可依据TCP、UDP、SMB、HTTP等网络层的各项参数设置自定义特征；全面设置TCP/IP应用层的特征比对内容而不受通信协议限制；支持跨数据包检测机制，包括：比对位移(matching offset)、比对长度(matching depth)、比对距离(matching distance)、比对范围(within)；支持基于流的数据包(stream-based)比对技术； **（请提供截图证明）** |
| 支持威胁详情URI和攻击数据解码；支持IPv6环境下入侵检测；支持IPv6威胁日志显示和下载；**（请提供截图证明）** |
| ▲Web防护 | 系统具备对网站外链检测功能；系统具备对CC攻击的检测；系统具备对跨站脚本攻击的检测能力；系统具备对SQL注入攻击的检测能力；**（请提供截图证明）** |
| 产品功能 | 产品具备IP/MAC绑定功能，支持手动添加和自动探测IP/MAC对应关系 |
| 产品具备DNS自学习安全缓存、DNS静态缓存功能来检测DNS欺骗、缓存污染、DNS劫持等DNS攻击行为 |
| 产品具备高级访问控制列表功能，可对源及目的MAC、报文头部信息（SYN标志、分片标志、TTL、DSCP、Precedence、TOS）、内网域地址、外网域地址、长连接超时时间等细粒度项进行配置 |
| 产品具备基于地域的访问控制列表功能，支持根据国家、地区等元素进行地域访问检测 |
| 产品具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IDS、可视、概览等多项元素实现快速配置上线 |
| 产品提供入侵检测特征库，特征数超过10000条。并提供基于正则表达式匹配方式的自定义特征检测策略 |
| 产品具备云端威胁情报功能，提供僵尸网络、钓鱼网站、恶意网站等10大类的威胁情报的检测，并对检测到的威胁事件执行记录日志、邮件、声音等动作 |
| 产品具备暴力破解检测功能，提供基于SMTP/IMAP/POP3/TELNET/FTP/RLOGIN/NNTP/TDS-MS-SQL等协议类型的频率检测机制 |
| 产品具备流量自学习功能，通过设置流量学习时间，通过报文、IP排名、域名统计类型建立网络流量基线 |
| 设备具备URL检测功能，用于对用户访问的网址进行检查，支持关键字和正则两种检测方式 |
| 产品具备关键字检测功能，支持基于论坛发帖、邮件协议、TELNET、DNS、RSH、FTP、HTTP协议的关键字检测功能 |
| 口令防护 | 支持对ftp、telnet、smtp、pop3、imap弱口令行为进行检测  支持对ftp、telnet、smtp、pop3、msrpc、sunrpc暴力破解行为检测 |
| 产品资质要求 | 所投产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》 |

**三、商务要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **商务条款** | **要求** |
| 1 | **供货渠道** | 1、所有产品均由制造商或其授权的分销机构所提供，具有合法透明的供货渠道，成交供应商及制造商须提供其产品品质和一切售后服务保障。 |
| 2 | **报价要求** | 1、报价不高于本项目的预算金额。  2、报价方式为广东省佛山市目的地竣工验收交付价。  3、报价中须包含整个项目的货物购置、安装、调试、培训辅导、质保期售后服务、全额含税发票等合同实施过程中的应预见和不可预见所有费用。 |
| 3 | **知识产权** | 1、供应商必须保证，我院在中华人民共和国境内使用标的货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向我院提出侵犯其专利权、商标权或其它知识产权的主张，该责任应由供应商承担。  2、报价应包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。 |
| 4 | **服务地点** | 我院（用户）指定地点。 |
| 5 | **项目实施要求** | 1、供应商须向我院提供详细的项目实施计划，包括实施进度、任务分工、管理及风险控制措施等。  2、在项目实施过程中，供应商需服从我院的组织、协调、监督、管理。  3、供应商需根据项目进展及时向我院报告。 |
| 6 | **工期** | 建设期限：自合同签署生效之日起至2023年12月31日内提供及安装调试完毕和交付，直至完成医院信息系统的测评； |
| 7 | **验收要求** | 1、我院组织相关部门严格依据项目标的参数、数量、品牌、规格型号（如有）等进行验收，如发现货品不符合要求时，供应商应无条件退货或换货。  2、实施项目通过试运行正常后，双方共同验收并出具验收报告。  3.供应商按照项目的要求，在规定时间内完成系统设计、研发、安装实施、测试、调试、验收等工作，并向采购人提交项目应用系统。若由于供应商原因，导致项目延误，每周每次扣除合同总金额的 5‰ 。  4.系统验收：对整个项目的验收包括检查整个系统是否实现了采购人要求的全部功能，是否满足招标文件、合同、系统需求规格说明书及双方签署的补充文件的要求。  5. 文档验收：供应商提交文档须符合验收文档要求，包括但不限于以下文档：《项目实施方案》、《设备安装手册》、《设备维护手册》、《设备用户操作手册》、《试运行总结报告》、《系统培训记录》、《开发进度月报》及采购人需要的其他文档。 |
| 8 | **售后服务要求** | 1、免费质量保修期限：三年。保修期限按项目验收采购人签字完成日起开始计算。期满后每年维保费不高于合同价5%，需另签合同。  2、保修服务内容：电话、网络等热线技术支持服务；7\*24小时响应。  3、现场技术支持服务：供应商维护人员需在接到维修通知24小时内响应，并在48小时之内把所出现的质量问题维修完毕。 |
| 9 | **培训要求** | 培训对象包括用户单位系统，如系统管理员、医师、科室主任等角色；通过培训使用户方能独立操作、维护、管理，从而使用户方能独立进行管理、故障处理、日常测试维护等日常工作，确保系统能正常安全运行。供应商必须作出培训承诺，含培训计划、培训内容、培训方法、培训时间、培训地点等。 |
| 10 | **付款方式** | 1、付款方式：分三期支付,首期：合同生效后，自收到完税发票之日起30个工作日内，支付合同款20%；二期：项目整体验收，双方签署验收报告后，自收到完税发票之日起30个工作日内，支付合同款75%；尾期：质保期满后，自收到完税发票之日起30个工作日日内，支付合同款5%。  2、收款方、出具发票方、合同乙方均必须与成交供应商名称一致。 |

**附件2：**

**佛山市中医院总务科采购项目**

**报名文件**

**项目名称：**

**项目编号：**

**供应商名称（加盖公章）：**

**联系人姓名：**

**联系电话（手机）： 座机：**

**E-mail：**

**日 期： 年 月 日**

**附件3**

**报名文件目录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 投标资料 | | 页码 | 审核情况（√） | 备注 |
| 1 | 三证合一的营业执照复印件 | |  |  |  |
| 或 | 企业法人营业执照（副本）复印件 |  |  |  |
| 税务登记证书（国、地税）复印件 |  |  |  |
| 组织机构代码证复印件 |  |  |  |
| 2 | 商事主体信息公示平台查询页（营业执照经营范围如注明“具体经营项目请登录商事主体信息公示平台查询”） | |  |  |  |
| 3 | 《信用信息报告》 | |  |  |  |
| 4 | 法人代表证明书 | |  |  |  |
| 5 | 法人代表第二代居民身份证复印件 | |  |  |  |
| 6 | 法人授权书 | |  |  |  |
| 7 | 授权代理人第二代居民身份证复印件 | |  |  |  |
| 8 | 授权代理人近三个月社保缴费证明 | |  |  |  |
| 9 | 提供遵纪守法、诚信经营、近三年内（自论证公告发布之日起往前推三年）无违规违法行为或采购活动中无不良记录的承诺书。（格式见附件6）。 | |  |  |  |
| 10 | **《方案书》一式五份（一正四副加盖公章），随论证（谈判）会当日自行携带入场提交。** | |  |  |  |

**附件4：**

**法定代表人资格证明书**

**佛山市中医院：**

同志，现任我单位职务，联系手机：，为法定代表人，代表我单位参与贵单位以下项目的采购活动，特此证明。

项目名称：

项目编号：

法定代表人（亲笔签名或签章）：

签发日期：年月日 单位名称（加盖公章）：

|  |  |  |
| --- | --- | --- |
| **法定代表人身份证**  **复印件正面粘贴处** |  | **法定代表人身份证**  **复印件反面粘贴处** |

说明：

1.法定代表人为企业事业单位、国家机关、社会团体的主要行政负责人。

2.须提供第二代居民身份证双面复印件，并加盖供应商公章。

**附件5：**

**法人授权书**

**佛山市中医院：**

我单位特授权委任 (姓名)现职员工，作为我方代表，参与贵方的采购项目，对该代表人所提供、签署的一切文书均视为符合我方的合法利益和真实意愿，我方愿为其行为承担全部责任。

项目名称：

项目编号：

有效期限：自本单位盖章之日起生效。

供应商名称（加盖公章）：

法定代表人（亲笔签名或签章）：

授权代理人（亲笔签名）： ，联系手机电话：

授权生效日期：年月日

|  |  |  |
| --- | --- | --- |
| **授权代理人身份证**  **复印件正面粘贴处** |  | **授权代理人身份证**  **复印件反面粘贴处** |

说明：1.本授权书内容不得擅自修改。

2.须提供第二代居民身份证双面复印件，并加盖投标人公章。

3.内容必须填写真实、清楚、涂改无效，不得转让、买卖。

**附件6：**

**承诺书**

我公司在参加本次采购项目活动中，作出如下承诺：

一、参加本次采购活动前三年内，在经营活动中没有重大违法记录。

二、未挂靠、借用资质进行投标等违法违规行为。

三、提供的相关文件均真实、有效。

若发现我方存在上述问题，愿参照政府采购相关规定接受处罚并列入医院供应商诚信黑名单。

供应商名称（加盖盖章）：

日期：

**附件7：**

**拟提供的业绩**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **客户名称** | **项目名称及合同金额**  **（万元）** | **合同签订时间** | **联系人及电话** | **备注** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| … |  |  |  |  |  |

供应商名称（加盖公章）：

授权代理人签字：

日 期：年月日

注：供应商未按上表和要求填报的，视为2020年1月1日起至今无用户。

**附件8：**

**报价书**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **数量** | **维保年限** | **单价（元）** | **小计（元）** |
| 1 | 下一代防火墙 | 2台 | 含三年软硬件维保升级服务 | ¥ | ¥ |
| 2 | Web防火墙 | 1台 | 含三年软硬件维保升级服务 | ¥ | ¥ |
| 3 | IDS入侵检测 | 1台 | 含三年软硬件维保升级服务 | ¥ | ¥ |
|  | 总计： | | | | ¥ |
|  | 大写：人民币 元 | | | | |
|  | 备注：  1、本项目预算金额：63万元。  2、供应商必须完全满足并响应本采购项目的用户需求书全部内容（除技术响应表内容）。  3、报价修正准则  ①　报名文件中报价表内容与报名文件中相应内容不一致的，以报价表为准。  ②　报价表大写金额和小写金额不一致的，以大写金额为准。  ③　单价金额小数点或者百分比有明显错位的，应以总价为准，并修正单价。  ④　总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。  ⑤　同时出现两种以上不一致的，按照上述规定的顺序修正。修正后的报价经报名人确认后产生约束力，报名人不确认的，其报价无效。  4、请严格按照本报价表报价，更改序号、物资名称、单位的报价单为无效报价单。  5、单项价格和总价超过本项目预算价为无效报价单。  6、本报价表纸质版，由供应商在院内论证（谈判）会当日自行携带入场。  7、人民币大写字：壹、贰、叁、肆、伍、陆、柒、捌、玖、拾、佰、仟、万、亿、元、角、分、零、整（正） | | | | |

　　　　　　　　　　　　 报价单位：（盖章）

年　 月　 日

**附件9：**

**技术响应表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购文件要求** | | **技术参数（是否响应）** | **备注** |
| **1** | 整改服务要求 | 1、协助测评：供应商的安全顾问或项目经理需配合测评机构的现场测评工作。安全顾问需陪同用户技术人员配合现场测评工作，协助回答测评人员问题，协助完成信息系统通过国家等级保护的相应测评。 |  |  |
| 2、准备资料：在用户向测评机构申请测评后，安全顾问需根据测评要求，协助补充和准备测评所需的文档资料，如机房安全管理制度及相关记录、安全职责书说明、安全漏洞检测和系统升级管理制度及相关记录、权限管理制度及相关记录、备份制度及相关记录、防病毒管理制度和记录、第三方人员管理制度、安全事件报告制度、应急管理制度和应用预案等，确保符合国家等级保护测评需要。 |  |  |
| 3、测评问题单整改：供应商根据测评机构提出的不符合项问题单进行梳理，提供技术服务并落实安全设备对医院的信息系统实施整改工作使之符合测评要求。 |  |  |
| 4、问题整改确认：供应商在根据医院信息系统的测评不符合项逐一整改完成后，提供整改确认服务，具体至少包含：安全漏洞扫描、安全基线核查、渗透测试复查和再次测试、安全管理体系落地性审核、非应用系统的整改包括但不限于操作系统补丁、数据库补丁等（若涉及停机则医院协调停机时间）。整改确认过程中所需使用的工具由供商提供并出具购买证明或远程授权证明，避免实施过程产生的授权纠纷。 |  |  |
| 5、现场协助：安全顾问需陪同医院技术人员配合现场测评工作，协助回答测评人员问题，协助医院完成主要信息系统通过国家等级保护的相应测评。 |  |  |

**2、硬件设备清单参数要求**

**1）下一代防火墙**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购文件要求** | | **技术参数（是否响应）** | **备注** |
| **技术指标** | **指标项** |
| 2 | 硬件和性能要求 | 6、▲标准架式设备，网络吞吐率≥20Gbps，IPS入侵防御吞吐量≧10Gbps；防病毒吞吐≧5Gbps；最大并发连接数≧300万；每秒新建会话数≥16万，配置业务端口≥8个千兆电口，≥4个千兆光口，≥8个万兆光口，1个空置扩展槽，1个console口，配置≥4T 硬盘，标配冗余电源。**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 7、▲本次配置需开通≥3年病毒防护特征库、入侵防御特征库、URL分类特征库、应用识别库等升级服务，IPSec VPN（并发隧道数）≥25个，SSL VPN（并发用户数）≥25个**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 3 | 部署模式 | 8、支持路由模式、透明（网桥）模式、混合模式、旁路模式； |  |  |
| 4 | 智能链路负载均衡 | 9、▲必须支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发；必须支持智能DNS提供入站负载均衡；必须支持基于源、基于源和目的、基于会话等多种负载均衡模式。**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 5 | IPv6支持 | 10、设备接口支持配置IPv6地址，并可使用IPv6地址管理设备；支持IPv6手动及自动的IP/MAC探测及绑定； |  |  |
| 11、支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别、反间谍软件等安全功能 |  |  |
| 6 | VPN | 12、SSLVPN支持安卓、IOS、MAC OS、windows、linux等平台的客户端 |  |  |
| 7 | 入侵防御 | 13、支持漏洞防护功能，并且漏洞特征库能细化分类，例如跨站脚本、SQL注入等，其中漏洞特征库可以至少查看攻击名称、CWEID、类型以及对应解决方案建议等信息，以及能针对发现的入侵行为至少满足记录日志、阻断、放行、重置等行为。 |  |  |
| 8 | Web防护 | 14、所投产品必须支持web防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类； |  |  |
| 9 | 病毒防护 | 15、支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持压缩文件查杀，支持设置例外特征，对特定的病毒特征不进行查杀。 |  |  |
| 10 | 数据包路径检测 | 16、防火墙支持数据包路径检测，可模拟数据包穿越设备，对设备的各个功能模块进行有效性检测，非传统意义的debug功能。 |  |  |
| 17、兼容并通过图形化以及文字描述的方式将检测过程及检测结果呈现给用户，以便快速的进行故障定位。 |  |  |
| 18、可检测的数据包来源包含模拟数据包、实时在线数据包。支持对检测结果以报告的形式导出，供管理员分析。 |  |  |
| 11 | 云端智能威胁检测 | 19、具有已知以及未知威胁的检测能力，支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能。 |  |  |
| 12 | SSL解密 | 20、所投产品必须支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计 |  |  |
| 13 | 高可用 | 21、支持A-S模式，A-A模式；支持NAT场景的非对称流量，同时支持BFD for static，ospf，BGP，保证网络的快速收敛 |  |  |
| 14 | 运维管理 | 22、▲支持将告警信息以SNMP Trap、邮件、声音、短信、安全运维APP等形式通知管理员，告警信息的范围不限于配置变更、病毒事件、攻击事件、失陷主机告警、CPU利用率、内存利用率、硬盘利用率等。**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 23、▲支持在线抓包功能，可基于源地址、目的地址、协议、应用等参数配置抓包条件； **（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 15 | 产品资质 | 24、要求提供国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）资质证书扫描件 |  | **请提供相应证书扫描件的页码** |

2）Web应用防火墙

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** |  | **采购文件要求** | **技术参数（是否响应）** | **备注** |
| **技术指标** | **指标项** |
| 16 | 硬件和性能要求 | 25、▲专用Web硬件防火墙，非防火墙、UTM、IPS设备，具备独立自主知识产权，标准机架式设备。**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 26、▲管理接口：10/100/1000Mbps RJ45口\*1、RJ45 Console\*1，USB接口\*2,1个HA口**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 27、▲业务接口：≥2个万兆光；≥8个千兆光；≥1个空闲接口扩展槽位，冗余电源，硬盘配置≥128GB SSD；**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 28、▲网络层最大吞吐量≥40Gbps；http最大吞吐量≥4.5Gbps；  http每秒新建事务数≥95,000；http最大并发连接数≥5000,000。**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 29、▲提供至少三年产品升级维保质保服务**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 17 | 部署要求 | 30、支持旁路镜像、透明代理、透明桥、路由代理和反向代理部署 |  |  |
| 31、支持双机HA模式。支持配置信息同步。 |  |  |
| 18 | 功能要求 | 32、具备http协议深层解码能力，支持递归解码，解码方式包括：URL解码、JSON解码、Base64解码、16进制转换、斜杠反转义、XML解析、PHP反序列化解析、UTF-7解码； |  |  |
| 33、支持从 XFF 中解析 ‘[IPv6]’ 格式的地址信息 |  |  |
| 34、▲具备网页防篡改功能。配置静态网页缓存和篡改监控功能，在检测到篡改发生时，可以将篡改前的缓存页面返回给用户**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 35、攻击检测：  具有独立防护能力的具有自主知识产权的智能分析检测引擎 |  |  |
| 36、支持SQL注入攻击检测； |  |  |
| 37、支持SQL非注入型攻击检测； |  |  |
| 38、▲具有漏洞扫描及防护功能，所投WAF应具备WEB漏扫功能，并且能够在扫描完成之后，根据扫描结果，新建虚拟补丁策略。**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 39、支持XSS注入检测，通过分析Html片段的DOM结构，解析存在的JS片段，进行智能分析，根据分析结果评估威胁等级并阻断； |  |  |
| 40、支持机器人检测，能够识别扫描器检测、爬虫检测、非浏览器请求； |  |  |
| 41、支持文件上传、文件包含攻击检测；  支持代码注入、命令注入攻击检测，支持检测上传文件中是否包含Java、Php代码注入信息； |  |  |
| 42、支持服务器响应信息检测，防止响应错误信息包含服务器列目录、SQL报错、服务器异常信息等； |  |  |
| 43、▲具备0day漏洞防护能力，实现告警和拦截；**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 44、支持访问审计功能，能够记录、查询所有用户对网站的访问情况 |  |  |
| 45、支持反序列化攻击检测，支持PHP、JAVA语言的反序列化攻击检测，能够识别相关程序语言的序列化流并进行分析、解码，进行告警和阻断； |  |  |
| 46、支持CSRF和SSRF检测，通过分析Payload代码特征，告警并阻断相关请求； |  |  |
| 47、支持深度检测功能，可在站点详情中的防护配置页面开启深度检测，即使该请求已在检测过程中已被判断为拦截，仍可继续进行所有攻击检测模块的检测，完整地记录攻击检测信息记录，便于进行更完整的分析 |  |  |
| 48、支持自定义基于正则表达式的防护规则； |  |  |
| 49、支持设置检测前解码，在自定义规则时，支持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。 |  |  |
| 50、支持访问IP溯源，能够从Socket、X-Forwarded-For和任意Http头中获取访问源IP； |  |  |
| 51、支持在线查看报告，支持PNG、PDF、HTML等多种格式的报告下载和外发。 |  |  |
| 52、支持站点全量访问日志的完整记录功能，属性包括：站点信息、访问地址、源IP、请求方法、响应码、请求开始时间；查看详情功能提供分类查看日志详情，可分为访问日志详情、请求检测信息、响应检测信息、HTTP响应展现。 |  |  |
| 53、支持IP组功能，进行配置的模块包括：自定义规则-匹配条件、访问频率控规则、不限制这些用户以及源IP获取方式-信任IP； |  |  |
| 54、支持Cookie防篡改，可配置三种防护方式，结合“观察”和“拦截”两种响应方式； |  |  |
| 55、支持设备信息实时监控，监控数据包括CPU使用率、内存使用率、磁盘使用率、网络读写、每秒新建连接数、每秒检测请求数； |  |  |
| 56、管理界面可见bypass状态；  支持流量镜像阻断功能，按照实际防护监测选择是否开启流量阻断； |  |  |
| 57、透明代理支持主动链路探测，链路故障时主动进行bypass，保障主备场景下链路切换时业务正常。 |  |  |
| 58、支持后端Web服务器集群的负载均衡，支持加权轮训法、最小连接数法和源地址哈希法三种调度策略； |  |  |
| 19 | 报表功能 | 59、支持定时报表，并外发至FTP服务器或管理员邮箱 |  |  |
| 60、提供大屏展示功能，可展示地理威胁分布、威胁事件类型、热点威胁事件、风险站点排名、WEB整机流量等内容。 |  |  |
| 20 | 产品成熟度 | 61、产品具有《计算机信息系统安全专用产品销售许可证》（须提供以上有效期内的资质证书） |  | **请提供相应证书扫描件的页码** |

3）IDS入侵检测要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购文件要求** | | **技术参数（是否响应）** | **备注** |
| **技术指标** | **指标项** |
| 21 | 硬件规格 | 62、▲标准机架式硬件设备，自适应电口≥8个10/100/1000，千兆SFP插槽≥8个千兆SFP插槽，万兆SFP+插槽≥4个，网络层吞吐量≥20Gbps，IDS吞吐量为≥12.5Gbps，最大并发连接数≥500万，硬盘配置≥1T ，冗余电源**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 22 | 产品部署 | 63、产品具备接口配置IPv6地址功能，包括接口名称、IP地址/掩码、地址类型和IPv6路由通告，并可以显示当前本机的IPv6邻居信息 |  |  |
| 64、产品具备透明接入、旁路部署等多种部署模式 |  |  |
| 23 | 入侵检测 | 65、▲支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测；**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 66、▲支持HTTP Get、Head、Put、Post等多种协议方法检查；**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 67、▲支持自定义入侵检测特征：可依据TCP、UDP、SMB、HTTP等网络层的各项参数设置自定义特征；全面设置TCP/IP应用层的特征比对内容而不受通信协议限制；支持跨数据包检测机制，包括：比对位移(matching offset)、比对长度(matching depth)、比对距离(matching distance)、比对范围(within)；支持基于流的数据包(stream-based)比对技术； **（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 68、▲支持威胁详情URI和攻击数据解码；支持IPv6环境下入侵检测；支持IPv6威胁日志显示和下载；**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 24 | Web防护 | 69、▲系统具备对网站外链检测功能；系统具备对CC攻击的检测；系统具备对跨站脚本攻击的检测能力；系统具备对SQL注入攻击的检测能力；**（请提供截图证明）** |  | **含有“需提供截图”的条款，请提供相应截图的页码** |
| 25 | 产品功能 | 70、产品具备IP/MAC绑定功能，支持手动添加和自动探测IP/MAC对应关系 |  |  |
| 71、产品具备DNS自学习安全缓存、DNS静态缓存功能来检测DNS欺骗、缓存污染、DNS劫持等DNS攻击行为 |  |  |
| 72、产品具备高级访问控制列表功能，可对源及目的MAC、报文头部信息（SYN标志、分片标志、TTL、DSCP、Precedence、TOS）、内网域地址、外网域地址、长连接超时时间等细粒度项进行配置 |  |  |
| 73、产品具备基于地域的访问控制列表功能，支持根据国家、地区等元素进行地域访问检测 |  |  |
| 74、产品具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IDS、可视、概览等多项元素实现快速配置上线 |  |  |
| 75、产品提供入侵检测特征库，特征数超过10000条。并提供基于正则表达式匹配方式的自定义特征检测策略 |  |  |
| 76、产品具备云端威胁情报功能，提供僵尸网络、钓鱼网站、恶意网站等10大类的威胁情报的检测，并对检测到的威胁事件执行记录日志、邮件、声音等动作 |  |  |
| 77、产品具备暴力破解检测功能，提供基于SMTP/IMAP/POP3/TELNET/FTP/RLOGIN/NNTP/TDS-MS-SQL等协议类型的频率检测机制 |  |  |
| 78、产品具备流量自学习功能，通过设置流量学习时间，通过报文、IP排名、域名统计类型建立网络流量基线 |  |  |
| 79、设备具备URL检测功能，用于对用户访问的网址进行检查，支持关键字和正则两种检测方式 |  |  |
| 80、产品具备关键字检测功能，支持基于论坛发帖、邮件协议、TELNET、DNS、RSH、FTP、HTTP协议的关键字检测功能 |  |  |
| 26 | 口令防护 | 81、支持对ftp、telnet、smtp、pop3、imap弱口令行为进行检测 |  |  |
| 82、支持对ftp、telnet、smtp、pop3、msrpc、sunrpc暴力破解行为检测 |  |  |
| 27 | 产品资质要求 | 83、所投产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》 |  |  |