**项目名称：泉州市中医院医院信息安全等级保护系统（三级）**

**一、项目建设需求清单**

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 数量 |
| 1 | 防火墙系统（下一代防火墙） | 3套 |
| 2 | 安全运维网关系统 | 1套 |
| 3 | 数据库安全审计系统 | 1套 |
| 4 | 准入控制系统 | 1套 |
| 5 | 防火墙系统 | 2套 |
| 6 | 安全事件统一管理系统 | 1套 |
| 7 | 防病毒系统 | 1套 |
| 8 | 等级保护咨询与加固服务 | 1项 |

**二、项目建设要求**

**（一）防火墙系统（下一代防火墙）（3套）**

1、1U标准机架式设备，配置千兆电口≥6个，扩展槽≥1个， USB口≥2个, COM口≥1个，硬盘≥1T，单电源；随机赠送一年IPS、AV、应用识别特征库升级服务。含3年系统软件升级服务。最大吞吐量≥5Gbps，并发会话≥120万，新建会话≥4万，VPN吞吐量≥200Mbps，IPS吞吐量≥800Mbps，防病毒吞吐量≥800Mbps，IPS防病毒吞吐量≥600Mbps；

2、适用于各种复杂网络，灵活支持透明、路由和混合模式；支持多种路由协议：静态路由、策略路由、动态路由（RIP v1、RIP v2、OSPF、BGP、多播路由）。

3、支持对密码探测扫描、间谍软件入侵、木马类入侵等行为进行防御和策略限制，具备防御rootkit，针对Client 、Server；UNIX、Linux服务器的木马后门入侵特征。

4、内置病毒特征库，至少支持HTTP、FTP、SMTP、POP3、IMAP、MSN、NNTP等11种协议的病毒防护，发现病毒自动阻断告警（提供相应功能截图证明）；

5、支持文档安全防护主控界面能够提供受控进程的配置项，进程类型包括明文进程、密文进程、信任进程、明文服务进程等；（提供相应功能截图证明）；

6、支持对ActiveX、Java applet、Cookies等小程序的过滤，防止有害脚本进入内网，过滤器支持Web续传屏蔽、不可用URL屏蔽、HTTP POST行为等。（提供相应功能截图证明）；

7.具备防止内网数据泄露功能，支持文档安全功能。客户端的安全模块对本地用户文档进行透明加解密，能够避免文档内容未授权访问，提供功能界面截图

8、提供原厂3年免费售后服务。

**（二）安全运维网关系统（1套）**

1、2U标准机架，配置10/100/1000M接口≥8个，1个扩展槽； USB口≥2个COM口≥，1个，企业级硬盘≥1T；内置APPBOX系统；最大支持200个并发会话。支持外接NAS，支持Telnet、FTP、SSH、SFTP、RDP、VNC协议，支持双机热备，默认150个license(管理资源数)，可扩展至400授权；

2、 通过堡垒机web页面内嵌运维工具访问目标资源。Web页面内嵌RDP协议管理工具及SecureCRT、FTP/SFTP、VNC/X11管理工具，支持剪切板、本地磁盘映射、自定义窗口分辨率、全屏自适应。

3、不改变用户使用习惯，无需登录Web页面，可联动本地CLI客户端实现透明的单点登录。

4、可生成远程桌面RDP登陆会话文件，并能够导出至本地快捷登陆。

5、支持对重要服务器的二次审批：即对重要服务器执行单点登录时，需通过领导二次审批方可操作。

6、支持对未授权资源的临时申请，临时申请需选择目标资源、访问协议、登陆账号、使用时间及申请原因，提供相应功能截图证明；

7、提供原厂3年免费售后服务。

**（三）数据库安全审计系统（1套）**

1、2U,模块化设计，配置10/100/1000M电口≥10个，2个扩展槽；硬盘≥4T；最大日处理SQL明细≥5000W条；入库速度≥8000(条/秒)；峰值事务处理能力≥20000(条/秒)；日志数量存储≥8亿条；

2、支持对TELNET、FTP、VNC、RDP等远程操作行为的会话审计，(提供功能界面截图)；

3、 内置不同HIS系统的防统方规则库，内置HIS系统不少于7个，且必须包含Caché数据的HIS系统。

4、支持对审计数据结果进行多条件组合查询，查询条件不少于23种。所支持的查询条件包括时间范围、源IP地址、操作方式、规则名、操作内容、排序方式、查询方式、排除内容、操作对象、计算机名、目标IP、应用程序名、数据库用户名、数据名、协议类型、会话流水号、语句流水号、长语句总耗时、长语句平均耗时、会话语句种类数、会话重复程度、最大单条耗时、会话语句数量、会话重复程度；支持对审计数据按关键词进行模糊查询，支持查询结果的二次过滤；

5、支持对高危报表元素进行二次编辑，使之产生更精确的报表，以图表方式展示各个字段，包括源IP、目标IP、SQL相似度、操作方式、操作对象、规则编号、应用程序名的统计情况，(提供相应功能截图证明)；

6、支持将结构化SQL语句转译为非计算机人员可直接阅读，并提供准确的事件概述，(提供功能界面截图）

7、采用在海量数据中发现异常技术，提供详细的技术实现方法说明，且该技术实现方法获得省级及以上政府权威机构网站发表，提供网站证明截图及网址，提供该技术的省级及以上政府权威机构认证的相关证明材料；

8、采用在海量SQL语句归并技术，提供详细的技术实现方法说明，且该技术实现方法获得省级及以上政府权威机构网站发表，提供网站证明截图及网址，提供该技术的省级及以上政府权威机构认证的相关证明材料；

9、采用分布式数据存储的修复技术，提供详细的技术实现方法说明，且该技术实现方法获得省级及以上政府权威机构网站发表，提供网站证明截图及网址，提供该技术的省级及以上政府权威机构认证的相关证明材料；

10、提供原厂3年免费售后服务。

**（四）准入控制系统（1套）**

1、2U模块化设计，配置10/100/1000M≥8个，1个扩展槽； USB口≥2个， COM口≥1个，硬盘≥1T，支持并发在线用户数≥1000，每秒认证会话数≥800，标配授权用户数800，可扩展至1000用户

2、支持旁路、网桥、网关3种部署方式；支持端口镜像旁路及串接方式部署，设备部署过程中不能改变原有网络结构及网络、安全等设备的配置且无客户端；

3、支持NACP准入模式、透明网桥模式、策略路由模式、802.1X模式，可根据实际需要同时启动多种准入模式；

4、支持阻断跨NAT路由器下未认证的计算机，放行合法的计算机；

5、支持无线wifi热点的准入控制，可禁止通过PC共享wifi热点；

6、针对终端安全性进行测评，符合管理员制定的各项测评要求才能接入网络；支持准入引导页面，详细描述终端用户被准入的原因；

7、支持组合身份鉴别方式，可根据用户、密码进行身份鉴别，支持LDAP、AD域联动身份鉴别、Email账号密码身份鉴别、USB Key身份鉴别、短信验证码身份鉴别等技术进行单一和组合方式对入网用户进行鉴别控制，提供功能界面截图；

7、提供原厂3年免费售后服务。

**（五）防火墙系统（2套）**

1、2U标准机架式设备，模块化设计， SFP 万兆接口≥2个；配置千兆管理口≥2个，千兆电口≥8个，万兆接口及模块≥2个，双机热备模块，扩展槽≥3个， USB口≥2个， COM口≥1个，企业级硬盘≥1T，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；

2、需支持虚拟防火墙，可划分成多个独立的虚拟防火墙系统，并可进行虚拟系统热切换，每个虚拟防火墙都是一个唯一的安全域，拥有独立的策略和资源，支持根防火墙管理员和虚拟防火墙管理员

3、支持文档安全防护主控界面能够提供受控进程的配置项，进程类型包括明文进程、密文进程、信任进程、明文服务进程等（提供相应功能截图证明）；

4、支持和IDS/IPS联动、安全准入系统、数据库审计系统联动，形成完善的安全防御体系，（提供相应功能截图证明）；

5、支持设备性能趋势统计分析：时间（最近1小时、最近1天、最近1周、最近1月、最近1年）、设备性能指标(CPU使用率、内存使用率、最大并发数、每秒新建会话、最大用户数)、统计(最大值、最小值、平均值、当前值) （提供相应功能截图证明）

6、支持多元带宽控制：支持基于用户对象、目标地址、应用服务类型、上/下行保证带宽、多级的上/下行弹性带宽，灵活分配用户和业务应用带宽使用权限，保障关键用户和关键业务带宽；

7、提供原厂3年免费售后服务。

**（六）安全事件统一管理系统（1套）**

1、2U标准机架设备， 1000M电口≥6个，扩展槽≥3个， USB口≥2个， COM口≥1个；硬盘≥4T；性能参数：日志处理能力≥7000EPS；日志容量≥20亿条；支持资源数≥220个。

2、支持采集网络流量，解析协议不少于ICMP、AMQP、Cassandra、DNS、HTTP、Memcache、MySQL、PgSQL、TNS、Redis、Thrift、MongoDB、NFS、TDS、Sybase、Drda、Dameng、POP、SMTP；（提供相应功能截图证明）；

3、支持对所管理设备的日志原始数据完整存储，海量数据加密存储，防篡改；支持数据自动、手动备份以及备份数据恢复查看。支持数据本地集中存储、本地离线备份存储、FTP离线存储、网络存储；

4、支持以世界地图和中国地图显示IP连接信息，显示IP地址地理位置，直观发现敏感外联日志（提供相应功能截图证明）；

5、支持根据时间范围、级别、规则类型、告警全文关键字等方式快速检索安全事件告警，检索结果支持Excel等格式导出。支持邮件、声音、syslog等多种告警方式，支持在全局显示告警提醒；可以针对不同类型、不同种类以及不同安全级别的安全事件制定不同的告警方式。

6、支持全文检索、短语检索、字段值精确查询、通配符检索、正则表达式检索高量显示。支持过滤条件不少于以下条件类型：设备IP、来源IP、目的MAC、来源端口、目的端口、目的地址IPV6、源MAC、源地址IPV6、操作用户、目的IP、事件名称、域名、事件级别、应用名称、请求信息、服务名称、错误信息、响应信息、资源类型、错误码、接收字节、数据库表名、状态码、协议、发送字节、请求方式等（提供相应功能截图证明）。

7、提供原厂3年免费售后服务。

**（七）防病毒系统（1套）**

1、管理端支持全中文界面，纯B/S架构，无需安装客户端软件。管理员只需通过浏览器登陆控制中心，即可对虚拟机进行管理。防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS病毒等进行查杀，提供主动防御系统防护等功能。含三年病毒库升级服务。客户端资源占用应小于50MB，有效节省终端资源使用率。授权30个Windows服务器端节点、800个PC终端节点。

2、支持对终端进行单/多标签标记；

3、控制中心支持全网/以分组、标签为单位/指定某些客户端定制操作，即时/定时实现客户端三种病毒查杀模式、显示通知、关机、重启、升级等操作，并对以上操作配置详情，客户端执行情况跟踪，实现控制中心对客户端的操作监控。支持对客户端上述操作的快速定制。

4、控制中心支持全网/以分组、标签为单位/指定某些客户端定制策略，支持指定客户端策略锁定。定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等；

5、支持设置客户端与控制中心的通讯时间间隔；

6、支持单/多客户端不同管理中心迁移；

7、支持虚拟补丁功能，针对网络数据流的深层分析，检测入站流量并保护应用程序免受攻击，有效阻止勒索病毒等高危威胁的入侵；

8、支持内容拦截主动防御，当文件被执行、修改、访问时，反病毒引擎对相应文件进行扫描，如扫描到威胁则阻断用户对该恶意威胁的触碰并根据需要进行隔离操作；支持规则拦截主动防御，程序执行时，规则拦截层开始生效，并根据基础防护或自定义防护规则，对程序产生的违例动作进行拦截；支持行为拦截主动防御，当发现威胁时，行为拦截层阻止威胁进程及关联进程、线程的执行，并尽可能地回滚已经产生的潜在风险，实现病毒行为监控，软件安装拦截；

9、支持报表内容、周期、推送、输出格式定制，内容设定模板任意组合包含终端/部门/责任人危险排行统计、防御类型分布统计、病毒类型分布统计、病毒排行统计、病毒趋势统计等统计情景及威胁Top10、Top20、Top30排行；周期设定任意组合日、周、月周期，定时生成报表；推送设定任意接收报表人员；输出格式设定Excel、Word、HTML、PDF等通用格式输出；

10、支持对客户端上报的安全日志进行审计、告警，可预置字段及自定义字段过滤详细日志，快速定位终端安全状况；定制符合企业敏感程度的告警规则，达到告警阈值，产生告警日志并定制推送，保证告警及时性；

11、能够支持客户端主动升级及平台即时/定时推送升级；支持全网/以分组、标签为单位/指定某些客户端定制不同版本升级包，实现差异管理、灰度升级；提供截图；

12、对流行病毒的检测能力超过98%的检出率，超过98%的清除率，小于0.1%的误报率，能够提供提供第三方测试证明；

13、提供原厂1年免费售后服务。

**（八）等级保护咨询与加固服务（1项）**

**一、项目范围**

★本项目应针对核心业务系统进行等级保护及加固改造服务，这些核心业务系统包括医院信息系统（HIS）、检验信息系统（LIS）、影像信息系统（PACS）、电子病历系统（EMR）等业务系统，供应商应充分考虑改造过程中所可能涉及的数据迁移、接口改造、业务流程对接等问题，在采购人参与沟通协调下，能够解决核心业务系统改造过程所可能导致的系统故障、医院业务中断、数据错误等突发事故，并充分考虑到报价中，采购人不再因此承担费用，供应商因对此做出书面承诺。

**二、服务周期**

自合同签定之日至备案系统通过测评或1年，以先到为止。

**三、服务内容**

★满足等级保护2.0的要求，供应商能够保证设计的方案符合等保2.0标准，测评机构必须按照等级保护2.0的测评标准进行测评。

针对服务范围内的信息系统开展信息安全服务工作，参照公安部印发《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》等标准规范要求，结合行业特点和安全需求，为信息系统提供物理安全、网络安全、主机安全、应用安全、数据安全以及安全管理制度等方面的信息安全需求分析、措施设 计、安全加固、制度编写等安全服务工作。

针对服务范围内信息系统安全服务具体工作内容如下：

**资产分析服务**

根据服务范围内的应用组成，派遣专业工程师到现场整理各个系统的网络结构拓扑以及相关联的资产，编制信息系统资产清单及资产报告；

对服务范围内信息系统开展物理环境、网络结构、设备配置、应用系统以及管理制度进行调研和梳理，编制信息系统详细描述文档。

**风险分析服务**

a) 对单位内网常见威胁进行评估并根据等级保护要求结合单位具体情况编写单位信息安全基线库。

b) 通过现场评估、脆弱性评估以及渗透测试等技术手段分析信息系统安全风险以及基线差距。

**差距分析服务**

a) 在安全评估和信息系统定级的基础上，根据《信息系统安全保护等级基本要求》将定级信息系统等级保护的各项基本要求与信息安全现状进行比较分析，从管理和技术两个层面找出存在的问题并进行分析。

b) 对于需要增加投资，部署新的信息安全产品和技术的整改措施，双方根据整改方案另行协商和实施。

**需求分析与设计服务**

a) 对服务范围内信息系统按照差距分析报告对应策略设计整改措施，面向保护对象设计安全计算环境安全、安全区域边界安全、安全通信网络等方面的整改设计方案；

b) 开展详细设计工作，完成网络结构框架设计、功能设计、性能设计、部署方案设计、安全策略设计等方面，形成安全整改实施规范书；

c) 提供信息安全等级保护建设详细方案书，应该包括具体的实施内容、实施流程、风险管理和进度控制等。

**安全整改加固服务**

a) 派遣专业工程师到为单位服务器实施服务器病毒检查与清理、主机安全加固、数据库安全加固建议以及应用安全加固辅导；

b) 安全加固实施前，应提交安全加固风险分析及风险规避说明书。

**策略复查服务**

a) 派遣专业工程师到现场针对加固前后的系统脆弱性进行复查，复查手段包括但不限于协议分析、漏洞扫描、漏洞验证以及配置核查等方法；

b) 复查结束后，形成加固前后对比复查报告。

**管理制度辅助建设服务**

辅助用户编写方针、制度、各类记录表格模板在内的三层结构的安全管理制度，达到等级保护测评要求。

**定级咨询服务**

在采购人信息系统自行定级的基础上，参照国家和地方对等级保护定级的有关要求，对信息系统开展摸底调查工作，掌握信息系统的基本情况，了解信息系统（包括信息网络）的业务类型、应用或服务范围、用户数量、系统结构、部署方式、安全策略、内控制度等信息，撰写信息系统定级报告，明确信息系统的边界和安全保护等级，说明定级的方法和理由。并收集整理定级系统参与福建省网络与信息安全测评中心安全等级测评所需的资料和文档。

**等保测评现场辅助服务**

在服务期内，采购人如有申请测评，供应商将协助测评方完成测评数据采集等工作，直至备案系统通过等级测评。

**备案咨询服务**

根据《信息安全等级保护管理办法》，信息系统安全保护等级为第三级以上的信息系统运营使用单位或主管部门，应到公安部网站下载《信息系统安全等级保护备案表》，供应商提供备案咨询服务，协助采购方填写《信息系统安全等级保护备案表》直到完成备案工作。

服务过程中提供的安全工具具有以下功能：

供应商或所依托安全服务商在服务过程中所采用的云主机安全监控系统上能展示所有监控主机资产信息，包括：分组/分类、IP地址/MAC、主机代号、标题/备注、主机名、操作系统、修改/锁定/删除。而且能够在主机监控页面上能直观展现告警趋势、监控详情、系统配置监控、采集记录情况。（提供功能截图）

**安全巡检服务**

在合同期内，每季度派遣专业技术人员到现场对目标系统服务器进行安全核查，对服务器进行网页木马、攻击行为、安全配置进行全面核查，发现高危漏洞，及时开展安全加固工作。针对现场安全巡检发现的问题提出加固建议和辅导服务，并提供现场安全巡检报告。

**服务工具要求**

采用的主机安全监控系统服务工具能够监控网页木马(webshell)，提供截图；供应商的演示者通过模拟黑客利用漏洞入侵应用系统，进行植入网页木马(webshell)等入侵行为，主机安全监控系统应能够在1分钟内发现网页木马并生成相关的告警，并能够查看告警信息和对应的敏感文件内容。供应商提供功能截图并通过光盘/U盘提供虚拟机环境下的录屏演示（录屏演示时间为3至5分钟).

主机安全监控系统服务工具对能够监控黑客入侵过程中修改系统账号、创建敏感文件、植入Rootkit后门等行为，供应商提供包括账号口令、权限控制、敏感文件、可疑后门等黑客入侵痕迹监测功能截图。供应商的演示者通过模拟黑客利用系统漏洞，向被监控的应用系统主机添加隐藏账号(例如：hack$)，主机安全监控系统应能在1分钟内生成相关的告警，并能够查看告警信息和对应的黑客添加的系统账号名称。供应商提供功能截图并通过光盘/U盘提供虚拟机环境下的录屏演示（录屏演示时间为3至5分钟）

主机安全监控系统服务工具能够提供基线检查和管理功能，对常见的系统共享配置、帐号等默认策略进行检测和管理，而且能够自主添加和删除新的策略，并能够对检查结果准备进行分类统计。供应商的演示者通过模拟黑客利用系统漏洞，向被监控的应用系统主机更改主机系统安全审计策略(例如：审核帐号管理)，主机安全监控系统应能在1分钟内生成相关的告警，并能够查看告警信息和对应的。提供功能截图并通过光盘/U盘提供虚拟机环境下的录屏演示（录屏演示时间为3至5分钟）

**四、应急响应服务要求**

1.遇到医院信息系统（网络设备、安全设备、服务器、操作系统、数据库）出现病毒传播、黑客攻击或不可用等紧急安全事情出现，并且远程支持无法解决时，要求2小时内到达现场，实施最有效的紧急救援及恢复补救方案。

2.实时关注业界安全动态，当有重要安全问题出现时，及时通知医院，并对安全漏洞原因、影响范围、风险进行评估，并提供解决建议。

**三、售后服务要求**

1、供应商须明确货物质量保证期，并按产品技术指标的质保期要求进行承诺。在实施及免费维护期内，需提供所投产品故障修复，性能调优和备品备件更换等服务，由此产生的费用均不再收取。

2、重大事项的即时响应：系统出现故障或意外情况导致系统不能正常运行时，供应商针对不同响应级别的即时响应包括：人员、时间和内容等,至少应能保证7×8小时服务，24小时内现场及时响应。

3、服务请求的方式：在采购人需要提供服务（包括即时的和非即时的）时，能够与供应商联系沟通的方式描述，应包括：服务热线电话和联系人、联系单位信息、信函/传真、电子邮件、服务网站。

4、供应商通过系统阶段验收后，应提供如下维护保障工作:

（1）故障修复维护技术支持：指系统发生突发性故障后，追查故障原因，并予排除修改的工作。若系统由于自身缺陷导致系统无法正常使用，供应商应在接获通知后的2小时内予以响应，调配有关技术人员远程或至现场进行技术维护支持，以使系统正常运行。远程技术支持包括：电话、传真或E－MAIL、远端故障诊断、补丁更新。现场技术支持是指当应用系统在远程支持无效的情况下，供应商应派遣技术支持人员在4小时内赶到采购人现场提供现场技术支持工作。

（2）定期走访技术支持：供应商应组织技术人员对系统每季度进行一次现场巡访。了解用户的产品使用情况，及时为用户解决技术问题。包括通过电话、传真、E-MAIL等方式由技术人员进行远程技术指导和故障排除。

（3）人员技术指导：供应商应对采购人以下人员进行产品使用技术指导，包括：①系统管理人员技术指导。②系统维护人员技术指导。③系统使用人员技术指导。