**采购需求**

**一、背景介绍**

随着网络安全形势的日益严峻，网络与信息安全已被提升为国家战略，国家有关部门先后出台了一系列文件，明确了等级保护的重要性。2017年6月1日起，《中华人民共和国网络安全法》正式实施，其中第二十一条规定“国家实行网络安全等级保护制度”。《安徽省卫生行业信息系统安全等级保护工作实施指南》要求全省医疗卫生行业信息网络和信息系统贯彻落实信息安全等级保护定级备案、建设整改和安全测评等工作；《安徽省卫生计生综合监督“十四五”发展规划》提出，落实信息安全等级保护制度，加强信息安全技术和管理体系建设。

为了进一步贯彻落实信息安全等级保护工作，依照国家《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全保护等级定级指南》等标准，需要提高安庆市第一人民医院网站业务系统的安全性，需要对安庆市第一人民医院网站业务系统进行安全加固。安庆市第一人民医院官网服务器部署在天翼云上，已在线备案提供访问服务，IP地址117.6\*.2\*.1\*，目前缺乏足够的安全性和防护措施。为了确保官网网站系统能够通过二级等保测评，需要增加以下服务：云下一代防火墙（含IPS、AV、URL过滤、应用识别、监控统计、访问控制、入侵防御（IPS)、用户认证功能）、日志审计、终端杀毒产品、支撑云下一代防火墙的云主机。利用云安全服务加强网站的安全性、监控和日志记录，满足行业监管要求，保护网站系统免受潜在的威胁，保障安庆市第一人民医院官网网站能够通过二级等保测评工作。

**二、服务需求**

为满足二级等级保护测评要求，本项目需要以下相关服务：

1、云下一代防火墙服务：新增云下一代防火墙，包含但不限于以下功能：（含IPS、AV、URL过滤、应用识别、监控统计、访问控制、入侵防御（IPS)、用户认证功能）需在官网网站服务器前部署，以确保网络安全和流量筛选。保障云下一代防火墙正常运行，确保官方网站二级等保测评顺利通过。

2、云主机服务：提供云主机，用于安装网站的云下一代防火墙、日志审计、终端杀毒产品。云主机应满足项目要求，包括性能和配置等，以确保云下一代防火墙、云日志审计、终端杀毒产品的正常运行。

3、终端杀毒：在医院官方网站服务器上安装终端杀毒产品，确保满足等级保测评要求。终端杀毒产品应定期更新病毒库和保持实时保护状态。

4、日志审计：部署日志审计服务，用于记录和分析网络和系统日志。日志审计服务应满足等级保测评要求，并能够提供必要的安全审计数据。

**三、总体设计要求**

1、设计要求

结合卫健行业监管要求及安庆市第一人民医院网站业务系统实际情况，应按照《信息系统等级保护安全设计技术要求》和《信息系统安全等级保护基本要求》等相关标准要求，以“一个中心、三重防护”为核心指导思想，从安全计算环境、安全区域边界、安全通信网络以及安全管理中心四个方面构建安全建设方案，以满足等级保护二级系统的相关要求。

2、设计依据

本项目应严格依据下列政策法规和标准规范：

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239- 2019）

《信息安全技术 网络安全等级保护定级指南》（GB∕T 22240-2020）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB\_T 25070-2019）

《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010）

《信息安全技术 信息安全等级保护整改规范》（GB/T20984-2007）

《信息技术 安全技术信息安全管理体系要求》（GB/T22080-2016）

《信息技术 安全技术信息安全管理实用规则》（GB/T22081-2016）

《信息技术 安全技术信息技术安全管理指南》（ISO/IECTR13335）

《信息技术 安全技术信息技术安全性评估准则》(GB/T18336-2001)

3、设计原则

安庆市第一人民医院网站业务系统的二级等保建设项目，按照以下原则进行方案设计：

（1）安全合规：信息系统等级保护建设方案设计符合国家相关信息安全政策和标准，确保设计的信息安全保障系统遵循国家法律且符合国家政策和国家标准。

（2）符合标准：安全建设符合安全建设的标准，做到安全风险可控的效果，提供云下一代防火墙（含IPS、AV）、日志审计、终端杀毒产品等安全模块。

（3）适度防护：从整体安全出发，各种安全设备资源有机结合，管理手段与技术手段结合，避免片面追求全面的安全防护，以防过度的投资带来资源浪费。

（4）持续运维：三分技术，七分管理。建立一套制度化、流程化、标准化的中心运维管理体系，以保障应用规范、有序、持久地运行，确保顺利通过测评。

**四、技术要求**

为确保项目的成功实施，供应商需满足以下技术要求：

1、云下一代防火墙服务：新增云下一代防火墙，包含但不限于以下功能：（含IPS、AV、URL过滤、应用识别、监控统计、访问控制、入侵防御（IPS)、用户认证功能）需在官网网站服务器前部署，以确保网络安全和流量筛选。保障云下一代防火墙正常运行，确保官方网站二级等保测评顺利通过。

2、云主机服务：提供云主机，用于安装网站的云下一代防火墙、日志审计、终端杀毒产品。云主机应满足项目要求，包括性能和配置等，以确保云下一代防火墙、云日志审计、终端杀毒产品的正常运行。

3、终端杀毒：在医院官方网站服务器上安装终端杀毒产品，确保满足等级保测评要求。终端杀毒产品应定期更新病毒库和保持实时保护状态。

4、日志审计：部署日志审计服务，用于记录和分析网络和系统日志。日志审计服务应满足等级保测评要求，并能够提供必要的安全审计数据。

**五、货物或服务需求一览表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **技术参数** | **单位** | **数量** |
| 1 | 云下一代防火墙 | 1、支持公网授权、内网授权验证方式； | 套 | 1 |
| 2、支持多达几千种的应用特征库，并支持网络实时更新；**（需提供产品功能截图）** |
| 3、支持基于加密流量的应用识别； |
| 4、支持QoS管道策略实际流量情况监控，支持子管道叠加情况监控；**（需提供产品功能截图）** |
| 5、支持基于深度应用识别的访问控制； |
| 6、支持链路状态监控，可查看指定应用/应用组详情，支持选择多条链路进行对比分析； |
| 7、支持外部服务器用户认证(RADIUS、LDAP、MS AD)； |
| 8、支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型；支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式；**（需提供产品功能截图）** |
| 9、支持通过监控C&C连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏，并定期升级更新僵尸网络服务器地址； |
| 10、支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测和防御； |
| 11、支持抵御所列所有攻击类型，包括：PortScan、DOS Flood、Sockstress、反射攻击、SSL攻击、应用层攻击等，动作支持记录、阻断两种模式。支持对不同安全域设定不同阈值和处理模式；**（需提供产品功能截图）** |
| 12、含IPS、AV、URL过滤、应用识别、监控统计、访问控制、入侵防御（IPS)、用户认证功能； |
| 13、支持通过监控C&C连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏，并定期升级更新僵尸网络服务器地址。**（需提供产品功能截图）** |
| 2 | 日志审计 | 1、支持无需另外安装软件组件，审计中心即可实现新增Oracle数据库自身日志的采集任务、新增SQL Server数据库自身日志的采集任务、新增Apache服务器日志的采集任务、新增Lotus Domino的日志采集任务；新增CheckPoint的日志采集任务；**（需提供产品功能截图）** | 套 | 1 |
| 2、支持针对文本格式的日志采集，支持本地文件、Windows共享和FTP、SFTP获取四种采集方式；**（需提供产品功能截图）** |
| 3、支持单级部署和级联部署，支持分布式部署； |
| 4、支持对资产的ping、telnet和远程访问等功能； |
| 5、支持以资产树的形式显示不同资产区域之间的关系； |
| 6、支持以列表的形式显示某个管理区域中的所有资产清单； |
| 7、支持可以根据日志源断点时间进行配置，并生成告警。点击单个日志源设备查看该设备最近7天的事件趋势；**（需提供产品功能截图）** |
| 8、支持可以对选中的日志进行地图定位，包括在线定位和离线定位；**（需提供产品功能截图）** |
| 9、支持实时统计和历史统计两种模式；**（需提供产品功能截图）** |
| 10、支持告警重定义、弹出提示框、发出警示音、发送邮件、发送SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送Syslog等方式、加入观察列表、从观察列表中删除。**（需提供产品功能截图）** |
| 3 | 终端杀毒 | 1、支持对系统进行实时防护，定期对虚拟机进行全盘扫描，手动对虚拟机进行磁盘扫描，感染的文件在虚拟机内部隔离； | 套 | 1 |
| 2、支持对Windows，Linux部署系统安全风险的全面洞察，帮助快速和准确地识别、调查、划分优先级和纠正漏洞； |
| 3、支持对文件安全性的实时分析，并返回杀毒控制中心文件结果，包含所有磁盘目录的文件； |
| 4、支持自定义查杀强度，自定义方式对终端进行扫描，支持选择启用的引擎类型，配置是否自动处理，是否扫描信任区； |
| 5、支持对终端隔离区指定时间段，指定文件路径或者文件名或者病毒文件进行恢复，恢复到原始路径； |
| 6、支持定时进行终端云查杀，每次云查杀包括终端提交一批文件MD5到云查杀引擎，完毕后给于反馈。 |
| 4 | 云主机服务 | 1、支持单独购买云硬盘挂载到云主机上，并提供多种存储类型，满足不同的I/O性能要求； | 台 | 2 |
| 2、支持专有网络，可灵活自定义网络空间； |
| 3、支持通过隧道技术实现 100%二层网络隔离，满足不同行业客户的安全隔离需要； |
| 4、支持自定义子网网段划分、IP 地址及路由策略，按需配置，即开即通； |
| 5、支持专线、VPN 等多种方式接入云端； |
| 6、支持块存储采用三副本技术，支持云硬盘自动备份，进一步保障数据安全性； |
| 7、支持多种镜像，助力业务批量快速部署，支持Linux、Windows 等多种公有镜像； |
| 8、支持可视化管理平台及控制台、远程终端等多种管理方式，操作便捷，多维度监控； |
| 9、支持多维度资源监挖，提供全面监控及告警机制，方便数据出现异常及时处理； |
| 10、用于部署日志审计云主机配置CPU≥8核、内存≥64G、磁盘≥500G、带宽≥10M；用于部署云下一代防火墙云主机配置CPU≥2核、内存≥4G、磁盘≥40G、带宽≥10M。 |

**六、服务期要求**

60日历天内完成云安全防护服务的部署及调试，维护服务期自云安全防护服务验收合格之日起一年。投标人在服务期内对系统应用软件部分根据业务需要免费提供功能性完善服务（免费升级、故障修复等）。

**七、售后服务**

1、提供电话、现场响应服务及现场维修服务，中标人须提供7×24小时的技术支持服务，中标人必须安排技术人员2小时内到现场进行免费维护，小故障应在2小时内修复，换件服务应在24小时之内修复。**（投标文件中提供承诺函，并加盖投标人公章）**

2、中标人应对招标人的相关人员进行免费现场培训。培训内容包括基本操作、保养维修、常见故障及解决办法等。**（投标文件中提供承诺函，并加盖投标人公章）**

3、中标人与招标人签订保密协议，在提供运维服务的过程中，获悉的一切资讯需严格遵守保密协议，严禁自行使用或向他人传播，泄漏或擅自使用或允许他人使用上述信息，由此造成的损失应承担相应的法律责任。**（投标文件中提供承诺函，并加盖投标人公章）**

**八、报价要求**

本项目按总价报价，其报价应包含但不限于采购范围内产品购买、产品安装调试、物耗以及售后服务涉及的人员劳务、社保、交通、食宿、税费、人员培训、测评及专家评审费用等一切费用。一旦成交，成交价不作任何调整。

**九、验收**

中标人和采购人双方共同实施验收工作，结果和验收报告经双方确认后生效。

**十、付款方式**

云安全防护服务部署调试完成，经采购人验收合格且通过等保测评后支付合同价款的90%，余款待维护服务期结束后一次性付清。