**附件9**

**项目技术需求**

## 项目背景

目前北京老年医院信息系统进行了网络安全建设，基本能够支撑内网相关业务系统的安全运行，满足医院发展需求，但随着国家医疗体制改革及行业信息化发展及医院业务的不断发展，现有信息系统仍需进一步进行安全加固及提升，建设更加完善的网络安全体系，加强网络安全防范能力。 因此北京老年医院结合医院发展和信息系统运行的实际需要，进一步开展信息系统安全整改工作。

## 项目目标

为落实国家网络安全等级保护政策、标准、卫生部关于《卫生行业信息安全等级保护工作的指导意见》、北京市卫生行业等级保护相关工作要求，本项目对北京老年医院现有网络系统进行加强建设，确保北京老年医院具备安全稳定的运行环境，降低网络安全风险，提升北京老年医院医疗信息化服务水平，发挥信息化的融合、带动作用，构建安全、可信的医疗环境，全面提升北京老年医院网络的综合防护能力和风险处置效率，减少信息系统中断风险，保证业务系统的高可用性，提升业务工作效率，不断完善业务和信息资源的管理。

## 采购需求

### 安全设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **单位** | **备注** |
| 1 | 防火墙 | 1 | 台 | 无 |
| 2 | 防病毒模块 | 2 | 个 | 针对华为防火墙（型号USG6670）增加防病毒软件功能 |
| 3 | 安全隔离与信息交换系统 | 1 | 台 | 无 |

### 安全服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **单位** | **备注** |
| 1 | 定级备案 | 1 | 次 | 服务期内提供1次 |
| 2 | 安全加固 | 2 | 次 | 服务期内提供2次 |
| 3 | 管理制度修订 | 1 | 次 | 服务期内针对三级系统提供1次 |
| 4 | 脆弱性检测 | 2 | 次 | 服务期内提供2次 |
| 5 | 应急响应 | 1 | 年 | 服务内按需提供，不少于3次 |
| 6 | 安全巡检 | 4 | 次 | 服务期内提供4次 |
| 7 | 堡垒机接口开发 | 1 | 次 | 双因素认证 |

## 产品及服务详细指标要求

### 产品详细指标要求

#### 防火墙

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 硬件、功能要求 | 1U机箱，单电源 |
| 最大并发连接数≥200万 |
| 应用层吞吐率（FW+APP）：≥3Gbps |
| 防火墙吞吐率≥6Gbps |
| ≥6个10/100/1000BASE-T接口，≥2个SFP插槽，不少于2个端口扩展卡插槽 |
| 支持路由、交换、混合、虚拟线工作模式 |
| 2 | 系统结构 | 设备应采用自主知识产权的专用安全操作系统 |
| 3 | 系统软件 | 系统应具有良好的扩展性，应支持扩展病毒防御、入侵防御、应用识别、网站分类库过滤、IPSEC VPN等功能。应开启病毒防御模块，配置特征库升级。 |
| 4 | 功能要求 | 应支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 应支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发； |
| 应支持GRE与IPSEC VPN接入； |
| 应支持IPv4/IPv6双栈工作模式； |
| 应支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置 |
| #应内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如P2P、web应用、移动应用、云应用、加密应用等；内置独立应用识别特征库，总数2100种以上，支持应用特征库在线或本地更新，支持应用特征自定义；  |
| #应支持监控功能，显示最近被拦截的IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制；  |
| #应内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持web攻击识别和防护，如跨站脚本攻击、SQL注入攻击；支持超过4100+攻击特征库 |
| 应内置流量检测清洗引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义； |
| #应支持基于TCP协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、FIN Flood、RST Flood、新建SESSION Flood、SESSION Flood等；支持SYN源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击；  |
| #应支持基于HTTP协议的检测清洗，包括但不限于：HTTP Flood、HTTP新建连接Flood、HTTP并发连接Flood、HTTP URI CC等攻击检测，同时支持对HTTP slow-header和HTTP slow-post设置最大传输时间以及异常会话数阈值，有效防御慢速攻击；  |
| #应内置病毒检测引擎，支持HTTP/SMTP/ POP3/FTP/IM等协议的病毒防御 |
| #应内置至少2种专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。病毒特征库规模应超过400万 |
| #应支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，可对微博、贴吧上传的内容及附件进行过滤，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；  |
| 在WEB界面提供资源监控开关，应可对cpu占用率、内存占用率、磁盘占用率设置阈值； |
| 应支持根据应用对通过设备的数据报文流量进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速； |
| #应支持根据用户/用户组对通过设备的数据报文流量进行统计，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速； |
| #应支持根据按照病毒防御、入侵防御、ADS攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名。 |
| 5 | 产品资质 | #提供公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供相关证明文件） |
| #提供中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》（提供相关证明文件） |
| #信息安全测评中心颁发的EAL3+证书（提供相关证明） |
| #IPV6金牌认证证书。（提供相关证明文件） |
| 6 | 服务 | 应免费提供三年硬件质保以及三年软件服务 |

#### 防病毒模块

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 要求 | #针对华为防火墙（型号：USG6670）增加防病毒软件功能 |

#### 安全隔离与信息交换系统

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 性能要求 | 用户数：应支持≥500用户 |
| 系统带宽≥500Mbps |
| 支持≥10GB的文件交换 |
| 应支持≥500个并发文件同步请求 |
| 硬盘不小于2T存储容量 |
| 2 | 部署方式 | 一体式部署，一台设备，部署在内外网之间 |
| 3 | 功能 | 用户管理：应提供对部门及人员的树状管理，提供系统管理员、审核员及审计员的三权分立机制 |
| 身份认证：应提供基于用户名/口令的认证方式 |
| IP绑定：应提供基于IP的使用人员绑定功能 |
| 硬件信息绑定：应提供基于硬件信息的使用人员绑定功能 |
| 原始数据摆渡：应提供基于网闸的文件内外网隔离摆渡功能，支持基于WebService、HTTP协议的服务调用模式； 服务调用模式在跨网隔离交换系统内部应采用文件同步实现。 |
| 文件管理：应支持内外网用户的双向个人文件交换，包括从内到外和从外到内；应提供C/S模式的文件上传及下载管理；应支持用户及多级部门管理功能；应支持用户导入导出功能；应支持用户及部门的排序和移动功能；应支持客户端用户路径和自启动设置功能；应支持客户端用户的个人文件接收提醒功能；应支持服务端传输日志查看功能；应支持用户将同一文件发送给多个用户的功能；应支持与第三方用户管理系统联动，实现统一用户管理。 |
| 应用文件传输：应支持基于FTP、SCP、SFTP、Samba等方式的文件同步； 应支持对文件及目录的同步，目录层次没有限制，文件大小没有限制；应支持同一个目录的文件双向同步；应支持备份、复制及移动传输模式；应提供内置FTP服务，使外网到内网的文件交换更为快捷；应提供内置SAMBA服务，使外网到内网的文件交换更为方便快捷；应支持主动传输模式（拉模式）、被动传输模式（推模式）及混合传输模式；应提供专有的外置程序，实现高效文件同步功能。 |
| 自动提醒：客户端对文件传输状态进行自动提醒，方便用户使用 |
| 文件摆渡方式：应支持一对一文件摆渡及一对多文件摆渡方式 |
| 文件摆渡方向：应支持单向及双向文件摆渡功能 |
| 人工审核：应提供严格的文件交换人工审核机制，支持委托审核功能 |
| 文件策略管理：应提供灵活的文件摆渡策略控制，适应外网到内网及内网到外网的不同应用场景  |
| 文件查看限制：应可以有效防止非授权管理员查看普通用户上传及下载的文件 |
| 4 | 安全性 | 文件源追踪：应支持对文件摆渡过程的全程审计功能，任何通过本系统交换的文件均能准确定位 |
| 文件源可信控制：应对交换的文件从上传开始追踪控制，应有效防止无关文件被夹带而传输到对方 |
| 文件安全检查：应提供对文件类型的深度检查、文件内容的关键字过滤及集成第三方的病毒查杀功能 |
| 认证安全性：应支持用户名/口令、IP绑定、硬件信息认证 |
| 防攻击：设备内外端应内置防入侵模块 |
| 基于安全通道的文件传输：终端计算机与文件服务器之间应采用加密通道 |
| 5 | 可用性 | 双机热备：应支持双机热备，主设备出现故障时，从设备迅速接替工作，保证业务持续性。 |
| 网口聚合：应支持平衡轮循环策略、主备份策略、平衡策略、广播策略、动态链路聚合、适配器传输负载均衡和适配器适应性负载均衡七种聚合模式 |
| 集群负载：具备自负载功能，无需使用第三方负载均衡设备。支持多台设备集群提升平台性能。 |
| 国产化支持：个人文件传输客户端应支持中标麒麟等国产化操作系统。 |
| 6 | 产品资质要求 | 具有公安部提供的销售许可证（三级或增强级）、提供证书复印件 |
| 具有计算机软件著作权登记证书、提供证书复印件 |
| 具有《信息技术产品认证证书》（ISCCC证书）、提供证书复印件 |
| 具有《信息技术产品安全测评证书》，不低于EAL3级、提供证书复印件 |
| 具有国家密码管理局提供的《密码检测证书》、提供证书复印件 |
| 7 | 服务 | 应免费提供三年硬件质保以及三年软件服务 |

### 服务详细指标要求

#### 定级备案

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 基于信息系统现状，参照信息系统安全等级保护定级指南，对系统现状进行调研，根据调研结果，确定定级对象，分析定级要素，根据等级保护对象受到破坏时所侵害的客体和对客体造成的侵害程度确定系统等级，编制定级报告并协助备案。 |
| 2 | 服务范围 | 北京老年医院指定系统 |
| 3 | 服务频次 | 服务期内提供1次 |
| 4 | 服务成果 | #《北京老年医院\*\*系统定级报告》 |

#### 安全加固

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 根据脆弱性检测等工作结果，结合用户信息系统业务需求，通过技术手段对信息系统相关的操作系统、数据库、中间件、网络与安全设备进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。 |
| 2 | 服务范围 | 北京老年医院指定系统 |
| 3 | 服务频次 | 服务期内提供2次 |
| 4 | 服务成果 | #《安全加固报告》 |

#### 管理制度修订

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 基于信息系统安全等级，根据分析和安全评估结果，依据国家信息安全等级保护管理要求，从网络安全管理制度、安全管理机构、人员安全管理、安全建设管理和安全运维管理五个方面编制网络安全等级保护管理制度体系。 |
| 2 | 服务频次 | 服务期内针对三级系统提供1次 |
| 3 | 服务成果 | #《北京老年医院网络安全等级保护管理制度体系》 |

#### 脆弱性检测

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 针对信息系统服务器操作系统、数据库、中间件、网络及安全设备等，采用工具扫描和手工检查相结合的方式对配置缺陷、漏洞等进行检查，以发现在网络、主机、应用等层面存在的安全隐患，通过专业化的技术分析，帮助用户了解自身信息系统的脆弱性。 |
| 2 | 服务范围 | 北京老年医院指定系统 |
| 3 | 服务频次 | 服务期内提供2次 |
| 4 | 服务成果 | #《北京老年医院\*\*系统脆弱性检测报告》 |

#### 应急响应

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 在信息系统发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持和快速响应，及时抑制和消除用户信息系统安全事件，减少损失和负面影响，提高用户信息系统业务连续性。 |
| 2 | 服务范围 | 北京老年医院指定系统 |
| 3 | 服务频次 | #服务期内按需提供（不少于3次） |
| 4 | 服务成果 | 《北京老年医院应急响应报告》 |

#### 安全巡检

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 利用检测工具和人工检测等多种方式定期对用户信息系统的服务器、网络及安全设备的健康状态进行检测，包括设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作,做好巡检记录，维护记录单，提交巡检报告。 |
| 2 | 服务范围 | 北京老年医院指定系统 |
| 3 | 服务频次 | 服务期内提供4次 |
| 4 | 服务成果 | #《北京老年医院安全巡检报告》 |

#### 堡垒机接口开发

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **规格要求** |
| 1 | 服务内容 | 针对北京老年医院的堡垒机开发接口，用于双因素认证 |
| 2 | 服务范围 | 北京老年医院堡垒机 |
| 3 | 服务频次 | 服务期内提供1次 |

## 项目服务要求

### （1）工期要求

本项目服务期限为1年，在本项目合同签订之后，1年内完成安全整改相关工作。

投标人的项目进度管理应该遵循以下原则：

（1）依据项目合同约定的工期目标，组织项目进度管理；

（2）在确保项目质量和安全的原则下，控制项目进度。

### （2）服务人员要求

投标人须为本项目组建稳定的、专业的、独立的项目团队，专门负责本项目服务实施工作，并进行相关的项目管控和随时调整项目实施方向。投标人须针对本项目成立专门的项目组，确保人力、物力的投入，项目组成员必须稳定，项目实施团队成员（不少于6人）在项目终验前如果人员退出或更换，需要征得招标人同意。

项目经理须具备丰富的信息安全知识，具有快速解决问题的能力，有较高判断故障和管理协调的能力，至少具有5年以上安全服务项目经验，能够深刻理解信息系统安全服务工作内容。

主要技术人员至少具有3年以上安全服务相关工作经验，具有网络安全相关认证资质证书。

### （3）质量保障要求

投标人在安全服务过程中应严格按照相关安全标准，针对安全服务的各个环节，提出有效质量管理计划、质量控制措施及风险控制规避计划,项目经理应在项目每一阶段，对实施过程的控制，调查、分析和解决发现的问题，问题及其解决办法都应写成文档（包括项目周报、会议记录等），保证项目按目标完成。

### （4）安全保密要求

投标人要严格遵守国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从北京老年医院的管理，严格遵守北京老年医院的保密规定和工作制度，并承担相应的保密责任。

投标人所有参与本项目的服务人员须签订《保密承诺书》。投标人负责对《保密承诺书》归档保管，接受北京老年医院检查。投标人要对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向北京老年医院报告。

投标人所有参与本项目的服务人员自觉接受北京老年医院的安全保密监督和管理，如违反安全保密条款，北京老年医院将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还应依法承担相应的民事责任。

### （5）验收要求

需提交的验收文件资料主要包括:

* 项目验收申请表；
* 项目设计方案及工程过程文档；
* 项目建设合同和有关修改、调整情况的纪要文件；
* 项目的技术报告和工作总结报告；
* 项目建设的技术资料及各阶段成果及过程记录文档；

**二、投标人的资格条件**

1) 投标人须为中华人民共和国境内注册的企业法人，且符合《中华人民共和国政府采购法》第二十二条的规定；

2) 具有良好的商业信誉和健全的财务会计制度；

3) 具有依法缴纳税收和社会保障资金的良好记录；

4) 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；

5) 具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类）证书；

6) 本项目不接受联合投标；

7) 符合法律、行政法规规定的其他要求。

**三、评分方法及标准**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目** | **评审内容** | **分值** | **评分标准** |
| 1 | 价格部分（30分） | 投标报价 | 30 | 价格分=最低价格/报价\*30\*100% |
| 2 | 商务部分（20分） | 企业资质 | 10 | 信息系统安全运维服务一级资质信息安全应急处理服务一级资质信息系统安全集成服务一级资质信息系统安全风险评估一级资质企业ISO27001信息安全体系认证证书每提供1个得1分。 |
| 同类项目业绩 | 10 | 投标人近三年（2016年1月1日起）所承担的50万及以上的信息安全运维服务项目（设备采购、设备租赁、软件开发金额除外），每提供一个得2分，最多10分。  |
| 3 | 技术部分（30分） | 需求理解 | 10 | 需求理解清晰、全面、准确，得8-10分；需求理解基本明确，不够全面、到位，得6-5；需求理解不够清晰、不准确，比较片面，得1-4分。 |
| 项目组人员情况 | 10 | 项目经理要求：项目经理需具有CISP证书、C-CCSK证书、ITIL证书、信息系统项目管理师证书及省部级专业职务任职资格评审机构颁发的高级工程师（信息安全专业）资格证书，5个证书全部具有得10分，有一项不满足整体扣2分。提供项目经理近三个月社保缴纳证明。 |
| 10 | 项目人员要求：核心骨干成员需要具备CISP资质证书每提供一个证书得1分，最高4分；项目团队其他成员需要具备CCIE资质证书每提供一个证书得1分，最高得3分；项目团队成员需具备CISSP证书，每提供1个证书得3分，最高的3分。 |
| 售后服务（20分） | 服务方式 | 14 | 1. 应免费提供三年硬件质保以及三年软件服务,10分。
2. 提供24小时电话、现场、远程、紧急和重大事件上门服务，每提供一种方式得1分。
 |
| 售后服务方案 | 3 | 售后服务方案全面细致可行、提供本地化服务，具备完善服务体系，具有完备的应急事件处置措施，服务标准不低于7\*24小时（优3分，良2，差1分）。 |
| 服务质量 | 3 | 根据响应时间及处理方案合理、可行性等横向评价，优3分，良2，差1分。 |