# 项目背景

本次项目将完善背景胸科医院信息系统的安全保障体系，建立多层次纵深的安全技术防护体系，降低信息系统的安全风险，确保业务的完整性、可用性。在信息系统满足等级保护三级要求的基础上，进一步强化安全措施，提高信息系统的安全防护水平。

# 预算金额

预算金额70万。

# 项目内容

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 数量 | 备注 |
| 1 | 业务域防火墙 | 2 | 更换业务域防火墙2台 |
| 2 | 零信任网关 | 1 | 新增零信任网关1台 |
| 3 | 防火墙授权更新 | 8 | 安管边界防火墙、二级域边界防火墙、政务专网和医保边界防火墙、医保-内网防火墙、原外网办公域防火墙、医保专网防火墙、PACS防火墙（2台） |

# 项目必要性

## 业务域防火墙更新必要性

（1）提升内网核心业务系统的安全性，抵御0day攻击、高级持续性威胁。

（2）安全合规，满足网络安全等级保护基本要求。

（3）提升处理能力和吞吐率，确保信息系统稳定运行。

## 零信任网关部署必要性

（1）确保每次访问都需验证，有效防御内部威胁，保护敏感数据。

（2）实现基于身份的细粒度权限管理，增强整体安全性。

（3）为远程医疗和移动办公提供安全通道，动态调整访问权限，保障数据安全。

## 防火墙授权更新必要性

（1）及时识别并防御新出现的网络威胁。

（2）修复漏洞，提升系统稳定性和性能，避免业务中断。

# 功能要求

## 防火墙

1、3年防病毒+IPS授权

2、吞吐≥8G，并发连接≥220万，新建连接≥6万

3、支持 IPSec VPN 功能

4、支持链路连通性检查功能。

5、支持基于IP对象的会话控制策略，实现并发和新建连接数的合理限制。

6、支持入侵防御

7、支持高可用或HA功能

8、支持双因素认证功能进行身份认证

## 零信任网关

1、支持国密算法

2、支持多种身份认证方式

3、支持异常登录行为审计功能。

4、支持配置虚拟专线功能，当用户登录零信任客户端之后，自动断开互联网连接，避免互联网威胁影响内网业务系统。

5、支持连接零信任网关前的终端状态检测

## 防火墙授权

### 安管边界防火墙

1、3年全功能模块升级订阅服务包（含应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）

2、3年硬件维保、软件升级服务及远程技术支持服务（95015电话支持、Email支持）

### 二级域边界防火墙

1、3年全功能模块升级订阅服务包（含应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）

2、3年硬件维保、软件升级服务及远程技术支持服务（95015电话支持、Email支持）

### 政务专网和医保边界防火墙

1年全功能模块升级订阅服务包（奇安信威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务）

### 医保-内网防火墙

1年全功能模块升级订阅服务包（奇安信威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务）

### 原外网办公域防火墙

1年全功能模块升级订阅服务包（奇安信威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务）

### 医保专网防火墙

软件升级、本地网关杀毒续费、深信服云智订阅软件（含安全特征库和URL库）1年授权

### PACS防火墙（2台）

1年病毒防护、1年IPS防护授权

# 售后服务

防火墙、零信任网关。3年软硬件免费质保。