**青浦区医疗付费“一件事”项目需求**

**包件一：青浦区医疗付费“一件事”区级平台项目需求**（P2-14）

**包件二：青浦区医疗付费“一件事”重要信息系统等级保护三级整改项目需求** (P15-82)

**包件三：社区卫生服务中心医疗付费“一件事”等应用改造升级项目需求** （P83-124）

**包件一：青浦区医疗付费”一件事”区级平台项目需求**

# 项目建设的背景

2019年底前市卫生健康委员会同申康中心组织各医疗机构鉴于国家医疗保障局尚无“脱卡支付”政策途径，因此仅对自费患者开展了移动支付，但仍不能满足医保患者的一次性移动支付需求。虽然，本市医疗机构通过增加诊间支付渠道，开设自助服务一体机，增开支持扫码支付的收费服务，柜台窗口等方式，从一定程度上提升群众诊疗付费便捷程度，各大医疗机构排队状况得到初步缓解，但距离群众期望还有较大差距。

目前医疗付费业务流程主要存在的问题是办事不够集约高效，在传统医疗服务流程中，医疗付费业务流程包括排队调整，排队付费（挂号费）、排队候诊，排队付费（检查检验费）、排队检查检验，排队付费（药费）、排队取药……就医过程中被动排队等待耗时占比比较多，本市三甲医院的门诊患者平均就诊时间约三个小时，其中排队时间占到75%，就诊时间只占到25%.

因此，为贯彻国务院“互联网+医疗健康”战略，坚持以人民为中心的发展思想，以患者高效办成医疗付费“一件事”为目标，紧扣“信用就医、无感支付、不排队、少往返，一网通办”等关键字，全面提升群众办事的便捷度、体验度和满意度。

# 建设目标

建设青浦区统一支付平台，以区为单位，依托市大数据中心“随申办”统一平台能力，作为医疗付费“一件事”总入口，打造“基于信用无感支付”的信用就医新型服务体系。

具体目标：

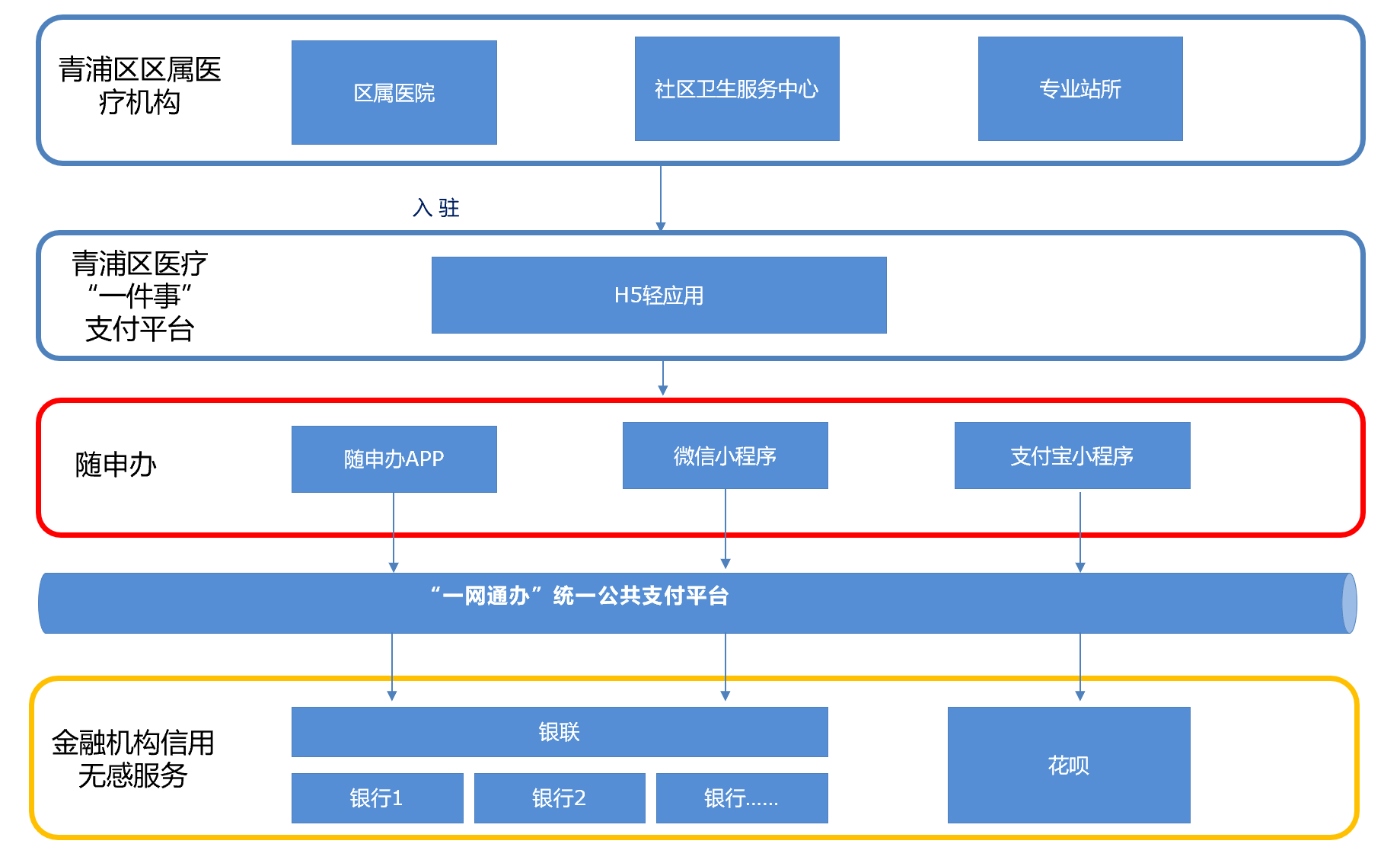
1、面向本市医保患者开展基于“医保电子凭证”的实名认证，提供线上签约和额度授信。

2、以H5标准页面形式入驻随申办APP,实现各级医疗机构统一入口、身份校验、协助付费对账和征信名单共享等服务功能。

3、推进医疗当日结算等支付聚合平台运行，实现各级医疗机构与上海市大数据中心每日实时对账与结算机制。

4、完成区级平台付费一件事与社区医院的HIS系统对接事宜。

# 总体架构



区各级医疗机构利用搭建的青浦区医疗一件事支付平台，接入“随申办”移动端信用就医总入口, 实现医保电子凭证在“随申办”上的申领服务，依托银行等金融机构信用体系及免密支付功能，实现“基于信用的无感支付”服务。

# 建设内容

## 认证授权

* + 1. “随申办”移动就医入口

“随申办”移动端是上海“一网通办”移动政务服务的总入口，包括随申办市民云APP、随申办微信小程序、随申办支付宝小程序三个渠道。

在入驻随申办前需先通过上海市民云开放平台进行应用服务商注册认证，认证后的应用可调用随申办开放接口，开发移动就医功能。

### 医保电子凭证认领

患者在使用随申办应用完成结算前，需在线签署支付协议，完成“医保电子凭证认领”。平台需与随申办用户实名认证体系进行对接，获取当前访问用户关联的姓名、身份证等实名信息，并获取用户医保电子凭证信息，用于向医保发起医保结算申请。

### 费用结算支付管理

与随申办应用提供的结算方式进行对接，包括银联、支付宝、微信等常见付款方式，用户进入收银台后可按需选择付款方式完成自费部分的付款。

### 亲情付代扣管理

对于已领取了医保电子凭证，不会使用手机移动支付的老年人、儿童等人群，支持“亲情付”代扣付费功能，通过关联绑定其父母、子女、配偶等银行卡，完成线上签约。

## 市大数据中心支付（基于信用的无感支付）

### 信用签约查询

基于市大数据中心的统一信用签约平台，为本市居民提供医疗信用专项额度，查询患者签约情况，符合使用条件的患者可使用信用免密支付功能。

### 信用免密支付

已签约信用就医的患者到达医疗机构并进行完诊疗服务后系统自动发起基于信用的无感支付服务，发生医疗费用的医保部分实时结算，自费部分由绑定的信用账户进行支付，在整个诊疗行为中患者无需任何付费动作，支付平台统一和大数据中心对接信用签约免密支付，协助医院系统完成患者整个信用就医的诊疗行为。

## 在线诊间支付

### 支付信息查询

支持患者完成诊疗行为后，在随申办app上查看待支付的订单信息，以及当天发生的所有费用信息

### 医保在线支付

支持医保患者支付时医保部分能实时结算，自费部分由随申办支付平台扣除，实现医保患者在线脱卡支付功能。

支持医保患者在线退费，退费渠道为原路返回，即返回患者医保账户。

### 自费在线支付

支持自费患者支付能实时结算，由随申办支付平台扣除，实现患者在线脱卡支付功能。

支持自费患者在线退费，退费渠道为原路返回，即返回患者金融账户。

### 入驻随申办app

4.1.1.1简述

医疗付费一件事H5页面加载于随申办APP中的医疗服务板块。市民打开随申办APP，点击医疗菜单，选择全市医疗机构线上服务专栏中的青浦区，即可跳转至上海青浦区卫健委页面办理结算支付等业务。

市民在医院诊疗完成后，首先在本区医院列表中选择医院，医院列表支持按医院等级排序，按医院距离排序方便市民选择医院。点选医院后跳转到对应的医院页面，显示市民的就诊卡信息供患者确认，显示门诊结算、结算记录等功能入口。

市民办理结算业务选择门诊结算，平台通过HIS接口获取到就诊人对应的结算信息，以结算详情页方式显示在H5页面上，就诊人确认结算信息无误后进行结算。平台HIS向医保发起完成医保结算。需要自费支付的部分进入收银台页面提示就诊人进行线上支付，支付完成后结算流程结束。

市民通过结算记录按钮查看自己的结算记录。进入结算记录页面后，可选择查询起始时间段（起始时间与结束时间），页面根据结算时间展示查询时间段内的结算信息，信息项中显示：就诊科室、就诊日期、主诊断以及结算详情按钮。市民选择要查看的结算项，点击结算详情按钮查看详情。结算详情以列表形式展示，详情项中显示结算时间、总金额、个人支付金额、医保支付金额以及其它按钮。市民点击其它按钮查看费用详情，详情页以细项显示药品费用等信息。

4.1.1.2建设功能模块

区属医院选择

在全市医疗机构页面选择青浦区后，显示青浦区医院列表，该页面包含三个模块：搜索框、附近医院、本区医院。

在搜索框中输入医院名称搜索医院。

附近医院模块自动显示显示地理位置离市民最近的那家医院。

在本区医院列表支持按医院等级排序，按医院距离排序，方便市民选择医院。列表中每家医疗机构项包含医院图标logo、医院等级（三级、二级、一级）、医院名称、距患者所在地距离以及医院地址。

查询就诊卡信息

患者选择就诊医院后，根据随申办用户实名认证返回的身份信息向his获取绑定的就诊卡。需提供用户界面，显示就诊人姓名、就诊卡号等信息，并提供切换就诊卡的功能，拥有多张就诊卡的患者可自由选择就诊卡进行结算。

查询待支付订单

患者选择就诊医院获取患者就诊卡信息后，查询患者在院内的待支付订单信息。需提供用户界面，显示订单金额、发生时间、收款项目、单价等信息，并提供付款入口，在患者确认订单信息无误后，可进入线上付款渠道。

医保预结算

患者选择订单支付时，平台需通知his向医保发起预结算，收到医保预结算信息后，由HIS将预结算结果发送至平台，平台进行记录并展示。

医保结算确认

患者支付订单若包含医保结算金额，则在患者完成支付后需通知HIS向医保发起结算确认，完成医保支付。

收银界面页

患者选择订单进行支付后，需提供用户界面，向患者展示医保结算金额、个人自费金额等信息，并可按需选择随申办提供的付款方式（目前仅支持银联），确认后可进行个人自费金额付款。

线上支付功能

平台需与随申办提供的付款方式（目前仅支持银联）进行对接，在患者选择付款方式提交付款后，可跳转相应的收银台完成线上支付。同时平台需服务商返回的付款结果，确保平台付款结果与服务商付款结果一致。

查询结算记录（包括信用付）

市民通过结算记录按钮查看自己的结算记录。进入结算记录页面后，可选择查询起始时间段（起始时间与结束时间），页面根据结算时间展示查询时间段内的结算信息，信息项中显示：就诊科室、就诊日期、主诊断以及结算详情按钮。市民选择要查看的结算项，点击结算详情按钮查看详情。

查询结算详情

结算详情以列表形式展示，详情项中显示结算时间、总金额、个人支付金额、医保支付金额以及其它按钮。市民点击其它按钮查看费用详情，详情页以细项显示药品费用等信息。

查询费用明细

患者在进行结算详情查询后，可向下查询包含的全部费用信息。需提供用户界面，显示收费项目名称、单价、数量、金额等信息，以便患者查阅确认。

区订单汇总功能（包括信用付）

平台需提供区属全部医院订单查询的功能，患者无需进入医院，可通过此功能查看在区属医院就诊，且通过平台完成结算的全部订单信息。需提供用户界面，显示就诊医院、科室、支付金额等信息，如果可退款，还需提供退款的入口。

线上退款功能

患者在选择区订单信息进行查阅时，平台需向his请求订单状态，若该订单尚未进行（即已完成支付，但未开始治疗），则可通过平台发起进行退款，his在接收退款信息后进入退费流程，并向平台返回退费结果。

就诊人管理功能

平台需提供就诊人管理功能，对部分没有能力自行使用平台完成付款的患者（如不善用手机的老人、儿童等），可由亲属或其他人员绑定就诊人完成付款。若需进行医保结算的，则应必须由亲属进行关联才可向医保发起结算。就诊人管理需提供用户界面，由用户录入患者姓名、身份证等信息完成绑定，绑定其他就诊人后可进行切换，并可查询其待支付订单，通过线上完成支付。

用户认证功能

平台需与随申办用户实名认证体系进行对接，获取当前访问用户关联的姓名、身份证等实名信息，通过平台查询医院订单、医保结算等都必须用实名信息进行关联。

4.1.1.3 H5页面建设清单

待结算单据页面

订单详情页面

结算记录页面

收银台页面

支付结果页面

选择医院页面

认证失败页面

结算详情页面

费用详情页面

## 支付渠道管理

### 微信支付

接入第三方微信支付的扫码付，支持通过对第三方微信支付渠道管理，实现微信交易信息下载与异常账目发现和处理，包括与微信进行支付、退款确认、还款，以及实现对网络异常导致的支付退款消息重发确认机制。

### 支付宝支付

接入第三方支付宝支付的扫码付，支持通过对支付宝的渠道管理，实现支付宝交易信息下载与异常账目发现和处理，包括与支付宝进行支付、退款确认、还款，以及实现对网络异常导致的支付退款消息重发确认机制。

### 其他支付方式

支持与其他第三方支付渠道连接进行充值、退款及相应的交易信息下载和确认。

## 信息管理

支付平台向医院及第三方支付平台开放对账后台，提供历史费用订单明细数据及时间范围条件下的总订单数量、订单总账和异常账数量及明细供查看。同时需支持提供简单的数据报表及数据导出功能，供进一步统计分析使用。

### 支付请求服务

提供支付请求的入口，来自移动端响应支付成功的通知。

### 聚合支付

整合支付宝、微信等多种当前热门的支付渠道，提供多种支付渠道同一个支付二维码的聚合支付服务。

### 支付信息识别

能够自动识别用户支付扫码信息，区分微信、支付宝等多种支付渠道，与对应的第三方支付平台进行支付服务对接，完成支付服务。

### 订单号生成服务

用户扫码后，统一支付平台将会动态的生成订单号，保证该次扫码支付的唯一性，避免了多人同时扫码、多渠道扫码支付等误操作造成的多次支付问题。

### 商户号管理

用户扫码支付后，统一支付平台请求第三方支付平台进行交易，根据交易订单动态生成商户号，为后续的异常退款、对账提供识别的依据。

### 支付信息确认

用户扫码后将会提供支付信息确认，包括充值卡号、姓名、手机号码、支付金额等，让用户进行支付信息的确认，减少支付错误的可能性。

### 交易信息确认

通过第三方确认完成的用户支付信息由平台统一管理，并形成有效的通知机制，返回给订单发起方，完成业务闭环。

## 退款管理

H5应用支持对在线完成支付且未进行医疗服务的订单申请退款，同时统一支付平台支持对异常账、单边账进行退款处理，对退款余额不足部分进入退款队列，无需人为干预，平台将根据退款优先级自动处理。此处退款只针对单笔充值的异常账退款，不涉及已充值成功的预交金部分，预交金退款需患者前往线下窗口。

### 自动退款管理

用户通过H5完成的支付订单可在线申请退款，若尚未进行医疗服务的，则由系统自动完成退款处理。

### 退款队列管理

针对支付超时、支付取消等操作，导致用户支付完成，但支付平台没有正常完成交易的支付问题时，业务经办人员可通过支付平台完成退款服务，避免了单边账的产生。

由于账户中的金额每天定时流转，在当天医院第三方账户收入不足时，将有可能导致隔日退款的用户存在无法成功退款的问题。统一支付平台支持通过退款队列服务，把退款任务依次加入到队列中进行自动退款操作，确保24小时内能够自动退款成功。

### 退款状态查询

成功退款后，具体到款时间将参照患者使用的第三方支付平台所规定的退款周期，有可能会有延迟。平台通过定时查询服务获取第三方退款状态，并记录退款明细。

## 统一对账

提供电子化的对账方式，各接入医院可以自行获取对账明细，平台也提供各家医院的交易对账报表。平台每日将自动生成前一日的清算汇总清单、清算明细单等数据文件。

### 交易信息查询

通过记录每一笔支付的请求信息与第三方交易明细进行比对，提供交易信息的查询服务，方便快速定位每一笔交易的交易时间、交易方式及交易支付方的信息。

### 成功充值统计

充值成功统计每一笔成功完成支付的订单信息，平台记录每笔订单的充值时间、患者姓名、充值金额及相关的订单号信息，方便管理人员查找每一笔交易记录。

### 异常充值统计

异常充值统计交易过程中由平台及第三方超时、取消等引起的充值异常，为管理人员对账管理，查找异常账、单边账提供入口。

### 分账统计及下载

根据所有医疗机构产生的支付记录根据不同的医疗机构维度，在支付平台上进行分账统计，最终根据分账统计结果，进行各医疗机构金融虚拟子账户的分账，同时为各医疗机构提供账单下载功能，方便各医疗机构自行对账。

### 自动下载对账

平台需支持自动从微信、支付宝及银行方面下载相应的交易记录和提现记录，进行平台内部自动对账，对于异常账款可进行自动标识，确保分账对账的可靠性。

## 基础平台

为保证支付平台及支付数据的安全，整个统一支付对账平台架设于基础安全平台之上，采用“数据+服务+应用”的模式设计，通过提供可供开放的数据服务，以信息资源服务目录列表形式在安全平台门户上展现，采用高效率、高质量的方式帮助开发者实现数据整合。

### 节点管理与授权

节点指安全服务组件以外与服务进行交互的接入端点，可以是基于平台的应用系统，也可以是平台外部的其它平台或系统。系统外部服务可以通过授权管理快速对服务进行适配，服务授权通过授权码和密钥来实现对调用机构的认证，对每个接入的实体分配一个授权码，并生成数据加密的公私钥，外部系统通过授权码进行相应服务的调用，以此判断接入者的身份，避免出现数据及系统的安全问题。

### 负载集群管理

为了提高系统的健壮性和稳定性，应对高并发的数据访问请求，组件接入的服务可以部署在多台服务器上，组成一个服务集群。用户发起API调用时，可以根据负载均衡算法，将请求发送到不同的服务器上，起到分流的效果。通过集群管理可以监控集群中服务器的运行状态，新增或删除集群服务器。

### 后备管理机制

作为一个为多种应用提供服务的安全管理组件，自身的高可用性也是一个非常重要的环节。当一台服务器出现故障后，能够自动地将服务请求切换到备份服务器上，保证服务的连续性和生存率。

### 日志审计机制

通过定期对用户的访问行为进行分析，对访问日志分级分类，设置服务的访问频率，把单位时间内不正常的访问行为设定为可能的非法行为，自动将访问用户IP加入黑名单，进行隔离。

通过日志审计机制，增强了组件的安全管控能力。

### 机构接入SDK

统一支付平台提供各医疗机构接入的SDK，各医疗机构可根据各自HIS系统的开发语言选择不同的SDK，进行开发接入。

## 软件建设要求

操作系统： Centos 7 64位；

数据库软件：MySQL（64位）

## 硬件及网络环境要求

**本项目硬件使用区政务云6台服务器。**

服务器配置如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 网络环境 | CPU (核) | 内存 (GB) | 硬盘 (GB) |
| 互联网 | 8 | 16 | 600 |
| 8 | 16 | 600 |
| 政务外网 | 8 | 64 | 600 |
| 8 | 64 | 600 |
| 8 | 16 | 600 |
| 8 | 64 | 600 |

# 项目建设周期

本项目建设周期为3个月。

# 验收要求

1. 建设内容完成后，中标方应对相关建设内容进行完善的系统测试，并通知用户方进入系统试运行期。系统试运行为期一个月，与此同时中标方提供试运行期系统测试文档和项目验收相关文档，并且对用户方相关人员提供完善的培训。
2. 中标方提供全套完善的项目验收资料文档，包括配置文档、使用说明书给用户，并想用户书面提出申请项目验收，用户方在审查验收资料无误后同意召开项目验收会。
3. 由用户指定时间地点并邀请相关专家参加项目验收会，就项目建设内容依据验收资料文档等进行项目验收，并出具专家验收意见书作为项目验收的结论性文件。
4. 该项目必须满足国家最新版信息安全三级等保建设要求。

# 其他要求

投标单位必须提供如下系统演示界面，以刻录光盘的形式提交，光盘的刻录格式要求建议：1）功能点分段录制2）每段不超过3分钟3）每个功能点建立名称。光盘内容包括但不限于如下功能点：

1. 对不同医院完成的线上支付订单可统一进行查询；  
   ② 在院内绑定多张就诊卡的，可切换查询不同就诊卡查询就诊信息；  
   ③ 在医院开具处方后，可使用平台查询就诊人待支付订单信息；  
   ④ 可查询订单包含的收费项目的价格明细。

**8、售后服务保障**

1. 本项目提供1年的免费质保服务（免费质保期自项目验收合格之日起计算）。免费质保期内提供包括邮件、电话、远程维护等方式，如遇重大故障或远程无法解决时，需排人现场解决，保证有足够的人员及技术支持电话负责本系统运维工作。
2. 投标人在投标文件中必须明确承诺达到用户的服务响应要求：免费质保期内提供7×24小时响应服务；重大故障应在接到通知后2小时内响应，一般故障应在接到通知后4小时内响应，要求在12小时内解决相关故障问题使其恢复正常。
3. 适应性和完善性维护：乙方提供应用软件功能维护、咨询和用户提出的不超过合同范围的功能修改。

**9、知识产权归属**

对已存在的知识产权归原拥有方所有，因本项目新开发出来的技术成果的知识产权（含著作权）归甲方所有。

**10、其他说明**

与本项目相关的第三方接口，须与甲方合力沟通协调，总报价不包含本区域内对接医疗单位的第三方接口费用。

**包件二：青浦区医疗付费“一件事”重要信息系统等级保护三级整改项目需求**

# 项目概述

## 项目概况

1. 项目名称：青浦区医疗付费“一件事”重要信息系统等级保护三级整改项目（以下简称“本项目”）
2. 总预算：864.66万人民币，区财政资金，超过预算金额的投标将不被接受（不包含二类费用）
3. 项目类型：系统集成及服务项目，包含设备安装调试、等保测评相关整改以及驻场运维服务等。
4. 建设位置：上海市青浦区华科路550弄7号楼（区卫生中心机房）以及青浦卫健委下辖11个社区卫生服务中心IT机房。
5. 建设内容概要：根据青浦卫健委和下辖11个社区卫生服务中心的网络安全实际情况和安全等保建设标准为基础，按照统一招标分级建设的原则，按照等保三级2.0标准和要求，完善必要的网络安全基础设施，建立一套完整可靠的信息安全防护系统，包括安全硬件、态势感知及安全运管平台软件、网络设备和相关安全服务等，最终以通过网安部门的三级等保测评为目标，旨在为区卫健委建立一套管理统一、标准统一、措施统一的信息安全防护和运维相结合的安全体系。
6. 建设单位及地址：上海市青浦区卫生健康区级中心及其辖区11个社区卫生服务中心，包括：
7. 青浦区卫生健康区级中心（地址：上海市青浦区华科路550弄）
8. 白鹤镇社区卫生服务中心（地址：上海市青浦区白鹤镇外青松公路2961号）
9. 华新镇社区卫生服务中心（地址：上海市青浦区华新镇华志路800号）
10. 金泽镇社区卫生服务中心（地址：上海市青浦区培育路271号）
11. 练塘镇社区卫生服务中心（地址：上海市青浦区练塘镇朱枫公路3619号）
12. 夏阳街道社区卫生服务中心（地址：上海市青浦区崧润路779弄）
13. 香花桥街道社区卫生服务中心（地址：上海市青浦区赵屯镇大盈社区新桥路1195弄1号）
14. 徐泾镇社区卫生服务中心（地址：上海市青浦区徐民路1088号）
15. 盈浦街道社区卫生服务中心（地址：上海市青浦区盈浦街道盈福路50号）
16. 赵巷镇社区卫生服务中心（地址：上海市青浦区赵巷镇巷居路289号）
17. 重固镇社区卫生服务中心（地址：上海市青浦区重固镇联茂路68号）
18. 朱家角镇社区卫生服务中心（地址：上海市青浦区朱家角镇曲池路39号）
19. 建设周期：签订合同后60个日历日完成项目建设工作。

## 项目政策背景

《卫生部关于印发<卫生行业信息安全等级保护工作的指导意见>的通知》（卫办发【2011】85号）明确要求：卫生行业各单位应当按照信息系统安全建设整改方案，完善安全保护设施，建立安全管理制度，落实安全管理措施，形成信息安全技术防护体系和信息安全管理体系，有效保障卫生信息系统安全。上海市卫健委高度重视医疗行业的等级保护工作，2012年就下发《关于组织开展本市卫生信息系统安全等级保护工作的通知》（沪卫办[2012]33号），将安全等保测评作为计生卫生行业的重要考核指标。

2019年初发布了《(沪卫计信息[2019]2号)关于进一步调整本市卫生健康行业重要信息系统等级范围的通知》，将区属医疗机构的核心业务系统纳入等级保护第三级要求，进行安全防护。但是目前区属各医疗机构的信息系统的安全保障工作目前已滞后于业务应用的发展，在关键应用区域边界、防入侵、防病毒、安全审计、漏洞扫描、态势感知、运维监控管理等方面不能适应信息化系统高可靠性及信息保密性的要求，系统在防范内部人员及外部人员等方面的技术措施有一定的差距，需要根据等级保护标准要求采取技术措施和管理措施，全面加强信息系统的安全保障工作。在各区属医疗机构现有安全体系架构基础上完成相关设备的集成实施工作，满足区属医疗机构信息系统安全定级需要以及提高整个区属医疗机构业务系统的安全性。

前期区卫健委对全区卫生信息化工作开展了大调研，其中专门针对各单位信息系统进行了信息安全专项检查，根据等级保护三级的相关要求，全面分析了各单位信息安全方面存在的问题，并就各单位后续开展信息系统安全等级保护建设给出指导意见。

根据区卫健委前期必要性评审结果和相关工作要求，结合社区卫生服务中心信息安全建设的实际情况，本次项目计划建设一个区级信息安全态势监管和安全运维管理处置平台，同时依据三级等保2.0标准，将卫健委中心机房以及社区卫生服务中心安全边界、核心业务、安全运维管理系统进行加固，完善必要的网络安全基础设施，提升整体业务系统安全性，并使目标系统通过三级等保2.0测评。

## 项目建设依据

2017年6月1日《中华人民共和国网络安全法》的正式实施。标志着从国家层面：维护网络空间主权和国家安全、社会公共利益。从企业层面：规范相关行业。从公民层面：保护公民法人和其他组织的合法利益。

2019年12月1日重新修订颁布的《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019），标志着等级保护正式进入了2.0的时代。

为确保本市卫生医疗机构重要信息系统安全平稳运行，切实提高卫生医疗机构信息安全保障能力，根据《信息系统安全等级保护管理办法》要求，市卫健委下发沪卫计信息11号文《关于调整本市卫生计生行业重要信息系统定级范围的通知》、沪卫计信息〔2019〕2号《关于进一步调整本市卫生健康行业重要信息系统等级范围的通知》，沪卫计信息〔2019〕2号中对三级等保的范围进一步明确，要求涵盖 HIS、LIS、RIS、PACS、电子病历核心数据库、医院信息才加及数据中心平台等的核心信息系统，安全保护等级原则上不低于第三级，等级保护2.0相关标准也已于2019年12月1日期开始实施。在最新的《关于印发2020年上海市卫生健康工作要点的通知》沪卫发〔2020〕003号，通知中继续要求开展全行业网络安全和信息化保障工作，重点指导行业内单位做好信息系统等级保护2.0。

## 项目建设的指导性文件

1. 《中华人民共和国网络安全法》
2. 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
3. 《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）
4. 《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）
5. 《信息安全技术网络安全等级保护安全管理中心技术要求》(GB/T 36958-2018)
6. (沪卫计信息[2019]2 号)关于进一步调整本市卫生健康行业重要信息系统等级范围的通知

## 项目建设总体目标

根据国家、上海市关于网络安全、网络安全等级保护和医疗卫生行业信息安全等级保护等方面的法律法规、标准规范、工作安排等要求，按照青浦区卫健委关于全区医疗卫生机构等级保护工作的统一要求和统筹安排，结合本单位的相关现状和前期青浦区信息化大调研的信息安全板块调研及分析研判结果，通过本项目安全相关内容的建设，机房整改建设、已经初步完成的既有安全技术措施策略完善和安全管理方面整改等工作内容，以管理为核心，以技术为手段，建设符合本单位实际安全需求、符合三级等保要求的技术体系、管理体系、服务体系，实现集防护、检测、响应、恢复于一体的安全保障体系，提高全区域医疗卫生机构的信息系统安全防护能力，降低信息系统被各种威胁源攻击、数据泄露等风险，确保全区域医疗卫生机构所支撑的各项业务、管理、服务工作的正常有序可靠开展，保持青浦区医疗卫生机构的良好形象，总体的安全等保三级测评得分达到82分以上，提升全区医疗卫生健康系统在全市的信息安全的相关排名。

在集约化建设方面，协同青浦区卫生健康委员会和各社区卫生服务中心作整体安全防护。“一个安全管理中心和11个安全管理子节点”，在青浦区卫生健康委员会中心机房部署安全管理中心节点，通过数据可视化平台将11个社区的安全态势展现出来。另外在11个社区卫生服务中心部署安全管理子节点和边界防火墙构建本地安全防护能力。设备选型在满足等保三级要求的前提下，充分考虑社区现有设备和安全服务情况，选择性能优、技术新、稳定性好的设备，补足社区端安全防护的不足。

整合青浦各社区卫生服务中心安全设备运行状态、运维保障状态的数据，建立以安全为视角的综合可视化全局视图。对每一个节点的安全子系统进行可视化监控呈现，实现整体安全过程的可视化展示，全面、准确、实时的反映安全运行状态。

以上目标可具体归纳为如下三点：

目标1：对上海市青浦区卫生健康委员会及其辖区内各社区卫生服务中心进行等级保护合规性整改，包含：安全物理环境改造、安全通信网络改造、安全区域边界改造、安全计算环境、安全管理中心改造等内容。青浦区卫生健康委员会及各社区卫生服务中心，12家单位需分别取得网络安全等级保护测评报告，并得分达到82分以上，提升全区医疗卫生健康系统在全市的信息安全相关排名。

目标2：对上海市青浦区卫生健康委员会及其辖区11个社区卫生服务中心重要网络和业务系统进行安全加固。

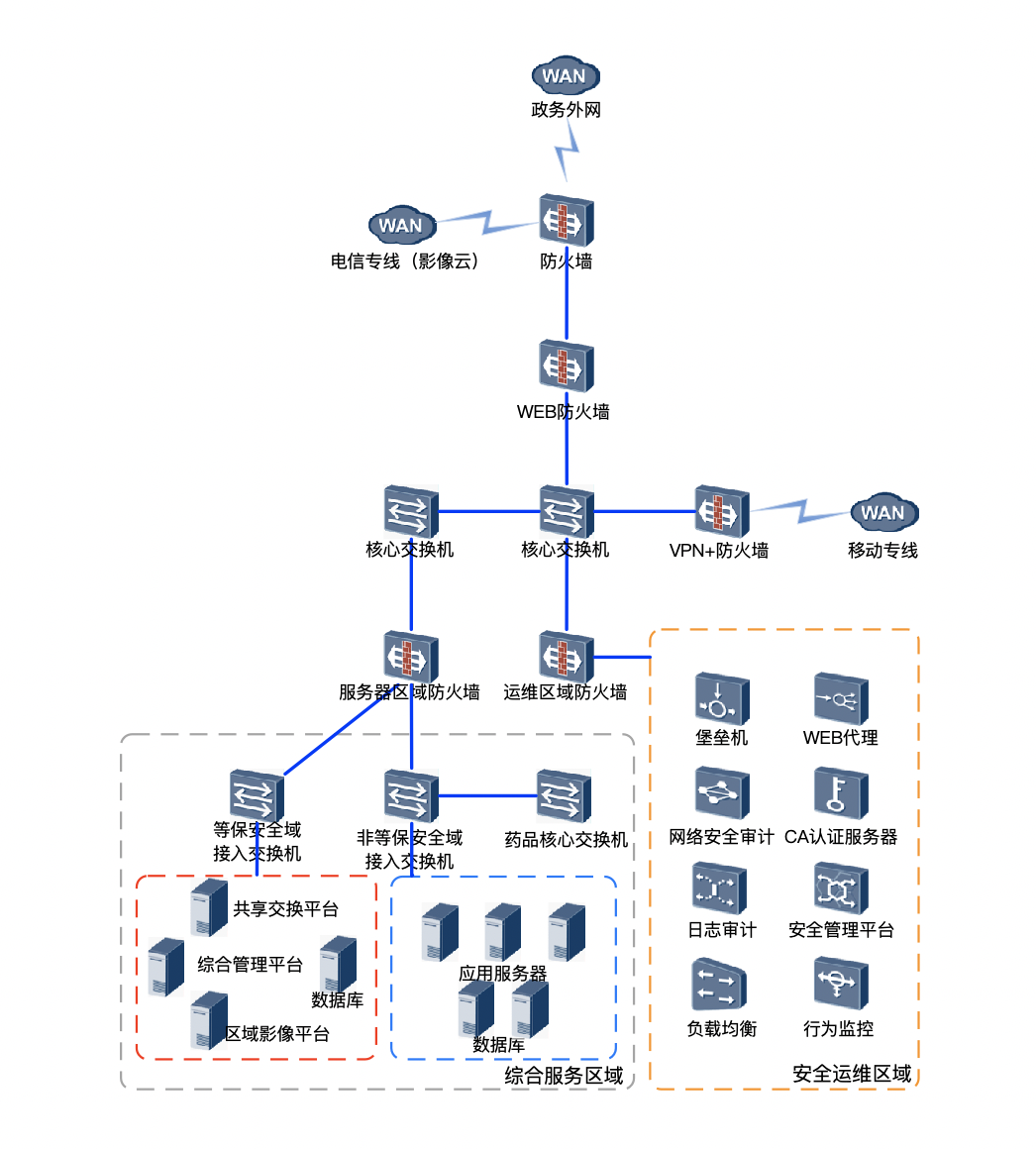
目标3：通过构建一个安全管理中心、三重防护体系来达到青浦卫生网络信息系统整体的网络安全数据可视化平台。

# 现状描述及建设要求

## 青浦卫健委网络系统现状

青浦区已建立连接区域内二级医院、社区卫生服务机构、卫健委及直属机构的卫生信息专用网络。区内5家二级医疗机构、11家社区卫生服务中心都采用电信的1000M 光纤专线接入政务外网，201家标准化村卫生室通过村村通接入政务外网。

青浦卫生信息网络拓扑图见下图：



## 总体建设要求

1. 投标方提供的设备符合等保要求，成熟度、安全性和先进性同时具备。
2. 投标方提供的设计方案符合青浦卫健委网络安全系统的现状要求和发展趋势。提供网信办，公安，卫生主管部门及区级主管部门的信息安全监管要求、政策法规文件、安全检查通知、安全事件预警等相关政策规范文件的发布和管理并形成安全管理知识库，能够与视频会议系统对接，形成视频培训资料知识库供全区在线学习使用。为全区贯彻落实信息安全政策和要求提供法律和政策依据。
3. 投标方承诺帮助青浦卫健委和下辖11个卫生社区服务中心通过等保三级测评，目标82分以上。
4. 安全数据可视化及运维管理平台：1）提供全区信息安全主要概况的整体大屏展示功能（可在地图上标识医疗卫生机构以及主要预警提示等）；2）管理中心可根据历次预测评、测评、季度常规检查、专项检查、重大保障检查以及各医疗卫生机构的事件上报等检查内容，汇总分析全区信息安全整体情况，针对不同的检查要求对全区医疗机构的安全问题进行综合排名，对全区共性的安全问题进行综合排名，对各医疗卫生机构的安全问题进行综合排名，需提供相关综合排名的算法规则模型；3）形成包括但不限于全区等保预测评汇总分析、正式测评汇总分析，季度常规检查汇总分析、专项检查汇总分析、重大保障检查汇总分析并可将分析报告（分析报告中需说明未及时反馈情况、安全问题反馈情况、主要安全漏洞情况、问题整改及跟踪情况等）。

## 设计规划原则

由于青浦卫健委安全等保三级建设过程中具有相关设备数量庞大、全区分布广、涉及系统面广、卫生数据庞杂且关键、业务重要性高、网络结构复杂、旧有软硬件历史年限长、等特点，给合以往项目中的网络设计、建设以及维护提出了更高要求。为了青浦区卫健委网络安全系统能够更好的吃撑业务为应用系统提供安全服务，将组建一套技术先进、扩展性强、冗余度高、易于实现和管理的网络安全系统，新建设的网络安全系统将完全是一个高效、稳定、可靠和安全的电子业务综合承载传输平台，将能够充分满足信息管理系统对网络支撑平台的要求。网络必须具有良好的安全防范措施，灵活方便的权限设定和控制机制，使系统具有多种有效手段，防范各种形式对网络的非法入侵和内部攻击，以保证网络的实体安全、网络安全、系统安全和信息安全，有效地保障正常的业务活动和防止内部信息数据不被非法窃取、篡改或泄漏。

1. 自主保护原则

信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

1. 重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。特别针对重要的信息管理系统，应采取足够强度的安全防护措施，确保其能够更好的支撑各类业务的运行。

1. 同步建设原则

信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

1. 动态调整原则

要跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

1. 标准型原则

本项目需要严格遵守国家相关政策和标准，进行全面的设计。

1. 灵活性原则

考虑到相应标准的不断完善过程和滞后性，在没有标准依据的地方，我们将通过对等级保护的理解，自行设计相应的保障措施，考虑到产品测评认证的滞后性和片面性，在没有相关通过认证的产品可选用时，将使用通过最高认证级别的产品。

1. 实用性原则

在确保信息系统性能和安全的前提下，充分利用资源，讲究实效，避免重复和盲目投资，积极采用国家法律法规允许的、成熟的先进技术和专业安全服务，运用科学的经营管理方法，降低成本，保障安全运行。

## 现场踏勘要求

本项目统一组织踏勘现场，踏勘时间2021年1月6日10:00,踏勘地址：青浦区华科路550弄7号楼三楼，踏勘联系人：丁佳俊，联系电话：69716215（只组织一次，踏勘卫健委指定的2个建设点）

招标方统一组织投标单位前往卫健委核心机房以及一个社区卫生服务中心机房进行现场踏勘，投标方取得经由招标方签字的现场踏勘记录，并根据现场踏勘情况提出网络安全加固改造方案。

## 投标报价要求

★为符合该项目区卫健委统一招标、区级和社区分级建设的要求，投标方提供的报价明细清单需针对卫健委中心端和11个社区卫生服务中心分别提供，方便各单位资产入库管理和维护，加总报价需为本项目投标总价。

**见招标文件格式**

## 方案可靠性要求

为确保投标方提供的安全产品选型、安全加固方案和安全运维服务能够最终帮助区卫健委中心端和11个社区卫生服务中心分别通过等保三级测评，并达到82分以上的要求，投标方需和具有信息系统安全等级保护测评资质的等保测评机构充分沟通，并取得等保测评机构针对本项目的合作协议或投标授权书。

## 信息保密要求

没有青浦区卫健委事先书面同意，投标单位不得将青浦区卫健委提供的与本工程相关的任何资料（文件、规格、工程计划、图纸等）以及为本工程设计的任何资料提供给任何第三方、与本工程无关的单位任何人。

对系统的保密范围要求：投标人承诺在实施和维护过程中，任何涉及用户及医院的信息，包括但不限于医 院数据、特有的功能需求等，未得到招标人同意的情况下不得对任何第三方展示、举例乃至销售，否则投标人将承担由此产生的一切后果。

投标单位参与本工程施工工作的任何人员，对上述资料遵守国家有关保密规定。

青浦区卫健委对投标单位提供的设计施工资料应遵守国家有关保密规定。一经发现一方泄密，按国家有关规定处理。

# 建设内容及分项技术要求

## 招标设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **简要功能配置要求** | **数量** | **备注** |
| **区卫健委中心管理端安全加固** | | | | |
| 1 | 出口边界防火墙一 | 网络层吞吐量≥10G，应用层吞吐量≥2.5G，至少16个千兆电口，8个千兆光口。含IPsec VPN模块、入侵检防御模块及防病毒模块，包含三年升级及维保。 | 2 | 异构配置 |
| 2 | 出口边界防火墙二 | 网络层吞吐量≥12G，应用层吞吐量≥2.5G，6个千兆电口，4个千兆光口插槽。含入侵检防御模块及防病毒模块。包含三年升级及维保。 | 2 |
| 3 | 区域边界防火墙一 | 网络层吞吐量≥10G，应用层吞吐量≥2.5G，至少16个千兆电口，8个千兆光口。含IPsec VPN模块、入侵检防御模块及防病毒模块，包含三年升级及维保。 | 2 | 异构配置 |
| 4 | 区域边界防火墙二 | 网络层吞吐量≥12G，应用层吞吐量≥2.5G，6个千兆电口，4个千兆光口插槽。含入侵检防御模块及防病毒模块。包含三年升级及维保。 | 2 |
| 5 | 网络准入控制系统 | 安全认证、终端合规、高级防护联动、资产管理；产品模块：有线网络认证、终端检测、网络准入控制；硬件形态：1U，包含三年升级及维保。 | 1 |  |
| 6 | WAF防火墙 | 2U机箱；4个千兆电口（支持两组电口Bypass），4个千兆光口，1个HA口,1个管理口；2个可插拨扩展槽；双电源；含3年特征库升级服务，并发连接≥120万；网络层吞吐率≥5Gbps，应用层吞吐率≥1Gbps，包含三年升级及维保。 | 2 |  |
| 7 | 上网行为管理 | 网络吞吐量≥2Gb，带宽性能≥1Gb，支持用户数≥6000，每秒新建连接数≥14000，最大并发连接数≥600000；硬件参数：规格：1U，内存大小≥8G，硬盘容量≥1T SATA，电源：单电源，接口≥6千兆电口+2万兆光口SFP+。包含三年升级及维保。 | 1 |  |
| 8 | 网络安全审计系统 | 1U设备，6电2光，审计处理能力≥600Mbps，包含三年升级及维保。 | 1 |  |
| 9 | 数据库审计 | 2U机架式结构，包含6电口（含管理口），4个SFP插槽；≥2T存储空间；审计处理能力≥1.2Gbps，峰值SQL处理能力≥8000条/秒。包含三年升级及维保。 | 1 |  |
| 10 | 堡垒机 | 含≥150个授权许可，6个千兆电口；≥8TB硬盘；最大支持150路图形会话或400路字符会话并发，包含三年升级及维保。 | 1 |  |
| 11 | 日志审计系统（安全设备日志） | 含≥150个授权许可，配备≥8T的硬盘，6个千兆电口，接口可扩展；支持获取各种主流网络及数据库访问行为，支持Syslog、WMI、OPSEC Lea、SNMP trap和LAS-1000专用协议等协议事件日志，包含三年升级及维保。 | 1 |  |
| 12 | 漏洞扫描系统 | 支持并发≥50台设备的扫描授权许可； 含配置核查、漏洞扫描、配置变更检查三大引擎。功能包括：任务管理、检测报告、结果对比，告警分析、综合报表、综合仪表板等；包含三年升级及维保。 | 1 |  |
| 13 | 态势感知区级平台 | 支持基于规则引擎对告警接收、过滤、压缩、归并、升级的事件处理流程，并具备基于AI算法的动态阈值与故障根源定位能力；提供可视化运行态势感知；支持与流程、自动化联动，实现故障派发工单、故障自愈等联动处置能力，实现故障处理的标准化与规范化。包含三年升级及维保 | 1 | 数据可视化平台 |
| 14 | 数据备份系统 | 备份容量大于等于16TB。支持文件，数据库，操作系统，虚拟机备份。支持windows,linux操作系统。支持重复数据删除功能。具备得2分，不具备不得分。包含三年升级及维保。 | 1 |  |
| 15 | 高级威胁防护 | ≥50+文件类型检测，全面识别未知恶意软件；秒级联动响应，快速拦截未知恶意软件；提供详细威胁报告，帮助运维、快速决策：详细展示文件检测结果，包括文件检测结果、文件相关会话信息、文件格式异常、文件行为异常、网络通讯异常、虚拟执行环境信息、网络行为和主机行为等。具备得2分，不具备不得分。包含三年升级及维保。 | 1 |  |
| 16 | 数据库防火墙 | 精准拦截，可基于IP地址、时间、操作、关键字、数据库账号等；应用协议识别控制，可自动识别DBA协议、运维协议；防APT攻击，根据访问行为的组合、统计模型迅速验证并阻断复杂的违规操作及恶意行为；支持旁路部署阻断模式，避免串联部署存在单点故障。包含三年升级及维保。 | 1 |  |
| 17 | 安管区域汇聚交换区 | 交换容量≥730G，包转发≥220Mpps,固化24千兆电口，4个万兆光口，一个扩展插槽，配置冗余电源和风扇，支持安全扩展板卡；包含三年升级及维保。 | 2 |  |
| 18 | 流量复制器 | 交换容量≥256Gbps，转发性能≥155Mpps，配置2个模块化电源，2个模块化风扇，主机固化≥24个千兆电口，≥4个万兆光口，支持M:N复制，包含三年升级及维保。 | 1 |  |
| **11个社区卫生服务中心安全加固** | | | | |
| 19 | 社区卫生中心出口防火墙 | 网络层吞吐量≥8G，应用层吞吐量≥2G，16个千兆电口，8个千兆光口,2个万兆光口；包含传统防火墙+IPS模块功能+防病毒模块，包含三年升级及维保 | 22 | 下一代防火墙 |
| 20 | 社区卫生中心服务器区边界防火墙一 | 网络层吞吐量≥10Gbps，应用层吞吐量≥3Gbps，包含传统防火墙+IPS模块功能+防病毒模块，包含三年升级及维保 | 11 | 核心交换机防火墙模块 |
| 21 | 社区卫生中心服务器区边界防火墙二 | 网络层吞吐量≥10Gbps，应用层吞吐量≥3Gbps，包含传统防火墙+IPS模块功能+防病毒模块，包含三年升级及维保 | 11 | 核心交换机IPS模块 |
| 22 | 社区服务器汇聚交换机 | 交换容量≥730G，包转发≥220Mpps,固化24千兆电口，4个万兆光口，一个扩展插槽，配置冗余电源和风扇，支持安全扩展板卡；包含三年升级及维保 | 22 |  |
| 23 | 态势感知社区子平台 | 将业务应用、平台资源、虚拟资源、物理资源等基础设施通过采集、计算、调度、控制、运营等技术手段进行数据可视化展现。包含三年升级及维保 | 11 | 数据可视化子平台 |
| 24 | 安全数据可视化及运维管理平台 | 支持云监控模式，服务监控；支持日志监控分析，集中存储管理、日志关联分析、日志数据可视、指标多维仪表展现；支持网络管理，网络发现与管理、完善的链路质量与性能监控、灵活的指标定义与事件预警。包含三年升级及维保 | 11 | 监测管理模块 |
| 25 | 支持运维自动化、岗责细化授权、开放接口；支持自定义安装计划、灵活的操作系统配置，简化配置过程。 | 11 | 自动化管理模块 |
| 26 | ITSM服务流程管理，兼容DevOps/ITIL理念、支持人工/自动节点混排；支持即时运维协同 ，基于职责和场景灵活建立群组、运维协同和任务执行可回溯审计。 | 11 | 流程协同模块 |
| 27 | 安管监控中心大屏系统 | 65寸电视机4台及相关投屏设备和工程用以安全管理中心监控安全数据可视化及运维管理平台软件内容监看和展示 | 1 |  |
| 28 | 等保一体机 | 内存≥48G，硬盘≥128G SSD 系统盘≥8T HDD 数据盘，网口： 1个管理电口、4个千兆电口、4个千兆光口，2U，双电源。包含三年升级及维保 | 11 | 安全管理主机 |
| 29 | 扩充存储空间许可，并将可用存储空间扩展至4TB | 11 | 日志审计模块（存储扩容） |
| 30 | 系统软件，应用层吞吐量≥200M，日志检索≥15000条/s | 11 | 数据库审计模块 |
| 31 | 提供≥50个资源授权，提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求 | 11 | 堡垒机模块 |
| 32 | 支持并发≥50台设备的扫描； 含配置核查、漏洞扫描、配置变更检查三大引擎。功能包括：任务管理、检测报告、结果对比，告警分析、综合报表、综合仪表板等；包含三年漏洞升级服务 | 11 | 漏洞扫描模块 |
| 33 | **驻场运维服务** | |  |  |
| 34 | 针对本项目提供2名或以上工程师驻场运维服务，从项目验收之后一年整。 | | 1 |  |

## 区卫健委中心端主要设备技术参数要求

### 出口边界防火墙一

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 兼容性 | 与安管区域汇聚交换机同品牌 |
| 硬件架构 | 采用非X86多核架构，配置冗余电源（多核架构需提供证明材料） |
| 接口及性能要求 | 主机至少需要固化千兆电口≥16，千兆光口≥8，万兆光口≥2，  在此基础上仍能进行万兆光口扩展，可扩展万兆光口数≥8  网络层吞吐量≥10G，应用层吞吐量≥2.5G，并发连接数≥1000万，每秒新建连接数≥15万/秒 |
| 安全应用 | 整机同时具备防火墙、链路负载均衡、IPS、防病毒、Web应用、应用识别等功能，实配3年防病毒，3年IPS授权 |
| 部署模式 | 实现路由模式、透明（网桥）模式、混合模式。 |
| 路由实现 | 实现静态路由、策略路由、RIP、OSPF、BGP等路由协议。 |
| NAT功能 | 实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 |
| VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 |
| 支持IPsec VPN隧道自动建立，无需流量触发； |
| 支持IPsec VPN智能选路，根据应用和隧道质量调度流量。 |
| 可基于每个SSL VPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。 |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 |
| 安全策略 | 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置 |
| 支持策略冗余分析， 冲突策略分析以及命中率统计。 |
| 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图） |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。（提供截图） |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。 |
| 加密流量检测 | 支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供截图） |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能。 |
| 支持IPV6下的访问控制、IPSec VPN、DDoS防护等安全功能。 |
| 国密算法 | 支持国密SM2/3/4算法。（提供功能截图） |
| 虚拟化能力 | 所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。 |
|
| 支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。 |
| 设备管理 | 支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。 |
| 为了保证整个网络的可靠稳定，要求本次采购的安全设备支持A/S，A/A方式部署，支持配置同步，会话同步和用户状态同步； |
| 提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |

### 出口边界防火墙二

|  |  |
| --- | --- |
| 指标 | 指标参数 |
| 硬件性能要求 | 多核AMP+架构，网络层吞吐量≥12G，应用层吞吐量≥2.5G，并发连接≥280万，每秒新建连接数≥20万， 2U机箱，单电源，配置至少6个10/100/1000M自适应电口，4个SFP插槽，支持2个扩展槽，1个Console口，支持液晶屏，实配含3年硬件维保服务，3年入侵防御模块，3年防病毒模块。 |
| 功能要求 | 所投产品必须支持手工指定、802.3ad协议等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份 |
| 所投产品必须支持MTU≥9012byte的巨型帧通过设备传输时不分段 |
| 所投产品必须支持不少于8条链路的ISP路由负载均衡，支持自定义链路负载权重，支持基于优先级的ISP路由链路备份；支持不少于4种的链路状态探测机制，实现失效链路快速切换 |
| 所投产品支持将特定用户、应用、URL分类标记为重点关注。支持单独呈现重点关注对象的流量、访问次数等统计信息。并可基于用户/IP地址、应用、URL分类执行筛选、关联式分析，快速挖掘异常用户及异常网络行为。 |
| 联动处置 | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万；支持与云端大数据中心联动； |
| ▲所投产品须实现基于终端健康状态的访问控制；并支持阻断终端网络活动的同时，提示被阻断原因及重定向至自定义网址。（投标文件需要提供能够体现上述功能及配置选项的截图等证明材料）； |

### 区域边界防火墙一

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 兼容性 | 与安管区域汇聚交换机同品牌 |
| 硬件架构 | 采用非X86多核架构，配置冗余电源（多核架构需提供证明材料） |
| 接口及性能要求 | 主机至少需要固化千兆电口≥16，千兆光口≥8，万兆光口≥2，  在此基础上仍能进行万兆光口扩展，可扩展万兆光口数≥8  网络层吞吐量≥10G，应用层吞吐量≥2.5G，并发连接数≥1000万，每秒新建连接数≥15万/秒 |
| 安全应用 | 整机同时具备防火墙、链路负载均衡、IPS、防病毒、Web应用、应用识别等功能，实配3年防病毒，3年IPS授权 |
| 部署模式 | 实现路由模式、透明（网桥）模式、混合模式。 |
| 路由实现 | 实现静态路由、策略路由、RIP、OSPF、BGP等路由协议。 |
| NAT功能 | 实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 |
| VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 |
| 支持IPsec VPN隧道自动建立，无需流量触发； |
| 支持IPsec VPN智能选路，根据应用和隧道质量调度流量。 |
| 可基于每个SSL VPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。 |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 |
| 安全策略 | 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置 |
| 支持策略冗余分析， 冲突策略分析以及命中率统计。 |
| 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图） |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。（提供截图） |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。 |
| 加密流量检测 | 支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供截图） |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能。 |
| 支持IPV6下的访问控制、IPSec VPN、DDoS防护等安全功能。 |
| 国密算法 | 支持国密SM2/3/4算法。（提供功能截图） |
| 虚拟化能力 | 所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。 |
|
| 支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。 |
| 设备管理 | 支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。 |
| 为了保证整个网络的可靠稳定，要求本次采购的安全设备支持A/S，A/A方式部署，支持配置同步，会话同步和用户状态同步； |
| 提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |

### 区域边界防火墙二

|  |  |
| --- | --- |
| 指标 | 指标参数 |
| 硬件性能要求 | 多核AMP+架构，网络层吞吐量≥12G，应用层吞吐量≥2.5G，并发连接≥280万，每秒新建连接数≥20万， 2U机箱，单电源，配置至少6个10/100/1000M自适应电口，4个SFP插槽，支持2个扩展槽，1个Console口，支持液晶屏，实配含3年硬件维保服务，3年入侵防御模块，3年防病毒模块。 |
| 功能要求 | 所投产品必须支持手工指定、802.3ad协议等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份 |
| 所投产品必须支持MTU≥9012byte的巨型帧通过设备传输时不分段 |
| 所投产品必须支持不少于8条链路的ISP路由负载均衡，支持自定义链路负载权重，支持基于优先级的ISP路由链路备份；支持不少于4种的链路状态探测机制，实现失效链路快速切换 |
| 所投产品支持将特定用户、应用、URL分类标记为重点关注。支持单独呈现重点关注对象的流量、访问次数等统计信息。并可基于用户/IP地址、应用、URL分类执行筛选、关联式分析，快速挖掘异常用户及异常网络行为。 |
| 联动处置 | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万；支持与云端大数据中心联动； |
| 所投产品必须支持与青浦区卫健委及下属社区卫生服务中心的杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断终端网络活动的同时，提示被阻断原因及重定向至自定义网址。（投标文件需要提供能够体现上述功能及配置选项的截图等证明材料）； |

### 网络准入控制系统

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 详细要求 |
| 基本要求 | 硬件要求 | 1U机架式结构；千兆电口数量不低于6个；千兆光口（SFP插槽）数量不低于2个；设备要求具有灵活的接口扩展能力，电口具有一组BYPASS接口，不低于2个扩展槽位， |
| 性能要求 | 不低于300个同时在线用户 |
| 许可要求 | 要求配置不低于300个同时在线用户许可 |
| 部署方式 | 系统部署简单，支持旁路或串联部署，支持命令行与B/S模式管理，提供系统首页图形化展示功能，可展示设备面板状态、CPU状态、内存状态、硬盘状态、在线用户、报警统计等信息。 |
| 可靠性 | 设备提供硬件BYPASS功能，支持双操作系统冷备、双机热备，在单机模式下，提供独立系统逃生工具。（需提供相关功能截图） |
| 客户端兼容 | ▲支持802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用。（需提供相关功能截图） |
| 支持802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用。 |

### WAF防火墙

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 规格要求 |
| 设备基本要求 | 专用的硬件和软件保障 | 采用专用硬件架构与专用安全操作系统，基于操作系统内核的完全检测技术；硬件设备可以机架安装，产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能。 |
| 硬件模块化设计 | 硬件采用模块化设计，可以通过扩展卡来增减业务接口，而非软件WAF。 |
| 端口数量和扩展能力 | 2U机箱；4个千兆电口（支持两组电口Bypass），4个千兆光口，1个HA口,1个管理口；2个可插拨扩展槽；双电源；含3年特征库升级服务，并发连接120万；含3年硬件维保。 |
| 电源 | 双电源 |
| MTBF | 不少于450000小时 |
| 性能要求 | 网络层吞吐率 | ≥5Gbps |
| 应用层吞吐率 | ≥1Gbps |
| 并发连接数 | ≥130万 |
| 网络部署 | 部署方式 | 无IP纯透明模式串联部署、旁路监测模式部署、负载均衡模式部署、反向代理模式部署 |
| 串联部署时服务器可以看到真实客户端源IP，而不是WAF的业务IP地址 |
| 网络适应性 | 支持VLAN划分，支持多VLAN环境下trunk的部署 |
| 支持虚拟线无论任何网络环境可强制数据从一个接口转发到另一个接口 |
| 支持网络层防火墙功能，支持源IP、源区域、目的IP、目的区域等条件的访问控制 |
| 攻击防护 | HTTPS支持 | 支持HTTP/HTTPS站点防护 |
| 协议合规检查 | 支持请求限制配置通过定义最大请求头长度、最大content-length、最大body长度、最大请求行长度、最大header行长度、最多cookies个数、最多header头个数、最大header长度等来对请用户数据做合规性检查 |
| WEB安全防护 | 支持900+条以上的应用层规则（提供截图证明） |
| 应能识别和阻断SQL注入攻击,Cookie 注入攻击，命令注入攻击（提供截图证明） |
| 应能识别和阻断跨站脚本(XSS)攻击 |
| 可对文件上传做控制，包括最多上传文件数、最大文件上传大小、可以通过对上传文件的扩展名、MIME类型及允许请求体编码类型等做上传控制 |
| 可对文件做下载控制，包括最大下载文件大小、禁止下载文件的扩展名、MIME类型等 |
| 检测功能 | 检测到攻击后支持阻断、只检测等动作且动作为阻断时用户可自定义阻断页面 |
| https证书支持直接将证书内容填充到waf内使用，不用再上传或者转换证书使用 |
| 网页防篡改 | 网关型网页防篡改，无需在服务器中安装任何插件，可以对动态网  站及静态网站文件内容进行防篡改，当检测到篡改后可以实时恢复篡改内容 |
| WEB漏洞扫描 | 支持多种WEB应用漏洞的安全扫描检测，如SQL注入、跨站脚本、目录遍历等 |
| 支持自定义WEB漏洞扫描任务，支持对需要认证登录的web系统进行漏洞扫描，支持自定义每日、每周、每月等扫描周期设置 |
| 可导出web漏洞扫描报告，报告支持pdf,html,txt,xml等格式导出 |
| 负载均衡 | 支持多服务器的负载均衡，支持轮叫、加权轮叫、原地址散列、最小连接等多种负载均衡算法 |
| 能配合现有的负载均衡设备协同工作，支持任意部署，而不影响客户现有拓扑 |
| 数据分析 | 网络数据分析 | Web界面可以直观查看WAF扩展卡、接口、USB口、管理口、HA口及业务口的运行状态 |
| 可以查看使用业务接口的上下行实时流量 |
| 可以查看通过WAF的所有IPV4及IPV6客户端和服务器IP地址及端口连接数及状态 |
| 可以实时查看设备并发连接数、每秒事务数及HTTP应用层吞吐率等数据并以可视化的方式展示 |
| 设备运行数据分析 | 可以实时查看设备CPU、内存、硬盘等自身使用率情况 |
| 日志报表数据分析 | 日志支持以syslog和welf两种格式向远端日志服务器发送日志 |
| 日志传输可加密，且管理员可以配置加密密码（提供截图证明） |
| 支持系统日志、管理员登录日志、调试日志的记录 |

### 上网行为管理系统

|  |  |  |
| --- | --- | --- |
| 项目指标 | | 具体功能要求 |
| 性能参数 | | 网络吞吐量≥2Gb，带宽性能≥1Gb，支持用户数≥6000，每秒新建连接数≥14000，最大并发连接数≥600000；硬件参数：规格：1U，内存大小≥8G，硬盘容量≥1T SATA，电源：单电源，接口≥6千兆电口+2万兆光口SFP+ |
| 部署方式 | 多种部署模式 | 支持网关、网桥、旁路模式部署；网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能 |
| 全面支持IPv6 | 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置；所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6； |
| 实时网络状态 | web访问质量监测 | ▲上网质量稳定是医院办公的基础性要求，要求所投产品的功能支持：针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向web访问质量检测。（提供产品界面截图） |
| 首页可视化分析展示 | 支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况； |
| 应用管理 | 应用标签功能分类管理 | 支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类； |
| 应用识别规则库 | 设备内置应用识别规则库，支持超过6000条应用规则数，支持超过2800种以上的应用，1000种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； |
| 应用细分控制 | 1.能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件等。  2.能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制；  3.能够对Github、百度网盘、百度文库等网络应用的上传动作进行细分控制；（所有功能必须提供产品界面截图） |
| 邮件管理 | SSL邮件管理 | 必须能基于关键字、发件人地址等识别和过滤使用邮件客户端外发SSL加密邮件的行为； |
| 加密SMTP、POP3邮件审计 | 支持对加密HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP邮件内容的审计。 |
| 网页管理 | SSL加密网页内容识别 | 识别并过滤SSL加密的钓鱼网站、非法网站等（提供自主知识产权证明）；支持SSL硬件加速卡解密，从而可提高SSL全流量解密性能； |

### 网络安全审计系统

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 详细要求 |
| 硬件配置 | 接口 | 1U机箱，至少6个千兆电口，2个SFP插槽，2个可插拔扩展槽位，至少1T存储空间，吞吐率：≥600Mbps。 |
| 基本要求 | 网络协议内容审计 | 支持实名审计，支持802.1x,PPPoE,AD等环境下终端IP地址和用户实名信息或主机信息绑定显示，可显示在线用户的PPPoE账号和AD域用户等信息。 |
| 支持SMTP、POP3、IMAP的邮件审计功能，可对邮件客户端收发邮件的行为进行审计，审计内容包括但不限于：发件人、收件人、抄送人、邮件主题和附件，并可以对邮件进行还原，还原可看到邮件正文及附件内容。 |
| IPv6环境 | 支持IPV6环境部署和IPV6环境下网络审计系统全部功能的审计。 |
| 功能要求 | 网络协议内容审计 | 支持实名审计，支持802.1x,PPPoE,AD等环境下终端IP地址和用户实名信息或主机信息绑定显示，可显示在线用户的PPPoE账号和AD域用户等信息。 |
| 支持对即时通讯的审计，可对使用即时消息通讯协议的网络行为审计。 |
| 支持共享协议（SMB文件共享、NFS共享）审计。 |
| 支持对网络入侵行为IPS规则的管理和侦听，并对攻击信息详细审计（攻击流行程度、风险等级、操作系统、攻击类型等）。 |
| 网络协议行为审计 | 支持330种以上国内常见应用协议行为的自动识别与审计记录。 |
| 审计规则 | 支持审计规则的优先级的调整，以防止误报、漏报等发生。 |
| 支持审计策略的自定义，可将时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件进行策略设置。 |
| 支持数据采集规则定义，对于不关心的数据可以不采集，有效保证系统审计的稳定性与针对性。 |
| 系统内置高危SQL查询和注入、远程命令执行、跨站脚本攻击等高危指令告警规则。 |
| 支持以字段名称和字段值作为分项响应条件进行审计策略设置（非正则表达式方式）。 |
| 流量分析 | 支持流量趋势分析、IP分组流量统计，可以对传输协议、应用协议、应用协议组、源目的地址、源目的端口进行统计分析，可以多条件组合分析。 |
| 支持基于流的流量分析功能，可对其他设备发送的Netflow进行分析，支持对Netflow v5/v9版本的流量分析。 |
| 功能要求 | 统计报表 | 支持WORD、PDF、CVS、EXCEL、HTML等格式导出报表。 |
| 支持邮件方式自动发送报表。 |
| 支持系统报警的自定义查询功能，可自定义查询系统内所有报警事件内容，包括：事件主体、事件客体、报警内容、报警级别、报警触发规则名称等。 |
| 功能要求 | 系统安全 | 提供管理员权限设置和分权管理，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 |
| 提供审计数据管理功能，可根据时间或磁盘空间状况实现对审计数据的自动备份、删除。 |
| 日志外发及日志数据安全 | 支持Syslog、SNMP Trap方式向外发送审计日志。 |
| 支持以SNMP方式，将系统运行状态提供给第三方网管系统。 |
| 支持NTP时间同步。 |

### 数据库审计

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 详细要求 |
| 硬件接口 | 接口 | 至少1个10/100/1000BASE-TX管理口，5个10/100/1000BASE-T电口采集口，4个SFP插槽,2个USB，个Console接口，2个可插拔扩展插槽，至少2T存储空间。 |
| 尺寸 | 2U |
| 电源 | 冗余双电源 |
| 授权 | ≥70个数据库实例授权，≥8个监听口授权 |
| 审计能力 | 审计处理能力≥1.2Gbps,峰值SQL处理能力≥8000条/秒，日志存储能力≥40亿条. |
| 基本要求 | 数据库类型 | 支持、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata、等数据库系统 |
| 审计查询 | 支持按数据库实例、数据库名、用户名、数据库表名、表字段名、操作类别、SQL语句、响应时间、连接时长、会话ID、关联规则ID、操作结果、SQL返回结果集、数据库客户端程序、数据库服务器端程序等作为查询和统计条件 |
| 审计能力 | 数据库类型 | 支持、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统 |
| 数据库监控展示 | 支持数据库名、实例名、数据库类型、数据库服务器负载、活跃会话数以及CPU、硬盘、内存等信息的展示（提供证明截图） |
| SQL操作统计 | 支持各类SQL操作数量以及占比情况 |
| 实名审计 | 支持以姓名、部门、域名、源IP、源MAC、邮箱、电话、数据来源等要素为条件的实名审计 |
| 会话回放 | 支持会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节 |
| 弱口令扫描 | 支持数据库服务器弱口令扫描，扫描出的密码需脱敏显示 |
| 基线管理 | 支持基于SQL操作进行基线构建和基线管理 |
| 业务关联审计 | 支持插件方式和非插件方式的业务关联审计，实现100%精准审计与灵活部署配置 |
| 系统管理 | 版本回滚 | 支持历史版本回退功能，系统内建历史版本库不少于3个 |
| 操作系统 | 安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统 |
| IPv6环境 | 支持IPv6网络环境下的数据库审计，可识别IPv6的相关主体与客体资源 |
| 云检测 | 支持云检测，可对本单位部署的同一品牌的多台审计或者多类型安全设备（版本号、序列号、型号、运行时长、CPU和内存占用、并发和新建连接数、设备流量等）进行远程统一检测，保障各设备的安全稳定运行（提供证明截图） |
| 系统抓包 | 支持抓包工具（可配置抓包个数、源和目的IP、协议等）、系统巡检、网络诊断、规则库升级（提供证明截图） |
| 一键巡检 | 支持系统本身主要运行功能服务模块的运行状态巡检，保证系统安全稳定运行 |
| 系统部署 | 支持单点旁路、多点多级部署 |
| 高可靠性 | 支持双机热备 |
| 报表格式 | 支持WORD、PDF、CVS、XLS、HTML等格式导出报表，并可通过邮件自动发给相关人员 |

### 堡垒机

|  |  |
| --- | --- |
| 指标 | 指标要求 |
| 性能指标 | 标准1U机架式，6个千兆电口,支持2个接口扩展槽位，内置至少8TB硬盘，单电源，支持液晶屏，支持150路图形会话或400路字符会话并发；含≥150个授权许可，含三年标准售后服务 |
| 资源管理 | 支持SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、、SQL Server、Rlogin等协议  支持Linux/Unix、Windows、H3C、Huawei、Cisco等系统 |
| 支持图形、字符，混合协议下的批量登录 |
| 支持IPv4、IPv6双栈网络运维审计支持 |
| 支持以云盘形式在堡垒机上存储文件，并自定义云盘大小，实现操作端、堡垒机、目标服务器三者之间文件共享 |
| 访问控制 | 支持按用户、账户组设置多对多的资源访问授权，用户组和账户组内的新增成员自动继承授权关系 |
| 预制Linux主机和网络设备的基本命令，支持正则表达式和通配符方式设置匹配规则，自定义命令黑白名单 |
| 支持对MySQL和数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制 |
| 自动运维 | 支持从Linux服务器推拉账户，实现堡垒机与纳管的资源服务器之间的账户同步 |
| 支持自动修改服务器资源帐号的密码，并且将改密后的密码分为A、B两段，发送到指定的两个人的邮箱，必须凑齐两部分密码才可以查看完整服务器密码。 |
| 支持混合协议（RDP/SSH/TELNET）批量运维 |
| 支持自定义运维任务，实现命令执行、脚本运行、文件批量分发自定义灵活组成自动化运维任务。 |
| 工单管理 | 支持通过工单申请资源，权限包括文件上传下载、RDP剪切板，流程可按多人多级审批模式或会签审批模式 |
| 支持对工单列表中的工单进行克隆，实现快速提交 |
| 支持通过工单形式对高危命令操作实现动态审批授权 |
| 操作记录 | 支持用户水印功能，避免数据泄露无法追责 |
| 支持对运维操作中的详细操作命令、步骤、以及双人授权、协同用户、剪切板拷贝行为进行记录，并可以通过关键字搜索定位回放，审计日志内容支持导出 |
| 系统内置多种运维、系统报表模板，支持按日、周、月为周期，自动生成Word、HTML、Excel和PDF格式报表 |
| 支持数据库命令级审计，数据库支持类型包括：DB2、MySQL、、SQL Server等 |
| 支持以图形、字符方式双重审计，完整详细还原操作记录 |

### 日志审计系统

|  |  |
| --- | --- |
| 指标 | 指标要求 |
| 性能指标 | 事件处理最高≥3000EPS。硬件规格：标准1U机箱，至少6个千兆电口，2个扩展插槽，1个Console接口，单电源，至少8T硬盘。含≥150个授权许可，包含三年标准维保。 |
| 管理范围 | 能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 审计对象 | 支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；  支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；  支持审计各种主机操作系统（包括Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400）配置日志、运行日志、告警日志等；  支持审计各种数据库（、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；  支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic等）配置日志、运行日志、告警日志等；  支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；  以及用户自己的业务系统的日志、事件、告警等安全信息. |
| 日志采集与转发 | 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能； |
| 支持按照Syslog-NG标准及自有格式进行转发，转发时包含原始日志源IP地址； |
| 日志交互式分析 | 系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件。系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件； |
| 用户可自定义事件搜索查询条件，并可保存为策略，以树形结构进行组织，形成一个搜索分析策略树；每个查询场景都可以查询策略的形式进行存储。 |
| 日志统计分析 | 可自定义统计场景，统计的字段条件和时间段以及过滤器等可自由设定； |
| 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D地球等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表等。图表数据支持数据下钻。 |
| 支持将统计结果保存为仪表板、报表和策略 |
| 日志综合展示 | 系统提供可编辑的灵活强大的自定义仪表板； |
| 系统内置仪表板至少包括日志源事件分析仪表板，Windows事件分析仪表板，网络设备分析仪表板，防火墙事件总览分析仪表板，WEB事件总览分析仪表板，FTP服务器日志分析等； |
| 仪表板支持自定义创建框架，用户根据需要在框架内添加不同的仪表板组件（数值、折线、面积、柱图、饼图、环状图、地图、组件、URL、文本、图片、列表等），支持组件位置自由摆放，组件大小自由拖曳等。 |
| 备份归档 | 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；  当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；  支持以FTP/SFTP方式将日志数据备份至外部存储空间，支持数据恢复 |
| 级联管理 | 提供标准的系统级联，支持对下级系统的注册与注销，可对下级系统的IP地址、系统信息、运行状态和性能进行集中监测。  上级指定下级系统进行告警和安全事件数据上报，上级系统可向下级系统下发通知与策略。 |
| 知识库 | 系统内置安全知识库，包括事件库、案例库、应急预案库、日志采集配置库和端口库等，支持自定义增加安全知识内容。  系统支持IP地理位置知识库并支持导入升级。 |
| 二次开发接口 | 系统提供二次开发接口，接口形式为Restful API，提供资产、事件、告警、报表等数据的统计、详情等接口；  支持用户认证接口，提供接口在线文档说明供开发人员使用。 |

### 漏洞扫描系统

|  |  |
| --- | --- |
| 指标 | 指标要求 |
| 性能指标 | Web扫描域名无限制，Web扫描任务并发数不少于5个域名。系统扫描IP地址支持不少于1024个，支持扫描A类、B类、C类地址，系统扫描支持50个IP地址并行扫描。标准1U机架式，1T硬盘，标准配置6个10/100/1000M自适应电口，2个扩展插槽,2个USB口，1个Console口，单电源。包含3年漏洞特征库升级，3年硬件维修服务。（同时支持50个授权并行扫描） |
| 系统扫描 | 产品应具备操作系统、数据库、网络设备等主流系统的漏洞库列表，并提供至少20种以上的漏洞库分类 |
| 产品漏洞库列表数量必须大于60000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准兼容 |
| 产品具备对主流的数据库软件的漏洞检查，支持、MySQL、SQL server、DB2等数据库的安全漏洞检查，并提供至少600种相关漏洞库 |
| 产品具备对主流虚拟机管理系统的漏洞检查，支持Vmware ESX\Vmware ESXi等相关漏洞 |
| 产品具备对DNS服务的安全漏洞检查，包括DNS缓存中毒、DNS拒绝服务漏洞、签名欺骗等至少100种以上的相关漏洞库 |
| 产品具备对iOS、Android、Blackberry、windowsphone等操作系统，并提供至少50种以上的相关漏洞库 |
| 产品具备对后门检测的安全漏洞检查，包括对Microsoft IIS、特洛伊木马检测、Mac OS X恶意程序等常见后门漏洞的安全检测，并提供至少100种以上的相关漏洞库 |
| 产品具备对常见P2P软件的安全漏洞检测，包含对常见的电驴、iTunes、BitTorrent等软件的安全检测，并提供至少50种以上的相关漏洞库 |
| WEB安全 | 产品具备基于OWASP组织发布的TOP 10攻击类型进行Web漏洞分类 |
| 产品具备对网页暗链、敏感词汇、网站木马的检测 |
| 产品具备对网站目录进行扫描识别，并用树形结构展示网站架构 |
| 产品需支持对Web网站漏洞扫描的同时，查看网站漏洞情况和Web目录结构，数据进行实时同步呈现 |
| 产品具备对扫描爬虫、扫描页面数、页面大小、例外URL、例外文件类型进行自定义检测设置 |
| 产品具备对网站的广度或深度进行检测设置 |
| 数据分析 | 产品具备漏洞在线查询功能，可以根据漏洞严重级别进行区别展示，并以颜色对漏洞级别进行区分 |
| 产品具备对检测任务、资产等类型进行漏洞情况查询 |
| 产品具备以漏洞为中心为查询对象，查询存在漏洞的相关资产，并可以查询深入的详细漏洞明细 |
| 产品具备漏洞变化趋势图，查询多次漏洞扫描情况的趋势情况，了解阶段性的漏洞安全问题 |

### 数据备份系统

|  |  |  |
| --- | --- | --- |
| 主指标项 | 子指标项 | 指标参数要求 |
| 硬件平台 | 备份一体机 | 机架式2U专用备份存储一体化设备；配置≧8个硬盘盘位；1颗BRONZE-3104\_XEON系列6核处理器，CPU可扩展；双电源冗余；配置≧16GB内存 支持可扩展≧512GB;支持缓存掉电保护；配置≧16TB (3.5寸SATA)企业级裸磁盘空间；支持RAID 0，1，5，50，6，60多种模式；配置≧2个千兆以太网接口，可扩展为万兆以太网接口；硬件三年原厂质保。（实配≧20TB的备份授权和存储空间） |
| 备份功能与要求 | 数据库定时备份 | 支持单机、 RAC、HA等架构的定时数据备份，支持Windows 2008/2012及以上版本,Centos6及以上版本、RHEL 6及以上版本、OEL 6及以上版本、SLES11及以上版本。支持10、11、12、18、19等版本。  支持通过数据库日志的方式进行数据保护，实现分钟级数据保护的。  ▲支持备份时不产生任何的缓存数据，不占用生产端空间。(要求提供软件功能截图并加盖原厂公章) |
| 整机定时备份 | 支持将Windows、Linux服务器整体环境（含操作系统、应用程序、应用配置、业务数据、逻辑磁盘等）备份成虚拟机映像，支持物理机、主机平台虚拟机、的定时整机备份。(要求提供软件功能截图并加盖原厂公章)  支持Windows 2008/2012及以上版本,Centos6及以上版本、RHEL 6及以上版本、OEL 6及以上版本、SLES11及以上版本。  支持恢复到原主机或手动恢复到指定主机；  支持V2V和V2P，将整机备份出来的虚拟机映像恢复到其他虚拟化平台或物理机上，满足不同的恢复需求。  支持分区备份和分区恢复，无论备份采用的是磁盘备份还是分区备份，恢复时都同时支持磁盘恢复和分区恢复。并且备份和恢复的空间都是和实际备份、恢复的有效数据大小保持一致，不和磁盘大小保持一致。  支持整机的文件恢复，仅恢复整机中的选定文件，提高恢复效率。  安装或卸载整机定时备份过程中，不重新启动或中断生产服务器，不影响生产业务。 |

### 高级威胁防护

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 详细要求 |
| 硬件配置 | 接口 | 至少4个SFP插槽和6个千兆电口，1个管理口。1个HA口，单电源， 系统盘250GB，存储盘2TB，综合监测吞吐600Mbps。 |
| 尺寸 | 1U |
| 电源 | 双电源 |
| 基本要求 | 硬件设备数量 | 必须为软硬一体化2U标准机架式设备，不能分为二台或多台设备来完成APT功能 |
| 功能要求 | 文件检测 | 支持从HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS、HTTP Proxy协议中还原出指定格式文件 |
| 文件静态检测支持检测包括邮件文件（EML）、Office、压缩包、脚本文件、图片文件、APK等60余种默认文件格式。（提供功能截图） |
| 支持对所有已检测过的文件HASH进行统一存储，并提供搜索、查看、重新检测功能（提供功能截图） |
| 沙箱支持文件行为监测、注册表、进程、模块、进程调用API情况、进程对窗口、进程的异常处理、网络行为、样本衍生物进行分析检测。沙箱支持文件伪装识别。能够识别出伪装成图片以及其它正常文件的恶意代码文件。 |
| 沙箱检测报告具有检测信息概要功能，概要内容包含：文件名、威胁级别、文件HASH检测结果、内容分析结果、行为分析结果、CVE信息、机器学习检测结果等重点信息的展示。（需提供相关功能截图） |
| 失陷主机检测 | 支持信誉检测机制，通过C&C信誉库（黑IP、黑URL、黑域名）来检测木马（如：ZeuS、Feodo等）、僵尸、蠕虫等恶意代码的活动行为 |
| 支持通信流量特征检测，基于流量中的通信特征，来检测木马、僵尸、蠕虫等恶意代码的主机上线、文件操作、屏幕监控等活动行为。 |
| 远程漏洞攻击检测 | 支持远程溢出漏洞检测，基于流量特征来检测远程漏洞扫描及利用的攻击行为，并将攻击事件会话PCAP文件记录、存储和PCAP文件在线查看功能 |
| Web攻击检测 | 支持Web攻击检测，能够检测Web漏洞扫描及利用行为 |
| 支持Webshell控制检测，能够检测Webshell控制行为 |
| 支持Web攻击事件会话PCAP文件记录、存储和PCAP文件在线查看功能 |
| 可视化关联分析 | 支持时间序列关联分析，以内网资产(必选)或者指定的外部IP地址作为基础，以时间、检测事件作为条件呈现当前资产或者IP的威胁态势情况。 |
| 资产威胁统计 | 支持以资产维度，展示资产的威胁信息，可展示资产的威胁统计、威胁分布、威胁排名。 |

### 数据库防火墙

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 详细要求 |
| 硬件配置 | 接口配置 | 2U机箱，至少6个千兆电口(支持1组bypass)、1个HA口、1个管理口，最大支持配置26，2个可扩展槽位，冗余电源。 |
| 系统性能 | 性能 | DB最大并发数：≥7000； SQL处理能力：≥12000/s； |
| 基本要求 | 部署模式 | 支持旁路部署方式、支持代理式串联部署模式、支持透明网桥串联部署模式 |
| 云环境下动态分配扩展性要求 | 支持云环境部署模式，提供云平台统一管理和资源动态分配扩展接口，能够与VMware、Hyper-V、OpenStack、Cloud Stack、KVM、Fusion等云平台管理系统或第三方的云管理平台进行无缝集成。 |
| 数据库兼容性 | 支持国际主流数据库： 、MySQL、SQLserver、DB2、Sybase、Informix、Teradata、PostgreSQL、Access、cache  支持国产数据库：达梦、南大通用、人大金仓、神通、浪潮KDB、湖南上容、翰高  支持非关系型数据库：Hive、Hbase、MongoDB等 |
|  | 动态建模：支持SQL自学习功能，可以自动学习应用程序访问数据库的行为特征，并自动建立安全访问规则，允许合法的访问行为，对异常SQL行为进行跟踪和阻断。（提供截图证明） |
| 能够根据不同的用户指定不同的数据访问策略，未授权用户在访问敏感数据时根据设置返回自定义的数据（提供截图证明）） |
| 被保护字段的权限控制应独立于数据库的权限控制，根据访问策略可限制DBA访问敏感数据，防止数据库用户的权限提升引起的数据泄密，但不影响DBA对数据库系统的正常维护 |
| 数据在线脱敏，支持前缀明文的脱敏方式，能够根据权限设置不同的脱敏方式，可对列中指定的前N字节不显示，例如对身份证号的前10个字节不显示（提供截图证明） |
| 提供利用CVE上已公开的数据库漏洞，进行攻击拦截的虚拟补丁； |
| 对超过特定行数阀值的批量数据导出，高危操作，no where 全表Update、Delete行为，口令攻击防护，高频访问行为等进行自动识别和阻断。 |
| 敏感数据发现 | 可以对指定的数据库基于名称、基于数据内容进行敏感数据扫描，发现数据库中存在的敏感数据的字段及其在服务器、数据库的分布情况。 |
| 阻断模式 | 会话阻断：对威胁的访问行为，中断数据库连接会话。  语句拦截：对需要阻断的访问，返回错误提示信息，当前语句被拦截，该会话不中断。 |
| 产品可靠性 | 支持主主、主备模式部署；支持HA双机主备自动切换，支持策略同步、会话同步机制，保障多设备间的一致性；  支持软硬件bypass功能，可自动启动和关闭网口间bypass导通，保障系统异常环境下的网络畅通； |
| 数据库状态监控 | 支持对数据库进行健康评分（提供截图证明） |
| 系统界面可以显示数据库的用户、缓冲区击中率、共享内存、索引效率、查询统计、查询缓冲命中率等信息 |
| 系统支持设置数据库状态参数阈值，触发阈值时可快速告警。 |
| 数据库风险扫描 | 内置风险扫描功能，自动扫描各种管理和系统风险，包括用户弱口令、权限配置、数据库配置风险、操作系统相关风险 |
| 服务发现 | 可以根据常用端口号、自定义端口号发现指定网段范围内存在的数据库服务，并可直接将发现的数据库服务直接加入到防护引擎 |
| 告警 | 内置自动告警设置，支持系统资源监控与告警；支持敏感语句告警策略；支持风险操作、SQL注入、漏洞攻击告警等等。告警必须提供级别设定，至少提供致命、高风险、中风险、低风险4种告警级别 |
| 支持短信、SYSLOG、SNMP 、邮件、FTP等多种事件告警和提示方式 |

### 安管区域汇聚交换机

|  |  |
| --- | --- |
| 功能及技术指标 | 参数要求 |
| 整机性能 | 交换容量≥730Gbps(以官网最小值为准) 转发性能≥220Mpps(以官网最小值为准) |
| 关键部件冗余 | 配置可插拔冗余风扇和电源 |
| 接口 | 主机至少需要固化24个千兆电口口，4个万兆光口并配置1个万兆光模块 |
| 扩展插槽 | ≥1个 |
| 堆叠 | 最大堆叠台数≥9台 |
| 最大堆叠带宽≥160G |
| 支持通过标准以太端口进行堆叠 |
| 支持远程堆叠 |
| 链路聚合 | 支持最多8个端口聚合；支持最多128个聚合组；支持LACP |
| 镜像功能 | 支持流镜像，N：4端口镜像，本地和远程端口镜像 |
| VLAN特性 | 支持基于端口的VLAN，IP子网的VLAN，协议VLAN，MAC VLAN，Voice VLAN，QinQ，灵活QinQ |
| 组播协议 | 支持IGMP Snooping，MLD Snooping，组播VLAN，PIM SM，PIM DM |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| Macsec | 支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准 |
| 支持多控制器（EQUAL模式、主备模式） |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| OAM | 支持802.1ag |
| 支持802.3ah |
| 安全特性 | 支持基于端口的认证和基于MAC的认证 |
| 支持SSH2.0 |
| 支持端口隔离 |
| 支持 Portal认证 |
| 安全扩展功能 | 支持AV防病毒，ACG，IPS等安全功能，提供第三方测试报告 |
| 有线无线一体化 | 支持无线AC功能，支持分层AC方案，可作为中心/本地AC，提供设备权威测试报告证明 |

### 流量复制器

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 自主可控 | 采用国产自主芯片，和安管区域汇聚交换机同品牌 |
| 硬件形态 | 基于ASIC架构，非CPU+FPGA架构 |
| 整机性能 | 交换容量≥256Gbps（以官网最小值为标准） 转发性能≥155Mpps （以官网最小值为标准） |
| 性能冗余 | 为了提高设备可靠性，配置2个模块化电源，2个模块化风扇 |
| 接口类型 | 主机至少需要固化24个千兆电口，4个万兆光口 |
| 扩展插槽 | ≥1个可扩展插槽 |
| 堆叠 | 最大堆叠台数≥9台 |
| 支持通过标准以太端口进行堆叠（万兆或40G均支持） |
| 支持远程堆叠 |
| 流量识别 | 支持端口入方向ACL，匹配字段包括二层头部、内外层VLAN、IP/IPv6五元组、优先级字段、分片报文。 |
| 支持GRE识别 |
| 支持对以上的识别需求组合设置 |
| 流量处理 | 包括复制、转发和丢弃；统计计数 |
| M:N模型 | M:N复制(M个源复制到N个目标) |
| 分片报文 | 支持分片报文处理 |
| IPv6复制 | IPv6复制 |
| 管理方式 | 命令行、Web、Netconf、RESTful API |
| 报文头部修改 | 支持使用VLAN Tag来标记入端口 |
| 支持内外层VLAN Tag修改 |
| 支持剥除VLAN标记 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN |
| 支持基于MAC的VLAN |
| 最大VLAN数(不是VLAN ID) ≥4094 |
| 链路聚合 | 支持最多8个GE口或4个10 GE端口聚合；支持最多128个聚合组（IRF2）；支持LACP |
| 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 |
| 支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准 |

## 社区卫生服务中心端主要设备技术参数要求

### 社区卫生中心出口防火墙

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 兼容性 | 与社区服务器汇聚交换机同品牌 |
| 硬件架构 | 采用非X86多核架构，配置冗余电源 |
|
| 接口要求 | 主机至少需要固化千兆电口≥16，千兆光口≥8，万兆光口≥2 |
| 性能要求 | 吞吐量≥ 8G 并发连接数≥ 800万 每秒新建连接数≥ 12万/秒 |
|
|
|
| 安全应用 | 整机同时具备防火墙、链路负载均衡、入侵防御、防病毒、WEB应用、应用识别等功能，提供官网截图证明并盖章，实配3年防病毒授权，3年入侵检测授权 |
| VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 |
| 支持IPsec VPN隧道自动建立，无需流量触发； |
| 支持IPsec VPN智能选路，根据应用和隧道质量调度流量。 |
| 可基于每个SSL VPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。 |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 |
| 应用识别 | 支持至少5000条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。 |
| URL过滤 | 设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤； |
| 设备支持管理者自定义新的URL地址和URL分类； |
| 支持联动云端URL地址库进行全面实施核查。 |
| 入侵防御 | 支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。 |
| 支持超过7000种特征的攻击检测和防御 |
| 防病毒 | 可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表； 支持基于文件协议、邮件协议（SMTP/POP3/imap)、共享协议（NFS/SMB）的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。 发现病毒发送的告警信息，支持用户编辑告警内容 |
| 支持云端防病毒，为保证检测时效性，特征缓存数至少保证20万条且缓存保留时间不应少于700分钟 |
| DDoS防护 | 能够防范DOS/DDOS攻击： Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP欺骗、TCP报文标志位不合法、超大ICMP报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片Flood、Tiny-Fragment。 |
| 支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略 |
| 诊断中心 | 支持基于接口及IP的报文捕获，并将捕获到的报文生成Wireshark（一种网络封包分析软件）可识别的.cap后缀文件，保存到本地或外部服务器，供用户分析诊断出入设备的流量 |
| 支持丢包统计功能，用与分析和记录设备的转发流程和安全业务模块（如：攻击防范、会话管理和连接数限制等）丢弃报文的详细原因，通过查看各个模块丢弃报文的详细原因，有利于管理员对网络故障的快速排查和定位。 |
| 支持网页诊断功能，用于当内网用户访问网页出现故障时，对网络进行基本的诊断，并给出故障原因。 |
| 具备信息产业信息安全测评中心出具的防火墙EAL4+级型式试验报告； |

### 社区服务器汇聚交换机

|  |  |
| --- | --- |
| 功能及技术指标 | 参数要求 |
| 整机性能 | 交换容量≥730Gbps(以官网最小值为准) 转发性能≥220Mpps(以官网最小值为准) |
| 关键部件冗余 | 配置可插拔冗余风扇和电源 |
| 接口 | 主机至少需要固化24个千兆电口口，4个万兆光口并配置1个万兆光模块 |
| 扩展插槽 | ≥1个 |
| 堆叠 | 最大堆叠台数≥9台 |
| 最大堆叠带宽≥160G |
| 支持通过标准以太端口进行堆叠 |
| 支持远程堆叠 |
| 链路聚合 | 支持最多8个端口聚合；支持最多128个聚合组；支持LACP |
| 镜像功能 | 支持流镜像，N：4端口镜像，本地和远程端口镜像 |
| VLAN特性 | 支持基于端口的VLAN，IP子网的VLAN，协议VLAN，MAC VLAN，Voice VLAN，QinQ，灵活QinQ |
| 组播协议 | 支持IGMP Snooping，MLD Snooping，组播VLAN，PIM SM，PIM DM |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| Macsec | 支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准 |
| 支持多控制器（EQUAL模式、主备模式） |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| OAM | 支持802.1ag |
| 支持802.3ah |
| 安全特性 | 支持基于端口的认证和基于MAC的认证 |
| 支持SSH2.0 |
| 支持端口隔离 |
| 支持 Portal认证 |
| 安全扩展功能 | 支持AV防病毒，ACG，IPS等安全功能，提供第三方测试报告 |
| 有线无线一体化 | 支持无线AC功能，支持分层AC方案，可作为中心/本地AC |

### 社区卫生中心服务器区边界防火墙一

|  |  |  |  |
| --- | --- | --- | --- |
| 主指标项 | 子指标项 | 指标参数要求 | |
| 基本要求 | 系统结构 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供相应资质证明）； |
| 操作系统 | 安全操作系统采用冗余设计，出于安全性考虑，多系统需在设备启动过程中进行选择不得在WEB维护界面中设置系统切换选项。 |
| 系统软件 | 系统具有良好的扩展性，支持扩展病毒防御、入侵防御、应用识别、网站分类库过滤、数据防泄漏、IPSEC VPN、APT防御等功能。 |
| 系统性能 | 整机吞吐率 | ≥10Gbps |
| 应用层吞吐率 | ≥3Gbps |
| 最大并发连接数 | ≥220万 |
| 机箱 | 1U |
| 硬件配置 | 接口配置 | 配置为6个千兆电口和2个SFP插槽，2个可插拔的扩展槽，含应用识别功能，含入侵防御、防病毒模块。 |
| 工作模式 | 支持路由、交换、混合、虚拟线工作模式； |
| 访问控制 | 入侵防御  （IDP模块） | 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； |
| 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4200+攻击特征库，同时支持自定义特征库,且厂商具备强大的漏洞和功放研究能力，为CNNVD一级支撑单位，能够确保每周至少更新1次攻击特征库。 |
| 安全防护 | 未知威胁防御 | 支持APT防御，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day漏洞）、木马、病毒具有检测能力；可根据用户环境，将APT工作模式设置为深度模式或者智能模式。 |
| DDOS防御 | 支持异常行为检测，内置统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警； |
| 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； |
| 病毒过滤  （AV模块） | 支持基于IP协议的检测清洗，包括但不限于：IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke等异常报文攻击； |
| 应用识别  （应用识别模块） | 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（提供P2P流量识别技术相关的专利证明）、web应用、移动应用、云应用、加密应用（需提供相关功能截图与加密流量识别相关的专利证明，当前此专利为实审阶段，请酌情使用）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（需提供相关功能截图）； |
| 文件过滤 | 内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM文件传输等应用类型以及HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过50种文档类型的文件过滤 |
| 内容过滤 | 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； |
| 配置维护 | 支持多个配置文件并存，配置文件数量不少于20个 |

### 社区卫生中心服务器区边界防火墙二

|  |  |
| --- | --- |
| 指标 | 指标参数 |
| 硬件性能要求 | 多核AMP+架构，网络层吞吐量10G，并发连接≥250万，每秒新建连接数15万， 标准2U机箱，单电源，标准配置6个10/100/1000M自适应电口，2个SFP插槽，支持1个扩展槽，1个Console口，支持液晶屏，含3年硬件维保服务，3年防病毒模块。 |
| 功能要求 | 所投产品必须支持手工指定、802.3ad协议等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份 |
| 所投产品必须支持MTU≥9012byte的巨型帧通过设备传输时不分段 |
| 所投产品支持将特定用户、应用、URL分类标记为重点关注。支持单独呈现重点关注对象的流量、访问次数等统计信息。并可基于用户/IP地址、应用、URL分类执行筛选、关联式分析，快速挖掘异常用户及异常网络行为。 |
| 联动处置 | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万；支持与云端大数据中心联动； |
| 所投产品必须支持与客户现有网络中心的桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断终端网络活动的同时，提示被阻断原因及重定向至自定义网址。 |

### 等保一体机

|  |  |
| --- | --- |
| 项目 | 指标要求 |
| 硬件参数 | 内存≥48G  硬盘≥128GB SSD+4TB SATA  千兆电口≥4个，千兆光口SFP≥4个  2U，冗余电源 |
| 产品形态 | 产品支持软、硬件一体化与软硬件解耦两种部署方式 |
| 部署模式 | 支持网桥、路由、旁路模式部署（提供界面截图证明并加盖厂商公章） |
| 平台要求 | 平台包含数据库审计模块、堡垒机模块、日志审计模块、漏洞扫描模块等安全功能模块 |
| 平台可根据实际业务环境定义业务安全区域，简化运维管理； |
| 综合考虑用户实际管理运维人数，为简化运维，缩短客户学习时间，要求所投产品的管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备。（提供界面截图证明并加盖厂商公章） |
| 为了提供更好的排障手段，支持在平台内节点抓包分析分析功能，能够设置抓包的网口、过滤条件、文件大小等参数 |
| 平台支持关键安全组件双机功能，保障安全组件高可用；在双机场景下，管理平台要支持双机配置同步，在硬件故障时保障无感知切换。 |
| ▲具备业务、用户风险视角等界面，支持针对业务、用户的风险事件进行分类，包含已经明确失陷的业务以及业务的威胁、脆弱性分析；产品能够针对已经实现、具备威胁与脆弱性不同阶段的安全事件进行等级描述、定位事件从何种安全组件上报。（提供界面截图证明并加盖厂商公章） |
| 支持针对安全组件账号的三权分立管理，实现平台管理员账号与安全组件账号权限的对应，防止平台管理员对安全组件进行越权操作。 |
| 集中管控 | 支持基于一体化平台的安全管理中心功能，能够对设备进行统一纳管，包括规则库与补丁包的统一升级、策略的统一配置、客户端补丁包统一升级等 |
| 支持等保2.0安全管理中心要求自评功能，能够进行完整度评估 |
| 支持安全管理中心交付模板，帮助用户快速交付安全管理中心各项功能 |
| 数据库审计功能要求 | 系统软件，数据库流量≥200M，日志检索≥15000条/s |
| 采用B/S管理方式； |
| 支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下4个维度:SQL模板、业务系统、URL地址及数据库条件； |
| 支持基于SQL命令的webshell检测，提供webshell日志查询；  可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威； |
| 堡垒机功能要求 | 提供不少于50个资产授权 |
| 能够记录RDP协议中的活动窗口名称、删除文件等动作，并能记录RDP会话中的键盘输入信息； |
| 日志审计功能要求 | 内置不少于50个主机审计许可证书 |
| 支持获取各种主流网络及数据库访问行为，支持Syslog、WMI、OPSEC Lea、SNMP trap和LogBase专用协议等协议事件日志，支持通过Http、Https、FTP、SFTP、SMB等协议获取各类文件型日志，支持基于SQL/XML标准内容获取； |
| 系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。 |

## 安全数据可视化及运维管理平台

青浦卫健委于2017年开始使用一套IT运维管理系统，实现了卫健委机房设备资产管理模块、运行故障处置管理流程以及资产、工单数据可视化展现功能。

本次运维平台建设需对接卫健委现有IT运维管理系统管理流程及可视化展现功能，实现面向设备、运维工作管理的运维能力，实现社区子平台的建设与对接，实现全区安全运维数据的统一可视化展现，最终建设成为区卫健委符合等保三级建设的“统一资产登记、集中监测管理、集中故障处置、自动化操作管理、统一服务流程管理、综合可视化展现”的安全运维管理平台。安全运维管理平台具有以下能力：

1、 实现本次项目建设的所有设备和软件资源的资产数据，都纳入到安全运维管理平台中统一管理，并进行资源访问权限控制。

2、 实现本次项目建设的所有设备和软件系统的集中监测，监测数据需集中汇聚到区安全运维管理平台进行统一管理。

3、实现本次项目建设的所有设备和软件系统的自动化操作管理能力，对设备进行等保巡检、对设备配置进行备份。

4、根据卫生等保建设要求，对日常运维过程中的服务申请、维护工作进行流程化管理。

5、集中汇聚社区安全运维子系统的运维数据，实现全区统一部署，支持分权控制。

6、实现安全态势感知平台的故障告警数据和统计分析数据需集中汇聚到安全运维管理平台，进行统一告警通知、统一流程化管理以及统一展现。

7、实现全区统一运维大屏可视化系统展现，综合展现资产、运行监测、安全管理、服务请求、服务保障各类运维数据。

### 区级安全运维管理平台

#### 统一资产与资源管理（CMDB）

系统需具备对本次项目建设的各类设备设施、软件资源和运维资源进行统一资产登记管理的能力，包括设备资产、软件资源、合同、项目、供应商等，提供资产模型适配能力、资产分类管理能力、资产变更控制能力、资产变更记录跟踪等。

（一）软硬件资产登记管理

系统需支持卫健委各类设备设施的统一资产登记管理，支持设备分类管理，登记的设备信息包括但不局限于：

1）设备资产基本信息，内容包括资产名称，资产编号，规格型号，资产类型，生产厂家，到货日期，存放位置，出厂日期，出厂编号，安装地点，上线日期，采购价格、使用部门，使用责任人、入库人姓名及工号、审核人姓名及工号等信息。

2）设备位置信息，如校区、楼、房间号等信息。

3）设备维保信息，包括：供应商、采购合同号、采购批次、采购日期、保修年限（到某年某月为止）等信息。

（二）网络布线登记管理

系统需支持对卫健委机房网络路线信息的登记管理，包括光缆、光纤以及五类线的连接信息管理，支持根据服务器、安全设备查询设备的连接链路信息。

（三）设备配置变更信息登记管理

系统需支持对网络、安全、服务器设备配置信息变更的登记管理，每一次信息变更，都产生一条变更记录，并支持以时间线的方式展现和查询变更信息。

（四）项目信息登记管理

系统需支持卫健委项目建设信息的登记管理，信息至少包括项目时间、项目名称、项目预算、项目招标文件、项目中标金额、项目建设单位、项目交付状态、项目服务厂商等信息。

（五）合同信息登记管理

系统需支持卫健委IT项目建设合同与维保服务合同信息登记管理，信息至少包括合同年份、合同类型、合同签订厂商、合同有效期限、合同服务条款等各项信息。

（六）服务商与人员信息管理

系统需具备供应商管理功能，支持对各类设备和软件系统的供应商的信息、联系方式、服务合同、服务周期进行管理。

（七）资产台账数据维护功能要求

系统需支持多种配置项收集手段，包括人工录入和批量导入等，同时支持针对多个数据源的配置数据调和能力。

系统需支持针对配置项数据的变更审核能力，并支持版本控制能力。

系统需支持配置维护导航树，从不同的维护角度来组织数据，能够支持配置维护的权限控制。

系统需支持全文检索查找配置项，全文检索支持关键信息预览（包含匹配关键字）。

系统需提供图形化的设备应用关系展现，提供多种样式的自动化布局。

系统需提供资产的提醒功能，针对资产的库存和过保状态进行提醒，支持提醒范围、提醒级别、提醒时机和通知方式等策略化定义。

（八）资产管理模型自定义管理

系统需具备资产管理数据模型在线的编辑能力，以适应卫健委持续的资产与资源台账管理需求，具备功能表现如下：

系统需支持灵活的动态建模功能，可根据实际管理环境和管理需要自由、灵活的定义和调整配置管理模型，实现精确化管理。

系统需支持面向资产配置项类型的界面化定义，支持添加新的资产类型。

系统需支持资产配置项数据属性的界面化定义，支持添加新的资产属性，支持设定属性类型。

系统需支持资产配置项用户交互表单的界面化定义，支持通过拖拽方式在线定义资产录入、浏览用户界面。

系统需支持资产配置项关系的图形化建模能力，支持在线设备不同资产项的安装关系，如操作系统与服务器设备的关联关系。

（9）设备资源配置发现功能

系统需支持通过程序自动发现设备资产数据，提升等保资产梳理能力，具备网络扫描与深度发现两种资源自动发现能力。支持定时和人工启动两种方式执行发现任务，支持多个发现任务的并行执行。

系统需支持向导式发现配置功能，支持ICMP、TCP、SNMP、WMI、Telnet、SSH、CCLI、Http、DNS、JDBC等多种协议来实现配置信息的自动发现，用户可以通过发现配置向导来实现发现范围、发现参数的设置。

系统需支持将发现结果导入到配置管理库中，并支持后台策略自动将资源归属到对应数据维护分区。

（十）资产资源访问权限管理

系统需对资产台账的用户访问权限监控有效控制，支持按系统或按负责厂商提供资产查看和编辑权限。

#### 集中监测与管控

（一）设备运行监测管理

设备运行监测管理需支持安全、网络、主机以及软件服务等各类软硬件资源的监测采集功能。监测管理支持多种监测采集方式，包括SNMP、SSH或API等远程协议方式，以及Agent等方式，保障设备运行数据的获取。

系统需支持获取安全设备状态、性能指标、端口流量等指标数据。

系统需支持获取主机设备状态、性能指标、容量指标、端口流量等指标数据，支持获取设备的运行日志数据。

系统需支持获取存储设备的状态、性能指标数据。

系统需支持获取数据库、中间件等基础软件的运行状态、性能指标数据。

系统需支持对本地在线设备的自动发现能力，支持网络拓扑的自动生成，支持对网络链路的监测和故障告警。

系统具有良好的扩展性，支持自定义的监控能力，提供可配置、脚本化的监控采集扩展。

（二）监控指标阈值分析管理

系统需支持将一个或多个指标的采集和阈值规则的配置，形成一个单独的策略模板，通过复制的方式进行克隆策略，对策略加以修改和引用到具体的监控对象。

系统监测阈值分析需具备预防误报功能，报警策略应支持时间条件，允许配置指标已经持续若干分钟达到阈值，才进行报警，以避免偶尔的性能波动引起频繁报警。

（三）设备安全等保自动化巡检

系统需支持根据三级等保安全管理要求，对网络、安全、服务器设备的安全合规性进行检查，支持基于安全策略进行系统巡检，并提供安全合规检查报告。

（三）自动化运维操作管理

自动化管理需实现对日常运维操作的自动化操作功能，对日常运维操作进行服务封装，通过流程编排建立自动化能力，将人工的运维任务转变为自动化作业，从而提高运维效率，规范操作规程，降低误操作风险。应具备的功能要求如下：

系统需提供内置的自动化操作脚本库，支持根据操作管理需求创建各种操作脚本，支持多种脚本语言，支持脚本的在线编辑与调试。

系统的操作脚本支持输入参数定义，支持多种参数类型。

系统需提供基于浏览器的可视化自动化作业流程编排设计器，支持多模式定义流程编排。

自动化作业编排支持设定手工或定时执行，通过作业管理进行管控。支持编排设定参与人，只有参与人才可编辑和执行该编排，所有人可查看编排信息、执行历史。

系统支持自动记录自动化操作的执行总时间、每个作业任务执行的耗时，可根据按任务维度查看、设备维度查看作业详情。

（四）核心系统用户访问监测

用户访问监测应当实现对业务系统应用前端（Web端）的运行性能、故障、用户操作体验及用户行为的监测分析，为应用前端性能优化、故障处理、用户体验优化、应用评估提供数据支撑。

系统应采用轻量级的监测插件，不应对应用业务逻辑进行改造。系统应具有良好的水平扩展能力，满足未来监控性能扩展要求。

系统应当提供前端应用总体访问分析能力，支持按访问用户数、操作数、错误数进行排序。

支持分析业务应用的界面性能、运行错误、用户轨迹、访问热图等，并提供性能、错误、用户访问等主题数据分析，展示数据变化趋势。用户访问热图支持展示用户访问业务系统的所关注页面区域，了解热点页面与热点操作。（提供功能截图证明）

系统支持监测页面各组件（如Html文档、JS文件、CSS、Ajax资源、图片、字体等）加载性能，如重定向、应用缓存、请求、响应、组件加载、渲染等全过程耗时情况。

支持按照浏览器、操作系统、区域等角度分析页面错误的分布情况。支持识别发生前端错误的用户列表，了解其所在的区域、使用的浏览器类型及版本、分辨率、终端浏览器类型等信息同时支持定位页面发生的代码位置。

（五）应用系统全景分析管理

应用系统全景分析管理以业务应用为中心，实现业务系统运维数据与管理功能场景的融合管理，包括系统资源、系统监测、故障告警、系统工单、系统逻辑拓扑等，实现数据与管理界面的统一。管理功能包括：

业务应用信息展示，支持查看应用系统的维护任务情况、资源状态、系统KPI，提供应用的健康度得分以及可用率，同时可以添加指标仪表。

业务应用工单管理，支持查看未关闭告警数、待处理事件工单数、逾期事件工单数、待处理变更工单数。

业务应用资源管理，支持查看所有资源的类型以及资源的状态；支持绘制应用拓扑，拓扑数据支持与资产与资源管理库（CMDB）同步。

#### 统一故障事件管理

系统需支持接入集中监测模块、安全设备、安全态势感知平台等设备与系统的故障告警信息，实现统一告警接入、分析处理和通知。系统具备对故障事件的完整的处理过程，包括格式化、过滤、压缩分析、自动消除、通知策略联动。

系统需支持事件的接入标准化功能，无需经过二次开发编译，通过配置界面配置接入规则，即可接入新的告警事件，支持装载SNMP MIB来解析Trap。

系统需支持告警的时间线分析能力，便于运维人员根据时间相关性快速分析告警的根源。

系统需支持事件过滤功能，通过配置事件过滤规则，对事件进行过滤，抛弃不需要关注的事件。

系统需支持告警压缩功能，通过配置界面设置事件压缩规则，将重复事件进行压缩处理，并根据条件更新告警的部分信息（如最新告警时间、告警次数等）。

系统需支持告警归并功能，可以设置告警归并规则，可对自动恢复的告警事件进行归并消除，例如：端口Up事件自动消除端口Down告警。

系统需支持告警升级，能够升级到指定级别，或者按照递增指定等级升级到相应告警等级；

系统需支持告警通知规则，可配置自动向告警责任人发送告警通知，支持声音、电子邮件等多种通知方式，支持工单派发接口。

#### 统一运维服务管理

（一）故障处置管理流程

系统需具备对安全运维故障事件的流程化处理，通过自动建单、人工建单、工单派发、工单审批、信息反馈等多场景工单处理，实现安全事件的流程化管控。

（二）应急响应管理流程

系统需具有安全事件应急响应流程，支持对重大安全事件或者特定类型事件发起应急响应流程，记录事件描述、发生时间、事件类型、响应时间、解决方案、主要负责人等事项。

（三）服务申请管理流程

系统需提供服务申请管理流程，对服务厂商到场巡检、进入机房、设备申请、配置修改等操作进行登记申请、配置记录和审核管理。提供的申请流程包含但不局限于：

外来人员进出机房申请管理；

设备进出机房申请管理；

设备外出申请管理；

设备配置变更申请管理；

系统外联申请管理；

系统数据拷贝申请管理；

账号权限申请管理；

重要安全配置调整申请管理；

等日常运维服务管理以及三级等保要求的管理工作，进行制度化、流程化和电子化的管理。

系统需提供服务定义、服务目录发布管理功能，支持运维管理人员在线定义和发布新的服务申请管理功能。

（四）厂商维保服务巡检管理

系统需支持对厂商巡检信息进行登记管理，包含但不局限于巡检时间、巡检人、巡检厂商、巡检内容、执行的服务合同、巡检记录附件等信息。

（五）驻场服务管理功能

系统需具备驻场服务工作管理的功能，对本次项目建设的所有设备和软件系统的周期性巡检维护工作进行在线登记，包括巡检时间、巡检类型、设备名称、巡检人等。系统具备自动生成巡检任务、对巡检任务进行提醒以及对设备巡检情况进行统计分析的功能。

（六）流程在线自定义功能

系统应支持灵活的流程设计能力，可根据实际管理环境和管理需要自由、灵活的定义和调整流程模型。需要满足以下要求：

流程设计：支持WEB在线的流程自定义，实现流程环节可定义，流程处理人可定义，流程展现可定义，无需任何编码。支持子流程、流程并发和会签节点，支持无序会签和依次会签两种模式。

流程表单：支持流程在不同环节展现不同的表单，表单支持自定义字段，字段类型包括时间、短文本、数字、长文本、富文本、附件、下拉列表、单选项、多选项、图片、部门、表格等，支持工单图片在线预览，表单支持复制功能；

流程动作：支持流程环节触发定时任务和自动任务，支持触发自动化作业等外部任务，支持动作触发器和时间触发器两种方式。流程流转到自动节点后自动调用编排执行并传递工单字段作为参数，等待执行结束后流程继续流转。支持调用第三方RESTful接口实现流程流转过程中触发调用。

流程模型：支持流程模型的复制、删除、启动和停用功能。支持流程模型的授权功能，不同的流程由不同的用户进行管理和使用。

#### 区-社区两级运维协同管理

流程协同管理系统支持社区管理人员以流程工单和即时消息协同的方式与区卫健委管理人员及运维人员进行在线交互。

（一）运维工单协同

运维工单协同通过区级、社区建立运维工单，实现区卫健委运维团队和社区运维人员之间运维工作的协同交互。

系统支持社区运维人员提交运维工单，由区运维组进行工单处置和运维信息反馈，社区人员对运维工作进行确认。

系统支持区运维组建立运维任务工单，由各社区运维人员进行工单处置。

（二）即时消息协同

即时消息协同通过提供IM实时通讯，整合各个运维工具高效协助工作，将所有的运维活动带入到沟通会话的过程中。

系统支持群组创建：支持按职责和场景划分群组，让信息互不干扰，同时兼顾信息透明和保密，保证团队成员间知识对等。

系统支持群组沟通，支持将监控故障告警、运维工单带入到沟通会话的过程中，沟通组人员点击数据即可关联到运维平台相关数据。

系统支持群组沟通，基于群组进行消息沟通，支持文本、富文本、文件等多种类型的消息格式。

#### 运维服务考核评估管理

系统需提供运维服务考核管理功能，对驻场运维人员的服务工作和外厂商服务合同执行情况进行评估。

（一）驻场人员考核

系统需对驻场服务人员的运维服务工作量、故障响应时间进行统计分析，评价服务人员服务工作的质量和效率。（提供功能截图证明）

（二）外厂商巡检工作考核

系统需具备对卫健委外场服务商的服务合同执行情况进行管理，包括服务合同条款、服务时间、服务条款执行情况（服务次数、服务质量），服务工作内容等多维护进行数据管理和考核分析。

#### 系统集成与平台配置要求

（一）态势感知平台数据集成

系统需与安全态势感知平台系统数据集成，实现单点登录，实现态势感知故障告警数据的集中汇聚、统一处理和展现。

（二）机房动环系统集成

系统需实现与卫健委机房动环系统集成，实现动环供电、温湿度等数据以及故障告警数据的集中汇聚，实现统一运维、统一展现。

（三）社区安全运维子系统对接

系统需支持集中接入社区监测管理模块、自动化操作管理模块数据对接，集中汇聚区节点的监测数据、管理数据，实现全区统一运维、集中展现。

（四）其他要求

升级后的系统需具备高效的数据处理能力，具备运维数据大数据存储和管理能力，各类设备的故障发现周期小于30秒，数据存储时间大于2年，除报表之外的功能界面访问的平均响应时间小于3秒。

系统应具备良好的开放性，可以融合第三方监控系统的资源信息、监控信息，提供开放的API接口，可随需扩展开发所需功能。

### 社区安全运维子系统

#### 跨网分布式部署

区级安全运维管理平台部署在政务外网，各社区中心的设备与服务在各自管理网中，两个网络相互独立，社区安全运维管理子系统需实现社区网设备运维管理，同时需支持通过跨网部署把设备运维数据推送给区级安全运维管理平台。

本次项目建设，各投标人需提供可行的区级-社区跨网安全运维管理平台部署和数据对接管理部署方案，并自备相应的设备及软件模块。

#### 监测管理

监测管理子系统需支持安全、网络、主机以及软件服务等各类软硬件资源的监测采集功能。监测管理支持多种监测采集方式，包括SNMP、SSH或API等远程协议方式，以及Agent等方式，保障设备运行数据的获取。

系统支持获取安全设备状态、性能指标、端口流量等指标数据。

系统支持获取主机设备状态、性能指标、容量指标、端口流量等指标数据，支持获取设备的运行日志数据。

系统支持获取存储设备的状态、性能指标数据。

系统支持获取数据库、中间件等基础软件的运行状态、性能指标数据。

系统具有良好的扩展性，支持自定义的监控能力，提供可配置、脚本化的监控采集扩展。

监测管理需支持与区级安全运维管理平台对接，实现监测数据实时上报到区级平台，实现统一存储、统一故障告警和统一展现。

#### 设备自动化操作管理

系统需支持对网络、安全设备的配置进行定期自动备份功能。

系统需支持根据等保要求，对设备进行安全合规性检查，支持基于安全策略进行系统巡检，并提供安全合规检查报告。

系统需提供内置的自动化操作脚本库，支持根据操作管理需求创建各种操作脚本，支持多种脚本语言，支持脚本的在线编辑与调试。

系统支持与区级安全运维管理平台对接，支持操作数据上报安全运维管理平台，实现统一存储、统一故障告警和统一展现。

### 全区运维大屏可视化系统

系统根据数据的业务逻辑和可视化场景分析，提供支持多层级的数据展现，从数据综合展现到单场景数据分类展现，从全局数据展现到单机构数据展现，以及数据指标钻取呈现等功能。

该平台软件需对青浦卫健委和下辖11个社区卫生服务中心的安全运维管理现状进行综合打分并对需要实现的管理目标做分项的绩效指标管理并展示。

（一）安全运维数据分析

系统需支持对区级安全运维管理平台的监控性能数据、告警告警、资产数据、运维工单等运维数据进行运维分析，提供环比、同比、分类等多种方式进行运维统计分析。

可用性分析：网络、服务器、数据库、中间件、虚拟机等软硬件的可用性统计报表；

性能分析：通过资源的运行性能进行分析，掌握运行性能趋势分析，诊断性能瓶颈；

容量分析：从业务数据、运行性能数据等角度提供IT基础设施的容量分析报表。

（二）态势感知分析数据抽取

系统需集中汇聚区级态势感知平台运行分析数据，包括综合态势统计分析、外网攻击态势数据、整网威胁态势数据、风险用户数据、扫描侦查数据、漏洞利用数据、恶意文件分析数据、权限获取数据、恶意通信数据、数据泄露数据、攻击阶段还原数据等数据，实现统一的可视化展现。

（三）安全与运维数据可视化呈现

▲可视化模块首界面需以青浦区地理空间为背景，具有良好的3D操作体验和可视化效果，支持各级管理中心在地图上标注，点击可查询详情数据。（提供功能截图证明）

数据综合展现。针对单一的综合性数据场景，通过设计逻辑场景视图，结合关键KPI数据指标，实现综合数据场景的设计，各类数据指标，支持向下钻取。

安全态势可视化呈现。安全态势可视化展现综合呈现卫健委三级等保安全运维数据，包括安全资产、外网攻击、威胁数据、漏洞数据、漏扫情况数据等以及安全故障告警信息和处置信息，直观的展现卫健委安全运行的情况。（提供功能截图证明）

网络可视化呈现。网络可视化呈现卫健委全区的核心、汇聚设备的在线可视化展现，系统支持按网络分区、网络分层对各类网络设备和资源进行可视化展现，如下图所示：

主机平台可视化呈现。系统可视化展现支持对主机平台和云平台的设备、运行、资源使用情况进行图形化展现，综合展现设备资源组成、设备在用、性能负载等各项数据。

业务系统可视化呈现。系统可视化呈现支持多维度、层次化的展现业务系统的组成和运行态势，提供基于应用系统整体运行态势监控视图，也提供基于应用系统基础架构组成关系的业务逻辑监控展现视图。

资源资产可视化呈现。资源可视化呈现视图实现对数据中心各类设备设施和系统类型、分布、所属部门等各类数据进行分类统计和可视化展现，综合展现负责维护管理的资源的整体情况。

运行维护管理数据可视化。运行维护管理数据可视化实现对日常运行维护过程中的日常巡检、报修维修、数据中心应用故障处理状态、统计数据的可视化展现。

机房实景3D可视化展现。系统能够根据运维资产配置数据，提供机房、机柜、设备的可视化展现，支持展现视图的自动生成。

3D机房支持与监控数据关联，实现设备位置展现、设备运行故障展现、空间容量计算等。

（四）在线可视化设计工具

系统提供可视化设计器，可通过拖拽进行展示视图的设计。

设计组件：支持柱形图、条形图、柱状拆线图、拆线图、饼图、玫瑰图、仪表盘、雷达图、热力地图、散点热力图、飞线地图、漏斗图、键值表、环状图、气泡图等图表，坐标轴图表：支持数据集、X轴值系列、Y轴值系列、图例、系列的配置，饼图类图表：支持数据集、分类系列、值系列、值标签、图例、系列；支持滚动计数器、温度计、时间、文字、图片、动态图片、表格等通用组件；支持网络设备、服务器设备、安全设备、存储设备、数据库、中间件等资源模具。

视图设计：支持基于可视化设计器构建资源拓扑关系视图，并支持根据资源性能指标设置光晕渲染效果，支持交互动作的设置。视图支持部件自由摆放、叠加和层级设置，支持背景图、背景色、透明度的设置，支持光晕、闪烁、火焰、涟漪、闪烁渲染效果。

视图编辑：支持将视图保存为模板，可支持模板进行视图创建，支持通过ctrl+c、ctrl+v、delete快捷键进行部件复制、粘贴、删除，支持跨，支持全屏预览。支持键盘的快捷键复制、粘贴、删除部件，支持上、下、左、右方向键调整部件位置。支持视图的导入导出功能。支持窗口宽高比配置、保持宽高比等配置，满足设计的窗口适应各种尺寸屏幕的展示。

视图交互：支持视图的下钻交互到其他图表或子视图；图表支持动效变化，当新数据变化时，图表动效展现变化；支持视图内数据支持联动，当选择图表组件数据时，视图内其他组件的相关会产生联动选择效果。支持的交互行为包括单击、双击、悬浮、右键等交互操作。

## 安全态势感知平台及流量探针

### 区级态势感知平台

|  |  |  |
| --- | --- | --- |
| 功能参数 | 功能及技术指标 | 参数要求 |
| 软件 | 接口开发 | ▲所投安全态势感知产品需要开放API等接口，并承诺可采集展现所投安全设备的各类数据，原厂商提供承诺函并盖公章 |
| 兼容性 | 响应联动要求 | ▲本管理软件要求与所投防火墙联动，实现阻断非法接入流量等功能（提供相关功能截图并盖章） |
| 硬件要求 | 硬件性能 | 架构要求：软件+通用X86服务器硬件，可以灵活调整服务器硬件配置 |
| 实配内存≥96G，可用扩展插槽≥18个 |
| 实配硬盘≥ 2\*600G SAS盘+ 2\*4TSATA盘 ≥10个硬盘插槽可用 |
| 配置独立Raid卡（2G缓存） |
| 标配1个mLOM 4\*GE（电） |
| 1个USB3.0，2个USB2.0 |
| 性能要求 | 性能要求 | 日志源接入数量为≥512个 事件入库性能≥4000条/秒 |
| 流量探针 | 硬件要求 | 至少需要固化千兆电口≥16，千兆光口≥2，支持万兆端口扩展，扩展插槽≥2，配置500G硬盘 |
| 性能要求 | 吞吐量≥5G 并发连接数≥120万 每秒新建连接数≥7万/秒 |
| 整网态势展示 | 综合态势 | 1.支持全网安全风险监控展示，包括但不限于安全度打分，资产和用户安全状态分布统计，攻击阶段分布统计，安全事件统计，TOP5风险资产，TOP5风险用户，综合报表统计（提供产品截图或者证明材料） 2.支持按天周月展示安全事件的攻击阶段分布、安全事件类型分布和周期性综合安全分析报告 3.支持自定义展示图表设置，可选择展示的内容，包括可选资产安全信息、用户安全信息、安全事件信息、综合报告和安全度最低分设置 4.支持根据不同区域进行呈现，事先根据网段或者部门区域定义，在首页可以直接选取不同区域进行相关安全状况展示 5.支持在首页主动威胁探测查询，可使用IP/URL/资产名称/域名进行快速风险明细查询（提供产品截图或者证明材料） |
| 外网攻击态势 | 支持实时监测外网对内部资产发起的攻击情况，包括但不限于总攻击数、总漏洞利用攻击数、总僵木蠕攻击数、未拦截攻击数、未拦截漏洞利用、未拦截僵木蠕、国内外攻击源IP排名、攻击目的资产排名、攻击目的端口与协议分布、漏洞利用攻击分布、攻击类型分布、僵木蠕攻击类型分布、实时对攻击事件进行滚动告警 |
| 整网威胁态势 | 支持实时监测整网遭受的威胁情况，包括但不限于展示当前存在的安全事件数、攻击源排名、实时威胁事件列表、事件攻击阶段分布、TOP5风险资产、威胁事件的排名（提供产品截图或者证明材料） |
| 用户安全评估 | 风险用户 | 支持按照已失陷、高危、低危、影响内网、影响外网统计风险用户的数量，并且能够列表展示风险用户的明细 |
| 用户画像 | 1.支持对风险终端用户进行分析，确定用户风险状态，展示风险用户用户名称、IP、所在区域、当前安全状态 2.支持展示风险终端用户遭受的安全事件的攻击阶段分布统计 3.支持展示风险终端用户30天内发生的安全事情趋势 4.支持以列表的形式展示风险资产遭受的安全事件详情，包括但不限于展示事件首次发生事件、最近发生时间、事件名称、事件描述、事件等级、事件关注点、源IP、目的IP、攻击阶段、失陷状态、情报IOC、攻击载荷等信息，不低于30个标签子项（提供产品截图或者证明材料） |
| 安全事件分析 | 扫描侦查类 | 支持主机扫描、端口扫描、网络拓扑扫描、应用扫描、操作系统扫描、数据库扫描、其他扫描、、敏感信息泄露等安全事件分析 |
| 漏洞利用类 | 支持溢出、内存破坏、代码执行、SQL注入、命令注入、文件包含、非信任路径搜索、文件上传、目录遍历、安全措施绕过、使用已知漏洞组件、CGI漏洞、不安全方法调用、跨站请求伪造、跨站脚本攻击、XPATH注入、LDAP注入、系统漏洞、应用漏洞、ICMP漏洞、SMTP漏洞、HTTP漏洞、SSL漏洞、TFTP漏洞、SMB漏洞、SSH漏洞、SNMP漏洞、DNS漏洞、POP漏洞、TELNET漏洞等安全事件分析 |
| 恶意文件类 | 支持感染型病毒、木马、蠕虫、僵尸网络、间谍软件、广告软件、勒索软件、后门、其他恶意软件、风险软件、垃圾文件、灰色软件、测试文件、黑客工具、钓鱼软件、Rootkit、恶意脚本文件、宏病毒、挖矿软件、Webshell、ShellCode等安全事件分析 |
| 权限获取类 | 支持本地提权、未授权访问、暴力破解、远程提权、其他提权控制等安全事件分析 |
| 恶意通信类 | 支持恶意主机通信、恶意邮件通信、恶意域名请求、C&C主机通信、挖矿程序通信、木马程序通信、勒索程序通信、后门程序通信、病毒程序通信、僵尸网络通信、钓鱼程序通信、蠕虫传播、ShellCode通信、WebShell通信、隐蔽隧道、反弹Shell、其他恶意程序通信等安全事件分析 |
| 数据泄露类 | 支持文件传输、数据传输等安全事件分析 |
| 攻击还原和取证 | 攻击阶段还原 | 1.支持对风险资产和风险用户按照扫描侦察、入侵、命令控制、横向渗透、网络黑产、数据盗取、系统破坏攻击链，显示整网安全事件所处的攻击阶段 2.支持显示每个阶段的安全事件数量，并且能够下钻显示安全事件明细 |
| 攻击取证溯源 | 1.支持对风险资产和风险用户遭受的安全事件进行溯源，以路径的形式表现威胁过程 2.支持对导致资产失陷的安全事件进行深度分析提取攻击载荷等信息 3.支持根据分析的安全事件结果手动联动本地流量探针或IPS设备抓包取证 4.支持识别网关设备的NAT日志，能够溯源原始攻击者和被感染安全事件的真实主机的IP地址 |
| 响应联动 | 安全设备响应联动 | 支持根据安全事件结果，手动/自动联动同品牌FW设备或者IPS设备，进行黑名单的下发和阻断策略的配置，并能够在FW设备或IPS设备上策略下发成功（提供产品截图或者证明材料） |
| 告警管理 | 告警策略 | 1.支持以邮件、短信方式进行告警 2.支持预定义告警模板与自定义告警内容 3.支持在一定时间内最多发送最大通知条数，超出最大条数则合并到下一个时间间隔发送告警方式控制的设置 |
| 告警记录 | 1.支持按照时间以列表形式展示已生成的告警结果，包括发送时间、告警策略名称、告警方式、收件人 2.支持按照时间段对告警记录进行查询； 3.支持按照告警方式、策略名称 4.支持对告警记录进行删除与清空 |
| 工单下发 | 支持以预置处置建议形式派发工单，支持工单流转状态跟踪，完成安全事件闭环处理，同时还能通过邮件进行派发及时通知相关责任人 |
| 异常流量分析 |  | 1.支持展示通过网络原始流量分析异常流量事件数量，包括异常流量事件总数、高危事件总数、中危事件总数、低危事件总数 2.支持统计异常流量事件类型分布，支持统计异常流量事件威胁度分布，支持按照资产与用户展示TOP10异常流量事件排名 3.支持以列表形式展示异常流量事件详情，包括IP、高危数、中危数、低危数、异常类型、异常总数 4.支持展示异常流量事件趋势 |
| 全局配置 | 平台自身访问管理 | 支持设置IP、IP段对平台的访问进行管理控制 |
| 数据清理设置 | 支持按照硬盘空间阈值百分比和时间阈值保存天数自动进行数据清理 |
| 系统参数配置 | 支持系统参数的设置，支持配置用户限制超时时间、登录失败锁定时间、允许登录失败次数、相同用户可同时登录、浏览器记录登录用户名\密码、漏洞导入统计阈值、Web网管登录协议\端口号等 |
| 系统监控管理 | 1.支持平台硬件系统的CPU使用率、内存使用率、系统区和数据区的磁盘使用率监控，能够按照策略进行系统告警 2.支持系统各组件服务和平台的各个节点进行CPU使用率、内存使用率的监控，能够按照策略进行系统告警 |
| 威胁情报管理 | 威胁情报配置 | 1.支持IP/URL威胁情报的在线升级、离线升级（导入情报）操作； 2.支持基于IP/URL地址的情报查询，支持列表展示IP/URL情报的详细信息；主要包括IP、分类、方向、热度值（事件发生次数）、可靠度、危害等级、开始时间、结束时间等； 3.支持自定义IP/URL情报的新增、删除、修改、导入、启用、停用等； 4.支持列表展示自定义IP/URL情报的详细信息，主要包括IP/URL、分类、方向、热度值（事件发生次数）、可靠度、危害等级、启用状态等； |
| 系统管理 | 分区分域管理 | 1.支持对用户网络进行区域划分，满足用户层级管理需求 2.支持一个父区域下最多可嵌套4层子区域 3.支持按照不同区域展示安全事件分析结果 4.支持本地用户绑定区域，各区域的管理员只能看所属区域的安全事件、流量、行为、资产、业务 |
| 资产管理 | 支持同品牌网络运维管理平台对接，形成运维管理与安全管理一体化的能力 |
| 1.支持资产自动发现，包括通过原始流量、安全日志自动发现网络资产和漏动扫描设备的扫描结果发现网络资产 2.支持对资产的手动增删改查和导入导出管理 3.支持对资产的性能值CPU、内存的利用率进行查看 4.支持对资产责任人进行分配和管理 5.支持对资产模板参数（SNMP\Telnet\SSH\SOAP）进行管理 |

### 流量探针（态势感知社区子平台）

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 硬件要求 | 主机至少需要固化千兆电口≥16，千兆光口≥2，支持万兆端口扩展，扩展插槽≥2，配置≥500G硬盘 |
| 性能要求 | 吞吐量≥5G 并发连接数≥120万 每秒新建连接数≥7万/秒 |
|
|
|
| 安全应用 | 整机具有链路负载均衡、IPS、防病毒、Web应用、应用识别功能，配置相关授权 |
| 部署模式 | 实现路由模式、透明（网桥）模式、混合模式。 |
| 路由实现 | 实现静态路由、策略路由、RIP、OSPF、BGP等路由协议。 |
| NAT功能 | 实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 |
| VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 |
| 支持IPsec VPN隧道自动建立，无需流量触发； |
| 支持IPsec VPN智能选路，根据应用和隧道质量调度流量。 |
| 可基于每个SSL VPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。 |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 |
| 安全策略 | 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置 |
| 支持策略冗余分析， 冲突策略分析以及命中率统计。 |
| 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。 |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。 |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。 |
| 加密流量检测 | 支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项 |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能。 |
| 支持IPV6下的访问控制、IPSec VPN、DDoS防护等安全功能。 |
| 国密算法 | 支持国密SM2/3/4算法。 |
| 虚拟化能力 | 所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。 |
|
| 支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。 |
| 设备管理 | 支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。 |
| 为了保证整个网络的可靠稳定，要求本次采购的安全设备支持A/S，A/A方式部署，支持配置同步，会话同步和用户状态同步； |
| 提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |

# 项目实施组织及进度安排要求

## 项目实施组织

投标人应本着认真负责态度，组织技术队伍，认真做好项目的实施工作。在签订合同前，提出具体实施、服务、维护以及今后技术支持的措施计划和承诺。投标人必须提供项目实施计划，经招标人同意后，严格执行。如果遇到问题，由项目组提出项目变更说明， 经招标人和系统提供商确定后，修改计划。投标人应负责在项目验收时将系统的全部有关技术文件、资料、安装、测试、验收报告等文档汇集成册交付招标人。 结合实际情况，拟定详细的系统实施计划，包括同医院现有信息系统的对接、个性化化定制、测试、试运行、培训及上线计划。承诺保证软硬件系统在合同规定时间内上线及上线后系统平稳运行。

### 项目管理要求

1. 项目管理首先要建立管理的原则，组织，协调机制和实施办法。投标方必须提供实施本项目的完整的项目管理方案，并在项目建设过程中严格执行。
2. 项目计划的制定和执行要体现安全等保加固建设类项目的特点。
3. 必须高度重视对过程的管理控制，高度重视对各类文档的管理，必须建立中间环节和文档的内部测试审核制度。
4. 在项目管理方案中，应充分体现投标方在项目管理方面的经验和能力以及对该项目管理的设想和具体方法，以下内容必须涉及：
5. 项目经理，项目组成员及项目组织结构。
6. 项目组成员除基本信息外，必须说明专业背景,相关资质和专长；
7. 组织管理(与系统集成相关)；
8. 项目计划(与项目整体管理相关)；
9. 文档清单，文档资料提交计划和文档质量控制办法；
10. 质量控制办法；
11. 项目需求变更控制和进度控制办法。
12. 投标人应保持项目团队稳定。未经用户方同意，项目经理在项目整体验收前不得变更；项目实施全过程中，项目经理应保证每月在本项目现场工作时间不得少于60%；项目团队成员变更不得大于30%，且须经用户方同意。

### 项目人员要求

为保证项目顺利实施，投标人在项目实施期间须提供现场不少于8人的项目实施团队，在投标书中提供书面名单，提供项目组成员姓名、其相关资质、在本项目中的职责及以前参与过的项目情况说明等，并提供对应的社保证明。

为保证后续安全服务质量，确保安全服务能够适应等保2.0要求，帮助用户梳理网络安全制度、建立安全管理体系、提高安全设备利用效率，切实做到防御重大信息安全危机，及时处理信息安全事件，提升青浦卫生健康系统信息安全能力，要求投标单位就本项目派遣2名或以上具有相关经验的驻场运维工程师，为期一年，驻场时间从项目正式验收之后起算，投标文件内需提供2名或以上驻场运维工程师名单、身份证、联系方式以及简要的运维服务经验。

投标人应提供项目经理个人简历和项目团队成员名单，且应提供本地化服务。项目团队成员应具有相应技能证书如CSIP等，项目经理应具有高级项目经理等相关证书。

项目建设期间，项目团队成员应常驻上海本地，业主方有权要求全部或部分项目成员工作日常驻业主方现场开展工作。

## 项目进度要求

本项目需在合同签订后60个日历日完成项目建设工作。投标供应商应在投标书中提供项目实施计划，并在中标后根据项目实施情况进行必要的调整，保障项目在要求时间内完成。

## 项目验收要求

1. 建设内容完成后，中标方应对相关建设内容进行完善的系统测试，并通知用户方进入系统试运行期。系统试运行为期一个月，与此同时中标方提供试运行期系统测试文档和项目验收相关文档，并且对用户方相关人员提供完善的培训。
2. 中标方完成建设内容之后，需要保证卫健委中心端和11个社区卫生服务中心都取得具备资质的等保测评机构出具的三级等保测评报告，作为验收条件之一。
3. 中标方提供全套完善的项目验收资料文档，包括配置文档、使用说明书给用户，并想用户书面提出申请项目验收，用户方在审查验收资料无误后同意召开项目验收会。
4. 由用户指定时间地点并邀请相关专家参加项目验收会，就项目建设内容依据验收资料文档等进行项目验收，并出具专家验收意见书作为项目验收的结论性文件。
5. 项目进入运维保障期，中标方持续提供招标文件要求的售后服务及设备保修服务。

# 安全文明施工

## 安全防护

1. 在工程施工、竣工、交付及修补任何缺陷的过程中，中标供应商应当始终遵守国家和上海市有关安全生产的法律、法规、规范、标准和规程等，按照合同条款的约定履行其安全施工职责。
2. 中标供应商应坚持“安全第一，预防为主”的方针，建立、健全安全生产责任制度和安全生产教育培训制度。在整个工程施工期间，中标供应商应在现场设立、提供和维护并在有关工作完成或竣工后撤除：
3. 设立在现场入口显著位置的现场施工总平面图、总平面管理、安全生产、文明施工、环境保护、质量控制、材料管理等的规章制度和主要参建单位名称和工程概况等说明的图板；
4. 为确保工程安全施工须设立的足够的标志、宣传画、标语、指示牌、警告牌、火警、匪警和急救电话提示牌等；
5. 洞口和临边位置的安全防护设施，包括护身栏杆、脚手架、洞口盖板和加筋、竖井防护栏杆、防护棚、防护网、坡道等；
6. 安全带、安全绳、安全帽、安全网、绝缘鞋、绝缘手套、防护口罩和防护衣等安全生产用品；
7. 所有机械设备包括各类电动工具的安全保护和接地装置和操作说明；
8. 主要作业场所和临时安全疏散通道24 小时36 伏安全照明和必要的警示等以防止各种可能的事故；

## 劳动保护

1. 中标供应商应遵守所有适用于本合同的劳动法规及其他有关法律、法规、规章和规定中关于工人工资标准、劳动时间和劳动条件的规定，合理安排现场作业人员的劳动和休息时间，保障劳动者必须的休息时间，支付合理的报酬和费用。中标供应商应按有关行政管理部门的规定为本合同下雇佣的职员和工人办理任何必要的证件、许可、保险和注册等，并保障发包人免于因中标供应商不能依照或完全依照上述所有法律、法规、规章和规定等可能给发包人带来的任何处罚、索赔、损失和损害等。
2. 中标供应商应按照国家《中华人民共和国劳动保护法》的规定，保障现场施工人员的劳动安全。中标供应商应为本合同下雇佣的职员和工人提供适当和充分的劳动保护，包括但不限于安全防护、防寒、防雨、防尘、绝缘保护、常用药品、急救设备、传染病预防等。
3. 中标供应商应为其履行本合同所雇佣的职员和工人提供和维护任何必要的膳宿条件和生活环境，包括但不限于宿舍、围栏、供水(饮用及其他目的用水)、供电、卫生设备、食堂及炊具、防火及灭火设备、供热、家具及其他正常膳宿条件和生活环境所需的必需品，并应考虑宗教和民族习惯。

## 安全措施

中标供应商应根据《中华人民共和国安全生产法》、《中华人民共和国消防法》、《中华人民共和国道路交通安全法》、《中华人民共和国传染病防治法实施办法》、《职业健康安全管理体系规范》（GB/T 28000）和地方有关的法规等，编制一份施工安全措施计划，报送工程师审批。

施工安全措施计划是中标供应商阐明其安全管理方针、管理体系、安全制度和安全措施等的文件，其内容应当反映现行法律法规规定的和合同条款约定的以及本条上述约定的中标供应商安全职责，包括但不限于：

1. 施工安全管理机构的设置；
2. 专职安全管理人员的配备；
3. 安全责任制度和管理措施；
4. 安全教育和培训制度及管理措施；
5. 各项安全生产规章制度和操作规程；
6. 各项施工安全措施和防护措施；
7. 危险品管理和使用制度；
8. 安全设施、设备、器材和劳动保护用品的配置；

## 文明施工

1. 中标供应商应遵守国家和工程所在地有关法规、规范、规程和标准的规定，履行文明施工义务，确保文明施工专项费用专款专用。
2. 中标供应商应当规范现场施工秩序，实行标准化管理：
3. 中标供应商的现场必须干净整治、做到无积水、无淤泥、无杂物，材料堆放整齐；
4. 现场应进行硬化处理，定期定时洒水，做好防治扬尘和大气污染工作；
5. 严格遵守“工完、料尽、场地净”的原则，不留垃圾、不留剩余施工材料和施工机具，各种设备运转正常；
6. 中标供应商修建的施工临时设施应符合工程师批准的施工规划要求，并应满足本节规定的各项安全要求；
7. 工程师可要求中标供应商在现场设置各级中标供应商的安全文明施工责任牌等文明施工警示牌；
8. 材料进入现场应按指定位置堆放整齐，不得影响现场施工或堵塞施工、消防通道。材料堆放场地应有专职的管理人员；
9. 施工和安装用的各种扣件、紧固件、绳索具、小型配件、镙钉等应在专设的仓库内装箱放置；
10. 现场风、水管及照明电线的布置应安全、合理、规范、有序，做到整齐美观。不得随意架设，造成隐患或影响施工。

# 产品供货要求

投标人提供的产品应符合开放性标准，并能与满足这样标准的产品集成。

中标方将其供货设备运送到采购人指定现场时应包装完好、数量与供货清单相符。中标方提供的产品送货 到采购人指定现场后，应该会同采购人和采购人认可的有关第三方（监理），进行开箱点货验收。点货验收前，中标方须提供完整清晰的供货清单。点货验收后，三方签字确认，并将货物的保管权移交给采购人。

采购人在保管期内只对货物的数量和外观原状负责。中标方负责组织原产品制造厂家的合格的技术人员或由原产品制造厂家直接授权的有资格的技术人员完 成供货产品的安装、测试和安装验收以及终验，并解决此过程中出现的有关问题和提供项目与技术服务。

按照采购人指定的时间，采购人、中标方和采购人认可的有关第三方在设备安装现场共同进行设备开箱和安装验收。 中标方提供的产品若具有固有的设计缺陷，则不能因超过质保期而解除中标方对该设备应承担的修复和更换责任。

中标方和原产品制造厂家有义务向采购人主动提供合同供货范围内的软件升级和修补版本，并协助采购人进行软件更新。如果升级版本超过合同规定的免费升级范围，则采购人有权选择是否进行升级。如果该软 件具有固有缺陷，则修复这种缺陷是中标方不可推卸的责任和义务。

# 技术培训要求

1. 投标单位须提供所需的培训设施和课程，以确保甲方人员能对投标单位所提供的系统、设备和装置的设计、日常的运作、故障和例行维护、事故的处理和解决方面等有全面性的认识和了解。
2. 培训应于卫健委中心和11个社区服务中心分别进行。投标单位须预先编制1套详尽的培训计划，列出每项课程的大纲、培训导师资料及培训所需时间，提交甲方审核。
3. 投标单位须委派施工项目经理进行每项培训工作，培训需以普通话作讲授。所有导师的资历须先提交甲方作审核认可。
4. 投标单位应向受训学员提供并解释有关设计资料、文件、图纸等，以便使学员对整套系统的各个方面都能熟练掌握。
5. 投标单位经得甲方同意可以利用已安装﹑测试和交工试运转的装置和设备对甲方人员进行培训。投标单位应提供足够的材料、设备、样本、模型、设备内部透视资料的复印本、幻灯、影片以及其它种种需要的培训教材文件，以便培训工作的进行。培训课程完成后，有关装备和教材将为甲方所有，以便日后甲方自行对其它员工进行辅助性培训之用。所有教材文件须以中文说明。
6. 上述培训所需的费用应包括在投标单位的投标价内。

# 售后服务及保修服务要求

## 整体运维服务

**硬件原厂保修3年，软件质保1年，整体运维服务一年**。投标人应设立常驻售后服务机构和软件开发中心，在接到报修电话通知后1小时内响应；2 小时内赶到现场处理故障，使系统恢复正常。免费期内对系统优化和常规安全检查。每年提供4次设备巡检服务。投标人应提供中文电话免费咨询服务。投标人负责所供软件及配套产品的售后服务，包括提供所供产品技术咨询、技术培训、到货验收、安装调 试以及负责所供产品的保修及其它售后技术服务。在质保期结束前，须由投标人工程师和招标人代表进行一次全面检查，任何缺陷必须由投标人负责修理，在修理之后，投标人应将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给买方，报告一式两份。

## 原厂保修服务

1. 所有硬件设备提供三年原厂保修，从到货之日起算
2. 所有软件开发系统提供一年免费升级服务和系统运行保障服务，从项目验收之日起算
3. 所有安全设备相关病毒库、特征库等提供三年免费升级更新服务，从到货之日起算
4. 提供原厂关于投标设备的质量保证承诺函

## 驻场运维服务

1. 驻场响应时间为每周5\*8小时，驻场运维人员负责本次项目建设范围内的安全设备维保、三级等保相关文档整理、三级等保需要的漏洞扫描和补丁升级等工作。并且对安全事件作出快速反应并在采购人要求时间内处理完成。
2. 投标单位针对本项目派遣2名或以上驻场运维工程师保障安全系统正常运行，从项目验收之后起为期一年。提供响应该服务的承诺函。
3. 2名或以上驻场运维人员资质要求：至少具备CISP、HCIE、RHCE等资质证书中的一种，并提供相关简历。

## 备品备件服务

1. 投标人提供相关备品备件清单及价格
2. 投标人需在主设备发生故障并且无法修复的情况下在24小时之内提供备品备件并恢复业务正常运行。

**包件三：社区卫生服务中心医疗付费“一件事”等应用改造升级项目需求**

# 项目建设概况

## 建设背景

为贯彻落实国务院“互联网+医疗健康”战略，响应市委、市政府“一网通办”号召，大力推进业务流程革命性再造，根据《2020年上海市深化“一网通办”改革工作要点》《上海市人民政府关于以企业和群众高效办成“一件事”为目标全面推进业务流程革命性再造的指导意见》等要求，经医疗付费“一件事”工作专班研究，现就业务流程优化再造工作提出该项目建设。

## 建设目标

根据《医疗付费“一件事”业务流程优化再造工作方案》要求，本方案分为“上海市医保中心系统与医院系统接口(第5版)对接”、“基于信用的无感支付”、“就医服务入驻随申办”和“医院电子票据服务优化”四部分，共同推进医疗付费“一件事”方案的实行。面向患者提供基于信用的无感支付、便捷的电子票据服务，以及医保患者基于医保电子凭证的实名认证。

1. 上海市医保中心系统与医院系统接口(第5版)对接

根据上海市医疗保险事业管理中心于2020年4月发布《中心系统与定点医疗机构接口规范（第 5 版试行）》对现有的医院系统接口标准进行细化调整及升级，进一步完善结算审核计算机管理系统，对现有的医保结算系统进行线上线下一体化的升级改造，为医保患者优化支付流程奠定基础。

1. 基于信用的无感支付

依托市大数据中心“随申办”统一平台能力，作为医疗付费“一件事”的总入口，实现不同场景的“基于信用无感支付”服务，提升患者付费业务的便捷性和效率，打造上海市的信用就医新型服务体系。

1. 就医服务入驻随申办

为医院在随申办APP医疗板块中提供预约挂号、门诊缴费和在线复诊等功能，并与医院现有的信息系统进行深度对接，帮助医院构建完整的全面的互联网医疗服务体系和流程闭环，通过此举为居民提供统一的互联网医疗服务入口。

1. 医保数据上传V1.0接口对接

调试与医保V1.0接口对接，完成病案首页信息、处方信息、医嘱信息、检验检查信息等数据上传。

## 建设内容

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **大类** | **系统** | **功能模块** |
| 1 | 医保五期接口及医疗付费“一件事”应用开发 | 医保五期接口开发 | 医保五期接口开发、HIS系统改造、村医系统改造升级 |
| 2 | 医疗付费“一件事”开发 | 诊间支付、线上支付 |
| 3 | 医保数据上传应用开发 | 医保数据上传 | （根据上海市医疗服务信息上报工作要求，包括不仅限于以下模块）上传基础模块、病案首页信息、住院非医保实时患者交易明细数据、出院小结信息、住院医嘱信息、门诊非医保实时病人交易明细数据、门诊处方信息、实验室检验报告、医学影像检查报告、录入病案首页信息及相关内容 |

## 建设周期

项目5个月内完成。

# 建设现状

青浦区内现有社区卫生服务中心11家，医保线路接入点21个，村卫生室201家，都开展了医疗服务和医保结算服务。目前各医院都上线了医保四期，除了夏阳街道社区卫生服务中心外，都未上线移动支付。

从业务覆盖的角度来看，医院现有系统基本能够支持门诊、住院、医技、运营各科室级日常工作，对于涉及跨部门业务协作，信息集成、系统集成的问题，也逐步通过医院信息平台来实现相关信息的调阅。我院相关信息系统的建设已基本满足临床需求。

在信息化建设的过程当中，各医院持续探索、积极改善患者就医付费排队体验，致力于付费流程的优化，通过开设自助服务一体机、增开支持扫码支付的收费服务柜台窗口等方式，从一定程度上提升群众就医付费便捷程度，各大医疗机构排队状况得到初步缓解，但距离群众期望还有较大差距。因此，各医院希望通过本次医疗付费“一件事”医保相关改造项目，旨在实现以下目标：

面向患者，解决在传统医疗服务流程中，付费业务被动化，排队等待耗时较长、排队次数较多、办事不够集约高效的问题，打造一项具有“高显示度、高集中度、高感受度”的数字惠民新应用，进一步优化患者诊疗流程，提升患者就医体验；

面向医院，根据上海市医疗保险事业管理中心于2020年4月发布的《中心系统与定点医疗机构接口规范（第 5 版试行）》，对现有的医院系统接口标准进行细化调整及升级，进一步完善结算审核计算机管理系统，对现有的医保结算系统进行线上线下一体化的升级改造，完善医保结算信息的对账模式；

已有项目是拟建项目的基础。拟建医疗付费“一件事”医保相关改造项目基于现有HIS、医生站、病案系统及医技系统实现：“与上海市医保中心系统对接”、“基于信用的无感支付”、“就医服务入驻随申办”。本次拟建项目将在保证现有系统稳定运行的基础上确保其延续性。

拟建项目是已有系统的延续和深化。拟建设项目是在已有系统的基础上按照上海市医疗服务信息上报工作要求，完成相关数据上传。同时，通过“基于信用的无感支付”、“就医服务入驻随申办”建设，打造一项具有“高显示度、高集中度、高感受度”的数字惠民新应用，进一步优化患者诊疗流程，提升患者就医体验。

# 项目建设需求

## 3.1总体要求

### 3.1.1 基本要求

投标人本着认真负责态度，组织技术队伍，认真做好项目的实施工作。在签订合同前，提出具体实施、服务、维护以及今后技术支持的措施计划和承诺。

投标人提供项目实施计划，经用户方同意后，严格执行。如遇到问题，由项目组提出项目变更说明，经用户方和系统提供商确定后，修改计划。

投标人负责在项目验收时将系统的全部有关技术文件、资料、及安装、测试、验收报告等文档汇集成册交付用户方。

结合实际情况，拟定详细的系统实施计划，包括安装、调试、试运行、验收等内容。

### 3.1.2总体架构要求

针对本项目建设，投标人需遵循“总体设计，按需驱动，分步建设”的原则，依托现有青浦区区域卫生信息平台基础，基于数据标准规范对总体架构进行合理设计，确保平台总体架构设计的合理性和可拓展性，以支撑按需驱动阶段建设及将来业务的扩展。

### 3.1.3标准规范建设

标准化建设，是卫生信息化建设的基础工作，也是进行信息交换与共享的基本前提，本项目建设需遵循“统一规范、统一代码、统一接口”的原则。

## 3.2性能及管理要求

系统稳定性：要求系统能够稳定可靠，保证7×24小时的不间断运行，年平均宕机时间小于4小时。

可管理性，提供管理工具帮助管理人员系统全面地监控、管理和配置，并为系统故障的判断、排错和分析提供支撑。

系统具有运行日志，记录系统的使用情况、运行状况，能够保留故障现场。

系统的软件体系结构应具有充分的可扩展性，系统具有统一的用户界面，设置灵活，适应性强。

## 3.3建设规模

本项目建设涉及青浦区内现有社区卫生服务中心11家，医保线路接入点21个。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 单位名称 | 医保接入点数量 | 备注 | 村卫生室 | 站点 |
| 1 | 青浦区金泽镇社区卫生服务中心 | 4 | 3个分中心 | 39家 |  |
| 2 | 青浦区练塘镇社区卫生服务中心 | 3 | 2个分中心 | 44家 |  |
| 3 | 青浦区朱家角镇社区卫生服务中心 | 2 | 1个分中心 | 20家 | 2个 |
| 4 | 青浦区盈浦街道社区卫生服务中心 | 1 |  | 2家 | 6个 |
| 5 | 青浦区夏阳街道社区卫生服务中心 | 1 |  | 8家 | 8个 |
| 6 | 青浦区香花桥街道社区卫生服务中心 | 2 | 1个分中心 | 13家 | 2个 |
| 7 | 青浦区白鹤镇社区卫生服务中心 | 2 | 1个分中心 | 23家 | 1个 |
| 8 | 青浦区华新镇社区卫生服务中心 | 3 | 2个分中心 | 19家 |  |
| 9 | 青浦区徐泾镇社区卫生服务中心 | 1 |  | 13家 |  |
| 10 | 青浦区重固镇社区卫生服务中心 | 1 |  | 10家 |  |
| 11 | 青浦区赵巷镇社区卫生服务中心 | 1 |  | 9家 | 1个 |
| 合计 |  | 21 |  |  |  |

具体建设地址如下：

1. 白鹤镇社区卫生服务中心（地址：上海市青浦区白鹤镇外青松公路2961号）
2. 白鹤镇社区卫生服务中心赵屯卫生服务分中心(地址：上海市青浦区白鹤镇赵屯村新赵路1号罗浦)
3. 白鹤镇白虬江站点（地址：上海市青浦区白虬江路252号）
4. 白鹤镇杜村卫生室（地址：上海市青浦区白鹤镇杜村卫生室）
5. 白鹤镇胥沟村卫生室（地址：上海市青浦区白鹤镇胥沟村卫生室）
6. 白鹤镇鹤联村中心卫生室（地址：上海市青浦区白鹤镇鹤联村中心卫生室）
7. 白鹤镇红旗村中心卫生室（地址：上海市青浦区白鹤镇红旗村中心卫生室）
8. 白鹤镇江南村卫生室（地址：上海市青浦区白鹤镇江南村卫生室）
9. 白鹤镇金项村中心卫生室（地址：上海市青浦区白鹤镇金项村中心卫生室）
10. 白鹤镇梅桥村卫生室（地址：上海市青浦区白鹤镇梅桥村卫生室）
11. 白鹤镇南巷村卫生室（地址：上海市青浦区白鹤镇南巷村卫生室）
12. 白鹤镇青龙村卫生室（地址：上海市青浦区白鹤镇青龙村卫生室）
13. 白鹤镇沈联村卫生室（地址：上海市青浦区白鹤镇沈联村卫生室）
14. 白鹤镇胜新村中心卫生室（地址：上海市青浦区白鹤镇胜新村中心卫生室）
15. 白鹤镇曙光村卫生室（地址：上海市青浦区白鹤镇曙光村卫生室）
16. 白鹤镇太平村卫生室（地址：上海市青浦区白鹤镇太平村卫生室）
17. 白鹤镇陈岳村卫生室（地址：上海市青浦区白鹤镇陈岳村卫生室）
18. 白鹤镇塘湾村卫生室（地址：上海市青浦区白鹤镇塘湾村卫生室）
19. 白鹤镇万狮村卫生室（地址：上海市青浦区白鹤镇万狮村卫生室）
20. 白鹤镇王泾村中心卫生室（地址：上海市青浦区白鹤镇王泾村中心卫生室）
21. 白鹤镇五里村卫生室（地址：上海市青浦区白鹤镇五里村卫生室）
22. 白鹤镇响新村卫生室（地址：上海市青浦区白鹤镇响新村卫生室）
23. 白鹤镇新江村卫生室（地址：上海市青浦区白鹤镇新江村卫生室）
24. 白鹤镇赵屯村中心卫生室（地址：上海市青浦区白鹤镇赵屯村中心卫生室）
25. 白鹤镇朱浦村中心卫生室（地址：上海市青浦区白鹤镇朱浦村中心卫生室）
26. 白鹤镇朱家村卫生室（地址：上海市青浦区白鹤镇白虬江路252号）
27. 华新镇社区卫生服务中心（地址：上海市青浦区华新镇华志路800号）
28. 华新镇凤溪社区卫生服务分中心（地址：上海市青浦区华新镇凤溪镇凤星路1520号）
29. 华新镇社区卫生服务分中心凤阁分中心（地址：上海市青浦区华新镇风强塘路与凤阁路交叉口东北100米）
30. 华新镇社区卫生服务中心叙南村卫生室（地址：上海市青浦区华新镇叙南村村委）
31. 华新镇社区卫生服务中心嵩山村中心卫生室（地址：上海市青浦区华新镇北青公路3488号）
32. 华新镇社区卫生服务中心凌家村中心卫生室（地址：上海市青浦区华新镇凌家村8号）
33. 华新镇社区卫生服务中心新木桥村卫生室（地址：上海市青浦区华新镇新木桥村村委）
34. 华新镇社区卫生服务中心白马塘村中心卫生室（地址：上海市青浦区华新镇白马塘村村委）
35. 华新镇社区卫生服务中心坚强村中心卫生室（地址：上海市青浦区华新镇坚强村村委）
36. 华新镇社区卫生服务中心秀龙村卫生室（地址：上海市青浦区华新镇徐华公路3728号）
37. 华新镇社区卫生服务中心陆象村中心卫生室（地址：上海市青浦区华新镇凤北路839号）
38. 华新镇社区卫生服务中心周浜村卫生室（地址：上海市青浦区嘉松中路1589号时奕大厦底楼）
39. 华新镇社区卫生服务中心徐谢村中心卫生室（地址：上海市青浦区华新镇徐谢村徐大桥）
40. 华新镇社区卫生服务中心华益村卫生室（地址：上海市青浦区华新镇华纪路189弄98号）
41. 华新镇社区卫生服务中心新谊村卫生室（地址：上海市青浦区华新镇新谊村中宅）
42. 华新镇社区卫生服务中心朱长村卫生室（地址：上海市青浦区华新镇华南路1号）
43. 华新镇社区卫生服务中心北新村卫生室（地址：上海市青浦区华新镇北新村新联路102号南侧）
44. 华新镇社区卫生服务中心杨家庄村中心卫生室（地址：上海市青浦区华新镇嘉松中路4188弄198号）
45. 华新镇社区卫生服务中心淮海村中心卫生室（地址：上海市青浦区华新镇华丹路1009号）
46. 华新镇社区卫生服务中心火星村中心卫生室（地址：上海市青浦区华新镇火星村村委）
47. 华新镇社区卫生服务中心镇叙中村中心卫生室（地址：上海市青浦区华新镇叙中村村委）
48. 华新镇社区卫生服务中心马阳村卫生室（地址：上海市青浦区华新镇纪鹤路3839号）
49. 金泽镇社区卫生服务中心（地址：上海市青浦区培育路271号）
50. 金泽镇社区卫生服务中心西岑分中心（地址：上海市青浦区金泽镇练西公路4152号）
51. 金泽镇社区卫生服务中心商榻分中心（地址：上海市青浦区金泽镇商榻商蔡路84弄5号）
52. 金泽镇社区卫生服务中心连盛分中心（地址：上海市青浦区金泽镇练西公路2780号）
53. 金泽镇沙港村中心卫生室（地址：上海市青浦区金泽镇沙港村朝阳6号）
54. 金泽镇双祥村中心卫生室（地址：上海市青浦区金泽镇双祥村祥坞399号）
55. 金泽镇王港村王巷卫生室（地址：上海市青浦区金泽镇王港村王巷385号）
56. 金泽镇王港村港娄卫生室（地址：上海市青浦区金泽镇王港村港娄1444号）
57. 金泽镇淀西村东风卫生室（地址：上海市青浦区金泽镇淀西村东风435号东侧）
58. 金泽镇淀西村前荇卫生室（地址：上海市青浦区金泽镇商前路2028号西侧）
59. 金泽镇雪米村石米中心卫生室（地址：上海市青浦区金泽镇雪米村雪米路226号）
60. 金泽镇雪米村湖雪卫生室（地址：上海市青浦区金泽镇雪米村湖雪1166号东侧）
61. 金泽镇南新村中心卫生室（地址：上海市青浦区金泽镇南新村南车1号）
62. 金泽镇陈东村中心卫生室（地址：上海市青浦区金泽镇陈新路320号）
63. 金泽镇蔡浜村卫生室（地址：上海市青浦区金泽镇蔡浜村148号）
64. 金泽镇建国村卫生室（地址：上海市青浦区金泽镇建国村111号南侧）
65. 金泽镇金姚村卫生室（地址：上海市青浦区金泽镇金姚村750号）
66. 金泽镇杨湾村卫生室（地址：上海市青浦区金泽镇杨湾村团结115号西侧）
67. 金泽镇徐李村中心卫生（地址：上海市青浦区金泽镇金湖路51号）
68. 金泽镇新池村中心卫生室（地址：上海市青浦区金泽镇新杨路203号）
69. 金泽镇东西村卫生室（地址：上海市青浦区金泽镇东西村88号）
70. 金泽镇淀湖村陈港卫生室（地址：上海市青浦区金泽镇淀湖村陈港161号）
71. 金泽镇淀湖村西蔡中心卫生室（地址：上海市青浦区金泽镇淀湖村西蔡301号）
72. 金泽镇西岑村张联卫生室（地址：上海市青浦区金泽镇西岑村张联204号）
73. 金泽镇西岑村山深卫生室（地址：上海市青浦区金泽镇西岑村山深109号）
74. 金泽镇岑卜村卫生室（地址：上海市青浦区金泽镇岑卜村220号）
75. 金泽镇三塘村卫生室（地址：上海市青浦区金泽镇沪青平公路7811号）
76. 金泽镇河祝村中心卫生室（地址：上海市青浦区金泽镇河祝村65号）
77. 金泽镇育田村育坪卫生室（地址：上海市青浦区金泽镇育田村育坪318号北侧）
78. 金泽镇任屯村任屯中心卫生室（地址：上海市青浦区金泽镇任屯村112号）
79. 金泽镇任屯村北任卫生室（地址：上海市青浦区金泽镇任屯村北任3号）
80. 金泽镇田山庄村卫生室（地址：上海市青浦区金泽镇田山庄村115号）
81. 金泽镇钱盛村中心卫生室（地址：上海市青浦区金泽镇莲钱路198号）
82. 金泽镇龚都村港都卫生室（地址：上海市青浦区金泽镇龚都村港都1号）
83. 金泽镇龚都村龚潭卫生室（地址：上海市青浦区金泽镇龚都村龚潭2号东侧）
84. 金泽镇新港村尤浜卫生室（地址：上海市青浦区金泽镇新港村尤浜188号）
85. 金泽镇新港村杜赖卫生室（地址：上海市青浦区金泽镇新港村杜赖113号）
86. 金泽镇莲湖村谢庄中心卫生室（地址：上海市青浦区金泽镇莲湖村谢庄161号）
87. 金泽镇莲湖村朱舍卫生室（地址：上海市青浦区金泽镇莲湖村朱舍4号）
88. 金泽镇爱国村爱国中心卫生室（地址：上海市青浦区金泽镇爱国村莲爱路118号）
89. 金泽镇爱国村西宋卫生室（地址：上海市青浦区金泽镇爱国村西宋3号）
90. 金泽镇爱国村南洋卫生室（地址：上海市青浦区金泽镇爱国村南洋105号）
91. 金泽镇东天村卫生室（地址：上海市青浦区金泽镇东天村67号）
92. 练塘镇社区卫生服务中心（地址：上海市青浦区练塘镇朱枫公路3619号）
93. 练塘镇社区卫生服务中心小蒸卫生服务分中心（地址：上海市青浦区练塘镇小蒸社区蒸浦路356号）
94. 练塘镇双联村中心卫生室（地址：上海市青浦区练塘镇双联路1号）
95. 练塘镇东叙村卫生室（地址：上海市青浦区练塘镇东淇村东叙407号）
96. 练塘镇东淇村中心卫生室（地址：上海市青浦区练塘镇东淇村淇浒路158号）
97. 练塘镇东团村卫生室（地址：上海市青浦区练塘镇东厍村东团177号）
98. 练塘镇长塘村中心卫生室（地址：上海市青浦区练塘镇长塘路北）
99. 练塘镇三河村卫生室（地址：上海市青浦区练塘镇长河村三河176号）
100. 练塘镇新庄村卫生室（地址：上海市青浦区练塘镇大新村新庄222号）
101. 练塘镇大浜村中心卫生室（地址：上海青浦区练塘镇大新村大浜123号市）
102. 练塘镇徐南村中心卫生室（地址：上海市青浦区练塘镇朱枫公路5525号）
103. 练塘镇沈练村卫生室（地址：上海市青浦区练塘镇朱枫公路5232号）
104. 练塘镇张家浜村卫生室（地址：上海市青浦区练塘镇张家浜村村委）
105. 练塘镇钟联村卫生室（地址：上海市青浦区练塘镇张联村钟联173号）
106. 练塘镇泖口村卫生室（地址：上海市青浦区练塘镇练东村泖口248号）
107. 练塘镇王家村卫生室（地址：上海市青浦区练塘镇王家村28号）
108. 练塘镇东泖村卫生室（地址：上海市青浦区练塘镇东泖村沈陶路108号）
109. 练塘镇尤家泾村卫生室（地址：上海市青浦区练塘镇泾珠村尤家泾68号）
110. 练塘镇长珠村卫生室（地址：上海市青浦区练塘镇泾珠村长珠102号）
111. 练塘镇金田村卫生室（地址：上海市青浦区练塘镇金田村金田路256号）
112. 练塘镇前进村卫生室（地址：上海市青浦区练塘镇前进村村委）
113. 练塘镇北王浜村卫生室（地址：上海市青浦区练塘镇北王浜路57号）
114. 练塘镇林家草村中心卫生室（地址：上海市青浦区练塘镇林家草171号）
115. 练塘镇顾巷村卫生室（地址：上海市青浦区练塘镇顾林路25号）
116. 练塘镇北庄村中心卫生室（地址：上海市青浦区练塘镇北庄303号）
117. 练塘镇网埭村卫生室（地址：上海市青浦区练塘镇网埭55号）
118. 练塘镇西叶厍村卫生室（地址：上海市青浦区练塘镇西叶厍143号）
119. 上海市青浦区练塘镇东叶厍村中心卫生室（地址：上海市青浦区练塘镇东叶厍155号）
120. 练塘镇长田村卫生室（地址：上海市青浦区练塘镇练高路19号）
121. 练塘镇朱家庄村中心卫生室（地址：上海市青浦区练塘镇朱家庄路38号）
122. 练塘镇干庄村卫生室（地址：上海市青浦区练塘镇干庄路180号）
123. 练塘镇四农村卫生室（地址：上海市青浦区练塘镇四农180号）
124. 练塘镇四联村卫生室（地址：上海市青浦区练塘镇四联57号）
125. 练塘镇星浜村中心卫生室（地址：上海市青浦区练塘镇星浜村明星381号）
126. 练塘镇蒸夏村中心卫生室（地址：上海市青浦区练塘镇唐夏1号）
127. 练塘镇芦潼村中心卫生室（地址：上海市青浦区练塘镇芦潼村芦周路101号）
128. 练塘镇浦江村卫生室（地址：上海市青浦区练塘镇庄浦路148号）
129. 练塘镇蒸南村卫生室（地址：上海市青浦区练塘镇蒸南路3号）
130. 练塘镇浦南村卫生室（地址：上海市青浦区练塘镇浦南村四合47号）
131. 练塘镇泖甸村卫生室（地址：上海市青浦区练塘镇泖甸路100号）
132. 练塘镇泾花村中心卫生室（地址：上海市青浦区练塘镇泾花村泾花路354号）
133. 练塘镇东庄村卫生室（地址：上海市青浦区练塘镇东庄村东圩路288号）
134. 练塘镇叶港村高家港卫生室（地址：上海市青浦区练塘镇叶港村高家港46号）
135. 练塘镇东厍村厍浜卫生室（地址：上海市青浦区练塘镇东厍村厍浜6088号）
136. 练塘镇双菱村菱浜卫生室（地址：上海市青浦区练塘镇双菱村120号）
137. 练塘镇练北卫生室（地址：上海市青浦区练塘镇练北新村44号105-107号505）
138. 蒸淀卫生服务分中心（地址：上海市青浦区练塘镇蒸淀蒸兴路147号）
139. 夏阳街道社区卫生服务中心（地址：上海市青浦区崧润路779弄）
140. 夏阳街道社区卫生服务中心东方社区卫生服务站（地址：上海市青浦区城中东路50号、52号）
141. 夏阳街道社区卫生服务中心祥龙社区卫生服务站（地址：上海市青浦区青安路380号（祥龙居委会楼下））
142. 夏阳街道社区卫生服务中心佳乐苑社区卫生服务站（地址：上海市青浦区盈港东路8300弄138号）
143. 夏阳街道社区卫生服务中心青水湾社区卫生服务站（地址：上海市青浦区华浦路268弄42号101室）
144. 夏阳街道社区卫生服务中心金地格林郡社区卫生服务站（地址：上海市青浦区沪青平公路5669弄63栋23号）
145. 夏阳街道社区（新城一站）卫生服务中心秀泉路社区卫生服务站（地址：上海市青浦区崧涵路190号201室）
146. 夏阳街道社区（新城一站）卫生服务中心华中苑社区卫生服务站（地址：上海市青浦区崧漪一路46弄17号101室）
147. 夏阳街道社区卫生服务中心德康社区卫生服务站（地址：上海市青浦区崧润路49弄8幢13号101室）
148. 夏阳街道社区卫生服务中心新阳村卫生室（地址：上海市青浦区夏阳街道新阳村260号）
149. 夏阳街道社区卫生服务中心王仙中心村卫生室（地址：上海市青浦区夏阳街道王仙村120号）
150. 夏阳街道社区卫生服务中心枫泾村卫生室（地址：上海市青浦区夏阳街道枫泾村路145号旁）
151. 夏阳街道社区卫生服务中心塔湾中心村卫生室（地址：上海市青浦区夏阳街道沪青平公路5251号）
152. 夏阳街道社区卫生服务中心城南中心村卫生室（地址：上海市青浦区夏阳街道南太路68号）
153. 夏阳街道社区卫生服务中心太来村卫生室（地址：上海市青浦区夏阳街道太来村188号）
154. 夏阳街道社区卫生服务中心塘郁中心村卫生室（地址：上海市青浦区夏阳街道塘郁村179号）
155. 夏阳街道社区卫生服务中心金家中心村卫生室（地址：上海市青浦区夏阳街道金家村青昆路688号）
156. 香花桥街道社区卫生服务中心（地址：上海市青浦区赵屯镇大盈社区新桥路1195弄1号）
157. 香花桥街道社区卫生服务分中心（地址：上海市青浦区香花桥街道悲情公路）
158. 香花桥街道社区卫生服务分中心民惠第二社区卫生服务站（地址：上海市青浦区民惠7区久远路1668弄2号会所）
159. 香花桥街道社区卫生服务分中心玫瑰湾社区卫生服务站（地址：上海市青浦区香花桥街道清河湾路425弄1号）
160. 香花桥街道社区卫生服务分中心爱星村卫生室（地址：上海市青浦区友爱路77号）
161. 香花桥街道社区卫生服务分中心曹泾村卫生室（地址：上海市青浦区曹泾村村委171号）
162. 香花桥街道社区卫生服务分中心大联村卫生室（地址：上海市青浦区大联村村委太联路太联村214号）
163. 香花桥街道社区卫生服务分中心东方村中心卫生室（地址：上海市青浦区东方路131号）
164. 香花桥街道社区卫生服务分中心郏一村中心卫生室（地址：上海市青浦区郏一村231号）
165. 香花桥街道社区卫生服务分中心金米村中心卫生室（地址：上海市青浦区金米村村委青赵公路4358号）
166. 香花桥街道社区卫生服务分中心泾阳村横泾卫生室（地址：上海市青浦区外青松公路横泾152号）
167. 香花桥街道社区卫生服务分中心泾阳村奚阳中心卫生室（地址：上海市青浦区姚奚路与向阳河路路口）
168. 香花桥街道社区卫生服务分中心民惠佳苑中心卫生室（地址：上海市青浦区久远路1669弄308号）
169. 香花桥街道社区卫生服务分中心东斜村卫生室（地址：上海市青浦区东斜村3281号）
170. 香花桥街道社区卫生服务分中心奚阳中心卫生室（地址：上海市青浦区青山居委崧达路39号）
171. 香花桥街道社区卫生服务分中心青山村卫生室（地址：上海市青浦区姚奚路与向阳河路路口）
172. 香花桥街道社区卫生服务分中心新桥村卫生室（地址：上海市青浦区新桥村村委大盈路255号）
173. 香花桥街道社区卫生服务分中心新民村卫生室（地址：上海市青浦区新姚村村委新胜路148号）
174. 徐泾镇社区卫生服务中心（地址：上海市青浦区徐民路1088号）
175. 徐泾镇社区卫生服务中心二联村卫生室（地址：上海市青浦区徐泾镇二联村村委 ）
176. 徐泾镇社区卫生服务中心光联村中心卫生室（地址：上海市青浦区徐泾镇光联村村委）
177. 徐泾镇社区卫生服务中心豪都中心卫生室（地址：上海市青浦区徐泾镇豪都国际花园）
178. 徐泾镇社区卫生服务中心金联村卫生室（地址：上海市青浦区徐泾镇金联村村委）
179. 徐泾镇社区卫生服务中心金云村卫生室（地址：上海市青浦区徐泾镇金云村村委）
180. 徐泾镇社区卫生服务中心陆家角村卫生室（地址：上海市青浦区徐泾镇陆家角馨苑）
181. 徐泾镇社区卫生服务中心民主村中心卫生室（地址：上海市青浦区徐泾镇民主村村委）
182. 徐泾镇社区卫生服务中心前明村卫生室（地址：上海市青浦区徐泾镇前明村杜家新区）
183. 徐泾镇社区卫生服务中心徐泾居委会卫生室（地址：上海市青浦区徐泾镇徐泾居委会）
184. 徐泾镇社区卫生服务中心迮庵村中心卫生室（地址：上海市青浦区徐泾镇迮庵村村委）
185. 徐泾镇社区卫生服务中心宅东居委会卫生室（地址：上海市青浦区徐泾镇高泾新区）
186. 徐泾镇社区卫生服务中心宅东居委会宅东卫生室（地址：上海市青浦区徐泾镇宅东新区）
187. 徐泾镇社区卫生服务中心玉兰清苑中心卫生室（地址：上海市青浦区徐泾镇龙联路58号玉兰清苑39号底楼）
188. 盈浦街道社区卫生服务中心（地址：上海市青浦区盈浦街道盈福路50号）
189. 盈浦街道社区卫生服务中心五浦汇站（地址：上海市青浦区崧子浦路289弄4号）
190. 盈浦街道社区卫生服务中心双桥站（地址：上海市青浦区盈米路14、16、18号）
191. 盈浦街道社区卫生服务中心万寿站（地址：上海市青浦区万寿路153号）
192. 盈浦街道社区卫生服务中心民乐站（地址：上海市青浦区盈港路1750弄综合楼1楼）
193. 盈浦街道社区卫生服务中心浩泽站（地址：上海市青浦区漕盈路555弄59号.）
194. 盈浦街道社区卫生服务中心盈中站（地址：上海市青浦区卫中路12号）
195. 盈浦街道社区卫生服务中心天恩桥村卫生室（地址：上海市青浦区天恩桥路88号）
196. 盈浦街道社区卫生服务中心南厍村卫生室（地址：上海市青浦区南厍村委会盈淀路北）
197. 赵巷镇社区卫生服务中心（地址：上海市青浦区赵巷镇巷居路289号）
198. 赵巷镇社区卫生服务中心金葫芦社区卫生服务站(地址：上海市青浦区赵巷镇民实路90号)
199. 赵巷镇方夏村刘夏卫生室(地址：上海市青浦区赵巷镇原刘夏村村委224号)
200. 赵巷镇方夏村方东卫生室(地址：上海市青浦区赵巷镇方夏村方东445号)
201. 赵巷镇方夏村方西卫生室(地址：上海市青浦区赵巷镇方夏村方西45号)
202. 赵巷镇垂姚村卫生室(地址：上海市青浦区赵巷镇垂盈路28号)
203. 青浦区赵巷镇沈泾塘村卫生室(地址：上海市青浦区赵巷镇沈泾塘村村委182号)
204. 赵巷镇崧泽村中心卫生室(地址：上海市青浦区赵巷镇崧泽村村委309号)
205. 赵巷镇中步村中伍卫生室(地址：上海市青浦区赵巷镇中伍村村委132号)
206. 赵巷镇中泽苑卫生室(地址：上海市青浦区赵巷镇中泽路234号)
207. 重固镇社区卫生服务中心地址：上海市青浦区重固镇联茂路68号）
208. 重固镇社区卫生服务中心郏店村中心卫生室（地址：上海市青浦区重固镇凤联路郏店村359号）
209. 重固镇社区卫生服务中心毛家角村卫生室（地址：上海市青浦区  
     北青公路6725弄38号）
210. 重固镇社区卫生服务中心中新村中心卫生室（地址：上海市青浦区秀横路中新村100号）
211. 重固镇社区卫生服务中心徐姚村中心卫生室（地址：上海市青浦区重固镇新重安路徐姚村368号）
212. 重固镇社区卫生服务中心章埝村卫生室（地址：上海市青浦区重固镇陈章路章埝村800号镇）
213. 重固镇社区卫生服务中心回龙村卫生室（地址：上海市青浦区重固镇回龙支一路回龙村178号）
214. 重固镇社区卫生服务中心新联村卫生室（地址：上海市青浦区重固镇福定路362号）
215. 重固镇社区卫生服务中心新丰村中心卫生室（地址：上海市青浦区重固镇新丰村支路新丰村458号）
216. 重固镇社区卫生服务中心钱家泾卫生室（地址：上海市青浦区重固镇福泉山路徐山路钱家泾100号）
217. 重固镇社区卫生服务中心福泉山村山前卫生室（地址：上海市青浦区重固镇北青公路7488号）
218. 朱家角镇社区卫生服务中心（地址：上海市青浦区朱家角镇曲池路39号）
219. 朱家角镇社区卫生服务分中心（地址：上海市青浦区朱家角镇祥凝浜路62号）
220. 朱家角镇周荡村卫生室（地址：上海市青浦区朱家角镇周荡村160号）
221. 朱家角镇薛间村卫生室（地址：上海市青浦区朱家角镇薛间村80号）
222. 朱家角镇薛间村龙星卫生室（地址：上海市青浦区朱家角镇薛间村龙星143号）
223. 朱家角镇周家港村卫生室（地址：上海市青浦区朱家角镇周家港村123号）
224. 朱家角镇小江村中心卫生室（地址：上海市青浦区朱家角镇小江村93号）
225. 朱家角镇万隆村卫生室（地址：上海市朱家角镇万隆村马家埭193号）
226. 朱家角镇横江村中心卫生室（地址：上海市青浦区朱家角镇横江村108号）
227. 朱家角镇淀峰村卫生室（地址：上海市青浦区朱家角镇淀峰村162号）
228. 朱家角镇山湾村中心卫生室（地址：上海市青浦区朱家角镇山湾村1号）
229. 朱家角镇庆丰村卫生室（地址：上海市青浦区朱家角镇庆丰村521号）
230. 朱家角镇王金村中心卫生室（地址：上海市朱家角镇王金村新泾149号）
231. 朱家角镇建新村卫生室（地址：上海市青浦区朱家角镇葑沃路350号）
232. 朱家角镇新胜村中心卫生室（地址：上海市青浦区朱家角镇沈砖路2205号）
233. 朱家角镇林家村卫生室（地址：上海市朱家角镇林家村倪马72号）
234. 朱家角镇张巷村卫生室（地址：上海市青浦区朱家角镇沈太路28号）
235. 朱家角镇李庄村中心卫生室（地址：上海市青浦区朱家角镇李庄村1688号）
236. 朱家角镇安庄村中心卫生室（地址：上海市青浦区朱家角镇朱天路132号）
237. 朱家角镇先锋村卫生室（地址：上海市青浦区朱家角镇朱天路333号）
238. 朱家角镇沈巷村卫生室（地址：上海市青浦区朱家角镇沈巷村徐家浜97号）
239. 朱家角镇张马村卫生室（地址：上海市青浦区朱家角镇沈太路211）
240. 朱家角镇泰安社区卫生站（地址：上海市青浦区朱家角镇泰安馨苑公寓邱家港18弄46号公共配套房内）
241. 青浦区朱家角镇西湖新村社区卫生服务站（地址：上海市青浦区朱家角镇漕平路149号）

## 3.4软件系统建设需求

### 3.4.1医保五期接口及医疗付费“一件事”应用开发

#### 3.4.1.1医保五期接口开发

##### 3.4.1.1.1 医保五期接口开发

医保接口主要是为了降低收费处的工作量，并且保证HIS和医保数据的一致性，方便医院对医保病人进行核算。  
 1、医保数据与HIS数据的对照。（可以开发通用的接口数据对照）主要是价格表的对照，有些接口要求上传科室、疾病编码等也需要对照。  
 2、写读卡函数，最好封装到一个对象中。  
 3、在涉及医保接口的地方，预留出调用接口的方法。接口的实现通过接口函数去调用封装好的医保接口对象。一般是通过病人的身份或费用类别进行判断，是否调用医保这个方法。  
 4、开发接口的过程（简单介绍一下，应该在医保接口对象中实现，具有通用性）。主要集中在收费，退费的过程中。挂号部分省略  
   （1）门诊收费：在录入完费用明细后，在结算时，通过医保接口对照，将费用传递给医保系统  （一般是调用动态库中的预结算方法，返回帐户支付和现金支付），如果确认无误后，在保存时，调用医保提供的保存方法。  
   （2）住院登记：在保存时调用医保提供的住院登记的方法。  
   （3）住院收费：在结算时，掉出病人的费用明细，通过对照表翻译成医保项目代码，其他的和门诊收费是一样的。  
   （4）退费：在退费时，判断是否是医保病人，如果是医保病人，则调用医保提供的退费方法，返回退费金额。

##### 3.4.1.1.2 HIS系统改造（门诊挂号、收费、入院登记、结算等相应改造，适应医保五期接口）

通过对门诊医生诊疗过程的记录，对主诉、体检、现病史及血压、血糖等客观指标的记录，对诊断结果、处方信息的全面处理，实现门诊诊疗的全过程进行全面管理。并可对医生诊断过程的质量、工作量等进行全面的统计分析。

##### 3.4.1.1.3 HIS系统改造（医保电子凭证支付改造）

对院内原有HIS系统进行改造，实现高价药流程、造口袋流程、住院大病减负流程以及实现植入材料的合并支付。

对线下窗口、自助机、医生站、医技科室等刷卡场景进行改造，兼容实体卡与电子凭证的应用。

实现自动每日对账及自动上传住院费用明细。

对电子凭证线上流程进行改造，实现互联网端医保接口的对接及医保交易。

**3.4.1.1.4 村医系统改造升级**

对村卫生室原有系统进行改造，实现高价药流程、造口袋流程以及实现植入材料的合并支付。

对线下窗口、自助机、医生站、医技科室等刷卡场景进行改造，兼容实体卡与电子凭证的应用。

实现自动每日对账及自动上传费用明细。

对电子凭证线上流程进行改造，实现互联网端医保接口的对接及医保交易。

#### 3.4.1.2医疗付费“一件事”开发

##### 3.4.1.2.1 诊间支付

上海医保接口规范（第5版）支持医保电子凭证，支持线上医保脱卡支付，为医保患者优化支付流程奠定了基础。目前医院线上业务涉及缴费的流程主要有常规挂号、缴费业务、互联网医院的复诊登记及药品缴费业务。

患者诊间就诊后，患者在诊间或者壁挂机上刷卡、扫描电子结算卡医保结算和支付

1） 挂号缴费

就诊日当天，患者选择已预约记录或者当日排班，点击“去结算”→调用渠道APP提供的获取医保电子凭证的接口，唤起电子凭证验证页面，获取医保电子凭证信息→传入医保电子凭证信息及挂号信息，调用HIS提供的挂号预算接口，由HIS和医保完成试算交易→展示返回的预算信息（包括个人支付、医保支付等）→患者点击“确认结算”→传入试算时获取的医保电子凭证信息，传入HIS，调用HIS的挂号结算接口→调用渠道APP的下单接口，唤起渠道APP的收银台，完成个人自费部分收费→HIS轮询医保结算结果→医保结算完成后完成本地医保信息回写→互联网应用轮询HIS挂号结算结果，结算成功后通知患者结算成功并显示后续就诊指引信息。

2） 门诊缴费

流程参照 “1）挂号缴费”。

互联网应用调用HIS的门诊缴费的预算、结算接口→HIS调用医保的门诊预算，结算接口。

3） 复诊登记缴费

流程参照“1）挂号缴费”

互联网应用传入复诊登记相关信息。

4） 复诊登记退费

复诊登记由于存在不符合互联网诊疗要求需要退费的情况，因此需要支持复诊登记退费。经互联网医院判断患者满足退费条件，将该登记置为可退费状态，患者发起在线退复诊费→调用渠道APP，唤起验证页面，获取医保电子凭证→调用HIS封装的退款接口→HIS调用医保的退费接口，改写本地数据→互联网应用显示退款状态。

5） 复诊药品缴费

流程参照“1）挂号缴费”。

6） 对账接入

自费和医保采取分开对账，医保部分的对账和改账由HIS完成。自费部分对账由对账平台完成。

7） 微信公众号

获取医保电子凭证→医保患者自费部分下单→自费部分对账账单下载及对账。

8） 支付宝生活号

获取医保电子凭证→医保患者自费部分下单→自费部分对账账单下载及对账。

9） 随申办APP入驻

用户信息打通→获取医保电子凭证→自费部分对账账单下载及对账。

10） 处方单扫码支付

医生站打印电子处方时从支付平台获取二维码并打印在纸质处方上→患者用微信、支付宝扫描二维码获取处方信息→系统发起预结算。

对院内原有HIS系统进行改造，对线下窗口、自助机、医生站、医技科室等场景进行改造，使其兼容实体卡与医保电子凭证的应用，并实现每日对账及自动上传住院费用明细，对医保电子凭证的线上使用流程进行改造，实现电子凭证的读卡及线下结算融合。

|  |  |  |
| --- | --- | --- |
| **序号** | **场景** | **功能模块** |
| 1 | 线下（窗口支付） | 医保接口封装 |
| 2 | HIS程序改造 |
| 3 | 电子凭证线下流程改造 |
| 4 | 自动对账、自动上传住院费用 |
| 5 | 线上（脱卡支付） | 线上接口改造 |

##### 3.4.1.2.2 线上支付

**1.支付信息查询**

患者完成诊疗行为后，可以在随申办app上查看待支付的订单信息，以及当天发生的所有费用信息

**2.医保在线支付**

医保患者支付时医保部分能实时结算，自费部分由随申办支付平台扣除，实现医保患者在线脱卡支付功能。

针对某些病人扣了费，但因故放弃相关检查或治疗项目，可通过“随申办”APP 统一发起退款申请，由医疗机构门办负责网上审核并通过后，再按原渠道做相关退款处理。

**3.自费在线支付**

自费患者支付能实时结算，由随申办支付平台扣除，实现患者在线脱卡支付功能。

针对某些病人扣了费，但因故放弃相关检查或治疗项目，可通过“随申办”APP 统一发起退款申请，由医疗机构门办负责网上审核并通过后，再按原渠道做相关退款处理。

**4.入驻随申办app**

提供移动端在线支付的功能，并且将系统入驻到随申办市民云app中。

**5、市大数据中心支付（基于信用的无感支付）**

1)信用签约查询

基于市大数据中心的统一信用签约平台，为本市居民提供医疗信用专项额度，统一签约与绑卡、解约与解卡的授权服务，并提供欠费提醒，欠费后相关线上信用限制告知，失信名单等征信服务。支付平台统一和大数据中心对接，获取患者信用签约状态，为患者后续基于信用的无感支付、先诊后付等医疗行为做支撑。

2)信用免密支付

在大数据中心签约信用就医的患者到达医疗机构并进行完诊疗服务后系统自动发起基于信用的无感支付服务，发生医疗费用的医保部分实时结算，自费部分由绑定的信用账户进行支付，在整个诊疗行为中患者无需任何付费动作，支付平台统一和大数据中心对接信用签约免密支付，协助医院系统完成患者整个信用就医的诊疗行为。

**6、支付渠道管理**

1）微信支付

接入第三方微信支付的信用就医，通过对第三方微信支付渠道管理，实现微信交易信息下载与异常账目发现和处理，包括与微信进行支付、退款确认、还款，以及实现对网络异常导致的支付退款消息重发确认机制。

2）支付宝支付

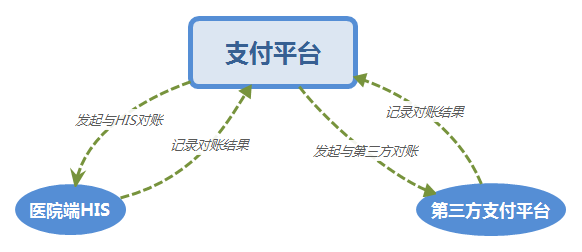
接入第三方支付宝支付的信用就医，通过对支付宝的渠道管理，实现支付宝交易信息下载与异常账目发现和处理，包括与支付宝进行支付、退款确认、还款，以及实现对网络异常导致的支付退款消息重发确认机制。

3）其他支付方式

支持与其他第三方支付渠道连接进行充值、退款及相应的交易信息下载和确认。

**7、信息管理**

支付平台向医院及第三方支付平台开放对账后台。支付平台订单记录有医院端HIS订单流水号、第三方支付平台订单流水号、商户号及支付平台自身订单流水号，支付平台通过分别发起与医院端HIS和第三方支付平台的对账，记录同一订单三方流水号完整性，并通过HIS及第三方平台返回的确认支付通知状态判断订单是否为异常单。在此基础上，对账后台提供历史费用订单明细数据及时间范围条件下的总订单数量、订单总账和异常账数量及明细供查看。同时可提供简单的数据报表及数据导出功能，供进一步统计分析使用。



1）支付请求服务

提供支付请求的入口，来自移动端响应支付成功的通知。

2）聚合支付

整合支付宝、微信、云闪付等多种当前热门的支付渠道，提供多种支付渠道同一个支付二维码的聚合支付服务。

3）支付信息识别

能够自动识别用户支付扫码信息，区分微信、支付宝等多种支付渠道，与对应的第三方支付平台进行支付服务对接，完成支付服务。

4）“随申办”移动就医入口

“随申办”移动端是上海“一网通办”移动政务服务的总入口，目前包括随申办市民云APP、随申办微信小程序、随申办支付宝小程序三个渠道。

开通本区居民基于以上入口的身份认证开通、支付、查询等

5）医保电子凭证认领

供本区医保参保人员在“随申办”上“基于信用的无感支付”的认证，进行患者实名认证审核，领取“医保电子凭证”，并网上签署相关支付协议，绑定银行卡或支付宝花呗等相关支付方式以完成“赋信”功能。

6）费用结算支付管理

开展用于费用结算支付的信用卡、支付宝花呗、本市医保参保人员医疗信用专项额度等渠道的统一签约与绑卡、解约与解卡的授权服务；

提供欠费提醒，欠费后相关线上信用限制告知、失信名单等征信服务。

7）亲情付代扣管理

对于已领取了电子医保凭证，不会使用手机移动支付的老年人、儿童等人群，支持“亲情付”代扣付费功能，通过关联绑定其父母、子女、配偶等银行卡，完成线上签约。

8）订单号生成服务

用户扫码后，统一支付平台将会动态的生成订单号，保证该次扫码支付的唯一性，避免了多人同时扫码、多渠道扫码支付等误操作造成的多次支付问题。

9）商户号管理

用户扫码支付后，统一支付平台请求第三方支付平台进行交易，根据交易订单动态生成商户号，为后续的异常退款、对账提供识别的依据。

10）支付信息确认

用户扫码后将会提供支付信息确认，包括充值卡号、姓名、手机号码、支付金额等，让用户进行支付信息的确认，减少支付错误的可能性。

11）交易信息确认

通过第三方确认完成的用户支付信息由平台统一管理，并形成有效的通知机制，返回给订单发起方，完成业务闭环。

**8、退款管理**

统一支付平台支持对异常账、单边账进行自动退款处理，对退款余额不足部分进入退款队列，无需人为干预，平台将根据退款优先级自动处理。此处退款只针对单笔充值的异常账退款，不涉及已充值成功的预交金部分，预交金退款需患者前往线下窗口。

1）自动退款处理

针对支付超时、支付取消等操作，导致用户支付完成，但支付平台没有正常完成交易的支付问题时，支付平台将通过自动退款服务，完成自动退款，避免了单边账的产生。

2）退款队列管理

由于账户中的金额每天定时流转，在当天医院第三方账户收入不足时，将有可能导致隔日退款的用户存在无法成功退款的问题。这时统一支付平台将通过退款队列服务，把退款任务依次加入到队列中进行自动退款操作，确保24小时内能够自动退款成功。

3）退款状态查询

成功退款后，具体到款时间将参照患者使用的第三方支付平台所规定的退款周期，有可能会有延迟。平台通过定时查询服务获取第三方退款状态，并记录退款明细。

**9、统一对账**

统一预交金管理平台提供电子化的对账方式，各接入医院可以自行获取对账明细，平台也提供各家医院的交易对账报表。平台每日将自动生成前一日的清算汇总清单、清算明细单等数据文件。

平台依据每日各医疗机构实际发生扣费交易情况给出清算报表，各接入医疗机构按每日实际发生在本院的区域预交金支付情况提供对账依据，平台与院内完成预交金对账后，提供该清算报表给银行进行最终清算。

1）交易信息查询

通过记录每一笔支付的请求信息与第三方交易明细进行比对，提供交易信息的查询服务，方便快速定位每一笔交易的交易时间、交易方式及交易支付方的信息。

2）成功充值统计

充值成功统计每一笔成功完成支付的订单信息，平台记录每笔订单的充值时间、患者姓名、充值金额及相关的订单号信息，方便管理人员查找每一笔交易记录。

3）异常充值统计

异常充值统计交易过程中由平台及第三方超时、取消等引起的充值异常，为管理人员对账管理，查找异常账、单边账提供入口。

4）分账统计及下载

分账统计是根据所有医疗机构产生的支付记录根据不同的医疗机构维度，在支付平台上进行分账统计，最终根据分账统计结果，进行各医疗机构金融虚拟子账户的分账。

分账下载是为各医疗机构提供账单下载功能，方便各医疗机构自行对账。

5）自动下载对账

平台可自动从微信、支付宝及银行方面下载相应的交易记录和提现记录，进行平台内部自动对账，对于异常账款可进行自动标识，确保分账对账的可靠性。

**10、基础平台**

为保证支付平台及支付数据的安全，整个统一支付对账平台架设于基础安全平台之上，采用“数据+服务+应用”的模式设计，通过提供可供开放的数据服务，以信息资源服务目录列表形式在安全平台门户上展现，采用高效率、高质量的方式帮助开发者实现数据整合。基础安全平台除了提供平台支付服务外，加入智能化的服务监测以及服务编排，打造自由灵活的安全服务平台。

1）节点管理与授权

节点指安全服务组件以外与服务进行交互的接入端点。可以是基于平台的应用系统，也可以是平台外部的其它平台或系统。例如银行应用。组件内的服务可以通过授权进行分发管理，接入组件的系统或者厂商只能访问其有权限的数据服务，彻底杜绝服务暴露的安全问题。

随着越来越多的外部系统接入，外部服务可以通过授权管理快速对服务进行适配，服务授权通过授权码和密钥来实现对调用机构的认证，对每个接入的实体分配一个授权码，并生成数据加密的公私钥，外部系统通过授权码进行相应服务的调用，这样可以判断接入者的身份，避免出现数据及系统的安全问题。

2）负载集群管理

为了提高系统的健壮性和稳定性，应对高并发的数据访问请求，组件接入的服务可以部署在多台服务器上，组成一个服务集群。用户发起API调用时，可以根据负载均衡算法，将请求发送到不同的服务器上，起到分流的效果。通过集群管理可以监控集群中服务器的运行状态，新增或删除集群服务器。

例如访问支付服务的服务器就要进行集群部署的方式，上一级服务器可以根据不同接入服务器的负载状况来决定使用哪台支付服务器来提供服务，从而更好地平衡访问压力，保证整个组件的高可用性。

3）后备管理机制

作为一个为多种应用提供服务的安全管理组件，自身的高可用性也是一个非常重要的环节。当一台服务器出现故障后，能够自动地将服务请求切换到备份服务器上，保证服务的连续性和生存率。

4）日志审计机制

安全服务组件采用基于日志的数据分析引擎通过对接入用户的访问规律进行分析，例如访问的高峰时间段、访问的频率、单位时间内（默认为每天，可以根据规则进行配置）访问的次数进行组合分析，得出用户日常访问习惯。当某一段时间内出现异常行为时，例如爆发性调用，非正常时间段内频繁访问等，进行异常提醒，并给出相应的可能导致威胁的处置机制。

通过定期对用户的访问行为进行分析，对访问日志分级分类，设置服务的访问频率，把单位时间内不正常的访问行为设定为可能的非法行为，自动将访问用户IP加入黑名单，进行隔离。

通过日志审计机制，增强了组件的安全管控能力，提高了系统在应对各种潜在威胁上的应对能力。

### 3.4.2 医保数据上传应用开发

**3.4.2.1上传基础模块**

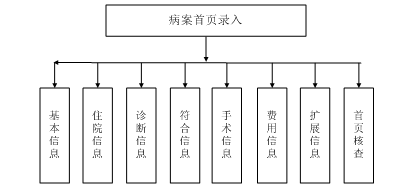
**1.系统管理**

对系统使用权限、系统参数、系统数据的管理，包括初始参数设置、用户组设置、用户设置、数据导出、数据导入、扩展字段设置；

**2.字典库设置**

设置系统的基本字典库信息，包括科室设置、ICD码设置、手术码设置、医生设置等。

**3.其他功能**

常见单病种设置、常见单病种一览表、常见单病种统计、自定义单病种管理、生成出院病人调查表、查询出院病人调查表、输出出院病人调查表、生成网络直报数据、上传卫生局、检查各报表平衡关系、查询未用病案号等

#### 3.4.2.2 病案首页信息

病案首页信息包含中心流水号信息、诊断信息、手术信息、费用信息、发票和结算信息、中心流水号信息等。

#### 3.4.2.3住院非医保实时患者交易明细数据

数据主要包括医疗费用发票明细、医疗费用明细信息、医疗费用细分明细等。

#### 3.4.2.4出院小结信息

出院小结信息包括就诊流水号、医保医疗机构代码、病区、床号、入院时主要症状及体征、实验室检查及主要会诊、住院期间特殊检查、诊疗过程、合并症、出院时情况、出院医嘱、治疗结果、主治医师医保医师代码、主治医师姓名、住院医师医保医师代码、住院医师姓名等。

#### 3.4.2.5住院医嘱信息

住院医嘱信息包括医保医疗机构代码、医嘱ID（序号）、就诊流水号、中心交易流水号、病区、下达科室编码、医嘱下达人医保医师代码、医嘱下达人医保医师姓名、医嘱下达时间、执行科室编码、医嘱执行人工号、医嘱执行人姓名、医嘱执行时间、医嘱终止时间、医嘱说明、医嘱组号、医嘱类别、医嘱明细医保编码、医嘱明细名称、是否药品、药品包装规格、药品包装规格单位、药品包装规格系数、药品用法、用药频次代码、用药频度、每次使用剂量、每次使用剂量单位、每次使用数量、每次使用数量单位、给药途径(用法)、用药天数、皮试判别、发药数量、发药数量单位、备注等。

#### 3.4.2.6门诊非医保实时病人交易明细数据

数据信息包括就诊流水号、医保医疗机构代码、门急诊标识、就诊卡号、科室编码、人员类型、医师编码、处方号、姓名、性别、出生日期、年龄、国籍、证件号码、证件类型、现住址、电话号码、联系人姓名、关系(联系人与患者关系)、联系人地址、联系人电话号码、医疗费用金额、医疗费用发票明细等。

#### 3.4.2.7 门诊处方信息

门诊处方信息包括医保医疗机构代码、处方号码、处方项目明细序号、就诊流水号、中心交易流水号、就诊科室代码、开方医生工号、开方医生姓名、开方时间、项目明细医保编码、项目明细名称、是否药品、药品用法、发药数量、发药数量单位、处方贴数、用药频次代码、用药频次、每次使用剂量、每次使用剂量单位、每次使用数量、每次使用数量单位、用药途径代码、用药天数、皮试判别等。

#### 3.4.2.8 实验室检验报告

实验室检验报告需要包含医保医疗机构代码、检验报告单号、报告日期、就诊流水号、中心交易流水号、门诊/住院标志、申请人医保医师代码、申请人医保医师姓名、报告人工号、报告人姓名、审核人工号、审核人姓名、申请科室编码、病区、床号、打印日期、申请日期、采集日期、检验日期、报告备注、标本代码、标本名称、报告单类别编码、报告单类别名称、检验结果、细菌结果、药敏结果等。

#### 3.4.2.9医学影像检查报告

医学影像检查报告包含检查报告明细、其它检查明细。

#### 3.4.2.10录入病案首页信息及相关内容

**1、首页录入功能**

1）首页录入界面有五个区：按钮区、标题区、标签区、录入区、提示区。其中，按钮区包括保存、清空、同步验证规则、同步编码、打印、关闭按钮；标题区有病案号、姓名、次数、年龄、录入员、录入日期内容，是用来显示病案的基本信息；录入区内容按照广东省病案首页标准；提示区一般列出的是基础字典选项内容。浏览标签区知，住院病案首页模块包括基本信息、住院信息、诊断信息、符合情况、手术信息、扩展信息、费用信息，这些都是每个医院必录模块，妇婴卡、肿瘤卡是专科医院必录的模块；

2）详细验证规则：有多种验证字段的操作，这些字段的验证和复杂度都不一样，字段包括病案号、姓名、附加手术..等；

3) 病案首页数据核查：对病案首页数据核查，旨在加强对病案首页录入质量的监控，利用各字段之间的逻辑关系进行检查、侦错，将核查出的错误列在列表上，供用户修改，同时可直接双击打开相应的记录并修改保存。系统提供打印、导出核查出错误信息功能，方便用户修改

4) 修改首页验证规则：修改首页验证规则是用来控制首页录入过程中弹出的提示框或错误窗口，用户可以根据自己实际需要设置某个字段是否必须录入，是否必须达到最大，错误是否可以通过，是否弹出错误，是否弹出警告以及它的最大位数。

5) 修改病案：修改病案是用来修改已录入病案的病案号或姓名或住院次数，除此外还可用来删除病案。

6) 批量修改病案号：由于医院有重复使用病案号情况，因此系统提供修改病案号功能，将重复病案号改成未用病案号。如果一个病案号有多次住院，则可批量修改病案号。

**2、首页查询：**

1) 病案综合查询：可根据用户的需要自由组合查询条件和显示结果，能够很好的满足医院的各类查询需求，具体操作包括自定义查询条件、自定义查询结果、显示模板设置、查询结果打印、查询结果导出。

2) 病案查询：本模块指对首页的一些常用、有针对性条件的查询，包括按病案号、姓名，按ICD码、疾病名称，按手术码、手术名称等查询。

3）打印病案索引卡：病案索引卡包括姓名索引卡、疾病索引卡、手术索引卡。

4）打印病案登记表：打印病案登记表包括打印出院病人分科登记表、病案登记一览表、死亡病人登记一览表、手术病人分科登记表、出院病人分科登记表（中医院）。

5) 查询分析器：为了能够满足用户更高要求的查询，本系统保留了旧版本的查询分析器，此功能只能查询数据库中的数据不能修改，本系统的查询分析器继承了原来的功能优点，并在原来基础上增加了一些功能，更加贴近用户。

6) 病案修改日志查询：本操作用来查询病案修改日志，供用户了解病案的修改人、修改时间。单击菜单“病案查询→病案修改日志查询”打开病案修改日志查询窗口。

7) 重复入院病人查询：此功能用来查询某个时间段内“七日内重复入院两次以上”的病案。

8）门诊医技日志录入：门诊医技日志录入分为科室门诊工作日志、医生门诊工作日志、医院工作报表医技科室、医技科室（自定义）项目、专科门诊病人数输入、观察室工作日志、急诊工作日志。如果工作日志日期输入错误，系统提供批量修改日志日期功能；

日志录入：

9）住院部分日志录入：住院部分日志录入分为病房工作动态日志、家庭病床工作日志、医院经费及收支情况。如果科室病床数需要更改，可使用修改动态表科室床位数功能；

10）日志查询；

**3、统计报表：**

1）住院部分：包括住院月、季、年、非正式报表、住院院内用表、住院增减表、住院台账、住院病人动态日报、住院一览表等。

2）门诊医技报表：包括门诊月、季、年、非正式报表、门诊部分院内用表、门诊部分统计台账、门诊日报表等。

**4、归档及借阅功能**

归档及借阅包括病案归档登记和病案借阅归还登记两大功能。病案归档登记功能用于对最新病案进行归档登记。病案借阅归还登记功能用于对已归档并已录入的病案进行借阅归还登记。病案归档、借阅、归还是病案管理室日常工作不可缺少的环节，利用统计病案管理系统对病案的归档、借阅、归还进行管理，极大地提高病案管理室的工作效率。出院病人的病案需归档到病案管理室，以备日后使用。通过借阅病案，医生可以了解在病人以往的病历情况，为病人的本次治疗提供参考。为避免病人病案的遗失，要求对借出的病案进行归还。归档及借阅包括病案归档登记、病案归档情况查询、病案归档情况统计、病案借阅、病案归还、病案借阅一览表、病案借阅情况统计七部分。

# 硬件需求

**所需硬件由各社区卫生服务中心自行提供，不在本项目建设范围内。**单个医保接入点硬件设备要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 参数要求 | 数量 |
| 1 | 前置机 | 医保专用前置机（针对中小型医疗机构）  机架式服务器 1个 Intel Xeon Bronze 3204 (6-Core, 1.9 GHz, 85W)处理器，最大2颗；Intel C621芯片;  16GB 2Rx8 PC4-2933Y-R (1x 16 GB)内存； 配置嵌入式 HPE Smart Array S100i SR Gen10 SW RAID SATA 控制器；  标配嵌入式4端口千兆以太网卡;  2个 HPE 500W 白金热插拔电源;  2个 HPE 1TB SATA 6G Entry 7.2K LFF (3.5in) RW 1y HDD 1U机架式，含便捷安装导轨，不含理线架；3年5\*9,NBD 含医保通讯专用软件 （医保交易代码配置，现场安装上架调试） | 1 |
| 操作系统：WINDOWS 2016 SERVER（含介质+标签序列号） | 1 |
| 2 | 路由器 | 医保专用路由器 企业级全千兆路由器 （含医保交易代码配置，现场安装调试） | 1 |
| 3 | 防火墙 | 多核AMP+架构，网络层吞吐量4G，并发连接≥180万，每秒新建连接数8万， 标准1U机箱，单电源，标准配置6个10/100/1000M自适应电口，另有1个接口板卡扩展插槽，1个Console口， 含3年硬件维保服务，1年入侵防御功能模块升级，1年病毒防护特征库升级服务。 | 1 |
| 4 | 扫码墩 | 采集方式：影像式，CMOS Sensor ；  采集速度：1/30 秒；  分辨率：640×480；  视场角度：对角 53°；  识别精度：二维≥10mil，一维≥6.7mil；  识读方式：连续识读、指令触发；  扫描角度：转角 360°，仰角 ± 50°，偏角 ± 50°；  支持码制：  2D: QR Code, Data Matrix, PDF417  1D: Code 128，UPC-E0/E1,UPC-A ，EAN-13,EAN-8 , ISBN-13, Code 39, Code93, Interleaved 2 of 5等；  适宜环境：工作温度：0℃ ~ 65℃；  储存温度：0℃ ~ 70℃；  湿度：相对湿度 5% ~ 95%（无凝结）；  环境光：Max.100,000 Lux；  电压电流：输入：VBUS 5V（±5%）；  工作电流：小于 40mA（不含LED、语音播报）；  打印对比度：最低 25%的反射差；  通讯接口：HID、虚拟串口；  打印对比度：最低 25%的反射差；  识读成功提示：蜂鸣、LED、语音播报； | 若干 |

# 安全要求

## 5.1安全及隐私要求

信息安全是任何业务开展的基础，投标人应对于本次项目涉及的居民疾病情况等信息安全和隐私实行保护措施，并结合实际情况给出详细可行的解决方案。

## 5.2数据安全

**1、数据存储和运行安全**

数据库系统必须支持不依赖于第三方软件和存储的容灾备份。

数据库支持联机快速备份、快速加载数据和快速备份数据恢复，具有数据块级的备份和恢复功能。

* 支持基于共享磁盘（shared disk）模式的集群处理, 并且集群服务器能够支持联机处理和数据仓库应用。
* 支持CLUSTER集群系统。
* 支持数据分区管理，包括范围、列表分区及复合分区等。
* 支持数据库自动实时性能跟踪、监控。

**2、数据访问安全**

* 支持多种认证方式；
* 对数据库访问的安全性控制，支持数据库存储加密，数据加密传输；
* 严格控制对数据的访问。通过人员可访问的功能、地区、业务等多方面的控制，实现对访问权限的限定；
* 集中的数据库审计平台；

## 5.3应用安全

系统应用级安全包括统一身份认证，统一权限管理等，而贯穿整个体系是安全管理制度和安全标准.以实现非法用户进不来，无权用户看不到，重要内容改不了，数据操作赖不掉。

## 5.4物理安全

物理安全风险主要是指网络周边的环境和物理特性引起的网络设备和线路的不可使用，从而会造成网络系统的不可使用，甚至导致整个网络的瘫痪。它是整个网络系统安全的前提和基础，只有保证了物理层的可用性，才能使得整个网络的可用性，进而提高整个网络的抗破坏力。例如：

* 机房缺乏控制，人员随意出入带来的风险；
* 网络设备被盗、被毁坏；
* 线路老化或是有意、无意的破坏线路；
* 设备在非预测情况下发生故障、停电等；
* 自然灾害如地震、水灾、火灾、雷击等；
* 电磁干扰等。

因此，在总体考虑安全风险时，应优先考虑物理安全风险。保证网络正常运行的前提是将物理层安全风险降到最低或是尽量考虑在非正常情况下物理层出现风险问题时的应对方案。

安全的建设符合国家三级等保的要求，实现物理安全、网络安全、主机安全、应用安全、数据安全。

# 6、验收要求

1. 建设内容完成后，中标方应对相关建设内容进行完善的系统测试，并通知用户方进入系统试运行期。系统试运行为期一个月，与此同时中标方提供试运行期系统测试文档和项目验收相关文档，并且对用户方相关人员提供完善的培训。
2. 中标方提供全套完善的项目验收资料文档，包括配置文档、使用说明书给用户，并想用户书面提出申请项目验收，用户方在审查验收资料无误后同意召开项目验收会。
3. 由用户指定时间地点并邀请相关专家参加项目验收会，就项目建设内容依据验收资料文档等进行项目验收，并出具专家验收意见书作为项目验收的结论性文件。
4. 项目建设必须满足信息安全三级等保要求。

# 7、售后服务要求

1. 本项目验收合格后，投标人必须为本项目提供的产品提供不少于1年的质保服务。软件的质保服务包括功能增强性维护和软件升级、免费技术维护服务。
2. 投标人承诺1小时响应、2小时到场，并提供房屋租赁合同。
3. 在实施过程中，要求至少2名现场服务技术人员，提供相关的实施工作。免费维护期内，要求至少1名现场服务技术人员提供驻场服务。
4. 必须提供7\*24小时支持维护服务，包括电话、远程维护、现场服务等方式。必须保证有足够的人员（专人专职）及技术支持电话负责本系统运维工作，并保证2小时内派工程师到达现场/24小时之内解决问题。
5. 对系统软件提供维护服务时应不影响医院医疗业务的正常运行和效率。
6. 今后因国家政策或政府、医院上级部门要求导致的被动性程序修改，投标方应及时提供程序修改服务，并确保系统的在政策要求的时限内正确运行，投标厂家承诺不推诿。

# 8、其他要求

1. 对于采购人提供给各投标方的招标文件和其他业务需求说明文件，投标方有为采购人保密的义务；
2. 中标人应在采购人指定的工作机房内对数据进行处理，不得对用户的数据进行拷贝、备份并带出工作机房，同时不得对外泄露用户数据资料（包括自然人、法人和其他共享数据）的具体内容。否则由此引起的用户损失、相关社会和法律责任，由中标人负责承担；
3. 中标人必须协助用户采取各种管理和技术的手段，确保用户的数据不外传和泄露；
4. 协助用户进行技术方案审理优化、进度质量控制和验收管理的一方，有为用户和包件中标方提供的项目有关文件和技术信息保密的义务。

5、投标人提供的服务，如涉及产品升级、设备更换扩展时不应改变整个系统的结构、通信方式、管理模式，不应破坏应用软件的正常工作环境。

6、投标人应该保证所提供的所有产品或服务皆不侵犯任何第三方的版权、知识产权和其他合法权利。

7、本项目包含社区医院HIS与区级付费一件事平台对接的接口费。

8、该项目用户单位包含社区医院及村卫生室且数量较多，要求投标单位需在医院进行现场操作并且制定实施方案进行项目实施，培训医院相关工作人员操作，便于在进行升级和更新的时候及时发现问题和解决。