# ZHENG FU CAI GOU

# 上海市徐汇区卫生健康委员会2023年区域网络安全和硬件续建政府采购项目

# 招标文件

招标编号：徐采中招2023-154

招标单位：上海市徐汇区政府采购中心

二〇二三年九月

# 总 目 录

# 第一部分 投标邀请

根据《中华人民共和国政府采购法》之规定，上海市徐汇区政府采购中心受采购人委托，就上海市徐汇区卫生健康委员会 2023 年区域网络安全和硬件续建政府采购项目进行国内公开招投标采购，特邀请合格的供应商前来投标。

一、合格的投标人必须具备以下条件：

（1）具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

（2）具有《电子与智能化工程专业承包资质》一级资质（电子资质证书应为有效使用件）；

（3）本项目**不允许**联合投标。

二、项目概况：

1、项目名称：上海市徐汇区政府采购中心——上海市徐汇区卫生健康委员会 2023 年区域网络安全和硬件续建政府采购项目

2、招标编号：（代理机构内部项目编号：徐采中招 2023-154）

3、预算编号：0423-02190

4、项目主要内容及要求：

采购内容：上海市徐汇区卫生健康委员会 2023 年区域网络安全和硬件续建项目主要包括管发中心计算资源集群系统扩容、路由交换网络系统升级改造等 21 项硬件系统集成、徐汇区区域卫生信息系统安全监管平台续建软件开发以及整体安全管理服务和安全运营维护服务等。具体技术要求详见招标文件第三部分。

5、服务地址：徐汇区卫生事业管理发展中心指定地点。

6、项目服务期限：详见招标文件第三部分。

7、采购项目需要落实的政府采购政策情况：根据上海市财政局沪财库[2009]19 号“关于落实政府采购优先购买福利企业产品和服务的通知”要求，本项目在同等条件下优先采购福利企业的产品和服务。同时项目采购应当符合采购价格低于市场平均价格、采购质量优良和服务良好的要求。本项目面向所有企业采购，对小型和微型企业投标人产品的价格给予**10%**的扣除，用扣除后的价格参与评审。其要求标准详见《政府采购促进中小企业发展管理办法》（财库[2020]46 号）中相关规定。

三、招标文件的获取

1、合格的供应商可于 2023-09-27 本公告发布之日起至 2023-10-11 截止，登录“上海政府采购网”（http://www.zfcg.sh.gov.cn）在网上招标系统中获取招标文件。

采购文件上午获取时间：00:00:00~12:00:00

采购文件下午获取时间：12:00:00~23:59:59

2、凡愿参加投标的合格供应商可在上述规定的时间内下载（获取）招标文件并按照招标文件要求参加投标。

注：投标人须保证报名及获得招标文件需提交的资料和所填写内容真实、完整、有效、一致，如因投标人递交虚假材料或填写信息错误导致的与本项目有关的任何损失由投标人承担。

四、投标截止时间及开标时间：

1、投标截止时间：2023 年 10 月 23 日 10:30，迟到或不符合规定的投标文件恕不接受。

2、开标时间：2023 年 10 月 23 日 10:30。

五、投标地点和开标地点

1、投标地点：上海政府采购网（政府采购云平台）http://www. zfcg. sh.gov.cn；根据上海市财政局相关规定，本项目招投标相关活动在上海市政府采购云平台（网址：www.zfcg.sh.gov.cn）进行。政府采购云平台是由市财政局建设和维护。投标人应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。投标人在政府采购云平台的有关操作方法可以参照政府采购云平台中相关专栏的有关内容和操作要求办理。

2、开标地点：上海政府采购网（政府采购云平台）http://www. zfcg. sh.gov.cn；本项目实行网上远程开标，按有关规定在开标时间内无法签到、解密的供应商将被取消投标资格，不纳入评审范围。响应投标的供应商请在开标时间开始后持投标时所使用的数字证书（CA 证书）参加远程开标。

3、开标所需携带其他材料：

本项目实行网上远程开标，按有关规定在开标时间内无法签到、解密的供应商将被取消投标资格，不纳入评审范围。响应投标的供应商请在开标时间开始后持投标时所使用的数字证书（CA 证书）参加远程开标。

六、发布公告的媒介：

以上信息若有变更我们会通过“上海政府采购网”通知，请供应商关注。

七、注意事项：

1、投标单位对招标文件有疑问的可在 2023 年 10 月 7 日上午 10 点整前以书面传真的形式向徐汇区政府采购中心提出，由采购中心负责统一解答。采购中心将于 2023 年 10 月 7 日下午 17 点前通过“上海政府采购网” （http://www. zfcg. sh.gov.cn）公开发布。

2、本项目采购预算为 27000000 元人民币，报价超过采购预算的投标不予接受。

3、投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在电子采购平台上的签收情况，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

八、联系方式

采购人：徐汇区城市网格化综合管理中心

地址：南宁路 969 号

联系人：高卉

电话：24092222*2511

采购代理机构：上海市徐汇区政府采购中心

地址：南宁路 969 号

联系人：曾妮

电话：24092222*2586

# 第二部分 投标人须知

## 一、总则

1、概述

1.1 本招标文件适用于本投标邀请中所述区域网络安全和硬件续建的招标投标。

1.2 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

1.3 根据上海市财政局相关规定，本项目招投标相关活动在上海市政府采购云平台（网址：www.zfcg.sh.gov.cn）进行。

2、定义：

2.1“招标人”指组织本次招标的上海市徐汇区政府采购中心和采购人。

2.2“采购人”指徐汇区卫生事业管理发展中心。

2.3**“招标项目”指本招标文件中第三部分所述相关区域网络安全和硬件续建，本项目属于软件和信息技术服务业**。

2.4“潜在投标人”指符合招标文件规定的合格供应商。

2.5“投标人”指按规定获取招标文件，并按照招标文件要求提交投标文件的供应商。

2.6“上海市政府采购云平台”系指上海市政府采购信息管理平台的门户网站上海政府采购网（www.zfcg.sh.gov.cn），是由市财政局建设和维护。

3、合格投标人的条件

3.1 具有本项目生产、供应或实施能力，符合、承认并承诺履行本文件各项规定的国内法人和其他组织均可参加投标。

3.2 投标人应遵守有关的国家法律、法规和条例，具备《中华人民共和国政府采购法》和本文件中规定的条件：

（1）具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

（2）具有《电子与智能化工程专业承包资质》一级资质（电子资质证书应为有效使用件）；

（3）本项目不允许联合投标。

3.3 只有在法律上和财务上独立运作并独立于采购中心的供应商才能参加投标。

3.4 如投标人代表不是法定代表人，须持有《法定代表人授权委托书》( 统一格式)。

4. 投标费用

4.1 投标人应承担所有与准备和参加投标有关的费用，采购中心和采购人在任何情况下均无

义务和责任承担这些费用。

4.2 本次招标工作由徐汇区政府采购中心自行组织实施，不收取任何中介费用。

**二、招标文件**

5.招标文件的构成

5.1 招标文件是阐明招标的项目范围、投标文件的编写、递交、招标投标程序、评标原则、中标条件和相关的协议条款的文件。招标文件由以下六部分内容组成：

第一部分 投标邀请（招标公告）；

第二部分 投标人须知；

第三部分 招标项目需求；

第四部分 合同参考范本；

第五部分 投标文件格式；

第六部分 评标办法

5.2 投标人应详细阅读招标文件的全部内容。如果投标人没有按照招标文件要求提交全部资料或者没有对招标文件在各方面的要求都做出实质性响应，可能导致其投标被拒绝。

6.招标文件的澄清

6.1 任何通过电子采购平台获取了招标文件的潜在投标人，均可要求对招标文件进行澄清。澄清要求应于投标邀请函所述日期前，按投标邀请书中的联系地址以书面形式（包括书面材料、信函、传真等，下同）送达采购中心，采购中心将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布相关答复。

6.2 采购中心将视情况确定是否有必要召开标前会（现场踏勘）。召开标前会（现场踏勘）的，所有投标人应根据招标文件或者招标人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

7.招标文件的修改

7.1 在投标截止期 15 日以前任何时候，采购中心无论出于何种原因，均可对招标文件用补充文件的方式进行修改。

7.2 对招标文件的修改，将通过“上海政府采购网” （http://www. zfcg. sh.gov.cn）公开发布。补充文件将作为招标文件的组成部分，对所有获取了招标文件的潜在投标人均具有约束力。

7.3 为使投标人有足够的时间按招标文件的修改要求考虑修正投标文件，采购中心可酌情推迟投标的截止日期和开标日期，并将具体变更情况通知上述每一投标人。

8.通知

8.1 对与本项目有关的通知，采购中心将通过“上海政府采购网” （http://www. zfcg. sh.gov.cn）公开发布。

8.2 招标文件的澄清、答复、修改或补充都应由采购中心以澄清或修改公告形式发布，除此

以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，招标人不承担任何责任。

**三、投标文件**

9.投标文件的语言和计量单位

9.1 投标人提交的以及投标人与采购中心就有关投标的所有来往函电均应使用中文简化字。

9.2 投标人所提供的技术文件和资料，包括图纸中的说明，应使用中文简化字。所使用的计量单位，应使用国家法定计量单位。

10.投标文件的组成及相关要求

10.1 投标文件由商务响应文件、技术响应文件两部份构成。

10.2 商务响应文件、技术响应文件所应包含的内容如下：

10.2.1 商务响应文件：

（1）投标函；

（2）投标报价明细表；

（3）设备安装调试集成费报价明细表；

（4）法定代表人证明书和法人代表委托书；

（5）主要产品厂商授权证明；

（6）主要产品检测报告（复印件加盖单位公章）；

（7）投标单位基本情况表及声明；

（8）供应商行贿犯罪记录承诺书；

（9）中小企业声明函；

（10）近三年同类型项目成功案例介绍及最终用户的有效联系方式，附相关采购合同复印件加盖单位公章；

**（11）资格证明文件，包括：投标单位营业执照、税务登记证、《电子与智能化工程专业承包》一级资质（电子资质证书均应为有效使用件）（复印件加盖单位公章）；投标人信用信息查询记录，投标人应当通过“信用中国”网站（www.creditchina.gov.cn）查询投标人主体信用记录（查询截止时点为 2023 年 10 月 20 日），并对查询的信用详情截屏打印并加盖单位公章；投标单位财务状况及税收、社会保障资金缴纳情况声明函。资格证明文件不满足招标要求的，将作为无效投标处理。**

（12）投标产品中属于国家强制性认证的，应提供相应认证证书等相关资料，并提供副本等明细材料以便于评标查阅；（复印件加盖单位公章）；

10.2.2 技术响应文件：

（1）产品选型及说明一览表；

（2）产品规格、技术参数偏离表；

（3）拟从事本项目人员及其技术资格一览表；

（4）硬件系统集成及软件开发设计方案　投标人自行编写的技术方案及图纸，包括但不限于以下内容：系统设计思想、各子系统设计说明、各子系统选用产品介绍（应包括设备及产品材质、原材料产地、规格、加工工艺、主要部件详细描述、质量等级、主要相关特性详细描述）；各子系统拓扑结构图；软件开发产品系统现状分析、设计思路、系统建设方案、功能详细说明以及主要界面和流程图等。

（5）安全服务方案 各项服务按招标需求实施，投标人编制的技术文件应能够证明投标人提供的安全服务是符合招标文件规定的合格的服务，包括但不限于采购项目各服务内容的理解以及投标人完成各服务的具体实施计划、服务流程、方法，人力、物力、技术力量的投入，相关应急预案，服务质量保证措施，成果提交方式、考核验收方案等；对服务满意度的自我考核测量方案以及投标人建议的服务质量检查方法或方案、对投诉处理的控制管理方案等；

（6）项目实施计划　　请投标单位自报项目实施周期，并根据项目实施具体情况制作详细实施周期及针对性施工组织方案、施工管理人员的资质（包括项目经理相关资质证书）、项目组成员工作内容与职责、项目组人员表(列表说明姓名、年龄、性别、学历、职称、从事本分系统工作年限、主要业绩)等项目质量、安全、工期保障措施，以确保项目优质按期安全完工；

（7）投标产品的说明书、产品厂家彩页性能介绍样本（catalog）等技术文件；

（8）售后服务承诺（保修期内售后服务的内容、期限、响应时间、应急保障措施等）及培训等相关伴随服务实施方案；

（9）规章制度一览表；

（10）投标人认为需要提供的其它说明和资料。

10.3 上述文件中凡招标文件提供格式文本的以及要求“加盖单位公章”的材料须上传原件彩色扫描件。

10.4 如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供，否则视作投标人放弃潜在中标资格，并且招标人将对该投标人进行调查，发现有欺诈行为的按有关规定进行处理。

10.5 本项目不接受纸质投标文件。

11.投标内容填写说明

11.1 获取了招标文件的潜在投标人应认真阅读招标文件的所有内容，按照招标文件和电子采购平台电子招投标系统要求的格式填写相关内容。

11.2 投标人必须保证投标文件所提供的全部资料真实可靠，并接受采购中心对其中任何资料进一步审查的要求。

11.3 开标一览表要求按格式统一填写，不得自行增减内容。

11.4 投标文件须对招标文件中的内容做出实质性和完整的响应，否则其投标将被拒绝。如果投标文件填报的内容资料不详，或没有提供招标文件中所要求的全部资料及数据，包括

但不限于第 10 条（投标文件的组成及相关要求）规定的内容，将可能导致投标被拒绝。

12.投标报价

12.1 所有投标报价均以人民币元为计算单位。投标价格应该已经扣除所有同业折扣以及现金折扣，应为考虑所有优惠后的最有竞争性价格，不得再以其他形式进行标后优惠，否则视为不诚信行为记入供应商诚信记录。投标报价应已经包含了购买相关服务的费用和所需缴纳的所有税费，并包含了完成全部服务内容所需的一切费用。

12.2 投标人提供的相关区域网络安全和硬件续建，应当符合国家有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

12.3 投标人应按照招标文件中提供的投标文件格式完整地填写开标一览表、报价明细表和报价构成表等，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

12.4 除招标文件说明并允许外，投标的每一种服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价将可能导致投标被拒绝。

12.5 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均将予以拒绝。

13.投标保证金

本项目不收取投标保证金。

14.投标文件的有效期

14.1 自开标日起 90 天内，投标文件应保持有效。有效期短于该规定期限的投标，将被拒绝。

14.2 在特殊情况下，采购中心可与投标人协商延长投标文件的有效期。这种要求和答复都应以书面形式进行。此时，按本须知规定的投标保证金的有效期也相应延长。投标人可以拒绝接受延期要求而不会被没收保证金。同意延长有效期的投标人除按照采购中心要求修改投标文件有效期外，不能修改投标文件的其他内容。

15.投标文件的签署及其他规定

15.1 组成投标文件的各项文件均应遵守本条。

15.2 投标文件中凡招标文件要求签署、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签署和加盖公章。投标人应写明全称。如果是由法定代表人授权代表签署投标文件，则必须按招标文件提供的格式出具《法定代表人授权书》并将其附在投标文件中。投标文件若有修改错漏之处，须加盖投标人公章或者由法定代表人或法定代表人授权代表签字或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

15.3 投标人应按招标文件和电子采购平台电子招投标系统规定的内容、格式和顺序编制投标文件。凡招标文件提供有相应格式的，投标文件均应完整的按照招标文件提供的格式打印、填写并按要求在电子采购平台电子招投标系统上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

15.4 用于网上招投标系统上传的扫描件等有关文件应确保清晰、可辨，投标人上传文件的

电子数据量不应过大，因数据量过大导致无法正常投标、开标的，投标人将自行承担其责任后果，招标人不承担任何责任。

**四、投标文件的递交和解密（开标）**

16.投标文件的递交和解密

16.1 投标单位在制作投标文件后应在上传投标文件截止时间之前在上海政府采购网上将电子投标文件加密上传。

16.2 举行开标会时，各投标供应商须带好本单位的 CA 证书及可以无线上网的笔记本电脑，按照规定的开标时间和地点到场后登陆上海政府采购网集中解密。按有关规定当场无法解密的供应商将被取消投标资格，不纳入评审范围。

16.3 在投标文件解密之后，投标人不得撤回投标。投标后撤回投标文件的行为将被记录在案，投标人今后参与同类政府采购项目的机会可能会受到影响.

17.投标截止时间

17.1 投标文件须按照招标文件规定的投标时间、地点解密。

17.2 采购中心推迟投标截止时间时，将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。在这种情况下，采购中心和投标人的权利及义务将受到新的截止期的约束。

**五、评标**

18.评标

18.1 采购中心根据有关法律法规和本招标文件的规定，结合本招标项目的特点组建评标委员会，对具备实质性响应的投标文件进行评估和比较。评标委员会由采购人、技术、经济、法律专家和其他有关方面的代表组成。

18.2 评标原则

（1）评标应严格按照招标文件的要求和条件进行；

（2）评标委员会只对实质上响应招标文件的投标进行评价和比较；

（3）评标委员会分别对每包进行独立评标，每包只限确定一家供应商为中标单位，但一家供应商可以中一包或多包；

（4）评标委员会在评标时除考虑投标报价因素外，同时还根据各项技术和服务因素对投标人和投标服务进行综合评价。

18.3 评标办法：本项目采用综合评分法，各评标因素所占权重见第六部分评标办法。

**19. 对投标文件的初审**

19. 1 开标后，采购中心将组织对投标文件进行资格性检查，依据法律法规和招标文件的规定，对投标文件中的资格证明、投标保证金等进行审查，以确定投标供应商是否具备投标资格。

19. 2 在详细评标之前，评标委员会对通过资格性检查的投标文件进行符合性检查，依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定

是否对招标文件的实质性要求作出响应。

（1）实质上响应的投标是指与招标文件的全部条款、条件和规格相符，没有重大偏离或保留。

（2）重大偏离或保留系指投标人货物的质量、数量和交货期限等明显不能满足招标文件的要求，或者实质上与招标文件不一致，而且限制了采购中心的权利或投标人的义务，纠正这些偏离或保留将对其他实质上响应要求的投标人的竞争地位产生不公正的影响。

（3）重大偏离不允许在开标后修正，但采购中心将允许修正投标中不构成重大偏离的地方，这些修正不会对其他实质上响应招标文件要求的投标人的竞争地位产生不公正的影响。

（4）如果实质上没有响应招标文件的要求，评标委员会将予以拒绝，投标人不得再对投标文件进行任何修正从而使其投标成为实质上响应的投标。

19.3 初审中，投标文件中如果有下列计算或表达上的错误或矛盾，将按以下原则或方法进行修正；其他错误或矛盾将按不利于出错投标人的原则进行修正：

（1）开标一览表内容与报价明细表及投标文件其他部分内容不一致的，以开标一览表内容为准。

（2）如果以文字表示的数据与数字表示的有差别，以文字为准修正数字。如果大小写金额不一致的，以大写金额为准。

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

（4）修正后的结果应对投标人具有约束力，投标人不同意以上修正，其投标将被拒绝。

19.4 评标委员会对投标文件的判定，只依据投标文件内容本身，不依据任何外来证明。

20.投标的澄清

20.1 评标委员会有权要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容等作必要的澄清、说明或者补正。投标人必须按照评标委员会通知的澄清内容和时间做出澄清。必要时评标委员会可要求投标人就澄清的问题作书面答复，该答复经投标人的法定代表人或投标人代表的签字认可，将作为投标文件内容的一部分。澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

20.2 如评委会一致认为某个投标人的报价明显不合理，有降低质量、不能诚信履行的可能时，评标委员会有权通知投标人限期进行解释。若该投标人未在规定期限内做出解释，或作出的解释不合理，经评标委员会取得一致意见后，可拒绝该投标。

21.评标过程保密

21.1 开标之后，直到授予投标人合同止，凡是属于审查、澄清、评价和比较投标的有关资料以及授标意向等，均不向投标人或其他与评标无关的人员透露。

21.2 在评标期间，投标人企图影响采购中心或评标委员会的任何活动，将导致投标被拒绝，并由其承担相应的法律责任。

## 六、授予合同

22.合同授予标准

22.1 买方将把合同授予符合招标文件的要求，并能圆满地履行合同的，对买方最为有利的得分最高的投标方。

22.2 最低报价不是被授予合同的保证。

23. 买方接受和拒绝任何或所有投标的权利

买方保留在授标之前任何时候接受或拒绝任何投标，以及宣布招标程序无效或拒绝所有投标的权利，对于受影响的投标人不承担任何责任，也无义务向受影响的投标人解释采取这一行动的理由。

24. 采购中心宣布废标的权利

24.1 出现下列情况之一时，采购中心有权宣布废标，并将理由通知所有投标人：

（1）符合专业条件的投标人或者对招标文件作实质性响应的投标人不足三家的；

（2）出现影响采购公正的违法、违规行为的；

（3）投标人的报价均超过了采购预算，采购人不能支付的；

（4）因重大变故，采购任务取消的。

24.2 有下列情况之一的投标文件，将做无效投标处理：

(1) 投标文件无法按规定解密；

(2) **不具备招标文件中规定的资格要求的；**

(3) **投标报价不按招标文件规定的计价办法投报或超过招标文件规定的预算金额或投标最高限价；**

(4) **投标文件未按招标文件要求签署、盖章的；**

(5) 未按规定格式填写,内容不全或字迹模糊,辨认不清；

(6) 经行贿犯罪档案查询，被政府采购监督管理部门禁止参加政府采购活动的；

(7) **经信用信息查询，投标供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；**

(8) 不同投标人的投标文件出现了评标委员会认为不应当雷同的情况；

(9) 投标人递交两份或多份内容不同的投标文件，按招标文件规定提交备选投标方案的除外；

(10) 投标文件未对招标文件作出完全的、实质性响应,导致投标无效；

(11) 投标文件含有采购人不能接受的附加条件的；

(12) 因不可抗力造成投标文件遗失或损坏的。

25.中标通知

25.1 评标结束后，采购中心将向中标单位签发《中标通知书》,《中标通知书》一经发出即发生法律效力。

25.2 采购中心同时通过指定网络发布评标结果公告。采购中心对未中标的投标人不作未中标原因的解释，不退还投标文件。

25.3 中标通知书是合同的组成部分。

26. 签定合同

26.1 中标人应按采购中心规定的时间、地点与采购人签定中标合同。中标人不得再与采购人签署订立背离合同实质性内容的其它协议或声明，否则按开标后撤回投标处理。

26.2 中标人应按照招标文件、投标文件及评标过程中有关的澄清文件的内容与采购人签订合同。

26.3 投标人一旦中标，签订合同后，未经监管部门书面同意不得转包，否则将被视为中标后撤回投标处理。

27. 履约保证金

27.1 中标人在总合同签定后十五（15）天内，应按照合同条款的规定，按照招标文件中提供的履约保证金格式向买方提交履约保证金。

27.2 如果中标人没有按照投标人须知第 26 条、第 27.1 条规定执行，买方将有充分理由取消原中标决定并没收其投标保证金。在此情况下，买方可将该标授予下一个综合评标得分最好的投标人，或重新招标。

28. 腐败和欺诈

28.1“腐败行为”是指提供、给予、接受或索取任何有价值的东西来影响采购人员在采购过程或合同实施过程中行为;“欺诈行为”是指为了影响采购过程或合同实施过程而谎报事实，损害采购人的利益，包括投标人之间串通投标（递交投标书之前或之后），人为地使投标丧失竞争性，损害采购人从自由公开竞争中所能获得的权益。

28.2 如果买方认为所建议的中标人在本合同的竞争中有腐败和/或欺诈行为，则将拒绝该授标建议。

**七、中标服务费**

29. 中标服务费

**29.1 本次招标不收取中标服务费，请投标人在测算投标报价时充分考虑这一因素。**

**八、询问和质疑**

**30 询问和质疑**

30.1 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

30.2 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知

道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，对招标文件的质疑，应当在其收到或下载招标文件之日起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。投标人提出质疑应当坚持依法依规、诚实信用原则，并应在法定质疑期内一次性提出针对同一采购程序环节的质疑。

30.3 质疑函应明确阐述招标文件、招标过程或中标结果中使自己合法权益受到损害的实质性内容，具体、明确的质疑事项和与质疑事项相关的请求，提供相关事实依据、必要的法律依据和证据及其来源或线索，以便于有关单位调查、答复和处理。

30.4 招标人将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人和其他有关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

30.5 对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的，招标人将通知提出询问或质疑的投标人，并在原招标公告发布媒体上发布变更公告。

30.6 投标人提起询问和质疑，应当按照《徐汇区政府采购中心质疑答复处理规程》的规定办理。质疑函应当由质疑供应商法定代表人签字并加盖公章。质疑函应当按照财政部制定的范本填写，范本格式可通过中国政府采购网（http://www.ccgp.gov.cn）右侧的“下载专区”下载。质疑供应商委托代理人办理质疑事务的，应当向徐汇区政府采购中心提交供应商法定代表人签署的授权委托书和身份证明。质疑函的递交可以采取邮寄、快递或当面递交形式。涉及采购需求技术内容的质疑，请向徐汇区卫生事业管理发展中心提出，联系人：张楠，联系电话：54012831，通讯地址：永川路 50 号 307 室；其余质疑内容请向徐汇区政府采购中心提出，接收质疑函的联系人：柳老师，联系电话：021-24092222*2591，通讯地址：上海市南宁路 969 号。

**九、保密和披露**

31. 保密和披露

31.1 投标人自领取招标文件之日起，须承诺承担本招标项目下保密义务，不得将因本次招标获得的信息向第三人外传。

31.2 采购中心有权将投标人提供的所有资料向其他政府部门或有关的非政府机构负责评审标书的人员或与评标有关的人员披露。

31.3 采购中心有权在认为适当时，或在任何第三人提出要求（书面或其他方式）时，无须事先征求中标人同意而披露关于已订立合同的资料、中标人的名称及地址、中标货物的有关信息以及合同条款等。

# 第三部分 招标项目需求

## 一、项目概述

1.1 项目名称

项目名称：上海市徐汇区卫生健康委员会 2023 年区域网络安全和硬件续建项目

项目建设单位：上海市徐汇区卫生事业管理发展中心（以下简称“管发中心”）

1.2 项目背景

区卫健委下属的管发中心及徐汇区区级医院，社区卫生服务中心等单位，在信息系统基础设施及信息安全建设方面经过多年的建设完善，已经具有了一定的坚实基础。根据近 2 年的信息安全等级保护测评工作的开展和日常运行维护中的实际情况，发现现有各系统仍存在如部分设备使用年限较长，功能授权临期，整体安全防护能力及架构尚有薄弱部分，信息系统运维监管分散等问题。针对现有问题，整合 2022 年与 2023 年共 2 年度的建设需求，提出本项目，通过对区域内各系统的进行续建以针对性解决问题，提升整体网络安全防护能力。

1.3 项目建设目标

依据《关于印发医疗卫生机构网络安全管理办法的通知》（国卫规划发〔2022〕29 号）、关于转发《关于印发〈关于加强本市网络数据安全工作的指导意见〉的通知》（沪卫信息便函〔2022〕62 号）等通知要求，通过对管发中心及下属各单位的信息相关系统软硬件设备进行增补和更替集成，实现系统在未来五年内具备技术先进性，费用合理性，规划可延性，使用高效性，功能完整性的目标。同时，在网络安全管理服务上采购专业的信息技术运维服务团队对系统、设备、数据等安全进行规范管理，实现信息系统管理能力的整体提高。

通过进一步开发建设安全监管平台体系，做到主动发现、提前预警，帮助区卫健委全面掌握网络管理事态，提升整体网络安全全局洞察力，有效应对新型、高级安全威胁，实时了解和感知攻击状况，降低运维难度提升管理效率，协助区卫健委在整体医疗系统网络安全管理方面进一步提升和改变。

## 二、项目建设内容

本次招标为上海市徐汇区卫生健康委员会2023年区域网络安全和硬件续建项目提供硬件集成、软件开发及安全服务，并包括相关以及材料供货、安装、设备测试、系统集成、试运行、建设方相关人员的培训、质量保证期内免费保养维修等内容。

本项目内容主要包括以下三大类：

- 硬件系统集成类

- 软件开发类
- 安全服务类

2.1 硬件系统集成类

1、管发中心计算资源集群系统扩容

2、管发中心路由交换网络系统升级改造

3、管发中心网络安全系统续建

4、管发中心异地灾备机房系统升级改造

5、管发中心内外网文件摆渡系统建设

6、“徐汇区区域卫生信息平台”业务专线系统升级改造

7、徐汇区疾病预防控制中心信息系统升级改造

8、徐汇区中心医院信息安全系统升级改造

9、徐汇区大华医院信息安全系统升级改造

10、徐汇区妇幼保健所信息系统升级改造

11、徐汇区徐家汇街道社区卫生服务中心信息屏系统建设

12、徐汇区斜土街道社区卫生服务中心 HIS 业务服务器集群系统升级改造

13、徐汇区田林街道社区卫生服务中心信息系统升级改造

14、徐汇区天平街道社区卫生服务中心网络系统升级改造

15、徐汇区龙华街道社区卫生服务中心服务器系统升级改造

16、徐汇区凌云街道社区卫生服务中心信息系统升级改造

17、徐汇区湖南街道社区卫生服务中心信息系统升级扩容

18、徐汇区枫林街道社区卫生服务中心计算资源系统升级改造

19、徐汇区漕河泾街道社区卫生服务中心信息系统升级改造

20、徐汇区华泾镇社区卫生服务中心信息系统升级改造

21、徐汇区区域卫生信息系统安全监管平台续建配套硬件采购

2.2 软件开发类

1、徐汇区区域卫生信息系统安全监管平台续建

2.3 安全服务类

1、整体安全管理服务

2、安全运营维护服务

**三、硬件系统集成需求**

硬件系统集成需求类部分所涉及的各项目内容中，工作量清单中所涉及的硬件设备，均需要包含设备安装上架、开局配置等基础部署工作并在实施过程中提供设备使用、配置、维护等文件，包括但不限于用户手册、配置手册、维护手册、测试及试运行报告等。其他集成要求在各部分的系统需求中及工作量清单中列出。

投标人提供的产品中，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术网络安全专用产品安全技术要求》等国家标准的强制性要求，提供具备资格的机构安全认证合格或安全检测符合要求的相关证明文件。

**3.1 管发中心计算资源集群系统扩容**

3.1.1 系统说明

计算资源集群系统包含物理计算服务器，虚拟化资源池服务器，SAN 存储设备，SAN 存储交换机等设备，负责运行及承载管发中心各业务的应用服务器，数据库服务器，虚拟机服务器等业务所需的服务端操作系统及软件。是管发中心数据中心提供信息化服务的核心系统。

系统内现有的部分计算资源服务器及数据存储已经到达使用年限，性能及容量等参数无法满足当前业务增长和发展的需求。需要集成部署新的计算集群资源，与现有计算资源系统整合集成，以实现业务计算资源系统扩容升级，满足业务需求。

3.1.2 系统需求

1、采用 4 台机架式服务器组成共享存储集群作为数据库服务器使用。集群网络层独立架设与现有系统不相接，SAN 存储层采用共享方式部署。

2、采用 4 台机架式服务器，采用四节点融合部署，作为虚拟化资源池服务器使用。该计算资源集群需要与现有计算资源系统整合，存储网络资源合并。投标人需负责对硬件设备的安装部署及现有虚拟化资源池与新虚拟化资源池的集成和存储网络对接工作，需要拟定合理集成方案以保障现有业务的持续性和稳定性。

3、并部署 1 套 SAN 存储系统及 2 台 SAN 存储交换机，对现有 SAN 存储系统进行扩容。SAN 存储网络与现有 SAN 存储网络进行对接。投标人需负责对原 SAN 存储网络中的各项配置，如 FC ZONE 配置，FC 端口角色配置等进行充分梳理排查，确保 SAN 网络对接后现有业务数据，卷，分区等设置无冲突，并保证存储系统与服务器之间的 FC 链路兼容性，确保集成后不影响业务系统及业务数据正常稳定运行。

3.1.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 机架式服务器（计算资源） | 硬件规格 | 处理器：每台节点配置 2 颗 CPU ，采用 2.0GHZ(28C）或以上的 CPU | 4 | 台 |
| | | | 内存：每台服务器内存≥512GB | | |
| | | | 接口：每台服务器配置≥6 个千兆电口，万兆光口≥2 个 | | |
| | | | 存储：每个节点配置 128G SATA≥2 块，1.92T-SSD≥2 块， ，8T 机械硬盘≥6 块 | | |
| | | 内建安全要求 | 云安全中心需集成于虚拟化平台中，一体化方式交付，无需第三方平台承载，平台必须能够提供虚拟主机安全防护安全能力，并对检测到的恶意活动可自动采取分布式防火墙隔离虚拟机、为虚拟机拍摄快照等防护手段（需提供产品界面截图） | | |
| | | 云计算平台要求 | 支持大屏展示便于客户直观查看虚拟化资源池的使用情况和健康状态，包括集群资源情况，各主机资源使用情况，存储资源池的 IO 次数、IO 速率、IO 时延、存储命中率、主机命中率，以及集群故障与告警，支持 Top 5 主机 CPU 和内存利用率、Top 5 虚拟机 CPU 和内存利用率信息大屏展示等 | | |
| | | | 支持跨地域的多集群管理，可纳管不少于 256 个物理机节点，支持不少于 30000 台云主机的规模 | | |
| | | | 支持主备切换，当主平台发生故障时，能够切换到备平台，保障云平台稳定运行 | | |
| | | | 支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件 | | |
| | | | 云计算管理平台，和底层资源池部分可以支持扩展网络和安全虚拟化（虚拟应用防火墙、虚拟应用负载均衡等）功能组件，以保障平台的扩展性和兼容性 | | |
| | | 计算虚拟化要求 | 虚拟化软件非 OEM 或贴牌产品，禁止借用第三方软件的整合，以保证功能的可靠性和安全性 | | |
| | | | 支持对平台的硬件进行监控和大屏展示，包含 CPU，内存，网卡，硬盘，存储，RAID 等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议 | | |
| | | | 支持一键还原已删除的虚拟机，可恢复 30 天内已删除的虚拟机。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 为避免主机假死导致系列问题发生，支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险 | | |
| | | | 虚拟化的管理平台、可以支持扩展存储虚拟化、网络功能虚拟化、虚拟应用防火墙、虚拟应用交付、SSL VPN 软件、数据库审计软件等功能组件的，并支持统一管理，以保障平台的扩展性和兼容性（需提供产品功能截图） | | |
| | | | 需支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用 License 激活的方式开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能。 | | |
| | | | 支持为虚拟磁盘配置不同的存储策略以满足特定场景的需求， 如系统盘和数据盘选择高性能策略， 备份盘选择低性能策略 | | |
| | | | 支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性 | | |
| | | 软件授权 | 提供计算虚拟化、网络虚拟化、存储虚拟化软件授权 | | |
| 2 | 机架式服务器（数据库） | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 4 | 台 |
| | | CPU 规格 | ≥4 颗 Intel Xeon SP 5318H(2.5GHz/18 核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥512GB DDR4 3200 内存模块 | | |
| | | 内存可扩展数量 | 本地提供≥48 个内存槽位，最大支持 18TB 物理内存,12TB 有效内存,支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘实配规格 | ≥4 块 960GB SSD 硬盘，热插拔；支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 本地提供≥8 个 2.5 寸硬盘槽位，支持≥48 块 2.5 寸热插拔硬盘。 | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆电网卡，≥1 张 2 端口 16GB FC HBA 卡（含模块），≥2 张 2 端口万兆光网卡（含模块） | | |
| | | 冗余电源 | ≥4 个 1200W 铂金版热插拔冗余电源；支持 1+1/N+N 冗余；支持 240VDC，380VDC，48VDC | | |
| | | 冗余风扇 | 热插拔冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块，提供防火墙、IPS、防病毒和 QoS 等安全防护功能。 | | |
| 3 | SAN存储系统 | 硬件架构 | 多控制器架构，多个控制器之间采用 PCI-E 总线点对点全网状直接互联，非外置线缆模式互联，非万兆网络或 FC 链路互联模式； | 1 | 台 |
| | | | 每个存储控制器架构相同且处理能力均衡，对于单一 LUN，多个控制器可以并行读写。 | | |
| | | | 配置≥2 个存储控制器。（不包括外接虚拟化网关或者 NAS 控制器等） | | |
| | | | 支持控制器在线升级，可在不更换控制器机框及不搬移硬盘的情况下将控制器升级至同系列存储任意其他控制器型号，实现容量和性能的在线升级，而无需数据迁移。 | | |
| | | 存储处理器 | 每个控制器配置 2 颗处理器。 | | |
| | | | 支持处理器升级，可在不更换控制器机框及不搬移硬盘的情况下对每个控制器的处理器进行升级，实现控制器处理器内核数的提升，无需数据迁移。 | | |
| | | 硬件规格 | 支持 16Gbps/32Gbps FC，10GbE/25GbE 接口等，支持≥16 个主机端口；配置≥2 张 4 端口 16Gbps FC HBA 卡 | | |
| | | 高速缓存 | 双控配置≥256GB 高速缓存 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持缓存升级，可在不更换控制器机框及不搬移硬盘的情况下对每个控制器的缓存升级至不少于 1TB,双控制器时最大可支持 2TB 缓存，实现控制器缓存的升级，无需数据迁移。 | | |
| | | | 数据缓存和控制缓存逻辑分离，读写缓存比例动态自适应调整，缓存刷新在线动态自适应调节。 | | |
| | | 磁盘配置 | 配置≥16 块 1.92TB 企业级 SAS SSD 硬盘 | | |
| | | 硬盘类别 | 支持 SAS SSD、SAS HDD、NLSAS HDD 等类型硬盘，支持混配 | | |
| | | 磁盘扩展 | 支持拓展到不少于 700TB 的有效存储容量 | | |
| | | RAID 级别 | 支持 RAID6/60 及以上 RAID 级别 | | |
| | | | 支持多类型磁盘多方向、无中断在线数据迁移，迁移过程不影响业务性能。 | | |
| | | | 具备去零功能，提高空间利用率。 | | |
| | | 高速磁盘故障恢复 | 采用高速多对多磁盘故障恢复方式，提高恢复速度的同时，可保证磁盘复期间应用的性能。 | | |
| | | | 无专用指定热备盘，重建全局并发。 | | |
| | | 智能资源池 | 存储可以根据当前配置（控制器，硬盘，扩展柜等）并依据最佳实践智能自动地创建存储资源池，确保最佳实践并减少人为操作的非最佳实践或操作失误的风险，此过程无需任何人工干预。 | | |
| | | 智能管理运维平台 | 配置图形界面管理软件，支持多种语言（至少包括简体中文和英文），支持多台设备集中管理，支持存储资源管理分析和资源使用历史记录分析，支持 WEB 管理，支持 CLI 管理。支持多种事件通知功能 | | |
| | | | 配置客户自助服务功能，存储具备简便的操作及运维功能，允许客户自行安装/更换/修复存储设备，简化运维复杂度。 | | |
| | | | 配置应用负载 IO 检测功能，可实现应用负载 IO 数据块结构检测，清晰展示不同数据块的存储数量，并依据应用负载 IO 数据块的规律呈现曲线图，IO 数据块粒度支持 4K，8K，16K，32K，64K，128K，256K，512K，可直观展示应用负载 IO 的特点、规律及压力，从而为每一个应用负载分配合理的资源。提供相关证明材料 | | |
| | | | 配置存储能力预测功能，可根据目前存储负载情况及现有配置情况，预测存储未来若干天的性能趋势，让存储性能变得可以预测和控制 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 配置应用上线计划功能，当需要增加一个或若干个应用时，可以在创建应用卷时展示出所有存储的负载情况及未来性能预测，从而可以无风险的选择应用部署的存储，让用户每个业务的整合都能提前知道结果 | | |
| | | | 配置智能管理运维平台，提供基于机器学习及大数据分析的智能管理运维技术，实时进行容量分析、性能趋势分析和健康状况检查等，并提供可用性预测、自动预警、健康预警和自动生成建议报告；实现端到端的应用分析，精准定位主机及虚拟机到存储之间的瓶颈所在，准确发现故障源并给出处理及修复建议，此功能无容量限制。 | | |
| | | LUN 数量 | 存储提供双控可设置 LUN 数量≥6 万个。 | | |
| | | LUN 应用属性 | 存储具备为 LUN 赋予不同的应用种类，可对存储上的 LUN 标注相应的业务应用，并对应用 LUN 集进行性能统计和监控，按照应用的维度展示性能分析视图。可支持应用种类不少于 8 个，包括 Oracle、SQL、VMWare ESXi、Exchange、Hyper-V、DB2、SharePoint、SAP HANA 等 | | |
| | | 克隆 | 配置全容量许可的克隆功能，后续扩容无需额外购买许可。 | | |
| | | 快照 | 配置全容量许可快照功能，有效预防各种软故障的发生，快照无需预留空间，后续扩容无需额外购买许可 | | |
| | | 数据保护 | 支持将快照直接备份到二级存储或者服务器上。 | | |
| | | | 支持二级存储/服务器上所备份的快照恢复到原磁盘阵列或其他磁盘阵列。 | | |
| | | | 支持硬盘扩展柜保护功能，当配置多个硬盘扩展柜时，可支持至少一个硬盘扩展柜掉电或故障时数据不丢失，应用不中断。 | | |
| | | QoS | 支持存储 QoS 授权许可，支持单卷和分区的 IOPS 上限和下限、Bandwidth 上限和下限、Response Time 设定（RT 最小 0.5ms）。 | | |
| | | 资源监控和预测 | 配置性能监控和分析软件，配置高级图形化报表软件，可以定制历史运行数据的图形化报表。 | | |
| | | | 提供基于虚拟机环境下的细粒度性能监控功能，可在存储管理界面下实时监测存储中每一个虚拟机的性能状态（图吞吐量、IOPS 及时延） | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 综合能力洞察 | 存储设备可通过自身的配置、性能、容量、业务压力及类别等信息计算出当前存储的综合能力，并通过计算分析展示当前业务的综合能力使用比。并可通过与云端数据中心的机器学习和智能计算相结合，不断地从云端修正和更新此综合能力，提供精准的存储能力预测服务。 | | |
| | | 高级性能管理 | 存储具备高级性能管理功能，不仅可以对存储整体、LUN 应用集合进行性能实时监控，展示其带宽、IOPS、时延的实时状态，并对热点卷排序；还可对性能问题给予分析和并展示影响当前性能的因素，快速精准进行性能管理。 | | |
| | | 重删压缩 | 配置全容量许可的在线重删压缩功能，可对指定 LUN 进行开启或关闭操作，后续扩容无需额外购买许可 | | |
| | | 远程复制 | 配置于同厂商高端型号以及全闪存阵列间实现存储底层复制，包括远程复制和可在线迁移卷。 | | |
| | | | 配置全面的企业级容灾功能，至少必须包含同步、异步周期主流模式 | | |
| | | 存储双活 | 支持并配置存储双活功能，在不加额外网关的情况下可以实现和同厂商中端和高端型号存储组成双活阵列，在一台阵列故障的情况下，主机 IO 访问可以无缝切换到另外一台阵列而不会中断业务，要求支持 VMWare、Windows Server、MS Hyper-V 和 Oracle RAC 等。 | | |
| | | 数据在线迁移 | 在不加额外网关的情况下可以实现和同厂商的高中端存储和全闪存存储的在线数据迁移，数据可以在多台存储之间按照性能、容量等策略进行在线数据迁移，迁移过程中业务可连续运行，对于主机平台透明。 | | |
| | | 存储 OS 在线升级 | 支持控制器在线升级存储操作系统，在存储操作系统更新补丁，更新数据服务模块时无需控制器切换且无需重启任何一个控制器即可实现在线升级，对上层应用透明。 | | |
| | | 操作系统 | 支持 Windows、Linux、VMware、UNIX（HP-UX、AIX、Solaris）等主流操作系统 | | |
| 4 | SAN存储交换机 | 硬件架构 | 无拥塞架构设计，所有 FC 端口全线速 | 2 | 台 |
| | | 硬件规格 | 最大可扩展端口≥48 个；实配≥48 个 16Gb FC 端口的授权，实配≥48 个 16Gb FC 多模模块以及相关光纤线缆 | | |
| | | 端口速率 | 同时支持 FC 128Gb/s，32Gb/s，16Gb/s，10Gb/s， 8Gb/s 和 4Gb/s 速率 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 端口类型 | 同时支持 F/E/M/D/EX 等端口类型 | | |
| | | 互联扩展 | 可支持多台交换机级联和 Fabric 扩展 | | |
| | | 链路捆绑 | 支持基于数据帧级的“即插即用”的链路捆绑功能，单个链路聚合带宽最大 256G | | |
| | | 系统延时 | 平均延迟≤2.1 微秒 | | |
| | | 监控管理 | 支持 SNMPv1/v3 的集中监控管理 | | |
| | | 安全性 | 支持数据的压缩及加密、基于数据帧级别的前向纠错和交换机接入认证功能 | | |
| | | 诊断 | 提供基于 D-Port 的端口自诊断功能，包括电/光环回、链路流量、延时和距离 | | |
| | | 管理功能 | 具备免费的 HTTP 方式的交换机管理并支持端口性能监控，参数修改等功能 | | |
| | | 冗余性要求 | 风扇电源等部件均可热插拔并支持在线升级微码 | | |

**3.2 管发中心路由交换网络系统升级改造**

3.2.1 系统说明

管发中心路由交换网络系统，整体架构包含核心交换层，区域汇聚层及接入层三层设计，负责承载管发中心从数据机房到桌面终端之间的以太网络数据路由交换，是管发中心各业务系统的数据传输交互骨干。

其中核心交换层负责对各安全区域间的数据进行基础三层路由及交换转发，各区域汇聚层负责各安全区域的三层网关边界及区域间三层路由详细规则控制，各接入层负责相应设备接入网络及 VLAN 隔离控制。实现整体网络的高效运转。

现有路由交换网络系统部分设备性能已不满足使用需求，需要采用新设备对现有路由交换网络系统进行设备集成，通过替换新设备使网络满足性能需求。投标人应进行现场配置梳理及网络配置结构调研，并根据现场调研结果拟定合理的集成方案，对路由交换网络进行设备替换的实施准备，实施时需保障现有业务的持续性。

3.2.2 系统需求

1、采用 2 台核心交换机设备对现有的 2 台内网核心交换机设备进行替换，用以补足现有系统中核心交换层的路由交换性能。

2、采用 2 台具有高带宽性能的服务器区 48 端口汇聚交换机，建设独立的计算资源池服务器汇聚。服务器汇聚交换机作为服务器间数据交换的核心节点，需要带有不少于 2 个 QSFP+接口以满足计算资源集群系统对数据交互的高带宽需求。

3、采用 6 台 48 端口汇聚交换机，每 2 台作为以太网 L3 汇聚交换机，分别用于建设独

立的外网汇聚区域、外部专线接入区、内网安全加固区三个安全区。外网、专线及安全管理区汇聚交换机应尽可能选用同样的型号以便于维护，需要满足不少于 4 个 SFP+上行端口实现将原有网络系统中的区域设计细化，相关业务数据流分区运行。现有相关设备需要割接移动至建设后的新安全区域中。

4、对以上共 4 组汇聚交换机采用三层网络对接模式进行配置，与核心交换机之间进行对接，同时需要设计应用相应的安全区域之间的路由交换安全策略。

5、配套采购所需要的光 SFP 模块，用于上述网络设备间光纤链路的连接。

3.2.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 核心交换机 | 性能要求 | 交换容量≥380Tbps，包转发率≥72000Mpps。 | 2 | 台 |
| | | 硬件规格 | 业务插槽数≥6，主控引擎模块≥2，每台设备配置双主控，双交换网板，双电源，双风扇；配置 2 块 48 端口万兆光板卡，2 块 48 端口千兆电板卡（需含 1 根万兆堆叠电缆，16 个万兆多模光模块） | | |
| | | 接口要求 | 支持千兆电口，千兆光口，万兆光口、万兆电口、25G 端口、40G 端口、100G 端口。 | | |
| | | | 支持单槽位万兆电端口密度≥48，单槽位万兆端口密度≥48；单槽位 40G 端口密度≥ 16，单槽位 100G 端口密度≥16。 | | |
| | | 链路聚合 | 支持 DRNI 跨设备链路聚合，支持对广播、组播、单播报文的均匀分担 | | |
| | | QOS | 每端口支持 8 个优先级队列,3 个丢弃优先级，支持 SP、WRR、SP+WRR 三种队列调度算法 | | |
| | | | 支持流量整形 Shapping | | |
| | | 堆叠 | 支持 4 框虚拟化技术,支持 16 条 40G/100G 堆叠链路，堆叠带宽能达到双向 3.2T | | |
| | | 智能网管 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级 | | |
| | | 可靠性 | 支持 INQA 功能，通过直接对业务报文进行标记的方法，实现对网络级和设备级的丢包统计 | | |
| | | | 支持主控板冗余，倒换时间为 0ms | | |
| | | | 支持 NSF/GR for OSFP/BGP/IS-IS | | |
| | | | 支持热补丁功能，可在线进行补丁升级 | | |
| | | 可视化 | 支持 Telemetry 流量可视化功能 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 融合 | 支持融合 AC 功能：无需额外配置单独硬件，并能在交换机上对所有上线的 AP 进行管理与配置 | | |
| | | MPLS | 支持 L3 VPN，支持 VLL，支持 VPLS | | |
| | | 安全特性 | 支持全端口 MACsec 加密技术，密钥长度为 256bit，支持可信计算：支持设备可信自检、证书签发功能 | | |
| | | NAS | 支持 802.1x 认证， 支持 mac 认证， 支持 IPv4 Portal、IPv6 Portal 及 Portal 双协议栈功能 | | |
| 2 | 汇聚交换机-48端口（服务器） | 硬件规格 | 支持 48 个 1/10G SFP Plus 端口,2 个 QSFP+端口，2 个扩展插槽，配置双电源双风扇。 | 2 | 台 |
| | | 性能要求 | 交换容量≥2.5Tbps，包转发率≥1000Mpps。 | | |
| | | VxLAN | 支持 VxLAN 二层网关，支持 VxLAN 三层网关，支持 EVPN | | |
| | | 性能指标 | MAC 地址表≥128K<br>路由表容量≥64K<br>ACL≥2K | | |
| | | 智能管理 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级 | | |
| | | ERPS | 支持 ERPS 功能，并且收敛时间小于 50ms | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN； | | |
| | | 镜像 | 支持本地端口镜像和远程端口镜像 RSPAN、支持流镜像 | | |
| | | 路由协议 | 支持 IPv4 静态路由；支持 IPv6 静态路由；支持 IPv4 和 IPv6 环境下的策略路由 | | |
| | | MPLS | 支持 MPLS L2VPN 功能；支持 MPLS L3VPN 功能；支持 MPLS SR 功能 | | |
| | | 可靠性 | 支持 BFD FOR VRRP 功能，支持 RRPP，支持 PVST 功能 | | |
| | | | 支持 Smartlink,支持 RSTP 功能,支持 MSTP 功能； | | |
| 3 | 汇聚 | 性能要求 | 交换容量≥430Gbps，包转发率≥160Mpps。 | 6 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 交换机-48端口（外网、专线、安全管理区） | 硬件规格 | 支持 48 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口，配置双电源 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 4 | 千兆单模光模块 | 硬件规格 | 光模块-SFP-GE-单模模块-(1310nm,10km,LC) | 2 | 个 |
| 5 | 千兆多模光模块 | 硬件规格 | 光模块-SFP-GE-多模模块-(850nm,0.55km,LC) | 96 | 个 |
| 6 | 万兆多模光模块 | 硬件规格 | 光模块-SFP+-10G-(850nm,300m,LC) | 106 | 个 |

### 3.3 管发中心网络安全系统续建

3.3.1 系统说明

管发中心网络安全系统，是在当前各信息化业务系统在网络威胁趋势日益严峻的环境下，为满足国家对信息系统安全等级保护的规范及管发中心各业务及数据的信息安全，对管发中心整体信息化架构进行安全保障的核心系统。

系统包括各安全区域的边界防火墙、入侵检测及防御、计算机病毒检测及对抗、日志及行为审计等各类信息系统安全设备，按照需求分布在各个安全区域，并统一管理。确保管发中心信息系统运行的安全可靠。

根据三级等保要求进一步集成完善管发中心网络安全系统，确保整体网络满足更高的安全标准。

3.3.2 系统需求

1、现有外网出口边界的安全设备性能已不满足需求，采用 2 台高可用外网出口链路负载均衡设备，及 2 台高可用外网出口防火墙，对现有外网出口区的出口链路上现有设备进行升级替换。外网出口链路负载均衡设备作为 NAT 边界，三层路由对接外网出口防火墙，由防火墙提供安全策略和对内路由。

2、现有 1 台深信服品牌的“AC-1000”上网行为管理设备，负责外网接入区域的客户端上网行为管理工作。根据等保要求（三级）中对于设备的高可用性要求，需要补充 1 台上网行为管理设备，与现有设备进行高可用部署，以满足外网出口边界的整体安全需求。投标人提供的上网行为管理设备需要与现有的设备形成高可用部署，提供的设备如无法满足与现有设备的双机高可用部署，投标人须提供 2 台设备确保高可用结构并负责原设备的割接替换。

3、DMZ 区域提供对外业务发布，现有 1 台深信服品牌的“WAF-1000-B1400”型号的 WAF 设备，根据等保要求（三级）中对于设备高可用的要求，需要补充 1 台 WAF 设备，与现有的 WAF 设备集成部署，组成双机高可用模式。

4、根据 DMZ 区域直接对接外网的特性，为满足其安全性需要，需要在 DMZ 区域部署独立的入侵防御系统、网页防篡改系统及抗 DDOS 系统，以补足 WEB 应用防御能力，并进一步实现对来自外部网络的入侵行为进行甄别、阻断、日志记录、篡改防护和 DDOS 流量清洗能力。

5、根据对外发布业务需求，网页防篡改设备需要支持同时对不少于 2 个域的站点进行保护，并支持向第三方开放 API 接口，以便于与现有的安全监管平台系统进行联动，处理安全事件自动上报。投标人应提供其接口相关资料及负责与现有监管平台对接过程中必要的开发工作。

6、抗 DDOS 设备应同时具有内向外的 DNS 防护能力，可对内向外访问进行基于域名的主动管控，在防御外向内 DDOS 攻击的同时，对 DMZ 区域内向外主动发起链接的行为进行管控，以期在安全事件发生时及时阻断传播途径。

7、管发中心对外发布业务中包含“徐汇区数据共享平台”和“徐汇区综合管理信息平台”2 个业务系统需要在公网发布，根据三级等保要求，对外发布业务应强制采用 HTTPS 协议进行加密及防篡改以保障数据机密性和完整性。通过购买 2 个 OV 级单域名 SSL 证书服务，对这 2 个业务进行 SSL 证书配置以满足 HTTPS 的 SSL 加密需求。

8、为满足内网及外网安全区之间的跨安全区数据交互需求，需要部署 1 台网闸设备，其内网端及外网端分别接入对应安全区，通过网闸的链路物理隔离、数据逻辑传递及内容安全控制能力，实现在内外网安全区相互隔离的环境下，对必要的跨区业务通信进行安全传输保障。

9、现有系统的内网外联安全区边界防火墙，其性能已无法满足目前业务对转发性能的需求，为满足业务性能需求，需要高可用部署 2 台内网外联安全区核心防火墙，对现有内网区域及外部专线接入区之间的边界防火墙进行替换，确保在安全策略及规则符合安全需求的情况下同时满足数据交换的性能。

10、系统中现有 1 台防毒墙设备，负责数据交互过程中的病毒防御。其业务界面同时覆盖内网及外网 2 大安全区域，为其客户端提供 C/S 架构防病毒软件业务。根据三级等保标准中对安全区域严格划分及设备高可用的要求，需要增设 3 台防毒墙设备。其中 1 台与现有防毒墙设备组成双机高可用部署在外网出口区，单独负责外网安全区的病毒防御，另外 2 台双机高可用部署在内网区域与外部专线接入安全区之间的安全边界，负责内网安全区域终端业务交互的病毒防御。

11、现有网络安全设备的安全能力，暂无法对无线终端接入网络的行为进行管理控制，需要部署 1 套终端准入系统，单独通过带外管理网络对接无线控制器及 AP 设备，集中对内网和外网的无线网络进行终端准入控制管理，确保无线终端设备的接入及数据交互的流程可控制、追溯及审计。

12、现有的业务系统数据库，均采用数据库本地日志审计方式进行数据库审计，根据三级等保要求，需要部署 1 套独立数据库审计系统，通过网络镜像及 Agent 客户端等技术，由数据库外部对各项业务数据库进行日志记录、存放、分析及审计功能，增强数据安全性。数据库审计设备要求同时可对不少于 20 个数据库进行审计，须支持 KAFKA 方式将审计信息外送以对接现有安全管理平台，投标人应负责对所投设备与安全监管平台对接过程中，涉

及的数据格式调整及 KAFKA 解析所需要的相关开发工作。

13、现有日志审计系统同时负责业务应用和安全设备的日志审计，根据三级等保中对安全管理区独立的要求，在安全管理区部署 1 套专用日志审计系统，独立对各网络安全设备进行日志存放及分析审计功能。

14、当前的各项业务及设备的运维工作均采用运维人员直接操作的方式进行，运维终端可能引入各类安全风险。根据三级等保要求，需部署 1 台堡垒机设备，并通过集成配置严格限制各业务和设备运维操作仅可通过该堡垒机进行。实现对运维人员的操作进行安全防护和记录审计，确保运维人员操作无法直接接入系统内部，保障运维过程中的安全性。

15、现有及本项目中建设的各类网络安全设备型号繁杂数量众多，为实现高效率对系统整体进行运行管理，需要采购 1 套安全管理平台系统，对各安全设备进行统一的运行监控及集中管理。该设备需要在安全管理区独立部署，采用 SNMP 等技术与各设备进行信息对接。实现统一监控统一管理。

16、投标人需负责所有设备的安装部署和集成配置，及部分安全设备要求的日志、网管协议对接等配置。

3.3.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 链路负载均衡设备 | 硬件规格 | 至少 6 个千兆电口，2 万兆光口 SFP | 2 | 台 |
| | | 性能要求 | 吞吐量≥20GB | | |
| | | 部署方式 | 支持串接部署方式和旁路部署方式，支持三角传输模式；支持 HA | | |
| | | 链路负载、应用负载、全局负载 | 提供多条出口线路的链路负载均衡功能，实现 inbound 和 outbound 流量的均衡调度，以及链路之间的冗余互备； | | |
| | | 功能集成 | 提供 L4/L7 内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求； | | |
| | | | 提供多站点业务发布的全局负载均衡功能，通过智能 DNS 等机制实现内外网用户对多个数据中心的最优接入路径选择； | | |
| | | 链路负载均衡 | 支持静态 IP 和 PPPOE 两种线路接入方式； | | |
| | | | 链路负载均衡支持轮询、带宽比例、加权最小流量、动态就近性和加权源 IP 哈希等算法； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 服务器负载均衡 | 支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应时间、加权最小流量、按主机加权最小流量、源 IP 源端口哈希、源 IP 哈希、URI 哈希和 HOST 哈希等; | | |
| | | 全局负载均衡 | 支持标准的 DNS 服务，支持正向解析和反向解析功能，支持常用的记录类型，包括 A、AAAA、CNAME、DNAME、MX、NS、TXT、PTR、SRV、DS、CAA、HINFO 和 NAPTR 等; | | |
| | | 功能授权 | 附带应用负载均衡模块授权 | | |
| 2 | WAF 防火墙设备 | 硬件规格 | 规格：1U，内存大小：≥4G，硬盘容量：≥128GB SSD，电源：冗余电源，接口：千兆电口≥6，千兆光口 SFP≥4 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥6Gbps，HTTP 应用层吞吐量：≥400Mbps，HTTP 新建连接数：≥60000，HTTP 并发连接数：≥1800000。 | | |
| | | 部署方式 | 支持虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求。 | | |
| | | 协议解析 | 支持 HTTP、HTTPS 协议流量检测。 | | |
| | | | 支持 XML、JSON 格式解析。 | | |
| | | Web 应用防护 | 支持不少于 6200 种防护规则。其中 Web 应用防护规则不少于 4900 种，Web 应用漏洞攻击防护规则不少于 1300 种。 | | |
| | | 机器人流量防护 | 产品原生支持 BOT 防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义 URL 保护范围和保护阈值。 | | |
| | | | 支持自定义 BOT 防护排除功能，支持通过 IP 地址白名单、User-Agent、URL 前缀的方式排除。 | | |
| | | 语义分析 | 支持语义引擎用于检测 Web 攻击，能对不同类型的 Web 攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。 | | |
| | | 业务学习 | 支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因 WEB 应用中因代码不规范和安全检测功能冲突导致的业务误判问题。 | | |
| | | | 支持参数防护，支持主动防护，学习访问 HTTP 的请求参数，总结出参数的路径、变量名、变量类型、长度范围、支持自定义参数防护。 | | |
| | | 口令防护 | 支持识别和拦截中低频、分布式等高级 WEB 口令爆破攻击方式。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 脆弱性识别 | 支持通过被动扫描功能，业务系统进行黑链检测、Web shell 检测、漏洞风险检测、配置风险检测、弱口令账户检测。 | | |
| 3 | 入侵防御系统 | 硬件规格 | 1U 机架式设备，万兆入侵防御类设备，硬盘≥480G，网口≥18 个千兆电口，≥2 个管理口，≥1 个 RJ45 串口，≥2 个万兆光口，冗余电源。 | 1 | 台 |
| | | 硬件架构 | 具备独立的攻击检测引擎与病毒检测引擎。 | | |
| | | 性能要求 | 网络吞吐量≥10G，最大并发连接数≥1000 万。 | | |
| | | 入侵防御 | 攻击特征库数量≥8500、病毒特征库数量≥600W、支持的协议识别数量≥5500、WEB 攻击特征库≥3500。 | | |
| | | | 集成入侵防御与检测、病毒防护、带宽管理和 URL 过滤等功能；所有特性支持 IPv6 | | |
| | | | 采用全面深入的分析检测技术，结合模式特征匹配、协议异常检测、流量异常检测、事件关联等多种技术，实现对黑客攻击、蠕虫/病毒、漏洞、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御 | | |
| | | | IPS 检测到攻击报文或攻击流量后，支持 Web 重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机。 | | |
| | | | 支持用户自定义规防护则导入。 | | |
| | | | 支持服务器异常外联检测，同时可配置服务器异常外联自动学习功能，并可配置连续学习时间，建立基线。 | | |
| | | | 发现病毒发送的告警信息，支持用户编辑告警内容，防病毒支持云查杀。 | | |
| | | 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。 | | |
| | | | 支持应用风险调优，通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险。 | | |
| | | URL 过滤 | 设备提供预分类的 URL 地址库，支持根据 URL 类别实现 URL 过滤，URL 过滤可以基于时间、主机，能够精细到单一 IP 地址，设备提供海量预分类的 URL 地址库，支持管理者自定义新的 URL 地址和 URL 分类。 | | |
| | | | 支持 URL 黑白名单 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 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。 | | |
| | | 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、SIP Flood、DNS reply Flood、HTTP Flood（cc）攻击、HTTP 慢速攻击检测、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 | 支持报文示踪功能，可对原始报文进行回放，网页诊断、报文捕获、一键诊断收集。 | | |
| | | 功能授权 | 支持攻击特征库的手动、自动升级。包含不少于 3 年更新授权。<br>支持病毒特征库的手动、自动升级。包含不少于 3 年更新授权。 | | |
| 4 | 抗 DDOS 设备 | 硬件规格 | 2U 机架式设备，内存≥32G，硬盘≥1T，网口≥4 个千兆电口，≥4 个万兆光口，冗余电源。 | 1 | 台 |
| | | 性能要求 | 吞吐量≥5G，最大并发连接数≥2000 万。 | | |
| | | 抗 DDoS 功能 | 支持流量攻击自动防御：可自动防御 SYN Flood 、SYN-ACK Flood、 ACK Flood、FIN/RST Flood、ICMP Flood、UDP Flood、IP Fragment Flood、Stream flood、Ping of death、Land、Teardrop、Smurf 等攻击。 | | |
| | | | 支持应用型攻击防御 ：可防御 DNS Query Flood、DNS Reply Flood、Connection Flood、HTTP Get Flood、HTTP Post Flood、CC 攻击等。 | | |
| | | | 支持自动指纹采样防御，可以自动采集分析包头、payload 样本，并自动过滤。 | | |
| | | | 支持动、静态 IP 黑、白名单。动态黑、白名单支持策略自动加入、支持手动添加、批量导入；动态黑名单内 IP 地址支持访问二次加黑延时；支持静态黑、白名单手动添加、导入/导出；支持全局动、静态黑、白名单，支持服务器动、静态黑、白名单。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 HTTPS 证书加/卸载，支持 HTTPS/HTTP 透明代理、反向代理；支持 HTTPS js\set-cookie 验证防御；支持对 HTTP/HTTPS 的 Method、URL、源 IP、Referer、User-Agent、Content-Length、Host、HttpCode、Http Version 等自定义规则防护。 | | |
| | | | 支持自定义特征码防御，自定义特征码报文限速、支持特征字符包内出现频率限制，支持特征包大小限制，自动加白、加黑特征源 IP、自定义含特征字符数据包关联匹配限制，自定义策略间联动等。 | | |
| | | | 支持多元组 ACL 过滤（外部地址、外部端口、内部地址、内部端口、协议、TCP 标志位、地区（洲、国家、省））。 | | |
| | | | 支持 DNS 防护：可防御 DNS Request Flood、DNS Replay Flood、DNS 缓存感染攻击（DNS 投毒）、防 DNS 欺骗攻击、DNS 宕机保护、支持 DNS 域名黑白、名单，DNS 静态解析、DNS QOS 配置、随机域名防护、域名劫持配置、DNS 防护报表等能力。 | | |
| | | 攻击分析 | 支持攻击时自动抓包功能，当系统检测到攻击时，自动启动抓包，及时保留攻击证据和攻击报文情况，为日后追责，分析攻击情况提供帮助；支持指定接口抓包；集群部署时支持所有设备同时抓包。 | | |
| | | | 支持自动流量封堵策略自定义：支持根据总流量定义封堵策略；支持根据 IP 范围/网段总流量定义封堵策略；支持配置指定周期内相同地址首次、2 次、3 次、10 次封堵时长自定义；支持根据时间、流量配置解封条件。 | | |
| | | | 支持攻击溯源，攻击溯源报表内可显示攻击源 IP、攻击次数、攻击类型、攻击源归属地、攻击源 ISP 线路、统计时段、攻击目标。 | | |
| | | DNS 防护 | 支持 DNS 防护：可防御 DNS Request Flood、DNS Replay Flood、DNS 缓存感染攻击（DNS 投毒）、防 DNS 欺骗攻击、DNS 宕机保护、支持 DNS 域名黑白、名单，DNS 静态解析、DNS QOS 配置、随机域名防护、域名劫持配置、DNS 防护报表等能力；（提供相关证明材料）。 | | |
| | | 异常流量管理 | 支持域名管控，支持域名自动提取；可对百万级 HTTP/HTTPS 访问域名进行黑、白名单过滤；支持域名阻断页在自定义。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持实时流量 TOPN 排名；支持实时协议（UDP、ICMP、TCP、SYN、ACK&RST、OTHER 报文）流量 TOPN 排名；支持大集群按子设备 TOPN 流量排名。 | | |
| | | | 支持自动流量封堵策略自定义，支持根据总流量定义封堵策略，支持根据 IP 范围/网段总流量定义封堵策略，支持配置指定周期内相同地址首次、2 次、3 次、10 次封堵时长自定义，支持根据时间、流量配置解封条件。 | | |
| | | 报表功能 | 支持按照日期、日期范围导出，攻击日志导出为 Excel 格式，报表导出为 pdf 格式文件；支持按天查看滤前流量、过滤后流量、拦截流量、并发连接、新建连接、过滤前包数、过滤后包数、拦截包数；支持按主机查看滤前流量、过滤后流量、拦截流量、并发连接、新建连接、过滤前包数、过滤后包数、拦截包数。 | | |
| | | | 支持多种日志类型，攻击事件日志、攻击趋势日志、攻击溯源日志、流量日志、操作日志、设备负载日志、报表推送日志、连接状态日志、系统故障日志等。流量日志包含（峰值日志、均值日志、端口流量日志、流量 TOPN）。 | | |
| 5 | 防火墙（外网出口） | 硬件规格及性能要求 | 规格：≤2U，内存大小：≥8G，硬盘容量：≥128G SSD，电源：冗余电源，接口：千兆电口≥8，万兆光口 SFP+≥2 | 2 | 台 |
| | | 性能要求 | 网络层吞吐量：≥15G，并发连接数：≥200 万，HTTP 新建连接数：≥9 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年入侵防御及防病毒模块授权。 | | |
| 6 | 上网行为管理设备 | 硬件规格 | 规格：1U，内存大小：≥4G，硬盘容量：≥128G SSD，电源：单电源，接口：千兆电口≥6。 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥3.5Gb，应用层吞吐量：≥450Mb，带宽性能：≥300Mb | | |
| | | 网关模式 | 支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能； | | |
| | | 网桥模式 | 支持网桥模式，以透明方式串接在网络中；支持电口 bypass； | | |
| | | 旁路模式 | 支持旁路模式，无需更改网络配置，实现上网行为审计； | | |
| | | 上网监控 | 实时显示设置过滤条件的用户上网行为监控，支持手动设置刷新时间； | | |
| | | 链路负载状态 | 支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略； | | |
| | | 策略适用多种对象 | 支持基于用户组、位置、终端类型、URL 类型配置上网策略； | | |
| | | 应用识别规则库 | 设备内置应用识别规则库，支持不少于 9000 条应用规则数、支持不少于 6000 种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制； | | |
| | | 加密证书自动分发 | 审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。 | | |
| 7 | 网页防篡改系统 | 硬件规格 | 1U 机架式设备，内存≥16G，硬盘≥2TB，网口≥4 个千兆电口，≥1 个 console 口，≥3 个 USB 口，冗余电源。 | 1 | 台 |
| | | 网页防篡改 | 支持向第三方提供 API 接口，包括：获取通知报警信息、获取主机列表、获取产品日志、获取策略列表、启用/禁用策略、执行应急处置（一键断网、一键锁屏、一键禁止 USB、一键替换画面、一键拒绝读写、一键拒绝操作）。需提供相关接口资料及文档等证明材料。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持网页防篡改与自动恢复：支持 Windows 和 Linux 平台驱动级事前拦截非法篡改；支持所有文件类型的保护与自动恢复，如有篡改，立即自动恢复；支持根据文件对象的路径、源进程路径、源进程用户名、会话 ID、时间和线程用户名设置例外项。 | | |
| | | | 提供应急处置，发现入侵能阻止事态蔓延：提供一键应急页面、一键拒绝访问、一键断网、一键替换画面功能。 | | |
| | | | 多维度产品自保护：防止产品进程、线程、服务、驱动、注册表、自启动、自身目录和文件被恶意终止或篡改，防止产品被未授权卸载。 | | |
| | | | 防护端和发布端的网络通讯支持使用 TlsV1.2 及更新版本协议的加密。 | | |
| | | | 提供用户通知：支持短信报警；支持邮件报警。 | | |
| | | 零信任防火墙 | 支持网络通信管制：限制进出栈 IP，支持白名单和黑名单。 | | |
| | | | 支持保护任意网络端口，限制连接 IP，动态放行特定 IP。 | | |
| 8 | 网闸设备 | 硬件架构 | 采用内外两端独立的物理结构，内外端机为 TCP/IP 网络协议的终点，阻断 TCP/IP 协议的直接贯通。内外端机之间采用专用硬件和专用协议进行连接，不可编程，实现物理隔离。 | 1 | 台 |
| | | 安全体系结构 | 仲裁审计系统部署于内端机上，通用协议不能通过外端机直接连接到仲裁系统 | | |
| | | | 只能通过内端机上的管理口对网闸进行配置，防止业务网络遭受攻击。 | | |
| | | 操作系统 | 采用安全操作系统、增强型内核，能够对 2 个主机系统提供多层次、高强度的安全防护，保护其重要进程、文件、数据不受黑客侵袭。 | | |
| | | | 采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性。 | | |
| | | | 不采用通用的指令库和函数库，只提供有限的内部调试用指令函数。 | | |
| | | | 内置病毒查杀库，可查杀基于 Linux 操作系统各种主流病毒，保证操作系统安全，保证网闸自身不受病毒、木马侵害。 | | |
| | | | 系统基于可信安全操作平台，提供内核级主动防御。 | | |
| | | 安全上网功能 | 提供安全的上网访问，支持 HTTP 协议及代理等 | | |
| | | | 访问控制对象：源地址、目标地址、源端口、目的端目、域名、URL、访问方式、时间等 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 内容过滤：关键字过滤 | | |
| | | | 脚本过滤：javascript、Applet、ActiveX 等 | | |
| | | | 其他过滤策略：文件类型、页面提交方式等 | | |
| | | | 能够对每个用户的上网带宽进行限定 | | |
| | | 安全邮件功能 | 提供安全的邮件访问，支持 POP3、SMTP 协议 | | |
| | | | 支持邮件主机地址、邮件内容、发件地址、收件地址、邮件主题过滤 | | |
| | | | 支持附件传输进行、邮件大小、访问时间控制 | | |
| | | | 支持邮件服务器之间的邮件传输，可黑白名设置允许通过的邮件服务器域名 | | |
| | | 文件传输功能 | 提供安全的文件传输功能，支持 FTP、NFS、SAMBA 等文件传输协议 | | |
| | | | 支持将所传输的文件保存在网闸本地；支持对传输文件的类型过滤非后缀 | | |
| | | 文件同步功能 | 可通过专用客户端和网闸主动获取两种方式提供安全的文件同步功能（提供两种方式的界面配置截图） | | |
| | | | 支持 windows 平台和 Linux 平台 | | |
| | | | 支持实时扫描、一对多或多对一传输、增量传输 | | |
| | | | 支持目录内子目录同步，至多支持 32 级目录 | | |
| | | | 支持中文文件名或目录同步 | | |
| | | | 支持传输后删除源文件 | | |
| | | | 支持对格式类型进行特征过滤，并允许用户通过样本文件自定义格式类型；（需提供配置界面截图） | | |
| | | | 支持文件在线编辑、在线预览等操作；（提供界面截图） | | |
| | | | 支持文件分享功能，可设置到期时间和提取密码。 | | |
| | | 数据库访问功能 | 提供对多种主流数据库（SQL、ORACLE、DB2、SYBASE 等）数据库系统的安全访问 | | |
| | | | 支持用户查询、修改、添加、删除等操作 | | |
| | | | 支持全表复制、增量更新、全表更新等 | | |
| | | | 支持各种实例访问 | | |
| | | | 支持对数据库用户、操作、表进行黑白名单过滤。 | | |
| | | 数据库同步功能 | 基于专用客户端与网闸安全连接方式，提供多种主流数据库（SQL、ORACLE、DB2、SYBASE 等）的单、双向数据交换 | | |
| | | | 无需修改数据库表结构，不涉及代码修改及二次开发 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 同步粒度可以达到表内具体字段 | | |
| | | | 支持多种增量同步方式，可分别定义增加、删除、修改的传输方式 | | |
| | | | 支持异构数据结构以及代码语义的转换规则定义，并实现源数据到目标数据之间的实时数据交换，支持数据整合业务（提供异构数据库同步配置界面截图） | | |
| | | | 支持数据一对一、一对多、多对多的单向或双向交换和同步 | | |
| | | | 支持实时交换或定时同步的策略定义 | | |
| | | 视频传输功能 | 实现视频网络与信息通信网的网络隔离，切断所有基于网络协议的连接； | | |
| | | | 支持多种视频硬件平台，如摄像头、DVR（数字硬盘机）、流媒体服务器、视频服务器等设备； | | |
| | | | 支持服务端口控制，对访问视频管理服务器的端口进行控制，其他视频端口默认关闭； | | |
| | | | 支持标准 SIP 协议 | | |
| | | | 支持 RTSP 协议 | | |
| | | | 支持符合 GB/ T28181 标准的视频业务 | | |
| | | 自定义功能 | 支持用户基于标准 TCP、UDP 开发的自定义协议软件，无需对自定义协议软件进行二次修改开发，可以根据需求开发新的专用协议处理过滤功能 | | |
| | | | 支持 OPC 控制协议，可动态分析 OPC 端口协议 | | |
| | | | 支持对基于 HTTP 的 SOAP 协议进行过滤，确保访问的安全。 | | |
| | | 安全功能 | 支持用户名与密码认证 | | |
| | | | 支持用户名与 IP-MAC 绑定，（非仅仅 IP/MAC 绑定） | | |
| | | | 支持访问时间控制 | | |
| | | | 支持病毒查杀功能 | | |
| | | | 支持对每个应用设定带宽及最大连接数 | | |
| | | 多机热备 | 可实现多台设备应用分流、互相冗余的应用模式 | | |
| | | 网口冗余 | 使一端机多网口冗余，可实现链路备份冗余或负载均衡的工作模式 | | |
| | | SNMP 支持 | 支持 SNMP 协议，可与标准网管平台无缝兼容 | | |
| | | SYSLOG 支持 | 支持 SYSLOG 协议，可与标准日志服务器平台无缝兼容，可实时发送网闸运行状态 | | |
| | | 入侵检测模块 | 内置独立的入侵检测模块，可与网闸联动对入侵行为做出处理 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 抗攻击模块 | 抗攻击模块具有抗 DOS、DDOS 功能，当攻击发生时能有效地保障正常应用请求的应答 | | |
| | | 管理配置功能 | 管理端采用 B/S 结构 | | |
| | | | 管理端：用于通道建立、策略制定、日志查询、分析、导出等； | | |
| | | | 安全终端管理：可通过串口终端管理方式对网闸进行维护； | | |
| | | | 支持 USB-KEY 登陆身份认证 | | |
| | | 接口要求 | 内网不少于 6 个 10/100M RJ45 接口（含一个管理口），1 个串口，2 个 USB 口 | | |
| | | | 外网不少于 6 个 10/100M RJ45 接口（含一个 HA 口），1 个串口，2 个 USB 口 | | |
| | | 性能指标 | 吞吐量：4G | | |
| | | | 系统整体时延：<1 毫秒 | | |
| | | | 并发连接数：12000 | | |
| 9 | 安全管理平台系统 | 硬件规格 | 硬件参数：规格：2U，内存大小：≥48G，硬盘容量：≥128GB SSD+4TB SATA，电源：冗余电源，接口：千兆电口≥4，千兆光口 SFP≥4， | 1 | 台 |
| | | 部署模式 | 支持网桥、路由、旁路模式部署 | | |
| | | 平台要求 | 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 | | |
| | | | 支持双因素认证功能，用户需在登录时进行双重认证，以此提高用户的安全性。 | | |
| | | | 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。 | | |
| | | 网管中心要求 | 支持对采用 SNMP V1、V2、V3 和 ICMP 等网络管理协议的主流品牌网络设备的监控。 | | |
| | | | 可自动扫描主流品牌的无线 AC、AP，对连接数、在线用户数、上下行吞吐量等无线 AC/AP 设备实时数据 | | |
| | | | 支持审计数据外发对接。 | | |
| | | 功能授权 | 配有管理≥10 台服务器及≥30 台网络设备的授权。 | | |
| 10 | 堡垒机设备 | 硬件规格 | 软硬一体化机架式设备，至少提供 6 个千兆电口，2 个万兆光口 | 1 | 台 |
| | | 部署模式 | 可管理资源数≥300 个 | | |
| | | | 物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 系统各模块支持以 B/S 方式管理，采用 https 加密方式访问 | | |
| | | 支持协议 | 字符协议：SSHv1、SSHv2、TELNET | | |
| | | | 图形协议：RDP、VNC | | |
| | | | 文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板 | | |
| | | 用户管理 | 内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴 | | |
| | | 资源管理 | 支持 RDP 安全模式（RDP、NLA、TLS、ANY）设置，以适应 RDP-TCP 属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合 FIPS 标准等加密级别 | | |
| | | 运维授权 | 支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问 | | |
| | | | 支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批 | | |
| | | 访问控制 | 支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人（需提供产品功能截图证明） | | |
| | | 运维方式 | 支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP 等客户端工具实现单点登录，不改变运维人员操作习惯 | | |
| | | 审计日志 | 图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放 | | |
| | | 客户端兼容 | 全面支持 H5 页面一站式运维，实现跨终端适应性 BYOD（Bring Your Own Device）（需提供产品功能截图证明） | | |
| | | 功能授权 | 配有不少于 150 个资源的授权。 | | |
| 11 | 防火墙（内网外联 | 硬件规格 | 规格：≤2U，内存大小：≥8G，硬盘容量：≥128G SSD，电源：冗余电源，接口：千兆电口≥8，万兆光口 SFP+≥2， | 2 | 台 |
| | | 性能要求 | 网络层吞吐量：≥15G，并发连接数：≥200 万，HTTP 新建连接数：≥9 万 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 区） | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备 URL 分类库。 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年入侵防御及防病毒模块授权。 | | |
| 12 | 防毒墙设备 | 硬件规格 | 1U 机架式设备，内存≥32G，硬盘≥1T，网口≥6 个 bypass 电口+2 千兆电口。 | 3 | 台 |
| | | 性能要求 | 网络层吞吐量≥10Gbps，防病毒吞吐量≥2Gbps。 | | |
| | | 部署模式 | 根据业务发展需要，需与现部署的防病毒网关设备组成双机热备模式，且支持统一平台进行管理。 | | |
| | | 技术性能 | 支持对威胁进行可视化展示，并支持单独对勒索、挖矿、病毒、漏洞利用威胁事件、APT 等的集中防护及统一展现，同时支持近 30 天威胁事件趋势、攻击源 IP TOP5、受影响主机 TOP5、勒索&挖矿事件拦截统计、热门威胁事件 TOP5、自定义黑名单 TOP5 等的展示。 | | |
| | | | 能够支持 SMBv1/SMBv2/SMBv3 文件共享协议的病毒检测与查杀 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 为提升威胁病毒查杀的速度及能力，产品需内置多个引擎，包括自研防病毒引擎、深度包解析和威胁情报引擎、高级威胁扫描引擎、文件防病毒引擎、网络攻击防护引擎，并支持多个引擎同时使用，提高威胁病毒的检测准确性，能够精准高效对勒索、挖矿、病毒、APT、漏洞利用威胁事件检测拦截，同时支持 0day 或者 N day 漏洞快速响应。 | | |
| | | 防病毒能力 | 支持对最多 20 层的压缩文件进行解压查杀。 | | |
| | | | 能够支持超过 100 种协议的解析， 包括但不限于 HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC 等。 | | |
| | | | 能够允许定义被扫描文件的大小范围，最大不小于 2G。 | | |
| | | 挖矿治理 | 产品需要具备在网络边界的挖矿检测和拦截能力，在界面上能展示矿池协议、挖矿事件的统计数据。 | | |
| | | 入侵检测及虚拟补丁 | 支持虚拟补丁功能，能通过 CVE 编号搜索对应的防护规则，在网络层面对漏洞攻击进行阻断，并支持实际测试。 | | |
| | | | 能够提供包括但不限于防止漏洞利用和 SQL 注入、命令注入、 Webshell 攻击、XSS 攻击，CSRF 攻击的能力。 | | |
| | | | 能够防御网内主机的零日漏洞攻击。 | | |
| | | | 所投产品需支持用户自定义 IPS 规则，支持设置严重等级、规则种类、源/目的 IP 地址、源/目的端口、协议类型（至少包含 HTTP、TCP、UDP 协议）等。 | | |
| | | 统一安全管理平台 | 所投产品需提供配套的统一安全管理平台，且该平台支持与现有及所投防病毒网关设备、流量探针网络系统等形成联动，当流量探针网络系统发现网络威胁时，能够第一时间通报至统一安全管理平台，并由统一安全管理平台下发至防毒墙设备，进行边界安全防护及威胁病毒查杀。（提供相关证明材料）。 | | |
| | | | 支持与现有及本次所投的防病毒网关、流量探针网络系统进行策略统一下发，并可对现有及本次所投防病毒网关设备进行产品补丁下发。 | | |
| | | 威胁情报 | 能够支持威胁情报能力以覆盖更大范围的威胁检测，可根据客户的实际情况进行开启或关闭。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持用户自定义黑/白名单，支持 URL 黑/白名单设置、支持邮件收发件人黑/白名单设置、支持基于 SHA1 的文件黑/白名单设置。 | | |
| 13 | 终端准入控制系统（无线） | 分布式部署 | 要求支持资源拓扑、告警、性能等功能模块；支持多服务器分布式虚拟化部署，可实现负载分担，满足大规模网络环境的统一管理 | 1 | 台 |
| | | 自定义主页 | 要求管理员可以首页中通过拖拽，自定义需要在准入首页展示页面，同时支持 Widget 扩展。 | | |
| | | 自动发现拓扑 | 自动发现网络中的所有网络设备，并自动绘制拓扑图，支持拓扑图自定义修改，包括设备、链路等。 | | |
| | | 故障管理 | 支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转 E-mail，转短信，转上级网管或其他网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能 | | |
| | | 性能管理 | 支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警 | | |
| | | VLAN 拓扑 | 以可视的方式对网络中的 VLAN 资源进行管理，查看拓扑视图中所有设备节点和链路是否允许某个特定 VLAN 通过 | | |
| | | 无线拓扑管理 | 支持查看 AC 与 AP 之间真实物理链路连接，有利于排查网络故障 | | |
| | | | 支持批量操作及文件导入设备信息。支持将网络设备按区域、类型划分管理，管理界面中以树形结构展示，不少于 5 级管理 | | |
| | | | 支持自定义视图并且在视图上显示设备告警和实时状态，可以导入背景图，方便管理员按需进行重点设备的重点管理 | | |
| | | | 在拓扑上支持查看 AP 当前在线 Station 及详细信息，可以实现设备和用户的统一管理，支持进行 Station 上线历史记录浏览 | | |
| | | 有线无线一体化管理 | 支持有线无线一体化管理，可统一管理 AC、AP、无线终端、PoE 交换机等设备，支持在拓扑上支持展示设备告警、状态 | | |
| | | 无线报表 | 支持分级报表，分级管理中网管上级可以方便地管理到下级报表 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 无线业务告警 | 内置丰富的无线业务告警，包括 AC CAPWAP 隧道建立告警、AC CAPWAP 隧道关闭告警、AP 工作模式变更告警、AP 配置失败告警、AP Radio 操作状态 DOWN 告警、AP Radio 操作状态 UP 告警、AP Radio 信道变更告警、Station MIC 错误告警、Station 认证错误告警、Station 认证失败告警、Station 关联失败告警、Station 去关联告警、Station 认证成功告警、发现非法设备告警、发现 ad-hoc 设备告警、发现未授权的 SSID 告警、非法设备消失告警。 | | |
| | | 授权要求 | 网络设备管理授权不少于 25 个，用户终端接入授权不少于 300 个。 | | |
| 14 | 数据库审计系统 | 硬件规格 | 2U 机架式（专用硬件平台），冗余交流电源，2GE 板载管理口，4GE 板载接口，2×接口板卡插槽。 | 1 | 台 |
| | | | 32GB 内存，1×4TB 硬盘。 | | |
| | | 性能要求 | 纯数据库流量 150Mbps、峰值 QPS（每秒 SQL 请求数）15000 条/秒、在线会话数 4500 个； | | |
| | | | 网络流量 1.5Gbps。 | | |
| | | 部署模式 | 镜像模式： | | |
| | | | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计（不需要提供 DBA 和任何数据库用户，不需要创建任何数据库用户）； | | |
| | | | 可支持 TAP 和 SPAN 模式。 | | |
| | | | 探针模式： | | |
| | | | 支持在目标数据库服务器主机上安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户），在审计平台可以实时监控服务器和 agent 的资源状态。 | | |
| | | | 支持镜像模式和探针模式混合部署。 | | |
| | | | 探针可适配常见 Linux 系统、Unix 系统及 Windows 系统，如 CentOS、Redhat、Ubuntu、Debian、HP-Unix、Euleros（欧拉）、openEuler、ky10、Solaris 、SUSE、UOS 等。 | | |
| | | | 支持虚拟化环境部署。 | | |
| | | 防护功能 | 支持旁路阻断 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 协议支持 | 国际数据库：Oracle、MySQL、SQL Server、Db2、Informix、PostgreSQL（EDB）、Sybase ASE、MariaDB、Percona、Greenplum、Caché、Teradata、SAP HANA、Vertica 等。 | | |
| | | | 国产数据库：达梦、南大通用、人大金仓、神通、OceanBase、GaussDB A、GaussDB T、TiDB、TeleDB、CirroData、EsgynDB、Gbase 8t 等。 | | |
| | | | 支持 Hive、HBase、Impala、HDFS、Spark SQL，ElasticSearch、MongoDB、Redis、Clickhouse、Solr、Hive 等大数据组件和非关系型数据库的审计。 | | |
| | | | 支持审计使用回环地址连接数据库的本地访问行为。 | | |
| | | | 支持数据库地址配置域名，通过域名对数据库进行审计。 | | |
| | | | 支持 Oracle CDB/PDB。 | | |
| | | | 支持 Oracle、MySQL、Hive 加密链路。 | | |
| | | | 支持 Oracle 高级安全加密。 | | |
| | | | 支持数据库使用动态端口。 | | |
| | | | 支持单向请求包审计。 | | |
| | | | 支持 telnet 协议审计。 | | |
| | | 自动发现 | 支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址等信息，并且自动添加到审计范围，无需用户提供网段、数据库地址等信息； | | |
| | | | 智能模式，根据系统资源使用率动态决定是否进行自动发现，从而不影响正常审计业务。 | | |
| | | | 支持自动添加自动发现的数据库。 | | |
| | | 审计能力 | 支持审计会话相关信息，包括：<br>客户端 IP、客户端端口、客户端 MAC、OS 用户、访问工具、主机名称、数据库名称、数据库用户、数据库会话标识、数据库 IP、端口、MAC、服务（实例）名、会话开始、结束时间等。 | | |
| | | | 支持审计 SQL 语句相关信息，包括：<br>SQL 标识、操作类型（DDL、DML、DCL 等）、影响行数、响应时间、语句长度、捕获时间、执行结果（DB 应答码、应答错误信息）、受影响对象、SQL 语句、SQL 语句模板、SQL 参数、结果集，等。 | | |
| | | | 支持表、视图、字段等。 | | |
| | | | 支持跨语句、跨多包的访问方式及绑定变量值的审计。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持对超长 SQL 操作语句审计，对于 Oracle 可支持 8M 长的 SQL 语句。 | | |
| | | | 支持配置返回行数和内容大小控制返回结果集大小，降低系统开销。<br>内置默认规则，支持场景：高危操作、权限变更、批量数据泄露或篡改、撞库、无 where 更新或删除、SQL 注入、系统表非法操作等。 | | |
| | | 审计规则 | 审计规则至少支持 20 个条件，规则各条件之间支持与、或、非逻辑关系。<br>在规则中可支持多种条件：<br>访问来源：源 IP、客户端工具、客户端 MAC、操作系统用户、主机名、数据库实例、数据库用户；<br>操作设置：select、update 等 SQL 操作、schema、表、字段；<br>条件控制：where 条件、关联表个数、SQL 语句关键字；<br>执行结果：影响行数、响应时间、执行结果关键字、结果集敏感行数、应答错误号；<br>SQL 命令特征（如 SQL 注释、常量表达式等）、SQL 函数、XSS 跨站；<br>时间范围。 | | |
| | | | 支持规则例外，使得特定行为或语句不命中规则；<br>访问来源：源 IP、客户端工具、客户端 MAC、操作系统用户、主机名、数据库实例、数据库用户；<br>操作设置：select、update 等 SQL 操作、schema、表、字段；<br>条件控制：where 条件、关联表个数、SQL 语句关键字；<br>SQL 命令特征（如 SQL 注释、常量表达式等）、SQL 函数、XSS 跨站；<br>时间范围。 | | |
| | | | 可支持对触发器定义、存储过程调用、视图、函数、包、绑定变量配置规则条件。 | | |
| | | | 支持审计白名单，以实现信任特定行为或语句，不会触发风险。 | | |
| | | | 支持对信任的行为或语句不进行审计。 | | |
| | | | 支持对 SQL 语句配置审计规则。 | | |
| | | | 支持频次规则，即在一段时间内对某对象的操作频率。<br>规则可关联数据库，也可关联数据库类型； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 关联数据库类型后，可选择自动关联后续添加的数据库。 | | |
| | | | 支持对工具语句的过滤。 | | |
| | | | 应具备漏洞攻击规则库，漏洞攻击规则应至少包括：漏洞名称、CVE 标识、CNNVD、漏洞类型、影响范围等内容。 | | |
| | | | 内置安全特征库规则，如 SQL 注入、缓冲区溢出、权限提升、数据泄露、拒绝服务、访问操作系统、改密码、Bypass FGAC、修改 FGAC、审计、游标注入、访问敏感组件、创建外部 JOB、恶意代码、非系统用户执行命令等常规漏洞。 | | |
| | | | 支持在全局启用结果集审计，也支持按照规则进行结果集审计，可以针对特定访问行为，审计结果集。 | | |
| | | | 告警数量支持最大告警数量限制，超过告警阈值之后便不告警。 | | |
| | | | 可以针对每条规则配置不同告警次数限制，灵活控制告警频率。 | | |
| | | | 支持 IP 地址、数据库用户、时间、对象、操作系统用户、客户端工具、数据库实例分组等，并且分组对象可以直接在规则中引用。<br>提供默认对象组，内置主流数据库的系统对象信息，可直接在规则中引用。 | | |
| | | 查询能力 | 支持对审计到的 SQL 语句、SQL 会话、触发的风险进行查看和检索。<br>对于 SQL 语句，支持多种查询条件：<br>客户端 IP、客户端 MAC、客户端工具、主机名、操作系统用户、数据库用户、<br>被保护数据库、数据库 IP、数据库端口、服务（实例）名、对象、影响行数、响应时间、语句总耗时、执行结果、SQL 操作、风险类型、风险级别、时间等。 | | |
| | | | 支持对结果集的关键字检索。 | | |
| | | | 支持将常用的查询条件保存成固定查询模板，方便后续快速查询。 | | |
| | | | 支持对查询结果以 CSV 文件格式导出到本地。 | | |
| | | | 支持导出任务，可后台执行，查询并导出大量结果，导出量在百万量级。 | | |
| | | | 在对审计到的数据进行查看时，支持对请求方向和结果集中可能存在的敏感数据进行掩码处理，防止敏感数据泄露。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持客户端 IP 进行别名配置，实现针对不同客户端 IP 自定义别名展现。 | | |
| | | | 支持自定义业务化语言，可将 SQL 语句翻译为业务化的语句进行展现。 | | |
| | | 统计分析 | 支持对会话详情展现，可对会话内执行的全部 SQL 进行展示，跟踪对数据库的访问行为。SQL 可按时间正序、倒序查看，方便事件追溯。 | | |
| | | | 支持对会话进行统计分析，包括：<br>－从访问来源对新建会话、在线会话进行统计；<br>－分析失败登录的来源和目的、时间和失败原因等。 | | |
| | | | 支持对 SQL 语句的统计分析，包括：<br>－根据操作类型、访问来源对 SQL 进行统计；<br>－根据语句模板，对 SQL 的执行次数进行统计、对执行历史进行追踪；<br>－分析失败语句的来源、错误原因等信息。 | | |
| | | | 支持对语句 Top SQL 的分析，可从语句的耗时和执行次数维度进行统计，评估数据库性能。 | | |
| | | | 支持对访问源的分析，可展现不同数据库节点的访问源统计、分析状态。 | | |
| | | | 支持对风险的统计，包括：<br>－从风险等级、规则等维度进行统计和展现；<br>－从语句模板的维度对风险命中情况进行统计。<br>在统计中支持钻取，可快速定位行为或风险。<br>对象统计：以操作类型为维度，统计表级别对象被访问次数，可生成行为轨迹图；<br>并可通过对象的访问次数，下钻追溯到该表对象下所有的访问语句详情，以及该表对象访问来源。<br>统计对比：获取同一数据库不同时间段及不同数据库同一时间段的 SQL 语句量和会话量的对比统计数据以及变化趋势。 | | |
| | | 报表 | 系统提供 40 个以上报表模型，分别基于全库、数据库组和单库维度进行展现。 | | |
| | | | 支持合规性报表，如 SOX 法案、等保、PCI 等专项报表展现。 | | |
| | | | 支持通过专项报表，针对风险、性能、访问源、数据库用户等信息做专项报表展现。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持自定义报表。 | | |
| | | | 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表。 | | |
| | | | 支持按日、周、月等时间周期生成报表。 | | |
| | | | 支持报表数据后台定期预生成，保障报表数据展现速度。 | | |
| | | | 支持将报表按指定的时间推送至指定管理员的邮箱。 | | |
| | | | 报表支持以 Word、PDF、HTML 等格式保存到本地。 | | |
| | | | 支持对特殊场景的分析，如运维人员共用数据库账号场景分析、对象访问热度分析等。 | | |
| | | 告警与外送 | 支持系统告警； | | |
| | | | 系统告警内容支持网卡异常、分区超限、异常关机、CPU 超限、内存超限、会话超限、包数超限、SQL 数超限、探针异常、证书服务过期等； | | |
| | | | 支持按照风险高、中、低、通知，进行告警通知。 | | |
| | | | 可及时发现系统问题，跟进处理。 | | |
| | | | 支持规则命中后的风险告警； | | |
| | | | 风险告警内容支持触发规则风险内容，并支持根据风险等级进行告警通知。 | | |
| | | | 支持规则告警与规则、数据库关联，实现不同规则、风险级别、数据库以及数据库类型的告警发送给不同收件人，方便进行风险的排查。 | | |
| | | | 告警方式包括：邮件、短信、SYSLOG、SNMP TRAP、企业微信、钉钉群告警、页面弹窗。 | | |
| | | | 支持 SYSLOG 方式外送数据，可外送审计数据、会话信息、语句模板、系统审计日志； | | |
| | | | 支持以文本格式； | | |
| | | | 支持自定义编辑外送模板 | | |
| | | | 支持 KAFKA 方式进行审计数据外送，可外送会话信息和审计数据； | | |
| | | | 支持文本、二进制、JSON 格式； | | |
| | | | 支持自定义编辑外送模板 | | |
| | | | 投标人需提供相关功能截图及数据格式资料等证明文件 | | |
| | | 数据管理 | 支持审计日志数据的备份，支持自动备份，备份时可以选择高性能或高压缩比； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持将备份的日志上传到的远程服务器，服务器类型支持 FTP、SFTP、NFS 方式。 | | |
| | | | 支持恢复已备份的审计日志数据，以便查看历史审计记录； | | |
| | | | 支持对存储空间的监控，当空间不足时可进行告警； | | |
| | | | 支持对审计数据的清理，可按在线天数、磁盘空间等阈值进行自动清理。 | | |
| | | 系统管理 | 支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色； | | |
| | | | 可以新建不同用户，分配不同数据库权限和不同的菜单管理权限，不同用户之间数据隔离； | | |
| | | | 可创建多层子账号； | | |
| | | | 系统支持 LDAP/AD 域对接，支持 AD 域用户关联审计系统用户，通过 AD 域账户统一登录审计系统； | | |
| | | | 支持密码策略的配置，可调整密码强度、登录安全相关配置； | | |
| | | | 支持多语言； | | |
| | | | 审计设备 WEB 界面提供自动诊断功能，可以自动收集实例级参数、策略中心参数、操作系统参数、组件参数，方便了解系统运行状态和排查问题； | | |
| | | | 具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录。 | | |
| | | | 支持 SNMP 服务配置，可供第三方监测系统状态 | | |
| | | | 在证书申请时，可以选择显示实际授权数量、显示为无限、不显示授权数。 | | |
| | | | 在用户登录数据库时，支持使用 UKey 认证、谷歌登录认证配合用户名密码进行用户登录双因素认证。 | | |
| | | 功能授权 | 标配不少于 20 个数据库（IP+Port）授权，包含相同的 Agent 探针授权。 | | |
| 15 | 日志审计系统（安全加固区） | 硬件规格 | 2U 机架式设备，内存≥64G，硬盘≥8T*4，网口≥4 个千兆电口，冗余电源。 | 1 | 台 |
| | | 性能要求 | 日志源≥150 个，日志处理性能≥8000EPS。 | | |
| | | 系统架构 | 系统应基于大数据平台架构，具备海量数据收集与快速检索能力。 | | |
| | | | 系统应基于 B/S 架构，支持 SSL 加密模式访问，可通过 web 方式直接对系统进行管理。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 基础要求 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统。 | | |
| | | | 审计工作不影响被审计对象的性能、稳定性或日常管理流程。 | | |
| | | | 审计结果存储于独立存储空间。 | | |
| | | | 自身用户管理与设备或主机的管理、使用、权限无关联。 | | |
| | | | 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件。 | | |
| | | 日志采集 | 支持 Syslog（UDP、TCP）、目录、远端软件（FTP、SFTP、HDFS、LOCAL）、WMI、SNMP(Trap)、数据库（ORACLE、DB2、MYSQL、SQLITE、POSTGRES、SQLSERVER）协议日志收集。 | | |
| | | | 支持使用代理（Agent）方式提取日志并收集。 | | |
| | | | 系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec（天融信）、DBAPP Security（安恒）、SANGFOR（深信服）、Hillstone（山石网科）、东软、瑞星、金山、网康、360 网神、DP tech（迪普）、艾科网信、Imperva、Juniper（瞻博网络）、F5、Symantec（赛门铁克）、Deep Security（趋势科技）、MacAfee（迈克菲）、Fortinet（飞塔）、Windows、Linux/Unix、Cisco（思科）、HUAWEI（华为）、H3C（华三）、中兴、Apache、nginx 、IIS、WebLogic、VMWare、KVM、Xen、OpenStack、Hyper-V、华为 FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等。 | | |
| | | | 系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。 | | |
| | | 日志分析 | 支持对设备日志查询和聚合分析。 | | |
| | | | 系统内置常见安全事件关联分析规则。 | | |
| | | | 支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。 | | |
| | | 日志审计 | 支持 SOX 审计包含 SOX 登录事件、SOX 对象访问、SOX 账号管理、SOX 策略更改。 | | |
| | | | 支持 PCI 审计包含 PCI 策略更改、PCI 对象访问、PCI 登录事件。 | | |
| | | | 支持 WEB 访问分析包含 WEB 访问概况、WEB 访问客户端分析、WEB 访问地区分析、WEB 异常访问分析。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 ISO27001 审计包含 ISO27001 对象访问、ISO27001 策略更改、ISO27001 账号管理、ISO27001 登录事件。 | | |
| | | 数据查询 | 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、地理城市等参数进行过滤查询 | | |
| | | | 支持可指定多个查询条件进行组合查询。 | | |
| | | 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义。 | | |
| | | | 基于角色的权限管理机制，通过角色定义支持多用户访问。 | | |
| | | 平台部署 | 支持多分支级联传输，统一审计和管理，并集中展现。 | | |
| 16 | SSL CA 证书服务 | 证书等级 | OV 级单域名，需通过国际主流的 WebTrust 认证，与市面主流操作系统和浏览器根信任、同时支持国际及国密算法证书 2 套 | 1 | 项 |
| | | 证书服务期 | 3 年 | | |

### 3.4 管发中心异地灾备机房系统升级改造

3.4.1.系统说明

为满足管发中心信息系统的灾备需求，分别在其下属单位上海市徐汇区牙病防治所及上海市徐汇区漕河泾街道社区卫生服务中心进行异地部署，建设异地灾备机房系统，以满足管发中心业务数据的灾备保障需求。

异地灾备系统需要具备数据备份、同步、验证、恢复等整套灾备保障能力，确保业务数据安全。

3.4.2 系统需求

1、上海市徐汇区牙病防治所数据中心现有 2 台普通机架式服务器负责管发中心异地数据备份，建设 1 套副本管理备份系统，通过专用副本管理备份软件对现有 2 台机架式服务器进行功能替换，以实现数据同步复制。

2、需要对现有的计算资源、数据库和虚拟机等业务已配置的备份工作流进行重新配置以对接副本管理备份系统，现有备份工作流切换完毕并正常运作后，将原有 2 台服务器转为冷备部署。

3、副本管理备份系统要求可管理数据库，并支持到数据级粒度。需要支持对接主流操作系统并对数据、文件、系统、数据库等进行备份及恢复。同时支持主流各品牌虚拟化系

统对接，可直接备份虚拟机。

4、部署 2 台高性能机架式服务器，通过副本管理备份系统进行统一管理，作为数据库备份验证服务器使用。需要对其进行配置，使之周期化对副本管理备份系统中的数据库副本进行恢复还原，并对备份副本进行数据验证。同时需要进行相关配置，使其在灾害发生时可转化为异地应急数据库服务器。投标人需要在服务器硬件安装部署完成后，配合采购单位进行数据恢复还原及验证的测试工作。后续验收工作需确保测试通过，灾备能力可靠。

5、副本管理备份系统及数据验证服务器之间需要大带宽数据交互，其灾备网络接入网络需要部署独立的万兆接入交换机设备，确保大量数据交互时的带宽需求。

6、为确保异地灾备机房的访问安全性，部署独立的边界防火墙设备，与独立的设备管理网络接入交换机，确保设备的业务层和带外管理网络物理隔离，且受专用防火墙保护。需要负责交换机及防火墙等网络设备的安装部署及安全策略配置。

7、建设三地异地备份，需要在上海市徐汇区漕河泾街道社区卫生服务中心部署 1 台备份一体机系统，实现三地异地灾备备份，确保数据高安全性。备份一体机需要采用数据异步复制方式周期实现数据冷备，以期在灾害时管发中心数据中心及牙病防治所的灾备系统均无法正常接替时，具有可随时恢复还原的冷备数据。硬件部署完成后需要进行备份恢复测试。需要支持对接主流操作系统并对数据、文件、系统、数据库等进行备份及恢复。同时支持主流各品牌虚拟化系统对接，可直接备份虚拟机。

3.4.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 副本管理备份系统 | 硬件规格 | 处理器：2 颗八核 2.1G, 8C/16T, 9.6GT/s, 11M 缓存， Turbo | 1 | 台 |
| | | | 硬盘： 3.5 英寸裸容量≥192TB 存储盘。 | | |
| | | | 内存：不少于 128GB RAM。 | | |
| | | | 网络接口：4 个千兆网络端口，2 个万兆网络端口，2 个 16Gb 光纤网口 | | |
| | | 兼容性要求 | 全面支持各种数据库及应用服务，包括 Microsoft SQL Server，Oracle，MySQL，瀚高、人大金仓、达梦、优炫、南大通用等。 | | |
| | | | 支持跨平台数据复制，至少包括 Windows、Linux 及龙芯、飞腾架构下中标麒麟、银河麒麟等自主可控操作系统。 | | |
| | | | 支持 Microsoft VPC/Hyper-V, VMware 等虚拟化平台备份。 | | |
| | | 功能要求 | 提供异步字节级别的持续复制功能，及数据实时同步功能，并提供相关功能证明材料。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持多规则、多并发的数据保护，灵活的规则管理策略，规则之间相互独立。 | | |
| | | | 支持数据压缩与重复数据删除功能，提高备份速度，节省存储空间。 | | |
| | | | 提供打开文件的镜像和复制功能。 | | |
| | | | 支持异构平台上各种应用和数据实时复制，比如 Windows 平台和 Linux 平台间的文件复制，同时要求灾备端文件和数据保留文件属性信息，严格保证数据的原始性和可用性 | | |
| | | | 客户端安装部署不需要生产端重启，要求在不停业务/不停机的情况下进行备份。 | | |
| | | | 支持 P2V，V2V，P2P，V2P 场景下的数据级复制；支持异构虚拟化平台之间的数据级复制；支持任意公有云或私有云之间的数据级复制；支持本地机房和云主机间的数据级复制；支持异地机房间、基于专线或广域网的数据级复制。 | | |
| | | | 支持集群环境（基于共享存储）到异地的数据复制；数据复制，支持按照文件后缀和类型进行自动过滤；支持文件复制过程自动执行文件名转换，支持正则表达式方式。 | | |
| | | | 支持可设定的任意历史点数据快速恢复，具备真正的 CDP 数据保护功能，精细度可恢复百万分之一秒任意数据版本。 | | |
| | | | 支持在 CDP 数据正式恢复之前，可快速查看灾备的文件目录信息，确定恢复时间点后，再正式进行 CDP 数据恢复。 | | |
| | | | 支持虚拟机复制级别容灾保护：当生产虚拟机出现故障时，备端可以接管生产端业务。支持临时切换和永久切换两种模式，临时切换支持不停止原先的同步规则。 | | |
| | | | 提供数据验证功能，要求支持源端与目标端数据进行在线的 MD5 值对比校验确保数据一致性，并生成报告。帮助用户清楚地验证生产数据和备份数据是否一致，杜绝因数据不一致导致无法恢复或数据丢失。 | | |
| | | 管理运维要求 | B/S 架构，WEB 中文操作界面，全图形化监控和管理。 | | |
| | | | 提供 WEB 管理控制台，能进行数据流量图形化统计，计算和规划带宽需求。 | | |
| | | | 提供管理控制台，具导航及配置工具。 | | |
| | | | 提供带宽及数据流控制功能，每个复制任务可根据时间动态调整带宽限制功能。 | | |
| | | | 支持电子邮件、短线告警等功能。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 提供任务的日志信息，包括用户在灾备系统上的操作，可追溯、可查询。例如复制任务的创建、执行，删除等 | | |
| | | | 支持复制任务记录功能，包括但不限于复制任务清单，每个任务的详情（启动时间，结束时间，复制过程记录等） | | |
| | | 授权要求 | 配置不少于 20 个节点的数据实时同步功能 | | |
| 2 | 备份一体机系统 | 硬件规格 | 处理器：2 颗八核 2.1G, 8C/16T, 9.6GT/s, 11M 缓存， Turbo | 1 | 台 |
| | | | 硬盘： 3.5 英寸裸容量≥192TB 存储盘。 | | |
| | | | 内存：不少于 128GB RAM。 | | |
| | | | 网络接口：4 个千兆网络端口，2 个万兆网络端口，2 个 16Gb 光纤网口 | | |
| | | 兼容性要求 | 全面支持各种数据库及应用服务，包括 Microsoft SQL Server，Oracle，MySQL，瀚高、人大金仓、达梦、优炫、南大通用等。 | | |
| | | | 支持跨平台数据复制，至少包括 Windows、Linux 及龙芯、飞腾架构下中标麒麟、银河麒麟等自主可控操作系统。 | | |
| | | | 支持 Microsoft VPC/Hyper-V, VMware 等虚拟化平台备份。 | | |
| | | 功能要求 | 提供异步字节级别的持续复制功能 | | |
| | | | 支持多规则、多并发的数据保护，灵活的规则管理策略，规则之间相互独立。 | | |
| | | | 支持数据压缩与重复数据删除功能，提高备份速度，节省存储空间。 | | |
| | | | 提供打开文件的镜像和复制功能。 | | |
| | | | 支持异构平台上各种应用和数据实时复制，比如 Windows 平台和 Linux 平台间的文件复制，同时要求灾备端文件和数据保留文件属性信息，严格保证数据的原始性和可用性 | | |
| | | | 客户端安装部署不需要生产端重启，要求在不停业务/不停机的情况下进行备份。 | | |
| | | | 提供对 VMware vSphere ESX/ESXi 虚拟化应用以虚拟机、资源池和整个集群为单位进行备份保护，无需在虚拟机内部安装代理，支持对 VMware vCenter 管理的虚拟化集群进行保护。 | | |
| | | | 支持虚拟机瞬时恢复功能；能够从生产中心和容灾中心的备份文件快速启动虚拟机用于生产，而无需将备份文件先恢复到生产存储的瞬时恢复功能。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 提供 NFS 直接访问，可通过基于文件的（NFS）主存储中直接备份，能够更快地执行 vSphere 备份、复制和还原，并降低对虚拟化环境的影响。 | | |
| | | | 支持 vSphere 环境下的 LAN-FREE 备份保护，备份数据直接通过 FC SAN/IP-SAN 写入到备份设备的磁盘中。提高备份速度，数据流不需经过 ESXI 主机，由平台直接读取存储内数据。 | | |
| | | | 支持虚拟机创建周期性演练计划，可以按照策略每天夜间自动对备份数据进行恢复，确认数据的有效性与可用性；支持虚拟机演练网络与生产网络隔离，并提供生产网访问演练网络功能。提供相关证明材料。 | | |
| | | | 支持虚拟机复制级别容灾保护：当生产虚拟机出现故障时，备端可以接管生产端业务。支持临时切换和永久切换两种模式，临时切换支持不停止原先的同步规则。 | | |
| | | | 提供数据验证功能，要求支持源端与目标端数据进行在线的 MD5 值对比校验确保数据一致性，并生成报告。帮助用户清楚地验证生产数据和备份数据是否一致，杜绝因数据不一致导致无法恢复或数据丢失。 | | |
| | | 管理运维要求 | B/S 架构，WEB 中文操作界面，全图形化监控和管理。 | | |
| | | | 提供 WEB 管理控制台，能进行数据流量图形化统计，计算和规划带宽需求。 | | |
| | | | 提供管理控制台，具导航及配置工具。 | | |
| | | | 提供带宽及数据流控制功能，每个复制任务可根据时间动态调整带宽限制功能。 | | |
| | | | 支持电子邮件、短线告警等功能。 | | |
| | | | 提供任务的日志信息，包括用户在灾备系统上的操作，可追溯、可查询。例如复制任务的创建、执行，删除等 | | |
| | | | 支持复制任务记录功能，包括但不限于复制任务清单，每个任务的详情（启动时间，结束时间，复制过程记录等） | | |
| | | 授权要求 | 配置基于硬件设备授权，配置不限制数量的文件备份模块，数据库备份模块，虚拟机备份模块，操作系统备份模块，配置数据对比模块，压缩模块，流量控制模块，永久增量模块。 | | |
| 3 | 机架式服务器 | 硬件规格 | 机架式，≤2U，标配原厂导轨 | 2 | 台 |
| | | CPU 规格 | ≥2 颗 Intel 4310(2.1GHz/12 核/18MB/120W)处理器，可支持最高 270W 处理器 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | （异地灾备恢复验证） | 内存规格 | ≥64GB 3200MHz DDR4 内存模块 | | |
| | | 内存可扩展数量 | 最大支持 32 根 DDR4 内存，最高速率 3200MT/s，支持 RDIMM 或 LRDIMM； | | |
| | | | 支持 16 根持久内存 PMem 200 系列（Barlow Pass）最大可支持内存容量高达 12TB | | |
| | | 实配硬盘 | ≥10 块 1.8TB 10K SAS HDD 硬盘。 | | |
| | | 硬盘槽位 | 本地提供≥8 个 2.5 寸硬盘槽位，支持 SAS/SATA HDD/SSD 硬盘，支持≥37 块 2.5 寸硬盘，热插拔 | | |
| | | 阵列控制器 | ≥1 个标准 PCIe 槽位阵列卡，支持 RAID0/1/10/5/6/50/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | PCI I/O 插槽 | 支持≥14 个 PCIE4.0 速率插槽。 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100/200 GE 网卡，IB 卡；本次配置≥1 张 4 口千兆网卡，≥1 张 2 口万兆网卡(含模块) | | |
| | | GPU | 支持≥4 个双宽 GPU 卡或 14 个单宽 GPU 卡。 | | |
| | | 接口 | 标配 1 个前置 VGA，1 个后置 VGA 和 1 个串口，6 个 USB 3.0（2 前置，2 后置，2 内置），1 个前置专用管理接口 | | |
| | | 冗余电源 | ≥2 个 800w 白金版热插拔冗余电源，支持 96%能效比的钛金级电源选件 | | |
| | | | 满配热插拔冗余风扇 | | |
| | | 工作温度 | 支持最高 5-45° C 标准工作温度 | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| 4 | 防火墙（异地灾备区） | 硬件规格 | 规格：1U，内存大小：≥4G，硬盘容量：≥128G SSD，电源：单电源，接口：千兆电口≥8，千兆光口 SFP≥2 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥4G，并发连接数：≥100 万，HTTP 新建连接数：≥2.5 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年的入侵防御及防病毒模块授权。 | | |
| 5 | 接入交换机-48 端口（异地灾备区接入网） | 性能要求 | 交换容量≥4.8Tbps。 | 1 | 台 |
| | | | 转发性能≥2000Mpps。 | | |
| | | 硬件规格 | 高度 1U，固定接口交换机 | | |
| | | | 配置双电源，五风扇框 | | |
| | | | 支持前后、后前风道 | | |
| | | | 整机最大功耗≤220W | | |
| | | | 工作环境温度 0℃～45℃ | | |
| | | 性能指标 | 整机最大路由地址表≥320K，最大 ARP 地址表≥270K，最大 MAC 地址表≥280K | | |
| | | 端口配置要求 | 固化 10GE 光口端口数量≥48 个，100 GE 光接口≥6 个，实配 10km 距离千兆及以上光纤模块一对。 | | |
| | | | 支持 Mini USB Console 接口 | | |
| | | 二层功能 | 支持基于端口、基于协议、基于 MAC 的 VLAN | | |
| | | | 支持动态 MAC、静态 MAC 和黑洞 MAC 表项 | | |
| | | 三层功能 | 支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议 | | |
| | | | 支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议 | | |
| | | MPLS | 支持 MPLS、MCE | | |
| | | | 支持 MPLS VPN | | |
| | | | 支持 MPLS TE | | |
| | | 可靠性 | 支持跨设备链路聚合技术 | | |
| | | | 兼容 PVST 协议，支持跨厂商生成树互通，提供第三方测试报告 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 20 台堆叠虚拟化技术 | | |
| | | DC 特性 | 实配支持 INT 可视化功能 | | |
| | | | 支持 streaming telemetry，支持线速提供可视化信息 | | |
| | | | 支持无损网络 RoCE，支持 PFC、ECN、ETS。 | | |
| | | | 端口转发时延小于 2 微秒 | | |
| | | | 支持二层、三层 Vxlan 网关和 BGP EVPN 特性 | | |
| | | | 支持服务链 Service chain 功能，提供官网截图证明 | | |
| | | 安全性 | 支持黑洞 MAC、动态 ARP 检测、ARP 防攻击 | | |
| | | | 支持 IP、MAC、端口和 VLAN 的组合绑定 | | |
| | | | 支持端口隔离 | | |
| | | | 支持 AAA、Radius 和 TACACS 认证 | | |
| | | | 支持 DHCP Snooping | | |
| | | 配置和维护 | 支持 sFlow/Netstream | | |
| | | | 支持端口镜像 ERSPAN | | |
| | | | 支持 SNMP、Telnet、RMON、SSH | | |
| | | | 支持配置回滚 | | |
| | | | 支持缓存的微突发 | | |
| | | | 支持零配置技术，配置自动下发 | | |
| 6 | 接入交换机-24 端口（异地灾备区管理网） | 性能要求 | 交换容量≥330Gbps，包转发率≥100Mpps。 | 1 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口。 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |

**3.5 管发中心内外网文件摆渡系统建设**

3.5.1 系统说明

目前管发中心下属多家社区卫生服务中心，采用的是内网及外网安全区分离部署，业务具有内网数据文件通过外网上报监管部门，及外网发布的文件数据传输到内网终端使用的需求。当前内网终端与外网终端之间的数据交换缺少有保障的文件数据交换手段，仅采用物理介质传输，容易引入安全威胁。通过建设内外网文件摆渡系统，作为内外网文件数据交互安全通道，内外网文件交互过程由文件摆渡系统负责，提供文件存储、跨安全区传输、文件内容安全审核、防病毒及用户角色权限控制等能力，确保内外网终端间文件数据交互安全可靠。

3.5.2 系统需求

1、在 6 家管发中心下属社区卫生服务中心各部署 1 套网间数据交换设备，具体部署单位在项目实施过程根据实际情况现场确定。设备内网端及外网端采用分别接入对应安全区域的方式部署，设备带外管理端单独接入安全管理区域。

2、投标人需要根据各单位的人员配置情况，对文件摆渡系统进行用户角色及权限配置，划分公共目录及私人目录，根据用户角色对传输方向，内容，进行规则限制，并配置防病毒检测策略。要求设备的防病毒等安全能力具有在线实时更新，确保安全防护能力的时效性。

3、管发中心各分支机构具有业务专线网络，要求文件摆渡系统设备管理端口可通过业务专线及同时在管发中心网络和分支机构管理网络可达。需要对设备进行管理角色和权限控制，管发中心需要具有完整系统管理员权限，分支机构具有安全管理员权限及审计管理员权限，严格执行三权分立配置模式满足三级等保要求。

3.5.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 文件摆渡系统 | 多区域隔离交换 | 单台设备支持 2 个隔离区域间文件相互交换，无需与其他设备或系统结合； | 6 | 台 |
| | | 性能要求 | 支持至少 50 名用户并发进行文件交换。 | | |
| | | 硬件规格 | 双路供电 | | |
| | | | ≥4 个千兆网口 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 存储容量≥4TB | | |
| | | 安全性 | 基于虚拟化技术，实现在不同网络间的数据安全交换。 | | |
| | | 防病毒检测 | 可对文件进行病毒和木马检测，识别可能导致系统风险的恶意文件并阻断。 | | |
| | | 审批功能 | 可根据数据交换的方向，灵活设置审批策略。可设置人工单向审批、人工多向审批或自动审批等。且需提供接口，支持与邮箱系统集成，从而实现邮件审批。（提供页面截图） | | |
| | | 公共目录 | 支持公共目录功能便于协同办公 | | |
| | | | 公共目录可设置空间的大小限制、可使用的网络侧、公共目录拥有者和应用范围、例外范围等； | | |
| | | | 可支持目录拥有者控制用户权限下放（包括上传、下载、删除、预览、编辑、子目录权限的分配）； | | |
| | | | 可支持子目录拥有者控制用户权限下放（包括上传、下载、删除、预览、编辑）； | | |
| | | 传输方向权限管控 | 支持依据网络设置指定源网络至目的网络间文件传输权限及审批控制 | | |
| | | 上传下载限速 | 支持依据网络限制指定时间段文件上传下载的速度 | | |
| | | 传输方式 | 支持用户通过客户端及 Web 页面方式传输文件；支持通过开放接口方式由服务器直接传输文件，服务器上无需安装客户端，不受操作系统限制； | | |
| | | 落地存储加密 | 文件落盘需加密存储，需符合国密算法；（提供相关证明材料） | | |

**3.6 “徐汇区区域卫生信息平台”业务专线系统升级改造**

3.6.1 系统说明

管发中心下属的 13 家社区卫生服务中心，与管发中心之间建设有“徐汇区区域卫生信息平台”业务专线系统，各家分支机构通过业务专线系统将业务数据进行上报汇总。

现有网络专线链路已建设完毕，为满足三级等保需求，对分支机构端的业务专线端点部署相应的安全设备及专用的数据上报前置机设施，确保业务系统独立安全运行。

3.6.2 系统需求

1、在下属 13 家分支机构的专线端点部署集成安全边界防火墙，作为分支机构和业务专线网络的安全边界设备，管控分支机构网络系统和管发中心网络系统间的数据交互。

2、投标人需要以最小化权限的方针为防火墙配置安全控制策略，最大化限制分支机构

与管发中心之间正常业务通讯以外的网络通讯行为，并通过防火墙的 IPS 及 AV 模块对正常业务数据的交互信息进行防病毒及入侵防护检查。确保在发生安全威胁时，阻断其通过业务专线扩散传播的途径。防火墙策略制定需要投标人在部署配置时现场依据各家分支机构的网络环境实际情况进行梳理。

3、在各分支机构的专线端点配套部署汇聚交换机，负责专线业务划分独立的安全区域，并提供专线网络内的三层路由能力，专线的管发中心端及各分支机构端之间采用三层路由模式，分割网络广播域。

4、在各分支机构部署 1 台专用数据上报前置机服务器，负责收集各机构的上报数据后通过专线系统汇总到管发中心的相应业务服务器。需配置部署好操作系统及网络设置。部分单位现有前置机服务器，性能已不满足需求，需要统一进行替换。前置机部署实施时，需配合采购单位对现有业务数据进行迁移，及必要业务软件的重新部署等工作。

5、具体的项目实施涉及的 13 家分支机构的清单如下：

徐汇区田林街道社区卫生服务中心

徐汇区康健街道社区卫生服务中心

徐汇区虹梅街道社区卫生服务中心

徐汇区斜土街道社区卫生服务中心

徐汇区湖南街道社区卫生服务中心

徐汇区天平街道社区卫生服务中心

徐汇区枫林街道社区卫生服务中心

徐汇区龙华街道社区卫生服务中心

徐汇区长桥街道社区卫生服务中心

徐汇区漕河泾街道社区卫生服务中心

徐汇区凌云街道社区卫生服务中心

徐汇区徐家汇街道社区卫生服务中心

徐汇区华泾镇社区卫生服务中心

3.6.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 防火墙（区 | 硬件规格 | 规格：1U，内存大小：≥4G，硬盘容量：≥128G SSD，电源：单电源，接口：千兆电口≥8，千兆光口 SFP≥2 | 13 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 域卫生信息平台边界） | 性能要求 | 网络层吞吐量：≥4G，应用层吞吐量：1G，防病毒吞吐量：≥500M，IPS 吞吐量：≥300M，并发连接数：≥100 万,HTTP 新建连接数：≥2.5 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | 应用识别 | 支持应用管控功能，应用特征识别库数量大于 8000 种。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG,支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 加密流量安全防护 | 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年入侵防御及防病毒模块授权。 | | |
| 2 | 汇聚交换机-24 端口（区域卫生信息平台站点汇聚） | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps | 13 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 3 | 机架式服务器（区域卫生信息平台前置机） | 硬件规格 | 机架式，≤2U，标配原厂导轨。 | 13 | 台 |
| | | CPU 规格 | ≥2 颗 Intel 4310(2.1GHz/12 核/18MB/120W）处理器，可支持最高 270W 处理器 | | |
| | | 内存规格 | ≥64GB 3200MHz DDR4 内存模块 | | |
| | | 内存可扩展数量 | 最大支持 32 根 DDR4 内存,最高速率 3200MT/s，支持 RDIMM 或 LRDIMM; | | |
| | | | 支持 16 根持久内存 PMem 200 系列（Barlow Pass）最大可支持内存容量高达 12TB | | |
| | | 实配硬盘 | ≥4 块 1.2TB 10K SAS HDD 硬盘。 | | |
| | | 硬盘槽位 | 本地提供≥8 个 2.5 寸硬盘槽位,支持 SAS/SATA HDD/SSD 硬盘，支持≥37 块 2.5 寸硬盘，热插拔 | | |
| | | 阵列控制器 | ≥1 个标准 PCIe 槽位阵列卡，支持 RAID0/1/10/5/6/50/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | PCI I/O 插槽 | 支持≥14 个 PCIE4.0 速率插槽。 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100/200 GE 网卡，IB 卡；本次配置≥1 张 4 口千兆网卡,≥1 张 2 口万兆网卡(含模块） | | |
| | | GPU | 支持≥4 个双宽 GPU 卡或 14 个单宽 GPU 卡 | | |
| | | 接口 | 标配 1 个前置 VGA，1 个后置 VGA 和 1 个串口，6 个 USB 3.0（2 前置，2 后置，2 内置），1 个前置专用管理接口 | | |
| | | 冗余电源 | ≥2 个 800W 白金版热插拔冗余电源，支持 96%能效比的钛金级电源选件 | | |
| | | | 满配热插拔冗余风扇 | | |
| | | 工作温度 | 支持最高 5-45° C 标准工作温度 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |

**3.7 徐汇区疾病预防控制中心信息系统升级改造**

3.7.1 系统说明

徐汇区疾病预防控制中心信息系统整体支撑徐汇区疾病预防控制中心的各项信息化业务运行需求。随着业务的逐渐发展和网络威胁形势的日益严峻，系统现有的业务承载能力和信息安全能力已不满足当前需求。通过对系统进行升级改造，强化系统的整体能力。

3.7.2 系统需求

1、现有核心交换机设备及服务器区汇聚交换机设备的路由交换性能已不满足业务要求，需采用 2 台核心交换机设备及 2 台服务器区汇聚交换机设备对现有的内网核心交换机及服务器汇聚交换机设备进行替换割接。同时配套路由交换链路中所需的光模块实现设备连接。现有服务器汇聚交换机，新设备部署后现有设备需要利旧作为带外管理安全区的接入交换机，相关配置需要重新配置。

2、根据三级等保要求，需采用 2 台防火墙设备高可用方式部署，作为服务器区安全边界防火墙，对现有老旧服务器区边界防火墙进行替换。将计算资源部分进行边界安全隔离。

3、部署 1 套数据库防火墙设备，通过在客户端和数据库之间串联的拓扑方式，对计算资源区域中的数据库业务进行相应防护，确保业务数据库信息安全。

4、现有 1 台入侵检测系统设备，其性能已不满足业务需求，采用 1 台入侵检测设备对现有设备进行升级替换。

5、部署 1 套安全态势感知设备，以实现对安全攻击检测能力、网络安全分析能力、用户行为分析能力等，对整体系统的安全性进行提升。

6、现有服务器区边界防火墙需要利旧移动至“院院通”专线出口边界，相关策略及配置需要重新配置。

3.7.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 核心交换机（疾控） | 性能要求 | 交换容量≥380Tbps，包转发率≥72000Mpps。 | 2 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 硬件规格 | 业务插槽数≥6，主控引擎模块≥2，配置双主控，双交换网板，双电源，双风扇;配置1块48端口万兆光板卡，1块48端口千兆电板卡，实配3米万兆SFP+堆叠线缆。 | | |
| | | 接口配置 | 支持千兆电口，千兆光口，万兆光口、万兆电口、25G端口、40G端口、100G端口 | | |
| | | | 支持单槽位万兆电端口密度≥48，单槽位万兆端口密度≥48；单槽位40G端口密度≥ 16，单槽位100G端口密度≥16 | | |
| | | 链路聚合 | 支持DRNI跨设备链路聚合,支持对广播、组播、单播报文的均匀分担 | | |
| | | QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法 | | |
| | | | 支持流量整形Shapping | | |
| | | 堆叠 | 支持4框虚拟化技术，支持16条40G/100G堆叠链路，堆叠带宽能达到双向3.2T | | |
| | | 智能网管 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级 | | |
| | | 可靠性 | 支持 INQA 功能，通过直接对业务报文进行标记的方法，实现对网络级和设备级的丢包统计 | | |
| | | | 支持主控板冗余，倒换时间为0ms | | |
| | | | 支持NSF/GR for OSFP/BGP/IS-IS | | |
| | | | 支持热补丁功能，可在线进行补丁升级 | | |
| | | 可视化 | 支持Telemetry流量可视化功能 | | |
| | | 融合 | 支持融合 AC 功能：无需额外配置单独硬件，并能在交换机上对所有上线的AP进行管理与配置 | | |
| | | MPLS | 支持L3 VPN，支持VLL，支持VPLS | | |
| | | 安全特性 | 支持全端口MACsec加密技术,密钥长度为256bit，支持可信计算：支持设备可信自检、证书签发功能 | | |
| | | NAS | 支持802.1x认证，支持mac认证，支持 IPv4 Portal、IPv6 Portal 及 Portal 双协议栈功能 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 2 | 汇聚交换机-48 端口（服务器） | 性能要求 | 交换容量≥430Gbps，包转发率≥160Mpps，具备双电源 | 2 | 台 |
| | | 硬件规格 | 支持 48 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 3 | 千兆多模光模块 | 硬件规格 | 光模块-SFP-GE-多模模块-(850nm,0.55km,LC) | 24 | 个 |
| 4 | 万兆多模光模块 | 硬件规格 | 光模块-SFP+-10G-(850nm,300m,LC) | 48 | 个 |
| 5 | 防火墙（服务器区） | 硬件规格 | 规格：≤2U，内存大小：≥8G，硬盘容量：≥128G SSD，电源：冗余电源，接口：千兆电口≥8，万兆光口 SFP+≥2 | 2 | 台 |
| | | 性能要求 | 网络层吞吐量：≥15G，并发连接数：≥200 万，HTTP 新建连接数：≥9 万 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年入侵防御及防病毒模块授权。 | | |
| 6 | 安全态势感知平台系统 | 硬件规格 | 规格：≤2U，内存大小：≥16G，硬盘容量：≥128GB SSD+4TB SATA，电源：单电源，接口：千兆电口≥6，万兆光口 SFP+≥2 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥1Gbps | | |
| | | 大屏可视 | 支持大屏轮播及自定义大屏顺序设置和大屏名称。自定义统计周期资产组划分、选择播放大屏及轮播时间间隔。 | | |
| | | 数据中心可视 | 可视区域基于数据中心、总部、租户等按照风险等级（优秀、良、中、差）来展示数据中心的情况。支持对数据中心正常反问的趋势和攻击者监视和分析威胁的说明。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 弱口令检测 | 弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web 空密码、账号白名单、密码白名单、txt 文件格式导入。 | | |
| | | 资产全生命周期管理 | 支持自定义资产多级分支管理，最多可至 15 级分支。支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。 | | |
| | | 资产发现 | 支持通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、MAC 地址、主机名等。 | | |
| | | 文件威胁分析 | 文件威胁分析支持平台内置的静态文件检测引擎，利用多种机器学习算法组合进行综合研判。支持采用 AI 技术针对无文件落地的恶意脚本进行检测。 | | |
| | | 异常流量分析 | 支持按照对外业务流量可视、横向流量可视、外联流量可视等开放的业务流量情况，展示服务器流量排行、最活跃源主机的内网服务器的流量情况，支持全球地图展示整体外联流量情况。 | | |
| | | DNS 日志接入 | 支持 DNS 服务器日志导入，可以接入 DNS 服务器的日志，安全分析引擎将结合 DNS 服务器的日志，定位出 DNS 服务器代理风险外连场景下真实源 IP，从而有效地进行风险处置闭环。 | | |
| 7 | 数据库防火墙系统（安全管理区） | 硬件规格 | 2U 机架式设备，内存≥32G DDR4，硬盘≥4T SATA 盘， | 1 | 台 |
| | | | 网口≥6 个千兆电口，冗余电源。 | | |
| | | 性能要求 | 默认流量≥100Mbps，数据库实例≥32 个，峰值 SQL 吞吐≥10000 条语句/秒。 | | |
| | | 数据库支持 | 支持 ORACLE、MYSQL、SQLSERVER、DB2、GBASE8.3S、HIVE、达梦、PG、人大金仓、优炫、Mongodb、SYBASE 等。 | | |
| | | 数据源发现 | 支持按单个 IP 或 IP 段发现数据源。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 防护策略能力 | 内置数据库漏洞虚拟补丁能力，且补丁库不少于 1600 个,可阻止黑客通过这些漏洞进行攻击； | | |
| | | | 注入攻击监控、漏洞攻击监控、敏感访问监控、系统运行监控、流量监控。 | | |
| | | | 支持数据库防漏扫，当特定的漏洞扫描器对数据库进行扫描时，实现防御拦截。 | | |
| | | | 通过对 SQL 特征进行识别，生成注入特征库，对 SQL 注入攻击进行防护。 | | |
| | | | 自动学习业务 SQL，捕获 SQL 语法，生成 SQL 白名单，通过 SQL 白名单进行访问控制。 | | |
| | | | 支持检测和审计密码猜测行为，通过设置密码猜测次数限制进行防护，当达到密码猜测限制时,锁定猜测终端，支持自动解锁和手工解锁。 | | |
| | | | 通过识别数据库自身的漏洞，通过虚拟补丁的方式进行防护，防止黑客利用数据库漏洞进行攻击。 | | |
| | | | 支持透明代理模式下的可信 IP，将加入到可信 IP 列表中的可信的终端设备 IP 地址,终端设备与数据库通信的流量将会进行 bypass 处理。 | | |
| | | | 支持多维身份管理，至少支持应用程序名、IP 地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U 盾等因素进行任意组合，形成新的登陆认证规则。 | | |
| | | | 支持敏感数据发现、敏感数据分级分类（提供相关证明材料）。 | | |
| | | 业务脱敏 | 支持业务系统查询数据时的动态脱敏，根据用户的身份与访问的数据库对象以及对应的脱敏规则，对不同授权的用户可返回真实数据、部分遮盖、全部遮盖以及其他脱敏算法得到的结果（提供相关证明材料）。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 脱敏规则需要支持以下脱敏算法：<br>放行：对于已授权用户，返回真实数据；<br>返回空：对含有敏感表格或敏感列的数据结果返回为空值；<br>遮盖：全遮盖：默认以遮盖符‘*’替换敏感列的值；<br>部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值；<br>随机映射：对数值、字符或字符串进行随机映射处理。 | | |
| | | 风险响应策略 | 支持风险响应策略，对不同信任度的身份和风险等级设置不同的响应行为（通过、告警、阻断行为、阻断连接）。 | | |
| | | 系统管理 | 支持双因子认证，支持短信认证、证书认证。 | | |
| | | 告警通知 | 支持多种安全响应措施，包括页面、邮件、短信方式进行告警。 | | |
| | | 报表生成方式 | 支持登录事件、访问事件、风险事件、告警事件等报表的生成。 | | |
| | | 三权分立 | 支持三权分立，可以对用户权限进行控制，三种账号互相约束。 | | |
| 8 | 入侵检测系统 | 硬件规格 | 规格：≤2U，内存大小：≥8G，硬盘容量：≥128G SSD，电源：冗余电源，接口：千兆电口≥8，万兆光口 SFP+≥2 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥15G，IPS 吞吐量：≥1G，并发连接数：≥200 万，HTTP 新建连接数：≥9 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | 应用识别 | 支持应用管控功能，应用特征识别库数量大于 8000 种。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 加密流量安全防护 | 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年功能及模块授权。 | | |

**3.8 徐汇区中心医院信息安全系统升级改造**

3.8.1 系统说明

徐汇区中心医院信息安全系统负责对其医疗信息化业务运行提供信息安全保障，通过合理组合各类用途的信息安全设备，对徐汇区中心医院提供三级等保要求所需的各项安全能力。

3.8.2 系统需求

1、 根据三级等保要求，需要部署 1 套终端准入控制系统，负责对内网有线安全区域的终端进行准入认证控制。终端准入控制系统应同时采用管理网段带外接入及三层旁路方式部署，通过 802.1x 协议对接路由交换部分中各接入层交换机，对终端进行端口级的准入控制。对无线终端进行 portal 准入控制。根据现有网络设备组网方式终端准入控制系统需支持基于 802.1x 的动态 ACL 下发的管控模式，通过三层对接下发动态 ACL 控制设备准入范围。

2、 高可用部署 2 套数据库防火墙系统，通过串联在客户端和服务器之间的拓扑方式，对数据库服务器进行安全防护及审计，确保业务数据库中的数据安全。

3、 部署 1 套全流量安全回溯取证系统，通过旁路镜像拓扑方式对网络链路中的全流量进行流量采集，分析取证网络中的行为。

4、 部署 1 台数据信息保护系统，与计算资源集群配置对接，实现对数据信息的实时保护。

5、 为满足安全设备部分中对各设备的运行情况进行整合管理的需要，部署 1 套信息

安全保障体系管控平台系统，通过对系统中各设备进行管理协议对接，实现对信息资产设备及信息安全设备进行统一的监控及管理。

6、 部署 1 台安全网关设备，对网络安全区域边界网关进行安全防御。

7、 现有 2 台安恒品牌的 DAS-NGFW2900 型号防火墙设备及 2 台安恒品牌的 WAF-1000AG 型号 WAF 防火墙设备，均已出保。需提供该 4 台设备为期 1 年的原厂授权服务，除设备硬件质保外，DAS-NGFW2900 设备原厂授权服务还需包括 IPS 及 AV 功能模块授权及特征库更新，WAF-1000AG 设备原厂授权服务还需包括 WAF 功能模块授权及特征库更新。

3.8.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 终端准入控制系统 | 硬件规格 | 最大可支持准入终端数不少于2000，电源：冗余双电源，接口：千兆电口≥4，具备不少于 2 个可拓展万兆的拓展槽。 | 1 | 台 |
| | | 系统架构 | 管理平台和准入网关支持一体化部署，也可采用分离部署架构； | | |
| | | | 设备无需其他计算资源独立运行； | | |
| | | | 管理平台支持对多个准入硬件网关设备进行统一集中管控； | | |
| | | 部署模式 | 支持 802.1x、WebAuth、Portal、端口镜像、策略路由、客户端等多种准入控制方式混合使用，一个系统可同时使用多种准入方式适应复杂网络环境； | | |
| | | | 准入未放行前支持 web 重定向、邮件重定向方式引导； | | |
| | | | 支持客户端准入控制阻断和提醒模式，可提醒并帮助用户自助安装客户端； | | |
| | | | 支持分级部署，设置统一管理平台，对不同的地区、部门使用的服务端进行分级部署； | | |
| | | | 支持分布式部署，可将系统自身功能组件（radius、web、数据库等组件、审计文档服务器等）独立模块化分布式部署。 | | |
| | | 功能拓展 | 支持客户端准入控制，可拓展一定桌面管理、终端检测响应等功能模块； | | |
| | | | 支持扩展对主流国产化 PC 系统的功能支持； | | |
| | | 策略管理 | 支持指定设备、设备组、用户、用户组、部门、IP、MAC 下发策略，支持策略离线生效，支持例外策略下发管理； | | |
| | | | 支持策略场景定义客户端在线、客户端离线等状态，等采取不同策略。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 客户端模式防护 | 支持客户端自我防护机制，客户端文件、进程、注册表、服务等都无法停止、修改、删除；客户端正常运行情况下安装目录隐藏； | | |
| | | | 支持客户端安全模式下运行，客户端策略依然生效； | | |
| | | | 支持客户端功能在线调整，在功能调整、问题验证等场景下支持客户端文件（配置文件、DLL 等）实时替换，无需覆盖安装、重启终端； | | |
| | | | 支持 Windows、macOS、Linux 客户端； | | |
| | | 802.1x 准入 | 支持 802.1x 有线无线网络环境下主流网络设备的动态 VLAN 切换（Guest VLAN、修复 VLAN、工作 VLAN）； | | |
| | | | 支持 802.1x 有线无线网络环境下主流网络设备的 ACL 动态下发；（提供系统截图证明） | | |
| | | | 支持 802.1x 技术下，终端通过 HUB 接入场景，每个终端分别进行认证； | | |
| | | 资产发现识别 | 支持自动发现识别接入设备的类型，包括：PC 设备、网络设备、服务器、移动设备、IoT 设备等； | | |
| | | | 支持自定义添加设备类型识别规则条件，以操作系统、开放端口、设备名、MAC 地址前缀、MAC 地址厂商、IP 地址范围等条件设置权重，自动将设备匹配归纳到新添加的设备类型列表中，自动分配网络访问权限。 | | |
| | | 身份认证对接 | 支持多种身份认证源：内置账户，AD/LDAP 用户，邮件服务器用户、证书认证，第三方 RADIUS 服务器认证，第三方扩展认证； | | |
| | | 策略准入功能 | 支持用户与计算机 MAC 地址、接入交换机端口号、接入控制点设备、客户端生成的主机码和随机码绑定；可对终端硬件生成唯一 ID、认证用户等进行灵活绑定； | | |
| | | | 支持 1 对 1，1 对多绑定，并支持设置对某用户在一定数量范围内的终端自动放行。 | | |
| | | | 支持应急逃生，系统检测到运行中出现的异常和故障需要能够自动应急；一定时间内连续出现多台终端准入失败自动临时放行且阈值可自定义（分钟级别），确保企业网络的可用性； | | |
| | | 功能授权 | 提供不少于 300 个终端准入控制授权。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 2 | 数据库防火墙系统 | 硬件规格 | 2U 机架式设备，内存≥32G DDR4，硬盘≥4T SATA 盘， | 2 | 台 |
| | | | 网口≥6 个千兆电口，冗余电源。 | | |
| | | 性能要求 | 默认流量≥100Mbps，数据库实例≥32 个，峰值 SQL 吞吐≥10000 条语句/秒。 | | |
| | | 数据库支持 | 支持 ORACLE、MYSQL、SQLSERVER、DB2、GBASE8.3S、HIVE、达梦、PG、人大金仓、优炫、Mongodb、SYBASE 等。 | | |
| | | 数据源发现 | 支持按单个 IP 或 IP 段发现数据源。 | | |
| | | 防护策略能力 | 内置数据库漏洞虚拟补丁能力，且补丁库不少于 1600 个，可阻止黑客通过这些漏洞进行攻击。 | | |
| | | | 注入攻击监控、漏洞攻击监控、敏感访问监控、系统运行监控、流量监控。 | | |
| | | | 支持数据库防漏扫，当特定的漏洞扫描器对数据库进行扫描时，实现防御拦截。 | | |
| | | | 通过对 SQL 特征进行识别，生成注入特征库，对 SQL 注入攻击进行防护。 | | |
| | | | 自动学习业务 SQL，捕获 SQL 语法，生成 SQL 白名单，通过 SQL 白名单进行访问控制。 | | |
| | | | 支持检测和审计密码猜测行为，通过设置密码猜测次数限制进行防护，当达到密码猜测限制时，锁定猜测终端，支持自动解锁和手工解锁。 | | |
| | | | 通过识别数据库自身的漏洞，通过虚拟补丁的方式进行防护，防止黑客利用数据库漏洞进行攻击。 | | |
| | | | 支持透明代理模式下的可信 IP，将加入到可信 IP 列表中的可信的终端设备 IP 地址，终端设备与数据库通信的流量将会进行 bypass 处理。 | | |
| | | | 支持多维身份管理，至少支持应用程序名、IP 地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U 盾等因素进行任意组合，形成新的登陆认证规则。 | | |
| | | | 支持敏感数据发现、敏感数据分级分类 | | |
| | | 业务脱敏 | 支持业务系统查询数据时的动态脱敏，根据用户的身份与访问的数据库对象以及对应的脱敏规则，对不同授权的用户可返回真实数据、部分遮盖、全部遮盖以及其他脱敏算法得到的结果。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 脱敏规则需要支持以下脱敏算法： | | |
| | | | 放行：对于已授权用户，返回真实数据； | | |
| | | | 返回空：对含有敏感表格或敏感列的数据结果返回为空值； | | |
| | | | 遮盖：全遮盖：默认以遮盖符‘*’替换敏感列的值； | | |
| | | | 部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值； | | |
| | | | 随机映射：对数值、字符或字符串进行随机映射处理。 | | |
| | | | 支持业务账号的授权脱敏 | | |
| | | | 支持应用全脱敏 | | |
| | | 风险响应策略 | 支持风险响应策略，对不同信任度的身份和风险等级设置不同的响应行为（通过、告警、阻断行为、阻断连接）。 | | |
| | | 系统管理 | 支持双因子认证，支持短信认证、证书认证。 | | |
| | | 告警通知 | 支持多种安全响应措施，包括页面、邮件、短信方式进行告警。 | | |
| | | 报表生成方式 | 支持登录事件、访问事件、风险事件、告警事件等报表的生成。 | | |
| | | 三权分立 | 支持三权分立，可以对用户权限进行控制，三种账号互相约束。 | | |
| 3 | 数据信息保护系统 | 硬件规格 | 处理器核心≥8 核心 16 线程，处理器主频≥2.4GHz，内存≥32GB | 1 | 台 |
| | | 存储空间要求 | 具有≥32TB 的存储空间 | | |
| | | | 至少采用 RAID5 模式的多盘冗余阵列，盘数≥6 盘位 | | |
| | | 数据保护功能 | 支持实时保护数据 | | |
| | | | 支持双向保护数据 | | |
| | | | 支持 Windiws 及 Linux 等主流操作系统 | | |
| 4 | 全流量安全回溯取证系统 | 硬件规格 | CPU≥10 线程 | 1 | 台 |
| | | | 内存≥96GB DDR4 | | |
| | | | 硬盘≥16T | | |
| | | | 网络接口：2 电口+2 光口 | | |
| | | 性能要求 | 数据采集性能：2000Mb/s | | |
| | | 功能要求 | 通过对网络链路全流量采集存储、全数据分析，面对更底层的网络数据包，其中包含更多信息元素，提供真实且充分的数据依据； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 集合深度报文解析、数据双向验证、网络数据的建模分析与可视化等技术，提升威胁检测精度和效率； | | |
| | | | 实现重点资产分析、安全策略评估，事中发现漏洞利用、木马通讯、异常检测、应急响应，事后对攻击过程进行回放，处置效果评估提供更有效的监测手段。解决传统网络安全措施无法解决的问题，建立紧密贴合用户专属场景的自适应安全网络架构 | | |
| 5 | 信息安全保障体系管控平台 | 硬件规格 | 硬件参数：规格：2U，内存大小：≥48G，硬盘容量：≥128GB SSD+4TB SATA，电源：冗余电源，接口：千兆电口≥4，千兆光口SFP≥4 | 1 | 台 |
| | | 部署模式 | 支持网桥、路由、旁路模式部署 | | |
| | | 平台要求 | 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 | | |
| | | | 支持双因素认证功能，用户需在登录时进行双重认证，以此提高用户的安全性。 | | |
| | | | 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。 | | |
| | | 网管中心要求 | 支持对采用 SNMP V1、V2、V3 和 ICMP 等网络管理协议的主流品牌网络设备的监控。 | | |
| | | | 可自动扫描主流品牌的无线 AC、AP，对连接数、在线用户数、上下行吞吐量等无线 AC/AP 设备实时数据 | | |
| | | 功能授权 | 配置不少于 30 台设备的 IT 管理平台授权 | | |
| 6 | 安全网关设备 | 硬件规格 | CPU≥2 核；内存≥2GB；硬盘≥500GB HDD。标准 1U 机架式设备。 | 1 | 台 |
| | | | 标准 1U 机架式设备，千兆电口≥10 个，千兆 SFP/RJ45 Combo 口≥2 个，可进行 Bypass。 | | |
| | | 性能要求 | 网络吞吐性能≥4Gbps，每秒新建连接数≥4 万条，最大并发连接数≥150 万条 | | |
| | | SSL VPN 性能 | 具备 SSL VPN 功能，并发用户数≥400 个。 | | |
| 7 | 防火墙设备授权 | 授权说明 | 适用于安恒 DAS-NGFW2900 设备<br>IPS 及 AV 功能模块、特征库更新授权及原厂质保 1 年，2 套 | 1 | 项 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 8 | WAF 防火墙授权 | 授权说明 | 适用于安恒 WAF-1000AG 设备<br>WAF 功能模块、特征库更新授权及原厂质保 1 年，2 套 | 1 | 项 |

**3.9 徐汇区大华医院信息安全系统升级改造**

3.9.1 系统说明

徐汇区大华医院信息安全系统负责对其信息化业务进行安全防护，通过部署各类信息安全设备，组合不同设备的安全能力，满足安全需要。根据三级等保要求，对徐汇区大华医院进行信息安全系统升级改造。

3.9.2 系统需求

1、 部署专线接入区防火墙，采用串行在专线端点和客户端之间的拓扑作为“院院通”专线接入区边界设备，通过其网络安全策略及防火墙 IPS 及 AV 模块对专线业务进行防护。

2、 采用 2 台互联网边界防火墙高可用部署，作为互联网接入区域边界，确保互联网接入安全区边界独立，与业务区域分离。

3、 采用 1 台内网无线区域边界防火墙，建设内网无线网独立安全区边界，将内网无线网络区域与有线网络区域分离，将无线终端需要访问的业务细化控制，进行访问权限最小化控制。

4、 根据三级等保要求中对安全管理区独立的要求采用 2 台安全运维区边界防火墙，建设独立的安全运维区域，并根据现场实际情况将现有相关网络安全设备的拓扑位置及管理端口统一移动到安全运维区域，实现设备的业务数据及管理数据分流。该安全运维区边界防火墙须支持 HTTPS 解密功能，支持 TCP 和 SSL 代理访问，确保数据链路层信息的保密性和完整性。

5、 本系统中本次项目采购的防火墙设备均需要配备 IPS 及 AV 功能模块，以满足三级等保的要求，实现对连接进行入侵检测及防病毒保护的能力。

6、 为满足设备的日志审计需求和三级等保中对内外网日志分别分区审计的要求，部署 2 套日志审计系统，分别收集内网安全区与外网安全区的设备日志并进行日志记录、分析及审计。

7、 在外网安全区业务数据库部署 1 套数据库审计系统，对外网安全区数据库服务器的数据交互进行日志记录审计。现有计算资源采用虚拟化集群部署，数据库与应用服务器

交互数据流在集群中终结，故数据库审计系统需采用 Agent 模式部署。同时外网数据库审计系统还需支持端口镜像组网方式。

8、 现有亚信防毒墙系统 1 套，其授权已经过期。需要提供 1 年的设备维保，版本升级，及特征库升级的原厂授权，保障设备的安全能力。

9、现有态势感知系统 1 套对网络流量进行监控，但虚拟化业务服务器流量交互在集群节点内完成，无法通过态势感知系统抓取。需提供虚拟化环境流量探针软件的为期 3 年的软件授权，作为态势感知系统的功能补充，实现对虚拟化环境的流量监控能力。需要将虚拟化探针 Agent 部署在相应虚拟机系统中。

10、提供 4 套灾备恢复系统软件系统为期 3 年的授权，分别对医院的 HIS 业务、LIS 业务、CIS 业务及 NIS 业务数据库提供容灾恢复保护。提供的软件系统应具有针对医疗行业信息系统的特性，具有适合医疗行业数据库的功能。

3.9.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 防火墙(专线接入区) | 硬件规格 | 规格：≤2U，内存大小：≥8G，硬盘容量：≥128G SSD，电源：冗余电源，接口：千兆电口≥8，万兆光口 SFP+≥2。 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥15G，并发连接数：≥200 万，HTTP 新建连接数：≥9 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截,压缩层数支持10层及以上。 | | |
| | | 入侵防御 | 产品内置不低于7000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。 | | |
| | | 功能授权 | 包括不少于3年的入侵检测及防病毒模块授权。 | | |
| 2 | 防火墙(互联网边界) | 硬件规格 | 规格：≤2U，内存大小：≥8G，硬盘容量：≥128G SSD，电源：冗余电源，接口：千兆电口≥8，万兆光口SFP+≥2。 | 2 | 台 |
| | | 性能要求 | 网络层吞吐量：≥15G，并发连接数：≥200万，HTTP新建连接数：≥9万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括ACL控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防DDOS攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持BGP、RIP、OSPF等常见动态路由协议。 | | |
| | | NAT功能 | 支持NAT穿透技术ALG,支持FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323等协议。 | | |
| | | IPv6功能 | 支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制 | | |
| | | URL分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的URL分类库。 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截,压缩层数支持10层及以上。 | | |
| | | 入侵防御 | 产品内置不低于7000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 功能授权 | 包括不少于 3 年的入侵检测及防病毒模块授权。 | | |
| 3 | 防火墙(内网无线区) | 硬件规格 | 支持 14 个千兆电接口，8 个千兆光接口，8 个万兆光接口，4 个扩展槽位，2 个 MGMT 接口。 | 1 | 台 |
| | | 性能要求 | 防火墙吞吐量≥25Gbps，应用层吞吐量≥15Gbps，最大并发连接数≥1000 万，每秒新建连接数≥24 万；SSL VPN 并发用户不低于 10000； | | |
| | | | IPSec VPN 隧道数不少于 7500。 | | |
| | | VPN | 支持 IPsec VPN 隧道自动建立，无需流量触发；实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能；支持 IPsec VPN 智能选路，根据隧道质量调度流量 | | |
| | | 存储 | 支持 480G SSD 硬盘 | | |
| | | 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。 | | |
| | | | NAT 地址池支持动态探测和可用地址分配 | | |
| | | 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，便于用户更好地管理安全策略。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | WEB 安全防护 | 可针对HTTP/HTTPS的安全策略来专门为Web应用提供保护。对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。 | | |
| | | | 支持SQL注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库等设备的专属特征分类，支持CC攻击防护，可基于检测请求报文头的X-forward-for字段，以获取真正的源IP地址；WAF规则支持用户自定义,同时支持导入和导出功能 | | |
| | | | 支持至少4000种的Web特征的攻击检测和防御 | | |
| | | 应用识别 | 支持至少6000条的应用识别，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。 | | |
| | | 终端识别 | 当终端流量流经设备时，设备可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时（比如将原厂商的摄像头换为其他厂商的摄像头）向用户发送日志，提示用户。 | | |
| | | URL 过滤 | 设备提供预分类的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地址库进行全面实时核查。 | | |
| | | 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。且缺省动作支持黑名单。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。IPS 发现攻击后抓取报文，并支持通过 WEB 下载对应抓包文件，供客户进行分析 | | |
| | | | 支持超过 14000 种特征的攻击检测和防御 | | |
| | | 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 | | |
| | | 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。 | | |
| | | | 支持报文示踪功能，支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和连接数限制等）对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。 | | |
| | | 国密算法 | 支持国密 SM1/2/3/4 算法 | | |
| | | DDoS 防护 | 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 | | |
| | | | 支持防范 DOS/DDOS 攻击； | | |
| | | 功能授权 | 包括不少于 3 年的入侵检测及防病毒模块授权。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 4 | 防火墙(安全运维区) | 硬件规格及性能要求 | 规格：2U，内存大小：≥8G，硬盘容量：≥128G SSD+480G SSD，电源：冗余电源，接口：千兆电口≥16，千兆光口 SFP≥2，万兆光口 SFP+≥4。 | 2 | 台 |
| | | 性能要求 | 网络层吞吐量：≥20G，应用层吞吐量：≥10G，防病毒吞吐量：≥1.5G，IPS 吞吐量：≥1.5G，全威胁吞吐量：≥1G，并发连接数：≥210 万，HTTP 新建连接数：≥13 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | 应用识别 | 支持应用管控功能，应用特征识别库数量大于 8000 种。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 加密流量安全防护 | 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包括不少于 3 年的入侵检测及防病毒模块授权。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 5 | 日志审计设备(外网区) | 硬件规格 | 2U 机架式设备，内存≥64G，硬盘≥4T*2，网口≥4 个千兆电口，≥1 个管理口，冗余电源。 | 1 | 台 |
| | | 性能要求 | 日志源≥150 个,日志处理性能≥8000EPS. | | |
| | | 系统架构 | 系统应基于大数据平台架构，具备海量数据收集与快速检索能力。 | | |
| | | | 系统应基于 B/S 架构，支持 SSL 加密模式访问，可通过 web 方式直接对系统进行管理。 | | |
| | | 基础要求 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统。 | | |
| | | | 审计工作不影响被审计对象的性能、稳定性或日常管理流程。 | | |
| | | | 审计结果存储于独立存储空间。 | | |
| | | | 自身用户管理与设备或主机的管理、使用、权限无关联。 | | |
| | | | 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件。 | | |
| | | 日志采集 | 支持 Syslog（UDP、TCP）、目录、远端软件（FTP、SFTP、HDFS、LOCAL）、WMI、SNMP（Trap）、数据库（ORACLE、DB2、MYSQL、SQLITE、POSTGRES、SQLSERVER）协议日志收集。 | | |
| | | | 支持使用代理（Agent）方式提取日志并收集。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 系统支持采集的设备厂家包括但不限于：NSFOCUS（绿盟科技）、Venustech（启明星辰）、Topsec（天融信）、DBAPP Security（安恒）、SANGFOR（深信服）、Hillstone（山石网科）、东软、瑞星、金山、网康、360 网神、DPtech（迪普）、艾科网信、Imperva、Juniper（瞻博网络）、F5、Symantec（赛门铁克）、Deep Security（趋势科技）、MacAfee（迈克菲）、Fortinet（飞塔）、Windows、Linux/Unix、Cisco（思科）、HUAWEI（华为）、H3C（华三）、中兴、Apache、nginx 、IIS、WebLogic、VMware、KVM、Xen、OpenStack、Hyper-V、华为 FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等。 | | |
| | | | 系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。 | | |
| | | 日志分析 | 支持对设备日志查询和聚合分析。 | | |
| | | | 系统内置常见安全事件关联分析规则。 | | |
| | | | 支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。 | | |
| | | 日志审计 | 支持 SOX 审计包含 SOX 登录事件、SOX 对象访问、SOX 账号管理、SOX 策略更改。 | | |
| | | | 支持 PCI 审计包含 PCI 策略更改、PCI 对象访问、PCI 登录事件。 | | |
| | | | 支持 WEB 访问分析包含 WEB 访问概况、WEB 访问客户端分析、WEB 访问地区分析、WEB 异常访问分析。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 ISO27001 审计包含 ISO27001 对象访问、ISO27001 策略更改、ISO27001 账号管理、ISO27001 登录事件。 | | |
| | | 数据查询 | 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、地理城市等参数进行过滤查询 | | |
| | | | 支持可指定多个查询条件进行组合查询。 | | |
| | | 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义。 | | |
| | | | 基于角色的权限管理机制，通过角色定义支持多用户访问。 | | |
| | | 平台部署 | 支持多分支级联传输，统一审计和管理，并集中展现。 | | |
| 6 | 日志审计设备(内网区) | 硬件规格 | 2U 机架式设备，内存≥64G，硬盘≥8T*3，网口≥4 个千兆电口，冗余电源。 | 1 | 台 |
| | | 性能要求 | 日志源≥500 个，日志处理性能≥10000EPS。 | | |
| | | 系统架构 | 系统应基于大数据平台架构，具备海量数据收集与快速检索能力。 | | |
| | | | 系统应基于 B/S 架构，支持 SSL 加密模式访问，可通过 web 方式直接对系统进行管理。 | | |
| | | 基础要求 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统。 | | |
| | | | 审计工作不影响被审计对象的性能、稳定性或日常管理流程。 | | |
| | | | 审计结果存储于独立存储空间。 | | |
| | | | 自身用户管理与设备或主机的管理、使用、权限无关联。 | | |
| | | | 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 日志采集 | 支持 Syslog（UDP、TCP）、目录、远端软件（FTP、SFTP、HDFS、LOCAL）、WMI、SNMP（Trap）、数据库（ORACLE、DB2、MYSQL、SQLITE、POSTGRES、SQLSERVER）协议日志收集（提供相关证明材料）。 | | |
| | | | 支持使用代理（Agent）方式提取日志并收集。 | | |
| | | | 系统支持采集的设备厂家包括但不限于：NSFOCUS（绿盟科技）、Venustech（启明星辰）、Topsec（天融信）、DBAPP Security（安恒）、SANGFOR（深信服）、Hillstone（山石网科）、东软、瑞星、金山、网康、360 网神、DPtech（迪普）、艾科网信、Imperva、Juniper（瞻博网络）、F5、Symantec（赛门铁克）、Deep Security（趋势科技）、MacAfee（迈克菲）、Fortinet（飞塔）、Windows、Linux/Unix、Cisco（思科）、HUAWEI（华为）、H3C（华三）、中兴、Apache、nginx 、IIS、WebLogic、VMware、KVM、Xen、OpenStack、Hyper-V、华为 FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等。 | | |
| | | | 系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。 | | |
| | | 日志分析 | 支持对设备日志查询和聚合分析。 | | |
| | | | 系统内置常见安全事件关联分析规则。 | | |
| | | | 支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。 | | |
| | | 日志审计 | 支持 SOX 审计包含 SOX 登录事件、SOX 对象访问、SOX 账号管理、SOX 策略更改。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 PCI 审计包含 PCI 策略更改、PCI 对象访问、PCI 登录事件。 | | |
| | | | 支持 WEB 访问分析包含 WEB 访问概况、WEB 访问客户端分析、WEB 访问地区分析、WEB 异常访问分析。 | | |
| | | | 支持 ISO27001 审计包含 ISO27001 对象访问、ISO27001 策略更改、ISO27001 账号管理、ISO27001 登录事件。 | | |
| | | 数据查询 | 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、地理城市等参数进行过滤查询 | | |
| | | | 支持可指定多个查询条件进行组合查询。 | | |
| | | 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义。 | | |
| | | | 基于角色的权限管理机制，通过角色定义支持多用户访问。 | | |
| | | 平台部署 | 支持多分支级联传输，统一审计和管理，并集中展现。 | | |
| 7 | 数据库审计系统(外网区) | 硬件规格 | 2U 机架式（专用硬件平台），冗余交流电源,2GE 板载管理口,4GE 板载接口+4GE(SFP）板载接口，2×接口板卡插槽。 | 1 | 台 |
| | | | 32GB 内存，1×6TB 硬盘。 | | |
| | | 性能要求 | 纯数据库流量 200Mbps、峰值 QPS（每秒 SQL 请求数)20000 条/秒、在线会话数 6000 个； | | |
| | | | 网络流量 2Gbps。 | | |
| | | 部署模式 | 镜像模式： | | |
| | | | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计（不需要提供 DBA 和任何数据库用户，不需要创建任何数据库用户）； | | |
| | | | 可支持 TAP 和 SPAN 模式。 | | |
| | | | 探针模式： | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持在目标数据库服务器主机上安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户），在审计平台可以实时监控服务器和 agent 的资源状态。 | | |
| | | | 支持镜像模式和探针模式混合部署。 | | |
| | | | 探针可适配常见 Linux 系统、Unix 系统及 Windows 系统，如 CentOS、Redhat、Ubuntu、Debian、HP-Unix、Euleros（欧拉）、openEuler、ky10、Solaris 、SUSE、UOS 等。 | | |
| | | | 支持虚拟化环境部署。 | | |
| | | 防护功能 | 支持旁路阻断 | | |
| | | 协议支持 | 国际数据库：Oracle、MySQL、SQL Server、Db2、Informix、PostgreSQL（EDB）、Sybase ASE、MariaDB、Percona、Greenplum、Caché、Teradata、SAP HANA、Vertica 等。 | | |
| | | | 国产数据库：达梦、南大通用、人大金仓、神通、OceanBase、GaussDB A、GaussDB T、TiDB、TeleDB、CirroData、EsgynDB、Gbase 8t 等。 | | |
| | | | 支持 Hive、HBase、Impala、HDFS、Spark SQL，ElasticSearch、MongoDB、Redis、Clickhouse、Solr、Hive 等大数据组件和非关系型数据库的审计。 | | |
| | | | 支持审计使用回环地址连接数据库的本地访问行为。 | | |
| | | | 支持数据库地址配置域名，通过域名对数据库进行审计。 | | |
| | | | 支持 Oracle CDB/PDB。 | | |
| | | | 支持 Oracle、MySQL、Hive 加密链路。 | | |
| | | | 支持 Oracle 高级安全加密。 | | |
| | | | 支持数据库使用动态端口。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持单向请求包审计。 | | |
| | | | 支持 telnet 协议审计。 | | |
| | | 自动发现 | 支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址等信息，并且自动添加到审计范围，无需用户提供网段、数据库地址等信息； | | |
| | | | 智能模式，根据系统资源使用率动态决定是否进行自动发现，从而不影响正常审计业务。 | | |
| | | | 支持自动添加自动发现的数据库。 | | |
| | | 审计能力 | 支持审计会话相关信息，包括： | | |
| | | | 客户端 IP、客户端端口、客户端 MAC、OS 用户、访问工具、主机名称、 | | |
| | | | 数据库名称、数据库用户、数据库会话标识、数据库 IP、端口、MAC、服务（实例）名、 | | |
| | | | 会话开始、结束时间等。 | | |
| | | | 支持审计 SQL 语句相关信息，包括： | | |
| | | | SQL 标识、操作类型（DDL、DML、DCL 等）、影响行数、响应时间、语句长度、捕获时间、执行结果（DB 应答码、应答错误信息）、受影响对象、SQL 语句、SQL 语句模板、SQL 参数、结果集，等。 | | |
| | | | 支持表、视图、字段等。 | | |
| | | | 支持跨语句、跨多包的访问方式及绑定变量值的审计。 | | |
| | | | 支持对超长 SQL 操作语句审计，对于 Oracle 可支持 8M 长的 SQL 语句。 | | |
| | | | 支持配置返回行数和内容大小控制返回结果集大小，降低系统开销。 | | |
| | | 审计规则 | 内置默认规则，支持场景：高危操作、权限变更、批量数据泄露或篡改、撞库、无 where 更新或删除、SQL 注入、系统表非法操作等。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 可自定义审计规则； | | |
| | | | 审计规则至少支持 20 个条件，规则各条件之间支持与、或、非逻辑关系。 | | |
| | | | 在规则中可支持多种条件： | | |
| | | | 访问来源：源 IP、客户端工具、客户端 MAC、操作系统用户、主机名、数据库实例、数据库用户； | | |
| | | | 操作设置：select、update 等 SQL 操作、schema、表、字段； | | |
| | | | 条件控制：where 条件、关联表个数、SQL 语句关键字； | | |
| | | | 执行结果：影响行数、响应时间、执行结果关键字、结果集敏感行数、应答错误号； | | |
| | | | SQL 命令特征（如 SQL 注释、常量表达式等）、SQL 函数、XSS 跨站； | | |
| | | | 时间范围。 | | |
| | | | 支持规则例外，使得特定行为或语句不命中规则； | | |
| | | | 规则例外中可配置： | | |
| | | | 访问来源：源 IP、客户端工具、客户端 MAC、操作系统用户、主机名、数据库实例、数据库用户； | | |
| | | | 操作设置：select、update 等 SQL 操作、schema、表、字段； | | |
| | | | 条件控制：where 条件、关联表个数、SQL 语句关键字； | | |
| | | | SQL 命令特征（如 SQL 注释、常量表达式等）、SQL 函数、XSS 跨站； | | |
| | | | 时间范围。 | | |
| | | | 可支持对触发器定义、存储过程调用、视图、函数、包、绑定变量配置规则条件。 | | |
| | | | 支持审计白名单，以实现信任特定行为或语句，不会触发风险。 | | |
| | | | 支持对信任的行为或语句不进行审计。 | | |
| | | | 支持对 SQL 语句配置审计规则。 | | |
| | | | 支持频次规则，即在一段时间内对某对象的操作频率。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 规则可关联数据库，也可关联数据库类型； | | |
| | | | 关联数据库类型后，可选择自动关联后续添加的数据库。 | | |
| | | | 支持对工具语句的过滤。 | | |
| | | | 应具备漏洞攻击规则库，漏洞攻击规则应至少包括：漏洞名称、CVE 标识、CNNVD、漏洞类型、影响范围等内容。 | | |
| | | | 内置安全特征库规则，如 SQL 注入、缓冲区溢出、权限提升、数据泄露、拒绝服务、访问操作系统、改密码、Bypass FGAC、修改 FGAC、审计、游标注入、访问敏感组件、创建外部 JOB、恶意代码、非系统用户执行命令等常规漏洞。 | | |
| | | | 支持在全局启用结果集审计，也支持按照规则进行结果集审计，可以针对特定访问行为，审计结果集。 | | |
| | | | 告警数量支持最大告警数量限制，超过告警阈值之后便不告警。 | | |
| | | | 可以针对每条规则配置不同告警次数限制，灵活控制告警频率。 | | |
| | | | 支持 IP 地址、数据库用户、时间、对象、操作系统用户、客户端工具、数据库实例分组等，并且分组对象可以直接在规则中引用。 | | |
| | | | 提供默认对象组，内置主流数据库的系统对象信息，可直接在规则中引用。 | | |
| | | 查询能力 | 支持对审计到的 SQL 语句、SQL 会话、触发的风险进行查看和检索。 | | |
| | | | 对于 SQL 语句，支持多种查询条件： | | |
| | | | 客户端 IP、客户端 MAC、客户端工具、主机名、操作系统用户、数据库用户、 | | |
| | | | 被保护数据库、数据库 IP、数据库端口、服务（实例）名、对象、 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 影响行数、响应时间、语句总耗时、执行结果、 | | |
| | | | SQL 操作、 | | |
| | | | 风险类型、风险级别、 | | |
| | | | 时间等。 | | |
| | | | 支持对结果集的关键字检索。 | | |
| | | | 支持将常用的查询条件保存成固定查询模板，方便后续快速查询。 | | |
| | | | 支持对查询结果以 CSV 文件格式导出到本地。 | | |
| | | | 支持导出任务，可后台执行，查询并导出大量结果，导出量在百万量级。 | | |
| | | | 在对审计到的数据进行查看时，支持对请求方向和结果集中可能存在的敏感数据进行掩码处理，防止敏感数据泄露。 | | |
| | | | 支持客户端 IP 进行别名配置，实现针对不同客户端 IP 自定义别名展现。 | | |
| | | | 支持自定义业务化语言，可将 SQL 语句翻译为业务化的语句进行展现。 | | |
| | | 统计分析 | 支持对会话详情展现，可对会话内执行的全部 SQL 进行展示，跟踪对数据库的访问行为。 | | |
| | | | SQL 可按时间正序、倒序查看，方便事件追溯。 | | |
| | | | 支持对会话进行统计分析，包括： | | |
| | | | －从访问来源对新建会话、在线会话进行统计； | | |
| | | | －分析失败登录的来源和目的、时间和失败原因等。 | | |
| | | | 支持对 SQL 语句的统计分析，包括： | | |
| | | | －根据操作类型、访问来源对 SQL 进行统计； | | |
| | | | －根据语句模板，对 SQL 的执行次数进行统计、对执行历史进行追踪； | | |
| | | | －分析失败语句的来源、错误原因等信息。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持对语句 Top SQL 的分析，可从语句的耗时和执行次数维度进行统计，评估数据库性能。 | | |
| | | | 支持对访问源的分析，可展现不同数据库节点的访问源统计、分析状态。 | | |
| | | | 支持对风险的统计，包括： | | |
| | | | 一从风险等级、规则等维度进行统计和展现； | | |
| | | | 一从语句模板的维度对风险命中情况进行统计。 | | |
| | | | 在统计中支持钻取，可快速定位行为或风险。 | | |
| | | | 对象统计：以操作类型为维度，统计表级别对象被访问次数，可生成行为轨迹图； | | |
| | | | 并可通过对象的访问次数，下钻追溯到该表对象下所有的访问语句详情，以及该表对象访问来源。 | | |
| | | | 统计对比：获取同一数据库不同时间段及不同数据库同一时间段的 SQL 语句量和会话量的对比统计数据以及变化趋势。 | | |
| | | 报表 | 系统提供 40 个以上报表模型，分别基于全库、数据库组和单库维度进行展现。 | | |
| | | | 支持合规性报表，如 SOX 法案、等保、PCI 等专项报表展现。 | | |
| | | | 支持通过专项报表，对风险、性能、访问源、数据库用户等信息做专项报表展现。 | | |
| | | | 支持自定义报表。 | | |
| | | | 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表。 | | |
| | | | 支持按日、周、月等时间周期生成报表。 | | |
| | | | 支持报表数据后台定期预生成，保障报表数据展现速度。 | | |
| | | | 支持将报表按指定的时间推送至指定管理员的邮箱。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 报表支持以 Word、PDF、HTML 等格式保存到本地。 | | |
| | | | 支持对特殊场景的分析，如运维人员共用数据库账号场景分析、对象访问热度分析等。 | | |
| | | 告警与外送 | 支持系统告警； | | |
| | | | 系统告警内容支持网卡异常、分区超限、异常关机、CPU 超限、内存超限、会话超限、包数超限、SQL 数超限、探针异常、证书服务过期等； | | |
| | | | 支持按照风险高、中、低、通知，进行告警通知。 | | |
| | | | 可及时发现系统问题，跟进处理。 | | |
| | | | 支持规则命中后的风险告警； | | |
| | | | 风险告警内容支持触发规则风险内容，并支持根据风险等级进行告警通知。 | | |
| | | | 支持规则告警与规则、数据库关联，实现不同规则、风险级别、数据库以及数据库类型的告警发送给不同收件人，方便进行风险的排查。 | | |
| | | | 告警方式包括：邮件、短信、SYSLOG、SNMP TRAP、企业微信、钉钉群告警、页面弹窗。 | | |
| | | | 支持 SYSLOG 方式外送数据，可外送审计数据、会话信息、语句模板、系统审计日志； | | |
| | | | 支持以文本格式； | | |
| | | | 支持自定义编辑外送模板 | | |
| | | | 支持 KAFKA 方式进行审计数据外送，可外送会话信息和审计数据； | | |
| | | | 支持文本、二进制、JSON 格式； | | |
| | | | 支持自定义编辑外送模板 | | |
| | | 数据管理 | 支持审计日志数据的备份，支持自动备份，备份时可以选择高性能或高压缩比； | | |
| | | | 支持将备份的日志上传到的远程服务器，服务器类型支持 FTP、SFTP、NFS 方式。 | | |
| | | | 支持恢复已备份的审计日志数据，以便查看历史审计记录； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持对存储空间的监控，当空间不足时可进行告警； | | |
| | | | 支持对审计数据的清理，可按在线天数、磁盘空间等阈值进行自动清理。 | | |
| | | 系统管理 | 支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色； | | |
| | | | 可以新建不同用户，分配不同数据库权限和不同的菜单管理权限，不同用户之间数据隔离； | | |
| | | | 可创建多层子账号； | | |
| | | | 系统支持 LDAP/AD 域对接，支持 AD 域用户关联审计系统用户，通过 AD 域账户统一登录审计系统； | | |
| | | | 支持密码策略的配置，可调整密码强度、登录安全相关配置； | | |
| | | | 支持多语言； | | |
| | | | 审计设备 WEB 界面提供自动诊断功能，可以自动收集实例级参数、策略中心参数、操作系统参数、组件参数，方便了解系统运行状态和排查问题； | | |
| | | | 具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录。 | | |
| | | | 支持 SNMP 服务配置，可供第三方监测系统状态 | | |
| | | | 在证书申请时，可以选择显示实际授权数量、显示为无限、不显示授权数。 | | |
| | | | 在用户登录数据库时，支持使用 UKey 认证、谷歌登录认证配合用户名密码进行用户登录双因素认证。 | | |
| | | 功能授权 | 标配 50 个数据库（IP+Port）授权，包含 20 个 RMAgent 探针授权。 | | |
| 8 | 防毒墙系统授权续期 | 授权说明 | 适用于亚信防毒墙系统 1 年期原厂授权，1 套 | 1 | 项 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 9 | 虚拟化环境流量探针软件 | 管理可视化 | 采用 B/S 架构的管理控制中心，具备主机安全可视，主机统一管理，统一威胁检测响应，病毒防御，日志记录与查询等功能 | 1 | 套 |
| | | 多维度威胁展示 | 支持首页展示全网风险、安全事件，包括但不限于安全事件统计、弱密码检测 Top5、漏洞影响面 Top5、未处理的安全事件、实时风险监控、资产概览等模块 | | |
| | | 应用安全防护 | 支持应用安全防护，支持检测的攻击类型：远程命令执行、反序列化、表达式注入、内存马、SQL 注入、文件上传漏洞。应包含应用攻击源、目 IP，支持展示攻击次数、攻击载荷（攻击者 IP、Payload、行为数据、检测点函数、漏洞详情、函数挂载点、堆栈信息等）、攻击请求信息（请求方法、请求参数、请求 URL、请求头 Header、请求内容等）、攻击请求包（应用路径、端口、类型、所属主机、应用运行命令等）。（提供产品界面截图） | | |
| | | 内存后门 | 支持 Java 环境内存马检测，包括：冰蝎、CobaltStrike，MSF 等内存马检测（需提供产品截图证明） | | |
| | | WebRce | 支持 Linux/Win 下的远程命令执行检测告警，告警信息包括：发现时间、失陷主机、远程执行命令、进程树信息、规则说明。 | | |
| | | 暴力破解 | 支持实时检测 SSH、RDP、SMB 暴力破解行为，可自定义暴力破解规则，设置对攻击源 IP 自动封堵等策略 | | |
| | | 异常命令 | 支持对黑客常用的恶意命令，异常编码绕过命令进行检测，对于符合特征的行为进行实时告警，并提供进程执行的详细进程树信息 | | |
| | | 远程命令执行 | 支持对黑客常用的恶意命令，异常编码绕过命令进行检测，对于符合特征的行为实时告警，并提供进程执行的详细进程树信息 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 授权期限 | 3 年 | | |
| 10 | 灾备恢复系统软件 | 总体要求 | 专项针对医院 HIS、CIS、EMR、LIS、RIS、PACS 等应用软件环境实现真实可用的业务应用级灾备应急系统； | 4 | 套 |
| | | | 有效防止主机房故障，以及群集系统、数据库系统等数据中心严重故障导致的业务中止，通过快速（3 分钟以内）启动灾备应急系统，使业务能够继续运行； | | |
| | | | 灾备应急软件基于 Oracle 和 SQL Server 数据库应用事务级高性能实时同步； | | |
| | | | 启用灾备应急系统所产生的新数据能够以增量方式自动完整的导入到主业务系统中； | | |
| | | 数据库支持 | 支持 SQL Server 和 Oracle 数据库系统； | | |
| | | 具体功能要求 | 支持 Windows、Linux、Unix 操作系统； | | |
| | | | 无需主备服务器的数据库文件存储设备一致，提高部署的灵活性； | | |
| | | | 无需在主业务服务器操作系统和数据库系统中安装代理程序文件或插件，可在线实现初始基准全量同步和增量同步，保障主备数据一致性； | | |
| | | | 支持数据库操作语言（DML）复制，在源数据库上对记录进行增、删、改操作可自动、实时复制到目标数据库 | | |
| | | | 支持数据库定义语言（DDL）复制，在源数据库上进行各类数据库对象的操作能自动复制到目标数据库，例如建表、修改字段等操作 | | |
| | | | 集中式管理，可在一个管理界面中，实现多个业务数据库实例扁平化管理 | | |
| | | | 操作简单便捷，可在管理界面执行“一键式”的切换演练操作。 | | |
| | | | 实时监控灾备状态，具有 CPU、内存、I/O 性能指标仪表盘； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 实时监控复制任务，可显示传输率、每秒事务数、提交时延等信息； | | |
| | | | 当网络连接中断时，系统应能记录断点，支持自动断点续传和重做功能； | | |
| | | | 支持数据文件和日志文件状态监控功能； | | |
| | | | 支持业务数据库死锁管理，树状展示进程依赖关系，显示死锁语句，并可结束死锁根源会话，需提供界面截图； | | |
| | | | 支持备端在线可读，实现业务生产与数据分析报表分离，减轻生产端压力；提供界面截图。 | | |
| | | 授权期限 | 3 年 | | |

**3.10 徐汇区妇幼保健所信息系统升级改造**

3.10.1 系统说明

徐汇区妇幼保健所信息系统承载徐汇区妇幼保健所信息化业务的运行。本次项目建设涉及无线网络、安全设备及虚拟云桌面系统三个部分。通过系统集成建设完善信息系统整体业务能力和安全防护能力。

1、无线网络

通过建设 POE 交换机、无线网络控制器及接入点对徐汇区妇幼保健所提供网络接入层升级及无线信号覆盖。

2、安全设备

通过部署信息安全设备，对系统中安全能力薄弱的部分进行改造，实现终端准入、数据脱敏、防火墙云特征库等安全防护能力，提升系统整体安全水平

3、虚拟云桌面

通过对虚拟云桌面服务端的升级扩容及客户端的增设，进一步扩大虚拟云桌面的应用范围，通过虚拟云桌面瘦终端改造原以 PC 机为终端的业务方式。

3.10.2 系统需求

1、部署 2 台带有安全终端准入功能的无线控制器设备，同时负责内网区域与外网区域的无线网络控制及终端准入认证控制。搭配部署 8 台室内 AP 接入点设备对办公区域进行无线信号覆盖。AP 需要由安全终端准入控制系统作为 AC 直接进行管控。

2、部署 POE8 台 24 口 POE 交换机及 4 台 48 口 POE 交换机及配套光模块，作为网络接入层承载包括有线网络部分的系统网络接入层运行。POE 交换机需要与终端准入系统进行对接，并可由终端准入控制系统直接进行准入管控。

3、带有安全准入控制功能的无线控制器需要同时支持传统有线设备的准入控制功能，通过 802.1x 协议与交换机接入层设备对接，同时为有线网络终端提供准入认证能力。

4、需部署 1 台医保专用路由器设备，负责医保专线线路的安全区边界及医保业务接入。

5、针对业务数据库，部署 1 台数据库防水坝系统设备，通过串行组网部署方式对业务数据库和客户端之间的数据交互进行信息安全管控。需要对数据库查询数据进行依据权限控制的动态脱敏，防止重要信息外泄。

6、部署 1 台防火墙设备，对现有防火墙设备进行升级替换，原有安全策略需要梳理合并后进行重新配置。防火墙设备具有云端实时安全能力，安全规则库在线实时获取，确保安全防护能力的时效性及可靠性。

7、 现有 5 台计算资源服务器，作为虚拟云桌面的计算资源池集群。首先需要对现有服务器进行升级改造，通过增加配件提升硬件性能。同时采购云桌面瘦客户端加入虚拟云桌面系统，需要配套 3 套为期 3 年云桌面服务器系统功能授权对虚拟云桌面部分进行扩容以满足使用需求。对该 5 台服务器，每台需要增加 8 条服务器 DDR4 16GB 内存条、2 块 800GB 容量 SSD 固态硬盘和 4 块 6TB 容量机械硬盘。云桌面瘦客户端扩容，共计增加 60 套虚拟云桌面瘦客户端对系统整体承载量进行扩容。投标人需提供增加的终端的相应接入授权

3.10.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 安全准入无线控制器 | 硬件规格 | 千兆以太网口数≥3 个； | 2 | 台 |
| | | | 1 个 RJ-45 Console 管理口； | | |
| | | | 1 个 Manage 口； | | |
| | | | 2 个 USB 口 | | |
| | | 内置存储 | 安全日志本地化存储，内置 SSD 硬盘≥100G。 | | |
| | | 无线协议 | 802.11a/b/g/n/ac/ac wave 2/ax | | |
| | | 转发模式 | 本地转发/集中转发/部分本地部分集中 | | |
| | | 部署模式 | 旁路部署/串行部署/网关部署/远程部署 | | |
| | | AP 管理 | 支持管理节点≥256 个无线接入节点； | | |
| | | | 支持不低于 5 级的 AP 分组管理，方便 AP 设备的管理维护； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | AP 和交换机支持直接生成网络拓扑图，可以直观查看 AP 和交换机拓扑情况，网络拓扑图支持状态信息查看和网络配置下发，方便网络的维护管理； | | |
| | | 准入管理 | 具有有线准入与交换机的对接管理能力，需要支持通过该系统实现统一的配置管理（非简单的 SNMP 网管协议），并且支持可视化的运维配置管理，以及多种方式在网管平台自动上线，包括但不限于二三层发现、DHCP Option43、DNS 域名。需提供相关证明材料 | | |
| | | 认证对接 | 支持关联 RADIUS、微软 AD 域、LDAP、数据库（Oracle、MySQL、MS-SQL）、Portal2.0、AS 等外置认证服务器，实现 802.1x、Portal 等第三方认证； | | |
| | | 安全能力 | 支持应用识别，能识别不低于 6000 种的网络应用，能识别邮件、游戏、P2P 流媒体、WEB 流媒体、金融交易、办公 OA、移动终端应用等主流应用。 | | |
| | | 安全统计 | 支持统计系统安全事件次数并呈现环比状态，包含但不限于呈现钓鱼 AP、非法 AD-Hoc、无线泛洪攻击等安全事件的次数； | | |
| | | | 支持基于时间、逻辑区域、服务类型、访问状态、访问行为、攻击类型等多个维度统计访问终端和被访问终端的详细信息，并生成报表； | | |
| | | | 可以自行对无线网络提供的服务进行检测，包括网络接入、DHCP、网关、DNS、网络地址等阶段的时延和质量检测，并以时光轴的方式进行展示具体时间点的检测情况，可以 24 小时周期性检测并第一时间告警运维人员。 | | |
| 2 | 无线 AP 接入点 | 硬件规格 | 支持 802.11ax 协议，兼容 802.11a/b/g/n/ac 协议，支持 2.4G 和 5G 同时工作，为保障无线网络体验，要求 2.4G 和 5G 射频最高支持 802.11ax 协议； | 8 | 台 |
| | | | 内置天线，千兆以太网口≥1 个，并需提供 1 个 RJ-45 Console 管理口；USB 接口≥1 个，可拓展物联网模块使用，可外接 U 盘； | | |
| | | 性能要求 | 满足三射频设计，2.4G 最大传输速率≥570Mbps，5G 最大传输速率≥2000Mbps，整机最大传输速率≥2.6Gbps； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 功能需求 | 支持 SSID 隐藏； | | |
| | | | 支持英文 SSID、中文 SSID 或中英文混合 SSID； | | |
| | | | 支持 Fat 和 Fit 两种工作模式，根据网络规划的需要，可以灵活地在 Fat 和 Fit 两种工作模式中切换，同时可以根据应用需求，选择工作模式； | | |
| | | | 支持 AP 零配置，支持二三层发现、DHCP Option43、DNS 域名等多种 AC 自动发现机制； | | |
| | | 安全能力 | 无线 AP 可以实现记录内网终端流量访问路径、识别异常终端访问行为、呈现全网异常访问趋势、下发策略阻断风险终端访问动作的全周期东西向流量安全可视化管控 | | |
| | | | 支持将内网终端用于的 ARP 扫描、IP 扫描、端口扫描达到阈值后告警或进入动态黑名单； | | |
| | | | 外部安全感知平台可拉取本系统用户信息，当安全探针和态势感知平台识别异常终端并加入黑名单，本系统会同步安全感知平台黑名单 | | |
| | | | 支持基于应用的无线空口的资源管道化精细管理，保证无线带宽资源合理分配，保障重要应用的优先传输； | | |
| | | | 可以自定义网络质量指标阈值进行编辑，包括网络地址、接入时间、DHCP 请求时间、DNS 解析平均时延、网关平均时延、网络丢包率，并以时光轴的方式进行展示具体时间点的检测情况； | | |
| | | | 支持显示每个 802.11 干扰源的详细情况，包括 BSSID、SSID、厂商、信号强度等信息，以方便对干扰源进行处理；提供相关证明材料 | | |
| | | | 可以看到包括信道总利用率、Wi-Fi 信道利用率、非 Wi-Fi 信道利用率、同频 AP 数量等信息可被识别，并随射频环境变化而变化； | | |
| 3 | POE 交换机-24 端 | 硬件规格 | 1 千兆 POE 电口≥24 个，万兆 SFP+光口≥4 个；Console 口≥1 个； | 8 | 台 |
| | | 性能要求 | 交换容量≥400Gbps；包转发率≥150Mpps； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 口 | 功能要求 | 支持 STP/RSTP/MSTP；支持基于源目 IP 地址、MAC 地址的 ACL 策略；支持端口聚合；支持手工和静态 LACP； | | |
| | | | 支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； | | |
| | | | 支持基于协议（OSPF、UDP、ARP 等），同时支持自定义协议号的 ACL 策略； | | |
| | | | 支持以下上线方式：支持二层广播自动发现网管中心平台；支持配置静态 IP 地址三层发现网管中心平台；支持 DHCP Option43 方式发现网管中心平台；支持 DNS 域名发现网管中心平台； | | |
| | | | 为保证网络安全性，要求交换机支持基于终端类型自动识别结果，禁止非法终端（例如私接路由器）接入； | | |
| | | | 为提高系统兼容性对接，需支持联动第三方安全设备或平台，通过联动实现从系统级接入层交换机对风险终端 MAC 地址进行封堵； | | |
| | | | 支持防网关 ARP 欺骗，支持端口保护、隔离，支持防止 DOS、ARP 攻击功能，支持 CPU 保护功能； | | |
| | | | 支持 DHCP Snooping，支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文； | | |
| 4 | POE 交换机-48 端口 | 硬件规格 | 1 千兆 POE 电口≥48 个，万兆 SFP+光口≥2 个，千兆 SFP 光口≥2 个；Console 口≥1 个，Manage 口 1 个； | 4 | 台 |
| | | 性能要求 | 交换容量≥400Gbps；包转发率≥190Mpps； | | |
| | | 功能要求 | 支持 STP/RSTP/MSTP；支持基于源目 IP 地址、MAC 地址的 ACL 策略；支持端口聚合；支持手工和静态 LACP； | | |
| | | | 支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； | | |
| | | | 支持基于协议（OSPF、UDP、ARP 等），同时支持自定义协议号的 ACL 策略； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持以下上线方式：支持二层广播自动发现网管中心平台；支持配置静态 IP 地址三层发现网管中心平台；支持 DHCP Option43 方式发现网管中心平台；支持 DNS 域名发现网管中心平台； | | |
| | | | 为保证网络安全性，要求交换机支持基于终端类型自动识别结果，禁止非法终端（例如私接路由器）接入； | | |
| | | | 为保证网络流量和设备运行状态可实时监控并追溯，支持通过网管平台查看交换机处于工作端口最近 5 分钟、1 小时、最近 1 天、最近 1 周发送与接收的流量趋势，要求支持查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作、接入设备类型、网络环路情况、链路聚合情况等； | | |
| | | | 支持防网关 ARP 欺骗，支持端口保护、隔离，支持防止 DOS、ARP 攻击功能，支持 CPU 保护功能； | | |
| | | | 支持 DHCP Snooping，支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文； | | |
| 5 | 万兆多模光模块 | 硬件规格 | 光模块-SFP+-10G-(850nm,300m,LC) | 48 | 个 |
| 6 | 路由器（医保网络） | 硬件规格 | 支持 16 个千兆电口,6 个万兆光口;双电源，支持 4 个 SIC 插槽，支持 2 个 HMIM 插槽，提供官网截图证明。 | 1 | 台 |
| | | 性能要求 | 交换容量≥260Gbps，包转发率≥60Mpps，，提供官网截图证明。 | | |
| | | SDN | 支持 Telemetry,Netconf 等管理控制协议，支持 Segment Routing、VxLAN、EVPN 等转发业务，可定义多种转发模型，满足不同业务组网需求, | | |
| | | | 支持 URL、U 盘、DHCP 零配置部署，满足批量、低成本、快速开局要求，支持 DPI 应用识别能力，对网络流量进行精准识别，实现网络流量可视化、自定义和灵活调度 | | |
| | | 安全 | 支持基于报文五元组过滤，ASPF 状态过滤、MAC 地址过滤、URL 过滤、基于域防火墙、IPS 等 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 802.1X/Portal 认证，EAD 安全检查认证、终端 MAC 地址认证等 | | |
| | | | 支持防 SYN 泛洪、ACK 泛洪、RST 泛洪、UDP 泛洪等攻击 | | |
| | | | 支持基于角色权限管理，能够基于角色进行资源分配、用户与角色的对应，灵活安全控制权限 | | |
| | | 负载分担 | 支持等价链路负载分担（ECMP）和非等价链路负载分担（UCMP），UCMP 支持根据链路带宽比例进行负载分担； | | |
| | | 智能网络管理 | 支持 Telnet/SSH、SNMP、TR069、Netconf 等多种网络管理方式 | | |
| | | | 支持 EAA（内嵌自动化架构）功能，具备 TCL 和 Phython 脚本自编程能力，可对系统软硬件部件的内部事件、状态进行监控，出现特定事件时自动执行预先定义的脚本 | | |
| | | 可靠性 | 支持链路毫秒级快速故障侦测技术（BFD），可实现同静态路由、RIP/OSPF/BGP/ISIS 动态路由、VRRP 和接口备份的联动 | | |
| | | | 支持网络业务质量智能检测技术，可实现与静态路由、VRRP 和接口备份等的联动。 | | |
| | | | 支持多设备的冗余备份和负载分担 | | |
| | | | 支持随业务的逐包性能检测技术，以实现对用户业务流进行直接的丢包、时延、流速等监测。 | | |
| 7 | 数据库防水坝系统 | 硬件规格 | 规格：1U 机架式设备；电源类型：单电源；接口≥4 个千兆电口；内存≥16G；存储≥2T；在线 SQL 存储数量≥40 亿条 | 1 | 台 |
| | | 数据库支持 | 支持 ORACLE、SQL SERVER、DB2、MySQL、PostgreSQL、ODPS、informix、达梦、impala、Mongodb、ocean base 等主流数据库、国产化数据库、大数据平台、云数据库，支持国密算法加密的 Qian base 数据库管控。 | | |
| | | 部署模式 | 支持反向代理、透明代理、透明代理 NAT、路由网关部署。 | | |
| | | 敏感数据发现能力 | 具备敏感数据探测能力，自动发现 SCHEMA（包括未知 SCHEMA）、表、列中的敏感资产，系统内置的敏感数据类型至少包括： | | |
| | | | 个人敏感信息：包括中文姓名、身份证、银行卡、医师资格证书、医师执业证书、护照、军官证、中国护照、港澳通行证、永久居住证、大陆居民往来台湾通行证、韩文姓名、英文姓名、姓名拼音等个人信息； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 机构敏感信息：组织机构代码、组织机构名称、医疗机构登记号、营业执照、社会统一信用代码、税务登记证、开户许可证、证券名称、证券代码、基金名称、基金代码、英文公司名等与企业机构相关的信息； | | |
| | | | 其他基础信息：电话、电子邮箱、地址、邮政编码、IP 地址、日期、货币金额、Json 串、车牌号码等。（提供相关证明材料） | | |
| | | 安全运维 | 通过账号托管功能，运维人员使用分配运维账号，运维用户与数据库用户及密码进行映射绑定，无需告知密码。 | | |
| | | 身份准入 | 支持身份的多因素认证，至少应支持应用程序名、IP 地址、主机名、操作系统账户、数据库用户、数字证书、身份敏感标签、日期、时间、时间域、身份类别、有效时间、应用用户名、终端 IP 等因素的任意组合，系统根据多维身份管理策略，自动判别登录主体的合法性，如不符合设定的身份管理策略，登录失败。 | | |
| | | 访问控制 | 支持数据库授权管理控制，包括数据库角色权限管理、数据库对象权限管控、数据库系统权限管理，主要如下： | | |
| | | | 1）支持针对数据库账号的角色权限进行控制，包括数据库系统管控授权（GRANT SYSDBA）、数据库管理员授权（GRANT DBA）、导入数据库授权（GRANT IMP_FULL_DATABASE）、导出数据库授权（GRANT EXP_FULL_DATABASE）等； | | |
| | | | 2）支持针对数据库账号的数据库对象权限进行控制，包括访问敏感对象授权（GRANT SENSITIVE OBJECT）、访问业务用户对象授权（GRANT SCHEMA OBJECT）、访问系统对象授权（GRANT SYS OBJECT）等； | | |
| | | | 3）支持针对数据库账号进行数据库系统权限授权，包括删除任意对象授权（GRANT DROP ANY）、创建任意对象授权（GRANT CREATE ANY）、更新任意数据授权（GRANT UPDATE ANY）、查询任意数据授权（GRANT SELECT ANY）、插入任意数据授权（GRANT INSERT ANY）、删除任意数据授权（GRANT DELETE ANY）等。 | | |
| | | | 支持账户访问频次控制，避免一定时间内的高频次访问，避免数据流失。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持修改、删除等操作的行数控制，避免数据大量泄漏。 | | |
| | | | 支持僵尸账号检测，对僵尸账号进行锁定，防止僵尸账号造成数据泄露。 | | |
| | | 数据脱敏 | 支持基于列的业务类型，设置脱敏策略，实现相同的业务类型同时设置脱敏策略(提供相关证明材料) | | |
| | | 删除保护 | 至少支持 oracle、SQL server、MySQL、DB2 数据库的误删除恢复，当使用 DROP 命令误删除敏感数据时，系统应及时记录操作的时间、数据库名称、操作类型、操作的对象类型、SCHEMA 名称、对象名称、当前状态、使用的 SQL 语句等信息，并提供一键恢复的功能，辅助完成数据的快速恢复，以支持系统恢复正常。（提供相关证明材料） | | |
| | | 访问审批 | 采用基于 WEB 界面的工单管理模式，而非授权码方式，通过工作流的方式对敏感表格和敏感 SQL 访问授权，形成逐级审批机制，只有当访问申请被工作流中的所有审核者审批通过时，才可在合理权限内访问数据库中的敏感资产，无需访问者进行二次输入，避免授权码泄漏带来的非法访问。 | | |
| | | | 支持统计数据库请求数、会话数、流量信息 | | |
| | | | 支持日报、月报、周报等生成，导出格式支持 PDF/word。 | | |
| | | | 支持与 AD、LDAP 系统联动登录系统。 | | |
| 8 | 防火墙（升级替换） | 硬件规格及性能要求 | 规格：1U，内存大小：≥4G，硬盘容量：≥128G SSD，电源：单电源，接口：千兆电口≥8，千兆光口 SFP≥2。 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥4G，应用层吞吐量：≥2G，并发连接数：≥200 万，HTTP 新建连接数：≥6 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | 应用识别 | 支持应用管控功能，应用特征识别库数量大于 8000 种。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 加密流量安全防护 | 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 | | |
| | | 云端安全能力 | 能实时从云端获取漏洞特征库、安全威胁库、病毒库及恶意 IP 名单等信息。提供相关证明材料。 | | |
| | | 功能授权 | 包含不少于 3 年的入侵检测、防病毒模块及云端安全能力授权。 | | |
| 9 | 配件—服务器内存 DDR4 | 兼容要求 | 适配 HPE 服务器 | 40 | 条 |
| | | 硬件规格 | DDR4 16GB 内存条 | | |
| 10 | 配件—服务器固态硬盘 | 兼容要求 | 适配 HPE 服务器 | 10 | 块 |
| | | 硬件规格 | 800GB SSD | | |
| 11 | 配件—服务器机械硬盘 | 兼容要求 | 适配 HPE 服务器 | 20 | 块 |
| | | 硬件规格 | ≥6TB SATA HDD | | |
| 12 | 桌面云瘦终端 | 兼容要求 | 要求所投产品与单位使用深信服桌面云 A-desk Server 软件保证兼容。提供证明材料。 | 60 | 套 |
| | | 硬件规格 | ARM 架构，CPU≥1.4Ghz、内存≥1G、存储≥4G、USB≥6 个、1 个 VGA、至少 1 个百兆电口。 | | |
| | | 管理方式 | 为了方便管理，管理方式为虚拟机和瘦终端统一管理，降低管理难度。 | | |
| | | | 在瘦终端的管理方面，需支持分组管理、批量移动、删除、关闭瘦终端，支持配置定时开关机计划及加电自启动功能，支持自定义开机画面、支持联动关机功能、配置自动登录和保存密码。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 为了简化管理，要求瘦终端支持远程唤醒，管理员可以使用桌面云控制器或者第三方教学软件，例如极域等，远程开机瘦终端。 | | |
| | | 接入安全 | 考虑到接入安全，需支持修改云终端配置和登录信息时需要密码，可限制未接入过环境的瘦终端的接入或者接入桌面环境需要输入密码。 | | |
| | | 功能授权 | 每套终端附带所需授权。 | | |
| 13 | 虚拟云桌面服务器系统扩容授权 | 授权说明 | 适用于深信服虚拟云桌面服务器系统（不限具体硬件型号）的系统软件授权 3 年期，3 套 | 1 | 项 |

**3.11 徐汇区徐家汇街道社区卫生服务中心信息屏系统建设**

3.11.1 系统说明

徐汇区徐家汇街道社区卫生服务中心信息屏系统通过部署显示设备，对院内信息系统的相关信息进行发布，为患者提供相关就诊信息，对办公人员举行会议提供便利。

3.11.2 系统需求

1、部署 55 英寸液晶平板电视 1 台，安装在康复室用于滚动播放预置院内医护人员信息以及就诊规范等。采用背挂支架嵌入式安装到墙面预留的槽位中，安装后与墙面需基本保持在同一垂直面上。

2、部署 86 英寸液晶平板电视 1 台，安装在 1F 大厅用于滚动播放就诊信息等。采用背挂支架嵌入式安装到墙面预留的槽位中，安装后与墙面需基本保持在同一垂直面上。

3、1 套 LED 显示屏，安装在 6F 会议室。要求采用 P1.86 拼接 LED 面板，要求画面无抖动、水波纹、频闪等不良现象。显示屏可显示文字、图形、图案、动画等并具有同时播放左右不同比例的画面及文字的功能。画面元素支持平移、滚动、旋转、划变、拉幕、单/多行平移、单/多行上/下移、左/右拉、上/下拉、翻页、移动、旋转、缩小、放大、闪烁、开窗等排列方式，配有网络接口，可与计算机联网，共享网络信息资源。同时具有音频接口，可与相关音响相结合，达到声像同步功能。显示屏整体必须满足防水、防尘、防腐蚀、防燃烧、电磁干扰的要求。电气防护方面必须满足过流、短路、断路、过压、欠压等保护措施。

4、LED 显示屏主要技术参数如下表：

| 序号 | 项目 | 规格 |
|---|---|---|
| 1 | 安装位置 | 6 楼会议室 |
| 2 | 像素点组成 | 1 红 1 绿 1 蓝 |
| 3 | 像素点间距 | ≤1.86mm |
| 4 | 屏幕分辨率 | ≥2752*1204 |
| 5 | 模组分辨率 | 172*86 |
| 6 | 模组尺寸 | 320*160 |
| 7 | 模组宽高比 | 2:1 |
| 8 | 屏幕净显面积 | 5.12m*2.24m |
| 9 | 像素密度 | 288906 点/㎡ |
| 10 | 维护方式 | 前维护 |
| 11 | 显示屏亮度 | 600nits |
| 12 | 色温 | 3200—9300K |
| 13 | 可视角度 | 水平 160° 垂直 160° |
| 14 | 对比度 | 3000:1 |
| 15 | 亮度均匀性 | ≥98% |
| 16 | 亮度控制 | 手动 |
| 17 | 色度均匀性 | ±0.003 |
| 18 | 峰值功耗 | 460W/㎡ |
| 19 | 平均功耗 | 280W/㎡ |
| 20 | 供电要求 | AC220-240V |
| 21 | 驱动方式 | 恒流驱动 |
| 22 | 换帧频率 | 60Hz |
| 23 | 刷新率 | ≥4200Hz |
| 24 | 工作温度 | -10℃~40℃ |
| 25 | 工作湿度 | 10%~80% |
| 26 | 开关电源 | 满足屏体要求 |
| 27 | 防雷接地 | 符合相应行业标准 |
| 28 | 内置降温设备 | / |

3.11.3 工作量清单及技术参数要求

| 序号 | 设备名称 | 参数 | 数量 | 单位 |
|---|---|---|---|---|
| 1 | 康复室 55 英寸液晶平板电视 | 1、分辨率≥3840*2160<br>2、刷新率≥60Hz<br>3、尺寸≥55 英寸。含背挂支架，背挂安装后厚度≤260mm<br>4、带智能操作系统，支持 Wi-fi 功能及以太网功能 | 1 | 台 |

| | | | | |
|---|---|---|---|---|
| 2 | 1F 大厅 86 英寸液晶平板电视 | 1、分辨率≥3840*2160<br>2、刷新率≥120Hz<br>3、尺寸≥86 英寸。含背挂支架，背挂安装后厚度≤442mm<br>4、带智能操作系统，支持 Wi-fi 功能及以太网功能 | 1 | 台 |
| 3 | 室内 P1.86 显示屏 | 详见 LED 显示屏主要技术要求 | 1 | 套 |
| 4 | 接收卡 | 1、集成 12 个标准 HUB75 接口，免接 HUB 板。<br>2、采用千兆网口，可以连接 PC 端。<br>3、支持逐点亮色度校正。<br>4、支持接收卡预存画面设置。<br>5、支持温度、电压、网线通讯和视频源信号状态检测。<br>6、支持 5Pin 液晶模块 | 1 | 块 |
| 5 | 二合一发送卡 | 支持画面全屏缩放、点对点显示、自定义缩放三种缩放模式；支持窗口位置、大小调整及窗口截取功能，至少支持 6 个预设场景 | 4 | 台 |
| 6 | 电源 | 1、额定输入 220VAC 50/60Hz<br>2、输出电压：5V<br>3、输出电流：30A<br>4、输出功率：200W | 40 | 台 |
| 7 | 配电箱 | 1、配电箱：容量：40kw，与显示屏体配套使用<br>2、配电系统有短路、断路、过流、过压、欠压以及漏电保护措施，具备烟雾报警及温升报警功能<br>3、配电柜内至少包含空气开关、漏电保护、熔断器、交流接触器、电流互感器、电压互感器<br>4、采用国标铜线，三相五线制供电<br>5、输入具有自动/手动切换功能，带 PLC 控制 | 1 | 套 |

| | | | | |
|---|---|---|---|---|
| 8 | 框架及基础施工 | 钢结构及基础施工满足结构规范等国家安全要求。焊接一个长度约为 5.22 米，高度约为 2.34 米，下沿高度距离舞台约 0.3 米，内嵌于 6F 会议室前侧墙体中的长方体钢结构框架，壁挂安装。正面长度约为 5.12 米，高度约为 2.24 米区域安装 LED 屏体，且最终屏体正面于墙面需基本保持在同一垂直面上，其他部位使用不锈钢外框包边。 | 1 | 项 |
| 9 | 拼接处理器 | 1、输入:4 路 HDMI 采集，3 路最高 1920x1200@60hz，1 路 HDMI2.0,4K@60。支持 EDID<br>2、输出：9 路 HDMI 输出，单口 1920x1200@60hz(单口可定制分辨率，用于 LED，完全同步，支持 230 万以内的点数，单台支持 2070W 以内点数)<br>3、4K 采集口可以采集特大图像，如 7680x2160@30hz 或 5760x3240@30hz 的分辨率<br>4、进 9 出处理器其中 1 路输入为 4k60hzHDMI 输入，3 路 1080@60 输入<br>9 路 1920*1200@60 输出 | 1 | 台 |
| 10 | 六类非屏蔽双绞线 | 1、六类非屏蔽，线芯规格：24AWG 的实芯裸铜线；<br>2、十字支撑架结构；<br>3、带宽：≥250MHz；<br>4、输入阻抗：100±6Ω@1-250MHz；<br>5、符合 ROHS。 | 240 | 米 |
| 11 | 电线电缆 | 电线电缆 RVV3*2.5 国标 | 120 | 米 |
| 12 | 镀锌电线管 | N25 规格 | 110 | 米 |

**3.12 徐汇区斜土街道社区卫生服务中心 HIS 业务服务器集群系统升级改造**

3.12.1 系统说明

徐汇区斜土街道社区卫生服务中心 HIS 业务服务器集群系统负责承载其 HIS 业务的运行，为其医疗信息系统提供稳定的 HIS 业务服务。现有 HIS 系统数据库是 2 台服务器双机热备，采用 NEC EXPRESSCLUSTER 集群软件提供双机高可用。目前现有服务器性能已不满足业务需求，对其实施升级改造。

3.12.2 系统需求

通过部署 2 台机架式服务器组成新的集群，并配合采购单位对现有 HIS 服务器中的应用软件及业务的迁移工作，由新服务器接替承载 HIS 业务及数据库运行，并将原有服务器配置为冷备集群，完成对 HIS 业务服务器集群系统的改造集成。

3.12.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 机架式服务器 | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 2 | 台 |
| | | CPU 规格 | ≥2 颗 Intel Xeon SP 5318H(2.5GHz/18 核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥384GB DDR4 3200 内存模块 | | |
| | | 内存可扩展数量 | 本地提供≥48 个内存槽位，最大支持 18TB 物理内存，12TB 有效内存，支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘实配规格 | ≥2 块 960GB SSD 硬盘，热插拔；支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 本地提供≥8 个 2.5 寸硬盘槽位，支持≥48 块 2.5 寸热插拔硬盘。 | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆网卡，≥1 张 2 端口万兆网卡（含模块），≥1 张 2 端口 16GB FC HBA 卡（含模块） | | |
| | | 冗余电源 | ≥2 个 1600W 铂金版热插拔冗余电源；支持 1+1/N+N 冗余；支持 240VDC，380VDC，48VDC | | |
| | | 冗余风扇 | 热插拔冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块，提供防火墙、IPS、防病毒和 QoS 等安全防护功能。 | | |

**3.13 徐汇区田林街道社区卫生服务中心信息系统升级改造**

3.13.1 系统说明

徐汇区田林街道社区卫生服务中心信息系统承载其信息化业务的运行。本次项目建设涉及业务服务器、安全设备和虚拟云桌面三个部分。通过对系统升级改造，完善系统整体安全防护能力和业务承载能力。

1、 业务服务器

通过更换新的服务器设备替换掉原有性能不足的旧设备。使硬件性能满足当前业务要求。

2、 安全设备

通过增加及替换信息安全设备，对现有系统的信息安全能力进行改造。实现终端准入、边界防护态势感知等安全能力，进一步满足等保要求。同时对现有设备进行扩容升级，保障其安全能力有效利用。

3、 虚拟云桌面

通过建设虚拟云桌面系统服务器及云桌面瘦终端改造原以 PC 机为终端的业务方式。

3.13.2 系统需求

1、 采用 2 台机架式服务器组成集群化，对原有业务服务器进行替换。

2、 为满足三级等保要求，部署 1 套安全准入控制系统，设置在内网区域，同时对内网有线和无线内网 VLAN 进行终端准入控制管理，实现终端准入控制能力。

3、 部署 1 台入侵防御系统设备，对现有老旧的入侵防御设备进行更换。增强现有系统对来自外部网络的入侵行为进行甄别阻断及日志记录能力。

4、 部署 1 台内外网边界防火墙，在现有内网区域及外部接入区之间建立网络安全边界，管控区域间流量。为满足内网安全区及外网安全区之间的跨区通信需求。

5、 部署 1 台网闸设备，内外网端分别接入各自安全区，实现在内外网安全区相互隔离的环境下，对必要的跨区业务通信进行安全传输保障。

6、 部署 1 套安全态势感知系统设备，通过日志及 SNMP 网管协议等对上述及现有安全设备进行信息对接，实现对网络内流量情况的监控，使系统具有对安全攻击检测能力、网

络安全分析能力、用户行为分析能力等安全防范能力。

7、 现有 1 台启明星辰品牌的日志审计系统设备，在安全设备增加后，其日志记录空间难以满足三级等保要求中关于审计日志留存期限的要求。需同时对日志审计系统的存储空间进行扩容。启明星辰日志审计系统空间升级需保障设备授权及系统软件等不受影响。

8、 部署 2 台用于建设虚拟云桌面系统的服务器一体机设备，采用集群部署组成计算资源集群，并配套虚拟云桌面瘦客户端 50 套建设虚拟云桌面部分。

3.13.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 机架式服务器 | 硬件规格 | 机架式，≤2U，标配原厂导轨 | 2 | 台 |
| | | CPU 规格 | ≥2 颗 Intel 4314(2.4GHz/16 核/24MB/135W)处理器,可支持最高 270W 处理器 | | |
| | | 内存规格 | ≥256GB 3200MHz DDR4 内存模块 | | |
| | | 内存可扩展数量 | 最大支持 32 根 DDR4 内存，最高速率 3200MT/s，支持 RDIMM 或 LRDIMM; | | |
| | | | 支持 16 根持久内存 PMem 200 系列（Barlow Pass）最大可支持内存容量高达 12TB | | |
| | | 实配硬盘 | ≥5 块 1.2TB 10K SAS HDD 硬盘。 | | |
| | | 硬盘槽位 | 本地提供≥8 个 2.5 寸硬盘槽位,支持 SAS/SATA HDD/SSD 硬盘，支持≥37 块 2.5 寸硬盘，热插拔 | | |
| | | 阵列控制器 | ≥1 个标准 PCIe 槽位阵列卡，支持 RAID0/1/10 | | |
| | | PCI I/O 插槽 | 支持≥14 个 PCIE4.0 速率插槽。 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100/200 GE 网卡，IB 卡；本次配置≥1 张 4 口千兆网卡 | | |
| | | GPU | 支持≥4 个双宽 GPU 卡或 14 个单宽 GPU 卡。 | | |
| | | 接口 | 标配 1 个前置 VGA，1 个后置 VGA 和 1 个串口，6 个 USB 3.0（2 前置，2 后置，2 内置），1 个前置专用管理接口 | | |
| | | 冗余电源 | ≥2 个 800W 白金版热插拔冗余电源，支持 96%能效比的钛金级电源选件 | | |
| | | | 满配热插拔冗余风扇 | | |
| | | 工作温度 | 支持最高 5-45° C 标准工作温度 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| 2 | 安全态势感知平台系统 | 硬件规格 | 规格：≤2U，内存大小：≥16G，硬盘容量：≥128GB SSD+4TB SATA，电源：单电源，接口：千兆电口≥6，万兆光口 SFP+≥2 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥1Gbps | | |
| | | 大屏可视 | 支持大屏轮播及自定义大屏顺序设置和大屏名称。自定义统计周期资产组划分、选择播放大屏及轮播时间间隔。 | | |
| | | 数据中心可视 | 可视区域基于数据中心、总部、租户等按照风险等级（优秀、良、中、差）来展示数据中心的情况。支持对数据中心正常反问的趋势和攻击者监视和分析威胁的说明。 | | |
| | | 弱口令检测 | 弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web 空密码、账号白名单、密码白名单、txt 文件格式导入。 | | |
| | | 资产全生命周期管理 | 支持自定义资产多级分支管理，最多可至 15 级分支。支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。 | | |
| | | 资产发现 | 支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、MAC 地址、主机名等。 | | |
| | | 文件威胁分析 | 文件威胁分析支持平台内置的静态文件检测引擎，利用多种机器学习算法组合进行综合研判。支持采用 AI 技术针对无文件落地的恶意脚本进行检测。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 异常流量分析 | 支持按照对外业务流量可视、横向流量可视、外联流量可视等开放的业务流量情况，展示服务器流量排行、最活跃源主机的内网服务器的流量情况，支持全球地图展示整体外联流量情况。 | | |
| | | DNS 日志接入 | 支持 DNS 服务器日志导入，可以接入 DNS 服务器的日志,安全分析引擎将结合 DNS 服务器的日志，定位出 DNS 服务器代理风险外连场景下真实源 IP，从而有效地进行风险处置闭环。 | | |
| 3 | 安全准入控制系统 | 硬件规格 | 最大可支持准入终端数不少于 2000，电源：冗余双电源，接口：千兆电口≥4，具备不少于 2 个可拓展万兆的拓展槽。 | 1 | 台 |
| | | 系统架构 | 管理平台和准入网关支持一体化部署，也可采用分离部署架构； | | |
| | | | 设备无需其他计算资源独立运行； | | |
| | | | 管理平台支持对多个准入硬件网关设备进行统一集中管控； | | |
| | | 部署模式 | 支持 802.1x、WebAuth、Portal、端口镜像、策略路由、客户端等多种准入控制方式混合使用，一个系统可同时使用多种准入方式适应复杂网络环境；（提供系统截图证明） | | |
| | | | 准入未放行前支持 web 重定向、邮件重定向方式引导； | | |
| | | | 支持客户端准入控制阻断和提醒模式，可提醒并帮助用户自助安装客户端；（提供系统截图证明） | | |
| | | | 支持分级部署，设置统一管理平台，对不同的地区、部门使用的服务端进行分级部署； | | |
| | | | 支持分布式部署，可将系统自身功能组件（radius、web、数据库等组件、审计文档服务器等）独立模块化分布式部署。 | | |
| | | 功能拓展 | 支持客户端准入控制，可拓展一定桌面管理、终端检测响应等功能模块； | | |
| | | | 支持扩展对主流国产化 PC 系统的功能支持； | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 策略管理 | 支持指定设备、设备组、用户、用户组、部门、IP、MAC 下发策略，支持策略离线生效，支持例外策略下发管理； | | |
| | | | 支持策略场景定义客户端在线、客户端离线等状态，等采取不同策略。 | | |
| | | 客户端模式防护 | 支持客户端自我防护机制，客户端文件、进程、注册表、服务等都无法停止、修改、删除；客户端正常运行情况下安装目录隐藏； | | |
| | | | 支持客户端安全模式下运行，客户端策略依然生效； | | |
| | | | 支持客户端功能在线调整，在功能调整、问题验证等场景下支持客户端文件（配置文件、DLL 等）实时替换，无需覆盖安装、重启终端； | | |
| | | | 支持 Windows、macOS、Linux 客户端； | | |
| | | 802.1x 准入 | 支持 802.1x 有线无线网络环境下主流网络设备的动态 VLAN 切换（Guest VLAN、修复 VLAN、工作 VLAN）； | | |
| | | | 支持 802.1x 有线无线网络环境下主流网络设备的 ACL 动态下发； | | |
| | | | 支持 802.1x 技术下，终端通过 HUB 接入场景，每个终端分别进行认证； | | |
| | | 资产发现识别 | 支持自动发现识别接入设备的类型，包括：PC 设备、网络设备、服务器、移动设备、IoT 设备等； | | |
| | | | 支持自定义添加设备类型识别规则条件，以操作系统、开放端口、设备名、MAC 地址前缀、MAC 地址厂商、IP 地址范围等条件设置权重，自动将设备匹配归纳到新添加的设备类型列表中，自动分配网络访问权限。 | | |
| | | 身份认证对接 | 支持多种身份认证源：内置账户，AD/LDAP 用户，邮件服务器用户、证书认证，第三方 RADIUS 服务器认证，第三方扩展认证； | | |
| | | 策略准入功能 | 支持用户与计算机 MAC 地址、接入交换机端口号、接入控制点设备、客户端生成的主机码和随机码绑定；可对终端硬件生成唯一 ID、认证用户等进行灵活绑定；（提供系统截图证明） | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持 1 对 1，1 对多绑定，并支持设置对某用户在一定数量范围内的终端自动放行。 | | |
| | | | 支持应急逃生，系统检测到运行中出现的异常和故障需要能够自动应急；一定时间内连续出现多台终端准入失败自动临时放行且阈值可自定义（分钟级别），确保企业网络的可用性； | | |
| | | 功能授权 | 提供不少于 300 个终端准入控制授权， | | |
| 4 | 入侵防御系统 | 硬件规格 | 规格：1U；电源：单电源；接口：千兆电口≥6；万兆光口 SFP+≥2 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥20Gbps；并发连接数：≥2200000;新建连接数：≥150000 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | 应用识别 | 支持应用管控功能，应用特征识别库数量大于 8000 种。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备 URL 分类库。 | | |
| | | 加密流量安全防护 | 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| 5 | 防火墙（内外网边界） | 硬件规格 | 规格：2U，内存大小：≥16G，硬盘容量：≥128G SSD+480G SSD，电源：冗余电源，接口：千兆电口≥16，万兆光口 SFP+≥6。 | 1 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 性能要求 | 网络层吞吐量：≥40G，应用层吞吐量：≥25G，防病毒吞吐量：≥4G，IPS 吞吐量：≥3.5G，并发连接数：≥420 万，HTTP 新建连接数：≥19 万 | | |
| | | 工作模式 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。支持，默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测、QOS、虚拟化防火墙、防 DDOS 攻击功能 | | |
| | | 路由特性 | 支持静态路由、策略路由、多播路由等常见路由类型。 | | |
| | | | 支持 BGP、RIP、OSPF 等常见动态路由协议。 | | |
| | | 应用识别 | 支持应用管控功能，应用特征识别库数量大于 8000 种。 | | |
| | | NAT 功能 | 支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 | | |
| | | IPv6 功能 | 支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制 | | |
| | | 防病毒 | 支持对压缩病毒文件进行检测和拦截，压缩层数支持 10 层及以上。 | | |
| | | URL 分类过滤 | 支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。 | | |
| | | 加密流量安全防护 | 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 | | |
| | | 入侵防御 | 产品内置不低于 7000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 | | |
| | | 功能授权 | 包含不少于 3 年的入侵检测及防病毒模块授权。 | | |
| 6 | 网闸设备 | 硬件规格 | 2U 设备，“双主机+隔离卡”架构，单主机硬件信息：千兆电口≥6，内存≥4GB，硬盘≥64G SSD，冗余电源。 | 1 | 台 |
| | | 性能要求 | 吞吐量（网络层流量）：≥300Mbps，最大并发连接数：≥5 万。吞吐量≥300Mbps。 | | |
| | | 系统架构 | 采用 2+1 系统架构即内网单元+外网单元+FPGA 专用隔离硬件。不能采用网线等形式直通。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 采用基于 Linux 内核的多核多线程专用安全操作系统，加固内核。 | | |
| | | 管理接口 | 外网端不允许配置任何形式的管理接口，所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置。 | | |
| | | 视频交换 | 支持平台级联及平台点播，支持 GB 28181 视频通信国家标准及相关厂商协议规范 | | |
| | | 数据库同步 | 系统支持数据库同步应用，支持 ORACLE、SQLSERVER、MYSQL、SYBASE、DB2、POSTGRESQL 等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步 | | |
| | | 工业控制应用 | 支持 DCS/SCADA 生产网络与办公网络之间的 OPC 应用数据的传输。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输（提供功能截图）； | | |
| | | | 支持 MODBUS 协议传输代理模块，可按照用户需求控制具体功能代码，比如只允许读取，不能控制等 | | |
| | | 时间模式 | 支持根据时间自动切换的安全策略。支持时间段以 24 小时制；支持以星期为周期；支持指定时间点一次性运行； | | |
| | | 诊断工具 | 系统提供 ping，traceroute，TCP 端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题 | | |
| | | 日志审计 | 系统可存储和审计包含：系统日志；管理日志；网络活动日志；入侵报警及处理日志；访问控制日志； | | |
| | | 双机热备 | 支持双机热备，保障业务可用性。 | | |
| | | 功能授权 | 提供文件交换、数据库访问和同步、视频交换、组播代理、访问交换等功能模块。 | | |
| 7 | 配件一日志审计硬盘升级 | 兼容要求 | 适配启明星辰日志审计 | 1 | 项 |
| | | 硬件规格 | ≥4TB 的机械硬盘 1 块 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 8 | 桌面云服务器一体机 | 硬件规格 | CPU≥12 核 2.4GHZ，内存≥192G、千兆网口≥6 个、万兆光口≥2 个、电源：冗余电源。系统盘不低于 2 块 240GB SATA SSD 硬盘、缓存盘不低于 2 块 960G-SSD 硬盘，数据盘不少于 4 块 6T 的 SATA 硬盘。 | 2 | 台 |
| | | 接入软件 | 支持发布专有桌面、还原桌面（包括池化桌面）、共享桌面、远程应用至少 5 种桌面资源，满足不同场景的应用需求。 | | |
| | | 虚拟化功能要求 | 单集群管理时无需部署集中管理平台，通过 Web 方式接入集群主服务器，实现对服务器、虚拟机、网络、存储虚拟化等进行统一管理。 | | |
| | | | 支持服务器端口汇聚技术（管理口、业务口、存储口），将多个网络端口聚合起来，提高网络带宽和容错能力 | | |
| | | | 支持虚拟机集中备份与恢复，可按需选择多个虚拟机或全部虚拟机备份至外置服务器，支持设置备份策略，实现全自动化备份。 | | |
| | | | 支持自动/手动将配置文件备份到 FTP 服务器。 | | |
| | | | 支持磁盘故障自动重建技术、支持磁盘横向/纵向扩展。 | | |
| | | | 支持集群冗余技术，当硬盘故障时，HA 机制就会自动触发虚机迁移动作，实现毫秒级切换，对用户来讲基本是无感知的；主机或者网络故障，虚拟桌面可以快速切换到另一台服务器拉起，约 3～5 分钟。以保障用户稳定地使用 | | |
| | | 功能授权 | 包含虚拟化平台软件使用授权。 | | |
| | | | 包含不限制虚拟存储容量的存储虚拟化授权。 | | |
| 9 | 桌面云瘦客户端 | 硬件规格 | ARM 架构，CPU≥1.6Ghz、内存≥1G、存储≥4G、USB≥6 个、1 个 HDMI、至少 1 个百兆电口。 | 50 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 管理方式 | 为了方便管理，管理方式为虚拟机和瘦终端统一管理，降低管理难度。 | | |
| | | | 在瘦终端的管理方面，需支持分组管理、批量移动、删除、关闭瘦终端，支持配置定时开关机计划及加电自启动功能，支持自定义开机画面、支持联动关机功能、配置自动登录和保存密码。 | | |
| | | | 为了简化管理，要求瘦终端支持远程唤醒，管理员可以使用桌面云控制器或者第三方教学软件，例如极域等，远程开机瘦终端。 | | |
| | | 接入安全 | 考虑到接入安全，需支持修改云终端配置和登录信息时需要密码，可限制未接入过环境的瘦终端的接入或者接入桌面环境需要输入密码。 | | |
| | | 功能授权 | 包含桌面云客户端授权。 | | |

**3.14 徐汇区天平街道社区卫生服务中心网络系统升级改造**

3.14.1. 系统说明

徐汇区天平街道社区卫生服务中心网络系统承载徐汇区天平街道社区卫生服务中心各业务系统的数据交互。系统现有核心层使用的核心交换机性能已不满足现有业务系统对带宽和交换性能的需求，对其进行升级改造以满足业务需求。

3.14.2. 系统需求

1、 采用 2 台核心交换机设备采用高可用部署方式，对现有的 2 台内网核心交换机设备进行更换。核心交换机割接计划需提前进行充分的配置梳理，拟定的计划尽量缩短割接时间，保障业务持续性。

2、 采用 1 台带有网管功能 24 端口接入交换机设备对现有的 1 台供院外分支机构接入使用的无网管交换机设备进行更换，实现对分支机构接入网络的管控。同时配套网络设备线路连接所需的光模块。

3.14.3. 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 核心交换机(天平) | 性能要求 | 交换容量≥38Tbps，包转发率≥7000Mpps。 | 2 | 台 |
| | | 硬件规格 | 业务插槽数≥3，主控引擎模块≥2，配置双主控，双电源，配置 1 块 48 端口千兆光板卡，1 块 48 端口千兆电板卡。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 接口要求 | 支持千兆电口，千兆光口，万兆光口，25G 端口，40G 端口，100G 端口 | | |
| | | | 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性。 | | |
| | | ACL | 支持双向 ACL，ACL≥4K；支持端口 ACL；支持 VLAN ACL | | |
| | | 可靠性 | 支持 NSF/GR for OSFP/BGP/IS-IS；支持热补丁功能，可在线进行补丁升级 | | |
| | | QOS | 支持精细化的流量监管，粒度可达 8K | | |
| | | | 支持流量整形 Shapping | | |
| | | | 支持 802.1p、TOS、DSCP、EXP 优先级映射 | | |
| | | 多业务融合化 | 支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 Windows Server 及 AD Campus director，实现方案与设备一体化部署 | | |
| | | MPLS | 支持 L3 VPN，支持 VLL，支持 VLPS | | |
| | | VxLAN | 支持 VXLAN，能够实现 VXLAN 二三层互通 | | |
| | | 安全特性 | 支持 IPv4 uRPF，支持 DHCP Snooping，支持 ARP 防攻击 | | |
| | | | 支持 MACsec 加密技术 | | |
| | | 管理特性 | 支持 Console/AUX/Telnet/SSH2.0，支持风扇、电源管理 | | |
| | | MAC | MAC 表≥1000K，学习速率≥128K/S | | |
| | | 虚拟化 | 支持一虚多技术(1:N)、多虚一技术(N:1)，支持 4 框虚拟化技术 | | |
| | | 网络安全一体化 | 支持安全业务插卡 FW、IPS、ACG、LB、SSL VPN | | |
| | | 可视化 | 支持 Telemetry 流量可视化功能 | | |
| 2 | 接入交换机-24端口(分支站点) | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps | 1 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能,能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 3 | 千兆多模光模块 | 硬件要求 | 光模块-SFP-1000M-(850nm,500m,LC) | 52 | 个 |

**3.15 徐汇区龙华街道社区卫生服务中心服务器系统升级改造**

3.15.1 系统说明

徐汇区龙华街道社区卫生服务中心服务器系统负责承载其医疗信息化业务运行，对其提供稳定的医疗信息化业务服务保障。现有服务器性能已无法满足当前业务需要，通过对其升级改造，满足业务的性能需求。

3.15.2 系统需求

采用 1 台机架式服务器对现有服务器进行替换。同时配合采购单位对现有的业务应用进行的迁移工作，保障原有业务平滑转移到新服务器，并将原有服务器配置为冷备。

3.15.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 机架式服务器 | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 1 | 台 |
| | | CPU 规格 | ≥2 颗 Intel Xeon SP 5318H(2.5GHz/18 核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥128GB DDR4 3200 内存模块 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 内存可扩展数量 | 提供≥48 个内存槽位，最大支持 18TB 物理内存,12TB 有效内存,支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘实配规格 | ≥6 块 2.4TB 10K SAS HDD 硬盘，热插拔；支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 提供≥8 个 2.5 寸硬盘槽位,支持≥48 块 2.5 寸热插拔硬盘。 | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆网卡 | | |
| | | 冗余电源 | ≥4 个 1600W 铂金版热插拔冗余电源；支持 1+1/N+N 冗余；支持 240VDC，380VDC，48VDC | | |
| | | 冗余风扇 | 热插拔冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块，提供防火墙、IPS、防病毒和 QoS 等安全防护功能 | | |

**3.16 徐汇区凌云街道社区卫生服务中心信息系统升级改造**

3.16.1 系统说明

徐汇区凌云街道社区卫生服务中心信息系统负责承载该单位的医疗信息系统业务的数据交互、无线接入及业务运行。通过升级改造其有线接入层和无线网络扩大其信息化接入覆盖，并配套计算资源和安全设备的升级提升系统整体业务承载水平。

3.16.2 系统需求

1、采用 31 台 48 端口楼层接入交换机及 8 台 24 端口 POE 交换机对接入层网络进行建设。同时配套所需光模块，使有线接入层满足承载业务系统网络通讯的需求。

2、部署 32 台无线 AP 接入点，通过 POE 对采购单位现场进行无线接入覆盖，并配套 2 台无线网络控制器，以双机高可用方式部署，用于控制管理无线网络接入点。

3、配套采购网络机柜 6 台用以在各楼层弱电间安装交换机设备。

4、现有计算资源服务器性能已无法满足业务需求。采用 2 台计算资源服务器集群部署，替换现有计算资源服务器，并配合采购单位对现有的业务应用进行的迁移工作。

3.16.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 接入交换机-48端口（楼层） | 性能要求 | 交换容量≥430Gbps，包转发率≥80Mpps。 | 31 | 台 |
| | | 硬件规格 | 支持 48 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口。 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 2 | POE | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps | 8 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 交换机-24端口 | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口，支持 POE+供电标准 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 3 | 千兆单模光模块 | 硬件规格 | 光模块-SFP-1000M-(1310nm,10km,LC) | 88 | 个 |
| 4 | 机柜-网络型 | 尺寸要求 | 42U 高度，宽*深 600*600mm，高度≥2000mm，≤2070mm； | 6 | 台 |
| | | 安装梁材质 | 厚度≥1.5mm | | |
| | | 方孔条材质 | 厚度≥2mm | | |
| | | 门板材质 | 厚度≥1.2mm | | |
| | | 通风要求 | 前后门需采用网孔通风设计，网孔通风率≥75% | | |
| | | 配件要求 | 附有万向轮，支撑脚，前后门锁及钥匙等 | | |
| | | 承重 | 安装支撑脚时≥500kg | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 5 | 无线AP接入点 | 工作模式 | 支持双频4流，可同时工作在802.11a/b/g/n/ac/ac wave2/ax模式 | 32 | 台 |
| | | 性能要求 | 整机协商速率≥1.7Gbps，其中5G射频速率≥1.2G，2.4G速率≥0.5G。 | | |
| | | 硬件规格 | 整机接口≥1个10/100/1000Mbps(RJ45)千兆接口 | | |
| | | 空口优化 | 支持基于空口利用率的SSID自动隐藏功能，当空口繁忙程度达到或超过配置的阈值时，SSID自动隐藏，为用户提供稳定可靠的无线服务 | | |
| | | 接入安全 | 支持WPA3个人级方式下的终端接入 | | |
| | | 供电 | 支持802.3af/PoE供电标准及本地54V DC供电方式 | | |
| | | 天线 | 内置天线 | | |
| | | 安装方式 | 支持壁挂、吸顶和86盒等多种安装方式 | | |
| | | 技术支持 | 支持OFDMA技术、IPv4/IPv6双协议栈 | | |
| 6 | 无线网络控制器 | 性能要求 | 吞吐量≥10Gbps，支持对802.11a/b/g/n/ac/ ac wave2/ax AP管理 | 2 | 台 |
| | | 硬件规格 | 千兆电口≥8个，万兆光口≥2个 | | |
| | | 技术支持 | 支持信道智能切换、智能AP负载分担、IPv4/IPv6双协议栈 | | |
| | | 电源 | 双电源 | | |
| | | 认证 | 支持802.1x认证，MAC地址认证，Portal认证等 | | |
| | | 无线漫游 | 支持快速的二、三层漫游 | | |
| | | 接入控制 | 支持Open system、Shared-Key、ARP防攻击、SSID防假冒 | | |
| | | QoS | 支持优先级映射、流量限速 | | |
| | | 安全 | 支持静态、动态黑名单、白名单、防无线泛洪攻击 | | |
| | | 节能 | 支持按需定时关闭AP射频口、逐包功率控制（PPC） | | |
| | | 数据转发 | 支持集中式转发、分布式转发、策略转发，用户根据业务需要和网络实际情况可以灵活设置转发方式。 | | |
| | | 管理AP数 | 支持常规AP最大数量≥140 | | |
| | | 用户数 | 用户数规格≥4K | | |
| | | 管理授权数 | 配置不少于32个AP的管理授权 | | |
| 7 | 机架式服务器 | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 2 | 台 |
| | | CPU规格 | ≥2颗Intel Xeon SP 5318H(2.5GHz/18核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥256GB DDR4 3200内存模块 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 内存可扩展数量 | 本地提供≥48 个内存槽位，最大支持 18TB 物理内存,12TB 有效内存,支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘实配规格 | ≥5 块 1.2TB 10K SAS HDD 硬盘，热插拔；支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 本地提供≥8 个 2.5 寸硬盘槽位,支持≥48 块 2.5 寸热插拔硬盘， | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆网卡 | | |
| | | 冗余电源 | ≥4 个 1600W 铂金版热插拔冗余电源;支持 1+1/N+N 冗余;支持 240VDC,380VDC,48VDC | | |
| | | 冗余风扇 | 热插拔冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块,提供防火墙、IPS、防病毒和 QoS 等安全防护功能 | | |

**3.17 徐汇区湖南街道社区卫生服务中心信息系统升级扩容**

3.17.1 系统说明

徐汇区湖南街道社区卫生服务中心信息系统负责承载该单位的医疗信息化业务运行，提供稳定的业务服务。通过增加计算资源，升级网络设施，部署安全设备等建设，提升系统的业务能力，增强系统的信息安全。

3.17.2 系统需求

1、 部署 1 台网络流量威胁检测设备，与现有各安全设备通过网管协议及日志协议对接。实现对网络中的流量进行采集分析，使系统具有识别安全事件、记录告警、根据日志的安全分析能力及审计日志留存能力。

2、 部署 1 套安全运维监控管理系统，对现有各安全设备进行网管协议对接，使系统中各设备可进行统一的运行监控及管理。

3、 现有 2 台网御星云品牌的防火墙设备，具备入侵防护及防病毒功能模块，但其授权已过期。需提供为期 3 年的 AV、IPS 功能模块授权，及特征库的更新服务，以确保该设备安全能力的时效性。

4、 现有的计算资源性能已无法满足业务对性能的需求。通过对现有服务器及存储增加硬件配件的方式，实现对现有计算资源池的性能进行升级。需对现有计算资源服务器及存储增加 16GB 服务器 DDR3 内存条 64 条、3.5 寸存储系统硬盘 10 块、2.5 寸存储系统硬盘 6 块、双端口 FC HBA 卡 2 张、四端口 SAS HBA 卡 2 张。同时投标人应负责对现有计算资源存储配件安装扩容后，对操作系统进行磁盘阵列的扩容配置。

5、 部署 2 套 SAN 存储系统，及 2 台 SAN 存储交换机，组成 SAN 存储网络，并将该 SAN 网络与现有 SAN 存储网络对接。投标人应负责对 SAN 网络中现有所有计算资源服务器进行设置，实现 SAN 存储共享卷映射。达到对现有虚拟化资源池的存储容量进行扩容的目的。同时配套安装 1 个 42U 标准服务器机柜用于安装该 SAN 存储系统设备。现有存储系统在升级改造后与新采购的存储系统共同运行，故需要确保其业务数据、磁盘卷、逻辑分区等可与其他 SAN 存储网络及服务器 HBA 卡等相关硬件兼容，割接前应拟定测试方案并进行充分的测试。机柜需配有 2 条 8 孔或以上的 PDU 单元。

6、 现有核心交换机设备性能已无法满足需求，采用 2 台核心交换机设备及对现有的 2 台内网核心交换机设备进行割接替换，并对原有配置进行重新配置。同时部署 1 台 24 端口接入交换机设备对现有的 1 台院外分支机构接入使用的无网管交换机设备进行替换，确保院外分支机构接入网络可管理，并配套所需光模块。

3.17.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 网络流量威胁检测 | 硬件规格 | 规格：≤2U，内存大小：≥16G，硬盘容量：≥128GB SSD+4TB SATA，电源：单电源，接口：千兆电口≥6，万兆光口 SFP+≥2 | 1 | 台 |
| | | 性能要求 | 网络层吞吐量：≥1Gbps | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 系统 | 大屏可视 | 支持大屏轮播及自定义大屏顺序设置和大屏名称。自定义统计周期资产组划分、选择播放大屏及轮播时间间隔。 | | |
| | | 数据中心可视 | 可视区域基于数据中心、总部、租户等按照风险等级（优秀、良、中、差）来展示数据中心的情况。支持对数据中心正常反问的趋势和攻击者监视和分析威胁的说明。 | | |
| | | 弱口令检测 | 弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web 空密码、账号白名单、密码白名单、txt 文件格式导入。 | | |
| | | 资产全生命周期管理 | 支持自定义资产多级分支管理，最多可至 15 级分支。支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。 | | |
| | | 资产发现 | 支持通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、MAC 地址、主机名等。 | | |
| | | 文件威胁分析 | 文件威胁分析支持平台内置的静态文件检测引擎，利用多种机器学习算法组合进行综合研判。支持采用 AI 技术针对无文件落地的恶意脚本进行检测。 | | |
| | | 异常流量分析 | 支持按照对外业务流量可视、横向流量可视、外联流量可视等开放的业务流量情况，展示服务器流量排行、最活跃源主机的内网服务器的流量情况，支持全球地图展示整体外联流量情况。 | | |
| | | DNS 日志接入 | 支持 DNS 服务器日志导入，可以接入 DNS 服务器的日志，安全分析引擎将结合 DNS 服务器的日志，定位出 DNS 服务器代理风险外连场景下真实源 IP，从而有效地进行风险处置闭环。 | | |
| 2 | 安全运维监控管理系统 | 硬件规格 | 硬件参数：规格：2U，内存大小：≥48G，硬盘容量：≥128GB SSD+4TB SATA，电源：冗余电源，接口：千兆电口≥4，千兆光口 SFP≥4 | 1 | 台 |
| | | 部署模式 | 支持网桥、路由、旁路模式部署 | | |
| | | 平台要求 | 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 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持双因素认证功能，用户需在登录时进行双重认证，以此提高用户的安全性。 | | |
| | | | 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。 | | |
| | | 网管中心要求 | 支持对采用 SNMP V1、V2、V3 和 ICMP 等网络管理协议的主流品牌网络设备的监控。 | | |
| | | | 可自动扫描支持 CISCO、HUAWEI、H3C、深信服等品牌的无线 AC、AP，对连接数、在线用户数、上下行吞吐量等无线 AC/AP 设备实时数据 | | |
| | | 功能授权 | 至少提供对 30 个监控对象授权。 | | |
| 3 | 配件—服务器内存 DDR3 | 兼容要求 | PC3 L | 64 | 条 |
| | | 硬件规格 | 16GB | | |
| 4 | 配件-3.5 寸存储系统硬盘 | 兼容要求 | 3.5 寸 | 10 | 块 |
| | | 硬件规格 | ≥4TB SAS 机械硬盘 | | |
| 5 | 配件-2.5 寸存储系统硬盘 | 兼容要求 | 2.5 寸 | 6 | 块 |
| | | 硬件规格 | ≥1.2TB SAS 机械硬盘 | | |
| 6 | 配件-双口服务器 HBA 卡 | 兼容要求 | 需要具有全高及半高挡板切换设计，且兼容主流服务器硬件； | 2 | 张 |
| | | 硬件规格 | 双端口 16Gb FC HBA 卡 | | |
| 7 | 配件—四口服务器 SAS 卡 | 兼容要求 | 需要具有全高及半高挡板切换设计，且兼容主流服务器硬件； | 2 | 张 |
| | | 硬件规格 | 四端口服务器 SAS 12Gb 卡 | | |
| 8 | 机柜-服务 | 尺寸要求 | 42U 高度，宽*深 600*1200mm，高度≥2000mm，≤2070mm； | 1 | 台 |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 器型 | 安装梁材质 | 厚度≥1.5mm | | |
| | | 方孔条材质 | 厚度≥2mm | | |
| | | 门板材质 | 厚度≥1.2mm | | |
| | | 通风要求 | 前后门需采用网孔通风设计，网孔通风率≥75% | | |
| | | 配件要求 | 附有万向轮，支撑脚，前后门锁及钥匙等 | | |
| | | 承重 | 安装支撑脚时≥800kg | | |
| 9 | SAN 存储系统 | 控制器数量 | 标配 2 个热插拔存储控制器 | 2 | 台 |
| | | 存储处理器 | 每个控制器配置 2 颗物理处理器。 | | |
| | | 缓存 | 双控配置≥24GB 缓存，存储系统掉电无需电池进行保护。 | | |
| | | 主机接口 | ≥8 个 16Gbps FC 主机接口/阵列，实配≥8 个 FC 接口的授权及模块。 | | |
| | | 硬盘类型 | 同时支持 SSD、15K SAS、10K SAS 和 7.2K NL-SAS 硬盘，支持硬盘混插；标配 2 块 1.92TB SSD，配置≥10 块 2.4T 10K SAS HDD 硬盘。 | | |
| | | 硬盘扩展 | 最大支持 240 块 SFF 或者 108 块 LFF+24SFF，同时支持 SFF 和 LFF 扩展柜混扩 | | |
| | | 可扩展容量 | 最大可扩展容量为 1.92PB | | |
| | | Raid 级别 | 支持 RAID 0/1/5/6/10 | | |
| | | 高速磁盘故障恢复 | 采用高速多对多磁盘故障恢复方式，提高恢复速度的同时，可保证磁盘复期间应用的性能。无专用指定热备盘，重建全局并发。 | | |
| | | 虚拟化阵列 | 允许数据卷跨越同时最多 240 块硬盘，无需进行线性 Raid 后空间再绑定 | | |
| | | 精简配置 | 配置卷的精简配置管理功能，即实际主机映射的存储空间超出存储实际拥有的磁盘空间。要求精简配置支持空间在线回收。 | | |
| | | LUN 数量 | 最大 512 个 LUN，配置 LUN 动态扩容许可，每个 LUN 最大支持 140TB | | |
| | | 智能写感知 | 配置智能写感知功能，通过写 I/O 分辨，将随机写 IO 数据自动存储到性能层（SSD），将顺序写 I/O 数据存储到更加经济的标准层和归档层，以提高存储介质存储选择的精准度，节约成本 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 智能分层 | 支持数据智能分层功能。单个 LUN 中的数据，可按照实际的 I/O 压力自动在性能层(SSD)、标准层(10/15K SAS)和归档层(7.2K NL-SAS)之间进行自动迁移，无需中断业务。自动分级存储功能支持 I/O 每个卷可在三个不同类型的硬盘之间进行自动迁移。可以进行手动或自动迁移。 | | |
| | | 远程复制 | 支持数据异步复制，支持阵列间的故障切换和切回功能。 | | |
| | | 健康状态检测 | 配置智能健康检测功能，对海量运行数据分析，分析引擎将收集常见故障特征，给出存储的运行状态和修复调整建议，从而实现潜在故障的预测和预防。 | | |
| | | 断电保护 | 支持断电时将控制器缓存数据写入硬件存储设备中，可永久保护，在保护过程中不需要电池保护方式 | | |
| 10 | SAN 存储交换机 | 系统架构 | 无拥塞架构设计，所有 FC 端口全线速 | 2 | 台 |
| | | 硬件规格 | 最大可扩展端口≥24，需要激活≥8 个 16Gb FC 端口，实配≥8 个 16Gb-FC 多模模块以及相关光纤线缆 | | |
| | | 端口速率 | 同时支持 FC 32Gb/s，16Gb/s， 8Gb/s 和 4Gb/s 速率 | | |
| | | 端口类型 | 同时支持 F/E/M/D/EX 等端口类型 | | |
| | | 互联扩展 | 可支持多台交换机级联和 Fabric 扩展 | | |
| | | 链路捆绑 | 支持基于数据帧级的“即插即用”的链路捆绑功能，单个链路聚合带宽最大 256G | | |
| | | 系统延时 | 平均延迟≤2.1 微秒 | | |
| | | 监控管理 | 支持 SNMPv1/v3 的集中监控管理 | | |
| | | 安全性 | 支持数据的压缩及加密、基于数据帧级别的前向纠错和交换机接入认证功能 | | |
| | | 诊断 | 提供基于 D-Port 的端口自诊断功能,包括电/光环回、链路流量、延时和距离 | | |
| | | 管理功能 | 具备的 HTTP 方式的交换机管理并支持端口性能监控，参数修改等功能 | | |
| 11 | 核心交换机(湖南) | 性能要求 | 交换容量≥38Tbps，包转发率≥7000Mpps。 | 2 | 台 |
| | | 硬件规格 | 业务插槽数≥3，每台设备配置双主控，双电源，1 块 48 端口千兆电板卡，1 块 48 端口千兆光板卡 | | |
| | | 接口要求 | 支持千兆电口，千兆光口，万兆光口，25G 端口，40G 端口，100G 端口 | | |
| | | | 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | ACL | 支持双向 ACL，ACL≥4K；支持端口 ACL；支持 VLAN ACL | | |
| | | 可靠性 | 支持 NSF/GR for OSFP/BGP/IS-IS；支持热补丁功能，可在线进行补丁升级 | | |
| | | QOS | 支持精细化的流量监管，粒度可达 8K | | |
| | | | 支持流量整形 Shapping | | |
| | | | 支持 802.1p、TOS、DSCP、EXP 优先级映射 | | |
| | | 多业务融合化 | 支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 Windows Server 及 AD Campus director，实现方案与设备一体化部署 | | |
| | | MPLS | 支持 L3 VPN，支持 VLL，支持 VLPS | | |
| | | VxLAN | 支持 VXLAN，能够实现 VXLAN 二三层互通 | | |
| | | 安全特性 | 支持 IPv4 uRPF，支持 DHCP Snooping，支持 ARP 防攻击 | | |
| | | | 支持 MACsec 加密技术 | | |
| | | 管理特性 | 支持 Console/AUX/Telnet/SSH2.0，支持风扇、电源管理 | | |
| | | MAC | MAC 表≥1000K，学习速率≥128K/S | | |
| | | 虚拟化 | 支持一虚多技术（1:N）、多虚一技术（N:1），支持 4 框虚拟化技术 | | |
| | | 网络安全一体化 | 支持安全业务插卡 FW、IPS、ACG、LB、SSL VPN | | |
| | | 可视化 | 支持 Telemetry 流量可视化功能 | | |
| 12 | 接入交换机-24端口（分支站点） | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps。 | 1 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 管理和维 | 支持 SNMP V1/V2/V3、RMON、SSHV2 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 护 | 支持 OAM(802.1AG， 802.3AH）以太网运行、维护和管理标准 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink,收敛时间≤50ms;支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 13 | 千兆多模光模块 | 硬件规格 | 光模块-SFP-1000M-(850nm,500m,LC) | 52 | 个 |
| 14 | 现有网御星云防火墙原厂授权续约 | 授权说明 | 适用于网御星云防火墙 3 年期原厂授权，包括 IPS 及 AV 功能模块授权及特征库更新授权，2 套 | 1 | 项 |

**3.18 徐汇区枫林街道社区卫生服务中心计算资源系统升级改造**

3.18.1 系统说明

建设徐汇区枫林街道社区卫生服务中心计算资源系统，为该单位提供虚拟化计算资源以承载虚拟机业务运行。现有计算资源已不满足当前业务需要，通过增设超融合计算集群，提升计算资源池的整体水平，满足业务的稳定运行和后续发展需要。

3.18.2 系统需求

采用三节点超融合方式部署 3 台机架式服务器，作为虚拟化资源池服务器使用，并配套部署 2 台超融合网络交换机组成集群节点间互联网络基础，保障节点间的高带宽数据通讯需求。

3.18.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 机架式服务器 | 硬件规格 | 处理器：每台节点配置 2 颗 CPU ，采用 2.4GHZ(10C）或以上的 CPU | 3 | 台 |
| | | | 内存：每台服务器内存≥128GB | | |
| | | | 接口：每台服务器配置≥6 个千兆电口，万兆光口≥2 个 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 存储：每个节点配置 960G-SSD≥2 块，配置 4T SATA≥4 块 | | |
| | | 云计算平台要求 | 支持大屏展示便于客户直观查看虚拟化资源池的使用情况和健康状态，包括集群资源情况，各主机资源使用情况，存储资源池的 IO 次数、IO 速率、IO 时延、存储命中率、主机命中率，以及集群故障与告警，支持 Top 5 主机 CPU 和内存利用率、Top 5 虚拟机 CPU 和内存利用率信息大屏展示等 | | |
| | | | 支持跨地域的多集群管理，可纳管不少于 256 个物理机节点，支持不少于 30000 台云主机的规模 | | |
| | | | 支持主备切换，当主平台发生故障时，能够切换到备平台，保障云平台稳定运行 | | |
| | | | 支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件 | | |
| | | | 云计算管理平台，和底层资源池部分可以支持扩展网络和安全虚拟化（虚拟应用防火墙、虚拟应用负载均衡等）功能组件，以保障平台的扩展性和兼容性 | | |
| | | 计算虚拟化要求 | 虚拟化软件非 OEM 或贴牌产品，禁止借用第三方软件的整合，以保证功能的可靠性和安全性 | | |
| | | | 支持对平台的硬件进行监控和大屏展示，包含 CPU，内存，网卡，硬盘，存储，RAID 等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议 | | |
| | | | 支持一键还原已删除的虚拟机，可恢复 30 天内已删除的虚拟机 | | |
| | | | 为避免主机假死导致系列问题发生，支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险 | | |
| | | | 虚拟化的管理平台、可以支持扩展存储虚拟化、网络功能虚拟化、虚拟应用防火墙、虚拟应用交付、SSL VPN 软件、数据库审计软件等功能组件的，并支持统一管理，以保障平台的扩展性和兼容性。 | | |
| | | | 需支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用 License 激活的方式即开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 支持为虚拟磁盘配置不同的存储策略以满足特定场景的需求， 如系统盘和数据盘选择高性能策略， 备份盘选择低性能策略 | | |
| | | | 支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性 | | |
| | | 内建安全要求 | 云安全中心需集成于虚拟化平台中，一体化方式交付，无需第三方平台承载，平台必须能够提供虚拟主机安全防护安全能力，并对检测到的恶意活动可自动采取分布式防火墙隔离虚拟机、为虚拟机拍摄快照等防护手段。 | | |
| | | 功能授权 | 提供计算虚拟化、网络虚拟化、存储虚拟化软件授权 | | |
| 2 | 接入交换机-24端口（服务器） | 硬件规格 | 万兆 SFP+光口≥12 个；千兆电口≥12 个； | 2 | 台 |
| | | 性能要求 | 交换容量≥1.28Tbps /12.8Tbps | | |
| | | | 包转发率≥480Mpps | | |
| | | 接入方式 | 支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时在控制器平台灵活的进行切换 | | |
| | | 访问控制策略 | 支持基于交换机单端口、聚合口的 ACL 策略； | | |
| | | | 支持基于源目 IP 地址、MAC 地址的 ACL 策略； | | |
| | | | 支持基于时间的 ACL 策略； | | |
| | | 生成树 | 支持 STP、RSTP、MSTP 协议 | | |
| | | 组播 | 支持 IGMP v1/v2/v3 Snooping | | |
| | | VLAN | 支持 4K 个 VLAN | | |
| | | EEE | 支持 IEEE 802.3az 标准的 EEE 节能技术：当 EEE 使能时，从而大幅度的减少端口在该阶段的功耗，达到了节能的目的。 | | |
| | | MAC | 支持 MAC 地址≥32K | | |
| | | | 支持 MAC 地址自动学习 | | |
| | | | 支持源 MAC 地址过滤 | | |
| | | | 支持接口 MAC 地址学习个数限制 | | |
| | | 端口聚合 | 支持端口聚合≥128 个 | | |
| | | | 支持手工和静态 LACP | | |
| | | ARP | ARP≥16K | | |
| | | DHCP | 支持 DHCP Server | | |
| | | 三层功能 | 支持静态路由 | | |
| | | | 路由表≥1000 | | |
| | | 网络管理 | 支持通过控制器平台跨广域网、NAT 远程管理智能交换机 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 交换机画像管理 | 支持通过在控制器平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息 | | |
| | | | 支持通过控制器平台图形化操作对交换机端口状态的开启与关闭； | | |

3.19 徐汇区漕河泾街道社区卫生服务中心信息系统升级改造

3.19.1 系统说明

徐汇区漕河泾街道社区卫生服务中心信息系统包括业务服务器、网络接入层、桌面云终端及机房 UPS 四个部分，承载该单位的信息系统业务运转。现有计算服务器和 UPS 基础设施使用年限较长，性能已不满足业务对性能和稳定的需求。对其进行升级改造强化系统整体水平。同时，扩大桌面云终端的应用范围，保障资源的高效利用率。

1、业务服务器

通过更换新的服务器设备替换掉原有性能不足的旧设备。使硬件性能满足当前业务要求。

2、网络接入层

通过部署新的接入层交换机设备替换掉原有性能不足的旧设备。使网络交换性能满足当前业务要求。

3、桌面云终端

增加虚拟云桌面瘦终端，扩大虚拟云瘦终端的使用范围。推进对客户端业务进行云桌面化改造，

4、UPS

UPS 设备作为供电设施是信息系统安全稳定运行的基础设备，现有设备负载能力不足，电池使用年限长。通过更换新设备对 UPS 整体进行升级改造。

3.19.2 系统需求

1、现有的 HIS 及 WEB 业务服务器性能已不满足当前业务需求，采用 2 台服务器分别对现有 HIS 业务及 WEB 业务服务器进行硬件替换，投标人在硬件部署完毕后，需配合采购单位对现有业务系统进行迁移的工作。机架式服务器替换操作前需提前进行方案步骤规划和测试，缩短切换过程中的中断时间。

2、现有接入交换机性能已无法满足业务对带宽的需要，采用 10 台楼层接入交换机对现有设备进行替换，其中中心站点部署 5 台，分支站点部署 5 台，且原有交换机的端口及

VLAN 等配置需要移植到新交换机设备。

3、现有系统承载桌面云系统运行，桌面终端数量无法满足业务需求。需要增设 15 套桌面云终端系统，配置接入现有桌面云计算资源服务器对云桌面系统进行扩容。

4、现有 UPS 设备负载能力已不满足当前设备的功耗需求，采用新 UPS 设备对现有设备进行更换。投标人在 UPS 设备安装替换过程中需配合采购单位提前进行设备断电前的检查及配置和数据的备份工作，确保电力恢复后各业务系统正常启动。UPS 设备替换应与其他设备替换分别进行。

3.19.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 机架式服务器（HIS） | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 1 | 台 |
| | | CPU 规格 | ≥2 颗 Intel Xeon SP 5318H(2.5GHz/18 核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥128GB DDR4 3200 内存模块 | | |
| | | 内存可扩展数量 | 本地提供≥48 个内存槽位，最大支持 18TB 物理内存，12TB 有效内存，支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘实配规格 | ≥5 块 600GB 10K SAS HDD 硬盘，热插拔；支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 本地提供≥8 个 2.5 寸硬盘槽位，支持≥48 块 2.5 寸热插拔硬盘。 | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆网卡 | | |
| | | 冗余电源 | ≥2 个 1600W 铂金版热插拔冗余电源；支持 1+1/N+N 冗余；支持 240VDC，380VDC，48VDC | | |
| | | 冗余风扇 | 热插拔冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块，提供防火墙、IPS、防病毒和 QoS 等安全防护功能 | | |
| 2 | 机架式服务器（WEB） | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 1 | 台 |
| | | CPU 规格 | ≥2 颗 Intel Xeon SP 5318H(2.5GHz/18 核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥128GB DDR4 3200 内存模块 | | |
| | | 内存可扩展数量 | 本地提供≥48 个内存槽位，最大支持 18TB 物理内存，12TB 有效内存，支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘实配规格 | ≥5 块 1.2TB 10K SAS HDD 硬盘，热插拔；支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 本地提供≥8 个 2.5 寸硬盘槽位，支持≥48 块 2.5 寸热插拔硬盘。 | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆网卡 | | |
| | | 冗余电源 | ≥2 个 1600W 铂金版热插拔冗余电源；支持 1+1/N+N 冗余；支持 240VDC，380VDC，48VDC | | |
| | | 冗余风扇 | 热插拔冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块，提供防火墙、IPS、防病毒和 QoS 等安全防护功能 | | |
| 3 | 接入交换机-48 端口（楼层） | 性能要求 | 交换容量≥430Gbps，包转发率≥80Mpps。 | 10 | 台 |
| | | 硬件规格 | 支持 48 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 4 | 桌面云瘦终端 | 硬件规格 | ARM 架构，CPU≥1.4Ghz、内存≥1G、存储≥4G、USB≥6 个、1 个 VGA、至少 1 个百兆电口。 | 15 | 台 |
| | | 运维管理 | 为了方便管理，管理方式为虚拟机和瘦终端统一管理，降低管理难度。 | | |
| | | | 在瘦终端的管理方面，需支持分组管理、批量移动、删除、关闭瘦终端，支持配置定时开关机计划及加电自启动功能，支持联动关机功能、配置自动登录和保存密码。 | | |
| | | | 为了简化管理，要求瘦终端支持远程唤醒，管理员可以使用桌面云控制器或者第三方教学软件，例如极域等，远程开机瘦终端。 | | |
| | | 接入安全 | 考虑到接入安全，需支持修改云终端配置和登录信息时需要密码，可限制未接入过环境的瘦终端的接入或者接入桌面环境需要输入密码。 | | |
| | | 兼容性 | 要求所投产品与单位现有使用桌面云软件保证兼容。 | | |
| | | 功能授权 | 配套所需授权 | | |
| 5 | UPS 系统 | UPS 类型 | 在线 UPS | 1 | 套 |
| | | UPS 额定容量 | 10KVA / 8KW | | |
| | | UPS 电源效率 | ≥90% | | |
| | | 输入电压范围 | 176-276V | | |
| | | 输出电压（VAC） | 220×(1±1%) | | |
| | | 并联方式 | 可多台扩容并联或 N+1 并联冗余 | | |
| | | 维护旁路 | 提供维修旁路开关 | | |
| | | 启动功能 | 具备直流启动功能 | | |
| | | 备用时间 | 电池时间按 30 分钟配置 | | |
| | | 电池管理 | 采用智能化电池管理系统 | | |
| | | 面板显示 | 状态管理控制显示 | | |
| | | 报警功能 | 市电异常、电池欠压、过载、UPS 故障 | | |
| | | 通讯功能 | 提供干接点通讯和 RS232，实现 UPS 的智能监控 | | |
| | | 电磁兼容 | 符合 GB7260.2-2003 | | |
| | | 电池 | 国内生产知名品牌，按单机延时 30 分钟配置，含配套电池柜 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 电池规格 | 12V 100AH，电池寿命不少于 5 年 | | |
| | | 电池类型 | 免维护密封铅酸电池防漏 | | |
| | | 售后服务 | 提供不少于 3 年质保 | | |

**3.20 徐汇区华泾镇社区卫生服务中心信息系统升级改造**

3.20.1 系统说明

徐汇区华泾镇社区卫生服务中心信息系统承载医疗业务运行及数据库服务。现有网络基础设施陈旧，计算基础设施性能不足，为满足医疗业务的需求增长，对系统进行升级改造，并增设患者自助终端等设施提高医疗业务整体水平。

3.20.2 系统需求

1、现有核心交换机已经无法满足业务需求，采用 2 台核心交换机设备进行高可用部署对现有设备进行替换。核心交换机需要附带所需 SFP+万兆堆叠线缆实现堆叠部署。

2、为满足三级等保要求中对于网络分层分区的要求，对现有网络结构进行调整，通过建设独立的服务器接入层，机房设备接入层和客户端接入层使网络结构进行分层化。采用 4 台服务器机柜 48 端口接入交换机设备堆叠部署建设服务器接入层，采用 4 台机房接入 24 端口交换机设备建设机房设备接入层，采用 8 台楼层接入 24 端口交换机、5 台楼层接入 24 端口 POE 交换机、7 台社区接入 24 端口 POE 交换机建设客户端接入层。

3、整合修改现有核心交换机配置，使本项目中建设的各接入层汇聚对接到本项目中建设的核心交换机，投标人应采用三层对接。隔离各区域广播域。并负责配套相应的网络设备线缆及光模块供设备间堆叠及链路连接使用。

4、核心交换机需要配套万兆单模光模块 2 个、服务器机柜 48 端口接入交换机需配套万兆单模光模块 16 个、机房接入 24 端口交换机需采购万兆单模光模块 16 个、楼层接入 24 端口交换机需采购千兆单模光模块 32 个、POE 楼层接入 24 端口交换机需采购千兆单模光模块 20 个、POE 社区接入 24 端口交换机需采购千兆单模模块 28 个。

5、现有数据库服务器已经无法满足业务性能需要。采用 2 台机架式服务器，组成数据库双机集群。根据现有医疗应用的需要，数据库必须采用 SQL Server 数据库软件，固服务器需要采用 Windows Server 操作系统。投标人需负责提供 2 台服务器所需的 Windows Server 操作系统软件。

6、Win 系统 SQL 数据库组件双机高可用集群需要采用 NEC ExpressCluster 方式，投标人需提供该数据库高可用集群软件 1 套，并负责组件数据库高可用集群配置工作，最终实现数据库双活结构满足性能和数据安全需求。

7、投标人需配合采购单位将原有数据库服务器配置为冷备使用的工作。

8、部署 3 台电子票据自助终端以满足患者对自助票据打印的需求。电子票据自助机内置的医保读卡器应支持上海市医保/社保卡，符合上海市医保有关部门的型号规格要求。

3.20.3 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 核心交换机（华泾镇） | 性能要求 | 交换容量≥75Tbps，包转发率≥8600Mpps。 | 2 | 台 |
| | | 硬件规格 | 业务插槽数≥6，主控引擎模块≥2，配置双主控，双电源；配置 1 块 48 端口万兆光板卡，1 块 48 端口千兆光板卡，3 米 SFP+万兆堆叠电缆。 | | |
| | | 接口要求 | 支持千兆电口，千兆光口，万兆光口，25G 端口，40G 端口，100G 端口 | | |
| | | | 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性 | | |
| | | ACL | 支持双向 ACL，ACL≥4K；支持端口 ACL；支持 VLAN ACL | | |
| | | 可靠性 | 支持 NSF/GR for OSFP/BGP/IS-IS；支持热补丁功能，可在线进行补丁升级 | | |
| | | QOS | 支持精细化的流量监管，粒度可达 8K | | |
| | | | 支持流量整形 Shapping | | |
| | | | 支持 802.1p、TOS、DSCP、EXP 优先级映射 | | |
| | | 多业务融合化 | 支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 Windows Server 及 AD Campus director，实现方案与设备一体化部署 | | |
| | | MPLS | 支持 L3 VPN，支持 VLL，支持 VLPS | | |
| | | VxLAN | 支持 VXLAN，能够实现 VXLAN 二三层互通 | | |
| | | 安全特性 | 支持 IPv4 uRPF，支持 DHCP Snooping，支持 ARP 防攻击 | | |
| | | | 支持 MACsec 加密技术 | | |
| | | 管理特性 | 支持 Console/AUX/Telnet/SSH2.0，支持风扇、电源管理 | | |
| | | MAC | MAC 表≥1000K，学习速率≥128K/S | | |
| | | 虚拟化 | 支持一虚多技术(1:N)、多虚一技术(N:1)，支持 4 框虚拟化技术 | | |
| | | 网络安全一体化 | 支持安全业务插卡 FW、IPS、ACG、LB、SSL VPN | | |
| | | 可视化 | 支持 Telemetry 流量可视化功能 | | |
| 2 | 接入交换机-48 端 | 性能要求 | 交换容量≥430Gbps，包转发率≥160Mpps。 | 4 | 台 |
| | | 硬件规格 | 支持 48 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口，双电源冗余。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | 口（服务器机柜） | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 3 | 接入交换机-24 端口（机房） | 性能要求 | 交换容量≥430Gbps，包转发率≥120Mpps。 | 4 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口，双电源冗余。 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 4 | 接入交换机-24 端口（楼层） | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps。 | 8 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口，双电源冗余。 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 5 | POE 交换机-24 端口（楼层） | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps。 | 5 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口，支持 POE+供电标准。 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 6 | POE 交换机-24 端口（社区） | 性能要求 | 交换容量≥330Gbps，包转发率≥50Mpps | 7 | 台 |
| | | 硬件规格 | 支持 24 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口，支持 POE+供电标准。 | | |
| | | 性能指标 | MAC 地址表≥16K；路由表容量≥1K；ARP 表项≥1K | | |
| | | ERPS | 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms | | |
| | | CPU 防护 | 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作 | | |
| | | 堆叠 | 支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； | | |
| | | 组播协议 | 支持 IGMP v1/v2/v3，MLD v1/v2；支持 PIM Snooping；支持组播 VLAN | | |
| | | 链路聚合 | 支持链路聚合基本功能及聚合零丢包 | | |
| | | 镜像功能 | 支持远程镜、支持流镜像、支持端口镜像 | | |
| | | 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 | | |
| | | VLAN | 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 可靠性 | 支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能；支持 MSTP 功能；支持 PVST 功能 | | |
| | | 路由协议 | 支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3 | | |
| 7 | 千兆单模光模块 | 硬件规格 | 光模块-SFP-1000M-(1310nm,10km,LC) | 80 | 个 |
| 8 | 万兆单模光模块 | 硬件规格 | 光模块-SFP+-10G-(1310nm,10km,LC) | 34 | 个 |
| 9 | 机架式服务器（数据库） | 硬件规格 | 机架式，≤4U，标配原厂导轨 | 2 | 台 |
| | | CPU 规格 | ≥4 颗 Intel Xeon SP 5318H(2.5GHz/18 核/24.75MB/150W）处理器 | | |
| | | 内存规格 | ≥256GB DDR4 3200 内存模块 | | |
| | | 内存可扩展数量 | 本地提供≥48 个内存槽位，最大支持拓展到 18TB 物理内存，12TB 有效内存，支持 24 个 Intel PMem 200 数据中心级持久内存，单条 128/256/512GB | | |
| | | 硬盘规格 | ≥2 块 480GB 读写混合型 SSD 硬盘，≥6 块 2.4TB 10K SAS HDD 硬盘，热插拔；可支持 2.5 寸 SAS/SATA/SSD/NVMe 硬盘 | | |
| | | 内置硬盘扩展 | 提供≥8 个 2.5 寸硬盘槽位，支持≥48 块 2.5 寸热插拔硬盘。 | | |
| | | NVMe 硬盘 | 支持最多 24 个前置 2.5 寸可热插拔 NVMe PCIe SSD 硬盘 | | |
| | | 阵列控制器 | ≥1 个阵列卡，配置 12Gbps SAS 磁盘阵列控制器，支持 Raid0/1/10/5/50/6/60；≥2GB 缓存，支持缓存数据保护，且后备保护不受时间限制 | | |
| | | IO 扩展插槽 | ≥6 个 PCI-e 3.0 全高插槽，可扩展至≥18 个全高标准 PCI-e 插槽。 | | |
| | | GPU | 支持≥3 张双宽 GPU 卡或 9 张单宽 GPU 卡 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100 GE 网卡，IB 卡；本次配置≥1 张 4 端口千兆网卡，≥2 张 2 端口万兆网卡（含模块），≥1 张 2 端口 16GB FC HBA 卡（含模块） | | |
| | | 冗余电源 | ≥4 个 1600W 铂金版热插拔型冗余电源；支持 1+1/N+N 冗余；支持 240VDC，380VDC，48VDC | | |
| | | 冗余风扇 | 热插拔型冗余风扇 | | |
| | | 工作温度 | 5℃～45℃ | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 安全性 | 支持安全机箱，TCM/TPM 安全模块，可选可信硅根固件保护模块，双因素认证；可选配置 PCIe 安全防护模块，提供防火墙、IPS、防病毒和 QoS 等安全防护功能。 | | |
| 10 | 电子票据自助机终端 | 屏幕尺寸 | 屏幕尺寸≥32 英寸。 | 3 | 台 |
| | | 触控要求 | 屏幕支持≥5 点的电容触控。 | | |
| | | 硬件规格 | 采用 x86_64 架构处理器，具备 7*24 小时开机的能力，内存容量≥4GB，固态硬盘，容量≥128GB | | |
| | | 宽行打印机 | 具备宽行打印机，可适应医院各科室要求，打印各种长度纸张，如收费处发票、清单，检验科化验单等 | | |
| | | | 具备自动切纸功能，并提供相关证明材料 | | |
| | | 凭条打印机 | 具备热敏技术凭条打印机。 | | |
| | | 条码扫描器 | 具备条码扫描器， 需要支持手机屏幕扫描二维码，纸质二维码，纸质一维码等各类条码。 | | |
| | | 读卡器 | 具备用于医保卡的磁条及 IC 读卡器及三代身份证读卡器。 | | |
| 11 | 数据库双机服务器配套操作系统授权 | 授权说明 | Windows Server 操作系统，服务期≥3 年的授权 2 套 | 1 | 项 |
| 12 | 数据库双机服务器配套集群软件授权 | 授权说明 | NEC EXPRESSCLUSTER 数据库群集软件，服务期≥3 年授权 1 套 | 1 | 项 |

**3.21 徐汇区区域卫生信息系统安全监管平台续建配套硬件采购**

为配套徐汇区卫生系统信息安全监管平台开发建设，需要分别在 6 家分支机构各部署 1

台网络流量探针、1 台 TAP 流量分流器、1 台安全管理中心一体机及 1 台分布式监管数据收集联动分析一体机。即 6 家分支机构各部署 4 台设备，作为运行信息安全监管平台系统的硬件支撑。

3.21.1 工作量清单及技术参数要求

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| 1 | 网络流量探针 | 硬件规格 | 1U 机架式设备，内存≥32G，硬盘≥1T*2，网口≥6 个千兆电口，≥2 个千兆光口，沙箱个数≥1 个，冗余电源。 | 6 | 台 |
| | | 性能要求 | 吞吐量≥1.5G。 | | |
| | | 威胁检测能力 | 提供多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等。矿池协议告警须提供虚拟币种类别；挖矿告警须提供专项告警页面，独立于其他告警；能够自动解析 DNS 响应的矿池及 IP 地址。（提供相关证明材料）。 | | |
| | | | 支持超过 100 种以上的网络协议支持，如 HTTP, FTP, TFTP, SMTP, POP3, IMAP, SNMP, IRC, DNS, DHCP, P2P, SMB, RDP, VNC, TELNET, TCP, UDP 等协议 | | |
| | | | 能够侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等，并支持多种高危病毒的侦测：Ransomware/ WORM_DOWNAD.E/ WORM_RONTKBR/ WORM_SILLYIM/ WORM_WALEDAC/ TROJ_ILOMO/ TROJ_FAKEAV/ PE_VIRUX。 | | |
| | | | 支持按照网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警进行分类，提高运维效率。 | | |
| | | 未知威胁分析能力 | 提供内置沙箱系统，内置沙箱允许用户导入自定义镜像。 | | |
| | | | 具有高度定制化，可以支持使用客户环境特性的 Windows 操作系统平台与应用。 | | |
| | | | 服务器级：Windows 2003/2008/2012 | | |
| | | | 用户端级：Windows XP/7/8/10 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 广泛的文档分析支持：Acrobat Reader 7, 8, 9, X, 微软 Office 常用版本（Word, Excel, PowerPoint）、Flash 常用版本、LNK、执行文件，微软 HTML Application（HTA）， JS, JSE, VBS, VBE, Java, Java Applet，PowerShell Script 等。 | | |
| | | | 提供灵活的沙箱投递策略，支持按照数据网络协议、文件类型等条件灵活配置投递策略。 | | |
| | | | 提供样本分析报告，报告内容包括：样本基本信息、执行后行为记录、重点标注恶意行为。 | | |
| | | | 支持未知威胁事件证据留存。 | | |
| | | 威胁检测特征自定义 | 支持网络威胁自定义与威胁情报自定义，网络威胁能自主添加规则名称，规则等级与规则类型，语法兼容业界最常用的 snort 规则的写法。威胁情报自定义包括 IP、URL、DOMAIN、文件 HASH 四种类型，可以根据具体的使用场景进行选择。威胁情报自定义的规则可以支持多个同类对象的集合，比如对多个 IP 同时进行监控。 | | |
| | | 联动能力 | 支持与现有及本次所投的防病毒网关、流量探针网络系统进行策略统一下发，并可对现有及本次所投防病毒网关设备进行产品补丁下发。 | | |
| | | 威胁溯源能力 | 能够以文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来。 | | |
| | | | 支持 pcap 回放功能，对导入的 pcap 进行回放并进行威胁检测，回放产生的告警必须和生产网络流量的告警分页面展示，避免干扰正常安全运营。 | | |
| | | 智能研判 | 支持失陷主机的智能研判功能。 | | |
| | | | 能够追踪到失陷主机 IP 号，攻击阶段数，命中规则数，攻击次数，是否外联，风险值等能力； | | |
| | | | 能够提供攻击详情分析，包含攻击结果，攻击者信息，攻击时间线，攻击规则汇总，入侵检测攻击上下文等； | | |
| | | | 支持报告详情下载； | | |
| | | 多设备日志统一呈现 | 支持多台设备的告警日志的统一收集和存储。 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 分级分权管理 | 平台支持多级组织分级分权管理，平级组织的数据（资产数据、告警数据、流量日志等）相互隔离，彼此不可见，上级组织用户对下级组织的数据可见、可运维。 | | |
| 2 | TAP 流量分流器 | 性能要求 | 交换容量≥4.8Tbps。 | 6 | 台 |
| | | | 包转发率≥2000Mpps。 | | |
| | | 硬件规格 | 支持 48 个万兆光口，2 个 QSFP+光口，4 个 QSFP28 光口，配置双电源，双风扇 | | |
| | | VxLAN | 支持 VxLAN 二层网关，支持 VxLAN 三层网关，支持 EVPN。 | | |
| | | 虚拟化 | 支持集群或堆叠多虚一技术，实现单一界面管理多台设备。 | | |
| | | 流量调度 | 支持 ACL、CAR、Remark 等动作； 支持 PQ、WFQ、PQ+WFQ 等队列调度方式 | | |
| | | TAP 镜像功能 | 镜像功能：支持本地端口镜像和远程端口镜像；支持 N：M 流量镜像 | | |
| | | 可靠性 | 支持 BFD FOR VRRP 功能，支持 RRPP，支持 PVST 功能 | | |
| | | | 支持电源的告警监视；电压和环境温度的监视； 支持电源、风扇模块在线热拔插 | | |
| 3 | 安全管理中心一体机 | 硬件规格 | 机架式，≤2U，标配原厂导轨 | 6 | 台 |
| | | CPU 规格 | ≥2 颗 Intel 4310(2.1GHz/12 核/18MB/120W）处理器，可支持最高 270W 处理器 | | |
| | | 内存规格 | ≥32GB 3200MHz DDR4 内存模块 | | |
| | | 内存可扩展数量 | 最大支持 32 根 DDR4 内存，最高速率 3200MT/s，支持 RDIMM 或 LRDIMM; | | |
| | | 硬盘 | ≥2 块 480GB SSD，≥2 块 600GB 10K SAS HDD 硬盘 | | |
| | | 硬盘槽位 | 本地提供≥8 个 2.5 寸硬盘槽位，支持 SAS/SATA HDD/SSD 硬盘，支持≥37 块 2.5 寸硬盘，热插拔 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100/200 GE 网卡，IB 卡；本次配置≥1 张 4 口千兆网卡，≥1 张 2 口万兆网卡（含模块） | | |
| | | 接口 | 标配 1 个前置 VGA，1 个后置 VGA 和 1 个串口，6 个 USB 3.0（2 前置，2 后置，2 内置），1 个前置专用管理接口 | | |
| | | 冗余电源 | ≥2 个 800W 白金版热插拔冗余电源，支持 96%能效比的钛金级电源选件 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | | 满配热插拔冗余风扇 | | |
| | | 工作温度 | 支持最高 5-45° C 标准工作温度 | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 功能要求 | 支持基于资产发现、威胁情报、漏洞库等方式的内容采集，支持与监管平台的数据对接，提供相关证明材料。 | | |
| | | | 具备整体风险评分，整体风险趋势，整体合规指数，高风险应用，攻击溯源，攻击类型统计，攻击目标，攻击应用，攻击源地图，攻击事件的统计能力； | | |
| | | | 具备展示入侵检测评分，入侵检测趋势，高危入侵告警，中危入侵告警，低危入侵告警，入侵源，攻击方法，受攻击目标，受攻击应用，外部入侵预警，恶意软件评分，恶意软件趋势，病毒数量，病毒趋势，感染病毒的主机，感染特定病毒，账号管理评分，账号管理趋势，发现的用户数，用户登录，账号管理，登录失败的账号名称，登录失败的账号数量趋势，高风险账号，登录失败的目的 IP，登录失败的应用，高风险应用，异常流量源，异常流量目的 IP，恶意外联源 IP，恶意外联目的 IP，总体流量安全事件，恶意外联安全事件。 | | |
| 4 | 分布式监管数据收集联动分析一体机 | 硬件规格 | 机架式，≤2U，标配原厂导轨 | 6 | 台 |
| | | CPU 规格 | ≥2 颗 Intel 4310(2.1GHz/12 核/18MB/120W）处理器，可支持最高 270W 处理器 | | |
| | | 内存规格 | ≥32GB 3200MHz DDR4 内存模块 | | |
| | | 内存可扩展数量 | 最大支持 32 根 DDR4 内存，最高速率 3200MT/s，支持 RDIMM 或 LRDIMM； | | |
| | | 硬盘 | ≥2 块 480GB SSD，≥2 块 600GB 10K SAS HDD 硬盘 | | |

| 序号 | 名称 | 指标项目 | 指标要求 | 数量 | 单位 |
|---|---|---|---|---|---|
| | | 硬盘槽位 | 本地提供≥8 个 2.5 寸硬盘槽位，支持 SAS/SATA HDD/SSD 硬盘，支持≥37 块 2.5 寸硬盘，热插拔 | | |
| | | 网卡 | 可选基于标准 PCIe 插槽的网络适配器，支持 1/10/25/40/100/200 GE 网卡，IB 卡；本次配置≥1 张 4 口千兆网卡，≥1 张 2 口万兆网卡（含模块） | | |
| | | 接口 | 标配 1 个前置 VGA，1 个后置 VGA 和 1 个串口，6 个 USB 3.0（2 前置，2 后置，2 内置），1 个前置专用管理接口 | | |
| | | 冗余电源 | ≥2 个 800W 白金版热插拔冗余电源，支持 96%能效比的钛金级电源选件 | | |
| | | | 满配热插拔冗余风扇 | | |
| | | 工作温度 | 支持最高 5-45° C 标准工作温度 | | |
| | | 远程管理功能 | 配置≥1 个 1Gb 独立的远程管理控制端口，配置虚拟 KVM 功能， 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。 | | |
| | | 功能要求 | 支持对所有存储资源进行监控并记录节点的使用情况，支持对分布式监管数据收集联动分析一体机进行管理，提供相关证明材料。 | | |
| | | | 分布式安全设备日志采集解析、数据存储、安全事件提取和分析平台进行 IOC 威胁情报联动分析。 | | |

**四、软件开发需求**

**4.1 徐汇区卫生系统信息安全监管平台续建**

徐汇区卫生系统信息安全监管平台通过在徐汇区卫健委建设统一的信息安全监管平台和可视化交互系统，部署安全数据采集设备，收集医疗网络的资产、流量、日志等数据，通过建立整体的安全监管平台体系，做到主动发现、提前预警，帮助徐汇区卫健委全面掌握网络管理事态，提升整体网络安全全局洞察力，有效应对新型、高级安全威胁，实时了解和感知攻击状况，降低运维难度提升管理效率，协助区卫健委在整体医疗系统网络安全管理方面进一步提升和改变。

该系统遵循徐汇区卫健委的医疗网络体系安全建设要求，通过多期建设，逐一递进的

方式，要求系统在 5 年之内具备技术先进性，费用合理性，规划可延性，使用高效性，功能完整性的目标。

该系统已完成对 4 家徐汇区医疗单位（徐汇区卫生事业管理发展中心、徐汇区大华医院、徐汇区牙病防治所、徐汇区凌云街道社区卫生服务中心）实施部署和接数纳管工作，对业务系统相关的网络设备、核心网络设备的各类操作和运行的监管日志数据进行采集、集中存储和检索，同时基于对日志数据进行标准化和过滤的基础上，综合合规要求、信息安全监管要求、监管资产管理等数据，进行安全事件的关联分析、告警展现，实现基于等保 2.0 的安全事件集中监管。

本次软件开发为该系统的续建内容，包含软件的功能模块升级（包括等保合规监管及信息安全事件监管）、6 家徐汇区医疗单位的软硬件平台部署集成。软件平台部署于管发中心机房，其他医疗单位通过配套硬件进行采集分析并上报到软件平台。

4.1.1 软件功能要求

4.1.1.1 等保合规监管

(1) 安全合规智能化监管评分

a. 合规风险指标化

参照等级保护要求建立多维度的合规风险模型，需将管辖的组织机构整体合规水平和合规差距进行指标化；

b. 合规风险指标

将物理环境安全合规评分、管理中心安全合规评分、区域边界安全合规评分、计算环境安全合规评分、通信网络安全合规评分的形式，需将多个维度的合规风险指标进行展示。

c. 智能化建模打分

需基于人工智能技术结合医疗监管指标构建面向医疗机构信息安全风险进行建模，使用建模打分，避免传统评估方式中可能存在的主观因素和不稳定性问题。同时该模型需要根据监管需求进行个性化模型参数配置，适应不同地区、不同类型机构的监管要求，提高监管效率和精准度。

(2) 信息安全合规风险监管

a. 合规监管态势

需结合信息安全监管评分，展示各组织机构整体合规风险度及合规评分趋势。

b. 合规监管覆盖面

需展示各组织机构内部应用数量，已实现相关合规监管应用数量。

c. 合规监管完成度概览

需展示各组织机构系统总体数量及已完成合规监管数量。

(3) 安全等保合规自动化评测

能够基于经验模型解构通用安全合规控制点，通过对安全运营数据的关联分析及逻辑映射。

a. 合规监管测评项目配置

需能够基于等级保护监管要求定制化配置合规监管评测项目。

b. 合规监管符合度配置

需基于安全监管评测各项目要求，对项目评测符合度情况进行配置。

c. 合规监管指标配置

需参照等级保护要求，基于各合规安全监管项目进行相关评测指标配置。

d. 一键等保合规自测

需基于等保评测模板，针对评测对象，实现等保项目一键自测，辅助管理人员对系统合规状态进行自我评测。

4.1.1.2 信息安全事件监管

基于现有软件平台的功能，完善安全监管场景的构建以及威胁建模和规则开发，主要侧重落实安全威胁监控能力，纳管范围包括管发中心和分支机构。

(1) 信息安全事件任务监管

以监管视角对安全运维的过程进行有效监管，结合监管要求，对分支机构的安全运营工作进行主动监管，结合安全监管数据，通过开发安全监管场景，自动生成安全监管任务计划。

a. 安全任务管理

需支持通过将所有安全任务进行分类、分配和跟踪，提高安全监管工作效率。

b. 事件任务监控

需支持通过建立任务管理体系，可以实时了解到安全监管事件任务的整体情况，从而能够及时应对最紧急，重要的安全问题。

(2) 信息安全威胁建模和规则优化

a. 告警事件压缩降噪

需支持对安全告警事件进行压缩，可通过策略规则，对安全告警进行降噪处理。

(3) 分支机构安全管理

a. 支机构安全管理界面

需设置分支机构安全管理界面，将监管考核要求拆解为分支机构的安全管理指标，支持分支机构安全管理界面，实现工作目标与安全监管目标相对应。

b. 安全管理考核指标

需支持建立分支机构的安全管理考核指标。

c. 数据对接

需支持各分支机构基于全流量探针、日志采集器、资产发现、威胁情报、漏洞库等方式的内容采集，数据采集、交互、抽取、数据管理等相关内容搭建安全管理中心，同时，支持数据传输保护、支持与一级监管平台的数据对接。

(4) 安全监管内部安全情报库

需支持通过自建内部情报库，形成包括：人员，账号，设备，网络地址等黑白名单内部情报，并通过平台实现内部情报界面化管理；支持提供情报收集功能，各级机构安全运维人员可以自己填写上报相关情报信息（黑白名单），徐汇区卫健委统一管理和审核。形成医疗卫生系统统一内部情报信息。

(5) 安全监管任务计划管理

结合安全监管数据，通过开发安全监管场景，自动生成安全监管任务计划。

a. 日常任务计划管理

需支持制定相关日常任务计划，明确任务责任人、边界、任务时间等内容，实现日常任务的管理。

b. 日常任务监管

需支持对监管流程事件形成任务计划，对流程进行计划跟踪，对未按时完成的流程任务进行提示。

c. 任务闭环监测

需支持对运营任务从发布、执行、处理等全过程进行闭环管理，实时监测任务进展情况。

(6) 信息安全监管联动

需支持对接入各分支机构的安全组织体系进行监管，建立徐汇区安全人员组织监管视图，安全事件处置流程化响应。支持医疗信息安全事件的应急响应机制，以快速响应和协同处置医疗信息安全事件。

(7) 医疗信息安全监管知识库

需建立医疗行业信息安全知识库，集中存储徐汇区医疗安全相关信息和资料，包括：已发布的信息安全政策、相关安全流程规范和操作指南，以及各种漏洞、攻击技术和威胁情报等信息，支持安全管理和监督，帮助安全人员快速掌握医疗卫生行业安全策略和标准，指导和支撑安全建设相关工作的任务。

a. 网络安全政策文件知识库

需建立网络安全政策文件知识库，包括国家、医疗行业两个维度，支持对网络安全相关政策文件的预览、下载等。

b. 安全能力技术资料知识库

需建立安全能力技术资料知识库，包括安全能力者、技术资料类型、安全能力分类三个维度，支持对安全能力技术资料的预览、下载等。

c. 自有知识库

需建立自有知识库，包括现有的信息安全管理制度、标准流程，支持对自有知识库文件的上传、预览、下载等。

(8) 监管工作信息通告管理

需将安全监管通告信息化，用于协调监管机构与被监管组织之间的沟通和合作，对监管部门发出的监管通告，自动形成安全任务工单流程，对通告内容及落实情况形成追踪反馈机制，实现安全监管通告的信息化管理。

a. 通告管理

需支持对监管通告的编写、发布和更新等功能，包括通告主题、内容、时间和范围等信息，并支持不同级别和类型的通告，提高通告的准确性和针对性。

b. 通告工单联络

需支持将通告转为监管任务工单，通过通告流程进行分发和处理工作，实现自动化的任务分配和流转，从而提高监管效率和准确性。

c. 通告反馈上报

需支持被监管分支组织对通告工单流程进行响应和反馈，包括相关措施的采取情况、隐患排查和整改计划等信息，便于监管机构了解企业或组织对通告要求的落实情况。

d. 历史通告查询

需实现历史通告查询和分析，包括已发布和已处理的通告记录，便于监管机构及时了解通告实施情况和效果。

(9) 设备资产漏洞事件监管

需对徐汇区各接入的分支机构卫生系统资产漏洞信息进行盘点，对发现的资产漏洞事件进行闭环监管，在漏洞对接，漏洞评估，漏洞修复，漏洞校验，漏洞关闭等阶段制定响应监管指标，实现漏洞管理全流程监管。

a. 资产库管理

从资产维度展示数字化资产的详细信息，需支持在此对资产进行新增、查看、修改、删除等操作。

b. 资产漏洞概览

需对全网资产存在漏洞的整体情况概览进行展示，支持下钻查看详情信息。

c. 单一资产漏洞统计

需对每个单一资产存在漏洞的情况进行统计监测，包括漏洞数量、漏洞名称、漏洞编号、漏洞级别、修复情况等。

d. 漏洞整改情况跟踪

需对全网资产可能存在的漏洞的整改情况进行动态跟踪管理。

(10)移动端安全事件监督管理

需支持移动端对信息安全监管工作台的访问。通过移动端告警推送和 H5 页面嵌入等方式，实现移动设备用户的安全事件监督和管理。

a. 移动端告警推送

将安全事件告警通告到安全负责人的微信，当出现安全事件时，系统自动推送告警信息给用户，包括事件类型、时间和地点等详细信息。

通过在公众号、小程序或其他移动端网页中嵌入安全事件监管的 H5 页面，向监管人员提供安全事件查询和处理等功能，使用户可以随时随地监管安全事件。

4.1.2 运行环境及性能要求

系统需要与采购单位现有“徐汇区卫生系统信息安全监管平台”集成，作为其功能的一部分。开发的代码需与安全监管平台系统兼容。

4.1.2.1 开发平台

开发平台为市场主流开发语言 Java、JavaScript。

4.1.2.2 服务器端及客户端运行平台

服务器端需支持 Ubuntu 20.04 LTS Server 及以上服务器版本操作系统。

终端通过 IE、Firefox、Chrome 等主流的浏览器访问信息安全监管平台，无需专用客户端。

4.1.2.3 性能要求

信息安全监管平台的性能主要关注响应时间及处理能力指标。在系统设计时，需要结合当前和将来预计接入的设备数量来测算事件量，同时对系统将来扩展能力要给予充分的考虑。本期项目对性能及容量要求如下：

(1) 同时支持 50 WEB-Client，用户登录时间小于 5 秒。

(2) 支持 15000 条/秒（EPS）的事件采集能力。

(3) 每日可处理及存储数据量不低于 500GB。

(4) 要求系统在线存储和脱机存储原始安全日志信息 2 个月、过滤后的日志信息保存六个月，应用（报表）数据至少存储 2 年。

(5) 查询性能 在 500GB 以下（含 500GB）的数据量中查询关键字并返回结果的时间不得超过 10 秒， 复杂搜索响应时间<60s。

**五、安全服务需求**

**5.1 整体安全管理服务需求**

5.1.1 服务说明

为管发中心提供为期 1 年的整体安全管理服务，本项目所涉及的安全管理服务内容包括：机房管理服务、IT 资产管理服务、运维工单管理服务、基础信息维护管理服务、安全策略及配置的维护管理、安全应急响应技术支持服务、重要时期保障服务、应急预案服务、安全培训服务、运维管理平台服务、信息系统综合监控预警平台、机房环境动力监测及信息安全咨询服务。

5.1.2 服务内容

5.1.2.1 机房管理服务

机房管理服务主要内容为备份存储、机房出入管理、供应商联系人管理、运维状态监控与预警服务。

- 服务要求

制定、检查、优化备份存储方案；

对人员、设备进出，各类操作、实施、调试等行为进行有效管理、记录，使所有的机房进出事件均留下合规化记录，完善机房运维规范，优化机房运维体系。

制定供应商（第三方）相关联系人清单，并及时更新完善并协助客户管理第三方。

提供运维状态监控分析与预警服务（含：CPU、内存、硬盘、网络等状态），并根据异常情况及时提供报警及处置。

- 服务指标

- 提供《管发中心机房管理记录》
- 提供《供应商联系人清单》
- 提供《事件记录》
- 5*8 现场服务

5.1.2.2IT 资产管理服务

为采购单位提供 IT 资产管理服务，依据 IT 资产和信息字体资产的全生命周期开展资产管理活动，使采购单位资产信息更精确。

- **服务要求**

对 IT 资产的出入库、贴标、整理、报废等环节做全生命周期的管理，帮助用户减少额外维护成本，最佳地使用许可证，减少未使用的资产和安全风险的数量，为审核做好准备，提高其 ITIL 流程效率，助力用户进行有效的购买决策，制定精确的预算等。

对信息系统资产实现全生命周期管理，完整记录信息系统资产入库、上架，经历使用中的维护、变更，到最终的下架、报废，呈现整个资产生命周期的所有节点及每条日志信息。

- **服务指标**

- 提供《资产管理清单》
- 5*8 现场服务

5.1.2.3 运维工单管理服务

对运维工单进行审核检查，确保其合规性与准确性，并定期根据工单数据汇总进行分析及优化建议。

- **服务要求**

部署工单管理系统，对运维工单进行审核检查，确保其合规性与准确性，并根据工单数据汇总进行分析及优化建议。

- **服务指标**

- 5*8 现场服务

5.1.2.4 基础信息维护管理服务

基础信息维护管理服务主要内容为梳理管发中心机房各类基础设备资产信息、梳理采购单位现有网络及安全设备资产信息、梳理网络及安全设备的策略。

- **服务要求**

提供梳理管发中心机房各类基础设备资产信息服务，对管发中心机房门禁、环境监控、消防、UPS、空调等设备进行统计梳理。

提供梳理设备资产信息及维护点位信息、拓扑图、机柜图、配置设备技术参数等信息系统基础信息，统计设备 IP 地址信息、设备型号、设备品牌等。确保整体基础信息的准确性和可追溯性。

对现有网络及安全设备的策略进行梳理，形成台账。

- **服务指标**

- 提供《IT 资产信息台账》
- 5*8 现场服务

5.1.2.5 安全策略及配置的维护管理

对采购单位所管理的各类安全设备进行安全策略及配置的维护管理，对各安全属性开展审计工作，并根据审计情况协助进行相应处置，确保安全设备监控、正常运行。

- **服务要求**

定期审核各类安全设备的 IOS 版本、特征库、病毒库等；

协助进行安全漏洞修补，加强安全配置、安全加固、处理确保安全设备在健康、可控并符合安全要求的前提下正常运行。

- **服务指标**

- 提供季度《安全设备审计报告》
- 5*8 响应服务

5.1.2.6 安全应急响应技术支持服务

保障采购单位在面对网络安全事件和业务安全风险问题时，开展应急响应工作，及时遏制风险，恢复单位安全。

- **服务要求**

在采购单位系统遭受网络攻击、病毒传播、黑客入侵等安全事件，业务中断、系统宕机、网络瘫痪、数据丢失、网页篡改等问题时，采取风险遏制措施和行动，对已经发生的安全事件进行监控、分析、协调、处理、保护资产安全属性。

- **服务指标**

- 提供《事件记录》
- 7*24 响应服务

5.1.2.7 重要时期保障服务

对采购单位所认定的重要时期提供保障服务，确保重要时期采购单位的网络安全及完成保障工作要求。

- **服务要求**

在重要时期协助采购单位完成安全保障工作。

- **服务指标**

- 7*24 现场值守

5.1.2.8 应急预案服务

识别应急事件场景，结合采购单位实际情况设计可行的应急预案。

- **服务要求**

对采购单位业务进行业务影响分析，识别可能发生的异常情况，并对异常情况，结合现有资源和能力手段设计可行的应急预案；

- **服务指标**

- 提供《应急预案》
- 5*8 响应服务

5.1.2.9 安全培训服务

结合法律法规和各类标准规范，定制适合采购单位的信息安全培训方案，以提升采购单位全员信息安全意识。

- **服务要求**

规范组织信息安全意识培训，至少组织 1 次信息安全意识培训，提升采购单位安全管理能力，保障组织信息安全，增强全员安全意识。

以理论讲解和讲师演示的方式，结合学员实际操练，加强学员对安全技术的认识。

- **服务指标**

- 提供《安全培训课件》
- 5*8 响应服务

5.1.2.10 运维管理平台服务

针对管发中心管理范围内的网络和信息系统，提供智慧型安全运维管理平台服务，为采购单位整体信息系统提供规范化管理部署并统一呈现，使数据实时、精准地汇总到本平台，对中心整体信息系统做规范化管理，实现对人，事，物的统一管理，以及对信息系统数据的统一呈现。

- **服务要求**

部署安全运维管理平台，使用统一的运维平台进行事件处理，故障报修，用统一的标准流程记录、处理、汇总事件数据。做到事件可追溯，紧密关联资产状态，支持事件状态随时查看，支持服务质量考核。实现采购单位的统一资产管理、统一运营管理、安全告警研判和安全处置，并实现威胁情报精准共享，为采购单位构建全面、有效的安全运维管理平台。

- **服务指标**

- 提供月度《安全运维分析报告》
- 7*24 响应服务

5.1.2.11 信息系统综合监控预警平台

信息系统综合监控预警平台，对采购单位信息基础设施，IT 基础架构，业务系统的运行情况进行监控，对异常状态进行预警，并分析。

- **服务要求**

通过预警平台工具，实现对基础设施，IT 基础架构，业务系统的运行情况进行监控，在业务系统中断前提前预警，给出准确的性能数据，实现故障与异常的实时发现与通知。并提供系统可用性状态报警及运维数据分析。

- **服务指标**

- 提供月度《运维分析报告》，含性能信息和运维数据分析等信息
- 7*24 自动监控预警服务

5.1.2.12 机房环境动力监测

通过监测工具对机房内能够支持统一监控的机房动环设备，并提供故障预警服务。

- **服务要求**

支持机房统一管理，对 UPS、空调等设备进行实时监控。多级的灵活阈值策略，实现动环设备故障前及时提醒，最大程度抑制故障发生。帮助运维管理人员随时掌握数据中心能效状况。支持多途径告警通知（声光、短信、邮件通知等）。

- **服务指标**

- 7*24 自动监控预警服务

5.1.2.13 信息系统咨询服务

通过源代码审计服务发现代码漏洞，并提供修订措施和安全建议，以提升采购单位应用系统的安全性。

- **服务要求**

帮助采购单位对信息安全制度流程进行审核，优化迭代；协助采购单位做好新场景的安全规范，合规化建议；

帮助采购单位进行信息化项目的可行性研究，方案制定，方案审核，及实施跟踪；

提供信息安全建设中涉及的决策、管理及运行操作问题的专业咨询；

为信息化工作提供建设性建议和报告。

- **服务指标**

- 提供不少于 1 次信息安全咨询服务，出具《信息化工作建议和报告》
- 5*8 响应服务

5.1.3 服务人员要求

服务周期内，选派在项目服务方面富有经验的团队人员负责本项目，项目团队服务人员数量不少于 2 人：其中负责人 1 名、小组成员不少于 1 名。

（1）负责人

本科及以上学历，具有国家工信部颁发的信息系统项目管理师证书。投标文件需提供有效证书扫描件和在投标人单位最近一个季度某一月份的社保缴纳证明。

（2）小组成员

具有信息安全专业技能以及相关从业经验。需提供有效证书扫描件和在投标人单位最近一个季度某一月份的社保缴纳证明。

5.1.4 工作量清单

| 序号 | 服务项名称 | 数量 | 单位 |
|---|---|---|---|
| 1 | 整体安全管理服务 | 1 | 项 |

**5.2 安全运营维护服务需求**

5.2.1 服务说明

需要投标人提供徐汇区中心医院为期 1 年的安全运营服务。

5.2.2 服务内容

包括三级等保建设咨询、漏洞扫描、渗透测试、安全事件应急响应及信息安全培训服务。

5.2.2.1 三级等保建设咨询

充分解读信息系统等级保护相关政策和标准，提供 1 次三级等保咨询服务，从定级、备案、整改、测试、监督检查五个规定流程上提供咨询支持，帮助用户单位达到等级保护的测试要求，降低安全风险。

需要交付《备案表》及《定级报告》

5.2.2.2 漏洞扫描

为徐汇区中心医院提供 1 年 12 次的定期漏洞扫描服务。覆盖用户指定的业务系统，不限数量，漏洞复测不限次数。要求漏洞扫描不能影响系统正常运行，不能在扫描中存在传播木马，病毒，拷贝、删除文件，修改文件等行为。并提交《漏洞扫描服务报告》。扫描内容主要包括以下 2 项：

1、 系统安全扫描：针对系统主机（操作系统）、网络设备、虚拟化平台等进行漏洞扫描，检测系统、协议的漏洞和补丁情况等，在漏洞被利用前给出安全隐患评估报告和修复建议。

2、 数据库安全扫描：针对 Oracle、Sybanse、SQL Server、DB2、MySql、Postgres、informinx 等主流关系型数据库进行安全漏洞检测，主动发现数据库是否存在安全漏洞，提醒客户及时更新补丁。

5.2.2.3 渗透测试

为徐汇区中心医院提供 1 年 2 次的渗透测试服务并交付《渗透测试服务报告》渗透测试内容主要包括以下 2 项：

1、 WEB 安全扫描：针对 SQL 注入、XSS 跨站脚本、信息泄露、网络爬虫、目录遍历等 WEB 攻击进行模拟黑客渗透攻击测试，评估网站的安全性。

2、 弱口令探测：根据检测工具内置的口令字典，对内网系统及应用的账户和密码进行探测，测试系统、设备、数据库、WEB 是否存在弱口令。

5.2.2.4 安全事件应急响应

在 1 年服务期限内，提供 7*24 小时安全事件应急响应服务。如发生安全事件，在接到用户的安全事件响应请求后，2 小时内到达现场，分析安全事件，并提交《安全事件响应报告》，给出安全事件的详细分析及抑制处理的方式、方法、流程等建议。并在用户授权的情况下进行处理安全事件的操作。

5.2.2.5 信息安全培训

定期开展对用户相关人员的安全培训服务，包含安全意识培训，安全技能培训，满足信息安全等保（三级）要求。安全培训 1 年提供 2 次，并交付安全培训课件等培训相关资料。

5.2.3 服务人员要求

服务周期内，选派在项目服务方面富有经验的团队人员负责本项目，项目团队服务人

员数量不少于 2 人：其中负责人 1 名、小组成员不少于 1 名。

（1）负责人

本科及以上学历，具有国家工信部颁发的信息系统项目管理师证书。投标文件需提供有效证书扫描件和在投标人单位最近一个季度某一月份的社保缴纳证明。

（2）小组成员

具有信息安全专业技能以及相关从业经验。需提供有效证书扫描件和在投标人单位最近一个季度某一月份的社保缴纳证明。

5.2.4 工作量清单

| 序号 | 服务项名称 | 数量 | 单位 |
|---|---|---|---|
| 1 | 安全运营维护服务 | 1 | 项 |

注：1、根据上海市财政局沪财库[2009]19 号“关于落实政府采购优先购买福利企业产品和服务的通知”要求，本项目在同等条件下优先采购福利企业的产品和服务。同时项目采购应当符合采购价格低于市场平均价格、采购质量优良和服务良好的要求。

2、本项目中各子系统间的同类产品尽可能使用同一品牌。

3、为完成本项目而配置的各类线缆、附件、配件的品牌、规格、数量、报价均应在附表中予以明确填报，计算务必完整，准确。采购方不因投标单位对此项的计算遗漏或其他因素而支付任何额外费用。

4、以上技术规范要求作为本项目参考技术要求，投标单位在深化设计方案制作中应注意补充增加，技术方案解释力求完整，完善并进一步深化。以上技术参数的未列项并不表示采购方以及采购单位放弃对此项技术指标的要求。

5、投标人应根据采购要求进行系统的深化设计，提供系统整体解决方案。系统各子模块功能无法一一列出，项目实施过程中需根据实际需求调研后对各子模块功能进行增加及修改，此类费用投标人应计入本次报价，今后采购人不再予以支付。

**六、项目人员要求**

为保障项目按计划正常开展，投标人在组织项目组成员时，应满足如下要求：

项目经理：应具有一级建造师及信息系统项目管理师资质证书、具有 10 年以上项目相关工作经验；具有医疗行业信息系统项目管理经验且担任过类似信息化项目的项目经理优先考虑；具备调动公司内部完成项目建设所需各项资源的能力，且在项目实施过程中，不能兼任其他项目。

核心技术负责人：应具有高级工程师、具有 10 年以上项目相关工作经验；具有医疗行

业信息系统项目规划设计经验且担任过类似信息化项目的规划设计的技术负责人优先考虑；具备对各类设备的规划设计能力并负责实施阶段中的具体方案设计；在项目实施过程中，不能兼任其他项目。

技术工程师：应具有人社部门颁发的高级工程师证书；具有医疗行业信息系统项目实施经验且担任过类似信息化项目的工程师优先考虑；具备熟练掌握相关设备配置部署的能力，且在项目实施过程中，不能兼任其他项目。

信息安全工程师：应具有中国信息安全测评中心颁发的注册信息安全专业人员资质证书；具有医疗行业信息系统项目规划设计经验且担任过类似信息化项目的规划设计的安全工程师优先考虑；具备对项目实施过程中的各项设计及各个安全设备的安全配置进行整体把控的能力；确保项目设计满足对信息安全的要求。在项目实施过程中，不能兼任其他项目。

投标人应详细列出项目实施团队人员姓名、相关认证资质、项目经验等并提供证明材料。在项目启动后，如需更换项目组人员，需与采购单位及监理单位协商并获得书面同意。如中标方提供的项目组人员态度与能力不符合项目要求，采购单位有权提出更换人员，中标方必须在 10 个工作日内解决，并对此而延误的项目工期负责。

**七、项目实施要求**

（一）安装和调试

**中标方须在合同签订后的 8 个月内完成本项目硬件集成及软件开发工作验收交付，**服务类采购内容提供为期 1 年的整体安全管理服务。投标人所提供的设备及其内部连线全部由投标人负责。投标人负责投标人设备之间线缆的布放以及投标人设备与买方已有相关设备之间的线缆布放。投标人负责对施工地点进行现场勘察，保证施工进行。安装调测时使用的工具、设备由投标人提供，通用工具由买方协助解决。双方应协商制定工程进度表，投标人负责按工程进度表进行施工。设备调试由投标人负责，并提出设备调试的内容、项目、指标和方法，并提供相应的仪器和工具，投标人有责任对买方的技术人员提出的问题作出解答。调试应进行详细记录，试运行 3 个月后进行最终验收，由投标人技术人员签字后交给买方验收。系统测试的条款应与技术规范一致。基于以上要求，投标人应提供测试条件、方法和过程的草案，招标以后，最终测试文件由双方共同拟定。

（二）验收

设备运抵安装现场后，买方将与中标人共同开箱验收。验收时发现短缺、破损，买方有权要求中标人立即补发和负责更换。同时中标人应提供必备的技术资料：

（1）相关的技术资料（测试报告、产品合格证书、保修卡等）；

（2）提供机房设备安装布置图及电气线路图和主要部件的技术性能参数（列出清单）；

（3）提供设备保养、维修操作规程；

（4）提供系统特殊件及配套件的清单、技术参数；

（5）进口设备应提供由独立的商检机构开具的所有设备的原产地证明。

设备安装、调试达到技术规范书规定的指标并正常运行 5 个工作日后，可进行系统验收测试。验收规范(包括项目、指标、方式和测试仪器等)应由中标人提交给买方。买方可根据合同及技术规范书进行修改和补充，经双方确认后形成验收文件作为验收依据。验收测试合格后，双方签署验收协议。

（6）软件产品开发验收要求：验收条件：1、项目全部建设内容，已按合同全部建成，能满足运行的需要；2、完成第三方软件测评；3、试运行无重大缺陷、无重大故障且试运行期间产生的所有问题都已得到解决；4、提供安全测评报告（软件安全功能满足等保三级要求）；5、项目文件资料齐全，并符合相关规定。验收标准及要求：双方签署最终验收文件时，投标人应提交规范、全套、完整的验收文档，包括但不限于需求分析报告、概要设计说明书、详细设计说明书、程序安装维护手册、使用手册、软件维护手册、系统上线实施手册，系统测试计划、系统测试报告、数据备份方案，技术手册、配置、管理及维护的全面技术资料，以及所有与用户、设备等相关联的说明、表格等资料文档，并有责任帮助整理、装订、归档。

（三）保修期

保修期，从初验完成之后开始计算，保修时间由投标方投标时明确。在保修期内，投标人应提供 7×24 小时电话或电子邮件响应服务，故障响应时间不超过 30 分钟。对于电话方式无法解决的问题，必须在 2 小时之内派员到现场维护并恢复系统正常运行，并根据实际需求修复或更换相应的硬件，由此发生的全部费用由投标人负责。**本项目产品及系统质量保修期不得低于 3 年，软件保修期不得低于 1 年。**设备开通后,，如发生软件升级及设备升级、扩展等有关情况，中标人应向买方提供必要的技术资料，并免费提供软件升级。保修期后，中标人应对其提供的设备提供终身技术支持（终身技术支持是指系统过保后，投标公司有能力免费提供终身的技术咨询服务，并以最优惠的价格提供续保服务）。**如项目质量保修期不满足招标文件要求的作无效投标处理。**

（四）技术服务

（1）投标人应说明工程技术维护队伍和机构情况，服务模式。

（2）投标人应提供设备安装调试时所需的工程设计资料，投标人有责任在保证安全和质量的前提下提供技术服务，包括技术咨询等。

（3）在设备安装和系统调测期间，买方派出技术人员参加，中标人有义务对其进行指导。

（4）网络运行后，中标人如对系统软件有所改进、增加新功能，均应免费提供买方使用。

（5）网络试运行后一周内，中标人应提供技术人员驻现场保障，以保证系统运行稳定，随时解决技术故障和操作疑问。

（6）在设备扩容及软件升级时，中标人应派技术人员到场指导。

（7）中标人应对其在国内的售后服务、技术支持方面、在上海市有无技术支持中心，固定地点等情况作出说明。

（8）在设备发生故障的情况下,投标人承诺在多长时间内赶赴现场，承诺在多长时间内排除故障。

（9）投标人应承诺能向买方保证提供相应设备的备品备件，当设备出现故障时，能及时更换坏掉的设备，保证整个系统的可用性。

（10）在系统设备运行期间，根据需要中标人有责任派技术人员按招标需要随时到现场指导维护工作。

（五）技术培训

中标人应负责采购单位人员的技术培训工作，保证其达到独立上岗操作与日常维护的水平。须在投标时提供相关培训方案计划，计划包括培训项目、人数、地点、日程、资料、培训讲师等详细内容。

（六）技术文件

中标人提供的书面技术资料应能满足确保系统正常运行所需的管理、运营及维护有关的全套文件。中标人提供的技术文件至少应包括：

（1）系统说明文件；

（2）技术手册(安装、测试、操作、维护、故障排除等)；

（3）用户使用手册；

（4）软件资料。

**八、其他要求**

1、投标报价要求：本项目为交钥匙工程。投标人必须对以上全部采购内容及相关服务进行报价，报价中应包含产品采购、安装到位、软件开发部署、测试、系统安装集成、各类服务提供、免费维护费用、验收合格、相关培训等伴随服务等全部明细内容，并将与本

项目有关的其他所有费用全部计入投标报价，采购人不再承担其他任何费用。

2、各服务项按招标文件要求的服务周期提供相应服务。请投标单位根据用户方需求自报项目实施周期，并制作详细实施周期及施工组织方案、人员安排等质量、安全、工期保障措施，以确保项目按期完工。

3、中标单位与采购人应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，采购人应当按照《徐汇区政府采购货物、服务项目合同履约验收管理办法》相关规定进行验收管理和支付相应合同价款，中标单位有义务参加并协助采购人验收，提供相关技术资料、合格证明等文件或材料，并对自己生产或销售的货物质量或提供的服务负责。验收书要求见附件。

4、如中标供应商实际供货产品与投标产品不一致，送货服务承诺无法完成，产品质量、服务被使用方有效投诉，经查实中标供应商要承担相应违约责任，并将按《徐汇区政府采购供应商诚信档案管理（暂行）办法》规定进行相应记载和处理，同时保留向市、区政府采购管理机构通报的权利。

# 第四部分 合 同 参 考 范 本

**包 1 合同模板：**

# [合同中心-合同名称]

**合同统一编号：** [合同中心-合同编码]

**合同内部编号：**

合同各方：

甲方：**[合同中心-采购单位名称]**
地址：**[合同中心-采购单位所在地]**
电话：**[合同中心-采购单位联系人电话]**
联系人：**[合同中心-采购单位联系人]**

乙方：**[合同中心-供应商名称]**
地址：**[合同中心-供应商所在地]**
电话：**[合同中心-供应商联系人电话]**
联系人：**[合同中心-供应商联系人]**

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

**1．乙方根据本合同的规定向甲方提供以下服务：**

1．1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见招标文件和投标文件。

**2. 合同价格、服务地点和服务期限**

2．1 合同价格

本合同价格为[合同中心-合同总价]元，人民币大写 [合同中心-合同总价大写]元。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 服务地点

2．3 服务期限

本服务的服务期限：起至。

**3．质量标准和要求**

3．1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

**4．权利瑕疵担保**

4．1 乙方保证对其交付的服务享有合法的权利。

4．2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4．3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。

4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

**5．验收**

5．1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

5．3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

5．4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

**6．保密**

6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

**7．付款**

7．1 本合同以人民币付款（单位：元）。

7．2 本合同款项按照以下方式支付。

项目付款方式为：甲乙双方约定按进度支付款项。

**8．甲方（甲方）的权利义务**

8．1、甲方有权在合同规定的范围内享受服务，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8．5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8． 6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的，应与乙方协商解决。

**9．乙方的权利与义务**

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9．4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9．8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

**10．补救措施和索赔**

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

**11．履约延误**

11．1 乙方应按照合同规定的时间、地点提供服务。

11．2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

**12．误期赔偿**

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

**13．不可抗力**

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

**14．履约保证金**

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为元人民币的履约保证金。履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

**15．争端的解决**

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，属于政府集中采购的项目，可以向徐汇区政府采购管理办公室提请调解。如果经调解不能达成协议，则在买方住所地有管辖权的人民法院提起诉讼。在诉讼期间，除了必须在诉讼过程中进行解决的那部分问题外，合同其余部分应继续履行。

**16．违约终止合同**

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

**17．破产终止合同**

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

**18．合同转让和分包**

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

**19．合同生效**

19．1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式叁份，以中文书就，签字各方各执一份，一份报徐汇区政府采购管理办公室备案。

19．3 合同有效期：[合同中心-合同有效期]

**20．合同附件**

20．1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20．2 本合同附件与合同具有同等效力。

20．3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

**21．合同修改**

21．1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）：

法定代表人或授权委托人（签章）：

日期：[合同中心-签订时间]

乙方（盖章）：

法定代表人或授权委托人（签章）：

日期：[合同中心-签订时间]

合同签订点:网上签约

# 第五部分 投标文件格式

投标文件格式详见网上招投标系统相关附件

## 附件 1 投标函

徐汇区政府采购中心：

_____（投标人全称）授权_____（投标人代表姓名）(职务、职称)为我方代表，参加贵方组织的_____(项目名称、项目编号、包号)招标的有关活动，并对此项目进行投标。为此：

1、我方同意在本项目招标文件中规定的开标日起 90 天内遵守本函中的承诺且在此期限期满之前均具有约束力。

2、我方按招标文件规定提供交付的的区域网络安全和硬件续建的投标总价为_____（大写）元人民币。

3、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的条件：

（1）具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

（2）具有《电子与智能化工程专业承包资质》一级资质（电子资质证书应为有效使用件）；

（3）本项目不允许联合投标。

4、我方已充分考虑到投标期间网上投标会发生的故障和风险，并对发生的任何故障和风险造成投标内容不一致或利益受损或投标失败，承担全部责任。

5、我方同意网上投标内容均以网上投标系统开标时的开标记录表内容为准，投标人的授权代表将在开标记录上签名以确认开标过程和结果，如果不签字，则由我们承担全部责任。

6、保证遵守招标文件的规定，忠实地执行双方所签订的合同，并承担合同规定的责任和义务。

7、如果在开标后规定的投标有效期内撤回投标，我方的投标保证金可被贵方没收。

8、我方完全理解贵方不一定接受最低价的投标或收到的任何投标。

9、我方愿意向贵方提供任何与本项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

10、我方已详细审核全部投标文件，包括投标文件修改书（如有的话）、参考资料及有关附件，确认无误。

11、我方承诺：采购中心若需追加采购本项目招标文件所列货物及相关服务的，在不改变

合同其他实质性条款的前提下，按相同或更优惠的折扣保证供货。

12、我方承诺接受招标文件中《中标合同》的全部条款且无任何异议。

13、我方将严格遵守《中华人民共和国政府采购法》的有关规定，若有下列情形之一的，将被处以采购金额 5‰以上 10‰以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动；有违法所得的，并处没收违法所得；情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

（1）提供虚假材料谋取中标、成交的；

（2）采取不正当手段诋毁、排挤其他供应商的；

（3）与采购人、其它供应商或者采购中心工作人员恶意串通的；

（4）向采购人、采购中心工作人员行贿或者提供其他不正当利益的；

（5）未经监管部门同意，在采购过程中与采购人进行协商谈判的；

（6）拒绝有关部门监督检查或提供虚假情况的。

与本投标有关的一切往来通讯请寄：

地址：_____

邮编：_____

电话：_____

传真：_____

投标人代表姓名：_____

投标人代表联系电话，e-mail：_____

投标人(公章)：

投标人代表(签字)：

日　期：

# 开标一览表

投标人（公章）：

投标人代表(签字)：

填写日期：

**上海市徐汇区政府采购中心——上海市徐汇区卫生健康委员会 2023 年区域网络安全和硬件续建政府采购项目包 1**

| 项目名称 | 产品及系统保修期 | 软件保修期 | 最终报价(总价、元) |
|---|---|---|---|
| | | | |

注：（1）所有价格均系用人民币表示，单位为元，保留到整数位。

（2）投标人应按照招标文件中有关投标报价要求进行报价，一旦中标不再调整。

（3）开标一览表内容与投标文件其它部分内容不一致时以开标一览表内容为准。

**附件 2-1 产品及系统集成投标报价明细表（按子系统分别填写）**

投标人（公章）：_____ 招标编号：_____ 价格单位：人民币元

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 货物名称 | 品牌 | 规格型号 | 产地 | 厂家 | 数量 | 设备单价 | 设备合价 | 技术服务费 | 安装费 | 其他服务费 | 分项合价 |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| 投标总价： | | | | | | | | | | | |

注： 1. 投标报价要求见招标文件的“投标人须知”相关要求。

2. 表中同一行中的第 8 栏数据＝第 6 栏数据×第 7 栏数据。

3. 表中第 9 栏、第 10 栏费用应根据招标文件的“投标人须知”相关要求列明细表。

4. 表中同一行中的第 12 数据＝第 8～第 11 栏数据之和。

5. 表中的“投标总价”＝Σ（第 12 栏的数据）。

6. 表中第 11 栏的费用如果有时，应注明具体内容。

**7、投标人必须按要求填报本明细表，否则会影响对投标文件的评判。**

投标人代表签名：_____ 日期：_____

**附件 2-2 软件开发投标报价明细表（明细内容根据实际工作内容自行填报，按子系统填写）**

| 内容 | 开发周期（天） | 开发人员（人数） | 开发工作量（人数） | 价格 |
|---|---|---|---|---|
| 一、系统建设方案 | | | | |
| 1、需求分析及架构、系统规划 | | | | |
| 2、系统详细设计 | | | | |
| …… | | | | |
| 二、功能模块开发 | | | | |
| 1、 | | | | |
| 2、 | | | | |
| 3、 | | | | |
| 4、 | | | | |
| …… | | | | |
| 三、其它费用 | | | | |
| | | | | |
| | | | | |

注：**上述投标报价内容明细表仅供参考，请各投标供货商根据自身情况按具体投标内容进行费用明细分解。**

投标人代表签字：_____

投标人（公章）：_____

日期：_____年 _____月____日

**附件 2-3 其他服务项报价明细表**

填报单位（公章）：　　第　页 共　页

| 序号 | 分类名称 | 费用（元） | 备注 |
|---|---|---|---|
| 1 | 整体安全管理服务 | | 详见明细（ ） |
| 2 | 安全运营维护服务 | | 详见明细（ ） |
| …… | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| **报价合计** | | | |

注：（1）所有价格均系用人民币表示，单位为元，保留到整数位。

（2）投标人应根据分类报价费用情况编制明细费用表并随本表一起提供。

（3）分项目明细报价合计应与开标一览表报价相等。

投标人代表签字：

投标人（公章）：

日期：　　年　　月

**附件 3　产品安装调试集成费报价明细表（如有，按子系统分别填写）**

价格单位：人民币元

| 序号 | 名称 | 品牌 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| 安装集成费总价 | | | | | |

注：　1. **本合同为闭口的总包价格.**

2. 投标要求见招标文件文件的“投标人须知”相关要求。

3. 表中的“安装集成费总价”＝Σ（系统设备的安装集成费合价）。

投标人代表签字：

投标人（公章）：

日期：　　年　　月　　日

**附件 4 产品选型及说明一览表（按子系统分别填写）**

| 序号 | 产品名称 | 型号规格及<br>主要技术参数 | 产地 | 数量 | 性能说明 | 备注 |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

注：各产品材质、详细技术参数表（请供应商也可根据自身情况调整列表予以说明），请供应商务必详细描述，如描述不清，将会影响到对投标文件的评判，请供应商充分重视。

投标人代表签字：

投标人（公章）：

日期：　　年　　月　　日

**附件 5 产品规格、技术参数偏离表（可根据实际情况自行设计表式填报）**

| 序号 | 产品名称及规格型号 | 数量 | 产地 | 招标产品配置要求 | 投标产品对应配置 | 偏差 | 备注 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**说明：1、投标人必须根据技术需求表来填写本表，如投标产品实际技术规格与技术需求无偏差，在“偏离”一列填写“无”。**

2、投标产品的规格、技术参数和性能与招标文件的要求如不完全一致，在“偏离”一列填写“有”，还需填写偏差说明，并注明是“正偏离”还是“负偏离”以及偏差的幅度（以百分比表示）。

投标单位（盖章）：

投标人代表签名：_____

日　期：_____

# 附件 6 法定代表人证明书和法人代表委托书

**法定代表人证明书**

_____先生/女士现担任_____职务，负责全面工作，为我单位的法定代表人。

特此证明。

投标人全称：_____

公章（盖章）：

_____年_____月_____日

**法人代表委托书**

兹委托_____先生/女士全权代理_____（招标项目和招标编号）政府采购招标项目的招标投标工作。

特此证明。

投标人法定代表人姓名（印刷体）：_____

投标人法定代表人签字、盖章：_____

公章（盖章）：

_____年_____月_____日

**附件 7-1　拟从事本项目实施人员及其技术资格一览表**

**人　员　名　册**

填报单位：　　第　页 共　页

| 序号 | 姓　名 | 出生年月 | 性别 | 学历 | 职称等级 | 相关认证资格 | 专业经历 | 成功案例 | 拟从事岗位 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

注：

1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。

2、**我方承诺以上人员均为本单位职工，并按时交纳四金。**并提供项目组人员身份证及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。

3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字)：

填写日期：

**附件 7-2　拟从事本项目软件开发人员及其技术资格一览表**

**人　员　名　册**

| 序号 | 姓　名 | 出生年月 | 性别 | 学历 | 职称等级 | 相关认证资格 | 行业工作年限和经验 | 成功案例 | 拟从事岗位 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

注：

1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。

2、**我方承诺以上人员均为本单位职工，并按时交纳四金。**并提供项目组人员身份证及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。

3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字)：

填写日期：

**附件 7-3 拟投入项目的服务人员配备及相关工作经历、资质汇总表**

**项目名称：**

| 序号 | 姓　名 | 出生年月 | 性别 | 学历 | 职称等级 | 相关认证资格 | 专业经历 | 成功案例 | 拟从事岗位 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

注：

1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。

2、**我方承诺以上人员均为本单位职工，并按时交纳四金。**并提供项目组人员身份证及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。

3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字)：

填写日期：

**附件 7-4 项目经理说明表**

| 姓名 | | 出生年月 | | 文化程度 | | 毕业时间 | |
|---|---|---|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 资格证书 | | 技术职称 | | |
| 获得证书时间 | | 聘任时间 | | |
| 从业年限 | | 进入本公司时间 | | |

主要工作经历：（包括起止年限、单位名称、从事的工作内容、证明人、证明人联系电话）

2020 年以来相关项目服务情况

| 序号 | 项目名称 | 参与时间 | 项目预算金额（万元） | 参与项目的角色 | 所附证明材料页码 |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| … | | | | | |

**注：我方承诺以上人员均为本单位职工，并按时交纳四金。并提供以上人员身份证及相关学历、资格证书、工作履历、业绩证明等证明材料复印件，并加盖单位公章。**

投标人（公章）：

投标人代表(签字)：

填写日期：

## 附件 7-5　软件开发、安全服务项目组成员的详细情况表（每人一表）

| 姓名 | | 出生年月 | | 文化程度 | | 毕业时间 | |
|---|---|---|---|---|---|---|---|
| 资格证书 | | | | 技术职称 | | | |
| 获得证书时间 | | | | 聘任时间 | | | |
| 从业年限 | | | | 进入本公司时间 | | | |
| 主要工作经历：（包括起止年限、单位名称、从事的工作内容、证明人、证明人联系电话） | | | | | | | |
| 2020 年以来相关服务情况 | | | | | | | |
| 序号 | 项目名称 | 参与时间 | 项目预算金额(万元) | 参与项目的角色 | 所附证明材料页码 | | |
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| … | | | | | | | |

**注：我方承诺以上人员均为本单位职工，并按时交纳四金。并提供以上人员身份证及相关资格证书、工作履历、业绩证明等证明材料复印件，并加盖单位公章。**

投标人（公章）：

投标人代表(签字)：

填写日期：

附件 8　规章制度一览表

| 序号 | 规章制度名称 | 执行起始时间 | 备注 |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| … | | | |
| … | | | |
| | | | |
| | | | |
| | | | |
| | | | |

各规章制度的具体内容另行提供。

投标人代表签字：_____

投标人（公章）：_____

日期：　　年　　月　　日

**附件 9　供应商行贿犯罪记录承诺书**

上海市徐汇区政府采购中心：

_____（投标供应商全称）现参与你单位组织的_____政府采购项目，并承诺本公司根据《上海市政府采购供应商登记及诚信管理办法》已申请加入上海市政府采购供应商库，且在 3 年内无行贿犯罪行为记录。

投标供应商全称：_____

公章（盖章）：

法定代表人签字、盖章：_____

**附件 10　中小企业声明函（服务）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称），属于软件和信息技术服务行业；承接企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于软件和信息技术服务行业；承接企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

注：各行业划型标准：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

附件 11 投标人近三年来已承接的主要类似项目一览表

| 序号 | 年份 | 项目名称 | 合同金额 | 业主情况 | | | 项目主要内容 |
|---|---|---|---|---|---|---|---|
| | | | | 单位名称 | 经办人 | 联系方式 | |
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| … | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

注： 1、如在本表格不能全部填写完，可按此表格格式自行制表填写。
2、提供相应采购项目合同复印件，加盖单位公章。

投标人代表签字：

投标人（公章）：

日期： 年 月 日

## 附件 12 财务状况及税收、社会保障资金缴纳情况声明函

我方（供应商名称）参加（单位名称）的（项目名称）采购活动，符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括:

1.具有健全的财务会计制度;

2.有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期:

# 附件 13 投标单位基本情况表及声明

（一）名称及其他资料：

1、单位名称：

2、地址：

3、邮编：

4、电话/传真：

5、工商注册日期：

6、企业类型：

7、注册资本：

8、法定代表人或执行事务负责人姓名：

9、人员情况

从业人员数

专业技术人数

（二）主要财务指标（2022 年 1 月 1 日至 2022 年 12 月 31 日）**并请如实另附单位财务状况报告，依法缴纳税收和社会保障资金的相关材料**

① 业务收入：_____

② 风险基金额：_____

③ 资产净值：_____

（三）**参加政府采购活动前三年内在经营活动中没有重大违法记录的声明：（请如实填写）**

上海市徐汇区政府采购中心：

按照政府采购法实施条例要求，我单位郑重声明：我单位参与_____政府采购项目，在参加本项目政府采购活动前三年内在经营活动中**（没有/有）**重大违法记录。特此声明。

就我方全部所知，兹证明上述声明是真实、准确的，并已提供了全部现有资料和数据，我方同意根据招标方要求出示文件予以证实。

投标单位（公章）：

投标人代表(签字)：

填写日期：

## 附件：上海市徐汇区政府采购项目验收书（服务类）

供应商：　　采购单位：

<table>
<tr><td>采购编号</td><td colspan="2">采购项目</td><td>金额（元）</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">项目金额合计</td><td></td></tr>
<tr><td colspan="4">验收内容</td></tr>
<tr><td rowspan="6">一、规章制度</td><td colspan="2">1、人员管理</td><td></td></tr>
<tr><td colspan="2">2、设备运维</td><td></td></tr>
<tr><td colspan="2">3、服务管理</td><td></td></tr>
<tr><td colspan="2">4、应急管理</td><td></td></tr>
<tr><td colspan="2">……</td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td rowspan="6">二、运行记录</td><td colspan="2">1、人员上岗及培训</td><td></td></tr>
<tr><td colspan="2">2、设备检测记录</td><td></td></tr>
<tr><td colspan="2">3、巡更记录</td><td></td></tr>
<tr><td colspan="2">4、内审记录</td><td></td></tr>
<tr><td colspan="2">……</td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td>三、现场实地检查情况</td><td colspan="3"></td></tr>
</table>

<table>
<tr><td rowspan="3">验收<br>意见</td><td colspan="2">验收小组意见：<br><br>结论：该服务采购项目验收合格（或不合格）。</td></tr>
<tr><td colspan="2">验收小组签字：<br>组长：<br>组员：<br><br>年　月　日</td></tr>
<tr><td>供应商盖章：</td><td>采购单位盖章：</td></tr>
</table>

备注：1、采购人须按照《徐汇区政府采购货物、服务项目合同履约验收管理办法》第三章第十条“验收的基本程序”组织验收。2、政府向社会公众提供的公共服务项目（包括：以物为对象的公共服务，如公共设施管理服务、环境服务、专业技术服务等；以人为对象的公共服务，如教育、医疗卫生和社会服务等），验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告。3、该表式仅供参考。

**第六部分**

**上海市徐汇区卫生健康委员会 2023 年区域网络安全和硬件续建项目**

**政府采购招标评标办法**

一、评标依据：

1、评标办法系本着公开、公平、公正的原则，按照《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》制定，作为本次采购招标选定中标单位的依据。本次采购招标采用“综合评分法”评标，根据评标细则规定的评分标准对所有投标单位的有效投标文件进行评议，各评标项目累计总分为 100 分。

2、评标委员会由专家和采购单位代表组成，对各投标单位的投标报价进行甄别并经算术修正后得出各投标报价的得分，最终结果取算术平均值。

**3、评标委员会依据投标文件评分结果汇总后，对各投标单位的得分按由高到低的顺序依次排列，得出相应名次，得分最高的投标单位作为本项目中标单位。如出现最高得分并列情况时，则取投标报价较低者作为中标单位,如出现最高得分并列且报价相同则由评标委员会以投票表决方式，得票最多者为中标单位。采购人授权评标委员会在投标供应商中直接确定本项目中标单位。**

二、评标规则：

（1）参加评标的专家为上海市政府采购咨询专家库中的专家，并在评标前按规定程序产生。

（2）任何人不得干预评标委员会成员的评审权利，评审表要保存备查。

（3）评标委员会成员必须对所有投标单位作出评审。

三、“综合评分法”评标细则

**1、报价（20 分）采用低价优先法计算**

（1）首先确定评标基准价：经评标委员会甄别确认，满足招标文件要求且投标价格最低的投标报价为评标基准价，其报价分为满分 20 分。

（2）确定其他投标报价分：计算公式为投标报价得分=评标基准价/打分投标单位的投标报价×20%×100。

注：①经评标委员会评审如投标单位的服务内容不能满足招标文件要求，该投标将不列入评审范围，其报价如为最低投标报价，将不作为评标基准价。②如果评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的投标报价,有可能影响产品质量或不能诚信履约的,将要求该投标人作书面说明并提供相关证明材料。投标人不能证明其报价合理性的,评标委员会应将其作无效投标处理。

**2、产品性能及质量（20-32 分）**

评审内容：投标人提供的各类产品性能及质量优劣情况。评审标准：投标响应的各类产品性能好、性价比高、产品成熟可靠、品牌知名度和市场占有率高、产品选型与配置好、品牌一致性强等情况进行综合评审。打分区间可根据主观评判划分为（32-28 分）、（28-24 分）、（24-20

分）三档。

**3、各项服务项服务方案（4-10 分）**

评审内容：投标人提供的相关本项目系统功能模块设计开发等情况及各项服务方案。评审标准：软件开发功能模块符合完整、系统可靠安全、系统设计原型或系统截图契合度高；对各项安全服务需求理解、分析到位，相关服务流程、方法，人力、物力、技术力量的投入情况，相关应急预案、成果提交方式、考核验收方案等的针对性、可操作性、合理性、安全性、先进性和高保障性等情况进行综合评审。打分区间可根据主观评判划分为（10-8 分）、（8-5 分）、（5-4 分）三档。

**4、项目技术支持力度（4-10 分）**

评审内容：投标人提供的项目实施人员配备等情况。评审标准：从事本项目各项实施服务等技术支持服务人员的配备数量充足、类似项目服务的业绩证明材料齐全、工作经历丰富、工作能力强等情况进行综合评审。打分区间可根据主观评判划分为（10-8 分）、（8-5 分）、（5-4 分）三档。

**5、项目实施计划及组织管理（4-10 分）**

评审内容：投标人提供的项目实施计划、项目组织管理等情况。评审标准：项目实施计划完整合理、进度安排合理满足要求、项目管理及项目相关保障措施得当有效等情况进行综合评审。打分区间可根据主观评判划分为（10-8 分）、（8-5 分）、（5-4 分）三档。

**6、售后服务（3-9 分）**

评审内容：投标人提供的项目保修期内售后服务等情况。评审标准：项目保修期长、项目培训等售后服务方案完整合理、售后服务人员配备充足、本地化服务响应及时、应急保障措施得当有效等情况进行综合评审。打分区间可根据主观评判划分为（9-8 分）、（8-5 分）、（5-3 分）三档。

**7、综合服务能力及投标响应度（3-9 分）**

评审内容：投标人综合服务能力及投标响应度。评审标准：投标人综合服务能力强、类似业绩多、相关信誉好、投标整体响应度高等情况进行综合评审。打分区间可根据主观评判划分为（9-8 分）、（8-5 分）、（5-3 分）三档。

累计最高得分 100 分。