编号：JSHCZB-2022071号

扬州市民卡有限责任公司硬件及服务采购项目

公开招标文件



**采 购 人：扬州市民卡有限责任公司**

**采购代理机构(章)：江苏汇诚投资咨询管理有限公司**

**发 放 日 期：** **2022年1月27日**

目 录

第一章 招标公告 3

第二章 投标人须知 6

第三章 合同条款及格式 19

第四章 项目需求 25

第五章 评标方法及评标标准 29

第六章 投标文件格式 32

# 第一章 招标公告

受[扬州市民卡有限责任公司]的委托，江苏汇诚投资咨询管理有限公司就[扬州市民卡有限责任公司硬件及服务采购]([JSHCZB-2022071号])项目进行公开招标采购，欢迎符合条件的供应商投标。

## 一、项目基本情况

1.项目编号：JSHCZB-2022071号

2.项目名称：扬州市民卡有限责任公司硬件及服务采购项目

3.预算金额：93万元

4.本项目设定最高限价，最高限价为 93万元。

5.采购需求：具体详见招标文件第四章。

6.合同履行期限：合同签订后叁年（除不可抗力、非乙方原因），系统正常运行，并完成全部验收工作。

7.本项目不接受联合体投标

8.有关本次招标的事项若存在变动或修改，敬请及时关注 “扬州市公共资源交易平台”、“扬州市城建国有资产控股（集团）有限责任公司网站”发布的信息或更正公告。

## 二、申请人的资格要求：

（一）满足《中华人民共和国政府采购法》第二十二条规定，并提供下列材料：

1 投标函**(原件)**

2 资格声明**(原件)**

3若法定代表人参加投标的，须提供本人身份证复印件**(原件备查)**；若授权代表参加的，须提供《法人授权书》原件和授权代表身份证复印件**（原件备查）**

4 营业执照副本**(复印件加盖投标人公章)**

5 依法缴纳职工社会保障资金的证明材料**(复印件加盖投标人公章)**(税务、银行或社会保险基金管理部门出具的连续三个月（2021年11月-2022年1月）缴纳职工社会保障资金的缴款凭证或缴款证明)

6 投标人近三个月内任意一个月（2021年11月-2022年1月）依法纳税的缴款凭证**(复印件加盖投标人公章)**

7 与第（6）条相对应的纳税申报表或经会计师事务所审计的2020年度财务报告（成立不满一年不需提供） **(复印件加盖投标人公章)**

8 投标人参加本次政府采购活动前3年内在经营活动中没有重大违法记录的书面声明**（原件）**

9供应商未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”(www.ccgp.gov.cn)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（提供网页查询截图并加盖供应商公章，查询时间为 2022年1月27日后 ）；

10供应商信用承诺书**（原件）**。

注一：如参加本项目的供应商为个体工商户、自然人或事业法人等非企业法人，则无

需提供上述 5-7 项，本文件中所需法定代表人相关材料、盖章及签字等可用供应商相关负责人的相应材料代替。

注二：投标文件的正本和副本中均须提供上述资格证明文件。资格证明文件须清晰可辨，若有缺失或不清晰，将导致投标被拒绝且不允许在开标后补正。

（二）本项目的特定资格要求：无

（三）拒绝下述供应商参加本次采购活动：

（1）供应商单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

（2）凡为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该项目的其他采购活动。

（3）供应商被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网"(www.ccgp.gov.cn)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。

（四）集中考察或召开答疑会：有

本项目组织供应商现场勘察，过时不候。法定代表人授权委托书（原件）、现场勘察确认函、身份证原件签到出席，并向采购人领取经采购人签字或盖章的现场勘察确认函。各供应商请务必对项目现场和周围环境进行仔细认真查勘，须充分了解本项目具体工作内容，在随后的采购活动中，对现场资料和数据所作出的推论、解释和结论及因勘察不到位造成的后果由供应商负责，并自行承担因了解不充分而影响报价准确性的风险。现场勘察确认函原件无须装订，需在开标现场递交，同时在投标文件中装订复印件。

现场勘察时间：2022年2月9日 上午9:30-11:00 （北京时间）

现场勘察地点：扬州市广陵区信息大道1号，“声谷”江苏信息服务产业基地（扬州）15号楼A座

现场勘察联系人：田源 联系电话：18118250720

## 三、获取招标文件

1、时间：2022年1月27日至 2022年2月8日，每日上午9时至11时30分，下午15时00分至17时30分（北京时间，法定节假日除外）。

2、地点：江苏汇诚投资咨询管理有限公司代理部一（扬州市邗江北路68号旺角西入口三楼）

3、方式：在“扬州市公共资源交易平台”、“扬州市城建国有资产控股（集团）有限责任公司网站”获取招标文件，如供应商确定参加投标，请于公告期内如实填写法定代表人授权委托书、被授权人身份证复印件、营业执照副本复印件加盖供应商公章、《供应商参加投标确认函》原件（授权委托书及供应商参加投标确认函投标人通过百度网盘链接自行下载），上述资料填写打印后加盖公章，拍照或扫描发送至邮箱并于代理机构人员确认（邮箱：2263852076@qq.com，邮件标题备注公司全称+项目简称，联系人：唐磊，电话：18752710910、0514-89787281），投标当日将确认函原件交到代理机构。如供应商未按上述要求去做，将自行承担所产生的风险。百度网盘链接: https://pan.baidu.com/s/1uNBJ0T3YZppkoHwmBMzFVw 提取码：hc28

4、售价：/

## 四、提交投标文件截止时间、开标时间和地点

1.2022年2月16日09点30分（北京时间）

2.地点：江苏汇诚投资咨询管理有限公司开标室, 邗江北路68号3楼西入口

## 五、公告期限

自本公告发布之日起5个工作日。

## 六、其他补充事宜

无

## 七、本次招标联系方式

1.采购人信息

名 称：扬州市民卡有限责任公司

地 址：扬州市邗江区史可法路58号

联系人：田源

联系电话：18118250720

2.江苏汇诚投资咨询管理有限公司信息

地　址：江苏汇诚投资咨询管理有限公司招标代理部一部, 邗江北路68号3楼西入口

联系人：唐磊

联系方式：18752710910；0514-80827735

## 八、其他

1.投标文件制作份数要求

投标人应提供纸质投标文件一式五份（一份正本， 四份副本）， 每份投标文件须清楚标明“ 正本”或“副本”。电子版投标文件 1 份（一般应为 PDF 格式、U 盘形式（单独封装）、随纸质正本文件一并提交）。当电子版文件和纸质正本文件不一致时，以纸质正本文件为准。电子版文件用于辅助评标和存档，投标人需承担前述不一致造成的不利后果。

2.潜在投标人对招标文件项目需求部分的询问、质疑请向采购人提出，由采购人负责答复。

3.本次投标保证金金额为人民币壹万元整

投标保证金缴纳账户信息：

户名：江苏汇诚投资咨询管理有限公司

开户银行：招商银行扬州分行开发区支行

请备注：投标保证金、项目名称

投标保证金必须在响应文件接收截止时间之前(2022年2月16日09:30)以银行汇票、本票的形式送达江苏汇诚投资咨询管理有限公司。（注：以其他形式或个人名义缴纳的保证金无效。请各供应商务必确认保证金在上述规定时间送达我单位，并备注项目编号，否则投标文件将被拒绝。）

**九、疫情防控期间，供应商注意事项：**

（1）供应商授权代表须无条件服从招标代理公司疫情防控措施，入场前进行实名登记、接受体温测量、自行戴好口罩、做好手部卫生消毒和投标文件等消毒防护，主动向代理公司说明近一周的个人身体情况、发热病人接触史以及近14天内的旅行史特别是较重疫区的旅行史。

1. 各供应商须明确项目授权代表，且出席活动的人数限1人。进场后的供应商应在指定开标室等候并参加开标活动，自觉配合场内秩序管理，不得擅自至非相关场所活动，聚集讨论。

江苏汇诚投资咨询管理有限公司

2022年1月27日

# 第二章 投标人须知

#### 1、招标方式

1.1 本次招标采取公开招标方式，本招标文件仅适用于JSHCZB-2022071号项目。

#### 2、投标人

#### 2.1 本招标文件中“供应商”，即“投标人”，是指参加投标竞争，并符合招标文件规定资格条件的法人、其他组织或者自然人。

#### 2.2合格的投标人

2.2.1 满足招标公告中供应商的资格条件要求的规定。

2.2.2 满足本文件实质性条款的规定。

#### 3、适用法律

#### 3.1 本次招标及由此产生的合同受中华人民共和国有关的法律法规制约和保护。

**4、投标费用**

4.1 投标人应自行承担所有与参加投标有关的费用，无论投标过程中的做法和结果如何，代理机构在任何情况下均无义务和责任承担这些费用。

4.2招标代理服务费

本次采购由采购人支付代理服务费，代理服务费约定按中标价\*1.5%\*40%计取，不足3000元按3000元收取，同时支付专家评审费（专家评审费暂按500元/人收取，按实结算，不提供发票、收据)。

（1）中标服务费支付方式：一次性以电汇或转账等形式支付。

#### 5、招标文件的约束力

5.1 投标人一旦参加本项目采购活动，即被认为接受了本招标文件的规定和约束。

#### 6、招标文件构成

6.1 招标文件有以下部分组成：

（1）招标公告

（2）投标人须知

（3）合同条款及格式

（4）项目需求

（5）评标方法与评标标准

（6）投标文件格式

请仔细检查招标文件是否齐全，如有缺漏请立即与代理机构联系解决。

6.2 招标的最小单位是包。招标服务数量及技术要求中未分包的，供应商对要求提供的服务不得部分投标；招标服务数量及技术要求中已经分包的，应当以包为单位投标。

6.3 招标文件如果要求供应商提交备选投标方案的，供应商可以提交备选方案；否则，备选方案将被拒绝。

6.4 投标人应认真阅读招标文件中所有的事项、格式、条款和规范等要求。按招标文件要求和规定编制投标文件，并保证所提供的全部资料的真实性，以使其投标文件对招标文件作出实质性响应，否则其风险由投标人自行承担。

#### 7、招标文件的澄清

7.1 任何要求对招标文件进行澄清的投标人，应在投标截止日期的十日前按投标邀请中的通讯地址，以书面形式通知代理机构。

#### 8、招标文件的修改

8.1 在投标截止时间前，代理机构可以对招标文件进行修改。

8.2代理机构在招标文件要求提交投标文件截止时间前，有权决定延长投标截止时间和开标时间，并在原采购信息发布媒体上发布变更公告。

8.3招标文件的修改将在“扬州市公共资源交易平台”、“扬州市城建国有资产控股（集团）有限责任公司网站”公布，补充文件将作为招标文件的组成部分，并对投标人具有约束力。

8.4投标人应在投标截止时间前关注原采购信息发布媒体上有关本招标项目有无变更公告。

#### 9、投标文件的语言、度量衡单位、货币和编制

9.1投标人提交的投标文件、技术文件和资料，包括图纸中的说明，以及投标人与代理机构就有关投标的所有来往函、电、通知和文件均应使用中文。投标文件中若有英文或其他语言文字的资料，应提供相应的中文翻译资料。对不同文本投标文件的解释发生异议的，以中文文本为准。投标文件以及投标人与代理机构就有关投标的所有来往通知、函件和文件均应使用简体中文。

9.2 除技术性能另有规定外，投标文件所使用的度量衡单位，均须采用国家法定计量单位。

9.3投标人应使用人民币报价。

9.4投标文件应字迹清楚、内容齐全、不得涂改。如有修改，修改处须有投标人加盖公章和法定代表人或其授权代表签字。

#### 10、投标文件构成

10.1 投标人编写的投标文件应包括：资信证明文件、投标产品配置与分项报价表、供货一览表、技术参数响应及偏离表、商务条款响应及偏离表、技术及售后服务承诺书、开标一览表等部分；

#### 10.2 投标人应将投标文件按顺序装订成册，应逐页编码，不得跳页（包括但不限于证明材料、声明及产品介绍、彩页等），并编制投标文件资料目录。由于编排混乱导致投标文件被误读或查找不到，责任由投标人承担。

#### 10.3 投标人应当根据招标文件要求编制投标文件，投标文件应对招标文件提出的要求和条件作出实质性响应，并在相应的投标文件中逐条标明满足与否。

#### 11、证明投标人资格及符合招标文件规定的文件

11.1投标人应按要求提交资格证明文件及符合招标文件规定的文件。

11.2投标人应提交证明其有资格参加投标和中标后有能力独立履行合同的文件。

11.3投标人除必须具有履行合同所需提供的货物以及服务的能力外，还必须具备相应的财务、技术方面的能力。

 11.4投标人应提交根据合同要求提供的证明产品质量合格以及符合招标文件规定的证明文件。

 11.5证明投标人所提供货物与招标文件的要求相一致的文件可以是手册、图纸、文字资料和数据。

#### 12、供货一览表和投标配置与分项报价表

12.1 投标人应按照招标文件规定格式填报供货一览表、投标配置与分项报价表，在表中标明所提供的设备品牌、规格、型号、原产地、主要部件型号及其功能的中文说明和供货期。每项货物和服务等只允许有一个报价，任何有选择的报价将不予接受(如有备选配件，备选配件的报价不属于选择的报价)。

12.2 标的物

采购人需求的货物供应、安装，调试及有关技术服务等。

12.3有关费用处理

招标报价采用总承包方式，投标人的报价应包括所投产品费用、安装调试费、测试验收费、培训费、运行维护费用、税金、国际国内运输保险、报关清关、开证、办理全套免税手续费用及其他有关的为完成本项目发生的所有费用，招标文件中另有规定的除外。

12.4其它费用处理

招标文件未列明，而投标人认为必需的费用也需列入报价。

12.5投标货币

投标文件中的货物单价和总价无特殊规定的采用人民币报价，以元为单位标注。招标文件中另有规定的按规定执行。

12.6 投标配置与分项报价表上的价格应按下列方式分开填写：

1、项目总价：包括采购人需求的货物价格、质量保证费用、培训费用及售后服务费用，项目在指定地点、环境交付、安装、调试、验收所需费用和所有相关税金费用及为完成整个项目所产生的其它所有费用。

2、项目单价按投标配置及分项报价表中要求填报。

**13、技术参数响应及偏离表、商务条款响应及偏离表及投标货物说明**

13.1 对招标文件中的技术与商务条款要求逐项作出响应或偏离，并说明原因；

13.2 提供参加本项目类似案例简介；

13.3 培训计划；

13.4 详细阐述所投货物的主要组成部分、功能设计、实现思路及关键技术；

13.5 投标人认为需要的其他技术文件或说明。

**14、服务承诺及售后服务机构、人员的情况介绍**

 14、1投标人的服务承诺应按不低于招标文件中商务要求的标准。

14、2提供投标人有关售后服务的管理制度、售后服务机构的分布情况、售后服务人员的数量、素质、技术水平及售后服务的反应能力。

#### 15、投标函和开标一览表

15.1 投标人应按照招标文件中提供的格式完整、正确填写投标函、开标一览表。

15.2 *开标一览表中的价格应与投标文件中投标配置与分项报价表中的价格一致，如不一致，不作为无效投标处理，但评标时按开标一览表中价格为准****。***

15.3 *开标一览表必须加盖公章，必须单独密封在信封中，在投标截止时间前与投标文件分别递交，否则视为无效投标。*

#### 16、投标保证金

16.1 投标人提交的投标保证金必须在投标截止时间前送达，并作为其投标的组成部分。

16.2在开标时，对于未按要求提交投标保证金的投标无效，代理机构拒绝接收其投标文件。

16.3未中标的投标人的投标保证金，将在中标通知书发出之日起5个工作日内凭代理机构经办人签署意见的保证金收据予以退还，不计利息。

16.4中标供应商的投标保证金，将在采购合同签订后退还，不计利息。

16.5 下列任何情况发生时，投标保证金将不予退还：

（1）投标人在投标有效期内撤回其投标；

（2）投标人提供的有关资料、资格条件证明文件被确认是不真实的；

（3）投标人之间被证实有串标（例如：统一哄抬价格）、欺诈行为；

（4）投标人被证明有妨碍其他人公平竞争、损害代理机构或者其他投标人合法权益的。

#### 17、投标有效期

17.1 投标有效期为代理机构规定的开标之日起**六十（60）天**。投标有效期比规定短的将被视为非响应性投标而予以拒绝。

17.2 在特殊情况下，代理机构于原投标有效期满之前，可向投标人提出延长投标有效期的要求。这种要求与答复均应采用书面形式。投标人可以拒绝代理机构的这一要求而放弃投标，代理机构在接到投标人书面答复后，将在原投标有效期满后五日内**无息退还其投标保证金**；同意延长投标有效期的投标人既不能要求也不允许修改其投标文件。本招标文件第16条有关投标保证金的规定在延长期内继续有效，同时受投标有效期约束的所有权利与义务均延长至新的有效期。

#### 18、投标文件份数和签署

18.1投标人应严格按照招标公告和招标文件要求的份数准备投标文件，每份投标文件须清楚地标明“正本”或“副本”字样。一旦正本和副本不符，以正本为准。

18.2投标文件正本中，除招标文件规定的可提交复印件外，其他文件均须提交原件。文字材料需打印或用不褪色墨水书写。投标文件的正本须经法定代表人或授权代表签署和加盖投标人公章。 本采购文件所表述（指定）的公章是指法定名称章，不包括合同专用章、业务专用章等印章。

18.3 除投标人对错处做必要修改外，投标文件不得行间插字、涂改或增删。如有修改错漏处，必须由法定代表人或授权代表签字或盖章。

#### 19、投标文件的密封和标记

19.1投标人应将投标文件正本和所有副本密封，不论投标人中标与否，投标文件均不退回。

19.2 密封的投标文件应：

19.2.1 注明投标人名称，如因标注不清而产生的后果由投标人自负。按招标公告中注明的地址送达；

19.2.2注明投标项目名称、标书编号及包号。

19.2.3未按要求密封和加写标记，代理机构对误投或过早启封概不负责。对由此造成提前开封的投标文件，代理机构将予以拒绝，作无效投标处理。

#### 20、投标截止日期

20.1 代理机构收到投标文件的时间不得迟于招标公告中规定的截止时间。

20.2 代理机构可以通过修改招标文件酌情延长投标截止日期，在此情况下，投标人的所有权利和义务以及投标人受制的截止日期均应以延长后新的截止日期为准。

#### 21、迟交的投标文件

21.1 代理机构拒绝接收在其规定的投标截止时间后递交的任何投标文件。

#### 22、投标文件的修改和撤回

22.1 投标人在递交投标文件后，可以修改或撤回其投标文件，但这种修改和撤回，必须在规定的投标截止时间前，以书面形式通知代理机构，否则，代理机构将拒绝。

22.2 投标人的修改或撤回文件应按规定进行编制、密封、标记和发送，并应在封套上加注“修改”或“撤回”字样。上述补充或修改若涉及投标报价，必须注明“最后唯一报价”字样，否则将视为有选择的报价。修改文件必须在投标截止时间前送达代理机构。

22.3 在投标截止时间之后，投标人不得对其投标文件作任何修改。

22.4 在投标截止时间至招标文件中规定的投标有效期满之间的这段时间内，投标人不得撤回其投标，否则其投标保证金将不予退还。

#### 23、开标

23.1 代理机构将在招标公告中规定的时间和地点组织公开开标。投标人应委派携带有效证件的代表准时参加，参加开标的代表需签名以证明其出席。投标人未参加开标的，视同认可开标结果。

 23.2开标仪式由代理机构组织，采购人代表、公证员、监委、投标人代表等参加。

23.3按照规定同意撤回的投标文件将不予开封。

23.4 开标时请投标人推选的代表查验投标文件密封情况，投标登记薄上作纪录无误后，代理机构当众拆封宣读每份投标文件中“开标一览表”的内容，未列入开标一览表的内容一律不在开标时宣读。开标时未宣读的投标报价信息，不得在评标时采用。

 23.5 代理机构将指定专人负责开标记录并存档备查，各投标人需仔细核对开标纪录相关内容并签字确认。

23.6 投标人在报价时不允许采用选择性报价，否则将被视为无效投标。

#### 24、评标委员会

 24.1开标后，代理机构将立即组织评标委员会（以下简称评委会）进行评标。

 24.2 评委会由采购人代表和有关技术、经济等方面的专家组成，且人员构成符合政府采购有关规定。

 24.3评委会独立工作，负责评审所有投标文件并确定中标候选人。

#### 25、评标过程的保密与公正

25.1公开开标后，直至签订合同之日止，凡是与审查、澄清、评价和比较投标的有关资料以及授标建议等，采购人、评委、代理机构工作人员均不得向投标人或与评标无关的其他人员透露。

25.2在评标过程中，投标人不得以任何行为影响评标过程，否则其投标文件将被作为无效投标文件。

25.3 在评标期间，代理机构将设专门工作人员与投标人联系。

25.4 代理机构和评委会不公布评标过程中的相关细节。

25.5 采用综合评分法的项目，未中标的投标人如需了解自己的评审得分及排序情况，可于中标结果公告期限届满之日起7个工作日内，由其法定代表人或授权代表携带本人有效身份证件到公共资源代理机构进行查询，逾期将不予受理。

#### 26、投标的澄清

26.1评标期间，为有助于对投标文件的审查、评价和比较，评委会有权以书面形式要求投标人对其投标文件进行澄清，但并非对每个投标人都作澄清要求。

 26.2接到评委会澄清要求的投标人应派人按评委会通知的时间和地点做出书面澄清，书面澄清的内容须由投标人法定代表人或授权代表签署，并作为投标文件的补充部分，但投标的价格和实质性的内容不得做任何更改。

 26.3 接到评委会澄清要求的投标人如未按规定做出澄清，其风险由投标人自行承担。

#### 27、对投标文件的初审

27.1投标文件初审分为资格检查和符合性检查。

27.1.1资格审查：依据法律法规和招标文件的规定，由采购人对投标文件中的资格证明文件进行审查。并将审查结论以书面形式向评委会反馈。

采购人在进行资格性审查的同时，将在“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网"(www.ccgp.gov.cn)对投标人是否被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重失信行为记录名单情况进行查询，以确定投标人是否具备投标资格。查询结果将以网页打印的形式留存并归档。

若接受联合体投标的项目，两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的,联合体成员存在不良信用记录的，视同联合体存在不良应用记录。

27.1.2符合性检查：依据招标文件的规定，由评委会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。

27.2在详细评标之前，评委会将首先审查每份投标文件是否实质性响应了招标文件的要求。实质性响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离或保留的投标。

所谓重大偏离或保留是指与招标文件规定的实质性要求存在负偏离，或者在实质上与招标文件不一致，而且限制了合同中买方（采购人）和见证方（代理机构）的权利或投标人的义务，纠正这些偏离或保留将会对其他实质性响应要求的投标人的竞争地位产生不公正的影响。是否属于重大偏离由评委会按照少数服从多数的原则作出结论。评委决定投标文件的响应性只根据投标文件本身的内容，而不寻求外部的证据。

27.3如果投标文件实质上没有响应招标文件的要求，评委会将予以拒绝，投标人不得通过修改或撤销不合要求的偏离或保留而使其投标成为实质性响应的投标。

27.4评委会将对确定为实质性响应的投标进行进一步审核，看其是否有计算上或累加上的算术错误，对开标一览表内容修正错误的原则如下：

（1）投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准。

（2）投标文件、“开标一览表”中报价的大写金额与小写金额不一致的，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。

（4）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。

同时出现两种以上错误的，按照前款规定的顺序修正。对不同文字文本投标文件的解释发生异议的，以中文文本为准。

27.5评委会将按上述修正错误的方法调整投标文件中的投标报价，调整后的价格应对投标人具有约束力。如果投标人不接受修正后的价格，则其投标将被拒绝，其投标保证金不予退还。

27.6评委会将允许修正投标文件中不构成重大偏离的、微小的、非正规的、不一致的或不规则的地方，但这些修改不能影响任何投标人相应的名次排列，否则不允许修正。

27.7采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由评标委员会按照招标文件规定的方式确定招标文件未规定的通过随机抽取的方式确定一个参加评标的投标人，其他投标无效。

使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由评标委员会根据招标文件规定的方式确定，招标文件未规定的采取随机抽取的方式确定一个中标候选人，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，招标文件中将载明其中的核心产品。多家投标人提供的核心产品品牌相同的，按前两款规定处理。

#### 28、无效投标、废标及投标人不足三家的处理

28.1无效投标条款

28.1.1未按要求交纳投标保证金的；

28.1.2未按照招标文件规定要求密封、签署、盖章的；

28.1.3投标人在报价时采用选择性报价；

28.1.4投标人不具备招标文件中规定资格要求的；

28.1.5投标人的报价超过了采购预算或最高限价的；

28.1.6未通过符合性检查的；

 28.1.7不符合招标文件中规定的其他实质性要求和条件的（*本招标文件中斜体且有下划线部分为实质性要求和条件，包括但不限于该范围）；*

28.1.8 投标人被 “信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网"(www.ccgp.gov.cn)列入失信被执行人或重大税收违法案件当事人名单或政府采购严重失信行为记录名单。若接受联合体的项目，两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，联合体成员存在不良信用记录的，视同联合体存在不良应用记录。

28.1.9 投标文件含有采购人不能接受的附加条件的。

28.1.10 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报价，有可能影响产品质量或者不能诚信履约的，要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

28.1.11其他法律、法规及本招标文件规定的属无效投标的情形。

28.2废标条款：

28.2.1符合专业条件的供应商或者对招标文件作实质响应的供应商不足三家的；

28.2.2投标人的报价均超过采购预算或最高限价；

28.2.3出现影响采购公正的违法、违规行为的；

28.2.4因重大变故，采购任务取消的；

28.2.5评标委员会认定招标文件存在歧义、 重大缺陷导致评审工作无法进行。

28.3投标截止时间结束后参加投标的投标人不足三家或者通过资格审查或符合性审查的投标人不足三家的，除采购任务取消情形外，按照以下方式处理：

28.3.1招标文件存在不合理条款或者招标程序不符合规定的，由采购人、代理机构改正后依法重新招标；

28.3.2 招标文件没有不合理条款、招标程序符合规定，需要采用其他采购方式采购的，采购人应当依法报财政部门批准。

#### 29、确定中标单位

29.1评委会根据本招标文件规定评标方法与评标标准向采购人推荐出中标候选人。

29.2 采购人应根据评委会推荐的中标候选人确定中标人。

29.3代理机构将在 “扬州市公共资源交易服务平台”、“扬州市城建国有资产控股（集团）有限责任公司网站”发布中标公告，公告期限为1个工作日。

29.4若有充分证据证明，中标人出现下列情况之一的，一经查实，将被取消中标资格：

29.4.1提供虚假材料谋取中标的；

29.4.2向采购人、代理机构行贿或者提供其他不正当利益的；

29.4.3恶意竞争，投标总报价明显低于其自身合理成本且又无法提供证明的；

29.4.4属于本文件规定的无效条件，但在评标过程中又未被评委会发现的；

29.4.5与采购人或者其他投标人串通投标的；

29.4.6采取不正当手段诋毁、排挤其他供应商的；

29.4.7不符合法律、法规的规定的。

29.5. 有下列情形之一的，视为投标人串通投标，投标无效：

29.5.1不同投标人的投标文件由同一单位或者个人编制。

29.5.2不同投标人委托同一单位或者个人办理投标事宜。

29.5.3 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人。

29.5.4不同投标人的投标文件异常一致或者投标报价呈规律性差异。

29.5.5不同投标人的投标文件相互混装。

29.5.6不同投标人的投标保证金从同一单位或者个人的账户转出。

#### 30、质疑处理

30.1投标人认为采购文件、采购过程和中标或成交结果使自己的权益受到损害的，可以在知道或应知其权益受到损害之日起七个工作日内，以书面形式向采购人或代理机构提出质疑。

30.1.1对采购文件提出质疑的，应当在获取采购文件之日或者采购文件公告期限届满之日起7个工作日内提出。

　　30.1.2对采购过程提出质疑的，为各采购程序环节结束之日起7个工作日内提出。

　　30.1.3对中标结果提出质疑的，为中标结果公告期限届满之日起7个工作日内提出。

30.2供应商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。质疑必须按《政府采购法》、《政府采购法实施条例》及《政府采购质疑和投诉办法》等相关规定提交。

30.3提出质疑的供应商（以下简称质疑供应商）应当是参与所质疑项目采购活动的供应商。

潜在供应商已依法获取其可质疑的采购文件的，可以对该文件提出质疑。对采购文件提出质疑的，应当在获取采购文件或者采购文件公告期限届满之日起7个工作日内提出。

30.4供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

　　30.4.1供应商的姓名或者名称、地址、邮编、联系人及联系电话；

　　30.4.2质疑项目的名称、编号；

　　30.4.3具体、明确的质疑事项和与质疑事项相关的请求；

　　30.4.4事实依据；

　　30.4.5必要的法律依据；

　　30.4.6提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

《质疑函》及《授权委托书》格式见网址：http://zfcg.yangzhou.gov.cn

30.5代理机构收到质疑申请后，将对质疑的形式和内容进行审查，如质疑内容、格式不符合规定，代理机构将告知质疑人进行补正。

30.6质疑人应当在法定质疑期限内进行补正并重新提交质疑函。

30.7代理机构应当在收到供应商的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。

30.8 诚实信用

30.8.1 投标人之间不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人和其他投标人的合法权益。

30.8.2 投标人不得以向代理机构工作人员、评标委员会成员行贿或者采取其他不正当手段谋取中标。经查实投标人有此行为的，政府采购管理部门将投标人列入不良行为记录名单，按照《政府采购法》有关规定处理。

30.8.3 投标人提出书面质疑必须有理、有据，不得虚假质疑和恶意质疑，并对质疑内容的真实性承担责任。一经查实，代理机构有权依据政府采购的有关规定，报请政府采购监管部门对该投标人进行相应的行政处罚并在网站上予以公示。如果投标人或者其他利害关系人通过捏造事实、伪造证明材料等方式提出质疑，干扰政府采购活动正常进行的，属于严重不良行为，代理机构将提请政府采购监管部门将其列入不良行为记录名单，并依法予以处罚。

30.8.4 投标人不得虚假承诺，否则，按照提供虚假材料谋取中标成交处理。

30.8．5 投标人应自觉遵守开标、评标纪律，扰乱开标评标现场秩序的，属于失信行为，根据《江苏省政府采购供应商监督管理暂行办法》，失信行为将被记入投标人诚信档案。

**31、中标通知书**

31.l中标结果确定后，代理机构将向中标供应商发出中标通知书。

31.2 中标供应商收到中标通知书后，应签字确认中标通知书已收到。若无回复，则公告后视同中标供应商已经知悉并同意接受。

31.3中标通知书将是合同的一个组成部分。对采购人和中标供应商均具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标供应商放弃中标项目的，应当依法承担法律责任。

31.4所有投标文件都将作为档案保存，不论中标与否，代理机构均不退回。

#### 32、 签订合同

32.l中标供应商应按中标通知书规定的时间、地点,按照招标文件确定的事项与采购人签订政府采购合同，且不得迟于中标通知书发出之日起三十日，否则投标保证金将不予退还，由此给采购人造成损失的，中标供应商还应承担赔偿责任。

32.2招标文件、中标供应商的投标文件及招标过程中有关澄清、承诺文件均应作为合同附件。

32.3 签订合同后，*中标供应商不得将货物及其他相关服务进行转包*。未经采购人同意，中标供应商也不得采用分包的形式履行合同，否则采购人有权终止合同，中标供应商的履约保证金将不予退还。转包或分包造成采购人损失或致使合同履行中发生违约现象的，中标供应商应承担赔偿责任。

32.4采购人不得向中标人提出任何不合理的要求作为签订合同的条件，不得与中标人私下订立背离合同实质性内容的协议。所签订的合同不得对招标文件确定事项和中标人投标文件作实质性修改。

#### 33、货物和服务的追加、减少和添购

33.1政府采购合同履行中，采购人需追加与合同标的相同的货物和服务的，在不改变合同其他条款的前提下，可以与中标供应商协商签订补充合同，但所有补充合同的采购金额不超过原合同金额10%。

33.2采购结束后，采购人若由于各种客观原因，必须对采购项目所牵涉的货物和服务进行适当的减少时，在双方协商一致的前提下，可以按照招标采购时的价格水平做相应的调减，并据此签订补充合同。

#### 履约保证金：/

**35、样品**

若项目要求提供样品的，中标人的样品由采购人负责保管、封存，并作为履约验收的参考。未中标人的样品将及时退还。

# 第三章 合同条款及格式

以下为中标后签定本项目合同的通用条款，中标供应商不得提出实质性的修改。关于专用条款将由采购人与中标供应商结合本项目具体情况协商后补充，但补充内容对招标文件和投标文件以及通用条款，不得作实质性修改。

**政府采购合同（货物）**

项目名称：扬州市民卡有限责任公司硬件及服务采购

编号：

甲方（采购人/买方）：扬州市民卡有限责任公司 乙方（供应商/卖方）：

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律法规的规定，甲乙双方按照江苏汇诚投资咨询管理有限公司关于本项目招标结果签订本合同。

**1、合同标的**

乙方根据甲方需求，提供下列货物： 。

货物名称、规格及数量等要求详见招投标文件。

**2、合同总金额**

2.1 本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元人民币（¥\_\_\_\_\_元）。

2.2 本合同总金额包括所乙方提供货物的产品费用、安装调试费、测试验收费、培训费、 运行维护费用、税金及其他有关的为完成本项目发生的所有费用，招标文件中另有规定的除外。

2.3 在招标文件未列明，而乙方认为履行本合同必需的费用也包含在合同总金额中。

2.4 本合同总金额还包含乙方提供的伴随服务/售后服务费用。

2.5 本合同签订后：甲方需追加与合同标的相同的货物和服务的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的增加的金额不超过原合同金额的10%；甲方若由于各种客观原因，必须对采购项目所牵涉的货物和服务进行适当的减少时，在与乙方协商一致后，可以按照招标采购时的价格水平做相应的调减，并据此签订补充合同；除上述情况外，本合同执行期间合同总金额不变。

**3、组成本合同的有关文件**

3.1乙方应按招标文件规定的时间向甲方提供使用货物的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

3.3 关于本项目政府采购的招投标文件或与本次采购活动方式相适应的文件及有关附件是本合同不可分割的组成部分，这些文件包括但不限于：

 （1）投标响应文件； （2）投标产品配置与报价文件；

 （3）供货一览表； （4）技术参数响应表；

 （5）服务承诺； （6）中标通知书；

 （7）甲乙双方补充协议； （8）乙方投标时提供的响应文件。

**4、知识产权保证**

乙方保证甲方在使用、接受本合同货物和服务或其任何一部分时，不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

**5、产权保证**

乙方保证所交付的货物的所有权无任何抵押、查封等权利瑕疵。

**6、履约保证金：/**

**7、转包或分包**

7.1 本合同禁止转包，本合同范围的货物，应由乙方直接供应的，不得转让他人供应。

7.2 经甲方同意，乙方可以依法采取分包方式履行合同，但是分包方式履行的，乙方应就采购项目向甲方负全责。

**8、质保期**

8.1 质保期 年。（自交货验收合格之日起计）

**9、交货期、交货方式及交货地点**

9.1 交货期：\_\_\_\_\_\_\_\_\_

9.2 交货方式：\_\_\_\_\_\_\_\_\_

9.3 交货地点：\_\_\_\_\_\_\_\_\_

**10、货款支付**

10.1 本合同项下所有款项均以人民币支付。

10.2 本合同项下的采购资金由甲方支付，付款前乙方向甲方开具发票。

10.3 甲方付款方式：设备到货后，10个工作日内乙方提供发票（发票分别按合同价的40%、合同价的55%、合同价的5%分别开票），甲方在10个工作日内支付设备总价（含税价）的40%；设备上架后，10个工作日内甲方进行验收项目，验收完成后甲方在10个工作日内支付设备总价（含税价）的55%。项目验收满三年，甲方10个工作日内支付设备总价（含税价）的5%；

**11、税费**

本合同执行中相关的一切税费均由乙方负担。

**12、质量保证及售后服务**

12.1 乙方应按招标文件规定及响应文件承诺的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品；若技术性能无特殊说明，则按国家有关部门最新颁布的标准及规范为准。

12.2乙方应保证其提供的货物在正确安装、正常使用和保养条件下，在其使用寿命内具有良好的性能。货物验收后，在质量保证期内，乙方应对由于设计、工艺或材料的缺陷所发生的任何不足或故障负责，所需费用由乙方承担。

12.3 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

12.4 如在使用过程中发生质量问题，乙方在接到甲方通知后在\_\_\_\_\_\_\_\_\_小时内到达甲方现场。

12.5 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

12.6上述的货物免费保修期为\_\_\_\_\_\_年，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

**13、交货、调试和验收**

13.1乙方应当在合同生效后 天内将货物交付甲方，地点由甲方指定，招标文件有约定的，从其约定。在发货前，乙方应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货初验收和使用的技术条件依据，检验的结果应随货物交甲方。

13.2 货到甲方后，甲乙双方须在 工作日内初验收，甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书、包装符合招标文件技术要求的，给予签收，初步验收不合格的不予签收。

13.3 乙方按照招标文件要求负责产品安装并培训甲方的使用操作人员，乙方在甲方使用前进行调试，调试直到符合技术要求的甲方才做最终验收。

13.4 对技术复杂的货物，甲方可请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告。验收时乙方必须在现场，验收完毕后作出验收结果报告；若聘请第三方中立机构验收，验收费用由甲乙双方协商解决。

13.5 甲乙双方关于调试和验收的其他约定： 。

**14、货物包装、发运及运输**

14.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

14.2 乙方发货时，产品使用说明书、检验证明书、随配附件和工具以及清单一并附于货物内。

14.3 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备甲方接货。根据甲方通知的时间和指定的地点，乙方负责安排送货、装卸、清点、堆放，设备初验收合格前的保管工作由乙方负责，费用乙方承担。

14.4 货物在交付甲方前发生的风险均由乙方负责。

14.5 货物在规定的交付期限内由乙方送达甲方指定的地点，经初步验收即视为货物交付。

**15、违约责任**

15.1 甲方无正当理由拒绝初验收和终验收货物的，甲方应按未付货款金额每日万分之五向乙方支付违约金。

15.2 甲方无故逾期验收和无故逾期办理货款支付手续的,甲方应按逾期付款金额每日万分之五向乙方支付违约金。

15.3乙方违约，在消除违约情形前，应按货款总额每日万分之五向甲方支付违约金，甲方可以从待付货款中扣除。

15.4乙方因逾期交货或因其他违约行为，导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

15.5 乙方所交的货物全部或部分品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，乙方更换货物但逾期交货的（甲方拒绝接受的除外），按乙方逾期交货处理；乙方拒绝更换货物的，甲方可选择解除本合同或本合同的一部分，并可追究乙方的其他违约责任。

15.6合同生效后，发现乙方投标属虚假承诺，或经权威部门监测提供的货物不能满足招标文件要求，造成合同无法继续履行的，乙方履约保证金不予退还外，还应向甲方支付不少于合同总价 %赔偿金。

**16、不可抗力事件处理**

16.1 在合同有效期内，甲乙双方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。不可抗力，是指不能预见、不能避免且不能克服的客观情况，例如战争、严重的地震、洪水等，但一方违约或疏忽导致合同不能履行的不属于不可抗力因素。

16.2不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。除甲方书面另行要求外，乙方应尽实际可能继续履行合同义务，以及寻求采取合理的方案履行不受不可抗力影响的其他事项。若不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

**17、争议解决**

17.1 因货物的质量问题发生争议的，可在国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。

17.2 因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决；如果协商不能解决争议，甲乙双方同意采取下列两种方式的第（ 1 ）种方式解决争议：

（1）向甲方所在地有管辖权的人民法院提起诉讼，适用中华人民共和国法律；

（2）向扬州仲裁委员会按其仲裁规则申请仲裁。

17.3 若甲乙双方任何一方都没有选择解除合同的，为避免扩大损失，在诉讼或仲裁期间，双方应继续履行。

**18、合同其它**

18.1 乙方应诚实信用，严格按照招标文件要求和投标承诺履行合同，不向甲方进行商业贿赂或者提供不正当利益。

18.2 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

18.2本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

18.3 本合同正本一式四份，具有同等法律效力，甲方、乙方各执贰份。

 甲方：扬州市民卡有限责任公司 乙方：

 地址： 地址：

 法定代表人或授权代表： 法定代表人或授权代表：

 联系电话： 联系电话：

日期： 年 月 日 日期： 年 月 日

**附件1**

**合同（协议）廉政通用条款**

1、协议双方均不得向对方或对方经办部门或其他与协议有直接或间接利益关系的人员索要、收受、提供、给予协议约定外的任何利益，包括但不限于明扣、暗扣、现金、购物卡、实物、有价证券、旅游、招待或其他非物质性利益等。

2、协议双方均严格禁止经办部门员工的任何商业贿赂行为，严禁在对方报销费用以及向对方提出个人利益要求或参加任何可能对履约有影响的宴请或娱乐活动。

3、严禁私自与对方就商务或项目合作进行私下商谈或达成默契，透露有关招投标内控信息及企业商业秘密。或采用任何方式在商务或项目合作中为自己、家属和亲友谋利益。

4、任何一方违反廉洁从业条款给对方造成损失的，违约方应赔偿因此给守约方造成的全部损失。

5、协议双方均应支持对方的廉洁诚信建设工作，如发现对方人员有违反上述约定的，应向对方纪检监察部门举报，被举报的一方不得以任何借口进行打击报复。

市民卡公司廉政举报邮箱：smklianzheng@foxmail.com。

协议方廉政举报邮箱：XXXXXXX

# 项目需求

以下技术参数中如出现产品品牌，均仅作为投标人参与投标时产品质量或标准的参考,投标人所投产品质量或标准不得低于参考品牌，投标人选择的产品不得低于参考品牌产品的参数要求，在满足参数要求的情况下，采购人接受其他品牌产品的投标。招标文件中推荐的型号也非指定的型号，投标人可在货物参数满足招标要求的情况下，选择相应的产品型号。

**一、项目背景**

为了贯彻和落实国家及行业信息安全等级保护相关政策文件要求，计划升级部分硬件系统，新增安全设备，增加系统的稳定性和安全性。

从安全技术体系、安全管理体系和运维服务体系三方面进行设计，通过本次整改建设，业务系统需具备以下能力：系统在统一的安全防护策略下具有抵御恶意攻击的能力；具有检测、发现、报警及记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；在业务系统遭受损害后，具备快速恢复正常运行状态的能力，最终根据实际情况在不过多投入资金成本的前提下，达到基本的网络安全运营的需求，对系统安全运营有一个基本的保障，同时对未来五年内，通过逐步完善安全体系，从而达到满足等保三级的目标打造一个坚实的基础，最终能够提供全方面、立体、纵深的安全保障防御体系，保证业务系统具备整体安全防御能力。

**二、项目需求清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **标的名称** | **单位** | **数量** | **备注** |
| **资金中心机房** |
| 1 | 交换机 | 台 | 1 |  |
| 2 | 安全网关 | 台 | 1 |  |
| 3 | 数据库审计系统 | 台 | 1 |  |
| 4 | 服务器 | 套 | 2 |  |
| 5 | 网闸 | 台 | 1 |  |
| 6 | 漏洞扫描 | 台 | 1 |  |
| 7 | 终端安全 | 台 | 1 |  |
| 8 | 态势感知探针 | 台 | 2 |  |
| **政府信息中心机房** |
| 9 | 交换机 | 台 | 2 |  |
| 10 | 防火墙 | 台 | 2 |  |
| 11 | VPN设备 | 台 | 1 |  |
| 12 | 备份一体机 | 台 | 1 |  |
| **维保设备以及安全服务** |
| 13 | 原设备维保 | 年 | 1 |  |
| 14 | 安全运维服务 | 年 | 3 |  |

**三、设备招标参数**

## 交换机

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 产品类型 | 千兆以太网交换机，  |
| 应用层级 | 三层 |
| 传输速率 | 10/100/1000Mbps，10000Mbps |
| 交换方式 | 存储-转发 |
| 背板带宽 | 336Gbps/3.36Tbps |
| 包转发率 | 108/126Mpps |
| 端口结构 | 非模块化 |
| 端口数量 | 52个 |
| 端口描述 | 48个10/100/1000Base-T以太网端口，4个万兆SFP+ |
| 堆叠功能 | 可堆叠 |

## 安全网关

|  |  |
| --- | --- |
| **硬件规格** | 国产品牌，机架式硬件设备，基于高性能硬件平台和专业安全操作系统 |
| ★本次配置8个10/100/1000MBase-T电口（含1对bypass接口），每个接口可划分到不同安全域实现各接口间的安全隔离，提供1个console口，2个USB口，1个MGT口。提供技术白皮书或产品彩页。 |
| ★防雷击，必须通过国家无线电监测中心检测中心浪涌（冲击）抗扰度（4KV）测试项目，并出具国家无线电监测中心检测中心委托测试报告 |
| **性能** | ★吞吐率(bps)≥5G，最大并发连接数≥170万，VPN吞吐量(bps) ≥3G，每秒新建连接数≥7万，IPS吞吐量≥4.5Gbps，AV病毒过滤吞吐量≥3.5Gbps，提供IPSec VPN隧道数≥6000条，并发SSL VPN用户许可≥100个，SSL VPN并发用户数支持扩展到3000个；提供防病毒模块授权3年服务。提供技术白皮书或者产品彩页。 |
| **网络适应性** | 支持透明、路由、混合、直连（虚拟线）模式 |
| 支持对3000+ 种应用的识别和控制，包括200+移动应用，要求支持多系统引导，并可在WEB界面上直接配置启动顺序；提供多个系统的配置截图以及WEB启动顺序截图证明, |
| 支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），提供产品界面截图证明 |
| 支持将任意接口数据完全镜像到设备自身的其他接口用于抓包分析，支持基于源IP、目的IP、源端口、目的端口、网络协议（TCP、UDP、ICMP）等条件对镜像流量进行过滤，并且支持选择入方向、出方向及双向流量镜像，提供产品界面截图证明 |
| ★支持BFD 功能，支持BFD与静态路由/OSPF/BGP进行联动。快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。通过与动态路由协议联动，缩短收敛时间，提升可靠性。提供产品界面截图证明 |
| 支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip等）限制新建连接、并发连接；支持基于应用协议的路由功能，根据应用类型进行路由选择。提供产品界面截图证明 |
| 支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断；支持为不同运营商的DNS设置不同权重，用户根据权重比例选择不同运营商DNS进行解析实现不同线路的负载均衡功能。提供产品界面截图证明 |
| ★支持线路过载保护功能，当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发，提供产品界面截图证明 |
| 支持基于接口时延的动态切换能力：系统从多出接口向外部某一个或多个目的地址探测时延。当自身接口的时延超过配置的阈值时，新建会话的流量就不再从这个接口转发，而是走其它接口。当此接口的时延回落到正常值以下后，新建会话的流量再允许从这个接口转发，提供产品界面截图证明 |
| **NAT功能** | 支持多对一、多对多的NAT地址转换，且公网地址池可选择逐一使用和同时使用两种模式。 |
| 为解决公网IP地址资源问题，要求必须支持NAT的端口扩展技术，支持NAT full cone模式。 |
| ★支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断，提供产品界面截图证明。 |
| **IPV6功能** | 支持IPV6邻居发现协议、IPV6 SNMP管理、IPV6路由配置、IPV6 DNS配置、IPV6策略配置、IPV6 ALG配置、IPV6 6TO4隧道配置、IPV6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置 |
| ★支持对IPV6用户的会话日志监控、流量监控、应用监控功能，并且能够对IPV6用户进行自定义监控统计功能，提供产品界面截图证明 |
| 支持对IPV6协议的网络层攻击防护功能、支持扩展IPV6协议的IPS入侵防御、AV病毒过滤功能。 |
| **VPN功能** | 支持标准IPSec协议，能够与Cisco等知名厂商的VPN设备互联互通；支持GRE、L2TP、Xauth等VPN连接 |
| 提供SSL VPN功能；必须支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、指定进程、系统补丁、浏览器版本、杀毒软件等方面，提供产品界面截图证明 |
| **IPS功能** | 支持旁路和在线两种模式，支持基于安全策略和安全域启用IPS功能，可在不同的攻击方向上启用IPS（至少支持流入\流出\双向等方向），提供产品界面截图证明 |
| ★支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法，提供产品界面截图证明 |
| ★具备数千种攻击特征库规则列表，并可自定义特征库，提供产品真实界面截图证明 |
| **防病毒功能** | 支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型；支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式，具备百万种以上病毒特征库数量。 |
| 支持在策略或者安全域启用防病毒功能。提供产品真实界面截图证明 |
| **管理功能** | 支持不少于8个配置文件并存，并支持配置文件备注以便配置回退。提供功能截图证明 |
| 提供标准的SNMPV1/V2/V3协议管理方式 |
| 支持基于IP地址的流量统计、支持基于应用的流量统计、支持基于IP地址的会话统计功能，支持基于应用的会话统计包括短时间周期和长时间周期（提供功能截图） |
| **资质要求** | ★《计算机信息系统安全专用产品销售许可证》（第二代防火墙千兆增强级），提供证明文件 |
| 具备中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》（增强级），提供证明文件 |
| 具备信息产业部颁发的电信设备进网许可证，提供证明文件 |
| ★提供近八年入围Gartner企业级防火墙魔力象限或者市场指南证明文件。 |
| ★NGFW(下一代防火墙)在最近5年内达获得NSS Labs最高评价推荐级,提供证明文件 |
| 加入微软安全响应中心（Microsoft Security Response Center）发起的MAPP（Microsoft Active Protection Program）计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。提供微软第三方证明或微软网站截图 |
| **服务要求** | 提供三年硬件及软件升级服务 |

## 数据库审计系统

|  |  |
| --- | --- |
| **★硬件规格** | 国产品牌，标准1U机架一体化设备（审计引擎和数据引擎一体化设备）；网络接口：配置≥4个千兆电口， USB2.0接口≥2个，RJ45串口≥1个，HA口≥1个，MGT口≥1个；支持≥4路审计监听功能；硬盘≥1T。 |
| **★性能要求** | 采用多核多平台并行操作系统，SQL处理能力≥12000条/秒，采用海量日志存储及高速检索技术，日志存储能力≥50亿条（1T存储），实配不少于8个数据库服务器或实例审计，数据库审计：支持IPv6网络环境的部署 |
| **部署方式** | 支持透明部署、代理部署模式、旁路部署方式，支持系统危险链路旁路阻断功能和危险链接串联阻断功能（需提供产品界面截图证明） |
| 支持agent代理部署模式，可实现虚拟化环境下的数据库审计 |
| **★多功能合一** | 单一设备即可同时支持包括数据库审计、风险扫描、状态监控、运维审计等功能，可按需扩展（需提供产品界面截图证明） |
| **★数据库兼容性** | 支持Oracle、SQLserver、MySQL、DB2、Sybase、Informix、Postgresql、Teradata、Cache、达梦、南大通用、人大金仓、神通、浪潮KDB、湖南上容、MongoDB、Hive、Hana、HWMPP、HighGo等23种主流数据库防护和审计（需提供产品界面截图证明） |
| **数据库审计** | 数据库访问记录应至少包括发生时间、业务用户名、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、响应时间、返回结果等关键信息 |
| 支持对SQL语句执行结果（成功/失败）、SQL语句执行时间、SQL语句执行异常等数据库操作响应信息的审计 |
| 支持变量绑定值的记录：很多基于数据库的查询是通过Bind Variable完成的。这就要求审计系统不光要记录查询中Bind Variable的变量的名字，还要记录Bind Variable的数值 |
| 支持时间、IP地址、用户名、终端名的黑白名单策略，将已知可信用户、可信时间之外的操作识别为高风险操作 |
| 支持定义事件类型，每种事件类型可以对应多个事件策略，不同策略命中的事件可以有高、中、低等多个风险级别支持定义所有SQL的相应威胁程度，至少包括高、中、低、提醒等告警级别 |
| 能够自动记录和分析SQL语句并快速制定安全策略，包括：将SQL语句归纳为不同的集群 |
| 系统提供白名单规则策略，系统提供黑名单规则策略，系统提供正则表达式规则策略，系统提供关键字表达式规则策略，系统提供例外规则策略 |
| 对数据库客户端运行过程中自动产生的SQL语句的过滤，减少不必要的审计记录 |
| 基于TDS，TNS等数据库协议还原数据库操作语句，而不是基于文本识别还原数据库语句 |
| 可对日志进行细粒度解析，支持审计数据库操作(DM)、对象管理(DD)、控制(DC)等操作语句的审计，解析后的日志记录至少包括访问发生时间、客户端IP地址、客户端MAC、终端程序、访问账号、访问数据库名、操作表名、SQL语句、数据库响应时间以及返回结果等关键信息（需提供产品界面截图证明） |
| 数据库旁路审计模式支持主备环境镜像，聚合接口镜像，数据库审计模式支持Oracle集群环境 |
| 通过三层关联技术，对应用服务器的真实用户/用户组的操作行为进行细粒度审计（需提供产品界面截图证明） |
| **审计策略与规则** | 设备必须自带默认审计策略，支持用户自定义策略和规则，系统必须支持配置操作行为的黑名单、白名单，方便用户灵活配置审计规则 |
| 支持以操作类型、时间、IP地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间、关键字、敏感数据、等作为事件识别规则及审计规则 |
| **审计告警** | 内置自动告警设置，允许用户设定威胁自动告警，告警必须提供级别设定，至少提供致命、高风险、中风险、低风险4种告警级别（需提供产品界面截图证明） |
| 支持SYSlOG、SNMP TRAP、邮件、FTP等多种事件告警和提示方式 |
| **白名单设置** | 支持对于符合条件的SQL语句直接放行，不进行记录功能，支持时间、IP地址、用户名、终端名的白名单策略，将已知可信用户、可信时间之外的操作识别为高风险操作 |
| **监控扫描** | 提供对数据库漏洞、不安全配置、弱口令、补丁等深层薄弱环节的安全检测及准确评估 |
| 支持服务扫描和发现功能，通过扫描网络中的开放端口以及确定监听这些端口的服务。如主机IP、端口、主机操作系统、服务的类型等。并实现自动或手动将这些服务添加到数据库引擎（需提供产品界面截图证明） |
| 支持对数据库服务器的扫描，自动识别数据库的表、字段等敏感信息的 |
| 支持对敏感数据分布的服务器进行统计，并以图表的形式展示，可导出为报表 |
| **状态监控** | 系统界面可以显示数据库状态、缓冲区击中率、库缓存大小等变化趋势图（需提供产品界面截图证明） |
| 系统界面可以显示数据库的会话明细、查询缓冲击中率等信息，支持将状态监控数据导出报表功能 |
| **检索** | 支持通过IP地址、用户名、操作类型、关键词、时间、策略名称、操作来源名称、风险级别、事件类型等基本条件查询审计事件，支持将审计日志的敏感字段进行模糊化处理，防止敏感数据泄露 |
| ★支持SQL关键字翻译功能，支持将审计记录中SQL语句关键字翻译成中文，便于非专业人员阅读（需提供产品界面截图证明） |
| 10亿条日志的任意关键字组合（包括通配符）检索时间<10分钟 |
| 提供对风险和危害访问的分析，包括：高危操作分析和追踪、大规模数据泄露分析和追踪、批量数据篡改分析和追踪、SQL注入行为分析和追踪 |
| **审计日志管理** | 支持按日志属性、日志类型、时间范围进行数据备份，自动与手动两种备份归档方式 |
| 支持FTP将数据备份到其他存储上，以备本机硬盘空间不够的情况下，数据能够依然保存 |
| 支持还原转出去的数据，还原之后数据可在系统中查询） |
| **报表功能** | 支持对SQL语句操作类型统计、事件类型统计、风险级别统计、流量统计，同时按在线用户、客户端IP、会话、模板数等支持在线信息统计（需提供产品界面截图证明） |
| 支持数据库分组管理，可以基于全局和单库多个维度进行统计分析，系统支持数据库的风险趋势图形化呈现，报表导出格式：WORD\ PDF\ Excel，支持报表预览语句分析页面SQL压力的显示功能，系统支持完全自定义报表，用户可自定义报表内容、报表条件 |
| **界面及安全管理** | 支持基于WEB方式的远程管理方式，采用HTTPS进行安全加密的配置管理 |
| 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能 |
| 系统支持设定多种不同角色的管理员、审计员，可以由审计员对管理员的操作进行审计记录 |
| **★产品资质** | 具备《计算机信息系统安全专用产品销售许可证》（三级）（需提供产品资质证书证明） |
| 具备计算机软件著作权登记证书（需提供产品资质证书证明） |
| 具备《中国国家信息安全产品认证证书》（增强级）（需提供产品资质证书证明） |
| 涉密信息系统产品检测证书（需提供产品资质证书证明） |
| **服务要求** | 提供三年硬件及软件升级服务 |

## 服务器

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 机架式 | ≥2U机架式，带导轨 |
| 处理器配置数目 | 配置2颗银牌4214R\*2 24核 2.4GHz。 |
| 内存类型 | ≥24个DDR4内存插槽,当前配置2根128GB ECC DDR4 2933MHz内存。 |
| 硬盘配置 | 本次配置2\*480G SSD  |
| 阵列控制器 | 配置1块独立12Gbps阵列控制器，2G缓存，配置超级保护电池；支持RAID 0/1/10/5/6/50/等功能  |
| 网卡 | 配置2块双口千兆以太网卡； |
| 电源 | 配置冗余高能效转换电源，实现1+1冗余，单个电源功率不低于750W，提供80Plus电源认证证书 |
| ★TPC-E规范 | 符合《网络关键设备和网络安全专用产品目录（第一批）》规范要求TPC-E ≥6500 tpsE标准。提供官网链接及截图 |
| ★可管理和维护性 | 提供独立前置USB端口支持手机或者平板等移动终端对服务器进行远程运维管理，提供且不限于服务器运行状态监控，远程查看以及日志信息采集等功能；手机/平板监控软件必须可以从app store以及安卓商城下载。（需提供下载地址及截图） |
| ★管理软件 | 提供统一的管理平台，支持同品牌服务器的硬件配置、微码、操作系统的统一管理，支持批量推送操作系统、批量配置服务器UEFI（BIOS）、批量裸机操作系统；提供管理软件可管理同品牌服务器、交换机与存储。 |
| ★高可靠性 | 全年非计划类停机时间超过4小时概率≤1%（需提供第三方官方证明）满足平均无故障时间MTBF的m1值≥150000小时（需提供国家级认证机构NCTC相关证明材料） |
| ★稳定性 | 支持ASHARE A4标准，工作温度最高支持45°C; （需提供国家级认证机构NCTC相关证明材料） |
| ★数据拯救 | 支持硬盘数据丢失拯救(须提供官网截图)，由原厂商提供数据拯救服务，原厂商数据拯救服务工程师需具备[全工业和信息化岗位技能水平考试证书—数据恢复高级工程师认证],（提供证书扫描件）。 |
| 认证 | 3C认证，CB,CE认证证书 |
| 售后服务 | 提供原厂商工程师安装调试与实施服务；提供原厂商3年7\*24免费质保、人工、部件服务。 |

## 网闸

|  |  |
| --- | --- |
| **系统架构** | 产品采用“2+1”（即双主机系统+物理隔离数据通道控制系统）体系结构；通过嵌入式数据通道控制系统隔离外部网络，而不是采用DMA、SCSI、网卡等方式实现；采用特有控制逻辑和专用通讯协议完全控制数据的实时交换，确保可信网络（域）和非可信网络（域）之间任何连接的断开，彻底阻断TCP/IP协议及其他网络协议 |
| **系统要求** | ★采用具有自主知识产权的基于linux内核的多核多线程并行安全操作系统；为提高系统可靠性，支持双系统引导，通过管理平台控制系统启动顺序，当前系统出现异常时，自动切换到备份系统，并支持系统相互备份和自动还原功能（提供功能截图） |
| **高可用** | ★具备多网口链路聚合功能，可实现内网网口和外网网口链路备份，分发策略支持Layer2、Layer2+3、Layer3+4；具备HA双机热备功能，可通过独立的热备端口或普通业务端口实现双机热备（提供功能截图） |
| **系统监控** | ★带液晶屏，液晶菜单可显示内外网机IP地址、CPU使用率和内存使用率等整机信息，面板可操控整机复位、关机，具有设备异常（如网络IP冲突、通讯异常等）监测报警功能（提供物理结构图和功能图） |
| **文件同步** | 文件同步支持SAMBA、NFS等文件传输协议，可以实现内网到外网、外网到内网、双向的文件传输；支持文件传输方向可控，实现单向或双向传输；支持病毒检测（投标时提供功能截图）；支持对文件内容智能语义分析，对指定文件的内容关键字过滤，确保只有符合保密、安全策略的数据文件才允许被同步（投标时提供功能截图）；文件同步支持时间段的控制：时间段可以是一次性执行、某个时间段执行、周期循环执行三种方式；（提供功能截图） |
| **数据库同步** | 持ORACLE、、MySQL、SQL Server、等主流数据库同步和支持国产达梦、南大通用等数据库的同步；支持多种同步方式（如先镜像后增量、增量），同步模式支持单向和双向同步（提供功能截图） |
| ★数据库同步支持时间段的控制，时间段可以是一次性执行、某个时间段执行、周期循环执行三种方式，且同步数据的数量可选及自定义；（提供功能截图） |
| ★支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃；可分别定义insert、update、delete的数据传输；同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安装任何第三方软件），支持Windows、Linux、Unix 等多种操作系统，且网闸无需开放端口以杜绝安全隐患（提供功能截图） |
| **视频交换** | 支持SIP、RTSP视频协议；支持视音频同时传输；支持基于动态端口传输的流媒体视频应用；支持视频管理服务器数据转发，视频管理服务器通道建立，支持视频SIP服务器数据转发，SIP管理服务器通道建立；能够严格区分视频数据流和控制信令流，根据策略配置可以控制视频数据的单向传输（提供功能截图） |
| **FTP访问** | ★支持文件名命名黑名单、扩展名类型黑名单、FTP命令字、FTP文件下载大小控制策略，FTP服务器地址过滤（提供功能截图） |
| **安全浏览** | 支持URL过滤；支持标准协议命令过滤；支持协议数据返回类型过滤；支持协议内容还原安全检查；支持协议内容还原病毒查杀。 |
| **邮件传输** | ★支持病毒扫描功能；支持基于SMTP协议的邮件发送和POP3协议的邮件接收，内外网隔离环境下可实现邮件收、发；支持附件及大小控制、支持字符/字符串过滤、文件类型过滤、支持邮件地址过滤及关键字检测（提供功能截图） |
| **入侵检测** | 具有实时入侵检测机制；支持对BasicAttack、 SMTP、FTP、DNS、DOS/DDOS 攻击、PortScan 的检测（提供功能截图） |
| **安全管理** | 支持CPU、内存、硬盘状态实时监控；支持HTTPS的Web方式管理，实现了远程管理信息加密传输；支持命令行方式管理，可以通过命令方式进行资源分配、排错、查看日志、深层次管理；支持远程SSH管理，远程管理的信息以密文形式传输（提供功能截图） |
| 必须通过内网主机系统来管理和配置网闸，而不是采用低安全的管理方式，如采用内外网口分别管理和配置网闸；系统登录界面采用USBkey和用户名与密码双因子进行认证（提供功能截图） |
| **防爆力破解限制** | 持时间控制管理，可设置多个时间点来控制网闸网络服务的启动、终止；支持系统防爆处理，对管理员登陆有密码次数限制，密码输入错误，超过限定次数，自动锁定设备，阻止非法管理员再次登录。根据限定期限，可自动解除锁定（提供功能截图） |
| **接入方式** | 支持IPV4/IPV6双栈接入 |
| **安全通道** | 系统应支持映射模式、网关模式、网桥模式，管理员可依据实际网络状况进行相应的部署。必须具备源地址转换功能和虚拟IP技术，可对外部隐藏内网真实地址。（提供功能截图） |
| **路由配置** | 支持IPV4静态路由，IPV6静态路由 |
| **集中管理** | 支持标准的SNMP协议，可与网管平台无缝对接；支持集中管理，支持对多台设备进行统一监控（提供功能截图） |
| **日志审计** | 记录内网预警信息日志、内网FTP同步日志、FTP代理日志、邮件发送日志、邮件接收日志、用户登录日志、内网链路日志、内网双机热备日志、文件共享同步日志、数据库同步日志、管理员日志（投标时提供功能截图）；记录外网预警信息日志、外网FTP同步日志、FTP代理日志、文件发送日志、文件接收日志、用户登录日志、外网链路日志、入侵检测日志、文件共享同步日志等（提供功能截图） |
| **日志管理** | 日志导出支持可选择任意时间段，日志导出类型支持XLSX加密及非加密等；日志下载可选日志导出类别（提供功能截图） |
| **日志空间管理** | 支持自定义日志空间大小，告警百分比，日志留存天数（提供功能截图） |
| **备份和恢复** | 支持备份、恢复功能，能对系统的各业务模块、通信配置单独等进行备份和恢复（提供功能截图） |
| **时间配置** | 支持修改系统时间和日期，可设置时间与Internet时间服务器同步 |
| **告警管理** | 支持对管理员的操作、FTP同步、文件共享同步、数据库同步等进行实时的告警，告警信息可显示告警级别、详细告警事件、备注信息、创建时间等，可以删除及批量删除历史过期的告警信息 |
| **系统调试** | 支持针对指定网卡进行故障测试，测试工具包含traceroute、telnet、ping、arp、tcpdump等（提供功能截图） |
| **系统检测** | 系统支持自动检测、周期性检测，可下载自动产测报告、周期性检测结果、messages（提供功能截图） |
| **服务要求** | 提供三年硬件及软件升级服务 |

## 漏洞扫描

|  |  |
| --- | --- |
| **硬件配置** | 标准1U机架式设备，内存≥8G，硬盘≥1T，千兆电口≥6，提供一个接口扩展槽，1个带外管理口，1个串口，2个USB口，支持两个万兆光纤接口，单电源（提供产品彩页或白皮书证明） |
| **性能配置** | 默认配置50个主机扫描IP并发数，支持10个任务并发进行，包括主机扫描、网站安全监控、数据库扫描、基线配置核查等 |
| **管理要求** | 支持HTTPS安全访问方式；支持远程管理；用户多次登录失败时，自动锁定登录账户。支持扫描范围自定义、资产导入扫描范围、从文件导入扫描范围 |
| **产品部署** | 支持单机部署，支持分布式部署，产品旁路接入网络，无需改变原有的网络架构，支持漏洞引擎热部署。 |
| **资产管理** | 支持资产树形结构对资产管理，并可自定义资产组，支持从文件导入资产，支持对选中资产的提供连通性测试，对测试不通过的资产提供可参考的信息 |
| 支持端口与服务发现。可对监控目标进行全端口扫描，并整理出服务的端口、应用软件类型、版本，并提供搜索接口可对目标进行搜索。 |
| ★端口扫描方式：支持TCP SYN扫描、connect扫描、TCP ACK扫描、UDP扫描、TCP FIN扫描、TCP NULL扫描、Xmas Tree扫描、idle扫描等（提供产品配置界面截图证明） |
| 资产属性变更历史查询：可针对扫描结果进行回溯，查找IP地址以往开启的端口状况，系统可针对扫描结果进行备注、添加标签 |
| ★支持自动生成网络拓扑图，并支持手动编辑拓扑图（提供产品配置界面截图证明） |
| **网站安全监控** | 支持HTTP、HTTPS协议，支持IIS、Websphere、Weblogic、ApacheTomcat、Nginx等web应用，支持Asp、Jsp、.Net、J2EE、Php等开发语言，支持Access、Mysql、ORACLE、DB2、PostgreSQL、Sybase、Informix、sqlite、MSSQL SERVER等数据库，支持WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件。 |
| 检测网站是否可用，检测服务器响应时间，检测域名劫持 |
| 支持Web组件识别。可对网站系统所使用web组件进行识别，包括OA系统、邮件系统、CMS系统、论坛社区等应用及其版本。 |
| 支持Web页面检索。可抓取网站系统的所有页面信息，并存储到数据库，并提供搜索功能。 |
| 支持SQL注入、XSS跨站脚本、命令执行、目录遍历、上传漏洞等检测 |
| ★自动化解析json、base64数据并进行扫描，系统支持自助式添加安全扫描插件，安全扫描插件可通过发包匹配关键字与自定义扫描代码方式添加（提供产品配置界面截图证明） |
| 追踪最新的安全漏洞，并及时更新，支持自定义扫描策略，支持输入POST数据，支持Web2.0扫描，支持flash解析，支持自定义不扫描的目标URL，支持自定义扫描深度 |
| ★支持输入Cookie信息和Cookie自动录制，进行登录扫描，支持自定义爬虫规则，支持设置UrlRewrite规则，提供配置界面截图截图证明 |
| 支持被动扫描，支持用户录入url ，支持自定义网站操作系统、数据库、中间件等信息，支持BASIC、NTLM等多种认证方式。，支持HTTPS双向认证站点扫描，支持代理设置，支持数据包调试，支持验证漏洞，支持白名单设置，支持图片MD5比较，支持页面标题比较，支持删除、更新链接提醒，支持页面相似度阀值设置 |
| ★支持定位到篡改的页面源码位置，高亮显示，身份证信息、银行卡等个人敏感信息识别，支持对附件如pdf、word、excel等检测（提供产品配置界面截图证明） |
| 支持自定义敏感关键字、图片文字识别、基于分词的语义分析、网马、暗链动态检测，支持Activex识别，支持检测钓鱼网站 |
| **主机扫描** | 支持NT、2000、XP、2003、Win7、2008、Win8、Win10等Windows系统，支持Amazon Linux 、CentOS 、Debian、Fedora、Red Hat、SuSE、Ubuntu等Linu系统，支持AIX、FreeBSD、HP-UX、Solaris、Mac OS X等Unix系统 |
| 支持Microsoft Internet Explorer 、PHP、IIS、Apache、Tomcat、PHP、Adobe Flash等应用程序；支持Vmware EXSi、XenServer等虚拟化平台 |
| 支持思科等网络设备，支持Juniper等安全设备 |
| ★支持安全扫描，保证扫描过程中目标系统正常运行，漏洞规则超过58000条（提供产品配置界面截图证明） |
| 覆盖缓冲区溢出漏洞、拒绝服务攻击漏洞、弱口令、信息泄露漏洞等全部常见漏洞 |
| 能够扫描常见的网络安全客户端软件（网络防病毒Symantec、TrendMicro、McAfee）的安全漏洞。 |
| 能够扫描常见的应用软件漏洞（如IE浏览器、MSN、Mozilla Firefox、Yahoo Messenger、MS Office、多媒体播放器、VMware虚拟机）的安全漏洞 |
| 提供专门针对DNS服务的安全漏洞的检测，支持自定义扫描策略，支持设置策略并发数，支持UDP扫描，支持扫描端口服务版本，支持登录扫描，如SMB登录、SSH登录等 |
| **数据库扫描** | 支持Oracle、Mysql、Sqlserver2000/2005/2008、Sybase、DB2、Informix、Postgresql等常见数据库 |
| ★支持人大金仓(Kingbase)、达梦(DM)、南大通用(GBase)等国产数据库，Mongodb、Redis、Couchdb、Memcache等nosql数据库（提供产品配置界面截图证明） |
| ★支持授权扫描、非授权扫描，支持扫描数据库中隐藏的木马病毒（提供产品配置界面截图证明） |
| 漏洞规则库包括1700多条策略，支持CVE、CNNVD等标准兼容，覆盖权限绕过漏洞、SQL注入漏洞、访问控制漏洞、执行权限过大漏洞、访问权限绕过漏洞、DBMS漏洞、提取漏洞等 |
| 支持对表、列等对象进行扫描，内置身份证、银行卡信息等敏感信息检测规则，支持用户自定义关键字 |
| **基线配置检查** | 操作系统：Windows（32位Windows XP/7 8/10/ Server、64位Windows XP/7/8/10/ Server）、Linux（Centos、Debian、Fedora、Redhat、Suse、Ubuntu等）、Unix（Aix、HP-UX、Solaris等） |
| ★国产操作系统（中标麒麟、红旗、深度、凝思等）等（提供产品配置界面截图证明） |
| ★针对windows系统可采集操作系统基本信息、硬件基本信息、应用软件、进程、活动端口开放情况、开机自启动项、用户列表、主机日志信息、补丁信息、安全审计信息和安全策略配置情况，能够采集浏览器上网记录、USB使用记录。 |
| 支持IIS、Apache、Tomcat、Weblogic、Websphere、Nginx、Jboss、Resin等中间件，支持Oracle、Mysql、DB2、Informix、Mssql、Sybase、达梦等数据库，支持Vmware EXSi、XenServer等虚拟化平台，支持H3C、思科、华为、中兴、锐捷、Juniper、力腾等网络设备进行数据采集，采集数据包括设备基本信息、开启服务信息、设备配置信息等 |
| 支持采集juniper、NetScreen、网神、山石、启明、网御星云、天融信、华三、华为、飞塔、思科、★风云、深信服、入侵防御系统等安全设备数据，采集数据包括设备基本信息、安全规则配置、安全策略配置、日志报警信息 |
| "支持通过SMB、Telnet、WinRM、Agent等检测windows，通过Agent检测时，支持结果手动上传，支持结果自动上报"，支持通过Telnet、SSH远程检测Linux、Unix、国产操作系统、虚拟化平台，支持Telnet、SSH远程检测路由交换防火墙，且支持将离线命令在目标设备上运行后，通过提供执行命令集Session Log方式检查，支持通过SMB、Telnet、SSH远程检测Windows和Linux中间件，支持远程检测数据库，支持对数据库和中间件设备安装路径自动探测功能。 |
| 对扫描失败的设备和检查项有非常准确的失败信息反馈，支持灵活的检查任务制定功能，可以设定手动、定时任务的配置任务检查方式，支持实时显示检查任务进度和检查任务状态，在建立核查任务时支持从“资产库获取、Excel导入”方式添加核查设备。 |
| 安全配置核查时，程序占用的资源应尽量的少，扫描主机的CPU平均占用率小于10％，内存占用小于50M；被扫描主机的CPU占用率小于1％，内存占用小于3M； |
| 系统提供密码文件模版下载功能，在建立核查任务时提供导入功能，系统读取设备信息后保存在内存中，在任务执行完毕后销毁，做到一次性使用。 |
| 系统默认可检查的配置检查点应不小于 2100个，支持检查项按设备类型管理，支持安全基线检查点的权重设定功能。 |
| ★支持安全基线检查项自定义功能 |
| **弱口令扫描** | 具备单独口令猜测扫描任务，支持对SMB、FTP、POP3、SMTP、SSH、TELNET、SNMP、RDP、redis、Oracle、MySQL等协议进行在线弱口令扫描，支持自定义用户名、口令字典 |
| **离线弱口令扫描** | 支持MD5、SHA1、BASE64、AES、3DES等常用加密算法及组合加密，根据资源类型匹配加密算法，在弱口令稽核时根据此加密算法进行密码破解。 |
| 支持用户自定义弱口令字典，工具内置弱口令字典，并提供弱口令字典维护功能。除此以外，工具应具有良好的稳定性，适应长时间大量加密口令的检验比对。 |
| 定期提供加密算法完善和字典更新，弱口令字典组与字典关联匹配，自定义分组管理，并在弱口令稽核时可选择对应的字典组。 |
| 密码文件采集脚本管理，针对不同应用类型密码文件，通过采用不同模式自动化脚本来收集弱口令离线核查工具所需的相关密码文件。（如使用shell脚本获取服务器上的shadow和passwd文件） |
| 针对已经核查出的资源弱口令，进行弱口令的确认、和修复后的二次确认，支持在线、离线等一次执行、周期执行的方式进行批量资源下发弱口令稽核任务，支持手动输入某口令核查其是否为弱口令（提供产品配置界面截图证明） |
| 支持redhat、Suselinux、Ubuntu等linux，Aix、Hpaix、solaris等Unix，Microsoft windows，Tomcat、Jboss、Weblogic等中间件，Oracle、Mysql等数据库，思科、华为主流型号交换机，支持思科、天融信等主流型号安全设备 |
| **安全功能** | 木马病毒检查，网站恶意代码检查 |
| **等保合规** | 支持新建等保测评任务，并支持设置基础信息系统SAG等级，支持录入基础信息系统内的机房、安全设备、网络设备等、服务器、终端、应用软件等，内置等保检查指标，支持将工具检查结果与指标一键关联，支持问卷调查，支持导出等保测评报告（提供产品配置界面截图证明） |
| **渗透测试** | 包括Whois信息获取、二级域名获取（搜索引擎模式、暴力破解模式等）等功能。包括Web指纹识别、端口扫描探测及端口指纹识别、Web路径扫描、旁注扫描等功能。SQL注入（获取数据库、表、执行任意命令等）、子域名爆破、GNU Bash 远程代码执行漏洞、Struts 2 S2-005、Struts 2 S2-007、Struts 2 S2-008、Struts 2 S2-009、Struts 2 S2-012、Struts 2 S2-013、Struts 2 S2-045、Struts 2 S2-048、Struts 2 S2-053、Adobe ColdFusion 文件读取漏洞、Couchdb 垂直权限绕过漏洞、Discuz 7.x/6.x 全局变量防御绕过导致代码执行、Drupal Drupalgeddon 2 远程代码执行漏洞等，包含HTTP请求编辑器 |
| **报表管理** | 应提供多维度报告统计功能，提供导出功能，格式支持Html、Excel、PDF、Word等主流格式，支持自动上报结果到FTP服务器，支持在线报告查看报告功能 |
| 报告包含漏洞详情、漏洞描述、漏洞风险级别、加固建议等，报表统计支持漏洞验证，要求提供详细的验证用例，且漏洞验证需要提供完整的http请求头，并要求提供详细的测试用例 |
| **第三方接口** | 提供XML和SYSLOG接口等二次开发接口给其他的安全产品或者安全管理平台调用，并且提供具体接口的说明文档; 具备对外接口，支持任务下发接口，根据任务ID将扫描结果上报接口，进度查询接口，获取策略接口，支持与微软WSUS补丁系统联动 |
| **管理功能** | 用户的增删查改、自定义用户角色、日志的增删改查、支持设置可以登录WEB管理页面的远程IP |
| 支持Ping、curl、traceroute等诊断工具、支持Base64、十六进制、MD5、AES、RC4等常见编码／解码，加解密方法 |
| **资质** | 所投产品具有公安部颁发的销售许可证，提供证书复印件 |
| 所投产品具有国家版权局颁发的软件著作权，提供证书复印件 |
| **服务要求** | 提供三年硬件及软件升级服务 |

## 终端安全

|  |  |
| --- | --- |
| 低资源占用 | ★支持本地和远程安装部署，客户端软件完整安装包文件小于10MB,运行后进程数量不大于2个，客户端安装目录对磁盘空间占用总量小于35MB。【提供产品界面截图】 |
| 操作系统兼容性 | 支持Windows server 2003/2008/2012/2016/2019；支持Windows XP、Vista、Windows 7/8/8.1/10；支持Linux kernel 2.6 及以后版本；支持国产主流操作系统，包括中标麒麟、银河麒麟、深度科技等；支持VMWARE ESX、Hyper-V、XEN和KVM等多种虚拟化平台部署。 |
| 安全探针 | ★安全探针部署在终端之后，无客户端托盘、无任何警告弹窗、无需终端用户做任何操作，所有操作均可在管理平台完成。【保留测试权利】 |
| 此次提供≥50个探针管理许可 |
| 资产管理 | 支持主机硬件资产管理，可自动收集已安装探针主机的硬件信息，如CPU、内存、硬盘、网卡等；资产变更状态、终端防护状态；系统信息，如操作系统版本、系统配置、在线状态等；资产数据可自定义导出。 |
| 资产自动分组 | 支持主机资产能自动分组，可自定义IP范围分组，上线的主机依据IP地址自动分类到相应分组，降低管理人员手动运维的工作量 |
| 资产安全评级 | 支持资产风险评级，对每个终端安全状态进行安全评级，至少包括正常、低危、中危、高危四个等级。 |
| 资产变更管理 | 支持记录主机资产变更情况，可记录每次变更时间及变更前后内容，并对资产变更事件进行告警，告警项可自定义。 |
| 主机账户管理 | ★支持实时检测Linux系统账户新增 删除 修改的变更，可在5秒内发现，并支持邮件告警【提供产品界面截图，保留测试权利】 |
| 远程批量部署 | ★支持对未安装探针的Linux主机进行远程批量部署安装，可批量导入或单个添加IP和账户信息，支持选择要安装的探针版本，支持查看批量部署任务状态，可看到已执行和应执行的主机数量和详细列表，支持批量重新安装。【提供产品界面截图】 |
| 风险行为防护 | 支持系统风险行为防护，包括Windows主机的office攻击、浏览器攻击、漏洞攻击等，Linux主机的SUID提权、系统漏洞提权、webshell越权执行等，防护模式可选择不处理、仅记录和阻止。 |
| 恶意程序防护 | 支持对木马程序、后门程序、蠕虫病毒、感染性病毒和漏洞攻击行为的检测与响应。 |
| 加密行为防护 | ★支持对文件异常加密行为检测和阻止，避免遭受勒索病毒等恶意文件加密，可对异常加密行为提供阻止、仅记录或不处理的响应动作【提供产品界面截图】 |
| 异常命令运行防护 | ★同时支持对Windows和Linux运行异常命令进行检测和阻止，避免攻击者利用系统合法程序执行恶意命令，达到对主机的攻击和破坏，支持区分Windows高危和低危命令并分别设定防护策略，可做阻止、仅记录和不处理的响应动作【提供产品界面截图】 |
| 漏洞攻击防护 | ★支持对主机主动发起或遭受系统漏洞攻击行为的检测和响应，包括永恒之类漏洞、RDP漏洞等，可有效防止利用漏洞传播勒索和挖矿。能够精准记录展示攻击源目的IP，关联并展示发起攻击的进程文件，找到攻击源。【提供产品界面截图】 |
| 网络威胁防护 | 支持对主机端口扫描、泛洪攻击、TCP洪水攻击等进行检测防御，并能自定义信任IP清单减少误报。 |
| 暴力破解防护 | 支持身份认证暴力破解检测和防护，可自定义监测方式，包括监控的端口、检测阈值，可自定义处理方式，包括不处理、仅记录、阻止、封禁问题IP时长等。 |
| 主机微隔离 | 支持以主机维度定义多个安全域，每个安全域可添加多个用户组或主机终端，可基于安全域设定出入站安全访问规则，安全访问规则可基于通信协议、通信对象、通信端口、防护动作多个维度进行定义。 |
| 支持自定义通信对象组和端口对象组，通信对象组可基于单个IP地址、IP范围、IP网段、用户组和终端多个维度定义，端口对象组可基于单个端口、端口范围进行定义。 |
| 黑白名单管理 | 支持Windows主机运行环境锁定，仅允许白名单内文件运行，支持批量和单个扫描、导入、删除文件白名单。 |
| 支持文件和证书黑白名单管理，可批量导入文件黑白名单，可对证书黑白名单进行管理，内置信任证书列表。 |
| 多维威胁检测 | ★支持检测Windows操作系统注册表中映像劫持、网络劫持、登陆劫持、开机自运行、任务计划、系统服务、驱动程序、浏览器插件的配置文件路径【提供产品界面截图】 |
| ★支持linux系统关键文件变更记录，包括文件的详细路径、文件哈希、文件存在终端数量、最后更新时间，并能在线查看文件内容。【提供产品界面截图】 |
| 主机异常变化检测 | ★支持对主机运行的文件、存在的网络端口、系统服务、系统账户等进行同组或全网主机横向分析对比，可显示覆盖的终端数量和终端列表。可对网络端口和系统服务关联到的进程名称和路径做展示，以及判断相关进程文件的安全性【提供产品界面截图】 |
| 主机异常离线检测 | ★支持主机在线状态的检测，可实施检测终端主机异常离线的时间、终端名称、重要级别、通知源头、通知发送状态、概要和详情等信息【提供产品界面截图】 |
| 网站后门检测 | 支持对网站后门防护，可实时监控和定时扫描，可指定需要监控和扫描的具体路径。 |
| 弱密码检测 | 支持Linux系统弱密码检测，可自定义弱密码字典，支持批量导入。 |
| 操作命令审计 | 支持对Linux主机执行的命令进行记录，包括时间、终端名称、用户、操作系统、远程终端、命令内容，记录的日志能够导出和筛选。【提供产品界面截图】 |
| 登录监控审计 | ★支持实时监测主机终端登录状态，包括登录时间、终端名称、登录帐号、登录远程IP等；支持记录主机终端历史登录日志，包括登录时间、终端名称、登录帐号、登录远程IP，支持对账号登录日志做查询，包括时间区间、终端名称、登录帐号、远程IP、登录动作等。【提供产品界面截图】 |
| 风险事件溯源 | ★支持以多种条件对风险事件进行筛选，包括发生时间、终端名称、事件类型、处理操作、用户名，并支持多种条件并行选择。【提供产品界面截图】 |
| ★支持追溯风险事件的根源主机，并以树形结构展示风险文件进程的调用关系，对事件详情进行描述，可追溯恶意进程的运行时间、详细路径、以及文件信息详情，并可手动加入黑白名单。【提供产品界面截图】 |
| ★支持对风险事件追溯分析，可记录事件发生时间、发生数量、关联主机名称、登录的用户账户、事件行为描述、事件关联文件详细路径、关联文件加载的模块信息、行为发生时的调用栈信息。【提供产品界面截图】 |
| ★支持对Linux主机执行的高危命令进行追溯，可记录事件类型、执行命令内容、执行命令时间、执行命令的用户名，并能查看命令上下文信息。【提供产品界面截图】 |
| 支持对网络攻击源IP、攻击范围追溯，可追溯发起网络访问的文件及具体路径。支持对风险文件来源和扩散范围追溯，可对文件分布主机范围及运行轨迹进行追溯。 |
| 网络访问日志溯源 | ★支持Windows系统安全访问规则匹配日志记录，可记录终端名称、访问时间、协议类型、出/入站方向、匹配次数、源IP地址、目的端口、关联主机进程、进程详细路径、进程安全级别等信息，可快速将进程文件加入黑白名单。【提供产品界面截图】 |
| 主机安全基线核查 | 支持对linux系统包括防火墙开启状态、FTP是否允许匿名登录、系统账户超时是否自动退出、以及风险文件检查；支持对Windows系统包括防火墙状态、系统必须服务、默认共享设置、登录超时设置、共享匿名访问等进行检查。 |
| 主机实时运维 | ★支持查看单主机实时进程列表，包括进程名称、进程路径、单进程CPU/内存占用情况、进程文件安全级别，并可以远程停止进程、将进程文件删除或隔离。【提供产品界面截图】 |
| ★支持查看主机磁盘目录，可查看每个路径或磁盘分区下的文件夹，以及每个文件夹内的文件信息，可显示文件名称、路径、大小，并能对文件进行隔离操作。【提供产品界面截图】 |
| 违规操作追溯 | ★支持记录管理员操作日志，可对比每次操作前后配置信息变化情况，对违规操作进行追溯。【提供产品界面截图】 |
| 风险主机定位 | 支持以文件hash或IP地址进行全局搜索，可检索到与文件hash相关的事件和主机信息，可检索到IP地址归属地及与该IP访问相关的主机列表以及详细进程文件清单。 |
| 文件全网搜索 | ★支持对指定路径下的指定文件在全网主机在线搜索，可显示包含被搜索文件的主机列表，包括主机名、文件描述、版本、HASH值等信息。【提供产品界面截图】 |
| 资质 | 本次投标的产品需提供公安部计算机信息系统安全专用产品销售许可证。【提供证书复印件有效】 |
| **服务要求** | 提供三年硬件及软件升级服务 |

## 态势感知探针

|  |  |
| --- | --- |
| **基本要求** | 国产品牌；基于高性能硬件平台和专业安全操作系统；  |
| 1U机架式设备，千兆电口≥4个 |
| 应用层吞吐≥300Mbps  |
| **可视化展示** | 提供服务器风险监控、电脑风险监控、威胁事件监控和外部攻击地理分布概览的可视化呈现 |
|  | 支持投屏监控 |
| **服务器风险监控** | 通过内网威胁透视镜呈现由服务器发起或指向服务器的网络威胁，通过不同的颜色标识服务器的风险程度，支持多维度的条件过滤 |
| 通过内网流量透视镜呈现由服务器发起或指向服务器的网络流量，以服务器为对象，监控与服务器互访的异常网络流量，支持多维度的条件过滤 |
| 提供服务器基本信息、风险指数、威胁行为和互访流量的可视化呈现 |
| 提供服务器风险TOP5列表和两周内的风险服务器趋势变化 |
| 透视镜视图增加了风险/流量TOP10排名，支持快速添加视图滤镜 |
| 透视镜视图支持基于管理员拖动后保存位置视图 |
| **电脑风险监控** | 通过风险电脑列表进行风险电脑威胁信息的可视化呈现，支持识别电脑名称、操作系统、浏览器，服务类型，统计记录电脑威胁行为及异常访问流量 |
| 通过内网威胁透视镜呈现由内网电脑发起或指向内网电脑的网络威胁 |
| 支持将被识别为某类服务类型的电脑一键设置成服务器 |
| 提供电脑基本信息、风险指数、威胁行为和异常流量的可视化呈现 |
| 提供电脑风险TOP5列表和两周内的风险电脑趋势变化 |
| **威胁事件监控** | 支持网络威胁检测的可视化呈现，包括威胁名称、威胁类型、风险级别、知识库、证据报文等信息，支持多维度的条件过滤 |
| 支持异常行为威胁事件的异常信息提取及呈现 |
| 提供所有IOC威胁事件分类统计和两周内威胁事件的趋势变化 |
| 支持攻击路径还原 |
| 通过对威胁事件的分析，提炼威胁事件的核心内容及影响，使专业的威胁事件转化为简单通俗易懂的描述，便于分析威胁事件的影响及内容。 |
| 支持对勒索，挖矿，木马，永恒之蓝，WannaCry，MIRAI等威胁事件进行标签标记，对标签发生次数进行统计分析，根据标签对服务器及终端进行威胁画像 |
| **网络层攻击检测** | 多种畸形报文攻击检测，SYN Flood、DNS Query Flood等多种DoS/DDoS攻击检测，支持ARP攻击检测，支持ARP欺骗检测 |
| **入侵攻击检测** | 基于签名状态的高性能攻击检测 |
| 实时攻击源IP检测、攻击事件记录  |
| 支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测 |
| 支持缓冲区溢出、SQL注入、CC攻击、外链攻击和跨站脚本攻击的检测 |
| 支持自定义应用层攻击特征，提供预定义检测配置模板 |
| 提供8000多种特征的攻击检测，特征库支持网络实时更新 |
| **病毒检测** | 基于流的病毒检测 |
| 支持压缩病毒文件的扫描  |
| 超过200万的病毒特征库，病毒库支持网络实时更新 |
| **高级威胁检测** | 基于高级威胁行为集的未知威胁检测 |
| 支持2000多种高级恶意软件家族的检测，包含Virus、Worm、Trojan、Over ow等类型 |
| Advance Malware Family特征库支持网络实时更新 |
| 支持主流的恶意勒索软件和挖矿软件检测 |
| **异常行为分析** | 基于建立电脑和服务器行为数据模型的异常行为检测 |
| 支持扫描、垃圾邮件、HTTP协议异常检测、可疑行为、暴力破解、DNS协议异常检测、挖矿等异常行为的检测 |
| 精准定位内网失陷电脑及风险服务器，通过证据报文溯源攻击细节 |
| 可灵活配置异常行为检测的灵敏度、学习周期、学习基值等属性，支持手动配置学习和不监测，应对业务变更或特例情况 |
| 支持手动设置异常行为检测中部分检测规则的检测阈值，适应真实环境 |
| **威胁关联分析** | 基于高级威胁、异常行为和应用行为之间的潜在关联性检测 |
| **威胁欺骗检测** | 本地设置欺骗检测，诱捕网络威胁攻击，确认威胁来源、威胁类型及影响范围 |
| 支持FTP、HTTP、MYSQL、SSH、TELNET，5中网络协议的行为欺骗检测 |
| **C&C检测** | 支持专业的僵尸主机地址、 Botnet外网恶意服务器IP地址和域名的检测 |
| **脆弱性监控** | 支持联动漏洞扫描设备；  |
| 支持手动获取漏洞扫描设备的扫描结果，并关联相关的IDS规则进行监控显示；  |
| **热点威胁情报** | 由云端实时推送目前业界已发现的最严峻的威胁信息至设备 |
| 设备支持以弹窗形式显示最新的威胁推送信息 |
| 支持每条威胁情报内容提供详细的名称、严重级别、详细信息、解决方案、受影响系统、CVE-ID、CVVND、参考信息链接等内容；  |
| **沙箱检测** | 基于云端架构的恶意软件虚拟运行环境，发现未知威胁 |
| 多重静态检测引擎快速过滤正常文件及已知威胁，提升沙箱检测效率 |
| 基于日志、报表、监控信息、文件行为报告等， 提供未知威胁可视化能力 |
| 对于判断为恶意的文件，提供完整的文件行为分析报告 |
| 支持HTTP、SMTP、POP3、IMAP4、FTP协议的检测 |
| 支持PE、APK、JAR、MS-OFFICE、PDF、SWF、RAR、 ZIP文件类型的检测 |
| 支持全局威胁情报共享，同步检测最新的未知威胁 |
| **垃圾邮件检测** | 实时的垃圾邮件分类和检测 |
| 支持明确的垃圾邮件、恶意群发邮件、可疑垃圾邮件、正常群发邮件 |
| 和语言、格式、内容无关的垃圾邮件检测能力，支持SMTP和POP3邮件协议，免监控域白名单 |
| **应用分析** | 可识别超过4000种以上的PC及移动端应用程序 |
| 能够准确识别IM、P2P下载、文件传输、邮件、在线游戏、股票软件、流媒体、非法信道等应用 |
| 支持基于安全域、接口、地域、用户、IP地址等多维度统计 |
| **CNNVD兼容性** | 威胁日志支持根据CNNVD ID进行搜索，CNNVD ID漏洞描述信息 |
| 特征描述支持CNNVD ID， 支持通过CNNVD ID搜索特征 |
| **设备监控** | 支持设备CPU、内存、温度、硬盘、物理接口等状态监控 |
| 支持设备整机流量、新建、并发连接的趋势监控 |
| **系统告警** | 支持设备条件告警，包括CPU利用率、内存利用率、磁盘空间利用率、新建连接、并发连接、接口带宽、机箱温度、CPU温度 |
| 支持基于应用的带宽和新建连接告警 |
| 支持Email的告警方式 |
| **对接态势感知平台** | 支持与大数据分析态势感知平台对接，上送威胁日志，供大数据平台进行全网威胁分析 |
| 必须兼容态势感知平台 |

## 防火墙

|  |  |
| --- | --- |
| **硬件规格** | 国产品牌，机架式硬件设备，基于高性能硬件平台和专业安全操作系统 |
| ★本次配置8个10/100/1000MBase-T电口（含1对bypass接口），每个接口可划分到不同安全域实现各接口间的安全隔离，提供1个console口，2个USB口，1个MGT口。提供技术白皮书或产品彩页。 |
| ★防雷击，必须通过国家无线电监测中心检测中心浪涌（冲击）抗扰度（4KV）测试项目，并出具国家无线电监测中心检测中心委托测试报告 |
| **性能** | ★吞吐率(bps)≥5G，最大并发连接数≥170万，VPN吞吐量(bps) ≥3G，每秒新建连接数≥7万，IPS吞吐量≥4.5Gbps，AV病毒过滤吞吐量≥3.5Gbps，提供IPSec VPN隧道数≥6000条，并发SSL VPN用户许可≥100个，SSL VPN并发用户数支持扩展到3000个；提供IPS和防病毒模块授权3年服务。提供技术白皮书或者产品彩页。 |
| **网络适应性** | 支持透明、路由、混合、直连（虚拟线）模式 |
| 支持对3000+ 种应用的识别和控制，包括200+移动应用，要求支持多系统引导，并可在WEB界面上直接配置启动顺序；提供多个系统的配置截图以及WEB启动顺序截图证明, |
| 支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），提供产品界面截图证明 |
| 支持将任意接口数据完全镜像到设备自身的其他接口用于抓包分析，支持基于源IP、目的IP、源端口、目的端口、网络协议（TCP、UDP、ICMP）等条件对镜像流量进行过滤，并且支持选择入方向、出方向及双向流量镜像，提供产品界面截图证明 |
| ★支持BFD 功能，支持BFD与静态路由/OSPF/BGP进行联动。快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。通过与动态路由协议联动，缩短收敛时间，提升可靠性。提供产品界面截图证明 |
| 支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip等）限制新建连接、并发连接；支持基于应用协议的路由功能，根据应用类型进行路由选择。提供产品界面截图证明 |
| 支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断；支持为不同运营商的DNS设置不同权重，用户根据权重比例选择不同运营商DNS进行解析实现不同线路的负载均衡功能。提供产品界面截图证明 |
| ★支持线路过载保护功能，当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发，提供产品界面截图证明 |
| 支持基于接口时延的动态切换能力：系统从多出接口向外部某一个或多个目的地址探测时延。当自身接口的时延超过配置的阈值时，新建会话的流量就不再从这个接口转发，而是走其它接口。当此接口的时延回落到正常值以下后，新建会话的流量再允许从这个接口转发，提供产品界面截图证明 |
| **NAT功能** | 支持多对一、多对多的NAT地址转换，且公网地址池可选择逐一使用和同时使用两种模式。 |
| 为解决公网IP地址资源问题，要求必须支持NAT的端口扩展技术，支持NAT full cone模式。 |
| ★支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断，提供产品界面截图证明。 |
| **IPV6功能** | 支持IPV6邻居发现协议、IPV6 SNMP管理、IPV6路由配置、IPV6 DNS配置、IPV6策略配置、IPV6 ALG配置、IPV6 6TO4隧道配置、IPV6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置 |
| ★支持对IPV6用户的会话日志监控、流量监控、应用监控功能，并且能够对IPV6用户进行自定义监控统计功能，提供产品界面截图证明 |
| 支持对IPV6协议的网络层攻击防护功能、支持扩展IPV6协议的IPS入侵防御、AV病毒过滤功能。 |
|  **VPN功能** | 支持标准IPSec协议，能够与Cisco等知名厂商的VPN设备互联互通；支持GRE、L2TP、Xauth等VPN连接 |
| 提供SSL VPN功能；必须支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、指定进程、系统补丁、浏览器版本、杀毒软件等方面，提供产品界面截图证明 |
| **IPS功能** | 支持旁路和在线两种模式，支持基于安全策略和安全域启用IPS功能，可在不同的攻击方向上启用IPS（至少支持流入\流出\双向等方向），提供产品界面截图证明 |
| ★支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法，提供产品界面截图证明 |
| ★具备数千种攻击特征库规则列表，并可自定义特征库，提供产品真实界面截图证明 |
| **防病毒功能** | 支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型；支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式，具备百万种以上病毒特征库数量。 |
| 支持在策略或者安全域启用防病毒功能。提供产品真实界面截图证明 |
| **管理功能** | 支持不少于8个配置文件并存，并支持配置文件备注以便配置回退。提供功能截图证明 |
| 提供标准的SNMPV1/V2/V3协议管理方式 |
| 支持基于IP地址的流量统计、支持基于应用的流量统计、支持基于IP地址的会话统计功能，支持基于应用的会话统计包括短时间周期和长时间周期（提供功能截图） |
| **资质要求** | ★《计算机信息系统安全专用产品销售许可证》（第二代防火墙千兆增强级），提供证明文件 |
| 具备中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》（增强级），提供证明文件 |
| 具备信息产业部颁发的电信设备进网许可证，提供证明文件 |
| ★提供近八年入围Gartner企业级防火墙魔力象限或者市场指南证明文件。 |
| ★NGFW(下一代防火墙)在最近5年内达获得NSS Labs最高评价推荐级,提供证明文件 |
| 加入微软安全响应中心（Microsoft Security Response Center）发起的MAPP（Microsoft Active Protection Program）计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。提供微软第三方证明或微软网站截图 |
| **服务要求** | 提供三年硬件及软件升级服务 |

## VPN设备

|  |  |
| --- | --- |
| **指标项**  | **技术规格**  |
| 性能指标 | 性能参数：最大理论加密流量（Mbps）≥100，最大理论并发用户数≥300，整机吞吐量≥150Mbps，千兆电口≥4个，提供50套接入授权； |
| 基本特性 | 支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持Windows、IOS、Android、塞班等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入；移动端（Android、IOS）支持通过PPTP、L2TP VPN方式接入； |
| 易用性 | 支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开；防止用户在无线网络环境下网络正常切换时VPN隧道断开； |
| 支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持Web参数修正，可针对Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题。 |
| 权限控制 | 支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统。 |
| 支持TOTP动态令牌认证，支持无需部署令牌认证服务器实现动态令牌认证，动态令牌认证客户端支持谷歌身份认证器、FreeOTP等。 |
| 应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限； |
| 终端安全 | 产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。 |
| 支持用户终端登录前、登陆后的安全性检测，检测范围包括：用户接入IP、接入时间、接入线路IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件； |
| 产品应提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用VPN； |
| 高速性 | 针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果； |
| 支持利用网页进行动态寻址的方法，客户端无需安装插件直接根据速度探测实现用户端接入线路的自动优选,大大降低了系统部署难度。 |
| 支持非对称式部署的传输协议优化技术（单边加速），可提升用户访问应用服务的速度。 |
| 支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议 |
| 支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输 |
| 服务要求 | 要求提供不少于3年的产品质保和软件升级服务。 |

## 备份一体机

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 备份节点硬件参数 | 基于Linux 64位系统(非Windows或Unix)的专用容灾备份存储设备，减少病毒感染机率，确保系统稳定。 |
| 一体机交付，与备份软件为统一品牌 |
| 2U机架式备份容灾存储设备，存储系统软件与备份容灾软件整合为一体，无需再额外配置备份服务器 |
| 1颗1.7GHz八核intel Bronze 3106 处理器 |
| 配置32GB高速缓存，可扩展至352GB |
| 备份设备系统盘采用2块240GB企业级SSD，通过硬件RAID1（考虑性能，不接受LVM和软RAID）保护，以确保备份系统的安全性和可用性 |
| 标配6块6TB SATA磁盘 |
| 提供2个板载千兆GE网口+2个10GE光口 ; 支持3个PCIe槽 ; 支持扩展8Gb/16Gb FC HBA卡 ; 支持扩展千兆/万兆网卡以及万兆光口网卡 |
| 资质认证 | 国内知名品牌（非外资和中外合资品牌），具有自主研发能力，非OEM |
| 提供软件著作权登记证书，软件产品登记证书 |
| 备份系统功能 | 一套备份与恢复系统 , 同时支持定时备份保护、持续数据保护、云备份和异地容灾 |
| 备份系统用户及权限管理 | ★支持系统管理员，审计管理员、安全管理员、租户,操作员和巡检员六类角色，通过分权管理，提升备份系统的管理安全性（分别提供六种角色登录后的账户信息截图并加该原厂商公章）。 |
| 系统管理员的职责：负责系统运维、管理操作员角色，系统运维包括管理系统告警、新建编辑指纹池、授权管理、SMTP管理、控制台通信、节点管理、磁盘管理、RAID管理、卷管理以及配置快照池等 |
| 审计管理员职责：主要负责对系统管理员和安全管理员的操作行为进行审计以及记录系统和设备的相关事件信息，并管理日志保留期限 |
| 安全管理员负责：负责为操作员分配和收回客户端、虚拟化平台和指纹池等资源，重置操作员密码，以及负责对审计管理员和操作员的操作行为进行监督，记录任务相关的所有事件信息 |
| 操作员职责：主要负责在安全管理员授予的客户端范围内进行客户端的配置，备份任务的管理，恢复任务管理，数据清理以及管理任务告警等。无权限进行任何系统管理和维护操作。 |
| 巡检员能够查看备份系统所有信息，但是只有查看权限，没有任何操作和配置权限。 |
| 支持通过配置密码提示问题和答案来找回账户密码，避免因遗忘账号密码而无法管理备份系统。 |
| 所有账户初次登录必须强制更改默认密码，提升管理安全性。 |
| 备份系统兼容性 | 具有Windows、Linux和Unix平台的保护能力，满足IT系统复杂性和兼容性需求 |
| 数据库及应用保护 | 支持对SQL Server、Oracle、DB2、GBase、MySQL,Exchange Server等主流数据库和应用进行在线备份保护。备份任务配置过程全部图形化向导指引完成，无需编写任何的脚本。 |
| Oracle数据库备份支持自定义脚本，支持RMAN备份参数的图形化配置。支持12C PDB高级特性 |
| 支持对Hadoop文件系统进行在线备份保护，支持文件、目录、格式和日期过滤，支持永久增量备份。支持备份数据恢复至原环境和其他Hadoop集群，支持恢复至其他文件系统。 |
| 卷级备份 | 支持SAP HANA单机&集群定时备份恢复 , 支持粒度为实例,租户数据库 , 支持数据源自动发现 , 支持流量控制 |
| 支持GaussDB 200/300 6.5.1备份恢复 |
| 支持Windows文件系统的卷级备份功能，以整卷为单位进行数据备份，提升海量小文件环境下的备份效率。支持整卷恢复和单文件目录级别的细粒度恢复 |
| ★源端重复数据删除技术 | 支持基于源端的可变长度切片的重复数据删除技术，多个备份任务可以共享同一个重复数据删除指纹池，也可以根据数据的不同单独设置专属指纹池，最大限度的提升重复数据删除效率，减轻带宽压力，降低传输数据量和备份数据存储成本。（提供该功能证明材料） |
| 支持并行重复数据删除，通过在多个不同的节点上构建指纹池，并将指纹并行分布于多个节点，有效解决单点性能和存储空间压力问题（提供该功能证明材料）。 |
| 采用内存级指纹池进行重删，所有指纹读写全部保存于内存中，从而提升指纹查询和处理效率，并且减少了因磁盘中指纹池增大所导致的随机IO压力。当指纹池不再需要进行备份时，将指纹同步到磁盘当中。指纹池构建在不同重删节点上，而生产数据可以基于多个不同的指纹池，执行并行重删。（提供该功能证明材料） |
| 支持使用配置文件的方式限制重删单个进程内存使用大小（提供该功能证明材料） |
| 采用内存进行重复数据删除加速，重复数据删除的计算和对比均在内存中进行。重删指纹池实现按需加载到内存，不使用时写入普通机械磁盘中，无须高性能的SSD。大幅提高重复数据删除速度和效率，降低投资成本。（提供该功能证明材料） |
| ★数据安全性 | 支持对备份数据进行加密传输和存储，支持AES256和SM4两种加密算法，提升传输过程以及存储的安全性。（提供该功能证明材料） |
| 支持备份数据基于内核级别的数据不可逆技术，能够有效防止勒索病毒等入侵。（提供支持功能截图） |
| ★永久增量备份 | 支持永久增量备份技术，初次备份对数据进行完全备份，之后只对新增加或改动过的数据做增量备份。每个增量备份的数据副本将自动合成为完全副本，能够大幅度减少备份时间，节省备份数据所需的存储空间，且提升了恢复效率（提供该功能截图）。 |
| Oracle实时复制 | 支持整个实例的复制 ; 支持整个实例的Switch Over ; 支持整个实例的Fail Over |
| KVM应用容灾 | 支持周期性同步数据， |
| 支持永久增量 |
| 支持根据历史时间的长短灵活配置cdp的数据保留策略。 |
| 无需额外配置日志卷。 |
| 支持保留1024个快照。 |
| 支持任意IO恢复，并且以心电图的形式呈现，IO时间点粒度到微秒级别。 |
| 支持配置接管机的IP和网络。 |
| Linux 下支持lvm的系统卷 |
| 服务 | 3年服务 |

## 设备维保

**原有设备清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 设备类型 | 型号 | 单位 | 数量 |
| 服务器 | DELL R740 | 台 | 1 |
| 服务器 | DELL R740 | 台 | 1 |
| 存储 | MD3800F | 台 | 1 |
| 光纤交换机 | 戴尔Brocade 300 | 台 | 1 |
| 光纤交换机 | 戴尔Brocade 300 | 台 | 1 |
| 防火墙 | 山石网科E2300 | 台 | 1 |
| 入侵防御 | 山石网科S1060 | 台 | 1 |
| 堡垒机 | 齐治 SHTERM-JL3 | 台 | 1 |

**服务要求：**

|  |  |  |
| --- | --- | --- |
| 序号 | 服务名称 | 服务内容 |
| 1 | 定期巡检 | 乙方工程师每2 个月(每个月月中)到现场对进行全面巡检，确认设备运行状态，检查系统错误记录，排除隐患故障并进行设备保修工作。在检测后两周内，乙方工程师向客户提供检测报告，巡检报告应包括：维保设备清单、巡检内容、巡检结果、发现的问题、风险隐患提示、维护建议等。 |
| 2 | 上门服务 | 乙方可提供20次/年的对产品的上门服务，根据甲方系统现状进行问题的解决和维护。在服务后两周内，乙方工程师向客户提供服务报告，服务报告应包括：设备清单、服务内容、服务结果，不包含优化建议等。 |
| 3 | 应急服务 | 乙方可提供10次/年的应急服务，甲方设备出现故障，通过电话无法解决问题，乙方要派遣工程师到达甲方现场，解决故障，恢复系统正常运行，问题处理完成后一周内向甲方提供系统故障分析报告。 |
| 4 | 远程电话邮件技术支持 | 乙方可提供7\*24小时电话邮件支持服务，当甲方系统遇到问题时，通过拨打乙方技术人员电话或发送邮件等方式，获得问题解答和技术咨询，当远程等操作无法解决后，可派乙方技术人员到达现场进行解决。 |
| 5 | 灾难演练 | 乙方可提供每半年1次的核心业务系统应急灾难演练，协助用户进行必要的业务系统切换测试。 |
| 6 | 培训服务 | 乙方可定期的针对甲方的应用环境，制定有先进技术的培训方案，对甲方进行周期性的培训指导。 |

## 安全运维服务

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 风险评估服务 | 风险评估对现有网络中的网络架构、网络协议、系统、数据库等资产安全现状进行发现和分析，确定系统在具体环境下存在的安全漏洞、隐患，以及被黑客利用后会造成的风险和影响。在此基础上对实施流程进行规划：即针对数据中心具体情况制定适合于自身的安全目标和安全级别，设计和实施相应的安全建设方案。 |
| 安全体系规划服务 | 通过对安全体系现状的分析，为信息安全保障总体规划提供了基础。根据当前国家关于信息安全保障的相关政策标准，结合本次咨询项目的具体情况，以及多年安全工作的经验，制定信息安全技术发展路线图。此规划能够满足当前的安全需求，适应今后的发展，指导未来三至五年的安全项目建设，以保证集团信息系统安全建设的连续性、前瞻性、先进性和可靠性。 |
| 安全加固 | 对网络结构中的高危项进行整改，确保系统中不存在高危风险项。访问控制层面的问题解决后，需要对网络结构中的安全审计、边界完整性检查、入侵防范和恶意代码防护等测评项进行整改。网络设备方面，根据等级保护要求的安全配置进行整改，包括网络设备和网络安全设备的基础安全配置，如用户口令的复杂度要求、登陆失败处理功能、登陆超时功能、远程管理协议、审计功能等。对主机安全的基础配置进行调整，包括访问控制、本地安全策略、审计功能、超时自动结束会话功能等安全基线配置的整改和加固。 |
| 定期安全巡检服务 | 有效的开展日常的维护，及时发现信息系统中可能存在的故障隐患。定期的出具巡检报告，发现巡检中网络设备、操作系统中的安全隐患，并且给出解决建议，保障信息系统的稳定性和业务的连续性。 |
| 漏洞扫描补丁更新 | 通过对主机操作系统、web应用漏洞、弱密码漏洞扫描，可以对于系统中存在的操作系统漏洞进行发现，并且根据扫描报告给出的修复建议进行对应的补丁安装或者软件版本更新。Web应用方面的漏洞则需要开发人员和运维人员共同进行修复。如若存在弱口令，则需要对口令进行重新设置。在每次扫描结束后，出具对应的扫描报告，并且及时更新漏洞补丁，确保单位的信息系统在发现漏洞后，能够有效的处理，确保信息系统的安全。 |
| 服务方式 | 每个月1次现场服务，提供服务报告，共计3年 |

**四、服务以及培训要求**

★（1）**服务承诺：**

所有新购设备中标后签订合同前提供不低于三年的原厂商服务承诺函证明文件。服务承诺函包含如下内容：所有产品的服务开始时间必须以项目验收之日起计算，并且产品注册的最终用户名称和招标文件对应，安全产品厂商提供针对本次项目的攻防演练服务为期一周，备份产品厂商需要提供原厂的备份演练服务。承诺所有产品截图文件和后期供货设备功能对应，否则有权追究责任。所有服务承诺加盖投标人公章。

## （2）服务响应要求

2.1投标人除了提供原厂的保修之外还需提供3年7×24小时运维服务，以及现场维保服务。

2.2投标人在服务期内负责对硬件设备及数据库出现的故障进行故障定位，故障排除，保修和技术支持。服务的级别为7×24小时现场，故障响应时间不超过半小时，故障响应后3小时内工程师到达现场。由投标人提供维护服务的设备投标人有偿提供的维修所需部件和材料。投标人提供的维修配件、易损件等零配件，保证这些部件和材料是通过合法途径购置并具有良好品质，确保设备更换后恢复正常运行。故障排除产生的一切费用由投标人承担。

2.3服务期内若出现故障且投标人的技术能力不能满足其工作需要，招标人有权立即请原厂商或第三方公司提供服务，由此而产生的所有费用由投标人承担。

2.4为保证核心系统安全，投标人需充分了解招标人的机房设备运行情况，并参加项目现场踏勘，若未进行项目现场踏勘的，投标人的投标文件可能会被拒绝。

## （3）常规巡检要求

投标人每季度进行硬件设备及数据库常规巡检保养服务，于每个自然月的最后10个工作日内完成。投标人提供法定节假日以及重大活动（由采购人制定并提前告知）的节前巡检服务，在每个法定节假日及重大活动前3个自然日内完成。常规巡检和节前巡检安排不得重合或过于接近。投标人应事先规划巡检安排，征得招标人同意后方可进行常规巡检及保养服务。

## （4）硬件设备运维要求

检查服务器存储是否正常运行，是否有指示硬件故障报警；检查操作系统，通过查看系统日志等方式分析判断系统的运行状况；检查CPU、内存、磁盘、网络等的使用情况，记录异常信息；在不影响设备及系统正常运行的前提下，清理磁盘的系统垃圾文件；分析判断服务器可能存在的故障隐患及原因，第一时间向采购人提出修复、改善建议；微码升级；扫描系统漏洞，征求采购人意见后更新操作系统补丁。

检查安全设备性能、硬件故障、检查相关安全设备的安全策略以及防护日志，提供合理建议以供甲方参考。

（5）服务人员要求

投标人提供的机房运维服务人员须满足招标人运行维护要求，需确保人员固定，如有人员变动需书面提交变更原因，且变更后人员资质不低于原运维服务人员。招标人有权根据资质、考核评价条件等标准提出更换人员，直至人员能真正满足运行维护要求。如果书面提交人员更换超过三次，招标人有权提前无偿终止合同。

投标人根据现有机房硬件设备、数据库实际情况，提供专业设备、工具等，选取有资质的专业人员组建运维团队，定期对服务器、存储设备、数据库进行检查，及时发现并处置相关故障。

硬件维保人员要求：应具有3年以上与本次服务有关服务器、存储设备的维护服务经验，需派遣维护人员不少于1名服务器认证工程师，1名网络工程师，且常规巡检及故障处理时至少有1人到现场（签订合同时需提供相关证书以及社保证明）。

（6）文档管理要求

投标人在服务期间需提供以下报告：

资产清单：投标人应对本次项目运维的设备进行资产登记、梳理和标识，建立台帐，编制资产清单，做好设备变更维护工作。资产清单信息主要包括：机柜号、机柜位置、购置时间、过保时间、设备高度、设备型号、操作系统、IP地址、设备应用、配置项目、责任人等。投标人应及时做好资产变动管理，对机房内设备及材料变更、设备配置变更等做好记录。

常规巡检报告：投标人每季度进行二次常规巡检，结束后一周内应将巡检操作事项及巡检结果等做出常规巡检记录报告提交招标人，针对发现的问题提出优化改善建议。

现场维修服务单：投标人运维服务人员在进行每一次现场服务时需填写《现场维修服务单》，详细记录故障描述、故障分析、处理方法、处理结果、预防措施等，涉及硬件设备故障处理还需记录维修设备的序列号等相关信息。

其他文档：硬件设备运维合理化建议。

投标人需要根据数据中心的特点，做好运维过程的所有文档的记录和归档工作，包括各种形式的服务总结、工作汇报、技术方案等，每年汇总一次，按照相关要求装订成册，提交给招标人。

（7）安全管理要求

7.1投标人必须服从招标人的各项管理规定和要求。

7.2投标人保证服务期内所使用的故障诊断软件、管理软件等相关软件是通过合法途径取得，投标人承担使用这些软件所带来的的版权、许可证等所有法律责任，一旦与第三方发生法律纠纷均与招标人方无关。

7.3投标人项目所有项目服务人员需与招标人签订《保密承诺书》。

（8）备品备件要求

8.1投标人承诺建立备件库，对维保范围涉及设备提供免费硬件更换服务。

8.2备品备件服务要求（中标后立即提供）。

8.3投标人需保证所提供的配件为原厂全新配件，需保证涉及维保设备的硬件都能够得到及时、准确的维修。

8.4如遇配件供给时间或故障问题复杂导致解决时间超过48小时，必要时需提供备机以保证业务系统正常运转，如甲方情况紧急，需要在甲方要求的时间内提供备用机器。

（9）培训要求

1.中标供应商应制定详细的培训方案，培训内容应涵盖服务器、存储、备份以及安全设备。培训时长、培训人数和培训地点由采购人确定。应由有多年系统开发经验的人员担任培训教师。

2.系统培训：对系统管理员进行培训，以系统管理员能熟练使用该系统为合格标准。

应用培训：面向系统管理员和应用编程人员。

3.现场工作培训：在安装过程中对有关人员进行有关设备安装、调试以及维护进行培训。

4.培训教材：提供PDF或DOC格式的中文或英文教材并提供可打印的电子版（PDF或DOC格式）和浏览器使用的电子版（html）。

**注：本次采购全部内容为“交钥匙”工程，所有的费用等均包含在报价内；请各投标供应商认真考虑各种风险。除合同另有规定之外，采购人不再另行支付。**

# 第五章 评标方法及评标标准

**一、评标方法**

本项目采用综合评分法，评委会将对确定为实质性响应招标文件要求的投标文件进行评价和比较。评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列，投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

**二、评标标准**

|  |  |
| --- | --- |
| 项目 | 评分标准 |
| 价格（30分) | 采用低价优先法计算，以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，其价格为满分30分。其他投标人的价格分统一按照下列公式计算：投标报价得分＝（评标基准价/投标报价）×30×100%。（保留两位小数）注：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报价，有可能影响产品质量或者不能诚信履约的，且投标人不能在评标现场合理的时间内证明其报价合理性的，评标委员会有权将其作为无效投标处理。 |
| 设备参数评价（40分） | 根据投标人提供的设备功能、参数响应情况及《详细配置一览表》、《技术要求响应及偏离表》等，结合投标人提供的相关厂商彩页、产品截图或检测检验报告（如有）等，就其对各设备的理解是否响应招标文件要求，功能是否合理、参数是否响应、设备性能是否满足进行详细评审，所投产品完全实质性响应招标文件要求的得40分。如果加“★”参数如出现负偏离，每个扣2分，扣完为止；如果非“★”参数如出现负偏离但能基本满足要求的每项少得1分，扣完为止。本项最低得0分。 |
| 业绩（5分） | 根据投标人提供的2018年1月1日以来类似项目成功案例（须包含安全设备）。考察成功案例的内容、性质，涵盖或与本项目要求基本一致的，每有一个得1分，最多得5分。考察成功案例的内容、性质如与本项目要求部分一致的，每有一个得0.5分，最多得1.5分。注：须提供有效的合同、清单、验收材料复印件加盖投标人公章，缺一不可，否则不得分。 |
| 项目前期勘查（3分） | 为了保证投标人对项目整体需求完全了解，投标人需在招标前对现场踏勘，提供项目调研服务，并且提供相关证明材料需甲方签字，满足得3分，未提供不得分。 |
| 实施方案评价（7分） | 根据投标人提供的项目施工组织方案,包括但不限于：项目实施的具体进度（货物运输、装卸、安装调试、时间进度、测试）、目标管理措施、安装方案、现状分析、整体规划、实施步骤等，方案完整、科学、合理，能够完全响应上述要求的得满分7分，方案稍有欠缺的得5分，有明显欠缺的得3分，未提供不得分。 |
| 验收方案评价（5分） | 根据投标人提供的项目验收方案，包括但不限于：验收内容、验收标准等。方案完整、科学、合理，能够完全响应上述要求的得满分5分，方案稍有欠缺的得3分，有明显欠缺的得1分，未提供不得分。 |
| 培训方案评价（5分） | 根据投标人提供的培训方案，包括但不限于：培训计划、培训内容、授课人员、招标文件服务要求中关于培训的要求等。方案完整、科学、合理，能够完全响应上述要求的得满分5分，方案稍有欠缺的得3分，有明显欠缺的得1分，未提供不得分。 |
| 售后服务方案评价（5分） | 根据投标人提供的售后服务方案，包括但不限于：服务方式、服务内容、问题故障的处理方法、完善的服务体系（地点、服务电话、相关制度等）、有完整的机构信息、技术人员、技术支持方案、售后服务的方式、响应时间等。方案完整、科学、合理，能够完全响应上述要求的得满分5分，方案稍有欠缺的得3分，有明显欠缺的得1分，未提供不得分。 |

#

# 第六章 投标文件格式

**投 标 文 件**

**项 目 名 称：**扬州市民卡有限责任公司硬件及服务采购项目

**编 号：**JSHCZB-2022071号

 **投标人名称 ：**

 **日 期 ：**

**评分索引表**

|  |  |
| --- | --- |
| **评分项目** | **在投标文件中的页码位置** |
|  |  |
|  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |
|  |  |
|  |  |
|  |  |
|  |
|  |  |
|  |  |

**投标主要文件目录**

一、资格性和符合性检查响应对照表

**二**、资信证明文件

三、开标一览表

四**、**投标配置与分项报价表

五、供货一览表

六、技术参数响应及偏离表

七、商务条款响应及偏离表

1. 现场勘查确认函
2. ……

**一、资格性和符合性检查响应对照表**

投标人全称（加盖公章）：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **资格性和符合性检查响应内容** | **是否响应****（填是或者否）** | **投标文件中的****页码位置** |
| ***1*** |  |  |  |
| *2* |  |  |  |
| *3* |  |  |  |
| *4* |  |  |  |
| *5* |  |  |  |
| *6* |  |  |  |
| *7* | *招标文件中的其他实质性要求* |  |  |

1. **资信证明文件要求**

**1、符合政府采购法律法规规定的条件目录**

*（1）投标函****(原件)***

*（2） 资格声明****(原件)***

*（3） 若法定代表人参加投标的，须提供本人身份证****复印件(原件备查)****；若授权*

*代表参加的，须提供《法人授权书》****原件和****授权代表身份证复印件****（原件备查）****；*

*（4） 营业执照副本****(复印件加盖投标人公章)***

*（5） 依法缴纳职工社会保障资金的证明材料****(复印件加盖投标人公章)****(税务、银行或社会保险基金管理部门出具的连续三个月（2021年11月-2022年1月）缴纳职工社会保障资金的缴款凭证或缴款证明)*

*（6）投标人近三个月内任意一个月（2021年11月-2022年1月）依法纳税的缴款凭证(复印件加盖投标人公章)*

*（7） 与第（6）条相对应的纳税申报表或经会计师事务所审计的2020年度财务报告（成立不满一年不需提供）****(复印件加盖投标人公章)***

*（8）投标人参加本次政府采购活动前3年内在经营活动中没有重大违法记录的书面声明****（原件）***

*（9）供应商未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”(www.ccgp.gov.cn)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（提供网页查询截图并加盖供应商公章，查询时间为 2022年1月26后 ）；*

*（10）供应商信用承诺书****（原件）****。*

注一：如参加本项目的供应商为个体工商户、自然人或事业法人等非企业法人，则无

需提供上述 5-7 项，本文件中所需法定代表人相关材料、盖章及签字等可用供应商相关负责人的相应材料代替。

注二：投标文件的正本和副本中均须提供上述资格证明文件。资格证明文件须清晰可辨，若有缺失或不清晰，将导致投标被拒绝且不允许在开标后补正。

**2、采购人根据本项目要求规定的特定条件：/**

**3、非实质性资信证明文件目录**

格式1 《联合体协议》（接受联合体供应商的项目招标文件中请加入此格式，其他项目不需加入此格式）

**投标函格式**

致：江苏汇诚投资咨询管理有限公司

根据贵方的JSHCZB-2022071号招标文件，正式授权下述签字人\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(姓名)代表我方\_\_\_\_\_\_\_\_\_\_\_\_\_\_（投标人的名称），全权处理本次项目投标的有关事宜。

据此函，\_\_\_\_\_\_\_\_\_\_签字人兹宣布同意如下：

1.按招标文件规定的各项要求，向买方提供所需货物与服务。

2.我们完全理解贵方不一定将合同授予最低报价的投标人。

3.我们已详细审核全部招标文件及其有效补充文件，我们知道必须放弃提出含糊不清或误解问题的权利。

4.我们同意从规定的开标日期起遵循本投标文件，并在规定的投标有效期期满之前均具有约束力。

5.如果在开标后规定的投标有效期内撤回投标或中标后拒绝签订合同，我们的投标保证金可不予退还。

6.同意向贵方提供贵方可能另外要求的与投标有关的任何证据或资料，并保证我方已提供和将要提供的文件是真实的、准确的。

7.一旦我方中标,我方将根据招标文件的规定，严格履行合同的责任和义务,并保证在招标文件规定的时间完成项目，交付买方验收、使用。

8.与本投标有关的正式通讯地址为：

地 址：

邮 编：

电 话：

传 真：

投标人开户行：

账 户：

行 号：

法定代表人或授权代表（签字）：

投标人名称（公章）：

日 期：\_\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

**资 格 声 明**

1、名称及其它情况：

（1）投标人名称：

（2）地址： 邮编：

电话： 传真：

（3）成立和/或注册日期：

（4）法定代表人：

（5）实收资本：

（6）近期资产负债表：（到20 年12月31日）

<1> 固定资产：

<2> 流动资金：

<3> 长期负债：

<4> 短期负债：

2、近三年同类投标货物和服务的主要销售业绩（无有效联系人、联系方式和合同复印件的视为未填报本项目）：

|  |  |
| --- | --- |
| 甲方名称、联系人、联系方式 | 项 目 名 称 |
|   |   |
|   |   |

3、本次招标要求的其他资格文件以及投标人认为需要声明的其他情况：

兹证明上述声明是真实的、正确的，并提供了全部能提供的资料和数据，我们同意遵照贵方要求出示有关证明文件，如有虚假，自愿丧失中标资格，一年内退出扬州政府采购市场。

投标人公章：

法定代表人或授权代表签字：

日期： 年 月 日

**（注：资格声明为格式文件,请勿修改，否则将导致投标文件无效。）**

**法人授权书**

本授权书声明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（投标人名称）授权\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（被授权人的姓名）为我方就JSHCZB-2022071号扬州市民卡有限责任公司硬件及服务采购项目采购活动的合法代理人，以本公司名义全权处理一切与该项目采购有关的事务。

本授权书于\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日起生效，特此声明。

被授权人签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_

联系电话（手机）：

 单位名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 授权单位盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

地址：

日期：

被授权人身份证复印件：

参加本次政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明

**声 明**

我公司郑重声明：参加本次政府采购活动前 3 年内，我公司在经营活动中没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

 供应商名称（公章）：

 法定代表人或授权代表签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 日期：\_\_\_\_\_\_年 月 日

**供应商信用承诺书**

承诺主体名称：

统一社会信用代码：

为维护公平竞争、规范有序的市场秩序，营造诚实守信的信用环境，共同推进社会信用体系建设完善，树立企业诚信守法形象，本企业对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目政府采购活动郑重承诺如下:

一、对提供给注册登记部门、行业管理部门、司法部门、行业组织以及在政府采购活动中提交的所有资料的合法性、真实性、准确性和有效性负责；

二、严格按照国家法律、法规和规章开展采购活动，全面履行应尽的责任和义务，全面做到履约守信，具备《中华人民共和国政府采购法》第二十二条第一款规定的条件;

三、严格依法开展生产经营活动，主动接受行业监管，自愿接受依法开展的日常检查；违法失信经营后将自愿接受约束和惩戒，并依法承担相应责任；

四、自觉接受行政管理部门、行业组织、社会公众、新闻舆论的监督；

五、自觉做到自我约束、自我管理，不制假售假、商标侵权、虚假宣传、违约毁约、恶意逃债、偷税漏税、垄断和不正当竞争，维护经营者、消费者的合法权益；

六、提出政府采购质疑和投诉坚持依法依规、诚实信用原则，在全国范围12个月内没有三次以上查无实据的政府采购投诉；

七、严格遵守信用信息公示相关规定，向社会公示信用信息；

八、在“信用中国”和“中国政府采购网”网站中无违法违规、较重或严重失信记录；

九、如违反承诺，自愿接受管理部门依法给予的行政处罚，同意将违反承诺的行为作为不良记录记入信用档案，依法依规进行信息公示，并承担所产生的一切法律责任和经济损失。

十、本承诺书自签订之日起生效。

 （注：法定代表人或负责人、主体名称发生变更的应当重新做出承诺。）

 承诺单位（签章）：

　　　　　　　　　 　 法定代表人（负责人）：

　　　　　　　　　 　年    月    日

**三、开标一览表**

投标人全称（加盖公章）：

项目名称：扬州市民卡有限责任公司硬件及服务采购项目

项目编号：JSHCZB-2022071号

分 包 号：

|  |  |
| --- | --- |
|  投标服务名称 |  投标总报价 |
|  | 大写：小写： （人民币） |
| 备注 |  |

 日期： 年 月 日

填写说明：

*1、开标一览表必须单独密封在信封中，在投标截止时间前与投标文件分别递交，否则视为无效投标。*

*2、开标一览表必须加盖投标人公章（复印件无效）。*

3、如有分包，投标人投任何一个包的标的，都需单独填写开标一览表。

**四、投标产品配置及分项报价表**

投标人全称（加盖公章）：

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| 服务名称及规格、型号 | 数量 | 单价 | 总价 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 合计 |  |

法定代表人或授权代表签字：

**五、供货一览表**

投标人全称（加盖公章）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 货物名称 | 型 号 | 产地 | 数量 | 交货期 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

法定代表人或授权代表签字：

**六、技术参数响应及偏离表**

投标人全称（加盖公章）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 招标要求 | 投标响应 | 超出、符合或偏离 | 原因 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

法定代表人或授权代表签字：

注：1、按照基本技术要求详细填列。

2、行数不够，可自行添加。

**七、商务条款响应及偏离表**

投标人全称（加盖公章）：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 招标文件要求 | 是否响应 | 投标人的承诺或说明 |
| 质保期 |  |  |  |
| 售后技术服务要求 |  |  |  |
| 交货时间 | 合同签订后 天内 |  |  |
| 交货方式 |  |  |  |
| 交货地点 |  |  |  |
| 付款方式 |  |  |  |
| 投标货币 |  |  |  |
| 备品备件及耗材等要求 |  |  |  |
| 其他 |  |  |  |

法定代表人或授权代表签字：

**现场勘查确认函**

**投标单位参与现场勘查确认函**

|  |  |  |
| --- | --- | --- |
| **采购项目名称** |  | **第一联** |
| **采购项目编号** |  |
| **投标单位名称** |  | 加盖公章 | **采购单位留存** |
| **投标单位联系人** |  |
| **办公电话** |  |
| **传真电话** |  |
| **移动电话** |  |

……………………………**（请投标人在此加盖骑缝公章）**………………………………

**投标单位参与现场勘查确认函回执**

|  |  |  |
| --- | --- | --- |
| **采购项目名称** |  | **第二联** |
| **采购项目编号** |  |
| **投标单位名称** |  | **投标人留存** |
| **投标单位名称** |  |
| **采购单位现场勘查负责人签字** |  | 加盖公章 |
| **现场勘查时间** | 年 月 日 时 分 |