政府采购

项目名称：乳源瑶族自治县中医医院网络信息安全等级保护建设项目

项目编号：GZQS2001HC06005X

竞争性磋商文件

采购人：乳源瑶族自治县中医医院

采购代理机构：广州群生招标代理有限公司

温馨提示：供应商投标/报价特别注意事项

一、一般情况下，投标/报价截止时间前半小时将开始接收投标/报价文件，投标/报价截止时间一到，将不接收任何投标/报价文件，因此，请适当提前到达。

二、采购代理机构有可能在相近时间有多个项目进行开标，请投标/报价人授权代表到达开标会场后按指示前往相应的会议室，或主动咨询工作人员，以免错误递交投标/报价文件。

三、投标/报价供应商授权代表参加开标会的，请凭法定代表人证明及授权书、身份证原件进入开标会场。

四、请仔细检查投标/报价文件格式中应盖章、签署之处是否有按要求盖公章、签名、签署日期。投标/报价文件需签名之处必须由当事人亲笔签署,法定代表人证明及授权书需法定代表人签字或签章处，应由法定代表人亲笔签署或加盖签章。

五、采购代理机构不对供应商登记获取采购文件时提交的相关资料的真实性负责，如供应商发现相关资料被盗用或复制，或出现同一供应商由两名或以上授权代表登记的，应遵循法律途径解决，追究侵权者责任。对一家供应商递交两份投标/报价文件的，评委会将按采购文件中有关无效投标/报价的规定处理。

六、供应商在登记时提交了资料不代表其已通过资格、符合性审查，供应商应在投标/报价文件中另行提供。

七、首次参与政府采购项目的供应商请在广东省政府采购网（http://www.gdgpo.gov.cn）进行供应商注册。

八、为了提高效率，节约社会交易成本与时间，希望登记获取了采购文件而决定不参加本次投标/报价的供应商，在投标/报价文件递交截止时间的 3 日前，按《投标/报价邀请函》中的联系方式，以书面形式告知我公司。对您的支持与配合，谨此致谢。

由于交通、天气等状况、停车位已满或电梯拥挤等原因，建议投标/报价人代表提前 15-30 分钟到达开标会场，我公司所处位置有多路公共交通线路到达，具体如下：

广州市东风东路 555 号（黄华路口）粤海集团大厦 2203-2204 室。主要路经的公交车有高峰快线 12 、高峰快线 14 、2 、11 、27 、33 、54 、56 、62 、65 、74 、83 、85 、133 、185 、204 、209 、224 、224A 、261 、283 、284 、289 、293 、305 、483 和 B3、B4 等在越秀桥站下车即可到达本公司。地铁可由一号线农讲所站或五号线小北站出站后步行约 20 分钟到达，地铁站与本公司距离较远，请查好路线后再选用。

（本提示内容非采购文件的组成部分，仅为善意提醒。如有不一致，以采购文件为准。）

目　录

第一章 磋商邀请函

广州群生招标代理有限公司受采购人的委托，拟对以下项目进行竞争性磋商，欢迎符合资格条件的供应商参加。

一、采购项目编号：GZQS2001HC06005X

二、采购项目名称：乳源瑶族自治县中医医院网络信息安全等级保护建设项目

三、采购预算：110 万元

四、采购数量：1 项

五、项目内容及需求：

网络等级保护系统建设1项，项目完成时间：合同签订之日起180天完成。

（报价人必须对项目进行整体报价，不允许仅对其中部分内容进行报价。）

供应商应在报价截止前完成广东省政府采购网（www.gdgpo.gov.cn）上的供应商注册工作。

六、供应商资格：

1.供应商具备《政府采购法》第二十二条所规定的条件。提供以下材料：

（1）具有独立承担民事责任的能力（提供法人营业执照或者其他组织登记文件等证明文件，自然人的身份证明）；

（2）具有良好的商业信誉和健全的财务会计制度（提供本年度财务状况报告（未完成编制的可提供上一年度，新成立单位可提供成立至今）或基本开户行出具的资信证明）；

（3）有依法缴纳税收和社会保障资金的良好记录（提供报价截止日前 6 个月内任意 1 个月依法缴纳税收和社会保障资金的相关材料。如依法免税或不需要缴纳社会保障资金的，提供相应证明材料）；

（4）提供具有履行合同所必需的设备和专业技术能力的书面声明（填写磋商文件格式 7 资格声明函）；

（5）提供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书面声明（填写磋商文件格式 7 资格声明函）；

2. 未列入“信用中国”网站中“记录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违法失信行为”的记录名单；不处于“中国政府采购网”中“政府采购严重违法失信行为信息记录”的禁止参加政府采购活动期间（以“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网(www.ccgp.gov.cn)查询结果为准，如在上述网站查询结果均显示没有相关记录，视为没有上述不良信用记录。如相关失信记录已失效，供应商须提供相关证明资料）。

3. 已登记并获取本项目采购文件。

4. 本项目不接受联合体报价。

（登记获取文件时提供《获取文件登记表》（版本从 www.gzqunsheng.com/常用文件一栏下载））

七、符合资格的报价供应商应当在 2020 年 6 月 9 日起至 2020 年 6 月 15 日期间（办公时间内，法定节假日除外）到广州群生招标代理有限公司（详细地址：广州市东风东路 555 号粤海集团大厦 2203-2204）登记获取磋商文件，磋商文件每套售价 300 元（人民币），售后不退。

八、提交磋商响应文件截止时间：2020 年 6 月 23 日 10 时 00 分 00 秒，提交磋商响应文件时间：2020 年 6 月 23 日上午 9 时 30 分 00 秒至 10 时 00 分 00 秒

九、提交磋商响应文件地点：广州市东风东路 555 号粤海集团大厦 2204

十、磋商时间：2020 年 6 月 23 日 10 时 00 分 00 秒

十一、磋商地点：广州市东风东路 555 号粤海集团大厦 2204

十二、本公告期限（3 个工作日）自 2020-6-9 日至 2020-6-11 日止。

十三、联系事项

（一）采购单位：乳源瑶族自治县中医医院

地址：韶关市乳源县城鹰峰中路 7 号

联系人：吴先生　　联系电话：0751-5370156

（二）采购代理机构：广州群生招标代理有限公司

地址：广州市越秀区东风东路 555 号粤海集团大厦

联系人：刘小姐　　联系电话：020-83812782

传真：020-83812783　　邮编：510060

电子邮箱：gzqunsheng@gzqunsheng.com

十四、本项目的所有相关公告会在中国政府采购网(www.ccgp.gov.cn)、广东省政府采购网（www.gdgpo.gov.cn）和广州群生招标代理有限公司网站（www.gzqunsheng.com）上公布，公布之日即视为有效送达之日，不再另行通知。

十五、根据《广东省实施〈中华人民共和国政府采购法〉办法》第三十五条的规定，现将本项目采购文件进行公示，公示期为本公告期限，供应商认为磋商文件的内容损害其权益的，可以在公示期或者自期满之日起七个工作日内以书面形式向我采购代理机构提出质疑。

第二章 报价人须知

1. 总体说明

1.1. 资金来源

财政性资金。

1.2. 适用范围

本项目仅适用于本磋商文件所述的报价内容。

1.3. 合格的报价人

1.4.1 具有符合磋商邀请中合格报价人资格要求及实质性要求；

1.4.2 已在本项目登记及获取磋商文件的报价人。

1.4. 报价人应承担所有参与本次报价的全部费用。

1.5. 合格的货物和服务

1.6.1 报价人提供的所有货物及服务，其来源均应符合《中华人民共和国政府采购法》等相关法律法规的规定。

1.6.2 本项目采购本国产品。

1.6.3 采购人将拒绝接受不合格的货物和服务。

1.6. 定义

1.6.1. “采购人”系指本磋商文件报价邀请中所叙述的采购人。

1.6.2. “业主/用户”系指本项目的采购人或采购人指定的最终使用单位。

1.6.3. “采购代理机构”系指广州群生招标代理有限公司。

1.6.4. “报价人”系指向采购代理机构提交报价响应文件的供应商。

1.6.5. “报价文件”、“报价响应文件”系指报价人提交的响应本次项目的响应文件。

1.6.6. “甲方”系指采购人或采购人指定的最终使用单位。

1.6.7. “乙方”系指成交供应商。

1.6.8. “日期”指公历日，“时间”指北京时间，24 小时制。

1.6.9. “服务”系指磋商文件规定供应商须承担的相关服务。

1.6.10. “书面形式”系指纸质文件形式，除非特别说明，不包含电子邮件、手机短信等非纸质形式。

1.6.11. “不可抗力”系指战争、严重火灾、洪水、台风、地震等或其他采购人（或采购人指定的最终使用单位）、双方认定的不可抗力事件。

1.6.12. “实质性响应”系指符合磋商文件实质性要求、条款、条件和规定，且没有重大偏离或保留。重大偏离或保留指影响到磋商文件规定的范围、质量和性能，或限制采购人的权利和报价人的义务的规定，而纠正这些偏离将影响到其他递交实质性响应磋商文件的报价人的公平竞争地位。

1.6.13. 磋商文件中的标题或题名仅起引导作用，而不应该作为对磋商文件内容的理解或解释。

1.7. 知识产权

1.7.1. 报价人必须保证，采购人在中华人民共和国境内使用报价货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。如报价人不拥有相应的知识产权，则应由报价人负责获得并提供给采购人使用，其报价中必须包括合法获取该知识产权的一切相关费用，如报价人没有单独列出的，视为已包含在相应报价中。一旦使用报价人提供的产品或服务，采购人不再承担第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。

1.8. 联合体报价（如适用）

对接受联合体报价的项目：

1.8.1. 两个以上供应商可以组成一个报价联合体，以一个报价人的身份报价。

1.8.2. 联合体各方均应当符合《政府采购法》第二十二条第一款规定的条件，根据采购项目的特殊要求规定报价人特定条件的，联合体各方或按本项目要求各方中至少应当有一方符合采购人规定的特定条件。

1.8.3. 联合体各方之间应当签订共同报价协议并在报价文件内提交，明确约定联合体各方承担的工作和相应的责任。联合体各方签订共同报价协议后，不得再以自己名义单独在同一项目中报价，也不得组成新的联合体参加同一项目报价。

1.8.4. 联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。

1.8.5. 联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

1.9. 关联企业

1.9.1. 除联合体外，法定代表人或单位负责人为同一个人或者存在直接控股、管理关系的不同供应商，不得同时参加同一项目或同一子包（子项、标段等）的报价。如同时参加，则评审时将同时被拒绝。

1.9.2. 同一报价人授权不同的人员参与同一项目或同一子包（子项、标段等）的报价，则评审时将同时被拒绝。

1.10. 提供前期服务的供应商

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，不得再参加该采购项目的其他采购活动。

1.11. 须落实的政府采购政策

1.11.1. （《政府采购促进中小企业发展暂行办法》（财库〔2011〕181 号），《关于政府采购支持监狱企 业发展有关问题的通知》(财库〔2014〕68 号)，《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号)，《关于环境标志产品政府采购实施的意见》（财库〔2006〕90 号），《节能产品政府采购实施意见》的通知（财库〔2004〕185 号）。

1.11.2. 中小微企业报价是指符合《中小企业划型标准规定》的报价人，通过报价提供本企业制造的货物、承担的工程或者服务，或者提供其他中小微企业制造的货物。本项所指货物不包括使用大型企业注册商标的货物。中小微企业报价应提供《中小微企业声明函》；提供其他中小微企业制造的货物的，应同时提供制造商的《中小微企业声明函（制造商）》。

1.11.3. 根据财库〔2014〕68 号《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业报价时，提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件，不再提供《中小微企业声明函》。

1.11.4. 根据财政部、民政部、中国残疾人联合会印发的《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，残疾人福利性单位视同小微企业。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供该通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责。一旦成交将在成交公告中公告其声明函，接受社会监督。报价人提供的《残疾人福利性单位声明函》与事实不符的，依照《政府采购法》第七十七条第一款的规定追究法律责任。

1.11.5. 报价人同时为小型、微型企业、监狱企业、残疾人福利性单位任两种或以上情况的，评审中只享受一次价格扣除，不重复进行价格扣除。

1.12. 磋商文件的解释权

本磋商文件的解释权归“广州群生招标代理有限公司”所有。

2. 磋商文件

2.1. 磋商文件的组成

（1）磋商邀请

（2）报价人须知

（3）采购人需求

（4）合同文本

（5）磋商细则

（6）报价文件格式

2.2.磋商文件的澄清或修改

2.2.1. 采购人或采购代理机构对磋商文件进行必要的澄清或修改的，澄清或者修改的内容可能影响报价文件编制的，于提交首次报价文件截止之日 3 个工作日前在指定媒体上发布公告，并通知所有登记及获取磋商文件的供应商。不足上述时间的，采购代理机构在征得当时已登记及获取磋商文件的供应商同意并书面确认后（可以电子邮件或传真形式），可不改变截止时间。

2.2.2.登记及获取磋商文件的供应商在收到澄清或修改通知后应按要求以书面形式（可以电子邮件或传真形式）予以确认，该澄清或修改的内容为磋商文件的组成部分，供应商在提交首次报价文件截止时间前不予书面确认的，视为已收到通知且对内容无异议。

2.2.3.采购过程中的一切修改文件或补充文件一旦确认后与磋商文件具有同等法律效力，报价人有责任履行相应的义务。

2.2.4.报价人在规定的时间内未对磋商文件提出询问、质疑的，将视其为无异议。对磋商文件中描述有歧义或前后不一致的地方，磋商小组有权进行评判，但对同一条款的评判应适用于每个报价人。

3. 报价总则

3.1. 报价文件的编写

3.1.1. 报价人应仔细阅读磋商文件的所有内容，按磋商文件的要求制作并递交报价文件，并保证所提供的全部资料的真实性、准确性，以确保其对磋商文件做出实质性响应；否则，将拒绝其报价。报价人若提供不真实的材料，无论其材料是否重要，都将有可能直接导致报价无效，并承担由此产生的法律责任。

3.1.2. 语言和计量单位：报价文件和来往函件应用简体中文书写，报价人提供的支持文件、技术资料

和印刷的文献可以用其他语言，但相应内容应附有中文翻译文本（经公证处公证），对不同文字文本报价文件的解释发生异议的，以中文文本为准。计量单位应使用国际单位制。

3.1.3. 报价人应用人民币报价。报价文件的大写金额和小写金额不一致的，以大写金额为准；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；单价金额小数点有明显错位的，应以总价为准，并修改单价。

3.1.4. 本项目要求总报价应包括货物采购、运输、安装、调试、相关部门验收及保修期内的维护保养等所有费用，以及报价人认为必要的其他货物、材料、安装、服务；报价人应自行增加货物整体正常、合法、安全运行及使用所必需但磋商文件没有包含的所有货物、版权、专利等一切费用，如果报价人在成交并签署合同后，在供货、安装、调试、培训等工作中出现货物的任何遗漏，均由成交供应商免费提供，采购人将不再支付任何费用。

3.1.5. 报价人在编写报价文件时，应填写磋商文件要求的内容及其附件，并根据实际情况补充评审所需资料，报价文件只填写和提供了磋商文件要求的部分内容和附件，或没有提供磋商文件中所要求的全部资料及数据，或没有按实际情况提供报价所需资料的，其可能导致的结果和责任由报价人自行承担。

3.1.6. 报价人的报价明显低于其他报价，使得其报价可能低于其个别成本的，有可能影响商品质量和不能诚信履约的，磋商小组应当要求该报价人作出书面说明并提供相关证明材料。报价人不能合理说明或者不能提供相关证明材料的，由磋商小组认定该报价人以低于成本报价，其报价应作无效报价处理。

3.1.7. 采购代理机构不接受电报、电话、电传、传真等非约定形式报价。

3.2. 报价文件的构成

报价人编写的报价文件格式详见报价文件目录表。

3.2.1. **报价人应按照磋商文件的要求编制带有目录和页码并装订成册的报价文件。**

3.2.2. 报价人必须自行承担因其报价文件的任何错漏而导致的一切后果。

3.3. 报价的修改及撤回

3.3.1. 在报价截止时间前，报价人可以以书面通知的形式向采购代理机构修改或撤回其报价文件。修改后的报价文件须按照本项目规定的报价截止时间之前重新递交，否则，采购代理机构将拒绝接受修改后的报价文件。

3.3.2. 在报价截止时间后，报价人不得对其报价文件作任何修改。从报价截止时间至报价有效期满之前，报价人不允许撤回其报价文件。

4. 报价要求

4.1.报价

4.1.1. 全部报价文件应一式三份，正本一份，副本二份，副本可由正本复印而成；报价文件电子版 1 份，光盘或 U 盘介质，WORD 或 EXCEL 格式，不留密码，无病毒，内容应与报价人打印产生的纸质报价文件内容一致，如有不同，以纸质报价文件为准。除特别注明外，报价文件应提交纸质文件。如果正本与副本不符，应以正本为准。报价文件应由报价人的合法授权代表正式签署，如有任何更改应由原签署人签字。无论报价结果如何，报价人的全部报价文件均不退回。另按要求单独提交一个“报价信封”。

4.1.2. 报价人应对报价项目提供完整的详细的实施方案。

4.1.3. 所有报价文件应在报价截止时间前送达磋商文件指定地点，交予采购代理机构专职负责人,任何迟于这个时间的报价将被拒绝。

4.1.4. 所有报价文件必须封入密封的信封或包装，在封口上加盖报价单位公章，并在每一信封或包装的封面上写明：

（正本/副本/报价信封）	
收件人名称：广州群生招标代理有限公司	
项目编号：	项目名称：
报价人名称：	报价人地址：
联系人：	联系电话：

4.1.5. 采购代理机构不接受电报、电话、电传、传真、邮寄报价。

4.2. 报价有效期

从报价截止日起，报价有效期为 90 天。在特殊情况下，采购代理机构可于报价有效期满之前要求报价人同意延长有效期，要求与答复均应以书面形式。报价人可以拒绝上述要求，同意延期的报价人根据原截止期所享有的权利及其所负有的义务相应也延至新的截止期。

4.3. 报价保证金

本项目不收取报价保证金。

5. 磋商、成交与签约

详见《第五章 磋商细则》

6. 采购代理服务费

成交供应商在领取《成交通知书》之前须向采购代理机构交纳的服务费，收费标准参照中华人民共和国国家计划发展委员会颁布的《招标代理服务收费管理暂行办法》（计价格[2002]1980 号）执行。本项目类型为服务类：

（1）以《成交通知书》确定的成交总金额作为收费的计算基数，按差额定率累进法计算。

（2）成交金额的各部分费率如下表：

成交金额（万元人民币）	货物招标费率
100 以下部分	1.5%
100-500 部分	1.1%
500-1000 部分	0.8%
1000-5000 部分	0.5%
5000-10000 部分	0.25%
10000-100000 部分	0.05%
1000000 以上部分	0.01%

如某服务项目，成交金额为 600 万，总共交纳的服务费为：

总共交纳的服务费＝（100 万以下部分的服务费）+（100 万～500 万部分的服务费）+（500 万～600 万部分的服务费）

＝100 万元×1.5%+（500-100）万元×1.1%+（600-500）万元×0.8%

=1.5 万元+4.4 万元+0.8 万元＝6.7 万元

（3）币种与《成交通知书》的币种相同。

（4）成交单位中标后，必须按规定向采购代理机构直接缴交采购服务费。

（5）服务费不在报价中单列。

（6）经依法取消或放弃成交资格的，采购代理服务费不予退还。

7.询问、质疑与投诉

7.1 供应商可以向代理机构提出询问和质疑，代理机构依照相关规定就采购人委托授权范围内的事项作出答复。

7.2 供应商认为采购文件的内容损害其权益的，可以在采购文件公示期间或者自期满之日起 7 个工作日内以书面形式向采购人或代理机构提出质疑，逾期质疑无效。

7.3 供应商在法定质疑期内须一次性提出针对同一采购程序环节的质疑。

7.4 供应商认为采购过程和中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到

损害之日起 7 个工作日内，以书面形式向采购人或代理机构提出质疑，逾期质疑无效。

7.5 质疑函应当署名。质疑供应商为自然人的，应当由本人签字并以右手食指手指手印作为确认；质疑供应商为法人或者其他组织的，应当由法定代表人签字并加盖公章。质疑内容不得含有虚假、恶意成份。依照谁主张谁举证的原则，提出质疑者必须同时提交相关确凿的证据材料和注明证据的确切来源，证据来源必须合法，代理机构有权将质疑函转发质疑事项各关联方，请其作出解释说明。对捏造事实、滥用维权扰乱采购秩序的恶意质疑者，将上报政府采购监督管理部门依法处理。

7.6 质疑供应商对采购人、代理机构的质疑答复不满意，或者采购人、代理机构未在规定期限内作出答复的，可以在答复期满后 15 个工作日内向采购人的同级政府采购监督管理部门提起投诉。

7.7 询问及质疑函应按相应格式进行填写及签署，并递交书面文件至代理机构，没有签署的质疑函将不予受理。具体格式详见 http://www.gzqunsheng.com/常用文件一栏。

7.8 询问、质疑受理单位：广州群生招标代理有限公司，联系电话：（020）83812782 或（020）83812935，投诉受理单位：韶关市政府采购监管处。

第三章 采购人需求

一、项目概况

本项目就以下内容进行竞争性磋商：

内容	数量	最高限价	项目完成时间
网络等级保护系统建设	1 项	110 万元	合同签订之日起 180 天完成

★注：第一次报价超出最高限价的将被视为无效报价，不能参加磋商。

项目清单：

序号	名称	数量	单位
1	HIS 系统等保三级测评	1	项
2	LIS 系统等保二级测评	1	项
3	PACS 系统等保二级测评	1	项
4	互联网边界防火墙	1	台
5	数据库中心防火墙	1	台
6	终端管控系统	1	套
7	准入控制系统	1	台
8	防病毒系统	1	套
9	运维堡垒机	1	台
10	日志审计系统	1	台
11	数据库审计系统	1	台
12	服务器	1	台
13	机柜	2	台
14	网络及系统的等保改造服务	1	项
15	等保管理制度梳理建立	1	年
16	安全培训服务	1	年

二、项目总体要求

1.报价人必须对用户需求书的技术参数、性能、材质等条款一一响应；

2.投标设备能满足招标文件要求，具备稳定、先进、可靠性；

3.投标设备的制造商具有稳定供货渠道，货源充足，供货安排科学高效；

4.报价人必须对安装、调试、验收方案及质保期、维护保养、应急维修时间安排等售后服务做出全面、

具体、合理的承诺。

三、技术要求

（1）互联网边界防火墙

指标项	指标要求
硬件规格性能	▲标准 1U 设备，千兆电口≥6 个，万兆光口≥2 个，扩展槽≥2 个，支持扩展≥8 个千兆电口/8 个千兆光口/4 电 4 光/4 个万兆口，接口定义 WAN 和 LAN 无限制，具备入侵防御模块、防病毒模块、应用识别模块、VPN 模块；提供 IPS 特征库、防病毒特征库、应用识别及 URL 分类库三年升级服务及三年硬件维保服务。
	▲整机吞吐≥8G，最大并发连接数≥650 万，新建连接数≥11 万。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
基础功能要求	▲支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。提供虚拟化防火墙 CPU、内存、硬盘配置截图。
	每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6 双栈等。
	开通 SSL VPN 功能，产品配置 SSL VPN 并发用户数不少于 200 个。
	开通网络入侵防御功能，系统默认自带 IPS 规则库≥4000 条。
	开通网络应用识别功能，系统默认自带应用识别≥1600 种。
	▲开通网络防病毒功能，系统默认自带防病毒库≥1200 万条；提供界面截图证明。
访问控制	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。
	支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
	支持路由、透明及混合部署模式
	支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路；提供界面截图证明。
	支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响；提供界

	面截图证明。
入侵防御	▲系统基于 SQL 注入、CC 攻击检测、注入攻击的规则的防御方式，提供自主知识产权关于 SQL 注入漏洞检测方法及系统、检测和防御 CC 攻击的方法及装置、一种脚本注入攻击检测方法和系统证明文件。
	▲具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CVE 漏洞发现数不低于 600 个。提供自主挖掘 CVE 列表。
	支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。
	具备协议自动识别功能；支持自定义事件功能；
APT 功能	支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。
	▲可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。
	内置多种沙箱环境与应用环境，使用反沙箱、时光加速、机器学习等领先技术，确保恶意样本逃逸率大幅降低。
威胁情报防护	支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。
安全可靠	通过国家信息安全测评信息技术产品安全测评 EAL4+，提供证明材料。
网络特性	支持静态路由、动态路由（RIP、OSPF、BGP4）。
	支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。
	支持专业链路负载均衡，提供轮询、加权轮询、哈希等 4 种及以上负载均衡算法；提供界面截图证明。
	支持通过ICMP、TCP、DNS、FDP、RADIUS、POP3、HTTP、HTTPS、UDP、LDAP、ORACLE、MSSQL、MYSQL等十五种以上协议，实现对链路可用性的多重健康检查；提供界面截图证明。
	支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT
	支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL＊NET
	支持标准 DHCP 服务功能，支持 DHCP 条件下的 IP/MAC 绑定及 IP 地址排除等功能。
	支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS

	服务器，且支持多台 DNS 服务器的负载均衡。
	支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A、NS、CNMAE、TXT、MX、PTR 等七种或以上记录方式；提供界面截图证明。
高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
	支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑。
	支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断。
系统管理	支持基于 WEB 和命令行的设备管理模式,WEB 界面和命令行模式下均可实现对设备所有功能的管理配置。
	支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的 TOP10 统计展示、基于具体威胁事件/威胁类型的 TOP10 统计展示等，统计展示的时间周期包括 1 小时/1 天/7 天/30 天。
	支持基于流量的 TOP100 用户和 TOP100 应用的流量曲线图，流量曲线图的统计周期包括小时、天、7 天和 30 天。
	支持基于并发会话数量的 TOP100 用户和 TOP100 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。
集中管理	支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。
	支持扩展集中策略分析模块，通过集中策略分析模块，实现：集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置；集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的。集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。提供上述功能截图。
资质服务要求	具备计算机信息系统安全专用产品销售许可证-增强级；提供有效的资质证明复印件。
	具备中国国家信息安全产品认证证书；提供有效的资质证明复印件。
	具备国家信息安全测评自主原创产品测评证书；提供有效的资质证明复印件。
	▲具备国家信息安全测评信息技术产品安全测评 EAL4+，提供证明材料。
	具备 IPv6 Ready logo Phrase 2 认证；提供有效的资质证明复印件。
厂商资质	所投产品厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CNNVD 漏洞发现数不低于 30 个。提供自主挖掘 CNNVD 证书证明。

	▲所投产品厂商为微软 MAPP 成员单位，提前收到安全漏洞信息，安全产品更有效的、更快地提供安全保护；提供官方 MAPP 证明文件。
	所投产品厂商具备工业信息安全测试评估机构能力认证证书（二级）；提供有效的资质证明复印件。
	所投产品厂商具备信息安全相关专利技术，提供自主知识产权颁发的相关技术数不低于 100 个。提供列表证明。
	▲为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级）。提供有效的资质证明复印件。
	所投产品厂商具备入围 2018 中国软件和信息技术服务综合竞争力百强企业名单。提供有效的证明文件复印件。

（2）数据中心防火墙

指标项	指标要求
硬件规格性能	▲标准 1U 设备，双冗余电源，千兆电口≥6 个，扩展槽≥1 个，支持扩展≥8 个千兆电口/8 个千兆光口/4 电 4 光/4 个万兆口，接口定义 WAN 和 LAN 无限制，具备入侵防御模块，提供三年入侵防御升级及三年硬件维保服务。
	▲整机吞吐≥6G，最大并发连接数≥500 万，新建连接数≥10 万。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
基础功能要求	▲支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。提供虚拟化防火墙 CPU、内存、硬盘配置截图。
	每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6 双栈等。
	开通 SSL VPN 功能，产品配置 SSL VPN 并发用户数不少于 200 个。
	开通网络入侵防御功能，系统默认自带 IPS 规则库≥4000 条。
	开通网络应用识别功能，系统默认自带应用识别≥1600 种。
	▲开通网络防病毒功能，系统默认自带防病毒库≥1200 万条；提供界面截图证明。
访问控	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。

制	支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
	支持路由、透明及混合部署模式
	支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路；提供界面截图证明。
	支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响；提供界面截图证明。
入侵防御	▲系统基于 SQL 注入、CC 攻击检测、注入攻击的规则的防御方式，提供自主知识产权关于 SQL 注入漏洞检测方法及系统、检测和防御 CC 攻击的方法及装置、一种脚本注入攻击检测方法和系统证明文件。
	▲具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CVE 漏洞发现数不低于 600 个。提供自主挖掘 CVE 列表。
	支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。
	具备协议自动识别功能；支持自定义事件功能；
APT 功能	支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。
	▲可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。
	内置多种沙箱环境与应用环境，使用反沙箱、时光加速、机器学习等领先技术，确保恶意样本逃逸率大幅降低。
威胁情报防护	支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。
安全可靠	通过国家信息安全测评信息技术产品安全测评 EAL4+，提供证明材料。
网络特性	支持静态路由、动态路由（RIP、OSPF、BGP4）。
	支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。
	支持专业链路负载均衡，提供轮询、加权轮询、哈希等 4 种及以上负载均衡算法；提供界面截图证明。

	支持通过ICMP、TCP、DNS、FDP、RADIUS、POP3、HTTP、HTTPS、UDP、LDAP、ORACLE、MSSQL、MYSQL等十五种以上协议，实现对链路可用性的多重健康检查；提供界面截图证明。
	支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT
	支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL＊NET
	支持标准 DHCP 服务功能，支持 DHCP 条件下的 IP/MAC 绑定及 IP 地址排除等功能。
	支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。
	支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A、NS、CNMAE、TXT、MX、PTR 等七种及以上记录方式；提供界面截图证明。
高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
	支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑。
	支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断。
系统管理	支持基于 WEB 和命令行的设备管理模式,WEB 界面和命令行模式下均可实现对设备所有功能的管理配置。
	支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的 TOP10 统计展示、基于具体威胁事件/威胁类型的 TOP10 统计展示等，统计展示的时间周期包括 1 小时/1 天/7 天/30 天。
	支持基于流量的 TOP100 用户和 TOP100 应用的流量曲线图，流量曲线图的统计周期包括小时、天、7 天和 30 天。
	支持基于并发会话数量的 TOP100 用户和 TOP100 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。
集中管理	支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。
	支持扩展集中策略分析模块，通过集中策略分析模块，实现：集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置；集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的。集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。提供上述功能截图。

资质服务要求	具备计算机信息系统安全专用产品销售许可证-增强级；提供有效的资质证明复印件。
	具备中国国家信息安全产品认证证书；提供有效的资质证明复印件。
	具备国家信息安全测评自主原创产品测评证书；提供有效的资质证明复印件。
	▲具备国家信息安全测评信息技术产品安全测评 EAL4+，提供证明材料。
	具备 IPv6 Ready logo Phrase 2 认证；提供有效的资质证明复印件。
厂商资质	所投产品厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CNNVD 漏洞发现数不低于 30 个。提供自主挖掘 CNNVD 证书证明。
	▲所投产品厂商为微软 MAPP 成员单位，提前收到安全漏洞信息，安全产品更有效的、更快地提供安全保护；提供官方 MAPP 证明文件。
	所投产品厂商具备工业信息安全测试评估机构能力认证证书（二级）；提供有效的资质证明复印件。
	所投产品厂商具备信息安全相关专利技术，提供自主知识产权颁发的相关技术数不低于 100 个。提供列表证明。
	▲为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级或以上）。提供有效的资质证明复印件。
	所投产品厂商具备入围 2018 中国软件和信息技术服务综合竞争力百强企业名单。提供有效的证明文件复印件。

（3）终端管理系统

指标	规格要求
管理平台基础功能	▲桌面运维管理授权：至少 300 个终端授权，三年版本升级及硬件维保服务，三年病毒特征库升级服务。
	▲支持管理员通过 Https 方式访问 Web 控制台，管理员分级管理，不同的管理员可以授权不同的区域或部门，基于部门管理，支持面向不同的终端组织机构下发不同的策略。(提供界面截图证明)。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
	能够对终端各事件行为进行查询和统计，且支持时间、状态等条件过滤，事件支持条件过滤查询和统计，且每个事件可进行事件快照查看详细内容

	支持针对部门的系统管理员关联和授权，指定管理员有权管理的部门列表。(提供界面截图证明)。
	支持分布式多服务器架构，服务器之间可以进行负载均衡和冗余，任何一个服务器宕机都不影响其管理范围内的终端正常下载安全策略。(提供界面截图证明)。
	支持多级多服务器级联管理，实现可管理终端数无限扩展。(提供界面截图证明)。
	支持级联策略管理，上级支持给下级下发策略。数据上报，下级的报表数据可上报至上级。(提供界面截图证明)。
桌面基线管理	▲支持进程黑名单，黑名单进程支持 MD5 校验，能够有效禁止运行与工作无关的软件。防止修改进程名逃避安全检查。对于运行的黑名单进程，既可以自动结束进程，也可以只进行违规提示。 支持黑名单进程的 MD5 校验和源文件名校验。(提供界面截图证明)。
	通过检测指定注册表项的存在，检测指定注册表值的存在，检测指定的注册表项和值的匹配关系来检查是否有隐藏的木马或病毒。(提供界面截图证明)。
	支持用户帐号权限分离，可以为指定用户组添加用户组成员，也可以将指定用户从用户组中移除，方便对系统用户帐号进行有效管理。(提供界面截图证明)。
	▲能够禁用和删除 Windows 系统无用帐户，锁定和删除与设备运行、维护等与工作无关的账户，降低 Windows 系统的安全风险。(提供界面截图证明)。
	▲支持基于字典的弱密码检测功能。可进行禁用状态下的弱密码检测，可根据检测结果设置终端安全状态。(提供界面截图证明)。
	可以通过下发屏保策略，启用或关闭终端屏保功能。可以设置屏保恢复时显示登陆界面,可以设置 Windows 当前登陆密码不为空,并可以设置启用屏保的等待时间。(提供界面截图证明)。
桌面运维管理	能够通过客户端注册自动绑定计算机所属部门、使用人等信息。实现终端资产与终端用户实名管理。(提供界面截图证明)。
	支持离线补丁升级，对不能连接互联网的网络环境，可以使用工具对补丁分发信息及文件进行导入。(提供界面截图证明)。
	补丁分发支持支持在空闲时进行补丁分发,也支持在指定的时间段内进行补丁分发，最低限度降低补丁分发对网络带宽的影响。(提供界面截图证明)。
	软件分发支持断点续传，软件分发支持流量控制。(提供界面截图证明)。
	支持对计算机 USB、并口、串口、红外、蓝牙、软驱、光驱、WLAN、1394、PCMCIA 卡、MODEM 等外设的启用及禁用。(提供界面截图证明)。
	能够识别 USB 移动硬盘、业务卡、USB 鼠标/键盘等 USB 设备，并分别设置控制策略。(提供界面截图证明)。

	能够单独禁用未知类型的外部设备，也可以禁用所有外部设备，然后只选择启用某些指定的外部设备。
	能够支持无线可信 SSID 管理，支持终端只能连接指定的 SSID，不在可信列表中的无线 SSID 不允许连接。(提供界面截图证明)。
	简明可靠的多网卡非法外联管理，可以设定只有与策略系统通讯的网卡才能发送和接收数据，禁止其他任何网卡发送和接收数据，包括多网卡、拨号连接，VPN 连接等。避免通过注册表设置禁用多网卡、拨号连接而易被破解。(提供界面截图证明)。
	▲能够为终端设定自动关机的条件，一旦条件符合，终端将自动关机，方便管理员对无人值守或者长期空闲的机器进行关机处理。(提供界面截图证明)。
安全防护	能够对终端访问的目的地址、服务以及发起访问的进程进行管理，只有允许的进程才能对指定目的地址和服务进行访问。(提供界面截图证明)。
	能够对终端接受访问的源地址、接受访问的服务以及接受访问的进程进行管理，只有允许的进程才能接受指定的访问者对指定服务的访问。(提供界面截图证明)。
	如果安全状态不符合要求，能够禁止终端进程访问网络，或者接受访问。(提供界面截图证明)。
	在客户端上实时监控每个远端端口、本端端口、目标地址的流量，实时自动抑制异常流量，自动限制超过阈值的流量，将蠕虫病毒或非业务流量对网络的影响减到最小。对不同端口和地址能够设置不同的流量限制规则。
	TCP 连接监控，保证客户端上每个进程的 TCP 同时连接数和单位时间内的连接数不超过指定的值。如果超过指定的值系统将被告警并禁止新的连接，TCP 连接白名单，对客户端上指定进程的 TCP 连接行为不予限制，提供截图证明。
	监控 UDP 的发包行为，保证客户端上每个进程在单位时间内发包总数和目标总数不超过指定的值。如果超过指定的值系统自动拦截该进程的网络访问并告警。
终端资产管理	支持对终端软硬件资产进行全面的管理，包括软硬件资产信息收集，报表汇总展现功能，当计算机终端关键硬件发生变化时，能够自动提供资产变更报警。
	可以实现对终端的硬件资产分布情况进行分析，包括硬盘大小、型号，内存大小、型号，CPU 大小、型号等信息的按日期分析功能，并支持按部门分别统计以上终端的分析内容。(提供界面截图证明)。支持以上数据按照分布图、趋势图、详细信息的展示方式，并支持导出、打印等功能。
	能够通过客户端注册自动绑定计算机所属部门、使用人等信息，并能通过后台自定义终端信息（包括固定资产编号、终端位置和联系电话等），实现终端资产与终端用户实名管理。
终端审计管理	能够对终端的非法外联行为进行监控和告警，一旦探测发现终端发生非法外联行为，即可根据设定的告警对象和告警方式，进行告警，直至非法外联行为中止后才会解除，提供截图证明。

	支持多种方式对非法外联行为进行审计和告警，告警方式包括：终端提示，上报告警事件及电子邮件告警，支持同时对多个用户发送告警信息。(提供界面截图证明)。
	支持离线审计策略，对指定进程操作进行审计和阻断。(提供界面截图证明)。
	对终端用户的打印行为进行审计，并可禁止终端的打印行为。
	审计终端用户上网行为，并能设置上网白名单和黑名单，即只能访问的网站和禁止访问的网站，控制终端通过 http 代理上网，规范上网行为。(提供界面截图证明)。
准入及审计控制	可以对使用浏览器进行访问的终端，通过浏览器进行友好提示，引导终端用户完成客户端的自助安装。(提供界面截图证明)。
	能够通过与支持 802.1x 协议的接入交换机互动，实现有线局域网网络准入，对接入的计算机及接入的用户进行认证。支持华为、H3C、3Com、Cisco 等主流网络设备，提供截图证明。
	▲支持无线网络的网络准入控制，能够接管所有支持 WPA 企业版的无线接入设备类型， 对通过无线网络接入的终端和用户进行准入控制认证。(提供界面截图证明)。
	▲HTTP 外发：基于协议识别，能够审计或阻止通过 Web 邮箱、博客、微博、论坛等网页形式发送文字的行为上报外发文字包含指定敏感信息等敏感信息的网页。(提供界面截图证明)。
	▲FTP：基于协议识别，能够审计 FTP 客户端外发敏感信息文件的行为，审计或阻止包含指定敏感信息的文件外发，基于协议识别，能够强制禁止 SFTP 协议。(提供界面截图证明)。
	▲审核申请信息以邮件的方式通知审核员,审核员与系统管理员独立权限管理,提交授权支持部门分级管理。(提供界面截图证明)。
	支持备份文件与事件相关联，支持对查看备份的授权处理。(提供界面截图证明)。
报表统计管理	在线状态分析：通过在线状态分析功能，可以对入网终端的在线情况进行分析，包括在线终端、离线终端、长期离线终端的按日期分析功能，并支持按部门分别统计以上终端的分析内容。
	测评状态分析：通过测评状态分析功能，可以按日期结合终端在线率对全网合格与不合格入网终端进行综合分析。
	入网风险分析：通过入网分析功能，可以按日期对全网终端分部门的入网状况进行综合分析，分析内容包括直接批准、通讯隔离的终端情况，通过对这些数据的综合分析。
	违规事件分析：通过违规事件分析功能，可以按日期对全网终端的违规事件进行分析，包括硬件变化、存储介质使用、非法外联、系统漏洞、ARP 攻击等内容，同时支持按部门分别统计以上终端的分析内容。
	全网安全趋势：通过全网安全趋势功能，可以按日期对网内具有安全隐患的用户进

	行趋势分析，隐患项目包括违规用户、测评未通过用户、非法接入用户信息，通过对这些数据的综合分析，便于管理员及时掌握网内安全趋势。
	硬件信息分析：通过硬件信息分析功能，可以实现对入网终端的硬件资产分布情况进行分析，包括硬盘大小、型号，内存大小、型号，CPU 大小、型号等信息的按日期分析功能，并支持按部门分别统计以上终端的分析内容。
	软件信息分析：通过软件信息分析功能，可以实现对入网终端的软件安装分布情况进行分析，包括操作系统、杀毒软件分布等软件资产的按日期分析功能，并支持按部门分别统计以上终端的分析内容。
	补丁安装情况：通过补丁分析功能，可实实现对入网终端补丁情况进行分析，包括补丁更新进度，未完成补丁更新终端和查看已经完成补丁安装终端情况。
资质	所投产品具备计算机信息系统安全专用产品销售许可证。需提供有效资质证明复印件。
	所投产品具备涉密信息系统产品检测证书。需提供有效资质证明复印件。
	▲所投产品具备国家信息安全测评信息技术产品安全测评证书 EAL2。需提供有效资质证明复印件。
	▲所投产品厂商具备国家级网络安全应急服务支撑单位资质证书。需提供有效资质证明复印件。
	▲所投产品厂商具备涉密信息系统集成甲级系统集成/软件开发资质。（需提供证明）；
	▲所投产品厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CVE 漏洞发现数不低于 500 个。提供自主挖掘 CVE 列表。
	▲所投产品厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CNNVD 漏洞发现数不低于 30 个。提供自主挖掘 CNNVD 证书证明。
	▲为保证所投产品厂商原创漏洞的能力，所投产品厂商在国家信息安全漏洞共享平台(CNVD)提交的原创漏洞数量情况。到目前为止，企业单位原创积分排名必须进入前三名，需提供 CNVD 官网的截图证明
	▲所投产品厂商具备信息安全相关专利技术，提供自主专利数不低于 100 个。提供列表证明。

（4）准入控制系统

指标项	指标要求
产品要求	须为标准机架式硬件产品，支持 Bypass 功能，当设备出现故障时，不影响业务中断。

	基于 Linux 内核，须为自主开发的 OS 安全操作系统。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
性能要求	1U 机架结构；标准配置 6 个 1000MBASE-T 接口，4 个 1000M 光口，包含管理口和 HA 口；每秒事务数（TPS)：≥3500（次/秒），最大吞吐量：≥2Gbps，最大并发连接数：3000（条） 至少提供 300 个终端设备的准入控制授权，终端安全检查授权；
双操作系统要求	▲支持双操作系统冷备，当常用系统出现故障，可以使用备用系统恢复。（功能截图）
双机要求	准入设备必须具备 HA 双机热备模式，通过心跳线实时探测，自动进行主/备模式切换。
客户端部署	▲准入设备应提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理（功能截图）
	使用客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
准入技术	支持基于802.1x的网络准入方式，包括有线环境802.1x与无线环境802.1x；
	▲准入设备支持VLAN隔离技术，实现无客户端下端口级准入控制；（功能截图）
	准入设备支持端口镜像准入技术；
	准入设备支持策略路由准入技术；
	准入设备支持DHCP准入技术；
	▲准入设备支持透明网桥方式的准入技术，并支持Bypass（功能截图）
	准入设备必须支持多种准入技术的复用，到少四种以上，如802.1x、DHCP、策略▲路由混合部署。（功能截图）
页面重定向	支持HTTP协议、HTTPS协议的页面重定向； 重定向页面支持自定义非80端口的WEB服务； 提供流程化的入网页面引导，包括但不限于身份认证、终端注册、客户端安装、检查结果等。（功能截图）
资源管理	要求可以自动关联接入设备的IP地址、MAC地址、主机名、使用人、接入端口、所属VLAN；
	要求可以自动收集终端设备，包括：终端、手机、平板、交换机，并根据设备类型自动分类；
	▲能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备。（功能截图）

IP 地址管理	能够通过图形化查看全网的在线IP地址、空闲IP地址、已分配IP地址、可用IP地址、离线IP地址等IP地址的使用状态；
	能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况；可实现用户、MAC、IP、交换机端口间的动态绑定。
网络拓扑管理	▲准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图。（功能截图）
	支持手工绘制、支持图像导出、支持拓扑图的放大缩小、支持拓扑图的全屏查看（适应屏幕）
	以交换机图表的方式显示用户、IP、MAC在交换机端口上的定位图；
	▲支持可网管型交换机面板图形化展现各接口状态（单终端、无终端、多终端、关闭状态、Trunk口）（功能截图）
Hub 管理	能够发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员；
	支持Hub下多个终端需分别认证才能入网。
移动终端管理	支持当前主流智能终端设备的安全准入控制； ▲能够提供移动终端入网的设备注册功能。（功能截图）
联动认证	支持 AD、LDAP 系统联动认证。
AD 域单点登录	能够与用户现有的 AD 域相结合，当用户登录到 AD 域后，无需二次认证即可入网，避免多次认证的繁琐流程。
本地认证	内置Radius认证服务，实现本地用户名/密码认证；
	▲支持指定的 Rdius 服务器共享密钥；（功能截图）
	支持指定Rdius认证协议包括但不限于PAP、CHAP、microsoft CHAP、microsoft CHAP2、EAP-MD5。
证书认证	▲支持数字证书认证方式，必须支持证书的本地管理和发放，实现证书签发、管理和操作。（功能截图）
短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在浏览器页面上利用短信验证码认证入网。
双因素认证	支持短信、证书、动态密码卡、CA KEY、USB KEY 等双因素认证。
动态令牌认证	支持动态令牌认证，支持硬件令牌和手机令牌。
访客管理	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长 员工可以为来宾申请来宾码，来宾使用来宾码可以接入网络；
检查策略	支持终端入网的安全基线检查、软件安全检查、账户密码安全检查、环境安全检查等检查项。

系统补丁	准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分发表等功能。 准入设备能够对补丁进行分级，分为：严重、重要、中等的类别。 能够在终端的浏览器页面显示入网终端的补丁检查情况。
防病毒软件	支持主流的杀毒软件检查，包括趋势、江民、卡巴斯基等，能够在页面显示出检查结果。
终端安全加固	支持启用或禁用 Windows 系统默认的 Guest 帐号，支持 windows 账号锁定； 支持密码策略检查、弱口令检查；
计算机健康性检测	支持对终端的系统版本、防火墙、垃圾文件、IE 主页、计算机名称等安全性配置进行检查和修复。
终端安全修复	能够提供多种修复方式，用户自行修复、自动修复。
移动存储设备管理	能够对存储介质进行只读、禁用、放行等做精细控制。
违规外联监测	能够针对3G拨号、双网卡、随身WIFI、代理等多种违规联网行为做实时检测； 支持对违规外联的终端进行告警或阻断；
	支持SSID白名单，可对连接到白名单之外的无线网络行为进行阻断。
终端资产管理	能够对全网计算机上软/硬资产进行统计，可以按照部门、名称提供精确查询以及软/硬件资产报表的导出。
	能够对终端硬件初始记录、最新记录和变动记录形成报表，并且能够查询变动的历史。
软件检查	▲支持软件安装的黑名单、白名单、红名单的检查（提供功能截图） 支持进程、服务的黑/白名单检查，支持P2P软件 检查。
主机 ACL	▲支持对终端访问的目的地址、服务以及发起访问的进程进行管理，只有允许的进程才能对指定目的地址和服务进行访问；（提供功能截图）
	▲支持对终端接受访问的源地址、接受访问的服务以及接受访问的进程进行管理，只有允许的进程才能接受指定的访问者对指定服务的访问。（提供功能截图）
哑终端发现	支持对网络中的哑终端进行主动探测识别，学习哑终端地址及指纹信息，通过主动探测与被动监听方式相结合，精准识别哑终端设备，包括打卡机、打印机、扫描仪、门禁、摄像头、车管终端等，并自动进行分类。
	▲操作系统级可识别：Windows XP、Window 7、Windows 8、Window 10、Windows Sever 2003、Windows Server 2008、Windows Server 2012以及Kylin、Ubuntu、RedHat、FreeBSD、CentOS等及部分特殊系统。（提供功能截图）
	识别哑终端指纹信息包括但不限于数据流量、流向、协议、IP、MAC、厂商、系统、类型等。
哑终端的管控	▲实时监测哑终端指纹信息的变化，当哑终端指纹信息变化时，可及时对其进行告警或阻断。（提供功能截图）
	支持针对网络流量的识别功能，发现资产及连接关系、通信协议、应用层访问指令等，并可以根据学习信息辅助生成安全访问控制规则；（提供功能截图）
行为分析画	▲支持摄像头、门禁、网络打印机、叫号机、自助查询机等各类业务终端资产的

像	行为画像；（提供功能截图）
哑终端行为分析与监测模块	▲支持根据行为模型的安全接入机制，可根据终端日常业务行为自动生成终端行为基线； （提供功能截图）
	自动判断网络中哑终端的异常行为及偏离程度，并对风险进行告警或阻断。
安全管理报表	能够展示违规检查项、违规次数统计、违规项数统计、操作系统安全检查、检查项统计、身份认证统计、安全检查趋势等展示信息； 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
报警信息	可以提供紧急、重要、次要、提示等多个级别自定义报警模式。 支持系统报警、网络报警、终端报警等报警类型， 支持报警信息通过Syslog、邮件、短信进行输出。
产品资质要求	公安部《计算机信息系统安全专用产品销售许可证》 国家版权局《计算机软件著作权登记证书》
厂商资质	▲为保证厂商原创漏洞的能力，厂商在国家信息安全漏洞共享平台(CNVD)提交的原创漏洞数量情况。到目前为止，企业单位原创积分排名必须进入前三名，需提供CNVD官网的截图证明
	▲所投产品厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的CVE漏洞发现数不低于1000个。提供自主挖掘CVE列表。
	▲为了保证所投产品厂商具备相应管理体系能力，需要具备以下体系认证证书：质量管理体系认证证书ISO9001,环境管理体系认证证书ISO14001，信息安全管理体系认证证书ISO27001

（5）防病毒系统

指标项	**指标要求**
安装部署	▲服务端：支持部署在 Windows Server 版本和主流 Linux 版本上。
	▲支持常见的 32 位和 64 位操作系统：Windows XP——Windows 10 、 Windows Server 2003——2012、主流 Linux；支持主流国产操作系统：中标麒麟、银河麒麟等。提供 10 个服务器防病毒授权，三年病毒库升级服务。
	支持多种安装方式，至少包括下载安装、远程安装、脚本登录安装和域组策略安装。
	支持通过产品部署安装包进行对全网现有反病毒软件进行统一自动卸载操作。
	支持卸载第三方不兼容软件，可以扫描网络中其它的软件或不兼容的软件并进行卸载。
	服务端安装包提供内置数据库支持，不需要额外安装诸如 SQL Server、MSDE、MySql、ACCESS 等数据库软件

功能要求	有良好的可扩展性和易用性，支持大型网络跨地域、跨网段的部署和管理，支持无限层网络架构，支持 C/S 及 B/S 两种模式对客户端进行管理。
	杀毒软件服务端具备企业内部云建设能力，可搭建私有云查杀平台，摒弃公有云，防止数据外泄，减少网络负载。
	杀毒软件服务端能对所有客户端进行集中管控，通过控制台直接给客户端发送命令，指令采用国际标准的 SSL 方式加密。
	支持标准 syslog 格式数据上报到安管平台
	自动扫描网络中不被保护的计算机，强制安装客户端，确保全网机器安全运行与完整部署。
管理能力	支持对已部署的全网各级各类终端进行集中的，统一的管控，包括各版本的 windows，linux 等。
	杀毒软件服务端能够实时监控客户端病毒查杀信息，并具备病毒日志查询与统计功能，可对网络中病毒动态进行查询统计，能按时间、按 IP 地址、机器名、按病毒名称、病毒类型进行统计查询，能将查询结果打印或导出。
	具备订制化安全策略能力，可根据企业用户环境，可自由定制个性化的终端安全防护策略，为企业打造私有云安全模型以提高计算机安全等级。
	具备使终端强制执行中控所下发策略的能力。杀毒软件服务端可以对所提供的不同系统平台以及应用系统下的防护终端进行策略配置，在配置成功后，管理员可自定义锁定客户端策略及权限，强制终端用户执行策略。
	具备提供多维度，多粒度的病毒情报展示能力，可按边界类型、病毒类型、时间范围、终端组织结构等等参数对病毒情报进行详细筛选，能对选定项进行清除或者加白，能导出报表。
审计日志	具备提供多维度，多粒度的日志汇总报表与分析报表的能力。并提供两种展示方式，图形报表和详细日志。
	图形报表：可折线图，饼状图等图表导出终端部署情况，日活统计，病毒库版本统计，病毒排名，感染情况统计等数据。
	详细日志：可展示所有终端的操作日志，通过触发原因，操作类型，操作状态，时间戳，操作员账户，终端名等搜索条件来筛选用户需要的信息，筛选完成后，可导出报表。
智能追溯	具备病毒文件审计追踪能力，可智能快速定位病毒，及早处理感染源，减少病毒爆发造成的损失。
自动升级	具备自定义病毒/软件版本升级时间能力，并且升级过程已进行智能负载均衡处理，避免占用过多内网带宽资源

定时扫描	具备自定义全网病毒查杀参数的能力。在指定的时间自动下发查杀指令至指定的终端进行病毒扫描 可配置扫描时间，扫描类型等。
发现病毒的处理方式	具备自定义病毒处理方式的能力，如通过下发查杀指令或定时扫描等方式发现了病毒，可设置是否直接自动清除
终端密码保护	具备保护终端不被非法退出或卸载的能力。用户在终端执行退出或卸载软件时，需要通过密码验证。
安全报警	具备将风险警报或者系统日志发送给管理员的能力。可在内网威胁程度满足触发条件时发送邮件告警或系统日志至指定收件人，使管理员能快速响应并处理计算机病毒。
服务器迁移	具备服务器 IP 地址迁移后，终端仍能接受管理的能力。如管理端的 IP 地址发生变动，迅速修改终端配置进行并正确的连接，确保全网终端的可控性。
自动清理	具备自动清理无效终端的能力。可自定义时间范围，自动清除长期未连接过控制中心的终端，可减少服务器冗余数据，提高管理效率。
查杀能力	杀毒软件具备基于深度学习和大数据的启发式查杀技术。
	产品须具备云端检测技术，由多款检出引擎联合工作，包含自有引擎和启发引擎。多款引擎的检出结果通过汇总给出最终的结果。每个引擎的虚拟机数量可灵活配置。
	基于多步行为判断的主动防御技术 根据样本一系列的行为特征来进行综合的风险判定，其监控和判断能力由后台的大数据训练集群支持。
	具备宏病毒查杀能力，可以准确的解析 office 所有常用版本的文档，从中抽取出宏脚本。配合多态扫描引擎，快速、准确的查出各种宏病毒。如若病毒使用加密方式（如 base64）加密，引擎也可以尽量解密。
	针对宏病毒的清除，可以细致的处理被感染的文档，将恶意代码清除而保留正常文档。清除操作的粒度可以到清除 excel 公式、宏脚本中某个函数等。
	具备压缩包查杀功能，支持 25 种解压缩格式，涵盖压缩包、安装包、文档格式解析能力。支持安装脚本级查杀，拦截流氓软件捆绑。
实时防护	对未安装的已知补丁进行防护，还支持通过系统内核加固、应用加固等手段对 0day 漏洞或未知漏洞进行防护
	具备主动防御模块，能够监控和清除来自各种途径的病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等。
	具备边界防护，对网页访问、程序下载、文件拷贝等敏感系统边界入口的实时监

	控，拦截危险文件的落地
产品更新	在与用户协定的服务期内，提供完全免费的病毒库更新和产品升级信息服务。
	在国内拥有更新服务器，以保证程序自动选择最快的更新服务器，使用最快的速度获取最新的反病毒数据库。
	反病毒软件在更新过程中遇不可抗力等意外情况下中断，在下次重新运行更新时，可使用增量更新技术，在中断之前更新的基础上继续更新，提高更新效率，节约网络流量。
	服务端更新后，能够自动迅速完成全网杀毒客户端的更新。
	要求有快速的反应能力，病毒库要求常规情况下，平均每周更新一次，反病毒更新模块允许从 Internet 或当地的服务器下载最新的反病毒数据库和组件。
	可以对反病毒数据库更新源进行定制（互联网更新服务器、本地文件夹、网络共享文件夹、内部更新站点、U 盘光盘等移动存储介质）。
产品资质	国家公安部销售许可证。(提供证明材料)
	所投产品具有《计算机软件著作权登记证书》。(提供证明材料)
	所投产品须具有计算机病毒防治产品检验中心检验报告，且评测等级为一级品。(提供证明材料)

（6）运维保垒机

指标项	指标要求
硬件规格	▲标准 1U 设备，标配≥6 个千兆电口，1 个 console 接口，具有 2 个扩展插槽,每个扩展槽支持扩展 8 个千兆电口/8 个千兆光口/4 电 4 光/2 万兆光口；物理存储≥1T，提供可管理设备数 100 个资产授权，运维用户无限制，提供三年软件版本升级及三年硬件维保服务。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
性能要求	▲字符协议并发≥1400；图形协议并发≥400。
部署方式	物理旁路，逻辑串联模式，不影响正常业务流量，并支持双机热备
	▲分布式部署：支持添加一台或多台协议代理服务器，分担审计中心性能压力；并支持通过不同的协议代理服务器节点访问不同的资源，多协议代理服

	务器节点可访问相同资源时实现自动负载均衡。提供界面截图证明。
	支持 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机
支持协议审计	字符协议：SSHv1、SSHv2、TELNET、RLOGIN；图形协议：RDP、VNC、X11；文件传输协议：FTP、SFTP
	数据库协议：支持 Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、TeraData 等数据库类型
	▲支持 web 页面防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址。提供界面截图证明。
目标资源访问方式	支持运维客户端功能，运维操作过程不依赖浏览器和 JAVA 环境。提供界面截图证明。
	支持通过堡垒机 web 页面内嵌 SSH、FTP、TELNET 运维工具访问目标资源
	支持通过堡垒机 web 页面调用本地工具访问目标资源
	支持客户端菜单模式访问：用户可通过字符菜单（TELNET、SSH 协议）或图形菜单（RDP、VNC 协议）方式选择目标服务器并进行访问
	SSH 协议支持私钥代填登录，最大程度保障运维安全。提供界面截图证明。
	RDP 协议支持剪切板、本地磁盘映射功能，所有图形协议支持自适应本地浏览器窗口大小
	▲RDP 协议支持 windows 服务端开启安全层 SSL 加密，加密级别符合 FIPS 标准，允许运行使用网络级别身份验证的远程桌面的计算机连接。提供界面截图证明。
	支持 TELNET、SSH 协议使用 SecureCRT 工具批量登录目标资源
身份认证及访问授权	基本认证：本地账号+密码认证；内置 USB-KEY 和动态口令卡，无需再单独配置服务器；短信认证（支持短信中间表和短信网关方式：中国移动 CMPP2.0 和中国联通 SGIP1.2 标准）吉大正元证书认证；北京数字证书认证；格尔证书认证；其它外部认证支持 Windows AD/RADIUS/LDAP；支持多种认证方式组合的双因素认证，可自定义组合，且每个用户可单独设置。提供界面截图证明。
	支持堡垒机双因素认证专用动态口令卡认证
	系统级账号三权分立，系统级账号包括：系统账号管理员，系统审计员，系统管理员；业务管理员以业务管理权限范围实现不同业务管理员权限的完全隔离，可设置业务管理员可管理的用户组和资源组范围。提供界面截图证明。
	从账号密码代填自动登录，使用人员不必知道服务器帐号及密码（包括

	http/https 访问的账号密码代填）支持基于角色管理的安全审计功能；提供自主知识产权关于基于角色管理的安全审计方法及系统证明文件。
	▲支持时间集管理，支持按时间集配置访问控制策略；支持 IP 集管理，支持按 IP 集配置访问控制策略。提供界面截图证明。
	运维用户多次登录失败自动锁定登录账号或账号功能
	▲支持用户忘记登录密码时，可通过邮件或短信方式获取验证码，验证通过后重置登录密码；提供界面截图证明并加盖厂商公章。
访问控制及异常告警	按用户、目标设备、系统帐号、命令集和生效时间等内容或按访问授权策略设定安全事件规则；支持指令黑白名单
	对违规或高危操作的指令（黑名单）进行日志提醒、忽略命令、阻断会话或二次审批
	支持对违规或高危指令的正则表达式设置匹配规则。提供界面截图证明。
深度解析	支持 Oracle、postgresql、sybase、mysql、sqlserver 数据库下行返回行数和 oracle 数据库变量绑定。提供界面截图证明。
用户及组管理功能	支持运维用户和用户组的管理，包括添加、修改、删除、启用/停用、移动资源和移除组成员功能
	支持运维用户账号的批量导入导出功能
	支持设置用户密码为：不能修改密码、密码永不过期、下次登录必须更改密码
	支持运维用户使用有效期配置；支持运维用户客户端 IP 和 MAC 限制。提供界面截图证明。
	支持运维用户密码策略，包括：最小密码长度、密码复杂度、密码周期、历史比对和登录锁定
操作行为记录	针对 SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录会话时间、命令执行时间、会话协议、服务端 IP、服务器端口、客户端 IP、客户端端口、操作命令、返回信息、运维用户帐号、审批用户帐号、资源账号等信息
	RDP 图形操作过程中键盘输入操作记录和鼠标点击行为记录；支持开启或关闭键盘输入审计功能；支持 RDP 窗口标题审计，并支持窗口标题内容检索定位回放；支持对剪贴板拷贝文件行为和文本信息内容的记录。提供界面截图证明。
密码管理	支持按设备、系统帐号、计划开始时间、改密周期等信息配置改密计划，到期自动执行

	随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置
	手工改密功能
	▲自动改密支持 Linux、Unix、Windows（采用 RPC 方式）、AIX 以及 Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE 的内置自身账号密码。提供界面截图证明。
	支持自动改密结果发送到指定改密计划的管理员邮箱
实时监控	实时监控当前连接发生的所有会话信息和阻断功能；实时监控审计系统 CPU、内存、磁盘的使用情况；记录审计系统自身的管理操作，保障审计系统自身安全。
	▲审计查询关键字和结果显示支持多种编码(UTF-8、Big5、EUC-JP、EUC-KR、GB2312、GB18030、ISO-8859-2、KOI8-R、KS_C_5601_1987、Shift_JIS、Window-874)，由用户自主选择；提供界面截图证明。
	以 CSV、HTML 方式生成并导出报表；管理员自定义审计报表；以日报、周报、月报的方式自动生成周期性报表
数据安全管理	支持数据备份；系统配置的导入、导出功能；配置和数据备份自动导出到 FTP 服务器
	空间自管理功能，存储空间不足时能够自动清理历史数据， 可自定义清理存储空间的阀值。提供界面截图证明。
系统管理功能	管理模式 B/S；支持自定义堡垒机自身默认端口
	页面下载系统相关软件，系统自带环境监测工具，无需手动安装产品证书及控件。提供界面截图证明。
	从 WEB 界面修改网卡 IP 设置、静态路由设置等内容，支持 IPv6。
	网口聚合功能（支持主备模式和负载模式），防止单点故障。
全局策略	限制运维用户同一时间只能从一个 IP 登录
外部扩展接口	基于 WebService 的外部系统资源同步接口。提供界面截图证明。
质量保障	▲为确保项目质量，所投产品是主流厂商产品，并且近两年(2016 年-2017 年)年市场占有率前三，提供 2017 年或 2018 年权威机构盖章的数据引用证明文件（如：IDC、CCID、Frost & Sullivan 等权威机构）。
资质服务要	产品具备计算机信息系统安全专用产品销售许可证。需提供有效资质证明复

求	印件。
	▲所投产品具备涉密信息系统产品检测证书。需提供有效资质证明复印件。
	所投产品具备中国国家信息安全产品认证证书。需提供有效资质证明复印件。
厂商资质	所投产品厂商具备工业信息安全测试评估机构能力认证证书（二级）；提供有效的资质证明复印件。
	▲所投产品厂商具备信息安全相关专利技术，提供自主专利数不低于 100 个。提供列表证明。
	▲确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成及软件开发）。需提供有效资质证明复印件。
	为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级）。提供有效的资质证明复印件。

（7）日志审计系统

指标项	指标要求
运行环境	▲标准机架式设备，配置≥6 个千兆电口，硬盘容量≥2T，提供三年硬件服务。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
	▲整机性能≥3000EPS，提供≥80 个审计对象授权。
管理范围	能对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。
支持采集方式	▲无需另外安装软件组件，审计中心即可实现新增 Oracle 数据库自身日志的采集任务【提供截图证明】、新增 SQL Server 数据库自身日志的采集任务【提供截图证明】、新增 Apache 服务器日志的采集任务【提供截图证明】、新增 Lotus Domino 的日志采集任务【提供截图证明】；新增 CheckPoint 的日志采集任务【提供截图证明】；
	针对文本格式的日志采集，支持本地文件、Windows 共享和 FTP、SFTP 获取四种采集方式。
	允许用户安装独立的日志采集器通过上述方式采集日志并转发给审计中心，支持安全日志分析；提供自主知识产权关于一种安全日志分析方法证明文件。

指标项	指标要求
部署方式	支持单级部署和级联部署，支持分布式部署。
资产管理	系统具有资产管理的功能，能够将被审计资产进行分组、分域的统一维护。
	系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点。
	在资产管理界面可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表；
工作台	工作台为用户提供了一个从用户自身业务需要出发使用本系统的快速入口。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为不同角色的用户建立不同维度的仪表板
	仪表板中的每个显示区域都能够放大、缩小、拖动；
日志传输和存储转发	日志可加密压缩传输，保证数据的完整性和机密性；
	可根据转发条件，将采集范式化后的数据转发到其他的目标地址；
	系统可以统计不同采集器和不同安全域下的设备个数并以饼图展示，统计采集器或安全域中事件量 Top10 以柱图展示，配以统计列表。
	支持加密压缩方式转发，定时转发。
日志合并	要支持对无用信息的自动合并，减少垃圾数据数量；
	可以建立日志合并规则，设定合并的时间范围。
日志分析	▲用户可自定义监视场景，每个监视场景都要以监视策略的形式进行存储，并形成一个监视树；提供截图证明。
	可以显示一段时间的动态日志移动图，能够在图上显示每个时间切片的日志数量、等级，并能够在图上显示每秒事件数；提供截图证明。
	可以手工对日志进行告警或者加入观察列表中。
	可以对选中的日志进行地图定位，包括在线定位和离线定位。
	▲可以以图形化的方式展示日志属性之间的聚合关系，显示多维事件分析图；提供截图证明。
	可以对选中的日志进行事件拓扑分析，并可视化的展示一幅描述日志之间的行为相关关系的事件拓扑图，支持海量日志关联分析；提供自主知识产权关于一种海量日志关联分析方法证明文件。

指标项	指标要求
	可以对选中日志进行视网膜视图分析，以可视化方式展示日志的源 IP 与目的 IP 分布走向；
	系统支持对日志进行柱图、饼图、堆积图、时间轴图、等级堆积图、折线图、折柱混合图等形式进行可视化的展示。
日志统计分析	系统允许管理员以统计场景的形式查看不同类型的日志信息；
	必须支持实时统计和历史统计两种模式。
	▲用户可自定义统计场景，每个统计场景都要以统计策略的形式进行存储，并形成一个统计树；提供截图证明。
日志查询	系统内置统查询策略，用户可以以策略选取方式快速进行日志查询操作；提供截图证明。
	▲用户可自定义查询条件，并以策略保存，并以树形结构进行组织，形成一个查询树；提供截图证明。
	系统支持对查询结果统计、钻取。
资源自定义	可以将日志中的 IP 地址、端口、时间等信息进行资源自定义，为规则所引用；提供截图证明。
日志告警	▲告警内容可以自定义，可以根据日志的实际情况将参数（即预定义变量）传递给命令行脚本；提供截图证明。
	▲可以自定义告警统计策略，并形成一棵统计策略树；提供截图证明。
	用户选中某条告警统计策略，就能展示某个统计图表，支持柱图、饼图、曲线图等统计表现形式。
告警抑制	▲告警抑制规则中的时间范围与合并数目可以手动进行配置，告警抑制规则可实时启用和停用；提供截图证明。
日志报表	提供内置报表模板；
	支持按照天、月度、季度、年度等时间周期生成报表；
	支持报表报告的导出，导出的格式支持 EXCEL、PDF、DOC、XML、HTML、RTF 等，支持 Office 2007 格式；系统内置报表编辑器，可以自定义报表。
	支持报表调度，即报表可设置首次生成时间和间隔生成时间，生成后可指定直接发送到接收人邮箱
	支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况；

指标项	指标要求
日志存储管理	系统应提供日志维护功能，能够自动定时备份采集上来的安全事件（日志），也支持手动备份与恢复；
	管理员可设置存储容量告警阈值；提供截图证明。
日志参考信息	▲系统内置日志参考知识库，方便用户查询不同原始日志信息的错误 ID 号和详细描述信息； 能够查看系统内置的事件库中事件类型名称及其描述信息；提供截图证明。
	▲内置 Cisco PIX 和交换机的事件编码知识库；提供截图证明。内置 Windows、Linux、Solaris、AIX 操作系统的事件 ID 知识库;提供截图证明。内置 Oracle、SQL Server、MySQL、Informix、DB2 数据库的事件编码知识库【提供截图证明】；
系统管理	可对日志采集器进行集中管理和配置；记录系统自身日志，可查询；
	可以对自身运行的 CPU、内存和磁盘空间等的使用率设置告警阈值；提供截图证明。
	支持系统时间同步,能够指定时钟服务器,确保审计系统与用户网络环境的时间保持同步；提供截图证明。
产品资质	所投产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》及《计算机软件著作权登记证书》；
	所投产品须获得国家保密局涉密信息系统安全保密测评中心《涉密信息系统产品检测证书》；
	所投产品须具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级；
	▲所投产品具有《IPv6 认证证书》
厂商资质	所投产品厂商具备国家级网络安全应急服务支撑单位资质证书。需提供有效资质证明复印件。
	▲为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级）。提供有效的资质证明复印件。
	▲所投产品厂商为微软 MAPP 成员单位，提前收到安全漏洞信息，安全产品更有效的、更快地提供安全保护；提供官方 MAPP 证明文件。
	所投产品厂商具备入围 2018 中国软件和信息技术服务综合竞争力百强企业名单。提供有效的证明文件复印件。
	为保证厂商原创漏洞的能力,厂商在国家信息安全漏洞共享平台(CNVD)提交的原创漏洞数量情况。到目前为止，企业单位原创积分排名必须进入前三名，需提供 CNVD 官网的截图证明

指标项	指标要求
	▲所投产品厂商具备 ISCCC 信息安全服务资质认证证书（信息安全风险评估服务一级服务资质）。需提供有效资质证明复印件。

（8）数据库审计系统

指标项	指标要求
硬件规格性能	▲标准机架式 2U 设备，双冗余电源，标配≥6 个千兆电口，≥4 个千兆光口。硬盘容量不低于 2T，不少于 13 个 DB 对象审计，提供三年原厂版本升级及硬件维保服务。
	▲抓包速度≥1200M/秒，审计系统审计事件每秒入库速度≥6000 条/秒；日审计量≥1 亿条。
	▲为保证系统的兼容性和维护便利性，要求所投的产品（互联网边界防火墙、数据库中心防火墙、终端管控系统、准入控制系统、运维堡垒机、日志审计系统、数据库审计系统）为同一品牌。
部署和管理	支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行。
	可 HA 部署，产品支持主备方式。
数据库审计	支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计。需提供截图证明。
	▲支持对 Oracle 数据库状态的自动监控，可监控会话数、连接进程、CPU 和内存占用率等信息；支持国产数据库人大金仓、达梦、南大通用、神通数据库的审计； 支持 MongoDB 数据库的审计； 支持对针对数据库的 XSS 攻击、SQL 注入攻击行为进行审计。
	提供对数据库返回码的知识库和实时说明，帮助管理员快速对返回码进行识别
	▲支持对超长 SQL 语句的审计，操作信息的提取审计、支持对数据库绑定变量方式访问的审计。提供自主知识产权关于数据库操作的信息提取和审计方法及其装置、系统证明文件。
	支持双向审计，支持对 Select 操作返回行数和返回内容的审计。
	支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计；支持数据库操作类、表、视图、索引、触发器、存储过程、

	游标、事物等各种对象的 SQL 操作审计。
	支持数据库存储过程自动获取及内容审计。
网络协议审计	支持 Telnet 协议的审计、FTP 协议的审计能够审计用户名、操作命令、命令响应时间、返回码等。
	支持审计网络邻居的用户名、读写操作、文件名；支持审计 NFS 协议的用户名、文件名；支持审计 Radius 协议的认证用户 MAC、认证用户名、认证 IP、NAS 服务器 IP。
	支持审计 HTTP 协议的 URL、访问模式、cookie、页面内容、Post 内容。。
	支持 RDP 协议审计，可审计关键的键盘输入，记录会话过程；支持 SSH 协议审计，能够审计用户名、操作命令、命令响应时间、返回码。
	支持 SCP 和 SFTP 协议审计，能够审计用户名、命令、文件、命令响应时间、返回码等。
	支持 IP-MAC 绑定变化情况的审计。
业务关联审计	▲支持自动方式建立 web 访问和 SQL 访问之间的对应关系，生成访问行为模型库。提供界面截图证明。
	支持中间件环境下的 SQL 语句关联到 HTTP 操作，HTTP 操作关联到 HTTP-ID，实现中间件环境下的审计追溯。
	支持实时关联模式，可实时查看关联审计结果，无须事后手工查询。
数据库异常行为智能审计	支持自动建立数据库操作行为基线。
	▲数据库操作行为基线包括数据库账号、操作类型（SQL 模板）等行为特征，安全威胁检测工鞲呢。提供自主知识产权关于检测数据库是否遭到跨站脚本攻击的方法证明文件。
	对超出数据库操作行为基线的操作可自动识别，并及时告警。
网络传输文件内容审计	可审计记录 FTP、邮件、HTTP 等方式传输的文件（包括文本、Word、Excel 等格式），并对传输的文件内容中包含关键字的行为进行告警。
审计策略支持	系统应自带不少于 100 个缺省的审计规则库，方便用户选择使用。
	用户可自定义审计策略，审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件。
	数据库审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件（非正则表达式方式）。

	审计策略支持字段名称和字段值作为分项响应条件（非正则表达式方式）。
响应方式	支持数据库操作的命令级阻断，可阻断单个操作，但会话保持。
	支持 Telnet 命令级阻断，可阻断单个操作，但会话保持。
	支持 SSH 命令级阻断，可阻断单个操作，但会话保持。
	支持按照风险级别进行告警，告警方式支持界面告警、Syslog 告警、SNMP trap 告警、短信告警、邮件告警。
日志查询统计	支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询。
	支持查询、统计的条件模板编辑与应用；
	支持多个查询、统计任务同时进行。
	支持对数据库的流量监控和访问量监控；可提供被审计数据库操作的变化趋势图，同一数据库的不同周期事件量和流量纵向对比图等。
	支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多 IP 登录、上下班操作量对比异常、操作响应时间超时等信息。
	数据库访问日志，支持按数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、SQL 语句关键字、数据库返回码、SQL 响应时间、数据库返回行数作为查询和统计条件。
	支持按每天、每周、每月、时刻生成报表，并且生成 Word、PDF、xls、HTML 格式的报表。
	支持邮件方式定期自动发送报表。
大数据库支持	支持审计系统扩展，可采用大数据平台存储和分析审计日志，极大的扩展存储空间和分析能力，产品本身具备安全防御能力。提供自主知识产权关于数据库安全保护方法和装置证明文件
第三方接口	支持 SNMP 方式，提供系统运行状态给第三方网管系统，支持 Syslog、SNMP 方式向外发送审计日志，支持 Syslog 方式接收第三方审计日志。
	支持 Syslog 方式接收第三方审计日志；支持 NTP 时间同步。
质量保障	▲为确保项目质量，所投产品是主流厂商产品，并且近两年(2016 年-2017 年)年市场占有率前三，提供 2017 年或 2018 年权威机构盖章的数据引用证明文件（如：IDC、CCID、Frost & Sullivan 等权威机构）。
资质要求	所投产品具有《计算机信息系统安全专用产品销售许可证》（增强级）。需

	提供有效资质证明复印件。
	所投产品具有中国信息安全认证中心颁发的强制认证证书（增强级）。需提供有效资质证明复印件。
	所投产品具备涉密信息系统产品检测证书。需提供有效资质证明复印件。
	所投产品具有中国信息安全测评中心的信息技术产品安全测评证书 EAL3+。需提供有效资质证明复印件。
	所投产品具备 IPV6 金牌认证；需提供有效资质证明复印件。
厂商资质	为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级）。提供有效的资质证明复印件。
	所投产品厂商为应用安全联盟成员单位。需提供有效编号证明复印件。
	▲所投产品厂商具备工业信息安全测试评估机构能力认证证书（二级）；提供有效的资质证明复印件。
	具备环境管理体系认证证书（ISO14001:2015）。提供有效的资质证明复印件。
	▲为保证厂商原创漏洞的能力，所投产品厂商在国家信息安全漏洞共享平台(CNVD)提交的原创漏洞数量情况。到目前为止，企业单位原创积分排名必须进入前三名，需提供 CNVD 官网的截图证明
	所投产品厂商具备国家信息安全测评信息安全服务资质证书（风险评估二级）。需提供有效资质证明复印件。

（9）服务器招标要求

指标项	指标要求
规格要求	2U 机架式服务器
处理器	配置≥2 颗 CPU，每颗 CPU 核心数≥8 核，每颗 CPU 主频≥2.1GHz
内存	配置≥32GB DDR4 内存，支持≥16 个内存插槽，最大可支持 2TB 内存容量，支持内存 ECC 保护、内存镜像、内存热备，支持 NVDIMM 和 NVDIMM-N 内存可实现意外断电时内存数据不丢失
硬盘	配置≥2 块 1T3.5 吋 7200 转 6GbSATA 硬盘，支持≥12 个外置热插拔硬盘，可支持 SAS/SATA 硬盘、SSD 混插，支持 8 个 NVMe U.2 SSD，支持 1 个 M.2 SSD，支持≥2 个后置热插拔 2.5 寸硬盘位

硬盘控制器	选支持 0/1/5/6/10/50/60 的、具备缓存的高性能 12Gb/sSAS RAID 控制器并可扩展缓存保护电池/电容，本次配置 2GB 缓存 raid 卡和电池
网卡	配置双口千兆网卡，支持 NCSI、网络唤醒，网络冗余，负载均衡等网络高级特性
扩展插槽	支持≥6 个 PCI-E 3.0 插槽（2 个专用插槽）
▲电源	配置热插拔铂金 1+1 冗余电源，单个电源功率≥550W；提供服务器电源认证，并加盖原厂商公章；支持 400WBBU 电池单元，提供二次备援功能支持 400W BBU 电池单元，提供二次备援功能，并提供支持该配置证明文件。
风扇	配置≥3 个热插拔高速系统风扇
▲SD 卡	主板支持 SD 卡插槽，可实现存储系统日志及 BMC 日志，提供功能截图并加盖原厂章；
▲管理	集成 BMC 芯片，支持 IPMI2.0 和 KVMOver IP 高级管理功能、黑匣子功能，提供黑匣子功能界面截图，并加盖原厂章
▲安全防护	提供如下功能，并提供软件主界面截图并加盖原厂章，与服务器同一品牌： （1）服务器优化功能，提升服务器主机系统安全，包括服务器体检、系统漏洞修复、系统服务优化、垃圾清理等功能； （2）网络防火墙功能，防火墙、安全策略、超级黑白名单三层防护层层过滤，为服务器网络安全保驾护航，提供界面截图； （3）主动防御功能，提供文件及目录保护，防止数据恶意窃取及篡改，提供文件及目录保护、账号保护以及远程桌面保护； （4）日志审计功能，防护日志记录服务器被攻击情况
▲服务器管理软件	配置服务器导航软件，按预定义或自定义的角色分组展现服务器状态信息，以及相关联的告警信息，并提供原厂商计算机软件著作权登记证书复印件，并加盖原厂章
产品兼容性	通过 Windows、VMware、Redhat、Oracle Linux、Citrix、Suse 等主流 OS 厂商的兼容性测试
▲产品认证	所投产品通过 3C 认证、CB 认证、CE 认证、节能、环标等认证，以上证书需要提供复印件并加盖原厂章 。
▲制造商资质认证	所投产品制造商通过 ISO9001 认证，三年以上国家级工业设计中心资质，省级以上单位颁发的高新技术企业证书和技术中心认定证书，CMMI 4 级证书等。以上证书需要提供复印件并加盖原厂章 。
服务	3 年原厂整机质保，3 年原厂免费上门服务（提供原厂项目授权函，原厂服

	务承诺函，原件）

（10）机柜招标要求

指标项	指标要求
硬件规格	▲标准 2U，宽 550mm 高 350mm 深 120mm
立体间距	465MM（19 英寸）
材质工艺	SSPCC 冷轧、方孔条镀锌板
表面处理	酸洗、脱脂、磷化、进口塑粉、静电喷塑
支持用途	安装服务器、路由器、配线架、KVM、UPS 网络设备

二、等保安全整改服务要求

1.	网络及系统的等保改造服务	按照等保要求，对所有网络设备进行优化，对操作系统和应用系统进行修补、加固和优化。包括针对全网信息平台各种设备、多种操作系统、多项应用的打补丁、停止不必要的服务、升级或更换程序、除去后门程序、修改配置及权限以及针对复杂问题的专门解决方案等服务。
2.	等保管理制度梳理建立	在对采购人安全管理制度调研的基础上，参考等级保护管理体系要求，评估乳源人民医院信息安全管理建设状况，提出相关安全管理体系加强规范的建议。
3.	安全培训服务	提供有时效性和有针对性的安全宣传素材给采购人相关人员，用于内部及外部宣传。使用户能在较短的时间内，掌握信息安全基础知识、安全攻防基础知识、安全事件应急预案等，掌握基本的信息安全事件的应急处置，协助用户在不同状况的应急预案处理，以保证信息系统的正常、安全地运行。

三、商务要求（技术要求中另有要求的从其要求）

1、交货方式

（1）项目地点：乳源瑶族自治县中医医院

（2）项目安装完成时间（含验收合格）：合同签订之日起 180 天完成。

2、付款方式：

（1）合同签订生效后，采购人支付至合同总价的 60%；

（2）采购设备全部发货至项目地点后，采购人支付至合同总价的 80%；

（3）项目验收合格并通过试运行，采购人支付至合同总价的 95%；

（4）余款 5%作为履约保证金在设备正常运行壹年后一次性付清。

3、售后服务

（1）货物经采购人验收合格交付使用之日起，成交供应商须提供不少于三年的免费上门维修维护的免费保修服务。

（2）在免费质量保修期内，如货物非因采购人的人为原因而出现质量问题，成交供应商承诺全额免费包维修、包更换或退换、包安装、包调试、包正常运行；如确属采购人人为原因损坏，亦须无条件维修、更换或退换、安装、调试并确保正常运行，但采购人应给予合理费用。

（3）有偿保修服务期内而需要维修或维护的，成交供应商仍应按本条约定的时间派员检查与维修，并确保优质服务和质量合格且能正常运行。有关修复费用由采购人承担，但成交供应商应给予最优惠价格

第四章 合同文本

注：本合同条款仅供参考，甲乙双方可根据磋商文件、报价文件中未约定事项进行补充。

一、总　　则

1. 合同当事人

甲方（采购人）：

乙方（成交供应商）：

根据《中华人民共和国合同法》、《中华人民共和国政府采购法》及_____项目（项目编号：_____）磋商文件的要求和磋商结果，经甲乙双方协商一致，签订本合同。双方共同遵守如下条款（其他有关合同项目的特定信息由合同附件予以说明，合同附件及本项目的磋商文件、报价文件、成交通知书、在实施过程中双方共同签署的补充文件等均为本合同不可分割之一部分）。

二、合同标的

1　乙方根据甲方要求提供以下货物：

货物品名	规格型号	单位	数量	单价	总价	随机配件

三、质　　量

1　货物质量

（1）乙方须提供全新的、未使用过的货物，是目前的型号，其质量、规格及技术特征符合合同附件的要求。

（2）产品必须提供出厂合格证。

（3）货物制造质量出现问题，乙方应负责三包（包修、包换、包退），费用由乙方负责。

（4）货到现场后由于甲方保管不当造成的质量问题，乙方亦应负责修理，但费用由甲方负担。

四、交货与验收

1　交货验收、安装调试必须在合同签订后___天内完成。

2　交货地点：甲方指定地点。

3　由甲方与乙方一起进行到货验收，由乙方免费完成货物的安装调试工作并交付甲方使用。

4 乙方应将所提供货物的装箱清单、用户手册、原厂保修卡、随机资料及配件、随机工具等交付给甲方；乙方不能完整交付货物及本款规定的单证和工具的，视为未按合同约定供货，乙方必须负责补齐，因此导致逾期交付的，由乙方承担相关的违约责任。

五、合同金额及付款方式

1 合同金额

本合同金额为人民币（大写）_____元整（￥_____元）。该合同总价包括货物采购、运输、安装、调试、相关部门验收及保修期内的维护保养等所有费用，以及乙方认为必要的其他货物、材料、安装、服务；乙方应自行增加货物正常、合法、安全运行及使用所必需但本项目招标文件没有包含的所有货物、版权、专利等一切费用，如果乙方在供货、安装、调试、培训等工作中出现货物的任何遗漏，均由乙方免费提供，甲方将不再支付任何费用。本合同执行期间合同总价不变。

2 付款方式

_____

六、售后服务

1 乙方应为甲方提供免费培训服务，并指派专人负责与甲方联系售后服务事宜。主要培训内容为货物的基本结构、主要部件的构造、日常使用操作、保养与管理、常见故障的排除、紧急情况的处理等，如甲方未使用过同类型货物，乙方还需就货物的功能对甲方进行相应的技术培训，培训地点主要在货物安装现场或由双方约定。

2 质量保证期（简称“质保期”）为___年。质保期自甲方在货物质量验收单上签字之日起计算，质保费用计入总价。

3 质保期内，乙方负责对其提供的货物实行包修、包换、包退、包维护保养，不再收取任何费用，但不可抗力（如火灾、雷击等）造成的故障除外。

4 货物故障报修___小时内响应。

5 所有货物质保服务方式均为乙方上门服务，即由乙方派员到货物使用现场维修，由此产生的一切费用均由乙方承担。

6 质保期后的货物维护由双方协商再定。

7 在质保期内，乙方须对所提供的设备做定期检查和保养。

8 其他售后服务条款

_____

七、违约责任

1 甲方无正当理由拒收货物、拒付货款的，甲方须向乙方交纳合同总价___%的违约金。

2 甲方逾期支付货款的，甲方须每日以欠款总额___‰的标准向乙方交纳违约金，累计不超过欠款总额的___% 。

3 乙方逾期 15 天未交付货物视为乙方不能交付货物。乙方不能交付货物，须向甲方交纳合同总价___%的违约金。

4 乙方逾期交付货物的，乙方须每日以逾期交货部分货款总额___‰的标准向甲方交纳违约金，累计不超过逾期交货部分货款总额的___%，逾期交货超过 15 天，甲方有权终止合同。

5 乙方所交付产品的型号、规格、数量和质量不符合合同规定标准的，甲方有权拒收。乙方须向甲方交纳合同总价___%的违约金。

6 乙方所供货物必须权属清楚，不得侵害他人的知识产权，否则构成对甲方违约。

7 其他违约责任

_____

八、不可抗力

1 “不可抗力”系指战争、严重火灾、洪水、台风、地震等或其他甲、乙双方认定的不可抗力事件。

2 甲方或乙方应当在不可抗力发生之日起_____天内以书面形式通知对方，证明不可抗力事件的存在。

3 不可抗力事件发生后，甲方和乙方应当积极寻求以合理的方式履行本合同。如不可抗力无法消除，致使合同目的无法实现的，双方均有权解除合同，且均不互相索赔。

九、争议及解决办法

1 因货物的质量问题发生争议，由广州市质量技术监督局或其指定的质量鉴定单位进行质量鉴定。货物符合质量标准的，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。

2 本合同发生争议，由双方协商或由政府采购监管部门调解解决，协商或调解不成时按以下第_____种方式解决：

（1）中国广州仲裁委员会仲裁；

（2）向甲方所在地人民法院提起诉讼。

十、其　　他

1 本合同一式___份，具有同等效力，甲、乙双方各执___份，采购代理机构执一份。合同自双方签字盖章之日起生效。

2 本合同未尽事宜，由双方协商处理。

甲方：（盖章）	**乙方：**（盖章）
签约代表：	**签约代表：**
地　　址：	**地　　址：**
电　　话：	**电　　话：**
传　　真：	**传　　真：**
签约日期：　　年　月　日	**签约日期：**　　年　月　日

第五章 磋商细则

一、磋商小组组成

磋商小组由采购人代表和有关专家共三人以上（达公开招标限额的项目为五人以上）单数组成，其中专家在政府采购专家库中随机抽取，如采购人不派代表参加评审，则磋商小组全部由从政府采购专家库随机抽取的专家组成。磋商小组本着公平、公正、科学、择优的原则，严格按照法律法规和磋商文件的要求推荐评审结果。磋商小组在磋商及评审过程中出现意见不一致时，应遵循少数服从多数原则。

磋商小组成员有下列情形之一的，受到邀请应主动提出回避，采购当事人也可以要求该成员回避：

1.本人、配偶或直系亲属3年内曾在参加该采购项目的供应商中任职（包括一般工作）或担任顾问，或与参加该采购项目的供应商发生过法律纠纷；

2.任职单位与采购人或参加该采购项目供应商存在行政隶属关系；

3.曾经参加过该采购项目的进口产品或磋商文件、采购需求、采购方式的论证和咨询服务工作；

4.是参加该采购项目供应商的上级主管部门、控股或参股单位的工作人员，或与该供应商存在其他经济利益关系；

5.磋商小组成员之间具有配偶、近亲属关系；

6.同一单位的评审专家在同一项目磋商小组成员中超过一名；

7.法律、法规、规章规定应当回避以及其他可能影响公正评审的。

二、磋商流程

（一）接收报价文件

采购代理机构按《磋商文件》规定的时间和地点接收报价文件和组织磋商会。报价人派出法定代表人或其授权代表人参加并签到；采购代理机构负责做好有关记录。报价人不派出其授权代表参加开标会的，视为完全同意开标内容及对开标会过程无异议。

（二）磋商

（1）磋商小组首先对报价人进行初审，初审内容包括资格性、符合性审查（内容详见附表1），出现不符合资格性、符合性初审表所列情形之一时，不得参与磋商，磋商小组将告知供应商并说明理由。

（2）磋商小组与通过初审的每一报价人分别进行磋商，报价人派出法定代表人或其授权代表参加，

如不参加，视为报价及磋商承诺按报价文件内容不变。

（3）磋商小组与报价人进行磋商后形成《磋商承诺》。《磋商承诺》是报价文件的有效组成部分。

（4）磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。磋商文件的变动内容须经采购人代表确认，并记载在《磋商纪要》中以通知所有磋商供应商。

（5）如磋商小组没有对磋商文件作实质性变动增加新的需求，最后报价不得高于首次报价。

（6）在磋商中，磋商的任何一方，不得透露与磋商有关的其他报价人的技术资料、价格和其他信息；

（7）磋商小组要求报价人在规定的时间内进行最终报价。除非报价人另有说明，最终报价总价与第一次报价总价下浮的比例，其报价明细项按相同比例下浮。磋商小组将向供应商公开各家报价。

（8）没有在规定时间内提交最后报价视为报价及磋商承诺按报价文件内容不变。

（9）《磋商纪要》及最终报价均提交给磋商小组后，磋商小组将进行最终符合性审查（内容详见附表 2），出现不符合最终符合性审查所列情形之一时，不得进入后续评审，磋商小组将告知供应商并说明理由。

（10）磋商完成后，磋商小组将进入评审流程。

三、评审流程

（一）评审形式

本次磋商采用一次评审，两轮或多轮磋商报价形式进行。经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

（二）报价文件差异修正准则

报价文件出现差异时，修正原则及优先修正顺序如下：

1.开标内容与报价文件对应内容不一致的，均以开标内容为准；

2.开标一览表与分项明细表或其它相关报价表报价不一致的，均以开标一览表为准；

3 分项报价表中的单价与对应的合计价不相符的，以单价为准，修正对应的该项合计价；

4.大写金额和小写金额不一致的，以大写金额为准；

5.单价金额小数点有明显错位的，应以总价为准，并修改单价；

6.对不同文字文本报价文件的解释发生异议的，以中文文本为准；

7.对出现以上情况或因明显笔误而需修正任何内容时，均以磋商小组审定通过方为有效；

8.对采购项目的关键、主要内容，报价人报价漏项的，作非实质性响应处理；

9.磋商小组认定为表述不清晰或无法确定的报价均不予修正。

（三）报价文件的澄清、说明或更正

1.磋商小组在对报价文件的有效性、完整性和响应程度进行审查时，可以要求报价人对报价文件中含义不明确、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出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出报价文件的范围或者改变报价文件的实质性内容。

2.磋商小组要求供应商澄清、说明或者更正报价文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。

3.磋商小组均应当阅读供应商的澄清、说明或者更正，但应独立参考澄清、说明或者更正对报价文件进行评审，整个澄清、说明或者更正的过程不得存在排斥潜在供应商的现象。

4.除上述规定的情形之外，磋商小组在评审过程中，不得接收来自评审现场以外的任何形式的文件资料。

（四）磋商小组认为，供应商的报价明显不合理或者明显低于其他供应商报价，有可能影响商品质量和不能诚信履约的，应当要求该供应商作出书面说明并提供相关证明材料。供应商不能合理说明或者不能提供相关证明材料的，由磋商小组认定该供应商为低于成本报价，报价无效。

（五）评审细则

1.商务评定

（1）由评委对所有有效报价文件的商务条件进行审核和评价，填写《商务评审表》，评审内容见附表3。

（2）将每一个评委的评分汇总进行算术平均，得出该报价人的商务评分。

2.技术评定

（1）由评委对所有有效报价文件的技术响应方案进行审核和分析，填写《技术评审表》。评审内容见附表 3。

（2）将每一个评委的评分汇总进行算术平均，得出该报价人的技术评分。

3.价格评定

1）对小型或微型企业投标的扶持（监狱企业、残疾人福利性单位视同小型、微型企业）：

1.1）报价人为小型或微型企业（包括成员全部为小型或微型企业的联合体）且投标产品含小型或微型企业产品时，报价给予 C1 的价格扣除（C1 的取值为 6%），即：评标价＝核实价－小微企业产品核实价×C1；

1.2）报价人为大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成的联合体，且联合体协议中约定小型、微型企业的协议合同金额（必须为小型或微型企业产品）占到联合体协议合同总金额30%以上的，对联合体报价给予C2的价格扣除（C2的取值为2%），即：评标价＝核实价×(1－C2)；

1.3）本条款所称小型或微型企业应当符合以下条件：符合小型或微型企业划分标准，提供本企业制造的货物或者提供其他小型或微型企业制造的货物；

1.4）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系；

1.5）本条款中上述优惠原则不同时使用。

2）符合上述条款的报价人，应填写《政策适用性说明》、《中小企业声明函》、《残疾人福利性单位声明函》（格式可在http://www.gzqunsheng.com/常用文件一栏下载）。

3）对于节能产品或环保产品的价格扣除，依据报价人填写的《节能、环境标志产品政策优惠表》（格式可在http://www.gzqunsheng.com/常用文件一栏下载）比例进行。

4）节能产品或环保产品或小型、微型企业的价格扣除比例如下：

序号	情形	节能产品占总报价比重	价格扣除比例	计算公式
1	节能产品（a）	（10%，20%]	1%	评标价＝总报价—节能产品价格×a%
		（20%，40%]	2%	
		（40%，60%]	3%	
		（60%，80%]	4%	
		（80%,100%]	5%	
2	环境标志产品（b）	（10%，20%]	1%	评标价＝总报价—环境标志产品价格×b%
		（20%，40%]	2%	
		（40%，60%]	3%	
		（60%，80%]	4%	
		（80%,100%]	5%	
3	供应商须为小型、微型企业	对小型和微型企业产品的价格扣除6%		评标价＝总报价—小型和微型企业产品的价格×6%

5）价格评分：价格分统一采用低价优先法计算，即满足磋商文件要求（通过资格审查和最终符合性审查）且价格最低的评标价(指按上述条款修正及价格扣除后报价，下同)为评标基准价，其价格分为满分。其他报价人的价格分统一按照下列公式计算：

价格评分=（评标基准价／评标价）×价格评分权重

4.本次评标采用综合评分法。评分比重如下：

评分项目	商务部分	技术部分	价格部分	总分
权重	15	75	10	100

（六）综合评分的计算

1.综合评分=商务得分+技术得分+价格得分。

2.各项得分按四舍五入原则精确到小数点后两位，如因计算软件四舍五入导致后两位小数相同的，则计算至后三位，依次类推，直接得出排序。将综合评分由高到低顺序排列。

（七）推荐成交供应商候选人

1.本项目磋商小组按综合总得分由高至低排序推荐得分前三名分别为第一、第二、第三成交供应商候选人。

2.总得分相同的，按最终报价由低到高顺序排列。总得分且最终报价相同的，按技术得分由高至低排列。

3.第一成交供应商候选人无正当理由不得随意放弃成交资格。

四、确定成交供应商

（一）采购人在评标报告确定的成交供应商候选人名单中按顺序确定成交供应商。

（二）采购人确认结果后，采购代理机构将成交结果以网上公告的方式通知所有未成交的成交供应商。

（三）成交结果公告后，采购代理机构以书面形式向成交供应商发出《招标代理服务费缴费通知书》。

（四）成交供应商凭采购代理机构开具的《招标代理服务费缴费通知书》到银行办理缴费手续，凭银行回单原件到采购代理机构开发票，领取《成交通知书》。《成交通知书》将作为授予合同资格的唯一合法依据。

（五）成交供应商放弃成交或被确定成交无效的，应当依法承担法律责任，同时，采购人可以按照评审报告推荐的成交供应商候选人名单排序，确定下一候选人为成交供应商，也可以重新开展政府采购活动。

（六）报价人必须对报价文件所提供的全部资料的真实性承担法律责任，并无条件接受采购人和政府采购监督管理部门对其中任何资料进行核实（核对原件）的要求。如有必要，采购人将核对报价文件资料，发现有不一致或供应商无正当理由不按时提供原件的，书面知会采购代理机构，并报同级财政部门核实后按成交无效处理。

五、签订合同

采购人与成交供应商应当在《成交通知书》发出之日起三十日内（如第二章采购需求有相应约定的从其约定），按照磋商文件确定的事项签订政府采购合同，合同条款不得与磋商文件和报价文件内容有实质性偏离。

采购人应当自政府采购合同签订之日起 2 个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

六、凡发现成交供应商有下列行为之一的，其成交无效，并移交政府采购监督管理部门依法处理。

1）提供虚假材料谋取成交的；

2）采取不正当手段诋毁、排挤其他供应商的；

3）与采购人、其他供应商或者采购代理机构工作人员恶意串通的；

4）向采购人、采购代理机构工作人员行贿或者提供其他不正当利益的；

5）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者提供虚假情况的；

7）有法律、法规规定的其他损害采购人利益和社会公共利益情形的。

七、项目采购失败情形

出现下列情形之一的，采购人或者采购代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

（1）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

（2）出现影响采购公正的违法、违规行为的。

附表 1 资格、符合性初审表

评审内容	报价人名称		
	报价人 A	报价人 B	报价人 C
具备磋商文件中规定报价人资格要求			
报价唯一，不高于采购人需求规定的最高限价			
符合报价文件的签署、盖章要求			
按磋商文件要求提供法定代表人证明及授权书的			
符合磋商文件报价有效期要求的			
满足磋商文件中带★号的条款和指标的			
未发现无效报价的其他情形的（见注 4）			
结论			

注：1、报价人分栏中填写“〇”表示该项符合磋商文件要求，“×”表示该项不符合磋商文件要求；

2、结论栏中填写“通过”表示该报价人报价文件符合磋商文件要求，“不通过”表示该报价人报价文件不符合文件要求；

3、结论汇总意见采取少数服从多数原则，即超过半数磋商小组成员的结论为“通过”则该报价人通过资格审查及符合性检查，否则不通过。

4、无效报价的其他情形

（1）除联合体外，法定代表人或单位负责人为同一个人或者存在直接控股、管理关系的不同供应商，同时参加本项目或同一子项目报价的。

（2）经磋商小组认定报价文件提供虚假材料的；

（3）报价人以他人的名义报价、串通报价、以行贿手段谋取成交或者以其他弄虚作假方式报价的；

（4）报价人对采购人、采购代理机构、磋商小组及其工作人员施加影响，有碍采购公平、公正的；

（5）报价文件附有采购人不能接受的条件；

（6）出现不符合相关法律、法规要求的情况的。

附表 2 最终符合性审查表

评审内容	报价人名称		
	报价人 A	报价人 B	报价人 C
报价唯一，不高于采购人需求规定的最高限价，如磋商小组没有对磋商文件作实质性变动增加新的需求，最后报价不高于首次报价；未被认定低于其成本报价。			
磋商后的承诺满足磋商文件中带★号的条款和指标的			
未发现无效报价的其他情形的（见注 4）			
结论			

注：1、报价人分栏中填写“〇”表示该项符合磋商文件要求，“×”表示该项不符合磋商文件要求；

2、结论栏中填写“通过”表示该报价人报价文件符合磋商文件要求，“不通过”表示该报价人报价文件不符合文件要求；

3、结论汇总意见采取少数服从多数原则，即超过半数磋商小组成员的结论为“通过”则该报价人通过资格审查及符合性检查，否则不通过。

4、最终符合性审查无效报价的其他情形

（1）经磋商小组认定报价文件提供虚假材料的；

（2）报价人以他人的名义报价、串通报价、以行贿手段谋取成交或者以其他弄虚作假方式报价的；

（3）报价人对采购人、采购代理机构、磋商小组及其工作人员施加影响，有碍采购公平、公正的；

（4）评审期间，报价人没有按磋商小组的要求提交澄清、说明或更正的；

（5）报价文件附有采购人不能接受的条件；

（6）出现不符合相关法律、法规要求的情况的。

附表 3

商务评审表

序号	评审内容	分值	评审标准
1	项目负责人	3 分	报价人为本项目投入团队需配置一名项目负责人，项目负责人具有： 1、计算机科学与技术类专业本科或以上毕业证书； 2、计算机科学与技术类专业本科或以上学位证书。 每项 1.5 分，最高得 3 分。 （提供资质证书复印件和在本公司任职的证明材料（加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月以内的《投保单》或《社会保险参保人员证明》））
		3 分	项目负责人的专业资质：由信息网络安全专业技术人员继续教育工作办公室颁发的《信息网络网络安全专业技术人员继续教育证书》得 3 分。 （提供资质证书复印件和在本公司任职的证明材料（加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月以内的《投保单》或《社会保险参保人员证明》））
		5 分	项目负责人经验：2018 年至今具有同类项目经验的得 5 分。 1、提供备案公安机关颁发的信息系统安全等级保护备案证明复印件； 2、提供备案系统的信息安全等级测评报告封面及测评结论页复印件； 3、提供项目经理在备案时间内担任技术负责人的任职或离职证明，任职时间应覆盖系统获得备案的时间。
2	综合服务支撑能力	3 分	投标人在项目所在地是否有常驻办事机构或固定办公场所。有得 3 分，否则得 0 分。 （须提供房产证明或租赁合同或合作协议，复印件加盖公章）
3	对不良信用记录的扣分	1 分	以“信用中国”（www.creditchina.gov.cn）网站为查询渠道，对列入企业经营异常名录的供应商每一条记录扣 0.2 分，最高扣 1 分。
合计		15 分	

技术评审表

序号	评审内容	分值	评审标准
1	对项目现状、需求与服务内容的整体理解情况	10 分	方案合理，内容详细，熟悉项目技术要求，完整、可行、科学、合理，充分考虑新增设备与现有环境搭配，安全解决方案完善，完全满足且优于用户需求，得 10 分； 方案合理、项目技术方案总体设计情况，完整、可行、科学、合理，完全符合用户实际情况的得 6 分； 方案比较合理，项目技术方案总体设计情况，完整、可行、科学、合理，基本符合用户实际情况的，得 2 分； 方案不合理，不能满足采购人技术要求，得 0 分。
2	安装、调试及检验验收方案	5 分	根据供应商提供的安装、调试及检验验收方案进行评价打分： 1）方案合理可行，符合本项目实际所需，得 5 分； 2）方案基本可行，基本满足本项目所需，得 3 分； 3）方案不够详细具体、完善，得 1 分； 4）不提供不得分。
3	设备技术参数响应情况	30 分	报价人所投产品对磋商文件《采购人需求》内所有产品要求参数响应情况全部满足或优于的得 30 分；标注“▲”号重要参数每一项负偏离或者无响应的扣 1 分，每个非“▲”指标负偏离或者无响应扣 0.5 分，扣完为止。报价人必须按货物实际参数进行响应，否则视为提供虚假材料谋取成交资格。
4	主要安全设备制造商（互联网边界防火墙、数据中心防火墙、终端管理系统、准入控制系统、运维保垒机、日志审计系统、数据库审计系统）整体实力（提供证明材料）	10 分	为保证主要安全设备制造商的整体实力，制造商需具备以下能力： （1）国家级应急服务支撑单位； （2）国家信息安全测评信息安全服务资质证书（安全工程类三级或以上）； （3）ISO 14001 环境管理体系； （4）中国国家信息安全漏洞库（CNNVD）技术支撑单位一级； （5）中国保密协会理事单位证书； （6）应用安全联盟会员证书； （7）信息安全服务资质（一级信息系统安全集成服务）； （8）国家信息安全测评信息安全服务资质证书（风险评估二级或以上）； （9）通信网络安全服务能力评定证书（安全培训一级）； （10）通信网络安全服务能力评定证书（应急响应服务一级） 安全设备制造商具备一个资质得 1 分，满分 10 分。无法提供证明文件或证明文件无效不得分。

5	主要安全设备制造商（互联网边界防火墙、数据中心防火墙、终端管理系统、准入控制系统、运维保垒机、日志审计系统、数据库审计系统）原创漏洞的研究能力（提供 CNVD 官网的截图证明）	10 分	主要安全设备制造商在国家信息安全漏洞共享平台(CNVD)提交的原创漏洞企业单位原创积分排名前三，得 10 分；排名 4-6，得 5 分，排名 7-10，得 2 分；其它情况 0 分。 需提供 CNVD 官网的截图证明，无法提供证明文件或证明文件无效不得分。
6	主要安全设备制造商（互联网边界防火墙、数据中心防火墙、终端管理系统、准入控制系统、运维保垒机、日志审计系统、数据库审计系统）在信息安全攻防研究能力（提供相关证明文件）	10 分	主要安全设备制造商自主发掘 1000 个以上 CVE 安全漏洞得 10 分、自主发掘 800-999 个 CVE 安全漏洞得 5 分、自主发掘 200-799 个 CVE 安全漏洞得 2 分、其它情况 0 分。 需提供 CVE 列表与链接证明材料，无法提供证明文件或证明文件无效不得分。
合计		**75 分**	

备注：报价人应提交与评价指标体系相关的各类有效资料。

第六章 报价文件格式

一、报价文件目录表

序号	文 件 名 称	是否提交	页码范围	备 注
一	报价文件			
1	★报价函（格式 1）			
2	★报价一览表（格式 2）			
3	★分项报价表（格式 3）			
4	政策适用性说明、中小企业声明函、残疾人福利性单位声明函、节能、环境标志产品政策优惠表（格式可在 http://www.gzqunsheng.com/常用文件一栏下载）			
二	资格、符合性审查文件			
1	★法人营业执照或者其他组织登记文件等证明文件，自然人的身份证明复印件			
2	组织机构代码证，国、地税务登记证副本复印件（三证合一除外）			
3	★本年度财务状况报告（未完成编制的可提供上一年度，新成立单位可提供成立至今）或基本开户行出具的资信证明复印件			
4	★依法缴纳税收和社会保障资金的良好记录（提供报价截止日前 6 个月内任意 1 个月依法缴纳税收和社会保障资金的相关材料。如依法免税或不需要缴纳社会保障资金的，提供相应证明材料			
5	★未列入失信被执行人、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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，提供信用中国网站 www.creditchina.gov.cn/及中国政府采购网 www.ccgp.gov.cn 查询结果截图并加盖公章			
6	获取采购文件的收据或发票复印件			
7	★法定代表人证明及授权书（格式 4）			
8	★实质性条款响应一览表（格式 5）			
9	★关于资格证明文件的声明函（格式 6）			
10	其他资格证明文件			
三	商务、技术文件			
1	商务、技术评审索引表（格式 7）			
1	近一年财务报表（含资产负债表及利润表，尽量提供具有审计资质的第三方出具的《审计报告》）			

2	近年同类项目业绩表（格式 8）			
3	报价人为本项目配置人员说明（格式自拟）			
4	质量保证、售后服务说明（格式自拟）			
5	与采购人需求差异表（格式 9）			
6	合同条款响应一览表（格式 10）			
7	缴交采购代理服务费承诺书（格式 11）			
8	同意磋商文件条款说明（格式 12）			
9	所报货物详细的技术方案（格式自拟）			
10	报价人认为需提交的其他资料			

二、报价信封

序号	文 件 名 称	是否提交	备注
1	报价一览表（与报价文件中的内容保持一致）；		
2	分项报价表（与报价文件中的内容保持一致）；		
3	（如有）《政策适用性说明》、《中小企业声明函》、《残疾人福利性单位声明函》、《节能、环境标志产品政策优惠表》		

（1）带“★”文件为必须提供的文件；

（2）上述文件如为复印件的，必须加盖报价人公章；

（3）如上述文件可通过互联网或者相关信息系统查询的信息，请供应商协助提供复印件的同时提供查询网址，最终结果以查询为准；

（4）报价人应自行承担所提供上述资料任何错漏而导致的一切后果。

格式 1　　报 价 函

广州群生招标代理有限公司：

我方确认收到你方提供的_____项目及其相关服务的磋商文件的全部内容。我方：（报价人名称）作为报价者正式授权（授权代表全名、职务）代表我方进行有关报价的一切事宜。在此提交的报价文件，正本一份，副本两份。我方已完全明白磋商文件的所有条款要求，并重申以下几点：

1.我方决定参加：项目编号为_____的报价；

2.本报价文件的有效期为报价截止日后 90 天有效，如被确定为成交供应商，有效期将延至合同终止日为止；

3.我方已详细研究了磋商文件的所有内容包括修正（如果有）和所有已提供的参考资料以及有关格式并完全明白，我方放弃在此方面提出含糊意见或误解的一切权利；

4.我方同意按照你方可能提出的要求提供与报价有关的任何其它数据或信息；

5.我方理解磋商小组不一定接受最低报价或任何你方可能收到的报价；

6.我方如被确定为成交供应商，将保证履行磋商文件以及磋商文件修改书（如有的话）中的全部责任和义务，按质、按量、按期完成《合同》中的全部任务；

7.我方自行完全承担因报价文件错误、缺漏、不清晰而导致的一切后果；

8.凡属于《中华人民共和国实施强制性产品认证的产品目录》的产品，我方将在交货时提供该产品的《中国强制认证》（CCC 认证）。

9.我方确认此次磋商中提供的一切资料均是真实的，准确的，并完全承担因此产生的一切后果。

10.我方的报价被接受，我方同意按照磋商文件规定向采购代理机构缴纳采购代理服务费。

所有与本磋商文件有关的函件请发往下列地址：

报价人全称（加盖公章）：_____

地址：_____　　邮政编码：_____

法定代表或其授权代表（签字）：_____

日　期：　　年　　月　　日

格式 2　　首次报价一览表

项目名称：　　项目编号：

报价人名称	总报价 （人民币 元）	项目完成时间

注：1.报价包括了项目的全部费用。

2.本表格须附在正副本的报价文件中，并另封装一份在 “报价信封”内，封口加盖公章。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日

格式 3　　分项报价表

本表将有可能在成交公告中公开，请报价人仔细填写

项目名称：　　项目编号：

序号	货物名称	型号规格	品牌产地	制造商	数量	单位	单价	其他费用	总价	备注
1										
2										
…										
合计报价（人民币大写）：_____ （人民币小写）_____										

注：报价人须针对项目实际情况编制完整详细的项目报价。本表格须附在正副本的报价文件中，并另封装一份在 “报价信封”内。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日

格式 4　　法定代表人证明及授权书

致:广州群生招标代理有限公司

本授权证明：*（法定代表人姓名）*是注册于*（省、市、县）*的*（报价人名称）*的法定代表人，现任*（法定代表人职务）*。在此授权*（被授权人姓名、职务）*作为我公司的全权代理人，在*（项目名称）*的报价（项目编号为：_____）及其合同执行过程中，以我公司的名义处理一切与之有关的事务。

本授权书于_____年____月____日签字生效，特此声明。

法定代表人

居民身份证正反面复印件粘贴处

被授权人(报价人授权代表)

居民身份证正反面复印件粘贴处

报价人全称（加盖公章）：　　地　　址：

法定代表人（签字或签章）：　　被授权人(报价人授权代表)（签字）：

格式 5　　实质性条款响应一览表

项目名称：　　项目编号：

序号	带“★”号响应内容	是否响应	偏离说明	响应页码
1	合格报价人资格要求			
2	报价文件格式带“★”内容			
3	第一次报价超出最高限价的将被视为无效报价，不能参加磋商。			

说明：1、报价人必须对应磋商文件的 “★”号条款逐条应答并按要求填写下表。

2、对完全响应的条目在下表相应列中标注“〇”。对有偏离的条目在下表相应列中标注“×”，并简述偏离内容。

3、本表“是否响应”、“偏离说明”、“响应页码”不填写内容的视为完全响应。

格式 6　　关于资格证明文件的声明函

广州群生招标代理有限公司：

我方愿响应你方_____年_____月_____日发布的_____项目（项目编号：_____）报价邀请，参与报价，提供采购人需求中规定的全部内容，并按采购文件要求提交所附资格文件且声明和保证如下：

1. 我方为本次报价所提交的所有证明我方提供货物和服务合格和我方资格的文件是真实的和正确的，并愿为其真实性和正确性承担法律责任；核验我方提供相关复印件与原件不一致的，或我方无法在规定时间内提供原件的，采购人或采购代理机构有权取消我方报价或成交资格；提供给采购人的货物及服务与报价承诺一致。
2. 我方在参与本次报价时，符合 《中华人民共和国政府采购法》第二十二条报价人资格条件要求及其他法律法规规定的其他条件。
3. 我方具有履行合同所必须的设备和专业技术能力。
4. 我方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。
5. 我方如成交，除不可抗力原因外，将在规定时间内与采购人签订合同。

如有违反上述声明之情形或我方声明与事实不符，我方对被取消成交资格无异议，同时，我方无条件接受相关部门以提供虚假材料谋取成交处理。

报价人全称（加盖公章）:

法定代表人或其报价人授权代表(签字)：　　日　　期：　　年　月　日

格式 7　　商务评审索引表

序号	评审内容 （注：此部分可直接引用磋商文件第五章评审细则相应内容）	响应情况	报价文件响应内容对应页码
1			
2			
…			

技术评审索引表

序号	评审内容 （注：此部分可直接引用磋商文件第五章评审细则相应内容）	响应情况	报价文件响应内容对应页码
1			
2			
…			

格式 8　　近年同类项目业绩表

项目名称：　　项目编号：

序号	**业主名称**	**项目名称**	**合同总价**	**完成时间**	**业主单位 联系人及电话**
1					
2					
…					
小计					

注：报价人应提供相关证明附件。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日

格式 9　　与采购人需求差异表

项目名称：　　项目编号：

序号	磋商文件要求		报价文件内容	
	原条目	简要内容	是否响应	偏离说明
	一	……		
	二	……		
	三	……		

注：报价人应根据其提供的货物和服务，逐条对照磋商文件《采购人需求》的内容要求填写，有差异的，不论是技术或商务上，均须在此表中列明两者的简要内容，以便查对和评审。除“偏离说明”栏所列的内容外，其余按《采购人需求》的内容执行。本表提供空表的视为完全响应。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日

格式 10　　合同条款响应一览表

项目名称：　　项目编号：

序号	磋商文件合同要求	报价文件内容	
	条款号	是否响应	差异说明

注：1.报价人应对照磋商文件第四章合同条款所列内容逐条对应填写，完全满足的在“是否响应”栏中填“响应”；有差异的则在“差异说明”栏中列出差异的具体内容。本表提供空表的视为完全响应。

2.除“差异说明”栏所列的内容以外，其余按《合同书》格式中的条款执行。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日

格式 11　　缴交采购代理服务费承诺书

致：广州群生招标代理有限公司

如果我方在贵公司组织的项目名称：_____（项目编号：_____）磋商采购项目中被确定为成交供应商候选人，我方保证在收到《成交通知书》前，按照磋商文件的规定向贵公司交纳采购代理服务费。

自成交公告发出之日起 5 个工作日内仍未能足额缴纳的，我司承诺按上述规定的 200%赔付贵方；15 个工作日仍未支付上述全部费用的，贵方有权公布我司未履行承诺状况并上报相关主管部门列入未诚信履约名单。

特此承诺！

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日

格式 12　　同意磋商文件条款说明

致：广州群生招标代理有限公司

为响应你方组织的项目名称：_____项目的竞争性磋商【项目编号：_____】，我方在参与报价前已详细研究了磋商文件的所有内容，包括修改文件（如果有的话）和所有已提供的参考资料以及有关附件，我方完全明白并认为此磋商文件没有倾向性，也没有存在排斥潜在报价人的内容，我方并同意磋商文件的相关条款。

特此声明。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：　　日　　期：　　年　　月　　日