WANG TAT
广州宏达工程顾问集团
Guangzhou Wangtat Project Management and Consultancy Group

项目编号：TPA-2022-C3-115

佛山电器照明股份有限公司
网络安全建设项目

招标文件

（修改）

采　　购　　人：佛山电器照明股份有限公司

采购代理机构：广州宏达工程顾问集团有限公司

日　　期：二〇二三年一月

温 馨 提 示

一、如无另行说明，响应文件递交时间为投标截止时间之前 30 分钟内。

二、投标截止时间一到采购代理机构不接收投标人的任何相关报价资料、文件。为此，请适当提前到达。

三、如需投标人支付的各种费用，如招标文件工本费、招标代理服务费等，招标文件将书面详细告知，请投标人（供应商）按招标文件规定的方式和金额支付。

四、请仔细检查响应文件是否已按招标文件要求盖章、签名、签署日期。

五、响应文件应按顺序编制页码。

六、如投标人以非独立法人注册的分公司名义代表总公司盖章和签署文件的，须提供总公司的营业执照副本复印件及总公司针对本项目投标的授权书原件。

七、为了提高采购效率，节约社会交易成本与时间。完成投标登记而决定不参加本次投标的投标人，在响应文件递交截止时间的 2 日前，按采购公告中的联系方式，以书面形式告知采购代理机构。对您的支持与配合，谨此致谢。

（本提示内容非招标文件的组成部分，仅为善意提醒。如有不一致，以招标文件为准）

目　录

第一章 招标公告.....3

第二章 投标人（供应商）须知.....4

第三章 采购人需求书.....17

第四章 合同文本.....18

第五章 响应文件格式及附件.....45

第六章 评标细则.....69

第一章 招标公告

（略）

第二章 投标人（供应商）须知

投标人（供应商）须知前附表

序 号	项 目	主 要 内 容		
1	招标代理服务费	**收费标准：**按原国家计委颁布的计价格[2002]1980 号、国家发改委印发的发改办价格[2003]857 号、发改价格[2011]534 号文按**货物类**计取。招标代理服务费以中标价为计费基准价。 **计算方法：**按差额定率累进法分段计算		
2	招标代理服务费支付方式	中标人（中标供应商）向采购代理机构一次性支付招标代理服务费。		
3	统一结算币种	人民币结算。		
4	投标有效期	自投标截止日起 90 天。		
5	响应文件数量	三份（一份正本、两份副本），响应文件电子版一份，首次报价信封一份。		
6	开标时间	2023 年 01 月 30 日上午 10:30（北京时间）。		
7	投标保证金	1.投标保证金的形式：银行电汇 2.投标保证金递交时间：须于 2023 年 01 月 30 日 10 时 30 分前递交，到账情况以开标前采购代理机构查询的信息为准。**为保证投标工作顺利进行，建议投标人在投标文件递交截止时间前两个工作日将保证金款项转达指定账户。** 3.银行电汇： （1）投标担保额度：2 万元； （2）电汇时请备注：佛山照明网络安全； （3）转账交至： 收款单位名称：广州宏达工程顾问集团有限公司 账号：44001581205053004103 开户银行：中国建设银行广州金海花园支行。 4.中标人（中标供应商）投标保证金在成交后转为履约保证金，采购项目完成并移交采购人后无息退还。		
8	投标最高限价	人民币 190.00 万（¥ 壹佰玖拾万元）。		
9	评审方法	综合评分法（100%）		
		技术权重 35%	商务权重 5%	价格权重 60%
10	实质性响应条款	详见招标文件“采购人需求书”		

投标人（供应商）须知

投标人（供应商）必须认真阅读以下内容，以免造成投标失败。

一、总体说明

1、 招标适用范围

1.1 本招标文件适用于本采购公告中所述项目的采购。

2、 招标适用法律

2.1 采购人及投标人（供应商）的一切采购活动参照相关的法规、规章执行。

2.2 在招标采购中，出现下列情形之一的，应予废标：

1）符合资格条件的投标人（供应商）或者对采购文件作实质响应的投标人（供应商）不足三家的；

2）出现影响采购公正的违法、违规行为的；

3）投标人（供应商）的报价均超过了采购预算，采购人不能支付的；

4）因重大变故，采购任务取消的。

3、 招标（采购）内容

3.1 本次招标（采购）内容为确定佛山电器照明股份有限公司网络安全建设项目的成交单位（投标人（供应商）的报价为设备送达采购方指定地点，经采购方验收合格并交货完毕所有可能发生的费用，包括但不限于软件开发、设备制造、运输、装卸、保险费、采购保管，税收以及售后服务等费用，采购人不再支付其他额外费用）。

3.2 服务地点：采购人指定地点。

4、 关于投标人（供应商）

4.1 具有采购公告中所述资格要求的中华人民共和国的法人或其他组织。

4.2 投标人（供应商）必须按相关法规的规定进行投标响应。

4.3 在采购活动中，采购人员及相关人员与投标人（供应商）有下列利害关系之一的，应当回避：

（一）参加采购活动前 3 年内与供应商存在劳动关系；

（二）参加采购活动前 3 年内担任供应商的董事、监事；

（三）参加采购活动前 3 年内是供应商的控股股东或者实际控制人；

（四）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（五）与供应商有其他可能影响采购活动公平、公正进行的关系。

（六）供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向采购人或者采购代理机构书面提出回避申请，并说明理由。采购人或者采购代理机构应当及时询问被申请回避人员，有利害关系的，被申请回避人员应当回避。

4.4 符合采购公告“二、投标人（供应商）资格要求”。

4.5 不同的投标人（供应商）之间有下列情形之一的，不接受作为参与同一采购项目竞争的投标人（供应商）：

4.5.1 彼此存在投资与被投资关系的；

4.5.2 彼此的经营者、董事会（或同类管理机构）成员属于直系亲属或配偶关系的；

4.5.3 单位负责人为同一人或者存在直接控股、管理关系的不同投标人（供应商），不得参加同一合同项下的采购活动。为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人（供应商），不得再参加该采购项目的其他采购活动。存在以上情形的投标人（供应商）应主动予以回避，否则自行承担相应的法律责任及后果。

5、 关于投标费用

不论投标的结果如何，投标人（供应商）应承担所有与其参加本次投标活动有关的费用。

6、 定义

6.1“采购人”系指佛山电器照明股份有限公司。

6.2“业主/用户”系指本采购项目的最终使用单位，本项目的业主/用户是佛山电器照明股份有限公司。

6.3“采购代理机构”系指广州宏达工程顾问集团有限公司。

6.4“投标人（供应商）”系指向采购代理机构提交响应文件的合格投标人（供应商）。

6.5“中标人（中标供应商）”系指经评标委员会评审推荐、采购人确认的获得本项目中标（成交）资格的投标人（供应商）。

6.6“实质性响应”系指符合招标文件的所有要求、条款、条件和规定，且没有不利于项目实施质量效果和服务保障的重大偏离或保留。

6.7“重大偏离或保留”系指影响到招标文件规定的范围、质量和性能或限制了采购人的权力和投标人（供应商）义务的规定，而纠正这些偏离将影响到其它投标人（供应商）的公平竞争地位。

6.8“服务”系指招标文件规定中标人须承担的有关服务。

6.9 本招标文件所涉及的日期时间，没有特别说明时系指北京时间，天数为日历日，24小时制。

7、 合格的服务和供货

7.1 投标人（供应商）提供的所有服务和供货安装，其来源地均应为中华人民共和国。

7.2 采购人将拒绝接受不合格的服务和供货安装，并有权不予支付任何费用，同时保留追究相关责任的权利。

8、 知识产权

投标人（供应商）必须保证，采购人在中华人民共和国境内使用投标资料、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或其它知识产权而引起的法律或经济纠纷。如投标人（供应商）不拥有相应的知识产权，则在投标报价中必须包括合法获取该知识产权的一切相关费用。

9、 纪律与保密事项

9.1 投标人（供应商）不得相互串通投标报价，不得妨碍其他投标人（供应商）的公平竞争，不得损害采购人或其他投标人（供应商）的合法权益，投标人（供应商）不得以向采购人、评标委员会成员行贿或者采取其他不正当手段谋取中标。除投标人（供应商）被要求对响应文件进行澄清外。

9.2 获得本招标文件者，不得将招标文件用作本次投标以外的任何用途，若有要求，开标后，投标人（供应商）应归还招标文件中的保密的文件和资料。由采购人向投标人（供应商）提供的图纸、详细资料、样品、模型、模件和所有其他资料，被视为保密资料，仅被用于它所规定的用途。除非得到采购人的同意，不能向任何第三方透露。开标结束后，应采购人要求，投标人（供应商）应归还所有从采购人处获得的保密资料。

10、 开标前答疑会

本项目采购人不组织招标开标前答疑会。

11、 现场踏勘

11.1 本项目不需要现场踏勘。

二、招标文件

12、 关于招标文件

招标文件是采购人作为阐明所需服务的基本要求，招标文件、响应文件、最终报价函、评标结果、合同书和相关承诺确认文件均作为任何一方当事人履约的重要依据。

13、 招标文件的组成

第一章 招标公告

第二章 投标人（供应商）须知

第三章 采购人需求书

第四章 合同文本

第五章 响应文件格式及附件

第六章 评标细则

14、 招标文件的澄清和修改

14.1 投标人（供应商）如对招标文件有任何疑问，均应在响应文件递交截止日 7 日前，把疑问的内容编辑成 WORD 版本及同内容盖公章扫描后的 PDF 版本，同时发送到邮箱 zb87562291@163.com，并至电 020-87562291 转 8313（张工），向采购代理机构提出澄清要求。

14.2 采购人或者采购代理机构可以对已发出的招标文件进行必要的澄清或者修改。澄清或者修改的内容可能影响响应文件编制的，采购人或者采购代理机构应当在投标截止时间至少 5 日前，以书面形式通知所有获取招标文件的潜在投标人；不足 5 日的，采购人或者采购代理机构应当顺延提交响应文件的截止时间。

14.3 对招标文件进行必要更正的，采购代理机构将在相关网站发布更正公告，一经发布视为送达到所有潜在投标人（供应商），并按最新的更正公告内容进行采购活动。

14.4 招标（采购）过程中的一切修改文件或补充文件一旦确认后与招标文件具有同等法律效力，投标人（供应商）有责任履行相应的义务。

三、投标总则

15、 响应文件的编写

15.1 投标人（供应商）应仔细阅读招标文件的所有内容，并按招标文件的规定及附件要求的内容和格式，提交完整的响应文件，并保证所提供全部资料的真实性，所有不完整的投标将被拒绝。

15.2 投标语言和计量单位。响应文件和来往函件应用中文书写，投标人（供应商）提供的支持文件、技术资料和印刷的文献可以用其它语言，但相应内容应附有中文翻译本，以中文为准，计量单位应使用国际公制单位。

15.3 投标人（供应商）必须以人民币报价。响应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；对不同文字文本响应文件的解释发生异议的，以中文文本为准。

15.4 投标人（供应商）投标总价是以投标人（供应商）可独立完成本项目，并在通过准确核算后，可满足预期实施效果、验收标准和符合自身合法利益的前提下所作出的综合性合理最终含税报价，对在响应文件和合同书中未有明确列述、投标方案遗漏失误、市场剧变、汇率、利率因素和不可预见的费用等均视为已完全考虑到并包括在投标总价之内。投标人（供应商）应自行增加项目正常、合法、安全运行及使用所必需但招标文件没有列明或包含的内容及费用，并在响应文件中加以详细说明，如果投标人（供应商）在中标并签署合同后，在提供招标范围内的服务工作中出现的任何遗漏，均由中标人免费提供，采购人将不再支付任何费用。对超出常规、具有特别意义或会引起竞争非议的报价须作出特别说明。

15.5 招标文件中，如标有“★”的地方均为必须完全满足指标，投标人（供应商）须进行响应，投标人（供应商）若有一项带“★”的条款未响应或不满足，将按无效投标处理。

15.6 招标文件中，如标有“#”的地方均为重要参数和指标要求条款，投标人（供应商）若有部分“#”条款未响应或不满足，将导致其响应性评审严重扣分。

15.7 投标人（供应商）应对投标内容提供完整的、详细的、清晰的技术说明，如投标人（供应商）对指定的技术要求建议做任何改动，应在响应文件中清楚地注明；投标人（供应商）对招标文件的对应要求应当给予唯一的实质性响应，否则将视为不响应。技术参数要求中标注有具体数值要求的，投标人（供应商）必须在服务响应表中标注实际

数值，不标注数值者视为不响应。

15.8 投标人（供应商）响应招标需求应具体、明确，含糊不清、不确切、直接复制招标需求指标要求的或伪造、变造证明材料的，按照不完全响应或完全不响应处理。构成提供虚假材料的，投标人（供应商）承担法律责任。

15.9 投标人（供应商）对招标文件的合同不允许实质性偏离，否则将视为不响应。

15.10 资格文件视为响应文件不可分割的一部份，投标人（供应商）应提供相关证件、证明文件的复印件，否则，评标委员会有权不予采信。

15.11 响应文件按规定加盖的投标人（供应商）公章必须为企业法人公章，且与投标人（供应商）名称一致，不能以其它业务章或附属机构章代替。需签名之处必须由法定代表人或投标授权代表签署。

16、 响应文件的组成

16.1 响应文件由资格证明部分、技术商务部分构成。

16.2 技术商务部分、资格证明部分须按照第五章的要求编制。

16.3 技术商务部分和资格证明部分可合装或分别单独装订成册。

17、 投标

17.1 **纸质响应文件一式三份（一份正本、两份副本），响应文件电子版一份，首次报价信封一份。副本内容可采用正本的复印件，如果正本与副本不符，应以正本为准。响应文件电子版（U 盘）与响应文件纸质版一起密封**。

17.2 响应文件电子版一份。响应文件电子的载体应为 U 盘，不留密码，无病毒，内容应与投标人（供应商）打印产生的纸质响应文件内容一致，如有不同，以纸质响应文件为准。

17.3 响应文件封面右上角显著注明“正本”和“副本”字样，并加盖公章。

17.4 响应文件由投标人（供应商）的法定授权代表或法人代表签署，响应文件的任何修改均须由法定授权代表或法人代表签署。

17.5 投标人（供应商）提交响应文件时应出具：法定代表人证明书、法定代表人授权书（如有）、本人身份证，用以投标或竞价时检查其身份有效性**（参与竞价环节的供应商代表必须是：法定代表人或法定代表人授权书的被授权人。若供应商不能证明其身份的有效性，或者拒绝参与竞价环节，其投标无效）。**

17.6 所有响应文件及样板或模型（如有）应在投标截止时间前送达响应文件递交地点（时间及地点以第一章采购公告为准），并当面交予采购代理机构专责人员，采购代理机构将拒绝以下情况之一的响应文件：

（1） 迟于投标截止时间递交的；

（2） 以电报、电话、电传、传真或邮递形式递交的；

（3） 密封不严、册装不整的。

17.7 所有响应文件必须封入密封的信封或包装，在封口上加盖投标人（供应商）的公章。响应文件的正本和副本可以分别封装也可以一起封装，并在每一信封或包装的封面上写明：

收件人名称：广州宏达工程顾问集团有限公司
项目编号：TPA-2022-C3-115
项目名称：佛山电器照明股份有限公司网络安全建设项目
包装内容：响应文件正本/副本/首次报价信封
投标人（供应商）名称：
投标人（供应商）地址：
联 系 人：
联系电话：
在规定的开标时间　　年　月　日　　时　分前不得启封

17.8 采购代理机构对不可抗力事件造成的响应文件的损坏、丢失不承担任何责任。

17.9 采购代理机构不退还投标人（供应商）的响应文件及递交的其它资料。

18、 投标有效期

18.1 投标有效期为 90 天，投标有效期自递交响应文件的截止之日起算。

18.2 在特殊情况下，采购人在原定投标有效期内，可以根据需要以书面形式向投标人（供应商）提出延长投标有效期的要求，对此要求投标人（供应商）须在收到采购人书面通知后 24 小时内以书面形式向采购人送达答复，不按此回复，且经催告后 12 小时仍不回复的，视为同意。投标人（供应商）可以拒绝采购人这种要求，其投标失效，但投标人（供应商）有权收回其投标保证金。同意延长投标有效期的投标人（供应商），其权利及义务相应也延至新的截止期，在延长的投标有效期内既不能要求也不允许修改其响应文件。

19、 投标的修改和撤回

19.1 投标人（供应商）在投标截止时间前，可采用书面通知的形式向采购代理机构修改或撤回其响应文件。

19.2 在投标截止时间后，投标人（供应商）不得对其响应文件作任何修改。在投标有效期内，投标人（供应商）不得撤回其投标。

20. 开标

20.1 采购代理机构在《招标公告》中规定的日期、时间和地点组织开标。开标时原则上应当有采购人代表和投标人（供应商）代表参加。参加开标的代表应签到以证明其出席。

20.2 开标时，由投标人（供应商）或其推选的代表检查响应文件的密封情况，经确认无误后由采购代理工作人员当众拆封，宣读投标人（供应商）名称、投标价格、响应文件的其他主要内容和蹉商文件允许提供的备选投标方案。

20.3 采购代理机构做好开标记录，开标记录由各投标人（供应商）签字确认。

20.4 开标结束后，投标人（供应商）授权代表应在评标会场外等候，按评标进程由代理机构通知进场与评委进行竞价。

21. 评标委员会的组成和蹉商方法

21.1 评标委员会成员由采购人依法组建，

21.2 评标委员会依法根据招标文件的规定与投标人（供应商）进行评审及对最终形成的响应文件和最终竞价结果进行评审,并据此推荐成交候选人。

21.3 具体见第六章《评标细则》。

22. 评标程序

22.1 评标委员会将以随机抽签的形式对在本须知规定的时间内递交响应文件的投标人（供应商）进行综合得分排序。

22.2 评标委员会将按综合得分高低排序的顺序逐一与投标人（供应商）分别就价格进行相同轮次（一个或多个回合）竞价，并形成纪要文件。竞价目的在于澄清报价、明确需求，使所有投标人（供应商）的响应具有可比性。在竞价中，竞价的任何一方不得透露与竞价有关的其他投标人（供应商）的技术资料、报价和其他信息。

22.3 第一轮/第二轮竞价：投标人（供应商）应在评标委员会规定的时间内统一提交第一轮/第二轮竞价（第一轮/第二轮竞价时间视评标进程由评标委员会决定）并统一现场公布。

（1）评标过程对用户需求（包括规格、数量和服务等涉及价格变动因素）没有作出改变的，报价供应商的后次报价不得高于其前次报价；

（2）若报价供应商的后次报价高于其前次报价的，评标委员会有权确定其报价为无效报价；

22.4 技术商务评标的时间及地点(见招标公告)。

22.7 在评审过程中，报价供应商提交的响应文件、澄清文件、最终响应文件等，由报

价供应商法人代表或授权代表当场签字后生效，报价供应商应受其约束。

23. 响应文件的澄清

23.1 评审期间，对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容， 评标委员会可以书面形式（应当由评标委员会专家签字）要求投标人（供应商）作出必要的澄清、说明或者纠正，但不得允许投标人（供应商）对投标报价等实质性内容做任何更改。投标人（供应商）的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出响应文件的范围或者改变响应文件的实质性内容。有关澄清的答复均应由投标人（供应商）的法定代表人或授权代表签字的书面形式作出。

23.2 投标人（供应商）的澄清文件是其响应文件的组成部分。

24. 投标的评价

24.1 评标委员会只对投标人（供应商）提交的蹉商响应文件进行评价和比较。

25. 授标

25.1 评标委员会按照蹉商文件确定的蹉商方法、步骤、标准，对响应文件进行评审，提出书面评审报告，按照得分由高到低的顺序推荐综合得分排名第一的投标人（供应商）为中标候选人。综合得分并列时，投标报价低的投标人（供应商）名次靠前；若综合总得分和投标报价都相同，按技术部分得分确定名次。

25.2 中标人确定后，将在相应网站发布中标公告，并向中标人发出《中标通知书》。《中标通知书》对中标人和采购人具有同等法律效力。

26. 替补候选人的设定与使用：中标人放弃中标、不按要求与采购人签订采购合同、因不可抗拒力或自身原因不能履行采购合同的，采购人可以与排位在中标人之后第一顺位的投标人签订采购合同，以此类推，或者重新进行招标。

27. 项目废标处理

27.1 根据相关规定，下列情况出现将作废标处理：

27.1.1 符合专业资格条件的投标人（供应商）或者对蹉商文件作实质响应的有效投标人（供应商）不足三家的；

27.1.2 出现影响采购公正的违法、违规行为的；

27.1.3 投标人（供应商）的报价均超过了采购预算，采购人不能支付的；

27.1.4 因重大变故，采购任务取消的。

28、 合同的订立和履行

23.1 中标人应按采购人指定的时间和地点与采购人签订合同。

23.2 中标人在征得采购人许可的情况下，根据工作要求，可就非主体、非关键性工作

委托具备相应资质条件的单位开展。

29、 质疑处理相关事项

29.1 投标人（供应商）认为招标文件、采购过程、中标或者成交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、采购代理机构一次性提出针对同一采购程序环节的质疑，逾期质疑无效。投标人（供应商）应知其权益受到损害之日，是指：

（1）对招标文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；

（2）对采购过程提出质疑的，为各采购程序环节结束之日；

（3）对中标结果提出质疑的，为中标结果公告期限届满之日。

29.2 采购人、采购代理机构在收到质疑函后 7 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。

采购代理机构：广州宏达工程顾问集团有限公司

联 系 人：周业连

联系电话：020-87562291-8313

地　址：广州科学城科学大道 99 号科汇金谷二街七号

邮　编：510663

29.3 投标人（供应商）提出质疑内容应当依据“谁主张谁举证”的原则，不得含有虚假、恶意成分。对于捏造事实、滥用维权扰乱采购秩序的恶意质疑者或举证不全查无实据被驳回次数在一年内达三次以上，将纳入不良行为记录名单并承担相应的法律责任。

29.4 投标人（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：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

质疑函应当署名。质疑供应商为自然人的，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。

29.6 投标人（供应商）对采购人或采购代理机构的答复不满意或他们未在规定时间内给予答复的，提出质疑的投标人可以在答复期满后 15 个工作日内，向采购项目所属的

监督管理机构投诉，投诉的事项不得超出已质疑事项的范围。

第三章 采购人需求书

采购人需求书

说明：

投标人须对本项目为单位的招标标的或服务内容进行整体响应，任何只对其中一部分招标标的或服务内容进行的响应都被视为无效投标。

招标文件中，如标有“★”的地方均为必须完全满足指标，投标人须进行响应，投标人若有一项带“★”的条款未响应或不满足，将按无效投标处理。

招标文件中，如标有“#”的地方均为重要参数和指标要求条款，投标人若有部分“#”条款未响应或不满足，将导致其响应性评审严重扣分。

第一章 佛山电器照明股份有限公司网络安全建设项目需求说明书

一、项目建设目标

本项目将优化调整禅城总部、高明公司及南宁燎旺公司的内部网络规划，增加相应专业安全设备，形成新的网络安全防护体系。主要目标及功能如下：

1、建立 IT 资产管理制度

通过本项目建全 IT 资产安全管理制度,规定信息系统资产管理的责任人员、责任部门和管理职责，协助项目推行落地。编制并保存与信息系统相关的资产、资产所属标识、所属关系、安全级别和所处位置等信息的资产清单。

2、网漏洞扫描

本项目根据已有的安全漏洞知识库，模拟黑客的攻击方法，检测工控主机、网络协议、网络服务、网络设备、应用系统等各种信息资产所存在的安全隐患和漏洞并加以弥补。

3、模拟渗透测试

在本项目进行渗透测试（Penetration Test），即完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全作深入的探测，发现系统最脆弱的环节，并在后期项目实施过程中对已经发现的问题进行整改。

4、基础网络的安全防护能力

本项目需有效提高禅城总部与高明公司、南宁燎旺公司的链路安全能力，并可进行数据传输加密。

5、促使生产网与办公网流量分离

本项目需在（高明公司）生产网与办公网之间建立流量汇聚交换机制，对生产网及办公网的流量进行逻辑划分，在保证生产网及办公网的数据交换基础上进行边界防护。

6、保障工控网络安全

本项目需增加（高明公司）网络安全防护设备，保障生产网络安全，阻止办公网络对生产网络的安全攻击。

7、增强入侵检测安全保护

本项目需针对（高明公司）生产网络内部的工控主机进行深度检测，即系统地采用特征检测技术、工控异常行为检测技术、黑白名单技术、基线技术等技术手段，对网络流量进行深度包解析和流解析，实现对病毒、木马、蠕虫、僵尸网络等各种威胁的全面有效检测。

8、提升工控主机安全保护

本项目需构建（高明公司）可控、可靠、可管理以及符合安全基线规范的工控网络的纵深安全防御体系。

9、净化公司互联网上网环境

本项目需在南宁燎旺公司增加上网行为管理及入侵检测设备，优化上网流量，净化上网环境，增加七层数据检测机制，优先保障重要业务带宽需求。

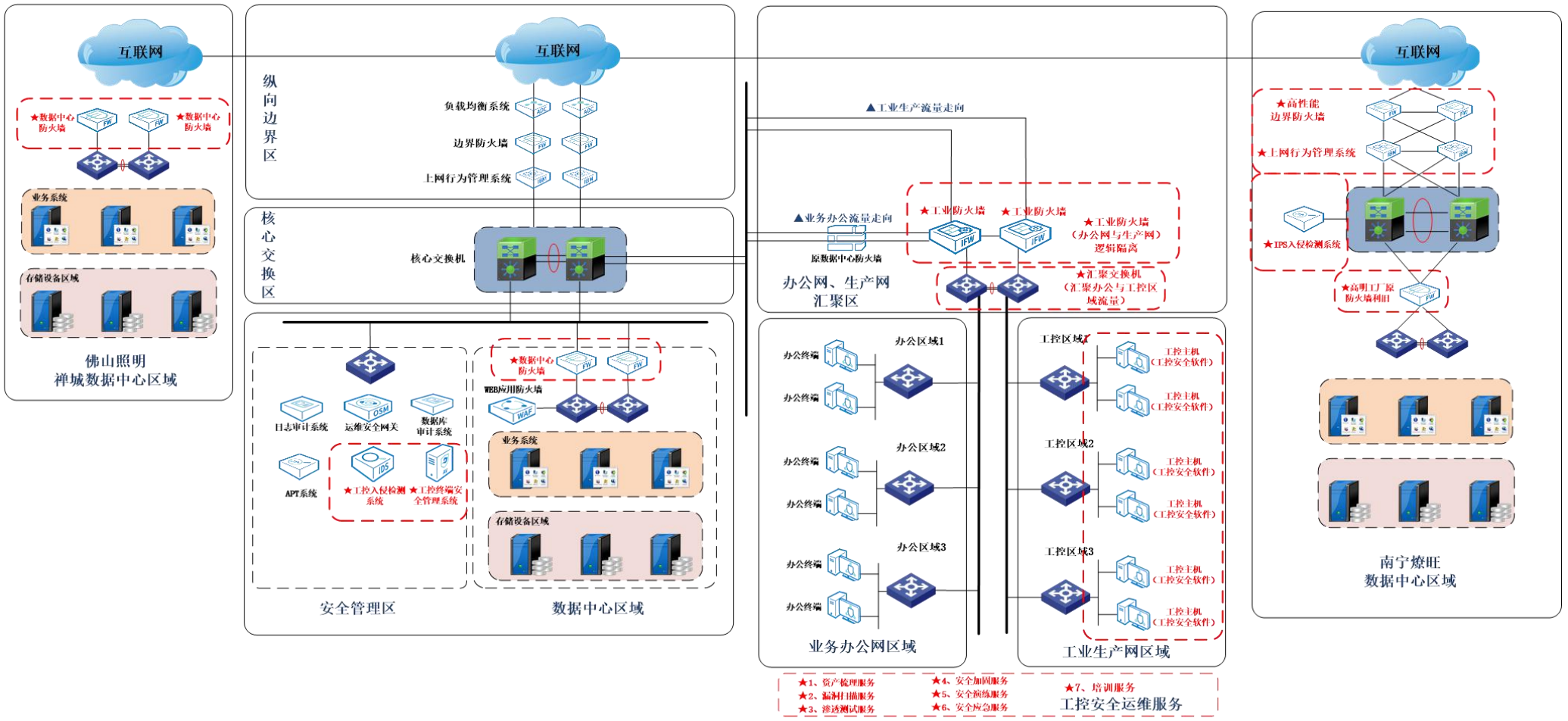
10、建立应急响应机制

信息安全事件应急响应机制是信息安全保障的最后一道防线，本项目需将各类突发信息安全事件的影响控制在可接受的范围之内。

二、项目建设内容

1、项目总体拓扑图

佛山照明网络安全加固建设项目拓扑图



2、项目建设内容

项目针对高明公司、南宁燎旺公司及公司总部进行网络安全升级加固。

（1）增加公司总部数据中心防火墙，建立公司总部与高明公司、南宁燎旺公司的数据加密链路，保证两地数据传输的完整性、安全性。

（2）高明公司增加部署数据中心防火墙，保障通过办公网络和生产网络访问数据中心的数据安全及传输安全，防止来自办公网络、生产网络的流量攻击及病毒，保障数据中心安全。

（3）高明公司生产内部网络当前对于工控主机没有防护能力，且面临着日益加大的网络攻击威胁，需在生产内部网络增加部署工业防火墙，防止从办公网络向生产网络的渗透攻击；增加部署工控入侵检测系统，安装工控主机安全卫士，保证工控主机系统安全。

（4）在南宁燎旺公司的互联网出口处增加边界防火墙，保障与禅城总部的数据加密传输，防止来自互联网的流量攻击及渗透，增加流量控制系统，针对互联网流量进行分析比对，保障网络通畅，阻断内部访问非工作的网站，过滤内部向外部的敏感信息，保障南宁燎旺公司的绿色办公环境，部署入侵检测系统和利旧原高明公司数据中心防火墙，防止外界对内网的渗透攻击。

（5）工控安全运维服务。

3、设备部署方式

序号	设备名称	部署地点	部署方式
1	数据中心防火墙	禅城总部、 高明厂区数据中心	路由部署
2	工控终端管理系统	高明公司数据中心	机柜安装部署
3	工业防火墙	高明公司数据中心	路由部署
4	工控入侵检测系统	高明公司数据中心	旁路/路由部署
5	汇聚交换机	高明公司数据中心	路由部署
6	互联网防火墙	南宁燎旺公司数据中心	路由部署
7	上网行为管理系统	南宁燎旺公司数据中心	旁路/路由部署
8	网络入侵防御系统	南宁燎旺公司数据中心	旁路/路由部署

4、设备、服务项目数量需求

序号	设备类别	数量	单位
1、安全设备部分			
1	防火墙（南宁燎旺厂区）	2	台
2	上网行为管理（南宁燎旺厂区）	2	台
3	入侵防御系统（南宁燎旺厂区）	1	台
4	数据中心防火墙（高明厂区）	2	台
5	工业防火墙（高明厂区）	2	台
6	工控入侵检测系统（高明厂区）	1	台
7	工业主机安全卫士（高明厂区）	400	个
8	数据中心防火墙（禅城总部）	2	台
9	统一安全运维平台	1	套
10	汇聚交换机（高明厂区）	2	台
2、安全服务部分			
9	IT 资产梳理服务 4 次，为期 1 年	1	项
10	漏洞扫描服务 4 次，为期 1 年	1	项
11	安全加固服务 4 次，为期 1 年	1	项
12	应急响应服务 2 次，为期 1 年	1	项
13	应急演练服务 2 次，为期 1 年	1	项

14	渗透测试服务 1 次，为期 1 年	1	项
15	安全培训服务 4 次，为期 1 年	1	项

附件五　网络安全技术参数指标

一、网络出口防火墙（南宁燎旺厂区）

序号	指标项	详细技术参数
1	★硬件参数要求	标准机架式，配备冗余电源，标准配置≥6 个 10/100/1000M 自适应千兆电接口，≥4 个千兆 SFP 接口，≥4 个 SPF+万兆接口；存储容量不少于 120G；
2	★性能参数要求	整机最大吞吐量≥25G；标准配置下最大并发连接≥590 万；每秒 TCP 新建连接数≥24 万/秒；IPSec VPN 吞吐量 bps≥4G；IPSec VPN 默认隧道数≥9800
3	★基础功能	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。
4		开通 SSL VPN 功能、网络入侵防御功能、网络应用识别功能、网络防病毒功能；配置 SSL VPN 并发用户数不少于 200 个。
5	部署适应性	支持路由模式、透明（网桥）模式、混合模式
6	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
7		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
8	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。
9		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）
10		具备协议自动识别功能；支持自定义事件功能。
11	#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。
12		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。 （提供相关界面截图）
13		内置多种沙箱环境与应用环境，使用反反沙箱、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。

14	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）
15	网络特性	支持静态路由、RIP v1/2、OSPF、BGP、策略路由等
16		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
17		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）
18		支持服务器负载均衡，支持一个公网 IP 映射到内网多台服务器，服务器间支持连接和源地址 hash,支持服务器健康检查（提供 WEB 配置截图）
19		#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
20		支持一对一、地址池等 NAT 方式，支持必须支持多种应用协议，支持策略 NAT 功能
21		支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323 等
22		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
23		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
24		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）
25	★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
26		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
27		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
28	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
29		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
30		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
31		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
32	SDWAN	支持广域网双边优化，通过使用 TCP 动态拥塞控制、TCP 窗口处理机制优化、TCP 选择性应答、使用快速 TCP 协议传输以及数据压缩机制，实现对业务访问的有效加速
33		#对 SD-WAN 隧道的时延、抖动、带宽占用率、丢包率等提供可视化展示；提供相关界面截图

34		#支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线；提供相关界面截图
35		通过 WAN 虚拟化技术实现多条链路捆绑，同一个 session 数据可以在多条链路上同时传输，加速大文件复制业务；提供相关界面截图
36	集中管理	#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
37	资质服务要求	销售许可证：产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，要求出具证书复印件。
38		产品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
39		产品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
40		产品具备国家计算机软件著作权登记证书，提供证明材料
41		产品具备 IPv6 Ready logo Phrase 2 认证；提供有效的资质证明复印件
42	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
43		#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
44	★服务	提供原厂三年维保服务，包括版本升级（包含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

二、上网行为管理（南宁燎旺厂区）

序号	指标项	详细技术参数
1	★硬件规格	标准机架式，标准配置≥12 个 10/100/1000M 自适应千兆电接口，≥12 个千兆 SFP 接口，≥2 个 SPF+万兆接口，存储容量不少于 500G
2	★性能要求	网络层吞吐量≥5.5Gb，应用层吞吐量≥800Mb，每秒新建连接数≥10000，最大并发连接数≥50 万，支持用户数≥3500。（提供厂商证明彩页）
3	部署适应性	支持路由模式、透明（网桥）模式、混合模式，支持镜像接口
4		支持静态路由、策略路由、动态路由、ISP 路由；策略路由支持七元组策略；动态路由支持 RIP、OSPF 等；ISP 路由支持运营商地址自定义
5		网络部署支持虚拟网线部署，且支持 vlan 标签的过滤（提供 WEB 配置截图）
6		支持针对链路质量的实时监控（提供 WEB 配置截图）

7	行为管控	系统内置多个常见场景的应用标签，且标签支持管理员自定义。（提供 web 截图）
8		用户管理、应用管理支持树型结构。（提供 WEB 配置截图）
9		支持 HTTPS 解密功能，支持页面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https 对象、域名排除等。支持针对 HTTPS 网站、HTTPS 搜索记录、HTTPS 邮箱等内容进行审计；HTTPS 邮箱支持审计主题、内容、附件等；支持 HTTPS 域名库，预定义域名以及自定义域名
10		基于 P2P 行为和迅雷行为的应用智能识别技术（提供 WEB 配置截图）
11		支持支持基于邮件收件人、发件人的黑白名单自定义控制方式（提供 WEB 配置截图）
12		支持终端类型检测和控制，以及显示终端趋势（提供 WEB 配置截图）
13		针对系统运行过程中的应用统计，支持应用的热度图（提供 WEB 配置截图）
14		基于全局白名单功能，可针对 IP 和 MAC 地址（提供 WEB 配置截图）
15		终端提示页面基于代码层面的用户自定义（提供 WEB 配置截图）
16	上网认证	支持 WEB Portal 认证功能，支持本地认证、Radius 认证、LDAP 认证 和 LDAP 用户同步，支持对接 IMC、SAM 等常见 AAA 服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向 URL，要求本机自身支持短信认证功能
17		支持二维码认证，终端可以通过管理员扫描二维码授权方式上网（提供 WEB 配置截图）
18		支持旁路部署 WEB 认证（提供 WEB 配置截图）
19	策略配置	#提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可在 WEB 界面显示检测结果；支持实时和周期性对所有安全策略进行分析(提供 WEB 配置截图)
20		支持阻断功能， 支持限流功能， 支持干扰功能， 支持告警功能， 支持输出报表功能， 支持基于用户、源/目的 IP、时间、应用等综合任意组合进行控制
21	安全防护	支持杀毒功能，可对 HTTP、FTP、POP3、SMTP、IMAP 协议的病毒进行查杀；支持多种压缩文件的病毒查杀。压缩默认支持 5 层，最大 20 层（提供 WEB 配置截图）
22		提供 WEB 防护功能，可对防盗链、CSRF 攻击、CC 攻击防护、网页防篡改等攻击行为进行防护。（提供 WEB 配置截图）
23		支持端口扫描功能，用于直观的了解网内主机所存在的安全问题。（提供 WEB 配置截图）
24		支持弱密码扫描功能，即时了解网内主机是否存在弱口令，内置弱口令库，并可自定义字典库。（提供 WEB 配置截图）
25		提供威胁情报功能，支持全网威胁情报的搜索查询，可供攻击溯源，预知风险；支持威胁情报订阅，及时对突发威胁进行防护建议;支持 20 余种威胁分类，包括 C&C、僵木蠕、勒索、钓鱼、垃圾邮件等（提供 WEB 配置截图）
26		#支持 IPS 功能，支持基于源、目的、规则集的入侵检测；支持针对 WEB 服务器防护，包括木马/后门、挖矿、病毒蠕虫、SQL 注入、木马外联、间谍软件、工控攻击等。（提供 WEB 配置截图）

27	流量报表	支持基于流量大小、用户属性、应用类型、IP 地址、时间段、使用频率等
28	其它	#系统支持软件补丁升级，以及热补丁技术（提供 WEB 配置截图）
29		系统管理员外部方式认证方式，外部认证服务器故障可以切换为本地认证（提供 WEB 配置截图）
30		针对设备系统健康检测功能，可以在某一时间段内逐级深入，并篡取任一时间内的详细信息，并可路转系统日志。（提供 WEB 配置截图）
31		支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其 Top 流量用户
32	资质服务要求	销售许可证：产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，要求出具证书复印件。
33		产品具备 IPv6 Ready logo Phrase 2 认证；提供有效的资质证明复印件
34		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
35		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
36		#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
37	★服务	提供原厂三年维保服务，包括版本升级（含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

三、网络入侵防御系统（南宁燎旺厂区）

序号	指标项	详细技术参数
1	★硬件规格	标准机架式，冗余电源，≥1 个 RJ-45 Console 口，≥1 个管理口，≥1 个 HA 口，≥4 个具备 BYPASS 功能的 10/100/1000 自适应千兆电接口，≥4 个千兆 SFP 接口，≥2 个 SPF+万兆接口，≥2 个扩展插槽，
2	★性能要求	开启 IPS 功能下最大吞吐量≥25G；开启 IPS 功能下最大并发连接≥500 万；每秒新建连接数≥20 万
3	入侵防御功能	#系统应支持自定义事件升级内容。升级界面中至少包含高中低三种级别事件的升级启用选项。并支持可自动修改动作为通过，满足业务高连续要求下的事件监测要求（提供功能截图）
4		系统应支持无线攻击检测和防护功能扩展，可手工或自动识别和区分内部 AP 和外部 AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法 AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支持多种类型流氓 AP 的检测与阻断（提供功能截图）
5		系统应内置未知恶意代码检测引擎，能检测流经的 http、ftp、邮件协议中包含的 office 文档、图片文档及压缩文档中的未知恶意文件,报警信息应包括源

		目的 IP、协议类型、文件基本信息、检测方法、危险等级及文件的应用的详细信息（如邮件的发件人、收件人、标题等），方便跟踪恶意文件，需说明此引擎和防病毒引擎的区别、实现原理和效果（提供功能截图）
6		#系统应支持单独的恶意样本检测规则升级功能，方便对恶意样本检测功能进行扩充（提供功能截图）
7		#系统应支持恶意样本自学习功能，除通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息（提供功能截图）
8		系统应支持未知 C&C 通道（隐蔽通道）检测功能，能够提供 C&C 通道的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址和端口等 C&C 通道信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等
9		可基于 IP 地址、网段、时间、VLAN、协议类型等条件设定 IPS 检测及响应方式
10		支持虚拟 IPS 功能，不同的用户可以方便定制满足自身要求的检测模版
11		系统应具备网络准入控制能力，通过和终端管理系统联动，拒绝不安全主机连入网络，说明网络准入控制原理和实现效果
12		威胁情报类型覆盖安卓恶意程序、APT 攻击、远控木马、僵尸网络、僵尸主机、挖矿、DDOS 攻击、欺诈、赌博、物联网/IOT 攻击网络、物联网/IOT 失陷主机、恶意网站、钓鱼、勒索软件、web 攻击主机、网络蠕虫等（提供功能截图）
13		系统应支持威胁情报，通过通用接口获得第三方的威胁情报，提升防御能力
14		系统应支持特殊环境下的攻击源真实地址还原能力
15		系统应具备终端和服务器环境感知能力，通过主动扫描和扫描结果导入获得终端环境情况（提供功能截图）
16		系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证
17		系统应支持多种事件响应方式，满足客户的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作
18		采用先进的模式匹配及协议分析技术实现对网络报文的分析
19		具备协议自动识别功能
20		支持检测规则自定义功能
21		系统应支持常见默认事件集，便于用户使用，默认事件集至少包括：全集、中高级事件、僵尸木马蠕虫事件集、WEB 事件
22		事件库应支持 CVE 和 CNNVD 兼容能力
23		系统应支持 QQ 和 MSN 应用识别功能，支持黑白名单功能，阻止或允许部分帐号登录（提供功能截图）
24		系统应支持密码穷举探测功能，提供至少 20 种密码穷举行为特征探测和阻断
25		系统应支持弱口令检测功能，需支持至少 8 种网络协议并支持至少 7 种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素
26		系统应提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护
27		#针对 SQL 注入和 XSS 攻击，设备应支持在线事件分析功能。SQL 注入至少提供攻击位置、攻击方法、解码后数据、攻击域、影响的数据库等，XSS 攻击至少提供协议字段、攻击数据、解码后数据、攻击域、编码方式等，并提供功能截图

28		#系统应针对 SQL 注入、XSS 攻击提供白名单功能。XSS 攻击白名单能够精确到检测点、属性和名称。SQL 注入白名单并支持至少 10 类和 70 个配置项目（提供功能截图）
29		系统应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 4 个不同级别的扫描容忍度/扫描敏感度
30	★部署方式	系统应提供旁路部署及在线、旁路混合部署等部署方式
31		系统应支持 IP 地址转换（NAT）功能，包括：源地址转换、目的地址转换、静态地址转换。
32		系统应支持桥组部署方式，并支持 STP 协议
33		系统应支持路由模式，至少包括：静态路由、策略路由、ISP 和 OSPF 路由协议
34		支持 DHCP 功能，包括 DHCP 服务器和 DHCP 中继功能。并可以作为客户端获得 IP 地址，满足客户自动化管理的需要。（提供功能截图）
35		系统应支持端口聚合/链路捆绑协议，并提供手工方式和 LACP 两种配置方式
36		系统应支持完善的会话管理功能，可实时查看当前会话状态，支持根据源地址、目的地址、端口号或协议类型查询会话
37	防病毒功能	系统应支持通过授权扩展支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能
38		系统应支持通过授权扩展支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的文件屏蔽功能，防止文件的下载和传输
39		系统应支持 VLAN、VoIP 数据流病毒过滤
40		系统应支持双病毒引擎，需提供包括国产厂商在内的防病毒引擎厂商合作证明
41		系统应支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 30 万
42		系统应支持 HTTP 协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息
43		系统应支持 Web 过滤功能，至少支持黑白名单、关键字过滤、禁止 HTTP 代理外，还支持 Script、 Java Applet 等过滤，并能通过统一模版设置
44	内容防护	系统应支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件 SMTP 命令、发件人、主题、附件、IP 及邮件大小进行过滤
45		系统应支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、固定电话号码、银行卡、IP 地址等敏感信息，并支持文件指纹识别和白名单功能。并说明支持的应用情况和处理方式（提供功能截图）
46	★高可用性	系统应支持双机热备和双机主备功能，并且主备热备时需支持连接状态和配置同步
47		系统应支持硬件 BYPASS。在设备故障、重启及断电的情况下可保障网络畅通，能够手动配置 BYPASS 的启停
48		系统应支持软件 Bypass 功能，通过 CPU 和内存阈值实现软件 Bypass 的开启，提供不同的阈值计算方式（最高值/平均值、时间区间等）
49		系统应支持重点资产和应用监控功能，当资产和应用出现异常时，通过 syslog 和邮件进行告警，并可以记录日志
50		系统应支持多种设备管理方式，包括 HTTPS、CONSOLE、SSH、TELNET 等
51	管理功能	系统应支持 WEB 登录图像验证码功能，防止暴力破解

52		系统应支持在线管理员数目限制和管理员唯一性检查功能，提高系统管理的安全性
53		需支持动态口令卡或 Ukey 方式的双因子认证，增强配置管理的安全性
54		系统应支持定期修改密码功能
55		系统应支持较强的密码安全性，提供首次登录密码修改功能，首次登录时提供强制修改和提醒修改两种方式
56		#系统应提供系统监控和趋势曲线图展示，至少支持内存占用率、CPU 占用率、总流量、每秒新建连接数、并发会话数的趋势图，可按照时间段展示趋势曲线（提供功能截图）
57		系统应支持历史入侵事件处理功能，直接对历史事件进行分析和处理，并用于未来事件检测。并可以查询处理情况
58		支持场景分析功能，提供进行更深入的分析能力，至少包括僵尸木马蠕虫的分布式攻击场景分析
59		系统应支持本地日志及 SYSLOG 日志发送，支持向至少 2 个 syslog 服务器发送日志
60		#系统应支持 syslog 格式修改功能，通过对日志内容裁剪、修改次序，满足用户安全管理平台日志格式要求。（提供功能截图）
61		系统应提供 netflow 日志发送功能，满足第三方管理平台对 netflow 日志的审计需求
62		系统应支持声音报警，通过设置事件级别、入侵事件级别和病毒事件进行声音报警
63		系统应支持报表个性化设置，通过自定义报表生成单位、报表生成人、单位 logo 和安全摘要信息等信息，快速生成符合单位特点的报告，减少工作量
64		系统应提供定期自定发送报表功能，通过邮件将 html、doc、xls、CSV 和 pdf 格式报表发送给管理员
65	日志功能	能够按照用户需求生成各种风格的统计报表，并可导出标准格式文档
66		支持本地磁盘、syslog 服务器、远端服务器等多种日志告警保存方式
67		支持提供实时和历史报告，该报告能够使网络操作员、安全管理员和用户能够通过详细信息检测攻击、制定策略并抵御攻击，支持用户自定义报表模版，支持将报告统计数据输出为文本文件，供后端定制或后续查看
68	产品资质	销售许可证：产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，要求出具证书复印件。
69		产品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。
70	★服务	提供原厂三年维保服务，包括版本升级（含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

四、数据中心防火墙（高明厂区）

序号	指标项	详细技术参数
1	★硬件规格	标准机架式；冗余电源，标准配置≥6 个 10/100/1000M 自适应千兆电接口，≥4 个千兆 SFP 接口，≥4 个 SPF+万兆接口，存储容量不少于 120G

2	★性能要求	整机最大吞吐量≥25G；标准配置下最大并发连接≥500 万；每秒 TCP 新建连接数≥24 万/秒；IPSec VPN 吞吐量 bps≥4G；IPSec VPN 默认隧道数≥9600；
3	★基础功能	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
4		开通 SSL VPN 功能、网络入侵防御功能、网络应用识别功能、网络防病毒功能；配置 SSL VPN 并发用户数不少于 200 个。
5		开通 WAF 功能
6	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
7		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
8		支持路由、透明及混合部署模式
9	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
10		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
11		具备协议自动识别功能；支持自定义事件功能
12	★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
13		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
14		内置多种沙箱环境与应用环境，使用反反沙箱、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
15	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
16	网络特性	支持静态路由、RIP v1/2、OSPF、BGP、策略路由等
17		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
18		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
19		#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
20		支持一对一、地址池等 NAT 方式，支持必须支持多种应用协议，支持策略 NAT 功能
21		支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL＊NET
22		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
23		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
24		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
25	★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

26		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
27		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
28	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
29		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
30		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
31		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
32	集中管理	#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。
33	资质服务要求	销售许可证：产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，要求出具证书复印件。
34		产品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
35		产品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
36		产品具备国家计算机软件著作权登记证书，提供证明材料
37		产品具备 IPv6 Ready logo Phrase 2 认证；提供有效的资质证明复印件
38	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
39		#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
40	★服务	提供原厂三年维保服务，包括版本升级（含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

五、工业防火墙

序号	指标项	详细技术参数
1	★硬件规格	标准机架式，冗余电源，标准配置≥6 个 10/100/1000M 自适应千兆电接口（2 对 bypass）,≥2 个千兆 SFP 接口，≥2 个 SPF+万兆接口，≥2 个扩展插槽
2	★性能要求	最大吞吐量≥4.8G，最大并发连接≥320 万；每秒新建连接数≥39600
3	系统管理	#支持系统盘、数据盘最少双存储磁盘结构，可以显示各磁盘使用率；（提供界面截图）
4		#支持双系统引导，可在管理界面配置启动顺序，自由选择当前启动系统，同时具有备份系统；（提供界面截图）

5		B/S 管理模式下，支持基于数字证书认证方式的管理员验证；（提供界面截图）
6		支持三权分立功能，内置系统管理员、安全管理员、系统审计员；并可设定管理员口令安全策略，可设置管理员有效期及休眠期；（提供界面截图）
7		支持 IPV4、IPV6 管理主机设置，具备基于白名单机制的管理主机列表功能；（提供界面截图）
8		支持异常行为特征库升级，包含病毒防护和入侵检测特征库，并显示特征库升级记录；（提供界面截图）
9	网络适应性	#产品支持串行部署及旁路部署；
10		串行部署支持路由、透明、冗余、trunk、镜像模式部署；（提供界面截图）
11		旁路模式支持单臂和流量镜像到工业防火墙，进行安全检查；
12		支持 VLAN 功能，支持 TRUNK 模式，可配置 ISL、dot1q、nego 等模式；（提供界面截图）
13		支持 IP/MAC 地址绑定功能，支持 IP 探测和网口探测两种方式；（提供界面截图）
14		支持地址转换，包括 SNAT、端口映射、IP 映射功能；（提供界面截图）
15	网络防护	#支持防火墙模式配置，支持全通模式、调试模式、防护模式、监听模式四种方式，其中监听模式采用旁路部署方式验证安全规则（截图证明）
16		访问控制规则支持引用时间对象、地址对象、协议及协议组、MAC 地址、接口对象等进行访问控制
17		#支持 OPC_Classical、FTP、H323、H323_GK、IRC、MMS、RTSP、SIP、TFTP 和 TNS 动态端口协议的访问控制
18		支持全局抗攻击功能（包括抗地址欺骗、抗源路由攻击、抗 SMURF 攻击、抗 LAND 攻击、抗 WINNUKE 攻击、抗 QUESO 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描、抗 Ping of Death）
19		支持基于包过滤规则的抗 SYN FLOOD、抗 UDP FLOOD、抗 ICMP FLOOD 和 IP 会话数控制
20	网络分析	基于整机、接口维度的流量统计
21		支持基于整机会话实时统计
22		支持根据连接数对 IP 进行实时排行
23	管理配置	支持通过 SSH 方式对设备进行管理
24		支持管理主机设置，具备基于白名单机制的管理主机列表功能
25		支持三权分立功能，内置系统管理员、安全管理员、系统审计员；并可设定管理员口令安全策略，可设置管理员有效期及休眠期
26		支持日志中文化，可显示配置命令日志的操作人
27	★高可用性	支持基于 802.3AD 标准的多端口聚合，实现零成本扩展带宽
28		支持 HA 主备工作模式（截图证明）
29		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
30	工业安全规则	支持自动学习工业网络的资产、流量、协议、IP、MAC、厂商信息等信息
31		支持工业协议（包含 Modbus、S7、DNP3、IEC104、EIP、OPC-DA、OPC-UA、SECS-GEM、MMS 等）指令的自动发现，并可自动生成白名单规则
32		具备访问控制规则向导助手功能，可自动学习网络连接关系，并支持自动聚合辅助快速生成访问控制规则

33	预置协议及模型	预置 64 种以上工业协议，并清晰显示相关协议的类型及使用端口
34		预置 128 种以上通用协议，并提供类型、端口及协议简介信息
35	OPC 协议深度内容检测及过滤	支持 OPC-classical 协议动态端口解析防护
36		支持 OPC-classical 协议完整性检查
37		支持 OPC 应用层内容细粒度管控，支持点位自学习并可实现点位控制（截图证明）
38		#支持 OPC 应用层内容细粒度管控，可实现方法自学习和控制（截图证明）
39	工业协议深度内容检测和过滤 DPI 功能	支持 Modbus、IEC104、EIP（Ethernet/ip）、DNP3.0、S7、OPC-UA、SECS-GEM 等主流工业协议深度内容监测和过滤：支持协议完整性校验和合法性检查；支持设备地址、功能码、寄存器、读写权限等字段解析和控制
40		支持基于阻断时的 RESET 回复
41	串行及现场总线协议深度过滤-MODBUS/RTU	产品支持串口 RS232、RS485 数据通信
42		支持串口通信参数配置，包括波特率、数据位、奇偶校验、停止位、流控。
43		支持 MODBUS/RTU 阻断情况下异常回复
44		支持 MODBUS/RTU 合规性及状态检查
45		支持 MODBUS/RTU 功能码、线圈地址、输入地址、设备地址、寄存器地址等协议报文内容的访问控制
46	工业威胁防御	自定义协议引擎规则：可支持协议变量、函数、运算操作符和数据类型的自定义规则生成
47		支持可以按照数据包内容手动自由定义协议响应特征，支持二层、三层工业协议自定义
48	工业 VPN	支持网关到网关模式的 IPSEC 隧道加密防护
49		支持隧道配置，可指定保护类型为接口或者 IP 地址段
50		支持隧道、隧道组监控功能，可实时显示隧道状态是否正常，并实时统计和显示隧道内流量及 SA 倒计时时间情况
51	集中管控	支持对设备统一管理、升级、配置下发、备份与恢复等批量操作
52		支持设备状态实时监控和历史状态查询，支持近 24 小时，近 7 天告警，支持告警规则配置，告警信息包括，高危级别、严重级别、普通级别、接口接收流量、接口发送流量、接口状态、CPU 使用率、内存使用率、硬盘空间利用率等
53	产品资质	具备公安部计算机系统安全产品质量监督检验中心签发的工控增强级检验检测报告
54		具备国家版权局颁发的《计算机软件著作权登记证书》
55		具备工信部《工业控制系统专用防火墙安全质量检测报告》
56		具备国家工业控制系统与产品安全质量监督检验中心、工信部出具的《工业智能设备安全防护装置》测试报告
57	★服务	提供原厂三年维保服务，包括版本升级（包含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

六、工控入侵检测系统

序号	指标项	详细技术参数
1	★硬件规格	标准机架式，冗余电源，≥1 个 RJ-45 Console 口，≥6 个 10/100/1000 自适应千兆电接口，≥2 个扩展插槽

2	★性能要求	实际网络环境处理能力≥2G；开启最大并发连接≥296 万；每秒新建连接数≥3.84 万
3	攻击检测	支持 Webshell 请求、XSS 攻击、SQL 注入、CSRF、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、越权访问、XXE 注入等常见入侵攻击
4		支持挖矿活动、勒索软件、僵木蠕等恶意程序检测
5		支持针对特定主机的 TCP FLOOD、UDP FLOOD、ICMP FLOOD 攻击等常见的拒绝服务攻击（DDOS）的检测，可通过控制界面配置攻击的检测时间和阈值条件
6		#支持离线检测技术
7	漏洞知识库	内置漏洞知识库，覆盖通用漏洞和工控资产漏洞检测
8	场景分析	#设备支持脆弱口令分析场景；支持分析登录用户名、用户口令（需特定账户查看）、访问时间
9		#支持口令暴力猜解，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态，能通过控制界面配置攻击的检测时间和阈值条件
10		#具备病毒检测分析场景，展示病毒文件名称、病毒名称、协议类型，传播时间等内容，可以对病毒日志文件进行下载
11	流量分析	支持 IP 地址、服务端口、区域、业务应用等不同视角的流量统计分析
12		支持对接口流量进行实时统计；支持总字节数、上下行字节数、总包数、上下行包数等不同粒度统计
13		支持自定义网络区域、自定义应用业务配置
14		违规流量检测，支持按时间范围、IP 等条件进行条件过滤，支持审计记录导出
15	工控协议审计	支持 iec61850mms、dnp3、egd、s7、iec104、cip、profinet、modbus、omron、opcua、opcda、enip 等工控协议进行识别
16		支持常见 HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、JABBER、SMB、Dcerpc、IRC、DNS、IKEV2、NFS、Krb5、DHCP、SNMP、SIP、RFB、RDP 等应用层协议
17		#支持对加密流量进行解密及还原：(HTTPS 证书支持 SSL3.0，TLS1.0/1.1/1.2)
18		支持 Modbus、S7、OPC、IEC104、IEC61850 等常用工控协议支持深度解析，审计粒度支持五元组、设备 id、类型、时间、控制点位、控制命令、控制值等
19		支持根据时间、IP 地址、端口号、协议、点号范围、指令码范围等条件过滤查询工具
20		支持对工控 DNP3、Profinet、enip、MQTT 等协议的深度解析和检测
21		支持对工控 Modubs、S7、IEC104 等协议遥控、遥调等关键操作行为进行监测
22	溯源取证	设备具备告警事件数据包留存能力，支持 pcap 格式
23		具备审计事件数据包留存能力，支持对告警事件，审计事件等进行报文录制用于取证分析，提供 16 进制原始报文和 pcap 包两种留存方式
24	资产管理	支持资产信息的全量导入导出
25		支持自动发现资产，支持发现终端、服务器、网络设备、安全设备、PLC、RTU、通信机、传感器、执行器等类型
26		支持通过扫描方式发现资产，资产支持的类型包括终端、视频设备、办公设备、网络设备、服务器、安全设备、PLC、RTU、通信机、传感器等
27		支持通过扫描实现对资产精准识别，粒度包含设备类型，操作系统类型（如 Windows，linux 等），MAC 地址，IP 地址，端口服务等资产信息
28	通信拓扑	支持基于流量会话自动绘制资产间的通信关系、并关联资产信息等
29		支持以可视化方式展示，支持导航器、拖动、放大、缩小、适应画布、实际尺寸、下载图片等
30	综合分析	支持综合统计、安全指数、TOP 统计、告警趋势、资产分布、协议分布、实时

		攻击等图表仪表
31		#支持以告警信息、攻击者、受害者、情报、资产等不同视角进行异常监测分析
32	基线自学习	支持通信白名单基线审计，支持自定义和自学习基线配置方式，支持手动启停基线策略，支持自定义时间段内基线自学习功能
33		支持自学习模型，可对内网资产进行学习识别，对非法地址的连接进行实时告警，快速发现违规连接
34	系统配置管理	支持入侵规则、工控规则、自定义规则管理，支持单条规则的启用停用，兼容 snort 规则
35		支持抓包工具，包括指定接口、指定五元组、指定抓包时间进行抓包
36		支持指定协议的启用停用，指定协议端口等
37		支持设备 CPU、内存、磁盘、运行时间展示，可以手动配置 CPU、内存和磁盘资源使用的预警范围，超过配置阈值，进行页面告警
38	接口外发	支持通过 syslog 方式将告警日志、违规连接日志、威胁情报日志、流数据日志、协议原始日志进行外发至第三方数据采集平台
39		#支持元数据外发，支持外发元数据协议不少于 30 种，解析深度要求解析到协议变量级别
40	报表功能	系统需具备数据报表统计能力，报表数据统计方式应从不同的维度进行分析，方便不同层次的技术人员进行数据汇总
41	用户管理	提供三权分立的用户管理能力：管理员、操作员、审计员相互独立
42	★服务	提供原厂三年维保服务，包括版本升级（包含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

七、工业主机安全卫士

序号	指标项	详细技术参数
1	★客户端授权要求	含三年期软件升级服务，包括版本升级及维护，远程支持，电话咨询等
2	客户端	★安装在 Windows PC 系统，包括 Windows PC: Windows 2000【SP4】、WinXP【SP3】32 位、Win7【各版本】32 位+64 位、Win8.1【各版本】32 位+64 位、Win10【各版本】32 位+64 位、Win11【各版本】32 位+64 位。
3		★安装在 Windows Server 系统，支持安装在 Server Win2003【SP1、SP2】32 位+64 位、Win2008【R2、企业版本】、Win2012【R2、企业版本】、Win2016【企业版本】、Win2019【企业版本】
4		★安装在 Linux 系统上，包括 Red Hat Linux 6.5/7.4、Ubuntu、OpenSUSE、Debian、CentOS、Fedora 等
5		支持客户端自我保护，提供卸载、停止客户端服务的密码保护，防止恶意停止和卸载客户端
6		支持客户端对违规安全基线自动修复或手动确认修复（包括防火墙、远程桌面、共享检查、屏保检查、进程黑名单、密码检查、服务检查、注册表检查）
7	控制中心	#支持自学习功能设置，可自定义自学习内容及自学习周期（提供界面截图）
8		#支持威胁情报功能设置，可针对文件、ip 分析功能自定义启用或禁用（提供界面截图）

9		采用 Web 方式进行管理。支持 Https 方式访问工业主机安全防护服务器。
10		工业主机安全防护客户端/服务器间通信需支持加密
11		支持账号“三权分立”，分别账号管理员管理系统管理员，系统管理员管理服务平台，审计管理员审计系统、账号管理员操作记录
12		支持自定义服务器访问端口
13		支持自动清除离线终端信息
14		支持对规则进行一键备份、一键恢复和日志定期清除
15		支持服务器安装目录磁盘空间不足告警提示功能，监控服务器端磁盘资源
16		支持 Syslog 方式发送报表到第三方平台
17	安全感知平台	支持查看事件类型 TOP5、威胁类型 TOP5
18		支持查看授权总数，授权数和未授权数，客户端总数包括在线数和离线数
19		支持查看威胁趋势，包括基础信息、攻击威胁、可疑行为、恶意站点、恶意软件、攻击组织和失陷主机
20		支持查看 7 天违规事件统计和趋势，包括非白名单、环境检查、软件安全和关键配置
21		支持查看今日非白名单、安全基线和威胁情报等事件高、中和低危风险等级的即时违规数据
22		支持根据不同风险等级查看安全基线评分概况
23	系统概览	服务端查看主机在线、离线、运行情况
24		支持查看今日事件数，事件总计，威胁事件总计，规则列表
25		#支持查看终端进程事件统计，进程运行事件统计，终端网络事件统计，网络访问事件，外设接入事件统计图形报表（提供界面截图）
26		支持查看进程运行趋势图形报表，通过对比当前周期与上一周期，更直观呈现进程运行趋势
27		#支持查看网络访问趋势图形报表，通过对比当前周期与上一周期，更直观呈现网络访问趋势（提供界面截图）
28		#支持查看外设接入事件趋势图形报表，通过对比当前周期与上一周期，更直观呈现外接设备事件趋势（提供界面截图）
29	事件概览	支持查看 TOP10 告警终端统计，TOP10 进程运行统计，TOP10 网络事件统计图形报表
30		支持快速选择时间段报表事件展示（今日、近一周、近一月、近三月、近六月，自定义）
31		支持查看基于进程、IP、端口的连入、连出的网络事件 TOP10 统计图形报表
32		支持查看条形图统计报表
33	分组管理	支持新建分组进行终端管理

34		支持分组删除、重命名等操作
35		支持查看终端信息（主机名、IP、系统版本等）
36		支持各分组终端数量显示
37		支持终端单独或批量分组转移
38	终端管理	#支持基于分组的终端概况展示（主机名，IP 地址，当前应用的白名单规则名，安全评分值、操作系统，客户端版本，所在分组等）（提供界面截图）
39		支持查看终端设备信息（硬件信息，软件信息，当前进程信息，当前网络连接信息，当前外设信息）
40		支持通过控制中心自助打包生成指向不同服务器的客户端，支持控制台下载客户端程序
41		支持在控制中心对终端进行单独或批量规则推送
42		支持单独或批量删除终端设备信息
43		支持在控制中心进行终端单独或批量升级
44		支持终端信息列表显示或平铺显示，方便查看
45		支持对终端进行备注，以便追踪溯源
46	白名单规则	支持进程白名单规则设置，通过对进程名、路径、MD5 的设置进行规则添加，白名单列表外的进程运行可设置记录或直接禁止
47		支持网络白名单规则设置，通过对进程、协议、方向(连入连出)、端口的设置进行规则添加，网络白名单外的网络访问可设置记录或禁止
48		#支持外设白名单规则设置，通过对设备类别、设备名称、设备标识的设置进行规则配置，外设白名单外的外设设备使用可设置为记录或禁止，支持添加所有鼠标和键盘到白名单功能（提供界面截图）
49		#支持帐户白名单规则设置，通过对白名单帐户的设置，禁止新增白名单外的帐户，防止白名单内的帐户被删除（提供界面截图）
50		#支持白名单取样功能，输入取样终端 IP，可对终端的（进程、网络访问、外设）进行采样操作，增加系统的便捷性（提供界面截图）
51		支持白名单规则按周期（每 1~24 个小时）自学习，能够自动采集周期内的系统相应运行情况并生成白名单规则
52		支持 AI 自学习方式一键自动生成按操作系统分类的白名单规则，并自动匹配威胁情报信息，自动过滤高危内容
53		支持 AI 自学习干涉，对机器学习进行人为介入，实现对自学习数据模型的调教优化
54		支持与 Venuseye 等权威威胁情报集成确保白名单规则内所有进程安全可信，支持对文件、进程（含进程加载的 dll/sys）、ip 等进行威胁分析及感知
55		不采用杀毒引擎技术实现对终端运行进程进行实时威胁分析
56	终端基线检测及加固功能	支持检查系统是否安装所需补丁
57		支持防火墙检测终端是否启用或关闭系统自带的专用和公用防火墙状态
58		支持远程桌面检测终端是否启用或禁用系统远程桌面功能状态
59		支持共享检测终端是否关闭或启用系统目录、打印机、IPC$共享功能状态
60		支持屏保检测终端是否关闭或启用系统屏幕保护程序及锁屏等待时间

61		支持密码检测终端密码组策略是否符合标准要求及是否存在弱口令账户
62		支持监控终端系统重要性能使用情况，如 CPU 使用率、内存使用率和系统盘剩余空间
63		支持进程红名单检测终端是否已运行了指定合规进程
64		支持进程黑名单检测终端是否非法运行了指定进程
65		支持软件红名单检测终端是否已安装了指定合规的应用软件
66		支持软件黑名单检测终端是否非法安装了未经许可的应用软件
67		支持服务检查检测终端的服务是否启用或禁用状态
68		支持防病毒软件检测终端是否已安装了指定的防病毒软件或已安装的防病毒软件病毒库版本号
69		支持文件目录检测终端的具体路径是否有指定文件存在
70		支持注册表检测终端指定注册表项、指定注册表值或指定的注册表项和值的匹配关系是否存在
71		支持网络黑名单检测指定端口与指定 IP 的指定端口连入或连出行为，以及访问的进程
72		支持外联检查通过 ping 或 telnet 探测方式检测终端是否可连通到指定的非法网络地址或域名。
73		支持对终端各安全检查项进行分数设定，支持各终端安全评分及健康状态展现
74	规则管理	支持规则导入、导出功能
75		支持同类规则全量合并
76		支持批量删除规则
77		支持规则立即执行、停用、复制、删除等操作
78		支持对终端规则执行率实时展示，可实时查看终端规则执行的情况（提供界面截图）
79	日志中心	支持事件日志查看及查询
80		支持日志详情展现（发生时间，上报时间，告警主机 IP 及 MAC，规则信息，执行结果等）
81		支持事件日志直接添加至白名单规则，方便管理员调整白名单规则
82		#支持记录事件类别、时间、设备信息、违反的白名单详情。可对违规事件进行深入详细分析，分析内容包括：进程的名称、路径、协议、端口、链接方向、目的地址、端口、进程 PID、PPID、父进程信息、文件大小、命令行信息、加载的模块、证书、md5、事件摘要、设备类别、设备名称、设备实例、服务名称、描述等等。同时威胁情报对进程、进程加载的文件（dll、sys）、进程连接的远端 ip 等进行安全威胁分析。（提供界面截图）
83		#进程白名单：支持事件类型，分组，主机名，上报 ip 地址，时间、动作类型、类别、进程名、父进程名、MD5 值等条件筛选（提供界面截图）
84		#网络白名单：支持事件类型，分组，主机名，上报 ip 地址，时间、动作类型、进程名、协议、方向、本地 ip、远端 ip、本地端口、远端端口等条件筛选（提供界面截图）
85		外设白名单：支持事件类型，分组，主机名，上报 ip 地址，时间、动作类型、类别、设备实例、设备名称、设备类别等条件筛选
86		帐户白名单：支持事件类型，分组，主机名，上报 ip 地址，时间等条件筛选
87		安全基线：支持事件类型，分组，主机名，上报 ip 地址，时间和基线各子模块等条件筛选

88		终端事件审计：支持事件类型，分组，主机名，上报 ip 地址，时间和日志类型（应用程序、安全、系统）等条件筛选
89		进程、网络和外设白名单记录事件，支持自定义加入白名单规则
90		支持威胁情报分析，包络：威胁事件分类统计、威胁情报趋势分析、威胁事件展示（含攻击与被攻击事件溯源分析），事件内容包括：事件类型、攻击源、被攻击者、危害等级、威胁类型、攻击组织、时间等（提供界面截图）
91	账号信息	支持账号个人信息查看
92		支持昵称设置及修改
93		支持密码修改
94		支持查看账号最近一次登录时间（提供界面截图）
95		支持展现最近登录记录（提供界面截图）
96	产品资质	计算机软件著作权登记证书
97		计算机信息系统安全专用产品销售许可证
98		产品具备公安部网络安全保卫局颁发的针对工业主机安全卫士的《计算机信息系统安全专用产品销售许可证》
99		产品具备中国网络安全审查技术与认证中心颁发的关于工业主机安全卫士的 IT 产品信息安全认证证书

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标。

八、数据中心防火墙（禅城总部）

序号	指标项	详细技术参数
1	★硬件规格	标准机架式；冗余电源，标准配置≥6 个 10/100/1000M 自适应千兆电接口，≥4 个千兆 SFP 接口，≥4 个 SPF+万兆接口，存储容量不少于 128G
2	★性能要求	整机最大吞吐量≥25G；标准配置下最大并发连接≥500 万；每秒 TCP 新建连接数≥24 万/秒；IPSec VPN 吞吐量 bps≥4G；IPSec VPN 默认隧道数≥9600；
3	★基础功能	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
4		开通 SSL VPN 功能、网络入侵防御功能、网络应用识别功能、网络防病毒功能；配置 SSL VPN 并发用户数不少于 200 个。
5		开通 WAF 功能
6	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
7		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
8		支持路由、透明及混合部署模式
9	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
10		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

11		具备协议自动识别功能；支持自定义事件功能
12	★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
13		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
14		内置多种沙箱环境与应用环境，使用反反沙箱、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
15	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
16	网络特性	支持静态路由、RIP v1/2、OSPF、BGP、策略路由等
17		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
18		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
19		#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
20		支持一对一、地址池等 NAT 方式，支持必须支持多种应用协议，支持策略 NAT 功能
21		支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL＊NET
22		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
23		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
24		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
25	★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
26		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
27		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
28	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
29		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
30		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
31		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
32	集中管理	#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

33	资质服务要求	销售许可证：产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，要求出具证书复印件。
34		产品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
35		产品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
36		产品具备国家计算机软件著作权登记证书，提供证明材料
37		产品具备 IPv6 Ready logo Phrase 2 认证；提供有效的资质证明复印件
38	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
39		#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
40	★服务	提供原厂三年维保服务，包括版本升级（包含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库等）及维护，7*24 小时远程支持，电话咨询，提供原厂售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标

九、统一安全运维平台

序号	技术指标	指标项
1	#等保运营管理	可实现全线上管理等保流程，包括：信息收集填报、定级、备案、在线快速自评和自动差距分析、整改管理、等保测评、持续监督等步骤管理。（提供功能截图）
2		根据上传的系统信息，可快速生成等保系统统计报表、系统差距分析报告，提出风险管理改进措施。（提供功能截图）
3		支持三级等保评分点≥1000 个。
4	#密评运营管理	可实现全线上管理密评流程，包括：系统调研、方案编制、建设测评、上线运营、持续监督等步骤管理。（提供功能截图）
5		根据国密建设情况进行实时打分，可提供差距分析和整改建议。（提供功能截图）
6	#安全产品纳管	可纳管安全产品的主流安全厂商≥25 家，提供统一的配置管理、策略分发和日志管理。（提供功能截图）
7		可纳管防火墙、Web 应用防火墙、漏洞扫描、VPN、堡垒机等安全产品。（提供功能截图）
8		可通过 API 接口纳管用户原有安全组件，并提供统一管理服务。（提供功能截图）
9	#安全服务	可提供覆盖应用、网络、数据、平台、主机、物理等层面的安全服务。
10		可提供用户现场、线上远程等服务模式，支持租户自己管理订购安全产品服务，实现自动化部署。
11	#安全态势感知	可对接国家计算机网络与信息安全管理中心，获取权威安全信息。
12		可实时对安全事件告警分析，掌握网络运行环境安全，动态监测、响应、处置、改善网络环境安全状态。
13		集中展示安全事件综合态势分析，实现及早预警、态势感知、攻击溯源和精确应对，减少安全运维的时间成本和技术成本。（提供功能截图）

14	#运营管理	支持标准化产品、服务的线上订购、线上交付、在线部署。
15		支持安全产品订单查询、智能出账等功能。（提供界面截图）
16		池化各类安全产品进行集中管理，支持自动进行安全业务智能编排设计。
17	#产品资质	具备计算机软件著作权登记证书，提供资质文件复印件。

十、汇聚交换机

序号	指标项	详细技术参数
1	★硬件规格	标准 1U 设备，冗余电源，≥1 个 RJ-45 Console 口，≥24 千兆 SFP 接口，≥24 万兆 SFP+接口,交换容量≥2.56Tbps/23.04Tbps,包转发率≥456Mpps。
2	MAC 地址表	支持静态、动态、黑洞 MAC 表项
		支持源 MAC 地址过滤
3	VLAN 特性	支持 4K 个 VLAN
		支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
4	IPv4 路由	静态路由、RIP V1/2、ECMP、支持 URPF
		OSPF、IS-IS、BGP
		支持 VRRP
		支持策略路由
		支持路由策略
5	QoS/ACL	支持对端口接收和发送报文的速率进行限制
		支持报文重定向
		支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP 地 址、目的 IP 地址、端口、协议、VLAN 的非法帧过滤功能
		支持基于队列限速和端口整形功能
6	可靠性	支持 STP（IEEE 802.1d），RSTP（IEEE 802.1w）和 MSTP（IEEE 802.1s）协议
		支持 BPDU 保护、根保护和环回保护
		支持 BFD for OSPF/ISIS/VRRP/PIM 协议
		支持增强 Trunk（E-trunk）
7	安全特性	支持防止 DOS、ARP 攻击功能、ICMP 防攻击
		支持 IP、MAC、端口、VLAN 的组合绑定
		支持端口隔离、端口安全、Sticky MAC
		支持 MAC 地址学习数目限制
		支持 IEEE 802.1X 认证，支持单端口最大用户数限制
		支持 AAA 认证，支持 Radius、HWTACACS、NAC 等多种方式
8	管理和维护	支持智能堆叠 iStack（业务口实现）
		支持 SNMPv1/v2c/v3
		支持网管系统、支持 WEB 网管特性
		支持系统日志、分级告警
9	★服务	提供三年维保服务，包括版本升级及维护，7*24 小时远程支持，电话咨询，提供售后服务承诺函。提供不低于原设备性能的备件支持。提供现场安装及简单操作培训。

备注：标“★”的指标项为关键指标；标“#”的指标项为重要指标

第四章 合同文本

佛山电器照明股份有限公司网络安全建设项目

采购合同

甲 方：_____

电 话：_____

地 址：_____

乙 方：_____

电 话：_____

地 址：_____

甲方（需方）：佛山电器照明股份有限公司

乙方（供方）：_____

经双方友好协商，本着平等互利和共同发展的原则，就乙方为甲方建设佛山电器照明股份有限公司网络安全建设项目，达成如下合作协议：

一 、采购内容

佛山电器照明股份有限公司建设网络安全加固及工控安全建设项目，包含南宁厂区互联网防火墙两台，出口流量管理（上网行为管理）设备两台，入侵防御系统设备一台；高明厂区数据中心防火墙两台（数据中心部署，一台原有设备利旧），工业防火墙两台（高明工业生产网出口部署，双机冗余），工控入侵检测系统一套（高明安全管理区部署），工业主机安全卫士（解决工控主机安全防护问题，400 个终端授权）；统一安全运维平台一套；高明厂区汇聚交换机两台；资产梳理服务，漏洞扫描服务，安全加固服务，应急响应服务，应急演练服务，渗透测试服务，安全培训服务及安装调试、上线服务。

二、合作期限与维保期

双方合作期限自合同签订并生效之日起，乙方应于合同生效之日起 120 日历天内完成建设，并达到佛山电器照明股份有限公司验收标准。维保期为自系统上线之日起**叁年内免费维保**。

三、合同价格、付款方式及条件

1．本合同总价为：￥_____元，人民币大写：_____，乙方开具增值税专用发票（设备硬件税率 13%，服务税率 6%），包括硬件设备、软件产品费、定制开发、实施、培训、维护服务、相关税费等费用。

各设备清单如下表（本表样式仅供参考，根据中标单位“分项报价表”进行完善）

序号	货物名称	规格型号	品牌	产地	制造商名称	**单价**	**数量**	**总价**

2.按照以下付款进度进行支付（**付款方式：5 万元以上，按付款条件付 6 个月银行承兑汇票，5 万元以下，3 个月支付现金。**）：

付款进度	付款比例	付款条件	备注
1	30%	合同生效后 15 个工作日内支付	
2	30%	硬件设备到货且提供对应设备原厂供货证明后 15 个工作日内支付	
3	35%	项目正式上线使用后 1 个月内支付	
4	5%	系统维保期满后 1 个月内支付。	

3.甲方开票资料及联系人信息：

公司名字：_____

地址、电话：_____

纳税人识别号：_____

开户行及账号：_____

4.乙方收款账号和开票账号

收款单位（乙方）：_____

开户行：_____

账号：_____

四、 双方的权利和义务

（一） 甲方的权利和义务

1．甲方须依合同规定向乙方按期支付全部款项。

2．甲方安排人员配合乙方的培训安排及安排人员参与系统的调试工作。

3．甲方应当保守在本合同履行中与履行完毕后获知的对方的商业秘密。

4．合同维保期期内，甲方有权要求乙方提供免费的售后服务。

5．甲方保证不扩散乙方的软件和资料，产品仅供甲方及其分（子）公司自行使用。

6．甲方应整理好数据初始化所需的基础数据。

（二） 乙方权利和义务

1．乙方负责整个项目的实施。应在合同规定的期限内按质按量完成合同所规定的所有建设内容，确保甲方正常运行。

2．乙方已有的框架类软件知识产权归乙方自己所有，但乙方必须保证其是拥有知识产权的产品，无产权纠纷，并且乙方提供终身的技术支持服务。

3．乙方应当保守在本合同履行中与履行完毕后获知的对方的商业秘密。

4.载体（光盘等）如非人为因素损坏，在免费服务期内，乙方应免费调换。

五、 验收标准和交付物

各阶段完成后，由项目组提交对应交付物，甲、乙方双方确认签字后视为验收完毕。

序号	阶段	交付件	开始时间	结束时间	乙方责任人	甲方责任人	备注
1	项目启动阶段	详细项目计划					
2		项目启动资料					
3	分析阶段	系统解决方案					
4	调试/割接阶段	现场设备及线缆调整					
5		新设备调试上线					
6		集成测试问题清单					
10	上线运行阶段	系统运行报告					输出实施部署报告
		培训情况报告					
11		系统验收报告					
12	上线后支持阶段	系统运维支持报告					

六、售后服务

1．在验收合格后，乙方对所提供的应用系统提供叁年免费的售后服务。

2．故障报修的响应时间：2 小时。若电话中无法解决，需在规定时间内到达现场进行维护；提供 7×24 小时的电话咨询服务，一旦出现故障，恢复时间原则上不能超过 24 小时。

3．售后服务内容包括软件缺陷、故障等，乙方应免费给予解决。

4．在售后服务期内，乙方保证在出现应用系统故障时应及时、积极响应，遇有特殊情况双方协商。

5. 每月超过故障报修的响应时间且经由甲方二次通知后，乙方仍未提供服务的，应按 1000 元/次向甲方支付违约金，且甲方有权委托第三方进行维修，费用由乙方承担。

七、违约责任

1．一般性违约

如任何一方违反本协议所规定的义务，违约方在收到守约方要求纠正其违约行为的书面

通知之日，应立即停止其违约行为，并在 10 日内赔偿守约方因此受到的所有损失。如违约方继续违约行为或不履行其义务，守约方除就其所有损失而获得违约方赔偿外，亦有权提前终止本合同。

2．具体违约

（1）乙方逾期完成项目建设的，每延迟一天按合同总金额的 5‰ 向甲方支付违约金，违约金累计计算至项目建设完成之日。如违约金的数额累计达到本合同总价款的 20% 时，甲方有权终止本合同，乙方应返回甲方已付款项，并向甲方支付合同金额 30%违约金。

（2）乙方应及时以书面形式将不能按时交付使用或延迟安装调试的理由、延误时间通知甲方。如本项目任一阶段建设逾期超过 10 个工作日的，甲方可要求乙方按每逾期一日向甲方支付本合同总金额 5‰ 的违约金并继续履行合同，或者终止本合同，乙方应返回甲方已付款项，并向甲方支付合同金额 30%违约金。

（3）乙方所交付的项目成果，不符合合同或甲方要求，或无法通过甲方验收，乙方应返回甲方已付款项，并向甲方支付合同金额 30%违约金。

（4）乙方保证所交付的项目成果不侵犯任意第三方的知识产权，若乙方交付的成果涉嫌或被认定为第三方侵权，由此造成的不良影响及经济损失及因涉嫌或被认定为侵权而承担的任何责任由乙方承担，乙方应负责处理或协助处理相关纠纷、争议并承担一切费用，包括但不限于赔偿、律师费、诉讼费及其他聘请第三方处理侵权事宜的费用等。

八、保密

1．本合同任何一方对在合作过程中所获知的对方未向社会公开的技术情报和商业秘密均负有保密义务，除法律规定外，未经对方书面许可，任何一方不得将其泄露给第三方，也不得用于在本合作项目之外的任何不当用途，否则应承担违约责任并赔偿损失。

2．在本合同中止之后，各方在本协议项下的保密责任并不随之中止，各方仍需遵守本合同的保密条款，履行其所承诺的保密义务，直到双方同意其解除此项义务。

九、廉政规定

双方力求建立健康的商业合作关系，杜绝商业贿赂行为，不得向对方业务人员提供任何形式的利益（包括但不限于现金、宴请、旅游、购物券、礼品等），对业务人员提出的类似要求有权拒绝，并有义务向其单位法定代表人举报。任何一方利用商业贿赂行为获取商业机会或利益的，不当方应按照合同金额的 30％承担违约责任。

十、附则

1．如果出现不可抗力，双方在本协议中的义务在不可抗力影响范围及其持续期间内将中止履行，合作期限可根据中止的期限而作相应延长，但须双方协商一致。任何一方均不

会因此而承担责任。

2．本合同未尽事宜由双方另行协商解决，并签订补充协议，经签字盖章后与本协议具有同等效力。

3．本合同自双方签字盖章之日起生效。

4．本合同**一式肆份**，其中甲方叁份，乙方壹份，具有同等法律效力。

十一、争议解决

1．凡与本合同有关的一切争议，甲、乙双方应通过友好协商，如经协商后仍不能达成一致，任何一方均可依据中华人民共和国法律法规的有关规定，向 佛山市禅城区人民法院提起诉讼。

2．诉讼结果对双方都有约束力，双方应遵照执行。

3．由上述过程发生的费用，除另有规定外，应由败诉方承担。

（本页无正文，为签章页）

甲方：（签章）	乙方：（签章）
甲方代表签字：	乙方代表签字：
甲方开户银行：	乙方开户银行：
银行账号：	银行账号：
年　月　日	年　月　日

第五章　响应文件格式及附件

一　响应文件格式

响应文件请按以下要求的顺序和格式编制，并编制页码。

目 录

（1）　投标意向书

（2）　投标人（供应商）基本情况表

（3）　报价一览表

（4）　采购需求（实质性条款）响应表

（5）　投标人（供应商）商务响应情况表

（6）　技术服务方案

（7）　法定代表人证明书

（8）　法定代表人授权委托书

（9）　投标人资格声明函

（10）　资格文件

一 、首次报价信封内容格式

首次报价信封必须单独密封（该信封不要放入其它信封内），封口加盖公章，与响应文件一同递交，其内装文件如下：

1.首次报价一览表；

2.首次投标报价清单明细（如有）；

3.法定代表人证明书；

4.授权委托证明书（如适用）。

二 、第一轮/第二轮报价信封内容格式

第一轮/第二轮报价信封无须与响应文件一同递交，第一轮/第二轮报价信封由供应商授权委托人自行保管。采购代理机构工作人员根据评审会议的进程通知供应商授权代表现场递交第一轮/第二轮报价信封。其内装文件如下：

1. 第一轮/第二轮报价一览表原件；

附件 1　投标意向书

致：佛山电器照明股份有限公司

根据贵单位　　（项目名称）（项目编号：TPA-2022-C3-115）　　的招标文件要求，（全名及职衔）经正式授权并以投标人（供应商）（投标人（供应商）名称）的名义投标。提交响应文件正本 1 份（内装响应文件纸质 1 份；响应文件电子版 1 份，WORD 或 EXCEL 格式， U 盘介质，不留密码，无病毒），副本 2 份（纸质）。

我司在此声明并同意：

1、我们愿意遵守采购代理机构招标文件中的各项规定，按招标文件的要求提供报价。以投标报价（首次报价）：_____元向贵单位提供技术服务和供货。

2、我们同意本投标自投标截止日起 90 天内有效。如果我们的投标被接受，则直至合同生效时止，本投标始终有效。

3、我们已经详细地阅读了全部招标文件及附件，包括澄清、补充及参考文件（如果有的话），我们完全理解并同意放弃对这方面有不明及误解的权利。

4、我们同意提供采购代理机构要求的有关投标的其他资料。

5、我们理解，本项目评标委员会及采购代理机构并无义务必须接受最低报价的投标或其他任何投标。

6、我方如果中标，保证履行响应文件中承诺的全部责任和义务，并按照招标文件的要求向本项目的采购代理机构足额交纳招标代理服务费。

7、所有有关本次投标的函电请寄：_____

法定代表人或投标授权代表（签字或签章）：_____

投 标 人 名 称：_____

投标人（供应商）（公章）：

电　话：　　传　真：

附件 2　投标人（供应商）基本情况表

1、公司名称：_____　　电话号码：_____

2、地　　址：_____　　传　　真：_____

3、法定代表人姓名：_____

4、注册资金：_____　　经济性质：_____

5、经营范围：_____

6、营业执照注册号：_____

7、公司开户银行名称及帐户：

开户名：_____

开户行：_____

账　号：_____

8、投标人（供应商）获得资质和代理权限资格证书复印件一览表（如有）

证书名称	发证单位	证书等级	证书有效期

我/我们声明以上所述准确无误，您有权进行您认为有必要的所有调查。

投标人（供应商）全称（盖公章）：

法定代表人或投标授权代表（签字或签章）：

日　　期：　　年　　月　　日

附件 3　投标报价一览表

项目名称：

项目编号：TPA-2022-C3-115

序 号	内 容	首次投标报价总价（元）
1	佛山电器照明股份有限公司网络安全建设项目	大写：
		小写：
2	合同履行期限（服务期限）	自签订合同之日起，四个月内完成系统建设。
3	项目负责人姓名	
4	投标有效期	自投标截止日起 90 天。
5	备　注	

投标人（供应商）全称（盖公章）：

法定代表人或投标授权代表（签字或签章）：

日　　期：

注：　1.此表的投标报价为综合报价，投标人（供应商）应综合考虑。

附件 3-1 分项报价表

项目名称：
项目编号：TPA-2022-C3-115

货币及单位：人民币/元

序号	货物名称	规格型号	品牌	产地	制造商名称	**单价**	**数量**	**总价**

投标人（供应商）全称（盖公章）：

法定代表人或投标授权代表（签字或签章）：

日　　期：

注：表样仅供参考，投标人根据“采购人需求书”中“项目功能清单”进行分项报价。

附件 3.1　第一轮报价一览表

项目名称：

项目编号：

序 号	内 容	第一轮投标报价总价（元）
1	佛山电器照明股份有限公司网络安全建设项目	大写：
		小写：

投标人（供应商）全称：

法定代表人或投标授权代表（签字或签章）：

日　　期：

注：　1.此表的投标报价为综合报价，投标人（供应商）应综合考虑。

2. 此表为投标人按评标进程现场填写或者供应商提前准备，放在第一轮报价信封内提交（响应文件不提供此表）。

3. 填写时保持字迹工整、填写完全、不要涂改！

附件 3.1　第二轮报价一览表

项目名称：

项目编号：

序　号	内　容	第二轮投标报价总价（元）
1	佛山电器照明股份有限公司网络安全建设项目	大写：
		小写：

投标人（供应商）全称：

法定代表人或投标授权代表（签字或签章）：

日　　期：

注：　1.此表的投标报价为综合报价，投标人（供应商）应综合考虑。

2. 此表为投标人按评标进程现场填写或者供应商提前准备，放在第二轮报价信封内提交（响应文件不提供此表）。

3. 填写时保持字迹工整、填写完全、不要涂改！

附件 4　采购需求（实质性条款）响应表

项目名称：

项目编号：

序号	实质性响应（★号）条款	是否响应	差异

投标人（供应商）全称（盖公章）：

法定代表人或投标授权代表（签字或签章）：

日　　期：　　年　　月　　日

注：1、投标人须按照第三章“采购人需求书”的★号条款进行逐条响应。

2、如果招标文件需求书中没有★号条款，则投标人不需要提供此表（或者表中填写“本项目需求书无★号条款”）。

附件 5　投标人（供应商）商务响应情况表

项目名称：

项目编号：

评审项目	内容或数据	查阅指引
		见第____至____页
		见第____至____页
		见第____至____页
		见第____至____页
		见第_____至____页
		见第_____至____页

注：按照招标文件第六章《评标细则》“附件 4 商务标评分标准”提供相应的证明材料。

投标人（供应商）全称（盖公章）：

法定代表人或投标授权代表（签字或签章）：

日　　期：　　年　　月　　日

附件 6　技术服务方案

“技术服务方案”是投标人（供应商）根据第三章采购人需求书及第六章《评标细则》的“附件 3 技术评分标准”，充分发挥报价人自身优势和对项目的理解，提出的完成本项目的“技术服务方案”。“技术服务方案”格式及内容自拟。

附件 7　法定代表人证明书

_____先生/女士，现任我公司_____职务，为法定代表人，特此证明。

单位（盖公章）：

附：

代表人性别：_____

年龄：_____

身份证号码：_____

营业执照（注册号）：_____

经济性质：_____

主营（产）：_____

加盖投标人（供应商）公章

（法人代表身份证复印件）

注：1、法定代表人的姓名必须与营业执照法定代表人姓名完全一致。

2、此证明书一式两份。一份装订在响应文件正本内；另一份放在首次报价信封内。

附件 8　法定代表人授权委托书（如有）

本授权书声明：注册于（国家或地区）的（投标人（供应商）名称）在下面签字的（法定代表人姓名、职务）代表本公司授权（单位名称）的在下面签字的（授权代表姓名、职务）为本公司的合法代理人，就项目编号为_____的（采购人名称）采购_____项目和服务的投标和合同执行，作为投标人（供应商）代表以本公司的名义处理一切与之有关的事宜。

代理人无转委托权。

本授权书于____年__月__日签字生效，有效日期至：____年__月__日，特此声明。

法定代表人签字或盖章：_____

职　　务：_____

投标人（供应商）代表（授权代表）签字或盖章：_____

加盖投标人（供应商）公章
（投标人（供应商）代表身份证复印件）

注：此委托书一式两份。一份装订在响应文件正本内；另一份放在首次报价信封内。

附件 9　投标人资格声明函

投标人资格声明函

致：佛山电器照明股份有限公司

关于贵单位_____年____月____日发布_____项目（项目编号：　）的采购公告，本公司（企业）愿意参加投标，并声明：

一、 本公司（企业）具备以下的条件：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件。

本公司（企业）的法定代表人或单位负责人与所参投的本采购项目的其他投标人的法定代表人或单位负责人不为同一人且与其他投标人之间不存在直接控股、管理关系。

本公司（企业）如为本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。否则，由此所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

本公司（企业）承诺在本次招标采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

特此声明！

备 注：

1） 本声明函必须提供且内容不得擅自删改，否则视为无效投标。

2） 本声明函如有虚假或与事实不符的，作无效投标处理。

投标人名称：_____

法定代表人或投标人授权代表（签署本人姓名或印盖本人姓名章）：_____

单位地址：_____

单位公章：_____

邮政编码：_____日期：_____

附件 10　资格文件

项目名称：

项目编号：

资格条件要求	内容或数据	查阅指引
具有独立承担民事责任的能力	提供有效的企业法人营业执照（或事业法人登记证等相关证明）副本复印件（分公司投标（响应）的，须取得具有法人资格的总公司出具给分公司的授权书，并提供总公司和分公司的营业执照复印件。	见第___页
有依法缴纳税收和社会保障资金的良好记录	提供资格声明函。	见第____页
具有良好的商业信誉和健全的财务会计制度	提供资格声明函。	见第____页
履行合同所必需的设备和专业技术能力	提供资格声明函。	见第____页
参加采购活动前 3 年内，在经营活动中没有重大违法记录	提供资格声明函。	见第____页
信用的查询情况证明	投标人提供信用中国网站（www.creditchina.gov.cn）“信用信息”、的查询情况证明（若暂未收录投标人信用信息记录，投标人应提供声明函原件，声明函格式及内容自拟），如有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，将不具备参与本次采购活动的资格。投标人若提供虚假声明函经查核后将被拒绝投标。	见第____页

资格条件要求	内容或数据	查阅指引
投标时验证身份的合法有效性	提供有效的法定代表人身份证明书、法定代表人授权委托书（如适用）、本人身份证，用以投标时验证身份的合法有效性。	见第____页
为本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	提供资格声明函。	见第____页
投标人的法定代表人或单位负责人与所参投的本采购项目的其他投标人的法定代表人或单位负责人不为同一人且与其他投标人之间不存在直接控股、管理关系	提供资格声明函。	见第____页
关于联合体	本项目不接受联合体投标	本小项不需要提供证明材料

投标人（供应商）全称（盖公章）：

法定代表人或投标授权代表（签字或签章）：

日　　期：　　年　　月　　日

附：1、本格式仅供参考，投标人（供应商）可根据实际情况自定。

2、投标人（供应商）应附上相应复印件。

第六章 评标细则

佛山电器照明股份有限公司

网络安全建设项目

评标细则

采 购 人：佛山电器照明股份有限公司

项目编号：

一.说 明

1、概述

根据国家及地方采购有关文件精神，在保证佛山电器照明股份有限公司网络安全建设项目项目（以下简称项目）在公开、公平、公正的基础上，结合项目的技术和商务需求，由广州宏达工程顾问集团有限公司编制本评标细则，经采购人确认。内容包括本次评标的评审过程和方法。

2、定义

采 购 人：系指佛山电器照明股份有限公司。

业主/用户：系指本项目的最终使用单位即佛山电器照明股份有限公司。

采购代理机构：系指广州宏达工程顾问集团有限公司。

3、评标委员会组成

评标委员会成员人数为 3 人，由采购人依法组建。

二.评标须知

1.关于评标方案

（1）评标委员会的每位成员（简称评委）应认真地阅读并确认已经正确理解了评标方案；

（2）评委如对评标方案有异议，应在评标开始前提出。

2.关于评标纪律

（1）评委不得与任何投标人（供应商）或者与招标结果有利害关系的人进行私下接触，不得收受投标人（供应商）、中介人、其他利害关系人的财物或者其他好处；

（2）评委应本着客观、公正的原则独立给出评价意见；

（3）评委之间不得相互串通进行评分；

（4）评委不得试图影响其他评委的评价意见。

3.关于评标责任

（1）评委应在其书面评审意见上签字确认；

（2）评委对其所提出的评审意见承担个人责任。

4.关于回避

有下列情形之一的，不得担任评委，如事先不知情的，应在采购代理机构宣读投标人（供应商）名单及评标纪律后主动提出回避：

（1）是投标人（供应商）或者投标人（供应商）主要负责人的近亲属；

（2）项目主管部门或行政监督部门的人员；

（3）与投标人（供应商）有经济利益关系，可能影响对投标公正评审的；

（4）曾因在招标、评标以及其他与招标投标有关活动中从事违法行为而受过行政处罚或刑事处罚的。

5.关于保密

评委和与评标活动有关的工作人员不得透露对响应文件的评审和比较、中标候选人的推荐情况以及评标有关的其他情况。

前款所称与评标活动有关的工作人员，是指评委以外的因参与评标监督工作或者事务性工作而知悉有关评标情况的所有人员。

6.罚则

（1）评委在评标过程中擅离职守，影响评标程序正常进行，或者在评标过程中不能客观公正地履行职责的，给予警告；情节严重的，取消担任评委的资格，不得再参加任何采购人开展的招标项目的评标；

（2）评委收受投标人（供应商）、其他利害关系人的财物或者其他好处的，评委或者与评标活动有关的工作人员向他人透露对响应文件的评审和比较、中标候选人的推荐以及与评标有关的其他情况的，给予警告，没收收受的财物；对有所列违法行为的评委取消担任评评委的资格，不得再参加任何采购人开展的招标项目的评标；构成犯罪的，依法追究刑事责任。

三.评标原则

评标工作应依据地方政府关于政府采购的有关规定，遵循“公平、公正、科学、择优”的原则进行。评标委员会将按照规定只对通过资格性检查及符合性检查的响应文件进行评价和比较。

四.评标方法及流程

本次招标（采购）的评标方法采用**综合评分方法**。

4.1 评标委员会对报价供应商的响应文件进行初步评审。无效报价的认定条件详见《资格性检查表》、《符合性评审表》所列各项内容。

4.2 按照评审程序的规定，评标委员会首先阅读报价供应商的响应文件，据此与报价供应商进行技术、商务、价格的澄清、修正和竞价。评标委员会在对响应文件的有效性、完整性和响应程度进行初步审查时，可以要求供应商对响应文件中含义不明确、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响应文件的范围或者改变响应文件的实质性内容。本项目如无特殊情况，评标委员会要求报价供应商进行二轮报价，**即第二轮报价为最终报价**。提交最终报价的供应商不得少于 3 家。

4.3 综合评分及其统计：按照评标程序、评分标准以及权重分配的规定，评标委员会分别就各个供应商的技术状况、商务状况及其对招标文件要求的响应情况进行评议和比较，评出其技术商务评分。各评委的评分的算术平均值即为该报价供应商的技术商务评分。然后，评出报价得分。将技术商务评分和价格评分分别乘以权重并相加得出综合得分，综合得分按由高到低顺序排列。综合得分相同的，优先排列顺序如下①最后报价低者②技术得分高者。按照最终得分由高到低的顺序推荐综合得分排名第一的投标人（供应商）为中标候选人。

（1）投标人（供应商）资格性检查和响应文件符合性检查

各评委先对投标人（供应商）进行资格性检查，对通过资格检查的各响应文件按照招标文件要求的响应情况进行符合性检查。符合性检查必须根据招标文件中对投标人（供应商）的要求和响应文件中的响应进行。

评标委员会可以书面方式要求投标人（供应商）对响应文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容作必要的澄清、说明或者补正。澄清、说明或者补正应以书面方式进行并不得超出响应文件的范围或者改变响应文件的实质性内容。

在评审中发现关键指标/服务要求等未能达到招标文件中的规定或有虚假情况时，评标委员会有权取消其评审资格。

投标人（供应商）只有完全通过符合性检查，才能进入下一阶段的详细评审，否则视为无效投标。（详见符合性检查表）

（2）响应文件详细评审

当通过资格性检查及符合性检查的合格投标人（供应商）多于或等于三家时，按照评标程序的规定和依据评分标准以及各项权重、资格性检查及符合性检查结果，各位评委单独就每个合格投标人（供应商）的技术状况、商务状况、价格进行评审和比较，评出其技术评分、商务评分和价格评分。将技术得分、商务得分和价格得分相加得出综合得分，并按综合得分由高至低排出名次（出现并列得分时，价格低者排名在前）。

当通过资格性检查及符合性检查的投标人（供应商）少于三家时，评标委员会否决所有响应文件，提请依法重新招标。

（3）投标竞价

本次报价根据投标参与单位的数量实行二轮淘汰制，每轮竞价结束后，评标委员会根据

投标单位最新一轮的报价重新计算其综合评分，按综合评分由高到低排名后进行淘汰（具体方法详见下表）。第二轮报价后综合评分最高的 1 家合格投标人确定为中标候选人。

评标委员会推荐第二轮报价后综合评分最高的分别作为中标候选人。

	第一轮竞价	第二轮竞价
二次报价参与单位	合格投标人单位≥4 家，淘汰至 3 家单位； 符合竞价参与单位＜4 家，不进行淘汰（不进行竞价，直接进入第二轮竞价）； 符合竞价参与单位＜3 家，本次竞价终止。	综合评分最高的 1 家确定为中标候选人。

投标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，评标委员会应当要求其在评标现场合理的时间内（1 小时内）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。

五.评分标准和权重

5.1.评分标准

5.1.1 评委根据通过资格性检查及符合性检查投标人（供应商）的响应文件，并逐项列出响应文件的全部投标偏差。

5.1.2 评分应考虑到响应文件与招标文件之间的细微偏差。细微偏差是指响应文件在实质上响应招标文件要求，但在个别地方存在漏项或者提供了不完整的技术信息和数据等情况，并且补正这些遗漏或者不完整不会对其他投标人（供应商）造成不公平的结果。细微偏差不影响响应文件的有效性。在详细评审时对细微偏差作不利于该投标人（供应商）的量化。

5.1.3 评委对响应文件的技术及商务响应情况进行评分。评分采用量化方法。技术、商务、价格评分应分别考虑下列因素：

（1）技术评审（见技术评分标准）

计算公式：技术得分 = 各评委评分总和 ÷ 评委人数

技术得分四舍五入精确到小数点后两位。

（2）商务评审（见商务评分标准）

计算公式：商务得分 = 各评委评分总和 ÷ 评委人数

商务得分四舍五入精确到小数点后两位。

（3）价格评审（见本章 5.1.4 款）

5.1.4 价格评分计算方法：评审基准价＝所有有效竞价参与单位的竞价平均价。

竞价参与单位的价格得分按以下公式计算：评审价低于或等于评审基准价的竞价参与单位，其价格得分为满分 60 分；评审价高于评审基准价的竞价参与单位，其报价得分＝（评审基准价/竞价总价）×60（结果出现小数，以四舍五入的方式保留 2 位小数）。

注：如竞价参与单位报价税率不相同时，按不含税价评分。

5.2.权重分配

评分项目	技术部分	商务部分	价格部分
权重	35%	5%	60%
满分	35 分	5 分	60 分

5.3.综合得分

综合得分 ＝ 技术得分 + 商务得分 + 价格得分

5.4.推荐中标候选人

评标委员会根据综合得分由高到低顺序排列。综合得分相同的，按投标报价由低到高排列。综合得分且投标报价相同的，按报价得分的高低顺序排列。评标委员会编写评标报告，并全体签字确认，推荐满足招标文件要求且综合得分排序的第一名为中标候选人。

六.定标和授标

采购代理机构应当自评审结束之日起 2 个工作日内将评审报告送交采购人。采购人应当自收到评审报告之日起 5 个工作日内在评审报告推荐的中标或者成交候选人中按顺序确定中标或者成交投标人（供应商）。

中标候选人未能通过资格后审或放弃中标、或因不可抗力提出不能履行合同的，采购人可以确定排名次高的投标人为中标人（中标供应商）。

七.附 件

本项目评标细则包括以下评标过程中所需文件附件：

附件 1　　资格性检查表

附件 2　　符合性检查表

附件 3　　技术评分标准

附件 4　　商务评分标准

附件 5　　价格评分标准

附件 1　资格性检查表

项目编号：

项目名称：

序号	投标人（供应商）名称 资格检查内容	……
1	具有独立承担民事责任的能力：提供有效的企业法人营业执照（或事业法人登记证等相关证明）副本复印件（分公司投标（响应）的，须取得具有法人资格的总公司出具给分公司的授权书，并提供总公司和分公司的营业执照复印件。	
2	有依法缴纳税收和社会保障资金的良好记录：提供资格声明函。	
3	具有良好的商业信誉和健全的财务会计制度：提供资格声明函。	
4	履行合同所必需的设备和专业技术能力：提供资格声明函。	
5	参加采购活动前 3 年内，在经营活动中没有重大违法记录：提供资格声明函。	
6	投标人提供信用中国网站（www.creditchina.gov.cn）“信用信息”的查询情况证明（若暂未收录投标人信用信息记录，投标人应提供声明函原件，声明函格式及内容自拟），如有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，将不具备参与本次采购活动的资格。投标人若提供虚假声明函经查核后将被拒绝投标。	
7	提供有效的法定代表人身份证明书、法定代表人授权委托书（如适用）、本人身份证，用以投标时验证身份的合法有效性。	
8	为本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：提供资格声明函。	
9	投标人的法定代表人或单位负责人与所参投的本采购项目的其他投标人的法定代表人或单位负责人不为同一人且与其他投标人之间不存在直接控股、管理关系：提供资格声明函。	
10	本项目不接受联合体投标。	
结论	是否通过资格检查，进入下一阶段	

备注：1、“是否通过并进入下一阶段评审”一栏应写“通过”或“不通过”。

2、合格的用“×”表示，不合格的用“〇”表示。出现一个“×”的结论为“不通过”。表中全部为“〇”，同意进入下一阶段评审。

评委签名：　　**日　　期：**　　年　月　日

附件 2

符合性检查表

项目编号：

项目名称：

序号	投标人（供应商）名称 符合性检查内容	……	……
1	投标有效期不符合要求（90 天）。		
2	没有法定代表人（负责人）证明书和法定授权代理人有效授权委托证明书（如适用）。		
3	响应文件没有投标人（供应商）盖章及其法定代表人（或法定代表人委托的投标授权代表）的签字或签章的。		
4	响应文件中只能有一个报价，有两个或多个报价的，没有声明哪个有效。		
5	响应文件未完全满足招标文件中带★条款，或不符合招标文件的其他要求，有重大偏离的。		
6	首次报价超过投标最高限价的。		
7	不符合法律、法规和招标文件中规定的其他实质性要求。		
结论	是否通过符合性检查，进入下一阶段		

备注：1、“是否通过并进入下一阶段评审”一栏应写“通过”或“不通过”。

2、凡出现以上任何一种情形用“×”表示，没有出现用“○”表示。出现一个“×”的结论为“不通过”。表中全部为“○”，同意进入下一阶段评审。

评委签名： **日　　期：** 年 月 日

附件 3

技术评分标准

序号	评审因素		评审细则	权重	分值
1	对项目需求的响应程度		该项满分 10 分，对于技术指标中重要响应栏带“★”的指标为关键指标，不满足该指标项将导致投标被拒绝；标记“#”的为重要参数指标，每不满足一项指标扣 1.0 分；无标记的一般指标项，每不满足一项指标扣 0.5 分；相关功能项如要求提供投标产品的功能截图或可证明的材料的需提供清晰证明材料，否则有权视该技术参数无效响应。	10%	10
2	整体方案	技术方案	根据项目需求提供技术方案： ①方案内容完整、详细、表述清晰、科学合理、切实可行，满足且优于采购需求，得 5 分； ②方案内容比较完整、详细、表述清晰、比较合理、可行，完全满足采购需求，得 3 分； ③方案内容基本完整、详细、表述基本清晰、合理、可行性稍差，不能完全满足采购需求，得 1 分； ④未提供，得 0 分。	5%	5
3		实施方案	根据需求提供售后实施服务方案： ①方案内容完整、详细、表述清晰、科学合理、切实可行，且具备 5 项以上相似项目案例（提供复印件），满足且优于采购需求，得 15 分； ②方案内容比较完整、详细、表述清晰、比较合理、可行，且具备 5 项以上相似项目案例（提供复印件），完全满足采购需求，得 10 分； ③方案内容基本完整、详细、表述基本清晰、合理、可行性稍差，且具备 3 项以上相似项目案例（提供复印件），不能完全满足采购需求，得 5 分； ④未提供，得 0 分。	15%	15
4		培训方案	根据需求提供培训方案： ①方案内容完整、详细、表述清晰、科学合理、切实可行，满足且优于采购需求，得 5 分； ②方案内容比较完整、详细、表述清晰、比较合理、可行，完全满足采购需求，得 3 分； ③方案内容基本完整、详细、表述基本清晰、合理、可行性稍差，不能完全满足采购需求，得 1 分； ④未提供，得 0 分。	5%	5
合 计				35%	35 分

附件 4

商务评分标准

项目名称：

项目编号：

序号	评审内容	评分标准	权重	分值
1	项目整体质保期为三年，是否提供更长的整体质保期	提供优于本项目要求的质保期：整体保修期在三年的基础上增加 1 年，得 0.5 分，合计最高得 1 分，只提供项目三年整体质保期，得 0 分。增加部分按年计算，不够一年不得分。	1%	1 分
2	综合能力	1、提供近三年（2019 年 1 月 1 日至今）网络安全建设项目相关合同，按单个合同总额高于 100 万元计，每有一个合同得 1 分，合计最高得 2 分。以上需提供合同关键页扫描件，以合同签订时间为准，否则不予计算。	2%	2 分
		2、提供本项目负责人或实施团队人员资质证明：系统集成、软件开发方面高级证书者，每有一个证书得 0.5 分，最高得 2.0 分。（需附相关人员在投标截止时间前 4 个月内任意一个月（含投标截止时间当月）在投标人单位参加社保资料证明材料，否则不予认定）。	2%	2 分
合　计			5%	5 分

附件 5

价格评审表

项目名称：

项目编号：

有效投标人（供应商）序号	有效投标人（供应商）名称	评审分项		价格得分
		经评审的投标报价	评标基准价	