单一来源采购文件

**项目名称：南宁金融集团综合管理平台公有云服务**

**项目编号：GXGJ2024-D0003-S**

**采购单位：南宁金融投资集团有限责任公司**

**采购代理机构：广西国建项目管理有限公司**

**2024年2月**

目 录

[第一章 单一来源采购邀请函 3](#_Toc92385216)

[第二章 报价人须知 6](#_Toc92385217)

[第三章 采购项目需求 13](#_Toc92385218)

[第四章 响应文件格式](#_Toc92385219) [48](#_Toc92385219)

[第五章 合同主要条款 56](#_Toc92385234)

# 第一章 单一来源采购邀请函

**广西国建项目管理有限公司关于南宁金融集团综合管理平台公有云服务项目（GXGJ2024-D0003-S）单一来源采购邀请函**

**中国电信股份有限公司南宁分公司：**

广西国建项目管理有限公司受南宁金融投资集团有限责任公司委托，拟就南宁金融集团综合管理平台公有云服务进行单一来源采购，特邀请贵单位参加协商，现将有关事项通知如下：

**一、项目基本情况**

项目编号：GXGJ2024-D0003-S

项目名称：南宁金融集团综合管理平台公有云服务

预算金额：850000.00元/年。（三年总预算2550000.00元）

采购需求：南宁金融集团综合管理平台公有云服务1项；详见采购文件。

合同履行期限：详见采购需求。

 **二、报价人资格要求：**

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.特定资格要求：无。

3.本项目不接受未购买本采购文件的供应商参加协商；

4.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的采购活动。除单一来源采购项目外，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；

5.参加采购活动前三年内，在经营活动中没有重大违法记录和不良信用记录；对在“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)等渠道列入失信被执行人、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，不得参与采购活动。

 **三、获取采购文件：**

1.时间：2024年2月5日至2024年2月5日，每天上午8：30至12：00，下午3：00至6：00（北京时间，法定节假日除外）

2.地点：广西南宁市白沙大道53号松宇时代17楼财务室（电话：0771-4915599）

3.方式：获取时间内，供应商代表携带授权委托书原件或复印件到获取地点购买。【邮购文件的，需于获取截止时间前，将以上材料邮寄或传真到采购代理机构，或发送到采购代理机构电子邮箱（gxguojian@126.com）进行报名，同时请注明采购项目名称、采购项目编号、供应商收件人、邮寄地址、邮编、电子邮箱、联系电话、传真号码等信息。】

4.售价：采购文件工本费每本 300 元，售后不退。如需邮购，每本另加邮费 50 元【需于获取截止时间前将工本费（邮购的另加邮费）汇到采购代理机构下述指定账号】；**依据《国家税务总局关于增值税发票开具有关问题的公告》国家税务总局公告2017年第16号的规定，报价人在索取发票时，请提供纳税人识别号或统一社会信用代码。**

开户名称：广西国建项目管理有限公司

开户银行：广西北部湾银行股份有限公司南宁市江南支行

银行账号：8001 1543 5100 037

 **四、响应文件提交**

时间：2024年2月6日15点30分（北京时间），供应商请于响应文件提交截止时间前将响应文件密封递交，逾期送达或未密封的将予以拒收，供应商可以由法定代表人（负责人）或委托代理人出席截标会。

地点：广西国建项目管理有限公司开标厅（广西南宁市白沙大道53号松宇时代17楼）。

**五、协商时间及地点**

1.时间：2024年2月6日15点30分（北京时间）后。

2.地点：广西国建项目管理有限公司评标室（广西南宁市白沙大道53号松宇时代17楼）。

**六、公告期限**

自本公告发布之日起3个工作日。

**七、其他补充事宜**

1.公告媒体：采购与招标网、广西国建项目管理有限公司网

**八、对本次招标提出询问，请按以下方式联系。**

1.采购人信息

名 称：南宁金融投资集团有限责任公司

地 址：广西南宁市青秀区朱槿路16号金菲豪园2号楼南宁金融集团

2.采购代理机构信息

名 称：广西国建项目管理有限公司

地 址：广西南宁市白沙大道53号松宇时代17楼

联系方式：0771-4915533

3.项目联系方式

项目联系人：方梦

电 话：0771-4915533

购买采购文件联系人：张艳芬 联系电话：0771-4915599

邮编：530000

广西国建项目管理有限公司

2024年2月5日

# 第二章 报价人须知

报价人须知前附表

|  |  |  |
| --- | --- | --- |
| 序号 | 条款号 | 内 容 |
| 1 | 1.1 | 项目名称：南宁金融集团综合管理平台公有云服务项目编号：GXGJ2024-D0003-S |
| 2 | 3.1 | 报价人资格：详见采购公告。 |
| 3 | 7.4 | 报价：报价人可就各分标的采购内容作完整唯一报价，漏项报价的或有选择的或有条件的报价，其报价将视为无效。 |
| 4 | 8.1 | 响应文件：正本一份 副本四份。报价在递交响应文件时，同时递交响应文件电子版。1.响应文件电子版份数：1份。2.响应文件电子版形式：可编辑的word文档格式。3.响应文件电子版密封方式：将响应文件电子版光盘或U盘与纸质版响应文件一并装入响应文件袋中。 |
| 5 | 9.1 | 响应文件递交截止时间：详见采购公告响应文件递交地址：详见采购公告 |
| 6 | 9.2 | 报价有效期：报价截止日期后60天。 |
| 7 | 10.2 | 报价保证金：详见采购公告 |
| 8 | 11.1 | 协商时间：详见采购公告协商地点：详见采购公告 |
| 9 |  | 履约保证金：本项目不收取履约保证金。 |

报价人须知

一、总　则

1. 适用范围

1.1项目名称：南宁金融集团综合管理平台公有云服务

 项目编号：GXGJ2024-D0003-S

本文件仅适用于本文件中所叙述的货物、服务类采购项目。

2. 定义

2.1“采购人”是指：南宁金融投资集团有限责任公司。

2.2“采购代理机构”是指：广西国建项目管理有限公司(以下简称“本公司”)。

2.3“报价人”是指响应本文件要求，参加协商的法人或者其他组织。如果该供应商在本次协商中成交,即成为“成交供应商”。

2.4“货物”是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。

2.5“服务”是指除货物和工程以外的其他采购对象。

2.6“单一来源采购响应文件”是指：供应商根据本文件要求，编制包含报价、技术和服务等所有内容的文件。

3. 报价人的基本条件

3.1报价人资格：详见须知前附表。

4. 协商费用、单一来源采购征求意见公示、采购文件的修改

4.1协商费用：报价人应自行承担所有与编写和提交单一来源采购响应文件有关的费用，不论协商结果如何，采购人和本公司在任何情况下无义务和责任承担此类费用。

4.2本公司可视具体情况，延长报价截止时间和开标时间。本公司至少在采购文件要求提交响应文件的截止时间一日前，将变更时间书面通知采购文件收受人。

二、单一来源采购响应文件的编制

5. 单一来源采购响应文件编制基本要求

5.1报价人对单一来源采购响应文件的编制应按要求装订和封装。

5.2报价人提交的单一来源采购响应文件以及报价人与本公司和采购人就有关协商的所有来往函电均应使用中文。报价人提交的支持文件和印刷的文献可以使用别的语言，但其相应内容必须附有中文翻译文本，在解释单一来源采购响应文件时以翻译文本为主。

5.3报价人应认真阅读、并充分理解本文件的全部内容（包括所有的补充、修改内容），承诺并履行本文件中各项条款规定及要求。对单一来源采购文件的实质性要求和条件作出响应是指报价人必须对单一来源采购文件标注▲号或必须满足的技术参数要求、商务条款及其他内容等实质性要求和条件**作出满足或者优于原要求和条件的承诺**。

5.4单一来源采购响应文件必须按本文件的全部内容，包括所有的补充通知及附件进行编制。

5.5如因报价人只填写和提供了本文件要求的部分内容和附件，而给评审造成困难，其可能导致的结果和责任由报价人自行承担。

5.6单一来源采购响应文件由价格文件和商务技术文件两个部分组成。

5.6.1价格文件

1）**报价表**；（附件一）**（必须提供）**

5.6.2 商务技术文件（应该有的必须提供,如未提供,协商小组有权拒绝其单一来源采购响应文件）

1）**报价函**；（附件二）**（必须提供）**

2）**商务、技术响应、偏离情况说明表**（附件三）；**（必须提供）**

3）**法定代表人（负责人）身份证正、反面复印件**；**[必须提供]**

4）**法定代表人（负责人）授权委托书原件和委托代理人身份证正、反面复印件**（附件四）**[委托代理时必须提供**]；

5）有效的营业执照等证明文件复印件；

①报价人有效的“营业执照”（报价人为事业单位的不需要提供“营业执照”，但需提供“事业单位法人证书”）等证明文件复印件；**[必须提供，原件备查]**

6）财务状况报告；**[格式自拟，必须提供]**

7）报价文件递交截止之日前半年内报价人连续三个月的依法缴纳税费或依法免缴税费的证明复印件；无纳税记录的，应提供由报价人所在地主管国税、地税部门出具的《依法纳税或依法免税证明》复印件**[格式自拟，必须提供]**。（新成立单位按实际提供）

8）报价文件递交截止之日前半年内报价人连续三个月的依法缴纳社保费的缴费凭证复印件**；**无缴费记录的，应提供由报价人所在地社保部门出具的《依法缴纳或依法免缴社保费证明》复印件**[格式自拟，必须提供]**。（新成立单位按实际提供）

9）参加采购活动前三年内在经营活动中没有重大违法记录和不良信用记录的书面声明；**[格式自拟，必须提供]**

10）具备履行合同所必需的设备和专业技术能力的证明材料；**[格式自拟，必须提供]**

11）售后服务承诺书（内容可以是提供的切实可行的售后服务和优惠承诺）；**[格式自拟，必须提供]**

12）本采购项目《采购需求》中要求必须提交的材料；**[如有要求，则必须提供]**

13）具备法律、行政法规规定的其他条件的证明材料[如有规定,则必须提供]；

14）本单一来源采购文件要求提供的其他资料和需要说明的问题。

6. 计量单位

6.1除技术要求中另有规定外，本文件所要求使用的计量单位均应采用国家法定计量单位。

三、协商报价要求

7.1对于本文件中未列明，而报价人认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付成交供应商没有列入的项目费用，并认为此项目的费用已包括在总报价中。

7.2成交供应商负责本项目所需货物的制造、运输、售后服务等全部工作。

7.3报价人应在报价表上标明单价和总价。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。除上述原因以外，如果因报价人原因引起的报价失误，并在协商时被接受，其后果由报价人自负。

7.4报价人可就所有采购内容作完整唯一报价，漏项报价的或有选择的或有条件的报价，其报价将视为无效。

四、单一来源采购响应文件的份数、封装和递交

8. 响应文件的份数和封装

8.1响应文件：正本一份 副本四份。报价人应将响应文件正、副本分别装订成册，在每个文本封面上标明项目名称、项目编号、报价人名称等内容，并在每个文本封面上标明“正本”或“副本”字样。报价人应将正、副本响应文件（正本一份、副本四份）装入响应文件袋中加以密封，并在每一封贴处密封签章（公章、密封章、法定代表人（负责人）或其委托代理人签字四种方式之一均可）。报价在递交响应文件时，同时递交响应文件电子版。

1）响应文件电子版份数：1份。

2）响应文件电子版形式：可编辑的word文档格式。

3）响应文件电子版密封方式：将响应文件电子版光盘或U盘与纸质版响应文件一并装入响应文件袋中。

8.2单一来源采购响应文件的信封上应写明：

1）单一来源采购项目编号；

2）单一来源采购项目名称；

3）协商货物、服务名称；

4）报价人名称。

9. 单一来源采购响应文件的递交

9.1所有单一来源采购的响应文件应于单一来源采购文件中规定的时间前递交到本公司指定地点。

9.2响应文件从报价截止日期后60天内有效。

10.履约保证金

本项目不收取履约保证金

五、协商的步骤

11.1资格审查

（1）协商小组审查单一来源采购响应文件的实质性内容是否符合单一来源采购文件的实质性要求。

（2）协商小组在对响应文件的有效性、完整性和响应程度进行审查时，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。

协商小组要求供应商澄清、说明或者更正响应文件以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人（负责人）或其授权代表签字或者加盖公章。

11.2协商

（1）协商时间及地点：详见本须知前附表第8项规定。

（2）协商小组所有成员应当集中与报价人进行协商。

（3）协商小组根据与供应商协商情况可能实质性变动的内容包括采购需求中的技术、服务要求。实质性变动的内容，须经采购人代表确认。

（4）对采购文件作出的实质性变动是采购文件的有效组成部分，协商小组应当及时以书面形式通知供应商。供应商应当按照采购文件的变动情况和协商小组的要求重新提交响应文件，并由其法定代表人（负责人）或授权代表签字或者加盖公章。逾时不交的，视同放弃协商。修正文件与响应文件同具法律效力。

（5）协商小组将通过资格审查的响应文件中的服务、合同条款及价格进行审查，如需与报价人进行协商的，代理公司将对协商过程和协商内容进行书面记录，直至协商达成一致，协商双方在记录上签字确认。

（6）协商评审在严格保密的情况下进行，协商的任何一方不得透露与协商有关的技术资料、价格和其他信息。

11.3响应供应商的最后报价超过了采购预算，采购人不能支付的，协商活动终止。

六、确定成交供应商办法

12.质量和服务均能满足单一来源采购文件实质性响应要求的供应商为成交供应商。

七、成交结果公告

13.1本公司在协商工作完成后2个工作日内将评审报告送采购人，采购人确认后，成交结果将在采购与招标网、广西国建项目管理有限公司网上公告。

1. 签订合同

14.1成交供应商在收到成交通知书后，应按成交通知书中规定的时间、地点与采购人签订合同。

14.2成交供应商不按成交通知书规定签订合同，则按成交供应商违约处理。

九、适用法律

15. 本次采购项目均参照有关法律法规和采购管理的有关规定及参照国际惯例编制。

十、其他事项

16.1签订合同前，成交供应商须向本公司一次付清成交服务费。

（1）采购代理机构按（桂价费 〔2011〕55号）的收费标准，以成交金额\*3年为基数按差额定率累进法计取成交服务费。签订合同前，成交人须向广西国建项目管理有限公司一次付清成交服务费。

（2）代理服务收费标准：

|  |  |  |  |
| --- | --- | --- | --- |
|  费率中标金额 | 货物招标 | 服务招标 | 工程招标 |
| 100万元以下 |  1.5%  | 1.5% | 1.0%  |
| 100～500万元 | 1.1%  | 0.8% | 0.7%  |
| 500～1000万元 |  0.8%  | 0.45% | 0.55% |
| 1000～5000万元 | 0.5%  | 0.25% | 0.35%  |
| 5000万元～1亿元 | 0.25%  | 0.1% | 0.2% |
| 1～5亿元 | 0.05% |  0.05% |  0.05% |
| 5～10亿元 | 0.035% |  0.035% | 0.035% |
| 10～50亿元 | 0.008% | 0.008% | 0.008% |
| 50～100亿元 |  0.006% | 0.006% | 0.006% |
| 100亿以上 |  0.004% | 0.004% | 0.004% |

注:招标代理服务收费按差额定率累进法计算。

（3）服务费指定银行账户：

开户名称：广西国建项目管理有限公司

开户银行：广西北部湾银行股份有限公司南宁市江南支行

银行账号：8001 1543 5100 037

16.2.解释权

本采购文件解释权属本公司。

16.3.有关事宜

所有与本单一来源采购文件有关的函电请按下列通讯地址联系：

广西国建项目管理有限公司

邮政编码：530000

通讯地址：广西南宁市白沙大道53号松宇时代17楼

电 话：0771—4915533

# 第三章 采购项目需求

**采购项目技术规格、参数及要求**

一、采购项目编号：GXGJ2024-D0003-S

二、采购项目类别：服务类

三、采购需求一览表

**说明：**

1、本项目需求表中带有“▲”的技术参数或要求为实质性要求，必须满足，竞标响应不得低于该技术指标或要求。

2、供应商商务响应与售后服务同一内容不相符的以低计算，不能满足基本要求的竞标无效。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项号** | **服务名称** | **数量** | **单位** | **内容和要求** |
|  | 专属云资源 | 1 | 项 | ▲1.租赁云资源需求及配置参数：（1）专属云计算单元：超分比1：1，总共提供vCPU：370核；内存：740G； （2）GPU加速型 p2s.2xlarge.8vCPU：8核；内存：64G；系统盘类型：超高IO；系统统盘大小40G；数据盘类型：超高IO；数据盘大小100G；云共享带宽20M；（3）超高I/O SSD云硬盘：①容量：9T超高I/O SSD云硬盘；②最高IOPS/磁盘：20000；③最大吞吐量/磁盘：350MBps；④时延：0.5～2ms；（4）SAS云硬盘：①SAS存储容量16T；②最高IOPS/磁盘：3000；③最大吞吐量/磁盘：180MBps；④时延：1～3ms。（5）SATA云硬盘①SATA存储容量0G；②最高IOPS/磁盘：1000；③最大吞吐量/磁盘：90MBps；④时延：5～10ms。（6）对象存储资源：①提供兼容Amazon S3接口的访问方式。②可通过SDK来调用OOS服务，提供开发支持文档。③服务设计可用性不低于99.9%，持久性可高达99.99999999999%。④存储规模可大规模在线扩展，不影响对外服务。⑤对象存储资源容量10T。（7）云主机备份服务：①备份对在线业务运行无影响，无需停机。②可定制任务实现一次性备份和周期性备份。③云主机内的多个云硬盘的备份为同一时间点创建。④备份的副本自动被加密，保障用户的备份数据安全。⑤云主机备份容量25T。（8）独享出口公网带宽：200M。（9）提供10个公网IP地址。2.专属云空间技术要求：▲（1）物理隔离：用户独享专属云内计算资源，弹性云服务器资源确保创建在物理隔离的专属云，用可自行在专属云资源内创建云服务器；▲（2）网络隔离：用户独占VPC，用户之间网络二、三层隔离；提供自定义网段，方便用户自配置网络；提供南北向和东西向的安全策略，方便用户构建立体防护网络；（3）分布式存储：专属云中的云服务器可挂载分布式存储的云硬盘，提供数据多副本，不会造成数据丢失；（4）资源管控：用户可以查看专属云下设备节点的计算资源总量及消耗情况，根据需要申请扩容资源； （5）专属云独立界面呈现专属计算资源消耗情况，包括专属云内存和CPU的使用容量；（6）用户在专属云中可任意创建和删除资源；（7）提供自定义网络；▲（8）支持虚拟化和物理资源混合组网，实现互联互通，灵活整合资源； 3.弹性云主机技术要求：（1）云主机可用性不低于99.95%，数据持久性不低于99.99995%；（2）支持控制台或者通过API调用方式对云主机进行包括创建、查询、销毁云主机实例等相关管理和操作；（3）支持云主机实例分钟级快速发放；（4）支持批量并发创建云主机；（5）提供多种类型的弹性云主机，可满足不同的使用场景；（6）云主机类型：至少支持通用型；（7）每种类型的弹性云主机包含多种规格；（8）通用型提供vCPU和内存比为1：1、1：2、1：4的规格；（9）支持通过公共镜像或者私有镜像创建弹性云主机，同时支持从其他租户上共享镜像创建云主机；（10）支持弹性云主机规格的变更，包括升级和降级；云主机规格（变更CPU和内存）变更需要先关闭云主机；（11）支持多网卡，可为云主机配置1张主网卡以及最多11张从网卡；可以设置不同的IP地址；（12）支持云主机添加和删除网卡，其中云主机主网卡不可删除；（13）支持修改配置云主机网卡的安全组规则；（14）支持绑定浮动私有 IP 地址，为网卡提供第二个IP地址，实现更灵活的网络功能，比如 HA双机热备时的浮动IP；（15）支持虚拟私有云（VPC）；（16）支持云主机安全组的设置；（17）支持自定义私网IP地址；（18）支持为云主机配置弹性IP，包括新分配弹性IP和使用已有弹性IP；支持云主机弹性IP解绑定；（19）支持云主机弹性IP带宽调整；（20）支持多种性能的云硬盘；提供普通IO（SATA）、高IO（SAS）、超高IO（SSD）三种类型的块存储；（21）Windows云主机的系统盘默认为40G；Linux 云主机的系统盘默认为40G；（22）云主机的数据盘大小可根据用户的需求进行设定，最小容量为10G，可以以10G步长增加，最大可指定32T；（23）云主机的数据盘可添加多块，单台云主机最多挂载23块数据盘；（24）支持云硬盘的扩容；对单块系统盘或数据盘进行扩容（磁盘卸载后），数据盘容量最大可扩展到32T；（25）支持云主机备份；（26）支持密码和证书两种登录方式，其中Windows云主机仅支持密码登录方式；（27）支持多种登录云主机方式，包括VNC登录，SSH方式登录（Linux云主机），MSTSC方式登录（Windows云主机）；（28）支持云主机创建时文件注入；（29）支持重装云主机操作系统；（30）支持重置云主机密码；（31）支持云主机多维度状态监控和告警；（32）支持弹性伸缩；（33）支持云主机的反亲和性部署。（34）支持弹性负载均衡。（35）提供云主机操作系统Windows Server授权。4.云硬盘技术要求：（1）支持云硬盘的创建/删除、批量创建/批量删除、查看、挂载、卸载；（2）支持对可用状态数据盘以及系统盘进行扩容；（3）支持云硬盘备份，可以手动执行备份，也可以通过设置备份策略进行自动备份；（4）支持共享云硬盘，可以创建共享云硬盘，最多同时挂载到16台云主机上；（5）支持从备份创建云硬盘，即根据现有的备份云硬盘来创建一块新的云硬盘；（6）支持创建SCSI模式磁盘，支持SCSI指令透传；（7）支持对云硬盘读速率、读操作速率、写速率、写操作速率的监控；（8）支持普通IO、高IO、超高IO三种类型的云硬盘，单盘最大支持32T容量，超高IO单盘最大吞吐量达到350MB，最大IOPS达到20000；（9）三副本冗余，数据持久性达99.99999%。5.云监控技术要求：（1）提供监控统一平台；提供基于Web的用户自助服务门户；（2）云监控服务支持对弹性云主机、云硬盘、弹性负载均衡、弹性伸缩和RDS等产品的监控，系统会自动识别用户正在使用的实例，并将其作为监控对象为用户提供实例性能监控数据；（3）控制台支持用户查看30天内的监控数据，用户查看历史数据时，可自定义数据查看时段、原始数据聚合时段以及原始数据聚合方式；支持用户导出2天内的原始监控数据；（4）支持虚拟资源的自动伸缩。包括但不限于：自动增加/减少虚拟负载均衡器后端数量，调整外部IP的带宽限制等；（5）支持对虚拟资源指定监控告警策略，告警策略中可以指定联系人，支持邮件&短信告知。6.开放性要求：（1）基于OpenStack基础架构；（2）支持Xen或KVM虚拟化引擎；（3）业务可移植性；（4）基于原OpenStack开发的管理平台。7.合规性：提供不低于符合国家三级等级保护要求的云安全服务能力，提供云平台整体的安全三级等保及网络资源。8.成熟度：（1）能够基于现有云资源完成两地三中心部署而无需通过其它数据中心；（2）云分布在多个城市，有同城多个可用区域，每个可用区有足量的资源并具有足够的冗余；（3）云平台本身的运营维护、安全升级和系统升级（如：当硬件或基础操作系统需要进行硬件维护、安全补丁的过程中）对云服务器和云数据库的可用性无影响；（4）可提供高可用和灾备的解决方案，并帮助进行这些解决方案在流程、应用架构和基础架构的落地咨询；（5）提供安全防护解决方案咨询服务，规划安全架构设计，产品选型。9.其它要求：投标时在投标文件中提供信息保护承诺书，即承诺保护客户的数据隐私，对于因服务提供方过失或故意导致的客户数据泄漏，以及由此引发的后续问题，承担刑事、民事等相关法律责任。▲10.服务要求：（1）7×24小时技术支持、故障申告电话；（2）7×24小时即时通讯工具技术服务支持；（3）提供对于发生的变更、故障、安全事件的完整文档材料，并在故障明确后12小时内提供；（4）提供审计便利；（5）承诺数据不出机房，不将客户数据作为商业变现手段；（6）专业的业务迁移服务，帮助客户完成传统业务、其他云上业务迁移到专属云平台。11.技术支持要求：（1）本地化服务、7×24小时到场服务；12.报价人所投云平台厂商或运营商要求：使用Openstack的开放标准，要求技术厂商品牌为国产品牌，并且不存在私有标准。13.安全方面要求：（1）告警服务方面，使用SOC系统实现安全告警，实时收集服务器和网络信息，通过机器学习，大数据安全分析，可对过去，现在以及未来的安全威胁有所察觉；（2）安全监控和调查的入口以及监控台的使用方面，支持客户监控台，使用DDOS防护和网站安全监测服务可以提供报告。▲14.信息安全防泄密承诺要求：不允许云服务商在ECS、裸机等云资源池内部植入信息采集客户端（Agent），包括使用该Agent进行内部应用状态监控，数据收集等侵犯租户私有信息，用于商业变现。 |
|  | 云下一代防火墙 | 2 | 套 | 1、第三方兼容性测试: 可提供第三方云平台兼容性测试证书/测试报告，并可在第三方云平台官网可查询2、Hypervisor：（1）支持vmware平台 （2）支持KVM平台 （3）支持Xen平台 （4）支持hyper-V平台3、自动化部署 ▲（1）支持使用VMware Tools完成初始化配置的注入 （2）支持使用Qemu Guset Agent完成初始化配置的注入 ▲（3）支持授权的自动化下发 ▲（4）支持使用cloud-init完成初始化配置的注入4、授权管理 ▲（1）授权可批量自动下发，自动回收 （2）支持公网授权验证方式 （3）支持内网授权验证方式5、性能要求（1）四层吞吐：2G （2）七层吞吐量：200M （3）最大并发连接：250K （4）每秒新建连接：40k （5）IPSEC VPN最大隧道数：500 （6）SSL VPN最大用户数:5006、用户认证 （1）支持本地用户认证 （2）支持外部服务器用户认证(RADIUS、LDAP、MS AD)  （3）支持AD/LDAP用户/组织结构同步 （4）支持Web认证 （5）支持基于MAC的用户认证 （6）支持Web认证后的SSO7、QOS流量管理 （1）支持两层八级管道嵌套，能够同时做到两个维度的流量控制,对多层级管道进行最大带宽限制、最小带宽保证、每IP或每用户的最大带宽限制和最小带宽保证 （2）支持链路状态监控，可查看指定应用/应用组详情，支持选择多条链路进行对比分析8、地址转换 ▲（1）为解决公网IP地址资源问题，支持NAT的端口扩展技术，实现单个公网IP的无限地址转换 ▲（2）支持NAT地址可用性探测，支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断9、高可靠性 （1）支持配置、会话同步 （2）支持修改虚拟MAC地址 （3）支持HA同步协商使用单播模式10、防病毒 ▲（1）支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型；支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式 （2）支持加密流量开启病毒过滤功能11、入侵防御 ▲（1）支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法 ▲（2）具备7000种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询，并支持网络实时更新 ▲（3）支持SQL注入、XSS防护及自动抓包，支持HTTP头域中的URL、Cookie、Referer、POST检查点配置防护策略12、VPN功能（1）支持IPSec/L2TP VPN及创新的PnP VPN （2）支持IKEv1、IKEv2协议 （3）支持 SSL VPN及TLSv1.2 ( 可选 USB-key) （4）支持Xauth协议 （5）支持OCSP和SCEP协议 （6）支持Android、iOS、Mac、linux等移动设备的安全接入13、未知威胁监测（1）支持SMTP、POP3、IMAP4、FTP等协议类型的检测 （2）支持对PE文件在上传云沙箱前进行文件可信证书检测 （3）支持APK、JAR、MS-OFFICE、PDF、SWF、RAR、ZIP等文件类型的检测 （4）独立出沙箱日志类型展示、支持行为报告PDF文件导出14、僵尸网络C2防御 ▲（1）支持通过监控C&C连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏，并定期升级更新僵尸网络服务器地址 ▲（2）支持TCP、HTTP、DNS协议检测 （3）支持C&C IP和域白名单 ▲（4）支持C&C IP和域名两种方式检测15、IP信誉库 支持对僵尸肉鸡、垃圾邮件发送者、Tor节点、失陷主机、暴力破解等风险IP的流量进行识别和过滤16、安全管理 （1）支持对管理员登录方式设定，包括Telnet、SSH、HTTP、HTTPS等 （2）至少内置三种管理角色，包括系统管理员、系统操作员、系统审计员 |
|  | 云数据库审计与防护 | 1 | 套 | 1、性能要求 （1）SQL处理能力≥30000条/秒 （2）采用海量日志存储及高速检索技术，日志存储能力≥25亿条（1T本地存储）▲（3）数据库实例：8个 2、云平台兼容性 支持公有云、私有云部署，支持目前市场上主流的云平台架构，如：VMware vCloud、 Openstack、 KVM、RHEV、Hyper-V、 CloudStack、 Apache Mesos等。3、多功能合一 ▲单一设备即可同时支持包括数据库审计、风险扫描、状态监控、运维审计等功能，可按需扩展，4、数据库兼容性 支持Oracle、SQLserver、MySQL、DB2、Sybase、Informix、Postgresql、Teradata、Cache、达梦、南大通用、人大金仓、神通、浪潮KDB、湖南上容、MongoDB、Hive、Hana、HWMPP、HighGo等20种主流数据库防护和审计5、数据库审计 （1）支持对SQL语句执行结果（成功/失败）、SQL语句执行时间、SQL语句执行异常等数据库操作响应信息的审计 （2）系统提供白名单规则策略，系统提供黑名单规则策略，系统提供正则表达式规则策略，系统提供关键字表达式规则策略，系统提供例外规则策略 ▲（3）支持定义事件类型，每种事件类型可以对应多个事件策略，不同策略命中的事件可以有高、中、低等多个风险级别支持定义所有SQL的相应威胁程度，至少包括高、中、低、提醒等告警级别 （4）对数据库客户端运行过程中自动产生的SQL语句的过滤，减少不必要的审计记录。 ▲（5）可对日志进行细粒度解析，支持审计数据库操作(DM)、对象管理(DD)、控制(DC)等操作语句的审计，解析后的日志记录至少包括访问发生时间、客户端IP地址、客户端MAC、终端程序、访问账号、访问数据库名、操作表名、SQL语句、数据库响应时间以及返回结果等关键信息。 ▲（6）通过三层关联技术，对应用服务器的真实用户/用户组的操作行为进行细粒度审计。6、审计策略与规则 设备必须自带默认审计策略，支持用户自定义策略和规则，系统必须支持配置操作行为的黑名单、白名单，方便用户灵活配置审计规则 ▲支持以操作类型、时间、IP地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间、关键字、敏感数据、等作为事件识别规则及审计规则7、审计告警 ▲（1）内置自动告警设置，允许用户设定威胁自动告警，告警必须提供级别设定，至少提供致命、高风险、中风险、低风险4种告警级别 （2）支持SYSlOG、SNMP TRAP、邮件、FTP等多种事件告警和提示方式8、白名单设置 （1）支持对于符合条件的SQL语句直接放行，不进行记录功能▲（2）支持时间、IP地址、用户名、终端名的白名单策略，将已知可信用户、可信时间之外的操作识别为高风险操作 9、访问控制功能 （1）能够根据不同的用户指定不同的数据访问策略，未授权用户在访问敏感数据时根据设置返回自定义的数据 （2）支持具备业务智能感知能力，可以自动学习应用程序访问数据库的行为特征，并自动建立安全访问规则，允许合法的访问行为，对异常SQL行为进行跟踪和阻断 （3）支持数据在线脱敏，支持前缀明文的脱敏方式，能够根据权限设置不同的脱敏方式，可对列中指定的前N字节不显示，例如对身份证号的前10个字节不显示。（支持数据库：人大金仓、MySQL）10、监控扫描▲（1）提供对数据库漏洞、不安全配置、弱口令、补丁等深层薄弱环节的安全检测及准确评估 （2）支持服务扫描和发现功能，通过扫描网络中的开放端口以及确定监听这些端口的服务。如主机IP、端口、主机操作系统、服务的类型等。并实现自动或手动将这些服务添加到数据库引擎 （3）支持对数据库服务器的扫描，实现对数据库的表、字段等敏感信息的自动识别11、检索 ▲（1）支持将审计日志的敏感字段进行模糊化处理，防止敏感数据泄露 ▲（2）支持SQL关键字翻译功能，支持将审计记录中SQL语句关键字翻译成中文，便于非专业人员阅读 |
|  | 云堡垒机 | 1 | 套 | 1、▲至少含50个授权；2、单点登录 ▲支持IE代填类型包括 JS、flash、HTML5等特殊登录页面；支持Google浏览器代填（仅支持HTTPS）3、支持协议类型 数据库类型： （1）Oracle：PLSQL、TOAD、SQLPLUS、SQLDEVELOPER （2）Mysql：MYSQLFRONT、HeidiSQL （3）SQL Server：SQLserver（2000-2012）（4）Informix：DBACCESS （5）Sybase：SCVIEW4 （6）DB2：DB2CMD、DB2QUEST （7）WEB应用：HTTP、HTTPS （8）KVM类:DSR、DSVIEW、RARITAN、RARITAN\_CC ▲（9）其它应用：AS400、PGADMIN、PCANYWHERE、RADMIN、DameWare、CiscoASDM、VMware vSphere Client ▲（10）其它应用：REALVNC4、系统自身安全性 ▲支持IP自动禁止功能，系统支持IP自动禁止功能，对连续登陆账号密码错误的来源IP自动屏蔽，可通过管理员解除屏蔽。5、无缝应用发布功能 ▲要求以上所有图形化应用在实际操作环境中均可以正常使用且可自由调整应用的窗口大小，做到无缝发布，拖拽窗口应自然流畅，无卡顿现象，像是在本地运行应用程序一样6、运维管理 ▲（1）支持向导模式，为管理员和运维人员提供操作向导模式，方便用户进行设备管理和使用 （2）支持自动化运维，可以制定计划任务，至字符类资产执行事先编辑好的脚本脚本超时执行时间为每个计划在单台机器上的超时时间。执行超过超时间后会断开连接 （3）支持首页自定义，用户在个人设置中自定义登录首页，首页可以配置为最近使用、常用、全局搜索等页面7、设备账号密码管理 （1）支持批量管理，在线批量设备帐号修改；支持设备帐号属性添加和修改，包括帐号密码、应用参数、帐号状态、特权帐号、应用端口、应用密码提示、帐号类型、帐号提示符、帐号同步、改密脚本 ▲（2）支持linux、unix、网络设备、windows2000/2003/2008的自动改密功能；无需通过插件、引擎或特殊端口对目标设备进行自动改密 ▲（3）在系统完成密码修改之后，自动进行新密码登录测试，以便进一步校验密码修改结果 ▲（4）支持将目标设备资产的账号密码进行密函打印导出 ▲（5）支持SSH公钥登录，通过ssh-keygen产生公钥和私钥密码对，上传堡垒机，可实现免密码登录服务器8、权限管理 （1）支持访问控制功能，系统提供访问控制功能，支持对系统的用户登录进行可配置的策略设置，根据策略因子：用户或用户组、日期、每月、每周、时间、源地址、目标地址、目标端口、目标账号、动作(接受、拒绝)来定制访问策略对用户或用户组行为进行控制 （2）支持SFTP和FTP目录锁定，默认规定用户登录后，只能在其目录下进行操作，不能随意跳转至其他目录进行操作，也可通过开关打开限制9、运维审计 （1）图形终端键盘操作记录：支持图形终端键盘操作记录，完整记录键盘动作 ▲（2）数据库运维SQL命令：系统应具备审计到详细的SQL语句，而非键盘符指令，并要求记录到SQL语句的执行时间 ▲（3）图形标题栏识别（OCR）：系统应具备对图形运维中的标题名进行智能提取，并可以从任意一个标题名开始回放。可支持中英文操作系统的标题栏体系。 （4）WEB在线回放完整会话；字符终端操作会话支持倍速播放；图形操作会话支持拖拉定位播放；支持暂停、停止、重新播放等播放控制操作 （5）审计录像采用数据流回放技术，空闲操作（无屏幕变化）日志无增长，节省了日志空间 ▲（6）系统应具备审计到FTP/SFTP传输的原始文件，并可以在审计系统上进行备份并下载查看其具体内容。支持人工开关自由选择是否备份原文件。 ▲（7）对大于一定大小的FTP/SFTP运维审计中的文件可进行异地转储，并可记录文件md5值，保障文件的完整性和有效性。 （8）提供搜索功能，可组合目标主机地址、登录地址、堡垒机用户、远程账号、时间、键盘输入的命令、标题栏等条件进行搜索，快速定位会话记录；搜索条件“用户命令”支持“或”和“与”逻辑关系 ▲（9）字符运维命令返回值搜索和屏幕导出，支持搜索命令的返回值信息，并支持将屏幕信息导出为文本10、告警模块 （1）支持图形操作告警，支持RDP会话针对操作行为告警（针对标题栏进行告警），可进行告警内容设置 （2）支持数据库操作告警，支持数据库应用针对操作命令进行告警，可进行告警内容设置（告警内容支持动作，表名等） |
|  | 云日志审计系统 | 1 | 套 | 1、性能参数 （1）支持2个虚拟网络接口 （2）日志处理速率：NAT日志20000/s、文本日志syslog3000/s （3）存储能力：2G链路下180天NAT日志存储 ▲（4）存储空间支持2TB ▲（5）支持集中和分级部署2、资产管理 **▲**（1）资产支持组织管理、网络管理 ▲（2）系统支持对IP对象的自动发现功能；对自动发现的设备可以转资产或删除3、日志处理速率 （1）二进制NAT日志：20,000EPS （2）SYSLOG日志：3,000EPS4、日志管理 ▲（1）支持IPv6的会话日志、NAT日志、PBR日志、SLB日志 ▲（2）被采设备无需安装任何代理 （3）支持通过以下种类进行日志浏览并可自定义查询条件，包括：事件日志、网络日志、配置日志、IPS日志、威胁日志、安全日志、会话日志、策略路由日志、NAT日志(含NAT444)、SLB日志、URL日志、IM（包含移动QQ、微信）上下线日志、论坛发帖日志、邮件日志、FTP日志 （4）支持查询条件记忆，记住最新使用的十个查询条件 ▲（5）支持第三方日志的收集和查询 （6）支持后台任务查询和邮件通知 ▲（7）支持分布式查询5、日志审计 ▲（1）支持显示审计事件分类统计列表，根据审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度展现 ▲（2）支持审计对象的定义，包括：审计目标对象、审计行为对象、审计行为执行者对象、审计来源对象、审计时间段对象等 ▲（3）提供预置审计策略模板，包括：Windows主机类审计策略模板、Linux/Unix主机类审计策略模板、防火墙类审计策略模板、扫描器类审计策略模板、IDS/IPS类审计策略模板、防病毒类审计策略模板、数据库系统类审计策略模板、萨班斯审计策略模版、等级保护审计模板等6、统计报表支持统计的报表内容包括： （1）系统资源、设备日志条数排名、设备日志所用空间排名、日志条数排名、日志所有空间排名、源IP日志量排名、目的IP日志量排名、日志接收趋势排名、威胁攻击次数、会话日志APP访问量、URL访问量等排名（2）支持按照天、周、月、季等周期生成周期性统计报表，统计粒度可达到分钟、小时和天，并能够通过邮件发送给指定人员。7、日志查询性能（1）10分钟内二进制日志查询低于20S （2）10分钟内文本日志查询低于20S （3）1天内二进制日志查询低于10min （4）1天内文本日志查询低于10min （5）1月内二进制日志查询低于100min8、设备监控 （1）支持对发送日志的设备状态监控 （2）支持自定义监控面板和监控内容9、基础系统 ▲基于Linux的专属安全系统，安全性高。 |
|  | 云WEB应用防火墙 | 1 | 套 | ▲1、性能要求 （1）网络层吞吐：5G（2）并发连接：40万 （3）HTTP吞吐量：1200M （4）HTTP并发连接/新建连接：10万/2800 （5）HTTPS吞吐量：200M （6）防护站点数量：102、Web应用防护 ▲（1）系统具备注入攻击防御能力，可以对SQL注入、LDAP注入、SSI指令注入、Xpath注入、命令注入、远程文件包含以及其他注入进行防御； （2）系统具备跨站攻击防御能力，可以对XSS和CSRF攻击进行防御； （3）支持SSL透明代理，可以对HTTPS网站进行保护； ▲（4）具备个人敏感信息防泄漏功能，可以检测到个人身份信息（包括中国大陆身份证号、港澳台身份证号、美国社会安全号）、银行卡号、信用卡号、邮件账号的信息泄露； （5）系统具备保护Cookie安全能力，可以防止Cookie被恶意篡改、Cookie被恶意劫持； （6）支持细粒度的HTTP命令级访问控制策略，可以根据客户端IP、HTTP操作方法、HTTP头名称、HTTP内容类型、HTTP协议版本、URI路径等进行访问控制； （7）系统具备特殊漏洞攻击防御能力，可以对针对Web服务器、Web框架、Web应用程序的漏洞攻击进行防御； （8）系统具备防御资源非法访问能力，可以对非法上传、非法下载和盗链攻击进行防御，支持根据文件大小、MIME文件类型进行非法下载控制； （9）部署在负载均衡设备或代理服务器之后时，可以解析源IP地址（支持X-Forward-For属性），对客户端的真实IP进行阻断； ▲（10）支持基于指纹技术的高级反爬虫和高级机器人流量识别；  ▲（11）周期性生成爬虫报告，区分非恶意爬虫，恶意爬虫，支持高级持久性爬虫；3、Web漏洞扫描及虚拟补丁 ▲（1）产品支持Web应用漏扫，支持的扫描各种类型的Web漏洞包括：SQL注入漏洞、XSS攻击漏洞、Web服务漏洞、信息泄露漏洞、异常访问漏洞；扫描方式支持普通扫描和侵入式扫描；支持手动扫描和定期扫描，可以定期自动扫描； ▲（2）可以对URL扫描深度、链接总数、文件数进行限制； （3）扫描报告可以进行导出，支持PDF、XML文件报告； ▲（4）支持根据扫描报告生成虚拟补丁，用户无需中断业务即可针对Web漏洞提供快速保护；4、网络层攻击保护 （1）支持各类拒绝服务攻击，包括：Ping of Death、Teardrop、IP分片、Land、ICMP大包、WinNuke等； （2）支持各类Flood攻击，包括ICMP Flood、UDP Flood、TCP-SYN Flood、ARP欺骗、DNS查询洪泛等；5、IPv6 （1）支持IPv4、IPv6双栈部署，可同时添加IPv4和IPv6地址为保护站点； （2）支持网站IPv6应用层改造；6、自学习策略 ▲（1）支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略；学习的内容包括：动态URL地址、URL参数、HTTP访问方法等信息； ▲（2）支持学习模式和保护模式，学习完成后可以自动切换到保护模式；7、应用加速及服务器负载分担 支持页面缓存及压缩、连接复用、支持SSL卸载；8、日志、报表和告警 ▲（1）提供韦富的日志信息，包括设备管理日志、网络安全日志、网页安全日志、防篡改日志、访问控制日志、自学习策略日志等 ▲（2）支持多级日志聚合，帮助管理员准确发现及定位威胁 ▲（3）支持记录攻击事件的HTTP所有请求头信息，含请求的URL、UserAgent、POST内容，cookie等 ▲（4）支持报表，提供安全风险概览、站点风险详情、攻击类型详情、站点篡改分析、站点访问量、网络层攻击汇总、系统运行状况等多维度报表模板，支持用户自定义报表9、运维操作 支持移动运维，通过手机 APP管理多台vWAF并监控其运行状态； |
|  | 网页防篡改系统 | 1 | 套 | ▲1、基本要求 （1）支持windows/Unix/Linux/Solarie/AIX/HP-UNIX等主流操作系统。 （2）支持IIS、Apache、Weblogic、Tomcat、WebSphere等WEB发布类型。 （3）B/S架构，可以支持多客户端管理。 （4）支持管理用户密码复杂度策略设置。 （5）核心技术采用基于文件过滤驱动保护技术。（6）License授权数量：102、性能要求 （1）响应时间：当网站文件遭到篡改攻击响应最短时间小于2ms。 （2）最多可保护对象：系统能够保护站点的最大文件和目录的数量不限。 （3）最大保护目录深度：系统能够保护站点的最长路径不得小于10级。 （4）资源占用率：系统运行过程中，被保护主机的CPU资源占用率和内存占用率小于2%。3、日志功能 （1）系统能够对用户操作、文件操作和修改、安全日志以及策略配置事件进行完整日志记录。 （2）系统支持日志记录查询及导出，支持excel报表导出查询。 （3）系统提供设备健康性日志图表统计。 （4）系统支持用户自定义模块报表生成。 （5）日志告警支持声音提示报警，支持邮件提示报警，系统支持报警提示框。 （6）系统需支持日志统计分析,根据操作类型,篡改文件等提供数据统计。4、防篡改功能 （1）支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 （2）支持自定义保护策略名称。 （3）支持仅监控保护功能。 （4）系统需支持用户权限分级,可以设立多个基于设备的受控管理员。 （5）支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 （6）系统支持管理设备图形化展示。 （7）系统配置完成后，系统后台运行，支持断线检测。 （8）系统支持在断线情况下对网页文件目录的防护功能。 （9）系统支持黑白名单设置功能，提供进程黑白名单设置。 （10）支持NFS网络文件系统防篡改保护。 （11）支持NAS等网络存储防篡改保护。 （12）支持docker容器应用的防篡改保护。 （13）支持设备性能实时监控，实时告警，并图形化展示。 （14）支持设备网络健康性监控，实时告警，并图形化展示。 （15）防篡改保护进程被意外终止后，依然可以进行网页防护。 （16）支持对系统关键文件目录的隐藏功能。 （17）支持用户在监控端手动启停保护功能，并需经过身份认证。 （18）可在管理平台对web服务器进行网络故障诊断。 （19）支持对系统服务进行监控功能。 |
|  | 安全管理中心 | 1 | 套 | 1、性能要求 可管理设备数量：20个2、部署方式 旁路部署、分布式部署3、登录方式 （1）支持HTTP/HTTPS/SSH登录方式管理HSM （2）支持本地和radius账户登录4、设备管理 （1）支持对NGFW设备进行集中管理 （2）支持K/X系列设备进行集中管理 （3）支持对NIPS设备进行集中管理 （4）支持对云·界进行集中管理 （5）支持对WAF进行集中管理 （6）支持对BDS进行集中管理 （7）支持对IDS进行集中管理 （8）支持通过IP/域名的方式从主动单台或批量添加设备 （9）支持设备主机名称、设备序列号、版本、管理IP、设备运行时间、接口状态、新建连接及会话等相关信息显示 （10）支持曲线图显示设备的接口状态、CPU利用率、内存使用率、会话数、总流量、应用流量以及用户流量等信息 （11）支持配置锁定 （12）支持批量重启NGFW设备 （13）支持批量修改NGFW密码 （14）支持NGFW自动化巡检 （15）支持按地域、VPN组网整理设备组 （16）支持设备组备份和恢复5、配置文件管理 （1）配置历史对比：基于高效文件比较算法,对两个配置文件进行快速比较，高亮显示差异内容 （2）配置文件恢复：支持配置文件单台/批量的导出、导入，支持通过本地的配置文件来恢复设备的配置 （3）配置变更管理：基于4W（Who、When、What\where）的审计方法，实时记录文件配置变更的内容 （4）配置文件定时获取：支持按照每天/周/月来定时获取配置文件6、升级管理 （1）支持对管理的防火墙、VFW和NIPS进行软件版本批量升级 （2）支持对APP、AV、IPS和URL特征库进行批量升级7、SD-WAN （1）支持VPN网络管理，包括VPN地图展示、列表展示 （2）支持上网业务和内网业务发布 （3）支持VPN星型组网，分支设备可通过U盘开局，快速组建VPN网络 （4）支持mesh组网8、策略运维 （1）支持对设备策略规则的统一集中管理，可以管理所有设备的策略规则，包括查看、编辑、删除设备本身的策略规则，创建共享策略规则并集中下发等 （2）支持单一设备的策略管理，可以管理单设备的策略规则，包括查看、编辑、删除设备本身的策略规则和策略下发等 （3）策略应用：给指定的设备策略统一在策略列表头部或者尾部批量添加安全策略，还可以为指定共享安全策略添加头部批量添加安全策略 （4）支持安全策略冗余检测和无用的对象检测,策略利用率、策略操作审计记录 （5）VSYS策略集中管理 （6）策略快照与回滚 （7）支持策略分组和策略导入导出 （8）支持批量添加私有策略 （9）策略匹配分析 （10）支持策略助手功能，通过分析FW的session日志，对已有策略进行分析，帮助用户生成更精细化的安全策略9、工单管理 （1）支持工单的新建、处理、审核、下发 （2）支持工单中对象名称自动生成，可自定义命名规则 （3）支持工单处理时自定义策略查找下发设备 （4）支持工单的新建、处理、审核、下发 （5）支持工单批量审核 （6）支持通过工单系统批量下发安全策略 （7）支持根据工单安全策略的源目IP地址自动匹配下发设备 （8）支持工单批量导入 （9）支持工单策略的冗余检测 （10）支持工单API，对接工单管理系统10、NAT配置管理 支持NAT规则的创建、删除和修改，支持NAT规则统一下发，支持NAT继承11、路由配置管理 （1）支持静态路由的创建、删除和修改 （2）支持私有策略路由的创建、删除和修改12、LLB集中管理 支持私有LLB模板配置管理，包括模板/规则的新建、编辑和删除13、IPS策略集中管理 支持私有和公有威胁防护策略创建，威胁防护列表维护；支持私有和公有IPS策略创建，IPS特征上传，支持IPS监控14、防病毒规则集中管理 支持私有和公有防病毒规则创建、删除、修改和管理并在策略中调用下发15、URL规则集中管理 支持私有和公有URL规则创建、删除、修改和管理并在策略中调用下发16、iQoS规则集中管理 支持私有和公有iQoS规则创建、删除、修改和管理17、SLB规则管理 支持在对象中添加SLB服务池，支持DNAT中配置SLB服务池18、AAA配置管理 支持在防火墙和VFW上对象中配置AAA服务器，支持AAA服务器的创建删除和配置修改19、用户配置管理 支持在防火墙和VFW上本地AAA服务器上的用户和用户组的创建、修改和删除，支持批量导入本地用户支持外部AAA服务器上的用户的同步和查看20、角色配置管理 支持在防火墙和VFW上创建、修改和删除角色，支持角色映射管理的创建修改和删除21、监测对象 支持私有监测对象的配置管理，包括新建、编辑、删除22、内存配置 支持mysql内存可配23、设备监控 （1）总设备数统计 （2）在线设备数统计 （3）最近一小时告警数统计 （4）设备告警信息实时监控 （5）设备运行状态实时监控 （6）支持实时的流量监控，并在客户端通过饼状图或者柱状图直观显示 （7）支持设备接口（TOP 10）流量查看， （8）支持指定接口TOP 10 IP流量查看，支持指定IP的TOP 10应用的流量查看 （9）支持指定接口TOP 10应用查看，支持指定应用的TOP 10 IP的流量查看 （10）支持实时的攻击情况监控，支持饼状图或者柱状图直观显示： （11）支持设备接口遭受攻击（TOP 10）查看；  （12）支持指定接口发起攻击TOP 10 IP查看，支持指定IP发起的TOP 10攻击类型查看 （13）支持指定接口TOP 10攻击类型查看，支持发起指定攻击类型的TOP 10 IP查看 （14）支持VPN状态监控，支持VPN拓扑图呈现 （15）支持实时的被管理设备的受病毒攻击情况监控，支持饼状图直观显示24、日志管理 （1）安全管理中心平台可接收设备发送的多种日志信息，经过系统处理后，用户可进行多维度、多条件的浏览，日志根据颜色区分级别 （2）支持通过以下种类进行日志接收并可自定义查询条件，包括：系统日志、配置日志、会话日志、地址转换日志（NAT和NAT444）、网页访问日志、主流网络应用日志（如即时通信、文件传输、BBS、邮件等） （3）支持数据安全日志 （4）支持策略路由日志接收和自定义条件查询 （5）支持日志搜索功能，搜索条件记录和书签 （6）支持日志导入和自动或手动导出，远程日志备份，支持日志清理功能 （7）支持将日志转发至第三方syslog平台进行存储解析 （8）支持基于日志查询结果导出可读日志至本地或FTP Server （9）支持日志过滤功能，过滤条件包括设备选择、日志类型、日志级别25、查询管理 （1）支持查看历史监控信息，通过定义历史查询条件，包括指定查询参数和设置查询时间，进行历史数据统计和分析 （2）可历史数据统计包括：流量统计分析、攻击统计分析、病毒统计分析、上网行为统计分析26、统计报表 （1）提供直观、丰富的统计报表，通过对设备信息、网络访问和用户行为进行综合分析，为用户呈现全方位、多角度的统计数据和图表 （2）支持按照天、周、月、季等周期生成周期性统计报表，统计粒度可达到分钟、小时和天，并能够通过邮件发送给指定人员 **支持统计的报表内容包括：**（1）设备状态、流量报表、网页浏览审计报表、即时通信审计报表、 网络行为审计报表、病毒过滤审计报表、设备的病毒数统计信息"（2）支持自定义报表任务和系统的预定义报表任务（3）支持自定义报表创建人（4）支持自定义报表输出邮件标题及正文（5）支持VPN断线统计报表27、告警 （1）支持基于攻击次数、病毒数阈值、特征事件、关键字、日志级别等多种告警条件定义  （2）支持通过邮件和短信方式外发告警信息28、权限管理 （1）基于角色的用户管理，支持预定义系统管理员、操作员和审计员等角色，并可自定义角色 （2）基于设备(或VSYS)的权限管理29、系统 （1）支持中英文界面并可切换 （2）支持系统时间/时区修改和internet同步 （3）支持系统磁盘自动清理 （4）支持配置备份和恢复，导出和导入 （5）诊断工具：通过DNS查询、ping、traceroute等方式进行网络排错 （6）支持系统自动修复功能 （7）支持HSM系统密码保护 （8）支持联动智源，可通过智源单点登录到HSM （9）支持HSM和防火墙使用FTPS方式进行数据传输 （10）支持admin账户修改默认用户名 （11）支持密码管理，包括密码锁定策略，密码策略 （12）支持监测进程健康状态，异常时可自动恢复 （13）支持监控syslog日志速率 （14）支持系统日志监测及自动清理机制 （15）支持预估HSM磁盘的剩余天数30、IPv6支持 （1）支持IPv6策略、NAT、地址薄配置管理 （2）支持IPv6日志采集和查询，包括NAT日志、SESSION日志、PBR日志 （3）IPv6格式的监控数据的采集、呈现、查询包含设备监控、用户监控、传统威胁监控、上网行为监控 |
|  | 漏洞扫描 | 1 | 套 | 1、性能要求 IP并发数默认50个，最大100个；任务并发数10个。2、资产管理 （1）支持资产树形结构对资产管理，并可自定义资产组 （2）可对选中资产的提供连通性测试，对测试不通过的资产提供可参考的信息3、资产探测 （1）支持端口与服务发现。可对监控目标进行全端口扫描，并整理出服务的端口、应用软件类型、版本，并提供搜索接口可对目标进行搜索。▲（2）端口扫描方式：支持TCP SYN扫描、connect扫描、TCP ACK扫描、UDP扫描、TCP FIN扫描、TCP NULL扫描、Xmas Tree扫描、idle扫描等 （3）资产属性变更历史查询：可针对扫描结果进行回溯，查找IP地址以往开启的端口状况▲（4）支持自动生成网络拓扑图，并支持手动编辑拓扑图4、漏洞检测 （1）支持SQL注入、XSS跨站脚本、命令执行、目录遍历、上传漏洞等检测,能追踪最新的安全漏洞，并及时更新 ▲（2）系统支持自助式添加安全扫描插件，安全扫描插件可通过发包匹配关键字与自定义扫描代码方式添加。 ▲（3）支持输入Cookie信息和Cookie自动录制，进行登录扫描 （4）支持自定义爬虫规则5、主机扫描 （1）扫描对象支持Windows系列、Linux系列、Unix系列、数据库、应用程序、虚拟化平台等▲（2）支持安全扫描，保证扫描过程中目标系统正常运行 （3）能够扫描常见的网络安全客户端软件（网络防病毒Symantec、TrendMicro、McAfee）的安全漏洞。 （4）能够扫描常见的应用软件漏洞（如IE浏览器、MSN、Mozilla Firefox、Yahoo Messenger、MS Office、多媒体播放器、VMware虚拟机）的安全漏洞 （5）提供专门针对DNS服务的安全漏洞的检测▲（6）漏洞规则超过58000条6、数据库扫描 ▲（1）支持授权扫描、非授权扫描 （2）漏洞规则库包括1700多条策略，覆盖权限绕过漏洞、SQL注入漏洞、访问控制漏洞、执行权限过大漏洞、访问权限绕过漏洞、DBMS漏洞、提取漏洞等 ▲（3）支持扫描数据库中隐藏的木马病毒7、基线配置检查 （1）支持的操作系统有：Windows（32位Windows XP/7 8/10/ Server、64位Windows XP/7/8/10/ Server）、Linux（Centos、Debian、Fedora、Redhat、Suse、Ubuntu等）、Unix（Aix、HP-UX、Solaris等）、国产操作系统（中标麒麟、红旗、深度、凝思等）等 ▲（2）针对windows系统可采集操作系统基本信息、硬件基本信息、应用软件、进程、活动端口开放情况、开机自启动项、用户列表、主机日志信息、补丁信息、安全审计信息和安全策略配置情况，能够采集浏览器上网记录、USB使用记录。 （3）扫描能力支持灵活的检查任务制定功能，可以设定手动、定时任务的配置任务检查方式 ▲（4）支持安全基线检查项自定义功能8、弱口令扫描 支持对SMB、FTP、POP3、SMTP、SSH、TELNET、SNMP、RDP、redis、Oracle、MySQL等协议进行在线弱口令扫描9、等保合规 （1）支持新建等保测评任务，并支持设置基础信息系统SAG等级 （2）支持导出等保测评报告10、渗透测试 支持SQL注入（获取数据库、表、执行任意命令等）、子域名爆破、GNU Bash 远程代码执行漏洞、Struts 2 S2-005、Struts 2 S2-007、Struts 2 S2-008、Struts 2 S2-009、Struts 2 S2-012、Struts 2 S2-013、Struts 2 S2-045、Struts 2 S2-048、Struts 2 S2-053、Adobe ColdFusion 文件读取漏洞、Couchdb 垂直权限绕过漏洞、Discuz 7.x/6.x 全局变量防御绕过导致代码执行、Drupal Drupalgeddon 2 远程代码执行漏洞等渗透测试功能11、基线配置核查 ▲（1）支持安全基线检查项自定义功能 （2）安全配置核查时，程序占用的资源应尽量的少，扫描主机的CPU平均占用率小于10％，内存占用小于50M；被扫描主机的CPU占用率小于1％，内存占用小于3M；12、报表管理 （1）应提供多维度报告统计功能，报告包含漏洞详情、漏洞描述、漏洞风险级别、加固建议等，提供导出功能，格式支持Html、Excel、PDF、Word等主流格式。 （2）报表统计支持漏洞验证，要求提供详细的验证用例，且漏洞验证需要提供完整的http请求头，并要求提供详细的测试用例13、补丁联动 支持与微软WSUS补丁系统联动 |
|  | 态势感知 | 1 | 套 | 1、流量解析预处理 支持常见的PPPOE、VLAN、MPLS等链路层协议；支持对HTTP、DNS、SMTP常用网络协议进行深度解析。2、协议识别 能够准确识别HTTP、DNS、SMTP、POP3、IMAP4、HTTPS、NFS、FTP、SSH等常见的网络应用；能够识别非标准端口上的各类常用应用，例如在非80、8080端口上运行的HTTP应用。3、资产发现 主动扫描和被动流量监控两种资产探测方式，实时精准的持续监控资产变化情况，可自动发现网络设备、主机、安全设备、操作系统、数据库、web应用等。识别和关联资产端口、服务、组件等信息，全面掌握网络资产状态。4、资产管理 自动统计网络资产数量、变化趋势、归属、端口分布、组件分类、操作系统分布等属性信息，自定义资产标签及硬件信息，根据资产属性特征或标签信息进行分类检索统计。自动关联资产存有漏洞及异常行为。5、脆弱性检测 通过漏洞扫描完成资产脆弱性评估，漏洞库可覆盖当前网络环境中主流的操作系统、数据库、web中间件、网络设备漏洞，同步更新国家能力中心漏洞检测规则，有效应对突发安全事件，支持以资产存在漏洞及漏洞影响资产两个维展示脆弱性资产。6、网络威胁检测 通过协议分析、内容萃取等报告对应的异常事件。可检测勒索软件、恶意软件、信息泄露、C&C通信、扫描探测、暴力破解、系统提权、web攻击等网络威胁。同步国家能力中心下发的恶意URL、域名等信誉数据，完成新型威胁及高级持续威胁的检测。7、攻击源警告 支持对存在恶意入侵或探测行为的攻击源IP，推送告警界面，以做警示威慑。8、恶意网站警告 通过国家信誉库自动同步恶意网站数据，在用户网络访问恶意网站检测，并对该用户推送警告页面，可自定义配置警告页面。9、威胁检测规则库 内置网络威胁检测规则不少于10000条。10、漏洞知识库 漏洞库不少于40000条。 |
|  | 云专线资源配置 | 1 | 项 | ▲1、线路带宽：1条 100M、1条10M； 2、接口类型：LC，FC，RJ45等； 3、线路技术指标：单条专线端到端可用率≥99.90%，电路比特误码率≤1×10-7，丢包率≤0.1%，各个节点最大时延≤10ms，时延抖动率≤10ms； ▲4、专线要求全网端到端必须采用光传输通信系统或裸光纤进行组网，提供端对端透明传输，为了确保采购方的网络安全、易维护性，采购方不接受采用PTN、IPSEC、MSAP等类似技术方式组网，并要求保证采购人的数字光纤线路为专用线路，并与其他网络物理隔离； 5、专线要求具有核心网全程网管监控功能，并实行7\*24小时实时监控，具备自动告警、日志查询等功能；6、要求光传输系统均为自愈环保护，具有故障自动倒换功能，能保证各电路不会因光传输系统环光缆内一侧光纤的意外阻断的故障而中断；自愈保护是指在网络发生故障（例如光纤断）时，无需人为干预，网络自动地在极短的时间内，使业务自动从故障中恢复； 7、接入地点：采购人指定地点。 |
|  | 等保安全运维服务 | 1 | 项 | 落实等保2.0的安全运维管理，提供日常安全运维，包括但不限于网络、服务器、云平台、安全设备配置策略的变更、调整和优化，定期进行安全巡检（客户提供EDR工具）、资产梳理、漏洞扫描（客户提供漏扫工具）、应急响应等服务。 |
| **一、商务条款** |
| **签订合同时间** | 自成交通知书发出之日起15日内。 |
| **质保期** | 自提交服务验收合格之日起至合同期满止 |
| **交货时间及地点** | 交货时间：合同签订生效后。交货地点：采购人指定地点。 |
| **售后服务要求** | 1、供应商应保证所提供的移动终端为符合国家知识产权法律法规要求的国产正版产品，质保期为一年，按国家有关规定执行产品“三包”，如因质量问题或故障，凭厂商维修中心或特约维修点的质量检测证明，10日内享受免费更换服务，15日以上在质保期内的享受免费保修服务，质保期外的服务费用由采购人和成交供应商另行商议。2、投标时须提供详细的技术方案、实施组织方案、售后服务、保密承诺等，并提供售后服务承诺书及售后服务机构及联系人名单；3、提供7×24小时热线电话服务,并提供故障申告途径及绿色通道，做到全方位响应，并指定专人负责业务调试、维护及检测工作；4、故障响应时效：接到故障处理要求后1小时内响应，一般性故障4小时内解决问题，重大故障8小时内解决。如8小时内无法解决，应向采购人提供备用方案。故障解决后48小时内，应向采购人提交故障处理报告。报告中必须说明故障种类、故障原因、故障处理方法等；5、服务期内，应对本次租赁范围内的系统技术支持、维护管理、变更割接等工作，不向用户收取额外费用；6、免费将所有货物送货上门，免费安装调试；7、对采购人进行现场技术培训；8、每季度不少于1次定期回访及对系统进行维护，并出具巡检报告；9、在服务期内免费安排至少1名工程师为该项目定向服务，以保障系统的实施不间断运行和充分地应急处理；10、保证网络系统的畅通，如果网络系统出现问题，必须在接到报告后2个小时内到达现场，负责排除故障，直到系统网络恢复正常，如网络设备故障在8小时内无法修复的应免费提供备件；11、每个季度对网络系统进行一次巡检，检查网络系统设备的运行情况，提交巡检报告；12、当用户系统需要扩展、迁移或升级时，供应商负责免费提供相应解决方案等技术支持；因供应商施工、系统网络割接等原因影响系统运行的，应当提前一天通知用户，并且尽快消除故障；13、在等保测评、攻防演练行动等专项安全任务期间，供应商协助采购人对云主机操作系统漏洞进行补丁升级，为保证升级后不影响业务，补丁应在采购人业务系统的测试环境中验证，并在升级前对云主机进行备份。 |
| **付款条件** | 1、资源开通后，按照年费的支付方式，根据成交供应商或成交供应商指定下属机构的收费通知单缴纳使用费。缴纳费用后，成交供应商或成交供应商指定下属机构向采购人开具相应金额的符合国家规定的发票。 |
| **合同期限** | 服务期：3年 |
| **其他要求** | ▲1、报价必须含以下部分，包括：（1）每项资源的单项服务价格；（2）各项税金；（3）其他（如运输、装卸、安装、调试、培训、技术支持、售后服务、验收等费用）。▲2、成交供应商提供的服务如果与投标时的承诺不相符，或提供虚假承诺的，采购人有权解除合同。 |
| **二、谈判小组根据与供应商谈判情况可能实质性变动的内容**未标识‘▲’及未表述为“须”或“必须”的采购项目技术规格、参数及要求。 |

# 第四章 响应文件格式

单一来源采购响应文件（封面）

采购项目名称：

采购项目编号：

响 应 内 容：

 （报价人名称）

 年 月 日

**目 录**

1）报价表…………………………………………………………………………………

2）报价函……………………………………………………………………………

3）商务、技术响应、偏离情况说明表……………………………………………………

4）法定代表人（负责人）授权书原件、法定代表人（负责人）及委托代理人身份证复印件（非委托代理时只须提供法定代表人（负责人）身份证复印件）……………………………………

5）有效的营业执照等证明文件复印件…………………………………………………

6）财务状况报告…………………………………………………………………………

7）纳税证明………………………………………………………………………………

8）社保缴纳证明…………………………………………………………………………

9）无重大违法记录和不良信用记录书面声明……………………………………………

10）具备履行合同所必需的设备和专业技术能力的证明材料………………………………

11）售后服务承诺书

12）本采购项目《采购需求》中要求必须提交的材料………………………………………

13）具备法律、行政法规规定的其他条件的证明材料………………………………………

14）本单一来源采购文件要求提供的其他资料和需要说明的问题……………………………

**（本目录可根据单一来源采购文件要求必须提供的资料排序，其余资料酌情提供）**

附件一

1、报 价 表

采购项目名称:

采购项目编号: 分标

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量/单位** | **报价（元）** | **交货时间** | **备注** |
| 1 |  |  |  |  |  |
| 总报价（人民币大写）： （￥ 元） |

注：1、所有价格均用人民币表示，单位为元，精确到个数位。

2、报价含服务、随配附件、备品备件、工具、施工配合费、税金及其他所有成本费用的总和及采购文件所要求的相关服务以及合同所示全部责任、义务和一般风险等全过程产生的所有成本和费用以及一切税费，对采购的全部服务进行完整唯一报价。

法定代表人（负责人）或委托代理人（签字）:

报价人名称（盖章）：

报价时间： 年 月 日

附件二

2、报 价 函

广西国建项目管理有限公司：

依据贵方（项目名称/文件编号）项目采购的邀请，我方（姓名和职务）经正式授权并代表报价人（报价人名称、地址）提交下述单一来源采购响应文件正本一份和副本 四 份。

1. 报价表；

2. 供货清单；

3. 商务、技术响应、偏离情况说明表；

4. 按单一来源采购文件报价人须知和技术规格要求提供的有关文件；

5. 资格证明文件；

在此，授权代表宣布同意如下：

1. 将按单一来源采购文件的约定履行合同责任和义务；

2. 已详细审查全部单一来源采购文件，包括（补遗文件）（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力；

3. 同意提供按照贵方可能要求的与其协商有关的一切数据或资料；

4. 与本单一来源采购有关的一切正式往来信函请寄：

电话/传真： 电子函件：

日期： 年 月 日

报价人或法定代表人（负责人）或授权代表签字或盖章：

报价人名称（签章）：

开户银行： 帐号/行号：

附件三

3、商务、技术响应、偏离情况说明表

采购项目名称:

采购项目编号:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称  | 单一来源采购文件要求 | 单一来源采购响应文件具体响应 | 响应/偏离 | 说明 |
|  | 商务部分 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| … |  |  |  |  |  |
|  | 技术部分 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| … |  |  |  |  |  |

说明：1、应写明单一来源采购响应文件对商务与技术要求的响应和偏离情况；

2、应对照单一来源采购文件“第三章 采购项目需求”，逐条说明所提供货物和服务已对单一来源采购文件的技术规格做出了实质性的响应，并申明与技术规格条文的响应和偏离。

法定代表人（负责人）或授权代表签字或盖章:

 年 月 日

附件四

4、法定代表人（负责人）授权书

广西国建项目管理有限公司：

兹授权 同志为我公司参加贵单位组织的（项目名称、项目编号）单一来源采购采购活动的报价代表人，全权代表我公司处理在该项目活动中的一切事宜。代理期限从 年 月 日起至 年 月 日止。

授权单位（签章）：

法定代表人（负责人）（签字或盖章）：

被授权代表（签字或盖章）：

签发日期： 年 月 日

附：代理人工作单位：

职务： 性别：

身份证号码：

|  |
| --- |
| 粘贴法定代表人（负责人）、被授权人身份证（正、反两面复印件） |

附件五

其 他 文 件

5、有效的营业执照等证明文件复印件；

报价人有效的“营业执照”（报价人为事业单位的不需要提供“营业执照”，但需提供“事业单位法人证书”）等证明文件复印件；**[必须提供，原件备查]**

6、财务状况报告；**[格式自拟，必须提供]**

7、报价文件递交截止之日前半年内报价人连续三个月的依法缴纳税费或依法免缴税费的证明复印件；无纳税记录的，应提供由报价人所在地主管国税、地税部门出具的《依法纳税或依法免税证明》复印件**[格式自拟，必须提供]**。（新成立单位按实际提供）

8）报价文件递交截止之日前半年内报价人连续三个月的依法缴纳社保费的缴费凭证复印件**；**无缴费记录的，应提供由报价人所在地社保部门出具的《依法缴纳或依法免缴社保费证明》复印件**[格式自拟，必须提供]**。（新成立单位按实际提供）

9）参加采购活动前三年内在经营活动中没有重大违法记录和不良信用记录的书面声明；**[格式自拟，必须提供]**

10）具备履行合同所必需的设备和专业技术能力的证明材料；**[格式自拟，必须提供]**

11）售后服务承诺书（内容可以是提供的切实可行的售后服务和优惠承诺）；**[格式自拟，必须提供]**

12）本采购项目《采购需求》中要求必须提交的材料；**[如有要求，则必须提供]**

13）具备法律、行政法规规定的其他条件的证明材料[如有规定,则必须提供]**；**

14）本单一来源采购文件要求提供的其他资料和需要说明的问题

**（以上附件可根据单一来源采购文件要求必须提供的资料排序，其余资料酌情提供）**

# 第五章 合同主要条款

**南宁金融集团综合管理平台公有云服务采购 合同**

**项目编号：**

**采购人： 南宁金融投资集团有限责任公司**

**中标单位：**

**目 录**

**一、合同书**

**二、合同附件**

1、中标通知书

2、招标文件服务需求一览表

3、招标文件的更改通知（如有）

4、投标函

5、投标报价表

6、投标服务技术资料表

7、商务条款偏离表

8、中标单位澄清函（如有请提供）

9、其他与本合同相关的资料（如有请提供）

**合同书**

项目名称： 南宁金融集团综合管理平台公有云服务采购

项目编号： GXTZ-ZB-2020第（1004）号

分标号（有分标时填写）： /

甲方（买方）： 南宁金融投资集团有限责任公司

乙方（卖方）：

根据 年 月 日 项目的单一来源采购中标结果，甲方接受乙方为本项目的中标人，甲乙双方在平等自愿、互利互惠的基础上,双方根据《中华人民共和国合同法》等法律、法规规定，按照招投标文件规定条款和中标人承诺，甲乙双方签订本合同。

**第一条服务内容**

1.1 甲方向乙方租用安全可靠的专属云服务实现应用系统的快速部署，满足甲方业务快速发展，需要乙方同意根据本合同约定和甲方要求提供专属云租赁服务。项目实施的地点为广西南宁市。

1.2 本服务的具体内容，以经甲乙双方共同签署的产品需求单（产品需求单模板见附件[一]）为准。甲乙双方在本合同期内拟增加或变更服务内容或配置，由甲乙双方另行签署产品需求单予以确认。

1.3乙方负责搭建服务门户，并向甲方提供在服务门户中具有唯一识别性的账户，供甲方通过该账户登陆服务门户、使用本服务。

**第二条服务费用及支付**

2.1甲方使用本服务，应当按照实际使用的服务项目向乙方支付服务费用。本项目合同金额暂定为： **人民币 元整（￥ ），**最终总价双方根据实际开通资源计算。

甲方在本合同期内按照本合同约定使用本服务并支付费用。

2.2支付方式和时间

资源开通后，按照年费的支付方式，根据乙方或乙方指定下属机构的收费通知单缴纳使用费。缴纳费用后，乙方或乙方指定下属机构向甲方开具相应金额的符合国家规定的发票。甲乙双方银行账户信息和税务信息如下：

甲方信息如下：

开户银行：[ ]

银行地址：[ ]

户名：[ ]

账号：[ ]

统一社会信用代码：[ ]

地址：[ ]

电话：[ ]

乙方信息如下：

开户行：[ ]

银行地址：[ ]

户名：[ ]

账号：[ ]

统一社会信用代码：[ ]

地址：[ ]

电话：[ ]

2.3甲方如对当期应支付服务费用有异议，应当以书面方式向乙方提出核对申请。经双方核对确有错误的，乙方将在次月对相应服务费用进行调整。

2.4本合同及附件中所称各项费用及资费标准均为含税价。

**第三条资质保证及服务账户**

3.1 甲方承诺以其真实身份开通和使用本服务，自本合同签订时至履行的全过程中，甲方应当持续具有合法有效的主体资格和业务资质，并按照本合同约定向乙方提供真实、合法、有效、完整的各类主体资格、业务资质文件。不具备前述条件的，乙方有权直接解除本合同，并追究甲方相应责任。

3.2 甲方使用本服务开展互联网信息服务等相关业务的，甲方保证于本合同签订时及本服务期限内持续具备开展该等业务所需的全部资质及/或履行相关手续。

3.3如甲方违反在本合同及附件中任一项保证的，包括但不限于在本合同签订时不具备开展业务所需的全部资质许可、履行相关手续，或在本服务期限内丧失全部或部分资质许可的，乙方有权暂停提供本服务，并要求甲方在限期内改正；如甲方在限期内未改正的，乙方有权解除本合同，并不承担任何责任。甲方应当承担违约责任，并赔偿乙方的相应损失。

3.4乙方负责搭建服务门户，并向甲方提供在服务门户中具有唯一识别性的账户，供甲方通过该账户登陆服务门户、使用云业务服务。甲方账号和密码是甲方办理、使用业务的重要凭证，除非另有约定或说明，凡该账户所发出的指令及相关行为均视为甲方的行为，甲方应承担由此造成的一切后果和责任。

3.5甲方负责其在乙方服务门户中的账号和密码的保密和使用安全，乙方向甲方提供本服务相关账户的初始密码，甲方应第一时间修改密码。如因甲方原因导致账号或密码泄露或为他人获取的，甲方自行承担损失和责任。甲方发现其账号或密码被他人非法使用或有使用异常的情况的，应及时根据乙方公布的处理方式通知乙方采取措施暂停该账号的登录和使用。乙方在收到甲方要求采取措施暂停其账号登录和使用的通知后，将要求甲方提供甲方的有效身份证件；经核实甲方所提供身份证件信息与其注册的身份信息相一致的，乙方应当及时采取措施暂停甲方账号的登录和使用。甲方没有提供其有效身份证件或者所提供身份证件所载信息与所注册的身份信息不一致的，乙方有权拒绝甲方前述请求，由此造成的损失由甲方自行承担。

**第四条甲方的权利和义务**

4.1甲方使用本服务的，必须遵守《中华人民共和国网络安全法》《中华人民共和国电信条例》《中华人民共和国计算机信息网络国际联网暂行规定》和其他有关法律、法规或相关规定，不得存在任何违法违规行为，不得侵犯乙方以及任何第三方的合法权益。

4.1.1除遵从本合同其他条款及附件要求外，甲方使用本服务所发布、传输或存储的信息内容不得存在以下任一情形，且不得为他人发布、传输或存储该类信息内容提供任何便利（包括但不限于设置URL、链接等）：

（1）违反国家规定的政治宣传和/或新闻信息。

（2）危害国家安全、泄露国家秘密的信息。

（3）宣扬封建迷信，散布淫秽色情、赌博、暴力、恐怖或者教唆犯罪的信息内容。

（4）违反国家民族政策和宗教政策的信息内容。

（5）博彩有奖、赌博游戏、“私服”、“外挂”等非法活动。

（6）侮辱或者诽谤他人，侵害他人合法权益。

（7）妨碍互联网运行安全的信息。

（8）其他有损于社会秩序、社会治安、社会公共道德，违反法律法规强制性规定，或侵害他人合法权益的信息内容。

4.1.2甲方不得有任何危害或可能危害乙方云业务服务相关平台、乙方服务门户、以及网络安全和信息安全的行为，包括但不限于：

（1）对乙方服务门户、相关平台的功能或者存储、处理、传输的数据和应用程序进行删除或者修改。

（2）利用网络及系统从事窃取或者破坏他人信息、损害他人合法权益的活动。

（3）故意制作、复制、传播计算机病毒或者以其他方式攻击他人服务。

（4）进行钓鱼、黑客攻击、网络诈骗等非法行为，网站或空间中含有或涉嫌散播病毒、木马、恶意代码等，或通过虚拟主机对其他网站、主机进行涉嫌攻击的行为，如扫描、嗅探、ARP欺骗、DOS等。

（5）危害网络安全和信息安全的其他行为。

4.1.3甲方不得利用乙方提供的服务发布不受欢迎的或者未经请求的电子邮件广告或包含反动、色情等违法或有害信息的电子邮件等电子信息。

4.1.4甲方不得建立或利用设备、配置运行与本服务无关的程序或进程，而大量占用乙方云计算资源（如云服务器、网络带宽、存储空间等）所组成的平台中服务器内存、CPU或者网络带宽资源，给乙方云业务服务相关平台、乙方服务门户或者乙方其他用户的网络、服务器（包括但不限于本地及外地和国际的网络、服务器等）、产品/应用等带来严重负荷，影响乙方与国际互联网或者乙方与特定网络、服务器及乙方内部的通畅联系，或者导致乙方云平台产品与服务或者乙方的其他用户网站所在的服务器宕机、死机或者用户基于云平台的产品/应用不可访问等。

4.1.5甲方不得进行任何改变或试图改变乙方提供的系统配置或破坏系统安全的行为。

4.1.6若甲方存在上述4.1.1至4.1.5条约定的任一情形的，乙方有权根据相关情况采取相应处理措施，包括但不限于立即中止服务、终止服务或删除相应信息，保存有关记录，并向政府主管部门报告，由此引起的一切后果和责任由甲方负责。同时，乙方有权解除本合同，并不承担任何责任。

4.2甲方使用本服务所引起的一切后果由甲方承担。如因甲方使用本服务所涉行为或内容不合法或侵权而导致乙方承担责任或对乙方造成损失的，甲方应负责解决，并赔偿乙方由此遭受的全部损失；同时乙方有权解除本合同。

4.3本服务期限内，甲方对由乙方分配的IP地址具有使用权，且不可以任何方式转由他人使用。甲方不得私自使用乙方未分配给甲方的IP地址。甲方不再使用本服务时，相关IP地址使用权由乙方收回。

4.4甲方承诺，不得通过转让、出租、无偿使用或其他任何方式许可甲方之外的任何第三人使用本服务。否则，乙方有权解除本合同，并追究甲方相应责任。

4.5对于甲方使用本服务所涉自身信息和资料、数据（包括但不限于商业机密等）、最终用户及其他相关主体的信息和资料、数据等，甲方负责保密，并自行承担由此产生的一切后果和责任。甲方使用本服务时，应自行对云主机上的数据进行定期备份（包括不限于应用程序、数据库、系统配置文件等）。

4.6甲方应向乙方提交执行本合同的联系人和管理甲方在服务门户中的账号和密码的人员名单和联系方式。如以上人员发生变动，甲方应自行将变动后的信息进行在线更新并及时通知乙方，因甲方提供的信息不真实、不准确、不完整，以及以上人员的行为或不作为而产生的结果，均由甲方承担。

4.7甲方知悉乙方无法保证其所提供的服务毫无瑕疵，但乙方承诺不断提升服务质量及服务水平。甲方确认并同意：若乙方提供的服务瑕疵是当时行业技术水平所无法避免的，将不视为乙方违约。甲方将配合乙方一同合作解决上述瑕疵问题。

**第五条乙方的权利和义务**

5.1 乙方负责按照本合同约定的条件提供云业务服务及相关的支撑服务。

5.2在本服务期限内，乙方承诺通过服务门户工单、邮箱等多种方式为甲方提供7日\*8小时的服务支持；其中，对于主机无法远程、网络访问中断问题，乙方通过服务热线电话为甲方提供7日\*24小时售后服务。

5.3 乙方有权对甲方对外公布的信息内容进行检查，一旦发现信息内容或者指向这些内容链接的数据或信息中含有任何违反相关法律法规规定、本合同约定或者超出经营许可或备案项目范围的内容的，乙方有权要求甲方进行修改、删除；如甲方不予改正，则乙方有权终止向甲方提供本服务。

5.4 乙方有权根据相关法律法规要求及本合同约定拒绝甲方发布的网站、信息数据内容，如甲方不同意乙方拒绝其提交的网站、数据内容或不进行答复的，则乙方有权终止向甲方提供本服务。

5.5对于甲方使用本服务时非因甲方原因出现的云计算资源、云存储资源、互联网接入故障，乙方应当解决，但因甲方原因和/或不可抗力引起的除外。

**第六条数据管理**

6.1为更好地向甲方提供服务之目的，乙方可能收集、使用和对外提供甲方的数据，包括但不限于向甲方发出产品和服务信息。本条所述“甲方的数据”是指甲方注册云账户时提供的注册资料及信息，以及甲方使用本服务时乙方系统自动接收并记录的甲方的浏览信息和行为轨迹，包括但不限于IP地址、浏览器的类型、使用的语言、访问日期和时间、软硬件特征信息及网页记录、安全信息，但不包括甲方使用本服务所存储的任何数据信息、以及云主机内的日志信息，另有约定除外。

6.2乙方承诺依据本合同6.1条获得的甲方的数据与乙方其他客户的数据互相隔离，不可互访。乙方数据中心遵守国家法律合法建设。甲方有权选择主数据的数据中心位置，有权选择备份数据与主数据不在同一个数据中心，但是无法选择备份数据的数据中心具体位置。甲方所有数据不会存储在境外数据中心。

6.3有下列情况之一时，乙方将依法全部或部分披露所收集的甲方数据信息：

6.3.1为确认甲方的真实身份，将甲方注册云账户时提供的注册信息及资料向第三方披露；

6.3.2经甲方事先同意，向第三方披露；

6.3.3根据法律的有关规定，或者行政或司法机构的要求，向第三方或者行政、司法机构披露；

6.3.4在甲方违反中国法律法规的情况下，依法向第三方披露；

6.3.5为提供甲方所要求的软件或服务，而必须和第三方分享信息。

6.4为服务之目的，乙方可能通过使用所收集的甲方信息，向甲方发出产品和服务信息等信息。甲方有权拒绝接受此类信息。

6.5乙方承诺甲方能够控制甲方使用本服务所存储数据的迁移，保证甲方在启用或弃用云主机时，可通过远程连接、FTP等应用进行数据迁入和迁出。如果数据量过大，乙方可代为迁入迁出，双方另行协商。

6.6 除相关法律法规规定或甲乙双方另行约定外，自本合同期满或因任何原因导致本合同提前终止后，甲方使用本服务所存储数据将被保留7日，7日后甲方该等数据将被彻底销毁。甲方应当自行承担其数据被销毁的一切后果。

**第七条知识产权条款**

7.1甲方使用本服务时，对于甲方自行提供并使用的软件，甲方应保证该等软件的合法性和不侵权。如任何第三方主张甲方所使用软件侵犯其所有权或者知识产权等合法权益，甲方应负责解决，并赔偿乙方就此而承担的一切费用和损失；同时，乙方有权视情况终止本服务的全部或部分内容。

7.2甲方使用本服务时，甲方应当保证所传输或存储的行为或内容的合法性和不侵权。如任何第三方主张甲方所传输或存储的行为或内容侵犯其所有权或者知识产权等合法权益，甲方应当负责解决，并赔偿乙方就此而承担的一切费用和损失；同时，乙方有权视情况终止本服务的全部或部分内容。

7.3甲方确认，乙方向甲方提供本服务所涉相关软件、资料、数据等的知识产权属于乙方或乙方具有许可/使用权；未经乙方同意，甲方无权复制、传播、转让、许可或提供他人使用这些资源，否则应承担相应的责任。对于乙方提供的操作系统等软件，甲方不得采取修改、翻译、改编、出租、转许可、在信息网络上传播或转让等方式，也不得逆向工程、反编译或试图以其他方式发现乙方提供的软件的源代码。

7.4乙方确认，甲方存放在乙方提供的云主机/服务器上的任何资料、软件、数据等的知识产权均不归属于乙方，未经甲方同意，乙方无权复制、传播、转让、许可或提供他人使用这些资源，否则应承担相应的责任。

7.5 乙方向甲方提供操作系统（如Windows、Linux等）等第三方软件的，乙方保证该等软件的提供和使用不违反知识产权相关法律规定要求。乙方并不是该等软件的技术提供或服务方，不承担由于该等软件所导致的一切技术问题及由此引发的责任或损失。

**第八条服务的变更、中断或终止**

8.1甲方同意遵守本合同以及乙方服务规则，并知悉乙方服务规则的内容可能会不时变更。如乙方服务规则任何内容发生变动，乙方应提前30日在服务门户的适当版面公告提示修改内容。若甲方不同意乙方所作修改，有权停止使用本服务，乙方将及时进行服务费用结算（如有），甲方应自行迁出使用本服务所存储数据。如果甲方继续使用本服务，则视为接受和同意遵守修改后的乙方服务规则。

8.2乙方因技术进步或国家法律、政策变动等原因可对本服务的服务内容、业务功能、操作方法等做出调整，但调整时应按本合同约定提前公告甲方并提供相应解决方案。

8.3如因系统维护或升级的需要而暂停本服务的，乙方将尽可能事先以公告方式通知甲方。

8.4乙方依据本合同约定暂停向甲方提供本服务的，应当通知甲方并告知暂停期间，暂停期间届满乙方应当及时恢复对甲方的服务。其中，非乙方原因造成的服务暂停，暂停期间甲方仍需正常付费。

8.5乙方依据本合同约定终止或解除本合同的，乙方有权立即终止提供服务并不退还任何款项（包括甲方尚未消费完毕的服务费用余额，本合同另有约定除外）。

**第九条违约责任**

9.1双方应共同遵守本合同条款及相应附件规定，如一方违约给对方造成损失的，违约方应赔偿守约方的损失。

9.2甲方使用本合同服务违反本合同约定的或在合同期内实施了任何违反国家法律法规行为的，乙方有权立即终止本合同，甲方应支付已使用未缴纳的费用，及未履行部分费用总额[100]%违约金；违约金不足以弥补损失的，甲方应当赔偿损失。

9.3如甲方逾期付费，除补交欠费之外，每逾期一日应按照所欠金额的[千分之三]支付违约金。逾期付费的，乙方有权暂停向甲方提供本服务直至终止本合同；同时，甲方还应承担乙方因追讨欠费支出的各项费用（包括但不限于律师费、诉讼费、保全费、财产保全担保费等）。

9.4 鉴于计算机、互联网的特殊性，下述情况不属于乙方违约：

9.4.1 乙方在进行服务器配置、维护时，需要短时间中断服务；

9.4.2 由于互联网通路阻塞或第三方原因造成甲方网站访问速度下降。

9.5如果因乙方自身及其控制范围内原因造成甲方不能按约定正常使用本服务的，包括云计算资源、云存储资源、云资源池互联网接入故障，甲方有权要求乙方进行赔偿。如果因乙方原因造成甲方连续72小时不能按约定正常使用服务的，甲方有权终止本服务，并要求乙方进行赔偿。

9.6本合同履行过程中，如甲方发生以下任一情形的，乙方有权视情节严重程度采取中止或终止履行合同、解除合同等措施并不承担违约责任。如该情形导致第三方向乙方提出法律或行政程序，甲方应负责解决。如该情形给乙方损失的，甲方应全额赔偿：

9.6.1被行政机关纳入“严重违法失信”名单；

9.6.2被人民法院纳入“失信被执行人”名单；

9.6.3被乙方（含乙方上级单位）纳入违规失信合作商名单；

9.6.4如存在网络和信息安全违法、违规行为的，包括但不限于因网络和信息安全问题承担刑事责任或受到行政处罚，被列入各级公安机关的涉通讯信息诈骗违法犯罪高危自然人或法人名单、业务经营不良名单、失信名单等;

9.6.5其他相关法律法规规定或有权机关认定的违法失信情形，以及可能导致合同履行风险或侵害乙方合法权益或声誉的违规失信情形。

9.7无论本合同其他条款是否有相反约定，乙方在本合同项下应承担的责任不超过乙方最近[壹]个月已经收取费用总额的[ ]%；乙方对因本合同项下违约行为而导致的甲方及其用户的可得利益损失、商业信誉损失以及数据丢失或损坏等其他损失不承担责任。

**第十条保密**

10.1未经对方书面许可，任何一方不得向第三方提供或者披露因本合同的签订和履行而得知的与对方业务有关的资料和信息，法律另有规定或本合同另有约定的除外。乙方向其关联公司提供或披露与甲方业务有关的资料和信息的，不受此限。

10.2本保密条款在服务期限内及服务终止后[ 5 ]年之内持续有效。

**第十一条不可抗力及免责**

11.1甲方了解乙方按照“现状”和“可得到”的状态向甲方提供本服务，并且乙方对本服务不作任何明示或暗示的保证，包括但不限于服务的适用性、没有错误或疏漏、持续性、准确性、可靠性、适用于某一特定用途。同时，乙方不对本服务所涉及的技术及信息的有效性、准确性、正确性、可靠性、质量、稳定、完整和及时性做出任何承诺和保证。但乙方应尽职尽责、诚实信用完成本服务。

11.2如由于战争、骚乱、恐怖主义、自然灾害、国家法律法规或规章变动、网络安全、网络无法覆盖、停电、通信线路被人为破坏、黑客攻击、计算机病毒侵入或发作等，导致甲乙双方或一方不能履行或不能完全履行本合同项下有关义务时，受影响方不承担违约责任，但应尽快书面通知对方。在影响消除后的合理时间内，一方或双方应当继续履行合同。如因此导致合同不能或者没有必要继续履行的，本合同可由一方解除。

11.3如政府管理部门提出要求的，乙方将暂停或终止提供相应服务，且不承担任何责任。

**第十二条法律适用和争议解决**

12.1本合同适用中华人民共和国法律。

12.2所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可将该争议提交所有因本合同引起的或与本合同有关的任何争议将通过各方友好协商解决。如果各方不能通过友好协商解决争议，则任何一方均可采取下述第（1）种争议解决方式：

（1）将争议提交[南宁]仲裁委员会，按照申请仲裁时该会的仲裁规则进行仲裁。仲裁在[南宁]进行。仲裁语言为中文。仲裁裁决是终局的，对双方均有约束力。仲裁费用由败诉方承担。

（2）向[ ]有管辖权的人民法院起诉。

12.3仲裁或诉讼进行过程中，双方将继续履行本合同未涉仲裁或诉讼的其他部分。

**第十三条服务期限**

13.1本合同确定的服务期限为[ ]个月，自服务实际开通之日起计算。

13.2除非任何一方在服务期届满前九十日书面通知另一方不再续展，否则服务期将自动续展，续展的服务期与本合同服务期相同，续展次数不受限制。除非双方另有约定，否则本合同内容对于续展期仍有约束力。

**第十四条合同生效及其他**

14.1本合同自[ ] 年[ ]月[ ]日起至[ ] 年[ ]月[ ]日止。

14.2本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

14.3本合同与乙方服务规则具有同等法律效力。如有冲突，以乙方服务规则为准。

14.4如果本合同的任何条款在任何时候被确定为不合法、无效或不可强制执行时，本合同的其他条款的效力和履行应不受影响。

14.5未得到对方的书面许可，一方均不得以广告或在公共场合使用或摹仿对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写，任何一方均不得声称对对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写拥有所有权。

14.6本合同的任何内容不应被视为或解释为双方之间具有合资、合伙、代理关系。

14.7本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、协议和合同等法律文件。

14.8本合同各条标题仅为提示之用，应以条文内容确定各方的权利义务。

14.9甲乙双方因履行本合同或与本合同有关的一切通知都必须按照本合同中的地址，以书面信函或者传真或者电子邮件或服务门户等方式进行。其中：

14.9.1除本合同另有约定外，有关下述任一事项的通知，均应当采用书面信函形式作出，否则，该通知无效，不产生本合同项下的任何通知效力：

（1）与本合同费用及支付事宜有关的通知；

（2）与本合同违约事宜有关的通知；

（3）与本合同终止、解除或变更事宜有关的通知；

（4）与本合同延续/续展有关的通知；

14.9.2本合同约定的各种通知方式的送达标准如下：

（1）如采用书面信函形式，应当使用挂号信或者具有良好信誉的特快专递送达，接受方签收挂号信或特快专递的时间（以邮局或快递公司系统记录为准）为通知送达时间；

（2）如采用传真方式，传真到达接受方指定传真系统的时间为通知送达时间；

（3）如采用电子邮件方式，电子邮件到达接受方指定电子邮箱的时间为通知送达时间。

（4）如通过服务门户发布公告或通知的，公告或通知的发布时间即为送达时间，除非公告或通知对送达时间另有规定。

如果因接受方原因（包括但不限于接受方拒收书面信函、接受方传真机关闭或故障、接受方电子邮箱地址不存在或者邮箱已满或者设置拒收等）导致通知发送失败，视为通知已经送达（发送方侧载明的书面信函寄出时间或者传真发送时间或者电子邮件发送时间视为通知送达时间）。

14.9.3本合同双方通知地址及方式如下：

甲方：

 地 址：

 联系人：

 电 话：

 传 真：

邮 编：

电子邮件：

乙方：

 地 址：

 联系人：

 电 话：

 传 真：

邮 编：

 电子邮件：

上述任何信息发生变更的，变更方应及时以书面形式通知另一方，未及时通知并影响本合同履行或造成损失的，应承担相应的责任。

14.10双方同意，附件为本合同不可分割的部分，若附件与合同正文有任何冲突，以合同正文为准。

本合同附件为：

附件一 产品需求单

**补充附页**

经友好协商，对本合同条款补充、修改如下，本补充附页为合同正文的一部分，与合同正文冲突时，以本补充附页为准：[无]

甲方：[ ]

法定代表人/负责人

或授权代表：

[ ]年[ ]月[ ]日

乙方：

法定代表人/负责人

或授权代表：

[ ]年[ ]月[ ]日

**附件一**

**产品需求单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 产品名称 | 配置 | 数量 | 单价（元/年） | 备注 |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |

**附件I：**

**合同验收报告（格式）**

 根据采购合同（采购合同编号：­   ）的约定，我单位对（采购项目名称） 采购项目 分标中标（或成交）供应商 （公司名称） 提供的货物（或服务）进行了验收，验收情况如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名  称 | 货物型号规格、标准及配置（或服务内容、标准） | 数量 | 金额 | 与合同约定是否一致 |
|  |   |   |   |   |  |
|  |   |   |   |   |  |
|  |  |  |  |  |  |
| 合 计 |  |  |  |
| 合 计 大 写 金 额 ：人民币 元 |
| 实际供货日期 |  | 合同交货验收日期 |  |
|  |  |  |  |
| 验收具体内容 |  (应按采购合同、采购文件、投标响应文件及验收方案等进行验收；并核对中标或成交供应商在安装调试等方面是否违反合同约定或服务规范要求、提供的质量保证证明材料是否齐全、应有的配件及附件是否达到合同约定等。可附件) |
| 验收小组意见 | 验收结论性意见： |
| 有异议的意见和说明理由： |
| 验收小组成员签字： |
| 参与验收其他或监督人员签字： |
| 中标（或成交）供应商签字或盖章：联系电话：          年  月  日 | 采购人的意见（盖章）：联系电话： 年  月  日 |

备注：本报告单一式三份（采购人1份、中标人1份、采购代理机构1份）。