岳普湖县维吾尔医医院信息化安全服务能力提升项目合同

项目名称：[岳普湖县维吾尔医医院信息化安全服务能力提升项目合同]

委托方(甲方)：岳普湖县维吾尔医医院

受托方(乙方)：中国电信股份有限公司喀什分公司

中华人民共和国科学技术部印制

填写说明

一、本合同为中华人民共和国科学技术部印制的技术服务合同示范文本，各技术合同登记机构可推介技术合同当事人参照使用。

二、本合同适用于一方当事人（受托方）以技术知识为另一方（委托方）解决特定技术问题所订立的合同。

三、签约一方为多个当事人的，可按各自在合同关系中的作用等，在“委托方”、“受托方”项下（增页）分别排列为共同委托人或共同受托人。

四、本合同未尽事项，可由当事人附页另行约定补充协议，并作为本合同的组成部分。

五、当事人使用本合同时约定无需填写的条款，应当在该条款处注明“无”等字样。

六、如有必要，可另行签订保密协议。

岳普湖县维吾尔医医院信息化安全服务能力提升项目合同

委托方（甲方）：[岳普湖县维吾尔医医院]

地址：[岳普湖县艾吾再力库木西路6号院]

法定代表人/负责人：[阿不都热合曼·巴拉提]

项目联系人：[李瑞倩]

通讯地址：[新疆喀什地区]

电　　话：[17793646994]

传　　真：[\ ]

电子邮箱：[\ ]

受托方（乙方）：中国电信股份有限公司喀什分公司

地址：[新疆喀什地区喀什市人民东路356号]

法定代表人/负责人：[杨益]

项目联系人：[姬文斌]

通讯地址：[新疆喀什地区]

电　　话：[19990903444]

传　　真：[\ ]

电子邮箱：[19990903444@189.cn]

本合同甲方委托乙方就[岳普湖县维吾尔医医院信息化安全服务能力提升项目合同]项目（“项目”）进行专项技术服务，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》以及相关法律法规的规定，达成如下合同，并由双方共同恪守。

第一条技术服务内容

1.1 技术服务的目标：[客户满意]。

1.2 技术服务的内容：[附件1]。

1.3 技术服务的方式：[技术服务]。

第二条技术服务时间和地点

2.1 技术服务地点：[岳普湖县]。

2.2 技术服务期限：[1年]。

第三条甲方提供的工作条件和协作事项

3.1 提供技术资料：[\ ]。

3.2 提供工作条件：[\ ]。

3.3 其他配合协作事项：[\ ]。

3.4 甲方提供上述技术资料、工作条件和配合协作事项的时间及方式：[\ ]。

第四条合同费用

4.13.1 本合同总价（含税价）：集成技术服务,大写人民币[壹佰零柒万贰仟捌佰元]，¥[1072800.00]；其中价款为大写人民币[壹佰零壹万贰仟零 柒拾伍元肆角柒分]，¥[1012075.47]元，增值税款为大写人民币[陆万零柒佰贰拾肆元伍角叁分]，¥[60724.53]元,税率为6%。

4.2 合同总费用由甲方按照以下第（2）种方式向乙方支付：

（1）一次性支付

验收合格后[10]个工作日内，甲方向乙方支付本合同费用。

（2）分期支付

甲方分期向乙方支付本合同费用：[第一批次支付本合同金额的30%，第二批次支付本合同剩余50%，第三批次支付本合同剩余的20%]。

4.3 甲乙双方银行账户信息和纳税人信息

甲方信息如下：

开户行：[岳普湖县维吾尔医院]

银行地址：[岳普湖县艾吾再力库木西路6号院]

户名：[岳普湖县维吾尔医院]

账号：[866101000120110001330l]

统一社会信用代码：[653128004030]

地址：[岳普湖县艾吾再力库木西路6号院]

电话：[17793646994]

乙方信息如下：

开户行：[中国农业银行股份有限公司喀什分行]

银行地址：[ ]

户名：[中国农业银行股份有限公司喀什岳普湖分公司]

账号：[30-475101040004105-0000000003]

统一社会信用代码：[916531007611404119]

地址：[新疆喀什地区喀什市人民东路356号]

电话：[19990903444]

4.3 若甲方存在欠费情况的，不论乙方开具发票和收费通知单的具体时间，乙方每次收到甲方付款按照甲方欠费的先后顺序自动抵充先到期的欠费，直至抵缴完毕。

第五条保密

5.1 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、法规、规章或监管要求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。

5.2 本保密条款在服务期限内及服务终止后二年之内持续有效。

第六条 本合同的变更应当由双方协商一致，并以书面形式确定。但有下列情形之一的，一方可以向另一方提出变更合同权利与义务的书面请求，另一方应当在收到书面请求后[\ ]个工作日内予以答复；逾期未予答复的，视为同意：

[ ]。

第七条验收

7.1 乙方完成技术服务工作的形式：[\ ]。

7.2 技术服务工作成果的验收标准：[合格]。

7.3 技术服务工作成果的验收方法：[\ ]。

7.4 验收的时间和地点：[岳普湖县]。

第八条侵权处理

8.1 如本合同以外的第三方指控乙方为甲方提供服务和/或其为甲方提供的服务成果侵犯该方的专利或著作权，乙方自费就上述指控自行和/或与甲方共同辩护，并支付法院和行政执法机关最终裁定的或经乙方同意的和解中包括的一切费用、损害赔偿金和合理的律师费用，前提条件是甲方：

（1）就指控立即书面通知乙方。

（2）容许乙方在辩护及任何有关的和解谈判中具有控制权，并配合乙方工作。

在满足上述条件的前提下，乙方就侵权指控对甲方承担本条约定的上述义务。

8.2 对因下列任何一项所引起的指控，无论本合同是否有其他约定，乙方均不承担责任：

（1）甲方提供的被并入服务成果之中的任何东西，或乙方遵照甲方或代表甲方的第三方所提供的任何设计、规格或关于实施方法的指示而提供的任何东西。

（2）甲方修改服务成果。

（3）甲方将服务成果与非由乙方提供的任何产品、数据、装置或商业方法一起结合、操作或使用，或为甲方以外的第三方的利益发行、操作或使用服务成果。

第九条个人信息保护和数据安全

为履行本合同，甲方委托乙方处理相关数据和个人信息的，双方同意按照本条约定执行：

9.1个人信息种类：[\ ]；乙方处理数据和个人信息的期限为：[\ ]；处理方式为：[\ ] 以及本合同约定的其他处理方式。

9.2甲方保证，其委托乙方处理个人信息已经向个人信息主体履行了法定告知义务，并取得了其同意。甲方保证，其委托乙方处理的个人信息和数据来源合法合规，不存在违反法律法规、监管要求的情况。

9.3 双方均应当严格按照相关法律法规规定，采取措施确保个人信息处理活动符合法律、行政法规的规定，防止未经授权的访问以及个人信息和数据的泄露、篡改、丢失。

9.4乙方有权对甲方提供的个人信息和数据来源合法合规性情况进行检查。对于乙方检查发现甲方个人信息和数据来源违反法律法规、监管要求，或者就其向乙方提供的个人信息未依法向个人履行法定告知义务、未取得个人同意，乙方有权要求甲方在一定期限内整改。如果甲方未按照乙方要求整改或整改未达到乙方的相关要求，乙方有权解除合同，且不承担赔偿责任；由此给乙方造成损失的，甲方应当全额赔偿。

9.5 甲方违反本合同及其附件个人信息保护和数据安全相关条款和相关法律法规、监管要求的，甲方应当承担一切民事、行政和刑事责任，如因此给个人信息主体、乙方或其他人造成任何损失的，甲方应当承担全部责任

第十条 履约责任

10.1甲方承诺遵守国家相关法律法规，不进行危害网络安全的活动，若乙方发现甲方有危害网络安全的事项等活动，乙方有权停止技术支持，并解除本合同不负违约责任，本合同项下所有款项不予退还。

10.2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，甲方应当负责解决。如该情形给乙方造成损失的，甲方应当全额赔偿：

（1）被行政机关纳入“严重违法失信”名单；

（2）被人民法院纳入“失信被执行人”名单；

（3）被乙方（含乙方上级单位）纳入违规失信合作商名单；

（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、电信业务经营不良名单、失信名单等；

（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。

第十一条 双方确定，在本合同有效期内，甲方指定[李瑞倩]为甲方项目联系人，乙方指定[姬文斌]为乙方项目联系人。

一方变更项目联系人的，应当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，应当承担相应的责任。

第十二条 双方确定，出现下列情形之一，致使本合同的履行成为不必要或不可能的，可以解除本合同：

12.1 发生不可抗力。

12.2[\ ]。

第十三条法律适用和争议解决

13.1 本合同适用中华人民共和国法律。

13.2 所有因本合同引起的或与本合同有关的任何争议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，则任何一方均可向[乙方住所地]有管辖权的人民法院起诉。

13.3 诉讼进行过程中，双方继续履行本合同未涉诉讼的其它部分。

第十四条不可抗力及免责

14.1 如由于战争、骚乱、恐怖主义、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、突发事件等，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，但应当尽快书面通知对方。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。

14.2 如乙方根据政府管理部门要求暂停或终止提供相应服务，乙方不承担任何责任。

第十五条合同生效和其他

15.1 本合同纸质文本一式四份，甲乙双方各执二份，自双方签字盖章之日起生效；若使用电子印章的，自双方盖章之日起生效。

若乙方加盖电子印章的，以加盖乙方电子印章的本合同电子文档所载内容为准。

15.2 如果本合同的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本合同的效力时，本合同的其他条款不受影响。

15.3 本合同各条标题仅为提示之用，应当以条文内容确定各方的权利义务。

15.4 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。

15.5 本合同的任何内容不应当被视为或解释为双方之间具有合资、合伙关系。

15.6 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、合同和协议等法律文件。

15.7 甲乙双方因履行本合同或与本合同有关的一切通知都应当按照本合同中的地址，

以书面信函或者传真或者电子邮件方式进行。其中：

15.7.1 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；

14.7.2 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。

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）。

15.7.3 本合同双方通知地址及方式如下：

甲方：[岳普湖县维吾尔医医院]

地址：[岳普湖县文化南路10号院]

联系人：[李瑞倩]

电话：[17793646994]

传真：[\ ]

邮编：[844400]

电子邮箱：[\ ]

乙方：中国电信股份有限公司喀什分公司

地址：[新疆喀什地区喀什市人民东路356号]

联系人：[姬文斌]

电话：[19990903444]

传真：[\ ]

邮编：[844400]

电子邮箱：[\ ]

上述任何信息发生变更的，变更方应当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，应当承担相应的责任。

15.8 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：网络及信息安全承诺书

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：[附件1]服务内容

（本页无正文）

甲方：[岳普湖县维吾尔医医院]

法定代表人/负责人

或授权代表：

乙方：中国电信股份有限公司喀什分公司

法定代表人/负责人

或授权代表：

签署日期：[ ]年[ ]月[ ]日

印花税票粘贴处：

（以下由技术合同登记机构填写）

合同登记编号：

1. 申请登记人：
2. 登记材料：(1)
   (2)
   (3)
3. 合同类型：
4. 合同交易额：
5. 技术交易额：

技术合同登记机构：（盖章）
经办人：
年　月　日

附件

网络及信息安全承诺书

中国电信[　　]公司：

本单位郑重承诺遵守本承诺书，如有违反本承诺书有关条款的行为，本单位承担由此带来的一切责任。

一、本单位承诺遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国电信条例》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《互联网信息服务管理办法》《非经营性互联网信息服务备案管理办法》《移动互联网应用程序信息服务管理规定》《网络信息内容生态治理规定》《电信和互联网用户个人信息保护规定》《公共互联网网络安全突发事件应急预案》《关键信息基础设施安全保护条例》和《网络安全审查办法》及有关法律、法规、规章和政策文件规定（“相关规定”）。

二、本单位承诺按照相关规定、政府主管部门要求以及合同/协议（“合同”）约定规范使用业务，不得超出合同约定的范围和用途使用业务，不将业务用于连接境内外的数据中心或业务平台开展电信业务经营活动，具备所从事业务的全部合法必要的资质条件。

三、本单位承诺按照用户真实身份信息制度（“实名制”）的要求提供身份信息、使用业务，并保证所提供信息、资料的真实、完整、准确、有效。

四、本单位承诺用户端接入设备与合同约定的一致，并同意贵公司对设备拍照存档，若接入设备变更，本单位应当及时书面告知贵公司。

五、本单位保证不利用网络（包括但不限于固定网、移动网、互联网，下同）从事危害国家安全、泄露国家秘密等违法犯罪活动，不侵犯他人的合法权益。

六、本单位承诺在处理个人信息前，已依法向个人信息主体（“个人”）履行了法定告知义务并取得个人的明确同意。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，本单位在处理个人信息前依法取得个人单独同意或书面同意。

七、本单位向贵公司提供个人信息或委托贵公司处理个人信息的，本单位承诺已依法向个人履行了告知义务，并依法取得了个人同意。本单位承诺，向贵公司提供或委托贵公司处理的个人信息和数据来源合法合规，不存在违反相关规定以及合同约定的情况。

八、本单位受贵公司委托处理个人信息等数据的，或本单位与贵公司共同处理个人信息等数据的，本单位承诺按照与贵公司的合同约定处理，不得超出约定的处理目的、处理方式等处理上述数据，严格遵循数据处理时限。

九、本单位承诺严格按照相关规定做好本单位网络安全、数据安全和个人信息保护管理工作，健全各项网络安全、数据安全和个人信息保护管理制度和操作规程，落实各项安全保护技术措施，实施个人信息和数据安全分级分类管理、依法落实个人信息保护影响评估和数据安全影响评估安全风险评估、报告、信息共享、监测预警机制，定期对从业人员进行安全教育和培训，依法设置网络安全、数据安全和个人信息保护责任人和管理机构，按政府主管部门要求设立信息安全责任人和信息安全审查员，当信息安全责任人发生变更时及时通知贵公司。否则，导致的一切后果由本单位承担，贵公司有权立即终止合同。

十、本单位承诺配合贵公司为公安机关、国家安全机关、网信部门等政府部门依法履行职责、维护国家安全和侦查犯罪等活动提供协助，如实提供有关安全保护的信息、资料

及数据文件，积极协助查处信息网络违法犯罪行为。

十一、本单位承诺利用网络发送的信息以及向贵公司提供的信息真实、准确、合法。该等信息内容内容应当严格符合相关规定，不通过网络制作、复制、查阅和传播有害信息，本单位不得通过通信网络、互联网散发传播违法、不健康、反动等信息，不得制作、复制、查阅和传播任何含有违反下列要求（即“九不准”及“六不许”）的信息：

“九不准”，即不准制作、复制、查阅和传播含有以下内容的信息：

1、反对宪法所确定的基本原则的；

2、危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

3、损害国家荣誉和利益的；

4、煽动民族仇恨、民族歧视，破坏民族团结的；

5、破坏国家宗教政策，宣扬邪教和封建迷信的；

6、散布谣言，扰乱社会秩序，破坏社会稳定的；

7、散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

8、侮辱或者诽谤他人，侵害他人合法权益的；

9、含有法律法规禁止的其他内容的。

“六不许”，即：

1、决不允许在群众中散布违背党的理论和路线方针政策的意见；

2、决不允许公开发表同中央的决定相违背的言论；

3、决不允许对中央的决策部署阳奉阴违；

4、决不允许编造、传播政治谣言及丑化党和国家形象的言论；

5、决不允许以任何形式泄露党和国家的秘密；

6、决不允许参与各种非法组织和非法活动。

十二、本单位承诺不通过网络从事危害中华人民共和国安全、泄露中华人民共和国国家秘密等活动，不从事任何危害网络安全、数据安全的活动，不从事侵犯他人合法权益的活动，包括但不限于：

1、未经允许进入网络或者使用网络资源；

2、未经允许对网络功能进行删除、修改或者增加；

3、未经允许对网络中存储或者传输的数据和应用程序进行删除、修改或者增加；

4、制作、传播、利用网络病毒等恶意程序或破坏性程序；

5、非法收集、使用、加工、传输或以其他方式处理个人信息等数据；

6、非法买卖、提供或者公开个人信息等数据；

7、从事危害国家安全、公共利益的个人信息和数据处理活动；

8、其他危害网络安全、数据安全、侵犯他人合法权益的活动。

十三、本单位使用语音接入类业务的（包括但不限于语音专线、短号码接入、400号码接入等），承诺遵守以下规定：

（一）使用业务的时段为[ ]，使用的频次为[ ]，业务外呼呼转功能默认为关闭。

（二）遵守实名制要求，不以个人名义申请、使用业务，真实落地目的码为本单位实名办理或合规使用的电话号码。

（三）不转租、转售业务，否则，贵公司有权在不通知本单位的情况下立即终止合同。

（四）规范使用业务，进行外呼业务的号码为贵公司或通信主管部门分配的号码，严格按照通信主管部门关于号码传送及信令传送的相关要求传送号码，传送真实号码，不擅自更改、传送、显示非合同约定的号码、虚假号码、违规号码、无使用权号码，不隐藏、

转让、变更、转租、转售、伪造、变造或者变相隐藏、转让、变更、转租、转售、伪造、变造号码。本单位承诺按要求提供所申请号码的使用用途、开放范围，不违规经营、不变更合同约定的使用用途，不开展无特定主被叫的话务批发业务，不私自转接国际来话，不通过技术手段为非法 VoIP、改号电话、网络电话（PC 软件/APP 等）提供语音落地，不采取自动语音群呼方式进行外呼。如违反上述承诺，贵公司有权在不通知本单位的情况下立即单方终止合同，所造成的一切后果由本单位承担。

（五）不通过任何技术手段将号码转接到其他地区使用，不通过 VOIP 转接互联网话务量，不使用业务进行多次转接、躲避号码溯源与甄别，呼叫中心或接入平台（小交换机）不使用异地主叫号码进行跨省外呼，不利用号码和平台进行电话诈骗、骚扰。诈骗或骚扰包括但不限于以下情形：

1、政府主管部门认定号码涉嫌诈骗或其他刑事案件的；

2、“12321 网络不良与垃圾信息举报受理中心”接到的用户投诉、举报涉及本单位所使用号码的；

3、贵公司或通信主管部门电话拨测、网络信令监测过程中发现本单位所使用号码出现异常外呼情况的。

（六）建立有效的信息安全管理制度和技术保障措施，确保备份呼叫内容录音文件，并接受政府主管部门及贵公司的管理、监督和检查，为相关主管部门提供技术支持。如相关规定、政府主管部门对信息安全管理有新要求，本单位将无条件配合贵公司落实整改举措，直至符合相关规定、政府主管部门的要求。

十四、本单位使用无线互联网（包括但不限于 CDMA1X、CDMA1X EVDO、WLAN）、短信网关（包括但不限于短消息资讯平台、ISAG 系统、综合办公业务平台）或短信类业务的，承诺遵守以下规定：

（一）不通过业务制作、复制、查阅和传播悖于社会公德、损害青少年身心健康的网络低俗内容，包括但不限于：

1、表现或隐晦表现性行为、令人产生性联想、具有挑逗性或者污辱性的内容；

2、对人体性部位的直接暴露和描写；

3、对性行为、性过程、性方式的描述或者带有性暗示、性挑逗的语言；

4、对性部位描述、暴露，或者只用很小遮盖物的内容；

5、全身或者隐私部位未着衣物，仅用肢体掩盖隐私部位的内容；

6、带有侵犯个人隐私性质的走光、偷拍、漏点等内容；

7、以挑逗性标题吸引点击的；

8、相关部门禁止传播的色情、低俗小说，音视频内容，包括一些电影的删节片断；

9、一夜情、换妻、SM 等不正当交友信息；

10、情色动漫；

11、宣扬血腥暴力、恶意谩骂、侮辱他人等内容；

12、非法的性用品广告和性病治疗广告；

13、未经他人允许或利用“人肉搜索”恶意传播他人隐私信息。

（二）不开展为淫秽色情网站代收费业务，否则，贵公司有权立即停止业务并停止一切结算。

（三）未经用户同意，不得向用户发送商业类电子信息或广告。

十五、本单位使用互联网接入类业务的（包括但不限于电路使用、互联网数据中心、互联网专线、云主机等），承诺遵守以下规定：

（一）具备从事互联网服务的全部合法必要的资质条件，已履行相关规定要求的手续或已取得有关资质证明文件。在签署合同前，本单位向贵公司提供主体资格文件、资质证明文件的原件供贵公司审核，复印件（加盖公章）供贵公司留存，并保证所提供资料的真实、完整、准确、有效。在合同有效期/服务期内，如本单位提交的主体资格、资质证明文件所记载内容出现变更，本单位在完成变更后尽快向贵公司提供最新的文件。前述主体资格文件、资质证明文件包括但不限于营业执照、增值电信业务经营许可证、广告经营许可证、非经营性互联网信息服务备案证明以及贵公司要求提交的其他文件。其中：

1、本单位如从事电子公告、新闻、出版、教育、医疗保健、药品和医疗器械、文化、广播电影电视节目等特殊互联网信息服务，应当根据相关规定经政府主管部门审核同意，履行批准或备案手续，并取得通信主管部门批准或备案文件。

2、本单位如从事非经营性互联网信息服务，应当首先履行互联网备案手续，并按期履行年度审核手续。本单位委托贵公司提供代备案服务的，应当向贵公司提供代备案所需信息并对该等信息进行动态维护和更新，定期向贵公司及通信主管部门报送网站管理所需信息。本单位承诺所提交的所有备案信息真实、完整、准确、有效，当备案信息发生变化时及时在备案系统中更新，如因未及时更新而导致备案信息不准确，贵公司有权依法采取暂停或终止提供服务、断开网络接入等关闭处理措施。

3、本单位如从事经营性互联网服务，应当取得相应的增值电信业务经营许可证。

4、本单位如从事经营性互联网服务，应当在其网站主页的显著位置标明其经营许可证编号；本单位如从事非经营性互联网服务，本单位网站开通时在主页底部的中央位置标明其备案编号，并在备案编号下方链接工业和信息化部备案管理系统网址，供社会公众查询核对；本单位按照工业和信息化部备案管理系统的要求，将备案电子验证标识放置在其网站的指定目录下。

（二）如经贵公司许可进入中国电信机房时，应当严格遵守机房的各项管理规定。

（三）根据当地公安局网监分局的要求，在入网后5个工作日内在网上提交备案信息，提交信息后10个工作日内办理备案。

十六、本单位承诺在业务使用过程中发生重大安全事故或发生或者可能发生个人信息等数据泄露、篡改、丢失时，立即采取应急措施，保留有关原始记录，在24小时内向有关部门报告并书面通知贵公司。如发生重大安全事故或其他影响网络安全、数据安全和个人信息保护的突发事件，贵公司有权采取包括但不限于停止业务等紧急措施，以保证网络安全、数据安全和保护个人信息。

十七、本单位如出现任何违反上述承诺的情况，将依据合同承担责任，接受有关政府主管部门的处理（包括但不限于限期整改、公开曝光），并直接承担相应法律责任，造成财产损失的，由本单位直接赔偿。同时，贵单位有权在不通知本单位的情况下暂停履行合同直至解除合同并不承担任何责任，一切责任后果全部由本单位自行承担。给贵公司造成损失或不良影响的，本单位将负责消除不良影响并赔偿贵公司相应损失。

十八、如出现任何违反上述承诺的情况引发的投诉、举报，由本单位负责解决并承担责任。当接到通信主管部门、“12321网络不良与垃圾信息举报受理中心”、中国电信10000热线等各类渠道投诉、举报时，贵公司有权在不通知本单位的情况下立即终止合同并不承担任何责任，一切责任后果全部由本单位自行承担。给贵公司造成损失或不良影响的，本单位负责消除不良影响并赔偿贵公司相应损失。

十九、本单位的信息安全责任人如下：

姓名：[阿卜拉·阿木提]

职务：[信息科副主任]

联系方式：[19190047199]

二十、本单位承诺与最终用户参照签订此类《网络及信息安全承诺书》，并督促最终用户履行相应责任。否则，本单位承担连带责任。

二十一、本承诺书经本单位签署后，与合同同时生效。

承诺单位（盖章）：[ ]

法定代表人（负责人）

或授权代表（签字）：

附件 1　项目服务内容

一、服务期：一年（具体要求以合同约定为准）

序号	服务名称	服务功能描述	数量
1	核心防火墙服务	1.提供 1 年功能服务（IPS特征库、病毒库、威胁情报、应用识别库、垃圾邮件库、网页分类库升级服务授权）。 2.★三层网络吞吐≥20Gbps，IPS吞吐量≥1.6Gbps，最大并发连接≥150 万，最大新建连接≥5.6 万；IPSEC VPN 隧道数≥2500；SSL VPN 并发用户数≥500， 3.支持 SD-WAN功能，支持基于用户、用户组的SD-WAN策略，包括多种带宽接入、带宽质量监控、链路优化、一键配置上线等　4.支持策略路由、组播路由、静态路由、BGP、RIP、RIPNG、OSPF、OSPFv6、ISIS、ISISv6等动态路由协议（非透传）； 5.内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户/用户组、应用、URL 类型、接入类型、地理位置、终端类型、设备组、服务、时间、安全引擎（入侵、URL过滤、病毒过滤、沙箱过滤、SSL代理） 的识别与控制。 6.为保障语音系统效果，支持 VoIP 防护，可基于SIP与SCCP协议防护，可限制SIP的注册请求，可限制SCCP的呼叫建立。 7.支持自定义 IPS特征，提供相关配置功能截图证明。 8.具备 11000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、严重程度、特征名称、应用类型等方式的查询 9.支持 IPSec VPN、SSL VPN 、L2TP VPN、GRE VPN、L2TP over IPSec VPN、GRE over IPSec VPN等VPN组网 10.★IPSec VPN支持阶段二下的DH组的秘钥交换方式，支持DH group 21、27、28、29、30、31 的类型，提供功能截图证明； 11.支持对文件类型过滤，至少基于包括doc、docx、exe、ppt、pptx、rar、txt、xls、xlsx、pdf、zip、gzip、tar等40种以上文件类型过滤 12.支持与云沙箱进行联动，动态分析恶意软件、恶意文件以及威胁URL； 13.支持WAF功能，具备HTTP特征库规则列表，至少包括SQL注入、XSS防护，支持HTTP报头的长度、cookie的个数等参数限制策略对Web服务器进行安全防护 14.支持0-day恶意软件变种、可疑文件等APT高级可持续威胁的统计功能	1

2	入侵检测防御服务	1. 提供一年入侵防御检测服务，三层网络吞吐≥20Gbps，最大并发连接≥100万，最大新建连接≥2万。 2. 支持路由模式、透明（网桥模式）、混合模式； 3. 为保障不同业务不同安全策略，要求支持单独为每个虚拟入侵检测防御系统设置会话数、策略数、用户数、硬盘空间使用量等，进行按需分配。 4 支持态势感知大屏展示，综合展示攻击风险情况 5 支持策略路由、静态路由协议（非透传）； 6 支持802.1Q Trunk，支持不同VLAN之间的数据隔离。 7.★内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户/用户组、应用、URL类型、设备组、服务、时间、安全引擎（入侵、URL过滤、病毒过滤、SSL代理）的识别与控制。提供产品功能界面截图证明。 8. 支持SYN Flood、UDP Flood、ICMP Flood、等攻击防护； 9. 支持对HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、MSSQL、ORACLE、NNTP、DHCP、LDAP、VoIP、NETBIOS、TFTP、SUNRPC和MSRPC等常用协议及应用的攻击检测和防御 10. 支持旁路和串联两种模式 11. 支持自定义IPS特征，并提供相关配置截图和指导文档有效 12. 具备13000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、严重程度、特征名称、应用类型等方式的查询 13. 支持对HTTP、FTP、SMTP、POP3、IMAP协议的应用进行病毒扫描和过滤 14. 支持对VPN传输隧道内容进行病毒过滤； 15. 支持对2000种以上应用的识别和控制 16. 为了支持业务扩展，要求支持IPv4/IPv6双栈 24. IPv6协议栈：TCP6、UDP6、ICMPv6、PathMTU、ACL6等；	1

3	上网行为管理服务	1.要求提供上网行为管理服务1年，并发在线用户数不低于1000，个功能在内不低于1G。 2.支持静态路由、RIPv1/v2、RIPng、OSPFv2等多种路由协议 3.为保证在多条外网线路情况下能够合理分配使用，设备必须支持多链路负载均衡，负载均衡可基于带宽等多种方式 4.应用路由效果可通过图表呈现；支持智能DNS，无需内部服务器做任何修改情况下，为外网用户提供一个与该用户相同运营商的链路对内访问； 5.★支持IP地址智能管理图形界面显示，可显示固态在线IP、固态离线IP、动态分配IP、接口IP、排除IP、冲突IP无需安装任何客户端、支持IP地址绑定，可单MAC绑定、IP+主机名绑定、IP+MAC绑定、IP+MAC+主机名绑定、IP+主机名+接入设备绑定、IP+MAC+主机名+接入设备绑定，进而实现DHCP无感知准入控制；提供产品功能截图证明，非加盖厂商公章或投标专用章。 6.支持终端迁移告警，可显示迁移终端IP及MAC，终端迁移时间，迁移前后接入设备IP及MAC，迁移前后VLAN及端口；本地认证支持微信认证、短信认证、二维码授权认证、二维码自助认证、LADP认证，支持与域认证联动实现单点登陆 7.支持流量识别保障功能：能够精确识别网络应用，保障关键业务的系统带宽，具备完善的应用协议库，协议识别数量≥2500种。 8.★产品内置多种流控模型，包括娱乐模版、办公模版、专家模板等，支持一键开启智能流量控制；提供设备功能截图证明。	1

		9.★支持VPN内流量的可视化监控；支持VPN内流量控制，提供设备功能截图。 10.产品配置上网行为管理URL数据库、应用分类库、地址库、内容审计特征库三年升级服务授权，出具生产厂商盖章承诺函。 11.支持网络资源加速（主动缓存），可对指定网络资源提供热点资源本地化服务，网络资源加速（主动缓存）支持通过定时、实时、立即缓存等多种方式进行缓存同步。 12.★支持安全域：支持基于IP的安全域划分，支持基于逻辑接口的安全域划分，提供设备配置界面截图； 13.支持应用缓存加速（被动缓存），可将用户访问过的APP（IOS及Android）均缓存到本地，供其他访问相同APP的用户在本地下载，提高下载速度，应用缓存加速（被动缓存）支持精确缓存指定的APP，避免浪费本地存储空间。 14.支持状态检测防火墙，支持TCP/UDP/ICMP/IP分片包等报文过滤；提供设备配置界面截图； 15.支持入侵防御功能：支持SQL注入攻击、XSS注入攻击、webshell攻击、挖矿木马恶意样本通信、僵尸家族恶意样本通信（紫狐、双枪、独狼等）、APT32组织恶意样本通信、海莲花组织恶意样本通信、勒索病毒恶意样本通信等，提供设备功能界面截图证明； 16.★支持防攻击：支持防land攻击、防Teardrop攻击、防Smurf攻击、防异常TCP Flag攻击、防Ping of Death攻击、防SYN Flood攻击、防UDP Flood攻击、防ICMP Flood攻击、防Fraggle攻击、防超长ICMP报文攻击、防Winnuke攻击、防ARP Flood报文攻击等 17.为方便用户远程接入，设备需支持SSL VPN，并配置≥800路SSL VPN接入授权；支持IPSec VPN，并提配置≥800路Ipsec VPN接入授权 18.ipsec vpn建立完成后能够自动生成拓扑图，便于监控各级单位设备在线状态；支持WINDOWS、安卓、MAC、IOS操作系统SSL VPN客户端软件 19.支持防共享上网，支持一键防共享开关，发现共享后可以提供只检测、不允许上网、限速上网三种处理方式	
4	核心交换服务	1.要求提供核心交换服务1年，要求交换容量≥85Tbps，包转发率≥57600Mpps，以最小值为准，提供官方证明。 2.支持大容量硬件表项：MAC≥1M，FIB≥3M，ARP≥256K，投标时提供具有CMA或CAL或CNAS认证章的第三方权威机构检验报告证明 3.支持N:1虚拟化：可将2台物理设备虚拟化为1台逻辑设备，虚拟组内设备具备统一的二层及三层转发表项，统一的管理界面，并可实现跨设备链路聚合 4.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6，支持路由协议多实例，支持GR for OSPF/IS-IS/BGP，支持策略路由 5.支持CPU保护机制功能，可将送CPU的报文，如ARP报文的速率进行限制，使CPU的使用率降低到15%以内，保障了CPU安全，投标时提供具有CMA或CAL或CNAS认证章的第三方权威机构检验报告证明。，投标时提供具有CMA或CAL或CNAS认证章的第三方权威机构检验报告证明。 6.支持基础安全保护策略，可实现ARP、DHCP、ICMP、IP扫描、	1

		DHCP V6、ND等各种攻击的自动防御。可自定义抗攻击的报文类型，投标时提供具有CMA或CAL或CNAS认证章的第三方权威机构检验报告证明。 7.支持BFD功能故障检测周期≤3ms，检测到故障并切换到备份路由的断流时间≤30ms，投标时提供具有CMA或CAL或CNAS认证章的第三方权威机构检验报告证明 8★需支持OpenFlow 1.3协议，提供权威机构的检测证书以及权威机构官网证书查询链接和截图并加盖厂商公章或投标专用章 9.本次核心交换服务要求配置≥双独立主控引擎，≥双电源模块，≥48个万兆光接口，≥48个千兆电接口。	
5	web防护服务	1、提供WEB防护服务1年； 2、HTTP吞吐量≥1.5Gbps，支持通过软件授权最大扩展WEB吞吐≥5Gbps，最大并发数≥900000。 3、支持旁路镜像监测模式、旁路镜像阻断模式、透明代理模式、透明检测模式、反向代理模式、路由模式、DNAT转化模式、网关模式； 4、★支持定时下线功能，能根据日期、工作日、时间等多因素控制网站访问时效（要求提供产品截图） 5、应支持可以对网络进行SNAT、DNAT进行访问过滤限制 6、支持多条链路数据的防护，防护路数不做限制，上限为硬件性能瓶颈 7、★支持以域名和IP多种方式进行防护；提供功能截图并加盖原厂商公章或投标专用章。 8、支持服务器探测功能，提供对服务器进行在线探测（要求提供产品截图） 9、支持ipv4/ipv6双协议栈； 10、应能识别和阻断SQL注入攻击,Cookie注入攻击，命令注入攻击 11、★支持爬虫防护、扫描防护；提供功能截图并加盖原厂公章或投标专用章。 12、支持文件上传、下载过滤，支持LDAP、XPATH、struct2/xworks检测和防护；应能识别阻断跨站脚本(XSS)注入式攻击，应能识别和阻断应用层拒绝服务攻击 13、应能识别和阻断敏感信息泄露、恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、缓冲区溢出攻击； 支持黑链检测（要求提供产品截图） 14、★支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护（要求提供产品截图）” 15、支持敏感词防护，内置敏感词库并自定义敏感词库（要求提供产品截图） 16、支持会话安全，并可结合cookie加固及加密保护。 17、支持网站自学习建模，可通过学习URL、host等信息展示网站结构树形图，并支持对URL的访问量和响应健康度进行图形化统计 18、支持通过自学习的URL参数的长度、类型、范围及请求方法等数据特点创建黑白名单模型，如果参数违反模型则判断为非法流量，直接执行阻断或封禁动作。 19、能进行配置自动分发功能，能进行跨不同服务器的网页防篡改。	1

		20、★应至少同时支持Window、Linux（CentOS Redhat Debian Ubuntun）等操作系统的网页防篡改，提供功能截图并加盖原厂商公章或投标专用章。 21、支持检测并清洗的攻击类型包括但不限于：Land、Winnuke、Smurf等；TCP（SYN、SYN ACK、ACK、RST、FIN等）；UDP（各种端口扫描、Flood等）；ICMP（不可达、Flood等）；DNS Query Flood、HTTP GET Flood、HTTP Post Flood、CC等。 22、★支持利用威胁情报规则进行防护，并支持基于威胁情报的日志查询（提供配置界面及日志截图） 23、★支持通过移动终端管理，实现网站快速应急处置：支持网站批量离线、网站批量恢复、网站一键断网、网站一键恢复操作，提供功能截图并加盖原厂商公章或投标专用章。	
6	日志审计服务	1. 要求提供日志审计服务1年 2. 系统要求支持针对网络中各类安全产品、网络设备、服务器、中间件、数据库等产品进行日志收集和标准化； 3. 系统采用ElasticSearch、hadoop等开源数据存储、索引引擎，保证数据不被绑定，便于未来数据的二次应用 4. 采用B/S架构，无需安装客户端软件，支持个中文WEB管理界面，支持SSL加密模式访问 5. 支持syslog、文件、WMI、SNMPTrap、数据库等多种接入方式，目标机无需安装任何代理，提供产品功能界面截图 6. ★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（提供功能截图）； 7. ★支持主流厂商安全设备、服务器、网络设备、中间件等设备日志自识别接入；并支持非主流设备日志的自定义接入解析。提供产品功能界面截图，系统满足设备的日志信息采集要求。 8. ★支持为安全事件收集功能设置过滤条件，可过滤无关安全事件，满足根据实际业务需求减少对网络带宽和数据库存储空间地占用。提供产品功能界面截图 9. 支持对收集的大量的安全事件中相同的安全事件，进行归并处理，只需发送一条已统计次数的安全事件，减少重复日志量 10. 事件查看支持对系统接入的原始事件/日志进行集中呈现，可查询、查看、导出各类安全事件/日志； 11. 支持在事件列表中输入相关字段的查询条件；其中查询结果可以导出csv格式。 12. 包括报表内置实例管理，可自定义报表参数，选择需要的数据，提供报表任务管理 13. 支持安全知识库功能，系统内置对应安全事件等知识，并支持自定义创建增加知识 14. 支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果；日志员只负责完成对系统本身的用户操作日志管理。 15. ★支持自定义审计策略，提供可视化方式进行策略制定，支持从审计策略模板直接创建策略，提供产品功能截图证明。 16. 整体安全概况、安全资产管理、安全事件管理等" 17. 支持自定义仪表板，可以选择对应的组件，组成需要关注的仪表展现内容 18. 系统全面支持IPV6，包括安全事件接入等。	1

		19. 支持设置[illegible]备份[illegible]，系统能自动保存[illegible]、、数据使用[illegible]；	

		20. 支持日志文件备份到外部存储设备，包括 FTP NFS 等； 21. 支持系统配置修改图形化，如修改主机名、IP 地址等；	
7	数据库审计服务	1、要求配置数据库审计服务 1 年。 2、采用全操作系统，内嵌数据库，用户无需另外安装操作系统及数据库管理系统 3、性能指标：网络存吐量≥1G、SQL 峰值存吐处理能力≥100Mbps，sql 峰值事件处理能力≥5000SQL/秒，sql 入库速率≥5000 条/s，并发会话数≥100，日志存储≥6 亿，审计记录查询性能≥2000 万条/秒， 4、包括审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置 5、支持 Oracle、SQL Server、DB2、Informix、Sybase、MySQL、PostgreSQL、人大金仓、达梦、神州通用等数据库的审计，满足信息化系统数据库的安全审计需要 6、可支持同时审计多个不同类型的数据库，审计数据统一存储、查询、分析、统计 7、★支持函数审计（sum求和函数等），防止进行数据库统计行为，提供截图证明 8、★支持数据库绑定变量审计，提供截图证明 9、支持端口重定向的审计 10、★在无需重启数据库情况下，支持对MS SQLSserver 加密协议的审计，提供截图证明 11、支持服务器虚拟化的审计，支持虚拟桌面操作的审计，支持 Telnet、FTP协议的审计 12、支持所有应用 http 以及web报表审计，并能支持工号（账号）审计，能详细定位到人；重要关键页面可以通过执行审计 url 输出返回内容信息。同时支持和数据库访问关联。提供截图证明 14、支持超长操作语句审计，针对传统型数据库，支持 3 万字节的审计而不截断 15、★中间件的支持，支持 COM、COM+、DCOM组件的三层架构审计，能精确定位到人（工号、账号），提供截图证明 16、审计数据支持 18 种以上查询条件，可支持按数据库操作命令（包括 select、create等 14 个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间（包括开始、结束日期）等为条件进行查询。 17、可集成等级保护报表，确保能通过公安部信息安全等级保护的评测，提供截图证明 18、可对可疑监控对象的操作语句进行回放，方便追溯。 19、审计报表加密设置，采用国际通用的AES 256位加密算法 20、系统本身具备能发现未知仿冒进程工具、防范非法 IP地址、防范暴力破解登录用户密码、设置系统黑白名单等安全功能。 21、★翻译功能：实现对 SQL语句转换成中文自然语言的描述功能，便于不同层次人员理解报警内容，提供截图证明。	1
8	运维审计服务	1.要求配置运维堡垒机服务 1 年。 2.图形并发≥80，字符并发≥700；自带设备管理数 50 个 3.业务数据采取轻型日录存储，支持多节点数据实时同步；支持双网卡冗余（双网卡虚拟单 ip）；支持 active-stanby 方式的 HA 部署；支持集群部署。	1

		4.支持从AD域抽取OU，方便快速建立组织结构。 5.主帐号支持从AD域内抽取，方便快速建立主账号。 6.支持柱形图方式在右系统中不同资源所占比例及数量。 7.unix资源、网络资源、windows资源、数据库资源、C/S资源、B/S资源、中间件资源、大型机资源。 8.支持对unix资源、网络资源、windows资源、数据库资源、中间件资源进行密码变更；密码变更可以根据密码策略的要求进行变更，变更的密码符合密码策略中关于密码强度的要求。（请提供产品截图证明） 9.定期检查平台存储的设备账号密码与设备实际密码是否匹配，以便进校验密码一致性，提高设备的安全性避免密码混乱无法登陆现象发生。 10.★支持自定义角色。将系统功能模块按需分配给角色，角色可按照组节点进行定义，从而实现分层分级管理模式。（请提供产品截图证明） 11.资源授权模式基于岗位授权，岗位上绑定资源账号，这样授权可迁移、授权粒度更细；并可针对岗位设置相关安全策略。（请提供产品截图证明） 12.运维人员可将经常访问的资源添加到收藏夹。 13.多个不同类型的资源批量单点登录 14.支持将登录配置保存为默认后，可以一键快速登录目标资源（请提供产品界面截图） 15.支持采用winscp工具连接FTP、SFTP、windows文件共享目标，并且支持大文件的断点续传。（请提供产品界面截图） 16.支持RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别，修改属性后能够保证正常连接RDP且不影响审计。（请提供产品截图证明） 17.★支持网络设备的脚本自动化执行，脚本编辑可以支持文本框方式和交互方式；（请提供产品界面截图） 18.编辑脚本可以针对对应资源进行脚本可运行性测试，保证脚本的正确和计划的正确执行；（请提供产品界面截图） 19.自行结果可以在页面进行下载，或者采用ftp，邮件形式发送到指定位置。 20.★内置VPN功能，无需专用VPN硬件支持，即可方便安全地通过远程接入系统；支持通过VPN实现跨网闸运维管理；（请提供产品截图证明） 21.图形资源访问时，支持键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放，（请提供产品截图证明） 22★RDP审计策略支持关键帧，帧间隔，录像文件压缩比等设置，以缩小录像文件大小。（请提供产品界面截图并加盖公章） 23.对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并且可以高亮显示高危命令。（请提供产品截图证明） 24.审计日志可以采用syslog形式分类外发，至少可以分为系统类日志，内部审计日志，行为审计日志，违规命令日志，违规登录日志等。 25.支持IPV6环境下的使用，包括IPV6地址资源的添加管理，单点登录等。 26.支持日志数据的外置存储备份，支持NFS和windows文件共享协议，远程审计存储和本地存储对审计员透明。	

9	漏洞扫描服务	1.要求在上海市扫描服务工作； 2.提供产品支持在线升级，可设置定期自动升级时间，指定时间自动检测升级到最新规则库；支持通过设置代理进行升级；（提供产品功能截图） 3.最大扫描站点数量≥1024个，保留测试权利； 4.最大扫描IP或域名数量≥1024个，保留测试权利； 5.系统漏洞扫描并发主机数量≥100个； 6.★产品集成系统扫描、WEB扫描、数据库扫描、弱口令扫描于一体，且为单独功能模块；（提供产品功能截图） 7.产品可灵活调整物理和网络位置，扫描结束后自动生成详细的安全评估报告； 8.可以进行地检查多个被评估目标，提供扫描策略定制；（提供产品功能截图） 9.需提供策略保证扫描的安全性，不影响应用系统和网络业务的正常运行； 10.支持分布式部署，统一下发策略，集中管理（提供产品功能截图） 11.产品网络配置需提供快速配置向导，支持快速部署上线；提供产品功能截图） 12.支持可信IP管理，自定义可访问主机网段或IP； 13.★支持同时下发系统扫描、Web扫描、弱口令扫描任务，无需单独下发扫描任务，扫描目标可以是IP、域名、URL的任一格式（提供产品功能截图） 14.支持自定义扫描策略模板，支持按照漏洞类别、漏洞风险等级、CVE编号筛选查看漏洞插件；（提供产品功能截图） 15.支持扫描执行优先级别设置，灵活调度任务（提供产品功能截图） 16.支持IPV4、IPV6双协议栈地址扫描；（提供产品功能截图） 17.★支持60000条以上系统漏洞库，并按照漏洞类别及漏洞威胁程度进行分类； 18.支持漏洞库涵盖标准包含CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq编号6种；（提供产品功能截图） 19.支持和微软WSUS补丁系统的联动，方便进行自动化的补丁修补；（提供产品功能截图） 20.支持可对Windows系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris等目标主机的系统进行扫描； 21.支持SNMP等协议的漏洞检测；（提供产品功能截图） 22.支持对国产化操作系统扫描； 23.支持SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS协议的登陆扫描；（提供产品功能截图） 24.支持主机存活探测，支持ARP、ICMPping、TCPping及UDPping四种类型；（提供产品功能截图） 25.支持根据节点名称、设备名称、设备IP范围、设备操作系统、设备风险等级、漏洞名称、时间段进行查询资产风险情况并将查询结果导出；（提供产品功能截图 26.爬虫结果支持树形结构展示，并支持在对应目录上显示相应漏洞；（提供产品功能截图） 27.支持自动发现网站IP地址、服务器架构类型、网站标题、页面编码、物理地址、页面总数等指纹信息；（提供产品功能截图） 28.★支持目前协议和数据库弱口令检测，TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、REDIS、Oracle、MySQL、PostgreSQL、	1

		MsSQL、DB2、MongoDB；（提供产品功能截图） 29.报表支持漏洞验证，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；（提供产品功能截图） 30.支持对资产及资产检测结果进行备份及恢复；（提供产品功能截图）	
10	SDN安全资源编排服务	要求配置SDN安全资源池服务1年 1.安全资源编排功能：支持将遵循OpenFlow1.3标准协议的安全类设备通过旁路部署于核心，组成安全资源区，对指定业务流经过安全资源区的各安全设备的顺序进行自定义编排。提供技术原理说明文件。 可以通过出口设备和SDN控制器旁挂核心的部署方式，实现按需引流的效果； ★支持旁挂设备透明模式、路由模式，并提供实际配置界面，加盖原厂投标专用章。 ★支持旁挂设备跨品牌负载均衡部署，并提供实际配置界面，加盖原厂投标专用章。 ★支持旁挂设备跨品牌主备部署，并提供实际配置界面，加盖原厂投标专用章。 为保护投资，安全资源编排服务里的安全设备不能有任何品牌限制，至少满足≥5家以上不同品牌主流安全设备的部署，为防止虚假应标，保留测试权利。 支持基于流量选择故障发生时是否自动bypass，并提供实际配置界面，加盖原厂投标专用章。 ★支持业务流可定制安全设备路径转发，业务流支持L2-L4层五元组匹配方式，并提供实际配置界面，加盖原厂投标专用章。 支持配置备份服务链，当主服务链故障时业务自动切换至备服务链；支持故障修复感知和迁回，当主服务链故障恢复时业务自动迁回 为控制新增物理安全设备上线风险，支持出口新增设备上线不动原有物理拓扑。为保证可用性，保留测试权利 2.逃生功能：1、当出现控制器故障时，支持逃生机制，不影响当前业务运行，用户的安全策略不变，提供第三方测试报告。 容量要求：支持双栈6W认证用户容量。 3.南向接口：支持OpenFlow V1.0、V1.3，NETCONF、telnet等。 北向接口：1、支持RestFul API接口，反向RestFul API，RESTful API Help提供在线接口说明，可进行关键字查询提供功能截图证明或官网截图证明。 4.北向接口需以标准Http的RestAPI形式提供。 5.控制器性能支持1000个网元节点规模的网络，提供官网截图并。 6.支持Packet In和Packet Out每秒≥100K的处理速度，提供官网截图并加盖原厂公章。 7.控制器可靠性，为确保控制器的稳定转发，支持控制器之间进行集群部署，且集群数量≥64台，并提供官网截图。 8、支持ISSU升级，升级时业务不中断。 9.在SDN控制器出现异常、重启、升级、主备倒换时，网元设备上的流表继续生效，而且不影响转发的连续性。 控制器安全性： 10.、支持分级分权限的用户添加、删除和修改，用户权限颗粒	1

		度可以细化到每一个功能点。 11、支持访问白名单和黑名单设定。 控制器易维护性： 12、要求控制器及所配置SDN方案提供GUI界面，能够查看网络配置，同时能够进行编辑与配置下发。 13、提供向导式配置界面，点击开始后即可逐步进行业务配置，帮助用户快速完成业务部署。 14、支持图形化web管理，可通过web界面进行节点管理、链路管理、业务管理、拓扑管理、故障感知等。 15.控制器开放性支持 Restful API标准北向接口，便于向第三方系统对接。 16.资质证书：产品为软硬一体化产品，提供SDN控制器软件著作权证书和SDN控制器硬件3C认证证书。 17.本次实际配置：SDN控制器实配以上所有功能及50个网络安全节点管理授权，配合核心交换机实现安全资源编排功能。 18.为提升安全问题及时、智能处理能力，要求本次招投标的大数据安全态势感知系统与本次投标当中的SDN安全资源管理系统联动实现发现问题、智能阻断，提供第三方权威机构盖章的测试报告，并加盖原厂投标专用章	
11	准入认证服务	要求配置认证准入服务1年；整个平台最高支持配置5000并发在线终端数授权，本次服务配置500并发在线数的授权许可	1
12	终端业务接入服务	要求提供接入端口服务1年,提供360个千兆下行速率接入服务，提供60个千兆上行速率接入服务。	1
13	探针态势感知服务	1、要求提供流量探针态势感知服务1年。 2、★支持HTTP网页标题、BBS、威胁情报、DGA、搜索关键词的网络会话分类审计（提供功能截图并加盖厂商公章）。 3、支持DNS威胁情报、DGA、解码错误、解码失败、解码超时的网络会话分类审计（提供功能截图并加盖厂商公章）。 4、★支持以图形方式展现网站浏览排行、访问异常分布、网络协议类型分布、南北向及横向互联关系、DNS解析情况（提供功能截图并加盖厂商公章证明）。 5、支持全流量的网络会话存储及检索查询（提供功能截图）。 6、支持可疑威胁数据包留存，支持用户自定义数据包全留存或部分协议留存，协议类型包括HTTP、FTP、DNS、MYSQL、SMB、邮件协议等30种以上（提供功能截图证明）。 7、支持精确到秒的数据包检索；支持数据包留存吞吐展示（提供功能截图并加盖厂商公章）。 8、★支持一键挂载外置数据包全留存存储（提供功能截图并加盖厂商公章）。 9、支持常见Web应用攻击：Weblogic、wordpress、Jenkins、KLOG、Joomla、PHPAccounts等上千种应用的注入、后门、代码执行、提权、路径遍历、XSS等监测（提供功能截图）。 10、支持DNS服务器识别，利用DNS服务器穿透技术，识别被DNS代理隐藏在子网内的恶意域名回连行为（提供功能截图）。 11、支持对于网站的隐藏链接进行检测，黑链检测的类型不低于7种（提供功能截图）。 12、不健康网站访问、P2P通讯检测、代理使用检测、游戏检测、聊天工具、明文传输检测等（提供功能截图并加盖厂商公章证明）。 13、具备发现带宽占用异常、ARP风暴、ICMP Flood、TCP建连时延过长、TCP重传过多、TCP零窗口过多等网络质量异常	1

		以上 14、★支持对于[illegible]AI检测，[illegible]加不[illegible]于 100种（提供功能截图并加盖厂商公章证明） 15、支持威胁情报云查溯源，支持恶意IP、恶意域名、恶意URL、恶意文件的溯源查询，呈现威胁情报详细信息，包含情报时间、情报标签、相关事件、相关样本等（提供功能截图） 16、威胁情报云数据hash量级：hash鉴定历史不少于1000亿，存储样本150亿，存储恶样本数据不少于10亿，白样本不少于20亿，样本数据覆盖PC、移动终端等领域，日均新增恶样本数量不低于30万（提供功能截图）， 17、支持基于AI算法的异常流量行为检测，支持智能动态基线、模式信息熵、离群分析等算法，通过一段时间学习，对象的流量特征分析、建模，智能生产该对象多维度的纵深检测机制，从而发现异常协议、异常端口、异常流量（提供功能截图）， 18、支持基于AI的木马心跳行为检测（提供功能截图） 19、★支持旁路威胁阻断防御，用户可以根据已命中的安全事件精准对已知和未知攻击进行实时阻断，系统提供多种特征组合的阻断方式，并支持用户查询执行阻断策略的网络会话（提供功能截图）， 20、支持检测结果Syslog转第三方系统，包括：发送攻击检测命中日志；发送威胁情报检测命中日志；发送DGA检测日志；发送文件安全检测日志；发送聚合的会话统计日志； 21、支持基于地图（国内/全球）的安全态势直观展现，以及全面的威胁行为统计，包括威胁次数、威胁趋势、威胁源、威胁目标、威胁目标端口、威胁类型、威胁协议、安全策略类型、命中威胁情报等统计展现； 22、支持主机网络性能实时监控，以图表的形式监控主机的带宽占用情况、端口/应用的流量分析、TCP建连成功率、TCP三次握手时延、TCP重传以及TCP零窗口等，并且支持查询模式回溯历史时间的网络质量情况； 23、支持实时统计流量使用情况，可通过列表查看每个主机的流入流量、流出流量，总流量，也可以通过配置交换机接口来监控各个网段的流入流量、流出流量、总流量并且可通过下钻单个主机或网段，查询主机或网段的流量趋势，以及进行对比各个时间段的流量情况； 24、支持动态执行环境文件，文件行为分析，包括注册表、进程、网络、释放恶意文件等行为，支持提取攻击的完整样本，并提供样本的下载能力；支持检测Word、Excel、PPT、PDF、EXE、DLL、ZIP、RAR、7z等主流文件类型； 25、支持系统敏感操作、系统环境探测、反检测行为、反调试行为、木马回连、远控木马、网络通讯、勒索软件、恶意软件行为等文件恶意行为检测； 26、通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构； 27、HTTPS访问，二层数据包解码：普通以太头解析、支持PPPoE、VLAN、VLAN QinQ；三层数据包解码：支持IPv4、IPv6；四层数据解码：支持TCP、UDP、ICMP、ICMPv6、SCTP、IGMP等； 28、HTTP数据解码和元数据分析：对HTTP请求的域名、URL、状态码、UserAgent、X-Forwarded-For等解析（提供功能截图）； 29、数据库数据解码和元数据分析：包括MYSQL、ORACLE、	

		SQLSERVER、SYBASE、DB2协议的用户名、密码、SQL语句等信息（提供功能截图）； 30、支持SMB文件、命令行等字段审计；支持邮件发件人、收件人、主题、邮件服务器、邮件服务器端口、应用协议、收发时间审计；支持Telnet用户名、密码、命令字段审计；支持SNMP服务器、客户端、开始时间、结束时间审计； 31、漏洞利用规则特征库数量≥6700+条；Web攻击检测规则数量≥8000+条；扫描探测检测规则数量≥500+条； 32、支持HTTP、ICMP、SSH、FTP、DNS、RDP、RPC、SMB、HTTPS、SSL、POP3、SMTP、IMAP、SQL、SNMP等协议的可疑信道检测，不低于2300种； 33、支持全面的网络情况可视化，包括网络安全状况可视化、网络带宽占用及网络质量可视化、网络流量可视化，支持实时统计流量使用情况，可通过列表查看每个主机的流入流量、流出流量，总流量；并且可通过下钻单个主机或网段，查询主机或网段的流量趋势，以及进行对比各个时间段的流量情况（提供功能截图）；	
14	光连接服务	提供千兆单模光连接服务1年	1