甲方合同编号：【　　】

乙方合同编号：【　　】

河南移动【南阳】分公司与【南阳市人民政府办公室】关于【南阳市人民政府办公室政务内、外网网络安全体系建设及运维服务】项目合作协议

甲方：【南阳市人民政府办公室】（盖章）

法定代表人：

住所：

授权代表签字：

电话：

联系人：

乙方：【中国移动通信集团河南有限公司南阳分公司】（盖章）

负责人：

住所：

授权代表签字：

电话：

联系人：

合同签订日期：【2023】年【 12】月【 13 】日

根据《中华人民共和国民法典》、《中华人民共和国电信条例》及其他有关法律、法规的规定，在平根据《中华人民共和国民法典》、《中华人民共和国电信条例》及其他有关法律、法规的规定，在平等、自愿、公平、诚实、信用的基础上，双方就南阳市人民政府办公室政务内、外网网络安全体系建设及运维服务项目有关事宜协商一致，达成合同如下：

第一条 合作内容

1.1 乙方在现有技术条件下、现有网络覆盖范围内，为甲方有偿提供【南阳市人民政府办公室政务内、外网网络安全体系建设及运维服务】项目系统集成服务，以及对应的设备销售、维保服务。

1.2 乙方为甲方提供的具体服务内容及要求详见【附件 1：价格清单及技术规范】。

第二条 资费标准和支付方式

2.1 本合同项下甲方应当向乙方支付的合同款项包括集成服务费、设备采购费、维保服务费。

2.2 本合同项下甲方应当向乙方支付的合同款项（含税）共计【1450000】元（大写：【壹佰肆拾伍万元整】），详见下表。

项目名称	合同内容	未含税总价（元）	税率（%）	增值税税额（元）	含税总价（元）
南阳市人民政府办公室政务内、外网网络安全体系建设及运维服务项目	系统集成费	682235.85	6%	40934.15	723170
	设备采购费	377725.66	13%	49104.34	426830
	维保服务费	283018.87	6%	16981.13	300000
合计		1342980.38	/	107019.62	1450000

2.3 合同项下所有款项由甲方向乙方以如下方式及比例支付：

【项目验收合格后（网络安全监测平台及配套设备完成集成、安装及调测，运行正常达到交付验收标准）20 日内甲方向乙方支付合同总金额的 50%即 725000 元（人民币大写：柒拾贰万伍仟元整整）。自项目验收通过之日起乙方为甲方提供维保服务，维保期为【3】年。第二年维保期结束后进行维保服务评估验收，验收通过（维保服务评估验收标准详见附件 1：价格清单及技术规范）20 日后甲方向乙方支付合同总金额的 50%即 725000 元（人民币大写：柒拾贰万伍仟元整）。】

2.4 双方银行账户信息

乙方名称：【中国移动通信集团河南有限公司南阳分公司】

纳税人识别号：【91411300719156858P 】

户名：【中国移动通信集团河南有限公司南阳分公司】

开户行：【中国银行南阳分行营业部】

账号：【246802555533】

地址：【南阳市张衡东路 1266 号】

联系电话：【0377-62081977】

任何一方如需改变上述账户信息（甲方名称和纳税人识别号不可改变），应在变更账户前十（10）日以书面通知另一方并征得对方同意。如一方未按本合同约定单独变更账户信息而使另一方遭受损失的，应予以赔偿。

2.5 结算周期内甲方向乙方支付的费用为：结算金额＝Σ（应付合同金额±违约金）（说明：如甲方违约则使用“＋”，若乙方违约则使用“－”）。

2.6 结算方式采用【转账】（现金/转账等）的形式。

2.7 在甲方支付本合同项下的综合服务费之前，乙方应当向甲方开具相应金额的增值税【普通】（普通/专用）发票。

第三条 服务期限

本合同自双方签字盖章之日起生效，乙方应自合同生效之日起【30】日内完成平台集成及调测，达到交付验收标准。

自项目验收通过之日起乙方为甲方提供维保服务，维保期为【3】年。

第四条 设备验收、集成验收

4.1 设备验收

4.1.1 甲方指定的地点及收货人：【南阳人民政府办公室、李涛】。

4.1.2 开箱检验在乙方将货物运送至甲方指定交货地点后【7】日内进行，双方根据合同约定检查货物，检验后无任何问题的签署开箱检验合格证书。

4.2 集成验收

4.2.1 根据中华人民共和国国家和履约地相关质量标准、行业技术规范标准、采购文件的要求及乙方的响应承诺验收。

4.2.2 在乙方完成集成服务 7 个工作日内，双方应对项目成果进行验收，各项功能及指标符合要求的，由双方签署项目验收合格报告。

4.3 甲方自收到乙方提交的验收申请后 7 个工作日内未组织验收，且自乙方催告后 3 个工作日内仍未组织验收的，视为验收通过。

第五条 售后服务

乙方维保具体内容如下：

5.1 为保证系统正常运行所需的预防性维护、日常维护支持、网络调整支持、数据备份支持等工作。

5.2 提供每周 7 天每天 24 小时的技术支持服务。如果出现紧急技术问题，在甲方通过电话或传真通知乙方的情况下，乙方的工程师应在 1 小时内予以答复。如果甲方要求紧急处理，乙方应在收到甲方通知后的 4 小时内赶到现场。当合同系统提供的业务中断时，乙方在提供远端服务的同时，

须在收到甲方通知后 2 小时内赶到现场，因不可抗力致使乙方未按时到达现场的除外。

5.3 硬件设备发生损坏的，若在质保期内，设备维修或更换的成本由乙方承担（因甲方故意或使用不当导致设备损坏的除外）；若在质保期外，设备维修或更换的成本由甲方承担。

第六条 双方的权利与义务

6.1 甲方的权利和义务

6.1.1 在本合同有效期内，甲方有权要求乙方根据本合同约定和产品使用说明的描述向甲方提供相应的产品和服务。

6.1.2 甲方同意，乙方有权协同第三方从事部分合同约定的乙方服务工作。但是，乙方应对第三方的服务行为向甲方承担责任。

6.1.3 甲方应当根据其所使用的业务的要求向乙方提供真实有效的证件、资料和信息（包括但不限于甲方单位及相关授权人真实有效的营业执照、身份证、授权委托书等证件，以及白名单的相关资料等）。

6.1.4 甲方承诺并保证不利用乙方提供的设备或服务进行任何违反国家政策法律法规、侵犯乙方或第三方合法权利的行为，否则，乙方有权立即停止向甲方提供所有产品和服务并解除本合同，一切后果由甲方承担。

6.1.5 甲方应本合同的约定，及时足额向乙方支付各项费用。

6.1.6 甲方应授权一名员工作为联系人，负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人需提供乙方所需的身份确认资料。甲方联系人如发生变更，需以书面形式通知乙方。

6.1.7 甲方使用乙方提供的本合同约定产品或服务时，需遵守对应的产品使用说明。甲方未按约定和相关要求使用产品或服务的，相关责任由甲方承担。

6.1.8 甲方成为乙方集团客户后，如果乙方提供了服务账号，甲方应妥善保管乙方提供的相关

服务账号和甲方设定的服务密码。服务账号和密码是甲方办理产品相关业务的凭证，凡使用服务密码进行的任何操作行为均被视为甲方或甲方授权行为。如因甲方服务账号和密码保管不善等原因发生服务中断、业务变更、高额费用等情况，甲方应立即以书面形式通知乙方，乙方应采取可行的补救措施。甲方应当承担因账号和密码保管不善产生的费用。

6.1.9 如因甲方提供的相关资料不准确、不真实、不完整或变更后未通知乙方等原因，使乙方无法将产品或服务提供给甲方，甲方承担由此造成的责任和后果。

6.1.10 未经乙方同意，甲方不得将乙方的软件、技术、设施、设备等用于双方合作项目以外的其他用途，且不得向第三方透漏、转让。若甲方违反本条款，乙方有权要求甲方赔偿损失，撤回设备、终止协议。

6.1.11 未经乙方书面同意，甲方不得擅自使用中国移动的企业及品牌名称和标识、乙方的地方性品牌的名称和标识。否则，乙方有权解除合同并要求甲方赔偿损失.

6.2 乙方的权利和义务

6.2.1 乙方应按合同约定向甲方提供相关硬件设备，并完成系统集成、维护等工作。乙方人员应携带相关证件及单位证明，与甲方相关部门联系并办理相关手续，甲方应及时提供相关配合。

6.2.2 乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用本合同约定产品或服务的，应提前通知甲方，甲方应给予必要的配合。

6.2.3 乙方受理甲方的故障申报，应及时安排故障处理。乙方按维护及业务规程的有关规定，为甲方提供优质服务。

6.2.4 在合同有效期内，乙方有责任按照国家标准负责系统的日常运行维护工作。保障系统的正常运行，如发生故障，及时响应。

6.2.5 因第三方实施破坏、网络攻击等非乙方原因导致甲方不能正常使用乙方产品和服务的，

不视为乙方违约，乙方不承担相应责任。

6.2.6 乙方有权本合同约定要求甲方及时足 预支付各项费用。

6.2.7 乙方应对其所委托的代为向甲方提供 本合同项下服务的第三方的服务行为向甲方承担责任，包括保证其提供的服务质量符合本合同约定，并对其服务瑕疵向甲方承担违约责任。

第七条　保密条款

7.1“保密信息”是指本协议拥有信息的一方（“提供方”）根据本协议向另一方（“接受方”）提供的信息，或接受方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于：技术信息、商业信息、商业秘密、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履行过程中形成的所有信息、数据、资料、意见、建议等。

7.2 保密信息只能由接受方及其人员为本协议目的而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方事先书面同意，接受方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。乙方关联公司，是指中国移动通信集团公司及其在中华人民共和国境内直接或间接控股的主营通信业务的公司，以及上述公司的合法继承公司。

7.3 双方不得向任何人透露用户的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除用户本人以外的任何单位或个人的查询；同时，双方应尽合理努力将电子支付交易数据以安全方式保存，并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取。

7.4 接受方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接受方可向其披露保密信息，但是，其应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。接受方应向提供方承担因己方聘请的上述专业顾问违反保密约定而给提供方造成的任何损失。

7.5 如相关政府部门或监管机构要求接受方披露任何保密信息，接受方可在该政府部门或机构要求的范围内做出披露而无需承担本协议项下的保密责任。但前提是，该接受方应立即将需披露的

信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接受方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。保密信息不包括以下任何信息：（1）非因违反本协议所致，已进入公众领域的信息；（2）在提供方依据本协议做出披露前，接受方已合法拥有的信息；（3）接受方从有权披露的第三方获得的信息；及（4）接受方独立开发的信息，未使用任何保密信息。

7.6 双方应严格遵守保密条款之约定，严格履行保密义务，直至有关保密信息合法公开之时止。本协议或其任何条款的终止、中止、失效、无效均不影响本保密条款的有效性及对甲乙双方的约束力。

7.7 由于保密信息接受方未履行保密义务给提供方造成损失的，接受方应当赔偿由此给提供方造成的损失。

7.8 在任何情形下，本合同约定的保密义务应永久持续有效。

第八条　违约责任

8.1 甲方未按照本合同约定的期限支付合同款项的，从逾期的次日起计算违约金，每滞后 1 天支付未缴金额的【1‰】。违约金总额超过合同金额的【20%】时，乙方有权解除本合同，并保留进一步追偿的权利。

因乙方原因导致乙方未按照本合同约定时间完成项目的，每逾期一天应向甲方支付合同金额1‰的违约金。当发生故障时，乙方需在 24 小时内恢复正常（1、设备损坏需更换设备，设备需从南阳市范围外地区送达；2、非乙方原因造成的故障，上述两种情况除外），如果出现超时未处理的，每出现一次应向甲方支付合同金额 0.5‰的违约金。

8.2 乙方在进行网络调整和维护时需要短时间中断服务，或者由于 Internet 上骨干网通路的阻塞造成甲方服务器访问速度下降，甲方认同属于正常情况，不视为乙方违约。

8.3 下列情况下乙方有权单方终止本合同，并停止向甲方提供服务。由此给甲方造成的损失，

乙方不承担责任，并有权要求甲方承担违约和赔偿责任：

（1）甲方（包括联系人）提供虚假证照的；

（2）甲方利用乙方提供的产品和服务实施违反国家法律、法规和政策的；

（3）甲方利用乙方提供的产品和服务从事其他不当用途（如：甲方将乙方提供用于本合同业务的相关设备转售、转租、转借第三方，或将乙方提供的设备、产品和服务接入其他通信服务提供商的业务）或侵犯第三方的合法权利；

（4）乙方根据国家有关部门的要求停止为甲方提供相关服务；

8.4 乙方仅对因其过错给甲方造成的直接损害结果承担赔偿责任，且不包括第三方提出的索赔要求、数据丢失或损坏的损失，不包括经营损失等一切间接损失。无论何种情况，乙方应对自身产品负责。

第九条　不可抗力及免责条款

9.1 本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

9.2 由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：（1）受阻方不能全部或部分履行其义务，是由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形；（2）受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；（3）不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五(15)天内提供有关该事件的公证文书和书面说明，书面说明中应包括对延迟履行或部分履行本合同的原因说明。

9.3 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

9.4 如果不可抗力事件的影响持续达三十（30）日或以上时，双方应根据该事件对本合同履行

的影响程度协商对本合同的修改或终止。如在一方发出协商书面通知之日起十（10）日内双方无法就此达成一致，任何一方均有权解除本合同而无需承担违约责任。

9.5 如因不可抗力造成的技术、网络故障或第三方原因造成甲方无法使用本协议项下服务的，不视为乙方违约，但乙方应尽合理努力争取在最短时间内解决，对此双方无异议。鉴于计算机、移动通信网络及互联网的特殊性，因黑客、病毒、电信部门技术调整和骨干线路中断等引起的事件，在乙方能够出具相关合理证明材料的情况下，甲方亦认同不属于乙方违约。

第十条 通知与送达

10.1 根据本合同需要发出的全部通知，均须采取书面形式，对本合同效力产生影响的、或解决合同争议时的通知或函件，以（A）专人递送，（B）特快专递发出。特快专递的交寄日以邮戳为准。上述书面通知均须标明合同对方为收件人。

10.2 上述书面通知按对方在本合同通知与送达条款中所列的地址发出。如双方中任何一方的地址有变更时，须在变更前十日以书面形式通知对方，因迟延通知而造成的损失，由延迟通知方承担责任。

10.3 双方将按如下约定确定通知送达完成时间：

10.3.1 以专人递送的，接收人签收之日视为送达；

10.3.2 以特快专递形式发出的，发往本市内的，发出后第【3】日视为送达。发往国内其他地区的，发出后第【5】日视为送达；

10.3.3 以特快专递形式发出的通知，必须向本合同通知与送达条款约定的地址或者依据本合同变更后的地址发出；任何一方未按照本合同约定的送达方式送达的，视为未履行通知送达义务；

10.3.4 以电子邮箱形式发出的，到达接收人电子邮箱所在系统之时视为送达；

10.3.5 以电子邮箱形式发出的通知，必须向本合同约定的电子邮箱发出；任何一方未按照本合同约定的电子邮箱送达的，视为未履行通知送达义务；

10.3.6 合同各方均明知：因各方提供或者确认的通信地址和联系方式不准确、 或者通信地址变更后未及时依程序告知对方和司法机关、或者当事人和指定接收人拒绝签收等原因，导致商业信函、诉讼文书等未能被当事人实际接收，以专人递送的，送达至通知与送达条款约定的地址之日即视为送达之日；以特快专递形式发出的，按照通知与送达条款约定的方式确定送达之日。

10.4 以特快专递形式发出的通知，必须向本合同约定的地址或者依据本合同第 10.2 条款变更后的地址发出；任何一方未按照本合同约定的送达方式送达的，视为未履行通知送达义务。

各方地址与联系方式如下：

甲方：【南阳市人民政府办公室】

地址：【南阳市范蠡路市民服务中心北区 1 号楼 9 楼】

电话：【0377-63152073】

电子邮件：【szfbwdk@163.com】

邮政编码：【473000】

乙方：【中国移动通信集团河南有限公司南阳分公司】

地址：【南阳市张衡东路 1266 号】

电话：【13837758288】

电子邮件：【13837758288@139.com】

邮政编码：【473000】

第十一条　争议解决

11.1 本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

11.2 如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或

效力有关，都应由双方通过友好协商解决。协商 立在一方向另一方送达关于协商的书面要求后立即开始。

11.3 如果在一方提出协商要求后的十(10)天 内，双方通过协商不能解决争议，则双方同意向甲方住所地人民法院提起诉讼。

11.4 诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续履行。本合同全部或部分无效的，争议解决条款依然有效。

第十二条　其他约定

12.1 本合同一式【肆】份，双方各持【贰】份，具有同等法律效力。

12.2 对于合同未尽事宜、双方可签订补充合同对本合同中的问题做出补充、说明、解释。本合同的补充合同作为本合同不可分割的一部分，与本合同具有同等的法律效力。

12.3 本协议附件作为本协议的一部分，与本协议具有同等法律效力。

12.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除本协议。任何一方欲变更或解除本协议，应提前30日向另一方提交书面说明。单方面解除协议的一方，应对另一方因此遭受的损失承担全部赔偿责任。

第十三条　本合同附件

附件1：价格清单及技术规范

附件2：网络与信息安全协议书

（以下无正文）

网络与信息安全协议书

甲方应按照《中华人民共和国网络安全法》等法律法规的要求，履行相关网络安全义务，承担网络安全责任。

第一条甲方承诺不利用乙方提供的服务及设备设施进行下列任何活动或发布、传播下列任何信息：

（1）从事危害国家安全、泄露国家秘密等犯罪活动；从事国家法律、法规、政策所禁止的活动或违背公共道德的活动；

（2）散布谣言，扰乱社会秩序，破坏社会稳定；散布垃圾邮件、病毒程序；黑客行为；侵权行为；博彩、赌博游戏等；

（3）危害国家安全、泄露国家机密、颠覆国家政权、破坏国家统一的信息；损害国家荣誉和利益的信息；煽动民族仇恨、民族歧视、破坏民族团结的信息；违反国家宗教政策的信息；宣扬邪教和封建迷信的信息；淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的信息；侮辱或者诽谤他人，侵害他人合法权益的信息；妨碍互联网运行安全的信息；其他有损于社会秩序、社会治安、公共道德的信息或内容；

（4）发布、传播其他违反国家法律、法规、政策内容的。

甲方同时承诺不为他人从事上述活动或发布、传播上述信息提供任何便利，如因甲方违反上述约定产生的一切责任和后果均由甲方承担。甲方认可乙方有权判断本协议项下甲方从事的活动或甲方发布的信息是否违法、违规或违反本协议有关规定，且乙方有权在提前通知甲方的情况下采取一切必要措施，包括但不限于暂停或终止提供本协

议项下的服务、要求甲方进行整改等，但乙方上述权利不应被视为乙方有审核甲方行为或信息内容的义务或保证其合法合规的任何责任。

第二条甲方不得有下列危害电信网络安全和信息安全的行为：

（1）对电信网络的功能或者存储、处理、传输的数据和应用程序进行违法删除或者修改。

（2）利用电信网络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电信网络等电信设施。

（4）危害电信网络安全和信息安全的其他行为。

若甲方存在上述任一情形的，乙方有权按相关规定暂停或停止提供服务、断开网络接入，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，乙方有权终止合同，并不承担任何责任。

第三条甲方不得将接入设备转借或租赁给其它单位和个人使用，以防止非法信息的传播；否则，由其承担相关责任，乙方有权立即停止相关服务。

第四条甲方应承担如下管理责任：

（1）向所属员工或使用者宣传国家及电信主管部门有关电信安全的法规规定。

（2）建立健全使用者档案，加强对使用者的管理、教育工作。

（3）有健全的网络安全保密管理办法。

第五条甲方有责任对其自身系统的网络安全状况负责，并定期对其系统的安全状况进行检查，若发生网络攻击、信息泄露等网络安全事件，乙方不承担相关责任。

第六条甲方侧数据由甲方负责，如出现信息泄露、信息篡改等安全事件，乙方不承担责任。

第七条甲方承诺采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。不得从事以下行为：

（1）利用自己或他人的机器设备，未经他人允许，通过非法手段取得他人机器设备的控制权；

（2）非授权访问、窃取、篡改、滥用他人机器设备上的信息，对他人机器设备功能进行删除、修改或者增加；

（3）向其他机器设备发送大量信息包，干扰其他机器设备的正常运行甚至无法工作；或引起网络流量大幅度增加，造成网络拥塞，而损害他人利益的行为；

（4）资源被利用进行网络攻击的行为或由于机器设备被计算机病毒侵染而造成攻击等一切攻击行为。

（5）有意通过互联网络传播计算机病毒；

（6）因感染计算机病毒进而影响网络和其它客户正常使用的行为。

第八条甲方业务如使用乙方提供的IP地址，甲方需承诺并确认：甲方所提交的所有备案信息真实有效，且备案信息不得出现乙方任何

内容。当提供的备案信息发生变化时应及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，乙方有权依法采取停止提供服务、断开网络接入等关闭处理措施。如因甲方原因造成信息未及时通知，引发相关网络信息安全事件的，由甲方自行承担相关责任。

甲方签字盖章：

年　　月　　日

附件 1：价格清单及技术规范

一、价格清单

南阳市人民政府办公室政务内、外网网络安全体系建设及运维服务项目						
序号	类别	名称	内容	单位	数量	含税金额（元）
1	系统集成	政务内、外网网络安全监测平台	包含主机健康与审计、防病毒、身份鉴别、打印刻录安全监控与审计四个模块，通过上述的模块配合使用，可以形成一个完整的安全防护体系。通过监控和分析网络数据、检测安全漏洞、限制访问权限等方式来保护政务内、外网络环境的安全。其可以有效地防止黑客攻击、病毒感染、数据泄露等安全威胁，保障政务信息资源不受损失。	项	1	723170
2	设备销售	防火墙	品牌型号：天融信 NGFW4000-UF(ZX-A)（千兆）V3	台	2	81830
3		核心交换机	品牌型号：华三 H3CS7503E-M	台	4	39040
4		入侵检测	品牌型号：天融信 TopSentry3000（ZX-A）（千兆）V3	台	2	99530
5		入侵防御	品牌型号：天融信 TopIDP 3000(ZX-A)（千兆）V3	台	2	102080
6		网络审计	品牌型号：天融信 TA-Net（ZX-A）V3	台	2	104350
7	维保服务	运维服务	提供 3 年安全运维服务包含：网络设备维护与管理、网络监控与故障处理、网络安全管理、网络性能优化以及服务报告和统计分析。	月	36	300000
合计				**	**	1450000

二、技术规范

1、维保服务考核

（1）、维护服务质量考核以整个服务期为一个考核期，每 3 个月进行评分。若最后一个评分期少于 3 个月，则按照实际维护时间进行评分作为半年度测评分。考核评分包括半年度测评分、考核期测评总分。

（2）、考核期测评总分＝Σ半年度测评分/半年度测评次数。

（3）、半年度测评分=Σ每项实际评分*权数。

（4）、考核期测评总分达到 80（含 80 分）以上视为维保服务评估验收通过。

由于实万工程师未能按照双方同意的维保服务期实施服

（5）、评估标准下

类别	服务内容	评估标准（注：扣分至满100分止）	总分	权数
标准服务	技术支持服务	远程技术支持未满足7*24小时要求，每次扣3分	100	10%
	系统升级服务	在服务过程中，若因客户的如下原因造成停机时间超过计划停机时间，则每超出1小时扣3分（不足1小时按1小时计算）：未制定实施计划、应急预案，或完全由于卖方原因未遵照计划实施，造成停机时间超过计划停机时间；	100	30%
		未提供升级小版本，每次扣3分。		
	故障处理服务	接到用户故障申告电话后应于30分钟内响应，如故障未能在2小时内通过远程支持得到解决，卖方应将根据用户要求指派服务工程师以最快方式赶往用户现场，提供不间断故障处理服务。（响应时间每超出1小时扣3分）	100	40%
		卖方服务工程师应于2小时内到达现场；如用户现场在其他地区，卖方服务工程师应于8小时内到达现场超出到场时限要求，每超出1小时扣3分（不足1小时按1小时计算）。		
		超出紧急故障恢复时限，每超出1小时扣3分（不足1小时按1小时计算）。免责事项：不是由于卖方产品故障导致的不可用；		
		不能够满足不间断处理需求的（只用于考核紧急故障），每次扣3分		
		故障处理完成时间超出规定时限的，每超出1小时扣10分（不足1小时按1小时计算）		
		对于系统中的故障部件（可更换板卡、模块直至整机），卖方服务工程师应携带替换部件到达现场进行更换，替换部件应全新、完好，且与故障部件型号相同或兼容、性能等同于或高于该故障部件。（若替换件不达标扣3分）		
		不能在3个工作日内提交故障分析报告，每超出一天扣3分		
	其它服务	卖方未按要求在服务例会上提交相应报告，每次扣3分	100	20%
		卖方制定的客户档案及服务计划不符合有关规范（由双方另行书面约定）要求，每次扣3分		
		卖方在双方约定的时间内未对买方根据合同约定提出的合理意见及建议进行反馈或执行，每次扣6分。		
		由于卖方工程师未能按照双方同意的维护服务规范或服务条款提供服务，买方提出书面投诉，投诉内容得到卖方		

		认可的每次扣 6 分。		
		乙方服务区域内的参[illegible]设备，一个季度内不得出现相同故障重复维修现象，否则，每出现一次，扣 1 分		
		对乙方服务区域内的[illegible]服务质量的现场考核由甲方所属分公司组织，每月/季度对服务区域内的设备进行抽查，抽查比例不得小于 10%；抽查结果符合甲方提出的服务质量要求的为合格，否则为不合格；每次抽查不合格扣 1 分		
		卖方不得以任何方式将有关用户的系统信息披露、发表或传播，并与用户签订相关保密协议。违反保密协议规定内容一次扣 3 分。		
		由于卖方工程师未能按照双方同意的维护服务规范或服务条款提供服务，买方提出书面投诉，投诉内容得到卖方认可并同意撤换工程师，卖方未按买方要求撤换工程师的，每次扣 6 分。		
可选服务	预防性维护	买方按照“维护服务内容及要求“或双方另行约定要求进行预防性维护服务，而卖方未实施，每次扣 50 分；	100	40%
		卖方预防性维护的内容未达到卖方的服务技术规范要求，每次扣 3 分；		
		卖方未能在双方约定的时间内提交检查计划、检查报告，每次扣 1 分。		
	系统调整	卖方工程师未按双方约定的时间要求，准时到达现场提供技术支持，每次扣 3 分；	100	60%
	工程支持服务	卖方工程师未按“维护服务内容及要求”或双方另行约定的系统调整和工程支持要求实施项目服务，每次扣 3 分；		

2、详细技术参数

项目名称	南阳市人民政府办公室政务内、外网网络安全体系建设项目						
（一）政务内、外网网络安全监测平台							
平台功能	序号	模块		功能简介	数量	单位	含税单价（元）
网络安全监测平台，包含主机健康与审计、防病毒、身份鉴别、打印刻录安全监控与审计	1	主机监控与审计系统	管理端（天融信 TSM(FT-A)）	1、 系统结构：软件形态，配置≥1 个管理中心授权，且管理中心支持级联。3 年质保工程师上门服务。 2、 支持 windows 客户端和信创客户端同一管理平台统管，不拆分为支持信创终端平滑替代。 3、 总体态势一览图形化展现（包括主机总数、主机在线数、今日告警数、昨日告警数、操作系统分布、告警趋势、	2	套	26600

四个模块，通过上述的模块配合使用，可以形成一个完整的安全防护体系。通过监控和分析网络数据、检测安全漏洞、限制访问权限等方式来保护政务内、外网络环境的安全。其可以有效地防止黑客攻击、病毒感染、数据泄露等安全威胁，保障政务信息资源不受损失。				告警排行及时间类型排名等）。 4、 支持单位组织结构的建立可创建、删除、更改部门，同时可创建管理用户可设置用户姓名、邮箱、电话等信息便于系统管理。 5、 支持按照 IP、时间、责任人、事件类型、风险级别、行为类别进查询，结果显示责任人、部门、IP 地址、事件类型、风险级别、行为类别、产生时间、报警类型、事件内容信息。并提供导导出功能。			
			客户端（天融信 TSM）	1、 系统结构：软件形态，≥200 个客户端授权。3 年质保工程师上门服务。 2、 支持对代理主机打印行为进行监控，检测内容包括打印文件名称、打印机名称、打印用户、打印页数、打印份数、打印时间、打印结果等，打印日志上报至服务端。 3、 客户端支持国产中标麒麟、银河麒麟、UOS 管理端支持 centos7.6 以上、中标麒麟、银河麒麟、UOSCPU 支持飞腾、龙芯、兆芯、锟鹏、海光。 4、 支持按照日志类型与事件进行查询，结果显示类型、时间、结果、描述等信息。 5、 支持对网络连接行为进行审计和监控，支持 TCP、UDP、ICMP 等网络协议，同时支持按照网络五元组即协议、源端口、源 IP、目的端口、目的 IP 对网络连接进行审计阻断或放行。 6、 支持监控光盘、移动存储设备、人体工程学设备的操作并审计。	400	套	290
	2	防病毒系统（天融信 TopEDR）		1、 系统结构：软件形态，≥200 个客户端防病毒功能授权，≥3 年病毒库升级许可；配置≥1 个管理中心授权，且管理中心支持级联。3 年质保工程师上门服务。 2、 支持多引擎、启发式扫描引擎、基因识别引擎和虚拟沙盒引擎，全方位提高终端防护水平。 3、 支持病毒自动隔离备份功能，能自动将病毒文件隔离到本地隔离区，同时支持从客户端恢复隔离文件。 4、 支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，	400	套	660

		监控与审计系统		用户标识、IP 时间对数据进行统计，支持实时或报表形式输出统计结果。 4、支持自行设置服务器开机运行时段。 5、支持按 IP、安装情况展示系统客户端安装信息，同时支持按 IP 进行终端搜索。 6、支持日志按异常报警、终端操作日志、管理员等类型分类统计，可记录详细的责任人、IP、事件详情、风险级别。			
			客户端（天融信 TSM）	1、系统结构：软件形态，≥300 个客户端授权。 2、支持中标麒麟、银河麒麟、中科方德操作系统；兼容国产各系列打印机、刻录机。 3、支持对终端运行进行监控，可监控终端的在线、离线时长并支持按时间段形式进行终端搜索。 4、支持新增打印机名称、型号、序列号、厂商、密级展示!并支持按名称、密级进行设备搜索。 5、支持新增刻录机名称、型号、序列号、厂商、密级展示并支持按名称、密级进行设备搜索。 6、支持为打印文本添加水印，水印可自定义文本、字体、颜色，并支持图片预览。 7、支持日志转发，可配置协议、端口、日志类型。	300	套	465

（二）配套设备

设备名称	序号	品牌	规格型号	设备参数	数量	单位	含税单价（元）
防火墙	1	天融信	NGFW4000-UF(ZX-A)（千兆）V3	1、标准式机架设备，配置兆芯芯片，中标麒麟操作系统；接口配置：≥5 个千兆电口，≥4 个千个光口；冗余电源；网络层吞吐量(双向)≥IPv4：5500Mbps，Ipv6≥5500Mbps。 应用层吞吐量(单向)：IPv4≥2000Mbps，IPv6≥2000Mbps。TCP 新建连接速率：IPv4≥10 万/秒，IPv6≥9.5 万/秒。 TCP 并发连接数： IPv4≥300.000 万，IPv6≥300.000 万；配置应用识别功能。 2、支持策略略路由，支持根据入接口、源/目的 IP 地址、协议、用户、应用、选路算法、探测等多种条件设置策略路	2	台	40915

				并可根据 IP 规则一键整理。 5、 当文件被执行、修改、访问时，反病毒引擎对相应文件进行扫描，如扫描到威胁则阻断用户对该恶意威胁的触碰并根据需要进行隔离操作。 6、 支持通过 PING、ARP、NMAP 方式扫描，及时发现尚未纳入管控的终端，支持以 IP 地址池方式展示终端的终端在线、离线、安装情况。			
	3	终端安全登录系统	终端安全管理端天（融信 TopTSL（FT-A）） 终端安全客户端（天融信 TSM）	1、系统结构：软件形态，配置≥1 个管理中心授权，且管理中心支持级联。3 年质保工程师上门服务。 2、支持图形化展示数据分析结果，可按用户标识、IP 时间对数据进行统计，支持实时或报表形式输出统计结果。 3、可以支持中标麒麟、银河麒麟、中科方德、统信操作系统。 4、支持按 IP、MAC、责任人、部门、策略状态等方式显示策略的下发详情。 5、支持根据管理员、时间进行管理员操作日志查看，显示操作者、时间、IP、状态等信息;支持审计管理员用户的登录、注销行为。 6、支持对单独的终端进行查看，可查看终端的责任人、部门、操作系统、在线状态、网络配置、计算机名等信息，并可对部分信息修改。	1	套	16700
				1、系统结构：软件形态，≥200 个客户端授权。 2、可以支持中标麒、银河麒麟、中科方德操作系统。3 年质保工程师上门服务。 3、支持设置登录密码复杂度、口令长度以及鉴别次数、口令有效期等。 4、支持根据类型、时间进行操作日志查看，显示类型、时间、结果、描述等信息。 5、屏幕保护策略：支持停止鼠标、键盘操作超过设定时间后锁定屏幕。	200	套	585
	4	打印刻录安全	管理端（天融信 TSM）	1、系统结构：软件形态，配置≥1 个管理中心授权，且管理中心支持级联。 2、支持中标麒麟、银河麒麟、中科方德操作系统；兼容国产各系列打印机、刻录机。 3、支持图形化展示数据分析结果，可按	1	套	16770

				由。 3、支持域名控制，支持对多级域名进行控制，域名对象支持通配符。 4、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源提高访问效率，同时支持通过配置多条 DNSDoctoring，实现内网资源服务器的负载均衡； 5、内置邮件安全防护功能，支持邮件过滤.邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测； 6、支持 NTP DDOS 防护，采用阀值检查、源目的限流、源认证等方式综合进行 NTPREQUEST FLOOD、NTP REPLY FLOOD 击防护； 7、内置行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警;支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势； 8、支持一体化安全策略配置，策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置,简化用户管理； 9、支持 DNS DDOS 防护，可对 DNS QUERYFLOOD、DNS REPLY FLOOD、DNS 投毒攻击 DNS 格式检查、DNS NX 异常比率检测等;支持 DNS QUERY 源认证、DNS REPLY 源认证&源限速&目的限速&域名限速等多种手提供段综合防护； 10、 支持对病毒防御、入侵防御、DDOS 攻击等按照威胁类型/攻击主机/受攻击主机三种维度结合威胁等级和时间周期进行统计、排名。			

核心交换机	2	华三	H3CS7503E-M	1.机型：机箱式多插槽交换机 2.业务槽位数：≥3 3.性能：交换能力≥38.4Tbps，转发率≥12300Mpps 4.支持主控：支持主控模块冗余，主控冗余时模块间支持状态化故障切换 5.可靠性：支持虚拟化背板堆叠，即多台设备可以统一界面管理 6.支持 L3 MPLS VPN、支持 L2 VPN:VLL、支持分层 VPLS、支持 LDP 协议 7.实配支持静态路由、动态路由：OSPF、BGP、IS-IS，路由条目数≥128000 8.支持 IPv4/IPv6 双协议栈、支持多种隧道技术，支持 IPv4/IPv6 的组播技术 9. 支持 802.1×/macPortal/Radius/Tacaca＋认证 10.支持防火墙业务板卡、无线控制业务板卡扩展 11.有线无线一体化：支持原生的无线 AC 板卡或带 AC 功能的接口板，即支持无限 AP 管理功能。 12.本次配置：24 千兆电＋4 万兆光，单主控、双电源	4	台	9760
入侵检测	3	天融信	TopSentry 3000（ZX-A）（千兆）V3	1、标准式机架设备，配置兆芯芯片，中标麒麟操作系统；接口配置：≥6 个千兆电口，≥4 个千兆光口；冗余电源；满检速率≥3Gbps，最大并发连接≥100 万；实配独立攻击检测模块，≥1 年独立的特征库升级授权许可；实配独立应用识别模块，≥1 年独立的特征库升级授权许可；实配独立的僵尸主机功能模块，≥1 年独立的特征库升级授权许可；实配独立的地理信息模块，≥1 年独立的特征库升级授权许可。 2、支持独立的攻击检测引擎，涵盖 13000 种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级应用类型、流行程度等方式进行分类。 3、支持攻击取证、僵尸主机取证、恶意程序样本、恶意程序无风险样本、威胁情报样本、威胁情报取证、WEB 防护取证、异常流量取证，取证类型支持报文取证和样本文件取证两种形式。	2	台	49765

				4、支持对 HTTP 应用、IM 文件传输、P2P 下载、P2 音频、P2P 视频、标准协议、财经软件 电子商务、工控物联网即时通讯、加密隧道、软件更新、社交网络、数据库、网上银行、网络游戏、网页视频、网页音频、网络硬盘、网页邮箱、语音电话 远程控制、移动应用、其他应用等 24 种类型超过 5000 种应用识别。 5、支持卸载 SSL，实现对 HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、MOTT、SIP 等加密流量的分析检测； 6、支持联动阻断，能够与同品牌防火墙联动处置，可设置联动防火墙名称、地址、共享密钥、上报数据；支持展示防火墙联动状态、设置防火墙连接封堵时间。 7、自定义规则描述信息支持配置攻击类型、应用类型、风险等级、CVE、CNNVD、解决方案等信息。 8、支持 DDoS 自学习模式检测，可设定学习时长，根据周期内流量状态自动学习，设置检测流量阈值。流量异常触发成值系统自动进行告警。 9、支持工控漏洞攻击、车联网漏洞攻击、物联网洞攻击如对施耐德、Siemens、SCADA、SERVER-WEBAPPLinksysE 系列、IGSSSCADA 系统、罗克韦尔、华为 HG532 路由产品、Vivotek 智能摄像头、Xiaomi MiwiFiR3G 路径遍历漏洞攻击等。 10、支持 ARP 攻击检测，支持基于 ARP 请求的源 IP 不合法、响应的源 IP 不合法、响应的目的 IP 不合法、请求的源 MAC 与以太网源 MAC 不同、响应的源 MAC 与以太网源 MAC 不同、响应的目的 MAC 与以太网目的 MAC 不同进行检测。			
入侵防御	4	天融信	TopIDP 3000(ZX-A)（千兆）V3	1、标准式机架设备，配置兆芯芯片，中标麒麟操作系统；接口配置：≥6 个千兆电口，≥4 个千兆光口；冗余电源；满检速率≥6Gbps，最大并发连接≥100 万；实配独立攻击检测模块，≥1 年独立的特征库升级授权许可；实配独立应用识别模块，≥1 年独立的特征库升级授权许可；实配独立的僵尸主机功能模块，≥1	2	台	51040
				DDoS 检测、加密流量检测、URL 过滤、黑名单等多种安全事件日志信息记录；			

				年独立的特征库升级授权许可；实配独立的地理信息模块，≥1 年独立的特征库升级授权许可。 2、 支持能够检测和防护包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击等在内的 17 大类超过 13000 种以上网络攻击事件。 3、支持对攻击逃逸报文进行深度智能检测，包括 I 分片、ICP 分段、RPC 分片分段、SMB 分片分段、HTTP-Header 折叠、HTTP-Body UTF-7 编码、HTTP-Body UTF-16 (LE/BE 编码、HTTP-Body UTF-32 (LE/BE) 编码、HTTP-Body 压缩、HTTP-Post 数据编码、邮件体编码、URL 多重编码 URL 斜线分隔符、URI 相对目录欺骗、HTTP-Javascript 编码、邮件头折叠等类型。 4、支持对非加密协议 SMTP、POP3、IMAP 和加密协议 SMTPS、POP3S、IMAPS 中传输的钓鱼邮件进行检测和防护，检测到的钓鱼邮件可进行告警、取证和阻断，支持发件人欺骗、URL 欺骗、钓鱼 URL 检测功能。 5、支持 DNS 投毒检测防护。 6、支持联动阻断，能够与同品牌防火墙联动处置，设置联动防火墙名称、地址、共享密钥、上报数据；支持展示防火墙联动状态、设置防火墙连接封堵时间. 7、支持实时连接信息展示，展示字段至少包括:源 IP、目的 IP、源端口、目的端口、协议、应用、连接状态。支持连接排名实时监控，支持连接信息搜索。 8、支持对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测和防护，可设置相应警告、阻断动作并可设置忽略知名应用。 9、支持对攻击检测、僵尸主机、恶意程序、威胁情报、WEB 防护、异常流量、DDoS 检测、加密流量检测、URL 过滤、黑名单等多种安全事件日志信息记录:			

				支持一键加白操作;能够根据安全事件类型对应查看原始报文预览，并可进行报文下载；支持在设备界面进行解码操作，解码工具支持 Unicode、UTF-8、URL、HEXBASE6 等。 10、邮件监测可设置保护邮箱域名和允许访问位置，并支持设置对应检测类型包括异地登录、异地下载、境外访问、境外保护、境外删除。			
网络审计	5	天融信	TA-Net (ZX-A)V3	1、标准式机架设备，配置兆芯芯片，中标麒麟操作系统；接口配置：≥5 个千兆电口，≥4 个千兆光口；冗余电源；抓包速率≥900Mbps，记录事件能力≥22500 条/秒；实配独立攻击检测模块，≥1 年独立的特征库升级授权许可；实配独立应用识别模块，≥1 年独立的特征库升级授权许可；实配独立的威胁情报功能模块，≥1 年独立的特征库升级授权许可。 2、支持对 HTTP 协议进行内容审计，审计内容包括不限于:访问域名,HTTP 引用页、URL、HTTP 请求类型、HTTP 响应类型、请求文件、请求参数、访问行为、响应码、访问浏览器、服务器、Cookie、源目的 IP 地址、信誉分值等。 3、支持 DNS 域名解析协议审计，可针对 DNS 协议对域名解析进行审计,审计内容包括不限于查询 IP、查询域名、查询状态、应答域 RR 内容等。 4、支持即时通讯的文件传输内容审计，能审计发送者、接收者、传输文件名，支持显示文件大小、可对传输内容进行文件还原并下载，包括 QQ 文件传输等常见即时通讯。 5、支持应用协议行为识别，应用识别规则库最少分为 24 大类，支持 4000 种以上的应用协议自动识别与审计记录。 6、支持黑名单检测，支持黑 URL、黑 IP、黑域名、黑账号检测等审计策略，支持报文留存。支持黑 URL 地址、黑域名、账号多种匹配类型，包括子串匹配、左匹配、右匹配、完全匹配及正则匹配。 7、支持资产发现，支持指定网络中的在线资产识别，支持主动监测，对网络中设备资产进行发现和梳理，能够对资产	2	台	52175

				IP、资产状态、系统版本、开放端口进行安全监测。 8、支持异常流量检测，支持 flood 攻击检测、接口流量监测。支持配置异常连接检测周期、接口流量上限及总流量上线。 9、支持系统状态阈值设置，包括不限于 CPU 阈值设置、硬盘空间阈值设置、内存空间阈值设置等当使用率达到预定的阈值时，系统会发出报警。 10、支持云审计功能，包括安装 Agent 引流进行审计以及反向代理模式审计。支持的反向代理配置类型包括 HTTPS、TCP、UDP、FTP、SSH。			
（三）日常维护							
类别	序号	名称	日常维护工作具体内容		数量	单位	单价含税（元）
维保服务费	1	网络设备维护与管理	1、提供网络设备的安装、配置、维护和升级服务。 2、定期检查网络设备的状态，包括交换机、路由器、防火墙等，并及时进行故障排除和修复。 3、提供现场巡检服务，包括设备巡检、机房及井道环境巡检及线路巡检等，主要涉及常见故障，性能管理，用户管理，安全管理，备份管理等内容；维护工程师每月至少一天到现场进行相关工作，提供巡检、监控等日常服务，解决运行中的常见问题等； 4、每季度进行一次系统全面的巡检，并根据巡检情况出具一份内容详尽的巡检报告，包含设备版本，登陆方式，物理位置，现场环境，设备型号用处及性能等，对存在的问题及时进行沟通并解决，并及时提供系统巡检报告及改进意见； 5、管理网络设备的访问权限，确保网络安全。		36	月	8333.33333
	2	网络监控与故障处理	1、实时监测网络设备和网络流量，及时发现并解决网络故障。 2、维护单位提供 7×24 小时不间断热线电话支持服务，通过电话可以直接联络技术工程师，寻求问题的解决方案、技术文档以及技术指导，电话支持需及时响应。				

			3、整网网络系统进行摸查梳理，形成文档，包括全网网络拓扑、设备型号、软件版本、网络设备配置、管理 IP 地址、登录方式、物理位置等网络系统基础信息；同时对现网网络系统进行分析，针对分析出来的现网问题隐患，提出整改建议方案具体包括设备配置优化、组网结构调整、机房线路整理等。 4、进行网络故障的分析和排查，提供相应的解决方案和报告。			
	3	网络安全管理	1、提供网络安全策略的制定和实施，包括防火墙配置、入侵检测和防范、漏洞扫描等。 2、定期进行网络安全评估和漏洞扫描，及时修复发现的安全漏洞。 3、提供网络安全事件的响应和处理，包括入侵事件、病毒攻击等。			
	4	网络性能优化	1、分析网络性能指标，提供网络性能优化建议和方案。 2、优化网络拓扑结构，提高网络传输效率和带宽利用率。 3、监测网络流量，提供网络流量管理和负载均衡策略。			
	5	服务报告和统计分析	1、提供定期的服务报告，包括服务工作的内容、故障处理情况和网络性能分析等。 2、统计分析网络设备的使用情况和性能指标，提供相应的数据报告和建议。			