石景山电子政务外网基础能力提升项目
集成服务合同

合同编号：

项目编号：11010726210200018730-XM001

项目名称：石景山电子政务外网基础能力提升项目集成服务

甲　　方：北京市石景山区经济和信息化局

乙　　方：首都信息科技发展有限公司

本合同由以下双方经友好协商，本着平等互利的原则签订：

甲方：北京市石景山区经济和信息化局

地址：北京市石景山区石景山路 18 号

法定代表人：姜博

邮编：100043

联系电话：010-88699892

传真：010-88699665

联系人：许致远

乙方：首都信息科技发展有限公司

地址：北京市海淀区知春路 49 号 4 层西部 401 房屋

法定代表人：夏晓清

邮编：100086

电话：010-88511155

传真：010-62690609

开户行：中国银行北京市分行

银行账号：331156006031

联系人：刘学海

甲方：北京市石景山区经济和信息化局

乙方：首都信息科技发展有限公司

依据《中华人民共和国民法典》的规定，经甲、乙双方协商一致，同意就石景山电子政务外网基础能力提升项目集成服务，签订本合同。

第一条 定义

（一）“合同”指本合同及其附件。

（二）“合同总价款”包含货物的价格、货物到达甲方指定地点的运输费、保险费、税收、劳务费、维修费、保修费及相关安装、调试、系统集成、应用开发、服务、验收、培训（不包括学员往返的差旅、住宿费）、系统备品备件、各种资料专用工具等保障甲方正常使用本合同项下所购货物及服务的一切费用。

（三）“货物”指本合同项下乙方须向甲方提供的硬件设备、软件、文档、备品备件等。

（四）“服务”指根据合同规定乙方应提供的有关设计、交货、安装、调试、集成与开发、试运行、验收、项目管理、培训、技术服务、售后服务，其他使系统正常运转所必需的服务等。

（五）“文档”是指用来描述产品的内容、组成、设计、功能规格、开发情况、测试结果及使用方法的文字资料和图表，如产品设计说明书、用户使用手册等。

（六）“甲方技术部门”是指代表甲方行使和履行合同中甲方技术部分权利和义务的甲方内部职能部门。

（七）“货币”指合同中涉及的货物及服务所采用的货币计量单位。本合同项下货物及服务均以人民币计量。

（八）“天”“日”指日历日。

（九）最终用户是指使用本合同项下所购货物的甲方及各派驻部门。

第二条 合同文件

下列文件构成本合同的组成部分，应视为一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先级次序如下：

a) 本合同书；

b) 合同附件。

第三条 合同内容及要求

本合同项下乙方需提供的货物及服务具体品牌/型号、规格参数和数量详见附件。

第四条 品质与保证

（一）乙方保证提供的货物为全新的厂商原装货物。该货物采用原厂包装，货物或其包装上必须标识货物的品牌、厂商及产地，提供货物厂商提供的货物装箱清单及货物质量检验合格证书。

（二）乙方提供货物及服务须满足技术需求，包括功能、可靠性、易使用性、可维护性、可移植性、产品使用性能等；货物规格、配置和技术参数等应满足附件中的要求，保证甲方在正常使用下，在其使用期内，均能够满足规定的性能、可靠性和扩展性，同时符合相关法律法规的规定。

（三）乙方保证提供的技术资料具有正确性、简明性、可操作性和规范性。

第五条　包装、运输与保险

（一）乙方提供的货物应为原厂包装，能够防止货物在正常运输中损坏或变质，每件包装箱内应附一份详细装箱清单和质量合格证。货物包装应采取防潮、防晒、防锈、防腐蚀、防震动及防止其他损坏的必要保护措施，从而保护货物能够经受多次搬运、装卸及长途运输。乙方应承担因包装或防护措施不当所造成任何损失的责任。

（二）乙方负责安排恰当的运输工具，并支付运费，确保按期交货。

（三）乙方负责为货物和在项目现场进行技术服务的乙方人员办理必要的保险并支付相关保险费，该保险的期限至货物到达甲方项目现场且通过终验为止。

第六条　交付与项目初验

（一）交付地点：甲方指定地点。

（二）交付时间：交付时间根据甲方需要可分批进行。

（三）货物运抵交付地点，甲方应进行验收，货物验收范围包括型号、规格、数量、设备包装、外观质量、软件介质、配件、货物装箱清单及货物质量检验合格证书等文件、资料。货物验收合格，甲乙双方签署《到货签收单》，该签收单并不免除乙方的产品质量责任。在双方签署《到货签收单》之前，所有货物的灭失毁坏风险由乙方承担。

（四）在交付验收过程中，因乙方原因交付货物的部分或全部不符合本合同约定的数量、质量标准，外观变形或损坏等情形，乙方应按甲

方要求在3日内更换、补齐，确保所交付的货物完好无损。否则甲方可以拒绝接受该货物或解除本合同；如因乙方交付的瑕疵货物使得本合同目的不能实现，导致甲方解除本合同的，乙方应退还全部已付费用，由此给甲方造成的损失由乙方赔偿。

（五）项目初验：项目包含的全部设备的安装部署、联调测试、网络配置，功能实现等工作完毕后，甲方进行初验，具备试运行条件的，甲乙双方签署《项目初验报告》；不具备试运行条件的，乙方应在甲方指定期限内完成整改。

（六）自合同签订之日起1个月内完成项目包含的全部设备的到货验收工作及完成项目包含的全部设备的安装部署、联调测试、网络配置，功能实现等工作，通过项目初验，具备试运行条件。

第七条　安装、调试与终验

（一）实施根据甲方需要分批进行。乙方应在接到甲方书面通知后7个工作日内，完成指定单位的设备安装、加电、测试、调试等实施服务，签署《设备安装调试报告》。

（二）试运行期限为30天，试运行完成后达到项目要求后开展验收工作。在试运行期间，若因乙方原因（包括但不限于设备硬件故障、软件缺陷、配置错误等）导致系统停机、关键业务中断或发生重大安全事件等，致使系统无法连续稳定运行的，甲方有权要求乙方进行整改；整改期间试运行中止计算；自系统修复并重新恢复正常运行之日起，试运行期重新计算，直至连续稳定运行满30天为止。

（三）项目验收服务。试运行完成后乙方于7个工作日内向甲方提交《项目验收申请》，甲方按相关要求进行终验，验收通过后签署《项

目终验报告》。

第八条　保修

（一）保修期限：项目经甲方终验通过后，所有货物及配件开始进入为期3年的原厂质保期。对于本项目涉及的所有软硬件产品，质保期为3年；保修期内，对于带有存储记忆功能的产品及配件（如硬盘等）提供不回收质保服务。

（二）保修日期自双方签署《项目终验报告》之日起计算。

（三）保修期内，乙方免费更换正常使用下损坏的配件；免费提供7*24小时（每周7天，每天24小时，下同）厂商软硬件质量保障服务和维护服务、定期对硬件和软件进行健康状况检查、免费升级、备份软件版本升级、补丁程序及技术支持等服务。若乙方需将有故障的货物或部件运至乙方指定的维修中心，乙方负责将货物运至乙方指定地点及运回甲方指定地点，由此发生的一切费用由乙方承担。乙方应免费提供备用更换件，以保障本合同项下系统正常运行。

（四）保修期内更换的配件必须是厂商生产的未使用过的原厂配件。

（五）保修期内，乙方提供的货物及相关部件配件发生故障损坏进行更换的，更换部分的保修期自更换后重新起算3年。同一部位部件发生3次以（含）上故障的，乙方必须更换相应部件。

第九条　售后服务

乙方应在货物部署地设立专门的售后服务机构，在货物的保修期内和厂商为甲方提供下列标准的服务，对于本项目必须保证售后服务至少

应达到以下服务水平：

（一）自系统终验合格之日起，乙方必须安排经甲方认可的技术人员提供 7*24 小时现场技术支持或电话技术支持服务（包括热线电话和传真支持服务），负责保修期内免费的系统日常维护及故障处理。如系统在质保期间出现故障，乙方应在接到甲方故障通知 10 分钟内及时响应；关键业务在接到甲方故障通知后 2 小时内解决故障并恢复业务运行，其他业务在接到甲方故障通知后 4 小时内解决故障并恢复业务运行。

（二）乙方应负责解决运行中出现的设备故障或系统故障。针对出现的故障，进行现场故障分析，并在故障解决后 12 小时内，向甲方提交故障处理报告，报告中必须说明故障种类、故障原因、故障处理方法等。同时负责针对引发故障的原因，给出日常运维建议或维护方案，避免同类故障再次发生。

（三）乙方应按季度对故障处理报告进行分类、统计、汇总、分析，逐步完善日常运维知识库，并提交甲方。

（四）本合同项下货物及安装调试、运行、服务等均在保修期内容和范围（产品、技术、模块）内，系统服务范围至少包括运维支持、系统迁移、系统升级、性能调优、设备维修、技术咨询、设备迁移、各种突发事件的应急策略、定期巡检等。

（五）乙方需向甲方提供保修期外的维护内容和范围（产品、技术、模块）以及年度维护费用报价清单。

（六）保修期内，如甲方要求乙方提供现场技术支持服务，乙方应当派人员到现场提供技术支持、维修维护服务，由此产生的一切费用均

由乙方承担。

第十条　培训

（一）总则

■乙方必须提供高水平的培训，负责为甲方所辖最终用户及相关部门培训技术人员。

■乙方派出的培训教员应具有丰富的理论知识和相应实践经验。

■乙方必须为被培训人员提供有关培训文字资料和讲义等用品。

■乙方必须提供相应的培训网络环境用于培训人员实际演练。

■乙方和厂商的培训课程和培训教员的安排必须得到甲方书面确认，如果甲方不满意，提出人员更换要求，乙方应在不增加费用的前提下进行调整和更换，直到符合甲方需求。

（二）培训人数、时间、地点、课程要求

■培训时间：具体的培训方式和时间安排由甲方和乙方协商确定。

■培训地点：具体地点由甲方和乙方协商确定。

■培训内容：具体内容由甲方和乙方协商确定。

■培训人数：具体人数由甲方和乙方协商确定。

■培训课程设置：培训课程的设置必须适应甲方所辖上述最终用户及相关部门的实际情况，以完成本项目的培训目标为目的。培训课程应包括基本配置、调试、诊断命令及常用的维护服务工具软件的讲解等。

第十一条　合同价款的支付

（一）合同金额：人民币（大写）壹仟零壹拾万零陆仟柒佰柒拾贰元整（¥10,106,772.00），此价格为含税价格。

（二）支付期限及金额：

阶段	说明	付款金额（元）	（人民币大写）
首付款（60%）	签订合同后十五个工作日内支付。	6,064,063.20	陆佰零陆万肆仟零陆拾叁元贰角整
进度款（30%）	通过初验后十五个工作日内支付。	3,032,031.60	叁佰零叁万贰仟零叁拾壹元陆角整
尾款（10%）	项目终验完成后十五个工作日内支付。	1,010,677.20	壹佰零壹万零陆佰柒拾柒元贰角整

乙方申请支付的同时需先向甲方提交等额的增值税普通发票，若乙方在甲方支付前未能开具发票或开具发票有误，甲方有权暂缓支付。

（三）本合同金额为乙方完成本合同项下全部合同内容所需全部费用，甲方不再向乙方支付其他任何费用。如有本合同履行内容相关费用的增加，由乙方自行承担。

（四）为保证乙方履行质保和售后义务，乙方需向甲方提交有效期至少为三年（覆盖质保期）由甲方认可的银行或担保机构出具的、不可撤销的、见索即付独立保函，保函担保金额为合同总额的 5%。当乙方未履行保修及售后服务义务时，甲方有权要求银行或担保机构履行担保义务。

第十二条　违约责任

（一）如乙方未能履行合同规定的相关义务，甲方有权要求乙方赔偿损失。

（二）因乙方及原厂商技术人员服务问题造成生产安全事故的，由

乙方赔偿甲方由此遭受的损失。因乙方所提供货物或服务造成甲方或任何第三方损害的，由乙方承担全部责任。

（三）乙方及原厂商未经甲方用户书面同意，擅自更换技术服务人员或者未能按时更换不符合要求的技术人员导致甲方发生损失的，甲方有权要求乙方赔偿相应损失。

（四）因乙方原因，在合同约定期限内未完成货物到货、安装、调试、测试，未能通过项目初验、进入试运行的，每逾期一日应按合同总价款千分之一支付违约金，逾期15日的，甲方有权单方解除合同，乙方应退还甲方已支付的全部款项并赔偿甲方全部损失。

（五）试运行期间设备系统出现运行故障等，乙方未按甲方要求的期限整改完成，或出现两次设备运行故障问题，甲方有权单方解除合同，乙方应退还甲方已支付的全部款项，并按合同总金额的20%向甲方支付违约金，如违约金不足以弥补甲方实际损失，乙方应赔偿甲方全部损失。

（六）如果由于乙方货物质量原因引起系统停业故障，视为服务未达标一次，乙方除延长相应保修期外，每出现一次还应支付相当于合同总金额0.1%的违约金，并赔偿给甲方所造成的经济损失。

（七）保修期内，乙方及原厂商未能按合同的约定提供维修服务或不能在承诺时间内修复故障，甲方有权请其他专业服务公司进行维修，由此造成的费用和损失由乙方承担。

（八）乙方违约造成甲方的费用增加和损失，甲方有权从待支付的合同剩余款项中直接扣除，如待支付的合同剩余款项不足以弥补甲方上述费用和损失，乙方应向甲方支付不足部分款项。

（九）乙方应赔偿甲方的损失范围包括但不限于甲方直接经济损失、向第三方承担的违约金赔偿金、律师费、诉讼费、保全费、保函保费等所有损失。

第十三条　知识产权与保密

（一）未经对方同意，任意一方不得以任何形式公开本合同及其附件的任何内容；

（二）各方在未征得对方同意的情况下，不得向第三方泄露在项目中涉及的任何情报、资料和数据；

（三）各方在未征得对方同意的情况下，不得为任何其他目的而自行使用或允许他人使用从对方获得的信息（包括但不限于所有的报告、摘录、纪要、文件、计划、报表、复印件和业务数据等），但社会公众可以通过合法渠道得知的信息除外；

（四）乙方应对参与项目的工作人员进行保密教育，严格遵守有关保密的法律法规，任何人不得将与本项目有关的资料信息泄露给与本项目无关的第三方；

（五）如果一方违反本条款的规定，并给对方造成损失，违约方应向守约方承担赔偿责任。触犯保密法律法规的情况由违约方独自承担相应法律责任；

（六）乙方保证，其根据本合同提供的货物及服务没有任何权利瑕疵，具有完全的知识产权或相应授权，并不侵犯任何第三方的合法权益，甲方在使用该货物或服务的任何一部分时，免受第三方提出的侵犯其知识产权或其他权益的起诉。如果任何人对甲方使用该货物及服务主张权利，由乙方负责处理一切纠纷及相关事宜。由此给甲方造成的损失，由

乙方承担，其承担范围包括但不限于：赔偿费、诉讼费（包括但不限于保全费、受理费、律师费及其他合理支出的费用）和相关的费用。基于本合同履行所产生的新成果的全部知识产权归甲方所有。

第十四条　不可抗力

（一）由于发生不能预见、不能避免并不能克服的不可抗力情形，致使直接影响本合同的履行或不能按照本合同项下之约定履行时，遇有不可抗力的一方应当立即书面通知对方，并在发生不可抗力之日起 5 天内，提供不可抗力详情及合同不能履行或部分不能履行，或需要延期履行理由的有效书面证明，该项证明文件应当由不可抗力发生地的公证机关出具。

（二）根据不可抗力对本合同的影响程度，双方应当协商是否解除本合同或部分、全部免除履行本合同的责任，或延期履行本合同。

第十五条　合同争议的解决

因本合同引起与本合同有关的一切争端双方应首先通过友好协商解决。如果协商不能解决，任何一方可向甲方所在地有管辖权的人民法院提起诉讼。

第十六条　合同的转让和修改

（一）合同双方都不得单方面修改合同内容。拟修改合同内容的一方应当就修改事项列明拟修改条款后以书面形式通知对方，双方协商同意后，应就修改条款签订补充协议。补充协议必须经双方法定代表人或授权代表签字并加盖公章后方可生效。补充协议为本合同的组成部分，一经签署即具有法律效力。补充协议与本合同内容不一致的，以补充协

议为准。

（二）未经双方书面同意，任何一方不得将本合同规定的权利和义务转让给第三方或委托第三方代理。

第十七条　合同的生效及其他

（一）本合同经双方法定代表人或授权代表签字并加盖公章后生效，合同一式肆份，甲乙双方各执贰份，均具有同等法律效力。

（二）本合同未尽事宜，按中华人民共和国有关法律法规办理。

（三）附件：项目清单

（以下无正文）

甲方：北京市石景山区经济和信息化局

地址：北京市石景山区石景山路18号

邮编：100043

电话：010-88699892

传真：010-88699665

（盖章）

法定代表人（或授权代表）签字：

日期：2026 年 5 月 29 日

乙方：首都信息科技发展有限公司

地址：北京市海淀区知春路 49 号 4 层西部 401 房屋

邮编：100086

电话：010-88511155

传真：010-62690609

（盖章）

法定代表人（或授权代表）签字：

日期：2026 年 5 月 29 日

项目清单：

序号	分项名称	品牌/型号	规格参数	数量	单价	合计
1	二级单位防火墙	启明星辰/USG-FW-N-G1110-DNRSJ	网络层吞吐量4Gbps，应用层吞吐量3.2Gbps，防病毒吞吐量800M，IPS吞吐量1.1Gbps，最大并发连接数400万，每秒新建连接数4.5万。 采用国产芯片及国产操作系统，1U设备，千兆电口6个，千兆光口4个，内存8G，内置ssd硬盘128G,双电源，开启IPS、AV、上网行为管理特征库升级服务3年，三年质保。 支持IPv6/IPv4翻译策略技术，包括支持静态NAT-PT、动态NAT-PT技术。 支持一体化安全策略配置,可以通过一条策略实现用户认证、IPS、AV、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。 支持基于策略的入侵检测与防护,可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。 支持基于策略的病毒扫描与防护,可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略。	40	45,000.00	1,800,000.00

			支持专业的 HTTPFlood 攻击防护；可以实现 get 和 post 的攻击防护，且 get 防护算法支持 4 类；支持独立 url 处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制。 支持静态路由，动态路由（OSPF、RIP、BGP、ISIS 等），VLAN 间路由，单臂路由，组播路由等。 支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。 支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。 可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。			
2	市政接入区防火墙	深信服 /AF-1000-L2200-9Q	品网络层吞吐量 20G，应用层吞吐量 15G，防病毒吞吐量 2G，IPS 吞吐量 2G，并发连接数 800 万，HTTP 新建连接数 16 万。 设备采用国产芯片及国产操作系统，内存 16G，硬盘容量 128G SSD，电源：冗余电源，接口 6 千兆电口+4 千兆光口 SFP。 支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势。 支持对≥9000 种应用的识别和控制，应用类型	1	75,000.00	75,000.00

			包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 内置漏洞规则库，支持在控制台界面查询漏洞特征信息，支持用户自定义 IPS 规则。 支持僵尸主机检测功能，内置僵尸网络特征库，可识别主机的异常外联行为。 支持勒索病毒防护功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略。 支持病毒扫描与防护，支持压缩病毒文件进行检测和拦截，压缩层数 15 层及以上。			
3	市政接入区 IPS	深信服 /NIPS-1000-L2200-3F	网络层吞吐量 20G，应用层吞吐量 15G，防病毒吞吐量 2G，IPS 吞吐量 2G，并发连接数 800 万，HTTP 新建连接数 16 万。 采用国产芯片及国产操作系统，内存 16G，硬盘容量 128G SSD，电源：冗余电源，接口 6 千兆电口+4 千兆光口 SFP。 支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势。 内置≥15000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE	1	120,000.00	120,000.00

			标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 支持僵尸主机检测功能，内置僵尸网络特征库≥128 万种，可识别主机的异常外联行为。 支持事前账号脆弱性、事中账号爆破、事后账号失陷的账号全生命周期安全防护，支持详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口等。 支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。			
4	交换机	华为/S5731-H48T4XC	交换性能 2/20Tbps；包转发率 620Mpps；千兆电口 48 个，万兆 SFP+光口 4 个。 支持 IPv4 和 IPv6 双协议栈；同时支持静态路由、RIP、RIPng、OSPF、OSPFv3 协议； 支持策略路由，支持路由策略。 支持基于端口的 VLAN，支持基于协议的 VLAN； 支持基于 MAC 的 VLAN；最大 VLAN 数 4K。 实配冗余电源；支持高可用，支持虚拟化。	4	18,000.00	72,000.00
5	交换机	华为 /S5735-L48T4X-A1	交换性能 432Gbps/4.32Tbps；包转发率 162Mpps；千兆电口 48 个，万兆 SFP+光口 4 个。 支持 IPv4 和 IPv6 双协议栈；同时支持静态路由、	7	6,000.00	42,000.00

			RIP、RIPng、OSPF、OSPFv3 协议；支持策略路由，支持路由策略。 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN；最大 VLAN 数 4K。 实配冗余电源；支持高可用，支持虚拟化。			
6	IPV6 功能授权	华为/CE12808，IPV6 功能授权	Huawei CE12808 交换机 IPV6 功能授权激活，软件需要升级至 V200R19C10SPC800 版本。	2	10,000.00	20,000.00
7	IPV6 功能授权	华为/交换机 S7706，IPV6 功能授权	Huawei S7706 交换机 IPV6 功能授权激活，软件版本需升级至 V200R013C00SPC500。	2	8,000.00	16,000.00
8	光模块	华为 /eSFP-GE-LX-SM1310	1310nm,10km,LC，单模双纤。	50	1,000.00	50,000.00
9	光模块	华为 /eSFP-GE-SX-MM850	850nm,0.55km,LC，多模双纤。	7	800.00	5,600.00
10	光跳线	耐威迪 /130S2LCLC-05M	5m 单模双纤。	50	133.00	6,650.00
11	互联网业务区权威 DNS-硬件	ZDNS/S6100-SD80K	设备采用国产芯片及国产操作系统；内存 16G；硬盘 1T；1 个串口，2 个 USB，8 个千兆电口，支持扩展千兆光口 4 个和万兆光口 4 个;配置交流冗余电源，故障电源更换支持热插拔。 单台设备 DNS 服务每秒查询次数 QPS≥80,000。 支持基于 ICMP、UDP、TCP_SYN、TCP、HTTP、HTTPS、FTP、SMTP、SNMP、TCP_KEEP、SNMP_LINK、DNS、	2	55,000.00	110,000.00
12	互联网业务区权威 DNS-软件授权	ZDNS/红枫下一代互联网域名服务软件 V3.0		2	220,000.00	440,000.00

			MYSQL 等的应用健康检测模板定制；支持对探测失败容忍时间进行设置，即探测失败时间超过容忍时间时才会对解析产生影响，不因某一个探测任务的结果进行判定。从而保证业务的真实性。 支持应用状态探测变更、多个探测模板中任一探测状态变更、节点间信息同步时连接状态变更均支持告警；支持对单个服务器单独配置探测协议，也可以通过资源池对引用的服务器指定公共的探测协议；支持探测节点间有冗余机制，当主用探测节点异常时可以由其他探测节点或者备份探测节点自动接替服务；支持域名级设置动态兜底的失败应答策略，减少人工重复配置。 支持对 A、AAAA、CNAME、NAPTR、SRV、MX 类型的域名配置首选和次选负载均衡算法，首先负载均衡算法至少包含静态就近性、轮询、加权轮询、全局可用性、CPU/内存、动态就近性、多维度可用性、丢包率；次选负载均衡算法至少包含轮询、加权轮询、全局可用性、CPU/内存、动态就近性、备选 IP、丢包率、静态保持。 支持 NXDOMAIN 转换功能，权威解析支持 NXDOMAIN 转换为 NOERROR，递归同样支持 NXDOMAIN 转换为 NOERROR。			

13	公共服务区权威 DNS、IPAM、DHCP、域名管理-硬件	ZDNS/S6100-SD80K	设备采用国产芯片及国产操作系统；内存 16G；硬盘 1T；1 个串口，2 个 USB，8 个千兆电口，支持扩展千兆光口 4 个和万兆光口 4 个；配置交流冗余电源，故障电源更换支持热插拔。 单台设备 DNS 服务每秒查询次数 QPS≥80,000； 单台设备 DHCP 服务每秒查询次数 LPS≥500。 支持自定义探测设备关联自定义健康检查模板对服务成员进行拨测，多个探测设备可以跨数据中心组成探测组，当选择多个探测设备组成探测组时支持轮询和全局可用的探测策略。支持对探测失败容忍时间进行设置，即探测失败时间超过容忍时间时才会对解析产生影响，不因某一个探测任务的结果进行判定。 支持活跃地址功能，正常活跃地址解析，服务节点数量在限制区间中，解析结果可以正常返回； 支持自定义设置探测组，设置内容包含探测策略、探测设备、且多设备之间探测结果相互同步，探测节点相互冗余。 支持 EUI-64 算法，支持 DHCPv6 下的 EUI-64 地址下发，且后缀地址生成基于 EUI-64 算法进行。 DHCPv6 地址下发支持动态前缀，支持 DHCPv6 无状态地址下发(下发信息方式包括动态前缀和固	2	55,000.00	110,000.00
14	公共服务区权威 DNS、IPAM、DHCP、域名管理-软件授权	ZDNS/红枫下一代互联网域名服务软件 V3.0		2	250,000.00	500,000.00

			定前缀两种方式）。 支持创建 IPv6 地址规划方案并设置固定前缀。支持在地址台账中应用 IPv6 规划方案，可以便捷添加 IPv6 网络。支持通过规划地图直观展示全网的 IPv6 地址规划情况。支持按照图形化方式拖拽规划 IPv6 地址空间，且每个空间标记不同的业务类型。支持为各地址空间配置空间标识，同时关联与上级标识并形成可落地的 IPv6 编址方案。 支持域名分级分层配置下发，支持对三级及以上域名进行 WEB 网管，且下级单位 DNS 节点可以作为本级域名管理节点的同时承接上级管理平台下发配置项（配置项包括上级域名授权、本级 DNS 域名、DNS 视图、本节点账号管理权限）。 支持节点集中管理，支持运行信息同步展示，下级节点的运行信息可以实时同步到上级管理平台展示（展示信息包括：CPU 使用率、CPU 温度、内存使用率）。 支持前台一键导出 DNS 配置项进行快速备份（导出的数据包含：视图配置、区配、域名记录配置、转发配置、域名调度对象、本地安全策略等）。			
15	公共服务区递	ZDNS/S6100-SD80K	设备采用国产芯片及国产操作系统；内存 16G；	2	55,000.00	110,000.00

	归 DNS-硬件		硬盘 1T；1 个串口，2 个 USB，8 个千兆电口，支持扩展千兆光口 4 个和万兆光口 4 个;配置交流冗余电源，故障电源更换支持热插拔。			
16	公共服务区递归 DNS-软件授权	ZDNS/红枫下一代互联网域名服务软件 V3.0	单台设备 DNS 服务每秒查询次数 QPS≥80,000。 做为递归服务器，支持通过 ECS 技术携带请求源地址，并可按指定映射关系替换 ECS 中源地址，满足权威服务器按照源地址智能调度需要。支持转发服务器分组，支持转发服务器健康探测和异常告警，对异常服务器支持复检，保证异常服务器恢复后快速可用。支持转发服务器按照预设的权重比例进行转发。 支持隧道攻击防护：支持对 DNS 请求类型、请求内容、及其规则特点的识别，配置相关参数（数据包大小、阈值频率、防护周期、TXT 类型防护启用、TXT 阈值频率、TXT 防护周期等）对 DNS 协议数据进行深度检测，对异常通信数据及时发现并阻断。 支持 DOT/DOH 功能，满足 DNS 报文传输安全需要，DOT/DOH 支持按 ACL 进行缓存分区和缓存管理功能。 支持解析拨测，可进行批量域名的拨测和多 DNS 间解析一致性对比；支持解析状态监控，可对内	2	240,000.00	480,000.00

			网域名解析情况监控，解析延迟、解析结果准确度、解析异常等指标进行实时拨测。			
17	零信任安全控制中心	深信服/aTrust-1000-LS1060C	理论并发用户数（个）≥ 6000。 实配零信任用户并发授权 2000；实配零信任沙箱授权数 1500。 2U，内存大小 16G，硬盘容量 480G SSD，电源：冗余电源，接口 6 千兆电口+4 千兆光口 SFP+2 万兆光口 SFP+，设备采用国产芯片及国产操作系统。 支持加密算法 SM1、SM2、SM3、SM4。 控制中心支持至少 2 个节点组建分布式集群，支持对集群节点的线路进行健康检查。集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。 在 WEB 模式发布资源时，支持发布 IP 或域名形式的后端服务器地址，支持配置业务应用的具体访问 URL 路径。 在隧道模式发布资源时支持发布 IP、IP 范围、IP 段及具体域名等形式的服务器地址。 支持本地账号密码认证、LDAP/AD 认证、OAuth2.0 标准协议的票据认证、CAS 标准协议	2	460,000.00	920,000.00
18		深信服/零信任接入授权		2000	120.00	240,000.00
19		深信服/零信任统一端点管理授权		1500	180.00	270,000.00

			的票据认证、Radius 账号认证、HTTPS 帐号认证等认证方式。支持配置在触发异常环境的条件时，用户需进行增强认证。 支持配置动态访问规则，支持对终端环境、用户身份、处置动作等进行配置。 支持划分虚拟网络域，实现用户登录零信任客户端后，在特定的网络域下只能主动访问网络域对应的 IP、IP 范围、IP 段、域名。 具备单包授权能力（SPA），未授权用户无法连接零信任设备，无法扫描到服务端口；支持以黑白名单的方式进行入侵防御，攻击者无法执行白名单外的攻击命令；支持 WAF(WEB 防护)，阻断基于 WEB 对设备发起的攻击。 零信任客户端兼容主流非国产终端，包括但不限于：Windows7 以及上版本、MacOS10 及以上版本以及 Android、iOS 非国产操作系统的终端；支持 IE8 及以上版本、Chrome 69 及以上版本、Edge、Firefox、Android、iOS、国产操作系统浏览器接入并访问 WEB 资源；支持管理员自行配置内网 DNS 解析，实现终端用户在零信任客户端登录后可以使用单位自建的内网 DNS 进行域名解析。			

			4、零信任客户端需同时兼容主流国产化 CPU 和国产化操作系统，CPU 包括：龙芯、飞腾、兆芯、海光；操作系统包括：麒麟、统信。 支持针对发布的 WEB 应用开启 WEB 水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露。 支持不同平台的终端同时在线，管理员可分别设置可同时在线的 PC 或移动终端个数、支持绑定授信终端。 支持 iOS、安卓、鸿蒙等主流手机 APP 集成零信任 SDK，实现安全接入、沙箱等功能。支持通过控制台上传 Android、iOS 原包应用进行自动封装，使 APP 具备零信任接入能力。支持单点登录功能，自动为 APP 用户填入管理员配置的接入地址及用户名账号等信息。 支持配置用户在满足特定条件的情况下才启用沙箱准入策略，条件配置项应包括但不限于：计算机名称、计算机 MAC 地址、运行进程、安装指定软件、零信任客户端版本、用户接入 IP、用户登录时间等。支持工作空间与个人空间的网络访问权限隔离。 支持在 PC 终端上基于沙箱技术生成隔离的安			

			全工作空间，实现 PC 端数据防泄密，PC 沙箱支持 Windows、macOS 系统以及统信 UOS 及麒麟 Kylin 等国产化系统。文件加密支持每个文件独立密钥，以确保沙箱组件被卸载、模块驱动被摘除的情况下，终端用户无法明文取出文件。支持基于设备/账号/终端三道防线的安全能力和效果的可视化及量化。支持基于用户、IP 产生的风险行为、可信行为等自动计算该用户的风险得分。支持通过还原用户接入系统后的会话信息，对用户访问行为进行自动分析并智能生成分析报告。 支持为沙箱工作空间文件导出功能创建审批模板；审批流程支持配置多级审批节点。支持配置允许/禁止工作空间文件导出到个人空间、开启文件审计功能功能，文件导出支持审批功能。支持启用剪切板内容审计，开启后将对工作空间到个人空间的拷贝行为进行审计，审计日志将上报到分析中心。支持为不同的工作空间关联不同的应用，为不同的工作空间关联不同的用户或用户组并配置相应的安全策略。			
20	零信任安全代理网关	深信服/aTrust-1000-LS1060	理论加密流量≥600Mbps，理论并发用户数≥6000。	2	380,000.00	760,000.00

		G	2U，内存大小 16G，硬盘容量 480G SSD，电源：冗余电源，接口 6 千兆电口+4 千兆光口 SFP+2 万兆光口 SFP+，满配光模块，设备采用国产芯片及国产操作系统。 支持加密算法 SM1、SM2、SM3、SM4。 支持本地集群部署，支持最少 2 台设备组建集群，集群中的节点可承载工作负载功能，不依赖其它外置设备。 支持将零信任安全接入平台的 WEB 资源访问流量解密，而后镜像给外部网络流量分析系统，如态势感知等设备，完善系统的用户行为审计溯源能力。防爆破：支持配置同 IP 用户连续登录错误超过上限时锁定 IP，并支持设置指定时长后自动恢复。防机器人：防机器人输入，提供强安全性的点击图像校验码机制。 支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告。 支持控制台超时时间配置检查，以及管理员登录防爆破、管理员首次登录强制修改密码的安全性登录配置检查。			
21	零信任数据	深信服/aTrust-1000	确保所投软件兼容国产 CPU 物理机或虚拟化平	1	450,000.00	450,000.00

	分析中心	V2.0A	台运行，同时配套提供国产操作系统等支撑软件。日志性能（EPS 每秒）≥1000。 支持管理员创建多种蜜罐（包括“SSH 蜜罐”，“FTP 蜜罐”，“HTTP”蜜罐），具备对应的协议特征用于欺骗攻击者，但不响应攻击者交互命令。支持应用诱饵伪装应用资源，支持管理员创建多个应用诱饵，下发到用户终端，将访问应用诱饵的请求引流至对应的蜜罐。支持管理员创建多种终端诱饵，并下发至用户终端，主动引诱攻击者查看并访问诱饵中的地址。支持管理员自定义蜜罐访问后的处置策略，锁定访问蜜罐的用户账号，自动发送告警提醒管理员等策略。 支持基于设备、账号、终端三道防线进行纵深防御分析，实现零信任 SDP 安全能力和效果的可视化及量化。基于全网用户数据，提供实时的大屏展示，展示登录、并发授权、终端、应用访问、地点实时信息。 支持通过还原用户接入系统后的会话信息，对用户访问行为进行自动分析并智能生成分析报告，展示整个访问过程，对关联的终端进行整体分析。 支持对接零信任控制中心设备日志。			

22	零信任高级威胁检测中心	启明星辰/TSOC-CSA-XDR8800XCSJ	网络流量的实时接收采集能力(多路)为25000EPS或日志数据采集流量为6Gbps。 采用国产芯片及国产操作系统，2U，CPU为64核，内存为256G，硬盘为48T，支持RAID50，其中SSD存储为960G。千兆电口4个，千兆光口2个，万兆光口4个，2个接口扩展槽，冗余电源。 支持8块大屏从多角度多维度的进行态势数据的呈现，包括态势总览、外部攻击态势、资产态势、运行态势、脆弱性态势、风险态势、情报态势、流态势等态势大屏。 支持以事件列表展示聚合后的安全事件,展示维度需支持事件名称、评分、标签、事件等级、事件状态、处置状态、创建时间、更新时间等维度，同时可对具体安全事件可查看事件详情及处置动作。 支持告警可视化分析,通过自定义方式创建告警可视化图表,用户可选择大字报、多彩标签表格、折线图、面积图、纵向柱状图、横向柱状图、饼状图、环形图、散点图、词云图、环形柱状图等方式对日志信息进行统计,统计方式包括但不限于计数、唯一计数、平均值、求和、最大值、最	1	700,000.00	700,000.00

			小值、占比等，参与统计的告警字段支持告警信息所有字段，支持预览，并支持发布到仪表板的面板库，方便仪表板进行告警数据分析。 支持形象地展示出安全域的风险矩阵，从可能性和影响性两个角度标注安全域中资产风险的分布情况，通过风险矩阵法，指导管理员进行风险分析，采取相应的风险处置对策。 内置24种安全场景的专项分析，每种场景需支持独立页面查看其详情，需支持但不限于如下场景：弱口令场景、失陷主机场景、挖矿软件发现场景、僵木蠕场景、横向访问、外部访问、可疑外联、扫描探测、可疑进程、webshell上传/访问、WEB攻击、DGA发现场景、隐蔽隧道、带外查询、代理、内网穿透、远程控制软件、反弹shell、TOR场景、暴力破解场景等等。 支持针对私域大模型基础设施设备安全场景分析，支持基于日志、流量和性能监控，对大模型应用基础设施设备场景安全进行分析；对于用户业务中的大模型基础设施所发生的安全日志进行分析，对大模型日常交互使用流量进行分析，对大模型的CPU、GPU、内存、存储进行监控。 支持按照不同扫描引擎厂商，开启对应的高级配			

			置参数能力，包括但不限于配置任务优先级、通知被扫主机内容、扫描延迟、主机存活探测、扫描速度、插件超时限制、socket 超时限制、危机插件扫描、最大重连次数、猜测时间、猜测间隔、猜测次数、猜测频率、HTTP 请求配置、Web 爬虫配置等。 支持基于特征抽取方式，利用统计、机器学习等方法进行异常分析的基础，系统支持特征管理功能，特征抽取的统计方法包括平均数、求和、最大值、最小值、标准差、分位数、熵值等。			
23	零信任高级威胁检测探针	启明星辰 /NT16000-5G-ASJ	在实际网络环境中支持处理能力为 15G，每秒新建连接数 10 万，最大并发连接数 800 万。 采用国产芯片及国产操作系统，2U，冗余电源，RJ-45 管理接口 1 个和 1 个 VGA 接口，USB 接口 4 个，千兆光口 2 个，万兆光口 2 个，存储 18T 硬盘，同时软件具备异常终端、信令风暴、非法信令分析场景，支持僵木蠕、挖矿等主流攻击检测。 支持程序具备 AI 引擎自动对攻击进行威胁情报云查，页面自动呈现情报云查信息，查询结果包含：威胁等级、标签、威胁类型、IP 地址、IP 类型、活跃时间、发现时间、国家、地区、运营	2	580,000.00	1,160,000.00

			商、恶意端口等。 支持通过页面对告警前后存储报文数量进行配置，并支持启用或禁用情报检测、弱口令检测以及敏感信息检测的 pcap 包存储功能。 支持外发日志类型 8 种，支持在界面上独立设置每种日志类型的外发选项包含：事件告警外发、异常连接告警外发、威胁情报告警外发、流数据外发、协议元数据外发、资产数据外发、审计日志外发、导流插件状态外发。 支持对检测的告警事件结合双向检测机制、原始数据包和关联分析研判模型进行深层次研判给出告警攻击的结果同时根据攻击事件分类给出失陷主机标识，告警结果呈现结果包含五个维度：告警数据展示、基础数据展示、事件描述、云查情报、流量还原。 支持加密流量攻击检测，通过验证服务端 X509 证书是否存在异常行为针对恶意流量进行检测。 具备专有的挖矿分析场景：基于特征库和威胁情报检测挖矿主机，对挖矿主机进行不同阶段的展示，包括连接矿池阶段、获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段，形成挖矿链可视跟踪。对网络中的挖矿主机活跃程度，挖矿币			

			种有直观的图形化展示。			
24	日志分析管理系统	深信服/SIP-Logger-L2000-AK	配置200个日志接入授权，最大可扩展审计主机许可数量：500；日志处理性能≥2500 EPS。 采用国产芯片及国产操作系统，接口4个千兆电口+2个万兆SFP+口，实配冗余电源。 支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析。支持对每个日志源设置过滤条件规则，自动过滤无用日志，支持根据实际业务需求减少发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。 支持SM3国密算法，保障日志完整性，可以有效防止日志篡改等攻击行为。 支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能。 支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量≥350条，支持自	1	300,000.00	300,000.00

			定义关联分析规则。 支持把告警通过 API 的方式发送至第三方接口，告警内容支持自定义。			
25	区电子政务核心机房 1 精密空调（含室内机与室外机）	英威腾/VCR030	机房精密列间空调总冷量：30.8kW。循环风量：5200m/h。加热量：4.5kW。加湿量：3kg/h。产品能效比（EER）≥3.5（工况：室内干球温度 37℃，相对湿度 24%，室外温度 35℃）。柜体显示屏：7 英寸高端真彩电容触摸屏。风机数量：6。风机类型：EC 风机，独立控制开关。制冷剂类型：环保型制冷剂 R410A。压缩机类型：全封闭变频压缩机。节能模式：采用氟泵技术。接口：RS485 和 SNMP 双接口。机组供电：380VAC/50Hz。柜体安装：列间空调支持与现有机柜并柜安装。群控功能：支持与机房内现有精密列间空调统一控制管理，N+1 冗余运行模式。电压监测：支持输入 A/B/C 每一相的电压和频率监测并显示的功能，实时掌握空调供电质量，保证机组平稳运行。历史告警记录功能，支持≥10000 条本地显示。	1	160,000.00	160,000.00
26	区电子政务核心机房 2 精密空调（含室内	英威腾/VCA040	机房精密列间空调总冷量：42.8kW。循环风量：8500m³/h。加热量：6kW。加湿量：3kg/h。产品	1	200,000.00	200,000.00

	机与室外机）		能效比（EER）≥3.5（工况：室内干球温度 37℃，相对湿度 24%，室外温度 35℃）。柜体显示屏：10 英寸高端真彩电容触摸屏。风机数量：2。风机类型：EC 风机，独立控制开关。制冷剂类型：环保型制冷剂 R410A。压缩机类型：全封闭变频压缩机。节能模式：采用氟泵技术。接口：RS485 和 SNMP 双接口。机组供电：380VAC/50Hz。 柜体安装：列间空调支持与现有机柜并柜安装。群控功能：支持与机房内现有精密列间空调统一控制管理，N+1 冗余运行模式。电压监测：支持输入 A/B/C 每一相的电压和频率监测并显示的功能，实时掌握空调供电质量，保证机组平稳运行。存储功能：支持本地存储历史记录≥2000 条。			
27	空调安装套件	首信科技/现场定制	空调安装套件。	2	2,000.00	4,000.00
28	空调冷媒管保温套	首信科技/现场定制	空调冷媒管保温套。	106	150.00	15,900.00
29	空调制冷剂	巨化/R410A	R410A。	6	1,500.00	9,000.00
30	空调室外机支架	首信科技/现场定制	方钢材质，据实定制。	2	1,200.00	2,400.00

31	区电子政务核心机房2 20KVA UPS	英威腾/HT33020	产品主机类型：三进三出20kVA高频安全电源主机；输入频率范围：40-70Hz；输入功率因数：≥0.99；输入电流谐波：≤3.0%；输出稳压精度：±1%；逆变器过载能力：<110%，1小时；110%~125%，10分钟；125%~150%，1分钟。 群控功能：支持与机房内现有UPS主机统一控制管理，N+1冗余运行模式；控制功能：采用全数字化双DSP控制，实现整流、逆变、充电、放电各个功率变换环节全部数字化控制；监控功能：UPS系统需具有黑匣子功能，全面监控关键部分参数，实现故障可控可管：记录和预警关键部位器件的数据，可设置风扇更换时间到期提示功能，提供不少于8个温度监控点，包含IGBT温度、进风口温度、出风口温度或SCR温度；电池组节数调节功能：电池组节数±16～±22节可设置，便于个别电池故障需要维护、更换时，可灵活调节电池节数的需要。	1	82,000.00	82,000.00
32	区电子政务核心机房1 30KVA UPS	英威腾/HT33030	产品主机类型：三进三出30kVA高频安全电源主机；输入频率范围：40-70Hz；输入功率因数：≥0.99；输入电流谐波：≤3.0%；输出稳压精度：±1%；逆变器过载能力：<110%，1小时；110%~125%，10分钟；125%~150%，1分钟。	2	98,000.00	196,000.00

			群控功能：支持UPS主机统一控制管理，N+1冗余运行模式；控制功能：采用全数字化双DSP控制，实现整流、逆变、充电、放电各个功率变换环节全部数字化控制；监控功能：UPS系统需具有黑匣子功能，全面监控关键部分参数，实现故障可控可管：记录和预警关键部位器件的数据，可设置风扇更换时间到期提示功能，提供不少于8个温度监控点，包含IGBT温度、进风口温度、出风口温度或SCR温度；电池组节数调节功能：电池组节数±16～±22节可设置，便于个别电池故障需要维护、更换时，可灵活调节电池节数的需要。			
33	蓄电池	英威腾/MF100-12	12V100AH密封铅酸免维护。	40	1,000.00	40,000.00
34	直流开关箱	施耐得/NSX100A	断路保护。	2	8,000.00	16,000.00
35	UPS线缆	朝阳/4*25mm+1*16	阻燃五芯电缆，规格4*25mm+1*16mm。	40	120.00	4,800.00
36	电池组铜排	天利/15*3mm	规格15*3mm。	40	80.00	3,200.00
37	抗静电活动地板	科华/600×600×35mm	全钢，规格600×600×35mm。	170	750.00	127,500.00
38	门禁主机	中控/F18	指纹、刷卡、密码一体化门禁主机。2.4寸彩屏显示;TCP/IP和RS485通讯可选;U盘功能,可上	5	3,000.00	15,000.00

			传下载记录等;支持指纹/ID 卡/MF 卡。			
39	单门磁力锁	中控/CL280S	280KG。	5	800.00	4,000.00
40	电源以及按钮	中控/现场定制	门禁系统供电，出门按钮。	5	1,000.00	5,000.00
41	智能 UPS 协议开发模块	万联/WEMS-V6.0	提供安全电源主机通讯协议。	2	1,500.00	3,000.00
42	智能精密空调协议开发模块	万联/WEMS-V6.0	需提供空调通讯协议。	2	1,500.00	3,000.00
43	采集主机	万联/CM-04M	4 口动力环境监控系统。	1	8,000.00	8,000.00
44	系统接入模块	万联/WEMS-V6.0	接入环境监控系统主机。	1	20,000.00	20,000.00
45	玻璃隔断拆除	首信科技/现场定制	外网机房现有玻璃隔断拆除。	1	6,000.00	6,000.00
46	机柜迁移	首信科技/现场定制	外网机房现有，含机柜内设备迁移。	1	16,000.00	16,000.00
47	冷通道封闭迁移	首信科技/现场定制	18 机柜位，含灯具迁移。	1	20,000.00	20,000.00
48	集成费	首信科技/现场定制	设备（含软件）采购总价 4%。	1	388,722.00	388,722.00
合计						**10,106,772.00**