广州番禺职业技术学院校园网基础网络环境及安全防护系统升级开发项目（二次）

（项目编号：CZ2023-0250）

合 同 书

甲方（采购人）：广州番禺职业技术学院

乙方（供应商）：赛尔网络有限公司

签 约 地 点：广州市番禺区

一、总　　则

第一条　合同当事人

甲方（采购人）：广州番禺职业技术学院

项目联系人：贾志伟

联系电话：13631403190

电子邮箱：jiazw@gzpyp.edu.cn

地址：广东省广州市番禺区市良路 1342 号

乙方（中标人）：赛尔网络有限公司

项目联系人：李晓梅

联系电话：18126845781

电子邮箱：lixiaom@cernet.com

地址：北京市海淀区中关村东路 1 号院清华科技园 8 号楼 B 座赛尔大厦

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及广州公共资源交易中心“广州番禺职业技术学院校园网基础网络环境及安全防护系统升级开发项目（二次）”（项目编号：CZ2023-0250）招标文件的要求和招标结果，经甲乙双方协商一致，签订本合同。双方共同遵守如下条款（其他有关合同项目的特定信息由合同附件予以说明，合同附件及本项目的招标文件、投标文件、中标通知书、在实施过程中双方共同签署的补充文件等均为本合同不可分割之一部分）。

二、合同标的

第二条　乙方根据甲方要求提供以下货物：

序号	货物品名	规格型号	单位	数量	单价（元）	总价（元）	备注
1	边界出口路由器	RG-RSR7708-X	套	1	371500	371500	详见“附件 1：锐捷产品的详细报价清单”
2	原有路由器板卡扩容	RSR77-SIP5-X	套	1	113800	113800	
3	原有路由器模块扩容	ENM-4XS	套	1	25000	25000	
4	高吞吐流量控制引擎	RG-EG3000XE	套	1	287300	287300	

5	IPV6 网络准入认证组件	RG-SAM+IPV6 组件	项	1	215500	215500	
6	智能 DDI（DNS+DHCP+IPAM）	D12000	套	1	369500	369500	详见“附件 2：亚信产品的详细报价清单”
7	主机安全系统	青藤主机自适应安全平台（主机监测）V3.0	套	1	299800	299800	详见“附件 3：青藤云产品的详细报价清单”
总价：人民币￥1682400.00 元（大写：壹佰陆拾捌万贰仟肆佰元整）							

三、质量

第三条 货物质量

（一） 乙方应提供原装、全新的、符合国家质量标准的设备，并随设备提供有关设备安装、调试、使用、维修和保养所需的足够的中文技术文件（包括但不限于说明书、图纸、手册、技术资料和关键配套件清单等）。

乙方保证己方为依法设立且合法存续的企业，有权签署、有资质及能力履行本合同，保证其供货渠道合法。在本合同签订之前，乙方应向甲方提供己方及实施本项目相关人员的资质证明文件、核心产品的生产企业出具的供货确认函原件、售后服务承诺函原件、货物出厂合格证及生产企业有效授权函原件等证明材料，并提供一份复印件交由甲方存档备查。

（二） 本合同涉及纳入《国家强制性产品认证目录》内的产品，乙方须提供 3C 认证证书。

（三） 货物质量出现问题的，乙方应负责三包（包修、包换、包退），费用由乙方负责。

（四） 货到现场并验收合格后，由于甲方保管不当造成的质量问题，乙方亦应负责修理，但费用由甲方负担。

四、交货与验收

第四条 交货、安装、调试、验收必须在合同签订后 20 个工作日内完成（节假日及寒暑假不计入）。

第五条 交货地点：广州番禺职业技术学院校本部。

第六条 甲方及甲方聘请的监理将依据市信息主管部门立项审核意见、市财政局批复文件、招标文件和合同等文件，按照《广州市财政投资信息化建设项目验收规范》及相关标准规定对货物进行验收。货物验收时若乙方不参与现场验收，则视为同意甲方验收结果，验收合格的，甲方按合同要求办理付款手续；验收不合格的，甲方或由甲方聘请的监理单位书面

反馈验收情况及处理意见给乙方。产品若有国家标准按照国家标准验收，若无国家标准按行业标准验收，为原制造商制造的全新产品，整体无污染、无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用，同时符合本合同约定的质量要求。产品规格、型号、技术参数、产地须与合同、招标文件规定一致，若出现不符，乙方应及时办理退换货并负责负担全部费用及由此给甲方造成的全部损失。

本项目验收分为校内验收、合同验收两部分：

1、校内验收：由校内外专家组成的专家组负责，项目监理、项目实施部门负责对整个验收过程进行监督。项目承建单位负责准备所有验收所需文档（含电子版），并进行建设汇报和功能演示。专家组验收后必须出具验收意见，对不能通过验收的项目，须出具整改报告。

2、合同验收：在完成校内验收，试运行满三个月后，乙方须完善项目遗留的问题和各项整改工作，通过并提交符合甲方上级相关主管部门终验要求的各类文档，由监理单位审核通过并出具文档审核报告。合同验收具体标准以甲方上级相关主管部门发布的验收规定为准。

第七条 乙方承诺，本项目将按甲方上级相关主管部门要求，在合同验收前通过由学校招标确定的第三方测评机构的验收测评及安全评估，相关验收标准以主管部门要求为准。

上述验收均合格后，视为乙方完成交付。

第八条 乙方应将所提供货物的装箱清单、用户手册、原厂保修卡、随机资料及配件、随机工具等交付给甲方；乙方不能完整交付货物及本合同约定的单证和工具的，视为未按合同约定供货，乙方必须负责补齐，因此导致逾期交付的，由乙方承担相关的违约责任。

五、合同金额及付款方式

第九条 合同金额

本合同金额为人民币（大写）壹佰陆拾捌万贰仟肆佰元整（￥1682400.00元）。该合同总价是货物设计、制造、包装、运输、安装、调试、检测、培训、技术服务及验收合格之前及质保期内服务及备品备件发生的所有含税费用。本合同执行期间合同总价不变。

第十条 付款方式

1、签署合同生效且财政资金到位后5个工作日内，甲方向乙方支付合同总价的40%，人民币（大写）陆拾柒万贰仟玖佰陆拾元整（￥672960.00元）；

2、货物全部到场齐全，经甲方及监理单位现场清点确认合格后10个工作日内，甲方向乙方支付合同总价的40%，人民币（大写）陆拾柒万贰仟玖佰陆拾元整（￥672960.00元）；

3、货物及系统软件安装调试完毕，满足甲方使用要求，且项目通过验收测评和校内验收后10个工作日内，甲方向乙方支付合同总价的15%，人民币（大写）贰拾伍万贰仟叁佰陆拾元整（￥252360.00元）；

4、项目试运行期满三个月，通过安全评估且合同验收合格后 10 个工作日内，甲方向乙方支付合同总价的 5%，人民币（大写）捌万肆仟壹佰贰拾元整（￥ 84120.00 元）。

以上款项在乙方提交付款申请（首期款无须申请）及等额的正规发票并由甲方聘请的监理单位审核确认后启动办理支付程序，乙方逾期交付发票或所开具的发票不符合约定的，甲方有权延期支付相应费用并不视为违约。

甲方使用的是财政资金，故甲方向财政主管部门完成支付材料的提交即视为完成支付手续，具体款项支付时间视财局资金到位情况而定。由于财政资金拨款导致付款迟延的，不视为甲方违约。

六、售后服务

第十一条 乙方需提供售后的技术服务支持，保证甲方顺利使用所购货物，具体售后服务包括但不限于提供设备的安装、调试、检验等；根据甲方需求提供不少于 2 天的技术培训等。由甲方确定接受培训人员和人数，分批分期进行。乙方应选派熟悉设备的技术人员，并提供详细的培训手册和教材，负责包括产品使用、功能应用、教学应用管理、日常维护、安装调试、运维监控等在内的技术培训工作。

培训形式应采用理论培训和上机实践操作相结合的方式。

（1）现场集中培训：由甲方指定地点，由乙方的技术员进行集中讲解授课，在实际平台操作环境下，使参加培训的管理人员能尽快掌握系统平台的使用。

（2）制作培训课件：乙方需针对甲方用户按照不同的角色按照不同的培训课程，安排不同的培训内容课程和制作不同的培训教材课件。

（3）个别培训：乙方需根据甲方安排，针对不同的功能应用，安排不同对象、不同场次的个别培训课程。

第十二条 乙方应为甲方提供货物的质量保证期限（以下简称“质保期”），质保期自甲方完成合同验收之日起计算，所有设备质量保证期为 3 年。质保期内系统软件升级、运维和硬件的维护属于免费服务范围，乙方不得另行收费。质保期后的货物维护由双方协商再定。

第十三条 质保期内，乙方负责对其提供的货物实行包修、包换、包退、包维护保养，不再收取任何费用，但不可抗力（如火灾、雷击等）造成的故障除外。乙方人员应遵守甲方的各项管理规定，不得影响甲方的正常管理秩序。乙方人员在甲方范围内发生事故或因乙方、乙方人员过错导致的一切人身损害或财产损失，乙方应妥善处理纠纷并承担全部赔偿责任（包括但不限于赔偿甲方因此支出的赔偿金/和解款、诉讼费/仲裁费、律师费等）。

第十四条 乙方所提供的售后服务应及时有效。乙方承诺，在广州市内设有维修服务点并提供电话服务热线，其工作人员在接到维修电话 1 小时内做出明确响应并安排专业人员处理，保证在接到故障电话后 5 个工作日排除故障。如 5 个工作日内不能排除故障的，乙方应

免费提供同等质量的货物供甲方使用，直至货物修复为止。如乙方未按照合同约定提供保修等售后服务的，甲方有权自行或聘请第三方服务，并有权要求乙方赔偿因此给甲方造成的一切费用和损失。

第十五条 乙方货物的销售人员需持有相应的培训证书。乙方应设专业的售后服务中心，同时能够提供常用耗材及配件的及时供应，提供维修服务的维修工程师需持有相应产品的维修授权证书。

第十六条 甲方将聘请项目监理单位，协助对本项目建设进行监督。乙方必须接受甲方及甲方聘请的监理对本项目的管理和监督，及时向甲方及监理同时提交各种设计方案、实施方案、报告等项目文档。对于监理对本项目实施过程中指出的问题，应该积极给与答复并解决。对于监理提出的合理的整改要求，积极限期完成整改。

第十七条 在质保期内，乙方须对所提供的设备做定期检查和保养。

七、违约责任

第十八条 甲方无正当理由拒收货物、拒付货款的，甲方须向乙方交纳合同总价 5 % 的违约金。如甲方无故变更、中止或者终止本合同的，应当对乙方受到的损失予以赔偿或补偿。

第十九条 甲方无故逾期支付货款的，甲方须每日以欠款总额 3 ‰的标准向乙方交纳违约金，累计不超过欠款总额的 5 % 。

第二十条 乙方无故逾期交付货物的，乙方须每日以逾期交货部分货款总额 3 ‰的标准向甲方交纳违约金，累计不超过逾期交货部分货款总额的 5 % 。逾期交货超过 30 天，视为乙方不能交付货物，须向甲方交纳合同总价 5 %的违约金。同时甲方有权单方解除本合同，并要求乙方赔偿由此造成的一切损失（包括但不限于直接损失、诉讼费/仲裁费、律师费等）。

第二十一条 如乙方未按照合同约定履行义务，包括但不限于所交付产品的型号、规格、数量和质量不符合甲方要求等，甲方有权拒收，并要求乙方在合同规定的交货时间内无条件更换合格的产品给甲方。若乙方拒不更换或按时更换后仍不符合甲方要求的，则视为乙方不能交付产品而违约，甲方有权单方解除本合同，不予支付相应费用，并有权要求乙方按照合同总价的 5 %支付违约金及赔偿损失（包括但不限于直接损失、诉讼费/仲裁费、律师费等），并须全额退还甲方已经付给乙方的货款及其利息。若乙方不能按时更换，则视作乙方逾期交付产品而违约，按“第二十条”规定，由乙方赔付违约金给甲方。

第二十二条 乙方所供货物、系统及服务必须权属清楚，不得侵害他人的知识产权，否则构成对甲方违约。如甲方因此遭受到第三方索赔、诉讼或任何权利请求的，乙方应妥善处理纠纷，并承担全部赔偿责任（包括但不限于赔偿甲方因此支出的赔偿金/和解款、诉讼费/仲裁费、律师费、差旅费等）。

第二十三条 由于政策的变化或不可抗力的原因导致项目停工，使合同无法继续履行的，视为项目终止。项目终止后，乙方应妥善做好已完成项目的保护和移交、质保工作，甲方按合同条款支付已完成工作量的价款。

八、不可抗力

第二十五条 由于不可预见、不可避免、不可克服等不可抗力的原因，一方不能履行合同义务的，应当在不可抗力发生之日起 7 天内以书面形式通知对方，证明不可抗力事件的存在。

第二十六条 不可抗力事件发生后，甲方和乙方应当积极寻求以合理的方式履行本合同。如不可抗力无法消除，致使合同目的无法实现的，双方均有权解除合同，且均不互相索赔。

九、争议解决办法及通知送达

第二十七条 因货物的质量问题发生争议，由广州市市场监督管理局或其指定的质量鉴定单位进行质量鉴定。货物符合质量标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。

第二十八条 本合同发生争议，由双方协商或由政府采购监管部门调解解决，协商或调解不成时按以下第 2 种方式解决：

1. 中国广州仲裁委员会仲裁；
2. 向甲方所在地人民法院提起诉讼。

第二十九条 任何一方因履行本合同而相互发出或者提供的所有通知、文件、材料，均以本合同所列明的地址送达，一方迁址或者变更联系方式的，应提前三日书面通知对方。否则，因联系方式错误致使无法送达而造成的不利后果均由未通知方承担。

十、其他

第三十条 本合同一式 柒 份，甲方执 伍 份，乙方执 贰 份，具有同等法律效力。合同自双方法定代表人或其授权代表签字盖章之日起生效。

第三十一条 本合同未尽事宜，由双方协商处理。

（以下无正文）

甲方：（盖章） 广州番禺职业技术学院

法定代表/授权代表：

签约日期： 2023 年 8 月 12 日

乙方：（盖章） 赛尔网络有限公司

法定代表人/授权代表：

签约日期： 2023 年 8 月 12 日

附件 1：锐捷产品的详细报价清单

序号	产品/服务名称	开票名称	型号	功能说明	数量	税率	单价	总价
1	IPV6 网络准入认证组件	锐捷 RG-SAM+认证计费管理平台	RG-SAM+-RS IPV6 组件	激活 RG-SAM+ IPv6 相关功能使用权限，包括 IPv4/IPv6 双栈准入准出，日志记录等	1 套	13%	179583	179583
	RG-CT Base 基础质保服务	技术服务	/	RG-CT Base 基础质保服务	1 项	6%	35917	35917
2	边界出口路由器	锐捷路由器	RG-RSR7708-X	RSR7708-X 主机箱。双路由引擎插槽，双交换网板插槽，4 个业务载板插槽，最大 12 个业务子卡插槽，2 个电源槽，带防尘网和风扇盘。路由引擎、业务载板及子卡、电源支持热拔插。	1 台	13%	9915	9915
		锐捷路由器产品软件平台	V1.0RSP-RSR7708-X		1 套		160264	160264
		锐捷路由引擎	RSR7708-SRCMI-X	RSR7708-X 路由引擎，固化 2 个 USB2.0 接口，1 个 USB-Console 口，1 个 MGMT 管理口，1 个 Console 口，1 个 AUX 口，1 个 SD 卡插槽	2 台		5356	10712
		锐捷路由器交换网板	RSR7708-DSF-X	RSR7708-X 交换网板	2 台		8644	17288
		锐捷路由器电源	RG-PA1600-RI	交流电源模块（可冗余,1600W）。标配国标 16A 电源线。	2 块		8458	16916
		锐捷路由器配件	RSR77-SIP5-X	增强型 ENM 业务处理载板，3 个 ENM 业务处理卡插槽。	1 台		46146	46146
		锐捷路由器模块	ENM-4XS	4 端口万兆以太网光接口模块。	1 个		10857	10857
		锐捷交换机线卡	DFNM-16GE/2XS	16 端口千兆以太网光电复用接口及 2 端口万兆以太网光接口模块，千兆电口支持 1000M/100M/10M 电，千兆光口只支持 1000M 光，万兆口只支持 10G 光。	1 台		57902	57902
	RG-CT Base 基	技术服务	/	RG-CT Base 基础质保服务	1 项	6%	41500	41500

	础质保服务							
3	原有路由器板卡扩容1	锐捷路由器配件	RSR77-SIP5-X	增强型ENM业务处理载板，3个ENM业务处理卡插槽。	1台	13%	94833	94833
	RG-CT Base基础质保服务	技术服务	/	RG-CT Base基础质保服务	1项	6%	18967	18967
4	原有路由器板卡扩容2	锐捷路由器模块	ENM-4XS	4端口万兆以太网光接口模块。	1个	13%	20833	20833
	RG-CT Base基础质保服务	技术服务	/	RG-CT Base基础质保服务	1项	6%	4167	4167
5	高吞吐流量控制引擎	锐捷网关	RG-EG3000XE	固化8个千兆电口，固化8个千兆光口，固化8个万兆光口，固化2个40G光口，32G内存，两个硬盘插槽，支持1T企业级硬盘。内置风扇，1+1冗余电源。	1台	13%	38307	38307
		锐捷网络安全软件平台系统	V1.0,NSSP-RG-EG3000X		1套		198716	198716
		锐捷网关硬盘配件	RG-Gateway-HDD-1T	该硬盘适用于EG3000系列高性能综合网关产品。	2块		1197	2394
	RG-CT Base基础质保服务	技术服务	/	RG-CT Base基础质保服务	1项	6%	47883	47883
							总计	**1013100**

附件 2：青藤云产品的详细报价清单

序号	产品/服务名称	描述	功能说明	数量	税率	单价	总价
1	青藤主机自适应安全平台（主机监测）V3.0	青藤主机自适应安全统一控制台	只支持（x64) Linux 服务器，功能包括：通知系统、主机管理、IP 通用设置、账户信息管理、服务监控、Agent 安装与管理、系统审计、权限管理。	1 套	13%	197270	197270
		青藤主机自适应安全 Agent 授权（300 个点）	"微隔离模块包括以下功能：连接可视化、网络访问控制、异常访问监控、主机管理、主机一键隔离。客户端版包含 QASA — Qingteng Adaptive Security Agent 提供支持平台上完整性监控功能 按照所需部署的客户端数量计价，无论部署于物理，或是虚拟机中。"				
			通过扫描和实时监控两种方式发现内存后门，可发现内存 Webshell、shellcode 和动态链接库注入等内存马攻击，并发送告警通知。				
			提供高价值的安全分析工具，用户可以灵活配置，自助检查各类系统问题，包括文件查询、网络工具、进程查询、Web 查询、账号控制、安全工具、其他等，利用这些工具，可以快速便捷地帮助用户进行查询分析或是响应处理。				
			面对漏洞修复空窗期的风险，关键业务漏洞修复风险，老旧系统补丁断更，监管侧的合规检查等一系列难题。				
2	信息技术服务	青藤产品规则库更新	青藤云安全通过在线或离线(每月定期通过邮件发送)的方式提供产品规则库 更新包，客户可通过上述方式获取更新包后完成产品规则库的更新。	3 年	6%	29580	88740
3	信息技术服务	安装部署服务	安装部署：软件安装、基础环境部署、授权激活。 系统配置：系统策略配置和安装部署演示指导 产品培训服务：提供一次培训服务，包含产品功能模块培训、产品日常维护培训、日常故障处理培训	1 项	6%	13790	13790
						总计	**299800**

附件 3：亚信产品的详细报价清单

序号	产品/服务名称	开票名称	型号	数量	税率	单价	总价
1	智能 DDI（DNS+DHCP+IPAM）	亚信智网域名服务和地址分配及管理系统[简称：AIDDI]V2.0	D12000	1 套	13%	369500	369500
						总计	**369500**

附件 4：设备详细参数表

序号	设备名称	技术参数要求
1	边界出口路由器	1.▲主控引擎=2，独立交换网板=2，整机线卡插槽数量=4 个，实际配置路由引擎=2 块、交换网板=2 块、交流电源=2 块、业务处理载板=1 块、配置千兆以太网电口=16 个、千兆以太网 SFP 光口=16 个、万兆以太网光接口=6 个； 2.交换容量=150Tbps，包转发率=24000Mpps。 3.▲单卡支持并实配=200 万条 NAT，整机支持 3200 万条 NAT。 4.全部业务板卡支持并实配 H-QoS 功能 5.支持并配置静态路由、等价路由、策略路由； 6.支持并配置 Telnet、SSH 管理模式； 7.产品支持 ipv6 相关功能：IPv6 ND、IPv6 PMTU、双栈转发、ACL、VRRP v3、DHCPv6 Server/relay/client、隧道技术（IPv6 手动隧道、IPv6-over-IPv4、GRE 隧道、6to4 隧道、ISATAP 隧道、6RD）、路由协议（静态路由、RIPng，OSPFv3，IS-ISv6，BGP4+）、组播协议（MLD、PIM-SM v6、PIM-SSM v6） 8.支持 SP、WRR、DRR、SP+WRR、SP+DRR 等队列调度机制 9.支持并实配支持 L2TP、IPSec VPN、GRE VPN、组播 VPN 功能， 10.▲支持并配置虚拟化功能，要求能与同型号设备支持 N：1 的多虚一功能。 11.▲支持并配置园区网出口多运营商智能自动选路、智能 DNS，可以与园区网运营管理平台进行联动；支持通过 PPPoE 代理直接对接地市 BRAS 设备。 12.支持对关键业务带宽资源预留及保障，能够实时识别业务流自动建立保障措施，并在业务完成后自动拆解保障通道，及时释放带宽资源，便于管理维护。 13.支持并配置 CLI、SNMP v1/v2/v3、RMON 1/2/4/9；支持并配置 Syslog 日志功能。 14.支持并可配置 RIPv1/v2、BGPv4、BGP4+等路由协议。 15.支持 PQ、CQ、WFQ、CBWFQ、LLQ、RTPQ 等拥塞管理机制； 16.支持 OSPF、RIP、BGP4、IS-IS 等路由协议，支持 MPLS VPN，支持 PE 功能； 17.支持并配置国家密码管理局商密 SM1~SM4 加密算法，支持 SM1 硬件加密。 18.支持并实配防火墙功能，可提供状态检测、URL 过滤、VPN 等多种安全特性，如需配置独立硬件板卡或购买 License 才能支持该功能特性，则要求必须配置相应独立硬件板卡或 License。 19.支持高速同步串口、E1/CE1、GE、10GE、40GE、155M/622M/2.5G POS、CPOS、155M ATM 等广域网接口 20.支持路由引擎、业务载板/模块、电源/风扇等关键部件的高可用性热插拔设计 21.全部业务板卡支持并实配国际标准的 IPFIX 功能 22.支持 PIM-DM、PIM-SM、PIM-SSM 等组播路由协议 23.支持 BFD for VRRP/OSPF/BGP4/ISIS/ISISv6/MPLS/静态路由等 24.支持防攻击保护、DoS/DDoS 防御、分片包攻击防御、SYN 攻击防御、IP 欺骗攻击防御 25.▲支持与学校现有的 RG-RSR77 系列出口路由器组成 HA，为满足实际需求，如需要进行测试、接口开发、追加设备所产生的任何额外费用，由乙方承担。
2	原有路由器板卡扩容	1.可支持 3 块 ENM 功能模块 2.▲支持在现网 RG-RSR7708-X 出口路由器上进行端口升级扩容。如需要进行

		测试、接口开发、追加设备所产生的任何额外费用，由乙方承担。
3	原有路由器模块扩容	1.可支持 4 个 SFP+端口 2.▲支持在现网 RG-RSR7708-X 出口路由器上进行端口升级扩容。如需要进行测试、接口开发、追加设备所产生的任何额外费用，由乙方承担。
4	高吞吐流量控制引擎	1.▲支持固化千兆电口=8 个，固化千兆光口=8 个，固化万兆接口=8 个，固化 40G 接口=2 个； 2.多核非 X86 架构，支持 1+1 冗余电源；支持双硬盘插槽，硬盘容量=1T，硬盘支持可插拔更换 3.支持 VPN 内流量的可视化监控； 4.支持 VPN 内流量流量控制； 5.NAT 转发吞吐率=30Gbps；并发 NAT 连接数=1600W；新建 NAT 连接数=15W 6.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，配置应用协议库，协议识别数量=1500 种。 7.配置 URL 数据库及应用特征库 5 年升级，另外 URL 数据库和应用特征库支持远程 HTTP 自动升级。 8.配置=4000 个 SSL VPN 接入授权，配置=3000 路 Ipsec VPN 接入授权。 9.▲支持对 TCP 优化，支持 CIFS、FTP、HTTP、POP3、SMTP、EXCHANGE、RDP 协议进行优化； 10.▲支持基于应用优化、TCP 优化、数据压缩、消除冗余数据的双边加速技术，提高用户的上网体验； 11.支持正向 DNS 代理功能，可根据配置实现对不同外网线路的 DNS 服务器地址管理。 12.支持 IPV6 环境 13.支持状态检测防火墙功能，实现网络安全防护 14.支持网关、网桥等多种部署模式，灵活安装。 15.支持 SNMPV2 和 V3 版本，支持多 TRAP 接收主机配置。 16.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； 17.支持 VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议) 18.DHCP 地址池分配状态，可生成 IP、MAC 对应关系列表 19.支持 HTTPS 和 HTTP 的 WEB 方式管理 20.▲URL 数据库和应用特征库支持远程 HTTP 自动升级。 21.▲支持多线路捆绑技术，避免跨运营商的数据访问；实现丢包恢复；报文压缩，增加带宽容量； 22.要求所投产品 IM 聊天可支持基于聊天内容关键字的策略控制，通过插件可以实现 QQ 聊天内容的审计 23.支持精准限速功能：能够有效降低对 P2P 软件进行限速而造成的流量废弃，提升外网带宽利用率； 24.支持应用所属分类查询功能，可针对应用确定所属分类； 25.支持应用自定义分类，将支持应用划分至保障、阻断等分组； 26.流控带宽升级功能：客户带宽升级后，只需要修改线路总带宽即可，其余策略都会自动按比例更新，无需每个策略调整； 27.流量控制支持时间对象设置，时间对象需精确至分钟级； 28.时间对象可支持 10 个以上时间段；

		29.支持用户并发会话数控制，并提供当前用户并发会话数信息作为策略条件参考； 30.支持流量控制前后流量对比；
5	IPV6 网络准入认证组件	1.支持 Pv4/IPv6 双栈准入准出 2.支持 Pv4/IPv6 双栈终端认证日志记录朔源 3.▲要求与学校现有的安全认证计费系统（RG-SAM+）上进行软件升级扩容，实现 RG-SAM+ IPv6 相关功能使用权限开启，为满足实际需求，如需要进行测试、接口开发、追加设备所产生的任何额外费用，由乙方承担。
6	智能 DDI（DNS+DHCP+IPAM）	1.提供包含域名服务、防火墙服务、地址分配名称的软件著作权登记证书，并提供资质证书扫描件。 2.设备具备公安部网络安全保卫局颁发的：计算机信息系统安全专用产品销售许可证需包含需包含域名服务、地址分配及访问控制系统的相关字样，并提供资质证书扫描件。 3.设备需具备国家网络与信息系统安全产品质量监督检验中心检测：信息技术产品安全测评证书需包含域名服务、地址分配及访问控制系统的相关字样，并提供资质证书扫描件。 4.设备厂家需提供第三方权威机构颁发的面向本次招标设备的能力证明，如 CNAS 实验室或者软件行业协会的检测报告（注，证明材料必须能够显示所投产品具备需 DNS（授权域管理、安全配置、视图与链路管理）DHCP(指纹管理、业务资源管理)、网络洞察（网络规划、网络发现））。 5.软件产品证书：需具备软件类别为应用软件-网络应用软件产品证书，需包含域名服务、地址分配及管理系统的相关字样，并提供资质证书扫描件。 6.设备厂家需具备中华人民共和国工业和信息化部颁发的：电信设备进网许可证，并提供认证证书扫描件。 7.提供 IPv6 Ready Logo Certified，需包含域名服务、地址分配及管理系统的相关字样，并提供认证证书扫描件。 性能要求： 1、DNS 性能（QPS）300000； DHCP（LPS 指标）单设备不低于 2000LPS；DHCP（IP 地址容量）单设备不低于 200000。 2、1U、6 个千兆电口，冗余电源 550W，2 个 8 核 CPU ,32G 内存，2 块 1TB 硬盘，支持 raid 0，1。 功能要求： DNS 标准 1、支持标准 DNS 协议:支持标准 DNS 协议 RFC1034、1035，支持扩展 DNS 协议 RFC2672、2782、3596。 2、递归解析功能:记录类型支持 A 记录、AAAA 记录、NS 记录、CNAME 记录、MX 记录、PTR 记录，对未命中缓存的 DNS 请求进行迭代解析，随机选择源端口用于发送迭代解析请求报文。 3、TTL 值优化功能:设定指定域名/泛域名/全局的最小 TTL 值，该域名请求的响应结果的 TTL 值不小于该值。 4、视图功能:用户根据源 IP 匹配视图，根据视图可以定义不同的 DNS 策略，支持系统默认视图：对所有源 IP 都生效，支持普通视图：具有明确的源 IP 地址范围，普通视图地址范围可以重叠。 5、视图优先级:当同一 IP 在多个视图中同时存在，有限匹配高优先级的视图，

		当优先级高的视图没有对应的策略，则顺延匹配低优先级的视图。 6、▲应用服务器健康检查:可以设定要检测的应用服务器，通过 dig/ping/wget 等技术，判断服务器的的健康状况以及响应时间，支持 HTTP/HTTPS/FTP/UDP/ICMP 等协议。支持双栈 IPv4、IPv6 探测能力。支持自定义探测模板、自定义探测协议类型。 7、多链路接入流量检测:当有多条链路接入的时候，可以检测到每条链路的繁忙情况，并且可以根据繁忙情况调整解析 IP 地址的归属。 8、▲授权域健康监测:支持针对整个授权域的拨测结果，同时在针对整个授权域的拨测结果中可以配置域的转发策略。 9、按用户组负载流量:支持划分用户组，指定用户组在解析时优先返回指定运营商线路的 IP，例如电信用户组，则递归解析的时候，优先返回部署在电信的应用的 IP 地址。 10、按比例负载流量:设定不同线路的百分百，按照不同百分比，解析出对应运营商部署应用的 IP 地址。 11、智能负载:支持 DNS 轮询、支持 DNS 筛选、服务器状态筛选，线路繁忙筛选等多种负载均衡算法。 12、内置 IP 地址库:内置 IP 地址库，可以根据 IP 地址判断归属地。 13、内置域名类型库:内置域名类型库，可以根据域名类型设定运营商类型和出口 IP 地址。 14、解析异常重定向功能:可以针对响应的解析结果类型为 NXDomain 等非正常解析响应结果，支持重定向到特定的内部门户网站。 15、▲域名请求转发:直接转发到企业内部授权，提高解析速度,支持 forward first、only、last，当内网 DNS 解析失败时，将域名 forward 到指定公共 DNS 提高 DNS 解析成功率。支持开启优先转发功能，在开启优先转发后，在进行 DNS 请求转发时，优先使用配置转发服务器列表内的第一个 IP 地址。支持对 Forward 服务器配置权，当存在多个转发服务器时支持按照权重比例进行转发。 16、域名强制解析:支持基于视图维度配置精确域名、泛域名、*域名的 A、AAAA、NS、CNAME、MX、PTR 记录强制解析，解析结果支持指定地址、noerror、nxdomain、servfail。 17、会话保持:支持配置指定域名会话保持，一段时间内对同一客户端返回固定的解析结果。 18、透明域:支持本地解析失败后，进行二次递归解析。 19、URL 显性/隐性转发:支持显性 URL 转发和隐性 URL 转发。 20、递归启用停用:支持界面设置每台服务器递归功能的启用、停用。 21、▲解析黑白名单:支持针对 IPv4、IPv6 的 A、AAAA 记录的解析域名黑白名单配置。IPv4、IPv6 能够单独开关控制，互不影响。 22、DNS 流量防劫持:支持被劫持的 DNS 流量重新引导至指定 DNS。 23、权威解析:支持查询 zone 配置得到域名的权威解析结果，支持 zone 配置的动态加载。 24、授权域审批:支持对授权域名的审批流程。 25、共享记录:可以新增授权域名共享到所有的授权域下。 26、多级智能调度解析:支持基于健康检查上报的多级智能调度需求。支持多级拨测，多级拨测任务、多级结果上报、多级拨测结果汇总。支持拨测结果

		策略设定，动态策略计算。 27、分线路智能解析:判断用户访问的线路信息，根据用户的所属运营商，返回对应的运营商部署应用的 IP 地址。 28、分区域智能解析:能够支持分区域智能解析，系统自带全国各省份 IP 地址信息，支持按省份的区域划分和 IP 地址更新，可按区域智能解析到相应区域线路对应的应用服务器 IP 地址。 29、★智能解析:检查应用服务器运行状态，依据建立连接时延、首字节响应时延、首屏下载时延、90%元素下载时延、全部下载时延、下载速率、首页 PING 时延、下载文件大小等，以及用户 IP 归属情况，综合判断返回最优 IP 地址。 30、▲数据库容灾切换:支持数据库容灾切换，支持 mysql、oracle 等数据库健康探测，支持第三方探测结果上报接口，支持固定结果优先场景，支持保持上一次优先场景。 31、EDNS:全面匹配支持 EDNS 功能。 32、Windows AD 域:支持与 Windows AD 域的对接。支持双向联动，即 DNS 能从 windowsDNS 同步数据，同时 DNS 有更新需要反向同步给 windows DNS。支持同时向多台 windows DNS 同步数据。 33、生命周期管理:支持定义授权域记录的使用到期时间，通知人邮箱。域名到期自动提醒及到期自动清除记录，自动发送邮件。 34、域名动态解析:持 IPv4/IPv6 双栈 DDNS 功能，用来动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，从而保证通过域名访问到正确的 IP 地址；支持邮件通知域名和 IP 地址之间的对应关系变动。 35、防 DDOS 攻击:能够内置防 DDOS 攻击模块,保护权威 DNS 和递归 DNS 的安全。 36、SERVFAIL 防护:能够支持防御 DNS SERVFAIL 攻击，客户端通过发起大量错误域名攻击触发递归无响应从而导致服务器性能拥塞，该设备能够自主识别该类攻击特征，进行攻击防护。 37、源 IP 限速:全局源 IP 限速、特定源 IP 限速、限制其 DNS 查询速率，超过速率的部分丢弃。 38、域名限速:全局域名限速、精确域名限速、泛域名限速，限制其 DNS 查询速率，超过速率的部分丢弃。 39、域名封堵:精确域名封堵、泛域名封堵。 40、缓存投毒:深层次多点匹配递归的请求和应答。 41、防劫持:基于数据特征和 DNSsec 技术，防止域名劫持。 42、DNSSEC:全面支持 DNSSEC 技术。 43、ACL 白名单功能:允许指定的 IP 范围内的终端访问 DNS 服务。 44、用户组智能解析：支持与锐捷路由器对接，锐捷路由器划分不同用户组，DDI 设备不同网卡可接收不同用户组流量，并依据目的 IP 区分不同视图递归至不同运营商，返回用户相应的运营商解析地址，保证用户不跨网访问，提高访问速度。 DNS 安全 1、多类型拦截：DNS 防火墙拦截时不仅能对 A 记录和 AAAA 记录进行拦截，同时能对 MX 记录、TXT 记录、NS 记录、CNAME 记录、PTR 记录，进行拦截； 2、恶意域名封堵：能够主动发现恶意域名，同时阻止恶意域名解析，重定

		向到告警页面。 3、▲自营云威胁情报中心：具备自主运营的云威胁情报中心，包含商业情报、官方情报、用户共享情报等多来源的情报数据。 4、内置威胁情报库：系统内置已知的恶意域名信息。 5、▲威胁情报云更新：在云端有威胁情报实时分析系统，动态分析恶意网站，查找有潜在威胁的恶意域名，并提供 DDI 设备下载。 6、威胁情报联动：支持与安全设备联动，获取威胁情报信息。威胁情报库手动更新：支持用户手动新增/删除/修改/查询，支持选择生效。 7、监测分析联动：支持与同厂商监测与分析系统的联动，阻断 DGA 与 DNS 隧道域名。 管理平台 1、管理方式：支持 WEB 方式对设备进行管理和维护；支持可视化中文界面：用户输入、报表、管理界面、告警事件等信息可全部通过 Web 中文方式完成管理；支持通过 API 接口的方式进行业务管理和设备维护。 2、账号源地址控制：支持在 UMP 管理平台上配置账号源地址控制，在配置了账号源地址后，只有源地址内的 IP 使用对应的账号才能登陆系统，在不配置账号源地址情况下，所有 IP 均可以访问系统，支持账号-ip 生效时间的设定。 3、用户管理：能够支持分权分域的用户管理模式，实现多层次的管理模式，可以为不同用户分配不同权限，需要控制到最小功能项，需要控制系统的读写权限。包括管理 DNS 的权限，系统管理权限。支持对接第三方 Radius 认证系统，进行登录。 4、★业务管理：支持对 DNS 业务的统一管理。业务配置下发可选服务器，管理平台在管理配置策略、配置数据、配置各类域名记录时，支持选择生效设备。 5、实名信息管理：将 IP 地址与员工信息、终端信息、自定义属性等信息进行绑定，便于企业后续的溯源审计工作。 6、集中管理：一个 IPAM 可以管理多个 DDI 设备，系统自动将监测到的服务加入管理列表，提供进程启动，停止功能。 7、日志记录：详尽完善的业务日志和操作日志管理，日志必须保存至少 6 个月。 8、分析报表：提供多维度的报表，包括：TOP 域名、DNS 业务量、封堵域名数据统计等。 9、平台监控：支持中文图形化方式的全局所有子节点监控，提供监测主机 CPU，内存，硬盘的使用情况，提供 CPU 温度检测，提供检查后台运行进程的功能，能够在异常情况下自动重新启动相关进程。可设定报警阈值，发生问题时可实时触发故障报警。 10、▲抓包工具：支持图形用户界面的 DNS 抓包，帮助获取运行真实数据分析和处理问题。 11、分权分域：支持不同用户分配不同的资源权限 12、NTP 时钟同步：同时支持 NTP 服务端及客户端。支持配置多个时钟同步服务器。 13、Syslog 转发服务器配置：支持配置 syslog 日志转发步服务器。 14、国际化：支持中、英文版本。

		15、系统升级：支持软件离线升级。 IPAM 地址分配 1、地址分配：支持 IP 地址动态分配、静态绑定、空闲地址分配、基于指纹地址分配等。 2、轮询分配：用户可以选择在 web 页面可以打开地址均衡分配的开关，使 DHCP 支持。根据配置的接口地址和地址池段，均衡分配地址给终端 3、IP 状态变更：设置某个 IP，IP 地址段为保留或分配状态 4、二次地址分配：支持二次地址分配。 5、记忆地址分配：DHCP 系统支持 IP 地址的分配记忆功能，终端设备每次上线会尽量的分配上次记忆的 IP 地址。 6、Option 自定义：支持根据业务需求手工自定义 option。 7、终端类型分配：支持不同终端类型分配不同地址段 IP。 8、中继 RelayID 分配：DHCP 系统支持中继的同一 Relay ID（网关地址）分配不同网段的地址。 9、地址冲突检测：在 DHCP 自动分配地址之前，自动检测下该 IP 地址是否已经占用。 10、▲地址冲突处理：支持 DHCP DECLINE 报文的地址冲突处理，持 IP 地址冲突检测，冲突地址隔离和隔离冲突地址定期回收功能。 11、禁止非法路由接入：禁止非法路由器的接入。 12、禁止私设 IP 地址：支持通过交换机联动禁止私设 IP。 13、指纹信息：支持现网及终端设备指纹识别，终端厂家标识等特征。 14、线路信息：支持 option 82 子集。 15、准入认证：支持 portal 协议、802.1X 协议的准入认证（账号、密码），账号密码支持本地保存，短信认证、ldap 认证、windows AD 认证、MAC 认证。 16、地址绑定：支持 MAC 和 DUID 的地址绑定。 17、地址释放：支持管理员手动释放已经分配的地址。 18、IPv6：支持 IPv6 地址分配。 19、DNS 服务器下发：支持地址分配下发多个 DNS 服务器。 20、网络拆分&合并：支持地址段的缩放拆分和合并。拆分：把一个大网段拆分成多个小网段。合并：合并就是把网络放大，把多个网络合并到一起。 21、DHCP Failover：支持业界标准的 DHCP Failover，Failover split 支持，在 Failover 中，一个 IP Pool 可分配的剩余 IP 数在两台 DDI 设备间始终是按 5:5 进行均衡的，支持 Partner down 参数设置，参数生效后，Secondary 或 Primary 可以接管所有剩余的可分配 IP。 22、防 ARP 病毒：预防 ARP 病毒造成 IP 地址冲突。 23、防伪造 DHCP：防范伪造 DHCP 服务对业务的影响。 24、来源 IP 校验功能：校验数据包来源地址是否已经在系统上进行登记，丢弃未登记的设备发来的数据包。 25、异常流量限速攻击防护：基于 MAC 地址限速、基于接口级限速、支持 MAC 地址黑名单、白名单。 26、支持 IPV4 和 IPV6 地址：支持 IPv4 和 IPv6 双栈的协议处理和地址获取。 IPAM 网络发现 1、终端信息自动发现：对网络内的 IP 使用情况进行主动探测分析，结合实

		名信息，记录 IP 地址对应的 MAC 地址、设备名称、设备类型、位置、联系人、用途等信息 2、网络信息自动发现：支持与交换机联动，主动采集交换机信息，包括端口信息、接口信息、路由信息、ARP /ND 信息等，实现网络全局可视化。 3、网络拓扑展示：支持网络拓扑结构展示，并支持进行导出。 4、OID 管理：支持管理配置网络发现用到的 OID 信息，不同厂家的 OID 如果存在差异的，每个 OID 支持添加多条，系统在使用 OID 查询可以循环查找信息。 5、交换机端口控制：可针对二层交换机，三层交换机的端口进行关闭，启动操作，实现用户终端的网络控制。 6、▲IP 地址回收：自动回收，对超过一定时间（时间可设置，单位天,默认 7 天）的 IP 实现可回收功能。手动回收，支持单个 IP 地址回收操作、支持选择多个 IP 地址回收操作、支持按照查询结果进行全部回收操作。 7、▲数据分析及告警：可快速针对当前数据创建基线数据，并定期每周、每月针对基线数据进行比对，一旦发现异常（可选择监控异常项）则进行告警。 8、自动化 IP 地址实时跟踪：使用主动扫描发现并跟踪子网及相关的地址块，查看子网内各 IP 地址当前的状态以及对应的设备信息。 9、▲网络探测任务配置：支持静态 IP、IP 范围段、子网的周期扫描任务，可编辑、删除任务；可配置执行中断期、暂停/开始任务、立即执行任务。 10、★网络探测扫描端口配置：支持自定义配置扫描端口及探测协议，以关注用户关心的服务，并监测服务运行状态，在服务启动/终止时告知用户。 11、终端凭证配置管理：可在交换机、路由器上配置 SNMP（v1/2c/v3）/CLI 凭证并测试凭证是否可用,以用于后期采集。 12、地址规划管理：提供子网掩码计算器，通过输入 IP 地址及子网掩码即可自动计算出需要规划的网段，包括可用地址数、掩码、网络、开始 IP 和结束 IP、广播地址等信息。地址规划需要提交审批，通过审批的 IP 地址方可分配给使用者使用，记录地址的使用者，方便追溯、管理。 13、地址冲突检测：平台支持监控 IP 地址使用情况，当规划地址与使用地址不符，或者 DHCP 分配的地址与实际使用地址不符而造成 IP 地址冲突时触发告警。 14、▲分析报表：提供多维度的的报表，包括：在线用户信息、分配历史信息、地址利用率等；在线用户报表信息需包含 IP 地址、上线时间、终端标识、属地、设备类型、主机名、所属接口等关键信息；地址分配历史查询报表需包含 IP 地址、属地、起始时间、终止时间、时长、终端标识等关键信息；地址利用率统计报表需包含分配地址数、地址总数、地址利用率、历史峰值利用率等关键信息。 15、用户注册审批：支持员工、访客用户的注册。支持自定义注册信息，要求可以定义必须填写的注册信息项，可根据需要启用/禁用自定义项。支持注册审核管理功能，已注册终端必须通过管理员手动审核通过之后才可以接入网络。支持注册及审核通过后手机/邮箱方式通知申请者。提供终端注册的日志记录功能。支持 MAC 账号、员工账号、手机验证码、访客验证码等账号管理。支持管理员预申请访客验证码。 16、▲身份认证：支持本地 Radius 认证系统，支持包含 PAP、CHAP 等加密

		认证方式。支持与 AD 域服务器、LDAP 服务器实现联动认证。支持外部访客以访客码、短信验证码形式登录。支持注册账号的有效时长设置，用户账号超时后不能认证通过。支持用户认证通过后主动下线，退出认证。支持在线终端强制踢下线，可选择是否加入黑名单控制用户不能再登录认证。支持用户登录密码忘记找回。 17、终端实名审计：支持终端实名录入，包括员工账号、姓名、联系方式、设备类型等信息。支持认证通过的在线终端展示，并可关联实名信息。
7	主机安全系统	通过部署轻代理，实现对主机安全管制，包括但不限于内存马监控、漏洞无效化、安全工具集合库、微隔离等功能模块，对东西向流量进行监控管理 1、★支持实时检测在内存中加载网站恶意文件，无任何本地文件、恶意代码注入的检测。需要展示内存对应的类名、父类名、所属类加载器、内存对应大小、MD5 信息等。 2、对于内存 Webshell 类型事件，支持下载内存中 dump 出的 class 文件，并直接对 class 文件进行反编译处理，还原为源代码文件，方便分析判断。 3、★提供高价值的安全分析工具，用户可以灵活配置，自助检查各类系统问题，包括文件查询、网络工具、进程查询、Web 查询、账号控制、安全工具、其他等，利用这些工具，可以快速便捷地帮助用户进行查询分析或是响应处理。 4、微隔离产品形态为基于代理的微隔离模式，服务端应支持私有化部署。 5、支持一键生成 Linux、Winoows 系统安装命令，安装过程无需重启。 6、支持一键启动微隔离功能，无需逐一登陆主机安装。 7、可点击主机查看当前主机具体信息，除基本信息（主机名、操作系统、业务组、标签）外，还应显示对外开放端口级所对应的服务/进程。 8、在拓扑图中提供基于端口、协议、进程的流量搜索功能 9、可按照流量的状态（正常、异常等）、类型（组内、组间等）、次数进行筛选查看不同流量 10、策略同步后统计同步成功和失败的主机数量，并可查看同步失败的主机和失败原因，根据失败原因修复后，主机可接收到最新策略，并且之前同步失败的提示消失。 11、策略管理可根据访问者、被访问者、服务等维度进行筛选。 12、提供宽松访问控制模式，对配有策略的服务端口，符合策略的访问为正常，其他访问为异常，进行告警或阻断；对无策略端口的访问为未处理状态。 13、★对于开启微隔离功能的主机，自动记录主机防火墙的状态，可通过控制台查看防火墙快照的详情。 14、在不实际阻断连接的前提下，对不符合策略的异常连接产生告警，以系统消息、邮件等形式通知管理员。 15、相同的异常告警聚合后被记录下来，并提供详细信息如被访问主机和来源主机的基本信息（如 IP、主机名、分组、标签）、端口、协议、进程、告警次数、首次发现时间、最新发现时间等 16、可对异常访问告警标记为已处理，告警被移除并生成处理记录，以后相同的访问仍会触发告警 17、可查看和导出处理历史，内容要素包括归档时间和告警事件的详细内容 18、调整主机的分组、标签时，检测是否会导致主机的策略发生变化，并提示主机将新增或删除哪些策略，管理员确认后才真正执行分组、标签的调整。

		19、基于流量监控技术，对识别的漏洞攻击流量进行针对化的屏蔽。 20、支持在主机伪造任意或漏洞文件，可自定义文件路径，文件名，文件大小等，并监控文件访问行为。 21、支持实时监控文件访问/操作行为，对于尝试访问/操作漏洞文件的异常行为进行实时告警，事件信息至少包含事件发现时间，主机 IP，文件路径，执行的操作，进程信息等。 22、支持根据文件路径、适用主机范围，批量在主机添加监控规则，监控已设置规则的文件，一旦尝试访问文件，或对文件进行操作，即上报告警。其中文件路径应支持输入多个。 23、支持查看事件的详情信息，可查看按照攻击来源视角聚合的事件，至少包含首次发现时间，最近发现时间，访问主机，文件操作的完整进程链，被访问漏洞文件的静态信息。