网络安全管理运维实训基地建设项目 采购项目

合 同

合同编号：ZX2026-03-43

甲 方：西安航空职业技术学院(采购人名称)

乙 方：深圳市讯方技术股份有限公司(中标人名称)

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律法规规定，西安航空职业技术学院（采购人名称）（以下简称：“甲方”）通过公开招标 采购（采购方式）确定 深圳市讯方技术股份有限公司（中标人名称）（以下简称：“乙方”）为 网络安全管理运维实训基地建设项目（项目名称）的中标 投标人。甲乙双方同意签署《网络安全管理运维实训基地建设项目（项目名称）合同》（合同编号：ZX2026-03-43，以下简称：“合同”）。

1. 合同文件

下列文件是构成本合同不可分割的部分：

（1）合同条款；

（2）中标通知书；

（3）招标文件；

（4）投标文件；

（5）其他（根据实际情况需要增加的内容）。

组成合同的各项文件应互相解释，互为说明。合同文件的解释优先顺序以上述文件先后顺序为准。

2. 合同主要标的及数量（**后附具体参数**）

乙方应按照合同的规定，提供本项目《招标（采购）文件》中有关要求的产品及服务，包括但不限于以下内容：

序号	货物名称	品牌	型号规格	单价（元）	数量	小计（元）	备注
1	下一代防火墙	奇安信 奇安信 奇安信 讯方	NSG2000-TE45 NSG2000-TC-4S-QW NSG-SSD-256-QW 定制	203000	2	406000	
2	入侵防御系统	奇安信 奇安信 讯方	P2000-TE20 P2000-TE-4X-Int-GF-RTU 定制	214000	1	214000	
3	上网行为管	奇安信	NBM200-DS120	200000	1	200000	

	理系统	奇安信 讯方	NBM-DS-4S-ZW-RTU 定制				
4	网络运维设备	华为 华为 华为 华为 华为 讯方 华为 讯方 讯方 讯方 Fusion Server 讯方 讯方 讯方	AR6121E USG6525F S5755-H24T4Y2CZ S5755-H24P4Y2CZ AirEngine 5773-21 EC616 S5735-L48T4XE-A-V2 定制 职前通在线学习与就业平台V3.0 讯方e-Bridge教学管理平台软件V1.0 2288H V6 讯方教学有方大模型智能应用平台V1.0 定制 定制	222500	4	890000	
5	信息安全教学实训设备	Fusion Server 奇安信 讯方	2288H V6 奇安信网神网络安全综合演练系统v7.0 定制	368000	1	368000	
合计				大写：人民币贰佰零柒万捌仟元整 小写：¥2078000元			

3.合同总金额及付款方式

3.1合同总金额

本合同总金额为人民币 贰佰零柒万捌仟元(¥2078000)。本项目包括但不限于税费、运输、保险、安装、调试、技术支持、质量保障、售后服务、培训和合同中规定乙方应承担的其他义务的费用已由乙方计入本合同总金额中。

3.2付款方式

一次付清，项目验收合格后10日内，支付合同总金额的100.00%。

3.3履约保证金

中标（成交）供应商在签订合同后5个工作日内，向采购人缴纳合同金额5%的履约保证金。履约保证金应优先用于支付乙方依据本合同约定应付的违约金，以及

因项目执行过程中造成的人身意外损害所产生的赔偿费用。

4. 合同签订地：陕西省西安市

5. 合同生效

合同附件为本合同不可分割的一部分，与本合同具有同等法律效力。合同一式五份，乙方一份，甲方三份，采购代理机构（见证方）一份。在甲、乙及见证方签字盖章，并甲方收到乙方提交的履约保证金后生效。

6. 其他约定：见证方只见证合同金额。

甲　方 西安航空职业技术学院	乙　方 深圳市讯方技术股份有限公司
（盖章）	（盖章）
地址：西安市阎良区人民路48号	地址：深圳市南山区招商街道沿山社区工业六路21号网谷创享大厦1栋A座1705-1706
邮编：710089	邮编：518067
全权代表：（签字）	法定代表人：戴毅
	被授权代表：（签字）
电话：02986852313	电话：0755-88866500
传真：	传真：
	开户银行：中国工商银行深圳蛇口支行
	账号:4000020219200697590
日期：2026年6月24日	日期：2026年6月17日
见证方	
（盖章）	
日期：2026年6月17日	

一、合同条款

合同条款前附表

序号	内容
1	合同名称：网络安全管理运维实训基地建设项目 合同编号：ZX2026-03-43
2	甲方名称：西安航空职业技术学院
	甲方地址：西安市阎良区迎宾大道500号
	甲方联系人：王小春　　电话：18143794542
3	乙方名称：深圳市讯方技术股份有限公司
	乙方地址：深圳市南山区招商街道沿山社区工业六路21号网谷创享大厦1栋A座1705-1706
	乙方联系人：　梁乔　　电话：18792663959
	乙方开户银行名称：中国工商银行深圳蛇口支行 账号：4000020219200697590
4	合同金额：大写：人民币贰佰零柒万捌仟元整　　小写：¥2078000元
5	包装方式及运输： （1）包装：产品包装应采取防潮、防晒、防腐蚀、防震动及防止其他损坏的必要措施。供应商应承担由于其包装或防护措施不妥而引起的货物锈蚀、损坏和丢失等任何损失造成的责任或费用。 （2）运输：运杂费一次包死在总价内，包括并不限于生产厂到施工现场所需的装卸、运输（含保险费）、现场保管费、二次倒运费、吊装费等费用。 （3）乙方负责设备的拆卸、运输、安装、调试等全流程工作，直至本项目验收合格，乙方应当选派具有相关作业资质的设备和作业能力的人员进行前述作业，作业期间若发生人员伤亡事故，由乙方自行承担赔偿责任，由此给甲方造成的一切经济损失，均由乙方负责承担。
6	交货时间及地点：自合同签订之日起2个月内完成项目交付；西安航空职业技术学院指定地点。
7	质量保证期：自项目最终验收合格之日起5年。
8	验收方式及标准：按照招标文件、投标文件及合同约定执行。
9	付款方式：一次付清，项目验收合格后10 日内，支付合同总金额的 100.00%。
10	履约保证金及其返还：项目验收合格后10日内，甲方无息由原缴费账户退还履约保证金全款。
11	违约金约定：
12	误期赔偿费约定： （1）如因乙方责任而造成延期交货，甲方可在合同未付款中直接扣除延期交货的违约金，每延期交货一天按合同总价款的0.03%向甲方支付违约金，该违约金由甲方在应支付货款中直接扣除，乙方对此无任何异议。逾

	期超过7日，甲方有权单方解除合同，乙方应按照合同总金额的5%承担违约责任。 （2）如整机验收不合格，且乙方在规定的整改期内整改后仍达不到验收标准的，视为乙方延期交货，甲方可在合同未付款中直接扣除延期交货违约金，每延期一天按合同总价款的0.03%扣除；同时，乙方应向甲方重新更换和投标文件一致的同生产厂家、同品牌、同型号、同规格的全新产品。二次交付仍不符合验收条件的，甲方有权单方解除合同，乙方应按照合同总金额的5%承担违约责任。
13	合同履行期限：自合同生效之日起至合同全部权利义务履行完毕之日止。
14	合同纠纷的解决方式： 首先通过双方协商解决，协商解决不成，则通过以下途径之一解决纠纷(请在方框内画“√”选择)： □提请_____仲裁委员会按照仲裁程序在_____(仲裁地)仲裁 ☑向甲方所在地人民法院提起诉讼

1.定义

本合同下列术语应解释为：

1.1 “甲方”是指采购人。

1.2 “乙方”是指中标人。

1.3 “合同”系指甲乙双方签署的、合同中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

1.4 “货物”是指根据本合同规定，乙方按照招标(采购)、投标文件，向甲方提供符合要求的全部产品，包括一切设备、机械、仪器仪表、备品备件、工具及与信息处理和交流有关的硬件、软件以及所有有关的文件等。

1.5 “服务”是指根据本合同规定，乙方承担与货物有关的相关服务，包括但不限于运输、保险、安装、调试、技术支持、质量保障、售后服务、培训和合同中规定乙方应承担的其他义务。

1.6 除非特别指出，“天”均为自然天。

2. 合同标的标准

2.1 乙方为甲方交付的货物及服务应符合招标文件所述的内容，如果没有

提及适用标准，则应符合相应的国家标准。这些标准必须是有关机构发布的最新版本的标准。

2.2 除非技术要求中另有规定，计量单位均采用中华人民共和国法定计量单位。

2.3 货物还应符合国家有关安全、环保、卫生的相关规定。

3. 质量保证

3.1 乙方应保证所供货物是全新的、未使用过的，并完全符合或高于合同要求的质量、规格和技术性能的要求。

3.2 乙方应保证其货物在正确安装、正常使用和保养条件下，在其使用寿命期内具有满意的性能，或者没有因乙方的行为或疏忽而产生的缺陷。在货物最终交付验收后不少于合同规定或乙方承诺(两者以较长的为准)的质量保证期内，本保证保持有效。

3.3 如果服务和交付物与合同不符或不符合甲方要求，或证实交付物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，由此引起的全部费用由乙方承担。若以上原因导致或引起甲方损失及导致或引起第三方受到损害的，全部赔偿责任均应由乙方承担。

3.4在质量保证期内所发现的缺陷，甲方应尽快以书面形式通知乙方。

3.5 乙方收到通知后应在本合同规定的响应时间内以合理的速度免费维修或更换有缺陷的货物或部件，零件费用及维修费用由乙方承担，如同一设备/软件连续出现同一故障超过5次，乙方应另行向甲方更换整套设备/软件，质保期限自收到更换设备/软件之日起重新起算。乙方指定【张玉乐】（电话：【18937509815】，邮箱：【zhangyule@xunfang.com】）为售后联系人，负责接收甲方维修通知，联系人变更应提前3个工作日书面告知甲方。乙方收到报修通知后1个工作小时内首次响应；远程故障4个工作小时内修复；需现场处理的，技术人员48

个工作小时内抵达现场，力争72个工作小时内（自报修时起算）修复。严重故障（导致甲方核心业务系统瘫痪的），乙方2个工作小时内响应、24个工作小时内到场、48个工作小时内恢复基本运行。维修结束后乙方向甲方提交书面维修报告，由甲方签字确认。上述时效中“工作日”不含法定节假日。

3.6　在质量保证期内，如果货物的质量或规格与合同不符，或证实货物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第10.1条规定以书面形式向乙方提出补救措施或索赔。

3.7　乙方在约定的时间内未能弥补缺陷，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方根据合同规定对乙方行使的其他权利不受影响。

3.8　本合同的质量保证期见合同条款前附表。

4.包装要求

4.1　除合同另有规定外，乙方提供的全部货物均应按标准保护措施进行包装，这类包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定现场。

4.2　乙方应承担由于其包装或防护措施不当而引起的货物损坏和丢失的任何损失责任和费用。

4.3　每一个包装箱内应附一份详细装箱单和质量证书。

5.知识产权

5.1　乙方应保证所提供的货物及服务免受第三方提出侵犯其知识产权(专利权、商标权、版权等)的起诉。如果甲方在使用乙方货物或货物的任何一部分过程中，第三方提出货物侵犯其专利权、工业设计权、使用权等知识产权，乙方应当修正以避免侵权。

5.2　如果甲方在使用乙方货物或货物的任何一部分过程中，第三方指控侵

犯其专利权、工业设计权、使用权等知识产权，乙方将自费为甲方、各采购人答辩，并支付法院最终判决的甲方应支付第三方的一切费用。

5.3 有关本项目的所有设计、施工文件的著作权属于甲方。乙方有保护甲方著作权的义务，并对在设计过程中所接触到的甲方的相关秘密有保密的义务。未经甲方书面同意，乙方不得将设计文件、成果另作其他商业用途或向任何第三方披露，不得将设计文件用于其他项目工程的建设，不得用于与本协议无关的工程。发生此类情况时，乙方应当赔偿甲方损失，甲方保留向乙方追偿的权利。

6. 权利瑕疵担保

6.1 乙方保证对其出售的货物享有合法的权利。

6.2 乙方保证在其出售的货物上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

6.3 如甲方使用该货物构成上述侵权的，则由乙方承担全部责任。

7. 保密义务

7.1 甲乙双方在采购和履行合同过程中所获悉的对方属于保密的内容，双方均有保密义务。

8. 履约保证金

8.1 乙方应以银行转账等非现金形式向甲方提供。乙方以银行、保险公司出具保函形式提交履约保证金的，经甲方书面同意后可执行。

8.2 履约保证金具体金额及返还要求见合同条款前附表。

8.3 如乙方未能履行合同规定的义务，甲方有权按照本合同的约定从履约保证金中进行相应扣除。乙方应在甲方扣除履约保证金后15天内，及时补充扣除部分金额。

8.4 乙方不履行合同，或者履行合同义务不符合约定使得合同目的不能实现，履约保证金不予退还，给甲方造成的损失超过履约保证金数额的，还应当对

超过部分予以赔偿。

9.交货与验收

9.1　交货地点：合同条款前附表指定地点。

9.2　交货时间：合同条款前附表指定时间。

9.3　甲方在收到乙方交付的货物后应当及时组织验收。

9.4　货物的包装：符合出厂规范及符合《商品包装政府采购需求标准（试行）《快递包装政府采购需求标准（试行）》，包装完整无破损，防雨、防潮等各种符号标识清楚，进口设备应具有原产国标识且标识清楚。货物的表面瑕疵，甲方应在验收时当面提出；对质量问题有异议的应在安装调试时进行记录。

9.5　在验收过程中发现数量不足或有质量、技术等问题，乙方应按照合同要求采取补足、更换或退货等处理措施，并承担由此发生的一切费用和损失。

9.6　甲方对货物进行检查验收合格后，甲方应在货物检查验收合格后3日内签署验收文件。如甲方在该期限内未提出书面异议，则视为验收合格。

9.7　大型或者复杂的货物采购项目，甲方可以邀请国家认可的质量检测机构参加验收工作，并由其出具验收报告。

9.8　在履约验收环节，乙方须按照《商品包装政府采购需求标准（试行）《快递包装政府采购需求标准（试行）》的环保要求出具检测报告。

9.9 乙方负责设备的拆卸、运输、安装、调试等全流程工作，直至本项目验收合格，乙方应当选派具有相关作业资质的设备和作业能力的人员进行前述作业，作业期间若发生人员伤亡事故，由乙方自行承担赔偿责任，由此给甲方造成的一切经济损失，均由乙方负责承担。

10.违约责任

10.1　质量缺陷的补救措施和索赔

(1)在合同条款规定的检验、安装、调试、验收和质量保证期内，如果乙方

提供的产品不符合质量标准或存在产品质量缺陷，甲方应在合理期限要求乙方进行整改。若整改后仍未达到合同约定的标准，甲方可根据法定质量检测部门出具的检验证书向乙方提出索赔，乙方应按照甲方同意的下列一种方式结合起来解决索赔事宜：

①乙方同意退货并将货款退还给甲方，由此发生的一切费用和损失由乙方承担。如甲方以适当的条件和方法购买与未履约标的相类似的货物，乙方应负担新购买类似货物所超出的费用。

②根据货物的质量状况以及甲方所遭受的损失，经过甲乙双方商定降低货物的价格。

③乙方应在接到甲方通知后7日内负责采用符合合同规定的规格、质量和性能要求的新零件、部件和设备来更换有缺陷的部分或修补缺陷部分，其费用由乙方负担。同时，乙方应在约定的质量保证期基础上相应延长修补和更换件的质量保证期。

(2)如果在甲方发出索赔通知后10日内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后10日内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付货款中扣除索赔金额或者没收履约保证金，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

10.2 迟延交货的违约责任

（1）如因乙方责任而造成延期交货，甲方可在合同未付款中直接扣除延期交货的违约金，每延期交货一天按合同总价款的0.03%向甲方支付违约金，该违约金由甲方在应支付货款中直接扣除，乙方对此无任何异议。逾期超过7日，甲方有权单方解除合同，乙方应按照合同总金额的5%承担违约责任。

（2）如整机验收不合格，且乙方在规定的整改期内仍达不到验收标准的，

视为乙方延期交货，甲方可在合同未付款中直接扣除延期交货违约金，每延期一天按合同总价款的0.03%扣除；同时，乙方应向甲方重新更换和投标文件一致的同生产厂家、同品牌、同型号、同规格的全新产品。二次交付仍不符合验收条件的，甲方有权单方解除合同，乙方应按照合同总金额的5%承担违约责任。

10.3 未履行合同义务的违约责任

(1)守约方有权终止全部或部分合同。

(2)乙方违约的，甲方有权没收全额履约保证金。

(3)由违约一方支付违约金，违约金标准见合同条款前附表(各单位可根据实际情况自行约定)。

(4)违约金不足以弥补守约方实际损失、可预见或者应当预见的损失，由违约方全额予以赔偿。

（5）乙方迟延履行质保义务，每逾期一日，应按照合同总价款的5‰计算违约金，乙方逾期履行质保义务致使甲方无法正常使用设备/软件超过7日，甲方有权单方解除合同或部分解除合同，同时，乙方应按照合同总价款的5%支付违约金。

11.不可抗力

11.1 如果合同双方因不可抗力而导致合同实施延误或合同无法实施，不应该承担误期赔偿或不能履行合同义务的责任。

11.2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

11.3 在不可抗力事件发生后，当事方应及时将不可抗力情况通知合同对方，在不可抗力事件结束后3日内以书面形式将不可抗力的情况和原因通知合同对方，并提供相应的证明文件。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理

的时间内达成进一步履行的协议。

12. 合同纠纷的解决方式

12.1 合同各方应通过友好协商，解决在执行合同过程中所发生的或与合同有关的一切争端。如协商30日内(根据实际情况设定)不能解决，可以按合同规定的方式提起诉讼。

12.2 诉讼应由甲方住所地人民法院管辖。财产保全担保保险费、财产保全申请费、律师代理费、差旅费、评估费、鉴定费及诉讼费等与仲裁或诉讼活动相关费用应由败诉方负担。

12.3 如诉讼事项不影响合同其他部分的履行，则在诉讼期间，除正在进行诉讼的部分外，合同的其他部分应继续执行。

13. 合同修改或变更

13.1 如无重大变故，甲方双方不得擅自变更合同。

13.2 如确需变更合同，甲乙双方应签署书面变更协议。变更协议为本合同不可分割的一部分。

13.3 在不改变合同其他条款的前提下，甲方有权在合同价款10%的范围内追加与合同标的相同的货物或服务，并就此与乙方签订补充合同，乙方不得拒绝。

14. 合同中止

14.1 合同在履行过程中，因采购计划调整，甲方可以要求中止履行，待计划确定后继续履行；合同履行过程中因投标人就采购过程或结果提起投诉的，甲方认为有必要或财政部门责令中止的，应当中止合同的履行。

15. 终止合同

15.1 若出现如下情形，在甲方对乙方违约行为而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面通知书，提出终止部分或全部合同，如合同终止，乙方应按照合同总价款的5%向甲方支付违约金：

(1)如果乙方逾期提供货物或服务超过7日或乙方未能在甲方同意延长的期限内提供货物或服务；

(2)如果乙方未能履行合同规定的其他任何义务，出现两次服务达不到承诺标准情况，甲方有权终止合同；

(3)如果甲方认为乙方在本合同的竞争或实施中有腐败和欺诈行为。

15.2 如果甲方根据上述第15.1条的规定，终止了全部或部分合同，甲方可以适当的条件和方法购买乙方未能提供的货物或服务，乙方应对甲方购买类似货物或服务所超出的费用负责。同时，乙方应继续执行合同中未终止的部分。

15.3 合同全部解除或部分解除后，乙方应当自收到甲方解除通知之日3个工作日内退还甲方已支付采购费用，逾期未退还的，应当已应退金额为基数，按照5‰/日计算逾期利息。

16.破产终止合同

16.1 如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。

16.2 该终止行为将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

17.其他终止合同情况

17.1 若因不可抗力导致本合同无法继续履行的，甲方可以终止合同。如设备已经运输，甲方可承担合同终止部分的设备运输费用。

17.2 乙方在执行合同的过程中发生根本违约，对履行合同有直接影响的甲方可以终止合回而不给予乙方任何补偿。

17.3 因国家法律法规或政策发生重大变化，导致本合同内容无法继续履行的，甲方可以终止合同。如设备已经运输，甲方可承担合同终止部分的设备运输费用。

18. 合同转让和分包

18.1　乙方不得以任何形式将合同转包，或部分或全部转让其应履行的合同义务。

18.2　除经甲方事先书面同意外，乙方不得以任何形式将合同分包。

19. 适用法律

19.1　本合同适用中华人民共和国现行法律、行政法规和规章，如合同条款与法律、行政法规和规章不一致的，按照法律、行政法规和规章修改本合同。

20. 合同语言

20.1　本合同语言为中文。

20.2　双方交换的与合同有关的信件和其他文件应用合同语言书写。

21. 合同生效

21.1　本合同应在双方签字盖章后生效。

22. 合同效力

22.1　除本合同和甲乙双方书面签署的补充协议外，其他任何形式的双方约定和往来函件均不具有法律效力，对本项目无约束力。

23. 检查和审计

23.1在本合同的履行过程中，甲方有权对乙方的合同履约情况进行阶段性检查，并对乙方投标时提供的相关资料进行复核。

23.2　在本合同的履行过程中，如果甲乙双方发生争议或者乙方没有按照合同约定履行义务，乙方应允许甲方检查乙方与实施本合同有关的账户和记录，并由甲方指定的审计人员对其进行审计。

24 通知及送达

双方确认本协议约定地址为各类通知、文件、法律文书的有效送达地址，适用于协议履行期间及后续产生争议时的协商、调解、仲裁、诉讼全流程。以纸质

文件寄送的，无论对方是否实际签收，文件自寄出后第3个工作日视为送达成功。任何一方变更送达地址的，应提前10个工作日以书面形式通知对方；未履行通知义务的，按上述地址送达即视为有效送达，由此产生的送达不能风险由变更方自行承担。

一、采购清单

序号	设备名称	数量（套）	备注
1	下一代防火墙	2	
2	入侵防御系统	1	
3	上网行为管理系统	1	
4	网络运维设备	4	
5	信息安全教学实训设备	1	核心产品

二、技术要求（技术要求中标注★号参数为实质性要求，投标人必须响应，并提供要求的佐证材料予以佐证，若不满足或未提供佐证材料或佐证材料无法佐证，按无效文件处理）

（一）下一代防火墙

1、硬件要求：

★1.1、每套包含4台设备（提供承诺函）；

1.2、单台设备性能要求为：网络层吞吐量≥10G，并发连接≥300万，每秒新建连接数≥10万；标准机箱≥2U，单电源；板载≥8个千兆电口，≥2个千兆光口，≥2个万兆光口，≥1个扩展插槽，≥1个Console口，≥2个USB接口；默认含≥200个IPsecVPN标配并发隧道数，默认含≥200个SSLVPN标配并发用户数；具备应用控制功能、URL过滤功能、病毒防护功能、入侵防御功能、威胁情报检测功能；

1.3、提供三年硬件维保服务（包含设备返修服务，维修备机服务，远程技术支持服务）、三年安全威胁情报数据订阅、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务；

2、产品功能：

●2.1、产品可实现MPLS流量透传操作，可对MPLS流量开展安全审查相关实操，具体可执行漏洞防护配置、反病毒查杀、间谍软件检测与清除、内容过滤规则设置、URL过滤策略调整、基于终端状态的访问控制策略部署等操作,适配实训过程中对MPLS流量安全管控的实操需求。(提供功能截图)

2.2、产品可进行静态路由、策略路由及动态路由的配置与调试操作;动态路由方面,可部署RIPv1、RIPv2、RIPng、OSPF、OSPFv3、BGP4/4+、ISIS等路由协议，完成各类动态路由的设置、运行及维护实操；可配置静态多播路由和动态多播路由，其中动态多播路由可部署PIM-SM（稀疏模式）协议，实现动态多播路由的相关实操配置。

●2.3、产品可进行NAT44和NAT66转换配置操作，可完成一对一、一对多、多对一的源地址转换及目的地址转换的配置与调试,可部署SYMMETRIC模式和FULL_CONE模式并完成两种模式的切换与调试实操；（提供功能截图）

2.4、产品可进行路由模式、透明模式下的HA部署操作，可将HA部署配置为主备模式、主主模式，并可实现会话、用户、配置的实时同步操作；可配置HA部署的接口联动功能，实操过程中当某个端口出现失效（DOWN）状态时，可实现同一接口组中其他端口同步进入失效（DOWN）状态；可对HA部署的接口权重进行配置与调整操作，同时可开展BFD链路探测操作，完成链路状态的探测与监测。

2.5、产品可进行虚拟防火墙的配置操作，可对物理防火墙的各类资源（包括新建、吞吐、会话数、安全策略数、源NAT数、目的NAT数、日志存储数量），以保留值及最大值的形式完成自动分配操作。

▲2.6、产品可基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种条件，进行访问控制策略的配置与部署操作；可执行地理区域对象的导入操作，同时可开展重复策略的检查操作。（提供功能截图）

2.7、产品可基于不同安全区域，开展各类 Flood 攻击的防御配置与调试操作，具体可针对 SYN Flood、UDP Flood、ICMP Flood、IP Flood、Frag Flood、DNS Flood、HTTP Flood、NTP Query Flood、NTP Reply Flood 和 SIP Flood 攻击，部署对应的防御策略；同时可配置警告、丢弃、普通防护、增强防护、授权服务器防护等多种防护措施。

2.8、产品可进行漏洞防护功能的配置与部署操作，可对漏洞防护特征库进行分类设置，至少可分为缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；可配置漏洞防护的执行动作，包括日志、阻断、放行、重置等，且可批量设置针对某一分类或全部攻击签名的执行动作；可基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议，开展漏洞防护的配置与调试操作。

3、下一代防火墙配件

3.1、业务扩展板卡：数量≥2 张,每张扩展板卡提供≥4 个千兆光口；

3.2、扩展硬盘：数量≥2 块，每块硬盘容量≥240G，硬盘类型为 SSD 硬盘。

4、配套机柜

4.1、功能：可安装交换机、路由器、配线架、KVM、UPS 电源等网络设备；

4.2、机柜尺寸：≥600*600*1000mm；

4.3、工业 PDU 机柜插座≥2。

（二）入侵防御系统

1、硬件要求：

★1.1、每套包含 8 台设备（提供承诺函）；

1.2、单台设备性能要求为：网络层吞吐量≥10G，IPS 吞吐≥2G，并发连接≥200 万，每秒新建连接数≥6 万；标准机箱≥1U，双电源，≥4TB 硬盘；板载≥8 个千兆电口（支持 3 组 bypass），≥4 个千兆光口，≥2 个扩展插槽，≥1 个 Console 口，≥2 个 USB 接口；

1.3、提供三年硬件维保服务（包含设备返修服务，维修备机服务，远程技术支持服务）。三年入侵防御特征库升级服务、应用识别库及威胁情报升级订阅服务；

2、产品功能：

2.1、产品可进行命中时间分析操作，可查看并展示被命中安全策略的名称、状态、命中数、策略创建时间、首次命中时间及最近命中时间；可开展安全策略推荐实操，可指定策略流量，对指定的策略流量进行分析后，自动生成源地址精度更高的安全策略；可基于源地址精确合并、源地址子网合并两种方式进行操作，并自动生成策略名称、源对象、目的对象及服务对象，全程贴合实训实操需求。

▲2.2、产品可进行应用识别相关配置操作，其应用特征库中包含的应用数量（非应用协议的规则总数）≥3000 种；可对每种应用的属性开展深度识别操作，可查看每种应用预定义的风险系数，同时可将应用基于类型、数据传输、风险等级等特征进行分类操作，贴合实训过程中应用识别相关的实操需求。（提供功能截图）

2.3、产品可基于关键字，开展 Email 发件人、收件人的接收过滤、发送过滤或双向过滤操作。

2.4、产品可对应用的文件传输行为，开展上传、下载及双向的文件类型过滤操作；可针对至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件、微博七种分类的应用，分别配置文件传输行为的文件类型过滤策略，完成各类应用下文件过滤的相关实操，贴合实训实操需求。

2.5、产品可基于安全区域，开展异常包攻击防御的配置与调试操作，可针对至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片、

圣诞树攻击、NTP monlist 在内的异常包攻击类型，部署对应的防御策略，保障不同安全区域的网络防护效果；

2.6、产品可开展弱口令检测相关实操，可配置并执行主动检测、被动检测两种弱口令检测方式；可基于网段、协议、用户名字典、弱口令字典，开展弱口令完整扫描操作，扫描执行方式可设置为手动执行或自动执行；可基于数字、字母、数字和字母组合、自然顺序、键盘顺序、特殊字符、用户名、重复字符等多种规则，开展弱口令检测操作。

●2.7、产品可开展暴力破解相关检测与防御操作，可针对至少包括 FTP、IMAP、WEBLOGIC、VNC、Telnet、RLOGIN、RDP 在内的 14 种协议，部署暴力破解检测策略；可手动设置攻击频率、持续检测时间的具体参数，完成相关配置调试；同时可配置日志、阻断、放行、重置和加入动态黑名单等处置动作，根据实际需求完成各类处置方式的设置与切换；（提供功能截图）

2.8、产品可对网络内威胁事件的数量及事件的严重性进行统计操作；可执行一键跳转操作，跳转后查看威胁事件详情，并自动显示关联日志；可基于网络连接、应用名称、威胁事件，开展威胁事件的处置操作。

2.9、提供网络安全方面的课程资源，课程采用虚机形式开展完成，课程资源包含 Web 中间件漏洞、Web 安全、漏洞利用、Web 渗透测试、Linux 防火墙、入侵检测、网络攻防等方面的学习内容。实验数≥190 个。

3、入侵防御系统配件

3.1、业务扩展板卡：数量≥2 张,每张扩展板卡提供≥4 个万兆光口。

4、配套机柜

4.1、功能：可安装交换机、路由器、配线架、KVM、UPS 电源等网络设备；

4.2、机柜尺寸：≥600*600*1000mm；

4.3、工业 PDU 机柜插座≥2。

（三）上网行为管理系统

1、硬件要求：

★1.1、每套包含 8 台设备（提供承诺函）；

1.2、单台设备性能要求为：网络层吞吐量≥8G，最大并发连接数≥200 万，最大新建连接数≥5 万；≥1U 硬件，标配≥6 个千兆电接口（其中含 1 个管理接口和 1 个 HA 接口），提供≥1 个扩展插槽，单电源，≥1T 机械硬盘。具备网页过滤、用户认证、应用控制、内容审计、带宽管理、行为监控分析等功能；

1.3、提供三年硬件质保服务。三年软件版本与协议库升级服务，包含系统版本升级服务，以及应用协议库、URL 特征库和审计特征库的升级服务。

2、产品功能：

2.1、产品可进行网关模式、镜像模式、网桥模式、多路桥接及 Portal 模式的配置与部署操作。

2.2、产品可在 IPV4/IPv6 环境下，开展网址访问审计操作、生成分析报表操作；可在 IPv6 环境下，正确审计并显示用户的 IPv6 地址，完成相关审计查看操作。

2.3、产品可自动识别网络中终端的 IP 地址、MAC 地址、终端类型、操作系统、终端厂商及网卡厂商等信息，完成终端信息的采集与查看操作。

2.4、产品可自动扫描发现网络中已占用的 IP 地址，可图形化展示指定 IP 地址的在线状态、当前使用者、MAC 地址及活跃时间，完成 IP 地址占用情况的查看与分析操作。

▲2.5、产品可基于云端大数据安全平台，开展恶意 URL 访问的封堵操作及日志记录操作；可进行与威胁情报大数据平台的对接操作，能够快速开展失陷主机的识别、封堵操作，并完成相关日志记录操作。（提供功能截图）

2.6、产品可对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用进行独立分类设置，并开展各类内容的识别与控制操作。

2.7、产品可配置独立的网安应用行为审计策略，可基于用户、时间、位置、工具，开展审计策略的设置操作。
2.8、产品可依据应用协议库，配置单用户应用使用时长限制操作；可依据应用协议库，配置单用户应用流量限制操作；具备配置仅与用户关联、与应用和流量无关的上网时长/次数限额策略。
●2.9、产品可在外发途径管控中，基于内容大小执行外发控制操作；支持不开启 SSL 的运行方式，对终端影响较小；仅对内容外发进行管控，不影响正常浏览、下载等行为。（提供功能截图）
●2.10、产品可对外发内容进行过滤操作，具备 SCP/SFTP 应用场景下的外发内容过滤；可基于关键字、正则表达式配置过滤规则；可对身份证号码、银行号码、电话号码、地址等敏感信息执行过滤操作。（提供功能截图）
2.11、提供系统安全方面的课程资源，课程采用虚机形式开展完成，课程资源包含日志分析、恶意代码、软件安全、容灾备份、计算机病毒、数字取证、信息隐藏、移动安全、逆向工程等方面的学习内容。实验数不低于 250 个。
3、上网行为管理系统配件
3.1 业务扩展板卡：数量≥2 张.每张扩展板卡提供≥4 个千兆光口。
4、配套机柜
4.1、功能：可安装交换机、路由器、配线架、KVM、UPS 电源等网络设备
4.2、机柜尺寸：≥600*600*1000mm
4.3、工业 PDU 机柜插座≥2。
（四）网络运维设备
1、网络运维设备-路由器
★1.1、每套包含 10 台设备（提供承诺函）；
1.2、交换容量≥20Gbps ，转发性能≥9Mpps，以官网最小值为准；
1.3、具有≥2 个扩展插槽；
1.4、千兆电口≥8 个，千兆 Combo 接口≥ 3 个，万兆光口≥1 个；
1.5、内存≥4GB ，flash≥1GB；
1.6、支持多种路由协议，如静态路由、RIP、OSPF、BGP 等；
1.7、具备 VPN 功能，可支持 IPsec VPN、GRE VPN 等；
1.8、支持基于 IP 地址、端口号、协议类型等信息对网络流量进行访问控制；
▲1.9、采用国产芯片，提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告；
1.10、配套实验仿真系统
●1.10.1 提供可扩展的、图形化网络仿真工具平台，主要对企业网路由器、交换机、防火墙、AC 控制器、AP、数据中心交换机进行软件仿真，支持大型网络模拟（提供软件界面配置截图）。
1.10.2 分布式部署：不仅支持单机部署，同时还支持 Server 端分布式部署在多台服务器上。分布式部署环境下能够支持更多设备组成复杂的大型网络，灵活部署。
1.10.3 高仿真度：控制台和仿真环境分离，仿真环境中运行产品仿真大包。
1.10.4 可与真实设备对接：通过虚拟设备接口与真实网卡的绑定，实现虚拟设备与真实设备的对接。
1.10.5 支持企业网三层交换机、数据中心交换机，支持型号不少于 3 种，交换机支持 GVRP、SEP、MPLS VPN、M-LAG、SVF、VXLAN、等协议，支持路由策略特性。
▲1.10.6 支持路由器模拟，路由器支持模块化（同异步 WAN 模块、LAN 模块），支持模拟路由器型号不少于 5 种。（提供软件界面配置截图）
1.10.7 支持无线局域网模拟，支持单独的 AC、AP 模拟，AC 支持 POE 供电，支持多种型号的设备。
1.10.8 支持防火墙模拟，状态防火墙、虚拟综合业务网关模拟。

●1.10.9 为保证系统兼容性，本次所用产品与路由器、核心交换机、POE 交换机、网络运维设备-防火墙、无线 AP 非同一品牌的，需提供产品对接兼容性测试报告。

2、网络运维设备-防火墙

★2.1、每套包含 2 台设备（提供承诺函）；

2.2、防火墙吞吐量≥2Gbps ，并发连接数≥300 万，每秒新建连接数≥8 万；

2.3、IPS 吞吐量≥1.8Gbps ，IPSec VPN 吞吐量≥2.1Gbps；SSL VPN 吞吐量≥300Mbps；

2.4、IPSec VPN 隧道数≥4000 ，SSL VPN 并发在线用户数≥100；

2.5、支持设备的 WEB 管理 CLI 控制命令；

2.6、支持 HTTP、FTP、SMTP、POP3、IMAP、NFS 等协议的病毒防护；

2.7、支持 SRv6 协议，支持 IPv6 协议栈；

2.8、支持 NAT 地址复用技术；

▲2.9、系统预定义 IPS 签名数量≥12000，支持用户自定义签名规则，支持正则表达式，可识别应用≥6000，访问控制精度到应用功能。应用识别与入侵检测、防病毒相结合，提高检测性能和准确率，提供官网截图或产品彩页或加盖厂家公章的产品说明书；

2.10、支持基于源 IP/目的 IP ，MAC 地址，服务类型，应用类型，安全域，时间段进行安全策略规则的配置；

2.11、千兆 Combo 接口≥8 ，千兆电口≥2 ，万兆光口≥2 ，交流电源，含 Advanced 软件功能包；

2.12、支持 IPSec VPN 、SSL VPN 、GRE 等 VPN 技术；

2.13、具备流量限制功能；

2.14、具备记录网络访问日志、攻击事件日志、系统运行日志等功能；

2.15、配套实训软件

2.15.1 软件须采用 C/S 模式架构，所有客户端必须登录服务端才能进入系统，服务端须能够控制学生终端连接数量，可查看进入系统的学生列表信息，包括主机名、主机 IP、登录时间等；

2.15.2 软件必须能够模拟管理网管、多种不同型号的传输网设备；系统应能够虚拟传输网的网管和网元等功能单元，并且能够实现该功能单元的配置及在线修改与告警联动，可在网管进行模拟业务配置，在测试终端上对所模拟的业务进行验证。

2.15.3 软件须具备模拟真实设备组网功能，学生可在此自由创建不同的传输网设备，并将之连接成不同的物理组网，组建完成之后，可在网管上进行网元创建、业务配置。

▲2.15.4 软件的模拟网管应提供真实设备中的大部分业务，可以配置多种业务链路；其网管配置界面必须完全模仿真实网管业务数据配置，配置内容与真实情况一致，能够真实反映工程现场数据配置和操作步骤；（提供功能界面截图）

▲2.15.5 软件应对网管配置进行分类导航，方便学生查看及操作，网管配置要包含网元管理、设备管理、业务管理、告警管理等；系统应具备仿真故障告警功能，在业务配置过程中出现错误时，该功能模块可给予系统告警，可及时查看和处理告警并定位到具体问题所在；（提供功能界面截图）

2.15.6 软件须支持一键清除当前客户端所有数据，以 excel 表形式导出实验报告、记录实验数据，数据包含设备组网规划图、网管逻辑组网图、业务配置数据；导入前期保存的数据等等。

●2.15.7 软件须支持读取客户端操作日志，客户端操作日志自动保存在服务端；显示客户端登录信息，包括学号、姓名、IP、登录模式、登录时间、在线状态。投标时提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告。

2.15.8 软件应具备仿真验证功能，最后进行结果验证，可通过在模拟真实设备视图中添加测试终端，点开测试终端用 PING 命令测试各终端的 IP 来确定业务是否正常联通。

●2.15.9 软件应具备业务配置、参数详解的功能。投标时提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告。

3、网络运维设备-核心交换机

★3.1、每套包含 6 台设备（提供承诺函）；

3.2、设备整机支持 10/ 100/ 1000BASE-T 以太网端口≥24 个，万兆 SFP+≥4 个；

3.3、整机交换容量≥2Tbps ，包转发率≥560Mpps；

3.4、 ≥1 个扩展插槽；

3.5、要求配置冗余电源，冗余风扇；

3.6、支持 MAC 表项≥256K ，ARP 表项规格≥128k；

●3.7、全端口支持 MACsec 功能，提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告；

4、网络运维设备-POE 交换机

★4.1、每套包含 4 台设备（提供承诺函）；

4.2、设备整机支持 10/100/1000BASE-T 以太网端口≥24 个，万兆 SFP+≥4 个，支持 POE+供电；

4.3、交换容量≥2Tbps ，包转发率≥560Mpps；

4.4、 ≥1 个扩展插槽；

4.5、冗余电源，冗余风扇；

4.6、支持 MAC 表项≥256K ，ARP 表项规格≥128k；

4.7、支持 VxLAN 功能，支持 BGP EVPN；

5、网络运维设备-无线 AP

★5.1、每套包含 4 台设备（提供承诺函）；

5.2、室内放装双频 AP，全频段均支持 802.11be 标准，兼容 IEEE 802.11a/b/g/n/ac/ax 标准；

5.3、支持 100M/1000M/2.5G 电口≥1 个；

5.4、支持空间流≥4，整机速率≥3.5Gbps；

5.5、内置智能天线，内置蓝牙；

5.6、提供 USB 接口，可用于扩展外置物联网（支持 ZigBee、RFID 等协议）；

5.7、支持 FIT/FAT/云管理工作模式，无需 WAC 可小型组网；

5.8、使用国产化 Wi-Fi 芯片，提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告。

6、网络运维设备-串口服务器

★6.1、每套包含 2 台设备；每台提供≥16 个设备管理串口（提供承诺函）；

6.2、支持 TCP 和 UDP Socket ，串口支持（如 TCP 、UDP 、TCP 和 UDP）；

6.3、处理器：≥32 位；内存：≥8 兆；网口速度：不低于 10/ 100M 自适应，支持手动设置，保护：≥2KV ESD；提供串口接口：≥16 个 RS-232 串口，形式：RJ45；支持信号：如 RS-232:TxD/ RxD/ RTS/CTS/ DTR/ DSR/ DCD/GND 等；支持串口通讯参数数据位：如 5/6/7/8；支持校验：如 None/Even/Odd/Space/Mark 等；支持停止位：如 1 ，2 等；支持流控：如 RTS/CTS ，XON/XOFF 等；支持串口可变速度范围：支持 300bps - 460.8Kbps；协议：支持 DHCP ，Telnet ，TCP ，UDP ，IP ，ICMP ，ARP 等；配置支持：包括但不限于 Telnet 、console 、WEB 浏览器；支持 TCP SERVER ，TCP CLIENT 和 UDP ，支持全兼容网络 API；支持 PPP ，以及 PAP ， DHCP 等协议。

7、网络运维设备-48 口接入交换机

★7.1、每套包含 1 台设备（提供承诺函）；

7.2、千兆电口≥48 个，万兆光口≥4 个，万兆光模块≥4 个；交换容量≥670Gbps，包转发率≥200Mpps；

7.3、支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持≥1024 认证用户同时在线；

7.4、支持 MAC 表项≥32K；

7.5、支持全组播协议；

7.6、支持 IPv4 路由表≥4K，支持 IPv6 路由表≥1K；

7.7、支持 ARP 表项≥2K。

8、网络运维设备-网络机柜及机柜辅材

★8.1、每套包含 2 台机柜（提供承诺函）；

8.2、功能：可安装交换机、路由器、配线架、KVM、UPS 电源等网络设备

8.3、机柜尺寸：≥600*600*2000mm

8.4、工业 PDU 机柜插座≥2。

9、网络运维设备--综合配套设备（所有网络运维设备共用 1 套）

9.1、在线网络课程资源学习平台

9.1.1 平台采用 B/S 架构，提供简洁明了的 Web 页面，兼容多种浏览器访问，包括但不限于谷歌、火狐、 360、IE，支持电脑、手机端、APP 应用访问学习，提供不低于 50 个账号，使用时长不少于 3 年。

9.1.2 平台拥有统一消息通讯功能，支持自定义的短信、邮件、系统消息通知管理。

9.1.3 系统用户角色访问模块分为学生端、管理员端；

9.1.4 学生用户权限包括课程、直播、考试、测评、就业、个人主页等；

9.1.5 覆盖 ICT 领域全技术方向体系课程、职业素养课程，用户可根据方向和分类选择对应课程或根据自身职业学习路径系统化学习，对学习课程有效评论；

●9.1.6 直播时间列表，允许学生通过 PC 或手机进行观看，可多维互动，支持互动聊天弹幕，讲师与学员音视频连麦，问答/提问，签到，抽奖，倒计时等，直播完成后可观看实时直播回放；（提供功能界面截图）

9.1.7 平台提供行业标准考试测评，考试类型分为顺序练习、随机练习、综合考试、专项智能学习和错题练习，有考试、背题和答题模式，学生参与练习、考试后支持能力评估、答案解析明细/报告，纠错反馈、笔记记录等；

9.1.8 根据学生求职意愿，进行岗位精准筛选，为学生提供个性化、实时职位信息，学生可进行简历投递，企业 HR 对简历进行查看、下载，对符合的简历下发面试通知等，支持企业与用户在线视频面试；

●9.1.9 涵盖 APESK 测试系统的初级量表：职业锚、霍兰德职业兴趣、DISC、PDP、16PF、荣格理论第一步；高级量表：荣格第二步、DISC 完整版测试、销售业务岗，研发岗性格评估等；15-30 分钟测评，自动生成报告，为测评者提供全面准确的评估报告和优化方案，提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告；

9.1.10 实时查看了解自己当前的学习情况：已完成的课程数量，累计观看视频时长。具体包括我的课程进度、考试情况、简历投递、订单明细、账号资料编辑，个人头像上传，更换手机号、修改密码、消息提醒等；

9.1.11 课程学习过程数据分析：查看/导出记录的学生在线学习开始时间、结束时间、学习时长，以及学习过程中随机打卡（在线弹窗打卡）等信息；

●9.1.12 数通初级认证课程资源：包含理论 PPT、视频及实验手册。具体数量：≥20 份文档 PPT，≥80 个视频，且视频总时长≥1600 分钟，≥15 个实验手册；该课程配套的相关资源支持在平台上进行观看，支持实验操作。知识点或实验：包含但不限于网络参考模型、网络设备操作系统、以太网交换基础、VLAN 原理与配置、生成树原理与配置、以太网链路聚合、IP 地址与配置、IP 路由基础、OSPF 原理与配置、IPv6 地址与配置、ACL 原理与配置、AAA 原理与配置、网络服务与

应用、NAT 原理与配置、数据中心网络基础、WLAN 技术基础、WLAN 组网架构、WLAN 工作原理与配置、网络设备管理、网络编程自动化、网络故障排除、园区网络典型组网方案等。（提供课程资源证明材料）

▲9.1.13 数通中级认证课程资源：包含理论 PPT、视频及实验手册。具体数量：≥40 份文档 PPT，≥25 个视频，且视频总时长≥3700 分钟，≥14 个实验手册；该课程配套的相关资源支持在平台上进行观看，支持实验操作。知识点或实验：包含但不限于 IP 路由基础、OSPF、IS-IS、BGP、路由和流量控制、以太网交换技术、组播、IPv6、网络安全、网络可靠性、网络服务与管理、WLAN、网络解决方案；IGP 高级特性、BGP 高级特性、IPv6 路由、以太网高级技术、MPLS 技术、网络运维、网络故障排除、网络割接等。（提供课程资源证明材料）

●9.1.14 安全初级认证课程资源：包含理论 PPT、视频及实验手册。具体数量：≥11 份文档 PPT，≥20 个视频，且视频总时长≥1300 分钟，≥7 个实验手册；该课程配套的相关资源支持在平台上进行观看，支持实验操作。知识点或实验：包含但不限于信息安全概念、信息安全标准与规范、常见攻击手段、防火墙安全策略、防火墙 NAT 技术、防火墙双机热备技术、入侵防御技术、密码学基础、PKI 机制、IPSec/SSL VPN 技术。（提供课程资源证明材料）

9.2、网络教学及设备管理系统

9.2.1 具备实训室实验室、设备、工位管理功能，具备实训室分类管理功能；具备真实的设备布放展示功能；（提供现场演示）

▲9.2.2 具备虚拟实验和真实实验的工位管理功能，按照 IP 地址分配状况添加相关工位，并可进行工位统一模板的导入，投标时提供具有 CMA/CNAS 资质认证的检测机构出具的检测报告；

9.2.3 具备实训室资产管理功能，包括设备的借出归还状态，记录资产登记在册的详细情况，可修改相关的资产信息；

9.2.4 具备多种格式教学资源的管理功能；具备多种实验接入方式，如第三方 CS 实验应用、自研类的接入。

9.2.5 具备同时多人多次上机实验功能，为实验的每组学生提供良好的上机环境和多人同时实验的实验方式；

9.2.6 具备商用设备软件控制功能，针对不同类型的设备进行定制化开发。

★9.2.7 具备设备控制，远程设备状态查看，远程设备数据配置中，数据下发及数据脚本导入功能（提供功能截图或官网截图或产品彩页或加盖厂家公章的技术说明书）；

9.2.8 具备设备分组、管理设备与学生分组；

9.2.9 具备设备状态监控，实时上报异常设备；

9.2.10 具备部分设备数据还原，设备复位；

9.2.11 具备脚本管理，脚本导入下发；（提供现场演示）

9.2.12 具备实验队列管理、实验项目管理、实验结果验证功能；

9.2.13 具备查看教学资源并同时操作支持 WEB 控制方式的设备；

●9.2.14 软件要求是成熟应用系统软件，投标时提供软件著作权登记证书。

9.2.15 配套硬件配置：≥2U 机架服务器，非 OEM 产品，自主研发；处理器：配置 2 颗 CPU，单颗主频:≥2.1GHz，核心≥12 核 ，缓存≥18M，采用 X86 架构；内存：配置 2*32GB ECC DDR4 内存,内存插槽数≥16 个插槽；硬盘：配置≥4*600GB 通用硬盘-SAS 12Gb/s-10K rpm-128MB；电源：配置 2 个≥900W 冗余热插拔电源，并提供配套的电源连接线；风扇：配置 4 个热拔插对旋风扇，支持 N+1 冗余；网络：≥2*GE+,2*10GE 含模块，机架安装导轨；可管理和维护性：1） 集成系统管理处理器支持：风扇监视和控制、电源监控、温度监控、服务启动/关闭、固件更新、日志管理，可通过可视化工具提供系统未来状况的可视显示； 2）具有图形管理界面及其他高级管理功能；3）配置独立的远程管理控制端口，支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作。

9.3、AI 辅助教学模块（提供不低于 3 个账号，使用时长不少于 3 年）

9.3.1 平台支持 web 端和移动 app 端双平台访问，兼容主流浏览器及操作系统自适应布局；支持跨平台部署，支持云化部署或一体机部署；

9.3.2 平台采用 B/S 架构，实现了高效、稳定的运行模式、支持大数据的实时多地采集；支持页面大小随分辨率自适应调整。

9.3.3 平台引入插件系统，插件机制将其中强耦合的模块进行解耦，通过插件市场，任何人都可以在这里安装、上传和分享插件。

9.3.4 平台支持使用 DeepSeek/Qwen/baichuan 大语言模型为基座，使用微调、RAG 等技术实现智能问答系统；支持实时多源数据采集与处理。

▲9.3.5 平台提供模型训练微调的工具集。支持在通用预训练大模型（如 DeepSeek、Qwen、baichuan 等）基础上，通过特定领域或任务的数据进行二次训练；支持在微调过程中自定义模型路径、选择不同的微调方法、不同参数的调整（例如学习率、训练轮数、最大梯度范数等），保存训练参数、导出训练模型。【提供功能截图】

9.3.6 平台支持智能体创建功能支持零代码/低代码配置工作流，集成 RAG（检索增强生成）、长期记忆、多工具调用。（提供现场演示）

9.3.7 具备多种智能体类型，基本对话、对话工作流、工作流等，用户快速构建人工智能应用。

▲9.3.8 平台支持工作流自定义编排，通过将复杂的任务分解成较小的步骤（节点）降低系统复杂度，减少了对提示词技术和模型推理能力的依赖，提高了 LLM 应用面向复杂任务的性能，提升了系统的可解释性、稳定性和容错性。为解决自动化和批处理情景中复杂业务逻辑，通过可视化拖拉拽的形式进行编排，支持串行和并行两种编排设计模式，工作流提供了丰富的逻辑节点，如代码节点、IF/ELSE 节点、模板转换、迭代节点等，方便构建自动化流程。【提供功能截图】

9.3.9 平台支持智能体市场管理、智能体审核管理；支持用户查看自己创建智能体的审核状态，并支持发布与收藏功能。

●9.3.10 智能体创建完成可发布 API、供外部系统对接。【提供功能截图】

9.3.11 平台内置行业应用。深度融合教育场景需求，构建智能服务体系。内置教育行业应用包含但不限于课程辅导、教案生成、智能出题、职业规划等。（提供现场演示）（课程辅导应用搭载 24 小时虚拟助教，支持快速对接学校本地课程数据提供个性化课程推荐；教案生成应用支持结合文档解析技术和生成式技术实现教案生成;智能出题应用支持对文档知识点抽取并生成与知识点相关的考题，类型包含但不限于单选题、多选题、填空题；职业规划应用支持提供个性化发展建议、提供岗位推荐。）

9.4、配套机柜

9.4.1 功能：可安装交换机、路由器、配线架、KVM、UPS 电源等网络设备

9.4.2 机柜尺寸：≥600*1000*1000mm

9.4.3 工业 PDU 机柜插座≥2。

9.5、提供基于本次项目采购硬件设备所需的配套设施。

（五）信息安全教学实训设备

1、硬件规格

1.1、≥2U 机架服务器，非 OEM 产品，自主研发；处理器：配置≥2 颗 CPU，单颗主频:≥2.5GHz，核心≥16 核 ，缓存≥24M，线程≥32，采用 X86 架构；内存：配置 8*32GB ECC DDR4 内存,内存插槽数≥16 个插槽；硬盘：≥8*960GSSD 通用硬盘，≥1*1.92T SSD；网络：≥4*GE +2*10GE 含模块；机架安装导轨（提供官网截图或产品彩页或加盖厂家公章的技术说明书）；

1.2、电源：配置 2 个≥900W 冗余热插拔电源，并提供配套的电源连接线；风扇：配置≥4 个热拔插对旋风扇；

2、功能指标

2.1、系统管理：

2.1.1 系统采用 B/S 架构，支持账号密码登录；多个业务模块如教学实训、考试测评、攻防竞赛等共用底层服务及硬件资源；

2.1.2 具备为每个学员生成能力画像，以雷达图形式展示学员能力等级测评达标情况；统计学员在全平台完成任务获得的能力点，并以可视化形式展示学员所掌握能力在各能力模型中的覆盖率情况。

2.2、资源管理：

●2.2.1 具备能力图谱管理，以树形图形式展示三级能力体系结构，自定义编辑能力方向、能力类别和能力点的名称和描述，支持批量导入导出图谱数据，支持批量展开/收起最后一级能力点，支持调整上级节点来变更在图谱中的位置，展示能力点关联资源数量统计并查看关联资源详情；（提供功能截图）

▲2.2.2 具备能力模型编排，每个能力模型支持自定义一到五级的能力等级，配置模型各等级对需要掌握能力点的要求程度，如熟悉、掌握和精通，支持按照能力要求模块设置权重，权重支持自动平均分配和手动配置两种模式。（提供功能截图）

2.2.3 具备虚拟设备的增、删、改、查功能，支持创建 KVM、容器两种类型的虚拟设备，可设置设备权限为公开还是私有，私有设备仅创建人可用，虚拟设备的创建支持上传镜像和安装 ISO 两种方式，支持对虚拟设备的名称、分类、图标、描述等基础信息设置，支持配置网卡名称、网卡数量、CPU、RAM、登录账号信息，KVM 类型设备支持网卡驱动、硬盘驱动、是否 UEFI 启动等信息配置，容器支持启动命令自定义配置；支持引用溯源，查看设备资源被哪些业务资源所引用；

2.3、拓扑编辑

2.3.1 具备自定义实验网络拓扑，拖拽虚拟设备、物理设备至画布区快速搭建实验拓扑，拓扑编辑时设备图标即拖即用，无需配置关联镜像，可自定义修改虚拟机设备的 CPU、内存、网卡数量、网卡驱动、硬盘驱动等参数；

2.3.2 具备网络设备模拟，模拟数字路由器和数字交换机，可通过页面简单配置完成网络调试，启动数字网络设备不占用算力资源；

2.3.3 具备空节点图标辅助搭建网络拓扑，既丰富拓扑展示效果，又不占用算力资源，支持文本框节点，在拓扑中自定义文本描述；

2.3.4 具备设备连线，支持设备分组划分区域展示，支持拓扑图导出、居中显示、放大缩小显示，支持输入设备名称查询并将设备居中选中显示；支持统计拓扑所需算力资源，计算最大并发套数；支持复制整个拓扑或单个虚拟机到其他拓扑中粘贴实现快速搭建拓扑；

2.3.5 具备一键启动/关闭拓扑设备，也支持单个设备启动/关闭，设备关闭时显示灰色图标，设备启动后变为蓝色图标；支持编辑后的虚拟机另存为私有虚拟设备模板；支持设置每个拓扑节点在学员端的展示和操作权限，权限包括是否显示节点，是否能操作，是否能启动；

●2.3.6 具备拓扑设备 IP 地址管理，支持 web 页面及虚拟机内部两种 IP 地址及分配操作，在 web 页面配置虚拟机及容器的 IP、掩码、网关信息，虚拟机内只需设置为自动获取 IP；虚拟机内配置静态 IP 信息，系统自动监测并同步显示在 web 页面；（提供功能截图）

●2.3.7 具备设备 VNC、RDP、SSH 几种连接访问模式，支持向虚拟机内粘贴文本和导入文件，可将所需文件从本地电脑通过 web 页面中的上传功能直接上传至虚拟机中，在 RDP/SSH 模式下虚拟机文件管理树形展示虚拟机内的文件列表，并支持将文件下载至本地电脑；支持标签页形式在多个设备控制台之间快速切换（提供功能截图）。

2.4、课程管理

2.4.1 具备自定义编辑教学课程内容，包括理论、仿真和虚实结合三种类型，新建课程可设置课程名称、描述、分类，可添加协作人一起编辑课程，具备课程版本管理，记录每次课程变化；

2.4.2 具备章节目录管理，包括章、节两级目录和小节单级目录两种类型，支持调整章节顺序和批量删除小节；

▲2.4.4 课程小节内容支持设置关联能力点、建议学习时长、实验手册、实验拓扑、课件资料（PDF/MP4）、学习任务等信息，学习任务支持理论题的课后习题、探针任务和 flag 任务、附件任务四种类型；手册支持 Markdown 在线编辑和上传文件两种类型，Markdown 类型的手册支持分步式实验手册设计，每一步可关联至学习任务，学员完成关联的学习任务后才能解锁手册的下一步，实现互动式学习；（提供功能截图）

2.5、教学管理

●2.5.1 具备教学任务下发，教员可根据不同任务类型安排授课方式、任务时长，可面向班级进行常规授课，也可面向部分学员进行定向授课；支持设置单人/分组的实验形式，自定义小组数量和每组人数上限，支持选择同一课程中的多个小节作为同一教学任务进行下发，下发后教员可增删教学任务中的小节，并灵活控制小节是否对学员可见；（提供功能截图）

2.5.2 具备下发任务时系统根据上课人数、实验拓扑自动计算所需硬件资源，若硬件资源不足，系统可自动提醒教员切换成分组的实验形式，并可根据资源情况自动计算设置小组数量；

2.5.3 教员可对当前课程学习模式进行个性化设置，自定义对学员开启/隐藏实验手册、实验环境、课件资料、学习任务等学习资源；

2.5.4 具备自定义创建学习方案，也可继承系统内已有的方案进行修改，方案自定义多个学习阶段，每个阶段关联课程和测评试卷。系统支持以时序图的形式展示每阶段的课程间的关联关系。

2.6、学员实训

2.6.1 前台系统具备日程表和任务列表两种形式展示学习任务，可按年/月筛选查看，进入课程任务详情，可查看视频、文档以及实操实验等方式进行学习；

2.6.2 实验环境具备关闭和销毁两种方式，关闭实验环境在虚拟机中的操作自动保存，下次启动实验时可在上次实验操作基础上继续实验，支持教员统一销毁学员的环境和系统定时自动销毁环境两种销毁机制；

2.6.3 系统具备学员自学模式，学员可自由从课程库选择课程学习，也可查看教员规划的学习方案，按照方案指导自学课程和自测考试。

2.7、项目实训

2.7.1 系统具备工程实践式的小学期项目实训模式，学员按照项目工作团队的形式分组参与实训，每组自定义一套实训拓扑环境共同完成同一个项目；

2.7.2 系统具备对项目综合实训的基本信息、项目流程、网络拓扑进行设置，项目流程默认包括项目启动、任务分工、项目规划、阶段审核、项目实施、项目测试、项目验收阶段，可根据每个项目的运行阶段添加、删除相关流程，可设计每个流程环节中的具体工作内容及任务；

●2.7.3 系统具备学员在项目实训过程中自定义编辑实验拓扑，教员控制学员编辑拓扑可用 VCPU 和内存资源限制。（提供功能截图）

2.8、题库及试卷管理

●2.8.1 具备多道仿真题共用一套题目环境，支持静态 flag、动态 flag、探测任务等多种答案形式；探测任务通过探针执行命令检测用户在虚拟机中的操作结果，动态 flag 通过关联路径、修改变量、命令执行或脚本执行等多种方式生成不同 flag；（提供功能截图）

2.8.2 系统具备试卷管理，设置试卷名称、难度、分类、合格分值和组卷方式，组卷方式支持题库自选、策略组卷和模型组卷三种；题库自选组卷模式从题库中选择题目组成固定试卷，具备批量和单独设置题目的分值；策略组卷模式通过设置试卷题目出题范围，如选择题目类型、分类、能力点、难度和出题数量，根据策略规则从题库中自动选题生成试卷；模型组卷根据能力模型的能力点和权重要求自动生成出题策略和试卷；

2.9、考试管理

2.9.1 考试任务的配置信息包括设置考试难度、使用试卷、考试时间和考试对象；支持考试答题次数的设置，在开放时间段内可多次答题考试；支持填空题平台阅卷、人工阅卷两种方式；自定义设置是否允许考生在提交试卷后查看成绩或答案；支持同一场考试配置多套试卷，系统随机为每位考生独立分配试卷；针对同套试卷支持题目乱序功能；

2.9.2 考试任务中教员可查看考试人员提交状态和每个考试人员的试卷答题情况；支持教员清除已答题学员的答题记录，让学员重新答题；

2.10、竞赛题库管理

2.10.1 CTF 题和攻防题环境具备容器和 KVM 两种虚拟化技术，自定义上传环境镜像，具备题目环境的参数配置，包括 CPU、RAM、访问端口、管理端口、登录账号密码等；CTF 题和攻防题支持自定义解题思路；

2.10.2 攻防题具备自定义检测规则设置，具备检测协议和检测脚本上传两种方式，根据需求可使用 HTTP、TCP 检测协议从服务端口、期望输出、URL 等方面设置，也具备使用脚本方式；

2.10.3 CTF 题具备动态 flag，可根据需求使用关联路径、修改变量、命令执行、curl、脚本执行等方式进行设置，CTF 题目支持多附件上传，不同附件不同答案；

2.11、竞赛任务管理

2.11.1 系统具备管理员对竞赛任务的增删改查操作，竞赛任务配置主要包括竞赛名称、竞赛开始及结束时间、竞赛 LOGO、竞赛形式、竞赛规则、竞赛题目、参赛团队或个人、计分规则、环境部署、展屏配置、协作管理人等信息；

2.11.2 系统具备管理员自由组合理论赛、CTF 赛和攻防赛模式，对赛前、赛中、赛后三个阶段的维护管理，实现对竞赛全流程的掌控，具备多场竞赛同时管理，具备多人协作管理一场竞赛；

▲2.11.3 系统具备题目、竞赛双策略计分规则，CTF 题目具备基础分和附加分规则设置，攻防赛具备初始分、固定得失分或零和机制设置；竞赛计分规则具备所得分值、所得分值/第一名所得分值两种基数计算方式，并分别设置理论赛、CTF 赛和攻防赛分值系数，在比赛结束后按照系数相加实现相对合理的总分统计；（提供功能截图）

●2.11.4 系统具备题目环境一键快速部署，根据参赛人员、题目类型自动分配虚拟机 IP，并以拓扑和列表两种样式展示题目部署情况，具备 CTF 题和攻防题分开启动/关闭，具备单个题目环境重置；竞赛选手访问题目环境具备系统内置 VPN 和局域网两种方式（提供部署前后功能截图）。

2.12、竞赛过程管理

2.12.1 系统具备竞赛管理员对竞赛开始/暂停状态进行控制，具备准备模式、全通模式、解题模式、解题+加固模式、加固模式、攻防模式的网络控制，各模式之间一键配置，分别对系统、题目进行访问控制、环境隔离控制；

2.12.2 系统具备多种防作弊机制，包括竞赛各阶段的网络控制、动态 flag、攻防赛题目环境异常状态检测、参赛人员来源 IP 验证、赛后提交 Writeup 等多个方面。

2.12.3 系统具备来源 IP 段输入验证、登录绑定，实现各团队题目环境隔离，具备来源 IP 启用/不启用、清除 IP 等操作；

2.12.4 系统具备竞赛中题目答题详情、团队答题详情的管理，CTF 题支持基础分、附加分、正确率、提交次数、提交时间、提交答案等数据记录展示，攻防题具备攻击成功次数、防守失败次数、答题状态、得分、失分等数据记录展示；

●2.12.5 系统具备 B/S 和 C/S 两种架构且不同风格的 CTF 赛和攻防赛 3D 可视化大屏展示，展示数据主要有答题动态、攻击路径、排行榜、得分趋势、得分详情等，布局上适用不同团队数量、不同题目分布，支持 16:9 和 32:9 两种规格展示效果。（提供功能截图）

2.13、竞赛训练

2.13.1 系统具备赛题训练模式，用户可自由选择训练题库的题目进行学习训练，CTF 题型具备查看解题思路，具备训练题目收藏；

2.13.2 教学课程资源：提供计算机基础及密码学方面的课程资源，课程采用虚机形式开展完成，课程资源包含 Python、Linux、Windows 操作系统、密码学、数据库、计算机网络等方面的学习内容。实验数不低于 200 个。

2.14、攻防竞赛资源

2.14.1 攻防竞赛题库资源，CTF 题目≥250 道，包含 CRYPTO、MISC、WEB、PWN、Reverse 五大方向；

2.14.2 WEB、PWN 类型的攻防题目合计≥40 道；

2.14.3 单选、多选、判断等理论题合计≥1200 道；

2.15、培训服务

2.15.1 为满足学校网络安全教学任务安排，须提供不少于每年 2 次每次不少于 24 课时的线下培训课程。

2.15.2 原厂专人负责学生战队的线上支持工作，包含协助运营校内网络安全攻防社区、每日群内更新攻防热点链接、新技术文章分项等，并组织线下技术讲座每年不少于 2 次。

（六）满足教学基础设施

严格按照安全规范完成设备所需要的供用电布线及网络综合布线施工，安装三相稳压器、壁挂式音箱系统（含配套麦克风），满足教学正常使用条件。