

合 同 书

合同编号： 豫财磋商采购-2025-1067

甲方（需方）：郑州轻工业大学

乙方（供方）：河南尔享科技有限公司

依据中华人民共和国相关的法律、法规，甲方针对豫财磋商采购-2025-1067 号招标文件的要求公开招标，乙方在公平竞争的条件下中标，为明确双方的权利和义务，经甲乙双方友好协商，签订合同如下：

一、 甲方向乙方采购设备一览表

序号	设备品牌及型号	技术参数	数量	单位	单 价（元）	总 计（元）
1	超聚变/2288H V5	详见附表	2	台	85500.00	171000.00
2	奇安信/奇安信网神网络安全实训系统 V6.0 (CSE-EDU-SMM)	详见附表	1	套	329000.00	329000.00
3	奇安信/奇安信网神网络安全实训系统 V6.0 (CSE-Course-JCVM)	详见附表	1	套	139000.00	139000.00
4	奇安信/网神 secWAF3600Web 应用防火墙 系统 V4.0 (W1500-LAB-A-PA-01)	详见附表	1	台	35800.00	35800.00
5	奇安信/网神 SecGate3600 防火墙系统 V3.6.6.0 (CSE-Course-JCCP-NGFW)	详见附表	1	套	69000.00	69000.00
6	奇安信/网神 SecGate3600 防火墙系统 V3.6.6.0 (CSE-Course-JCCP-WAF)	详见附表	1	台	45000.00	45000.00
7	奇安信/网神 SecGate3600 防火墙系统 V3.6.6.0 (NSG3000-LAB-A-PA-02)	详见附表	1	套	68600.00	68600.00
8	绿盟科技/绿盟网络入侵防护系统 V5.6 (NIPSNX3-HFB300)	详见附表	1	台	53000.00	53000.00
9	安恒信息/DAS-USM190-PRO	详见附表	1	套	55000.00	55000.00
10	安恒信息/DAS-TBTOOL-W3	详见附表	1	套	16200.00	16200.00
11	奇安信/奇安信天擎终端安全管理系统 V10.0	详见附表	1	套	7000.00	7000.00
12	奇安信/奇安信网神云锁服务器安全管理 系统 V8.0	详见附表	1	套	8000.00	8000.00

13	盛科/V530-48T4X	详见附表	1	台	17000.00	17000.00
14	康海/NC608BR	详见附表	1	台	4500.00	4500.00
15	新华三/LS-5135S-52P-SI	详见附表	1	台	3500.00	3500.00
16	尔享科技/尔享定制	详见附表	1	批	18000.00	18000.00
合 计		(人民币大写) 壹佰零叁万玖仟陆佰圆整, ¥1039600.00 元				
备 注		设备清单明细部分详见附件 1				

二、合同签订、交货时间、地点及方式

1. 甲乙双方签订合同后, 乙方负责在合同签订日起 30 天(日历日) 内将全部设备运到甲方指定地点, 并安装调试完毕。
2. 乙方在发货前应通知甲方, 甲方在收到乙方通知的当日, 向乙方提供收货联系人及详细收货地址。
3. 交货安装地点: 郑州轻工业大学科学校区
4. 交货方式: 免费送货、免费安装、免费调试。

三、验收标准及方法

1. 在乙方安装调试和培训完毕后, 由甲乙双方共同完成验收工作; 验收时, 由甲方组织专家及相关管理部门参加验收, 乙方派项目负责人与技术人员参加验收。
2. 所有设备的验收, 严格按照招标文件、投标文件和合同中所列的技术参数比照进行。
3. 乙方要协助使用单位完成校级验收所需的各种资料。

四、售后服务及承诺

1. 乙方应按本合同附表中规定的设备技术参数要求向甲方提供全新合格产品, 并有详细的中文或英文操作规程说明书等资料。产品性能严格符合该产品出厂的参数标准, 且完全提供该产品出厂时所配备的附件, 并保证产品质量标准。否则, 甲方有权要求乙方更换, 其间所发生一切费用由乙方负担。
2. 乙方提供的设备实行 5 年免费质保, 5 年上门服务(人力+配件), 终身保修。质保期过后终身上门免费维修, 维修只收取材料费, 不收取维修费, 软件免费升级。(具体售后服务及承诺按招投标文件执行)
3. 其他售后服务要求, 均按照厂商标标准售后服务执行。

五、付款方式

乙方把合同全部货物(系统)交货(完工)完成后, 并按照甲方指定的地点完成安装, 调试和操作培训。经甲乙双方验收合格后, 乙方凭中标通知书、合同、增值税专用发票等凭证办理付款手续, 甲方向乙方支付合同货款的 100%“人民币大写壹佰零叁万玖仟陆佰圆整”(¥1039600.00 元), 货款通过银行转帐(或电汇)支付。自验收合格之日起, 合同约定全部货物(系统)正常使用满 1 年无质

量问题后，学校无息退还履约保证金的 50%；合同约定内容履约完成后，学校无息退还剩余履约保证金。

单位名称：河南尔亨科技有限公司

开户行：中国建设银行郑州文博支行

账号：41050167283500000130

账号名称：河南尔亨科技有限公司

统一社会信用代码：91410102MA45NN162Q

企业规模：小型

六、保证、索赔、违约金

1. 乙方提供所有货物，必须为合同附件中标明的原厂全新正品，乙方不能交付设备，乙方向甲方支付未交付设备款总额 10%的违约金；乙方逾期交付设备，甲方有权拒收设备；乙方所交的设备品牌、型号、规格、质量不符合招标文件及合同规定，甲方有权拒收设备，乙方应负责更换并承担因更换而支付的实际费用；因更换而造成逾期交货，按逾期交货处理。

2. 若甲方无正当理由而拒收设备或不能按合同约定回款的，向乙方偿付拒收拒付部分设备款总额 10%的违约金。

3. 本合同所有设备在甲方未付款前，所有权归乙方，乙方有权收回。

七、争议的解决

甲乙双方应友好协商解决与合同或合同执行有关所产生的任何争议。如未能友好解决，双方可以向本地仲裁委员会申请仲裁，仲裁依据为该委员会颁布的仲裁条例。仲裁地点为郑州。仲裁裁决是终局裁决，对甲乙双方均有约束力，任何一方不得再寻求通过法院或其他机构修改该仲裁裁决，最终仲裁费用由败诉的一方承担。在仲裁期间，双方均应继续执行合同中除有争议的部分以外的其它部分。

八、不可抗力

由于台风、地震、水灾、战争、火灾以及其他非甲、乙方责任造成的，不能预见的、不能避免的、不能克服的客观情况为不可抗力。遇有不可抗力而造成甲方延期/无法付款或乙方延期/无法交货，甲方或乙方不承担责任，并应在以上所提及的不可抗力发生后立刻通知对方，并在随后的 14 个工作日内将事件的详情以及合同不能履行、或部分不能履行、或需要延期履行的理由的有效证明文件以特快专递的方式邮寄给对方。按照事件对履行合同的影响程度，由甲乙双方协商决定是否解除合同、部分免除履行合同的责任或延期履行。

九、未尽事宜

本合同的未尽事宜，甲乙双方可以协商解决或另行签定补充协议，补充协议与本合同为不可分割的组成部分。甲方在合同执行中如有其他额外的要求，乙方将提供有偿服务。

十、其他

本合同采购文件及其修改、响应文件及其修改、澄清、合同附件均为本合同的组成部分，与本合同具有同等的法律约束力，与本合同约定不一致之处，以本合同为准。本合同一式八份，甲方四份，乙方两份，招标公司两份，经双方代表签字盖章后生效。

(内容完)

甲方：郑州轻工业大学

地址：郑州市科学大道136号

代表：张永霞

联系电话：(0371)-86608291

日期：2025.10.23

乙方：河南尔享科技有限公司

地址：河南省郑州市高新技术产业开发区银屏路15号

代表：张永霞

联系电话：0371-63288507

日期：2025.10.23

合同附件 1:

设备分项报价一览表

序号	名称	规格型号	品牌	制造商	单位	数量	单价 (元)	合计 (元)	备注
1	综合运行硬件平台	2288H V5	超聚变	超聚变数字技术有限公司	台	2	85500.00	171000.00	
2	网络空间安全综合实验平台	奇安信网神网络安全实训系统 V6.0 (CSE-EDU-SMM)	奇安信	奇安信网神信息技术(北京)股份有限公司	套	1	329000.00	329000.00	
3	网络空间安全教学实验资源包	奇安信网神网络安全实训系统 V6.0 (CSE-Course-JCVM)	奇安信	奇安信网神信息技术(北京)股份有限公司	套	1	139000.00	139000.00	
4	Web 防火墙虚实结合联动实验设备	网神 secWAF3600Web 应用防火墙系统 V4.0 (W1500-LAB-A-PA-01)	奇安信	奇安信网神信息技术(北京)股份有限公司	台	1	35800.00	35800.00	
5	Web 防火墙虚实结合实验资源	网神 SecGate3600 防火墙系统 V3.6.6.0 (CSE-Course-JCCP-NGFW)	奇安信	奇安信网神信息技术(北京)股份有限公司	套	1	69000.00	69000.00	
6	防火墙虚实结合联动实验设备	网神 SecGate3600 防火墙系统 V3.6.6.0 (CSE-Course-JCCP-WAF)	奇安信	奇安信网神信息技术(北京)股份有限公司	台	1	45000.00	45000.00	

7	防火墙虚实结合实验资源	网神 SecGate3600 防火墙系统 V3.6.6.0 (NSG3000-LAB-A-PA-02)	奇安信	奇安信网神信息技术(北京)股份有限公司	套	1	68600.00	68600.00	
8	入侵防御虚实结合联动实验设备	绿盟网络入侵防护系统 V5.6 (NIPSNX3-HFB300)	绿盟科技	北京神州绿盟科技有限公司	台	1	53000.00	53000.00	
9	运维与风险控制联动系统	DAS-USM190-PRO	安恒信息	杭州安恒信息技术股份有限公司	套	1	55000.00	55000.00	
10	恶意代码检测工具	DAS-TBTOOL-W3	安恒信息	杭州安恒信息技术股份有限公司	套	1	16200.00	16200.00	
11	终端安全实验平台	奇安信天擎终端安全管理系统 V10.0	奇安信	奇安信网神信息技术(北京)股份有限公司	套	1	7000.00	7000.00	
12	综合运行硬件平台安全加固平台	奇安信网神云锁服务器安全管理系统 V8.0	奇安信	奇安信网神信息技术(北京)股份有限公司	套	1	8000.00	8000.00	
13	SDN 交换机	V530-48T4X	盛科	苏州盛科通信股份有限公司	台	1	17000.00	17000.00	
14	串口服务器	NC608BR	康海	北京康海电子技术有限公司	台	1	4500.00	4500.00	

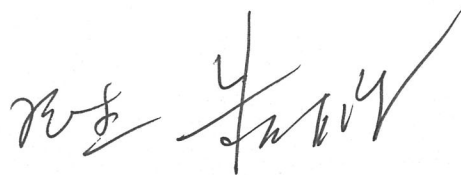
15	网络交换机	LS-5135S-52P-S I	新华三	新华三技术有限公司	台	1	3500.00	3500.00	
16	综合布线	尔享定制	尔享科技	河南尔享科技有限公司	批	1	18000.00	18000.00	
合计：人民币大写壹佰零叁万玖仟陆佰圆整，¥1039600.00 元									

合同附件 2:

备品、专用工具和消耗品表

序号	名称	型号和规格	数量	单价	总价	备注
1	网线	山泽六类网线	1批	0	0	投标报价 已包含
2	光纤跳线	山泽光纤跳线	1批	0	0	
3	扎带	山泽扎带	1批	0	0	
4	专用工具	山泽网络寻线测试仪	1批	0	0	

合同附件 3:



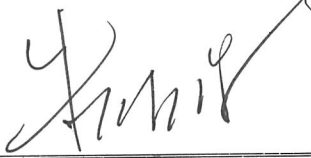
设备技术参数一览表

序号	产品名称	技术参数	备注
1	综合运行硬件平台	1、2U；4个千兆网口，2个万兆网口，2个万兆模块；2颗16核CPU；256内存；8*960GB SSD 硬盘；1*1.92T NVME硬盘；双电源； 2、支持与实训系统环境集成构建虚拟资源池，内置服务接口，为实训系统提供虚拟机资源调度与分配,支持虚拟化安全设备的授权统一维护及管理。 3、支持系统基于虚拟化管理架构和容器管理架构，提供对多平台的kvm、虚拟化和Docker容器进行统一虚拟化管理功能； 4、支持可实现内置包括网络设备、开源安全设备、基础服务器、web服务器、数据库、PC终端、武器库、CMS服务器等虚拟仿真环境，用户可自定制虚拟仿真环境。 5、可为网络安全实训平台提供计算资源，满足 60 人计算资源并发使用。	
2	网络空间安全综合实验平台	1、系统采用 B/S 架构，可提供资源概览，可显示基础教学、题库数量、实训项目、虚拟资源、安全工具的总体数量，支持显示当前平台知识点分布情况、知识点占比情况、基础内容分布情况； 2、系统支持对课程资源的管理功能，课程资源支持以发布状态或未发布状态显示，教师可对所属教学资源进行公开或私有设置，教师只对自己创建课程具有管理和编辑权限，支持教师对课程资源权限移交功能； 3、系统支持对课程内容的新建功能，课程资源类型包括理论、单机、仿真、产品四种类型，新建课程资源可对建议课时、包含知识点进行设置，课程内容需主要包括基本信息、操作手册、实验拓扑、视频、课件、工具资料等内容； 4、系统支持虚拟仿真实验环境，实验环境界面支持显示实验拓扑及配套实验手册、视频讲解和随堂练习等内容，实验拓扑环境支持显示操作机用户名、密码，支持对操作机时间进行延时操作； 5、系统支持自定义网络拓扑功能，创建实验环境支持以拓扑拖拽形式进行组建，提供拓扑图导出功能、居中显示、放大显示、拓扑全屏显示等拓扑查看功能； 6、网络拓扑支持快速复制粘贴功能，以便创建新实验环境下的拓扑的快速复用，支持虚拟资源拓扑可以粘贴到物理资源拓扑，物理资源拓扑只能粘贴到物理资源拓扑； 7、系统支持机架视图功能，机架视图场景化可提高实验操作物理体验，可形象展示设备面板情况以及网络连接情况，机架视图贯穿课程实验、实训项目等实操环节； 8、系统支持支持 WEB 文件上传功能，教师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，在实验环境下支持物理主机桌面中文本复制至 web 虚拟桌面； 9、系统支持虚实结合功能，在不改变用户原有拓扑环境，可将虚拟化设备和真实物理设备同时加入到同一个网络拓扑中进行实验，支持包含防火墙、上网行为管理、入侵防御、漏扫、WAF 等多种安全硬件设备； 10、系统支持老师根据教学需要自定义设置教学方案，教学方案支持对平台现有方	

	案继承，支持教师自己创建全新的教学方案，方案课程可进行先后排序，并支持课程内容以时序图的形式为老师提供参考授课计划，支持自定义调整时序图； 11、系统支持项目实训功能，支持对用户实际网络架构进行仿真还原，可仿真模拟包括企业网等保测评项目、企业网应急响应项目、企业网安全运维项目的环境及流程； 12、系统支持对项目实训的基本信息、项目流程、网络拓扑进行设置，项目流程包括项目启动、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，支持对每个阶段的流程环节内容的设计，支持对流程的添加、删除等功能； 13、项目实训过程中默认支持实验的断点保存功能，可自动保存实验内容，并支持对实训过程中对项目网络拓扑的编辑修改，如重新规划网络架构，增加新设备资源，更设备改连接线； 14、系统支持考试测评的试卷管理功能，平台提供试卷模板，试卷模板提供公开、私有属性选项，公开属性下平台的所有教师用户可使用并且编辑，私有属性下试卷模板只能被当前教师所查看。 15、系统支持对试卷的添加、删除、筛选功能，试卷支持名称、试卷分类等信息进行设置，试卷选题支持基于知识点和基于分类两种方式，试卷组卷支持智能组卷和手动组卷两种方式。试卷添加过程可指定各类题目数量、分数快速形成考试试卷，并支持对当前试卷的预览，包括试卷建议课时、题目数量、分数、难易度、所需工具、涵盖知识点等信息； 16、系统支持考试测评的题库管理功能，支持单选题、多选题、填空题、单机题、仿真题、CTF 题、简答题等多种题型，支持题目的分类功能，支持按照题目难易度、题目类型进行筛选，支持选择题的批量导入功能，支持导入模板的下载，教师可对题目进行创建，可对题目分类、题干、难易度、关联知识点、涉及工具等内容进行修改和查看； 17、硬件设备，可修改设备资产的设备名称、设备类型、设备图标、设备面板、设备描述等信息。可设置设备的串口端口及网络端口的对应端口号，支持网络端口的增、删、改； 18、系统支持仿真资源管理，支持对系统镜像、虚拟设备、物理设备、图形设备的虚拟组件的自动调用； 19、系统支持对虚拟组件的添加、删除和编辑，虚拟设备的创建支持上传和安装两种方式，支持对虚拟设备的信息编辑，包括对包括设备名称、设备类型、设备图标、设备描述等信息的修改； 20、支持在线启动和查看虚拟设备，启动时可动态设置 CPU 数量及内存大小。可快速克隆虚拟设备，并支持增量和完整两种克隆方式，可查看引用该虚拟设备的相关课程。可查看物理设备被占用的相关课程学习小组等详情； 21、系统支持在线学习支持教学、自学两种模式，提供自学模式下的学习周期管理，可对自学的起止时间进行设置，支持自学时间的周期循环设置； 22、系统支持课程表管理功能，课程表以日历表的形式展开，课程表支持以年/月/周的形式进行排课设置，支持查看排课表教学任务详情； 23、系统支持教学任务的下发，教学任务类型包括课程、考试、项目实训，教师可
--	--

陈书 朱明华

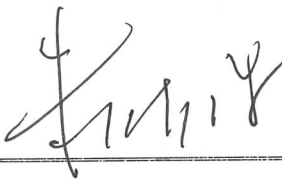
		根据授课方式、任务时长、课时安排、面向对象（学生或班级）进行常规授课和定向授课； 24、系统支持教师对当前课程的个性化设置，支持标准学习和扩展学习两种模式，教师可对实验指导手册、实验视频、拓扑环境等内容进行开启或隐藏； 25、系统支持教学事务管理功能，教学事务包含教师下发的所有课程，可查看每节课的出勤情况、实验报告、上课状态、学习状态等信息，可查看课程学习的详细内容，包括分数、排名等信息，可对学生实验报告进行批阅评分，并支持教学事务日志的导出功能；系统支持数据分析功能，提供对教师教学数据的统计汇总，支持对教学的课时、基础教学成绩、考试测评成绩、项目实训成绩的分析及图形化展示； 26、提供正式出版发行的配套教材 20 套，教材内容需包含：网络安全的攻防体系、TCP/IP 网络体系结构及计算机网络的脆弱性、网络安全实验环境的配置、对称密码技术、基于第 2 层隧道协议的 PPTP VPN 和 L2TP、双宿多宿主机模式防火墙、入侵检测的概念及模型、Windows 和 Linux 系统的安全等相关内容。 27、系统支持学生在线提交实验报告，支持实验报告模板下载，对于已经提交的实验报告支持重复提交； 28、系统支持教师、学生、管理员三种角色，支持对用户头像、姓名、密码等信息进行管理维护，支持账号的批量导入和导出功能，支持账号的单独禁用和批量禁用功能，平台支持查看当时教师、学生在线人数，支持对专业、班级信息的管理和维护，班级需要绑定专业； 29、系统支持知识库功能，可实现一键式查询可通过知识脉络对基础教学内容、项目实训、技能测评等多个方面实现关联，方便老师对平台所有课程知识点进行操作管理； 30、系统提供后台管理功能，支持对平台资源监控，可对内存、硬盘、CPU 使用情况进行图形化展示，支持对平台服务器 IP 地址修改及重启等功能，支持对教学课表的全局设置管理功能，包括上课时间安排、上课时长安排等； 31、系统制造商具备协助学校完善信息安全人才市场需求调研的能力，在未来三年（2026 年-2028 年）每年为学校提供信息安全人才市场需求的专属指导调研报告。 32、可以满足 60 人使用，免费提供现场培训，产品及系统、知识库及相关实验资源提供免费升级。	
3	网络空间安全教学实验资源包	本次投标产品可以满足下列参数： 1、计算机基础与密码学课程资源包：可提供100个实验，300个课时，可提供实验手册等，课程内容包含本课程资源包为用户提供计算机网络、路由交换基础、Linux操作系统及应用、Windows Server系统管理、Python开发技术、Mysql数据库、数据库及系统加固、密码学基础、密码学算法编程、密码学应用等方向的实操课程内容。 2、网络安全课程资源包：可提供150个实验，400个课时，提供实验手册等，本课程资源包为用户提供Web渗透测试平台DVWA、kerberos域安全、入侵检测基础、网络安全技术基础、Web安全综合实战、网络攻防技术、Metasploit漏洞利用、Linux防火墙技术、web中间件漏洞实战、Python安全脚本开发等方向的实操课程内容。 3、可提供正式出版发行的配套教材 20 套，教材内容需包含：网络安全的威胁及风	

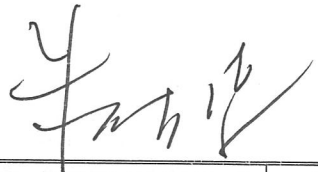
		险分析、实体安全与隔离技术、虚拟专用网 VPN 技术、电子数据取证技术、常用的黑客攻防技术、密码破译与密钥管理、OSI、TCP/IP 及攻防体系结构等相关内容。 4、系统安全课程资源包：可提供 200 个实验，500 个课时，提供实验手册等，本课程资源包为用户提供计算机病毒、Linux 操作系统安全、容灾备份课程、软件安全、二进制漏洞分析与利用、逆向工程技术实战、恶意代码理论与实践、逆向工程技术实战、日志分析基础、KaliLinux、数字取证、移动安全、安卓应用安全、安全评估、信息隐藏与数字水印等方向的实操课程内容。 5、为保障相关实验教学资源包能够与网络空间安全综合实验平台进行联动，产品与网络空间安全综合实验平台为同一厂商。	
4	Web 防火墙虚实结合联动实验设备	1、标准1U机箱，网络吞吐量为800Mbps，应用层处理能力为300Mbps，网络并发连接数40万，HTTP并发为12万，HTTP新建连接数大于3500/s。1TB硬盘，单电源，标准配置千兆6个10/100/1000M自适应电口，2个千兆SFP插槽，2组bypass，1个Console口，2个USB口，可提供软硬件三年维保服务。 2、Web 防火墙具备攻击防护实验功能：支持 CC 攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie 注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等 WEB 攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并阻断经逃逸技术处理的攻击行为。 3、Web防火墙具备IPv6安全实验功能：支持IPv6 的网络环境并能有效运行其安全功能和自身安全功能，能够满足IPv6核心协议、IPv6NDP协议、IPv6 Autoconfig协议、ICMPv6协议和IPy6 PMTU协议的一致性要求，能抵御IPv6、ICMPv6、TCP for IPv6 Server等畸形报文攻击，满足IPv6协议健壮性的要求，并支持IPv6过渡网络环境。 4、访问控制功能：支持基于源/目的IP地址、源/目的端口的访问控制功能，具备WEB应用访问控制功能，支持对HTTP传输内容的关键字、HTTP 请求方式(GET、POST、PUT、HEAD等)、HTTP请求文件类型、HTTP协议头中各字段长度(general-header、request-header、response-header等)、HTTP上传文件类型、HTTP请求频率、HTTP返回的响应内容、HTTPS等进行控制。 5、攻击防护功能：支持CC攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等WEB攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并阻断经逃逸技术处理的攻击行为。 6、日志与告警功能：安全审计日志记录内容包括：事件发生的日期和时间、主体、客体、描述、协议类型、源地址、目标地址、源端口和目标端口等，告警信息包括事件发生的日期和时间、主体、客体、描述、危害级别等，能够对高频发生的相同告警事件进行合并告警，能够按照IP地址、时间段和应用类型条件和以上条件组合对应应用流量进行统计，能够以报表形式输出统计结果。 7、网页防篡改功能：支持Windows、Debian、Ubuntu、CentOS、Redhat、统信、欧拉、麒麟等操作系统防护客户端下载，可自动探测防护端主机名、插件ID、IP地址、操作系统类型、版本号等信息，并可进行防护端配置。 8、代理功能：支持透明代理、反向代理、负载均衡，具备客户端IP还原、数据压	

吴生 Family

		缩、高速缓存、响应URL改写、绑定代理IP等功能，高速缓存支持html、gif、jpg、jpeg、png、bmp、swf、js、CSS等多种文件类型，数据压缩支持text/plain application/x-javascript text/css application/xml等多种MIME类型。 9、运维工具功能：支持Ping、Telnet、Tcpdump、Traceroute等多种运维工具，并可通过点击生成按钮完成一键信息收集。 10、机器学习功能：支持GET、HEAD、POST、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK、PATCH等请求方法的自学习，可生成URL结果，支持资产树形图和URL列表视图展示。 11、流量限速功能：提供TCP并发连接数量、TCP新建连接速率、TCP带宽、UDP带宽、ICMP带宽、HTTP GET 速率、HTTP POST 速率、HTTP其他请求速率、DNS 查询请求速率、并发IP数量阈值设置，处理动作支持阻断、通过和封禁。 12、在联动实验中，为满足学生对漏洞特征库资源的实验需求，设备原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升设备应用层防护能力，2022-2024任意一年向国家漏洞共享平台CNVD提交漏洞数30000个。	
5	Web 防火墙虚实结合实验资源	1、课程资源包部署在实验系统内，Web 防火墙课程资源包包含课程大纲、教学 ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足一个学期的理论和实验教学需求。课程环境基于 Web 防火墙构建，主要介绍 Web 防火墙的基本知识、结构、配置方法。通过本课程能够学习 Web 防火墙环境的部署运维。同时在联动实验中，为满足学生对漏洞特征库资源的实验需求，在联动实验中，为满足学生对漏洞特征库资源的实验需求，产品厂商具备漏洞挖掘能力，近 5 年在国家信息安全漏洞共享平台（CNVD）报送累计 20 万条以上安全漏洞。 2、能够提供设备厂商正式出版的 Web 防火墙相关的网络空间安全重点规划丛书 20 套。	
6	防火墙虚实结合联动实验设备	1、多核 AMP+架构，网络处理能力 4G，并发连接 180 万，每秒新建连接 6 万/秒，1U 机箱，单电源，标准配置 6 个 10/100/1000M 自适应电口，另有 1 个扩展板卡插槽，1 个 Console 口， 64G SSD 硬盘，可提供三年硬件质保及全功能模块升级服务（APP/URL/AV/IPS/IOC）。 2、防火墙具备网络攻击防护的实验功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑IP、Flood攻击防护等功能。 3、策略管理功能：支持冗余策略分析，可进行完全冗余策略分析和部分冗余策略分析，可对分析出的冗余数据单条或批量删除，支持策略命中分析，包含命中数、策略创建时间、首次命中时间、最近命中时间等数据，并可在命中分析界面直接编辑策略，支持安全策略推荐，可针对已配置的安全策略基于目的地址和服务进行分析，可基于分析结果实现源地址精确合并和源地址子网合并后生成安全策略。 4、基础网络功能：支持 IPv4 和 IPv6 双协议栈，具备 DNS、DHCP、MAC、静态路由、策略路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP、IPSec VPN、SSL VPN、GRE VPN、DS-Lite、6in4 隧道、VXLAN、BFD、接口联动、802.1x 认证等功能。 5、WEB 攻击防护功能：支持防扫描、HTTP 异常防护、SQL 注入攻击、跨站脚本攻击、命令执行攻击、代码执行攻击、目录遍历攻击、敏感信息泄露、webshell 防护、HTTP 行为管控、HTTP Flood 攻击防护、WAF 动态防护、Web 浏览病毒页面重新定	

		向、Web 漏洞攻击防护等功能。 6、协同防护功能：支持与其他安全产品联动构建联防联控的网络安全防护体系，包含终端管控类系统联动、威胁监测与分析类系统联动、态势感知与安全运营类平台联动、蜜罐联动等功能。 7、漏洞扫描功能：支持web漏洞扫描、系统漏洞扫描、物联网漏洞扫描、弱口令检查等功能。 8、SSL 解密功能：解密后的数据会进入到高级功能中进行扫描，用以实现加密流量的安全防护， 9、网络攻击防护功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑 IP、Flood 攻击防护等功能。 10、抗拒绝服务攻击功能：能够抵御 ICMPFlood、UDPFlood、SYNFlood、TearDrop、Land 和 Ping of Death 等基本的拒绝服务攻击，渗透成功的包数量小于 5%，正常连接建立大于 90%。 11、流量编排功能：支持将其他硬件设备作为网元对象进行流量编排纳管，具备串联和旁路两种工作模式，并可基于链路健康检查和回环检测对网元健康状态进行检测；支持服务链管理，串接链可定义各网元组之间的逻辑连接关系，包含置顶、之前、之后、末尾四类方向关系，旁路链可直接指定网元组名称；支持引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、源地区、目的地区、服务、应用、VLAN、流量方向等因素将匹配的数据流量引流至服务链处理，并可设置保留或删除 TCP 时间戳、窗口大小、选择确认等参数；支持服务链监控管理，可查看服务链的流量大小和包个数，并可一键勾选服务链 Bypass。 12、蜜罐诱捕功能：支持对接蜜罐产品，基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN 等因素将匹配的数据流量引流至蜜罐设备进行攻击诱捕。 13、网络诊断功能：支持 ping 检测、traceroute 检测、TCP 端口检测、UDP 端口检测等网络诊断检测工具，可基于抓包数量、接口、源地址、源端口、目的地址、目的端口和表达式设置抓包策略。 14、配置管理功能：支持导出最后保存配置、当前配置、历时配置，可将配置文件导出至本地、FTP 服务器、TFTP 服务器，并可配置密文导出，支持导入本地、FTP 服务器、TFTP 服务器的配置文件，并支持三份历史配置文件存储和切换。 15、在联动实验中，为满足学生对漏洞特征库资源的实验需求，要求设备原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升设备应用层防护能力，2022-2024 任意一年向国家漏洞共享平台 CNVD 提交漏洞数 30000 个。	
7	防火墙虚实结合实验资源	1、课程资源包部署在实验系统内，防火墙课程资源包包含课程大纲、教学 ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足高校一个学期的理论和实验教学需求。以防火墙为教学基准，主要介绍行为管理的基本知识、结构、配置方法。通过本课程能够学习防火墙产品的部署运维。 2、能够提供设备厂商正式出版的防火墙相关的网络空间安全重点规划丛书 20 套。	无偏离
8	入侵	1、规格性能：国产化操作系统和国产化 CPU，1U 标准机架式，交流双电源，硬盘	无偏

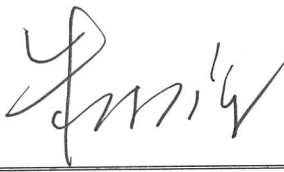
防御 虚实 结合 联动 实验 设备	256G SSD, 2 个 USB 接口, 1 个 RJ45 串口, 1 个 GE 管理口, 10 个千兆电口 (2 对 bypass), 4 个千兆 combo 口, 2 个接口扩展槽; 网络吞吐量 3Gbps, 应用层吞吐量 300Mbps, 最大并发会话数 80 万, 每秒新增会话数 7 万。 2、系统可提供覆盖广泛的攻击特征库, 可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断, 攻击特征库数量为 1 万种以上。 支持敏感数据保护功能, 能够识别、阻断通过自身的敏感数据信息 (身份证号、银行卡、手机号等)。 3、支持基于 SCADA 等工控协议的相关漏洞攻击检测与防护。 4、系统可提供先进的 DoS/DDoS 攻击防护能力, 支持双向阻断 TCP/UDP/ICMP/ACK Flooding, 以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击。 5、支持通过 X-Forwarded-For、X-Real-IP、Cdn-Src-IP 来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务的客户端最原始的 IP 地址, 并可自定义 X-Forwarded-For、X-Real-IP、Cdn-Src-IP 三个字段的识别优先级顺序。 6、系统支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护。 7、支持与沙箱的完美融合形成白环境解决方案, 纵深防御, 覆盖已知威胁与未知威胁检测。 8、流量控制: 支持用户以安全区、IP 地址 (网段)、时间、用户、应用多维度的对流量进行管理和控制, 包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每 IP 的进行应用流量控制 9、智能用户识别: 能够有效识别某 IP 上登录的用户并将用户名关联在该 IP 触发的安全事件上。用户信息来源于: 网站登录用户、数据库用户、远程登录用户、即时通讯用户、文件传输、邮件用户等。 10、可提供正式出版发行的配套教材 20 套, 教材内容需包含: 高级持续性渗透攻击 (APT)、HIPAA 隐私和安全规则、CIA 三元组和其他模型、密码保护 CMOS、实施 ARP 中毒防御、非结构化数据安全等内容。 11、告警功能: 系统可提供服务器异常告警功能, 可以自学习服务器正常工作行为, 并以此为基线检测处服务器非法外联行为。状态监控: 系统能提供 CPU 利用率、内存利用率、会话状态、流量监控、电源状态、电压状态、风扇状态、系统温度状态及接口信息状态等监控信息展示。 12、首页状态分布支持对威胁事件分布、入侵事件-攻击类别分布、入侵事件-攻击类别趋势、TOP 入侵事件、TOP 入侵事件目的 IP、TOP 入侵事件源 IP、TOP 源 IP 地理分布等威胁事件的下钻分析, 点击对应的威胁事件可下钻到对应日志分类查看威胁事件的详细信息。 13、APP 运维管理支持设备云端托管服务, 将设备上确认威胁告警事件风险上报到云端平台, 通过 APP 即时查看告警, 实现 APP 运维管理。 14、厂商获具有国家认可的信息安全服务 (安全开发类二级及以上) 资质证书 15、原厂五年质保服务及五年入侵防御特征库升级服务。	离
9	运维	1、1U 软硬一体设备, 支持用户多角色划分功能, 如系统管理员、部门管理员、运



与风险控制联动系统	维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持自定义用户权限； 2、可提供基于项目的隔离能力，支持自由配置项目内的用户及资产数据，实现灵活的数据权限划分管理。支持平台角色和项目角色划分，平台角色权限可自定义，降低越权风险。可实现同一用户在不同项目内分别承担不同的角色，实现不同项目中权限的灵活分配。 3、支持标准化对接 CAS、JWT、SAML2 单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 4、支持自定义标签，可自定义标签名称及颜色并绑定资产、账号，便于进行分类管理。支持自定义新增资产及账户属性，至少支持字符串、数字、日期、自定义内容的下拉菜单等字段属性。 5、支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。 6、支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。 7、支持按部门组织架构管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；系统支持风险运维审计实时告警，并通过企业微信或钉钉自动下发，提供相应的技术功能呈现证明材料或承诺函；支持与 get、post、soap 发送方式的 http 短信网关平台联动，实现短信动态口令双因素认证机制；支持常用的运维协议；可通过应用发布的方式进行协议扩展，如数据库、浏览器等客户端工具；支持主流数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机； 8、支持对常见数据库及国产数据库的自动改密功能，包括 DB2、oracle、mysql、sqlserver、PG、人大金仓、GBase8a、GBase8s、达梦、HighGo、Redis、GaussDB 数据库等。 9、支持对 Web 应用的自动改密功能，并且支持随堡垒机提供的改密插件录制向导，通过改密插件自动生成 web 应用的改密脚本。 10、支持复杂账号改密流程自定义编排，支持基于用户/用户组，资产/资产账号/资产目录/资产标签/账号标签/动态账号组等等维度的绑定，并支持授权生效时间段，生效 IP 段。 11、支持通过基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。运维报表自动定期发送，支持一键导出符合等级保护、SOX 法案要求的综合分析报告； 12、内置丰富的报表统计模板，内置根据运维人员和组生成各种维度的分析报表。 13、支持动态对象授权，可提供基于属性策略的动态授权能力。支持主机命令集配置，可提供命令解析/正则匹配方式，并提供 5 种日志级别可选，包括提示、低危、中危、高危、非法。 14、运维客户端自带运维工具，可不依赖 xshell/SecureCRT/mstsc 等工具进行运维
-----------	---

张 牛

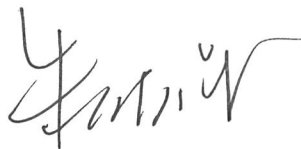
		操作产品厂商具备隐私安全管理系统认证。 15、客户端支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等能力。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之间独立。 16、客户端支持 VPN 登录功能。支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备。 17、具备自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。动作流会按设定好的顺序进行执行，对于常见的运维工作，如升级、巡检等，均可通过此能力快速执行。 18、可提供用户、资产、授权的增删改查等 API 接口，允许校园网任何第三方平台安全调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化配置工作量； 19、支持国密 TLS 单向认证通信，使用国密算法保证 HTTPS 协议层面的数据机密性和完整性；开启后需使用支持国密算法的浏览器才能访问堡垒机。支持采用国密加密算法进行核心敏感数据进行加密存储，且支持使用软件/硬件方式加密，以保证重要数据在系统内存储的机密性。使用硬件进行数据加密时，针对硬件加密组件可提供《商用密码产品认证证书》。 20、产品获得《国家信息安全漏洞库兼容性资质证书》。	
10	恶意代码检测工具	1. 系统界面友好，并有详尽的技术支持文档，所有图形界面要求中文，系统为 B/S 架构，并采用 SSL 加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 2. 支持各类 WEB 编程语言的应用的深度网页后门检测；支持常见的 asp、php、jsp、aspx 等多种 WebShell 的有效扫描；支持实时结果的展现；支持生成统计报表；支持 IIS、Websphere、Weblogic、Apache 等所有的应用服务器；支持 Asp、Jsp、.Net、J2EE、Php、Perl 等所有的 WEB 应用编程语言。 3. 支持实时结果的展现，展现内容应包含扫描对象、类型、描述、特征、危险等级和修改时间；支持一键导出单个或所有恶意代码，并以相应的形式进行展示；支持从界面直接打开文件所在目录；引擎应支持黑白名单编辑功能，可添加相应的黑名单和白名单；引擎应支持 win2003/win2008/win2012/win2016win7/win8/win10 等类型的 win 操作系统；引擎应支持 Redhat/CentOS/suse/ubuntu 等 unix 操作系统； 4. 支持快速扫描功能：支持根据文件类型自动选择内置扫描策略进行扫描，例如当进行扫描 index.ASP 文件时程序会自动选择 ASP 对应的策略进行扫描而忽略其他的扫描策略； 5. 支持全盘扫描功能，支持扫描所有内置的策略以及用户自定义策略；支持自定义扫描功能，支持文件类型、优先级、扫描策略等用户自定义。 6. 硬件支撑：采用安全的 Linux 操作系统，双核或双核以上 CPU，8G 以上内存，1T 硬盘空间；提供用户概述功能，详细展示客户端使用登录、使用情况，上传的文件样本数及人工审核确认数；	无偏离

		7. 支持对系统参数进行配置，包括网络配置及系统安全参数的配置，如登录失败处理功能、最大并发、用户登录超时时间等；可提供接口管理功能，能与其他系统进行对接；提供引擎管理功能，能对引擎进行配置改造；支持对引擎的检测记录进行展示功能；支持对单条检测记录的展示，展示的内容至少包含扫描文件数、威胁数量、扫描 IP、客户端版本号、扫描时间、扫描用时； 8. 支持提供离线检测工具；离线检测工具包含 windows 和 linux 版本；离线检测工具应支持实时生成检测报告；平台可以对恶意代码的特征进行分析和展示。提供多权分立的账户体系，用户能根据其地域对下属单位进行管理； 9. 可提供系统 5 年免费质保及升级服务。	
11	终端安全实验平台	1. 采用 B/S 架构管理端，具备终端分组管理、策略制定下发、统一漏洞修复、统一管控、统一终端准入合规、终端软件管理、资产管理、EDR 威胁追踪、数据防泄漏以及各种报表和查询等功能，支持展示全网终端日志； 2. 客户端支持防卸载，支持设置保护密码，终端退出或卸载时需要输入正确的密码方可执行 3. 支持控制中心防暴力破解，支持采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证，要求令牌 APP 自主研发； 4. 支持控制中心迁移、数据备份、数据恢复；支持邮件报警，支持设定多种触发条件，满足条件后自动发送邮件到相关人；控制中心支持热备部署 5. 支持与 NGFW、上网行为管理、准入产品联动，达到网关边界联动防御效果 6. 支持资产自助登记、自助分组功能，支持硬盘序列号收集、支持 SN 号收集；支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息； 7. 支持自动发现接入网内的终端设备，支持统计全网终端安装率统计，支持插件清理，可清理指定或全部插件 8. 支持 ldap 联动，终端实名认证后自动同步资产信息 9. 可提供多引擎检测能力，包括但不限于云查引擎、人工智能 AI 引擎、启发式引擎。 10. 扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件； 11. 支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理； 12. 支持文件解压缩病毒查杀，支持对 zip、rar、7z 等多种格式的压缩文件查杀能力；支持设置压缩包的扫描层数，压缩包的格式类型，最大扫描压缩包的大小； 13. 具备公有云检测能力，并且公有云特征储备超过 50 亿； 14. 具备自有漏洞补丁管理服务器，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理。 15. 支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况 16. 支持 Windows 10 补丁预热，提高终端下载补丁成功率 17. 补丁通告解读：发布补丁库时会同步发布一篇补丁通告，详述每次发布的补丁的详细情况， 18. 支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再	无偏离

石 牛

	次使用； 19. 支持冗余有线网卡、无线网卡、3G 网卡、MODEM、ADSL、ISDN 等设备的外联控制； 20. 支持禁止终端创建热点，支持设置可信 ssid 白名单，支持设置可信 ssid 与 mac 地址校验功能。 21. 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。 22. 支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMCIA）设置使用权限； 23. 支持能耗管理，支持定时关机策略，支持性能监控 24. 支持管理员对入网的移动存储介质进行注册，支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批； 25. 支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限； 26. 支持移动存储介质读写权限划分设置，有效控制不明来历的移动存储可能带来的病毒传播等隐患 27. 支持针对 Windows XP 系统可带来风险隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 28. 支持针对 Windows 7 系统可带来风险隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 29. 支持移动存储设备、网络共享服务器、本地硬盘特定扩展名或特定目录下的文件访问、修改、删除、移动等行为的审计 30. 支持网络打印操作、本地打印操作、虚拟打印操作审计；支持邮件发送审计；支持终端访问的互联网全日志的审计；支持对应用程序的启动和停止进行记录；支持 USB、蓝牙或红外等终端外设接口接入外设的使用情况审计；支持终端的启动、关闭、待机、休眠、等状态的记录与统计； 31. 支持本机账户或域账户登录日志统计；支持 U 盘操作日志的审计，支持离网使用日志审计。 32. 支持全部拦截和全屏拦截两种模式，开启弹窗防护功能后自动拦截第三方软件的弹窗，使用场景更加灵活。 33. 支持终端用户通过天擎自动抓取非主流第三方软件弹窗规则并上报拦截申请，弹窗防护无死角。 34. 支持管理员通过手动添加或处置终端用户拦截申请来运维本地弹窗规则黑名单，可对非主流第三方软件的弹窗进行拦截。 35. 支持管理员按分组、按时间查看弹窗拦截报表、不同维度的数据统计和拦截日志详情。 36. 支持持续自动化运营弹窗规则，支持定期从云端更新弹窗防护规则库，提高弹窗拦截能力。 37. 支持对终端操作系统之间东西流量访问控制，支持基于数据包流向（任意/流入/流出）、协议（TCP/UDP/ICMP/TCP+UDP）、端口和 IP 的访问控制。 38. 支持对主机防火墙日志集中呈现，支持时间、计算机名、通信 IP、分组、规则	
--	---	--

		名称、协议、命中次数、IP 和端口等日志字段显示。	
12	综合运行硬件平台安全加固平台	1、具备服务器加固应急实验功能，包括：风险点排查、外网暴露面收敛、操作系统加固、文件监控与防护、病毒实时防护、勒索诱饵防护、系统原点和卷影保护、勒索病毒查杀、勒索病毒一键隔离、勒索病毒防护模版、登录控制等功能，支持 Windows、Centos、RHEL、Ubuntu、麒麟、UOS、Debian 等多种操作系统。 2、防勒索功能：具备勒索专项治理功能，可在一个界面查看已处置外网暴露端口数量、未处置外网暴露端口数量、已开启暴力破解防护数量、未开启暴力破解防护数量、已开启远程登录控制数量、未开启远程登录控制数量、弱口令数量、复用口令数量、已处置漏洞数量、未处置漏洞数量、已检出 Webshell 数量、已开启勒索实时防护数量、未开启勒索实时防护数量、已开启勒索诱饵防护数量、未开启勒索诱饵防护数量、已开启内核免疫数量、未开启内核免疫数量、已开启系统还原点和卷影保护数量、未开启系统还原点和卷影保护数量、已开启操作系统加固数量、未开启操作系统加固数量、已开启文件监控与防护数量、未开启文件监控与防护数量、已处置病毒数量、未处置病毒数量、已感染服务器数量、未感染服务器数量，以上功能需在一个界面实现，无需多界面跳转查询。 3、主机发现功能：支持调用多台服务器发起扫描任务，可扫描发起服务器的内网网段、指定网段，扫描方式支持 ARP 缓存方式、Ping 方式、Nmap 方式，并可设置并发扫描最大数量、每秒最大发包数等参数。 4、虚拟补丁功能：虚拟补丁库规则数量 7000 条，可查看每条规则适用的操作系统类型、影响、漏洞编号等信息。 5、流量转发功能：支持基于 VXLAN 和 GRE 的流量转发，可配置流量接受对象 IP 地址、转发端口、转发速率阈值，并可通过 BPF 语法自定义过滤规则采集流量。 6、攻击检测功能：支持报告并记录相应的安全事件，包括：端口扫描、强力攻击、缓冲区溢出攻击、可疑连接攻击，记录的内容包括事件名称、攻击源地址、目的地址、事件发生时间、重要级别等信息。 8、事件记录功能：支持安全事件按照严重程度进行分级，事件等级分为：危急、高危、中危、低危，可对高频度发生的相同安全事件进行合并告警，能够显示包括事件名称、发生次数、源 IP 等信息。 8、报表功能：支持以默认的报告模板生成详尽的检测结果报告并以饼图和折线图等形式对数据区间内的事件类型、发生次数进行了统计，可输出 WORD、HTML 格式的检测结果报告，可修改和定制报告内容，能够定制包括：报告模板、报告格式、服务器范围。 9、在联动实验中，为满足学生对漏洞特征库资源的实验需求，系统厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升软件防护能力，2022-2024 任意一年向国家漏洞共享平台 CNVD 提交漏洞数 30000 个。 10、产品具备云计算产品信息安全认证证书。	无偏离
13	SDN 交换机	1、标准 1RU 盒式设备，吞吐量 880Gbps，整机超低功耗； 2、支持 OpenFlow 1.3.x/1.4.x 版本，支持 3.5K * 流表，支持 L2 到 L4 完整匹配域，支持基于单条流表项的多种行为；支持二层 GRE/NvGRE/VXLAN 隧道；支持 MPLS L2 VPN/MPLS，支持 QinQ；Meter 表项最大支持 1000 * meter ID；支持	

张 牛

		Group(all/select/indirect/fast failover); 支持队列; 支持 Bond;	
14	串口服务器	串口服务器 8 口 RS232/422/485 机架式 220V	
15	网络交换机	1. 性能: 整机交换容量 496Gbps; 转发性能 144Mpps 2. 端口: 48 千兆电+4 千兆 SFP 3. MAC 地址表 16K, IPv4 路由表容量 512, ARP1K 4. 支持 IPv4/IPv6 静态路由, 支持 RIP/RIPng, OSPFV2/V3 5. 交换机支持 9 台物理设备虚拟化技术, 支持完善的堆叠分裂检测机制, 堆叠分裂后能自动完成 MAC 和 IP 地址的重配置, 无需手动干预 6. 实现 ERPS 功能, 能够快速阻断环路, 链路收敛时间 50ms 7. 实现 CPU 保护功能, 能限制非法报文对 CPU 的攻击, 保护交换机在各种环境下稳定工作 8. 支持 RRPP (快速环网保护协议), 环网故障恢复时间不超过 50ms, 支持支持 Smartlink, 支持支持 PVST 功能; 9. 支持 SNMP V1/V2/V3、RMON、SSHV2; 支持端口休眠, 关闭没有应用的端口, 节省能源	
16	综合布线	针对实验室进行信息安全文化场景建设及实验室整体优化改造: 1. 实验室所需优化的网线采用六类网线, 六类水晶头, 网线外护套采用 PVC (聚氯乙烯), 绝缘层采用 PE (聚乙烯), 导体采用优质无氧铜, 内部具有弹性十字骨架分隔线对保证传输性能。相关执行标准按 GB/T 3939.1-2004 进行执行; 2. 实验室所需优化的电源线和插座, 根据实验室电量负载需求, 完成强电室内布线。相关执行标准按 GB/T 28567-2022 进行执行。 3. 实验室所需优化的强、弱电改造采用不锈钢线槽, 全部沿线槽规范布线, 有强电和弱电走同一个不锈钢线槽要求分支电缆采用 RVV6mm2 以上铜缆, 使用金属穿线管敷设。相关执行标准按 GB/T 28567-2022 进行执行。 4、实验室综合布线符合国家《综合布线系统工程设计规范》GB/T 38002.2-2022 标准, 所有实施材料严格按照国家相关产品技术标准, 确保实验室整体网络、电路、通信等综合环境安全运行。 5、可提供在不影响实验室所在楼层教学活动的项目实施, 内容结合实际, 符合学校实验场地现场要求。	无偏离

合同附件 4:

中标单位质保服务承诺

我公司就贵单位组织的项目名称：郑州轻工业大学网络空间安全基础实验平台项目 采购招标编号：豫财磋商采购-2025-1067 招标活动并投标，我们郑重声明如下产品质量保证及售后服务承诺：

我公司保证本次项目提供所有产品均为全新、未使用过的正品，具有一定的先进性和可靠性。我公司提供的服务是 7×24 小时响应服务，对于故障要求 30 分钟内响应，3 小时内赶到现场并处理，如不能及时修复 24 小时内免费提供备用机满足教学正常需要。我公司有一整套完备的售后服务体系，包括严密的组织体系、高素质的人才队伍、完整严谨的服务流程等。依靠这套售后服务体系，我公司完成了众多大型项目的策划、组织、实施、维护和服务。

通过优质的服务，为用户创造价值。完善的售后服务是系统长期稳定运行的保障。良好的售后服务能充分体现现有价值，相对于技术日新月异而言，系统稳定、保值即是增值，所以我们的宗旨是“不断通过服务为用户创造价值”。

“以技术为本，以用户为中心”的服务理念贯穿于我公司的售后服务体系中。在多年的发展过程中，我公司深刻认识到，用户需要前瞻性的战略规划咨询、先进合理的技术方案与高效稳定运行的系统。我们更充分理解只有更注重服务的质量才能全面保障信息系统的稳定运行。因此，通过规范化和高水平的售后服务方式的技术支持，能为用户提供及时满意的服务是我们发展壮大和生存的根本。

我们理解的售后服务是长期持久的，它贯穿系统生命周期的始终：从系统建设之初直至系统消亡所经历的每个阶段、每个环节，都将融入我公司周到的服务，服务是您能够获得最有价值的产品之一。

我公司的售后服务体系以面向用户的客户服务中心、技术支持中心为主体，其他部门配合的一体化的售后服务体系。

客户服务中心负责所有用户的投诉申报、建议和故障请求的接受、记录、跟踪。为保证用户的请求能够及时响应和处理，客户服务专员根据故障处理流程，及时反映和上报相关人员。同时定期或不定期进行主题电话访问，主动发现并解决问题。

为确保技术体系和服务体系有效配合，由我公司首席技术作为技术服务体系的总负责人，负责整个公司的技术发展规划，技术方向、技术产品的总体设计；协调客户服务部、技术、应用中心和商务部，以及所有我公司可以调用的资源为用户提供服务支持；并对用户重大故障的处理和协调。

免费维修时间：我公司针对本项目提供所投产品提供 5 年质保。质保期外所有设备免费保修（只收取材料费），免费上门服务。

售后服务响应方式及响应时间：自接到用户报修后，1 小时内响应，3 小时内到达用户现场并解决

问题，如不能及时解决问题要提供备机服务、直到原设备修复（特殊情况另行商议）。

服务体系：保修期内如产品出现重大问题影响正常使用，我方给予采购人最大限度的技术支持，提供备品、备件或备机等措施。在保修期内，更换在保修范围内零部件时，无须另外支付任何费用，由此发生的费用我公司全权负责，并提供现场服务；保证期外终身提供优质服务，适当收取零配件费用；

技术培训：我公司负责在现场免费为所投项目培训至少 2 名专业讲师，使培训人员达到熟练掌握、灵活运用程度。

售后服务机构信息：维修单位名称：河南尔亨科技有限公司，总部设立在郑州市，并且配备有专业售后服务技术人员。维修单位地址：河南省郑州市高新技术产业开发区银屏路 15 号

售后负责人：程宇锋

联系电话：0371-63288507

我们完全响应贵方的要求，若中标将严格执行投标文件的所有条款，我公司保证服从校方的统筹调度，配合各责任主体职责范围内的工作，在项目过程中，我们将始终信守合，将履行合同条款作为我们的一切行动的中心目标，我公司对本项目承担总包责任，不转包项目，确保项目质量。

合同附件 5:

设备生产厂家服务承诺

奇安信网神信息技术（北京）股份有限公司

售后服务承诺函

本服务政策仅适用于 郑州轻工业大学网络空间安全基础实验平台 项目，
招标编号：豫财磋商采购-2025-1067 中的奇安信网神信息技术（北京）股份
有限公司（以下简称“奇安信网神”）生产的信息安全产品。
秉承专业、及时、高效的服务宗旨，奇安信网神公司做出如下承诺：

1 硬件质保服务

1.1 质保期限

用户新购奇安信网神产品（以下简称“产品”或“设备”），奇安信网神提
供 90 天内保换，5 年硬件质保服务（以购买的硬件质保合同为准）。

1.2 起始日期

产品出厂后三个月开始计算。

注：如果不能得到有效的产品出厂信息，奇安信网神将不提供免费保修服务。

1.3 保换期服务

用户购买奇安信网神硬件产品后 90 天内如发生非人为产品故障，经过奇安
信网神技术支持人员定位为硬件故障，或一年以内主要硬件（主板、硬盘、内存、
CPU、电源）维修三次及以上仍不能正常使用的，则奇安信网神提供免费更换新
硬件产品，新硬件到达用户后，重新提供 90 天的硬件故障免费更换期。随设备
附带的网线，电源线等附件均不在保修范围内。因客户人为因素造成的产品损坏
不在免费更换范围之内。

1.4 保修期服务

1.4.1 设备返修服务

用户购买奇安信网神设备后发生硬件故障或新机购买后超过 90 天后发生硬
件故障的情况下，奇安信网神提供返厂维修服务，最长维修周期不超过 10 个工
作日（若有特殊情况不能保证时间，将提前向用户说明）。

1.4.2 维修备机服务

用户购买奇安信网神产品后发生硬件故障需要返厂维修，若收到货后 10 个
工作日未能维修完毕，奇安信网神可以根据用户的需求，向用户提供同型号或高



型号备机，等到故障机维修完毕后收回备机。

1.4.3 注意事项

- ✧ 如未经奇安信网神95015客服中心报修和奇安信网神技术人员确认而直接寄来的维修产品，不能提供相应硬件维修服务，奇安信网神不对未经报修确认的设备的丢失、损坏承担任何责任。
- ✧ 对于产品硬件质保期内的设备维修，奇安信网神将修复用户设备至故障前的完好的软、硬件状态。
- ✧ 特别提醒：在设备维修前请用户自行做好数据的备份工作，因设备的严重故障而导致用户的配置数据和历史日志无法保留的，奇安信网神不承诺恢复数据配置和历史日志到故障前的状态，并不承担任何因数据丢失而导致的赔偿责任。
- ✧ 若经维修后的硬件产品的剩余硬件质保期不足三个月的，则本次维修的部件从维修结束之日起享受三个月免费保修服务。
- ✧ 超出保修期的设备如需维修，用户需承担设备维修检测费，奇安信网神在收到具体维修配件的费用后方可进行硬件维修。
- ✧ 在保修期内，如发生部件更换，奇安信网神拥有更换后故障部件的所有权。
- ✧ 若产品发生更换，更换后的保修期按照原有设备剩余的保修期继续计算。

1.4.4 免除免费保修义务

属于下列情况的产品（包括部件）出现的故障或损坏，不在免费保修之列：

- ✧ 产品或配件超出质保服务期限的，奇安信网神不再提供超期产品或配件的免费服务。
- ✧ 用户或第三方人员未按照说明书要求，错误安装、保管、使用而造成的产品或配件故障、损坏的；私自对产品进行拆解而造成的产品或配件故障、损坏的，不在奇安信网神免费服务范围内。
- ✧ 因意外因素或人为原因（包括但不限于操作失误、划伤、搬运、磕碰、输入不合适的电压、篡改等）导致的奇安信网神产品或配件故障、损坏的，不在奇安信网神免费服务范围内。
- ✧ 因自然灾害等不可抗力或不可预见的情形（如：雷击、地震、火灾、水灾、战争、黑客攻击、计算机病毒侵入或发作、电脑病毒、通信线路故障等非可归责于奇安信网神的原因等）造成的产品或配件故障、损坏的，以及其他需

要技术支持的，不在奇安信网神免费服务范围内。

2 技术支持服务

2.1 服务内容描述

2.1.1 远程技术支持服务

服务方式	服务时限	服务内容	服务结果
免费热线 远程协助 邮件支持 在线客服	3 年 以购买的产品基础维保合同为准	当用户在使用奇安信网神产品遇到疑问或问题时可以通过远程基础支持服务得到有效的技术支持，快速解决问题	通过电话、远程、邮件等方式解决产品使用过程中遇到的问题

2.1.2 现场技术支持服务

服务方式	服务时限	服务内容	服务结果
现场支持	3 年 以购买的现场服务合同为准	购买过上门服务；远程排查仍然无法解决的，定位是奇安信网神设备本身故障导致时，提供现场支持	现场解决客户问题或定位设备需返厂维修

2.1.3 软件升级服务

服务方式	服务时限	服务内容	服务结果
软件版本升级	3 年 以购买的软件升级服务合同为准	用户与奇安信网神确认版本升级不影响现有客户使用情况下进行系统版本升级	设备升级后将会获得新版本的新增功能或功能优化

2.1.4 特征库更新服务

服务方式	服务时限	服务内容	服务结果
特征库更新	3 年 以购买的特征库更新合同为准	设备可定期自动更新相应的特征库信息	更新特征库后，将会提高设备相应的检测识别能力

2.2 远程技术支持方式

方式	联系方式	支持时间说明
电话支持	95015	7*24 小时
远程技术支持	95015	7*24 小时
投诉与建议	95015	工作时间段（5*8 小时）
Email 支持	kefu@qianxin.com	工作时间段（5*8 小时）

公司名称：奇安信网络安全信息（北京）股份有限公司

日期：2025 年 10 月 9 日

绿盟科技服务承诺函

编号: NSS-HVNNAN4

致: 郑州轻工业大学

我们 北京神州绿盟科技有限公司 是按中华人民共和国法律成立, 主要营业地点设在 北京市海淀区北洼路4号5层501。

我方在中华人民共和国办理贵方 项目名称: 郑州轻工业大学网络空间安全基础实验平台项目, 经销商: 河南尔亨科技有限公司, 招标编号: 豫财磋商采购-2025-1067中, 我方承诺提供原厂服务, 服务内容包括:

- 1、产品服务: 原厂五年质保服务及五年入侵防御特征库升级服务。
- 2、专业安全服务: 无。
- 3、运营服务: 无。
- 4、其他服务: 无。

我方于2025年09月29日签署本文件, 此承诺书有效期至2026-02-26。

供应商: 北京神州绿盟科技有限公司法人: (签字章)日期: 2025年09月29日



售后服务承诺

我们 杭州安恒信息技术股份有限公司 是按 中华人民共和国 法律成立的
一家制造商，主要营业地点设在 浙江省杭州市滨江区西兴街道联慧街 188 号 参加
贵方项目名称：郑州轻工业大学网络空间安全基础实验平台项目，项目编号：豫
财磋商采购-2025-1067 项目招标邀请要求提供的由我方提供如下的技术服务：

1. 保修和维护服务：我方对负责提供的系统承诺五年的免费保修服务和软件升级服务。
2. 售后服务热线：我方保证提供 7*24 的远程技术支持服务，及时响应用户的售后服务需要、及各种技术咨询。
3. 故障响应：在接到用户的故障报修信息后，我方会在 2 小时内给予实质性响应，指派工程师或第三方服务代理商立即协助用户对故障情况进行处理。
4. 在试运行期间，我方会指定有经验的技术人员负责系统的运行和维护，若系统出现问题或故障，免费进行故障处理和软件更新。
5. 在维护期内，我方向用户单位提供 7*24 小时的远程技术支持服务，保证用户单位可以随时找到相应的技术人员。

本服务承诺书有效期至本次招标事宜完成时止，以此为证。

出具服务承诺书的制造商名称：杭州安恒信息技术股份有限公司（盖章）

授权日期：2025 年 09 月 29 日



合同附件 6:

技术规格偏差表

序号	产品名称	磋商文件的技术条款	响应文件的技术条款	偏离说明
1	综合运行硬件平台	1、2U；4个千兆网口，2个万兆网口，2个万兆模块；2颗16核CPU；256内存；8*960GB SSD 硬盘；1*1.92T NVME硬盘；双电源； 2、支持与实训系统环境集成构建虚拟资源池，内置服务接口，为实训系统提供虚拟机资源调度与分配，支持虚拟化安全设备的授权统一维护及管理。 3、支持系统基于虚拟化管理架构和容器管理架构，提供对多平台的kvm、虚拟化和Docker容器进行统一虚拟化管理功能； 4、支持可实现内置包括网络设备、开源安全设备、基础服务器、web服务器、数据库、PC终端、武器库、CMS服务器等虚拟仿真环境，用户可定制虚拟仿真环境。 5、为网络安全实训平台提供计算资源，满足不少于 60 人计算资源并发使用。	1、2U；4个千兆网口，2个万兆网口，2个万兆模块；2颗16核CPU；256内存；8*960GB SSD 硬盘；1*1.92T NVME硬盘；双电源； 2、支持与实训系统环境集成构建虚拟资源池，内置服务接口，为实训系统提供虚拟机资源调度与分配，支持虚拟化安全设备的授权统一维护及管理。 3、支持系统基于虚拟化管理架构和容器管理架构，提供对多平台的kvm、虚拟化和Docker容器进行统一虚拟化管理功能； 4、支持可实现内置包括网络设备、开源安全设备、基础服务器、web服务器、数据库、PC终端、武器库、CMS服务器等虚拟仿真环境，用户可定制虚拟仿真环境。 5、可为网络安全实训平台提供计算资源，满足 60 人计算资源并发使用。	无偏离
2	网络安全综合实验平台	1、系统采用 B/S 架构，提供资源概览，可显示基础教学、题库数量、实训项目、虚拟资源、安全工具的总体数量，支持显示当前平台知识点分布情况、知识点占比情况、基础内容分布情况； 2、系统支持对课程资源的管理功能，课程资源支持以发布状态或未发布状态显示，教师可对所属教学资源进行公开或私有设置，教师只对自己创建课程具有管理和编辑权限，支持教师对课程资源权限移交功能；	1、系统采用 B/S 架构，可提供资源概览，可显示基础教学、题库数量、实训项目、虚拟资源、安全工具的总体数量，支持显示当前平台知识点分布情况、知识点占比情况、基础内容分布情况； 2、系统支持对课程资源的管理功能，课程资源支持以发布状态或未发布状态显示，教师可对所属教学资源进行公开或私有设置，教师只对自己创建课程具有管理和编辑权限，支持教师对课程资源权限移交功能；	无偏离

	3、系统支持对课程内容的新建功能，课程资源类型包括理论、单机、仿真、产品四种类型，新建课程资源可对建议课时、包含知识点进行设置，课程内容需主要包括基本信息、操作手册、实验拓扑、视频、课件、工具资料等内容； 4、系统支持虚拟仿真实验环境，实验环境界面支持显示实验拓扑及配套实验手册、视频讲解和随堂练习等内容，实验拓扑环境支持显示操作机用户名、密码，支持对操作机时间进行延时操作； 5、系统支持自定义网络拓扑功能，创建实验环境支持以拓扑拖拽形式进行组建，提供拓扑图导出功能、居中显示、放大显示、拓扑全屏显示等拓扑查看功能； 6、网络拓扑支持快速复制粘贴功能，以便创建新实验环境下的拓扑的快速复用，支持虚拟资源拓扑可以粘贴到物理资源拓扑，物理资源拓扑只能粘贴到物理资源拓扑； 7、系统支持机架视图功能，机架视图场景化可提高实验操作物理体验，可形象展示设备面板情况以及网络连接情况，机架视图贯穿课程实验、实训项目等实操环节； 8、系统支持支持 WEB 文件上传功能，教师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，在实验环境下支持物理主机桌面中文本复制至 web 虚拟桌面； 9、系统支持虚实结合功能，在不改变用户原有拓扑环境，可将虚拟化设备和真实物理设备同时加入到同一个网络拓扑中进行实验，支持包含防火墙、上网行为管理、入侵防御、漏扫、WAF 等多种安全硬件设备； 10、系统支持老师根据教学需要自定义设置教学方案，教学方案支持对平台现有方案继承，支持教师自己创建全新的教学方案，方案课程可进行先后排序，并支持课程内容以时序图的形式为老师提供参考授课计划，支持自定义调整时序图；	3、系统支持对课程内容的新建功能，课程资源类型包括理论、单机、仿真、产品四种类型，新建课程资源可对建议课时、包含知识点进行设置，课程内容需主要包括基本信息、操作手册、实验拓扑、视频、课件、工具资料等内容； 4、系统支持虚拟仿真实验环境，实验环境界面支持显示实验拓扑及配套实验手册、视频讲解和随堂练习等内容，实验拓扑环境支持显示操作机用户名、密码，支持对操作机时间进行延时操作； 5、系统支持自定义网络拓扑功能，创建实验环境支持以拓扑拖拽形式进行组建，提供拓扑图导出功能、居中显示、放大显示、拓扑全屏显示等拓扑查看功能； 6、网络拓扑支持快速复制粘贴功能，以便创建新实验环境下的拓扑的快速复用，支持虚拟资源拓扑可以粘贴到物理资源拓扑，物理资源拓扑只能粘贴到物理资源拓扑；同时要求产品厂商具备国家标准 GB/T37988-2019《信息安全技术数据安全能力成熟度模型》DSMM 数据安全能力成熟度三级认证，要求提供具有法律效应的证书及颁发机构官方链接查询的有效截图证明材料。 7、系统支持机架视图功能，机架视图场景化可提高实验操作物理体验，可形象展示设备面板情况以及网络连接情况，机架视图贯穿课程实验、实训项目等实操环节； 8、系统支持支持 WEB 文件上传功能，教师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，在实验环境下支持物理主机桌面中文本复制至 web 虚拟桌面； ★9、系统支持虚实结合功能，在不改变用户原有拓扑环境，可将虚拟化设备和真实物理设备同时加入到同一个网络拓扑中进行实验，支持包含防火墙、上网行为管理、入侵防御、漏扫、WAF 等多种安全硬件设备；（需提供该项功能的有效截图
--	--	---

	图证明) 10、系统支持老师根据教学需要自定义设置教学方案，教学方案支持对平台现有方案继承，支持教师自己创建全新的教学方案，方案课程可进行先后排序，并支持课程内容以时序图的形式为老师提供参考授课计划，支持自定义调整时序图； 11、系统支持项目实训功能，支持对用户实际网络架构进行仿真还原，可仿真模拟包括企业网等保测评项目、企业网应急响应项目、企业网安全运维项目的环境及流程； ★12、系统支持对项目实训的基本信息、项目流程、网络拓扑进行设置，项目流程包括项目启动、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，支持对每个阶段的流程环节内容的设计，支持对流程的添加、删除等功能；（需提供该功能的有效截图证明） 13、项目实训过程中默认支持实验的断点保存功能，可自动保存实验内容，并支持对实训过程中对项目网络拓扑的编辑修改，如重新规划网络架构，增加新设备资源，更设备改连接线； 14、系统支持考试测评的试卷管理功能，平台提供试卷模板，试卷模板提供公开、私有属性选项，公开属性下平台的所有教师用户可使用并且编辑，私有属性下试卷模板只能被当前教师所查看。 15、系统支持考试测评的试卷管理功能，平台提供试卷模板，试卷模板提供公开、私有属性选项，公开属性下平台的所有教师用户可使用并且编辑，私有属性下试卷模板只能被当前教师所查看。 16、系统支持对试卷的添加、删除、筛选功能，试卷支持名称、试卷分类等信息进行设置，试卷选题支持基于知识点和基于分类两种方式，试卷组卷支持智能组卷和手动组卷两种方式。试卷添加过程可指定各类题目数量、分数快速形成考试试卷，并支持对当前试卷的预览，包括试卷建议课时、题目数量、分数、难度、所需工具、涵盖知识点等信息； 17、系统支持考试测评的题库管理功能，支持单选题、多选题、填空题、单选题、仿真题、CTF题、简答题等多种题型，支持题目的分类功能，支持按照题目难度、题目类型进行筛选，支持选择题的批量导入功能，支持导入模板的下载，教师可对题目进行创建，可对题目分类、题干、难度、关联知识点、涉及工具等内容进行修改和查看；	11、系统支持项目实训功能，支持对用户实际网络架构进行仿真还原，可仿真模拟包括企业网等保测评项目、企业网应急响应项目、企业网安全运维项目的环境及流程； 12、系统支持对项目实训的基本信息、项目流程、网络拓扑进行设置，项目流程包括项目启动、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，支持对每个阶段的流程环节内容的设计，支持对流程的添加、删除等功能； 13、项目实训过程中默认支持实验的断点保存功能，可自动保存实验内容，并支持对实训过程中对项目网络拓扑的编辑修改，如重新规划网络架构，增加新设备资源，更设备改连接线； 14、系统支持考试测评的试卷管理功能，平台提供试卷模板，试卷模板提供公开、私有属性选项，公开属性下平台的所有教师用户可使用并且编辑，私有属性下试卷模板只能被当前教师所查看。 15、系统支持对试卷的添加、删除、筛选功能，试卷支持名称、试卷分类等信息进行设置，试卷选题支持基于知识点和基于分类两种方式，试卷组卷支持智能组卷和手动组卷两种方式。试卷添加过程可指定各类题目数量、分数快速形成考试试卷，并支持对当前试卷的预览，包括试卷建议课时、题目数量、分数、难度、所需工具、涵盖知识点等信息； 16、系统支持考试测评的题库管理功能，支持单选题、多选题、填空题、单选题、仿真题、CTF题、简答题等多种题型，支持题目的分类功能，支持按照题目难度、题目类型进行筛选，支持选择题的批量导入功能，支持导入模板的下载，教师可对题目进行创建，可对题目分类、题干、难度、关联知识点、涉及工具等内容进行修改和查看；
--	--	--

	题、填空题、单机题、仿真题、CTF题、简答题等多种题型，支持题目的分类功能，支持按照题目难易度、题目类型进行筛选，支持选择题的批量导入功能，支持导入模板的下载，教师可对题目进行创建，可对题目分类、题干、难易度、关联知识点、涉及工具等内容进行修改和查看； 17、硬件设备，可修改设备资产的设备名称、设备类型、设备图标、设备面板、设备描述等信息。可设置设备的串口端口及网络端口的对应端口号，支持网络端口的增、删、改；（需提供该项功能的有效截图证明） 18、系统提供支持仿真资源管理，支持对系统镜像、虚拟设备、物理设备、图形设备的虚拟组件的自动调用； 19、系统支持对虚拟组件的添加、删除和编辑，虚拟设备的创建支持上传和安装两种方式，支持对虚拟设备的信息编辑，包括对包括设备名称、设备类型、设备图标、设备描述等信息的修改； 20、支持在线启动和查看虚拟设备，启动时可动态设置CPU数量及内存大小。可快速克隆虚拟设备，并支持增量和完整两种克隆方式，可查看引用该虚拟设备的相关课程。可查看物理设备被占用的相关课程学习小组等详情； 21、系统支持在线学习支持教学、自学两种模式，提供自学模式下的学习周期管理，可对自学的起止时间进行设置，支持自学时间的周期循环设置； 22、系统支持课程表管理功能，课程表以日历表的形式展开，课程表支持以年/月/周的形式进行排课设置，支持查看排课表教学任务详情； 23、系统支持教学任务的下发，教学任务类型包括课程、考试、项目实训，教师可根据授课方式、任务时长、课时安排、面向对象（学生或班级）进行常规授课和定向授课； 24、系统支持教师对当前课程的个性化设置，支持标准学习和扩展学习两种模式，教师可对实验指导手册、实验视频、拓扑环境等内容进行开启或隐藏； 25、系统支持教学事务管理功能，教学事务包含教师下发的所有课程，可查看每节课的出勤情况、实验报告、上课状态、学习状态等信息，可查看课程学习的详细内容，包括分数、	17、硬件设备，可修改设备资产的设备名称、设备类型、设备图标、设备面板、设备描述等信息。可设置设备的串口端口及网络端口的对应端口号，支持网络端口的增、删、改； 18、系统支持仿真资源管理，支持对系统镜像、虚拟设备、物理设备、图形设备的虚拟组件的自动调用； 19、系统支持对虚拟组件的添加、删除和编辑，虚拟设备的创建支持上传和安装两种方式，支持对虚拟设备的信息编辑，包括对包括设备名称、设备类型、设备图标、设备描述等信息的修改； 20、支持在线启动和查看虚拟设备，启动时可动态设置CPU数量及内存大小。可快速克隆虚拟设备，并支持增量和完整两种克隆方式，可查看引用该虚拟设备的相关课程。可查看物理设备被占用的相关课程学习小组等详情； 21、系统支持在线学习支持教学、自学两种模式，提供自学模式下的学习周期管理，可对自学的起止时间进行设置，支持自学时间的周期循环设置； 22、系统支持课程表管理功能，课程表以日历表的形式展开，课程表支持以年/月/周的形式进行排课设置，支持查看排课表教学任务详情； 23、系统支持教学任务的下发，教学任务类型包括课程、考试、项目实训，教师可根据授课方式、任务时长、课时安排、面向对象（学生或班级）进行常规授课和定向授课； 24、系统支持教师对当前课程的个性化设置，支持标准学习和扩展学习两种模式，教师可对实验指导手册、实验视频、拓扑环境等内容进行开启或隐藏； 25、系统支持教学事务管理功能，教学事务包含教师下发的所有课程，可查看每节课的出勤情况、实验报告、上课状态、学习状态等信息，可查看课程学习的详细内容，包括分数、
--	--	--

	24、系统支持教师对当前课程的个性化设置，支持标准学习和扩展学习两种模式，教师可对实验指导手册、实验视频、拓补环境等内容进行开启或隐藏； 25、系统支持教学事务管理功能，教学事务包含教师下发的所有课程，可查看每节课的出勤情况、实验报告、上课状态、学习状态等信息，可查看课程学习的详细内容，包括分数、排名等信息，可对学生实验报告进行批阅评分，并支持教学事务日志的导出功能；系统支持数据分析功能，提供对教师教学数据的统计汇总，支持对教学的课时、基础教学成绩、考试测评成绩、项目实训成绩的分析及图形化展示； ★26、提供正式出版发行的配套教材 20 套，教材内容需包含：网络安全的攻防体系、TCP/IP 网络体系结构及计算机网络的脆弱性、网络安全实验环境的配置、对称密码技术、基于第 2 层隧道协议的 PPTP VPN 和 L2TP、双宿多宿主主机模式防火墙、入侵检测的概念及模型、Windows 和 Linux 系统的安全等相关内容。 27、系统支持学生在线提交实验报告，支持实验报告模板下载，对于已经提交的实验报告支持重复提交； 28、系统支持教师、学生、管理员三种角色，支持对用户头像、姓名、密码等信息进行管理维护，支持账号的批量导入和导出功能，支持账号的单独禁用和批量禁用功能，平台支持查看当时教师、学生在线人数，支持对专业、班级信息的管理和维护，班级需要绑定专业； 29、系统支持知识库功能，可实现一键式查询可通过知识脉络对基础教学内容、项目实训、技能测评等多个方面实现关联，方便老师对平台所有课程知识点进行操作管理； 30、系统提供后台管理功能，支持对平台资源监控，可对内存、硬盘、CPU 使用情况图形化展示，支持对平台服务器 IP 地址修改及重启等功能，支持对教学课表的全局设置管理功能，包括上课时间安排、上课时长安排等； 31、系统制造商具备协助学校完善信息安全人才市场需求调研的能力，在未来三年（2026 年-2028 年）每年为学校提供信息安全人才市场需求的专属指导调研报告。 32、可以满足 60 人使用，免费提供现场培训，产品及系统、	排名等信息，可对学生实验报告进行批阅评分，并支持教学事务日志的导出功能；系统支持数据分析功能，提供对教师教学数据的统计汇总，支持对教学的课时、基础教学成绩、考试测评成绩、项目实训成绩的分析及图形化展示； 26、提供正式出版发行的配套教材 20 套，教材内容需包含：网络安全的攻防体系、TCP/IP 网络体系结构及计算机网络的脆弱性、网络安全实验环境的配置、对称密码技术、基于第 2 层隧道协议的 PPTP VPN 和 L2TP、双宿多宿主主机模式防火墙、入侵检测的概念及模型、Windows 和 Linux 系统的安全等相关内容。 27、系统支持学生在线提交实验报告，支持实验报告模板下载，对于已经提交的实验报告支持重复提交； 28、系统支持教师、学生、管理员三种角色，支持对用户头像、姓名、密码等信息进行管理维护，支持账号的批量导入和导出功能，支持账号的单独禁用和批量禁用功能，平台支持查看当时教师、学生在线人数，支持对专业、班级信息的管理和维护，班级需要绑定专业； 29、系统支持知识库功能，可实现一键式查询可通过知识脉络对基础教学内容、项目实训、技能测评等多个方面实现关联，方便老师对平台所有课程知识点进行操作管理； 30、系统提供后台管理功能，支持对平台资源监控，可对内存、硬盘、CPU 使用情况图形化展示，支持对平台服务器 IP 地址修改及重启等功能，支持对教学课表的全局设置管理功能，包括上课时间安排、上课时长安排等； 31、系统制造商具备协助学校完善信息安全人才市场需求调研的能力，在未来三年（2026 年-2028 年）每年为学校提供信息安全人才市场需求的专属指导调研报告。 32、可以满足 60 人使用，免费提供现场培训，产品及系统、
--	---	--

		IP地址修改及重启等功能，支持对教学课表的全局设置管理功能，包括上课时间安排、上课时长安排等； 31、系统制造商具备协助学校完善信息安全人才市场需求调研的能力，在未来三年（2026年-2028年）每年为学校提供信息安全人才市场需求的专属指导调研报告。（提供厂商参与的近5年来任意三年网络安全人才需求调研报告证明文件） 32、须满足60人使用，免费提供现场培训，产品及系统、知识库及相关实验资源提供免费升级。	知识库及相关实验资源提供免费升级。
3	网络安全教学实验资源包	1、计算机基础与密码学课程资源包：提供不少于100个实验，300个课时，提供实验手册等，课程内容包括本课程资源包为用户提供计算机网络、路由交换基础、Linux操作系统及应用、Windows Server系统管理、Python开发技术、Mysql数据库、数据库及系统加固、密码学基础、密码学算法编程、密码学应用等方向的实操课程内容。 2、网络安全课程资源包：提供不少于150个实验，400个课时，提供实验手册等，本课程资源包为用户提供Web渗透测试平台DVWA、kerberos域安全、入侵检测基础、网络安全技术基础、Web安全综合实战、网络攻防技术、Metasploit漏洞利用、Linux防火墙技术、web中间件漏洞实战、Python安全脚本开发等方向的实操课程内容。 ★3、提供正式出版发行的配套教材20套，教材内容需包含：网络安全的威胁及风险分析、实体安全与隔离技术、虚拟专用网VPN技术、电子数据取证技术、常用的黑客攻防技术、密码破译与密钥管理、OSI、TCP/IP及攻防体系结构等相关内容。提供相关教材的封面截图及教材相关内容截图。 4、系统安全课程资源包：提供不少于200个实验，500个课时，提供实验手册等，本课程资源包为用户提供计算机病毒、Linux操作系统安全、容灾备份课程、软件安全、二进制漏洞	本次投标产品可以满足下列参数： 1、计算机基础与密码学课程资源包：可提供100个实验，300个课时，可提供实验手册等，课程内容包括本课程资源包为用户提供计算机网络、路由交换基础、Linux操作系统及应用、Windows Server系统管理、Python开发技术、Mysql数据库、数据库及系统加固、密码学基础、密码学算法编程、密码学应用等方向的实操课程内容。 2、网络安全课程资源包：可提供150个实验，400个课时，提供实验手册等，本课程资源包为用户提供Web渗透测试平台DVWA、kerberos域安全、入侵检测基础、网络安全技术基础、Web安全综合实战、网络攻防技术、Metasploit漏洞利用、Linux防火墙技术、web中间件漏洞实战、Python安全脚本开发等方向的实操课程内容。 3、可提供正式出版发行的配套教材20套，教材内容需包含：网络安全的威胁及风险分析、实体安全与隔离技术、虚拟专用网VPN技术、电子数据取证技术、常用的黑客攻防技术、密码破译与密钥管理、OSI、TCP/IP及攻防体系结构等相关内容。 4、系统安全课程资源包：可提供200个实验，500个课时，提供实验手册等，本课程资源包为用户提供计算机病毒、

		分析与利用、逆向工程技术实战、恶意代码理论与实践、逆向工程技术实战、日志分析基础、KaliLinux、数字取证、移动安全、安卓应用安全、安全评估、信息隐藏与数字水印等方向的实操课程内容。	Linux 操作系统安全、容灾备份课程、软件安全、二进制漏洞分析与利用、逆向工程技术实战、恶意代码理论与实践、逆向工程技术实战、日志分析基础、KaliLinux、数字取证、移动安全、安卓应用安全、安全评估、信息隐藏与数字水印等方向的实操课程内容。
Web 防火墙虚实结合联动实验设备	4	5、为保障相关实验教学资源包能够与网络空间安全综合实验平台进行联动，产品需与网络空间安全综合实验平台为同一厂商提供联动承诺函。 1、标准1U机箱，网络吞吐量为800Mbps，应用层处理能力为300Mbps，网络并发连接数40万，HTTP并发为12万，HTTP新建连接数大于3500/s。1TB硬盘，单电源，标准配置千兆6个10/100/1000M自适应电口，2个千兆SFP插槽，2组bypass，1个Console口，2个USB口，提供软硬件三年维保服务。 2、Web 防火墙具备攻击防护实验功能：支持 CC 攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie 注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等 WEB 攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并阻断经逃逸技术处理的攻击行为，提供第三方检测机构出具检验报告关键页证明。 ★3、Web防火墙具备IPv6安全实验功能：支持IPv6 的网络环境并能有效运行其安全功能和自身安全功能，能够满足IPv6核心协议、IPv6NDP协议、IPv6 Autoconfig协议、ICMPv6和IPy6 PMTU协议的一致性要求，能抵御IPv6、ICMPv6、TCP for IPv6 Server等畸形报文攻击，满足IPv6协议健壮性的要求，并支持IPv6过渡网络环境，提供第三方检测机构出具检验报告关键页证明。 4、访问控制功能：支持基于源/目的IP地址、源/目的端口的	5、为保障相关实验教学资源包能够与网络空间安全综合实验平台进行联动，产品与网络空间安全综合实验平台为同一厂商。 1、标准1U机箱，网络吞吐量为800Mbps，应用层处理能力为300Mbps，网络并发连接数40万，HTTP并发为12万，HTTP新建连接数大于3500/s。1TB硬盘，单电源，标准配置千兆6个10/100/1000M自适应电口，2个千兆SFP插槽，2组bypass，1个Console口，2个USB口，可提供软硬件三年维保服务。 2、Web 防火墙具备攻击防护实验功能：支持 CC 攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie 注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等 WEB 攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并阻断经逃逸技术处理的攻击行为。 3、Web防火墙具备IPv6安全实验功能：支持IPv6 的网络环境并能有效运行其安全功能和自身安全功能，能够满足IPv6核心协议、IPv6NDP协议、IPv6 Autoconfig协议、ICMPv6协议和IPy6 PMTU协议的一致性要求，能抵御IPv6、ICMPv6、TCP for IPv6 Server等畸形报文攻击，满足IPv6协议健壮性的要求，并支持IPv6过渡网络环境。 4、访问控制功能：支持基于源/目的IP地址、源/目的端口的访问控制功能，具备WEB应用访问控制功能，支持对HTTP传输内容的关键字、HTTP 请求方式(GET、POST、PUT、HEAD等)、

	访问控制功能，具备WEB应用访问控制功能，支持对HTTP传输内容的关键字、HTTP 请求方式 (GET、POST、PUT、HEAD等)、HTTP请求文件类型、HTTP协议头中各字段长度 (general-header、request-header、response-header等)、HTTP上传文件类型、HTTP请求频率、HTTP返回的响应内容、HTTPS等进行控制。 5、攻击防护功能：支持CC攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等WEB攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并阻断经逃逸技术处理的攻击行为，提供第三方检测机构出具的检验报告关键页证明。 6、日志与告警功能：安全审计日志记录内容包括：事件发生的日期和时间、主体、客体、描述、协议类型、源地址、目标地址、源端口和目标端口等，告警信息包括事件发生的日期和时间、主体、客体、描述、危害级别等，能够对高频发生的相同告警事件进行合并告警，能够按照IP地址、时间段和应用类型条件和以上条件组合对应用流量进行统计，能够以报表形式输出统计结果。 7、网页防篡改功能：支持Windows、Debian、Ubuntu、CentOS、Redhat、统信、欧拉、麒麟等操作系统防护客户端下载，可自动探测防护主机名、插件ID、IP地址、操作系统类型、版本号等信息，并可进行防护端配置。 8、代理功能：支持透明代理、反向代理、负载均衡，具备客户端IP还原、数据压缩、高速缓存、响应URL改写、绑定代理IP等功能，高速缓存支持html、gif、jpg、jpeg、png、bmp、swf、js、CSS等多种文件类型，数据压缩支持text/plain application/x-javascript text/css application/xml等多种MIME类型。 9、运维工具功能：支持Ping、Telnet、Tcpdump、Traceroute	HTTP请求文件类型、HTTP协议头中各字段长度 (general-header、request-header、response-header等)、HTTP上传文件类型、HTTP请求频率、HTTP返回的响应内容、HTTPS等进行控制。 5、攻击防护功能：支持CC攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等WEB攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并阻断经逃逸技术处理的攻击行为。 6、日志与告警功能：安全审计日志记录内容包括：事件发生的日期和时间、主体、客体、描述、协议类型、源地址、目标地址、源端口和目标端口等，告警信息包括事件发生的日期和时间、主体、客体、描述、危害级别等，能够对高频发生的相同告警事件进行合并告警，能够按照IP地址、时间段和应用类型条件和以上条件组合对应用流量进行统计，能够以报表形式输出统计结果。 7、网页防篡改功能：支持Windows、Debian、Ubuntu、CentOS、Redhat、统信、欧拉、麒麟等操作系统防护客户端下载，可自动探测防护主机名、插件ID、IP地址、操作系统类型、版本号等信息，并可进行防护端配置。 8、代理功能：支持透明代理、反向代理、负载均衡，具备客户端IP还原、数据压缩、高速缓存、响应URL改写、绑定代理IP等功能，高速缓存支持html、gif、jpg、jpeg、png、bmp、swf、js、CSS等多种文件类型，数据压缩支持text/plain application/x-javascript text/css application/xml等多种MIME类型。 9、运维工具功能：支持Ping、Telnet、Tcpdump、Traceroute
--	---	---

	swf、js、CSS等多种文件类型，数据压缩支持text/plain application/x-javascript text/css application/xml等多种MIME类型。 9、运维工具功能：支持Ping、Telnet、Tcpdump、Traceroute等多种运维工具，并可通过点击生成按钮完成一键信息收集，提供上述功能截图。 10、机器学习功能：支持GET、HEAD、POST、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK、PATCH等请求方法的自学习，可生成URL结果，支持资产树形图和URL列表视图展示， 11、流量限速功能：提供TCP并发连接数量、TCP新建连接速率、TCP带宽、UDP带宽、ICMP带宽、HTTP GET 速率、HTTP POST 速率、HTTP其他请求速率、DNS 查询请求速率、并发IP数量阈值设置，处理动作支持阻断、通过和封禁，提供上述功能有效截图证明。 12、在联动实验中，为满足学生对漏洞特征库资源的实验需求，要求设备原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升设备应用层防护能力，2022-2024任意一年向国家漏洞共享平台CNVD提交漏洞数≥30000个，提供CNVD出具的提交证明。	等多种运维工具，并可通过点击生成按钮完成一键信息收集。 10、机器学习功能：支持GET、HEAD、POST、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK、PATCH等请求方法的自学习，可生成URL结果，支持资产树形图和URL列表视图展示。 11、流量限速功能：提供TCP并发连接数量、TCP新建连接速率、TCP带宽、UDP带宽、ICMP带宽、HTTP GET 速率、HTTP POST 速率、HTTP其他请求速率、DNS 查询请求速率、并发IP数量阈值设置，处理动作支持阻断、通过和封禁。 12、在联动实验中，为满足学生对漏洞特征库资源的实验需求，设备原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升设备应用层防护能力，2022-2024任意一年向国家漏洞共享平台CNVD提交漏洞数30000个。	
5	Web 防火墙虚实结合实验资源	1、课程资源包部署在实验系统内，Web 防火墙课程资源包包含课程大纲、教学 ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足一个学期的理论和实验教学需求。课程环境基于 Web 防火墙构建，主要介绍 Web 防火墙的基本知识、结构、配置方法。通过本课程能够学习 Web 防火墙环境的部署运维。同时在联动实验中，为满足学生对漏洞特征库资源的实验需求，在联动实验中，为满足学生对漏洞特征库资源的实验需求，要求产品厂商具备漏洞挖掘能力，近 5 年在国家信息安全	无偏离

		漏洞共享平台（CNVD）报送累计 20 万条以上安全漏洞，要求提供相关漏洞报送证明材料。 ★2、要求能够提供设备厂商正式出版的 Web 防火墙相关的网络安全空间安全重点规划丛书 20 套，提供相关 ISBN 书号证明和购买链接地址。	共享平台（CNVD）报送累计 20 万条以上安全漏洞。 2、能够提供设备厂商正式出版的 Web 防火墙相关的网络安全空间安全重点规划丛书 20 套。
6	防火墙 虚实结合 联合实验 设备	1、多核 AMP+架构，网络处理能力 4G，并发连接 ≥180 万，每秒新建连接 6 万/秒，1U 机箱，单电源，标准配置 6 个 10/100/1000M 自适应电口，另有 1 个扩展板卡插槽，1 个 Console 口，64G SSD 硬盘，提供三年硬件质保及全功能模块升级服务（APP/URL/AV/IPS/TOC）。 ★2、防火墙需具备网络攻击防护的实验功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑 IP、Flood 攻击防护等功能，提供第三方检测机构出具的检验报告关键页证明。 3、策略管理功能：支持冗余策略分析，可进行完全冗余策略分析和部分冗余策略分析，可对分析出的冗余数据单条或批量删除，支持策略命中分析，包含命中数、策略创建时间、首次命中时间、最近命中时间等数据，并可在命中分析界面直接编辑策略，支持安全策略推荐，可针对已配置的安全策略基于目的地址和服务进行分析，可基于分析结果实现源地址精确合并和源地址子网合并后生成安全策略，提供上述功能有效截图证明。 4、基础网络功能：支持 IPv4 和 IPv6 双协议栈，具备 DNS、DHCP、MAC、静态路由、策略路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP、IPSec VPN、SSL VPN、GRE VPN、DS-Lite、6in4 隧道、VXLAN、BFD、接口联动、802.1x 认证等功能。 5、WEB 攻击防护功能：支持防扫描、HTTP 异常防护、SQL 注入攻击、跨站脚本攻击、命令执行攻击、代码执行攻击、目录遍历攻击、敏感信息泄露、webshell 防护、HTTP 行为管控、HTTP Flood 攻击防护、WAF 动态防护、Web 浏览病毒页面重	1、多核 AMP+架构，网络处理能力 4G，并发连接 180 万，每秒新建连接 6 万/秒，1U 机箱，单电源，标准配置 6 个 10/100/1000M 自适应电口，另有 1 个扩展板卡插槽，1 个 Console 口，64G SSD 硬盘，可提供三年硬件质保及全功能模块升级服务（APP/URL/AV/IPS/IOC）。 2、防火墙具备网络攻击防护的实验功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑 IP、Flood 攻击防护等功能。 3、策略管理功能：支持冗余策略分析，可进行完全冗余策略分析和部分冗余策略分析，可对分析出的冗余数据单条或批量删除，支持策略命中分析，包含命中数、策略创建时间、首次命中时间、最近命中时间等数据，并可在命中分析界面直接编辑策略，支持安全策略推荐，可针对已配置的安全策略基于目的地址和服务进行分析，可基于分析结果实现源地址精确合并和源地址子网合并后生成安全策略。 4、基础网络功能：支持 IPv4 和 IPv6 双协议栈，具备 DNS、DHCP、MAC、静态路由、策略路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP、IPSec VPN、SSL VPN、GRE VPN、DS-Lite、6in4 隧道、VXLAN、BFD、接口联动、802.1x 认证等功能。 5、WEB 攻击防护功能：支持防扫描、HTTP 异常防护、SQL 注入攻击、跨站脚本攻击、命令执行攻击、代码执行攻击、目录遍历攻击、敏感信息泄露、webshell 防护、HTTP 行为管控、HTTP Flood 攻击防护、WAF 动态防护、Web 浏览病毒页面重

	遍历攻击、敏感信息泄露、webshell 防护、HTTP 行为管控、HTTP Flood 攻击防护、WAF 动态防护、Web 浏览病毒页面重定向、Web 漏洞攻击防护等功能 6、协同防护功能：支持与其他安全产品联动构建联防联控的网络安全防护体系，包含终端管控类系统联动、威胁监测与分析类系统联动、态势感知与安全运营类平台联动、蜜罐联动等功能，提供第三方检测机构出具的检验报告关键页证明。 7、漏洞扫描功能：支持web漏洞扫描、系统漏洞扫描、物联网漏洞扫描、弱口令检查等功能，提供第三方检测机构出具的检验报告关键页证明。 8、SSL 解密功能：解密后的数据会进入到高级功能中进行扫描，用以实现加密流量的安全防护， 9、网络攻击防护功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑 IP、Flood 攻击防护等功能。 10、抗拒绝服务攻击功能：能够抵御 ICMPFlood、UDPFlood、SYNFlood、TearDrop、Land 和 Ping of Death 等基本的拒绝服务攻击，渗透成功的包数量小于 5%，正常连接建立大于 90%，流量编排功能：支持将其他硬件设备作为网元对象进行流量检查和回环检测对网元健康状态进行检测；支持服务链管理，串联链可定义各网元组之间的逻辑连接关系，包含置项、之前、之后、末尾四类方向关系，旁路链可直接指定网元组名称；支持引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、源地区、目的地区、服务、应用、VLAN、流量方向等因素将匹配的数据流量引流至服务链处理，并可设置保留或删除 TCP 时间戳、窗口大小、选择确认等参数；支持服务链监控管理，可查看服务链的流量大小和包个数，并可一键勾选服务链 Bypass。 12、蜜罐诱捕功能：支持对接蜜罐产品，基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN 等因素将	新定向、Web 漏洞攻击防护等功能。 6、协同防护功能：支持与其他安全产品联动构建联防联控的网络安全防护体系，包含终端管控类系统联动、威胁监测与分析类系统联动、态势感知与安全运营类平台联动、蜜罐联动等功能。 7、漏洞扫描功能：支持web漏洞扫描、系统漏洞扫描、物联网漏洞扫描、弱口令检查等功能。 8、SSL 解密功能：解密后的数据会进入到高级功能中进行扫描，用以实现加密流量的安全防护， 9、网络攻击防护功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑 IP、Flood 攻击防护等功能。 10、抗拒绝服务攻击功能：能够抵御 ICMPFlood、UDPFlood、SYNFlood、TearDrop、Land 和 Ping of Death 等基本的拒绝服务攻击，渗透成功的包数量小于 5%，正常连接建立大于 90%。 11、流量编排功能：支持将其他硬件设备作为网元对象进行流量编排纳管，具备串联和旁路两种工作模式，并可基于链路健康检查和回环检测对网元健康状态进行检测；支持服务链管理，串联链可定义各网元组之间的逻辑连接关系，包含置项、之前、之后、末尾四类方向关系，旁路链可直接指定网元组名称；支持引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、源地区、目的地区、服务、应用、VLAN、流量方向等因素将匹配的数据流量引流至服务链处理，并可设置保留或删除 TCP 时间戳、窗口大小、选择确认等参数；支持服务链监控管理，可查看服务链的流量大小和包个数，并可一键勾选服务链 Bypass。 12、蜜罐诱捕功能：支持对接蜜罐产品，基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN 等因素将
--	---	---

	服务链监控管理，可查看服务链的流量大小和包个数，并可一键勾选服务链 Bypass。 12、蜜罐诱捕功能：支持对接蜜罐产品，基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN 等因素将匹配的数据流量引流至蜜罐设备进行攻击诱捕，提供上述功能的有效截图证明。 13、网络诊断功能：支持 ping 检测、traceroute 检测、TCP 端口检测、UDP 端口检测等网络诊断检测工具，可基于抓包数量、接口、源地址、源端口、目的地址、目的端口和表达式设置抓包策略，提供上述功能的有效截图证明。 14、配置管理功能：支持导出最后保存配置、当前配置、历史配置，可将配置文件导出至本地、FTP 服务器、TFTP 服务器，并可配置密文导出，支持导入本地、FTP 服务器、TFTP 服务器的配置文件，并支持三份历史配置文件存储和切换，提供上述功能的有效截图证明。 15、在联动实验中，为满足学生对漏洞特征库资源的实验需求，要求设备原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升设备应用层防护能力，2022-2024 任意一年向国家漏洞共享平台 CNVD 提交漏洞数≥30000 个，提供 CNVD 出具的提交证明。	匹配的数据流量引流至蜜罐设备进行攻击诱捕。 13、网络诊断功能：支持 ping 检测、traceroute 检测、TCP 端口检测、UDP 端口检测等网络诊断检测工具，可基于抓包数量、接口、源地址、源端口、目的地址、目的端口和表达式设置抓包策略。 14、配置管理功能：支持导出最后保存配置、当前配置、历史配置，可将配置文件导出至本地、FTP 服务器、TFTP 服务器，并可配置密文导出，支持导入本地、FTP 服务器、TFTP 服务器的配置文件，并支持三份历史配置文件存储和切换。 15、在联动实验中，为满足学生对漏洞特征库资源的实验需求，要求设备原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升设备应用层防护能力，2022-2024 任意一年向国家漏洞共享平台 CNVD 提交漏洞数 30000 个。	
7	防火墙虚实结合实验资源	1、课程资源包部署在实验系统内，防火墙课程资源包包含课程大纲、教学 ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足高校一个学期的理论和实验教学需求。以防火墙为教学基准，主要介绍行为管理的基本知识、结构、配置方法。通过本课程能够学习防火墙产品的部署运维。 ★2、要求能够提供设备厂商正式出版的防火墙相关的网络空间安全重点规划丛书 20 套，提供相关 ISBN 书号证明和购买链接地址。	无偏离

8	入侵防御 虚拟实验 结合实验 设备	1、规格性能：国产化操作系统和国产化 CPU，1U 标准机架式，交流双电源，硬盘 ≥256G SSD，2 个 USB 接口，1 个 RJ45 串口，1 个 GE 管理口，≥10 个千兆电口（2 对 bypass），≥4 个千兆 combo 口，≥2 个接口扩展槽；网络吞吐量 ≥3Gbps，应用层吞吐量 ≥300Mbps，最大并发会话数 ≥80 万，每秒新增会话数 ≥7 万。 2、系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量为 1 万种以上，要求提供攻击特征库数量的有效截图证明。 支持敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等）。 3、支持基于 SCADA 等工控协议的相关漏洞攻击检测与防护，要求提供有效功能截图证明，要求提供第三方测评机构出具的检测报告关键页证明。 4、系统应提供先进的 DoS/DDoS 攻击防护能力，支持双向阻断 TCP/UDP/ICMP/ACK Flooding，以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击。 5、支持通过 X-Forwarded-For、X-Real-IP、Cdn-Source-IP 来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务的客户端最原始的 IP 地址，并可自定义 X-Forwarded-For、X-Real-IP、Cdn-Source-IP 三个字段的识别优先级顺序，要求提供功能的有效截图证明。 6、系统支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护。 ★7、支持与沙箱的完美融合形成白环境解决方案，纵深防御，覆盖已知威胁与未知威胁检测，要求提供功能有效截图证明，要求提供第三方测评机构出具的检测报告关键页证明。	1、规格性能：国产化操作系统和国产化 CPU，1U 标准机架式，交流双电源，硬盘 256G SSD，2 个 USB 接口，1 个 RJ45 串口，1 个 GE 管理口，10 个千兆电口（2 对 bypass），4 个千兆 combo 口，2 个接口扩展槽；网络吞吐量 3Gbps，应用层吞吐量 300Mbps，最大并发会话数 80 万，每秒新增会话数 7 万。 2、系统可提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量为 1 万种以上。 支持敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等）。 3、支持基于 SCADA 等工控协议的相关漏洞攻击检测与防护。 4、系统可提供先进的 DoS/DDoS 攻击防护能力，支持双向阻断 TCP/UDP/ICMP/ACK Flooding，以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击。 5、支持通过 X-Forwarded-For、X-Real-IP、Cdn-Source-IP 来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务的客户端最原始的 IP 地址，并可自定义 X-Forwarded-For、X-Real-IP、Cdn-Source-IP 三个字段的识别优先级顺序。 6、系统支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护。 7、支持与沙箱的完美融合形成白环境解决方案，纵深防御，覆盖已知威胁与未知威胁检测。 8、流量控制：支持用户以安全区、IP 地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每 IP 的进行应用流量控制 9、智能用户识别：能够有效识别某 IP 上登录的用户并将用户名关联在该 IP 触发的安全事件上。用户信息来源于：网站	无偏 离
---	----------------------------	--	--	---------

	8、流量控制：支持用户以安全区、IP地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每IP的进行应用流量控制 9、智能用户识别：能够有效识别某IP上登录的用户并将用户名关联在该IP触发的安全事件上。用户信息来源于：网站登录用户、数据库用户、远程登录用户、即时通讯用户、文件传输、邮件用户等。 ★10、提供正式出版发行的配套教材20套，教材内容需包含：高级持续性渗透攻击（APT）、HIPAA隐私和安全规则、CIA三元组和其他模型、密码保护CMOS、实施ARP中毒防御、非结构化数据安全等内容，提供相关教材的封面截图及教材相关内容截图。 11、告警功能：系统应提供服务器异常告警功能，可以自主学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。状态监控：系统能提供CPU利用率、内存利用率、会话状态、流量监控、电源状态、电压状态、风扇状态、系统温度状态及接口信息状态等监控信息展示。 12、首页状态分布支持对威胁事件分布、入侵事件-攻击类别分布、入侵事件-攻击类别趋势、TOP入侵事件、TOP入侵事件目的IP、TOP入侵事件源IP、TOP源IP地理分布等威胁事件的下钻分析，点击对应的威胁事件可下钻到对应日志分类查看威胁事件的详细信息。 13、APP运维管理支持设备云端托管服务，将设备上确认威胁告警事件风险上报到云端平台，通过APP即时查看告警，实现APP运维管理。 14、厂商获具有国家认可的信息安全服务（安全开发类二级及以上）资质证书 15、原厂五年质保服务及五年入侵防御特征库升级服务。	登录用户、数据库用户、远程登录用户、即时通讯用户、文件传输、邮件用户等。 10、可提供正式出版发行的配套教材20套，教材内容需包含：高级持续性渗透攻击（APT）、HIPAA隐私和安全规则、CIA三元组和其他模型、密码保护CMOS、实施ARP中毒防御、非结构化数据安全等内容。 11、告警功能：系统可提供服务器异常告警功能，可以自主学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。状态监控：系统能提供CPU利用率、内存利用率、会话状态、流量监控、电源状态、电压状态、风扇状态、系统温度状态及接口信息状态等监控信息展示。 12、首页状态分布支持对威胁事件分布、入侵事件-攻击类别分布、入侵事件-攻击类别趋势、TOP入侵事件、TOP入侵事件目的IP、TOP入侵事件源IP、TOP源IP地理分布等威胁事件的下钻分析，点击对应的威胁事件可下钻到对应日志分类查看威胁事件的详细信息。 13、APP运维管理支持设备云端托管服务，将设备上确认威胁告警事件风险上报到云端平台，通过APP即时查看告警，实现APP运维管理。 14、厂商获具有国家认可的信息安全服务（安全开发类二级及以上）资质证书 15、原厂五年质保服务及五年入侵防御特征库升级服务。
--	--	--

		15、提供原厂三年质保服务及三年入侵防御特征库升级服务。	
9	运维与风险控制联动系统	1、1U 软硬一体设备，支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持自定义用户权限； 2、提供基于项目的隔离能力，支持自由配置项目内的用户及资产数据，实现灵活的数据权限划分管理。支持平台角色和项目角色划分，平台角色权限可自定义，降低越权风险。可实现同一用户在不同项目内分别承担不同的角色，实现不同项目中权限的灵活分配。（需提供相关功能有效截图证明） 3、支持标准化对接 CAS、JWT、SAML2 单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 4、支持自定义标签，可自定义标签名称及颜色并绑定资产、账号，便于进行分类管理。支持自定义新增资产及账户属性，至少支持字符串、数字、日期、自定义内容的下拉菜单等字段属性。 5、支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。（需提供相关功能有效截图证明） ★6、支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。（提供相关有效功能截图证明） 7、支持按部门组织架构管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；系统支持风险运维审计实时告警，并通过企业微信或钉钉自动下发，提供相应的技术功能呈现证明材料或承诺函；支持与 get、post、soap 发送方式的 http 短信网关平台联动，实现短信动态口令双因素认证机制；支持短信网关平台联动，实现短信动态口令双因素认证机制；支持	1、1U 软硬一体设备，支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持自定义用户权限； 2、可提供基于项目的隔离能力，支持自由配置项目内的用户及资产数据，实现灵活的数据权限划分管理。支持平台角色和项目角色划分，平台角色权限可自定义，降低越权风险。可实现同一用户在不同项目内分别承担不同的角色，实现不同项目中权限的灵活分配。 3、支持标准化对接 CAS、JWT、SAML2 单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 4、支持自定义标签，可自定义标签名称及颜色并绑定资产、账号，便于进行分类管理。支持自定义新增资产及账户属性，至少支持字符串、数字、日期、自定义内容的下拉菜单等字段属性。 5、支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。 6、支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。 7、支持按部门组织架构管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；系统支持风险运维审计实时告警，并通过企业微信或钉钉自动下发，提供相应的技术功能呈现证明材料或承诺函；支持与 get、post、soap 发送方式的 http 短信网关平台联动，实现短信动态口令双因素认证机制；支持常用的运维协议；可通过应用发布的方式进行协议扩展，如数

	常用的运维协议；可通过应用发布的方式进行协议扩展，如数据库、浏览器等客户端工具；支持主流数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机； 8、支持对常见数据库及国产数据库的自动改密功能，包括 DB2、oracle、mysql、sqlserver、PG、人大金仓、GBase8a、GBase8s、达梦、HighGo、Redis、GaussDB 数据库等。（需提供相关有效功能截图证明） 9、支持对 Web 应用的自动改密功能，并且支持堡垒机提供的改密插件录制向导，通过改密插件自动生成 web 应用的改密脚本。（需提供相关有效截图证明） 10、支持复杂账号改密流程自定义编排，支持基于用户/用户组、资产/资产账号/资产目录/资产标签/账号标签/动态账号组等等维度的绑定，并支持授权生效时间段，生效 IP 段。（需提供相关有效截图证明） 11、支持通过基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。运维报表自动定期发送，提供一键导出符合等级保护、SOX 法案要求的综合分析报告； 12、内置丰富的报表统计模板，内置根据运维人员和组生成各种维度的分析报表； 13、支持动态对象授权，提供基于属性策略的动态授权能力。支持主机命令集配置，提供命令解析/正则匹配方式，并提供 5 种日志级别可选，包括提示、低危、中危、高危、非法。（需提供相关有效功能截图证明） 14、运维客户端自带运维工具，可不依赖 xshell/SecureCRT/mstsc 等工具进行运维操作产品厂商具备	数据库、浏览器等客户端工具；支持主流数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机； 8、支持对常见数据库及国产数据库的自动改密功能，包括 DB2、oracle、mysql、sqlserver、PG、人大金仓、GBase8a、GBase8s、达梦、HighGo、Redis、GaussDB 数据库等。 9、支持对 Web 应用的自动改密功能，并且支持堡垒机提供的改密插件录制向导，通过改密插件自动生成 web 应用的改密脚本。 10、支持复杂账号改密流程自定义编排，支持基于用户/用户组、资产/资产账号/资产目录/资产标签/账号标签/动态账号组等等维度的绑定，并支持授权生效时间段，生效 IP 段。 11、支持通过基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。运维报表自动定期发送，支持一键导出符合等级保护、SOX 法案要求的综合分析报告； 12、内置丰富的报表统计模板，内置根据运维人员和组生成各种维度的分析报表。 13、支持动态对象授权，可提供基于属性策略的动态授权能力。支持主机命令集配置，可提供命令解析/正则匹配方式，并提供 5 种日志级别可选，包括提示、低危、中危、高危、非法。 14、运维客户端自带运维工具，可不依赖 xshell/SecureCRT/mstsc 等工具进行运维操作产品厂商具备隐私安全管理系统认证。 15、客户端支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等能力。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之
--	---	--

	隐私安全管理系统认证提供相关证明。 15、客户端还支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等功能。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之间独立。（需提供相关有效截图证明） 16、客户端支持 VPN 登录功能。支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备。（需提供相关功能有效截图证明） 17、具备自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。动作流会按设定好的顺序进行执行，对于常见的运维工作，如升级、巡检等，均可通过此能力快速执行。（需提供相关有效截图证明） 18、需提供用户、资产、授权的增删改查等 API 接口，实现用户、资产的增删改查等 API 接口，允许校园任何第三方平台安全调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化配置工作量； 19、支持国密 TLS 单向认证通信，使用国密算法保证 HTTPS 协议的增删改查等 API 接口，启用后需使用支持国密算法的浏览器才能访问堡垒机。支持采用国密加密算法进行核心敏感数据进行加密存储，且支持使用软件/硬件方式加密，以保证重要数据在系统内存储的机密性。使用硬件进行数据加密时，针对硬件加密组件可提供《商用密码产品认证证书》。 20、产品获得《国家信息安全漏洞库兼容性资质证书》提供相关有效证明材料。	间独立。 16、客户端支持 VPN 登录功能。支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备。 17、具备自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。动作流会按设定好的顺序进行执行，对于常见的运维工作，如升级、巡检等，均可通过此能力快速执行。 18、可提供用户、资产、授权的增删改查等 API 接口，实现用户、校园任何第三方平台安全调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化配置工作量； 19、支持国密 TLS 单向认证通信，使用国密算法保证 HTTPS 协议的增删改查等 API 接口，启用后需使用支持国密算法的浏览器才能访问堡垒机。支持采用国密加密算法进行核心敏感数据进行加密存储，且支持使用软件/硬件方式加密，以保证重要数据在系统内存储的机密性。使用硬件进行数据加密时，针对硬件加密组件可提供《商用密码产品认证证书》。 20、产品获得《国家信息安全漏洞库兼容性资质证书》。	
10	恶意代码检测	1. 系统要求界面友好，并有详尽的技术支持文档，所有图形界面要求中文，系统为 B/S 架构，并采用 SSL 加密通信方式，	1. 系统界面友好，并有详尽的技术支持文档，所有图形界面要求中文，系统为 B/S 架构，并采用 SSL 加密通信方式，用

工具	用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 2. 支持各类 WEB 编程语言的应用的深度网页后门检测；支持常见的 asp、php、jsp、aspx 等多种 WebShell 的有效扫描；支持实时结果的展现；支持生成统计报表；支持 IIS、Websphere、Weblogic、Apache 等所有的应用服务器；支持 Asp、Jsp、.Net、J2EE、Php、Perl 等所有的 WEB 应用编程语言。（提供有效功能截图证明）； 3. 支持实时结果的展现，展现内容应至少包含扫描对象、类型、描述、特征、危险等级和修改时间；支持一键导出单个或所有恶意代码，并以相应的形式进行展示；支持从界面直接打开文件所在目录；引擎应支持黑白名单编辑功能，可添加相应的黑名单和白名单；引擎应支持 win2003/win2008/win2012/win2016/win7/win8/win10 等类型的 win 操作系统；引擎应支持 Redhat/CentOS/suse/ubuntu 等 unix 操作系统同时产品厂商具有云服务信息管理体系认证提供相关证明文件； 4. 支持快速扫描功能：支持根据文件类型自动选择内置扫描策略进行扫描，例如当进行扫描 index.asp 文件时程序会自动选择 ASP 对应的策略进行扫描而忽略其他的扫描策略；（提供有效功能截图证明）； 5. 支持全盘扫描功能，支持扫描所有内置的策略以及用户自定义策略；支持自定义扫描功能，支持文件类型、优先级、扫描策略等用户自定义。 6. 硬件支撑要求：采用安全的 Linux 操作系统，双核或双核以上 CPU，8G 以上内存，至少 1T 硬盘空间；提供用户概述功能，详细展示客户端使用登录、使用情况，上传的文件样本数及人工审核确认数；	用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 2. 支持各类 WEB 编程语言的应用的深度网页后门检测；支持常见的 asp、php、jsp、aspx 等多种 WebShell 的有效扫描；支持实时结果的展现；支持生成统计报表；支持 IIS、Websphere、Weblogic、Apache 等所有的应用服务器；支持 Asp、Jsp、.Net、J2EE、Php、Perl 等所有的 WEB 应用编程语言。 3. 支持实时结果的展现，展现内容应包含扫描对象、类型、描述、特征、危险等级和修改时间；支持一键导出单个或所有恶意代码，并以相应的形式进行展示；支持从界面直接打开文件所在目录；引擎应支持黑白名单编辑功能，可添加相应的黑名单和白名单；引擎应支持 win2003/win2008/win2012/win2016/win7/win8/win10 等类型的 win 操作系统；引擎应支持 Redhat/CentOS/suse/ubuntu 等 unix 操作系统； 4. 支持快速扫描功能：支持根据文件类型自动选择内置扫描策略进行扫描，例如当进行扫描 index.asp 文件时程序会自动选择 ASP 对应的策略进行扫描而忽略其他的扫描策略； 5. 支持全盘扫描功能，支持扫描所有内置的策略以及用户自定义策略；支持自定义扫描功能，支持文件类型、优先级、扫描策略等用户自定义。 6. 硬件支撑：采用安全的 Linux 操作系统，双核或双核以上 CPU，8G 以上内存，1T 硬盘空间；提供用户概述功能，详细展示客户端使用登录、使用情况，上传的文件样本数及人工审核确认数； 7. 支持对系统参数进行配置，包括网络配置及系统安全参数的配置，如登录失败处理功能、最大并发、用户登录超时时间等；	离
----	---	--	---

11	终端安全实验平台	★7. 支持对系统参数进行配置,包括网络配置及系统安全参数的配置,如登录失败处理功能、最大并发、用户登录超时时间等;提供接口管理功能,能与其他系统进行对接;提供引擎管理功能,能对引擎进行配置改造;支持对引擎的检测记录进行展示功能;支持对单条检测记录的展示,展示的内容至少包含扫描文件数、威胁数量、扫描 IP、客户端版本号、扫描时间、扫描用时; 8. 支持提供离线检测工具;离线检测工具包含 windows 和 linux 版本;离线检测工具应支持实时生成检测报告;平台可以对恶意代码的特征进行分析 and 展示。提供多权分立的账户体系,用户能根据其地域对下属单位进行管理; 9. 可提供系统 5 年免费质保及升级服务。	可提供接口管理功能,能与其他系统进行对接;提供引擎管理功能,能对引擎进行配置改造;支持对引擎的检测记录进行展示功能;支持对单条检测记录的展示,展示的内容至少包含扫描文件数、威胁数量、扫描 IP、客户端版本号、扫描时间、扫描用时; 8. 支持提供离线检测工具;离线检测工具包含 windows 和 linux 版本;离线检测工具应支持实时生成检测报告;平台可以对恶意代码的特征进行分析 and 展示。提供多权分立的账户体系,用户能根据其地域对下属单位进行管理; 9. 可提供系统 5 年免费质保及升级服务。	
		1. 采用 B/S 架构管理端,具备终端分组管理、策略制定下发、统一漏洞修复、统一管控、统一终端准入合规、终端软件管理、资产管理、EDR 威胁追踪、数据防泄漏以及各种报表和查询等功能,支持展示全网终端日志; 2. 客户端支持防卸载,支持设置保护密码,终端退出或卸载时需要输入正确的密码方可执行 ★3. 支持控制中心防暴力破解,支持采用手机 APP 动态令牌方式进行二次认证,针对控制中心高危操作支持动态口令验证,要求令牌 APP 自主研发;(提供产品界面和手机动态令牌 APP 有效截图证明) 4. 支持控制中心迁移、数据备份、数据恢复;支持邮件报警,支持设定多种触发条件,满足条件后自动发送邮件到相关人;控制中心支持热备部署 5. 支持与 NGFW、上网行为管理、准入产品联动,达到网边界联动防御效果(提供相关有效功能截图证明) 6. 支持资产自助登记、自助分组功能,支持硬盘序列号收集、	1. 采用 B/S 架构管理端,具备终端分组管理、策略制定下发、统一漏洞修复、统一管控、统一终端准入合规、终端软件管理、资产管理、EDR 威胁追踪、数据防泄漏以及各种报表和查询等功能,支持展示全网终端日志; 2. 客户端支持防卸载,支持设置保护密码,终端退出或卸载时需要输入正确的密码方可执行 3. 支持控制中心防暴力破解,支持采用手机 APP 动态令牌方式进行二次认证,针对控制中心高危操作支持动态口令验证,要求令牌 APP 自主研发; 4. 支持控制中心迁移、数据备份、数据恢复;支持邮件报警,支持设定多种触发条件,满足条件后自动发送邮件到相关人;控制中心支持热备部署 5. 支持与 NGFW、上网行为管理、准入产品联动,达到网边界联动防御效果 6. 支持资产自助登记、自助分组功能,支持硬盘序列号收集、支持 SN 号收集;支持按终端维度展示终端的硬件、软件、操	无偏离

	支持 SN 号收集；支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息； 7. 支持自动发现接入网内的终端设备，支持统计全网终端安装率统计，支持插件清理，可清理指定或全部插件 8. 支持 ldap 联动，终端实名认证后自动同步资产信息 9. 提供多引擎检测能力，包括但不限于云查引擎、人工智能 AI 引擎、启发式引擎。 10. 扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件；（提供相关有效功能截图证明） 11. 支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理； 12. 支持文件解压缩病毒查杀，支持对 zip、rar、7z 等多种格式的压缩文件查杀能力；支持设置压缩包扫描层数，压缩包格式类型，最大扫描压缩包的大小； 13. 具备公有云检测能力，并且公有云特征储备超过 50 亿； 14. 具备自有漏洞补丁管理服务，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理。 15. 支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况 16. 支持 Windows 10 补丁预热，提高终端下载补丁成功率（提供相关有效功能截图证明） 17. 补丁通告解读：发布补丁库时会同步发布一篇补丁通告，详述每次发布的补丁的详细情况， 18. 支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用； 19. 支持冗余有线网卡、无线网卡、3G 网卡、MODEM、ADSL、ISDN 等设备的外联控制；	作系统、网络、进程等信息； 7. 支持自动发现接入网内的终端设备，支持统计全网终端安装率统计，支持插件清理，可清理指定或全部插件 8. 支持 ldap 联动，终端实名认证后自动同步资产信息 9. 可提供多引擎检测能力，包括但不限于云查引擎、人工智能 AI 引擎、启发式引擎。 10. 扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件； 11. 支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理； 12. 支持文件解压缩病毒查杀，支持对 zip、rar、7z 等多种格式的压缩文件查杀能力；支持设置压缩包的扫描层数，压缩包格式类型，最大扫描压缩包的大小； 13. 具备公有云检测能力，并且公有云特征储备超过 50 亿； 14. 具备自有漏洞补丁管理服务，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理。 15. 支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况 16. 支持 Windows 10 补丁预热，提高终端下载补丁成功率 17. 补丁通告解读：发布补丁库时会同步发布一篇补丁通告，详述每次发布的补丁的详细情况， 18. 支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用； 19. 支持冗余有线网卡、无线网卡、3G 网卡、MODEM、ADSL、ISDN 等设备的外联控制； 20. 支持禁止终端创建热点，支持设置可信 ssid 白名单，支持设置可信 ssid 与 mac 地址校验功能。 21. 支持终端进程红名单、黑名单、白名单功能，可设置核心
--	--	--

	20. 支持禁止终端创建热点，支持设置可信 ssid 白名单，支持设置可信 ssid 与 mac 地址校验功能。 21. 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。 22. 支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMCIA）设置使用权限； 23. 支持能耗管理，支持定时关机策略，支持性能监控 24. 支持管理员对入网的移动存储介质进行注册，支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批； 25. 支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限； 26. 支持移动存储介质读写权限划分设置，有效控制不明来历的移动存储可能带来的病毒传播等隐患 27. 支持针对 Windows XP 系统可带来风险隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 28. 支持针对 Windows 7 系统可带来风险隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 29. 支持移动存储设备、网络共享服务器、本地硬盘特定扩展名或特定目录下的文件访问、修改、删除、移动等行为的审计 30. 支持网络打印操作、本地打印操作、虚拟打印操作审计；支持邮件发送审计；支持终端访问的互联网全日志的审计；支持对应用程序的启动和停止进行记录；支持 USB、蓝牙或红外等终端外设接口接入外设的使用情况审计；支持终端的启动、关闭、待机、休眠、等状态的记录与统计； 31. 支持本机账户或域账户登录日志统计；支持 U 盘操作日志的审计，支持离网使用日志审计。 32. 支持全部拦截和全屏拦截两种模式，开启弹窗防护功能后自动拦截第三方软件的弹窗，使用场景更加灵活。	进程必须运行，也可保护核心进程不被结束。 22. 支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMCIA）设置使用权限； 23. 支持能耗管理，支持定时关机策略，支持性能监控 24. 支持管理员对入网的移动存储介质进行注册，支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批； 25. 支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限； 26. 支持移动存储介质读写权限划分设置，有效控制不明来历的移动存储可能带来的病毒传播等隐患 27. 支持针对 Windows XP 系统可带来风险隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 28. 支持针对 Windows 7 系统可带来风险隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 29. 支持移动存储设备、网络共享服务器、本地硬盘特定扩展名或特定目录下的文件访问、修改、删除、移动等行为的审计 30. 支持网络打印操作、本地打印操作、虚拟打印操作审计；支持邮件发送审计；支持终端访问的互联网全日志的审计；支持对应用程序的启动和停止进行记录；支持 USB、蓝牙或红外等终端外设接口接入外设的使用情况审计；支持终端的启动、关闭、待机、休眠、等状态的记录与统计； 31. 支持本机账户或域账户登录日志统计；支持 U 盘操作日志的审计，支持离网使用日志审计。 32. 支持全部拦截和全屏拦截两种模式，开启弹窗防护功能后自动拦截第三方软件的弹窗，使用场景更加灵活。
--	---	--

	的审计，支持离网使用日志审计。 ★32. 支持全部拦截和全屏拦截两种模式，开启弹窗防护功能后自动拦截第三方软件的弹窗，使用场景更加灵活。（提供相关有效功能截图证明） 33. 支持终端用户通过天擎自动抓取非主流第三方软件弹窗规则并上报拦截申请，弹窗防护无死角。（提供相关有效功能截图证明） 34. 支持管理员通过手动添加或处置终端用户拦截申请来运维本地弹窗规则黑名单，可对非主流第三方软件的弹窗进行拦截。（提供相关有效功能截图证明） 35. 支持管理员按分组、按时间查看弹窗拦截报表、不同维度的数据统计和拦截日志详情。 36. 支持持续自动化运营弹窗规则，支持定期从云端更新弹窗防护规则库，提高弹窗拦截能力。 37. 支持对终端操作系统之间东西流量访问控制，支持基于数据包流向（任意/流入/流出）、协议（TCP/UDP/ICMP/TCP+UDP）、端口和 IP 的访问控制。 38. 支持对主机防火墙日志集中呈现，支持时间、计算机名、通信 IP、分组、规则名称、协议、命中次数、IP 和端口等日志字段显示。	33. 支持终端用户通过天擎自动抓取非主流第三方软件弹窗规则并上报拦截申请，弹窗防护无死角。 34. 支持管理员通过手动添加或处置终端用户拦截申请来运维本地弹窗规则黑名单，可对非主流第三方软件的弹窗进行拦截。 35. 支持管理员按分组、按时间查看弹窗拦截报表、不同维度的数据统计和拦截日志详情。 36. 支持持续自动化运营弹窗规则，支持定期从云端更新弹窗防护规则库，提高弹窗拦截能力。 37. 支持对终端操作系统之间东西流量访问控制，支持基于数据包流向（任意/流入/流出）、协议（TCP/UDP/ICMP/TCP+UDP）、端口和 IP 的访问控制。 38. 支持对主机防火墙日志集中呈现，支持时间、计算机名、通信 IP、分组、规则名称、协议、命中次数、IP 和端口等日志字段显示。	
综合运行硬件平台安全加固平台	1、具备服务器加固应急实验功能，包括：风险点排查、外网暴露面收敛、操作系统加固、文件监控与防护、病毒实时防护、勒索诱饵防护、系统原点和卷影保护、勒索病毒查杀、勒索病毒一键隔离、勒索病毒防护模板、登录控制等功能，支持 Windows、Centos、RHEL、Ubuntu、麒麟、UOS、Debian 等多种操作系统。 ★2、防勒索功能：具备勒索专项治理功能，可在一个界面查看已处置外网暴露端口数量、未处置外网暴露端口数量、已开	1、具备服务器加固应急实验功能，包括：风险点排查、外网暴露面收敛、操作系统加固、文件监控与防护、病毒实时防护、勒索诱饵防护、系统原点和卷影保护、勒索病毒查杀、勒索病毒一键隔离、勒索病毒防护模板、登录控制等功能，支持 Windows、Centos、RHEL、Ubuntu、麒麟、UOS、Debian 等多种操作系统。 2、防勒索功能：具备勒索专项治理功能，可在一个界面查看已处置外网暴露端口数量、未处置外网暴露端口数量、已开启	无偏离

	启暴力破解防护数量、未开启暴力破解防护数量、已开启远程登录控制数量、未开启远程登录控制数量、弱口令数量、复用口令数量、已处置漏洞数量、未处置漏洞数量、已检出 Webshell 数量、已开启勒索实时防护数量、未开启勒索实时防护数量、已开启勒索诱饵防护数量、未开启勒索诱饵防护数量、已开启内核免疫数量、未开启内核免疫数量、已开启系统还原点和卷影保护数量、未开启系统还原点和卷影保护数量、已开启操作加固数量、未开启操作加固数量、已开启文件监控与文件监控与防护数量、未开启文件监控与防护数量、已处置病毒数量、未处置病毒数量、已感染服务器数量、未感染服务器数量、以上功能需在一个界面实现，无需多界面跳转查询。（提供相关有效功能截图证明） 3、主机发现功能：支持调用多台服务器发起扫描任务，可扫描发起服务器的内网网段、指定网段，扫描方式支持 ARP 缓存方式、Ping 方式、Nmap 方式，并可设置并发扫描最大数量、每秒最大发包数等参数，提供上述功能有效截图证明。 4、虚拟补丁功能：虚拟补丁库规则数量≥7000 条，可查看每条规则适用的操作系统类型、影响、漏洞编号等信息。 5、流量转发功能：支持基于 VXLAN 和 GRE 的流量转发，可配置流量接受对象 IP 地址、转发端口、转发速率阈值，并可通上述功能有效截图证明。 6、攻击检测功能：支持报告并记录相应的安全事件，包括：端口扫描、强力攻击、缓冲区溢出攻击、可疑连接攻击，记录的内容包括事件名称、攻击源地址、目的地址、事件发生时间、重要级别等信息，要求提供第三方测评机构出具的检测报告关键页证明。	暴力破解防护数量、未开启暴力破解防护数量、已开启远程登录控制数量、未开启远程登录控制数量、弱口令数量、复用口令数量、已处置漏洞数量、未处置漏洞数量、已检出 Webshell 数量、已开启勒索实时防护数量、未开启勒索实时防护数量、已开启勒索诱饵防护数量、未开启勒索诱饵防护数量、已开启内核免疫数量、未开启内核免疫数量、已开启系统还原点和卷影保护数量、未开启系统还原点和卷影保护数量、已开启操作加固数量、未开启操作加固数量、已开启文件监控与防护数量、未开启文件监控与防护数量、已感染服务器数量、未感染服务器数量、以上功能需在一个界面实现，无需多界面跳转查询。 3、主机发现功能：支持调用多台服务器发起扫描任务，可扫描发起服务器的内网网段、指定网段，扫描方式支持 ARP 缓存方式、Ping 方式、Nmap 方式，并可设置并发扫描最大数量、每秒最大发包数等参数。 4、虚拟补丁功能：虚拟补丁库规则数量 7000 条，可查看每条规则适用的操作系统类型、影响、漏洞编号等信息。 5、流量转发功能：支持基于 VXLAN 和 GRE 的流量转发，可配置流量接受对象 IP 地址、转发端口、转发速率阈值，并可通过 BPF 语法自定义过滤规则采集流量。 6、攻击检测功能：支持报告并记录相应的安全事件，包括：端口扫描、强力攻击、缓冲区溢出攻击、可疑连接攻击，记录的内容包括事件名称、攻击源地址、目的地址、事件发生时间、重要级别等信息。 8、事件记录功能：支持安全事件按照严重程度进行分级，事件等级分为：危急、高危、中危、低危，可对高频度发生的相同安全事件进行合并告警，能够显示包括事件名称、发生次数、源 IP 等信息。
--	---	--

		7、事件记录功能：支持安全事件按照严重程度进行分级，事件等级分为：危急、高危、中危、低危，可对高频率发生的相同安全事件进行合并告警，能够显示包括事件名称、发生次数、源IP等信息，要求提供第三方测评机构出具的检测报告关键页证明。 8、报表功能：支持以默认的报告模板生成详尽的检测结果报告并以饼图和折线图等形式对数据区间内的事件类型、发生次数进行了统计，可输出WORD、HTML格式的检测报告，可修改和定制报告内容，能够定制包括：报告模板、报告格式、服务器范围。 9、在联动实验中，为满足学生对漏洞特征库资源的实验需求，系统厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升软件防护能力，2022-2024任意一年向国家漏洞共享平台CNVD提交漏洞数30000个。 10、产品具备云计算产品信息安全认证证书。	8、报表功能：支持以默认的报告模板生成详尽的检测结果报告并以饼图和折线图等形式对数据区间内的事件类型、发生次数进行了统计，可输出WORD、HTML格式的检测报告，可修改和定制报告内容，能够定制包括：报告模板、报告格式、服务器范围。 9、在联动实验中，为满足学生对漏洞特征库资源的实验需求，系统厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关防护规则提升软件防护能力，2022-2024任意一年向国家漏洞共享平台CNVD提交漏洞数30000个。 10、产品具备云计算产品信息安全认证证书。	
13	SDN交换机	1、标准1RU盒式设备，吞吐量≥880Gbps，整机超低功耗； 2、支持OpenFlow 1.3.x/1.4.x版本，支持3.5K*流表，支持L2到L4完整匹配域，支持基于单条流表项的多种行为； 支持二层GRE/NvGRE/VXLAN隧道；支持MPLS L2 VPN/MPLS，支持 QinQ；Meter表项最大支持1000* meter ID；支持 Group (all/select/indirect/fast failover)；支持队列；支持 Bond；	1、标准1RU盒式设备，吞吐量880Gbps，整机超低功耗； 2、支持OpenFlow 1.3.x/1.4.x版本，支持3.5K*流表，支持L2到L4完整匹配域，支持基于单条流表项的多种行为； 支持二层GRE/NvGRE/VXLAN隧道；支持MPLS L2 VPN/MPLS，支持 QinQ；Meter表项最大支持1000* meter ID；支持 Group (all/select/indirect/fast failover)；支持队列；支持 Bond；	无偏离
14	串口服务器	串口服务器 8 口 RS232/422/485 机架式 220V	串口服务器 8 口 RS232/422/485 机架式 220V	无偏离

15	网络交换机	1. 性能: 整机交换容量 $\geq 496\text{Gbps}$; 转发性能 $\geq 144\text{Mpps}$ 2. 端口: ≥ 48 千兆电+4 千兆 SFP 3. MAC 地址表 $\geq 16\text{K}$, IPv4 路由表容量 ≥ 512, ARP $\geq 1\text{K}$ 4. 支持 IPv4/IPv6 静态路由, 支持 RIP/RIPng, OSPFV2/V3 5. 交换机支持 ≥ 9 台物理设备虚拟化技术, 支持完善的堆叠分裂检测机制, 堆叠分裂后能自动完成 MAC 和 IP 地址的重配置, 无需手动干预 6. 实现 ERPS 功能, 能够快速阻断环路, 链路收敛时间 $\leq 50\text{ms}$ 7. 实现 CPU 保护功能, 能限制非法报文对 CPU 的攻击, 保护交换机在各种环境下稳定工作 8. 支持 RRRP (快速环网保护协议), 环网故障恢复时间不超过 50ms, 支持 Smartlink, 支持支持 PVST 功能; 9. 支持 SNMP V1/V2/V3、RMON、SSHV2; 支持端口休眠, 关闭没有应用的端口, 节省能源	1. 性能: 整机交换容量 496Gbps; 转发性能 144Mpps 2. 端口: 48 千兆电+4 千兆 SFP 3. MAC 地址表 16K, IPv4 路由表容量 512, ARP 1K 4. 支持 IPv4/IPv6 静态路由, 支持 RIP/RIPng, OSPFV2/V3 5. 交换机支持 9 台物理设备虚拟化技术, 支持完善的堆叠分裂检测机制, 堆叠分裂后能自动完成 MAC 和 IP 地址的重配置, 无需手动干预 6. 实现 ERPS 功能, 能够快速阻断环路, 链路收敛时间 50ms 7. 实现 CPU 保护功能, 能限制非法报文对 CPU 的攻击, 保护交换机在各种环境下稳定工作 8. 支持 RRRP (快速环网保护协议), 环网故障恢复时间不超过 50ms, 支持 Smartlink, 支持支持 PVST 功能; 9. 支持 SNMP V1/V2/V3、RMON、SSHV2; 支持端口休眠, 关闭没有应用的端口, 节省能源	无偏离
16	综合布线	针对实验室进行信息安全文化场景建设及实验室整体优化改造: 1. 实验室所需优化的网线采用六类网线, 六类水晶头, 网线外护套采用 PVC (聚氯乙烯), 绝缘层采用 PE (聚乙烯), 导体采用优质无氧铜, 内部具有弹性十字骨架分隔线对保证传输性能。相关执行标准按 GB/T 3939.1-2004 进行执行; 2. 实验室所需优化的电源线 and 插座, 根据实验室电量负载需求, 完成强电室内布线。相关执行标准按 GB/T 28567-2022 进行执行。 3. 实验室所需优化的强、弱电改造采用不锈钢线槽, 全部沿线缆槽规范布线, 有强电和弱电走同一个不锈钢线槽要求分支电缆采用 RVV6mm² 以上铜缆, 使用金属穿线管敷设。相关执行标准按 GB/T 28567-2022 进行执行。 4、实验室综合布线符合国家《综合布线系统工程设计规范》	针对实验室进行信息安全文化场景建设及实验室整体优化改造: 1. 实验室所需优化的网线采用六类网线, 六类水晶头, 网线外护套采用 PVC (聚氯乙烯), 绝缘层采用 PE (聚乙烯), 导体采用优质无氧铜, 内部具有弹性十字骨架分隔线对保证传输性能。相关执行标准按 GB/T 3939.1-2004 进行执行; 2. 实验室所需优化的电源线 and 插座, 根据实验室电量负载需求, 完成强电室内布线。相关执行标准按 GB/T 28567-2022 进行执行。 3. 实验室所需优化的强、弱电改造采用不锈钢线槽, 全部沿线缆槽规范布线, 有强电和弱电走同一个不锈钢线槽要求分支电缆采用 RVV6mm² 以上铜缆, 使用金属穿线管敷设。相关执行标准按 GB/T 28567-2022 进行执行。 4、实验室综合布线符合国家《综合布线系统工程设计规范》	无偏离

		GB/T 38002.2-2022 标准，所有实施材料严格按照国家相关产品技术标准，确保实验室整体网络、电路、通信等综合环境安全运行。 ★5、提供在不影响实验室所在楼层教学活动的项目实施方案，方案内容要结合实际情况，符合学校实验场地现场要求。	GB/T 38002.2-2022 标准，所有实施材料严格按照国家相关产品技术标准，确保实验室整体网络、电路、通信等综合环境安全运行。 5、提供在不影响实验室所在楼层教学活动的项目实施，内容结合实际，符合学校实验场地现场要求。	
--	--	---	---	--

合同附件 7:

商务条款偏差一览表

序号	招标文件的商务条款	投标文件的商务条款	说明
1	营业执照	已经提供营业执照	无偏离
2	2024 年度审计报告	已经提供相应的年度审计报告;	无偏离
3	纳税缴纳凭证	已经提供依法缴纳税收证明材料;	无偏离
4	社保缴纳凭证	已经提供依法缴纳社会保障资金的证明材料;	无偏离
5	具备履行合同所必需的设备和专业技术能力的证明材料	已经提供履行合同所必需的设备和专业技术能力 (提供承诺书);	无偏离
6	参加政府采购活动前三年内, 在经营活动中没有重大违法记录的书面声明	已经提供参加政府采购活动前 3 年内在经营活动中没有重大违法记录的声明;	无偏离
7	单位负责人为同一人或者存在直接控股、管理关系的不同供应商, 不得参加同一合同项下的政府采购活动承诺书	已经提供不同投标人单位负责人不是同一人或者未存在直接控股、管理关系的承诺书;	无偏离
8	未被列入失信被执行人网站查询	已经提供未被列入失信被执行人网站查询;	无偏离
9	重大税收违法案件当事人名单网站查询	已经提供重大税收违法案件当事人名单网站查询;	无偏离
10	未被列入政府采购严重违法失信行为记录名单网站查询	已经提供未被列入政府采购严重违法失信行为记录名单网站查询;	无偏离

11	反商业贿赂承诺书	已经提供反商业贿赂承诺书;	无偏离
12	履约承诺书	已经提供履约承诺书;	无偏离



