2026

金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）

网络安全

BRICS-FS-28

技术规程(选拔赛)

2026 年 06 月

目 录

1.赛项简介

1.1 赛项基本信息

赛事名称：2026 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）

赛项名称：网络安全

赛项编号：BRICS-FS-28

赛制（人/选手）：2 人

赛事类型：省级/区域选拔赛（线上赛）

1.2 赛项简要描述

2026 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）网络安全赛项作为培育与锻造网络空间安全技术人才的关键平台，赛项紧跟网络空间安全攻防实战需求，致力于精准选拔具备实战能力的网络空间安全人才，着重对数字化转型进程中新技术融合场景下的网络空间安全风险，全面考核选手在安全规划设计、漏洞管理、应急响应处置及前沿技术安全治理等领域的综合能力。

重点考核参赛选手网络安全实战能力，包括基础环境构建、网络安全理论及职业能力考核、网络与数据安全基础技能应用、网络安全运营技能应用、新技术、新应用领域产生的网络安全挑战（如可信数据空间安全）安全技能应用，具体包括：

（1）参赛选手需要具备网络安全法规与标准理解能力

掌握核心法律法规及标准规范，包括但不限于《中华人民共和国网络安全法》《中华人民共和国数据安全法》 《中华人民共和国个人信息保护法》 《中华人民共和国密码法》 《关键信息基础设施安全保护条例》及《网络与信息安全管理员》《信息通信网络运行管理员》等。

（2）参赛选手需要具备扎实的网络及安全技术基础知识与安全竞赛基础能力

掌握计算机硬件、软件、操作系统、数据库、网络协议等基础知识；具备网络与信息安全管理的基础素养；熟悉基础物理环境配置及图纸绘制、设备选型等。

（3）参赛选手需要具备网络安全事件响应与取证分析能力

能够针对企业发现的安全事件，开展调查、分析与取证工作，具体包括：电子证据的收集、保存、处理、分析与提供；入侵行为的审计追踪；以及被破坏文件或系统的恢复。

（4）参赛选手需要具备渗透测试与漏洞挖掘实战能力

能够熟练运用各类渗透测试工具，对预设的网络环境进行安全分析、漏洞挖掘和综合渗透，以模拟攻击者视角发现和验证安全风险。

（5）参赛选手需要具备应对新兴技术安全威胁的检测与防护能力

针对可信数据空间安全为代表的新技术/新应用领域的安全挑战，具备专项的安全检测和安全防护能力。

2. 技能标准

技能标准规定了在技术和职业表现方面代表国际最佳实践的知识、理解及特定技能。该标准反映了全球范围内对相关工作角色或职业在行业与企业中所代表内容的共识。

技能竞赛旨在体现该技能标准所描述的国际最佳实践及其所能达到的水平。因此，该标准是技能竞赛所需培训与准备的指南。

（1）网络安全法律法规

参赛选手应了解：《中华人民共和国网络安全法》《中华人民共和国数据安全

法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》及《网络与信息安全管理员（数据安全管理员）国家职业标准》等。

参赛选手应掌握：具备将网络安全和隐私原则融入总体程序测试与评估过程的设计和记录的能力，涵盖保密性、完整性、可用性、身份验证及数字签名不可抵赖性等关键要素；能够独立全面地评估管理、操作和技术安全控制，精准判断信息技术系统内部及其集成控制的有效性；具备开发、维护计算机应用程序、软件的能力，包括新建与修改，同时能够分析其安全状况并提供可靠结果；具备开展软件系统研究的能力，能够开发具备网络安全防护功能的新功能，评估网络安全系统薄弱环节；依据技术规范和要求，具备计划、实施系统测试的能力，能够进行分析评估并形成报告，全面测试信息系统安全，覆盖系统开发生命周期。

（2）基础网络安全攻防实战

参赛选手应了解：基础环境搭建设计及设备选型、操作系统基础（Linux 文件和目录结构、环境安装部署等）、基础命令、配置与管理，以及 Linux 文件系统、Shell 和文本操作；应用服务器原理、网页知识；网络各层协议及组网通信技术；脚本语言、PHP、Java、前端语言等开发基础。

参赛选手应掌握：具备网络拓扑设计及绘制能力；物理平面图绘制能力；能够根据预算精准设备选型能力；具备数据库及数据库管理系统管理的能力；能够实施流程和工具管理，保障机构知识资产和信息的有效性；具备问题处理能力，涵盖安装、配置、故障排除，依据需求提供维护培训；具备采集数据准确性验证的能力；具备网络设备和防火墙（软硬件）全生命周期管理的能力，保障信息共享传输安全；具备服务器（软硬件）管理的能力，确保信息三大属性；具备账户、防火墙、系统补丁管理的能力；具备访问控制及账户密码管理的能力；能够检查优化机构计算机系统和流程。

（3）安全事件应急响应

参赛选手应了解：行业技术标准、分析原则方法工具；威胁调查报告工具法规；网络安全事件分类处理方法；网络防御漏洞评估工具功能；已知安全风险应对；身份验证授权访问方法。

参赛选手应掌握：具备运用防护措施和多源信息识别分析报告网络事件的能力；具备管理硬件软件基础架构的能力，保障网络防护服务；具备监控网络记录未授权活动的能力；在专业领域具备有效响应危机降低威胁的能力；具备运用缓解准备措施响应恢复保障安全的能力；具备调查分析应急响应活动的能力；具备评估威胁漏洞的能力；能够依据风险水平制定业务非运营场景缓解措施。

（4）WEB 漏洞挖掘与防护

参赛选手应了解：网络威胁行为者背景方法；检测可利用活动技术；网络情报收集能力资源；网络威胁漏洞；Web、服务器漏洞及探测工具原理；各类漏洞利用方法及提权原理。

参赛选手应掌握：具备使用漏洞探测工具精准探测各类漏洞的能力；具备运用技术手段进行弱口令爆破、敏感文件获取、数据库信息提取、恶意代码注入执行等操作的能力；熟练掌握并运用常用渗透工具的能力。

（5）威胁分析与调查取证

参赛选手应了解：威胁调查报告工具法规；恶意软件分析；电子证据处理流程及监管链维持；司法流程及证据要求；数据类型及取证方法；漏洞具体影响。

参赛选手应掌握：具备规范进行计算机证据收集处理保存分析的能力，助力调查并减轻网络脆弱性。

（6）新技术、新应用领域网络安全挑战

参赛选手应了解：在新技术、新应用场景下数据安全面临的核心挑战，包括：复杂环境（如多源、跨系统/地域流动）中的数据面临的非授权访问、窃取、泄露风险；新架构（如云原生、边缘计算）带来的信任边界模糊化导致的权限控制、隔离与审计挑战；高级持续性威胁（APT）中的隐蔽数据窃取、滥用及精细的数据篡改与破坏风险；大规模数据聚合、关联分析导致的隐私侵犯与去匿名化风险；以及通过模型输出或系统特性可能引发的敏感原始数据泄露风险（如模型逆向、成员推理攻击）。同时，需掌握关键合规要求，如重要数据识别与管理、数据分类分级标准（核心、重要、一般数据）以及《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等核心法规的基本原则（数据安全义务、个人信息处理规则、数据出境安全评估）和相关国家/行业标准在新场景下的适用性。

参赛选手应掌握：针对新技术、新应用场景，系统地开展数据安全风险评估，识别数据处理全生命周期（采集、传输、存储、处理、共享、发布、销毁）中的潜在风险点及关键数据资产威胁；基于风险评估和合规要求，设计并制定覆盖数据全生命周期的有效安全策略与措施（包括但不限于：数据最小化采集与脱敏/匿名化应用；设计细粒度、可审计的访问控制（如 RBAC/ABAC）与权限管理；规划并实施适用的数据传输（如 TLS）与静态存储加密；应用技术（如哈希、签名）保障数据完整性；设计安全的数据传输与共享机制；定义数据留存与安全销毁策略）；具备配置或集成主流数据安全技术（如 DLP、数据库审计、密钥管理、安全网关、日志审计分析等）来有效实施上述策略，保障数据的机密性、完整性和可用性；持续跟踪数据安全技术发展、新兴威胁态势及法规标准更新，主动学习以适应变化提升能力；快速识别、研判和响应数据泄露、非法访问、篡改、破坏等安全事件，有效执行应急响应流程进行处置、恢复。

3. 竞赛内容

竞赛采用线上闭卷形式，全程通过网络安全竞技平台完成，四个阶段连续进行，各

阶段合并计时、到点自动收卷，阶段间不设休息时间。

竞赛阶段	阶段名称	竞赛时间（分钟）	权重	评分方式
第一阶段	职业素养与理论技能	第一天上午 30 分钟	10%	自动评分
第二阶段	安全网络架构设计及设备选型	第一天上午 30 分钟	15%	人工评分
第三阶段	安全网络架构构建	第一天上午 60 分钟	35%	人工评分
第四阶段	网络安全技能应用	第一天上午 60 分钟	40%	人工评分
合计		180 分钟	100%	

（1）第一阶段：职业素养与理论技能

知识点	说明
职业素养	涵盖网络安全规范意识、安全意识以及纪律意识等内容。要求参赛选手熟悉网络安全行业的准则与最佳实践，主动预防安全风险，严格遵守工作和竞赛纪律，按时完成各项任务。
法律法规	包含《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》等法律法规，以及其它与网络和数据安全相关的法律法规和标准规范。参赛选手需深入理解这些法律法规，确保在网络安全实践中的合法合规性。
漏洞挖掘	包括 Web 漏洞原理知识，如 SQL 注入、跨站脚本（XSS）、跨站请求伪造（CSRF）等，以及服务器漏洞原理知识。同时，还需掌握各类漏洞的基本利用方法，例如利用弱口令进行爆破、利用文件类漏洞获取

	或上传敏感文件、利用命令执行漏洞运行恶意命令、利用 SQL 注入漏洞获取数据库信息等。
数据安全	涉及数据安全法规政策、基础理论、技术理论、管理流程、安全评估以及个人数据安全意识等方面。参赛选手需了解数据安全相关的法规政策，掌握数据的完整性、保密性、可用性等基础理论，熟悉加密、访问控制、数据备份等技术理论，知晓数据生命周期管理、数据分类分级等管理流程，能够评估数据安全风险并制定防护措施，同时提高个人数据安全意识。
应急响应	要求参赛选手掌握应急响应的原理流程与排查方法。在 Linux 和 Windows 系统中，能够进行账户排查，包括特权账户和影子账户；网络通信与端口排查，使用相关工具查看网络连接；进程分析，通过命令分析系统进程；启动项分析，检查系统启动项；定时任务排查，查看 crontab 等定时任务；服务分析，分析系统服务；Webshell 排查，检测 Webshell 文件；系统后门排查，查找系统后门；还能识别常见 web 漏洞攻击特征、敏感信息漏洞利用特征以及 sql 注入漏洞利用特征等。
安全加固	在 Windows 系统中，涉及账户与密码的安全策略设置，如设置强密码策略；用户和用户组的权限管理，合理分配用户权限；审核功能的启用，记录系统活动；以及利用日志和安全模板分析配置计算机。在 Linux 系统中，要求掌握账号和组的管理，了解弱口令密码的风险及检查方法，知晓检查空口令和系统中其它 id 为 0 用户的方法，熟悉 Linux 文件系统的文件格式分类。
网络安全架构与防御技	掌握网络拓扑设计、IP 地址规划、子网划分、VLAN 隔离、网络部署

术	技术、安全设备（FW、IPS、WAF 等）基础原理、网络安全设备工作原理。

（2）第二阶段：安全网络架构设计及设备选型

知识点	说明
安全网络架构设计	要求参赛选手熟练掌握绘图工具，能够设计并绘制包含多元化安全组件的网络环境图。 内容需涵盖网络基础架构及关键安全防护设备的部署，明确防火墙、入侵防御系统、Web 应用防火墙等设备在网络中的逻辑位置与物理连接。准确标注设备名称、型号、IP 地址及互联接口，科学规划子网与 VLAN。 能够根据业务场景（如办公网、数据中心），绘制集成了网络设备、安全设备的网络平面图及机柜图，确保图面信息完整，清晰展示安全流量走向与设备防护边界。
设备选型	参赛选手需根据网络规模、业务性能及安全防护需求进行设备及物料选型。依据预算，对于网络及安全设备，需确保设备具备相应的安全功能模块（如防火墙访问控制、IPS 入侵防御、WAF 应用防护等），并能与网络架构有效融合。设备应满足基础的高速数据转发与冗余容错能力，同时需对所需物料进行估算，重点考量设备间的协议兼容性及未来安全策略部署的灵活性。

（3）第三阶段：安全网络架构构建

知识点	说明
基础网络架	网络拓扑搭建配置要兼顾安全性与功能性。提升带宽与可靠性。设置

构部署	安全设备，划分安全区域，配置安全策略，阻挡非法访问。构建高可靠、高安全的网络传输底座。选手需部署高性能交换与路由架构，实现内部网络的高效互通与逻辑隔离；部署 VPN 等远程接入方案，支撑零信任网络架构下的安全连接。开启日志记录与监控功能，便于及时发现并处理潜在安全威胁。
安全功能防护	安全配置需确保全面防护：防火墙启用状态检测及严格的安全策略，隔离拓扑流量；IPS、IDS 实时监测并阻止入侵行为；WAF 防御 SQL 注入、XSS 和 CSRF 攻击；网络设备配置安全防护。

（4）第四阶段：网络安全技能应用

知识点	说明
网络攻防渗透与漏洞挖掘	要求参赛选手能够使用漏洞探测工具，准确探测 Web 漏洞、网络服务脆弱性以及服务器漏洞。具备利用漏洞进行攻击的能力，包括利用弱口令爆破，利用文件类漏洞获取敏感文件或上传恶意代码，利用命令执行漏洞运行恶意命令，利用 SQL 注入漏洞获取数据库信息，利用 XSS 漏洞实现恶意代码注入和执行，利用目录遍历漏洞访问任意文件，利用 XXE 漏洞执行探测和攻击，利用 CSRF 漏洞伪造请求，利用 SSRF 漏洞伪造请求，以及通过信息泄露漏洞访问敏感信息等。
数据安全分析与应用	主要考察选手的数据包分析和数据取证能力，包括检测和防止敏感信息泄露、对数据进行分类管理、应用数字水印技术保护数字内容版权和完整性，以及掌握常见加解密算法如 AES、RSA 等。
网络安全事件	要求参赛选手掌握入侵检测、抑制处置、系统恢复和证据收集等知

响应	识点，并能够将其运用到实际操作中。能够及时发现入侵行为，采取有效措施阻止攻击进一步发展，迅速恢复系统正常运行，同时妥善收集和保存证据，为后续分析提供支持。
安全加固与溯源分析	安全加固方面，要求参赛选手掌握如何增强系统防御能力的方法，如合理配置安全策略、更新系统补丁、强化访问控制等。溯源分析则要求选手具备追踪攻击来源、分析攻击路径的能力，能够通过分析系统日志、网络流量等信息，还原攻击过程，找出攻击源头，为防范类似攻击提供依据。
可信数据空间安全	针对新技术、新应用场景，系统地开展数据安全风险评估，识别数据处理全生命周期（采集、传输、存储、处理、共享、发布、销毁）中的潜在风险点及关键数据资产威胁；基于风险评估和合规要求，设计并制定覆盖数据全生命周期的有效安全策略与措施（包括但不限于：数据最小化采集与脱敏/匿名化应用；设计细粒度、可审计的访问控制（如 RBAC/ABAC）与权限管理；规划并实施适用的数据传输（如 TLS）与静态存储加密；应用技术（如哈希、签名）保障数据完整性；设计安全的数据传输与共享机制；定义数据留存与安全销毁策略）；具备配置或集成主流数据安全技术（如 DLP、数据库审计、密钥管理、安全网关、日志审计分析等）来有效实施上述策略，保障数据的机密性、完整性和可用性；持续跟踪数据安全技术发展、新兴威胁态势及法规标准更新，主动学习以适应变化提升能力；快速识别、研判和响应数据泄露、非法访问、篡改、破坏等安全事件，有效执行应急响应流程进行处置、恢复。
安全合规与审	聚焦企业常态化安全运营与合规治理能力，核心知识点覆盖《网络

计	安全等级保护基本要求》（GB/T 22239-2019）三级标准中主机安全、应用安全、安全审计的核心控制项，Linux 系统日志与 Web 服务日志的全生命周期管理机制，访问控制与最小权限原则，以及企业安全运营的基础流程与合规管理规范。技能层面要求选手能够对照等保标准逐项开展系统合规性自查，精准识别不符合项并提出可落地的整改建议；能够独立完成系统日志、Web 访问日志的轮转策略与留存周期配置，满足合规审计的日志留存要求；能够审计现有系统权限与访问策略的风险点，基于最小权限原则输出策略优化方案，全面匹配安全运营专员、等保测评助理等岗位的基础工作能力要求。

4. 评分标准

（一）评分设计总体思路

1.本赛项第一阶段实行竞赛平台自动评分，后三个阶段人工评分。在评分过程中，为保障信息安全，需进行两次加密操作。加密工作由专门的加密裁判负责，确保加密过程规范、准确。

2.第一组加密裁判负责首次抽签，产生参赛编号，替换选手个人身份信息，并记录加密过程。

3.第二组加密裁判组织第二次抽签，确定赛位号，替换参赛编号，并记录加密过程。

4.所有加密结果均须经加密裁判和监督人员签字确认，确保加密过程的透明性和可追溯性。

5.四个阶段成绩汇总解密后，由裁判长进行复核并签字确认，确保成绩的准确性

和公正性。最后，成绩由工作人员录入系统，完成整个评分流程。

（二）评分模块与分值构成

竞赛按任务评分，满分为 100 分，详细评分要求见下表。

竞赛阶段	阶段名称	任务阶段	评分方式
第一阶段(权重 10%)	职业素养与理论技能	题 1…N	自动评分
第二阶段(权重 15%)	安全网络架构设计及设备选型	任务 1…N	人工评分
第三阶段(权重 35%)	安全网络架构构建	任务 1…N	人工评分
第四阶段(权重 40%)	网络安全技能应用	任务 1…N	人工评分

（三）模块评分要点设计

模块 1：职业素养与理论技能（10 分），涵盖网络安全规范意识、法律法规、安全法规、网络安全防御等知识点。

模块 2：安全网络架构设计及设备选型（15 分），设备选型、网络安全架构设计及平面图规划。

模块 3：安全网络架构构建（35 分），基础网络架构部署及安全防护功能部署。

模块 4：网络安全技能应用（40 分），网络攻防渗透与漏洞挖掘、网络安全事件响应、安全加固与溯源分析、安全合规与审计。

（四）评分方式设计

1. 系统自动评分与专家评分相结合，客观题自动计分，主观操作题按要点赋分。

2. 所有评审材料统一加密、匿名处理，实行盲评。

3.实行“双评复核”机制，两名裁判独立评分，差值超限则提交裁判长裁定。

4.严格按照赛前公布标准执行，不临时调整、不人为放宽。

（五）成绩合成与排名规则设计

1.总成绩=模块 1+模块 2+模块 3+模块 4（满分 100 分）。

2.按总成绩从高到低排名。

3.总分相同情况下的优先级规则：第 1 优先级：模块 4（网络安全技能应用）得分高者排名靠前；第 2 优先级：模块 3（安全网络架构构建）得分高者排名靠前；第 3 优先级：模块 2（安全网络架构设计及设备选型）得分高者排名靠前；第 4 优先级：模块 1（职业素养与理论技能）得分高者排名靠前。

（六）评分质量保障设计

1.赛前对所有裁判进行统一培训，明确评分尺度、扣分标准、判定原则。

2.成绩由系统自动统计，避免人工计算错误。

3.对总成绩前 30%参赛选手成绩全部复核，其余成绩抽检比例不低于 15%。

4.成绩公示期间接受参赛单位统一复核申请，确保公平公正。

5. 技能管理与沟通

5.1 专家组

技能专家组由首席专家、副首席专家和专家成员组成，负责共同进一步修订本赛项相关技术文件等。首席专家所在单位不能选派参赛队伍参加本赛项。

5.2 裁判组

金砖国家职业技能大赛实行“首席专家负责制”，即首席专家可以兼任裁判长。裁判组成员从全国非参赛院校、企业专家中遴选具备丰富教学与实操经验的人员，经

专家组统一培训、评估合格后参与执裁，严格执行回避制度。裁判组按职责分为加密裁判、线上巡考裁判、评分裁判，各司其职、互不兼任，全程接受仲裁组监督。

5.3 仲裁组

仲裁组由第三方监督人员组成，全程监督裁判工作、成绩抽检复核，受理参赛队伍书面申诉并组织复议，对赛事过程中的违规行为进行核查与处置，保障赛事公平公正。

5.4 技术支持组

由技术支持单位相关技术人员、平台供应商技术骨干组成，全程负责竞赛平台保障、设备调试、故障处理、技术答疑，确保竞赛系统稳定、安全、顺畅运行。

5.5 赛项执行工作组

由金砖国家职业技能大赛中方组织单位、执行承办单位、协办单位、技术支持单位等工作人员组成，承接赛项执行各项工作，负责赛事组织、培训实施、宣传推广、成绩统计、后勤统筹等全流程执行，确保赛事按计划推进。

5.6 官方沟通交流

比赛前有关报名参赛、软硬件准备、考试环境部署等相关疑问，参赛单位可进入“2026 金砖网络安全赛项交流群”（QQ 群：565864284）进行沟通讨论。本赛项的训练交流，比赛前，比赛中以及比赛后交流等也可通过官方交流群进行。

注意：请各参赛单位谨慎甄别群内信息出处，谨防诈骗。

6. 竞赛材料和设备

6.1 基础设施列表

基础设施清单详细列出了参赛方参赛所需要的设备和设施，见“2026 金砖国家职

业技能大赛网络安全赛项基础设施清单”。

6.2 竞赛设备清单

1．技术平台

序号	平台名称	数量	备注
1	网络安全竞技平台	1	

2．规格参数

序号	平台名称	规格参数
1	网络安全竞技平台	一、统一平台系统： 1. 系统后端、前端均采用合规开源协议的稳定技术栈构建，所有组件均完成安全加固，运用“扁平化、响应式”设计思路，无缝适应电脑、平板、手机等多类型终端； 2.平台首页可以展示服务器性能占用情况，至少包含 cpu、内存、磁盘、在线人数、启动时间等信息； 3.为保证系统及账号的安全性，账号登陆界面使用验证码进行验证，验证码两分钟更新； 4.系统采用浏览器 session 会话的保持，且管理员及教师账号可以看见在线的用户情况； 5.系统支持教师学生账号的批量导入并支持重置密码功能； 6.系统支持角色管理，可以为不同角色用户分配不同的菜单权限； 7.系统支持参数设置，可以修改账号的初始密码、开关验证

		码、密码最大错误次数及密码错误锁定时间等功能； 8.系统支持日志管理，可以查看用户的登录情况及登录系统后的操作情况，日志里至少包含用户名、操作地址、操作地点、浏览器、操作系统等信息； 9.系统支持访问控制，可以限制某些 IP 可以访问平台，某些 IP 不可访问平台； 10. 所有功能模块及配套组件需在统一平台系统内实现。 二、技能测评模块： 1.系统支持考试功能，支持单选、多选、判断、简答类型的试题； 2.系统支持防切屏功能，可以设置防切屏次数； 3.系统支持试题的一键导入与一键导出功能； 4.试题题目及试题答案支持上传多张图片； 5.创建的试卷可以对用户完全公开，也可以单独下发给部分用户； 6.系统采用客观题自动评分，主观题人工评分的方式； 7.系统的考试界面支持考试倒计时功能，倒计时结束自动保存答案交卷 ； 8.系统的考试界面显示作答与未作答的题目，可以选择对应的题目作答； 9.学生误交卷时，教师可以让此学生重新作答试卷。

		三、技术规划模块： 1.系统采用 B/S 架构，用户修改创建的图纸都保存在服务器上； 2.管理员账号可以查看并修改用户绘制的图纸，可以一键清除所有用户创建的图纸； 3.系统支持拓扑图、机架图及楼宇平面图的绘制； 4.系统支持绘制的图纸一键导出图片； 5.系统支持图片的导入； 6.系统支持设备物料清单的自定义导入，支持通过模板的方式一键导入； 7.管理员账号可以查看并修改用户创建的设备物料清单； 8.用户选用的设备物料清单支持一键导出表格； 9.管理员可以单独清除用户某个清单或者一键清除所有清单； 10. 为更好的选择网络设备与集成物料，可以根据产品型号、名称等条件进行筛选。 四、配套网络仿真实训组件： 1.融合 Dynamips、IOL、QEMU/KVM、Docker 虚拟化引擎，支持 Intel VT-x/AMD-V 硬件辅助虚拟化加速，适配国产 x86 架构服务器，保障多节点并行运行的稳定性与运行效率；

		2. 平台提供标准化镜像适配能力，支持用户自行导入设备镜像，平台保障镜像正常运行的适配环境； 3.支持国产统信、麒麟等主流国产操作系统，及 Windows、Linux 主流 x86 操作系统虚拟机运行，内置 Docker 容器引擎，可部署 DNS、DHCP、Web 服务、测试工具等轻量级容器化节点，有效降低平台运行资源占用； 4.提供可视化拖拽式拓扑编辑器，支持画布缩放、节点批量操作、链路属性自定义标注；具备热连接功能，可在设备运行状态下实时增删修改链路连接，无需重启设备节点； 5.具备完整的实验全生命周期管理能力，支持为同一拓扑保存多套独立的设备启动配置，可快速切换不同实验场景，支持多套实验拓扑并行运行，各实验环境完全隔离、互不干扰； 6.具备网络链路质量仿真能力，可针对拓扑内任意链路自定义带宽、单向 / 双向时延、抖动、丢包率，精准模拟广域网、弱网等各类真实网络环境，验证网络协议与业务系统的环境适配性； 7.支持虚拟网络与物理网络无缝打通，提供桥接、NAT 等多种网络接入模式 8.内置 HTML5 Telnet/SSH 命令行控制台与 VNC 图形化控制台，无需第三方终端工具，浏览器内即可批量打开多设备并行控制台会话，完成设备配置与调试操作；

		9.内置在线流量抓包分析工具，支持对拓扑内链路、设备接口进行实时抓包，可完整解析二层至七层网络数据包，无需安装本地抓包软件，实现配置调试与流量排障无缝衔接； 10.支持多用户并发访问，提供精细化角色与权限管理体系，可针对不同用户 / 角色分配功能权限、CPU / 内存 / 硬盘资源配额。

6.3参赛侧设备与环境要求

1.必备设备

作答主机 2 台：使用 Windows10 及以上 64 位系统，具备内置或外接摄像头、麦克风、扬声器，CPU 等同于酷睿 i5 及以上，内存 8G 及以上，屏幕分辨率不低于 1920×1080 的计算机；安装指定浏览器与监考客户端。

监控辅机 2 台：具备内置或外接摄像头、麦克风、扬声器的智能设备，用于两机位多面监控，全程拍摄选手作答画面与手部动作。

稳定网络：上下行带宽不低于 10Mbps，推荐有线网络连接，避免竞赛中断。

2.环境要求

独立、封闭、安静的空间，光线充足，无逆光、背光；

桌面仅保留作答设备、电源、鼠标键盘，不得摆放任何纸质资料、电子设备、书籍等；

竞赛全程无其他人员进入监控范围。

3.禁止使用的材料与设备

纸质资料、笔记、书籍等任何参考材料；

手机、智能手表、蓝牙耳机等通讯与智能穿戴设备；

U 盘、移动硬盘等外接存储设备；

远程控制软件、即时通讯工具、搜索类工具等与竞赛无关的程序；

多台辅助电脑、计算器等其他电子设备。

6.4 线上参赛环境规范

主机摄像头正对选手面部，全程清晰拍摄人脸，不得佩戴口罩、帽子、墨镜等遮挡面部的物品；

辅机位放置于选手侧后方 45° 位置，高度约 1.5 米，画面需覆盖选手全身、作答电脑屏幕与桌面区域；

竞赛全程不得关闭摄像头、麦克风，不得切换监控画面角度；

选手需提前30分钟完成设备调试与环境检查，确保设备、网络、监控均正常。

7. 竞赛试题

专家组在正式比赛前一个月左右在大赛官方网站

（http://www.brskills.com/jzzy/productjs2026.html）发布竞赛样题，样题题型与正式比赛题型内容约 70%一致，赛题思路约 80%一致。

8. 申诉与仲裁

1.参赛队对竞赛过程、监考判罚、评分结果有异议的，均可提出申诉。

2.申诉需在当前场次比赛结束后 2 小时内，由参赛队领队通过官方指定邮箱或竞赛平台申诉通道提交书面申诉材料，材料需明确申诉事项、事实依据与佐证截图/录屏片段。

3.仲裁组要认真负责地受理选手申诉，并将书面处理意见通知当事人领队。

4.仲裁组的裁决为最终裁决。

9. 竞赛须知

（一）选手须知

1.参赛选手应按有关要求如实填报个人信息，赛前按要求完成身份核验与环境测试，信息不实或环境不达标者取消参赛资格。

2.竞赛开始前 30 分钟，凭参赛账号登录竞赛平台与监考系统，完成人脸核验与环境检查，等候开赛指令。

3.全程独立作答，禁止任何人员进入参赛空间，禁止以任何形式与他人交流试题与答案。

4.全程开启双机位监控与屏幕共享，不得遮挡摄像头、脱离监控范围，不得擅自关闭监考程序。

5.禁止携带违禁资料、电子设备、通讯工具进入参赛区域；禁止运行与竞赛无关的软件。

6.竞赛全程启用防切屏机制，未经允许不得切换作答界面，违规次数达到阈值按作弊处理。

7.竞赛时间截止后平台自动收卷，须立即停止操作。

8.所有结果通过竞赛平台线上提交，禁止以任何形式外传赛题、作答截图与录屏。

9.竞赛结束后，按指令有序退出平台与监考系统。

10.未尽事宜，由赛事裁判组裁决。

（二）指导专家须知

1.指导专家（教师）应该根据专业教学计划和赛项规程合理制定训练方案，认真

指导选手训练，培养选手的综合职业能力和良好的职业素养，克服功利化思想，避免为赛而学、以赛代学。

2.指导专家（教师）应及时查看大赛专题网站有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

3.指导专家（教师）应该根据赛项规程要求做好参赛选手保险办理工作，并积极做好选手的安全教育。

4.竞赛期间，不得进入选手参赛房间，不得以任何形式远程协助答题，不得通过通讯工具传递试题、答案相关信息。

5.参赛代表队若对竞赛过程有异议，在规定时间内由领队向赛项仲裁工作组提出书面报告。

6.对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或对处理意见不服从而停止比赛，否则以弃权处理。

10. 竞赛表彰

（一）证书发放

参赛队伍可获得由印度主办方及中方组织方共同签发的获奖证书。

（二）省级/区域选拔赛奖励办法（非省厅牵头组织的省级或区域选拔赛）

以省级/区域实际参赛队比赛成绩为依据，设一等奖占比 10%，二等奖占比 20%，三等奖占比 30%，其他为优秀奖。按获奖等级赛后由印度主办方及中方组织方共同签发选拔赛电子版国际获奖证书。

（三）国际总决赛奖励办法

1. 金牌、银牌、铜牌和优胜奖牌

金砖+国家参赛队统一排名，对获得前 6 名的国内外参赛队，相应颁发金、银、铜牌及证书；对未获得金银铜奖牌但成绩优异的线下参赛队颁发优胜奖奖牌及证书（上限为 3 支队伍）。

奖牌评奖细则如下：

（1）各参赛国成绩排名第一的本国参赛队有资格进入金牌排名，成绩排名第一的参赛队得金牌；

（2）除金牌参赛队外，各参赛国成绩最好的一支本国参赛队有资格进入银牌排名，其中成绩最好的前两支参赛队获得银牌；

（3）除金牌参赛队和银牌参赛队外，各参赛国成绩最好的一支本国参赛队有资格进入铜牌排名，其中成绩最好的前三支参赛队获得铜牌；

（4）对未获得金银铜奖牌但成绩优异的线下参赛队颁发优胜奖奖牌（上限为 3 支队伍）；

（5）线上国际参赛队不颁发实物奖牌，只颁发相应奖牌证书。

2. 一等奖、二等奖和三等奖

对参加中国赛区国际总决赛的中方参赛队，依据四舍五入的原则，设一等奖占比 10%，二等奖占比 20%，三等奖占比 30%，颁发相应国际获奖证书。其他为优秀奖。

3.其他奖励

（1）为参与执裁的执裁裁判颁发国际执裁证书；

（2）为获得一等奖、二等奖队伍的指导专家颁发国际优秀指导专家证书；

（3）为组织大赛作出突出贡献的单位颁发“突出贡献奖”牌匾及证书；

（4）为积极组织参赛、开展赛前选拔集训、赛中未发生违规违纪行为的省级或区域选拔赛承办单位颁发“优秀组织奖”证书。

4. 技能护照

参赛队总成绩达到 60 分（100 分制）及以上的参赛选手，可以自愿申领 A 级“技能护照”证书（详见后续申领通知）。

11. 违规处理规定

为严肃竞赛纪律，保证竞赛进程的公开、公平、公正，对违反比赛纪律的人员作如下处理：

1．发现参赛队不符合报名规定条件的、冒名顶替和弄虚作假的，报经竞赛办公室核实后，取消该参赛队比赛资格；已获奖者取消其获奖资格，责令其退回所获证书及奖品，并通过媒体向社会公布。

2．参赛选手有下列情节之一的，竞赛成绩记零分：

(1)考试期间违规翻阅书籍、笔记、纸条等资料；

(2)竞赛期间未报备脱离监控范围、有无关人员进入参赛区域的；

(3)借助远程协助、代答、场外提示等方式作弊的；

(4)故意关闭、遮挡监控设备，或篡改、绕过监考系统的；

(5)切屏次数超出规定阈值，或擅自打开无关软件的；

(6)扰乱线上竞赛秩序，辱骂裁判、工作人员或其他参赛选手的；

(7)私自传播、泄露赛题内容或作答内容的；

(8)其他违反比赛规则不听劝告。

3．参赛选手不得对竞赛支撑系统与相关资源进行任何形式的网络攻击、漏洞探

测、篡改或未授权访问等，包括但不限于攻击赛场管理平台、横向渗透其他参赛队环境、传播恶意代码等，一经发现取消参赛资格，追究相关单位与人员责任；造成损失的，由当事人单位承担赔偿责任（视情节而定），情节严重的，依法送有关机关处理。

4．对于违反纪律的各代表队非参赛人员，将视情节轻重给予警告、通报批评，并视情节轻重，由大赛组织委员会决定是否通报其所在单位。

5．对违反竞赛纪律的裁判员、工作人员，裁判长报经省竞赛组委会核实后，视情节轻重给予警告或取消其资格。

6．选手参加比赛前，应进行安全检查，如发现问题应及时解决，无法解决的问题应及时向裁判报告，裁判视情况予以判定，并协调处理。准备工作完毕后报裁判批准，方可进行实际操作。对选手未发现的安全隐患，裁判应及时指出并酌情扣除选手实际操作分。