

第七届淮安技能状元大赛网络安全 (职工组) 项目技术文件

第七届淮安技能状元大赛组委会技术工作组
2026年10月

目录

一、技术描述

- (一) 项目概要.....1
- (二) 基本知识与能力要求..... 1

二、试题与评判标准

- (一) 试题内容.....3
- (二) 评判标准.....6

三、竞赛细则

- (一) 裁判员分组和职责.....6
- (二) 赛场管理制度.....6
- (三) 技术违规处理.....8

四、竞赛场地、设施设备等安排

- (一) 赛场规格要求.....8
- (二) 场地布局图.....8
- (三) 基础设施清单.....9

五、安全要求

- (一) 赛场人员安全要求.....10
- (二) 场地设备安全要求.....10

六、附件：样题及评分表

- (一) 试题内容.....11
- (二) 评判标准.....18

一、技术描述

（一）项目概要

本项目以《网络与信息安全管理员》国家职业技能标准（2020 年版）中三级/高级工（网络安全管理员、信息安全管理员）的技能要求和相关知识要求，以及网络安全相关国家职业标准（高级工及以上级别）为依据，参照第八届江苏技能状元大赛技术文件体例，结合淮安市电子信息、智慧产业等重点产业链人才需求制定竞赛内容与评判标准。

竞赛以单人赛方式进行，设职工组。本赛项不设理论知识考试（不命题理论试卷），全部竞赛内容均为技能操作考核，重点考核选手在网络与信息安全防护、网络与信息安全管理、网络与信息的安全处置三大职业功能上的综合实操能力，包括：网络设备（交换机、路由器）安全加固与路由部署、边界防护设备（防火墙）安全策略与地址转换部署、VPN 安全互联部署、网络故障分析与排除、Web 应用漏洞识别与利用（CTF 攻防实操）及安全事件处置，以及职业素养与操作规范。

竞赛网络设备采用华为 eNSP 模拟器（Enterprise Network Simulation Platform）仿真实现，设备类型包括路由器（AR2200/AR1220 系列）、交换机（S5700/S3700 系列）与防火墙（USG6000v），命令体系为华为 VRP；CTF 考核采用国产化 CTF 竞赛平台，为每位选手动态分发独立的容器化靶机环境。竞赛总时长 240 分钟，满分 100 分。

（二）基本知识与能力要求

本竞赛是对网络安全项目相关技能的展示与评判，选手须掌握操作所必备的理论知识，具备相应的技能水平。选手应具备的知识与能力要求及权重比例见下表。

相关要求	权重比例 (%)	基本知识	工作能力
1 职业素养	5	熟悉健康与安全法规、安全用电知识； 了解《网络安全法》《数据安全法》	能遵守安全规程、规范操作设备； 能正确使用工具与仪表，保持工位

		《个人信息保护法》《密码法》等法律法规；理解网络安全等级保护 2.0 基本要求；了解职业道德与职业守则、竞赛纪律“三个禁止”要求。	整洁；具备风险识别与应急处理能力；诚实守信，提交的文档、截图与命令行中不出现任何个人信息。
2 路由交换与接入安全部署	30	掌握 VLAN、Access/Trunk/Hybrid 端口、STP/RSTP/MSTP、链路聚合等交换技术；掌握端口安全、MAC 地址绑定、DHCP Snooping 等接入安全机制；掌握 IPv4/IPv6 地址规划、静态路由、RIP、OSPF、IS-IS、BGP 基本原理；掌握 ACL、路由策略与流量控制；了解 VRRP、BFD 等可靠性技术与 WLAN 组网架构。	能在华为 eNSP 中对交换机（S5700/S3700）、路由器（AR 系列）进行命令行操作；能完成 VLAN 划分、端口类型配置与端口安全 MAC 绑定；能配置扩展 ACL 限制服务器端口访问；能部署 OSPF 等路由协议实现总部与分支网段互通；能配置静态路由与默认路由；能排查二层、三层配置错误。
3 边界防护与 VPN 安全部署	25	掌握防火墙安全区域与安全策略、状态检测机制；掌握源 NAT（NAPT、地址池、Easy IP）与目的 NAT（NAT Server）原理；掌握 IPsec VPN 体系（AH/ESP、IKE、SA、预共享密钥）与 SSL VPN 原理；了解入侵防御（IPS）、黑名单/白名单、日志审计；了解对称加密、非对称加密、哈希算法与国密算法。	能在 eNSP 中配置防火墙（USG6000v）安全区域并规划安全策略；能配置源 NAT 地址池实现内网访问公网；能配置 NAT Server 发布内网服务器；能配置 IPsec VPN 实现站点间安全互联；能配置黑白名单与入侵防护；能验证 NAT 与 VPN 结果并排查故障。
4 网络故障分析与安全处置	15	掌握网络故障排查的分层法、分段法、对比法、替换法；掌握 ping、tracert、display vlan、display ip routing-table、display ospf peer 等诊断命令；了解 ARP 欺骗、拒绝服务、端口扫描等常见威胁及防范；了解安全事件监控、阻断、日志留存与上报流程。	能依据故障现象定位园区网内、园区网间故障点；能识别并修正 VLAN/Trunk、端口安全、ACL、路由、NAT、安全策略、IPsec 参数等错误配置；能恢复业务互通并留存验证截图；能规范填写故障原因、处置方法与配置记录。
5 CTF 安全攻防与漏洞处置	25	掌握 Web 应用常见漏洞（弱口令、文件上传、SQL 注入、反序列化、远程代码执行等）原理与危害；掌握端口扫描、服务识别、目录爆破等信息收集方法；了解 OWASP Top 10 与主流框架漏洞（ThinkPHP、Fastjson、Log4j2 等）特征；了解渗透测试授权边界、日志留存与痕迹清理规范；了解《网络安全法》等关于不得非法侵入他人网络的禁止性规定。	能在授权靶机上使用扫描与抓包工具识别开放端口与服务；能识别并利用文件上传等 Web 漏洞获取 Flag；能复现主流框架漏洞并读取敏感文件获取 Flag；能按规范提交 Flag；能清理操作痕迹与日志、复位靶机环境。
合计	100		

二、试题与评判标准

（一）试题内容

1.基本内容

本赛项为技能操作考核，不设理论知识考试。参赛选手依据赛场提供的任务书（赛题）、拓扑图与设备命令手册，在华为 eNSP 模拟器中完成网络设备的配置部署与故障排除，在 CTF 竞赛平台上完成 Web 安全与基础渗透实操任务，具体完成以下模块任务。

模块编号	模块名称	考核内容	时长(分钟)	分值	权重
A	路由交换与接入安全部署	VLAN 与端口安全、三层互通、OSPF 路由部署、扩展 ACL 服务器防护、广域网路由与全网互通	80	30	30%
B	边界防护与 VPN 安全部署	防火墙安全区域与安全策略、源 NAT 地址池、目的 NAT (NAT Server)、IPsec VPN 站点互联	60	25	25%
C	网络故障分析与排除	园区网内网间故障现象自查、故障定位、错误配置修正与业务恢复验证	40	15	15%
D	CTF 安全攻防实操	信息收集与端口扫描、Web 漏洞利用（文件上传等）、主流漏洞复现（框架 RCE 等）、Flag 提交与痕迹清理	60	25	25%
E	职业素养与操作规范	安全用电、规范操作、工位整洁、诚实守信与信息安全，贯穿竞赛全程	贯穿全程	5	5%
合计			240	100	100%

2.设备与平台

（1）竞赛网络设备以华为 eNSP 模拟器内置的路由器（AR2200/AR1220 系列）、交换机（S5700/S3700 系列）、防火墙（USG6000v）为准，命令体系为华为 VRP；同一场次 eNSP 软件版本与设备镜像版本保持一致。

（2）赛场在每台竞赛终端部署华为 eNSP 模拟器，实现设备仿真、拓扑搭建、配置保存与结果采集；竞赛拓扑与初始配置由赛场统一提供并导入，选手不得擅自修改设备型号与拓扑连接。

（3）CTF 考核采用国产化 CTF 竞赛平台（GZ::CTF），为每位选手动态分发独立的容器化靶机，支持动态 Flag 生成、提交校验、实时计分与作弊检测；靶机仅限

赛场分配的授权目标。

（4）考试电脑提供华为设备产品文档（命令手册）及赛场指定的 CTF 工具集供查阅与使用，禁止使用搜索引擎及其他求助方式。

（5）选手须将关键配置命令、状态信息与验证结果截图，以及 CTF 模块的操作过程截图与 Flag 提交结果截图填入 Word 版答题文件并上传至竞赛服务器；模块 D 的 Flag 须同时在 CTF 平台提交。

3.样题及赛题变化

本赛项属于赛前提前公布样题的项目，样题随本技术文件一并公布（见第六部分附件），包含网络设备配置模块与 CTF 模块样题。竞赛前 2 天，裁判长结合赛场的设施设备、工具、平台等实际情况，对已公布的样题提出不超过 30%的更改方案（可包括 CTF 题目的等量替换、靶机环境与参数调整），修改确定后当日当场打印封存；封存的试题在比赛当天拆封并向选手正式公布。本赛项不命制理论试卷与理论题库。

4.成果提交与注意事项

（1）模块 A、模块 B 将关键配置命令、状态信息与验证结果截图保存至答题文件；模块 C 将故障现象、原因分析与正确配置截图保存至答题文件；模块 D 将信息收集、漏洞利用、漏洞复现的操作过程截图与 Flag 提交结果截图保存至答题文件。

（2）考试时间结束后停止编写答题文件，并将保存后的答题文件上传至竞赛服务器。

（3）提交的文档、截图、命令行中不得出现工位号、姓名、单位等个人信息，否则本模块成绩按零分处理。单位

（4）严格落实省人社厅关于严明职业技能竞赛纪律“三个禁止”的要求，竞赛不向选手和参赛单位收取任何费用。

（5）模块 D 的 Flag 须在 CTF 平台同步提交并以平台记录为计分依据；答题文件截图与平台提交记录不一致或未在平台提交的，该处 Flag 不予计分。

（二）评判标准

1.竞赛试题配分

本赛项采用 100 分制，各模块配分与评价方式见下表。

模块编号	模块名称	评价分	测量分	总计	评价方式
A	路由交换与接入安全部署	0	30	30	测量
B	边界防护与 VPN 安全部署	0	25	25	测量
C	网络故障分析与排除	0	15	15	测量
D	CTF 安全攻防实操	0	25	25	测量
E	职业素养与操作规范	5	0	5	评价
总计		5	95	100	

2.成绩计算方式

本项目采用 100 分制，各个评分项的分数应精确到小数点后一位，各模块原始成绩直接相加即为参赛选手最终竞赛成绩。

3.评判方法

（1）竞赛设立裁判组，每个机房设现场裁判 3 名（1 名裁判长、2 名裁判员）或 5 名裁判员，依据评分表对参赛选手的操作规范、完成质量与现场表现进行评分，采取过程评判与结果评判相结合的方式；模块 D 以 CTF 平台提交记录与答题文件截图共同确认。

（2）测量评分（客观）：凡可采用客观数据表述的评判称为测量。测量评分时每个评分项除非另有说明，只能给予满分或 0 分；如需使用 0 分到满分之间的分数，该项中应有清晰的解释说明。测量分以功能结果与关键配置为准，命令名称、视图与参数正确即可得分；命令缩写、序号取值不同但功能等效的不扣分。

（3）评价评分（主观）：每个评价分评分项由不少于 2 名裁判为一组，裁判各自单独评分，再取平均值计算出实际得分，分数精确到小数点后 2 位，四舍五入。

（4）评分过程中允许选手在不修改配置的前提下按裁判指令展示功能与运行结果；进行测量评分时每项最多运行评判 2 次。

4.成绩并列

按比赛总成绩从高到低排列参赛选手名次。如遇总成绩相同，则依次按模块 A、模块 B、模块 C、模块 D 成绩高低排序；如仍相同，以模块 A 完成时间短者为优；

如仍相同，以 CTF 平台记录最后一处 Flag 提交时间早者为优。

三、竞赛细则

本赛项竞赛内容在同一场次内完成，竞赛总时长 240 分钟，其中模块 A、模块 B、模块 C 在华为 eNSP 模拟器中完成，模块 D 在 CTF 竞赛平台上完成。参赛选手在规定时间内，根据赛场提供的任务书（赛题）、拓扑图与设备命令手册，以现场技能操作方式完成全部模块任务。

（一）裁判员分组和职责

本次竞赛设立裁判组，裁判组由裁判长 1 名、2 名裁判员组成。裁判长负责组织全体裁判员培训、试题确认与成绩审核；裁判长助理协助裁判长开展工作；现场裁判负责现场执裁、过程记录与评分，其中模块 D 成绩以 CTF 平台提交记录与答题文件截图共同确认。人员配备与职责见下表。

序号	岗位	人数	主要职责
1	现场裁判(1 名裁判长,2 名裁判员)	3 人	现场执裁、过程记录、评分与结果确认
2	现场技术人员（竞赛技术人员）	2 人	eNSP 模拟器与 CTF 平台保障、设备与环境故障处置
3	质量督导人员	1 人	竞赛纪律与流程监督
4	场外配备人员	2 人	检录、引导与场外保障
5	技术保障人员	2 人	网络、供电与终端保障（含 CTF 靶机服务器）
6	安保人员	1 人	赛场秩序与安全保卫
7	CTF 平台技术人员	2 人	靶机容器分发、动态 Flag 校验、平台运维与应急处置

（二）赛场管理制度

1.竞赛流程：推荐抽签不分组，所有选手同时比赛；选手工位与裁判人员安排通过抽签决定。

2.检录与入场：选手须持有效证件按时检录，签署诚信参赛承诺书，接受身份核验；迟到超过规定时间不得入场。

3.工位管理：每位选手 1 个工位，共设 30 个正式工位与 10 个备用工位，无需候

考室；选手不得擅自更换工位或调换设备。

4.设备与资料：竞赛终端提供华为设备命令手册（电子版）供查阅，模块 E 可使用赛场指定的工具集；严禁使用搜索引擎、外部存储设备、通讯工具及其他求助方式；严禁对赛场网络设备、服务器及其他选手靶机等非授权目标发起扫描、爆破与攻击。

5.过程管理：答题过程中遇电脑、平台或设备异常，应举手示意并联系监考老师或技术人员处理，不得自行处置。

6.成果提交：选手须在规定时间内将答题文件保存并上传至竞赛服务器，提交后通报裁判，签名确认完成，并接受裁判检查。

7.成绩管理：成绩记入《网络安全项目竞赛成绩汇总表》，由裁判组签字确认，竞赛全过程接受质量督导；竞赛不收取任何参赛费用。

8.选手管理：入围选手进入市级集训队，实行动态管理，择优推荐参加省级竞赛及第八届江苏技能状元大赛相关赛项选拔。

（三）技术违规处理

1.选手携带通讯、存储、拍照录像等违禁设备或资料进入工位，或在竞赛中使用搜索引擎及外部求助方式的，由裁判长视情节给予警告、扣分直至取消本模块成绩的处理。

2.提交的答题文件、截图、命令行中出现工位号、姓名、院校等个人信息的，本模块成绩按零分处理。

3.选手擅自更换工位、调换设备、干扰他人竞赛或破坏赛场设施设备的，取消本模块成绩；情节严重的，取消竞赛资格并报大赛组委会处理。

4.竞赛期间发生安全事故或违规用电行为的，立即终止其竞赛，并按赛场安全预案处置。

5.因设备或平台故障导致竞赛中断的，由裁判长与技术人员确认后按赛场应急预案处理，不另行补时的，须由裁判组集体研究决定并记录在案。

6.选手对评判结果有异议的，应在成绩公布后规定时间内向质量督导人员提出书

面申诉，由大赛组委会技术部按程序复核答复；涉及模块 E 成绩的，可调取 CTF 平台提交日志核查。

7.模块 D 中选手超出本人授权靶机范围操作，对赛场网络设备、服务器或其他选手靶机发起扫描、爆破与攻击，或篡改平台数据与提交记录的，取消本模块成绩；情节严重的，取消竞赛资格并报大赛组委会处理。

四、竞赛场地、设施设备等安排

（一）赛场规格要求

竞赛场地由承办单位申报、大赛组委会确定，须满足 40 个工位、100M 带宽、双路供电、网络安全隔离与 CTF 平台服务器部署要求。具体要求见下表。

项目	规格要求
工位数量	30 个正式工位+10 个备用工位，共 40 个；每位选手 1 个工位
工位面积	每个工位使用面积不小于 2.5 平方米，工位间隔不小于 0.8 米
网络条件	竞赛网络带宽不低于 100M，与互联网安全隔离，具备独立的竞赛 VLAN 与访问控制
终端与平台要求	竞赛终端可稳定运行华为 eNSP 与 CTF 平台客户端，与 eNSP 仿真设备、CTF 靶机服务器网络互通，竞赛网络与互联网安全隔离
供电要求	双路供电并配备 UPS 不间断电源，每工位不少于 2 个三孔插座，供电可靠接地
照明与环境	照度不低于 300lx，通风良好，温度适宜，噪声符合机房标准
消防安全	配备灭火器、应急照明与疏散指示，安全通道畅通，符合消防规范
功能分区	设置竞赛区、裁判工作区、技术支持区、检录区与设备（配电）间，分区明确

（二）场地布局图

赛场按功能分区布置，竞赛区工位呈矩阵排列，主通道居中贯通，裁判区与技术支持区就近设置，检录区设于入口处。场地布局示意如下。

检录与身份核验区	技术支持与设备（配电）间	消防与安全保障区
竞赛区（工位 01—15）	主通道	竞赛区（工位 16—30）
竞赛区（备用工位 31—40）	主通道	监控与质量督导区

裁判区（成绩录入与复核）	主通道	答题文件与 CTF 平台服务器区
--------------	-----	------------------

说明：实际布局以承办单位申报并经大赛组委会确认的赛场平面图为准；竞赛区工位须保证间距与疏散通道符合要求。

（三）基础设施清单

赛场按 40 个工位配置，主要基础设施清单见下表（网络设备仿真以华为 eNSP 模拟器为准，CTF 考核以国产化 CTF 竞赛平台为准，同场次软件版本与设备镜像版本保持一致）。

序号	名称	规格要求	数量	备注
1	竞赛终端（PC）	CPU i5 及以上（建议 i7）、内存 16GB 及以上、硬盘 512GB 及以上，Windows 10 64 位操作系统，安装华为 eNSP（含 VirtualBox、Wireshark、WinPcap）、CTF 平台客户端、Office、终端仿真软件与浏览器	41 台	含备用 1 台
2	华为 eNSP 模拟器及设备镜像	eNSP 1.3.100 及以上版本，含 AR2200/AR1220 路由器、S5700/S3700 交换机、USG6000v 防火墙设备镜像，支持拓扑搭建、配置保存与结果采集	1 套	每台终端部署，版本一致
3	局域网接入交换机	24 口千兆以太网交换机（物理设备，用于组建竞赛局域网）	按工位配置	支持 VLAN 划分与端口隔离
4	CTF 竞赛平台	国产化 CTF 竞赛平台（GZ::CTF），支持动态容器靶机分发、动态 Flag、提交校验、实时计分与作弊检测	1 套	含平台服务器（8 核 16G 以上）
5	CTF 靶机服务器	支持 Docker 容器化靶机动态分发、资源限制与答题结束后自动销毁	1 台	可与平台服务器合并部署
6	答题文件服务器	支持答题文件上传与集中存储，具备访问控制与备份	1 台	FTP/HTTP 方式
7	华为设备命令手册	华为 VRP 配置命令手册（路由器、交换机、防火墙，电子版）	1 套	随平台提供给选手
8	网络线缆	超五类及以上网线等	若干	按工位与赛场网络配置
9	UPS 与配电设施	双路供电、UPS 不间断电源、可靠接地	1 套	满足 40 工位供电
10	监控与消防设施	视频监控、灭火器、应急照明、疏散指示	1 套	覆盖竞赛区与关键区域

五、安全要求

（一）赛场人员安全要求

1.选手须签署诚信参赛承诺书与安全承诺书，严格遵守赛场安全规程与设备操作规程，服从裁判与工作人员管理。

2.竞赛期间严禁携带易燃易爆、有毒有害及其他危险物品进入赛场；严禁在工位内饮食、吸烟。

3.安全用电：严禁私拉乱接电源线，严禁湿手接触电气设备与插座；发现设备冒烟、异味、漏电等异常，应立即断电并举手报告。

4.选手应熟悉赛场安全通道与应急疏散路线，发生火灾或其他紧急情况时，按应急预案有序撤离，不得拥挤、滞留。

5.注意操作卫生与劳逸结合，避免长时间连续操作导致视觉疲劳与身体不适；发生人身伤害时，由赛场医疗保障人员按预案处置。

6.现场裁判、技术人员须佩戴身份标识，选手不得擅自进入技术支持区、配电间等非竞赛区域。

（二）场地设备安全要求

1.所有网络设备、服务器与终端须可靠接地，配置 UPS 不间断电源与防雷、防静电措施，避免电压波动与静电损坏设备。

2.竞赛网络与互联网安全隔离，边界部署访问控制，严禁利用竞赛设备对外发起扫描、攻击等任何危害网络安全的行为；CTF 靶机仅限选手本人授权使用，严禁扫描、访问其他选手靶机、赛场服务器等非授权目标，平台须留存操作与提交日志备查。

3.eNSP 仿真环境、CTF 平台与答题文件服务器须设置分级账号与访问权限，定时备份竞赛数据与平台日志，防止数据丢失与泄露。

4.设备上电、下电须由技术人员按规程操作，严禁选手带电插拔设备模块与线缆；eNSP 拓扑文件与 CTF 靶机由赛场统一导入与回收，严禁选手私自拷贝、外传。

5.竞赛产生的配置数据、截图与成绩数据须妥善保存，成绩数据实行双人复核，赛后按档案管理规定留存。

6.赛场须配备足量消防器材并定期检查，电气设备与线路须符合安全规范，赛前由安全保障人员进行全面检查并签字确认。

六、附件：样题及评分表

（一）试题内容

第七届淮安市技能状元大赛“网络安全”项目技能考核试卷（样题）

考试说明

1.本试卷依据《第七届淮安市技能状元大赛"网络安全"项目技术文件》命制，考核内容与技术文件第二部分完全一致；本赛项不设理论知识考试。

2.竞赛总时长 240 分钟，其中模块 A 路由交换与接入安全部署 80 分钟、模块 B 边界防护与 VPN 安全部署 60 分钟、模块 C 网络故障分析与排除 40 分钟、模块 E CTF 安全攻防实操 60 分钟；模块 D 职业素养与操作规范由裁判依据选手现场表现评定。

3.网络设备采用华为 eNSP 模拟器仿真，路由器为 AR2200/AR1220 系列、交换机为 S5700/S3700 系列、防火墙为 USG6000v，命令体系为华为 VRP；命令名称、视图与参数正确、功能等效即可。模块 E 在赛场 CTF 竞赛平台上完成，靶机环境、工具集与账号由赛场统一提供。

4.考试电脑提供华为设备产品文档（命令手册）及赛场指定的 CTF 工具集供查阅与使用，禁止使用搜索引擎及其他求助方式。

5.选手须将关键配置命令、状态信息与验证结果截图，以及模块 E 的操作过程与 Flag 提交结果截图填入 Word 版答题文件并上传至竞赛服务器；模块 E 的 Flag 须同时在 CTF 平台提交。

6.提交的文档、截图、命令行中不得出现工位号、姓名、单位等个人信息，否则本模块成绩按零分处理。

7.考试过程中遇电脑、平台或设备异常，应举手示意并联系监考老师或技术人员处理。

8.模块 E 的操作范围仅限平台分配给本人的靶机，严禁对赛场网络设备、服务器及其他选手靶机等非授权目标发起扫描、爆破与攻击，违者本模块成绩按零分处理。

模块 A 路由交换与接入安全部署（80 分钟，30 分）

[拓扑描述]

集团企业总部与分支机构通过运营商网络连接。总部部署接入交换机 SW1、出口路由器 R1 与 R2；总部通过 SW1 接入 PC1、PC2 与服务器 SERVER；分支机构部署路由器 R5 与 PC3；运营商网络部署路由器 R3、R4。本模块在华为 eNSP 模拟器中完成：SW1 使用 S5700 交换机，R1—R5 使用 AR2220 路由器（或赛场指定型号），终端与服务器使用 eNSP 中的 PC、Client、Server 设备模拟；拓扑文件与初始配置由赛场统一下发。

[网络介绍]

1.企业总部：出于安全考虑，交换机 SW1 部署 VLAN，并在连接终端的端口上配置端口安全，绑定计算机 MAC 地址，防止非法计算机接入；路由器 R1 与 R2 部署 OSPF 骨干区域，R2 部署指向运营商的静态路由，R1 部署内网网关；在 R1 上应用高级访问控制列表（ACL 3000 及以上），仅允许访问服务器 SERVER 的 TCP 443 端口，防范针对服务器的端口攻击。

2.运营商网络：路由器 R3 与 R4 完成总部与分支机构之间的路由互通（可采用静态路由或动态路由，具体以赛场任务书为准）。

3.企业分支机构：路由器 R5 部署默认路由，分支机构其他设备省略。

[任务说明]

1.二层交换与接入安全部署：在 SW1 中使用 vlan batch 命令创建 VLAN 101、VLAN 102、VLAN 109；连接 PC1 的端口配置为 Access 类型并加入 VLAN 101，连接 PC2 的端口配置为 Access 类型并加入 VLAN 102，连接 SERVER 的端口配置为 Access 类型并加入 VLAN 109，连接 R1 的端口配置为 Trunk 类型并放行 VLAN 101、102、109，使 PC1、PC2、SERVER 与 R1 互通；在连接终端的端口上启用端口安全

(port-security enable)，限制最大 MAC 地址数为 1 (port-security max-mac-num 1) 并绑定终端 MAC 地址 (port-security mac-address sticky)，违规动作配置为关闭端口 (port-security protect-action shutdown)。(11 分)

2.三层互通与路由部署：在 R1 上配置子接口 (dot1q termination vid 封装) 作为各 VLAN 网关并配置 IP 地址，开启子接口 ARP 广播功能 (arp broadcast enable)；在 R1 与 R2 上部署 OSPF 进程 1、骨干区域 Area 0 并配置 Router ID, R1 使用 network 命令 (含反掩码) 将 PC1、PC2、SERVER 所在网段及互联网段发布到 OSPF 中，使 R2 学习到相应路由。(10 分)

3.访问控制与安全加固：在 R1 上配置高级 ACL (编号 3000 及以上或命名 ACL)，仅允许访问 SERVER 的 TCP 443 端口，拒绝其他访问 SERVER 的 IP 流量，并在 SERVER 网关子接口的正确方向应用 (traffic-filter)；关闭设备不必要的服务 (如 HTTP、Telnet 等)。(5 分)

4.广域网路由与全网互通：R2 配置去往运营商网络的静态路由，R5 配置默认路由，并按任务书要求完成运营商路由器 R3、R4 的路由配置 (静态路由或动态路由)，使总部与分支机构路由可达。(4 分)

[结果要求]

1.PC1、PC2、PC3 可以互相 PING 通；

2.PC1、PC2 可以访问 SERVER 的 TCP 443 端口，其他端口访问被拒绝 (可通过 display acl 命中统计或 Client/Server 设备验证)；

3.接入非法终端时，对应交换机端口因端口安全违规被关闭 (端口进入 error-down 状态)；

4.eNSP 拓扑与配置保存完整，验证结果截图留存于答题文件。

[协商参数]

设备	接口	地址	对端设备/说明
PC1	/	172.20.11.2/30	交换机 SW1 (VLAN 101)
PC2	/	172.20.12.2/30	交换机 SW1 (VLAN 102)
SERVER	/	172.20.19.2/30	交换机 SW1 (VLAN 109)
PC3	/	172.20.13.2/30	路由器 R5

R1	GE0/0/1.101	172.20.11.1/30	SW1（VLAN 101 网关）
R1	GE0/0/1.102	172.20.12.1/30	SW1（VLAN 102 网关）
R1	GE0/0/1.109	172.20.19.1/30	SW1（VLAN 109 网关）
R1	GE0/0/2	10.21.1.1/30	路由器 R2
R2	GE0/0/1	10.21.1.2/30	路由器 R1
R2	GE0/0/2	10.21.2.1/30	路由器 R3
R3	GE0/0/2	10.21.2.2/30	路由器 R2
R3	GE0/0/3	10.21.3.1/30	路由器 R4
R4	GE0/0/3	10.21.3.2/30	路由器 R3
R4	GE0/0/2	10.21.4.1/30	路由器 R5
R5	GE0/0/1	10.21.4.2/30	路由器 R4
R5	GE0/0/2	172.20.13.1/30	PC3

模块 B 边界防护与 VPN 安全部署（60 分钟，25 分）

[拓扑描述]

企业总部与分支机构通过因特网连接。总部部署路由器 R1、防火墙 FW1 和服务 器 SERVER，分支机构部署防火墙 FW2 与路由器 R2，因特网中部署路由器 ISP 与公 网主机 PC4。本模块在华为 eNSP 模拟器中完成：FW1、FW2 使用 USG6000v 防火 墙，R1、R2 与 ISP 使用 AR 系列路由器（或赛场指定型号），拓扑文件与初始配置 由赛场统一下发，防火墙登录账号由赛场提供。

[网络介绍]

- 1.企业总部：路由器 R1 与防火墙 FW1 之间部署 OSPF 协议学习总部内网路由， FW1 部署去往因特网的缺省路由。
- 2.企业分支机构：防火墙 FW2 部署去往因特网的缺省路由。
- 3.总部与分支机构之间通过因特网部署 IPsec VPN。
- 4.防火墙配置安全区域、NAT 策略、IPsec 以及相应的安全策略；防火墙接口按 需开启 service-manage（如 ping），便于连通性验证。

[任务说明]

- 1.安全区域与安全策略部署：在 FW1 上使用 firewall zone 命令将连接路由器的 接口加入 Trust 区域、连接服务器的接口加入 DMZ 区域、连接因特网的接口加入

Untrust 区域，安全区域使用缺省优先级；配置安全策略（security-policy）使 PC1、PC2 可以访问服务器 SERVER，并放通总部与分支机构之间的 IPsec VPN 流量，未匹配安全策略的流量缺省拒绝。（9 分）

2.源 NAT 部署：在 FW1 中创建 NAT 地址池 PoolA（220.1.1.20—220.1.1.30，nat address-group），配置源 NAT 策略（nat-policy）使 PC1、PC2 使用 PoolA 中的地址访问公网主机 PC4。（6 分）

3.目的 NAT 部署：在 FW1 上部署目的 NAT（nat server），将公网地址 220.1.1.200 的 TCP 80 端口映射至内网服务器 172.20.20.2 的 TCP 80 端口，使公网主机可以通过公网地址访问服务器。（5 分）

4.IPsec VPN 部署：在 FW1 与 FW2 之间配置 IPsec VPN，包括感兴趣流 ACL、IPsec 安全提议（esp authentication-algorithm sha2-256、esp encryption-algorithm aes-128）、IKE 安全提议与 IKE 对等体（预共享密钥 Huawei@2025 或赛场指定密钥、正确配置远端与本端地址）、IPsec 安全策略，并在公网出接口引用安全策略组（ipsec policy），实现总部与分支内网安全互通。（5 分）

[结果要求]

- 1.PC1、PC2 可以 PING 通服务器 SERVER；
- 2.PC1、PC2 可以 PING 通公网主机 PC4（源地址转换为 PoolA 地址）；
- 3.PC3 通过公网地址 220.1.1.200 可以访问服务器提供的 HTTP 服务；
- 4.总部与分支内网通过 IPsec 隧道互通，PC3 可以 PING 通 PC1。

[协商参数]

设备	接口	地址	对端设备/说明
FW1	GE1/0/1	10.40.10.1/24	Trust（连接总部路由器 R1）
FW1	GE1/0/2	172.20.20.1/24	DMZ（连接服务器 172.20.20.2/24）
FW1	GE1/0/3	220.1.1.1/28	Untrust（连接因特网）
FW2	GE1/0/1	10.40.30.1/24	Trust（连接分部路由器 R2）
FW2	GE1/0/3	220.1.2.1/28	Untrust（连接因特网）
ISP	GE0/0/1	220.1.1.14/28	因特网路由器
ISP	GE0/0/2	220.1.2.14/28	因特网路由器

PC1	/	10.40.10.2/24	总部办公终端
PC2	/	10.40.10.3/24	总部办公终端
PC3	/	10.40.30.2/24	分部办公终端
PC4	/	220.1.1.60/28	因特网主机
SERVER	/	172.20.20.2/24	DMZ 区 Web 服务器
地址池 PoolA	/	220.1.1.20—220.1.1.30	源 NAT 地址池
公网发布地址	/	220.1.1.200	目的 NAT (NAT Server) 公网地址

模块 C 网络故障分析与排除（40 分钟，15 分）

[拓扑描述]

园区网与企业分支互联环境，核心层、汇聚层与接入层设备已完成连接，设备中存在预置的若干错误配置或故障点。本模块在华为 eNSP 模拟器中完成，故障拓扑与预置错误配置由赛场统一下发。

[故障现象]

- 1.总部办公终端 PC1 无法访问服务器 SERVER;
- 2.分支机构终端 PC3 无法访问总部内网;
- 3.内网主机无法访问公网（NAT 转换失效）。

[任务说明]

1.故障排查：使用 ping、tracert、display vlan、display port-security、display acl、display ospf peer、display ip routing-table、display nat-policy、display security-policy 等命令，按分层法、分段法定位故障，记录故障现象与产生原因（可能涉及 VLAN 划分与 Trunk 放行、端口安全 MAC 绑定、ACL 规则、路由协议 network 声明、静态/默认路由、NAT 配置、安全策略、IPsec 参数等）。（6 分）

2.故障排除：修正错误配置，恢复全网互通与业务访问，并将故障原因、修复方法与正确配置截图填入答题文件。（6 分）

3.验证与记录：对恢复后的业务进行验证（PC1 访问 SERVER、PC3 访问总部内网、内网访问公网），留存验证结果截图，文档规范、表述清晰。（3 分）

[结果要求]

- 1.总部终端可以访问服务器 SERVER;
- 2.分支机构终端可以访问总部内网;
- 3.内网主机可以正常访问公网;
- 4.答题文件完整记录故障原因、修复方法与验证结果。

模块 D CTF 安全攻防实操（60 分钟，25 分）

[考核说明]

- 1.本模块在赛场部署的 CTF 竞赛平台（GZ::CTF）上进行，平台为每位选手动态分发独立的容器化靶机，题目 Flag 随机生成、唯一有效。
- 2.选手通过本人账号登录平台并提交 Flag，Flag 格式统一为 flag{...}；同一 Flag 首次正确提交计分，重复提交不重复计分，错误提交不扣分。
- 3.本模块的操作范围仅限平台分配给本人的靶机；严禁对赛场网络设备、服务器及其他选手靶机等非授权目标发起扫描、爆破与攻击。
- 4.平台与终端提供统一的工具环境（浏览器、扫描与抓包工具等），禁止使用搜索引擎及外部求助方式；靶机访问地址与端口以赛场公布为准。

[题目清单与分值]

序号	题目名称	分值	Flag 与提交要求
1	基础信息收集与弱口令检测	4	提交第一处 Flag，格式为 flag{...}
2	Web 漏洞利用（文件上传）	10	提交第二处 Flag，并留存上传与访问截图
3	主流漏洞复现（框架 RCE）	8	提交第三处 Flag，并留存 POC 执行截图
4	操作规范与痕迹清理	3	提交清理完成截图，靶机环境复位
合计		25	

[任务说明]

- 1.基础信息收集（4 分）：对本人靶机进行端口扫描，识别开放的 Web 服务与数据库服务；对数据库服务进行弱口令检测并成功登录，从数据表中读取第一处 Flag

并在平台提交。（4分）

2.Web 漏洞利用（10分）：靶机部署存在文件上传漏洞的 Web 应用，要求依次绕过前端 JS 校验、MIME 类型检测与黑名单后缀过滤，成功上传 Webshell 并访问，读取 Web 目录下的第二处 Flag 并在平台提交。（10分）

3.主流漏洞复现（8分）：靶机部署存在远程代码执行漏洞的业务系统（如 ThinkPHP 5.0.23），要求识别框架与版本特征，构造标准 POC 执行系统命令，读取系统敏感文件中的第三处 Flag 并在平台提交。（8分）

4.操作规范与痕迹清理（3分）：完成全部操作后，清理靶机中上传的临时文件与 Webshell，清除 Web 访问日志与命令执行历史，复位靶机环境，并将清理完成截图保存至答题文件。（3分）

[结果要求]

- 1.三处 Flag 均在平台正确提交，平台提交记录与答题文件截图一致；
- 2.答题文件完整记录信息收集、漏洞利用与漏洞复现的关键步骤与结果截图；
- 3.靶机环境复位，无残留临时文件、Webshell 与日志；
- 4.全过程未对非授权目标发起扫描、爆破与攻击，未使用搜索引擎及外部求助方式。

（二）评判标准

1.模块 A 评分表（30 分，测量分）

序号	评分项目	分值	评分内容与评分标准
1	VLAN 创建与端口类型配置	5	使用 vlan batch 正确创建 VLAN 101/102/109；连接终端端口配置为 Access 并加入对应 VLAN；连接 R1 端口配置为 Trunk
2	Trunk 放行与二层互通	3	Trunk 端口放行 VLAN 101、102、109；PC1、PC2、SERVER 与 R1 二层互通
3	端口安全与 MAC 绑定	6	启用端口安全（port-security enable），最大 MAC 地址数为 1，绑定终端 MAC 地址，违规动作为 shutdown；接入非法终端时端口进入 error-down
4	三层子接口与网关配置	4	子接口 dot1q termination vid 封装正确，网关地址配置正确，开启 arp broadcast enable，各 VLAN 网关可达

5	OSPF 部署与路由学习	7	OSPF 进程 1、Router ID、骨干区域 Area 0 配置正确；network 声明（反掩码）覆盖总部网段与互联网段；R2 学习到总部路由
6	高级 ACL 与服务器防护	3	ACL 规则正确（仅放通访问 SERVER 的 TCP 443 端口，拒绝其余 IP 流量），并在 SERVER 网关子接口正确方向应用 traffic-filter
7	广域网路由与全网互通验证	2	R2 静态路由、R5 默认路由配置正确；PC1、PC2、PC3 互相 PING 通并留存验证截图
合计		30	

2.模块 B 评分表（25 分，测量分）

序号	评分项目	分值	评分内容与评分标准
1	安全区域划分	3	FW1 各接口使用 firewall zone 正确加入 Trust、DMZ、Untrust 区域，使用缺省优先级
2	安全策略配置	6	security-policy 规则允许 PC1、PC2 访问 SERVER；放通总部与分支 IPsec VPN 流量；未匹配流量缺省拒绝
3	源 NAT 部署	6	nat address-group 正确创建地址池 PoolA（220.1.1.20—220.1.1.30）；nat-policy 源 NAT 策略正确，PC1、PC2 可访问公网主机 PC4
4	目的 NAT(NAT Server)	5	nat server 将公网地址 220.1.1.200 的 TCP 80 正确映射至内网服务器 172.20.20.2:80，公网主机可访问 HTTP 服务
5	IPsec VPN 部署	5	感兴趣流 ACL、IPsec 安全提议（sha2-256、aes-128）、IKE 安全提议与对等体（预共享密钥、远端/本端地址）配置正确并在出接口应用 ipsec policy；总部与分支内网互通
合计		25	

3.模块 C 评分表（15 分，测量分）

序号	评分项目	分值	评分内容与评分标准
1	故障定位与原因分析	6	正确使用 ping、tracert、display 等诊断命令定位故障点；准确记录故障现象与产生原因（VLAN/Trunk、端口安全、ACL、路由、NAT、安全策略、IPsec 等）
2	故障排除与业务恢复	6	错误配置修正正确；总部终端访问 SERVER、分支访问总部内网、内网访问公网全部恢复
3	验证与文档规范	3	留存业务验证截图；答题文件记录完整、表述清晰、格式规范
合计		15	

4. 模块 D 评分表（25 分，测量分）

序号	评分项目	分值	评分内容与评分标准
1	基础信息收集	4	完成端口扫描并识别开放端口与服务（2 分）；弱口令检测成功并登录数据库（1 分）；读取第一处 Flag 并正确提交（1 分）
2	Web 漏洞利用	10	识别文件上传漏洞的校验规则（2 分）；绕过前端 JS 校验与 MIME 类型检测（3 分）；绕过黑名单后缀过滤上传 Webshell（3 分）；访问 Webshell 读取第二处 Flag 并提交（2 分）
3	主流漏洞复现	8	识别目标框架与版本特征（2 分）；构造标准 POC 执行系统命令（4 分）；读取系统敏感文件获取第三处 Flag 并提交（2 分）
4	操作规范与痕迹清理	3	清理靶机中上传的临时文件与 Webshell（1.5 分）；清除 Web 访问日志与命令执行历史（1.5 分）
合计		25	

5. 模块 E 评分表（5 分，评价分）

序号	评分项目	分值	评分内容与评分标准
1	安全用电与规范操作	2	遵守安全规程与设备操作规程，正确使用工具与终端软件，无违规带电操作
2	工位整洁与工具使用	1	工位保持整洁，设备与线缆摆放规范，爱护赛场设备
3	诚实守信与信息安全	2	遵守竞赛纪律与“三个禁止”要求；答题文件、截图、命令行中未出现工位号、姓名、院校等个人信息；CTF 操作仅限本人授权靶机，未对非授权目标发起扫描、爆破与攻击
合计		5	

评分说明

1. 测量评分以功能结果与关键配置为准：每个评分项除非另有说明，只能给予满分或 0 分；如需使用 0 分到满分之间的分数，该项中应有清晰的解释说明。

2. 命令名称、视图与参数正确即可得分；命令缩写、序号取值不同但功能等效的不扣分；设备命令以赛场实际设备（华为 eNSP 模拟器，VRP 命令体系）为准。

3. 评价评分由不少于 2 名裁判独立评分后取平均值，分数精确到小数点后 2 位，

四舍五入。

4.参赛选手提交的答题文件、截图、命令行中出现工位号、姓名、单位等个人信息的，本模块成绩按零分处理；模块 D 另按 CTF 平台记录核对。

5.模块 D 以 CTF 竞赛平台提交记录为计分依据，Flag 格式错误、未在平台提交或平台记录与答题文件截图不一致的，该处 Flag 不予计分；同一 Flag 仅首次正确提交计分；操作规范与痕迹清理项由裁判依据答题文件截图判定。

6.各模块原始成绩相加即为选手最终成绩，成绩保留小数点后一位。