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

赛项样题(选拔赛)

2026 年 06 月

目　录

一、竞赛内容分布

模块一：职业素养与理论技能（10%）

模块二：安全网络架构设计及设备选型（15%）

模块三：安全网络架构构建（35%）

模块四：网络安全技能应用（40%）

二、竞赛时间

竞赛时间为 3 个小时。

三、竞赛注意事项

1. 竞赛所需的硬件、软件和辅助工具由组委会统一布置，选手不得私自携带任何软件、移动存储、辅助工具、移动通信等进入赛场。

2. 请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

3. 操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆动硬件连接。

4. 比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

5. 裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，不得以任何形式体现参赛院校、工位号等信息。

四、竞赛模块任务

考生按照每个模块的题目要求，仔细作答后按照要求提交竞赛结果文件。

赛题背景

某企业业务规模持续发展壮大，正全面推进内部信息化建设，以赋能业务高效增长、支撑内外部协同沟通。为实现数据精细化管理与服务能力升级，企业决定构建一套自主可控的安全网络架构，核心目标是保障数据交互的高效性、可靠性与安全性，同时提升业务部署的弹性与灵活性。

为避免员工互联网访问流量挤占核心业务带宽、干扰业务数据稳定传输，企业规划申请独立的运营商互联网专线，实现办公上网流量与核心业务流量的隔离分流；同时针对互联网访问行为部署全量审计与管控机制，规范办公用网行为，筑牢网络接入安全防线。此外，为满足员工异地办公、远程协作的业务需求，网络需具备安全的远程接入能力，保障外部人员合规、安全地访问内网业务资源。

模块一：职业素养与理论技能

单选部分

1. WAF 设备的主要防护场景是（）

A. 防护 Web 应用攻击（SQL 注入、XSS 等）

B. 防护硬件物理损坏

C. 优化服务器硬件性能

D. 监控本地桌面操作

2. 用户权限安全加固的核心原则是（）

A. 最大权限分配

B. 最小权限、按需分配

C. 所有用户权限一致

D. 普通用户开放管理员权限

3. Linux 系统中，UID 为 0 的账户权限是（）

A. 普通用户权限

B. 超级管理员 root 权限

C. 访客权限

D. 只读权限

4. Linux 系统中查看定时任务的核心命令是（）

A. crontab

B. ls

C. cd

D. ping

5. 数据保密性的核心含义是（）

A. 数据随时可被所有人访问

B. 数据仅被授权主体访问，杜绝非法泄露

C. 数据内容不可修改

D. 数据永久存储不丢失

6. 数据生命周期管理的完整流程不包括（）

A. 采集、存储

B. 使用、传输

C. 销毁、归档

D. 无限制永久留存

7. XSS 跨站脚本漏洞的核心危害是（）

A. 占用服务器带宽

B. 执行恶意脚本，窃取用户 Cookie、劫持用户会话

C. 导致服务器断电

D. 压缩网页文件体积

8. CSRF 跨站请求伪造漏洞的主要原理是（）

A. 服务器未校验请求来源，冒用用户身份发起恶意请求

B. 恶意代码注入数据库

C. 网页脚本过滤不严

D. 服务器端口开放过多

9. 文件上传漏洞的核心风险是（）

A. 上传图片文件压缩失真

B. 绕过文件格式校验，上传 Webshell 等恶意文件

C. 占用服务器存储空间

D. 降低网页加载速度

10. SQL 注入漏洞的核心攻击目标是（）

A. 服务器日志文件

B. 网站数据库，窃取、篡改、删除数据

C. 客户端浏览器缓存

D. 网络路由配置

11. 以下最容易引发 SQL 注入漏洞的代码场景是（）

A. 直接拼接用户输入参数至 SQL 语句

B. 对用户输入做过滤转义

C. 使用预编译语句查询数据库

D. 限制输入字符长度

12. 服务器弱口令漏洞最常见的风险场景是（）

A. 密码复杂度高、定期更换

B. 使用默认密码、简单数字/字母密码

C. 密码绑定设备

D. 开启二次验证

13. 目录遍历漏洞可导致的直接危害是（）

A. 读取服务器任意路径敏感文件

B. 篡改网站前端代码

C. 关闭服务器端口

D. 清空系统日志

14. 处理涉密网络安全日志时，合规操作是（）

A. 拷贝日志至个人私人 U 盘留存

B. 截图发布至技术交流社群

C. 仅在内网涉密终端查看，不外传

D. 离职时带走日志用于个人学习

15. 第三方人员临时接入内网开展运维，首要管控动作是（）

A. 直接开放全部内网权限

B. 登记身份、临时最小权限授权、全程旁站监督

C. 允许第三方使用私人设备接入

D. 不记录接入日志

16. 绕过前端 JS 校验上传 Webshell 的核心思路是（）

A. 修改本地系统时间

B. 抓包修改请求包后缀绕过前端校验

C. 压缩文件后缀

D. 修改浏览器编码

17. Windows IIS 短文件名漏洞可实现（）

A. 枚举服务器隐藏文件名

B. 直接获取系统管理员权限

C. 远程桌面登录

D. 删除系统文件

18. Webshell 蚁剑连接流量特征（）

A. 请求体 Base64 编码后加密传输

B. 明文传输系统命令

C. 无 Cookie 字段

D. 固定 80 端口访问

19. 网络安全从业人员在工作中发现未公开的系统漏洞，正确的做法是（）

A. 私下利用漏洞测试系统权限

B. 第一时间上报相关负责人，合规处置

C. 将漏洞细节分享给同行交流

D. 留存漏洞后门方便后续排查

20. 关于网络安全行业准则，下列说法错误的是（）

A. 坚守合法合规、诚信自律原则

B. 严禁非法入侵他人网络系统

C. 可随意收集、留存用户敏感数据

D. 恪守行业职业道德，保守工作涉密信息

21. 根据《中华人民共和国网络安全法》，国家实行网络安全（）保护制度，这是我国网络安全防护的核心基础制度。

A. 等级

B. 分级

C. 分类

D. 分层

22. 依据《中华人民共和国数据安全法》，国家建立数据（）治理体系，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露

或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

A. 统一集中

B. 分类分级

C. 全量备案

D. 属地专属

23. 下列选项中，不属于个人信息处理基本原则的是（）。

A. 合法、正当、必要

B. 公开透明，明示处理规则

C. 最大化采集用户信息

D. 保证个人信息质量准确

24. 《网络安全等级保护基本要求》（GB/T 22239-2019）将我国信息系统的安全保护等级划分为（）个级别。

A. 三

B. 四

C. 五

D. 六

25. 根据网络安全等级保护三级基本要求，网络设备、安全设备、操作系统及业务应用的安全日志留存时间应不少于（）。

A. 1 个月

B. 3 个月

C. 6 个月

D. 12 个月

26. 按照数据重要程度与泄露危害程度的通用分级标准，企业数据通常划分为核心数据、重要数据和（）三个基础等级。

A. 敏感数据

B. 一般数据

C. 公开数据

D. 涉密数据

27. 下列技术手段中，不属于常用数据脱敏处理方式的是（）。

A. 字符替换与遮蔽

B. 数据随机打乱

C. 数据加密存储

D. 全量数据备份

28. 网络安全事件应急响应的标准处置流程中，确认事件发生后的首要操作环节是（）。

A. 根除攻击痕迹

B. 遏制攻击扩散

C. 恢复业务系统

D. 撰写总结报告

29. 排查 Linux 系统入侵痕迹时，用于查看系统历史用户登录记录的核心命令是（）。

A. ps

B. last

C. top

D. ifconfig

30. 企业安全网络架构中，专门用于部署面向互联网对外服务的服务器、实现内外网流量隔离缓冲的区域是（）。

A. 内网核心区

B. DMZ 非军事区

C. 办公终端区

D. 运维管理区

多选部分

31. 常用的数据安全防护技术有（）

A. 数据加密、脱敏

B. 访问控制、权限管控

C. 数据备份、容灾恢复

D. 数据水印、溯源追踪

32. 数据安全风险评估的核心内容包括（）

A. 识别数据资产等级

B. 排查各环节安全风险

C. 评估风险影响范围、等级

D. 制定风险整改防护方案

33. XSS 漏洞的分类包含（）

A. 存储型 XSS

B. 反射型 XSS

C. DOM 型 XSS

D. 物理型 XSS

34. Windows 系统安全日志加固与审计加固的正确做法包括（）

A. 扩大安全日志默认存储上限，开启日志覆盖前备份，防止日志被恶意清空

B. 启用审核对象访问策略，监控系统敏感目录的读写、删除行为

C. 关闭本地安全策略中“审核登录事件”，减少日志占用磁盘空间

D. 限制 Guest 账户本地登录权限，禁止 Guest 访问系统安全日志

35. Nginx 中间件配置不当引发的原生漏洞及利用方式，说法正确的有（）

A. 开启 alias 目录匹配错误，可导致任意文件读取，读取服务器 /etc/passwd 敏感文件

B. 未关闭目录浏览模块，攻击者可遍历网站全部源码、备份压缩包

C. 开启 gzip 压缩模块，直接引发远程代码执行漏洞

D. 解析漏洞可通过构造 xxx.jpg/.php 路径，绕过文件后缀检测解析执行

php 木马

36. 下列属于网络安全违法行为的是（）

A. 非法入侵他人计算机信息系统

B. 非法获取、篡改网络数据

C. 制作、传播网络恶意程序

D. 合规开展授权安全测试

37. 服务器常见高危漏洞及风险包括（）

A. 弱口令漏洞-暴力爆破权限

B. 命令执行漏洞-远程控权

C. 目录遍历漏洞-读取敏感文件

D. 权限绕过漏洞-越权访问

38. 文件类漏洞的危害包括（）

A. 上传 Webshell 控制网站

B. 读取服务器配置、密钥文件

C. 包含恶意文件执行代码

D. 篡改网站源码文件

39. 网络安全行业最佳实践包含（）

A. 最小权限分配

B. 常态化风险排查、安全加固

C. 数据分级分类防护

D. 安全事件及时上报处置

40. 常见的 Web 应用漏洞包括（）

A. SQL 注入

B. XSS 跨站脚本

C. CSRF 跨站请求伪造

D. 文件上传漏洞

41. 根据《中华人民共和国网络安全法》，网络运营者应当履行的安全保护义务包括（）。

A. 制定内部安全管理制度和操作规程，确定网络安全负责人

B. 采取防范计算机病毒、网络攻击、网络侵入等危害网络安全行为的技术措施

C. 采取监测、记录网络运行状态、网络安全事件的技术措施，留存合规日志

D. 未经安全评估，擅自向境外提供境内收集产生的个人信息和重要数据

42. 网络安全等级保护2.0标准中,技术层面的核心安全要求维度包括()。

A. 物理和环境安全

B. 网络和通信安全

C. 设备和计算安全

D. 应用和数据安全

43. 数据全生命周期管理中，数据销毁阶段的合规操作要求包括（）。

A. 采用消磁、物理粉碎等不可恢复的方式销毁存储介质

B. 留存销毁审批记录、操作日志与全程监督凭证

C. 将存储过敏感数据的旧硬盘直接丢弃或二手转卖

D. 针对不同等级数据执行差异化的销毁审批流程

44. 网络安全应急响应遵循 “先遏制、再根除、后恢复” 的处置原则，以下属于遏制阶段可执行操作的有（）。

A. 封禁攻击源 IP 地址与恶意端口

B. 隔离已失陷的主机，断开受影响网段的网络连接

C. 清除系统后门、Webshell 等恶意程序

D. 临时关停受攻击的非核心业务，避免横向扩散

45. 企业网络边界处通常部署的安全防护设备包括（）。

A. 下一代防火墙

B. 入侵防御系统（IPS）

C. 出口路由器

D. 数据库审计系统

46. 合理的网络安全架构与防御技术能够有效抵御外部威胁。以下关于网络安全架构与防御技术的描述，正确的有（ ）

A. 通过网络拓扑设计、子网划分和 VLAN 隔离，可以实现网络区域的逻辑或物理隔离，限制广播域和攻击面

B. 防火墙（FW）主要基于预设的安全规则和 IP/端口控制网络流量，实现

基础的访问控制

C. 入侵防御系统（IPS）能够深度检测网络流量，并主动阻断已识别的网络攻击行为

D. Web 应用防火墙（WAF）专门用于防护 Web 应用程序，能够有效缓解 SQL 注入、XSS 等应用层攻击

47. 系统安全加固是提升操作系统抗攻击能力的重要手段。以下关于 Windows 和 Linux 系统安全加固的描述，正确的有（ ）

A. 在 Windows 系统中，应设置强密码策略，并合理分配用户和用户组的权限

B. 在 Windows 系统中，启用审核功能并利用日志和安全模板分析，有助于记录和规范系统活动

C. 在 Linux 系统中，应定期检查弱口令、空口令，并排查系统中是否存在除 root 外其他 UID 为 0 的特权用户

D. 在 Linux 系统中，无需关注文件系统的文件格式分类和权限设置，因为 Linux 默认具有极高的安全性

48. 针对 Web 服务器和应用程序的应急响应，需要重点排查 Webshell 及识别各类攻击特征。以下描述正确的有（ ）

A. 可通过检查文件修改时间、文件内容特征及流量行为等方式排查 Webshell 文件

B. 在日志中识别 SQL 注入漏洞利用特征，如包含 UNION SELECT、SLEEP() 等

关键字

C. 系统后门排查仅需关注网络端口，无需检查系统内核模块或隐藏文件

D. 敏感信息漏洞利用特征可能表现为短时间内大量下载或遍历敏感目录的异常请求

49. 数据安全是保护数据免受破坏、泄露和非法使用的关键。以下关于数据安全基础与技术理论的描述，正确的有（ ）

A. 数据安全的三个基本属性包括保密性、完整性和可用性（CIA）

B. 数据加密技术可以保障数据在传输和存储过程中的保密性

C. 访问控制机制用于确保只有经过授权的用户才能访问特定数据

D. 数据备份技术的主要目的是提升数据在网络中的传输速度

50. Web 漏洞挖掘是网络安全测试的重要环节。以下关于常见 Web 漏洞原理的描述，正确的有（ ）

A. SQL 注入漏洞是由于应用程序未对用户输入进行严格过滤，导致恶意 SQL 语句被数据库执行

B. 跨站脚本（XSS）漏洞允许攻击者在受害者的浏览器中执行恶意脚本，从而窃取信息或劫持会话

C. 跨站请求伪造（CSRF）漏洞是利用受害者已登录的身份，在受害者不知情的情况下发送恶意请求

D. 文件包含漏洞仅能包含本地文件，绝对无法通过远程 URL 包含恶意文件

模块二：安全网络架构设计及设备选型

集团公司最近在香港新租用了一栋综合商住两用楼用于公司临时办公，考虑到公司网络安全建设，公司领导强烈要求考虑网络的安全可靠性，公司网络与安全部建议通过部署网络及安全设备提高网络健壮性，用于购置设备的预算为 18.5 万元，具体需求如下，请结合附表设备参数、业务实际需求，在预算限额内择优选型，设计性价比最优方案，选用设备满足全部业务功能，尽可能控制采购总成本、选取贴合项目的配置。

企业员工 500 名，租用 3 条 1000Mbps 运营商光纤专线接入互联网（三条运营商专线包含以太网光纤线路，老式广域串行链路接入等）；内部划分不同安全区域，管控跨区域访问权限，全网进出流量需要统一查杀病毒、恶意代码，阻断病毒通过网络下载、内网横向扩散传染，同时需要实时深度检测，拦截端口扫描、恶意木马等入侵行为；设置服务器区搭建企业官网与线上业务系统，对外面向互联网用户访问，需防范 SQL 注入、XSS 跨站、恶意爬虫等网络攻击；企业办公分布 6 层，其中 3 层主力楼层每层部署近 120 台办公终端，点位集中密集，企业日常办公网页、ERP 业务并发连接量大，高峰期全网同时在线连接峰值约 180 万，剩余 3 层附属楼层为零散小办公室，每层仅 20 台以内终端；所有工位终端就近点位布线入网，内网按照行政、财务、研发等不同部门划分独立逻辑网段，各网段之间需要互相通信；全部楼层点位设备统一远程光纤上联至中心机房两台枢纽设备，承载整网终端的跨网段数据转发；且为规范员工日常办公上网，需要管控网页浏览、软件下载、流媒体、短视频访问，可记录上网日志、按需限流并封堵违规网站。

1. 业务背景及需求：

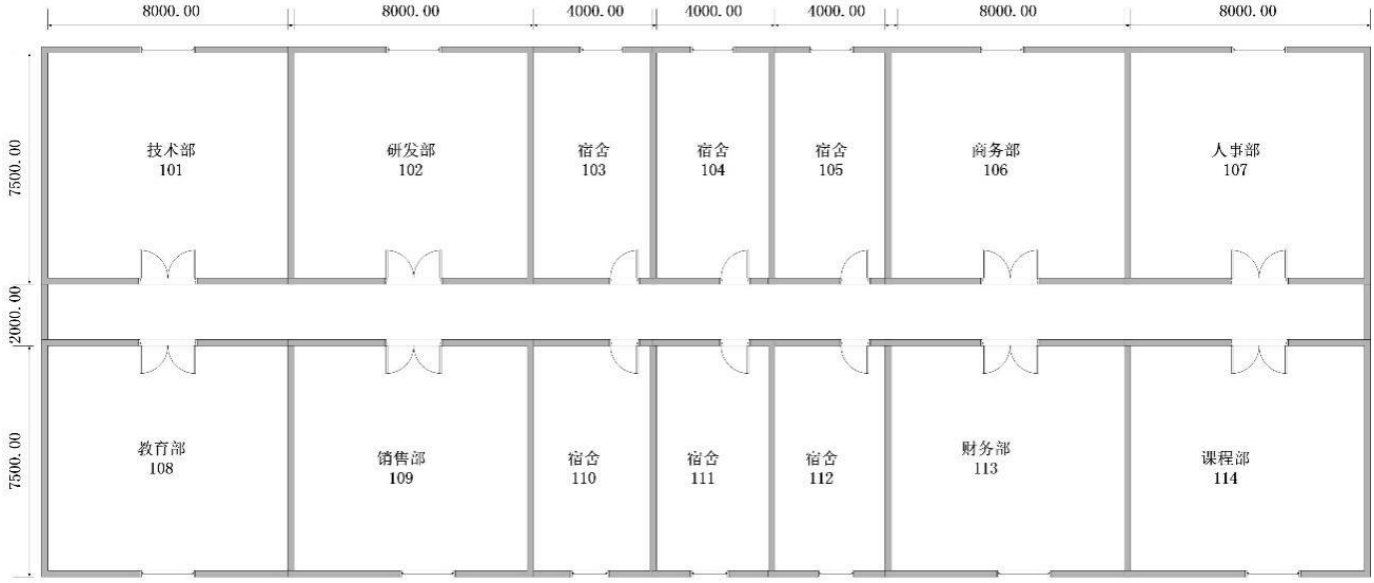
- **楼宇的相关信息如下：**

建筑使用说明：该楼宇为一栋商住综合楼，可供公司员工住宿、办公和

会议。

建筑现场情况：该楼宇原有强电布线室内外均采用了 pvc 线槽敷设，和管理处协商后确认，只允许在宿舍区进行穿墙施工。

建筑物弱电间情况：该楼宇目前没有独立的弱电间，经同管理处协商，弱电间位置位于最左侧走廊，安装位置为在 108 房间外，核心机房部署在 6 楼，整层建筑的平面布局图如图 1-1 所示：



备注：墙高：300cm
门宽度：90cm，高度：200cm
单位：mm

图 1-1 平面布局图

- **网络产品的参数与价格**

表 1-1 交换产品价格表

型号	交换容量	包转发率	端口类型及数量	价格（元）
core1	4.8Tbps	2000Mpps	48 个 1/10GE SFP Plus 端口，4 个 40/100GE QSFP28 端口	12000
core2	12.8Tbps	4482Mpps	64 个 100GE QSFP28 以太网端口	20000

core3	688Gbps	171Mpps	24 个 10/100/1000Base-T 自适应以太网端口，4 个 1/10GE SFP+口	4000
access1	672Gbps	171Mpps	24 个 10/100/1000BASE-T 自适应以太网端口，4 个 1000BASE-X SFP 端口	2200
access2	672Gbps	171Mpps	24 个 10/100/1000BASE-T 电口，4 个 1/2.5/10GE SFP+端口	2500
access3	672Gbps	207Mpps	48 个 10/100/1000BASE-T 电口，4 个 1/2.5/10GE SFP+端口	3500

表 1-2 路由产品价格表

型号	出口带宽	带机量	端口类型及数量	价格（元）
router1	10Gbps	1500	8*GE 电+ 5*10GE 光	17000
router2	1000Mbps	500	8*GE(电)+ 2*GE(光)	5000
router3	3Gbps	800	8*GE 电+ 3*10GE 光	7000

表 1-3 安全产品价格表

型号	出口带宽	并发连接数	端口类型及数量	带机量	价格（元）
FW1	1Gbps	80 万	6GE 电 + 2GE 光	200	20000
FW2	8Gbps	400 万	8GE 电 + 6*10GE 光+2*40G 接口	1000	70000（已包含 AV 授权& WAF 授权）
FW3	3Gbps	180 万	6GE 电 + 4*10GE 光	650	36000
FW4	6Gbps	250 万	8GE 电 + 4*10GE 光	750	42000（已包含 AV 授权）
防火墙的 AV 防病毒授权	NA	NA	NA	NA	9000
防火墙的 WAF 防病毒授权	NA	NA	NA	NA	11000
行为管理 1	1Gbps	80 万	6GE 电 + 2GE 光	200	30000
行为管理 2	4Gbps	220 万	8GE 电 + 4×10GE 光	600	50000
IPS1	3.5Gbps	220 万	8GE 电 + 8GE 光 +4×10GE 光	600	40000
IPS2	3Gbps	200 万	8GE 电 + 6GE 光 +4×10GE 光	550	30000

2. 网络架构规划

➢ 设备选型

请根据公司预算及需求，使用竞赛平台中设备选型模块，选择合适的设备型号及数量，并导出设备选型的 Excel。

➢ 逻辑拓扑设计

结合选择的设备型号及数量，结合办公业务背景说明信息使用竞赛平台的图纸制作模块，输出网络拓扑图，网络拓扑图要明确标注线缆类型、设备端口、逻辑区域等内容。

➢ 物理环境规划

根据提供的建筑平面布局图、项目预算和业务需求进行的规划与设计，使用竞赛平台输出一楼层电子位图，包含设备位置、信息点位置等。

模块三：安全网络架构构建

答题须知

1.拓扑图在平台中已搭建好，参赛选手登录操作即可，切勿删除移动设备或链路等；

2.操作过程为防止设备崩溃，建议参赛选手对设备配置及时保存。

（一）基础网络配置

1.根据附录一拓扑图、附录二地址规划表，配置设备接口、安全区域及主机名信息等；

2.在网络设备上均开启 SSH 服务端功能，其中用户名和密码为 admin/Aa@123789，只允许 10.10.110.110PC 登录设备；

3.网络设备配置 SNMP，SNMP 服务器部署在数据中心区，地址为 10.10.110.100/24。SNMP 协议为 V2C，团体字为 Bb@123456，只读权限。

（二）网络拓扑搭建

1.接入设备启用端口安全功能，控制用户安全接入；

2.接入设备端口配置为边缘端口，开启 BPDU 防护功能，端口因触发 BPDU 防护禁入禁用状态后 200 秒自动恢复；

3.总部在 Core1、Core2 上配置 DHCP 服务器功能，接入设备启用 DHCP 安全防护机制，通过硬件 IP/MAC 表项过滤匹配保证主机安全；

4.配置 RSTP 与 VRRP，以 Core1 为主设备，Core2 为从设备。生成树优先级为 0 与 4096，VRRP 优先级为 200 与 150；

5.Core1、Core2、FW1、FW2 之间使用 OSPF 路由协议，进程号 10；FW3、Core 之间使用 OSPF 路由协议，进程号 20；R1、R2、R3 之间使用 OSPF 路由协议，进程号 30；OSPF 验证 md5 密钥为 brskills；

6.R1、R2、R3 配置 MPLS LDP，基于 VRF 实现总分部财务网络三层 VPN 互通。

7.总分部只允许销售网络可以访问互联网，其中分部访问互联网路径为 FW3-SW-FW4，当 FW3 连接 SW 线路故障时，访问互联网路径为 FW3-Core-SW-FW4；

8.Core1 与 Core2 的上联口双向流量通过端口镜像镜像至 IDS，进行入侵检测；

9.总部 VPN 设备映射到 FW1 的公网出口，地址端口为 39.1.1.10:36666；

10.数据中心服务器网关在Core-data设备上,配置路由策略把流量送往WAF安全防护；

11.FW1 与 FW2 配置 HA，以 FW1 为主，FW2 为备；

12.FW3、Core、FW4 之间配置 RIP 路由协议；

（三）安全设备防护

1.FW3 配置虚拟防火墙，财务流量走虚拟墙策略；

2.FW4 与 FW1 配置 IPSEC VPN，MPLS 线路故障时，总分部可以通过互联网走 IPSEC 进行数据传输；

3.总部配置 SSL VPN，供互联网或外部用户拨号上网；

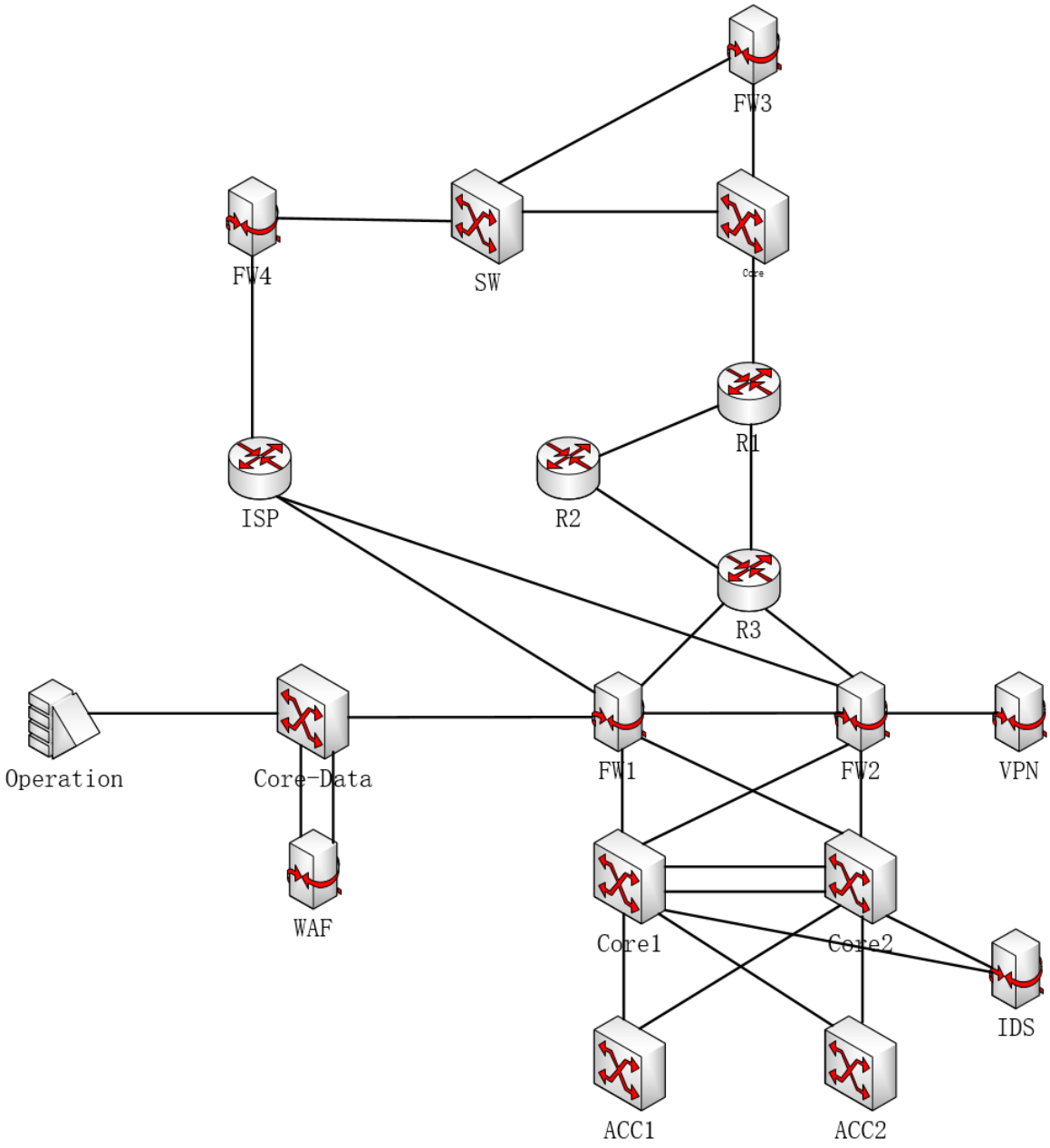
4.WAF 配置开启可疑 UA 检测，只记录日志；关注 XSS 注入检查，开启抓包只记录日志；

5.FW1、FW2、FW4 配置病毒过滤，创建规则名称 AV_new，扫描类型包含 ZIP、MAIL、HTML，当识别非法行为时阻断网络；

6.IDS 配置只记录日志，使用通用宽松型模板；

7.配置防火墙策略时，要求每条策略严格精确到协议端口，不允许出现宽松策略。

附录一：拓扑图


FW3
FW4
SW
Core
R1
ISP
R2
R3
Operation
Core-Data
FW1
FW2
VPN
WAF
Core1
Core2
IDS
ACC1
ACC2

附录二：地址规划表

设备名称	接口或 VLAN	IP 地址/掩码	说明
FW1	E0/0	10.1.1.1/30	
	E0/1	10.1.1.5/30	
	E0/2	10.1.1.9/30	
	E0/3	10.1.1.17/30	
	E0/4	10.1.1.13/30	
	E0/5	39.1.1.2/24	To_ISP
FW2	E0/0	10.1.1.2/30	
	E0/1	10.1.2.5/30	
	E0/2	10.1.2.9/30	
	E0/3	10.1.2.17/30	
	E0/4	10.1.2.13/30	
	E0/5	39.1.2.2/24	To_ISP
FW3	E0/0	10.2.10.254/24	Sales
	E0/1	10.2.20.254/24	Finance
	E0/2	10.2.0.2/24	
	E0/3	10.2.1.2/30	
FW4	E0/0	10.2.0.3/24	
	E0/1	39.1.3.2/24	To_ISP
VPN	E0/0	10.1.2.18/30	
WAF	E0/0	10.1.3.2/30	
	E0/1	10.1.3.6/30	
Core1	GE1/0/6	10.1.1.6/30	
	GE1/0/7	10.1.2.6/30	
	Vlanif10	10.1.10.253/24	Sales
	Vlanif20	10.1.20.253/24	Finance
Core2	GE1/0/6	10.1.1.10/30	
	GE1/0/7	10.1.2.10/30	
	Vlanif10	10.1.10.252/24	Sales
	Vlanif20	10.1.20.252/24	Finance
Core-Data	GE1/0/3	10.1.1.18/30	
	GE1/0/1	10.1.3.1/30	
	GE1/0/2	10.1.3.5/30	
Core	GE1/0/1	10.2.1.1/30	
	GE1/0/2	10.2.1.5/30	
	GE1/0/3	10.2.0.1/24	
R1	Gi1/0	10.0.0.1/30	
	Gi2/0	10.2.1.6/30	

	Gi3/0	10.0.0.5/30	
R2	Gi1/0	10.0.0.6/30	
	Gi2/0	10.0.0.9/30	
R3	Gi1/0	10.1.1.14/30	
	Gi2/0	10.1.2.14/30	
	Gi3/0	10.0.0.2/30	
	Gi4/0	10.0.0.10/30	

模块四：网络安全技能应用

（一）任务描述

完成企业安全网络架构搭建与安全设备部署后，集团核心业务系统“工贸综合管理系统”正式上线运行。该系统覆盖集团全链路业务管控，包含客户档案管理、购销订单、仓储出入库、财务台账、内部人事、企业公告资讯、单据自定义打印、系统运维配置八大业务模块，存储有客户联系方式、采购合同底价、财务对账凭证、内部员工薪资账号等核心敏感经营数据，是集团已完成备案的等级保护三级信息系统。

近期系统即将迎接官方等级保护测评，同时企业安全监控平台监测到业务服务器存在异常扫描访问行为与可疑外联告警，数据泄露与系统失陷风险突出。为全面保障业务系统安全合规运行，筑牢应用层与主机层安全防线，现由安全运维团队对该系统开展全流程安全保障工作，涵盖漏洞检测验证、系统安全加固、安全事件应急处置、合规运营审计四大核心工作环节。

（二）任务说明

参赛选手身份：企业信息安全部专职安全工程师。

工作授权：已获得企业正式书面授权，可对目标业务系统与对应服务器开展漏洞检测、加固整改、应急处置与合规审计工作。

操作规则：

所有操作仅限指定目标靶机，禁止对非授权系统、网络设备进行扫描与攻击；禁止执行删除业务数据、强制关停核心服务等破坏性操作。

漏洞检测采用黑盒模式，可通过浏览器访问业务系统前端。

应急处置环节须遵循“先遏制、再根除、后恢复”的行业标准流程，原始日志、恶意文件等攻击痕迹须完整留存，不得直接删除原始证据。

所有操作结果须按答题卡模板规范填写，关键操作、验证结果须附操作截图佐证；所有加固、配置类操作完成后，须确保业务系统可正常访问、核心功能可正常使用。

系统访问地址：http://靶机 IP:8000

任务 1：Web 漏洞检测与验证

按照集团《信息系统上线安全管理规范》与等级保护测评要求，业务系统全面推广启用前，须完成首轮全面安全漏洞检测。

该系统由集团技术部自研开发，此前仅完成业务功能测试，未开展专业安全测试；且系统多轮迭代过程中，开发人员频繁调整功能逻辑，多个模块的身份鉴权、输入校验机制存在疏漏，已被初步判定存在较高安全风险。

本次漏洞检测为授权合规测试，要求测试人员针对业务系统核心功能模块开展探测与人工验证，精准识别系统存在的 Web 安全漏洞，确认漏洞可利用性，依据《信息安全技术 信息安全风险评估规范》判定风险等级，形成正式漏洞清单，为后续加固整改工作提供精准依据。检测过程中不得篡改业务数据、不得影响系统功能的正常运行。

任务 2：主机与 Web 系统安全加固

完成漏洞检测与风险定级后，安全团队须依据《网络安全等级保护基本要求》（GB/T 22239-2019）三级要求，以及集团《主机安全配置基线》《Web 应用安全开发规范》，针对检测发现的问题开展全维度加固整改：一是 Web 漏洞修复，二是操作系统层面安全基线加固，三是数据库服务安全配置优化。

加固工作须兼顾安全性与业务可用性，所有整改操作不得导致业务系统核心功能失效、普通员工无法正常访问系统。加固完成后须对已识别漏洞进行复测，验证加固措施生效；同时形成完整的加固操作记录，明确每项加固对应的风险点、操作命令/修改内容、验证结果，作为等保测评的整改佐证材料。

任务 3：安全事件应急响应

企业安全运营平台于当日凌晨 02:17 触发多条高危告警：业务服务器出现境外IP异常外联请求、Web访问日志中存在大量恶意扫描与攻击记录、系统后台出现非工作时间的全量用户数据导出行为。经安全团队研判，该

服务器已遭受非法入侵，攻击者疑似利用系统漏洞上传恶意程序，存在核心经营数据泄露风险。

集团立即启动一般网络安全事件应急响应流程，要求应急响应人员立即接入目标服务器开展现场处置，全面排查系统入侵痕迹，还原完整攻击链路，精准定位攻击入口与影响范围，完成攻击遏制与恶意内容清除，恢复系统正常运行状态。最终提交完整的应急响应处置报告，明确事件定级、根因分析、处置过程与长效整改建议。处置过程中须妥善留存原始日志与攻击证据，不得破坏攻击现场原始数据。

任务 4：安全合规与运营审计

该业务系统为等级保护三级备案系统，预计 1 个月后将迎来第三方测评机构的现场测评。同时为完善企业日常安全运营体系，落实日志审计、访问管控等常态化运营要求，安全团队须对照等保合规和本单位要求完成系统自查，并完成基础安全运营配置优化。

本次工作须完成四项核心内容：一是对照等保 2.0 标准中主机安全、应用安全的核心控制项（高风险项）开展合规性检查，识别系统现存的不符合项，输出可落地的整改建议；二是配置操作系统日志、Web 服务日志的留存与轮转策略，满足等保要求的日志留存期限，实现日志规范化、可追溯管理；三是审计当前系统访问控制与权限分配策略，结合最小权限原则提出优化方案，降低日常运营中的越权访问、数据泄露风险；四是针对业务系统导出的敏感数据进行分类分级标注，针对给定的流量包或日志，排查敏

感数据泄露行为。

五、竞赛结果文件提交

1.模块一：使用竞赛平台作答后，在平台直接提交。

2.其它模块（模块二、模块三、模块四）需提交竞赛结果文件。

①制作竞赛结果文件：严格按照 “答题卡.docx”文档格式要求制作输出竞赛结果文件。

②同时在每台设备上备份配置文件，将结果文件分别保存到独立的 TXT 文件中，文件名以设备编号命名（Core1、FW1、IDS、R1 等），并把所有的 TXT 文件存放在“设备配置”文件夹下。

③考生将“答题卡.docx”以及“答题卡.pdf”和“设备配置”文件夹保存到桌面上，以 PDF 为最终评分依据，规定配置文件为设备配置文件完整输出，编码为 UTF-8。

注意：*考生在所提交的文件是竞赛结果的唯一依据，请考生一定确保文件确实有效，能够正常读取。如有疑问，可咨询现场工作人员。*