**第4部分**

操作技能复习题

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置路由器实现网络互连

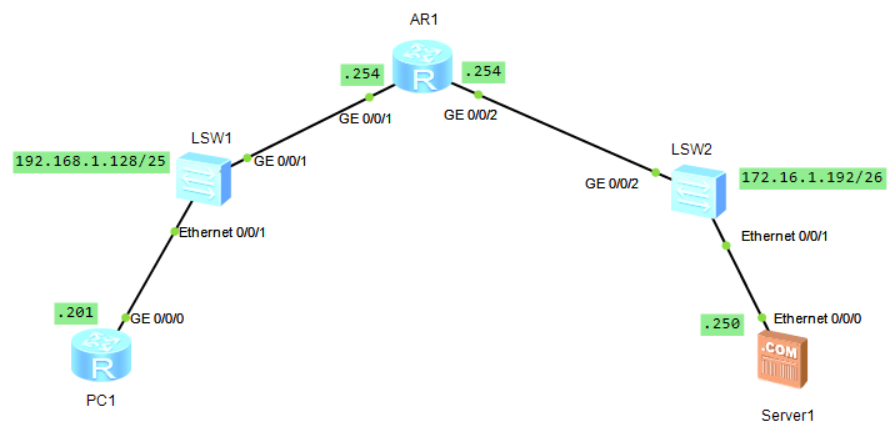
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

图1是某公司网络规划图，需要根据图中规划的IP信息完成网络设备的基础配置，图中使用路由器来模拟PC1,保证PC1能访问Server1，作为公司的IT工程师，需要打开考题四级-1.1.1.paper,完成以下任务：  
（1）配置AR1路由器的主机名为AR1;  
（2）按图1中的信息配置AR1路由器的G0/0/1-G0/0/2接口的IP地址、子网掩码；  
（3）添加AR1路由器的G0/0/1接口描述为inside，G0/0/2接口描述为outside；  
（4）配置AR1路由器第0到第4个vty远程登录的身份验证方式为密码，密码值为Admin@123；  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4\”，并生成答案文件。  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。  
  
  
  
  
图1



**3.**技能要求

（1）能配置网络设备基础IP信息；   
（2）能配置网络设备基础登录信息。

**4.**质量指标

（1）路由器主机名配置正确；   
（2）路由器接口IP配置正确；   
（3）路由器接口描述信息配置正确；   
（4）路由器远程登录身份验证设置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置路由器实现网络互连

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 路由器G0/0/1接口IP地址和子网掩码配置正确； | 根据数据 |  |  |
| M2 | 2 | G0/0/1接口描述配置正确； | 根据数据 |  |  |
| M3 | 3 | 路由器G0/0/2接口IP地址和子网掩码配置正确； | 根据数据 |  |  |
| M4 | 2 | G0/0/2接口描述配置正确； | 根据数据 |  |  |
| M5 | 2 | 路由器的主机名配置正确； | 根据数据 |  |  |
| M6 | 2 | 远程登录的身份验证方式正确； | 根据数据 |  |  |
| M7 | 1 | 密码设置正确。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置三层交换机实现网络互连

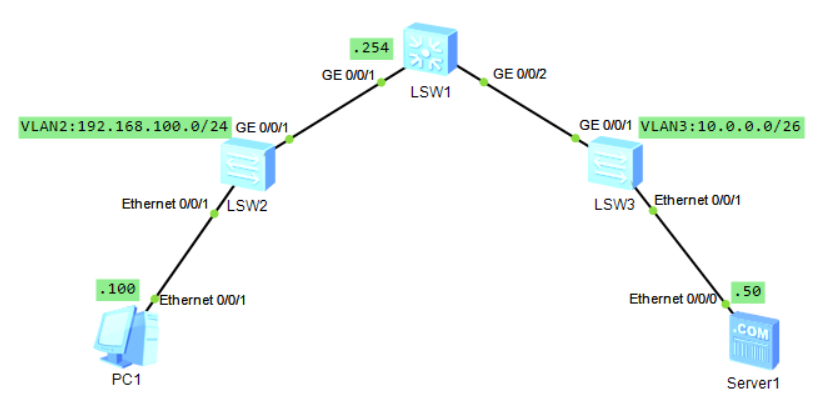
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

图1是某公司的网络拓扑图，根据图中的IP规划信息，对网络设备进行基础配置，确保PC1能够访问Server1。作为公司的IT工程师，需要打开考题四级-1.1.2.paper，完成以下任务：  
（1）按图1信息配置3台交换机的名称；  
（2）按图1信息配置LSW2的VLAN信息；  
（3）按图1信息配置LSW3的VLAN信息；  
（4）按图1信息配置LSW1的VLAN及IP信息；  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4”，并生成答案文件。  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。  
  
图1



**3.**技能要求

（1）能配置网络设备的基础信息；   
（2）能配置网络设备的VLAN信息；   
（3）能配置网络设备的IP信息。

**4.**质量指标

（1）交换机主机名配置正确；   
（2）交换机的VLAN配置正确；   
（3）交换机的IP配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置三层交换机实现网络互连

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | LSW1主机名正确； | 根据数据 |  |  |
| M2 | 2 | LSW1的VLAN配置正确； | 根据数据 |  |  |
| M3 | 1 | LSW1的VLAN2接口IP正确； | 根据数据 |  |  |
| M4 | 1 | LSW1的VLAN3接口IP正确； | 根据数据 |  |  |
| M5 | 1 | LSW1的G0/0/1加入VLAN正确； | 根据数据 |  |  |
| M6 | 1 | LSW1的G0/0/2加入VLAN正确； | 根据数据 |  |  |
| M7 | 1 | LSW2主机名正确； | 根据数据 |  |  |
| M8 | 1 | LSW2的VLAN配置正确； | 根据数据 |  |  |
| M9 | 1 | LSW2的E0/0/1加入VLAN正确； | 根据数据 |  |  |
| M10 | 1 | LSW2的G0/0/1加入VLAN正确； | 根据数据 |  |  |
| M11 | 1 | LSW3主机名正确； | 根据数据 |  |  |
| M12 | 1 | LSW3的VLAN配置正确； | 根据数据 |  |  |
| M13 | 1 | LSW3的E0/0/1加入VLAN正确； | 根据数据 |  |  |
| M14 | 1 | LSW3的G0/0/1加入VLAN正确； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：建立无线网络连接

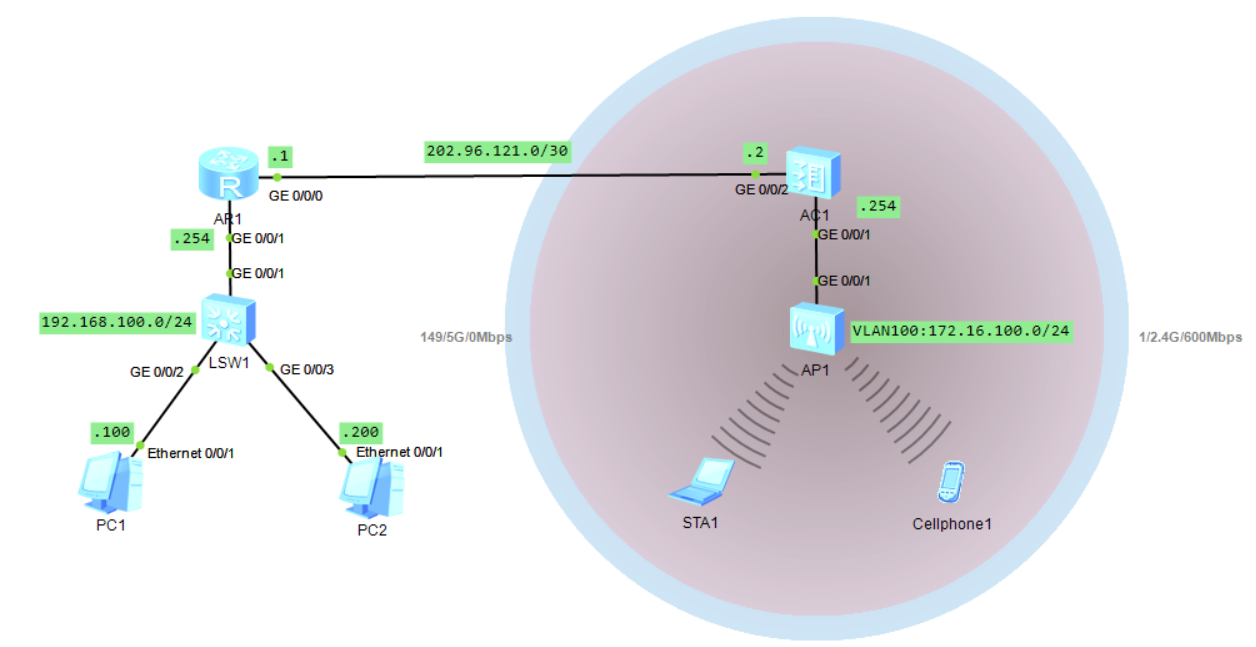
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络架构图如图1所示，基于图中规划的IP信息，我们需要对无线设备进行基本设置，以确保STA1和Cellphone1能够成功互访。作为公司的IT工程师，需打开考题四级-1.1.3.paper，完成以下任务：  
（1）按图1信息配置AC1的VLAN信息，并设置AC连接路由器AR1和AP1的两个接口IP信息（G0/0/2接口属于VLAN200）；  
（2）按图1信息配置AC1到左侧网络的缺省路由；  
（3）按图1信息配置AC1的DHCP信息，确保可以给图中的无线设备分配172.16.100.0/24网段地址；  
（4）配置AC1的无线SSID为office，密码为88888888，加密手段wpa2、psk，加密算法aes；  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4\”，并生成答案文件。  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。  
  
图1



**3.**技能要求

（1）能配置无线设备的IP信息；   
（2）能配置无线设备的路由信息；   
（3）能配置无线设备的DHCP信息；   
（4）能配置无线设备的无线参数。

**4.**质量指标

（1）无线AC的接口IP地址正确；   
（2）无线AC的路由信息正确；   
（3）无线AC的DHCP信息正确；   
（4）无线AC的SSID设置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：建立无线网络连接

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 无线AC的VLAN添加正确； | 根据数据 |  |  |
| M2 | 2 | 无线AC的VLAN100接口IP正确； | 根据数据 |  |  |
| M3 | 2 | 无线AC的G0/0/2接口加入正确VLAN； | 根据数据 |  |  |
| M4 | 2 | 无线AC的VLAN200接口IP正确； | 根据数据 |  |  |
| M5 | 1 | 无线AC的缺省路由配置正确； | 根据数据 |  |  |
| M6 | 1 | 无线AC的DHCP启动正确； | 根据数据 |  |  |
| M7 | 1 | 无线AC的VLAN100接口DHCP配置正确； | 根据数据 |  |  |
| M8 | 1 | 无线AC的SSID模版名称正确； | 根据数据 |  |  |
| M9 | 1 | 无线AC的SSID安全模版正确； | 根据数据 |  |  |
| M10 | 1 | 无线AC的vap-profile调用SSID模版正确； | 根据数据 |  |  |
| M11 | 1 | 无线AC的vap-profile调用安全模版正确。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：建立有线与无线网络连接

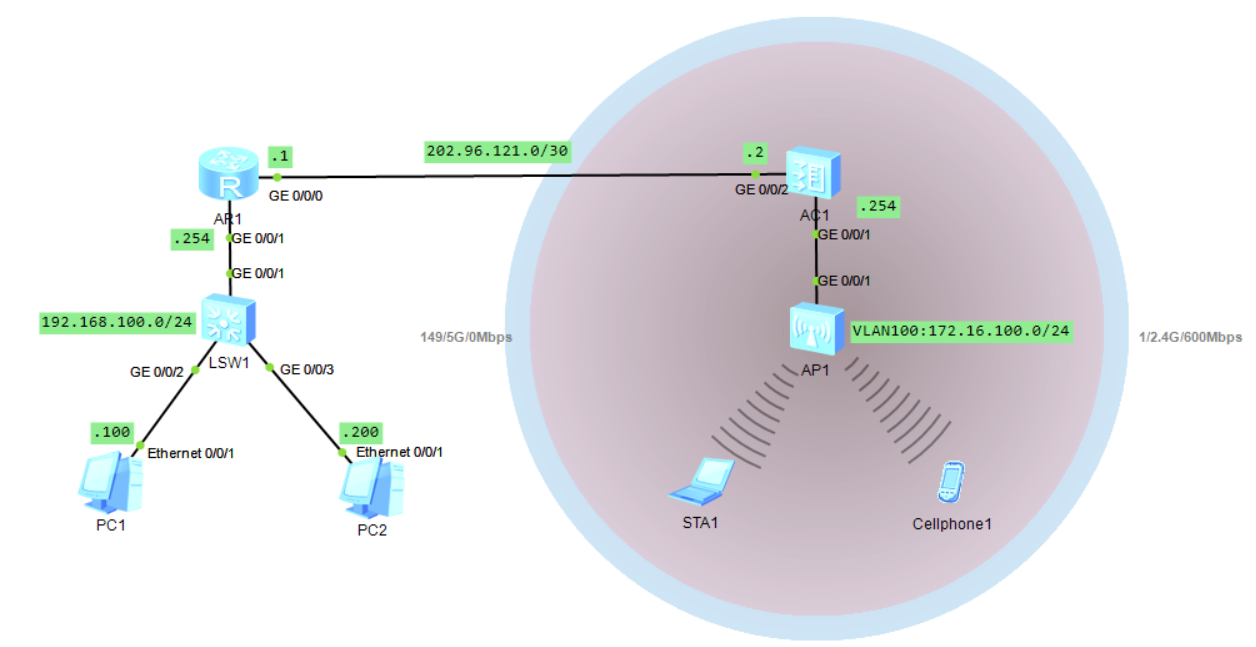
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络架构图如图1所示，基于图中规划的IP信息，需要对网络设备做配置，确保左侧的PC能够访问右侧的无线网络。作为公司的IT工程师，需打开考题四级-1.1.4.paper，完成以下任务：  
（1）按图1信息配置AC1的VLAN信息，并设置AC连接路由器AR1和AP1的两个接口IP信息（G0/0/2接口属于VLAN200）；  
（2）按图1信息配置AR1到右侧网络和AC1到左侧网络的缺省路由；  
（3）按图1信息配置AC1的DHCP信息，确保可以给图中的无线设备分配172.16.100.0/24网段地址；  
（4）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4”，并生成答案文件。  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。  
  
  
  
图1



**3.**技能要求

（1）能配置路由器和无线设备的IP信息；   
（2）能配置路由器和无线设备的路由信息；   
（3）能配置路由器和无线设备的DHCP信息。

**4.**质量指标

（1）路由器和无线AC的接口IP地址正确；   
（2）路由器和无线AC的路由信息正确；   
（3）无线AC的DHCP信息正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：建立有线与无线网络连接

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 路由器的G0/0/0接口IP正确； | 根据数据 |  |  |
| M2 | 2 | 路由器的G0/0/1接口IP正确； | 根据数据 |  |  |
| M3 | 2 | 路由器的缺省路由正确； | 根据数据 |  |  |
| M4 | 2 | 无线AC的VLAN添加正确； | 根据数据 |  |  |
| M5 | 1 | 无线AC的VLAN100接口IP正确； | 根据数据 |  |  |
| M6 | 1 | 无线AC的G0/0/2接口加入正确VLAN； | 根据数据 |  |  |
| M7 | 1 | 无线AC的VLAN200接口IP正确； | 根据数据 |  |  |
| M8 | 2 | 无线AC的缺省路由配置正确； | 根据数据 |  |  |
| M9 | 1 | 无线AC的DHCP启动正确； | 根据数据 |  |  |
| M10 | 1 | 无线AC的VLAN100接口DHCP配置正确； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：交换网络基础安全

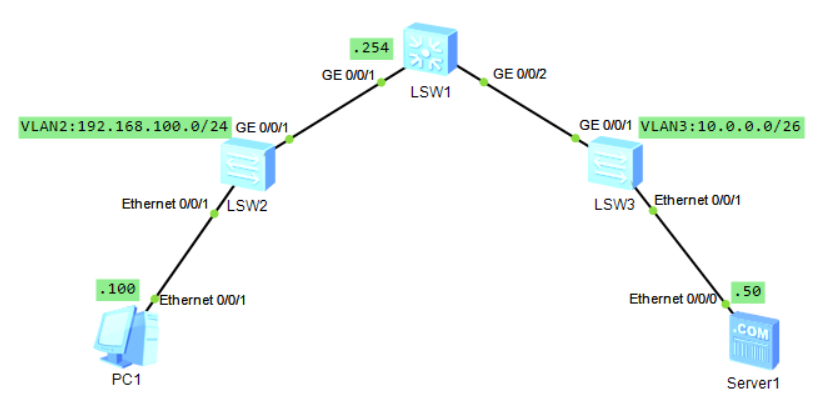
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

图1是某公司的网络拓扑图，根据图中的IP规划信息，对网络设备进行基础配置，确保PC1能够访问Server1。作为公司的IT工程师，需要打开考题四级-1.1.5.paper，完成以下任务：  
（1）按图1信息配置3台交换机的名称;  
（2）按图1信息配置LSW1的VLAN及IP信息；  
（3）配置LSW1的G0/0/1和G0/0/2接口的端口安全，启用MAC地址绑定，并启用接口遇到安全问题就关闭的功能；  
（4）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4”，并生成答案文件。  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。  
  
图1



**3.**技能要求

（1）能配置网络设备的基础信息；   
（2）能配置网络设备的VLAN信息；   
（3）能配置网络设备的IP信息；   
（4）能配置网络设备的基础安全。

**4.**质量指标

（1）交换机主机名配置正确；   
（2）交换机的VLAN配置正确；   
（3）交换机的IP配置正确；   
（4）交换机的端口安全配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：交换网络基础安全

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | LSW1、LSW2主机名正确； | 根据数据 |  |  |
| M2 | 1 | LSW1的VLAN配置正确； | 根据数据 |  |  |
| M3 | 1 | LSW1的VLAN2接口IP正确； | 根据数据 |  |  |
| M4 | 1 | LSW1的VLAN3接口IP正确； | 根据数据 |  |  |
| M5 | 1 | LSW1的G0/0/1加入VLAN正确； | 根据数据 |  |  |
| M6 | 1 | LSW1的G0/0/2加入VLAN正确； | 根据数据 |  |  |
| M7 | 1 | LSW1的G0/0/1端口安全启用正确； | 根据数据 |  |  |
| M8 | 1 | LSW1的G0/0/1端口MAC地址绑定配置正确； | 根据数据 |  |  |
| M9 | 2 | LSW1的G0/0/1端口遇到安全问题就关闭功能配置正确； | 根据数据 |  |  |
| M10 | 1 | LSW1的G0/0/2端口安全启用正确； | 根据数据 |  |  |
| M11 | 1 | LSW1的G0/0/2端口MAC地址绑定配置正确； | 根据数据 |  |  |
| M12 | 2 | LSW1的G0/0/2端口遇到安全问题就关闭功能配置正确； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows 系统密码与账户的安全策略

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

作为网络安全防护人员，为保证公司的Windows服务器系统的账户安全，要进行以下安全加固：  
（1）设置账户策略，要求密码必须满足复杂性要求，设置密码最小长度为 8 个字符，最长使用期限为30天；  
（2）为防止暴力破解，设置账户锁定策略，账户锁定阈值为 5 次，账户锁定时间为 20 分钟并重置；  
（3）建立Administrator1作为陷阱账户，并加入 Guests组，设置密码为 ertg123@，并将该账户禁用；  
（4）建立账户test，设置初始密码 QAZ^12er，将该账户隶属于管理员组。

**3.**技能要求

（1） 能配置系统密码安全策略；   
（2） 能建立伪Administrator1账号并禁用；   
（3） 能建立新用户赋予管理员身份。

**4.**质量指标

（1）账户策略配置正确；   
（2）账户锁定策略配置正确；   
（3）伪Administrator1账号建立并禁用正确；   
（4）新用户test配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows 系统密码与账户的安全策略

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 设置账户策略，要求密码必须满足复杂性要求； | 根据数据 |  |  |
| M2 | 2 | 设置密码最小长度为 8 个字符； | 根据数据 |  |  |
| M3 | 2 | 设置密码最长使用期限为 30 天； | 根据数据 |  |  |
| M4 | 2 | 设置账户锁定策略，账户锁定阈值为 5 次； | 根据数据 |  |  |
| M5 | 2 | 设置账户锁定时间为 20 分钟； | 根据数据 |  |  |
| M6 | 1 | 建立陷阱账户Administrator1； | 根据数据 |  |  |
| M7 | 1 | Administrator1加入Guest组； | 根据数据 |  |  |
| M8 | 1 | Administrator1账户禁用； | 根据数据 |  |  |
| M9 | 1 | 建立test账户； | 根据数据 |  |  |
| M10 | 1 | 设置test账户属于管理组； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Linux 系统密码与账户的安全策略

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

作为网络安全防护人员，为保证公司的CentOS服务器系统的账户安全，要进行以下安全加固：  
（1）为避免使用“root”用户管理系统，需要新建一个用户“user01”，并将该用户添加到系统管理员组中，密码设置为强密码“Tp5@3fm% ”；  
（2）设置用户密码的有效期为90天，密码过期前3天提醒用户；  
（3）用户zf要休假3个月，需要对其账户进行锁定，使之无法登录系统。

**3.**技能要求

（1） 能建立新用户并赋予管理员身份;   
（2） 能配置系统密码安全策略；   
（3） 能对账户进行锁定。

**4.**质量指标

（1）新管理员用户user01配置正确；   
（2）密码策略配置正确；   
（3）账户锁定正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Linux 系统密码与账户的安全策略

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确建立新用户user01； | 根据数据 |  |  |
| M2 | 3 | user01加入root组；（用id user01查看）； | 根据数据 |  |  |
| M3 | 3 | 设置/etc/login.defs文件中密码最长使用期限为 90 天； | 根据数据 |  |  |
| M4 | 3 | 设置/etc/login.defs文件中密码过期前3天提醒用户； | 根据数据 |  |  |
| M5 | 3 | 能对账户zf进行锁定。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows Server 防火墙

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司的服务器内有一套业务系统GMF，为了提升系统安全性，设置Windows系统自带防火墙的出入站规则，要求：  
（1）该业务系统使用 5080/TCP 端口，添加入站规则，开放此端口，规则命名为GMF-in；  
（2）添加此业务系统的出站规则，应用程序路径为D:\kaoshi\_4\1.2.3\gmf.exe，规则命名为GMF-out；  
（3）在防火墙入站规则中，所有文件和打印机共享规则启用，并且只允许安全连接。

**3.**技能要求

（1）能以端口或应用程序方式配置防火墙入站规则;   
（2）能以端口或应用程序方式配置防火墙出站规则。

**4.**质量指标

（1）配置防火墙入站规则正确；   
（2）配置防火墙出站规则正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows Server 防火墙

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 添加入站规则，本地端口正确得2分，协议正确得1分； | 根据数据 |  |  |
| M2 | 3 | 入站规则命名为GMF-in； | 根据数据 |  |  |
| M3 | 3 | 添加出站规则，选择应用程序D:\kaoshi\_4\1.2.3\gmf.exe； | 根据数据 |  |  |
| M4 | 3 | 出站规则命名为GMF-out； | 根据数据 |  |  |
| M5 | 3 | 文件和打印机共享启用只允许安全连接的规则，启用规则得2分，设置安全连接得1分； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Linux防火墙

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

公司有一台重要的Linux服务器，上面运行着关键的应用系统。为了确保这台服务器的安全，你需要对服务器的firewalld防火墙进行详细的配置。具体任务如下：  
（1）配置firewalld，允许访问HTTP服务和HTTPS服务，允许访问21/tcp端口；  
（2）配置firewalld，不允许访问3306/tcp端口；  
（3）以上防火墙规则立即生效；  
（4）列出防火墙规则。

**3.**技能要求

（1）能添加防火墙策略,允许对服务或端口的访问；   
（2）能删除防火墙策略,禁止对服务或端口的访问。

**4.**质量指标

（1）正确配置防火墙允许访问服务；   
（2）正确配置防火墙允许访问端口；   
（3）正确配置防火墙禁止访问其他服务或端口；   
（4）正确列出防火墙允许访问的服务和端口列表。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Linux防火墙

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确配置firewalld允许访问HTTP服务； | 根据数据 |  |  |
| M2 | 3 | 正确配置firewalld允许访问HTTPS服务； | 根据数据 |  |  |
| M3 | 3 | 正确配置firewalld允许访问21/tcp端口； | 根据数据 |  |  |
| M4 | 3 | 正确配置不允许访问3306/tcp端口； | 根据数据 |  |  |
| M5 | 2 | 正确使防火墙立即生效； | 根据数据 |  |  |
| M6 | 1 | 正确列出防火墙规则； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows Server的审核策略

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司需要网络安全防护人员对公司的Windows服务器进行一些安全事件审核的设置，具体包括：  
（1）开启审核策略，对成功和失败的事件都要进行审核；  
（2）对备份和还原权限的使用进行审核；  
（3）对账户锁定策略的成功与失败进行审核；  
（4）对账户登录进行审核；  
（5）对系统完整性为成功与失败进行审核。

**3.**技能要求

（1）能配置Windows各种审核策略。

**4.**质量指标

（1）开启审核策略配置正确；   
（2）启用备份和还原权限的审核策略配置正确；   
（3）对账户锁定的审核策略配置正确；   
（4）对账户登录进行审核；   
（5）系统完整性审核策略配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows Server的审核策略

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 开启审核策略为成功与失败配置正确； | 根据数据 |  |  |
| M2 | 3 | 启用备份和还原权限的审核策略配置正确； | 根据数据 |  |  |
| M3 | 3 | 对账户锁定的审核策略为成功与失败配置正确； | 根据数据 |  |  |
| M4 | 3 | 对账户登录的审核策略为成功与失败配置正确； | 根据数据 |  |  |
| M5 | 3 | 系统完整性审核策略为成功与失败配置正确； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置web应用服务的基本安全防护

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某企业的Windows服务器安装有IIS，现需要对IIS的Web和FTP服务进行安全配置，具体要求如下：   
（1）检查并启动IIS服务（如果未启动）；  
（2）配置IIS服务器，禁用TRACE、ADD和DELETE方法；  
（3）配置FTP服务器，禁用匿名登录；  
（4）配置FTP服务器，禁用全局虚拟目录，对用户访问进行隔离；  
（5）配置FTP服务，指定FTP访问源IP地址为192.168.1.23(拒绝该网段其他地址)。

**3.**技能要求

（1） 能配置Web服务的安全访问；   
（2） 能配置FTP服务的安全访问。

**4.**质量指标

（1）表单验证设置正确；   
（2）TRACE、ADD和DELETE禁用正确；   
（3）匿名登录设置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置web应用服务的基本安全防护

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 检查并启动IIS服务 | 根据数据 |  |  |
| M2 | 1 | 禁用TRACE方法，添加正确； | 根据数据 |  |  |
| M3 | 1 | 禁用ADD方法，添加正确； | 根据数据 |  |  |
| M4 | 1 | 禁用DELETE方法，添加正确； | 根据数据 |  |  |
| M5 | 1 | 配置FTP服务器，禁用匿名登录，设置正确； | 根据数据 |  |  |
| M6 | 1 | 配置FTP服务器，禁用全局虚拟目录； | 根据数据 |  |  |
| M7 | 1 | 对用户访问进行隔离，设置正确； | 根据数据 |  |  |
| M8 | 1 | 配置FTP服务，指定允许访问IP地址为192.168.1.23，设置正确； | 根据数据 |  |  |
| M9 | 1 | 拒绝该网络其他地址192.168.1.0/24，设置正确； | 根据数据 |  |  |
| M10 | 1 | 顺序是允许在前，拒绝在后，设置正确； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows系统下web和FTP应用服务

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

为了满足企业的发展需求，公司需要在Windows服务器系统中搭建 web 站点和FTP站点。具体要求如下：   
（1）检查并启动IIS服务（如果未启动）；   
（2）建立web站点，端口为8080，网站名称1.3.2\_web，首页index.html位于D:\kaoshi\_4\1.3.2\web目录。建完后，用浏览器访问新建网站；  
（3）建立ftp站点，端口为2121，不自动启动ftp站点，ftp名称1.3.2\_ftp，目录为D:\kaoshi\_4\1.3.2\ftp。

**3.**技能要求

（1）能启动IIS服务；   
（2）能新建web站点，访问web站点；   
（3）能新建ftp站点和ftp目录。

**4.**质量指标

（1）正确新建web站点的访问；   
（2）正确新建FTP站点。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows系统下web和FTP应用服务

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 启动IIS服务正确； | 根据数据 |  |  |
| M2 | 1 | web名称正确； | 根据数据 |  |  |
| M3 | 1 | web根目录正确； | 根据数据 |  |  |
| M4 | 1 | web端口正确； | 根据数据 |  |  |
| M5 | 2 | 浏览器能访问web； | 根据数据 |  |  |
| M6 | 1 | ftp不自启动正确； | 根据数据 |  |  |
| M7 | 1 | ftp名称正确； | 根据数据 |  |  |
| M8 | 1 | ftp端口正确； | 根据数据 |  |  |
| M9 | 1 | ftp目录正确； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Linux系统下web应用服务

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

为了满足企业的发展需求，企业需要在Linux服务器系统中搭建一个web 网站，站点所安装的web服务为nginx，具体配置要求如下：  
（1）配置web服务，取消80端口，设置web站点的新访问端口为9000；  
（2）设置站点文件的存放目录为/var/web，里面包含站点的首页index.html，并设置index.html为默认页；  
（3）能启动nginx服务使以上设置生效。

**3.**技能要求

（1）能配置web服务的访问端口；   
（2）能配置web服务的主目录；   
（3）能启动web服务。

**4.**质量指标

（1）正确配置web服务的访问端口；   
（2）正确配置web服务的主目录；   
（3）正确启动web服务。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Linux系统下web应用服务

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确配置取消80端口； | 根据数据 |  |  |
| M2 | 2 | 正确设置新访问端口为9000； | 根据数据 |  |  |
| M3 | 2 | 正确设置主目录local\_root=/var/web； | 根据数据 |  |  |
| M4 | 2 | 正确启动ngnix； | 根据数据 |  |  |
| M5 | 2 | 查看ngnix状态； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置web服务基本防护

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司在对外开放web站点之前，需要做好安全管理，具体要求如下：  
（1）检查并启动IIS服务（如果未启动）。  
（2）配置默认web站点的“IP 地址和域限制”，拒绝IP地址为 192.168.1.100的访问；  
（3）配置默认web站点的访问端口为“9090”；  
（4）配置默认web站点不允许“匿名身份验证”，仅使用“windows 身份验证”，并开启“接受扩展保护”高级功能，启用“内核模式身份验证”。

**3.**技能要求

（1）能配置web站点的IP地址访问限制；   
（2）能配置web站点的访问端口；   
（3）能配置web站点的身份验证。

**4.**质量指标

（1）正确配置web站点的IP地址访问限制；   
（2）正确配置web站点的访问端口；   
（3）正确配置web站点的身份验证

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置web服务基本防护

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确启动IIS； | 根据数据 |  |  |
| M2 | 2 | 正确配置拒绝指定IP地址的访问； | 根据数据 |  |  |
| M3 | 2 | 正确更改默认web站点的访问端口为9090； | 根据数据 |  |  |
| M4 | 1 | 正确设置web站点禁用“匿名身份验证”； | 根据数据 |  |  |
| M5 | 1 | 正确设置web站点启用“windows 身份验证”； | 根据数据 |  |  |
| M6 | 1 | 正确开启“windows 身份验证”的“接受扩展保护”高级功能； | 根据数据 |  |  |
| M7 | 1 | 正确启用“windows 身份验证”的“内核模式身份验证”； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置邮件服务基本防护

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司内部有一台Windows Server服务器，现需要使用hMailServer提供邮件服务，具体要求如下：  
（1）启用日志功能，记录邮件收发协议的日志；  
（2）配置邮件服务器的反病毒功能，对查出病毒的邮件进行删除；  
（3）启用过滤特定附件，并增加一个扩展名是vbs的过滤项。

**3.**技能要求

（1）能启用邮件服务的日志功能，并按要求进行日志记录；   
（2）能配置邮件服务的反病毒功能。

**4.**质量指标

（1）正确启用邮件服务的日志功能，记录SMTP、POP3和IMAP协议的日志；   
（2）正确配置邮件服务的反病毒功能，可以对带病毒的邮件进行删除。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置邮件服务基本防护

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 启用邮件服务的日志功能； | 根据数据 |  |  |
| M2 | 1 | 添加记录SMTP 的日志； | 根据数据 |  |  |
| M3 | 1 | 添加记录POP3 的日志； | 根据数据 |  |  |
| M4 | 1 | 添加记录IMAP的日志； | 根据数据 |  |  |
| M5 | 2 | 配置邮件服务的反病毒功能，可以对带病毒的邮件进行删除； | 根据数据 |  |  |
| M6 | 2 | 启用block attachemnets； | 根据数据 |  |  |
| M7 | 1 | 添加vbs项目； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置交换机VLAN实现网络隔离

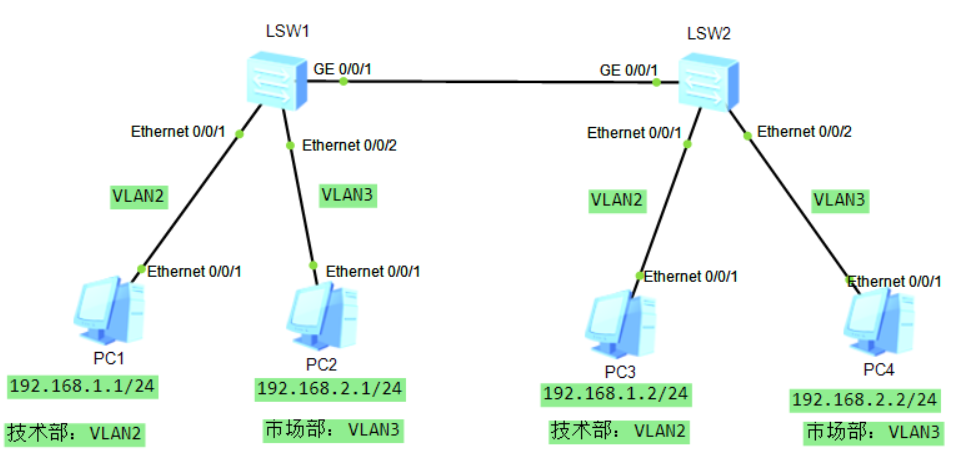
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

图1是某公司网络规划图，打开考题四级-2.1.1.paper，根据图中规划的IP信息完成交换机的VLAN划分，保证同属技术部的PC1和PC3能互相访问，同属市场部的PC2和PC4能互相访问，但技术部和市场部不能直接互相访问，作为公司的IT工程师，需要完成以下任务：  
（1）按图1中的信息添加交换机LSW1和LSW2的VLAN；  
（2）按图1中的信息配置交换机LSW1上与PC1和PC2对应的接口信息；  
（3）按图1中的信息配置交换机LSW2上与PC3和PC4对应的接口信息；  
（4）配置交换机LSW1和LSW2的G0/0/1为Trunk模式。  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4\”，并生成答案文件。  
注意：各设备的IP基础信息请保持跟图1一致。  
  
图1<br>



**3.**技能要求

（1）能划分交换机的VLAN；   
（2）能配置交换机的接口。

**4.**质量指标

（1）交换机的VLAN添加正确；   
（2）交换机LSW1的端口加入VLAN正确；   
（3）交换机LSW2的端口加入VLAN正确；   
（4）交换机的VLAN Trunk配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置交换机VLAN实现网络隔离

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 交换机LSW1的VLAN添加正确； | 根据数据 |  |  |
| M2 | 1 | 交换机LSW2的VLAN添加正确； | 根据数据 |  |  |
| M3 | 1 | 交换机LSW1的E0/0/1端口模式正确； | 根据数据 |  |  |
| M4 | 1 | 交换机LSW1的E0/0/1端口加入VLAN正确； | 根据数据 |  |  |
| M5 | 1 | 交换机LSW1的E0/0/2端口模式正确； | 根据数据 |  |  |
| M6 | 1 | 交换机LSW1的E0/0/2端口加入VLAN正确； | 根据数据 |  |  |
| M7 | 1 | 交换机LSW2的E0/0/1端口加入VLAN正确； | 根据数据 |  |  |
| M8 | 1 | 交换机LSW2的E0/0/2端口加入VLAN正确； | 根据数据 |  |  |
| M9 | 1 | 交换机LSW1的VLAN Trunk配置正确； | 根据数据 |  |  |
| M10 | 1 | 交换机LSW2的VLAN Trunk配置正确。 | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：基于接口划分交换机VLAN

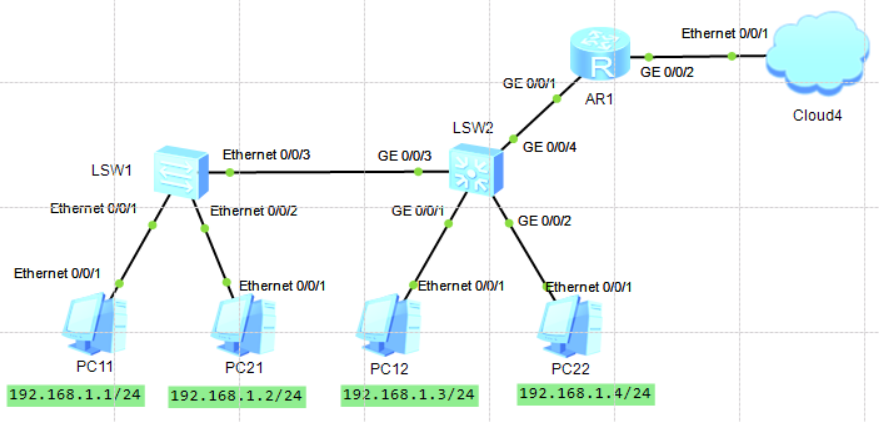
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，LSW1和LSW2是不同楼层的两台交换机，PC11和PC12属于部门1，PC21和PC22属于部门2，假定已经根据图1的IP规划设置好了全部PC机的IP地址、掩码和网关（PC机网关均为192.168.1.254），现要求在LSW1和LSW2交换机上根据图1所示划分基于接口的VLAN，实现部门内的PC机可以互访，不同部门的PC机不能互访。打开四级-2.1.2.paper，完成以下任务：  
（1）在LSW1上创建VLAN10和VLAN20;  
（2）在LSW1上进入接口E0/0/1，设置接口类型为access,允许接口通过VLAN10；  
（3）在LSW1上进入接口E0/0/2，设置接口类型为access,允许接口通过VLAN20；  
（4）在LSW1上进入接口E0/0/3，设置接口类型为trunk，允许接口通过VLAN10和VLAN20；  
（5）在LSW2上创建VLAN10和VLAN20;  
（6）在LSW2上进入接口G0/0/1，设置接口类型为access,允许接口通过VLAN10；  
（7）在LSW2上进入接口G0/0/2，设置接口类型为access,允许接口通过VLAN20；  
（8）在LSW2上进入接口G0/0/3，设置接口类型为trunk，允许接口通过VLAN10和VLAN20；  
（9）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4\”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能划分交换机的VLAN；   
（2）能配置交换机的接口。

**4.**质量指标

（1）交换机的VLAN添加正确；   
（2）交换机LSW1的端口加入VLAN正确；   
（3）交换机LSW2的端口加入VLAN正确；   
（4）交换机的VLAN Trunk配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：基于接口划分交换机VLAN

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 交换机LSW1的E0/0/2接口类型配置正确； | 根据数据 |  |  |
| M2 | 1 | 交换机LSW1的E0/0/2接口加入VLAN配置正确； | 根据数据 |  |  |
| M3 | 1 | 交换机LSW1的E0/0/3接口类型配置正确； | 根据数据 |  |  |
| M4 | 1 | 交换机LSW1的E0/0/3允许通过的VLAN配置正确； | 根据数据 |  |  |
| M5 | 1 | 交换机LSW2的G0/0/1接口类型配置正确； | 根据数据 |  |  |
| M6 | 1 | 交换机LSW2的G0/0/1接口加入VLAN配置正确； | 根据数据 |  |  |
| M7 | 1 | 交换机LSW2的G0/0/2接口类型配置正确； | 根据数据 |  |  |
| M8 | 1 | 交换机LSW2的G0/0/2接口加入VLAN配置正确； | 根据数据 |  |  |
| M9 | 1 | 交换机LSW2的G0/0/3接口类型配置正确； | 根据数据 |  |  |
| M10 | 1 | 交换机LSW2的G0/0/3允许通过的VLAN配置正确。 | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：交换机VLAN绑定PC机的MAC地址

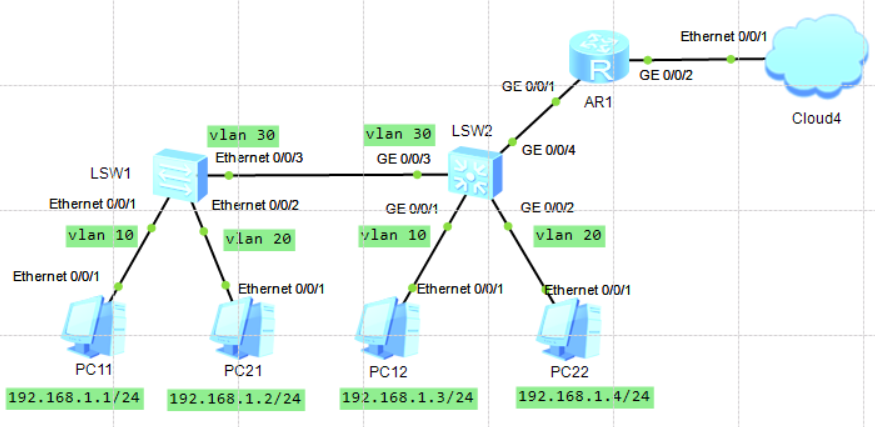
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，LSW1和LSW2是不同楼层的两台交换机，PC11和PC12属于部门1，PC21和PC22属于部门2，假定已经完成了基于端口的VLAN划分，使得部门内的PC机可以互访，不同部门的PC机不能互访。现在为了提高终端的安全性，要求在LSW1和LSW2交换机上，将VLAN跟拓扑图中的PC机MAC地址绑定。打开四级-2.1.3.paper，完成以下任务：  
（1）在LSW1上进入VLAN10,将VLAN10跟PC11的MAC地址54-89-98-C2-80-7C绑定；  
（2）在LSW1上进入VLAN20,将VLAN20跟PC12的MAC地址54-89-98-A9-16-86绑定；  
（3）在LSW1上进入E0/0/1接口，开启基于MAC地址划分VLAN的功能；  
（4）在LSW1上进入E0/0/2接口，开启基于MAC地址划分VLAN的功能；  
（5）在LSW2上进入VLAN10,将VLAN10跟PC12的MAC地址54-89-98-C2-34-6C绑定；  
（6）在LSW2上进入VLAN20,将VLAN20跟PC22的MAC地址54-89-98-27-11-6E绑定；  
（7）在LSW2上进入G0/0/1接口，开启基于MAC地址划分VLAN的功能；  
（8）在LSW2上进入G0/0/2接口，开启基于MAC地址划分VLAN的功能；  
（9）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能将VLAN跟PC机的MAC地址绑定；   
（2）能开启接口基于MAC地址划分VLAN的功能。

**4.**质量指标

（1）PC机的MAC地址查找正确；   
（2）VLAN跟PC机的MAC地址绑定正确；   
（3）开启基于MAC地址划分VLAN的功能正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：交换机VLAN绑定PC机的MAC地址

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 在LSW1上进入VLAN10,将VLAN10跟PC11的MAC地址绑定正确； | 根据数据 |  |  |
| M2 | 1 | 在LSW1上进入VLAN20,将VLAN20跟PC12的MAC地址绑定正确； | 根据数据 |  |  |
| M3 | 2 | 在LSW1上进入E0/0/1接口，正确开启基于MAC地址划分VLAN的功能； | 根据数据 |  |  |
| M4 | 1 | 在LSW1上进入E0/0/2接口，正确开启基于MAC地址划分VLAN的功能； | 根据数据 |  |  |
| M5 | 1 | 在LSW2上进入VLAN10,将VLAN10跟PC12的MAC地址绑定正确； | 根据数据 |  |  |
| M6 | 1 | 在LSW2上进入VLAN20,将VLAN20跟PC22的MAC地址绑定正确； | 根据数据 |  |  |
| M7 | 1 | 在LSW2上进入G0/0/1接口，正确开启基于MAC地址划分VLAN的功能； | 根据数据 |  |  |
| M8 | 1 | 在LSW2上进入G0/0/2接口，正确开启基于MAC地址划分VLAN的功能。 | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置交换机telnet远程登录

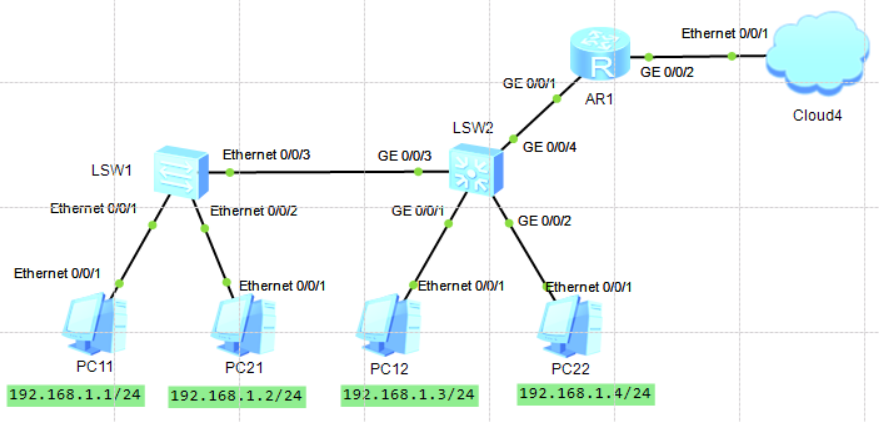
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，LSW2是三层交换机5700，现根据需要，要求配置客户端172.16.1.1能够telnet进行远程管理。打开四级-2.1.4.paper，在LSW2交换机上完成以下任务：  
（1）开启服务器端telnet功能；  
（2）添加编号为2001的acl；  
（3）在acl下面，定义允许远程登录的客户端地址172.16.1.1；  
（4）配置vty用户界面，默认编号范围是0到4；  
（5）在acl中添加telnet协议；  
（6）将编号2001的acl与vty用户界面绑定；  
（7）配置vty用户界面的认证方式为aaa；  
（8）配置客户端telnet登录的用户名为admin123，密码为Admin@1234；  
（9）配置admin123用户只能用于telnet登录；  
（10）配置telnet登录的用户安全级别为3；  
（11）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4\”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能开启服务器端telnet功能；   
（2）能配置telnet功能。

**4.**质量指标

（1）服务器端telnet功能开启正确；   
（2）允许telnet远程登录的客户端地址配置正确；   
（3）允许telnet远程登录的用户名和密码配置正确；   
（4）远程登录的用户安全级别配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置交换机telnet远程登录

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 修改LSW2交换机主机名正确； | 根据数据 |  |  |
| M2 | 1 | 添加编号为2001的acl配置正确； | 根据数据 |  |  |
| M3 | 1 | 定义允许远程登录的客户端地址为172.16.1.1，配置正确； | 根据数据 |  |  |
| M4 | 1 | 进入VTY04用户界面,配置远程登录协议为telnet正确； | 根据数据 |  |  |
| M5 | 1 | 配置编号为2001的acl与vty用户界面绑定正确； | 根据数据 |  |  |
| M6 | 2 | 配置vty用户界面的认证方式为aaa，配置正确； | 根据数据 |  |  |
| M7 | 1 | 进入aaa，telnet登录的用户名和密码配置正确； | 根据数据 |  |  |
| M8 | 1 | admin123用户只能用于telnet登录，配置正确； | 根据数据 |  |  |
| M9 | 1 | admin123用户安全级别配置正确。 | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置路由器stelnet远程登录

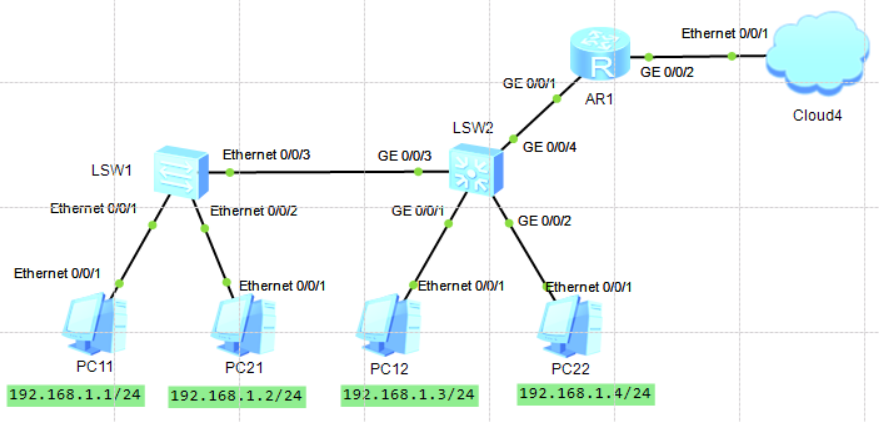
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，AR1是边界路由器，现需要实现stelnet远程管理，要求配置AR1路由器能够stelnet远程登录。打开四级-2.1.5.paper，在AR1路由器上完成以下任务：  
（1）开启服务器端stelnet功能；  
（2）生成本地RSA主机密钥对;  
（3）进入vty用户视图，默认编号范围是0到4；  
（4）设置用户认证方式为aaa；  
（5）设置vty协议只支持ssh；  
（6）进入aaa视图；  
（7）配置客户端stelnet登录的用户名为admin123，密码为Admin@1234；  
（8）配置admin123用户只能用于stelnet登录；  
（9）配置stelnet登录的用户安全级别为3；  
（10）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_4”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能开启服务器端stelnet功能；   
（2）能配置stelnet功能。

**4.**质量指标

（1）服务器端stelnet功能开启正确；   
（2）vty只支持ssh协议配置正确；   
（3）允许stelnet远程登录的用户名和密码配置正确；   
（4）远程登录的用户安全级别配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置路由器stelnet远程登录

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 修改AR1路由器主机名正确； | 根据数据 |  |  |
| M2 | 2 | 开启AR1路由器stelnet功能正确； | 根据数据 |  |  |
| M3 | 2 | 进入vty 0 4用户视图，配置用户认证方式为aaa正确； | 根据数据 |  |  |
| M4 | 2 | 配置vty只支持ssh正确； | 根据数据 |  |  |
| M5 | 1 | 进入aaa视图，配置客户端stelnet登录的用户名为admin123，密码为Admin@1234正确； | 根据数据 |  |  |
| M6 | 1 | 配置admin123用户只能用于stelnet登录； | 根据数据 |  |  |
| M7 | 1 | 配置stelnet登录的用户安全级别正确； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Linux 系统文件的安全设置

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某企业有一台 Linux服务器，现需要在此服务器上的/TestFile目录下存放测试组文档，关于该目录的访问权限，要求如下：  
（1）创建测试组test和测试组负责人leader，创建目录/TestFile，将测试组负责人设为/TestFile目录的所有者，测试组能对/TestFile目录进行任何操作；  
（2）创建上级领导chief，只能查看/TestFile目录中的文件（上级领导不属于测试组test）；  
（3）除了领导chief和测试组用户，其余人员不能查看/TestFile目录。

**3.**技能要求

（1） 能创建用户和组；   
（2） 能设置目录的所有者，以及不同用户对目录的访问权限；   
（3） 能对单个用户设置目录的访问权限。

**4.**质量指标

（1）Linux用户和组创建正确；   
（2）目录所有者和所属组设置正确；   
（3）Chief用户的目录访问权限设置正确；   
（4）其它用户的目录访问权限设置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Linux 系统文件的安全设置

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 正确创建组test； | 根据数据 |  |  |
| M2 | 2 | 正确创建leader用户得1分；leader用户加入test组得1分； | 根据数据 |  |  |
| M3 | 1 | 正确创建目录/TestFile； | 根据数据 |  |  |
| M4 | 1 | 正确配置/TestFile的所有者为leader； | 根据数据 |  |  |
| M5 | 1 | 正确配置测试组能对/TestFile目录进行任何操作， | 根据数据 |  |  |
| M6 | 1 | 正确创建chief用户； | 根据数据 |  |  |
| M7 | 2 | 正确配置chief只能查看/TestFile； | 根据数据 |  |  |
| M8 | 1 | 正确配置剩余人员不能查看/TestFile； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：管理Linux用户和组

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司内部有一台 Linux 服务器，需要在这台服务器上设置多用户登录。  
（1）要求管理员在服务器上创建用户 user1和user2；  
（2）创建测试组 test\_group；  
（3）并且将user1的主属组设为test\_group，将user2所属的附加组设为test\_group。

**3.**技能要求

（1）能创建用户和组；   
（2）能管理用户和组。

**4.**质量指标

（1） 正确创建用户user1、user2；   
（2） 正确创建组test\_group；   
（3） 正确将user1和user2添加到 test\_group 测试组。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：管理Linux用户和组

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确创建用户user1 | 根据数据 |  |  |
| M2 | 2 | 正确创建用户user2 | 根据数据 |  |  |
| M3 | 2 | 正确创建组test\_group | 根据数据 |  |  |
| M4 | 2 | 正确配置user1的主属组为test\_group； | 根据数据 |  |  |
| M5 | 2 | 正确配置user2的附加组为test\_group； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：设置Windows文件的访问权限

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司要求对Windows 系统的文件资源进行访问限制，不同用户对不同的文件具有不同的访问权限。目标文件夹是D:\kaoshi\_4\2.2.4\下的dir\_A、dir\_B和Public文件夹，  
（1）创建Anne和John用户；  
（2）设置dir\_A是Anne的专属文件夹，Anne和管理员可以任意读写各自的文件夹，其他人无法访问；  
（3）设置dir\_B是John的专属文件夹，John和管理员可以任意读写各自的文件夹，其他人无法访问；  
（4）所有Users组成员都可以读取并修改Public文件夹下的文件，但无法删除该文件夹下的文件。

**3.**技能要求

（1） 能创建用户；   
（2） 能设置不同用户对不同文件夹的访问权限。

**4.**质量指标

（1）创建用户正确；   
（2）正确设置文件夹的访问权限。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：设置Windows文件的访问权限

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 创建Anne用户正确； | 根据数据 |  |  |
| M2 | 2 | 创建John用户正确； | 根据数据 |  |  |
| M3 | 2 | dir\_A文件夹的访问权限设置正确得1分，其余用户读写权限正确得·1分； | 根据数据 |  |  |
| M4 | 2 | dir\_B文件夹的访问权限设置正确得1分，其余用户读写权限正确得·1分； | 根据数据 |  |  |
| M5 | 2 | 正确配置Users组对Public文件夹的访问权限； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：设置Linux文件的访问权限

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

一家企业拥有一个开发部门，该部门下设两个项目组：dep1和dep2。现在对组以及权限进行管理要求进行如下操作：  
（1）分别创建2个用户组：dep1、dep2；  
（2）创建用户leaderA,隶属于dep1组，创建用户leaderB,隶属于dep2组；  
（3）在根目录创建2个目录devA、devB；  
（4）设置devA的所有者为leaderA，设置devB的所有者为leaderB；  
（5）通过chmod命令使得devA和devB目录只允许各自组的成员查看和读取，其他组的成员不能访问。

**3.**技能要求

（1） 能创建用户和组；   
（2） 能创建目录；   
（3） 能设置目录的所有者和该目录的访问权限。

**4.**质量指标

（1）创建组dep1和dep2正确；   
（2）创建用户leaderA和leaderB正确；   
（3）创建目录devA和devB正确；   
（4）设置目录devA和devB的所有者正确；   
（5）设置目录devA和devB的访问权限正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：设置Linux文件的访问权限

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 创建组dep1； | 根据数据 |  |  |
| M2 | 1 | 创建组dep2； | 根据数据 |  |  |
| M3 | 1 | 创建用户leaderA，隶属于dep1组； | 根据数据 |  |  |
| M4 | 1 | 创建用户leaderB，隶属于dep2组； | 根据数据 |  |  |
| M5 | 1 | 创建目录devA； | 根据数据 |  |  |
| M6 | 1 | 创建目录devB； | 根据数据 |  |  |
| M7 | 1 | 设置目录devA的所有者为leaderA； | 根据数据 |  |  |
| M8 | 1 | 设置目录devB的所有者为leaderB； | 根据数据 |  |  |
| M9 | 1 | 设置目录devA的访问权限为750； | 根据数据 |  |  |
| M10 | 1 | 设置目录devB的访问权限为750； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：病毒处置和防护

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司的安全运维技术人员发现Windows服务器C:\Windows\Temp有可疑病毒文件123.exe，现需要对其进行处理，任务如下：  
（1）将可疑文件压缩并重命名为“virus.rar”, 然后删除可疑文件；  
（2）导出本机系统日志为evtx格式，压缩并命名为“systemlog.rar”。筛选警告级别的应用程序日志，导出保存txt格式。导出本机注册表信息，压缩并命名为“register.rar”；  
（3）开启系统的Windows Defender的“自动提交示例“。

**3.**技能要求

（1）能发现病毒并对其进行压缩和删除；   
（2）能对系统日志进行备份；   
（3）能对系统注册表进行备份；   
（4）能开启Windows Defender的防护策略。

**4.**质量指标

（1）正确对病毒进行压缩和删除；   
（2）正确对系统日志进行备份；   
（3）正确对系统注册表进行备份；   
（4）正确开启Windows Defender的“自动提交示例”策略。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：病毒处置和防护

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 正确对病毒进行压缩； | 根据数据 |  |  |
| M2 | 1 | 正确删除病毒； | 根据数据 |  |  |
| M3 | 2 | 正确导出系统日志得1分，进行压缩得1分； | 根据数据 |  |  |
| M4 | 2 | 正确筛选出警告级别应用程序日志得1分，导出txt文件得1分； | 根据数据 |  |  |
| M5 | 2 | 正确导出注册表得1分，进行压缩得1分； | 根据数据 |  |  |
| M6 | 2 | 正确设置Windows Defender的“自动提交示例“ | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：解析企业网站域名

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

公司拟自建网站，并已通过域名备案，域名为 x.com.cn ,其所申请的网站www.x.com.cn，ip地址假定为 127.0.0.1，你需要在windows服务器上为其配置DNS记录：  
（1）检查并启动DNS服务（如果未启动）；  
（2）配置DNS服务，增加一个新区域x.com.cn；  
（3）配置DNS服务，为网站 www.x.com.cn 配置主机IP地址为 127.0.0.1；  
（4）将本机ip地址设为DNS服务器地址，使用ping命令验证www.x.com.cn主机dns设置。

**3.**技能要求

（1）能开启DNS服务；   
（2）理解域名解析及相关配置。

**4.**质量指标

（1）正确开启服务；   
（2）正确配置DNS服务器；   
（3）成功添加域名解析记录。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：解析企业网站域名

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确开启DNS服务； | 根据数据 |  |  |
| M2 | 2 | 正确配置DNS主域； | 根据数据 |  |  |
| M3 | 2 | 正确配置网站名称为www； | 根据数据 |  |  |
| M4 | 1 | 正确配置网站ip为127.0.0.1； | 根据数据 |  |  |
| M5 | 2 | 正确配置本机dns服务器地址； | 根据数据 |  |  |
| M6 | 1 | ping命令结果正确； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：备份DNS服务器

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

公司拟自建网站，并已通过域名备案，域名为 x.com.cn ,其所申请的网站www.x.com.cn，ip地址假定为 192.168.0.1，你需要在windows服务器上为其配置DNS解析并进行备份：  
（1）检查并启动DNS服务（如果未启动）；  
（2）配置DNS服务，增加一个新区域x.com.cn，区域文件重新命名为“4.2.3.2”；  
（3）配置DNS服务，为网站 www.x.com.cn 配置主机IP地址为 192.168.0.1；  
（4）备份当前dns数据文件到d:\kaoshi\_4\2.3.2目录下。

**3.**技能要求

（1）能开启DNS服务；   
（2）理解域名解析及相关配置；   
（3）能对DNS数据文件进行备份。

**4.**质量指标

（1）正确开启服务；   
（2）正确配置DNS服务器；   
（3）正确备份DNS数据文件。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：备份DNS服务器

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确开启DNS服务； | 根据数据 |  |  |
| M2 | 2 | 正确配置DNS主域； | 根据数据 |  |  |
| M3 | 1 | 正确设置区域文件名为4.2.3.2； | 根据数据 |  |  |
| M4 | 2 | 正确配置网站名称为www； | 根据数据 |  |  |
| M5 | 1 | 正确配置网站ip为192.168.0.1； | 根据数据 |  |  |
| M6 | 2 | 正确备份dns； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：邮件交换器的域名解析及检查

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

新千公司拟自建网站，并已通过域名备案，域名为 x.com.cn ,其所申请的网站www.x.com.cn，ip地址假定为 127.0.0.1，你需要在服务器上为其配置邮件交换器并用nslookup进行检查：  
（1）检查并启动DNS服务（如果未启动）；  
（2）配置DNS服务，增加一个新区域x.com.cn；  
（3）配置DNS服务，增加主机 dns1.x.com.cn 配置主机IP地址为 127.0.0.1；  
（4）配置DNS服务，增加邮件交换器mail， 配置其主机为dns1.x.com.cn；  
（5）将本机DNS服务器地址设为127.0.0.1，并在命令提示符中启动nslookup进行验证mail.x.com.cn。

**3.**技能要求

（1）能开启DNS服务；   
（2）理解域名解析及web应用配置；   
（3）能操作专门DNS工具软件进行检查。

**4.**质量指标

（1）正确开启服务；   
（2）正确配置DNS服务器；   
（3）成功添加域名解析记录；   
（4）正确用nslookup进行结果验。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：邮件交换器的域名解析及检查

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确开启DNS服务； | 根据数据 |  |  |
| M2 | 2 | 正确配置DNS主域； | 根据数据 |  |  |
| M3 | 2 | 正确配置主机，主机名称正确得1分，主机ip正确得1分； | 根据数据 |  |  |
| M4 | 2 | 正确配置邮件交换器，主机或子域正确得1分，完全限定的域名正确得1分； | 根据数据 |  |  |
| M5 | 2 | 正确使用nslookup； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：企业域名备案

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）模拟备案相关材料与“备案中心”网站。

**2.**工作任务

公司拟自建网站，需要向有关部门进行，域名为 x.com.cn ,其所申请的网站www.x.com.cn，ip地址假定为 127.0.0.1，你需要为其申请备案：  
（1） 使用“备案中心”程序根据备案背景与应用背景信息，使用置于桌面的“备案材料”文件夹中的资料填写备案信息；  
（2） 备案背景：新千公司位于上海市长宁区 535号，公司性质为“民营企业”，持有“营业执照”，统一社会信用代码为“4350931216019”；应用计划使用域名“x.com.cn”，公司法人兼主体负责人为“马飞”，手机号码为“13501763375”与“13916378667”，电子邮件地 址 为 “mafei@ x.com.cn ”， 持 “ 居 民 身 份 证 ”， 证 件 号 码 为“110101198707158199”；网站负责人为“晓飞，手机号码为“13001763376”与“13016378668”，电子邮件地址为“xiaofei@ x.com.cn”，持“居民身份证”，证件号码为“110101198707159263”；  
（3） 应用背景：应用“新千在线”以“综合门户网站”的形式向客户提供24 小时的在线服务，网站语言使用“简体中文”。

**3.**技能要求

（1） 能对企业域名进行备案。

**4.**质量指标

（1） 正确对企业域名进行备案。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：企业域名备案

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确填写网站域名； | 根据数据 |  |  |
| M2 | 2 | 正确填写公司信息； | 根据数据 |  |  |
| M3 | 2 | 正确填写法人信息； | 根据数据 |  |  |
| M4 | 2 | 正确填写负责人信息； | 根据数据 |  |  |
| M5 | 2 | 正确描述网站功能 | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：网站及邮件服务器备份

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

你作为信息安全管理员负责维护一家公司的内部网站和邮件服务。最近，公司决定升级其服务器硬件，为了确保迁移过程中的数据完整性和服务连续性，需要制定一套详尽的备份计划，包括 IIS 应用池、站点配置、网站目录文件以及邮件服务器配置和内容的备份：  
（1）使用命令导出iis应用程序池，应用程序池名为my\_pool，导出路径为D:\kaoshi\_4\2.3.5\my\_pool.xml；  
（2）使用命令导出iis站点，站点名为my\_web，导出路径为D:\kaoshi\_4\2.3.5\my\_web.xml；  
（3）my\_web站点下的文件打包压缩成zip文件，保存在D:\kaoshi\_4\2.3.5\web.zip；  
（4）备份导出hMailServer邮件服务器的设置，域名，信息，不压缩文件，导出路径为D:\kaoshi\_4\2.3.5。

**3.**技能要求

（1）能导出网站配置文件；   
（2）能打包网站资源文件；   
（3）能导出邮件服务器配置以及内容。

**4.**质量指标

（1）导出网站命令正确，导出路径正确；   
（2）正确压缩网站资源文件；   
（3）正确导出邮件服务器配置以及内容。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：网站及邮件服务器备份

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确导出应用程序池； | 根据数据 |  |  |
| M2 | 1 | 应用程序池导出路径正确； | 根据数据 |  |  |
| M3 | 2 | 正确导出站点配置文件； | 根据数据 |  |  |
| M4 | 1 | 站点配置文件导出路径正确； | 根据数据 |  |  |
| M5 | 1 | 正确打包网站资源文件； | 根据数据 |  |  |
| M6 | 1 | 正确导出邮件服务器设置； | 根据数据 |  |  |
| M7 | 1 | 正确导出邮件服务器域名； | 根据数据 |  |  |
| M8 | 1 | 正确导出邮件服务器域名信息； | 根据数据 |  |  |
| 合计配分 | 10 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障

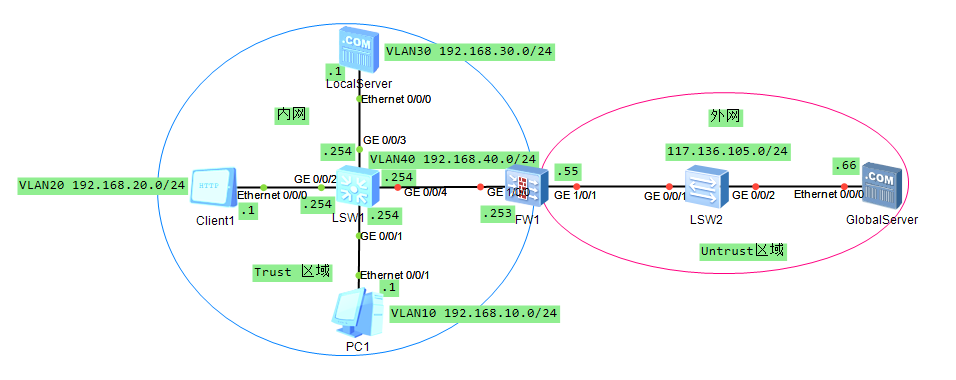
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

图1是某公司网络结构，因规划调整导致网络出现了部分的访问故障，作为公司的IT工程师，请打开3.1.1.paper完成以下任务来识别并解决故障：  
（1）PC1无法访问Client1，请利用诊断工具ping命令识别故障，并解决故障；  
（2）PC1无法访问LocalServer，请利用诊断工具ping、tracert等命令识别故障，并解决故障；  
（3）尝试切换PC1的TCP/IP参数为自动获取，验证能否成功。如获取失败，请识别故障并解决故障；  
（4）请保存PC1的ipconfig命令结果、PC1成功访问LocalServer的ping命令与结果、PC1成功访问LocalServer的ping命令与结果共3部分内容在3.1.1.txt文件，并将该文件储存在D:\kaoshi\_4\目录；同时将LSW1的配置信息保存至上述文件内（3.1.1.txt）；  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码，FW1登录账号及密码为admin/12345.Com。  
  
图1



**3.**技能要求

（1）能使用诊断工具ping命令；   
（2）能使用诊断工具tracert命令；   
（3）能配置PC及服务器IP基础设置；   
（4）能配置网络设备VLAN基础设置。

**4.**质量指标

（1）交换机LSW1的IP基础配置正确；   
（2）PC1能成功访问Client1；   
（3）PC1能成功访问LocalServer；   
（4）PC1能成功自动获取TCP/IP参数。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | PC1的TCP/IP 参数配置正确： 192.168.10.1/24 (网关192.168.10.254) | 根据数据 |  |  |
| M2 | 2 | Client1的TCP/IP 参数配置正确： 192.168.20.1/24 (网关192.168.20.254) | 根据数据 |  |  |
| M3 | 2 | LocalServer的TCP/IP 参数配置正确： 192.168.30.1/24 (网关192.168.30.254) | 根据数据 |  |  |
| M4 | 2 | LSW1 VLAN信息、SVI接口信息正确 interface GigabitEthernet0/0/3 port link-type access port default vlan 3 | 根据数据 |  |  |
| M5 | 2 | LSW1的DHCP配置信息正确 Dhcp enable Ip pool vlan10 Network 192.168.10.0 mask 24 Gateway-list 192.168.10.254 Dns-list 192.168.30.1 Int vlan 10 Dhcp select global | 根据数据 |  |  |
| M6 | 1 | Client1的IP地址正确 | 根据数据 |  |  |
| M7 | 2 | 3.1.1.txt文件存在且内容正确 | 根据数据 |  |  |
| M8 | 2 | LSW1的配置文件存在且内容正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（VLAN间路由）

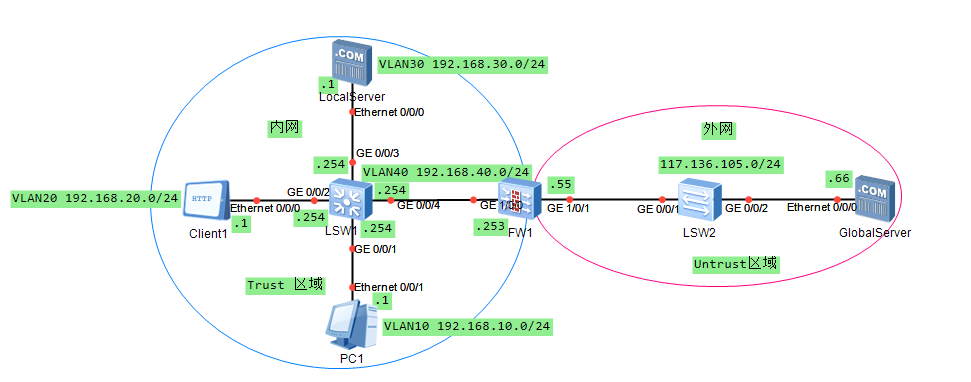
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

图1是某公司网络结构，因规划调整导致网络出现了部分的访问故障，作为公司的IT工程师，请打开3.1.2.paper完成以下任务来识别并解决故障。  
（1）PC1无法访问Client1，请利用诊断工具ping命令识别故障，并解决故障；  
（2）PC1无法访问LocalServer，请利用诊断工具ping命令识别故障，并解决故障；  
（3）LocalServer上运行了HTTP服务，并设置了web站点www.abc.com，Client1也无法访问LocalServer上的网站，请利用诊断工具ping命令结合LocalServer上DNS服务器配置信息识别故障，并解决故障；  
（4）请保存PC1的ipconfig命令结果、PC1成功访问Client1的ping命令与结果、PC1成功访问LocalServer的ping命令与结果、PC1成功访问LocalServer网站的命令与结果（ping www.abc.com）共4部分内容存放在3.1.2.txt文件中，并将该文件储存在D:\kaoshi\_4\目录，同时将LSW1的配置信息保存至上述文件内（3.1.2.txt）；  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码，FW1登录账号及密码为admin/12345.Com。  
  
图1



**3.**技能要求

（1）能配置PC机的IP地址、掩码及网关   
（2）能使用诊断工具ping命令；   
（3）能使用诊断工具tracert命令；   
（4）能维护交换机VLAN配置信息；   
（5）能配置交换机SVI接口实现VLAN间路由。

**4.**质量指标

（1）正确配置计算机的IP地址、掩码、网关及DNS地址；   
（2）正确配置交换机LSW1实现VLAN间路由；   
（3）PC1能成功访问Client1；   
（4）PC1能成功访问LocalServer；   
（5）PC1能成功访问www.abc.com网站。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（VLAN间路由）

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | PC1、Client网关设置正确 | 根据数据 |  |  |
| M2 | 2 | LocalServer DNS服务配置正确 | 根据数据 |  |  |
| M3 | 2 | LSW1 VLAN配置正确 Vlan 3 interface G0/0/3 port link-type access port default vlan 3 | 根据数据 |  |  |
| M4 | 2 | LSW1 SVI接口配置正确 Int vlan 3 Ip add 192.168.30.254 24 | 根据数据 |  |  |
| M5 | 2 | 查看3.1.2.txt文档，内容包含PC1的IP信息正确、PC1访问Client1信息正确 | 根据数据 |  |  |
| M6 | 2 | 查看3.1.2.txt文档，内容PC1访问Local Server信息正确 | 根据数据 |  |  |
| M7 | 1 | PC1能成功访问LocalServer网站： | 根据数据 |  |  |
| M8 | 2 | LSW1配置文件存在 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（内网访问防火墙本地）

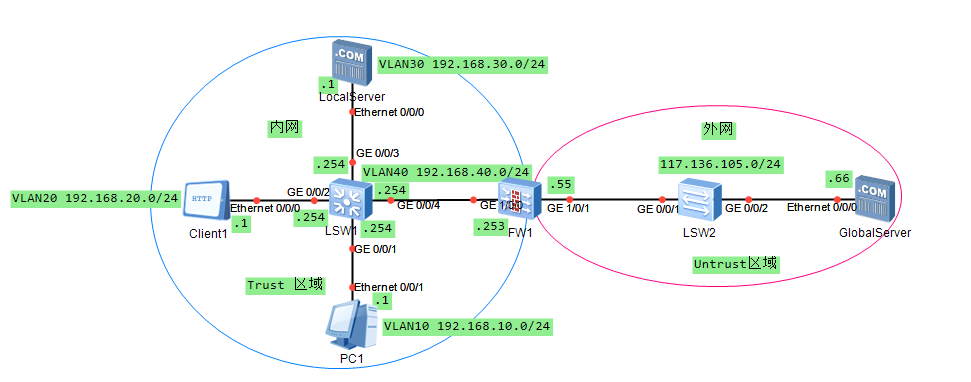
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

图1是某公司网络结构，因规划调整导致网络出现了部分的访问故障，作为公司的IT工程师，请打开3.1.3.paper完成以下任务来识别并解决故障：  
（1）PC1无法访问LocalServer，请利用诊断工具ping命令识别故障，并解决故障；  
（2）LocalServer上运行了HTTP服务，并设置了web站点www.abc.com，Client1也无法访问LocalServer上的网站，请利用诊断工具ping、tracert等命令识别故障， 并解决故障；  
（3）PC1无法访问FW1（内网接口），请利用诊断工具ping命令识别故障，并解决故障；  
（4）请保存PC1的ipconfig命令结果、PC1成功访问LocalServer的ping命令与结果、PC1成功访问LocalServer网站的命令与结果（ping www.abc.com）、PC1成功ping访问FW1内网接口的命令和结果共4部分内容存放在3.1.3.txt文件中，并将该文件储存在D:\kaoshi\_4\目录;同时保存LSW1和FW1的配置文件至上述文件内（3.1.3.txt）；  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码，FW1登录账号及密码为admin/12345.Com。  
  
图1



**3.**技能要求

（1）能使用诊断工具ping命令；   
（2）能配置SVI接口实现VLAN间路由；   
（3）能配置静态路由实现内网和FW1之间数据双向访问；   
（4）能配置防火墙FW1的接口地址、区域及安全策略。

**4.**质量指标

（1）能正确配置LSW1的VLAN信息及SVI接口；   
（2）能正确防火墙FW1的接口、区域及安全策略；   
（3）PC1能成功访问LocalServer；   
（4）PC1能成功访问FW1。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（内网访问防火墙本地）

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | PC1网关设置正确、LocalServer DNS服务配置正确 | 根据数据 |  |  |
| M2 | 2 | LSW1 VLAN配置正确 Vlan 3 interface G0/0/3 port link-type access port default vlan 3 | 根据数据 |  |  |
| M3 | 2 | LSW1 SVI接口配置正确 Int vlan 3 Ip add 192.168.30.254 24 | 根据数据 |  |  |
| M4 | 2 | FW1路由配置正确 Ip route-static 192.168.10.0 255.255.255.0 192.168.40.254 Ip route-static 192.168.20.0 255.255.255.0 192.168.40.254 Ip route-static 192.168.30.0 255.255.255.0 192.168.40.254 | 根据数据 |  |  |
| M5 | 2 | FW1接口、区域配置正确 FW1本地接口安全策略配置正确 Int g0/0/0 Service-manage all permit | 根据数据 |  |  |
| M6 | 2 | 查看3.1.3.txt文档，内容正确 | 根据数据 |  |  |
| M7 | 1 | LSW1配置文件存在，内容正确 | 根据数据 |  |  |
| M8 | 2 | FW1配置文件存在，内容正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（内网访问外网）

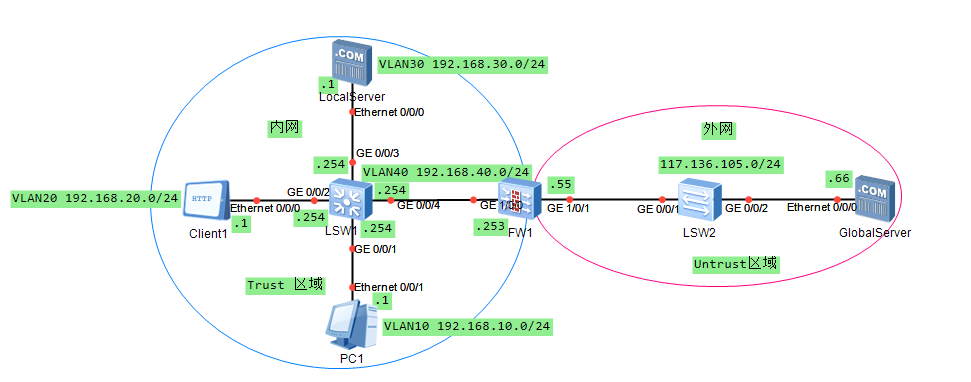
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

图1是某公司网络结构，因规划调整导致网络出现了部分的访问故障，作为公司的IT工程师，请打开3.1.4.paper完成以下任务来识别并解决故障：  
（1）PC1无法访问Client1，请利用诊断工具ping命令识别故障，并解决故障；  
（2）LocalServer上运行了HTTP服务，并设置了web站点www.abc.com，PC1无法访问LocalServer上的网站，请利用诊断工具ping、tracert等命令识别故障，并解决故障；  
（3）PC1无法访问GlobalServer，请检查FW1的配置信息并进行故障排查；  
（4）请保存PC1的ipconfig命令结果、PC1成功访问Client1的ping命令与结果、PC1成功访问LocalServer网站的ping命令和结果（ping www.abc.com）、PC1成功访问GlobalServer的ping命令和结果共4部分内容存放在3.1.4.txt文件中，并将该文件储存在D:\kaoshi\_4\目录;同时将LSW1和FW1的配置信息保存至上述文件内（3.1.4.txt）；  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码，FW1登录账号及密码为admin/12345.Com。  
  
图1



**3.**技能要求

（1）能使用诊断工具ping、tracert命令；   
（2）能配置PC及服务器IP网络参数；   
（3）能配置防火墙的接口网络参数、区域；   
（4）能配置防火墙NAT网络地址转换功能；   
（5）能配置防火墙的安全策略。

**4.**质量指标

（1）正确配置计算机的IP地址、掩码、网关及DNS地址；   
（2）正确配置交换机的VLAN及SVI接口信息；   
（3）正确配置防火墙FW1的NAT网络地址转换；   
（4）正确配置防火墙的安全访问策略。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（内网访问外网）

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | PC1网关设置正确、LocalServer DNS服务配置正确 | 根据数据 |  |  |
| M2 | 2 | LSW1 SVI接口配置正确 Int vlan 3 Ip add 192.168.30.254 24 | 根据数据 |  |  |
| M3 | 2 | LSW1 缺省路由配置正确 Ip route 0.0.0.0 0.0.0.0 192.168.40.253 | 根据数据 |  |  |
| M4 | 2 | FW1路由配置正确 Ip route-static 192.168.10.0 255.255.255.0 192.168.40.254 | 根据数据 |  |  |
| M5 | 2 | FW1 NAT策略配置正确 | 根据数据 |  |  |
| M6 | 2 | 查看3.1.4.txt文档，内容正确 | 根据数据 |  |  |
| M7 | 1 | LSW1配置文件存在，内容正确 | 根据数据 |  |  |
| M8 | 2 | FW1配置文件存在，内容正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（内网服务器端口映射）

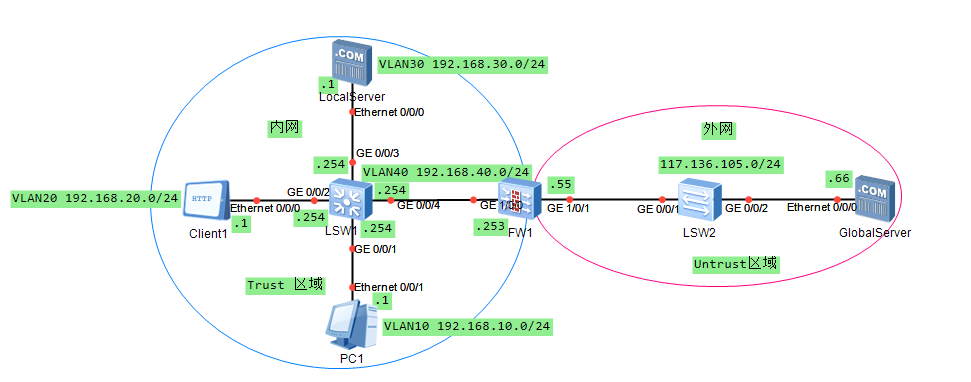
考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

图1是某公司网络结构，因规划调整导致网络出现了部分的访问故障，作为公司的IT工程师，请打开3.1.5.paper完成以下任务来识别并解决故障：  
（1）PC1无法访问Client1，请利用诊断工具ping命令识别故障，并解决故障；  
（2）PC1无法访问GlobalServer，请利用诊断工具ping命令识别故障，并解决故障；  
（3）公司拟采用端口映射的方案方便公司在外出差用户也能够访问内网服务器（假定映射FW1外网接口8080端口），请检查FW1等设备的配置信息识别故障， 并解决故障；  
（4）请保存PC1的ipconfig命令结果、PC1成功访问Client1的ping命令与结果、PC1成功访问GlobalServer的ping命令与结果、出差用户远程访问内网LocalServer的网站结果（日志信息）共4部分内容存放在3.1.5.txt文件中，并将该文件储存在D:\kaoshi\_4\，同时将LSW1和FW1的配置信息保存至上述文件内（3.1.5.txt）；  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码，FW1登录账号及密码为admin/12345.Com。  
  
  
  
图1



**3.**技能要求

（1）能使用诊断工具ping、tracert命令；   
（2）能配置交换机SVI接口实现VLAN间路由；   
（3）能配置FW1通过NAT方式上网；   
（4）能配置FW1的端口映射实现远程访问。

**4.**质量指标

（1）正确配置计算机的IP地址、掩码、网关及DNS地址；   
（2）正确配置交换机实现VLAN间通信；   
（3）正确配置防火墙实现NAT技术上网；   
（4）正确配置防火墙端口映射。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用诊断工具识别并处理网络故障（内网服务器端口映射）

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | PC1网关设置正确、LocalServer DNS服务配置正确 | 根据数据 |  |  |
| M2 | 2 | FW1接口区域设置 Firewall zone trust Add Int g1/0/0 Firewall zone untrust Add Int g1/0/1 | 根据数据 |  |  |
| M3 | 2 | FW1路由配置正确 Ip route-static 192.168.10.0 255.255.255.0 192.168.40.254 Ip route-static 192.168.30.0 255.255.255.0 192.168.40.254 | 根据数据 |  |  |
| M4 | 2 | FW1内网用户上网NAT策略配置正确 | 根据数据 |  |  |
| M5 | 2 | FW1内网用户上网NAT策略对应的安全策略配置正确 | 根据数据 |  |  |
| M6 | 2 | FW1内网服务器端口映射配置正确 | 根据数据 |  |  |
| M7 | 2 | FW1内网服务器端口映射功能对应的安全策略配置正确 | 根据数据 |  |  |
| M8 | 1 | 查看3.1.5.txt文档，内容正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用系统工具还原系统及应用数据

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司的公共应用数据因误操作导致了部分丢失，作为公司的IT工程师，需要完成以下任务来恢复数据，同时设置自动备份来保障数据的安全：  
（1）利用服务器管理器安装“Windows Server 备份”功能；  
（2）使用“Windows Server备份”功能手工恢复应用数据，恢复到原始位置；  
（3）利用任务计划程序制定名为auto-bk的任务计划，每周三、五的23:00运行自动备份项目资料的脚本（脚本存放路径：d:\kaoshi\_4\3.2.1\autobk.bat）。

**3.**技能要求

（1）能安装数据备份工具；   
（2）能利用数据备份工具恢复数据；   
（3）能制定数据自动备份任务计划。

**4.**质量指标

（1）数据备份工具安装正确；   
（2）数据恢复正确；   
（3）数据自动备份任务计划配置正确。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用系统工具还原系统及应用数据

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | Windows server 备份功能安装正确，服务器管理器中的工具里存在windows server备份菜单； | 根据数据 |  |  |
| M2 | 2 | 能成功打开windows server备份配置界面； | 根据数据 |  |  |
| M3 | 2 | 应用数据恢复日志存在； | 根据数据 |  |  |
| M4 | 2 | 数据恢复成功，C盘存在项目资料目录，目录中存在投标文件.zip文件； | 根据数据 |  |  |
| M5 | 2 | 投标文件.zip文件大小跟上次备份的文件大小一致； | 根据数据 |  |  |
| M6 | 1 | 自动备份任务计划名称为auto-bk； | 根据数据 |  |  |
| M7 | 1 | 任务计划时间为每周三、五的23点； | 根据数据 |  |  |
| M8 | 2 | 自动备份的脚本添加正确； | 根据数据 |  |  |
| M9 | 2 | 任务计划的状态为正在运行； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：设置防病毒软件并检查系统威胁

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

为了提升公司的业务效率和系统安全性，公司IT管理员决定进行一次服务器安全审查。为有效减少潜在的安全威胁，现计划对服务器执行病毒扫描和清理工作。以下是具体的实施要求：  
（1）启用Windows Defender的实时保护功能、基于云的保护、自动提交示例；  
（2）使用Windows Defender对系统“d:\”进行自定义扫描，在选择自定义目录时候截图；  
（3）查看扫描到的潜在威胁，点击显示详细信息，选择“删除”操作，删除完成后截图；

**3.**技能要求

（1）能设置Windows Defender实时保护功能；   
（2）能使用Windows Defender进行快速扫描；   
（3）能处置潜在威胁文件或程序。

**4.**质量指标

（1）正确开启Windows Defender实时保护功能；   
（2）正确执行Windows Defender进行快速扫描；   
（3）正确处置潜在威胁文件或程序。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：设置防病毒软件并检查系统威胁

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确开启Windows Defender实时保护功能； | 根据数据 |  |  |
| M2 | 2 | 正确开启基于云的保护； | 根据数据 |  |  |
| M3 | 2 | 正确开启自动提交示例； | 根据数据 |  |  |
| M4 | 3 | Windows Defender对自定义路径进行扫描； | 根据数据 |  |  |
| M5 | 2 | 查找到威胁； | 根据数据 |  |  |
| M6 | 3 | 删除威胁； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：使用防病毒工具检查系统威胁并执行计划性扫描

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

为了提升公司的业务效率和系统安全性，公司IT管理员决定进行一次服务器安全审查。为有效减少潜在的安全威胁，现计划对服务器执行病毒扫描和清理工作。以下是具体的实施要求：  
（1）打开Windows Defender程序，开启实时保护功能；  
（2）使用Windows Defender对系统“d:\”进行自定义扫描，在选择自定义目录时候截图；  
（3）查看扫描到的潜在威胁，点击显示详细信息，选择“删除”操作，删除完成后截图；  
（4）启用Windows计划任务，设置每周六晚上22：00自动执行服务器完全扫描。

**3.**技能要求

（1）能设置Windows Defender实时保护功能；   
（2）能使用Windows Defender进行快速扫描；   
（3）能处置潜在威胁文件或程序；   
（4）能配置Windows Defender定期扫描计划任务。

**4.**质量指标

（1）正确开启Windows Defender实时保护功能；   
（2）正确执行Windows Defender进行快速扫描；   
（3）正确处置潜在威胁文件或程序；   
（4）正确配置Windows Defender定期扫描计划任务。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：使用防病毒工具检查系统威胁并执行计划性扫描

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确开启Windows Defender实时保护功能 | 根据数据 |  |  |
| M2 | 1 | Windows Defender实时保护操作截图存在 | 根据数据 |  |  |
| M3 | 2 | 正确执行Windows Defender进行快速扫描 | 根据数据 |  |  |
| M4 | 2 | Windows Defender自定义扫描操作截图存在 | 根据数据 |  |  |
| M5 | 2 | 正确处置潜在威胁文件或程序 | 根据数据 |  |  |
| M6 | 2 | 处置潜在威胁文件或程序操作截图存在 | 根据数据 |  |  |
| M7 | 2 | 正确配置Windows Defender定期扫描计划任务 | 根据数据 |  |  |
| M8 | 2 | Windows Defender定期扫描计划任务截图存在 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：使用Windows Defender设置排除项以及自定义扫描

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

近期，公司网络安全部门接到了一则报告，称有员工可能不小心下载了一个来自不可信来源的文件，并怀疑该文件可能包含恶意代码。为了防止恶意代码对公司网络造成损害，你需要立即采取行动。以下是具体的实施要求：  
（1）打开Windows Defender程序，开启实时保护功能，以及增强型通知功能；  
（2）添加Defender的扫描排除项，排除目录C:\Windows\Boot,排除扩展名包括txt、jpg、png；  
（3）对C:\Windows\SysWOW64进行一次自定义扫描，在选择自定义目录时候截图，对扫描结果进行截图；

**3.**技能要求

（1）能设置Windows Defender实时保护功能；   
（2）能配置Windows Defender扫描排除项；   
（3）能使用Windows Defender进行自定义扫描。

**4.**质量指标

（1）正确开启Windows Defender实时保护功能；   
（2）正确配置Windows Defender扫描排除项；   
（3）正确执行Windows Defender自定义扫描。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：使用Windows Defender设置排除项以及自定义扫描

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确开启Windows Defender实时保护功能； | 根据数据 |  |  |
| M2 | 2 | 正确开启增强型通知； | 根据数据 |  |  |
| M3 | 2 | 正确设置目录排除项； | 根据数据 |  |  |
| M4 | 3 | 正确设置扩展名排除项，存在jpg得1分，存在png得1分，存在txt得1分； | 根据数据 |  |  |
| M5 | 3 | 自定义扫描位置正确； | 根据数据 |  |  |
| M6 | 3 | 完成一次自定义扫描； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（四级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：使用Windows日志分析识别常见系统安全事件

考核时间：15min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

作为公司的系统管理员，需要负责监控和分析Windows服务器的安全日志。最近，系统管理员注意到服务器上可能存在一些异常活动。系统管理员准备分析Windows安全日志，识别出常见的系统安全事件，并给出相应的处理建议。具体要求如下：  
（1）使用Windows事件查看器（Event Viewer）打开安全日志；  
（2）筛选出登录成功的安全事件,导出txt结果保存到d:\kaoshi\_4\3.2.5-1.txt；  
（3）筛选出登录失败的安全事件,导出txt结果保存到d:\kaoshi\_4\3.2.5-2.txt；  
（4）设置Windows系统组策略安全设置：账户锁定策略，当用户输错超过3次密码，自动锁定账户，30分钟后解除锁定。

**3.**技能要求

（1）能正确打开Windows事件查看器，并能导航到安全日志部分；   
（2）能通过事件ID筛选出系统登录安全事件；   
（3）能对异常情况的识别分析；   
（4）能设置系统账户安全策略。

**4.**质量指标

（1）能正确打开Windows事件查看器；   
（2）能准确识别并描述每个事件ID对应的系统安全事件；   
（3）能对异常情况的分析准确，并能识别出潜在的安全威胁；   
（4）能设置合理的策略降低潜在的安全风险。

**信息安全管理员（四级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：使用Windows日志分析识别常见系统安全事件

考核时间：15min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确打开Windows事件查看器； | 根据数据 |  |  |
| M2 | 1 | 显示安全日志部分； | 根据数据 |  |  |
| M3 | 2 | 正确导出登录成功的安全事件； | 根据数据 |  |  |
| M4 | 2 | 导出登录成功的安全事件文件为txt； | 根据数据 |  |  |
| M5 | 2 | 正确导出登录失败的安全事件； | 根据数据 |  |  |
| M6 | 2 | 导出登录失败的安全事件文件为txt； | 根据数据 |  |  |
| M7 | 2 | 正确设置当用户输错超过3次密码，自动锁定账户； | 根据数据 |  |  |
| M8 | 2 | 正确设置30分钟后解除锁定； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）