2017 年下半年网络规划设计师下午案例分析真题及答案解析

试题一

阅读以下说明，回答问题 1 至问题 4。

政府部门网络用户包括有线网络用户、无线网络用户和有线摄像头若干，组网拓扑如图 1-1 所示。访客通过无线网络接入互联网，不能访问办公网络及管理网络，摄像头只能跟 DMZ 区域服务器互访。

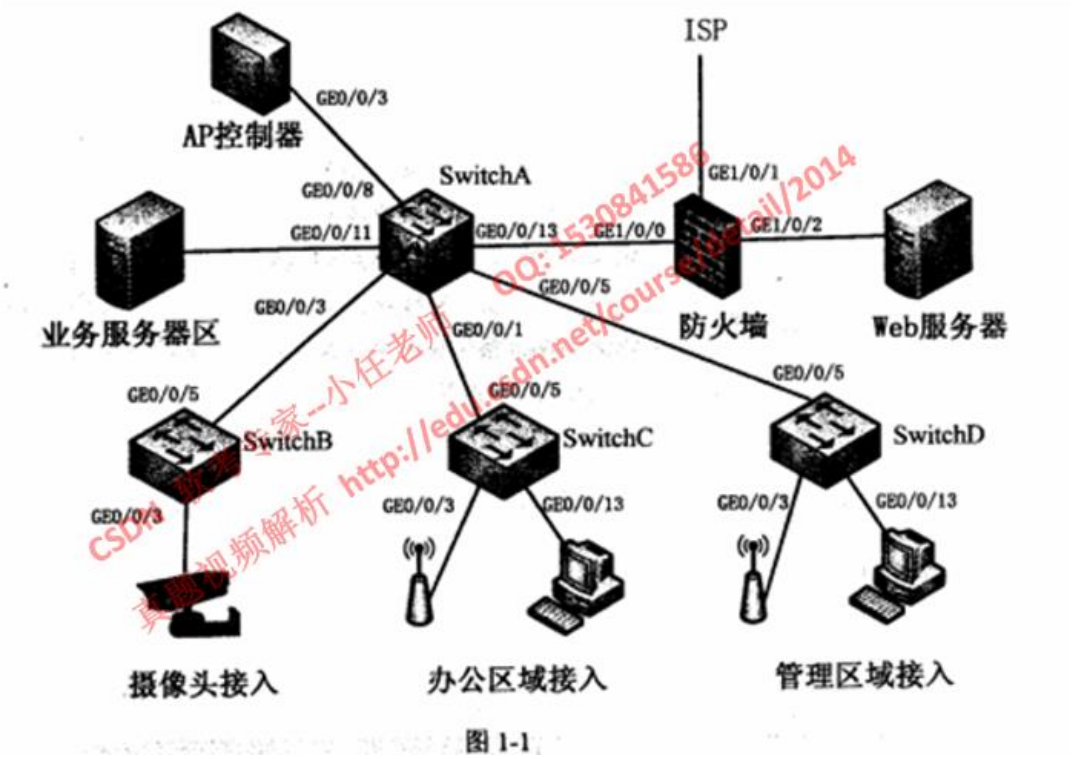

图 1-1

表 1-1 网络接口规划

设备名	接口编号	所属 VLAN	IP 地址
防火墙	GE1/0/0	--	10.107.1.2/24
	GE1/0/1	--	109.1.1.1/24
	GE1/0/2	--	10.106.1.1/24
AP	GE0/0/3	100	VLANIF100: 10.100.1.2/24
SwitchA	GE0/0/1	101 102 103 105	VLANIF105:10.105.1.1/24
	GE0/0/3	104	VLANIF104:10.104.1.1/24
	GE0/0/5	101 102 103 105	VLANIF101:10.101.1.1/24 VLANIF102:10.102.1.1/24 VLANIF103:10.103.1.1/24
	GE0/0/8	100	VLANIF100:10.100.1.1/24
	GE0/0/11	108	VLANIF108:10.108.1.1/24
	GE0/0/13	107	VLANIF107:10.107.1.1/24

表 1-2 VLAN 规划

项目	描述
VLAN 规划	VLAN100:无线管理 VLAN VLAN101:访客无线业务 VLAN VLAN102:员工无线业务 VLAN VLAN103:员工有线业务 VLAN VLAN104:摄像头的 VLAN VLAN105:AP 所属 VLAN VLAN107:对应 VLANIF 接口上行防火墙 VLAN108:业务区接入 VLAN

【问题 1】（6 分）

进行网络安全设计，补充防火墙数据规划表 1-3 内容中的空缺项。

表 1-3 防火墙数据规划

案例策略	源安全域	目的安全域	源地址/区域	目的地址/区域
egress	trust	untrust	（ 1 ）	--
dmz_camera	dmz	trust	10.106.1.1/24	10.104.1.1/24
untrust_dmz	untrust	dmz	--	10.106.1.1/24
源 net 策略 egress	trust	untrust	srcip	（ 2 ）
源 net 策略 camera_dmz	trust	dmz	camera	（ 3 ）

备注：NAT 策略转换方式为地址池中地址，ip 地址 109.1.1.2

【问题 2】（8 分）

进行访问控制规则设计，补充 SwichA 数据规划表 1-4 内容中的空缺项。

表 1-4 SwichA 数据规划

项目	VLAN	源 IP	目的 IP	动作
ACL	101	（ 4 ）	10.100.1.0/0.0.0.255	丢弃
		10.101.1.0/0.0.0.255	10.108.1.0/0.0.0.255	（ 5 ）
	104	10.104.1.0/0.0.0.255	10.106.1.0/0.0.0.255	（ 6 ）
		10.104.1.0/0.0.0.255	（ 7 ）	丢弃

【问题 3】（8 分）

补充路由规划内容，填写表 1-5 中的空缺项。

表 1-5 路由规划表

设备名	目的地址/掩码	下一跳	描述
防火墙	（ 8 ）	10.107.1.1	访问访客无线终端的路由
	（ 9 ）	10.107.1.1	访问摄像头的路由
SwitchA	0.0.0.0/0.0.0.0	10.107.1.2	缺省路由
AP 控制器	（ 10 ）	（ 11 ）	缺省路由

【问题 4】（3 分）

配置 SwitchA 时，下列命令片段的作用是（ ）

```
[SwitchA] interface Vlanif 105
[SwitchA-Vlanifl05] dhcp server option 43 sub-option 3 ascii 10.100.1.2
[SwitchA-Vlanifl05] quit
```

试题二（共 25 分）

阅读下列说明，回答问题 1 至问题 5。

图 2-1 所示为某企业桌面虚拟化设计的网络拓扑。

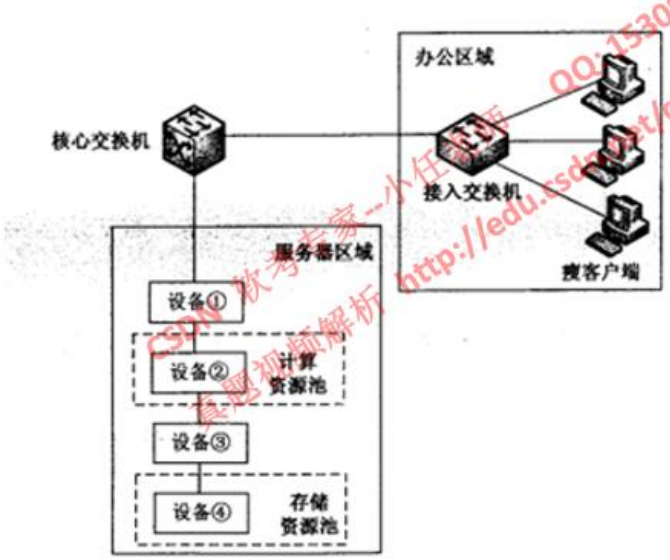

图 2-1

【问题 1】（6 分）

结合图 2-1 拓扑和桌面虚拟化部署需求，①处应部署（ 1 ）、②处应部署（ 2 ）、③处应部署（ 3 ）、④处应部署（ 4 ）。

（1）~（4）备选答案（每个选项仅限选一次）

A. 存储系统
B. 网络交换机
C. 服务器
D. 光纤交换机

【问题 2】（4 分）

该企业在虚拟化计算资源设计时，宿主机 CPU 的主频与核数应如何考虑？请说明理由。设备冗余上如何考虑？请说明理由。

【问题 3】（6 分）

图 2-1 中的存储网络方式是什么？结合桌面虚拟化对存储系统的性能要求，从性价比考虑，如何选择磁盘？请说明原因。

【问题 4】（4 分）
对比传统物理终端，简要谈谈桌面虚拟化的优点和不足。

【问题 5】（5 分）
桌面虚拟化可能会带来（ 5 ）等风险和问题，可以进行（ 6 ）等对应措施。
（5）备选答案（多项选择，错选不得分）
A. 虚拟机之间的相互攻击
B. 防病毒软件的扫描风暴
C、网络带宽瓶颈
D、扩展性差
（6）备选答案（多项选择，错选不得分）
A、安装虚拟化防护系统
B. 不安装防病毒软件
C、提升网络带宽
D. 提高服务器配置

试题三（共 25 分）
阅读下列说明，回答问题 1 至问题 4。
某企业网络拓扑如图 3-1 所示，该企业内部署有企业网站 Web 服务器和若干办公终端，Web 服务器（http://www.xxx.com） 主要对外提供网站消息发布服务， Web 网站系统采用 JavaEE 开发。

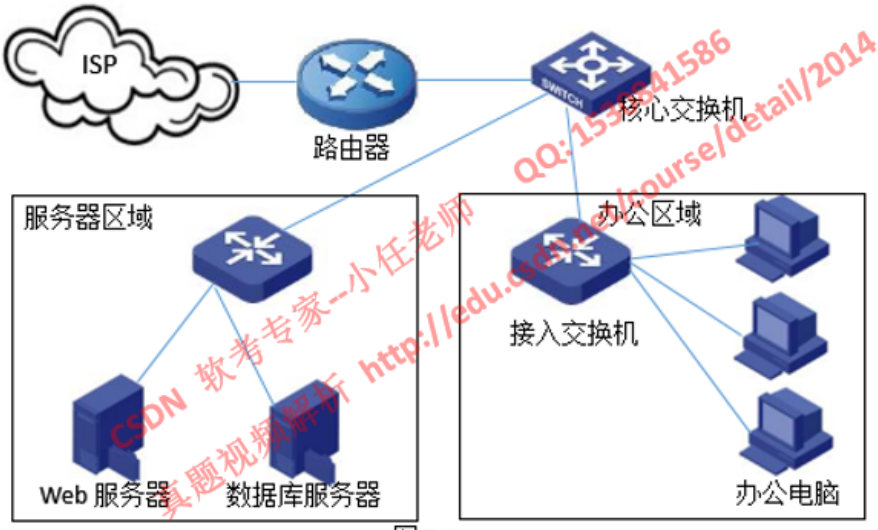

图 3-1

【问题 1】（6 分）
信息系统一般从物理安全、网络安全、主机安全、应用安全、数据安全等层面进行安全设计和防范，其中，“操作系统安全审计策略配置”属于（ 1 ）安全层面； “防盗防破坏、防火”属于（ 2 ）安全层面； “系统登录失败处理、最大并发数设置”属于（ 3 ）安全层面； “入侵防范、访问控制策略配置、防地址欺骗”属（ 4 ）安全层面。

【问题 2】（3 分）
为增强安全防范能力，该企业计划购置相关安全防护系统和软件，进行边界防护、Web 全防

护、终端 PC 病毒防范，结合图 3-1 拓扑，购置的安全防护系统和软件应包括：（ 5 ）、（ 6 ）、（ 7 ）。

（5）~（7）备选答案：

A.防火墙

B.WAF

C.杀毒软件

D.数据库审计

E.上网行为检测

【问题 3】（6 分）

2017 年 5 月，Wannacry 蠕虫病毒大面积爆发，很多用户遭受巨大损失。在病毒爆发之初，应采取哪些应对措施？（至少答出三点应对措施）

【问题 4】（10 分）

采用测试软件输入网站 www.xxx.com/index.action. 执行 ifconfig 命令，结果如图 3-2 所示。

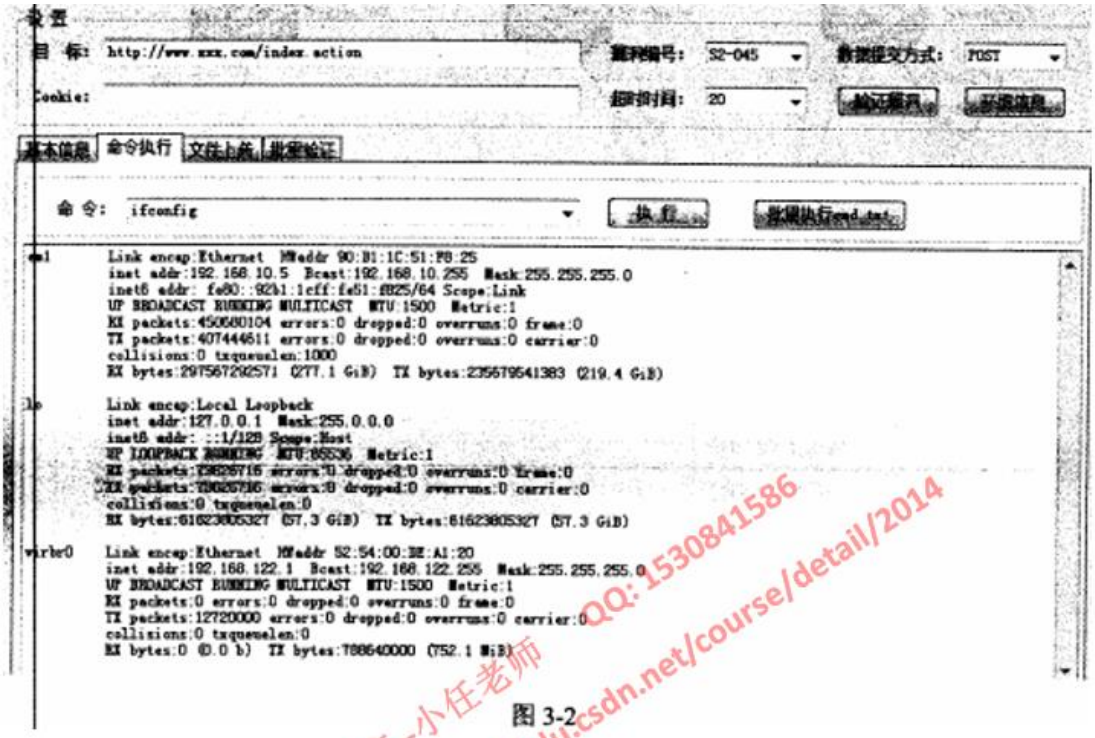

图 3-2

从图 3-2 可以看出，该网站存在（ 8 ）漏洞，请针对该漏洞提出相应防范措施。

（8）备选答案：

A. Java 反序列化

B. 跨站脚本攻击

C. 远程命令执行

D. SQL 注入

2、 通过浏览器访问网站管理系统，输入 www.xxx.com/login?f_page=-->'"><SVGonload=prompt(/x/)> ，结果如图 3-3 所示。

图 3-3

从图 3-3 可以看出，该网站存在（ 9 ）漏洞，请针对该漏洞提出相应防范措施。

（9）备选答案：

A.Java 反序列化

B.跨站脚本攻击

C.远程命令执行

D.SQL 注入

2017 年下半年网络规划设计师下午案例分析真题及答案解析

试题一 单击下面链接查看真题解析视频 http://edu.csdn.net/course/detail/2014

问题 1

（1）10.96.0.0/12 （2）- （3）10.106.1.1/24

问题 2：

（4）10.101.1.0/0.0.0.255 （5）丢弃

（6）允许 （7）any

问题 3：

（8）10.105.1.1/24 （9）10.104.1.1/24

（10）0.0.0.0/0.0.0.0 （11）10.100.1.1

问题 4

DHCP 通过 option 43 把 AC 的地址 10.100.1.2 给 AP

试题二

问题 1

（1）B （2）C （3）D （4）A

问题 2

计算资源池物理虚拟化应遵循以下原则：

1) 单个虚拟云服务器 CPU、内存最大配置不能超过物理计算资源集群中单台物理服务器的最大 CPU、内存配置；

2) 单台物理服务器上所有云主机的 VCPU 之和不超过物理机总核心的 1.5 倍；

3) 单台物理服务器上所有云主机内存之和不超过物理机内存的 120%；

4) 考虑到 HA 及 DRS 所要求的资源冗余，以及业务高峰，所有运行虚机在正常负载下，总体资源使用率不应超过三分之二；

5) 设备冗余采用 N+1 的方式，开启 HA 功能，当某台主机出现故障时，则该故障主机上面的虚拟桌面可自动在该资源池的其他有空闲资源的主机上自动启动。

问题 3

是 FC SAN(或光纤存储区域网络)。

系统盘的所有读操作都会放在 replica 盘中，当用户对操作系统有更新时，生成的数据会放在新生成的 delta 盘里。也就是说，replica 只提供读操作，而 delta 有读有写。而 Replica 盘读操作非常大，可能有数百个用户同时读操作，所以建议使用 SSD，EFD 盘。而用户的数据盘建议将其放在共享存储中，可以使用 SAS 盘或光纤硬盘。同时磁盘子系统还可以部署 RAID 5，以保证系统的可靠性。

问题 4

桌面虚拟化的优势：

1. 减少服务器的数量，提供一种服务器整合的方法，减少初期硬件采购成本
2. 简化服务器的部署、管理和维护工作，降低管理费用
3. 提高服务器资源的利用率，提高服务器计算能力
4. 通过降低空间、散热以及电力消耗等途径压缩数据中心成本

5. 通过动态资源配置提高 IT 对业务的灵活适应力
6. 提高可用性，带来具有透明负载均衡、动态迁移、故障自动隔离、系统自动重构的高可靠服务器应用环境
7. 支持异构操作系统的整合，支持老应用的持续运行

不足：

1、初始成本比较高。
2、虚拟桌面的性能不如物理桌面。
3、虚拟桌面的高度管控可能会引起用户反感。

问题 5：

（5）A、B、C
（6）A、C、D

试题三

问题 1

（1）主机　（2）物理　（3）应用　（4）网络

问题 2

（5）A　（6）B　（7）C

问题 3

对于蠕虫病毒的攻击，在爆发之初一般可以采用下面一些措施：
1、开启系统自动更新，检测更新并安装系统最新补丁。
2、开启防火墙，防火墙设置禁止 135、137、139、445 端口访问连接。
3、及时备份重要的业务资料，办公电脑上的文件更要采取内外网隔离和移动存储的方式进行备份，以防止电脑中毒，文件丢失。

问题 4

（8）C

防范措施：

1.假定所有输入都是可疑的，尝试对所有输入提交可能执行命令的构造语句进行严格的检查或者控制外部输入，系统命令执行函数的参数不允许外部传递。
2.不仅要验证数据的类型，还要验证其格式、长度、范围和内容。
3.不要仅仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。
4.对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行安全检查。
5.在发布应用程序之前测试所有已知的威胁。

（9）B

防范措施：

1.验证所有输入数据，有效检测攻击
2.对所有输出数据进行适当的编码，以防止任何已成功注入的脚本在浏览器端运行。

一、小任老师高级网络规划设计师视频教程

1、网络规划设计师-综合知识视频精讲 http://edu.csdn.net/course/detail/2012

2、上午历年真题解析视频 http://edu.csdn.net/course/detail/2391

3、下午案例分析历年真题解析视频 http://edu.csdn.net/course/detail/2014

4、论文写作技巧精讲视频 http://edu.csdn.net/course/detail/2015

二、小任老师软考高级信息系统项目管理师视频教程：

1、 高级--项目管理(上) 视频教程 http://edu.csdn.net/course/detail/1385

2、 高级—上午历年真题视频精讲 http://edu.csdn.net/course/detail/1864

3、高级--案例分析历年真题视频精讲 http://edu.csdn.net/course/detail/1394

4、高级--论文写作技巧解析视频 http://edu.csdn.net/course/detail/1395