# 软考资料免费获取

- 1、最新软考题库
- 2、软考备考资料
- 3、考前压轴题



## 命 微信扫一扫,立马获取







免费备考资料

PC版题库: ruankaodaren.com

手机端题库: 微信搜索「软考达人」 / PC端题库: www.ruankaodaren.com

## 2019年下半年网络规划设计师考试下午真题(专业解析+参考答案)

#### 1 案例分析 难度:一般

## 网络新技术

## [案例题]

阅读以下说明,回答问题1至问题4。

#### 【说明】

某物流公司采用云管理平台构建物流网络,如图1-1所示(以1个配送站为例),数据规划如表1-1所示。

## 项目特点:

- 1.单个配送站人员少于20人,仅一台云防火墙就能满足需求;
- 2.总部与配送站建立IPSec, 配送站通过IPSec接入总部, 内部用户需要认证后才有访问网络的权限;
- 3.配送站的云防火墙采用IPSec智能选路与总部两台防火墙连接,IPSec智能选路探测隧道质量,当质量不满足时切换另外一条链路;
- 4.配送站用户以无线接入为主。

(备注: Agile Controller-Campus是新一代园区与分支网络控制器,支持网络部署自动化、策略自动化,SD-WAN等,让网络服务更加便捷。)

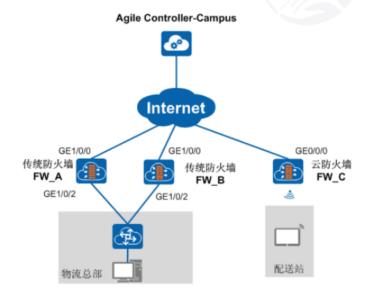


图1-1





## 手机端顯麻 微信搜索 要數考达人」 / PC端题库设计内容v.ruankaodaren.con

角色设计       用户账户       用户账号名称/用户账号密码         架构设计       网络拓扑       见图1-1         设备选型       云防火墙, USG6510-WL         站点       站点名称, test_mix, 站点类型, FW         总部传统防火墙FW_A       上行连接运营商网络接口, GB1/0/0         下行连接内网交换机接口; GB1/0/2       上行连接运营商网络接口IP地址, 10.10.1.1/24         上行连接运营商网络接口; GB1/0/0       下行连接内网交换机接口IP地址, 10.10.1.1/24         总部传统防火墙FW_B       上行连接运营商网络接口; GB1/0/0         下行连接内网交换机接口IP地址, 2.2.2.2/24       下行连接应营商网络接口IP地址, 2.2.2.2/24         下行连接应营商网络接口IP地址, 10.10.1.2/24       云防火墙FW_C         上行连接运营商网络接口IP地址, 3.3.3.3/24       以太网接入, 静态IP方式, 采用命令行配置         W大进到Agile       采用命令行配置         Controller-Campus的南向IP地址为, 192.168.84, 208, 端口号为, 10020         NAT       在网关(云防火墙)上开启NAT功能         用户线端的IP地址       配送站职工(无线接入)         用户终端的IP地址       DHCP方式获取, IP地址范围为, 10.1.2.0/24         用户所属的VLAN       222         无线终端接入SSID与认证方式       SSID名称为test-emp, PSK认证	端顯麻	微信搜索要款考达	人」 / PC端题库设immerv.ruankaodaren.
设备选型   云防火墙: USG6510-WL   站点   本は点名称: test_mix; 站点类型: FW   お点名称: test_mix; 站点类型: FW   上行连接运营商网络接口: GE1/0/0   下行连接内网交换机接口: GE1/0/2   上行连接运营商网络接口IP地址: 1.1.1.1/24   下行连接内网交换机接口IP地址: 10.10.1.1/24   总部传统防火墙FW_B   上行连接运营商网络接口IP地址: 10.10.1.1/24   总部传统防火墙FW_B   上行连接运营商网络接口IP地址: 2.2.2.2/24   下行连接内网交换机接口IP地址: 2.2.2.2/24   下行连接内网交换机接口IP地址: 10.10.1.2/24   云防火墙FW_C   上行连接运营商网络接口IP地址: 3.3.3.3/24   以太网接入,静态IP方式,采用命令行配置   采用命令行配置   采用命令行配置   系引e Controller-Campus的南向IP地址为: 192.168.84.208, 端口号为: 10020   NAT   在网关(云防火墙FM_C   上开启NAT功能   用户经端的IP地址   即户等理   配送站职工(无线接入)   田户所属的VLAN   222   元线终端接入SSID与   CSTD名称为tastastastastastastastastastastastastast	角色设计	用户账户	用户账号名称/用户账号密码
対点	架构设计	网络拓扑	见图1-1
送部传统防火墙FW_A		设备选型	云防火墙: USG6510-WL
上行连接运营商网络接口:GE1/0/0 下行连接内网交换机接口:GE1/0/2 上行连接运营商网络接口IP地址:1.1.1.1/24 下行连接内网交换机接口IP地址:10.10.1.1/24 总部传统防火墙FW_B 上行连接运营商网络接口:GE1/0/0 下行连接内网交换机接口:GE1/0/2 上行连接运营商网络接口IP地址:2.2.2.2/24 下行连接内网交换机接口IP地址:10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口:GE0/0/0 上行连接运营商网络接口IP地址:3.3.3.3/24 以本网接入,静态IP方式,采用命令行配置 采用命令行配置 采用命令行配置 采用命令行配置 系言1e Controller-Campus的南向IP地址为:192.168.84.208,端口号为:10020 和AT 在网关(云防火墙)上开启NAT功能 用户上线设计 用户管理 配送站职工(无线接入) 用户终端的IP地址 DHCP方式获取,IP地址范围为:10.1.2.0/24 DHCP Server:云防火墙FW_C 222 无线终端接入SSID与 SSID名整为teaterem、PSWildIT		站点	站点名称: test_mix; 站点类型: FW
下行连接内网交换机接口。GE1/0/2 上行连接运营商网络接口IP地址:1.1.1.1/24 下行连接内网交换机接口IP地址:10.10.1.1/24 总部传统防火墙FW_B 上行连接运营商网络接口。GE1/0/0 下行连接内网交换机接口。GE1/0/2 上行连接运营商网络接口IP地址:2.2.2.2/24 下行连接内网交换机接口IP地址:10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口IP地址:3.3.3.3/24 设备上线设计		设备接口互联	总部传统防火墙FW_A
上行连接运营商网络接口IP地址: 1.1.1.1/24 下行连接内网交换机接口IP地址: 10.10.1.1/24 总部传统防火墙FW_B 上行连接运营商网络接口: GE1/0/0 下行连接内网交换机接口: GE1/0/2 上行连接运营商网络接口IP地址: 2.2.2.2/24 下行连接内网交换机接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口IP地址: 3.3.3.3/24 设备上线设计			上行连接运营商网络接口: GE1/0/0
下行连接内网交换机接口IP地址: 10.10.1.1/24 总部传统防火墙FW_B 上行连接运营商网络接口: GE1/0/0 下行连接内网交换机接口: GE1/0/2 上行连接运营商网络接口IP地址: 2.2.2.2/24 下行连接内网交换机接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口IP地址: 3.3.3.3/24 设备上线设计 网关获取IP地址方式 以太网接入,静态IP方式,采用命令行配置 网关注册到Agile Controller-Campus的南面IP地址为: 192.168.84.208,端口号为: 10020 NAT 在网关(云防火墙)上开启NAT功能 用户上线设计 用户管理 配送站职工(无线接入) 用户终端的IP地址 DHCP方式获取,IP地址范围为: 10.1.2.0/24 DHCP Server: 云防火墙FW_C 用户所属的VLAN 222			下行连接内网交换机接口: GE1/0/2
总部传统防火墙FW_B 上行连接运营商网络接口: GE1/0/0 下行连接内网交换机接口: GE1/0/2 上行连接运营商网络接口IP地址: 2.2.2.2/24 下行连接内网交换机接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口: GE0/0/0 上行连接运营商网络接口IP地址: 3.3.3.3/24 设备上线设计 网关获取IP地址方式 以太网接入,静态IP方式,采用命令行配置 网关注册到Agile 采用命令行配置 Agile Controller-Campus的南向IP地址为: 192.168.84.208,端口号为: 10020 NAT 在网关(云防火墙)上开启NAT功能 用户上线设计 配送站职工(无线接入)  用户修订的IP地址 即户管理 配送站职工(无线接入)  用户终端的IP地址 即户下式获取,IP地址范围为: 10.1.2.0/24 DHCP 方式获取,IP地址范围为: 10.1.2.0/24 DHCP Server: 云防火墙FW_C 用户所属的VLAN 222 无线终端接入SSID与 CSID名称为+ceteory PCKildit			上行连接运营商网络接口IP地址: 1.1.1.1/24
上行连接运营商网络接口: GE1/0/0 下行连接内网交换机接口: GE1/0/2 上行连接运营商网络接口IP地址: 2.2.2.2/24 下行连接内网交换机接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口: GE0/0/0 上行连接运营商网络接口: GE0/0/0 上行连接运营商网络接口IP地址: 3.3.3.3/24  设备上线设			下行连接内网交换机接口IP地址: 10.10.1.1/24
下行连接内网交换机接口;GE1/0/2 上行连接运营商网络接口IP地址;2.2.2.2.2/24 下行连接内网交换机接口IP地址;10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口;GE0/0/0 上行连接运营商网络接口IP地址;3.3.3.3/24 设备上线设 计 网关获取IP地址方式 以太网接入,静态IP方式,采用命令行配置 网关注册到Agile 采用命令行配置 Agile Controller-Campus的南向IP地址为;192.168.84.208,端口号为;10020 NAT 在网关(云防火墙)上开启NAT功能 用户上线设 计 配送站职工(无线接入) 用户终端的IP地址 即任P方式获取,IP地址范围为;10.1.2.0/24 DHCP方式获取,IP地址范围为;10.1.2.0/24 DHCP Server;云防火墙FW_C			总部传统防火墙FW_B
上行连接运营商网络接口IP地址: 2.2.2.2/24 下行连接内网交换机接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口IP地址: 3.3.3.3/24 设备上线设 计			上行连接运营商网络接口: GE1/0/0
下行连接内网交换机接口IP地址: 10.10.1.2/24 云防火墙FW_C 上行连接运营商网络接口: GEO/O/O 上行连接运营商网络接口IP地址: 3.3.3.3/24 设备上线设 计 网关获取IP地址方式 以太网接入,静态IP方式,采用命令行配置 网关注册到Agile		.0	
云防火墙FW_C			
上行连接运营商网络接口: GEO/O/O         上行连接运营商网络接口IP地址: 3.3.3.3/24         设备上线设计       网关获取IP地址方式       以太网接入,静态IP方式,采用命令行配置         网关注册到Agile       采用命令行配置         Controller-Campus方式       Agile Controller-Campus的南向IP地址为: 192.168.84.208,端口号为: 10020         NAT       在网关(云防火墙)上开启NAT功能         用户上线设计       配送站职工(无线接入)         用户终端的IP地址       DHCP方式获取,IP地址范围为: 10.1.2.0/24         DHCP Server: 云防火墙FW_C       用户所属的VLAN         222       无线终端接入SSID与         SSID名称为test=sym. PSV;LiT		0	
上行连接运营商网络接口IP地址: 3.3.3.3/24         设备上线设计       网关获取IP地址方式       以太网接入,静态IP方式,采用命令行配置         网关注册到Agile       采用命令行配置         Agile Controller-Campus的南向IP地址为: 192.168.84.208,端口号为: 10020         NAT       在网关(云防火墙)上开启NAT功能         用户上线设计       用户管理         市户终端的IP地址       DHCP方式获取,IP地址范围为: 10.1.2.0/24 DHCP Server: 云防火墙FW_C         用户所属的VLAN       222         无线终端接入SSID与       CSID名称为test-corp. PSVilit	13		
设备上线设计       网关获取IP地址方式       以太网接入,静态IP方式,采用命令行配置         网关注册到Agile       采用命令行配置         Agile Controller-Campus的南向IP地址为: 192.168.84.208,端口号为: 10020         NAT       在网关(云防火墙)上开启NAT功能         用户上线设计       用户管理         DHCP方式获取,IP地址范围为: 10.1.2.0/24         DHCP Server: 云防火墙FW_C         用户所属的VLAN       222         无线终端接入SSID与       SSID名称为test=sym. PSViliT			
计       网关注册到Agile       采用命令行配置         Controller-Campus方式       Agile Controller-Campus的南向IP地址为: 192.168.84.208,端口号为: 10020         NAT       在网关(云防火墙)上开启NAT功能         用户上线设计       配送站职工(无线接入)         H户终端的IP地址       DHCP方式获取,IP地址范围为: 10.1.2.0/24         DHCP Server: 云防火墙FW_C       用户所属的VLAN         222       无线终端接入SSID与         SSID名称为test=sym. PSV; LiT	VB E 1 / 15 VB		上行连接运营商网络接口IP地址: 3.3.3.3/24
(四天社册到Agile Controller-Campus方式       果用命令行配直 Agile Controller-Campus的南向IP地址为: 192.168.84.208,端口号为: 10020         (NAT 在网关(云防火墙)上开启NAT功能         用户上线设计       配送站职工(无线接入)         (日户终端的IP地址 DHCP方式获取,IP地址范围为: 10.1.2.0/24 DHCP Server: 云防火墙FW_C         用户所属的VLAN 222         无线终端接入SSID与 SSID与 SSID SSID		网关获取IP地址方式	以太网接入,静态IP方式,采用命令行配置
式     192.168.84.208,端口号为:10020       NAT     在网关(云防火墙)上开启NAT功能       用户上线设计     配送站职工(无线接入)       H户终端的IP地址     DHCP方式获取,IP地址范围为:10.1.2.0/24       DHCP Server:云防火墙FW_C     用户所属的VLAN       222     无线终端接入SSID与       SSID名称为test=sym. PSV;LiT		网关注册到Agile	采用命令行配置
NAT     在网关(云防火墙)上开启NAT功能       用户上线设计     用户管理     配送站职工(无线接入)       用户终端的IP地址     DHCP方式获取,IP地址范围为: 10.1.2.0/24       DHCP Server: 云防火墙FW_C     用户所属的VLAN     222       无线终端接入SSID与     SSID名称为test-corp. PSVilit			
用户上线设计       用户管理       配送站职工(无线接入)         用户终端的IP地址       DHCP方式获取,IP地址范围为: 10.1.2.0/24         DHCP Server: 云防火墙FW_C       用户所属的VLAN         222       无线终端接入SSID与         SSID名称为test=sym. PSV;life	m + 1 460	-	
计DHCP方式获取, IP地址范围为: 10.1.2.0/24用户终端的IP地址DHCP Server: 云防火墙FW_C用户所属的VLAN222无线终端接入SSID与SSID名称为test-serve, PSVilville			
用户终端的IP地址DHCP方式获取,IP地址范围为: 10.1.2.0/24DHCP Server: 云防火墙FW_C用户所属的VLAN222无线终端接入SSID与SSID名称为test=sym. PSV; life	计	用户管理	配送站职工(无线接入)
DHCP Server: 云防火墙FW_C 用户所属的VLAN 222 无线终端接入SSID与 SSID名称为test-serv. PSVilit		用户终端的IP地址	DHCP方式获取,IP地址范围为: 10.1.2.0/24
无线终端接入SSID与 esiD名称为test-own, Bevilia			DHCP Server: 云防火墙FW_C
1		用户所属的VLAN	222
			SSID名称为test-emp; PSK认证

【问题1】 配置传统防火墙FW\_A配置命令的注释。



软考达人: 软考专业备考平台, 免费提供6w+软考题库, 1TB免费专业备考资料

(1) 〈FW\_A〉 system 手机端题库:微信搜索「软考达人」 / PC端题库:www.ruankaodaren.com [FW\_A] interface GigabitEthernet 1/0/0 [FW A-GigabitEthernet1/0/0] ip address 1.1.1.1 24 [FW\_A-GigabitEthernet1/0/0] gateway 1.1.1.254  $[FW_A-GigabitEthernet1/0/0]$  service-manage enable  $[FW\_A-GigabitEthernet1/0/0] \quad service-manage \ ping \ permit$ [FW\_A-GigabitEthernet1/0/0] quit [FW\_A] interface GigabitEthernet 1/0/2  $\hbox{[FW\_A-GigabitEthernet1/0/2] ip address 10.10.1.1 24}$ [FW\_A-GigabitEthernet1/0/2] quit [FW\_A] firewall zone trust [FW\_A-zone-trust] add interface GigabitEthernet 1/0/2 [FW\_A-zone-trust] quit [FW\_A] firewall zone untrust [FW\_A-zone-untrust] add interface GigabitEthernet 1/0/0 [FW\_A-zone-untrust] quit (3) [FW\_A] security-policy [FW\_A-policy-security] rule name 1 [FW\_A-policy-security-rule-1] source-zone trust [FW\_A-policy-security-rule-1] destination-zone untrust [FW\_A-policy-security-rule-1] source-address 10.10.1.0 24 [FW\_A-policy-security-rule-1] destination-address 10.1.2.0 24 [FW\_A-policy-security-rule-1] action permit  $[FW\_A-policy-security-rule-1] \quad quit$ [FW\_A-policy-security] rule name 2 [FW\_A-policy-security-rule-2] source-zone untrust [FW\_A-policy-security-rule-2] destination-zone trust  $[FW\_A-policy-security-rule-2] \quad source-address \ 10.\ 1.\ 2.\ 0\ 24$  $\hbox{[FW\_A-policy-security-rule-2]} \quad destination-address \ 10.10.1.0 \ 24$ 

[FW\_A-policy-security-rule-2] action permit

[FW\_A-policy-security-rule-2] quit

```
(4)
[FW_A-policy-s要机端题库!le微槽搜索「软考达人」
                                                  / PC端题库: www.ruankaodaren.com
[FW_A-policy-security-rule-3] source-zone local
[FW_A-policy-security-rule-3] destination-zone untrust
[FW A-policy-security-rule-3] source-address 1.1.1.1 32
[FW_A-policy-security-rule-3] destination-address 3.3.3.3 32
[FW A-policy-security-rule-3] action permit
[FW_A-policy-security-rule-3] quit
[FW_A-policy-security] rule name 4
[FW_A-policy-security-rule-4] source-zone untrust
[FW_A-policy-security-rule-4] destination-zone local
[FW_A-policy-security-rule-4] source-address 3.3.3.3 32
[FW_A-policy-security-rule-4] destination-address 1.1.1.1 32
[FW_A-policy-security-rule-4] action permit
[FW_A-policy-security-rule-4] quit
                                  (5)
[FW A] acl 3000
[FW_A-acl-adv-3000] rule permit ip source 10.10.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[FW_A-acl-adv-3000] rule permit icmp source 1.1.1.1 0 destination 3.3.3.3 0
[FW_A-acl-adv-3000] quit
                                  (6)
[FW_A] ipsec proposal tran1
[FW_A-ipsec-proposal-tran1] encapsulation-mode tunnel
[FW_A-ipsec-proposal-tran1] transform esp
[FW A-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[FW_A-ipsec-proposal-tran1] esp encryption-algorithm aes-256
[FW A-ipsec-proposal-tran1] quit
                                  (7)
[FW_A] ike proposal 10
[FW_A-ike-proposal-10] authentication-method pre-share
[FW_A-ike-proposal-10] authentication-algorithm sha2-256
[FW_A-ike-proposal-10] integrity-algorithm aes-xcbc-96 hmac-sha2-256
[FW_A-ike-proposal-10] quit
[FW A] ike peer b
[FW_A-ike-peer-b] ike-proposal 10
[FW_A-ike-peer-b] pre-shared-key Test@12345
[FW_A-ike-peer-b] undo version 2
[FW_A-ike-peer-b] quit
                                  (9)
[FW_A] ipsec policy-template map_temp 1
[FW_A-ipsec-policy-template-map_temp-1] security acl 3000
[FW_A-ipsec-policy-template-map_temp-1] proposal tran1
[FW_A-ipsec-policy-template-map_temp-1] ike-peer b
[FW_A-ipsec-policy-template-map_temp-1] quit
[FW_A] ipsec policy map1 10 isakmp template map_temp
[FW_A] interface GigabitEthernet 1/0/0
[FW_A-GigabitEthernet1/0/0] ipsec policy map1
[FW_A-GigabitEthernet1/0/0] quit
(1)~(10)备选答案:
A.配置IKE Peer
B.引用安全策略模板并应用到接口
C.配置访问控制列表
D.配置序号为10的IKE安全提议
E.配置接口加入安全域
F.允许封装前和解封后的报文能通过FW_A
G.配置接口IP地址
H.配置名称为tran1的IPSec安全提议
I.配置名称为map_temp、序号为1的IPSec安全策略模板
J.允许IKE协商报文能正常通过FW_A
【问题2】(4分)
```

物流公司进行用户(配送站)侧验收时,在配送站FW\_C. 上查看IPSec智能选路情况如下图所示,则配送站智能接入的设备是 (11),该选路策略在 (12)设备上配置。

Name :8864a216e7914f6

Detection number :10
Detection interval :1

 $\begin{array}{lll} \mbox{Detection source IP} & :3.\ 3.\ 3.\ 3 \\ \mbox{Detection destination IP} & :1.\ 1.\ 1.\ 1 \end{array}$ 

Cycles :3 Switched times :0

Switch mode :detection-based

State :enable

IPSec policy alias :5528010a-3e60-49a0-93a1-3e5c7ef508c2

link list:

ID local-address remote-address loss(%) delay(ms) state

1 3.3.3.3 1.1.1.1 0 7 active 2 3.3.3.3 2.2.2.2 100 -- inactive

【问题3】 (5分)

物流公司组建该网络相比传统网络体现出哪些优势?

【问题4】 (6分)

简要说明该云管理网络构建及运营与MSP(Mananaged Sservices Provider)的区别?

🔂 视频解析

2 案例分析 难度: 一般

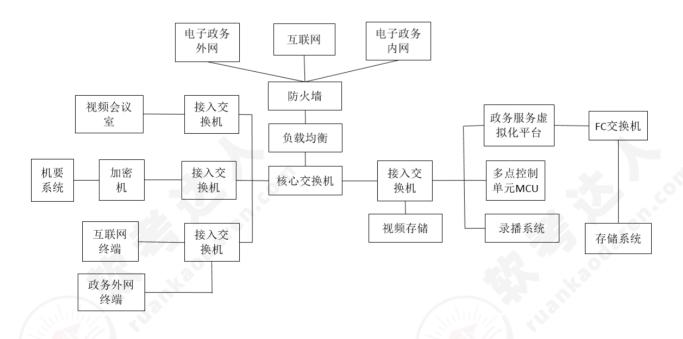
网络存储

[案例题]

阅读下列说明,回答问题1至问题4。

#### 【说明】

图2-1为某政府部门新建大楼,网络设计拓扑图,根据业务需求,共有三条链路接入,分别连接电子政务外网、互联网、电子政务内网(涉密网),其中机要系统通过电子政务内网访问上级部门机要系统,并由加密机进行数据加密。3条接入链路共用大楼局域网,通过VLAN逻辑隔离。大楼内部署有政府服务系统集群,对外提供政务服务,建设有四个视频会议室,部署视频会议系统,与上级单位和下级各部门召开业务视频会议及项目评审会议等,要求录播存储,录播系统将视频存储以NFS格式挂载为网络磁盘,存储视频文件。



(9分)

- (1) 图2-1所示设计的网络结构为大二层结构,简述该网络结构各层的主要功能和作用,并简要说明该网络结构的优缺点。
- (2) 图2-1所示网络设计中,如何实现互联网终端仅能访问互联网、电子政务外网终端仅能访问政务外网,机要系统仅能访问电子政务内网?
- (3) 机要系统和电子政务内网设计是否违规?请说明原因。

【问题2】 (6分)

- (4) 视频会议1080p格式传输视频,码流为8Mbps ,请计算每个视频会议室每小时会占用多少存储空间(单位要用MB或者GB),并说明原因。
- (5) 每个视频会议室每年使用约100天(每天按8小时计算),视频文件至少保存2年。图2-1中设计的录播系统将视频存储挂载为网络磁盘,存储视频文件,该存储系统规划配置4TB(实际容量按3.63TB计算)磁盘, RAID6方式冗余, 设置全局热备盘1块。请计算该存储系统至少需要配置多少块磁盘并说明原因。 【问题3】 (6分)
- (6) 各视频会议室的视频终端和MCU是否需要一对一做NAT,映射公网IP地址?请说明原因。
- (7) 召开视频会议使用的协议是什么2需要在防火境开放的CP端口是什么? 【问题4】 (4分) 软考达人:软考专业备考平台,免费提供6w+软考题库,1TB免费专业备考资料

图2-1所示的虚拟化平台连接的存储系统连接方式是(8)视频存储的连接方式是(9)。

## 手机端题库: 微信搜索「软考达人」 / PC端题库: www.ruankaodaren.com

🗔 视频解析

## 3 案例分析 难度: 一般

网络安全方案

### [案例题]

回答问题1至问题3。

## 【问题1】(4分)

安全管理制度管理、规划和建设为信息安全管理的重要组成部分。一般从安全策略、安全预案、安全检查、安全改进等方面加强安全管理制度建设和规划。其中,(1)应定义安全管理机构、等级划分、汇报处置、处置操作、安全演练等内容;(2)应该以信息安全的总体目标、管理意图为基础,是指导管理人员行为,保护信息网络安全的指南。

#### 【问题2】(11分)

某天,网络安全管理员发现web服务器访问缓慢,无法正常响应用户请求,通过检查发现,该服务器CPU和内存资源使用率很高、网络带宽占用率很高,进一步查询日志,发现该服务器与外部未知地址有大量的UDP连接和TCP半连接,据此初步判断该服务器受到 (3)和(4)类型的分布式拒绝服务攻击( DDos),可以部署(5)设备进行防护。这两种类型的DDos攻击的原理是(6)、(7)。

(3)~(4)备选答案(每个选项仅限选一次):

A Ping洪流攻击 B SYN泛洪攻击

C Teardrop攻击 D UDP泛洪攻击

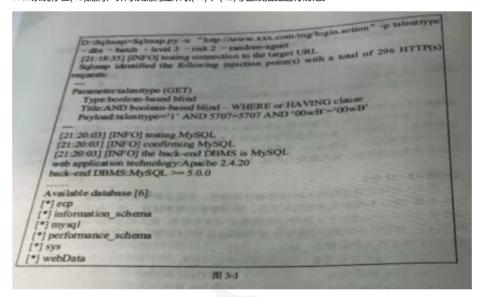
(5)备选答案:

A 抗DDoS防火墙 B Web防火墙

C 入侵检测系统 D 漏洞扫描系统

## 【问题3】(10分)

网络管理员使用检测软件对Web服务器进行安全测试,图3-1为测试结果的片段信息,从测试结果可知,该Web系统使用的数据库软件为(8)Web服务器软件为(9)该Web系统存在(10)漏洞,针对该漏洞应采取(11)、(12)等整改措施进行防范。



3 视频解析



