

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。）

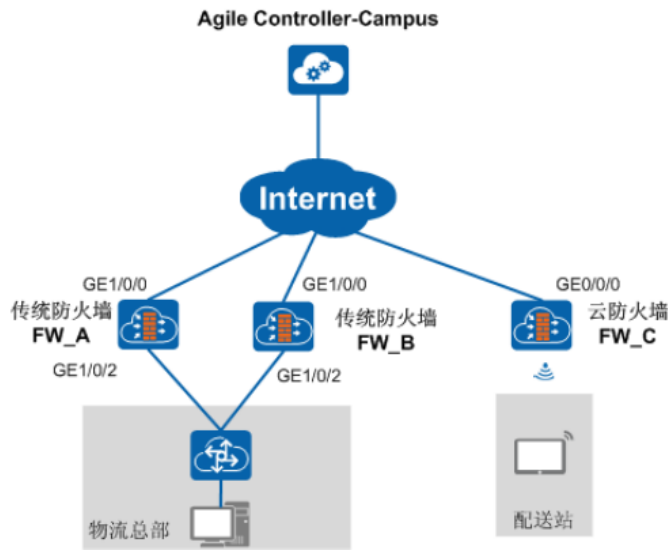


图1-1

表1-1

设计项	设计要点	设计内容
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
	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：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
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方式	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	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与认证方式	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。

(1)

```
<FW_A> system-view
[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] service-manage ping permit
[FW_A-GigabitEthernet1/0/0] quit
[FW_A] interface GigabitEthernet 1/0/2
[FW_A-GigabitEthernet1/0/2] ip address 10.10.1.1 24
[FW_A-GigabitEthernet1/0/2] quit
```

(2)

```
[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] 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] source-address 10.1.2.0 24
[FW_A-policy-security-rule-2] 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-security] rule name 3
[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
```

(8)

```
[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
```

(10)

```
[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。

```
<FW_C> display ipsec smart-link profile
```


```
=====
Name                               :8864a216e7914f6
Detection number                   :10
Detection interval                 :1
Detection source IP                :3.3.3.3
Detection destination IP          :1.1.1.1
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

参考答案：

【问题1】

- (1) G
- (2) E
- (3) F
- (4) J
- (5) C
- (6) H
- (7) D
- (8) A
- (9) I
- (10) B

【问题2】

- (11) FW_A
- (12) Agile Controller-Campus

【问题3】

云管理网络的优势在于：

1、安全可靠、支持多种认证

依托华为云数据中心，Netconf协议，报文加密，操作日志加密记录。你下班，云管理永不下班、支持员工密码认证，访客微信认证。更有短信/API等多种认证方式内置支持，云端轻松配置。

2、即插即用、极简结构、自动升级

插上网线，扫码激活。剩下的配置，交给云端远程配置，批量下发，喝着咖啡就把网络布好，白天完成配置，预约夜间自动升级，从此告别现场熬夜值守，深夜寂寞的机房不再有工程师的身影。

3、大数据分析

丰富的业务使用情况统计，网络情况和业务记录全掌握；云管理网络将所有设备统一纳管，通过智能的数据统计和分析，可为企业提供丰富的运营报表功能。

4、云网规、云管理、云排障

上传图纸，自动规排，信号仿真，输出网规报告。可视化在线云网规，做网规比画画还容易、远程云端运维管理，想看就看，网络健康尽在掌握。更有云端代维服务，为你配置全天候专属网络管家，随时随地可查看全网异常告警，远程故障分析和处理。

【问题4】

MSP能提供的云管理服务包括了：

专业服务（Professional Service），例如咨询，迁移，实施等服务；

托管服务（Managed Service），包括监控，运维，优化等等

云管理工具（Cloud Management Platform）：基于企业云管理平台BSP，企业可以对各种云环境一目了然，帮助企业真正实现混合云管理；通过简单明了的资源利用趋势图，深入了解云成本和云资源情况，并提供资源和成本优化方案。

试题解析： 【问题1】

- (1) G
- (2) E
- (3) F
- (4) J
- (5) C
- (6) H
- (7) D
- (8) A
- (9) I

(10) B

【问题2】

(11) FW_A

(12) Agile Controller-Campus

【问题3】

云管理网络的优势在于：

1、安全可靠、支持多种认证

依托华为云数据中心，Netconf协议，报文加密，操作日志加密记录。你下班，云管理永不下班、支持员工密码认证，访客微信认证。更有短信/API等多种认证方式内置支持，云端轻松配置。

2、即插即用、极简结构、自动升级

插上网线，扫码激活。剩下的配置，交给云端远程配置，批量下发，喝着咖啡就把网络布好，白天完成配置，预约夜间自动升级，从此告别现场熬夜值守，深夜寂寞的机房不再有工程师的身影。

3、大数据分析

丰富的业务使用情况统计，网络情况和业务记录全掌握；云管理网络将所有设备统一纳管，通过智能的数据统计和分析，可为企业提供丰富的运营报表功能。

4、云网规、云管理、云排障

上传图纸，自动规排，信号仿真，输出网规报告。可视化在线云网规，做网规比画画还容易、远程云端运维管理，想看就看，网络健康尽在掌握。更有云端代维服务，为你配置全天候专属网络管家，随时随地可查看全网异常告警，远程故障分析和处理。

【问题4】

MSP能提供的云管理服务包括了：

专业服务（Professional Service），例如咨询，迁移，实施等服务；

托管服务（Managed Service），包括监控，运维，优化等等

云管理工具（Cloud Management Platform）：基于企业云管理平台BSP，企业可以对各种云环境一目了然，帮助企业真正实现混合云管理；通过简单明了的资源利用趋势图，深入了解云成本和云资源情况，并提供资源和成本优化方案。

【问题1】

(1) G

(2) E

(3) F

(4) J

(5) C

(6) H

(7) D

(8) A

(9) I

(10) B

【问题2】

(11) FW_A

(12) Agile Controller-Campus

【问题3】

云管理网络的优势在于：

1、安全可靠、支持多种认证

依托华为云数据中心，Netconf协议，报文加密，操作日志加密记录。你下班，云管理永不下班、支持员工密码认证，访客微信认证。更有短信/API等多种认证方式内置支持，云端轻松配置。

2、即插即用、极简结构、自动升级

插上网线，扫码激活。剩下的配置，交给云端远程配置，批量下发，喝着咖啡就把网络布好，白天完成配置，预约夜间自动升级，从此告别现场熬夜值守，深夜寂寞的机房不再有工程师的身影。

3、大数据分析

丰富的业务使用情况统计，网络情况和业务记录全掌握；云管理网络将所有设备统一纳管，通过智能的数据统计和分析，可为企业提供丰富的运营报表功能。

4、云网规、云管理、云排障

上传图纸，自动规排，信号仿真，输出网规报告。可视化在线云网规，做网规比画画还容易、远程云端运维管理，想看就看，网络健康尽在掌握。更有云端代维服务，为你配置全天候专属网络管家，随时随地可查看全网异常告警，远程故障分析和处理。

【问题4】

MSP能提供的云管理服务包括了：

专业服务（Professional Service），例如咨询，迁移，实施等服务；

托管服务（Managed Service），包括监控，运维，优化等等

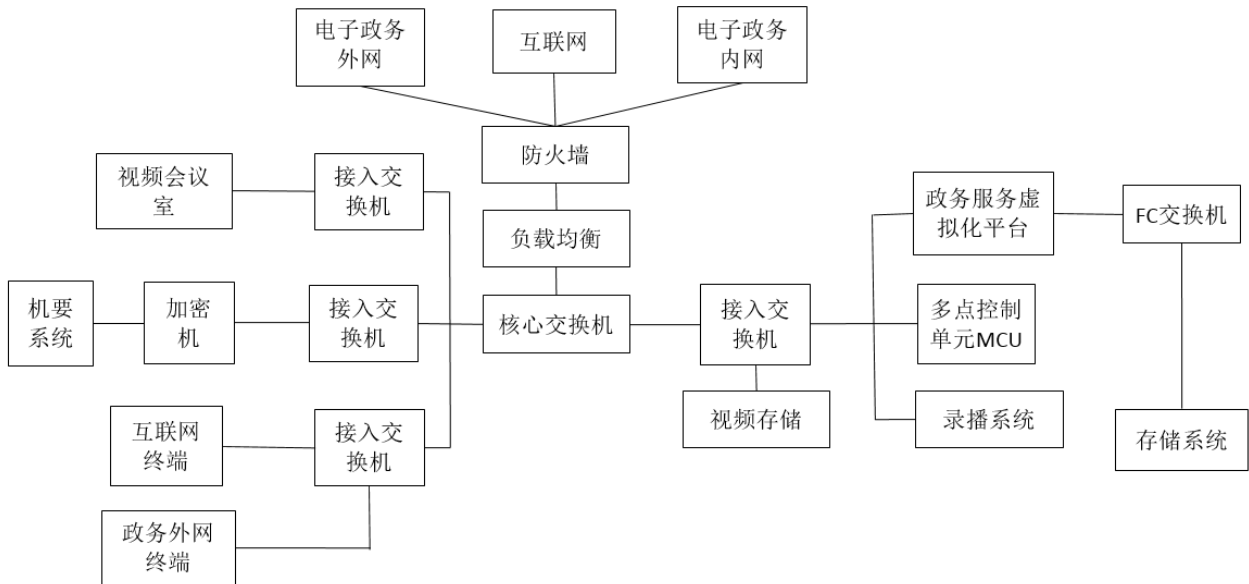
云管理工具（Cloud Management Platform）：基于企业云管理平台BSP，企业可以对各种云环境一目了然，帮助企业真正实现混合云管理；通过简单明了的资源利用趋势图，深入了解云成本和云资源情况，并提供资源和成本优化方案。

[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？需要在防火墙开放的TCP端口是什么？

【问题4】(4分)

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)。

参考答案：

视频解析

【问题1】

(1) 大二层网络结构包括接入层和核心层。

园区网是一种用户高密度的网络，在有限的空间内聚集了大量的终端和用户。扁平化大二层网络的设计注重的是三个“易”：易管理，易部署，易维护。

1、易管理：扁平化的大二层网络，整体简化了网络结构，网络中大量的接入、汇聚作为逻辑二层设备只需要做简单的VLAN划分、端口隔离配置即可，不需要过多管理，核心设备作三层网关，启用路由、认证、安全相关功能，日常维护中，管理员只需要维护核心设备即可，大大降低了网络的运维难度，简化了工作量。

2、易部署：大二层网络，无论是用户还是无线用户，无论是采用802.1x认证还是portal认证，认证统一集中在核心，部署方便快捷。同时，在大二层的环境中，大量的接入、汇聚设备配置基本类似，一些专注在行业的厂商也推出了快速配置工具用于批量设备上线时的快速配置下发，利用配置工具，操作过程简便，之前需要耗时几天的部署工作在2个小时内即可完成。

3、易维护：网络结构的简化将带来维护工作的简化，设备配置的简化必然会大幅度降低设备出问题的概率。从另一方面看，园区网的维护，需要在网络出现问题时能够快速定位，在网络管理层面上，需要把用户和端口对应起来，明确用户是从哪个端口接入上网，大二层架构中，利用VLAN聚合技术，可以轻松定位用户到具体的端口。

缺点是容易形成广播风暴，不适合大规模复杂网络。

(2) 通过对用户终端固定分配IP的方式，然后在路由设备上做策略路由。

(3) 机要终端信息系统不能接入其他网络中，应该是一个独立的网络；电子政务内网和电子政务外网之间需要使用物理隔离设备网闸、电子政务外网和互联网之间需要逻辑隔离设备防火墙。

【问题2】

(4) 每个视频会议每小时占用的存储空间为：8Mbps*3600/8=3600MB。

(5) 总的数据量=3600*4*2*100*8/1024*1024=22TB，存储这些用户数据需要22TB/3.6TB=7，题目说明用的RAID6以及有全局热备盘，所以还需要2块校验盘+1块热备盘，一共需要10块磁盘。

【问题3】

(6) 视频终端不需要。召开视频会议时候，由MCU连接各会场的视频终端，召开多方会议；局域网以外的其他部门的终端通过互联网访问MCU，需要对MCU配置一对一的NAT，映射公网IP，以供外部访问。

(7) 本视频会议用的是标准协议H.323，需要在防火墙的规则中， 打开端口。

端口 1503 (TCP) : Microsoft NetMeeting T.120 数据共享。

端口 1718 (UDP) : 网守查找。

端口 1719 (UDP) : 网守 RAS (必须为双向)。

端口 1720 (TCP) : H.323 呼叫设置 (必须为双向)。

端口 1731 (TCP) : 音频呼叫控制 (必须为双向)。

【问题4】

FC-SAN, NAS。

试题解析： 【问题1】

(1) 大二层网络结构包括接入层和核心层。

园区网是一种用户高密度的网络，在有限的空间内聚集了大量的终端和用户。扁平化大二层网络的设计注重的是三个“易”：易管理，易部署，易维护。

1、易管理：扁平化的大二层网络，整体简化了网络结构，网络中大量的接入、汇聚作为逻辑二层设备只需要做简单的VLAN划分、端口隔离配置即可，不需要过多管理，核心设备作三层网关，启用路由、认证、安全相关功能，日常维护中，管理员只需要维护核心设备即可，大大降低了网络的运维难度，简化了工作量。

2、易部署：大二层网络，无论是有线用户还是无线用户，无论是采用802.1x认证还是portal认证，认证点统一集中在核心，部署方便快捷。同时，在大二层的环境中，大量的接入、汇聚设备配置基本类似，一些专注在行业的厂商也推出了快速配置工具用于批量设备上线时的快速配置下发，利用配置工具，操作过程简便，之前需要耗时几天的部署工作在2个小时内即可完成。

3、易维护：网络结构的简化将带来维护工作的简化，设备配置的简化必然会大幅度降低设备出问题的概率。从另一方面看，园区网的维护，需要在网络出现问题时能够快速定位，在网络管理层面上，需要把用户和端口对应起来，明确用户是从哪个端口接入上网，大二层架构中，利用VLAN聚合技术，可以轻松定位用户到具体的端口。

缺点是容易形成广播风暴，不适合大规模复杂网络。

(2) 通过对用户终端固定分配IP的方式，然后在路由设备上做策略路由。

(3) 机要终端信息系统不能接入其他网络中，应该是一个独立的网络；电子政务内网和电子政务外网之间需要使用物理隔离设备网闸、电子政务外网和互联网之间需要逻辑隔离设备防火墙。

【问题2】

(4) 每个视频会议每小时占用的存储空间为：8Mbps*3600/8=3600MB。

(5) 总的数据量=3600*4*2*100*8/1024*1024=22TB，存储这些用户数据需要22TB/3.6TB=7，题目说明用的RAID6以及有全局热备盘，所以还需要2块校验盘+1块热备盘，一共需要10块磁盘。

【问题3】

(6) 视频终端不需要。召开视频会议时候，由MCU连接各会场的视频终端，召开多方会议；局域网以外的其他部门的终端通过互联网访问MCU，需要对MCU配置一对一的NAT，映射公网IP，以供外部访问。

(7) 本视频会议用的是标准协议H.323，需要在防火墙的规则中， 打开端口。

端口 1503 (TCP) : Microsoft NetMeeting T.120 数据共享。

端口 1718 (UDP) : 网守查找。

端口 1719 (UDP) : 网守 RAS (必须为双向)。

端口 1720 (TCP) : H.323 呼叫设置 (必须为双向)。

端口 1731 (TCP) : 音频呼叫控制 (必须为双向)。

【问题4】

FC-SAN, NAS。

【问题1】

(1) 大二层网络结构包括接入层和核心层。

园区网是一种用户高密度的网络，在有限的空间内聚集了大量的终端和用户。扁平化大二层网络的设计注重的是三个“易”：易管理，易部署，易维护。

1、易管理：扁平化的大二层网络，整体简化了网络结构，网络中大量的接入、汇聚作为逻辑二层设备只需要做简单的VLAN划分、端口隔离配置即可，不需要过多管理，核心设备作三层网关，启用路由、认证、安全相关功能，日常维护中，管理员只需要维护核心设备即可，大大降低了网络的运维难度，简化了工作量。

2、易部署：大二层网络，无论是有线用户还是无线用户，无论是采用802.1x认证还是portal认证，认证点统一集中在核心，部署方便快捷。同时，在大二层的环境中，大量的接入、汇聚设备配置基本类似，一些专注在行业的厂商也推出了快速配置工具用于批量设备上线时的快速配置下发，利用配置工具，操作过程简便，之前需要耗时几天的部署工作在2个小时内即可完成。

3、易维护：网络结构的简化将带来维护工作的简化，设备配置的简化必然会大幅度降低设备出问题的概率。从另一方面看，园区网的维护，需要在网络出现问题时能够快速定位，在网络管理层面上，需要把用户和端口对应起来，明确用户是从哪个端口接入上网，大二层架构中，利用VLAN聚合技术，可以轻松定位用户到具体的端口。

缺点是容易形成广播风暴，不适合大规模复杂网络。

(2) 通过对用户终端固定分配IP的方式，然后在路由设备上做策略路由。缺点：1、成本提高。缺省汇聚设备，导致对万兆/10万兆的端口数增加；2、对设备本身转发机制，计算处理能力，甚至产品架构提出更高要求，设备损耗老化较快。

(3) 机要终端信息系统不能接入其他网络中，应该是一个独立的网络；电子政务内网和电子政务外网之间需要使用物理隔离设备网闸、电子政务外网和互联网之间需要逻辑隔离设备防火墙。

【问题2】

(4) 每个视频会议每小时占用的存储空间为：8Mbps×3600/8=3600MB。

(5) 总的数量=3600×4×2×100×8/1024×1024=22.5TB，存储这些用户数据需要22TB/ 3600MB/1024TB=7，题目说明用的RAID6以及有全局热备盘，所以还需要2块校验盘+1块热备盘，一共需要10块磁盘。

【问题3】

(6) 视频终端不需要。召开视频会议时候，由MCU连接各会场的视频终端，召开多方会议；局域网以外的其他部门的终端通过互联网访问MCU，需要对MCU配置一对一的NAT，映射公网IP，以供外部访问。

(7) 从题目的描述来看，本视频会议用的是标准协议H.323，需要在防火墙的规则中，在防火墙中打开您在媒体端口范围（UDP 和 TCP）字段中指定的同一端口范围。还必须打开防火墙中的以下端口：

端口 1503（TCP）：Microsoft NetMeeting T.120 数据共享。

端口 1718（UDP）：网守查找。

端口 1719（UDP）：网守 RAS（必须为双向）。

端口 1720（TCP）：H.323 呼叫设置（必须为双向）。

端口 1731（TCP）：音频呼叫控制（必须为双向）。

【问题4】

图中存储系统连接FC交换机，应该是FC-SAN，视频存储题干已经说明以NFS格式挂载存储视频文件，所以是NAS。

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。

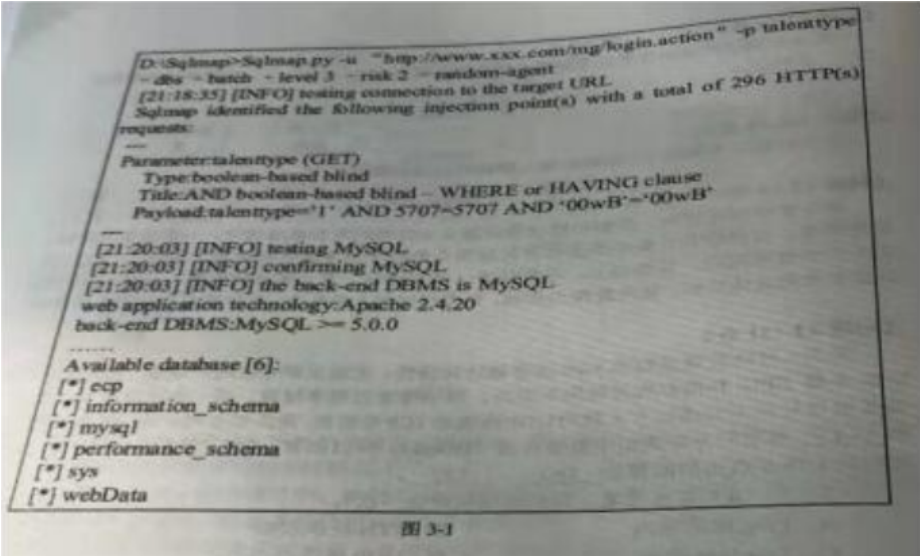


图 3-1

参考答案：

【问题1】

- (1) 安全预案
- (2) 安全策略

【问题2】

- (3) UDP泛洪攻击
- (4) SYN flooding攻击
- (5) A

(6) UDP泛洪（UDP flood）：攻击者通过向目标主机发送大量的UDP报文，导致目标主机忙于处理这些UDP报文，而无法处理正常的报文请求或响应。
 (7) SYN flooding攻击，通常发生在TCP连接需要进行三次握手过程中。当客户端向服务端发出请求时，首先会发送一个TCP SYN数据包。而后响应一个SYN ACK数据包。服务器随后将等待从客户端收到一个ACK 数据包。如果服务器没有收到ACK 数据包，TCP连接将处于半打开状态，直到服务器从客户端收到ACK数据包或者连接因为计时器超时为止。当一个攻击者有意地、重复地向服务器发送 SYN数据包，但不对服务器发回的SYN ACK 数据包答复ACK数据包时，就会发生TCP SYN flooding攻击。这时，服务器将会失去对资源的控制，无法建立任何新的合法TCP连接。WAF防护应用层流量的拒绝服务攻击，适合防御HTTP Get攻击等。

WAF服务并不提供针对四层及以下流量的防护，例如：ACK Flood、UDP Flood等攻击，这类攻击建议使用DDoS及IP高防服务进行防护。

【问题3】

- (8) mysql
- (9) Apache
- (10) SQL注入攻击
- (11) 使用参数化的过滤性语句
- (12) 使用专业的漏洞扫描工具、IPS、WAF等设备。

试题解析： 【问题1】

- (1) 安全预案
- (2) 安全策略

【问题2】

- (3) UDP泛洪攻击
- (4) SYN flooding攻击
- (5) A

(6) UDP泛洪（UDP flood）：攻击者通过向目标主机发送大量的UDP报文，导致目标主机忙于处理这些UDP报文，而无法处理正常的报文请求或响应。

(7) SYN flooding攻击，通常发生在TCP连接需要进行三次握手过程中。当客户端向服务端发出请求时，首先会发送一个TCP SYN数据包。而后响应一个SYN ACK数据包。服务器随后将等待从客户端收到一个ACK 数据包。如果服务器没有收到ACK 数据包，TCP连接将处于半打开状态，直到服务器从客户端收到ACK数据包或者连接因为计时器超时为止。当一个攻击者有意地、重复地向服务器发送 SYN数据包，但不对服务器发回的SYN ACK 数据包答复ACK数据包时，就会发生TCP SYN flooding攻击。这时，服务器将会失去对资源的控制，无法建立任何新的合法TCP连接。WAF防护应用层流量的拒绝服务攻击，适合防御HTTP Get攻击等。

WAF服务并不提供针对四层及以下流量的防护，例如：ACK Flood、UDP Flood等攻击，这类攻击建议使用DDoS及IP高防服务进行防护。

【问题3】

- (8) mysql
- (9) Apache
- (10) SQL注入攻击
- (11) 使用参数化的过滤性语句
- (12) 使用专业的漏洞扫描工具、IPS、WAF等设备。

【问题1】

(1) 网络与信息安全应急预案：为了切实做好财政系统网络与信息安全突发事件的防范和应急处理工作，提高财政系统预防和控制网络与信息安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保财政系统网络与信息安全，结合工作实际，制定本预案。在安全预案中需要明确安全等级划分、安全管理机构、处置机构、处置流程、处置方法等内容。

(2) 安全策略是对信息系统安全管理的目标和意图的描述，是对信息系统安全进行管理和保护的指导原则，是指导管理人员的行为、保护信息网络安全指南，在安全策略的指导下制定安全管理制度、组织实施、检查改进、保证信息系统安全保护工作的整体性、计划性和规范性，确保技术保护措施和管理手段的正确实施，使得信息系统数据的完整性、机密性和可用性受到全面的保护

【问题2】

(3) (4) (6) (7) 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，可以判断为SYN flooding攻击和UDP泛洪攻击。
 UDP泛洪（UDP flood）：攻击者通过向目标主机发送大量的UDP报文，导致目标主机忙于处理这些UDP报文，而无法处理正常的报文请求或响应。

SYN flooding攻击，通常发生在TCP连接需要进行三次握手过程中。当客户端向服务端发出请求时，首先会发送一个TCP SYN数据包。而后响应一个SYN ACK数据包。服务器随后将等待从客户端收到一个ACK 数据包。如果服务器没有收到ACK 数据包，TCP连接将处于半打开状态，直到服务器从客户端收到ACK数据包或者连接因为计时器超时为止。当一个攻击者有意地、重复地向服务器发送 SYN数据包，但不对服务器发回的SYN ACK 数据包答复ACK数据包时，就会发生TCP SYN flooding攻击。这时，服务器将会失去对资源的控制，无法建立任何新的合法TCP连接。

- (5) A

【问题3】

(8) 从图中可以清晰地看出是mysql数据库，web服务器使用的软件是Apache，改WEB服务器存在SQL注入攻击漏洞，防范措施可以使用参数化的过滤性语句、使用专业的漏洞扫描工具、使用IPS、WAF等设备。