2021年11月 网络规划设计师 模考大赛 下午

一、问答题 (本大题共13个小题，总75分)

试题一（共25分）
阅读以下说明，回答问题1至问题5，将解答填入答题纸对应的解答栏内。
某集团公司在在全国各省均有分公司，由于公司的信息化系统需要升级改造，现管理员决定在总部与分公司之间通过IPSEC VPN建立连接。根据拓扑图1-1，完成下列问题。

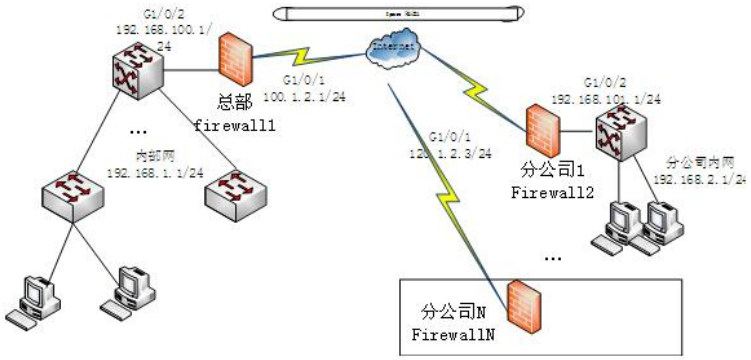

图 1-1

1/[问答题] 子问题1 (3分)

[问题1](3分)
该公司所选用的VPn技术为IPSec。它工作在TCP/IP协议栈的（1）层，能为TCP/IP通信提供访问控制机密性、数据源验证、抗重放、数据完整性等多种安全服务。其中能够确保数据完整性，但是不确保数据机密性的协议是（2），既能报数数据传输的机密性又能保证数据完整性的是协议是（3）。

2/[问答题] 子问题2 (8分)

[问题2]（8分）：请将相关配置补充完整。
总部防火墙firewall1的部分配置如下。
…
配置Trust域与Untrust域的安全策略，允许封装前和解封后的报文能通过
[FIREWALL1] （5）
[FIREWALL1-policy-security] rule name 1
[FIREWALL1-policy-security-rule-1] source-zone （6）
[FIREWALL1-policy-security-rule-1] destination-zone untrust
[FIREWALL1-policy-security-rule-1] source-address （7）
[FIREWALL1-policy-security-rule-1] destination-address（8）
[FIREWALL1-policy-security-rule-1] quit
[FIREWALL1] acl 3000
[FIREWALL1-acl-adv-3000] rule （9）ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[FIREWALL1-acl-adv-3000] quit
---------- 下面的这一段配置的作用是（10）
[FIREWALL1-policy-security] rule name 3
[FIREWALL1-policy-security-rule-3] source-zone local
[FIREWALL1-policy-security-rule-3] destination-zone untrust
[FIREWALL1-policy-security-rule-3] source-address 202.1.3.1 32

[FIREWALL1-policy-security-rule-3] destination-address 202.1.5.1 32
[FIREWALL1-policy-security-rule-3] action permit

---------- 下面的这一段配置的作用是（11）
[FIREWALL1] acl 3000
[FIREWALL1-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[FIREWALL1-acl-adv-3000] quit
---------- 下面的这一段配置的作用是（12）
[FIREWALL1] ipsec proposal tran1
[FIREWALL1-ipsec-proposal-tran1] encapsulation-mode tunnel
[FIREWALL1-ipsec-proposal-tran1] transform esp
[FIREWALL1-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[FIREWALL1-ipsec-proposal-tran1] esp encryption-algorithm aes
[FIREWALL1-ipsec-proposal-tran1] quit

3/[问答题] 子问题3 (4分)

[问题3] [4分]
在采用IKE动态协商方式建立IPSec隧道时，SA有两种：分别是IKE SA和IPSec SA，简述这两种SA的区别。

4/[问答题] 子问题4 (5分)

[问题4][5分]
IKE协商阶段有两种模式，分别是主模式和野蛮模式。管理员检查配置后发现，VPN两端都是基于IP地址实现预共享秘钥，并且公司希望创建VPN时，需要对对端身份进行保护，确保较高的安全性。因此应该选择哪种模式？为什么？

5/[问答题] 子问题5 (5分)

[问题5][5分]
IPSec提供的两种封装模式分别是传输Transport模式和隧道Tunnel模式，基于公司对传输数据的要求，适合选择的模式是哪一种？为什么？

试题2
某大型连锁零售企业X拥有总部网络和多个营业部网络，在各地营业部网络和总部网络之间通过互联网网络连接。每个营业部大约有员工50~60多人。具体拓扑如图1所示。

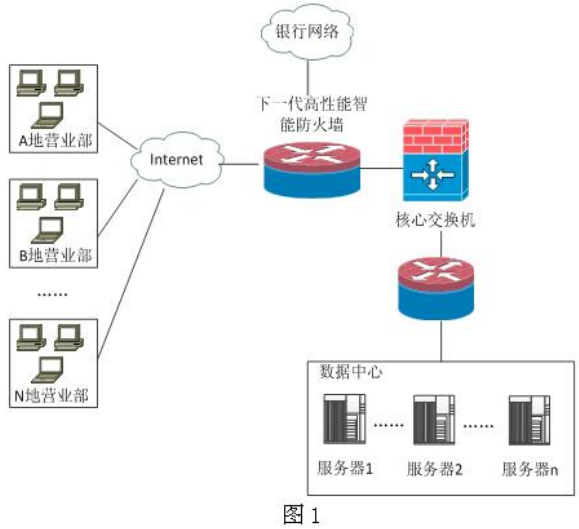

图 1

6/[问答题] 子问题1 (10分)

【问题1】（10分）

随着信息技术的发展，企业的信息系统越来越成为企业生存发展的核心资源，为了确保核心资源信息安全，需在不同位置部署不同的安全设备，进行安全防范。

为了避免公司电子商务平台Web服务器被非法攻击和篡改，需要部署（1）

为了提高管理员应对网络攻击的管理能力，需要部署（2），对日志进行备份和后期对网络攻击行为进行进一步分析，提高安全防御能力。

为了规范公司员工的网络行为，避免工作时间处理非工作业务，可以部署（3）。

为了确保公司关键商业数据，需要对数据进行备份，部署（4），可以实现虚拟化备份。

为了规范管理员对商品的打折，上架，下架等处理，需要部署（5）对商品数据的修改/删除等行为进行监管。

A.入侵检测系统 B. 漏洞扫描系统 C. 入侵防御系统 D.WAF

E.数据库审计 F.日志备份与审计 G.上网行为管理系统　H.备份一体机

7/[问答题] 子问题2 (4分)

【问题2】（4分）

为了满足总部海量数据的分析处理，要求数据中心的服务器能高效利用硬件资源，公司决定在数据中心区进行服务器虚拟化，适合采用的方式是（6），它的特点包括（7）（8）（9）。【从操作系统支持，运维效率和性能等方面回答】

8/[问答题] 子问题3 (3分)

【问题3】

lan-free这种备份方式从字面意思就可以知道几乎不占用局域网资源；因此基本特点就是备份速度快而对网络几乎不存在传输压力，这种备份方式通常都是基于San结构来进行，在备份过程中需要服务器参与，因此投资包含了SAN部分相对较高。周一采用完全备份后续周二至周五均采用增量备份是数据量最小的一种备份方式因此可以节省存储空间。

这里注意一下：

增量备份,是在一次全备份或上一次增量备份后,以后每次的备份只需备份与前一次相比增加或者被修改的文件。 差异备份,是复制上次全备份以来所有变更数据的一种备份。?增量备份没有重复的备份数据,备份的数据量不大,备份所需的时间很短,备份速度快。同时由于增量备份在做备份前会自动判断备份时间点及文件是否已作改动,所以相对于完全备份其对于节省存储空间也大有益处。

9/[问答题] 子问题4 (6分)

【问题4】（6分）

某天，网络管理员检测到部分攻击日志如图2所示，则该攻击为(14) 攻击， 图3访问日志所示的攻击行为是(15) 攻击。 可以发现并利用给定的URL漏洞的自动化的工具是(16)。

112.102.*.* 访问 www.xxx.com/default/accept.php 可疑行为：eval(base64_decode(S_POST['term'];?,已拦截

图 2

112.102.*.* 访问 www.xxx.com/GoodsType.php/type= 'union select 0，username+CHR(124)+password from admin

图 3

备选答案:

A.一句话木马　B. SQL注入　C.DDOS　D. APT

E.DDos　F.蠕虫病毒　G.SQLMAP H.Nmap

试题三：

阅读以下说明，回答问题1至问题4，将解答填入答题纸对应的解答栏内。

【说明】

某电子商务公司网络拓扑结构如图 3-1 所示。网络规划如表3-1所示。

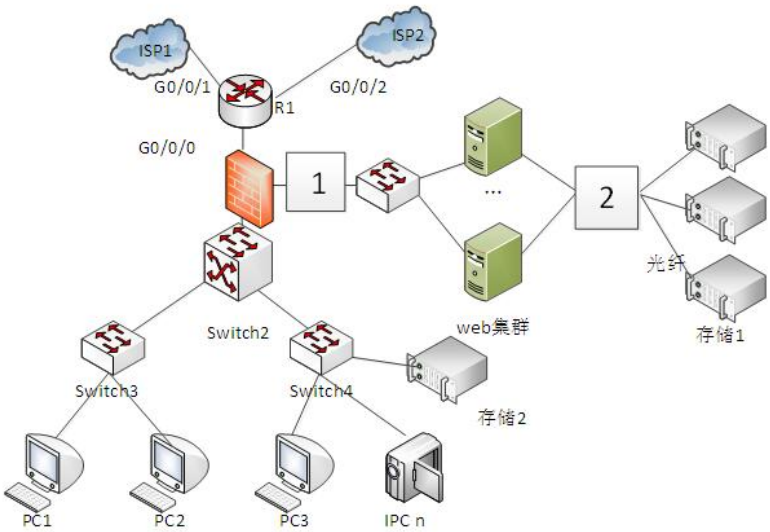

图 3-1

设备	接口	IP 地址	描述
Isp1		58.60.36.1/29	Isp1 的网关地址
Isp2		113.250.13.1/30	Isp1 的网关地址
R1	GE0/0/0	192.168.200.1/24	R1 的 GE0/0/0 接口地址
	GE0/0/1	58.60.36.2/29	R1 的 GE0/0/1 接口地址
	GE0/0/2		R1 的 GE0/0/2 接口地址
Switch2	Vlanif 10	192.168.8.254/24	网段 1
	…	…	…
	Vlanif 12	192.168.190.254/24	网段 n
	Vlanif 200	192.168.200.3/24	Vlan 接口地址，连出口设备

10/[问答题] 子问题1 (6分)

【问题1】（6分，每空1分，问题4分）公司的Web集群经常遭到各种攻击，典型的如SQL注入，XSS等，为了提高公司web服务器集群的可用性，应该图中标注为1的方框处添加（1）设备,为了提高存储效率和性能，在图中标注2的方框处添加（2）设备。公司的主要业务全部基于WEB应用，因此对WEB系统的可靠性要求比较高，从现有拓扑图看，可能影响公司WEB系统可靠性的问题有哪些，如何解决（列举2点即可）？

11/[问答题] 子问题2 (5分)

【问题2】（5分，选择每空1分）

如图3-1所示，防火墙的三个接口由内而外的默认名字分别是（ 3 ）、（ 4 ）、（ 5 ）。从本题的拓扑图来看，该防火墙工作在（6）模式。

（3）~（5）备选项：

A.trust区域　B.untrust区域　C.DMZ区域

12/[问答题] 子问题3 (8分)

【问题3】（8分，每空2分）

如图3-1所示，ISP1作为公司的默认互联网出口。该公司拥有2条出口链路，要保证内网机器能够访问互联网，需要在路由器上配置（ 7 ），管理员希望服务器网段的流量都走ISP2出去，则需要在路由器上配置（8 ），因为服务器网段的IP地址是内网地址，服务器要对Internet提供服务，需要在路由器上配置（ 9 ），生产区和办公区访问互联网默认走ISP1，需要在路由器上配置（ 10 ）。

（7）~（10）备选项：

A.策略路由　B.缺省路由　C. 源NAT　D.目的NAT

13/[问答题] 子问题4 (8分)

【问题4】（8分，每空2分）

图中采用的SAN技术中，对应存储1与存储2分别是（11）和（12），公司现有业务系统的数据为400MB，为了保证数据的安全，目前采用的备份策略是每周一采用完全备份，周二到周五每天采用增量备份，公司的业务系统只在周一到周五期间运行，每个工作日新增的业务数据约40MB，公司要求所有数据备份保留半年，采用raid5保存数据（备份数据单独采用raid5系统保存），则备份系统至少需要（13）TB才能满足需求，如果采用8TB的硬盘来组成阵列，需要（14）块硬盘组成。