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。

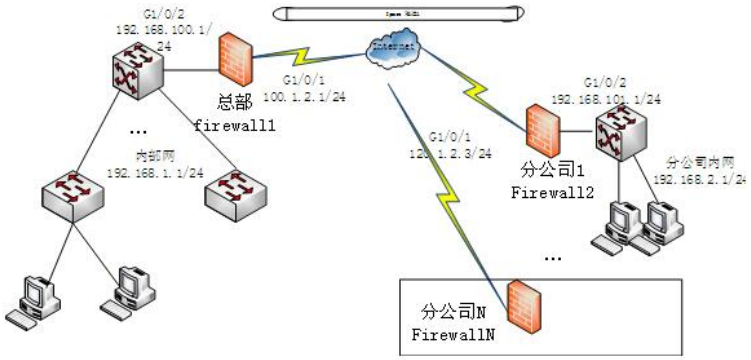

图 1-1

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）。

参考答案:

（1）网络 （2）AH （3）ESP

答案解析：IPSec工作在TCP/IP协议栈的网络层，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。

（1）AH。

认证头（Authentication Header，AH）是IPSec体系结构中的一种主要协议，它为IP数据报提供完整性检查与数据源认证，并防止重放攻击。AH不支持数据加密。AH常用摘要算法（单向Hash函数）MD5和SHA1实现摘要和认证，确保数据完整。

（2）ESP。

封装安全载荷（Encapsulating Security Payload，ESP）可以同时提供数据完整性确认和数据加密等服务。ESP通常使用DES、3DES、AES等加密算法实现数据加密，使用MD5或SHA-1来实现摘要和认证，确保数据完整。

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 1
92.168.2.0 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

参考答案：

(5) security-policy（6) trust （7） 192.168.1.0 24

(8) 192.168.2.0 24？(9) permit

（10）配置Local域与Untrust域的安全策略，允许IKE协商报文能正常通过FIREWALL1

（11） 配置访问控制列表，定义需要保护的数据流。

（12）配置名称为tran1的IPSec安全提议

答案解析：1. 配置安全策略，允许私网指定网段进行报文交互。

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] security-policy

[FIREWALL1-policy-security] rule name 1

[FIREWALL1-policy-security-rule-1] source-zone trust

[FIREWALL1-policy-security-rule-1] destination-zone untrust

[FIREWALL1-policy-security-rule-1] source-address 192.168.100.0 24

[FIREWALL1-policy-security-rule-1] destination-address 192.168.200.0 24

[FIREWALL1-policy-security-rule-1] action permit

[FIREWALL1-policy-security-rule-1] quit

.....

配置Local域与Untrust域的安全策略，允许IKE协商报文能正常通过FIREWALL1。

[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

[FIREWALL1-policy-security-rule-3] quit

[FIREWALL1-policy-security] rule name 4

[FIREWALL1-policy-security-rule-4] source-zone untrust

[FIREWALL1-policy-security-rule-4] destination-zone local

[FIREWALL1-policy-security-rule-4] source-address 202.1.5.1 32

[FIREWALL1-policy-security-rule-4] destination-address 202.1.3.1 32

[FIREWALL1-policy-security-rule-4] action permit

[FIREWALL1-policy-security-rule-4] quit

[FIREWALL1-policy-security] quit

3. 配置IPSec隧道。

配置访问控制列表，定义需要保护的数据流。

[FIREWALL1] acl 3000

[FIREWALL1-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.16

8.2.0 0.0.0.255

[FIREWALL1-acl-adv-3000] quit

配置名称为tran1的IPSec安全提议。

[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。

参考答案：

建立IKE SA目的是为了协商用于保护IPSec隧道的一组安全参数【2分】，建立IPSec SA的目的是为了协商用于保护用户数据的安全参数【2分】，但在IKE动态协商方式中，IKE SA是IPSec SA的基础。

答案解析：IKE SA 和 IPSec SA的区别

在采用IKE动态协商方式建立IPSec隧道时有两种形式的SA：一种IKE SA，另一种是IPSec SA。其中IKE SA的作用是为了协商用于保护IPSec隧道的一组安全参数，而IPSec SA的目的是为了协商用于保护用户数据的安全参数，在IKE动态协商方式中，IKE SA是基础，后续IPSec SA的建立都是使用的IKE SA建立的一系列密钥完成的。

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？

参考答案：

主模式 【1分】

1.两端时基于IP地址的形式进行预共享秘钥，适合用主模式。【2分】

2.只有主模式才能对对端身份进行保护，安全性较高。【2分】

答案解析：对于二端IP地址不固定的时或者两边都是主机名的时就必须用野蛮模式来协商。而本题中发现两端时基于IP地址的形式因此可以是用主模式。同时，只有主模式才能对对端身份进行保护，安全性较高。

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？

参考答案：
隧道模式 【1分】
1.传输模式在处理前后IP头部保持不变，主要用于End-to-End的应用场景。【2分】
2.隧道模式则在处理之后再封装了一个外网IP头，主要用于Site-to-Site的应用场景。【2分】

答案解析：传输模式和隧道模式的区别：
1.传输模式在处理前后IP头部保持不变，主要用于End-to-End的应用场景。
2.隧道模式则在处理之后再封装了一个外网IP头，主要用于Site-to-Site的应用场景。理论上?隧道模式适合任意的应用场景，但是在本题中，是总部和各个分公司的之间的连接，因此应该选隧道模式。

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。

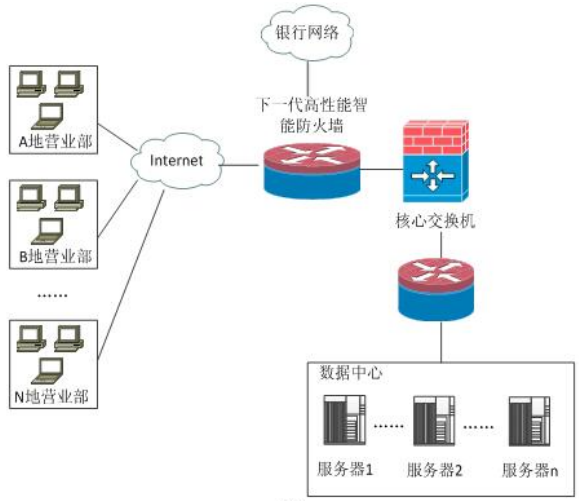

图 1

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

参考答案：

【问题1】（10分）

（1）D（2）F（3）G（4）H（5）E

答案解析：【问题1】

本题实际考的就是基本概念。一定要充分了解题干中的详细说明这个关键词所表达的意思，再对照选项即可进行选择。

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】

参考答案：

【问题2】（4分）

(6),裸金属架构/原生架构

7～9,特点：（可以交换顺序）

1.可支持多操作系统多应用

2.运维高效便捷

3.资源利用率高

答案解析：【问题2】

从题干的要求是要提高效率充分发挥服务器的能力以满足高性能的需求，因此需要选用裸金属架构。裸金属架构的特点是可以支持多操作系统多应用并且资源利用率高，不依赖于主机操作系统直接由虚拟层进行管理，运维高效便捷。

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。

参考答案：

【问题3】（5分）

(10),A

(11),C

(12),D(10～12可以变换位置)

(13),增量备份，(2分)

答案解析：【问题3】（5分）

(10),A

(11),C

(12),D(10～12可以变换位置)

(13),增量备份，(2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

参考答案:

【问题4】（6分）

（14）,A

（15）B

（16）,G

答案解析：【问题4】

关键词eval(base64_decode(S_POST[])实际就是PHP中的一个常用的函数，它会将使用base64编码的内容解码之后，再执行，通常可以在其中执行一行语句的代码以实现木马，所以称为一句话木马。

在网页中如果有嵌入SQL代码的一些关键词如select，Insert，update，union等，往往就是典型的SQL注入。

sqlmap是一个自动化的SQL注入工具，其主要功能是扫描，发现并利用给定的URL的SQL注入漏洞，日前支持的数据库是MS-SQL,,MYSQL,ORACLE和POSTGRESQL。

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。

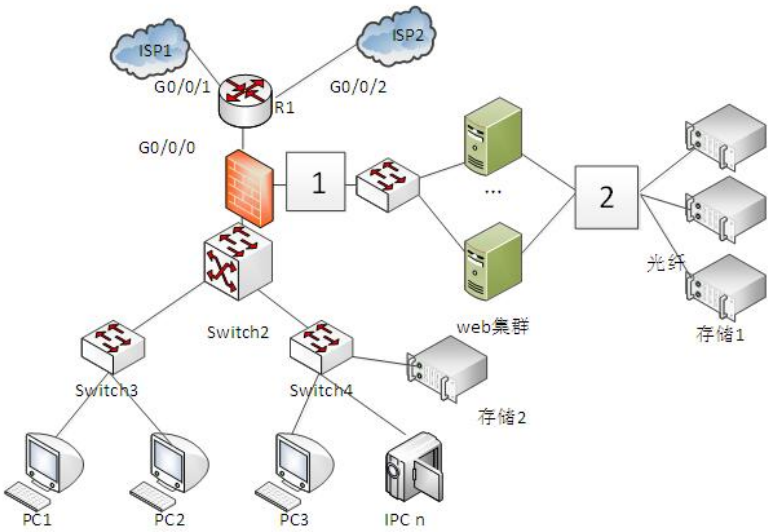

图 3-1

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）？

参考答案：

（1）WAF,【1分】

（2）FC交换机,,【1分】

,,,（只要能言之有理的影响web集群可靠性的因素都可以）【4分】

,,如：交换机处存在单点故障，可以部署两台交换机，使用生成树协议。

,,,,出口路由器存在单点故障，可以部署双路由器。

答案解析：显然从拓扑图可以看出，web集群所在的位置应该能对外提供web服务，在防火墙的DMZ区中，web集群与防火墙之间的设备可能是一种安全设备。而WAF是一种专门针对web应用的安全设备，通常接在web服务器前，因此这个设备可能是WAF。服务器后端是一个光纤连接的存储资源池，因此应该是FC交换机。

可能影响web系统可靠性的主要是从web系统到ISP端可能存在的设备单点故障。如web集群前面的交换机做成双机，采用冗余线路。防火墙和路由器多可以使用双设备等，或者其他可行答案。

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

参考答案：

（3）A,（4）C,（5）B,（6）透明

答案解析：防火墙的三个接口分别接内网，外网和非军事化区，在华为设备中，这三个区域分别叫做trust区域，untrust区域 和DMZ区域。从路由器R1内部接口地址和Switch2出口地址可以看到，同属于192.168.200.0/24,因此防火墙应该是透明模式。

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

参考答案：

（7）C,（8）A,（9）D,（10）B

答案解析：内网机器使用的内部地址，不能访问internet，因此需要配置基于原地址的NAT。不同的内网段走不同的出口访问Internet，配置策略路由即可实现。在进行内网地址映射的时候，实际也可以配置基于目的的nat。默认走某个接口，配置默认路由即可。

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。

参考答案：

（11）FC-SAN ,(12),IP-SAN。

（13）78.7GB,（14）,11

答案解析：从拓扑可以看出，存储1是直接接在以太网交换机上组成的存储区域网络，应该是IPsan

而存储2所在的SAN是基于FC交换机的FC SAN。

每周一完全备份，需要400MB，每个工作日增加40MB数据，并且周二到周五都进行增量备份。因此到下周周一数据量变为：400MB+40M*5=600MB；这一周的备份数据有一个完全备份400MB，5个增量备份总共200MB，总的备份数据为600M。每过一周，备份数据增加200MB。

因此总的备份数据量M=600MB+800MB+1000MB+.....（一共24项），求这个等差数列的和即可。

$$S_n = na_1 + \frac{n(n-1)}{2}d, n \in N^*$$

半年时间约等于=26周。因此N=26，a1=600，d=200，代入公式Sn=24*600+12*23*200=80600MB

折合成GB=80600MB/1024=78.9GB。约合79TB。

Raid5 的硬盘利用率为（n-1）/n，因此需要的硬盘数为79/8+1=11块。