

一、技巧:

• 复习时选择题区域快速过，看资料时很多东西只要大概了解就行，重点在主观题。

选择题以刷题进行记忆为主。

• 如果简答题一个答案不确定，可以如下这样写，把可能性最大的那个写前面

问：请问：X最有可能代表的安全设备是什么？简要描述该设备的工作原理。

答：

可以使用网闸，原理是xxx

也可以使用入侵检测系统IDS，原理是xxx

也可以使用入侵防护系统IPS，原理是xxx

• 自己复习或做整理时，到第二遍的时候，认为不重要的不写或者直接删掉好了，反正也背不过来。

二、新考纲简答题预测：

4. 隐藏Apache软件的版本号

修改httpd.conf, 设置

ServerSignature Off

ServerTokens Prod

重启apache

5. Apache目录访问安全性增强

三步

(1) 禁止使用目录索引文件（即没有index.html的情况会列出目录）

修改配置文件httpd.conf

Options -Indexes FollowSymLinks

三、常见考点：

面向数据挖掘的隐私保护技术：

基于数据失真的隐私保护技术

~数据匿名

~数据加密

网络安全基本属性：机密性、完整性、可用性、抗抵赖性、可控性

CIA

信息安全特性： 保密性、完整性、可用性、抗抵赖、可控

密码学安全目标：保密性、完整性、可用性及抗抵赖性。

三类专用地址

A类：10.0.0.0 - 10.255.255.255

B类：172.16.0.0 - 172.31.255.255

C类：192.168.0.0 - 192.168.255.255

BLP模型：

安全性是不可上读

特性是不可下写

即控制策略是上写下读

保证了信息的秘密性。

上读下写保证了数据的完整性，上写下读保证了信息的秘密性。

PKI包含五个实体部分：

1. CA 证书授权机构，证书的颁发、废止和更新；（可信第三方机构）
证书管理、签发、验证、撤销
2. RA 证书注册登记机构、担保；
3. 客户端
4. 终端实体
5. 目录服务器

防火墙过滤不去匹配 源端口，不检查数据包内容。

国产商用密码算法

SM1 对称加密算法

SM2 椭圆曲线数字签名算法

SM3 杂凑算法 消息分组长度为512位，输出256

SM4 对称加密算法 无线局域网产品使用，WAPI协议

SM9 标识数字签名算法

SM2椭圆曲线数字签名算法 和 SM9标识数字签名算法是我国国家密码管理局发布的数字签名标准。

2017年11月 德国柏林 sm2椭圆曲线 sm9标识签名算法 成为国际标准。

2006 年我国政府公布了自己的商用密码算法sm4

我国制定的无线局域网强制标准是WAPI，用到了sm4

linux目录解析

/etc/passwd shadow group 各个字段含义

/etc/passwd 权限644 rw- r-- r--
/etc/group 权限644 rw- r-- r--
/etc/shadow 权限640 r-- --- --

答题时把数字，字符形式以及权限描述都写上去吧

PPTP L2TP是第二层的VPM隧道协议，IPsec是第三层的VPN隧道协议。

防火墙三种数据处理方式：

Accept、Reject、Drop

53端口DNS udp

防火墙防御体系结构：

1. 基于双宿主主机防火墙结构：

将一个内部网络和外部网络分别连接在不同的网卡上。使不同的内外网络不能直接通信。即一台主机，两张网卡，连接内外网。这样一台主机被被称为双宿主主机。

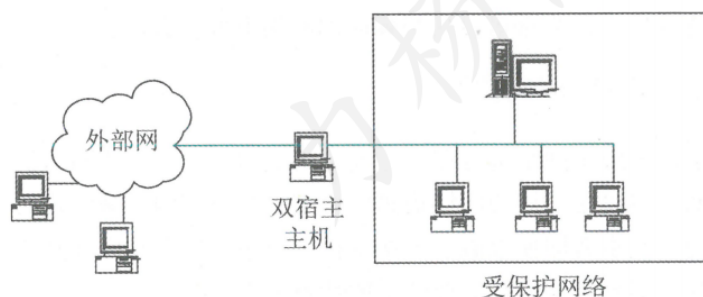


图 8-12 双宿主主机防火墙结构

2. 基于代理型防火墙结构：

由一台主机代理内部网和外部网的通信，

代理服务器主机 与外网之间还经过 过滤路由器过滤。

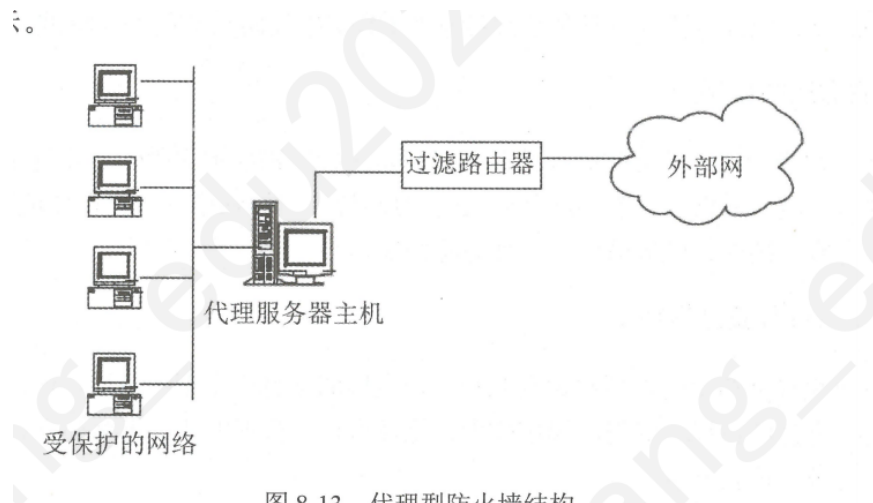


图 8-13 代理型防火墙结构

3. 基于屏蔽子网防火墙结构:

在代理型结构中增加了一层周边网络的安全机制，使内部网络和内部网络有两层隔离带。

代理服务器主机与内网之间也加了一台过滤路由器保护。

外面那个过滤外网对被屏蔽子网的访问，里面那个过滤被屏蔽子网对内部网络的访问

优点：安全

缺点：复杂、成本高

堡垒机和DMZ区在两个过滤之间。

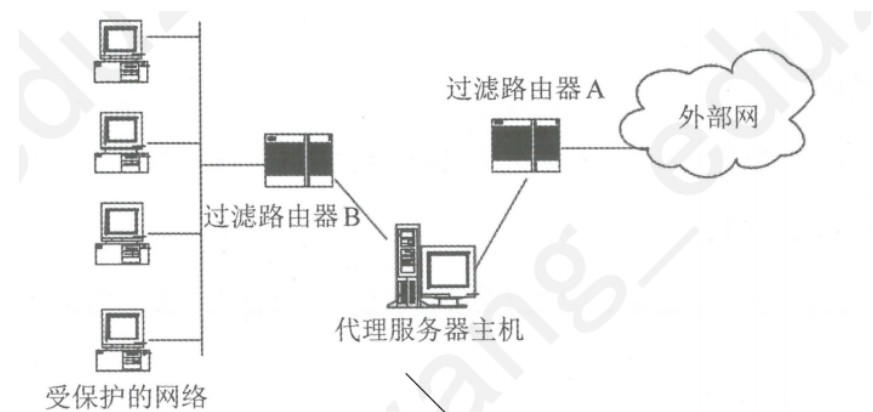


图 8-14 屏蔽子网防火墙结构

S/key口令 一次性口令 对抗重放。

kerberos身份认证协议加密算法是DES。

1. 通过iptables防火墙关闭23端口

```
1 iptables -A INPUT -p tcp --dport 23 -j DROP
2 iptables save
```

//

httpd.conf

```
1 <Directory "你要限制访问的目录">
2     Order Deny,Allow//允许指定字段访问，禁止其他所有字段
3     Deny from all
4     Allow From 192.168.0.0/24 //允许指定字段的访问
5     Allow From 127.0.0.1
6     Allow From 59.37.x.x/28
7     //----如果是以下，即为限制从192.168.0 和 127.0.1这两个字段内的用户访问，别的
    用户可以
8     Allow From all
9     Deny From 192.168.0
10    Deny From 127.0.0.1
11 </Directory>
12
13
14
15 <Files "你要限制访问的文件名">
16     Order Deny,Allow
```

```
17 //允许指定字段访问，禁止其他所有字段
18     Deny from all
19 Allow From 192.168.0.0/24 //允许指定字段的访问
20 Allow From 127.0.0.1
21 Allow From 59.37.x.x/28
22 //----如果是以下，即为限制从192.168.0 和 127.0.1这两个字段内的用户访问，别的
    用户可以
23 Allow From all
24 Deny From 192.168.0
25 Deny From 127.0.0.1
26 </Files>
```

linux目录解析

/etc/passwd shadow group 各个字段含义

/etc/passwd 权限644 rw- r-- r--

/etc/group 权限644 rw- r-- r--

/etc/shadow 权限640 r-- --- --

Linux有7种运行模式 init 0-6

0 关机

1 单用户模式

2 多用户模式

3 切换到命令行模式 服务一般处于这种模式

4 未被使用的模式

5 切换到桌面模式

6 重启

网络安全等级保护工作主要包括 定级、备案、建设整改、等级测评、监督检查 五个阶段。

安全保护五个等级：

- 第一级（用户自主保护级）
- 第二级（系统保护审计级）
- 第三级（安全标记保护级）
- 第四级（结构化 保护级）
- 第五级（访问验证保护级）

四、一般考点:

网络安全事件分级：

网络安全事件级别	描述
特别重大网络安全事件（Ⅰ级）	特别严重威胁、特别严重影响
重大网络安全事件（Ⅱ级）	严重威胁、严重影响
较大网络安全事件（Ⅲ级）	较严重威胁、较严重影响
一般网络安全事件（Ⅳ级）	一定威胁、一定影响

zuc祖冲之算法是非线性算法。

SSL协议不能提供可用性，位于应用层和TCP层之间。运行在传输层之上

信息安全风险评估：资产识别、威胁识别、脆弱性识别

代码静态分析：模式匹配、定理证明、模型检测

sm4 分组和密钥都是128位。

数字证书包含：用户身份信息、持有者的公开秘钥以及CA的数字签名信息。

IDEA 是国际数据加密算法的简记，是一个分组加密处理算法，其明文 和密文分组都是 64 比特，密钥长度为 128 比特。

应用：

PGP(Pretty Good Privacy) 使用IDEA作为其密钥管理算法。

- 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存 相关的网络日志不少于六个月。
- 网络安全等级保护的主要工作可以概括为定级、备案、建设整改、等级测评、运营维护。

五、次级考点：

hash：单向性、抗弱碰撞性、抗强碰撞性

TCP/IP协议

SYN：建立连接，同步握手信号。

ACK：响应，确认字符

FIN：关闭连接

非对称加密算法：

[RSA](#)、[Elgamal](#)、[Rabin](#)、[DH](#)、[ECC](#)（椭圆曲线加密算法）。

