10、传输模式和隧道模式有何区别？

答：传输模式：主要为上层协议服务，保护原 IP 数据包的有效载荷部分；隧道模式：为整个 IP 数据包做保护。

11、为什么 ESP 包括一个填充域？

答：加密算法要求明文为某字节的倍数（分组密码），填充域用于拓展字节；ESP 格式要求“填充长度”和“下一个头”字段右对齐，填充域用来对齐。隐藏有效载荷长度，用以保密。

【注：要大致清楚 ESP 协议报文格式、字段，AH 协议报文字段。特别是其中的这两个协议如何实现消息认证，消息认证的 HMAC 长度、使用的 HMAC 算法有那些。】

12、假设当前的重放窗口由 120 拓展到 530：

A、如果下一个进来的已认证包序列号 105，则接收者如何处理该包？处理后的窗口参数（窗口值）是多少？

B、如果下一个进来的已认证包序列号 440，则接收者如何处理该包？处理后的窗口参数（窗口值）是多少？

C、如果下一个进来的已认证包序列号 540，则接收者如何处理该包？处理后的窗口参数（窗口值）是多少？

答：A、105<120，丢弃分组，不改变窗口参数值

B、120<440<530，在窗口中，校验 MAC 值，如果是认证的，则相应的序列号在窗口中被标记，如果已经标记，则是重复分组，则丢弃。两种情况不会造成窗口值变化。

C、540>530，在窗口右侧，则校验 MAC，判断是否已经标记，如果没有标记，则窗口进行滑动，参数值为 120~540。

【注：需要要求学生对抗重放窗口原理掌握熟练，面对这种预设的现实考题，需要学生试用相关原理进行作答。考查的形式多种多样，但是考点不会脱离书本内容。学生面对一道题目，需要明白出题人是要考察哪些知识点。按知识点进行答题，才能得到全部分数。比如此题，考察的就是抗重放窗口的原理，碰到不同序列号的报文，抗重放窗口是如何处理的。衍生的考察点还有，抗重放窗口的大小？当序列号用尽时候是该做什么处理？由什么模块负责处理序列号用尽？常见重放攻击主要分为几

种？抵御重放攻击主要方法有哪些？给你个具体场景，请你设计一个抵御重放攻击的协议....等等，见考纲教材 P142】

13、表中显示了一个 IP 地址从 192.168.1.0 到 192.168.1.254 的网络的包过滤规则例子，请描述每条规则的作用。

	源地址	源端口	目的地址	目的端口	动作
1	任意	任意	192.168.1.0	>1023	允许
2	192.168.1.1	任意	任意	任意	拒绝
3	任意	任意	192.168.1.1	任意	拒绝
4	192.168.1.0	任意	任意	任意	允许
5	任意	任意	192.168.1.2	SMTP	允许
6	任意	任意	192.168.1.3	HTTP	允许
7	任意	任意	任意	任意	拒绝

答：1、允许返回的 TCP 连接能进入内部网络

2、阻止防火墙本身想外直接连接（此处 192.168.1.1 应为应用网关防火墙）

3、阻止外网用户直接访问防火墙

4、内部用户可以连接外部服务器

5、允许外部向子网内发送邮件

6、允许外部用户连接内网的 Web 服务器

7、以上被允许进入之外的所有接入被拒绝

【注：目前 837 没有考察过任何网络防御的知识点，包括 Netfilter/IPtables，入侵检测系统这些知识点。从未考察过大题，需要引起一下重视。】

14、填空题：电路级网关工作在（ ）层？

答：传输

15、填空题：只有一块网卡的防火墙被称为（ ）；双宿堡垒主机可以（ ）；三宿堡垒主机可以建立（ ）

答：单宿堡垒主机、将内外网隔离、DMZ 区

【注：教材中没有防火墙体系结构的内容，但是哈工大本部翟健宏老师 PPT、许海燕老师 PPT 中均对这部分内容进行了较为详细的讲解。如果出设计题目，可能要学生从防火墙体系结构的角度出发设计内网结构。具体见哈工大(威海)信息安全导论期末试卷题目与解答，解答见笔记基础部分。】

16、填空题：木马隐藏通信的方法有：（ ）、（ ）

答：端口复用，反弹端口

【注：木马隐藏技术主要有隐藏进程、隐藏文件、隐藏通信这三种。需要学生对三种隐藏技术的原理进行了解，比如隐藏进程方法主要是：修改 API 入口函数，隐藏文件方法：拦截 API 函数调用。】

17、NT 安全子系统中，WinLogan 最先调用（ ）模块

答：GINA

【注：访问控制一章中，书本教材用了很大篇幅讲解 Windows 系统的安全管理，但是 837 考试中至今没有出现过相关考点，而考纲上面是明确列出这个知识点。需要引起重视，特别是 Windows 系统安全体系结构，服务的调用过程，Windows 系统是怎么实现访问控制（即原理）这些加以学习。】