1. 安全服务和安全机制的区别和联系是什么？

联系：安全服务通过安全机制来实现安全策略.

区别：安全服务是加强数据处理系统和信息传输的安全性的一种处理过程或通信服务.其目的在于利用一种或多种安全机制进行反攻击.

安全机制是用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程.或实现该过程的设备

2. 简述IPSec的两种工作模式

传输模式：主要为直接运行在IP层之上的协议，如TCP，UDP和ICMP，提供安全保护，一般用于在两台主机之间的端到端通信

隧道模式：对整个IP包提供保护，为了达到这个目的，当IP数据包附加了AH或ASP域之后，整个数据包加安全域被当作一个新IP包的载荷，并拥有一个新的外部IP头，一般用于两个网络之间的通信

3. ESP协议和AH协议有哪些不同？

AH协议为IP数据包提供数据完整性校验和身份验证，还可选择的抗重放攻击保护，但不提供数据加密机制，认证基于消息鉴别码(MAC)，双方必须共享同一个密钥

ESP协议为IP数据包提供数据完整性校验、身份验证和数据加密，还有可选择的抗重放攻击保护ESP用一个密码算法提供机密性，数据完整性则由身份验证算法提供.

4. SSL记录协议包括哪几个主要步骤？

SSL记录协议接收上层应用消息，将数据分段为可管理的块，可选择地压缩数据，应用MAC，加密添加一个SSL记录头，并将结果传送给TCP

5. 简述SSL握手协议的处理过程

阶段1：建立安全能力，包括协议版本、会话标识、密码组、压缩方法和初始随机数

阶段2：服务器发送证书、交换密钥，证书请求，hello完成消息.

阶段3：如果接收到请求，客户端发送其证书；发送交换密钥，也可以发送证书验证消息.

阶段4：改变密码，结束握手协议