入一个假冒的 TCP 报文段，该报文段具有正确的 TCP 检验和及序号（以及正确的 IP 地址和端口号）。在接收侧 SSL 将接受该假冒分组并传递载荷给接收应用程序吗？为什么？

P22. 下列是有关图 8-28 的判断题。

a. 当在 172.16.1/24 中的主机向一台 Amazon.com 服务器发送一个数据报时，路由器 R1 将使用 IPsec 加密该数据报。

b. 当在 172.16.1/24 中的主机向在 172.16.2/24 中的主机发送一个数据报时，路由器 R1 将改变该 IP 数据报的源和目的地址。

c. 假定在 172.16.1/24 中的主机向在 172.16.2/24 中的 Web 服务器发起一个 TCP 连接。作为此次连接的一部分，由 R1 发送的所有数据报将在 IPv4 首部字段最左边具有协议号 50。

d. 考虑从在 172.16.1/24 中的主机向在 172.16.2/24 中的主机发送一个 TCP 报文段。假定对该报文段的应答丢失了，因此 TCP 重新发送该报文段。因为 IPsec 使用序号，R1 将不重新发送该 TCP 报文段。

P23. 考虑图 8-28 中的例子。假定 Trudy 是中间人，她能够在从 R1 和 R2 发出的数据报流中插入数据报。作为重放攻击一部分，Trudy 发送一个从 R1 到 R2 发送的数据报的冗余副本。R2 将解密该冗余的数据报并将其转发进分支机构网络吗？如果不是，详细描述 R2 如何检测该冗余的数据报。

P24. 考虑下列伪 WEP 协议。其密钥是 4 比特，IV 是 2 比特。当产生密钥流时，IV 被附加到密钥的后面。假定共享的密钥是 1010。密钥流的 4 个可能输入如下：

101000：00101011010101010011011010100100…

101001：10100110110010101101001001011101…

101010：00011010001111000101001010011111…

101011：11111010100000001010101000101111…

假定所有报文都是 8 比特长。假定 ICV（完整性检查）是 4 比特长，并且通过用数据的后 4 比特异或数据的前 4 比特来计算。假定该伪 WEP 分组由 3 个字段组成：首先是 IV 字段，然后是报文字段，最后是 ICV 字段，这些字段中的某些被加密。

a. 我们希望使用 IV = 11 和 WEP 发送报文 $m = 10100000$。在这 3 个 WEP 字段中将有什么样的值？

b. 说明当接收方解密该 WEP 分组时，它恢复报文和 ICV。

c. 假定 Trudy 截获了一个 WEP 分组（并不必要使用 IV = 11）并要在向接收方转发前修改该分组。假定 Trudy 翻转了第一个 ICV 比特。假定 Trudy 并不知道用于任何 IV 的密钥流，则 Trudy 也必须翻转哪些其他比特，使得接收到的分组通过 ICV 检查？

d. 通过修改（a）中 WEP 分组中的比特，解密所生成的分组，并验证完整性检查来评价你的答案。

P25. 对于尽可能限制但能实现下列功能的一台有状态防火墙，提供一张过滤器表和一张连接表：

a. 允许所有的内部用户与外部用户创建 Telnet 会话。

b. 允许外部用户冲浪公司位于 222.22.0.12 的 Web 站点。

c. 否则阻挡所有入流量和出流量。

内部网络为 222.22/16。在你的答案中，假设连接表当前缓存了 3 个从内向外的连接。你需要虚构适当的 IP 地址和端口号。

P26. 假设 Alice 要使用 TOR 类似的服务访问 Web 站点 activist.com。该服务使用两个不串通的代理服务器 Proxy1 和 Proxy2。Alice 首先从某个中央服务器获得对 Proxy1 和 Proxy2 的证书（每个都包含一个公钥）。用 $K_1^+()$、$K_2^+()$、$K_1^-()$ 和 $K_2^-()$ 表示加密/解密时所使用的 RSA 公钥和 RSA 私钥。

a. 使用一幅时序图，提供一个（尽可能简单的）协议允许 Alice 创建一个用于 Proxy1 的共享会话密钥 S_1。$S_1(m)$ 表示为使用共享密钥 S_1 对数据 m 加密/解密。

b. 使用时序图，提供一个（尽可能简单的）协议允许 Alice 创建一个对于 Proxy2 的共享会话密钥 S_2，而不向 Proxy2 透露她的 IP 地址。