# ASA站点到站点IPSec VPN

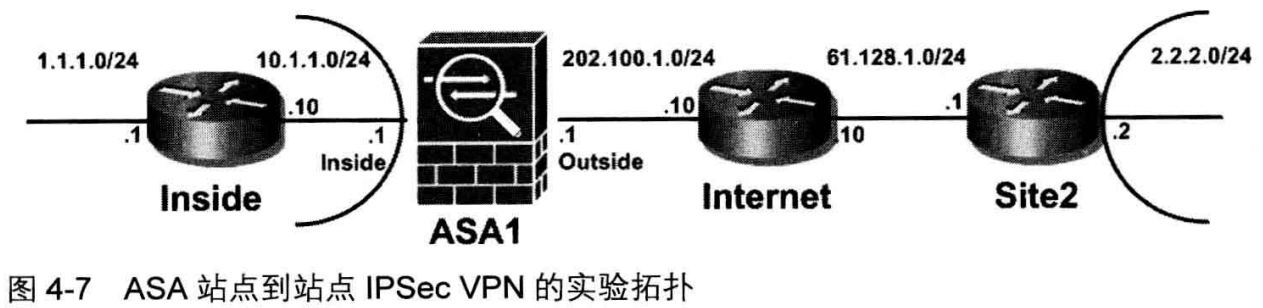
## 实际接线状况

图4-6所示为ASA 站点到站点IPSec VPN的实际接线状况。本实验一共需要使用3台路由器和1台ASA防火墙。由左至右分别模拟公司站点一内部路由器（Inside)、公司站点一(ASA1)、互联网路由器(Internet)和公司站点二(Site2)。路由器Inside和Site2分别使用Loopback0模拟公司内部网络。路由器Inside使用FaO/0接口与ASA1的EO/O接口对接，ASA1使用EO/1接口和Internet的Fa1/0接口对接，路由器Internet和Site2使用接口Fa2/0实现对接。



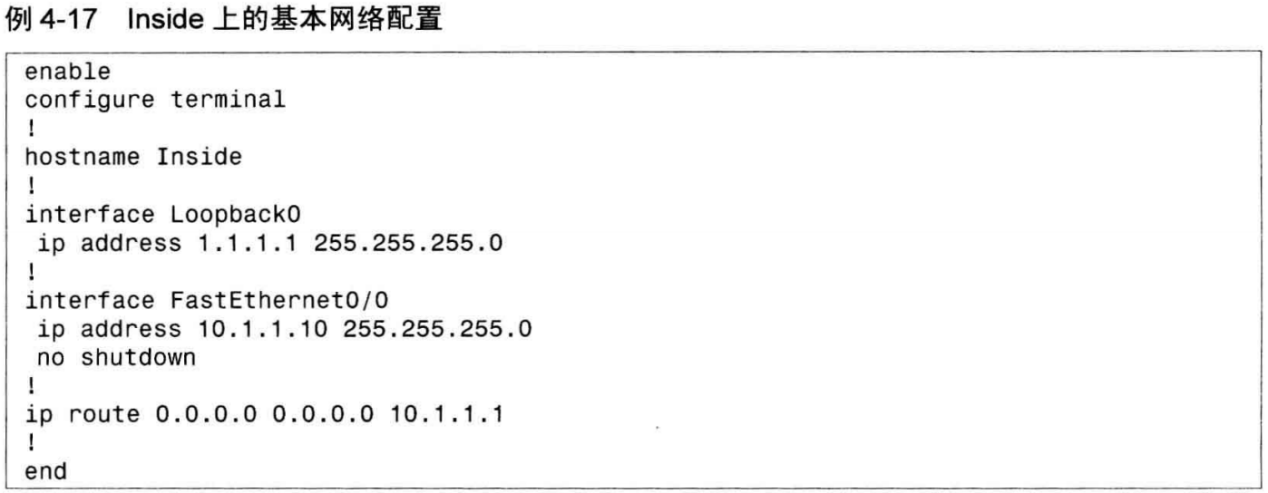
## **实验拓扑介绍**

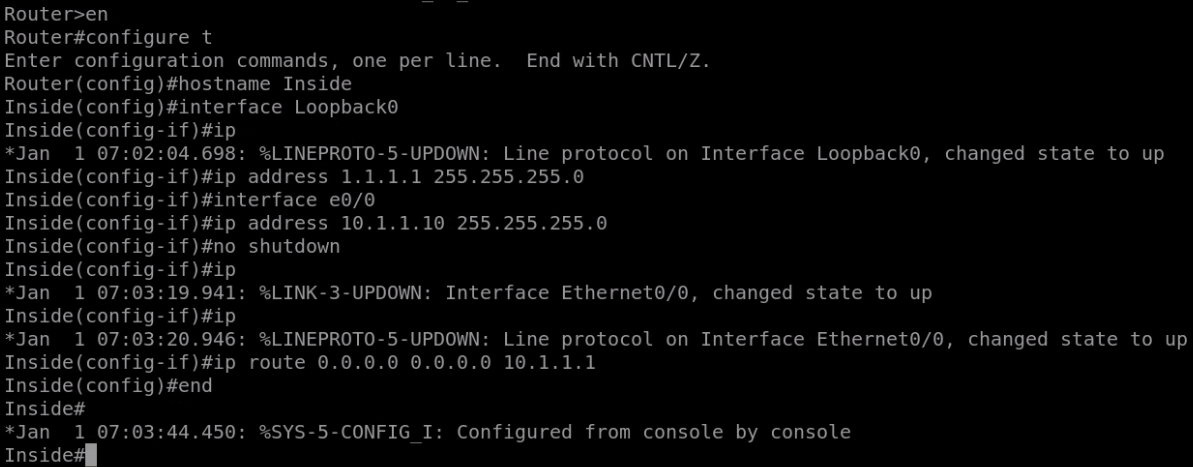
图4-7所示为ASA站点到站点IPSec VPN 的实验拓扑。该拓扑是一个经典站点到站点VPN拓扑，ASA1 (202.100.1.1）和Site2(61.128.1.1）是两个VPN站点连接互联网的网关设备，也是IPSec VPN的加密设备。本次实验的通信网络为Inside路由器身后的1.1.1.0/24网络和Site2身后的2.2.2.0/24网络。本次实验需要在ASA1和Site2之间建立隧道模式的IPSec VPN，以保护通信网络之间的流量。

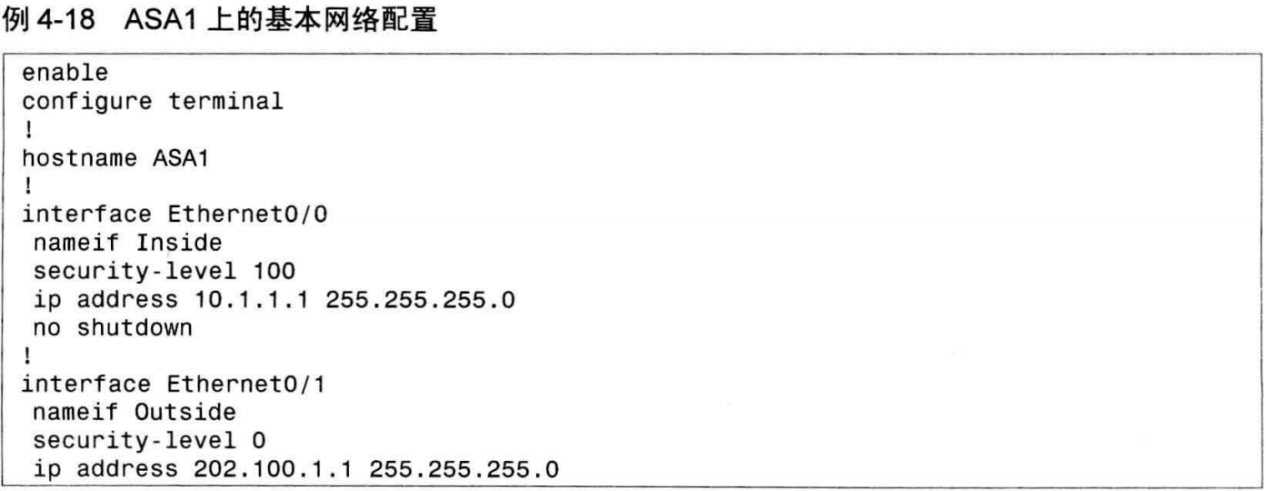


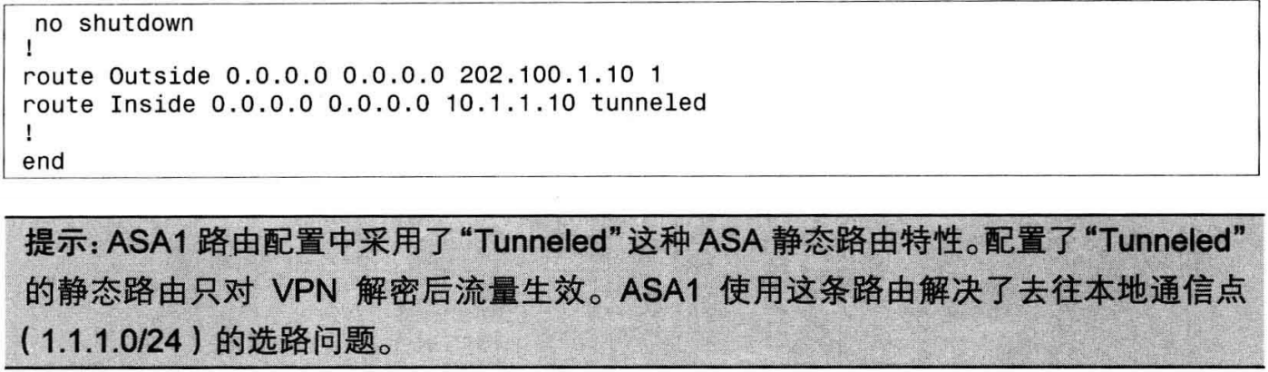
## **基本网络配置**

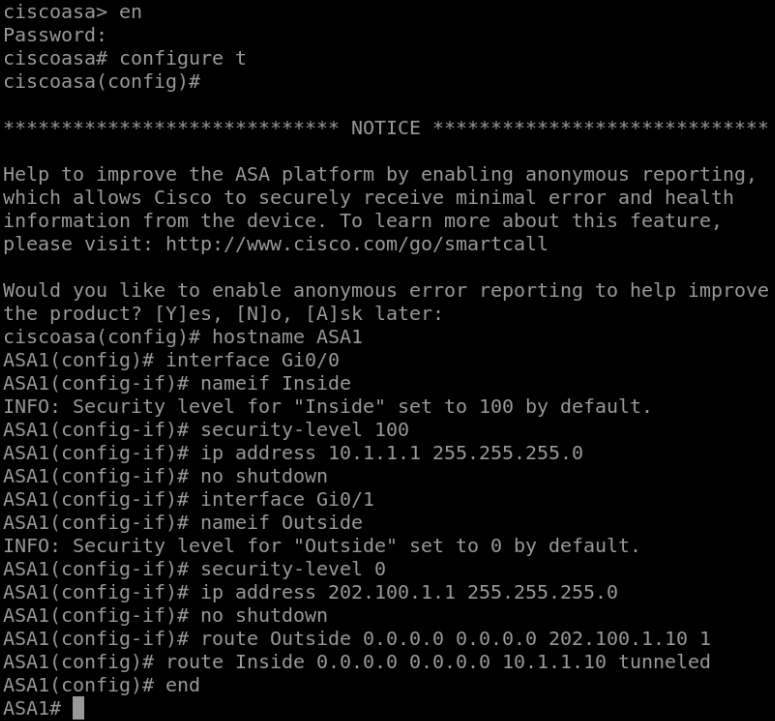
在介绍和配置IPSec VPN之前，我们需要首先配置路由器和ASA防火墙的IP地址与路由，即执行基本网络配置。例4-17、例4-18、例4-19和例4-20分别介绍了在Inside、ASA1、Internet和 Site2路由器上需要执行的基本网络配置。

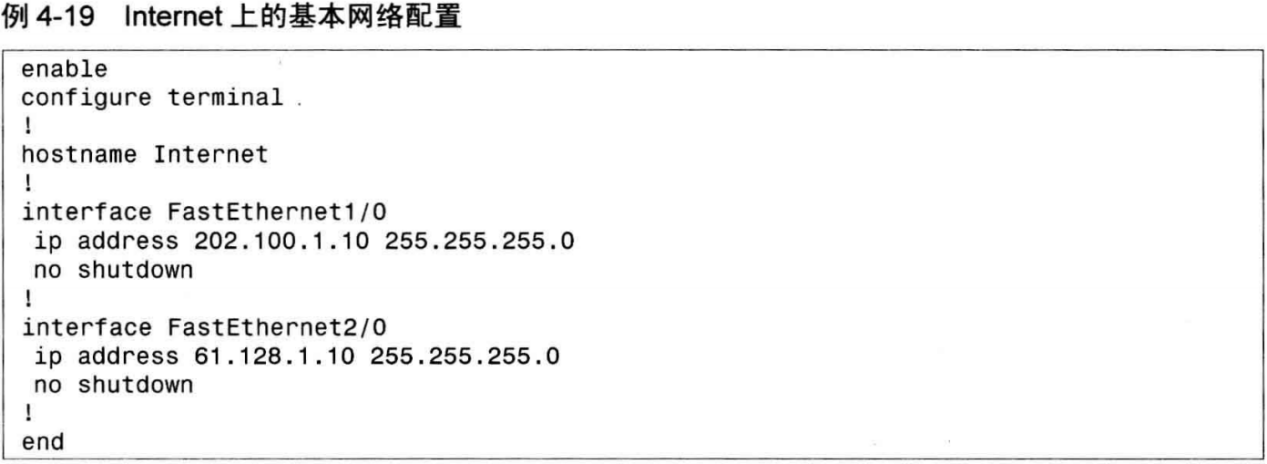


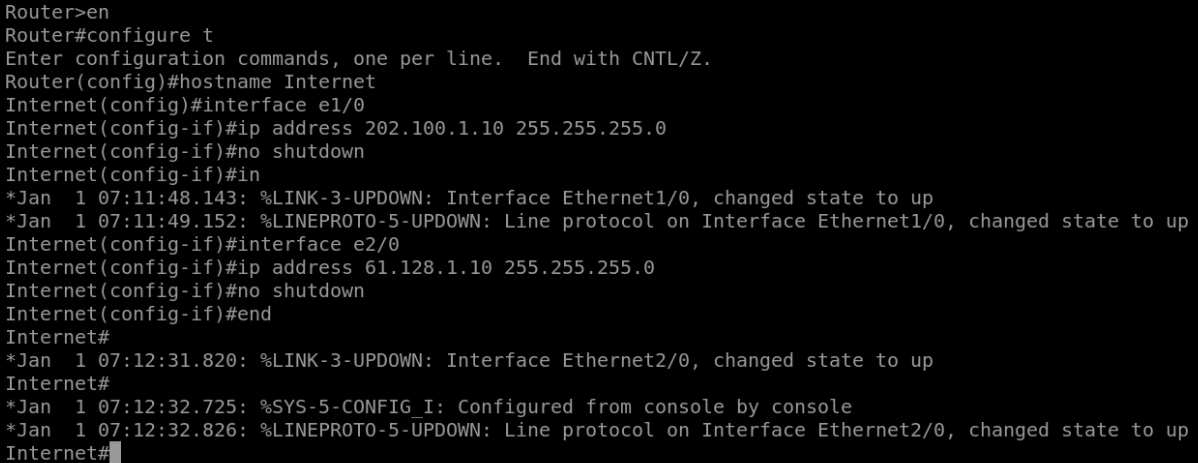


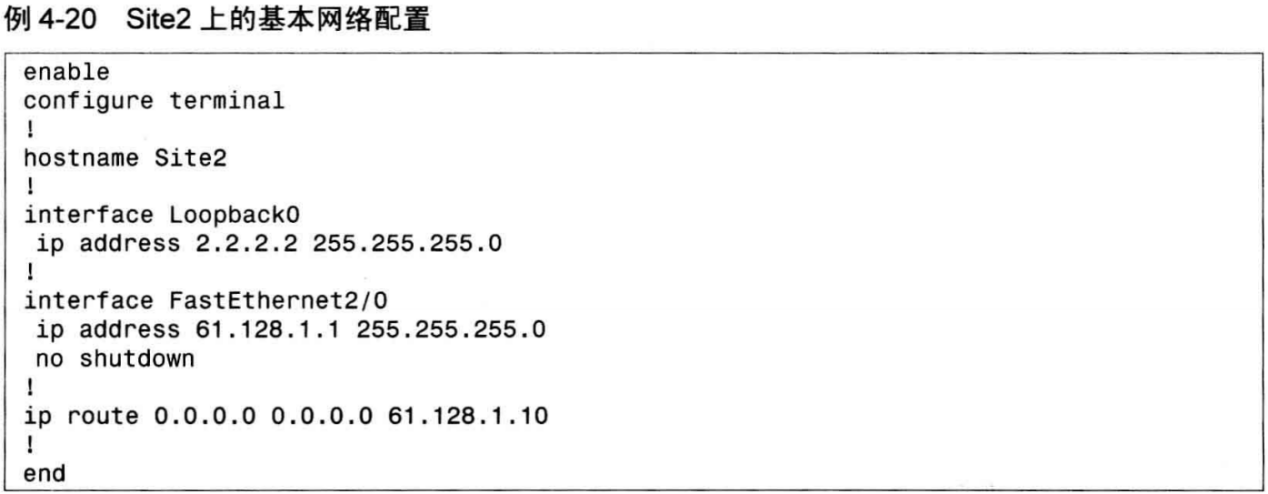


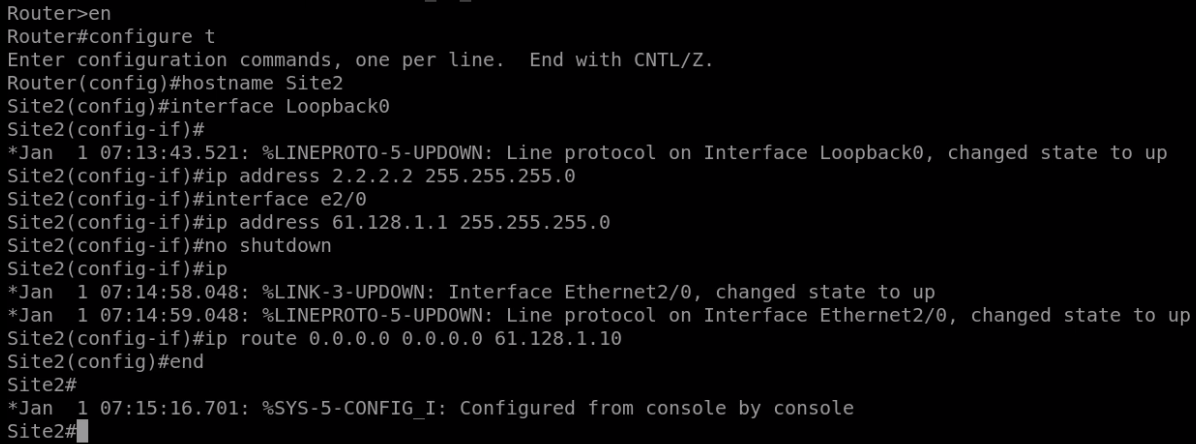






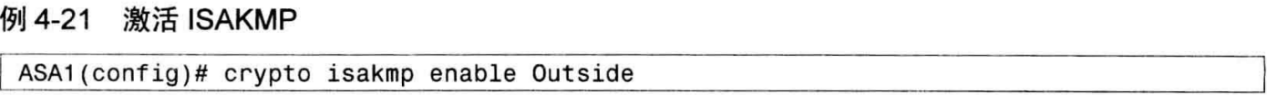




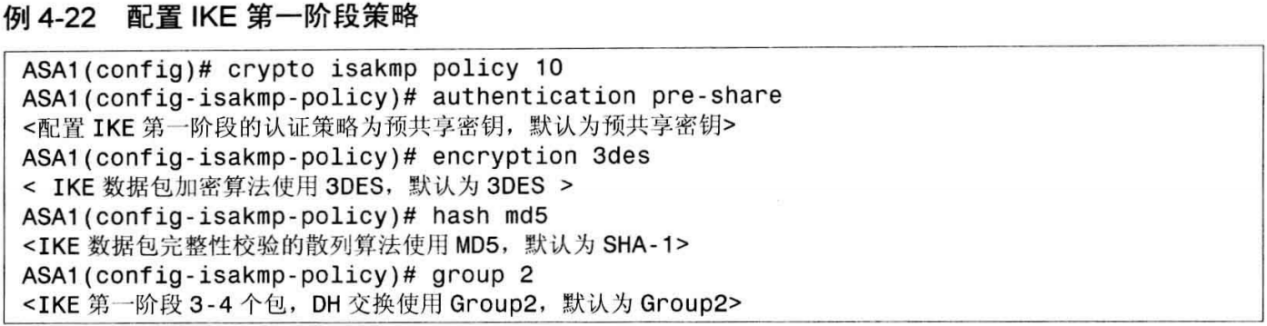


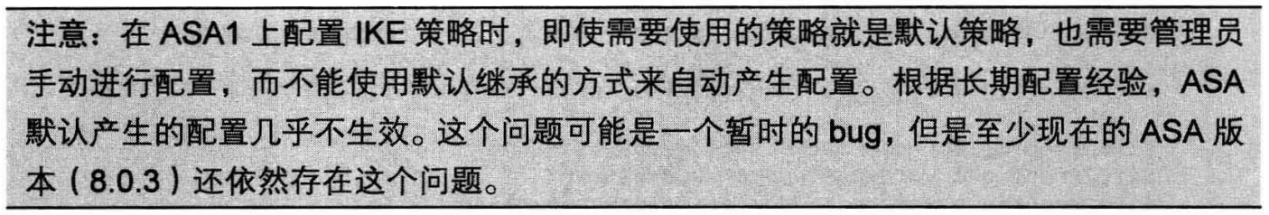
## **ASA站点到站点IPSec VPN配置**

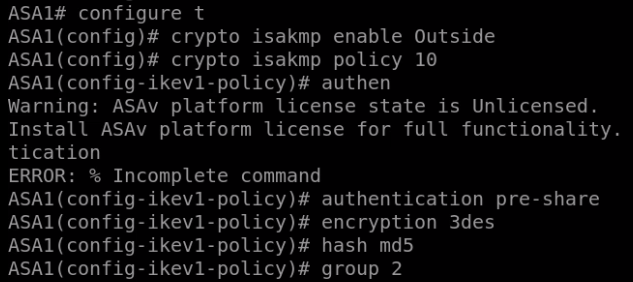
激活ISAKMP，如例4-21所示。



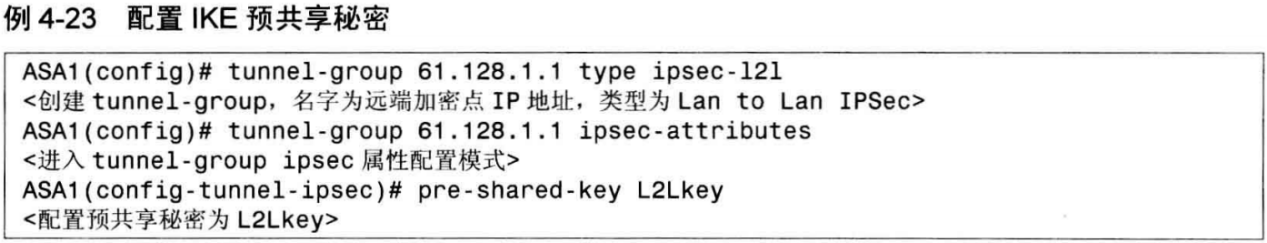
配置IKE第一阶段策略，如例4-22所示。

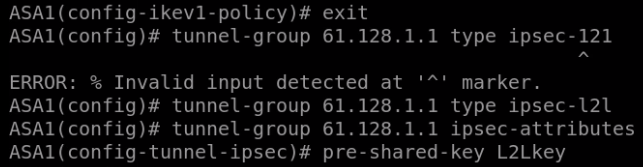




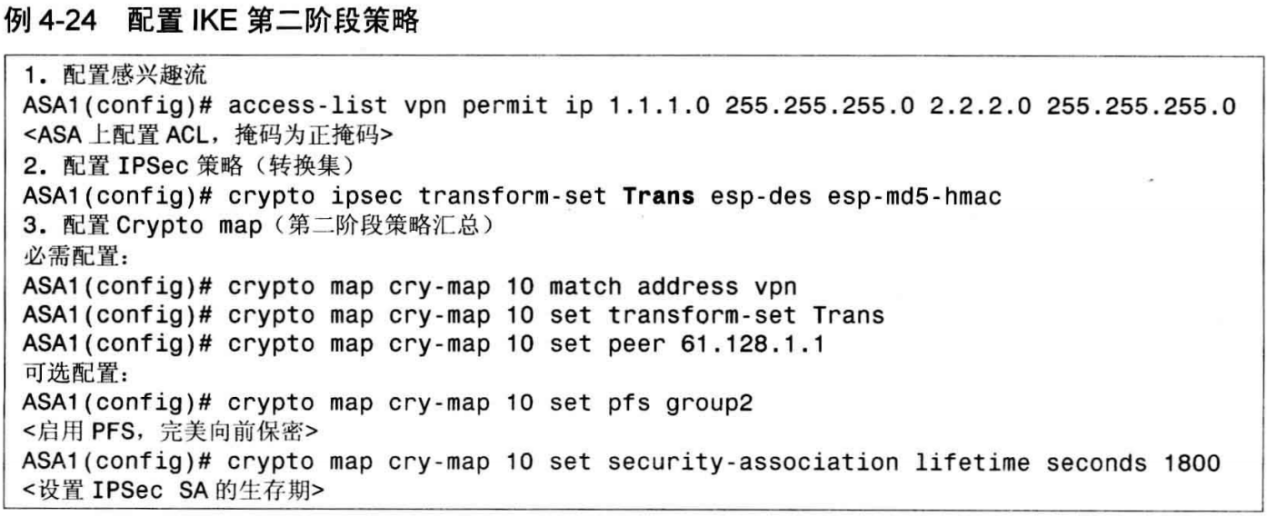


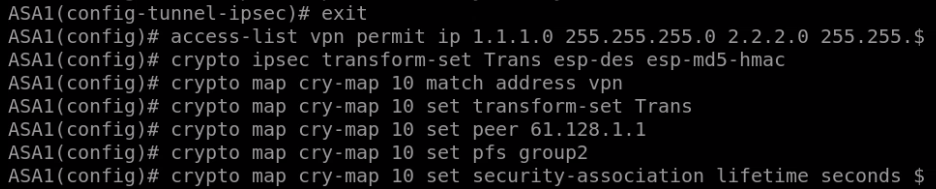
配置IKE预共享密钥，如例4-23所示。





配置IKE第二阶段策略，如例4-24所示。





将Crypto map应用到接口，如例4-25所示。





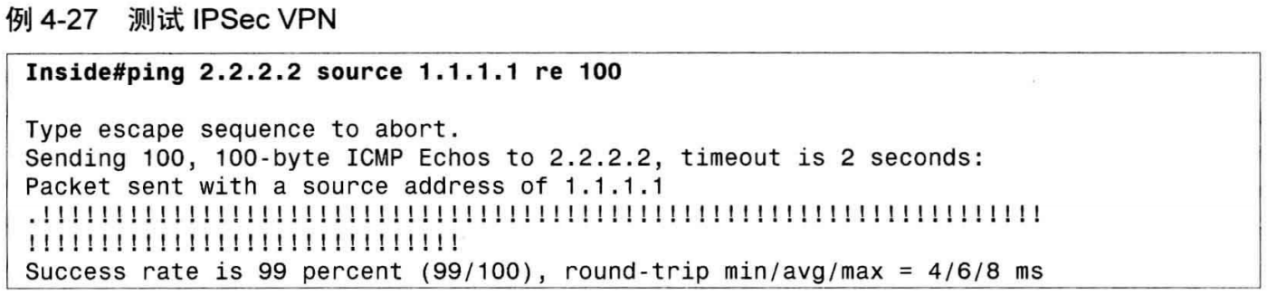
在 Site2上配置IPSec VPN，如例4-26所示。

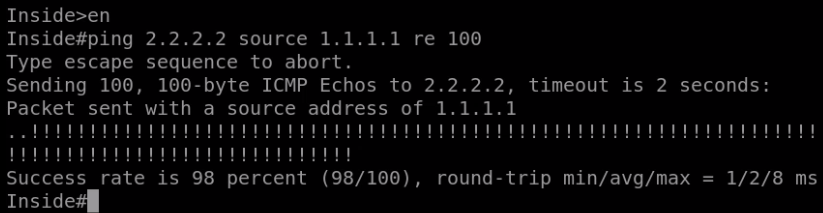




## **测试IPSec VPN**

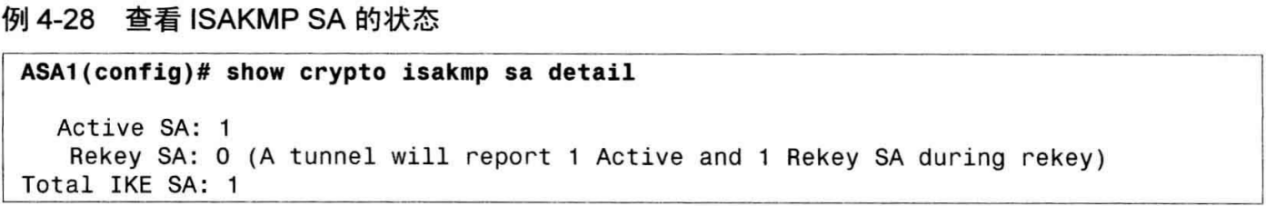
现在ASA与路由器之间的经典IPSec VPN已经配置完毕，我们可以通过在 Inside路由器上使用ping 制造感兴趣流来进行测试，如例4-27所示。需要注意的是，本次ping 的目的为2.2.2.2，源为1.1.1.1，这就是IPSec VPN加密的感兴趣流。

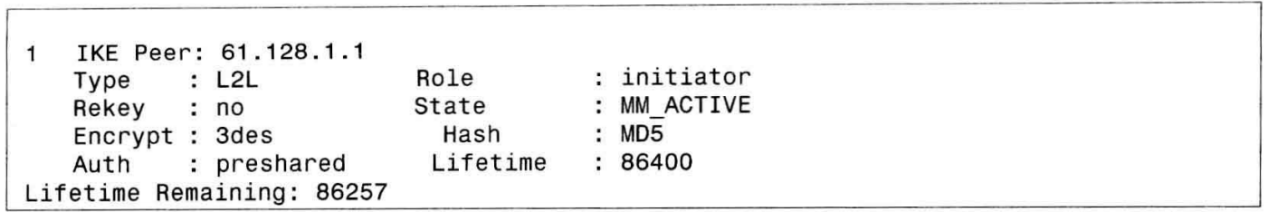




## **ASA查看IPSec VPN的相关状态**

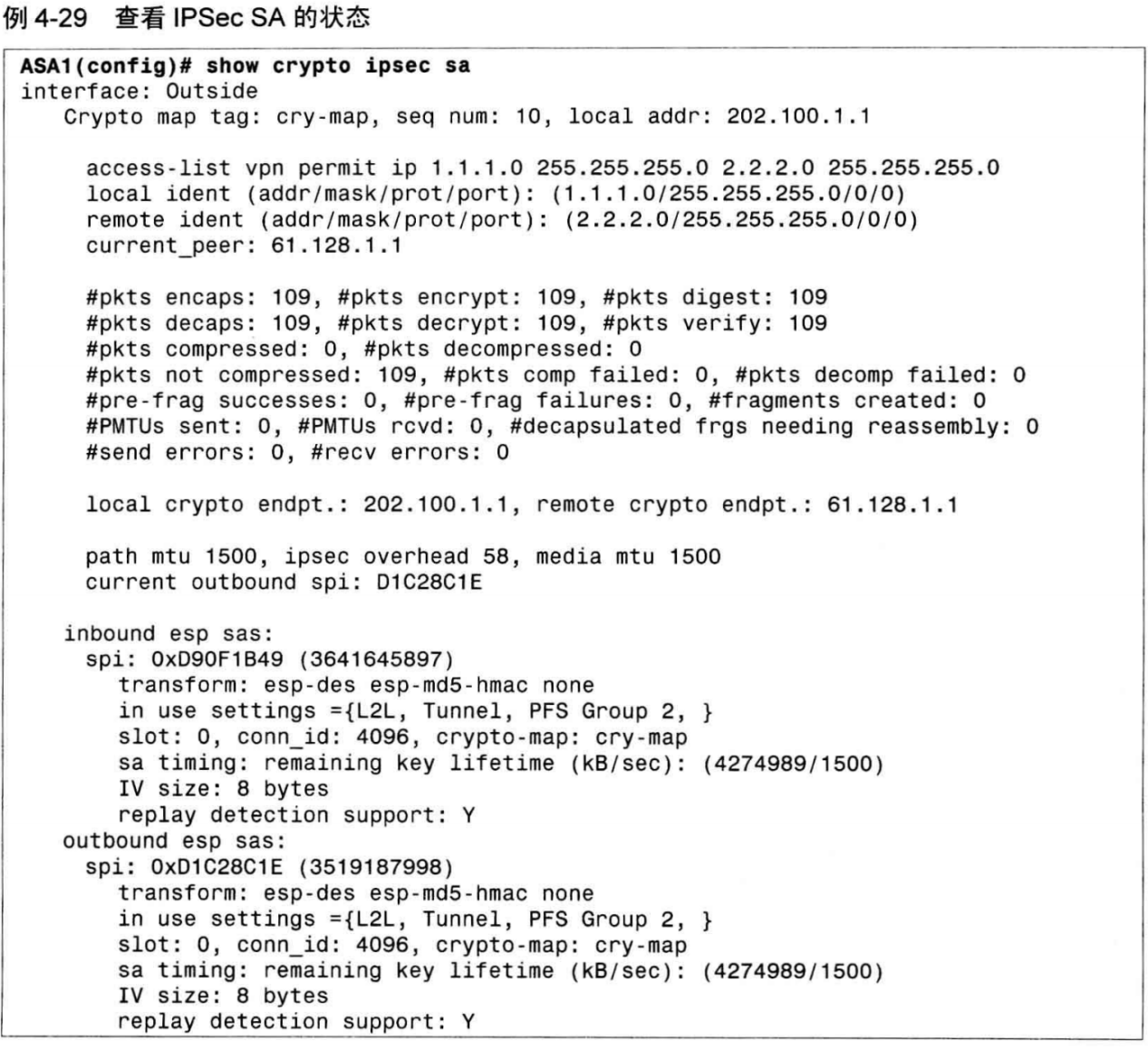
在ASA1上执行show crypto isakmp sa detail命令，查看ISAKMP SA的状态，如例4-28所示。

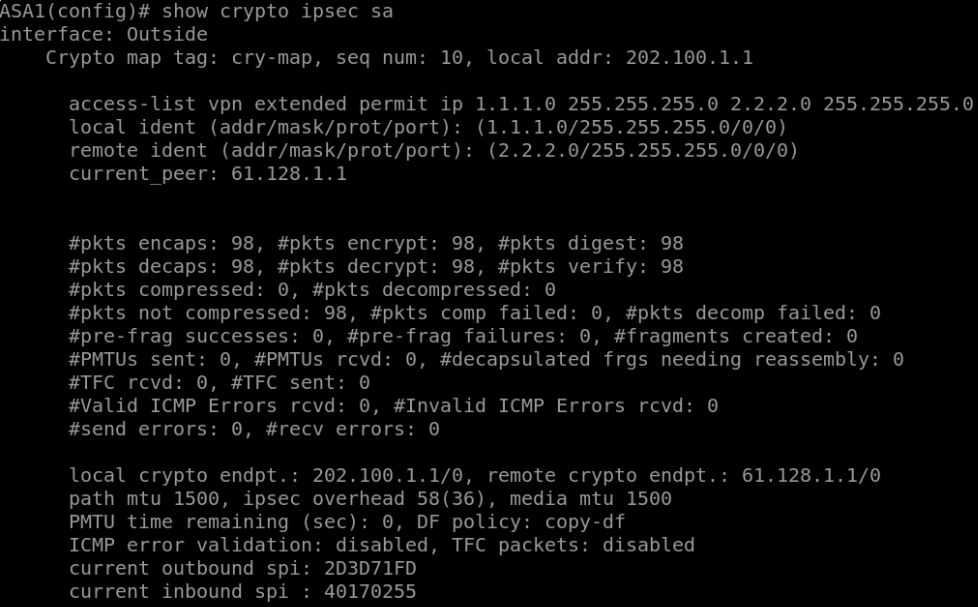


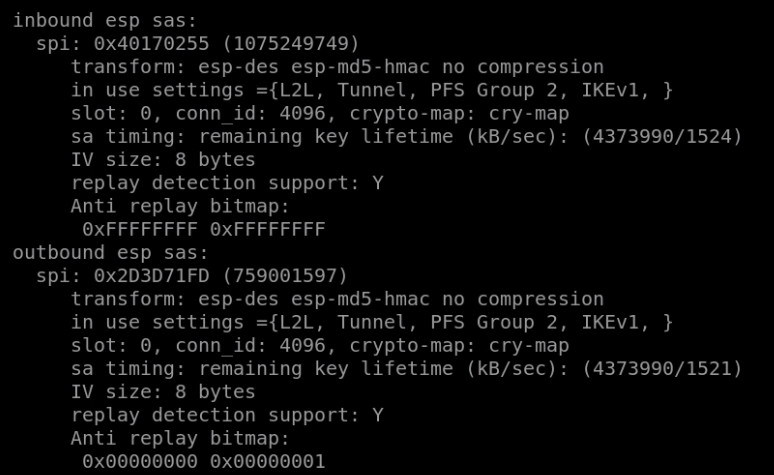




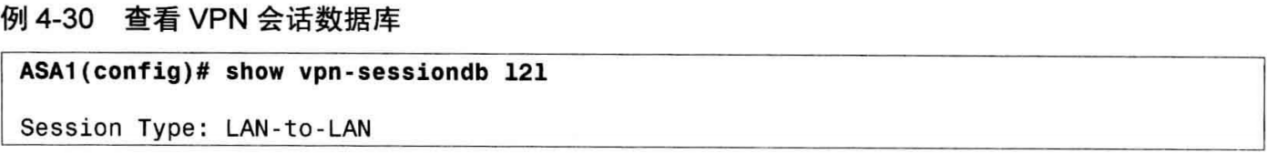
在ASA1上执行show crypto ipsec as命令,查看IPSec SA的状态如例4-29所示。

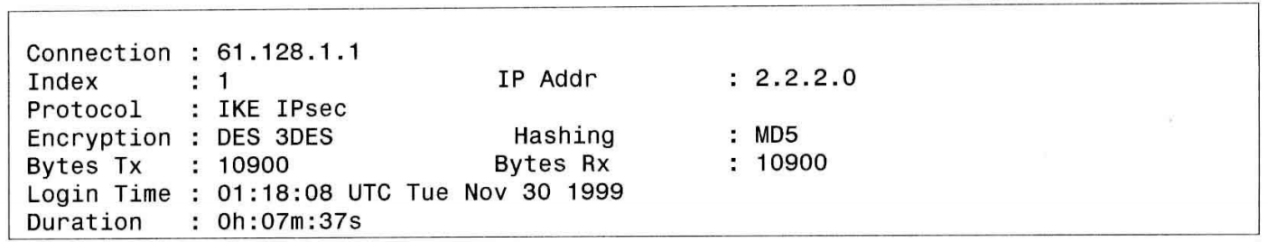


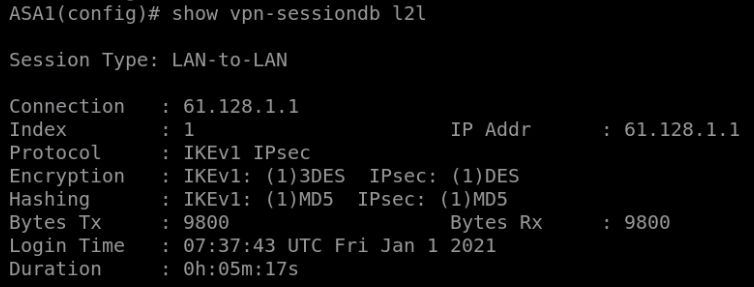




在ASA1上执行show vpn-session db l21命令，查看VPN会话数据库，如例4-30所示。







在ASA1上执行show crypto protocol statictics ipsec命令，查看IPSec协议状态，如例4-31所示。

