 工作原理：一边服务器的网络子网为192.168.1.0/24路由器为100.10.15.1另一边的服务器为192.168.10.0/24路由器为200.20.25.1.执行下列步骤：1. 确定一个预先共享的密钥(保密密码)(以下例子保密密码假设为noIP4u) 2. 为SA协商过程配置IKE. 3. 配置IPSec. 配置IKE：Shelby(config)#crypto isakmp policy 1
Shelby(config-isakmp)#group 1 注释：除非购买高端路由器，或是VPN通信比较少，否则最好使用group 1长度的密钥，group命令有两个参数值：1和2.参数值1表示密钥使用768位密钥，参数值2表示密钥使用1024位密钥，显然后一种密钥安全性高，但消耗更多的CPU时间。
Shelby(config-isakmp)#authentication pre-share 注释：告诉路由器要使用预先共享的密码。 Shelby(config-isakmp)#lifetime 3600 注释：对生成新SA的周期进行调整。这个值以秒为单位，默认值为86400，也就是一天。值得注意的是两端的路由器都要设置相同的SA周期，否则VPN在正常初始化之后，将会在较短的一个SA周期到达中断。 Shelby(config)#crypto isakmp key noIP4u address 200.20.25.1 注释：返回到全局设置模式确定要使用的预先共享密钥和指归VPN另一端路由器IP地址，即目的路由器IP地址。相应地在另一端路由器配置也和以上命令类似，只不过把IP地址改成100.10.15.1。 编辑特别推荐: Cisco交换机DHCPSnooping功能 Cisco认证知识:Switch命令大全 