利用PIX与路由器做点对点VPN[2] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E5_88_A9_E7_94_A8PIX_E4_c101_142698.htm 创建IKE策略： 定义认证方法为预共享密 isakmp policy 1 authentication pre-share 定义认证方法为预加密方式，以及算法，组，生命周期（默认是86400） isakmp policy 1 encryption 3des isakmp policy 1 hash md5 isakmp policy 1 group 1 isakmp policy 1 lifetime 1000 在接口上应用IKE策略（outside指外网口） isakmp identity address isakmp enable outside 这里记得还要补上一条：因为点对点的VPN之间的网络互相访问的时候是不做NAT出去的，所以要加上一条ACL阻止这两个网络之间访问是不能做NAT出去。 access-list nonat permit ip 10.0.X.0 255.255.240.0 192.168.X.0 255.255.255.0 nat （inside） 0 access-list nonat 路由器上的配置：原理同PIX的配置是一样的，但是在命令以及应用上有些稍的差别： 先建立访问控制列表130，为下面的VPN加密调用：access-list 130 permit ip 10.0.X.0 0.0.0.255 192.168.X.0 0.0.0.255 access-list 130 permit ip 192.168.X.0 0.0.0.255 10.0.X.0 0.0.0.255 在配置模式下：crypto isakmp policy 1 创建IKE策略hash md5 定义散列算法authentication pre-share 定义预认证方法为预共享密 crypto isakmp key ******** address 210.211.198.14 配置预共享密crypto ipsec transform-set sharks esp-3des esp-md5-hmac 配置IPSec变换集crypto map testvpn 1 ipsec-isakmp 创建加密图set peer 210.211.198.14 指定对等体set transform-set sharks 指定变换集match address 130 引用加密访问列表确定受保护的流量 在接下模式下，应用加密图：interface FastEthernet0/0 crypto map

testvpn 这里还需要注意一点是路由器内网段不做NAT出去：ip nat pool internet 120.56.147.112 120.56.147.112 netmask 255.255.255.252 ip nat inside source route-map nonat pool internet overload route-map nonat permit 10 match ip address 130 接口上应用NAT：ip nat outside 在外网口应用NAT ip nat inside 在内网口应用NAT 当然这只是一部分的测试步骤，也是最基本的site to site VPN的配置方法，这次是跟美国的一个客户做这和PIX对路由器做VPN，而我们公司本来已经在两台PIX之间已经做好了site to site VPN，所以跟上面的配置还是有些区别的。 另外一点是，老外采用的VPN方式跟我们平常做的还不一样，他们喜欢用一个公网IP来代替内部一个网段来做这种site to site VPN，这无形中又产生了些微的差别。但总体的配置步骤以及方式方法都还是一样的。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com