路由器设置V 应用[I ec篇] PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E8_c101_251110.htm L2TP VPN虽然简单易用，效率较高，使用的也是非常广泛，但由于其保密性能不是非常强，在很多场合的应用中都受到了限制！而IPSec是能够更强的保密特性的，如数据加密，认证等等！ IPSec在协商时主要分为两个阶段：第一阶段为ISAKMP/IKE阶段，主要进行验证方法、加密方法及密钥协商的确定，这可以通过手工设置（Manual），也可以通过通信双方的协商（IKE）来设置，前者都是手工静态指定，这样虽然可以减轻路由器运算压力，但是密钥指定之后不会改变，不够安全！后者虽然是路由器协商确定，且定期变更的，安全性比较高！第二阶段主要是去调用上述的验证方法、加密方法及密钥，以达到形成IPSec安全通道！ 一般情况下，我们都是采用IKE方式来确定加密和认证算法的！ 这里先介绍一下，两个路由器之间建立IPSec通道的案例！ 网络结构简要如下： LAN1（192.168.0.0/24）RT1（10.0.0.1/24）（10.0.0.2/24）RT2LAN2（172.16.0.0/24） RT1#show runBuilding configuration...Current configuration:! !version 1.3.2Cservice timestamps log dateservice timestamps debug dateno service password-encryption! hostname RT1! crypto isakmp key 123456 10.0.0.2 255.255.255.255 //ISAKMP的密钥，与对端一致! crypto isakmp policy 100 //建立ISAKMP策略hash md5 //哈希算法，保障数据完整性! crypto ipsec transform-set 100 //建立变换集合transform-type ah-md5-hmac esp-des //md5认证和des加密，可自定，但要与对端一致! //前

面是第一阶段的配置；从这里开始第二阶段的协商crypto map bdcom 100 ipsec-isakmp //建立ipsec映射set peer 10.0.0.2 //指定对端路由器（运行ipsec）ipset transform-set 100 //调用变换集合match address ACL //调用访问控制列表，指定哪些数据流量需要ipsec保护! interface Loopback0 //建立loopback端口，模拟本地局域网网段ip address 192.168.0.1 255.255.255.0no ip directed-broadcast! !interface Ethernet1/2 //路由器外网口ip address 10.0.0.1 255.255.255.0no ip directed-broadcastcrypto map bdcom //将ipsec应用到物理端口上，生效duplex half! interface Serial1/0no ip addressno ip directed-broadcast! interface Serial1/1no ip addressno ip directed-broadcast! interface Serial2/0no ip addressno ip directed-broadcast! interface Serial2/1no ip addressno ip directed-broadcast! interface Serial2/2no ip addressno ip directed-broadcast! interface Serial2/3no ip addressno ip directed-broadcast! interface Async0/0no ip addressno ip directed-broadcast! !ip route 172.16.0.0 255.255.255.0 10.0.0.2 //静态路由，下一跳ip为ipsec隧道端口地址! gateway-cfgGateway keepAlive 60shutdown! !ip access-list extended ACL //扩展型访问列表，定义哪些ip数据要被保护permit ip 192.168.0.0 255.255.255.0 172.16.0.0 255.255.255.0 //这里只能配置一条，即使有多条，也只能是第一条生效! !ivr-cfg! ! RT2#show run!version 1.3.1Sservice timestamps log dateservice timestamps debug dateno service password-encryption! hostname RT2! !crypto isakmp key 123456 10.0.0.1 255.255.255.255 //ISAKMP的密钥，与对端一致! crypto isakmp policy 100 //定义ISAKMP策略，hash md5 //哈希算法! crypto ipsec transform-set 100 //所有的配置、

注释和RT1一致，但注意两端保持一致transform-type ah-md5-hmac esp-des! crypto map bdcom 100 ipsec-isakmpset peer 10.0.0.1set transform-set 100match address ACL! !interface Loopback0ip address 172.16.0.1 255.255.255.0no ip directed-broadcast! !interface FastEthernet0/0ip address 10.0.0.2 255.255.255.0crypto map bdcomno ip directed-broadcast! interface Serial1/0no ip addressno ip directed-broadcast! interface Async0/0ip address negotiatedno ip directed-broadcast! !ip route 192.168.0.0 255.255.255.0 10.0.0.1! gateway-cfgGateway keepAlive 60shutdown! !ip access-list extended ACLpermit ip 172.16.0.0 255.255.255.0 192.168.0.0 255.255.255.0! ivr-cfg! 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