 随着现在互联网的飞速发展，企业规模也越来越大，一些分支企业、在外办公以及SOHO一族们，需要随时随地的接入到我们企业的网络中，来完成我们一些日常的工作，这时我们VPN在这里就成了一个比较重要的一个角色了。 Remote VPN设备有很多。如Cisco 路由器、Cisco PIX防火墙、Cisco ASA 防火墙、Cisco VPN3002 硬件客户端或软件客户端。这极大地简化了远程端管理和配置。说的简单点就是在Server 端配置复杂的策略和密钥管理等命令，而在我们的客户端上只要配置很简单的几条命令就能和Server 端建立VPN链路的一种技术，主要的目的当然就是简化远端设备的配置和管理。 前面我们也讲解过如何在路由器上面配置Remote VPN，那么今天我又带家来一起看看这个在ASA防火墙上面如何配置我们的Remote VPN呢。 第一步：建立一个地址池。 远程访问客户端需要在登录期间分配一个IP地址，所以我们还需要为这些客户端建立一个DHCP地址池，不过如果你有DHCP服务器，还可以使用DHCP服务器。
QUANMA-T(config)# ip local pool vpnpool 192.168.10.100-192.168.10.199 mask 255.255.255.0 第二步：建立IKE第一阶段。 QUANMA-T(config)# isakmp policy 1
QUANMA-T(config-isakmp-policy)# authentication pre-share
QUANMA-T(config-isakmp-policy)# encryption 3des
QUANMA-T(config-isakmp-policy)# hash sha
QUANMA-T(config-isakmp-policy)# group 2

QUANMA-T(config-isakmp-policy)# lifetime 43200 QUANMA-T(config-isakmp-policy)# exit 第三步：将IKE第一阶段应用在outside接口上面。 QUANMA-T(config)# isakmp enable outside 第四步：定义转换集 QUANMA-T(config)# crypto ipsec transform-set vpnset esp-3des esp-sha-hmac 这里设置的转换集名字为vpnset。 第五步：动态加密映射配置 QUANMA-T(config)# crypto dynamic-map outside-dyn-map 10 set transform-set vpnset QUANMA-T(config)# crypto dynamic-map outside-dyn-map 10 set reverse-route QUANMA-T(config)# crypto dynamic-map outside-dyn-map 10 set security-association lifetime seconds 288000 第六步：在静态加密映射中调用动态加密映射并应用在接口上面 QUANMA-T(config)# crypto map outside-map 10 ipsec-isakmp dynamic outside-dyn-map QUANMA-T(config)# crypto map outside-map interface outside 第七步：NAT穿越 它的主要作用是将三层IPSEC的ESP流量转发为四层的UDP流量。ESP是一个三层的包，只有协议号，没有端口号，当它想穿越一个PAT设备时，由于PAT设备是基于端口的转换，所以ESP包过不了，这时就要将它封装进UDP包才能正常传输（源目端口都是UDP4500） QUANMA-T(config)# crypto isakmp nat-traversal //缺省keepalives时间20秒 