陈安【技术大咖】 2006-12-14 发表

MSR系列路由器 L2TP OVER IPSEC功能配置 关键字: MSR;L2TP;IPsec;VPN;野蛮模式;安全模板 一、组网需求: 移动用户通过L2TP客户端软件接入LNS以访问总部内网,在PC和LNS之间交互的数 据通过IPsec加密后传输。 设备清单: MSR系列路由器1台 PC 1台 二、组网图: PC作为LAC接入 G0/0 Loopback0 10.1.1.2 三、配置步骤: 适用设备和版本: MSR系列、Version 5.20, Beta 1105后所有版本。 LNS 配置 # sysname H3C l2tp enable //使能L2TP # ike local-name Ins //设置本端IKE名字 domain h3c //建立域,并配置ip pool ip pool 1 11.1.1.1 11.1.1.23 # //设置IKE邻居 ike peer pc exchange-mode aggressive //采用野蛮模式 pre-shared-key 123 id-type name id-type name //采用名字方式识别 remote-name pc //设置IKE PEER的名字 ipsec proposal 1 # ipsec policy-template temp1 1 //建立IPsec虚模板 ike-peer pc proposal 1 //将IPsec Policy与虚模板绑定 ipsec policy pc 1 isakmp template temp1 # local-user usera //创建本地用户usera password simple usera service-type ppp //采用ppp方式 # I2tp-group 1 //创建L2TP组 undo tunnel authentication allow l2tp virtual-template 0 # interface GigabitEthernet0/0 port link-mode route ip address 10.1.1.1 255.255.255.0 ipsec policy pc //在接口G0/0应用IPsec Policy # interface Virtual-Template0 //创建L2TP虚模板 ppp authentication-mode pap domain h3c/采用PAP的域认证方式 remote address pool 1 //设置地址池 ip address 11.1.1.111 255.255.255.0 # interface LoopBack0 ip address 1.1.1.1 255.255.255.255 # PC的配置如下:

在PC端,采用SECPOINT拨号软件,因此首先需要按照SECPOINT软件,然后再进 行拨号连接。在此假设已经按照此软件,接下来的配置如下: 第一步、创建一个连接,输入LNS地址10.1.1.1,如下:



第二步、设置Pre-share-key为123

818419191 184191191	VEU P	/ VPN WIZARD
	第三步: 请设置IPSE	C相关属性
	验证方法 身份验证字	PRE-SHARE
H3C SecPoir	 ●使用LNS服务器I ●使用其她IPSECII IPSEC服务器IP 	P 员务器

第三步、输入VPN的名字"l2tp",单击完成

		NEW VP	I WIZARD
	第四步:	请输入VPN连接的名	称
	[12tp		
H3C Sec	Point		

第四步、双击刚创建好的连接"l2tp",设置VPN连接属性,单击高级

VFN连接基本设置 LNS服务器IP 备用LNS服务器IP 阿卡选择		1 . 1	~1
☞ 启用IPSEC安全协 验证方法 身份验证字	PRE-SHARE	•	
- IPSEC服务器IP ○ 使用LNS服务器 ○ 使用其它IPSEC IPSEC服务器I	IP 服务器IP P地址		-
☑ 连接成功后不允许 ☑ 启用ADSL拨号 (10)	访问Internet Windows90)		265625

第五步、选择IKE设置栏,设置野蛮模式,名字认证方式,并输入本端安全网关名字"pc"和对端安全网关设备名字"Ins"。注意要与LNS侧配置一致。点击确定,此时就已经配置好PC,双击连接"I2tp",输入用户名usera和密码usera,就可以连入LNS,访问内网了。

协商模式	野蛮模式	▼ 10的类型	名字	*
验证算法	SHA	▼ 加密算法	DES-CBC	-
Diffie-Hellman 组标识	Group1	-		
ISAIMP-SA生存周期 本端安全同关名字 对端安全同关设备名字		86400		秒
		pc		
		Ins		
厂 定时发送Keep 时间间隔 「	alive报文 秒	此日时时间	r	10

- 四、配置关键点:
- 1) L2TP的认证最好采用域方式认证
- 2) IPsec协商方式采用野蛮方式,采用名字识别
- 3) 在接口里应用IPsec Policy
- 4) PC侧的配置要与LNS上的配置一致