L2TP VPN IPSec VPN 史晓虎 2019-08-21 发表

## 组网及说明

# 1 配置需求或说明

## 1.1 适用产品系列

本案例适用于如MSR810、MSR93X系列的路由器。

## 1.2 配置需求及实现的效果

路由器采用固定IP地址的方式部署在公司互联网出口,运营商提供的IP地址为198.76.28.30/30,内网 地址为192.168.1.1/24。外网用户为了访问公司的内网资源,出于安全考虑采用I2tp over ipsec的方式 拨入公司内网进行访问。

2 组网图



# 配置步骤

# 3 配置步骤

#### 3.1 配置路由器基本上网

#路由器基本上网配置省略,具体设置步骤请参考"2.2.2 路由器外网使用固定IP地址上网配置方法"章节中"MSR830-WiNet系列路由器基本上网(静态IP)WEB配置(V7)"案例

#### 3.2 配置路由器

#开启L2TP功能 system-view [H3C]l2tp enable #创建地址池 [H3C]ip pool 1 192.168.10.2 192.168.10.200 #创建一个虚模板,指定地址池 [H3C]interface Virtual-Template1 [H3C-Virtual-Template1] ppp authentication-mode chap domain system [H3C-Virtual-Template1]remote address pool 1 [H3C-Virtual-Template1]ip address 192.168.10.1 24 [H3C-Virtual-Template1]quit #创建l2tp组 [H3C]l2tp-group 1 mode lns [H3C-l2tp1] allow l2tp virtual-template 1 [H3C-l2tp1]undo tunnel authentication [H3C-l2tp1]quit #创建本地用户 [H3C]local-user 123 class network [H3C-luser-network-123]password simple 123456 [H3C-luser-network-123]service-type ppp [H3C-luser-network-123]quit #创建多个ike安全提议,采用不同的加密算法和验证算法 [H3C]ike proposal 1 [H3C-ike-proposal-1]encryption-algorithm aes-cbc-128

[H3C-ike-proposal-1]authentication-algorithm md5 [H3C-ike-proposal-1]dh group2 [H3C]ike proposal 2 [H3C-ike-proposal-2]encryption-algorithm 3des-cbc [H3C-ike-proposal-2]authentication-algorithm md5 [H3C-ike-proposal-2]dh group2 [H3C]ike proposal 3 [H3C-ike-proposal-3]encryption-algorithm 3des-cbc [H3C-ike-proposal-3]dh group2 [H3C]ike proposal 4 [H3C-ike-proposal-4]encryption-algorithm aes-cbc-256 [H3C-ike-proposal-4]dh group2 [H3C]ike proposal 5 [H3C-ike-proposal-5]dh group2 [H3C]ike proposal 6 [H3C-ike-proposal-6]encryption-algorithm aes-cbc-192 [H3C-ike-proposal-6]dh group2 #配置ike keychain, 配置对端地址为0.0.0.0, 预共享密钥为123456 [H3C]ike keychain 1 [H3C-ike-keychain-1]pre-shared-key address 0.0.0.0 0 key simple 123456 #配置ike profile,引用ike keychain和ike安全提议,本端公网地址为198.76.28.30 [H3C]ike profile 1 [H3C-ike-profile-1]keychain 1 [H3C-ike-profile-1]exchange-mode aggressive [H3C-ike-profile-1]local-identity address 198.76.28.30 [H3C-ike-profile-1]match remote identity address 0.0.0.0 0.0.0.0 [H3C-ike-profile-1]proposal 1 2 3 4 5 6 #配置多个ipsec安全提议,采用不同的验证算法和加密算法 [H3C]ipsec transform-set 1 [H3C-ipsec-transform-set-1]encapsulation-mode transport [H3C-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128 [H3C-ipsec-transform-set-1]esp authentication-algorithm sha1 [H3C]ipsec transform-set 2 [H3C-ipsec-transform-set-2]encapsulation-mode transport [H3C-ipsec-transform-set-2]esp encryption-algorithm aes-cbc-256 [H3C-ipsec-transform-set-2]esp authentication-algorithm sha1 [H3C]ipsec transform-set 3 [H3C-ipsec-transform-set-3]encapsulation-mode transport [H3C-ipsec-transform-set-3]esp encryption-algorithm 3des-cbc [H3C-ipsec-transform-set-3]esp authentication-algorithm sha1 [H3C]ipsec transform-set 4 [H3C-ipsec-transform-set-4]encapsulation-mode transport [H3C-ipsec-transform-set-4]esp encryption-algorithm des-cbc [H3C-ipsec-transform-set-4]esp authentication-algorithm sha1 [H3C]ipsec transform-set 5 [H3C-ipsec-transform-set-5]encapsulation-mode transport [H3C-ipsec-transform-set-5]esp encryption-algorithm aes-cbc-192 [H3C-ipsec-transform-set-5]esp authentication-algorithm sha1 [H3C]ipsec transform-set 6 [H3C-ipsec-transform-set-6]encapsulation-mode transport #配置一个名字为1,序号为1的安全策略模板,引用ike profile和ipsec安全提议 [H3C]ipsec policy-template 1 1 [H3C-ipsec-policy-template-1-1] [H3C-ipsec-policy-template-1-1]transform-set 1 2 3 4 5 6 [H3C-ipsec-policy-template-1-1]ike-profile 1 #引用ipsec安全策略模板,创建ipsec安全策略 [H3C]ipsec policy 1 1 isakmp template 1 #在公网口调用ipsec安全策略 [H3C]interface GigabitEthernet 0/0 [H3C-GigabitEthernet0/0]ipsec apply policy 1

3.3 手机侧配置

取消	L2TP over IPSec	
类型		L2TP
描述	L2TP over IPSec	
服务器	198.76.28.30	
帐户	123	
RSA Secu	rID	$\bigcirc$
密码	•••••	
密钥	•••••	
发送所有济	<b>流量</b>	

## 3.4 Windown7电脑侧配置

1. 在命令行模式下执行regedit命令,弹出"注册表编辑器"对话框。在左侧注册表项目中逐级找到:HK EY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters,单击Parameters 参数,然后双击ProhibitIpSec,把值改为0.

ø	注册表编	編業				-		-	
3	マ件(F) 编	辑(E) 查看	₣(V) 收藏	夹(A)	帮助(H)				
	Þ - 🌗	PxHelp2	0	^	名称	类型	数据		
	Þ - 🌗	ql2300			•••)(默认)	REG_SZ	(数值未设置)		
	Þ - 🌗	ql40xx			88 AllocatedLuids	REG_BINARY	02 00 00 00 03 00 00 00		
	Þ - 🔰	QWAVE			AllowL2TPWea	REG_DWORD	0x00000000 (0)		
	Þ - 🌖	QWAVE	drv		BIOWPPTPWea	REG_DWORD	0x00000000 (0)		
	Þ - 🎍	RasAcd			ab CustomDLL	REG_MULTI_SZ			
	P	RasAgile	Vpn		KeepRasConn	REG DWORD	0x00000000 (0)		
	P	RasAuto			ab Medias	REG MULTI SZ	rastapi		
	Þ ••	Rasl2tp			B ProhibitIpSec	REG_DWORD	0x00000000 (0)		
	4 🔰	RasMan			ab ServiceDII	REG EXPAND SZ	%SystemRoot%\System32\rasmans.dll		
		Parar	meters		ServiceDIIUnlo	REG DWORD	0x00000001 (1)		
		C			-	-			
		RacDone	niy		编辑 DWORD (32 位	立)值			
		RacCeto	Je -		数值名称 (N):				
		rdbee		=	ProhibitIpSec				
		rdobus			新值数据 (V)	其約			
		RDPCDD	,		0	 ● +☆讲	NI GO		
	b - 1	RDPDD				○ 十进制	0)		
		RDPDR							
	Þ - 1	RDPENC	DD			确定	取消		
	Þ - 1	RDPNP							
	b - 1	RDPREFI	MP						
	Þ - 🚺	RDPWD		-					
4		III	,						
ìt	算机\HKE\	LOCAL N		YSTE	M\CurrentControlSet	\services\RasMan\P	arameters		-

2. 打开控制面板/系统与安全/windows防火墙高级设置/属性/IPSec设置,如图

<b>域配</b> 署文件	生 专用配罟文件 公用配罟文件 IPSec 设罟
IPsec	默认值 指定 IPsec 用于建立安全连接的设 置。
IPSec	免除 从所有 IPSec 要求免除 ICMP 可以简化网络连接问 题的解决。
	从 IPSec 免除 ICMP(E): 否(默认值) 🔻
IPSec	隧道授权 指定授权建立与此计算机的 IPSec 隧道连接的用户 和计算机。
	◎ 无 00)
	◎ 高級 (0) 目定 X (0)
	<b>确定 取消</b> 应用 (A)

#选择SHA-1, 3DES, Group2

定义 IPsec 设置 🛛	· **	估计算机上的毫级安全 Windows 防 ▲	
当具有活动连接安全规则时,IPsec 将使用这些设置建立安全连	自定义高级密钥交换设置	1-38.	
度。 使用默认违项时,将使用 GPO 中优先级较高的任意设置。	安全方法 ec 对密钥交换使用以下安全方法。首先	先尝试使用位于列表较高位置的方法。	
泰田交換(主種で)	安全方法 (C):		_
② 默认值(推荐) (0)	完整性 加密 密制	期交換算法	
● 高级 (A) 自定义 (C)	SHA-1 3DES Dif	ffie-Hellman Group 2 (Stik)	
熱播保护(快達復式) ○ 默认值(維荐) 0.) ● 高级(Y) 自定火(5)			
身份验证方法	M 添加(A) [編輯 (2) [ 新	图(余 (R.)	
受 默认值 (P)	密钥生存期	密制交换选项(T)	
○ 计算机和用户 (Kerberos V5) (K)	[1] 描定生成新密钥的时间。如果同时 [1] 描。法则第二个通道时生成新字组。	き探两个法 門 将 Diffie-Hellman 用 的安全性 00。	于增强
● 計算机 (Kerberos V5) (K)		le av to service der	***
()用) <sup></sup> (Lerotros V5)(0)		当 sindows vista Aug 兼容。	CIENT(+
BYEY WITH	分钟(#):	480 🛖	
	会话(5):	0	
7解有关 IPsec 设置的详细信息	了解影响交换设置的详细信息		
<u>+么是财认值?</u>	A 仕么是默认值?		The Lak
确定 取消	H	朝定	#UA

选择加密参数

自定义 IPsec 设置	8	自定义数据保护设置				100	1.18		23
当具有活动连接安全规则时,IPsec 将创 接。	使用这些设置建立安全连	连接安全规则使用数据保护设	责保护网络流星。			-	-		
使用默认违项时,将使用 GPO 中优先级	较高的任意设置。	<ul> <li>要求使用这些设置的所有5 数据完整性 使用下列宗整性算法防止在</li> </ul>	安全连接使用加密 (Q)。 网络上给改数据。列表中最		数据完整性 使用下列	和加密 影繁性和加速	1. 美国王 1.	网络上修改数据并信	時保
密視交換(主模式) ② 默认值(推荐)(0)		上方的优先使用。			密性。列出	長中蔵上万日 まわれなおう	3优先使用。 E.00)·		
<ul> <li>高級(A)</li> </ul>	自定义(C)	BOURDELLE OF ALL OF		1	KOCMEPCZE I	2.194/04/25/99-1	L (40).	-	
数据保护(快速模式) ○ 默认值(推荐)(L) ◎ 京(5())	自安义(5)	ESP SHA-1 60	0/100,000 0/100,000		ESP	SHA-1 SHA-1	3DES AES-CB	60/100,000 60/100,000	1
身份验证方法 ② 財車机(加用户(Kerberos V5) 00) ③ 计車机(Kerberos V5) 00) ③ 用户(Kerberos V5) 00)				•					
● 高級 60	自定义(1)	添加(A)		-	添加(0).		α)][8	(修余 (81)	
了嚴有关 IP144 设置的详细信息 什么思想认道2	<b>确</b> 定   取消	了結合关于 IFace 保护的问题 什么是默认值?	各通信的完整件,加完和硬件	hoi#eni##	的意思			- HC	取消

选择预共享密钥,数值需要与IKE 配置中的数值相同,然后确定,应用

自定义 IPsec 设置				- under all		E.aa	
当具有活动连接安全规则时,IPsec 将使用 接。 使用默认选项时,将使用 GP0 中优先级标题 密钥交换(主模式)	这些设置建立安全连 1299任意设置。	自定义率级身份验证方法 第一身份验证 指定在 IFs+c 协商 先尝试使用位于列 第一身份验证方法	去 [过程中使用的计算机身 表较高位置的方法。 (7):	份验证方法。首	第二身份验证 指完在 IPsec + 证书。首先尝证 第二身份验证方	5.商过程中使用的用户身份验 使用位于列表板高位置的方 法(S):	≥≥ 会证方法或健康 法。
<ul> <li>○ 默认值(推荐)(0)</li> <li>◎ 高級(A)</li> </ul>	自定义(0)	方法	其他信息	_	方法	其他信息	
数据保护(快速模式) ○ 默认值(推荐)(L) ④ 高级(V)	自定义(\$)	1644年1月21日	123	*			*
身份验证方法 ② 数认值 (?) ③ 计算机和用户 (Kerberos V5) (K) ③ 计算机 (Kerberos V5) (k)		添加(3)) [編	[編 (2)] ( ) 勝原( (2)		添加 (0))	(網羅 (I)) ( 開始: 00)	
<ul> <li>● 用户(Kerberos V5)(0)</li> <li>● 高級(00)</li> </ul>	自定义(0)	🔄 第一身份验证可	]选(τ)		□第二身份验证 每一身份验证方 身份验证。	正可迭 (8) 法列表中存在预共享密制时	,不能指定第二
了解有关 IFace 设置的详细信息 什么是默认信?	陸軍軍消	<u>了解身份验证设置的证</u> <u>什么要账认值?</u>	<u>羊細信息</u>			補定	取為

### 3. 打开window7自带客户端设置连接,选择新建连接

控制面板主页			
管理无线网络 更改适配器设置	<b>局括 14</b> 公用网络	访问类型: 无法连接到网络 连接: 및 本地连接	
更改電線共享设置	未识别的网络 公用网络	动向典型: 无法连接到网络 连续: ♀ VMware Network Adapter VMnet1 ♀ VMware Network Adapter VMnet8	
	→ 完設网络设置 ● 設置新約連接或网络 ● 设置新約連接或网络 ● 设置无线、宽带、拨号、临时或 VI	29 连接,或设置随由器或访问点。	
	连接到网络 连接到或重新连接到无线、有线、目	医导成 VPN 网络连接。	
另请参阅 Internet 选项	送探家庭组和共享透现 访问位于其他网络计算机上的文件	ichTich机,或更改共享设置。	
Windows 防火塘	建建煤解答 法案件体性网络问题 #55度物的。	1540 <b>年前</b>	

#### 选择连接到工作区



选择设置Internet连接



🚱 🌆 连接到工作区		
键入要连接的 Inte	ernet 地址	
网络管理员可提供此地	at.	
Internet 地址(I):	198.76.28.30	
目标名称(E):	L2TP over IPSec	

右击VPN连接点属性





使用密钥:也就是ike的共享密钥:如果选证书可以拨号成功只是触发不了ipsec,填上错误的密码拨号不成功(即使写l2tp的隧道密码也不行)。



🍨 连接 L2TP c	over IPSec
用户名(0):	123
密码(P):	•••••
蜮(M):	
<ul> <li>□ 为下面用户</li> <li>○ 只是我</li> <li>③ 任何使</li> </ul>	<b>P保存用户名和密码(S):</b> (R) 用此计算机的人(A)
	[ 取消 ] 属性 (0) 帮助 (H)

配置关键点