<u>L2TP VPN</u> <u>孙铁宁</u> 2018-09-24 发表

设备为MSR3620, 配置L2TP VPN, 使用Windows自带客户端拨入。

使用Windows自带客户端拨入时报错,无法建立VPN隧道。

1.检查客户的设备侧配置的VPN是单纯的L2TP VPN还是L2TP over IPsec,因为Windows客户端默认是L2TP over IPsec,如果是单纯的L2TP VPN,需要修改Windows注册表禁用IPsec。

按"Win+R"组合键打开运行,输入regedit; 依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\RasMan\Parameters,新建DWORD值,名称为ProhibitlpSec,值为1;**重新启动计算机**, IPsec就 被成功禁用。同样,如果想启用IPsec,将创建的DWORD值删除,重启计算机即可。



2.如果是L2TP over IPsec,则确认Windows的IKE与IPsec服务处于开启状态,否则无法正常发起IPsec协商。 需要注意使用iNode客户端拨入L2TP over IPsec之后这两个服务会被自动禁用。

按"Win+R"组合键打开运行, 输入services.msc, 找到下面两个服务。

名称	描述	状态	启动类型	登录为	
🔍 IKE and AuthIP IPsec Keying Modu	IKEEXT 服务托管 Internet 密钥交换(IKE)和身份验证 Intern		禁用	本地系统	
🕮 ImDisk Virtual Disk Driver Helper	Helper service for ImDisk Virtual Disk Driver.	已启动	自动	本地系统	
治 称	猫还	状态	启动类型	登录力	
🐫 IPsec Policy Agent	Internet 协议安全(IPSec)支持网络级别的对等身份验证、数		禁用	网络服务	
🖄 Ktos Day few Distributed Transportion	はアンナデキなと理は、周辺ないのでの「のもはまな数」周辺のケ		20.0h		

右键属性,将启动类型改为自动,然后点击应用,再点击启用,如下图。

I	KE and A	uthIP IPs	ec Keying Modules 的属性(本地计算机)	x
	常规	登录	恢复 依存关系	
	服务名 显示名 描述: 可执行	称: 称: 文件的路	IKEEXT IKE and AuthIP IPsec Keying Modules IKEEXT 服务托管 Internet 密钥交換(IKE)和 身份验证 Internet 协议(AuthIP)確控模块。 径:	*
	C:\Win 启动类	.dows\sys 型(E):	tem32\svchost.exe -k netsvcs 自动	•
	帮助我	配置服务	启动洗项。	
	服务状 启述 当从此	态: 动(S) 处启动服	已停止 停止(T) 暂停(P) 恢复(R) 务时,您可指定所适用的启动参数。	
	启动参	数(M) :		
			确定 取消 应用	1 (A)

3.Windows自带客户端默认采用证书作为身份验证方式。如果设备侧配置的是预共享密钥方式,需要右键VPN 连接属性,然后按照下图所示修改为预共享密钥作为身份验证方式。注意这个是IPsec的预共享密钥,不是L2 TP的隧道密码。

命名 UPN 连接 属性 🛛 🖉]
常规 选项 安全 网络 共享 以N 类型(T): 自动 y Ne 数据加密(0):	irtual)) irtual)))))))))))))
■ MUALT ■ MUALT 高级属性 ■ I2TP IKEv2 ● 使用预共享的密钥作身份验证 (P) 密钥 (C):	送网: 连接 icros
 ● 将证书用于身份验证 (C) ✓ 验证服务器证书的"名称"和"用法"属性 (V) → 确定 取消]

4.Windows自带客户端IKE与IPsec的安全提议配置方式。

按"Win+R"组合键打开运行, 输入wf.msc, 点击Windows防火墙属性。



选择IPsec设置选项卡,点击自定义。

域配置文件 委用配置文件 公用配置文件 IPSec 设置 IPsec 默认值 指定 IPsec 用于建立安全连接的设 自定义 ©) IPSec 免除 M IPSec 免除 ● ● ● ● ● ● ● ● ●	高级安全 Windows 防火墙 - 本地计算机 属性
IPsec 默认值 指定 IPsec 用于建立安全连接的设 自定义 ©) IPsec 免除 M IF IPsec 要求免除 ICMP 可以简化网络连接问 M IPsec 免除 ICMP (E): 否 (法认值) IPsec 陸道授权 IPsec 陸道授权 指定授权建立与此计算机的 IPsec 隧道连接的用户 ● 无 (E) ● 无 (E) ●	域配置文件 专用配置文件 公用配置文件 IPSec 设置
IPSec 免除 ● 从所有 IPSec 要求免除 ICMP 可以简化网络连接问 ● ● ● M IPSec 免除 ICMP (E): IPSec 陸道授权 ● ● 指定授权建立与此计算机的 IPSec 隧道连接的用户 ● 无 (E)	IPsec 默认值 指定 IPsec 用于建立安全连接的设
IFSec 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。 ③ 无 20)	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) •
◎ 无 ⑭	IFSec 隧道授权 指定授权建立与此计算机的 IFSec 隧道连接的用户
◎ 高級 @	 ● 无 ⑭ ● 高級 ⑭ 自定义 ⋃

按照下图将密钥交换(IKE)与数据保护(IPsec)设置为高级。需要注意的是虽然密钥交换后面括号里写着的是主模式,但是实际上**主模式和野蛮模式都可以。**

自定义 IPsec 设置	×
当具有活动连接安全规则时,IPsec 将创 接。	則这些设置建立安全连
使用默认选项时,将使用 GPO 中优先级	较高的任意设置。
密钥交換(王稘式)	
◎ 默认值(推荐) @)	
 高级(A) 	
数据保护(快速模式)	
◎ 默认值(推荐)(L)	
◎ 高级 (⊻)	自定义 (S)
身份验证方法	
◎ 默认值 健)	
○ 计算机和用户(Kerberos V5)(K)	
◎ 计算机(Kerberos V5)(R)	
○ 用户(Kerberos V5)(U)	
◎ 高级 00	自定义 (D
│ │ <u>了解有关 IPsec 设置的详细信息</u>	
<u>什么是默认值?</u>	
	确定 取消

点击密钥交换里面的自定义,然后点击添加设置IKE安全提议。

	Larta		
元登性 SHA-1 SHA-1	AES-CBC 128 3DES	密钥父换具法 Diffie-Hellman Gro Diffie-Hellman Gro	oup 2 (默认) oup 2
密钥生存期 指定生成新密 页,达到第一	钥的时间。如果 个阈值时生成新?	司时选择两个选 密钥。	密钥交换选项 (I) 同 将 Diffie-Hellman 用于增强 的安全性 (U)。
		100	与 Windows Vista 和更高版本 兼容。
7 S & F & An S		4811 🕋	

点击数据保护里面的自定义,然后点击**右边**的添加设置IPsec安全提议(由于我们设备侧一般配置的是ESP加密,因此设置的是数据完整性和加密)。

自	定义数据保	护设置	diamon and	-		-	-		X	
j	连接安全规则使用数据保护设置保护网络流量。									
	要求使用 数据完整性 使用下列 上方的优	用这些设置的) 生 完整性算法防 先使用。	所有安全连接使用加密 @)。 j止在网络上修改数据。列表中	最	数据完整性 使用下列 密性。列	和加密 完整性和加密 表中最上方的	©算法防止在⊠ 的优先使用。	网络上修改数据并保持	寺保	
	数据完整	[性算法 (I):			数据完整	性和加密算法	生 (M):			
	协议	完整性	密钥生存期(分钟/KB)		协议	完整性	加密	密钥生存期(
	ESP AH	SHA-1 SHA-1	60/100, 000 60/100, 000		ESP ESP	SHA-1 SHA-1	AES-CB 3DES	60/100,000 60/100,000		
									4	
	添加 (Q) 編輯 (E) 删除 (E) 添加 (Q) 編輯 (C) 删除 (E) 了留有关受 IPsec (保护的网络通信的完整性、加密和硬件加速的详细信息 化少星戰让億? (A) (A) (A) (A)									
	确定 取消									

5.Windows自带客户端**只支持传输模式**,因此如果IPsec安全提议配置的是隧道模式,在设备侧debug ike all可以看到Windows发过来的封装模式是传输模式,因此提议不被接受,IPsec SA协商失败。

*Sep 16 14:54:30:194 2018 LNS IKE/7/PACKET: vrf = 0, src = 192.168.56.10, dst = 192.168.56.1/500

Encapsulation mode is Transport.

*Sep 16 14:54:30:194 2018 LNS IKE/7/PACKET: vrf = 0, src = 192.168.56.10, dst = 192.168.56.1/500

The proposal is unacceptable.

*Sep 16 14:54:30:194 2018 LNS IKE/7/ERROR: vrf = 0, src = 192.168.56.10, dst = 192.168.56.1/500

Failed to negotiate IPsec SA.

6.Windows自带客户端**不支持L2TP隧道验证**,如果设备侧没有关闭隧道验证,在设备侧debug l2tp all信息可以看到隧道密码错误的报错。

*Sep 16 15:12:30:805 2018 LNS L2TPV2/7/ERROR:

Parsed Challenge-Response AVP:tunnel password is wrong.

*Sep 16 15:12:30:805 2018 LNS L2TPV2/7/EVENT:

TunnelID=51450: Processed invalid SCCCN packet in Wait-connect state, sent StopCCN packet to the pee r and deleted the local tunnel. 7.Windows自带客户端默认将自己的计算机名作为L2TP隧道名称,如果设备侧用remote指定了隧道名称旦跟 计算机名称不一样,在设备侧debug l2tp all信息可以看到接收到无效的SCCCN报文。

*Sep 24 14:40:10:822 2018 LNS L2TPV2/7/EVENT:

TunnelID=22554: Processed invalid SCCCN packet in Wait-connect state, sent StopCCN packet to the pee r and deleted the local tunnel.

1.Windows自带客户端默认是L2TP over IPsec, 想要只拨L2TP VPN需要修改Windows注册表禁用IPsec。

2.如果是L2TP over IPsec,确保IKE and AuthIP IPsec Keying Modules与IPsec Policy Agent这两个服务是处于开启状态。

3.Windows自带客户端默认采用证书作为身份验证方式,若设备侧配置的是预共享密钥方式,需要修改VPN连接的属性。

4.Windows自带客户端IKE与IPsec的安全提议至少一条要与设备侧的其中一条配置一致。

5.Windows自带客户端只支持传输模式,设备侧需要在ipsec transform-set里面配置encapsulation-mode tran sport。

6.Windows自带客户端不支持L2TP隧道验证,设备侧需要在I2tp-group里面配置undo tunnel authentication。

7.Windows自带客户端默认将自己的计算机名作为L2TP隧道名称,除非能够确认每台终端的计算机名称并且确保每一个都有对应的l2tp-group,否则不要在l2tp-group 1中用remote指定隧道名称。