某局点MSR3620无法使用Windows自带客户端拨入L2TP VPN处理经验案例

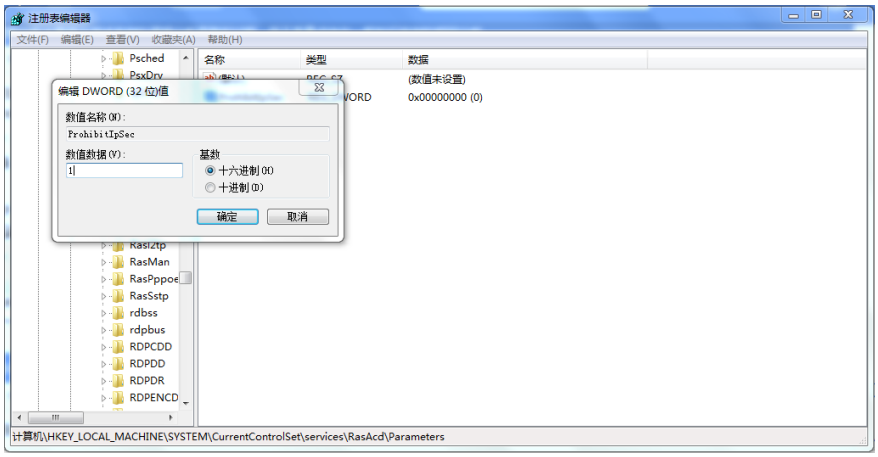
L2TP VPN 孙轶宁 2018-09-24 发表

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。

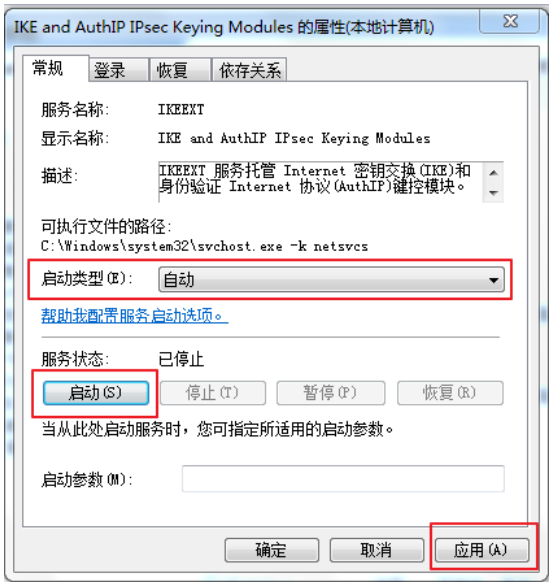
按“Win+R”组合键打开运行，输入regedit；依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters，新建DWORD值，名称为ProhibitIpSec，值为1；**重新启动计算机**，IPsec就被成功禁用。同样，如果想启用IPsec，将创建的DWORD值删除，重启计算机即可。



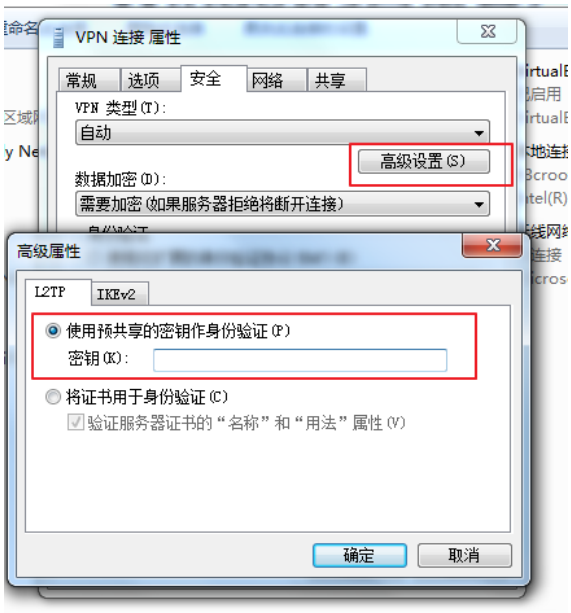
2.如果是L2TP over IPsec，则确认Windows的IKE与IPsec服务处于开启状态，否则无法正常发起IPsec协商。**需要注意使用iNode客户端拨入L2TP over IPsec之后这两个服务会被自动禁用。**

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

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。

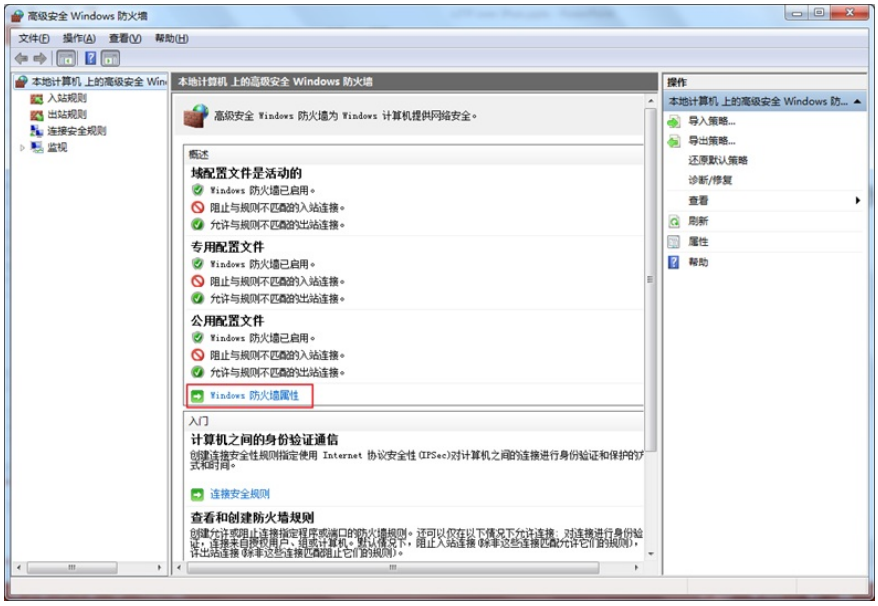


3.Windows自带客户端默认采用证书作为身份验证方式。如果设备侧配置的是预共享密钥方式，需要右键VPN连接属性，然后按照下图所示修改为预共享密钥作为身份验证方式。**注意这个是IPsec的预共享密钥，不是L2TP的隧道密码。**

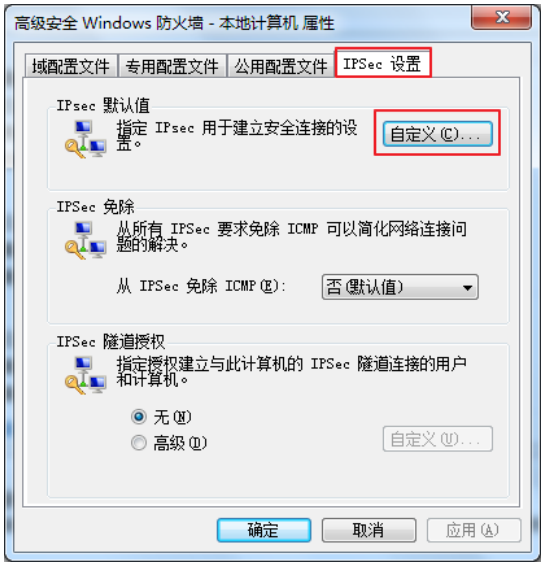


4.Windows自带客户端IKE与IPsec的安全提议配置方式。

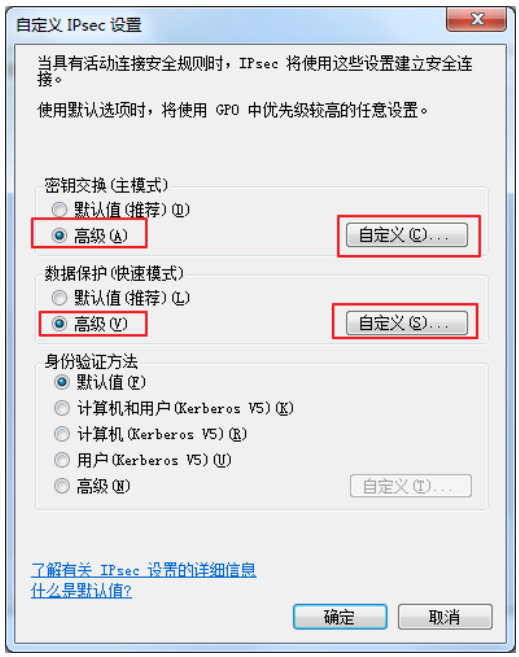
按“Win+R”组合键打开运行，输入wf.msc，点击Windows防火墙属性。



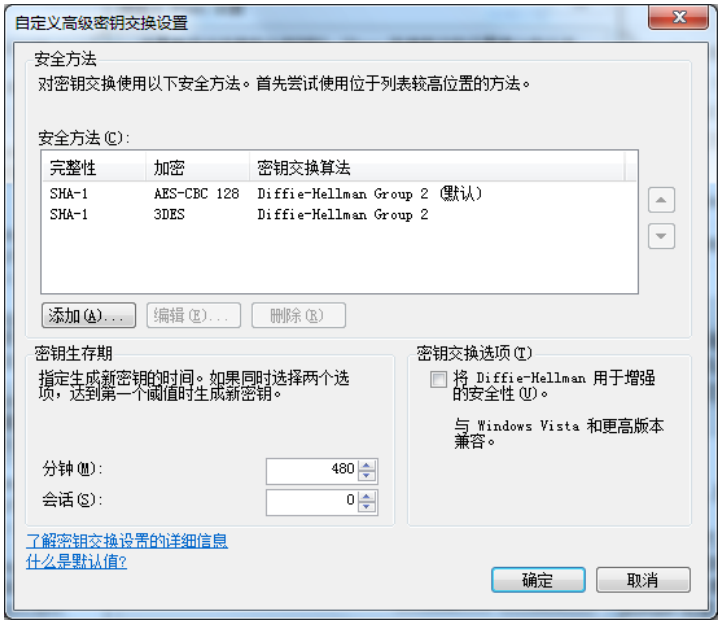
选择IPsec设置选项卡，点击自定义。



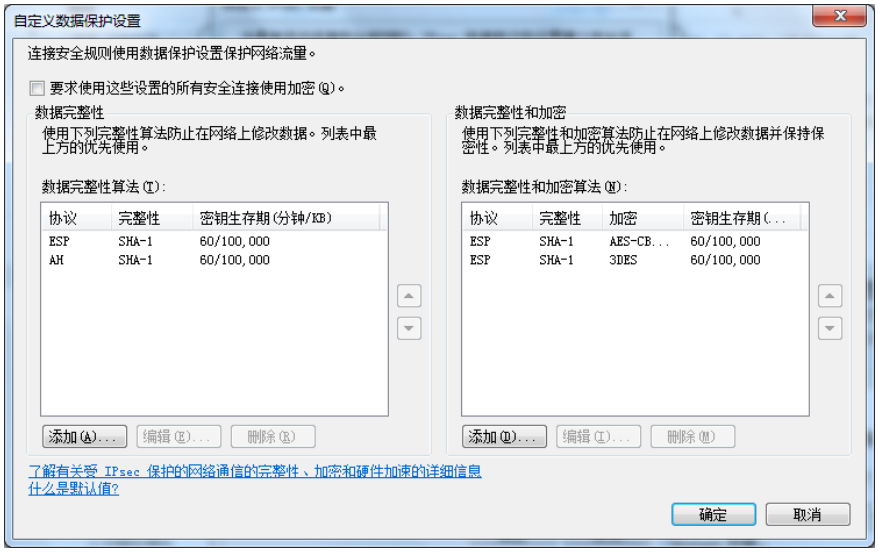
按照下图将密钥交换（IKE）与数据保护（IPsec）设置为高级。需要注意的是虽然密钥交换后面括号里写着的是主模式，但是实际上**主模式和野蛮模式都可以。**



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。



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）。



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 peer 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指定了隧道名称且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 peer 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 transport。

6.Windows自带客户端不支持L2TP隧道验证，设备侧需要在l2tp-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。