# 虚拟专用网

**【实验目的】**

(1)掌握在Windows Server2000上配置虚拟专用网（VPN）功能的技能；

(2)了解VPN的基本概念并理解其工作原理；

(3)通过实验掌握虚拟专用网的实现原理、协议和配置，理解并掌握在Windows操作系统中利用IPSec（IP协议安全协议）配置VPN的方法，以及硬件VPN的配置方法。

**【实验仪器】**

 安装Windows2003Server操作系统的一台计算机作为服务器，及若干与其联网的Windows2003Server或windowsXP计算机。

**【实验原理】**

(1)VPN介绍

   对于某些安全性数据传输有需求的用户来说，利用网络专线技术可实现此目的。它保证了数据的传输在一个封闭的网络中进行，连接网络的用户都是内部用户，这种专线网络不受公共网络的影响，实现了数据的安全传输。但是，它的缺点也非常明显，专线连接的成本非常高，针对跨国家用户以及工作地点经常变动的用户，则不适用。

   针对上述情况，虚拟专用网VPN（Virtual Private Network）应运而生，它克服了专线网络的缺点，实现了绝大多数用户安全传输数据的需求，包括全球用户，以及位置经常变动的用户，并且资本低廉、结构灵活、部署简单。

    VPN，就是两个具有 VPN发起连接能力的设备（计算机或防火墙）通过 Internet 形成的一条安全的隧道。在隧道的发起端（即服务端），用户的私有数据通过封装和加密之后在 Internet 上传输，到了隧道的接收端（即客户端），接收到的数据经过拆封和解密之后安全地到达用户端。此种方式能在非安全的互联网上安全地传送私有数据来实现基于internet 的联网操作。VPN技术的效果类似于传统的DDN专线联网方式。VPN网络连接类型按照网络连接类型区分，VPN可分为Client-LAN和LAN-LAN两种类型。

①Client-LAN类型的VPN

    Client-LAN类型的VPN也称Access VPN，即远程访问VPN。它提供了一种安全的远程访问手段。远程访问的客户端首先通过拨号网络连接到当地的ISP，利用ISP提供的服务通过互联网连接到企业的远程访问服务器，在采用VPN隧道协议的情况下，企业的远程访问服务器会和远程访问客户端建立一个安全的VPN连接。针对出差在外的员工、有远程办公需要的分支机构，都可以采用这种类型的VPN，实现安全的企业内部网络资源进行远程访问。

②LAN-LAN类型的VPN

    LAN-LAN类型的VPN也称为网关到网关类型的VPN，它可以在不同区域网络之间建立安全的数据传输通道。对于物理距离较远的企业与分公司、分支机构和合作企业间的网络连接，利用基本的Internet和Internet网络建立起全球范围内物理的连接，再利用LAN-LAN类型的VPN协议实现安全保密需要，就可以满足安全的网络连接。这种类型的VPN通常采用IPSec协议建立加密传输数据隧道。

一个完整的IPSec隧道建立过程如下:

  第一步，IPSec的一端收到另一端的IPSec数据流后，将产生IKE会话。

  第二步，IPSec两端使用IKE的主模式或者主动模式进行协商，交换IKE SA，建立安全隧道。

  第三步，IPSec两端使用IKE的快速模式协商，交换IPSec SA，建立IPSec安全通道。

  第四步，上述协商完成并建立IPSec安全通道后，传输的数据ESP或者AH协议进行封装后就可以在加密的通道上传输了。

   由上面的介绍可知，IPSec提供了数据加密、身份认证和完整性检验这3个安全措施，保证通过IPSec建立的VPN的安全性。

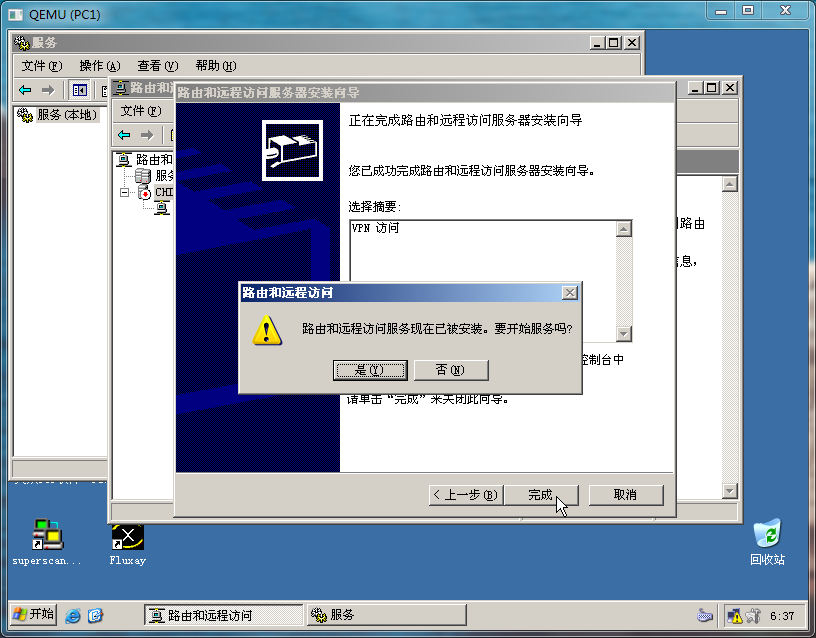
**【实验内容及步骤】**

利用Windows自带的VPN功能完成VPN服务器和客户端的配置，模拟一个远程客户拨入的虚拟专用网连接。配置Windows环境下的IPSec安全策略，并分析在应用Ipsec安全策略之后的通信情形。

**实验步骤一：启用Windows2003 VPN服务器**

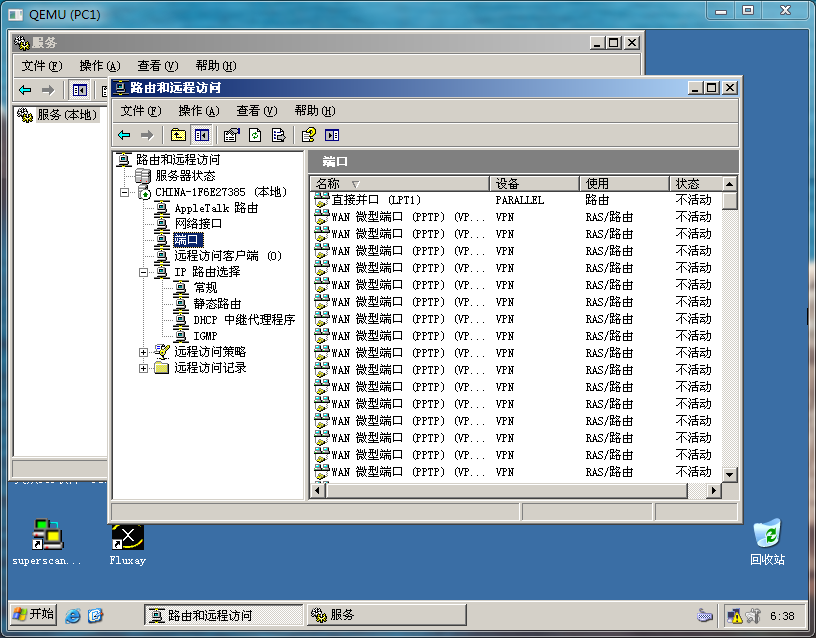
1. 配置并启用VPN服务

   在Windows2003Server 中选择“开始”，进入“管理工具”，单击“路由和远程访问”。弹出对话框，右击对话框右侧的服务器名称，在弹出的对话框中进入“配置并启用路由和远程访问”,出现路由和远程服务向导，单击“下一步”按钮,在向导中，选中“自定义配置”，如下图所示，单击“下一步”。选中“VPN访问”，单击“下一步”。点击“完成”，弹出路由和远程访问服务询问是否开启。点击“是”，开启路由和远程访问服务。



  (2)配置VPN端口

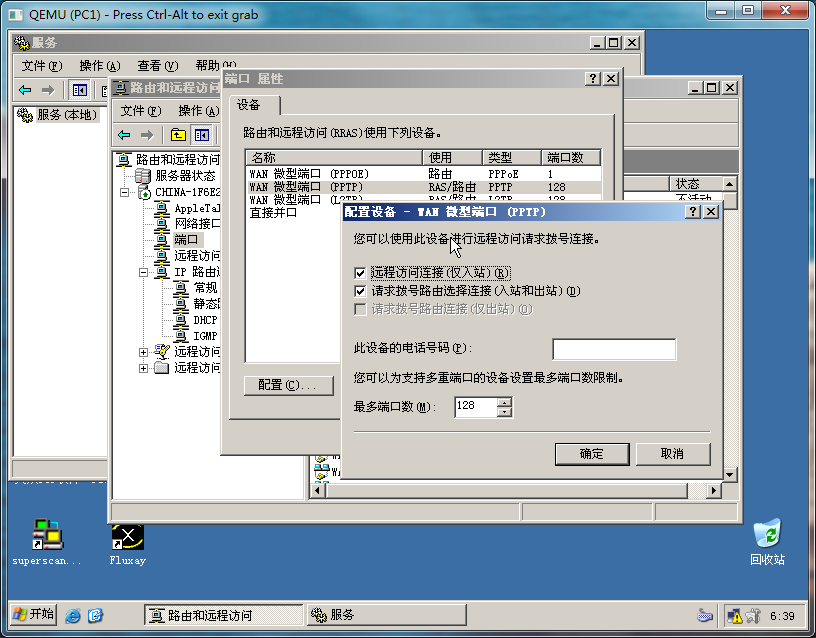
仍然在“管理工具”下，打开“路由和远程访问”，选择“端口”，会显示出配置过得端口，此时，由于未建立PPTP的VPN连接，所以端口状态都是“不活动”状态，



右击“端口”，选择属性，可以配置端口使用的VPN协议，默认设置中首先使用PPTP协议，然后再考虑L2TP协议。选择一个设备，例如PPTP，

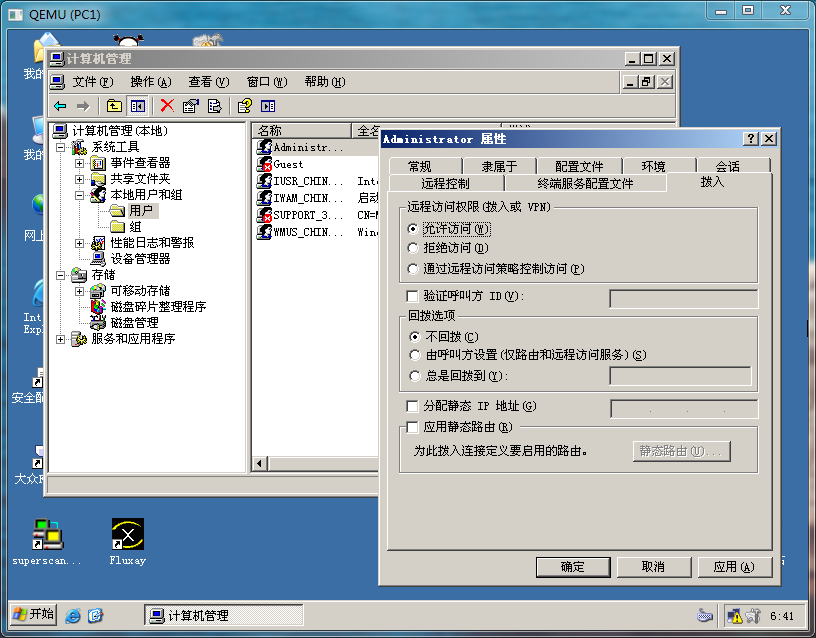


单击“配置”。选中“远程访问连接”则可以启动这个设备，选择“请求拨号路由选择连接”则可以启动这个设备的路由功能，在“最多端口数”中可以写入VPN连接同时打开的连接数。单击“确定”，完成对其端口的设置。



（3）配置VPN用户账户

依次单击“开始”->“管理工具”->“计算机管理”->“本地用户和组”，在弹出的窗口中打开域名，在user栏中找到允许拨入的用户，例如administrator，单击鼠标右键，单击“属性”，在“administrator”的属性窗口中，打开“拨入”菜单，选中“允许拨入”，以允许客户端以“administrator”用户的身份拨入VPN服务器，如下图所示：



**实验步骤二：配置VPN客户端**

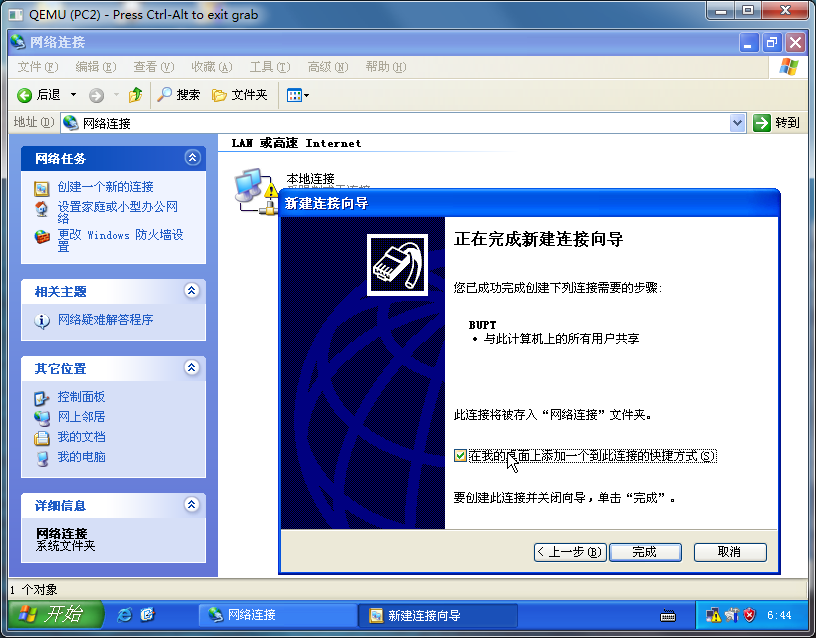
（1）在WindowsXP/Windows2003中选择“网络连接”，进入“新建连接向导”界面，选择“连接到我的工作场所的网络”，单击“下一步”按钮。

（2）在创建的网络连接界面中，选择“虚拟专用网络连接”，单击“下一步”按钮。

（3）在弹出的连接界面中，输入为此连接起的名字，然后单击“下一步”按钮。

（4）单击“下一步”按钮，此窗口要求输入VPN服务器端的IP地址或者主机名。

（5）单击“下一步”按钮，选中创建快捷方式，单击“完成”按钮。



完成后会弹出：



（6）依次单击“开始”->“连接到”->“网络连接”，可以看到新建立的BUPT连接，打开这个BUPT连接，则弹出界面，输入用户名和密码即可发起VPN连接。



（7）VPN客户端的连接属性配置，可以单击图“属性”按钮，在弹出的属性配置窗口中，打开“安全”菜单，可以选中“高级”，单击“设置”按钮，进一步配置VPN采用的加密方式和身份认证协议。

**实验步骤三：建立VPN连接**

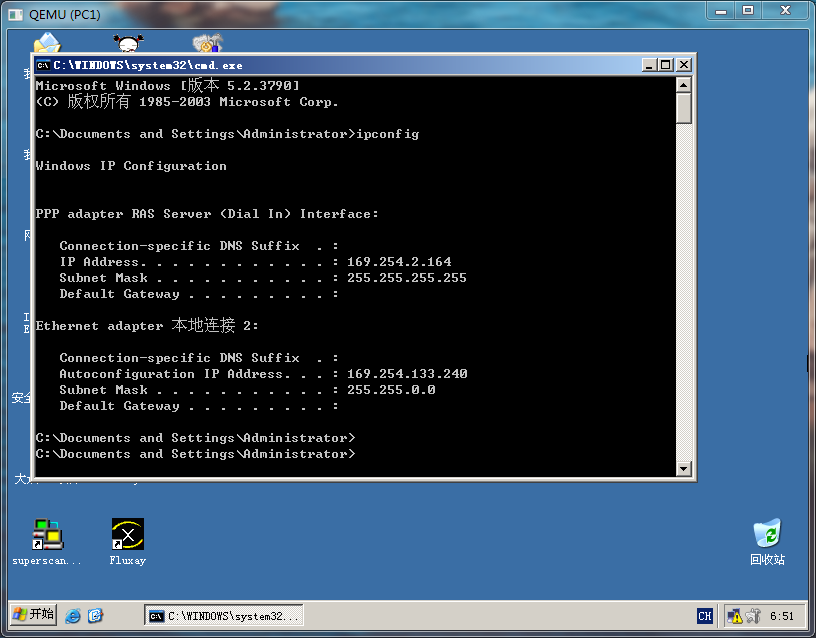
（1）建立VPN连接前，在客户端查看目前网络连接的配置情况，可以看出目前只有一个本地连接

（2）输入用户名（如administrator）和密码建立与VPN服务器的连接。

（3）成功建立起VPN客户端和服务器端的连接后，我们再看VPN客户端网络连接状况时，可以看到新增了一个VPNClient网络连接。

（4）在VPN的服务器端，使用命令“IPConfig”查看网络连接情况，看到多了RSA（remote access server）连接。

（5）打开“路由和远程访问”窗口，单击端口，可以看到一个WAN微型端口的状态已经成为“活动”状态。



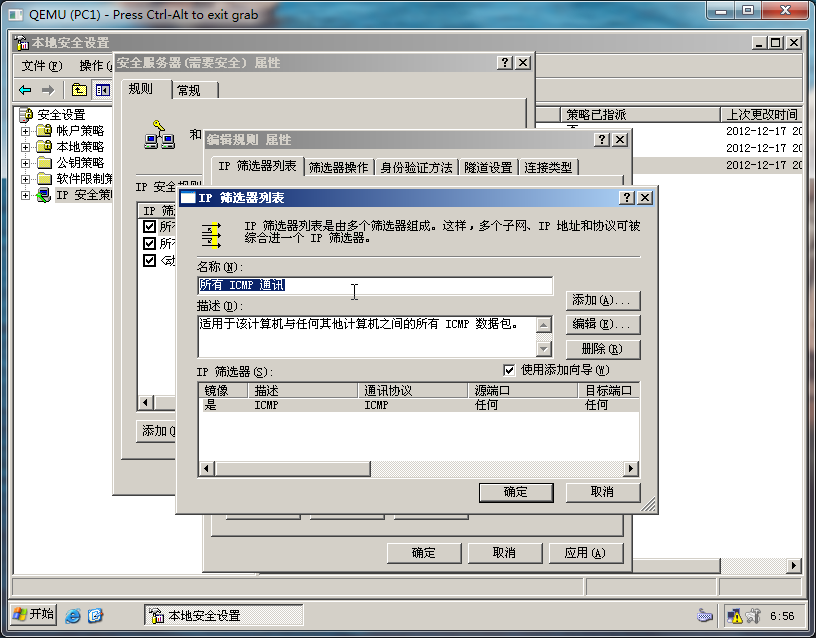
**实验步骤四：在Windows中配置端到端的IPSec VPN**

(1)Windows内置了IPSec安全策略，选择“开始”,进入“管理工具”—>“本地安全策略”， 进入“本地安全策略”下的IP安全策略。

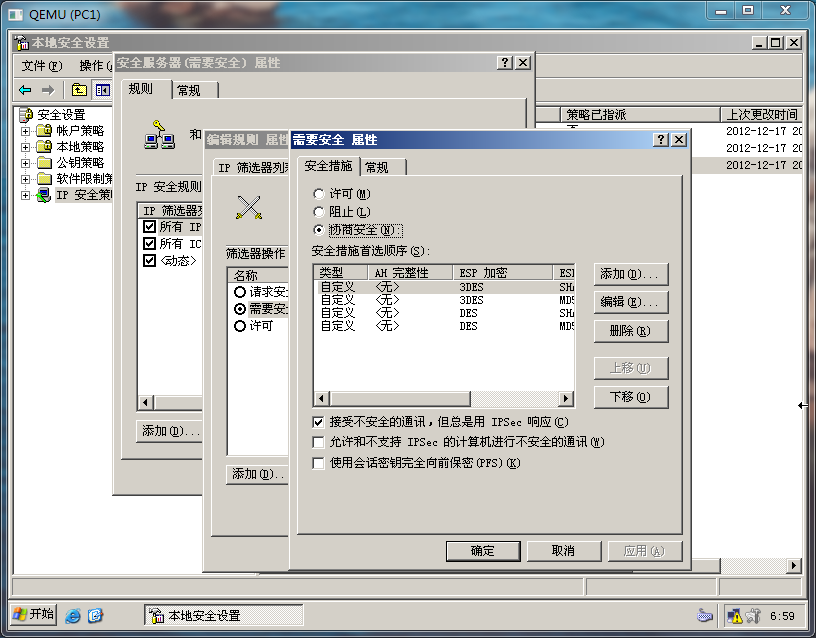
(2)双击“安全服务器”，弹出如图9-3所示的菜单，学生可自行增加或删除IP安全规则。

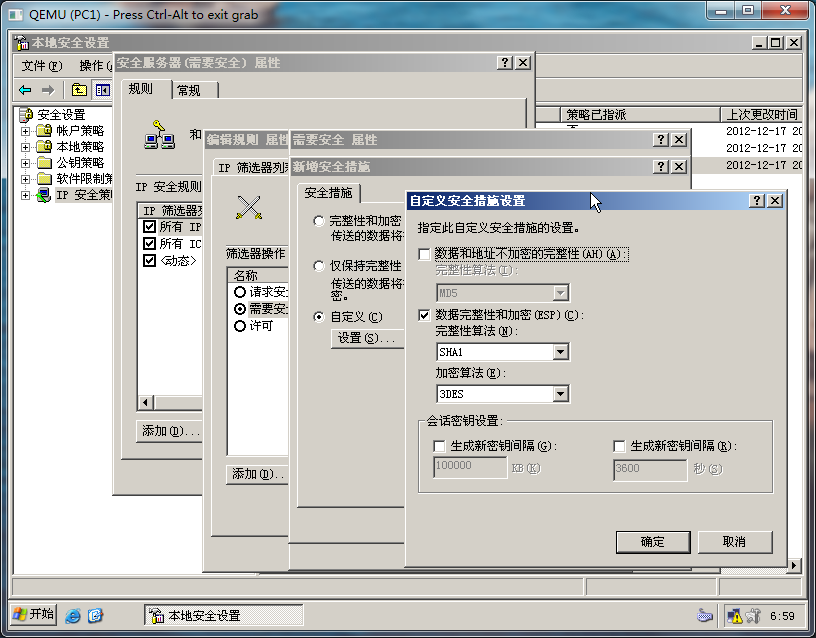
(3)下面查看每一条规则的安全规则包含的安全属性，并进行配置。双击“所有ICMP通讯量”，就可以出现如下图9-4所示的菜单。每一条IP安全规则包含：“IP筛选器列表”、“筛选器操作”、“身份验证方法”、“隧道设置”和“连接类型”5项安全属性。

a)“IP筛选器列表”如图9-5所示。源地址和目的地址可以设定启用VPN通道的具体IP地址。打开协议菜单，可以设定传输什么协议和端口时启用VPN安全协议。

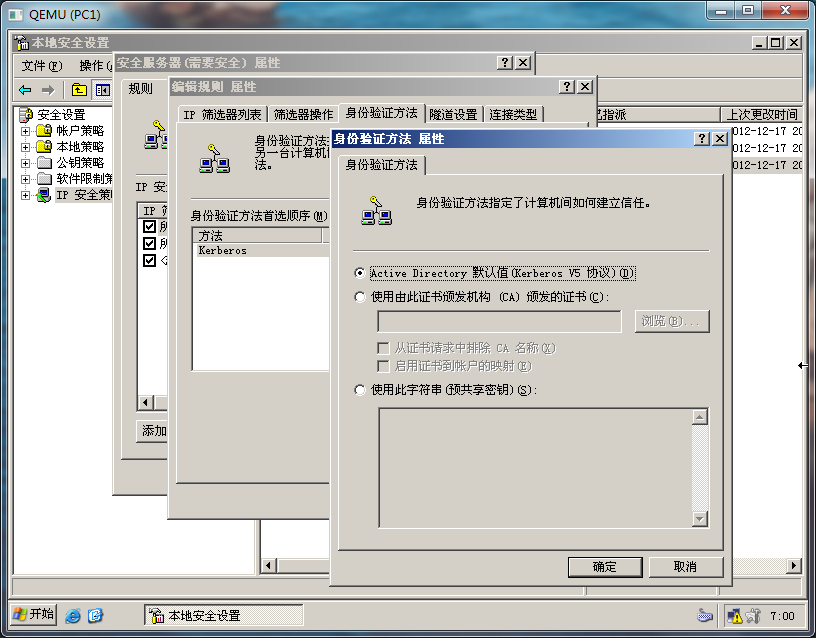


b)“筛选器操作”菜单如图9-6所示。这个菜单中共包括3个安全操作，安全性从高到低依次是“需要安全”、“请求安全”、“许可”，为了看到IPSec VPN的协商和加密过程，本实验选“需要安全”（如图9-7所示）。“需要安全”后可单击“编辑”按钮，在打开的“需要安全属性”菜单中，IPSec VPN所对应的默认选项是“协商安全”。可继续单击“编辑”按钮查看具体的安全措施，如图9-8所示，在“修改安全措施”菜单中，选中自定义后单击“设置”，在弹出的“自定义安全措施设置”对话框中，如图9-9所示可以看到IPSec所包含的AH和ESP协议的不同功能。





c)“身份认证菜单”如图9-10所示。在此菜单中规定了三种身份认证方法，Active Directory默认值是Kerberos V5协议进行身份认证的方法，第二种方法是采用数字证书认证，第三种方法是采用两端用户事先都知道的预共享密钥的方法。本实验采用方法三。



d)“隧道设置”属性采用传统模式，不采用网关到网关的隧道模式，所以保留默认选项“此规则不指定隧道”即可。

“连接类型”属性可设置网络连接的类型，同样采用默认的“所有网络连接”即可。

(1)在上述5条安全属性配置完成后，“所有ICMP通讯量”规则就配置完成了。可以自行按照上述步骤配置“所有IP通讯量”这条规则。对于“<动态>”规则，在实验中可不启用此条规则。

(2)安全规则设置完成后，右击“安全服务器”单击“指派”，这样将此计算机设置为VPN的“安全服务器”。至此，本机的IPSec VPN设置完成。

(3)同样，在另一台同样系统的计算机上也做上面的配置。在保证两台计算机之间网络通的情况下，从一台计算机用Ping命令测试两者之间的连接是连通的。