实验 4 用 Windows2003 实现网关-网关 VPN

中国科学技术大学 曾凡平

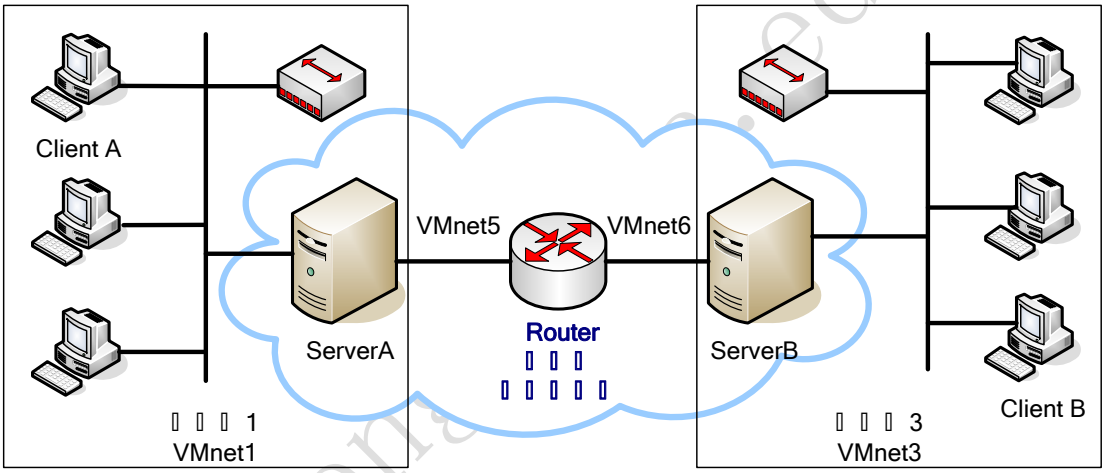
(2019 年 5 月 5 日)

4.1 实验目的

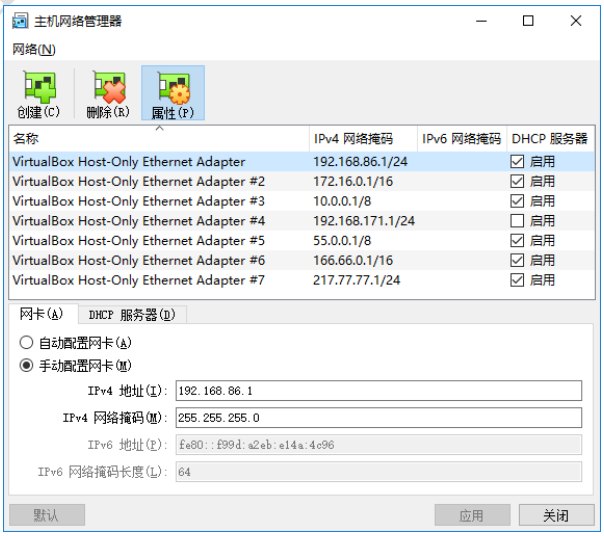
用 IPsec 隧道方式配置网关-网关 VPN，连接被 Internet 隔开的两个局域网(VMnet1 和 VMnet3)，使之进行安全通信，实现信息的保密和完整。

4.2 实验设计

从 ftp://cybersecurity.ustc.edu.cn/Windows2003SP2.zip 下载 Windows2003SP2.zip，配置 5 台 Windows2003SP2 虚拟机，分别用作 ServerA、ServerB、Router、ClientA 和 ClientB。用 **VirtualBox Host-Only Ethernet Adapter** 模拟两个局域网和一个广域网（用**路由器**模拟）。每个局域网含若干台客户机和一台 Windows server 2003 组成。具体设计和规划如下图：



虚拟网卡 VMnet1 和 VMnet3 分别模拟两个局域网，VMnet5、VMnet6 和 Router 模拟因特网，ServerA 和 ServerB 模拟互联网上的**边界路由器** (远程服务器)，建立 IPSec 隧道以连接两个局域网，用于保证通信安全。VirtualBox 的网络配置如下图所示：



实验所用的虚拟机配置如下表所示：

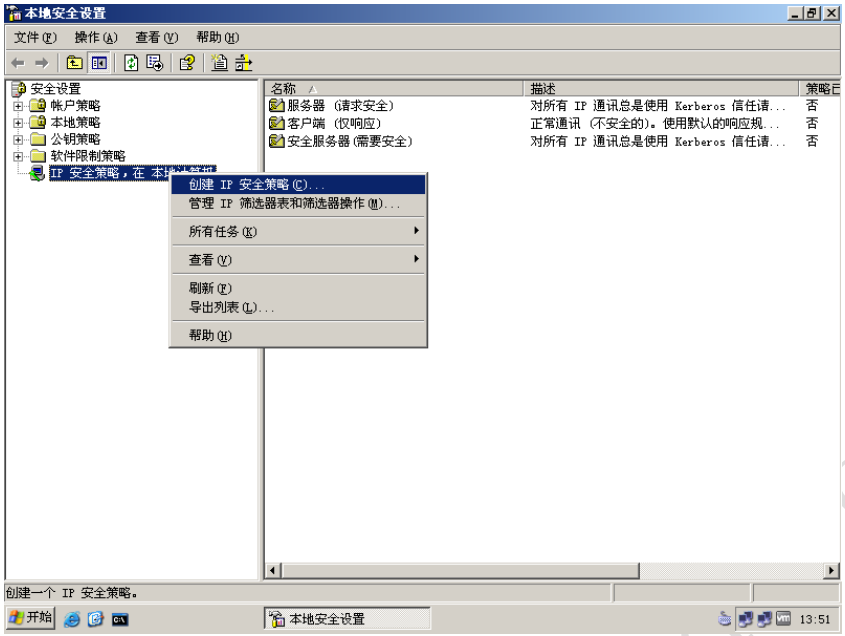
机器名	系统及必备软件	虚拟网络	IP 地址信息
Client A	Windows Server 2003 或任何其他 Windows	VMnet1	IP: 192.168.86.202 Subnet Mask: 255.255.255.0 GateWay: 192.168.86.203
Server A	Windows Server 2003	VMnet1 VMnet5	IP: 192.168.86.203 Subnet Mask: 255.255.255.0 GateWay: IP: 55.55.55.203 Subnet Mask: 255.0.0.0 **GateWay: 55.55.55.233**
Router	Windows Server 2003 **必须安装 Wireshark 软件** http://www.wireshark.org/	VMnet5 VMnet6	IP: 55.55.55.233 Subnet Mask: 255.0.0.0 **GateWay:** IP: 166.66.66.233 Subnet Mask: 255.255.0.0 **GateWay:**
Server B	Windows Server 2003	VMnet6 VMnet3	IP: 166.66.66.213 Subnet Mask: 255.255.0.0 **GateWay: 166.66.66.233** IP: 10.0.0.213 Subnet Mask: 255.0.0.0 GateWay:
Client B	Windows Server 2003 或或任何其他 Windows	VMnet3	IP: 10.0.0.202 Subnet Mask: 255.0.0.0 GateWay: 10.0.0.213

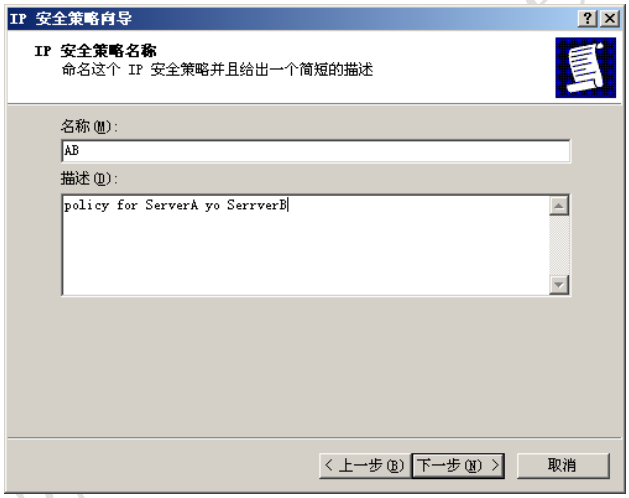
注意：可 2 人为一组进行实验，每人模拟一个局域网(或不用 ClientA 和 ClientB)

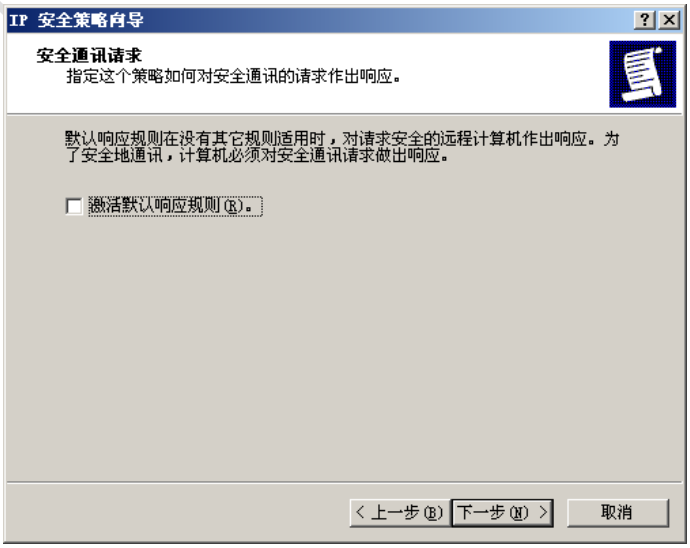
4.3 实验步骤

4.3.1 创建 ServerA 的 IPSec 策略

(1) 管理工具中打开”本地安全策略”--右击”IP 安全策略,在本地计算机”—“创建 IP 安全策略”--命名为”AB”--取消选择”激活默认响应规则”--.编辑”AB”属性,添加新规则(不使用添加向导)

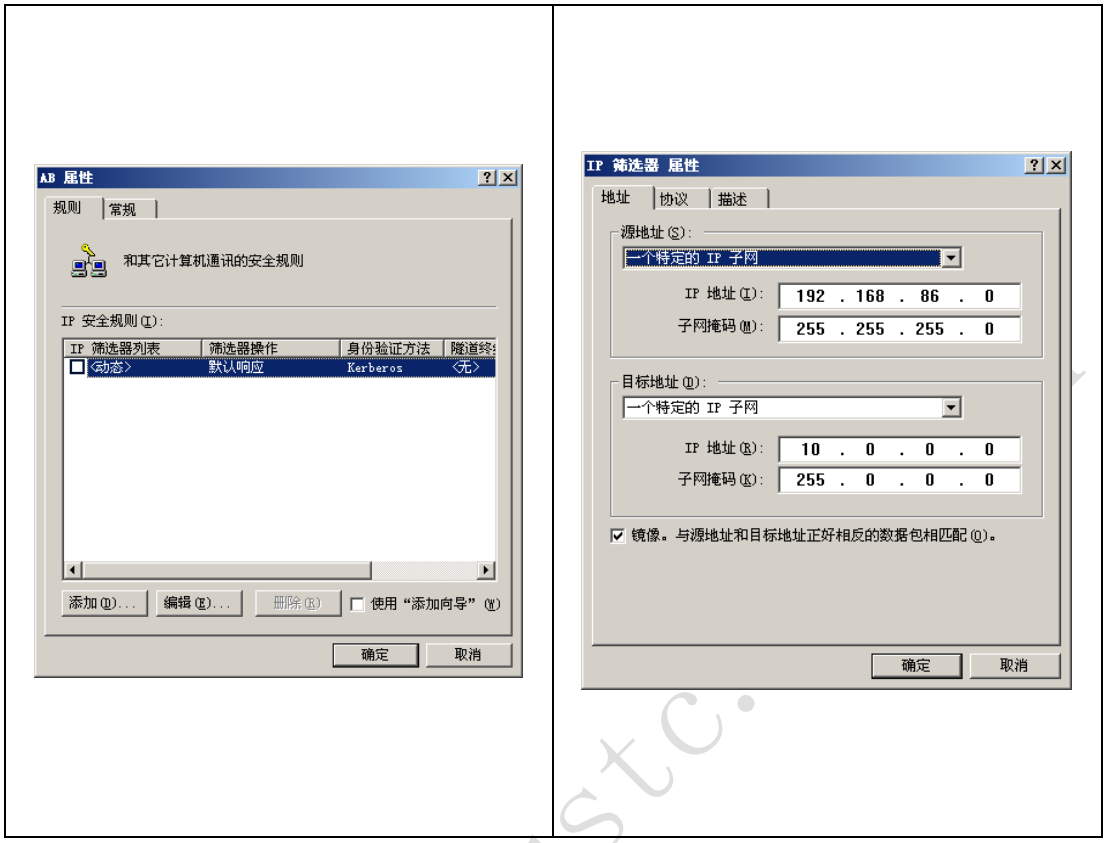




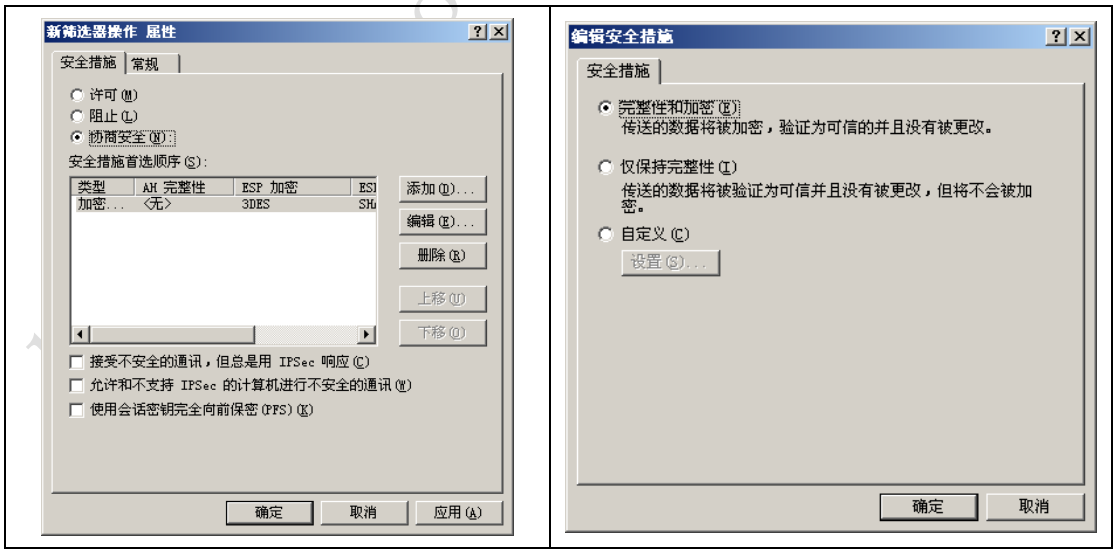


(2) 添加"IP 筛选器列表",命名为"A to B"--添加属性(不使用添加向导),设置源地址为"特

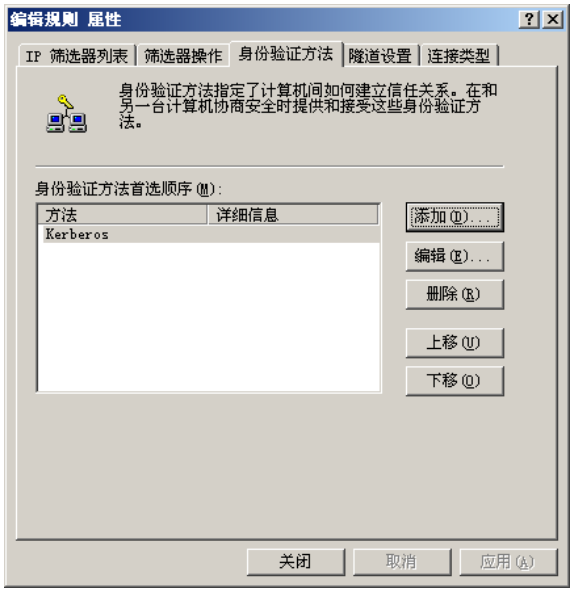
定 IP 子网:192.168.86.0",目的地址设置为"特定 IP 子网:10.0.0.0"--取消选择"镜像"--协议设定为默认值:"任意"。

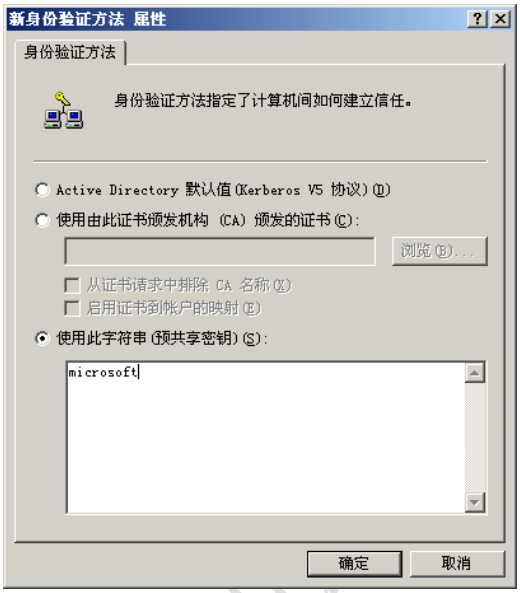


(3) 筛选器操作(不使用添加向导):安全措施为"协商安全",新增安全措施为"完整性和加密"

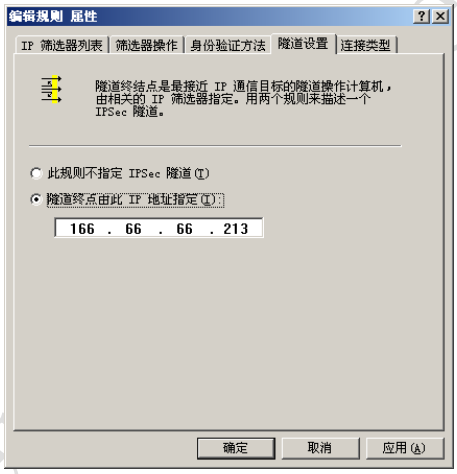


(4) 身份验证方法,使用预共享密钥: microsoft

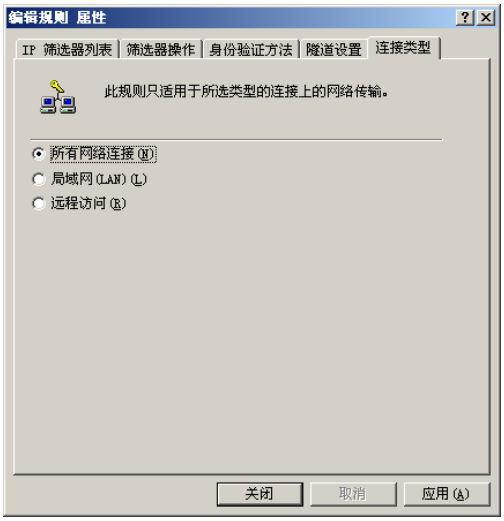




(5) 隧道设置,指定隧道终点 IP 地址(Server B 的外网 IP 地址：166.66.66.213)



(6) 连接类型为"所有连接"



(7) 重复(2)-(6),创建 IP 筛选器列表"B to A"

设置从 ServerB 到 ServerA 的 IP 策略。将“源子网(IP)”和“目的子网(IP)”互换，隧道终点

设置为 55.55.55.203。

(8) 在本地安全设置中,右击策略"AB"—指派

4.3.2 创建 ServerB 的 IPSec 策略

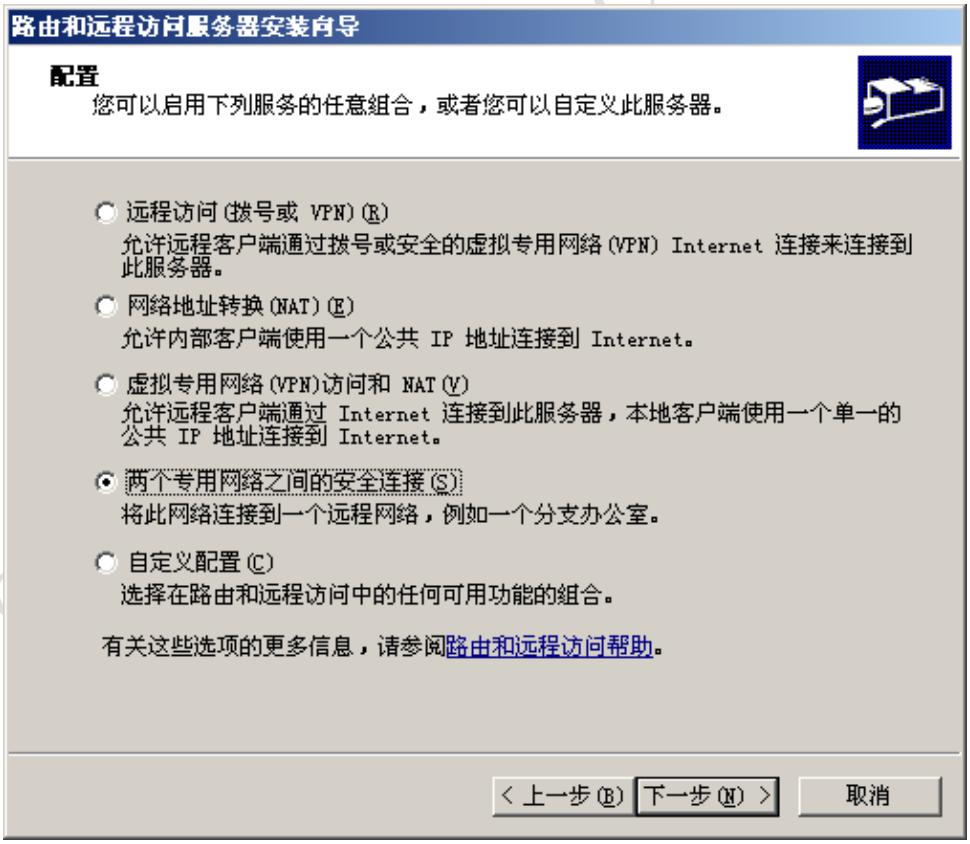
按相同的方法步骤，创建 ServerB 的 IP 安全策略并指派。

4.3.3 配置远程访问/VPN 服务器

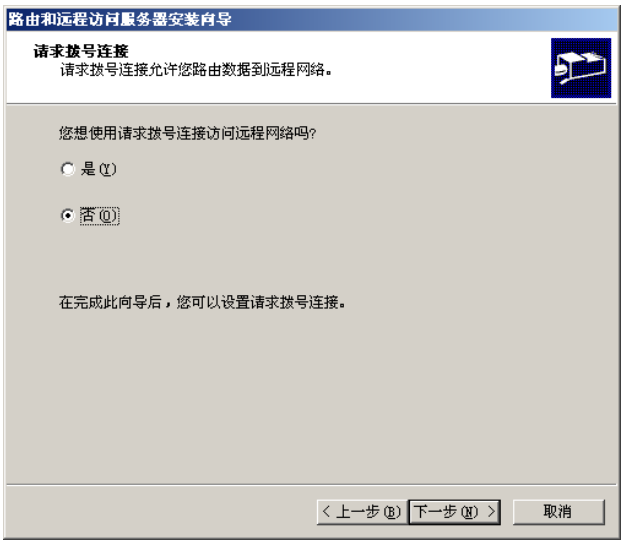
配置 Server A、Router 和 Server B 为路由器。在“开始”—“所有程序”—“管理工具”菜单中选择“路由和远程访问”，如下图所示：

打开“路由和远程访问”管理界面，选择“配置并启用路由和远程访问”，如下图所示：

配置为“两个专用网络之间的安全连接”，如下图所示：



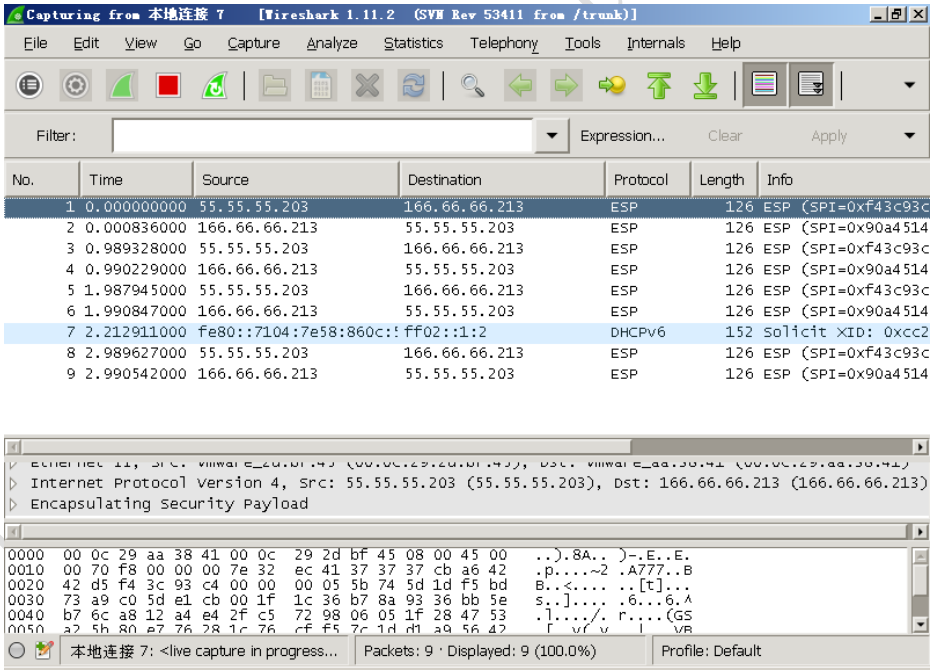
不选择拨号 VPN，如下图所示：



配置完成后，ServerA 可以和 ServerB 互联互通。

4.3.4 ping 测试(Client A)

在 Client A 的 cmd 中输入>ping 10.0.0.202，或者在 Client B 的 cmd 中输入>ping 192.168.86.202。如果两方的 IPsec 策略未配置正确，不会 ping 通。如果正确则说明两个局域网互联互通。



在数据通道中的路由器用 wireshark 检测到的是 ESP 数据包，因此实现了数据的完全保密，通信内容无法被窃听。

4.4 上机实践(过关测试)

实验老师检查路由器中的 wireshark 的输出，若检测到的是 ESP 数据包，则 VPN 配置成功；否则，重做实验。