

# 实验四：用Windows2003实现网关-网关VPN

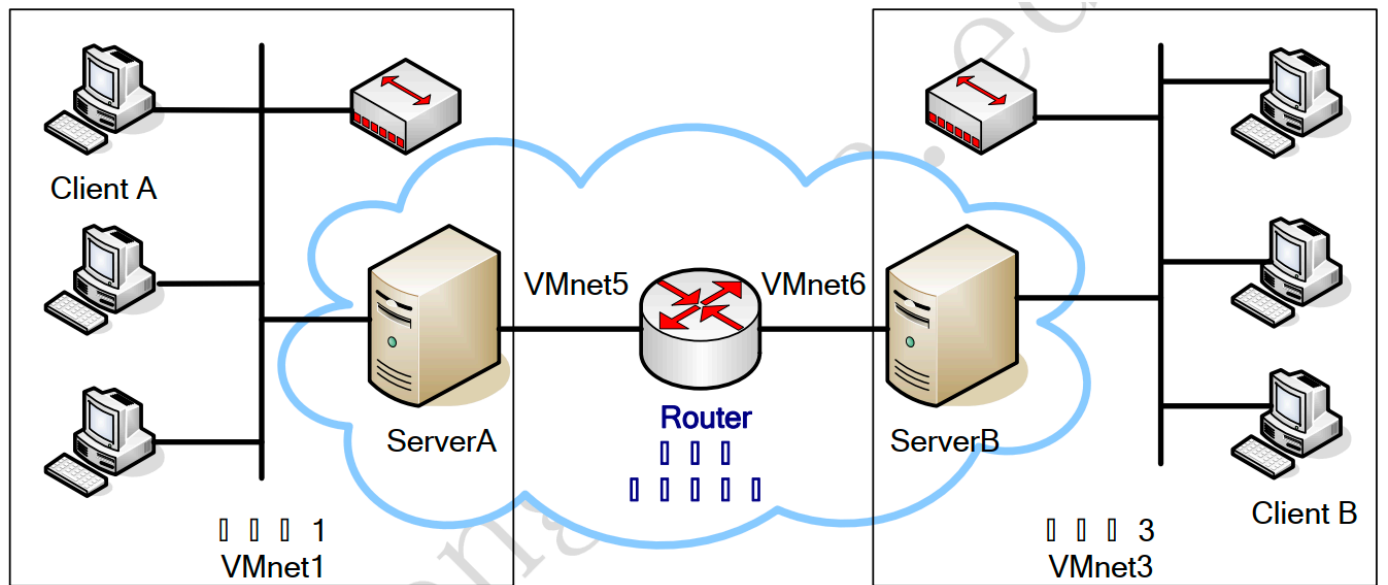
吴毅龙 PB19111749

## 1. 实验目的

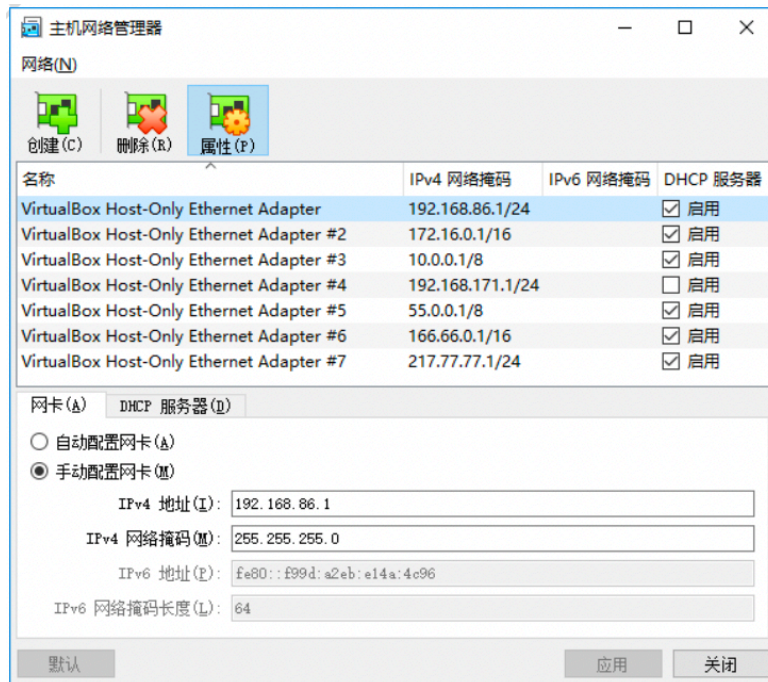
用 IPsec 隧道方式配置网关-网关 VPN，连接被 Internet 隔开的两个局域网(VMnet1 和 VMnet3)，使之进行安全通信，实现信息的保密和完整。

## 2. 实验设计

下载并导入到虚拟机。然后复制 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 server2003 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：



按照实验指导的配置表格配置各个虚拟机的网络设置。其中相同颜色框选出的IP地址应该相同。

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 <b>GateWay: 192.168.86.203</b>
Server A	Windows Server 2003	VMnet1 VMnet5	<b>IP: 192.168.86.203</b> Subnet Mask: 255.255.255.0 GateWay: IP: 55.55.55.203 Subnet Mask: 255.0.0.0 <b>GateWay: 55.55.55.233</b>
Router	Windows Server 2003 <b>必须安装 Wireshark 软件</b> <a href="http://www.wireshark.org/">http://www.wireshark.org/</a>	VMnet5 VMnet6	<b>IP: 55.55.55.233</b> Subnet Mask: 255.0.0.0 <b>GateWay:</b> <b>IP: 166.66.66.233</b> Subnet Mask: 255.255.0.0 <b>GateWay:</b>
Server B	Windows Server 2003	VMnet6 VMnet3	IP: 166.66.66.213 Subnet Mask: 255.255.0.0 <b>GateWay: 166.66.66.233</b> <b>IP: 10.0.0.213</b> Subnet Mask: 255.0.0.0 GateWay:
Client B	Windows Server 2003 或任何其他 Windows	VMnet3	IP: 10.0.0.202 Subnet Mask: 255.0.0.0 <b>GateWay: 10.0.0.213</b>

将路由器、ClientA 及 ClientB 的 IPv4 地址的第 4 个点分十进制数（如 192.168.86.202 的第 4 个点分十进制数为 202）改成你学号的最后 3 位数字%200（进行“模 200”运算），其他部分的 IP 地址也可能需要修改以避免 IP 地址重复。实际 IP 地址信息配置如下所示：

机器名	虚拟网络	IP地址信息
Client A	VMnet1	IP: 192.168.86.149 Subnet Mask: 255.255.255.0 <b>GateWay: 192.168.86.203</b>
Sever A	VMnet1 VMnet5	<b>IP: 192.168.86.203</b> Subnet Mask: 255.255.255.0 GateWay:  IP: 55.55.55.203 Subnet Mask: 255.0.0.0 <b>GateWay: 55.55.55.149</b>
Router	VMnet5 VMnet6	<b>IP: 55.55.55.149</b> Subnet Mask: 255.0.0.0 GateWay:  <b>IP: 166.66.66.149</b> Subnet Mask: 255.255.0.0 GateWay:
Server B	VMnet6 VMnet3	IP: 166.66.66.213 Subnet Mask: 255.255.0.0 <b>GateWay: 166.66.66.149</b>  <b>IP: 10.0.0.213</b> Subnet Mask: 255.0.0.0 GateWay:
Client B	VMnet3	IP: 10.0.0.149 Subnet Mask: 255.0.0.0 <b>GateWay: 10.0.0.213</b>

- 配置结果如下所示：
- Client A

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\work>ipconfig

Windows IP Configuration

Ethernet adapter net1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.86.149
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.86.203

C:\work>
```

- Server A

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\work>ipconfig

Windows IP Configuration

Ethernet adapter net6:

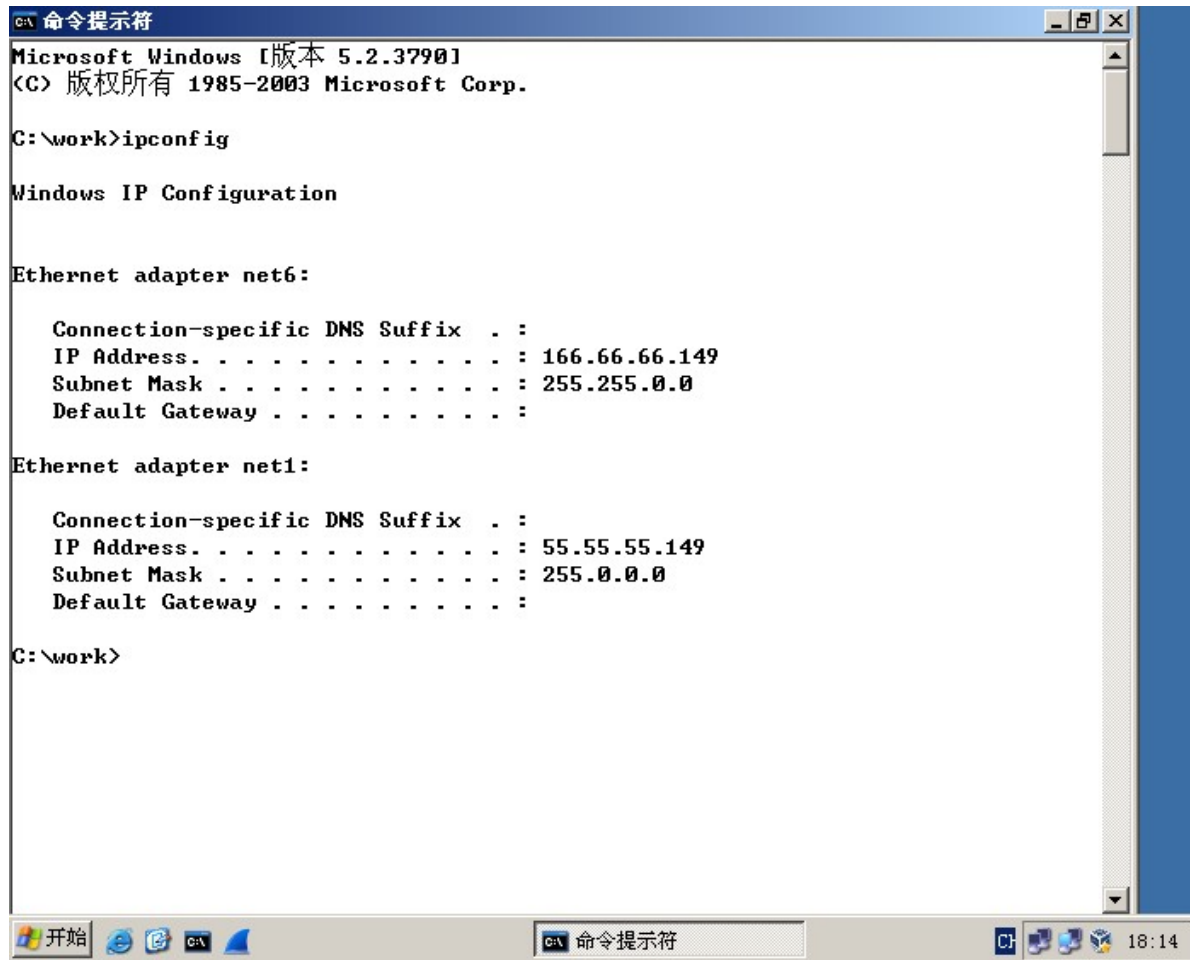
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 55.55.55.203
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 55.55.55.149

Ethernet adapter net1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.86.203
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\work>
```

- Router



```
C:\ 命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\work>ipconfig

Windows IP Configuration

Ethernet adapter net6:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 166.66.66.149
    Subnet Mask . . . . .             : 255.255.0.0
    Default Gateway . . . . .         : 

Ethernet adapter net1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 55.55.55.149
    Subnet Mask . . . . .             : 255.0.0.0
    Default Gateway . . . . .         : 

C:\work>
```

The screenshot shows a Windows XP desktop with a taskbar at the bottom. The taskbar includes the '开始' (Start) button, several application icons, and a system tray showing the time as 18:14. The active window is a command prompt titled 'C:\ 命令提示符'. The command prompt displays the output of the 'ipconfig' command, showing details for two network adapters: 'net6' and 'net1'. Adapter 'net6' has an IP address of 166.66.66.149 and a subnet mask of 255.255.0.0. Adapter 'net1' has an IP address of 55.55.55.149 and a subnet mask of 255.0.0.0. Both adapters have no default gateway or DNS suffix configured.

- Server B

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\work>ipconfig

Windows IP Configuration

Ethernet adapter net6:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 166.66.66.213
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 166.66.66.149

Ethernet adapter net1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.0.213
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 

C:\work>
```

- Client B

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\work>ipconfig

Windows IP Configuration

Ethernet adapter net1:

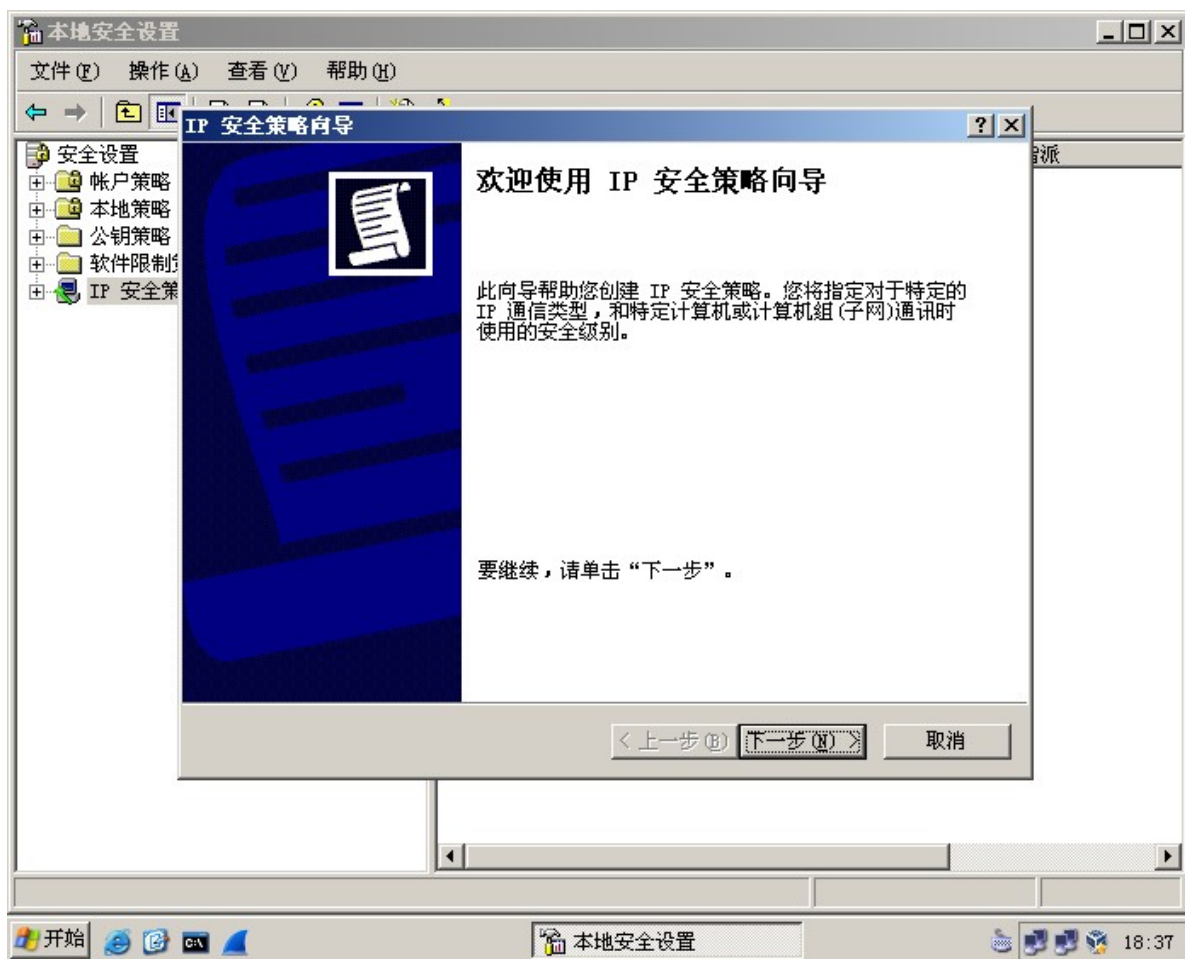
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.0.149
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.0.0.213

C:\work>
```

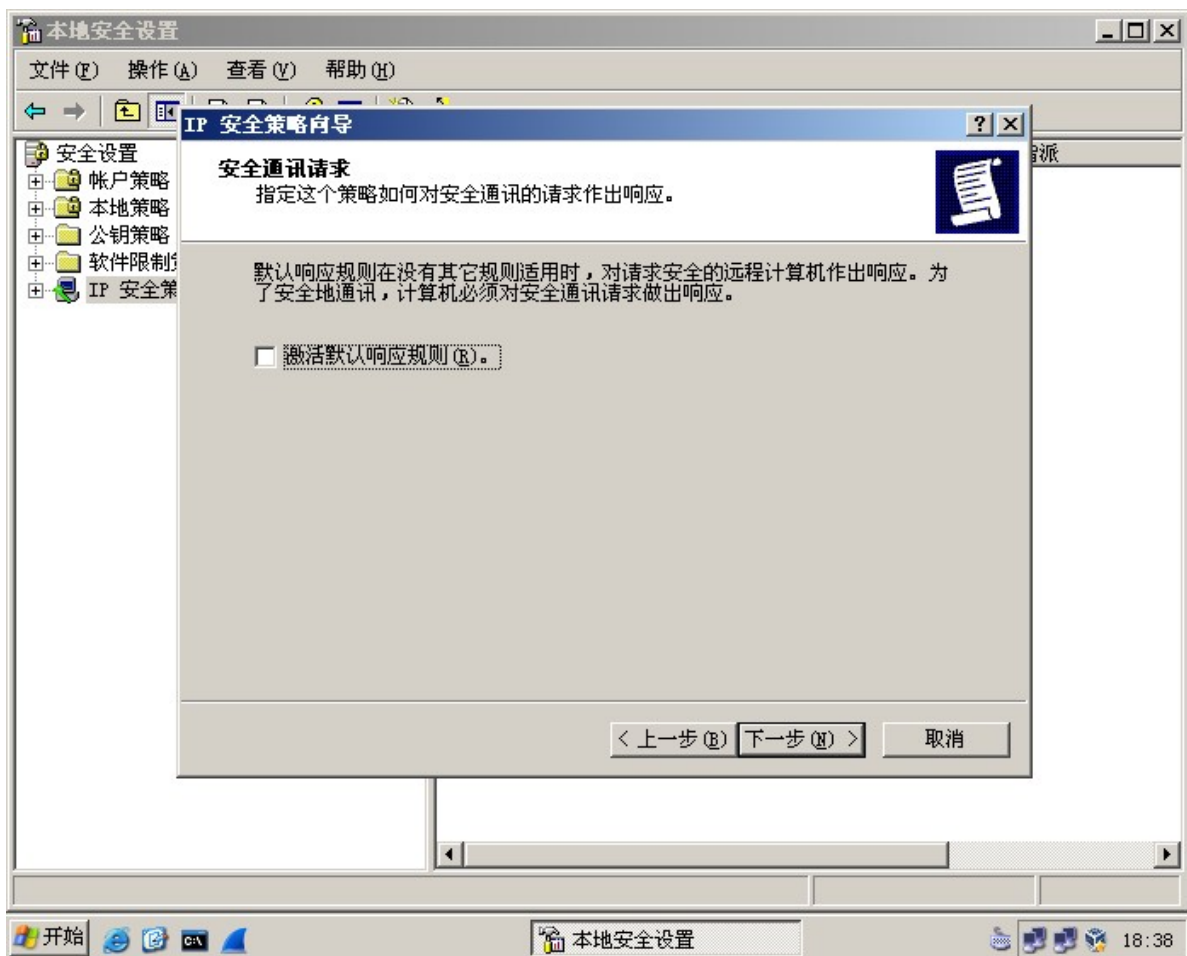
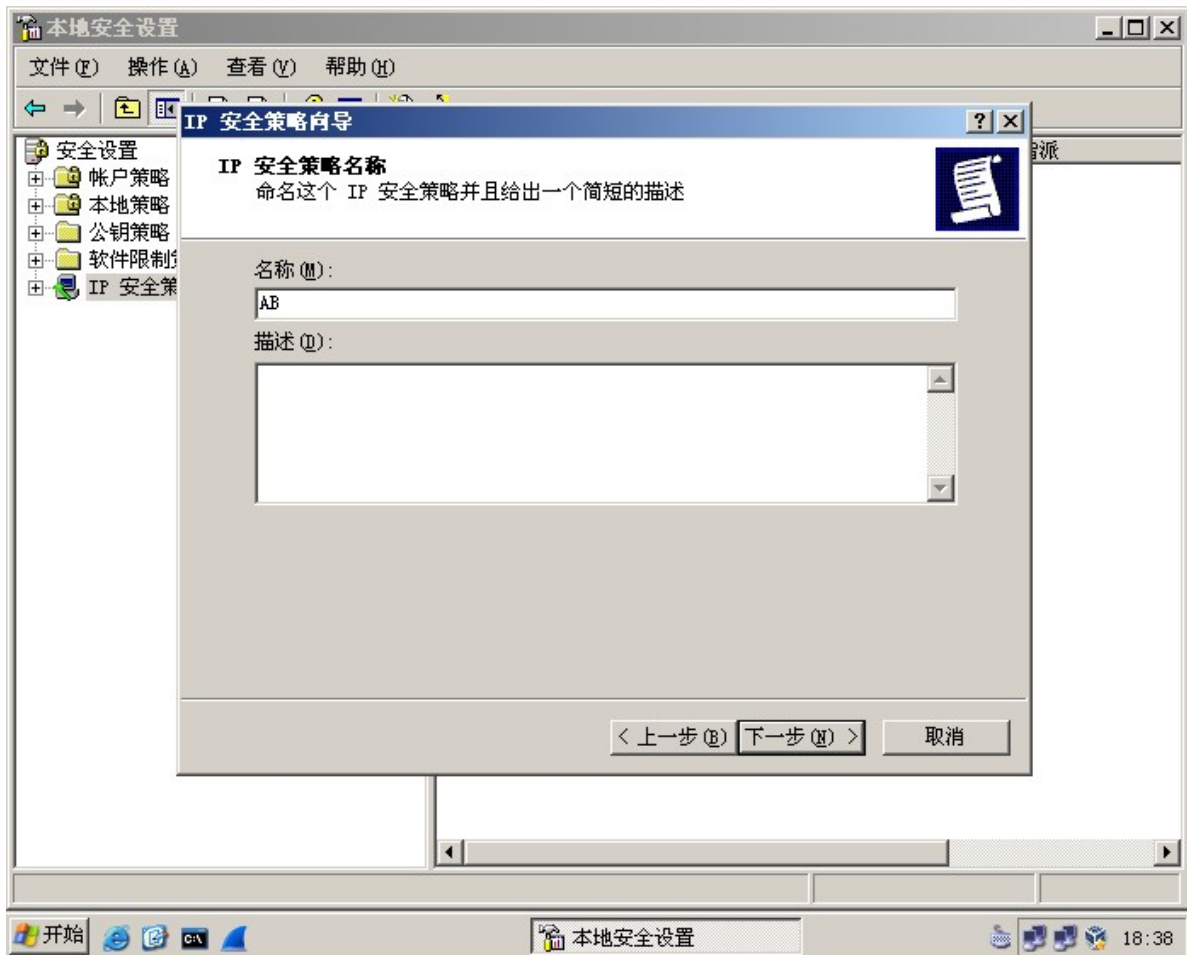
### 3. 实验步骤

#### 3.1 创建Sever A的IPSec策略

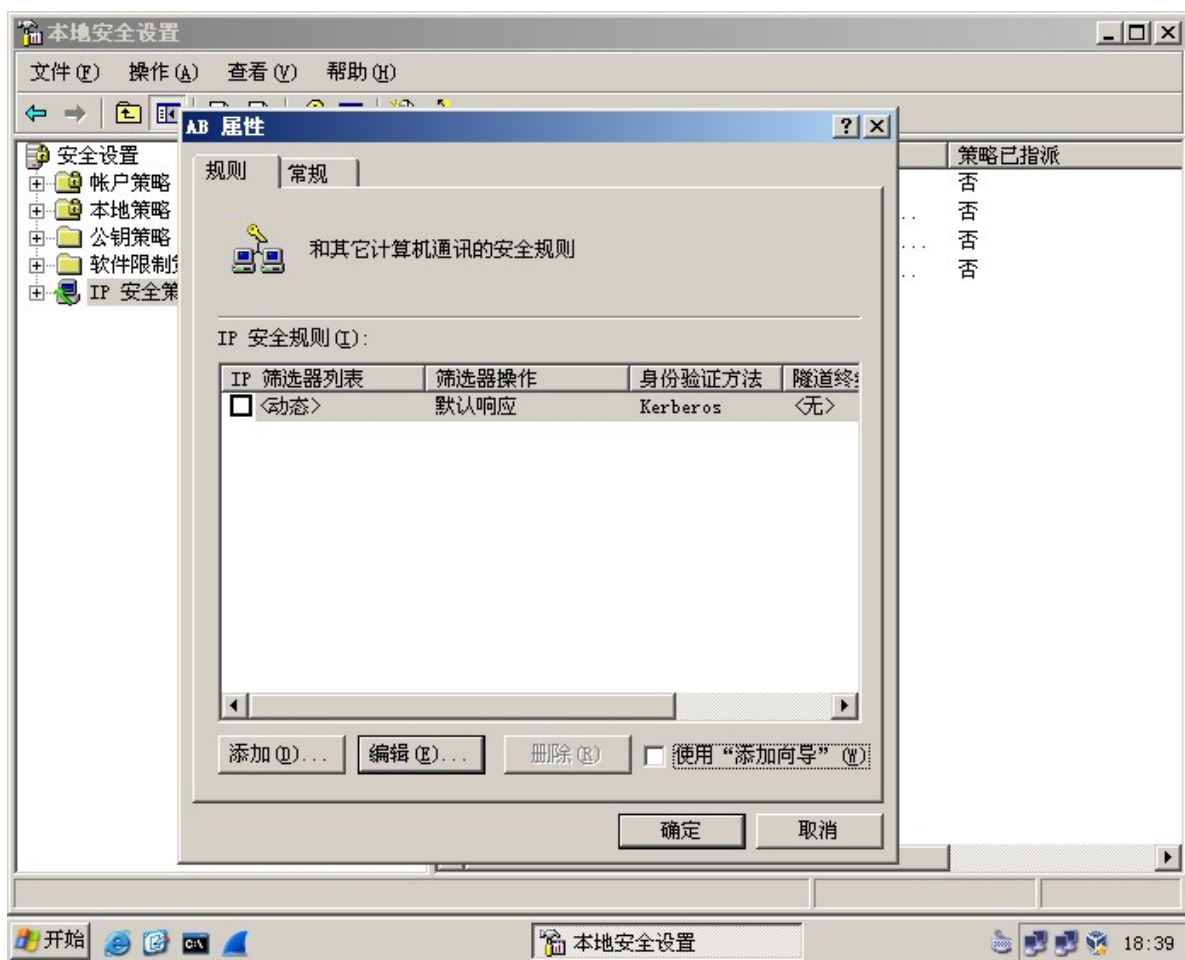
- 管理工具中打开“本地安全策略”--右击“IP 安全策略,在本地计算机”--“创建 IP 安全策略”--命名为“AB”--取消选择“激活默认响应规则”--.编辑“AB”属性,添加新规则(不使用添加向导)

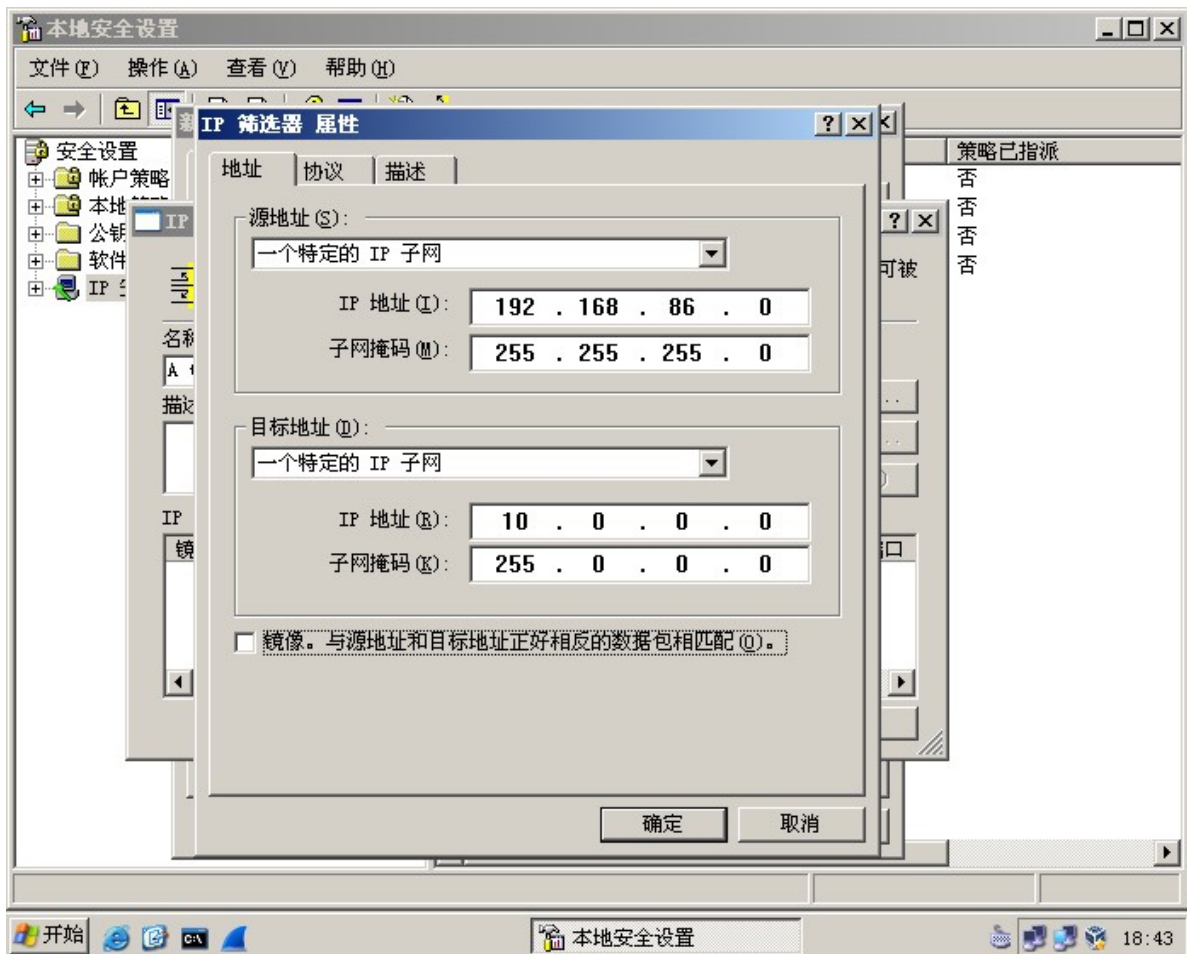
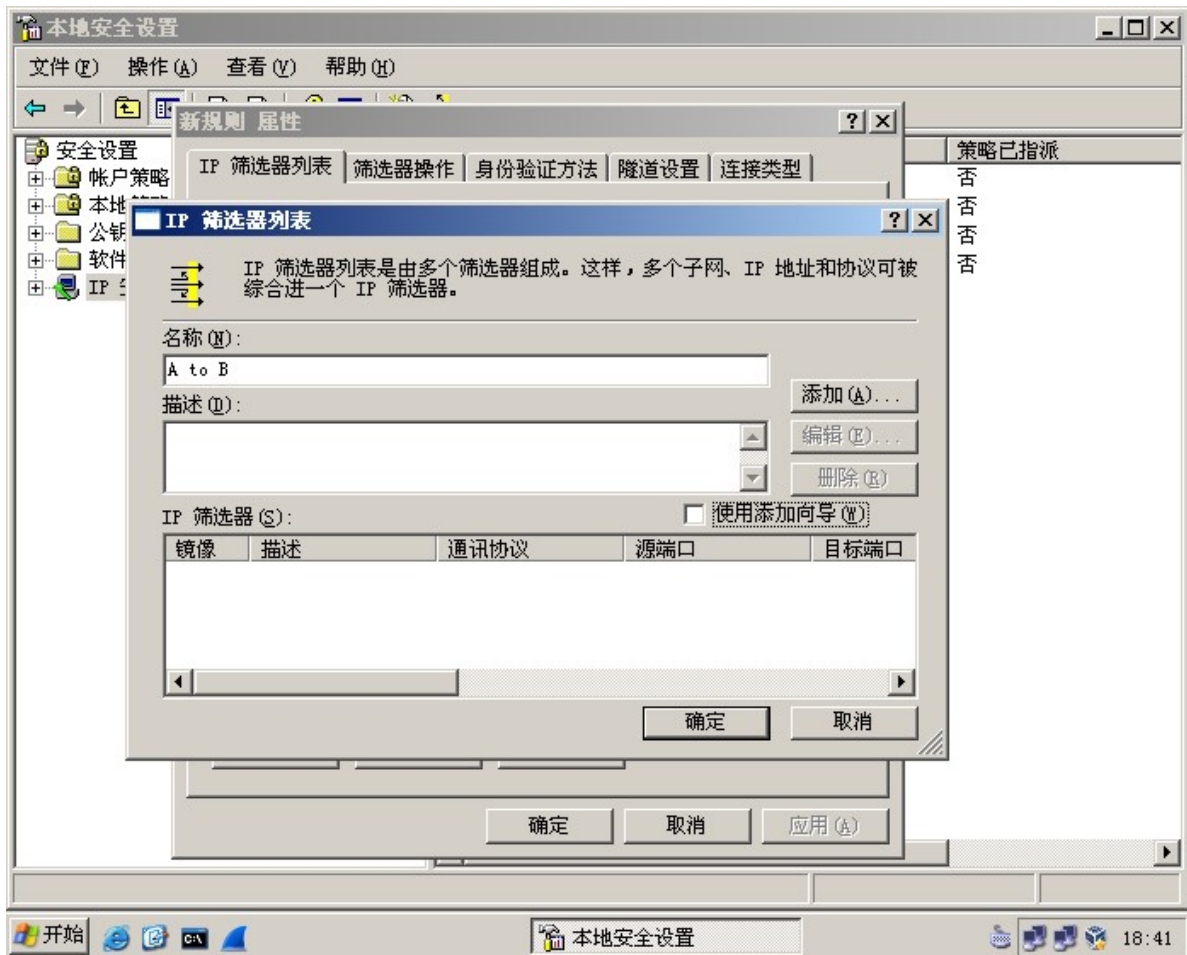


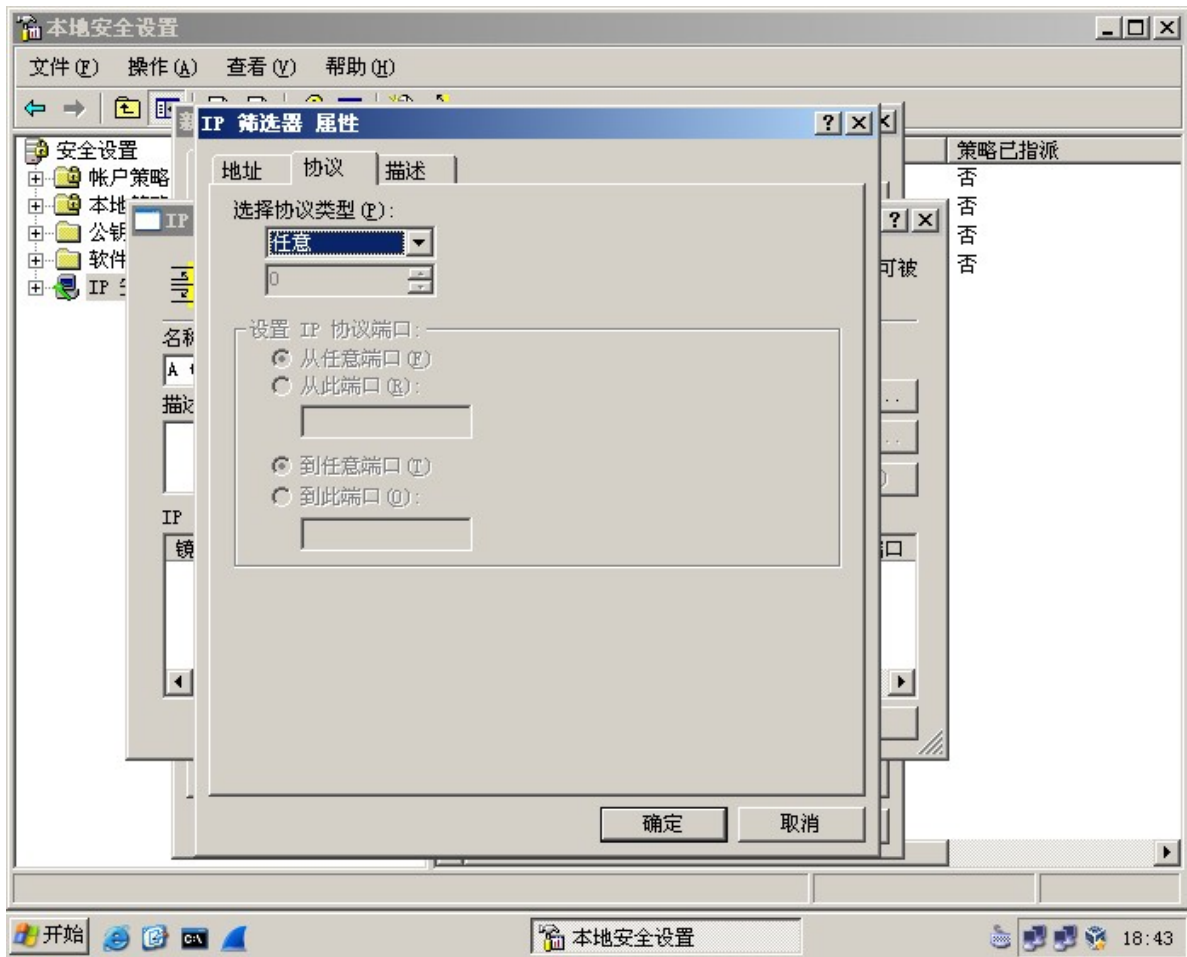




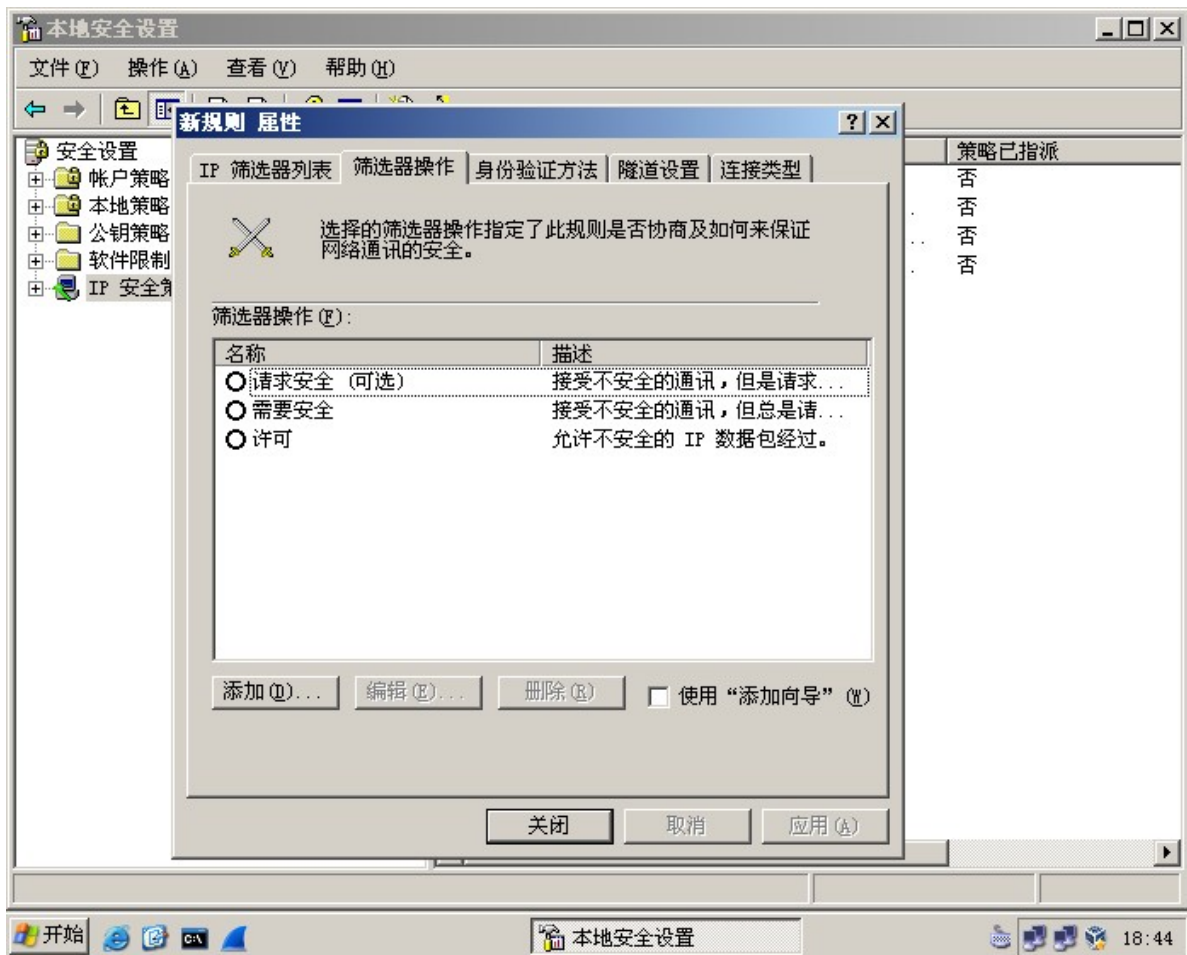
- 添加"IP 筛选器列表",命名为"A to B"--添加属性(不使用添加向导),设置源地址为"特定 IP 子网:192.168.86.0",目的地址设置为"特定 IP 子网:10.0.0.0"--取消选择"镜像"--协议设定为默认值:"任意"。

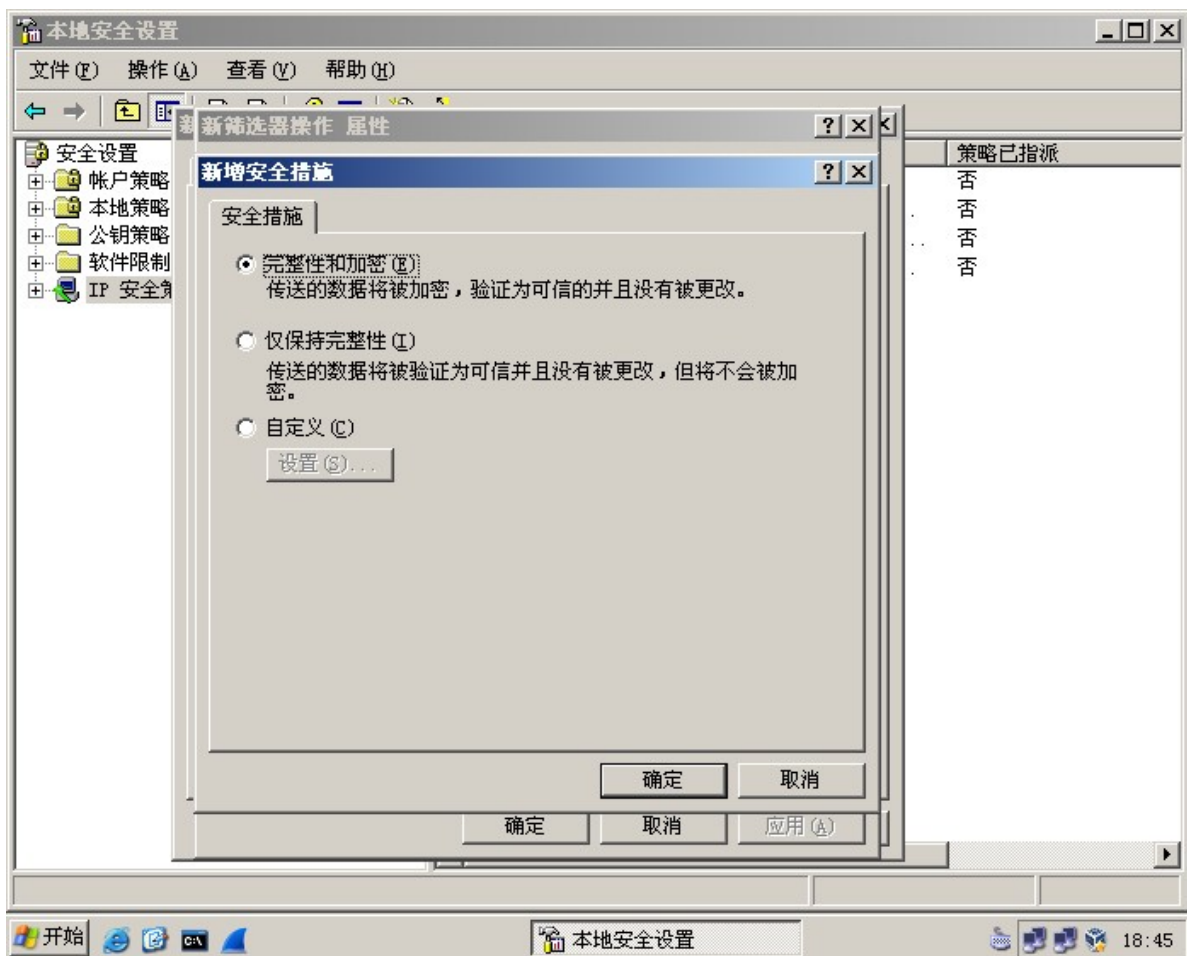
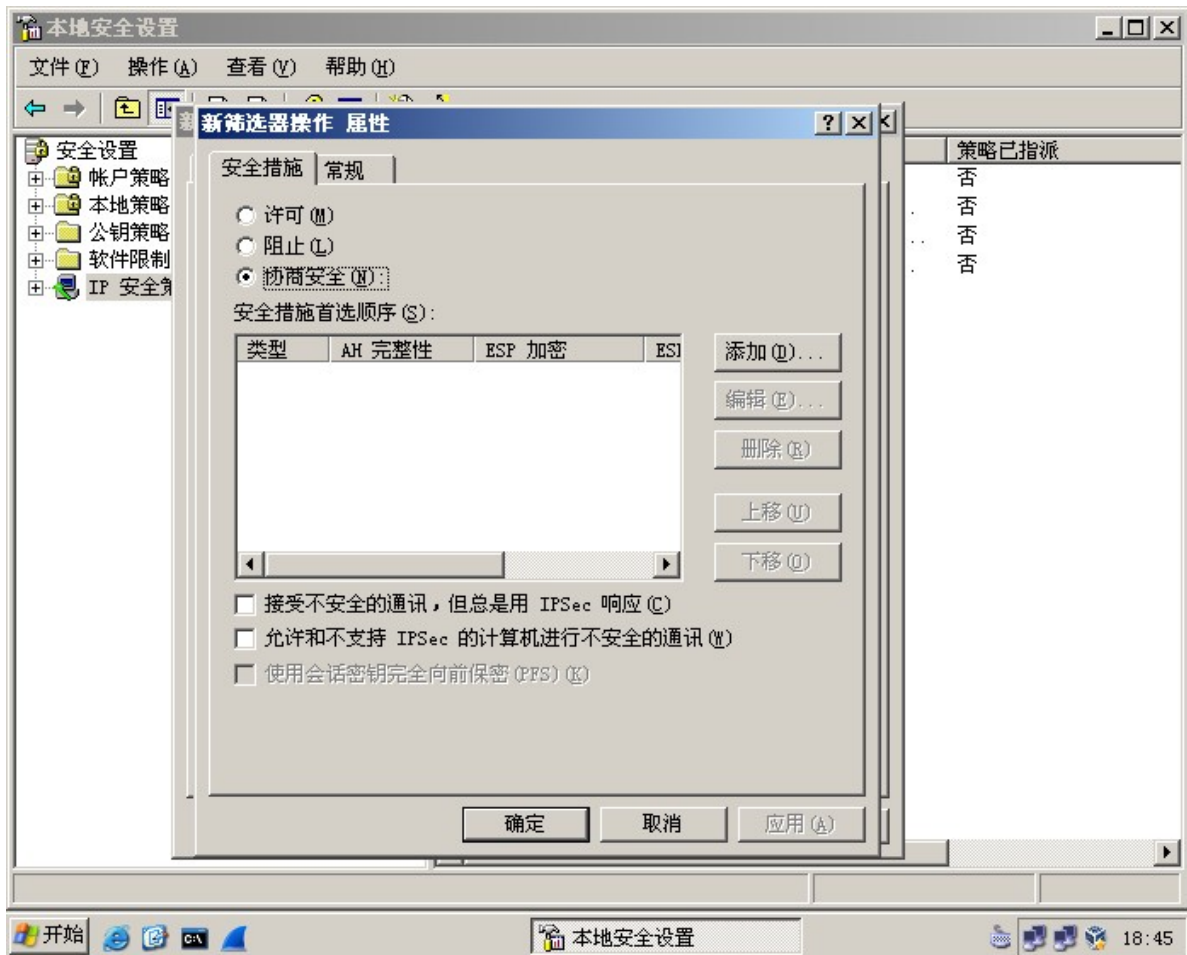






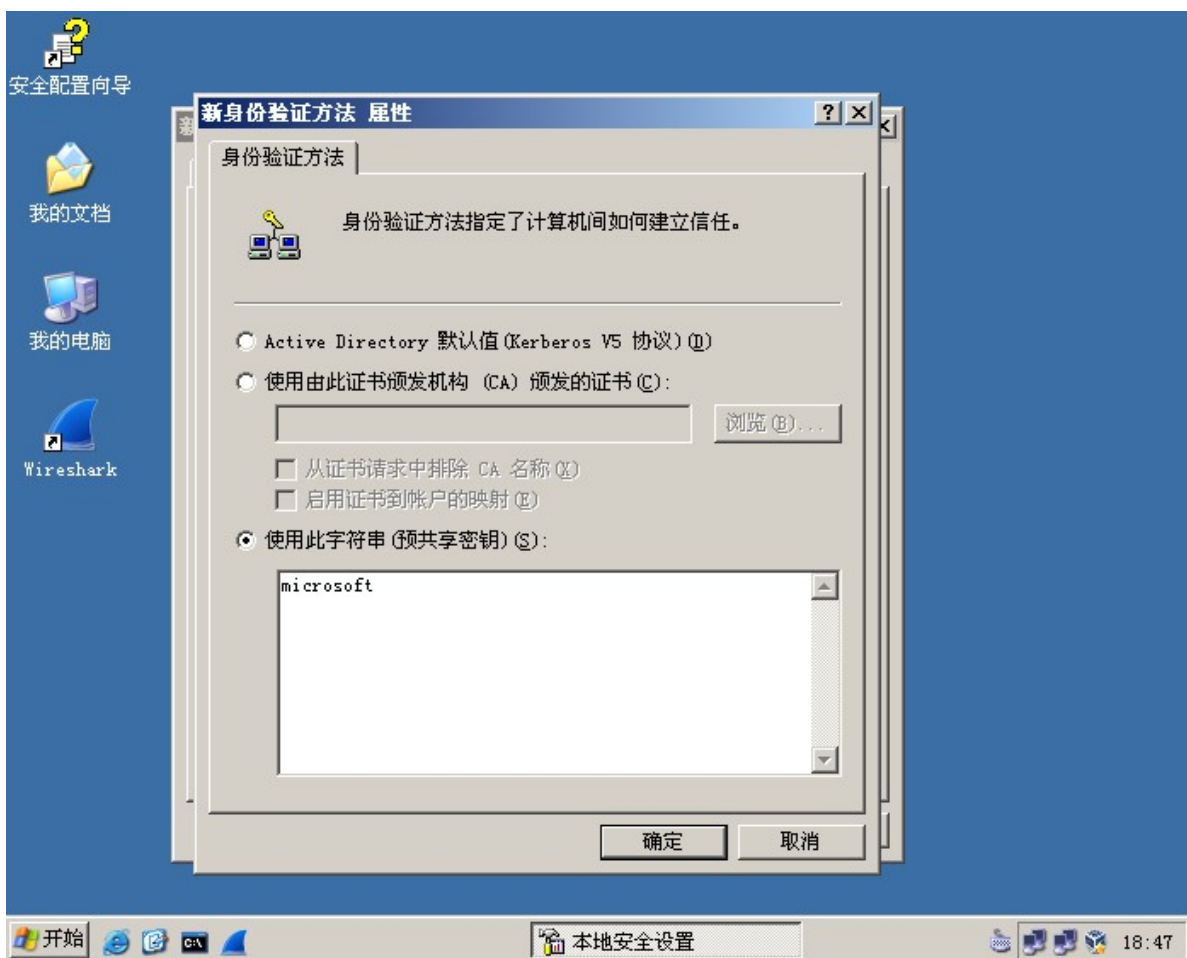
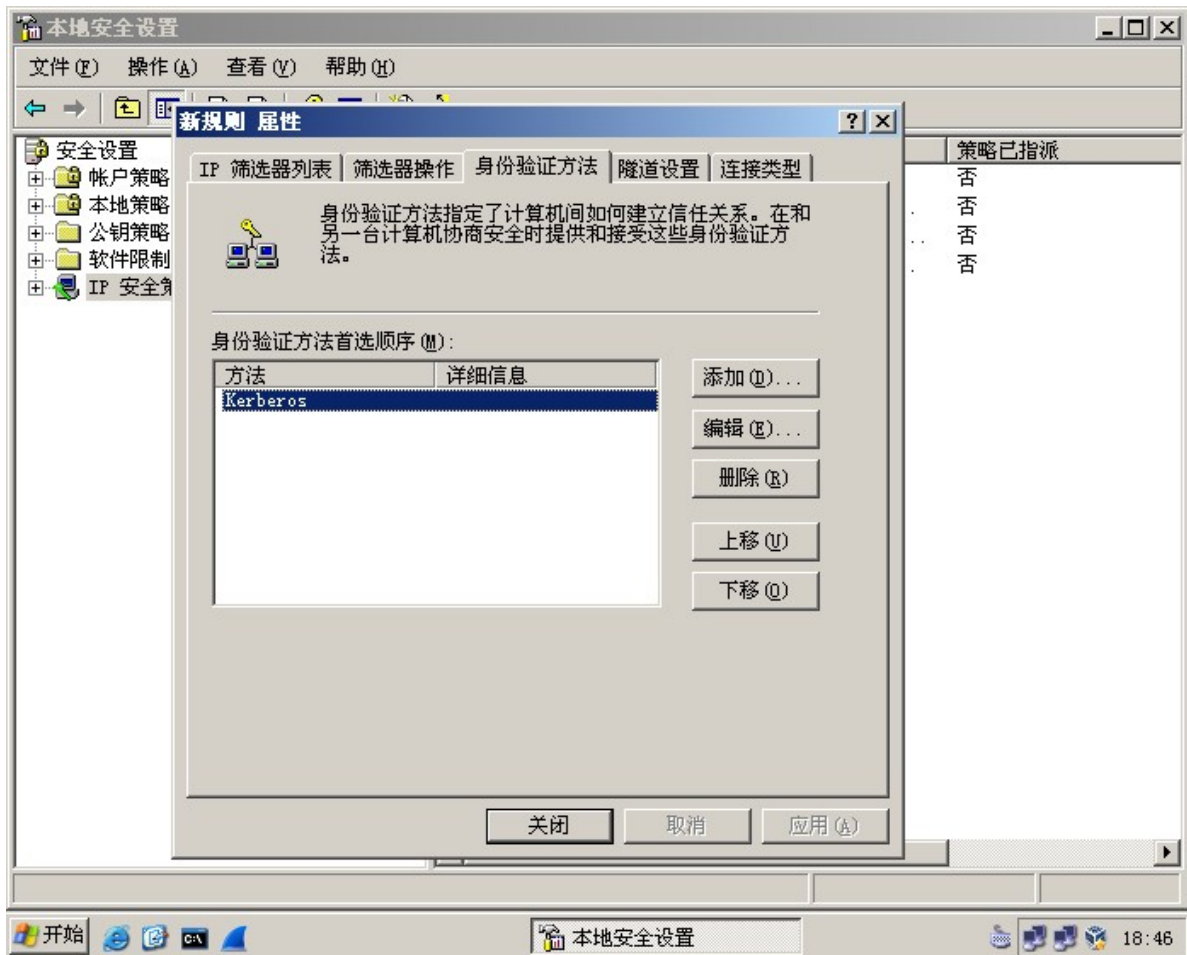
- 筛选器操作(不使用添加向导):安全措施为"协商安全",新增安全措施为"完整性和加密"



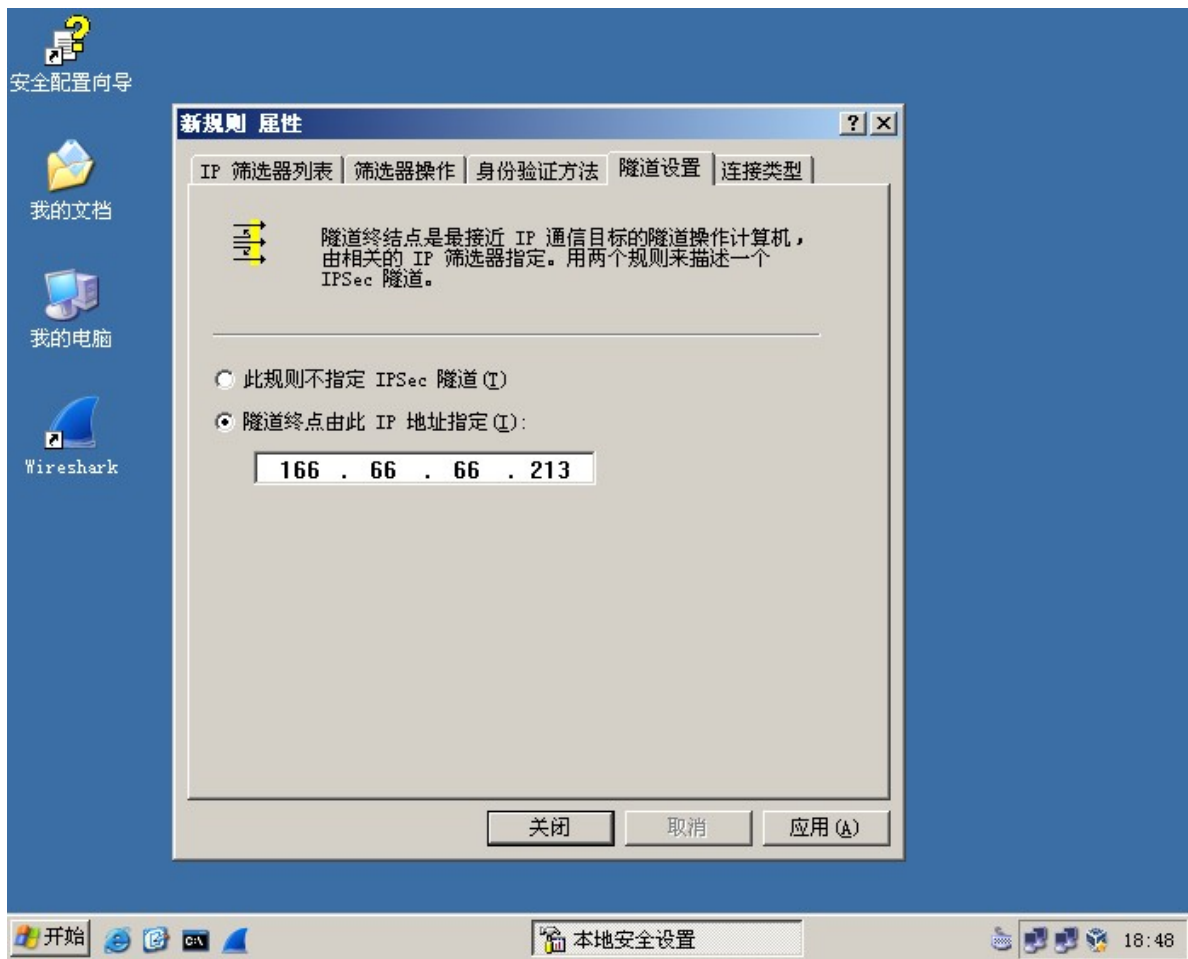


- 身份验证方法,使用预共享密钥: microsoft

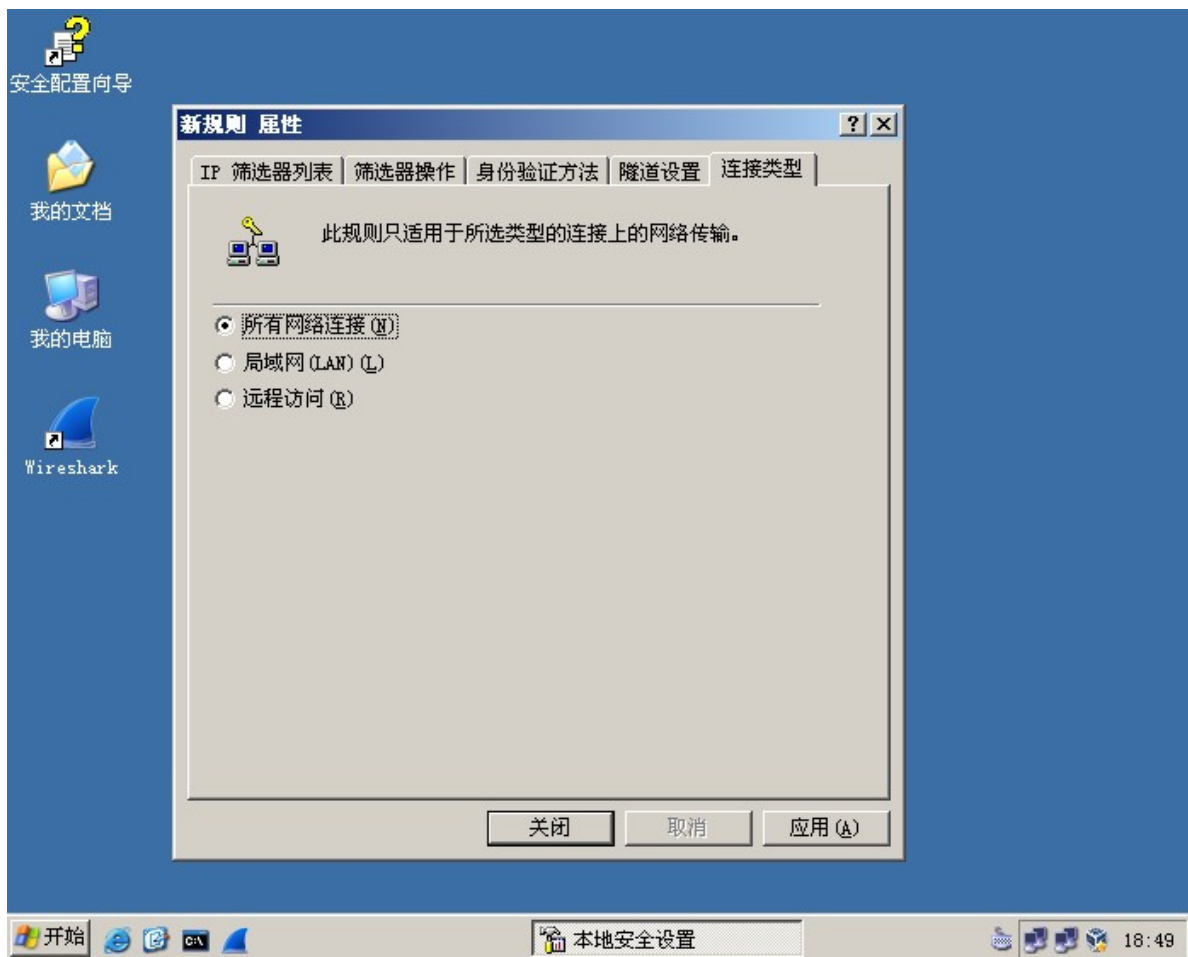




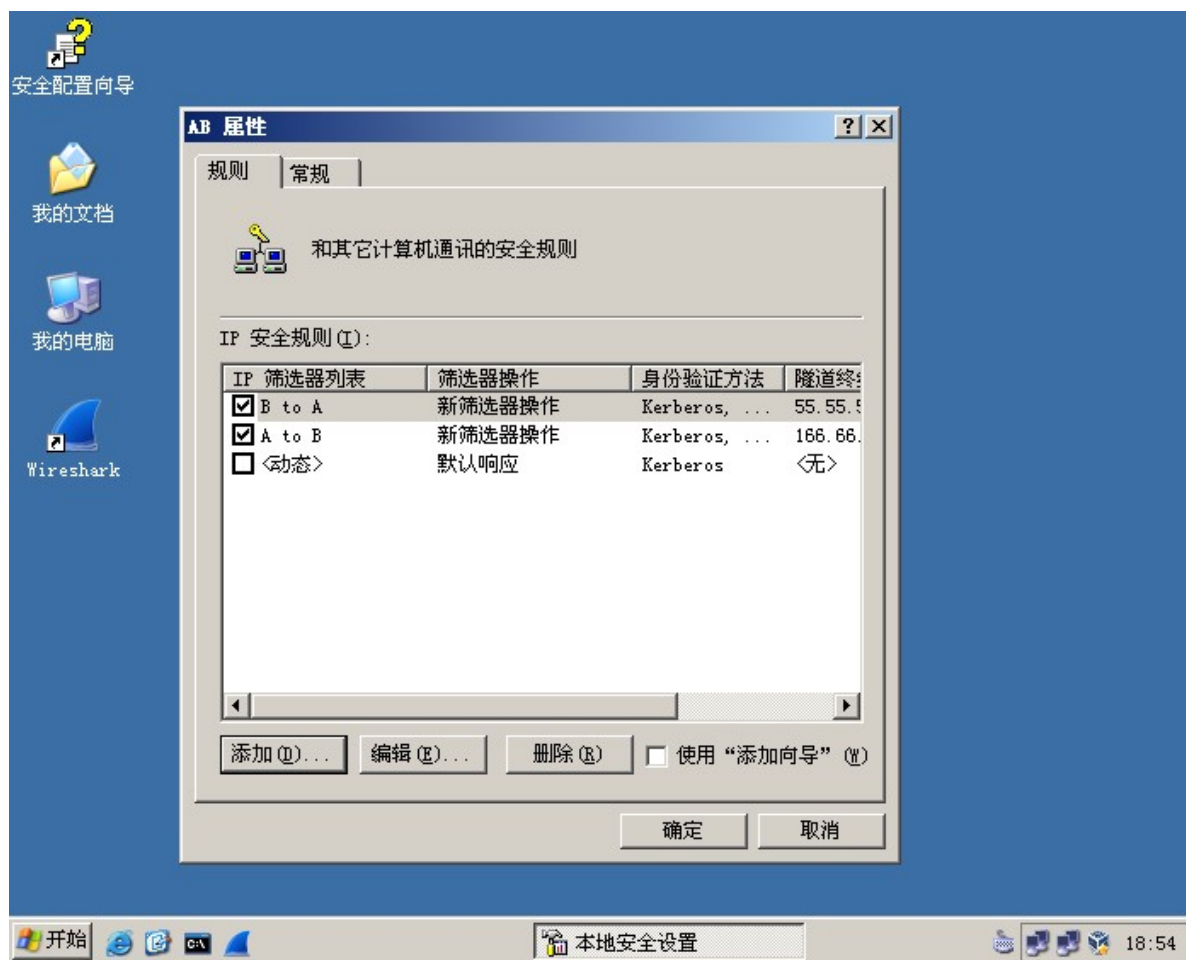
- 隧道设置,指定隧道终点 IP 地址(Server B 的外网 IP 地址: 166.66.66.213)



- 连接类型为"所有连接"

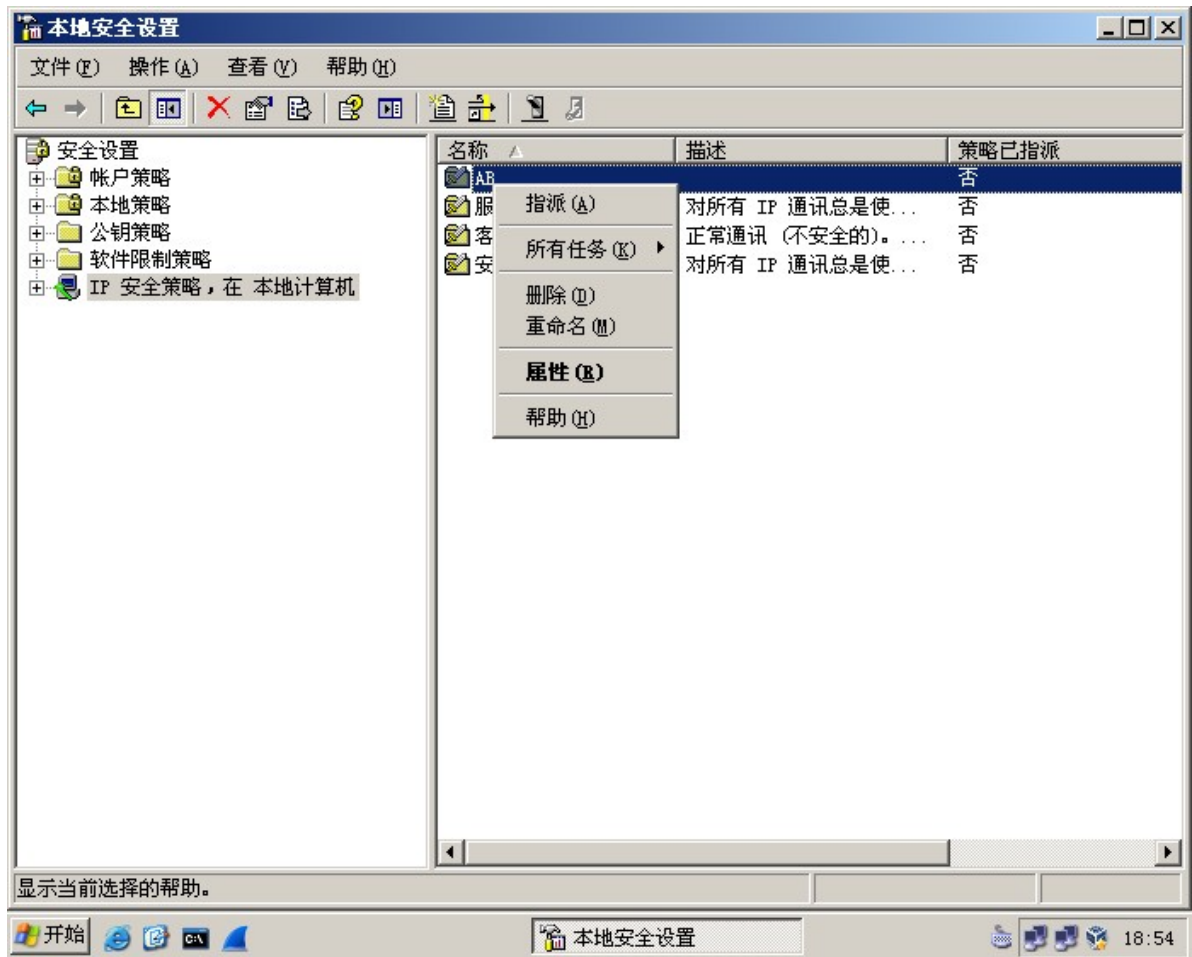


- 重复(2)-(6),创建 IP 筛选器列表"B to A"。设置从 ServerB 到 ServerA 的 IP 策略。将“源子网(IP)”和“目的子网(IP)”互换， 隧道终点设置为 55.55.55.203



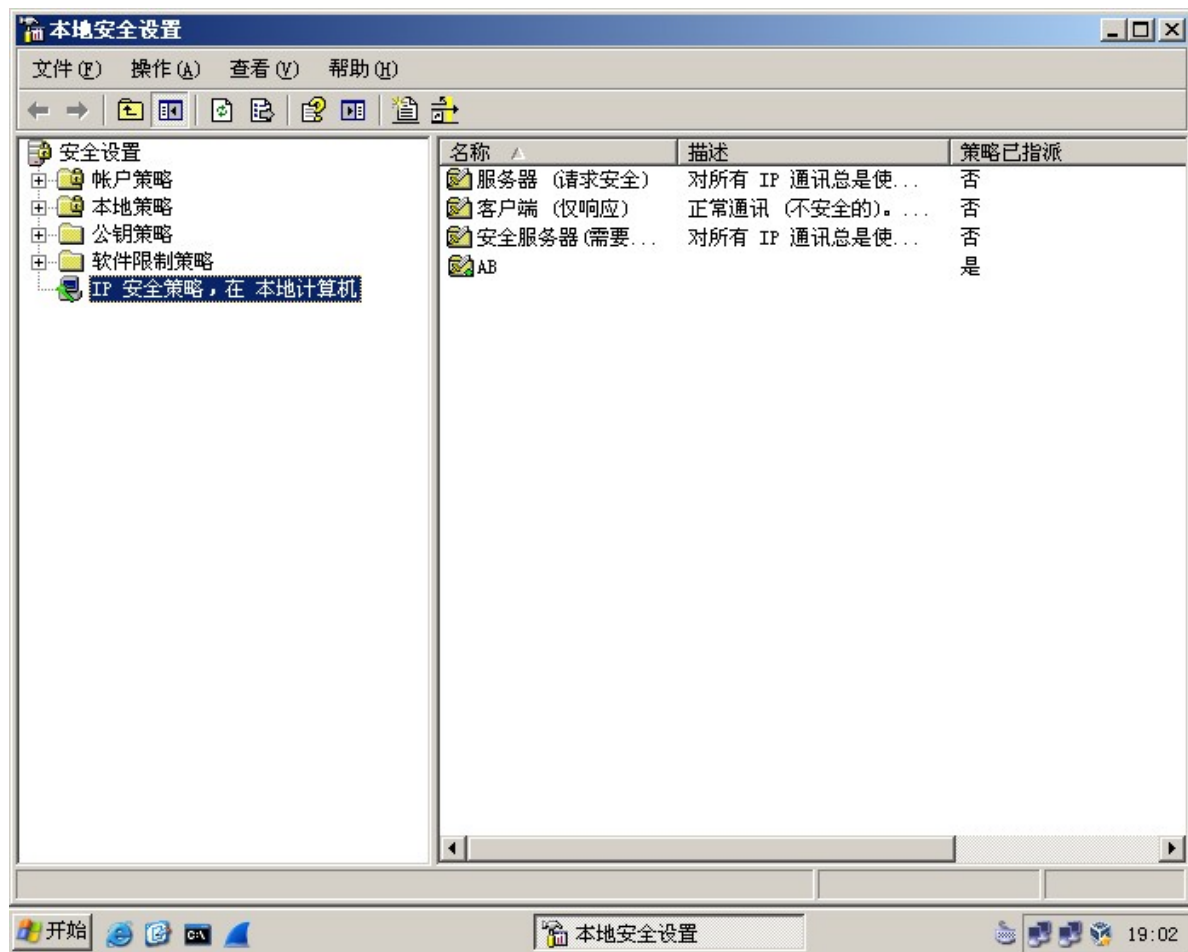
- 在本地安全设置中,右击策略"AB"—指派





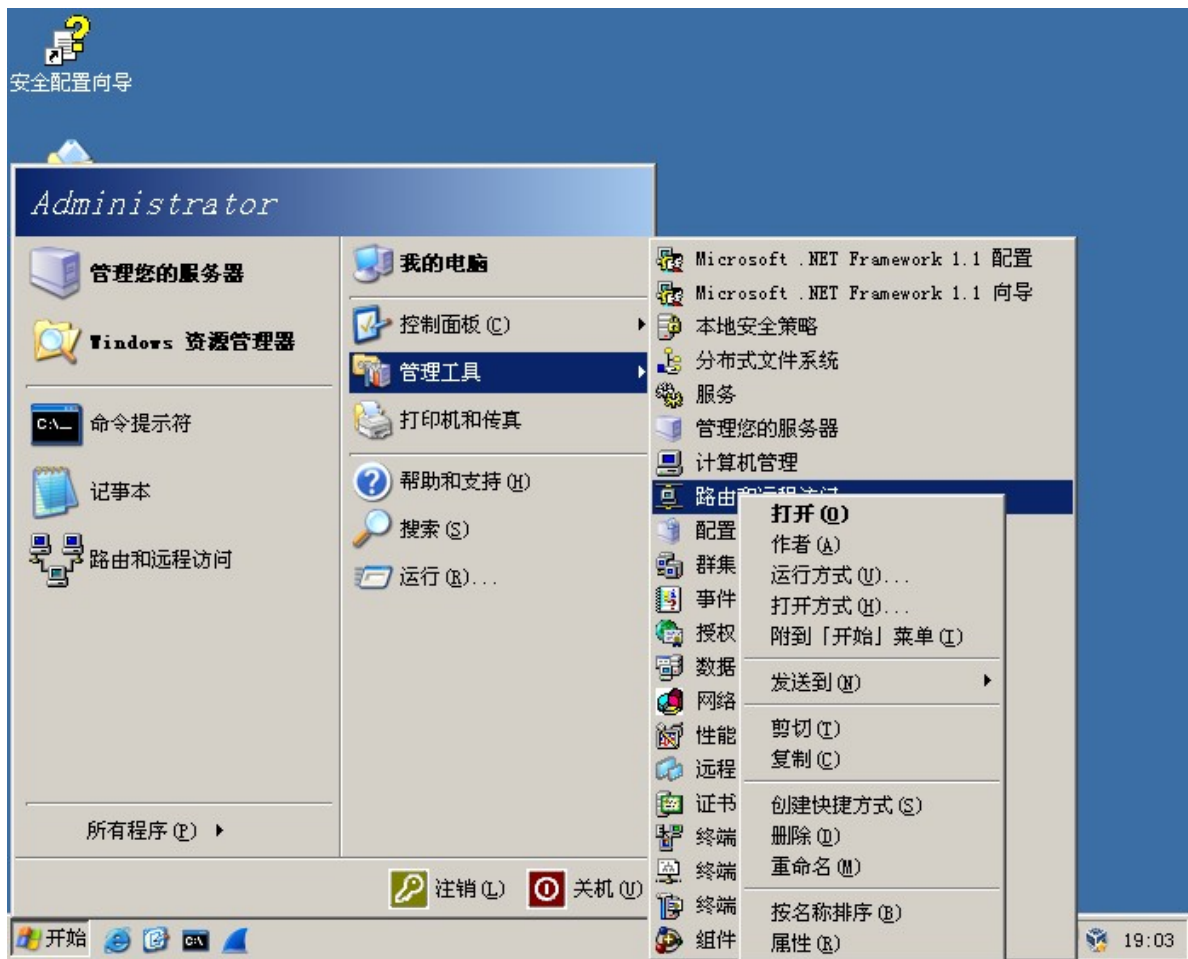
## 3.2 创建 ServerB 的 IPsec 策略

按相同的方法步骤，创建 ServerB 的 IP 安全策略并指派。

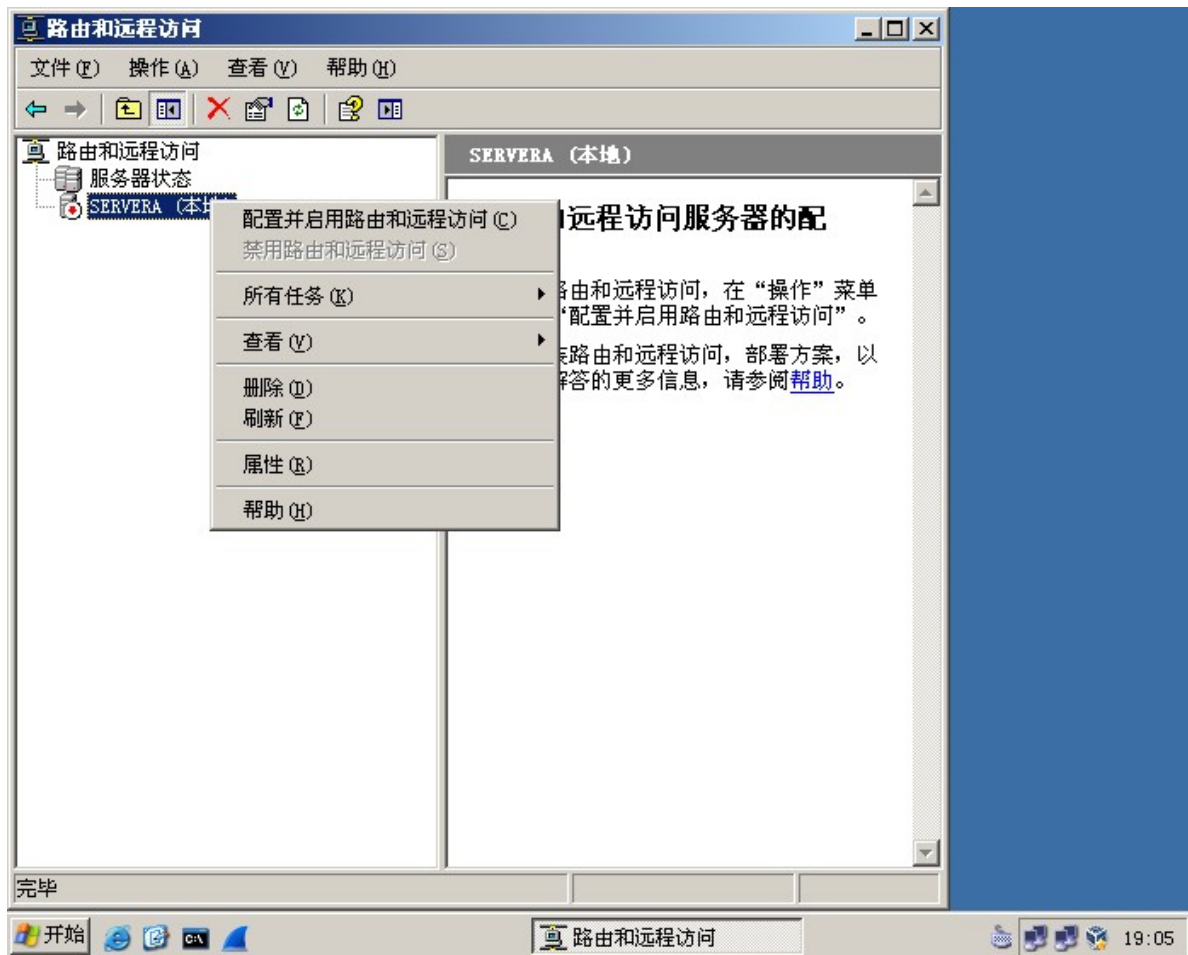


### 3.3 配置远程访问/VPN 服务器

- 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。

### 3.4 ping 测试(Client A)

在 Client A 的 cmd 中输入 >ping 10.0.0.149，或者在 Client B 的 cmd 中输入 >ping 192.168.86.149。如果双方的 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。

```
C:\>命令提示符

C:\work>ping 10.0.0.149

Pinging 10.0.0.149 with 32 bytes of data:

Reply from 10.0.0.149: bytes=32 time<1ms TTL=128
Reply from 10.0.0.149: bytes=32 time<1ms TTL=128
Reply from 10.0.0.149: bytes=32 time<1ms TTL=128
Reply from 10.0.0.149: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\work>_
```