

# 第4章

## 虚拟专用网络 (VPN) 技术配置实例

### Windows Server 2012的VPN

中国科学技术大学

曾凡平

billzeng@ustc.edu.cn

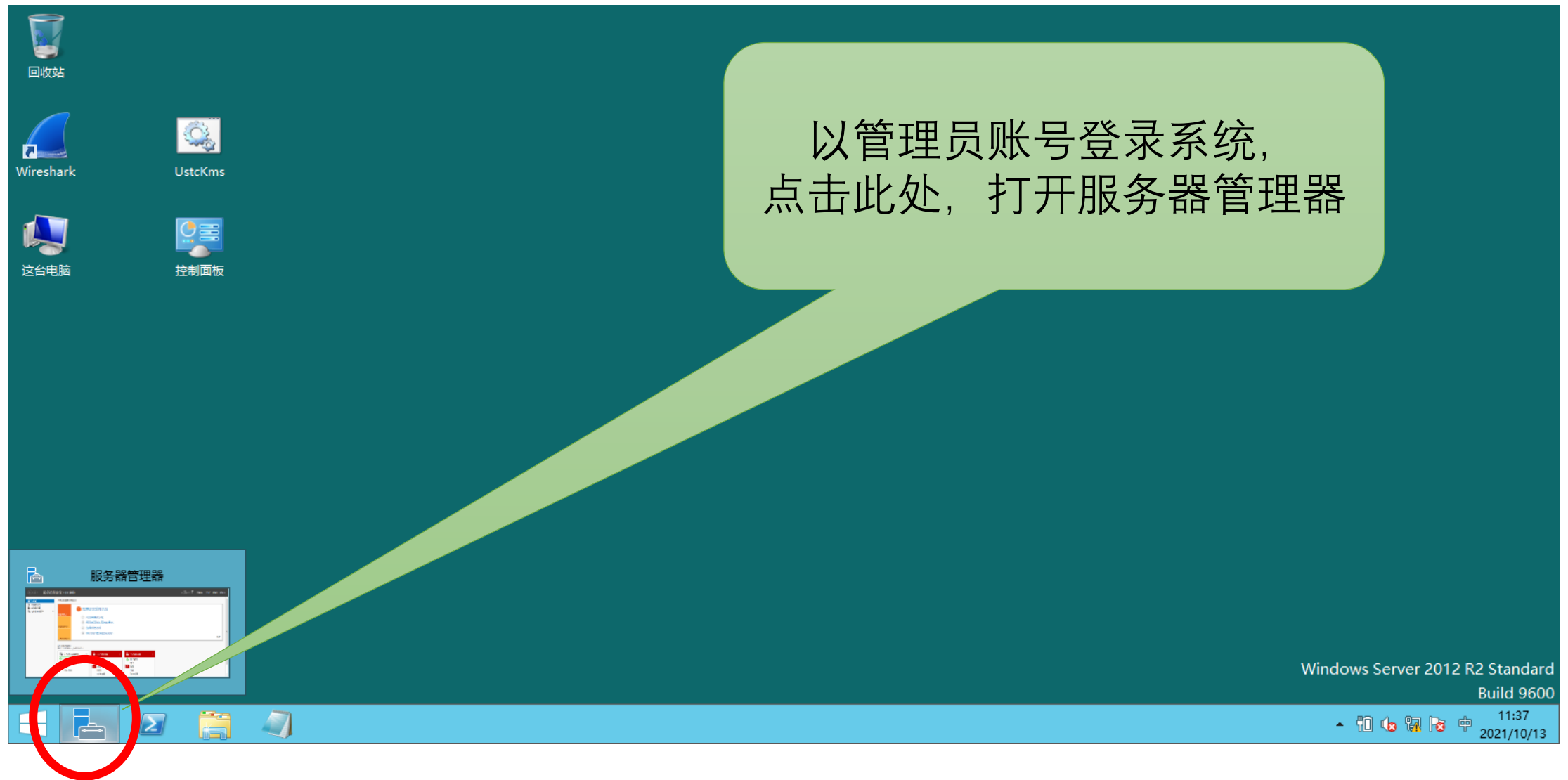
# New: Windows Server 2012及后续版本对VPN的支持

- Windows Server 2003的后续版本对VPN提供了支持，**配置方式是相似的。**

## VPN配置实例

### Windows Server 2012的VPN

# Windows Server 2012的PPTP VPN



服务器管理器

服务器管理器 · 仪表板

管理(M) 工具(T) 视图(V) 帮助(H)

仪表板

- 本地服务器
- 所有服务器
- 文件和存储服务

欢迎使用服务器管理器

快速启动(Q)

新增功能(W)

了解详细信息(L)

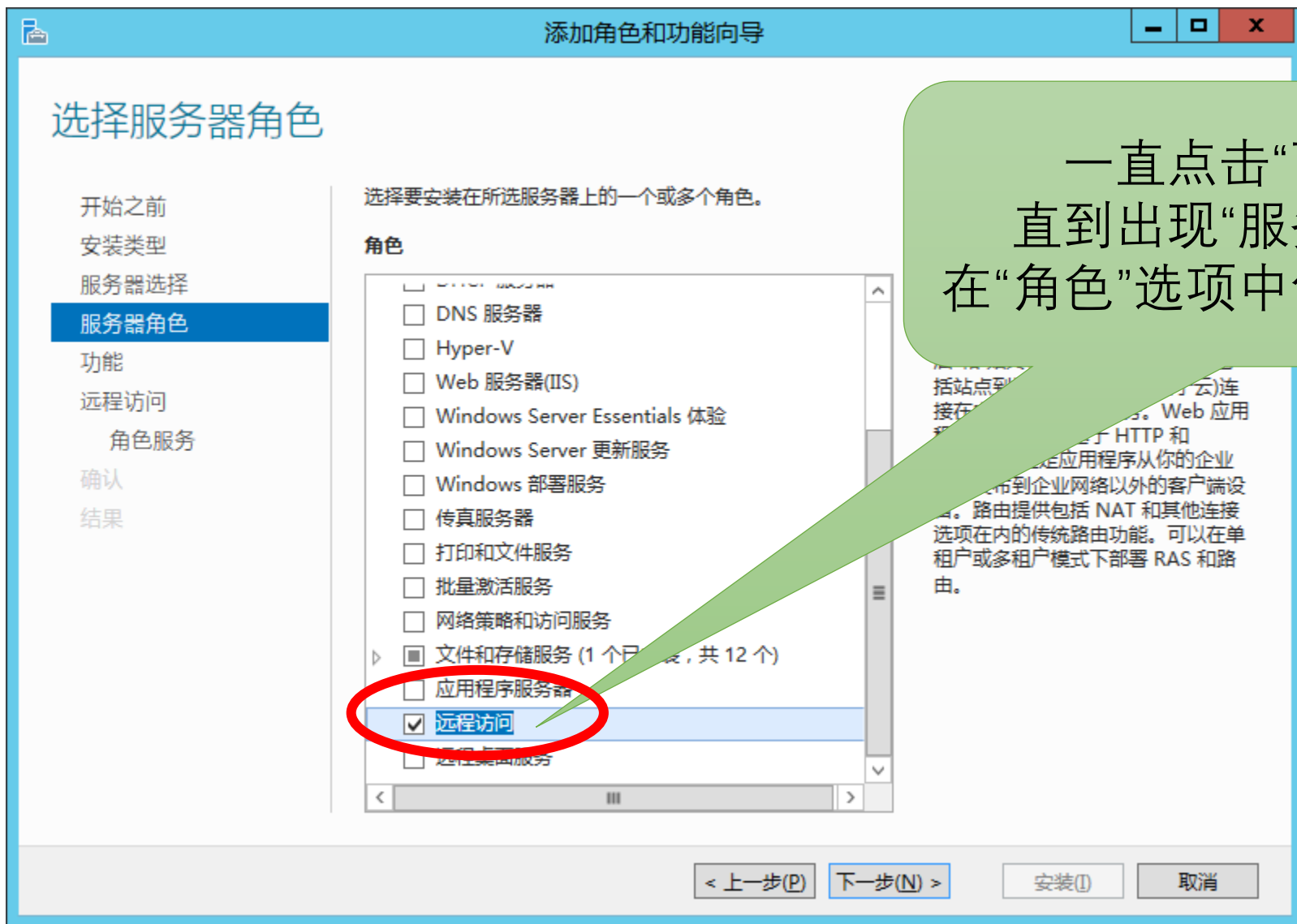
- 1 配置此本地服务器
- 2 添加角色和功能
- 3 添加要管理的其他服务器
- 4 创建服务器组
- 5 将此服务器连接到云服务

角色和服务组

角色: 1 | 服务器组: 1 | 服务器总数: 1

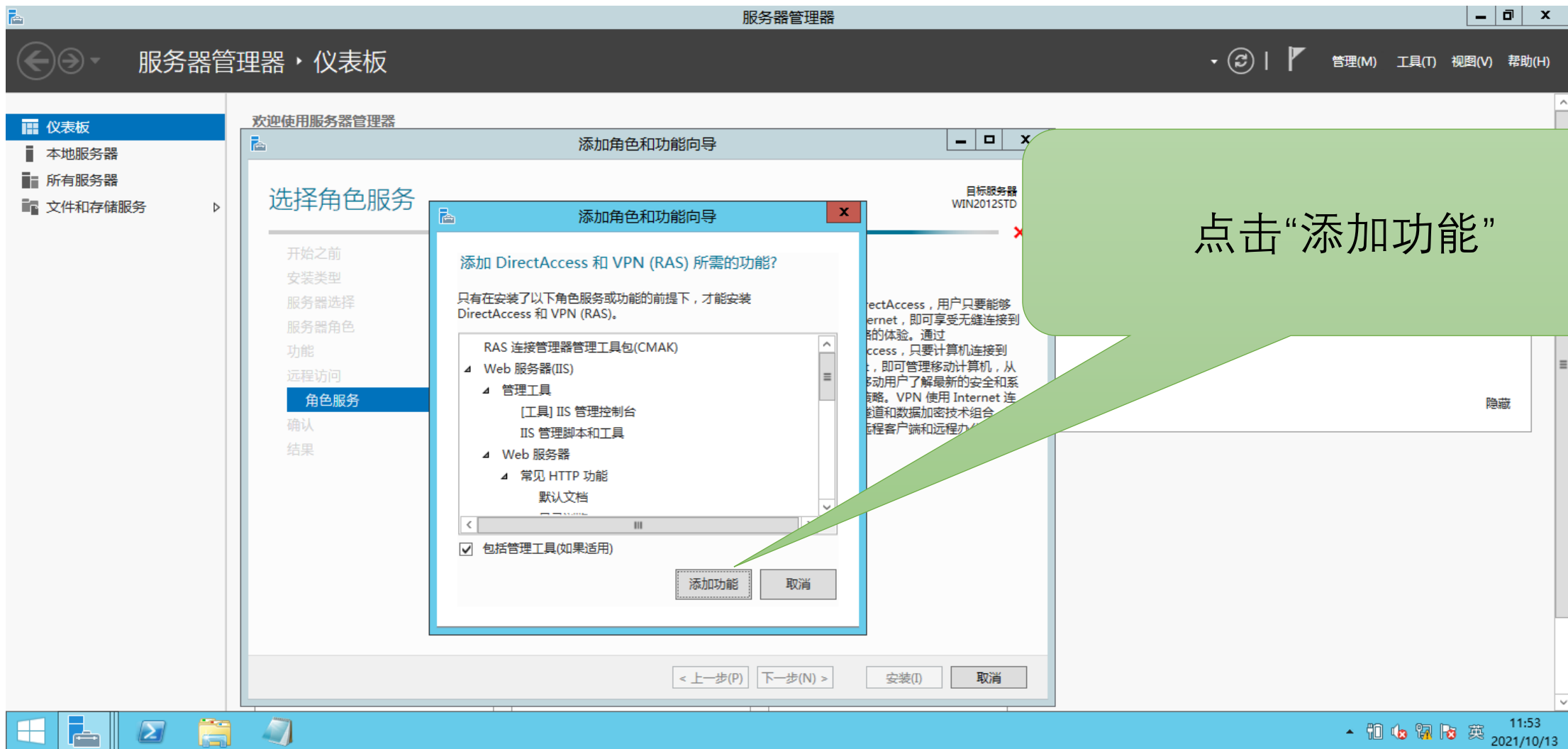
文件和存储服务	本地服务器	所有服务器
1	1	1
可管理性	可管理性	可管理性
事件	事件	事件
性能	3 服务	3 服务
BPA 结果	性能	性能
	BPA 结果	BPA 结果

点击此处，  
添加角色和功能





继续点击“下一步”，  
直到出现“角色服务”，  
勾选“DirectAccess和VPN(RAS)”





继续点击“下一步”，  
直到出现“确认”，  
然后点击“安装”





等待，直到“安装成功”  
然后点击“关闭”

# 远程访问“角色和功能”安装成功之后的配置



打开“控制面板-网络和Internet-网络连接”，找到与路由器相连的网卡。  
然后点击“更改此连接的设置”

Internet 协议版本 4 (TCP/IPv4) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址(O)

☒ 使用下面的 IP 地址(S)

IP 地址(I): 166 . 66 . 66 . 213

子网掩码(U): 255 . 255 . 0 . 0

默认网关(D): 166 . 66 . 66 . 233

☐ 自动获得 DNS 服务器地址(B)

☒ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): . . .

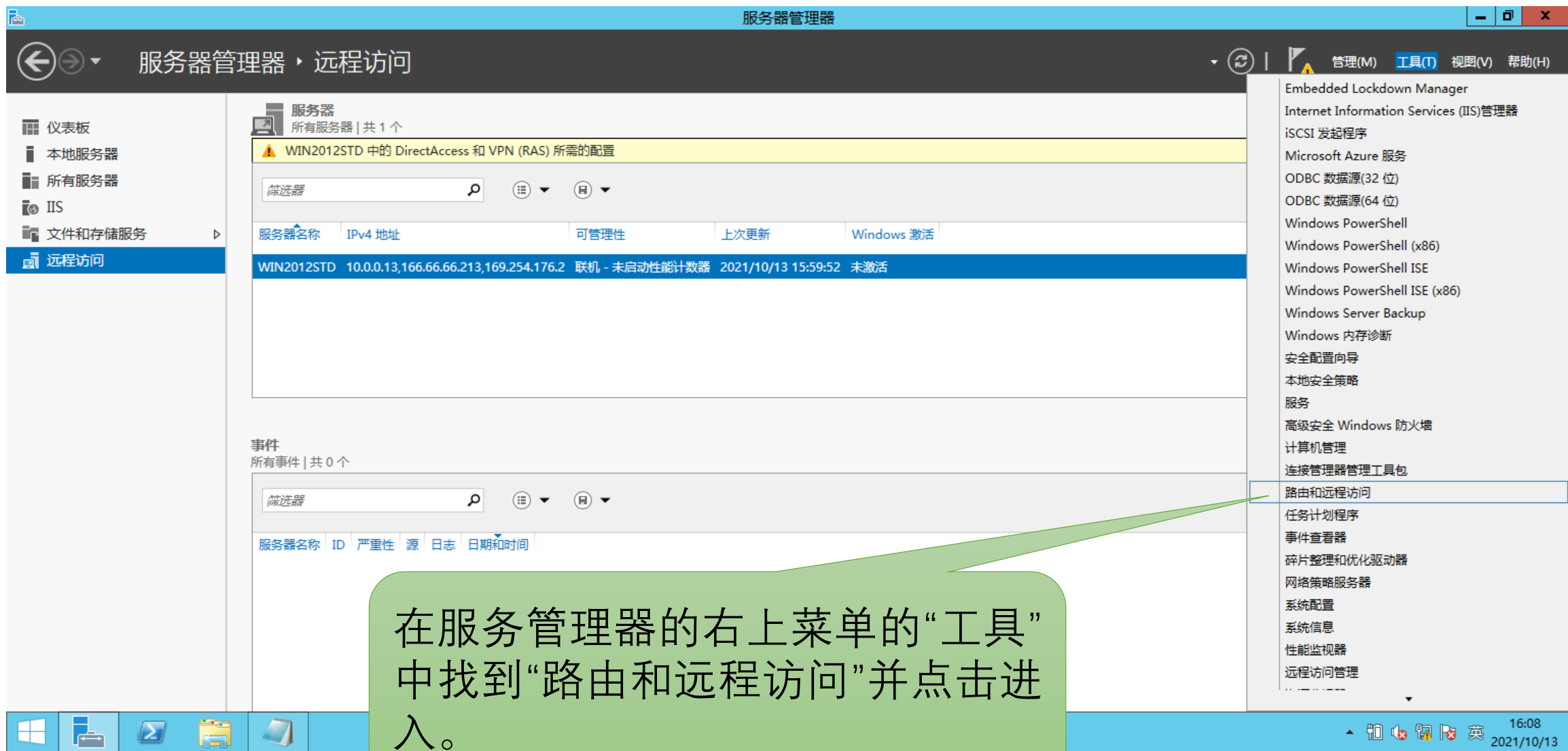
备用 DNS 服务器(A): . . .

☐ 退出时验证设置(L)

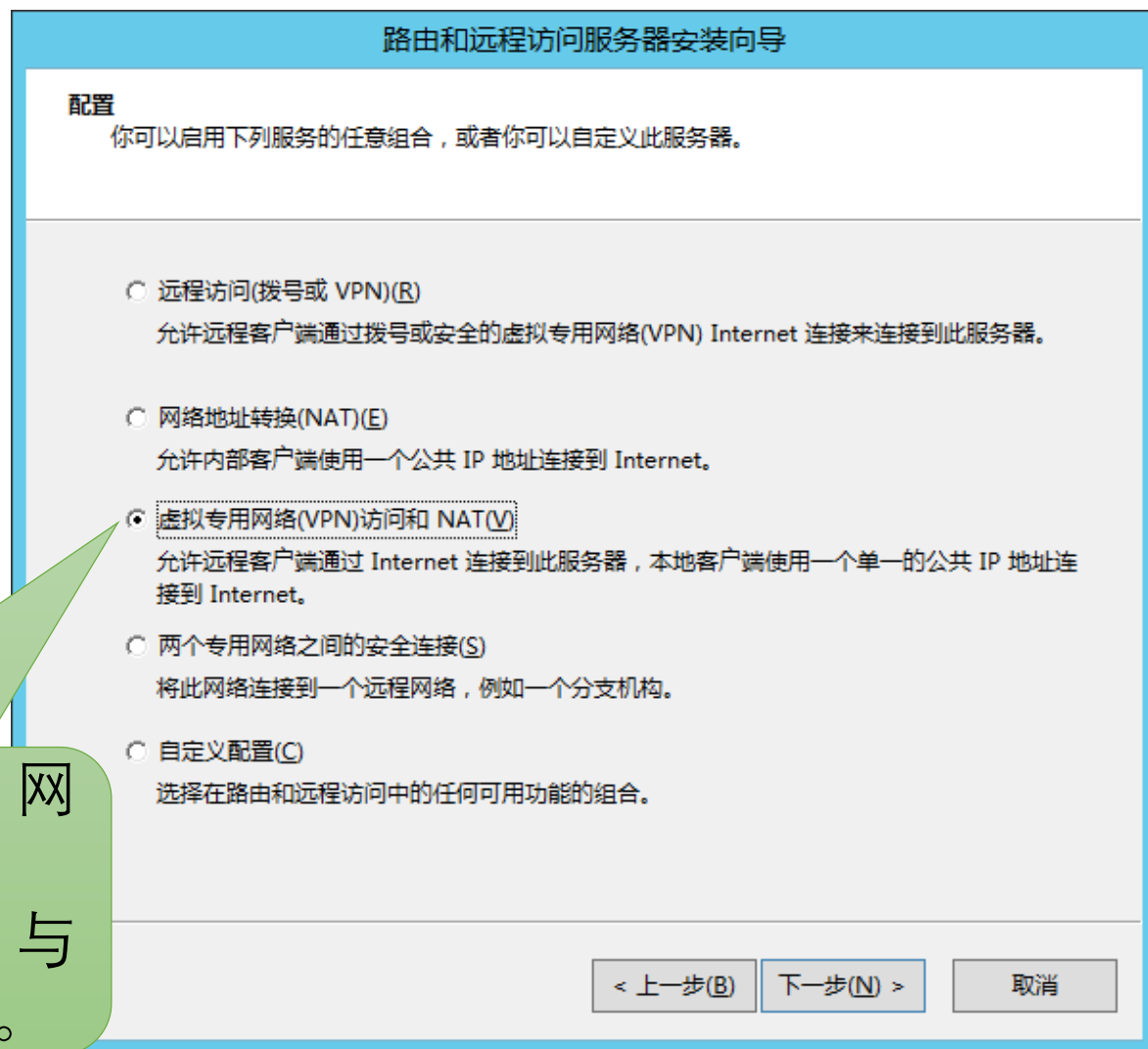
高级(V)...

确定 取消

正确设置IP地址和默认网关的IP地址。



# 路由和远程访问的配置：同Windows 2003



在此选择“虚拟专用网(VPN)访问和NAT”；其他的配置方法与Windows2003完全一样。

# VPN用户的设置：同Windows 2003

计算机管理

名称	全名	描述	操作
Administrat...		管理计算机(域)的内置帐户	用户
Guest		供来宾访问计算机或访问域的内...	更多操作
vpn	vpn		vpn
			更多操作

vpn 属性

常规 隶属于 配置文件 环境 会话

远程控制 远程桌面服务配置文件 拨入

网络访问权限

- ☒ 允许访问(W)
- ☐ 拒绝访问(D)
- ☐ 通过 NPS 网络策略控制访问(P)

☐ 验证呼叫方 ID(Y):

回调选项

- ☒ 不回调(C)
- ☐ 由呼叫方设置(仅路由和远程访问服务)(S)
- ☐ 总是回拨到(Y):

☐ 分配静态 IP 地址(I)

定义要为此拨入连接启用的 IP 地址。 静态 IP 地址(I)...

☐ 应用静态路由(R)

为此拨入连接定义要启用的路由。 静态路由(R)...

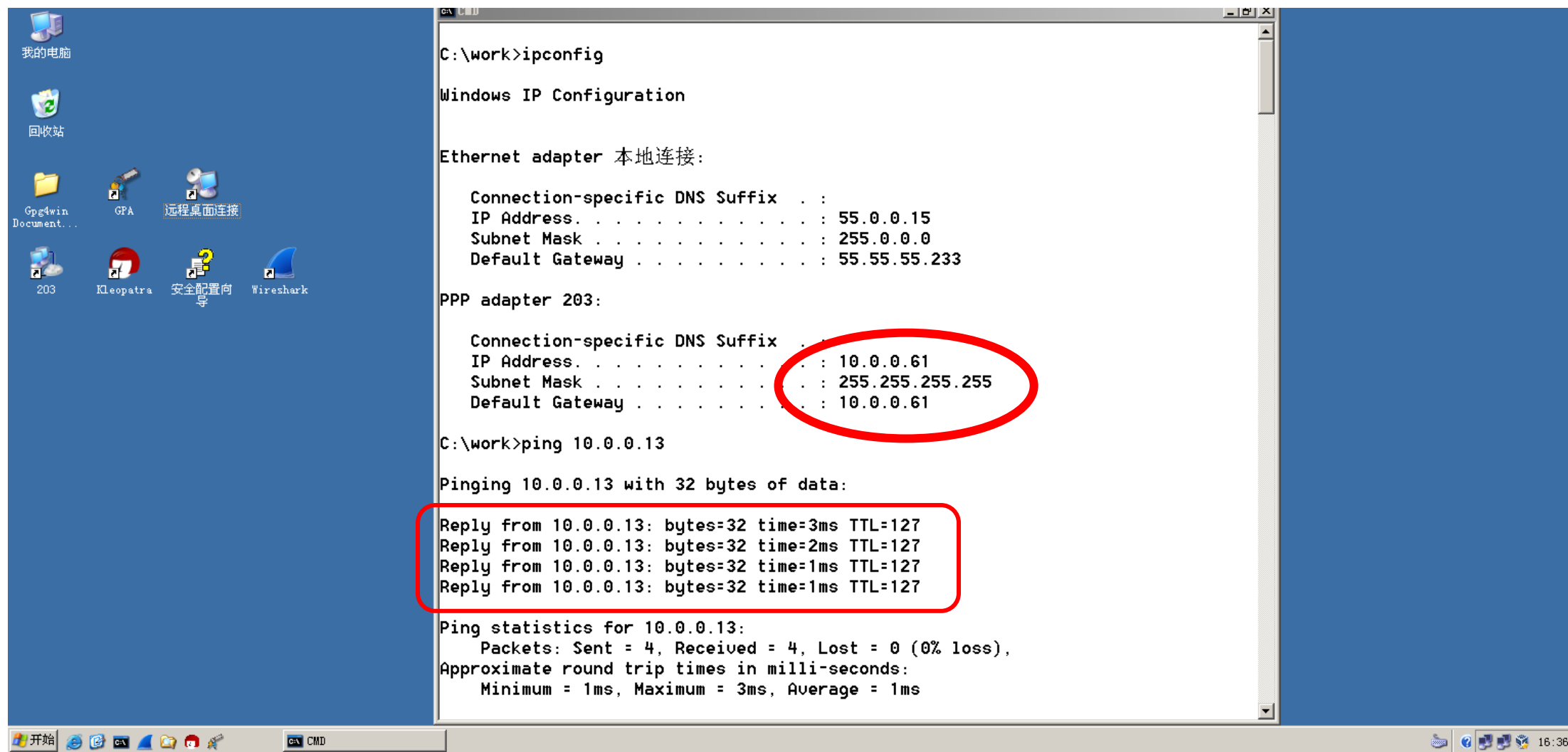
确定 取消 应用(A) 帮助

er 2012 R2 Standard  
Build 9600

16:32  
2021/10/13

设置用户vpn的“拨入”属性为“允许访问”

# 远程客户端的VPN拨入



# 在路由器上用wireshark观察到的现象

The image shows a Wireshark 1.10.6 window titled "Capturing from VMnet6 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]". The interface includes a menu bar, a toolbar, a filter bar, and a packet list pane. The packet list pane displays 17 captured packets. The selected packet (No. 1) is expanded in the packet details pane, showing the following structure:

- Frame 1: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0
- Ethernet II, Src: CadmusCo\_36:72:8a (08:00:27:36:72:8a), Dst: CadmusCo\_5c:15:1b (08:00:27:5c:15:1b)
- Internet Protocol Version 4, Src: 55.0.0.15 (55.0.0.15), Dst: 166.66.66.213 (166.66.66.213)
- Generic Routing Encapsulation (PPP)
- Point-to-Point Protocol
- PPP Compressed Datagram

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates "Packets: 17 · Displayed: 17 (100.0%)" and "Profile: Default".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	55.0.0.15	166.66.66.213	PPP Com	111	Compressed data
2	0.00073900	166.66.66.213	55.0.0.15	PPP Com	115	Compressed data
3	0.09445300	55.0.0.15	166.66.66.213	GRE	60	Encapsulated PPP
4	1.02095600	55.0.0.15	166.66.66.213	PPP Com	111	Compressed data
5	1.02141500	166.66.66.213	55.0.0.15	PPP Com	115	Compressed data
6	1.11539200	55.0.0.15	166.66.66.213	GRE	60	Encapsulated PPP
7	1.99688700	55.0.0.15	166.66.66.213	PPP Com	111	Compressed data
8	1.99766900	166.66.66.213	55.0.0.15	PPP Com	115	Compressed data
9	2.09734200	55.0.0.15	166.66.66.213	GRE	60	Encapsulated PPP
10	2.99886300	55.0.0.15	166.66.66.213	PPP Com	111	Compressed data
11	2.99976900	166.66.66.213	55.0.0.15	PPP Com	115	Compressed data
12	3.09774400	55.0.0.15	166.66.66.213	GRE	60	Encapsulated PPP
13	4.73014400	CadmusCo_5c:15:1b	CadmusCo_36:72:8a	ARP	60	who has 166.66.66.233? Tell 166.66.66.213
14	4.73019400	CadmusCo_36:72:8a	CadmusCo_5c:15:1b	ARP	42	166.66.66.233 is at 08:00:27:36:72:8a
15	7.77730300	166.66.66.213	55.0.0.15	PPTP	70	Echo-Request
16	7.77812900	55.0.0.15	166.66.66.213	PPTP	74	Echo-Reply
17	7.83926000	166.66.66.213	55.0.0.15	TCP	60	pptp > 1030 [ACK] Seq=17 Ack=21 Win=63664 Len=0

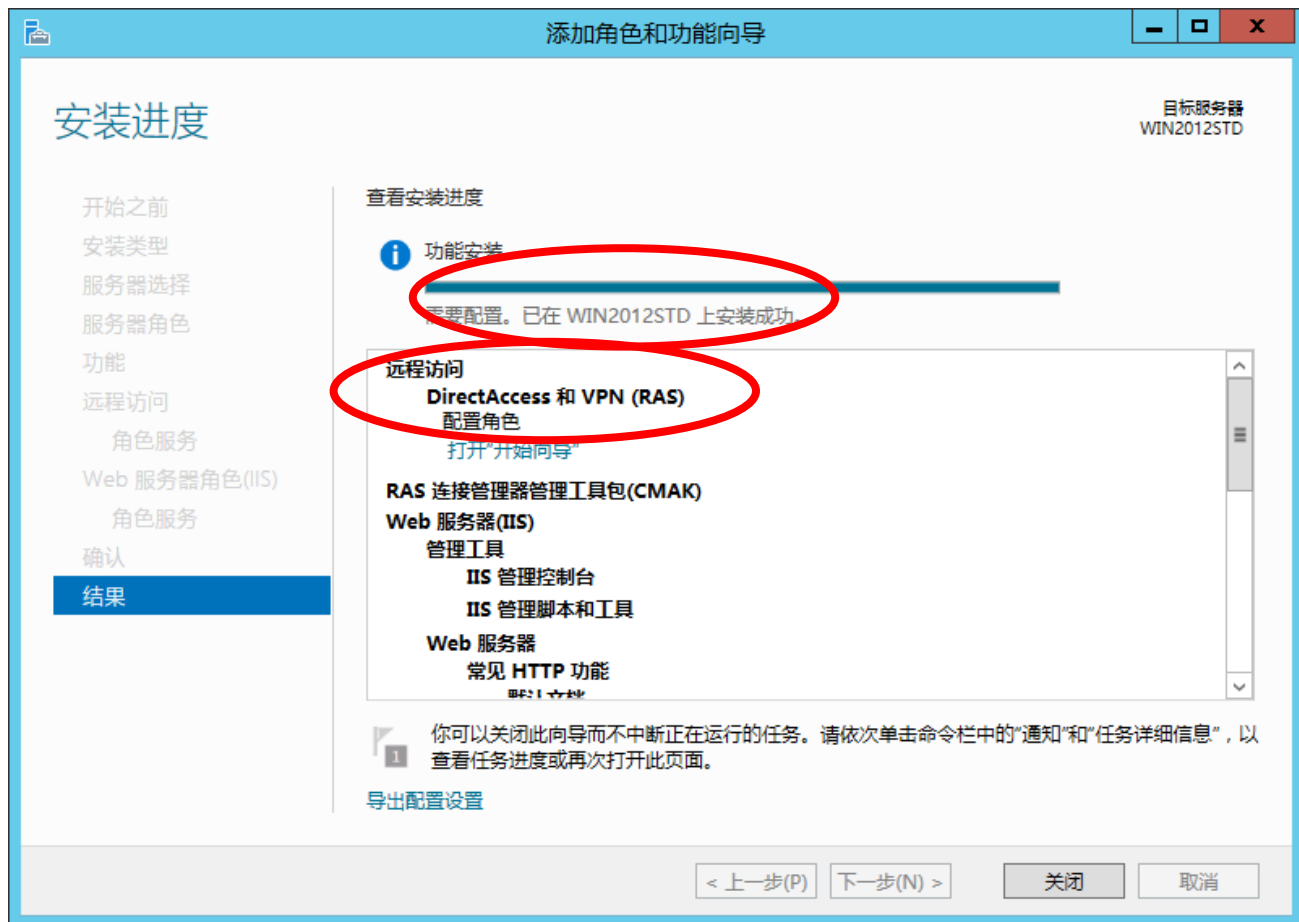


# Windows Server 2012的“网关—网关” VPN

配置方法与Windows 2003的相似

# 在VPN网关上安装“远程访问”角色和功能

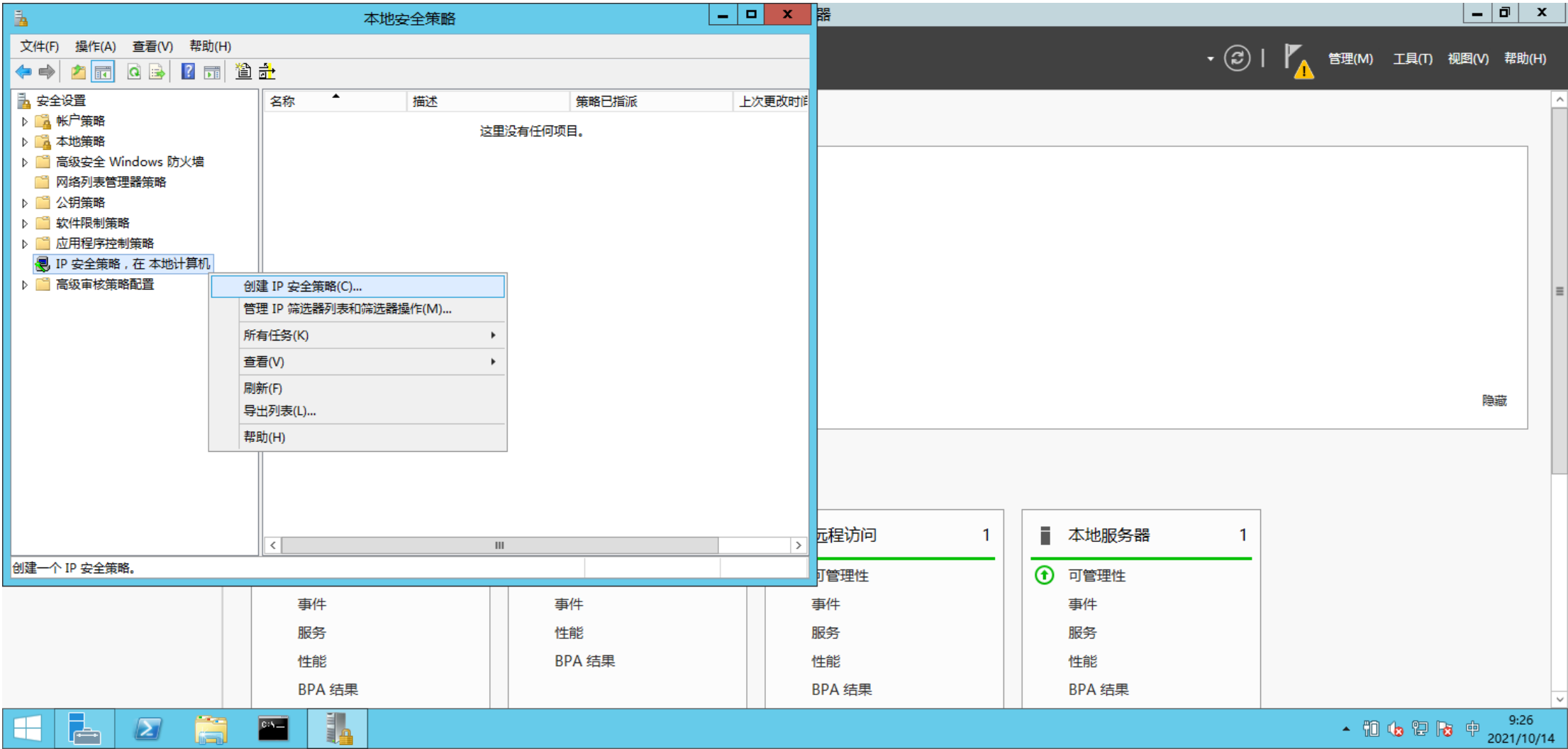
配置方法同Windows 2012的  
远程访问VPN (PPTP VPN)



# 通过“服务管理器”-“工具”选择“本地安全策略”



# VPN网关上的“IP安全策略”的配置



# IP安全策略向导



IP 安全策略向导

IP 安全策略名称

命名这个 IP 安全策略并且给出一个简短的描述

名称(M):

VPN(网关A和网关B的IPSec)

描述(D):

网关A(55.55.55.203)——网关B(166.66.66.213)VPN的B端：  
C类网(192.168.86.0/24)和B类网(172.16.0.0/20)的IPSec链接

< 上一步(B)

下一步(N) >

取消

IP 安全策略向导

安全通讯请求

指定这个策略如何对安全通讯的请求作出响应。

默认响应规则在没有其他规则适用时，对请求安全的远程计算机作出响应。为了安全地通讯，计算机必须对安全通讯请求做出响应。

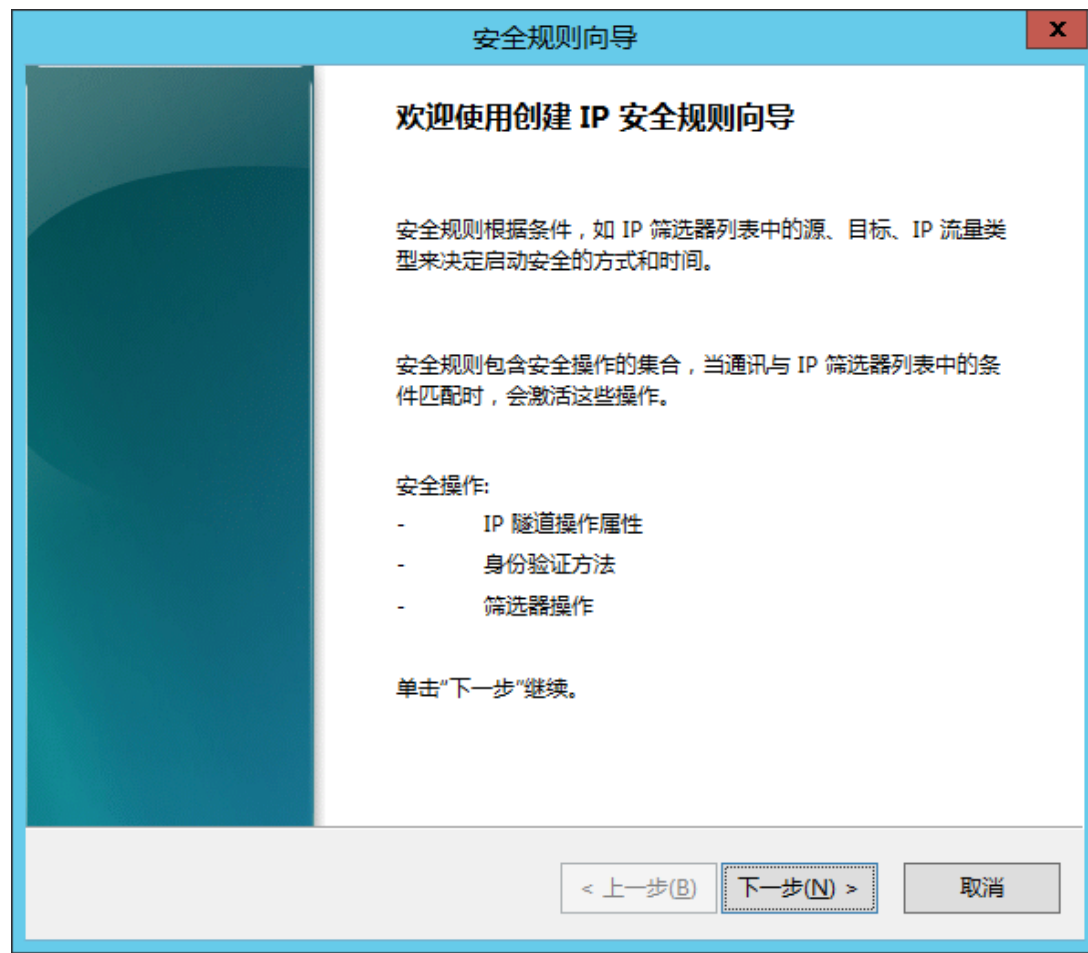
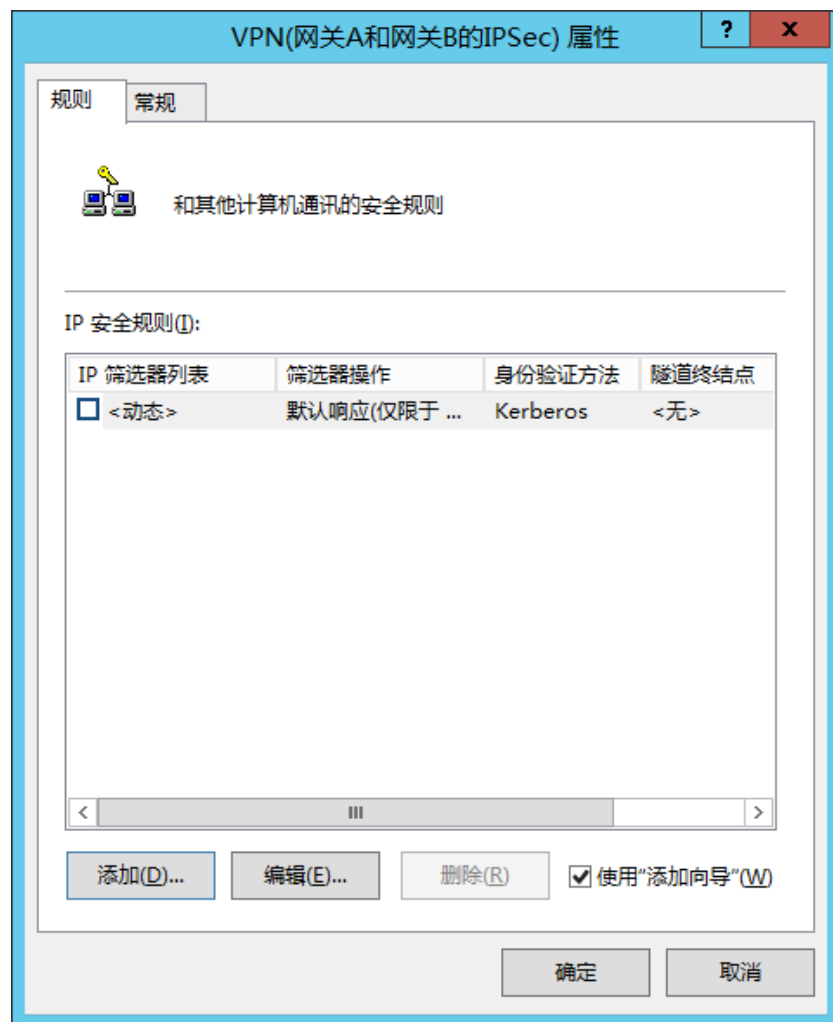
注意: 仅在运行 Windows 2003 和 Windows XP 的计算机上支持默认响应规则。

☐ 激活默认响应规则(仅限于 Windows 的早期版本)(R)。

< 上一步(B)

下一步(N) >

取消



安全规则向导

隧道终点

隧道终点是最接近 IP 流量目标的隧道操作计算机，正如安全规则的 IP 筛选器列表所指定的。

IPsec 隧道允许数据包在两台计算机间以直接的专用连接的安全级别通过公用或专用网络。

指定 IP 安全规则的隧道终点:

☐ 此规则不指定隧道(T)

☒ 隧道终点由下列 IP 地址指定(I):

IPv4 隧道终点:

IPv6 隧道终点:

< 上一步(B)

下一步(N) >

取消

安全规则向导

网络类型

安全规则必须应用到一种网络类型。

选择网络类型:

☒ 所有网络连接(C)

☐ 局域网(LAN)(L)

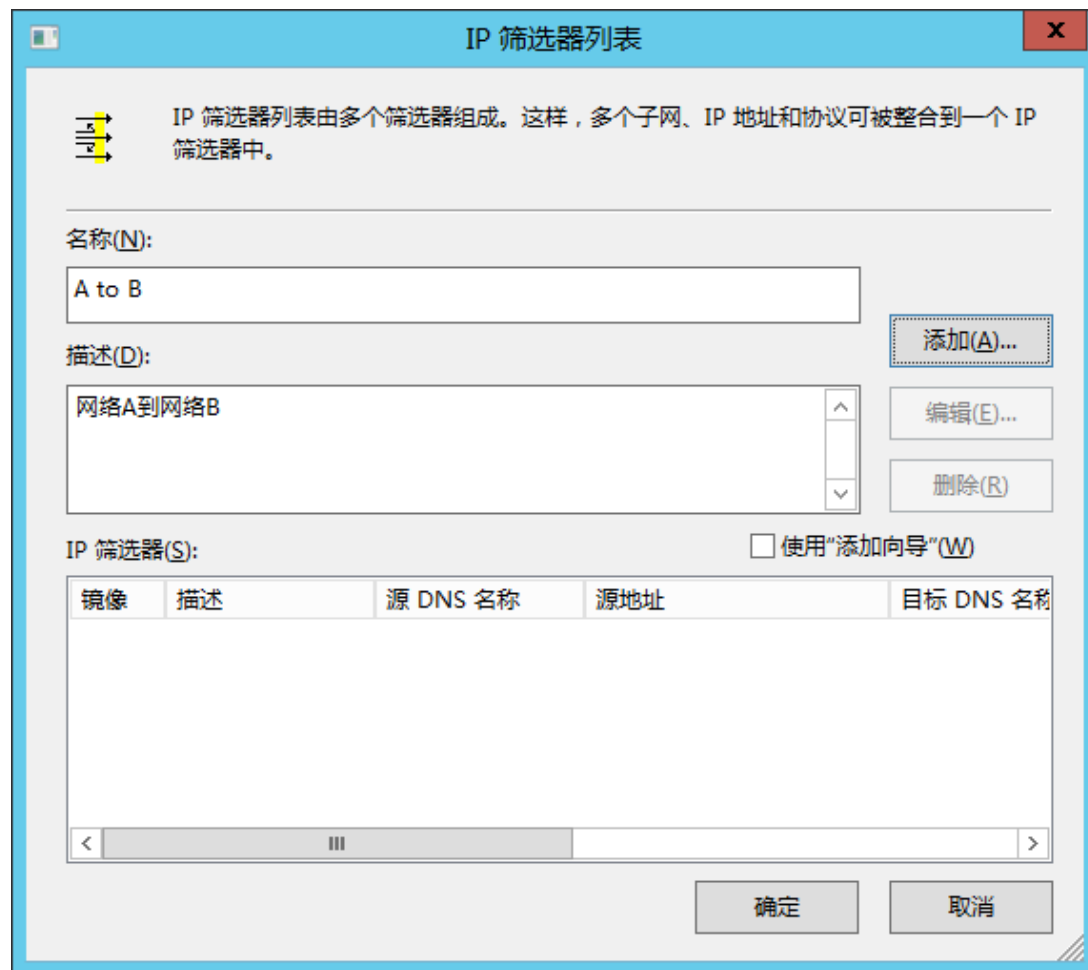
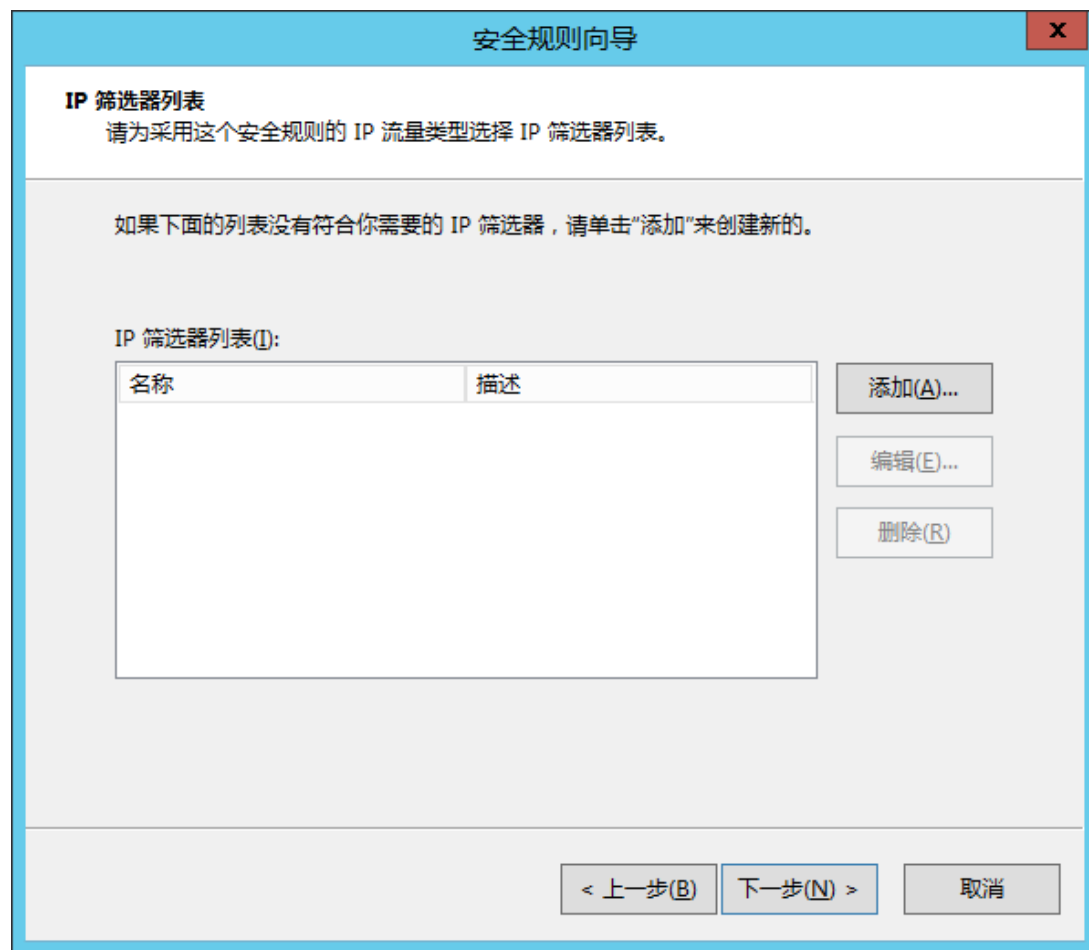
☐ 远程访问(R)

< 上一步(B)

下一步(N) >

取消





IP 筛选器 属性

地址

协议

描述

源地址(S):

一个特定的 IP 地址或子网

IP 地址或子网(I): 192.168.86.0/24

目标地址(D):

一个特定的 IP 地址或子网

IP 地址或子网(R): 10.0.0.0/8

☐ 镜像(O)。与源地址和目标地址正好相反的数据包相匹配。

确定

取消

安全规则向导

IP 筛选器列表

请为采用这个安全规则的 IP 流量类型选择 IP 筛选器列表。

如果下面的列表没有符合你需要的 IP 筛选器，请单击“添加”来创建新的。

IP 筛选器列表(I):

名称	描述
<input checked="" type="radio"/> A to B	网络A到网络B

添加(A)...

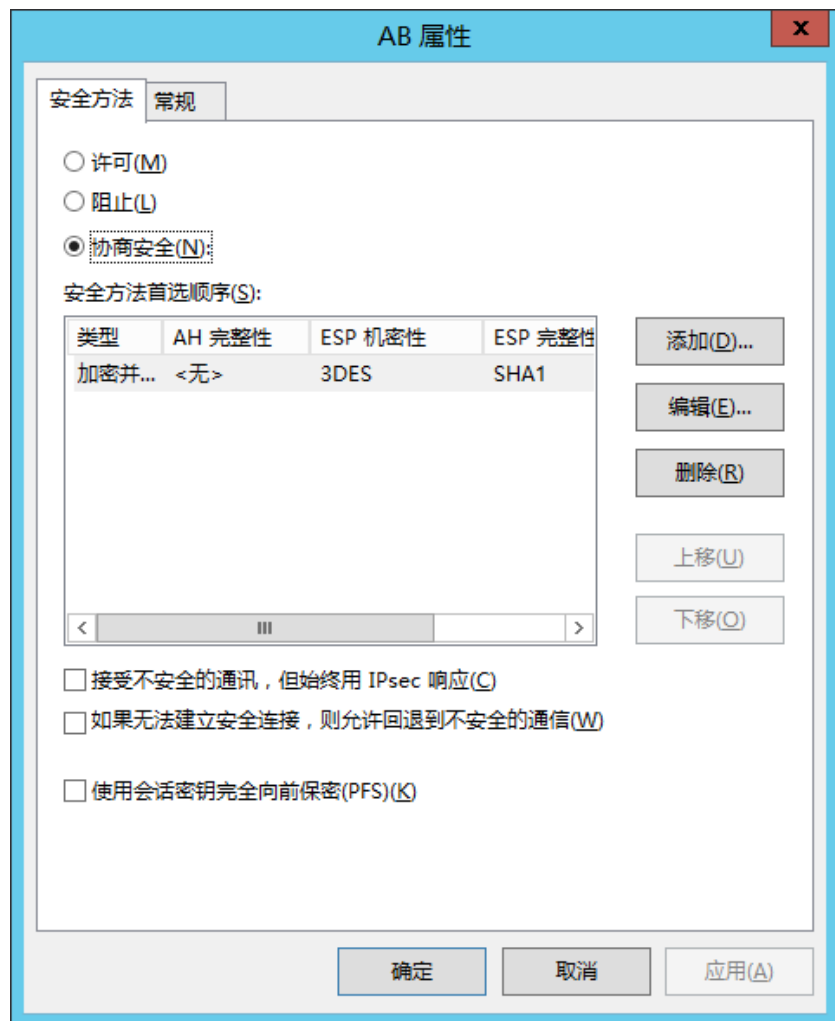
编辑(E)...

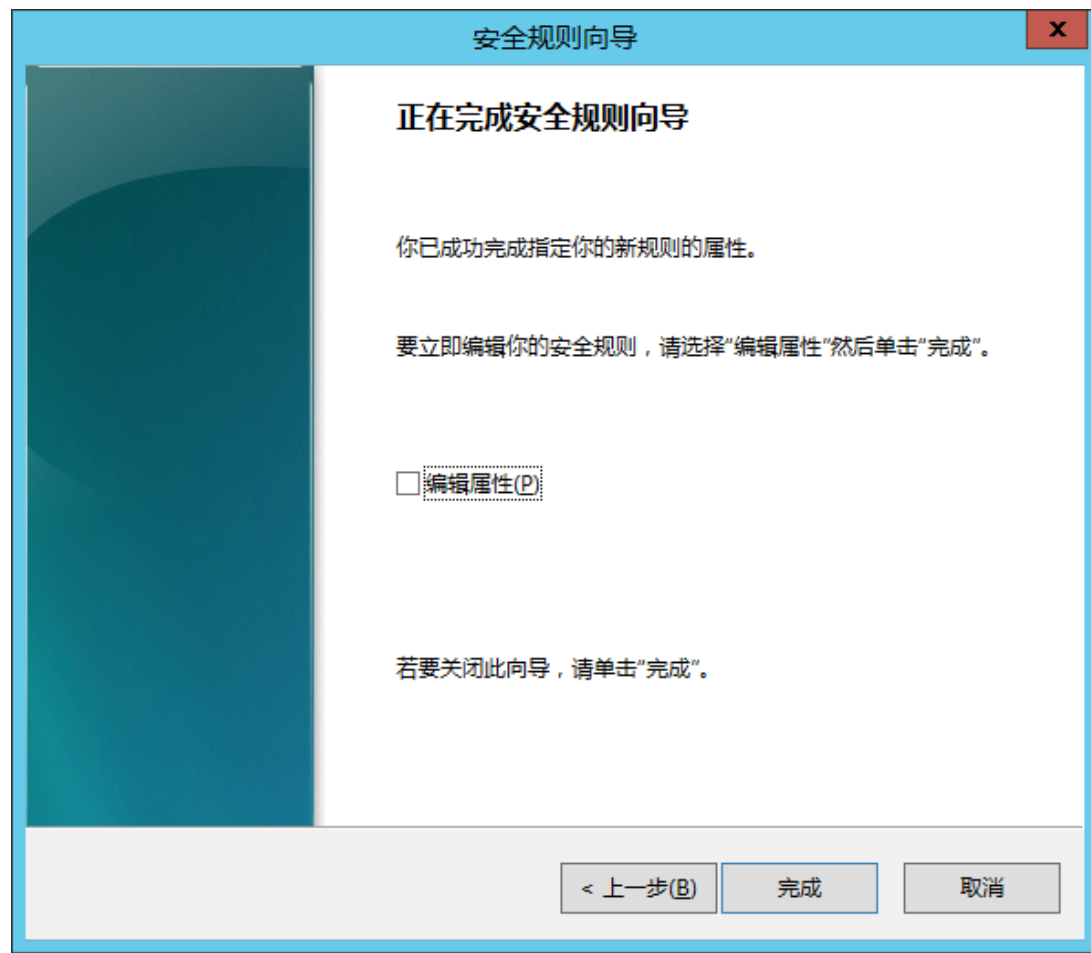
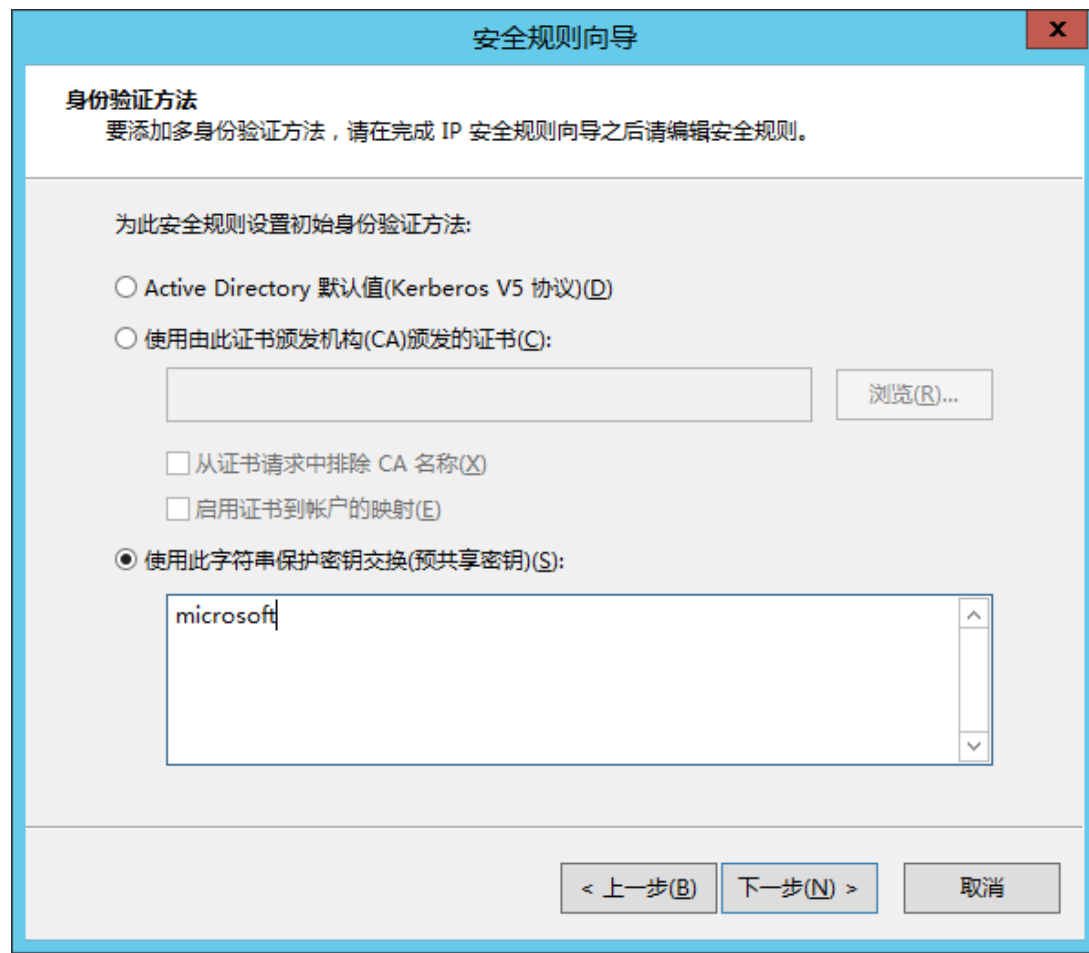
删除(R)

< 上一步(B)

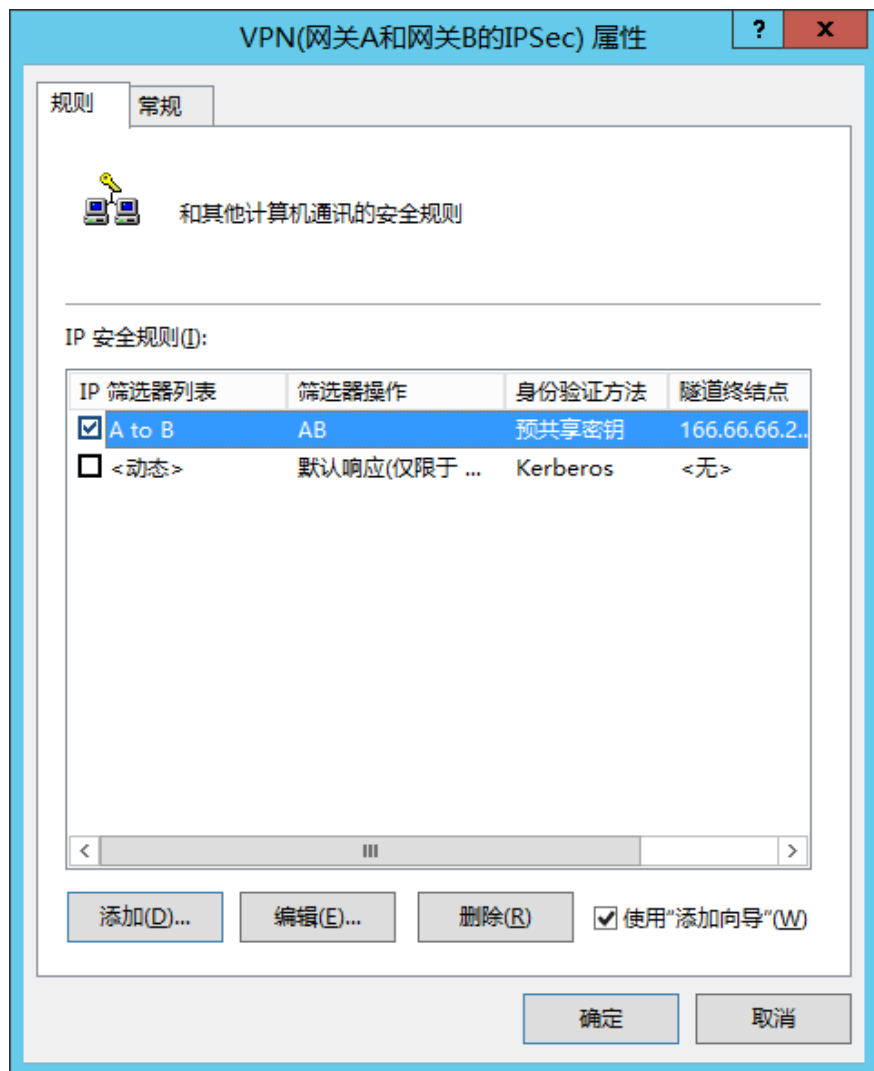
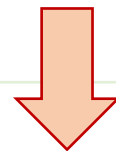
下一步(N) >

取消





# B to A方向的安全规则



安全规则向导

网络类型

安全规则必须应用到一种网络类型。

选择网络类型:

☒ 所有网络连接(C)

☐ 局域网(LAN)(L)


☐ 远程访问(R)

< 上一步(B)

下一步(N) >

取消

IP 筛选器列表

 IP 筛选器列表由多个筛选器组成。这样，多个子网、IP 地址和协议可被整合到一个 IP 筛选器中。

名称(N):  
B to A

描述(D):

添加(A)...

编辑(E)...

删除(R)

IP 筛选器(S): ☐ 使用“添加向导”(W)

镜像	描述	源 DNS 名称	源地址	目标 DNS 名称
----	----	----------	-----	-----------

<

III

>

确定

取消

### IP 筛选器 属性

地址

协议

描述

源地址(S):

一个特定的 IP 地址或子网

IP 地址或子网(I): 10.0.0.0/8

目标地址(D):

一个特定的 IP 地址或子网


IP 地址或子网(R): 192.168.86.0/24

☐ 镜像(O)。与源地址和目标地址正好相反的数据包相匹配。

确定

取消

### IP 筛选器列表

 IP 筛选器列表由多个筛选器组成。这样，多个子网、IP 地址和协议可被整合到一个 IP 筛选器中。

名称(N):

B to A

添加(A)...

描述(D):

网络B到网络A

编辑(E)...

删除(R)

IP 筛选器(S): ☐ 使用“添加向导”(W)

镜像	描述	源 DNS 名称	源地址	目标 DNS 名称
否	B to A	<一个特定的 IP ...	172.16.0.0/20	<一个特定的 I

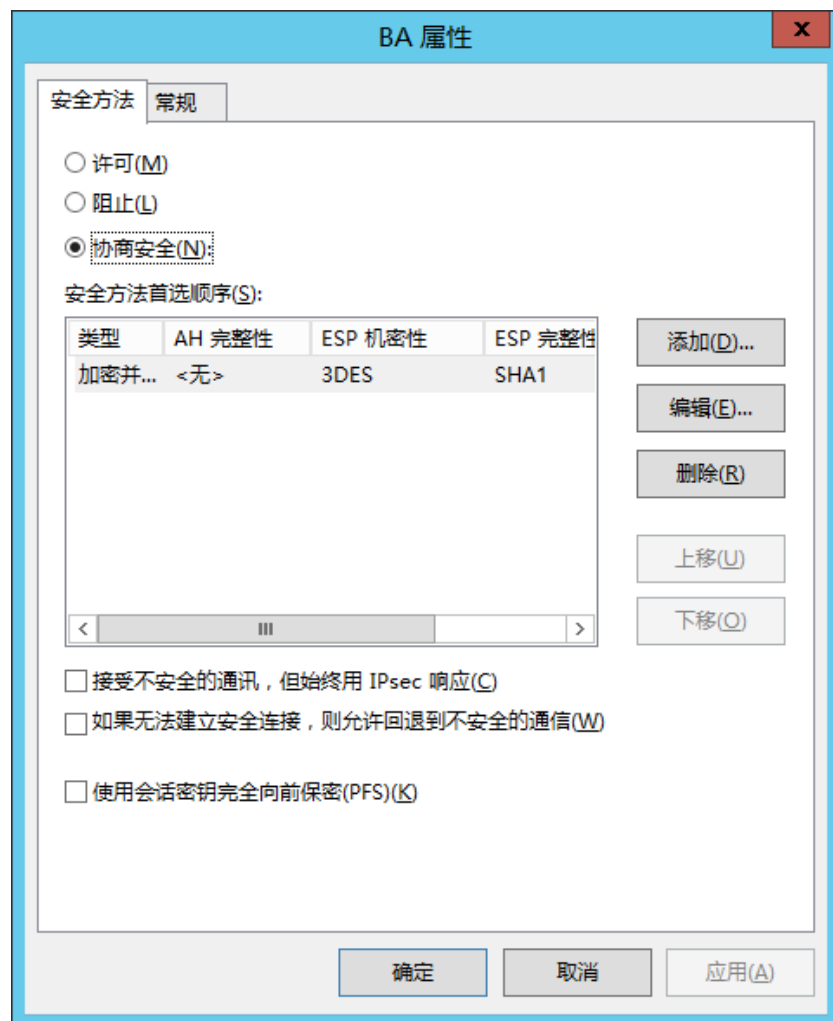
<

III

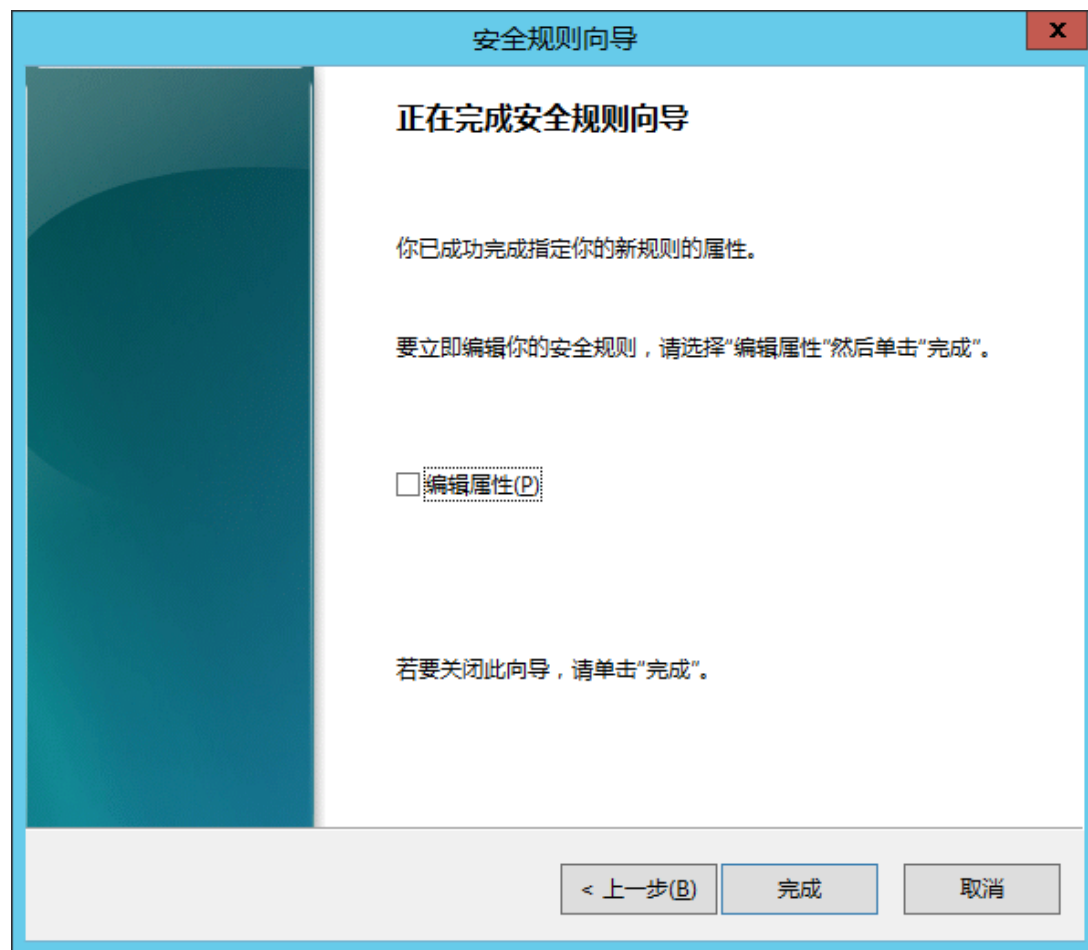
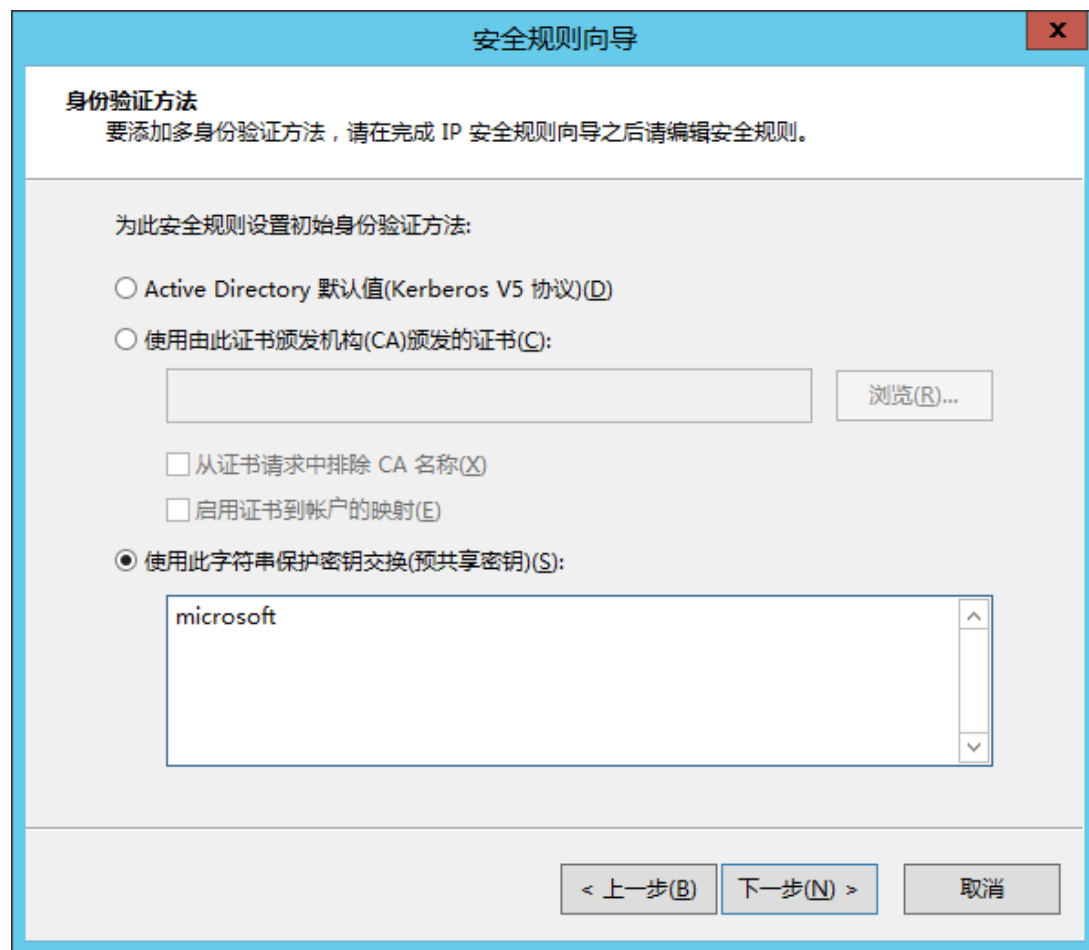
>

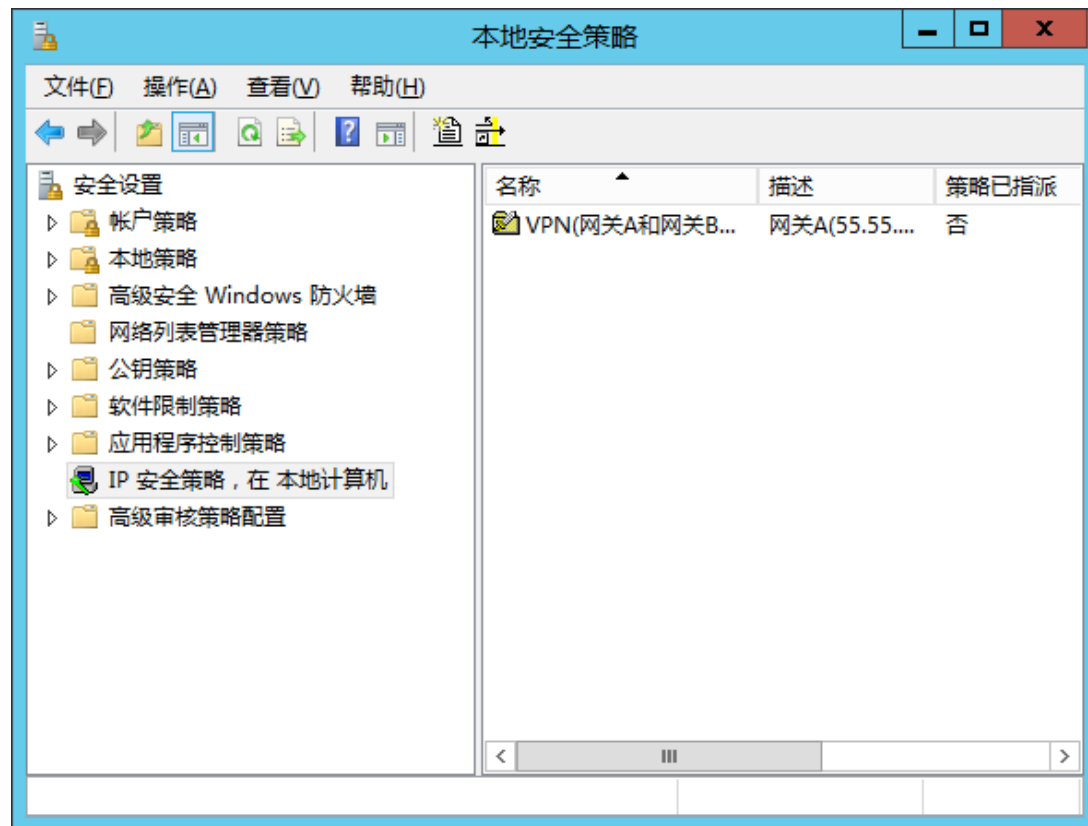
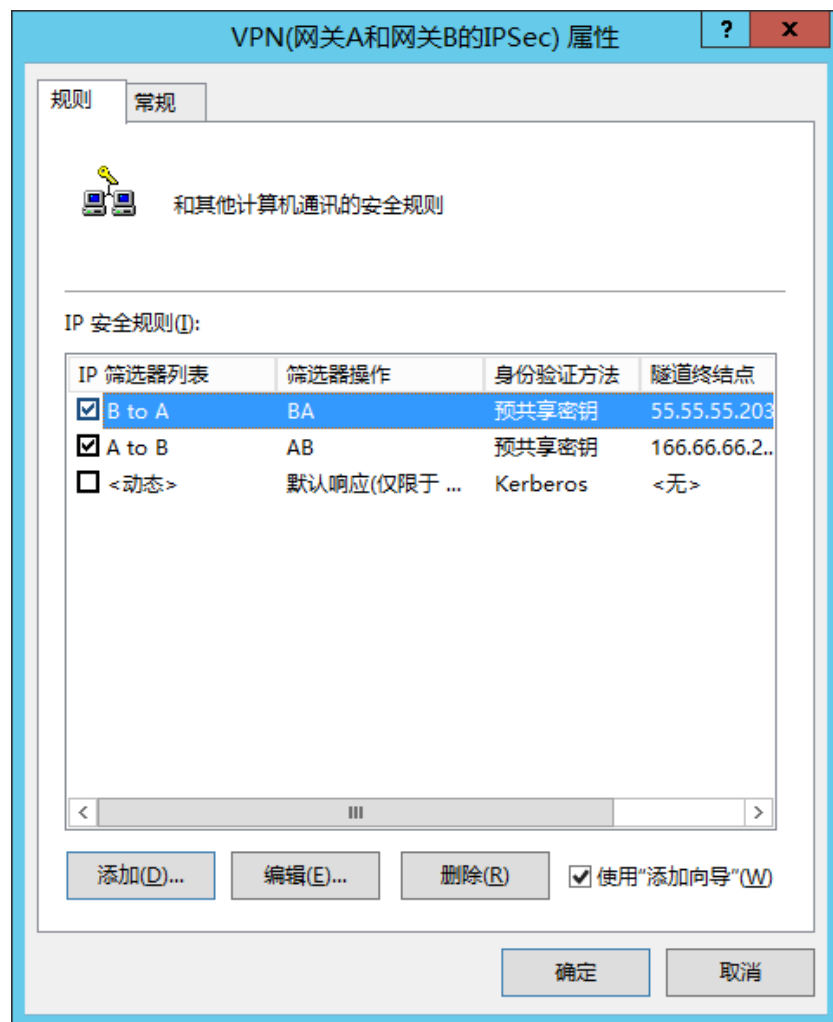
确定

取消

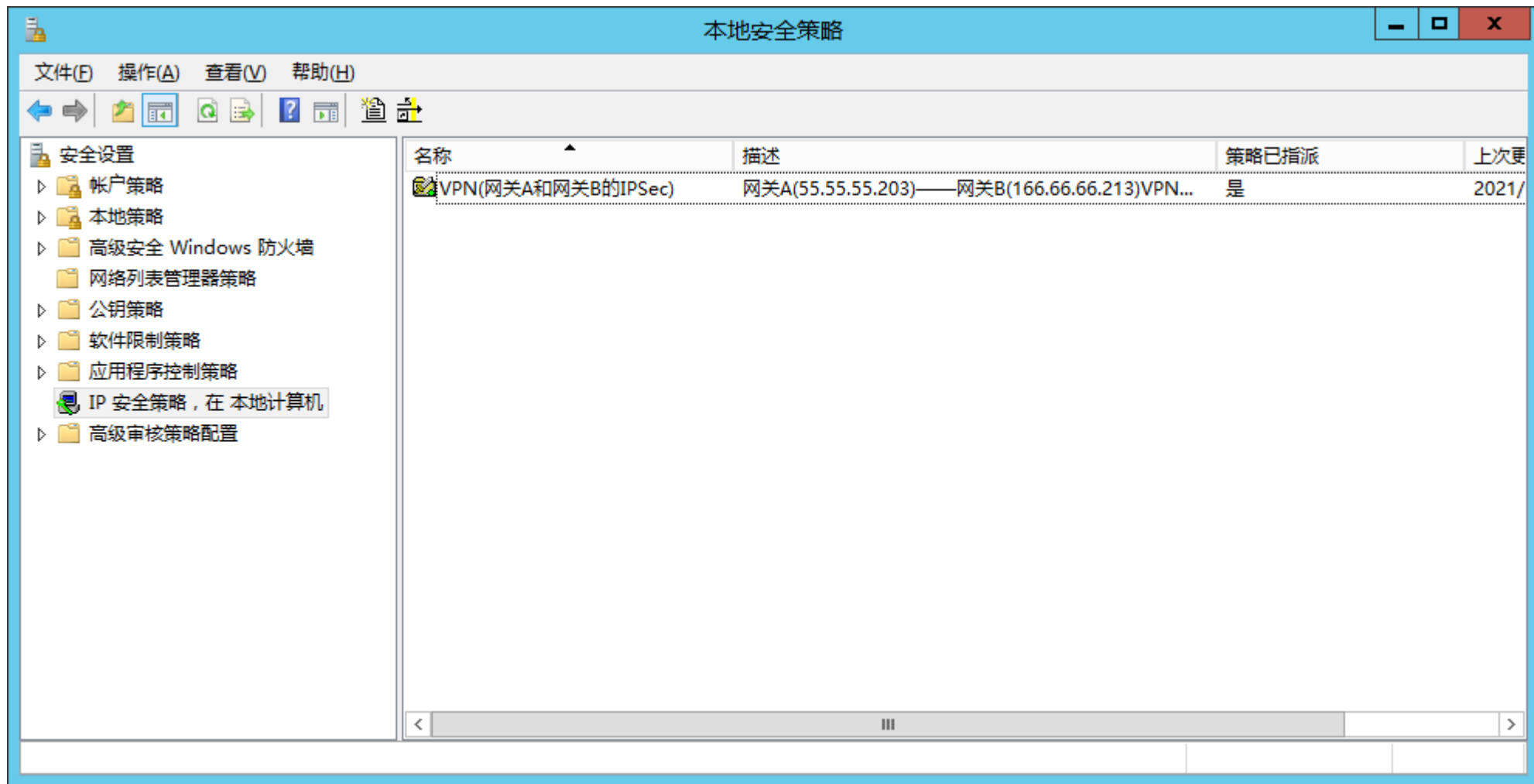






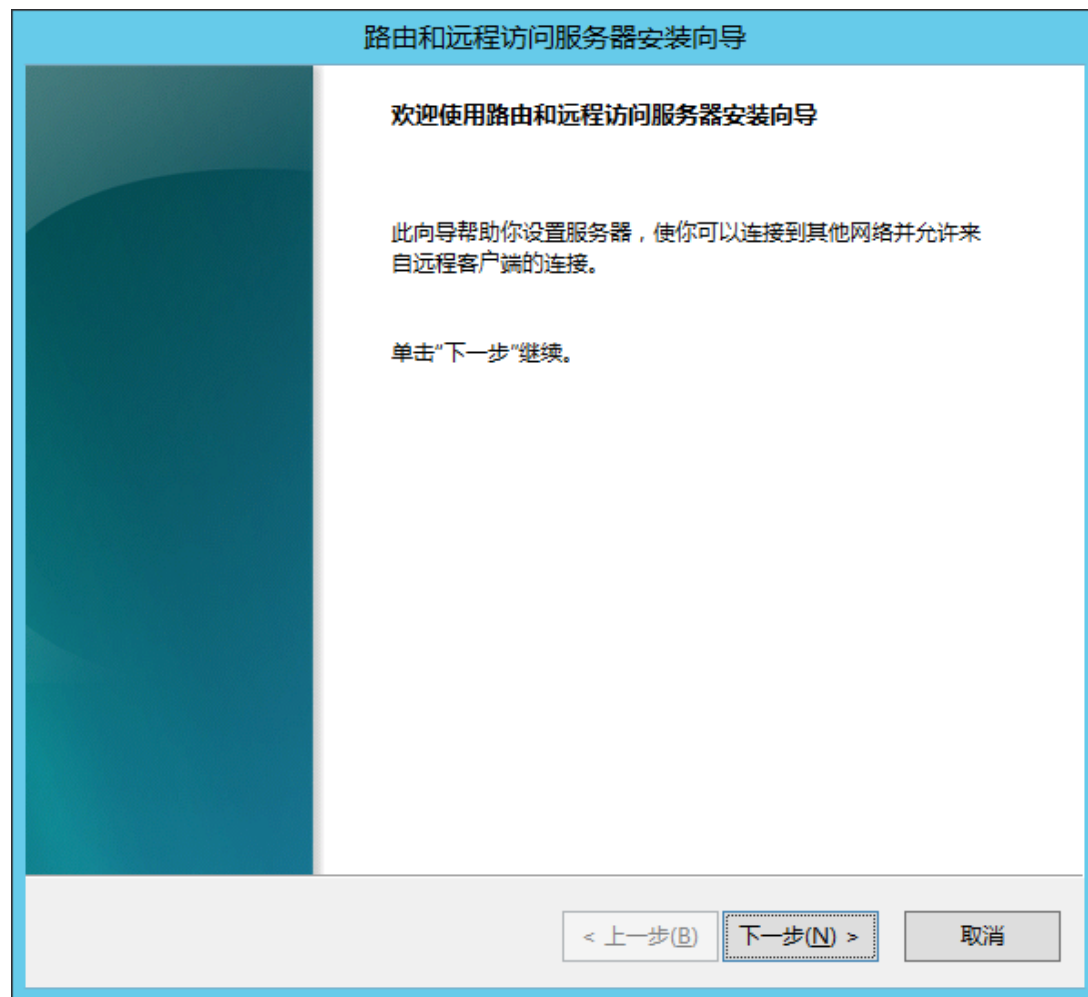
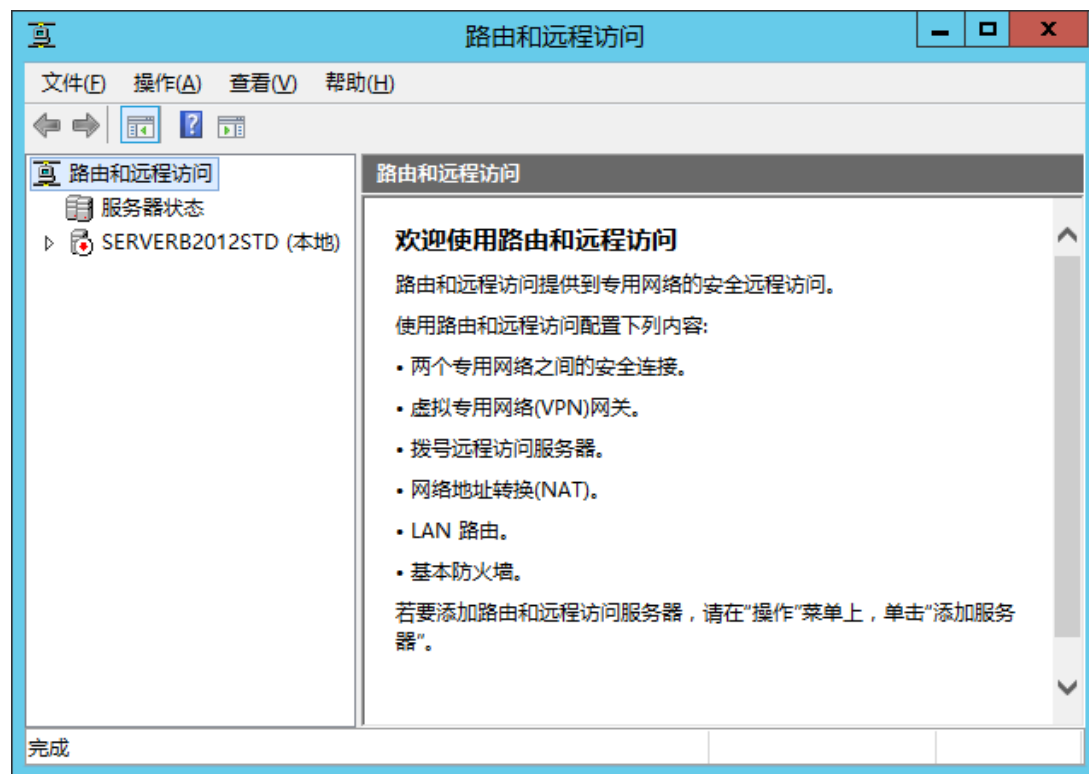


右击策略“VPN(网关A和网关B的IPSec)”并“分配”



# 在“路由和远程访问”中配置VPN服务器网关





路由和远程访问服务器安装向导

配置

你可以启用下列服务的任意组合，或者你可以自定义此服务器。

☐ 远程访问(拨号或 VPN)(R)

允许远程客户端通过拨号或安全的虚拟专用网络(VPN) Internet 连接来连接到此服务器。

☐ 网络地址转换(NAT)(E)

允许内部客户端使用一个公共 IP 地址连接到 Internet。

☐ 虚拟专用网络(VPN)访问和 NAT(V)

允许远程客户端通过 Internet 连接到此服务器，本地客户端使用一个单一的公共 IP 地址连接到 Internet。

☒ 两个专用网络之间的安全连接(S)

将此网络连接到一个远程网络，例如一个分支机构。

☐ 自定义配置(C)

选择在路由和远程访问中的任何可用功能的组合。

< 上一步(B)

下一步(N) >

取消

路由和远程访问服务器安装向导

请求拨号连接

请求拨号连接允许你路由数据到远程网络。

你想使用请求拨号连接访问远程网络吗？

☐ 是(Y)

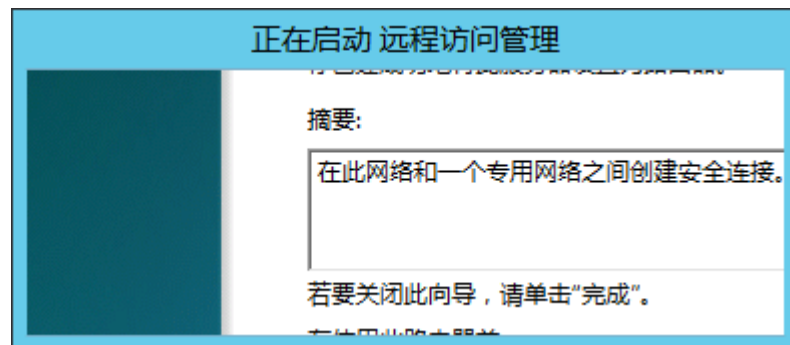
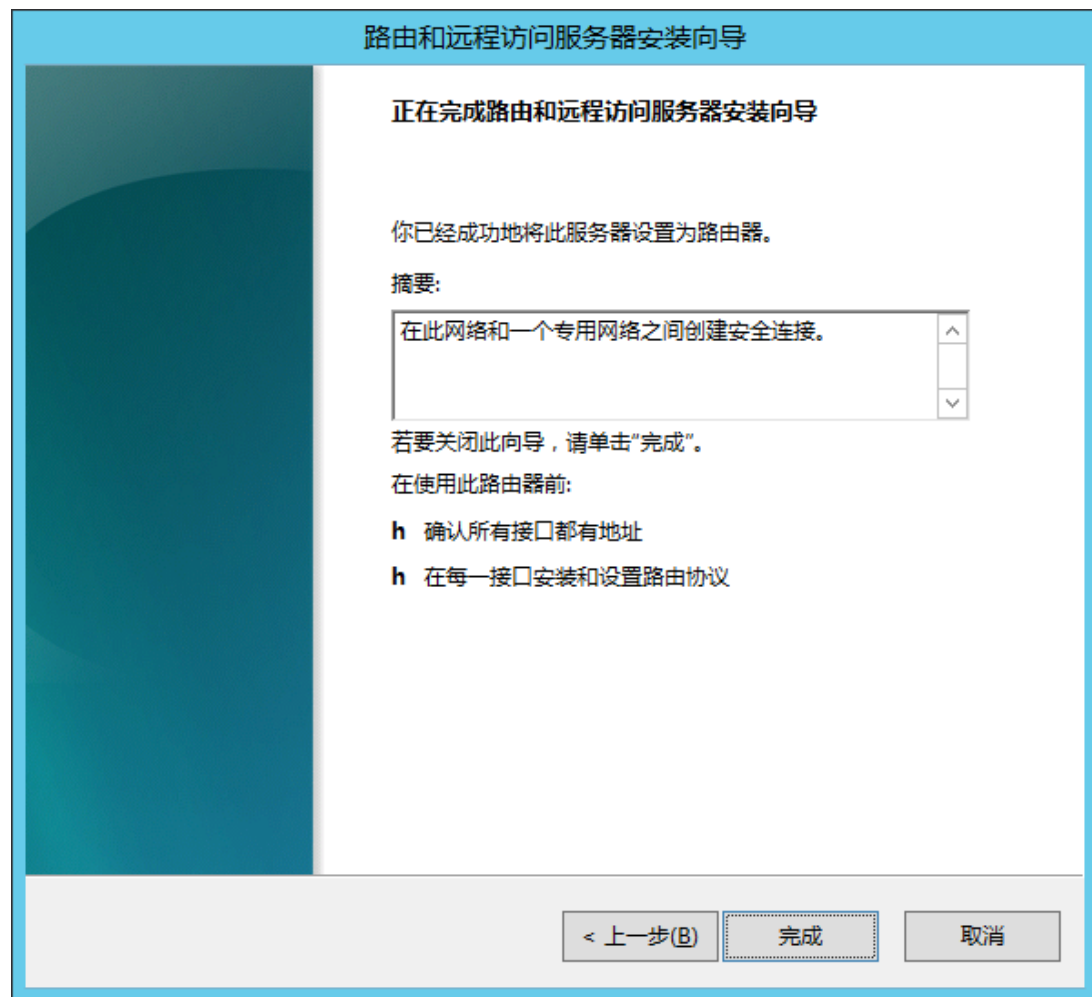
☒ 否(N)

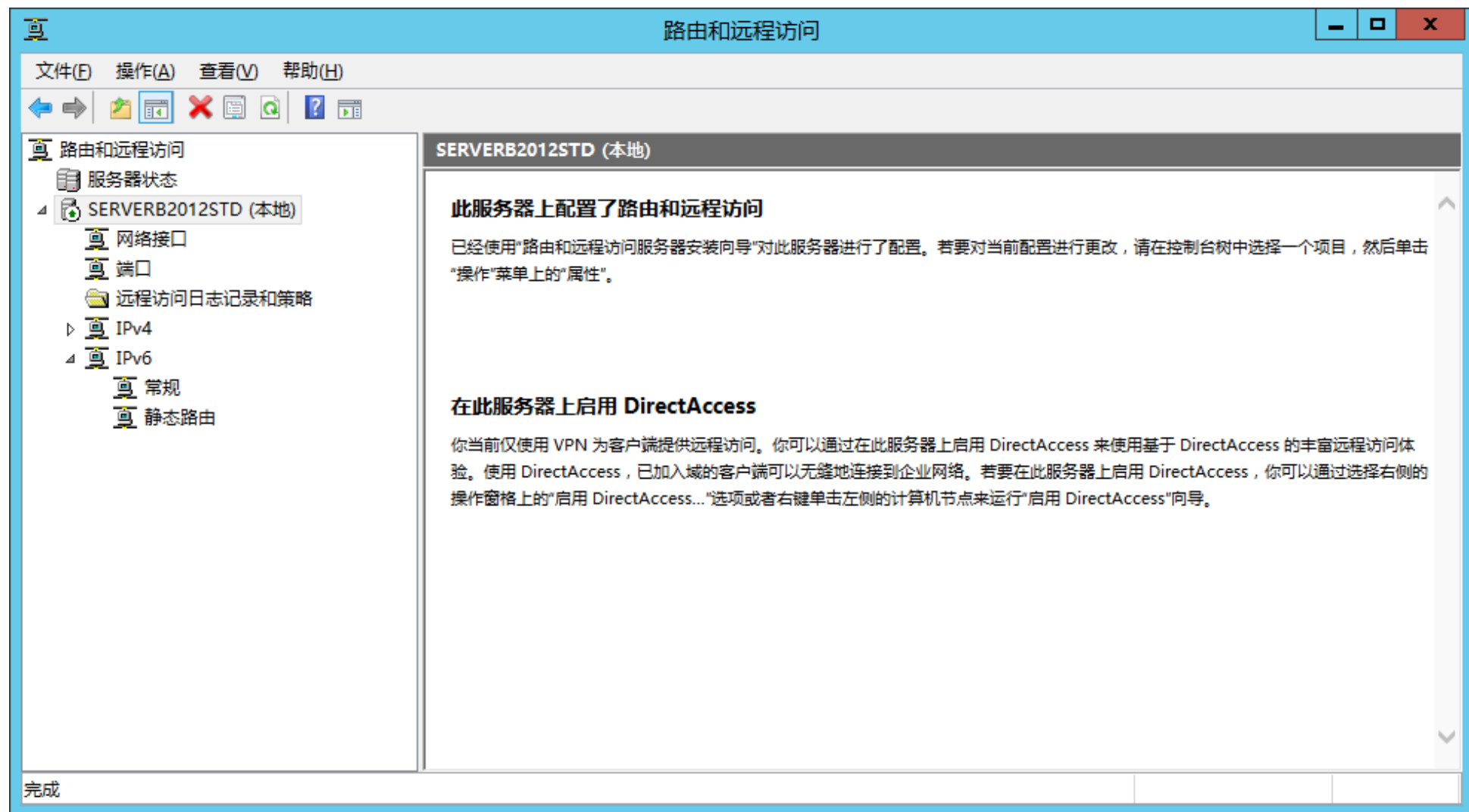
完成此向导后，你可以设置请求拨号连接。

< 上一步(B)

下一步(N) >

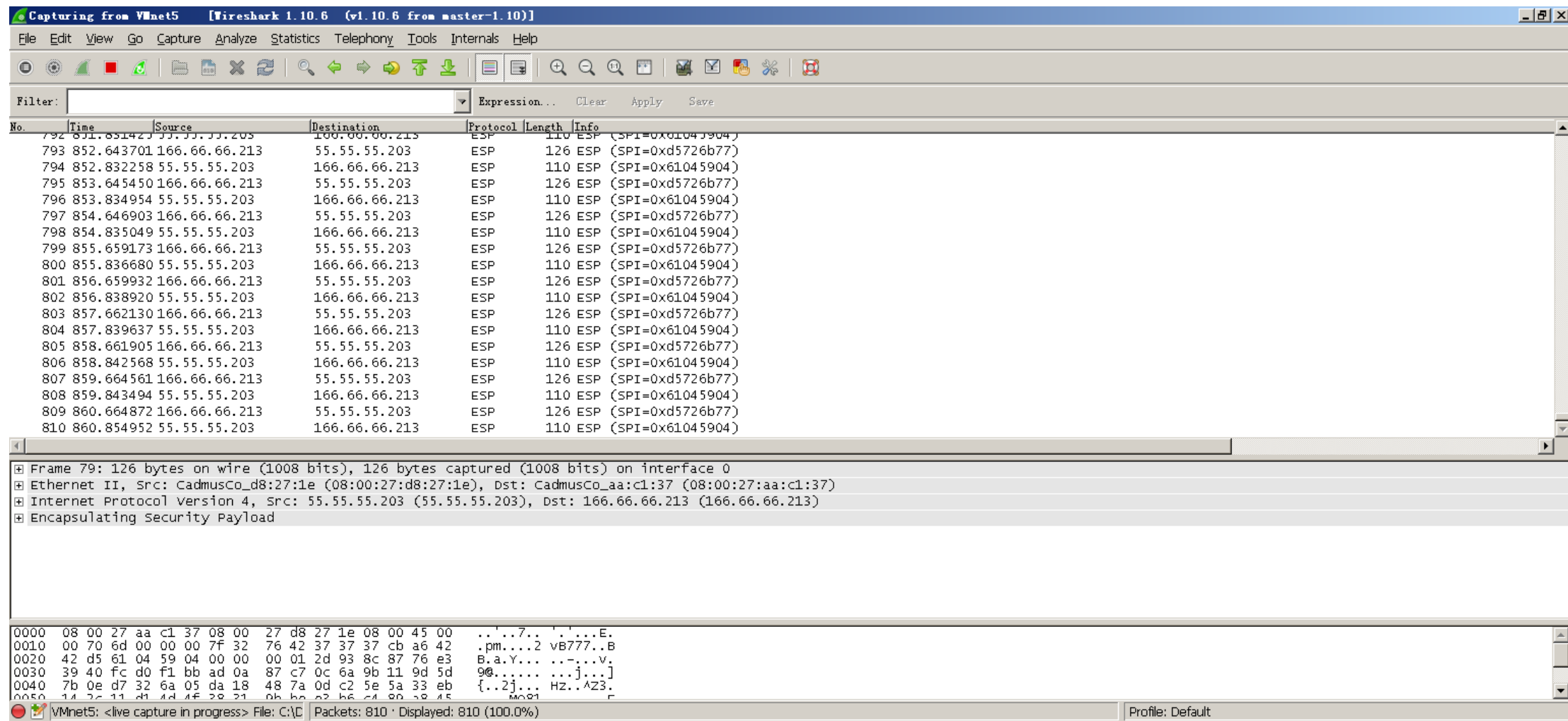
取消







# 2个局域网之间的安全通信 (IPSec VPN)



谢谢！