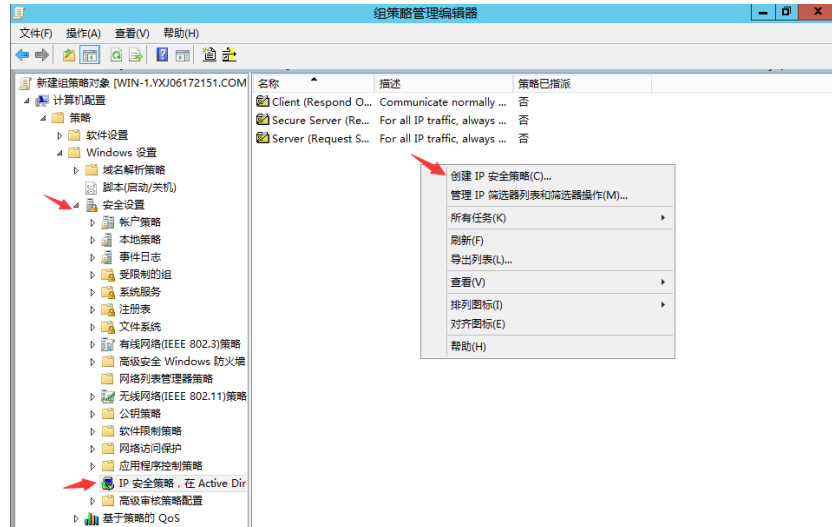


## 目 录

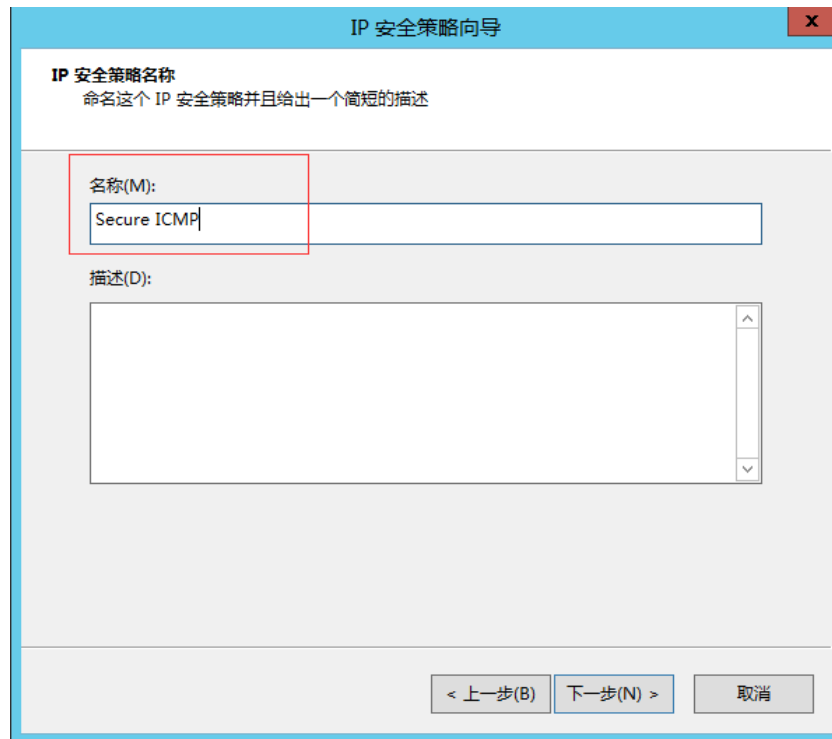
1 利用 IPSec 实现安全传输.....	2
2 利用 L2TP 和 IPSec 实现 VPN .....	13
3 SSL/TLS 实现网站安全 HTTPS (PKI 实验中已做)	

## 1 利用 IPsec 实现安全传输

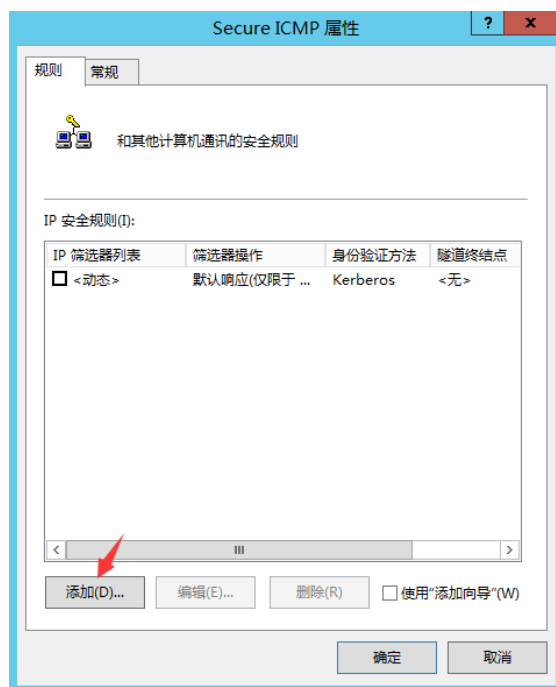
(1) 在顶域机器 (192.168.1.101) 上打开“组策略管理编辑器”，在“IP 安全策略”中右键选择“创建 IP 安全策略”：



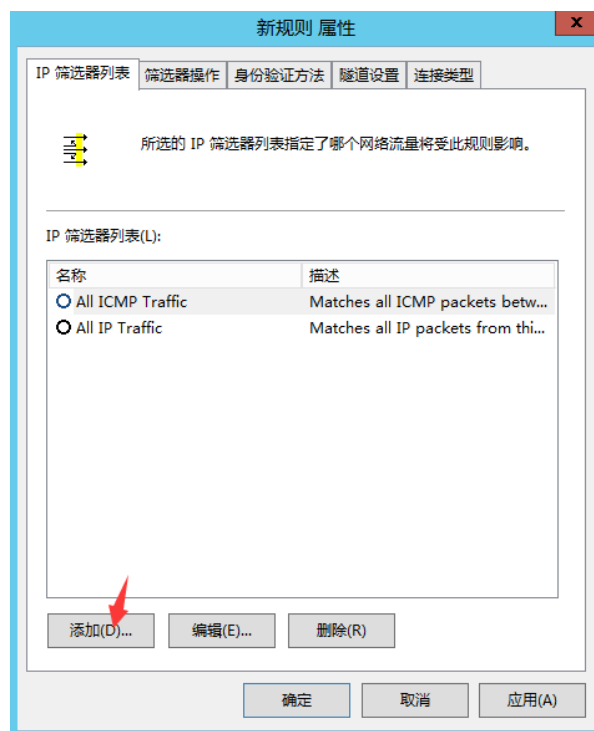
(2) 设置 IP 安全策略名称：



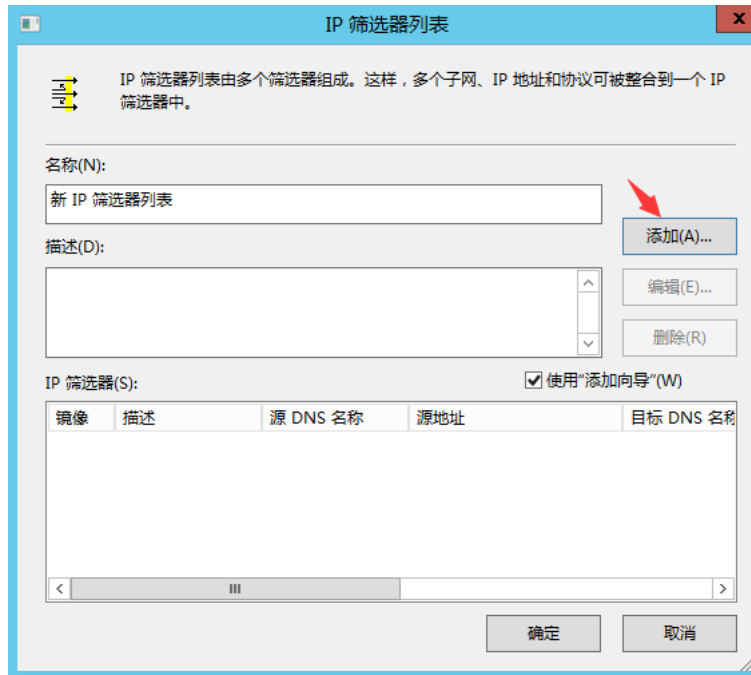
(3) 对 IP 安全策略进行属性编辑，添加新的 IP 安全规则：



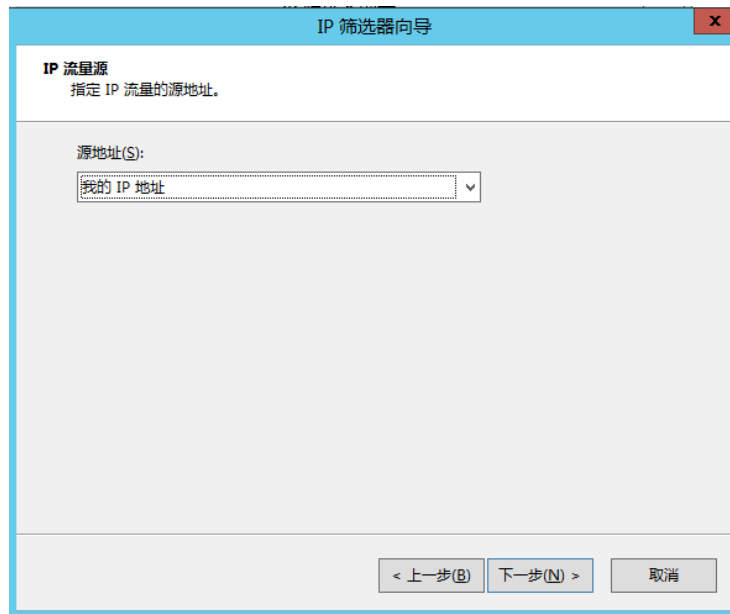
(4) 添加新的 IP 筛选器列表：



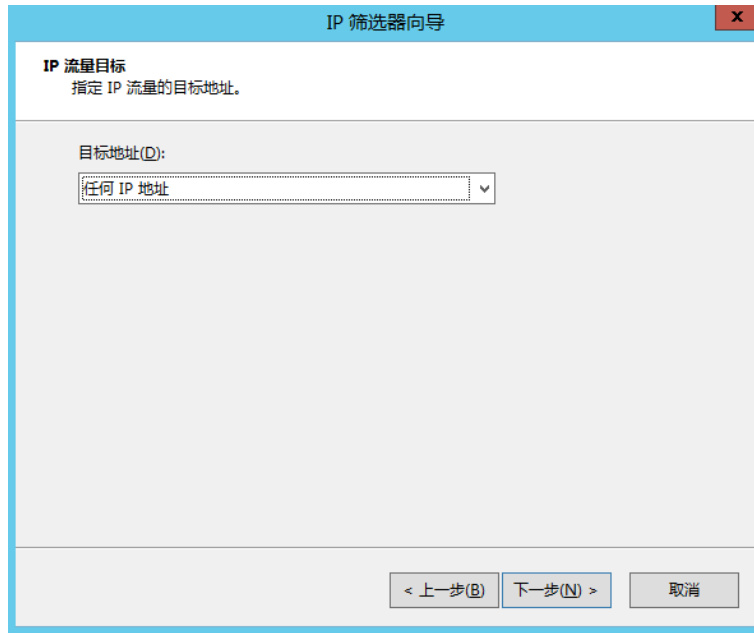
对筛选器列表进行编辑：



IP 流量源选择“我的 IP 地址”：



IP 流量目标选择“任何 IP 地址”：



IP 筛选器向导

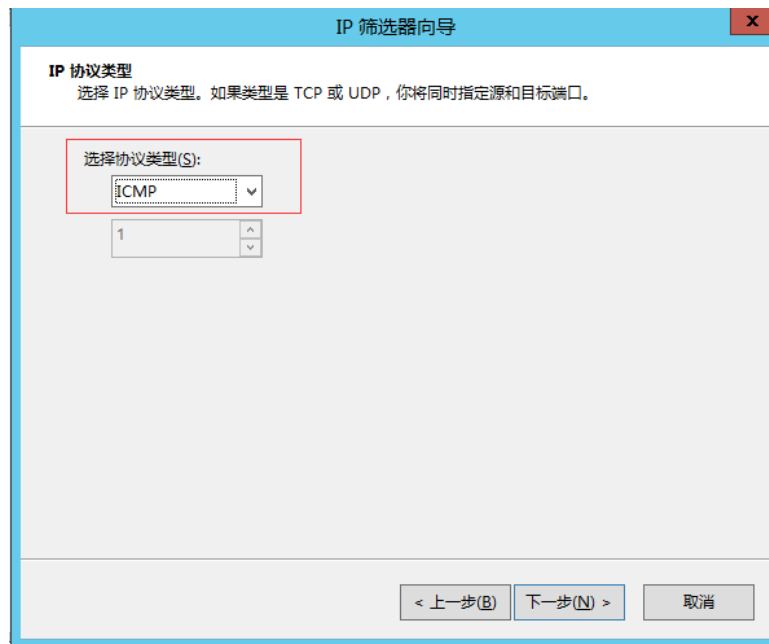
**IP 流量目标**  
指定 IP 流量的目标地址。

目标地址(D):

任何 IP 地址

< 上一步(B)   下一步(N) >   取消

协议类型选择“ICMP”：



IP 筛选器向导

**IP 协议类型**  
选择 IP 协议类型。如果类型是 TCP 或 UDP，你将同时指定源和目标端口。

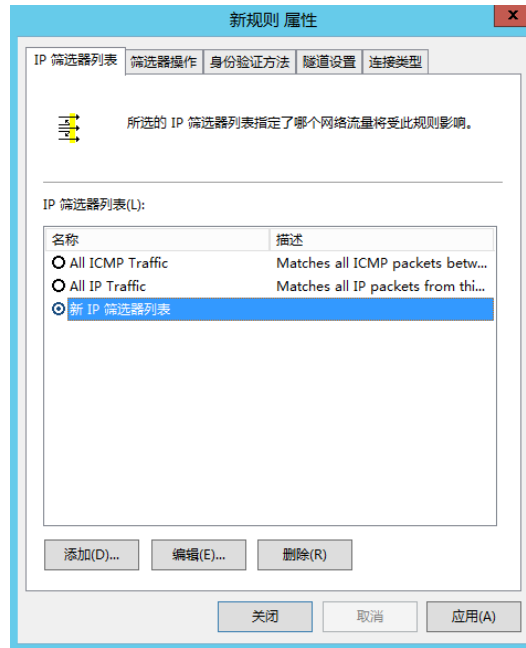
选择协议类型(S):

ICMP

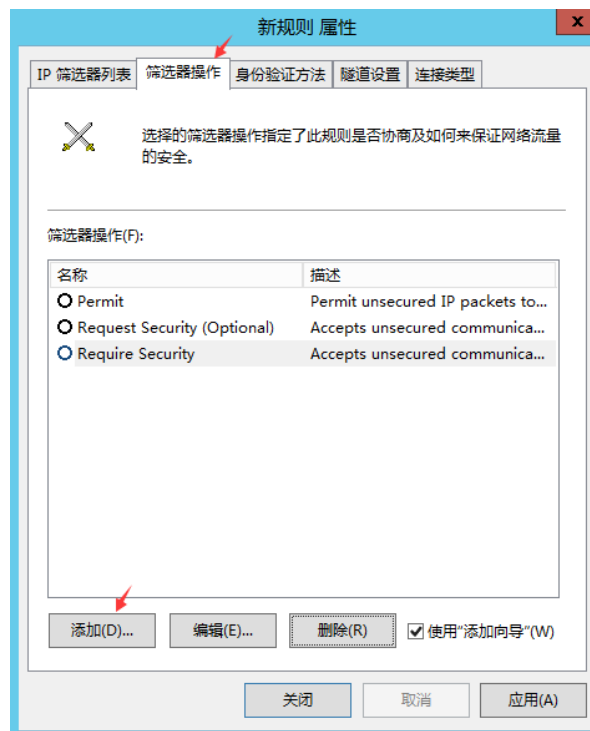
1

< 上一步(B)   下一步(N) >   取消

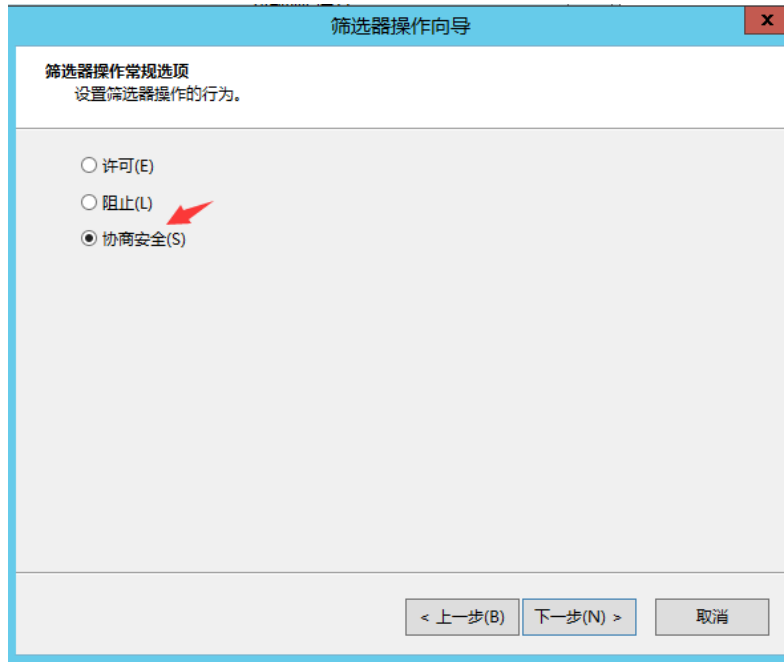
最后选择刚才新建的“新 IP 筛选列表”：



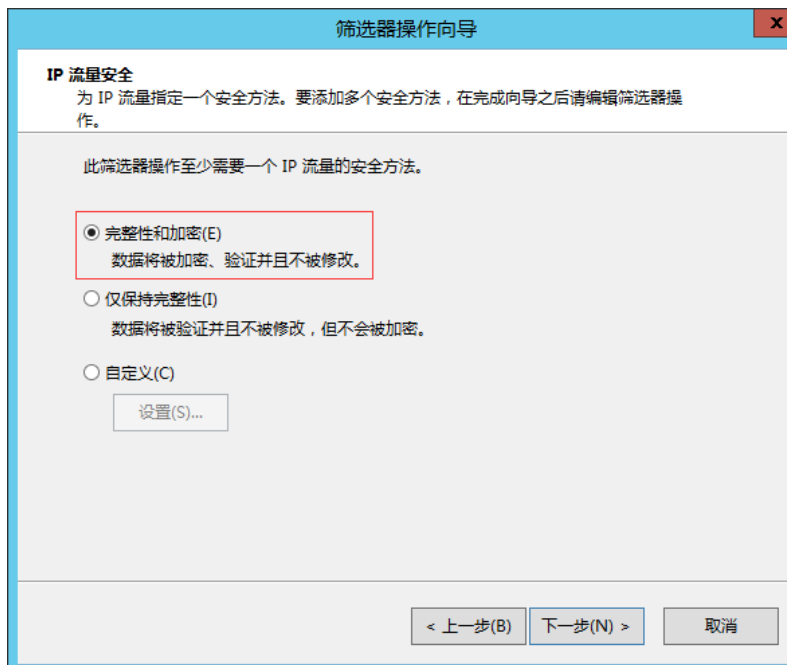
(5) 添加新的“筛选器操作”：



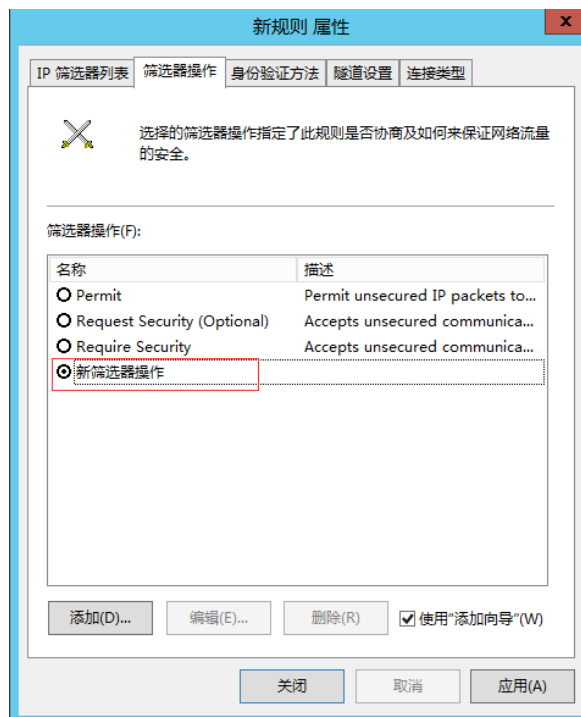
选择“协商安全”：



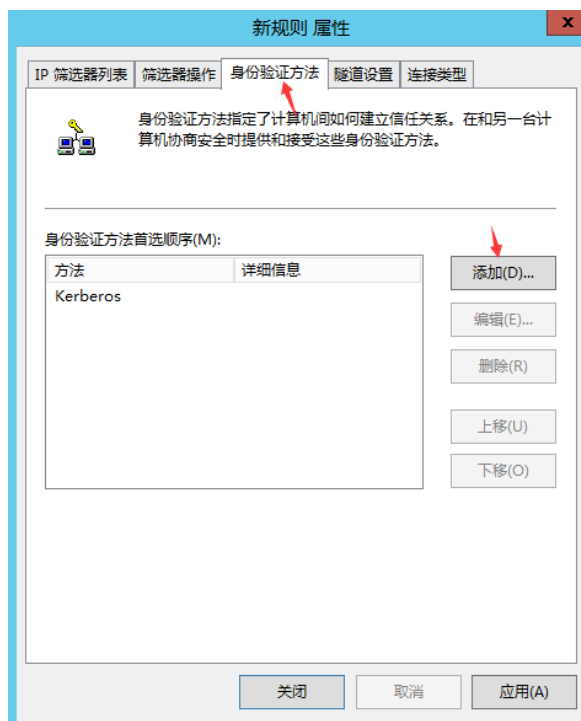
选择“完整性和加密”：



最后选择上刚才新建的“新筛选器操作”：

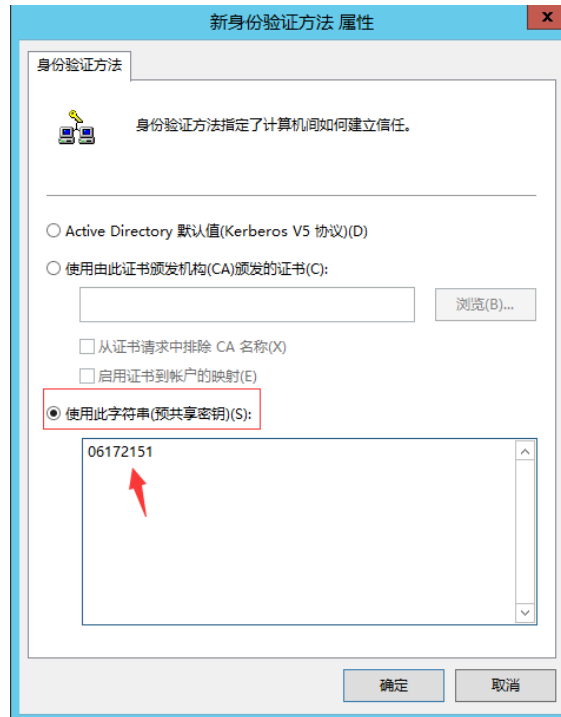


(6) 添加“身份验证方法”：

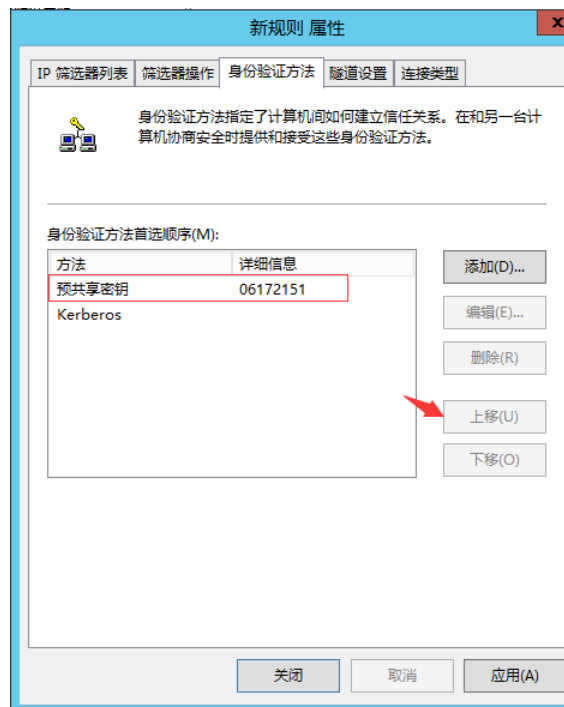




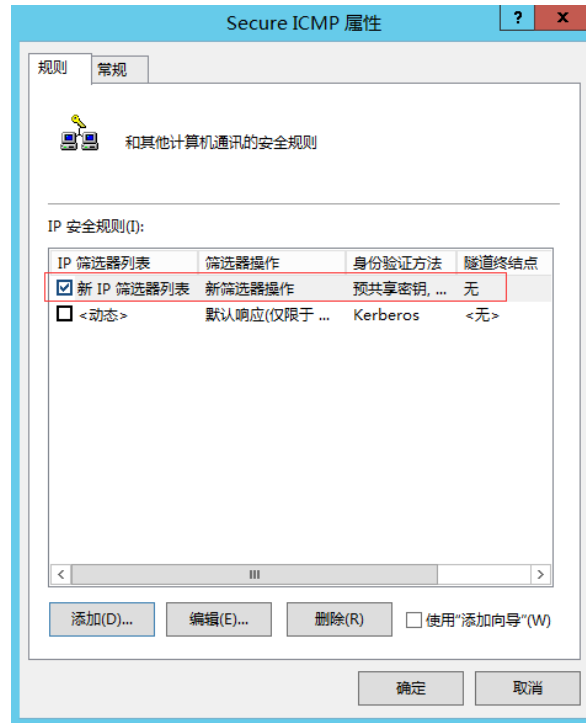
选择“预共享密钥”，并自定义密钥 06172151：



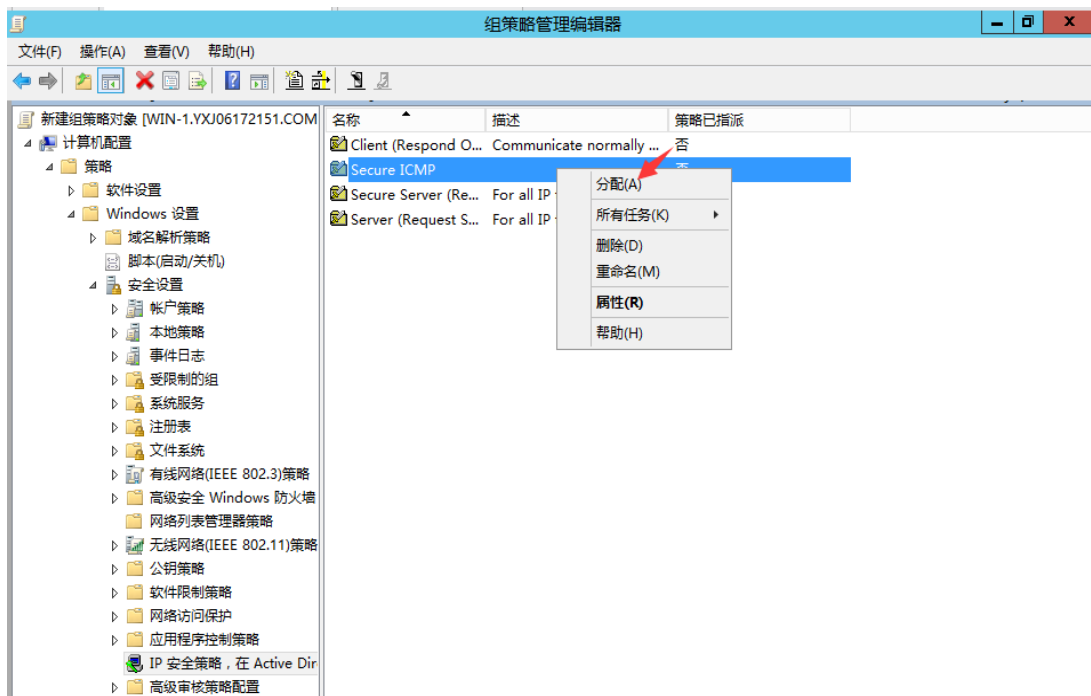
将预共享密钥方式设为首选：



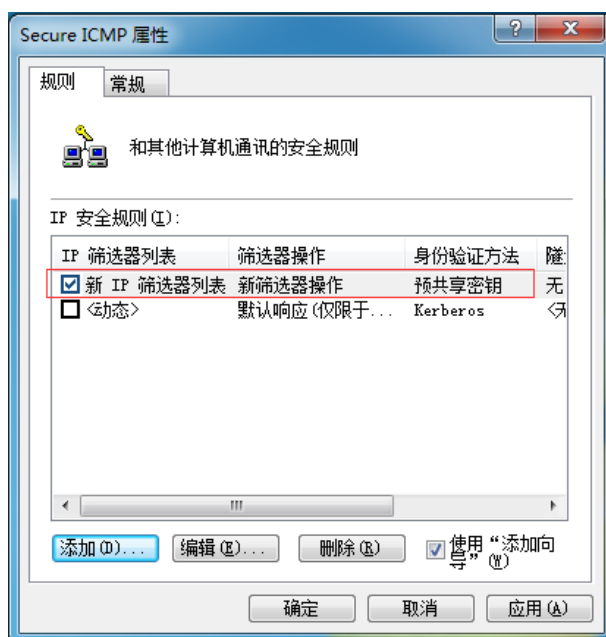
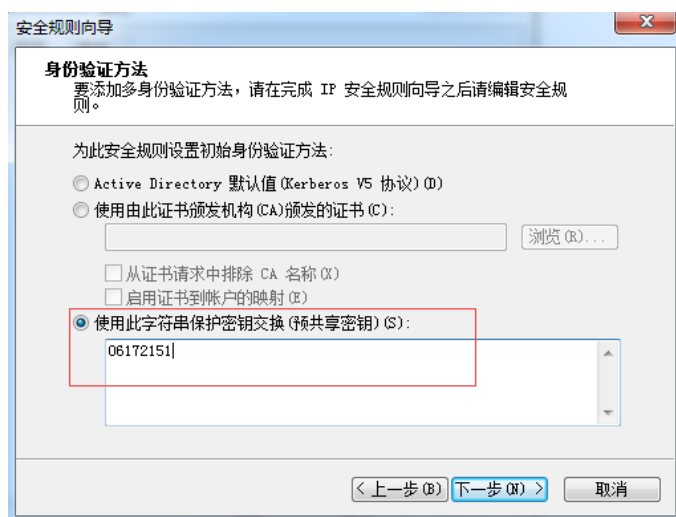
(7) 编辑完成后，将“IP 安全规则”设置为新建的“新 IP 筛选器列表”：



然后将策略进行指派：



(8) 然后在与其通信的另一台客户机 (192.168.1.104) 上以同样的方式建立“IP 安全规则”，预共享密钥同样设置为 06172151：



(9) 在客户机不指派该“IP 安全策略”前，发现两台机器无法 ping 通：


名称	描述	策略已指派	上次更改时间
Secure ICMP		否	2020/4/29 20:12:55

```
PS C:\Users\Administrator> ping 192.168.1.104

正在 Ping 192.168.1.104 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.104 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

(10) 将客户机的“IP 安全规则”也进行指派之后，相互可以 ping 通，成功实现了端到端的加密安全传输：

名称	描述	策略已指派	上次更改时间
 Secure ICMP		是	2020/4/29 20:12:55

```
PS C:\Users\Administrator> ping 192.168.1.104

正在 Ping 192.168.1.104 具有 32 字节的数据:
来自 192.168.1.104 的回复: 字节=32 时间=10ms TTL=128
来自 192.168.1.104 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.104 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.104 的回复: 字节=32 时间<1ms TTL=128

192.168.1.104 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 10ms, 平均 = 2ms
```

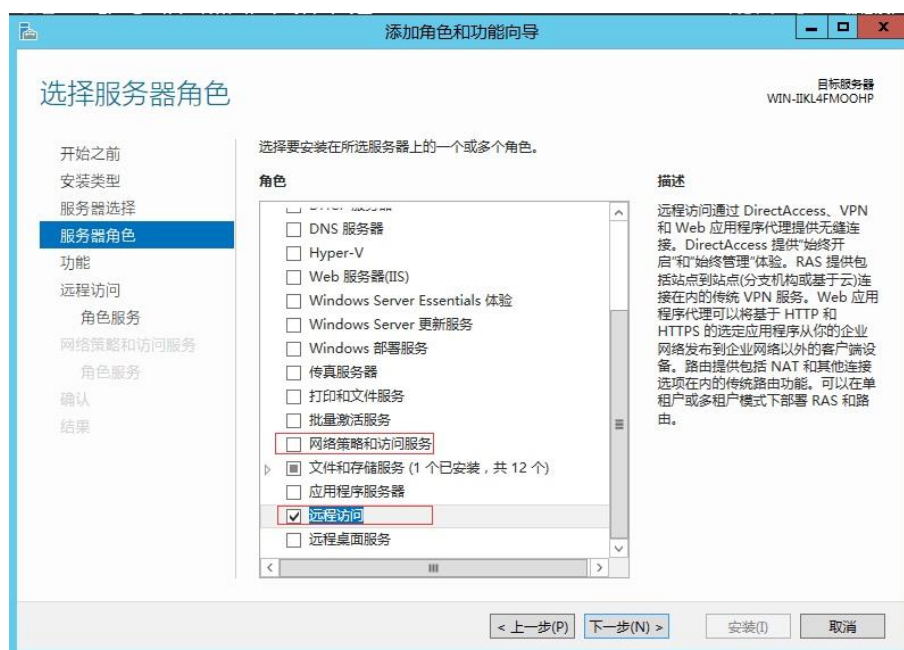
## 2 利用 L2TP 和 IPSec 实现 VPN

实验拓扑如下：

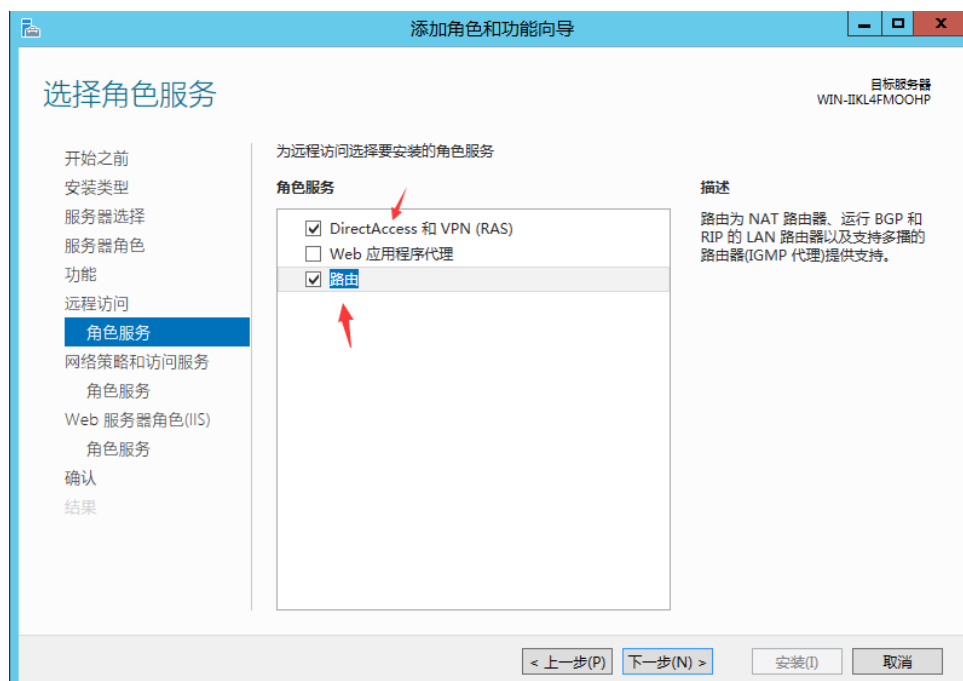
- ① 一台 Windows Server 2012 作为 AD 域控制器和 RADIUS 服务器，位于 192.168.1.0/24 子网，IP 地址为：192.168.1.101
- ② 一台 Windows 7 作为远程用户客户机，位于 192.168.110.0/24 子网，IP 地址为：192.168.110.132
- ③ 一台 Windows Server 2012 作为 VPN 网关，内网网卡 IP 地址为：192.168.1.129，外网网卡 IP 地址为：192.168.110.130

(1) 设置 Windows 7 客户机 IP 地址为 192.168.110.132；DNS 服务器地址为域控的 IP 地址 192.168.1.101；将 VPN 网关服务器的两个网卡分别设置为内网 IP 192.168.1.129 和外网 IP 192.168.110.130。

(2) 在 VPN 网关服务器上安装“远程访问”功能：



选择“VPN”和“路由”服务：



其他选项默认即可，直至安装成功。

(3) 进入“路由和远程访问”服务进行配置：



选择“远程访问(拨号或 VPN)”：

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

选择“VPN”：

路由和远程访问服务器安装向导

**远程访问**

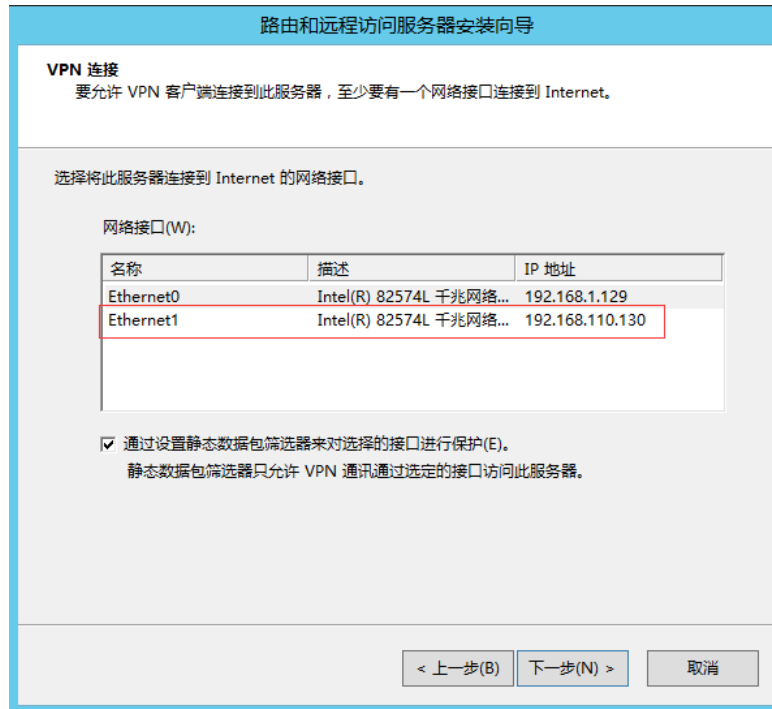
你可以配置此服务器接受拨号连接和 VPN 连接。

☒ VPN(V)  
VPN 服务器(也称为 VPN 网关)可以通过 Internet 从远程客户端接受连接。

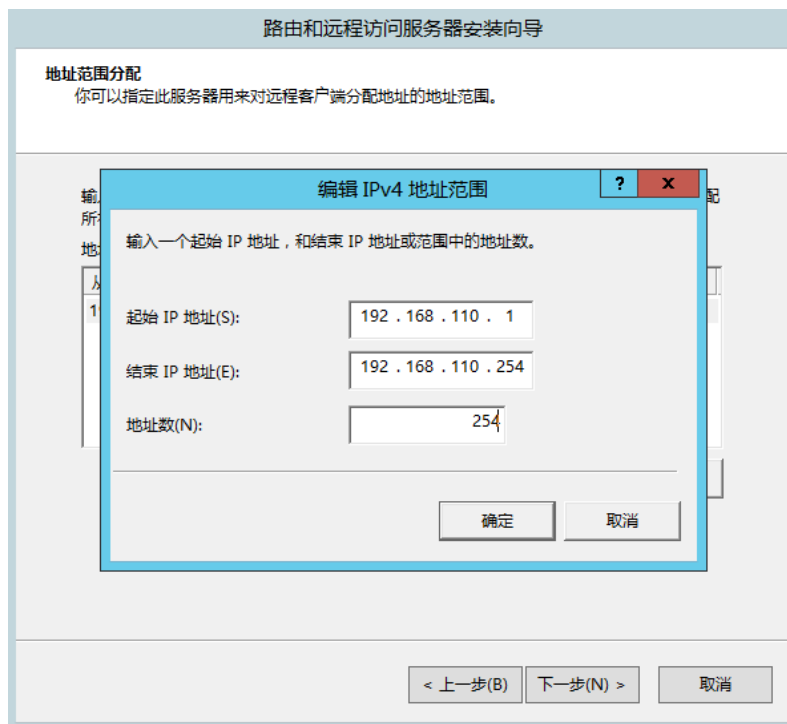
☐ 拨号(D)  
拨号远程访问服务器可以通过拨号媒体，例如调制解调器，从远程客户端直接接受连接。

< 上一步(B)    下一步(N) >    取消

选择相应的外网网卡：



设置 VPN 客户端的网段：





选择使用 RADIUS 服务器进行验证：

路由和远程访问服务器安装向导

**管理多个远程访问服务器**  
连接请求可以在本地进行身份验证，或者转发到远程身份验证拨入用户服务(RADIUS)服务器进行身份验证。

虽然路由和远程访问可以对连接请求进行身份验证，包含多个远程访问服务器的大型网络通常使用一个 RADIUS 服务器来集中进行身份验证。

如果你在网络上使用一个 RADIUS 服务器，你可以设置此服务器将身份验证请求转发到 RADIUS 服务器。

你想设置此服务器与 RADIUS 服务器一起工作吗？

☐ 否，使用路由和远程访问来对连接请求进行身份验证(O)

☒ 是，设置此服务器与 RADIUS 服务器一起工作(Y)

< 上一步(B)    下一步(N) >    取消

设置 RADIUS 服务器地址以及共享密码(yuan123)：

路由和远程访问服务器安装向导

**RADIUS 服务器选择**  
你可以指定想用来执行身份验证和记帐的 RADIUS 服务器。

输入此服务器要作为远程身份验证和记帐使用的主和辅 RADIUS 服务器。

主 RADIUS 服务器(P): 192.168.1.101

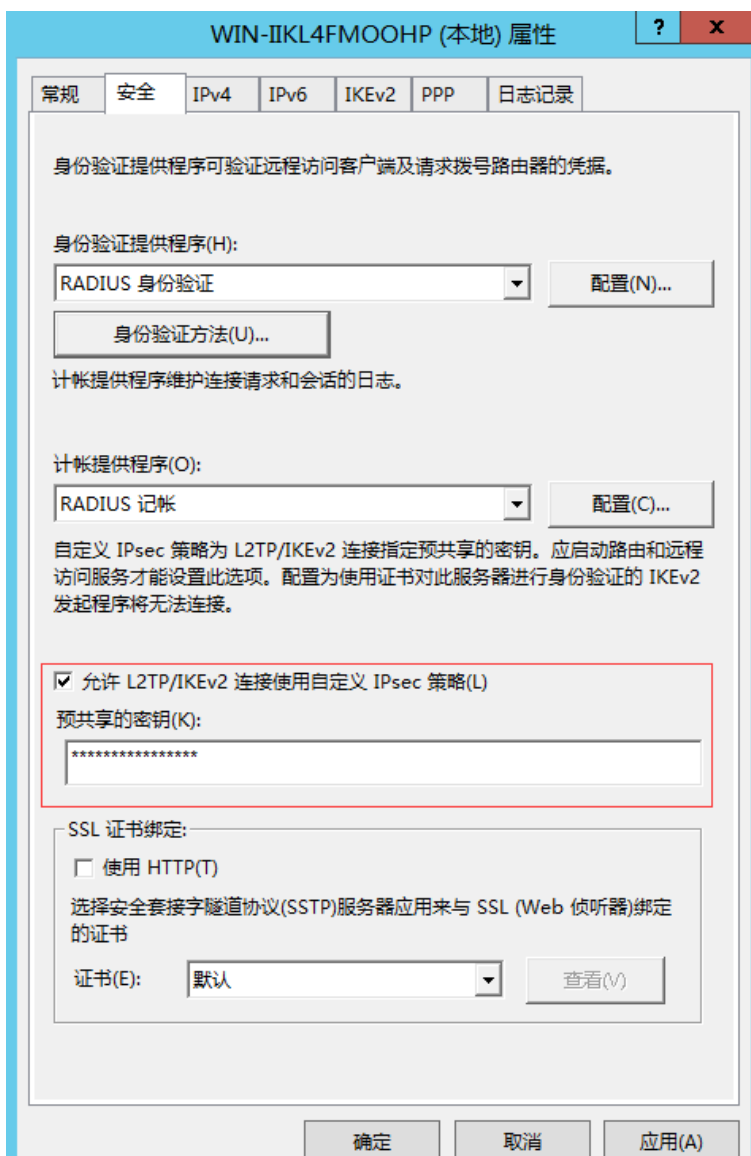
辅 RADIUS 服务器(A):

键入用来联系这些 RADIUS 服务器的共享机密(密码)。

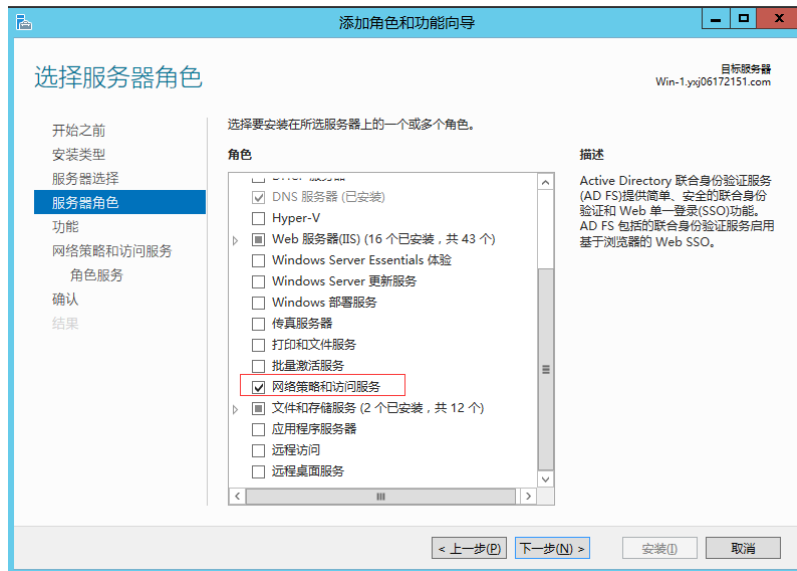
共享机密(S):

< 上一步(B)    下一步(N) >    取消

配置完后，进入右键属性—安全，设置 L2TP/IKEv2 的预共享密钥为 yxj06172151：



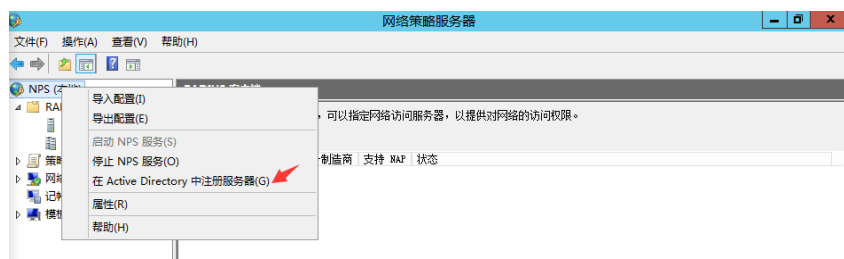
(4) 在域控服务器上安装 Radius 服务。 打开“添加角色和功能向导”，并安装“网络策略和访问服务”，其他选项默认“下一步”即可：



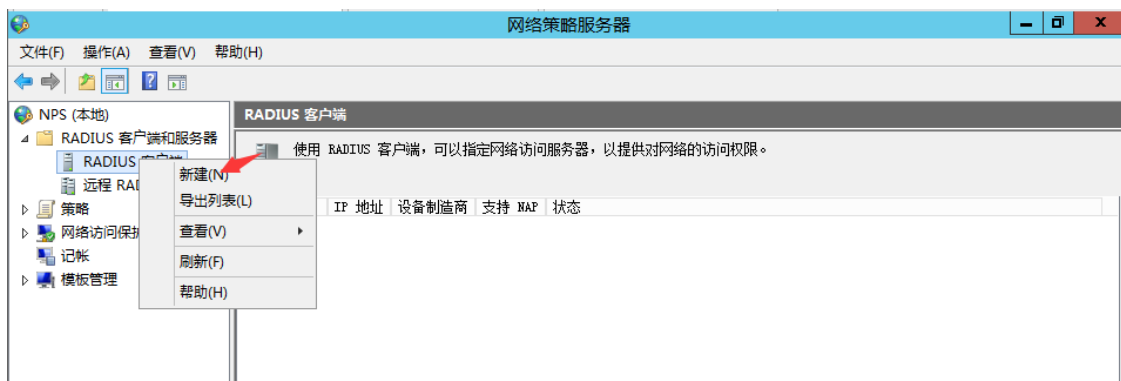
可以看到成功安装了 RADIUS 服务：



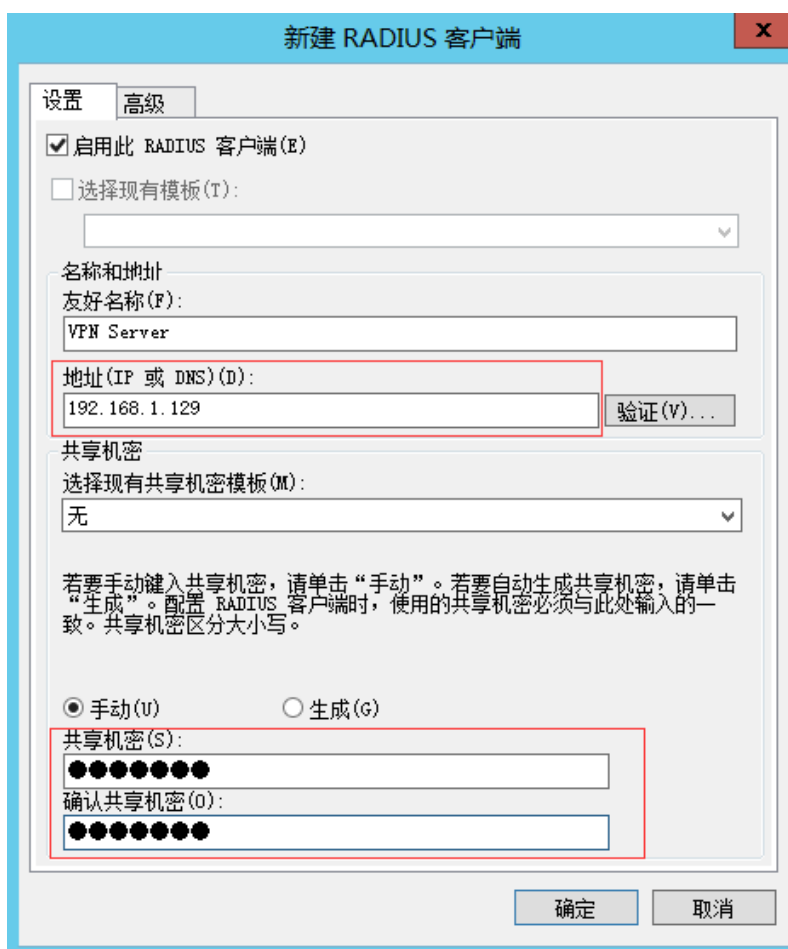
(5) RADIUS 安装完成后，还需要在 AD 中注册服务器：



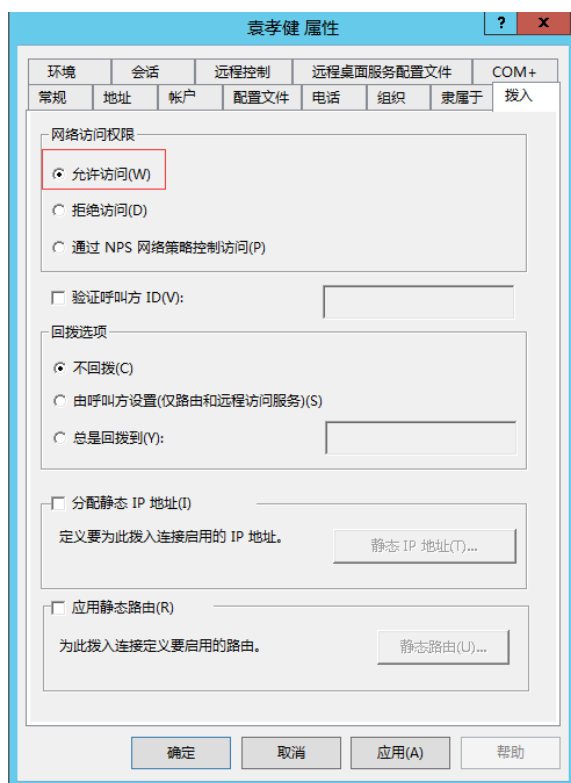
(6) 然后将 VPN 服务器新建为 RADIUS 的客户端：



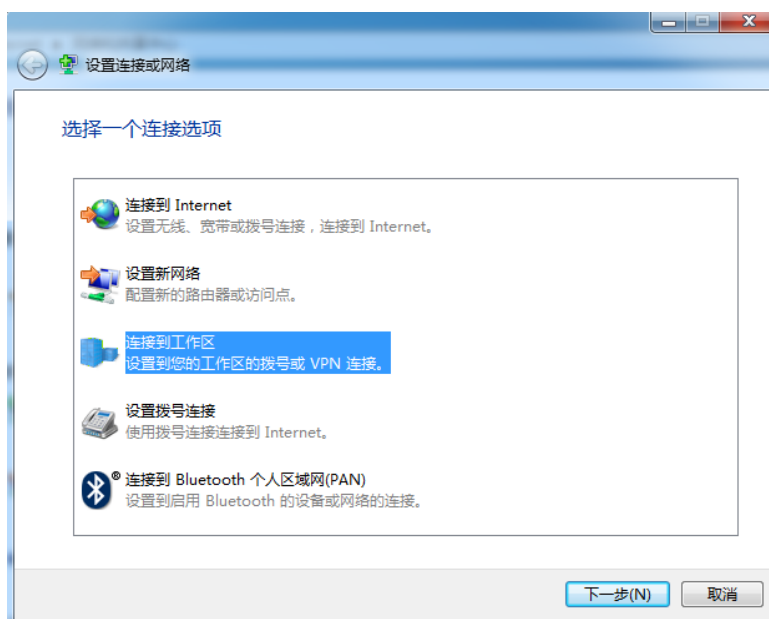
输入 VPN 服务器内网网卡地址以及设置的共享密码(yuan123)：



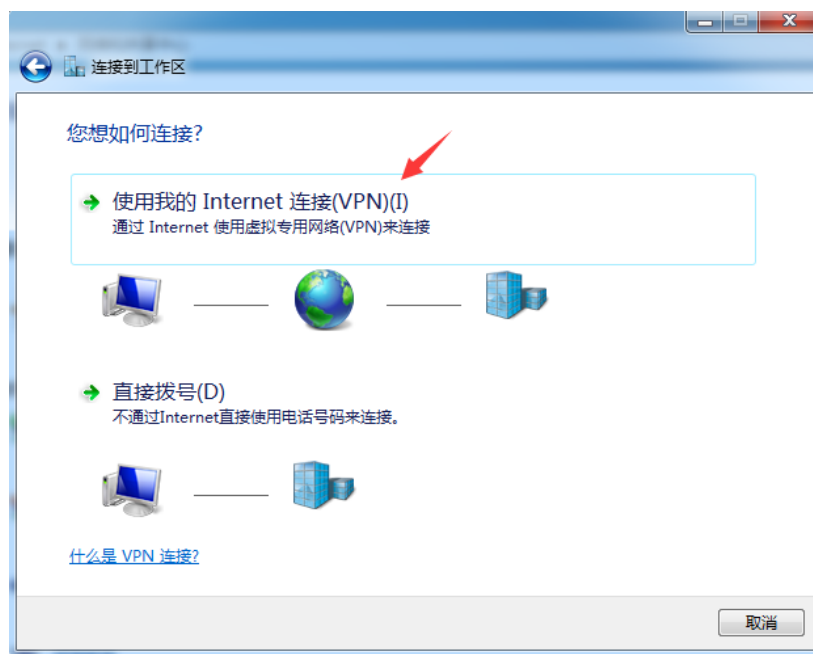
(7) 最后将我们用于登录 VPN 的域账户(yuanxiaojian1)设置运行网络访问的权限，至此域控服务器上的配置结束：



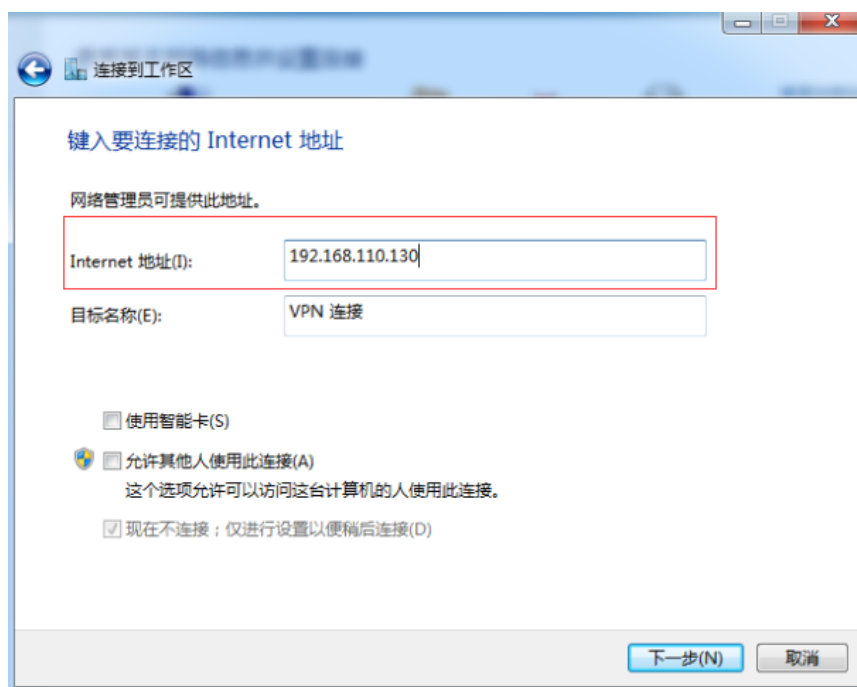
(8) 然后我们进入客户机中，进行“设置连接或网络“，选择”连接到工作区“：



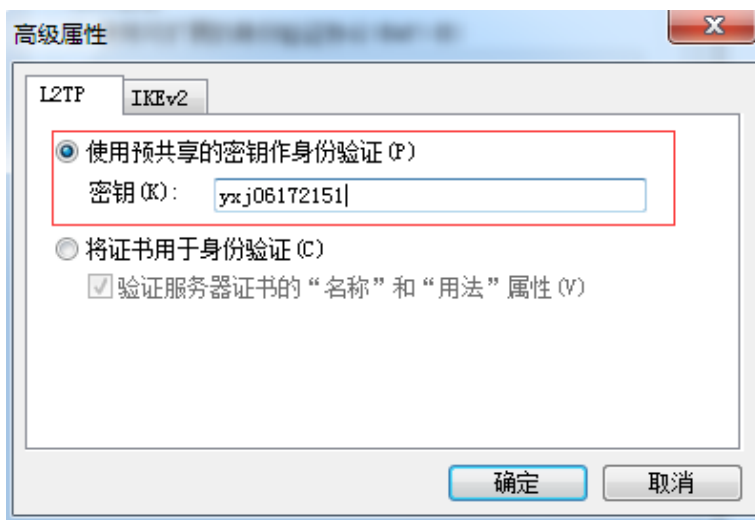
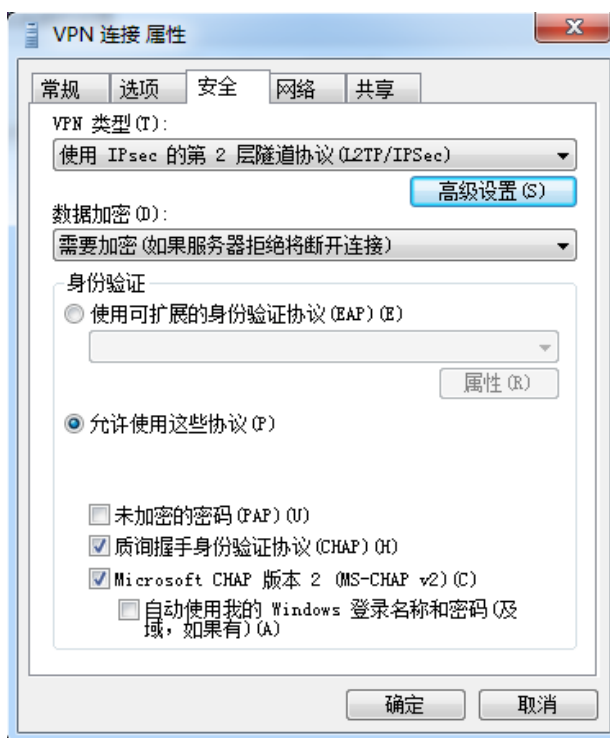
选择 VPN:



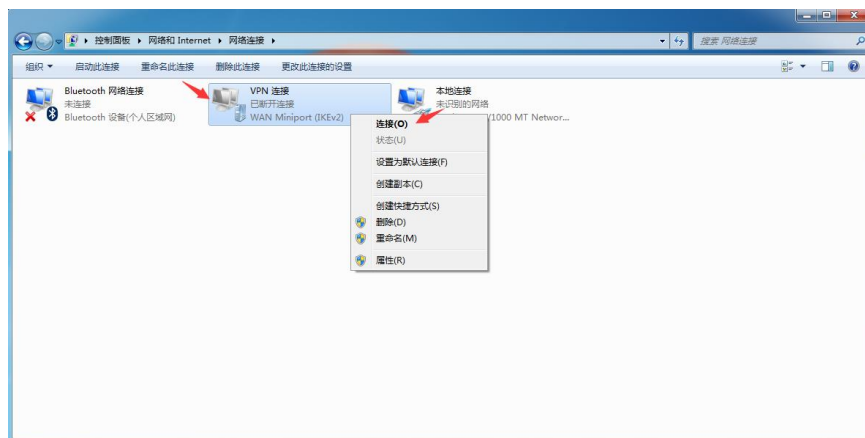
选择“稍后设置 Internet 连接”，然后设置 VPN 服务器的内网网卡地址,后续的用户名和密码可以先不填:



(9) 设置完成后可以看到新建的 VPN 连接，右键选择“属性”—“安全”，选择“L2TP”并在“高级设置中”设置 L2TP 的预共享密钥(yxj06172151)：



(10) 配置完成后，右键进行连接：



(11) 输入之前已配置过权限的域用户(yuanxiaojian1)及密码：



(12) 验证通过后连接变为蓝色，则说明 VPN 连接成功：

