**VPN服务配置安装文档**

创想空间（北京）有限公司

目录

[**1.** **VPN服务文档说明** 3](#_Toc391562018)

[**2.** **VPN服务使用范围** 3](#_Toc391562019)

[**3.** **VPN服务器拓扑图** 3](#_Toc391562020)

[**4.** **VPN安装环境及服务版本** 4](#_Toc391562021)

[**5.** **VPN隧道技术** 4](#_Toc391562022)

[**5.1点到点隧道隧道协议-PPTP** 4](#_Toc391562023)

[**5.2.第二层隧道协议-L2TP** 4](#_Toc391562024)

[**5.3.IPSec协议** 4](#_Toc391562025)

[**5.4.SOCKS v5协议** 5](#_Toc391562026)

[**6.** **VPN安全技术** 5](#_Toc391562027)

[**6.1认证技术** 5](#_Toc391562028)

[**6.2加密技术** 5](#_Toc391562029)

[**6.3密钥交换和管理** 5](#_Toc391562030)

[**7.** **VPN组网模式** 5](#_Toc391562031)

[**7.1客户端到客户端** 5](#_Toc391562032)

[**7.2 Access VPN （远程访问VPN）：客户端到网关** 5](#_Toc391562033)

[**7.3 Intranet VPN（企业内部VPN）：网关到网关** 5](#_Toc391562034)

**[7.4 Extranet VPN (扩展的企业内部VPN)：与合作伙伴企业网构成的Extranet](#_Toc391562035)** [6](#_Toc391562035)

[**8.** **VPN的基本原理** 6](#_Toc391562036)

[**8.1 VPN的两种类型** 6](#_Toc391562037)

[**8.2 VPN的三种协议：** 6](#_Toc391562038)

[**9.** **VPN服务的安装** 6](#_Toc391562039)

1. **VPN服务文档说明**

本文档主要介绍了，vpn服务器安装，vpn的工作原理及该文档中使用的技术。

1. **VPN服务使用范围**
2. **VPN服务器拓扑图**



拓扑图说明：

1. 基本网络环境：

vpn服务器采用了双网卡，根据远程客户端不同的请求进行不同的数据转发，需要一个网卡连接外网，一个网卡连接内网。

1. 数据包传递过程

* 当不同需求时可能需要在家中，或出差中，或非专线的办公区域，需要vpn连接公司内部服务，如：在家（之后称为A端）中访问公司内网网站（之后称为B端）。则发出需要访问的数据包的目的地址为B端的ip地址。
* 当vpn服务器接收到A端发送的访问数据包时，对其目标地址进行检测，由于数据包目标地址为B端，则发送给B端，在B端看来，该数据的源地址为A端。
* B端会将返回数据进行封包，发送给VPN服务器，vpn同样解包，发现目地地址为远端内部ip。所以通过wan口，将数据通过专用vpn隧道进行数据传出。

1. **VPN安装环境及服务版本**

|  |  |  |
| --- | --- | --- |
| VPN服务器系统 | Windows Enterprise | 2008R2 |
| VPN服务软件 | 路由和远程访问服务 | \* |

1. **VPN隧道技术**

目前隧道技术有4种：只详细介绍目前我们适用的隧道技术。

**5.1点到点隧道隧道协议-PPTP**

此协议将控制包和数据包分开的，控制包采用了tcp控制，数据包先封装在PPP协议中，然后封装到GRE V2协议中，目前此协议已被淘汰，不再单一使用在vpn中。

**5.2.第二层隧道协议-L2TP**

L2TP是国际标准隧道协议，它结合了PPTP协议以第二层转发L2F协议的优点，能以隧道的方式是PPP包通过各种网络，但是L2TP没有任何的加密措施，更多是与IPSec协议结合使用，提供隧道验证。

**5.3.IPSec协议**

IPSec协议工作在OSI模型中的网络层。它提供所有在网络层上的数据保护和透明的安全通信。IPSec协议可以设置成两种模式：一种是隧道模式，一种是传输模式。

隧道模式：把IPv4数据包封装在安全的IP帧中。

传输模式：为了保护端到端的安全性，不会隐藏路由信息，为了IPSec的扩展，在IPSec协议中加上了ISAKMP协议，其中还包括密钥分配协议。

目前大部分vpn使用了IPSec协议保护数据和L2TP隧道协议。

优点：它定义了一套用于保护私有性和完整性的标准协议，可确保在tcp/ip协议上的vpn之间的互相操作性。

缺点：除了包过滤外，他没有指定其他访问控制方法，对于采用nat方式访问公共网络的情况比较难处理。

此服务器最合适可信LAN到LAN之间的vpn。

**5.4.SOCKS v5协议**

SOCKS v5 工作在osi的第五层-会话层，可作为建立高度安全的vpn的基础。该协议的优势在于访问控制，适用与安全性较高的vpn。

优点：非常详细的访问控制，在会话层可控制手段会比网络层多一些，由于工作在会话层，能同低层协议如，ipv4，ipsec，pptp，l2tp一起使用，能为认证，加密和密钥管理提供插件模块。让用户自由的采用自己所需要的技术。Socks v5 可根据规则过滤数据流。

缺点：某些性能比低层次协议差，必须指定更复杂的安全管理策略。

适用场景：最合适用于客户机到服务器的连接模式，适用于客户端vpn和远程访问vpn。

1. **VPN安全技术**

**6.1认证技术**

认证技术防止数据的伪造和被篡改，它采用一种称为摘要技术，主要采用HASH（哈希）函数将一段长的豹纹通过函数变换，映射为一段短的报文摘要。由于HASH函数的特性，两个不同的报文具有相同的摘要几乎不可能。该特性使得摘要技术在vpn中的用途：验证数据的完整性，用户认证。

**6.2加密技术**

IPSec 通过ISAKMP/IKE/Oakley协议确定几种可选的数据加密算法，如DES,3DES等。DES密钥长度为56位，容易被破解，3DES采用了三重加密在大大加大了安全性。当然还有其他更严格和更安全的加密方式，但是均被企业或国家部门使用。

**6.3密钥交换和管理**

vpn密钥分发有两种方法：1.通过手动配置的方式，2.采用密钥交换协议动态分发。手工配置的方法由于密钥，适合于复杂网络的情况且密钥可快速更新，可以提高vpn的安全性。目前主要的密钥交换与管理标准有IKE(互联网密钥交换)，SKIP(互联网简单密钥管理)和Oakley。

1. **VPN组网模式**

**7.1客户端到客户端**

**7.2 Access VPN （远程访问VPN）：客户端到网关**

远程用户拨号接入到本地的isp，使用与流动性人员远程办公，可降低电话拨号的费用，SOCKS v5 协议适合这类连接。

**7.3 Intranet VPN（企业内部VPN）：网关到网关**

适用与公司异地机构或部门的局域网连接，在internet上组建世界范围内的企业网，利用internet的线路保证网络的互联性，而且用隧道，加密等vpn特性可以保证信息在整个intranet VPN上安全传输。IPSec隧道协议可满足所有网关到网关的VPN连接。

**7.4 Extranet VPN (扩展的企业内部VPN)：与合作伙伴企业网构成的Extranet**

因不同公司的网络会出现相互通信的情况，所以要考虑更多设备的互联，地址协调，安全策略的协商问题。它也属于网关到网关的连接。

1. **VPN的基本原理**

**8.1 VPN的两种类型**

* **拨号式连接VPN**：是客户端通过拨号或ip连接的方式连接至VPN网关。
* **专用式VPN**：是通过网关到网关的一种连接方式，专用VPN通常适用与多个帐号进行连接。

**8.2 VPN的三种协议：**

* **MPLS**: 是一种基于MPLS技术的IP VPN。是在网络路由和交换设备上应用MPLS（多协议标记交换）技术，简化核心路由器的路由选择方式。利用结合传统路由技术标记交换，实现ip虚拟专用网络(IP VPN)。这种基于标记的ip路由选择方式，需要整个交换网络中间所有路由器都识别这个标签，会出现不同运营商之间没有协调好，标签无法交换的问题。
* **SSL:** 一般该方式vpn是在企业防火墙的后方，放置一个SSL代理服务器，如果用户希望那个安全的连接到公司网络上，那么当用户在浏览器上输入URL后，连接将被SSL代理服务器取得，并验证身份信息，然后代理服务器将提供一个远程用户和各种不同的应用服务器之间连接。
* **IPSec：**该协议类似于包过滤防火墙，可以看作是对包过滤防火墙的一种扩展。当接收到一个ip数据包时，包过滤防火墙使用其头部在一个规则表进行匹配。二档找到一个相匹配的规则时，包过滤防火墙就按照该规则指定的方法对接收ip数据包进行处理。处理只有两种结果：丢弃或转发。

1. **VPN服务的安装**

**9.1. vpn服务的基本环境**：

* **搭载服务系统**：windows 2008 R2 标准版
* **网络环境**：物理网卡两块。
* **帐号认证**：使用公司域帐号认证。
* **网络连接策略**：使用NSP服务进行连接认证。
* **证书认证：**使用CA服务颁发证书。

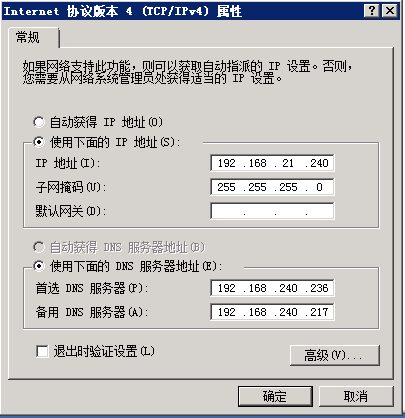
**9.2准备vpn服务的基本环境：**

* **安装服务器系统**：

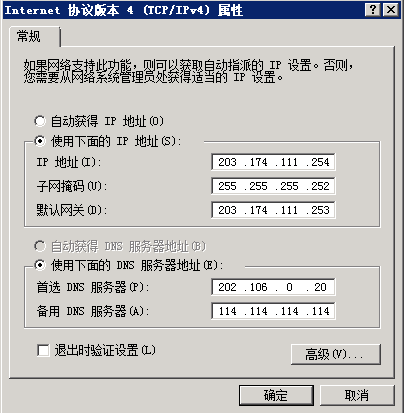
请参考《windows2008系统安装》

* **网络设置：**
* **内网ip地址设置：**（注意：内网设置是没有网关的，且需要指定域服务器网段的路由地址，才能内网互通。）
* **加入域服务器网段路由：**

route add 192.168.240.0 mask 255.255.255.0 192.168.21.254 metric 1 -p

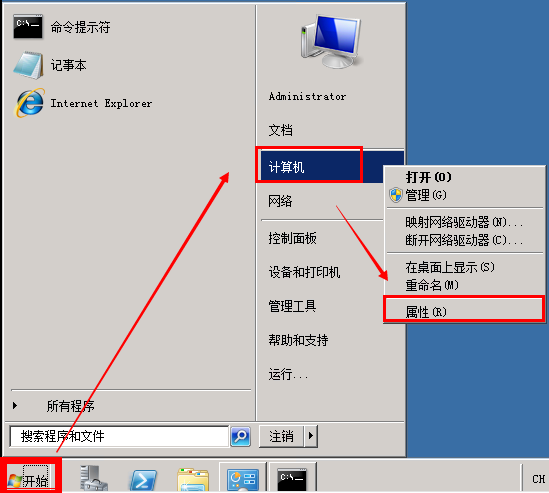


* **外网ip地址设置**



* **将vpn服务器加入域环境：**

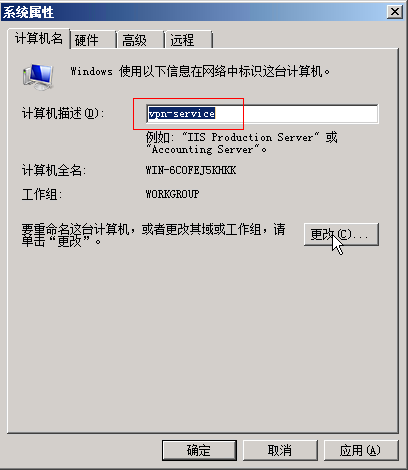
1. 找到计算机，右键“**属性**”。



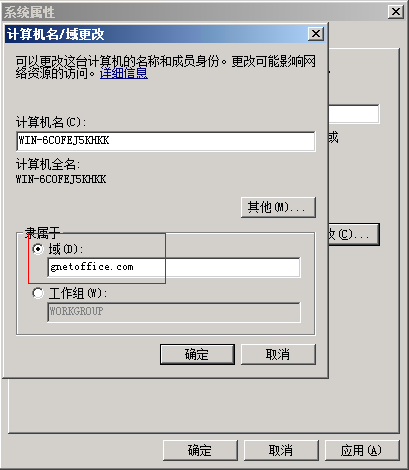
2.找到计算机名“**更改设置**”选项



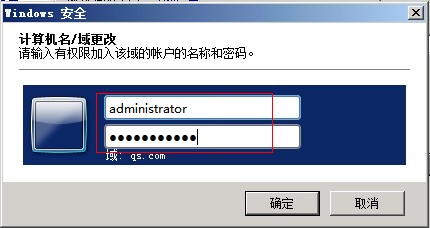
3.建议更改计算机描述，这样你能更方便的在域环境中找到你的计算机。



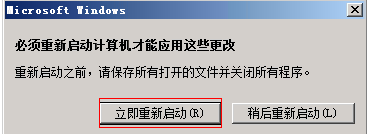
4.选择更改：选择隶属于“**域**”，并输入域的URL。



5. 点击“**确定**”，需要帐号认证，输入管理员帐号或管理组中的帐号，登录并授权。



6. 加入成功后，需要重新启动服务。重启结束后，加入域完成。



* **网络连接策略：**

请参考NPS服务安装文档。

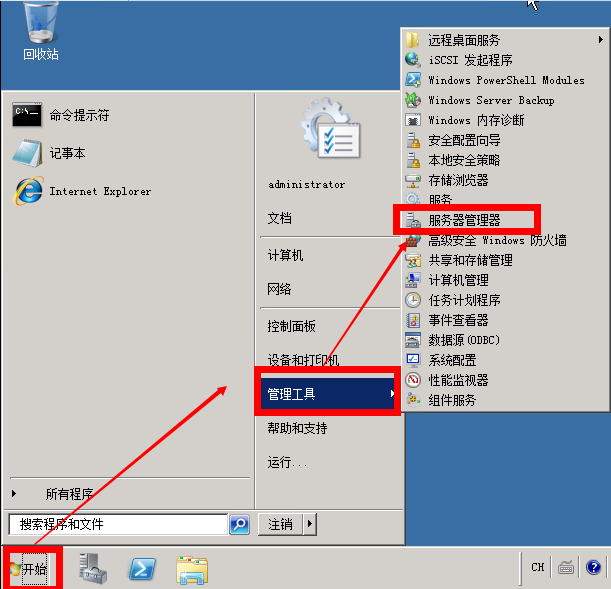
* **证书颁发服务：**

请参考CA服务安装文档。

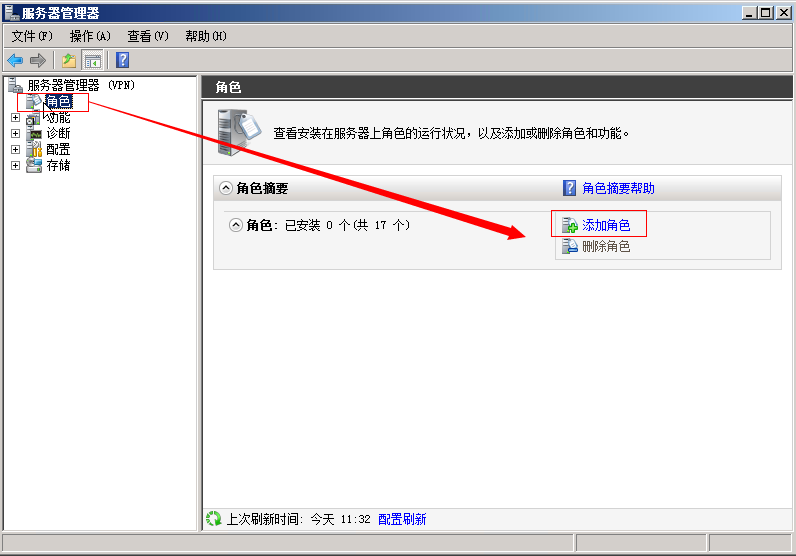
**9.3安装并配置VPN服务：**

* **安装网络策略和远程访问服务**

1.打开“**服务器管理器**”；



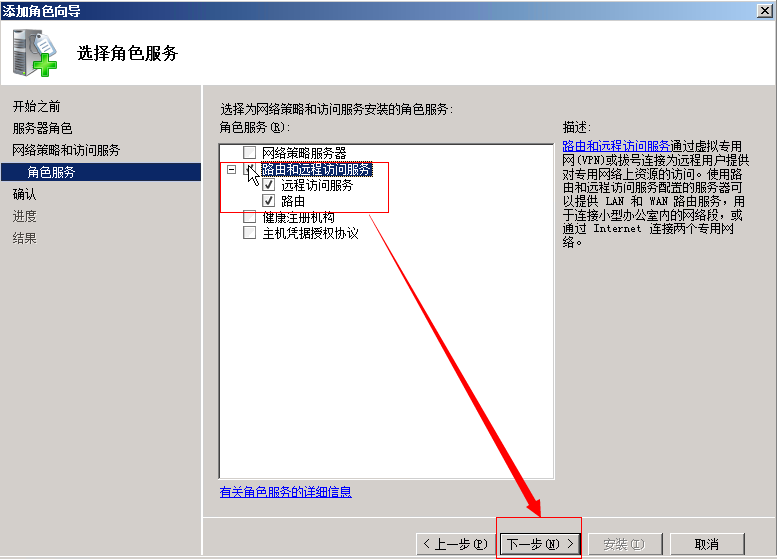
2.选择“**角色**”，“**添加角色**”；



3.选择vpn服务“**网络策略和访问服务**”。

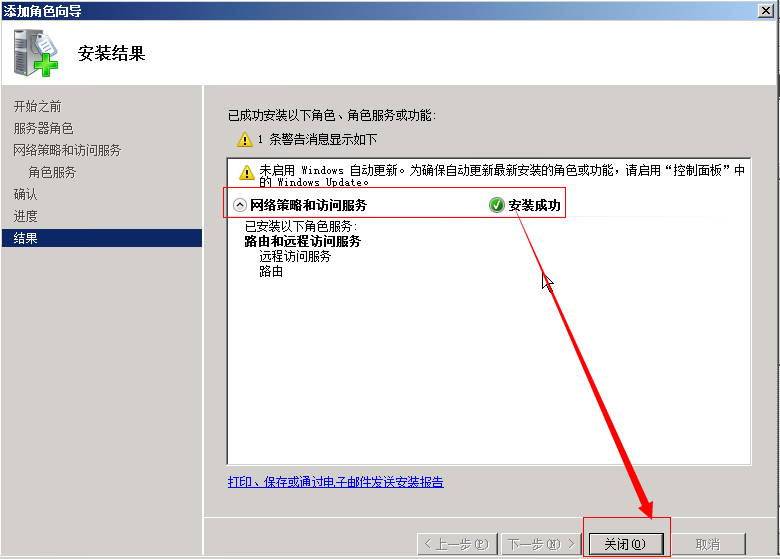


4．勾选需要安装的角色服务“**路由远程访问服务**”。



5.点击安装，等待安装完成，**关闭**；

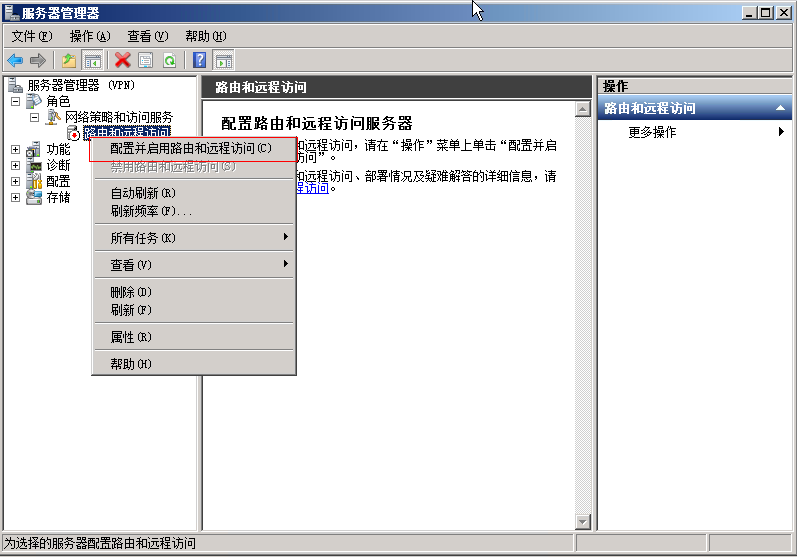




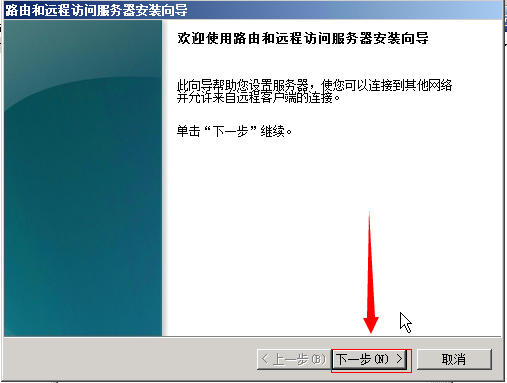
* **配置路由和远程访问；**

1.选择“**路由和远程访问**”，右键“**配置并启用远程访问**”；

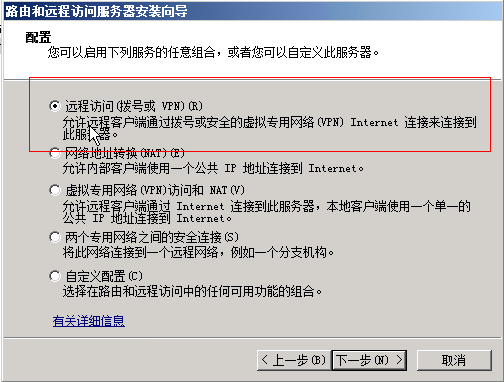




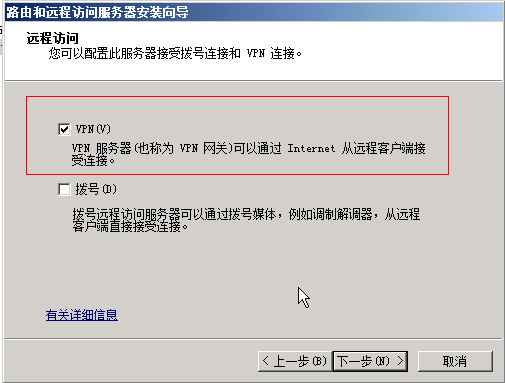
1. 根据配置向导提示选择**下一步**；



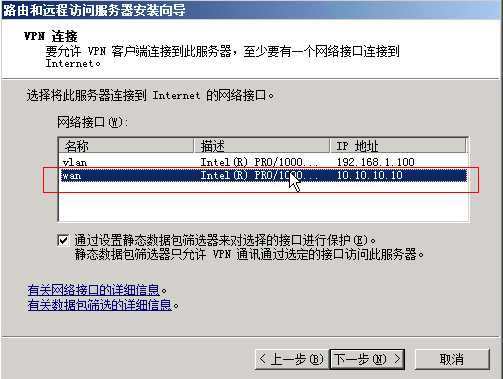
1. 选择远程访问启用的功能。选择“**远程访问（拨号或vpn）**”；



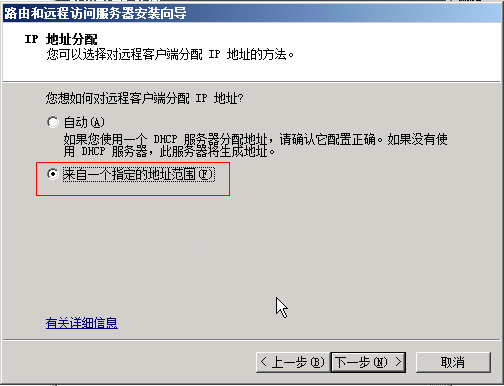
1. **勾选vpn**，目前拨号几乎很少会使用。选择**下一步**；

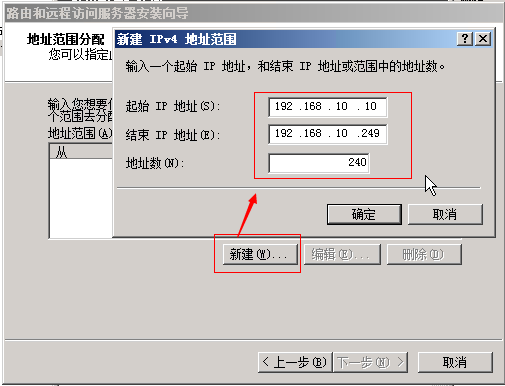


1. 选择连接外网的网卡接口，根据自己标识外网网卡进行选择；

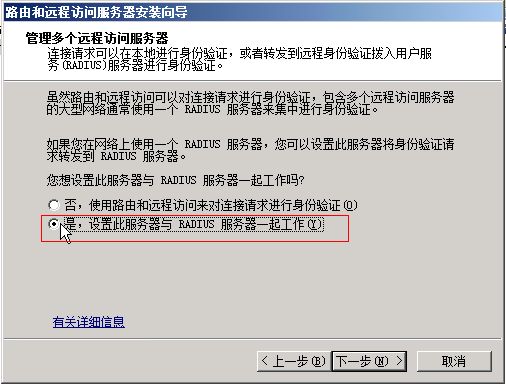


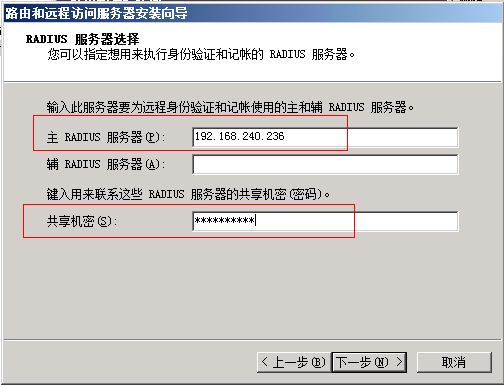
1. 配置远程连接后获取虚拟ip地址，选择“**来自一个指定的地址范围**”这里使用本服务分配地址，并指定ip段，确保该段ip未在内网中被使用。



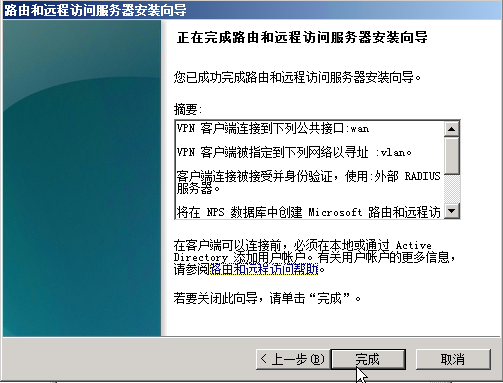


1. 配置使用RADIUS服务进行帐号认证。输入RADIUS服务器地址和共享密钥。





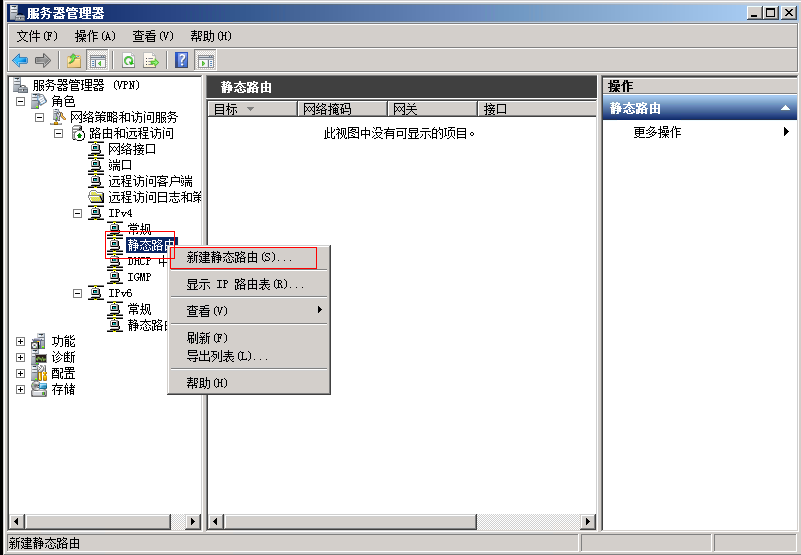
1. 配置完成。



* **添加服务静态路由：**

注意选择网卡接口，这里设置静态路由因，内网网卡没有网关，除了此方法，也可在系统中直接加入路由表。

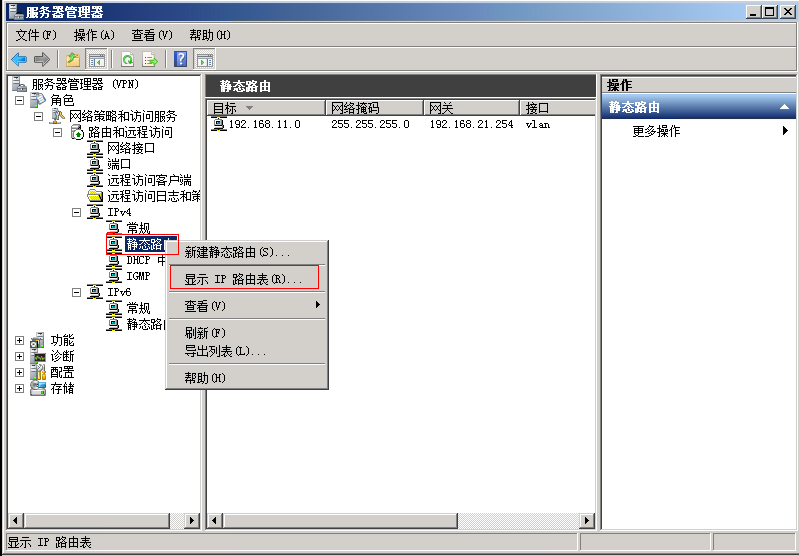
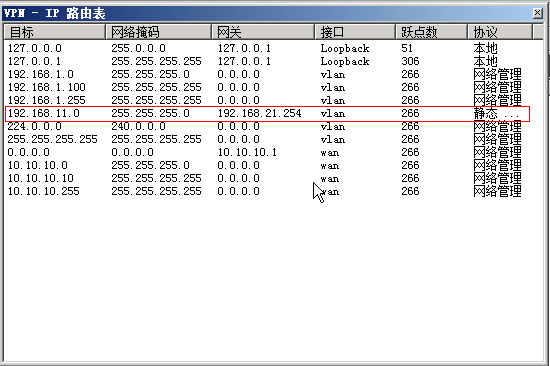
1.选择“**静态路由**”，“**右键新建静态路由**”；添加目标网段并指定路由网关；





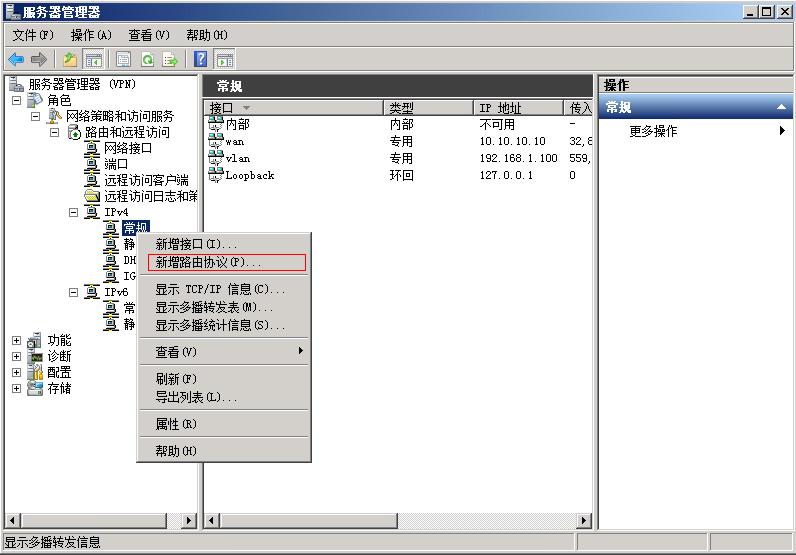
2.如何查看已有的路由表；

选择“**静态路由**”，右键选择“**显示ip路由表**”，你会看到刚刚加入的路由条目；

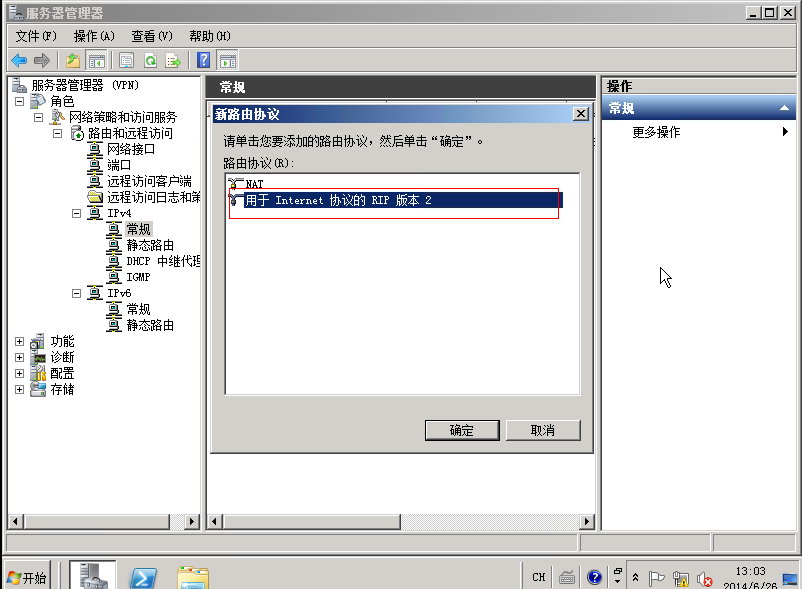
  


* **添加路由RIP协议。**

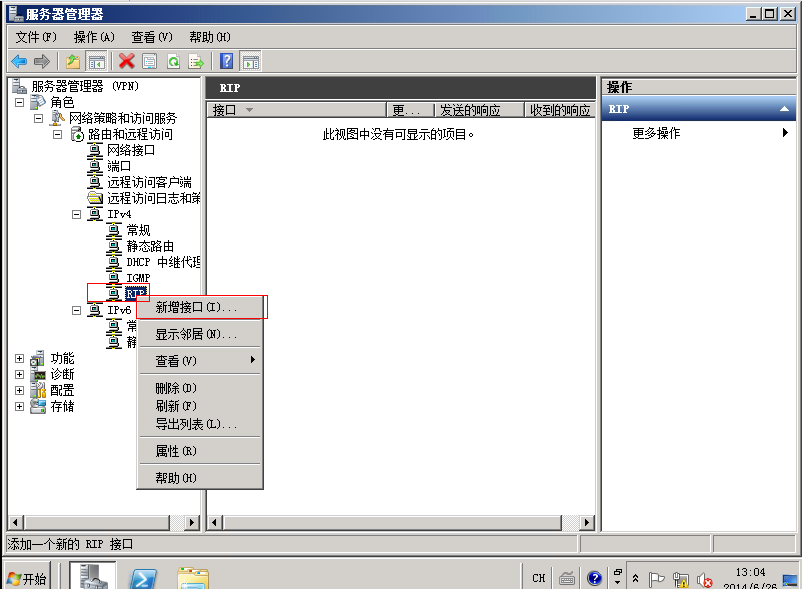
1.选择“**常规**”，右键“**新增路由协议**”

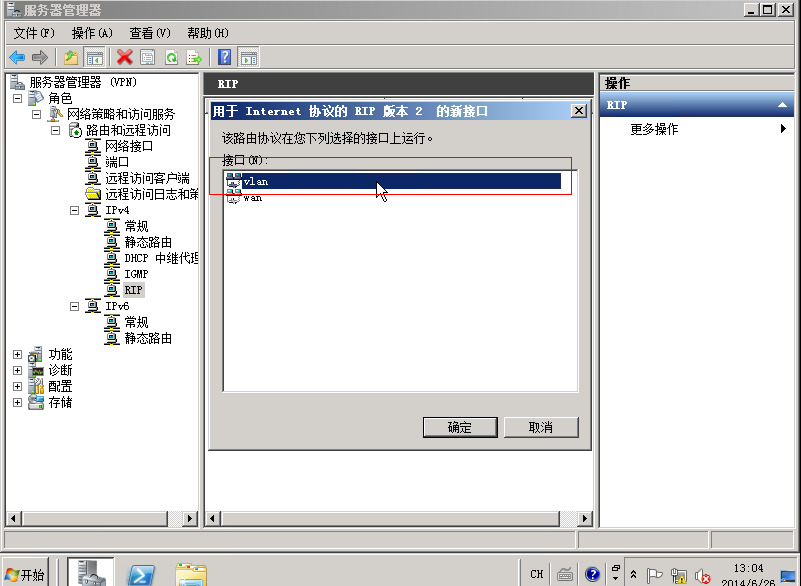


2.选择“**用于internet协议的RIP版本2**”选项；



3.选择RIP，选择“**新增接口**”；并将内网网卡启用该协议；

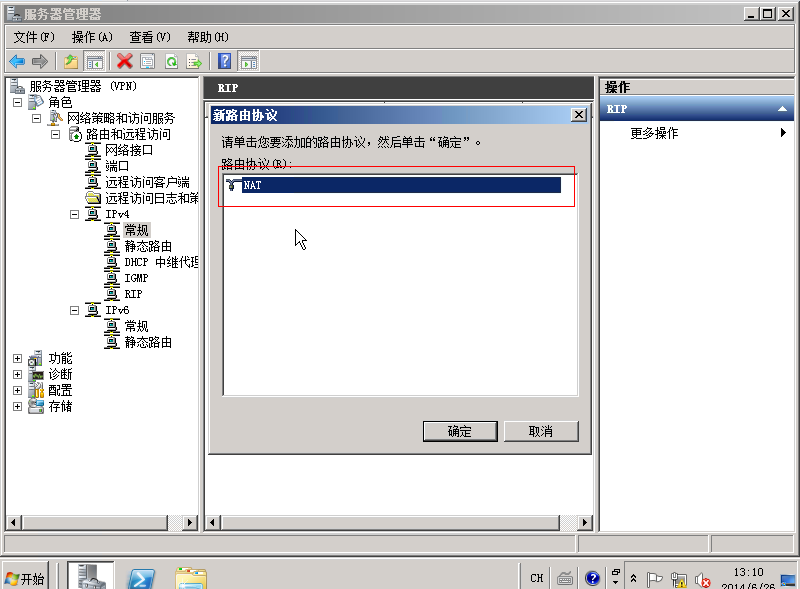




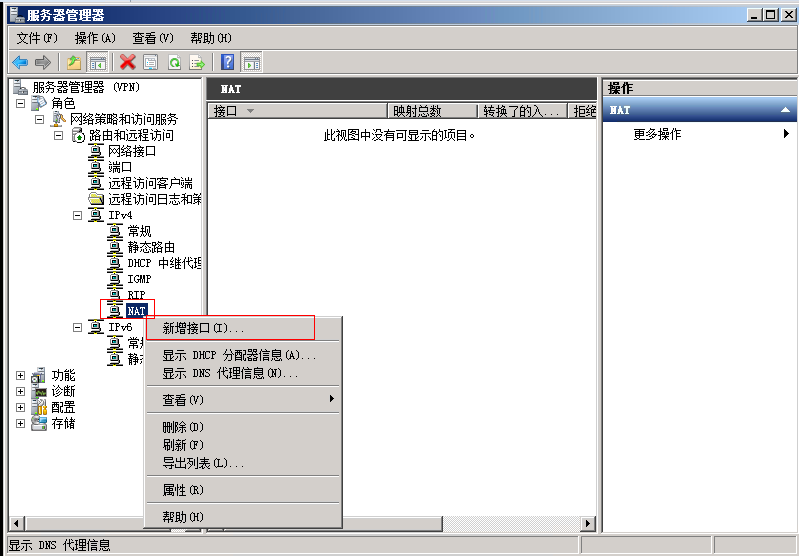
* **配置启用NAT协议**

启用NAT协议，支持远程连接后通过外网网卡进行数据转换。

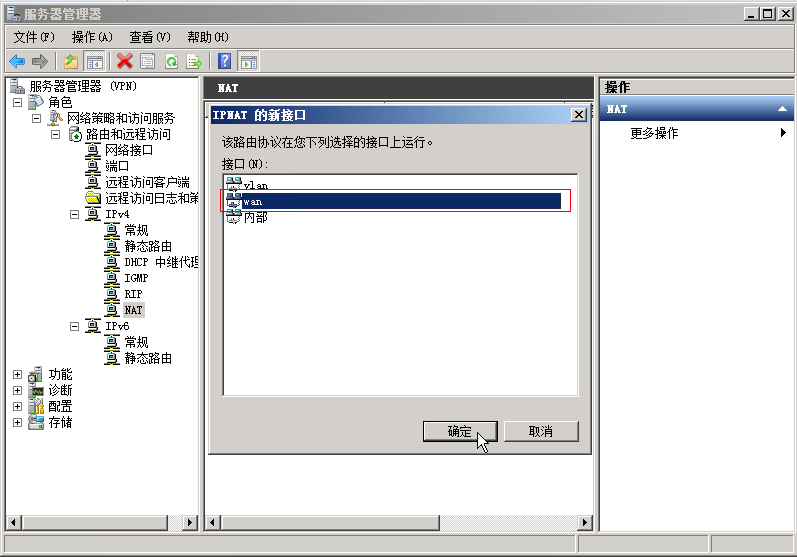
1.选择“**常规**”添加新路由协议，添加“**NAT协议**”；



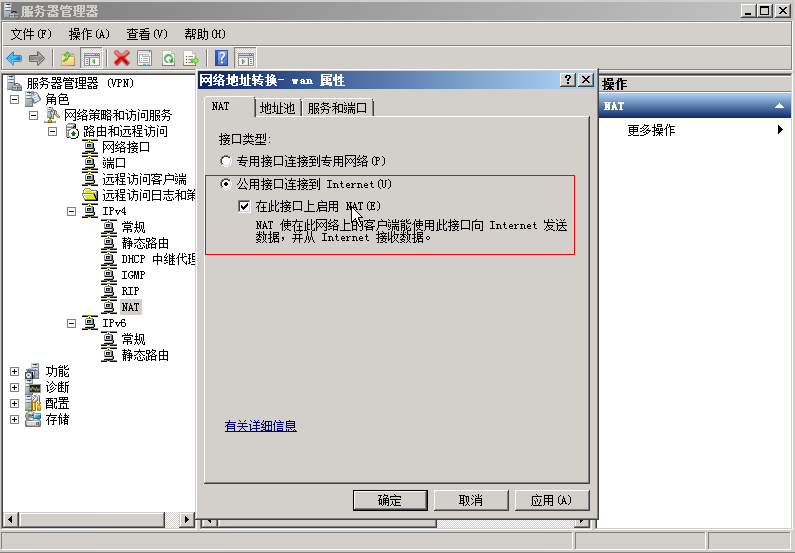
2.选择“**NAT**”右键选择“**新增接口**”



3.选择需要做NAT转换的接口；



4.启用公网数据进行NAT转换，选择“公用接口连接到Internet”，同时勾选“在此接口上启用NAT”。



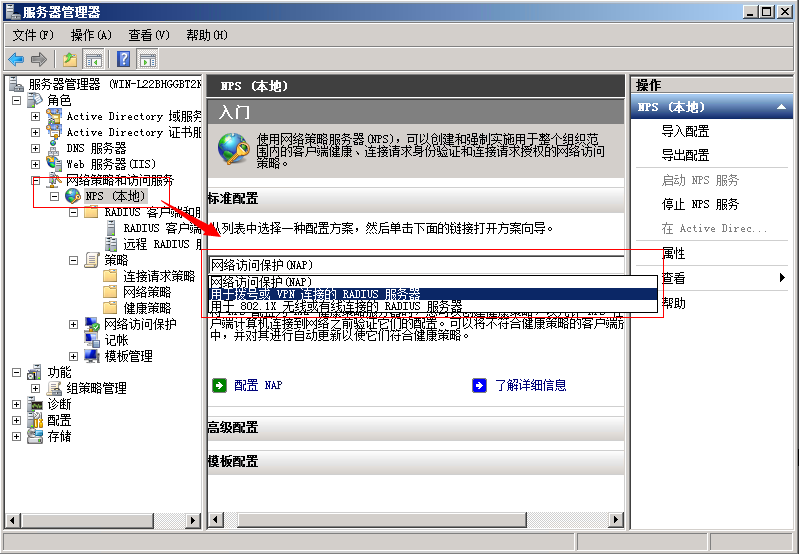
**9.4配置NPS服务**

* **新建vpn使用NPS服务**；

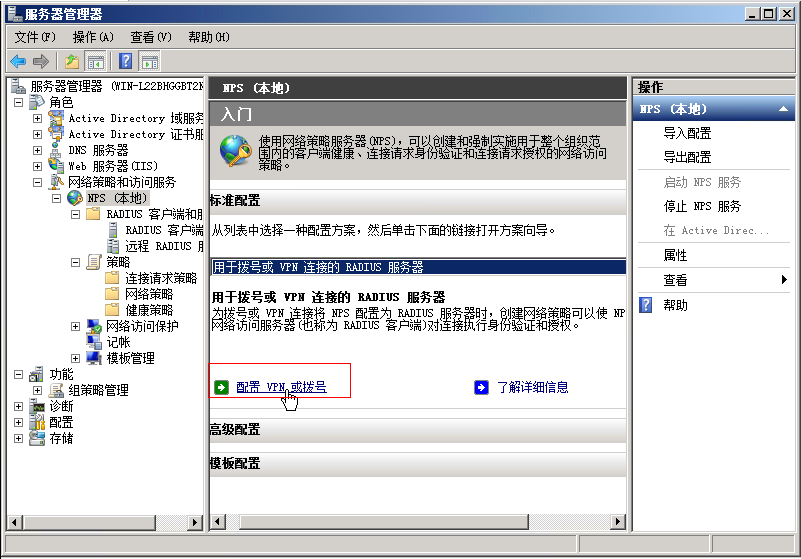
1.在NPS服务器上找到NPS服务选项；



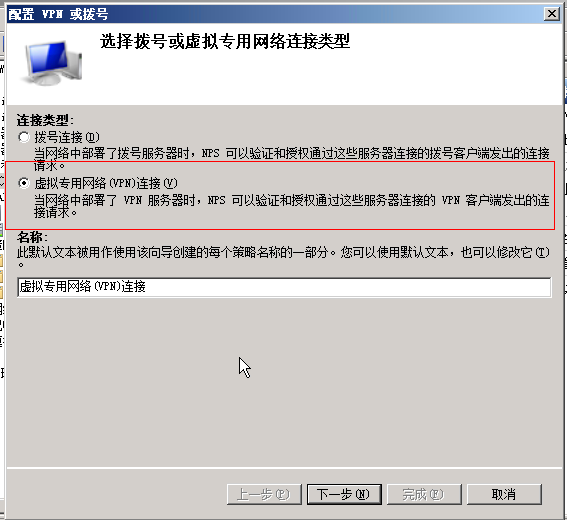
2.选择“**NPS（本地）**”，选择“**用于拨号或vpn连接的RADIUS服务器**”；



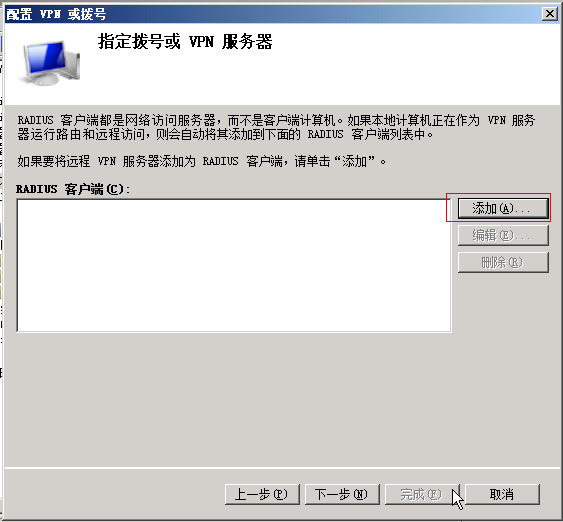
3．选择“**配置vpn或拨号**”

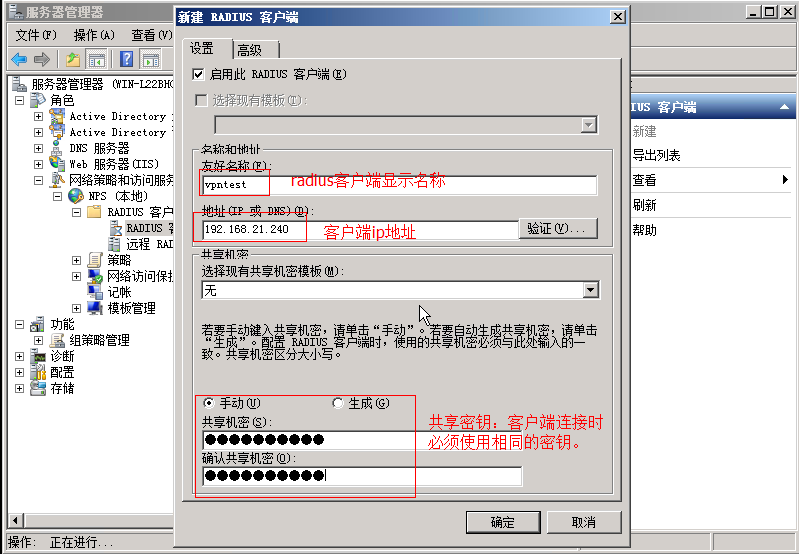


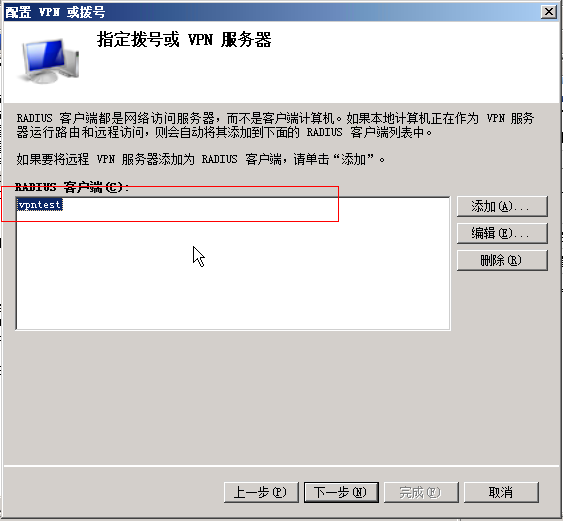
4.选择vpn类型，选择“**虚拟专用网络（VPN）连接**”；名称可根据需求自行填写；



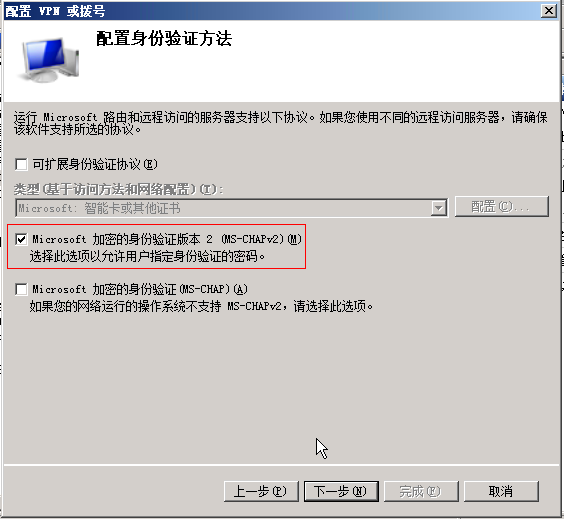
5.添加RADIUS客户端；选择“**添加**”；根据图片提示填写相应的内容；



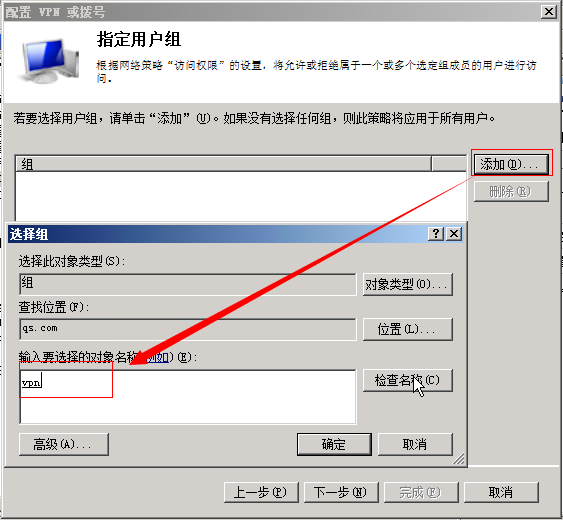




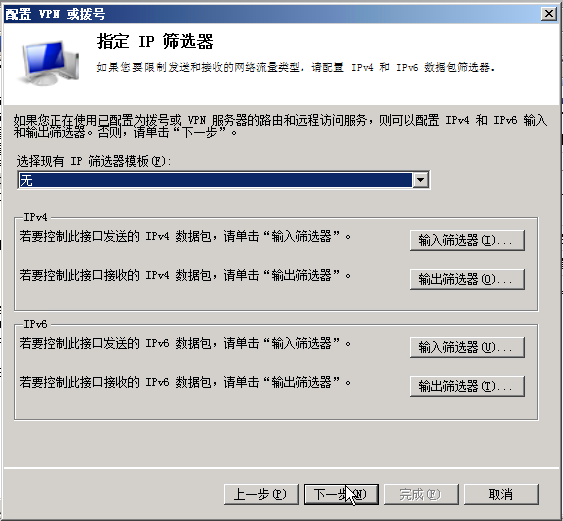
6.选择什么验证的方法，若无特殊要求，默认选择即可；



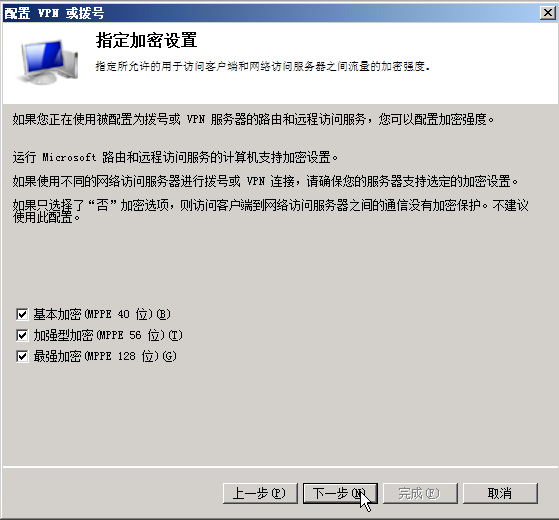
7.添加需要认证的帐号或组；选择“**添加**”，查找到相应的帐号组；



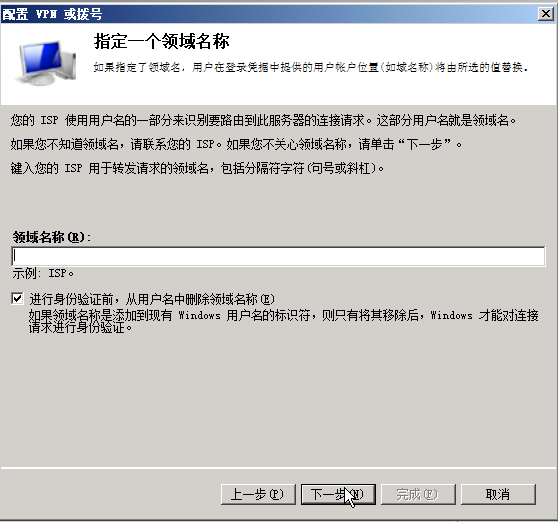
8.筛选器选择方法，默认不进行筛选；请根据需求配置。



9.配置通道和数据加密方式，默认三项都要选择；因为不同的客户端支持不同的加密方式。



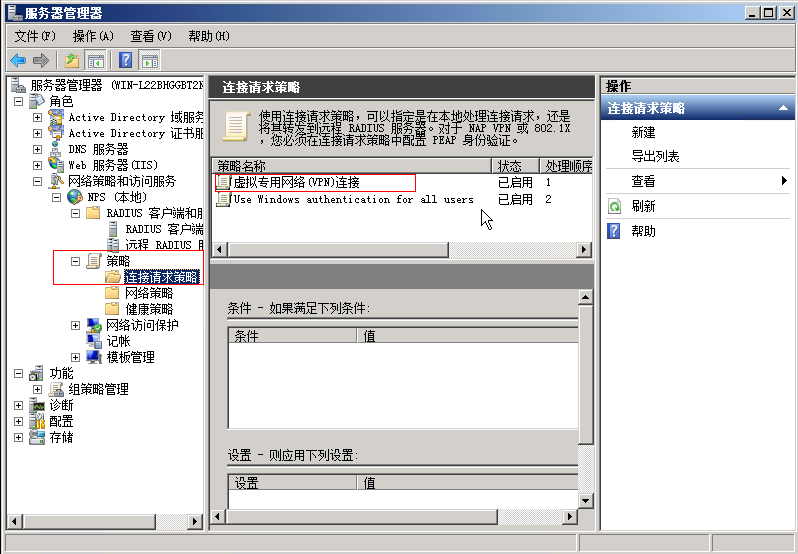
10.指定isp领域名称，默认无需指定，直接下一步完成；NPS监控VPN服务连接创建完成。

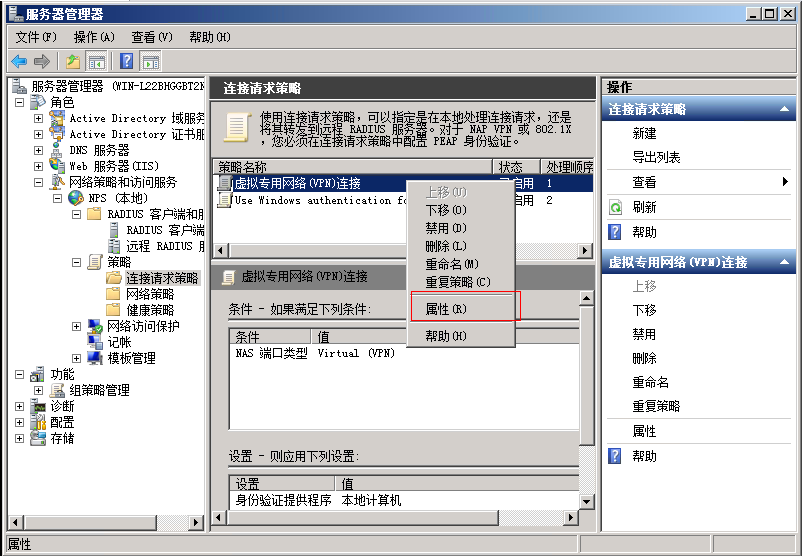




* **配置NPS策略**
* 配置vpn连接策略；

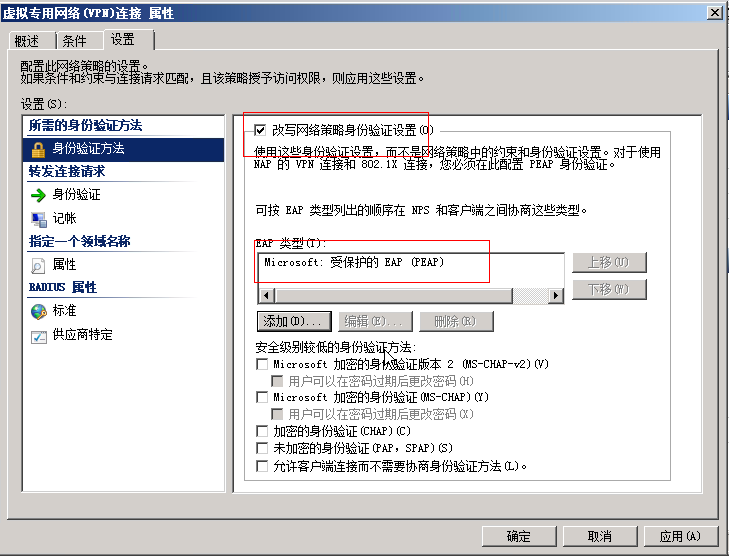
1.选择虚拟专用网络VPN连接，右键“**属性**”；





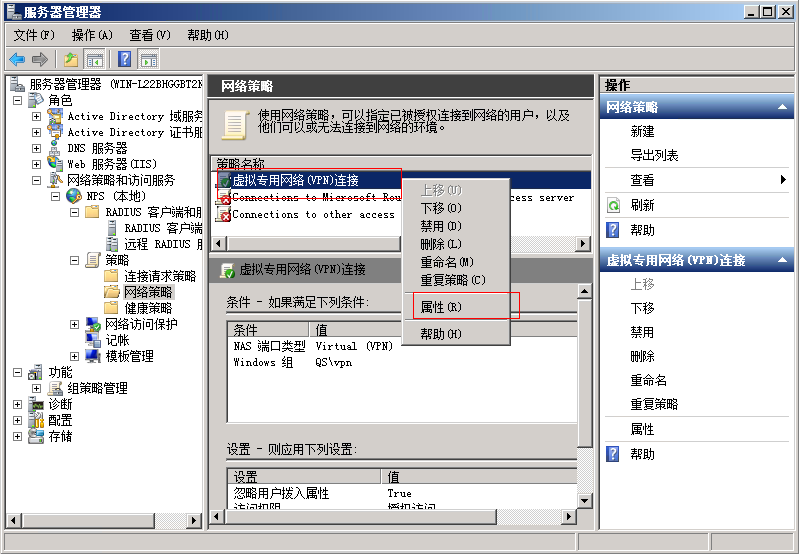
2．选择“**设置**”选项卡，勾选“**改写网络策略身份验证设置**”；并添加“**EAP类型**”；

若安全级别较低的身份验证方法不勾选，手机客户端或ipad客户端无法连接vpn。

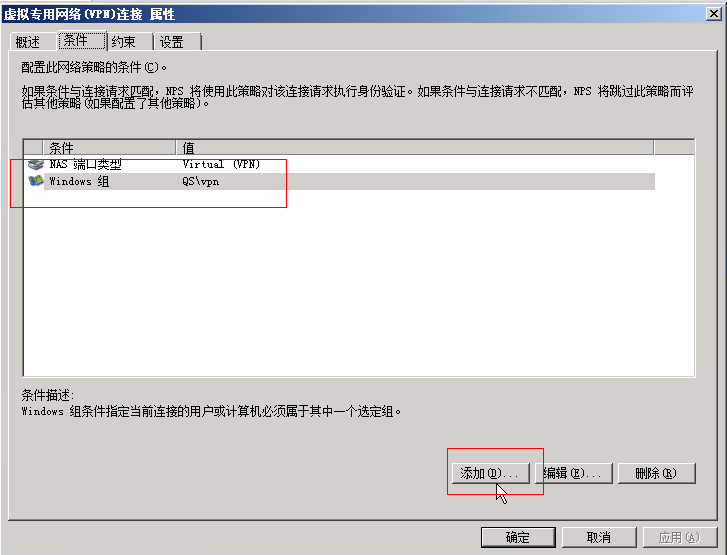


* 配置网络策略

1.选择“**虚拟专用网络（VPN）连接**”；右键“**属性**”；



2.选择“**条件**”选项卡，可添加认证组，和认证帐号。



3.选择“**约束**”，并让身份验证方法，结合请求连接，选择“**EAP类型**”。若连接请求和约束不匹配，则拒绝访问。

