LAB 13 – RADIUS QUẢN LÝ VPN

1. **Chuẩn bị**

   Một máy DC làm file server, một máy radius server, và một máy VPN server

2. **Tiến hành**

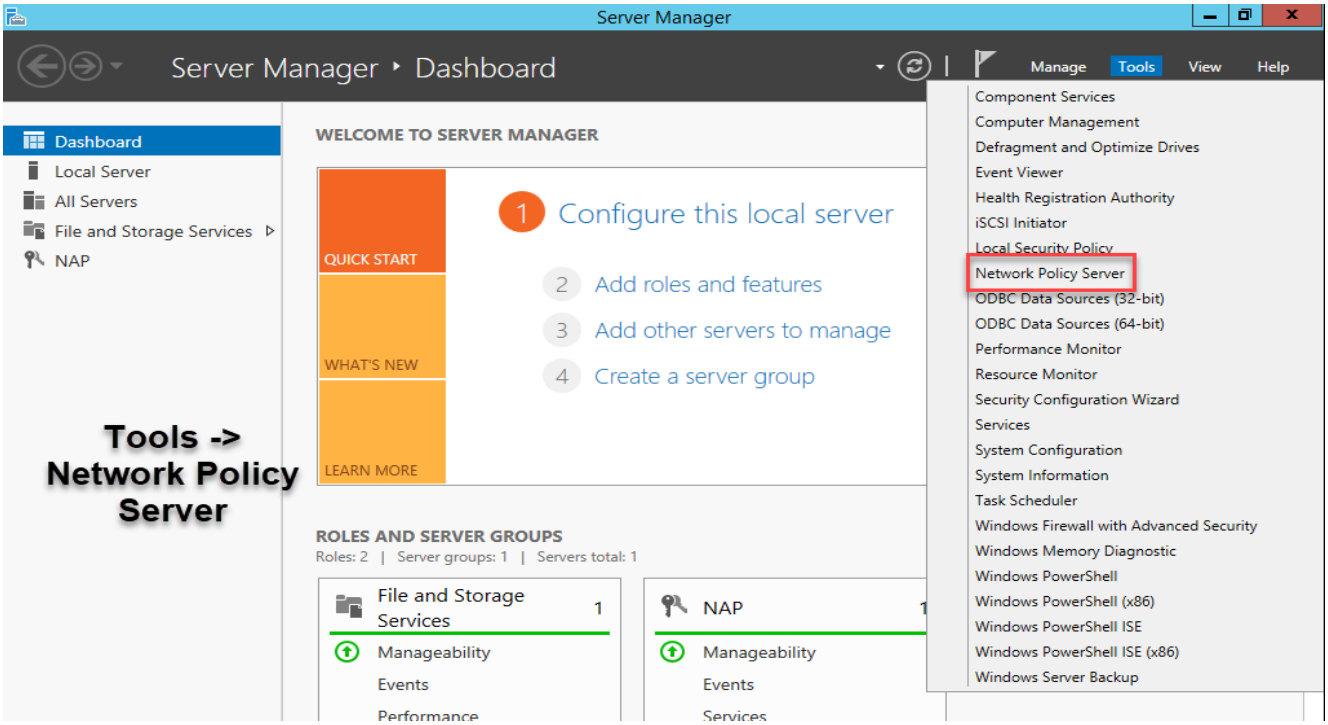
   + Máy DC tạo thư mục share và các user group.

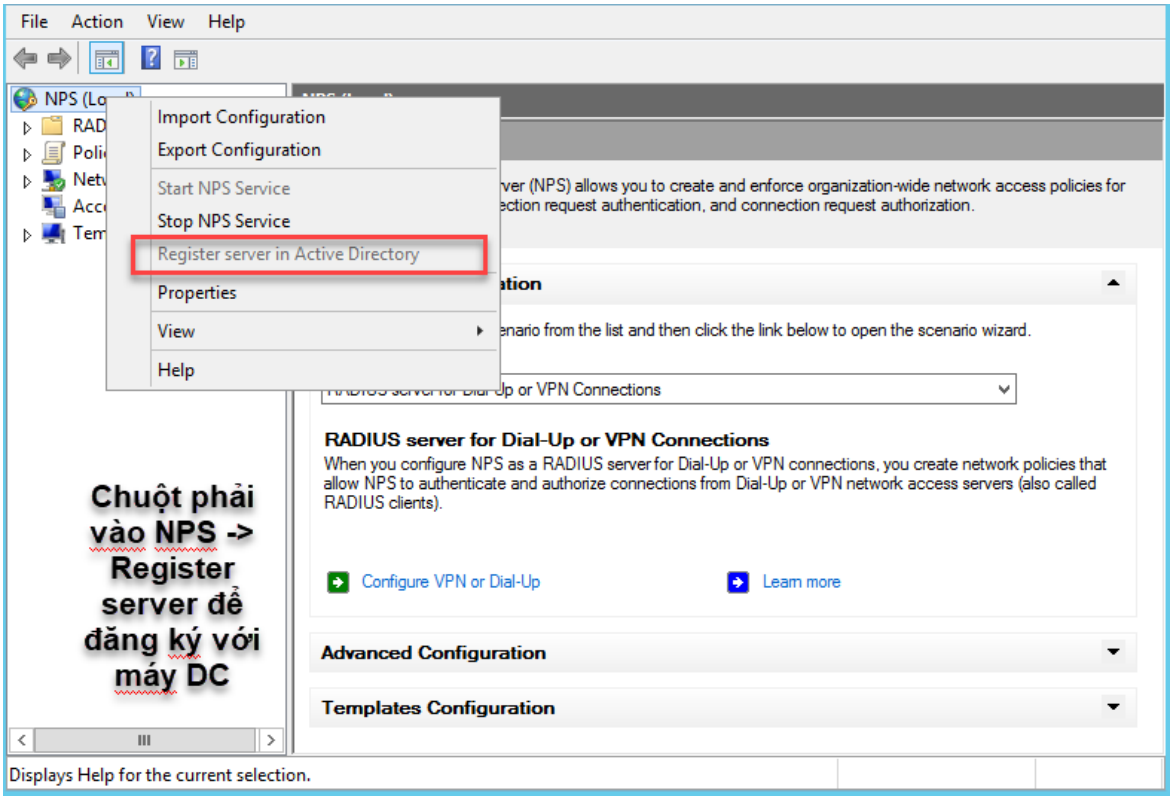
   + Máy Radius server join domain và tiến hành cài dịch vụ Network Policy and Access services như bài lab trước.

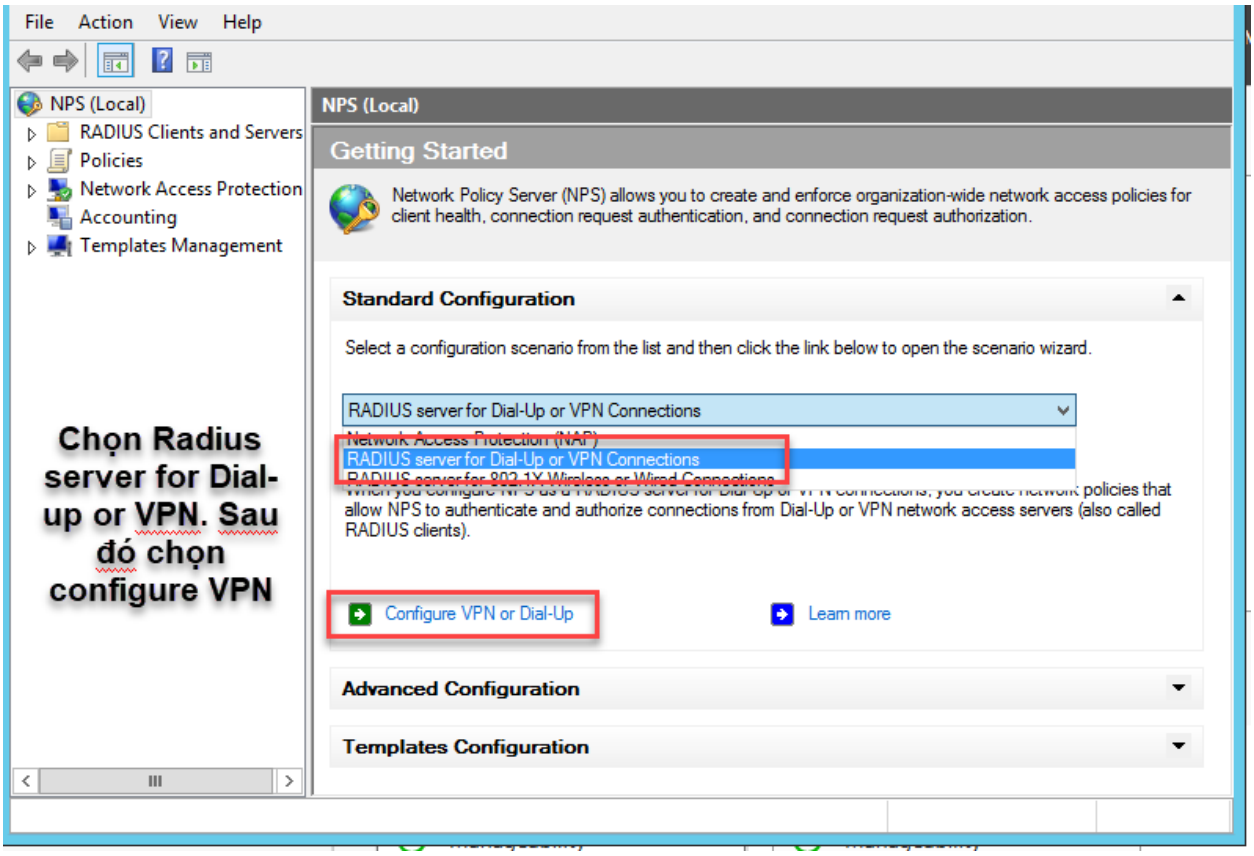
   + Trên máy VPN server tiến hành cài dịch vụ Remote Access. Máy VPN server phải có 2 card mạng một nối với DC và Radius sv, 1 card mạng nối ra internet.

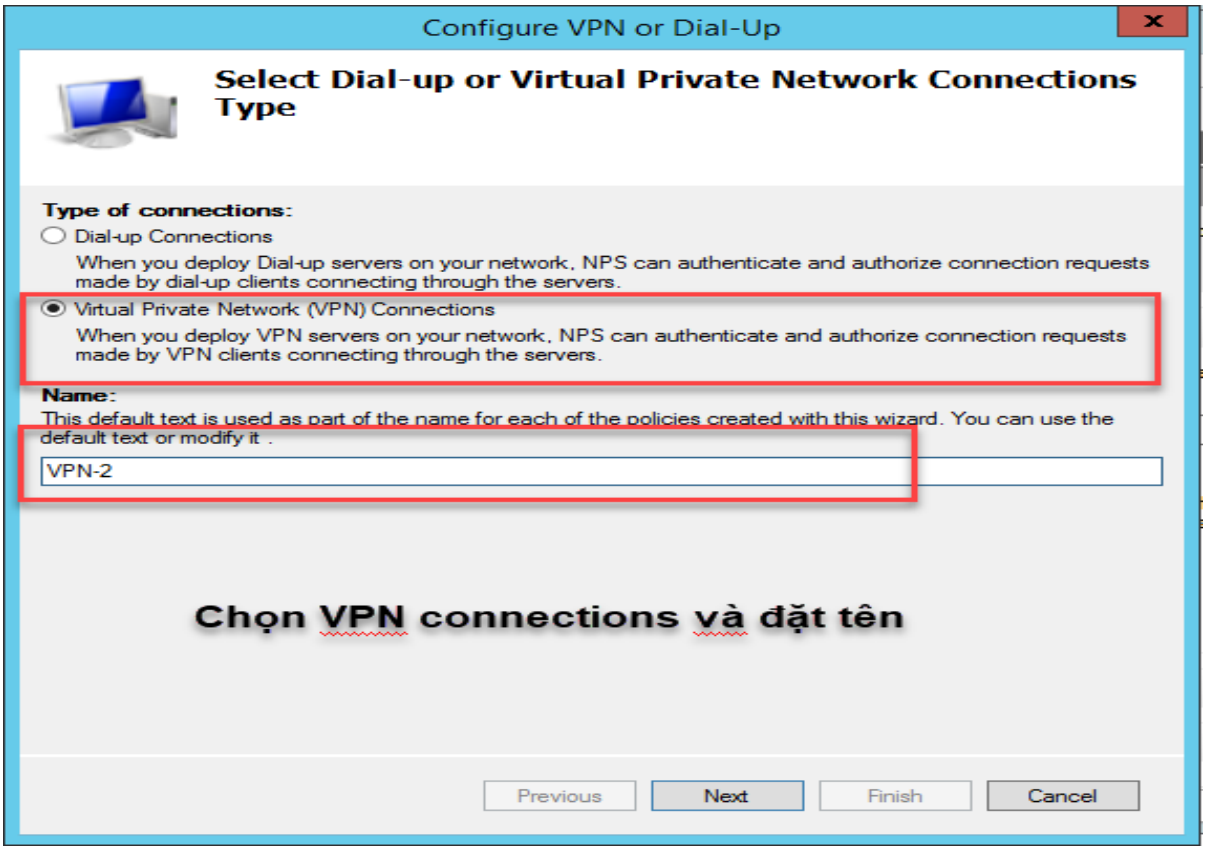
   + Sau khi cài xong các dịch vụ ta tiến hành cấu hình.

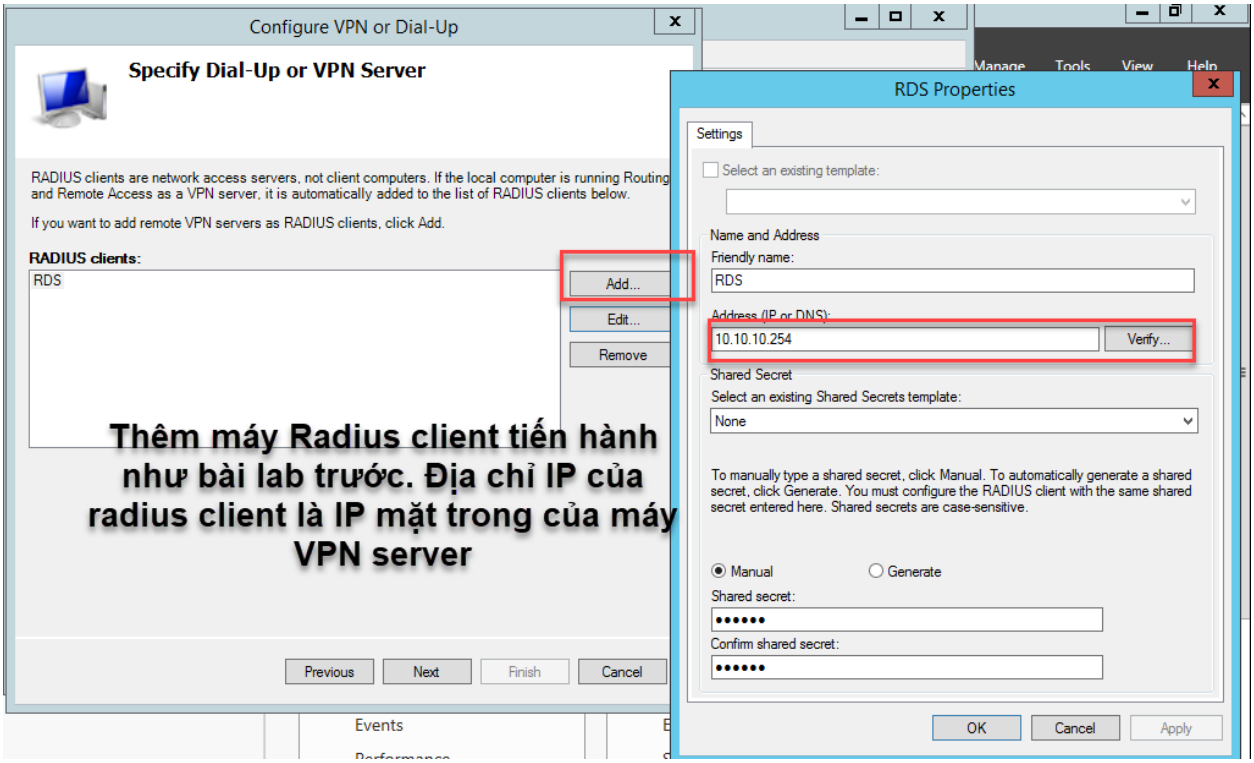
   Trên máy Radius server:

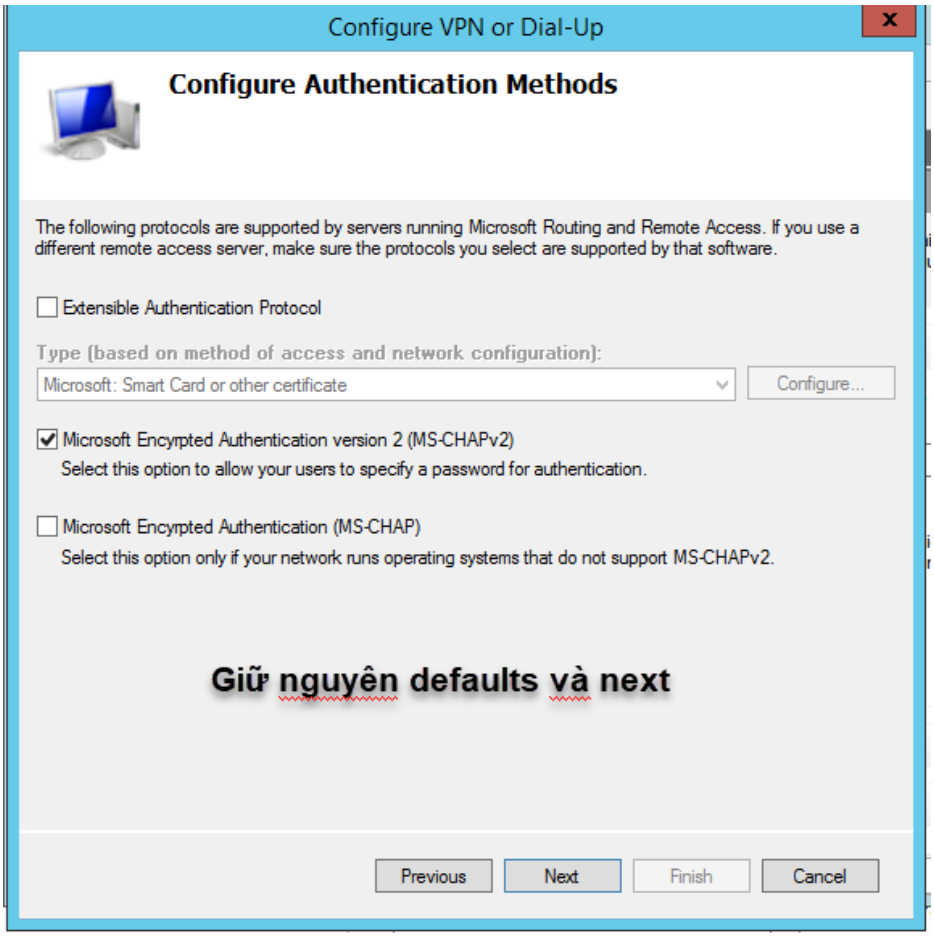


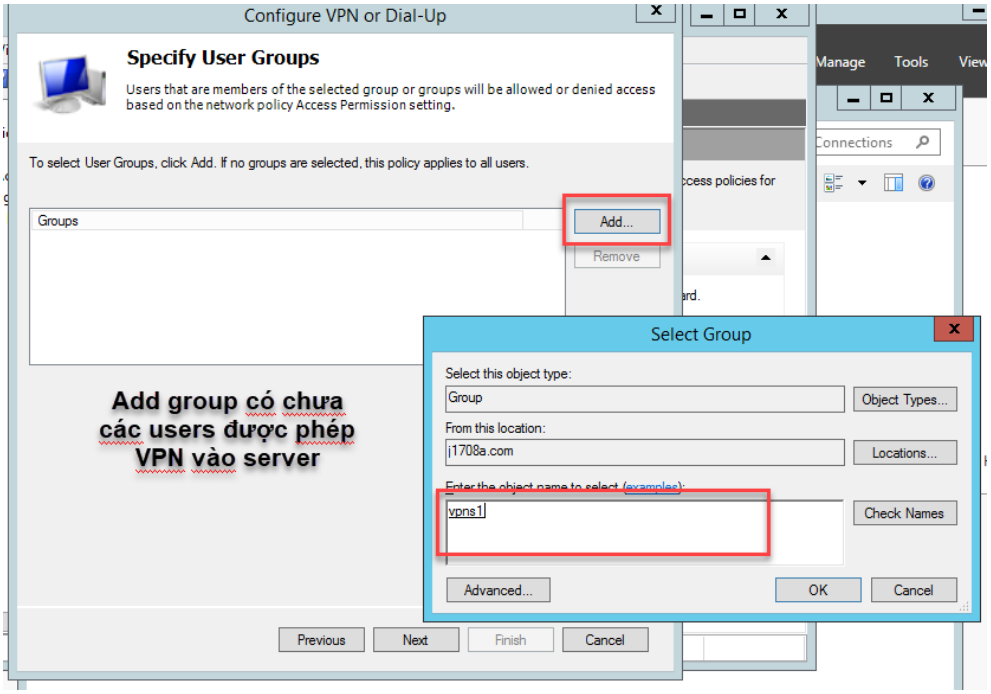

File Action View Help
Import Configuration
Export Configuration
Start NPS Service
Stop NPS Service
Register server in Active Directory
Properties
View
Help
Chuột phải vào NPS -> Register server để đăng ký với máy DC
RADIUS server for Dial-Up or VPN Connections
When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).
Configure VPN or Dial-Up
Learn more
Advanced Configuration
Templates Configuration
Displays Help for the current selection.

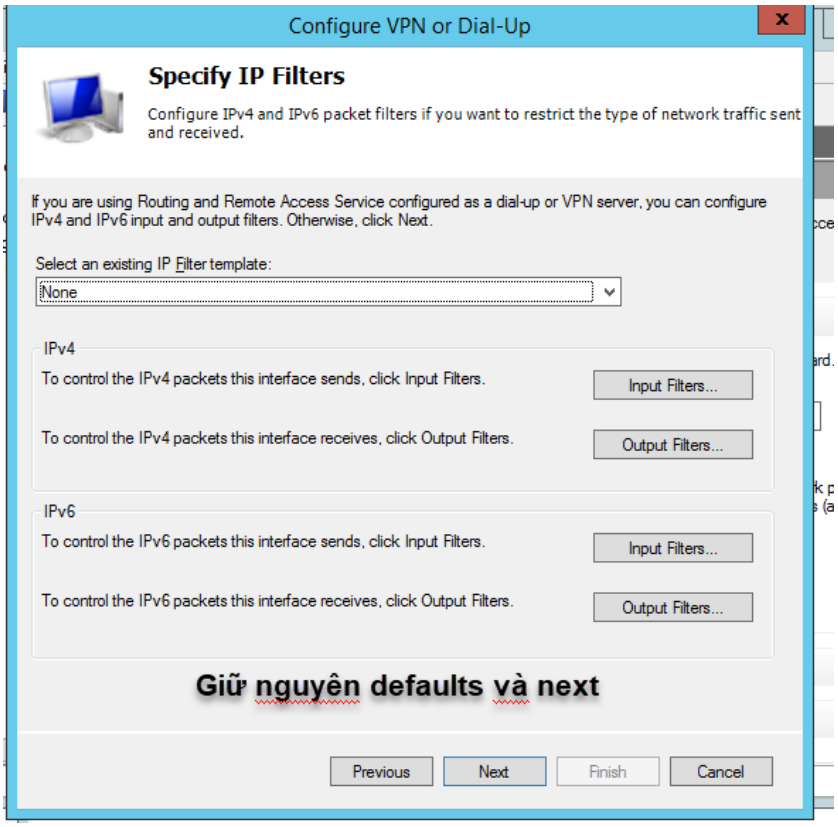

File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Network Access Protection
Accounting
Templates Management
Getting Started
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.
Standard Configuration
Select a configuration scenario from the list and then click the link below to open the scenario wizard.
RADIUS server for Dial-Up or VPN Connections
Network Access Protection (NAP)
RADIUS server for Dial-Up or VPN Connections
RADIUS server for 802.1X Wireless or Wired Connections
Chọn Radius server for Dial-up or VPN. Sau đó chọn configure VPN
allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).
Configure VPN or Dial-Up
Learn more
Advanced Configuration
Templates Configuration


Configure VPN or Dial-Up
Select Dial-up or Virtual Private Network Connections Type
Type of connections:
Dial-up Connections
When you deploy Dial-up servers on your network, NPS can authenticate and authorize connection requests made by dial-up clients connecting through the servers.
Virtual Private Network (VPN) Connections
When you deploy VPN servers on your network, NPS can authenticate and authorize connection requests made by VPN clients connecting through the servers.
Name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .
VPN-2
Chọn VPN connections và đặt tên
Previous
Next
Finish
Cancel

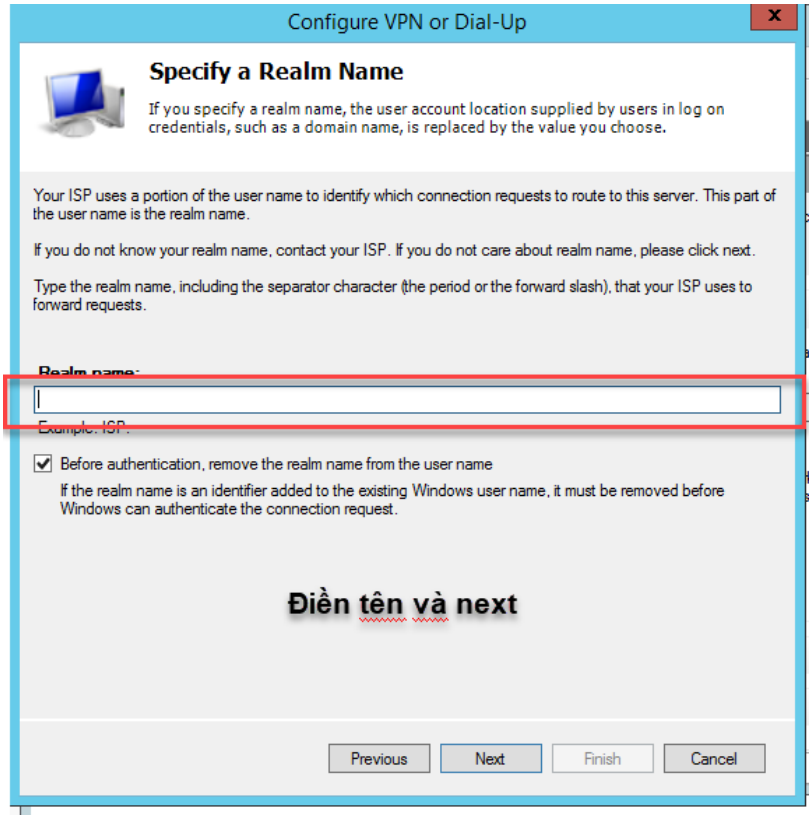

Configure VPN or Dial-Up
Specify Dial-Up or VPN Server
RADIUS clients are network access servers, not client computers. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients below.
If you want to add remote VPN servers as RADIUS clients, click Add.
RADIUS clients:
RDS
Add...
Edit...
Remove
Thêm máy Radius client tiến hành như bài lab trước. Địa chỉ IP của radius client là IP mặt trong của máy VPN server
Previous
Next
Finish
Cancel
RDS Properties
Settings
Select an existing template:
Name and Address
Friendly name:
RDS
Address (IP or DNS):
10.10.10.254
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Apply
Events

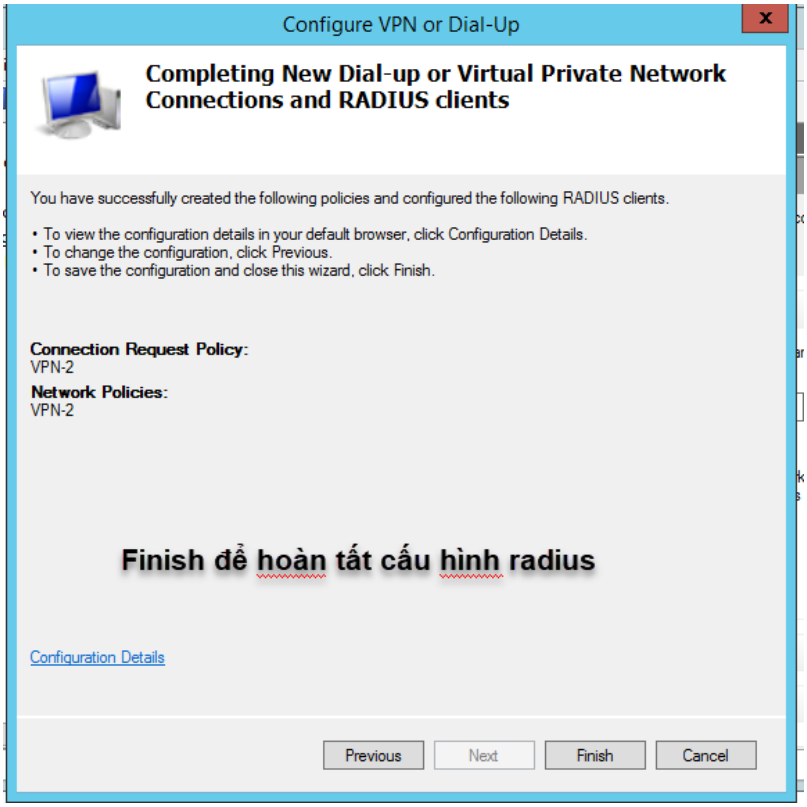

Configure VPN or Dial-Up
Configure Authentication Methods
The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.
Extensible Authentication Protocol
Type (based on method of access and network configuration):
Microsoft: Smart Card or other certificate
Configure...
Microsoft Encrypted Authentication version 2 (MS-CHAPv2)
Select this option to allow your users to specify a password for authentication.
Microsoft Encrypted Authentication (MS-CHAP)
Select this option only if your network runs operating systems that do not support MS-CHAPv2.
Giữ nguyên defaults và next
Previous
Next
Finish
Cancel


Configure VPN or Dial-Up
Specify User Groups
Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.
To select User Groups, click Add. If no groups are selected, this policy applies to all users.
Groups
Add...
Remove
Add group có chưa các users được phép VPN vào server
Previous
Next
Finish
Cancel
Select Group
Select this object type:
Group
Object Types...
From this location:
i1708a.com
Locations...
Enter the object name to select (examples):
vpns1
Check Names
Advanced...
OK
Cancel
Manage
Tools
Connections

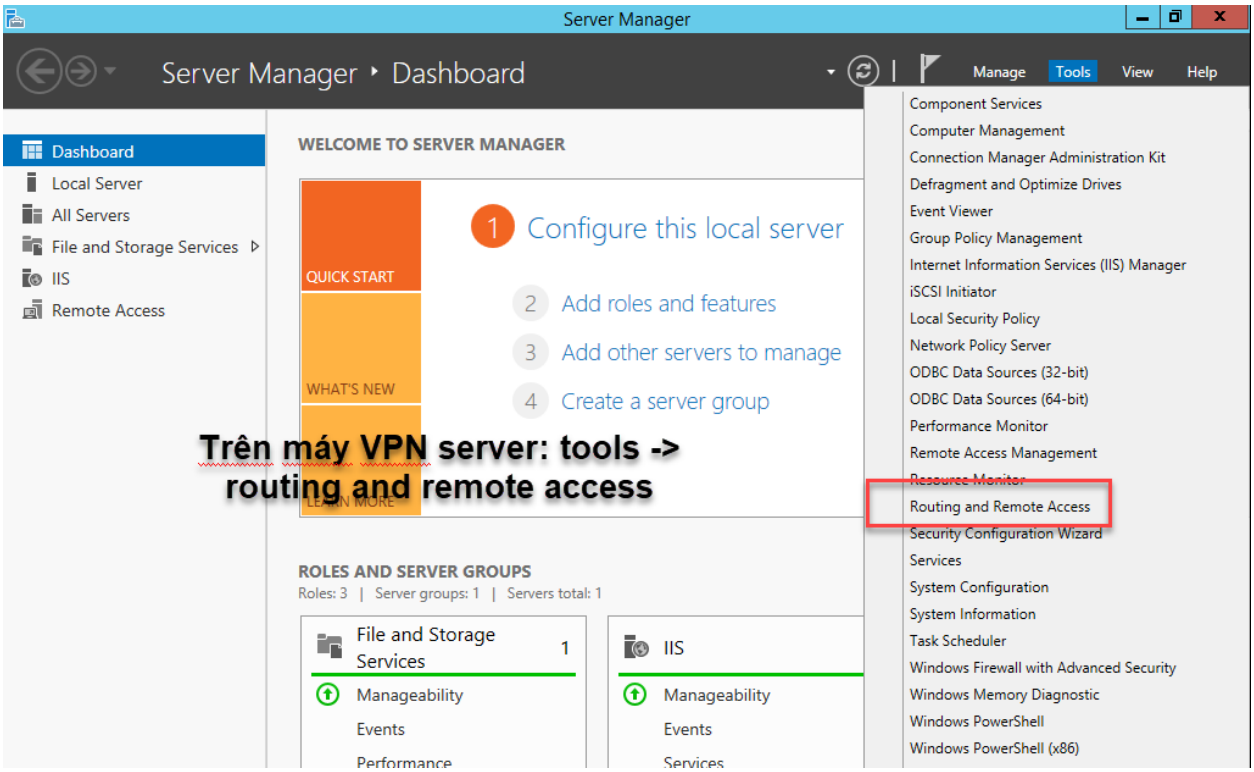

Configure VPN or Dial-Up
Specify IP Filters
Configure IPv4 and IPv6 packet filters if you want to restrict the type of network traffic sent and received.
If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure IPv4 and IPv6 input and output filters. Otherwise, click Next.
Select an existing IP Filter template:
None
IPv4
To control the IPv4 packets this interface sends, click Input Filters.
Input Filters...
To control the IPv4 packets this interface receives, click Output Filters.
Output Filters...
IPv6
To control the IPv6 packets this interface sends, click Input Filters.
Input Filters...
To control the IPv6 packets this interface receives, click Output Filters.
Output Filters...
Giữ nguyên defaults và next
Previous
Next
Finish
Cancel

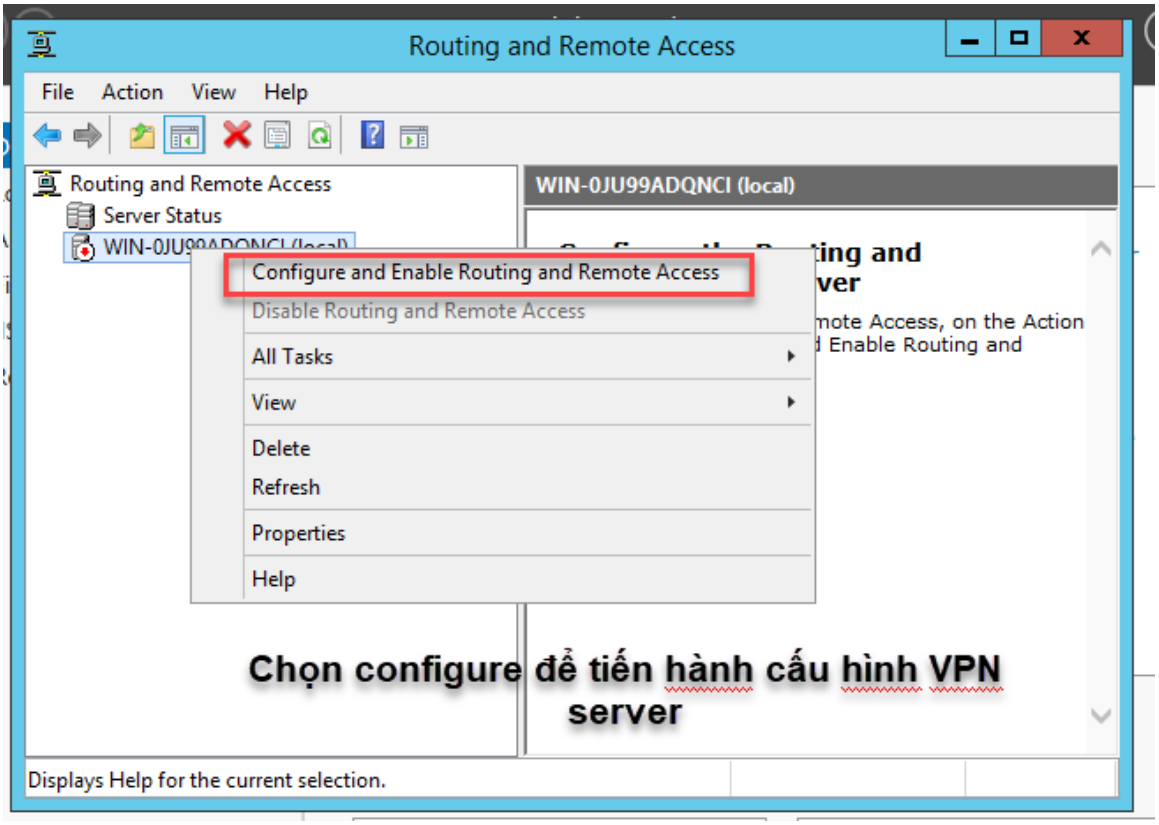

Configure VPN or Dial-Up
Specify Encryption Settings
Specify the allowed encryption strengths used for traffic between access clients and the network access server.
If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure encryption strength.
The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.
If you use different network access servers for dial-up or VPN connections, ensure that the encryptions settings you select are supported by your servers.
If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.
Basic encryption (MPPE 40-bit)
Strong encryption (MPPE 56-bit)
Strongest encryption (MPPE 128-bit)
tiếp tục next
Previous
Next
Finish
Cancel

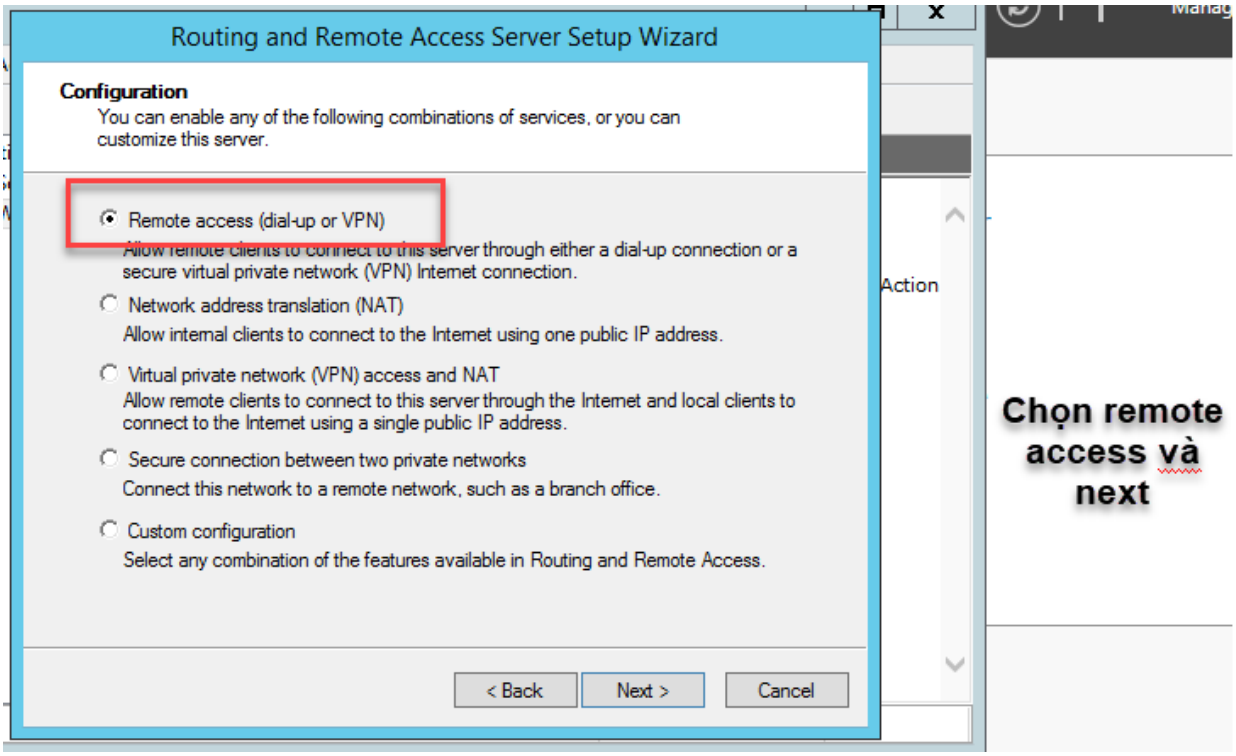

Configure VPN or Dial-Up
Specify a Realm Name
If you specify a realm name, the user account location supplied by users in log on credentials, such as a domain name, is replaced by the value you choose.
Your ISP uses a portion of the user name to identify which connection requests to route to this server. This part of the user name is the realm name.
If you do not know your realm name, contact your ISP. If you do not care about realm name, please click next.
Type the realm name, including the separator character (the period or the forward slash), that your ISP uses to forward requests.
Realm name:
Example: ISP
Before authentication, remove the realm name from the user name
If the realm name is an identifier added to the existing Windows user name, it must be removed before Windows can authenticate the connection request.
Điền tên và next
Previous
Next
Finish
Cancel

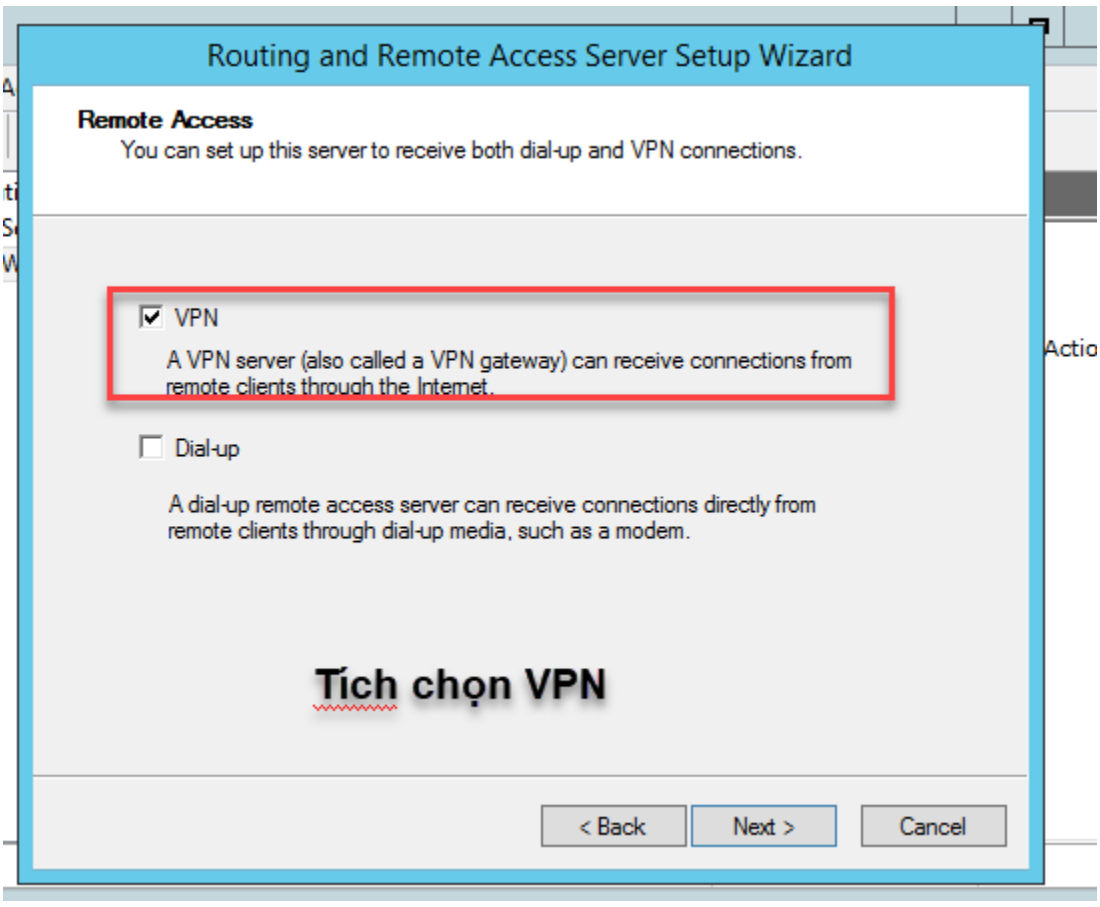

Configure VPN or Dial-Up
Completing New Dial-up or Virtual Private Network Connections and RADIUS clients
You have successfully created the following policies and configured the following RADIUS clients.
• To view the configuration details in your default browser, click Configuration Details.
• To change the configuration, click Previous.
• To save the configuration and close this wizard, click Finish.
Connection Request Policy:
VPN-2
Network Policies:
VPN-2
Finish để hoàn tất cấu hình radius
Configuration Details
Previous
Next
Finish
Cancel

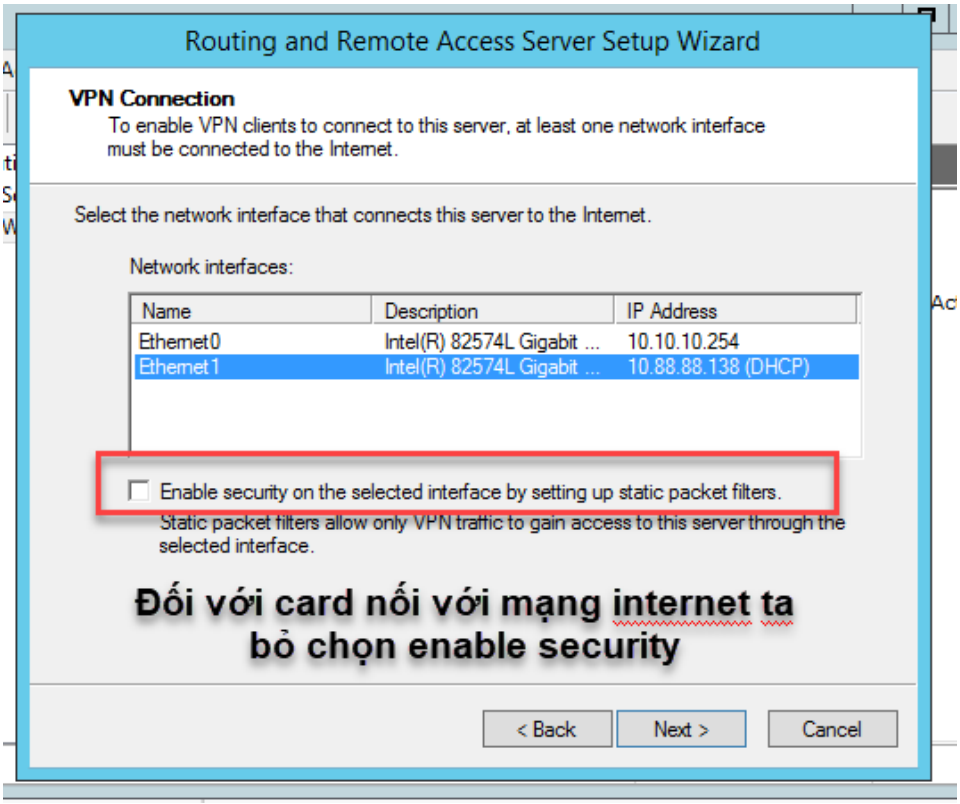
+ Trên máy VPN server:

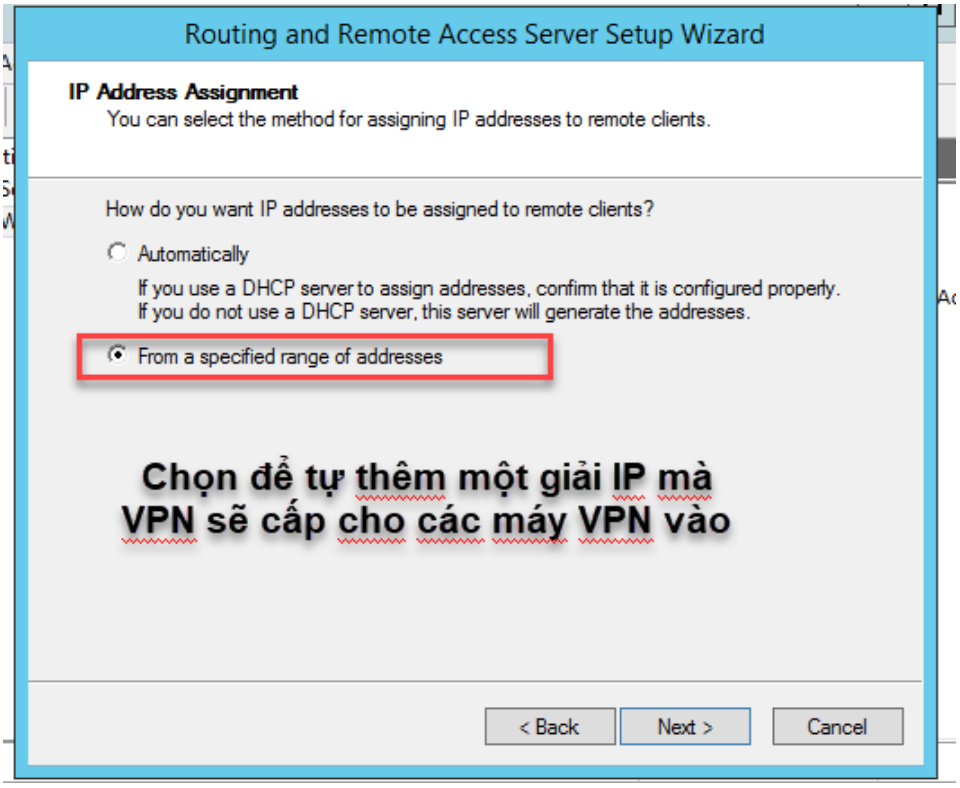


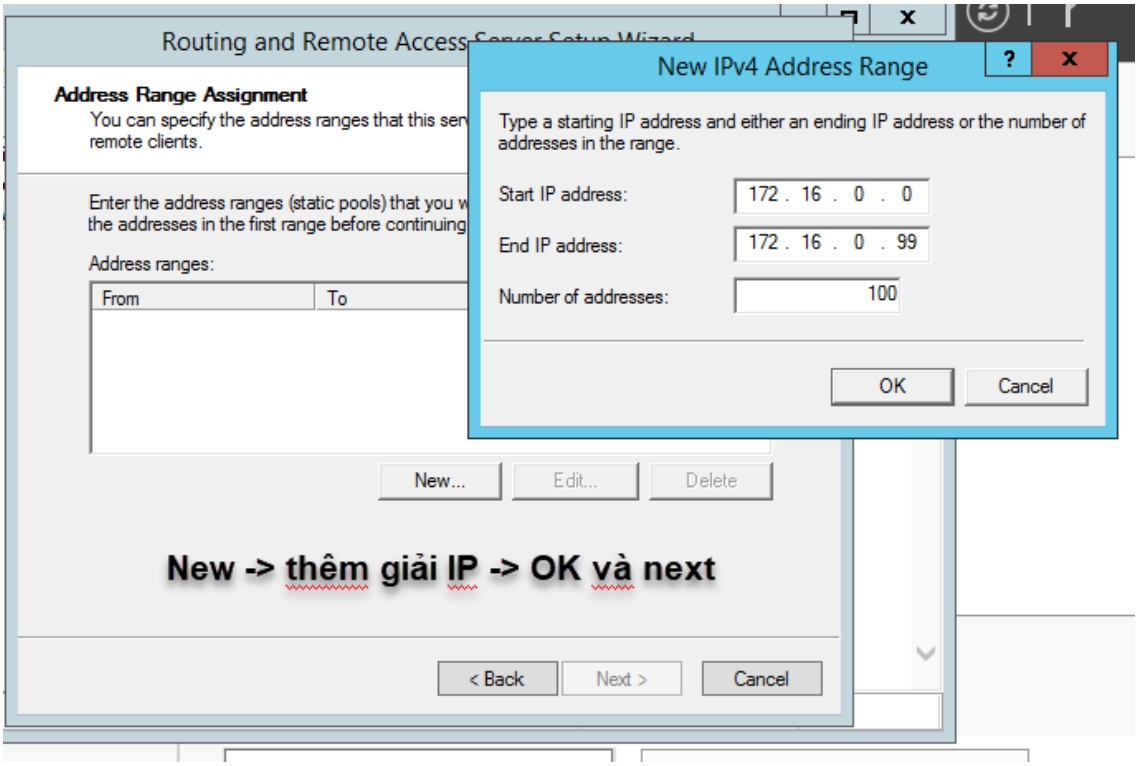


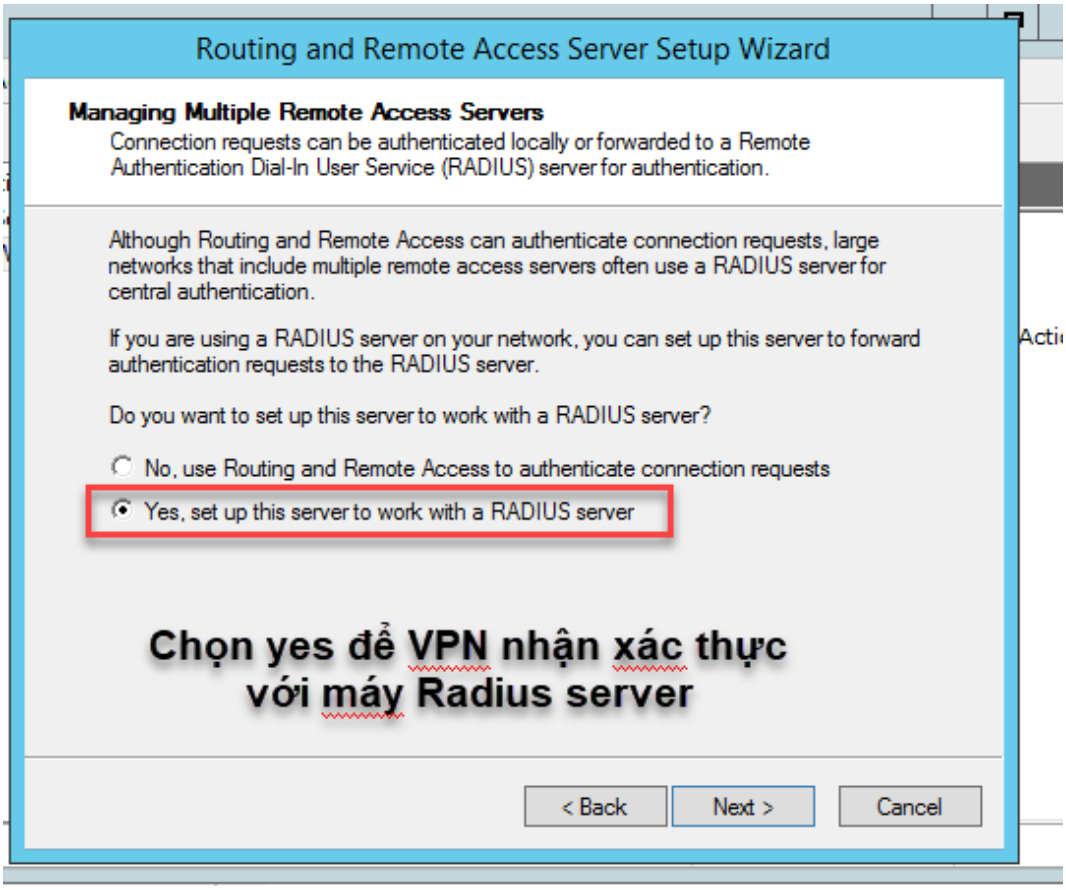

Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel
Action
Chọn remote access và next

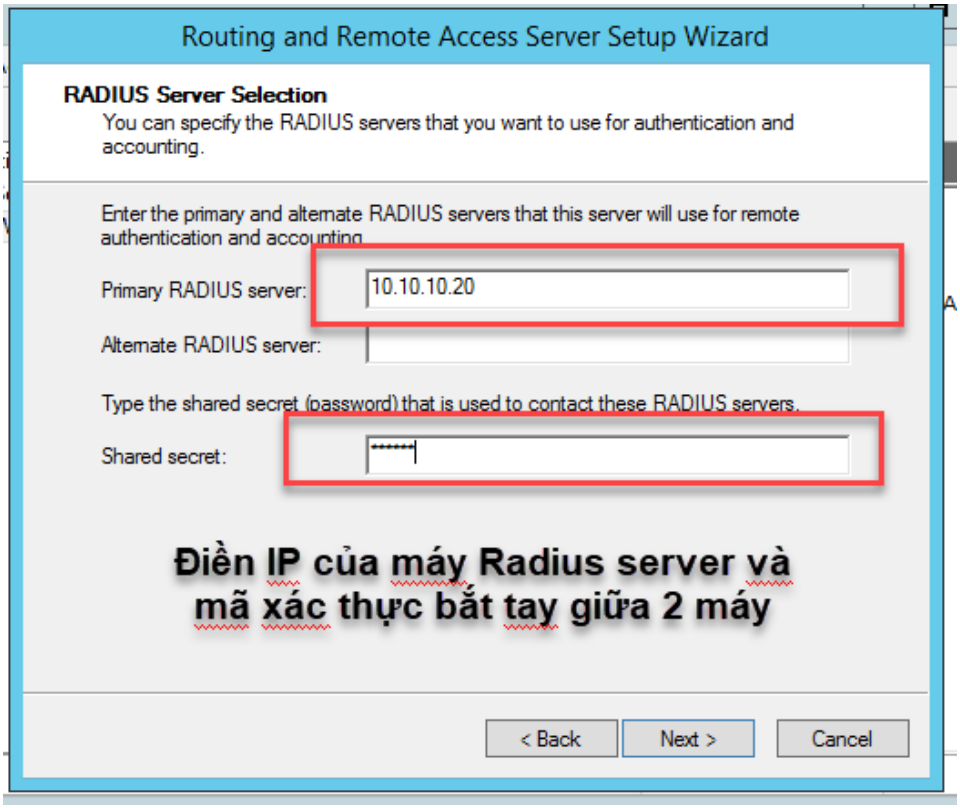

Routing and Remote Access Server Setup Wizard
Remote Access
You can set up this server to receive both dial-up and VPN connections.
VPN
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.
Dial-up
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.
Tích chọn VPN
< Back
Next >
Cancel

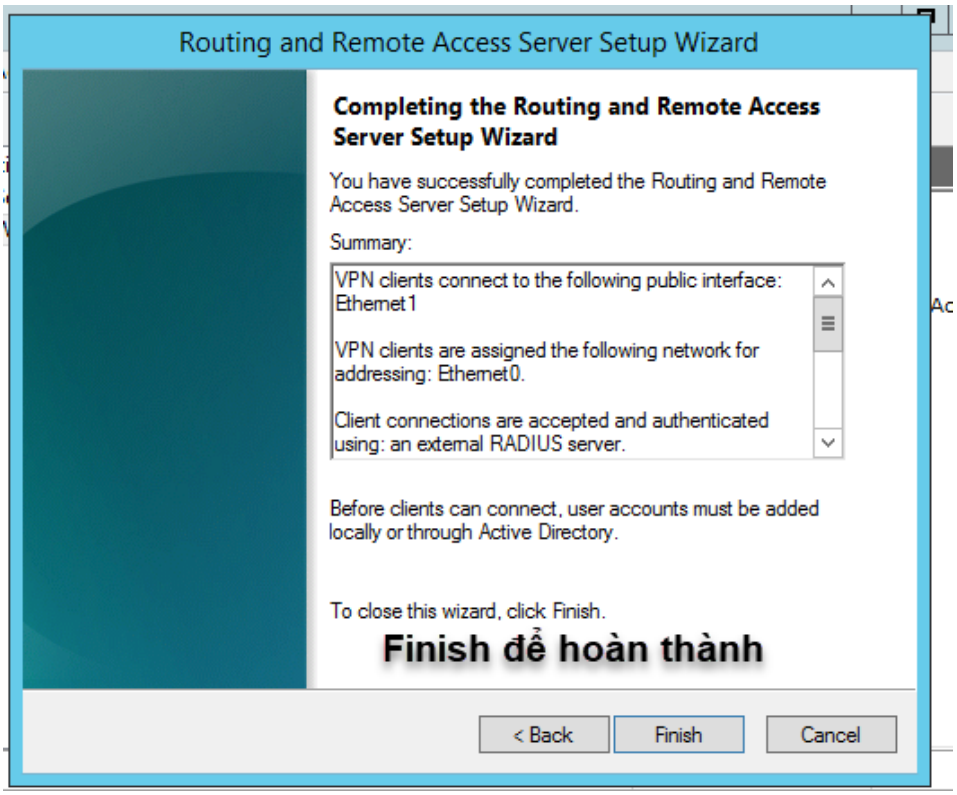

Routing and Remote Access Server Setup Wizard
VPN Connection
To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.
Select the network interface that connects this server to the Internet.
Network interfaces:
Name
Description
IP Address
Ethernet0
Intel(R) 82574L Gigabit ...
10.10.10.254
Ethernet1
Intel(R) 82574L Gigabit ...
10.88.88.138 (DHCP)
Enable security on the selected interface by setting up static packet filters.
Static packet filters allow only VPN traffic to gain access to this server through the selected interface.
Đối với card nối với mạng internet ta bỏ chọn enable security
< Back
Next >
Cancel

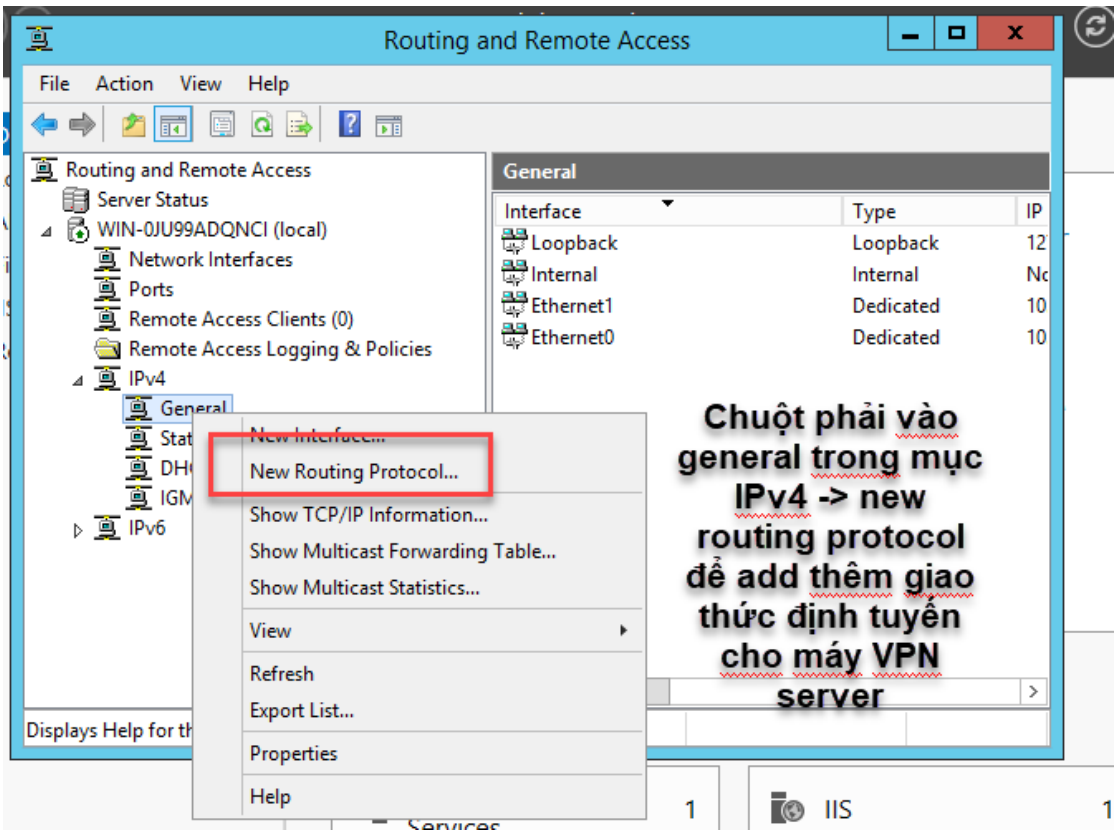

Routing and Remote Access Server Setup Wizard
IP Address Assignment
You can select the method for assigning IP addresses to remote clients.
How do you want IP addresses to be assigned to remote clients?
Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.
From a specified range of addresses
Chọn để tự thêm một giải IP mà VPN sẽ cấp cho các máy VPN vào
< Back
Next >
Cancel

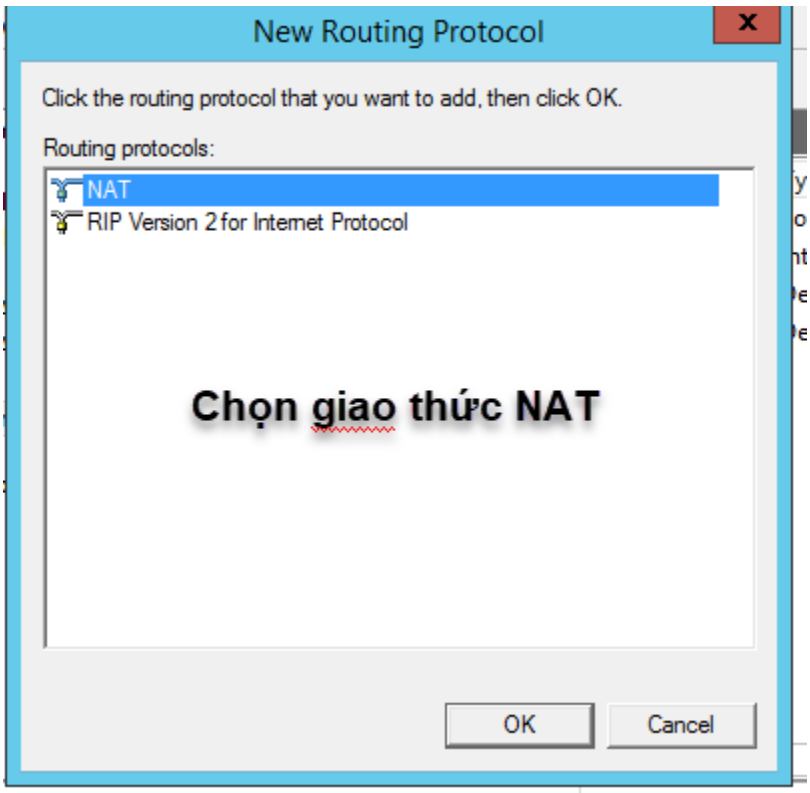

Routing and Remote Access Server Setup Wizard
Address Range Assignment
You can specify the address ranges that this ser
remote clients.
Enter the address ranges (static pools) that you w
the addresses in the first range before continuing
Address ranges:
From
To
New...
Edit...
Delete
New -> thêm giải IP -> OK và next
< Back
Next >
Cancel
New IPv4 Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address:
172 . 16 . 0 . 0
End IP address:
172 . 16 . 0 . 99
Number of addresses:
100
OK
Cancel

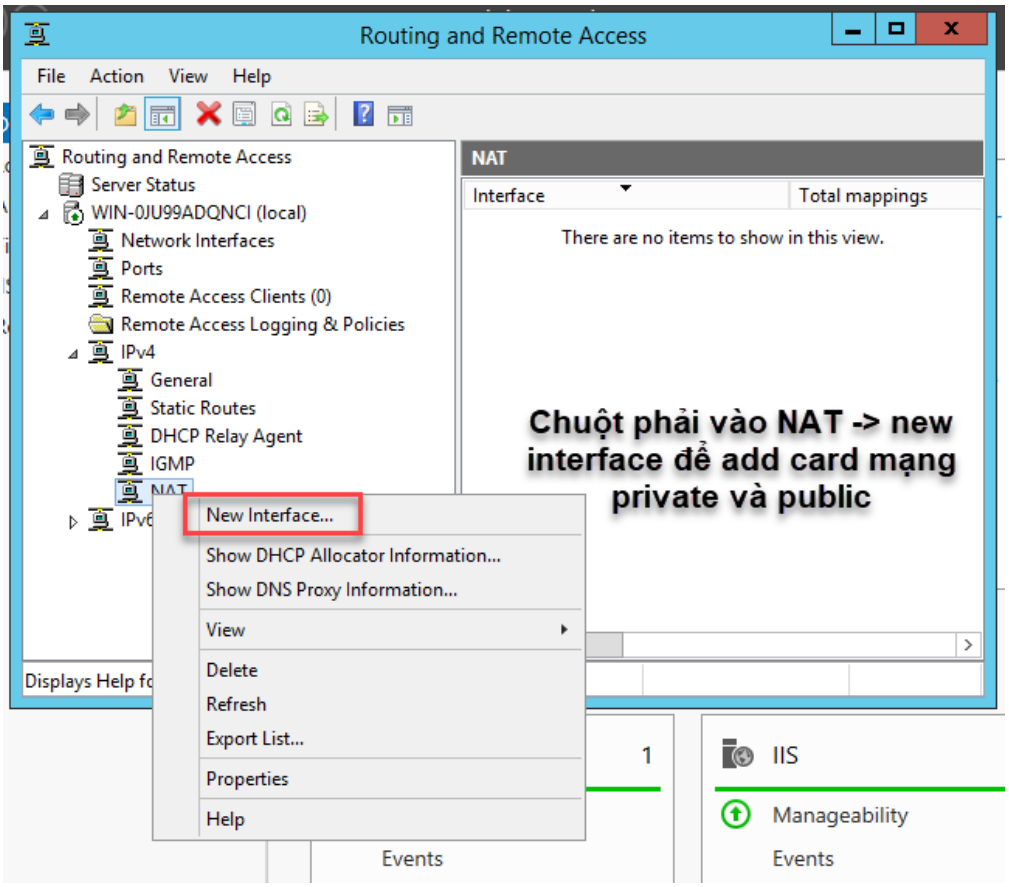

Routing and Remote Access Server Setup Wizard
Managing Multiple Remote Access Servers
Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.
Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.
If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.
Do you want to set up this server to work with a RADIUS server?
No, use Routing and Remote Access to authenticate connection requests
Yes, set up this server to work with a RADIUS server
Chọn yes để VPN nhận xác thực
với máy Radius server
< Back
Next >
Cancel

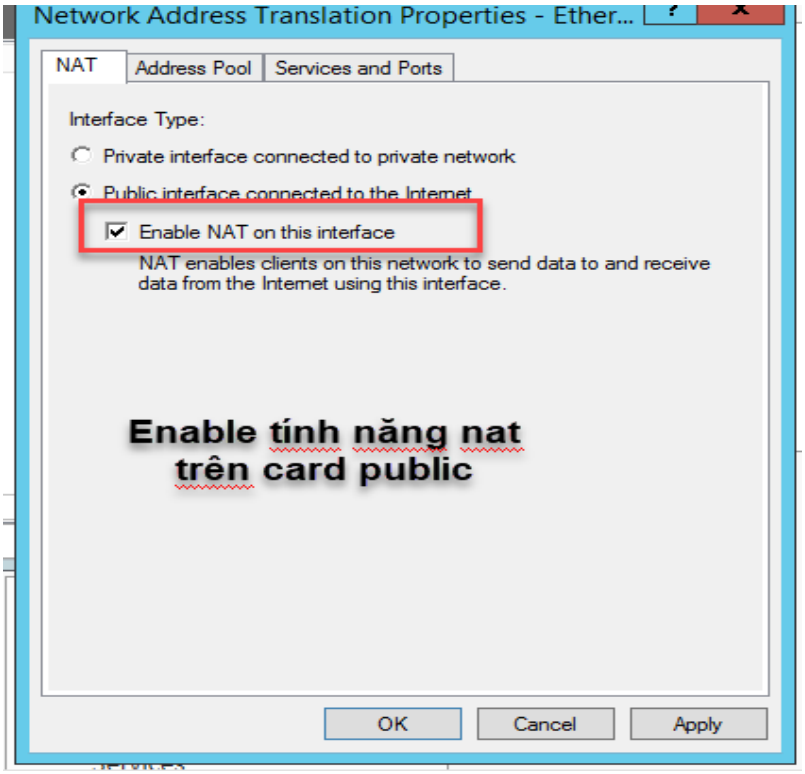

Routing and Remote Access Server Setup Wizard
RADIUS Server Selection
You can specify the RADIUS servers that you want to use for authentication and accounting.
Enter the primary and alternate RADIUS servers that this server will use for remote authentication and accounting.
Primary RADIUS server:
10.10.10.20
Alternate RADIUS server:
Type the shared secret (password) that is used to contact these RADIUS servers.
Shared secret:
Điền IP của máy Radius server và mã xác thực bắt tay giữa 2 máy
< Back
Next >
Cancel


Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup Wizard.
Summary:
VPN clients connect to the following public interface: Ethernet 1
VPN clients are assigned the following network for addressing: Ethernet 0.
Client connections are accepted and authenticated using: an external RADIUS server.
Before clients can connect, user accounts must be added locally or through Active Directory.
To close this wizard, click Finish.
Finish để hoàn thành
< Back
Finish
Cancel


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN-0JU99ADQNCI (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
IPv6
General
Interface
Type
Loopback
Loopback
Internal
Internal
Ethernet1
Dedicated
Ethernet0
Dedicated
New Routing Protocol...
Show TCP/IP Information...
Show Multicast Forwarding Table...
Show Multicast Statistics...
View
Refresh
Export List...
Properties
Help
Chuột phải vào general trong mục IPv4 -> new routing protocol để add thêm giao thức định tuyến cho máy VPN server
IIS


New Routing Protocol
Click the routing protocol that you want to add, then click OK.
Routing protocols:
NAT
RIP Version 2 for Internet Protocol
Chọn giao thức NAT
OK
Cancel


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN-0JU99ADQNCI (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
DHCP Relay Agent
IGMP
NAT
IPv6
NAT
Interface
Total mappings
There are no items to show in this view.
Chuột phải vào NAT -> new interface để add card mạng private và public
New Interface...
Show DHCP Allocator Information...
Show DNS Proxy Information...
View
Delete
Refresh
Export List...
Properties
Help
Displays Help fo
1
Events
IIS
Manageability
Events


Network Address Translation Properties - Ether...
NAT
Address Pool
Services and Ports
Interface Type:
Private interface connected to private network
Public interface connected to the Internet
Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.
Enable tính năng nat trên card public
OK
Cancel
Apply

+ Sau khi cấu hình xong, ta sử dụng một máy win 7 hoặc 10 tạo VPN client đăng nhập vào máy chủ