## GENERAL INFORMATION ABOUT THE PRACTICE

**Practice name:** Practicing Site-to-Site VPN on Windows Server 2008 system

**Number of students working together:** 01

**Score:** 01 point

**Practice location:** Computer room

**Request:**

- Hardware requirements: Each student is provided with 01 computer with minimum configuration: CPU 2.0 GHz, RAM 16GB, HDD 100GB

- Software requirements on the machine:

+ Operating system Windows Server 2008, Windows 7

+ VMware Workstation 9.0 or higher

- Practice tools: VMware virtual machine:

+ Windows Windows Server 2008, Windows 7

- LAN connection required: yes

- Internet connection required: no

- Requirements: projector, whiteboard, pen/chalk

## PREPARATION FOR PRACTICE

**For instructors:**

Before preparation for practice the lesson, the instructor (practice instructor) needs to check the suitability of the actual conditions of the practice room with the requirements of the practice lesson.

No other requirements.

**For students:**

Before starting the practice, it is necessary to create copies of the virtual machines for use. Also specify the storage location for the tools specified in the requirements section

# PART 1. CONFIGURATION OF VPN NETWORK ACCORDING TO CLIENT MODEL TO-SIDE

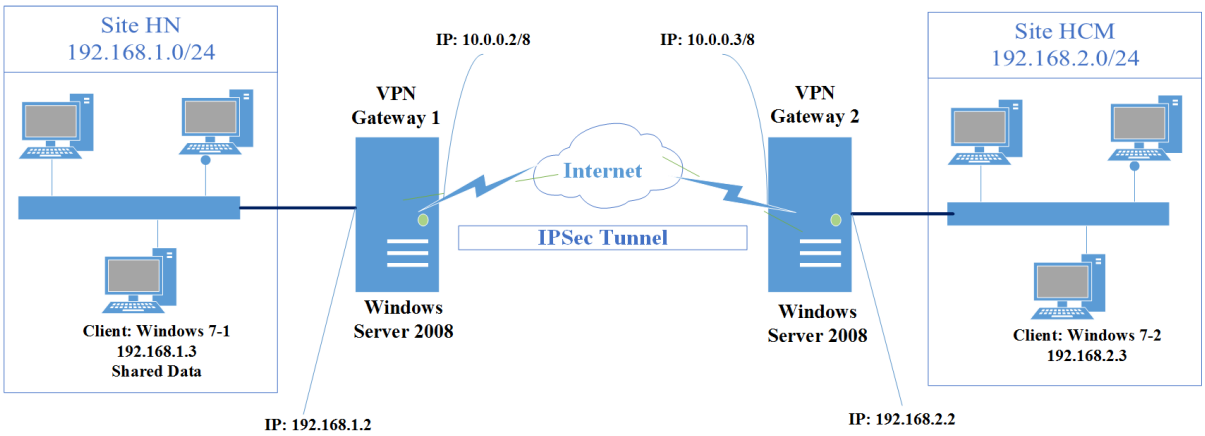
## 1.1. Description

In IPSec/VPN scenarios on Windows OS, IPSec Site to Site VPN is the most popular scenario applied in network systems of organizations and businesses today. In this section, the document will guide students on how to exploit and use IPSec Site to Site VPN on Windows Server 2008 OS.

## 1.2. Preparation

- 02 virtual machines running Windows Server 2008 operating system.
- 02 virtual machine running Windows 7 operating system.

## 1.3. Deployment model




## 1.4. Description of work to be performed

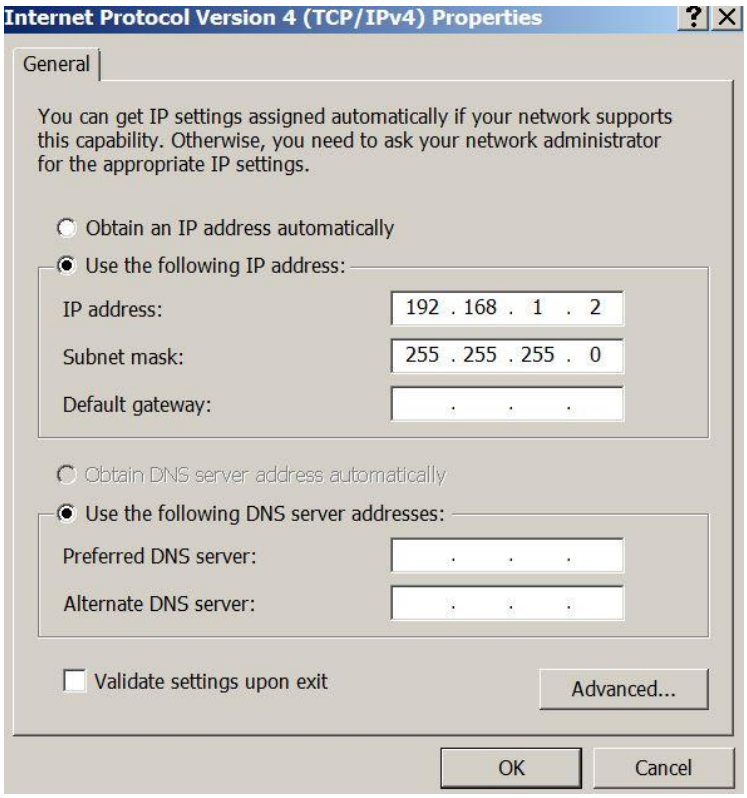
- Create a user account that grants VPN access.
- Install Routing and Remote Access service.
- Configure Site to site VPN service on Windows Server 2008.
- Check the connection between networks in Site to Site VPN
- Share user data via Site to Site VPN

## 1.5. Implementation steps

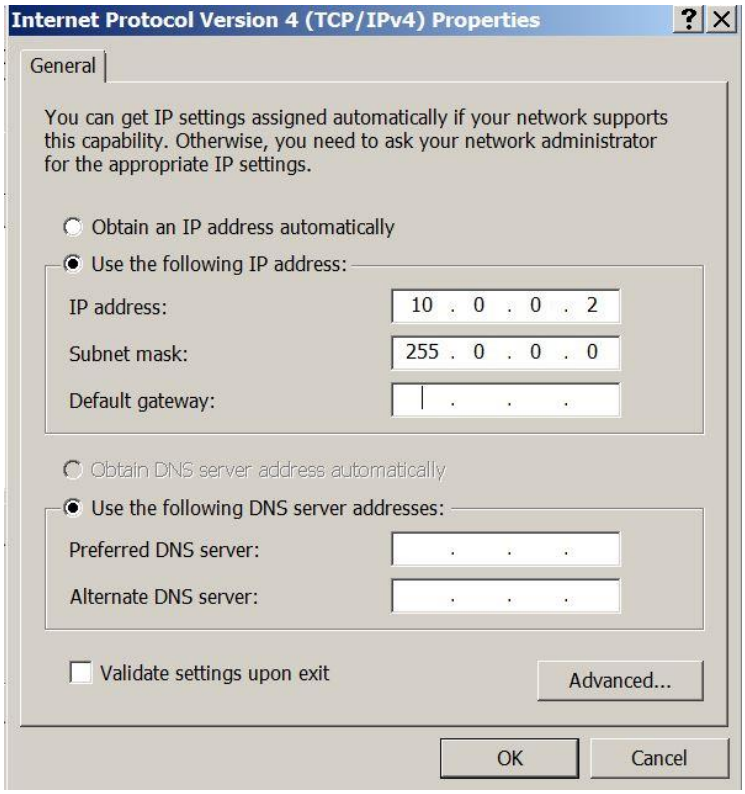
### 1.5.1. Perform on Windows server 2008:

a. VPN Gateway 1 server has 2 network cards configured with corresponding IP addresses as follows:

- Card number 1 connects to Hanoi system website:

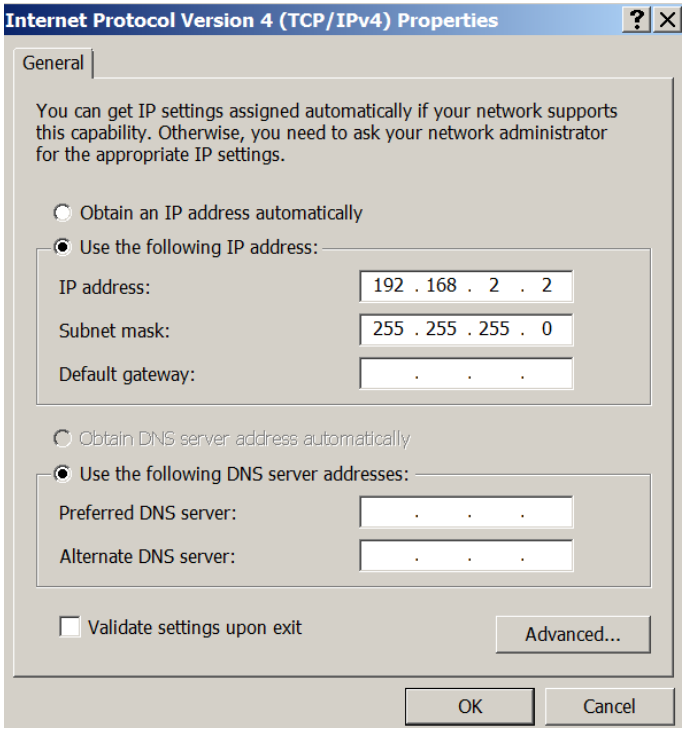



- Card number 2 connects to internet (In the model connects to VPN Gateway 2)

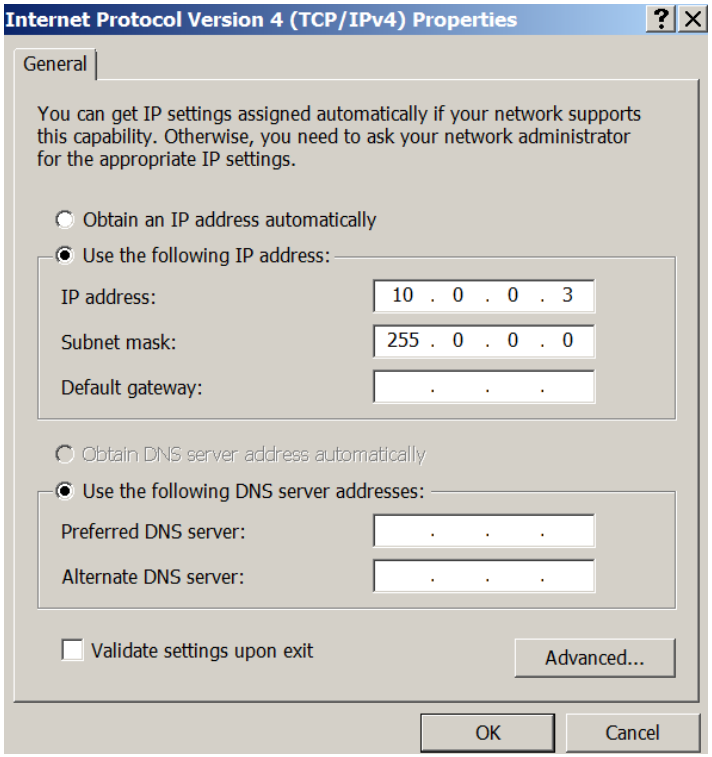



b. VPN Gateway 2 server has 2 network cards configured with corresponding IP addresses as follows:

- Card number 1 connects to HCM system website:

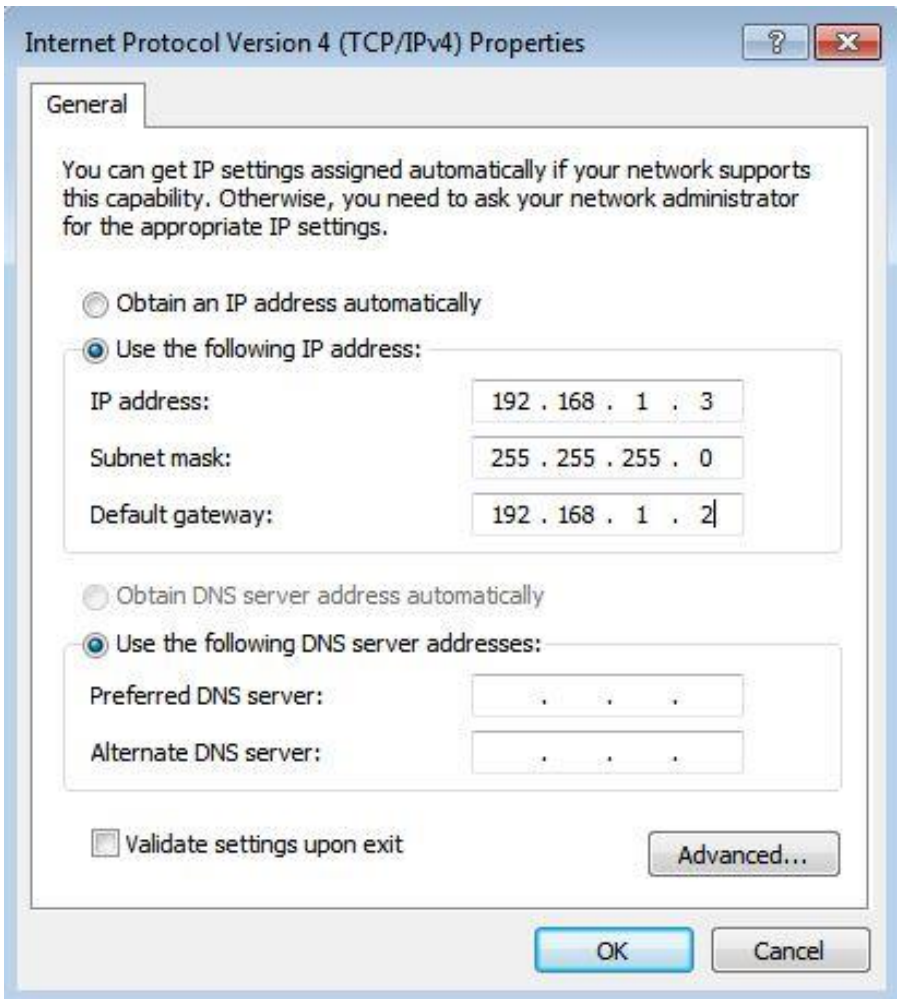



- Card number 2 connects to internet (In the model connects to VPN Gateway 1)

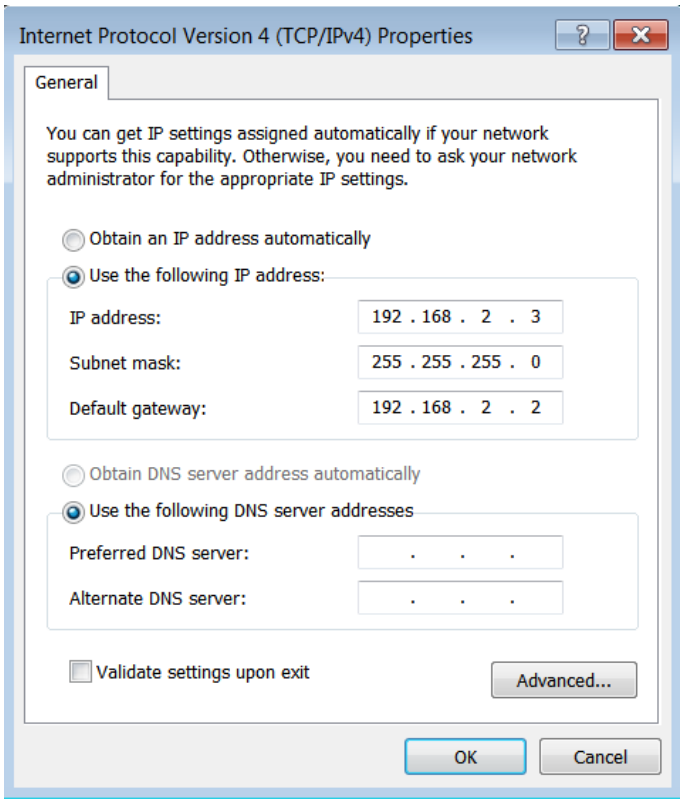



### 1.5.2. Perform on Win 7 machine

a. The Win 7-1 workstation has a network card configured with the following IP address:

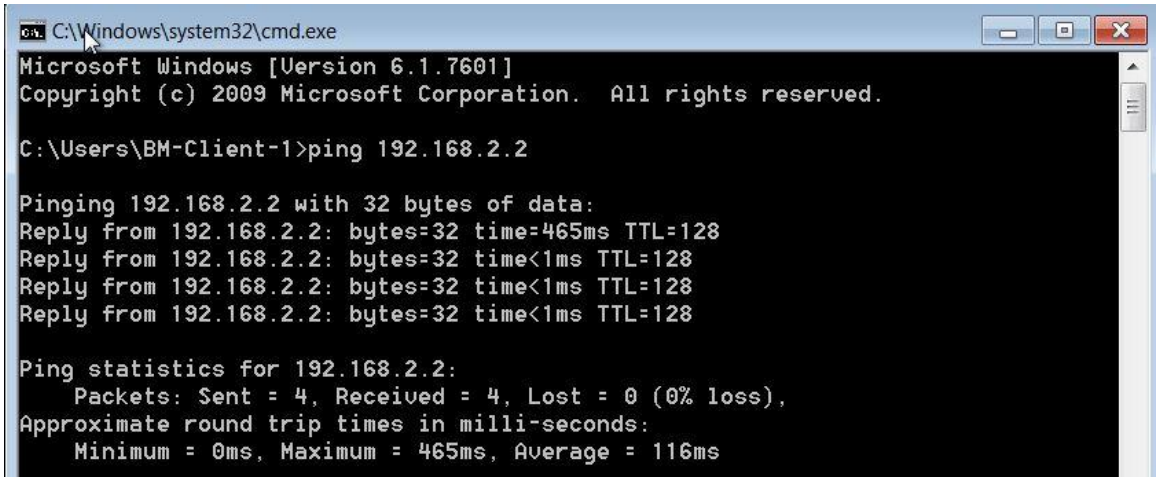



b. The Win 7-1 workstation has a network card configured with the following IP address:



### 1.5.3. Check connection

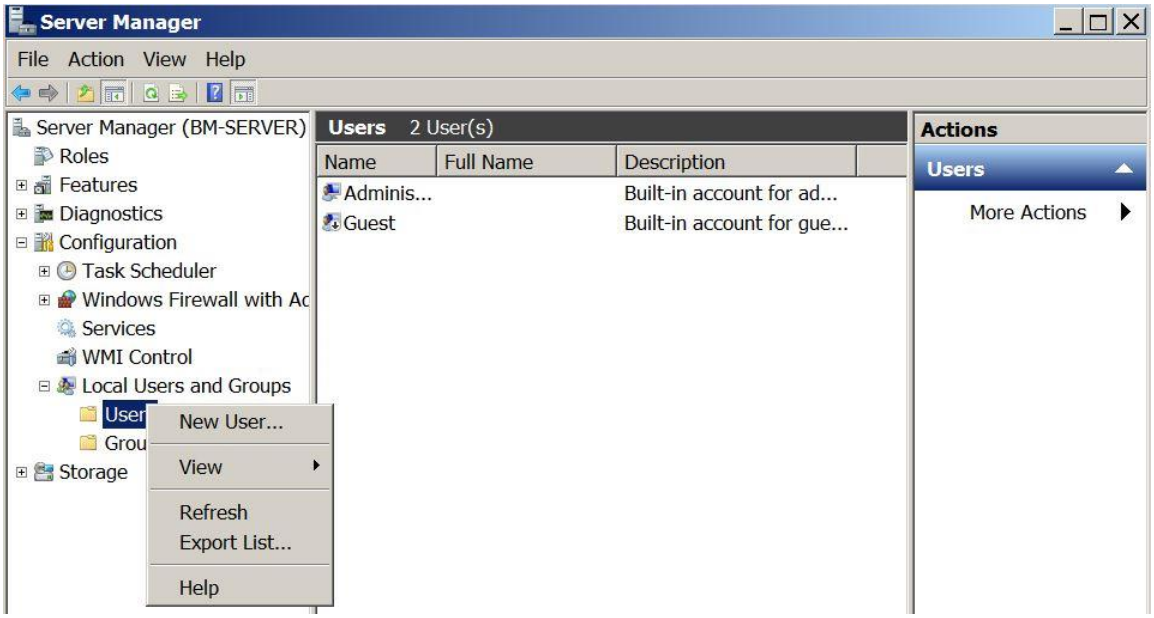
- Example of testing connection from Win 7-2 workstation to VPN Gateway 2:



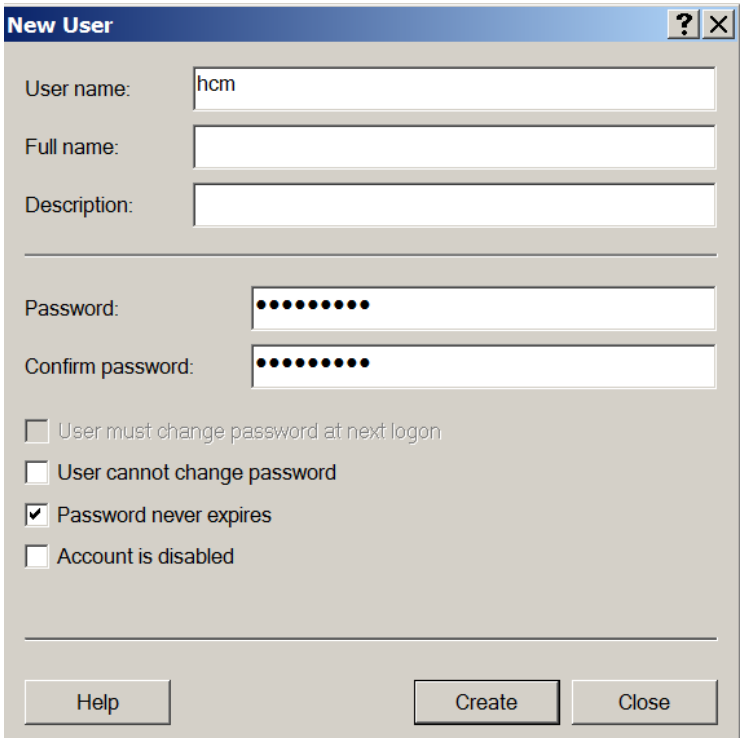

- Note: In case the connection test fails, the information can be resolved by turning off the Windows firewall in Windows of the machine. Another way can be to create rules in the Windows Firewall to allow the ICMP protocol to execute the ping command to test the connection and the ports PPTP: 1723 TCP 47 GRE, L2TP over IPSEC: 1701 TCP 500 UDP, SSTP: 443 TCP for Site to Site VPN setup types.

### 1.5.4. Create an account and grant VPN permissions

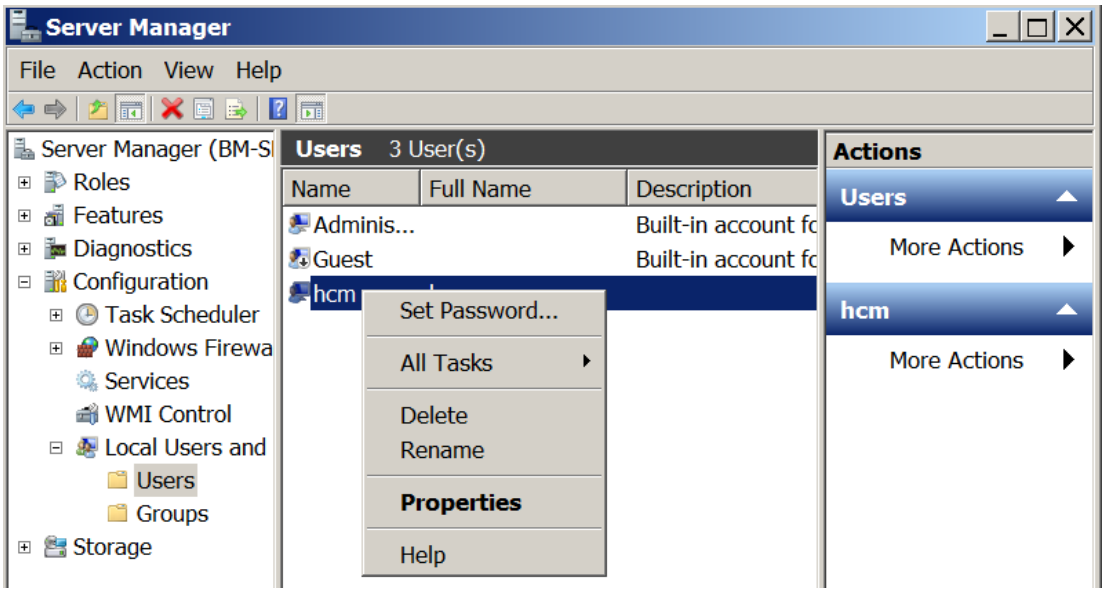
a. Create account (execute on VPN Gateway 1 machine):

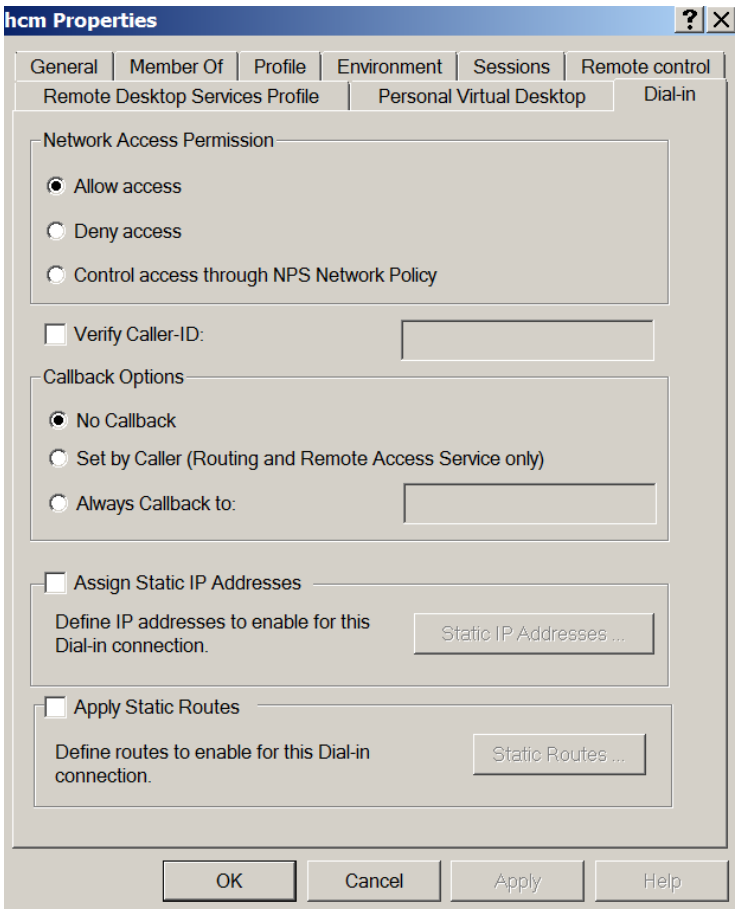



Assign a name and password to the account:

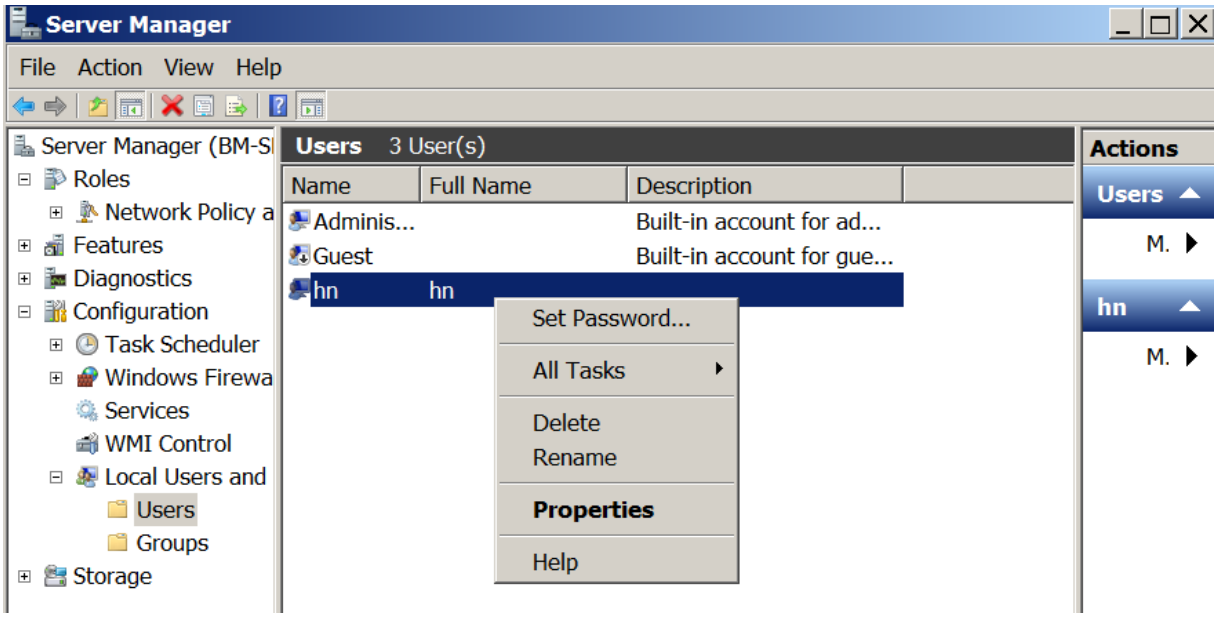



Grant VPN permissions to the account:



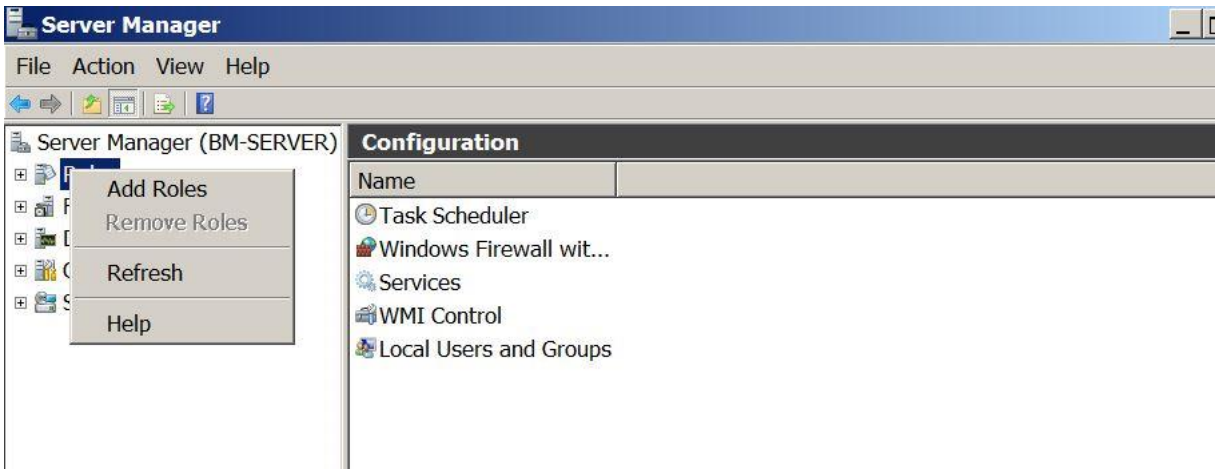


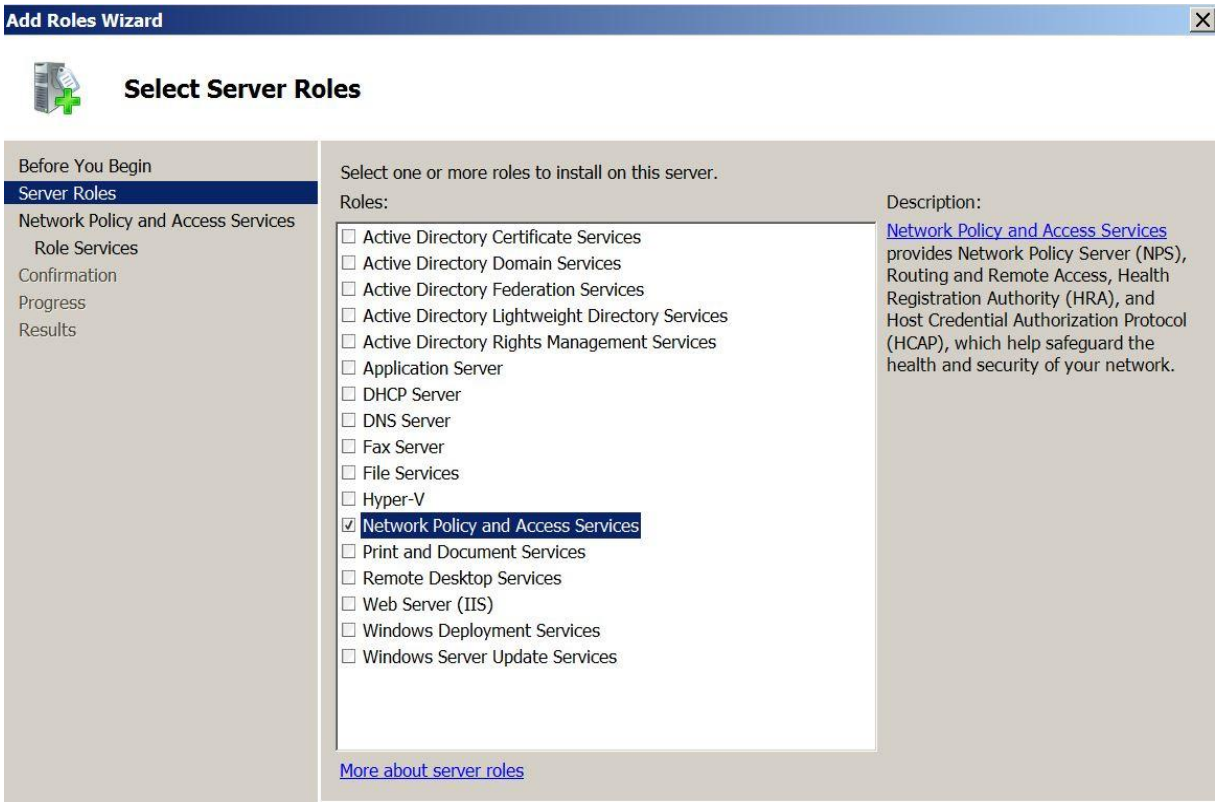

b. Create an account on VPN Gateway 02 server then grant VPN permission.

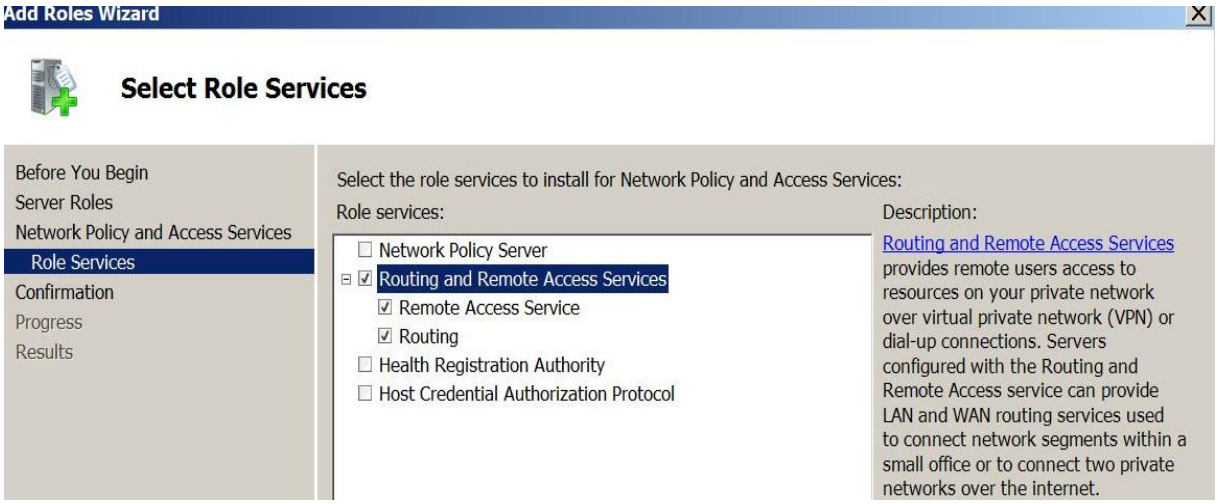


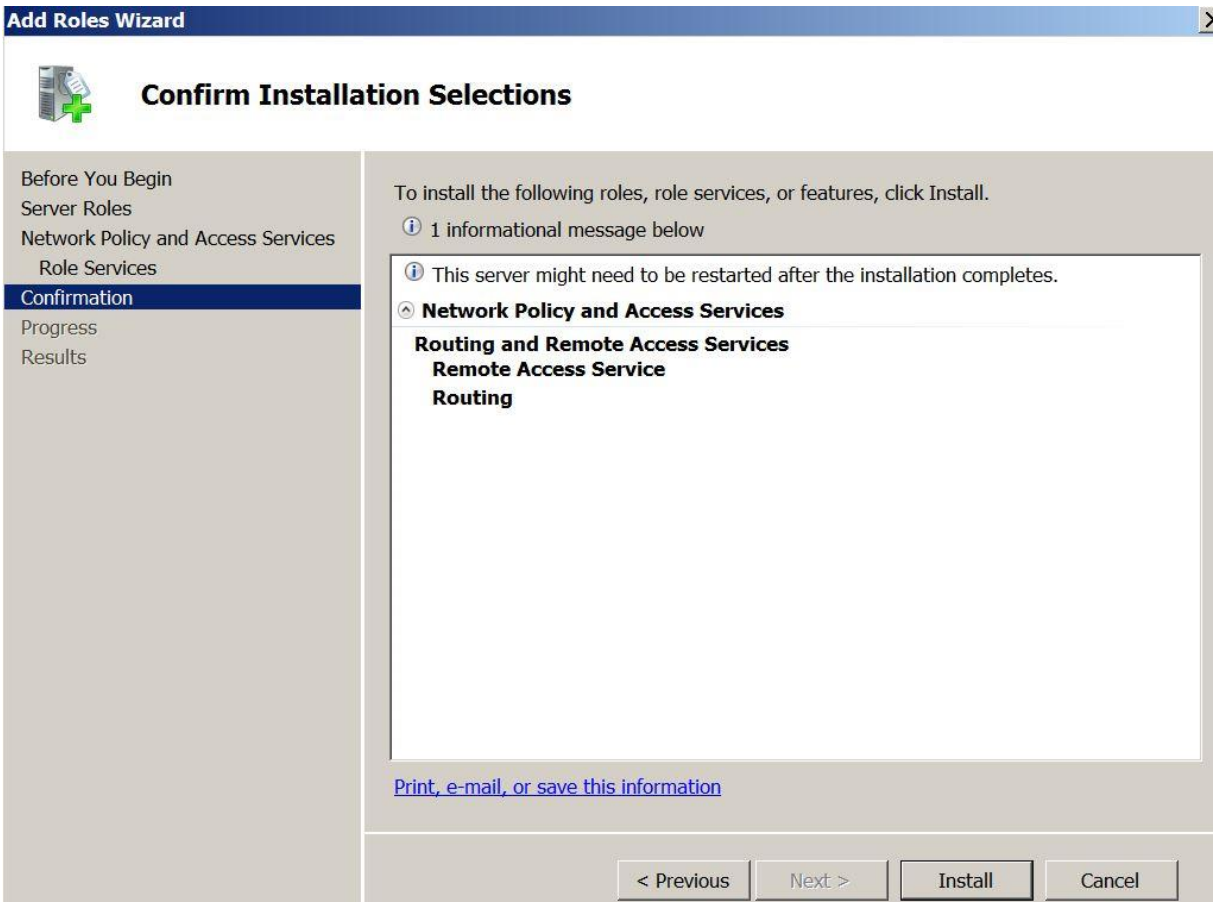

c. Install Routing and Remote Access service

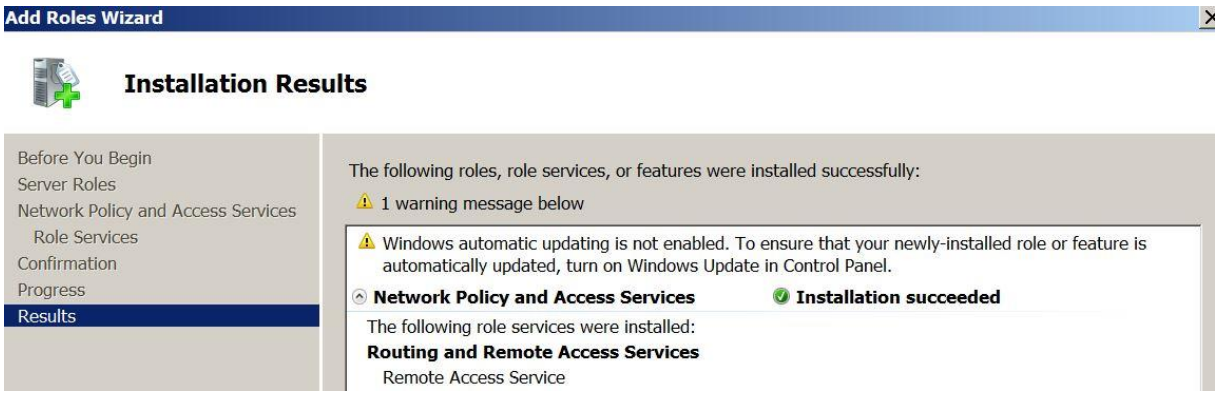
Execute on VPN Gateway 1:


Server Manager
File Action View Help
Server Manager (BM-SERVER)
Add Roles
Remove Roles
Refresh
Help
Configuration
Name
Task Scheduler
Windows Firewall wit...
Services
WMI Control
Local Users and Groups


Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Desktop Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description:
Network Policy and Access Services provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.
More about server roles


Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Network Policy and Access Services:
Role services:
Network Policy Server
Routing and Remote Access Services
Remote Access Service
Routing
Health Registration Authority
Host Credential Authorization Protocol
Description:
Routing and Remote Access Services provides remote users access to resources on your private network over virtual private network (VPN) or dial-up connections. Servers configured with the Routing and Remote Access service can provide LAN and WAN routing services used to connect network segments within a small office or to connect two private networks over the internet.

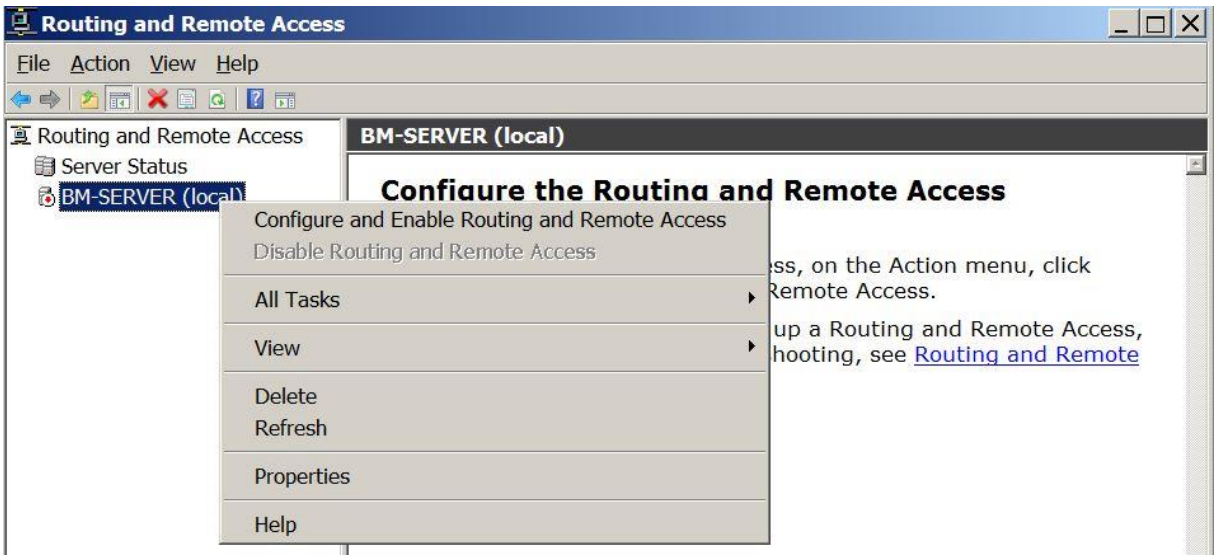


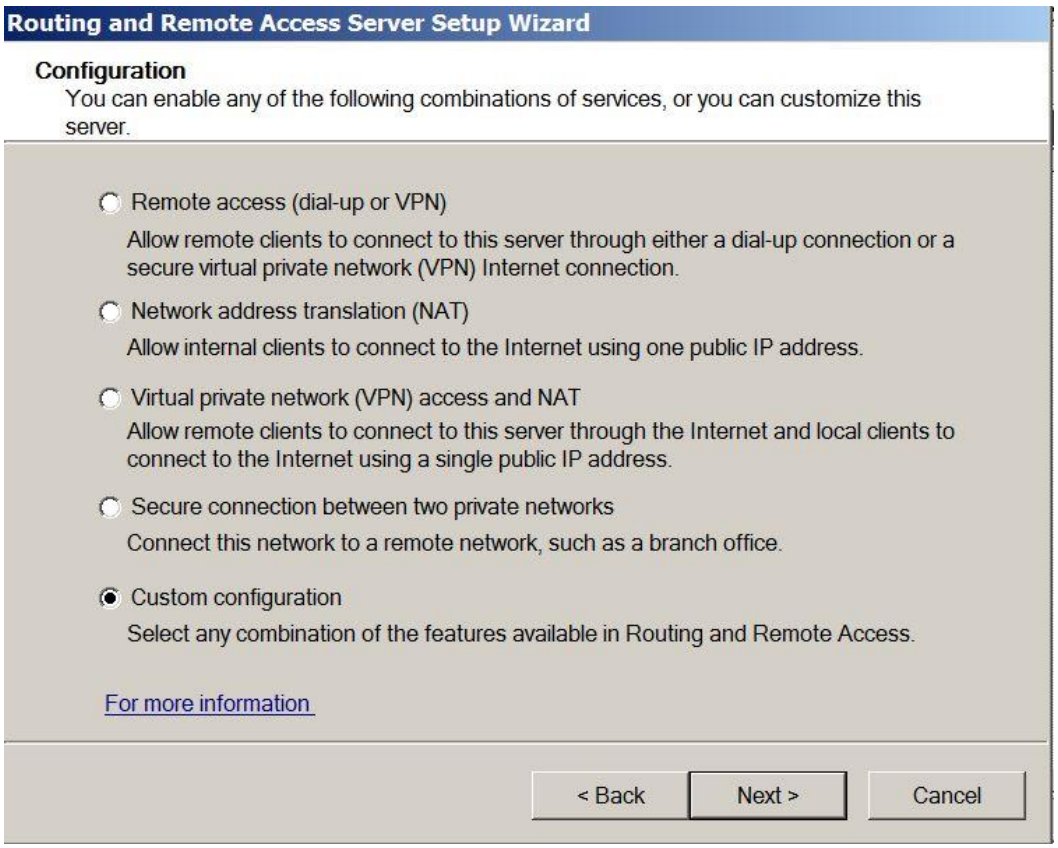

The process of installing the Routing and Remote Access service on VPN Gateway 2 is similar to that on VPN Gateway 1.

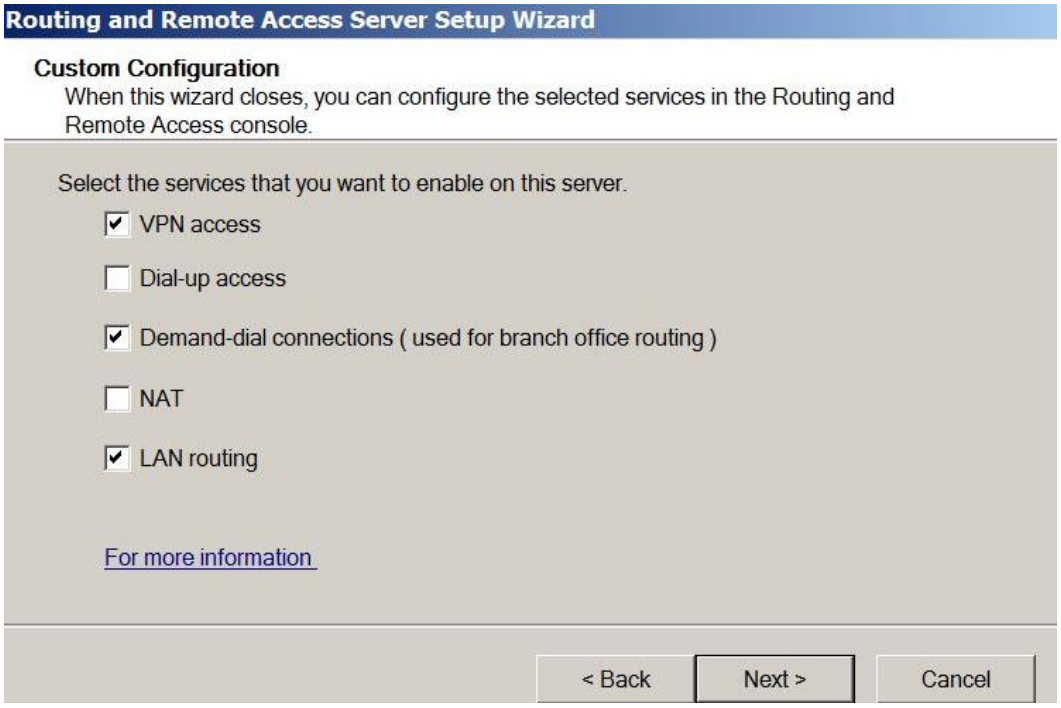
### 1.5.5. Configuration Site to Site VPN

Execute on VPN Gateway 1

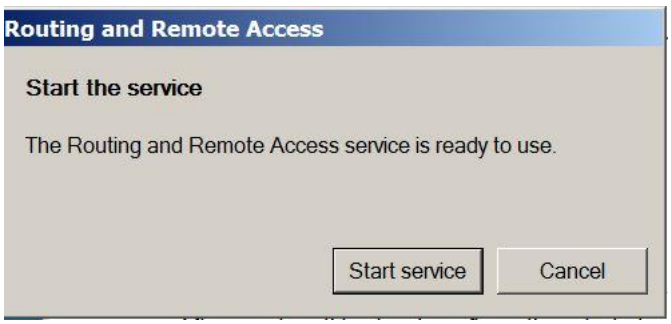

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
BM-SERVER (local)
BM-SERVER (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
Remote Access.
up a Routing and Remote Access,
hooting, see Routing and Remote

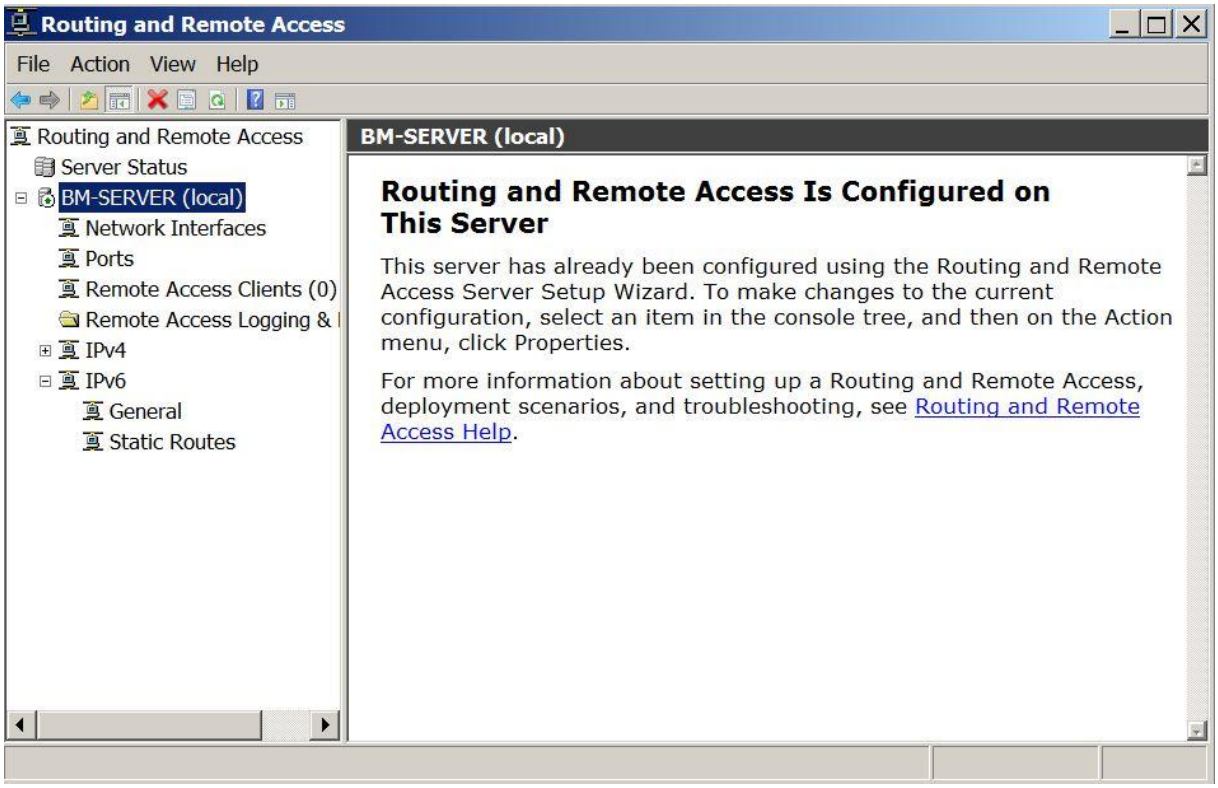

Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
< Back
Next >
Cancel

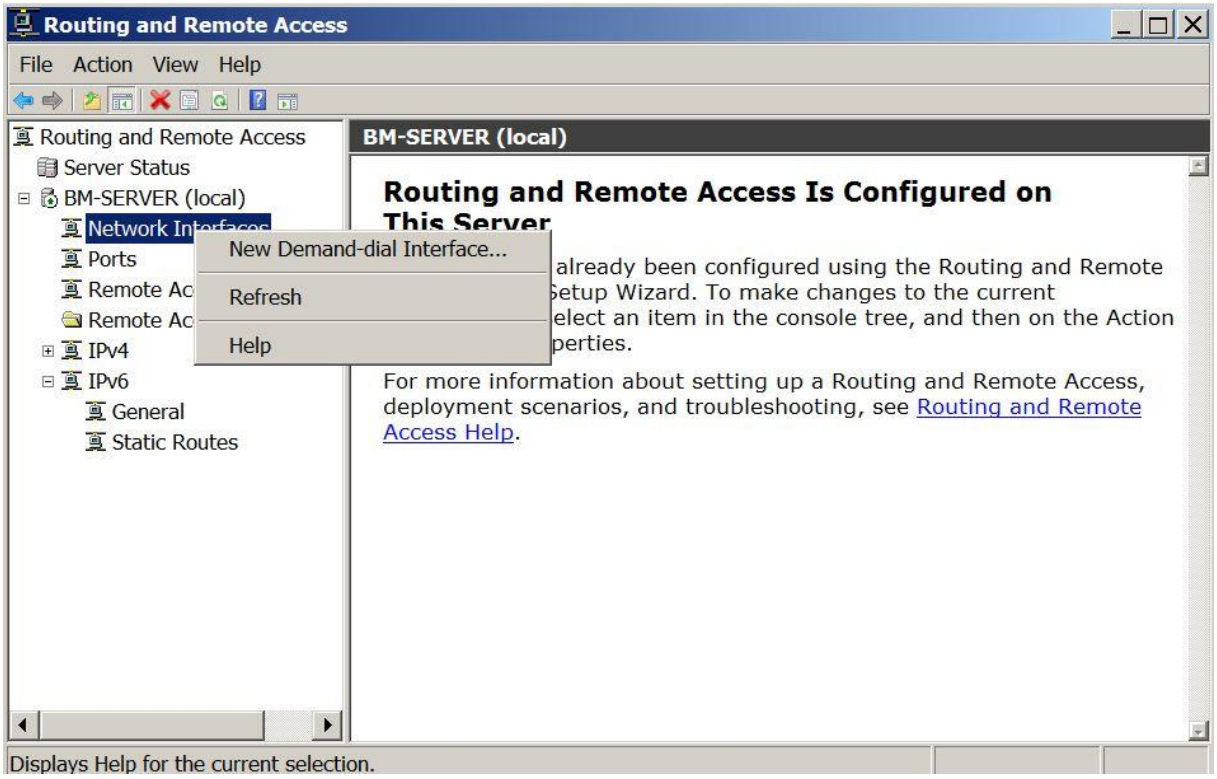


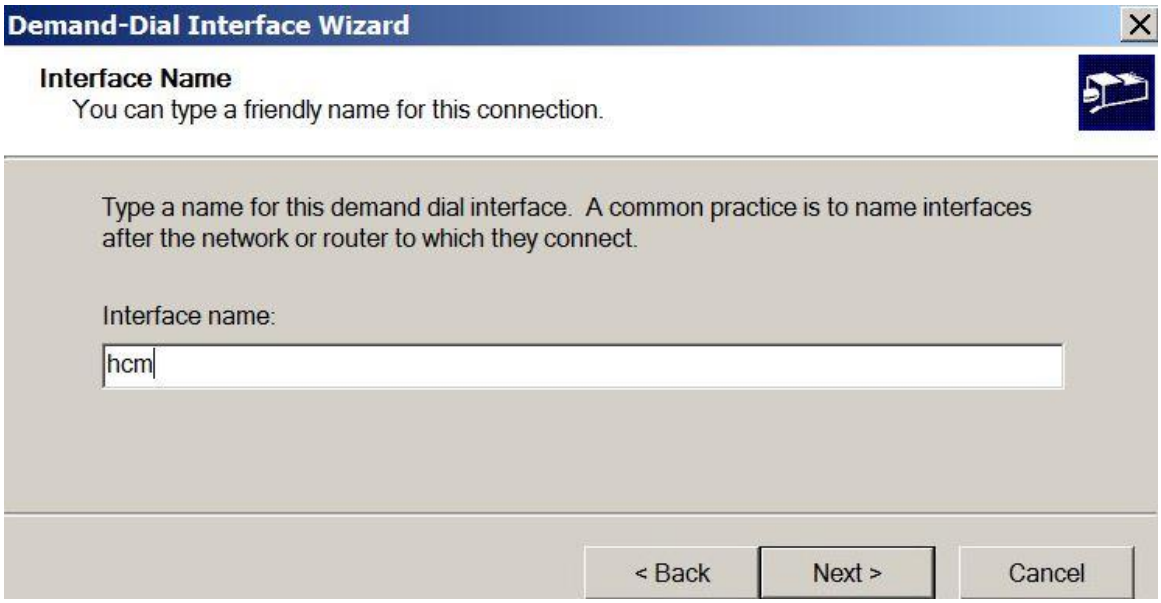



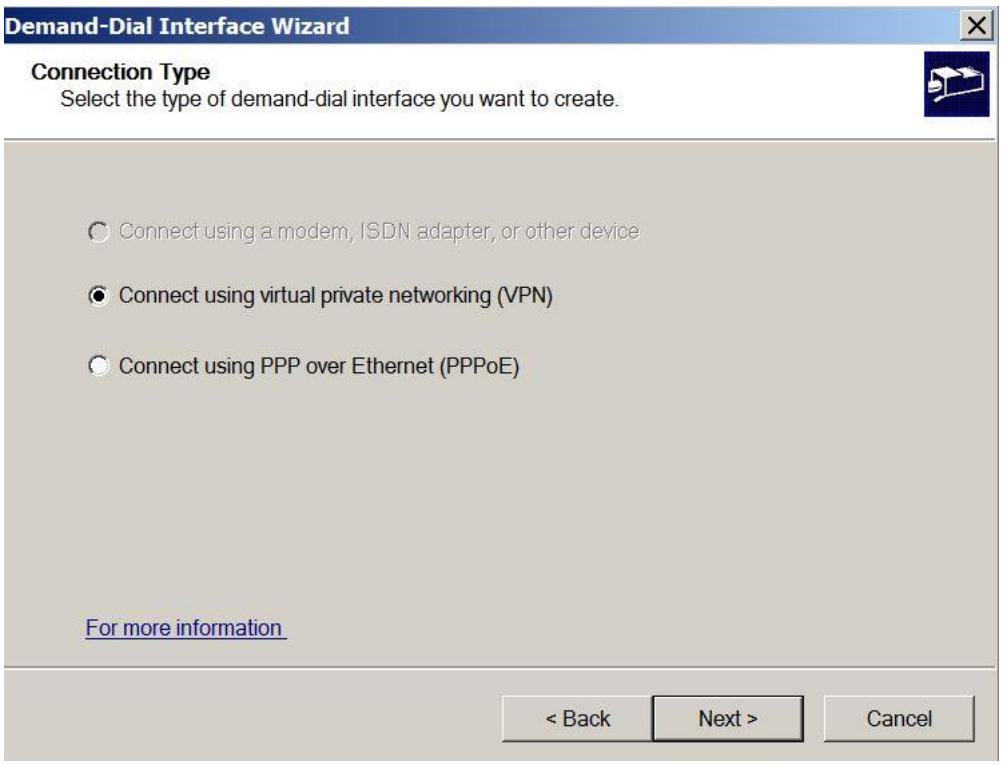

Click Finish and Start Service to start the VPN services to select on VPN Gateway:

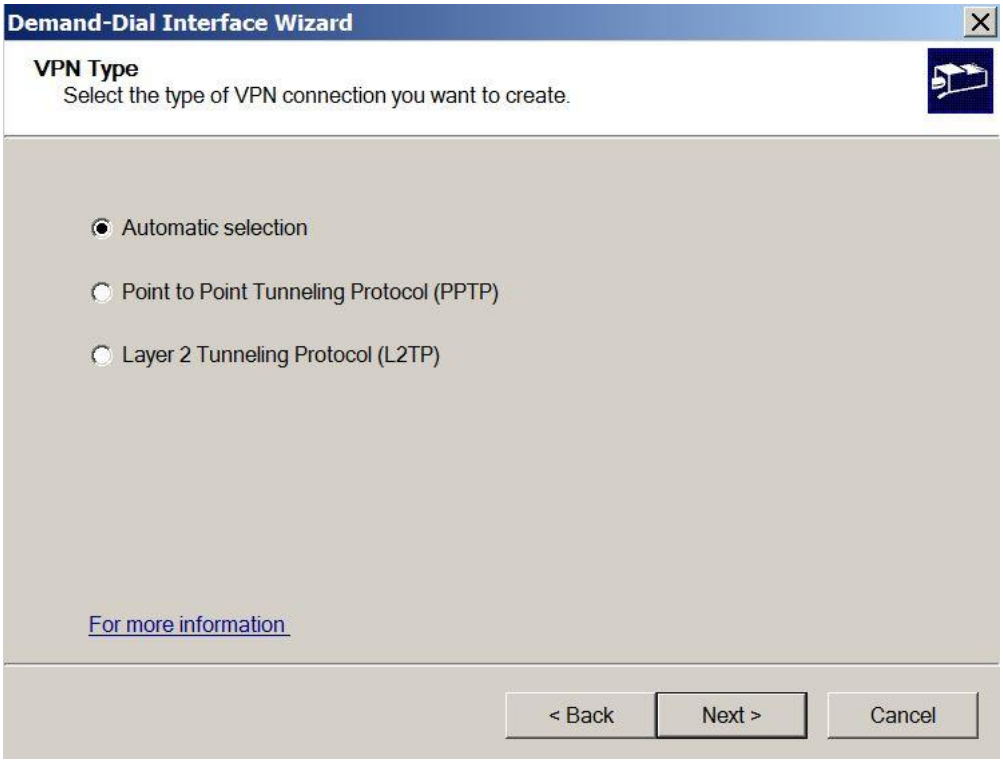

Routing and Remote Access
Start the service
The Routing and Remote Access service is ready to use.
Start service
Cancel


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
BM-SERVER (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging &
IPv4
IPv6
General
Static Routes
BM-SERVER (local)
Routing and Remote Access Is Configured on This Server
This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.
For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
BM-SERVER (local)
Network Interfaces
Ports
Remote Ac
Remote Ac
IPv4
IPv6
General
Static Routes
New Demand-dial Interface...
Refresh
Help
BM-SERVER (local)
Routing and Remote Access Is Configured on This Server
already been configured using the Routing and Remote
Setup Wizard. To make changes to the current
elect an item in the console tree, and then on the Action
perties.
For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.
Displays Help for the current selection.


Demand-Dial Interface Wizard
Interface Name
You can type a friendly name for this connection.
Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.
Interface name:
hcm
< Back
Next >
Cancel


Demand-Dial Interface Wizard
Connection Type
Select the type of demand-dial interface you want to create.
Connect using a modem, ISDN adapter, or other device
Connect using virtual private networking (VPN)
Connect using PPP over Ethernet (PPPoE)
For more information
< Back
Next >
Cancel


Demand-Dial Interface Wizard
VPN Type
Select the type of VPN connection you want to create.
Automatic selection
Point to Point Tunneling Protocol (PPTP)
Layer 2 Tunneling Protocol (L2TP)
For more information
< Back
Next >
Cancel

**Demand-Dial Interface Wizard**

**Destination Address**
What is the name or address of the remote router?

Enter the name or IP address of the router you are connecting to.

Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111 ):

10.0.0.3

< Back | Next > | Cancel

**Demand-Dial Interface Wizard**

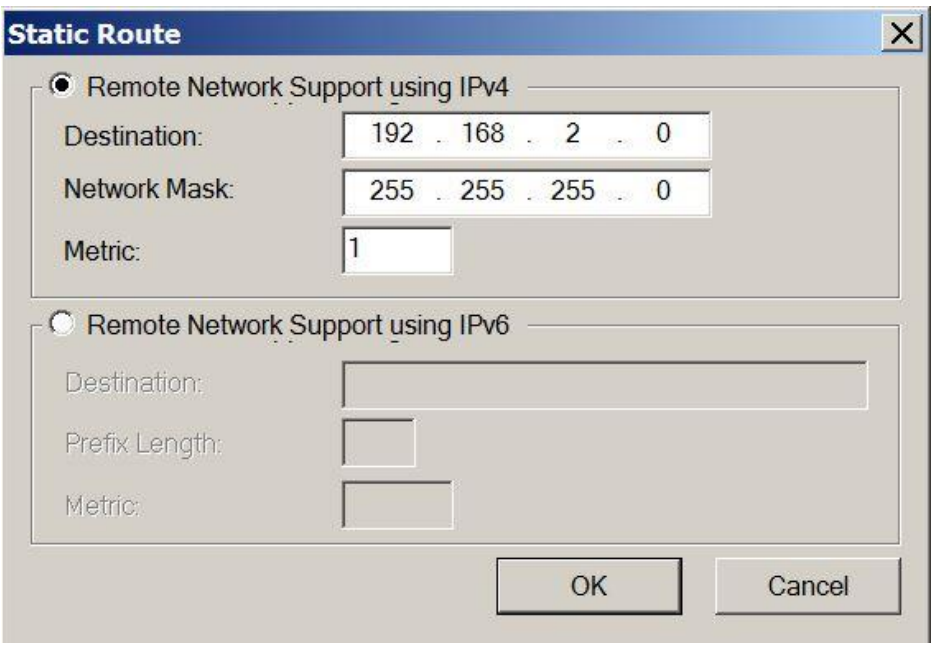
**Protocols and Security**
Select transports and security options for this connection.

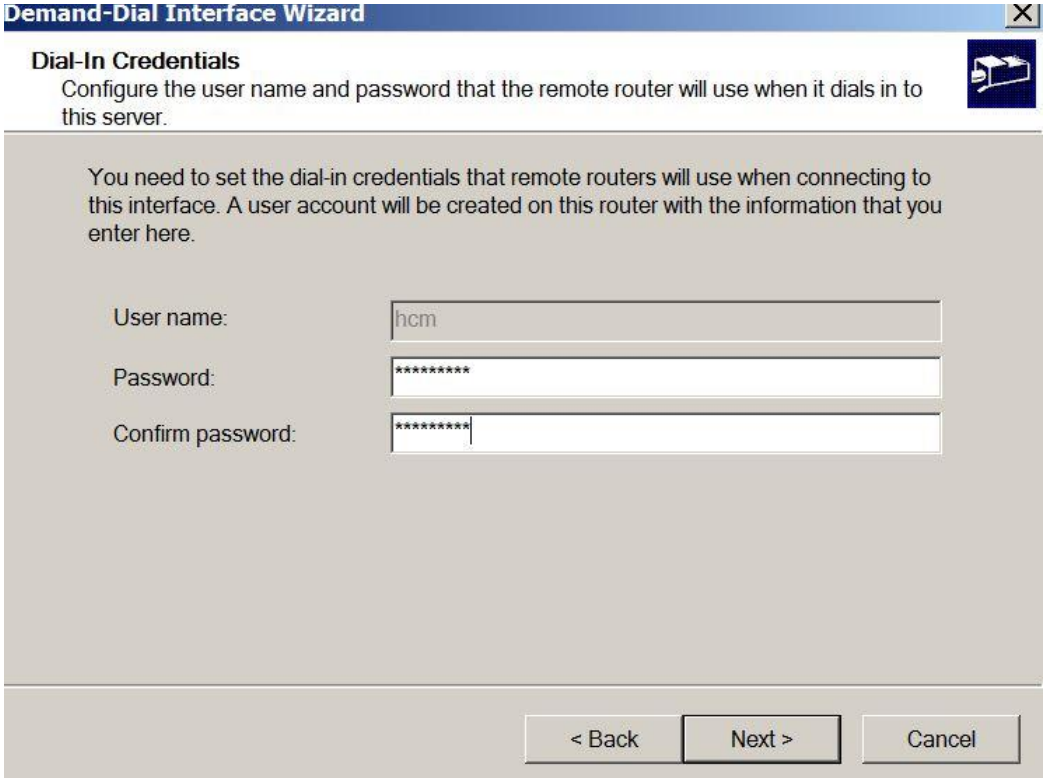
Select all that apply:

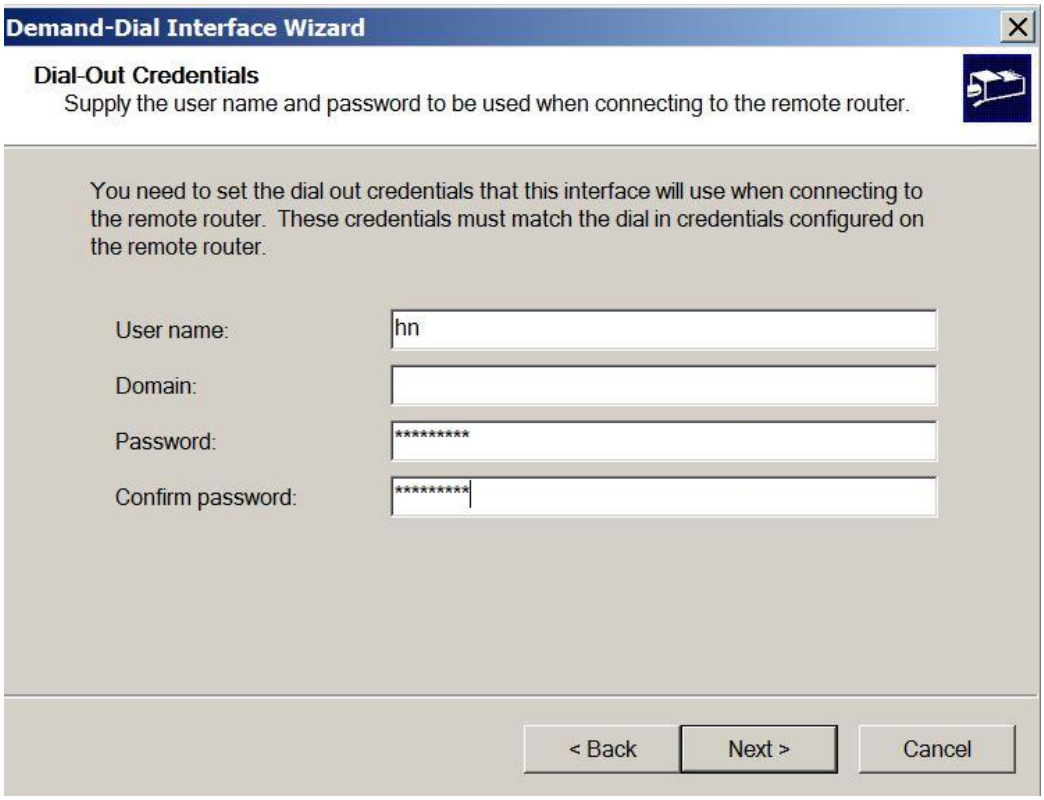
- [x] Route IP packets on this interface.
- [x] Add a user account so a remote router can dial in
- [ ] Send a plain-text password if that is the only way to connect
- [ ] Use scripting to complete the connection with the remote router

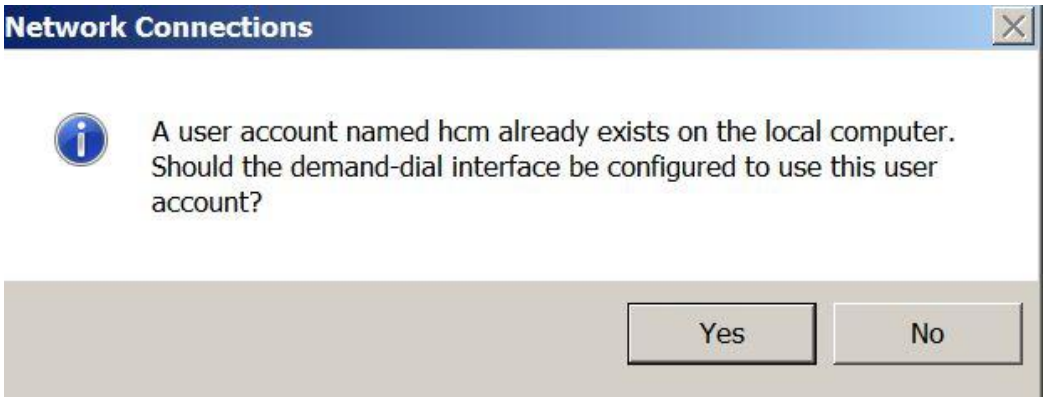
For more information

< Back | Next > | Cancel

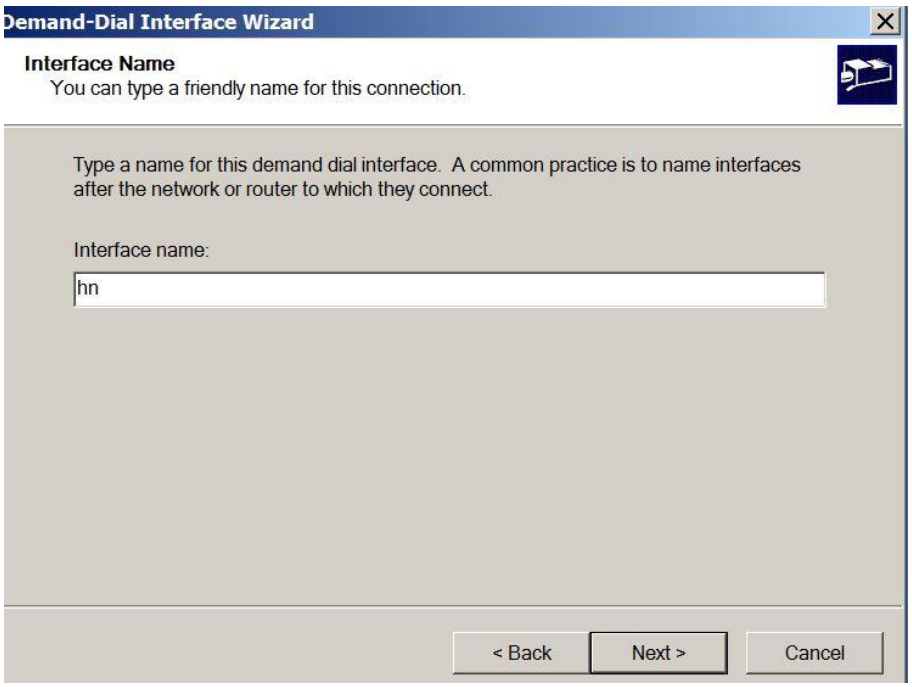

Static Route
Remote Network Support using IPv4
Destination:
192 . 168 . 2 . 0
Network Mask:
255 . 255 . 255 . 0
Metric:
1
Remote Network Support using IPv6
Destination:
Prefix Length:
Metric:
OK
Cancel

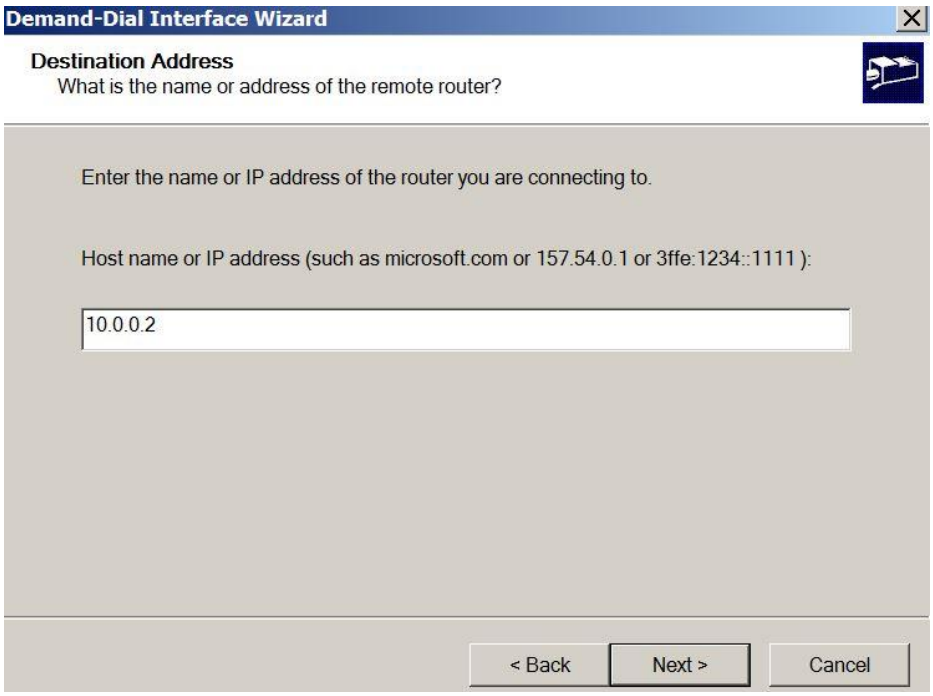

Demand-Dial Interface Wizard
Dial-In Credentials
Configure the user name and password that the remote router will use when it dials in to this server.
You need to set the dial-in credentials that remote routers will use when connecting to this interface. A user account will be created on this router with the information that you enter here.
User name:
hcm
Password:
*********
Confirm password:
*********
< Back
Next >
Cancel

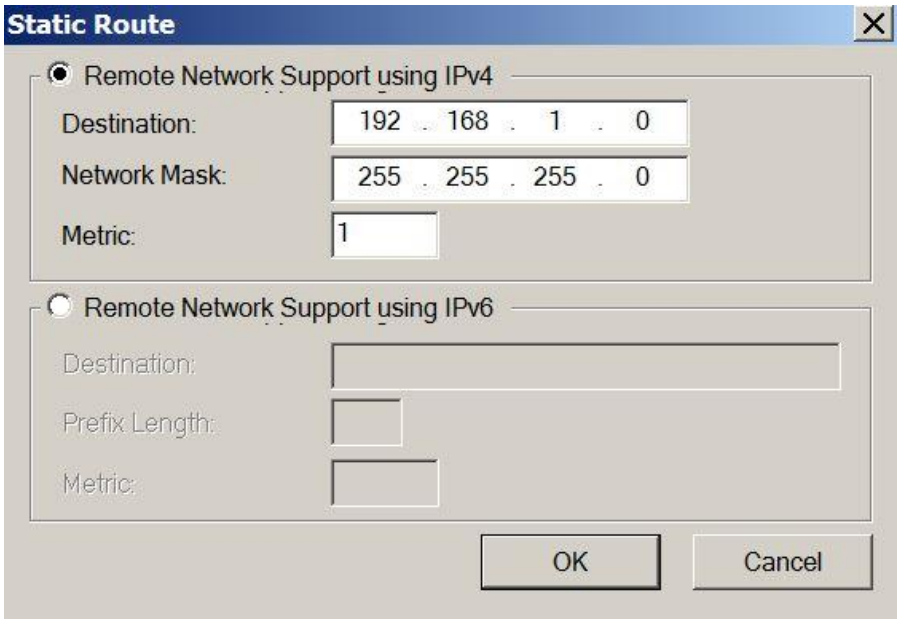


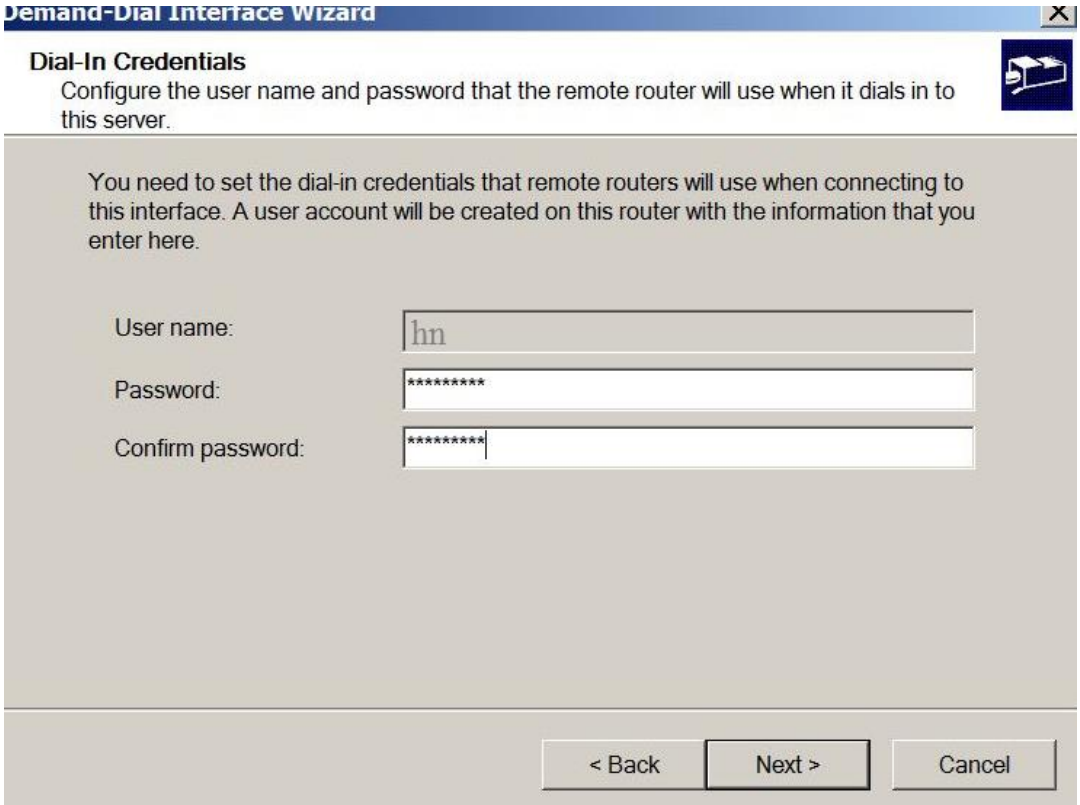



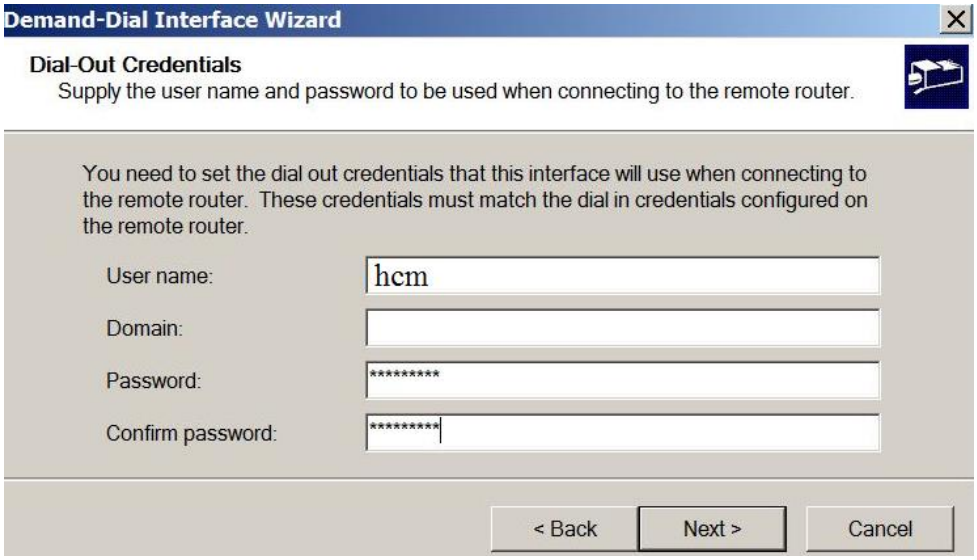

Site to Site VPN configuration on VPN Gateway 2 is performed similarly to that on VPN Gateway 1. Note the following related configuration parameters:


Demand-Dial Interface Wizard
Interface Name
You can type a friendly name for this connection.
Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.
Interface name:
hn
< Back
Next >
Cancel

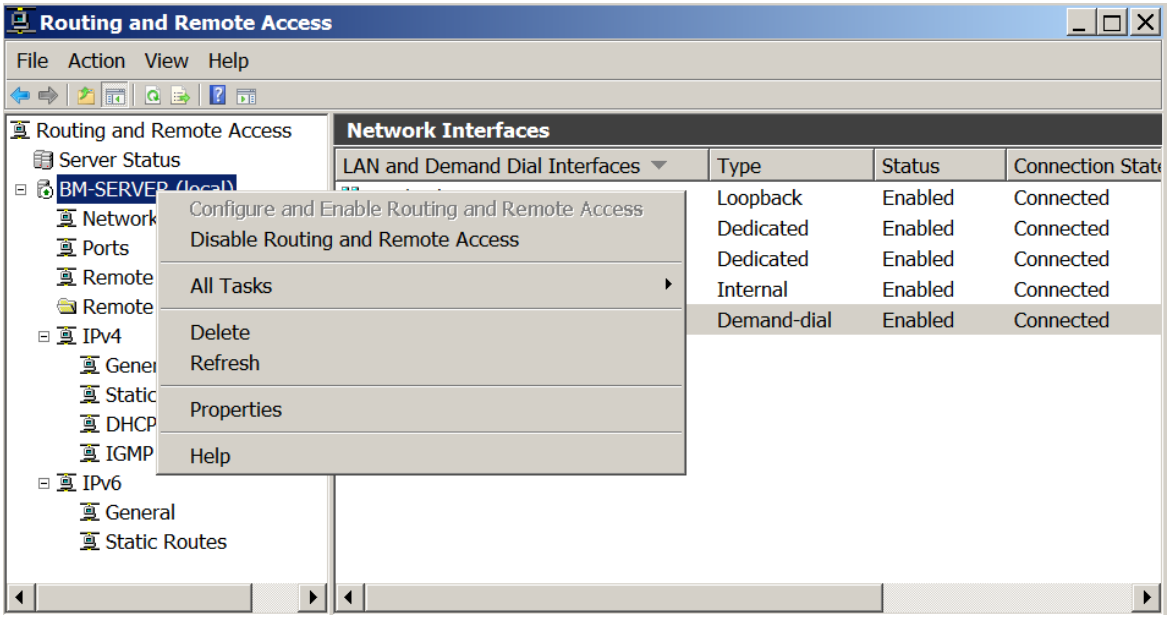

Demand-Dial Interface Wizard
Destination Address
What is the name or address of the remote router?
Enter the name or IP address of the router you are connecting to.
Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111 ):
10.0.0.2
< Back
Next >
Cancel

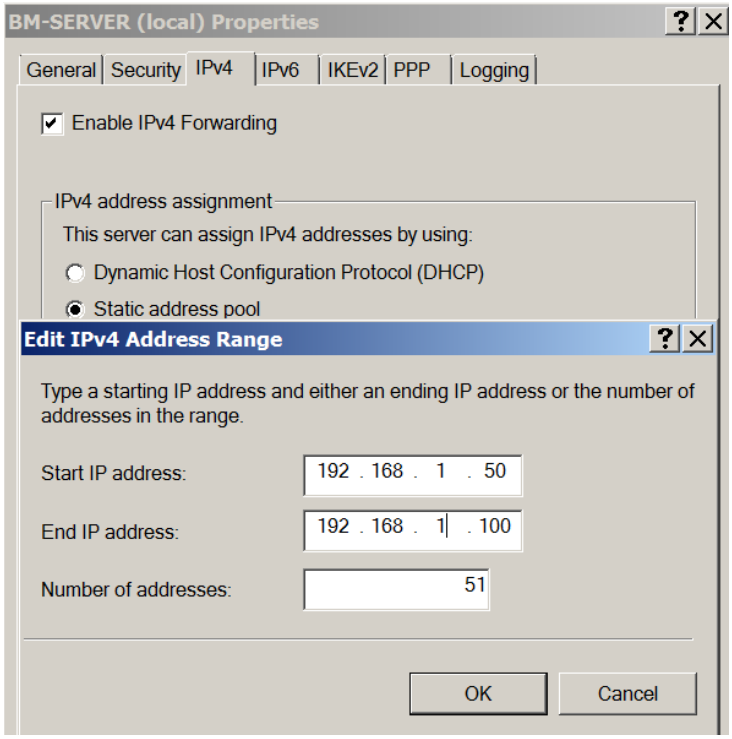

Static Route
Remote Network Support using IPv4
Destination:
192 . 168 . 1 . 0
Network Mask:
255 . 255 . 255 . 0
Metric:
1
Remote Network Support using IPv6
Destination:
Prefix Length:
Metric:
OK
Cancel



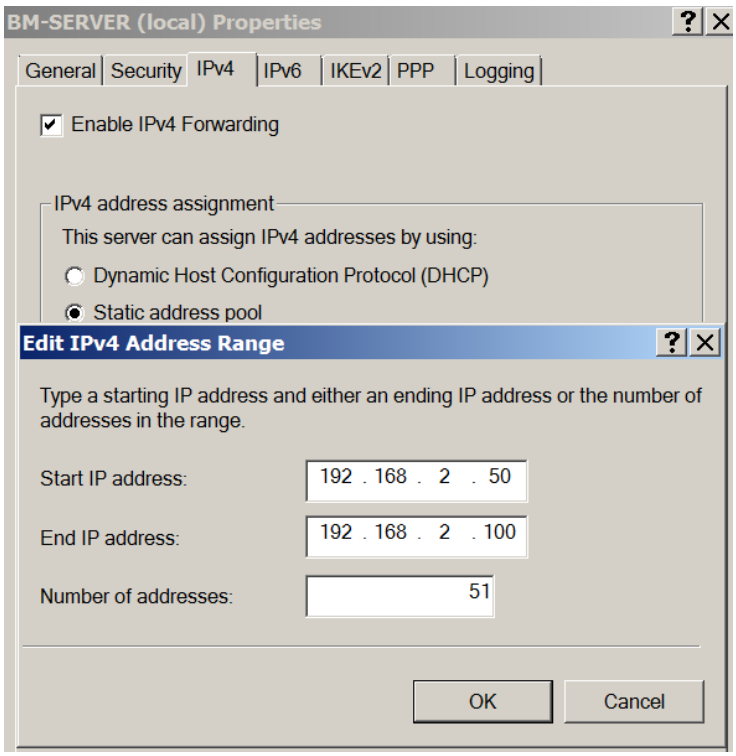




Note: If the system network in the HN and HCM sites does not have a DHCP server providing IP addresses to the stations, it is necessary to configure additional IP addresses for the VPN server to provide to the stations when performing IPSec Vpn:



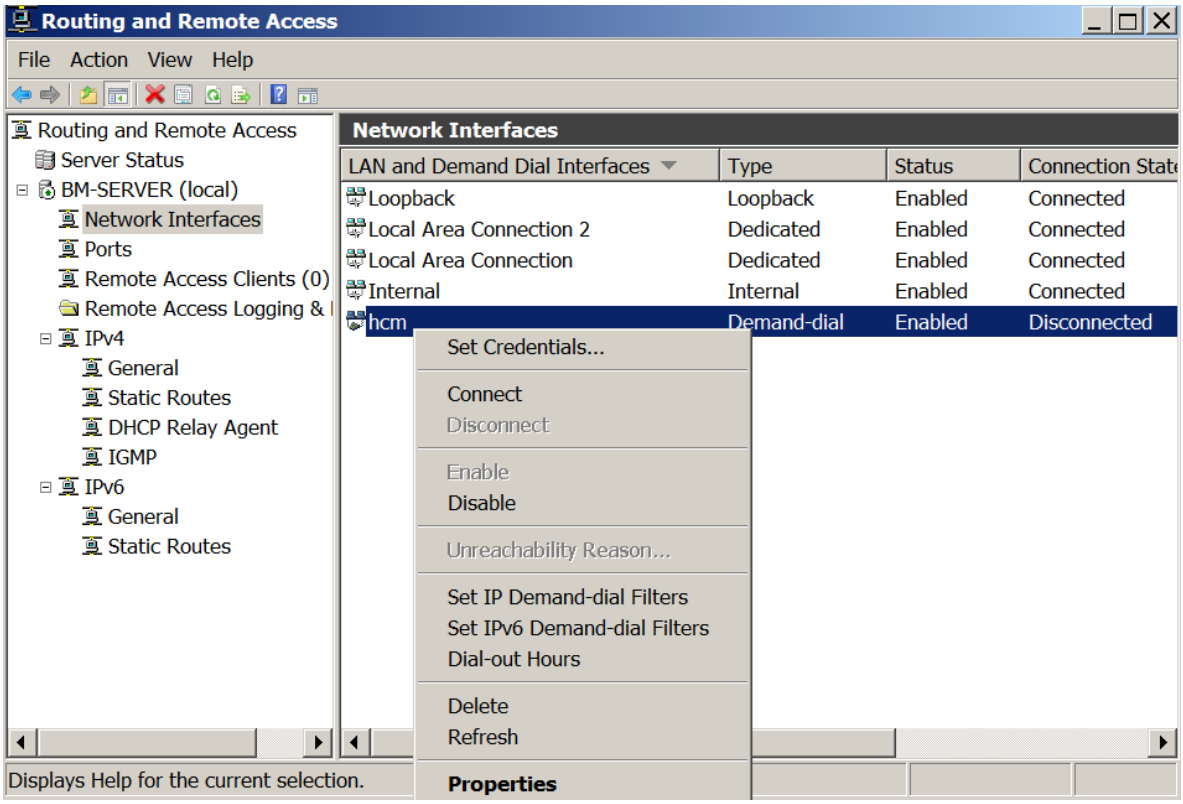




Do the same with VPN Gateway 2:

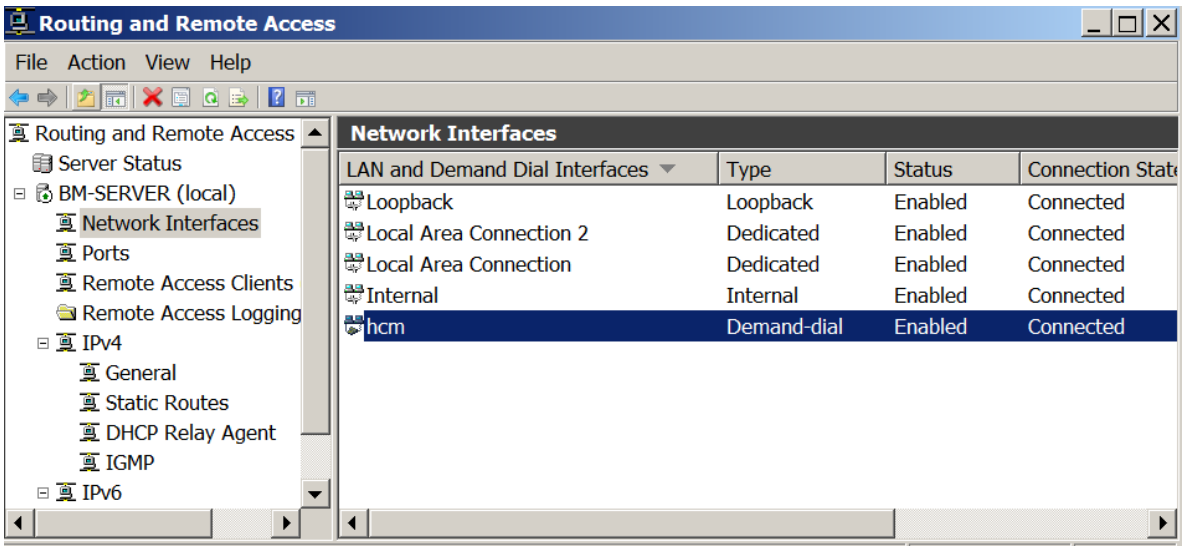



### 1.5.6 Implement IPSec VPN connections between VPN Gateways

In VPN Gateway 1

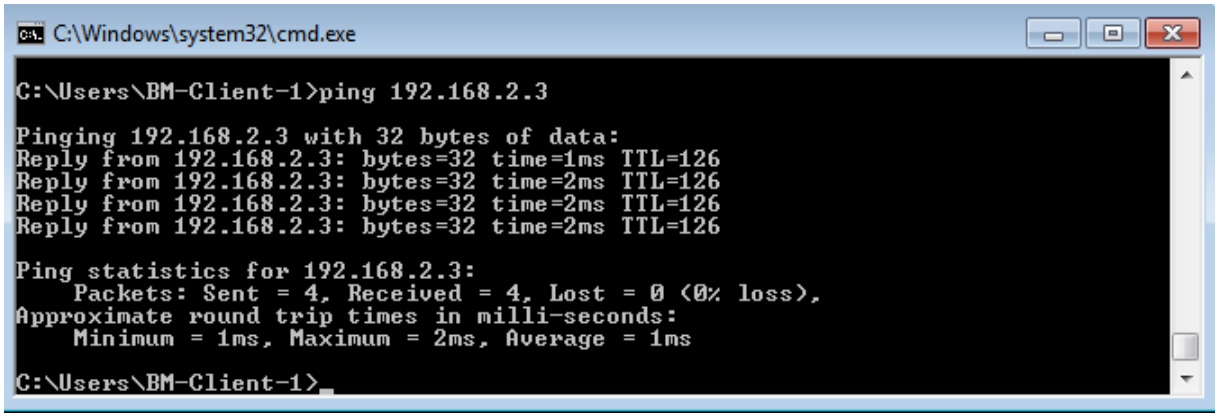



IPSec VPN is successfully executed when the Connected status is set at the hcm interface. Then, at the Routing and Remote Access window at VPN Gateway 2, the hn interface will also have the Connected status.

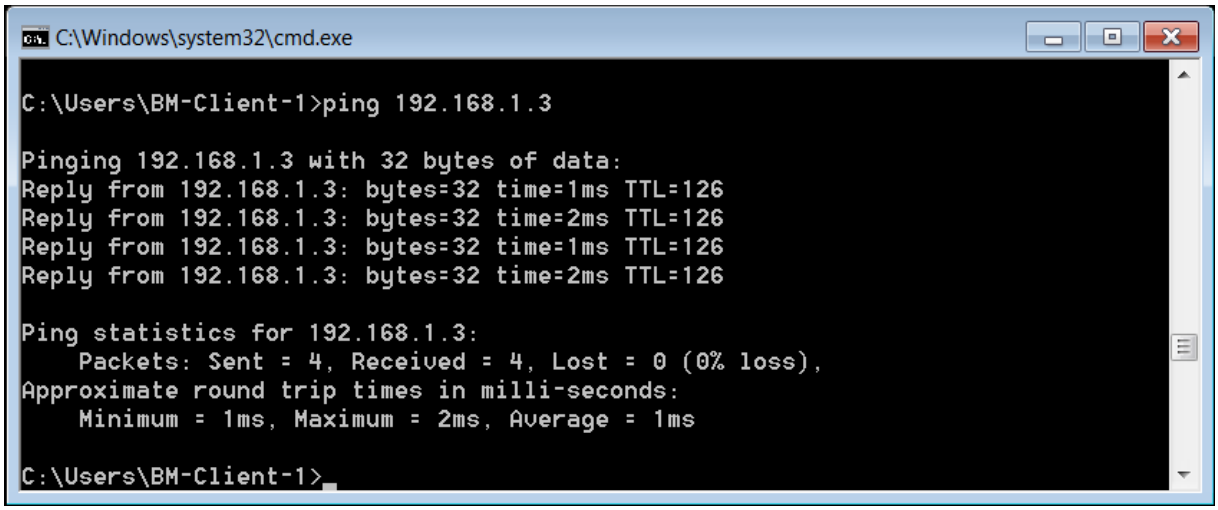



### 1.5.7. Test connectivity between networks in VPN

On Win 7-1 machine (on site HN), pinging Win 7-2 machine (on site HCM) shows successful ping.




Similarly, ping from Win 7-2 to Win 7-1 machine is successful




Complete user data sharing via Site to Site VPN

**End of practice**