

HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN



BÀI THỰC HÀNH SỐ 05.1

CẤU HÌNH MẠNG VPN CLIENT TO SITE TRÊN NỀN TẢNG WINDOWS SERVER 2012 R2

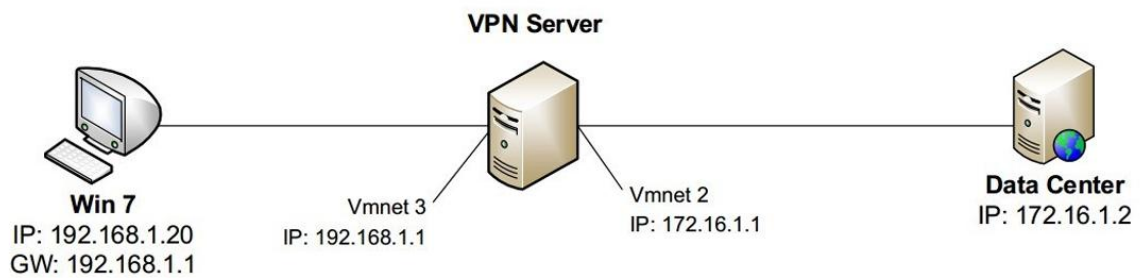
Sinh viên thực hiện: Nguyễn Hữu Văn – AT190157

Hà Nội, 2025

Mục Lục

I. Mô hình triển khai.....	3
II. Các bước thực hiện	4
Thực hiện trên máy Data Center:	4
Thực hiện trên máy chủ VPN Server	6
Thực hiện trên máy Win 7:.....	14
III. Cấu hình VPN với giao thức L2TP kết hợp với IPSec	17
Thực hiện trên máy VPN Server	17
Thực hiện trên máy Win7	17

I. Mô hình triển khai



Cần 1 máy Win 7 và 2 máy Win 2012, 1 máy làm VPN Server, 1 máy làm Data Center

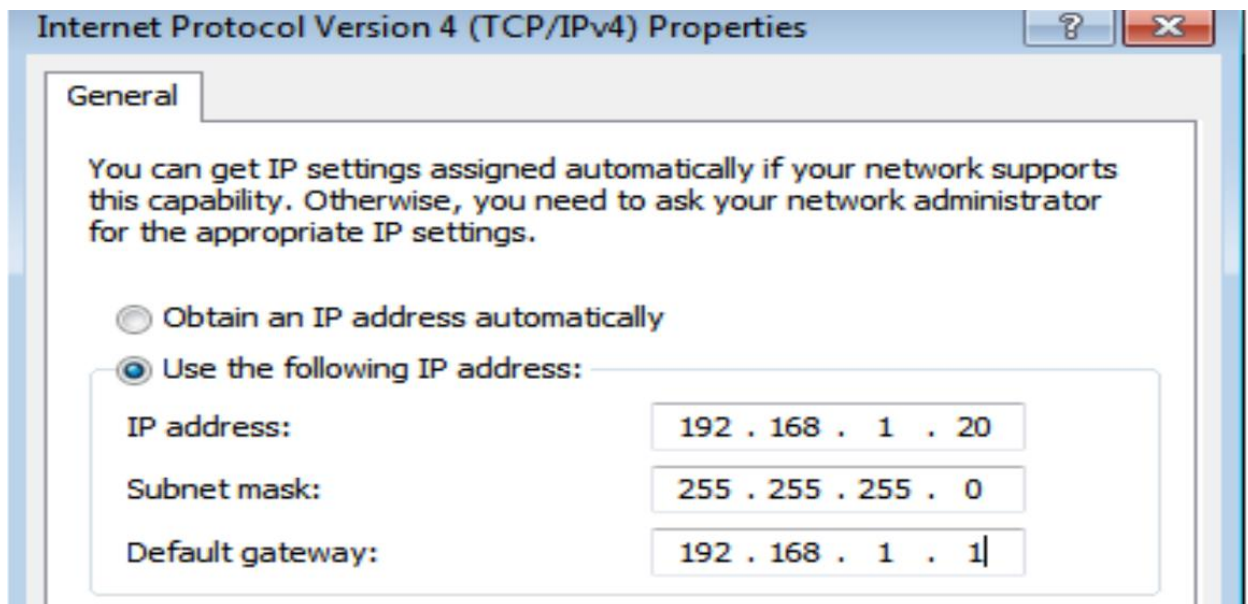
Đặt giao diện mạng và IP máy Window 7:

Giao diện mạng:

▼ Devices

Memory	2 GB
Processors	1
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Using file F:\Win...
Floppy	Using file autoin...
Network Adapter	Custom (VMnet3)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

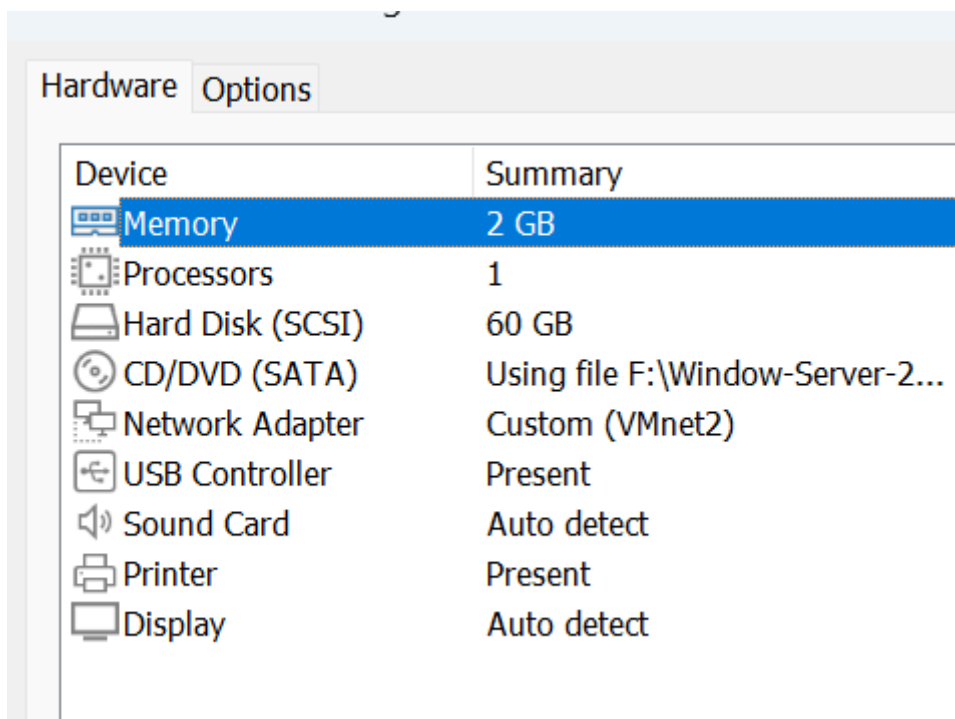
Địa chỉ IP máy Win7:



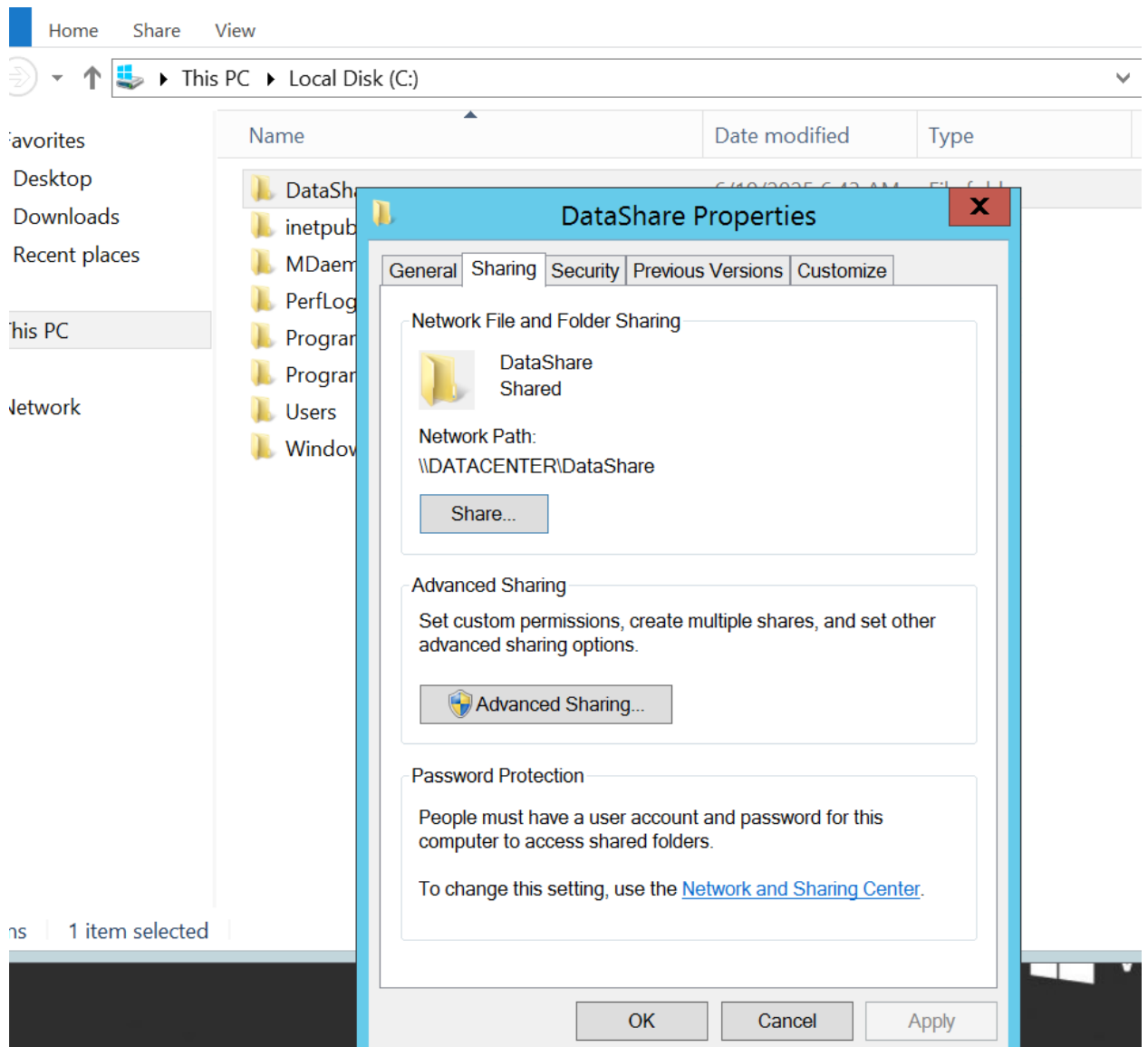
II. Các bước thực hiện

Thực hiện trên máy Data Center:

Giao diện mạng:



Tạo thư mục và chia sẻ thư mục DataShare:



Cấu hình IP:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

172 . 16 . 1 . 2

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

172 . 16 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:











.

Alternate DNS server:

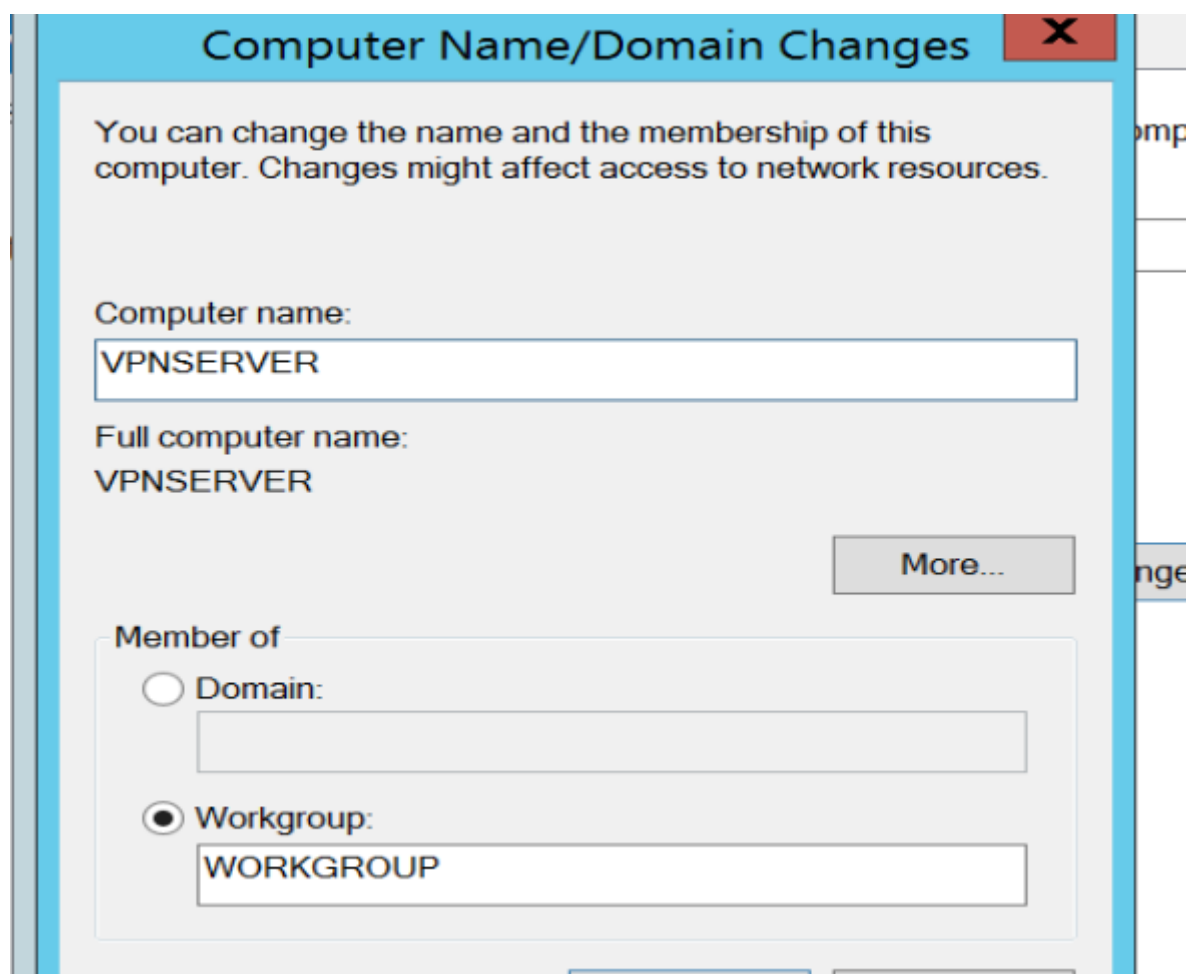
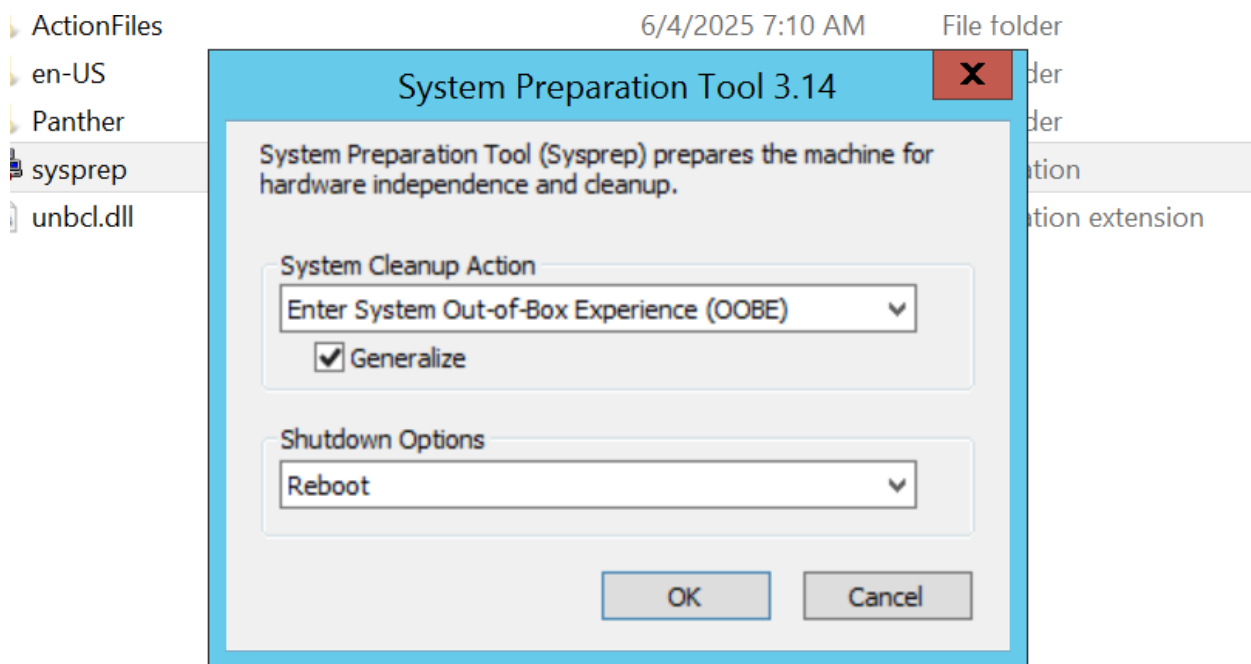
.

Thực hiện trên máy chủ VPN Server

Giao diện mạng:

Device	Summary
 Memory	2 GB
 Processors	1
 Hard Disk (SCSI)	60 GB
 CD/DVD (SATA)	Using file F:\Window-Server-2...
 Network Adapter	Custom (VMnet2)
 Network Adapter 2	Custom (VMnet3)
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect

Thay đổi SID và tên máy chủ hiện tại:



cấu hình địa chỉ IP cho 2 giao diện mạng:

Ethernet0 địa chỉ IP:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 172 . 16 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Ethernet1 địa chỉ IP:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Kết thúc, Ping tới các máy DataCenter và Win7 để kiểm tra kết nối:


```

C:\Users\Administrator>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=2ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
Control-C
^C
C:\Users\Administrator>

```

Cài đặt dịch vụ Remote Access:

Add Roles and Features Wizard

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Confirmation

Results

Select one or more roles to install on the selected server.

Roles	Description
<input type="checkbox"/> Application Server	Remote Access provides connectivity through VPN, and Web App DirectAccess provides and Always Managed RAS provides traditional services, including secure (branch-office or cloud) connectivity. Web App enables the publish HTTP- and HTTPS-based applications from your network to client devices on the corporate network. Remote Access provides traditional capabilities, including connectivity options. Routing can be deployed on a per-tenant or multi-tenant basis.
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
▶ <input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input checked="" type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	
<input type="checkbox"/> Windows Server Essentials Experience	
<input type="checkbox"/> Windows Server Update Services	

Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Web Server Role (IIS)

Role Services

Select the role services to install for Remote Access

Role services

☒ DirectAccess and VPN (RAS)

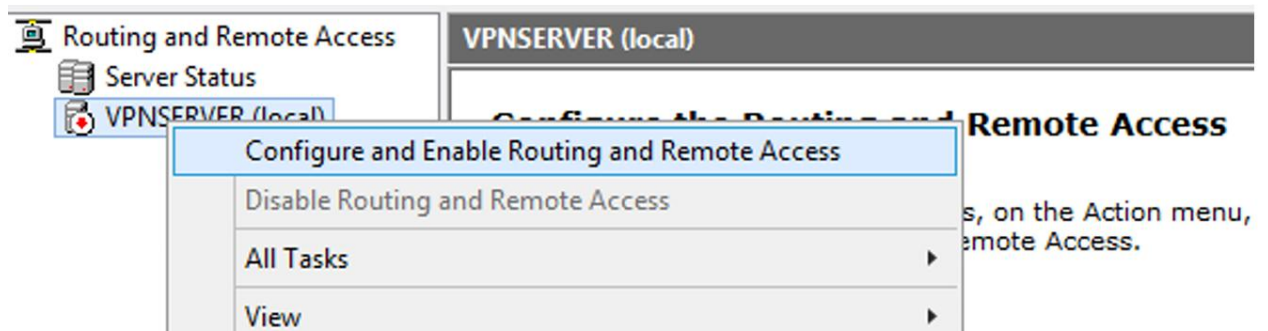
☒ **Routing**

☐ Web Application Proxy

Cấu hình dịch vụ Routing and Remote Access:

trong giao diện Server Manager, các chức năng trên góc phải chọn Tools → Routing and Remote Access

tiếp tục



Configuration

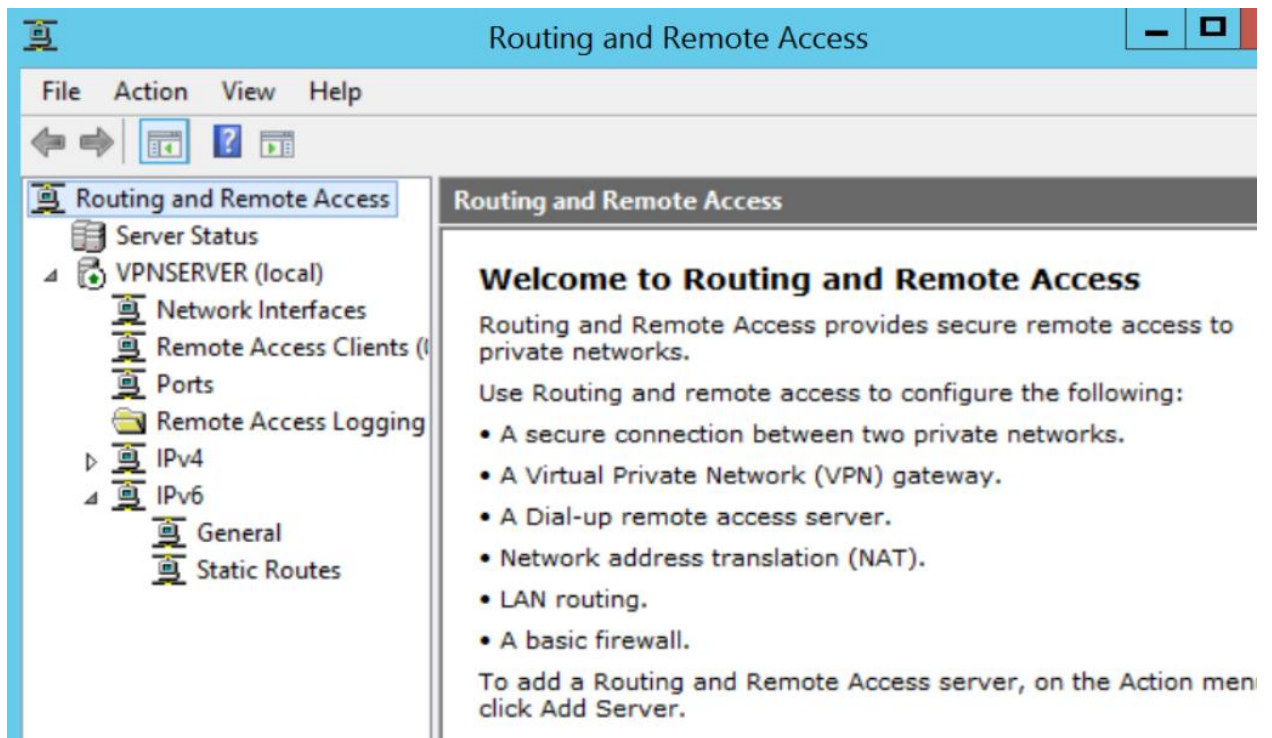
You can enable any of the following combinations of services, or you can customize this server.

- ☐ 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.

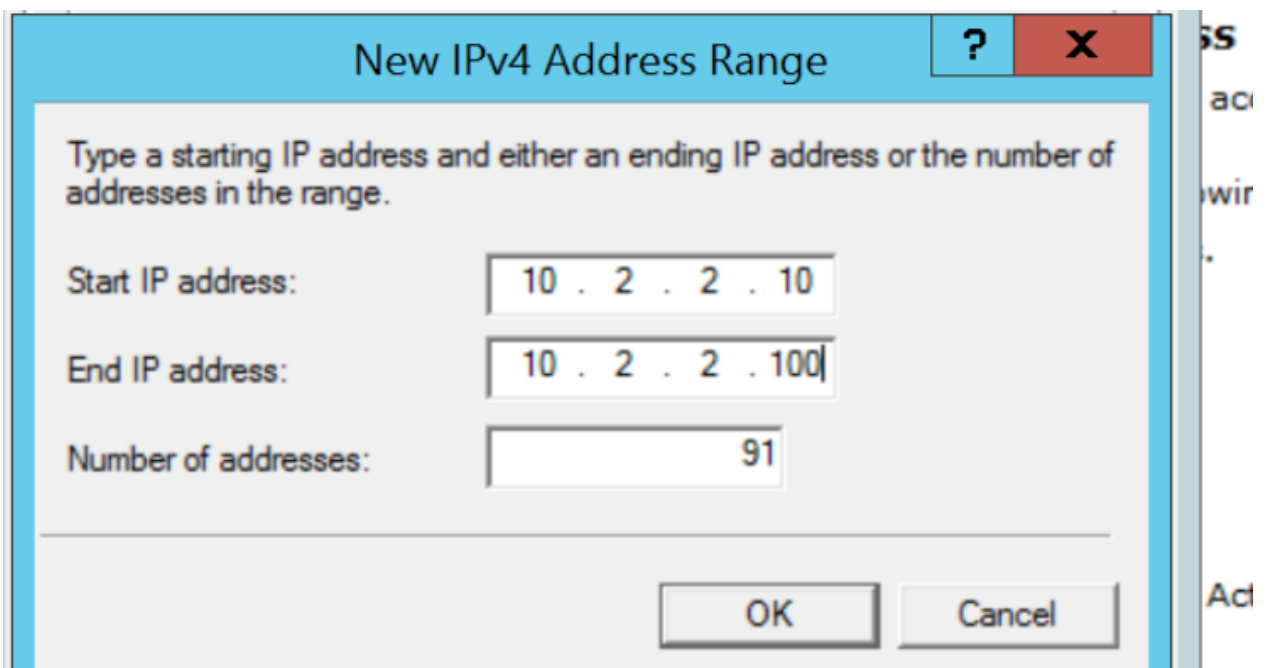
Select the services that you want to enable on this server.

- ☒ VPN access
- ☐ Dial-up access
- ☐ Demand-dial connections (used for branch office routing)
- ☐ NAT
- ☒ LAN routing

Sau khi cấu hình giao diện như sau:



Tiếp theo cần phải cấu hình địa chỉ IP sử dụng cho đường hầm. Chuột phải vào VPNSERVER chọn Properties → IPv4 → static address pool → Add:



Tạo người dùng VPN:

Tiếp theo cần phải tạo tài khoản người dùng VPN, tài khoản này sử dụng để xác thực người dùng truy cập từ xa. Từ Server Manager → Tools → Computer Management → Local User and Group → Users. Chuột phải chọn New User

New User

User name: vpnuser

Full name:

Description:

Password: ●●●●●●●●

Confirm password: ●●●●●●●●

☐ User must change password at next logon

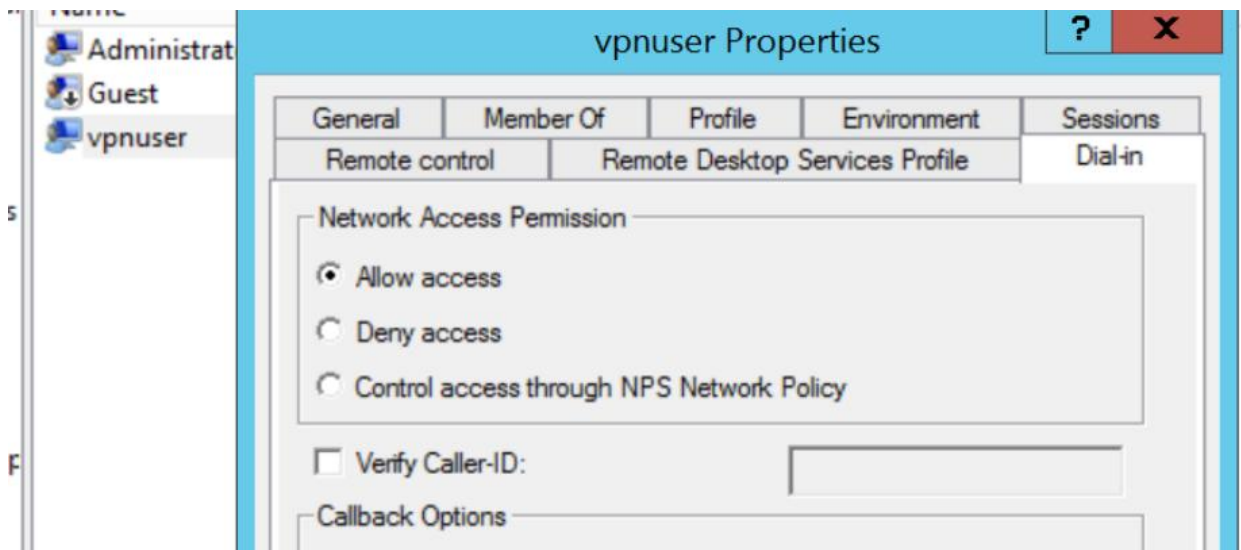
☐ User cannot change password

☒ Password never expires

☐ Account is disabled

Help Create Close

Sau khi tài khoản được tạo xong, chuột phải vào tên tài khoản chọn Properties. Trong tab dial-in chọn Allow access.

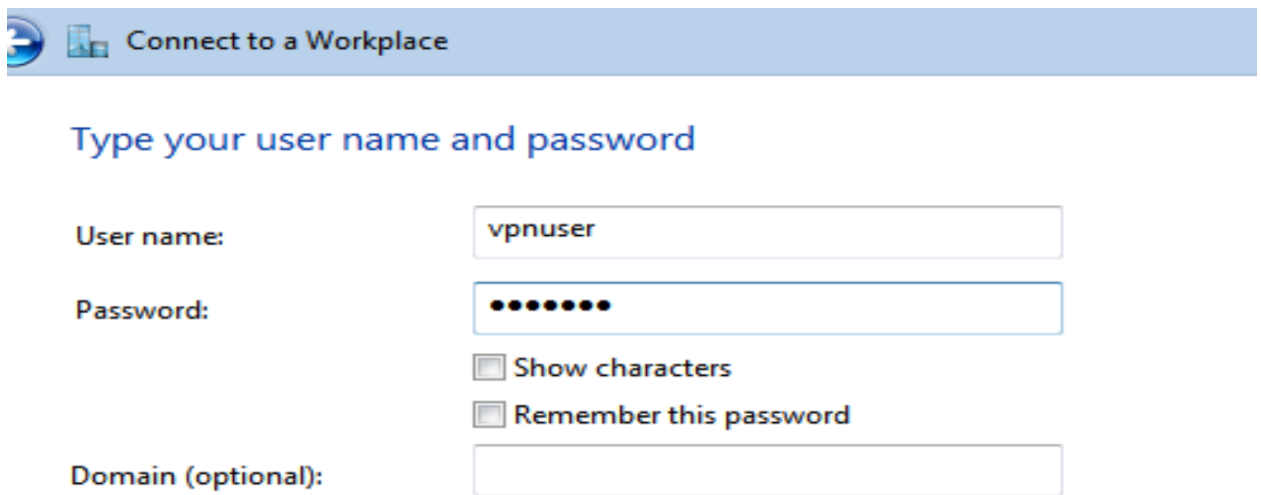


Thực hiện trên máy Win 7:

Tạo kết nối VPN:

Bật của sổ quản trị Network. Kích chọn Setup a new connection. Cửa sổ tiếp theo chọn Connect to a workplace → Next Giao diện tiếp theo chọn Use my Internet Connection Giao diện tiếp theo chọn I'll set up an Internet connection later. Giao diện tiếp theo nhập địa chỉ IP bên ngoài của máy chủ VPN (thông thường đây chính là địa chỉ IP Public).

Giao diện tiếp theo nhập tên tài khoản và mật khẩu đã tạo trên máy chủ



Connect to a Workplace

Type your user name and password

User name:

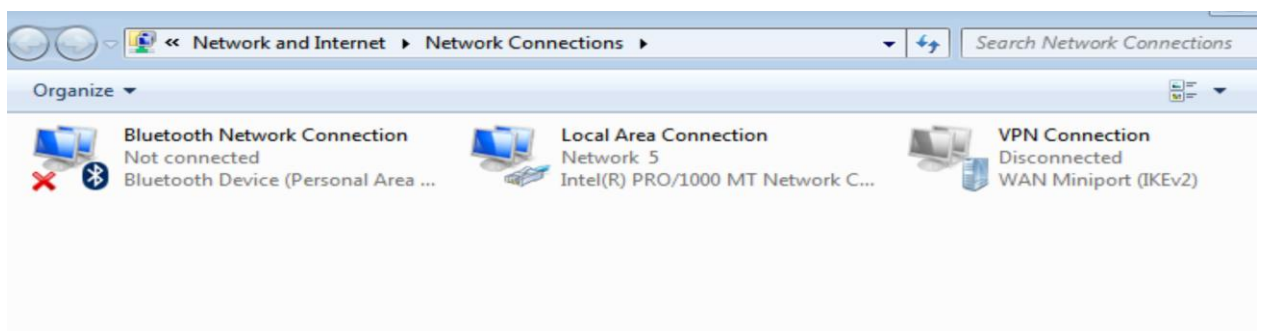
Password:

☐ Show characters

☐ Remember this password

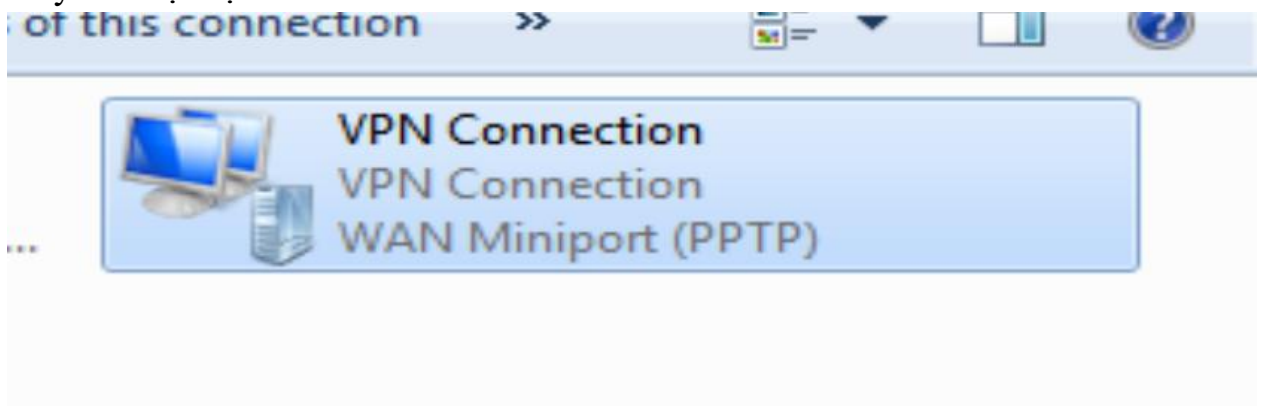
Domain (optional):

Tiếp theo thực hiện kết nối vào mạng bên trong sử dụng mạng VPN. Truy cập vào giao diện quản trị Network.



Chúng ta thấy biểu tượng kết nối mạng VPN. Kích đúp vào biểu tượng kết nối VPN. Giao diện đăng nhập xuất hiện, nhập mật khẩu cho tài khoản vpn → Connect.

Kết nối thành công, lúc này người dùng từ xa có thể truy cập tới tài nguyên trên máy chủ nội bộ của tổ chức DataCenter



Kiểm tra kết nối - Ping tới máy chủ DataCenter:

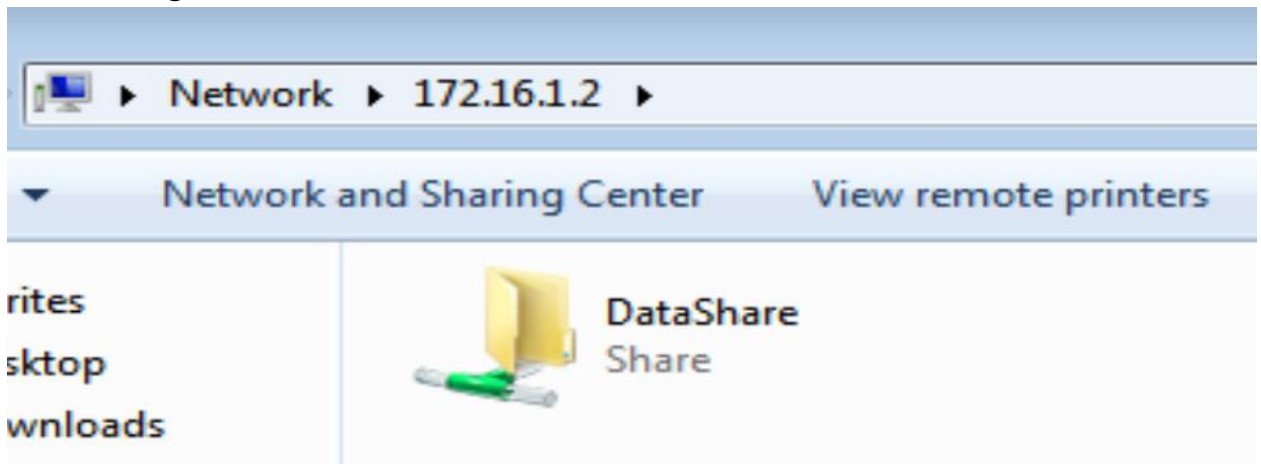
```
C:\Users\at190157>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Truy cập tới tài nguyên chia sẻ. Vào RUN gõ [\\172.16.1.2](http://172.16.1.2)

Thành công



Cài đặt công cụ WireShark trên máy chủ VPN Server, và lắng nghe trên giao diện mạng bên ngoài (Ethernet1).

Gói tin trên đường truyền đã được đóng gói và mã hóa với GRE và PPP. Do sử dụng cấu hình mặc định nên VPN đang sử dụng giao thức PPTP để tạo đường hầm.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.20	PPP Co...	280	Compressed data
2	0.000752	192.168.1.1	192.168.1.255	BROWSER	243	Host Announcement VPNSERV
3	0.103152	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP

Frame 1: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0	0000	0010	0020	0030	0040	0050	0060
▶ Ethernet II, Src: VMware_e2:23:7a (00:0c:29:e2:23:7a), Dst: 01:00:5e:00:00:00	00 0c 29	54 f8 64 00 0c	29 e2 23 7a 08 00	01 0a 67 6c 00 00	80 2f 00 00 c0 a8 01 01	01 14 30 01 88 0b 00 ea	6a 92 00 00 00 a0
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.255	90 2a fb 75 a4 20 57 4b	ba 6e 1d fd 0e 64 7a 38 05 fa 5e 7f e2 a2	03 6a fc 27 e6 6d b3 0c 8f 87 a2 9f 5e e3	cd c0 df 07 d9 18 27 7e 06 bc 76 1d 1c 59	54 9e 5e c3 05 28		
▶ Generic Routing Encapsulation (PPP)							
▶ Point-to-Point Protocol							
▶ PPP Compressed Datagram							

III. Cấu hình VPN với giao thức L2TP kết hợp với IPSec

Thực hiện trên máy VPN Server

Tại giao diện quản trị VPN Routing and Remote access. Chuột phải vào tên máy chủ VPN Server → Properties. Chọn tab Security:

set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☒ Allow custom IPsec policy for L2TP/IKEv2 connection

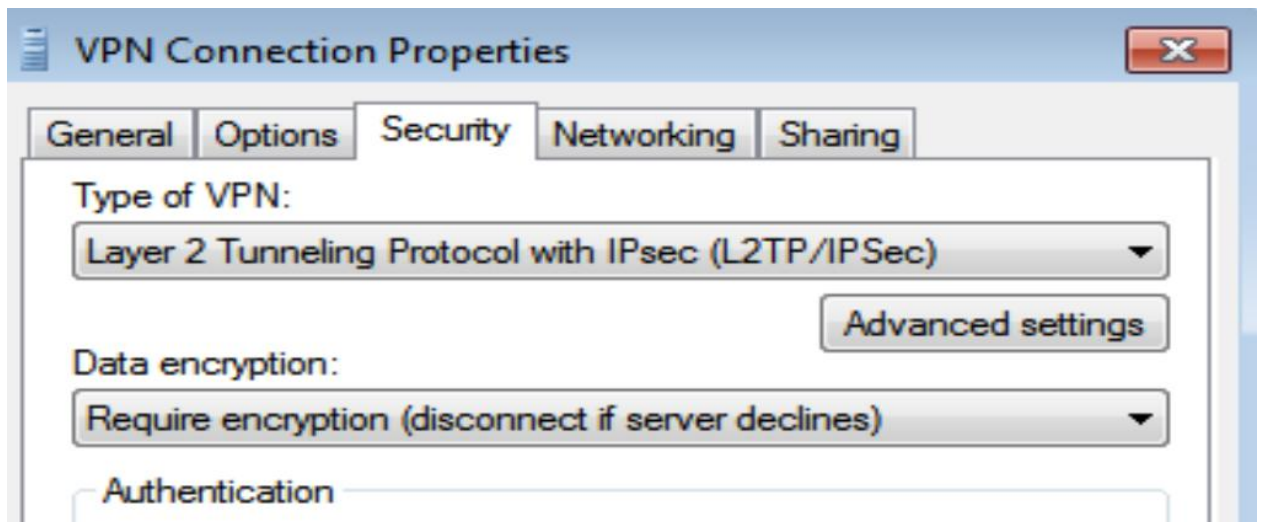
Preshared Key:

1234567890

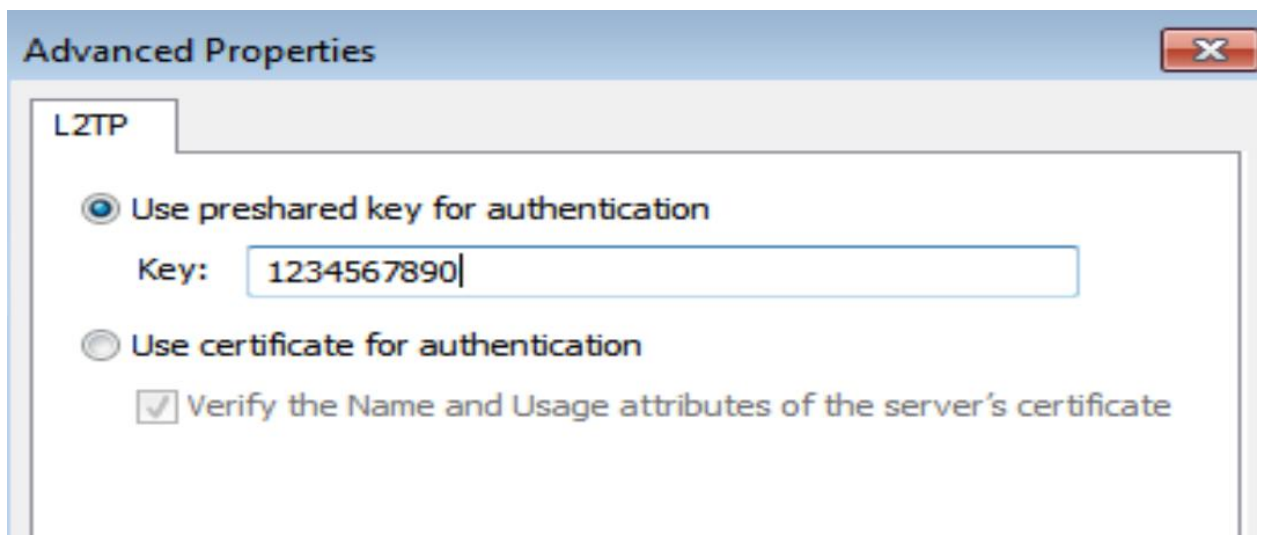
☐ SSL Certificate Binding:

Thực hiện trên máy Win7

Bật giao diện kết nối VPN. Chọn Properties. Chọn tab Security. Trong mục Type of VPN, chọn L2TP/Ipsec



Trong mục Advance setting ngay ở dưới, kích chọn và nhập khóa chia sẻ như đã nhập trên VPN Server.



Tại giao diện kết nối chính, nhập tài khoản người dùng truy cập từ xa. Nhấn Connect để kết nối.

Kiểm tra kết quả: - Thực hiện Ping từ máy Win 7 vào máy DataCenter:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\at190157>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=3ms TTL=127
Reply from 172.16.1.2: bytes=32 time=1ms TTL=127
Reply from 172.16.1.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.1.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
Control-C
  
```

Chặn bắt gói tin trên máy VPN Server (lắng nghe tại cổng phía ngoài):

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.20	ESP	102	ESP (SPI=0x883a2102)
2	0.000669	192.168.1.20	192.168.1.1	ESP	102	ESP (SPI=0xb3f02b26)

Lúc này lưu lượng dữ liệu kết nối đã được mã hóa bằng giao thức ESP của Ipsec. Kết thúc bài thực hành.