

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 05.1

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

Người xây dựng bài thực hành:

ThS. Cao Minh Tuấn

HÀ NỘI, 2017

MỤC LỤC

Mục lục	2
Thông tin chung về bài thực hành	3
Chuẩn bị bài thực hành	4
Đối với giảng viên	4
Đối với sinh viên	4
 Phần 1. CÀI ĐẶT CẤU HÌNH MẠNG vpn THEO MÔ HÌNH CLIENT-TO-SIDE.....	 5
1.1. Chuẩn bị	5
1.2. Mô hình triển khai	5
1.3. Mô tả công việc cần thực hiện.....	5
1.4. Các bước thực hiện.....	6
<i>1.4.1. Thực hiện trên máy chủ Data Center.....</i>	<i>6</i>
<i>1.4.2. Thực hiện trên máy chủ VPN Server.....</i>	<i>6</i>
<i>1.4.3. Thực hiện trên máy Win 7</i>	<i>14</i>
1.5. Cấu hình VPN với giao thức L2TP kết hợp với IPSec	18
<i>1.5.1. Thực hiện trên máy VPN Server</i>	<i>18</i>
<i>1.5.2. Thực hiện trên máy Win7</i>	<i>18</i>

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Cấu hình mạng riêng ảo VPN trên nền tảng Windows Server 2012 R2

Số lượng sinh viên cùng thực hiện: 02

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 8GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows Server 2012 R2, Windows 7
 - + VMware Workstation 9.0 trở lên
- Công cụ thực hành:
 - + Máy ảo VMware: Windows Server 2012 R2, Windows 7
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: không
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

-
-

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

PHẦN 1. CÀI ĐẶT CẤU HÌNH MẠNG VPN THEO MÔ HÌNH CLIENT-TO-SIDE

1.1. Mô tả

Công nghệ mạng riêng ảo VPN là công nghệ tạo một đường mạng riêng trên nền tảng mạng công cộng như Internet. Mạng riêng này được đảm bảo an toàn như mã hóa, xác thực và toàn vẹn.

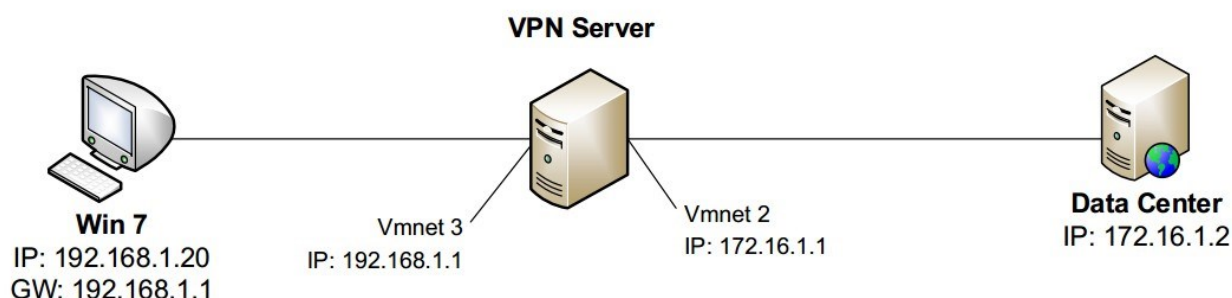
Khi triển khai mạng VPN theo mô hình Client to Side phục vụ cho người dùng truy cập từ xa tới mạng nội bộ của công ty, tổ chức. Trong mô hình này sử dụng các phương pháp mã hóa và xác thực như sau:

- Mã hóa theo giao thức PPTP
- Mã hóa theo giao thức L2TP/IPSec
- Mã hóa theo giao thức SSTP
- Xác thực theo giao thức RADIUS

1.2. Chuẩn bị

- 02 máy ảo chạy hệ điều hành Windows Server 2012.
- 01 máy ảo chạy hệ điều hành Windows 7.

1.3. Mô hình triển khai



Máy ảo VPN Server phải có 02 giao diện mạng, mỗi giao diện kết nối với Data Center và Win 7.

1.4. Mô tả công việc cần thực hiện

Thực hiện trên máy Data Center:

- Tạo thư mục chia sẻ dữ liệu: DataShare
- Thực hiện trên máy VPN Server:
- Thêm giao diện mạng mới Vmnet 3.

- Thay đổi SID và tên máy chủ hiện tại.
- Cài đặt dịch vụ Remote Access
- Cấu hình dịch vụ Routing and Remote Access
- Tạo người dùng VPN Thực

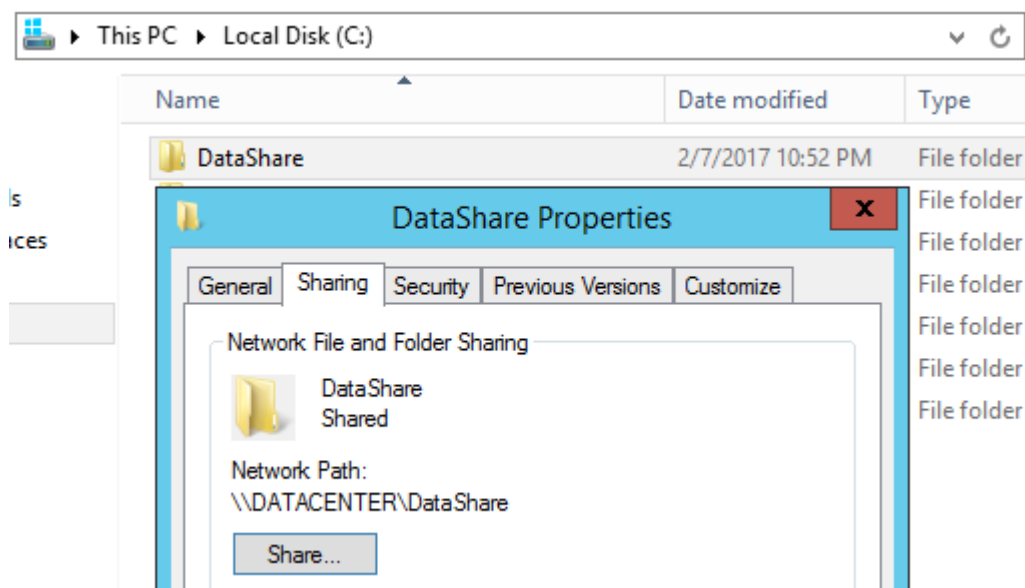
hiện trên máy Win 7:

- Tạo kết nối VPN
- Kiểm tra kết nối VPN

1.5. Các bước thực hiện

1.4.1. Thực hiện trên máy chủ Data Center:

Tạo thư mục và chia sẻ thư mục:



Cấu hình địa chỉ IP:

☐ 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:

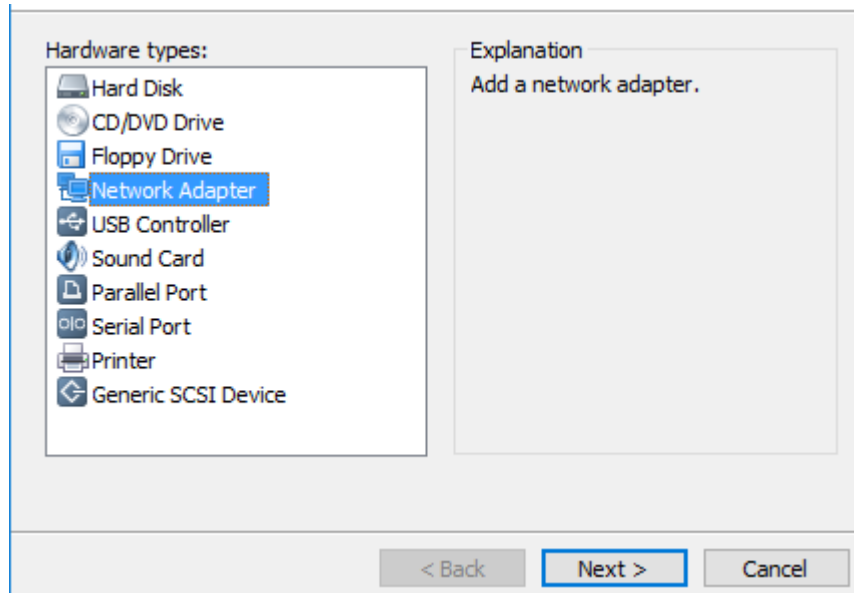
Preferred DNS server:	. . .
Alternate DNS server:	. . .

1.4.2. Thực hiện trên máy chủ VPN Server

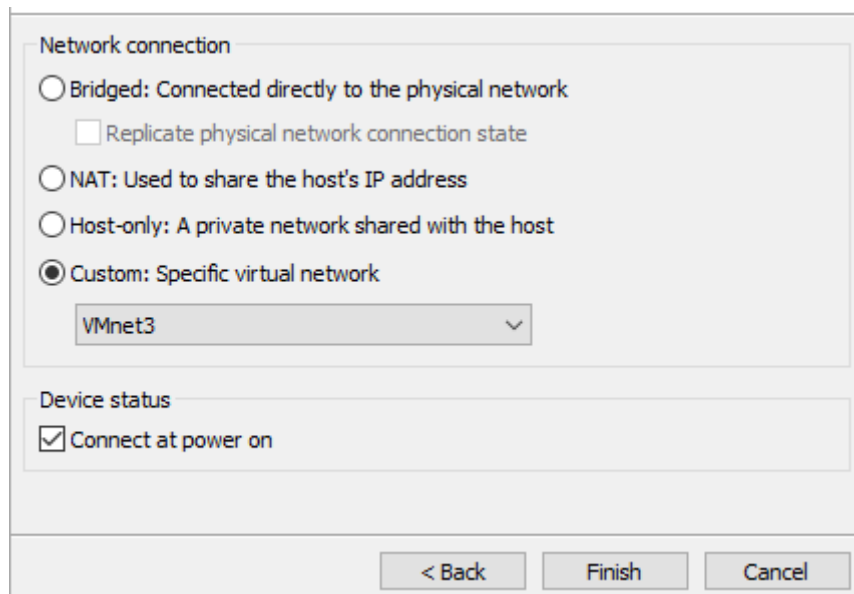
Bước 1: Thêm giao diện mạng và cấu hình địa chỉ IP

Trong giao diện quản trị Vmware khi máy ảo chưa chạy, chọn Edit virtual machine settings.

Cửa sổ xuất hiện chọn Add. Cửa sổ mới xuất hiện chọn Network Adapter.

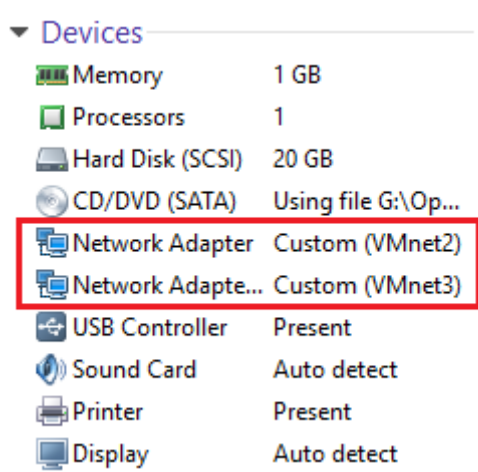


Chọn Next để tiếp tục.



Chọn Vmnet3 và Finish để kết thúc.

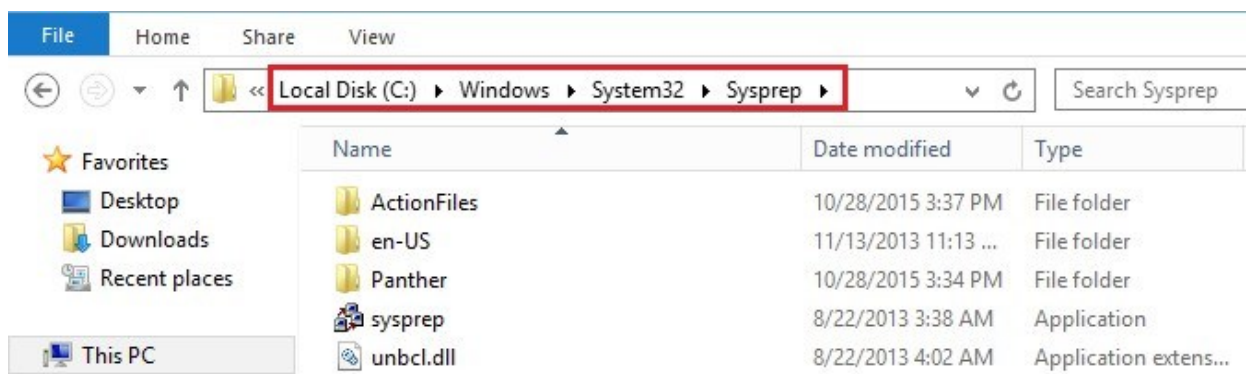
Kết quả khi chọn Vmnet cho 2 giao diện mạng như sau:



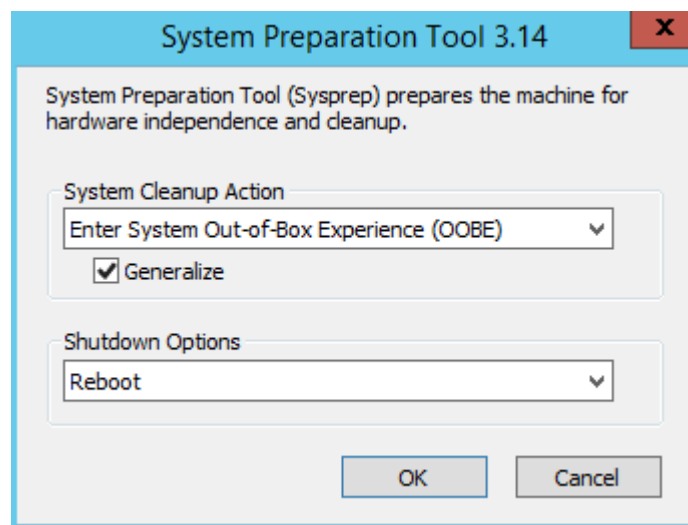
Bước 2: Thay đổi SID và tên máy chủ hiện tại

Khi sử dụng cùng một máy ảo để giải nén thành nhiều máy ảo khác thì giá trị SID và tên máy ảo bị trùng nhau. Vì vậy cần phải thay đổi giá trị này để các máy chủ có thể xác thực được với nhau trong quá trình kết nối, đặc biệt trong VPN.

Truy cập vào thư mục với đường dẫn sau:



Chuột phải vào tệp sysprep chọn Run as administrator.

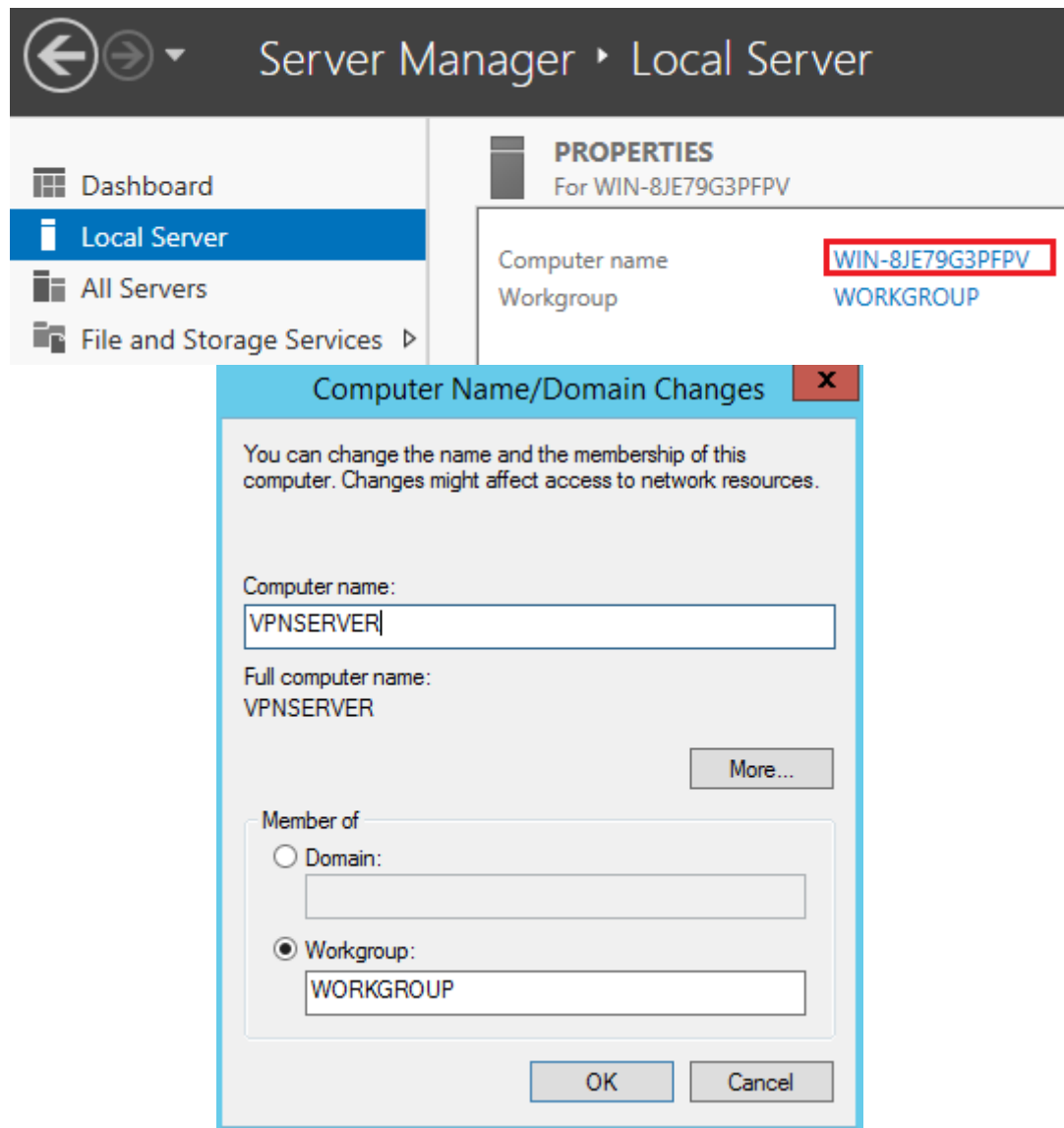


Tích vào ô **Generalize**. Và chọn OK.

Hệ thống sẽ tự động thay đổi tên máy chủ theo mặc định và giá trị SID.

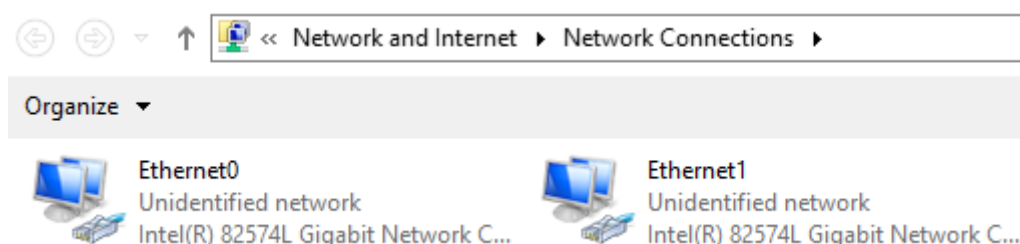
Khi máy chủ khởi động lại sẽ có một số xác nhận và thực hiện theo mặc định.

Đăng nhập vào máy và chạy ứng dụng Server Manager. Truy cập vào chức năng quản lý Local Server, giao diện bên phải thấy Computer Name, kích vào tên máy và thực hiện thay đổi lại tên theo chức năng của máy.



Chọn OK để kết thúc, khởi động lại máy.

Tiếp tục cấu hình địa chỉ IP cho 2 giao diện mạng:



Với Ethernet0 thuộc Vmnet2 nằm trong dải mạng LAN, Ethernet1 thuộc Vmnet3 là IP Public kết nối Internet.

Ethernet0 địa chỉ IP:

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:	172 . 16 . 1 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

Ethernet1 địa chỉ IP:

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:	192 . 168 . 1 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

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
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 = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

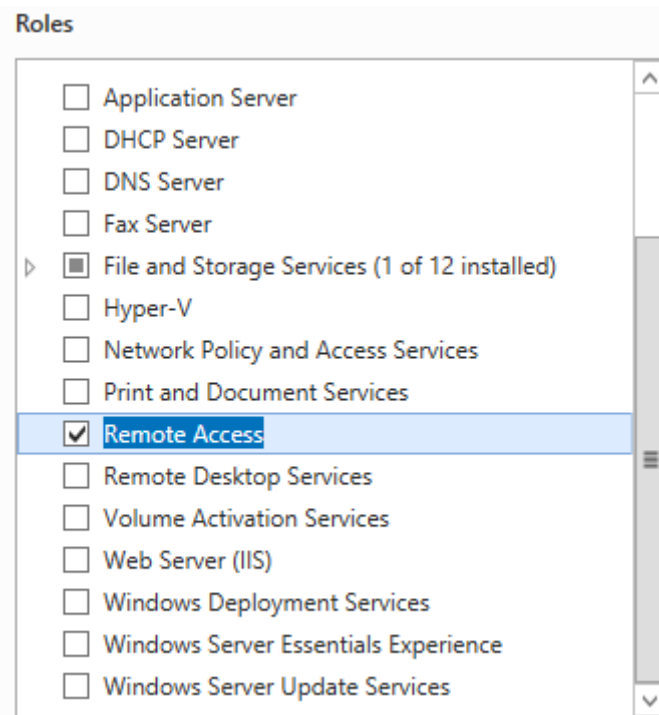
C:\Users\Administrator>ping 192.168.1.20

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

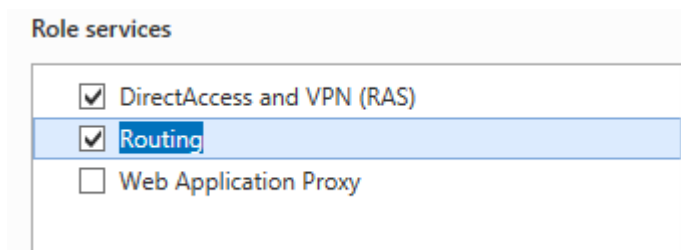
Bước 3: Cài đặt dịch vụ Remote Access

Bật ứng dụng Server Manager → Dashboard → (2) Add roles and features

Giao diện cài đặt dịch vụ xuất hiện, nhấn Next đến giao diện lựa chọn dịch vụ:



Tích vào dịch vụ Remote Access để cài đặt. Nhấn Next để tiếp tục.



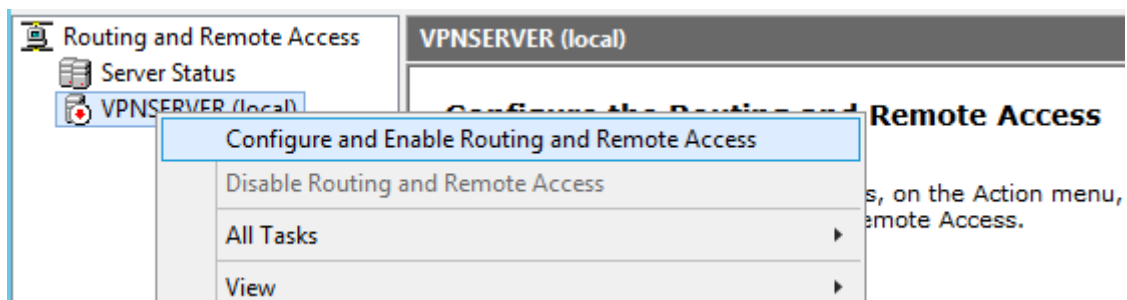
Lựa chọn 2 dịch vụ sử dụng là VPN và Routing.

Các giao diện tiếp theo để mặc định và chọn Install để cài đặt. Thời gian cài đặt dịch vụ này khá lâu (khoảng 15 phút với cấu hình máy như trên).

Bước 4: Cấu hình dịch vụ Routing and Remote Access

Sau khi cài đặt xong dịch vụ Remote Access, trong giao diện Server Manager, các chức năng trên góc phải chọn Tools → Routing and Remote Access

Giao diện cấu hình xuất hiện.



Chuột phải vào tên máy chủ VPN và chọn Configure and Enable...

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.

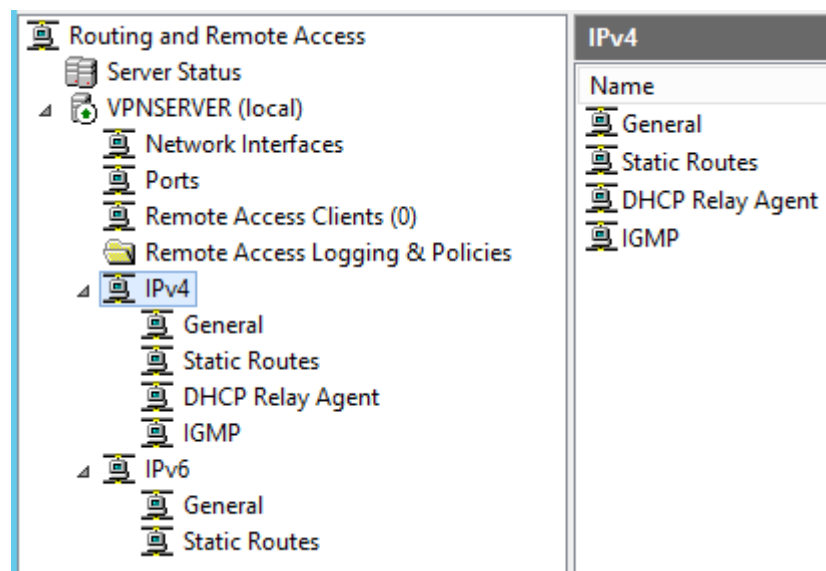
Giao diện cấu hình chọn Custom. Next để tiếp tục

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

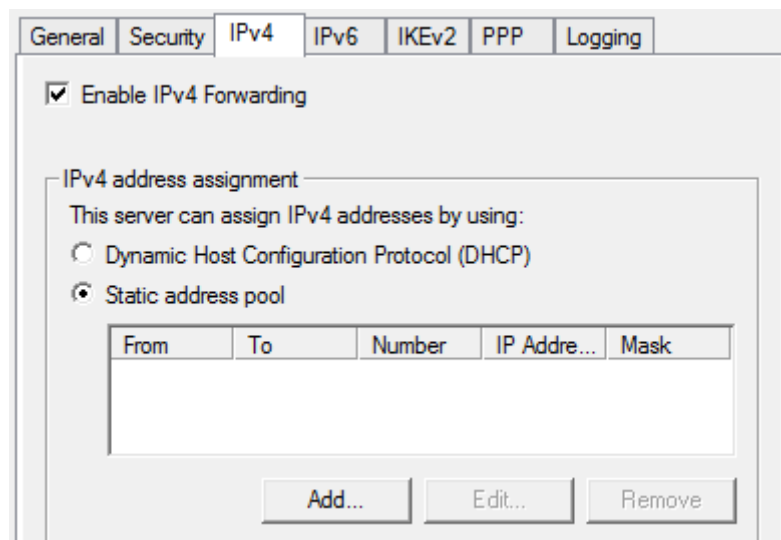
- ☒ VPN access
- ☐ Dial-up access
- ☐ Demand-dial connections (used for branch office routing)
- ☐ NAT
- ☒ LAN routing

Tích chọn 2 chức năng VPN và LAN routing. Next để tiếp tục và kết thúc, Start dịch vụ.

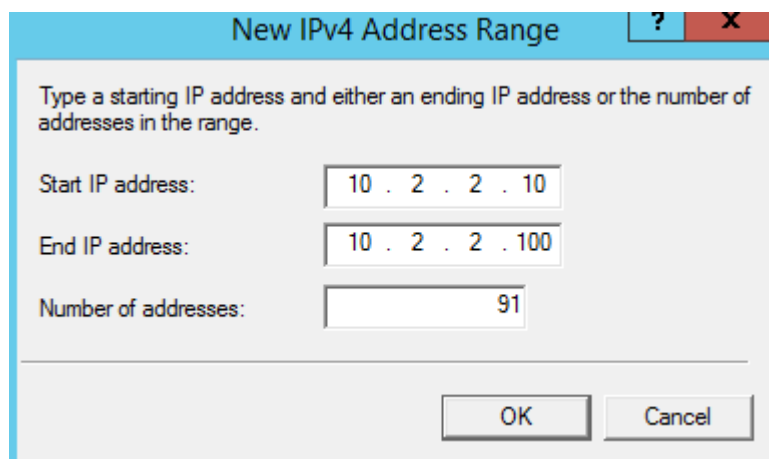
Sau khi cấu hình giao diện như sau:



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.



Tại đây nhập dải địa chỉ IP sử dụng.

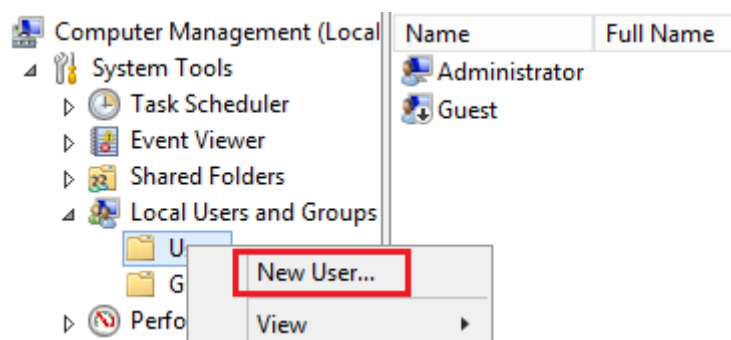


Nhấn OK để kết thúc.

Bước 5: 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.



Đặt tên tài khoản và mật khẩu:

The 'New User' dialog box is shown with the following fields and options:

- User name: vpnuser
- Full name: (empty)
- Description: (empty)
- Password: (masked with dots)
- Confirm password: (masked with dots)
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled
- Buttons: Help, Create, Close

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

The 'Properties' dialog box for a user is shown with the 'Dial-in' tab selected. The 'Network Access Permission' section has the following options:

- ☒ Allow access
- ☐ Deny access
- ☐ Control access through NPS Network Policy

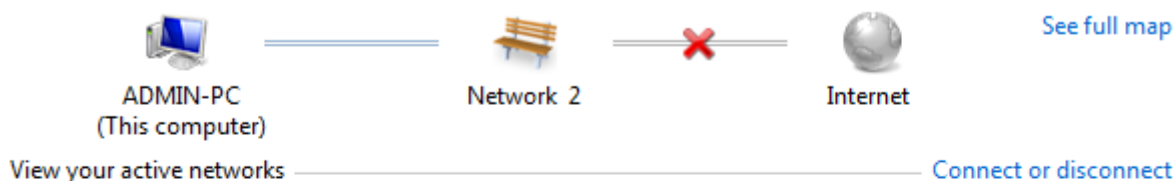
Nhấn Apply và kết thúc.

1.4.3. Thực hiện trên máy Win 7

Bước 1: Tạo kết nối VPN

Bật của sổ quản trị Network.

View your basic network information and set up connections



Access type: No Internet access
Connections: Local Area Connection

Change your networking settings



Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.



Connect to a network

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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).

Type the Internet address to connect to

VPN.

Your network administrator can give you this address.

Internet address:

192.168.1.1

Destination name:

VPN Connection

Nhấn Next để tiếp tục.

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

Type your user name and password

User name:

Password:

☐ Show characters

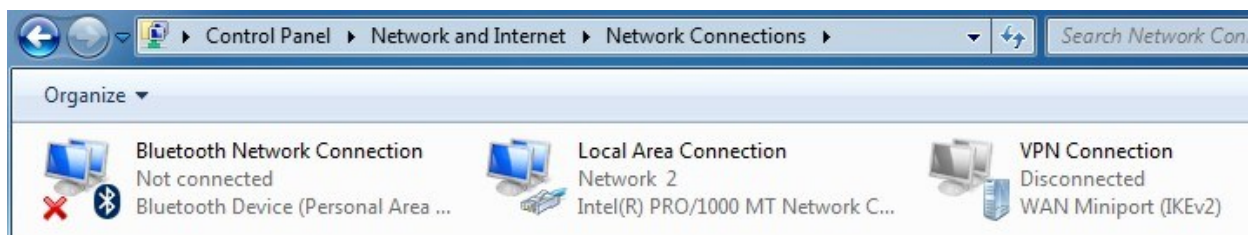
☐ Remember this password

Domain (optional):

Nếu máy chủ VPN gia nhập vào miền trong Domain Controller thì trong mục Domain nhập thêm tên miền. Nhấn Create để tạo kết nối.

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.

Bước 2: Kiểm tra kết nối

- Ping tới máy chủ DataCenter:

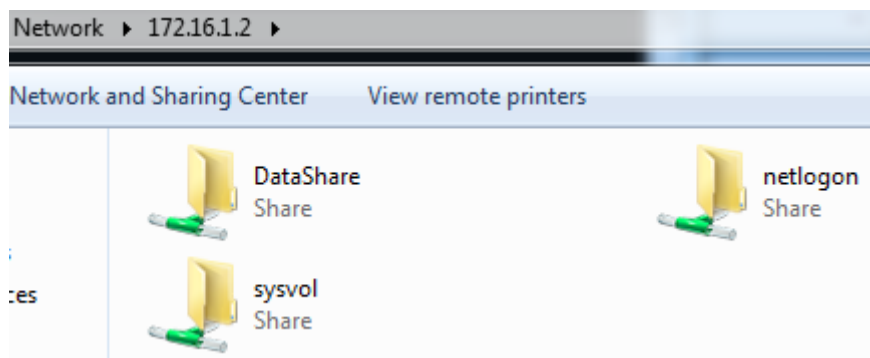
```
C:\Users\admin>ping 172.16.1.2

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

Kết quả thành công.

- Truy cập tới tài nguyên chia sẻ.

Vào RUN gõ [\\172.16.1.2](#)



Kết quả thành công.

- Tiếp tục chặn bắt dữ liệu trên đường truyền để kiểm tra dữ liệu đã được mã hóa hay chưa:

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fe80::f9bb:1841:36ff02::1:2		DHCPv6	150	Solicit XID: 0xc44295 C
2	8.45306000	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
3	8.45387300	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
4	8.54803300	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP
5	9.46926300	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
6	9.47014700	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
7	9.57792800	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP
8	10.4834860	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
9	10.4844640	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
10	10.5921200	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP
11	11.4817260	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
12	11.4827690	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
13	11.5902690	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP

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.

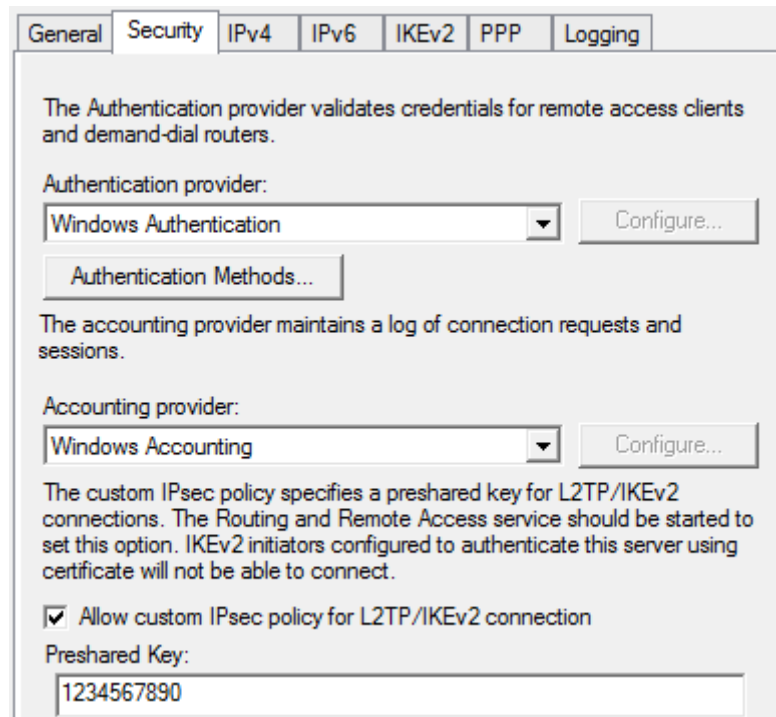
1.5. Cấu hình VPN với giao thức L2TP kết hợp với IPSec

1.5.1. 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:



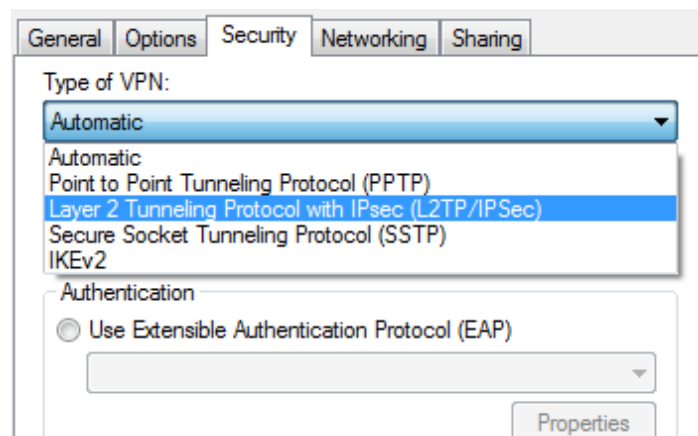
Tích chọn vào ô Allow custom IPsec... Nhập khóa chia sẻ giữa 2 máy là VPN Server và Win7. Khóa này giữ bí mật.

Nhấn Apply → OK. Restart lại dịch vụ VPN.

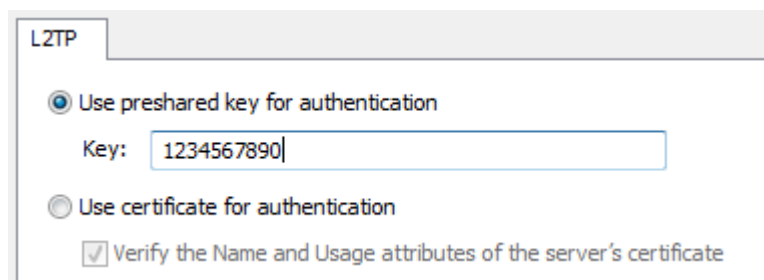
1.5.2. Thực hiện trên máy Win7

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.



L2TP

☒ Use preshared key for authentication

Key: 1234567890

☐ Use certificate for authentication

☒ Verify the Name and Usage attributes of the server's certificate

Nhấn OK để kết thúc.

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



User name: vpnuser

Password:

Domain:

☒ Save this user name and password for the following users:

☐ Me only

☒ Anyone who uses this computer

Connect Cancel Properties Help

Nhấn Connect để kết nối.

Kiểm tra kết quả:

- Thực hiện Ping từ máy Win 7 vào máy DataCenter:

```
C:\Users\admin>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=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
Reply from 172.16.1.2: bytes=32 time=1ms TTL=127
```

Thành công.

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

No.	Time	Source	Destination	Protocol
1	0.00000000	vmware_b8:c3:80	vmware_27:72:af	ARP
2	0.00051400	vmware_27:72:af	vmware_b8:c3:80	ARP
3	0.28401500	192.168.1.20	192.168.1.1	ESP
4	0.28499800	192.168.1.1	192.168.1.20	ESP
5	1.29857400	192.168.1.20	192.168.1.1	ESP
6	1.29969800	192.168.1.1	192.168.1.20	ESP
7	2.29656500	192.168.1.20	192.168.1.1	ESP
8	2.29750300	192.168.1.1	192.168.1.20	ESP
9	3.31023600	192.168.1.20	192.168.1.1	ESP
10	3.31109600	192.168.1.1	192.168.1.20	ESP
11	4.32440300	192.168.1.20	192.168.1.1	ESP
12	4.32534400	192.168.1.1	192.168.1.20	ESP
13	5.33850300	192.168.1.20	192.168.1.1	ESP

Lúc này lưu lượng dữ liệu kết nối đã được mã hóa bằng giao thức ESP của Ipsec.

Kết thúc bài thực hành.