

GENERAL INFORMATION ABOUT THE PRACTICE

Practice name: Configuration of vpn client to site on windows server 2012 r2 platform

Number of students working together: 02

Score: 05 point

Practice location: Computer room

Request:

- Hardware requirements: Each student is provided with 01 computer with minimum configuration: CPU 2.0 GHz, RAM 8GB, HDD 50GB
- Software requirements on the machine:
 - + Operating system Windows Server 2012 R2, Windows 7
 - + VMware Workstation 9.0 or higher
- Practice tools: VMware virtual machine:
 - + Windows Server 2012 R2, 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

Virtual Private Network (VPN) technology is a technology that creates a private network on a public network platform such as the Internet. This private network is guaranteed to be secure such as encryption, authentication and integrity.

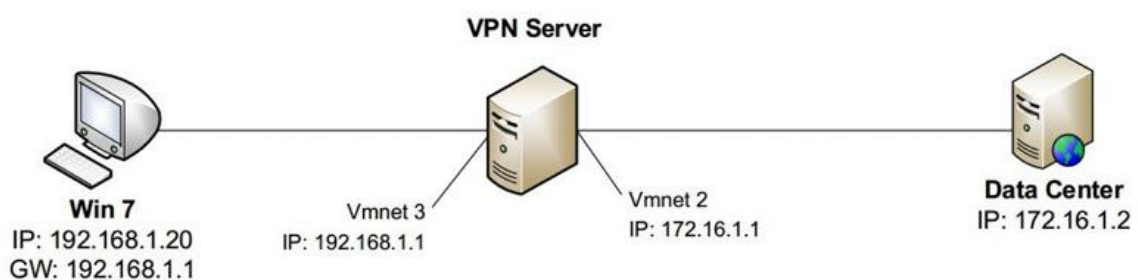
When deploying a VPN network according to the Client to Side model to serve users to remotely access the internal network of a company or organization. In this model, the following encryption and authentication methods are used:

- Encrypted by PPTP protocol
- Encryption by L2TP/IPSec protocol
- Encrypted by SSTP protocol
- Authentication by RADIUS protocol

1.2. Preparation

- 02 virtual machines running Windows Server 2012 operating system.
- 01 virtual machine running Windows 7 operating system.

1.3. Deployment model



The VPN Server virtual machine must have 02 network interfaces, each interface connects to the Data Center and Win 7

1.4. Description of work to be performed

Perform on Data Center machine:

- Create data sharing folder: DataShare
- Perform on VPN Server

- Add new network interface Vmnet 3.
- Change the current SID and hostname.
- Install Remote Access service
- Configure Routing and Remote Access service
- Create Real VPN user

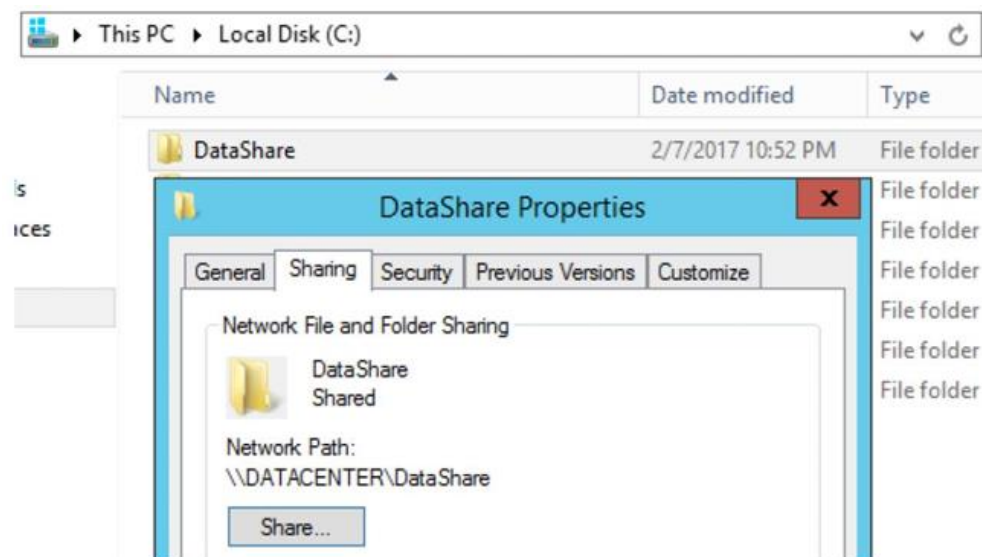
Shown on Win 7 machine:

- Create VPN connection
- Check VPN connection

1.5. Implementation steps

1.5.1. Perform on Data Center server:

Create folders and share folders:



IP address configuration:

☐ Obtain an IP address automatically
☒ Use the following IP address:

IP address:
 Subnet mask:
 Default gateway:

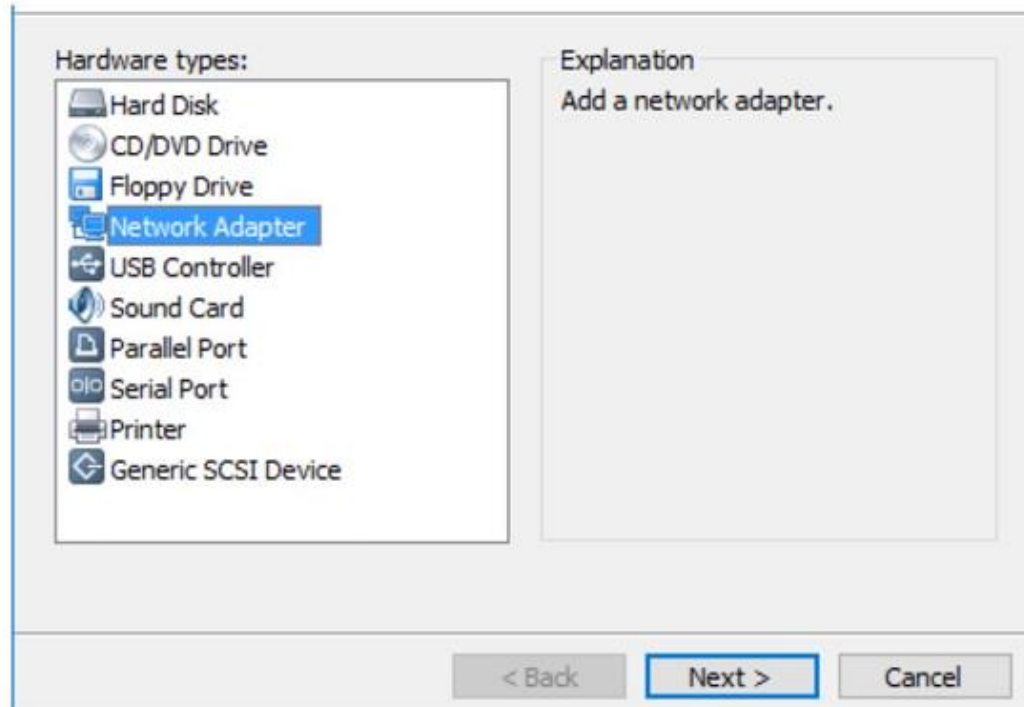
☐ Obtain DNS server address automatically
☒ Use the following DNS server addresses:

Preferred DNS server:
 Alternate DNS server:

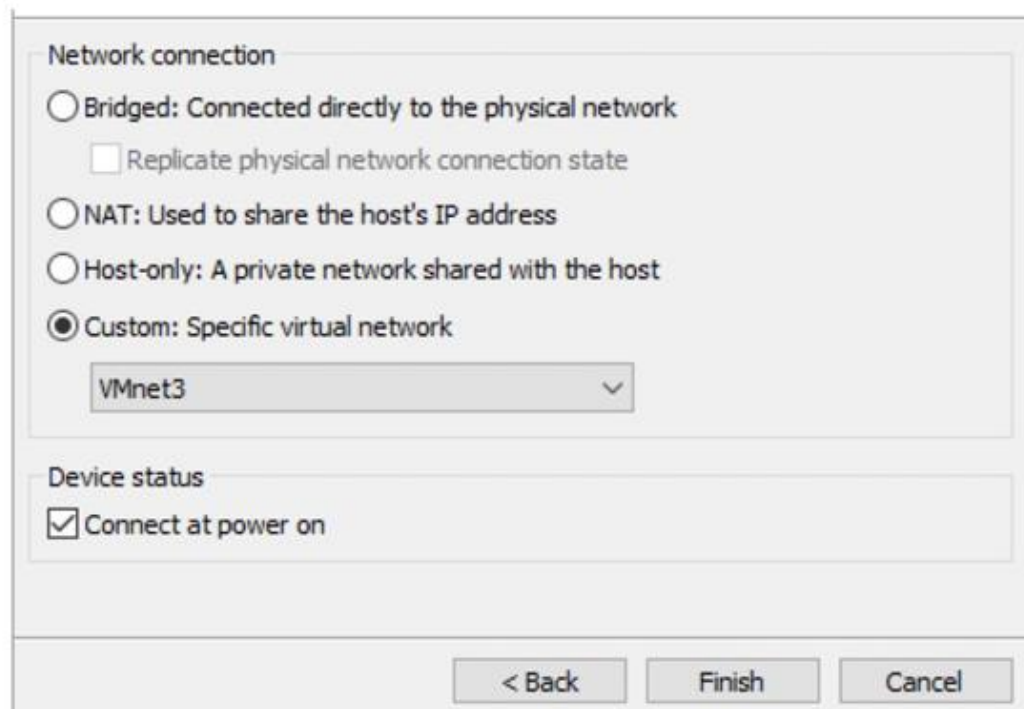
1.5.2. Implementation on VPN Server

Step 1: Add network interface and configure IP address In the Vmware administration interface when the virtual machine is not running, select Edit virtual machine settings

A window appears, select Add. A new window appears, select Network Adapter.

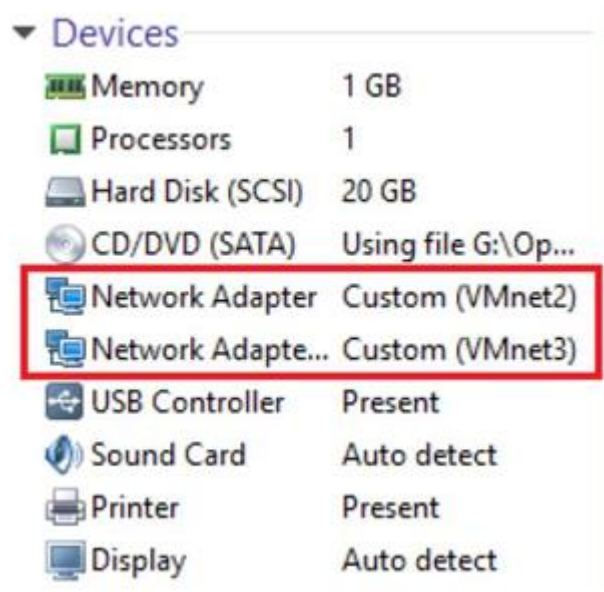


Select Next to continue.



Select Vmnet3 and Finish to finish.

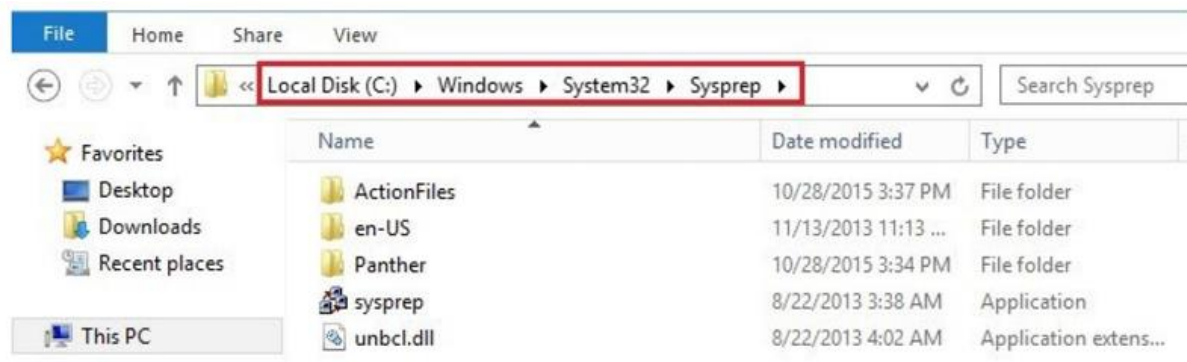
The result when selecting Vmnet for 2 network interfaces is as follows



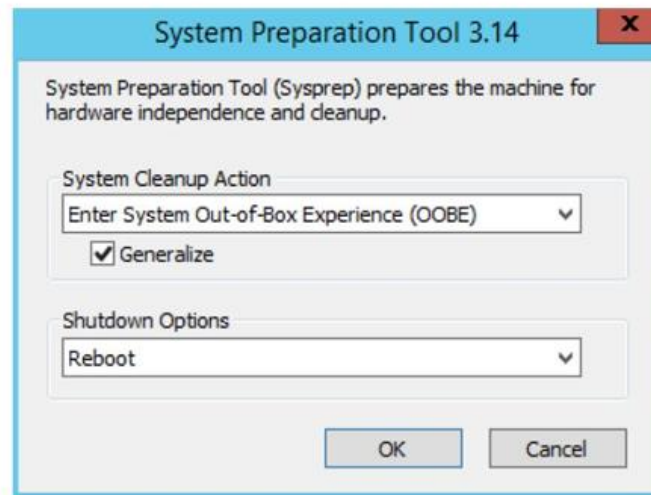
Step 2: Change the current SID and hostname

When using the same virtual machine to decompress into many other virtual machines, the SID value and virtual machine name are duplicated. Therefore, it is necessary to change this value so that the servers can authenticate with each other during the connection process, especially in VPN.

Access the folder with the following path:



Right click on the sysprep file and select Run as administrator.

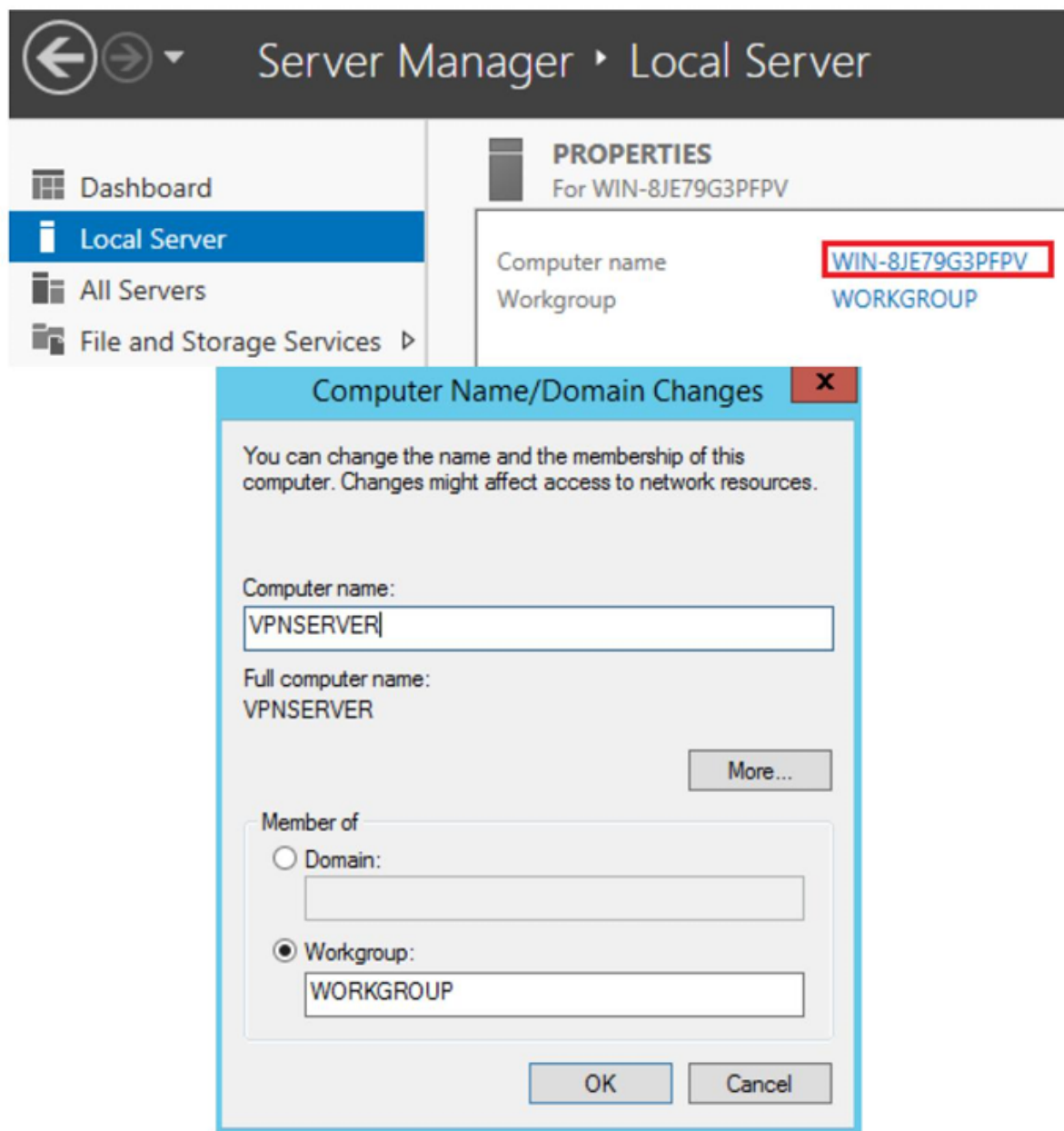


Check the **Generalize** box. And select OK

The system will automatically change the default hostname and SID value.

When the server restarts there will be some confirmation and execution by default

Log in to the computer and run the Server Manager application. Access the Local Server management function, the right interface shows Computer Name, click on the computer name and change the name according to the computer's function



Select OK to finish, restart the computer.

Continue configuring IP addresses for the 2 network interfaces:



With Ethernet0 belonging to Vmnet2 on the LAN network strip, Ethernet1 belongs to Vmnet3 is the Public IP connecting to the Internet.

Ethernet0 IP address:

☐ 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 IP address:

☐ Obtain an IP address automatically

☒ Use the following IP address:

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

Finally, Ping to the DataCenter and Win7 machines to test connectivity:

```
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

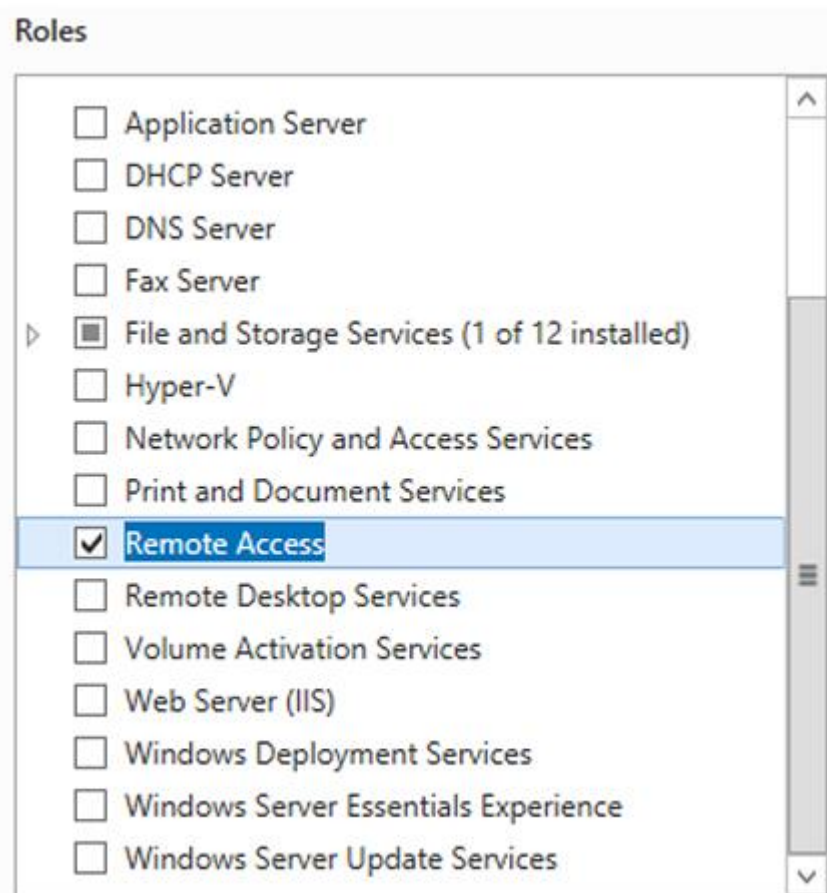
C:\Users\Administrator>ping 192.168.1.20

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
```

Step 3: Install Remote Access service

Turn on the Server Manager → Dashboard → (2) Add roles and features

The service installation interface appears, click Next to go to the service selection interface:



Check the Remote Access service to install. Click Next to continue



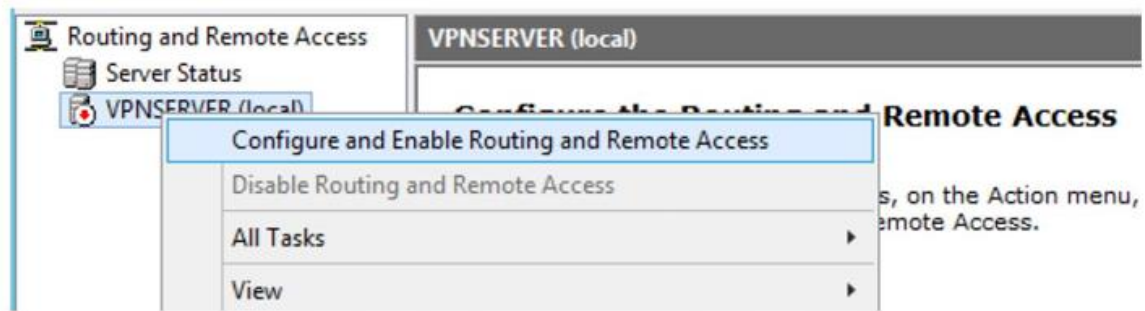
Choose 2 services to use: VPN and Routing.

Leave the next interface as default and select Install to install. Installation time This service takes quite a while (about 15 minutes with the above computer configuration).

Step 4: Configure Routing and Remote Access service

After installing the Remote Access service, in the Server Manager interface, in the upper right corner, select Tools → Routing and Remote Access.

The configuration interface appears:



Right click on the VPN server name and select 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.

Configuration interface select Custom. Next to continue

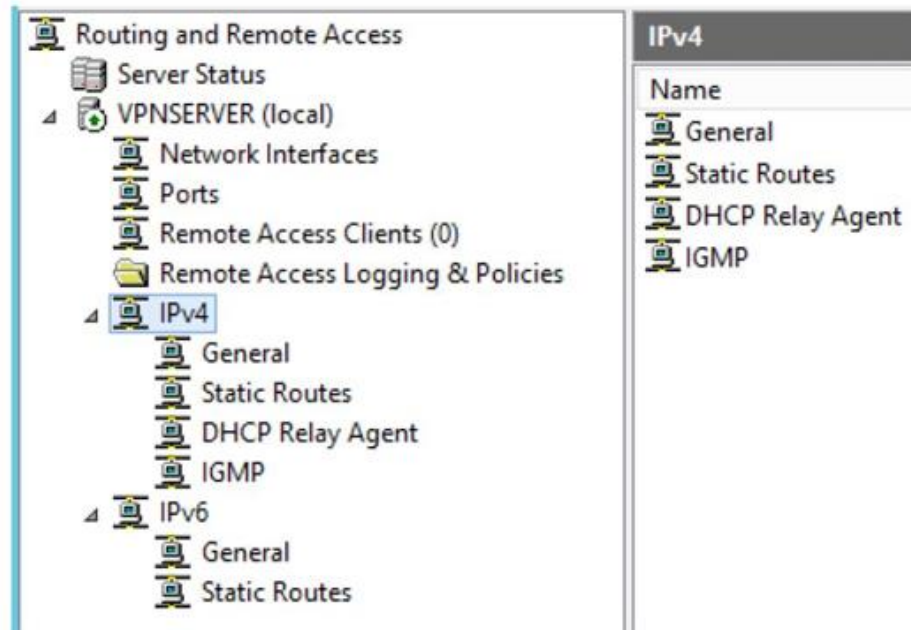
Select the services that you want to enable on this server.

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

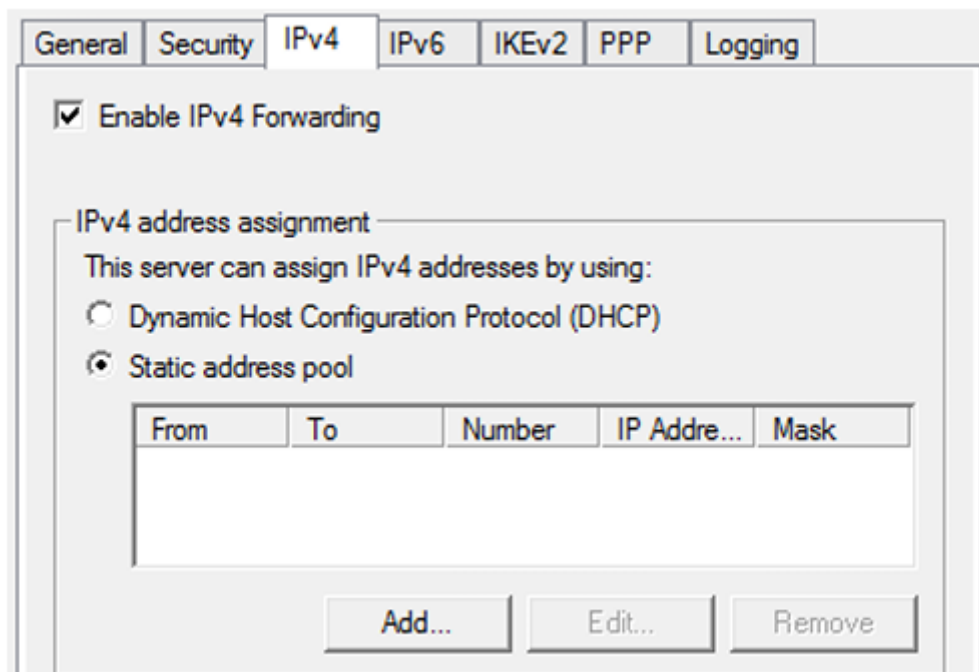
Select 2 functions VPN and LAN routing. Next to continue and finish, Start service.

After configuring the interface as follows:

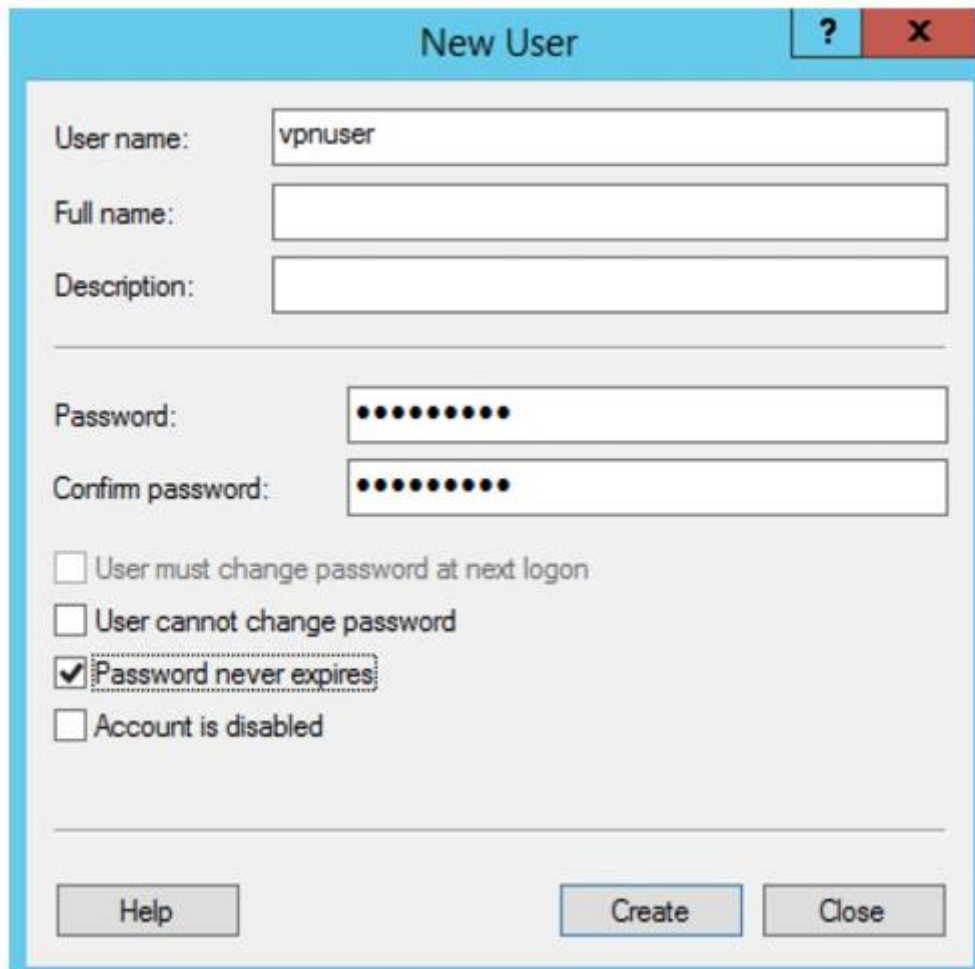
After configuring the interface as follows:



Next you need to configure the IP address to use for the tunnel. Right click Go to VPN SERVER and select Properties → IPv4 → static address pool → Add.



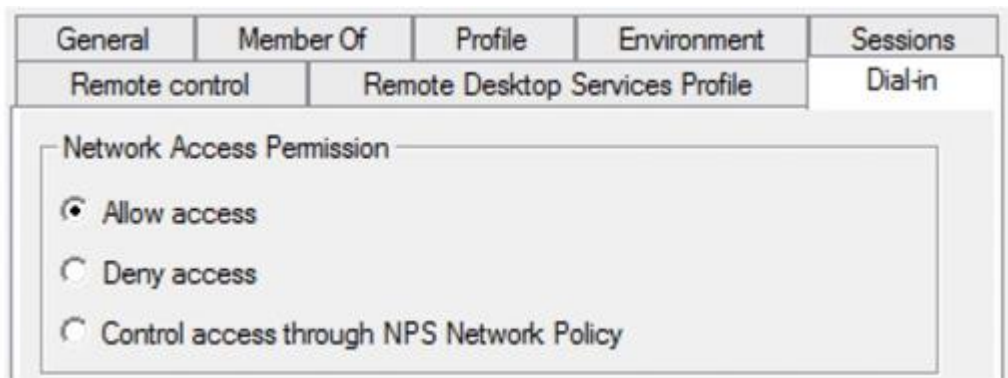
Here enter the IP address range to use



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

- User name:** vpnuser
- Full name:** (empty field)
- Description:** (empty field)
- Password:** (masked with 10 dots)
- Confirm password:** (masked with 10 dots)
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled
- Buttons:** Help, Create, Close

Select Create to create a user. Once the account is created, right-click Go to the account name and select Properties. In the dial-in tab, select Allow access



The 'Remote Desktop Services Profile' dialog box is shown with the following tabs and options:

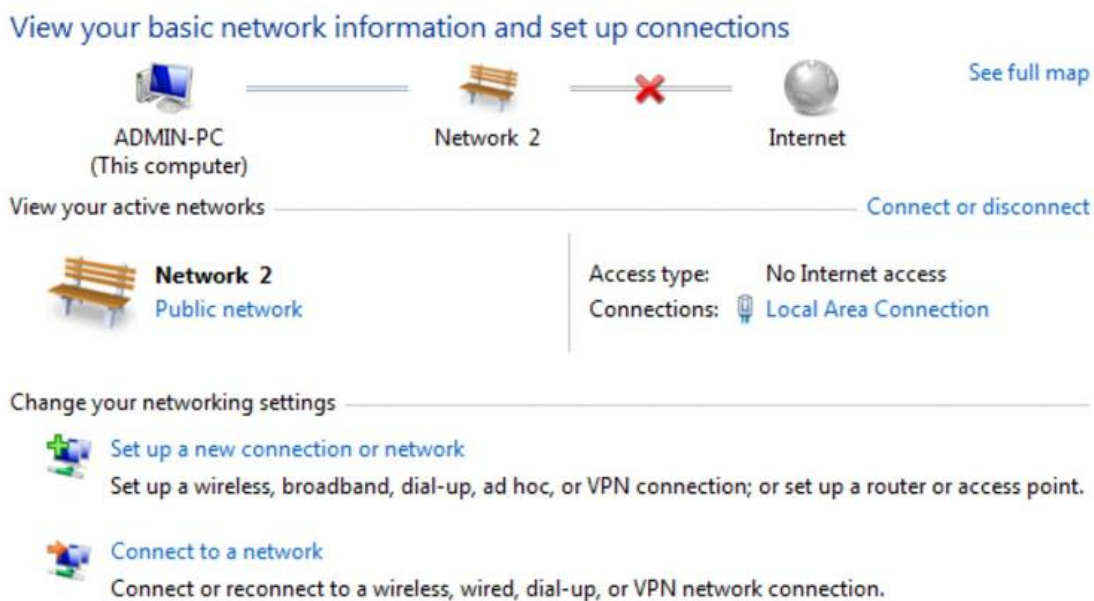
- Tabs:** General, Member Of, Profile, Environment, Sessions
- Sub-tabs:** Remote control, Remote Desktop Services Profile, Dial-in
- Network Access Permission:**
 - ☒ Allow access
 - ☐ Deny access
 - ☐ Control access through NPS Network Policy

Click Apply and finish

1.5.3. Perform on Win 7 machine

Step 1: Create VPN connection

Turn on Network administration window.



Click Setup a new connection.

Next window select Connect to a workplace → Next

Next interface select Use my Internet Connection

Next interface select I'll set up an Internet connection later.

The next interface enters the external IP address of the VPN server (via This is usually the Public IP address)

Type the Internet address to connect to

VPN. Your network administrator can give you this address.

Internet address:

Destination name:

Click Next to continue.

The next interface enters the account name and password created on the server.

Type your user name and password

User name:	<input type="text" value="vpnuser"/>
Password:	<input type="password" value="••••••••"/>
	<input type="checkbox"/> Show characters
	<input type="checkbox"/> Remember this password
Domain (optional):	<input type="text"/>

If the VPN server joins a domain in the Domain Controller, enter the domain name in the Domain field. Click Create to create the connection.

Next, connect to the internal network using VPN.

Access the Network administration interface



We see the VPN connection icon.

Double click on the VPN connection icon. The login interface appears, enter Password for account vpn → Connect.



Connection successful. The remote user can now access resources on the DataCenter organization's internal server.

Step 2: Check connection

- Ping to DataCenter server

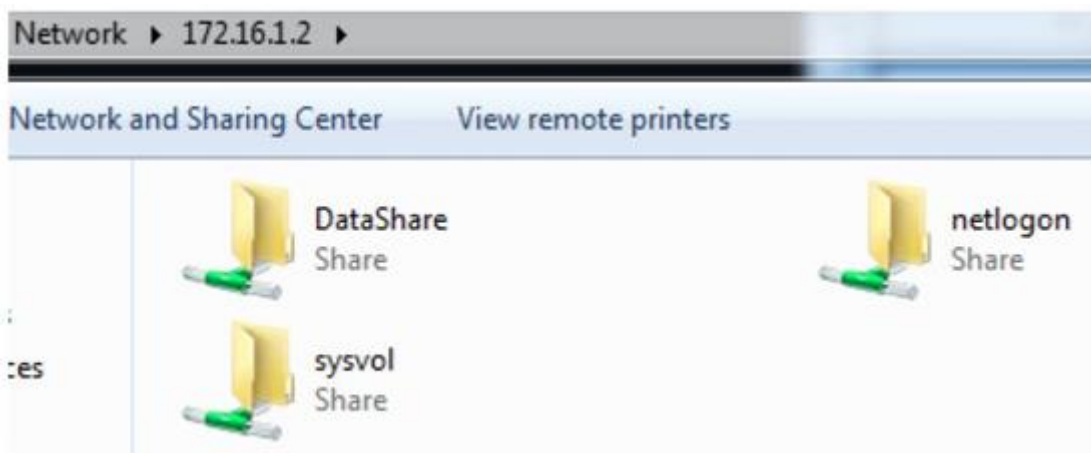
```
C:\Users\admin>ping 172.16.1.2

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
```

Successful results.

- Access to shared resources.

In RUN type [\\172.16.1.2](#)



Successful results.

- Continue to intercept data on the transmission line to check the data encrypted or not:

Install WireShark tool on VPN Server, and listen on external network interface (Ethernet1)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fe80::f9bb:1841:36f:ff02::1:2		DHCPv6	150	Solicit XID: 0xc44295 CI
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

The packets on the line are encapsulated and encrypted with GRE and PPP. Due to the default configuration, the VPN is using the PPTP protocol to create the tunnel

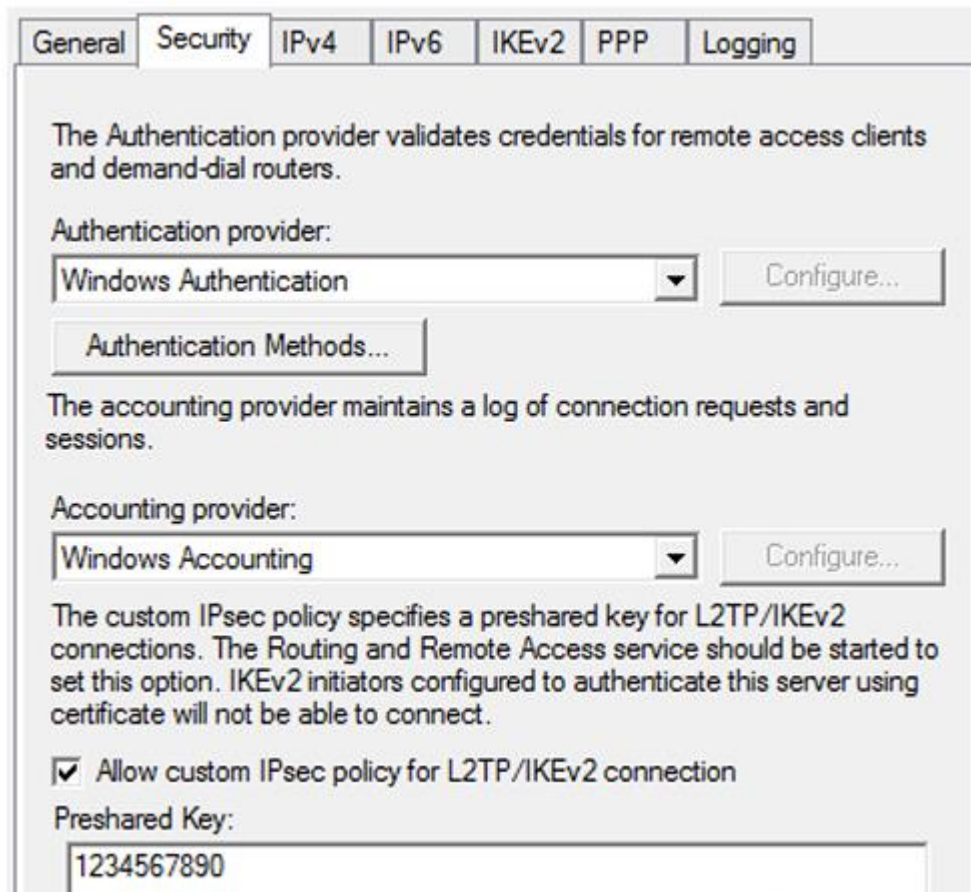
1.6. Configure VPN with L2TP protocol combined with IPSec

1.6.1. Perform on VPN Server

At the VPN Routing and Remote access administration interface.

Right click on the VPN Server → Properties.

Select the Security tab



The packets on the line are encapsulated and encrypted with GRE and PPP. Due to the default configuration, the VPN is using the PPTP protocol to create the tunnel

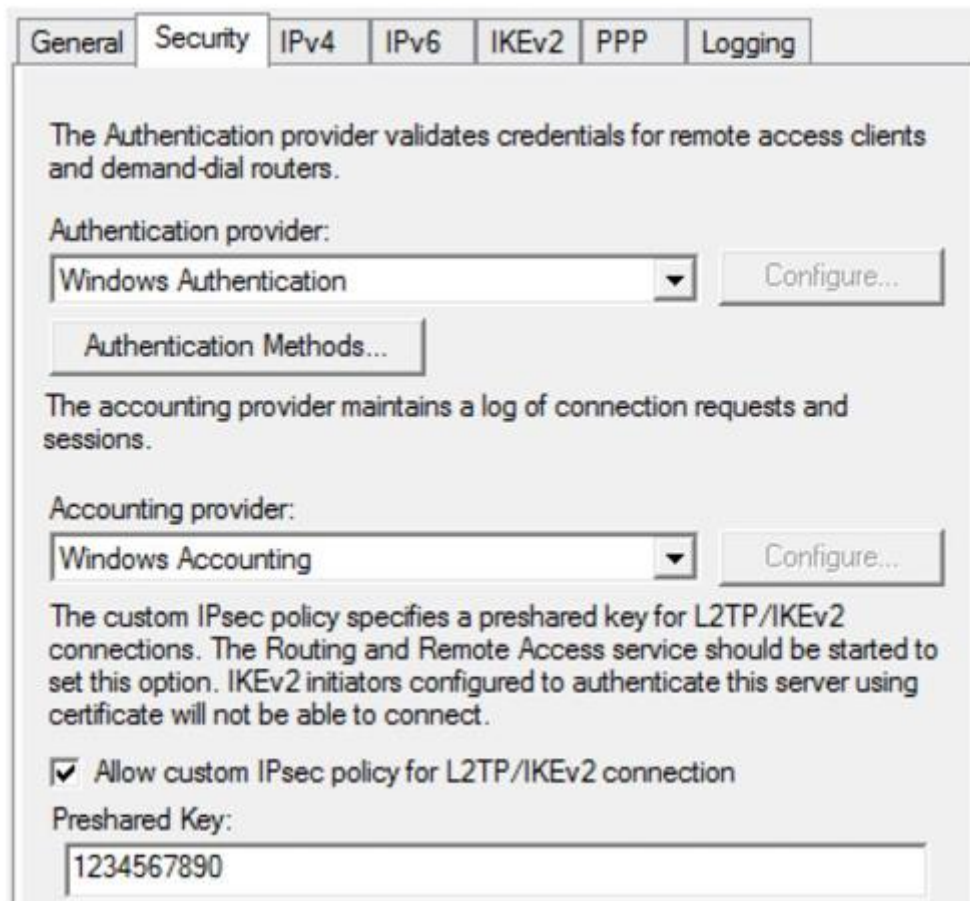
1.7. Configure VPN with L2TP protocol combined with IPsec

1.7.1. Perform on VPN Server

At the VPN Routing and Remote access administration interface.

Right click on the VPN Server → Properties.

Select the Security tab



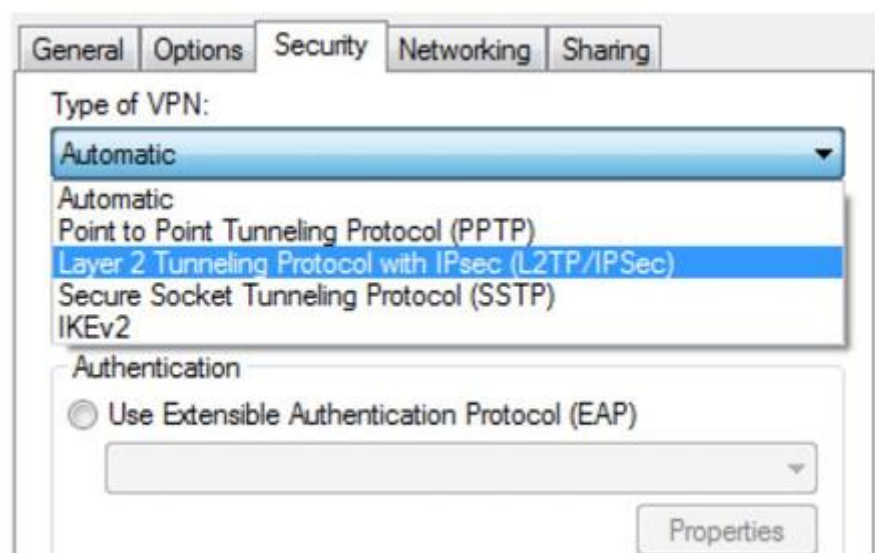
Check the box Allow custom IPsec... Enter the shared key between the two computers, VPN Server and Win7. This key is kept secret.

Click Apply → OK. Restart the VPN service.

1.7.2. Perform on Win7 machine

Enable the VPN connection interface. Select Properties.

Select the Security tab. Under Type of VPN, select L2TP/Ipsec.



In the Advance setting section right below, click and enter the shared key as entered on the VPN Server

The image shows a Windows L2TP configuration window. At the top, there is a tab labeled 'L2TP'. Below the tab, there are two radio button options. The first option, 'Use preshared key for authentication', is selected. Below this option is a text box labeled 'Key:' containing the value '1234567890'. The second option, 'Use certificate for authentication', is not selected. Below the second option is a checked checkbox labeled 'Verify the Name and Usage attributes of the server's certificate'.

Click OK to finish.

At the main connection interface, enter the remote access user account.

The image shows a Windows VPN connection window. At the top, there is a graphic showing a laptop, a globe, and a desktop computer connected by a green line. Below the graphic, there are three text boxes: 'User name:' containing 'vpnuser', 'Password:' containing a series of dots, and 'Domain:' which is empty. Below these text boxes is a checkbox labeled 'Save this user name and password for the following users:'. Below this checkbox are two radio button options: 'Me only' and 'Anyone who uses this computer'. The 'Anyone who uses this computer' option is selected. At the bottom of the window, there are four buttons: 'Connect', 'Cancel', 'Properties', and 'Help'.

Click Connect to connect.

Check the results:

- Perform Ping from Win 7 machine to DataCenter machine:


```
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
```

Success.

- Capture packets on VPN Server (listen at external port):

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

At this point the connection data traffic is encrypted using Ipsec's ESP protocol.

End of practice