

# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

Last updated: 2022-03-17

# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

## Problem statement

In a VVR environment, the replication data that is transferred over a public network, is not secured. Such data needs to be encrypted during an over-the-wire transmission.

## Solution

A virtual private network (VPN) configuration extends a private network across a public network so that the data being transmitted can be remotely accessed through the public network in a secure manner. You can also use a VPN to secure your internet activity by using the VPN server as a proxy server.

You can configure an L2TP/IPsec VPN on a Windows network and use it to access your business network.

This VPN is configured by using the built-in Routing and Remote Access (RRAS) feature of Microsoft Windows Server. Then, a VPN tunnel is created from the VVR primary to the VVR secondary. Finally, the replication data is encrypted by using the IPsec VPN before it is sent over the wire.

## What is IPsec?

IPsec is a set of protocols that are used together to configure encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets along with authenticating the origin of the packets.

## How does IPsec work?

Configuring IPsec connections includes the following steps:

- **Key exchange:** Keys are necessary for encryption; a key is a string of random characters that can be used to lock (or encrypt) and unlock (or decrypt) messages. IPsec sets up keys with a key exchange between the connected devices, so that each device can decrypt the messages from the other device.
- **Addition of packet headers and trailers:** All data that is sent over a network is broken down into smaller pieces called packets. Packets contain both, a payload, or the actual data being sent, and headers, or information about that data, so that computers receiving the packets know what to do with them. IPsec adds several headers to data packets containing authentication and encryption information. It also adds trailers, which are sent after the payload of each packet, instead of before.
- **Authentication:** IPsec provides authentication for each packet, like a stamp of authenticity on a collectible item, which ensures that the packets are from a trusted source and not from an attacker.
- **Encryption:** IPsec encrypts the payloads within each packet and the IP header of each packet unless the transport mode is used instead of the tunnel mode—refer to the details further in this document. This encryption keeps the data sent over IPsec secure and private.

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

- **Transmission:** Encrypted IPsec packets travel across one or more networks to their destination using a transport protocol. At this stage, IPsec traffic differs from regular IP traffic in that it most often uses UDP as its transport protocol, rather than TCP, sets up dedicated connections between devices, and ensures that all the packets have arrived. UDP does not set up these dedicated connections. IPsec uses UDP because it allows IPsec packets to get through firewalls.
- **Decryption:** At the other end of the communication, the packets are decrypted, and applications (for example, browsers) can now use the delivered data.

### Which protocols does IPsec use?

A networking protocol is a specified way of formatting data so that any networked computer can interpret it. The IPsec suite of protocols comprises the following:

- **Authentication Header (AH):** The AH protocol ensures that the data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption and so they do not help conceal the data from attackers.
- **Encapsulating Security Protocol (ESP):** ESP encrypts the IP header and the payload for each packet unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.
- **Security Association (SA):** SA refers to a group of protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

Finally, while the Internet Protocol (IP) is not part of the IPsec suite, IPsec runs directly on top of IP.

### Which port does IPsec use?

IPsec usually uses port 500.

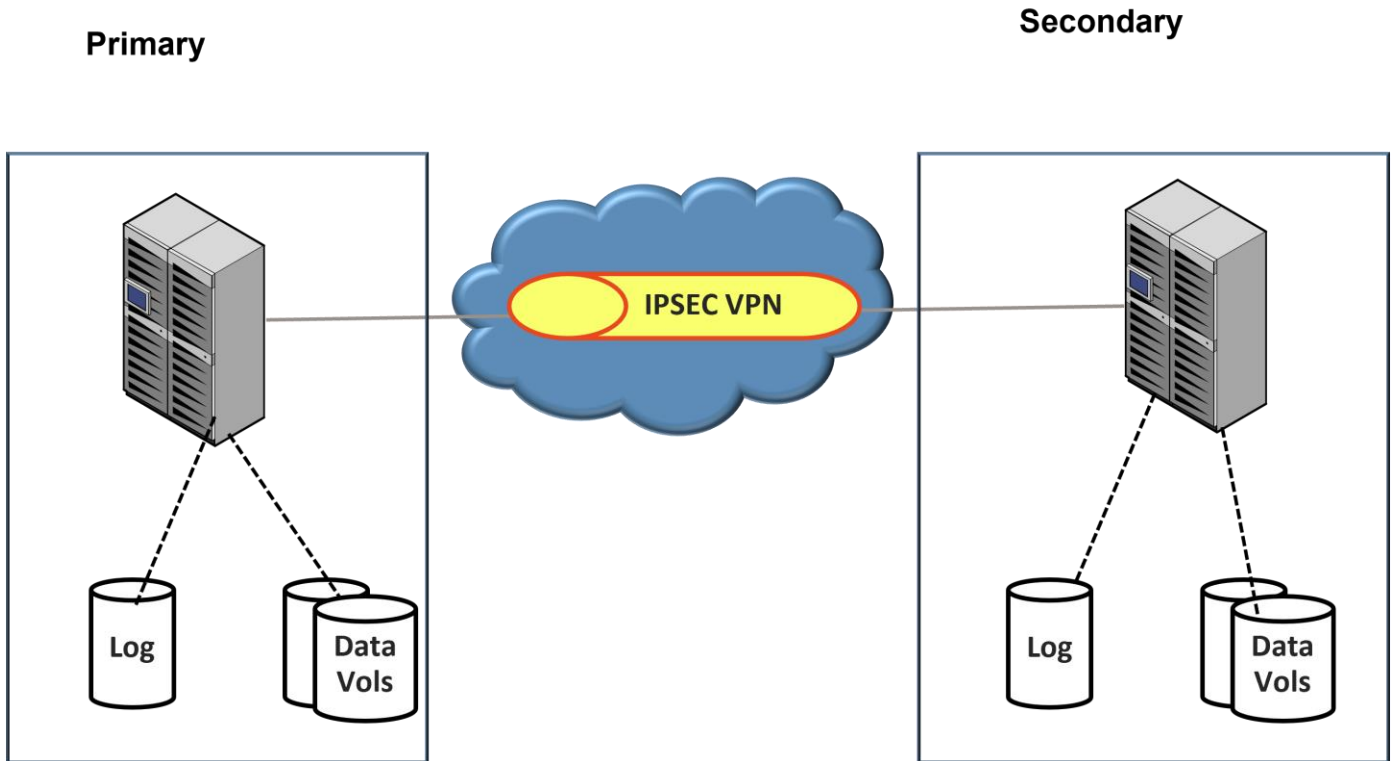
### Operating system supported with InfoScale

Windows Server 2016

# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

## Deployment Diagram

The proposed configuration has been validated on 1 primary and 1 secondary in DR scenario.



## Setting up the IPsec VPN

### Step 1

Log in to both the InfoScale servers—the VVR primary and the VVR secondary—and make sure that they have the latest updates installed.

### Step 2

Install the Remote Access role on both the servers.

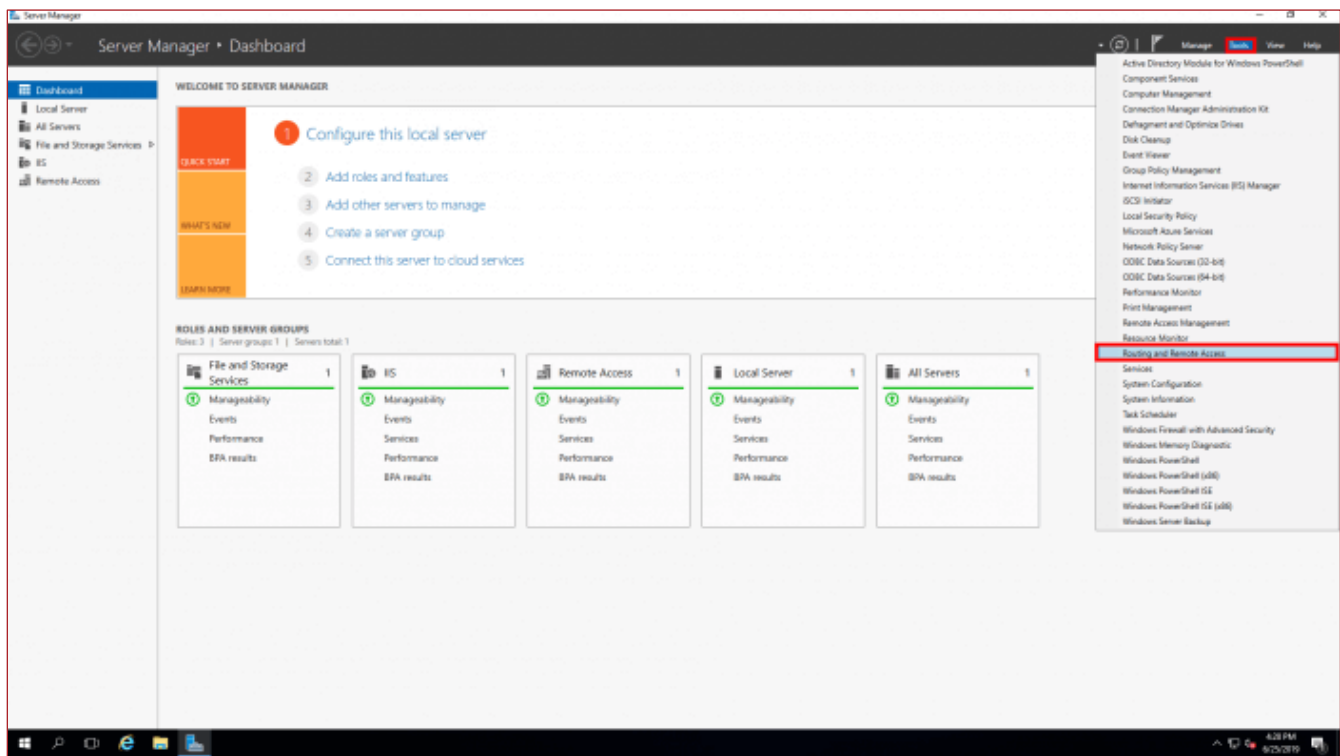
1. Open the Server Manager window.
2. Click **Manage > Add Roles and Features**.

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

3. Select the server from server pool, select **Remote Access** in the **Server Role** section, and click **Next**.
4. On the Remote Access wizard, select **DirectAccess and VPN (RAS)** and **Routing**.
5. On the popup that appears, click **Add Features** and then click **Next**.
6. Make sure that **DirectAccess and VPN (RAS)** and **Routing** are selected in the **Role services** section, and then click **Next**. Accept the defaults on the further pages and click **Next**.
7. On the Confirmation page, select **Restart the destination server automatically if required** checkbox, and then click **Install**.

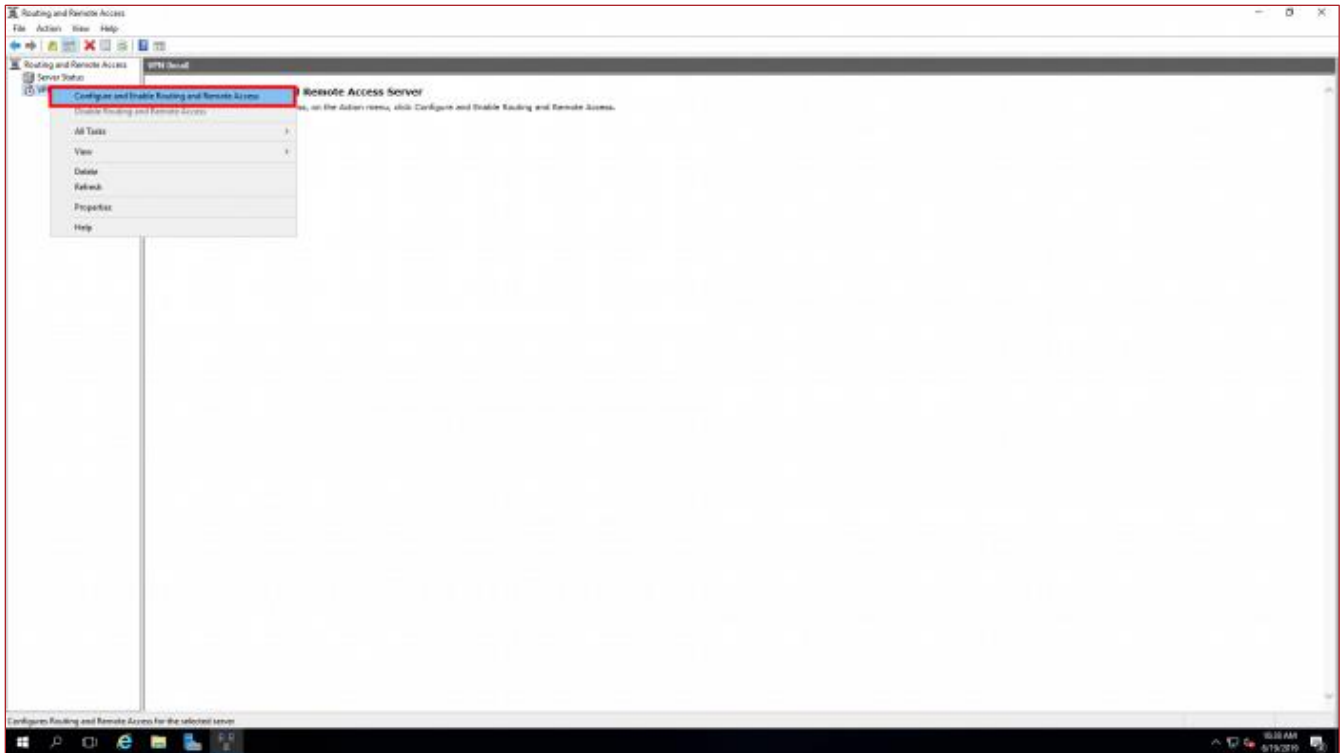
### Step 3

1. Open Server Manager > Tools > Routing and Remote Access.



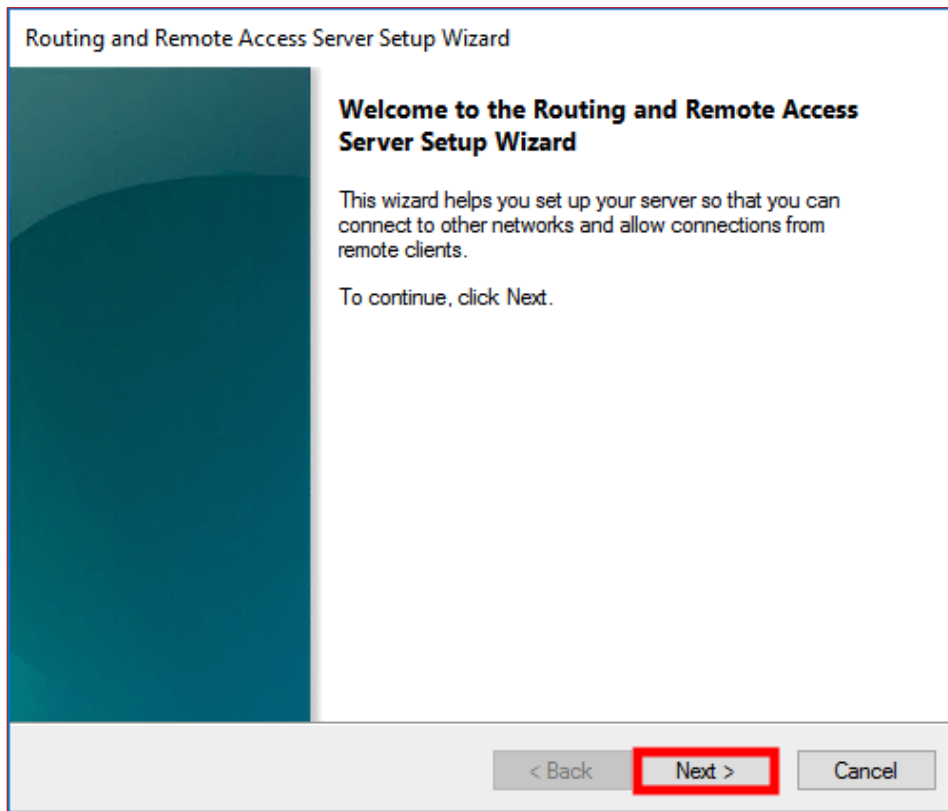
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

2. On the new screen that appears, right-click the server name and click **Configure Routing and Remote Access**.

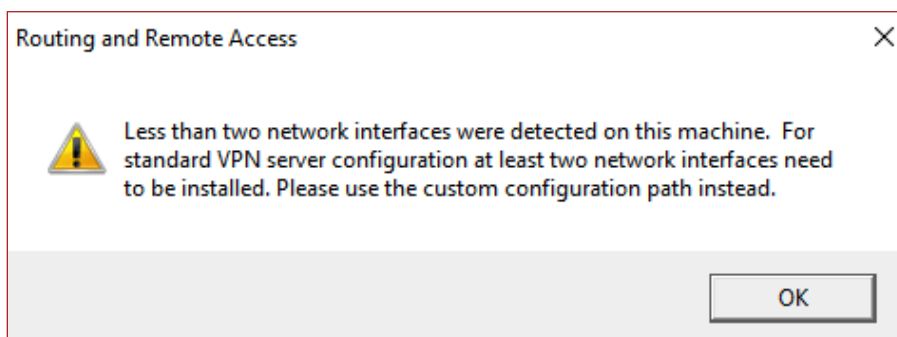


## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

3. On the Routing and Remote Access Server Setup Wizard, click **Next**.



4. Use a custom configuration because the VPN access and NAT require two or more network interfaces.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

5. Select **Custom configuration** and click **Next**.

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

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

6. Select **VPN access** and **NAT** and click on **Next**.

Routing and Remote Access Server Setup Wizard

**Custom Configuration**  
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

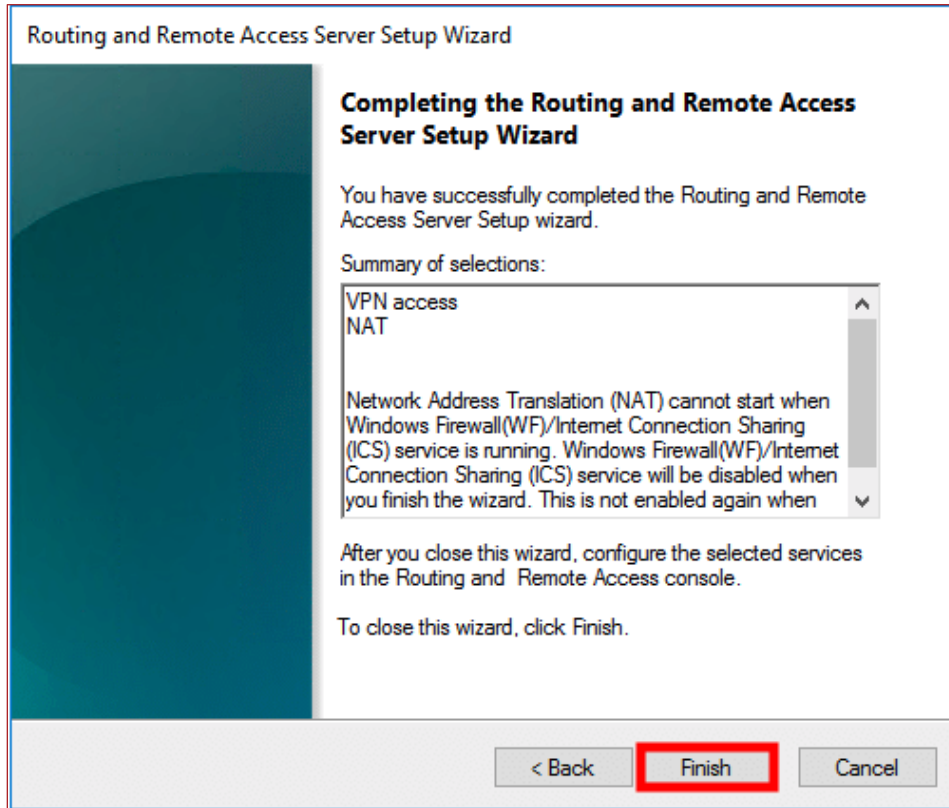
Select the services that you want to enable on this server.

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

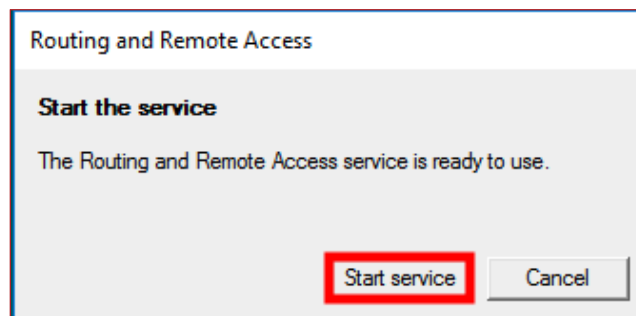
< Back   Next >   Cancel

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

7. Review the summary and click **Finish**.

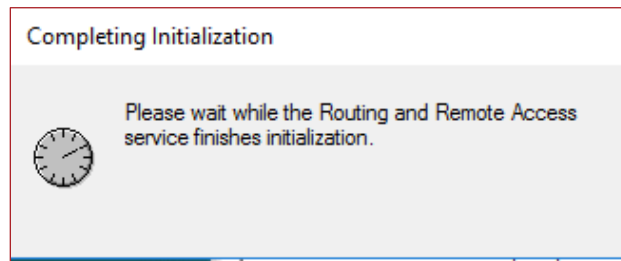


8. On the Routing and Remote Access confirmation box, click **Start service**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

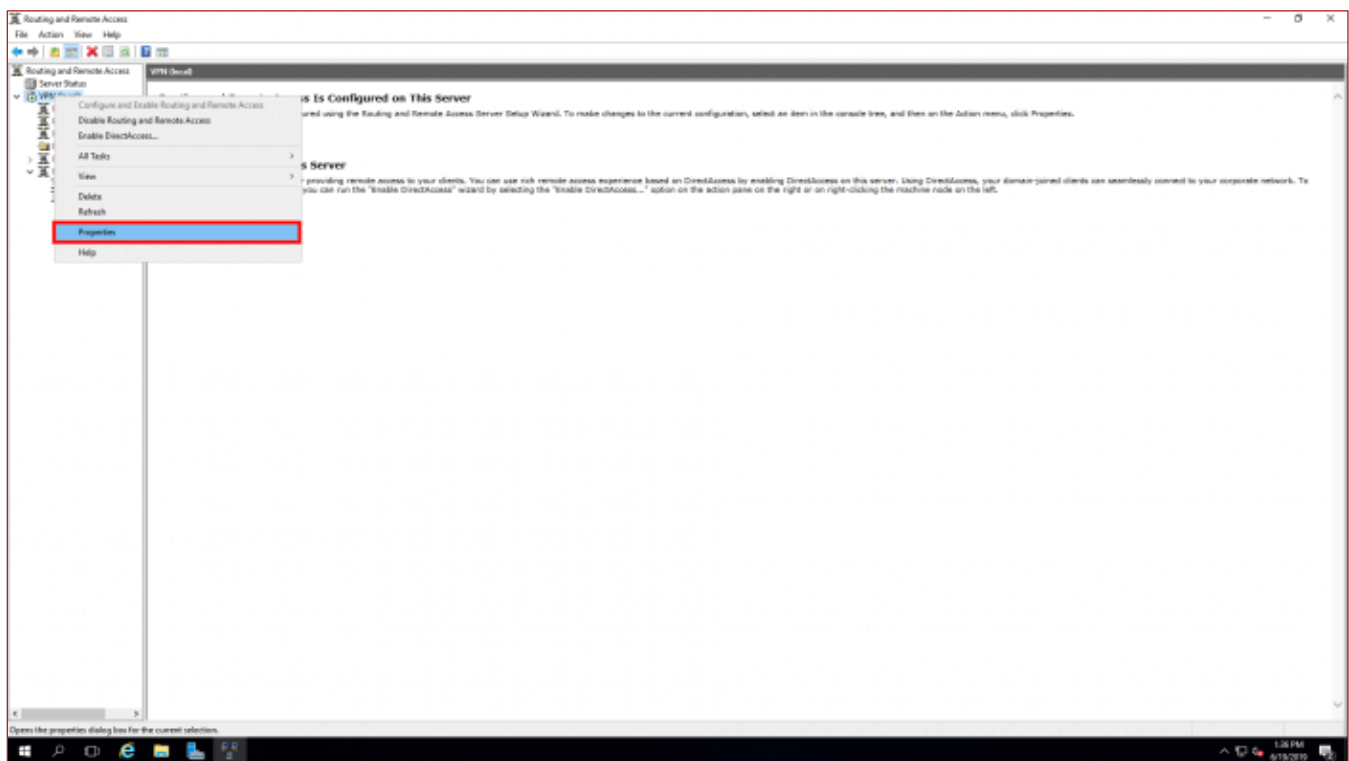
A message box indicates that the initialization is in progress.



### Step 4

Configure Routing and Remote Access.

1. Right-click the server name (VPN) and click **Properties**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

2. Navigate to the Security tab and select **Allow custom IPsec policy for L2TP/Ikev2 connection**. Provide a strong password as the **Preshared Key** value.

The screenshot shows the 'VPN (local) Properties' dialog box with the 'Security' tab selected. The 'Authentication provider' is set to 'Windows Authentication' and the 'Accounting provider' is set to 'Windows Accounting'. The 'Allow custom IPsec policy for L2TP/Ikev2 connection' checkbox is checked and highlighted with a red box. Below it, the 'Preshared Key' field is empty. The 'SSL Certificate Binding' section is also visible, with 'Use HTTP' unchecked and the 'Certificate' set to 'Default'.

VPN (local) Properties

General Security IPv4 IPv6 IKEv2 PPP Logging

The Authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider:  
Windows Authentication Configure...

Authentication Methods...

The accounting provider maintains a log of connection requests and sessions.

Accounting provider:  
Windows Accounting Configure...

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to 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:  
[Empty text box]

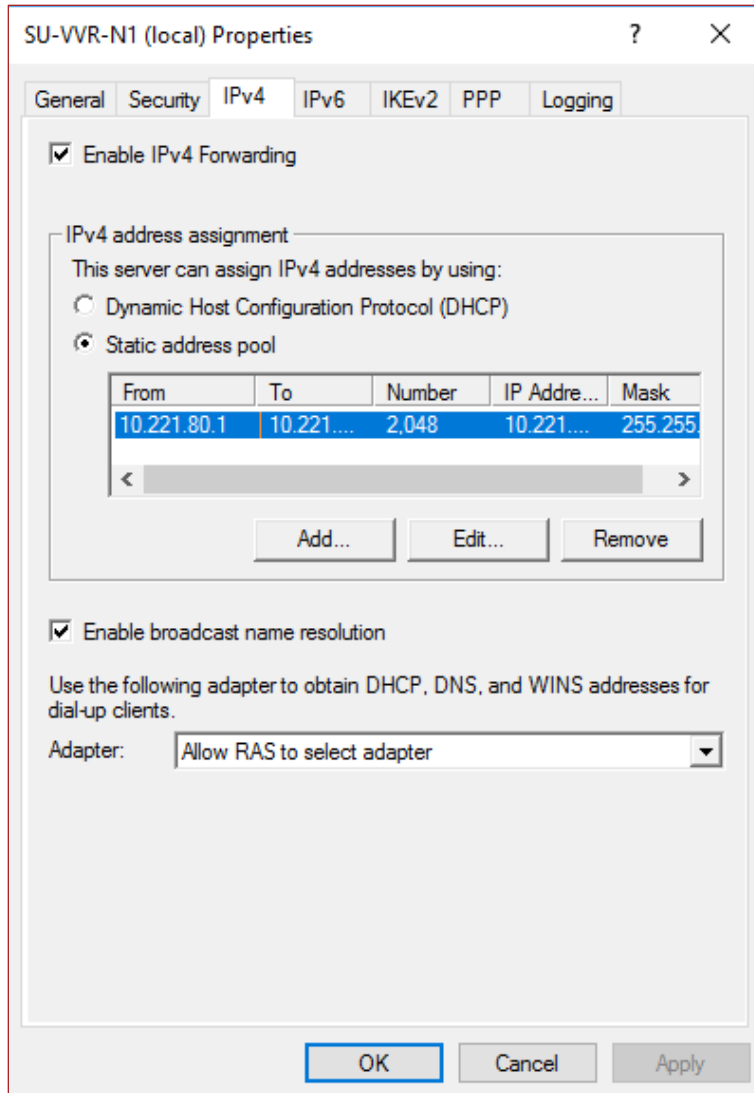
SSL Certificate Binding:  
 Use HTTP  
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Certificate: Default View

OK Cancel Apply

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

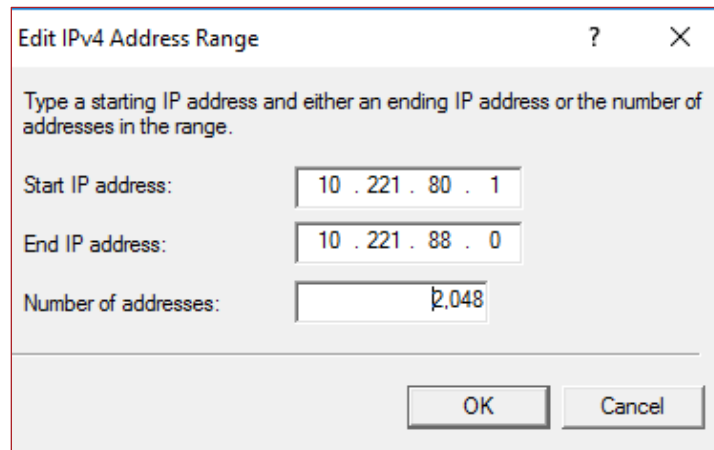
3. Navigate to the IPv4 tab. This sample configuration does not use a DHCP server but uses the **Static address pool** option instead. Click **Add...** to enter your IP address range.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

4. Use the following values and click **OK** to save them:

- **Start IP address:** 10.221.80.1
- **End IP address:** 10.221.88.0
- **Number of addresses:** 2048



The screenshot shows a dialog box titled "Edit IPv4 Address Range". The dialog contains the following text and fields:

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address:

End IP address:

Number of addresses:

At the bottom right, there are two buttons: "OK" and "Cancel".

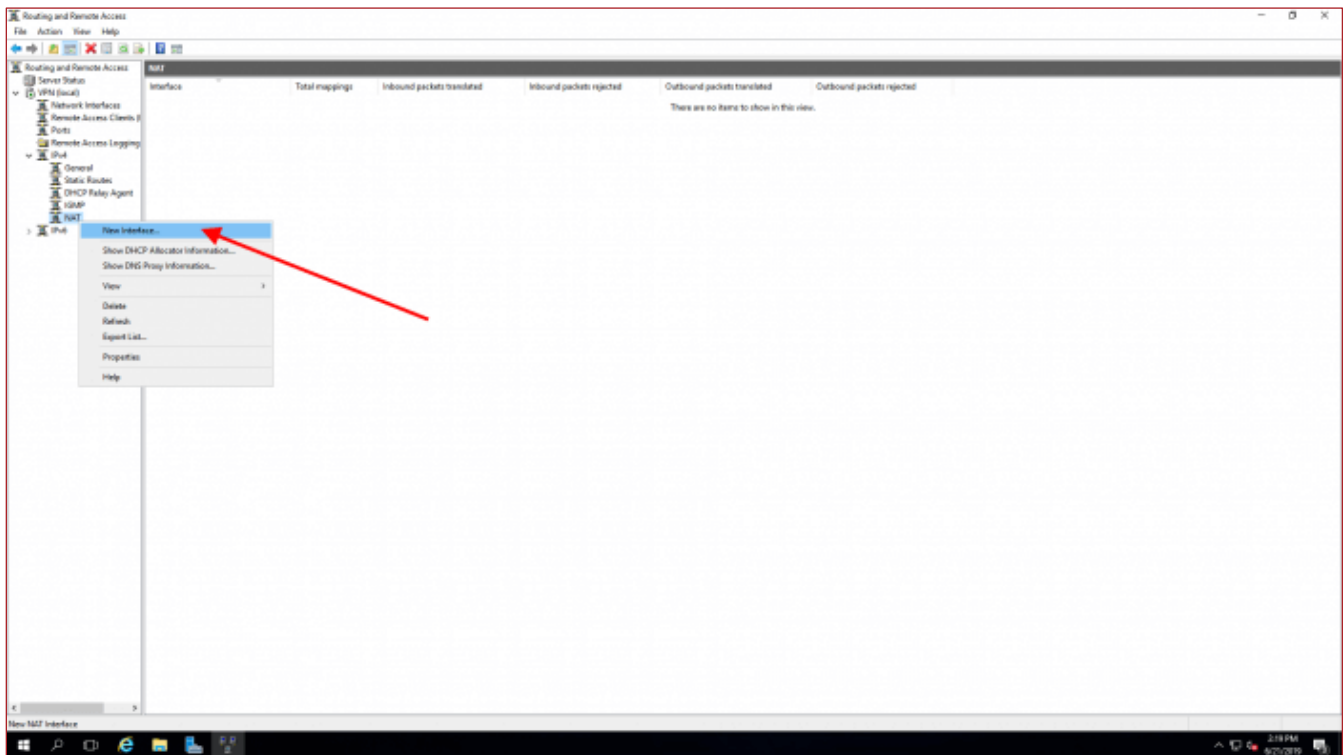
5. Click **OK** to apply the changes made to the Routing and Remote Access service properties. A message box appears to inform you about the required service restart; click **OK**.

# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

## Step 5

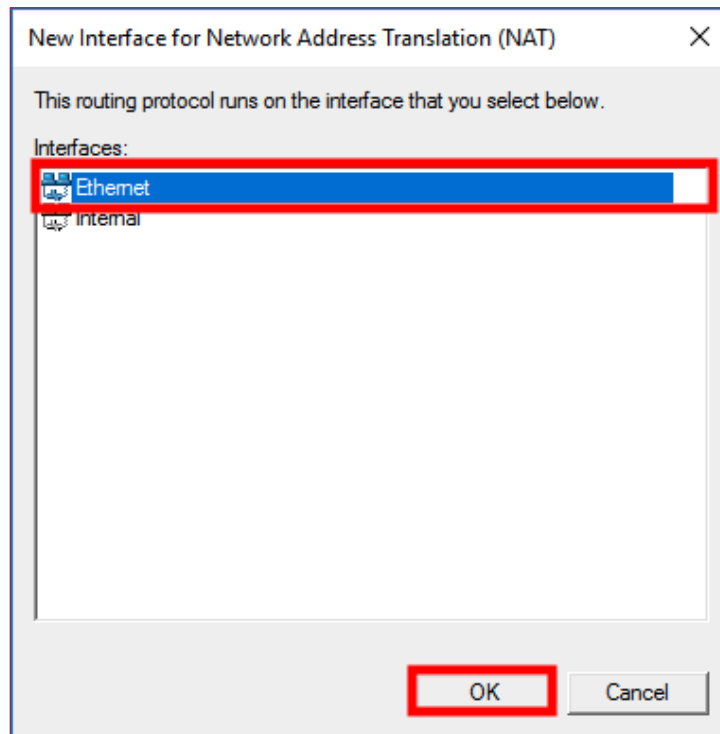
Configure NAT.

1. Navigate to **Routing and Remote Access** > **VPN (server name)** > **IPv4** > **NAT** and click **New Interface...** from the context menu.



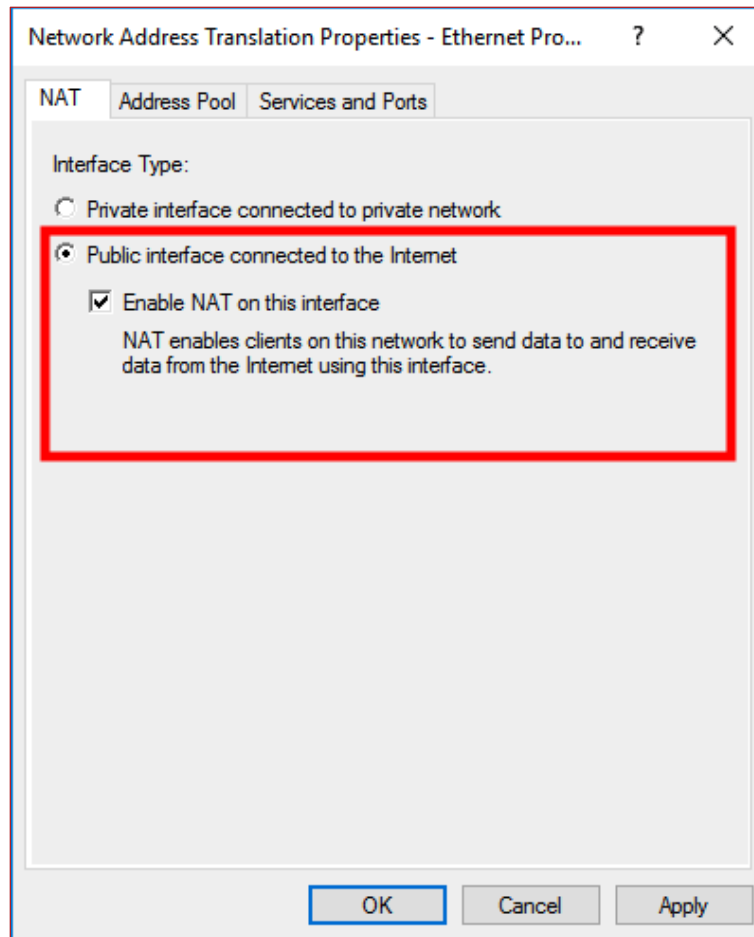
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

2. On the New Interface for Network Address Translation (NAT) dialog box, select **Ethernet** and click **OK**.



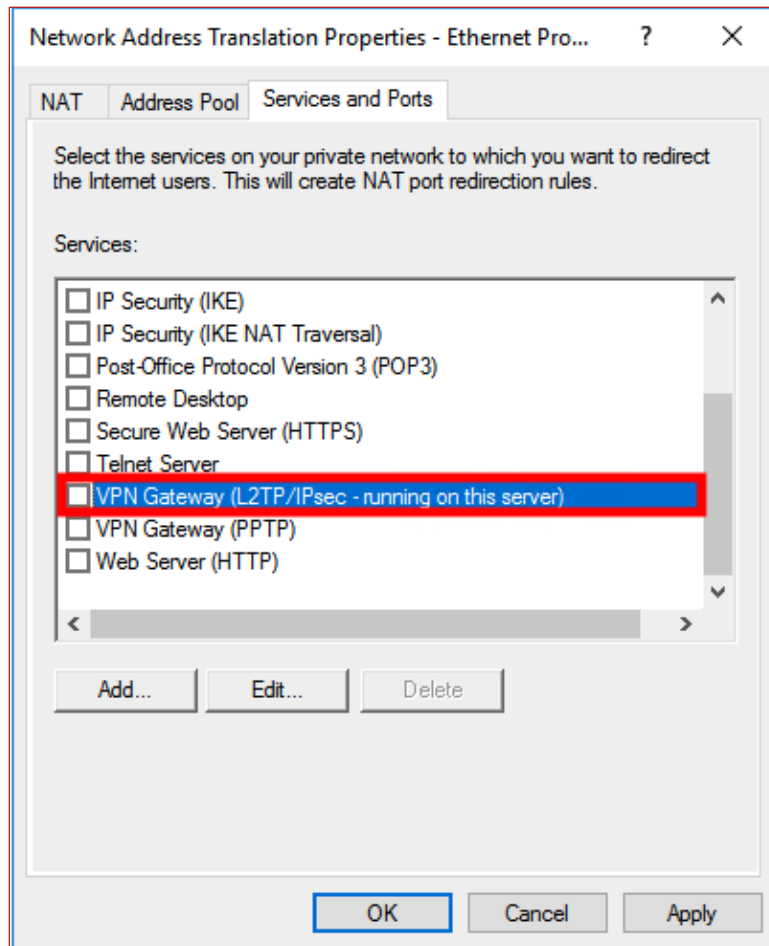
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

3. On the NAT tab of the Network Address Translation Properties screen, select **Public interface connected to the Internet** and **Enable NAT on this interface**.



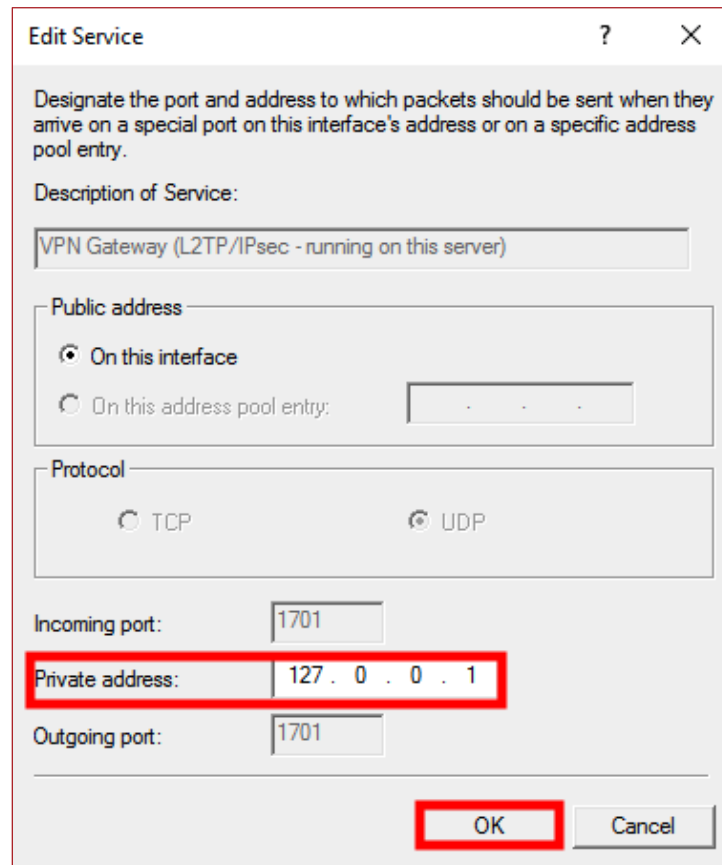
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

4. On the Services and Ports tab, select **VPN Gateway (L2TP/IPsec - running on this server)** from the list of services.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

5. On the Edit Service dialog box, edit the **Private address** from **0.0.0.0** to **127.0.0.1** and click **OK**.



**Edit Service** ? X

Designate the port and address to which packets should be sent when they arrive on a special port on this interface's address or on a specific address pool entry.

Description of Service:

VPN Gateway (L2TP/IPsec - running on this server)

**Public address**

On this interface

On this address pool entry: . . .

**Protocol**

TCP  UDP

Incoming port: 1701

**Private address:** 127 . 0 . 0 . 1

Outgoing port: 1701

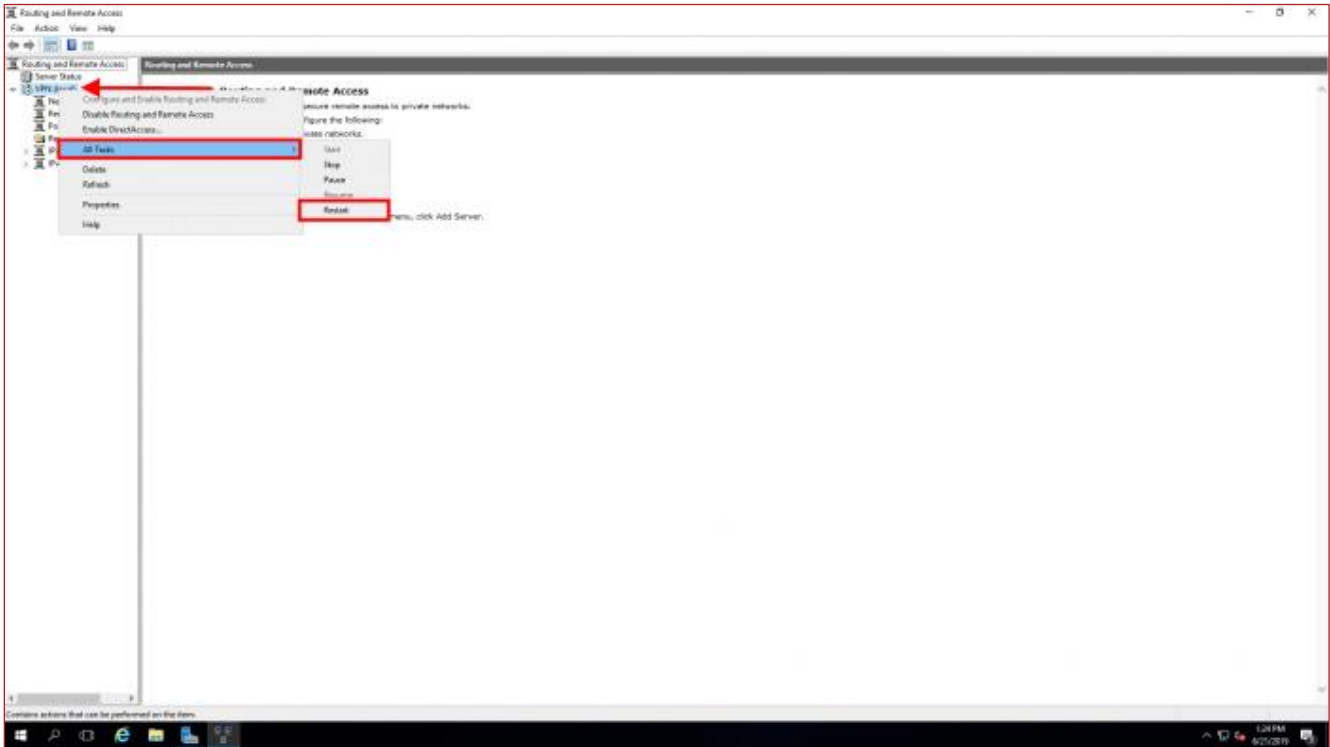
**OK** Cancel

6. Click **OK** to close the NAT properties screen.

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

### Step 6

Restart the Routing and Remote Access service—right-click the server name (VPN) and select **All Tasks > Restart**.

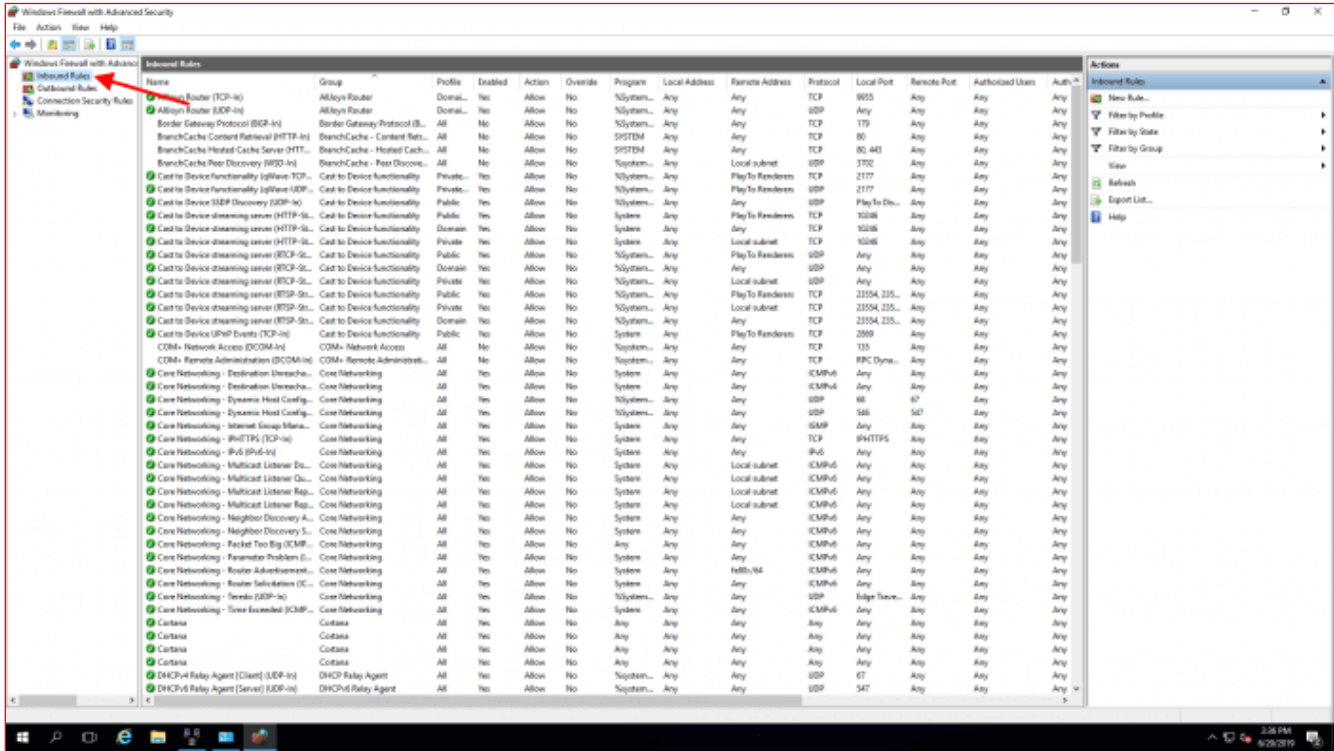


# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

## Step 7

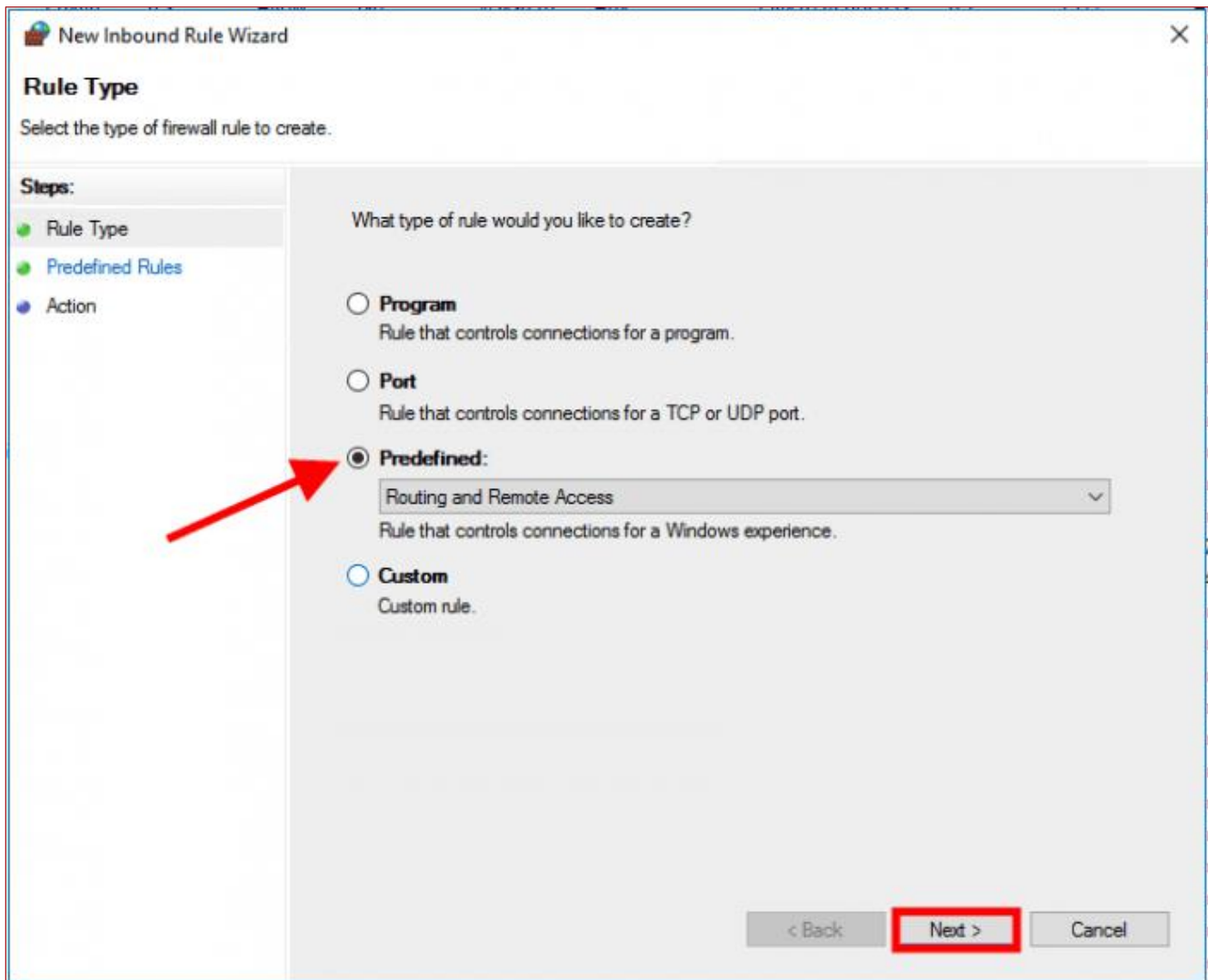
Set the Windows firewall rules.

1. Open the Windows firewall settings page, select **Advanced Settings > Inbound Rules > New Rule...**



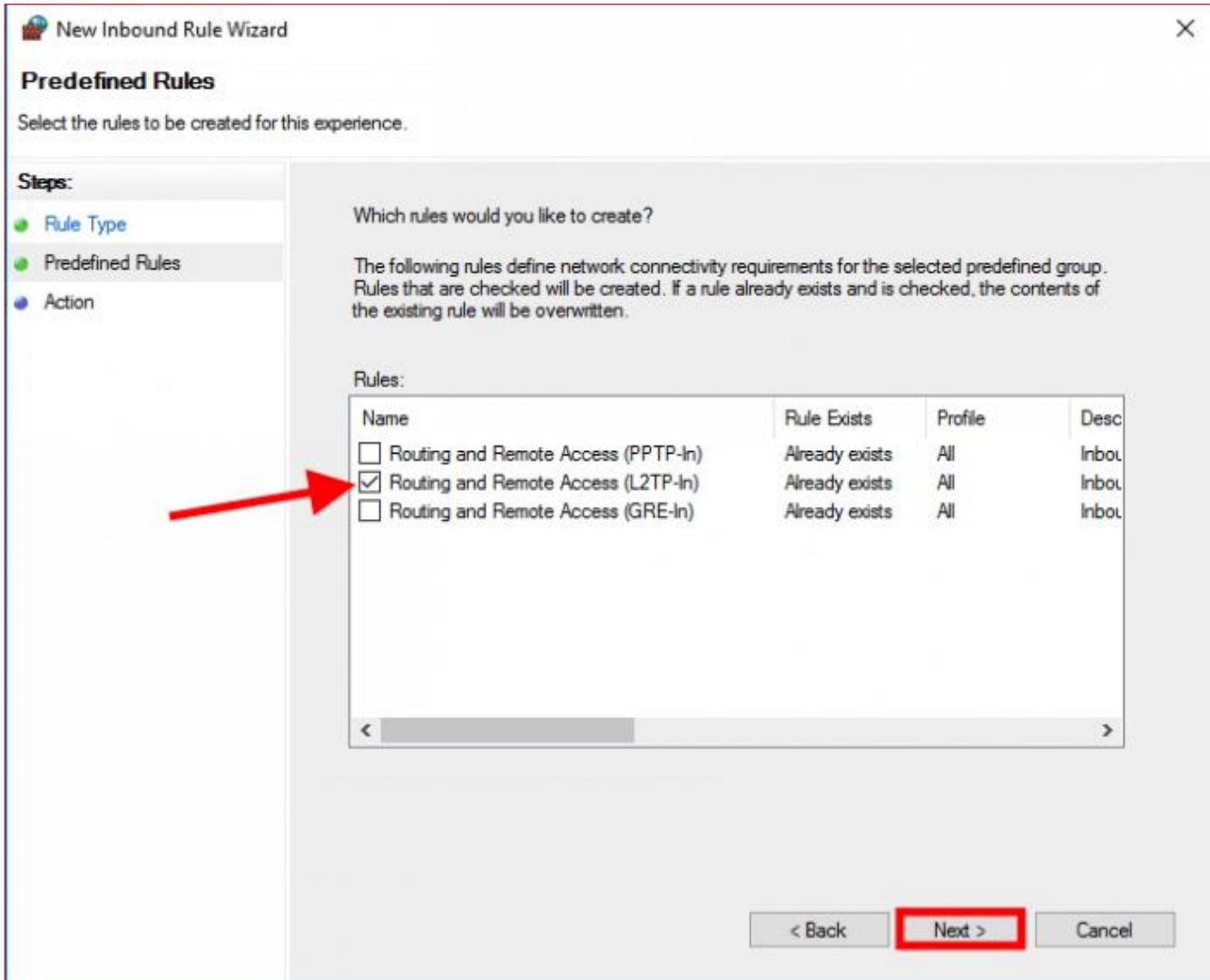
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

2. On the New Inbound Rule Wizard, select **Predefined: > Routing and Remote Access** and click **Next**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

3. Select **Routing and Remote Access (L2TP-In)** and click **Next**.



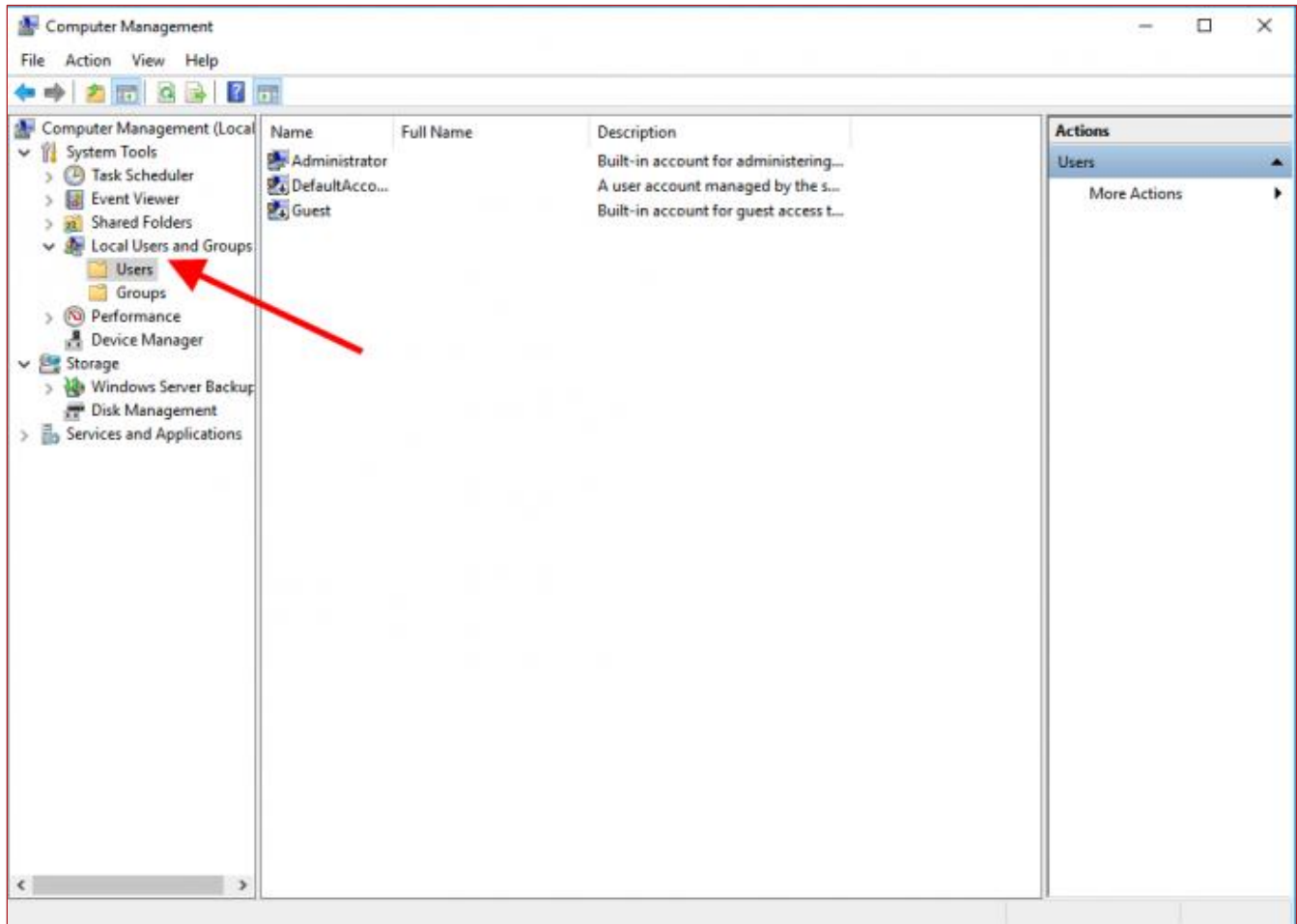
4. Click **Finish** and then verify that the rule is created.

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

### Step 8

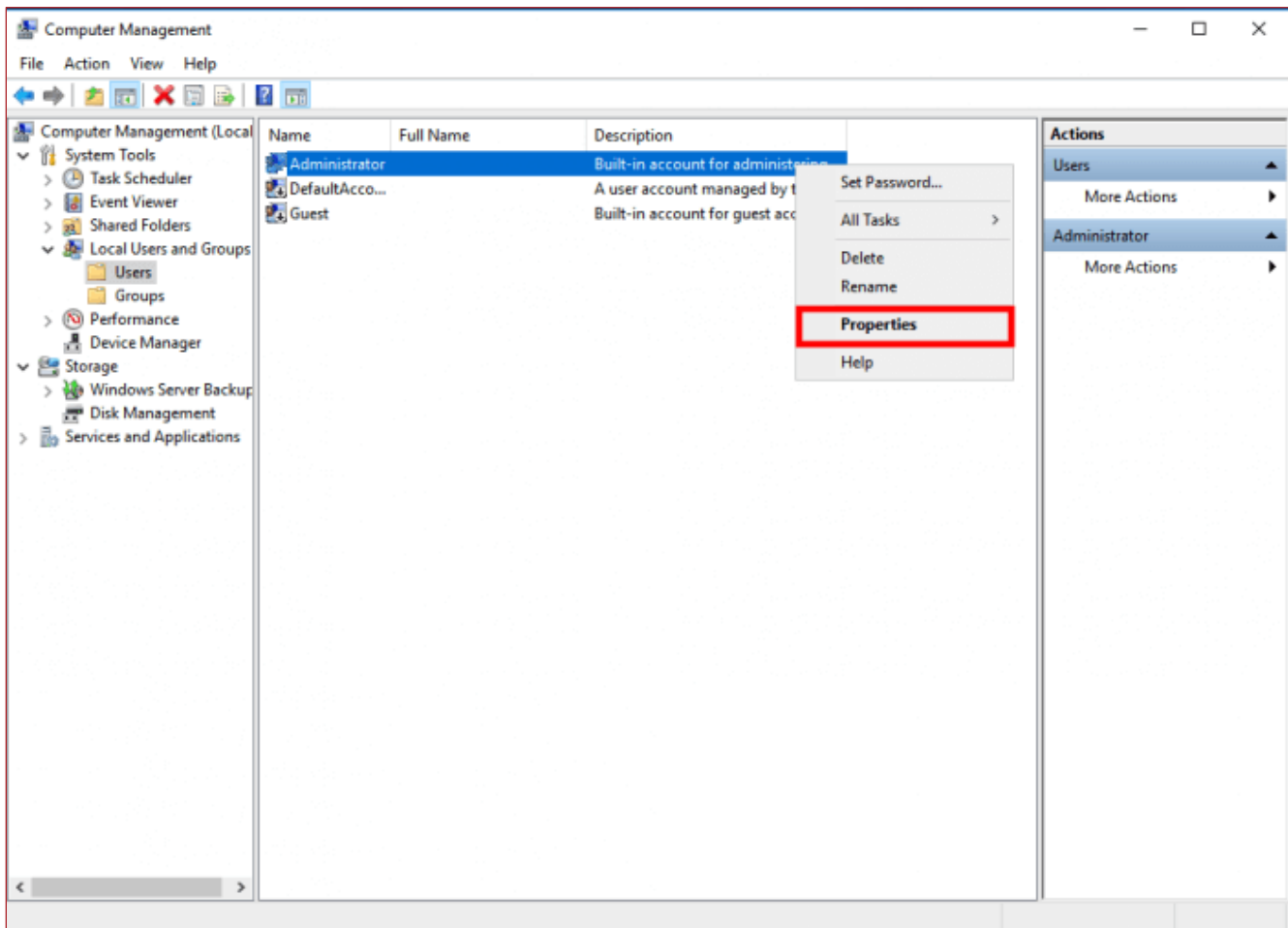
Assign network permissions to the appropriate users so that they can start using the VPN.

1. Open the Computer Management window and expand **Local Users and Groups > Users**.



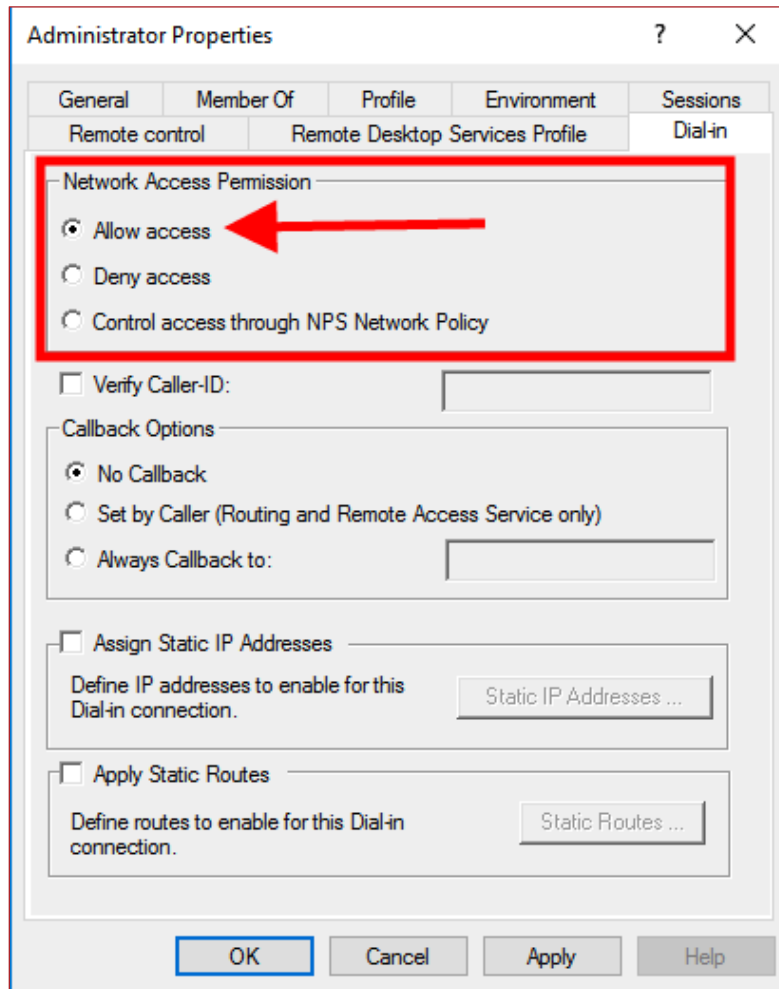
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

2. Right-click each user account for which you want to enable VPN access and click **Properties**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

3. On the properties screen that appears for a user account, provide the required values. For this sample configuration, on the Dial-in tab of the Administrator Properties screen, select **Allow access** in the **Network Access Permission** section.



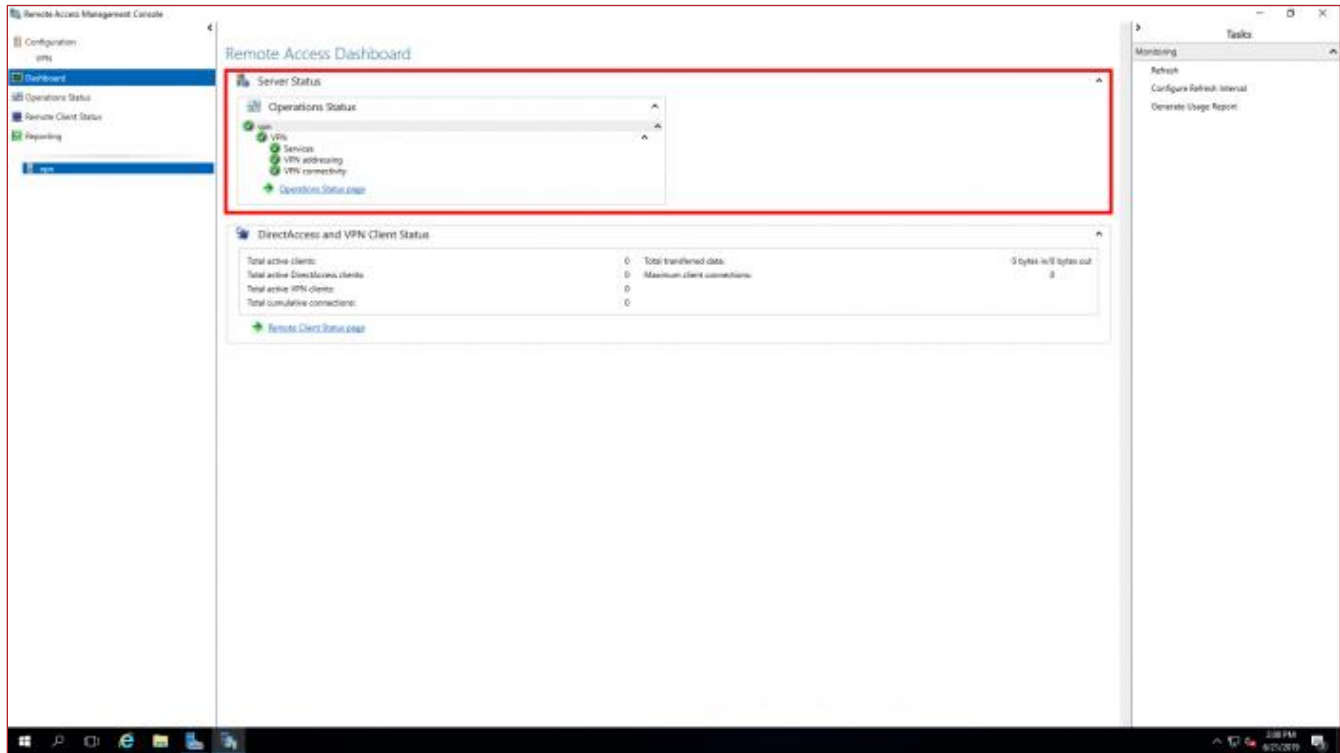
4. Click **OK** and close the Computer Management window. The Administrator user now has the permission to connect to the server via the L2TP/IPsec VPN connection.

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

### Step 9

View and manage remote access information.

1. Open the Server Manager window and click **Tools > Remote Access Management**.



2. On the Remote Access Management Console, the Remote Access Dashboard indicates that the services are running without any warnings.

### Step 10

Restart the server.

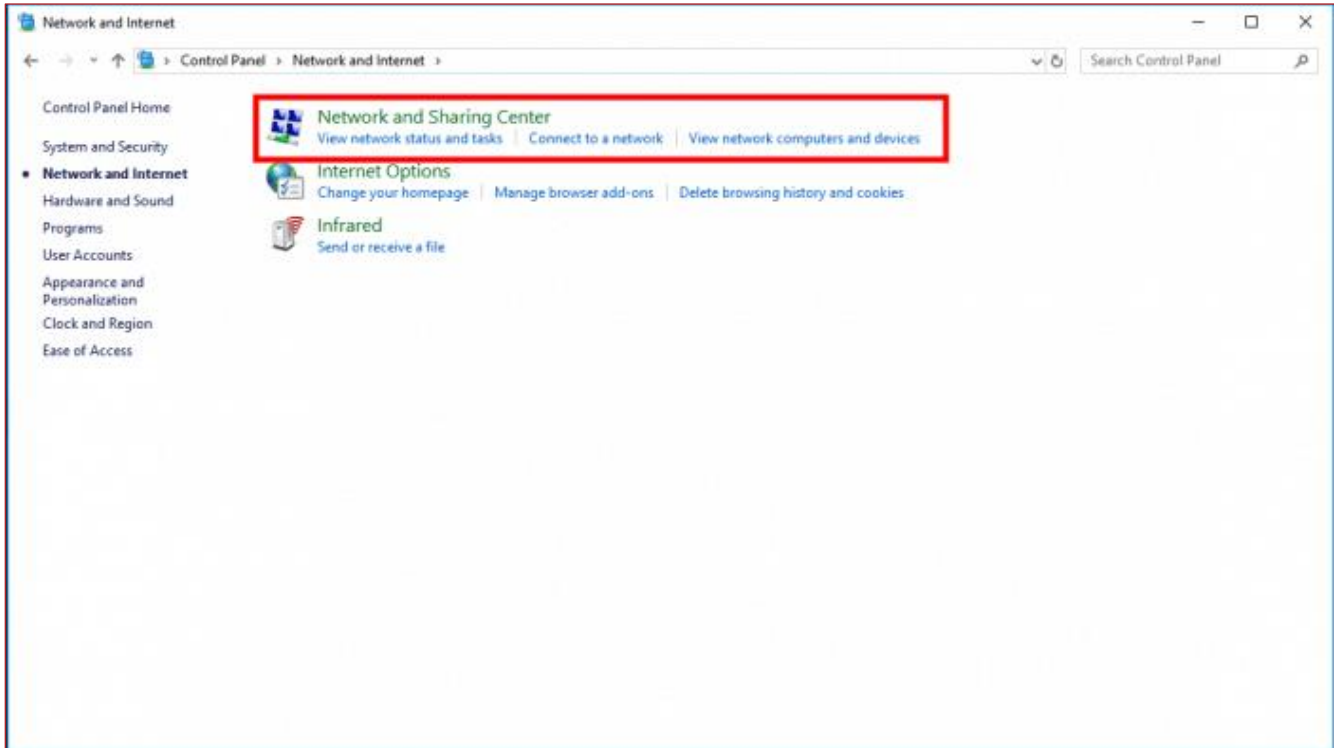
### Step 11

Repeat all the previous steps in this procedure to configure the secondary server as well.

## Connecting the L2TP/IPsec VPN

### Step 1

Log in to the primary server, open the Control Panel window, and click **Network and Internet**.

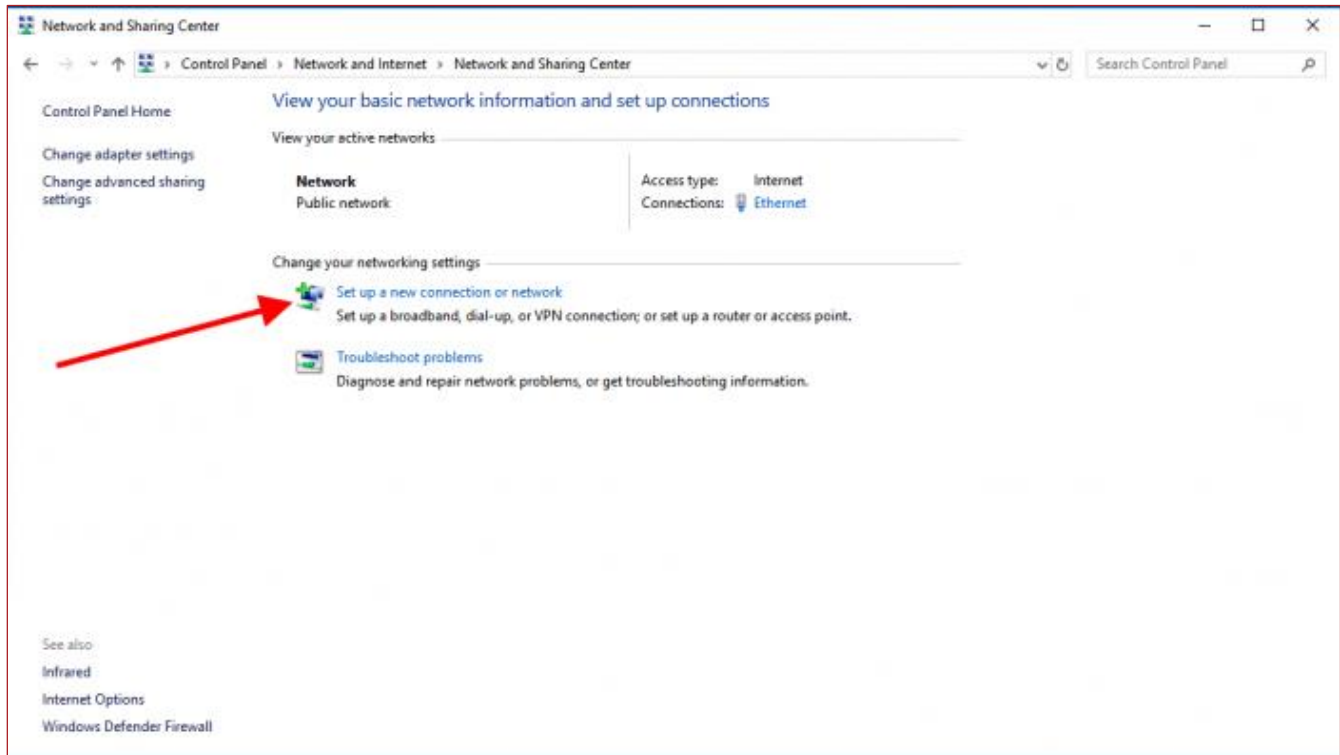


# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

## Step 2

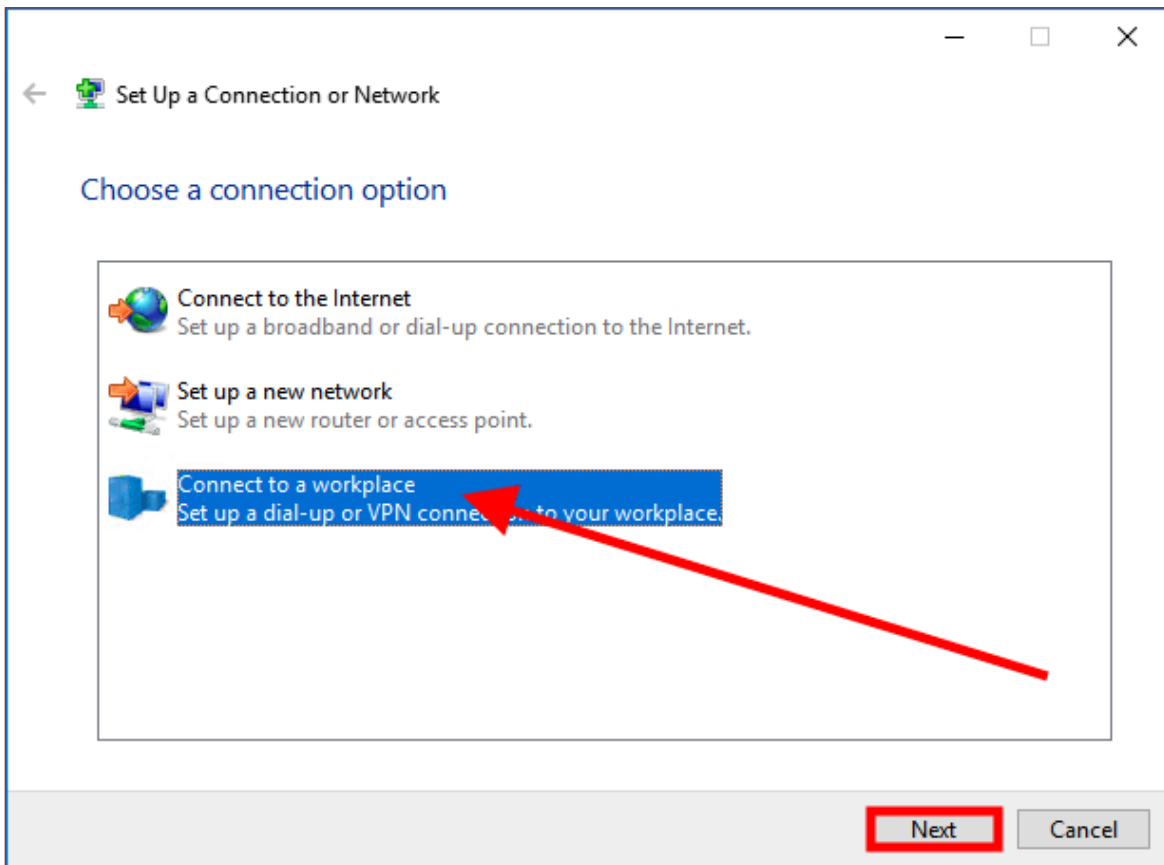
Configure the VPN.

1. On the Network and Sharing Center screen, click **Set up a new connection on a network**.



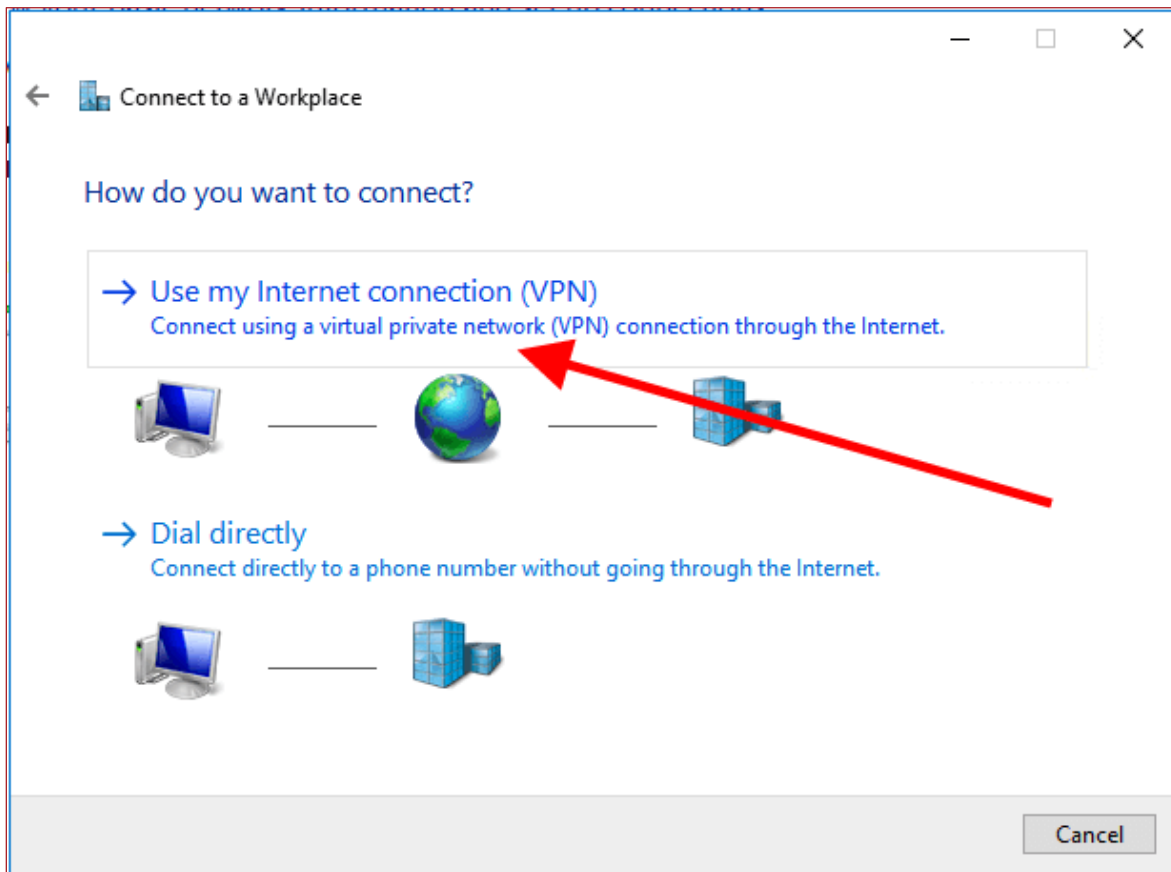
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

2. On the Set Up a Connection or Network wizard, select **Connect to a workplace** and click **Next**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

3. On the Connect to a Workplace screen, click **Use my Internet connection (VPN)**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

4. On the Connect to a Workplace screen, enter your IP address in the **Internet address:** field, and click **Create**. In this sample configuration, the IP address of the secondary server, 193.33.61.185, is used.

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 193.33.61.185

Destination name: VPN Connection

Use a smart card

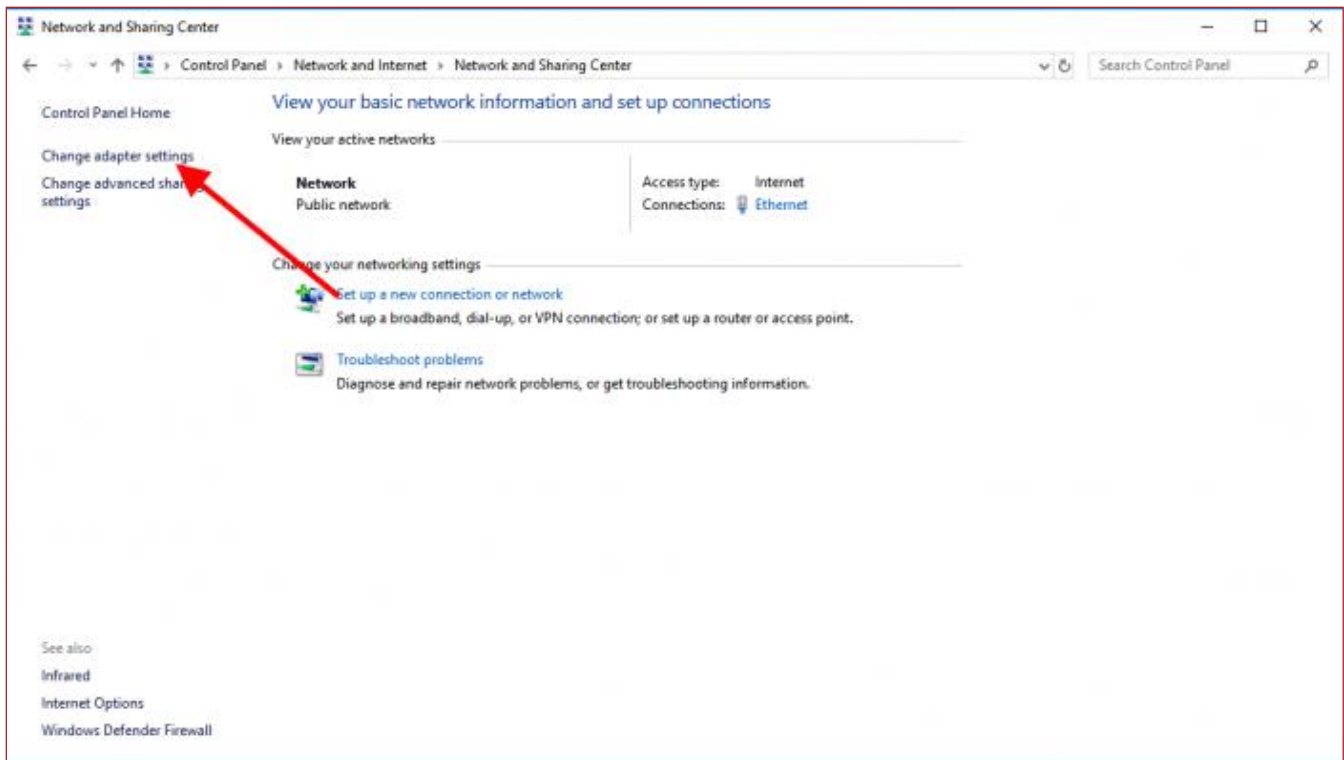
Remember my credentials

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

Create Cancel

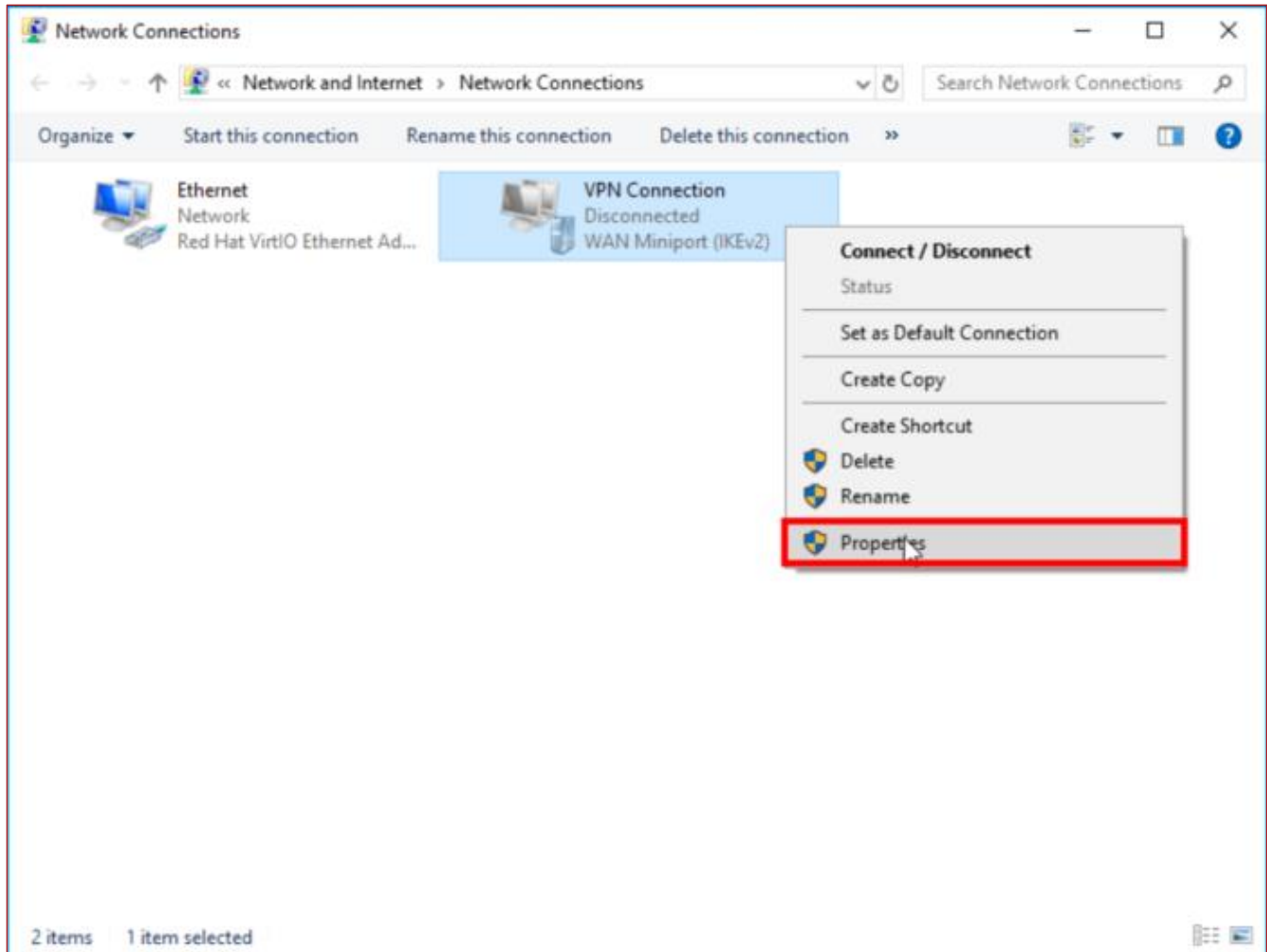
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

5. On the Network and Sharing Center screen, click **Change adapter settings** in the navigation menu on the left.



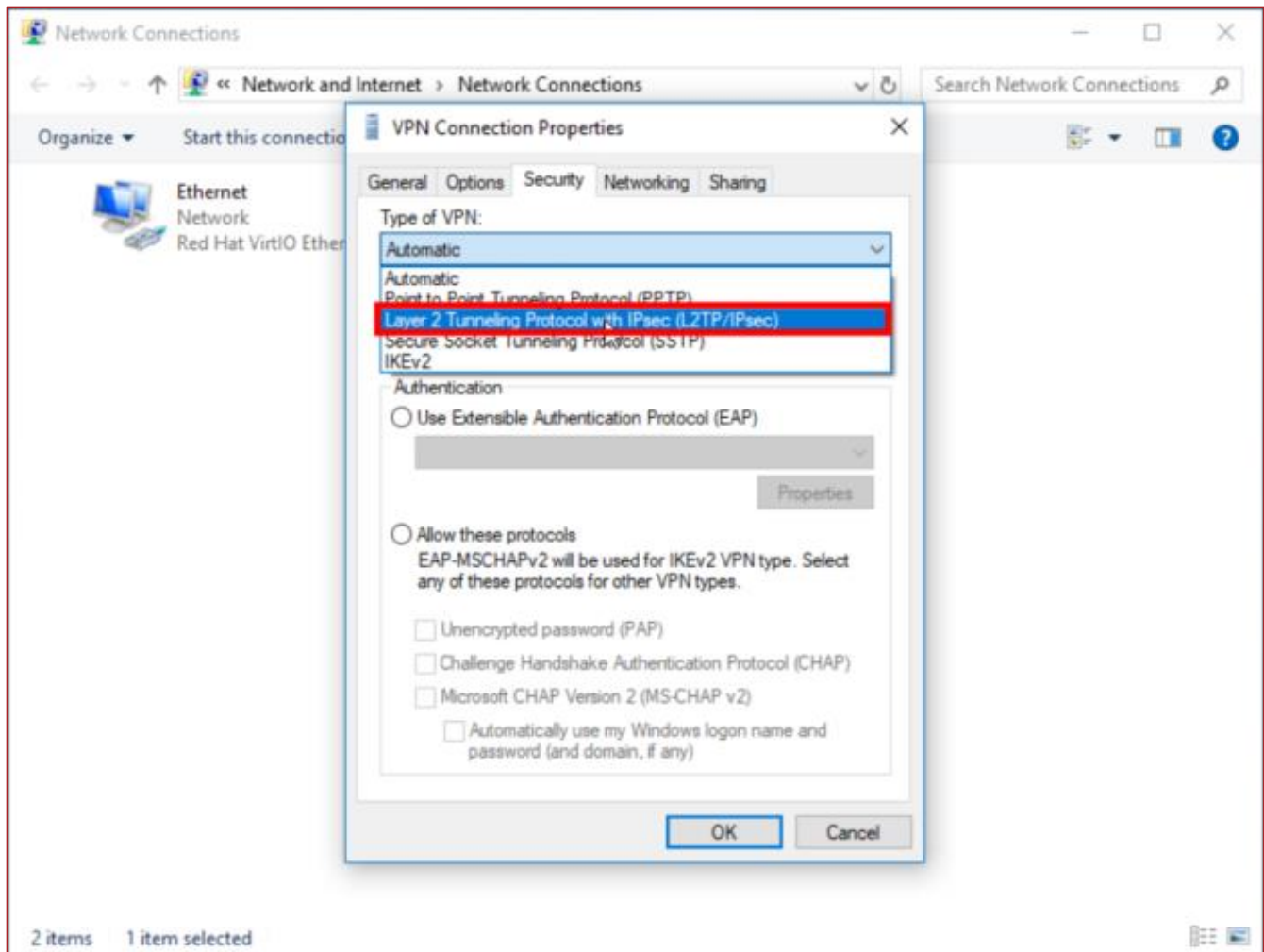
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

6. On the Network Connections screen, the VPN connection that you created earlier appears among all the available interfaces. Right-click the **VPN Connection** interface and click **Properties**.



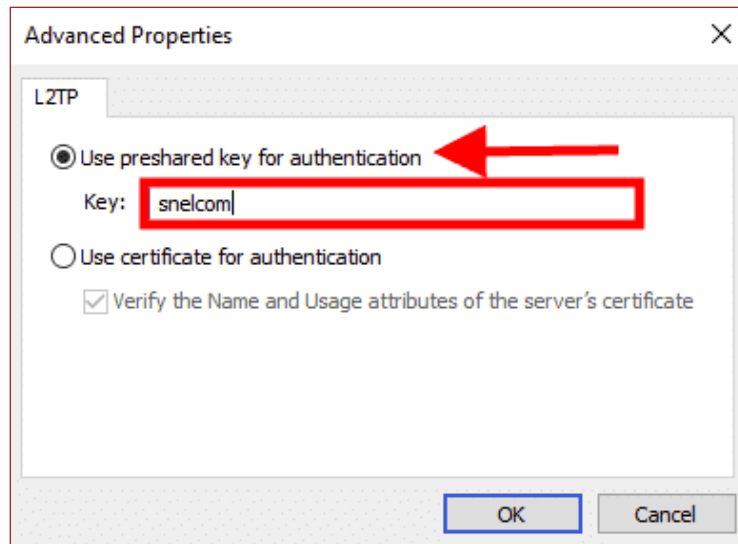
## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

7. On the VPN Connection Properties screen, open the Security tab, select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** from the **Type of VPN:** dropdown, and click **Advanced settings**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

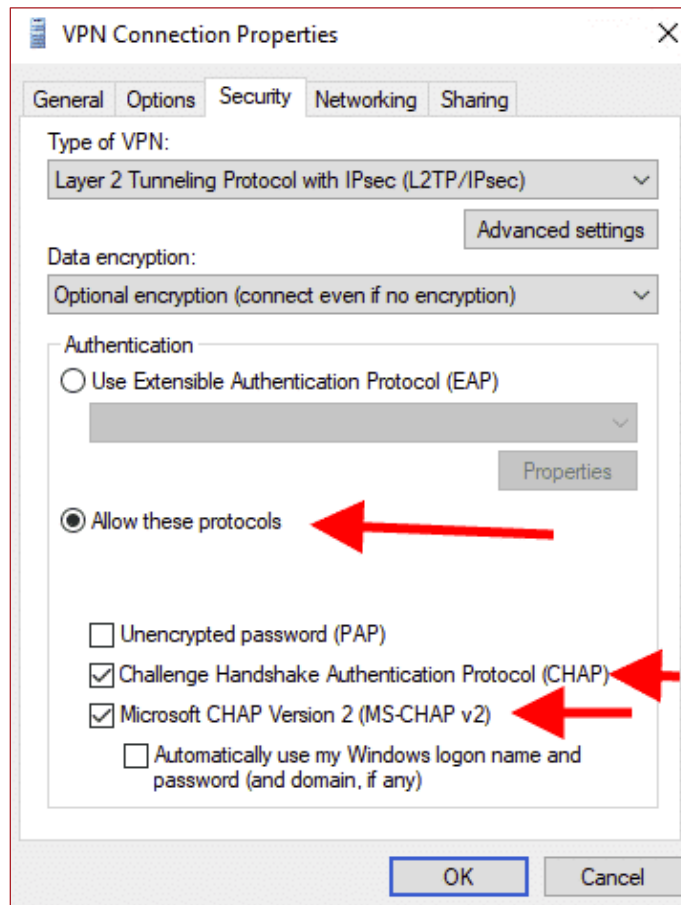
8. On the Advanced Properties dialog box, select **Use preshared key for authentication**, enter the preshared key that you created on the Windows Server, and click **OK**.



## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

9. On the Security tab, select **Allow these protocols**, select the following options, and then click **OK**:

- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP Version 2 (MS-CHAP v2)



### Step 3

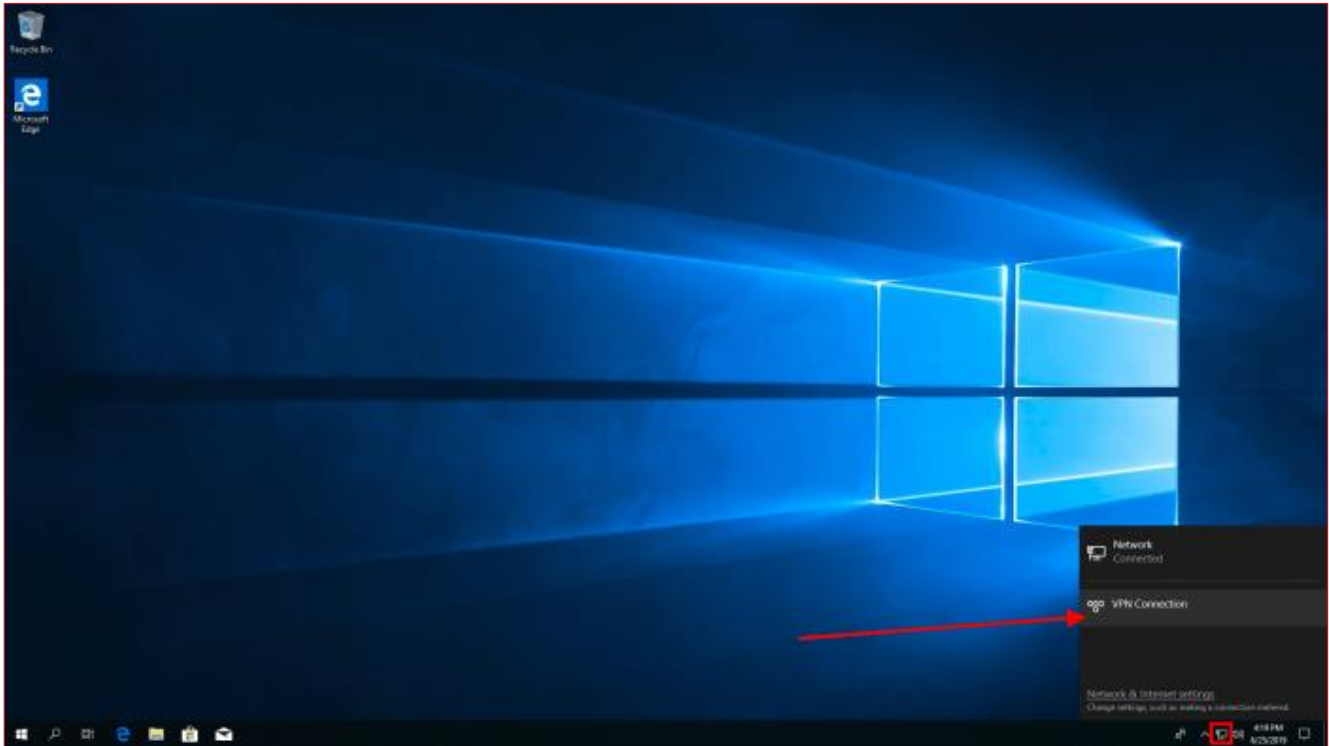
Configure the same settings on the secondary server. Use the internet address of the primary server while creating the VPN on the secondary server.

## Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

### Step 4

Connect to the VPN server

1. Click the Network icon in the system tray, click **VPN Connection**, and click **Connect**.



2. When prompted for credentials, enter the Administrator username and password.

The IPsec VPN connection is now established between the primary and the secondary, and the replication data being transmitted between the servers will be encrypted.

# Encryption of VVR Replication Data Over-the-Wire Using L2TP/IPsec VPN

---

## About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers— including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at [www.veritas.com](http://www.veritas.com). Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

2625 Augustine Drive, Santa Clara, CA 95054  
+1 (866) 837 4827  
[veritas.com](http://veritas.com)

For specific country offices  
and contact numbers,  
please visit our website.

**VERITAS™**