Configuration Guide

For VPN

TL-ER6120/TL-ER6020/TL-ER604W/TL-R600VPN

1910012268 REV1.0.0

January 2018

CONTENTS

1 VPN

1.1 Overview

VPN (Virtual Private Network) provides a means for secure communication between remote computers across a public WAN (Wide Area Network), such as the internet. Virtual indicates the VPN connection is based on the logical end-to-end connection instead of the physical end-to-end connection. Private indicates users can establish the VPN connection according to their requirements and only specific users are allowed to use the VPN connection.

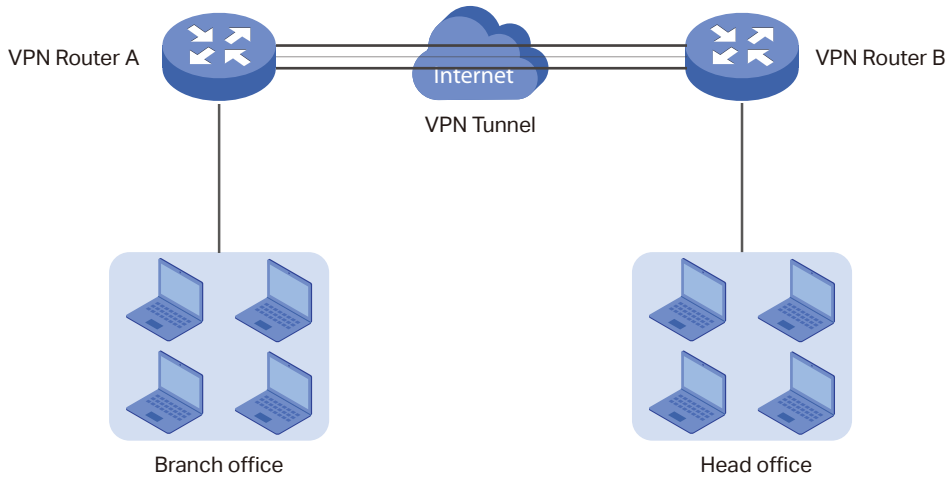
The core of VPN is to realize tunnel communication, which fulfills the task of data encapsulation, data transmission and data decompression via the tunneling protocol. Common tunneling protocols are Layer 2 tunneling protocol and Layer 3 tunneling protocol.

Depending on your network topology, there are two basic application scenarios: LAN-to-LAN VPN and Client-to-LAN VPN.

- LAN-to-LAN VPN

In this scenario, different private networks are connected together via the internet. For example, the private networks of the branch office and head office in a company are located at different places. LAN-to-LAN VPN can satisfy the demand that hosts in these private networks need to communicate with each other. The following figure shows the typical network topology in this scenario.

Figure 1-1 LAN-to-LAN VPN

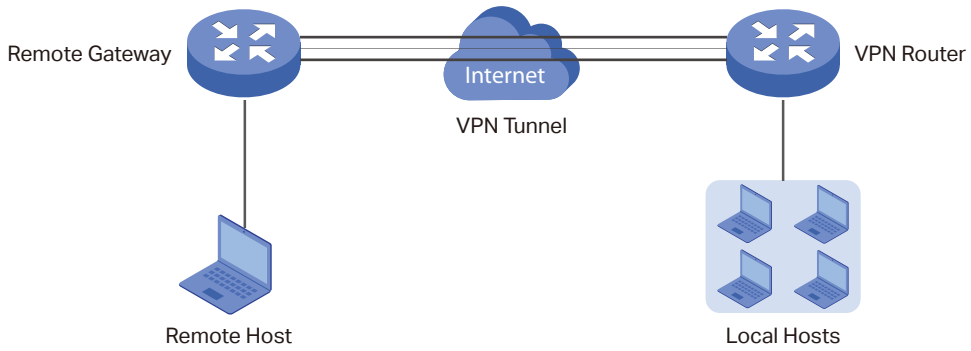


- Client-to-LAN VPN

In this scenario, the remote host is provided with secure access to the local hosts. For example, an employee on business can access the private network of his company

securely. Client-to-LAN VPN can satisfy this demand. The following figure shows the typical network topology in this scenario.

Figure 1-2 Client-to-LAN VPN



1.2 Supported Features

TP-Link SafeStream VPN Routers support Layer 2 tunneling protocol (PPTP, L2TP) and Layer 3 tunneling protocol (IPsec).

Note:

TL-R600VPN V3 or below doesn't support L2TP.

IPsec

IPsec (IP Security) can provide security services such as data confidentiality, data integrity and data origin authentication at the IP layer. IPsec uses IKEv1 (Internet Key Exchange version 1) to handle negotiation of protocols and algorithms based on the user-specified policy, and generate the encryption and authentication keys to be used by IPsec. IKEv1 negotiation includes two phases, that is IKEv1 Phase-1 and IKEv1 Phase-2. The basic concepts of IPsec are as follows:

- Proposal

Proposal is the security suite configured manually to be applied in IPsec IKEv1 negotiation. Specifically speaking, it refers to hash algorithm, symmetric encryption algorithm, asymmetric encryption algorithm applied in IKEv1 Phase-1, and security protocol, hash algorithm, symmetric encryption algorithm applied in IKEv1 Phase-2.

- Negotiation Mode

The negotiation mode configured for IKEv1 Phase-1 negotiation determines the role that the VPN router plays in the negotiation process. You can specify the negotiation mode as responder mode or initiator mode.

Responder Mode: In responder mode, the VPN router responds to the requests for IKEv1 negotiation and acts as the VPN server or the responder.

Initiator Mode: In initiator mode, the VPN router sends requests for IKEv1 negotiation and acts as the VPN client or the initiator.

- Exchange Mode

The exchange mode determines the way VPN routers negotiate in IKEv1 Phase-1. You can specify the exchange mode as main mode or aggressive mode.

Main Mode: In main mode, the identification information for authentication is encrypted, thus enhancing security.

Aggressive Mode: In aggressive mode, less packets are exchanged, thus improving speed.

- Authentication ID Type

The authentication ID type determines the type of authentication identifiers applied in IKEv1 Phase-1. It includes the local ID type and the remote ID type. The local ID indicates the authentication identifier sent to the other end, and the remote ID indicates that expected from the other end. You can specify the authentication ID type as IP address or name.

IP Address: The router uses the IP address for authentication.

Name: The router uses the FQDN (Fully Qualified Domain Name) for authentication.

- Encapsulation Mode

The encapsulation mode determines how packets transfered in the VPN tunnel are encapsulated. You can select tunnel mode or transport mode as the encapsulation mode. For most users, it is recommended to use the tunnel mode.

- PFS

PFS (Perfect Forward Secrecy) determines whether the key generated in IKEv1 Phase-2 is relevant with that in IKEv1 Phase-1. You can specify PFS as none, dh1, dh2, or dh5. None indicates that no PFS is configured, and the key generated in IKEv1 Phase-2 is relevant with that in IKEv1 Phase-1, whereas dh1, dh2, or dh5 means different key exchange groups, which make the key generated in IKEv1 Phase-2 irrelevant with that in IKEv1 Phase-1.

L2TP

L2TP (Layer 2 Tunneling Protocol) provides a way for a dial-up user to make a virtual PPP (Point-to-Point Protocol) connection to a VPN server. Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. The basic concepts of L2TP are as follows:

- IPsec Encryption

IPsec encryption determines whether the traffic of the tunnel is encrypted with IPsec. You can select encrypted or unencrypted as the IPsec encryption. If encrypted is selected,

a pre-shared key needs to be entered, and then the L2TP traffic will be encrypted with a default IPsec configuration. If unencrypted is selected, the VPN tunnel traffic will not be encrypted.

- Authentication

L2TP uses an account name and password for authentication on the VPN server. Only legal clients can set up a tunnel with the server, thus enhancing network security.

PPTP

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the internet. The basic concepts of PPTP are as follows:

- MPPE Encryption

MPPE (Microsoft Point-to-Point Encryption) scheme is a means of representing PPP packets in an encrypted form defined in RFC 3078. You can select encrypted or unencrypted as MPPE encryption. If encrypted is selected, the VPN tunnel traffic will be encrypted with RSA RC4 algorithm to ensure data confidentiality. If unencrypted is selected, the VPN tunnel traffic will not be encrypted.

- Authenticaiton

PPTP uses an account name and password for authentication on the VPN server. Only legal clients can set up a tunnel with the server, thus enhancing network security.

1.3 Configuration Guidelines

VPN does not involve the creation of a new physical connection. Instead, it is an additional feature built on the basis of the current network connection. Hence, the first step when creating a VPN tunnel is to acquire basic information about the network, such as the network topology. The necessary information is as follows.

- The IP addresses of both ends of the VPN tunnel

- The network topology of both ends of the VPN tunnel

Generally, if both ends are private networks, establish a LAN-to-LAN VPN tunnel. If one end is a remote client and the other end is a private network, establish a Client-to-LAN VPN tunnel.

- Whether any NAT devices exist between the ends of the tunnel

NAT devices may affect the establishment of VPN tunnel, so specific configuration needs to be implemented in that case, and IP addresses of NAT devices are also necessary. Please contact your ISP for that information.

- Whether you wish the remote client access the internet via the VPN proxy gateway

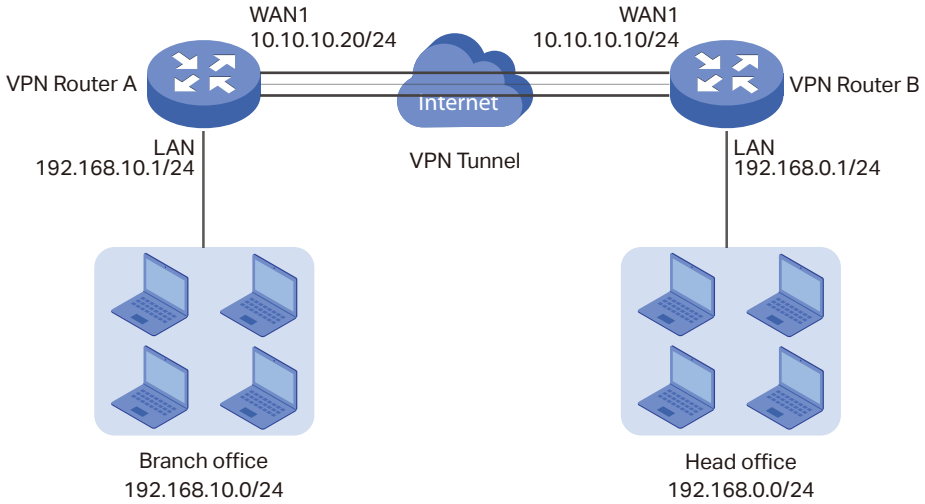
To satisfy this demand, you can establish an L2TP/PPTP Client-to-LAN VPN tunnel with specific configuration.

2 LAN-to-LAN VPN Configuration

2.1 Network Topology

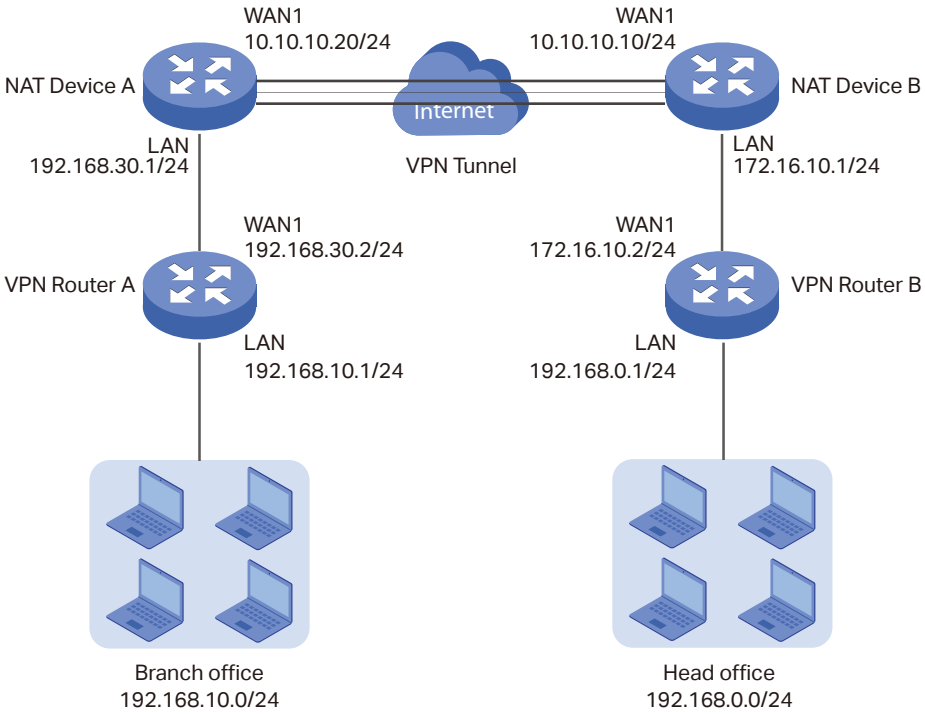
LAN-to-LAN VPN is deployed when different private networks are connected together via the internet. For example, the branch office and head office of a company are located at different places, and need to communicate with each other privately over the internet. The following figure shows the typical network topology.

Figure 2-1 LAN-to-LAN VPN



In actual network environments, NAT devices may exist in front of the VPN routers. The following figure shows the network topology in this scenario.

Figure 2-2 LAN-to-LAN VPN with NAT



LAN-to-LAN VPN can be established via three methods, including IPsec LAN-to-LAN VPN, PPTP LAN-to-LAN VPN, and L2TP LAN-to-LAN VPN. The topology shown in Figure 2-1 is used as an example, with TL-ER6120 used as the VPN router for demonstration purposes. Configuration instructions for the three methods are given below.

2.2 IPsec LAN-to-LAN VPN Configuration

To configure the IPsec LAN-to-LAN VPN, follow these steps:

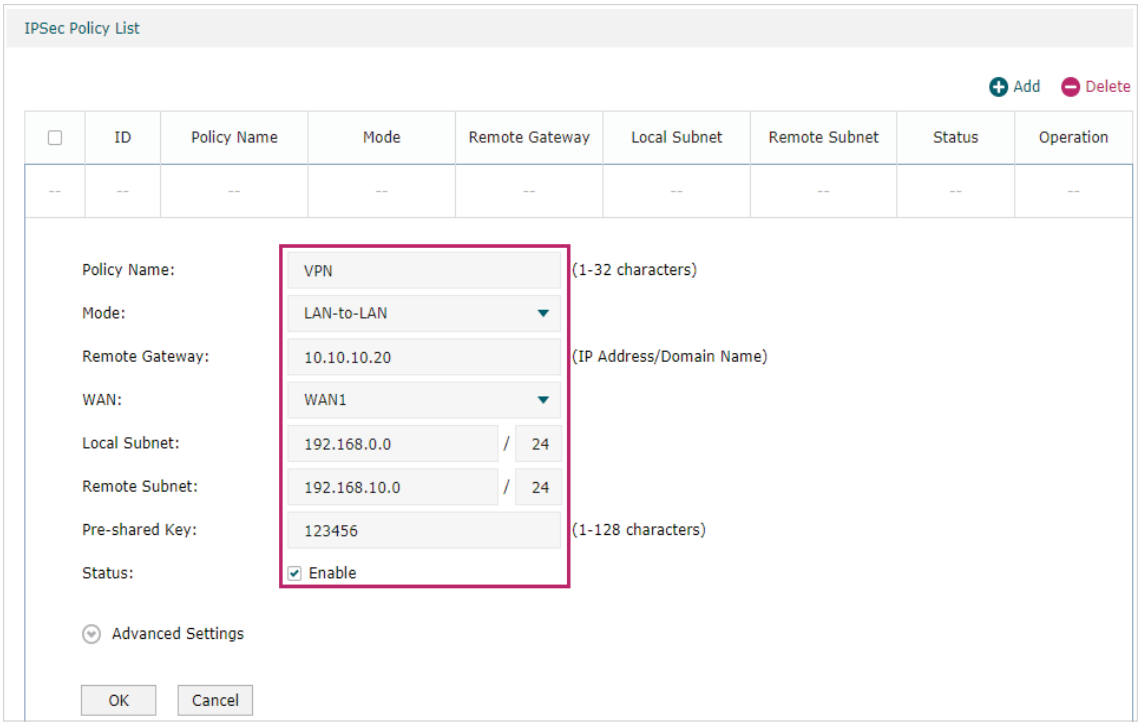
1) Configure the IPsec policy for the responder.
2) Configure the IPsec policy for the initiator.
3) (Optional) Implement configuration for NAT devices.
4) Verify the connectivity of the IPsec VPN tunnel.

2.2.1 Configuring the IPsec Policy for the Responder

Select any one of the VPN routers as the responder. Here we select VPN Router B as the responder. Follow these steps to configure IPsec policy for the responder.

1) Choose the menu **VPN** > **IPSec** > **IPSec Policy** and click **Add** to load the following page. Configure the basic parameters for the IPsec policy.

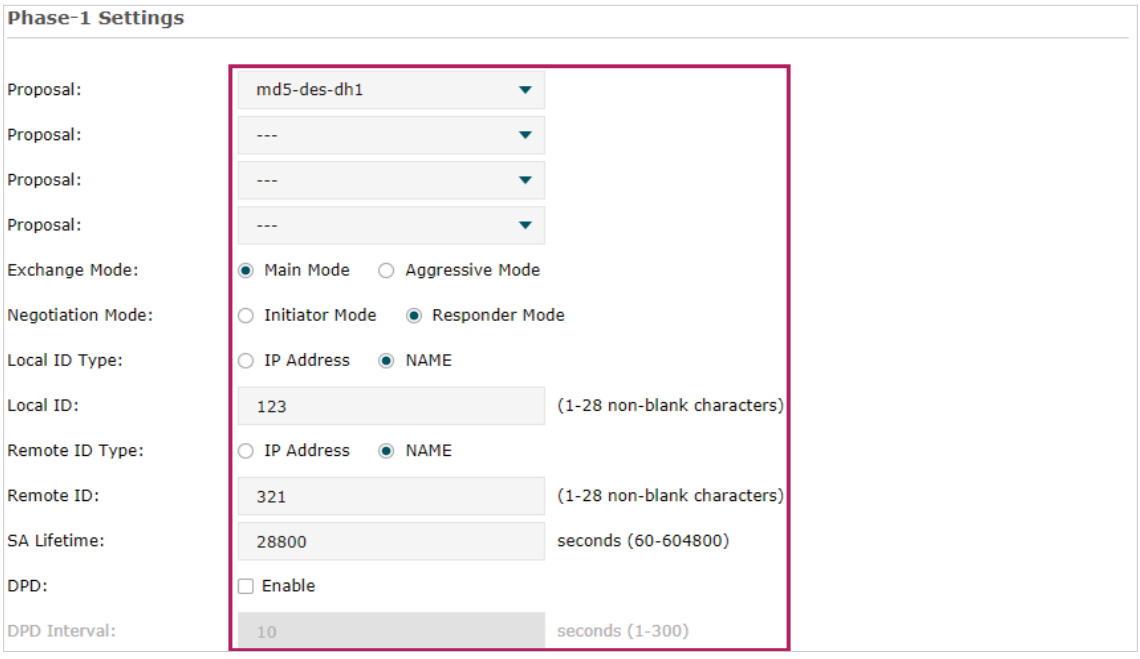
Figure 2-3 Configuring the IPsec policy



Policy Name	Specify the name of IPsec Policy. Here we enter **VPN**.
Mode	Specify the mode as **LAN-to-LAN.**
Remote Gateway	Specify the remote gateway as **10.10.10.20**. This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as **192.168.0.0/24**. This should be the subnet address of the local network.
Remote Subnet	Specify the remote subnet as **192.168.10.0/24**. This should be the subnet address of the remote network.
Pre-shared key	Specify the pre-shared key as you like. Here we enter **123456**.
Status	Enable the IPsec policy list entry.

2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Figure 2-4 Configuring the IKE phase-1 parameters

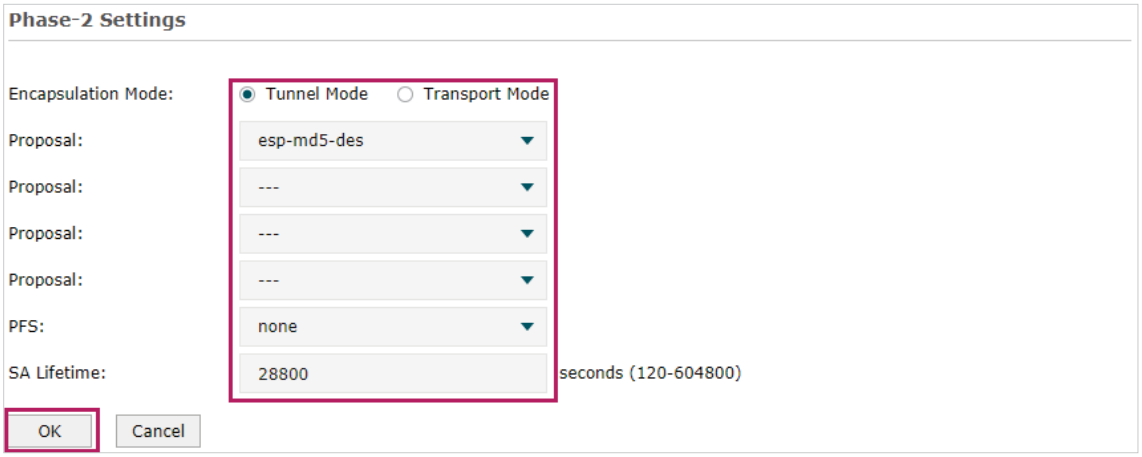


Proposal	Select the proposal from the drop-down list. Here we select **md5-des-dh1**.
Exchange Mode	Specify the exchange mode according to your needs. Here we specify the exchange mode as **Main Mode**.
Negotiation Mode	Specify the negotiation mode as **Responder Mode.**
Local ID Type/ Remote ID Type	Specify the local ID type and remote ID type as you like. Here we specify the local ID type and remote ID type as **NAME**.

Local ID/ Remote ID	Specify the local ID and remote ID as you like. Here we specify the local ID as **123** and remote ID as **321.**
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.
DPD	Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

3) In the **Phase-2 Settings** section, configure the IKE phase-2 parameters for the IPsec policy. Click **OK**.

Figure 2-5 Configuring the IKE phase-2 parameters



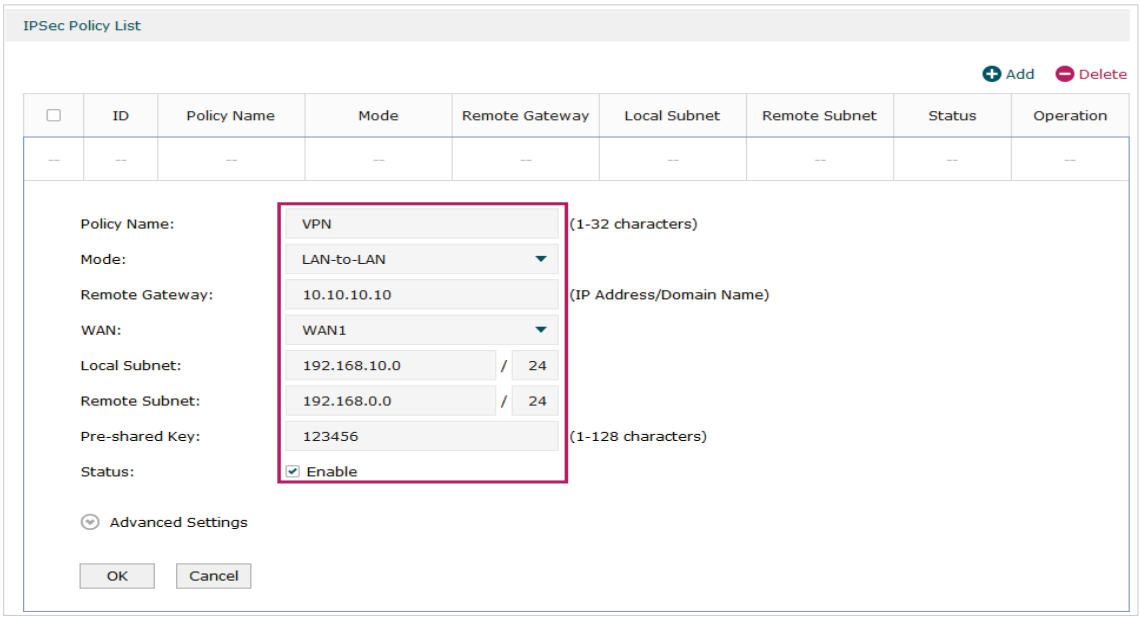
Encapsulation Mode	Specify the encapsulation mode as **Tunnel Mode.**
Proposal	Select the proposal from the drop-down list. Here we select **esp-md5-des**.
PFS	Select the PFS from the drop-down list according to your needs. Here we select **none**.
SA Lifetime	Specify the SA lifetime according to your needs. Here we keep the default setting.

2.2.2 Configuring IPsec Policy for the Initiator

Select the other VPN Router as the Initiator of IPsec negotiation. Here we select VPN Router A as the Initiator. Follow these steps to configure IPsec Policy for the initiator.

1) Choose the menu **VPN** > **IPSec** > **IPSec Policy** and click **Add** to load the following page. Configure the basic parameters for the IPsec policy.

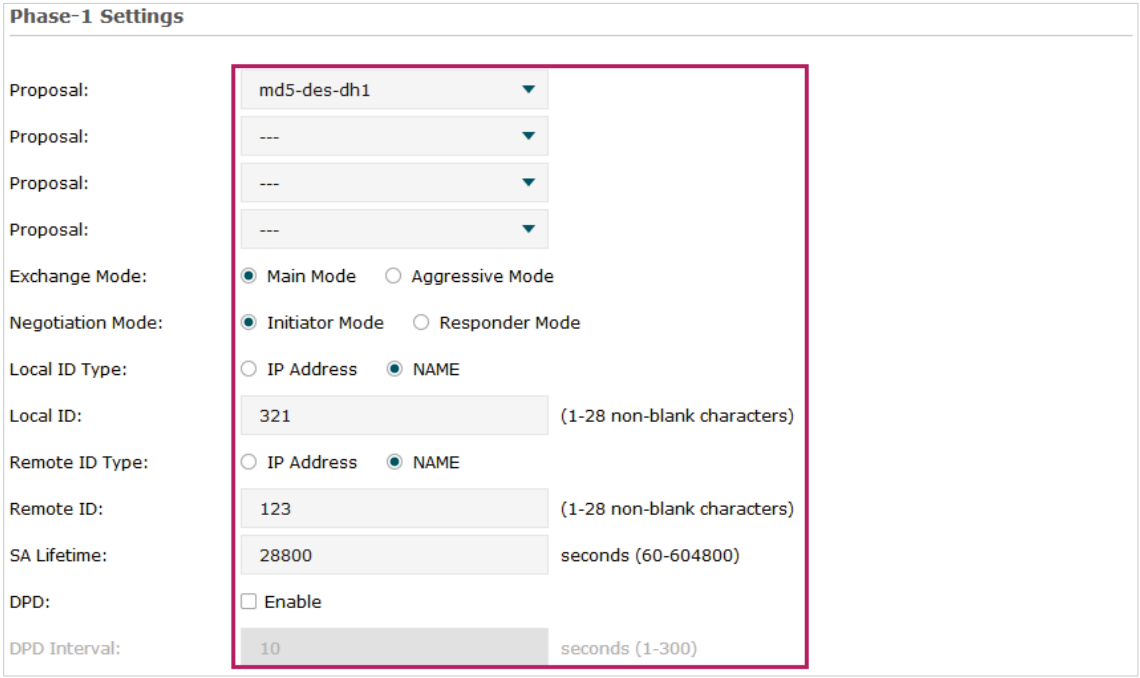
Figure 2-6 Configuring the IPsec policy



Policy Name	Specify the name of IPsec policy. Here we enter **VPN**.
Mode	Specify the mode as **LAN-to-LAN.**
Remote Gateway	Specify the remote gateway as **10.10.10.10**. This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as **192.168.10.0/24**. This should be the subnet address of the local network.
Remote Subnet	Specify the remote subnet as **192.168.0.0/24**. This should be the subnet address of the remote network.
Pre-shared key	Specify a pre-shared key as **123456**. This should be kept the same as that of the responder configuration.
Status	Enable the IPsec policy list entry.

2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

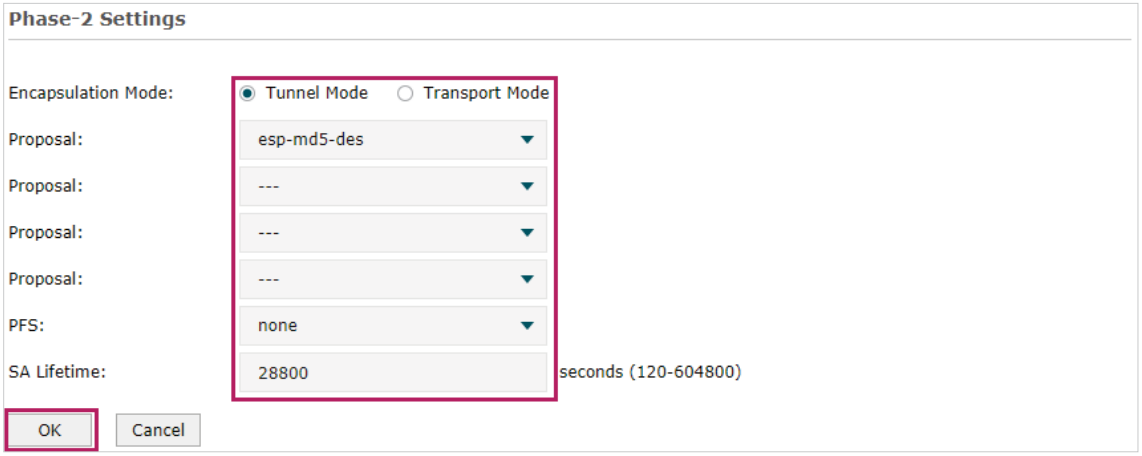
Figure 2-7 Configuring the IKE phase-1 parameters



Proposal	Select **md5-des-dh1** as the proposal**.** This should be kept the same as that of the responder configuration.
Exchange Mode	Specify the exchange mode as **Main Mode**. This should be kept the same as that of the responder configuration.
Negotiation Mode	Specify the negotiation mode as **Initiator Mode.**
Local ID Type/ Remote ID Type	Specify the local ID type and remote ID type as **NAME**. The local ID type and remote ID type should be kept the same as that of the responder configuration.
Local ID/ Remote ID	Specify the Local ID as **321** and Remote ID as **123.** The local ID and remote ID should be reversed in comparison to the responder.
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.
DPD	Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

3) In the **Phase-2 Settings** section, configure the IKE phase-2 parameters for the IPsec policy. Click **OK**.

Figure 2-8 Configuring the IKE phase-2 parameters



Encapsulation Mode	Specify the encapsulation mode as **Tunnel Mode.**
Proposal	Select **esp-md5-des** as the proposal. This should be kept the same as that of the responder configuration.
PFS	Select **none** as the PFS. This should be kept the same as that of the responder configuration.
SA Lifetime	Specify the SA Lifetime according to your needs. Here we keep the default setting.

2.2.3 (Optional) Implementing configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 2-2. In this scenario, please verify the configuration on both VPN routers, configure virtual servers on NAT Device B, and configure IPsec ALG on both NAT devices. The configuration steps are as follows:

1) For both VPN routers, choose the menu **VPN** > **IPSec** > **IPSec Policy**, select the IPsec policy list entry which is previously created, and click to load the following page. Please make sure that in the **Phase-1 Settings** section, the local ID type and remote ID type are both specified as **NAME**, and in the **Phase-2 Settings** section, the proposal is **not** specified as **ah-md5** or **ah-sha1**. Otherwise, the VPN tunnel may fail to be established.

Figure 2-9 Verifying the phase-1 configuration

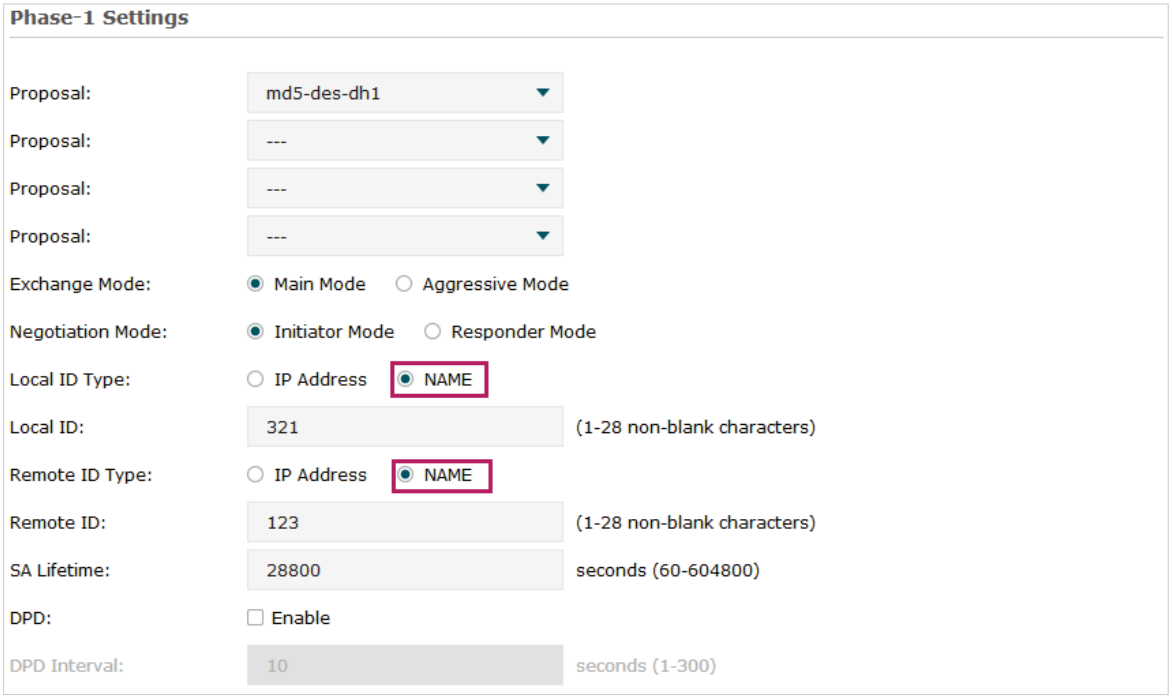
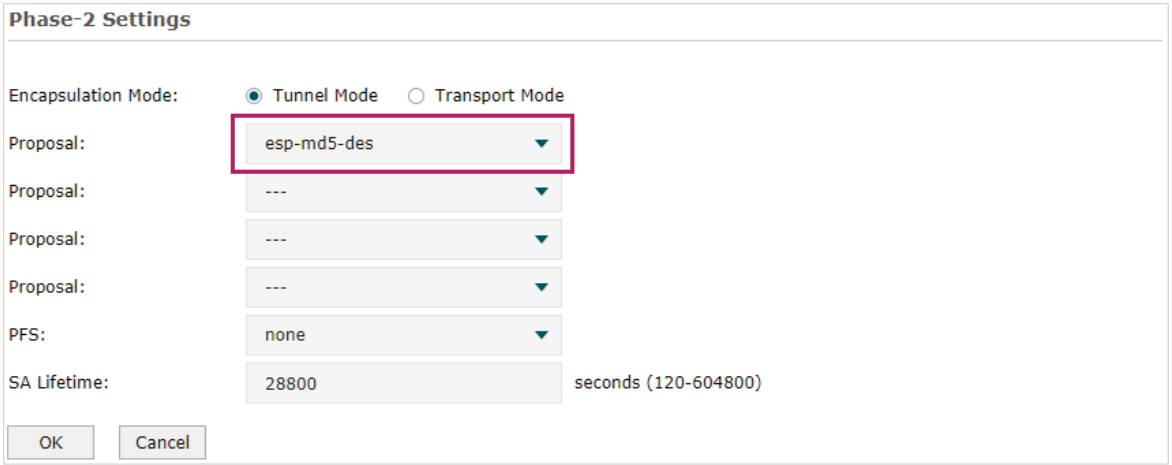
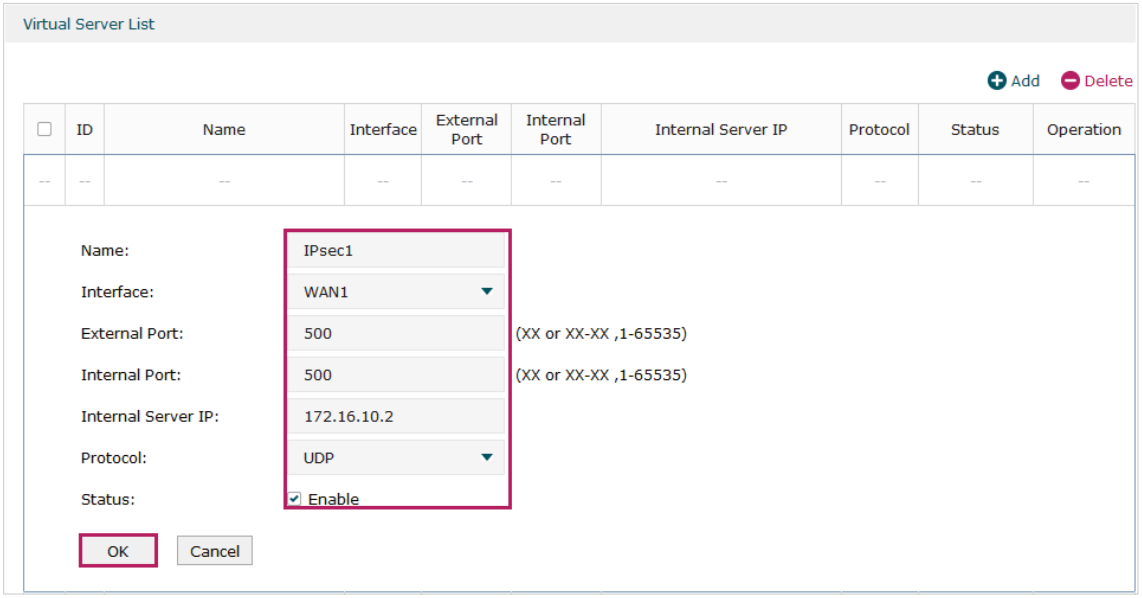


Figure 2-10 Verifying the phase-2 configuration



2) For NAT Device B, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page. Configure the parameters for the virtual server. Click **OK**.

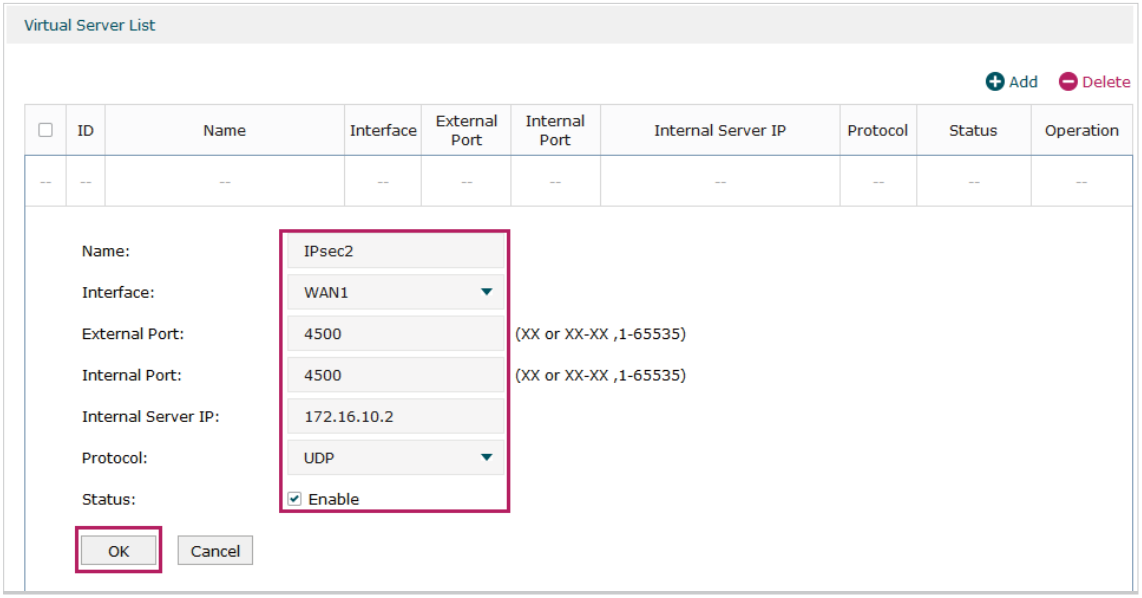
Figure 2-11 Configuring virtual server for IPsec



Name	Specify a name for the virtual server list entry. Here we enter **IPsec1**.
Interface	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the external port and the internal port as **500**.
Internal Server IP	Specify the internal server IP as **172.16.10.2.** This should be the WAN IP address of the responder.
Protocol	Specify the protocol as **UDP**.
Status	Enable the virtual server list entry.

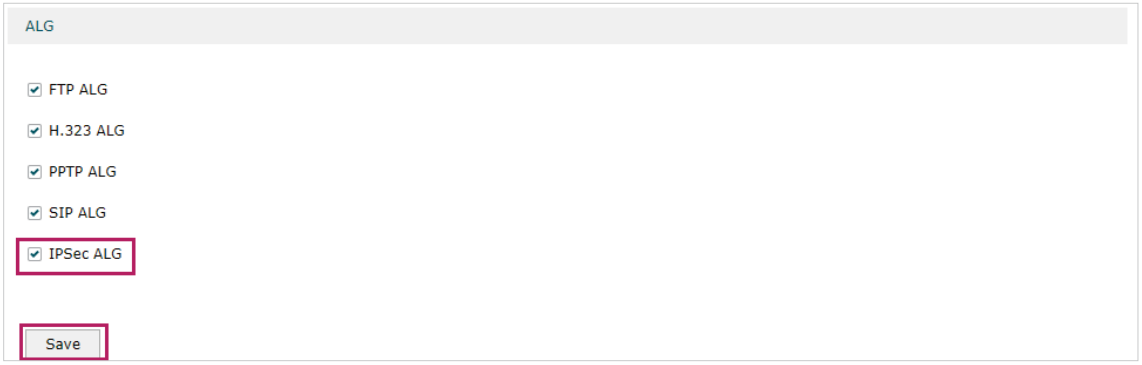
Similarly, add another virtual server list entry, with the name IPsec2, and set the external and internal port as 4500.

Figure 2-12 Configuring virtual server for IPsec



3) For NAT Device A and NAT Device B, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable the IPsec ALG, and click **Save**.

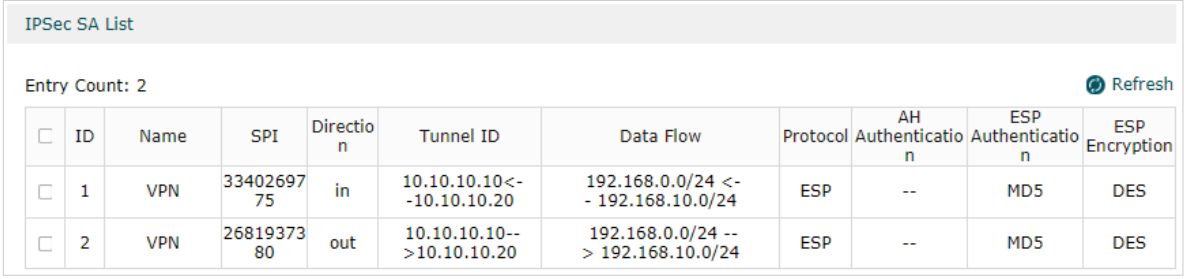
Figure 2-13 Configuring IPsec ALG



2.2.4 Verifying the Connectivity of the IPsec VPN Tunnel

Choose the menu **VPN** > **IPSec** > **IPSec SA** to load the following page.

Figure 2-14 IPSec SA list



The IPsec SA list shows the information about the established IPsec VPN tunnel. Here, you can verify the connectivity of the IPsec VPN tunnel.

2.3 L2TP LAN-to-LAN VPN Configuration

To complete the L2TP LAN-to-LAN VPN, follow these steps:

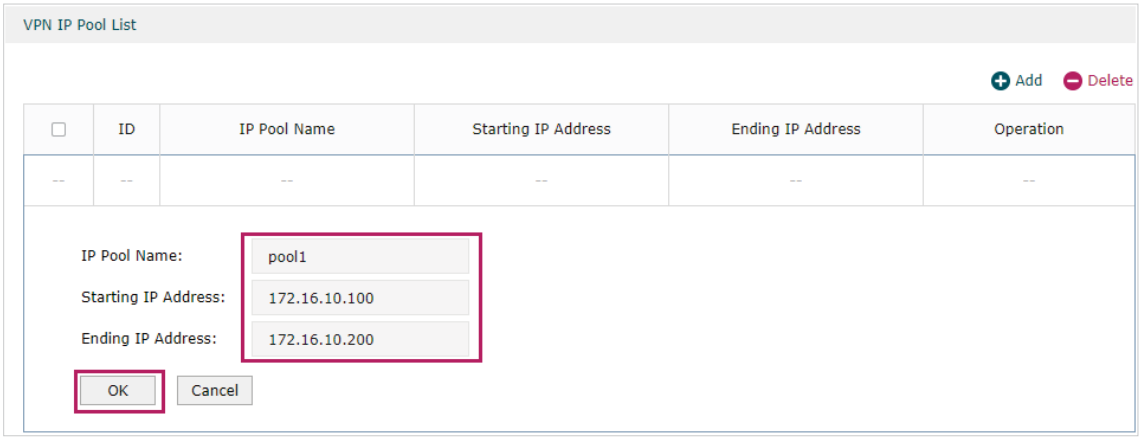
1) Configure L2TP VPN server.
2) Configure L2TP VPN client.
3) (Optional) Implement configuration for NAT devices.
4) Verify the connectivity of the L2TP VPN tunnel.

2.3.1 Configuring L2TP VPN Server

Select any one of the VPN routers as the VPN server. Here we select VPN Router B as the VPN server. Follow these steps to configure the L2TP VPN server.

1) Choose the menu **Preferences** > **VPN IP Pool** > **VPN IP Pool** and click **Add** to load the following page. Configure the parameters for the VPN IP pool. Click **OK**.

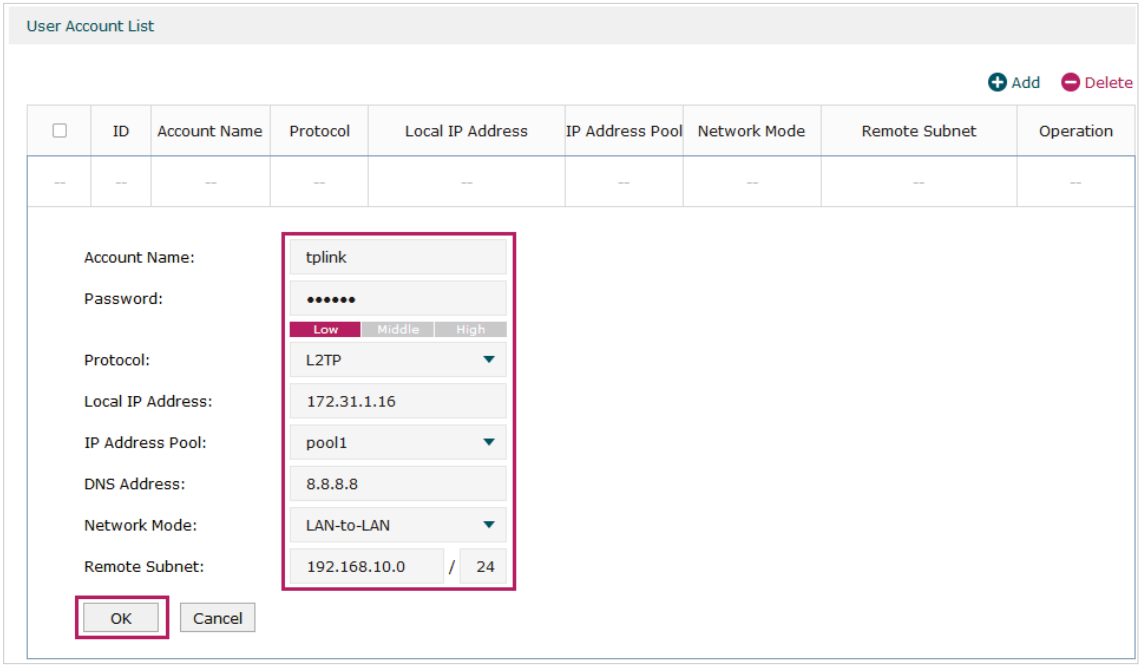
Figure 2-15 Configuring VPN IP Pool list



IP Pool Name	Specify the IP pool name as you like. Here we enter **pool1.**
Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address for the VPN IP pool. The VPN server will assign an IP address to the remote client when the tunnel is established. You can specify any reasonable IP address that will not cause conflict. Here we specify the starting IP address as **172.16.10.100** and the ending IP address as **172.16.10.200.**

2) Choose the menu **VPN** > **Users** > **Users** and click **Add** to load the following page. Configure the parameters for the user account. Click **OK**.

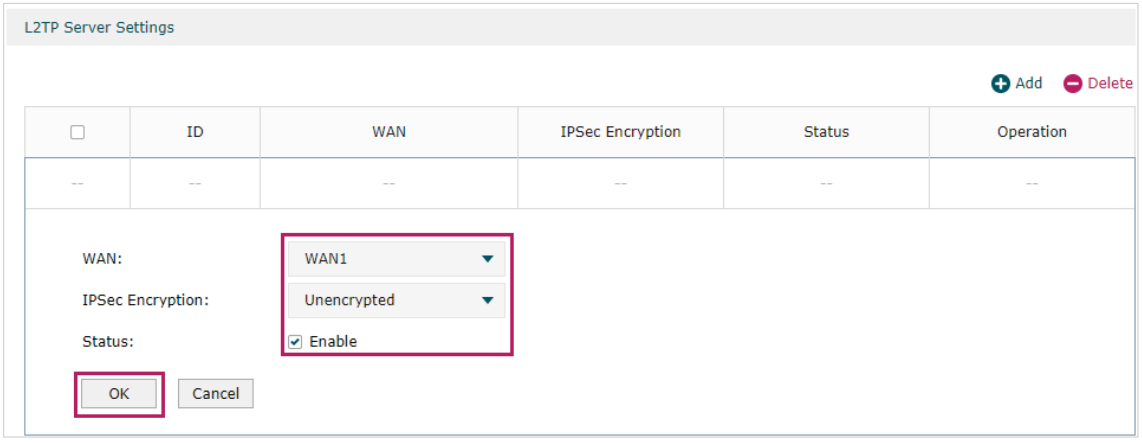
Figure 2-16 Configuring L2TP users



Account Name	Specify the account name as you like. Here we enter **tplink**.
Password	Specify the password as you like. Here we enter **123456**.
Protocol	Specify the protocol as **L2TP.**
Local IP Address	This is the virtual IP address which the remote client will set up a point-to-point connection with. You can specify any reasonable IP address that will not cause conflict. Here we specify the Local IP address as **172.31.1.16**.
IP Address Pool	Select **pool1** as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote client. Here we enter **8.8.8.8**.
Network Mode	Specify the network mode as **LAN-to-LAN**.
Remote Subnet	Specify the remote subnet as **192.168.10.0/24**. This should be the subnet address of the remote network.

3) Choose the menu **VPN** > **L2TP** > **L2TP Server** and click **Add** to load the following page. Configure the parameters for the L2TP server. Click **OK**.

Figure 2-17 Configuring L2TP server

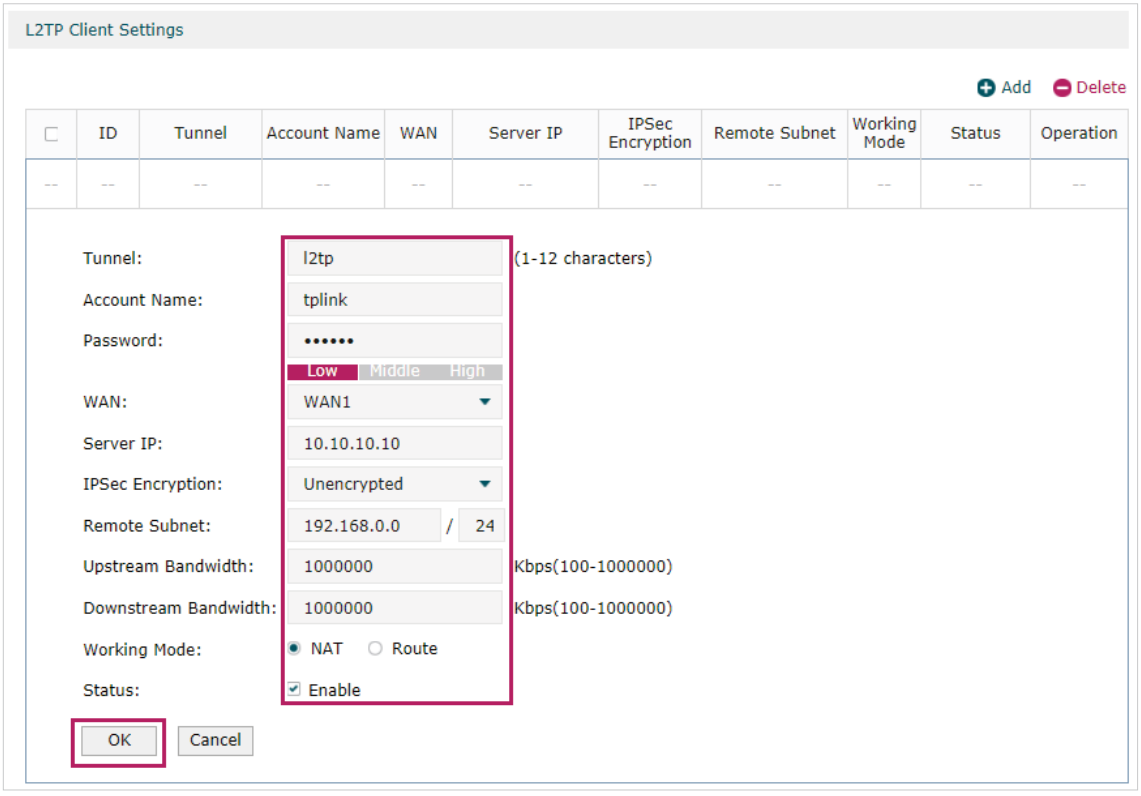


WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
IPsec Encryption	Specify the IPsec encryption according to your needs. Here we specify the IPsec encryption as **Unencrypted**.
Status	Enable the L2TP server.

2.3.2 Configuring L2TP VPN Client

Here we select the VPN Router A as the L2TP VPN client. For VPN Router A, choose the menu **VPN** > **L2TP** > **L2TP Client** and click **Add** to load the following page. Configure the parameters for the L2TP client. Click **OK**.

Figure 2-18 Configuring L2TP client



Tunnel	Specify the tunnel name as you like. Here we enter **l2tp**.
Account Name	Specify the account name as **tplink.** This should be kept the same as that of the L2TP server configuration.
Password	Specify the password as **123456.** This should be kept the same as that of the L2TP server configuration.
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Server IP	Specify the server IP as **10.10.10.10**.
IPSec Encryption	Specify IPSec encryption as **Unencrypted**. This should be kept the same as that of the L2TP server configuration.
Remote Subnet	Specify the remote subnet as **192.168.0.0/24**. This should be the subnet address of the remote network.
Upstream Bandwidth/ Downstream Bandwidth	Specify upstream and downstream limited rate in Kbps for L2TP tunnel. Here we keep the default configuration.

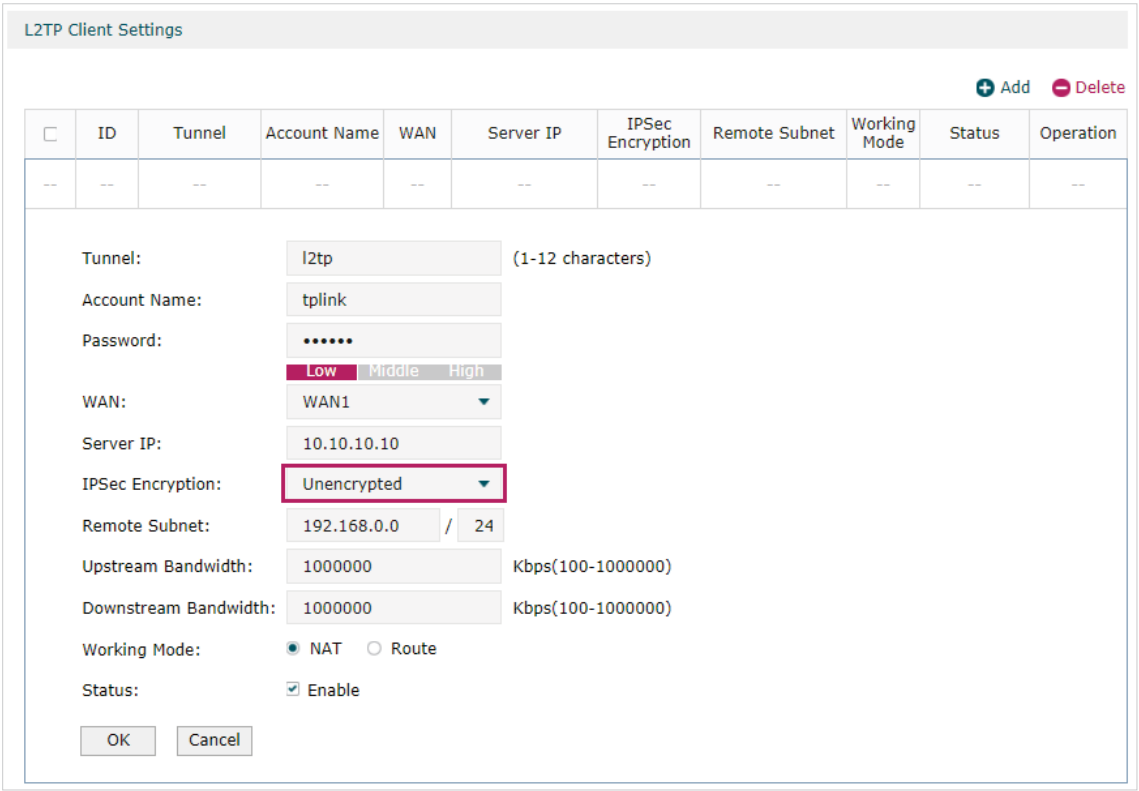
Working Mode	Specify the working mode as **NAT** or **Route** according to your needs. Here we specify the working mode as **NAT**. **NAT**: NAT mode allows the router to translate source IP address of L2TP packets to its WAN IP when forwarding L2TP packets. **Route**: Route mode allows the router to forward L2TP packets via routing protocol.
Status	Enable the L2TP client.

2.3.3 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 2-2. In this scenario, please verify the configuration on both VPN routers, and configure virtual servers on NAT Device B. The configuration steps are as follows:

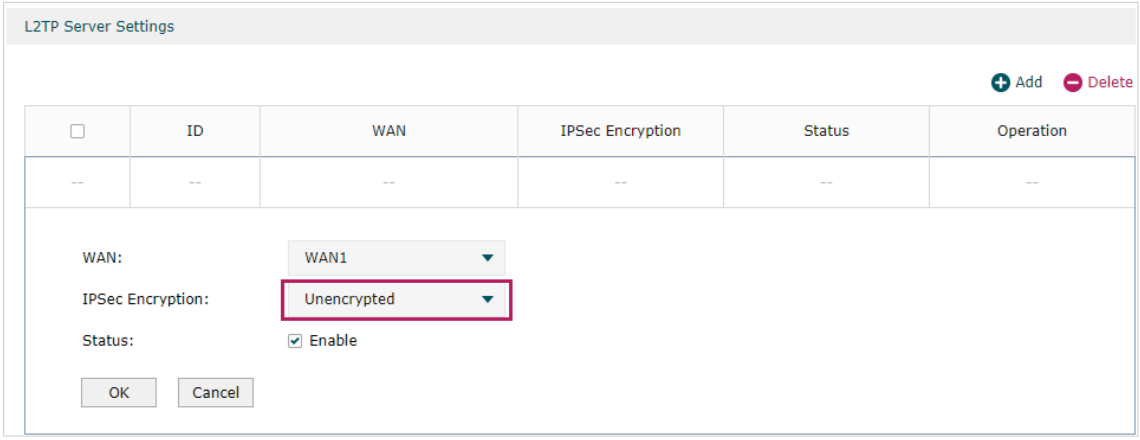
1) For VPN Router A, choose the menu **VPN** > **L2TP** > **L2TP Client**, select the L2TP client list entry which is previously created, and click to load the following page. Please make sure that the IPsec encryption is specified as **Unencrypted**. Otherwise, the VPN tunnel may fail to be established.

Figure 2-19 Verifying the L2TP client configuration



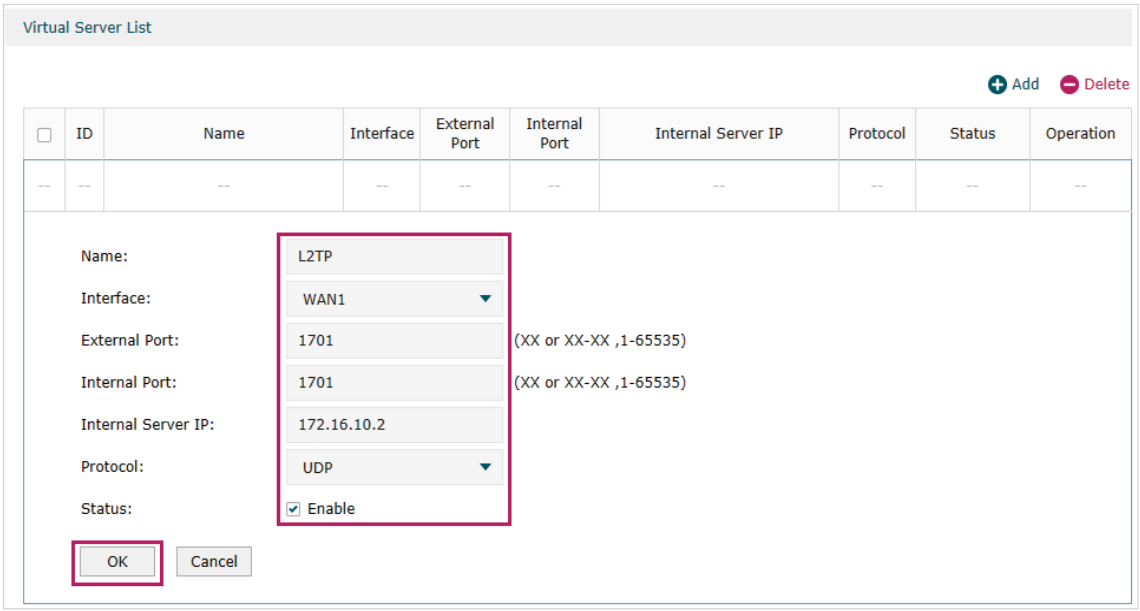
2) For VPN Router B, choose the menu **VPN** > **L2TP** > **L2TP Server**, select the L2TP server list entry which is previously created, and click to load the following page. Please make sure that the IPsec encryption is specified as **Unencrypted**. Otherwise, the VPN tunnel may fail to be established.

Figure 2-20 Verifying the L2TP server configuration



3) For NAT Device B, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page. Configure the parameters for the virtual server. Click **OK**.

Figure 2-21 Configuring virtual server for L2TP



Name	Specify the name for the virtual server list entry. Here we enter **L2TP**.
Interface	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the external port and internal port as **1701**.
Internal Server IP	Specify the internal server IP as **172.16.10.2.** This should be the WAN IP address of the VPN server.

Protocol	Specify the protocol as **UDP**.
Status	Enable the virtual server list entry.

2.3.4 Verifying the Connectivity of the L2TP VPN Tunnel

Choose the menu **VPN > L2TP > Tunnel List** to load the following page.

Figure 2-22 L2TP tunnel list

The tunnel list shows the information about the established VPN tunnel. Here, you can verify the connectivity of the L2TP VPN tunnel.

2.4 PPTP LAN-to-LAN VPN Configuration

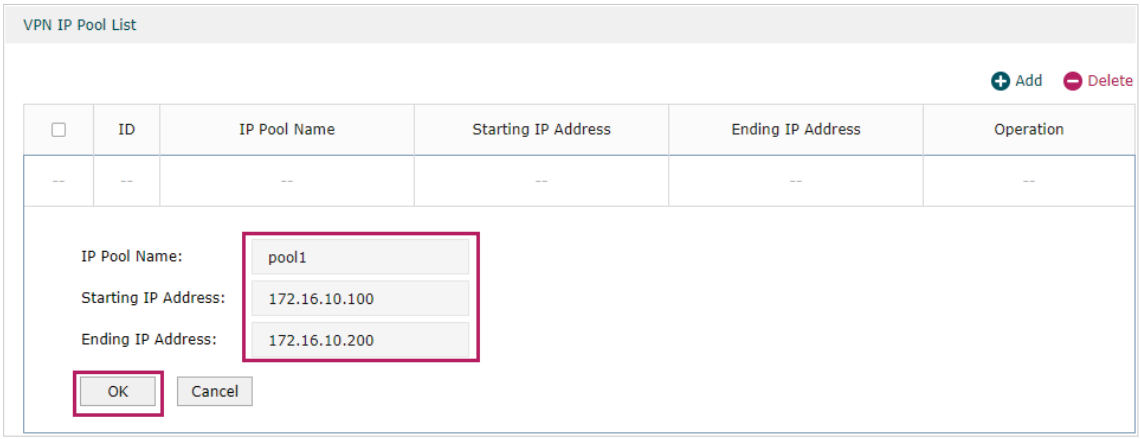
To configure the PPTP LAN-to-LAN VPN, follow these steps:

1) Configure PPTP VPN server.
2) Configure PPTP VPN client.
3) (Optional) Implement configuration for NAT devices.
4) Verify the connectivity of the PPTP VPN tunnel.

2.4.1 Configuring PPTP VPN Server

1) Choose the menu **Preferences > VPN IP Pool > VPN IP Pool** and click **Add** to load the following page. Configure the parameters for the VPN IP pool. Click **OK**.

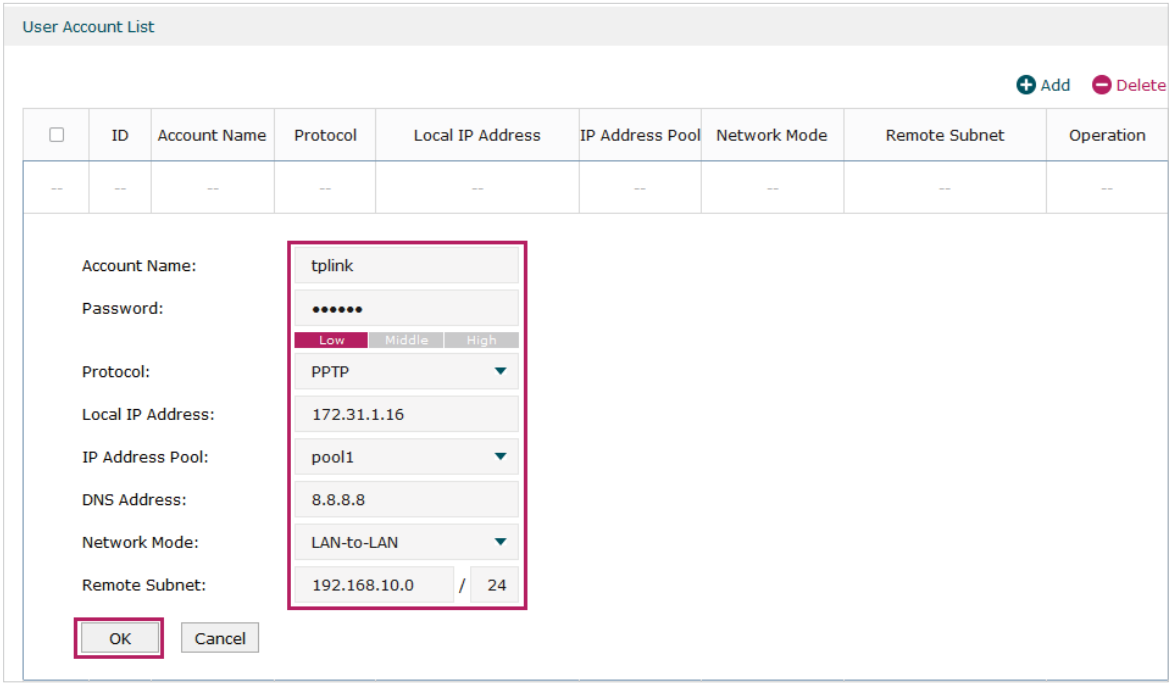
Figure 2-23 Configuring VPN IP pool list



IP Pool Name	Specify the IP pool name as you like. Here we enter **pool1.**
Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address for the VPN IP pool. The VPN server will assign an IP address to the remote client when the tunnel is established. You can specify any reasonable IP address that will not cause conflict. Here we specify the starting IP address as **172.16.10.100** and the ending IP address as **172.16.10.200.**

2) Choose the menu **VPN** > **Users** > **Users** and click **Add** to load the following page. Configure the parameters for the PPTP user account. Click **OK**.

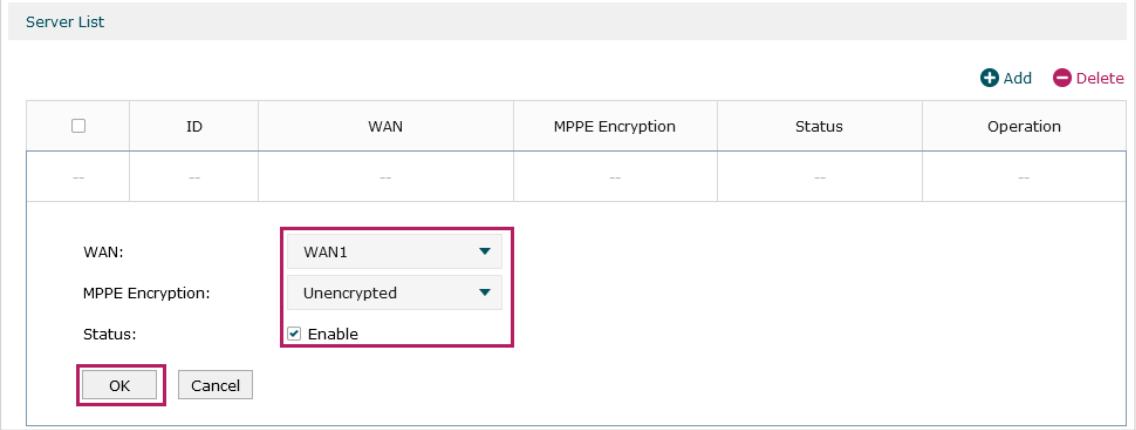
Figure 2-24 Configuring PPTP users



Account Name	Specify the account name as you like. Here we enter **tplink**.
Password	Specify the password as you like. Here we enter **123456**.
Protocol	Specify the protocol as **PPTP.**
Local IP Address	This is the virtual IP address the remote client will set up a point-to-point connection with. You can specify any reasonable IP Address that will not cause conflict. Here we specify the local IP address as **172.31.1.16**.
IP Address Pool	Select **pool1** as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote client. Here we enter **8.8.8.8**.
Network Mode	Specify the network mode as **LAN-to-LAN**.
Remote Subnet	Specify the remote subnet as **192.168.10.0/24**. This should be the subnet address of the remote network.

3) Choose the menu **VPN** > **PPTP** > **PPTP Server** and click **Add** to load the following page. Configure the parameters for the PPTP server. Click **OK**.

Figure 2-25 Configuring PPTP server

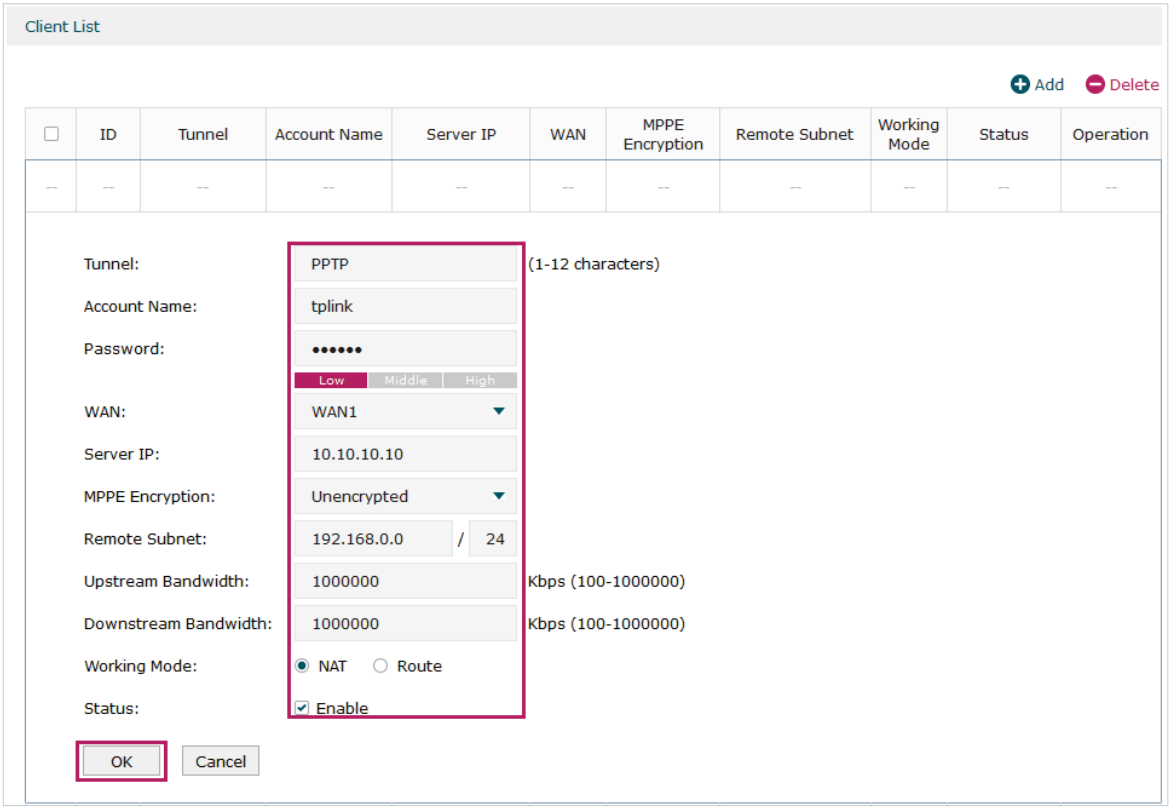


WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
MPPE Encryption	Specify the MPPE encryption according to your needs. Here we specify the MPPE encryption as **Unencrypted**.
Status	Enable the PPTP server.

2.4.2 Configuring PPTP VPN Client

Here we select the VPN Router A as PPTP VPN client. For VPN Router A, choose the menu **VPN** >**PPTP**> **PPTP Client** and click **Add** to load the following page. Configure the parameters for PPTP client. Click **OK**.

Figure 2-26 Configuring PPTP client



Tunnel	Specify the tunnel name as you like. Here we enter **PPTP**.
Account Name	Specify the account name as **tplink.** This should be kept the same as that of the PPTP server configuration.
Password	Specify the password as **123456.** This should be kept the same as that of the PPTP server configuration.
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Server IP	Specify the server IP as **10.10.10.10**.
MPPE Encryption	Specify MPPE encryption as **Unencrypted**. This should be kept the same as that of the PPTP server configuration.
Remote Subnet	Specify the remote subnet as **192.168.0.0/24**. This should be the subnet address of the remote network.
Upstream Bandwidth/ Downstream Bandwidth	Specify upstream and downstream limited rate in Kbps for PPTP tunnel. Here we keep the default configuration.

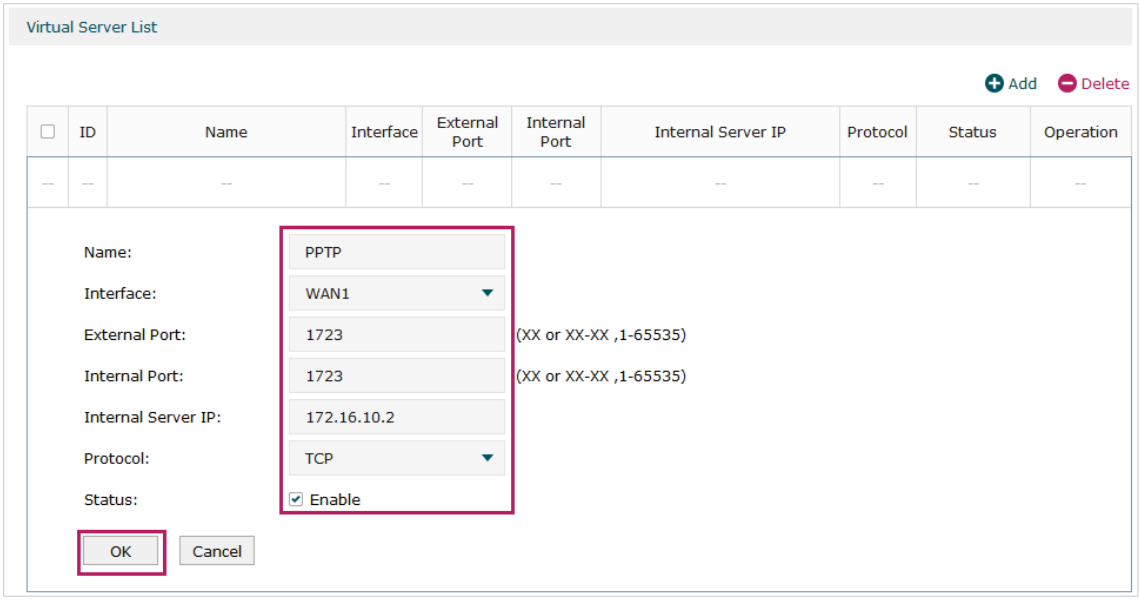
Working Mode	Specify the working mode as NAT or Route according to your needs. Here we specify the working mode as **NAT**. **NAT**: NAT mode allows the router to translate source IP address of PPTP packets to its WAN IP when forwarding PPTP packets. **Route**: Route mode allows the router to forward PPTP packets via routing protocol.
Status	Enable the PPTP client.

2.4.3 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 2-2. In this scenario, please configure virtual servers on NAT Device B, and configure PPTP ALG on both NAT devices. The configuration steps are as follows:

1) For NAT Device B, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page. Configure the parameters for virtual server. Click **OK**.

Figure 2-27 Configuring virtual server for PPTP

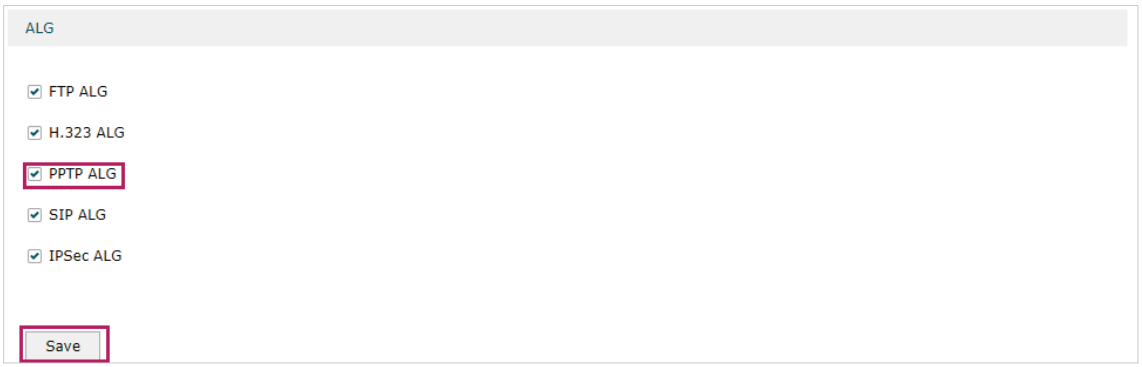


Name	Specify the name for the virtual server list entry. Here we enter **PPTP**.
Interface	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the External Port and Internal Port as **1723**.
Internal Server IP	Specify the Internal Server IP as **172.16.10.2.** This should be the WAN IP address of the VPN server.
Protocol	Specify the protocol as **TCP**.

Status	Enable the virtual server list entry.

2) For NAT Device A and NAT Device B, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable the PPTP ALG, and click **Save**.

Figure 2-28 Configuring PPTP ALG



2.4.4 Verifying the Connectivity of the PPTP VPN Tunnel

Choose the menu **VPN** > **PPTP** > **Tunnel List** to load the following page.

Figure 2-29 PPTP tunnel list

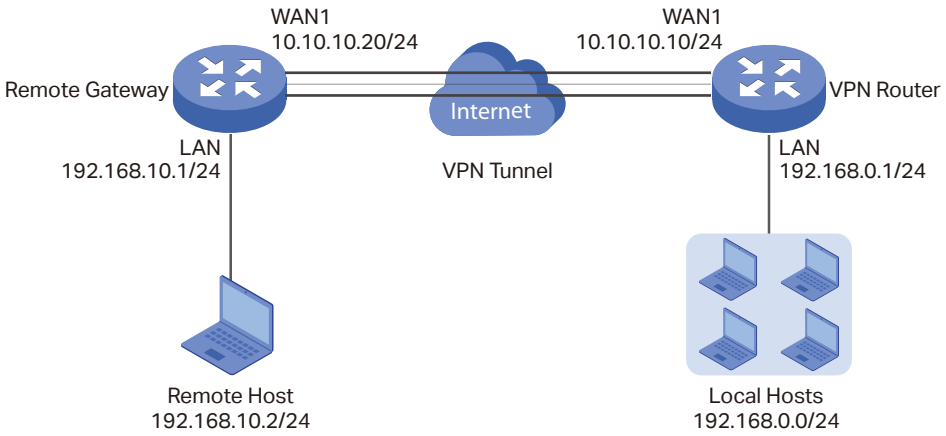
The tunnel list shows the information about the established VPN tunnel. Here, you can verify the connectivity of the PPTP VPN Tunnel.

3 Client-to-LAN VPN Configuration

3.1 Network Topology

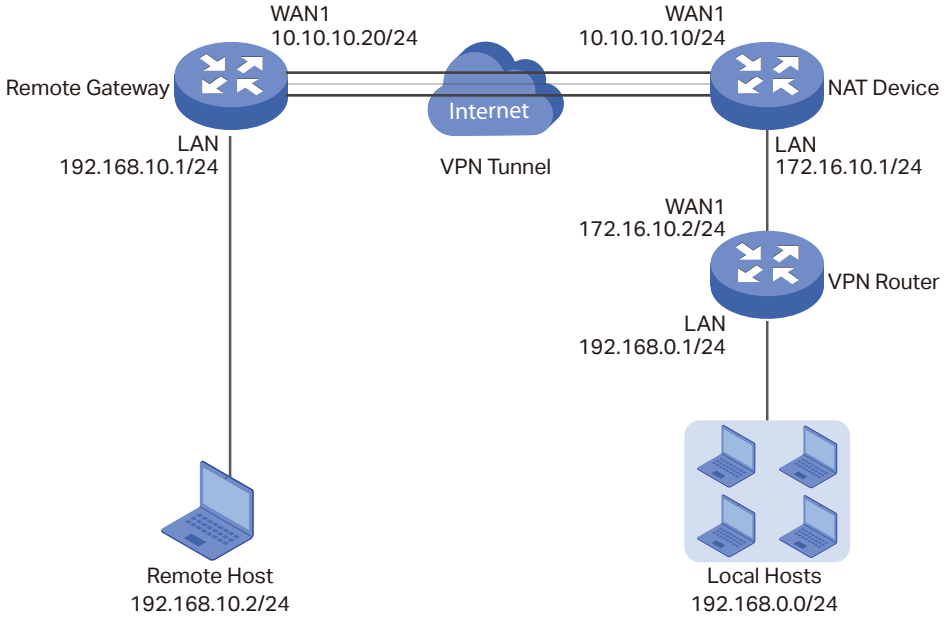
Client-to-LAN VPN is deployed when a remote host is provided with secure access to the local hosts. For example, an employee on business needs to access the private network of his company securely via the internet. The following figure shows the typical network topology.

Figure 3-1 Client-to-LAN VPN



In actual network environments, NAT devices may exist in front of the VPN router. The following figure shows the network topology in this scenario.

Figure 3-2 Client-to-LAN VPN with NAT



Client-to-LAN VPN can be established via three methods, including IPsec Client-to-LAN VPN, PPTP Client-to-LAN VPN, and L2TP Client-to-LAN VPN. To establish an IPsec

Client-to-LAN VPN, it is recommended to use a 3rd-party IPsec VPN client software, such as TheGreenBow VPN client software, whereas to establish a PPTP or L2TP Client-to-LAN VPN, you can use the built-in client software of the operating system. The topology shown in Figure 3-1 is used as an example, with TL-ER6120 used as the VPN router for demonstration purposes. Configuration instructions for the three methods are given below.

3.2 IPsec Client-to-LAN VPN Configuration

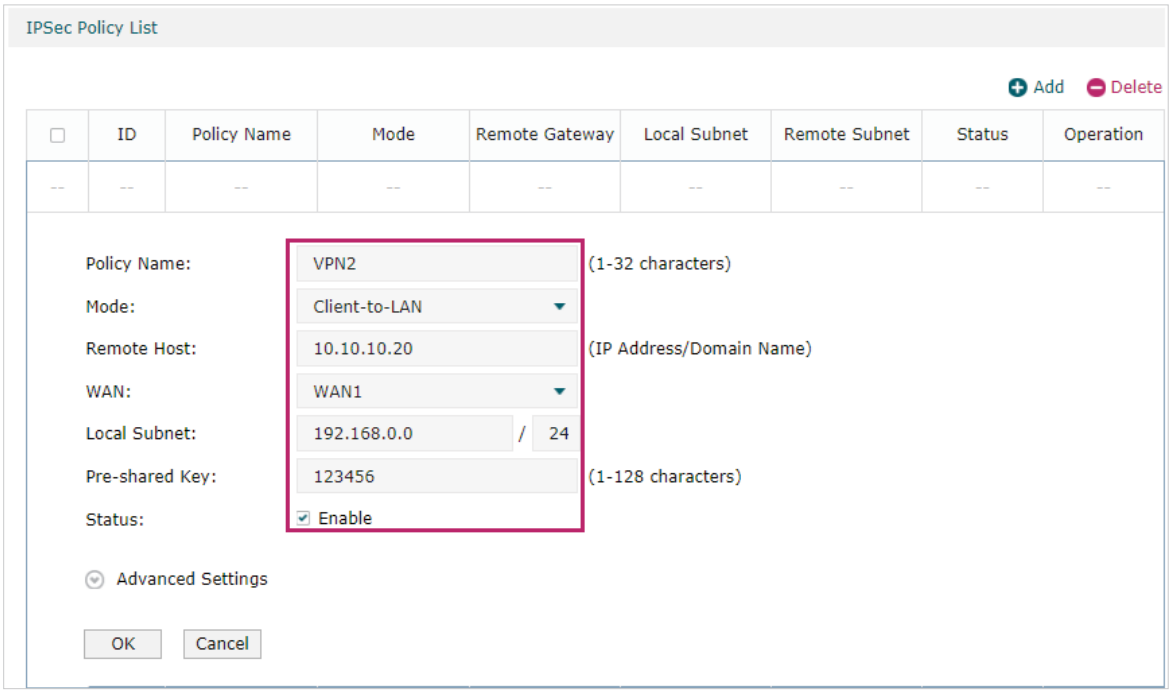
To complete the IPsec Client-to-LAN VPN, follow these steps:

1) Configure IPsec VPN server.
2) (Optional) Implement configuration for NAT devices.
3) Configure the IPsec VPN client software.
4) Verify the connectivity of the IPsec VPN tunnel.

3.2.1 Configuring IPsec VPN Server.

1) Choose the menu **VPN > IPSec >IPSec Policy** and click **Add** to load the following page on the VPN router. Configure the basic parameters for the IPsec policy.

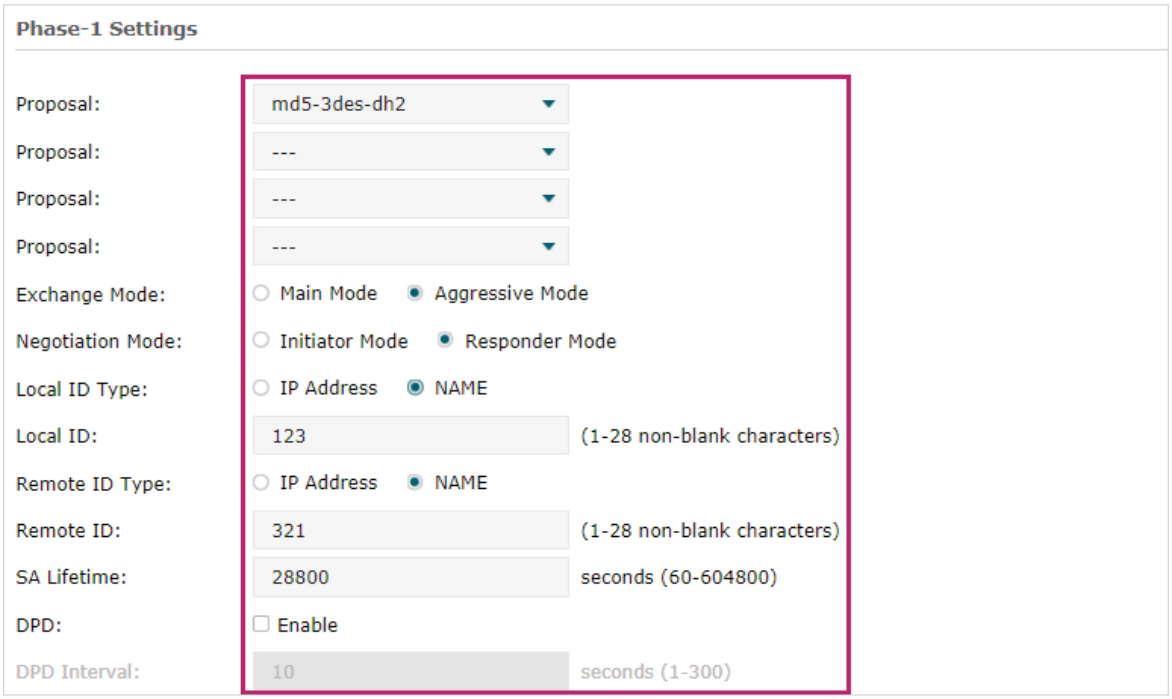
Figure 3-3 Configuring the IPsec policy



Policy Name	Specify the name of IPsec policy. Here we enter **VPN2**.
Mode	Specify the mode as **Client-to-LAN.**
Remote Host	Specify the remote host as **10.10.10.20**. This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as **192.168.0.0/24**. This should be the subnet address of the local network.
Pre-shared key	Specify the pre-shared key as you like. Here we enter **123456**.
Status	Enable the IPsec policy list entry.

2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Figure 3-4 Configuring the IKE phase-1 parameters

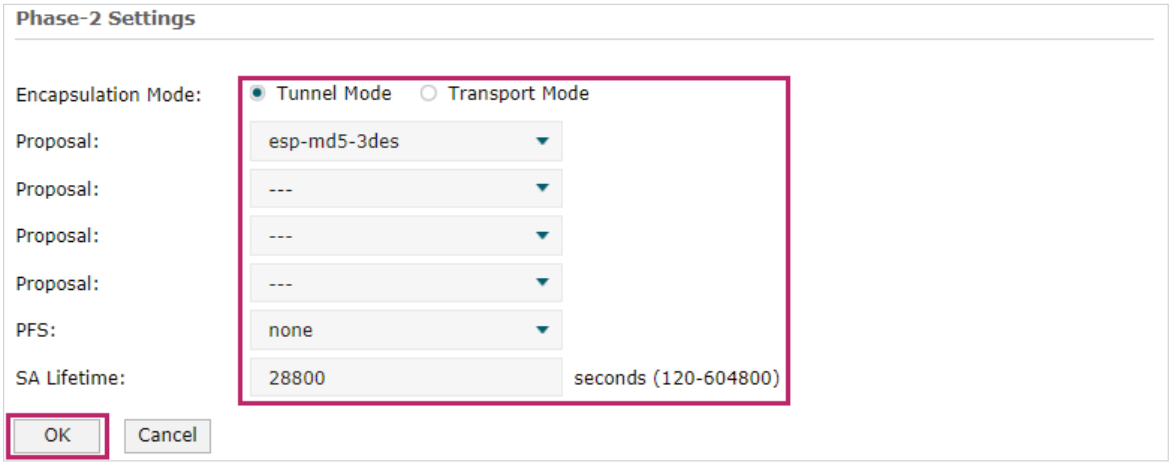


Proposal	Select the proposal from the drop-down list. Here we select **md5-3des-dh2**.
Exchange Mode	Specify the exchange mode according to your needs. Here we Specify the exchange mode as **Aggressive Mode**.
Negotiation Mode	Specify the negotiation mode as **Responder Mode.**
Local ID Type/ Remote ID Type	Specify the local ID type and remote ID type as you like. Here we specify the local ID type and remote ID type as **NAME**.

Local ID/ Remote ID	Specify the local ID and remote ID as you like. Here we specify the local ID as **123** and remote ID as **321.**
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.
DPD	Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

3) In the **Phase-2 Settings** section, configure the IKE phase-2 parameters for the IPsec policy. Click **OK**.

Figure 3-5 Configuring the IKE phase-2 parameters



Encapsulation Mode	Specify the encapsulation mode as **Tunnel Mode**.
Proposal	Select the proposal from the drop-down list. Here we select **esp-md5-3des**.
PFS	Select the PFS from the drop-down list according to your needs. Here we select **none**.
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.

3.2.2 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 3-2. In this scenario, please verify the configuration on the VPN router, configure virtual servers on the NAT device, and configure IPsec ALG on both the remote gateway and the NAT device. The configuration steps are as follows:

1) For the VPN router, choose the menu **VPN** > **IPSec** > **IPSec Policy,** select the IPsec policy list entry which is previously created, and click to load the following page. Please make sure that in the **Phase-1 Settings** section, the local ID type and remote ID type are both specified as **NAME**, and in the **Phase-2 Settings** section, the proposal is **not** specified as **ah-md5** or **ah-sha1**. Otherwise, the VPN tunnel may fail to be established.

Figure 3-6 Verifying the phase-1 configuration

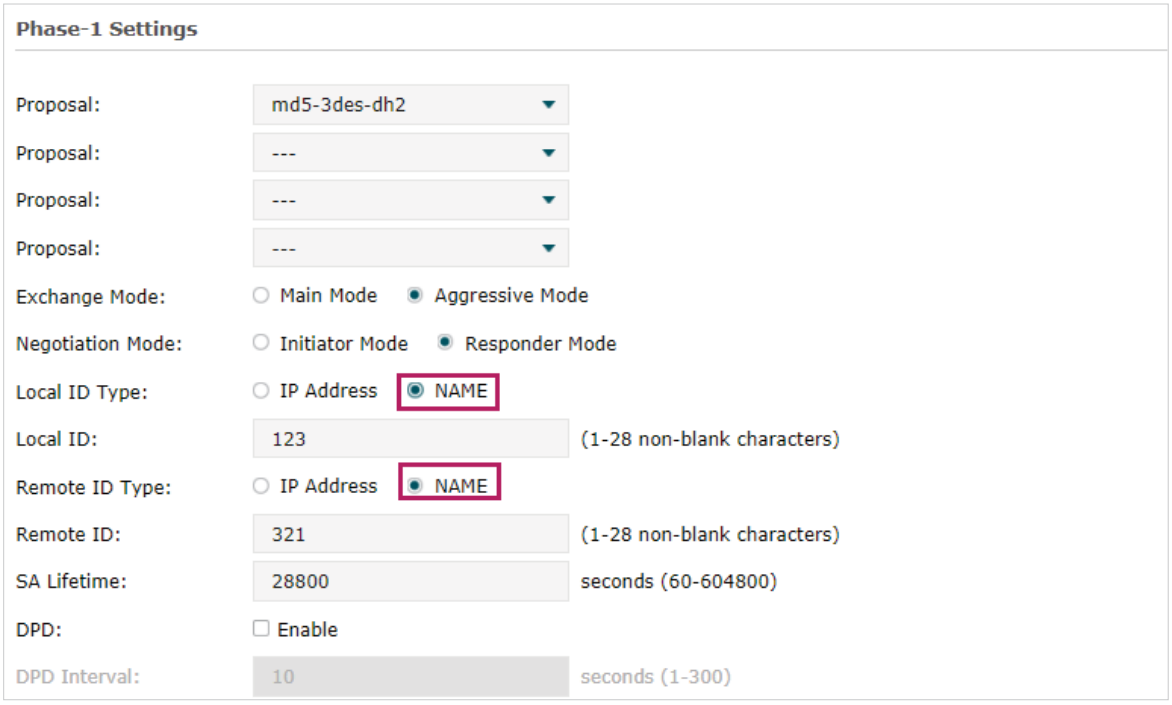
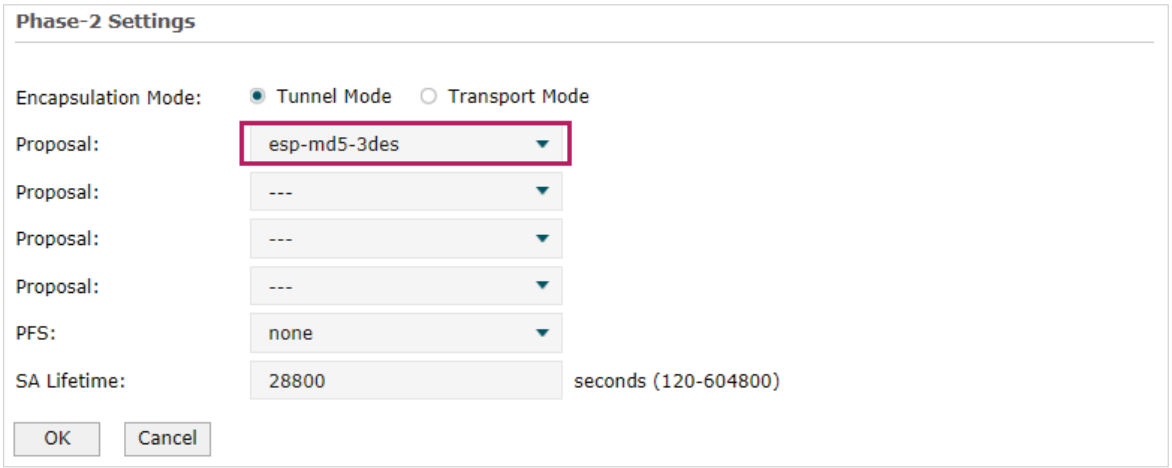
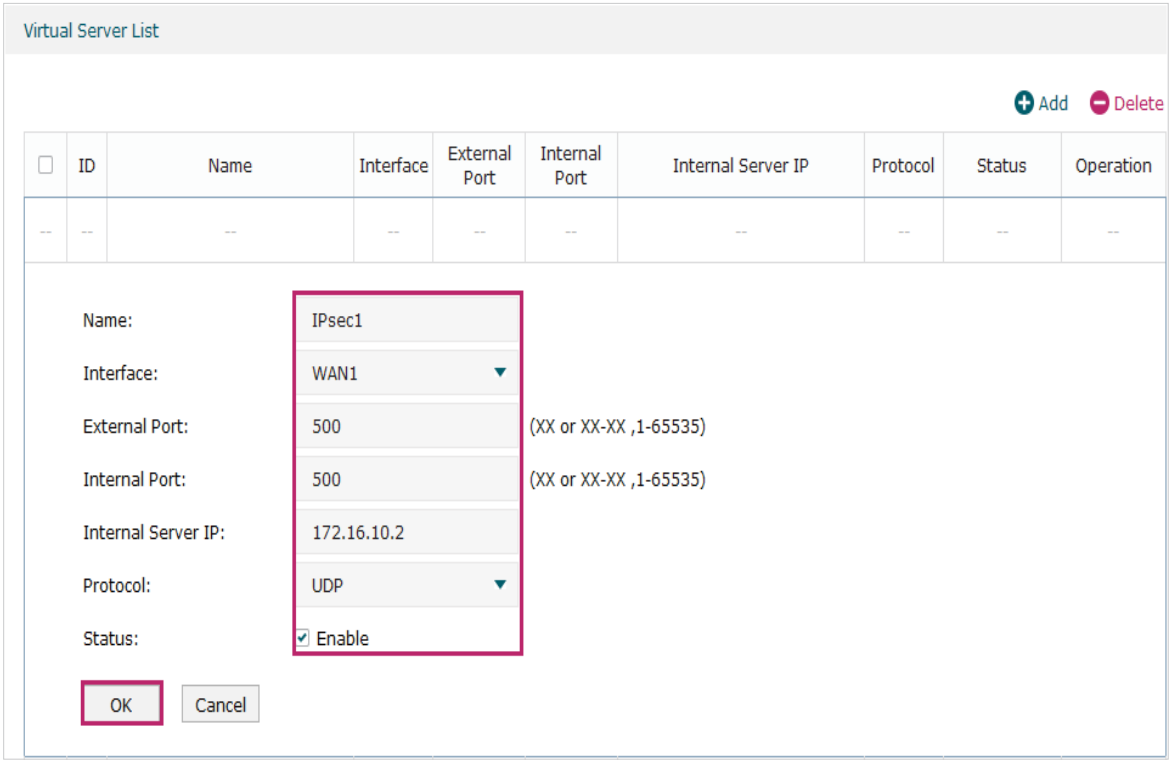


Figure 3-7 Verifying the phase-2 configuration



2) For the NAT device, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page. Configure the parameters for the virtual server. Click **OK**.

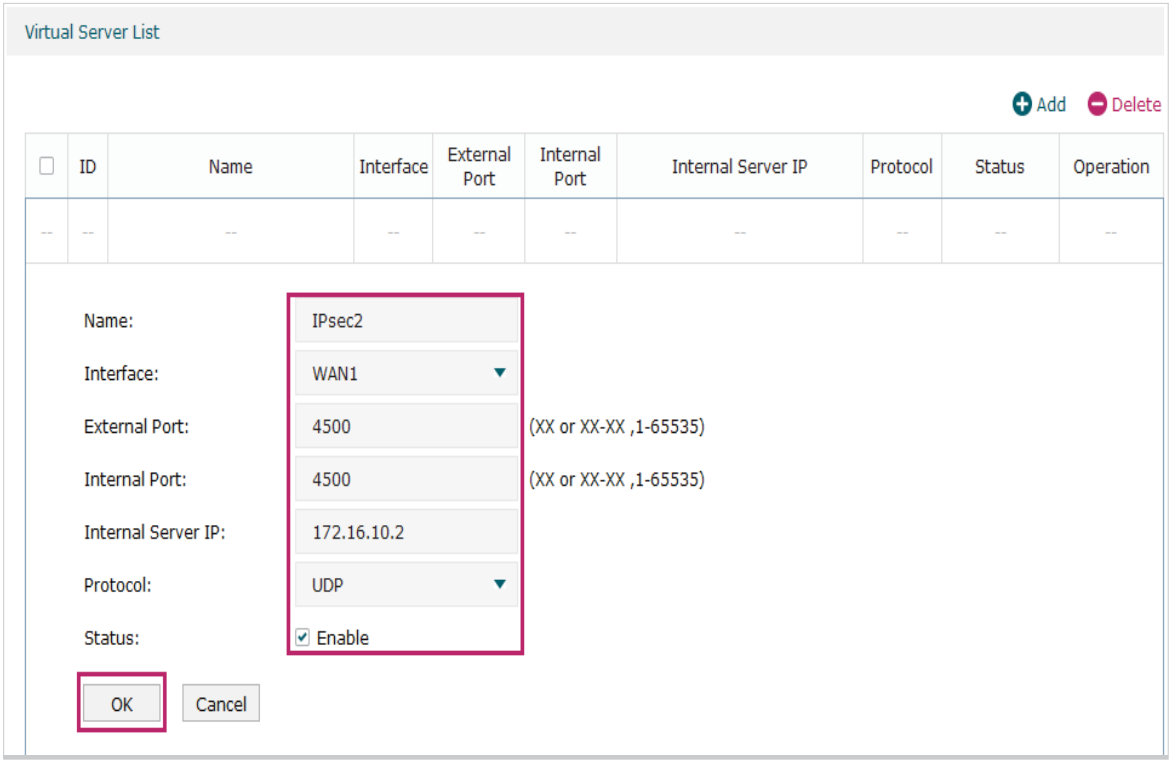
Figure 3-8 Configuring virtual server for IPsec



Name	Specify the name for the virtual server list entry. Here we enter **IPsec1**.
Interface	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the external port and internal port as **500**.
Internal Server IP	Specify the internal server IP as **172.16.10.2.** This should be the WAN IP address of the VPN server.
Protocol	Specify the protocol as **UDP**.
Status	Enable the virtual server list entry.

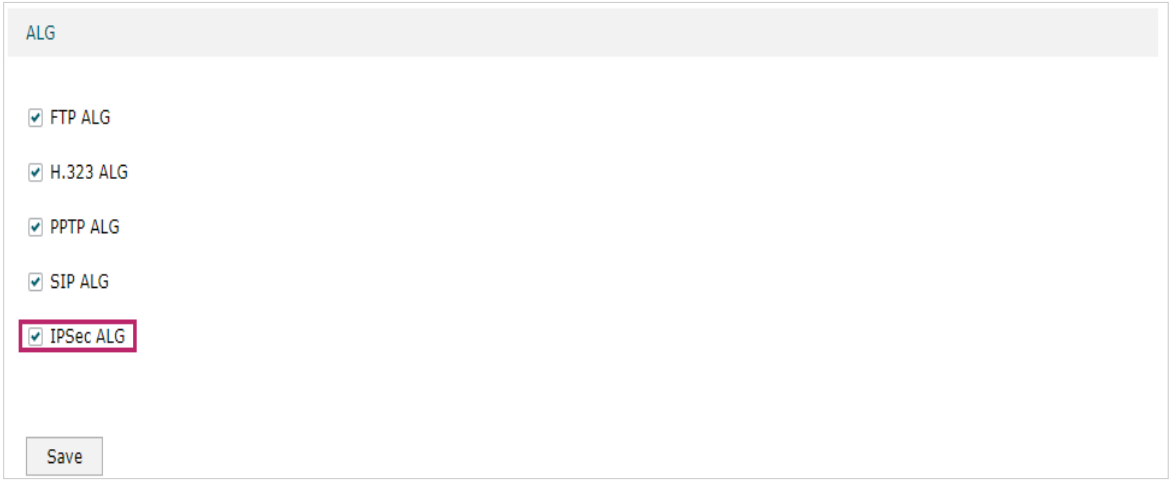
Similarly, add another virtual server list entry with the name IPsec2, and set the external and internal port as 4500.

Figure 3-9 Configuring virtual server for IPsec



3) For the remote gateway and the NAT device, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable IPsec ALG, and click **Save**.

Figure 3-10 Configuring IPsec ALG



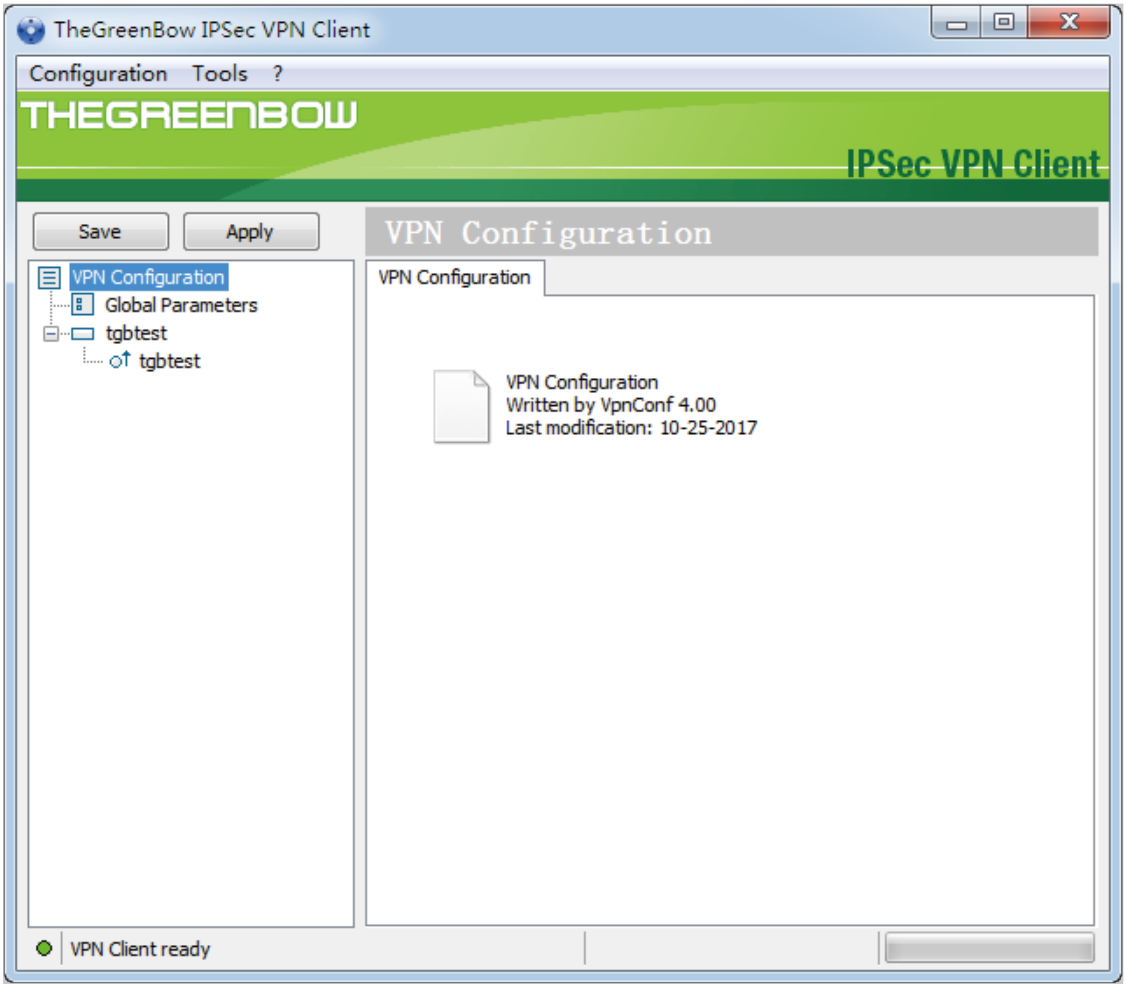
3.2.3 Configuring the IPsec VPN Client Software

There are many 3rd-party IPsec VPN client softwares. With any one of them launched on the remote host, you can set up an IPsec Client-to-LAN VPN tunnel with the VPN router successfully. Here we take TheGreenBow VPN client software for example. Follow these steps to configure TheGreenBow VPN client software.

1) Go to the website http://www.tp-link.com/en/download/TL-ER6120_V1.html to download TheGreenBow VPN client software. Then install and launch the client software.

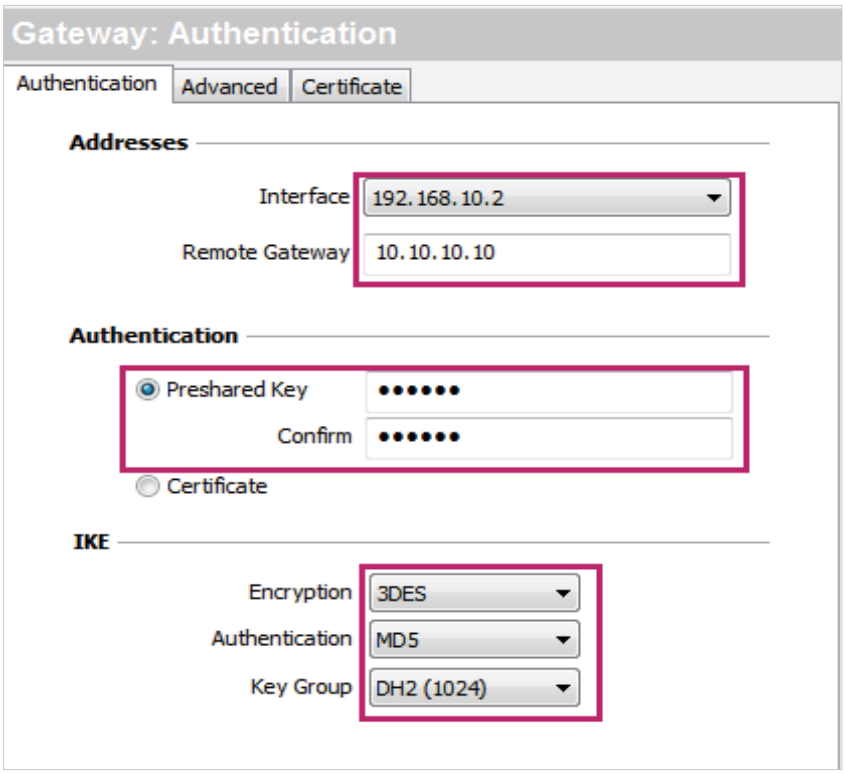
2) Click the client icon in the toolbar on the bottom of your desktop to load the following page.

Figure 3-11 Configuring TheGreenBow IPSec VPN client



3) Right click **VPN Configuration**, click **New Phase 1** and then choose the menu **Gateway > Authentication** to load the following page. Configure the parameters for the IPsec policy.

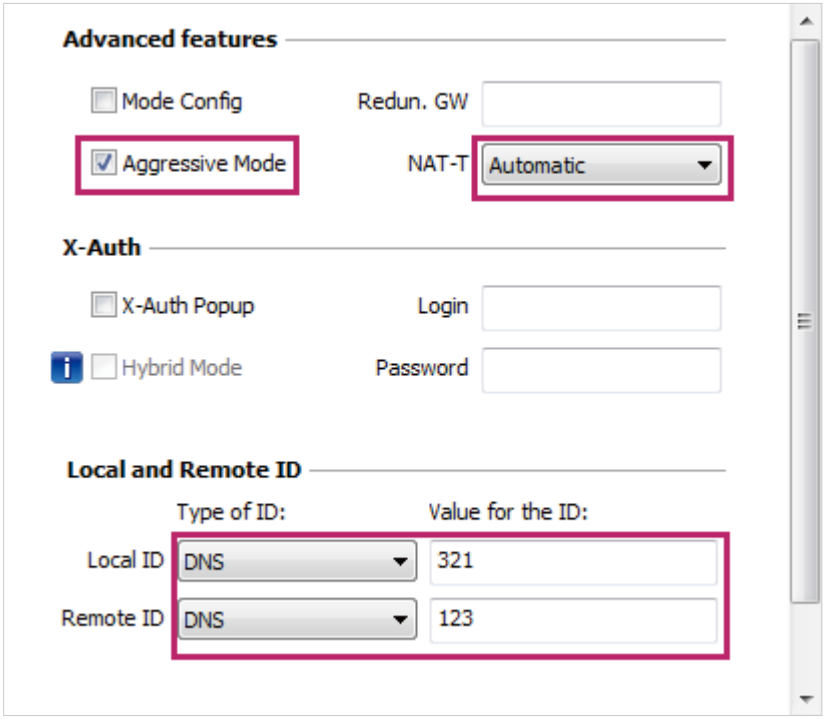
Figure 3-12 Configuring TheGreenBow IPSec VPN client



Interface	Select **192.168.10.2** as the Interface from the drop-down list. This should be the IP address of the remote host.
Remote Gateway	Specify the remote gateway as **10.10.10.10**. This should be the IP address of the other end of the VPN tunnel.
Preshared Key	Specify the preshared key as **123456**. This should be the same as the VPN server configuration. Then confirm the preshared key by inputting it again in **Confirm**.
Encryption/ Authentication/ Key Group	Specify encryption as **3DES**, authentication as **MD5**, Key Group as **DH2 (1024)**. This should be kept the same as the VPN server configuration.

4) Choose the menu **Gateway > Advanced** to load the following page. Configure the parameters for the IPsec policy.

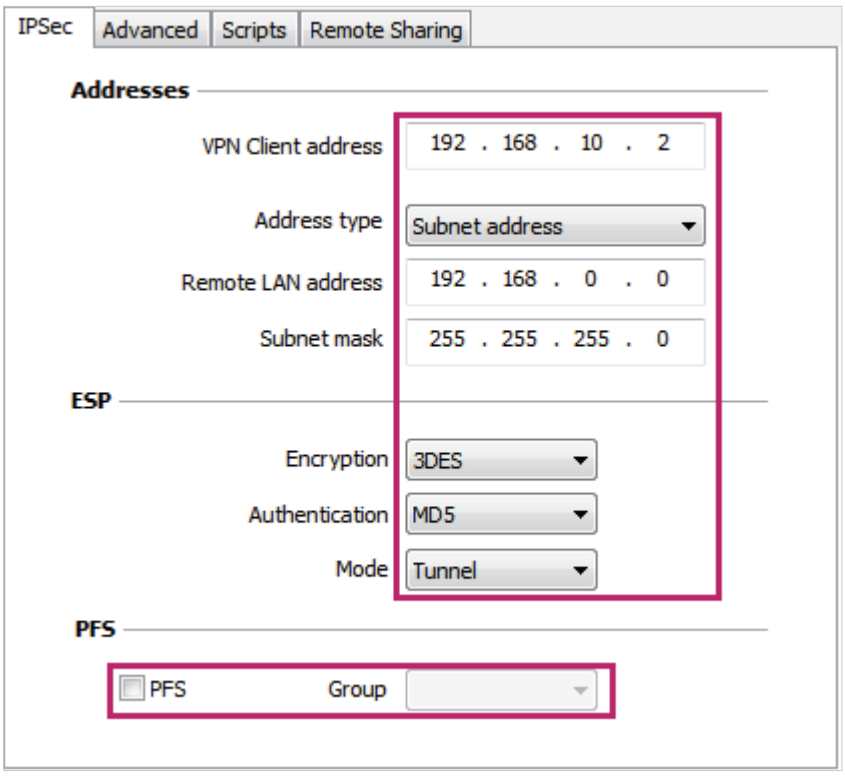
Figure 3-13 Configuring TheGreenBow IPSec VPN client



Aggressive Mode	Check **aggressive mode**. This should be kept the same as the VPN server configuration.
NAT-T	Select **Automatic** as NAT-T from the drop-down list.
Local ID/ Remote ID	Specify type of local ID and remote ID as **DNS**. Specify the local ID as **321** and the remote ID as **123**. This should be reversed in comparison to the VPN server configuration.

5) Right click **Gateway** and click **New Phase 2**. Choose the menu **Tunnel > IPSec** to load the following page. Configure the parameters for the IPsec policy.

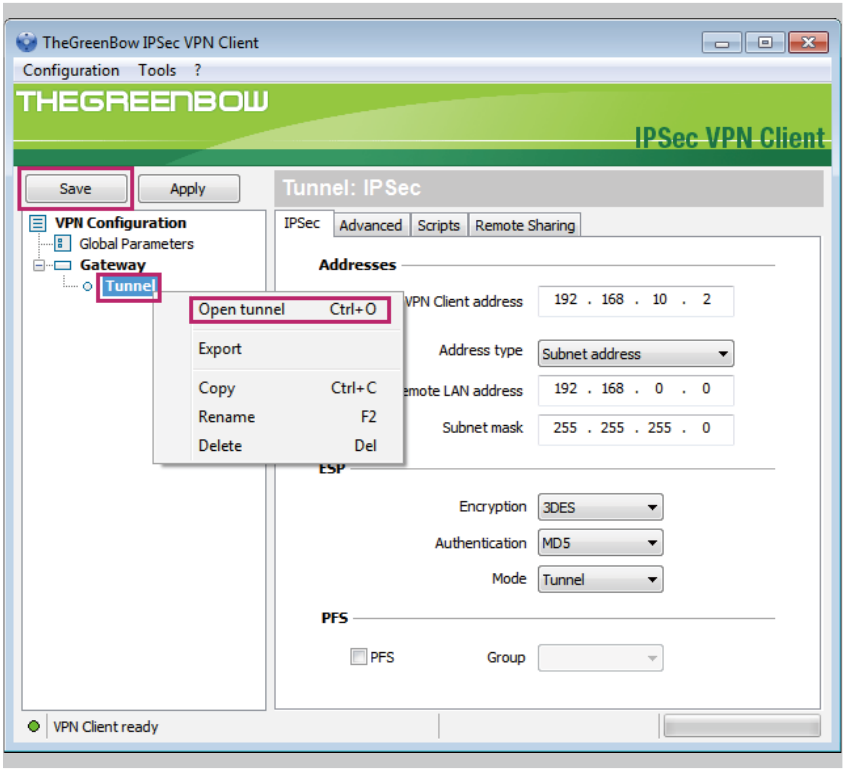
Figure 3-14 Configuring TheGreenBow IPSec VPN client



VPN Client Address	Specify the VPN client address as **192.168.10.2** . This should be the IP address of the remote host.
Address Type	Select **subnet address** as the address type from the drop-down list.
Remote LAN Address/ Subnet Mask	Specify the remote LAN address as **192.168.0.0** and subnet mask as **255.255.255.0**. This should be the IP address and subnet mask of the local hosts.
Encryption/ Authentication/ Mode	Specify encryption as **3DES**, authentication as **MD5**, mode as **Tunnel**. This should be kept the same as the VPN server configuration.
PFS	Uncheck the PFS. This should be kept the same as the VPN server configuration.

6) Click **Save.** Right click **Tunnel** and then click **Open tunnel** on the following page to establish the IPsec VPN tunnel.

Figure 3-15 Configuring TheGreenBow IPSec VPN client



3.2.4 Verifying the Connectivity of the IPsec VPN Tunnel

Choose the menu **VPN > IPsec > IPsec SA** to load the following page.

Figure 3-16 IPSec SA list

IPSec SA List

Entry Count: 2 Refresh

ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
1	VPN2	3485457663	in	10.10.10.10<--10.10.10.20	192.168.0.0/24 <-- 192.168.10.2/32	ESP	--	MD5	3DES
2	VPN2	1164488972	out	10.10.10.10-->10.10.10.20	192.168.0.0/24 --> 192.168.10.2/32	ESP	--	MD5	3DES

The IPsec SA list shows the information about the established IPsec VPN tunnel. Here, you can verify the connectivity of the IPsec VPN tunnel.

3.3 L2TP Client-to-LAN VPN Configuration

To configure the L2TP Client-to-LAN VPN, follow these steps:

1) Configure L2TP VPN server.
2) (Optional) Implement configuration for NAT devices.

3) Configure the L2TP VPN client software.

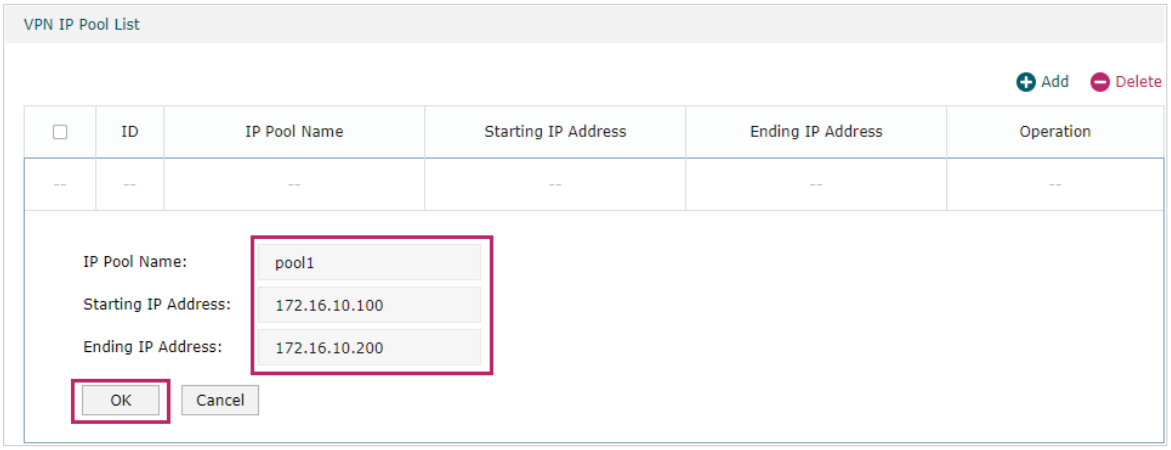
4) Verify the connectivity of the L2TP VPN tunnel.

5) (Optional) Configure access to the internet via proxy gateway.

3.3.1 Configuring L2TP VPN Server

1) Choose the menu **Preferences > VPN IP Pool > VPN IP Pool** and click **Add** to load the following page on the VPN router. Configure the parameters for the VPN IP pool. Click **OK**.

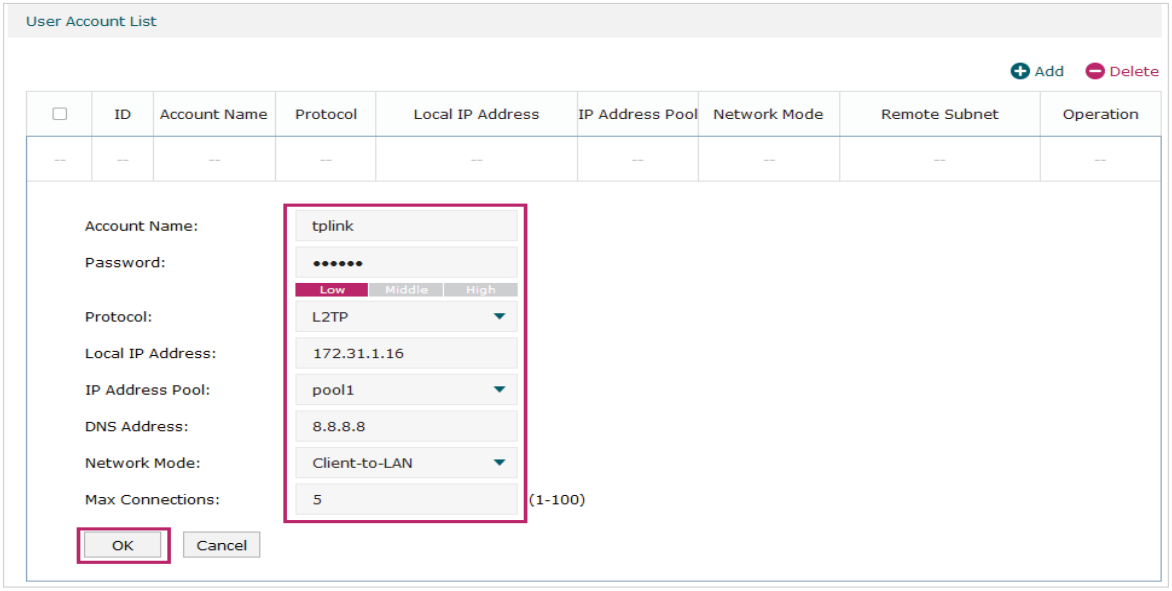
Figure 3-17 Configuring VPN IP pool list



IP Pool Name	Specify the IP pool name as you like. Here we enter **pool1.**
Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address for the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause conflict. Here we specify the starting IP address as **172.16.10.100** and the ending IP address as **172.16.10.200.**

2) Choose the menu **VPN > Users > Users** and click **Add** to load the following page. Configure the parameters for the L2TP user account. Click **OK**.

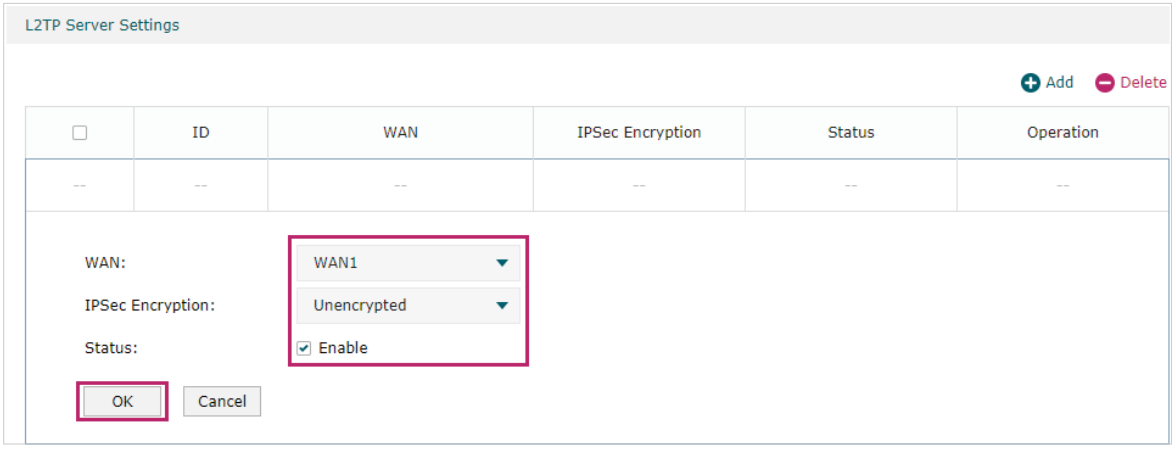
Figure 3-18 Configuring L2TP users



Account Name	Specify the account name as you like. Here we enter **tplink**.
Password	Specify the password as you like. Here we enter **123456**.
Protocol	Specify the Protocol as **L2TP.**
Local IP Address	This is the virtual IP address which the remote host will set up a point-to-point connection with. You can specify any reasonable IP address that will not cause conflict. Here we specify the Local IP Address as **172.31.1.16**.
IP Address Pool	Select **pool1** as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote host. Here we enter **8.8.8.8**.
Network Mode	Specify the network mode as **Client-to-LAN**.
Max Connections	Specify the max connections according to your needs. Here we specify max connections as 5.

3) Choose the menu **VPN > L2TP > L2TP Server** and click **Add** to load the following page. Configure the parameters for the L2TP server. Click **OK**.

Figure 3-19 Configuring L2TP server



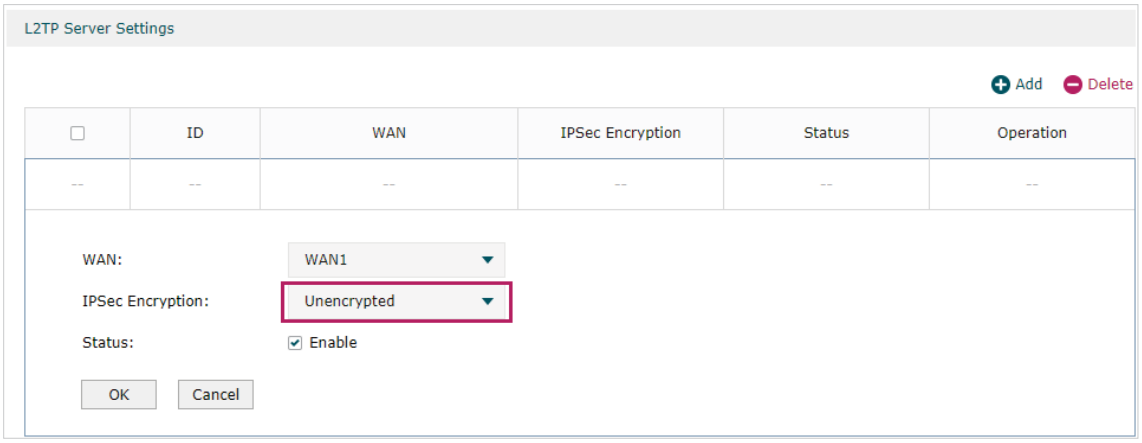
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
IPsec Encryption	Specify the IPsec encryption according to your needs. Here we specify the IPsec encryption as **Unencrypted**.
Status	Enable the L2TP server.

3.3.2 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in **Figure 3-2**. In this scenario, please verify the configuration on the VPN router, and configure virtual servers on the NAT device. The configuration steps are as follows:

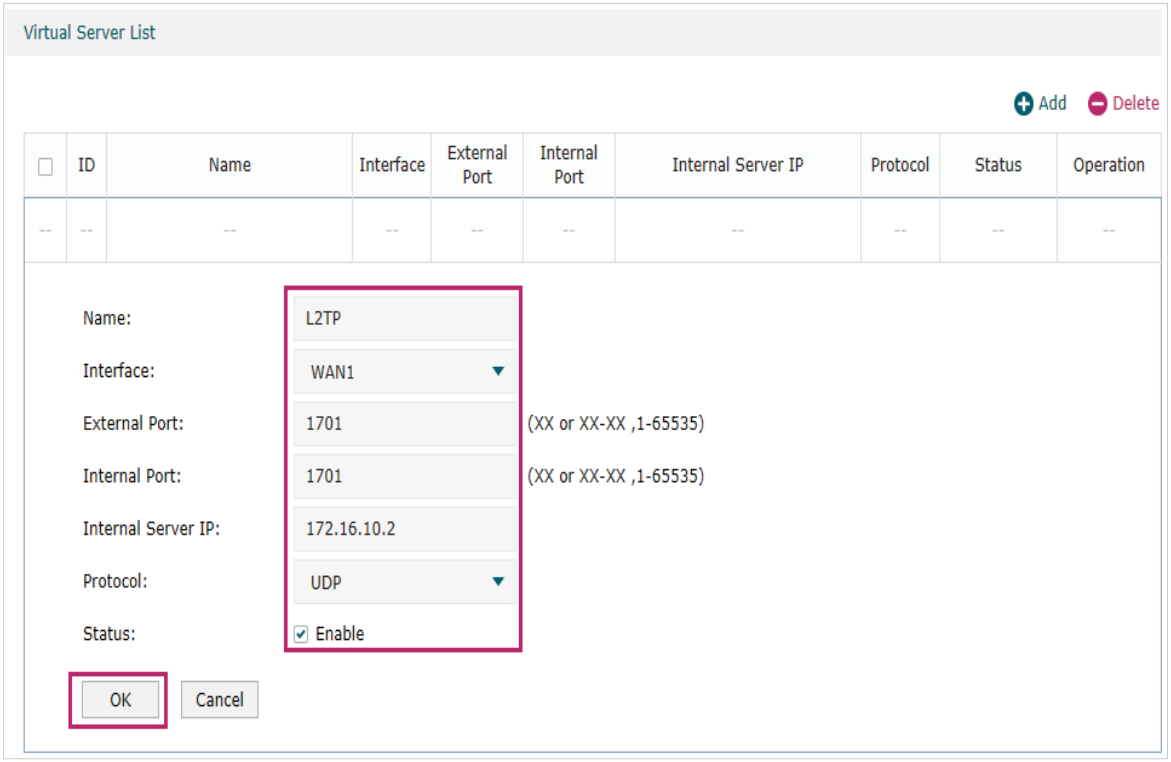
1) For the VPN router, choose the menu **VPN** > **L2TP** > **L2TP Server**, select the L2TP server list entry which is previously created, and click to load the following page. Please make sure that the IPsec encryption is specified as **Unencrypted**. Otherwise, the VPN tunnel may fail to be established.

Figure 3-20 Verifying the L2TP server configuration



2) For the NAT device, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page . Configure the parameters for the virtual server. Click **OK**.

Figure 3-21 Configuring virtual server for L2TP



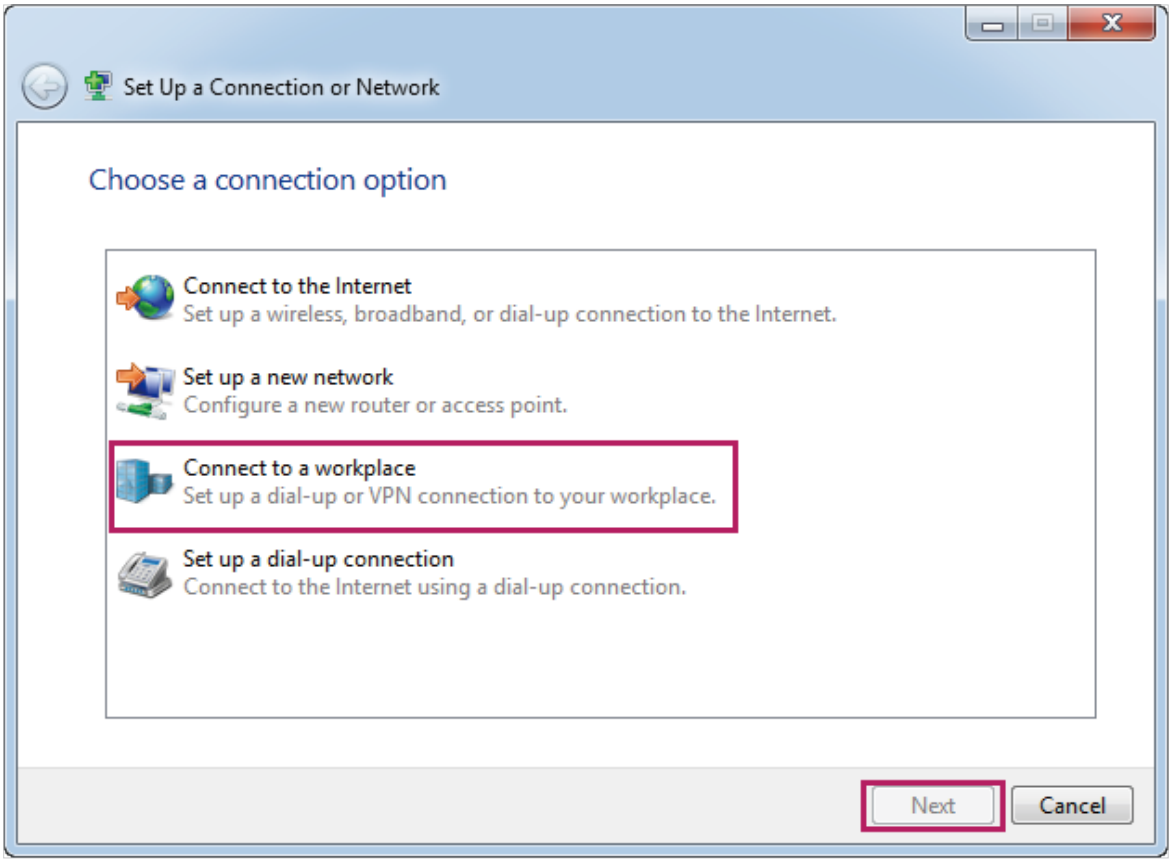
Name	Specify the name for the virtual server list entry. Here we enter **L2TP**.
Interface	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the external port and internal port as **1701**.
Internal Server IP	Specify the internal server IP as **172.16.10.2.** This should be the WAN IP address of the VPN server.
Protocol	Specify the protocol as **UDP**.
Status	Enable the virtual server list entry.

3.3.3 Configuring the L2TP VPN Client Software

Here we use the built-in VPN client software in Windows7 Operating System on the remote host. To configure the VPN client software, follow these steps.

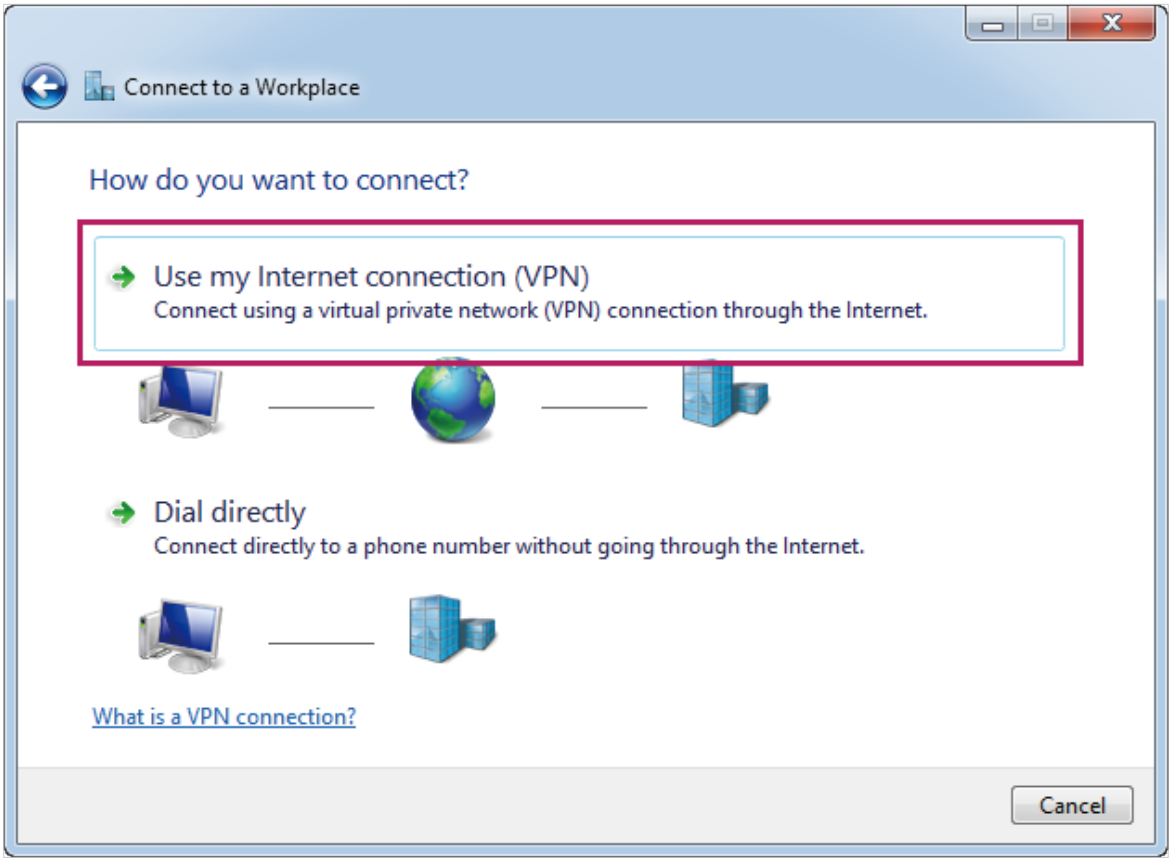
1) In Windows Control Panel, choose the menu **Network and Internet > Network and Sharing Center**. Click **Set up a new connection or network** to load the following page.

Figure 3-22 Configuring the L2TP VPN client



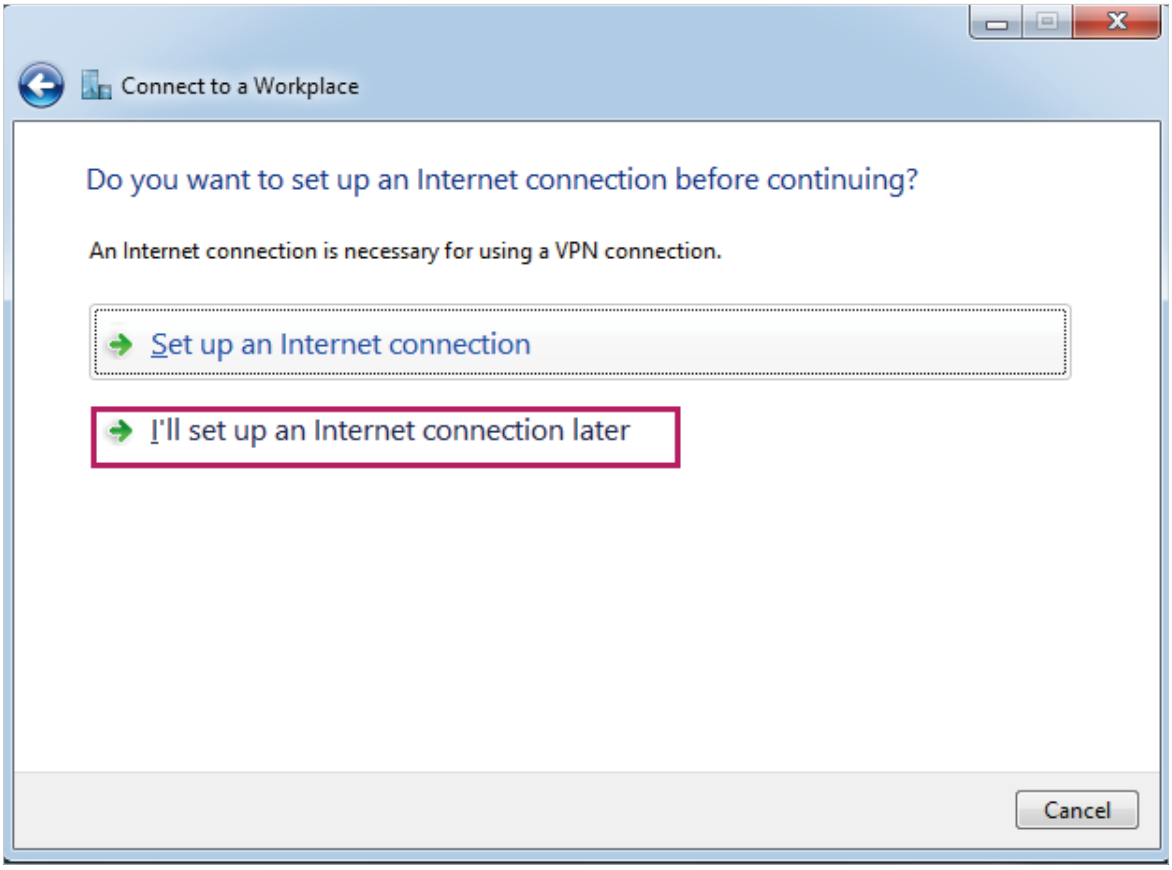
2) Click **Connect to a workplace** and click **Next** to load the following page.

Figure 3-23 Configuring the L2TP VPN client



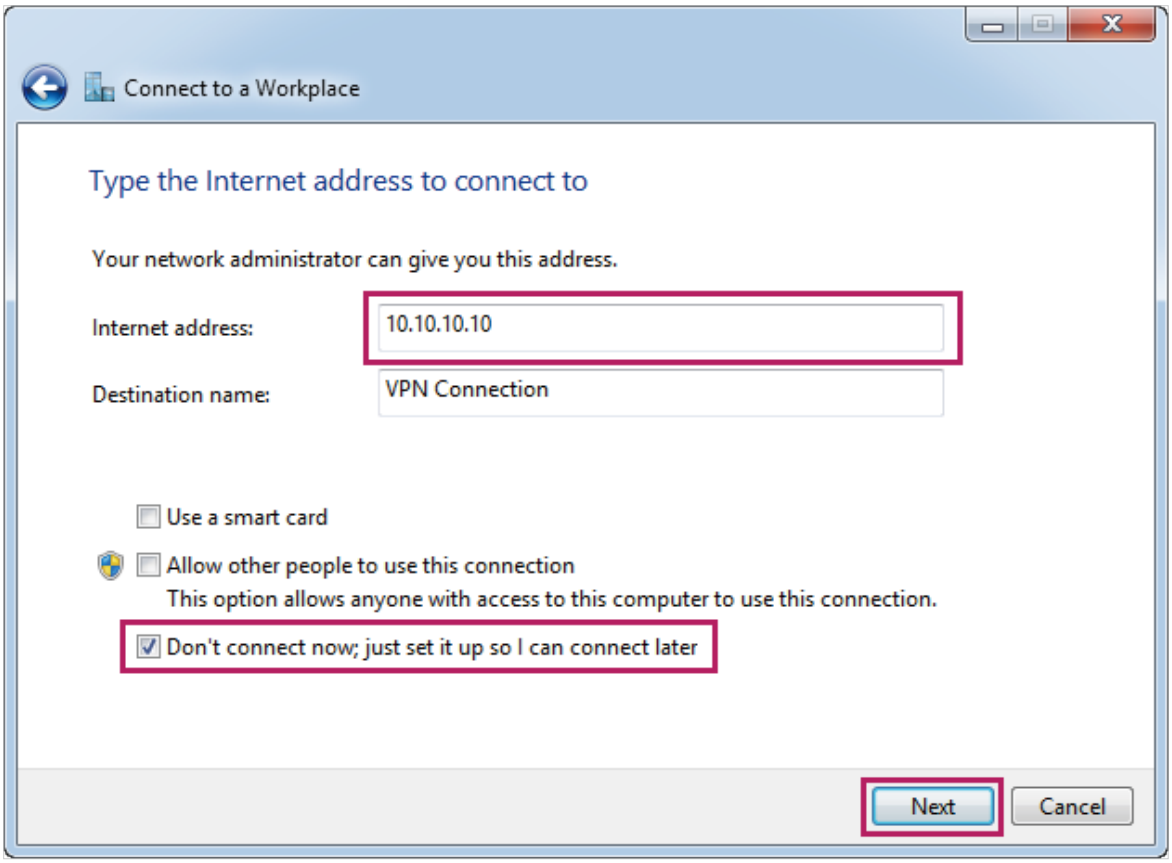
3) Click **Use my Internet connection (VPN)** to load the following page.

Figure 3-24 Configuring the L2TP VPN client



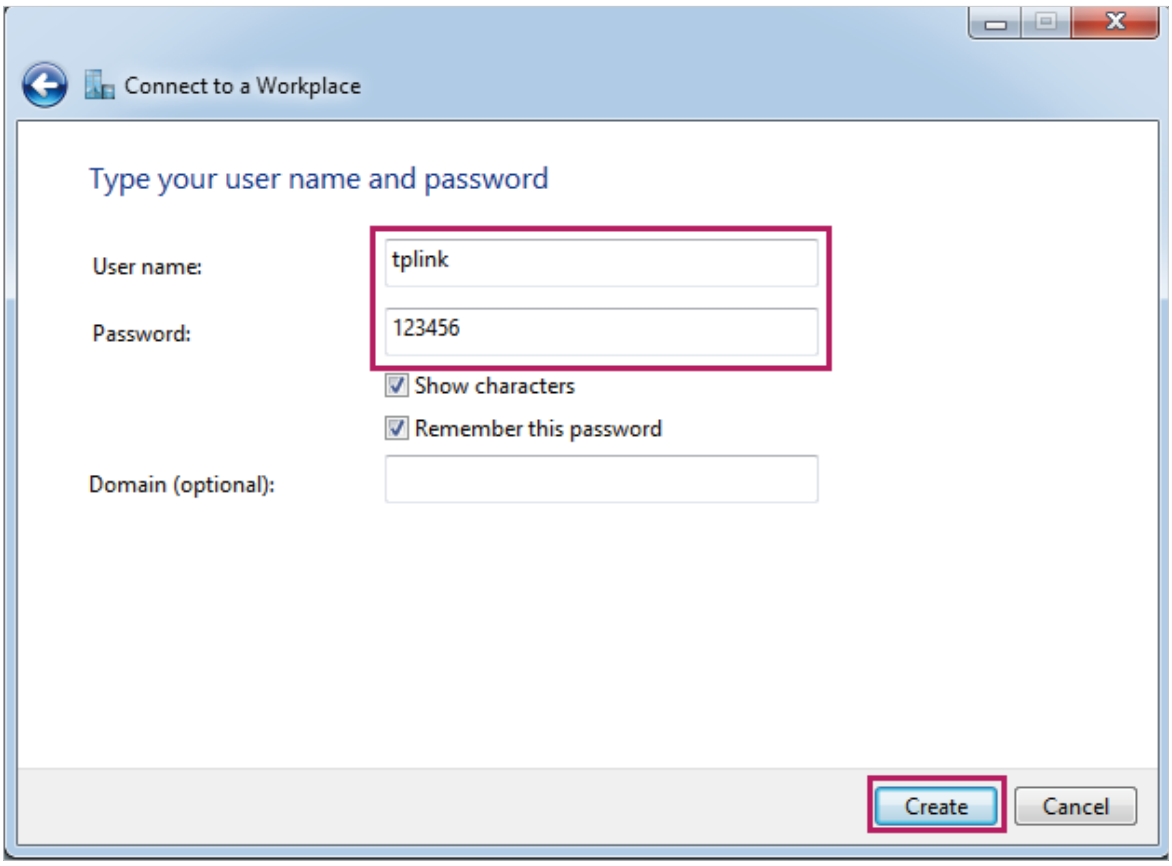
4) Click **I'll set up an Internet connection later** to load the following page. Specify the internet address as 10.10.10.10. Check **Don't connect now, just set it up so I can connect later**.

Figure 3-25 Configuring the L2TP VPN client



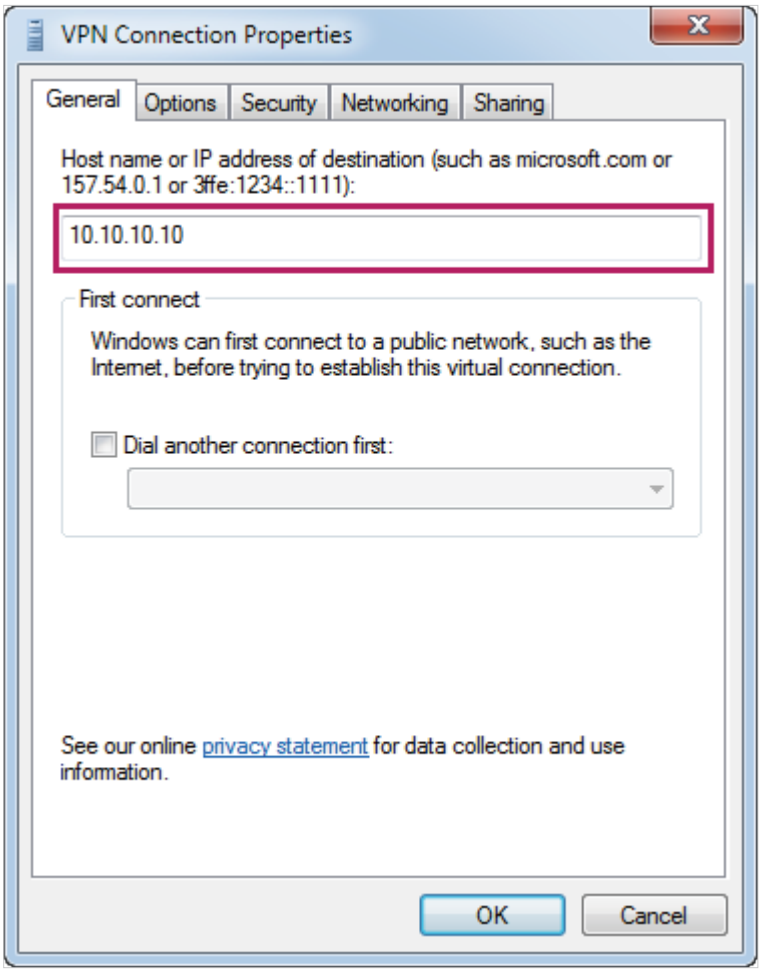
5) Click **Next** to load the following page. Specify the User name as **tplink** and Password as **123456**. This should be the same as the VPN server configuration. Click **Create**.

Figure 3-26 Configuring the L2TP VPN client



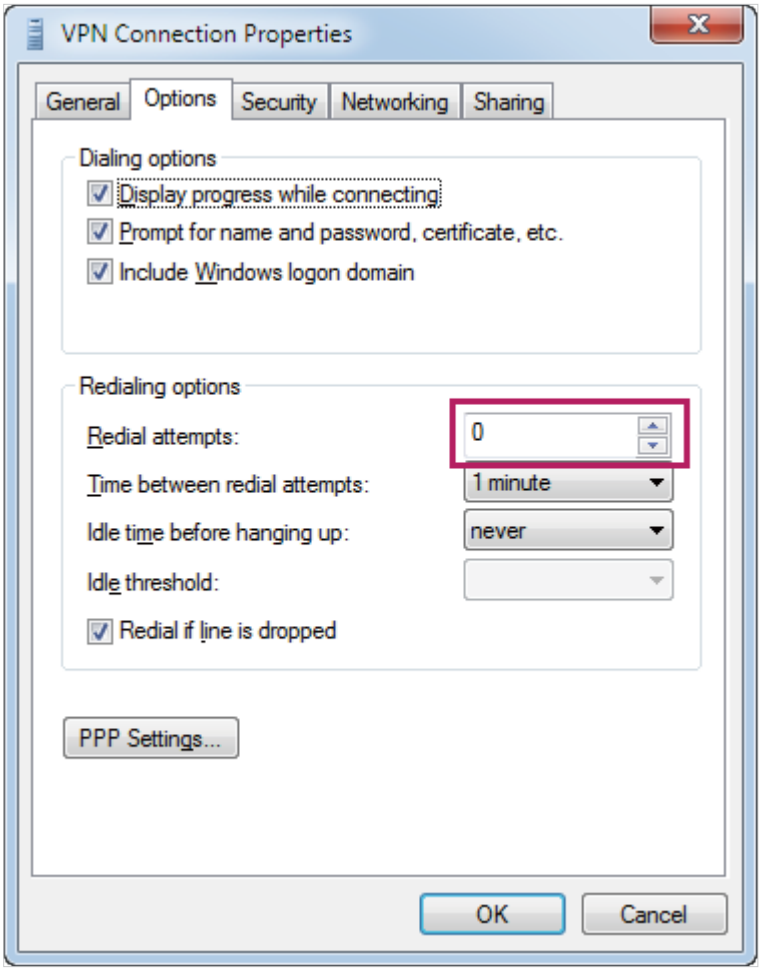
6) In Windows Control Panel, choose the menu **Network and Internet > Network and Sharing Center**. Click **Change adapter settings**. Right click **VPN Connection** and click **Properties** to load the following page. Specify the host name or IP address of destination as **10.10.10.10**.

Figure 3-27 Configuring the L2TP VPN client



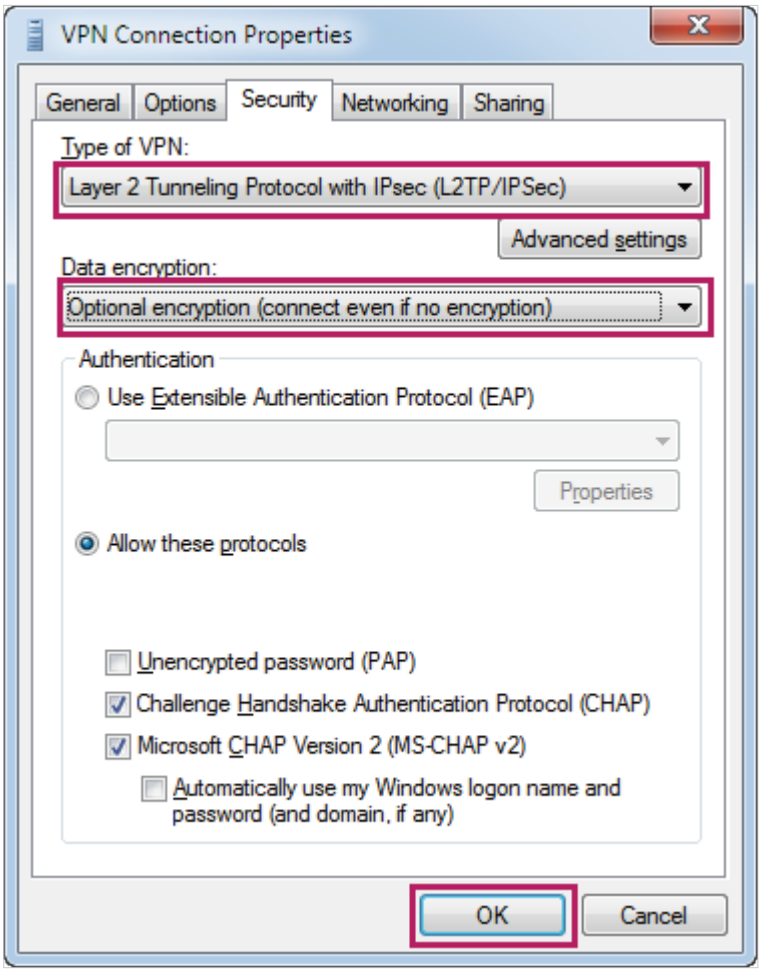
7) Choose the menu **Options** to load the following page. Specify Redial attempts as **0**.

Figure 3-28 Configuring the L2TP VPN client



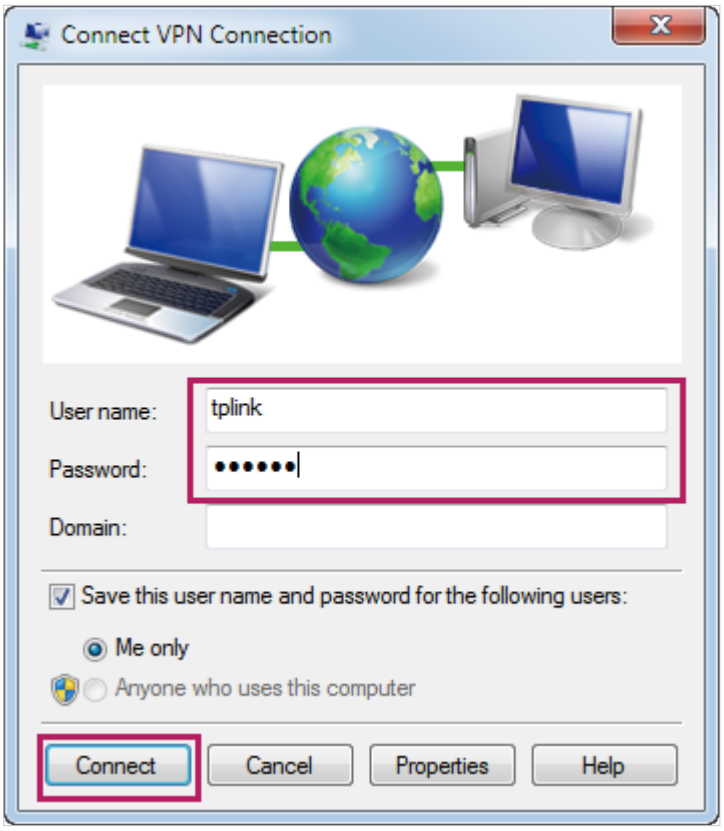
8) Choose the menu **Security** to load the following page. Select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)** as the type of VPN from the drop-down list. Select **Optional encryption (connect even if no encryption)** as data encryption from the drop down list. Click **OK**.

Figure 3-29 Configuring the L2TP VPN client



9) Right click **VPN Connection** and click **Connect** to load the following page. Specify the User name as **tplink**, and the Password as **123456**. This should be the same as the VPN server configuration. Click **Connect** to establish the VPN tunnel.

Figure 3-30 Configuring the L2TP VPN client



3.3.4 Verifying the Connectivity of the L2TP VPN Tunnel

Choose the menu **VPN > L2TP > Tunnel List** to load the following page.

Figure 3-31 L2TP tunnel list

Tunnel List

Refresh

ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	tplink	Server	---	172.31.1.16	10.10.10.20	172.16.10.100	---

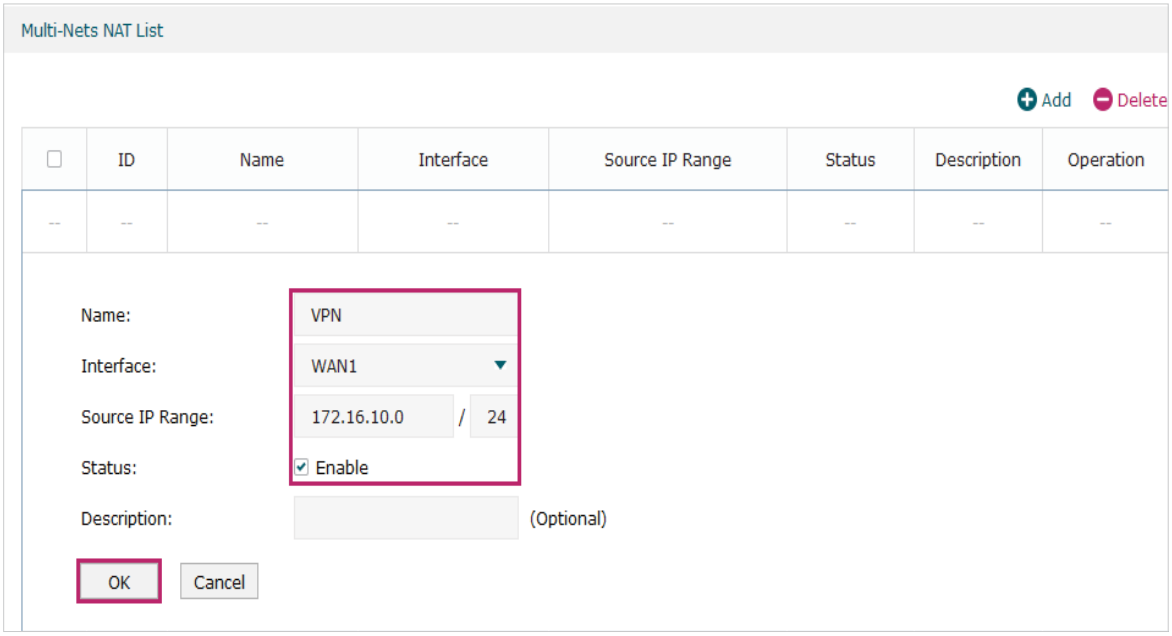
The tunnel list shows the information about the established VPN tunnel. Here, you can verify the connectivity of the L2TP VPN tunnel.

3.3.5 (Optional) Configuring Access to the Internet via Proxy Gateway.

In this scenario, the remote host accesses the internet via the VPN router, and the VPN router acts as a proxy gateway. To meet this demand, please configure Multi-Nets NAT on the VPN router, and configure **Use default gateway on remote network** on the remote host.

1) For the VPN Router, choose the menu **Tansmission > NAT > Multi-Nets NAT** and click **Add** to load the following page. Configure the parameters for Multi-Nets NAT. Click **OK**.

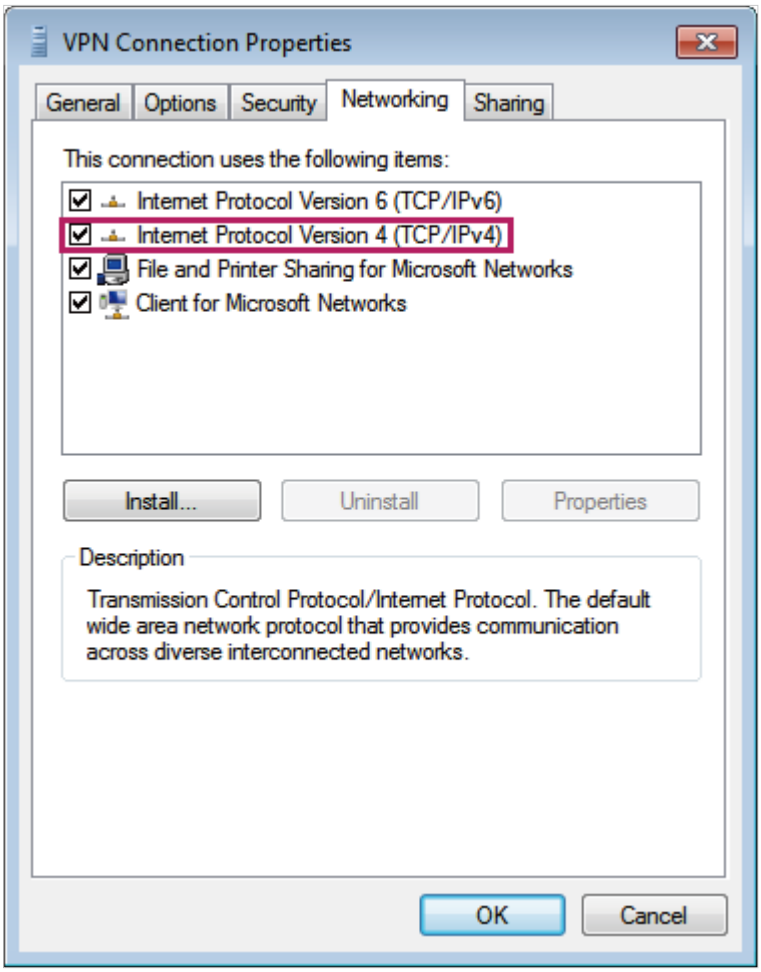
Figure 3-32 Configuring Multi-Nets NAT



Name	Specify the name for the Multi-Nets NAT list entry. Here we enter **VPN**.
Interface	Specify the interface as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Source IP Range	Specify the source IP range as **172.16.10.0/24**. This should include the VPN IP pool configured for the VPN router.
Status	Enable the Multi-Nets NAT list entry.

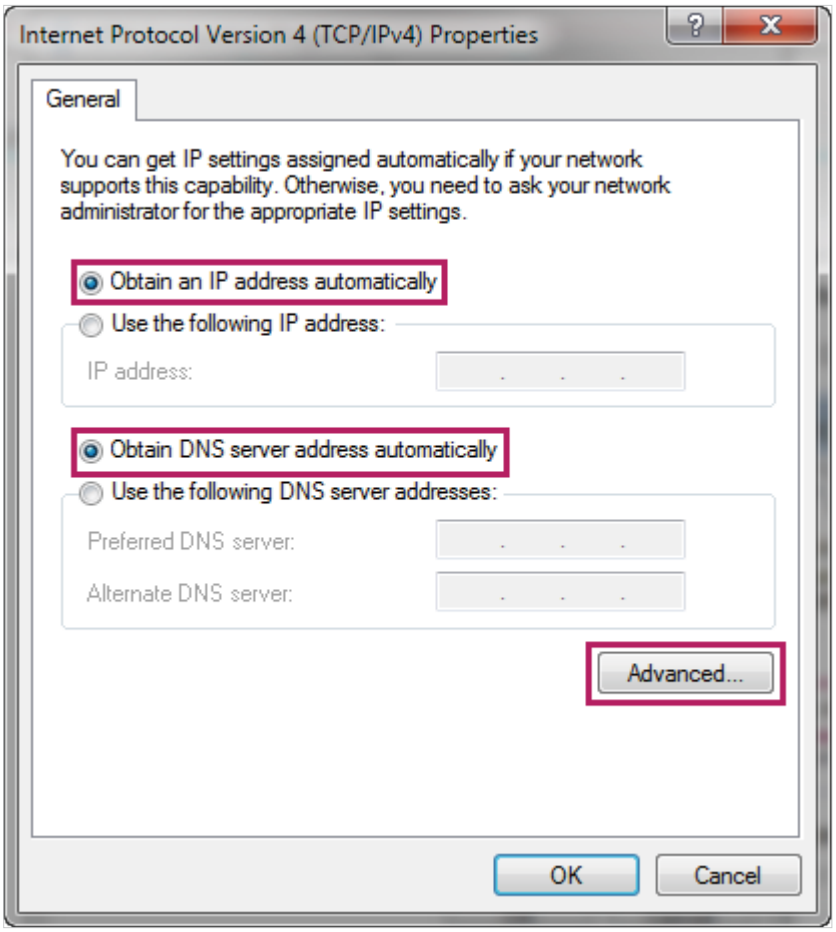
2) For the remote host, choose the menu **Network and Internet > Network and Sharing Center** in Windows Control Panel. Click **Change adapter settings**. Right click **VPN Connection** and click **Properties**. Choose the menu **Networking** to load the following page.

Figure 3-33 Configuring the L2TP VPN client connection properties



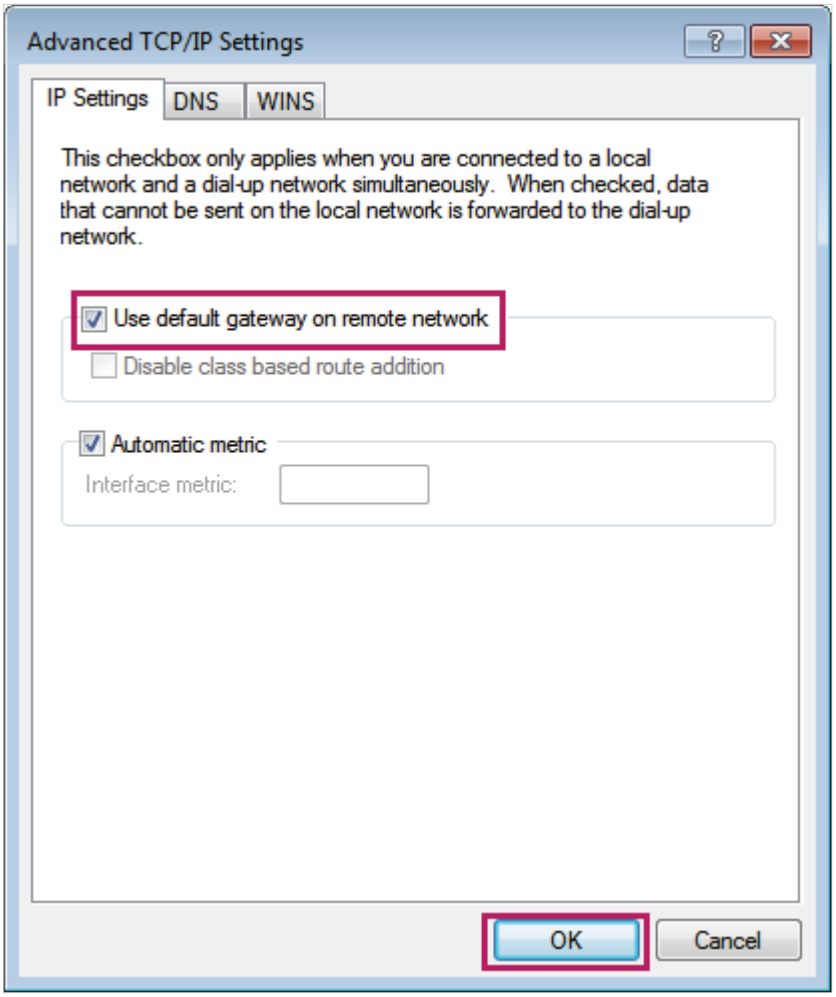
3) Double click **Internet Protocol Version 4 (TCP/IPv4)** to load the following page. Select **Obtain an IP address automatically** and select **Obtain DNS server address automatically**.

Figure 3-34 Configuring the L2TP VPN client connection properties



4) Click **Advanced** to load the following page. Please check **Use default gateway on remote network**. Click **OK**.

Figure 3-35 Configuring the L2TP VPN client connection properties



3.4 PPTP Client-to-LAN VPN Configuration

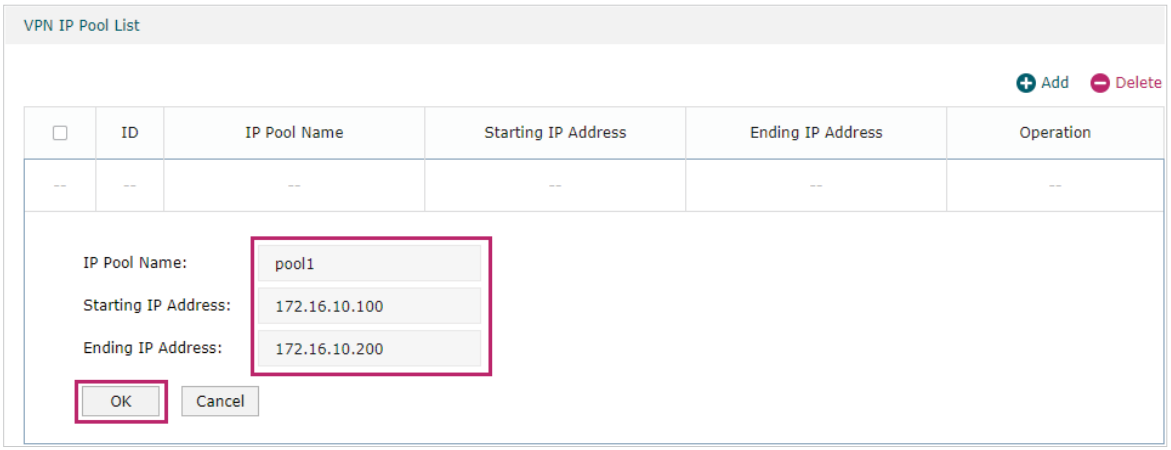
To complete the PPTP Client-to-LAN VPN, follow these steps:

1) Configure PPTP VPN server.
2) (Optional) Implement configuration for NAT devices.
3) Configure the PPTP VPN client software.
4) Verify the connectivity of the PPTP VPN tunnel.
5) (Optional) Configure access to the internet via proxy gateway.

3.4.1 Configuring PPTP VPN Server

1) For the VPN router, choose the menu **Preferences > VPN IP Pool > VPN IP Pool** and click **Add** to load the following page. Configure the parameters for the VPN IP pool. Click **OK**.

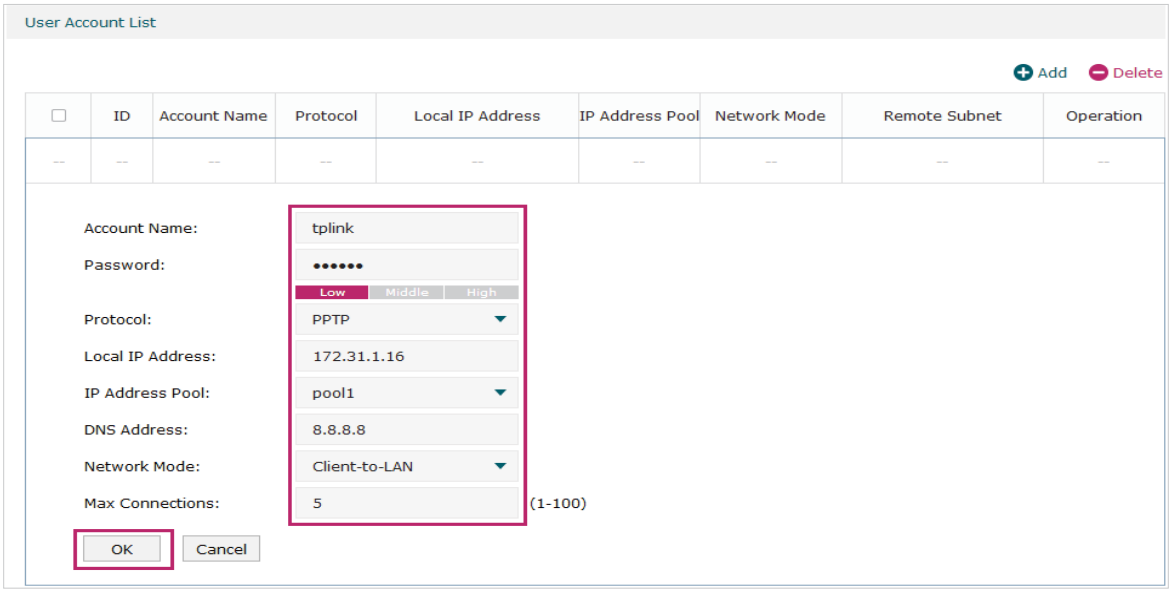
Figure 3-36 Configuring VPN IP pool list



IP Pool Name	Specify the IP pool name as you like. Here we enter **pool1.**
Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address for the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause conflict. Here we specify the starting IP address as **172.16.10.100** and the ending IP address as **172.16.10.200.**

2) Choose the menu **VPN > Users > Users** and click **Add** to load the following page. Configure the parameters for the PPTP user account. Click **OK**.

Figure 3-37 Configuring PPTP users

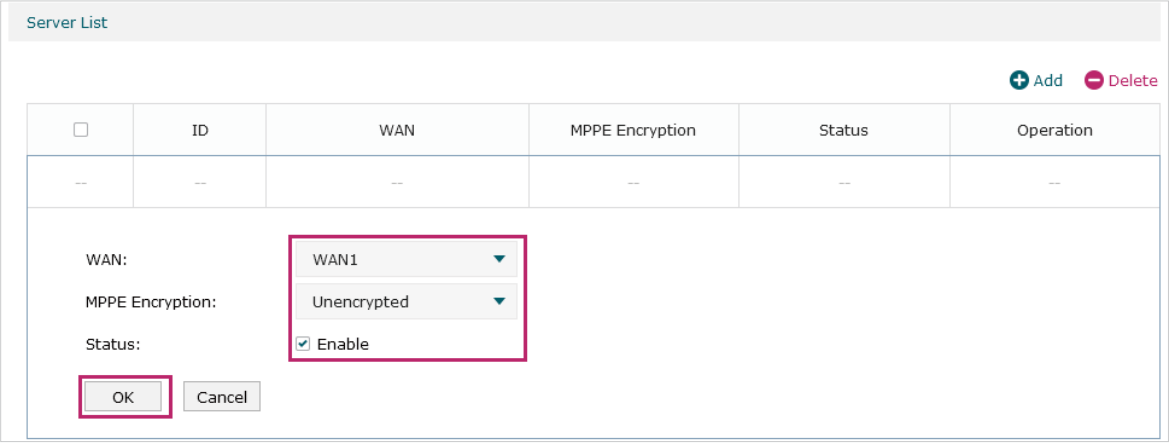


Account Name	Specify the account name as you like. Here we enter **tplink**.

Password	Specify the password as you like. Here we enter **123456**.
Protocol	Specify the protocol as **PPTP.**
Local IP Address	This is the virtual IP address which the remote host will set up a point-to-point connection with. You can specify any reasonable IP address that will not cause conflict. Here we specify the local IP address as **172.31.1.16**.
IP Address Pool	Select **pool1** as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote host. Here we enter **8.8.8.8.**
Network Mode	Specify the network mode as **Client-to-LAN**.
Max Connections	Specify the max connections according to your needs. Here we specify max connections as 5.

3) Choose the menu **VPN > PPTP > PPTP Server** and click **Add** to load the following page. Configure the parameters for the PPTP server. Click **OK**.

Figure 3-38 Configuring PPTP server



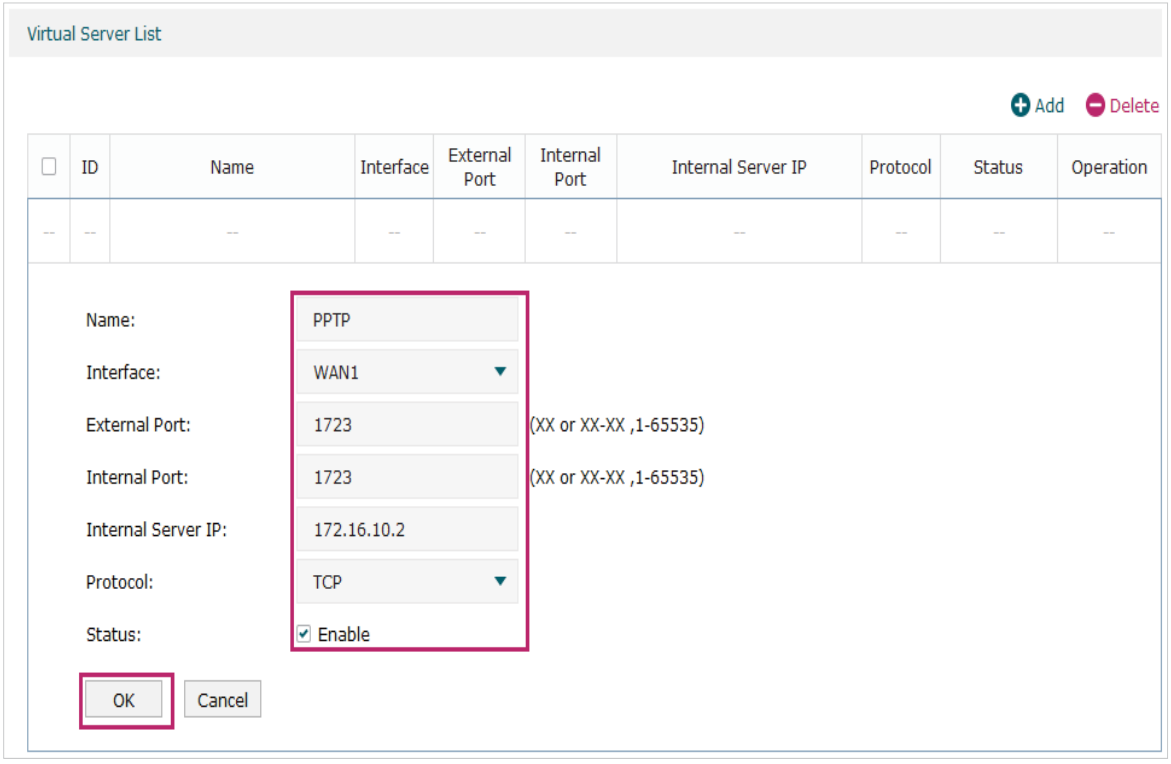
WAN	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
MPPE Encryption	Specify the MPPE encryption according to your needs. Here we specify the MPPE encryption as **Unencrypted**.
Status	Enable the PPTP server.

3.4.2 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 3-2. In this scenario, please configure virtual servers on the NAT device, and configure PPTP ALG on both the NAT device and the remote gateway. The configuration steps are as follows.

1) For the NAT device, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page. Configure the parameters for the virtual server. Click **OK**.

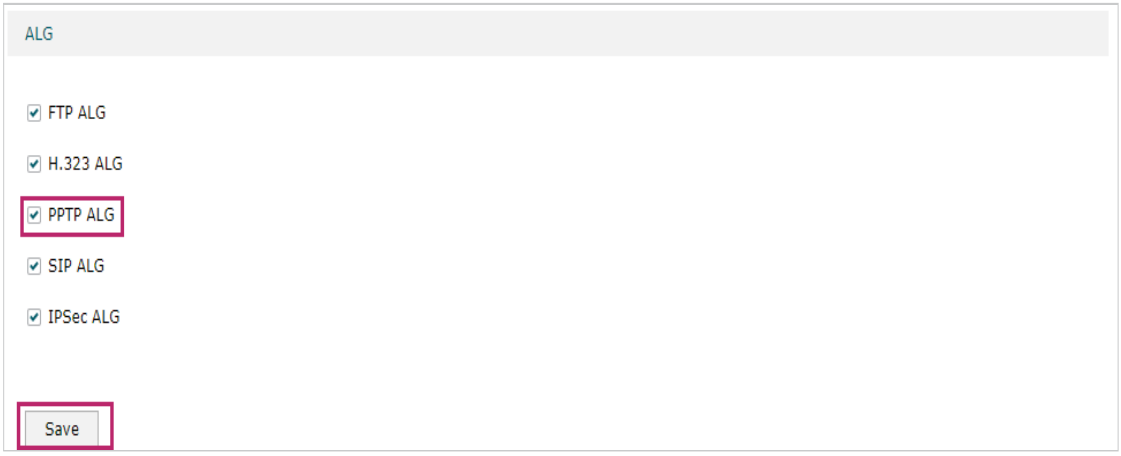
Figure 3-39 Configuring virtual server for PPTP



Name	Specify the name for the virtual server list entry. Here we enter **PPTP**.
Interface	Specify WAN as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the external port and internal port as **1723**.
Internal Server IP	Specify the internal server IP as **172.16.10.2.** This should be the WAN IP address of the VPN server.
Protocol	Specify the protocol as **TCP**.
Status	Enable the virtual server list entry.

2) For the remote gateway and the NAT device, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable PPTP ALG, and click **Save**.

Figure 3-40 Configuring PPTP ALG

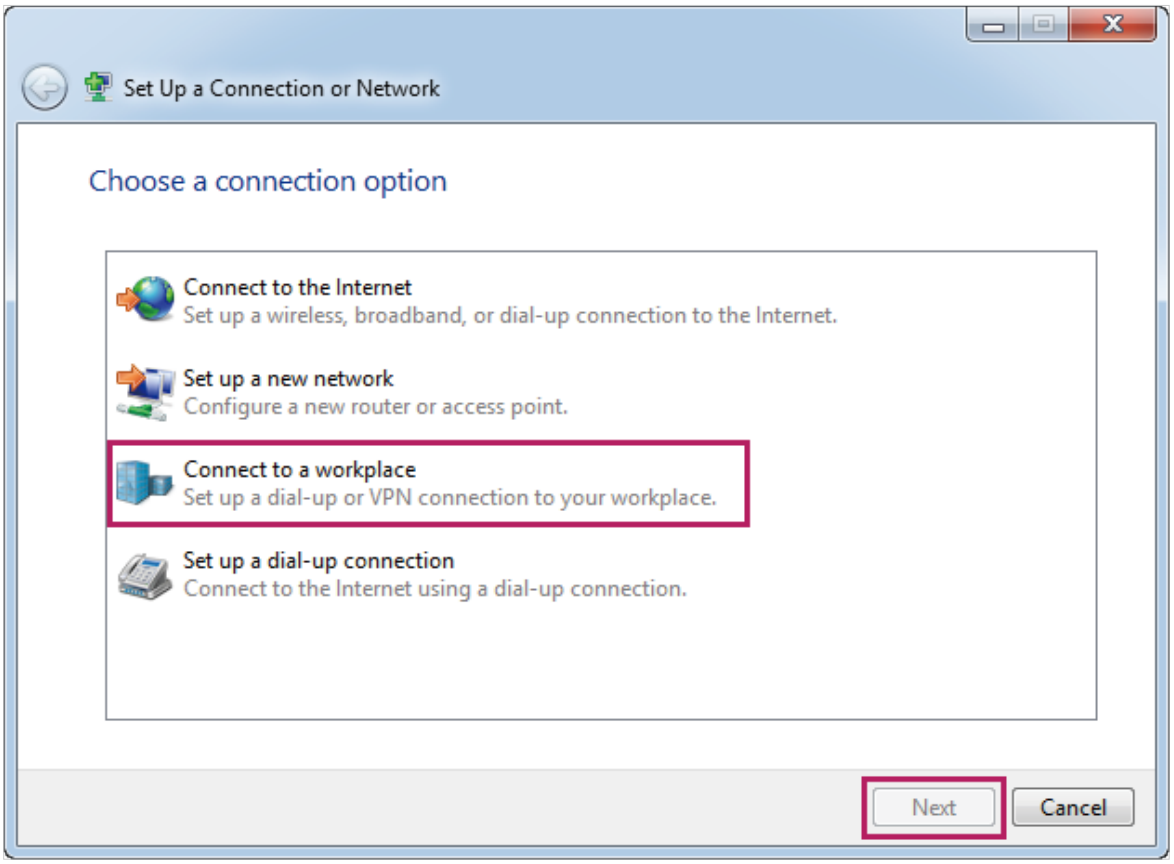


3.4.3 Configuring the PPTP VPN Client Software

Here we use the built-in VPN client software in Windows7 Operating System on the remote host. To configure the VPN client software, follow these steps.

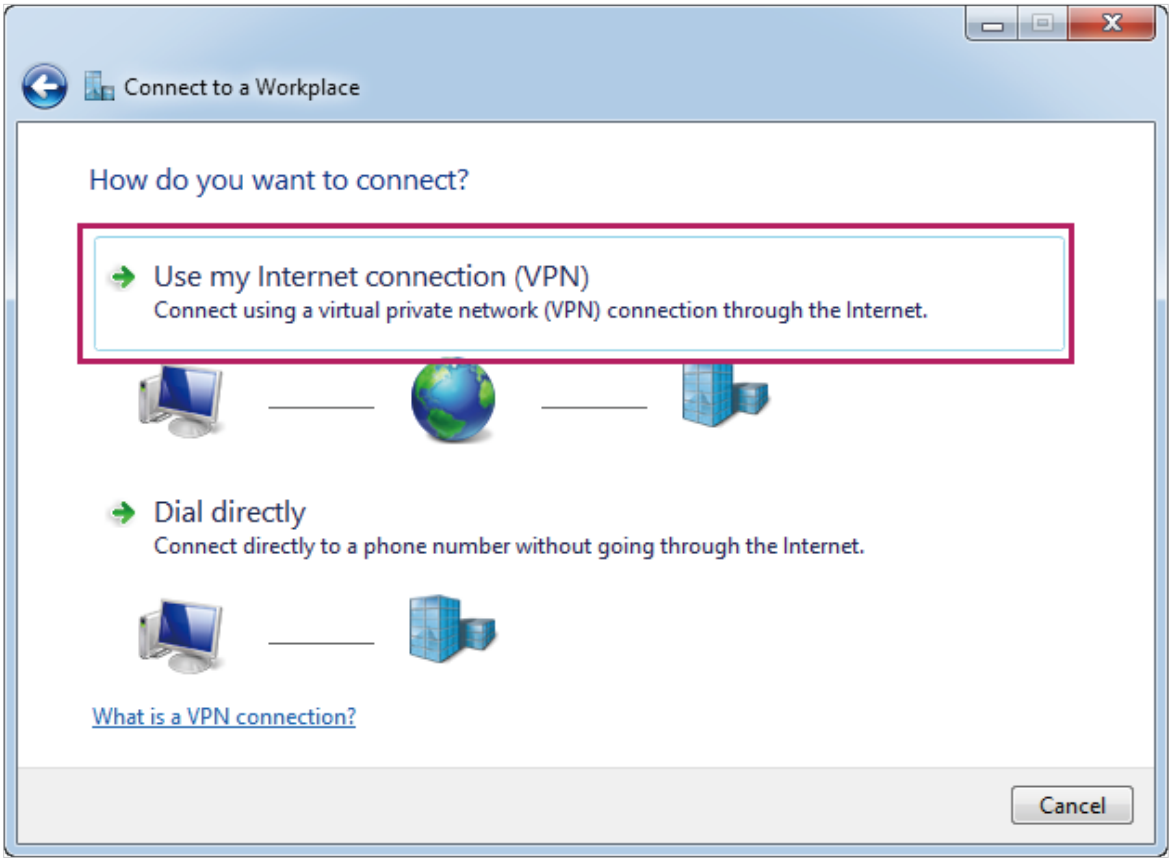
1) In Windows Control Panel, choose the menu **Network and Internet > Network and Sharing Center**. Click **Set up a new connection or network** to load the following page.

Figure 3-41 Configuring the PPTP VPN client



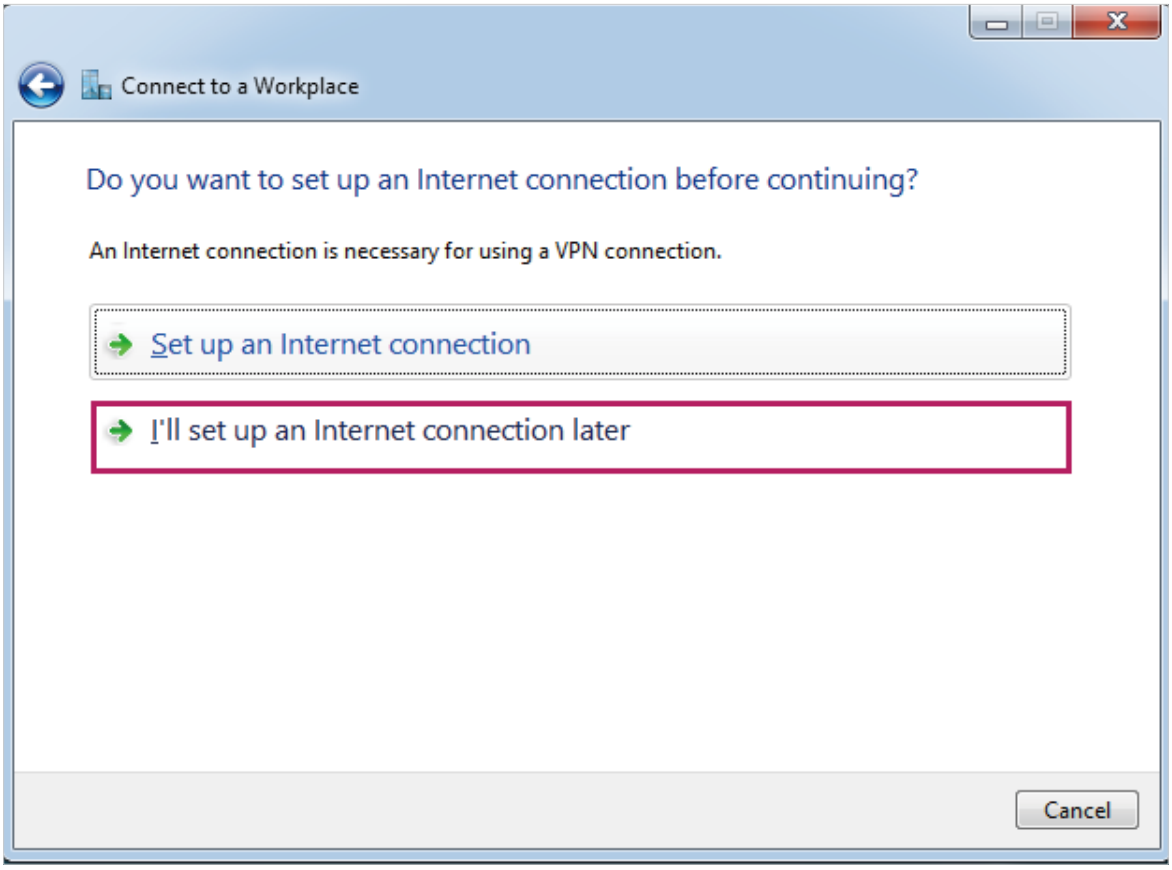
2) Click **Connect to a workplace** and click **Next** to load the following page.

Figure 3-42 Configuring the PPTP VPN client



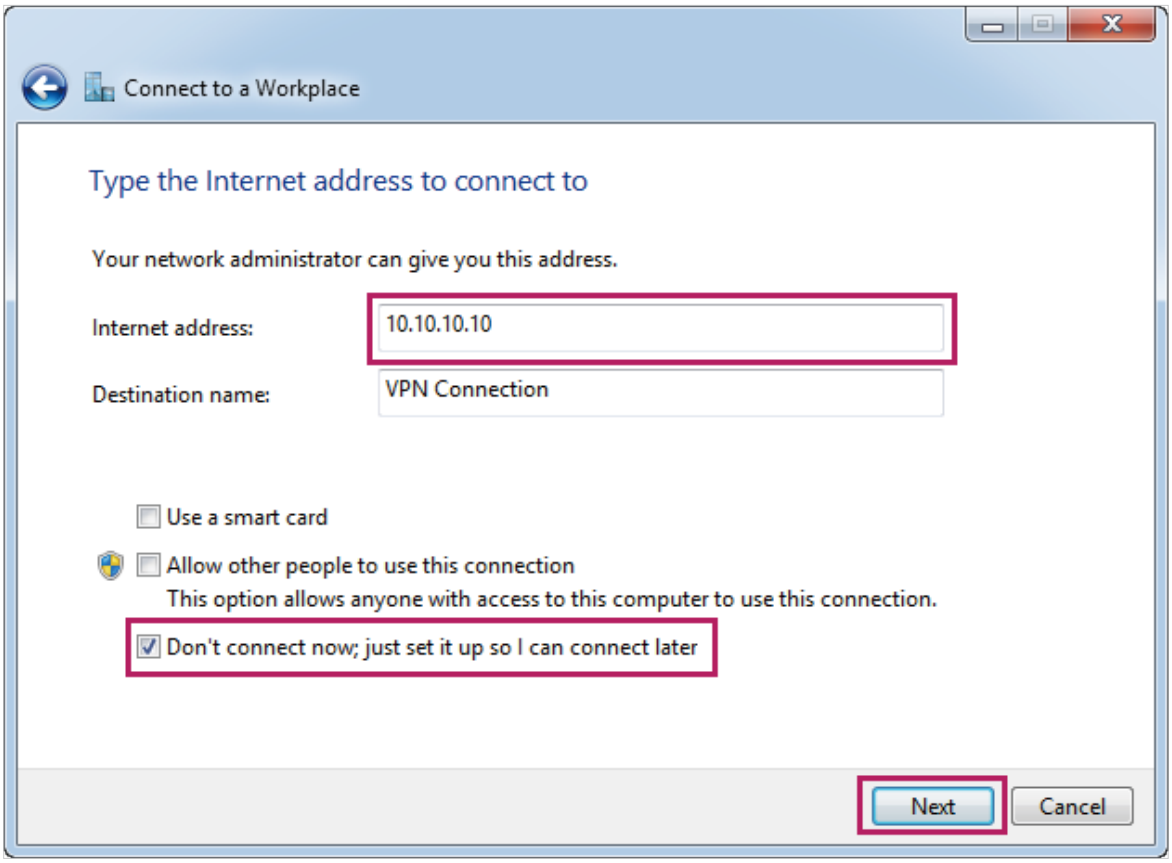
3) Click **Use my Internet connection (VPN)** to load the following page.

Figure 3-43 Configuring the PPTP VPN client



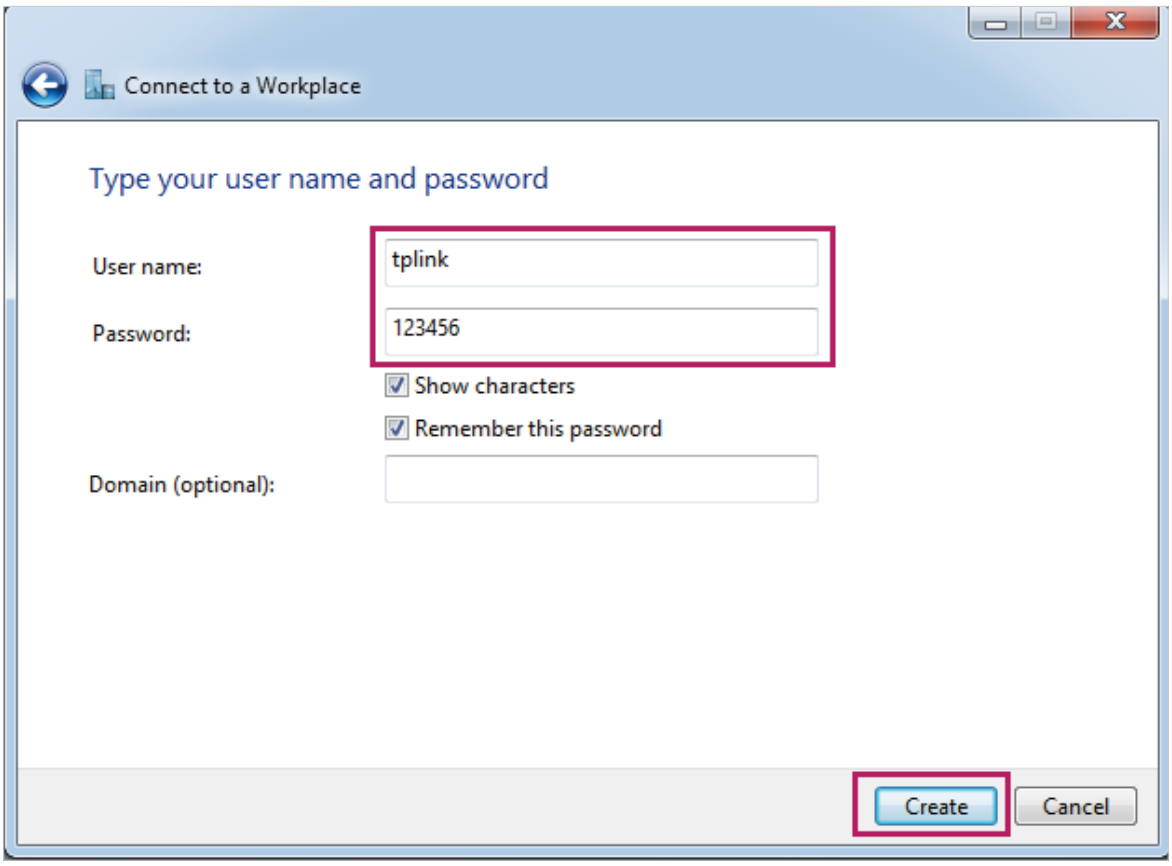
4) Click **I'll set up an Internet connection later** to load the following page. Specify the internet address as **10.10.10.10**. Check **Don't connect now, just set it up so I can connect later**.

Figure 3-44 Configuring the PPTP VPN client



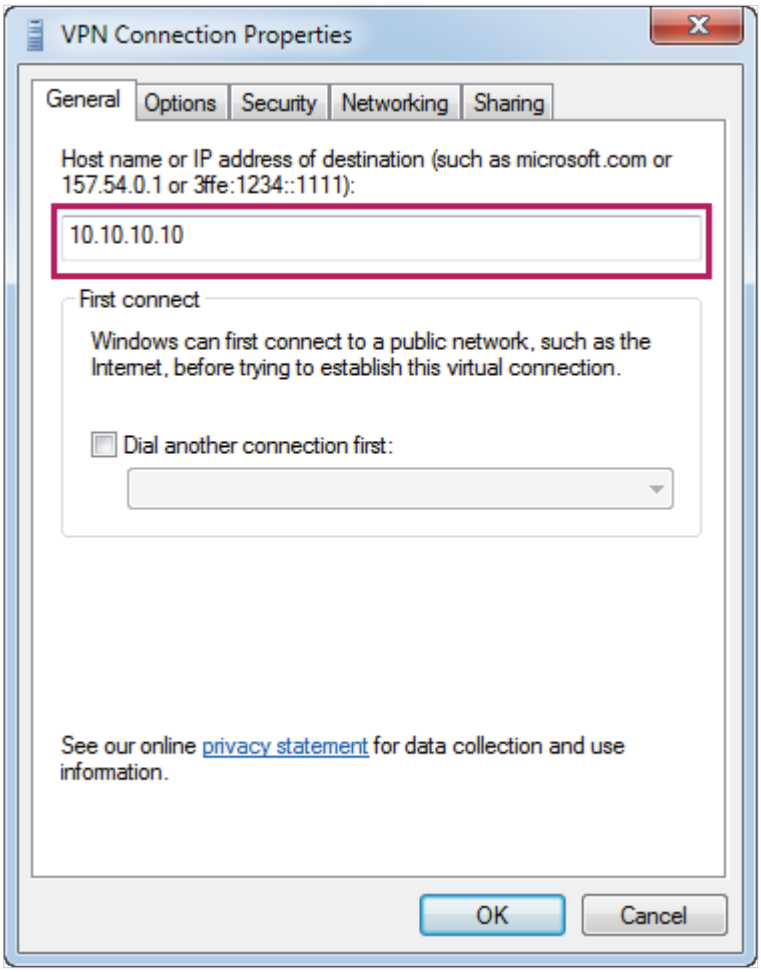
5) Click **Next** to load the following page. Specify the user name as **tplink** and password as **123456**. This should be the same as VPN server configuration. Then click **Create**.

Figure 3-45 Configuring the PPTP VPN client



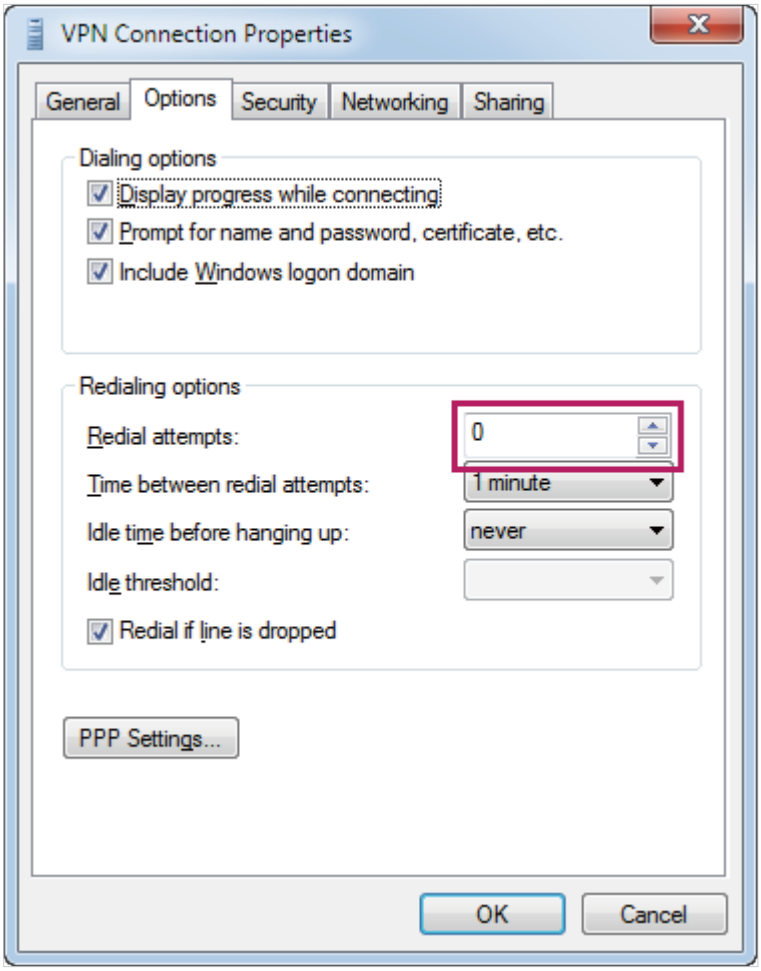
6) In Windows Control Panel, choose the menu **Network and Internet > Network and Sharing Center**. Click **Change adapter settings**. Right click **VPN Connection** and click **Properties** to load the following page. Specify the host name or IP address of destination as **10.10.10.10**.

Figure 3-46 Configuring the PPTP VPN client



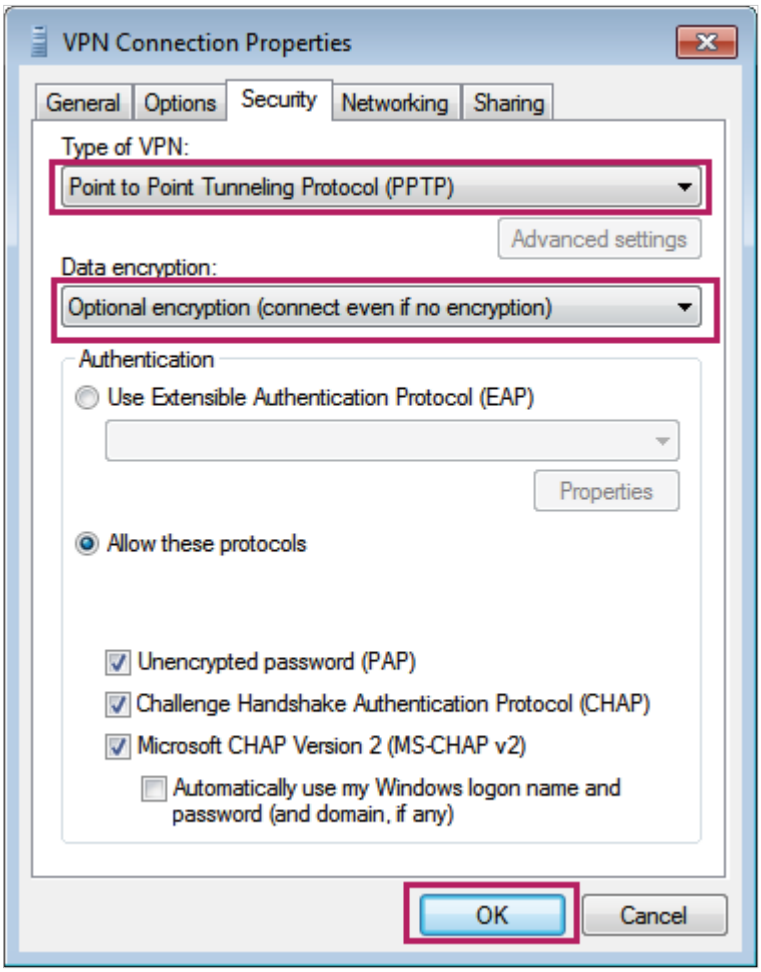
7) Choose the menu **Options** to load the following page. Specify redial attempts as **0**.

Figure 3-47 Configuring the PPTP VPN client



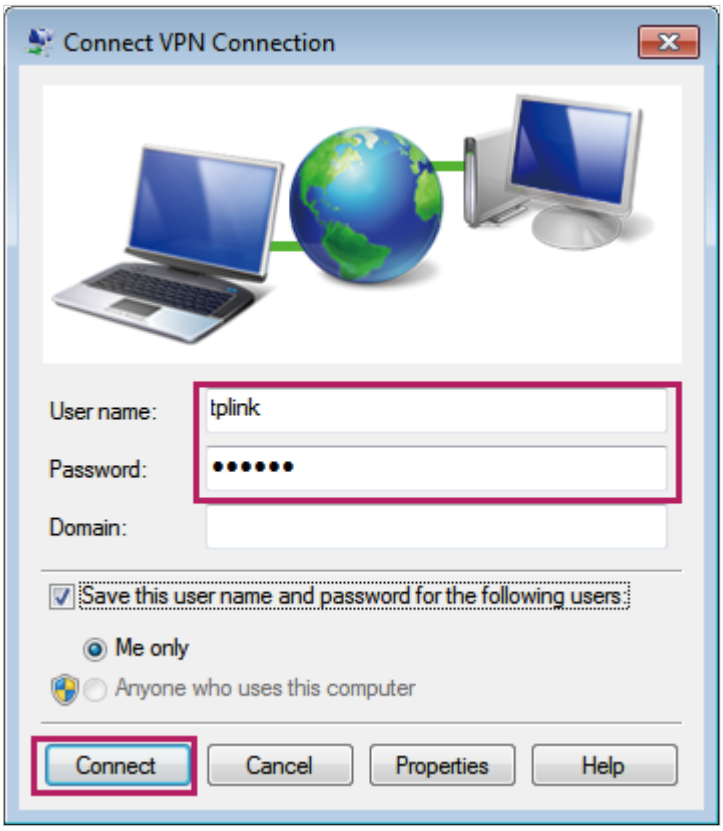
8) Choose the menu **Security** to load the following page. Select **Point to Point Tunnel Protocol (PPTP)** as the type of VPN from the drop-down list. Select **Optional encryption (connect even if no encryption)** as data encryption from the drop down list. Click **OK**.

Figure 3-48 Configuring the PPTP VPN client



9) Right click **VPN Connection** and click **Connect** to load the following page. Specify the user name as **tplink**, and the password as **123456**. This should be the same as the VPN server configuration. Click **Connect** to establish the VPN tunnel.

Figure 3-49 Configuring the PPTP VPN client



3.4.4 Verifying the Connectivity of the PPTP VPN Tunnel

Choose the menu **VPN > PPTP > Tunnel List** to load the following page.

Figure 3-50 PPTP tunnel list

Tunnel List

Refresh

ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	tplink	Server	---	172.31.1.16	10.10.10.20	172.16.10.100	---

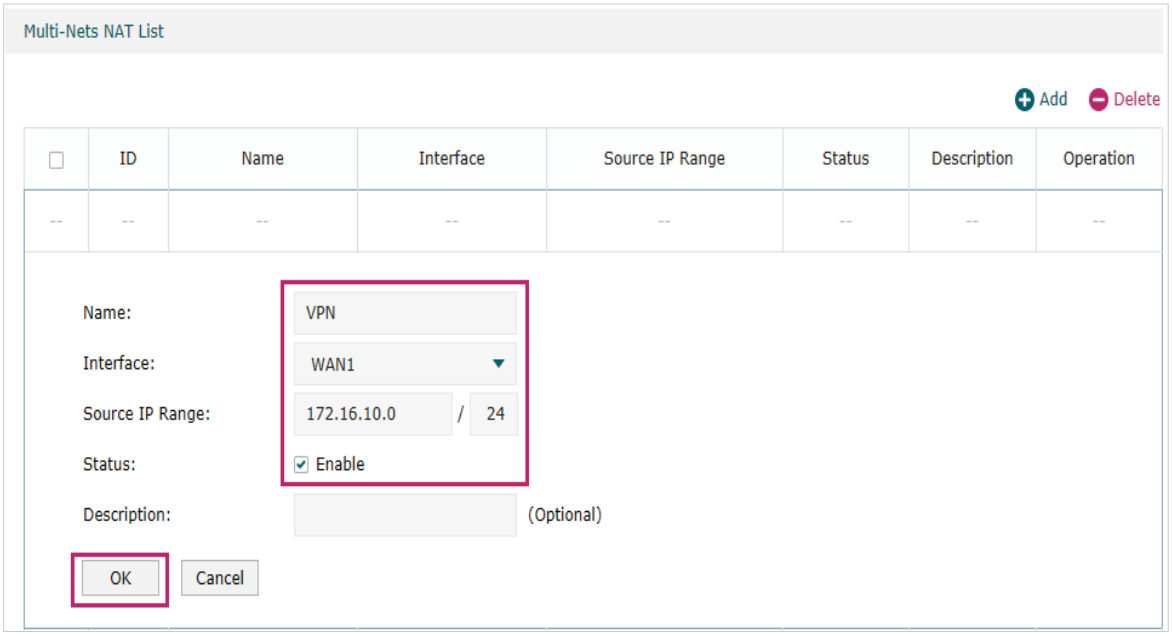
The tunnel list shows the information about the established VPN Tunnel. Here, you can verify the connectivity of the PPTP VPN tunnel.

3.4.5 (Optional) Configuring Access to the Internet via Proxy Gateway.

In this scenario, the remote host access the internet via the VPN router, and the VPN router acts as a proxy gateway. To meet this demand, please configure Multi-Nets NAT on the VPN router, and configure **Use default gateway on remote network** on the remote host.

1) For the VPN router, choose the menu **Tansmission > NAT> Multi-Nets NAT** and click **Add** to load the following page . Configure the parameters for the Multi-Nets NAT. Click **OK**.

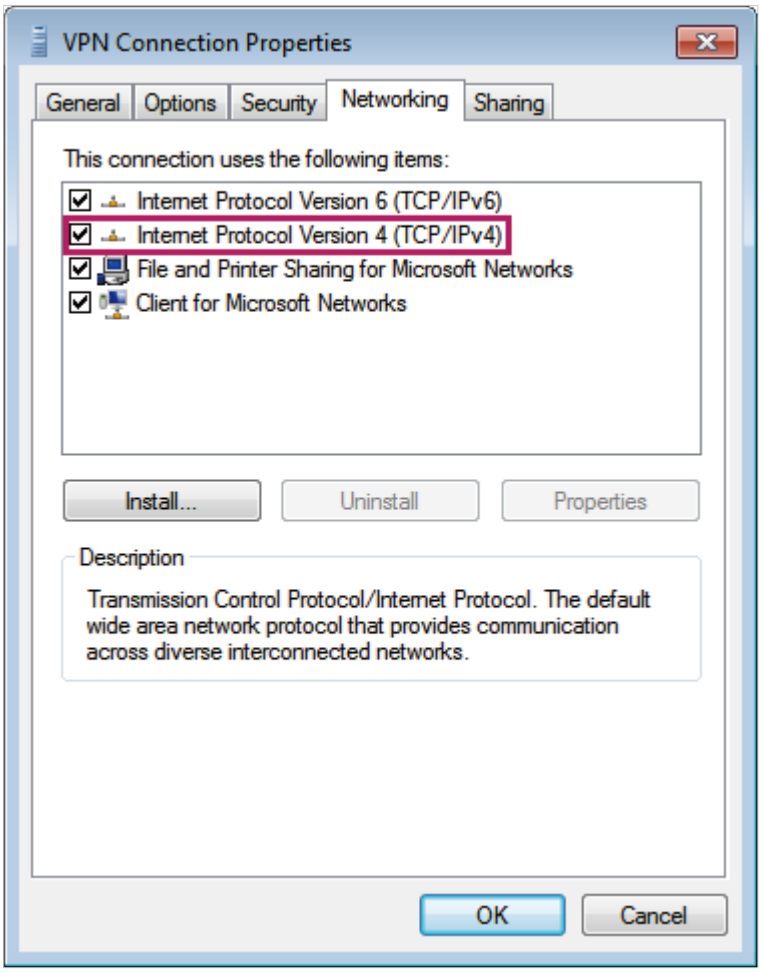
Figure 3-51 Configuring Multi-Nets NAT



Name	Specify the name for the Multi-Nets NAT list entry. Here we enter **VPN**.
Interface	Specify the interface as **WAN1**. This should be the WAN port which the VPN tunnel is established on.
Source IP Range	Specify source IP range as 172.16.10.0/24. This should include the VPN IP pool configured for the VPN router.
Status	Enable the Multi-Nets NAT list entry.

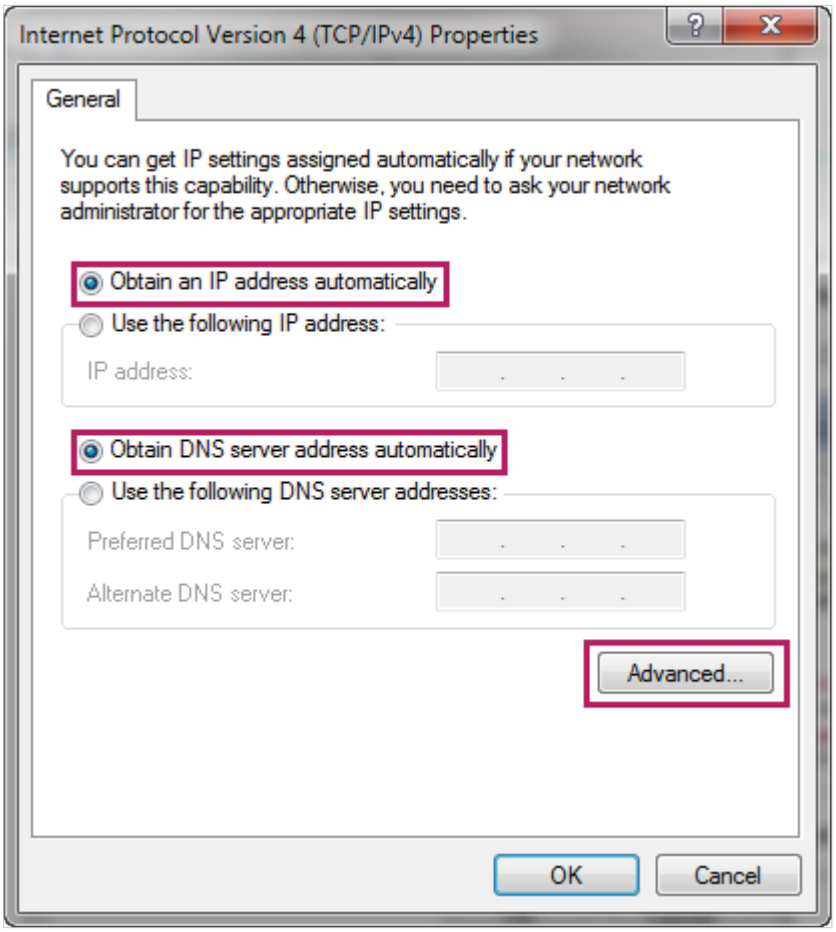
2) For the remote host, choose the menu **Network and Internet > Network and Sharing Center** in Windows Control Panel. Click **Change adapter settings**. Right click **VPN Connection** and click **Properties**, Choose the menu **Networking** to load the following page.

Figure 3-52 Configuring the PPTP VPN client connection properties



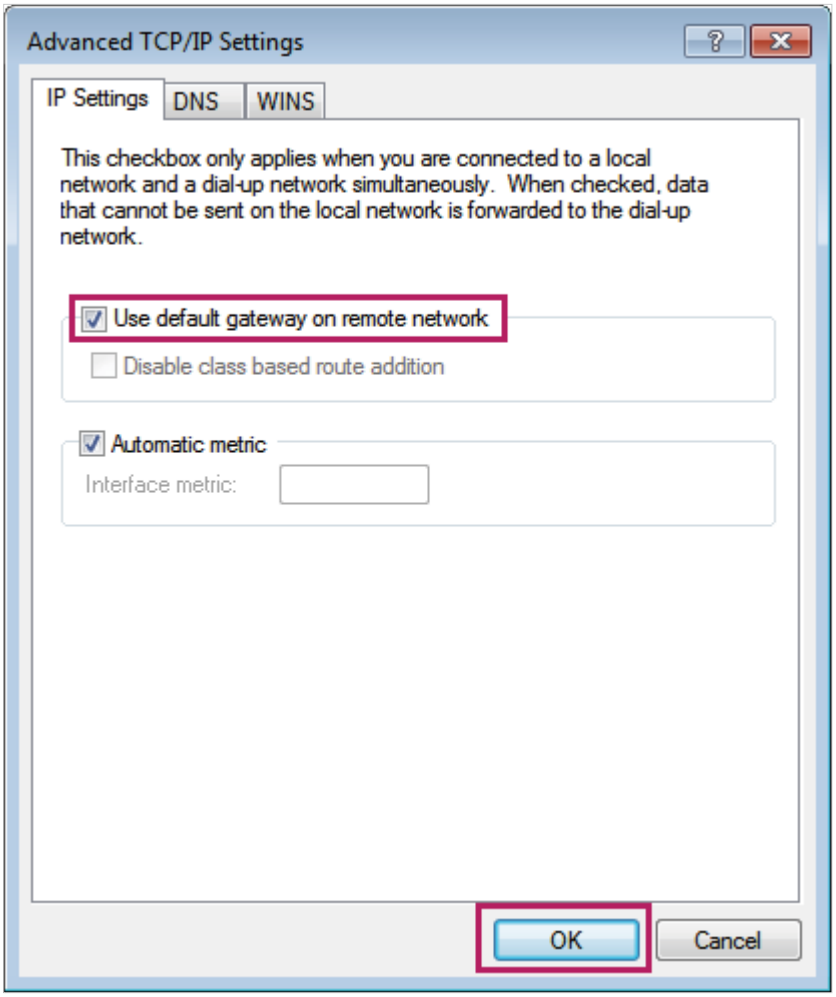
3) Double click **Internet Protocol Version 4 (TCP/IPv4)** to load the following page. Select **Obtain an IP address automatically** and select **Obtain DNS server address automatically**.

Figure 3-53 Configuring the PPTP VPN client connection properties



4) Click **Advanced** to load the following page. Please check **Use default gateway on remote network**. Click **OK**.

Figure 3-54 Configuring the PPTP VPN client connection properties



COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

http://www.tp-link.com